CCNSP

Cyberoam Certified Network & Security Professional

CCNSP Training Handbook

Cyberoam©

Unified Threat Management

TABLE OF CONTENTS

Training & Certification Programs

As network security assumes significance for businesses and investment in security infrastructure grows by the day, the need to validate the knowledge and skills of network security professionals has also grown proportionately.

Cyberoam Certification Program helps these professionals achieve and demonstrate competency in addition to gaining industry recognition for skills in identity-based networking and security as well as in deploying, configuring and managing the Cyberoam CR appliances. With Cyberoam certification, one becomes an expert not just with the current networking and security knowledge, but also with the identity-based security technology that takes future trends into account.

The program consists of two certifications - CCNSP and CCNSE - for which instructor-led training is provided on demand. CCNSP and CCNSE are thoughtfully designed to increase efficiency in maximizing the benefits of Cyberoam appliances not only for customers and partners, but also for the certified professional's career.

CCNSP (Cyberoam Certified Network & Security Professional):

The CCNSP is designed for acquiring expertise necessary for the installation and configuration of all Cyberoam features and functionality. To attain the CCNSP certification, one needs to clear the exam for accreditation after acquiring expertise in Firewalls and VPN, IPS, Anti-Virus and Anti-Spam and trouble shooting.

The CCNSP Training course

- Module 1: Introduction to Cyberoam & Cyberoam USP
- Module 2: Deployment & Multi link Manager
- Module 3: Identity Based Firewall
- Module 4: Authentication & Content filtering
- Module 5: Advance Deployment
- Module 6: Anti-Virus, Anti-Spam
- Module 7: IPS – Intrusion Prevention System
- Module 8: VPN
- Module 9: General Administration & Reports
- Module 10: Trouble Shooting

CCNSE (Cyberoam Certified Network & Security Expert):

The CCNSE exam structure consists of one lab and one exam. Accreditation is achieved based on clearing the exams. The CCNSE professional is certified for product installation, integration, support & management, advanced deployment and advanced troubleshooting. This also helps in bundling services such as technical support and Customised reports.

The CCNSE Training course

- Module 1: Advanced configuration for Cyberoam
- Module 2: Advanced configuration for VPN
- Module 3: Advancde configuration for User Authentication
- Module 4: Advanced configuration for Content Filtering, IPS, Anti--Virus / Anti-Spam
- Module 5: HA configuration
- Module 6: Complex Deployment
- Module 7: Trouble Shooting with Logging
- Module 8: Trouble shooting with Console
- Module 9: Trouble shooting with HTTP Diagnostic tool

To appear in the CCNSE training or certification exam, the individual must have CCNSP certification

Training to Achieve Certification

- These courses include hands-on tasks and real-world scenarios to gain valuable practical experience.
- Access to an up-to-date database of answer to your questions is provided.
- Instructors traverse the globe to deliver training at various centres.
- Instructor led 2-day courses are available with all the hardware necessary for practising.

Benefits of Cyberoam Certification

- Advances your career rapidly
- Certifies your competence and understanding in handling the CR appliance
- Increases your credential in the market as Cyberoam Certified Engineer
- Brings recognition from peers and competitors
- Increases credibility with customers
- Brings a sense of personal accomplishment

How to become CCNSP & CCNSE

For those of you aspiring for the CCNSE certification, you must acquire a prior CCNSP certification. Though you can undertake the certification exams directly without training to achieve the CCNSP and CCNSE certifications, Cyberoam recommends successful completion of the instructor-led training programs for hands-on experience and in-depth understanding of topics

Also, in order to clear the exams for the certifications, you are required to achieve 75% or higher score in the exams.

Cyberoam Online Video Training:

Cyberoam provides online comprehensive free video training program covering all basic modules.

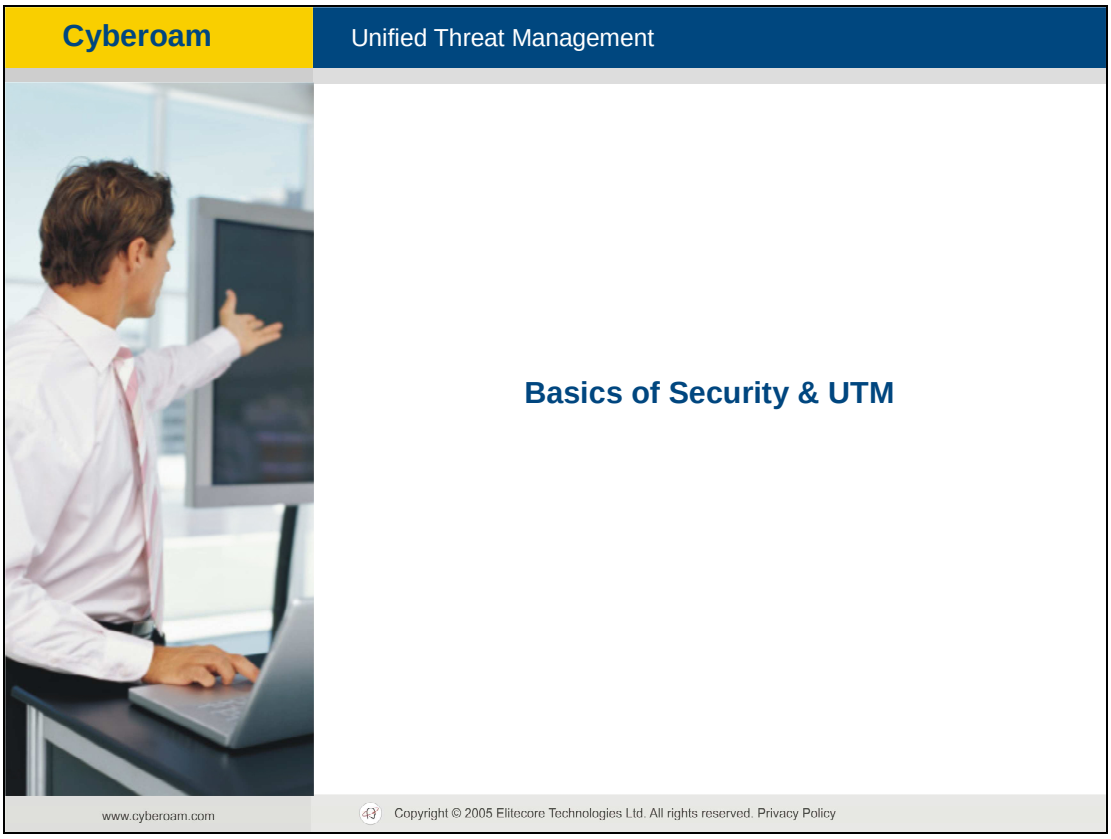
Access detail:

URL: http://connect.elitecore.com/trainingondemand
Username: online.video@cyberoam.com
Password: onlinevideo

Training Contact Details:

USA Toll Free: +1-877-380-8531
India Toll Free: +1-800-301-00013
EMEA / APAC: +91-79-66065777
Email: training@cyberoam.com

Module 1: Basics of Networking & Security

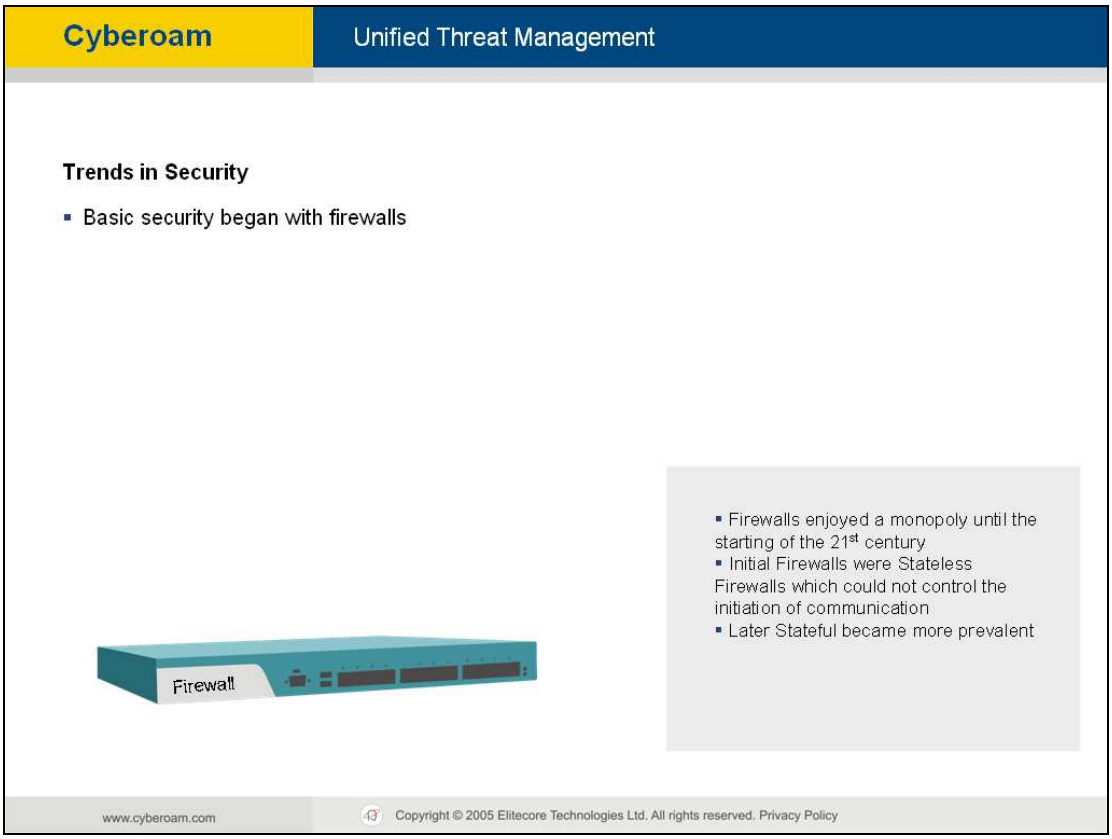


Agenda:

- Basics of Security & UTM(Unified Threat Management)

Basics of Security & UTM (Unified Threat Management):

Before understanding UTM, let's first understand Internet security trends:



Trends in Security: Basic security began with firewalls:

Initial network deployments began protecting networks using a firewall solution and using the firewall to restrict the traffic flow.

A firewall is a device that is part hardware, part software and is used to secure network access.

Types of Firewall:

In the past, an organisation may have had one firewall that protected the edge of the network. Some companies did not have their network attached to the Internet or may have had perhaps one or two stations that would dial up to the Internet or to another computer that they needed to exchange data with. After the late 1990's however, the need for the Internet, its information and e-mail was undeniable.

With the requirement for instantaneous e-mail access, comes the requirement for an always-on Internet connection. At first, companies would place their systems directly on the Internet with a public IP address. This, of course, is not a scalable solution for the long term. With limited IP addresses and unlimited threats, a better solution is required. At first, the border router that connected the Internet medium to the local network was used to provide a simple layer of access control between the two networks. With the need for better security, new types of firewalls were developed to meet the new needs for an Internet-enabled office. Better security, the ability for the firewall to provide more secured segments and the need to thwart newer styles of attacks brought firewalls to where they are today.

Packet Filters:

The most basic firewall technology is the packet filter. A packet filter is designed to filter packets based on source IP, destination IP, source port, destination port, and on a packet-per-packet basis to determine if that packet should be allowed through.

The basic security principles of a packet filter, such as allowing or denying packets based upon IP address, provide the minimum amount of required security. So then, where does the packet filter go wrong? A packet filter cannot determine if the packet is associated with any other packets that make up a session. A packet filter does a decent enough job of protecting networks that require basic security. The packet filter does not look to the characteristics of a packet, such as the type of application it is or the flags set in the TCP portion of the packet. Most of the time this will work for you in a basic security setting, However, there are ways to get around a packet filter. Because the packet filter does not maintain the state of exactly what is happening, it cannot determine the proper return packets that should be allowed through the connection.

For example, if you wanted to permit outbound access to DNS on UDP port 53, you would need to allow access for the return packet as well. A packet filter cannot determine what the return packet will in order to let it in. So now you have to allow access inbound for that DNS entry to return. So its source port would be UDP 53 and the inbound destination port would be the source port, which could be 1024-65535. Now add that up with all of the other applications you need to allow through the firewall and you can see the problem. As the packet filter has no way to dynamically

create an access rule to allow inbound traffic, the packet filter is not effective as a security gateway.

Application Proxy:

Application proxies provide one of the most secure types of access you can have in a security gateway. An application proxy sits between the protected network and the network that you want to be protected from. Every time an application makes a request, the application intercepts the request to the destination system. The application proxy initiates its own request, as opposed to actually passing the client's initial request. When the destination server responds back to the application proxy, the proxy responds back to the client as if it was the destination server. This way the client and the destination server never actually interact directly. This is the most secure type of firewall because the entire packet, including the application portion of the packet, can be completely inspected.

However, this is not dominant technology today for several reasons. The first downfall of the application proxy is performance. Because the application proxy essentially has to initiate its own second connection to the destination system, it takes twice the amount of connections to complete its interaction. On a small scale the slowdown will not be as a persistent problem, but when you get into a high-end requirement for many concurrent connections this is not a scalable technology. Furthermore, when the application proxy needs to interact with all of today's different applications, it needs to have some sort of engine to interact with the applications it is connecting to. For most highly used vanilla applications such as web browsing or HTTP this is not a problem. However, if you are using a proprietary protocol, an application proxy might not be the best solution for you.

Stateful Inspection:

Stateful inspection is today's choice for the core inspection technology in firewalls. Stateful inspection functions like a packet filter by allowing or denying connections based upon the same types of filtering. However, a stateful firewall monitors the "state" of a communication. So, for example, when you connect to a web server and that web server has to respond back to you, the stateful firewall has the proper access open and ready for the responding connection. When the connection ends, that opening is closed. Among the big three names in firewalls today, all of them use this reflexive technology. There are, as mentioned above, protocols such as UDP and ICMP that do not have any sort of state to them. The major vendors recognise this and have to make their own decisions about what exactly constitutes a UDP or ICMP connection. Overall, though, most uses of stateful technology across vendors have been in use for some time and have worked the bugs out of those applications.

Many companies that implement stateful inspection use a more hybrid method between application proxy and stateful inspection when inspecting specific protocols. For example, if you were to do URL filtering on most firewalls, you may need to actually employ application proxy-type techniques to provide the proper inspection. This, much like application proxy firewalls, does not scale and is not a good idea for a large amount of users. Depending on the vendor and function, your mileage may vary.

Cyberoam | Unified Threat Management

Trends in Security

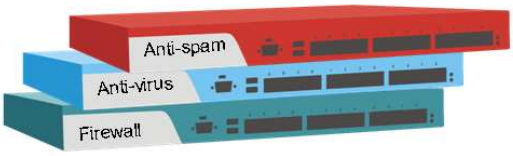
- Basic security began with firewalls
- As threats increased, other solutions were introduced
- Virus attacks rose in number and intensity

- 6 % business emails contained viruses – *IBM*
- That's a staggering cost of $281-$304 per PC
- Email became more prevalent

Cyberoam | Unified Threat Management

Trends in Security

- Basic security began with firewalls
- As threats increased, other solutions were introduced
- Virus attacks rose in number and intensity
- Spam rose



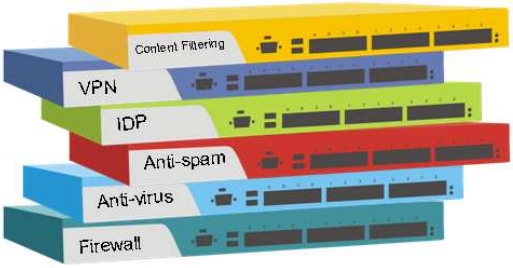
- Average spam messages per day – 18.5
- Time spent deleting them – 2.8 mintues.
- Average time lost in a day – 51.8 mts

- 14 % spam recipients actually read spam
- 4 % buy products advertised by spam
- 21 % spam in Jan 2005 was porn

Cyberoam | Unified Threat Management

Trends in Security

- Basic security began with firewalls
- As threats increased, other solutions were introduced
- Virus attacks rose in number and intensity
- Spam rose
- Slammer fueled the need for Intrusion Detection & Prevention
- High number of employees start accessing the Internet
- Connectivity to branches, partners and remote workers
- Blended threats emerge to exploit extensive Internet usage



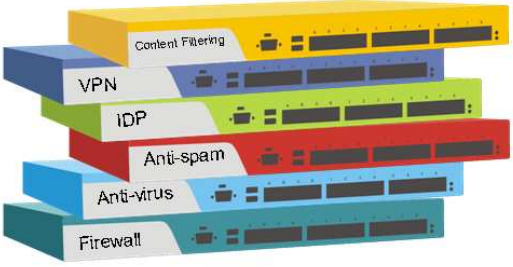
- 25 % systems to be infected with spyware by this year– *Forrester*
- 65 % companies say they will invest in anti-spyware tools and upgrades
- Phishing mails grew 5,000 % last year
- Pharming makes an entry

But multiple solutions brought in their share of problems

Cyberoam | Unified Threat Management

Problem with Multiple Security Solutions

- They resulted in high Capital Expense
- Operating Expense rose too
  - Dealing with multiple solution operation, vendors and updates
  - Multiple AMCs and subscriptions
  - Multiple reports redundancy lead to excessive time spent in understanding threat patterns



Unified Threat Management Systems came into picture

Cyberoam — Unified Threat Management

Benefits of UTM Appliances

- Reduced Capex
- Reduced Opex

But at what cost?

- Sacrificed flexibility as they compromised granularity of individual solutions
- They could not handle dynamic situations – Wi-Fi & DHCP environments
- Internal threats were not yet given their required importance

Potentially dangerous internal threats remained anonymous

Cyberoam — Unified Threat Management

Internal threats rise

- Internal threats played havoc with networks
  - Indiscriminate surfing exposed network to external threats
    - E.g. Spyware, virus download via P2P sites
    - Exposure to Phishing & Pharming
  - Employee with malicious intent posed a serious internal threat
  - Theft of confidential information

Solutions

- Counter Social Engineering
- Need for User Identification

Identity recognition and management is critical to current and future security

➢ **Phishing** refers to the stealing of personal identifiers such as Pin numbers, Credit card numbers and passwords via a spoof web site or email.
➢ It is baiting the end users by playing on their fear and greed.

➢ **Pharming** involves Trojans & worms that attack the Internet browser address bar. When users type in a valid URL they are redirected to the criminals' websites instead of the valid website.

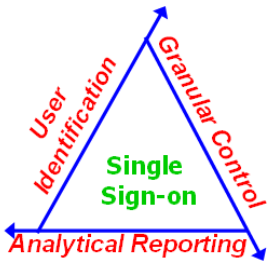
- **50 % of security problems originate from internal threats – *Yankee Group***

Cyberoam | Unified Threat Management

Why do we require Identity-based UTM

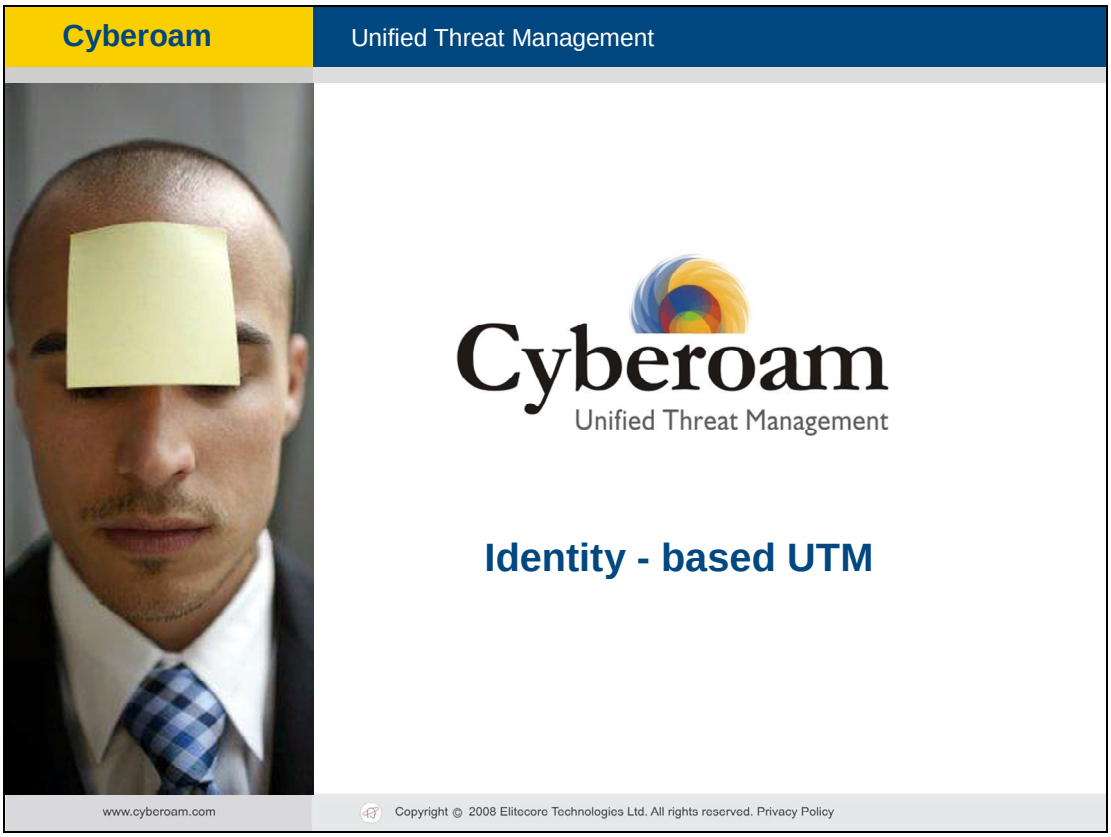
- To Counter Social Engineering
  - ✓End-user's identity – User Name not just IP Address
  - ✓Analytical reporting to identify anomalous individual behavior patterns
- Granular controls to fine tune the individual application
  - ✓ Granular control over all services provided by UTM is required
  - ✓ Granular controls used to implement customized user policies
  - ✓ Granular controls augment the effectiveness of UTM

➢ **Social engineering** is the practice of obtaining confidential information by manipulation of legitimate users.
➢ Social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes.
➢ It is generally agreed upon that "**users are the weak link**" in security and this principle is what makes social engineering possible.



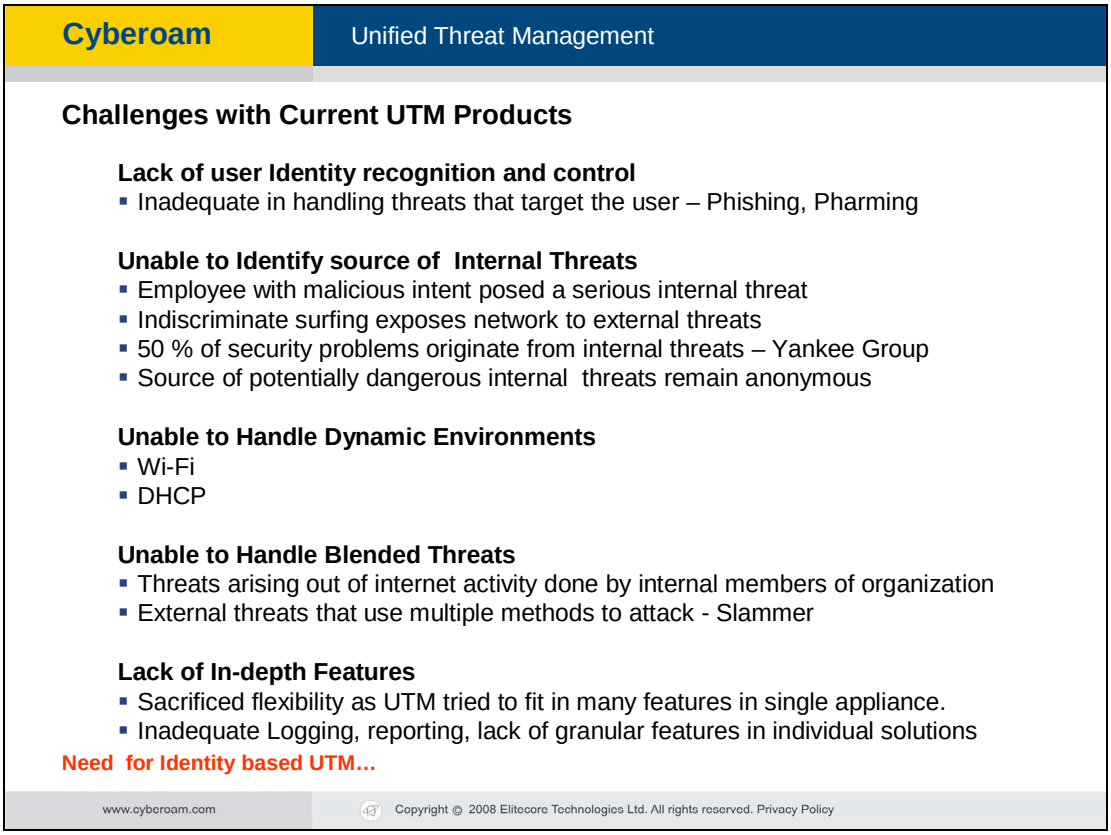
How to establish the Identity...

Module 2: Cyberoam Identity Based UTM



Agenda:

- Challenges with Current UTM Products
- Cyberoam's Security Approach
- Layer 8 Firewall
- Identity Based Technology



Challenges with Current UTM Products

Lack of user Identity recognition and control

- Inadequate in handling threats that target the user – Phishing, Pharming

Unable to identify source of Internal Threats

- Employee with malicious intent posed a serious internal threat
- Indiscriminate surfing exposes network to external threats
- 50 % of security problems originate from internal threats – Yankee Group
- Source of potentially dangerous internal threats remain anonymous

Unable to Handle Dynamic Environments

- Wi-Fi
- DHCP

Unable to Handle Blended Threats

- Threats arising out of internet activity done by internal members of organisation
- External threats that use multiple methods to attack - Slammer

Lack of In-depth Features

- Sacrificed flexibility as UTM tried to fit in many features in single appliance.
- Inadequate Logging, reporting, lack of granular features in individual solutions

Cyberoam's Security Approach

Cyberoam | Unified Threat Management

Cyberoam: Identity-based Security

Overview of Cyberoam's Security Approach:

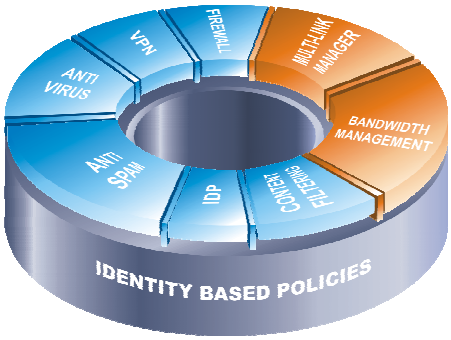
- Who do you give access to: An IP Address or a User?
- Whom do you wish to assign security policies: Username or IP Addresses?
- In case of an insider attempted breach, whom do you wish to see: User Name or IP Address?
- How do you create network address based policies in a DHCP and a Wi-Fi network?
- How do you create network address based policies for shared desktops?

www.cyberoam.com

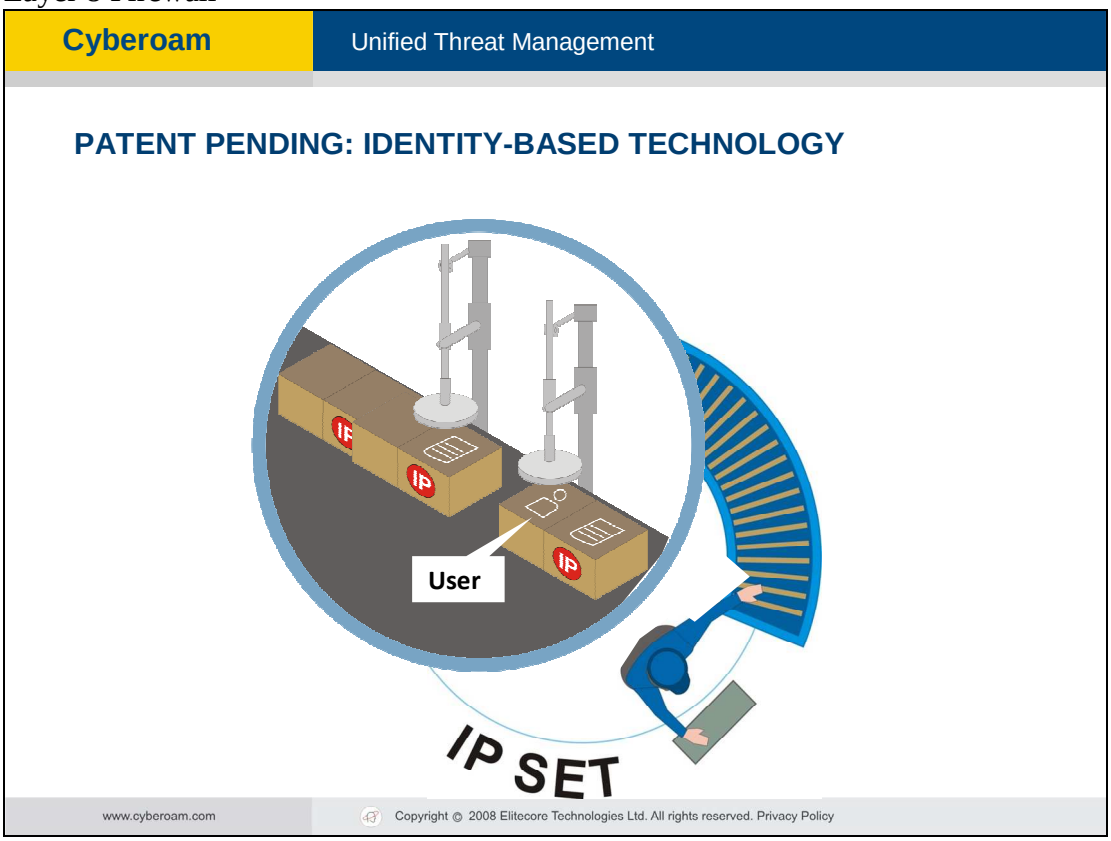
Cyberoam | Unified Threat Management

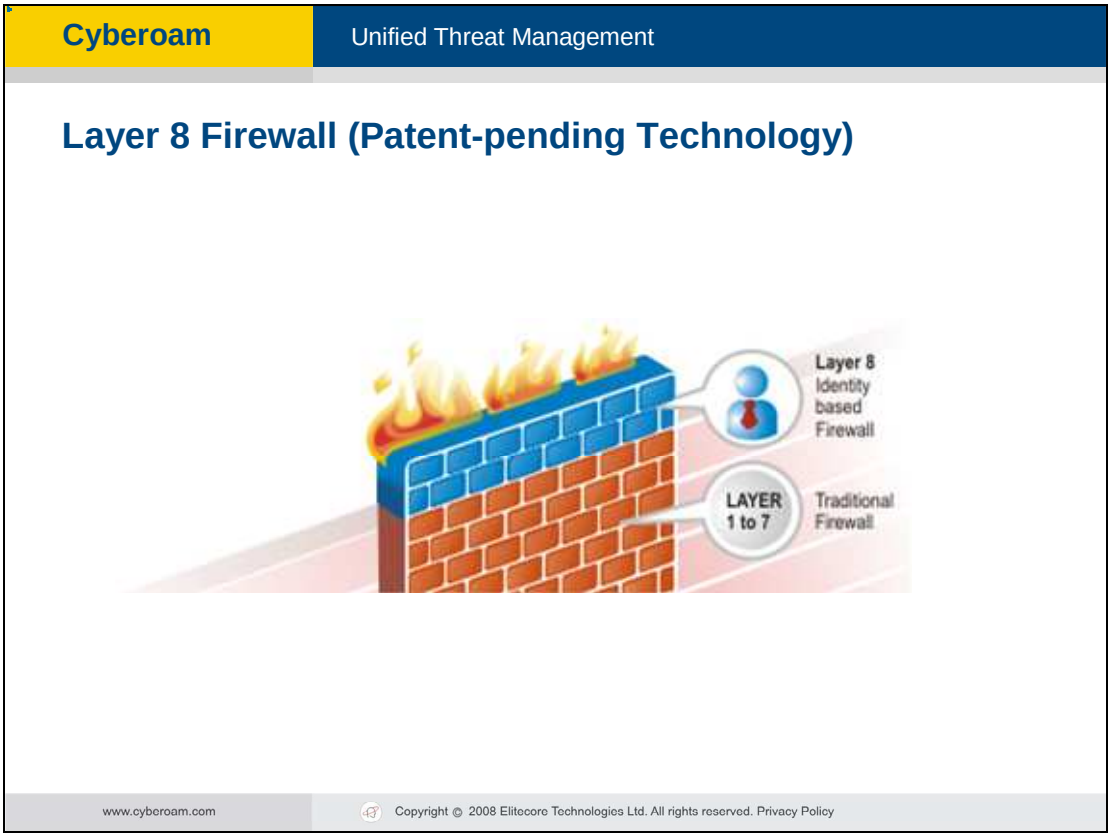
Cyberoam – **Identity Based Security**

Cyberoam is the only **Identity-based Unified Threat Management** appliance that provides integrated Internet security to enterprises and educational institutions through its unique granular user-based controls.



Layer 8 Firewall





Identity-Based Security - Patent Pending Technology

Cyberoam is the only UTM that embeds user identity in the firewall rule matching criteria, offering instant visibility and proactive controls over security breaches. It offers LDAP, Active Directory and RADIUS authentication too.

Protection against Insider Threats

Cyberoam's identity-based security offers protection against insider threats, including data leakage as well as indiscriminate surfing that leave the network vulnerable to external threats.

Eliminates Dependence on IP Address

Unlike traditional firewalls, Cyberoam's identity-based firewall does not require an IP address to identify the user. This empowers administrators to control user access irrespective of login IP.

Complete Security in Dynamic IP Environments

Cyberoam provides complete security in dynamic IP environments like DHCP and Wi-Fi where the user cannot be identified through IP addresses.

One Step Policy Creation

Cyberoam's identity-based security links all the UTM features, offering a single point of entry to effectively apply policies for multiple security features. This delivers truly unified controls in addition to ease-of-use and troubleshooting.

Dynamic Policy Setting

Cyberoam offers a clear view of usage and threat patterns. This offers extreme flexibility in changing security policies dynamically to meet the changing requirements of different users.

Regulatory Compliance

Through user identification and controls as well as Compliance templates and reports, Cyberoam enables enterprises to meet regulatory compliance and standards. With instant visibility into 'Who is accessing what in the enterprise', Cyberoam helps shorten audit and reporting cycles.

Module 3: Cyberoam Products

Agenda:

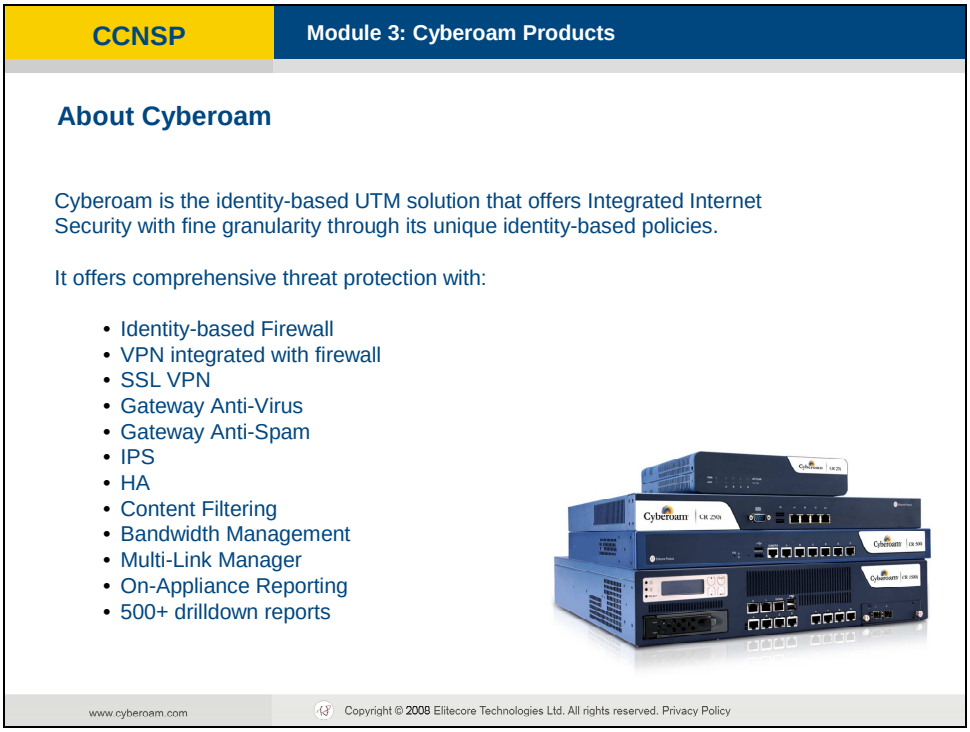
- Cyberoam UTM Appliances
  - Features
  - Appliance Family
- Cyberoam Subscriptions
  - Basic Appliance Solution
  - Subscription Based Solution
  - CR 25i User Licensing
  - Demo V/s Sales Appliance
- Cyberoam Aggregated Reporting & Logging (CARL)
- Cyberoam Central Console (CCC)
- Cyberoam VPN Client

Cyberoam UTM Appliances

Features:

Cyberoam offers a well-coordinated defence through tightly integrated best-of-breed solutions over a single interface. The result is a complete, dependable shield that Internet threats find extremely difficult to penetrate.

- Identity-based Firewall
- VPN integrated with firewall
- SSL VPN
- Gateway Anti-Virus
- Gateway Anti-Spam
- IPS
- HA
- Content Filtering
- Bandwidth Management
- Multi-Link Manager
- On-Appliance Reporting
- 500+ drilldown reports



Cyberoam Appliance Family

SOHO and ROBO Security Appliances

Small offices implementing limited security like a firewall and anti-virus leave themselves exposed to the high volume and range of external and internal threats.

Cyberoam CR15i, CR 25ia, CR 35ia and CR50ia are powerful identity-based network security appliances, delivering comprehensive protection from blended threats that include malware, virus, spam, phishing and pharming attacks. Their unique identity-based security protects small office and remote, branch office users from internal threats that lead to data theft and loss.

These appliances deliver the complete set of robust security features, including Stateful Inspection Firewall, VPN, gateway Anti-virus and Anti-malware, gateway Anti-Spam, Intrusion Prevention System System, Content Filtering, Bandwidth Management and Multi-Link Manager over a single security appliance.

Small Office Protection

Cyberoam CR15i, CR25ia, CR35ia and CR50ia offer comprehensive security that is cost-effective and easy-to-manage, lowering capital and operating expenses for small and home offices. At the same time, these security appliances eliminate the need for technical manpower to configure and manage them.

Remote Office Protection

For enterprises with branch and remote offices CR15i, CR25ia, CR35ia and CR50ia security appliances offer complete visibility into and control over remote users, showing “Who is doing what”. Given this identity information with user access patterns, enterprises can meet regulatory compliances and shorten audit cycles.

Enterprises can create access policies based on user work profiles, enabling them to deploy the same level of security in remote offices that central offices with high security infrastructure and technical resources function in.

- CR15i

  - Delivers 3 10/100 Ethernet ports
  - Configurable internal/DMZ/WAN ports
  - Supports 30,000 concurrent sessions
  - With 90 mbps firewall throughput and 15 mbps UTM throughput

- CR25ia -

  - Configurable internal/DMZ/WAN ports
  - Supports 130,000 concurrent sessions
  - Has 4 10/100/1000 Gigabit ports
  - With 250 mbps firewall throughput and 50 mbps UTM throughput –easily accommodates the requirements of SOHO – ROBO

CR35ia

  - Configurable internal/DMZ/WAN ports
  - Supports 175,000 concurrent sessions
  - Has 4 10/100/1000 Gigabit ports
  - With 500 mbps firewall throughput and 90 mbps UTM throughput –easily accommodates the requirements of small enterprises.

- CR50ia

  - Configurable internal/DMZ/WAN ports
  - Supports 220,000 concurrent sessions
  - Has 6 10/100/1000 Gigabit ports
  - With 750 mbps firewall throughput and 125 mbps UTM throughput

Small & Medium Enterprises (SMEs) - Gateway Security Appliance

It isn't true that large enterprises are at greater risk from Internet threats. Small and medium enterprises face the same or higher amount of risk from the focused attacks that attackers are shifting to with great success. These enterprises need to protect their networks as much as a large enterprise with a large security budget.

Cyberoam CR100i, CR200i, CR300i and CR500i are powerful identity-based unified threat management appliances, delivering comprehensive protection to small and

medium enterprises (SMEs) with limited investment in financial and technical resources.

Cyberoam gateway security appliance offers protection from blended threats that include malware, virus, spam, phishing and pharming attacks, at a small business price. Their unique identity-based security protects enterprises from internal threats that lead to data theft and loss by giving complete visibility into and control over internal users.

Comprehensive Security

These gateway security appliances deliver the complete set of robust security features, including Stateful Inspection Firewall, VPN, gateway Anti-virus and Anti-malware, gateway Anti-Spam, Intrusion Prevention System, Content Filtering, Bandwidth Management and Multiple Link Management over a single security appliance. Cyberoam security appliances offer a comprehensive, yet cost-effective and easy-to-manage solution that lowers capital and operating expenses in addition to lower technical resource requirement.

Regulatory Compliance Through user identification and access control policies for information protection, Cyberoam gateway security appliance enables enterprises to meet regulatory compliances like HIPAA, GLBA, PCI-DSS, SOX, CIPA and more. Further, it helps shorten audit and reporting cycles through instant visibility into “Who is accessing what” in the enterprise network.

- CR100ia

  - Configurable internal/DMZ/WAN ports
  - Supports 400,000 concurrent sessions
  - Has 6 10/100/1000 Gigabit ports
  - With 1 Gbps firewall throughput and 160 mbps UTM throughput

- CR200i

  - Configurable internal/DMZ/WAN ports
  - Supports 450,000 concurrent sessions
  - Has 6 10/100/1000 Gigabit ports
  - With 1500 mbps firewall throughput and 250 mbps UTM throughput – caters to the needs of small to medium enterprises.

- CR300i

  - Configurable internal/DMZ/WAN ports
  - Supports 500,000 concurrent sessions
  - Has 6 10/100/1000 Gigabit ports
  - With 1800 mbps firewall throughput and 350 mbps UTM throughput – caters to the needs of small to medium enterprises.

- CR500i

  - Configurable internal/DMZ/WAN ports
  - Supports 400,000 concurrent sessions
  - Has 6 10/100/1000 Gigabit ports
  - With 2Gbps firewall throughput and 450 mbps antivirus throughput caters to the needs of medium-sized enterprises.

Large Enterprises - Network Security Appliance

For large enterprises with distributed networks, implementing a secure, reliable and centrally managed network is critical to derive true business benefits. Deployment of a range of individual security solutions brings in issues of management and control of the solutions, particularly at the time of security incident, delaying response. In addition, with insider threats accounting for 50 % of threats, identifying the user becomes critical to security.

Cyberoam CR1000i and CR1500i are powerful identity-based network security appliances that deliver comprehensive protection to large enterprises from blended threats that include malware, virus, spam, phishing and pharming attacks. Cyberoam's unique identity-based Network Security Appliance protects large enterprise users from internal threats that lead to data theft and loss too.

Comprehensive Security

The Check Mark Level 5 certified Cyberoam Network Security Appliance delivers the complete set of robust security features that are built to support the demanding security requirements of a large enterprise, including Stateful Inspection Firewall, VPN, Gateway Anti-virus and Anti-malware, Gateway Anti-Spam, Intrusion Prevention System System, content filtering, bandwidth management and Multiple Link Management over a single appliance, lowering capital and operating expenses.

Cyberoam's Intrusion Prevention System System along with stateful inspection firewall, gateway Anti-virus and Anti-spyware, gateway Anti-spam and content filtering offer comprehensive, zero-hour protection to enterprises against emerging blended threats.

Secure Remote Access

Cyberoam IPSec VPN offers encrypted tunnels for secure communication between remote offices and the central office. An unmatched Firewall-VPN performance offers branch offices a secure, remote access to corporate resources. The VPNC certified Cyberoam VPN is compatible with most VPN solutions available and supports IPSec, L2TP and PPTP connections. It provides automatic failover of VPN connectivity for IPSec and L2TP connections.

Enterprise-Class Security

Integrated High Availability feature of CR1000i and CR1500i appliances maximises network uptime and ensures uninterrupted access. Cyberoam's Network Security Appliance offers Dynamic Routing that provides rapid uptime, increased network throughput with low latencies and trouble-free configuration and supports rapid network growth. Cyberoam's VLAN capability enables large enterprises to create work profile-based policies across distributed networks from a centralised location or head office.

- CR1000i

- Configurable internal/DMZ/WAN ports
- Supports 600,000 concurrent sessions
- Has 10 10/100/1000 Gigabit ports

- With 3.5 Gbps firewall throughput and 600 Mbps anti-virus throughput caters to the needs of large enterprises.

- CR1500i

- Configurable internal/DMZ/WAN ports
- Supports 1,000,000 concurrent sessions
- Has 10 10/100/1000 Gigabit ports
- With 6 Gbps firewall throughput and 800 Mbps anti-virus throughput caters to the needs of large corporate environments, educational institutions and government organisations.

CCNSP | Module 3: Cyberoam Products

Basic Appliance – One time sale

- Identity-based Firewall
- 8 x 5 Support for the first year.
- VPN behind firewall
- SSL VPN (Promotional offer)
- Bandwidth Management
- Multiple Link Management

CCNSP | Module 3: Cyberoam Products

Subscriptions

Module wise subscription

- Gateway Anti-Virus Subscription (Anti-malware, phishing, spyware protection included)
- Gateway Anti-spam Subscription
- Web & Application Filtering Subscription
- Intrusion Prevention System (IPS)
- 24 x 7 Premium Support
- IPSec VPN Clients (Per Device-Life Time)

(Subscription services are available on 1 Year, 2 Year or 3 Year subscription basis)

Bulk Subscription

It is a one time subscription with a combination of following modules:

- Gateway Anti Virus
- Gateway Anti-spam
- Intrusion Prevention System
- Web and Application Filter
- 8 X 5 Support

Cyberoam Subscriptions

Basic Appliance Solution

- Identity-based Firewall
  - Layer 2 / Layer 3 Deployment Mode (Bridge / Gateway Mode)
  - Stateful and Deep Packet Inspection Firewall
  - Multi Zone Security
  - VLAN
  - Denial of Service Attack Protection
  - Virtual Host (NAT Capability)
  - High Availability (HA)
- Static & Dynamic Routing using Cisco compliance CLI
  - RIPv1 & RIPv2
  - OSPF
  - BGP
- Multicast Support
- VPN
  - IPSec Site to Site with Fail-over
  - IPSec Remote Access
  - L2TP
  - PPTP
  - Threat free Tunnelling for IPSec,L2TP and PPTP
  - SSL VPN
- Bandwidth Management
  - Identity based QoS Policies
- Multiple Link Module
  - Multiple Gateway Load Balancing & Failover
- Intelligent Reports
- 8 x 5 Support as per country time zone for first year.

Subscription Based Solutions

Module wise subscription

- Gateway Anti-Virus Subscription (Anti-malware, phishing, spyware protection included)
- Gateway Anti-spam Subscription
- Web & Application Filtering Subscription
- Intrusion Prevention System (IPS)
- 24 x 7 Premium Support
- IPSec VPN Clients (Per Device-Life Time)

(Subscription services are available on 1 Year, 2 Year or 3 Year subscription basis)

Bulk Subscription

It is a one time subscription with a combination of following modules:

- Gateway Anti Virus
- Gateway Anti-spam
- Intrusion Prevention System

- Web and Application Filter
- 8 X 5 Support

Cyberoam's "Bundle Subscription" service provides subscribers a purchase option to choose between single subscription module and a bundle of modules.

Benefits:

- Subscription bundle will reduce Administrator's task of subscribing each module individually as all the modules in the bundle will be subscribed in a single step using just one key.

- Along with customers, the feature is also beneficial to the suppliers as one can achieve the desired cost reduction for the bundled pack.

Bundle Subscription (TVS & SVS)

Bundle Subscriptions are available as:

(1) Total Value Subscription (TVS) includes:

(1) Anti Virus
(2) Anti Spam
(3) Web & Application filter
(4) IPS
(5) 8*5 Support (if bought for more than 1 year as first year support is included for free)

(2) Security Value Subscription (SVS) includes:

(1) Anti Virus
(2) Web & Application filter
(3) IPS
(4) 8*5 Support (if bought for more than 1 year as first year support is included for free)

How to subscribe:

- Subscriber will be provided a single key for all the modules included in the bundle.
- For renewal, subscriber can choose to renew the pack or the single module.

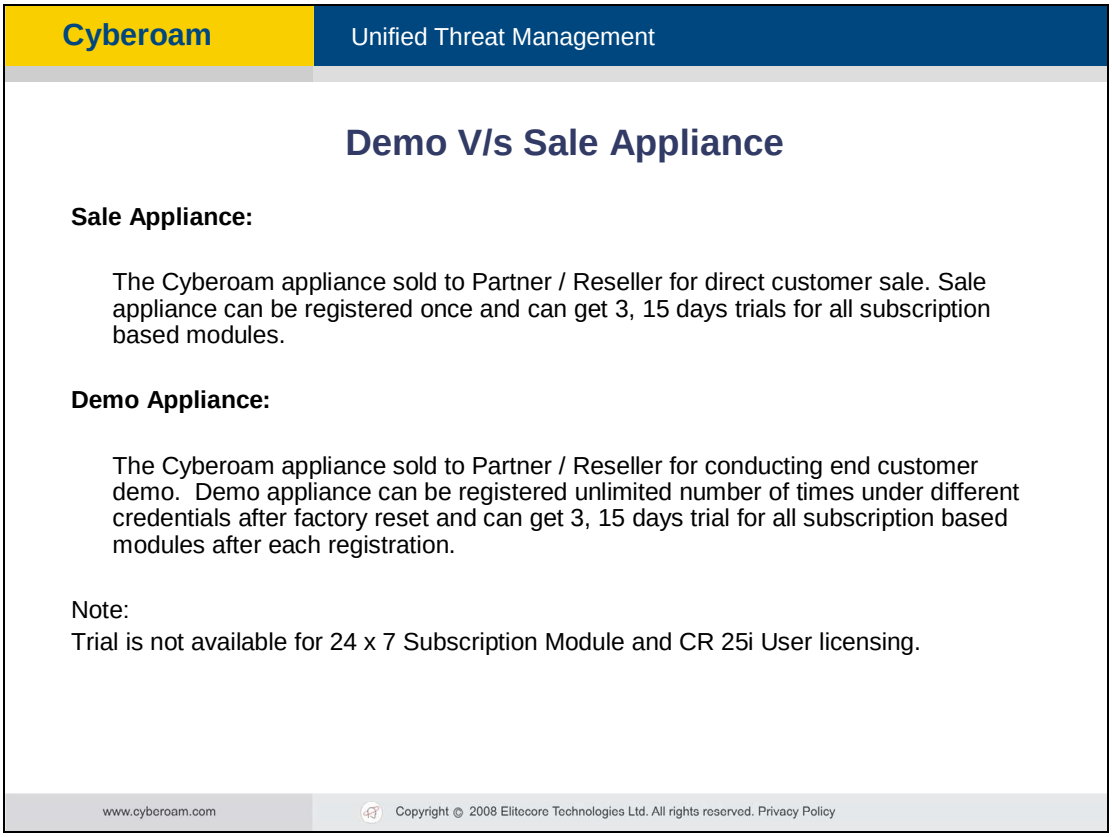
Subscription Screen in Cyberoam appliance:

Module Subscription Details

Module	Status	Expiration Date	Manage	
24 x 7 Support	Unsubscribed	-	-	Subscribe
User License	Unsubscribed	-	-	Subscribe
Bundle Subscription	-	-	-	Subscribe
Web and Application Filter	Trial	2010-02-24	Trial	Subscribe
Intrusion Prevention System (IPS)	Trial	2010-02-24	Trial	Subscribe
Gateway Anti Virus	Trial	2010-02-24	Trial	Subscribe
Gateway Anti Spam	Trial	2010-02-24	Trial	Subscribe
SSL VPN	Trial	2010-03-11	Trial	Subscribe
8 x 5 Support	Subscribed	2011-02-09	-	Subscribe

- Each module comes with 3 free trials of 15 days each. Trials can be activated by clicking on “Trial” So, after registering the appliances, customer can use these trail subscriptions before purchasing the subscription keys.

- If customer has already purchased the subscription keys, he can click on “Subscribe” and provide the subscription key.



Demo V/s Sale Appliance

Sale Appliance:

The Cyberoam appliance sold to Partner / Reseller for direct customer sale. Sale appliance can be registered once and can get 3, 15 days trials for all subscription based modules.

Demo Appliance:

The Cyberoam appliance sold to Partner / Reseller for conducting end customer demo. Demo appliance can be registered unlimited number of times under different credentials after factory reset and can get 3, 15 days trial for all subscription based modules after each registration.

Note: Trial is not available for 24 x 7 Subscription Module and CR 25i User licensing.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

CR SSL Series : CR-SSL-800, CR-SSL-1200, CR-SSL-2400

Cyberoam SSL VPN

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Benefits

- Secure SSL VPN – Access from anywhere.
- Trusted Remote Access – extend access to partners, telecommuters, wireless users.
- Easy to use – Fast installation, less ongoing management, less downtime.
- Continuous Access – provides reliable, available and scalable access.
- Endpoint Security.
- Hardened Secure OS.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam SSL-VPN features

- SSL based VPN
- Browser Based Access
- Connect From Anywhere
- Hardened Platform
- Web Based Management
- Built-in SSL Client Certificate Authentication
- Strong authentication for administrators
- VPN load balancing and High Availability
- Application Load balancing
- Integrates with Ad/LDAP/Radius
- Granular Policy Enforcement
- Device Profiles
- User Role
- Endpoint Security
- MAC ID and IP address based login
- Hide Network Information
- Client platforms - Windows, Linux, MAC OSX
- Application Gateway not Layer 2
- Delegated Administration

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Models & Licenses

- **Base License**
  - Default 5 User License valid for 30 days.
  - No EPS.
- **Software Based**
- **Appliance Based**
  - CR-SSL-0800 (Supports upto 50 Concurrent Users).
  - CR-SSL-1200 (Supports upto 250 Concurrent Users).
  - CR-SSL-2400 (Supports upto 1000 Concurrent Users).

Cyberoam SSL-VPN unique features

- Complete inbuilt PKI Solution.
  - Certificate based Security with no manual intervention.
  - Benefits:
    - No manual distribution of usernames & passwords.
    - Reduction in Administrative overheads.
- Available in software version.
- Unlimited User License.
- User Provisioning via Email.
- Automated User Enrollment.
- Secure certificate distribution.
- No revelation of internal IP addresses.
  - Applications published through user friendly names.
- Tunnel Adapter independency.
  - No installation of extra virtual interfaces on client PCs'.
  - Malicious Network traffic Protection.
- MAC Based Device Profiling.
- Application Load Balancing.
- N+1 Clustering.
- Session Persistence.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Models & Licenses

- **Base License**
  - Default 5 User License valid for 30 days.
  - No EPS.
- **Software Based**
- **Appliance Based**
  - CR-SSL-0800 (Supports upto 50 Concurrent Users).
  - CR-SSL-1200 (Supports upto 250 Concurrent Users).
  - CR-SSL-2400 (Supports upto 1000 Concurrent Users).

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam End Point Data Protection

Protect Your Data, Protect Your Assets

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam End Point Data Protection

- **Comprehensive End Point Data Protection Suite**
- **Modules**
  - Data Protection & Encryption
  - Device Management
  - Application Control
  - Asset Management

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam End Point Data Protection

Benefits

- **Enhanced protection to all your Endpoints**
  - Across geographic locations
  - Centralized controls
  - Regulatory and Security Compliance
- **Rapid installation**
- **Easy to use**
- **Maintains security with flexibility**
- **Clear ROI**

www.cyberoam.com

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam End Point Data Protection

Licenses (Per-user one time licenses)

1. Data Protection & Encryption
2. Device Management
3. Application Control
4. Asset Management

Note: All the modules include 1 year maintenance support. A single key would be issued for the modules purchased. Need to buy the same number of licenses for all the modules. i.e. Not possible to buy 10 licenses for Device management & 50 for Asset management.

Renewal (year on year)

Maintenance support to be renewed for all the modules purchased each year.
It includes version upgrades & technical support.

www.cyberoam.com

Cyberoam iView – Open Source Logging and Reporting Solution

Cyberoam iView is an open source logging and reporting solution that helps organizations monitor their networks across multiple devices for high levels of security, data confidentiality while meeting the requirements of regulatory compliance.

Enabling centralized reporting from multiple devices across geographical locations, Cyberoam iView offers a single view of the entire network activity. This allows organizations not just to view information across hundreds of users, applications and protocols, it also helps them correlate the information, giving them a comprehensive view of network activity.

Monitoring Security
With Cyberoam iView, organizations receive logs and reports related to intrusions, attacks, spam and blocked attempts, both internal and external, enabling them to take rapid action throughout their network anywhere in the world.

Identity-based Reports
Cyberoam iView offers reports based on the user identity allowing organizations to see "Who is doing What" anywhere in the network. Given the criticality of insider threats in network security and data confidentiality, these reports give an instant view of a user profile through indepth user identity-based reporting across applications, protocols and multiple devices and solutions, allowing organizations to take preventive measures.

Regulatory Compliance
Cyberoam iView's user identity-based drill down reports form a critical element in enabling organizations to meet the access control, audit and forensic requirements of regulatory compliances like HIPAA, GLBA, SOX, PCI-DSS, CIPA, BECTA and others.

Log Management

The highly connected world, changing Internet threat scenario, advent of social networking and new business technologies make it imperative for organizations to add advanced security solutions and devices like firewalls, content filtering systems, unified threat management solutions, routers, servers, applications, operating systems and more in their networks which generate a vast amount of log data.

To maintain security, data confidentiality and meet the requirements of regulatory compliance, continuous log monitoring becomes essential, allowing administrators to interpret unusual events and respond in real-time. But a comprehensive analysis of

network logs becomes a difficult and time-consuming task with multiple devices leading to multiple management systems and proprietary technologies that deliver logs in different formats.

Cyberoam iView – One-Stop Log Management
Cyberoam iView is an open source logging and reporting solution that enables organizations, especially SMEs with tight budgets and limited technical personnel, to manage logs effortlessly and in near real-time, reducing administrative complexities involved in the process. In addition, as an open source solution, it reduces capital and operating costs significantly.

Centralized Log Collection, Intelligent Storage, and Instant Retrieval
Cyberoam iView allows quick collection, storage and retrieval of log data from multiple devices across geographical locations at a central location, eliminating the need to trade-off between speed of log collection and quick retrieval. Its powerful Log Collection Agent aggregates data from multiple sources at remote sites and forwards it rapidly to the centralized location. It compresses logs, significantly reducing storage requirements and associated costs and archives data for easy and secure recovery.

Although log information is critical during emergencies, each minute spent in search and retrieval translates into millions of dollars of lost revenues for organizations. Cyberoam iView offers indexing in archives and easy-search on various parameters, allowing practically instant retrieval of the required information across terabytes of log data.

Identity with Security Management
Cyberoam iView enables organizations to match “who should be accessing what” with “who is actually accessing what”. When integrated with identity-based perimeter security devices like firewalls, anti-virus and anti-spam systems, content filtering systems, unified threat management solutions and more, it generates logs that give a fingerprint of user activity within the network through the username. iView’s logging with user identity allows the matching of these details with user rights and privileges easily, revealing discrepancies in user activity.

Compliance Management
Cyberoam iView helps organizations comply with PCI-DSS, HIPAA, GLBA and SOX requirements with audit logs, many useful reports and rapid search to investigate an incident, enabling organizations to demonstrate their compliance capability.

Reporting
Cyberoam iView delivers comprehensive and graphical reporting on network traffic, security incidents, bandwidth usage, most used applications and hosts, and more, allowing easy regulatory compliance, resource management and quick incident response. It offers centralized reporting of selected or all devices in the network on a single dashboard.

Aggregated Reporting

With multiple devices deployed in the network, rising threats from insiders and external entities, organizations need to look deeper and monitor network activities not as isolated incidents which individual logs enable them to do, but as comprehensive activity.

Data from firewalls, content filtering systems, unified threat management solutions, routers, servers, applications or operating systems must be viewed across users in flexible reporting format for indepth actionable view of activity

Cyberoam iView – Integrated Reporting from Multiple Devices
Cyberoam iView is the open source centralized logging and reporting solution that provides comprehensive drill-down reports offering administrators a clear view of activity across any device, user, location or activity throughout the organization. The graphical reports can be drilled down to the third level of information, allowing administrators to view multiple reports on a single page for uninterrupted view of multiple network parameters.

The centralized view of events and activity across all devices and applications on iView's single dashboard enhances IT efficiency and security while lowering costs involved. Administrators can also prioritize the placement of reports based on organizational requirements through the high degree of customization offered by iView.

Identity-based Reporting
External threats targeting insiders' ignorance as well as insider threats that breach network security and data confidentiality are on the rise. Cyberoam iView's detailed drill-down reports with a clear view of the user and his / her activity over any device, location or activity throughout the organization allows administrators to see "Who is doing What" in the network.

Knowing a person's activity is not just a matter of viewing reports by the username, application or protocol. It requires comprehensive tracking of activity via keywords, attacks and intrusions with a combination of user, application and protocols available at a click and in the form of drill-down graphical and tabular reports.

Cyberoam iView's user identity-based reports give a clear view of the user's network usage like websites visited, time and duration for which the user accessed them, sites that were denied access to, bandwidth consumed by the user across different protocols, and more. This information allows administrators to judge the user's activity profile, the understanding of which enables them to correct policies, taking preventive action against potential security breaches.

Meeting Regulatory Compliance

Access control and auditing form the basis of regulatory compliance requirements across the world. Cyberoam iView offers reports that cover user activity accessing critical data, including attempts to access data where access is denied to the user as well as data leakage by the user across multiple protocols. This allows organizations to meet the requirements of regulatory compliances like HIPAA, GLBA, PCI-DSS, SOX and more.

Identity-based Reporting

Insiders like current and former employees, suppliers and partners cause 83 % of security breaches, according to a PriceWaterhouse Coopers' global survey. 35 % of breaches are of intellectual property theft. Hence, Identity-based Reporting that gives visibility into who is accessing critical network resources, the extent of usage and user privileges is a critical element of network security.

Cyberoam iView – Identity Monitoring
Cyberoam iView is the open-source logging and reporting solution that shows "who is accessing what" in the network, reporting network usage, violation of privileges, entry of malware or spam that can be traced to users, enabling organizations to enhance security levels while meeting the requirements of regulatory compliance.

User activity over a range of protocols like HTTP, FTP, email, IM, P2P and more across different user IDs alerts organizations to internal security breaches and their source, allowing them to take immediate action.

Data Loss Prevention
Identity-based reporting of user access plays a key role in controlling data loss. Consider this scenario. A user attempts to access sensitive documents in the database server to which he does not have access privilege. Firstly, Cyberoam iView reports his blocked attempts. Secondly, if the user attempts access via different client devices, administrators would be notified through the reporting which gives both the username and the IP address from which the attempts are made. Such deviation from normal practice alerts administrators to potential violations and data loss.

Consider another scenario where the user tries to access the database server through login ids of other employees from her device. Administrators would know such takeover attempts through Cyberoam iView, allowing them to take rapid action.

Employees on notice can be monitored and their past records revisited and reports provided to HR or the respective departments, offering critical information related to the users' access practices during the most vulnerable period for sensitive data during the employee life cycle.

Security Monitoring
Cyberoam iView provides security reports related to malware download or upload,

spam received and sent, indicating unsafe practices of users. In addition, reports of attacks, attackers, victims, applications used by the attacks, break-down of attacks by severity, top spam recipients, senders, applications used to send spam as well as of viruses, bifurcated into web, mail, FTP through which viruses entered offer effective security monitoring.

Web Usage
Cyberoam iView allows administrators to know when users' web usage deviates from acceptable policies based on time of activity and volume of data downloaded or uploaded, through web usage reports of users, categories, domains, content, web hosts and applications. Reports of blocked web attempts offer information related to attempts to compromise user privileges. A combination of these web usage reports offers a comprehensive view of user web activity, allowing administrators to correct user privileges to enhance productivity and security.

Security Management

Complexity of IT environments is rising with the use of multiple network devices, applications, protocols; so is the sophistication of security threats. While organizations continue to grapple with the source and form of threats, attackers are targeting not just the network itself but also databases, servers and employee identities in organizations to reap financial rewards.

Discovering the disguised threats that most attackers resort to and correlating them with the causes is essential to maintaining high levels of security. This involves logging and analyzing thousands of logs generated through multiple network devices across geographic locations on a continuous basis.

Cyberoam iView – Security Reporting
Cyberoam iView is the open source logging and reporting solution that offers a comprehensive security view of an organization on a single screen. iView delivers identity-based logging and reporting across multiple devices, protocols and locations, enabling organizations to discover not just the threats, but also allows them to correlate these with the who, what, why, where, when of an attack.

This comprehensive approach enables organizations to understand the historic patterns of activity and hence be alerted to deviation in activity that signals an attack and take the precise action required to prevent or contain the attack. Further, it allows them to identify disguised attacks, while eliminating false positives.

Security at a Glance
Organizations can instantly locate network attacks, their source and destination through a quick glance at the iView dashboard. Further, Cyberoam iView's drill down reports and identity-based logging, reporting related to traffic denied by firewall, content filter, dropped mail by anti-spam, anti-virus and IPS solutions, assists

organizations in locating an attack, the source-destination and taking rapid action.

Traffic anomalies like a spike in ICMP traffic or in bandwidth consumption that indicate a DoS attack or spyware infection respectively, emails to suspicious mail addresses, are some examples of how Cyberoam-iView enables administrators to identify malicious activity, the source and destination, including the user identity where relevant, reducing the response time to threats.

Audit Trail and Forensics
With full archival and storage of logs, Cyberoam-iView aids in audit trail and forensic analysis offering comprehensive security logging and reporting across multiple devices and geographical locations.

Compliance Reporting and Security Audit

Regulatory compliance has become a priority for organizations, requiring overwhelming effort, time and cost in the form of retrieval and storage of logs and reports from multiple devices. Correlating the vast amount of logs and reports to complete the compliance picture is a complicated and time-consuming task.

At the same time, visibility into who has accessed what and when and audit logs hold the key to compliance efforts. Inability to meet compliance requirements can lead to loss of reputation, legal liability and financial losses.

Cyberoam iView – Compliance Reporting
Cyberoam iView is an open-source logging and reporting solution that enables organizations to meet the requirements of PCI-DSS, HIPAA, GLBA and SOX.

iView eliminates the complexities in compliance reporting by providing access reports and audit logs that alert the administrator of deviations from security practices, significantly reducing the cost to compliance as well as risk to the organization.

Centralized Security Repository
Cyberoam iView offers near-real time reporting of logs and security events on a single dashboard, which can be drilled down to get the third level of information. One-step access to critical information through multiple reports allows end users to monitor security violations in the network, accelerating incident response and facilitating compliance.

Audit Logs
Cyberoam iView enables organizations to maintain integrity of application controls. Organizations can easily identify system configuration changes made by

administrators. Concerned personnel can be alerted regarding unauthorized changes, facilitating quick corrective actions.

Forensic Analysis

Ensuring security is a matter of meeting three requirements - continuously judging security readiness to take corrective action, preventing a security breach and in the case of a breach happening, that of minimizing legal liability.

Forensics is the security element that enables organizations to meet these three requirements through logs and reports that are captured based on potential breaches and legal requirements. In contrast to routine data capture that merely gives historic visibility, a forensic view foresees and meets the real security and legal requirements in organizations.

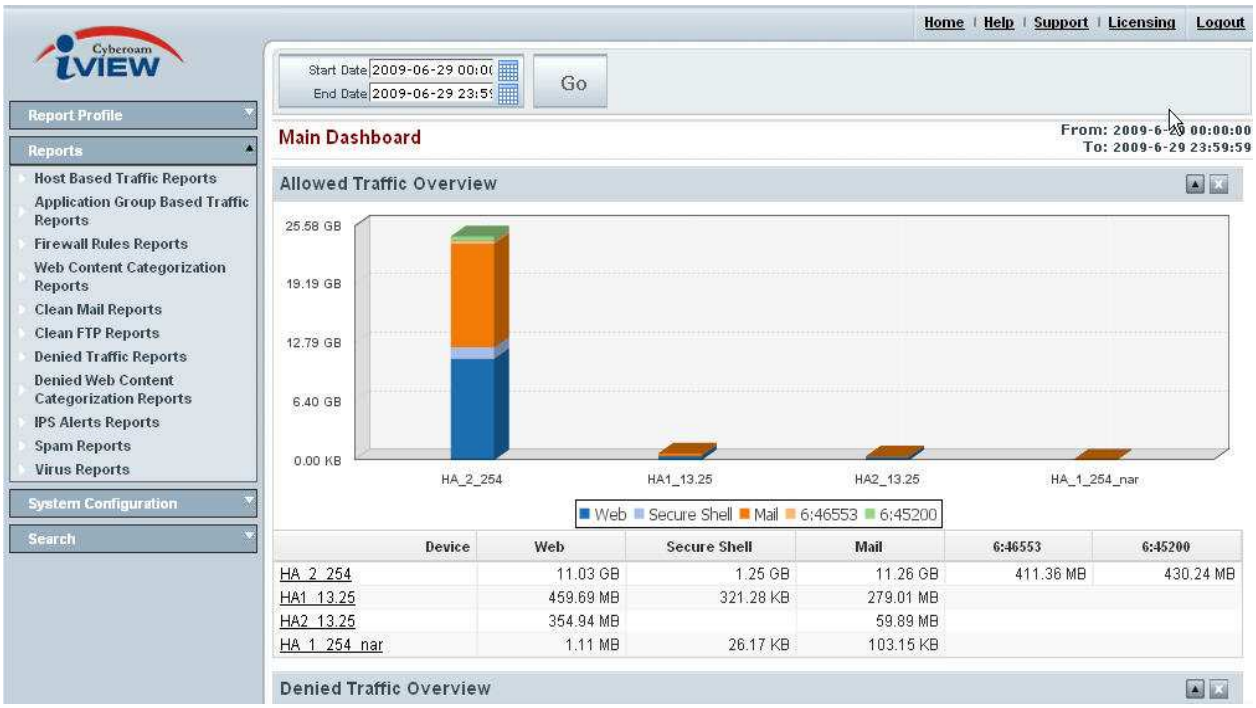
Cyberoam iView – Forensic Analysis
Cyberoam iView is an open source logging and reporting solution that enables organizations to mine historical data from network events. Organizations can reconstruct the sequence of events that occurred at the time of security breach through iView logs and reports. They can reduce the cost of investigation and analysis and minimize network downtime while gathering historical information with Cyberoam iView.

Reduce Legal Liability
Cyberoam iView enables organizations to prove conformance to compliance requirements and reduce legal liability. Consider a scenario where sensitive data kept in the organization's database server is accessed by a user through a stolen identity.

First and foremost, iView reports and audit logs have the capability of identifying the source of breach depending on the security parameters used by the organization.

Further, it enables the organization to prove that it had complied with the security norms and had taken the necessary security precautions to avoid breach in security. Besides this, the network log reports provide evidence that security was intentionally breached by an insider in an otherwise secure network, providing further proof regarding the organization's security preparedness.

With logs and reports that provide such comprehensive visibility with legal validity, Cyberoam iView helps organizations save significantly on legal costs.


Home | Help | Support | Licensing | Logout
Cyberoam iVIEW
Start Date 2009-06-29 00:0
End Date 2009-06-29 23:5
Go
Report Profile
Reports
Host Based Traffic Reports
Application Group Based Traffic Reports
Firewall Rules Reports
Web Content Categorization Reports
Clean Mail Reports
Clean FTP Reports
Denied Traffic Reports
Denied Web Content Categorization Reports
IPS Alerts Reports
Spam Reports
Virus Reports
System Configuration
Search
Main Dashboard
From: 2009-6-29 00:00:00
To: 2009-6-29 23:59:59
Allowed Traffic Overview
25.58 GB
19.19 GB
12.79 GB
6.40 GB
0.00 KB
HA_2_254
HA1_13.25
HA2_13.25
HA_1_254_nar
Web Secure Shell Mail 6:46553 6:45200
Device Web Secure Shell Mail 6:46553 6:45200
HA_2_254 11.03 GB 1.25 GB 11.26 GB 411.36 MB 430.24 MB
HA1_13.25 459.69 MB 321.28 KB 279.01 MB
HA2_13.25 354.94 MB 59.89 MB
HA_1_254_nar 1.11 MB 26.17 KB 103.15 KB
Denied Traffic Overview


Welcome, admin
Home | Help | Feedback | Logout
SELECT DEVICE
Start Date 2009-08-26 00:0(
End Date 2009-08-26 23:5
GO
Web user gabriel@rediffmail.com
From: 2009-8-26 00:00:
To: 2009-8-26 23:59:
DASHBOARDS
REPORTS
Source Host Based Usage
Application Based Usage
Firewall Rule Based Usage
Web Usage
Top Web Users
Top Categories
Top Domains
Top Content
Top Web Hosts
Top Applications
Mail Usage
FTP Usage
Blocked Attempts
Blocked Web Attempts
Attacks
Spam
Virus
CUSTOM VIEWS
SYSTEM
Version
0.0.0.2 Beta
Top Categories
SearchEngines
NewsAndMedia
InformationTechno...
EducationalInstitut...
Music
Category
0.00 KB
5.17 MB
10.35 MB
15.52 MB
20.70 MB
Bytes
Top Domains
safebrowsing-cac...
khm3.google.com
khm1.google.com
khm0.google.com
khm2.google.com
Domain
0.00 KB
2.97 MB
5.95 MB
8.92 MB
11.90 MB
Bytes
Category Hits Bytes
SearchEngines 1281 19.71 MB
NewsAndMedia 208 1.20 MB
InformationTechnology 169 969.40 KB
EducationalInstitutions 69 384.96 KB
Music 15 194.19 KB
View All
Domain Hits Bytes
safebrowsing-cache.google.com 215 11.33 MB
khm3.google.com 64 1.13 MB
khm1.google.com 63 1.11 MB
khm0.google.com 61 1.09 MB
khm2.google.com 57 1.01 MB
View All
Top Contents
application/v...
image/jpeg
image/png
application/x-javascript
application/xm...
Content
0.00 KB
2.97 MB
5.95 MB
8.92 MB
11.90 MB
Bytes
Top URLs
safebrowsing-cac...
safebrowsing-cac...
safebrowsing-cac...
safebrowsing-cac...
news.google.co...
URL
0.00 KB
104.56 KB
209.13 KB
313.69 KB
418.26 K
Bytes
Content Hits Bytes
application/vnd.google.safebrowsing-(215 11.33 MB
image/jpeg 317 5.06 MB
image/png 723 4.28 MB
application/x-javascript 83 454.30 KB
application/xml; charset=UTF-8 7 349.23 KB
View All
URL Hits Bytes
safebrowsing-cache.google.com/saf 2 398.34 KB
safebrowsing-cache.google.com/saf 2 398.02 KB
safebrowsing-cache.google.com/saf 2 386.15 KB
safebrowsing-cache.google.com/saf 2 374.68 KB
news.google.com/?output=rss 7 349.23 KB
View All
Top Hosts
192.168.13.129
Host
0.00 KB
6.06 MB
12.13 MB
18.19 MB
24.25 MB
Bytes
Top Applications
http
Application
0.00 KB
6.06 MB
12.13 MB
18.19 MB
24.25 MB
Bytes
Host Hits Bytes
192.168.1.39 1885 23.10 MB
Application Hits Bytes
http 1885 23.10 MB

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam iView appliances

- CR-iVU 25
- CR-iVU 100
- CR-iVU 200

Products supported

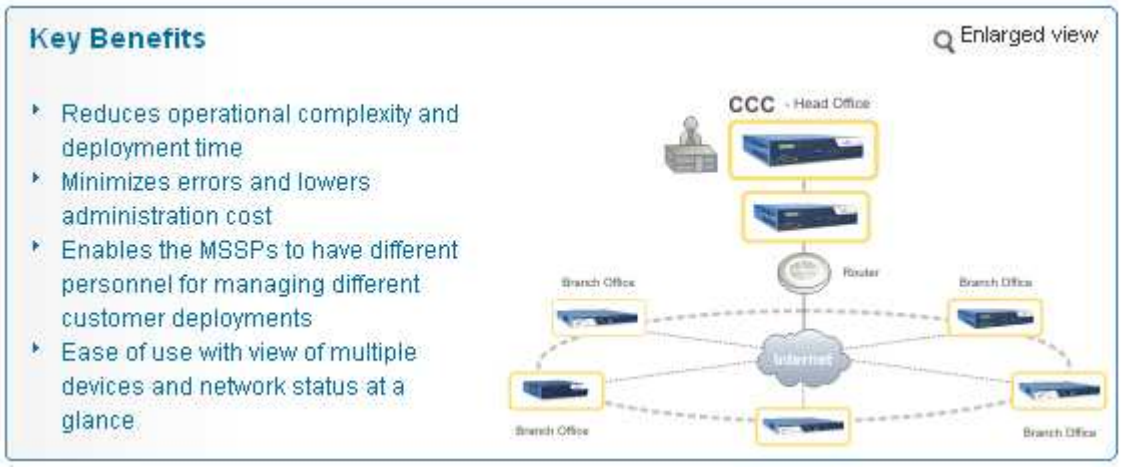
- Network Devices: Linux IPtables / Netfilter Firewall,Cyberoam, Fortigate, Sonicwall.

- HTTP Proxy: Squid

- Syslog Compatible Devices: Any product with Syslog support

Cyberoam Central Console (CCC)

Cyberoam Central Console (CCC) with its centralised management and control offers coordinated defence against zero-hour and blended threats across distributed networks. It enables enterprise-wide implementation of corporate Internet policy, ensuring high productivity and security. Being an appliance based solution; CCC lowers the deployment cost while offering complete control over distributed networks.



CCC supports Cyberoam CR25i, CR50i, CR100i, CR200i, CR 300i, CR500i, CR1000i and CR1500i.

Centralised Threat Management and Control:

Cyberoam Central Console enables enforcement of global policies for Firewall, Intrusion Prevention System and Anti-virus scanning. This supports the creation and implementation of enterprise-wide security policy to strengthen branch and remote office security while lowering operational complexity.

The Cyberoam Central Console enables administrators to assign security policies based on user's work profile even in remote locations. This fully leverages Cyberoam's unique user identity-based security approach.

Key Benefits

- Real-time visibility of threat summary and trends
- Instant enforcement of security policies in response to zero hour threats
- Reduced operational complexity and deployment time
- Ease of use with view of multiple devices and network status at a glance

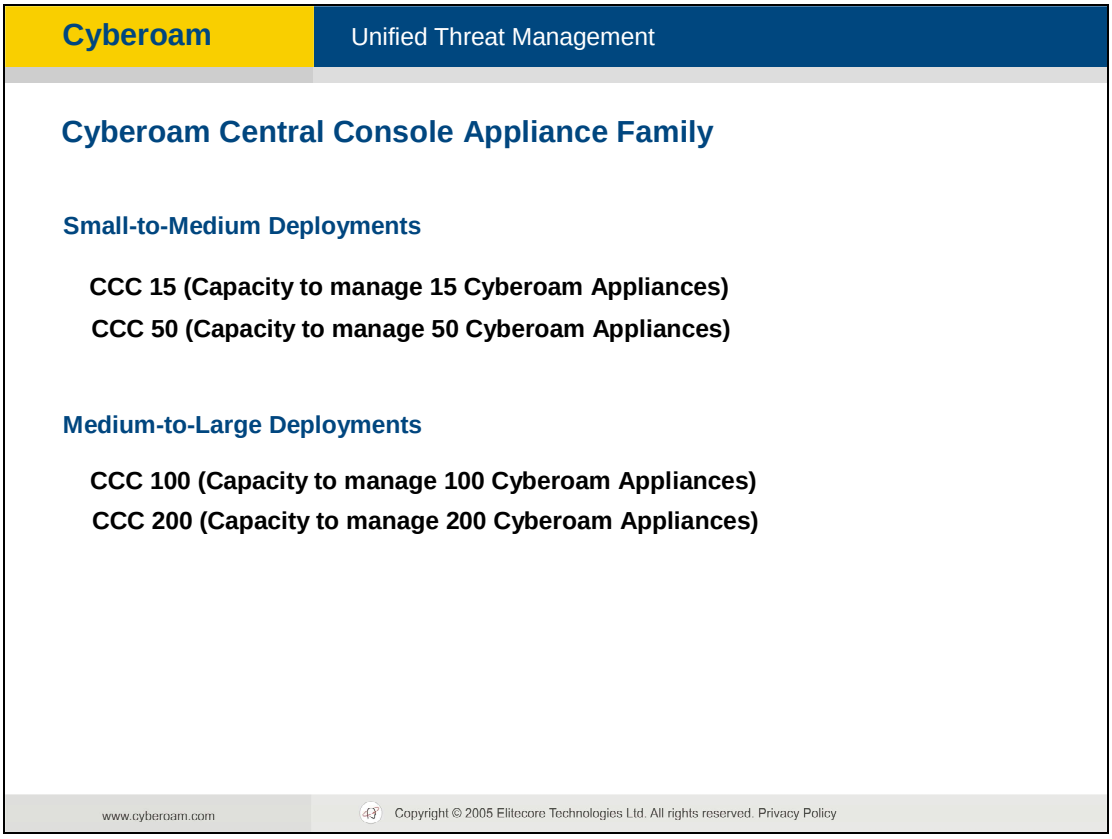
Cyberoam Central Console for MSSPs and Large Enterprises:

With the increasing complex networks which are spread over multiple geographical locations, the security infrastructure of large enterprises and Managed Security Service Providers (MSSPs) demands complete visibility into remote network activities. The enterprises struggle to implement, monitor and control a single enterprise-wide security policy, raising security, productivity and legal issues so as to identify and take rapid enterprise-wide action and enforce distributed security.

Cyberoam Central Console imparts MSSPs the ability to implement a broad security policy across multiple clients which simplifies operations while maintaining high security levels across client networks.

For the large enterprises having multiple devices at distributed branches, Cyberoam Central Console enables the administrators to push work-profile based security policies to remote locations thus allowing implementation of enterprise wide standard security policy. Cyberoam's centralised Web GUI enables remote management of all distributed Cyberoam security devices including policy management, compliance enforcement, monitoring and control. Cyberoam's easy-to-deploy and configure central console manages the task of configuring remote groups, devices, users and roles in easy steps.

CCC Online Demo is available at: http://demo.cyberoam.com



Cyberoam Central Console – Product Screen Shots - Dashboard

Click to view "Device Level Dashboard" for all devices under this group.

Cyberoam IPSec VPN Client

Cyberoam IPSec VPN client is software for Windows that allows establishing secure connections over the Internet between a remote user and the Corporate Intranet. IPSec is one of the most secure ways to connect to the enterprise as it provides strong user authentication, strong tunnel encryption with ability to cope with existing network and firewall settings

Where most of the competitors are hardware dependant, Cyberoam IPSec VPN Client is interoperable and compatible with all VPN IPSec compliant gateways and runs on Windows 98, Me, NT4, 2000, XP, Vista, Windows 7 (32 & 64 bits) workstations.

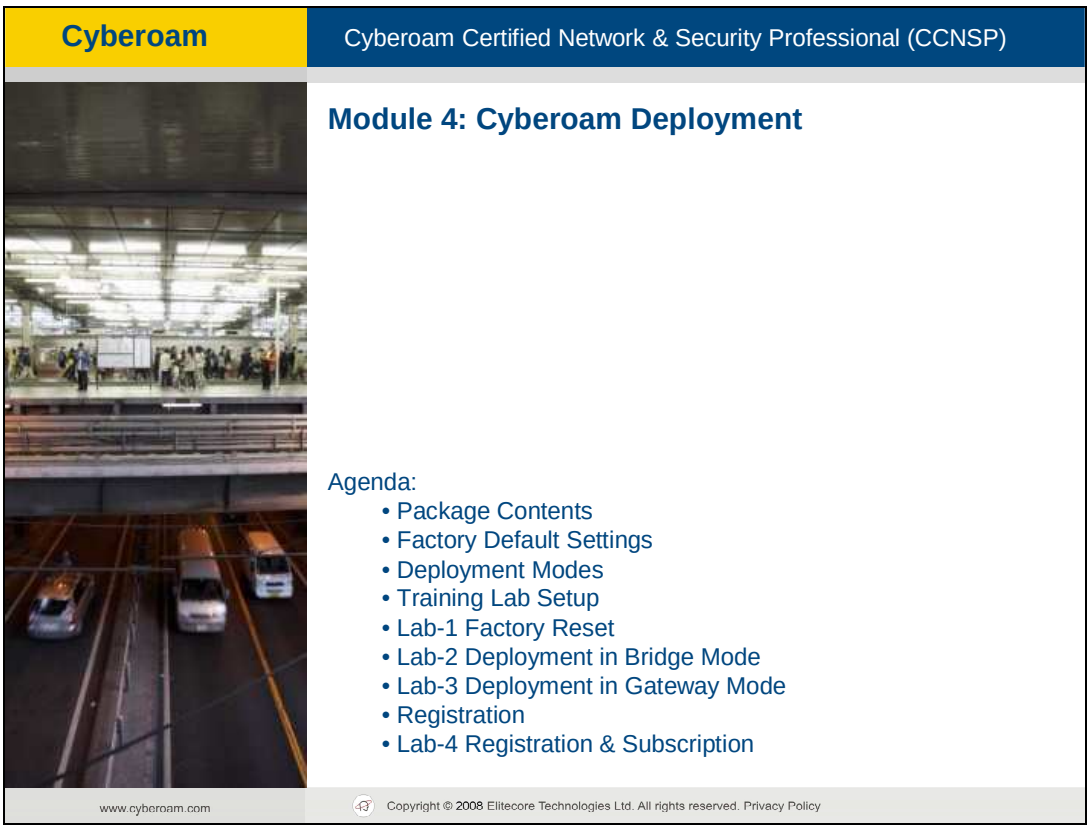
Cyberoam solution auto generates the configuration file for the VPN client, eliminating the need for technical know-how and simplifying configuration. Cyberoam IPSec VPN delivers secure, encrypted tunnels with high performance and low bandwidth requirements.

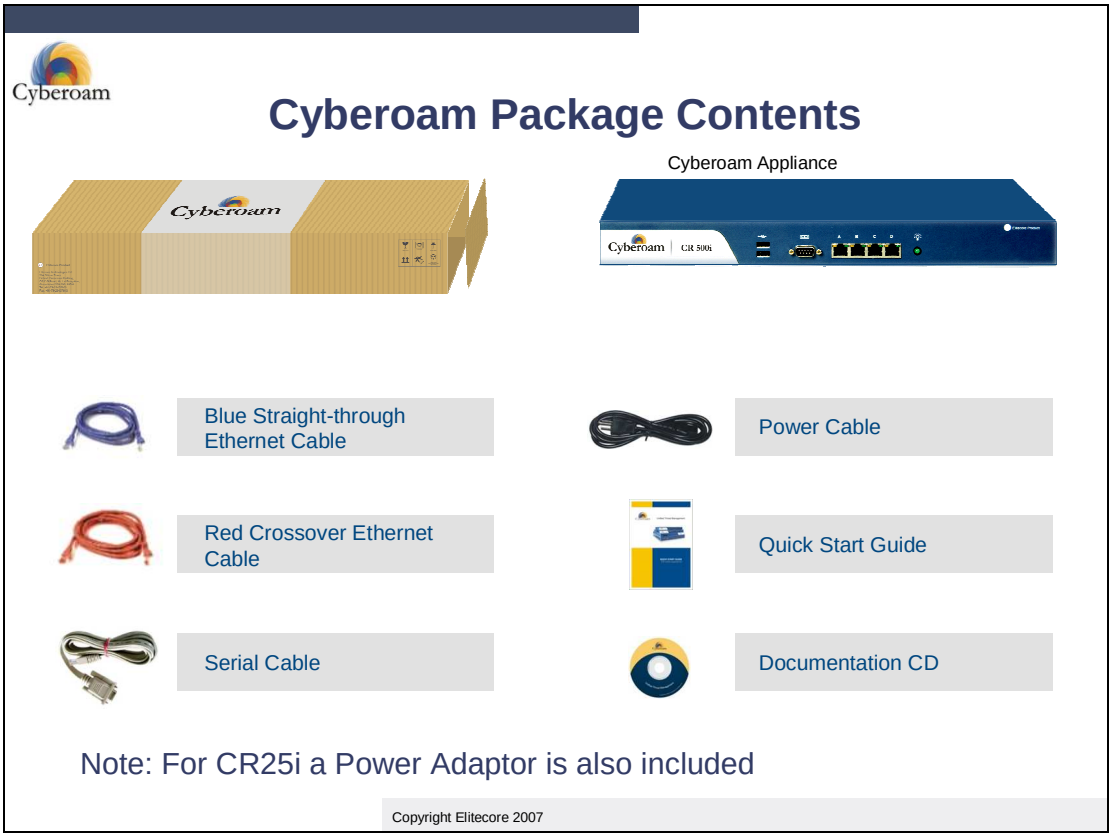
Cyberoam provides a simple interface with which setting up a VPN does not remain a painful task.

Licensing: Cyberoam IPSec VPN Client license is based on per device license with life time validity.

Download Client:
http://www.cyberoam.com/downloads/vpnclient/CyberoamVPNClient_Setup.exe

Module 4: Cyberoam Deployment



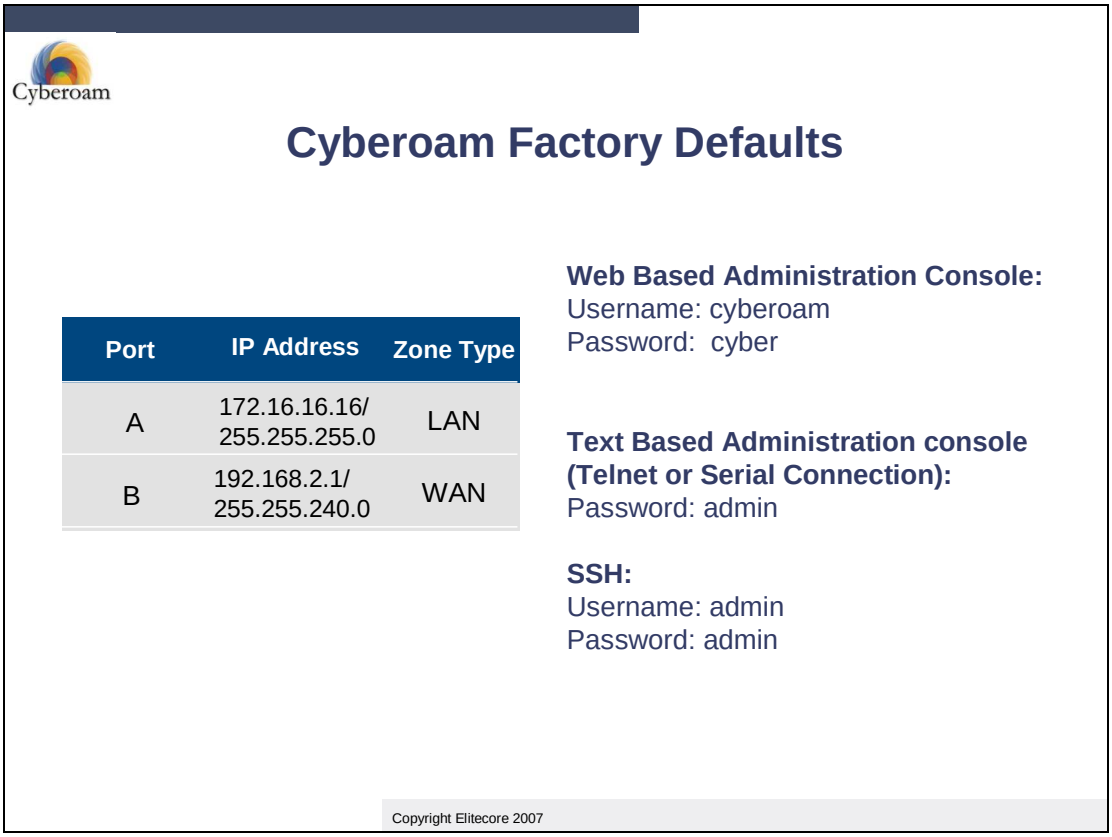


Cyberoam Package Contents

Checking the package contents - Check that the package contents are complete.

- One Cyberoam Appliance
- One Serial Cable (Null-Modem Cable)
- One Straight-through Ethernet Cable
- One AC Adapter Cable
- One Crossover Ethernet Cable
- One Cyberoam Quick Start Guide
- Documentation CD

Factory Default Settings



Cyberoam Factory Default Settings

Default IP addresses

Ethernet Port	IP Address	Zone
A	172.16.16.16/255.255.255.0	LAN
B	192.168.2.1/255.255.240.0	WAN

Default Username & Password

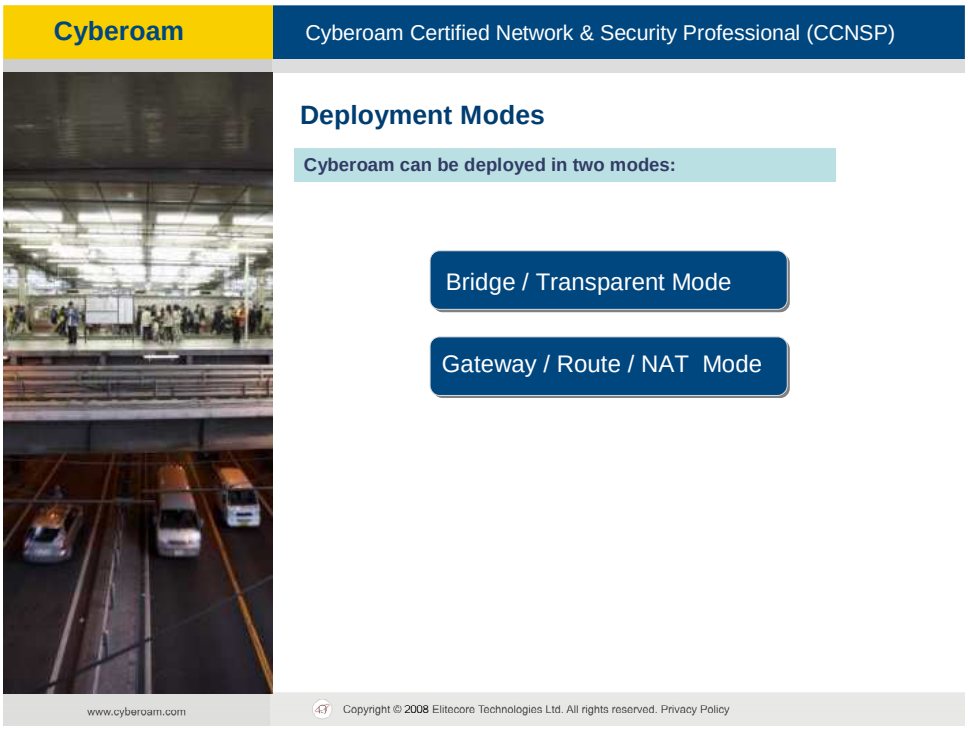
Web Admin Console	
*Username	cyberoam
*Password	cyber

CLI Console (SSH/Serial Connection)	
*Password	admin

* Username and Password are case sensitive

Deployment Modes

Deployment Modes



Before configuring, you need to plan the deployment mode of Cyberoam. Cyberoam can be placed in Bridge or Gateway/Route mode according to your requirement.

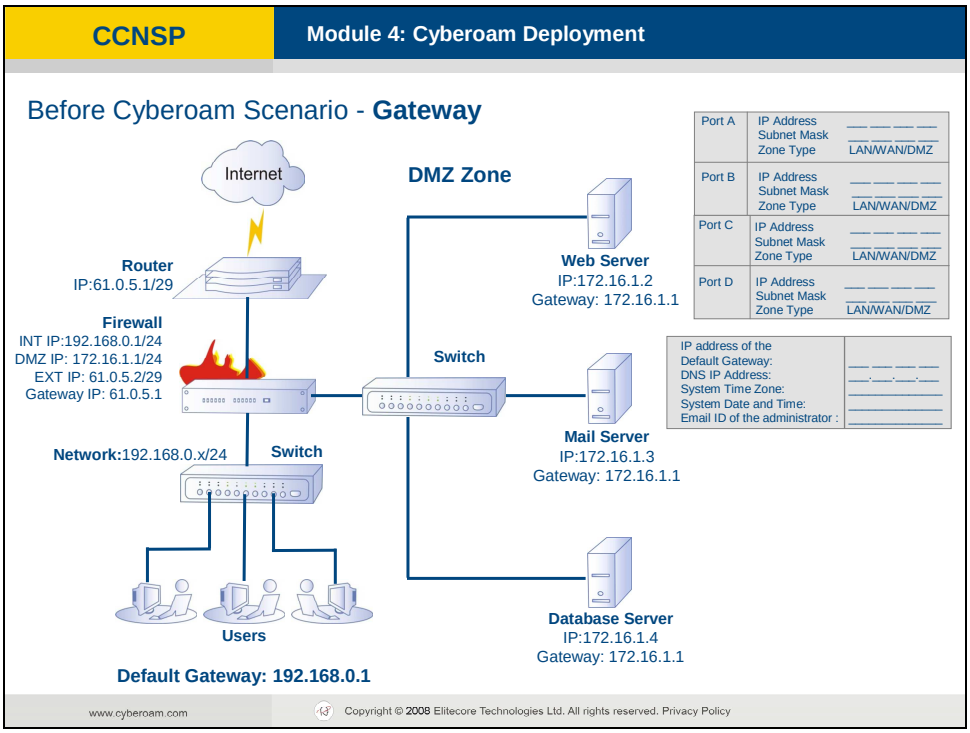
To control the Internet access through Cyberoam the entire Internet bound traffic from the LAN network should pass through Cyberoam.

Gateway mode:

Cyberoam | Unified Threat Management

Gateway/Route/NAT Mode

- You want to replace your existing firewall or router acting as a gateway for your network with Cyberoam
- You want your gateway to act as a VPN server
- You want redundancy in your network with by utilizing the multilink and HA (High-Availability) features of Cyberoam
- You want to configure separate DMZ zone to protect servers from LAN & WAN zone.


CCNSP
Module 4: Cyberoam Deployment
Before Cyberoam Scenario - Gateway
Internet
Router
IP:61.0.5.1/29
Firewall
INT IP:192.168.0.1/24
DMZ IP: 172.16.1.1/24
EXT IP: 61.0.5.2/29
Gateway IP: 61.0.5.1
Network:192.168.0.x/24
Switch
Users
DMZ Zone
Switch
Web Server
IP:172.16.1.2
Gateway: 172.16.1.1
Mail Server
IP:172.16.1.3
Gateway: 172.16.1.1
Database Server
IP:172.16.1.4
Gateway: 172.16.1.1
Default Gateway: 192.168.0.1
Port A
IP Address
Subnet Mask
Zone Type
LAN/WAN/DMZ
Port B
IP Address
Subnet Mask
Zone Type
LAN/WAN/DMZ
Port C
IP Address
Subnet Mask
Zone Type
LAN/WAN/DMZ
Port D
IP Address
Subnet Mask
Zone Type
LAN/WAN/DMZ
IP address of the Default Gateway:
DNS IP Address:
System Time Zone:
System Date and Time:
Email ID of the administrator :
www.cyberoam.com
Copyright © 2008 Elitecore Technologies Ltd. All rights reserved. Privacy Policy

Gateway Mode

Gateway

Gateway is a network point that acts as an entry point to another network or subnet to access the resources. In Enterprises, the gateway is the appliance that routes the traffic from a workstation to the outside network. In homes, the gateway is the ISP that connects the user to the Internet.

Gateway Mode

Cyberoam when deployed in Gateway mode acts as a Gateway for the networks to route the traffic.

When to use Gateway Mode:

Gateway mode provides an ideal solution for networks that already have an existing firewall and plans to replace their existing firewall and wish to add the security through Cyberoam's deep-packet inspection, Intrusion Prevention System Services, Gateway Anti Virus, and Gateway Anti spam. If you do not have Cyberoam security modules subscriptions, you may register for free trial.

Choose gateway mode if you want to use Cyberoam as

- A firewall or replace an existing Firewall
- A gateway for routing traffic
- Link load balancer and implement gateway failover functionality
- VPN Gateway
- A redundant (High Availability) gateway

Features supported in Gateway mode

All the features except Hardware bypass (LAN bypass) are available in Gateway mode.

Bridge Mode

Cyberoam when deployed in Bridge mode acts as a Transparent for the networks. Device will act as a transparent bridge and will operate in Layer 2 - MAC layer.

When to use Bridge Mode:

Bridge mode provides the ideal solution for networks that already have an existing firewall or router acting as a Gateway and customer don't want to replace the firewall, but still wish to add the security through Cyberoam's deep-packet inspection, Intrusion Prevention System Services, Gateway Anti Virus, and Gateway Anti spam. If you do not have Cyberoam security modules subscriptions, you may register for free trial.

This mode of deployment is agreed without changing any network schema of the organisation's internal infrastructure.

Choose bridge mode if you want to use Cyberoam as

- You already have a firewall or a router acting a gateway for your network and you don't want to change the existing setup
- Want to use Cyberoam for reporting.
- Want Cyberoam as a drop-in solution for Viruses, Spam, Content-Filtering and IPS and Bandwidth Management.
- Want to try-out Cyberoam without changing your existing setup.

Features supported in Bridge Mode

All the features except the following features won't be available in Bridge mode.

- Virtual Private Network (VPN)
- Multi Link Manager (MLM)
- DMZ Zones
- High Availability (HA)

CCNSP | Module 4: Cyberoam Deployment

Hardware Bypass in Transparent Mode

- When the appliance is deployed in Transparent mode and if there is a power failure, hardware problem or a software malfunction the appliance goes into 'Bypass' mode.
- In Bypass mode the bypass interfaces of the appliance get bridged and start acting like a hub.
- The traffic flow is not interrupted thus resulting in high network uptime.
- Hardware Bypass functionality is only available in Transparent Mode not in Gateway Mode.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Hardware Bypass in Transparent Mode

- CR 50ia,CR 100ia,CR200i, CR 300i, CR500i, CR1000i and CR1500i come with hardware bypass feature
- In CR 50ia, CR 100ia, ports A and B have the bypass functionality available only on power failure.
- In CR 200ia and CR 300i ports C and D have the bypass functionality available.
- In CR500ia ports "A and B" and "C and D" have the bypass functionality available.
- In CR 1000i and CR1500i ports "A and B" "C and D" have the hardware bypass function available.
- A Blue LED on the front panel of the appliance blinks when hardware bypass is active.

Web Proxy mode:

Cyberoam can also act as a Web proxy server.

To use Cyberoam as a Web proxy server, configure Cyberoam LAN IP address as a proxy server IP address in your browser setting and enable access to Web proxy services from Local ACL section.

Under Web Proxy Configuration:

This configuration is applicable only when Cyberoam is configured as Web Proxy.

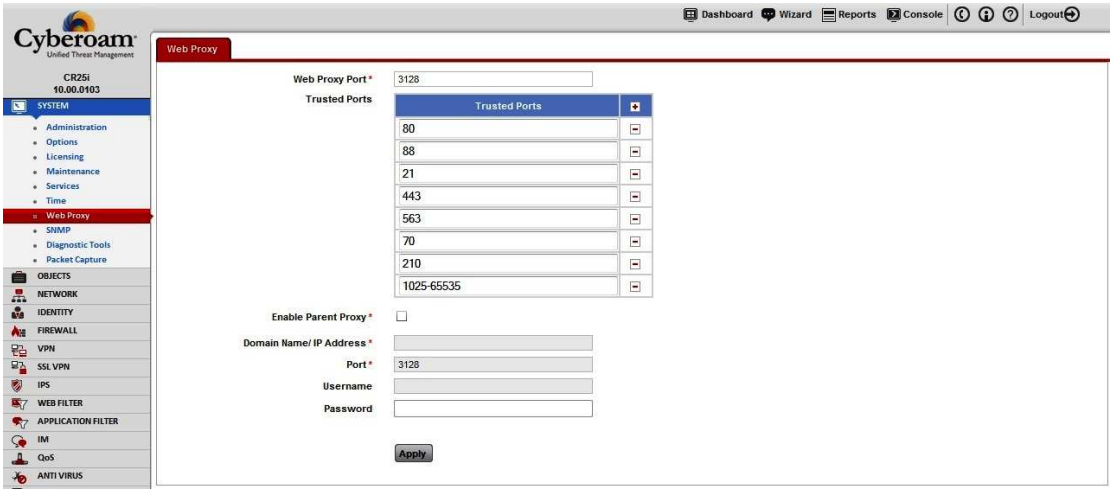
Enter Port number which is to be used for Web Proxy and click Save
Under Web Proxy Trusted Ports Setting, click Add to add the trusted ports.
Cyberoam allows the access to those sites which are hosted on standard port only if deployed as Web proxy. To allow access to the sites hosted on the non-standard ports, you have to define non-standard ports as trusted ports.

Under Parent proxy setting:

Click 'Enable Parent Proxy'. If enabled all the HTTP requests will be sent to HTTP Parent proxy server via Cyberoam. One needs to configure Parent Proxy when the HTTP traffic is blocked by the upstream Gateway.

When do we require Cyberoam to be configured in Web proxy mode?

- You would like to replace existing software / appliance based proxy solution
- You would like to use Cyberoam Identity based features along with Content Filtering / Bandwidth Management / Anti-virus / User based Reporting.
- You want to use Cyberoam as a drop in solution in proxy mode.
- You don't want to make any major changes with you existing proxy setup



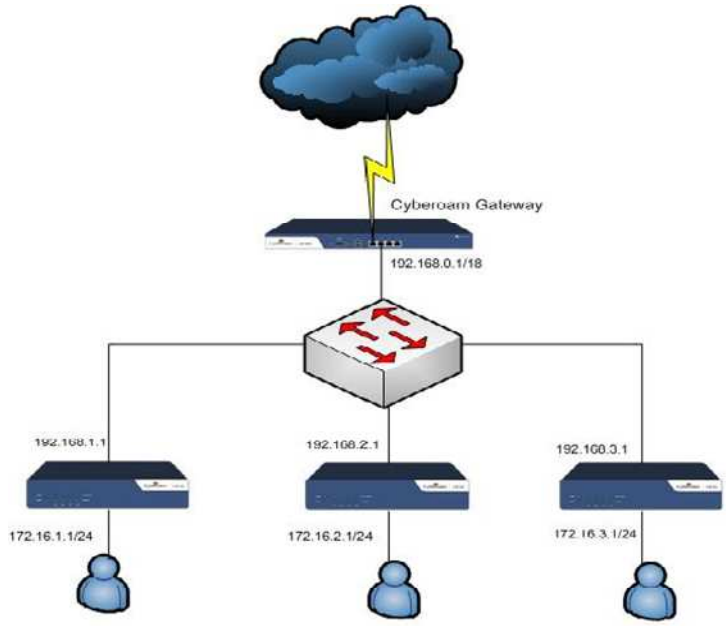
- The Default Web Proxy port is 3128. Cyberoam listens on this port number 3128 for proxy requests from the users.

- Parent Proxy can be enabled and the IP address of external proxy server can be provided. If the external proxy server is asking for authentication, the username and password can be also configured.

Training Lab Setup

Cyberoam | Unified Threat Management

Lab Setup



Cyberoam | Unified Threat Management

Lab IP Schema:

Lab Setup:

Each student will be given one Cyberoam appliance. Below is going to be IP Schema of Lab:

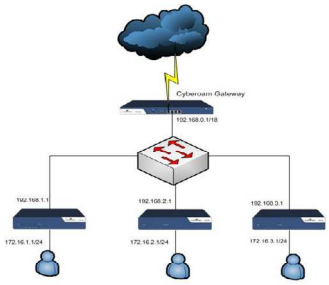
Lab Gateway Appliance:

Gateway device will provide internet connectivity to student appliances. Gateway device will just act as a firewall and will not do Anti-Virus / Anti-Spam / IPS / Content Filtering task.

Gateway LAN IP: 192.168.0.1 Subnet Mask: 255.255.0.0

Student IP Schema:

Student x: (x = student number)
WAN IP: 192.168.x.1 Subnet Mask: 255.255.0.0
LAN IP: 172.16.x.1 Subnet Mask: 255.255.255.0
DMZ IP: 10.10.x.1 Subnet Mask: 255.255.255.0



Lab Setup:

Each student will be given one Cyberoam appliance. Below is going to be IP Schema of Lab:

Lab Gateway Appliance:

Gateway device will provide internet connectivity to student appliances. Gateway device will just act as a firewall and will not do Anti-Virus / Anti-Spam / IPS / Content Filtering task.

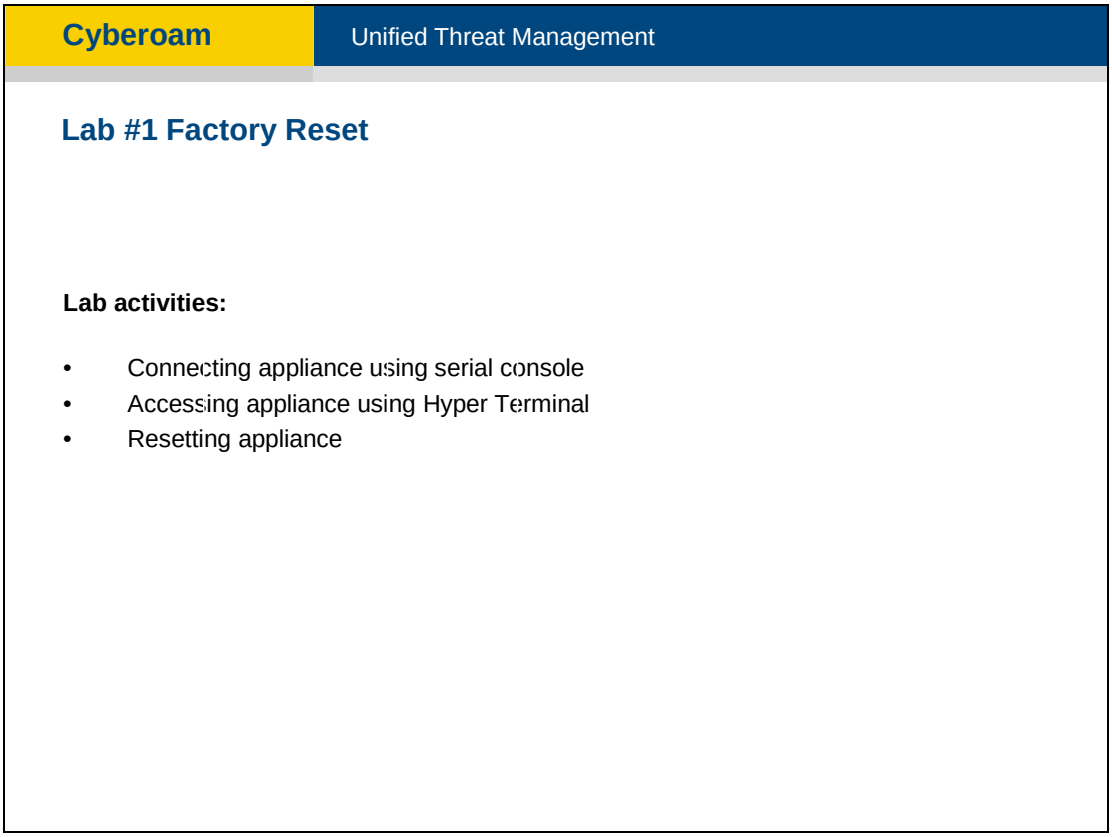
Gateway LAN IP: 192.168.0.1 Subnet Mask: 255.255.0.0

Student IP Schema:

Student x: (x = student number)

WAN IP: 192.168.x.1 Subnet Mask: 255.255.0.0
LAN IP: 172.16.x.1 Subnet Mask: 255.255.255.0
DMZ IP: 10.10.x.1 Subnet Mask: 255.255.255.0

Lab #1 Factory Reset



Lab #1 Factory Reset

Lab activities:

1. Connecting appliance using serial console
2. Accessing appliance using Hyper Terminal
3. Resetting appliance

Lab #1 Factory Reset

Objective:

Factory reset the Cyberoam appliance.

Factory Reset will remove all user configurations and will bring appliance back into Factory Default configuration.

Factory reset is useful in following cases:

- New deployments – Good to do the factory reset and start deployment with initial steps.
- Lost both Web Admin Console and CLI password.

Note: Factory reset will remove entire user configuration so please backup Cyberoam configuration before proceeding.

Lab #1 Factory Reset
Activity 1: Connecting Appliance using serial console

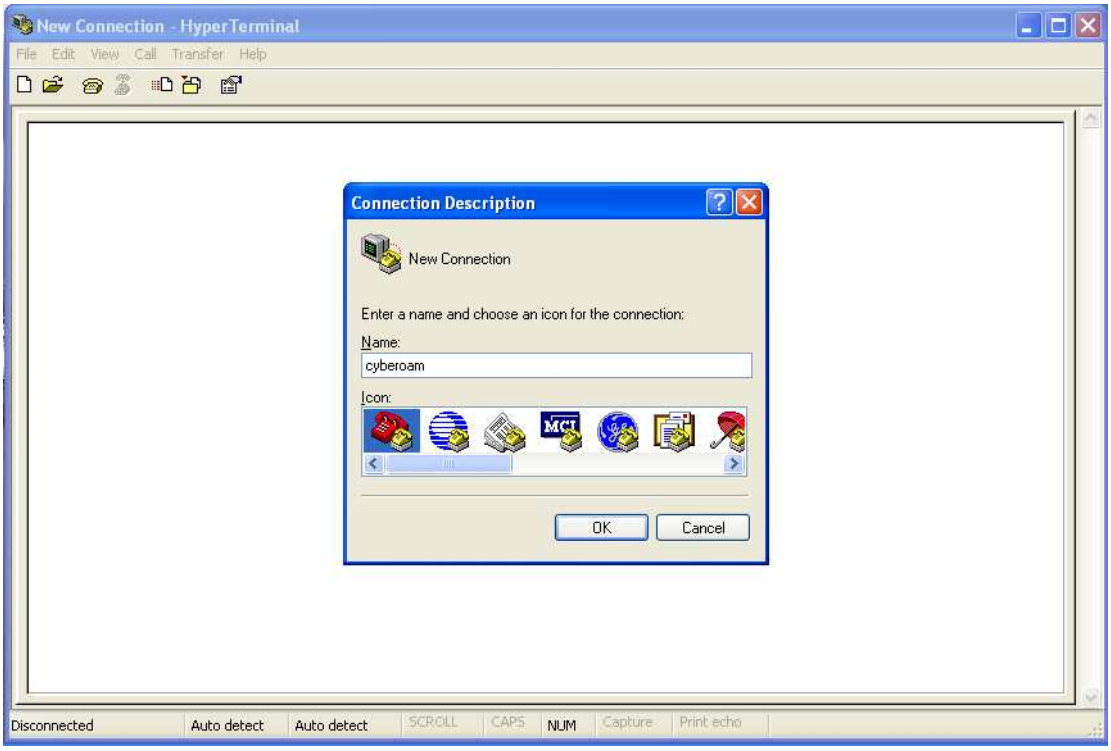
Due to security reasons, a factory reset can be done only from serial console as factory reset will wipe out entire user defined configuration and reports.

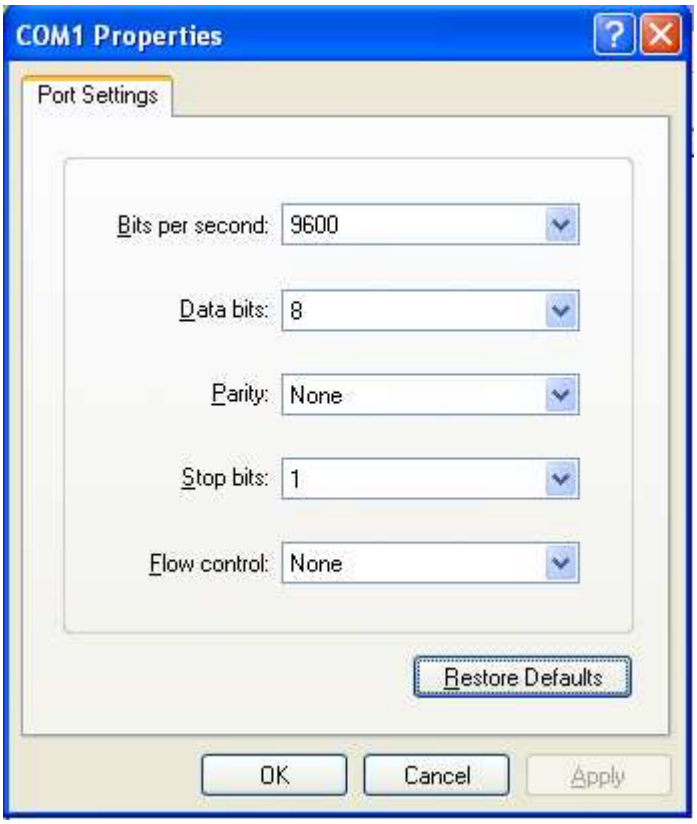
Each appliance ships with a serial console cable. Connect the serial console cable to computer serial port and front side serial port of appliance.

Lab #1 Factory Reset
Activity 2: Accessing appliance using Hyper Terminal

Hyper terminal or Secure CRT can be use to access Cyberoam appliance connected using serial console cable.

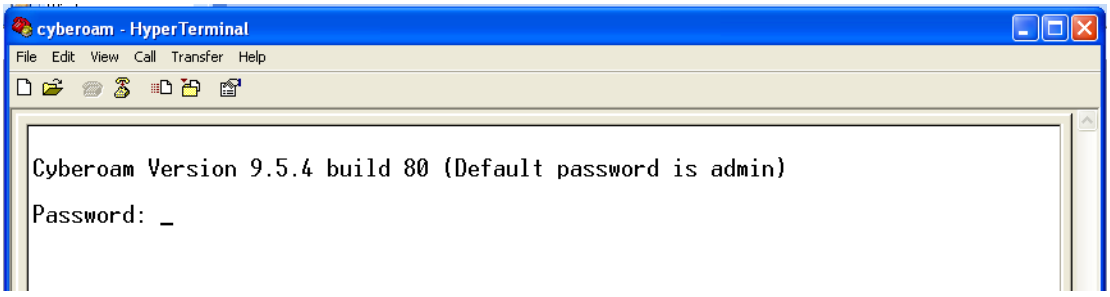
The screenshots below show how to access Cyberoam using Hyper Terminal:





Note: Cyberoam will use the default configuration port settings. Click on “Restore Defaults” before proceeding.

After successfully connecting Cyberoam with the serial console, you should be able to see Cyberoam password prompt as shown in below screen:



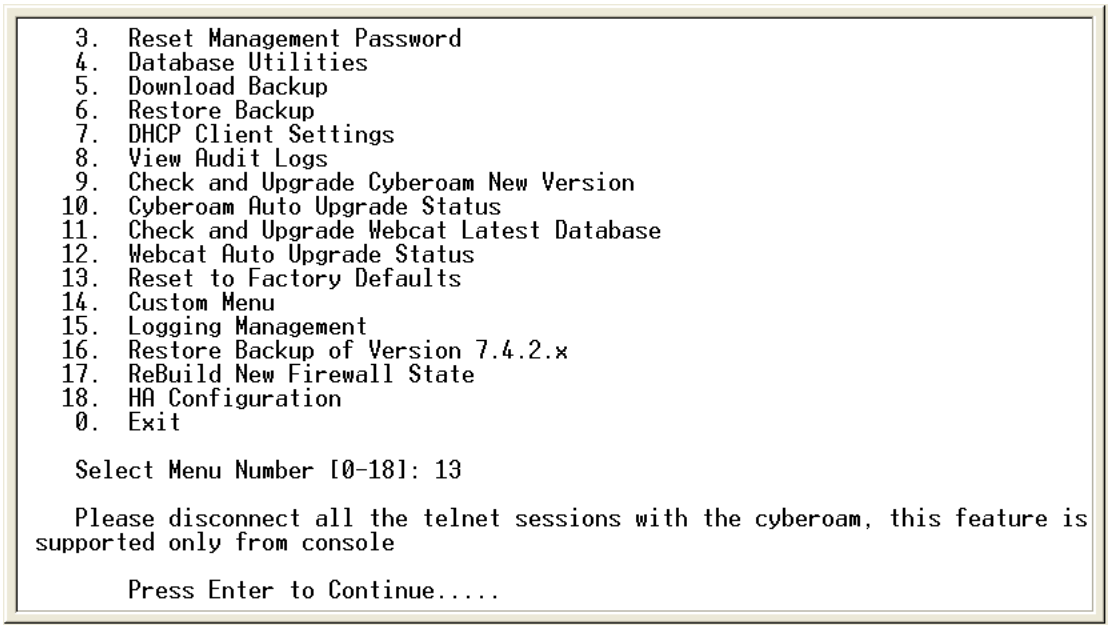
Lab #1 Factory Reset
Activity 3: Resetting appliance

The Cyberoam factory reset can be carried out in two ways:

- Type “RESET” on password prompt if you forgot both Web Admin Console and CLI password.
- Type password on prompt and select:
  - Option 5: Cyberoam Management
  - Option 13: Reset to factory defaults

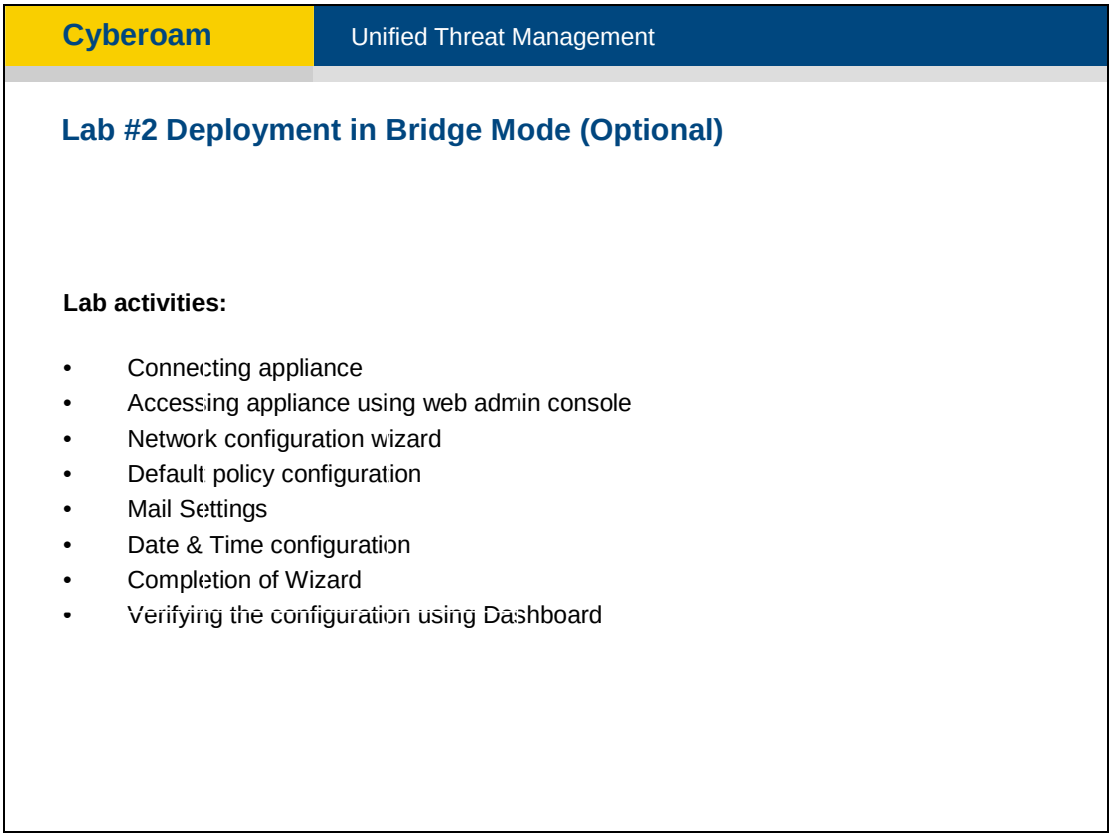
```
Cyberoam Corporate Version 9.5.4 build 80

Main Menu

    R.  Restart Management Services
    1.  Network  Configuration
    2.  System   Configuration
    3.  Route    Configuration
    4.  Cyberoam Console
    5.  Cyberoam Management
    6.  Upgrade  Version
    7.  Bandwidth Monitor
    8.  VPN Management
    9.  Shutdown/Reboot Cyberoam
    0.  Exit

    Select Menu Number [0-9]:
```

```
Cyberoam Management

    1.  Restart Management Services
    2.  Remove Firewall Rules
    3.  Reset Management Password
    4.  Database Utilities
    5.  Download Backup
    6.  Restore Backup
    7.  DHCP Client Settings
    8.  View Audit Logs
    9.  Check and Upgrade Cyberoam New Version
   10.  Cyberoam Auto Upgrade Status
   11.  Check and Upgrade Webcat Latest Database
   12.  Webcat Auto Upgrade Status
   13.  Reset to Factory Defaults
   14.  Custom Menu
   15.  Logging Management
   16.  Restore Backup of Version 7.4.2.x
   17.  ReBuild New Firewall State
   18.  HA Configuration
    0.  Exit

    Select Menu Number [0-18]:
```



Now appliance will reboot and will come up with factory default settings.

Lab #2 Deployment in Bridge Mode (Optional)



Deployment Lab #2 Deployment in Bridge Mode (Optional)

Lab activities:

- Connecting appliance
- Accessing appliance using web admin console
- Network configuration wizard
- Default policy configuration
- Mail Settings
- Date & Time Configuration
- Completion of Wizard
- Verifying the configuration using Dashboard

Lab #2 Deployment in Bridge Mode

Objective:

Deployment of Cyberoam UTM Appliance in Bridge Mode as per given LAB setup.

This example lab will use IP Schema of student-1, student need to use their student number in IP Schema.

IP Schema of student-1

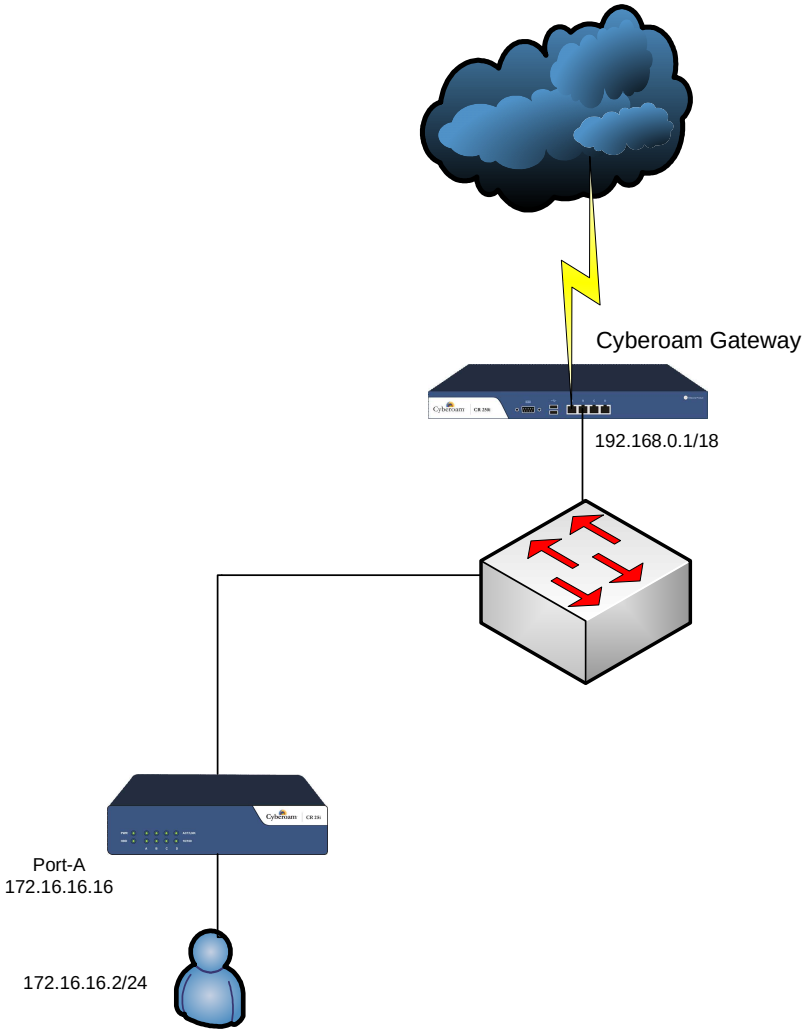
Bridge IP: 192.168.1.1 Subnet Mask: 255.255.0.0
Bridge Gateway: 192.168.0.1 Subnet Mask: 255.255.0.0

Computer IP: 192.168.1.2 Subnet Mask: 255.255.0.0
Computer Gateway: 192.168.0.1 Subnet Mask: 255.255.0.0

Lab #2 Deployment in Bridge Mode
Activity 1: Connecting Appliance

Connect port A of the Appliance to your computer Ethernet interface using crossover Ethernet cable. A crossover cable is provided with the appliance.

Connect port B of the Appliance to switch for WAN connectivity using the straight Ethernet cable.



Lab #2 Deployment in Bridge Mode
Activity 2: Accessing appliance using web admin console

The appliance has the following factory default settings:

Port-A: 172.16.16.16/24

Set the IP address of your computer to 172.16.16.2/24.

Connecting to Web Admin Console

Browse to https://172.16.16.16 to access Cyberoam Web Console (GUI). The Cyberoam login page is displayed and you are prompted to enter login credentials.

Use the default username and password to log on.

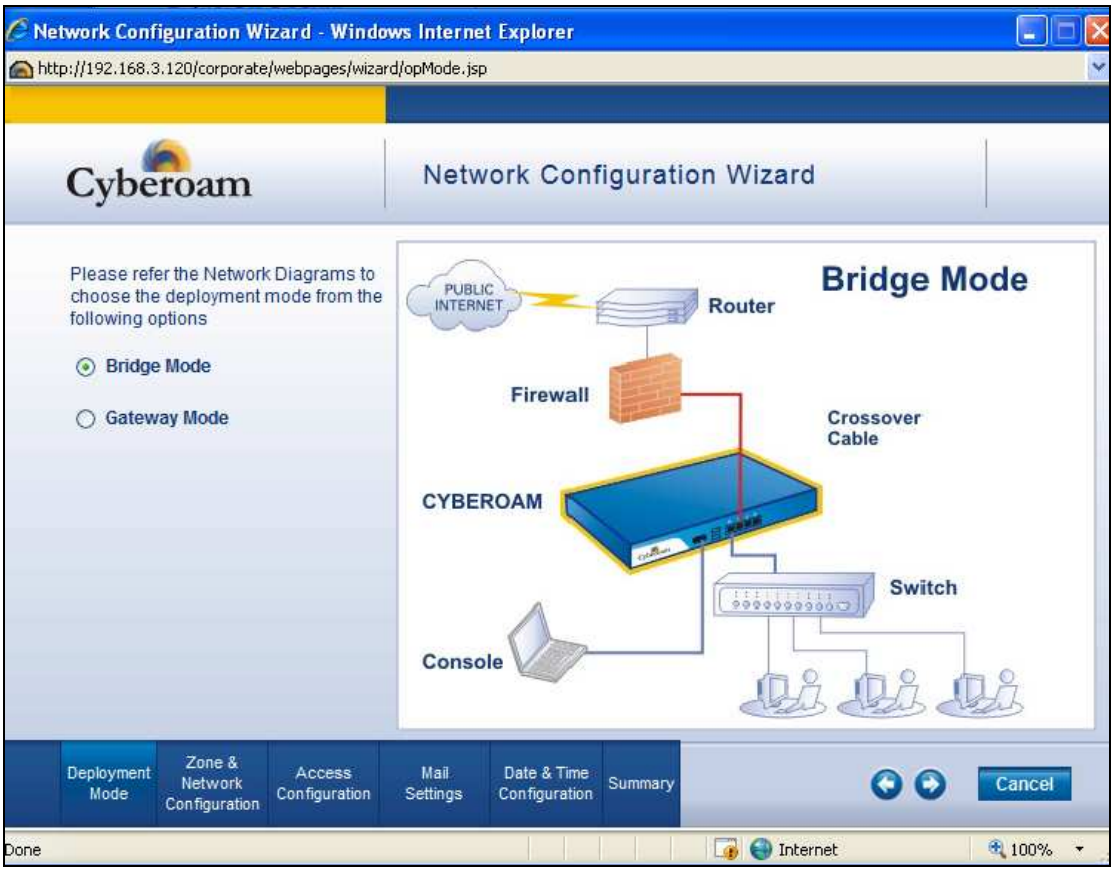
Default username: cyberoam
Password: cyber

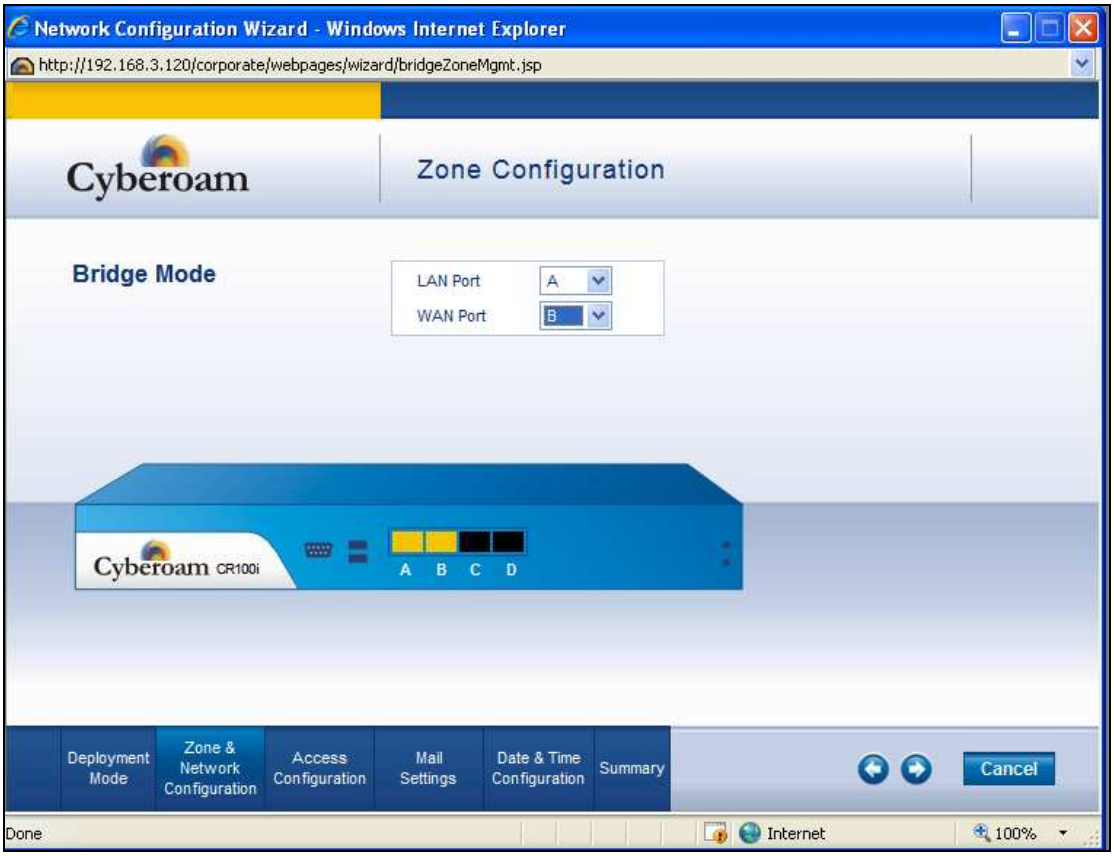
If you cannot log on, verify the following configurations:

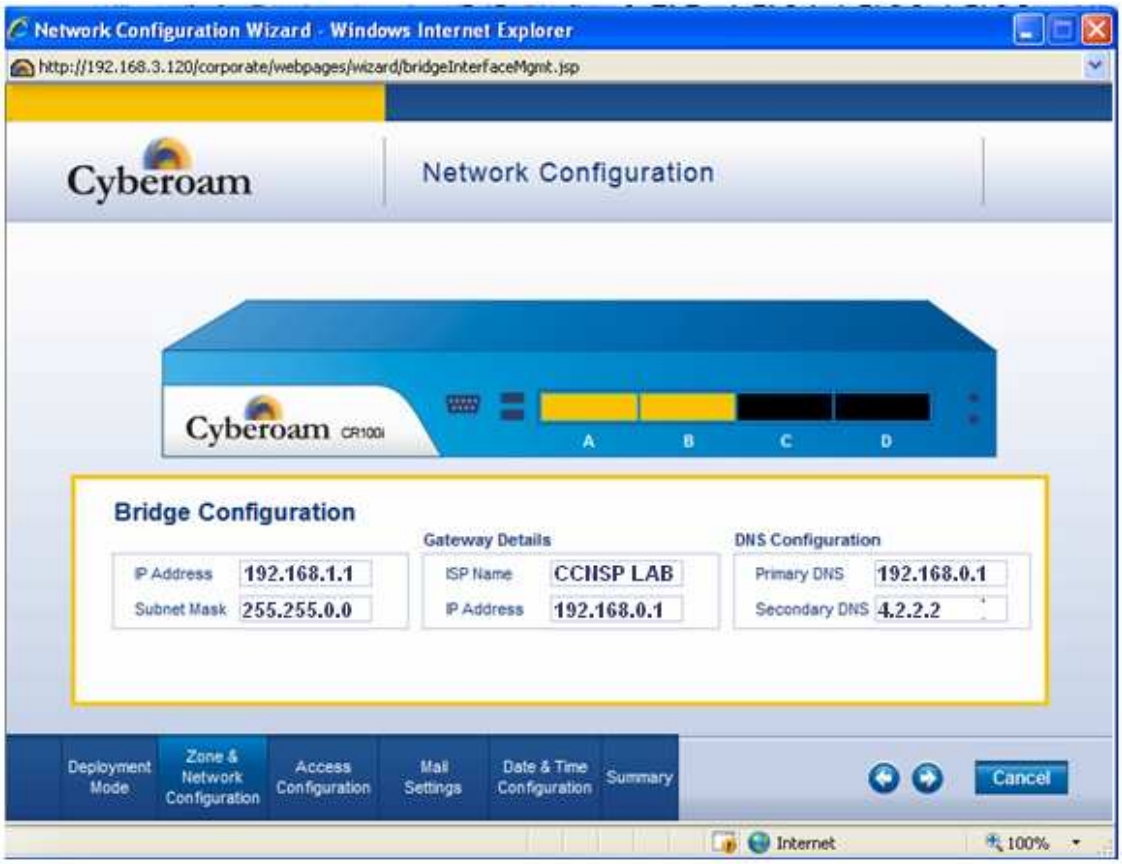
- Did you plug your computer Ethernet cable into the port A on the appliance? - Deployment can only be performed through port A.
- Is the link light glowing on both the computer and the Appliance? – If not, check and replace the cable
- Is your computer set to a static IP address of 172.16.16.16 and subnet as 255.255.255.0?
- Did you enter correct IP address in your Web browser?

Lab #2 Deployment in Bridge Mode
Activity 3: Network Configuration Wizard

Click the Wizard button on the top right of the Dashboard to start Network Configuration Wizard and click Start.


Network Configuration Wizard - Windows Internet Explorer
http://192.168.3.120/corporate/webpages/wizard/opMode.jsp
Cyberoam
Network Configuration Wizard
Please refer the Network Diagrams to choose the deployment mode from the following options
Bridge Mode
Gateway Mode
Bridge Mode
PUBLIC INTERNET
Router
Firewall
Crossover Cable
CYBEROAM
Switch
Console
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
Done
Internet
100%


Network Configuration Wizard - Windows Internet Explorer
http://192.168.3.120/corporate/webpages/wizard/bridgeZoneMgmt.jsp
Cyberoam
Zone Configuration
Bridge Mode
LAN Port
A
WAN Port
B
Cyberoam CR100i
A B C D
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
Done
Internet
100%


Network Configuration Wizard - Windows Internet Explorer
http://192.168.3.120/corporate/webpages/wizard/bridgeInterfaceMgmt.jsp
Cyberoam
Network Configuration
Cyberoam CR100i
A
B
C
D
Bridge Configuration
Gateway Details
DNS Configuration
IP Address 192.168.1.1
Subnet Mask 255.255.0.0
ISP Name CCNSP LAB
IP Address 192.168.0.1
Primary DNS 192.168.0.1
Secondary DNS 4.2.2.2
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
Internet
100%

Lab #2 Deployment in Bridge Mode
Activity 4: Default Policy Configuration

With the Cyberoam being firewall device, it blocks all inter zone traffic. The wizard gives the option to select policy for LAN -> WAN traffic from three pre-defined policies.

The following are the three pre-defined policies:

Monitor Only:

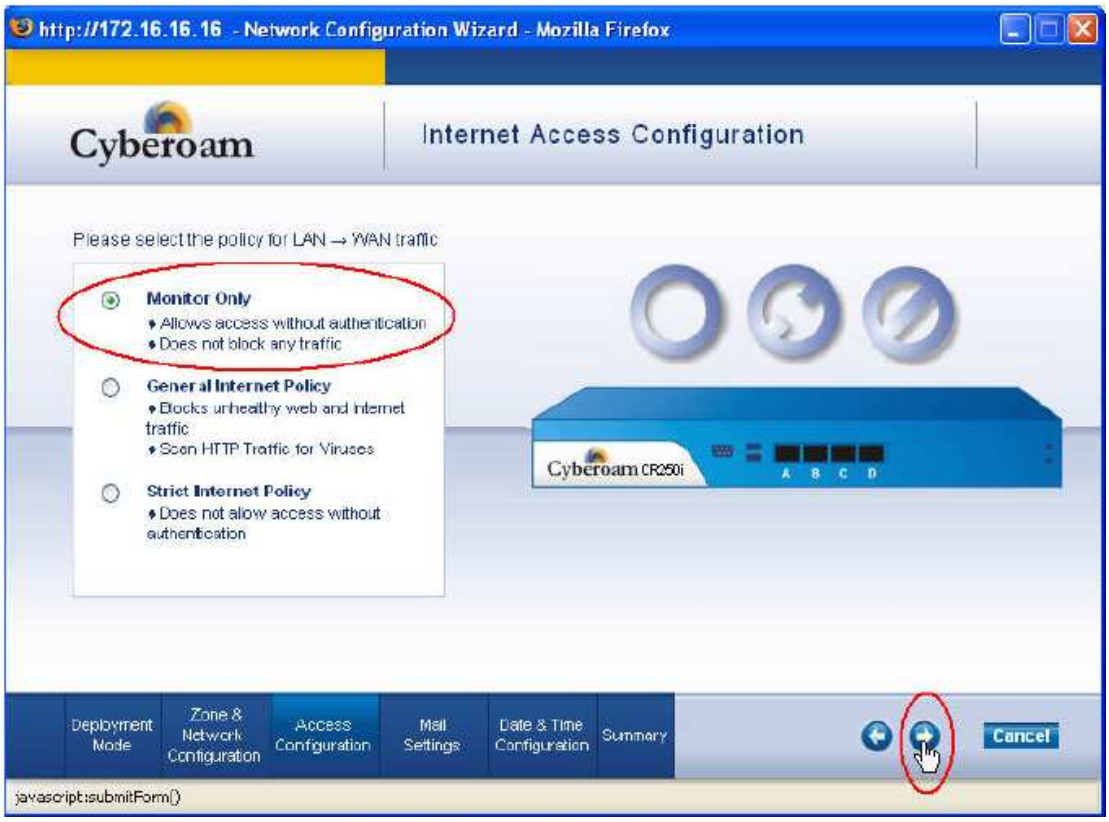
- Allow all outbound traffic without any authentication.
- No scanning.
- No content filtering.

General Internet Policy:

- Allow all outbound traffic without any authentication.
- Web traffic will be scanned for virus / malware / spyware.
- Content filtering will be “ON” by using default content filtering policy “General Corporate Policy” which blocks below web URL categories:
    - Porn, Nudity, Adult Content, URL Translation Sites, Drugs, Crime and Suicide, Gambling, Militancy and Extremist, Phishing and Fraud, Violence, Weapons

Strict Internet Policy:

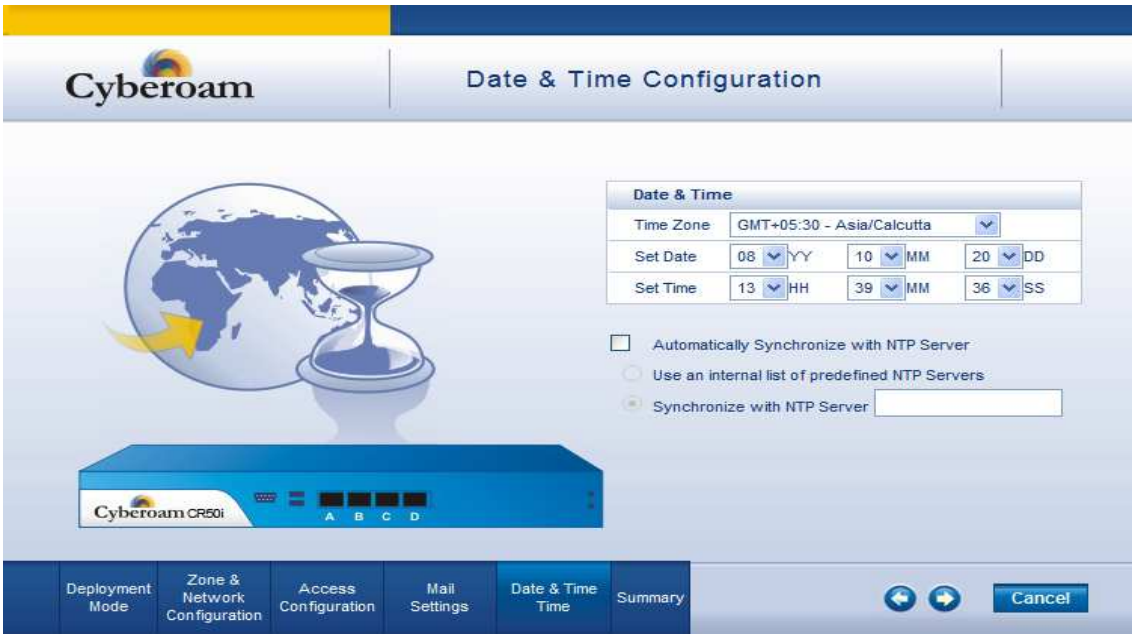
- Block all outbound unauthenticated traffic.
- Web traffic will be scanned for virus / malware / spyware.
- All traffic will be scanned by IPS engine.


http://172.16.16.16 - Network Configuration Wizard - Mozilla Firefox
Cyberoam
Internet Access Configuration
Please select the policy for LAN → WAN traffic
Monitor Only
• Allows access without authentication
• Does not block any traffic
General Internet Policy
• Blocks unhealthy web and internet traffic
• Scan HTTP Traffic for Viruses
Strict Internet Policy
• Does not allow access without authentication
Cyberoam CR250i
A B C D
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
javascript:submitForm()

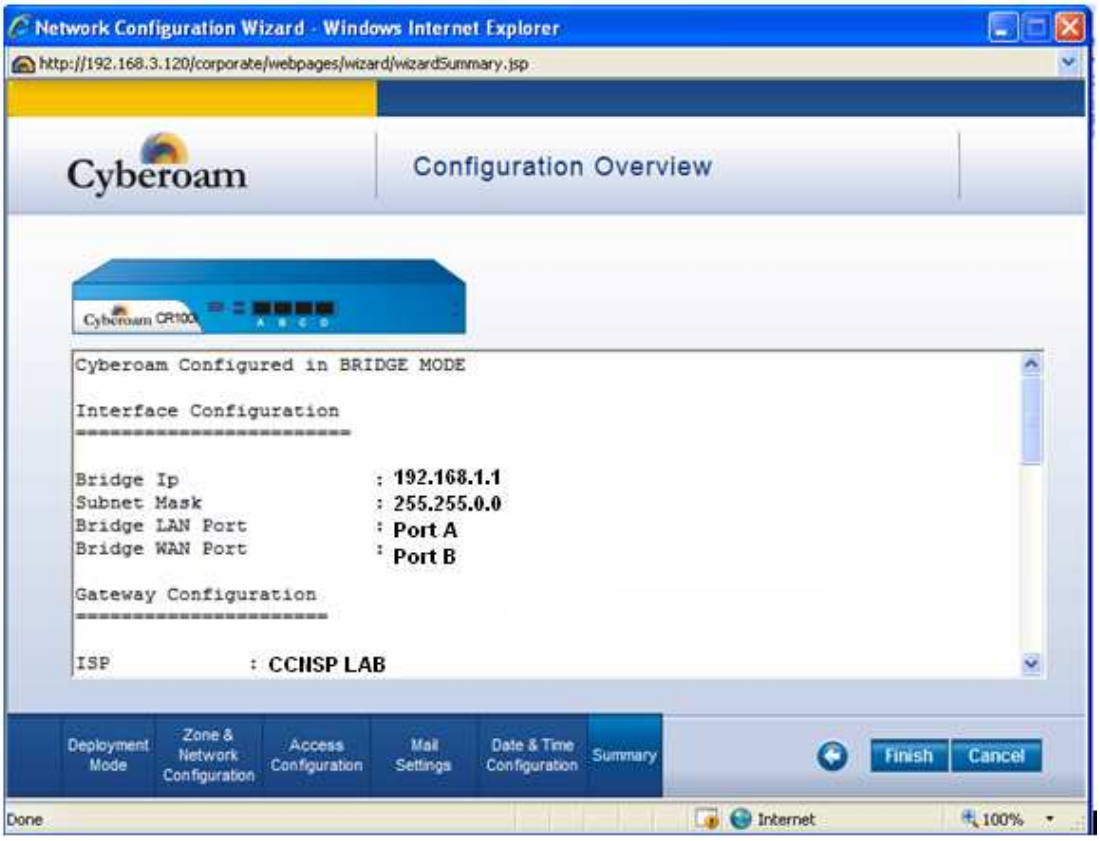
Lab #2 Deployment in Bridge Mode
Activity 5: Mail Settings

Configure mail server IP address, administrator email address from where the notification mails will be send and the email address of the notification recipient.

Lab #2 Deployment in Bridge Mode
Activity 6: Date & Time Configuration



Lab #2 Deployment in Bridge Mode
Activity 7: Completion of Wizard



Cyberoam will take time to restart, please wait for some time before clicking to access the Web Admin Console.

Now change your computer IP as default Cyberoam is changed from 172.16.16.16 to 192.168.1.1 and no more your computer will be able to access the appliance.

Change your computer IP as per your student number. For student #3 below is going to be IP:

Computer IP: 192.168.1.2 Subnet Mask: 255.255.0.0
Computer Gateway: 192.168.0.1 Subnet Mask: 255.255.0.0
DNS: 192.168.0.1

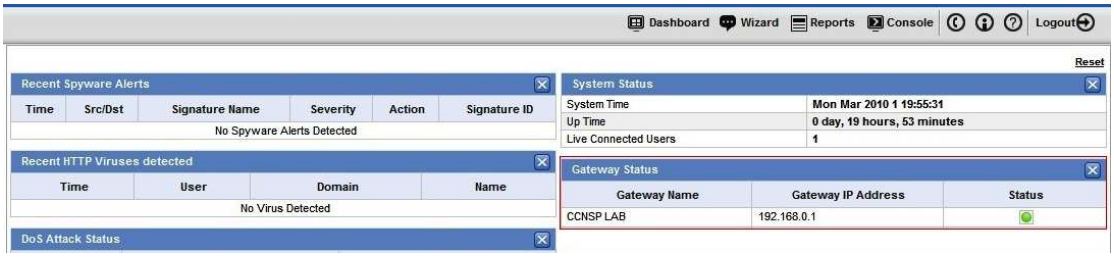
This completes the basic configuration of Cyberoam and now you are ready to use the Appliance.

Lab #2 Deployment in Bridge Mode
Activity 8: Verifying the configuration using Dashboard:

Browse to https:\\192.168.1.1 and log on to Web Admin Console using default username and password. Dashboard page is displayed on successful log on.

1. Verify appliance information
Check the Appliance Information section of Dashboard to verify configuration.

2. Verify gateway status
Check the Gateway Status of Dashboard and verify that the status of the gateway green i.e. UP.



3. Verify IP assignments

Go to Network →Interface page and check IP address assigned to Interfaces.

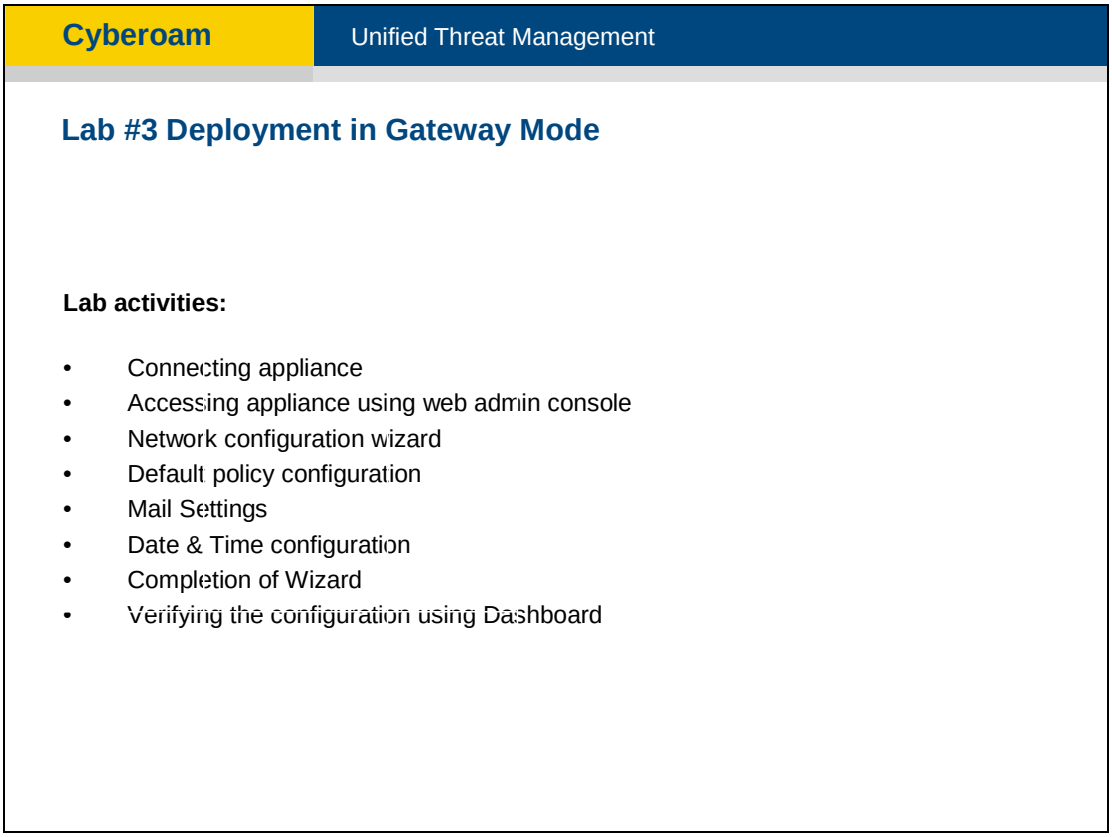
If you have not configured IP scheme properly, you can run the Network Configuration wizard and change the IP address.

4. Verify DNS status

In GUI, go to System → Services, and verify the DNS service is running as below:

Services	Status	Manage
Anti Spam	Running	Stop
Anti Virus	Running	Stop
Authentication	Running	Restart
DHCP Server	Stopped	Start
DNS	Running	Stop
IPS	Running	Stop
Web Proxy	Running	Restart

Lab #3 Deployment in Gateway Mode



Lab #3 Deployment in Gateway Mode

Lab activities:

- Connecting appliance
- Accessing appliance using web admin console
- Network configuration wizard
- Default policy configuration
- Mail Settings
- Date & Time Configuration
- Completion of Wizard
- Verifying the configuration using Dashboard

Lab #3 Deployment in Gateway Mode

Objective:

Deployment of Cyberoam UTM Appliance in Gateway Mode as per given LAB setup.

This example lab will use IP Schema of student-1, student need to use their student number in IP Schema.

IP Schema of student-1

WAN IP:
192.168.1.1 Subnet Mask: 255.255.0.0

WAN Gateway:
192.168.0.1 Subnet Mask: 255.255.0.0

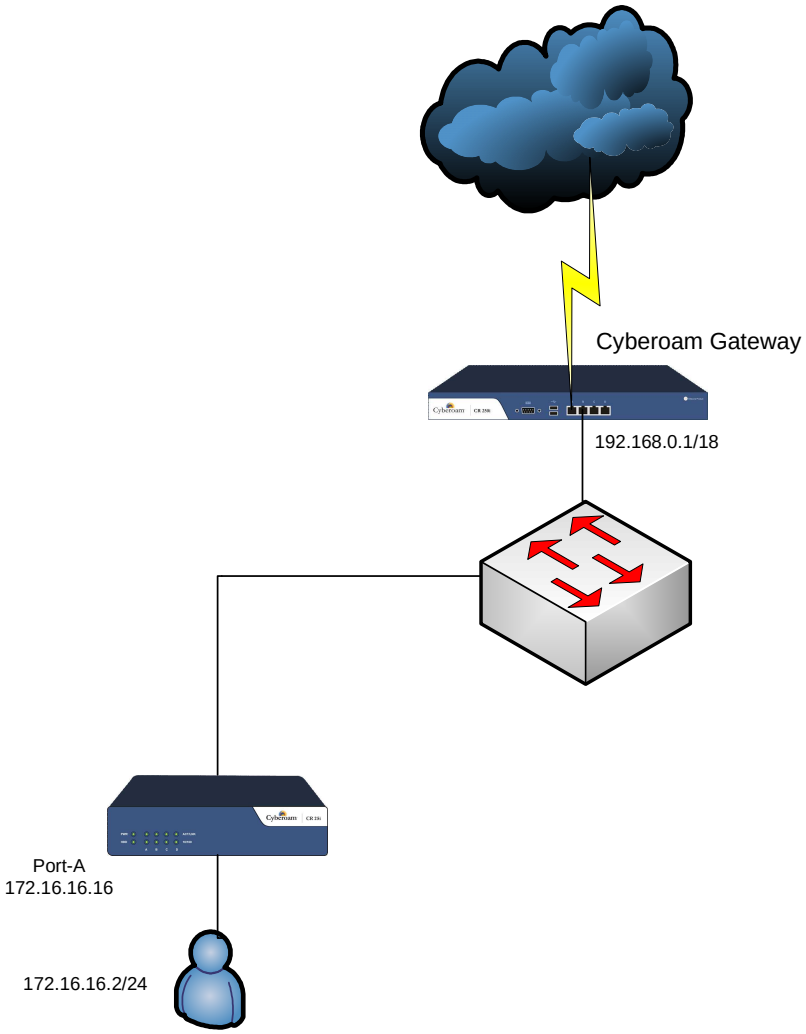
LAN IP:
172.16.1.1 Subnet Mask: 255.255.255.0

DMZ IP:
10.10.1.1 Subnet Mask: 255.255.255.0

Lab #3 Deployment in Gateway Mode
Activity 1: Connecting Appliance

Connect port A of the Appliance to your computer's Ethernet interface using the crossover Ethernet cable. A red crossover cable is provided with the appliance.

Connect port B of the Appliance to switch for WAN connectivity using the straight Ethernet cable.



Lab #3 Deployment in Gateway Mode
Activity 2: Accessing appliance using web admin console

The appliance has the following factory default settings:

Port-A: 172.16.16.16/24

Set the IP address of your computer to 172.16.16.2/24.

Connecting to Web Admin Console

Browse to https://172.16.16.16 to access Cyberoam Web Console (GUI). Cyberoam login page is displayed and you are prompted to enter login credentials.

Use default username and password to log on.

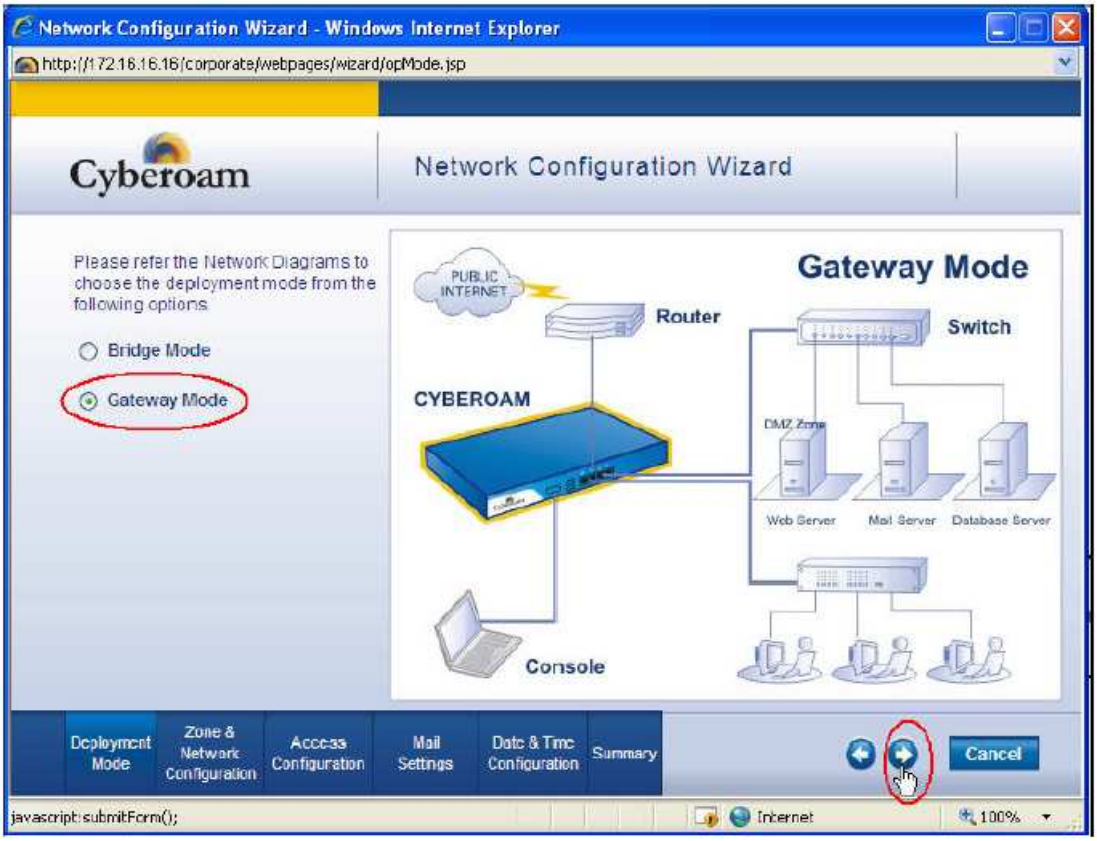
Default username: cyberoam
Password: cyber

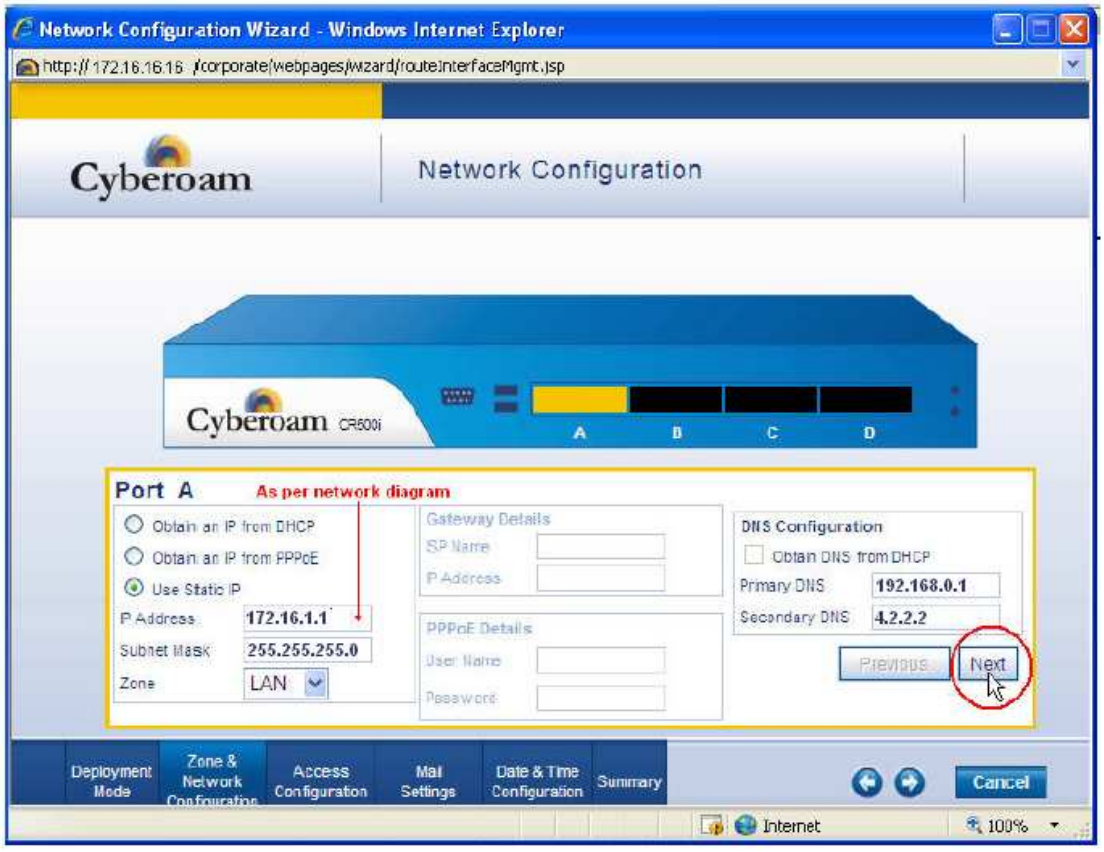
If you cannot log on, verify the following configurations:

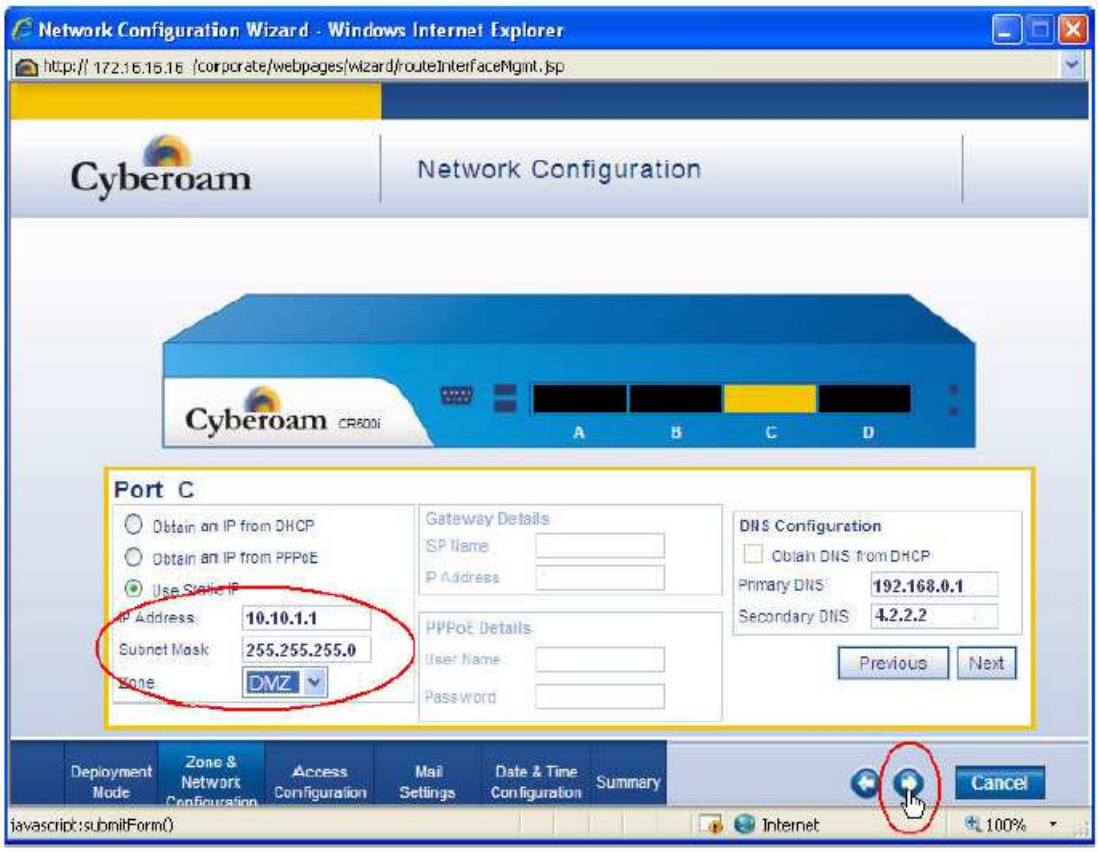
- Did you plug your computer Ethernet cable into the port A on the appliance? - Deployment can only be performed through port A.
- Is the link light glowing on both the computer and the Appliance? – If not, check and replace the cable
- Is your computer set to a static IP address of 172.16.16.16 and subnet as 255.255.255.0?
- Did you enter correct IP address in your Web browser?

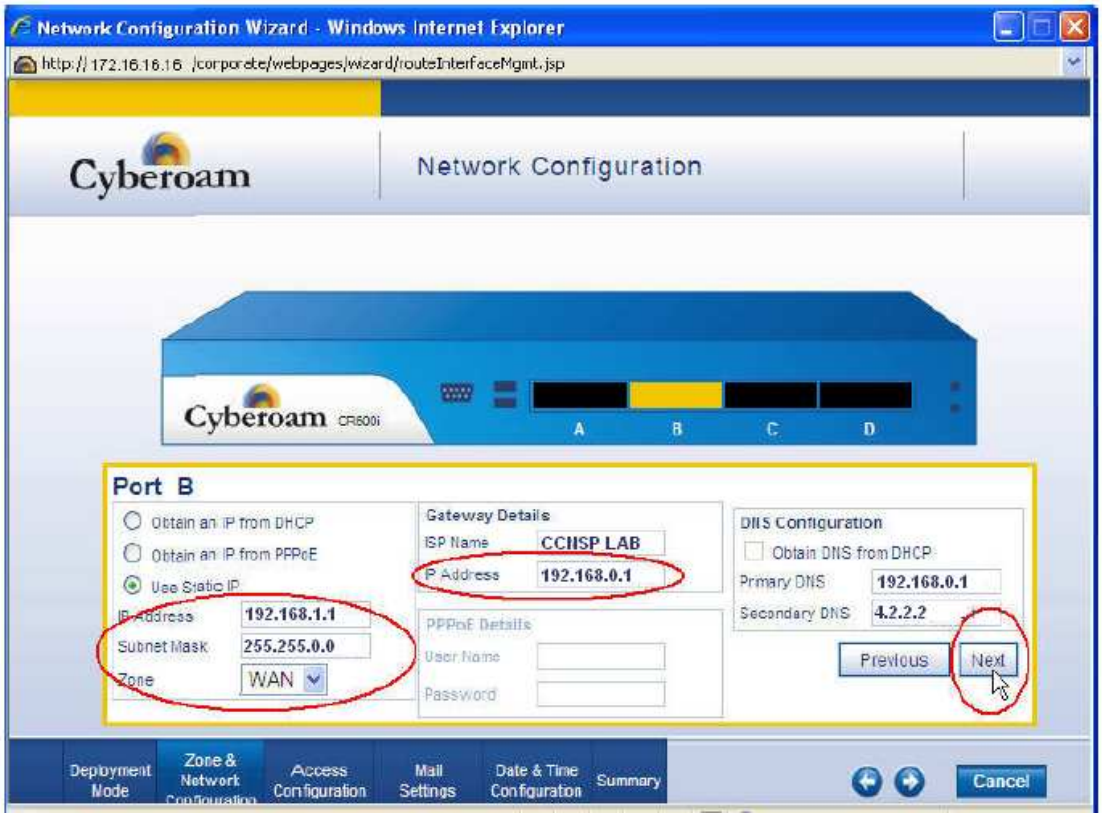
Lab #3 Deployment in Gateway Mode
Activity 3: Network Configuration Wizard

Click the Wizard button on the top right of the Dashboard to start Network Configuration Wizard and click Start.


Network Configuration Wizard - Windows Internet Explorer
http://172.16.16.16/corporate/webpages/wizard/opMode.jsp
Cyberoam
Network Configuration Wizard
Please refer the Network Diagrams to choose the deployment mode from the following options
Bridge Mode
Gateway Mode
Gateway Mode
PUBLIC INTERNET
Router
Switch
CYBEROAM
DMZ Zone
Web Server
Mail Server
Database Server
Console
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
javascript:submitForm();
Internet
100%


Network Configuration Wizard - Windows Internet Explorer
http://172.16.16.16/corporate/webpages/wizard/routeInterfaceMgmt.jsp
Cyberoam
Network Configuration
Cyberoam CR500i
A
B
C
D
Port A
As per network diagram
Obtain an IP from DHCP
Obtain an IP from PPPoE
Use Static IP
IP Address 172.16.1.1
Subnet Mask 255.255.255.0
Zone LAN
Gateway Details
ISP Name
IP Address
PPPoE Details
User Name
Password
DNS Configuration
Obtain DNS from DHCP
Primary DNS 192.168.0.1
Secondary DNS 4.2.2.2
Previous
Next
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
Internet
100%


Network Configuration Wizard - Windows Internet Explorer
http:// 172.16.16.16 /corporate/webpages/wizard/routeInterfaceMgmt.jsp
Cyberoam
Network Configuration
Cyberoam CR600i
A
B
C
D
Port C
Obtain an IP from DHCP
Obtain an IP from PPPoE
Use Static IP
IP Address 10.10.1.1
Subnet Mask 255.255.255.0
Zone DMZ
Gateway Details
ISP Name
IP Address
PPPoE Details
User Name
Password
DNS Configuration
Obtain DNS from DHCP
Primary DNS 192.168.0.1
Secondary DNS 4.2.2.2
Previous
Next
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
javascript:submitForm()
Internet
100%


Network Configuration Wizard - Windows Internet Explorer
http:// 172.16.16.16 /corporate/webpages/wizard/routeInterfaceMgmt.jsp
Cyberoam
Network Configuration
Cyberoam CR600i
A
B
C
D
Port B
Obtain an IP from DHCP
Obtain an IP from PPPoE
Use Static IP
IP Address 192.168.1.1
Subnet Mask 255.255.0.0
Zone WAN
Gateway Details
ISP Name CCNSP LAB
IP Address 192.168.0.1
PPPoE Details
User Name
Password
DNS Configuration
Obtain DNS from DHCP
Primary DNS 192.168.0.1
Secondary DNS 4.2.2.2
Previous
Next
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel

Lab #3 Deployment in Gateway Mode
Activity 4: Default Policy Configuration

As the Cyberoam is a firewall device, it will blocks all inter zone traffic. The wizard gives the option to select policy for LAN -> WAN traffic from three pre-defined policies.

Following are three pre-defined policies:

Monitor Only:

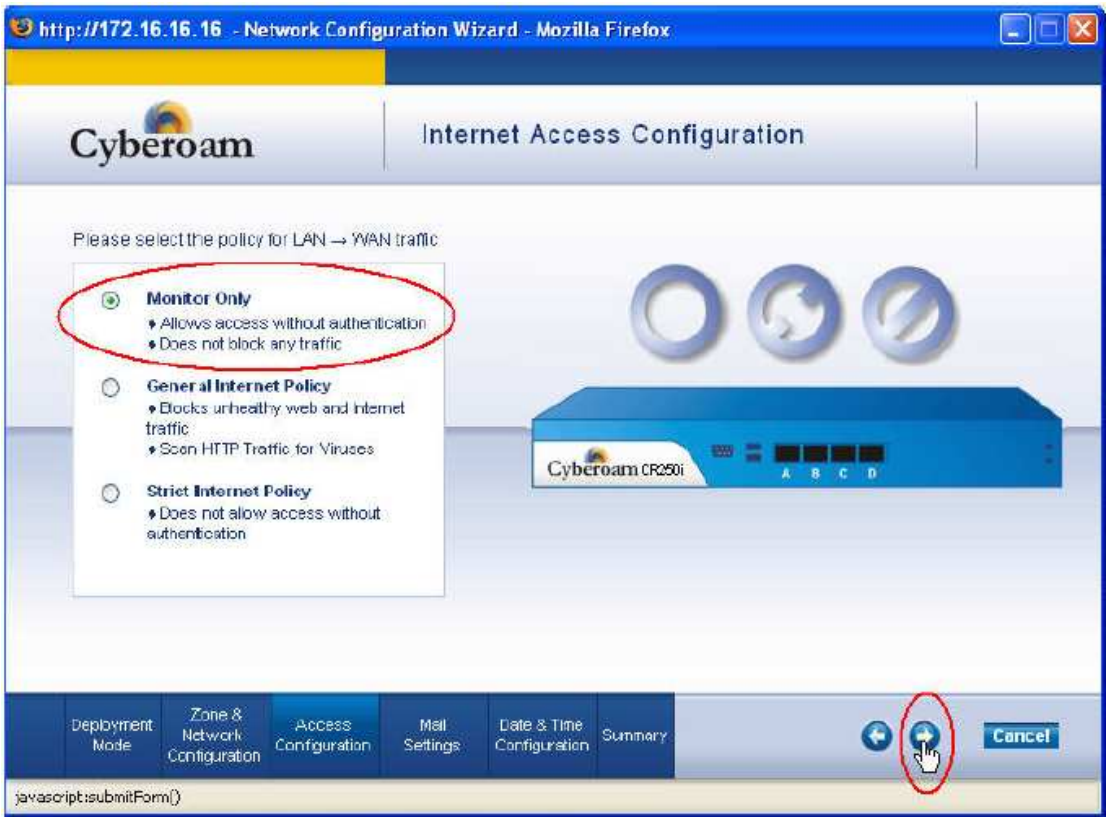
- Allow all outbound traffic without any authentication.
- No scanning.
- No content filtering.

General Internet Policy:

- Allow all outbound traffic without any authentication.
- Web traffic will be scanned for virus / malware / spyware.
- Content filtering will be “ON” by using default content filtering policy “General Corporate Policy” which blocks below web URL categories:
    - Porn, Nudity, Adult Content, URL Translation Sites, Drugs, Crime and Suicide, Gambling, Militancy and Extremist, Phishing and Fraud, Violence, Weapons

Strict Internet Policy:

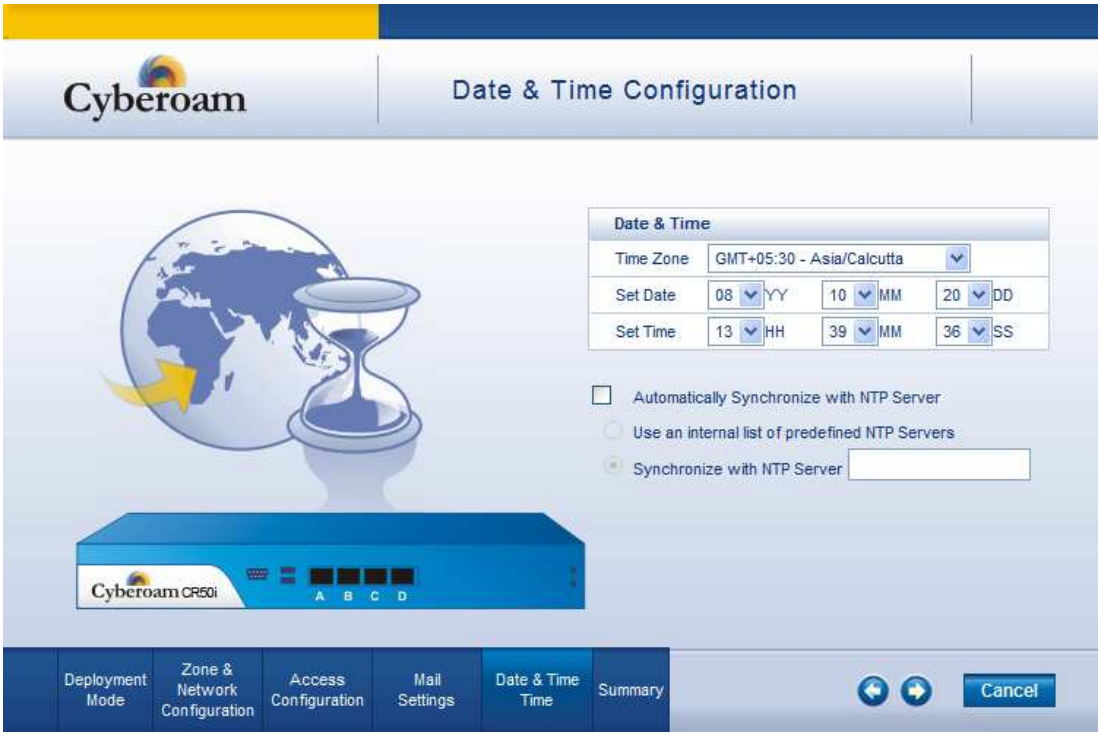
- Block all outbound unauthenticated traffic.
- Web traffic will be scanned for virus / malware / spyware.
- All traffic will be scanned by IPS engine.


http://172.16.16.16 - Network Configuration Wizard - Mozilla Firefox
Cyberoam
Internet Access Configuration
Please select the policy for LAN → WAN traffic
Monitor Only
• Allows access without authentication
• Does not block any traffic
General Internet Policy
• Blocks unhealthy web and internet traffic
• Scan HTTP Traffic for Viruses
Strict Internet Policy
• Does not allow access without authentication
Cyberoam CR250i
A B C D
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel
javascript:submitForm()

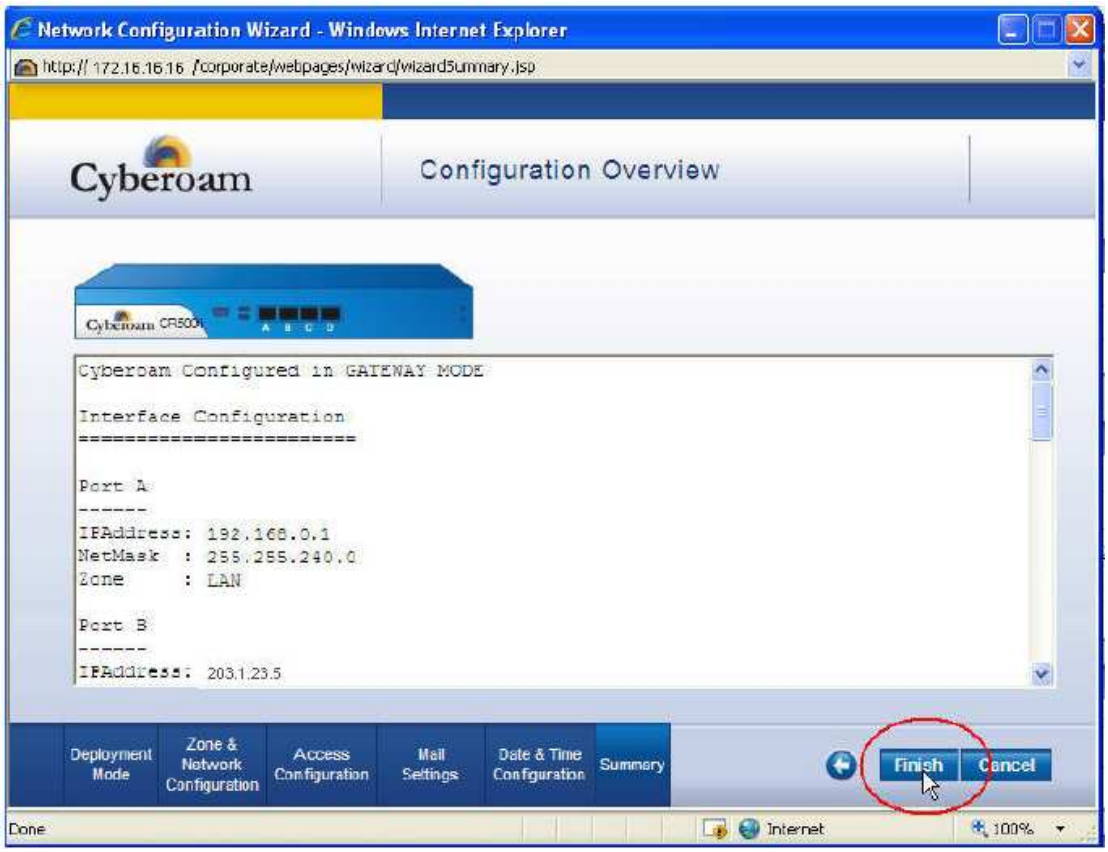
Lab #3 Deployment in Gateway Mode
Activity 5: Mail Settings

Configure mail server IP address, administrator email address from where the notification mails will be send and the email address of the notification recipient.

Lab #3 Deployment in Gateway Mode
Activity 6: Date & Time Configuration



Lab #3 Deployment in Gateway Mode
Activity 7: Completion of Wizard



The Cyberoam will take time to restart, please wait for some time before clicking to access the Web Admin Console.

Change your computer IP as per your student number. Replace x with your student number.

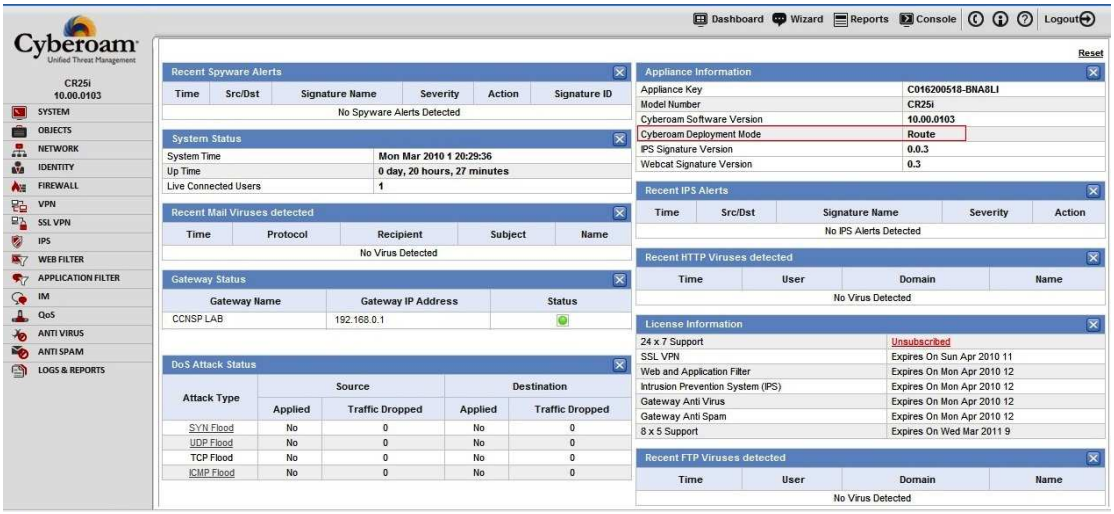
Computer IP: 172.16.1.x Subnet Mask: 255.255.255.0
Gateway: 172.16.1.1
DNS: 172.16.1.1

This completes the basic configuration of Cyberoam and now you are ready to use the Appliance.

Lab #3 Deployment in Gateway Mode
Activity 8: Verifying the configuration using Dashboard:

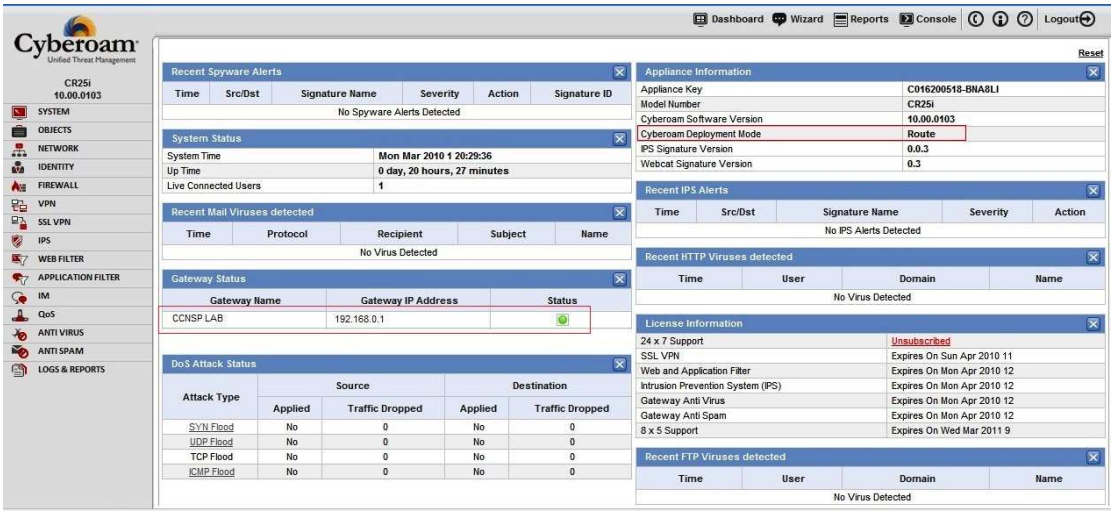
Browse to https:\\172.16.1.1 and log on to Web Admin Console using default username and password. Dashboard page is displayed on successful log on.

1. Verify appliance information
Check the Appliance Information section of Dashboard to verify configuration.



2. Verify gateway status

Check the Gateway Status of Dashboard and verify that the status of the gateway green i.e. UP.



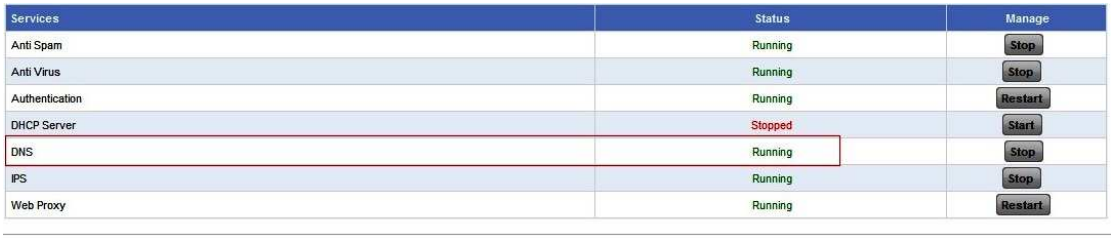
3. Verify IP assignments

Go to Network → Interface page and check IP address assigned to Interfaces.

If you have not configured IP scheme properly, you can run the Network Configuration wizard and change the IP address.

4. Verify DNS status

In GUI, go to System → Services, and verify the DNS service is running as below:



Services	Status	Manage
Anti Spam	Running	Stop
Anti Virus	Running	Stop
Authentication	Running	Restart
DHCP Server	Stopped	Start
DNS	Running	Stop
IPS	Running	Stop
Web Proxy	Running	Restart

Cyberoam Registration

Cyberoam	Unified Threat Management

Cyberoam Registration

Cyberoam Registration

What is registration?

Registration is process which will create customer account in Cyberoam central registration database.

Why to register?

Registration is mandatory task as without this subscription modules cannot be subscribed.

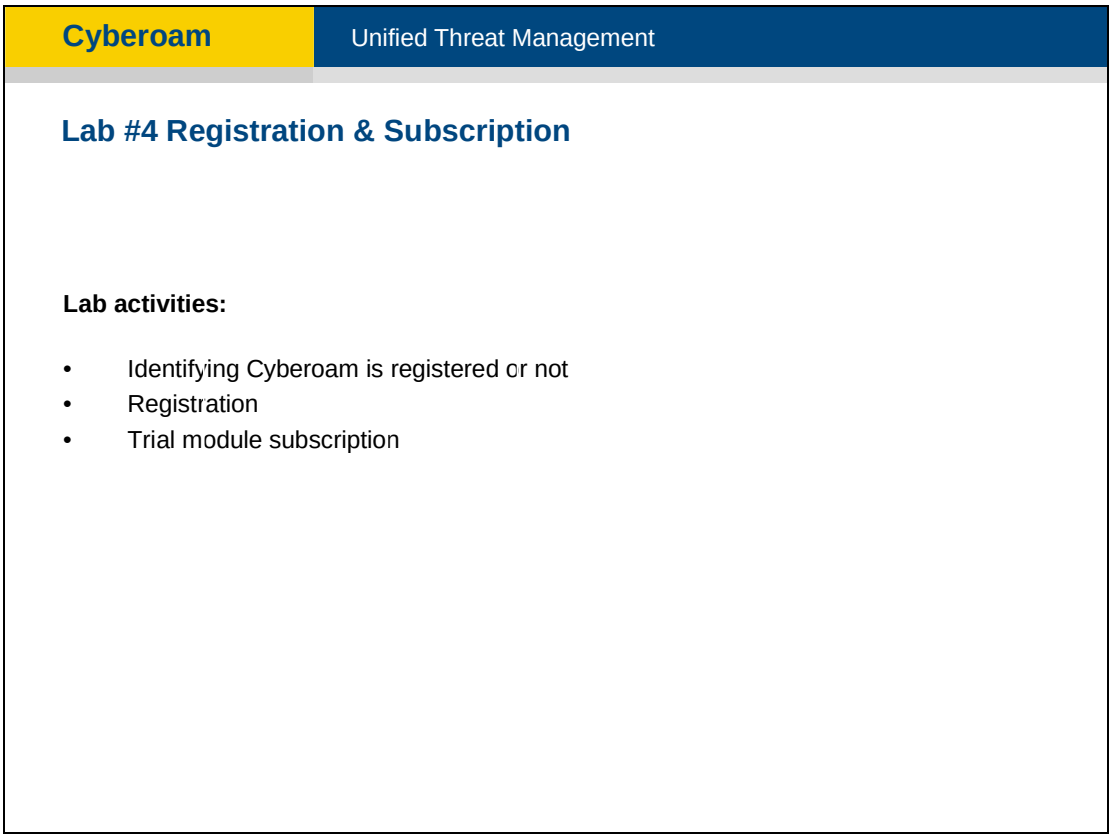
Registration gives following benefits:

- 8 x 5 Support as per country time zone for next one year.
- Free trial of following Cyberoam Subscription Modules:
    - Gateway Anti-Virus
    - Gateway Anti-Spam
    - Web & Application Filter
    - Intrusion Prevention System (IPS)
- Access of customer my account for
    - Support ticket management
    - Subscription management

Customer my account can be accessed from: http://customer.cyberoam.com

Multiple Cyberoam appliances can be registered using same customer account so that customer can manage all support tickets under one customer account.

Lab #4 Registration & Subscription



Lab #4 Registration & Subscription

Lab activities:

1. Identifying Cyberoam is registered or not
2. Registration
3. Trial module subscription

Lab #4 Registration & Subscription

Objective:

Register the Cyberoam appliance with a new customer account and subscribe to all four modules using trial license.

Lab #4 Registration & Subscription
Activity 1: Identifying Cyberoam is registered or not

The register icon will be visible in top bar / main page if Cyberoam appliance is not registered.

Click on this icon for the registration page to open up.

Lab #4 Registration & Subscription
Activity 2: Registration

Click on registration icon 

or go to Help -> Licensing to open the registration page

Fill up registration page with required information and click on “Register”

Note:

- Email-id will be used as a username to access customer my account.
- If you already have customer account with Cyberoam then you can click “If you already have a customer account click here” but in Lab create new customer account.
- If Cyberoam is not having direct internet connectivity and you are using web proxy then specify proxy information in “External Proxy Server Information”

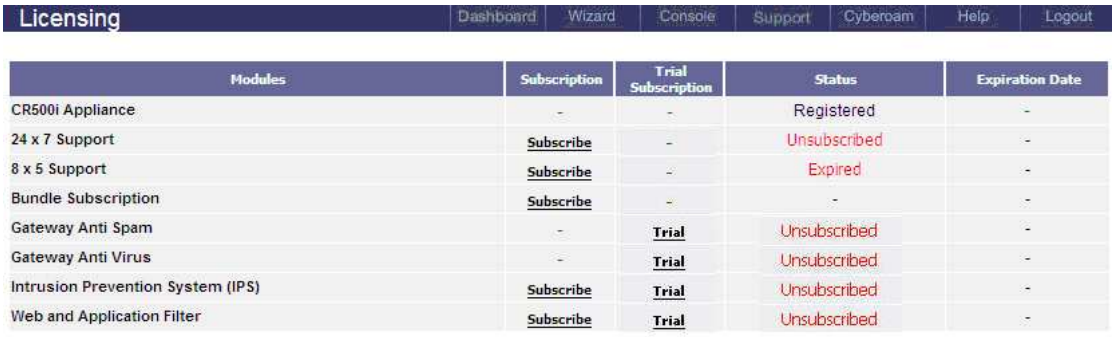
Once appliance get registered you can verify the registration from Help -> Licensing

Modules	Subscription	Trial Subscription	Status	Expiration Date
CR500i Appliance	-	-	Registered	-
24 x 7 Support	Subscribe	-	Unsubscribed	-
8 x 5 Support	Subscribe	-	Expired	-
Bundle Subscription	Subscribe	-	-	-
Gateway Anti Spam	-	-	Subscribed	-
Gateway Anti Virus	-	-	Subscribed	-
Intrusion Prevention System (IPS)	Subscribe	Trial	Unsubscribed	-
Web and Application Filter	Subscribe	Trial	Unsubscribed	-

Lab #4 Registration & Subscription
Activity 3: Trial module subscription

To subscribe trial module after registration, go to Help -> Licensing

Click on trial button under Trial Subscription and provide email-id and password used during Cyberoam registration.



Modules	Subscription	Trial Subscription	Status	Expiration Date
CR500i Appliance	-	-	Registered	-
24 x 7 Support	Subscribe	-	Unsubscribed	-
8 x 5 Support	Subscribe	-	Expired	-
Bundle Subscription	Subscribe	-	-	-
Gateway Anti Spam	-	Trial	Unsubscribed	-
Gateway Anti Virus	-	Trial	Unsubscribed	-
Intrusion Prevention System (IPS)	Subscribe	Trial	Unsubscribed	-
Web and Application Filter	Subscribe	Trial	Unsubscribed	-

Module 5: Firewall

Agenda

- Access Control (Local ACL)
- IP Management
- Firewall Management
- Default Firewall Rules
- L2 Firewall support
- Outbound NAT (Source NAT)
- Inbound NAT (Virtual Host)
- Denial of Service (DoS)
- Cyberoam Unified Threat Control under Firewall

Access Control (Appliance Access)

Use Appliance Access to limit the Administrative access to the following Cyberoam services from LAN/WAN/DMZ:

- Admin Services
- Authentication Services
- Proxy Services
- Network Services

Default Access Control configuration

When Cyberoam is connected and powered up for the first time, it will have a default Access configuration as specified below:

Admin Services
HTTPS (TCP port 443) and SSH (TCP port 22) services will be open for administrative functions for LAN zone

Authentication Services
Cyberoam (UDP port 6060) and HTTP Authentication (TCP port 8090) will be open for User Authentication Services for LAN zone. User Authentication Services are not required for any of the Administrative functions but required to apply user based internet surfing, bandwidth and data transfer restrictions.

Customise Access Control configuration

Use access control to limit the access to Cyberoam for administrative purposes from the specific authenticated/trusted networks only. You can also limit access to administrative services within the specific authenticated/trusted network.

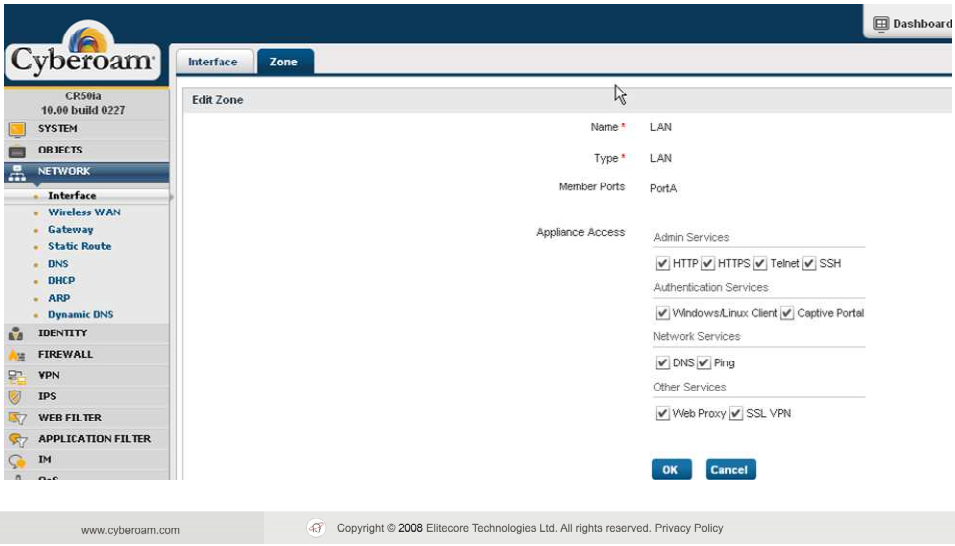
In GUI, go to System → Administration → Appliance Access Tab

Alternatively, one can control appliance access via Zone configuration page.
In GUI, navigate to Network→Interface→Zone

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Appliance Access (via Zones)

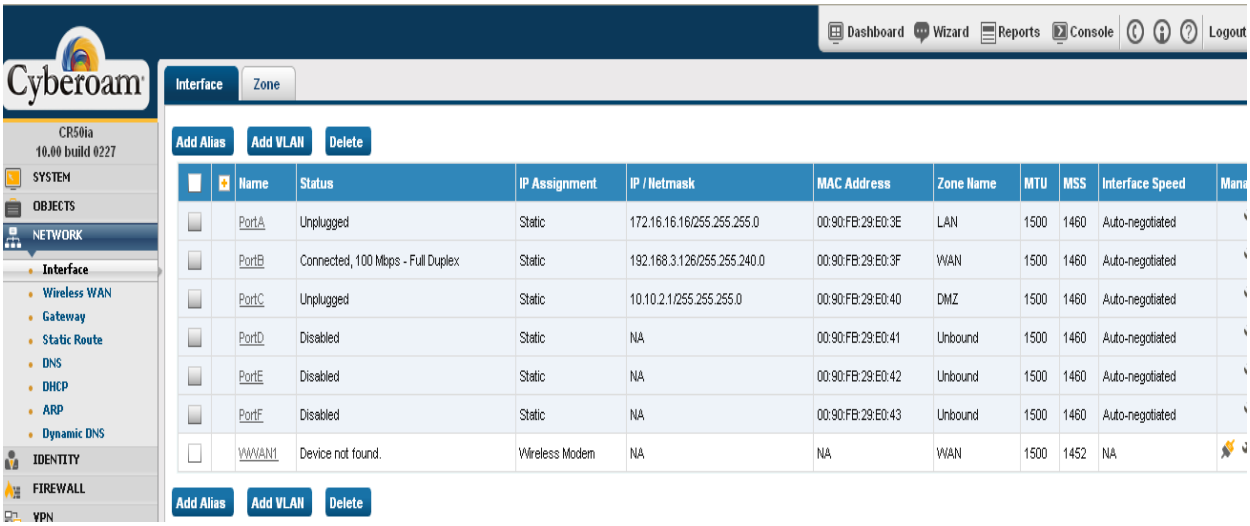
Network → Interface → Zone



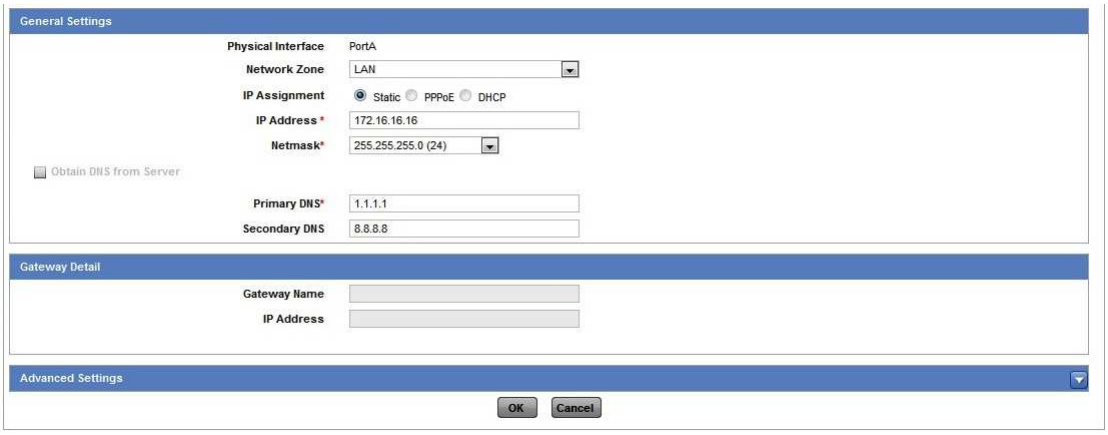
IP management

Select **Network → Interface** to view port wise network (physical interface) and zone details. If virtual sub-interfaces are configured for VLAN implementation, they are also nested and displayed beneath the physical interface.

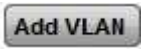
Interface - Physical interfaces/ports available on Cyberoam. If virtual sub-interface is configured for the physical interface, it also displayed beneath the physical interface. Virtual sub-interface configuration can be updated or deleted.

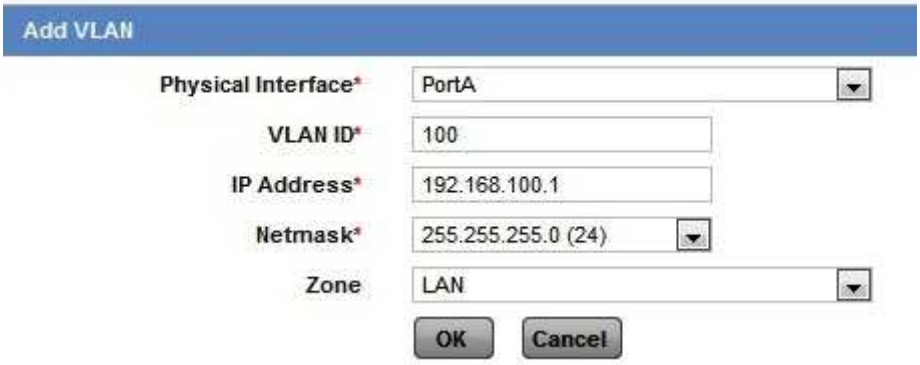


Click  to edit IP address and netmask of physical or virtual interfaces



Click  to specify alias IP address for the interface

Click  to add VLAN interface



Firewall Management

Zone Management

Default Zones Types

(1) LAN – Depending on the appliance in use and on your network design, Cyberoam allows to group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone. By default the traffic to and from this zone is blocked and hence the highest secured zone. However, Cyberoam allows traffic between the ports belonging to the same zone.

(2) DMZ (De-Militarised Zone) - This zone is normally used for publicly accessible servers. Depending on the appliance in use and on your network design, Cyberoam allows to group one to five physical ports in this zone.

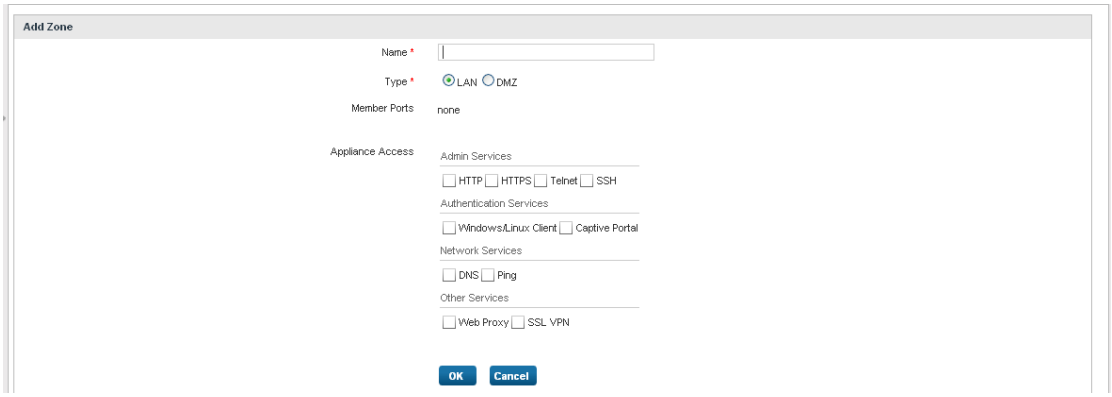
(3) WAN – Zone used for Internet services. It can also be referred as Internet zone.

(4) VPN - This zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical port/interface. Whenever the VPN connection is established, port/interface used by the connection is automatically added to this zone and on disconnection; port is automatically removed from the zone.

(5) Local - Entire set of physical ports available on the Cyberoam appliance including their configured aliases are grouped in LOCAL zone. In other words, IP addresses assigned to all the ports fall under the LOCAL zone.

Create Zone

Select **Network → Interface → Zone → Add** to open the create page



Service Management

Services represent types of Internet data transmitted via particular protocols or applications.

Protect your network by configuring firewall rules to

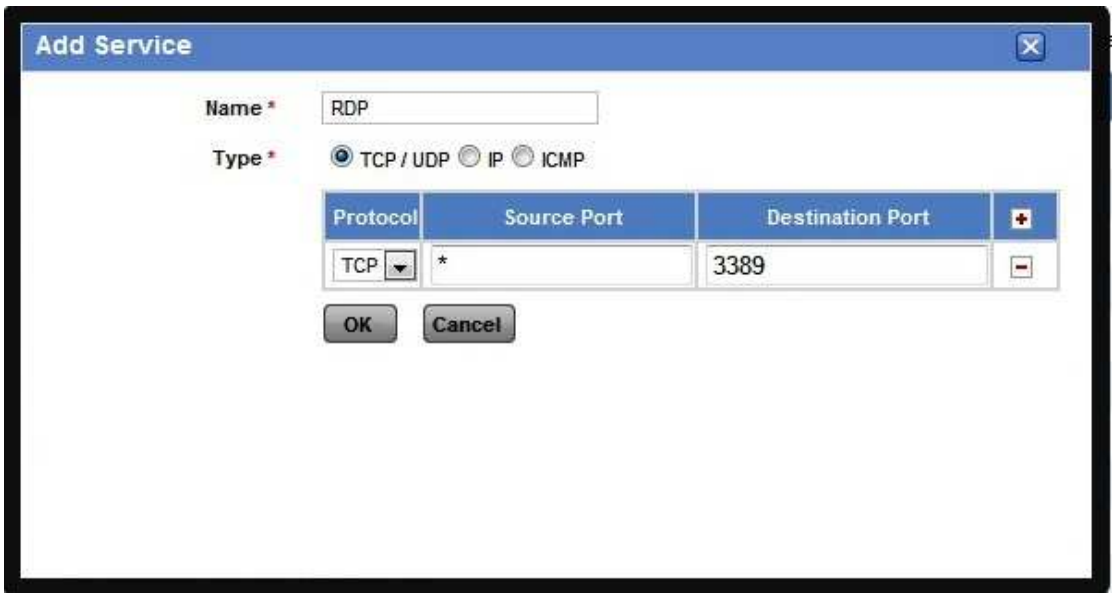
- block services for specific zone
- limit some or all users from accessing certain services
- allow only specific user to communicate using specific service

Cyberoam provides several standard services and allows creating:

- Customised service definitions
- Firewall rule for Customised service definitions

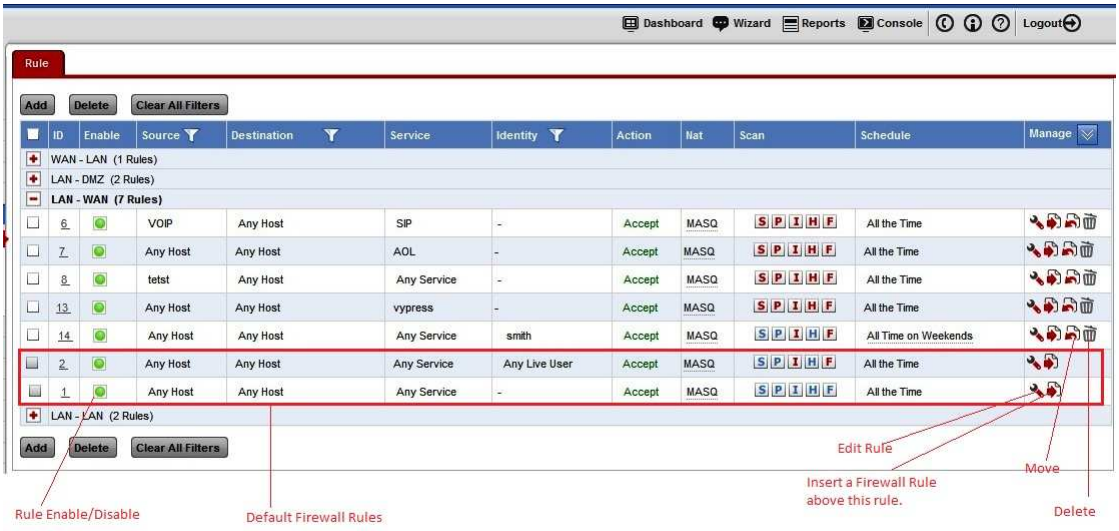
Define Custom Service

Select **Objects → Services → Add** to open the create page



Rule Management

Select **Firewall→Rule** to display the list of rules



Manage – Click to customise the number of columns to be displayed on the page

Subscription icon - Indicates subscription module. To implement the functionality of the subscription module you need to subscribe the respective module. Click to open the licensing page.

Enable/Disable rule icon - Click to activate/deactivate the rule. If you do not want to apply the firewall rule temporarily, disable rule instead of deleting.

- Green – Active Rule
- Red – De-active Rule

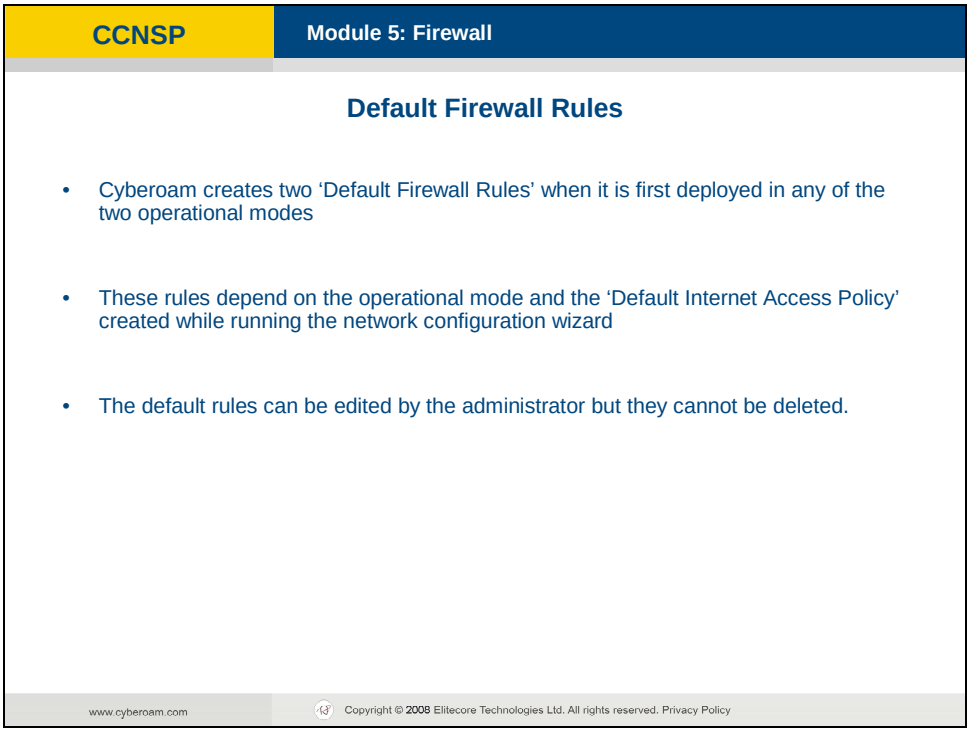
Edit icon - Click to edit the rule.

Insert icon - Click to insert a new rule before the existing rule.

Move icon - Click to change the order of the selected rule.

Delete Icon - Click to delete the rule. Refer to Delete Firewall Rule for more details.

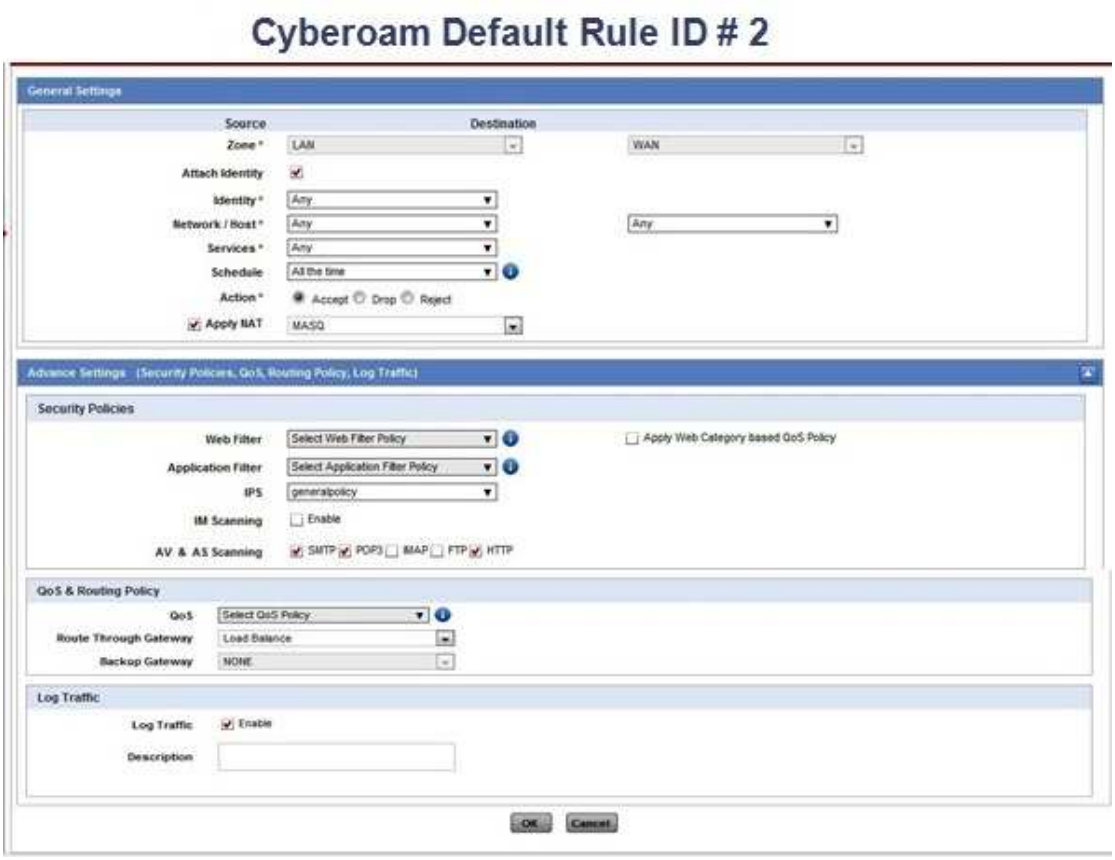
Default Firewall Rules



At the time of deployment, Cyberoam allows to define one of the following Internet Access policies using Network Configuration Wizard:

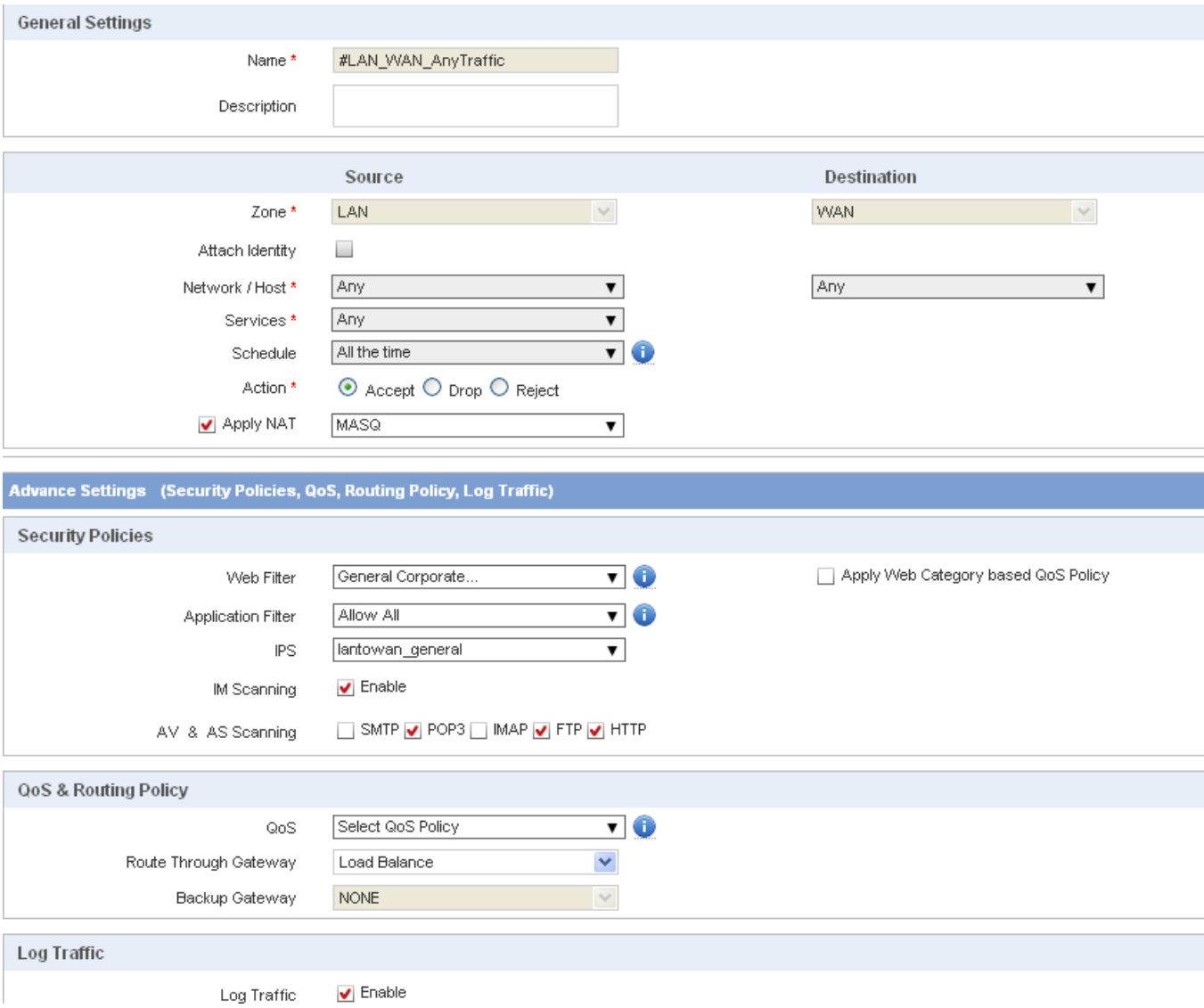
- Monitor only
- General Internet policy
- Strict Internet policy

Default firewall rules for "Monitor only" IAP



Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:

- Web Filter – User specific
- Application Filter – User specific
- QoS Policy – User specific
- Anti Virus & Anti Spam policy – Allows SMTP, POP3, IMAP and HTTP traffic without scanning



Masquerade and allow entire LAN to WAN traffic for all the users without scanning SMTP, POP3, IMAP and HTTP traffic

Default firewall rules for "General Internet policy"

1. Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:
    - Web Filter & Application Filter – User specific
    - QoS policy – User specific
    - Anti Virus & Anti Spam policy - Scan SMTP, POP3, IMAP and HTTP traffic

2. Masquerade and Allow entire LAN to WAN traffic for all the users after applying following policies:
    - **Web Filter** – Applies 'General Corporate Policy' to block Porn, Nudity, AdultContent, URL TranslationSites, Drugs, CrimeandSuicide, Gambling, MilitancyandExtremist, PhishingandFraud, Violence, Weapons categories
    - **IPS Policy** – General policy
    - **Anti Virus & Anti Spam policy** - Scan SMTP, POP3, IMAP and HTTP traffic

Default firewall rules for "Strict Internet policy" IAP

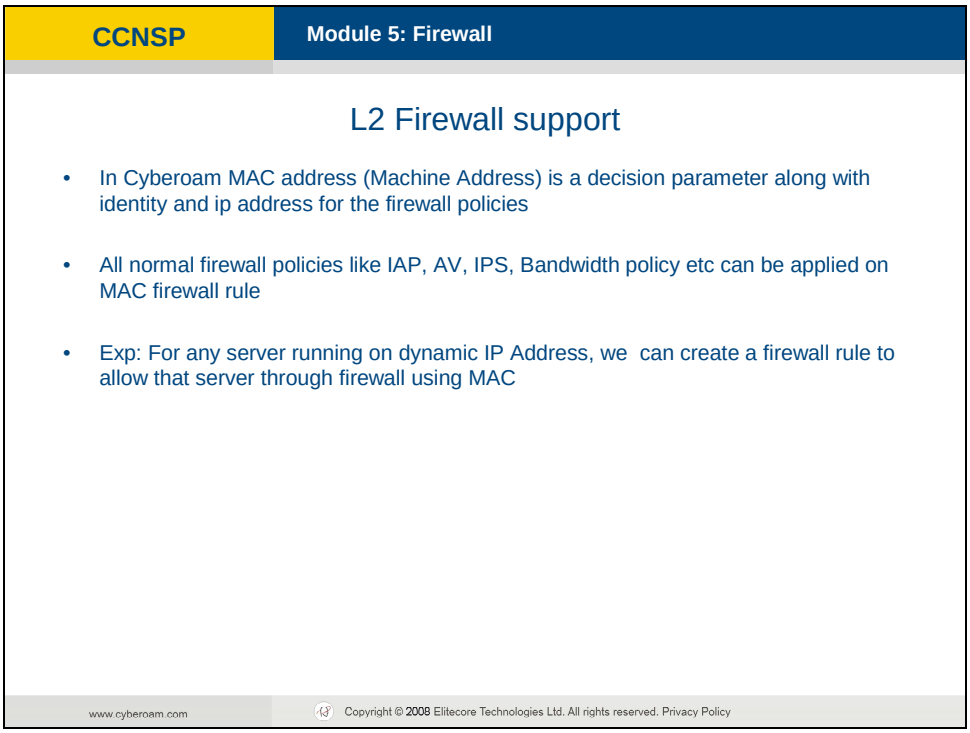
1. Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:
    - Web Filter & Application Filter – User specific
    - QoS policy – User specific
    - IPS policy – General policy
    - Anti Virus & Anti Spam policy - Scan SMTP, POP3, IMAP and HTTP traffic

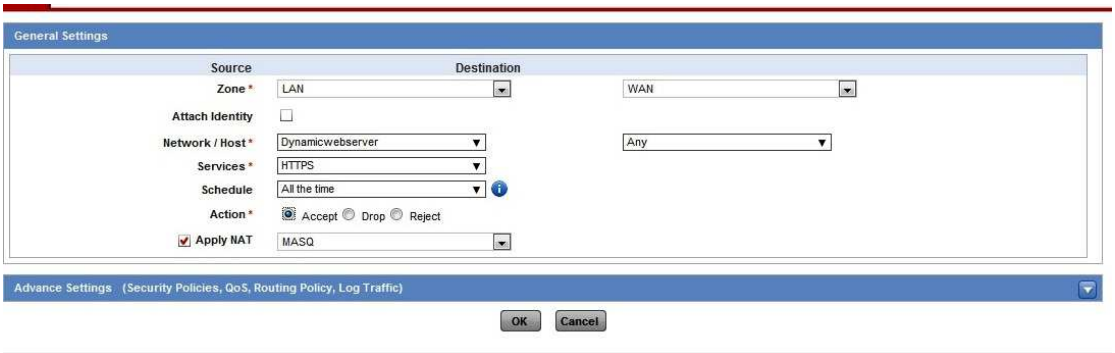
2. Drop entire LAN to WAN traffic for all the users

Note

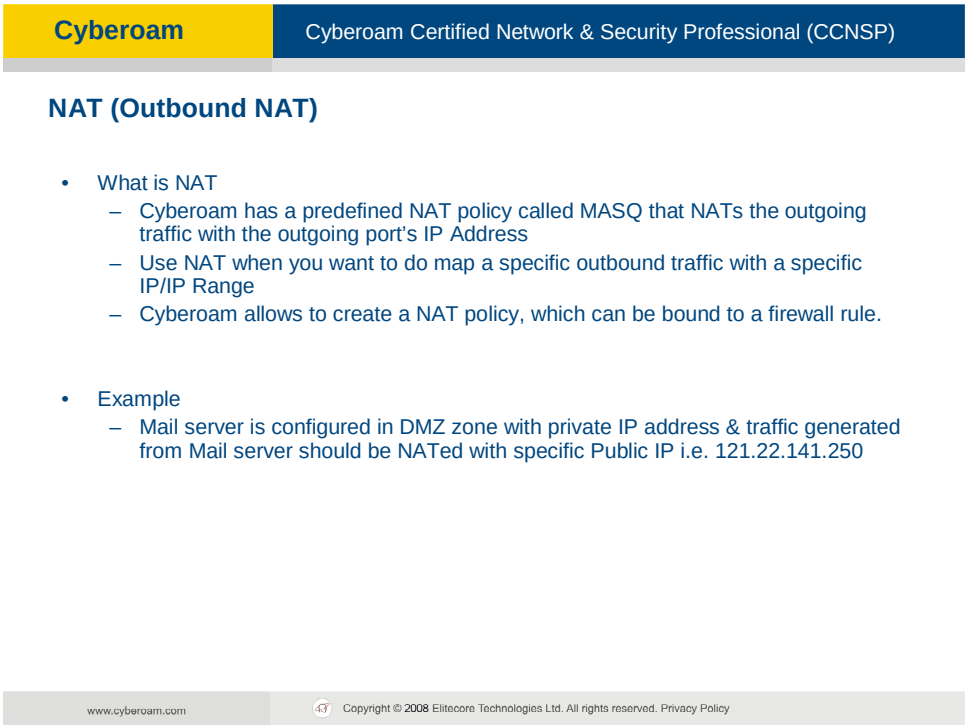
- Default Firewall rules can be modified as per the requirement but cannot be deleted
- IPS policy will not be effective until the Intrusion Prevention System (IPS) module is subscribed.
- Virus and Spam policy will not be effective until the Gateway Anti Virus and Gateway Anti-spam modules are subscribed respectively.
- If Internet Access Policy is not set through Network Configuration Wizard at the time of deployment, the entire traffic is dropped.

L2 Firewall Support:





NAT (Outbound NAT)



NAT Policy

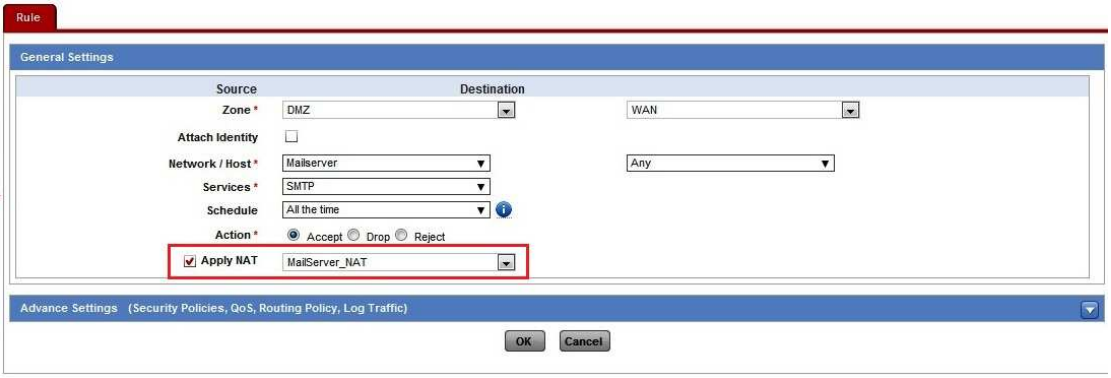
NAT policy tells firewall rule to allow access but after changing source IP address i.e. source IP address is substituted by the IP address specified in the NAT policy

Create NAT policy

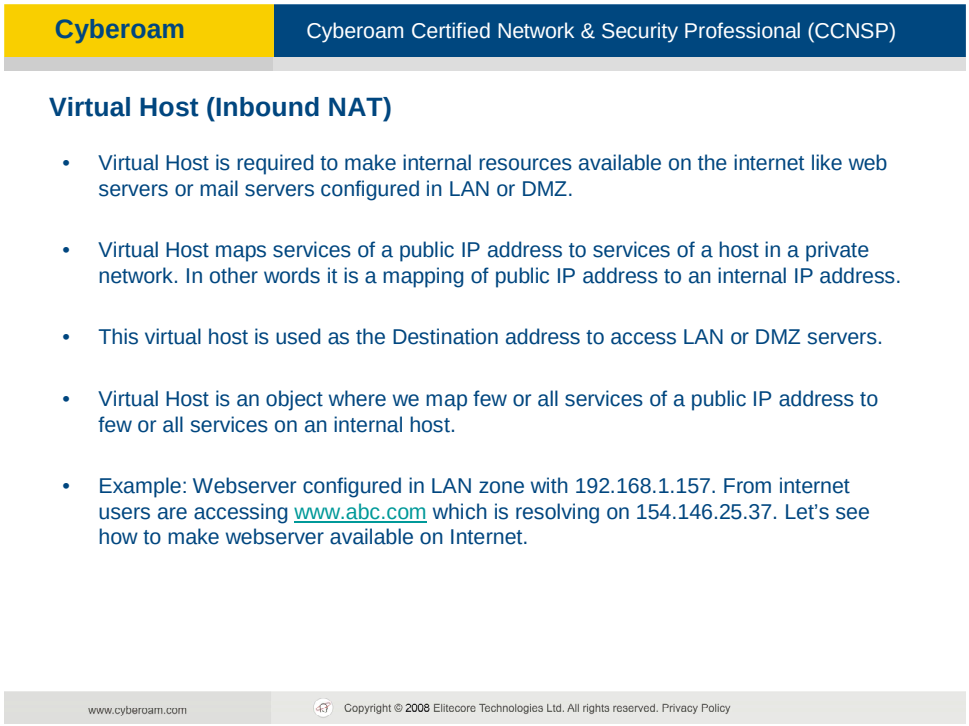
Select **Firewall** → **NAT policy** → **Add** to open the create page

Create a Firewall rule to include the NAT policy

Select **Firewall** → **Rule** → **Add** to open the create page



Virtual Host (Inbound NAT)

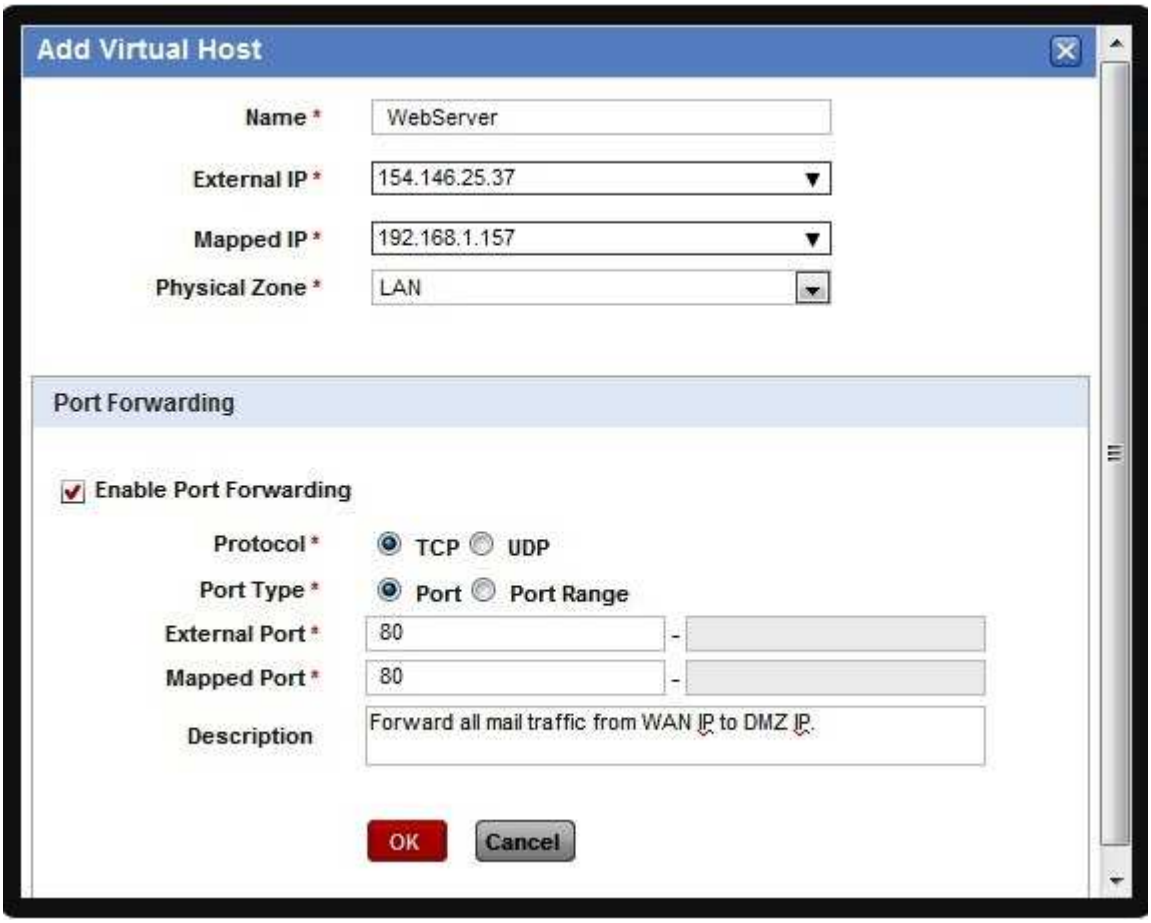


Virtual Host maps services of a public IP address to services of a host in a private network. A Virtual host can be a single IP address or an IP address range or Cyberoam interface itself.

Cyberoam will automatically respond to the ARP request received on the WAN zone for the external IP address of Virtual host. Default LAN to WAN (Any Host to Any Host) firewall rule will allow traffic to flow between the virtual host and the network.

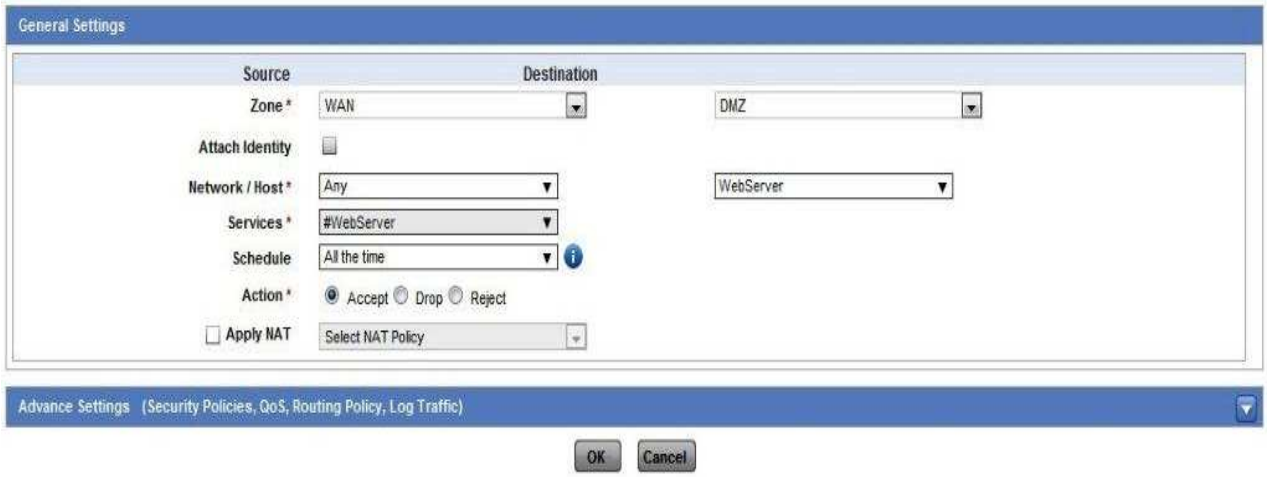
Create Virtual host

Select **Firewall → Virtual Host → Add**



Create Firewall rule to include the Virtual Host

Select **Firewall→ Rule → Add**



Create firewall rules to allow external host (from the Internet) to access a virtual host that maps to internal servers. You must add the virtual host to a firewall policy to actually implement the mapping configured in the virtual host i.e. create firewall rule that allows or denies inbound traffic to virtual host.

Loopback firewall rule

	ID	Enable	Source	Destination	Service	Identity	Action	Nat	Scan	Schedule	Manage
	DMZ - DMZ (1 Rules)										
	9		Any Host	MailServer	#MailServer	-	Accept	MASQ	S P I H F	All the Time	

Once the virtual host is created successfully, Cyberoam automatically creates a loopback firewall rule for the zone of the mapped IP address. Loopback firewall rule is created for the service specified in virtual host. If port forwarding is not enabled in virtual host then firewall rule with “All Services” is created.

Loopback rules allow internal users to access the internal resources using its public IP (external IP) or FQDN.

Port Forwarding Concept

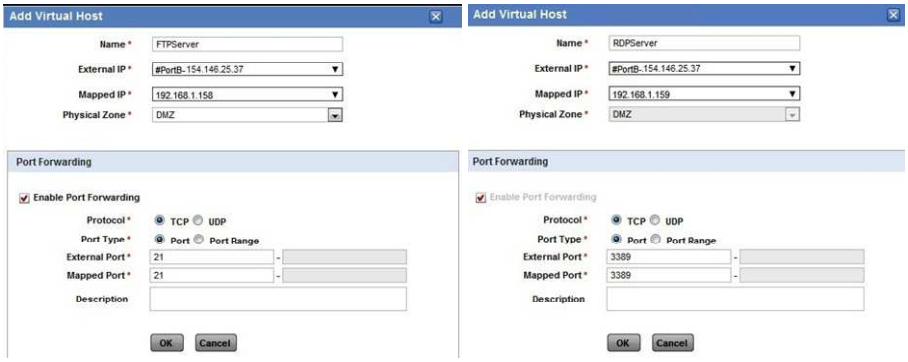
Example: We have one public IP 154.146.25.37. In the DMZ, we have connected multiple servers like Web Server (192.168.1.157), FTP Server (192.168.1.158) and RDP Server (192.168.1.159). We want to publish all these servers using only one public IP 154.146.25.37.

In this case, we will use Port Forwarding while configuring the Virtual Host.

We will have to create 3 Virtual Hosts for above 3 servers with same external IP and different Internal IP addresses, with port forwarding.

We have already created a Virtual Host for the Web Server with port 80, now we will create remaining two Virtual Hosts for FTP and RDP.

Creation of Virtual Hosts

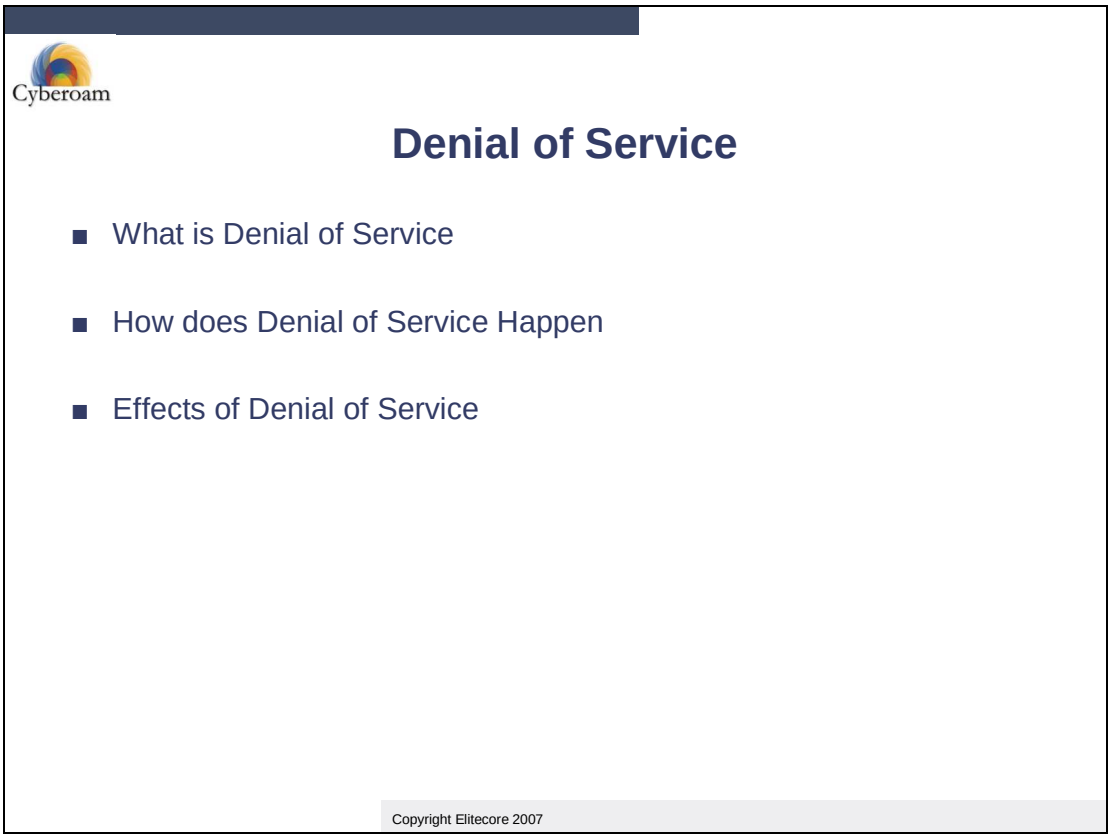


	Name	Public Address	Mapped Address	Public Port	Mapped Port	Manage
	FTPServer	154.146.25.37	192.168.1.158	21(TCP)	21(TCP)	
	RDPServer	154.146.25.37	192.168.1.159	3389(TCP)	3389(TCP)	
	WebServer	154.146.25.37	192.168.1.157	80(TCP)	80(TCP)	

Creation of Firewall Rules

	ID	Enable	Source	Destination	Service	Identity	Action	IM Scanning	Manage
	VPN - VPN (2 Rules)								
	VPN - DMZ (2 Rules)								
	VPN - WAN (2 Rules)								
	VPN - LAN (4 Rules)								
	DMZ - VPN (2 Rules)								
	DMZ - DMZ (3 Rules)								
	WAN - VPN (2 Rules)								
	WAN - DMZ (3 Rules)								
	25		Any Host	WebServer	#WebServer	-	Accept		
	27		Any Host	RDPServer	#RDPServer	-	Accept		
	26		Any Host	FTPServer	#FTPServer	-	Accept		

Denial of Service (DoS)



A "denial-of-service" attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- flooding a network, thereby preventing legitimate network traffic;
- disrupting a server by sending more requests than it can possibly handle, thereby preventing access to a service;
- preventing a particular individual from accessing a service;
- disrupting service to a specific system or person

Types of DoS Attacks

- **SYN flood** attack creates so many half-open connections that the system becomes overwhelmed and cannot handle incoming requests any more.

- **UDP Flood**: This attack links two systems. It hooks up one system's UDP character-generating service, with another system's UDP echo service. Once the link is made, the two systems are tied up exchanging a flood of meaningless data.

- **TCP flood:** This attack sends huge amount of TCP packets than the host/victim computer can handle.

- **ICMP flood** is based on sending the victim an overwhelming number of ping packets. It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

DoS protection settings

- How many connections is each LAN host generating (take an average)?

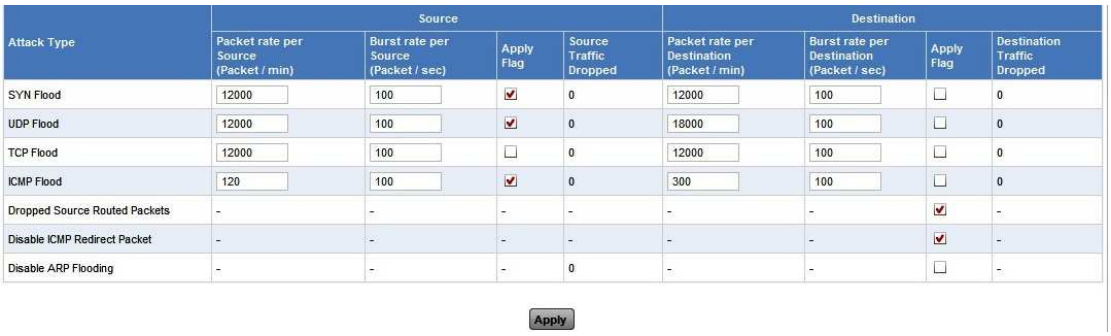
- Multiply that by the number of hosts in your network.

- Destination based checking of DOS attacks should be disabled unless you suspect that there is a host inside your network generating a DOS attack.

- Turn off checking for TCP flood unless specifically instructed by the Cyberoam Support Staff

DoS Configuration

Select Firewall→DoS → Settings tab



Attack Type	Source				Destination			
	Packet rate per Source (Packet / min)	Burst rate per Source (Packet / sec)	Apply Flag	Source Traffic Dropped	Packet rate per Destination (Packet / min)	Burst rate per Destination (Packet / sec)	Apply Flag	Destination Traffic Dropped
SYN Flood	12000	100	☑	0	12000	100	☐	0
UDP Flood	12000	100	☑	0	18000	100	☐	0
TCP Flood	12000	100	☐	0	12000	100	☐	0
ICMP Flood	120	100	☑	0	300	100	☐	0
Dropped Source Routed Packets	-	-	-	-	-	-	☑	-
Disable ICMP Redirect Packet	-	-	-	-	-	-	☑	-
Disable ARP Flooding	-	-	-	0	-	-	☐	-

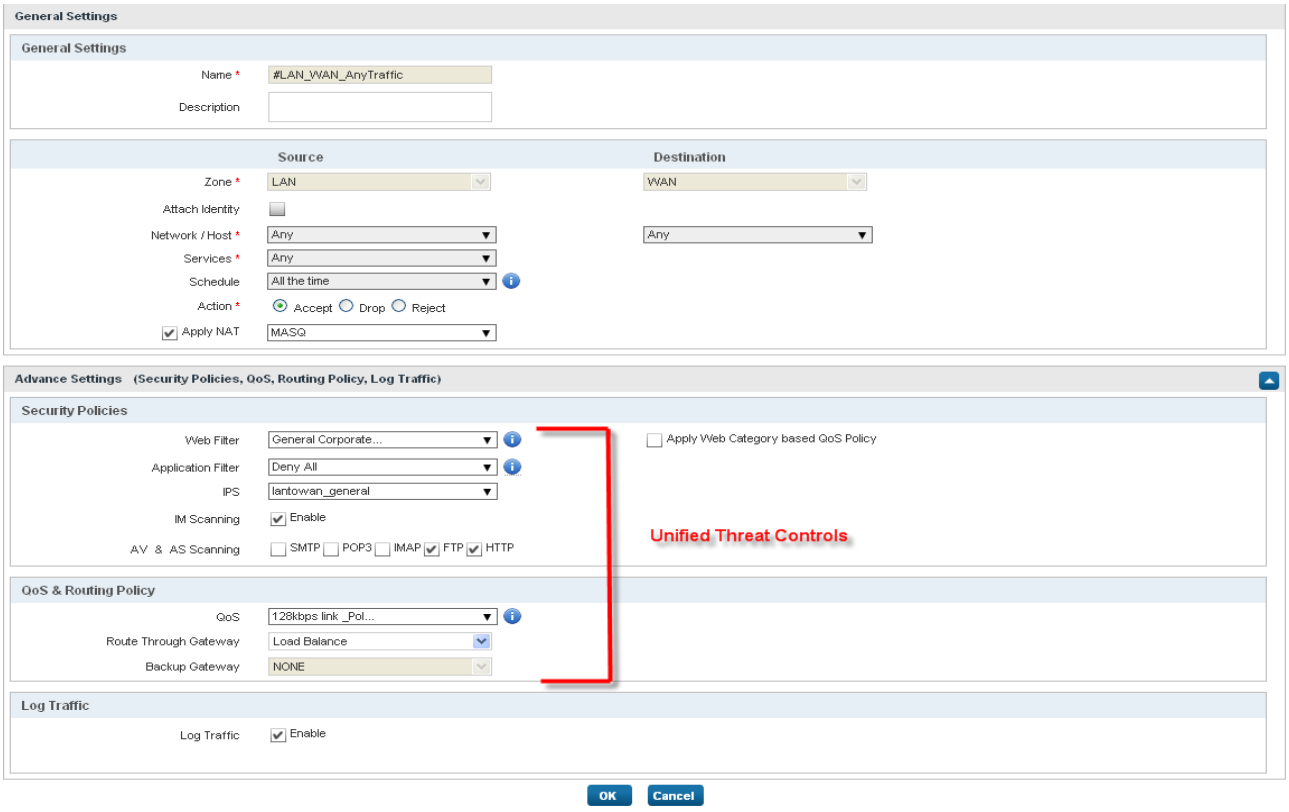
Apply

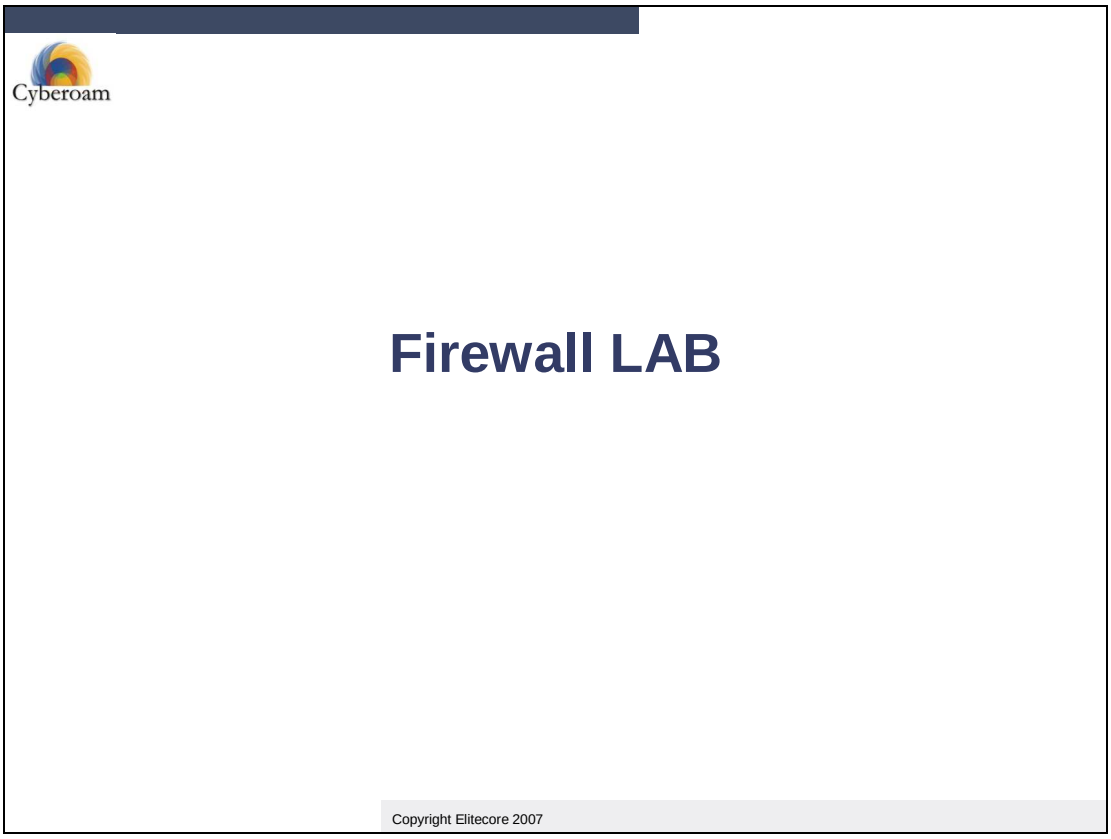
When traffic from a specific source or to a specific destination exceeds the burst rate value, it is considered as an attack by Cyberoam. It provides DoS attack protection by dropping all the excess packets from the particular source/destination. Cyberoam will continue to drop the packets till the attack subsides. Because Cyberoam applies threshold value per IP address, only traffic from the particular source/destination will be dropped while the rest of the network traffic will pass through unaffected.

Cyberoam Unified Firewall Controls

Cyberoam's unified firewall control provides with a single page configuration. One can attach all the policies including IPS, Internet access policy, Bandwidth policy, AV/AS scanning and routing policy from a single firewall page.

Select Firewall→Manage Firewall




Cyberoam
Firewall LAB
Copyright Elitecore 2007

Lab #5 Securing the Appliance

a) Navigate to System → Administration → Appliance Access and disable Ping both from the LAN and WAN Zones. Observe the behaviour by pinging the appliance now enable ICMP on the LAN Zone.

Zone	Admin Services				Authentication Services		Network Services		Other Services	
	HTTP	HTTPS	Telnet	SSH	Windows/Linux Client	Captive Portal	DNS	Ping	Web Proxy	SSL VPN
DMZ	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
VPN	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐
LAN	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑
WAN	☑	☑	☑	☑	☐	☐	☐	☑	☐	☑

Apply

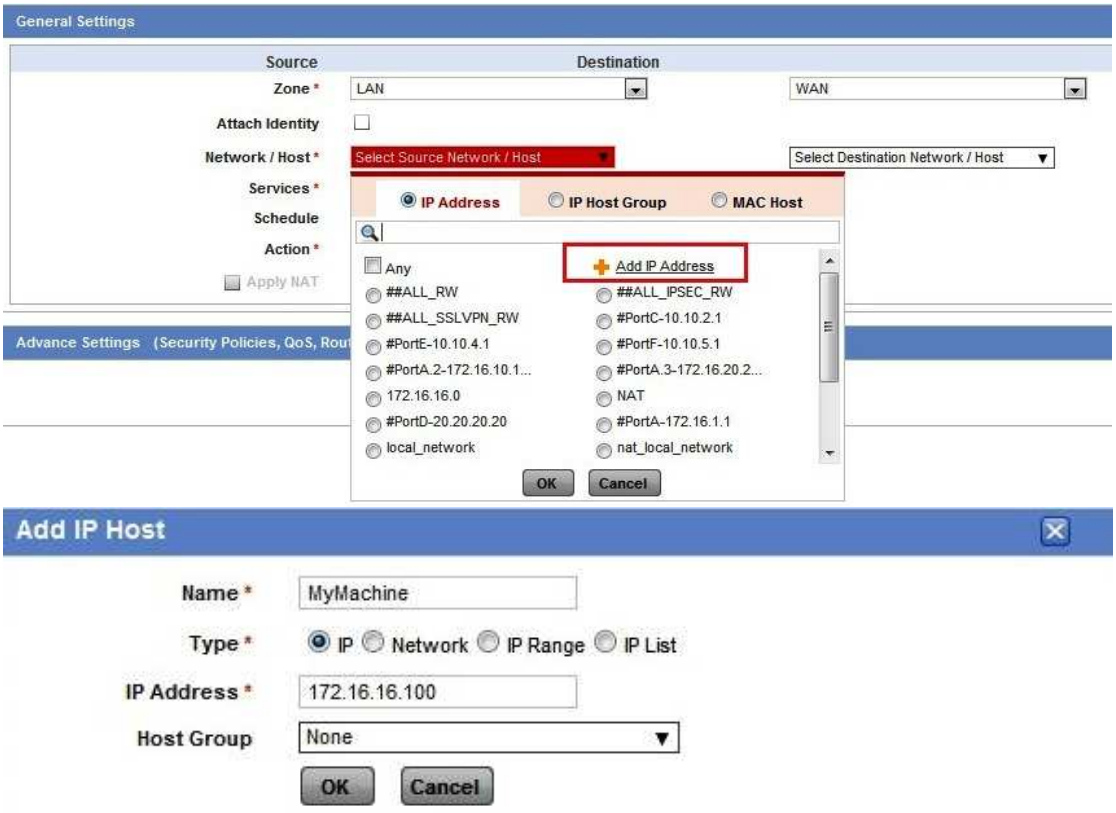
b) Using the Appliance Access page stop unencrypted access to Cyberoam administration service, i.e disable Telnet & HTTP access.

Zone	Admin Services				Authentication Services		Network Services		Other Services	
	HTTP	HTTPS	Telnet	SSH	Windows/Linux Client	Captive Portal	DNS	Ping	Web Proxy	SSL VPN
DMZ	☐	☑	☐	☑	☑	☑	☑	☑	☑	☑
VPN	☐	☑	☐	☑	☑	☑	☑	☑	☑	☐
LAN	☐	☑	☐	☑	☑	☑	☑	☑	☑	☑
WAN	☐	☑	☐	☑	☐	☐	☐	☑	☐	☑

Apply

Lab #6 Create a DROP firewall rule for your machine's IP address.

- Navigate to Firewall→ Rule → Add. Add a host for the Source Zone. The IP address will be that of user's machine, 172.16.16.100 in the example below.

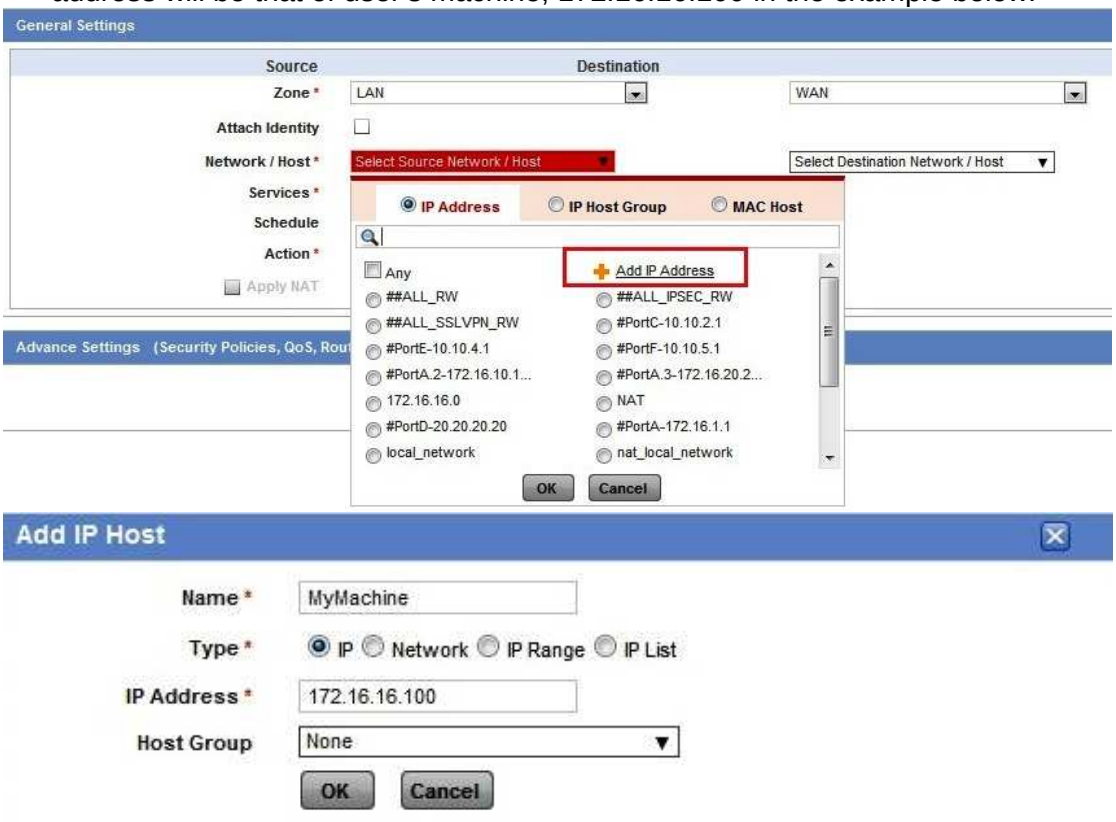


- Set the Firewall action to DROP and create the rule

- Make sure the above created rule is above all the generic rules. Verify by accessing internet from your machine.

Lab #7 Create a ACCEPT firewall rule for your machine's IP address.

- Navigate to Firewall→ Rule → Add. Add a host for the Source Zone. The IP address will be that of user's machine, 172.16.16.100 in the example below.

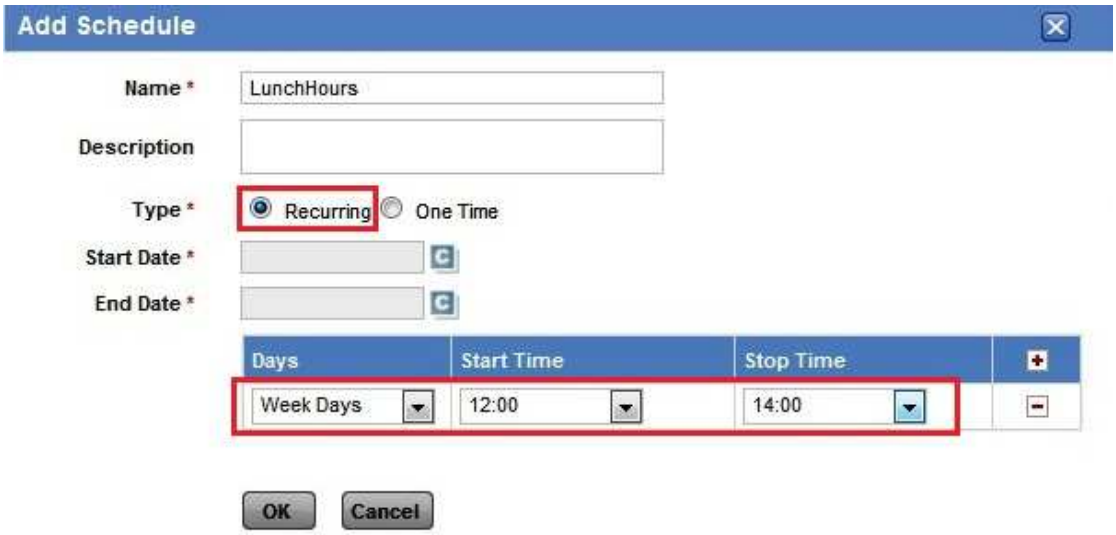


- Set the Firewall action to ACCEPT and create the rule

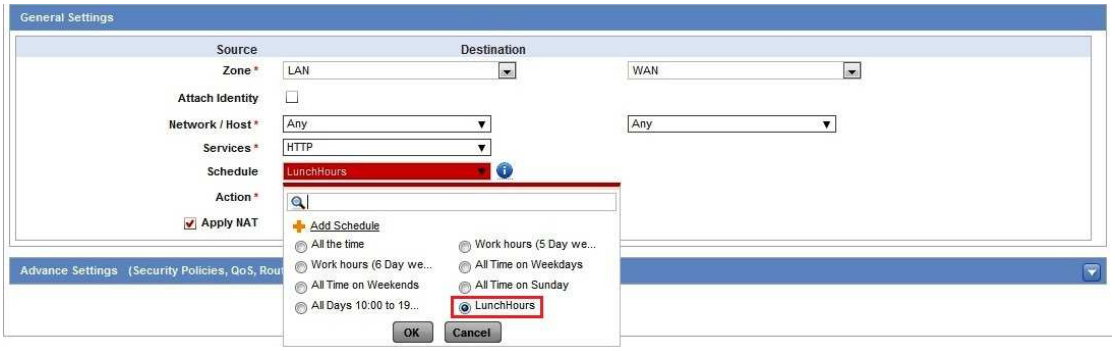
- Make sure the above created rule is above all the generic rules. Verify by accessing internet from your machine.

Lab #8 Create Schedule & Apply in Firewall Rule

- Navigate to Objects → Schedule → Add. Define schedule to allow internet access during lunch time on recurring basis on weekdays

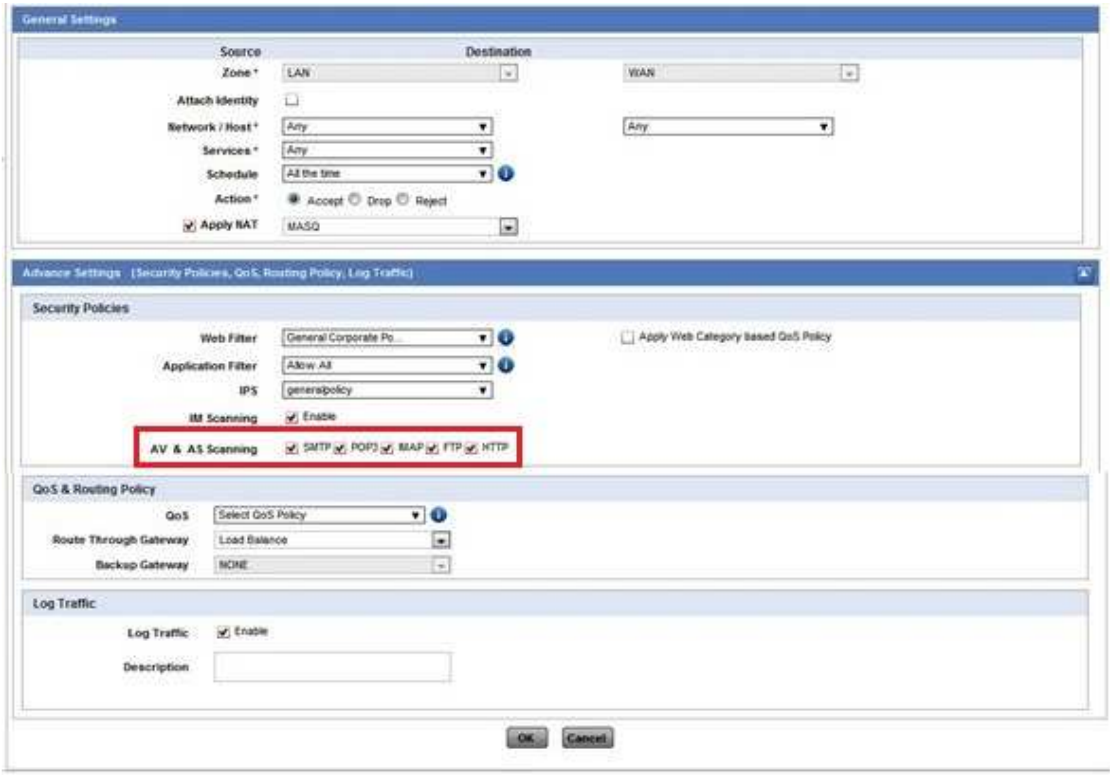


- Create a firewall rule as follows to choose the schedule created in the step above.



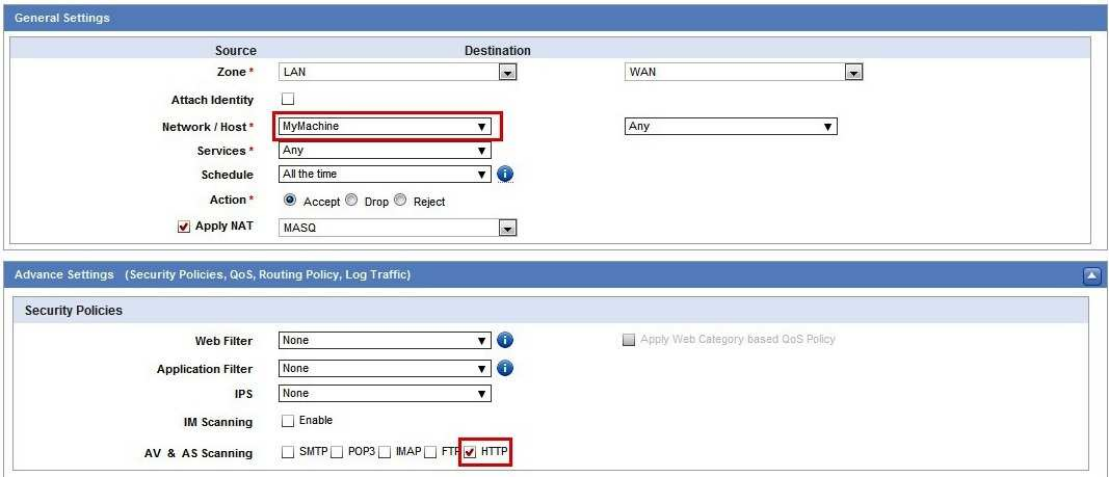
Lab #9 Enable / Disable Anti-Virus & Anti-Spam Scanning

Edit the default firewall rule or the rules created in the above Labs to enable disable scanning. Check/Uncheck the protocols to enable/disable scanning.



Lab #10 Test Anti-Virus Scanning

- Navigate to Firewall → Rule → Add and create a firewall rule from LAN-WAN for your machine's IP address (Create Host). Enable HTTP scanning in the same firewall rule.



- Browse to the URL http://www.eicar.org/download/eicar.com.txt and you will see the Virus Alert message from Cyberoam.

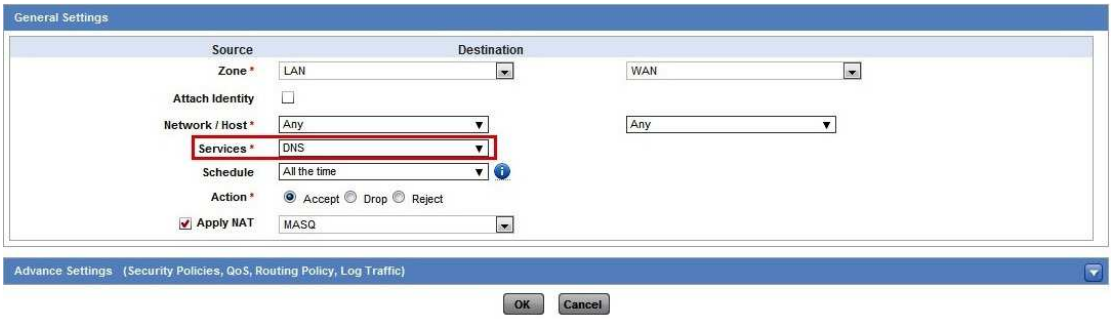
Cyberoam Anti Virus Alert

The URL you are trying to access has been blocked as it contains the malware "**EICAR-Test-File**"

URL : **www.eicar.org/download/eicar.com.txt**

Lab #11 Create Firewall Rule to Allow DNS Traffic

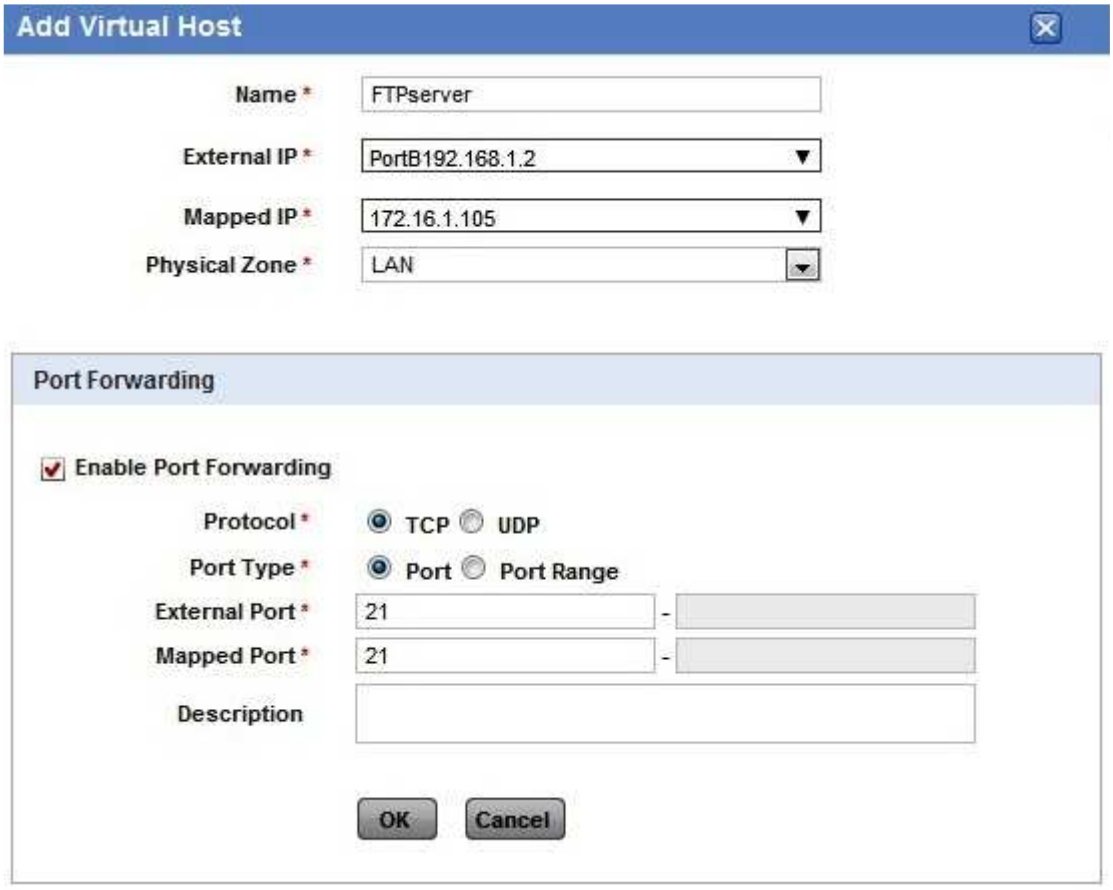
Navigate to Firewall→Create rule and create a LAN-WAN firewall rule with services as DNS.



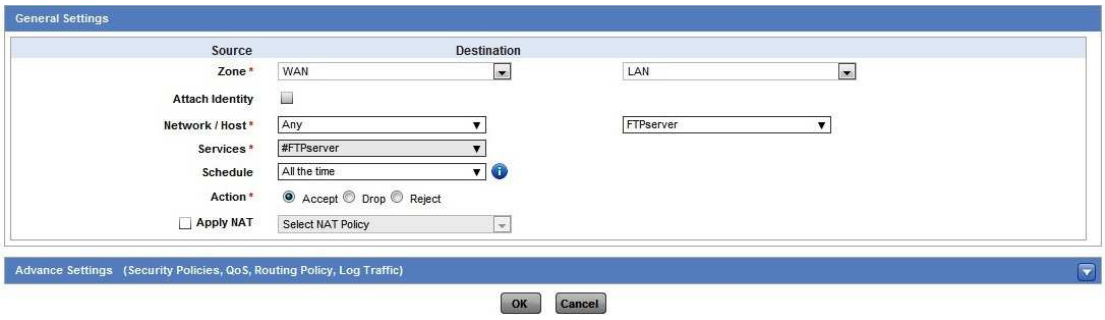
Lab #12 Create Virtual Host to Publish a FTP Server residing in the LAN

IP Schema used:
Cyberoam WAN IP: 192.168.1.2
Cyberoam LAN IP: 172.16.1.1
FTP Server IP: 172.16.1.105

- Navigate to Firewall→Virtual Host→Add and create a Virtual Host



- Navigate to Firewall → Rule → Add and create a WAN-LAN rule using the virtual host created above as the Destination host.

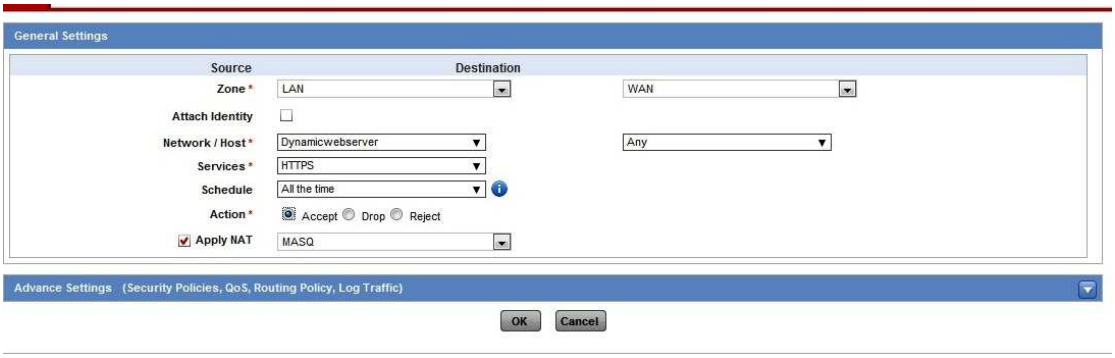


- All the requests for the WAN IP of Cyberoam (192.168.1.2) for FTP service will be routed to the internal FTP server (172.16.1.105)

Lab 13# Create MAC based host for Dynamic web server and create MAC based firewall rule

Create MAC based host for Dynamic web server

Now create MAC based firewall rule



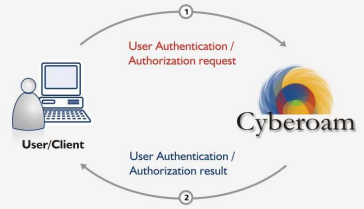
Module 6: User Authentication

Agenda:

- Local & External Authentication
- Authentication Settings
- Type of Authentication
- Single Sign On Concept
- Identity Based Policy
- Group Management
- User Management
- Identity Based Firewall
- Traffic Discovery
- Labs

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Local Authentication Flow



User Authentication process initiates, when the client tries to authenticate.

User Authentication process initiates, when the client tries to login with the login credentials.

Cyberoam | Unified Threat Management

External Authentication Flow

Cyberoam provides an authentication mechanism; where in users registered with two different servers can be validated.

Local & External Authentication:

To filter Internet requests based on identity based policies assigned, Cyberoam must be able to identify a user making a request. Cyberoam can be configured to allow or disallow users based on username and password. In order to use User Authentication, you must select at least one database against which Cyberoam should authenticate users.

When the user attempts to access, Cyberoam requests a user name and password and authenticates the user's credentials before giving access.

In a local authentication flow, User level authentication can be performed using the local user database on the Cyberoam and Before users log on to Cyberoam, Administrator has to create all the users in Cyberoam, assign them to a Group and configure for local authentication. In this flow, Cyberoam authenticate and authorise the Users by checking the local database.

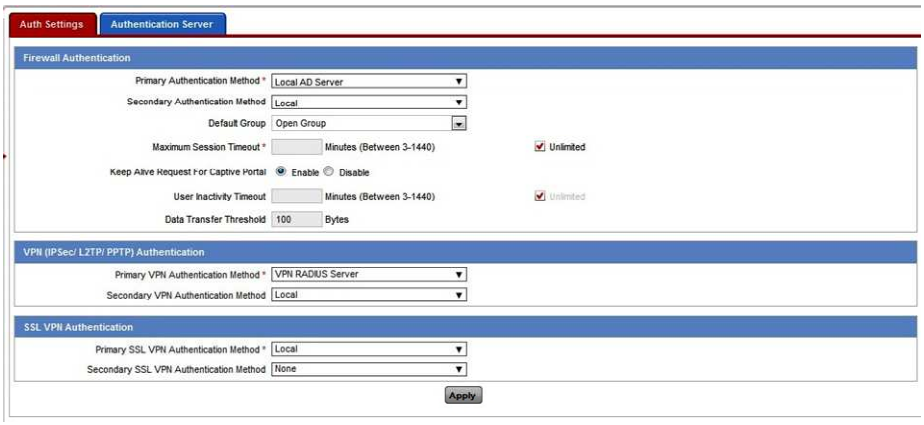
Similarly, In External Authentication flow, Cyberoam needs to be integrated with External authentication servers. In this flow, Cyberoam intercepts the authentication request and query the external server for authenticating the users.

Cyberoam also provides a feature of Multiple Authentication with two different networks. Two servers can be configured simultaneously, with one serving as a Primary Server and other as a Secondary Server. This assures secure access to the network’s internal resources and guarantees that the authenticated users are able to login successfully.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Authentication Settings

Identity → Authentication → Auth Settings



Note: All users need not authenticate against the same authentication server. VPN & SSL-VPN users can now authenticate against a different server than the one selected for firewall authentication.

Authentication Settings:

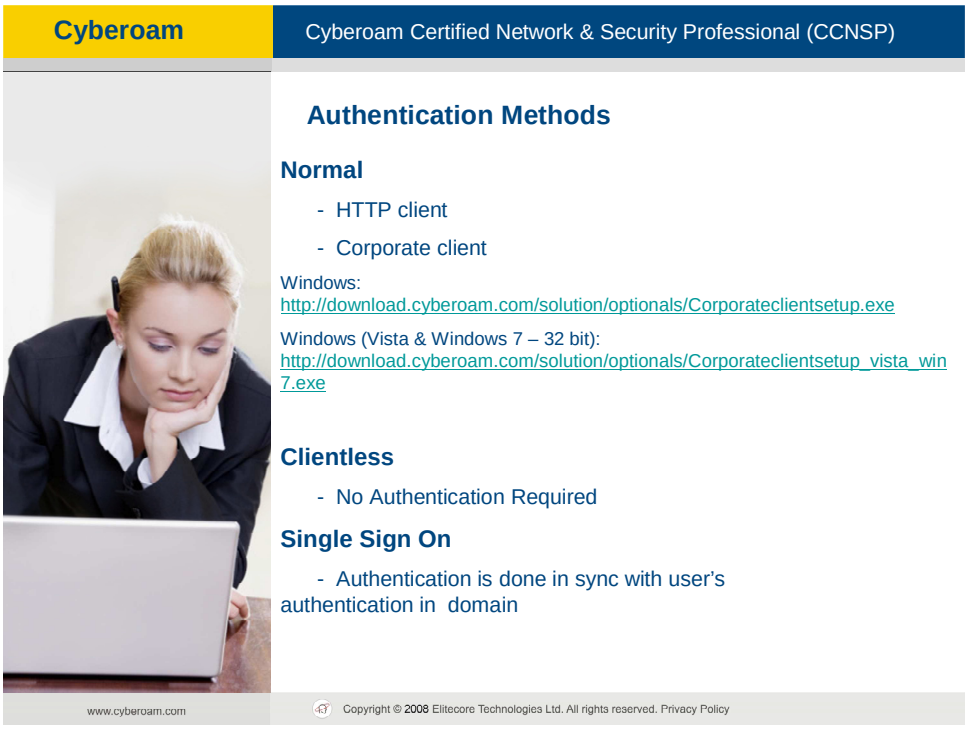
Cyberoam can be integrated with local and external authentication server for authenticating the users. It supports user authentication against:

External Authentication Server
- Active Directory
- LDAP server
- RADIUS server

Local Authentication Server
- Internal database defined in Cyberoam

You can configure Cyberoam to communicate against any of the above authentication server.

With the External Authentication Server, there is no need to create the users locally on the Cyberoam, username will be transparently created on the Cyberoam when users authenticate for the first time. However, it's necessary to create the username and groups when Local database is selected under Authentication settings.



Type of Authentication:

Cyberoam supports three types of authentication method:

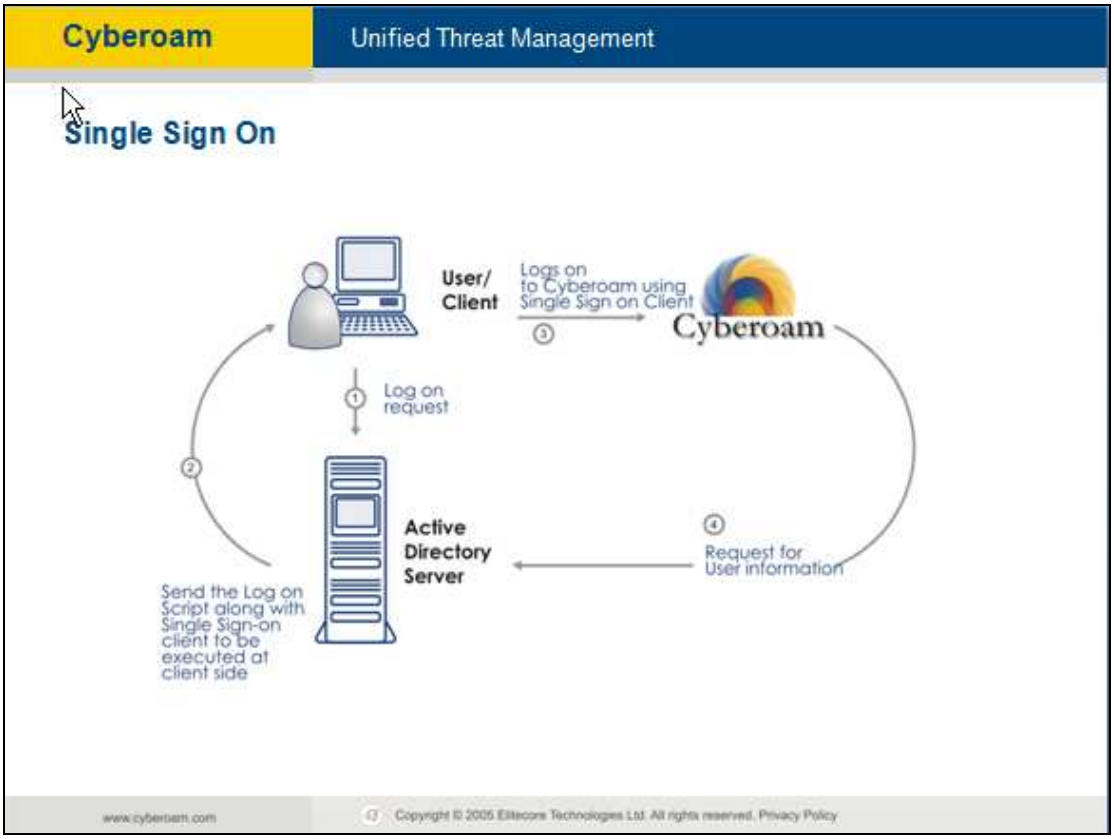
1. Normal
2. Clientless
3. Single Sign on (SSO)

Normal User has to logon to Cyberoam. Requires Cyberoam Corporate client (client.exe) on the User machine or user can use HTTP Client component (H) and all the policy-based restriction can be applied. This method is mainly required when authentication settings sets to Local Database, LDAP and Radius server.

Clientless does not require user to authenticate with Cyberoam either by Client.exe or HTTP Client, which is represented as "User name (C)". Users are authenticated against the IP address. This method main required when you are having Server like Exchange or Update Server, and wants these server to be able to access Internet without asking for any login credentials.

Single Sign On (SSO), If User is configured for Single Sign On, whenever User logs on to Windows domain; he/she is automatically logged to the Cyberoam, which is represented as "User name (S)". This method is applicable only for ADS and Windows Domain Controller.

Single Sign On Concept



Single Sign-On (SSO) is a transparent user authentication mechanism that provides privileged access to Web resources with a single workstation login. Users logged into a workstation locally but not logged into the domain will not be authenticated. For users that are not logged into the domain, manual login will be required for further authentication and that can achieved with HTTP or Client.exe.

SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SSO is transparent to end users and requires minimal administrator configuration.

Benefits of SSO include:

- Ease of use — Users only need to sign in once to gain automatic access to Web resources.
- Improved user experience — Windows domain credentials can be used to authenticate user for any traffic type without logging in using a Web browser.
- Transparency to users — Users are not required to re-enter user name and password for authentication.

How Single Sign on Works in Cyberoam

In Cyberoam, SSO works when it's integrated with ADS (Windows 2000 & onwards) and Windows Domain Controller (Windows NT).

Authentication Process completes in 4 steps which are mentioned below:

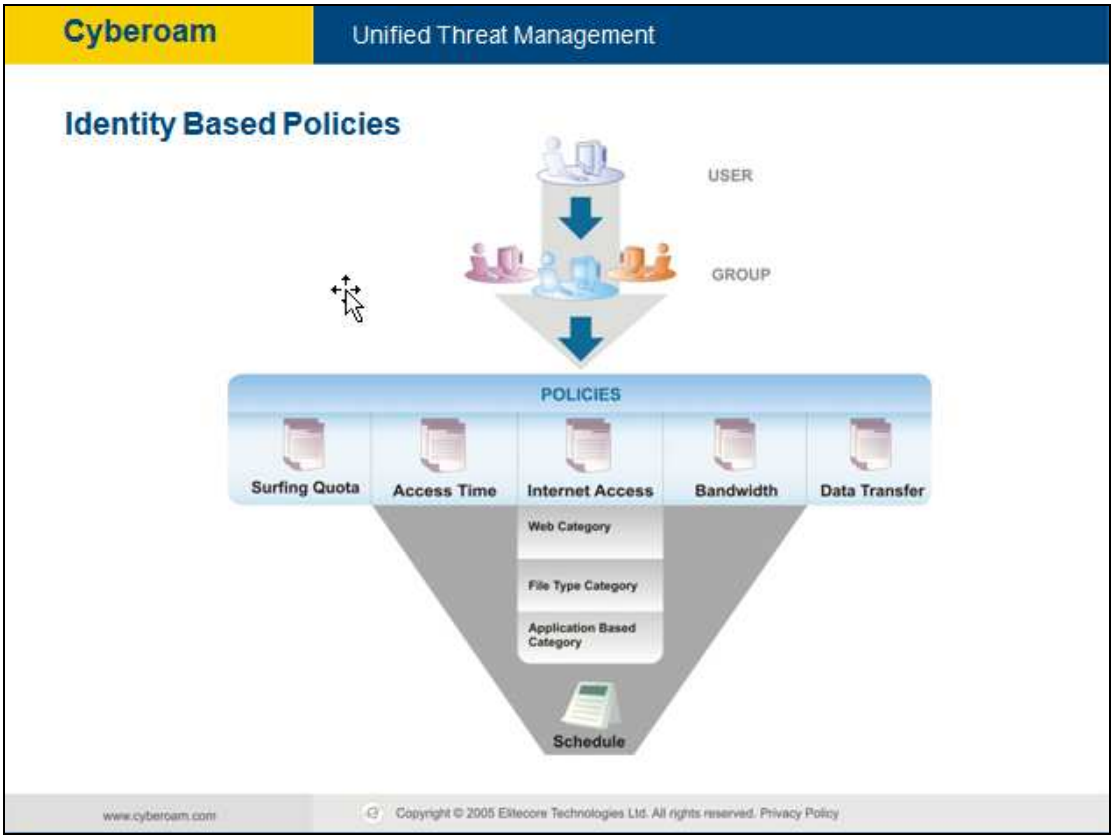
1) Whenever users login to system which is part of domain, a log on request is sent to Domain Server which authenticates the user to login to the system,

2) Domain server sends the log on script along with SSO client to be executed at the client side. This SSO client installation will be transparent to the end users.

3) After the successful installation, SSO client sends authentication request to Cyberoam for authorising it for web resources.

4) Cyberoam checked the username and password against the domain server and authorise it for the web resources. During this step, username will be created locally on the Cyberoam as well and become the part of Group (according to Domain group membership).

Identity Based Policies

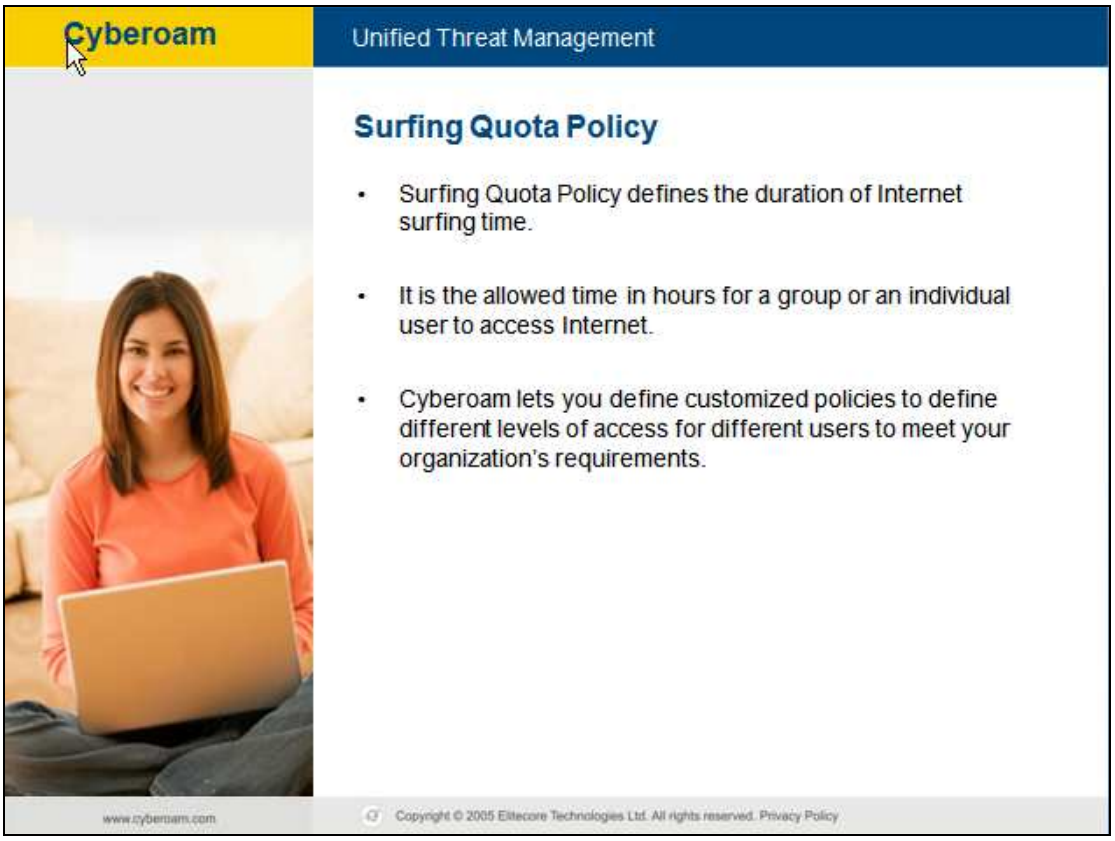


Cyberoam allows controlling access to various web resources with the help of Policy and allows defining following types of policies:

- Control individual user surfing time by defining Surfing quota policy.
- Schedule Internet access for individual users by defining Access time policy.
- Control web access by defining Internet Access policy.
- Allocate and restrict the bandwidth usage by defining Bandwidth policy.
- Limit total as well as individual upload and/or download data transfer by defining data transfer policy.

Cyberoam comes with several predefined policies. These predefined policies are immediately available for use until configured otherwise. Cyberoam also lets you define customised policies to define different levels of access for different users to meet your organisation's requirements.

Let's take all the policies one by one.


Cyberoam
Unified Threat Management
Surfing Quota Policy
• Surfing Quota Policy defines the duration of Internet surfing time.
• It is the allowed time in hours for a group or an individual user to access Internet.
• Cyberoam lets you define customized policies to define different levels of access for different users to meet your organization's requirements.
www.cyberoam.com
Copyright © 2005 Elitecore Technologies Ltd. All rights reserved. Privacy Policy

Surfing quota policy:

- Allocates Internet access time on cyclic or non-cyclic basis
- Single policy can be applied to number of Groups or Users

To create Surfing Quota policy, select Identity → Policy → Surfing Quota

Name: Name to identify the Policy. Duplicate names are not allowed.

Cycle Type: Select Cycle type.

Available Options:

Cyclic – Restricts surfing hours up to cycle hours defined on predefined time duration.

Non Cyclic – Surfing hour restriction is defined by total allotted days and time

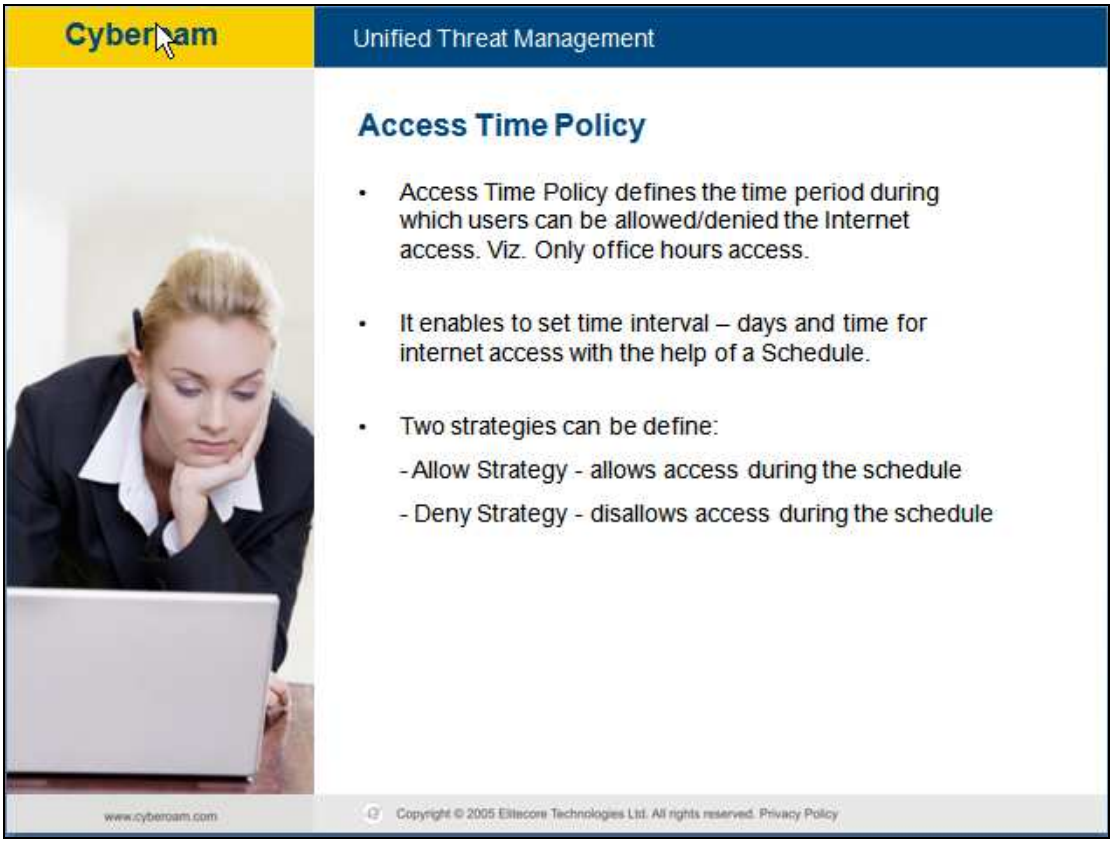
Cycle Hours: Specify Cycle Hours. Cycle hours define the upper limit of surfing hours for cyclic types of policies i.e. Daily, Weekly, Monthly and Yearly.

At the end of each Cycle, cycle hours are reset to zero i.e. for 'Weekly' Cycle type, cycle hours will to reset to zero every week even if cycle hours are unused.

Validity: Specify Validity in number of days. Validity defines the upper limit of total surfing days allowed i.e. restricts total surfing days to valid allotted days.
OR
Click Unlimited Days, if you do not want to restrict the total surfing days

Maximum Hours: Specify Maximum Hours. Maximum hours define the upper limit of total surfing hours allowed i.e. restricts total surfing hours to maximum hours.
OR
Click Unlimited Hours, if you do not want to restrict the total surfing hours.

Description: Specify Policy Description


Cyberoam
Unified Threat Management
Access Time Policy
• Access Time Policy defines the time period during which users can be allowed/denied the Internet access. Viz. Only office hours access.
• It enables to set time interval – days and time for internet access with the help of a Schedule.
• Two strategies can be define:
- Allow Strategy - allows access during the schedule
- Deny Strategy - disallows access during the schedule
www.cyberoam.com
Copyright © 2005 Elitecore Technologies Ltd. All rights reserved. Privacy Policy

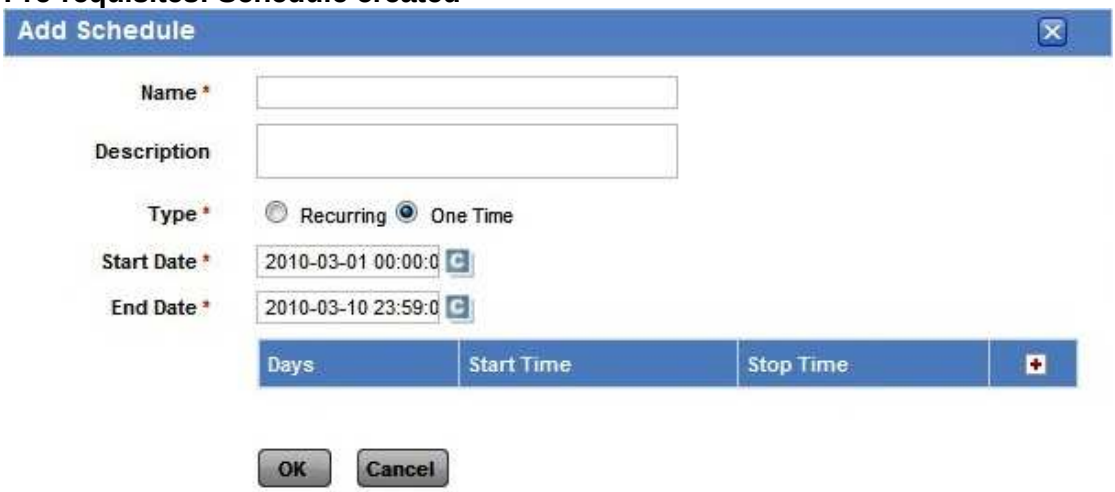
Access Time Policy:

A time interval defines days of the week and times of each day of the week when the user will be allowed or denied the Internet access.

Access time policy strategies:

Allow strategy - By default, allows access during the schedule
Deny strategy - By default, disallows access during the schedule

Pre-requisites: Schedule created



Screen Elements	Description
Schedule details	
Name	Specify schedule name. Choose a name that best describes schedule
Schedule Type	Specify type of schedule Recurring – applied at specified times of the day or on specified days of the week One time – applied only once for the period of time specified in the schedule
Start time & Stop time **(only if Schedule Type is 'One Time')**	Defines start and stop time for the schedule Start & stop time cannot be same
Description	Specify full description of schedule
Create button	Creates schedule Refer to Add Schedule Entry details to add time details

Table - Define Schedule screen elements

To create Access Time Policy, select Identity → Policy → Access Time

Screen Elements	Description
Access Time policy details	
Name	Specify policy name. Choose a name that best describes the policy to be created. One cannot create multiple policies with the same name.
Schedule	Specify policy schedule Users will be allowed/disallowed access during the time specified in the schedule. Click *Schedule* list to select Click *View details* link to view the details of selected schedule Refer to Define Schedule on how to create a new schedule
Strategy for selected	Specify strategy to policy
Schedule	Allow – Allows the Internet access during the scheduled time interval Disallow - Does not allow the Internet access during the scheduled time interval Click to select
Description	Specify full description of policy
Create button	Creates policy

Table - Create Access Time policy screen elements

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Web & Application Filter

• Web Filter Policy controls user's web access. It specifies which user has access to which sites and allows defining powerful security policies based on almost limitless policy parameters like Individual users, Groups of users, Time of day, Location/Port/Protocol type, Content type, Bandwidth usage (for audio, video and streaming content).

• Application Filter Policy controls user's application access. It allows administrator to control access to applications based on almost limitless policy parameters like Individual users, Groups of users, Time of day.

•Default web & application filtering policy is based on LAN→WAN policy selected while running "Network Configuration Wizard".

•Applying default policy allows all the users to surf without login depending on the default policy applied and web surfing reports are generated on IP address as user has actually not logged on to Cyberoam.

www.cyberoam.com

Web Filter Policy:

When defining a policy, you can deny or allow access to any Web category/File Type Category.

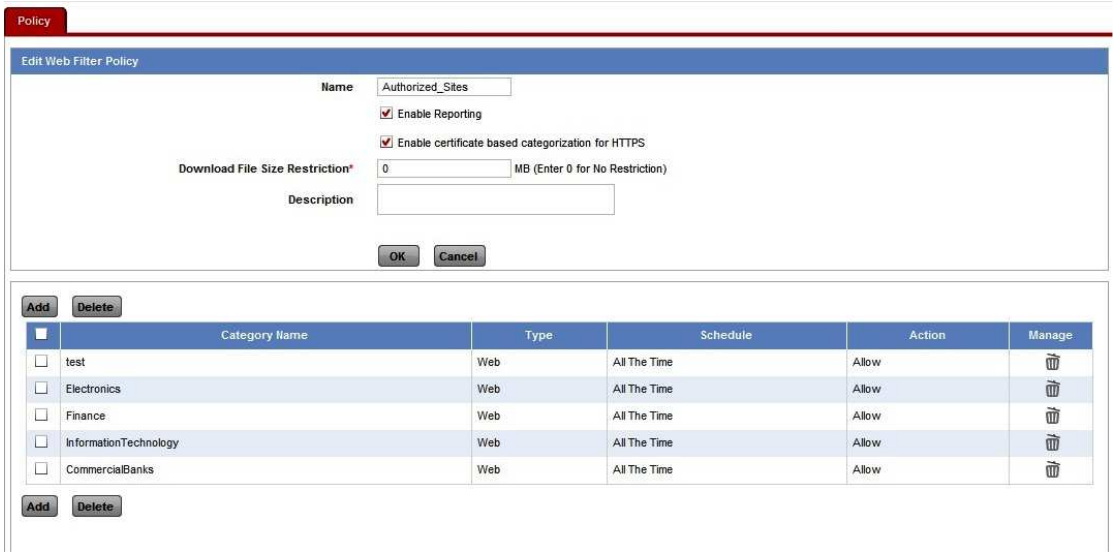
Web Filter policy types:

- Allow - By default, allows user to view everything except the sites and resources specified in the rule. E.g. To allow access to all sites except Mail sites

- Deny - By default, prevents user from viewing everything except the sites and files specified in the rule. E.g. To disallow access to all sites except Information Technology Sites.

It is not possible to allow Application categories in "Deny all" policy

To create Web Filter policy, select Web Filter → Policy → Add



Name: Name to identify the Policy. Duplicate names are not allowed.

Template: Select a template if you want to create a new policy based on an existing policy and want to inherit all the categories restrictions from the existing policy.

Enable Reporting: By default, Internet usage report is generated for all the users. But Cyberoam allows bypassing reporting of certain users.

Enable the 'Enable Reporting' checkbox to create Bypass reporting web filter policy. Internet usage reports will not include access details of all the users to whom this policy will be applied.

Enable Certificate based categorization for HTTPS:
Enable the 'Enable Certificate based categorization for HTTPS' check box to enable filtering of HTTPS traffic based on domain names using site X.509 certificates.

If enabled, users will not be able to bypass and access blocked sites using URL translation or HTTP proxy websites hosted on HTTPS.
In other words, if enabled Cyberoam will block attempts to by web content filtering and sites hosted on SSLv2, SSLv3 and TLS protocols.

By default, it is enabled. Enabling categorization from Web Admin Console will not have any effect if it is disabled from CLI console. By default, the categorization from CLI is enabled.
Use CLI command: show secure-scanning HTTPS to confirm. For more details, check Cyberoam Console Guide.

Download File Size Restriction: Specify the file size (in MB) in the textbox against Download File Size Restriction to configure the maximum allowed file download size. User will not be allowed to download file greater than the configured size.

Description: Specify Policy Description. Add rules after policy is added successfully.

Category Name: Select Web Category or File Type Category to be added. You can select more than one category by selecting the checkbox. You can also search the category name from the search text box provided.

Action: Specify Action for the categories selected - Allow OR Deny

Schedule: Select the Schedule for categories selected.

Application Filter

Application Filter Policy controls user's application access. It specifies which user has access to which applications and allows defining powerful security policies based on almost limitless policy parameters like:
•Individual users
•Groups of users
•Time of day

Two strategies based on which Application Filter Policy can be defined:

Allow: By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.

Deny: By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.

Cyberoam comes with the following predefined policies for applications: Allow All and Deny All. These two predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization's requirements.

To add application filter policies, go to Application Filter → Policy → Policy.

Parameters

Name	Name to identify the Policy. Duplicate names are not allowed.
Description	Specify Policy Description. Add rule after policy is created successfully.
Select Categories	Select Application Category from the list of available categories.
Select Application	Select the Applications under the Category selected. You can also select more than one application using the checkbox. You can search for the application using the Search textbox.
Action	Select the Action: Allow OR Deny
Schedule	Select the Schedule from the list of schedules available.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

QoS Policy

•The primary objective of QoS Policy is to manage and distribute total bandwidth on certain parameters and user attributes.

•It allocates and limits the maximum bandwidth usage of the user and controls web and network traffic.

Policy can be defined/created for:

•User - To restrict bandwidth of a particular user. Can be applied to a user's profile.

•Firewall Rule – This policy can be applied in the firewall rule only. Bandwidth restriction will be enforced on the traffic matching the firewall rule.

•Web Category – To apply bandwidth restrictions on custom or default web categories. Policy can only be assigned to custom or default web categories.

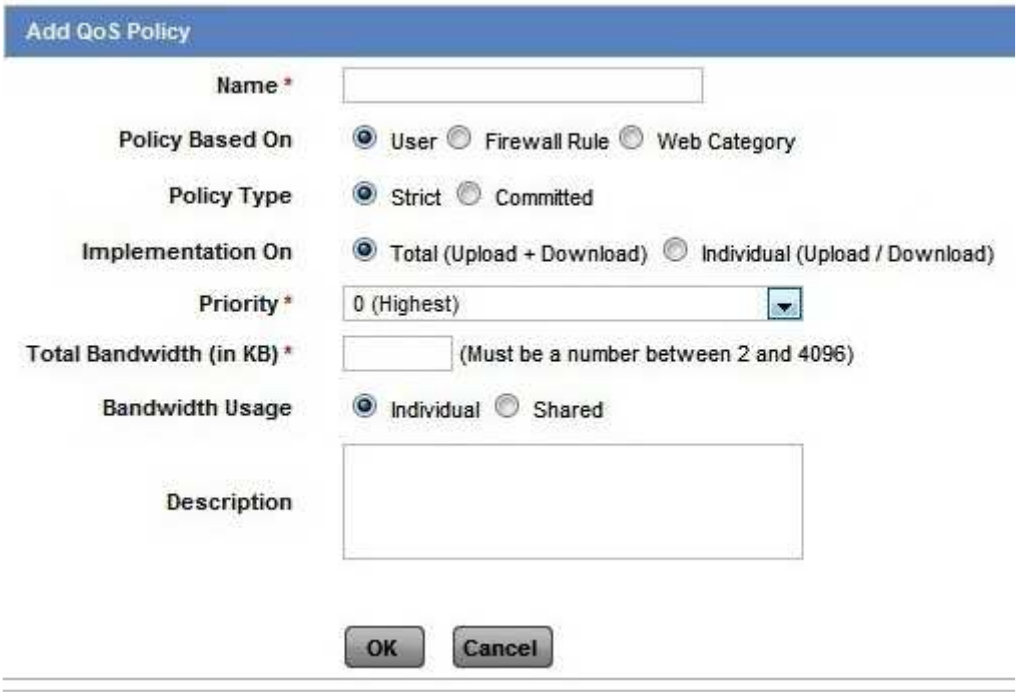
www.cyberoam.com

QoS Policy:

Bandwidth is the amount of data passing through a media over a period of time and is measured in terms of kilobytes per second (kbps) or kilobits per second (kbits) (1 Byte = 8 bits).

Policy can be defined/created for:

- User - It restricts the bandwidth of a particular user.
- Firewall Rule - It restricts the bandwidth for any entity to which the firewall rule is applied.
- Web Category – It restricts the bandwidth for the URL categorized under the Web category. To implement restriction, policy is to be assigned through firewall rule.



Strict - In this type of bandwidth restriction, user cannot exceed the defined bandwidth limit. Two ways to implement strict policy:

- Total (Upstream + Downstream)
- Individual Upstream and Individual Downstream

Implementation on	Bandwidth specified	Example
Total (Upstream + Downstream)	Total bandwidth	Total bandwidth is 20 kbps and upstream and downstream combined cannot cross 20 kbps
Individual Upstream and Individual Downstream	Individual bandwidth i.e. separate for both	Upstream and Downstream bandwidth is 20 kbps then either cannot cross 20 kbps

Table - Implementation types for Strict - Bandwidth policy

Committed - In this type of bandwidth restriction, user is allocated the guaranteed amount of bandwidth and user can draw bandwidth up to the defined burstable limit, if available.

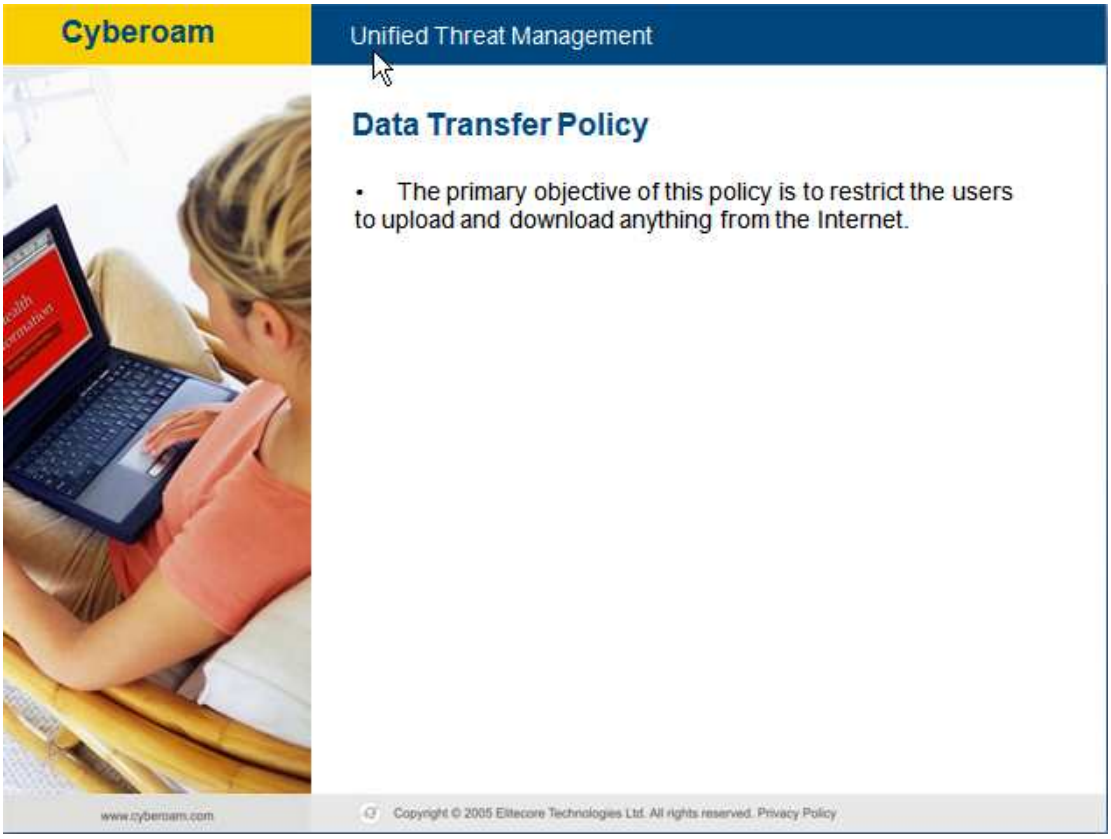
It enables to assign fixed minimum and maximum amounts of bandwidth to users. By borrowing excess bandwidth when it is available, users are able to burst above guaranteed minimum limits, up to the burstable rate. Guaranteed rates also assure minimum bandwidth to critical users to receive constant levels of bandwidth during peak and non-peak traffic periods.

Guaranteed represents the minimum guaranteed bandwidth and burstable represents the maximum bandwidth that a user can use, if available. Two ways to implement committed policy:

- Total (Upstream + Downstream)
- Individual Upstream and Individual Downstream

Implementation on	Bandwidth specified	Example
Total (Upstream + Downstream)	Guaranteed bandwidth	Guaranteed bandwidth is 20 kbps then upstream and downstream combined will get 20 kbps guaranteed (minimum) bandwidth
	Burstable bandwidth	Burstable bandwidth is 50 kbps then upstream and downstream combined can get up to 50 kbps of bandwidth (maximum), if available
Individual Upstream and Individual Downstream	Individual Guaranteed and Brustable bandwidth i.e. separate for both	Individual guaranteed bandwidth is 20 kbps then upstream and downstream get 20 kbps guaranteed (minimum) bandwidth individually Individual burstable bandwidth is 50 kbps then upstream and downstream get maximum bandwidth up to 50 kbps, if available individually

Table - Implementation types for Committed - Bandwidth policy



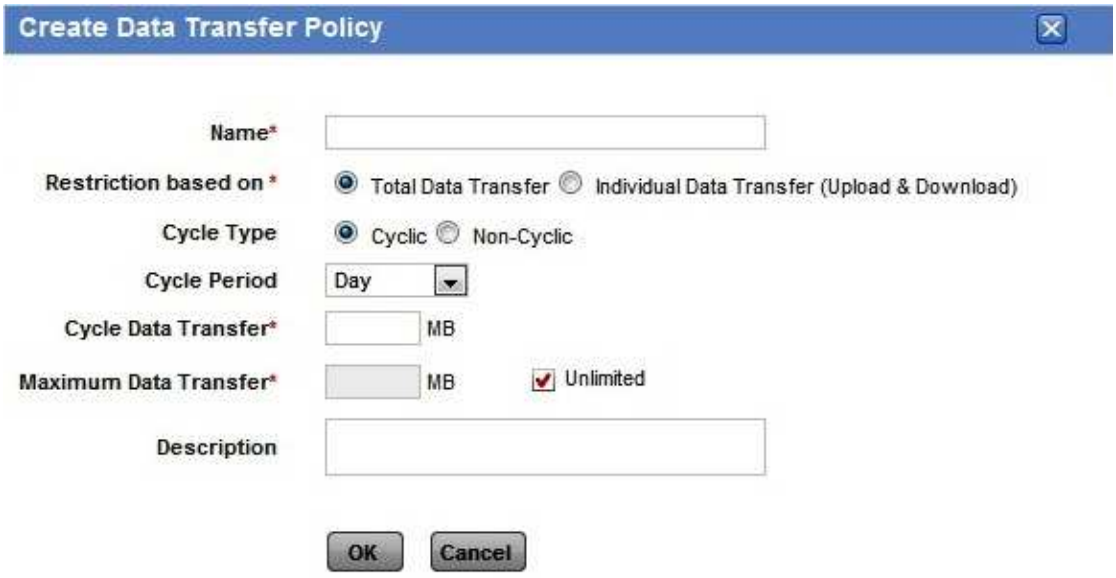
Data Transfer policy

- Limits data transfer on a cyclic or non-cyclic basis.
- Single policy can be applied to number of Groups or Users.

Data transfer restriction can be based on:

- Total Data transfer (Upload + Download)
- Individual Upload and/or Download

Cyberoam provides several predefined policies, which are available for use until configured otherwise. You can also define Customised policies to define different limit for different users to meet your organisation's requirements.



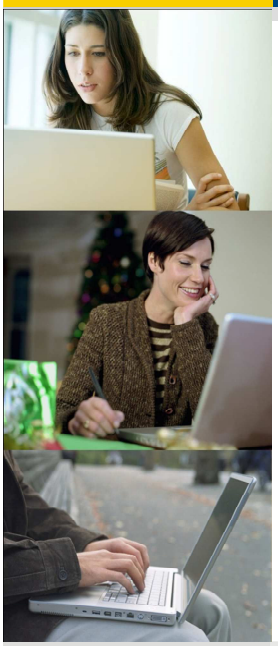
Screen Elements	Description
Create Data Transfer policy	
Name	Specify policy name. Choose a name that best describes the policy
Cycle type	Specify cycle type Available options Daily – restricts data transfer up to cycle hours defined on daily basis Weekly – restricts data transfer up to cycle hours defined on weekly basis Monthly – restricts data transfer up to cycle hours defined on monthly basis Yearly – restricts data transfer up to cycle hours defined on yearly basis Non-cyclic – data restriction is defined by the Total data transfer limit
Restriction based on	Specify whether the data transfer restriction is on total data transfer or on individual upload or download

	Click *Total Data Transfer* to apply data transfer restriction on the Total (Upload + Download) data transfer Click *Individual Data Transfer* to apply data transfer restriction on the Individual Upload and Individual Download data transfer
Shared allotted data transfer with group members **Only if Cycle Type is 'Non-cyclic'**	Specify whether the allotted data transfer will be shared among all the group members or not Click to share
Policy Description	Specify full description of the policy
Restriction Details	
Cycle Total Data Transfer Limit (MB) **Only if Cycle Type is not 'Non-cyclic' and Restriction is based on 'Total Data Transfer'**	Specify Cycle Total Data transfer limit It is the upper limit of total data transfer allowed to the user per cycle. User gets disconnected if limit is reached.
Cycle Upload Data Transfer Limit (MB) **Only if Cycle Type is not 'Non-cyclic' and Restriction is based on 'Individual Data Transfer'**	Specify Cycle Upload Data transfer limit. It is the upper limit of upload data transfer allowed to the user per cycle. User will be disconnected if limit is reached OR if you do not want to restrict upload data transfer per cycle, click Unlimited Cycle Upload Data transfer
Cycle Download Data Transfer Limit (MB) **Only if Cycle Type is not 'Non-cyclic' and Restriction is based on 'Individual Data Transfer'**	Enter Cycle Download Data transfer limit. It is the upper limit of download data transfer allowed to the user per cycle. User will be disconnected if limit is reached OR if you do not want to restrict download data transfer per cycle, click Unlimited Cycle Download Data transfer
Total Data Transfer Limit (MB) **Only if Restriction is based on 'Total Data Transfer'**	Specify Total Data transfer limit. It is the data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed OR if you do not want to restrict total data transfer, click Unlimited Total Data Transfer
Upload Data Transfer Limit (MB) **Only if Restriction is based on 'Individual Data Transfer'**	Specify Upload Data transfer limit. It is the total upload data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed OR if you do not want to restrict total upload data transfer, click Unlimited Upload Data Transfer
Download Data Transfer Limit (MB) **Only if Restriction is based on 'Individual Data Transfer'**	Specify Download Data transfer limit. It is the upper download data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed OR if you do not want to restrict total download data transfer, click Unlimited Download Data Transfer
Create button	Creates policy
Cancel button	Cancels the current operation and returns to Manage Data transfer policy page

Table – Create Data transfer policy screen elements

Group Management

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)



Group Management

- Group is a collection of users having common policies that can be managed as a single unit.
- Its a mechanism of assigning various policies to a number of users in one operation/step.
- It simplifies the user configuration.
- Users that belong to a particular group are referred to as a group user.

www.cyberoam.com

Group Management

A Group is a collection of users having common policies and a mechanism of assigning access of resources to a number of users in one operation/step. Instead of attaching individual policies to the user, create group of policies and simply assign the appropriate Group to the user and user will automatically inherit all the policies added to the group. This simplifies user configuration.

A group can contain default as well as custom policies. Various policies that can be grouped are:

- Surfing Quota policy which specifies the duration of surfing time and the period of subscription
- Access Time policy which specifies the time period during which the user will be allowed access
- Internet Access policy which specifies the access strategy for the user and sites
- Bandwidth policy which specifies the bandwidth usage limit of the user
- Data Transfer policy which specifies the data transfer quota of the user

Group types

Two types of groups:
1. Normal
2. Clientless

Normal A user of this group need to logon to Cyberoam using the Cyberoam Client to access the Internet

Clientless A user of this group need not logon to Cyberoam using the Cyberoam Client to access the Internet. Access control is placed on the IP address, which is represented as **Group name (C)**

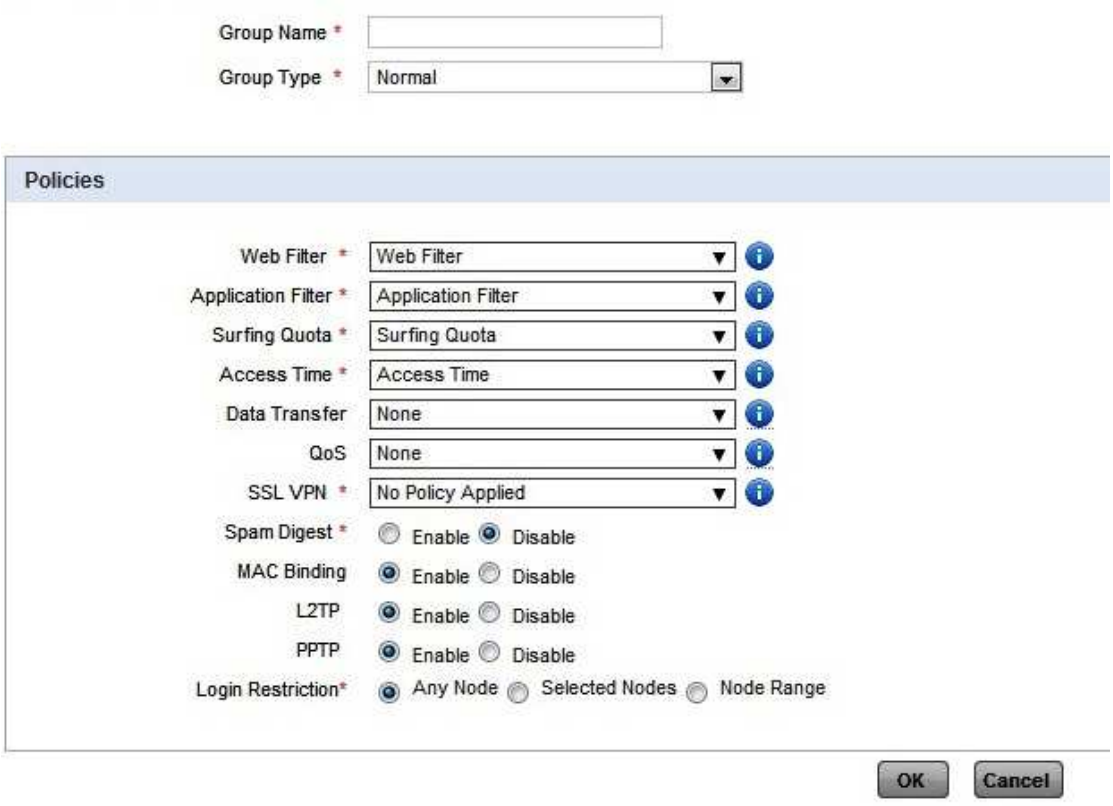
Use the below given decision matrix to decide which type of group will best suited for your network configuration.

Decision matrix for creation of Group

Feature	Normal Group	Clientless Group
Logon into Cyberoam required	Yes	No
Type of User Normal Clientless	 Yes No	 No Yes
Apply Login restriction	Yes	No
Apply Surfing Quota policy	Yes	No
Apply Access Time policy	Yes	No
Apply Bandwidth policy	Yes	Yes
Apply Internet Access policy	Yes	Yes
Apply Data transfer policy	Yes	No

Table - Group creation - Decision matrix

To create a Normal group, select Identity → User → User Group → Add



Web Filter	Select the Web Filter Policy from the list. You can also directly create policy from this page.
Application Filter	Select the Application Filter Policy from the list. You can also directly create policy from this page.
Surfing Quota	Select the Surfing Quota Policy from the list. You can also directly create policy from this page.
Access Time	Select the Access Time Policy from the list. You can also directly create policy from this page.
Data Transfer	Select the Data Transfer Policy from the list. You can also directly create policy from this page.
QoS	Select the QoS Policy from the list. You can also directly create policy from this page.
SSL VPN	Select SSL VPN policy from the dropdown list. If user is not to be provided the SSL VPN access then select “No Policy Applied”.
L2TP	Enable if user can get access through L2TP connection
PPTP	Enable if users can get access through PPTP connection
Spam Digest	Configure Spam Digest. Spam digest is an email and contains a list of quarantined spam messages filtered by Cyberoam and held in the user quarantine area. If configured, Cyberoam will mail the spam digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action. Available Options: **Enable** – User will receive the spam digest daily and overrides Group setting. **Disable** – User will not receive spam digest and overrides Group setting.
Simultaneous Logins	Specify number of concurrent logins that will be allowed to user OR Click ‘Unlimited’ for allowing unlimited Concurrent logins. The specified setting will override the global setting specified in the •client preferences.
MAC Binding	Enable/disable “MAC Binding”. By binding User to MAC address, you are mapping user with a group of MAC addresses.
MAC Address List	Specify MAC addresses for example 01:23:45:67:89:AB. Once you enable MAC binding, user will be able to login through pre-specified machines only. To configure multiple MAC addresses use comma for example 01:23:45:67:89:AB, 01:23:45:67:89:AC or specify each address in new line.

Login Restriction	Select the appropriate option to specify the login restriction for the user. Available Options: **Any** - Select to allow user to login from any of the nodes in the network **User Group Node(s)** - Select to allow user to login only from the nodes assigned to the group. **Selected Nodes** - Select to allow user to login from the specified nodes only. Specify IP address and click Add icon to add more nodes and remove icon to delete nodes. **Range** – Select to allow range of IP Address. Specify IP Address range.

Managing the Groups: Identity → User → User Group

Add Button: Add a new User Group.

Web Filter Policy:Web Filter Policy applied

Application Filter Policy: Application Filter Policy applied.

Surfing Quota Policy: Surfing Quota Policy applied.

Access Time Policy: Access Time Policy applied.

Data Transfer Policy: Data Transfer Policy applied.

QoS Policy: QoS Policy applied.

SSL VPN: SSL VPN policy applied.

MAC Binding:
- If MAC Binding Disabled
- If MAC Binding Enabled

L2TP
- If L2TP Configuration Disabled
- If L2TP Configuration Enabled

PPTP
- If PPTP Configuration Disabled
- If PPTP Configuration Enabled

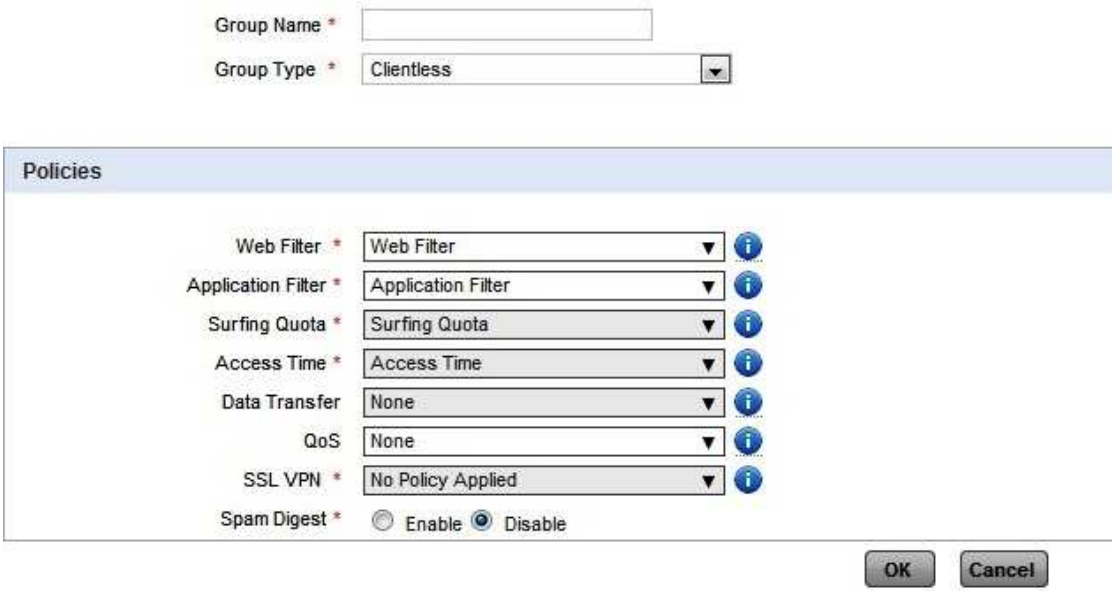
Spam Digest
- If Spam Digest Disabled
- If Spam Digest Enabled

Login Restriction: Login Restriction applied – Any, Selected Nodes or Range.

Edit Icon: Edit the User Group.

Delete Button: Delete the User Group.

Clientless Groups: Identity → User → User group → Add



User Management

User Management:

Users are identified by an IP address or a user name and assigned to a group. All the users in a group inherit all the group policies. Refer to Policy Management to define new policies.

User types

Cyberoam supports three types of Users:
1. Normal
2. Clientless
3. Single Sign on

Normal User has to logon to Cyberoam. Requires Cyberoam client (client.exe) on the User machine or user can use HTTP Client component and all the policy-based restriction can be applied.

Clientless Does not require Cyberoam client component (client.exe) on the User machines, which is represented as **User name (C)**

Single Sign On If User is configured for Single Sign On, whenever User logs on to Windows, he/she is automatically logged to the Cyberoam, which is represented as **User name (S)**

Use the given decision matrix below to decide which type of the user should be created.

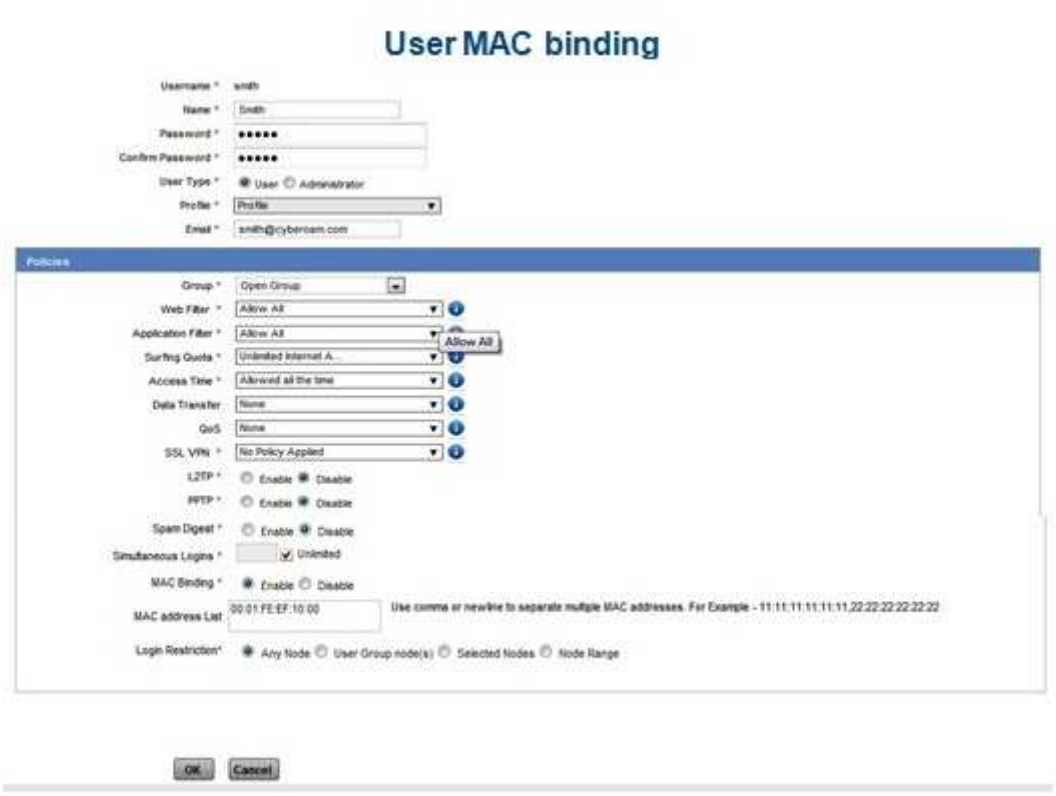
Decision matrix for creation of User

Feature	Normal User	Clientless User	Single Sign on User
User Login required	Yes	No	No
Type of Group Normal Clientless	 Yes No	 No Yes	 Yes No
Apply Login restriction	Yes	Yes	Yes
Apply Surfing Quota policy	Yes	No	No
Apply Access Time policy	Yes	No	No
Apply Bandwidth policy	Yes	Yes	Yes
Apply Internet Access policy	Yes	Yes	Yes
Apply Data Transfer policy	Yes	No	Yes

Table - Create User - Decision matrix

With External Authentication Server, there is no need to create the users locally on the Cyberoam, username will be transparently created on the Cyberoam when users authenticate for the first time. However, it's necessary to create the username when Local database is selected under Authentication settings.

User/MAC address binding



Cyberoam provides a way to bind one user to one computer so that only one user is allowed to login to the network from a specific computer.

In other words, User can login to Cyberoam and use the internet only from his/her own computer. User will not be able to login from any other computer and no one else will be able to login from his/her computer.

This is a major security feature which prevents anyone from 'impersonating' someone else even if they have changed their IP address.

By default, it is disabled and can be enabled from CLI console using "set usermac" command. One is required to restart management services from CLI after making any changes. It is possible to configure MAC addresses for individual users or group from Web Admin console only after binding is enabled from CLI.

User/MAC binding is supported only with Windows Cyberoam Corporate Client and Windows Single Sign On Client.

Username	Specify username, which uniquely identifies user and will be used for login.
Name	Specify Name of the User
Password	Specify Password
Confirm Password	Specify Password again for confirmation. You must use the same spelling. Password is case sensitive.
User Type	Click User Type list to select the type of user.

	Available options: User or Administrator
Profile	Select the Profile from the list. This option is only available for Administrator user type. Depending on user group type default Web Admin Console access control will be applied. You can create and manage profiles from System → Administration → Profile. Alternately, You can directly create profile from this page too.
Email	Specify Email ID.
Policies	
Group	Select Group in which user is to be added. User will inherit all the policies assigned to the group.
Web Filter	Select the Web Filter Policy from the list. You can also directly create policy from this page.
Application Filter	Select the Application Filter Policy from the list. You can also directly create policy from this page.
Surfing Quota	Select the Surfing Quota Policy from the list. You can also directly create policy from this page.
Access Time	Select the Access Time Policy from the list. You can also directly create policy from this page.
Data Transfer	Select the Data Transfer Policy from the list. You can also directly create policy from this page.
QoS	Select the QoS Policy from the list. You can also directly create policy from this page.
SSL VPN	Select SSL VPN policy from the dropdown list. If user is not to be provided the SSL VPN access then select “No Policy Applied”.
L2TP	Enable if user can get access through L2TP connection
PPTP	Enable if users can get access through PPTP connection
Spam Digest	Configure Spam Digest. Spam digest is an email and contains a list of quarantined spam messages filtered by Cyberoam and held in the user quarantine area. If configured, Cyberoam will mail the spam digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action. Available Options: **Enable** – User will receive the spam digest daily and overrides Group setting. **Disable** – User will not receive spam digest and overrides Group

	setting.
Simultaneous Logins	Specify number of concurrent logins that will be allowed to user OR Click 'Unlimited' for allowing unlimited Concurrent logins.
	The specified setting will override the global setting specified in the client preferences.
MAC Binding	Enable/disable "MAC Binding". By binding User to MAC address, you are mapping user with a group of MAC addresses.
MAC Address List	Specify MAC addresses for example 01:23:45:67:89:AB. Once you enable MAC binding, user will be able to login through pre-specified machines only. To configure multiple MAC addresses use comma for example 01:23:45:67:89:AB, 01:23:45:67:89:AC or specify each address in new line.
Login Restriction	Select the appropriate option to specify the login restriction for the user. Available Options: **Any** - Select to allow user to login from any of the nodes in the network **User Group Node(s)** - Select to allow user to login only from the nodes assigned to the group. **Selected Nodes** - Select to allow user to login from the specified nodes only. Specify IP address and click Add icon to add more nodes and remove icon to delete nodes. **Range** – Select to allow range of IP Address. Specify IP Address range.

User configuration is given precedence over Group configuration i.e. User MAC binding and policies configuration is given priority over Group configuration.

Add Clientless users

Clientless Users are the Users who can bypass Cyberoam Client login to access resources. It is possible to add a single clientless user as well as more than one clientless user at a time. When you add multiple clientless users, users are represented by IP addresses and not by the name.

To create the clientless users, Identity → User → Clientless User

Username: Specify username, which uniquely identifies user and will be used for login.

IP Address: Specify IP Address.

Group: Select Group for Clientless User.

Name: Name of the User.

Email: Specify Email ID.

Spam Digest:
Configure Spam Digest. Spam digest is an email and contains a list of quarantined spam messages filtered by Cyberoam and held in the user quarantine area. If configured, Cyberoam will mail the spam digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.

Available Options:

Enable – User will receive the spam digest daily and overrides Group setting.

Disable – User will not receive spam digest and overrides Group setting.

Apply Group's Settings - User will receive Spam Digests as per configured for the Group user belongs to.

Add Icon Click the Add Icon to add a new Clientless User.

Remove Icon Click the Remove Icon to delete a Clientless User

NOTE
Duplicate Usernames cannot be created

Make sure that subnets or individually defined IP addresses do not overlap

Create Group before assigning it to a User. Refer to Create Groups to create new groups

Manage Users: Identity → User

Add Button: Add a new Clientless User.

ID: User ID for Clientless User.

Username: Unique username to identify the User.

Group: Group Name to which user belongs.

Status: Status of the Clientless User

- Deactive. User is not is active.
- Active.

Name: Name of the user.

Spam Digest: Configured Digest Setting – Enable, Disable or Apply Group's Setting.

Edit Icon: Edit the Clientless User

Delete Button: Delete the Clientless User

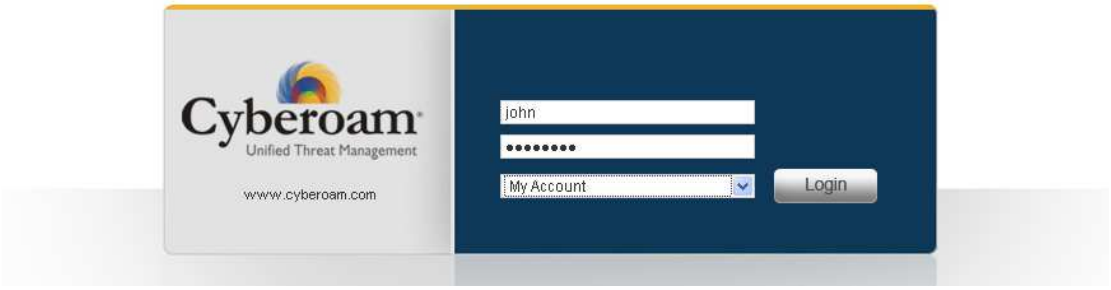
Manage Clientless Users

Select **Identity → User → Clientless Users** to view list of Users and click User name to be modified.

User My Account

User My Account gives details like Personal details and Internet usage of a particular user. User can change his/her password using this tab.

1. Normal Users can view their My Account details from GUI.



Personal
Allows viewing and updating password and personal details of the user.

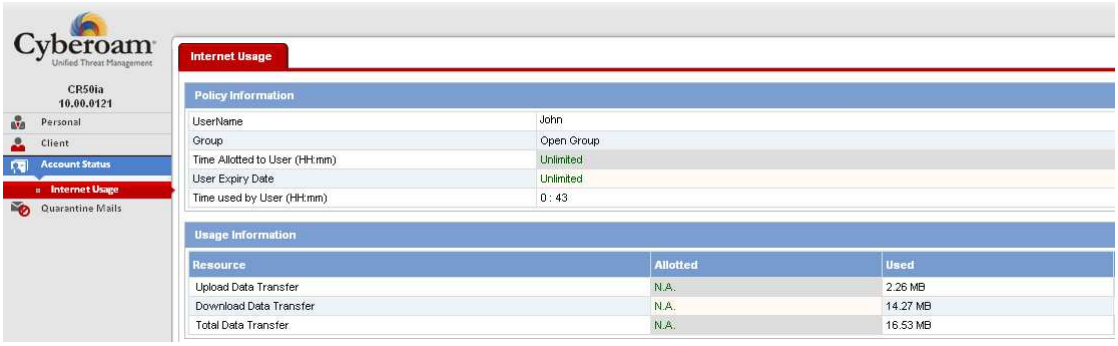
Change Password

In case of authentication with external server, changing the password doesn't make any sense as Cyberoam will not replicate the user password to the Server. This is valid for normal users who are created locally on the Cyberoam database.

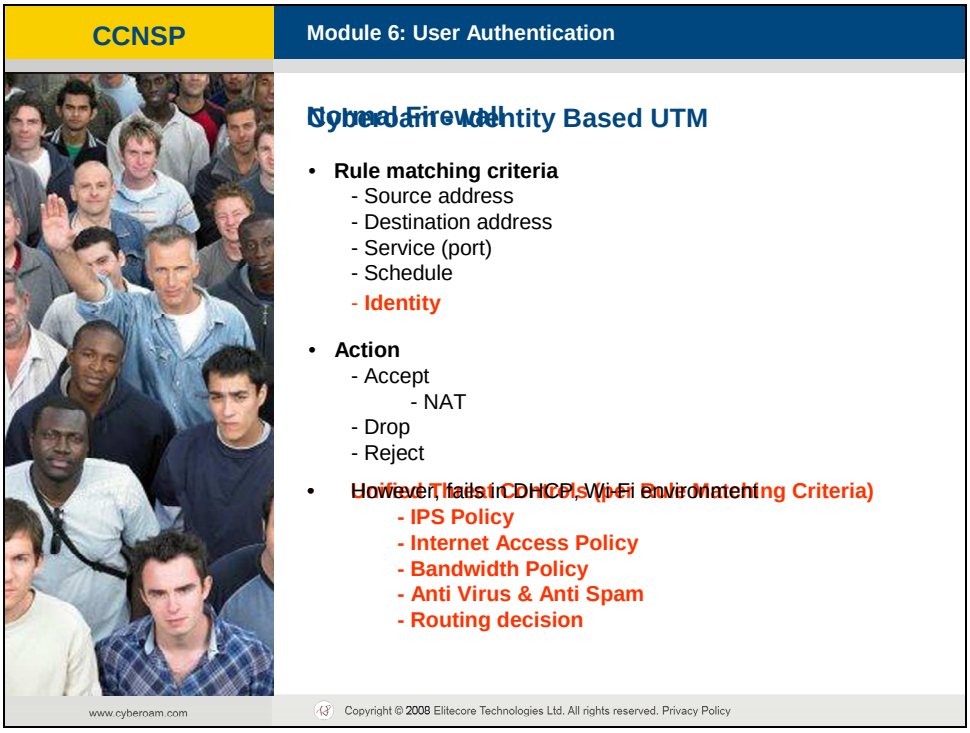
Change Personal Details

Account Status

Allows viewing Internet usage of the user.



Identity Based Firewall



Identity Based Firewall

A firewall protects the network from unauthorised access and typically guards the LAN and DMZ networks against malicious access; however, firewalls may also be configured to limit the access to harmful sites for LAN users.

The responsibility of firewall is to grant access from Internet to DMZ or Service Network according to the Rules and Policies configured. It also keeps watch on state of connection and denies any traffic that is out of connection state.
Firewall rules control traffic passing through the Cyberoam. Depending on the instruction in the rule, Cyberoam decides on how to process the access request. When Cyberoam receives the request, it checks for the source address, destination address and the services and tries to match with the firewall rule. ***If Identity match is also specified then firewall will search in the Live Users Connections for the Identity check. If Identity (User) found in the Live User Connections and all other matching criteria fulfils then action specified in the rule will be applied.*** Action can be allow or deny.

You can also apply different protection settings to the traffic controlled by firewall:

- Enable load balancing between multiple links.
- Configure antivirus protection and spam filtering for SMTP, IMAP, POP3, HTTP, FTP and FTP over HTTP traffic. To apply antivirus protection and spam filtering, you need to subscribe for Gateway Anti Virus and Gateway Anti Spam modules individually.
- Implement Intrusion Prevention System. To apply IPS policy you need to subscribe for Intrusion Prevention System module.
- Configure Web content filtering policies. To apply content filtering you need to subscribe for Web and Application Filter module.
- Apply bandwidth policy restriction.

Create Firewall rule

Cyberoam's Identity based firewall allows you to create firewall rules embedding user identity into the firewall rule matching criteria.

Firewall rule matching criteria now includes:

- Source and Destination Zone and Host
- User
- Service

One can attach the following policies to the firewall rule as per the defined matching criteria:

- Intrusion Prevention System(IPS)
- Anti Virus
- Anti Spam
- Web & application filter
- QoS policy
- Routing policy i.e. define user and application based routing

To create a firewall rule, you should:

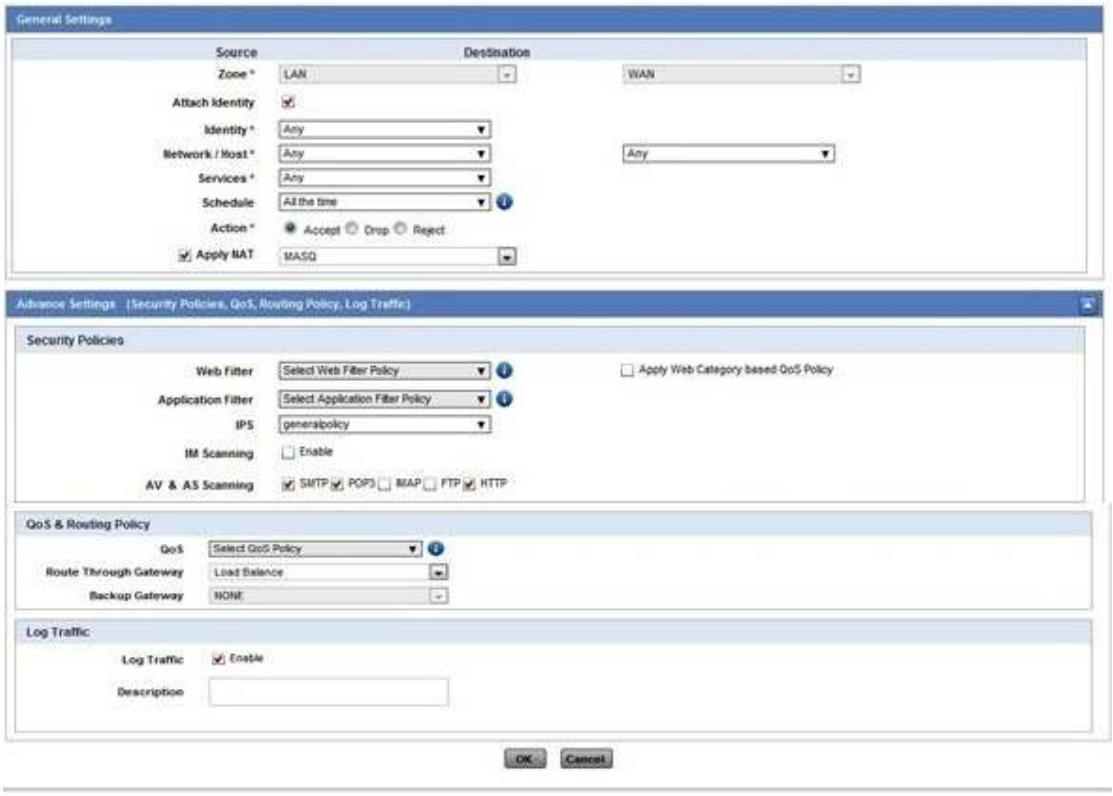
- Define matching criteria
- Associate action to the matching criteria
- Attach the threat management policies

For example, now you can:

- Restrict the bandwidth usage to 256kb for the user John every time he logs on from the IP 192.168.2.22
- Restrict the bandwidth usage to 1024kb for the user Mac if he logs on in working hours from the IP 192.168.2.22

Processing of firewall rules is top downwards and the first suitable rule found is applied. Hence, while adding multiple rules, it is necessary to put specific rules before general rules. Otherwise, a general rule might allow a packet that you specifically have a rule written to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list.

Select **Firewall → Rule → Add**



Parameters

Zone	Specify source and destination zone to which the rule applies.
Attach Identity (Only if source zone is LAN/DMZ/VPN)	Attach identity allows you to check whether the specified user/user group from the selected zone is allowed the access of the selected service or not. Click to attach the user identity. Enable check identity to apply following policies per user: Web policy and Application policy for Content Filtering (User's policy will be applied automatically but will not be effective till the Web and Application Filtering module is subscribed) Schedule Access IPS (User's IPS policy will be applied automatically but will not be effective till the IPS module is subscribed) Anti Virus scanning (User's anti virus scanning policy will be applied automatically but it will not be effective till the Gateway Anti Virus module is subscribed) Anti Spam scanning (User's anti spam scanning policy will be applied automatically but it will not be effective till the Gateway Anti Spam module is subscribed) QoS policy - User's QoS policy will be applied automatically

	policy selected in the 'Route through Gateway' field is the static routing policy that is applicable only if more then one gateway is defined and used for load balancing. limit access to available services.
Network/Host	Specify source and destination host or network address to which the rule applies. Host dropdown list also displays MAC based host and dynamic hosts and host groups which are automatically added on creation of VPN Remote Access connections(IPSec and SSL). It will also display the default hosts created for Remote Access connection - ##ALL_RW, ##ALL_IPSEC_RW, ##ALL_SSLVPN_RW You can define new IP host, MAC host, host group and virtual host directly from the firewall rule itself.
Service/Service group	Services represent types of Internet data transmitted via particular protocols or applications. Select service/service group to which the rule applies. If Virtual host is selected as Destination host, you will be able to configure services only if the selected virtual host is not port forwarded. You can directly add custom service or service group from firewall rule itself. Protect by configuring rules to block services at specific zone limit some or all users from accessing certain services allow only specific user to communicate using specific service
Schedule	Select Schedule for the rule
Action	Select rule action Accept – Allow access Drop – Silently discards Reject – Denies access and 'ICMP port unreachable' message will be sent to the source When sending response it might be possible that response is sent using a different interface than the one on which request was received. This may happen depending on the Routing configuration done on Cyberoam. For example,

	If the request is received on the LAN port using a spoofed IP address (public IP address or the IP address not in the LAN zone network) and specific route is not defined, Cyberoam will send a response to these hosts using default route. Hence, response will be sent through the WAN port.
Apply NAT (Only if Action is 'ACCEPT')	Select the NAT policy to be applied It allows access but after changing source IP address i.e. source IP address is substituted by the IP address specified in the NAT policy. This option is not available if Cyberoam is deployed as Bridge

Advanced Settings

Toggle Drill Down icon – Click to apply different protection settings to the traffic controlled by firewall. You can:

Enable load balancing and failover when multiple links are configured. Applicable only if Destination Zone is WAN

Configure antivirus protection and spam filtering for SMTP, IMAP, POP3, and HTTP policies. To apply antivirus protection and spam filtering, you need to subscribe for Gateway Anti Virus and Gateway Anti Spam modules individually. Refer to Licensing section for details.

- Implement Intrusion Prevention System. To apply IPS policy you need to subscribe for Intrusion Prevention System module. Refer to Licensing section for details.
- Configure content filtering policies. To apply content filtering you need to subscribe for Web and Application Filter module. Refer to Licensing section for details.

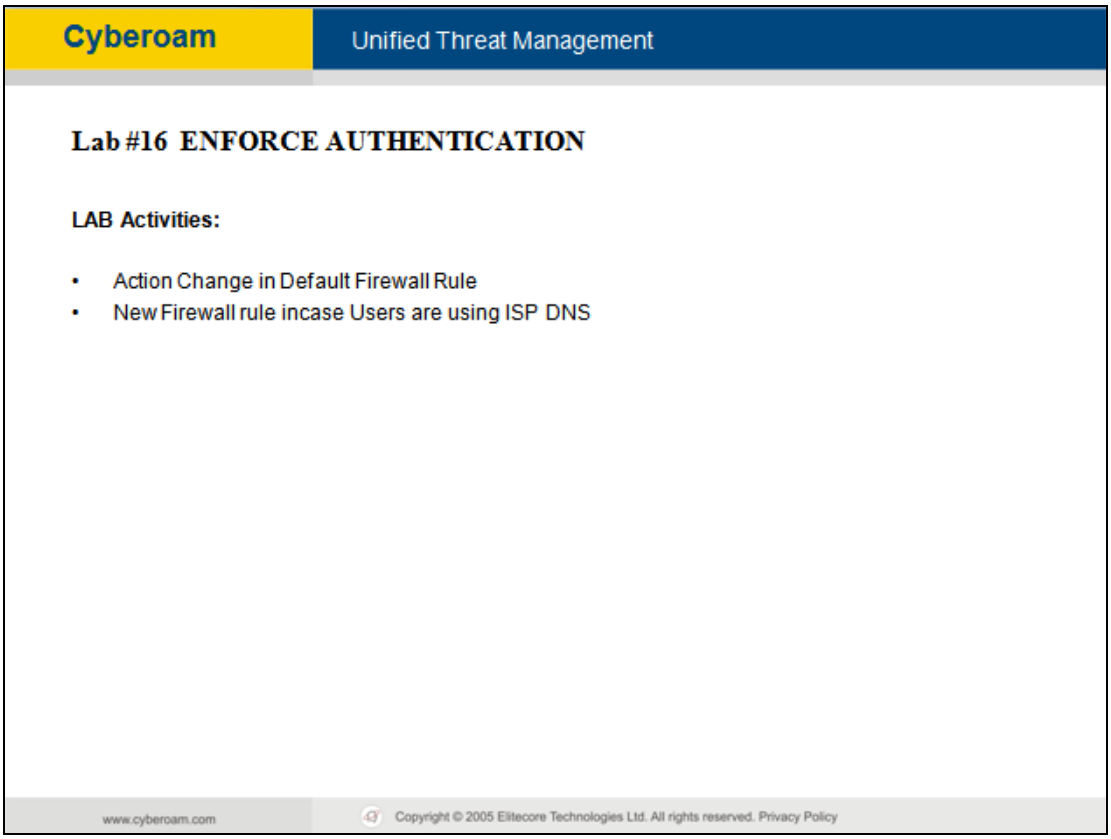
Apply QoS policy

Security Policies

Web filter policy	Select web filter policy for the rule. One can apply web filter policy on LAN to WAN rule only. It controls web access control and block access to inappropriate web sites.
Apply Web Category Based QoS Policy	Click to restrict bandwidth for the URLs categorized under the Web category. A three step configuration is required as follows: Create QoS policy from menu item "QoS → Policy → Add" Assign above created QoS policy to the Web category from menu item "Web Filter → Category". Policy can be assigned to the default as well as custom web categories. Enable "Web Category based QoS Policy" from Firewall rule

	Above configured policy will be applicable, whenever the URL falling under the Web category is accessed.
Application filter policy	Select Web & Application Policy for the rule. One can apply policy on LAN to WAN rule only. It controls access to application like IM and P2P, VOIP.
IPS Policy	Select IPS policy for the rule. To use IPS, you have to subscribe for the module. Refer to Licensing for more details.
IM Scanning	Click 'IM Scanning' Checkbox to enable IM scanning. If enabled, all the messaging applications' traffic is scanned.
AV & AS scanning	Click the protocol for which the virus and spam scanning is to be enabled By default, HTTP scanning is enabled. To implement Anti Virus and Anti Spam scanning, you have to subscribe for the Gateway Anti Virus and Anti Spam modules individually. Refer to Licensing for more details.
QoS and Routing policy	
QoS Policy	Select QoS policy for the rule. Only the Firewall Rule based QoS policy can be applied. QoS policy allocates & limits the maximum bandwidth usage of the user.
Route Through Gateway	Select routing policy. Option is available only if more than one gateway is configured.  This option is not available if Cyberoam is deployed as Bridge
Backup Gateway	Specify the backup gateway. The traffic will be routed through the configured gateway incase gateway configured in "Route Through Gateway" goes down.  This Option is available only if "Load Balance" is not selected for "Route Through Gateway"
Log Traffic	
Log Traffic	Click to enable traffic logging for the rule i.e. traffic permitted and denied by the firewall rule.
Description	Specify full description of the rule

Lab #14 Enforce Authentication



Lab #14 ENFORCE AUTHENTICATION

Lab Activities:

- Action Change in Default Firewall Rule
- New Firewall rule in case Users are using ISP DNS

Objective:

- With Cyberoam being an identity based appliance only authenticated user's needs to be allowed to access the Web resources. This practical lab enforces the HTTP authentication page to the users who are not authenticated with Cyberoam and requires access to web resources.

Lab #14 ENFORCE AUTHENTICATION (Activity#1 Action Change in Default Firewall Rule)

Go to Firewall -- > Rule

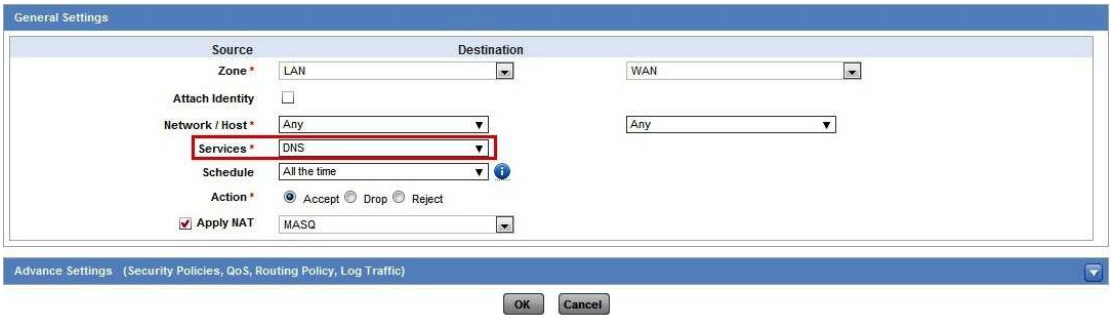
Edit the Default rule no. 1 -- > Make the action as Drop instead of Accept/Reject -- > Save the Firewall rule.

Lab #14 ENFORCE AUTHENTICATION
(Activity#2 New Firewall rule in case Users are using ISP DNS)

In case users in the internal network are using Cyberoam as DNS then there is no need to create this Firewall rule to allow the DNS Traffic. This Firewall rule is only required if users in Internal network are using ISP/Public DNS in their System for name resolving.

Note: Cyberoam forces authentication page only for HTTP traffic, and that's the reason DNS traffic needs to be allowed unauthenticated.

Got to Firewall -- > Rule -- > Add



Lab #15 How to Authenticate users through HTTP Login Page / Cyberoam Corporate Client (client.exe)

Lab Activities:

- Allow authentication on the Cyberoam Interface
- Authenticating the user with HTTP Login Page
- Authenticating the user with Cyberoam Corporate Client (client.exe)

Objective:

- This practical lab will explain the different method of authenticating the users with Cyberoam in case SSO is not configured. Users can authenticate themselves with Cyberoam by any of the method as per the choice.

Lab #15 How to Authenticate users through HTTP Login Page / Cyberoam Corporate Client (client.exe) (Activity#1 Allow authentication on the Cyberoam Interface)

Go to Firewall -- > Local ACL -- > Check the Authentication services

Zone	Admin Services				Authentication Services		Network Services		Other Services	
	HTTP	HTTPS	Telnet	SSH	Windows/Linux Client	Captive Portal	DNS	Ping	Web Proxy	SSL VPN
LAN	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

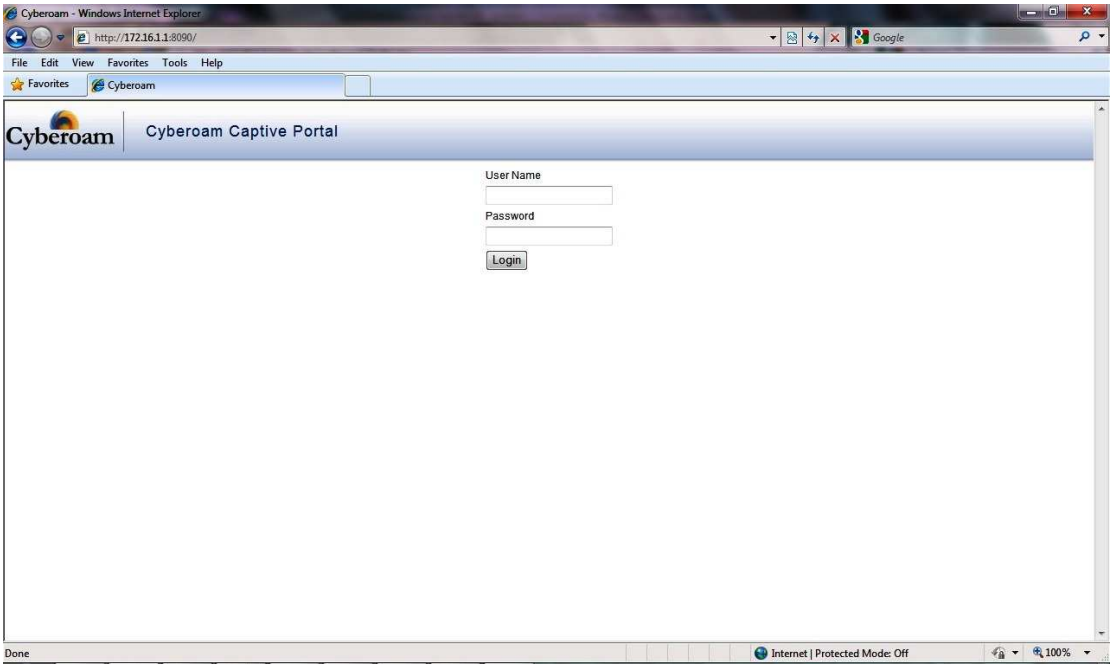
Similarly it needs to be checked for DMZ users.

Lab #15 How to Authenticate users through HTTP Login Page / Cyberoam Corporate Client (client.exe)
(Activity#2. Authenticating the user with HTTP Login Page)

If users are using Cyberoam as DNS and Default rule no. 1 has the action as “Drop”, or users are using ISP DNS and Firewall rule is created to allow the DNS traffic unauthenticated to Internet, then in both these scenarios, the HTTP login page will automatically popup asking for credentials.

Note: Please follow the Lab#16 for more details about the configuration for getting the HTTP login page automatically popup.

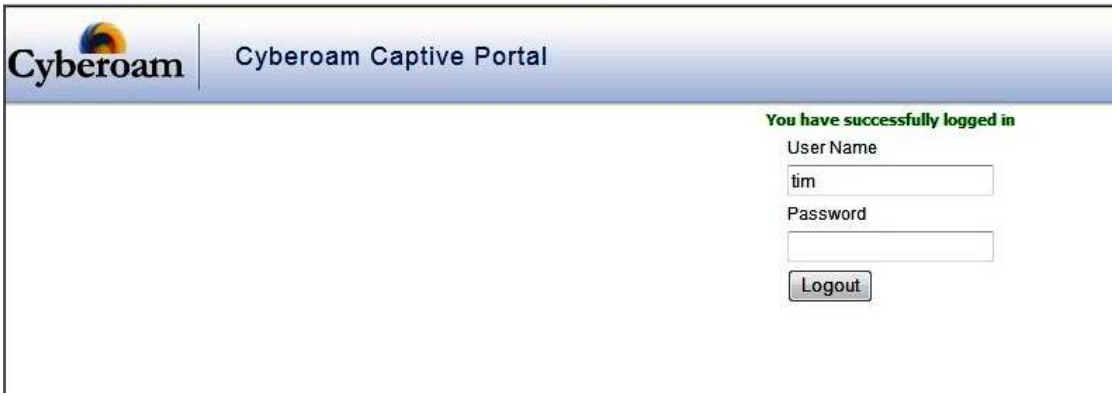
Cyberoam will give the HTTP login page in case user is not authenticated and trying to access the web resources.



Alternatively, users can open the HTTP login page in their browser for authentication purpose, if for some reason the HTTP Login page doesn’t popup.

Open the web browser and type http://Cyberoam-ip:8090 i.e. http://172.16.1.1:8090

Note: HTTP login page works over TCP/8090.

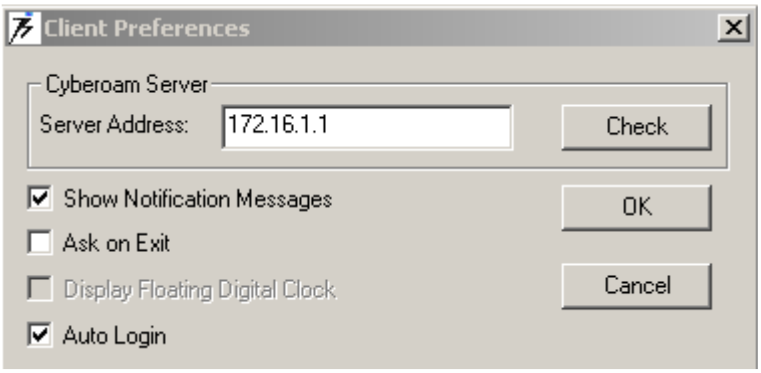


Once logged on to the HTTP login page, don't close this window and keep it upon until the time you want to do the web browsing.

Lab #15 How to Authenticate users through HTTP Login Page / Cyberoam Corporate Client (client.exe)
(Activity#3 Authenticating the user with Cyberoam Corporate Client)

The Cyberoam corporate client can be downloaded from the Cyberoam website http://www.cyberoam.com/cyberoamclients.html

Once installed, it will be available in windows Program menu and can be minimised in Task bar. Right Click on the  and click on preferences and configured the IP address of Cyberoam as Server address.



After configuration, log on with the users credentials to access the web resources.

Lab #16 Create Custom Policies

Lab #16 Create Custom Policies

Lab Activities:

- Create Time Schedule
- Create Surfing Quota policy
- Create Access Time Policy
- Create Internet Access Policy
- Create Bandwidth Policy

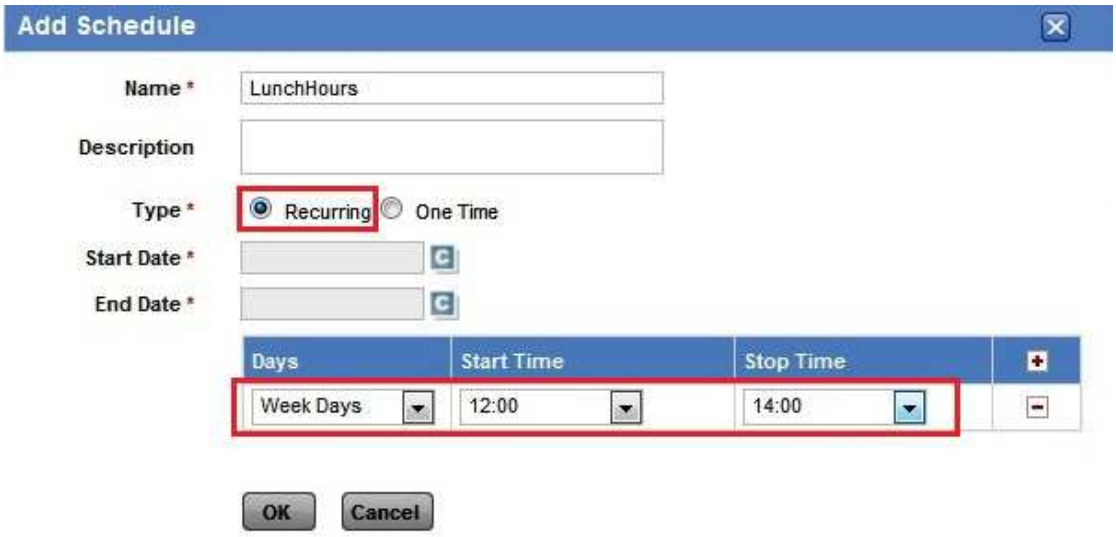
- Create Data Transfer Policy

Objective:

- This practical lab will explain the different policies which can be applied to the individual user / groups.

Lab #16 Create Custom Policies
(Activity #1 Create Time Schedule)

Go to Objects -- > Schedule -- > Add



Types of Schedules:
• Recurring – use to create policies that are effective only at the specified times of the day or on specified days of the week.

• One-time - use to create firewall rules/policies that are effective once for the period of time specified in the schedule.

Schedule is all days of week and between 12:00-1400. Add the schedule and Save it.

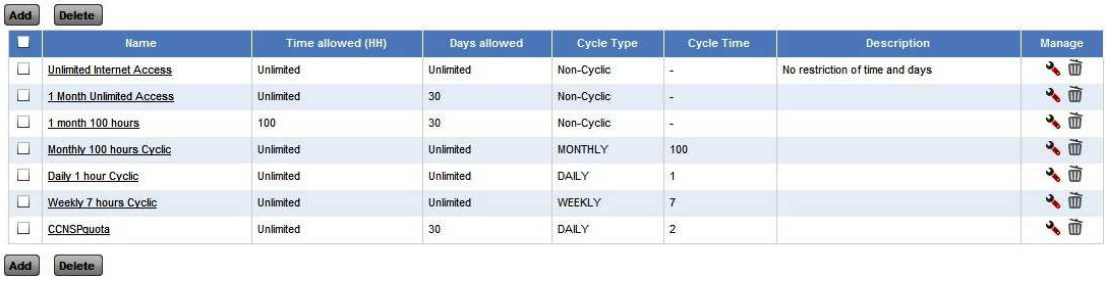
Lab #16 Create Custom Policies
(Activity #2 Create Surfing Quota Policy)

Go to Identity → Policy → Surfing Quota → Add

Surfing quota policy:

- Allocates Internet access time on cyclic or non-cyclic basis
- Single policy can be applied to number of Groups or Users

Surfing Quota is defined as Cyclic 2 hrs a day for next 30 days.



Lab #16 Create Custom Policies
(Activity #3 Create Access Time Policy)

Go to Identity → Policies -- > Access Time → Add

Access time policy strategies:

Allow strategy - By default, allows access during the schedule
Deny strategy - By default, disallows access during the schedule

Schedule is selected between 12:00-14:00 with strategy as allow to provide the web resources access. Before 12:00 and after 14:00, web resources will not be available to the user.

Lab #16 Create Custom Policies
(Activity #4a Create Web Filter Policy)

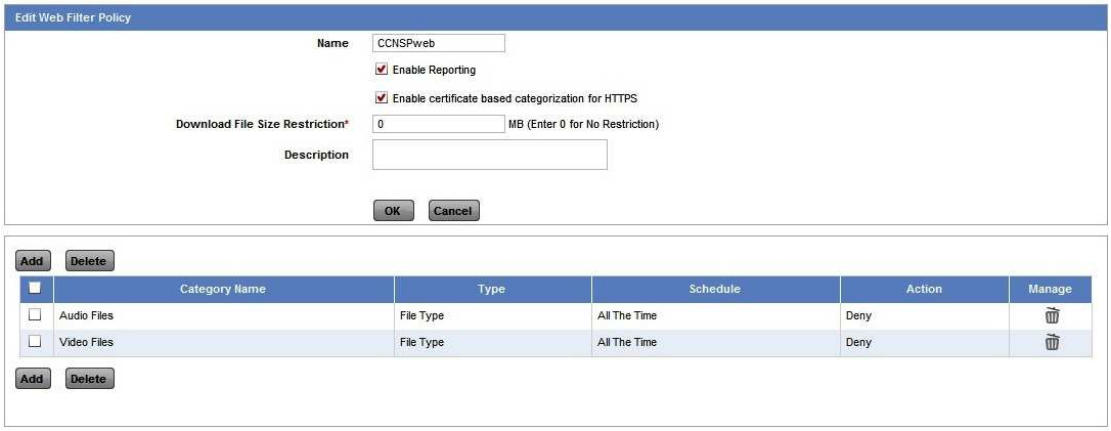
Go to Web Filter → Policy → Add

Policy types:

• Allow - By default, allows user to view everything except the sites and files specified in the web categories. E.g. To allow access to all sites except Mail sites
• Deny - By default, prevents user from viewing everything except the sites and files specified in the web categories. E.g. To disallow access to all sites except certain sites

It is not possible to allow Application categories in "Deny All" policy

HTTPS Categorisation is checked. It can be unchecked if you don't want the HTTPS based sites to be categorised.



Internet access policy is selected where Web based Email, Video and Audio Files, All Chat applications, P2P applications and Streaming media is not allowed all time during the day.

(Activity #4b Create Application Filter Policy)

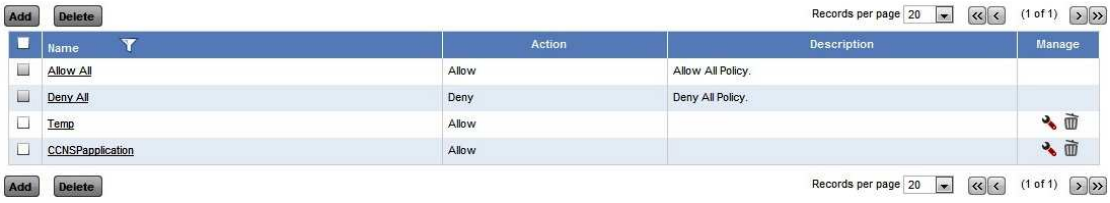
Go to Application Filter → Policy → Add

Press OK to create the custom policy.

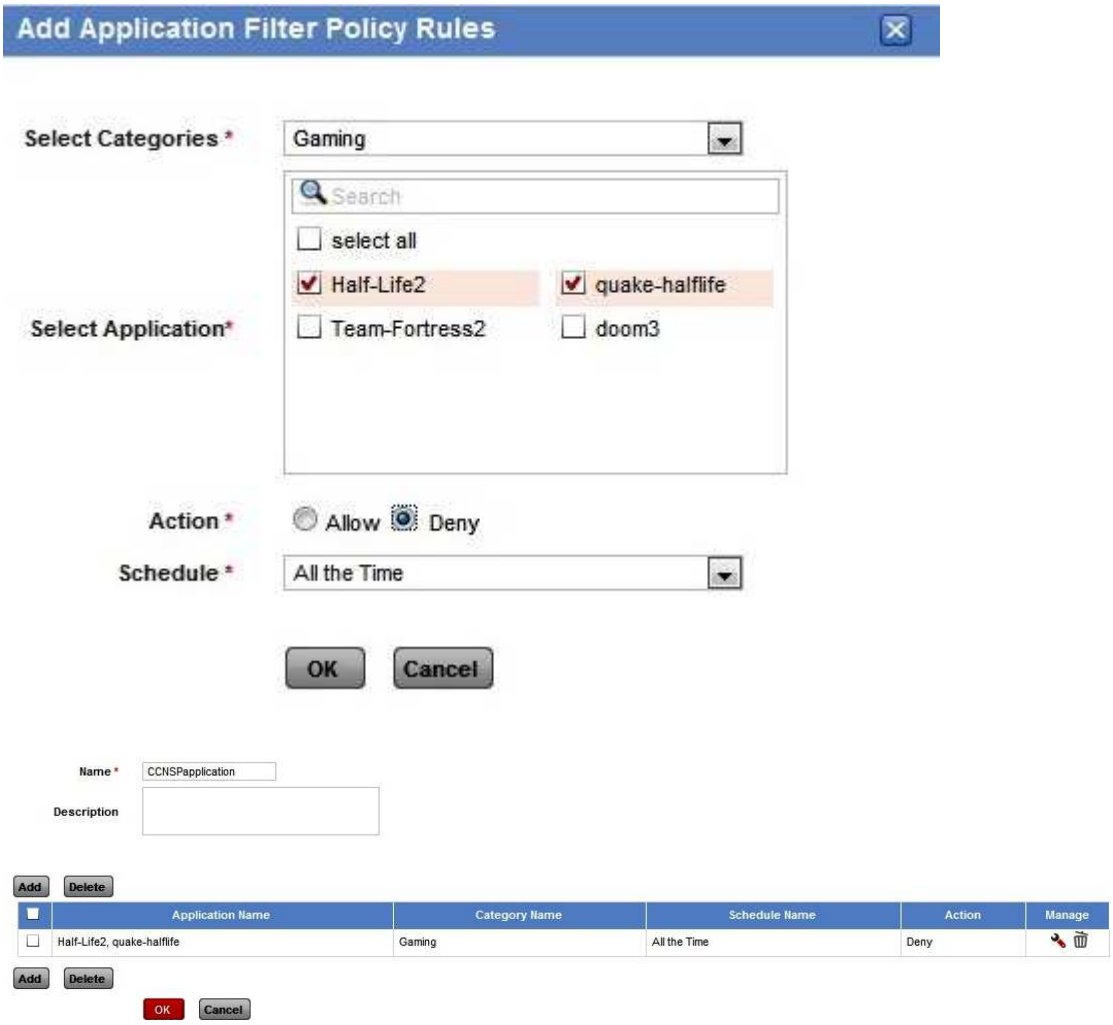
Two strategies based on which Application Filter Policy can be defined:

Allow: By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.

Deny: By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.



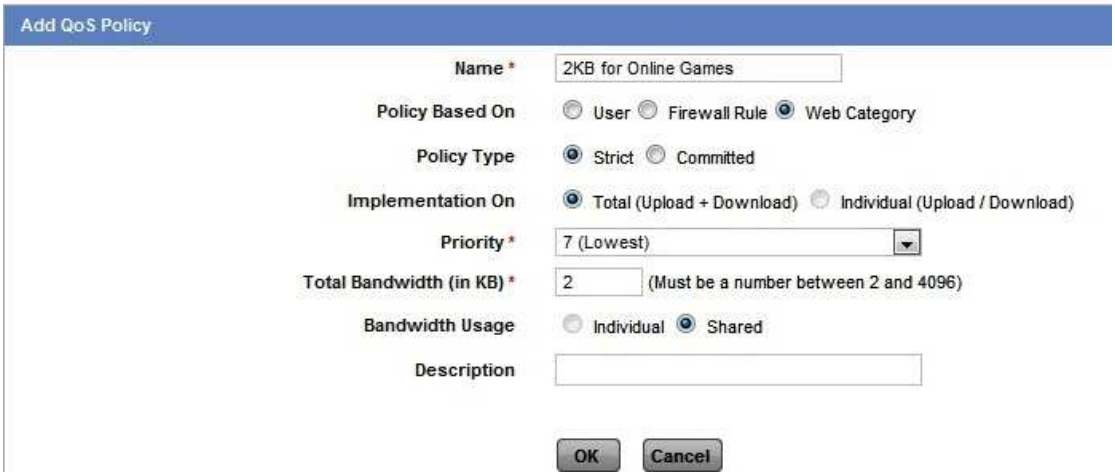
Click on the policy to edit and add the categories to deny.


Add Application Filter Policy Rules
Select Categories *
Gaming
Search
select all
Half-Life2
quake-halflife
Select Application*
Team-Fortress2
doom3
Action *
Allow
Deny
Schedule *
All the Time
OK
Cancel
Name *
CCNSPapplication
Description
Add
Delete
Application Name
Category Name
Schedule Name
Action
Manage
Half-Life2, quake-halflife
Gaming
All the Time
Deny
Add
Delete
OK
Cancel

Lab #16 Create Custom Policies
(Activity #5 Create QoS Policy)

Go to QoS → Policy → Add

Create a QoS Policy with strict bandwidth of 2KB for online games



Policy can be defined/created for:

- **Web Category** – It restricts the bandwidth for the URL categorized under the Web category. To implement restriction, policy is to be assigned through firewall rule.
- **User -** It restricts the bandwidth of a particular user.
- **Firewall Rule -** It restricts the bandwidth of any entity to which the firewall rule is applied.

There are two types of bandwidth restriction

- Strict - In this type of restriction, user cannot exceed the defined bandwidth limit.
- Committed - In this type of restriction, user is allocated the guaranteed amount of bandwidth and user can draw bandwidth up to the defined burstable limit, if available.

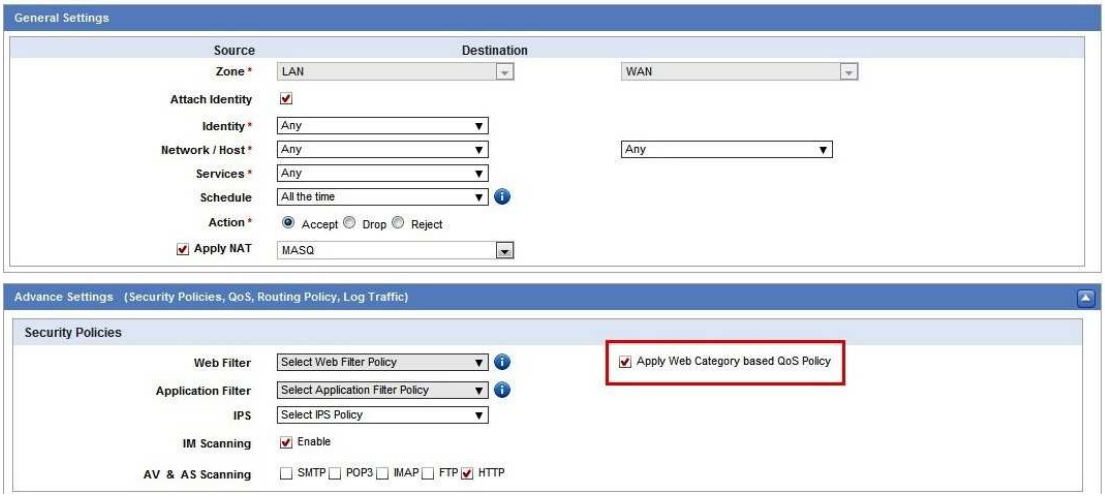
Priority – 8 different priority levels can be selected for the user with 0 being the highest and 7 being the lowest priority.

Bandwidth can be assigned to individual or shared level.

Create an Online Games web category and apply the QoS Policy of 2KB to it.

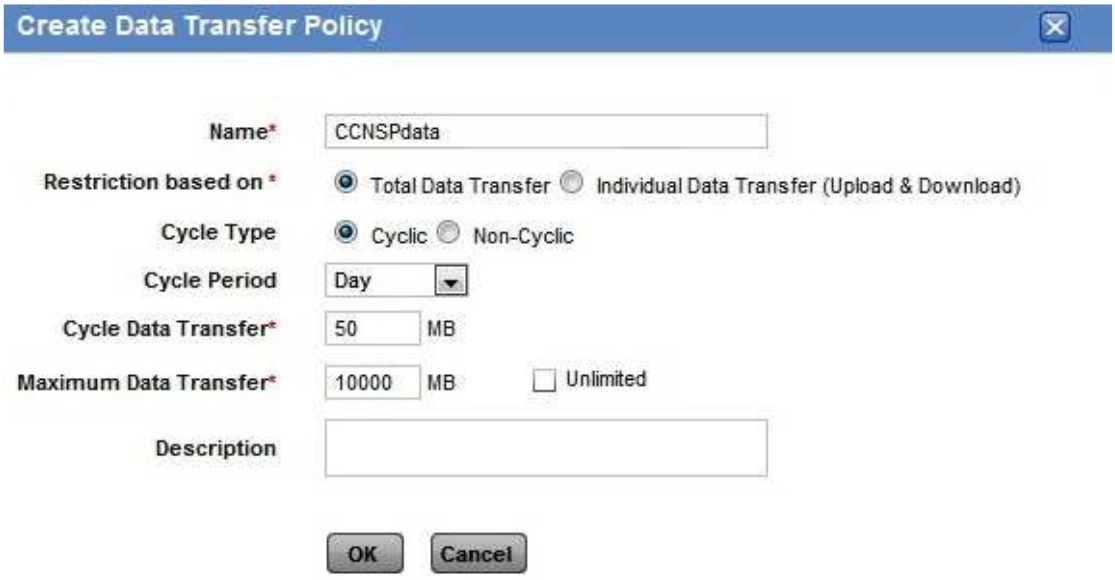
To create a custom web category, go to Web Filter → Category → Add

Now apply the policy of all internal users in LAN



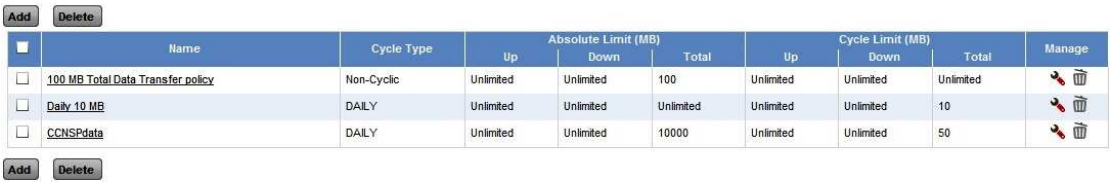
Lab #16 Create Custom Policies
(Activity #6 Create Data Transfer Policy)

Go to Identity → Policy → Data Transfer



Data transfer policy:

- Limits data transfer on a cyclic or non-cyclic basis.
- Single policy can be applied to number of Groups or Users.



Data Transfer is configured for the user with maximum allowed limit of 50MB per day till it reaches 10000 MB.

Lab #17 Create Group, User and apply Custom Policies

Lab Activities:

- Create Normal Group
- Create Normal User
- Place User in Newly Created Group
- Assign all the 5 Policies to the Group Level

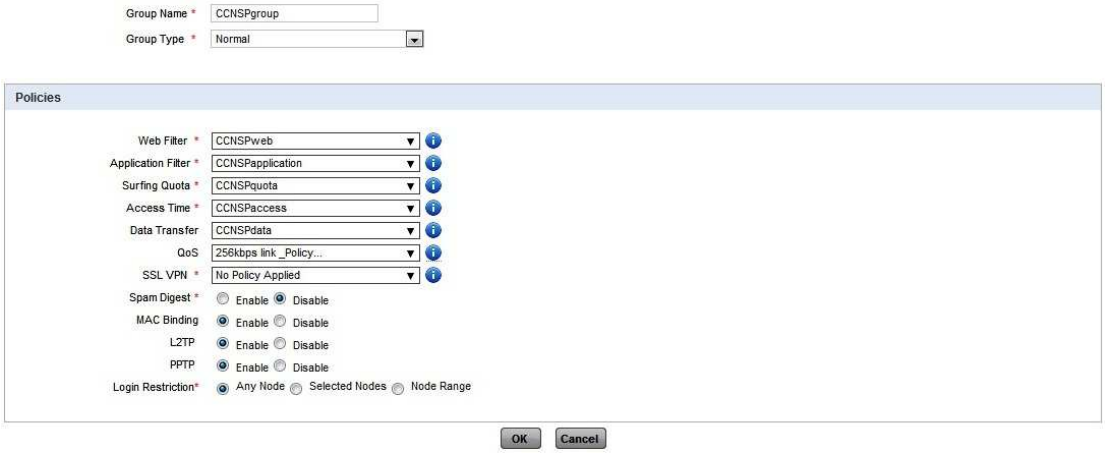
Objective:

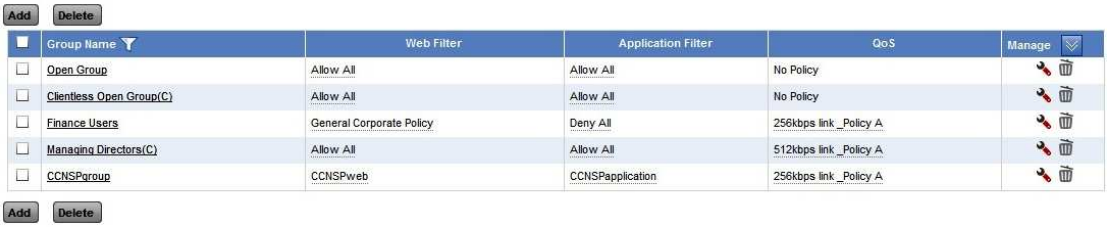
- This practical lab will explain the Creation of Group, Users and how to assign policies at Group/user Level.

Lab #17 Create Group, User and apply Custom Policies
(Activity #1 Create Normal Group)

Go to Identity → User → User Group → Add

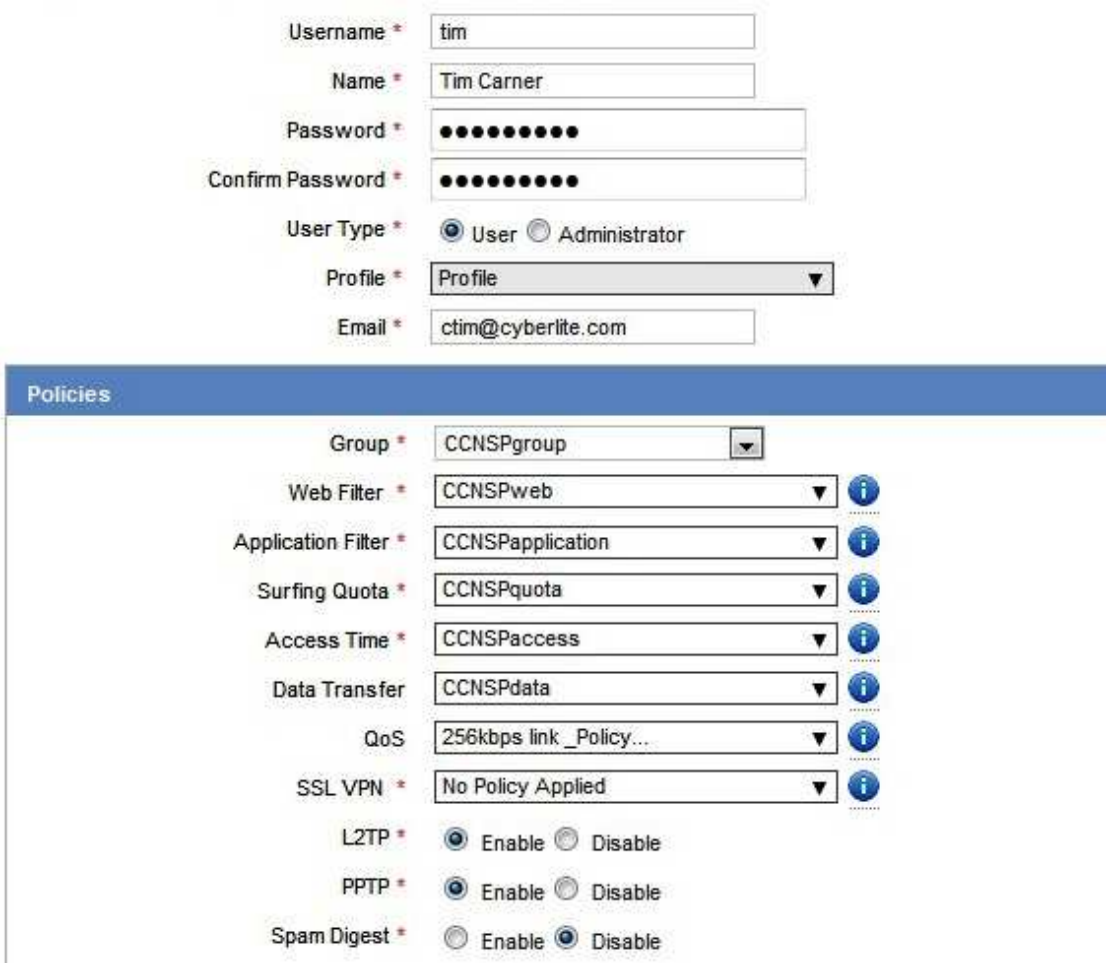
We can use all the policies (Created in LAB#18), and apply to the group level.





Lab #17 Create Group, User and apply Custom Policies (Activity #2 Create Normal User)

Go to Identity -- > User -- > Add



Normal user is created and placed in the group (Created in the last activity Lab#19-Activity#1).

Lab #18 Monitor User Activities

Lab Activities:

- Check Manage Live Users
- Check Reporting Section

Objective:

- This practical lab will explain the monitoring of user activities who authenticated with Cyberoam.

Lab #18 Monitor User Activities
(Activity #1 Check Manage Live Users)

Go to Identity → Live User

Use Live users page to

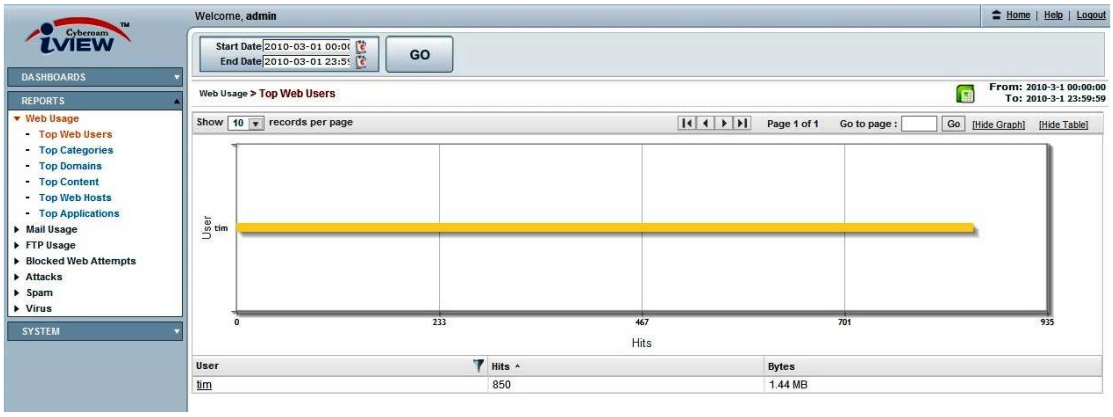
- view list of all the currently logged on Users
- modify user details
- send message to any live user
- disconnect any live user

Report Columns	Description
Concurrent Sessions	Displays currently connected total users (Normal, Clientless, and Single sign on client Users)
Current System time	Displays current system time in the format - Day, Month Date,HH:MM
ID and User name Click to change the display order	Displays ID and name with which user has logged in Click User name link to View/Update user details
Name	Displays User name Click Name link to view Group and policies details attached to the User
Connected from Click to change the display order	Displays IP address of the machine from which user has logged in
Public IP	Displays Public IP address if User has logged in using public IP address
Start time Click to change the display order	Displays login time
Time (HH:mm)	Displays total time used in hours and minutes
Upload Data transfer Click to change the display order	Displays Data uploaded
Download Data transfer Click to change the display order	Displays Data downloaded
Bandwidth (bits/sec)	Displays Bandwidth used
Select	Select User for sending message or disconnecting More than one User can be selected
Send Message button	Sends message to the selected User(s)
Disconnect button	Disconnects the selected User(s)

Table – Manage Live User screen elements

Lab #18 Monitor User Activities
(Activity #2 Check On-Appliance Reporting Section)

Go to Logs & Reports → View Reports, iView will open. Provide admin username and admin password, and see the usage reports by user.



Lab #19 Single Sign On Implementation with Active Directory (Optional)

Lab #19 Single Sign on Implementation with Active Directory (Optional)

Lab Activities:

- Pre-requisites
- Create ADS user groups
- Define Authentication parameters
- Configure Cyberoam to use Active Directory
- Add Domain Query
- Test Active Directory integration
- Single Sign on Implementation
- Checks if SSO is installed properly or not

Objective:

- This practical lab will explain Single Sign on Configuration with Active Directory. After the Setup, there is no need to create any user locally on the Cyberoam and users also need not to authenticate anywhere manually to access the web resources.

Lab #19 Single Sign on Implementation with Active Directory (Activity #1 Pre-requisites)

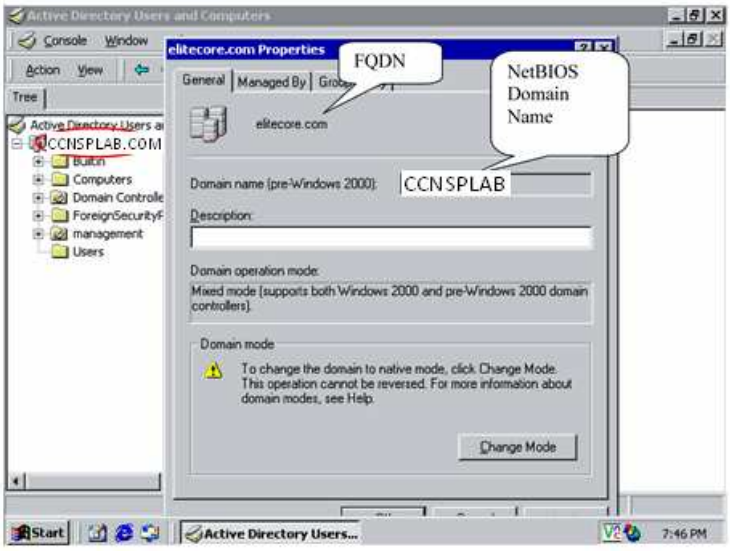
Cyberoam – ADS integration feature allows Cyberoam to map the users and groups from Active Directory for the purpose of authentication.

- NetBIOS Domain name - **CCNSPLAB**
- FQDN Domain name - **CCNSPLAB.COM**
- Search DN - **DC=CCNSPLAB, DC=COM**
- Active Directory Server IP address - **172.16.1.100**
- Administrator Username and Password (Active Directory Domain) – **administrator/admin**
- IP address of Cyberoam Interface connected to Active Directory server Subnet
- Active Directory Groups on the Cyberoam – **172.16.1.1**

Determine NetBIOS Name, FQDN and Search DN

On the ADS server:

- Go to Start>Programs > Administrative Tools > Active Directory Users and Computers
- Right Click the required domain and go to Properties tab
- Search DN will be based on the FQDN. In the given example FQDN is CCNSPLAB.COM and Search DN will be DC=CCNSPLAB, DC=COM



Lab #19 Single Sign on Implementation with Active Directory (Activity #2 Create ADS Groups)

Create ADS user groups

Please check Cyberoam version before you continue as this is version specific step.

All Versions below 9.5.3 build 14

Go to Group> Add Group and create all the ADS user groups

For mapping the ADS user groups with the Cyberoam user groups, create all the ADS user groups into Cyberoam before ADS users log on to Cyberoam for the first time. If the ADS groups are not created in Cyberoam, all the users will be assigned to the Default group of Cyberoam.

If all the ADS user groups are created in Cyberoam before users log on to Cyberoam then user will be automatically created in the respective group when they log on to Cyberoam.

Version 9.5.3.14 or above

Instead of creating groups again in Cyberoam, you can import AD groups into Cyberoam using Import Wizard. One can import groups only after integrating and defining AD parameters into Cyberoam.

Lab #19 Single Sign on Implementation with Active Directory (Activity #3 Define Authentication Settings)

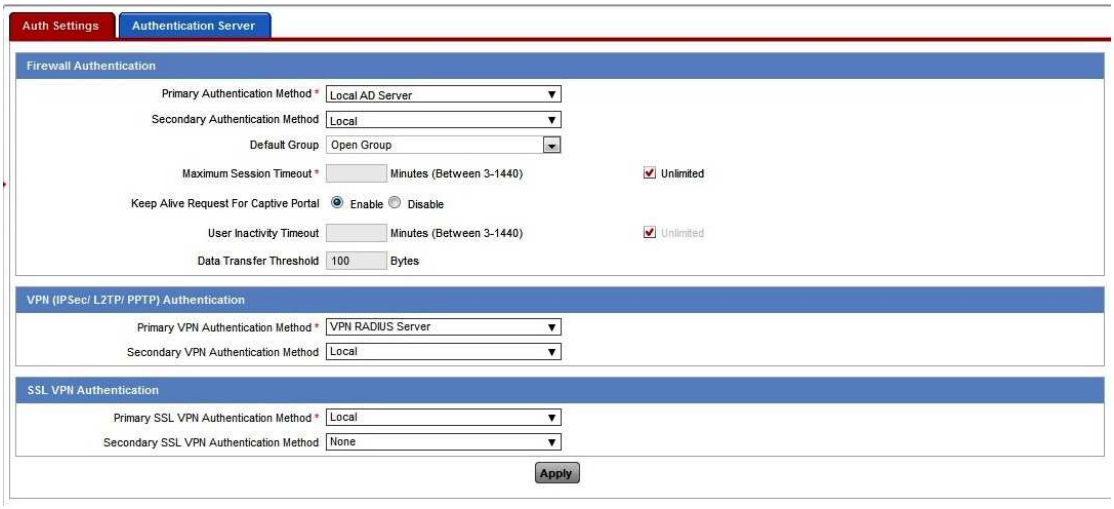
Define Authentication parameters

Go to Identity --> Authentication → Auth Settings

User Authentication process initiates, when the client tries to login with the login credentials. Cyberoam provides an authentication mechanism where in users registered with two different servers can be validated.

Previously, a single authentication was provided to access the firewall rules as well as VPN connections and thus users generally belonged to only a single server. So with multiple authentications, cyberoam allow users from two different servers to have different authentication for Firewall rules and VPN connections. A same server cannot be chosen as primary as well as secondary server but two ADS or LDAP servers can be used for configuration.

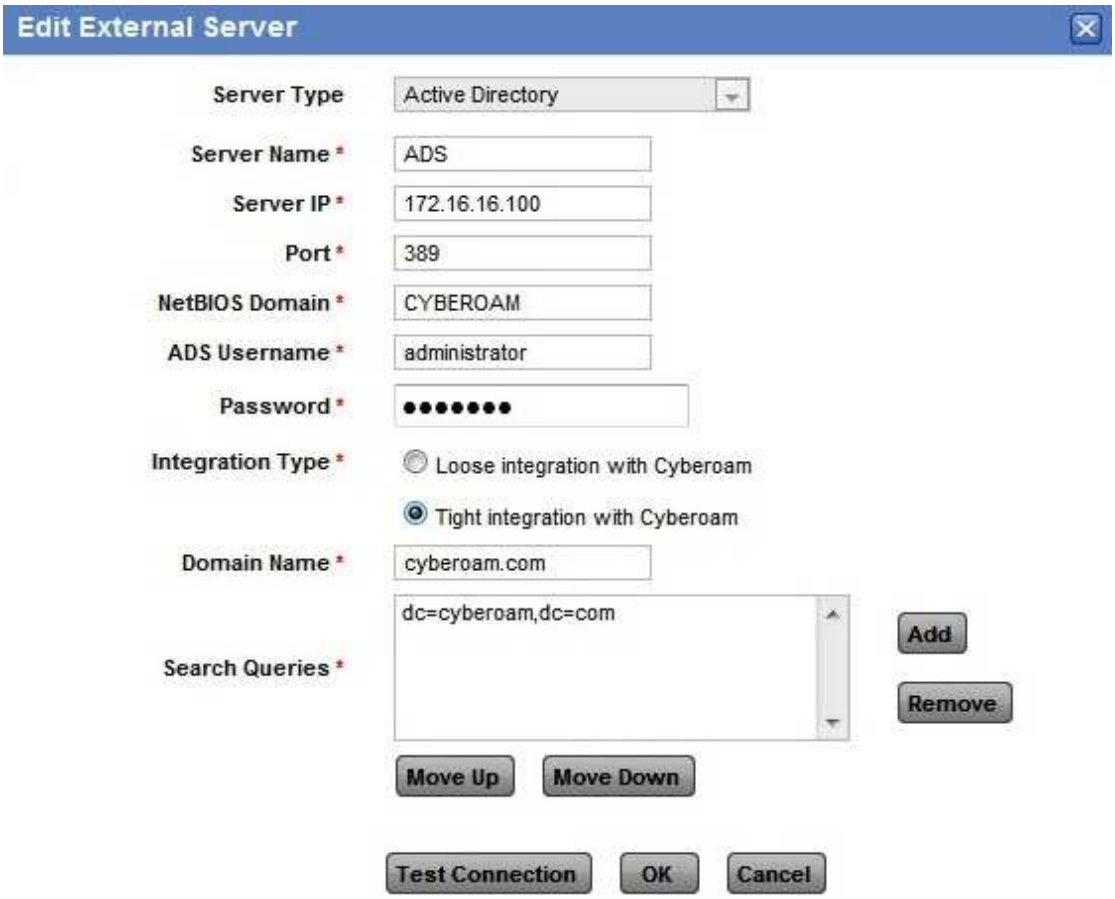
Primary Server	Secondary Server
Local	ADS, LDAP, RADIUS
ADS	Local, ADS, LDAP, RADIUS
LDAP	Local, ADS, LDAP, RADIUS
RADIUS	Local, ADS, LDAP, RADIUS



Lab #19 Single Sign on Implementation with Active Directory (Activity #4 Configure Cyberoam to use Active Directory)

Go to Identity → Authentication → Authentication Server → Add

Click Add to configure Active Directory parameters and Specify IP address of Active Directory.



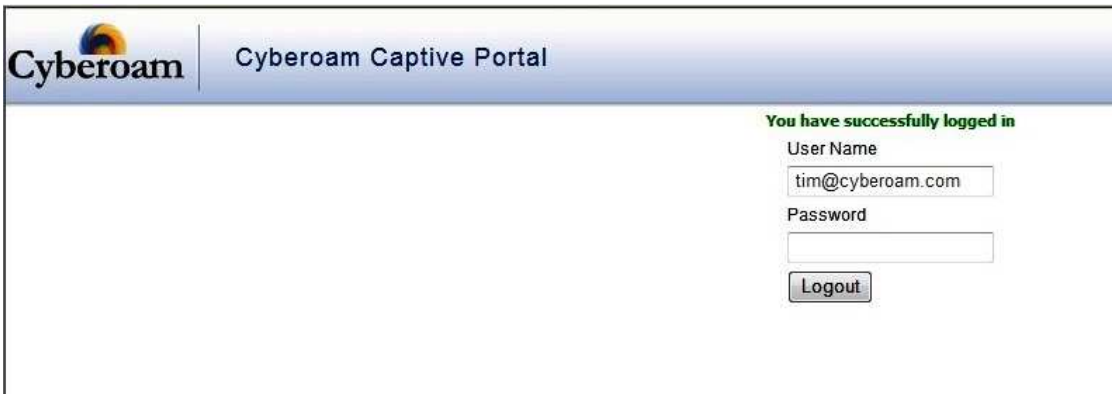
Specify TCP/IP port number in Port field. It is the port on which ADS server listens for the authentication requests. On Cyberoam appliance, the default port for ADS traffic is 389. If your AD server is using another port, specify port number in Port field.

Click “Test Connection” to check whether Cyberoam is able to connect to the Active Directory or not. If Cyberoam is able to connect to the Active Directory, click Add to save the configuration.

Lab #19 Single Sign on Implementation with Active Directory (Activity #5 Test Active Directory integration)

Open the browser and browse to http://cyberoam-IP:8090

The Cyberoam captive portal will open.



Username will be displayed on Identity >User > Live Users page if user is able to log on to Cyberoam successfully.

This completes the AD configuration.

Lab #19 Single Sign on Implementation with Active Directory (Activity #6 Single Sign on Implementation)

Use the following procedure for implementing Single Sign On (SSO) for ADS if the SSO Client is to be installed on Windows 2000, Windows XP or Windows 2003:

Download SSCyberoamAutoSetup.zip from http://cyberoam.com/cyberoamclients.html

Create directory SSOsetup and unzip SSCyberoamAutoSetup.zip.

Following files will be extracted:

1. SSCyberoamSetup.exe
2. SSCyberoamConfigSetup.exe
3. SSCyberoamConfig.ini
4. ElitecoreAdmin.exe
5. ElitecoreRun.exe

Run ElitecoreAdmin.exe to create Admin.ini file to store the user account credentials which has administrative rights (local administrative rights) for all desktop computers. Administrative right is required to run SSCyberoam setup and install Client on the user machine.

Specify username, password, and windows domain name (NetBIOS Domain Name) from where users will log on.

This will create Admin.ini file in the SSOsetup directory.

Admin.ini file is passed as a parameter to Elitecorerun.exe to run SS Cyberoam setup.

Setup your configuration in SSCyberoamConfig.ini file using following syntax:

Domain Name=CCNSPLAB.COM

Server=172.16.1.1
Domain Controller=ADS

Copy following files to “cyberoam” directory under “NETLOGON” of the domain controller:

1. SSCyberoamSetup.exe
2. SSCyberoamConfigSetup.exe
3. SSCyberoamConfig.ini
4. Admin.ini
5. ElitecoreRun.exe

You can access NETLOGON directory using: \\172.16.1.100\netlogon

Configure logon script

Log on script is executed every time user logs on to the local computer. Each user could have an individual log on script or all users could share the same logon script.

Default location of logon script: NETLOGON directory

Update logon script (If logon script is already created)

Edit the existing logon script by using any Text Editor and add the lines specified in the batch at the end of the script.

Batch File:

\\172.16.1.100\netlogon\cyberoam\ElitecoreRun.exe
\\172.16.1.100\netlogon\cyberoam\Admin.ini -c
"\\172.16.1.100\netlogon\cyberoam\SSCyberoamSetup.exe"

\\172.16.1.100\netlogon\cyberoam\ElitecoreRun.exe -p
\\172.16.1.100\netlogon\cyberoam\Admin.ini -c
"\\172.16.1.100\netlogon\cyberoam\SSCyberoamConfigSetup.exe 0
\\172.16.1.100\netlogon\cyberoam\SSCyberoamConfig.ini"

If all users share the common logon script then, you need to update only the common script else you need to update all the scripts created for each user.

Create logon script (If logon script is not already created)

Edit the above batch file in text editor and save as “cyberoam.bat” in the NETLOGON directory

Define logon script - cyberoam.bat as a default logon script for all the users using following method:

Log on to Cyberoam Web Admin Console

Go to User -> Migrate Users and click "User Logon Script Updation Utility" from to download updatelogonscript.bat file

Execute this script file from the domain controller itself or any other machine which is part of the domain as follows: updatelogonscript.bat cyberoam.bat

Please note you will require administrative privilege to run the script

When the user logs on for the first time after the above configuration, logon script runs SSCyberoamSetup.exe and installs Cyberoam Single Sign On Client (Cyberoam SSO Client) on the user machine. Cyberoam will authenticate user based on the details specified in SSCyberoamConfig.ini and Windows username.

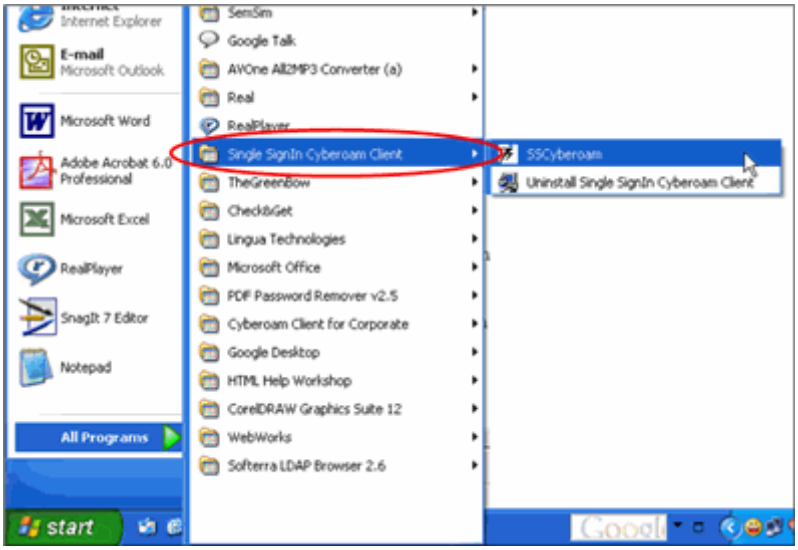
Note:

On every log on attempt, SSCyberoamSetup.exe is executed which installs Cyberoam SSO Client if Client is not available on user machine.

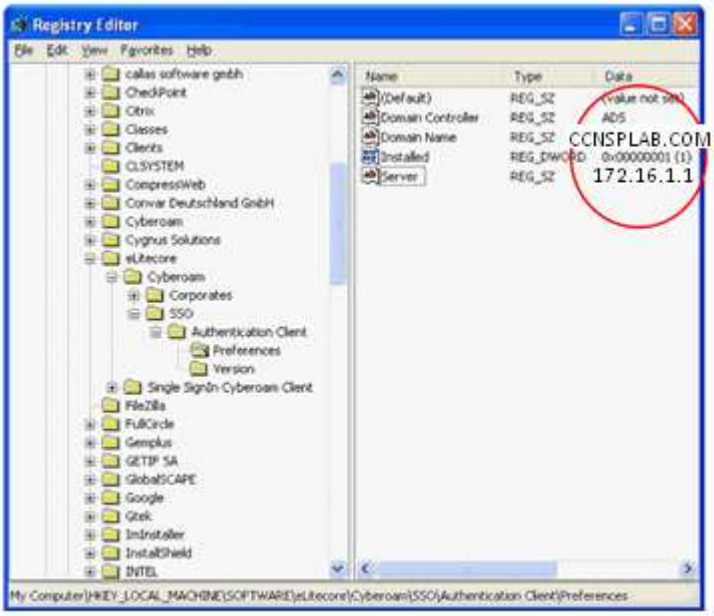
Lab #19 Single Sign on Implementation with Active Directory (Activity #7 Checks if SSO is installed properly or not)

Check whether Cyberoam SSO Client is installed and configured properly from any of the local machine.

a) Check for “Single SignIn Cyberoam Client” folder from Start Programs. If client is installed properly, Single SignIn Cyberoam Client folder will be created.



b) Check SSO version and server IP address from HKEY_LOCAL_MACHINE/SOFTWARE/eLitecore/Cyberoam of the registry of the local machine.



Lab #20 Customise Cyberoam Captive Portal

Lab Activities:

- How to Customise the page

Objective:

- This practical lab will explain you the customization of HTTP Client login page.

Lab #20 Customise Cyberoam Captive Portal
(Activity #1 How to Customise the login page)

Cyberoam provides flexibility to customise the HTTP Client Login page. This page can include your organisation name and logo.

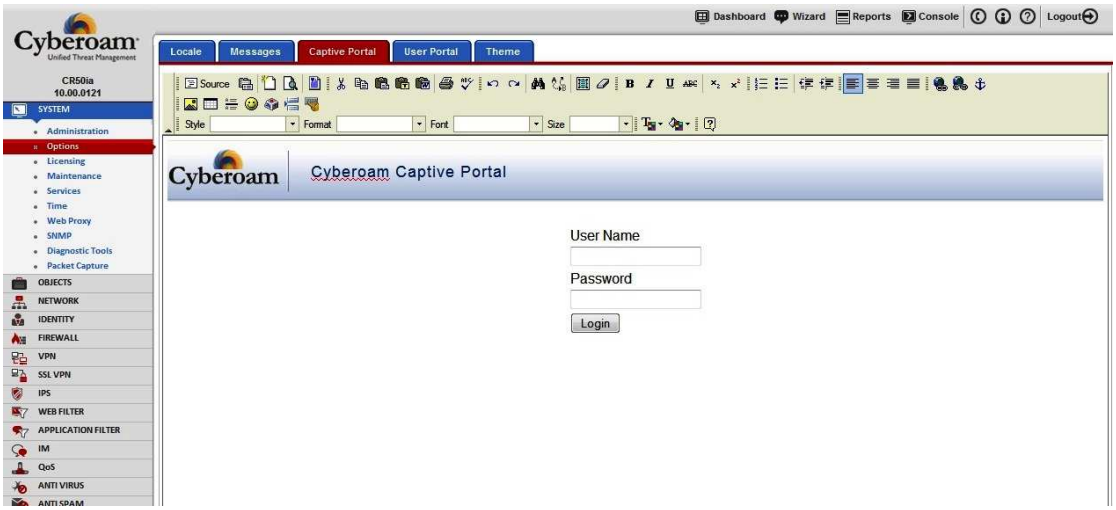
Cyberoam has included a fully integrated Template Editor to design the page. It supports numerous placement and arrangement options for each field and a provision to add a personalized message or inserting logo or any other image.

Cyberoam also supports Customised page in languages other than English.

Cyberoam provides a default template that can be modified to customise the HTTP Client login page.

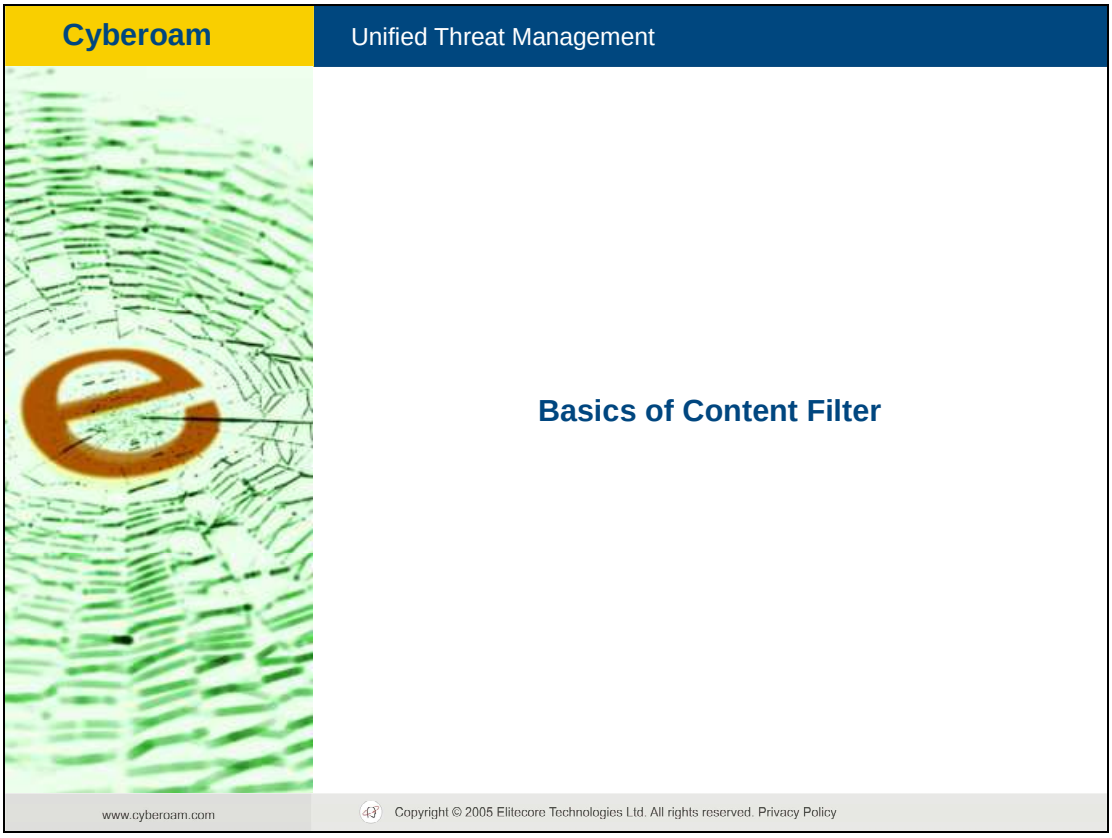
Go to System -- > Options -- > Captive Portal

Before Editing:



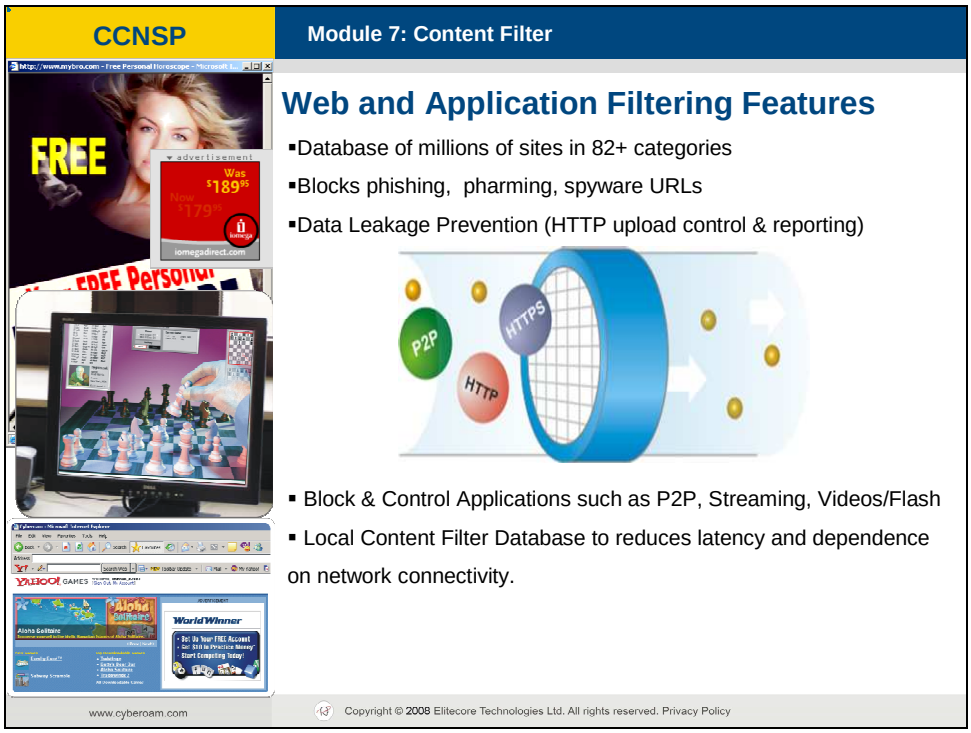
After Editing:

Module 7: Content Filter



Basics of Content Filter

In today's competitive business, everyone relies on the Web for access to information and resources. As the Web is continuously and increasingly being used as a source of variety of attacks, using rapidly evolving and dynamic interactive web applications, enterprises face heavy financial damage as it leads to entry of viruses, malware, worms, Trojans, spyware, and more through malicious websites. Phishing, pharming and spyware may lead to theft of passwords, identity theft and loss of other confidential information. Indiscriminate Internet surfing by internal users leaves enterprises vulnerable to legal liabilities, besides loss of productivity. Unrestricted use of file-sharing applications like IM and P2P and multimedia downloads cause risk of data loss or leakage as well as bandwidth choking, draining the enterprise resources. The answer to this is a Comprehensive Content Filtering Solution that determines what content will be available on a particular machine or network. The motive is often to prevent persons from viewing content which the computer's owner(s) or the authorities may consider objectionable. This results in increased productivity of the employees, prevents loss of confidential data and reduce legal liabilities for the business.



Cyberoam Content Filter Features

The web content filtering solution offered by Cyberoam is based on a combination of categories, keywords, URLs, domain names and file types, making it a comprehensive filtering mechanism. Cyberoam Content Filtering is Checkmark certified service. It offers comprehensive protection to enterprises against spyware, pharming, phishing, malicious site content and much more with its internet content filtering solution. Cyberoam's internet content filtering solution plays a critical role in ensuring CIPA certification to school districts and libraries.

Comprehensive Site Database

Cyberoam delivers dependable content filtering through WebCat, Cyberoam's web Categorisation engine. With a comprehensive database of millions of region-specific popular sites across the globe, grouped in 82+ categories, it delivers great dependability. The comprehensive database ensures the safety and security of minors' online, supporting CIPA compliance for schools and libraries.

HTTPS URL Filtering

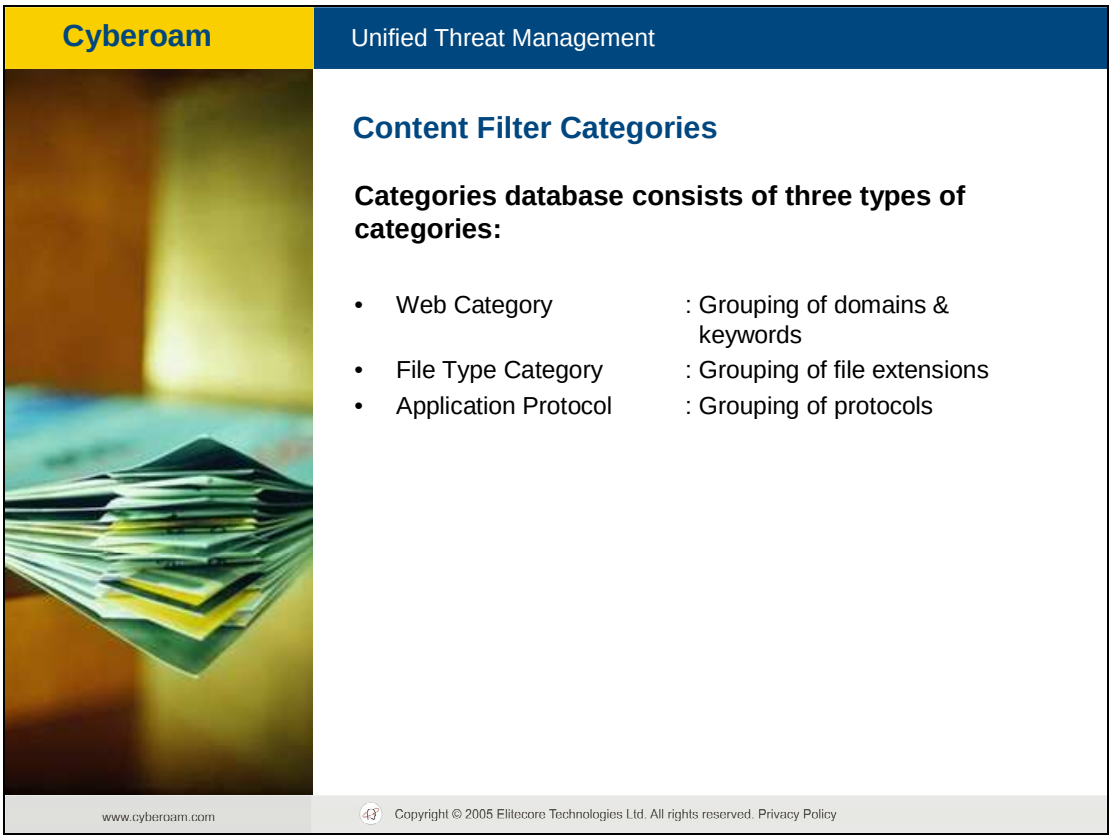
Cyberoam can also control access to websites hosted over HTTPS by categorising the domain names using the comprehensive website database. This feature helps the administrator to block access to unauthorised and unsafe websites like anonymous proxies and malware hosting websites, hosted over HTTPS.

Granular Control

Cyberoam breaks free from static IP-based and blanket policies with its granular, user-identity based policy capabilities to apply pre-defined surfing policies to any user, anywhere in the network. Enterprises can define and apply user, group and application based policies by hierarchy, department or any combination with access restriction to certain sites during specific time of the day.

Application Filtering

Cyberoam's surfing security extends beyond standard web traffic to include applications like IMs (Instant Messaging) including Yahoo, MSN, AOL, Skype as well as P2P (peer to peer) exchanges. It offers a complete view and user based controls to match the dynamic threat scenario.



Web Filter Categories

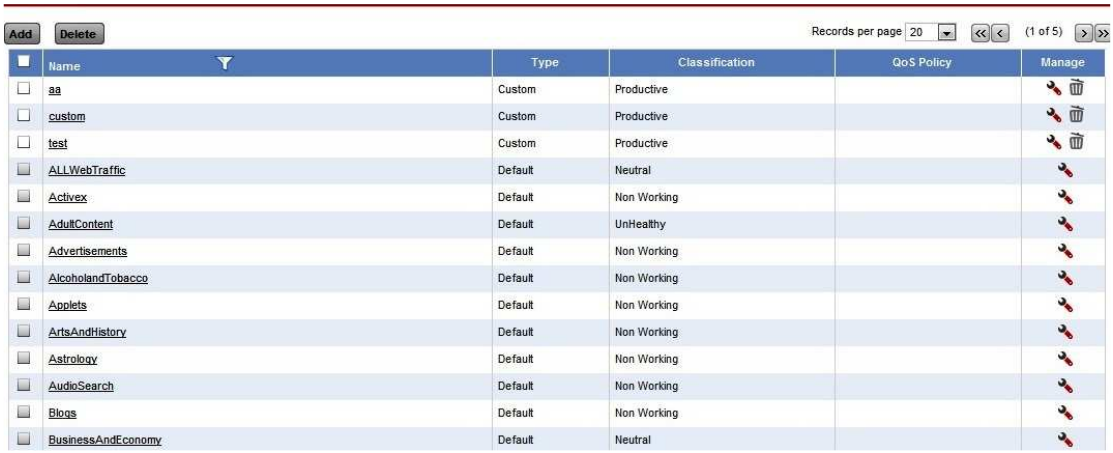
Web Filter in Cyberoam consists of two categories: Web Category and File Type Category. Both category types have default categories defined, and we can create Custom categories as well.

Web Category

Web category is a group of Domains and URL keywords used for Internet site filtering. Cyberoam has 82+ default categories enabling to filter more than 40 million URLs. Each category is grouped according to the type of sites.

The below screen shot displays the default categories:

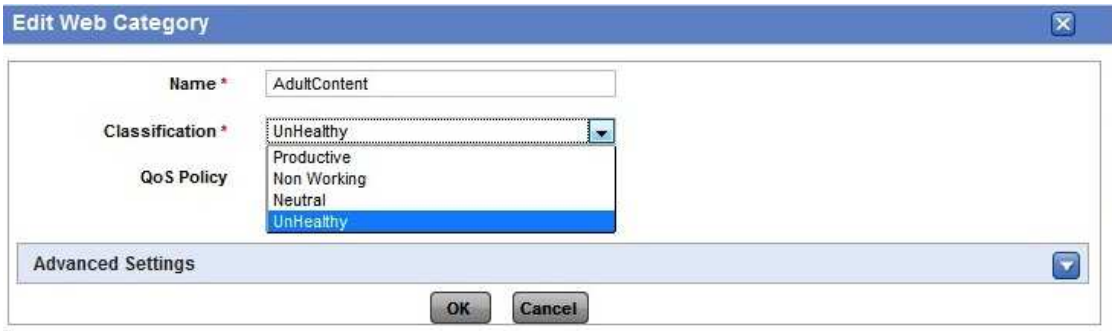
To see default web categories, go to Web Filter → Categories



Furthermore, each category is classified into four types specifying whether the categories are considered as:

- Productive
- Non Working
- Neutral
- Unhealthy

This classification can be modified according to the nature of business, as shown below:



File Type Category

File type category is a grouping of file extensions. Cyberoam has default categories that categorised most commonly used file types:

- Audio Files
- Dynamic Files
- Executable Files
- Image Files
- Video Files

Application Filter

Application Filter menu in Cyberoam allows to configure and manage filtering on various applications. The traffic coming from the web is filtered by various policies and categories.

Below is how the default application protocol categories look like:

Go to Application Filter → Category

Name	Description
File Transfer	File Transfer
Gaming	Gamig
General Internet	General Internet
IM	Instant Messengers
Internet Protocol	Internet Protocol
Network Services	Network Services
P2P	P2P
Proxy	Proxy
Remote Access	Remote Access
Streaming Media	Streaming Media
VOIP	VOIP

Content Filter Policies: Web Filter, Application Filter & IM

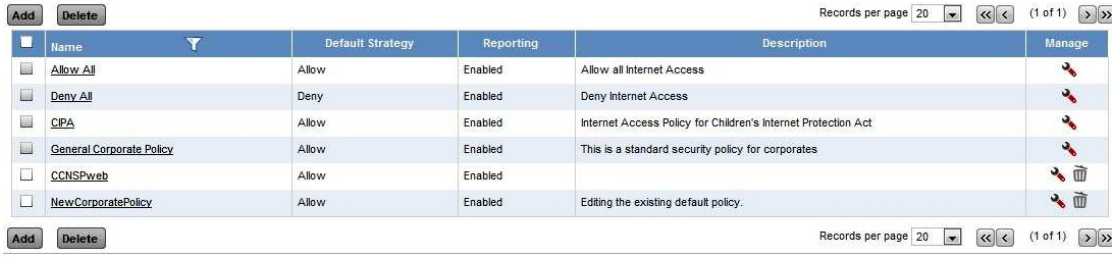
- Web Filter Policy controls user's web access. It specifies which user has access to which sites and allows defining powerful security policies based on almost limitless policy parameters like:
  Individual users, Groups of users, Time of day, Location/Port/Protocol type, Content type, Bandwidth usage (for audio, video and streaming content)

- Application Filter Policy controls user's application access. It specifies which user has access to which applications and allows defining powerful security policies based on almost limitless policy parameters like:
  Individual users, Groups of users, Time of day

- IM (Instant Messaging) allows to configure and manage restrictions on instant messaging services provided by the Yahoo and MSN messengers. The traffic coming from the web in form of files and chat is filtered by various rules and content filtering strategies. You can add an IM contact or IM contact group for configuring rules.

You can edit the existing default policies to add more categories, remove / change the behaviour of existing ones, turn off/on the reporting and also check for HTTPS access. To edit the existing policies, you need to create a new policy and use the existing default policy as template, as shown below:

Category Name	Type	Schedule	Action
Porn	Web	All The Time	Deny
Nudity	Web	All The Time	Deny
AdultContent	Web	All The Time	Deny
URLTranslationSites	Web	All The Time	Deny
Drugs	Web	All The Time	Deny
CrimeandSuicide	Web	All The Time	Deny
Gambling	Web	All The Time	Deny
MilitancyandExtremist	Web	All The Time	Deny



Now, you can add/remove the categories by editing the new policy.

Cyberoam has the flexibility to create custom Web Filter Policy to be applied to users or group of users. While creating a custom policy, you can either use an existing policy as a template or start from a blank policy as shown below:

The policy type defines the default action for the policy. You can enable / disable HTTPS blocking and reporting for the policy.

Once you create the policy, you will be shown the below screen to add categories to the policy.

On clicking “Add”, all the categories will be listed to be selected for the policy. You also need to select the action for each category – either “Allow” or “Deny” along with the schedule:

Custom Category

For the URLs and file extensions not listed under the default database, you can create custom web category to include the URLs and custom file type category to include file extensions that needs to be blocked.

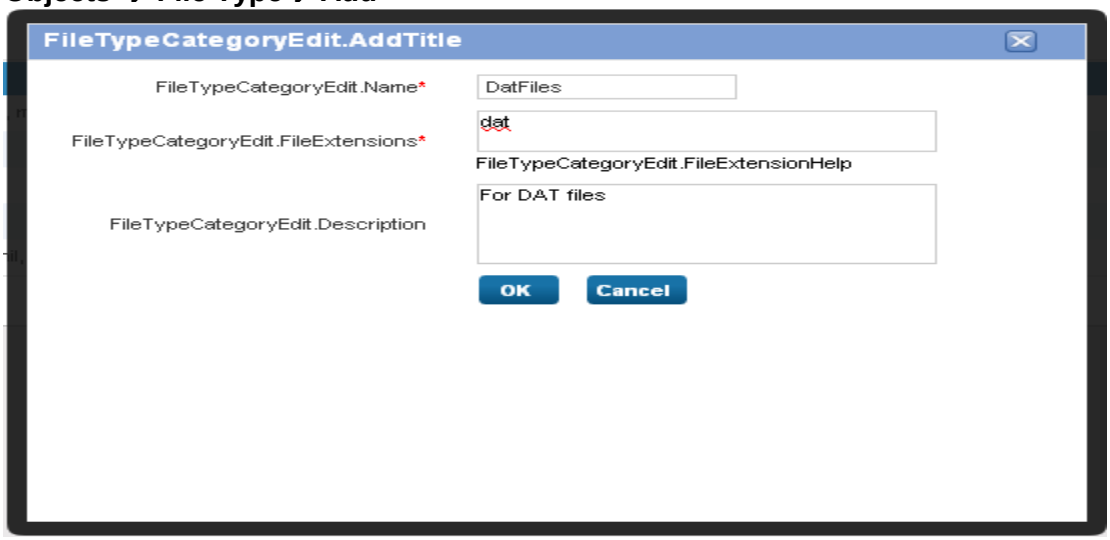
Web Filter → Category → Add

With custom web category, you can block domain names and URL containing the keywords defined in the category. The keyword has higher priority over domain names. Also, if you add a domain name already present in an existing category, custom category will take priority over the default one. The search URL feature is used to know if an URL is already present in any category.

File Type Category

For custom file type applications, file extensions can be added by creating a new custom file type category.

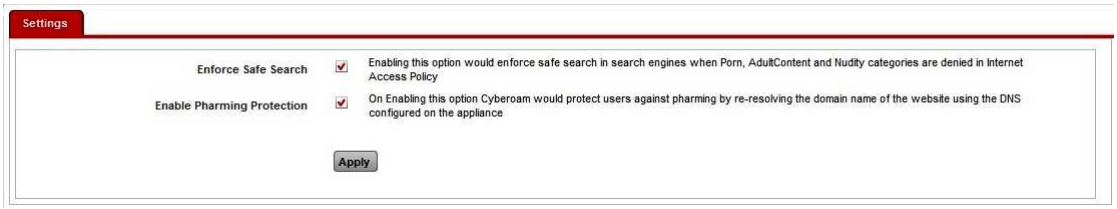
Objects → File Type→ Add



Safe Search capability to filter Adult Content

As soon as enabled, web sites containing pornography and explicit sexual content are blocked from the Google and Yahoo search results. This will be applicable only when access to Porn, Adult Content and Nudity categories is denied in Internet Access policy.

Go to Web Filter → Settings

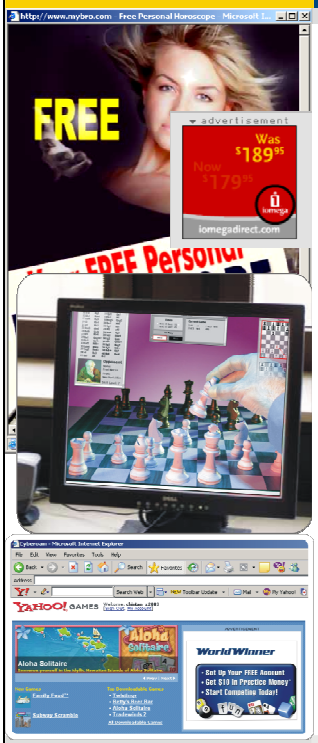


Cyberoam | Unified Threat Management

Content Filter Upgrade

www.cyberoam.com

Cyberoam | Unified Threat Management



Upgrade:

The Web Category database is automatically updated twice a week. The latest database version can be checked with the Cyberoam Security Center website at http://csc.cyberoam.com.

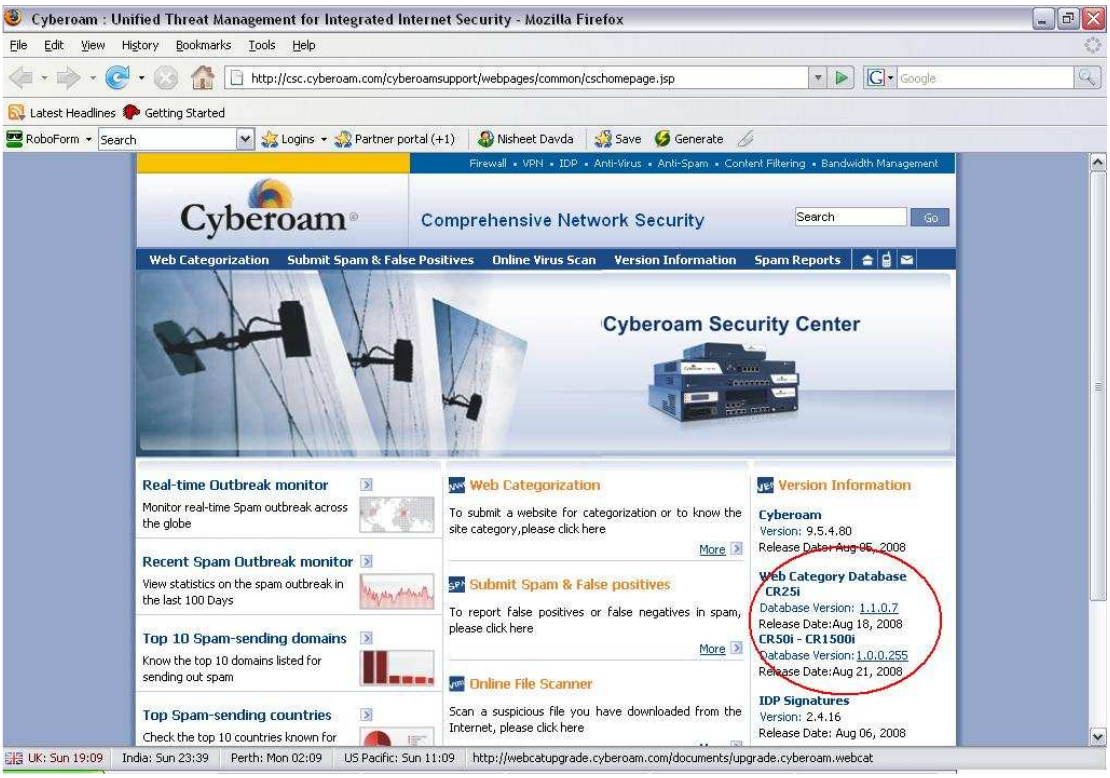
Upgrade Methods:

- Auto Upgrade
- Manual Upgrade through CLI
- Manual Comprehensive Upgrade through CLI

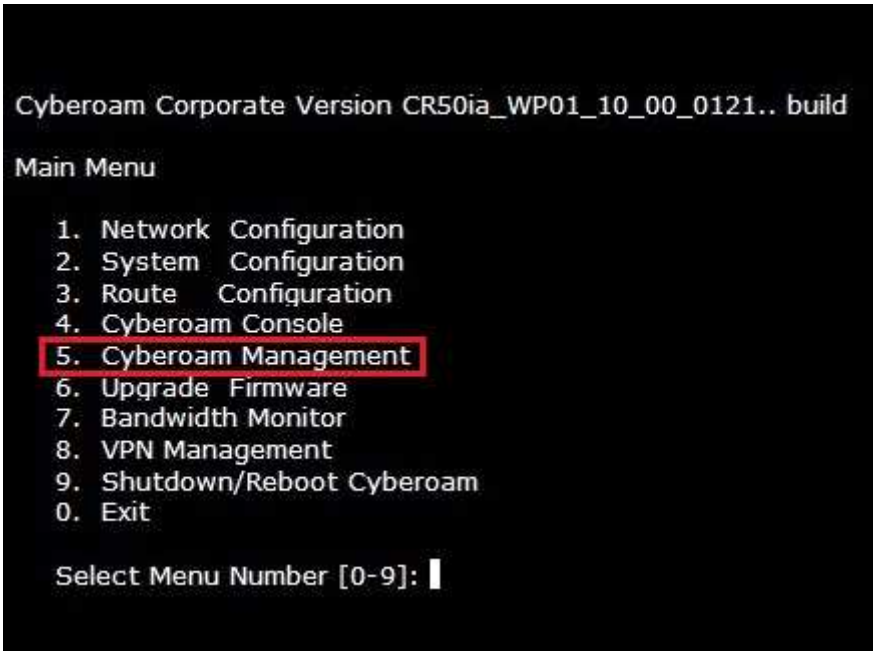
www.cyberoam.com

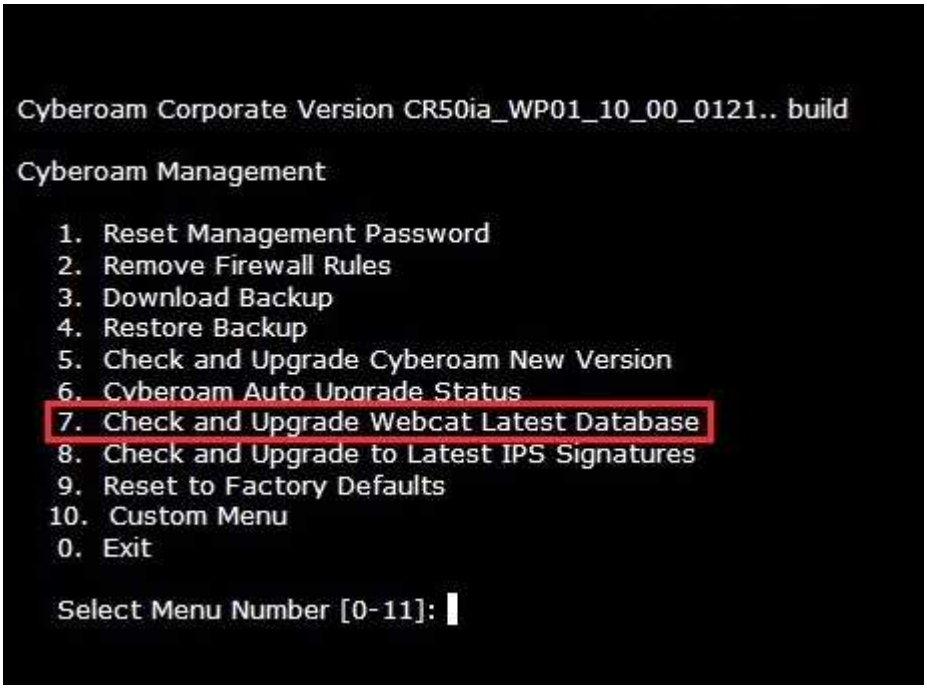
Upgrade

The Web Category database is automatically updated everyday for models CR25ia to CR1500i and twice a week for CR15i. The latest database version can be checked with the Cyberoam Security Centre website at http://csc.cyberoam.com.



You can also manually upgrade the Webcat database through the CLI Option 5 > Option 7.





A manual comprehensive upgrade is also available through Cyberoam GUI. This will allow you to upgrade Webcat directly to the latest version.

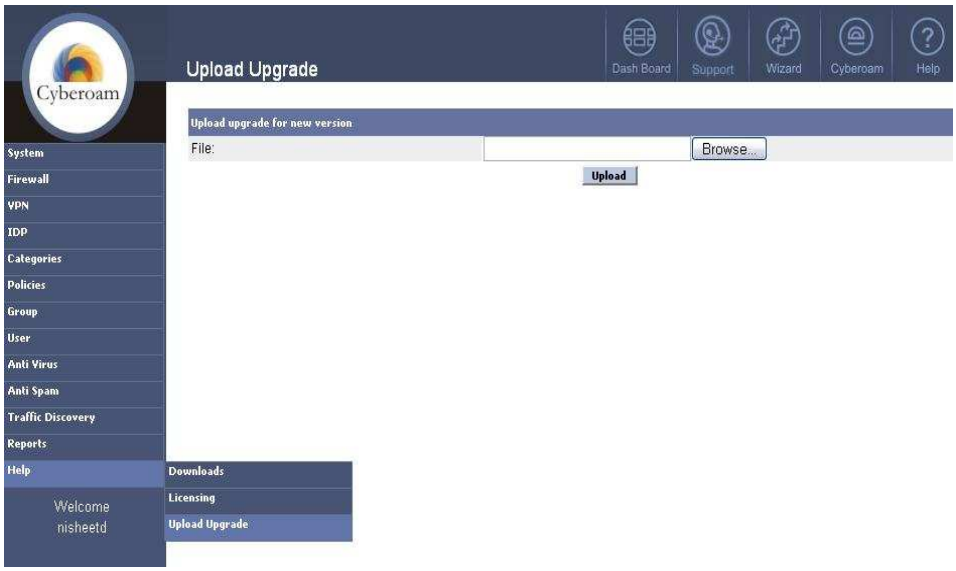
For example, if the latest released Webcat version is 1.0.0.255 and current Webcat version in your Cyberoam is 1.0.0.42, then with this upgrade you will be able to directly upgrade to the latest version 1.0.0.255 instead of upgrading each intermediate version individually.

The procedure is:

1. **Download Upgrade** from CSC website: http://csc.cyberoam.com

2. **Upload upgrade file from Web Console**

   Log on to Cyberoam Web Console
   Go to Help>Upload Upgrade
   Upload the above downloaded file
   Log out from Web Console

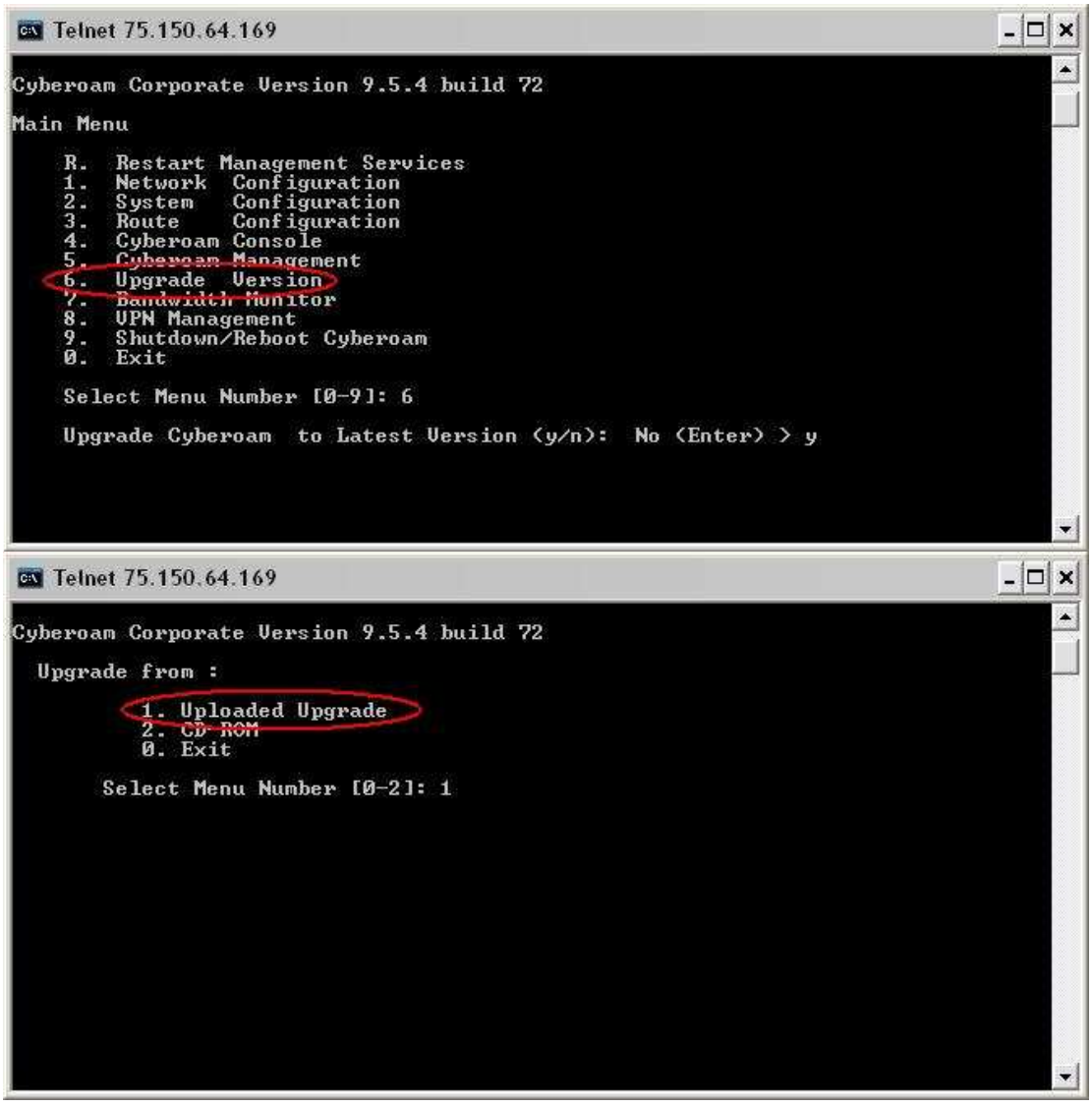


3. **Upgrade from Telnet Console**

Log on to Telnet Console

Select Option 6 Upgrade Version and press 'y' followed by '1'. Successful message will be displayed if Engine is upgraded successfully

Log out from Telnet Console



IM

IM (Instant Messaging) allows to configure and manage restrictions on instant messaging services provided by the Yahoo and MSN messengers. The traffic coming from the web in form of files and chat is filtered by various rules and content filtering strategies. You can add an IM contact or IM contact group for configuring rules.

•IM Contact
•IM Rules
•Content Filter

IM Contact

IM Contact is used to register various Yahoo and MSN messaging application users. A Contact can be created for a user having access any of the two IM applications. Along with the contacts, IM Contact Groups can also be created. Once the users are registered, various IM rules can be created for monitoring them. The rules can be set on groups as well as users individually.

•IM Contact
•IM Contact Group

IM

IM → IM Contact → Add

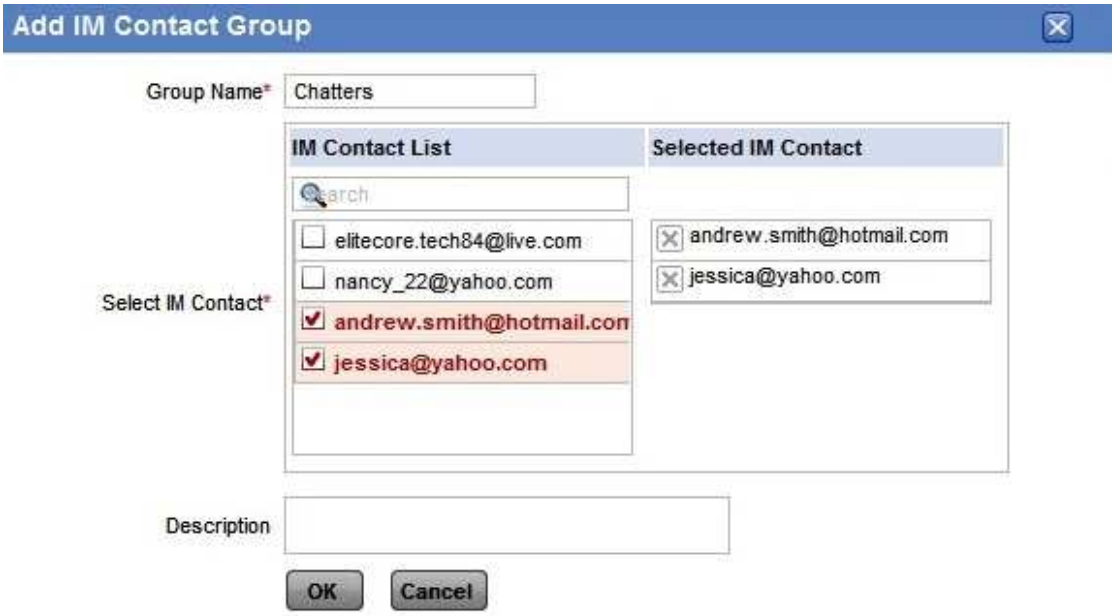
Protocol: Select the application used for instant messaging.

Available Options: Yahoo or MSN

IM Username: Username to identify the IM contact. The username can either be an email address or name of the user.

IM Group: Select the IM group to which the IM contact will be assigned.

To manage IM contact groups, go to IM → IM Contact → IM Contact Group.



IM Rules

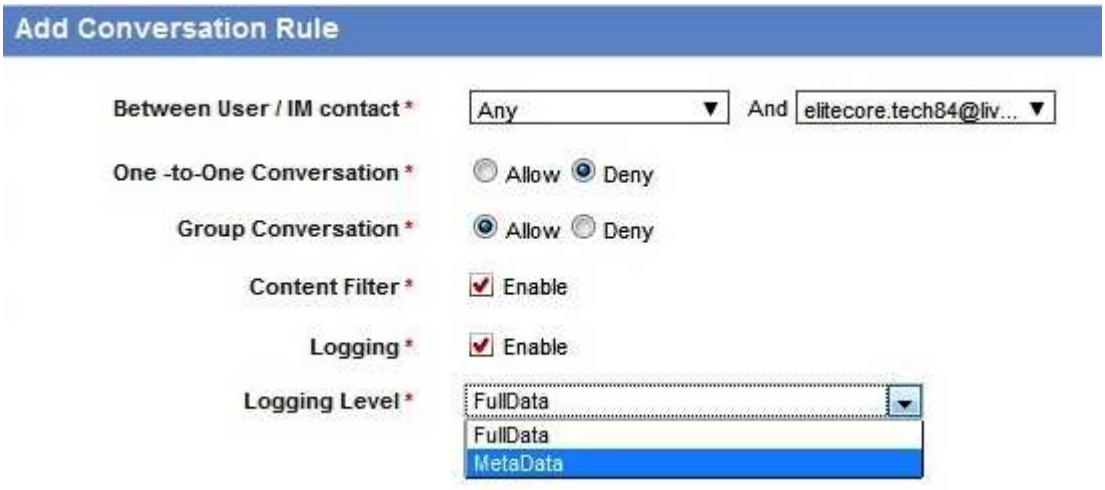
IM Rule controls user's instant messaging access. It specifies which users have access to IM applications. Individual rules for Conversation (chats), File Transfer, Webcam access and Login can be defined based on parameters like:

- One-to-One Conversation – One-to-One conversations can be allowed/denied between individual contacts or contacts within groups.
- Group Conversation – Group conversations between multiple users can be allowed/denied between individual contacts or contacts within groups.
- Content Filtering
- Virus Scanning
- Archiving
- Maintaining Logs

.

Allow/deny access can be set for an IM contact or entire IM contact group, or even normal users or user groups. For example, you can define a rule that blocks access to all one-to-one conversations between an IM contact group and a user group.
If IM access between contacts is restricted by configuring rules, an access restriction message is displayed in the conversation window.

•Conversation
•File Transfer
•Webcam
•Login



Between User / IM Contact : Select the Participants between whom the Conversation Rule is to be defined.

Available Options:

IM Contact
IM Contact Group
User
User Group

You can also add above contacts from the Add Conversation Rule Page itself.

One-to-One Conversation: Specify Action for the one-to-one conversation - Allow OR Deny

Group Conversation: Specify Action for the group conversation or chat - Allow OR Deny

Content Filter: Enable Content Filtering,

Logging: Enable Logging, if the log has to be maintained for the conversation.

If logging is enabled, the logs can be viewed from Logs & Reports → Event Viewer. Select 'Conversation' from 'Event Modules' list

Logging Level: Select the Logging Level if the Logging is enabled.

Available Options:

- Full Data – Full Data contains the entire information about conversation including the content of the chat, the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.
- Meta Data – Meta Data contains the information about the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.

IM Rules: File Transfer

- File Transfer page allows to configure and manage file transfer rules between any of the two identities. The files transfers between these two identities is monitored and logged.
- If file transfer access between contacts is restricted and contact tries to transfer a file, an access restriction message is displayed in the conversation window.

Go to IM → IM Rules → File Transfer

Virus Scanning: Enable Virus Scanning, if the file transferred between contacts is to be scanned.

Archiving: Enable Archiving, if the files are to be archived for further information.

Logging: Enable Logging, if the log has to be maintained for the transfer of files.

If logging is enabled, the logs can be viewed from Logs & Reports → Event Viewer. Select 'File Transfer' from 'Event Modules' list

Logging Level: Select the Logging Level if the Logging is enabled.

Available Options:

Full Data – Full Data contains the entire information about conversation including the content of the chat, the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.

Meta Data – Meta Data contains the information about the File Transferred including Login time, logout time, file transfer action defined and name of User or Groups between whom the file transfer happened.

IM Rules: Webcam

- Webcam page allows to configure and manage webcam rules between any of the two identities.
- If video conversation access between contacts is restricted and the contact tries to use the webcam, an access restriction message is displayed in the conversation window.

Go to IM → IM Rules → Webcam

Once the rule is created, it can be view as per below screen:

IM Rules: Login

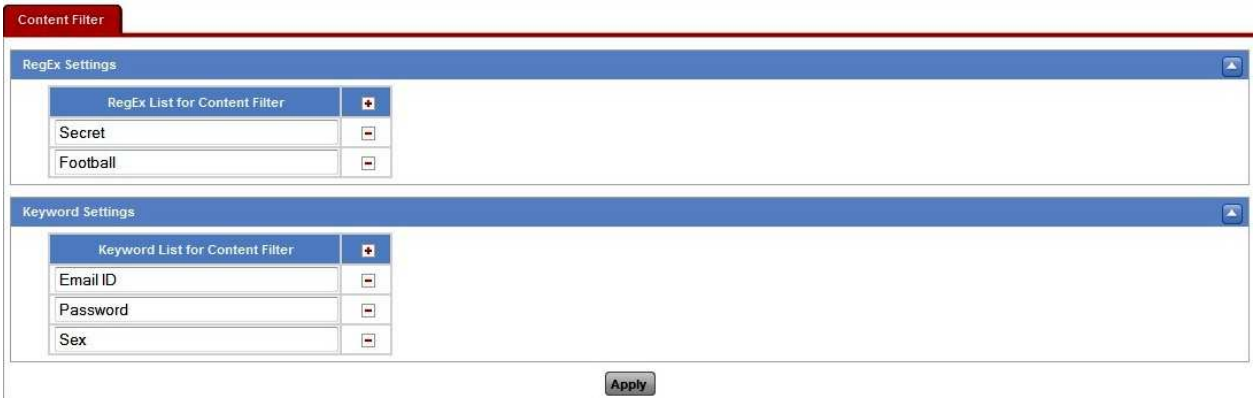
- Login page allows you to configure and manage login rules for IM Contact, IM Contact Group, User and User Group.

Go to IM → IM Rules → Login

IM Content Filter

- Content Filtering feature in Cyberoam is applied to Instant Messaging applications wherein content can be removed from the conversation if encountered.
- Content Filter page allows you specify list of keywords and regular expressions to be blocked, if encountered in any of the chat conversation. These configured keywords are removed and an error message is displayed for the same.

Go to IM → Content Filter



RegEx Settings: Specify Regular Expressions to be removed from the IM applications

You can add multiple regular expressions. Click Add icon to add more expressions and remove icon to delete expressions.

Keyword Settings: Specify Keywords to be removed from the IM applications

You can add multiple keywords. Click Add icon to add more keywords and remove icon to delete keywords.

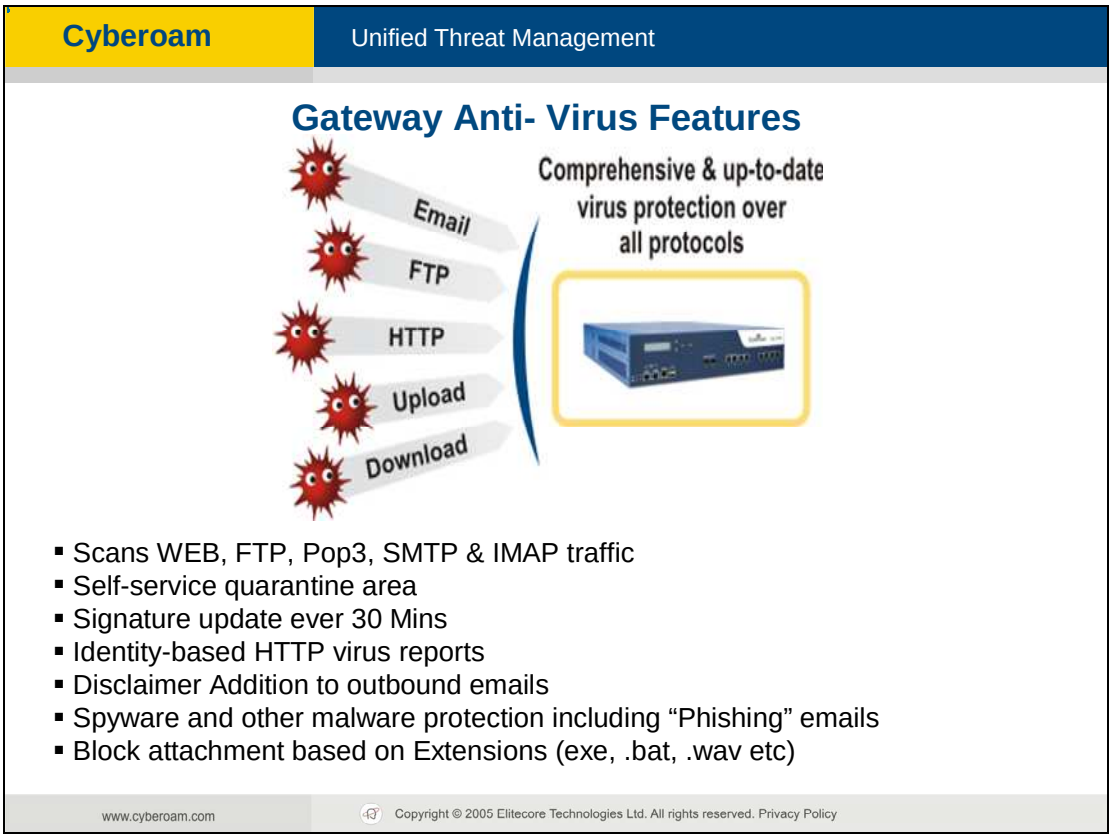
Applying the IM scanning on Firewall rule:

- After the IM Contacts, Rules and Content Filter are configured, we need to enable IM Scanning on the Firewall rule, so that all the messeging applications' traffic is scanned.

Module 8: Gateway Anti-Virus / Anti-Spam

Agenda:

- Gateway Anti-Virus Features
- Basics of Virus / Spyware / Malware / Phishing
- Web Anti-Virus Configuration
- Mail Anti-Virus Configuration
- FTP Anti-Virus Configuration
- Gateway Anti-Spam Features
- Basics of Spam
- Basics of Anti-Spam Technologies
- Cyberoam RPD Technology
- Anti-Spam Policies
- Anti-Spam Rules
- Upgrade
- Reports



Gateway Anti-Virus Features

Cyberoam Anti Virus is a part of unified solution and along with Anti Spam and IPS (Intrusion Prevention System), provides real time virus scanning that protects all network nodes – workstations, files servers, mail system from known and unknown attacks by worms and viruses, Trojan, Spy ware, AD Ware, spam, hackers and all other cyber threats.

Cyberoam Gateway Anti Virus provides a powerful tool for scanning and detecting infection and spam in the mail traffic (SMTP, POP3, and IMAP) as well as web (HTTP) traffic that passes through Cyberoam. Cyberoam UTM has an OEM with **Kaspersky Labs** and it uses Kaspersky’s Gateway AV

It guards users against infected messages, and delivers only the clean or disinfected messages, along with information on scanning results for every message. Additional filtration of messages from configured IP address and URL decreases the load on the server when scanning email traffic for viruses.

Cyberoam Anti Virus scans:

- HTTP
- FTP
- SMTP
- POP3
- IMAP

Cyberoam Anti Virus allows to:

- Scan email messages for viruses
- Detect infected, suspicious, and password-protected attachments and message
- Stop users from sending/receiving messages with any type of attachments
- Perform anti-virus processing of infection revealed in email messages by scanning
- Define policies to take appropriate action based on the protocol i.e. define action policy on how to handle for SMTP, POP3, FTP traffic and HTTP traffic if infection is detected
- Notify senders, recipients, and the administrator about messages containing infected, suspicious, or password protected attachments
- Quarantine messages - Quarantine feature allows to isolate and move infected and suspicious mails in a quarantine directory defined by a network administrator.
- Customise the anti virus protection of incoming and outgoing e-mail messages by defining scan policies.
- Cyberoam Gate way Anti Virus is fully compatible with all the mail systems and therefore can be easily integrated into the existing network.

Cyberoam | Unified Threat Management

Basics

- Virus
- Spyware
- Malware
- Phishing

Basics of Virus / Spyware / Malware / Phishing

Virus is a self-replicating malicious code that spreads by attaching itself to an application program, any executable system component, or documents and leaves no obvious signs of its presence. Viruses are hard to detect, easy to propagate, and difficult to remove.

With the number of computer users growing and the exchange of information via the Internet and email increases in volume, virus scares are becoming an almost everyday occurrence. Real mass attacks have become common place, and the consequences are serious, resulting in financial loss for individuals and corporations alike.

The number of threats and frequency and speed of attacks is increasing every day. Antivirus protection is therefore a priority for anyone who uses a computer.

Although viruses are transmitted mainly through emails or attachments to an e-mail note and Internet download, a diskette or CD can also be a source of infection. Therefore, the task of comprehensive protection against potential threats now extends beyond simple regular virus scans to real time anti virus protection.

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

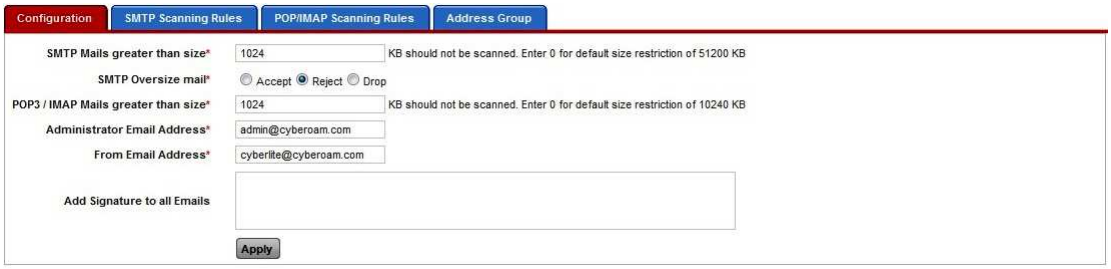
Spyware programs can collect various types of personal information, such as Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs. In an attempt to increase the understanding of Spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.

In response to the emergence of Spyware, a small industry has sprung up dealing in Anti-Spyware software. Running Anti-Spyware software has become a widely recognised element of computer security best practices for Microsoft Windows desktop computers. A number of jurisdictions have passed anti-Spyware laws, which usually target any software that is surreptitiously installed to control a user's computer.

Malware, also known as “Malicious Software”, is software designed to infiltrate or damage a computer system without the owner's informed consent. The term is a combination of the words **malicious** and **software**. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered Malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most root kits, Spyware, dishonest adware, and other malicious and unwanted software

In computing, **Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from Pay Pal, eBay, Youtube or online banks are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a website. Phishing is an example of social engineering techniques used to fool users. Attempts to deal with the growing number of reported Phishing incidents include legislation, user training, public awareness, and technical security measures.

Anti Virus General Configuration



The anti virus general configuration page displays the Anti Virus Engine status, the Anti Virus definitions data base version installed and being used. It also displays the date when it was last updated. Cyberoam detects viruses and disinfects using the antivirus definition database that contains definitions of all currently known viruses. It is extremely important to update your anti-virus definition database periodically because new viruses appear every day. By default, database updates are automatically downloaded and installed on your computer every 30 minutes.

Under the **Notifications Settings** option you can specify email address which will be used to send the action notification messages to mail receiver/sender along with the administrator email address and Mail Server IP/Port Number which would be used by the Cyberoam relay emails.

The **File Size Restriction** option specifies maximum size (in KB) of the file to be scanned. Files exceeding this size received through SMTP will not be scanned. Also specify the action to be taken on oversize files. If 'Accept' action is specified, all the oversize mails will be forwarded to the recipient without scanning.

The "**POP3 and IMAP Mails Greater than size**" specifies the maximum size (in KB) of the file to be scanned. Files exceeding this size received through POP3/IMAP will not be scanned and forwarded to the recipient without scanning.

The "**Add Signature to outgoing emails**" option helps to add a signature or disclaimer at the end of each outgoing email message. Please refer screens hot below:

NOTE: While anti-virus settings can be configured for system-wide use, they can also be implemented with specific settings on a per user basis. The firewall module on Cyberoam is used to enabling AV and AS scanning for particular traffic.

Web Anti-Virus Configuration

Cyberoam | Unified Threat Management

How does Cyberoam HTTP AV work?

Blocks all virus infected files being downloaded

Cyberoam Virus Definition includes

- Viruses
- Worms
- Trojans & Spyware
- Hacker Utilities
- Malware

How does it help?

- Blocks spyware not only from spyware sites but also from innocent sites
- Malware being stopped at gateway level

www.cyberoam.com

Cyberoam | Unified Threat Management

HTTP Configuration

Two Modes of Scanning

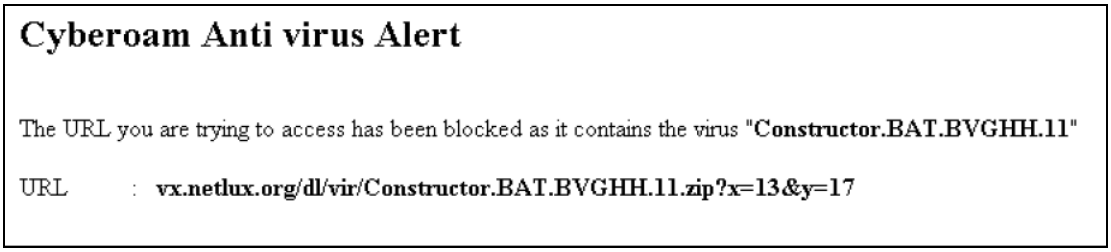
- Batch Mode
- Real Time Mode

www.cyberoam.com

Cyberoam can be configured for real time or batch mode scanning for HTTP traffic. Anti virus scan modes can be defined on the Cyberoam (i.e. real time or batch mode scanning for HTTP traffic). In batch mode virus scanning will start only after the complete file is downloaded. This would mean that large files would take some time to scan. Thus, configuring in real mode is the best option you have while downloading bulky files.

You can configure the maximum file size that can be buffered to the memory for scanning. This will also prevent the unintentional download of virus file hidden in the fragmented files.

By default, Cyberoam will not scan any HTTP traffic (i.e. you have to enable HTTP traffic scanning by defining HTTP rule). Define HTTP rule specifying from which source and destination IP address HTTP traffic should not be allowed to pass without scanning. If virus scanning is enabled and viruses detected, receiver will receive a notifying message as shown below.



To Configure Anti Virus Scanning for HTTP, select **Anti Virus** -> **HTTP -> Configuration.** The screen elements are described below:

Scan Mode: We can define anti virus scan modes on Cyberoam (i.e. real time or batch mode scanning for HTTP traffic). In batch mode virus scanning will start only after the complete file is downloaded. This would mean that large files would take some time to scan. Thus, configuring in real mode is the best option you have while downloading bulky files.

File Size Threshold: This option is used to specify file size threshold for Anti Virus scanning for the HTTP protocol. Files that exceed configured threshold will not be scanned.

Also we can define HTTP rule to scan/bypass web pages based on URLs, Source IP and destination IP. To add an HTTP rule you've got to navigate to Anti Virus -> HTTP -> Scanning rule. The screen that comes up is shown below:

Add HTTP scanning Rule Page

In the screen above, Scanning can be enabled /bypassed based on the Source IP, Destination IP, and URL Regex using the Rule Action drop down menu.

With HTTP scanning rules, you can customise levels of protection. For example, while traffic between internal and external IP addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. Rules are ordered by their priority. When the rules are applied, they are processed from the top downwards and the first suitable rule found is applied. Hence, while adding multiple rules, it is necessary to put strict rules before moderate and general rules.

Also the HTTP rule scanning order can be changed and Customised as per requirement. The tabs at the bottom namely "Move up", "Move Down", "Update order" are used for changing the HTTP rule scanning order.

Mail Anti-Virus Configuration

The Mail Anti-Virus Configuration can be done for three protocols on Cyberoam UTM namely SMTP, IMAP and POP3.

Cyberoam | Unified Threat Management

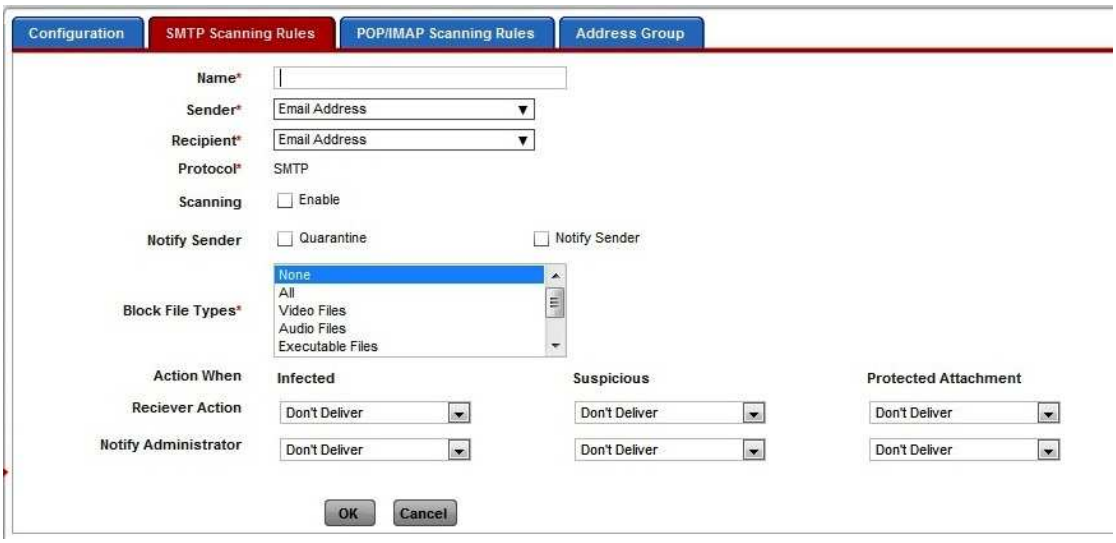
SMTP Scan Policy

- Default SMTP policy is applicable for all SMTP traffic defined in the Scan Rules.
- Cyberoam allows you to define multiple policies for instead of one blanket policy

www.cyberoam.com

Cyberoam gives you an option to create custom scan policies along with the default scan policy which is preconfigured on the appliance. With custom scan policy you can define whether to quarantine the message or not, the action to be taken if a mail is infected, whether to block the message containing a specific file type or with any type of file attachment and finally whether to send notifications to the sender, receiver and the administrator about the receipt of an infected message

Antivirus Configuration for SMTP (Anti Virus → Mail → SMTP)



As soon as you register Cyberoam Gateway Anti Virus; default SMTP policy is applicable to all inbound and outbound email traffic. The default policy is the general

policy and not fit-for-all policy and hence might not fit in your network requirement. Cyberoam allows you to define multiple policies instead of one global policy, as per your requirements. You can fine tune the policies as per the network requirements.

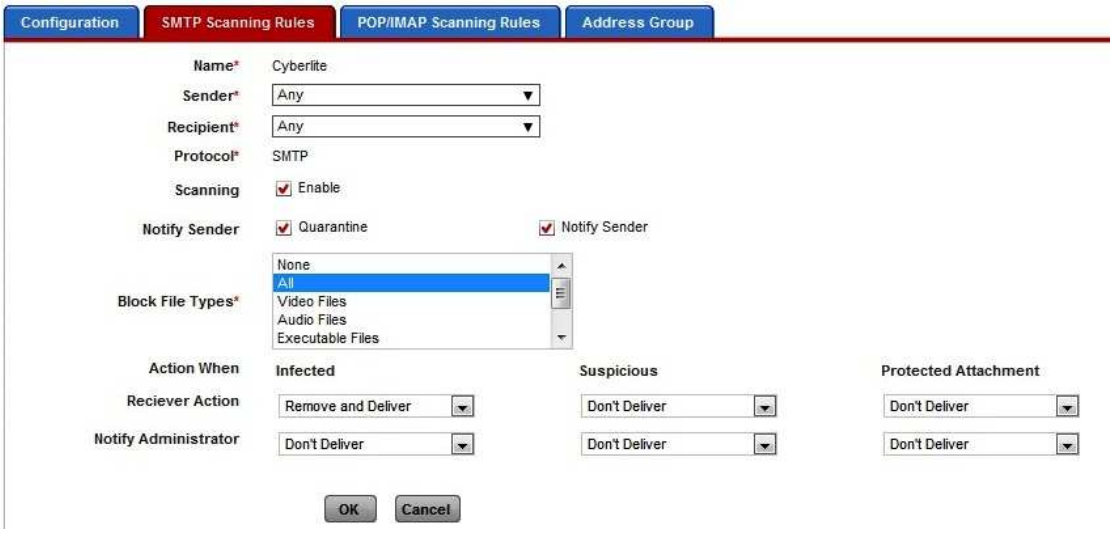
Address Groups

To create, go to Antivirus → Mail → Address Group → Add

The scanning rules described above can either be applied to an individual or group of email addresses, IP address or network (can be applied to anti spam rule only), RBL (Real-time Black List) applied to anti spam rule only. This is done using the email scanning rules and the email IDs, IP addresses or RBL are grouped using **Address Groups**. Address group is the group of email addresses, network or IP addresses, or RBL. When the policy is applied to the address group, policy is applied to all the addresses included in the group.

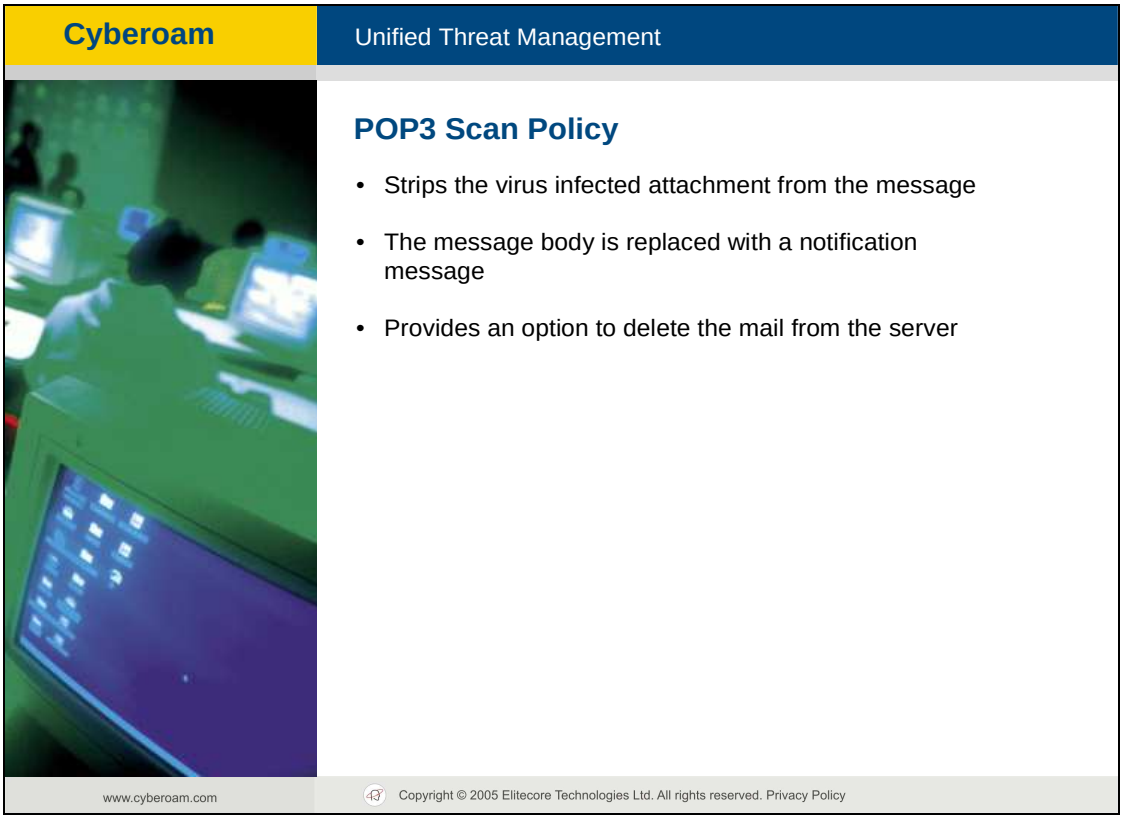
Email Scanning Rules

Go to Antivirus → Mail → SMTP Scanning Rules → Add



Finally scanning rules defines which scanning policy is to be applied to which pair of sender-recipient email address i.e. map scanning policy with the email address/address groups. Cyberoam provides the default email scanning rule which cannot be deleted.

Antivirus Configuration for POP3



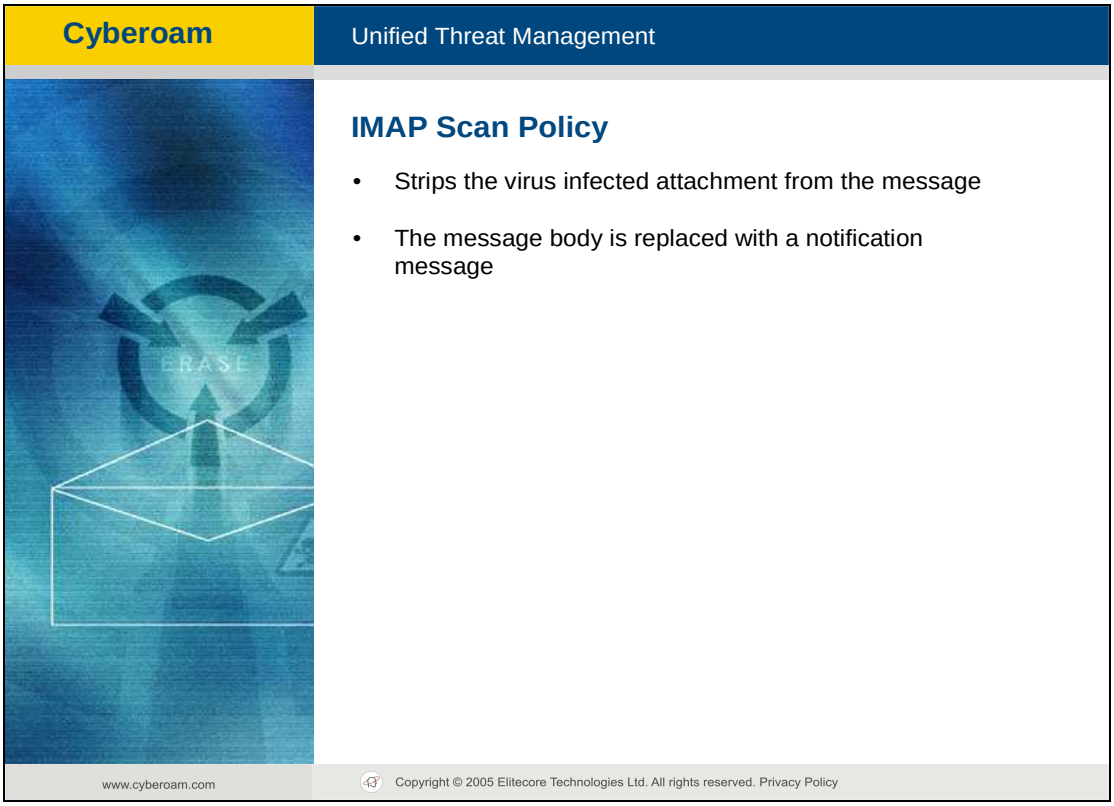
Cyberoam allows individual action policy for POP3, SMTP, IMAP and HTTP traffic.

POP3 policy is applied to the POP3 traffic only i.e. when the virus is detected in POP3 traffic, POP3 policy is applied. When the message containing virus is detected, depending on POP3 policy, Cyberoam deletes message from the POP3 server or simply sends the notification to the receiver stating that mail was not delivered because it was infected. POP3 configuration allows you to enable or disable the deletion of the infected message from the POP3 server. Go to **Anti Virus** -> **POP3** -> **Configuration** to configure POP3 policy.

Below is a sample message sent to the recipient :

```
Subject: **VIRUS FOUND MAIL REJECTED**

Virus infected attachment(s) have been removed from this mail.
Virus Name(s): "Virus name list"
Attachment Name(s): "File names list" [From > sender name] [Date]
```

Antivirus Configuration for IMAP



Cyberoam allows defining the individual action policy for POP3, SMTP, IMAP and HTTP traffic. IMAP policy is applied to the IMAP traffic only. When the message containing virus is detected, infected message is replaced with a message notifying the receiver that mail was not delivered because it was infected.

Below is a sample message:

Original Subject: Calculating staffing needs

Subject: **VIRUS FOUND MAIL REJECTED**

Virus infected attachment(s) have been removed from this mail.
Virus Name(s): "Virus name list"
Attachment Name(s): "File names list" [From > sender name] [Date]

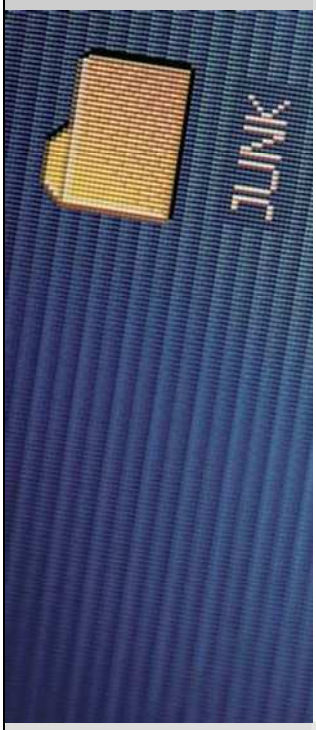
FTP Anti-Virus Configuration

Cyberoam detects a virus and removes the infected file from FTP download or from an email message. You can configure the maximum file size for scanning.

The mails greater then the specified size will not be scanned as shown in the figure below:

Go to Antivirus → FTP

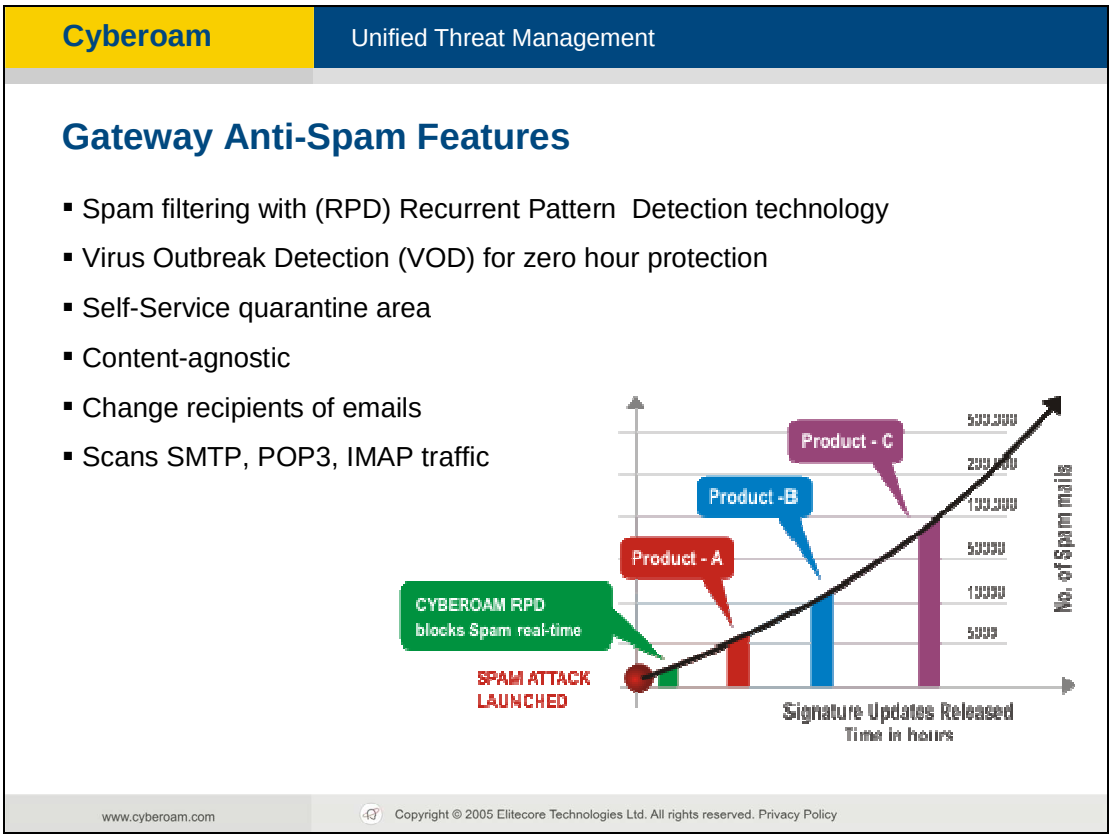
Cyberoam | Unified Threat Management



Gateway Anti-Spam

www.cyberoam.com

Gateway Antispam Features



Gateway Anti-Spam Features

Cyberoam Anti Spam as a part of unified solution along with Anti Virus and IPS (Intrusion Prevention System), provides real time virus and spam scanning. Anti Spam module is an add-on module which needs to be subscribed before use.

Cyberoam Gateway Anti Spam provides you with powerful tools for scanning and detecting spam in the e-mail traffic. Cyberoam Gateway Anti Spam inspects all incoming emails - SMTP, POP3 and IMAP traffic - before the messages are delivered to the receiver's mail box. If spam is detected, depending on the policy and rules set, emails are processed and delivered to the recipient unaltered, reject and generate a notification on the message rejection, add or change subject or change the receiver.

Cyberoam Gateway Anti Spam is fully compatible with all the mail systems and therefore can be easily integrated into the existing network.

Cyberoam Anti Spam allows to:

- Scan email messages for spamming by protocols namely SMTP, POP3 and IMAP
- Monitor and proactively detect recurrent patterns in spam mails and combat multi-format – text, images, HTML etc. and multi-language threats
- Monitors mails received from Domain/IP address
- Detect spam mails using RBLs.
- Accept/Reject messages based on message size and message header
- Customise protection of incoming and outgoing e-mail messages by defining scan policies
- Set different actions for SMTP, POP and IMAP spam mails
- Configure action for individual email address
- Notify receivers about spam messages

Basics of Spam

Basics of Spam

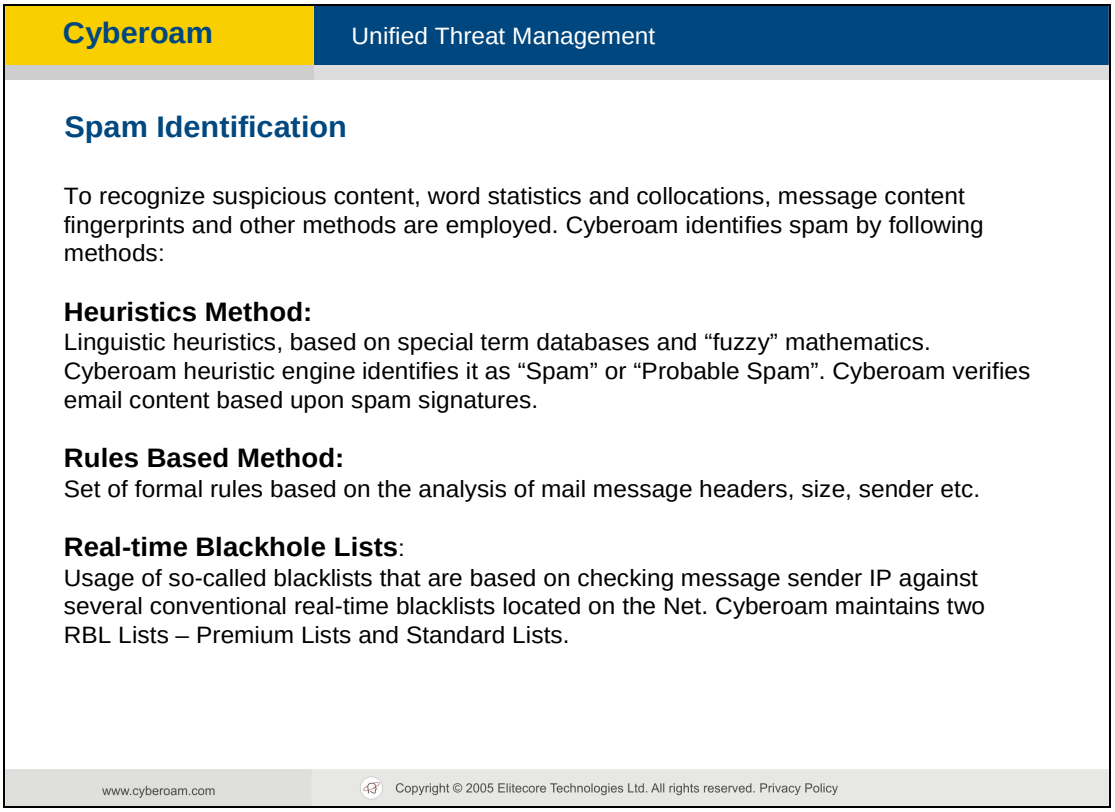
Spam refers to electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail.

Spamming is to indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. In other words, it is an inappropriate attempt to use a mailing list, or other networked communications facility as a broadcast medium by sending the same message to a large number of people who did not ask for it.

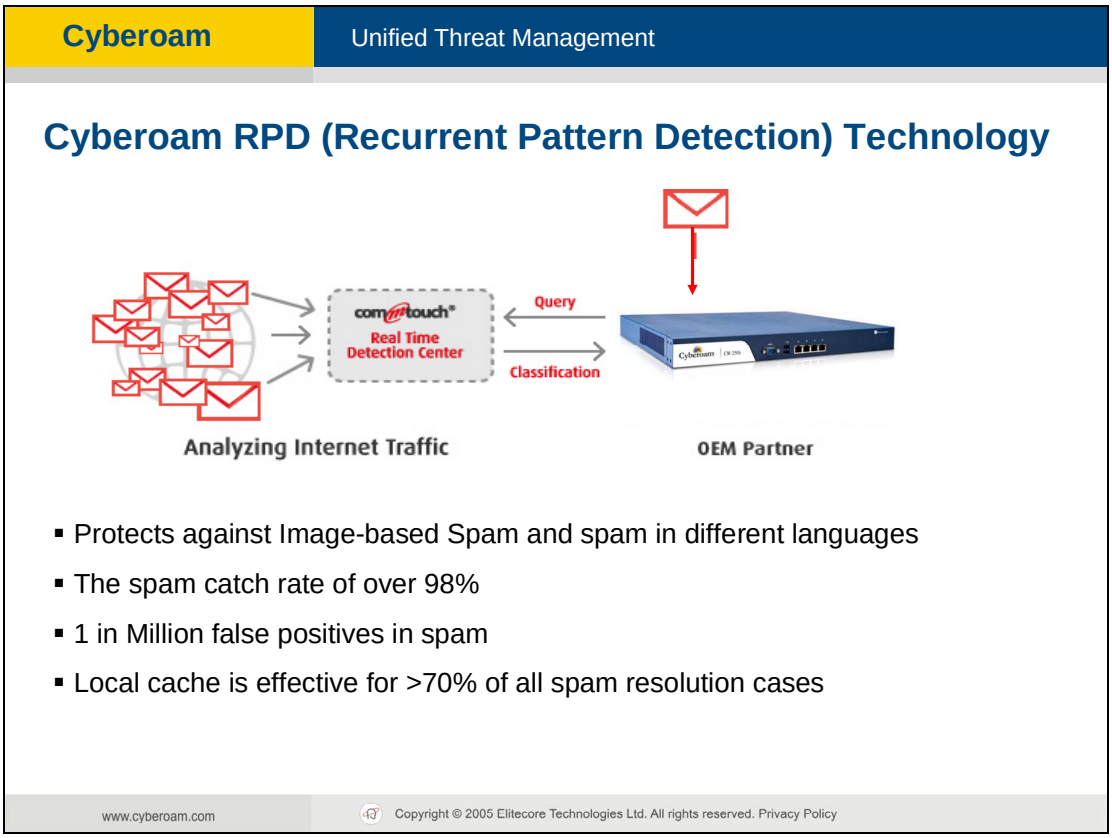
In addition to being a nuisance, it also eats up a lot of network bandwidth. As the Internet is a public network, little can be done to prevent spam, just as it is impossible to prevent junk mail. However, the use of software filters in e-mail programs can be used to remove most spam sent through e-mail to certain extent.

With the number of computer users growing and the exchange of information via the Internet and email increases in volume, spamming has become an almost everyday occurrence. Apart from network bandwidth, it also affects the employees productive as deletion of such mails is a huge task. Anti spam protection is therefore a priority for anyone who uses a computer

Basics of Anti-Spam Technologies



Cyberoam RPD Technology



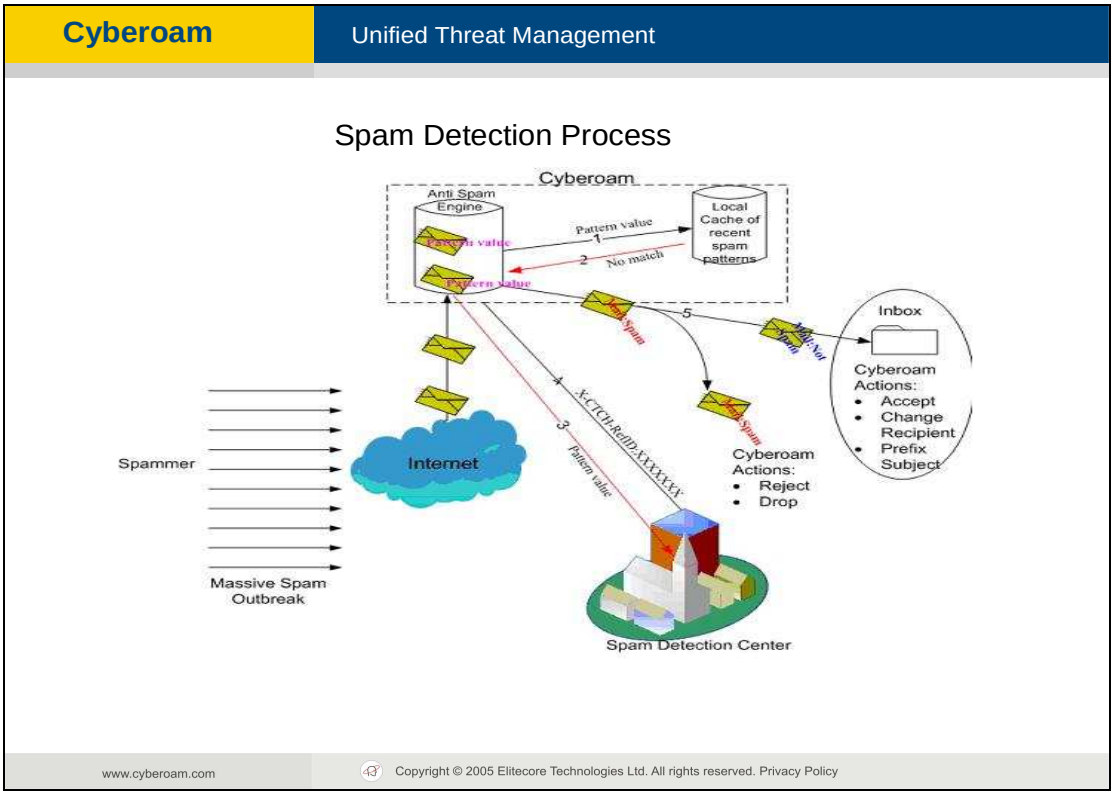
Cyberoam RPD Technology:

Cyberoam's spam protection strategy is based on the most fundamental characteristic of all spam and Malware – their mass distribution over the Internet.

Cyberoam customers worldwide, query the Spam Detection Centre and receive message classification in real-time. The result is instant protection from new outbreaks – far ahead of signatures or software updates.

Cyberoam focuses on detecting patterns in spam attacks, rather than on a lexical analysis of the contents of individual email messages. It is content-agnostic and can detect spam in any language, format or encoding method.

RPD (Recurrent Pattern Detection) technology responsible for proactively probing the Internet to gather information about massive spam outbreaks from the time they are launched. This technology is used to identify recurrent patterns that characterise massive spam outbreaks.



Cyberoam Spam detection process

1. Spammer sends the massive spam attack over the Internet. Mail arrives at Cyberoam.

2. Cyberoam Anti Spam Engine sends Message Pattern Characteristics to its Local Cache. Local cache stores the spam patterns of all the recent attacks. If a message pattern characteristic is found, Engine performs step 5.

3. If the matching pattern is not found in Local Cache, Message Pattern Characteristics is send to the remote Spam Detection Centre.

4. Within few milliseconds, Detection Centre classifies the message and sends reply to Anti Spam Engine.

5. Anti Spam Engine forwards message to the mail recipient if it is not spam else it will reject the mail.

6. Cyberoam stores the newly classified pattern in its local cache for future use.

IP Reputation

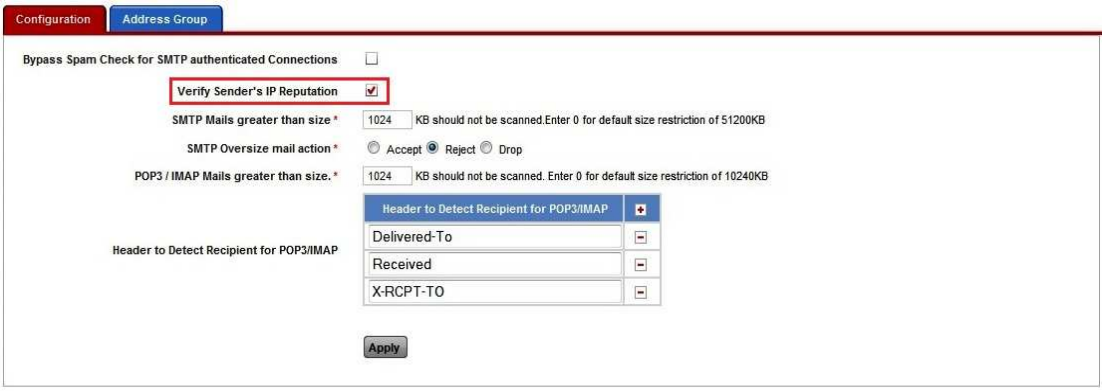
IP Reputation

- It dynamically classifies and reclassifies the reputation of each source IP and maintains a database of addresses used spammers and legitimate mailers.
- It fights the unwanted mail at the perimeter, reducing the incoming spam messages at the entry-point, before these messages enter the network resulting into reduced system resources and bandwidth usage.

Enabling IP Reputation

- Feature available as “Verify Sender’s IP reputation” (Anti Spam ◊ Configuration) in the Web Admin Console.
- If enabled, Cyberoam dynamically checks the sender IP address and rejects the SMTP connection if IP address is found to be responsible for sending spam mails.
- As it is a global option, if spam scanning is enabled, all the mails will be first subjected to IP reputation filtering followed by filtering based on actions configured in spam policy.
- If above mentioned option is not visible in the Web Admin console , one is required to purchase a new license of Gateway Anti Spam module and re-subscribe the module with the key. The new key enables both RPD & IP Reputation filtering.

Anti Spam → Configuration



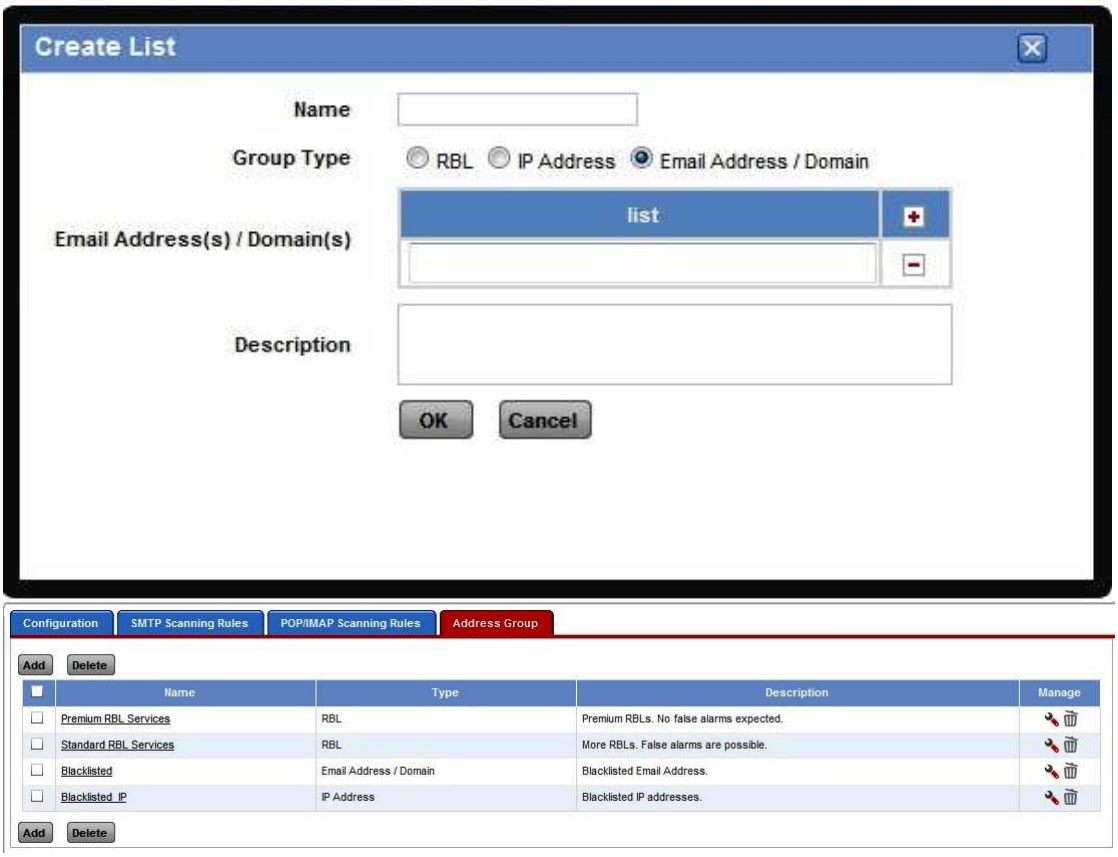
Anti Spam Configuration

Scanning rule can be defined for individual or group of

- Email address
- IP address
- RBL (Real-time Black List)

Address group is the group of email addresses, IP addresses, or RBLs. Whenever the policy is applied to the address group, policy is applied to all the addresses included in the group. RBL is a list of IP addresses whose owners refuse to stop the proliferation of spam i.e. are responsible for spam or are hijacked for spam relay. This IP addresses might also be used for spreading virus.

Address Groups



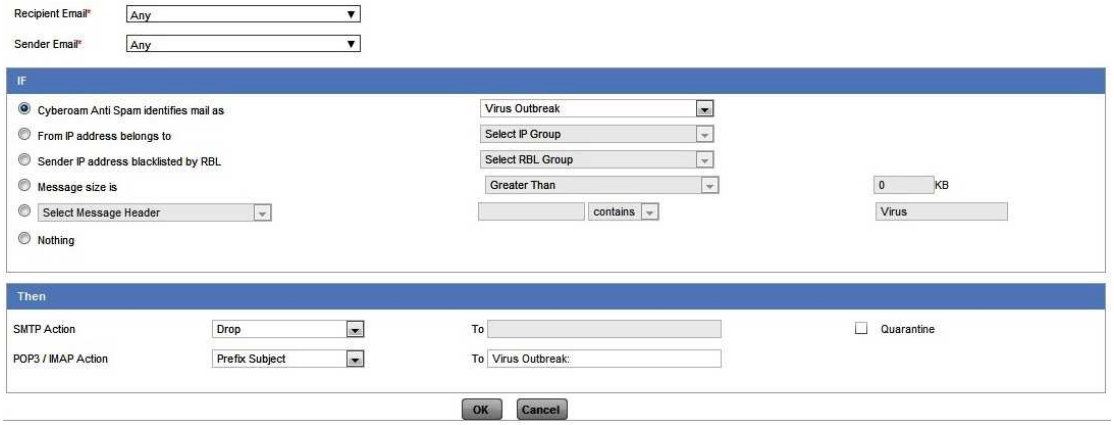
Cyberoam will check each RBL for the connecting IP address. If the IP address matches to the one on the list then the specified action in policy is taken.

Anti-Spam Rules

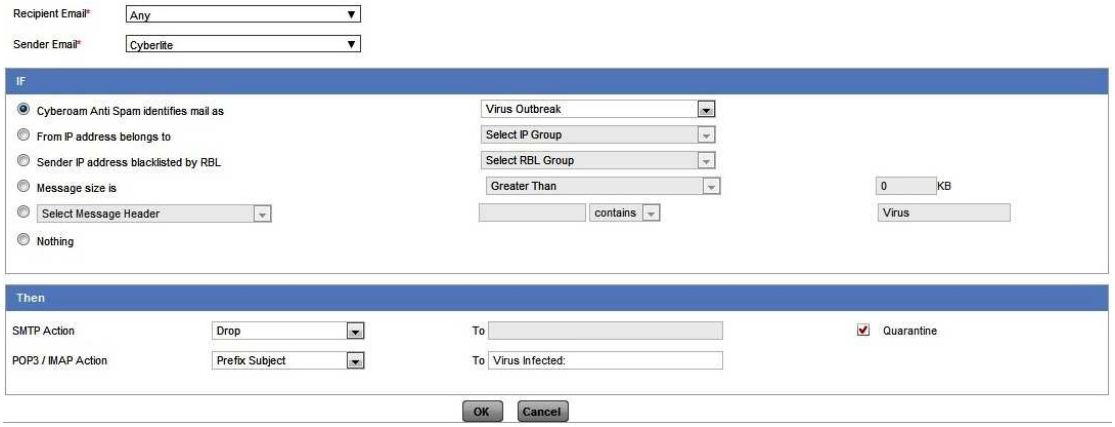
Antispam → Spam Rules

The default rule:

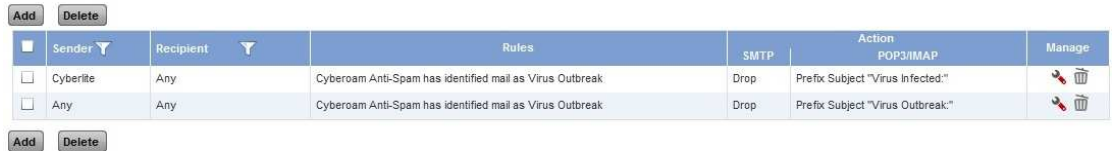
To edit the default rule, press  icon:



To Add a new spam rule, go to Antispam → Spam Rules → Add



This new rule will be added on above the default rule:



Quarantine: Spam Digest & Quarantine Area

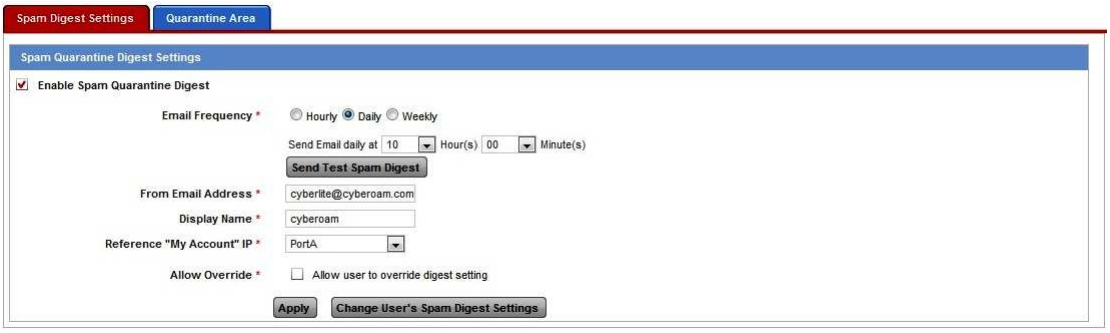
Spam digest is an email and contains a list of quarantined spam messages filtered by Cyberoam and held in the user quarantine area. If configured, Cyberoam mails the spam digest as per the configured frequency to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.

Spam Digest Settings:

Digest service can be configured globally for all the users or for individual users. Cyberoam mails the spam digest as per the configured frequency to the user.

The Spam Digest provides following information for each quarantined message:
•Date and time: Date and time when message was received
•Sender: Email address of the sender
•Recipient: Email address of the receiver
•Subject: Subject of the message

To manage spam rules, go to Anti Spam → Quarantine → Spam Digest Settings.



Enable Spam Quarantine Digest: Enable Spam Quarantine Digest to configure digest service for all the users.

Email Frequency: Specify the spam digest mail frequency.

Digest can be mailed every hour, every day at configured time or every week on the configured day and time.

Click “Send Test Spam Digest” and specify the email address to send the test spam digest mail.

From Email Address: Specify email address from which the mail should be sent.

Digest mail will be send from the configured mail address.

Display Name: Specify mail sender name. Digest mail will be send with the configured name.

Reference “My Account IP”: Select Interface/Port IP from the ‘Reference “MyAccount” IP’ dropdown list.

User My Account link in Digest mail will point to this IP address. User can click the link to access his quarantined messages and take the required action. The users not falling under the specified Interface will have to access the quarantine mail directly from their MyAccount.

Allow Override: Enable “Allow user to override digest setting”, if you want each user to override the digest setting i.e. user can disable the digest service so that they do not receive the spam digest.

Change User’s Spam Digest Settings: Click “Change User’s Spam Digest Settings” button to change the digest setting of the individual users. It allows to select group and update the spam digest setting of group members.

Change User’s Spam Digest Settings:

Click “Change User’s Spam Digest Settings” button to change the digest settings of the individual users. It opens a new page which allows you to search groups and users for updating the spam digest settings of group members.

You can individually search for user and user groups.

Quarantine Area: Under Quarantine Area, Quarantined mails can be searched based on sender email address, receiver email address, and subject.

Cyberoam reserves 5GB for Quarantine area. To maintain the total size of Quarantine area, Cyberoam removes older mails once the repository is filled by 80% i.e. once the repository level crosses 4GB, Cyberoam automatically deletes the oldest quarantined mails.

Use ‘Filter Result’ section to search for mails from the list of Quarantined Mails. To view and release the quarantined mails go to, Anti Spam → Quarantine → Quarantine Area.

Enable Scanning:

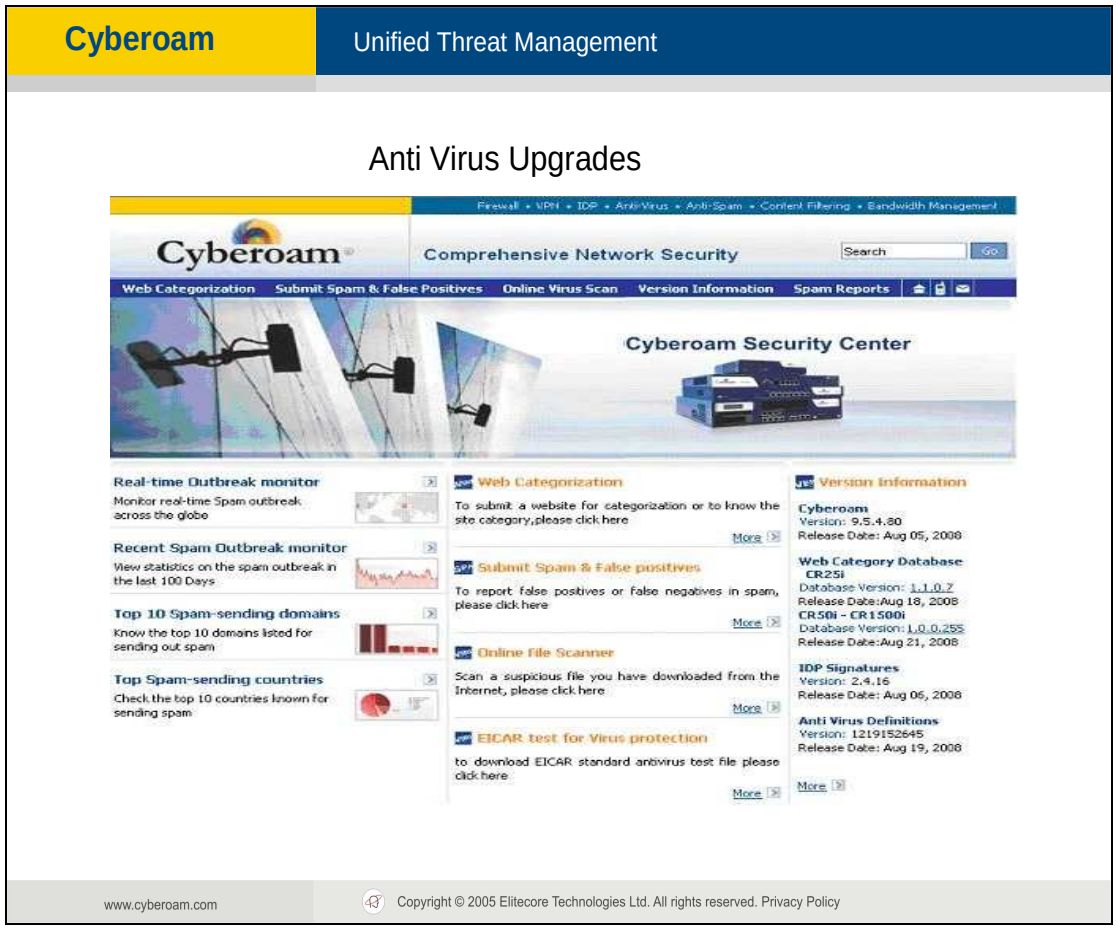
Enable anti-spam scanning using firewall rules. While anti-spam settings can be configured for system-wide use, they can also be implemented with specific settings on a per user basis.

You can enable anti spam scanning by creating firewall rule for:

- Zone
- User/User Group
- Host/Host Group

By enabling scanning through firewall, you can customise levels of protection. For example, while traffic between LAN and WAN might need strict protection, traffic between trusted internal addresses might need moderate protection. Hence you can enable/disable scanning for particular combination of source and destination IP address or domain.

Upgrade



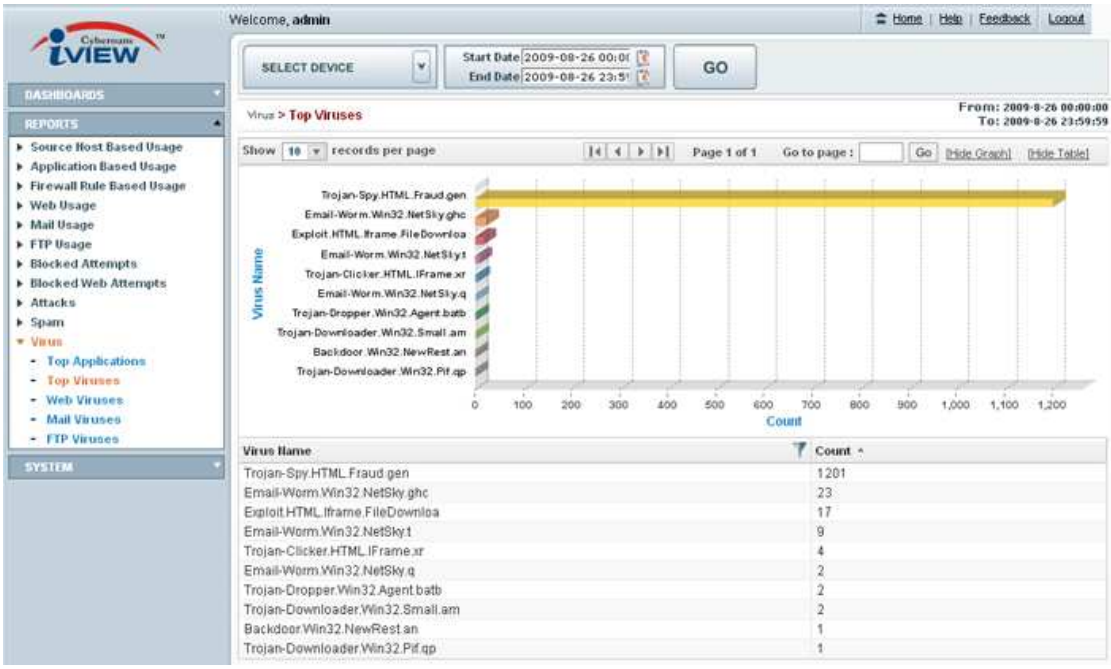
Cyberoam automatically updates its **Anti Virus** definitions every 30 minutes.

You can check the database version used by your Cyberoam from Web Admin Console Antivirus>Mail>General Configuration page. You can also check the latest available database version from http://csc.cyberoam.com

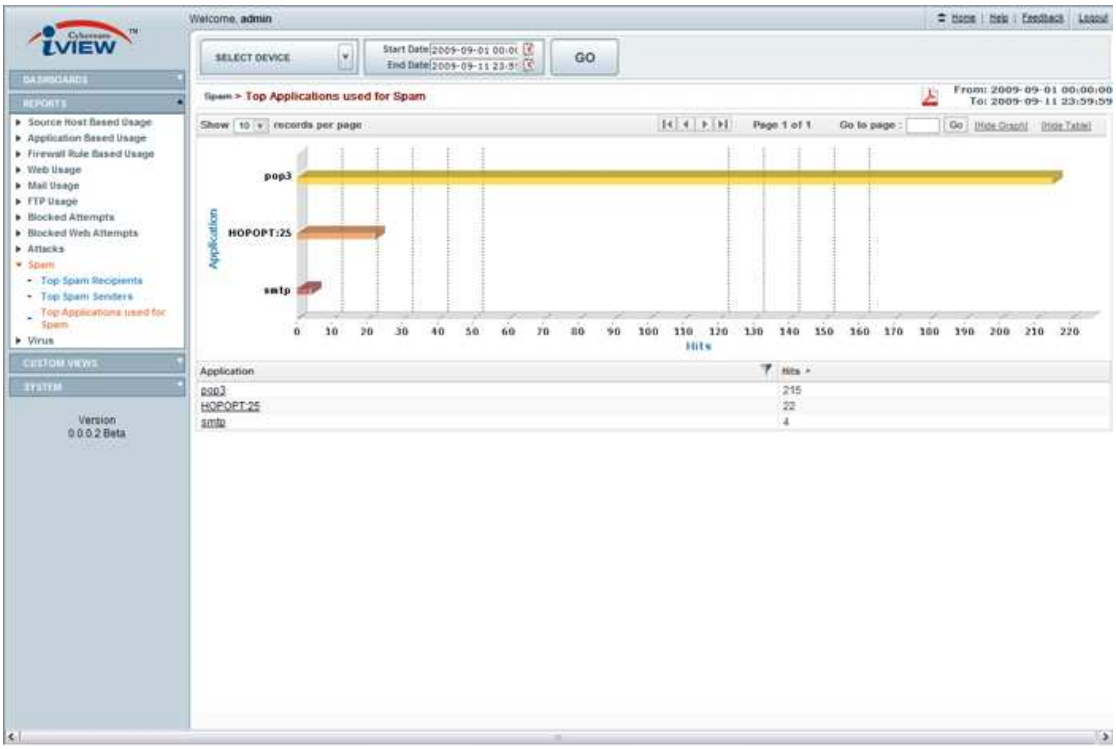
Cyberoam is using signature less technology called Recurrent Pattern Detection (RPD) for **Anti Spam**. Periodic definition update concept is not there in Cyberoam.

Reports

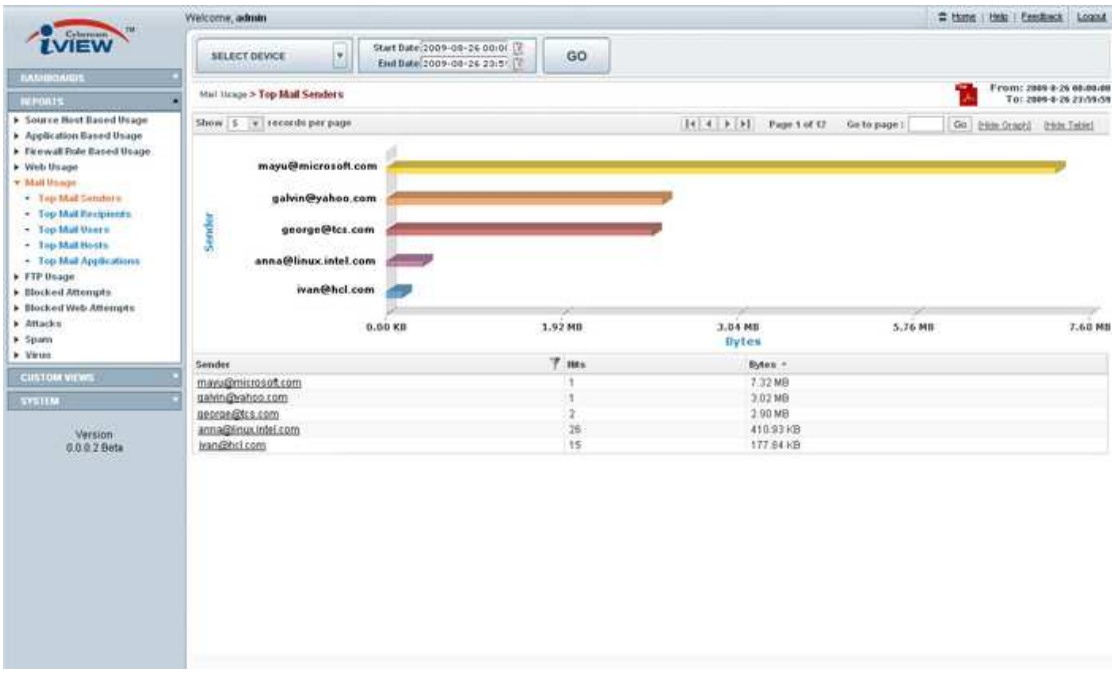
Anti Virus Reports:



Top Spam Applications:

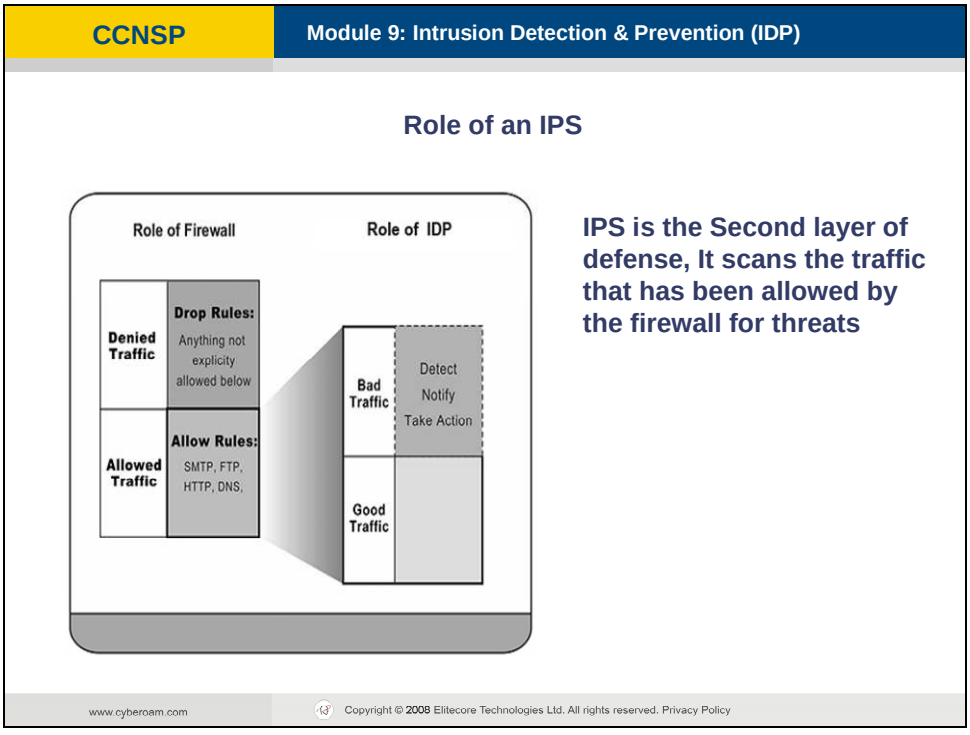


Top Mail Senders



Module 9: Intrusion Prevention System (IPS)

IPS Basics:



Intrusion Detection System (IDS):

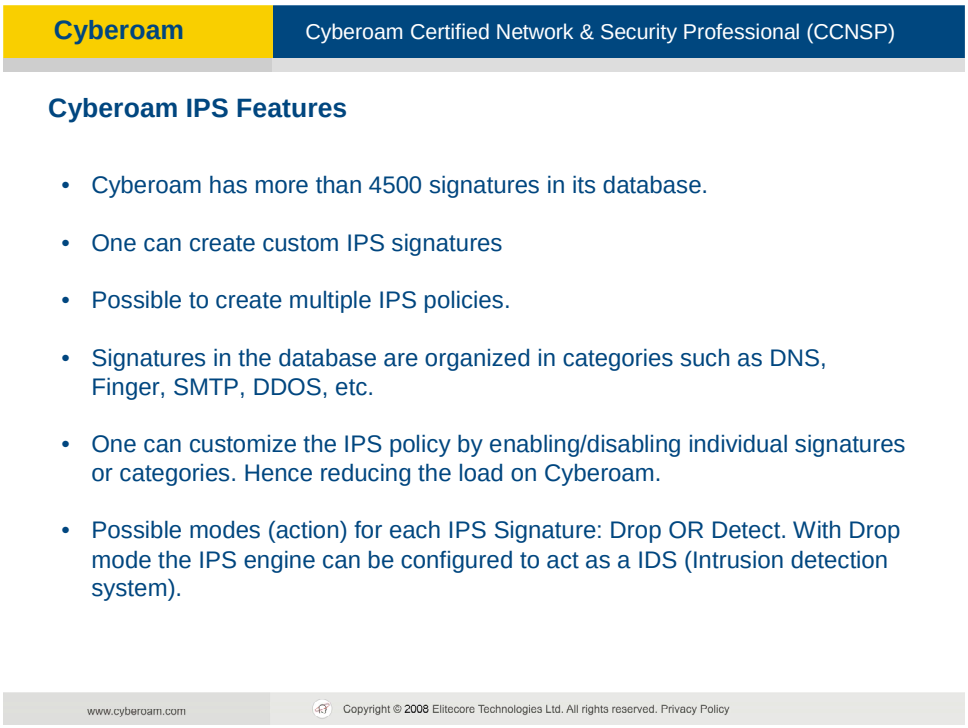
An **Intrusion Detection System** (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place − not prevent them. An IDS essentially reviews your network traffic and data and will identify probes, attacks, exploits and other vulnerabilities. IDS can respond to the suspicious event in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. In some cases the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion. An IDS specifically looks for suspicious activity and events that might be the result of a virus, worm or hacker. This is done by looking for known intrusion signatures or attack signatures that characterise different worms or viruses and by tracking general variances which differ from regular system activity. The IDS is able to provide notification of only known attacks.

Intrusion Prevention System (IPS):

An **Intrusion Prevention System** is a null computer security device that monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent those activities. Network-based IPS, for example, will operate in-line to monitor all network traffic for malicious code or attacks. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Intrusion prevention technology is considered by some to be an extension of intrusion detection (IDS) technology.

Firewall works as privilege that is provide the host or the user to access particular resources, IPS is the second layer of defence that scans the traffics that has been allowed by firewall for threats.

Cyberoam IPS Features:



Cyberoam IPS also uses Signatures to identify the malicious activity on the network but instead of providing only one policy (global) for managing multiple networks/hosts, allows to tailor the policy per network/host i.e. allows to defining multiple policies for managing multiple networks/hosts.

Cyberoam IPS consists of a signature engine with a predefined database of signatures. Predefined signatures are not editable.

As per your network requirements, Cyberoam allows you to define multiple policies instead of one global policy, to decrease packet latency and reduce false positives.

Policy allows you to view Cyberoam predefined signatures and customise the intrusion prevention configuration at the category as well as individual signature level. Categories are signatures grouped together based on the application and protocol vulnerabilities.

Each IPS policy contains a set of signatures that the Cyberoam searches for, and log and block and allows to:

- Enable or disable category from IPS protection
- Enable or disable individual signature in a category to tailor IPS protection based on your network environment
- Define the action to be taken when the matching traffic pattern is found. Cyberoam can either detect or drop the connection. In either of the case, Cyberoam generates the log and alerts the Network Administrator.

To enable the Intrusion Prevention System functionality, apply the policy using firewall rule.

You can create rule to apply

- Single policy for all the user/networks
- Different policies for different users/networks or hosts

As firewall rules control all traffic passing through the Cyberoam, and decides whether to allow or drop the connection, IPS policy will be applied to only that traffic/packet which firewall passes.

IPS Signatures

Cyberoam has more than 4500 signatures in its database. One can create custom IPS signatures, for the one that is not included in our database. Signatures are organised in categories such as DNS, Finger, DDOS and many more.

One can disable the particular category or a signature inside it. Moreover, in a particular Category, Cyberoam has two IPS modes:

- Drop
- Detect

Drop mode - If IPS is enabled in Drop mode, Cyberoam-IPS automatically drops and resets the connection and prevents the traffic to reach its destination, if detects any traffic that matches the signature.

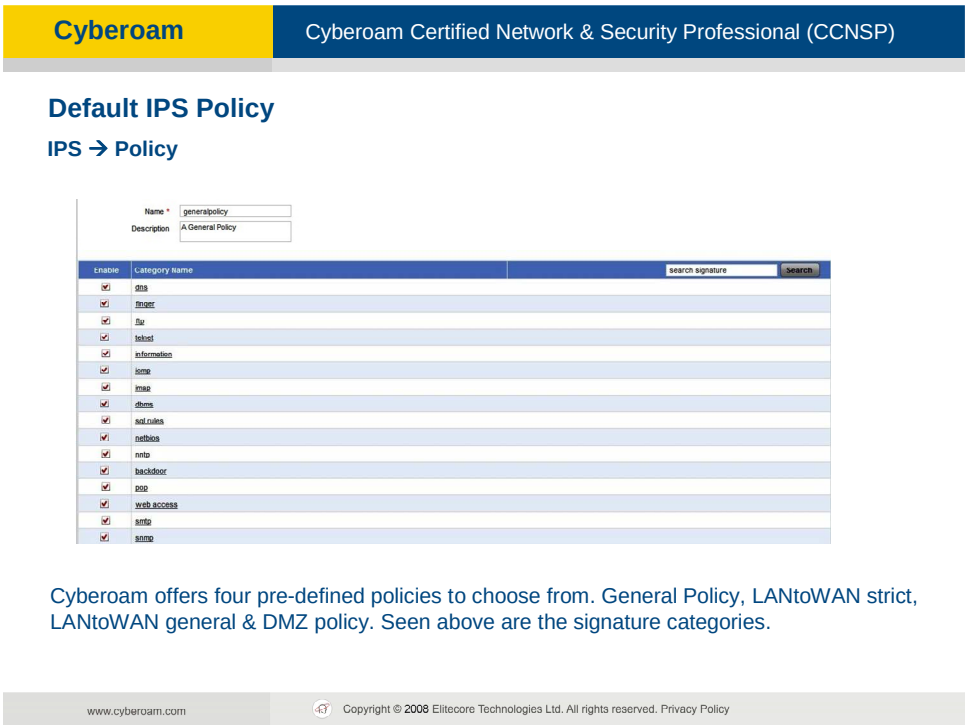
Detect mode - If IPS is enabled in Detect mode for a signature, Cyberoam-IPS detects and logs any traffic that matches the signature, but does not take any action against the traffic and the connection proceeds to its intended destination.

Cyberoam provides alert in both the IPS modes and notify the action taken by it and the user who was trying to access to.

These signature categories are listed in the policy.

You will find IPS signature under, IPS → Policy → Create/Manage policy

IPS Policies:

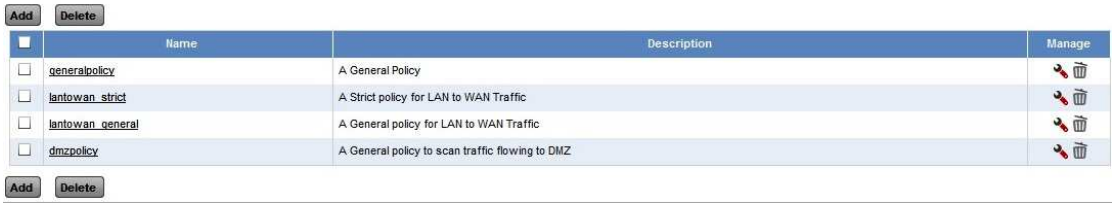


IPS policy consists of signature categories. Signature categories can be enabled or disabled as per traffic requirement.

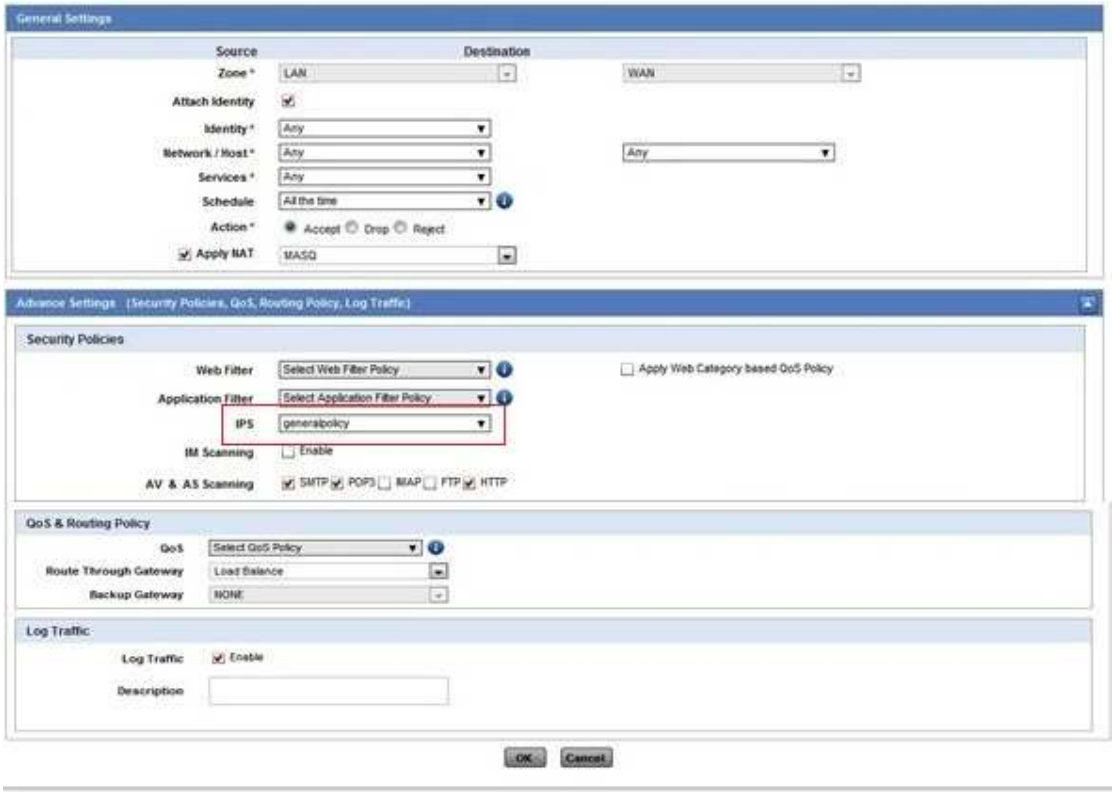
Cyberoam provides following default IPS policies:

1) generalpolicy
2) lantowan policy
3) lantowan general
4) dmzpolicy

IPS policies can be customised as per need. Default policies are located under IPS → Policy



IPS Policy can be applied to firewall rule for protection. Below example shows you how to apply IPS policy in firewall rule:



Create custom IPS policy and select set of categories based on application / user requirement.

Custom IPS Signature:

Custom signatures provide the flexibility to Customise IPS for diverse network environments. Default signatures included in Cyberoam cover common attacks while custom signatures protect your network from uncommon attacks that are due to the use of proprietary server, custom protocol, or specialized applications used in the corporate network.

Create custom signature to define custom IPS signatures for your own network and use to allow or block specific traffic.

Select **IPS → Custom Signature → Add**

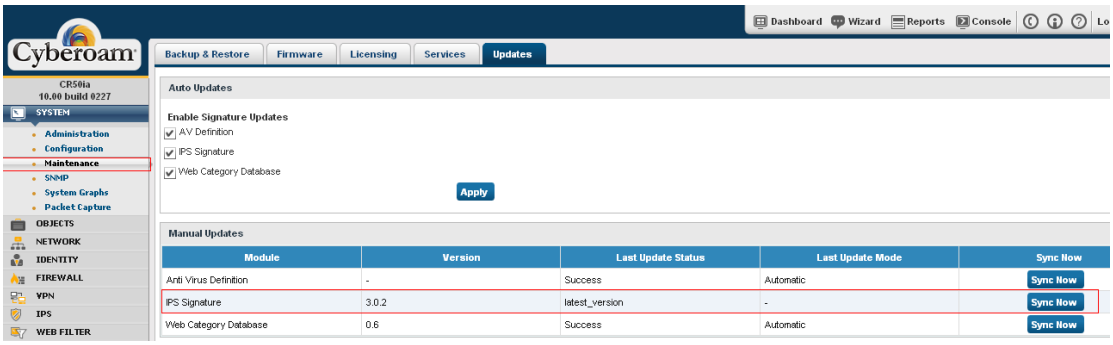
Refer Cyberoam knowledge based article for more information about custom IPS signature: http://kb.cyberoam.com/default.asp?id=393&SID=&Lang=1

Upgrade

Cyberoam IPS gets upgraded automatically once in a week, no manual assistance is required.

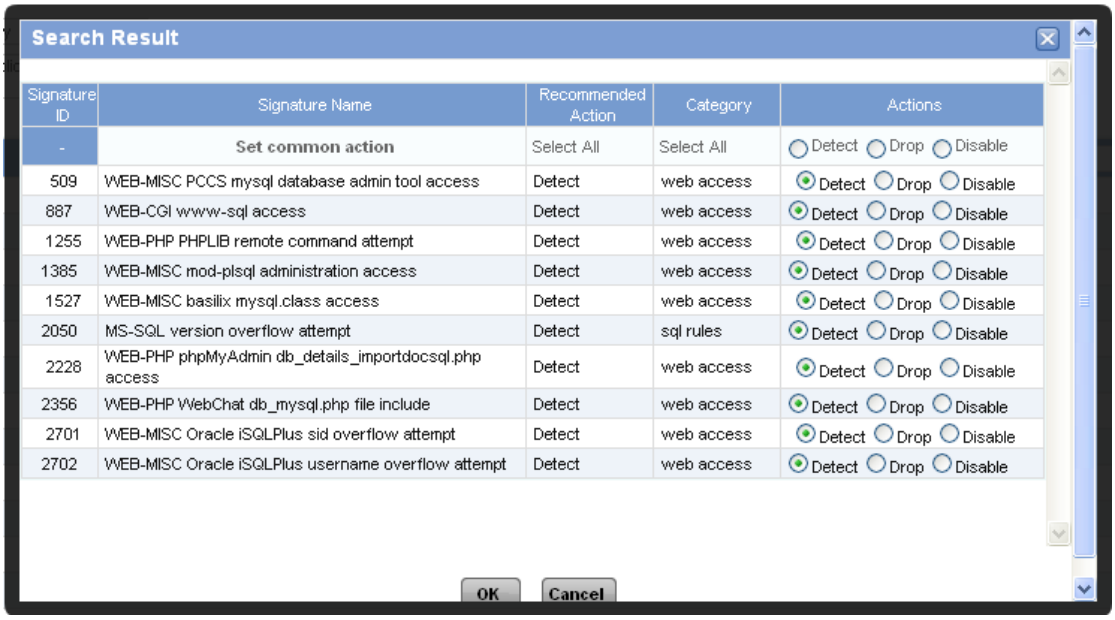
One can check the status of the upgrade from System → Maintenance → Updates

The detail includes version number, last update attempt and last update status.



With the use of Signature Identification (SID), one can get the detail idea about the alerts.

Go to IPS → Policy → Open the policy → Enter the SID or Signature Name in search

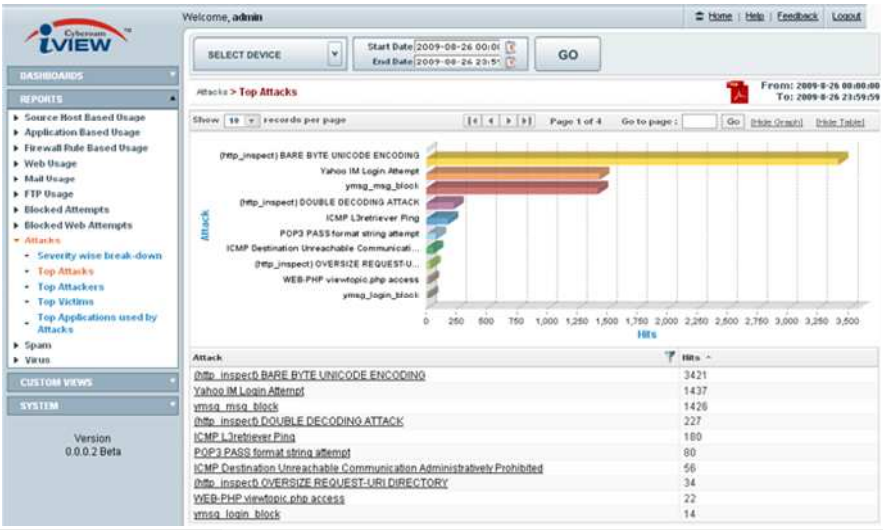


The detail report on IPS is provided while navigating from Reports → IPS.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

IPS Reports

Reports → Attacks (IPS)



Module 10: Virtual Private Network (VPN)

Cyberoam | Unified Threat Management

VPN Basics

What is VPN?

- A Virtual Private Network is a tunnel that carries private network traffic from one endpoint to another over a public network such as the Internet.
- The traffic is unaware about the intermediate hops between the endpoints.
- Similarly the intermediate hops are unaware that they are carrying the network packets that are traversing the tunnel.
- The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and a measure of security.

Advantages:

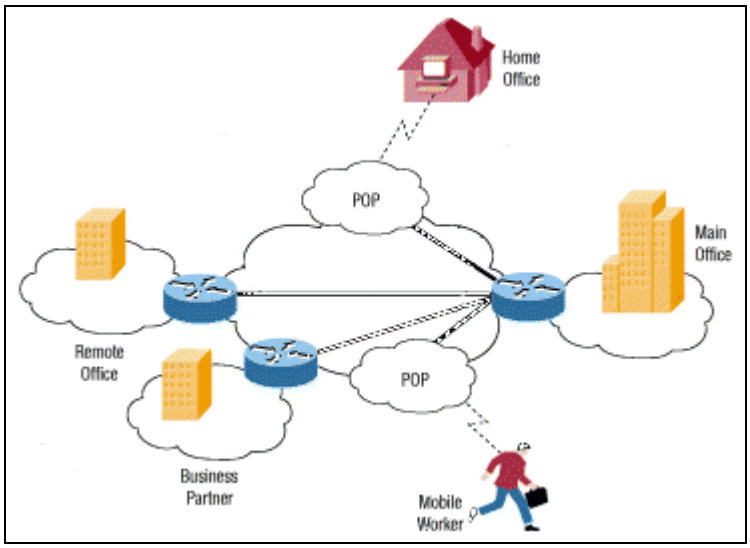
- To extend communications to regional and isolated offices
- To establish secure links with business partners
- To significantly decrease the cost of communications for an increasingly mobile workforce.
- To transform the daily method of doing business faster than any other technology.

www.cyberoam.com

VPN Basic

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organisation. The goal of a VPN is to provide the organisation with the same capabilities, but at a much lower cost.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunnelling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.



A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.

In a similar term, VPN is a private network uses public network (i.e. the internet to connect to remote sites to access the resources.)

Points to Summarise:

- VPN extends communications to regional and isolated offices
- It establish secure links with business partners
- It significantly decreases the cost of communications for an increasingly mobile workforce.
- To transform the daily method of doing business faster than any other technology

Cyberoam | Unified Threat Management

IPSec Protocol Basics

www.cyberoam.com

IPSec Protocol Basics

IPSec is framework that is built into various security products to provide end-to-end security in wide area networking communications. Using strong encryption, and public key cryptography, IPSec can secure data links that would otherwise be insecure and susceptible to exploitation.

IPSec is a bundle of protocols and algorithms and is a flexible framework that allows vendors who build it into their products to select the algorithms, keys, and authentication methods they want to use. One should assume that two different implementations of IPSec are not necessarily the same as far as protocols and algorithms go.

Cyberoam uses the following bundle of protocols, hashing, and encryption algorithms in IPSec:

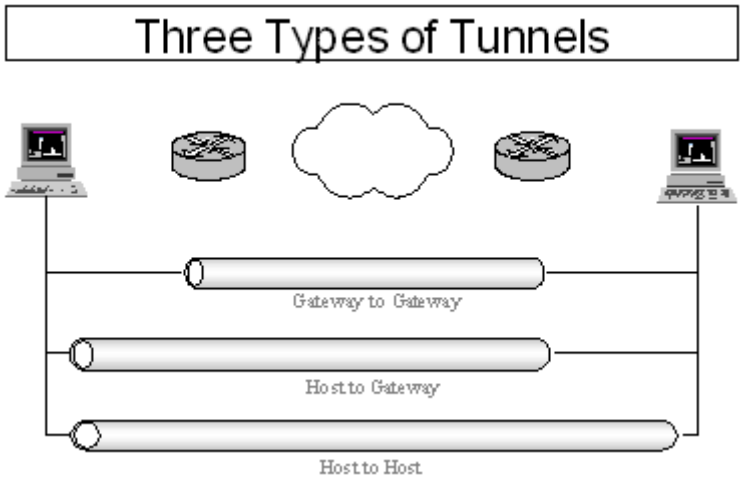
* IKE [Internet Key Exchange protocol]
* ISAKMP [Internet Security Association and Key Management Protocol]
* ESP [Encapsulating Security Payload]
* AH [Authentication Header protocol]
* ESP [Encapsulating Security Payload protocol]
* TwoFish/BlowFish
* HMAC [Hash Message Authentication Code]
* MD5 [Message Digest 5]
* SHA-1 [Security Hash Algorithm]
* 3DES [Triple Data Encryption Standard]
* Serpent
* XAUTH [Extended Authentication]
* AES [Advanced Encryption Standard]

To understand IPSec better, the two protocols worth understanding first are AH and ESP. AH is used to authenticate users, and ESP applies cryptographic protections that provide authentication, integrity, and confidentiality of messages.

There are two modes of operation for IPSec: transport mode and tunnel mode. In transport mode, only the payload of the message is encrypted. In tunnel mode, the payload, the header, and the routing information are all encrypted. Needless to say, using IPSec is transport mode is far more risky that using it in tunnel mode.

There are three types of Tunnels:

1) Host to Gateway (Remote Access)
2) Gateway to Gateway (Site-to-Site)
3) Host to Host



Transport mode only supports Host to Host connectivity.

IPSec VPNs are network connections that are based on public and private key cryptography. Users of IPSec implementations are issued public keys and private keys that are associated with their respective identity. When a message is sent from one user to another, it is automatically signed with the user's private key. The receiver uses the sender's public key to decrypt the message. VPN endpoints essentially act as databases that manage and distribute keys and security associations in similar ways that a Certificate Authority (CA) does.

How IPSec Works

IPSec negotiates between two machines on a connection using the UDP protocol from port 500 and port 4500 if IPSec NAT traversal is used.
IPSec involves many component technologies and encryption methods. Yet IPSec's operation can be broken down into five main steps:

1. "Interesting traffic" initiates the IPSec process. Traffic is deemed interesting when the IPSec security policy configured in the IPSec peers starts the IKE process.
2. IKE phase 1. IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.
3. IKE phase 2. IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers.
4. Data transfer. Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. IPSec tunnel termination. IPSec SAs terminate through deletion or by timing out.

Benefits of IPSec

IPSec is typically used to attain confidentiality, integrity, and authentication in the transport of data across insecure channels. Though, it's original purpose was to secure traffic across public networks, it’s implementation are often used to increase the security of private networks as well, since organisations cannot always be sure if weaknesses in their own private networks are susceptible to exploitation. If implemented properly, IPSec provides a private channel for sending and exchanging vulnerable data whether the data is email, ftp traffic, news feeds, partner and supply chain data, medical records, or any other type of TCP/IP based data.

Cyberoam | Unified Threat Management

L2TP Protocol Basics

L2TP Protocol Basics

L2TP acts like a data link layer (layer 2 of the OSI Model) protocol for tunnelling network traffic between two peers over an existing network (usually the Internet). L2TP is in fact a layer 5 protocol sessions and uses the registered UDP port 1701. The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPSec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPSec.

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this L2TP session is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP.

The packets exchanged within an L2TP tunnel are categorised as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel.

L2TP, Layer 2 Tunnelling Protocol, is used to provide IP security at the network layer.

A L2TP based VPN is made up by these parts:

- Point-to-Point Protocol (PPP)
- Authentication Protocols (PAP, CHAP, MS-CHAP v1, MS-CHAP v2)
- Microsoft Point-To-Point Encryption (MPPE)

L2TP uses UDP to transport the PPP data; this is often encapsulated in IPSec for encryption instead of using MPPE.

Note: Cyberoam L2TP VPN only supports PAP for authentication.

Cyberoam | Unified Threat Management

PPTP Protocol Basics

www.cyberoam.com

PPTP Protocol Basics

PPTP is a network protocol used in the implementation of Virtual Private Networks (VPN). RFC 2637 is the PPTP technical specification.

PPTP works on a client server model. PPTP clients are included by default in Microsoft Windows and also available for both Linux and Mac OS X. Newer VPN technologies like L2TP and IPSec may replace PPTP someday, but PPTP remains a popular network protocol especially on Windows computers.

PPTP technology extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP operates at Layer 2 of the OSI model. As a network protocol, PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking.

PPTP, Point-to-Point Tunnelling Protocol, is used to provide IP security at the network layer.

A PPTP based VPN is made up by these parts:

- Point-to-Point Protocol (PPP)
- Authentication Protocols (PAP, CHAP, MS-CHAP v1, MS-CHAP v2)
- Generic Routing Encapsulation (GRE)
- Microsoft Point-To-Point Encryption(MPPE)

PPTP uses TCP port 1723 for its control connection and GRE (IP protocol 47) for the PPP data. PPTP supports data encryption by using MPPE.

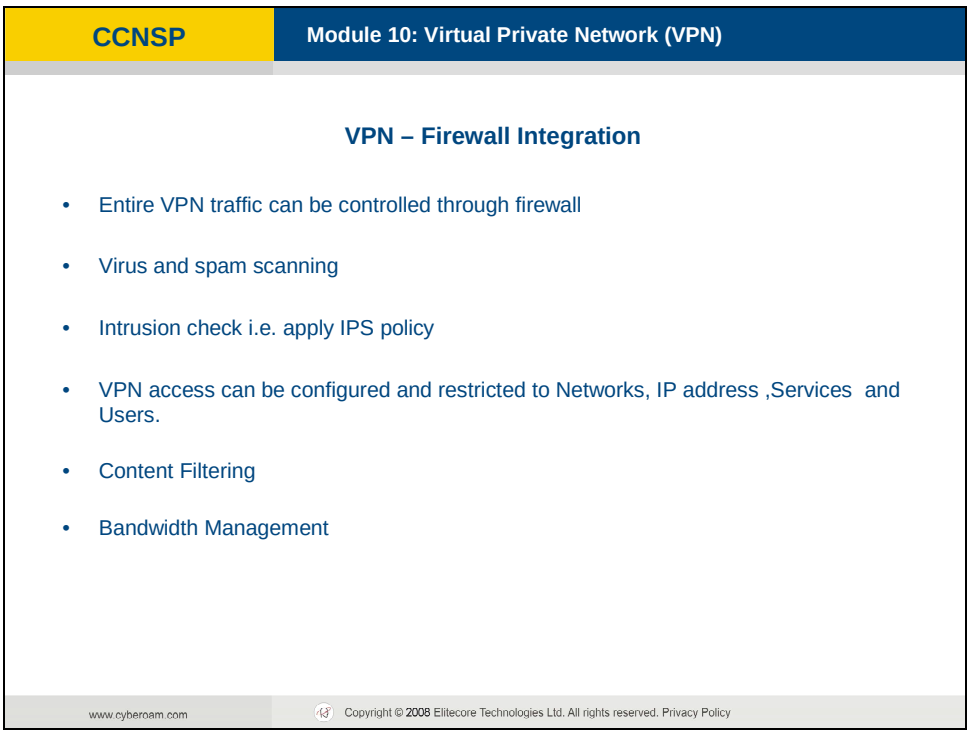
Note: Cyberoam PPTP VPN only supports PAP for authentication.

Cyberoam | Unified Threat Management

Cyberoam VPN Features

www.cyberoam.com

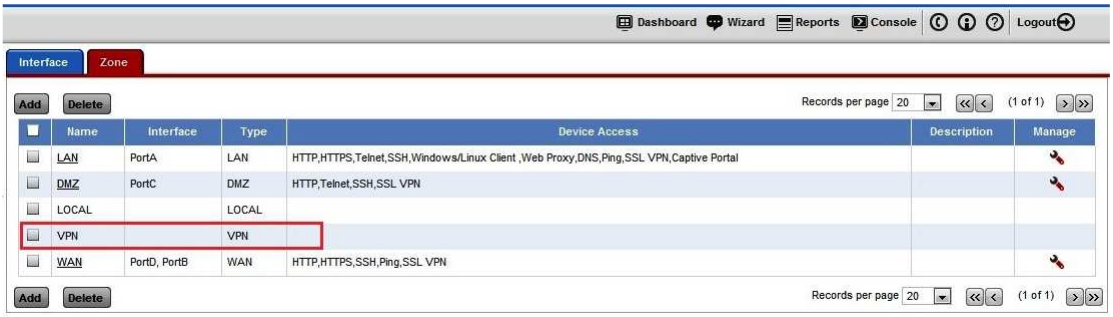
Cyberoam VPN Features



With the threat free tunneling, firewall rules can be applied even to the VPN traffic resulting into the clean VPN traffic. In other words, VPN traffic coming in or out of the tunnels will be Threat Free since it would have been scanned for viruses, spam, intrusion attempts, inappropriate web content and unwanted network applications.

The major features of TFT-VPN are:

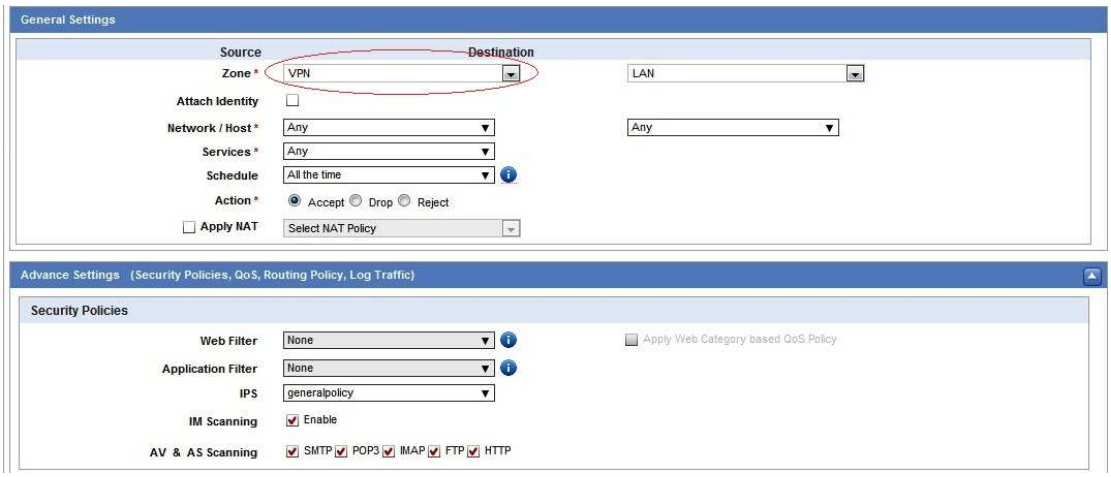
Cyberoam Default VPN zone:

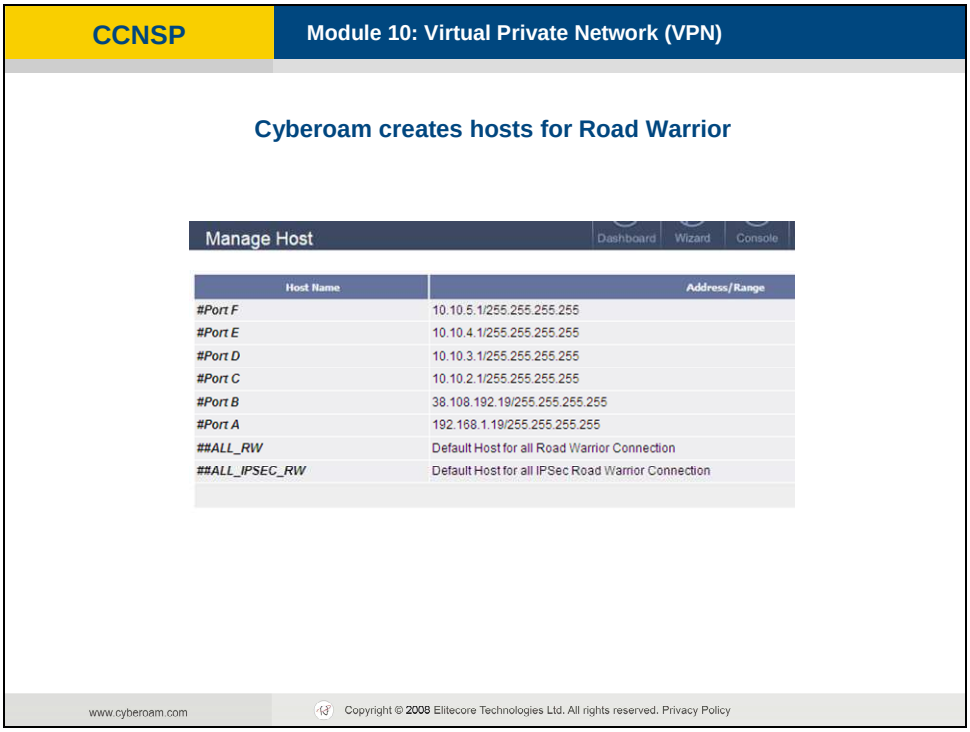


Cyberoam creates VPN zone which is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical port/interface. Whenever the VPN connection is established, port/interface used by the connection is automatically added to this zone and on disconnection; port is automatically removed from the zone.

To implementing threat free tunneling, one has to apply following policies to the VPN zone from firewall rule to:

- Virus and spam scanning i.e. apply virus and spam policy to block viruses from entering your network
- Intrusion check i.e. apply IPS policy





Host list displays dynamic hosts and host groups which are automatically added on creation of VPN Remote Access connections. It will also display the default hosts created for Remote Access connection - ##ALL_RW, ##ALL_IPSEC_RW.

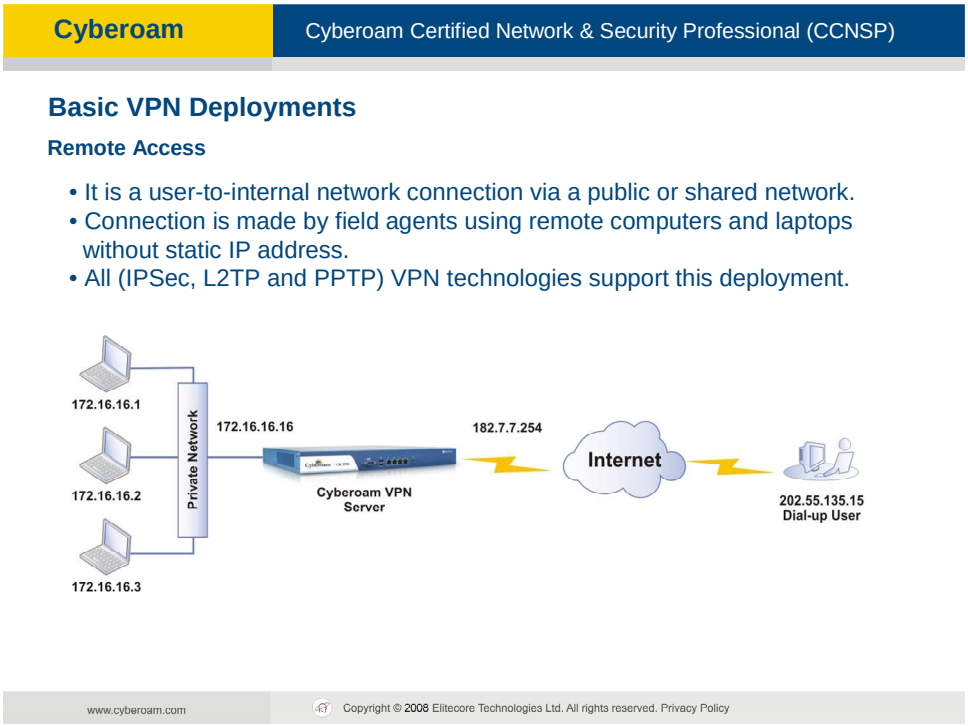
Default VPN Firewall Rules:

Cyberoam provides following two types of VPN connections:

Remote Access

A Remote Access is simply a machine that is out on the internet somewhere, which may or may not have a static IP address, and wishes to communicate back to the office. The most common example of this situation is that of a laptop dialled up to some ISP. This is perhaps the simplest case, and is not very hard to setup.

IPSec, L2tp and PPTP VPN technologies support Remote Access deployment.

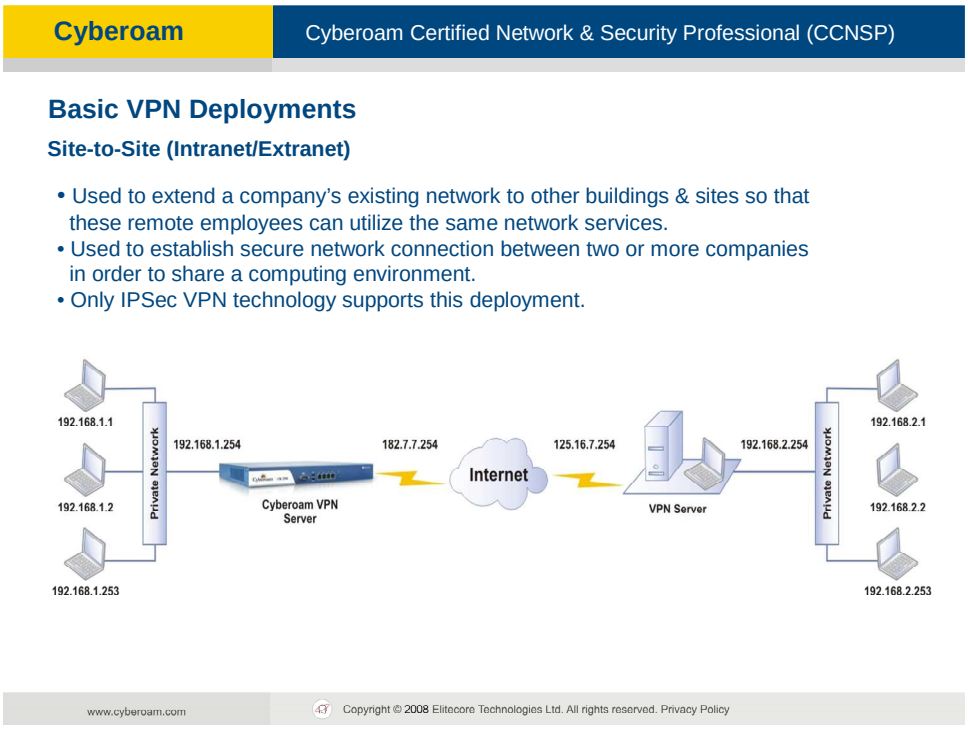


Site-to-Site

Site-to-Site VPN is a secure form of communication between computer networks. It provides confidentiality of the data in transit through the use of encryption. Additionally, it allows the user on one side to have a high confidence level in the identity of the user on the other side through the use of authentication mechanisms.

The technology also provides data integrity, ensuring that the data received is exactly the same as data sent. This type of VPN does not require client software to be loaded on either end of the VPN. Since the technology is embedded on Cyberoam, neither user accounts nor logging in is required.

This can be only achieved through IPSec.



Cyberoam VPN Technology Comparison

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam VPN Technology Comparison Matrix

- The following table compares all VPN Technologies supported by Cyberoam and will help to make decision which VPN Technology to be used

VPN Technology	Security level	Deployment Requirement
IPSec	High	This can be deployed in Remote Access and Site-to-Site scenario. In case of Remote Access, Cyberoam VPN Client is required and it's a licensed product. In case of Site-to-Site, Cyberoam is compatible with all major VPN Gateways those supports standard IPSec architecture.
SSL-VPN	High	This can be deployed in Remote Access or can be used as a web based portal without installing any SSL-VPN client SSL-VPN client is free of cost.
L2TP	High	This can be deployed in Remote Access scenario only. No third party VPN client required as Windows 2000 onward all OS have inbuilt L2TP VPN Client.
PPTP	Moderate	This can be deployed in Remote Access scenario only. No third party VPN client required as all windows OS have inbuilt PPTP VPN Client.

www.cyberoam.com

SSL VPN:

The VPN feature is extended to include SSL VPN functionality within Cyberoam to provide secure access for the remote users. It delivers set of features and benefits to make them easier to use and control to allow access to the corporate network from anywhere, anytime.

It provides the ability to create point-to-point encrypted tunnels between remote employees and your company's internal network, requiring combination of SSL certificates and a username/password for authentication to enable access to the internal resources.

In addition, it offers a secure web portal, which can be accessed by each authorized user to download a free SSL VPN client, SSL certificates and a client configuration.

It offers granular access policies, bookmarks to designated network resources and portal customization.

To restrict the access to the Corporate network, it operates in two modes: Full Access and Web Access mode.
Web access – for the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise Web applications/servers through web browser only. In other words, it is a clientless access.

Full access – for the remote users who are to be provided with the Corporate network access from laptops, Internet cafes, hotels etc. It requires an SSL VPN Client at the remote end. Remote users can download and install SSL VPN Client from the End-user Web Portal.

The basic and common administrative configuration for both the modes of operation can be configured from the Global settings and portal settings.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

On-Appliance SSL VPN

- Cyberoam VPN includes SSL VPN functionality within the appliance to provide secure access for the remote users.
- Easier to use and control to allow access to the Corporate network from anywhere, anytime.
- Any device that has browser can access SSL VPN.
- It provides the ability to create point-to-point encrypted tunnels between remote employees and your company's internal network.
- It requires a combination of SSL certificates and a username/password for authentication to enable access to the internal resources.
- To restrict the access to the Corporate network, it operates in two modes: Full Access and Web Access mode.
- User's access to private network is controlled through his SSL VPN policy while Internet access is controlled through his Internet Access policy.

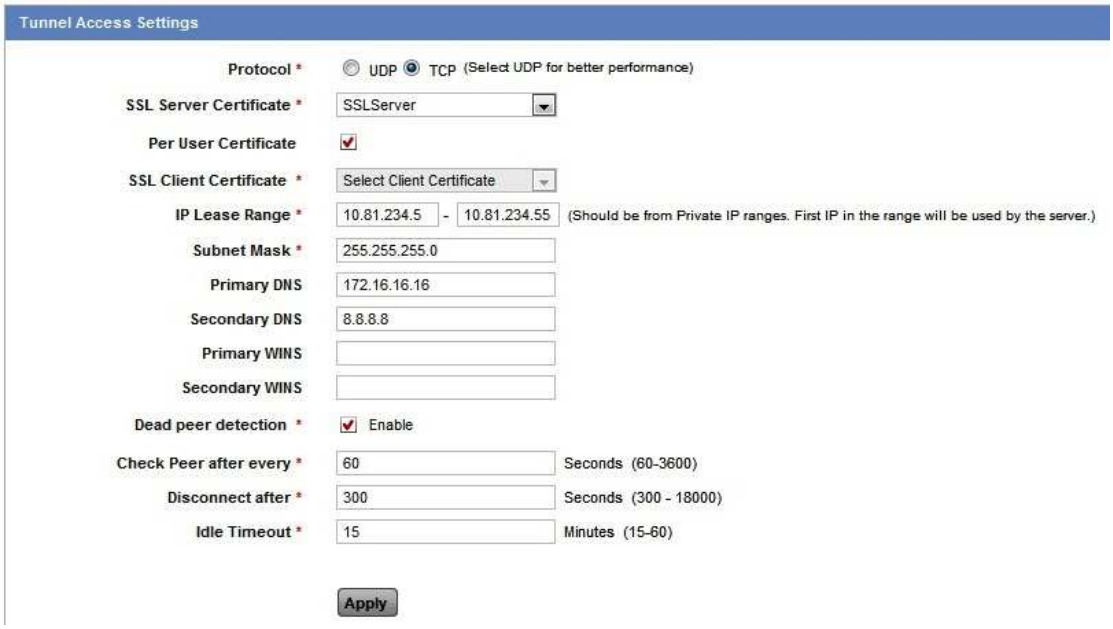
Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Cyberoam SSL-VPN Features

- Client and Location independent access
- Authentication - AD, LDAP, RADIUS, Cyberoam
- Multi-layered Client Authentication - Certificate, Username/Password
- User & Group policy enforcement
- Network access - Split and Full tunneling
- End user Web Portal - Clientless access
- SSL VPN Tunneling Client - Granular access control to all the Enterprise Network resources
- Administrative controls: Session timeout, Dead Peer Detection,
- Portal customization

• The SSL VPN feature would not be a chargeable module and would be enabled by default in all appliances 25i, 50i,100i, 200i, 300i, 500i, 1000i and 1500i.

SSL VPN Global Settings: SSL VPN → Global Settings



SSL VPN → Global Setting page allows you to configure certain parameters globally for both the type of Access.

Select SSL Server certificate from the dropdown list to be used for authentication. If you do not have certificate, generate certificate signing request (CSR) using the default CA from Objects → Certificate → Add

The selected certificate is bundled with the Client installer and is downloaded when remote users install SSL client. Remote users/SSL Clients represent the selected certificate to the server for authenticating themselves. Same certificate can be used for both SSL Server and Client.

Bookmarks: SSL VPN → Bookmark → Add

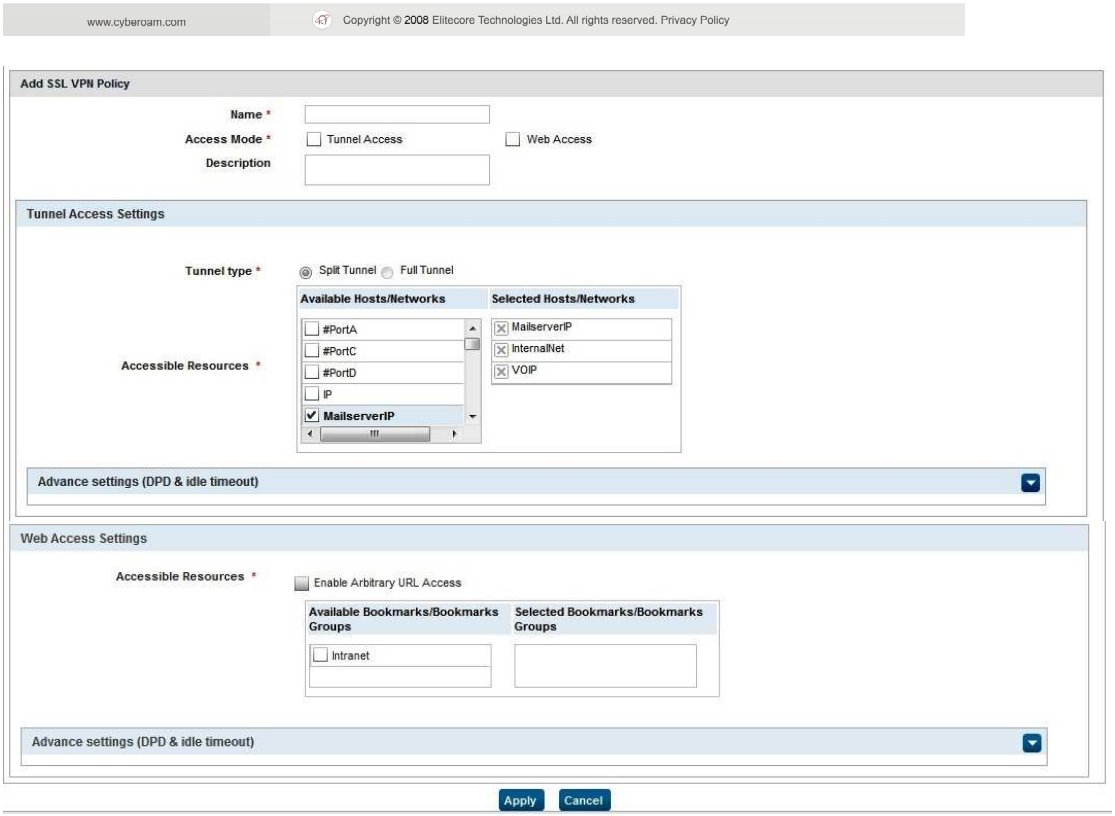
Bookmarks are the resources whose access will be available through End-user Web portal. These resources will be available in “Web Access” mode only and is to be configured in SSL VPN Policy.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

SSL-VPN Modes

Web Access & Full Access Mode

- **Web Access mode (Web based or clientless)**
  - Does not require any client to be installed
  - Can be accessed using browser
  - Limited to use on web resources only
- **Full Access mode (Client mode)**
  - Require client to be installed
  - Works in two modes
    - Split Tunnel
      - » Allows access to only defined network resources in the policy
    - Full Tunnel
      - » Routes all traffic to Cyberoam, internet through HO
      - » Allows access to only defined internal network resources
      - » Full access to WAN



Select the access mode by clicking the appropriate option

Available options

Full Access mode – for the remote users who are to be provided with the Corporate network access from laptops, Internet cafes, hotels etc. It requires an SSL VPN Client at the remote end. Remote users can download and install SSL VPN Client from the End-user Web Portal.

Web access – for the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise Web applications/servers through web browser only. It provides clientless network access using any web browser through End-user Web Portal. Remote users are authenticated by Cyberoam and redirected to the End-user Web Portal through which Enterprise Web applications/servers can be accessed.

By default, only Full access mode is enabled.

Under Full Access Setting:

Select tunnel type. Tunnel type determines how the remote user's traffic will be routed.
Split tunneling ensures that only the traffic for the private network is tunneled and encrypted while in full tunneling private network traffic as well as other Internet traffic is also tunneled and encrypted.

By default, split tunnel is enabled.

Accessible Resources allows restricting the access to the certain hosts of the private network. User's access to private network is controlled through his SSL VPN policy while Internet access is controlled through his Internet Access policy.

'Available Host/Network' list displays the list of available hosts and network. All the hosts added from Firewall, Add Host page will be displayed in the list.

End Client SSL VPN access:

Remote users can download SSL VPN client, and Configuration file from the portal. All the downloadable components will be displayed only if the remote user is allowed the "Full" access

Remote user will be displayed the list of all the bookmarks. User will also be displayed the URL Address bar if allowed in the User SSL VPN policy. User can type the URL in the Address bar to access other URLs than bookmarks.

The user logs in through the client login page:

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

SSL-VPN Portal

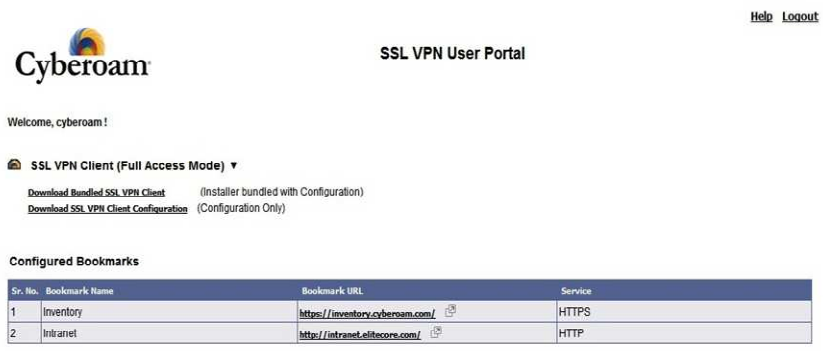
SSL-VPN users authenticate on the portal with their username/password. If Cyberoam is integrated with external authentication server, the user needs to enter the credentials accordingly.

SSL VPN User Portal:

User can access the resources allotted to him:

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

SSL-VPN Portal (Welcome Page)



Once logged into the portal the users get access to the bookmarks & the link to download the configuration file required for tunnel mode access.

Lab #22 IPSec Remote Access Configuration using Pre-Shared Key

Objective:

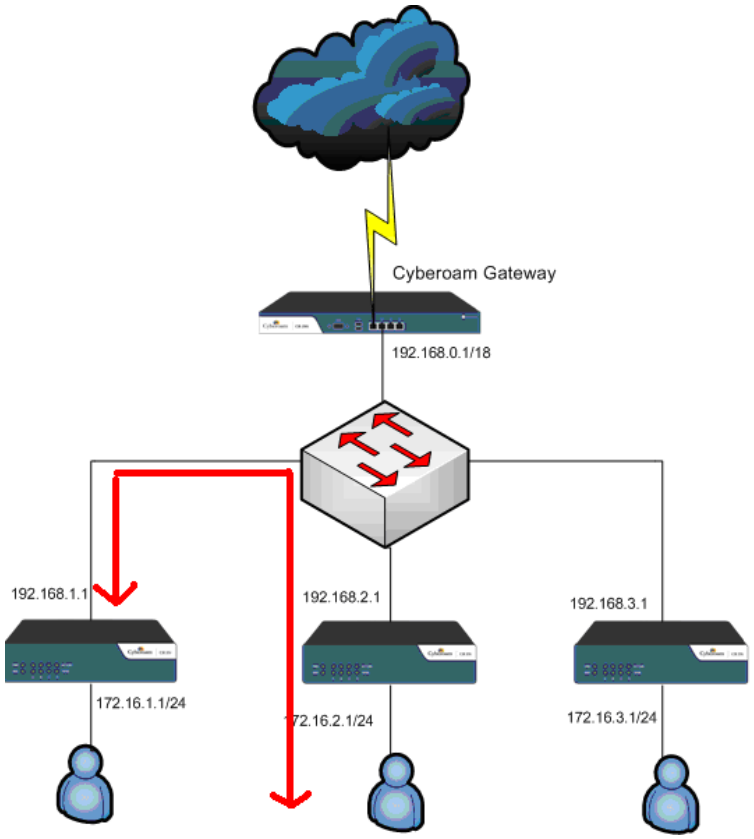
Setup Cyberoam IPSec Remote Access connection configuration using pre-shared key.

IPSec Remote Access VPN client is license product. One can download the 30 days evaluation copy of this software from http://www.cyberoam.com/vpnhelp.html.

Lab activities:

1. IPSec Remote Access Connection Configuration
2. Export IPSec Connection Parameters
3. Activate Connection
4. VPN Client Configuration
5. Establish the Connection

We are going to setup IPSec Remote Access connection under below Lab setup:



Below table shows VPN configuration parameter for IPSec connection:

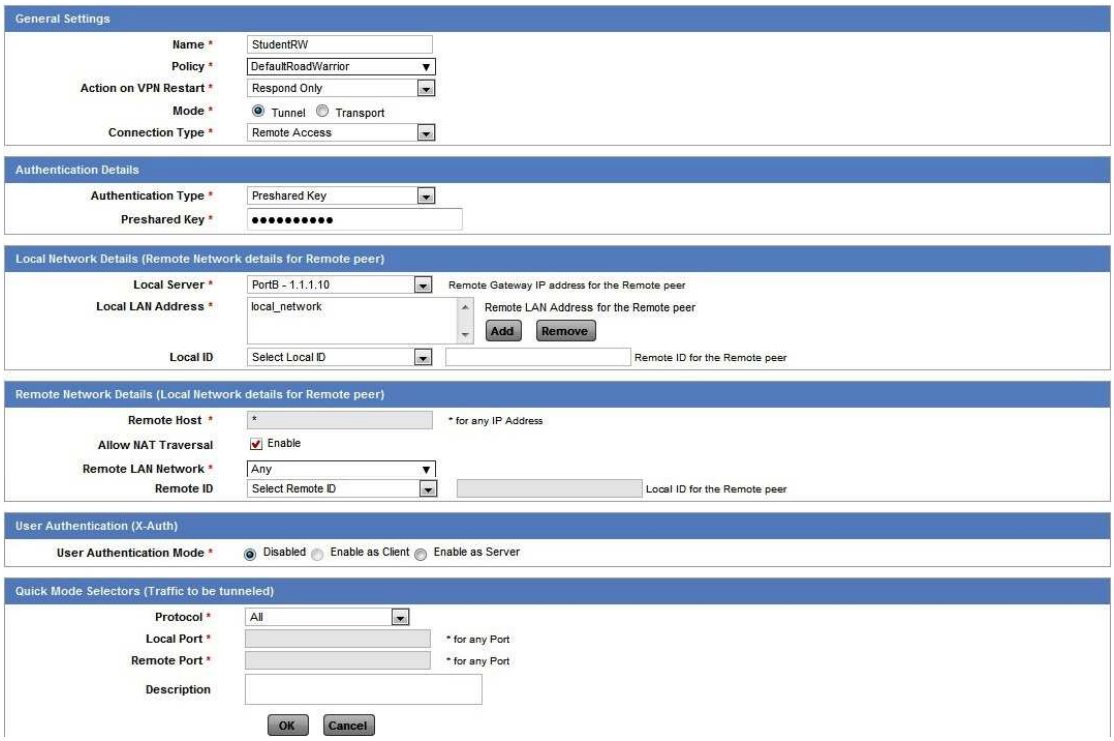
Configuration Parameters	Cyberoam	Cyberoam VPN Client
IPSec Connection (Remote Access)	**Local Network details**	**Local Network details**
	Cyberoam WAN IP address – 192.168.1.1	VPN Client IP address – *
	Local Internal Network – 172.16.1.0/24	Local Internal Network – 0.0.0.0/0
	Preshared Key - 0123456789	Preshared Key – 0123456789
	Remote Network details	**Remote Network details**
	Remote VPN server – IP address – *	Remote VPN server – IP address – 192.168.1.1
	Remote Internal Network – 0.0.0.0/0	Remote Internal Network – 172.16.1.0/24

Lab #24 IPSec Remote Access Configuration
Activity 1: IPSec Remote Access Connection Configuration

Create IPSec Remote Access connection from:

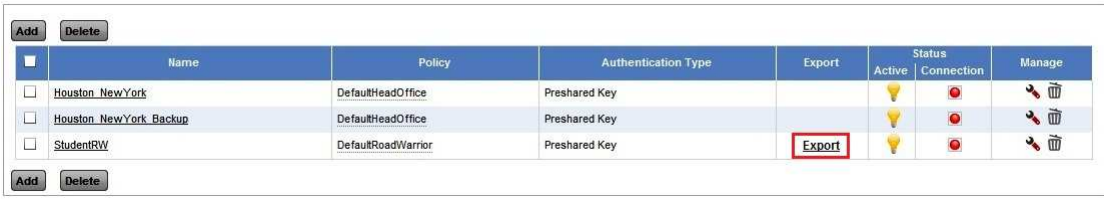
VPN → IPSec Connection → Create Connection

Select default IPSec Remote Access policy "**DefaultRoadWarrior**" and specify parameters as per below screen shot



Lab #24 IPSec Remote Access Configuration
Activity 2: Export IPSec Connection Parameters

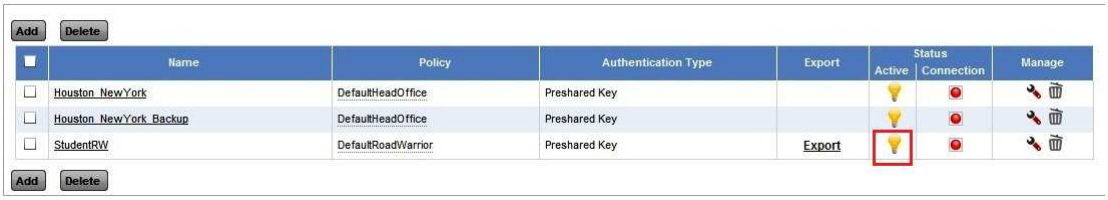
Go to **VPN → IPSec** and click Export against the connection whose detail is to be exported and used for connection. Cyberoam will prompt to save the connection parameter in the tgb format. Save and mail the saved file to the remote user.



Lab #24 IPSec Remote Access Configuration
Activity 3: Activate Connection

Go to **VPN → IPSec**

To activate the connection, click  button under Connection Status against the Student1RW connection



Note

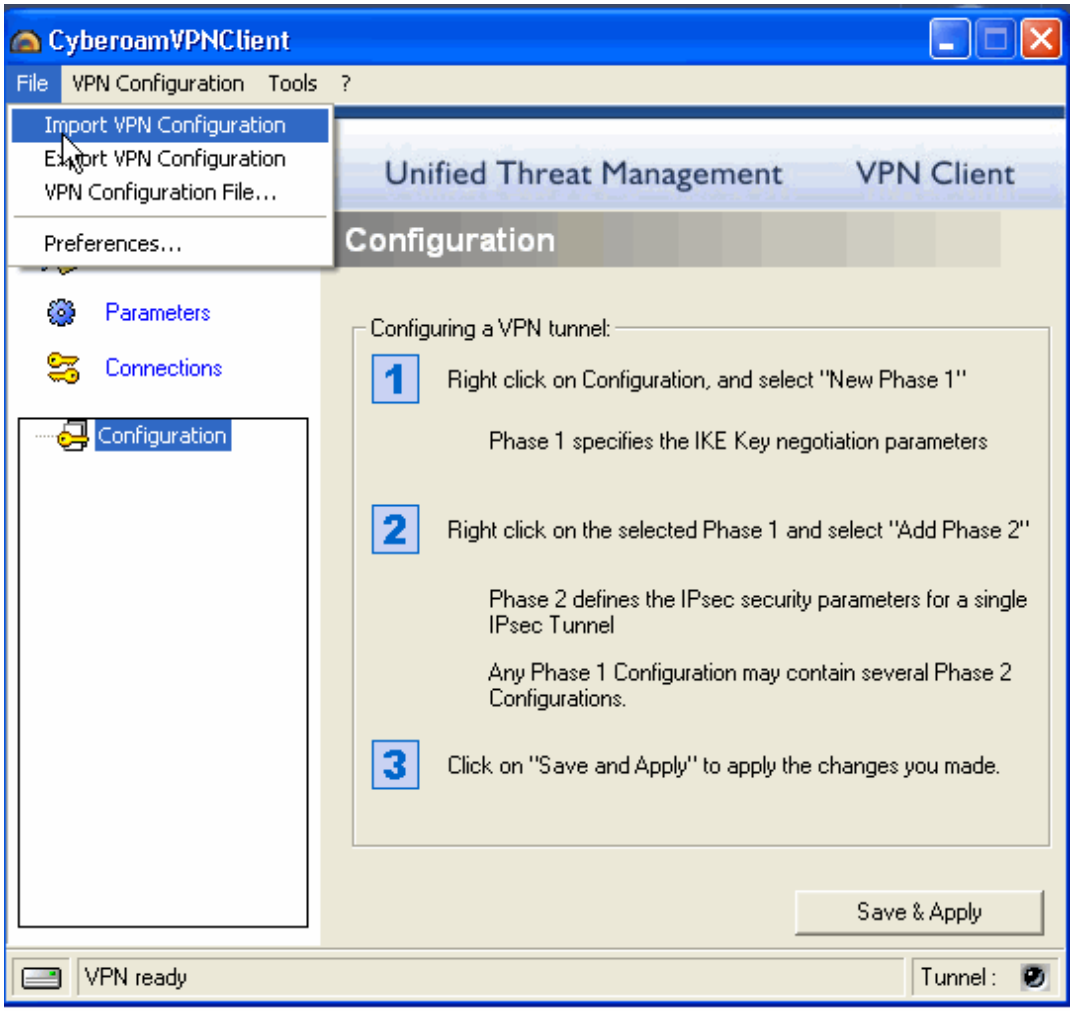
At a time only one connection can be active if both the types of connection - Digital Certificate and Pre-shared Key - are created with the same source and destination. In such situation, at the time of activation, you will receive error 'unable to activate connection' hence you need to deactivate all other connections.

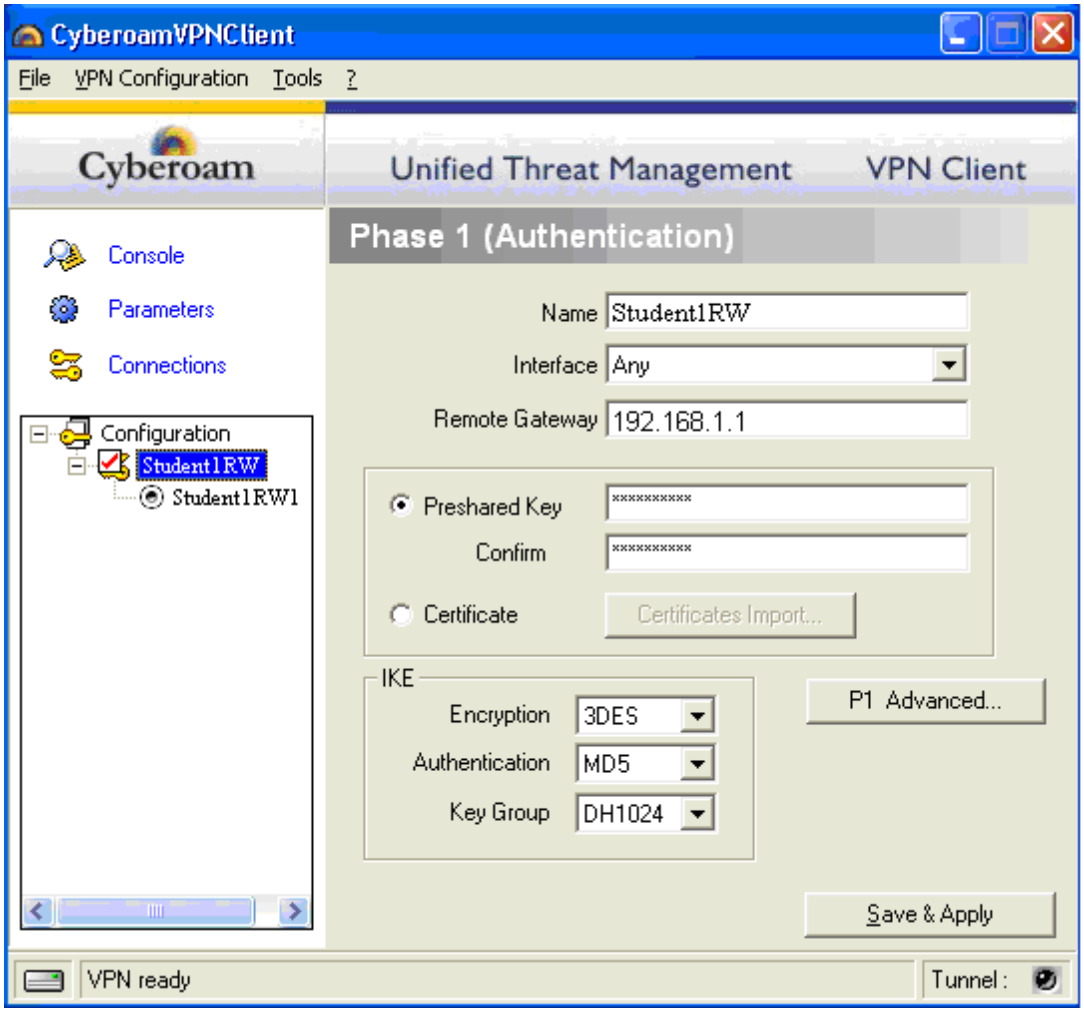
Lab #24 IPSec Remote Access Configuration
Activity 4: VPN Client Configuration

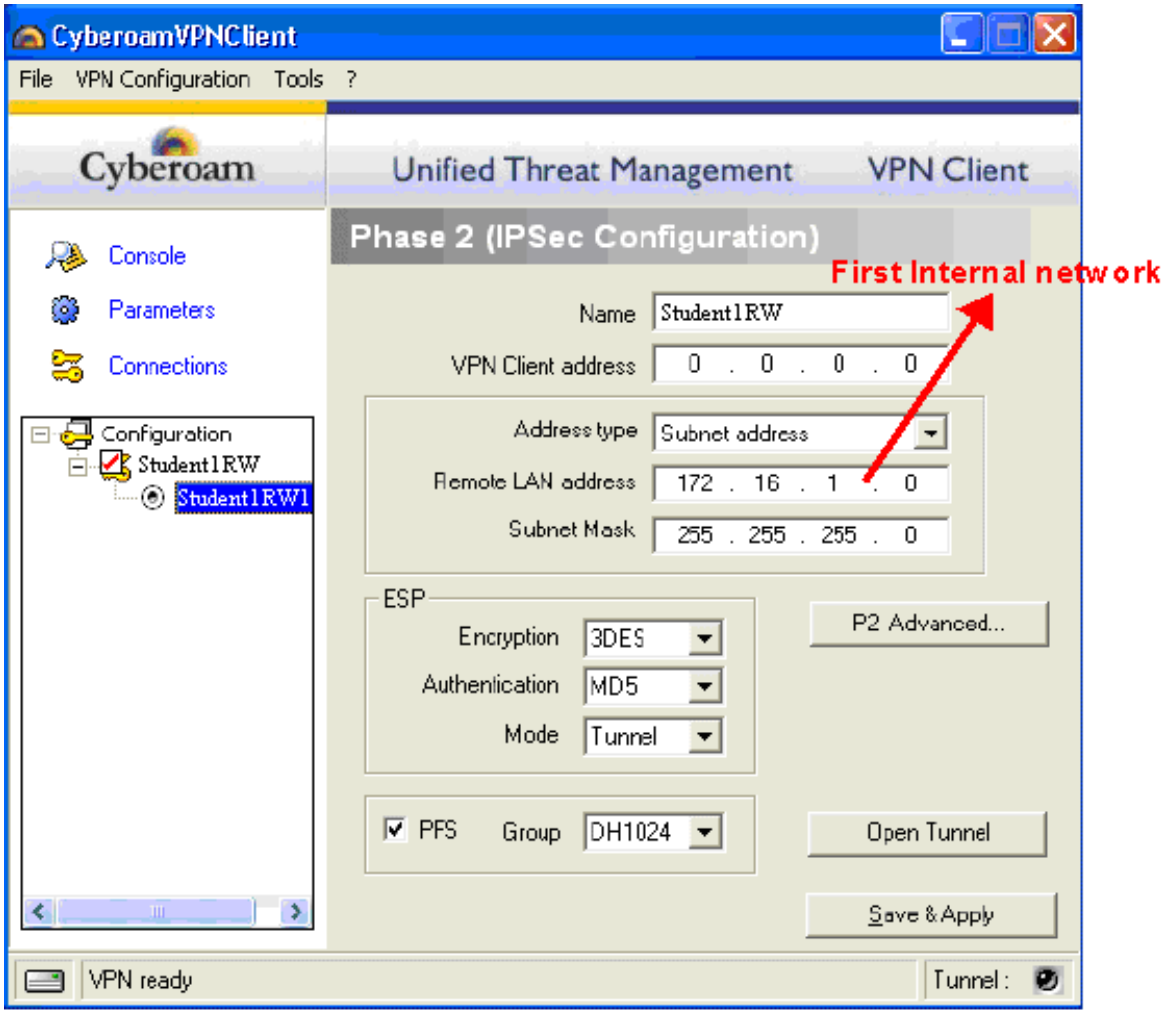
Launch Cyberoam VPN client and go to File>Import VPN Configuration to import connection parameter file (.tgb) received from the remote end. (Step 3)

Note

- Importing VPN configuration will over-write the existing VPN configuration.
- VPN Client creates one phase 1 policy based on the VPN connection.
- VPN Client creates phase 2 policy for each internal network specified in the VPN connection.



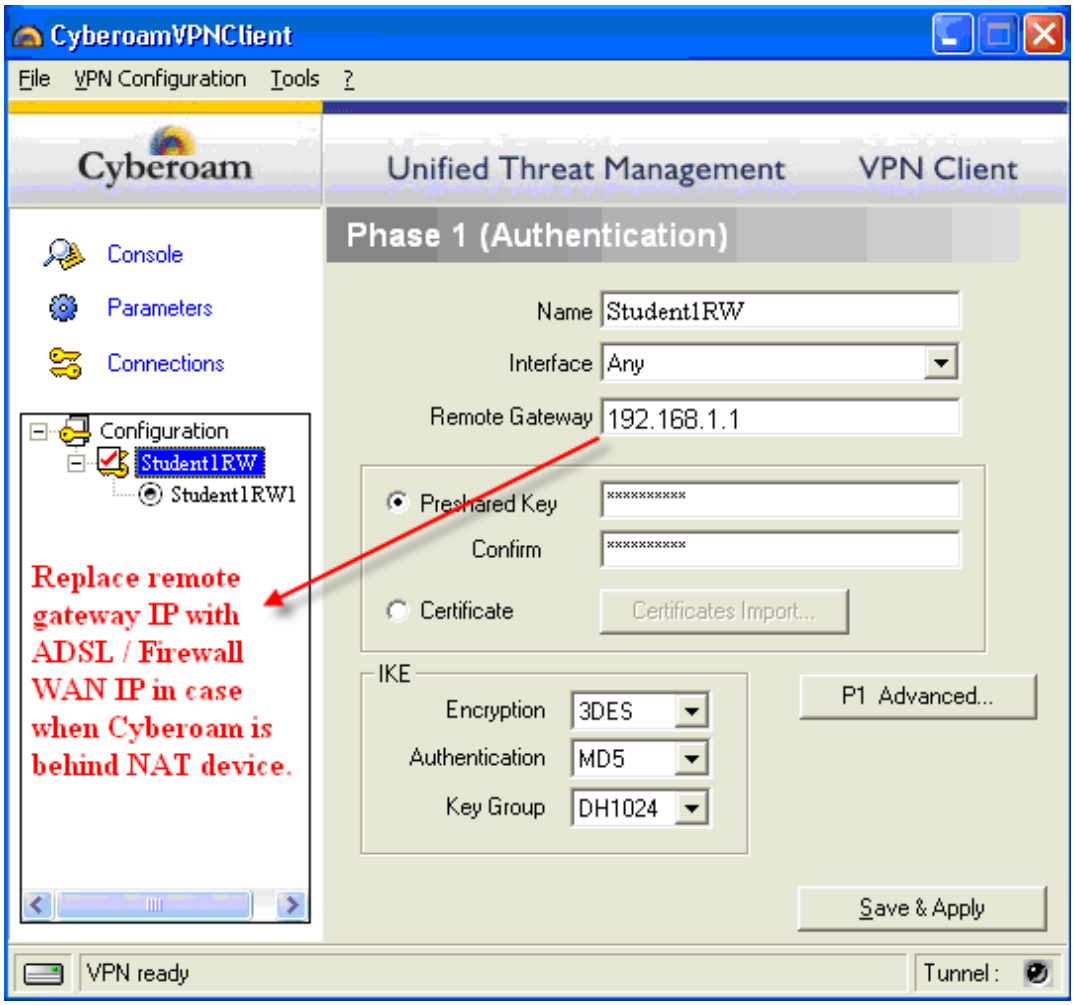

CyberoamVPNClient
File
VPN Configuration
Tools
?
Cyberoam
Unified Threat Management
VPN Client
Console
Parameters
Connections
Configuration
Student1RW
Student1RW1
Phase 1 (Authentication)
Name
Student1RW
Interface
Any
Remote Gateway
192.168.1.1
Preshared Key
Confirm
Certificate
Certificates Import...
IKE
Encryption
3DES
Authentication
MD5
Key Group
DH1024
P1 Advanced...
Save & Apply
VPN ready
Tunnel :


CyberoamVPNClient
File
VPN Configuration
Tools
?
Cyberoam
Unified Threat Management
VPN Client
Console
Parameters
Connections
Configuration
Student1RW
Student1RW1
Phase 2 (IPSec Configuration)
First Internal network
Name
Student1RW
VPN Client address
0 . 0 . 0 . 0
Address type
Subnet address
Remote LAN address
172 . 16 . 1 . 0
Subnet Mask
255 . 255 . 255 . 0
ESP
Encryption
3DES
Authentication
MD5
Mode
Tunnel
P2 Advanced...
PFS
Group
DH1024
Open Tunnel
Save & Apply
VPN ready
Tunnel :

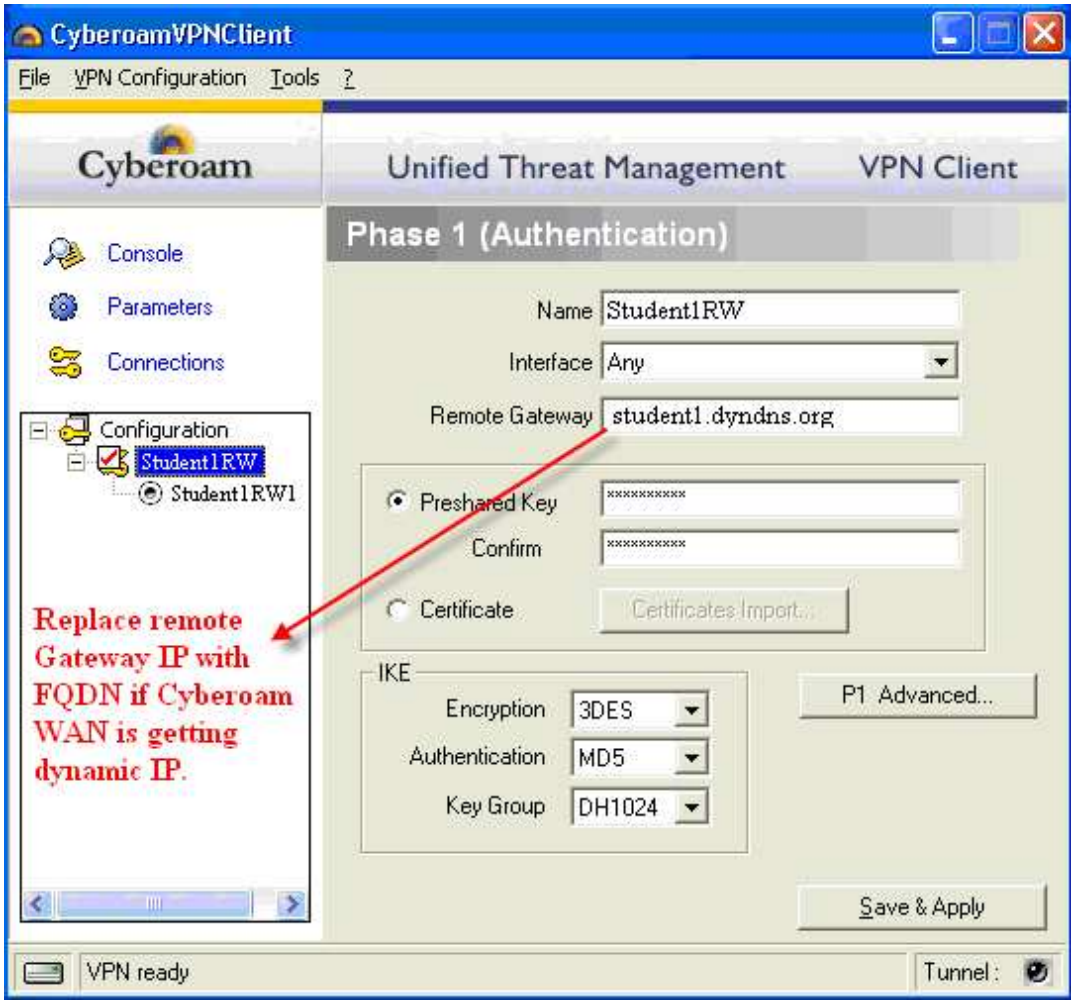
Case I: Private IP address assigned to Cyberoam WAN interface

This situation occurs when Cyberoam is deployed behind any firewall or ADSL device and ADSL device port forwards the request to the Cyberoam.

In this case, specify the public IP address of firewall or ADSL manually in the Remote Gateway field in Phase 1 of VPN Client as connection parameter file will forward private IP address to the VPN Client.



Case II: Dynamic IP address assigned to Cyberoam WAN interface



When Cyberoam WAN interface is assigned IP address dynamically via DHCP or PPPoE and Dynamic DNS is used to map dynamic IP address with a static FQDN, specify FQDN name manually in the Remote Gateway field in Phase 1 of VPN Client.

Lab # IPSec Remote Access Configuration
Activity 5: Establish the Connection

VPN Client automatically opens tunnel on traffic detection. Status bar displays green light for “Tunnel” if connection is successfully established.

Lab #23 IPSec Site-to-Site Configuration using Pre-Shared Key

Objective:

Configure IPSec Site-to-Site connection using pre-shared key so that private networks can communicate.

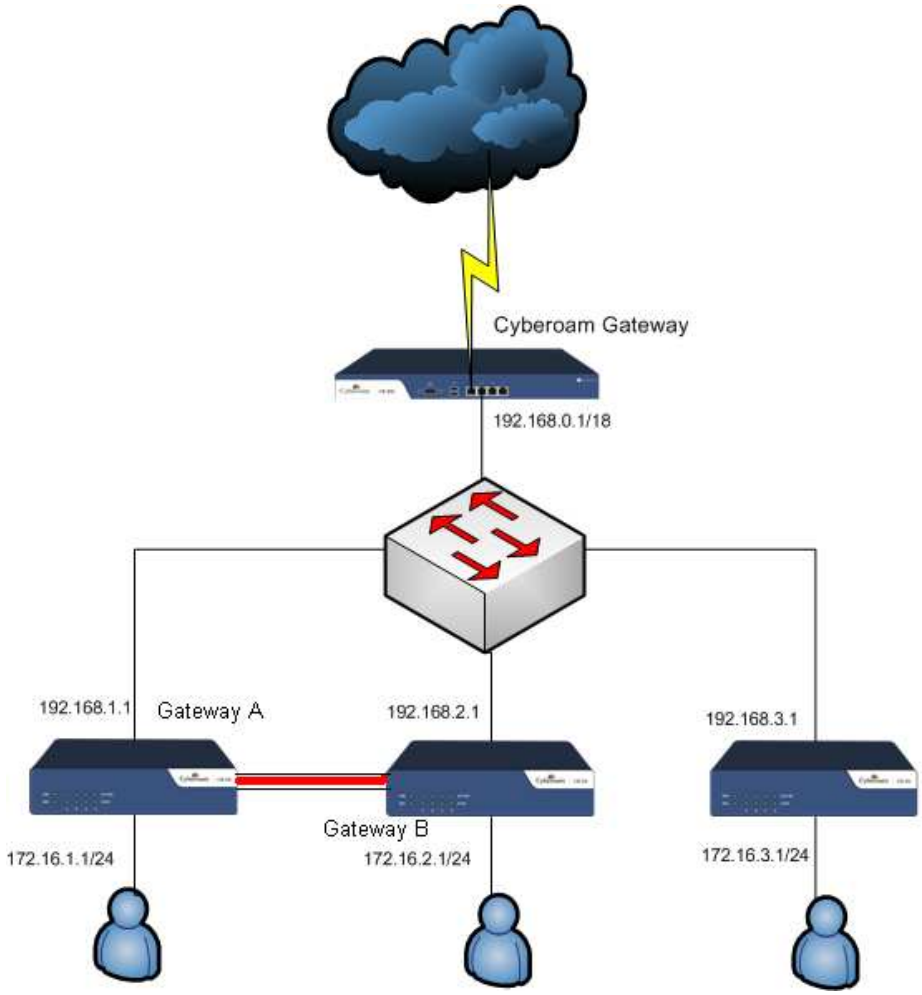
Lab activities:

1. IPSec Site-to-Site Connection Configuration on Site1 (Gateway-A)
2. Activate Connection on Site1 (Gateway-A)
3. IPSec Site-to-Site Connection Configuration on Site2 (Gateway-B)
4. Activate Connection on Site2 (Gateway-B)
5. Establish the Connection

We are going to setup IPSec Site-to-Site connection under below lab setup:

Gateway A connects the internal LAN 172.16.1.0/24 to the Internet. Gateway A's LAN interface has the address 172.16.1.1/24, and its WAN (Internet) interface has the address 192.168.1.1.

Gateway B connects the internal LAN 172.16.2.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 192.168.2.1. Gateway B's LAN interface address, 172.16.2.1/24, can be used for testing IPSec but is not needed for configuring Gateway A.



Below table shows VPN configuration parameter for IPSec connection:

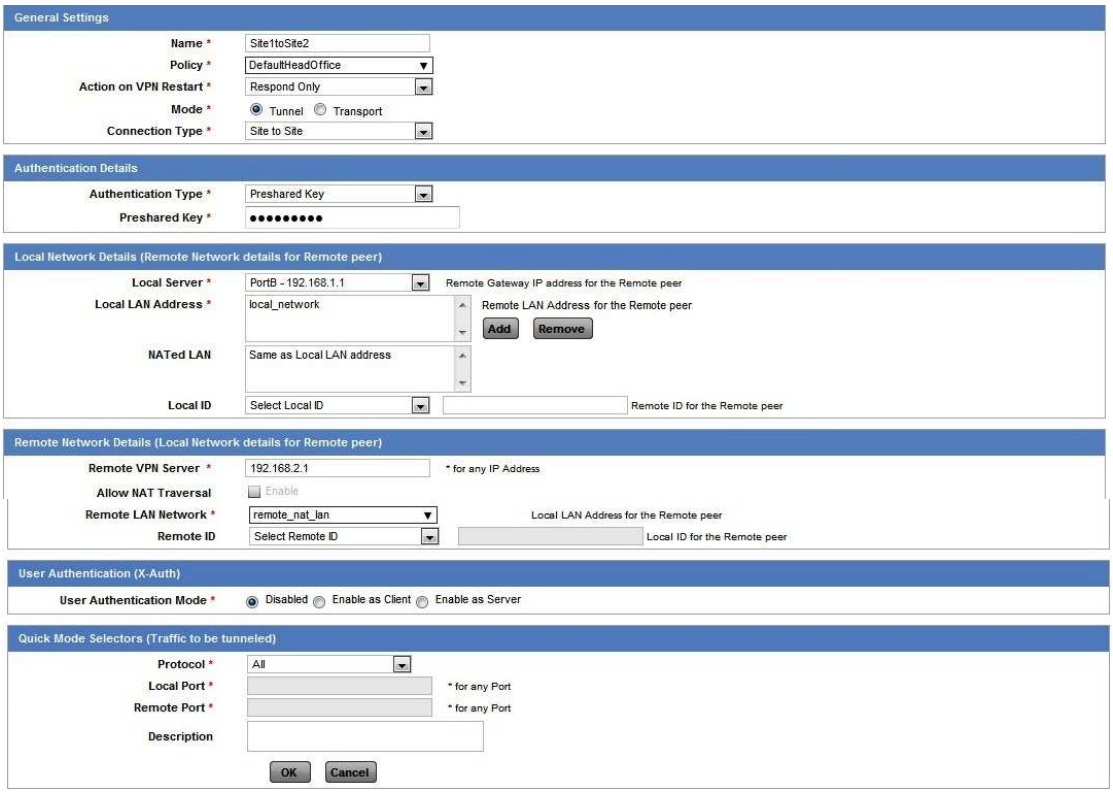
Configuration Parameters	Site1 (Gateway-A)	Site2 (Gateway-B)
IPSec Connection	**Local Network details**	**Local Network details**
	Cyberoam WAN IP address – 192.168.1.1	Cyberoam WAN IP address – 192.168.2.1
	Local Internal Network – 172.16.1.0/24	Local Internal Network – 172.16.2.0/24
	Preshared Key - 0123456789	Preshared Key - 0123456789
	Remote Network details	**Remote Network details**
	Remote VPN server – IP address 192.168.2.1	Remote VPN server – IP address 192.168.1.1
	Remote Internal Network – 172.16.2.0/24	Remote Internal Network – 172.16.1.0/24

Lab #23 IPSec Site-to-Site Configuration using Pre-Shared Key
Activity 1: IPSec Site-to-Site Connection Configuration on Site1 (Gateway-A)

Create IPSec Site-to-Site connection from:

VPN → IPSec Connection → Create Connection

Select default IPSec Head Office policy "**DefaultHeadOffice**" and specify parameters as per below screen shot



Lab #23 IPSec Site-to-Site Configuration using Pre-Shared Key
Activity 2: Activate Connection on Site1 (Gateway-A)

Go to **VPN** → **IPSec Connection** → **Manage Connection**

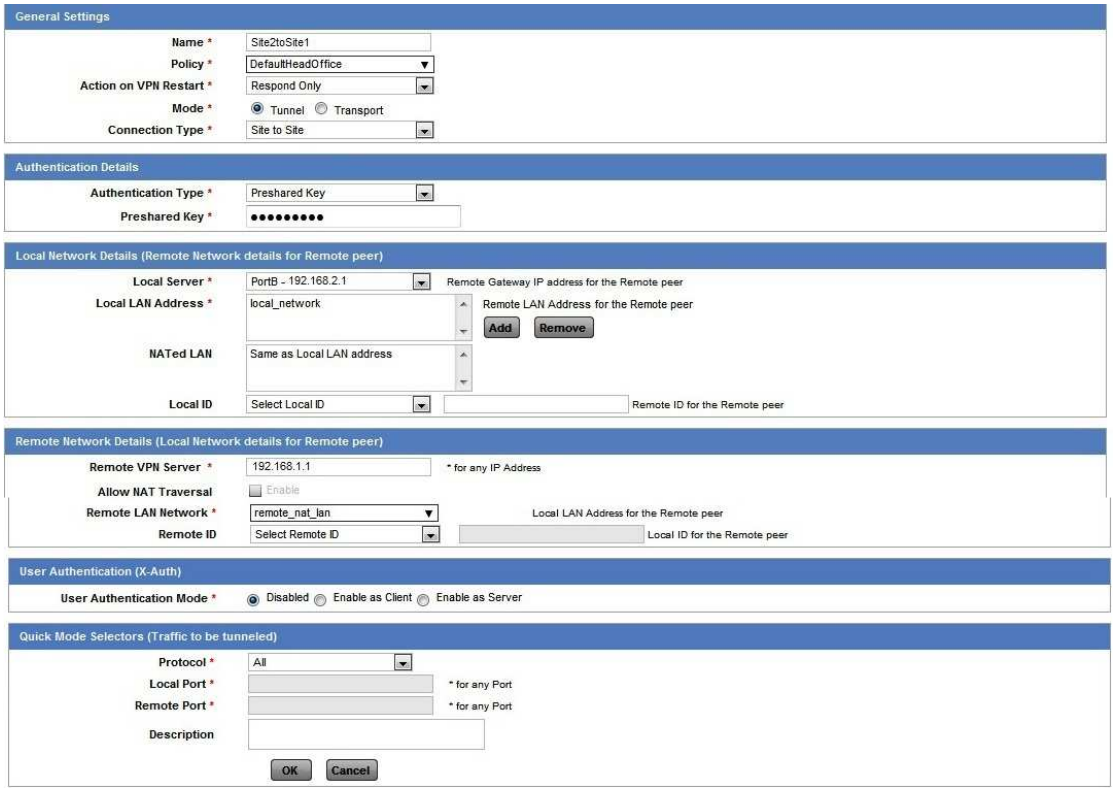
To activate the connection, click  under Connection Status against the Site1toSite2 connection

Lab #23 IPSec Site-to-Site Configuration using Pre-Shared Key
Activity 3: IPSec Site-to-Site Connection Configuration on Site2 (Gateway-B)

Create IPSec Site-to-Site connection from:

VPN → IPSec → Add

Select default IPSec Head Office policy "**Default Branch Office**" and specify parameters as per below screen shot



Lab #23 IPSec Site-to-Site Configuration using Pre-Shared Key
Activity 4: Activate Connection on Site2 (Gateway-B)

Go to **VPN** → **IPSec**

To activate the connection, click under Connection Status against the Site1toSite2 connection

Lab #23 IPSec Site-to-Site Configuration using Pre-Shared Key
Activity 5: Establish the connection

Go to **VPN** → **IPSec**

To establish the tunnel, click  under Connection Status against the Site1toSite2 connection.

Generally Branch Offices act as a tunnel initiator and Head Office act as a responder due to following reasons:

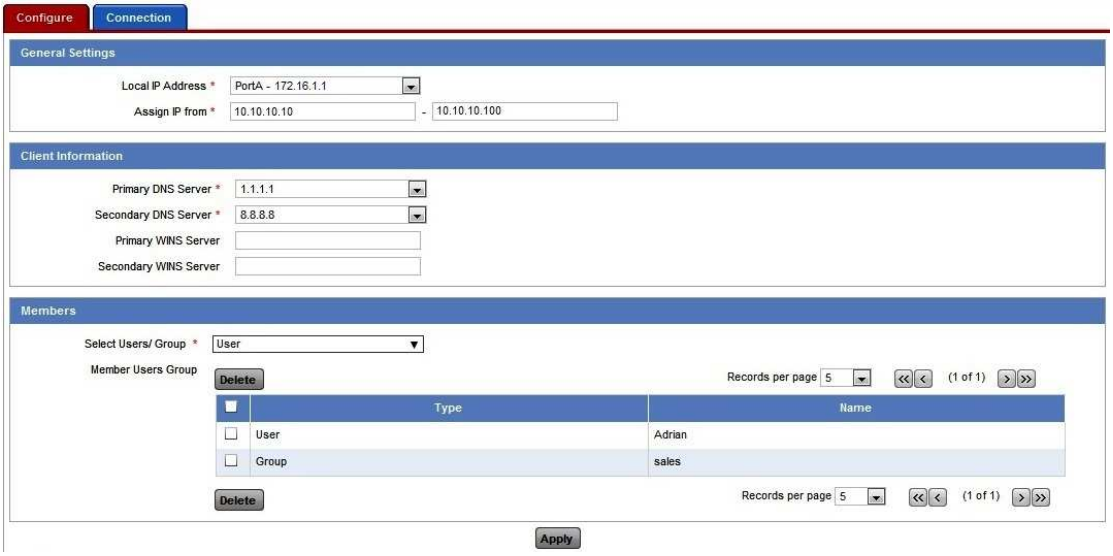
1. Mostly Branch Offices will have dynamic IP so Head Office will not be able to initiate the connection. If remote site is on dynamic then Head Office will not be able to initiate the connection.
2. This will reduce the load on Head Office as Branch Offices will keep retrying the connection instead of one Head Office to keep retrying all Branch Office connections.

In this Lab scenario, both are having static IP, so connection can be initiated by any site.

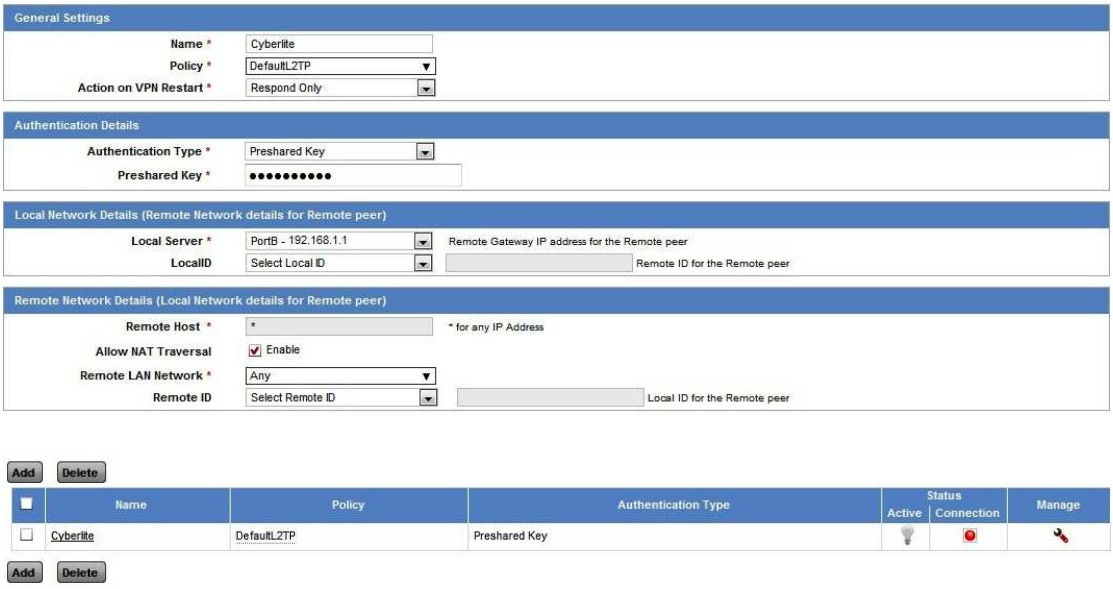
Lab24# Create L2TP Tunnel allowing the tunnel users to access only web services of Intranet in LAN enabling the DMZ IPS policy.

Go to VPN → L2TP → Configure

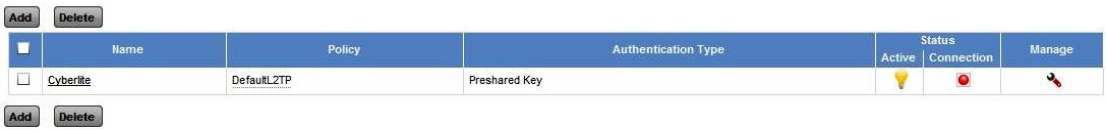
Create L2TP configuration assigning IP from 10.10.10.10 to 10.10.10.100



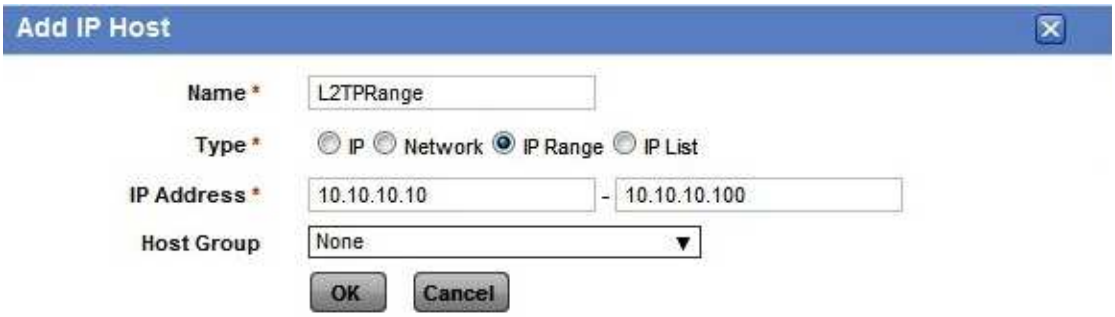
Create L2TP connection: Go to VPN → L2TP → Connection



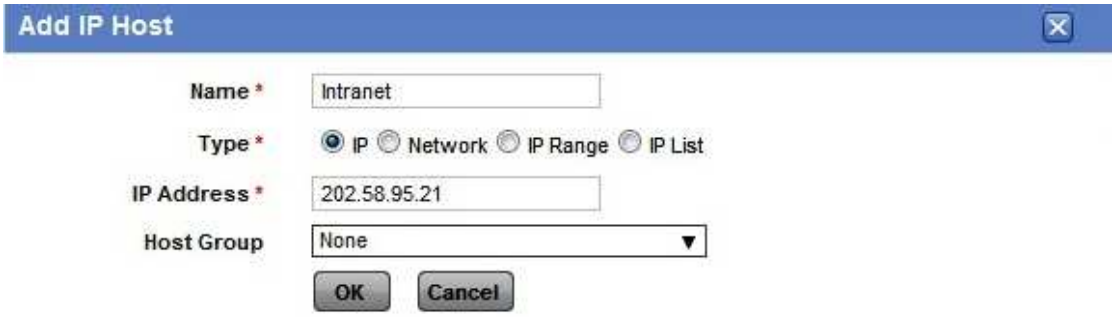
Click the  button under the Active column to Activate the connection:



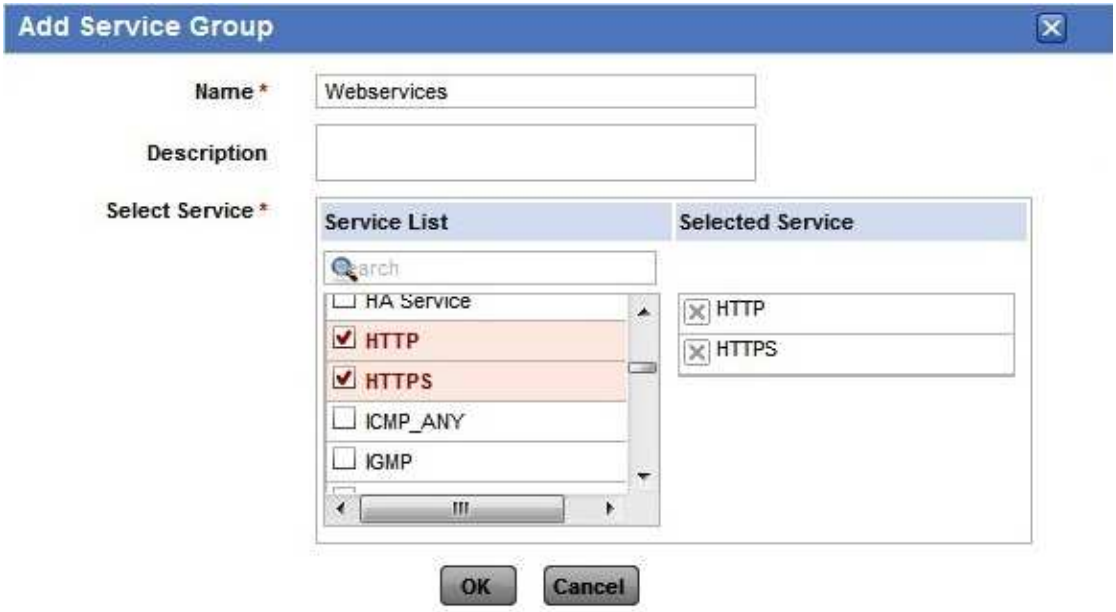
Create Host for the L2TP range of users



Create Destination Host:



Create Service group for web services:

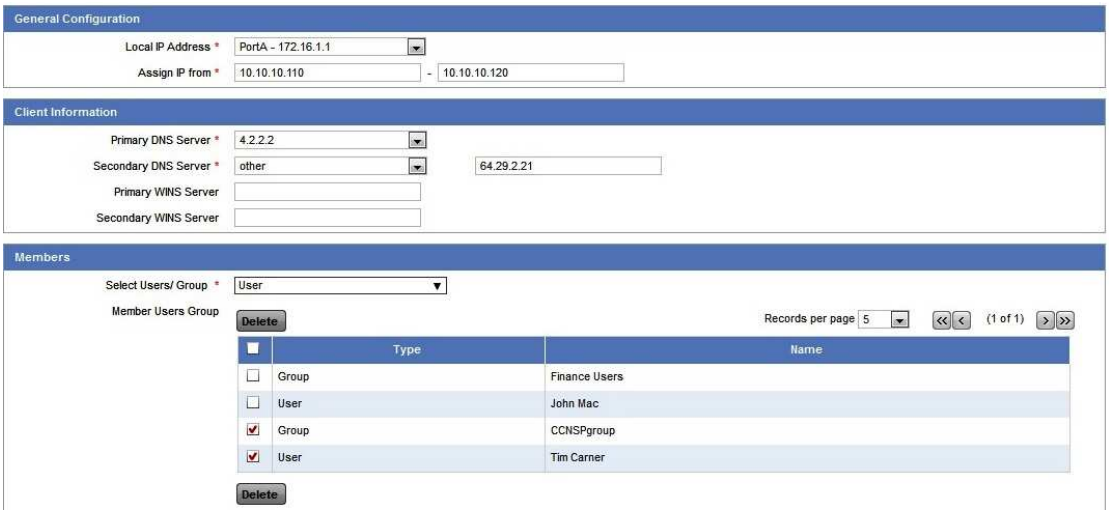


Now creating a firewall rule:

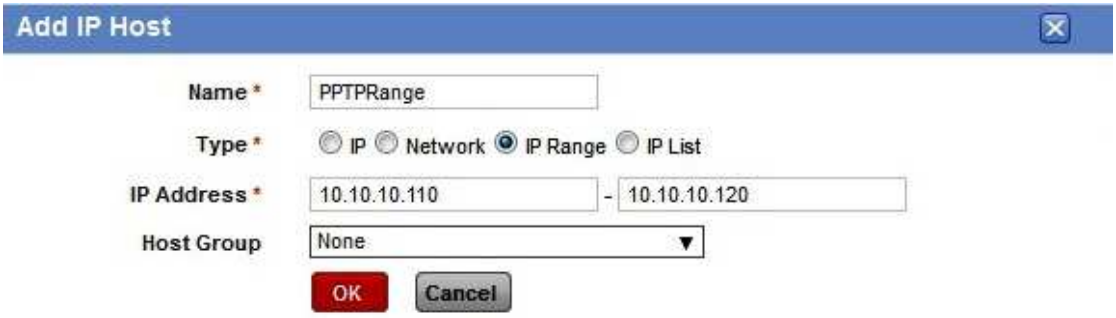

Source
Destination
Zone *
VPN
LAN
Attach Identity
Network / Host *
L2TPRange
Intranet
Services *
Webservices
Schedule
All the time
Action *
Accept
Drop
Reject
Apply NAT
Select NAT Policy
Advance Settings (Security Policies, QoS, Routing Policy, Log Traffic)
Security Policies
Web Filter
Select Web Filter Policy
Apply Web Category based QoS Policy
Application Filter
Select Application Filter Policy
IPS
dmzpolicy
IM Scanning
Enable
AV & AS Scanning
SMTP
POP3
IMAP
FTP
HTTP

Lab#25 Create PPTP Tunnel allowing the tunnel users to access only web services of Internal network in LAN enabling the DMZ IPS policy.

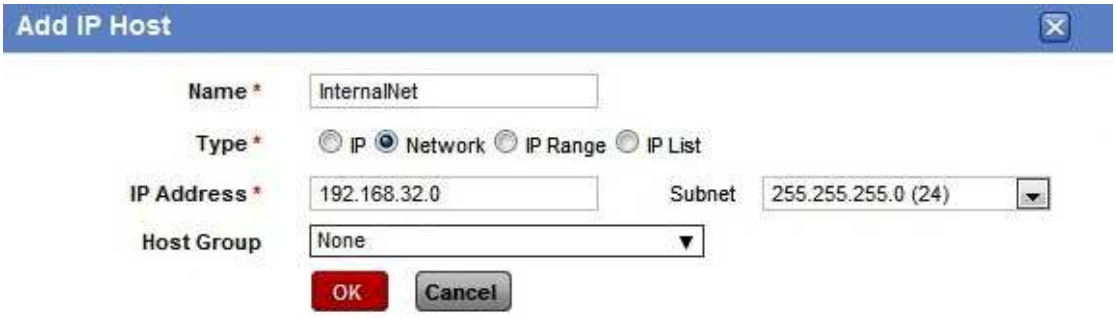
Create PPTP Configuration: VPN → PPTP



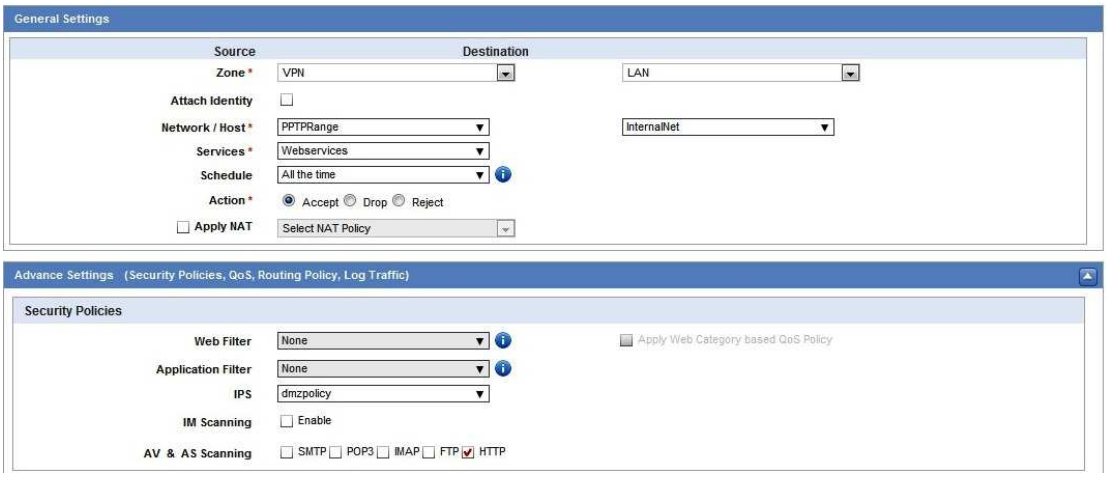
Create Host for PPTP Range of users



Create destination host for Internal Network



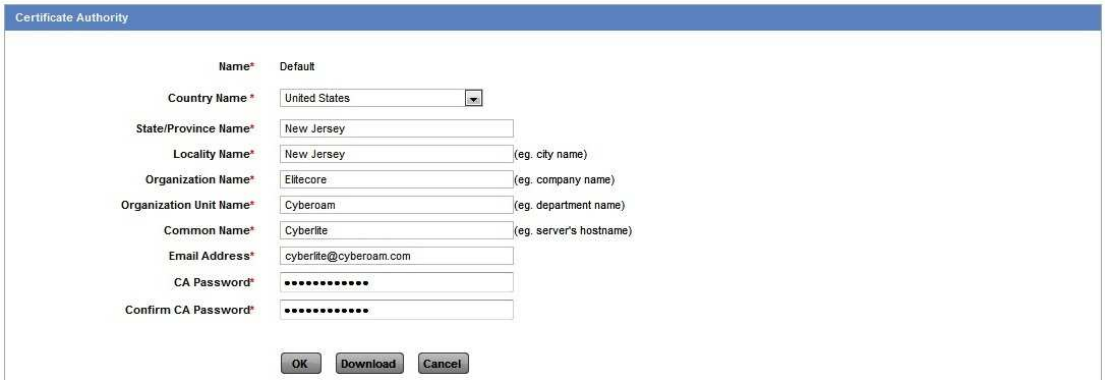
Create firewall rule for the same



Lab 26# Create Global policy for SSL VPN using self signed certificates for client and sever.

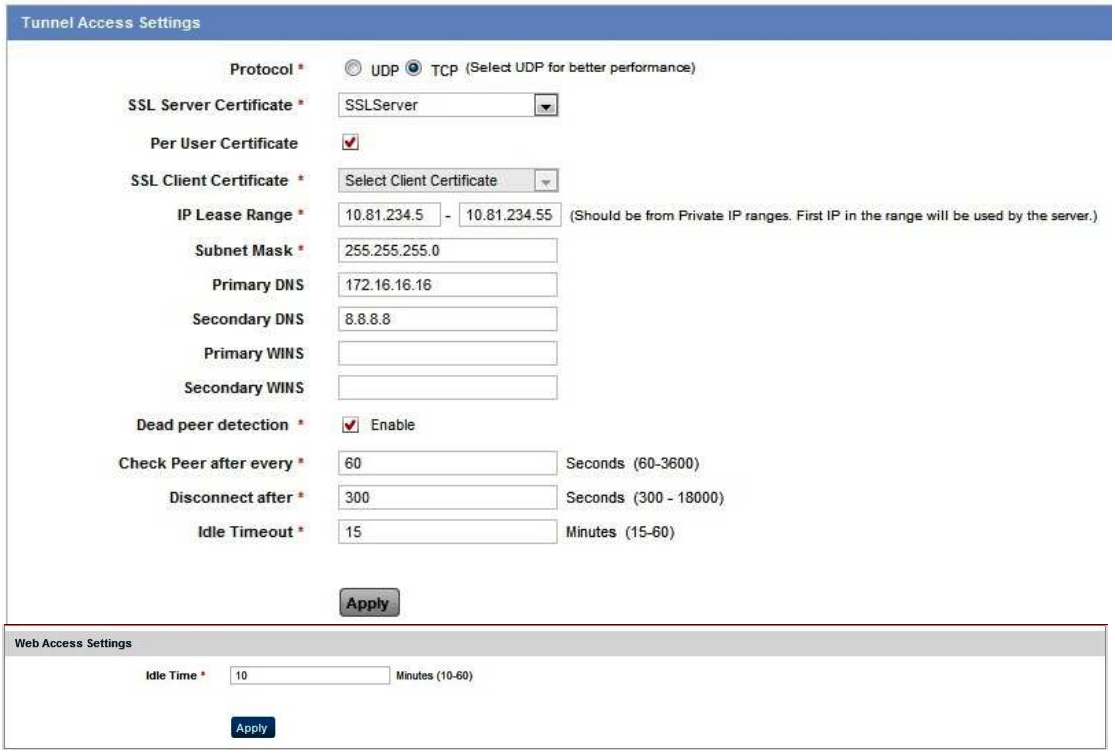
For this Lab, we will use the Default Certificate Authority of Cyberoam. To use it, we have to enter the information in the Default Certificate Authority.

Go to Objects → Certificate → Certificate Authority → Click on Default



Create a self signed certificate for Client end: Objects → Certificated → Add

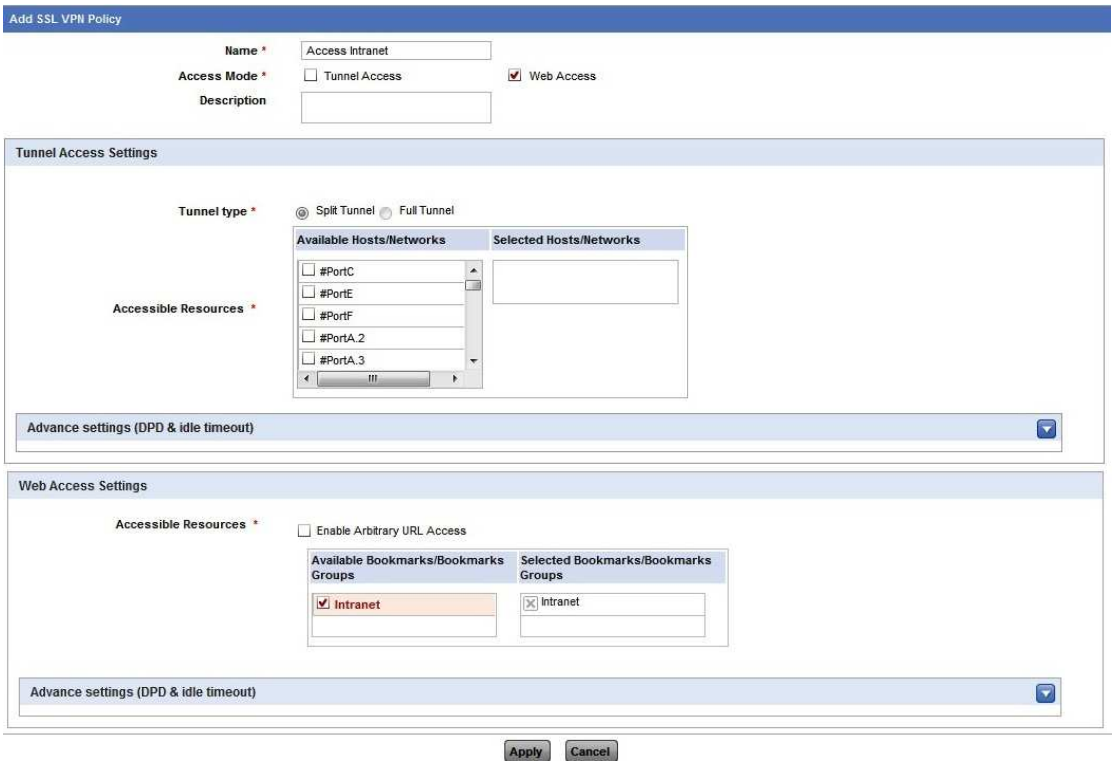
Apply the certificates to the Global Settings specifying the IP Lease range:
Go to SSL VPN → Global Settings



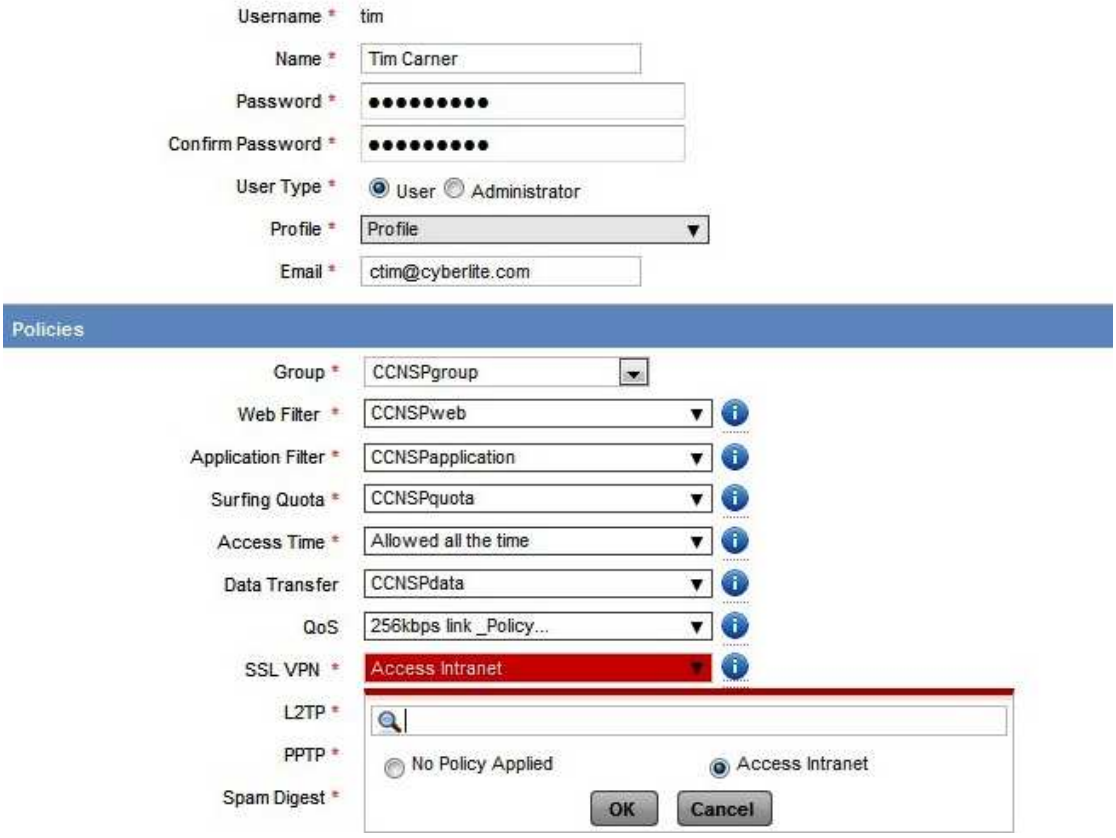
Lab 27#Create an SSL VPN tunnel with Web access applying it to user with access only to Intranet.

Create a bookmark for the internal network

Create a Web access SSL-VPN Policy

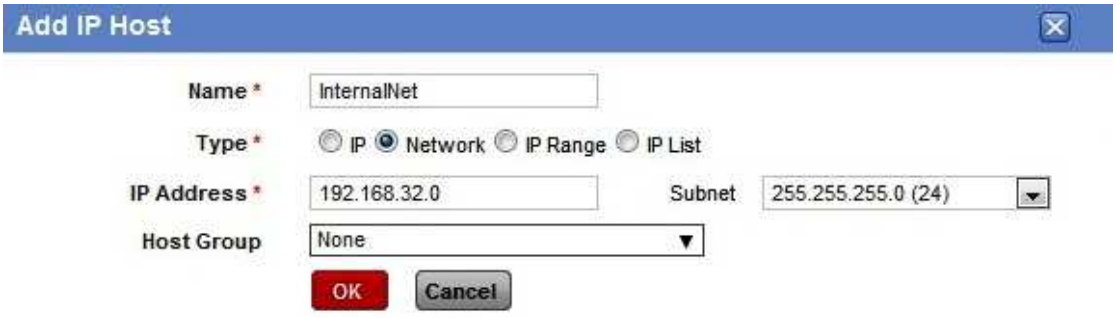


Now apply it to the user.

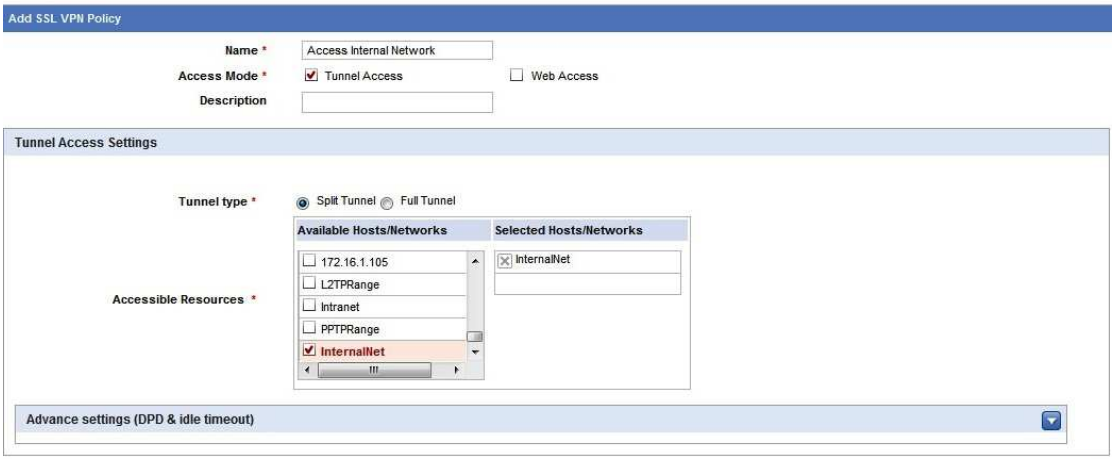


Lab 28# Create an SSL VPN tunnel with Full access in split tunnel mode applying it to Manager User giving access to the internal network.

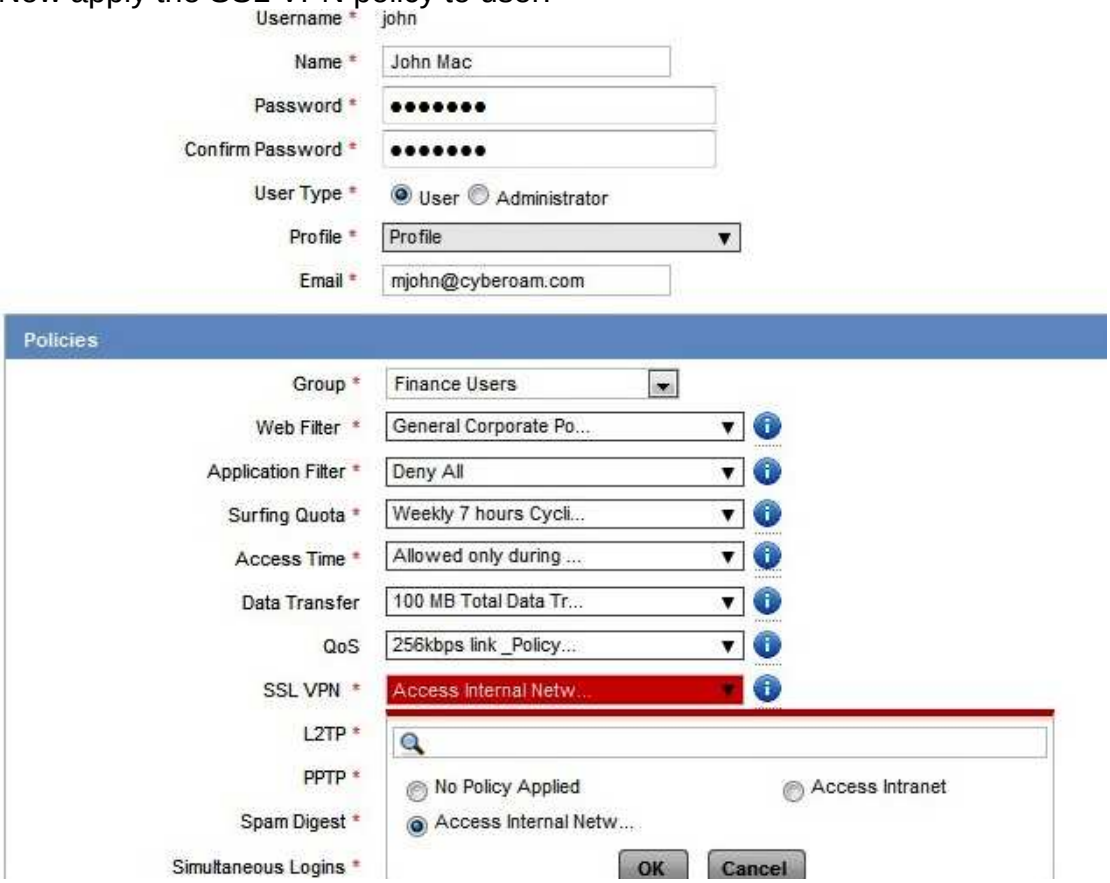
Create host for internal network



Create Full Access Mode, split tunnel SSL VPN Policy



Now apply the SSL VPN policy to user:



Lab #29 L2TP Configuration (Online – Optional)

Please refer below Cyberoam Knowledge Base article to configure L2TP connection:

http://kb.cyberoam.com/default.asp?id=956&SID=&Lang=1

Lab #30 PPTP Configuration (Online – Optional)

Please refer below Cyberoam Knowledge Base article to configure PPTP connection:

http://kb.cyberoam.com/default.asp?id=380&SID=&Lang=1

Cyberoam VPN Failover Overview

Cyberoam VPN Connection Failover is a feature that enables to provide an automatic backup connection for VPN traffic and provide “Always ON” VPN connectivity for IPSec and L2TP connections.

A VPN tunnel allows you to access remote servers and applications with total security. With VPN auto failover, a VPN connection to be re-established when one of the two WAN connections drops. Solution also achieves failover latency of a few seconds by constantly monitoring the link and instantaneously switching over in the event of a failure.

Advantages

- Reduce the possibility of a single point of failure
- Reduce the reliance on manual intervention to establish new connection
- Reduce the failover time of a VPN connection with redundant VPN tunnels and VPN monitoring

Cyberoam implements failover using VPN connection Group. A VPN group is a set of VPN tunnel configurations. The Phase 1 and Phase 2 security parameters for each connection in a group can be different or identical except for the IP address of the remote gateway. The order of connections in the Group defines fail over priority of the connection.

When the primary connection fails, the subsequent active connection in the Group takes over without manual intervention and keeps traffic moving. The entire process is transparent to users.

For example if the connection established using 4th Connection in the Group is lost then 5th Connections will take over.

VPN Logs:

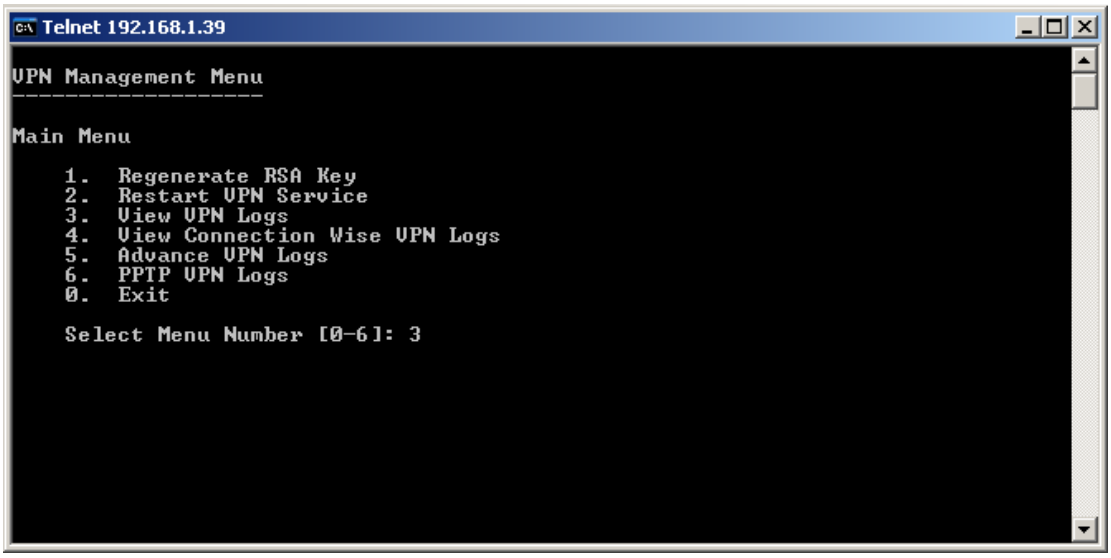
To view VPN logs, connect Cyberoam through telnet/ssh console.

The default password is: Admin.

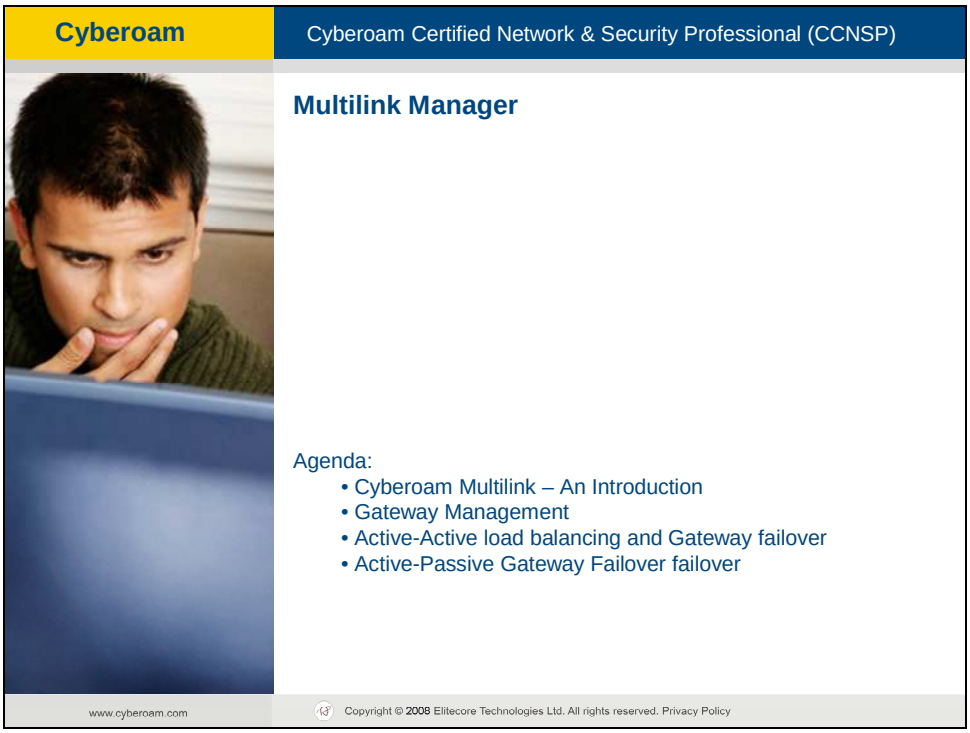
Select option number 8, i.e. VPN Management.

```
Main Menu

    1. Network  Configuration
    2. System   Configuration
    3. Route    Configuration
    4. Cyberoam Console
    5. Cyberoam Management
    6. Upgrade  Firmware
    7. Bandwidth Monitor
    8. VPN Management
    9. Shutdown/Reboot Cyberoam
    0. Exit

    Select Menu Number [0-9]:
```

After selecting option number 8, select option number 3.



Module 11: Multilink Manager



Cyberoam | Unified Threat Management

Multi-Link- An Introduction

Introduction:

- In a typical organization scenario, multiple WAN links may be required to be deployed.
- Organizations may want to take advantage of multiple links to increase performance by maintaining high uptime.
- Cyberoam Multi-Link can be configured only in **Gateway mode** and not in Bridge mode.

Benefits:

- **Load Balancing**
  It balances traffic between various links, optimizes utilization and thereby assist in cutting operating cost.
- **Automatic ISP Failover Detection**
  It detects link failure and passes the traffic to operating link.
- **High Uptime**
  Improves performance because of high uptime.
- **Bandwidth Scalability**
  Facilitates increased bandwidth scalability

www.cyberoam.com

Cyberoam Multilink – An Introduction

Cyberoam's integrated Internet security solution is purpose-built to meet the unified threat management needs of corporate, government organisations and educational institutions. It also provides assistance in improving Bandwidth management, increasing Employee productivity and reducing legal liability associated with undesirable Internet content access.

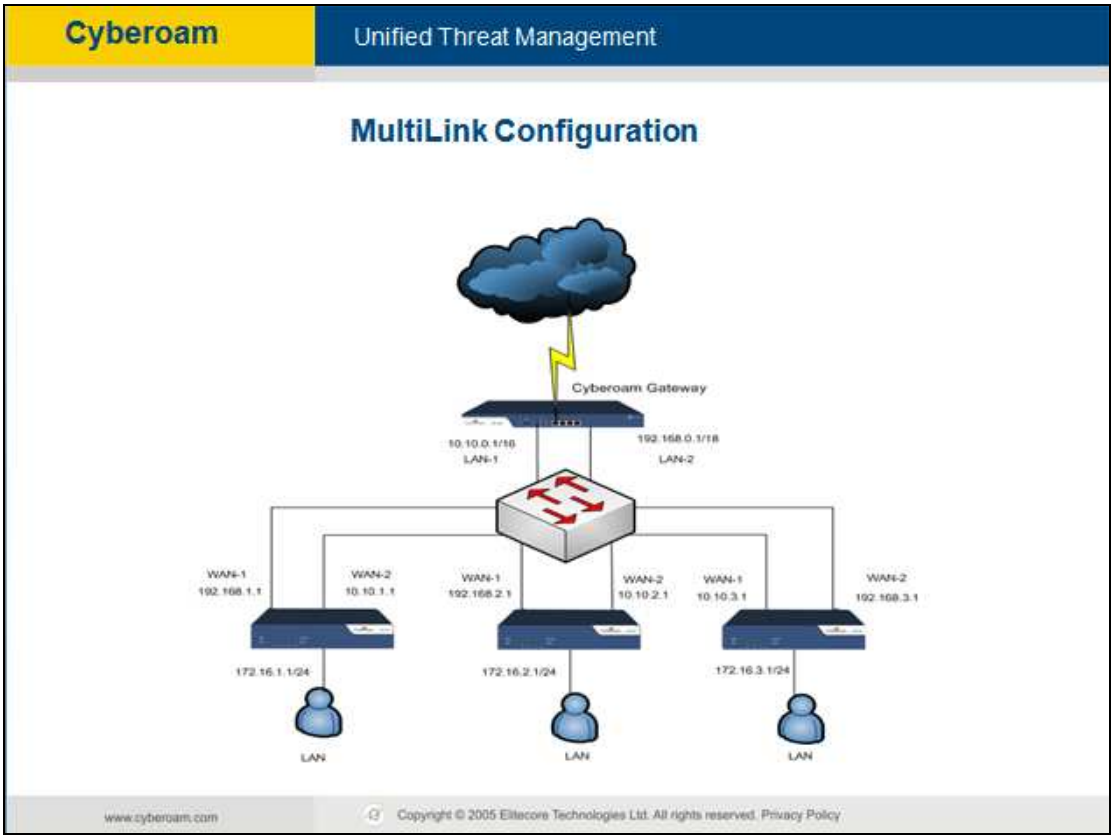
Cyberoam's - Weighted Round Robin Load Balancing feature enables Network Managers to optimise network traffic and balance the load between multiple gateways/links. It also supports the failover detection and switchover mechanism to an alternate link when an active link goes down.

Load balancing is a mechanism that enables balancing traffic between various links. It distributes traffic among various links, optimising utilisation of all links to accelerate performance and cut operating costs. Employing a weighted round robin algorithm for load balancing, Cyberoam enables maximum utilisation of capacities across the various links.

In addition to distributing traffic, Cyberoam detects link failure i.e. when a gateway stops responding or goes down and passes the traffic to the operating link. This safeguard helps you provide uninterrupted, continuous Internet connectivity to your users.

Using link load balancing provides organisations a way to achieve:

1. Traffic distribution that does not overburden any link
2. Automatic ISP failover
3. Improved User performance because of no downtime
4. Increased bandwidth scalability



How it works

Load balancing is determined by the load metric/weight. Each link is assigned a relative weight and Cyberoam distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.

Administrators can set weight and define how the traffic should be directed to providers to best utilize their bandwidth investments. Weight can be selected based on:

1. Link capacity (for links with different bandwidth)
2. Link/Bandwidth cost (for links with varying cost)

By Default all the Gateways are having weight as "1", so Cyberoam will do the Load balancing in 1:1 across all Gateways'.

CCNSP | Module 11: Multilink Manager

Multi-Link- How it works

Cyberoam does load balance using Weighted Round Robin (WRR)

Load balancing is determined by the load metric i.e. Weight

Cyberoam does load balance only on new connection

Weight can be selected based on:
- Weight can be decided on Link Capacity
- Weight can be decided on Link Cost

By Default all the Gateways are having weight as “1”, so Cyberoam will do the Load balancing in 1:1 across all Gateways’.

CCNSP | Module 11: Multilink Manager

Gateway Management

What needs to be done if Multiple ISP links are available?

- Active-Active load balancing and gateway failover
- Active-Passive Gateway Failover

Active-Active load balancing and gateway failover

By default, all the gateways defined through Network Configuration Wizard will be defined as "Active" gateway.

For Active Gateway

Depending on the weight, Cyberoam will select gateway for load balancing. Cyberoam distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link.

To specify the weight, go to Network → Gateway → Click the Gateway Name

To add Gateway Failover Rule, go to Network → Gateway → Click the Gateway Name → Failover Rules

Gateway failover provides link failure protection i.e. when one link goes down; the traffic is switched over to the active link. This safeguard helps provide uninterrupted, continuous Internet connectivity to users. The transition is seamless and transparent to the end user with no disruption in service i.e. no downtime.

To achieve WAN failover between multiple links:

To achieve WAN failover between multiple links:

- Configure links in Active-Backup setup
- define Active gateway/interface
- define Backup gateway/interface – traffic through this link is routed only when active interface is down
- define failover rule

In the event of Internet link failure, the Multilink Manager automatically sends traffic to available Internet connections without administrator intervention. If more than one link is configured as backup link, traffic is distributed among the links in the ratio of the weights assigned to them. On fail over, Backup gateway can inherit the parent gateway's (Active gateway) weight or can be configured.

Failover rules

The transition from dead link to active link is based on the failover rule defined for the link.

Failover rule specifies:
•how to check whether the link is active or dead
•what action to take when link is not active

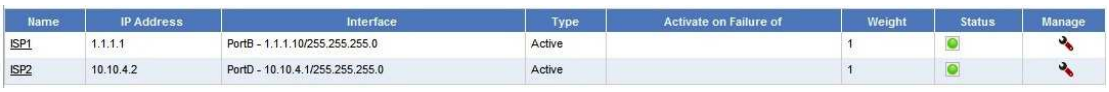
Failover rule has the form:

IF
Condition 1
AND/OR
Condition 2
then
Action

Depending on the outcome of the condition, traffic is shifted to any other available gateway.

By default, Cyberoam creates Ping rule for every gateway. Cyberoam periodically sends the ping request to check health of the link and if link does not respond, traffic is automatically sent through another available link. Selection of the gateway and how much traffic is to be routed through each gateway depends on number of configured active and backup gateways.

Configure both the gateways as active

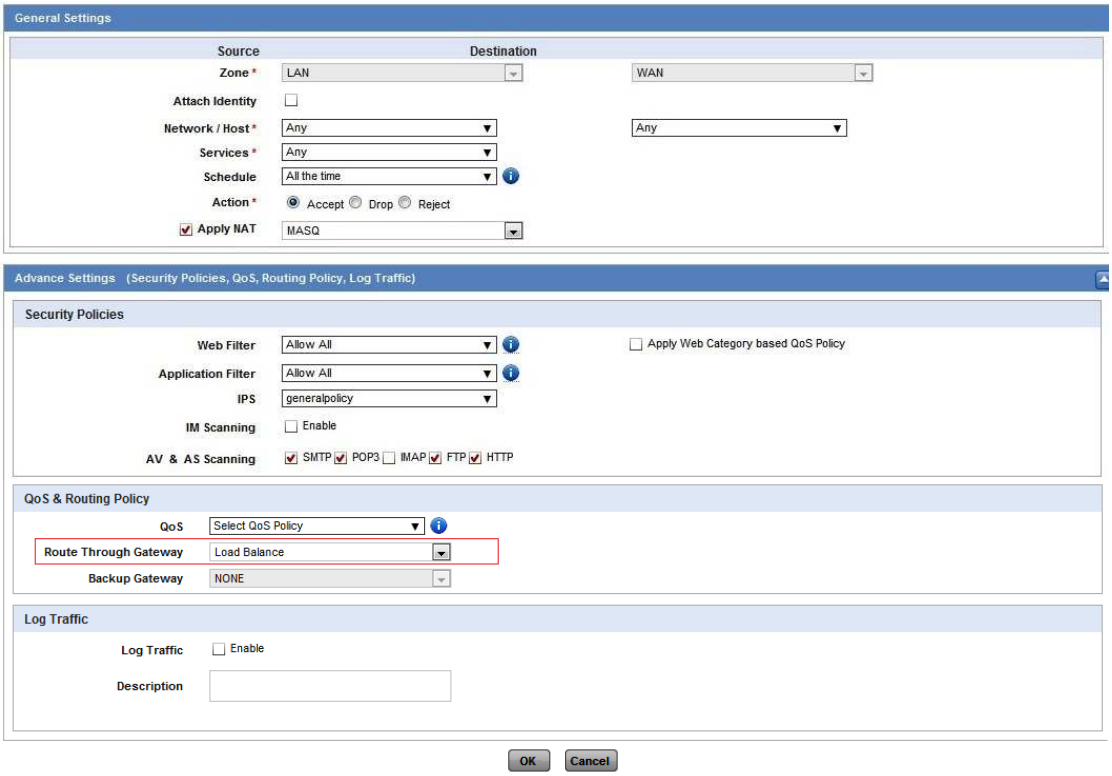


Name	IP Address	Interface	Type	Activate on Failure of	Weight	Status	Manage
ISP1	1.1.1.1	PortB - 1.1.1.10/255.255.255.0	Active		1		
ISP2	10.10.4.2	PortD - 10.10.4.1/255.255.255.0	Active		1		

Gateway Load Balancing

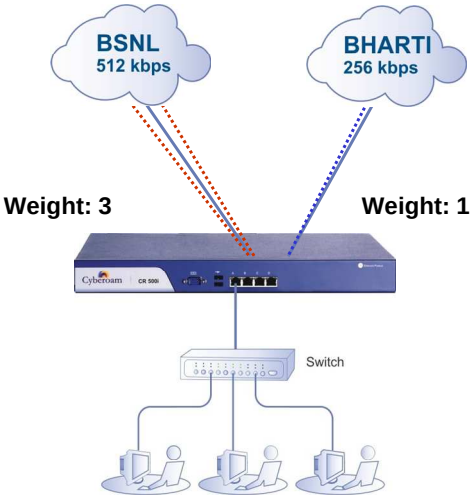
By default, all the Firewall traffic is load balanced across all the ISP links in proportion to the weight.

Firewall -- > Edit any of the rule.



CCNSP | Module 11: Multilink Manager

Active-Active gateway Load Balancing



CCNSP | Module 11: Multilink Manager

Active-Active gateway Failover

- Depending on the weight, Cyberoam will select gateway for load balancing.
- Cyberoam distributes traffic across links in proportion to the ratio of weights assigned to individual link.
- This weight determines how much traffic will pass through a particular link relative to the other link.

Active-Passive Gateway Failover

The Feature:

1. Configure a redundant link on Cyberoam.
2. Configure multiple backup links.
3. Backup links for specific routes.

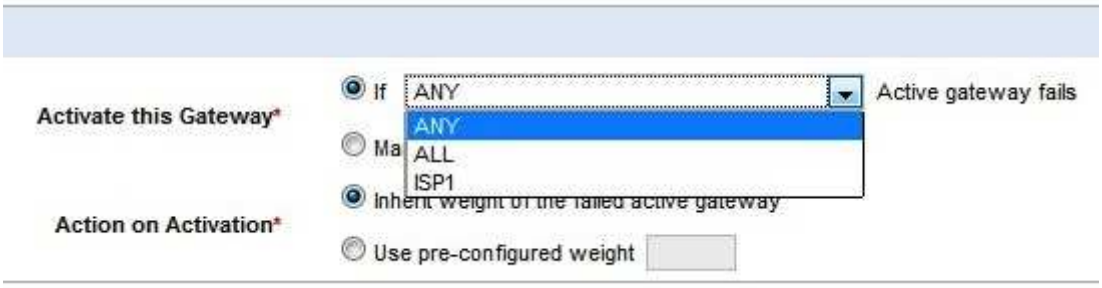
Benefit:

Provides the link failure protection

Backup – A gateway that can be used in an active/passive setup, where traffic is routed through Backup gateway only when Active gateway is down

This option is only available when two or more Gateways are configured in Cyberoam.

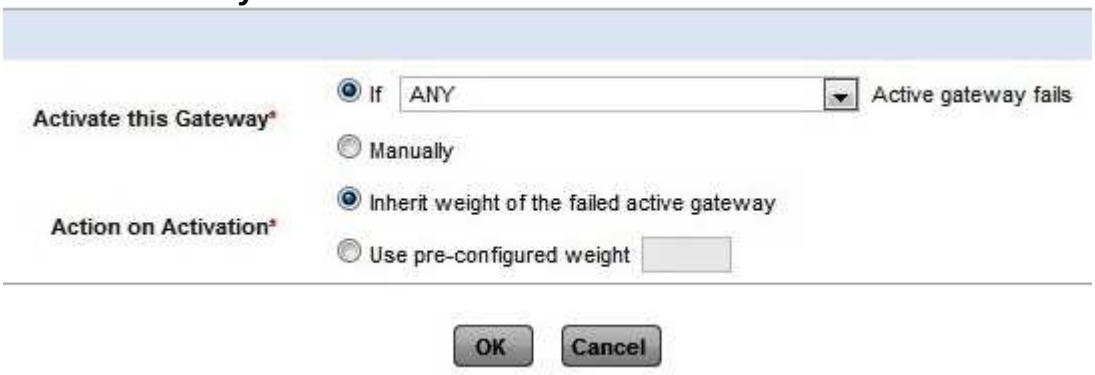
Backup Gateway Details:
Activate this Gateway – Configure when the Backup gateway should take over the active gateway.



Automatic failover
From the dropdown list specify when the backup gateway should take over from active Gateway. This takeover process will not require administrator's intervention.

Options:
Specific Gateway - Dropdown will list all the configured gateways. Backup gateway will take over and traffic will be routed through the backup gateway only when the selected gateway fails.
ANY – Backup gateway will take over and traffic will be routed through backup gateway when any of the active gateway fails
ALL - Backup gateway will take over and traffic will be routed through backup gateway when all the configured active gateways fail

Manual Gateway Failover

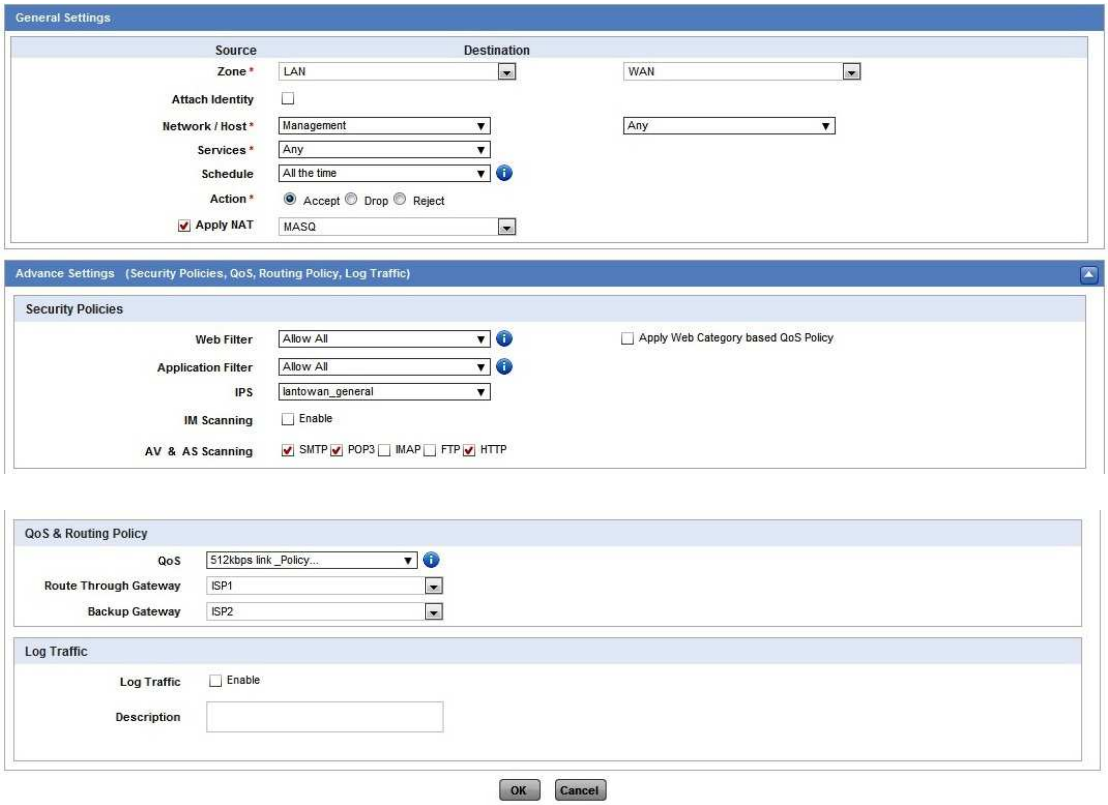


Manual failover
If you select "Manually", Administrator will have to manually change the gateway if the active gateway fails.

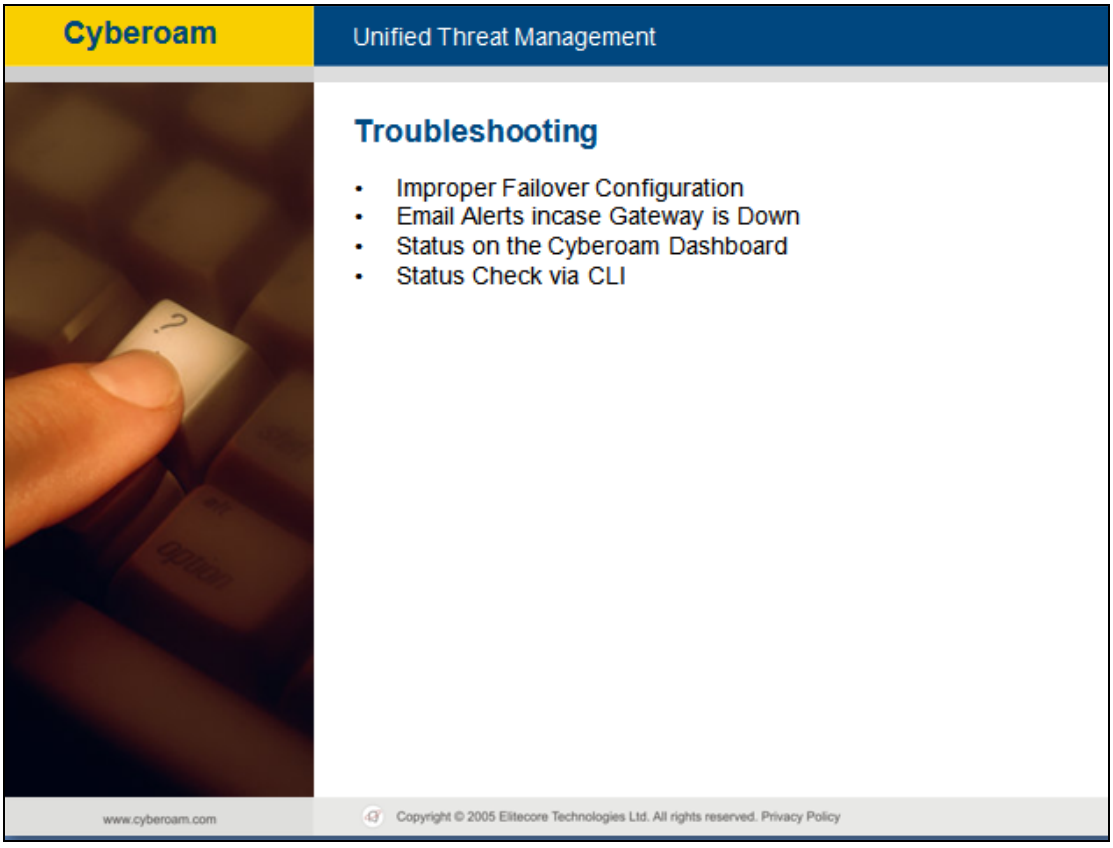
Action on Activation – Configure weight for the backup gateway . Cyberoam distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.

Select "Inherit weight of the failed active gateway" if you want Backup gateway to inherit the parent gateway's (Active gateway) weight or select "User pre-configured weight" and specify weight.

Active-Passive gateway failover through Firewall rule itself



ISP1 has been included in the Route Through Gateway and ISP2 as Backup Gateway. When the ISP1 goes down it will automatically shift all traffic over ISP2


Cyberoam
Unified Threat Management
Troubleshooting
Improper Failover Configuration
Email Alerts incase Gateway is Down
Status on the Cyberoam Dashboard
Status Check via CLI
www.cyberoam.com
Copyright © 2005 Elitecore Technologies Ltd. All rights reserved. Privacy Policy

Troubleshooting

Gateway Failover Conditions

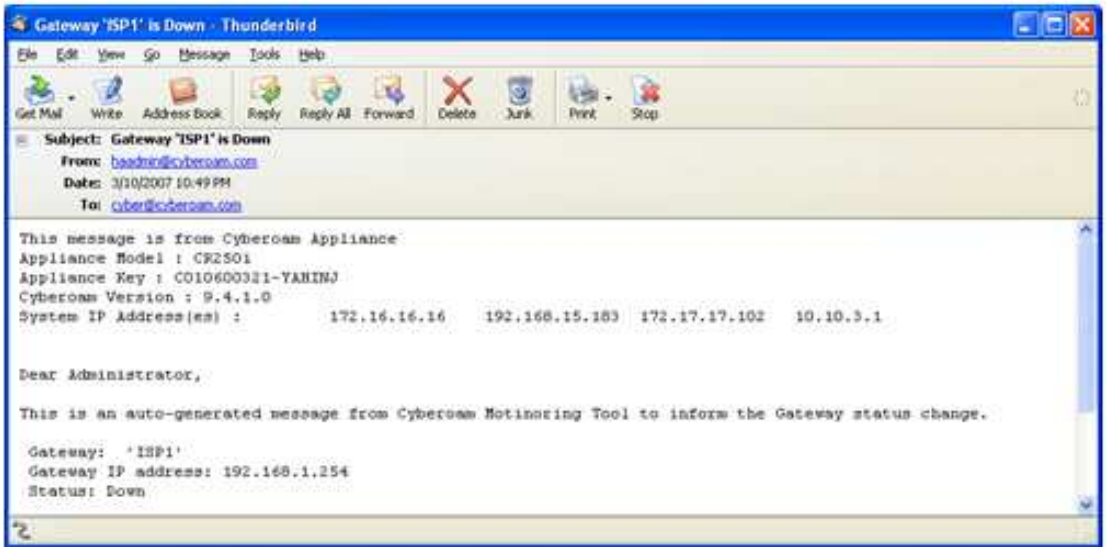
Make sure to have the correct Gateway failover conditions configured on the appliance, otherwise traffic will not be failover in case of link down.

Refer to failover condition slides to configure it properly.

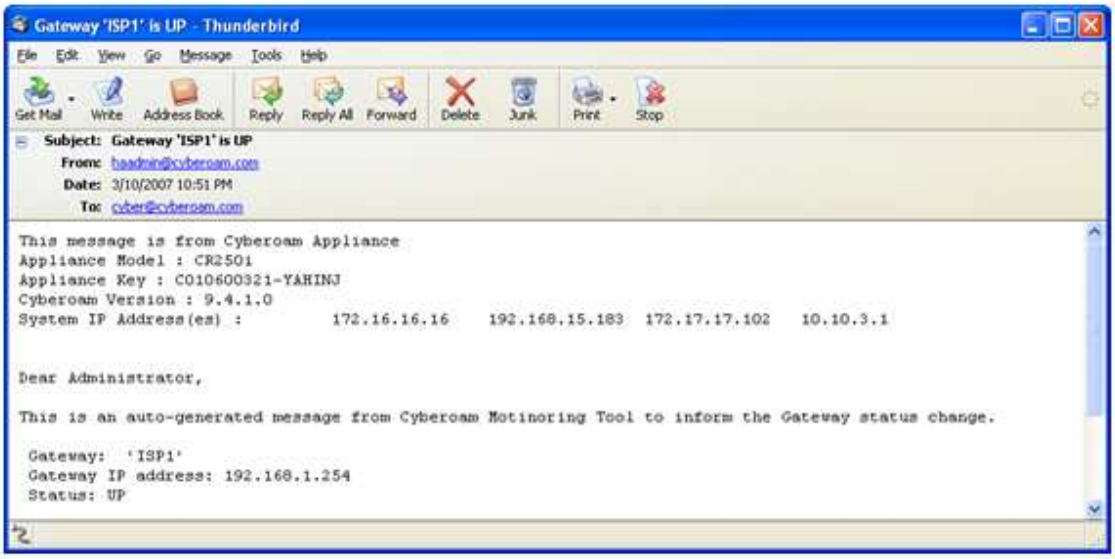
Email Alerts

Cyberoam will automatically send the mail alert to the administrator whenever the gateway status changes. This applies to only when Cyberoam is deployed with the Multi Gateway.

Alert mail showing the gateway status “Down “



Alert mail for the gateway status " up "



Status on Dashboard

One can always check the status of the gateway from the dashboard. Green colour against the gateway shows that the gateway is up, while Red shows that gateway is down.

Module 12: Routing

Basics of Routing

Cyberoam | Unified Threat Management

Basics of Routing

- What is routing?
- Routing Algorithm
  - Static versus dynamic
  - Single-path versus multi-path
  - Link state versus distance vector

www.cyberoam.com

Basics of Routing

What is routing?

Routing is a way to get one packet from one destination to the next. Routers or software in a computer determines the next network point to which a packet should be forwarded toward its final destination. The router is connected to at least two networks and makes a decision which way to send each data packet based on its current state of the networks it is connected to. A router is located at any point of networks or gateway, including each Internet POP. A router creates or maintains a table of the available routes and their conditions and uses this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination.

Algorithm Types

- Static versus dynamic
- Single-path versus multi-path
- Link state versus distance vector

Dynamic vs. Static

Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator prior to the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, changing networks. Most of the dominant routing algorithms in the 1990s are dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way.

Single-Path vs. Multipath

Some sophisticated routing protocols support multiple paths to the same destination. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are obvious: They can provide substantially better throughput and reliability.

Link State vs. Distance Vector

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the inter-network. Each router, however, sends only the portion of the routing table that describes the state of its own links. Distance- vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbours. In essence, link- state algorithms send small updates everywhere, while distance- vector algorithms send larger updates only to neighbouring routers.

Because they converge more quickly, link- state algorithms are somewhat less prone to routing loops than distance- vector algorithms. On the other hand, link- state algorithms require more CPU power and memory than distance- vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support. Despite their differences, both algorithm types perform well in most circumstances.

Cyberoam Routing Features

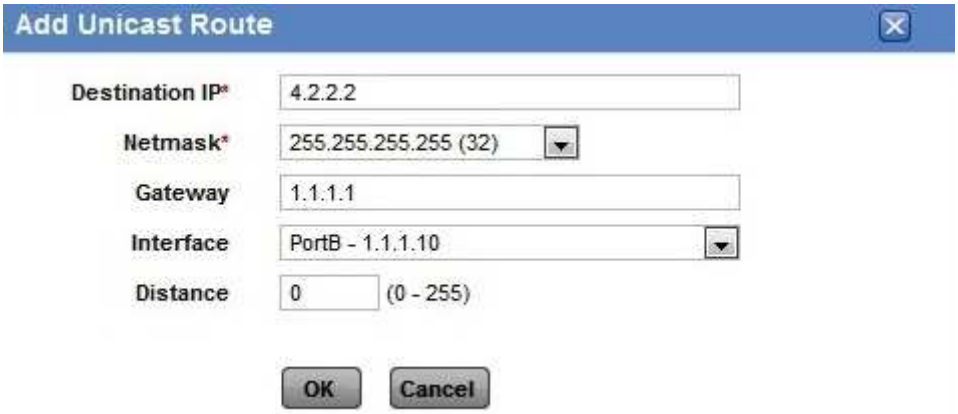
Static Routing

Static routing can be configured by adding static routes when you want to route traffic destined for specific network/host via a different next hope instead of a default route. To add static route it is required to know Destination network/Host, netmask for destination network & Next hope IP address. The gateway address specifies the next-hop router to which traffic will be routed.

A static route causes packets to be forwarded to a different next hope other than the configured default gateway. By specifying through which interface/gateway the packet will leave and to which device the packet should be routed, static routes control the traffic exiting Cyberoam.

Example: All the traffic to 4.2.2.2 should always be routed via ISP1 (1.1.1.1) This traffic will be dropped in case the interface is down.

To add the static route, in GUI, go to Network → Static Route → Add



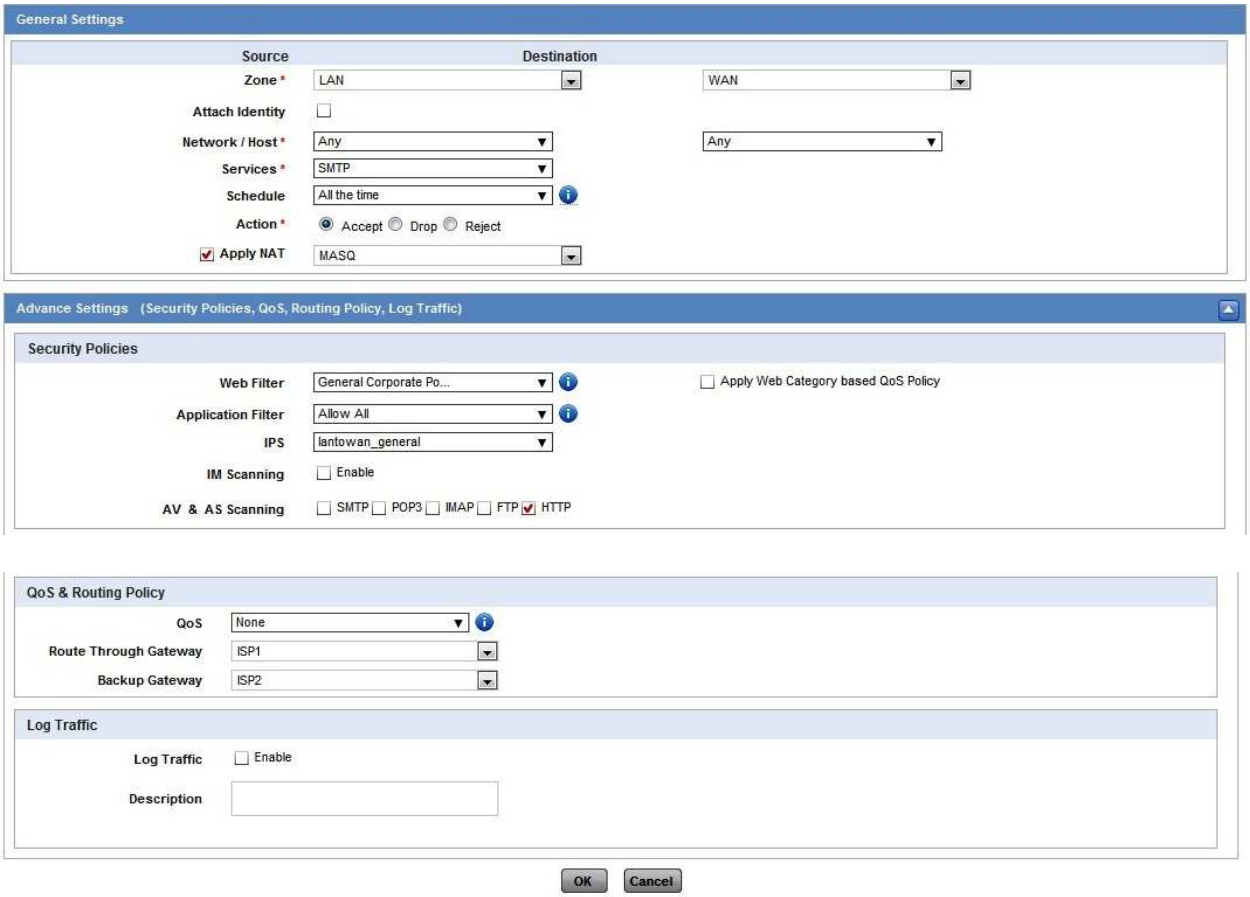
Policy Based Routing

Static routing method satisfies most of the requirements, but is limited to forwarding based on destination address only.

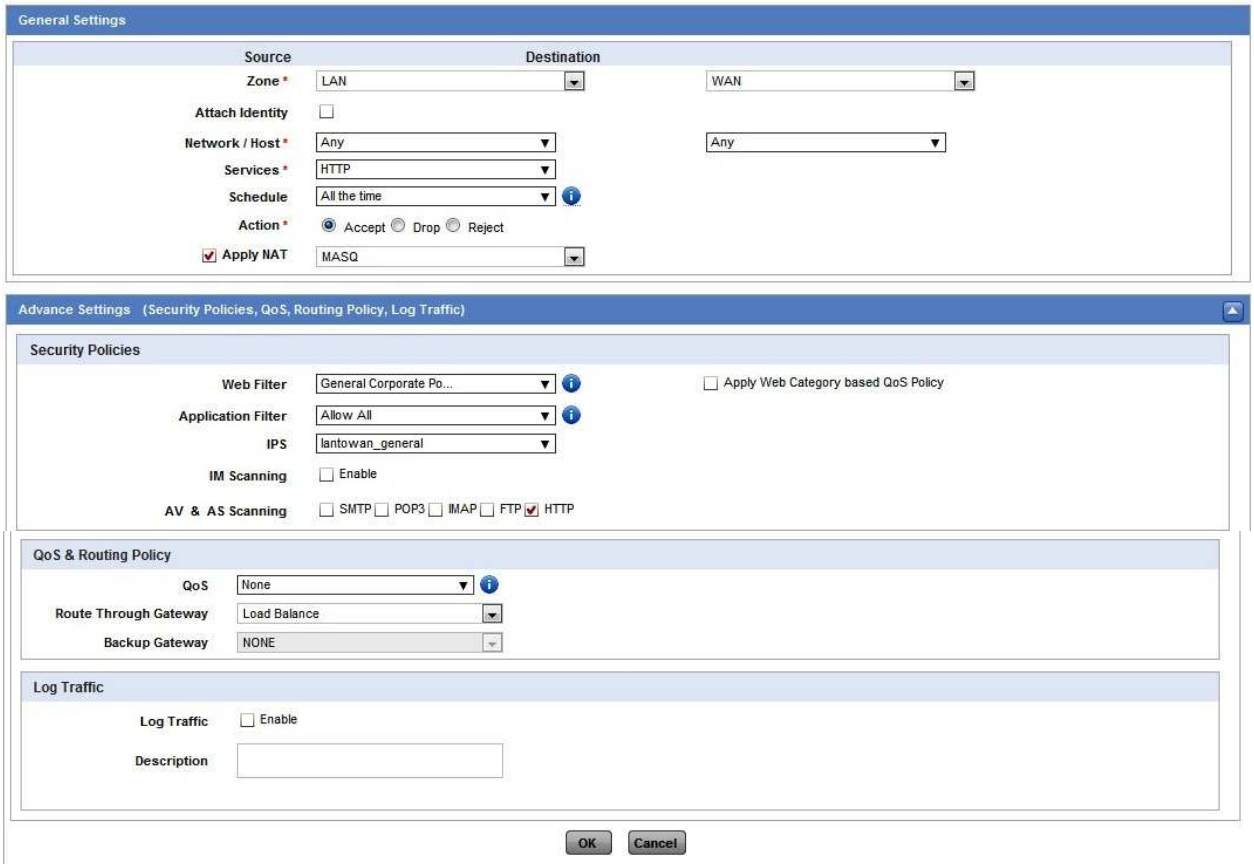
Policy based routing is extended static routes which provide more flexible traffic handling capabilities. It allows for matching based upon source address, service/application, and gateway weight for load balancing. Hence, it offers granular control for forwarding packets based upon a number of user defined variables like:

- Destination
- Source
- Application
- Combination of all of the above

All SMTP traffic routed through ISP1 with active-active gateway failover



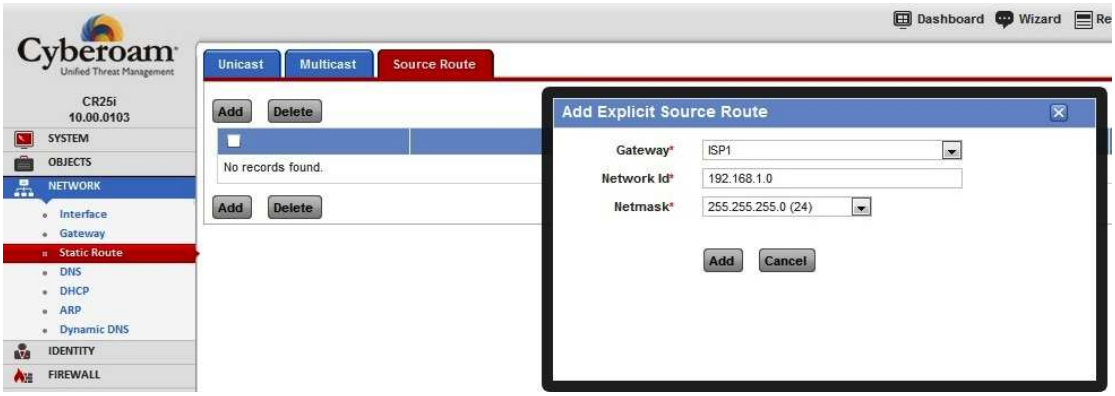
All the HTTP Traffic from LAN to WAN is active-active load balanced



Source Based Routing

Source Network routing allows Administrators to direct traffic generated from particular Network over designated links according to the business policies. When you define Source based routing for a particular subnet, all the traffic coming from that subnet will be forwarded to the defined Interface.

Select **Network → Static Routes → Source Route** and click gateway through which network traffic is to be routed



Dynamic Routing

Cyberoam supports RIP, OSPF & BGP dynamic routing protocols.

Routing Information Protocol (RIP)
Routing Information Protocol (RIP) is a distance-vector routing protocol documented in RFC 1058. RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information.
The Cyberoam implementation of RIP supports:

- RIP version 1 (as described in RFC 1058)
- RIP version 2 (as described in RFC 2453) and Plain text and Message Digest 5 (MD5) authentication for RIP Version 2

Open Shortest Path First (OSPF)
OSPF (Open Shortest Path First) is one of IGPs (Interior Gateway Protocols). Compared with RIP, OSPF can serve much more networks and period of convergence is very short. OSPF is widely used in large networks such as ISP backbone and enterprise networks.
The Cyberoam implementation of OSPF supports OSPF version 2 (as described in RFC 2328) and plain text and Message Digest 5 (MD5) authentication

Border Gateway Protocol (BGP)
BGP (Border Gateway Protocol) is a path vector protocol that is used to carry routing between routers that are in the different administrative domains (Autonomous Systems) e.g. BGP is typically used by ISPs to exchange routing information between different ISP networks.

The Cyberoam implementation of BGP supports Version 4 (RFC 1771), Communities Attribute (RFC 1997), Route Reflection (RFC 2796), Multi-protocol extensions (RFC 2858) and Capabilities Advertisement (RFC 2842)

Additionally, a firewall rule is to be configured for the zone for which the BGP traffic is to be allowed i.e. LAN to LOCAL or WAN to LOCAL.

Note: Configuration of RIP, OSPF & BGP is beyond the scope of CCNSP and is a part of CCNSE curriculum. Please refer the document on Cyberoam knowledgebase sites for configuration:

- RIP: http://kb.cyberoam.com/default.asp?id=1000&SID=&Lang=1
- OSPF: http://kb.cyberoam.com/default.asp?id=999&SID=&Lang=1
- BGP: http://kb.cyberoam.com/default.asp?id=1001&SID=&Lang=1

Multicast Routing:

Cyberoam supports multicast traffic forwarding in both Gateway / Bridge Mode. Multicast forwarding is controlled by specifying static routes for multicast traffic.

In Gateway mode, multicast forwarding needs to be enabled and then static routing needs to be configured.

In Bridge mode, only multicast forwarding needs to be enabled.

Multicast routing configuration is beyond the scope of CCNSP and is a part of CCNSE curriculum.

Refer knowledge base article for multicast routing configuration:
http://kb.cyberoam.com/default.asp?id=1021&SID=&Lang=1

Module 13: General Administration

Port Settings

System → Administration → Settings → Port Settings

Use Settings tab to make modifications in the general port settings and Web Admin Login parameters. Make changes to the login parameters for restricting the local and remote users based on the time.
By default, the port numbers are assigned to various functions performed by Cyberoam and can be modified using this tab.

Role Based Administration

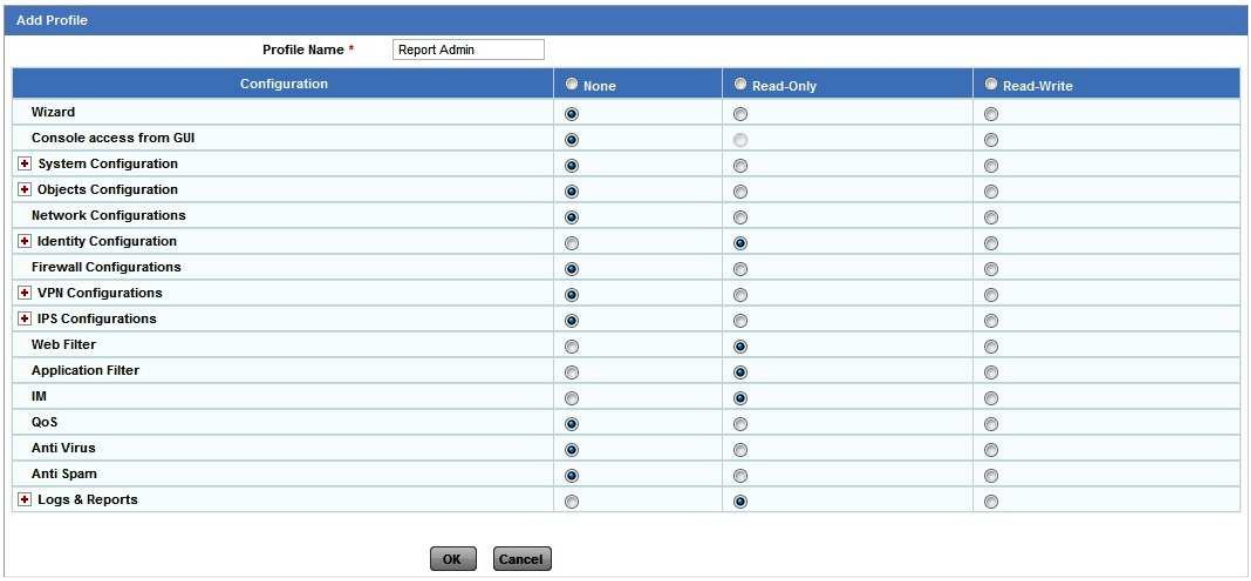
System → Administration → Profile

Use Profile tab to create profiles for various administrator users. An administrator can have various levels of privileges and thus Cyberoam provides the facility of creating profiles.

All the profiles have a different level of access to Cyberoam Web Admin Console and CLI.

Default Admin Profiles:

To Add new profile: System → Administration → Profile → Add



Available Options:

None – No access to any page

Read-Only – View the pages

Read-Write – Modify the details

Access levels can be set for individual menus as well. You can either set a common access level for all the menus or individually select the access level for each of the menu.

Click on icon against a menu to view the items under that menu.

For example, if you set access level as Read-Only against the Web Filter, the profile user would only be able to view the Web Filter menu but would not be able to make any modifications.

Now create a new user and assign the profile created before

As per the above new user configuration, profile option is only activated if we set the user type as Administrator.
Here, we have selected the user type as Administrator and we have selected the profile as we created in previous slide.

Logging Management

Cyberoam provides extensive logging capabilities for traffic, system and network protection functions by sending the logs to a remote Syslog Server. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network misuse and abuse.

Cyberoam appliance sends a detailed log to an external Syslog server in addition to the standard event log. The Cyberoam Syslog support requires an external server running a Syslog daemon on any of the UDP Port.

The Cyberoam captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred.

For Cyberoam to send logs to a Syslog Server, add Syslog Server on Cyberoam by following the below given steps from Web Admin Console:

- Select Logs & Reports → Configuration → Syslog Server → Add
- Specify unique name for Syslog server
- Specify IP address and port of the Syslog server. Cyberoam will be sent logs to the configured IP address. Default port: 514
- Select facility. Facility indicates to the Syslog server the source of a log message. It is defined by the Syslog protocol. You can configure facility to distinguish log messages from different Cyberoams. In other words, it can be helpful in identifying the device that recorded the log file.
- Select the Severity level of the messages logged. Severity level is the severity of the message that has been generated. Cyberoam logs all messages at and

above the logging severity level you select. For example, select 'ERROR' to log all messages tagged as 'ERROR,' as well as any messages tagged with 'CRITICAL,' 'ALERT' and 'EMERGENCY' and select 'DEBUG' to log all messages.

- Cyberoam produces logs in the specified format.
- Click Create to save the configuration

You can add maximum five Syslog servers on Cyberoam. Repeat above steps if you want to add multiple Syslog servers.

Once you add the Syslog server, configure logs to be send to the Syslog sever from GUI menu System → Logging → Log configuration page. If multiple servers are configured various logs can be send on different servers.

To record logs you must enable the respective log and specify logging location. Administrator can choose between on-appliance (local) logging, Syslog logging or disabling logging temporarily.

Log Type(System)	Local	SysLog
		SysLog
Firewall		
Firewall Rules	☐	☑
Invalid Traffic	☐	☑
Local ACLs	☐	☑
DoS Attack	☐	☑
Dropped ICMP Redirected Packet	☐	☑
Dropped Source Routed Packet	☐	☑
Dropped Fragmented Traffic	☐	☑
MAC Filtering	☐	☑
IP-MAC Pair Filtering	☐	☑
IP Spoof Prevention	☐	☑
IPS		
Anomaly	☐	☑
Signature	☑	☑
Anti Virus		
HTTP	☑	☑
FTP	☑	☑

IP-MAC Pair Filtering	☐	☑
IP Spoof Prevention	☐	☑
IPS		
Anomaly	☐	☑
Signature	☑	☑
Anti Virus		
HTTP	☑	☑
FTP	☑	☑
SMTP	☑	☑
POP3	☑	☑
IMAP4	☑	☑
Anti Spam		
SMTP	☑	☑
POP3	☑	☑
IMAP4	☑	☑
Content Filtering		
HTTP	☑	☑

Apply

Report Management

One of the best features of Cyberoam is the on-appliance User-based reporting. Cyberoam reports are generated and stored on local hard drive of the appliance.

The reports are available in various formats like:

- Tabular: All the reports are displayed in a tabular with clear explanation of each metric. We can sort by columns and drill down any specific information.
- Graphical: With this format, the reports are easy to read and understand.
- Printer Friendly: Reports are also available in printer friendly tabular format.
- CSV: All the reports can be exported and saved in CSV format, hence helping for long term report analysis.

There are a couple of ways to see the reports on Cyberoam.

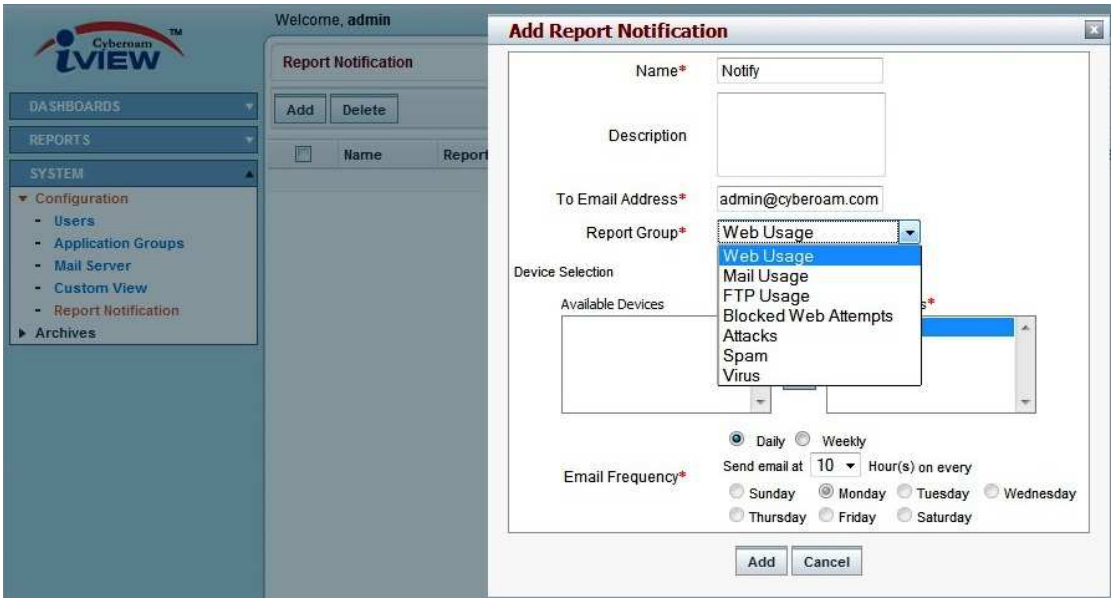
1. Login to Cyberoam Management GUI, go to Logs & Reports and click View Reports.

2. On the login page of iView, after entering the administration username (admin) and password (admin), select “Reports” from the menu


Cyberoam
iVIEW
Intelligent Logging & Reporting
Sign In
Username
Password
Login
© Elitecore Technologies Ltd.
The Program is provided AS IS, without warranty. Licensed under GPLv3. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License version 3 as published by the Free Software Foundation including the additional permission set forth in the source code header.
An Initiative by
Cyberoam
Elitecore Technologies Ltd.

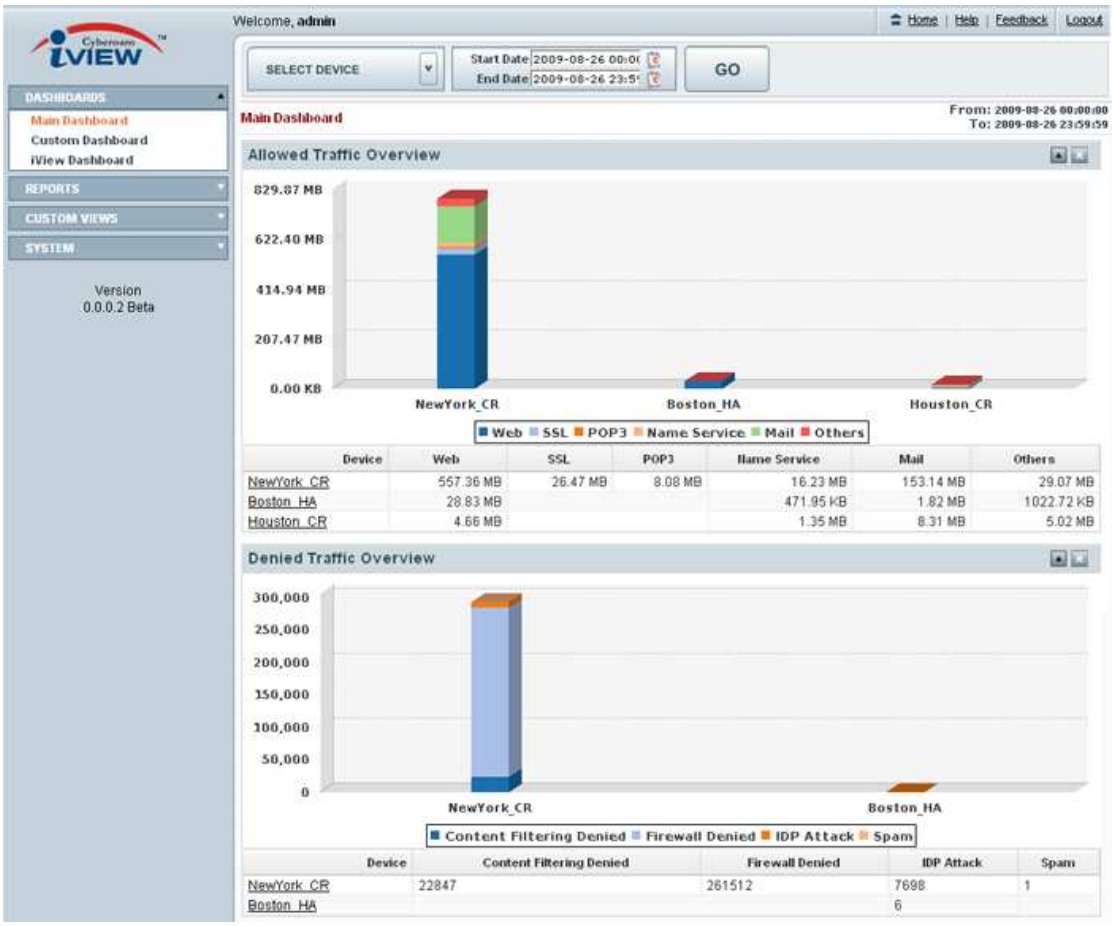
Cyberoam provides comprehensive on-appliance user-based reporting for all the UTM features including Web surfing reports, Anti-virus & Anti-spam report, Intrusion Prevention System reports along with VPN reports, Data Transfer reports, Web Trend reports for analysis and Compliance reports and Appliance Audit reports for Organisation Auditing.

The administrator can also configure to receive pre-defined reports via email on a daily or a weekly basis, from left hand menu Configure > Reports Notification.

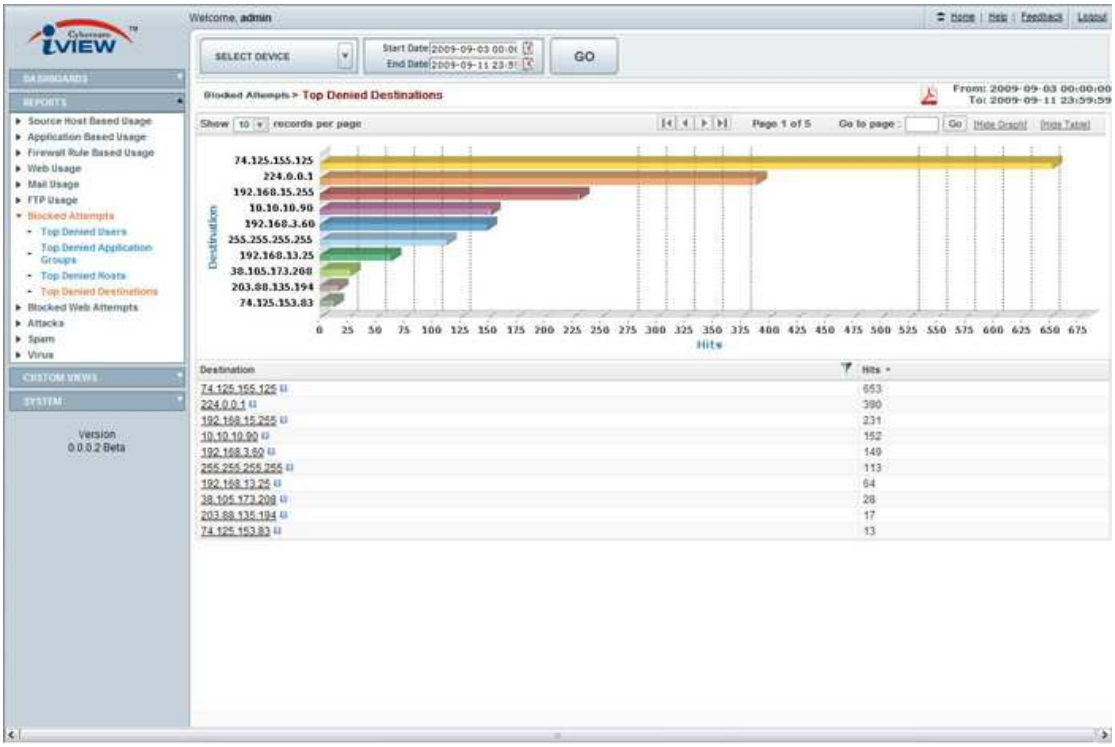


Sample Reports:

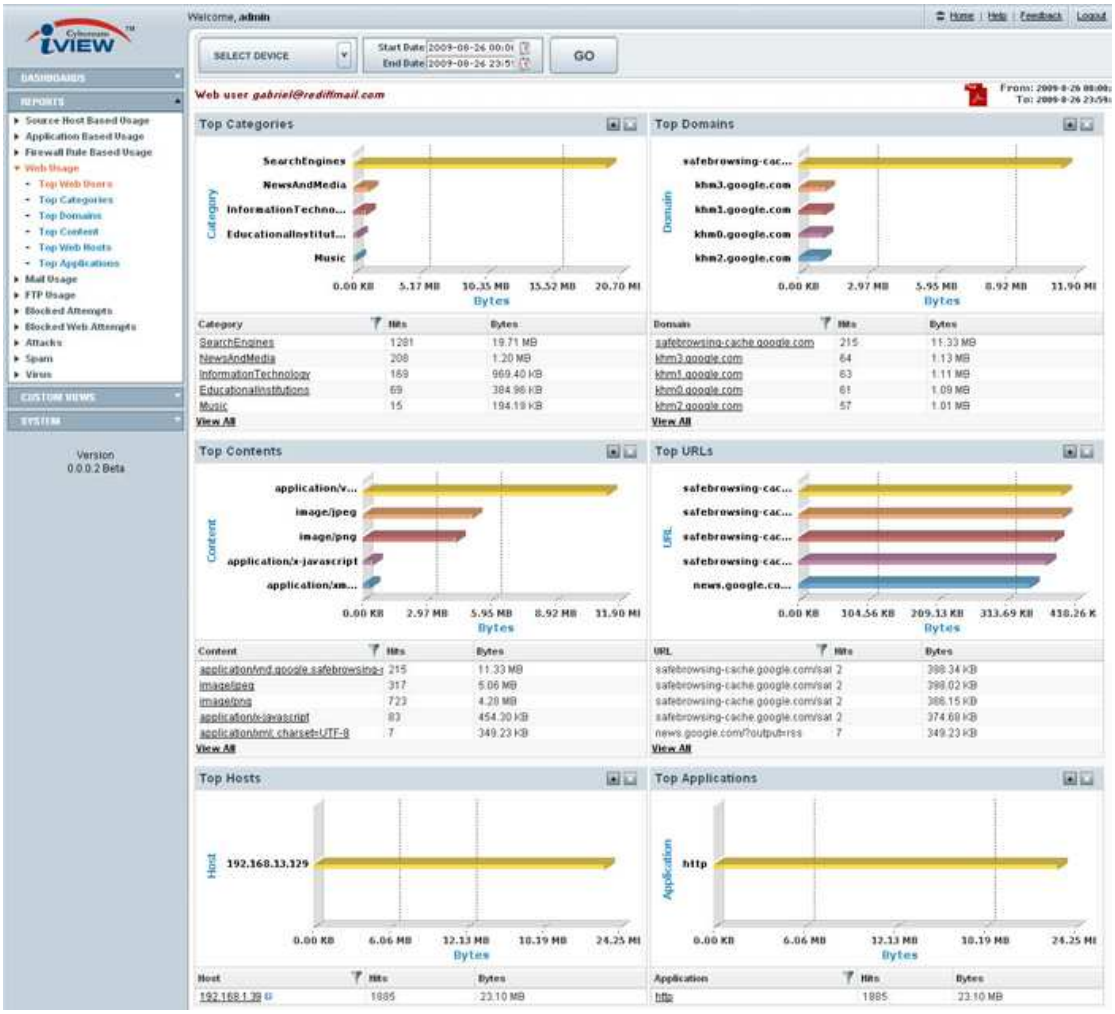
Cyberoam Reports home page: iView Main Dashboard



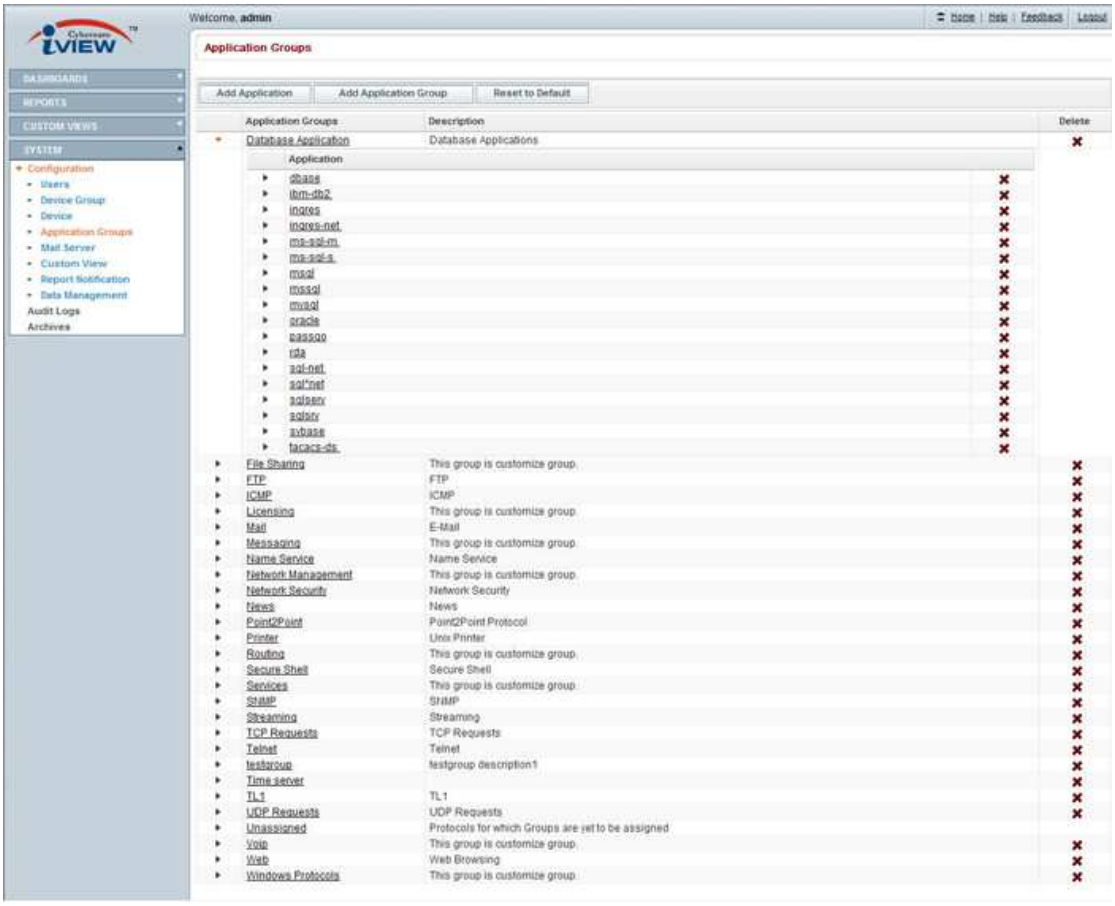
Blocked Attempt Report


Welcome, admin
Home | Help | Feedback | Logout
SELECT DEVICE
Start Date 2009-09-03 00:00
End Date 2009-09-11 23:59
GO
DASHBOARD
REPORTS
Source Host Based Usage
Application Based Usage
Firewall Rule Based Usage
Web Usage
Mail Usage
FTP Usage
Blocked Attempts
Top Denied Users
Top Denied Application Groups
Top Denied Hosts
Top Denied Destinations
Blocked Web Attempts
Attacks
Spam
Virus
CUSTOM VIEWS
SYSTEM
Version
0.0.0.2 Beta
Blocked Attempts > Top Denied Destinations
From: 2009-09-03 00:00:00
To: 2009-09-11 23:59:59
Show 10 records per page
Page 1 of 5
Go to page :
Go
Hide Graph
Hide Table
Destination
74.125.155.125
224.0.0.1
192.168.35.255
10.10.10.90
192.168.3.60
255.255.255.255
192.168.13.25
38.105.173.208
203.88.135.194
74.125.153.83
0 25 50 75 100 125 150 175 200 225 250 275 300 325 350 375 400 425 450 475 500 525 550 575 600 625 650 675
Hits
Destination
Hits
74.125.155.125 653
224.0.0.1 390
192.168.15.255 231
10.10.10.90 152
192.168.3.60 149
255.255.255.255 113
192.168.13.25 64
38.105.173.208 28
203.88.135.194 17
74.125.153.83 13

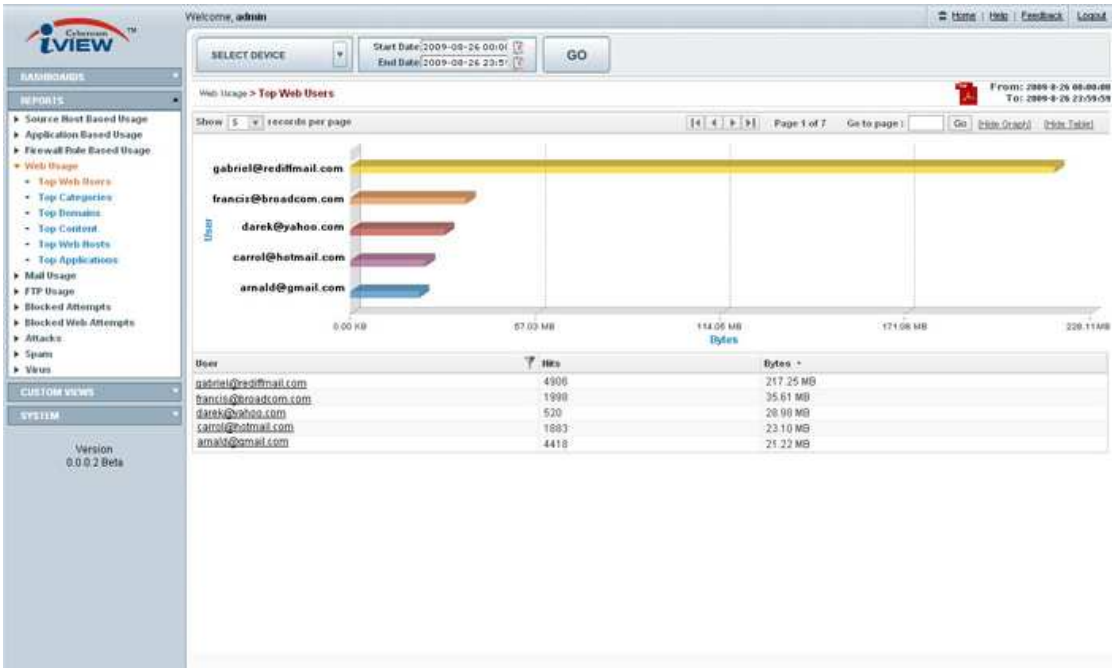
User wise Site Visit Report



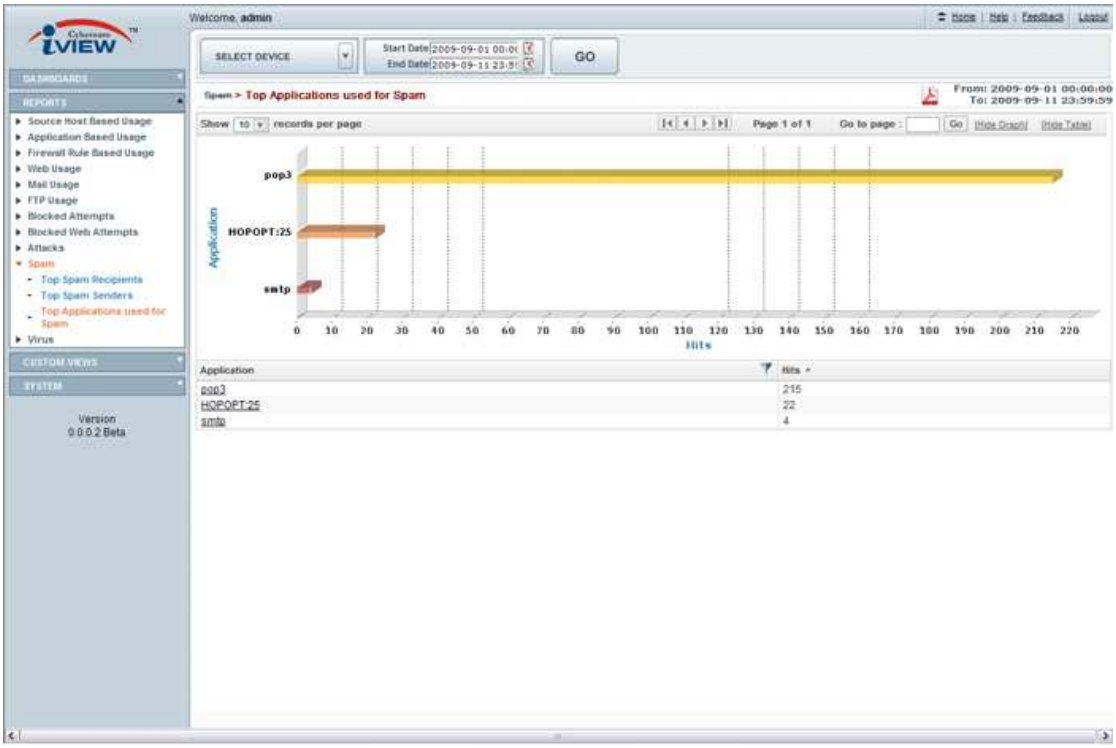
Application Groups


Welcome, admin
Home | Help | Feedback | Logout
Application Groups
DASHBOARD
REPORTS
CUSTOM VIEWS
SYSTEM
Configuration
Users
Device Group
Device
Application Groups
Mail Server
Custom View
Report Notification
Data Management
Audit Logs
Archives
Add Application
Add Application Group
Reset to Default
Application Groups
Description
Delete
Database Application
Database Applications
Application
dbase
ibm-db2
ingres
ingres-net
ms-sql-m
ms-sql-s
msql
mssql
mysql
oracle
passgo
rda
sql-net
sql*net
sqlserv
sqlsrv
sybase
tacacs-ds
File Sharing
This group is customize group
FTP
FTP
ICMP
ICMP
Licensing
This group is customize group
Mail
E-Mail
Messaging
This group is customize group
Name Service
Name Service
Network Management
This group is customize group
Network Security
Network Security
News
News
Point2Point
Point2Point Protocol
Printer
Unix Printer
Routing
This group is customize group
Secure Shell
Secure Shell
Services
This group is customize group
SNMP
SNMP
Streaming
Streaming
TCP Requests
TCP Requests
Telnet
Telnet
testgroup
testgroup description1
Time server
TL1
TL1
UDP Requests
UDP Requests
Unassigned
Protocols for which Groups are yet to be assigned
Voip
This group is customize group
Web
Web Browsing
Windows Protocols
This group is customize group

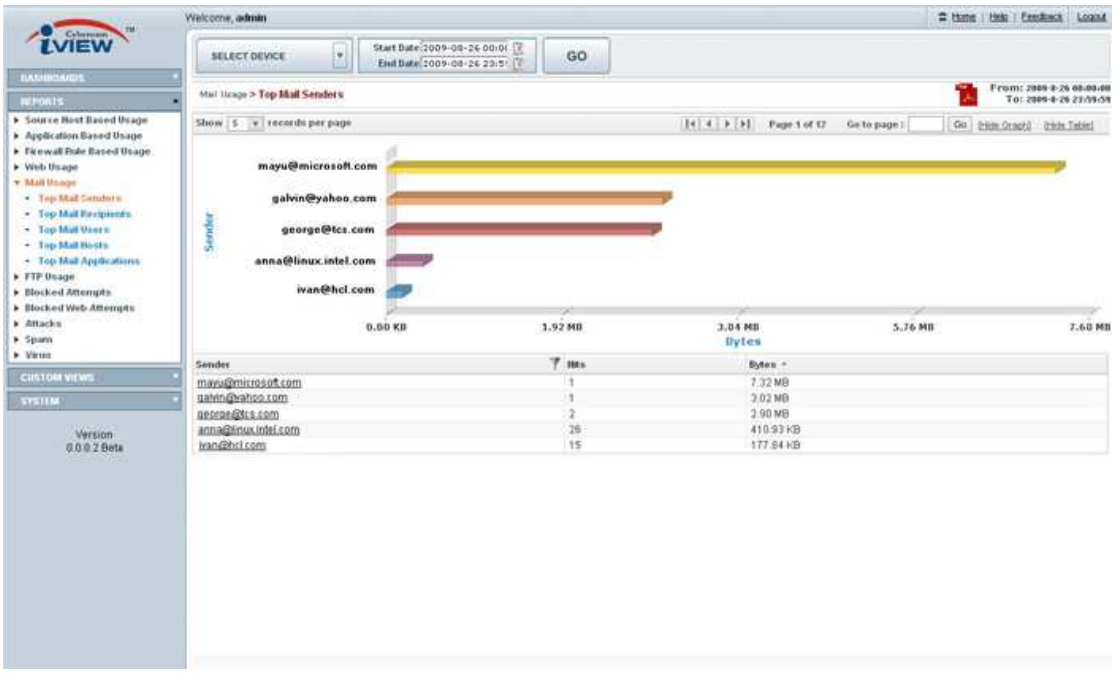
Top Web Users



Top Applications used for spam:



Top Mail Senders



DNS Management

The Domain Name System (DNS) is a system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses. In other words, it translates domain names to IP addresses and vice versa.

DNS server is configured at the time of installation. You can also add additional IP addresses of the DNS servers to which Cyberoam can connect for name resolution from GUI:

- Select Network → DNS
- Click “Obtain DNS from DHCP” to override the appliance DNS with the DNS address received from DHCP server. This option is available if enabled from Network Configuration Wizard.
- Click Add
- Enter DNS Server IP address
- Click Ok
- Click Save to save the configuration

To add multiple DNS repeat the above-described procedure. Use Move Up & Move Down buttons to change the order of DNS. If more than one Domain name server exists, query will be resolved according to the order specified.

You can change the DNS order or remove DNS entries. To change the order:

- Select Network → DNS
- Click the Server IP address whose order is to be changed

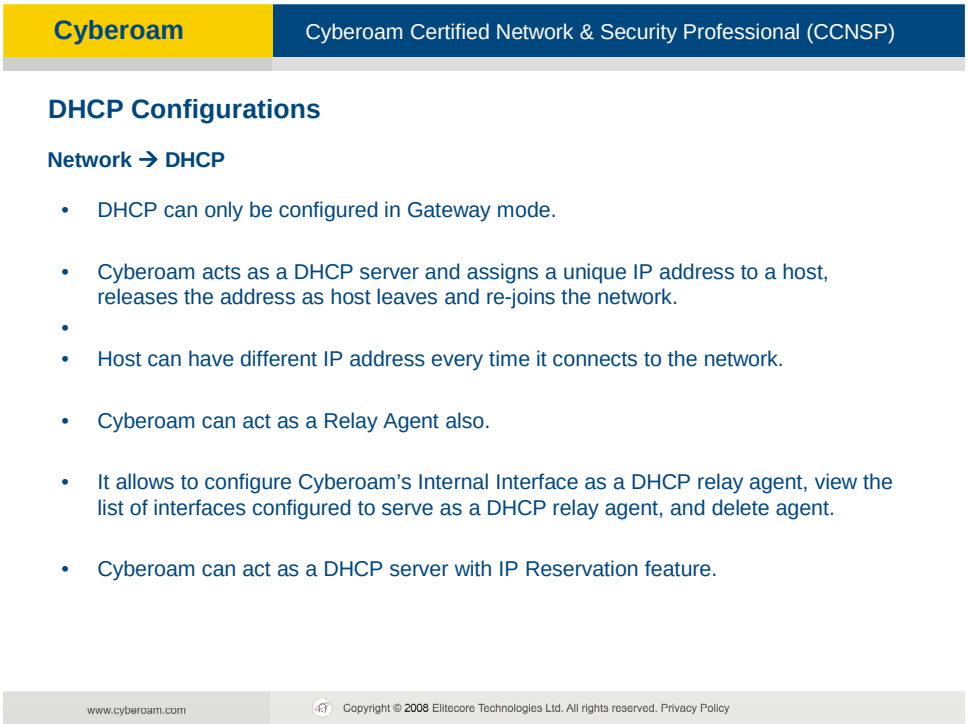
- Click Move up or Move Down as per the requirement
- Click Save to save the changes

To remove DNS Server:

1. Select Network → DNS
2. Click the Server IP address you want to remove
3. Click Remove
4. Click Save to save the changes

Multiple DNS server can also be deleted. Select multiple servers using Ctrl key

DHCP Configurations:

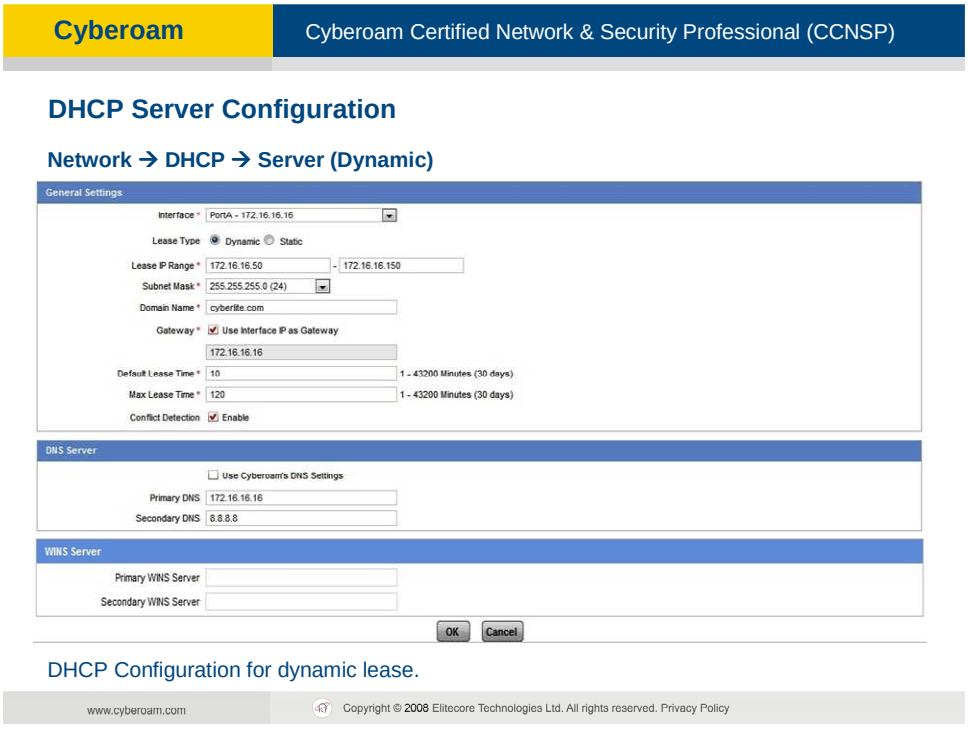


Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address for the hosts on a network reducing the Administrator's configuration task. Instead of requiring administrators to assign, track and change (when necessary) for every host on a network, DHCP does it all automatically. Furthermore, DHCP ensures that duplicate addresses are not used.

Cyberoam acts as a DHCP server and assigns a unique IP address to a host, releases the address as host leaves and re-joins the network. Host can have different IP address every time it connects to the network. In other words, it provides a mechanism for allocating IP address dynamically so that addresses can be re-used.

Go to **Network → DHCP Server → Add** to add the DHCP server, view the list of interfaces configured to serve as a DHCP server, view list of leased IPs and delete server.

DHCP Dynamic Lease:

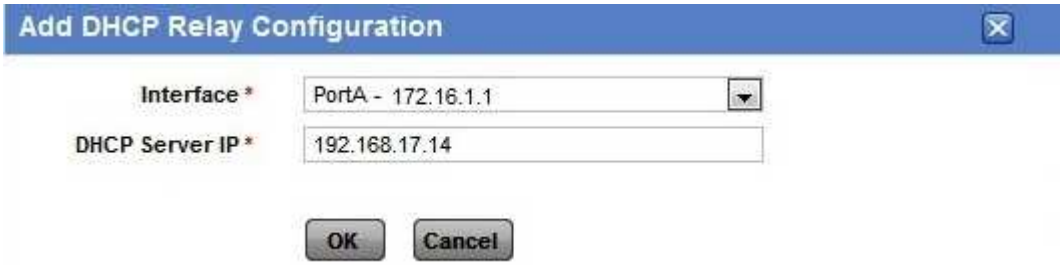


Each internal Interface can act as a DHCP server. You can disable or change this DHCP Server configuration. Cyberoam cannot act as DHCP server and DHCP Relay Agent simultaneously. Hence if Cyberoam is configured as DHCP server, you will not be able to configure it as a Relay agent and vice-versa.

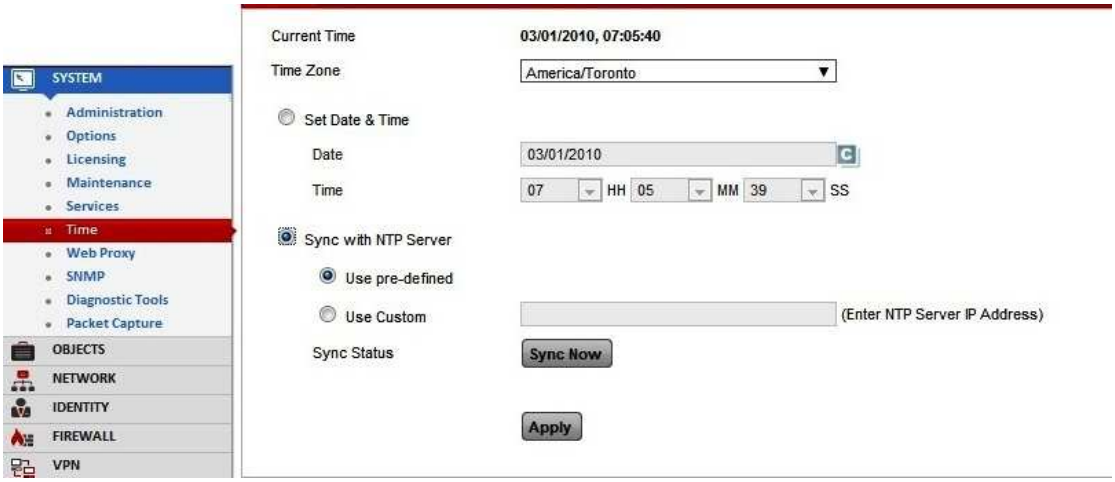
The DHCP Relay Agent allows place DHCP clients and DHCP servers on different networks. Deploying DHCP in a single segment network is easy. All DHCP messages are IP broadcast messages, and therefore all the computers on the segment can listen and respond to these broadcasts. But things get complicated when there is more than one subnet on the network. This is because the DHCP broadcast messages do not, by default, cross the router interfaces.

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If DHCP Relay Agent is not configured, clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet.

Cyberoam can act as a Relay Agent and agent can be configured from **Network → DHCP → Relay**. Page allows to configure Cyberoam's Internal Interface as a DHCP relay agent, view the list of interfaces configured to serve as a DHCP relay agent, and delete agent.



NTP Time Server support for time synchronization



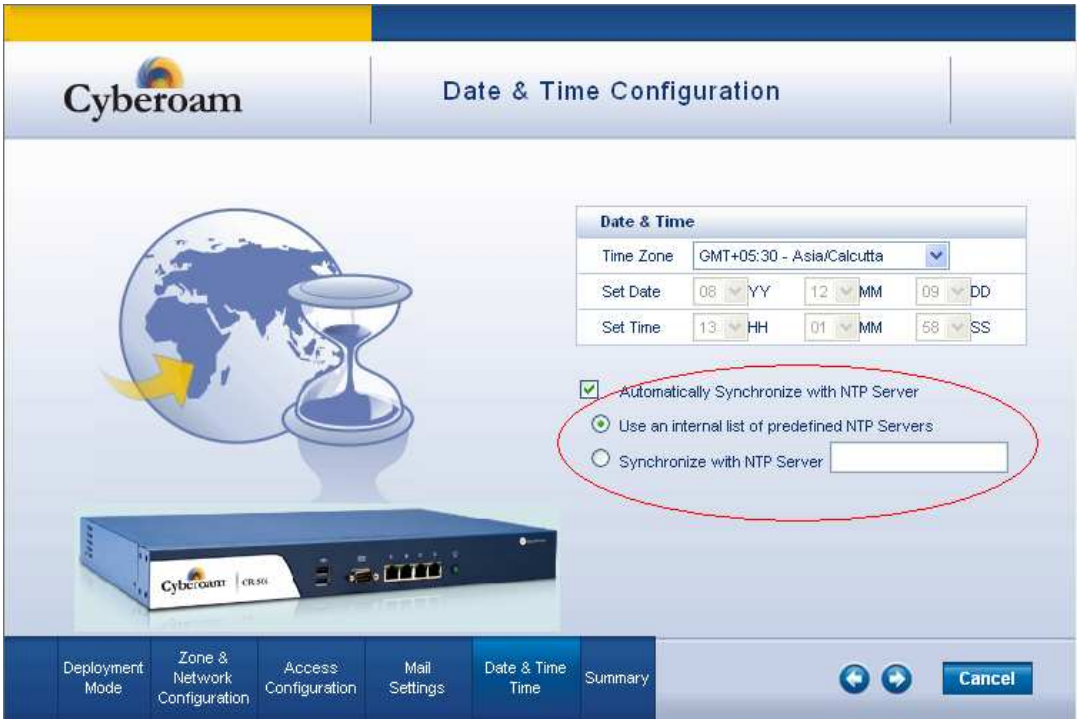
Time settings

Current date and time can be set according to the Cyberoam's internal clock or Cyberoam can be configured to synchronize its internal clock with an NTP server. Cyberoam's clock can be tuned to show the right time using global Time servers so that logs show the precise time and Cyberoam activities can also happen at a precise time.

1.Select **System → Time**
2.Select time zone according to the geographical region in which Cyberoam is deployed.

3. Select "System Date & Time" if you want to set Cyberoam's internal clock and set correct time and date
4. Select "Synchronize with NTP server" if you want Cyberoam to get time from an NTP server. Specify NTP server IP address if you want to synchronize time with a specific NTP server else use the pre-defined NTP servers.
5. Click Update button to save the configuration

Configure NTP Time Server support from Wizard



Cyberoam Upgrade

Cyberoam regularly releases new versions to include new features and bug fixes. You can check the latest Cyberoam version from Cyberoam Security Centre website – http://csc.cyberoam.com.

The current version of your Cyberoam is can be seen on the lower left hand side of the Web Admin Console as well as on the dashboard.

By default, AutoUpgrade mode is ON/Enabled which will automatically upgrade Cyberoam whenever an auto-upgrade is available.

The automatic upgrading of Cyberoam can be enabled / disabled by:

- Log on to Telnet Console
- Go to option 4 Cyberoam Console
- At the command prompt, issue the following command:

  cyberoam autoupgrade off

If automatic upgrade is disabled, you will have to upgrade Cyberoam manually. Below is the method to manually upgrade Cyberoam to the latest version.

Step 1. Check for Upgrades from Web Admin console

Press F10 to go to Dashboard from any of the screens.

Under the Installation Information section, click Check for Upgrades. Page displays the list of available upgrades and the upgrade details like release date and size.

Alternately, download upgrades from http://downloads.cyberoam.com

Repeat steps 2 to 4 for each upgrade if more than one upgrade is available. Order specifies the sequence in which Cyberoam should be upgraded. If more than one upgrade is available, please upgrade in the same sequence as displayed on the Available Upgrades page.

Step 2. Download Upgrades

Click Download against the version to be downloaded and follow the on-screen instructions to save the upgrade file.

Step 3. Upload downloaded version to Cyberoam

Select **Help → Upload Upgrade**

Type the file name with full path or select using 'Browse' and click Upload

Step 4. Upgrade

Once the upgrade file is uploaded successfully, log on to Console to upgrade the version.

Log on to Cyberoam Telnet Console

Type '6' to upgrade from the Main menu and follow on-screen instructions

Type '1' to upgrade from the uploaded file and follow on-screen instructions

Backup – Restore Management

System → Maintenance → Backup & Restore

Backups are necessary in order to recover data from the loss due to the disk failure, accidental deletion or file corruption.

Different types of logs are generated and maintained by Cyberoam. Cyberoam provides a facility of taking backup of all the logs, both through scheduled automatic backup and manual backups.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Backup-Restore Management

System → Maintenance → Backup & Restore

- Once the backup is taken, you need to upload the file for restoring the backup.
- Restoring data older than the current data will lead to the loss of current data.
- The restore facility is version dependent, it will work only if the backup and restore versions are the same. Also, if HA is configured, you need to disable HA before restoring the backup.
- Upload the backup file: **System → Maintenance → Backup & Restore**

- After upload, log on to Console based Administration (using TELNET) Go to Option 5 – Cyberoam Management > Option 6 – Restore Backup and follow screen steps to restore data.

Diagnostic Tools

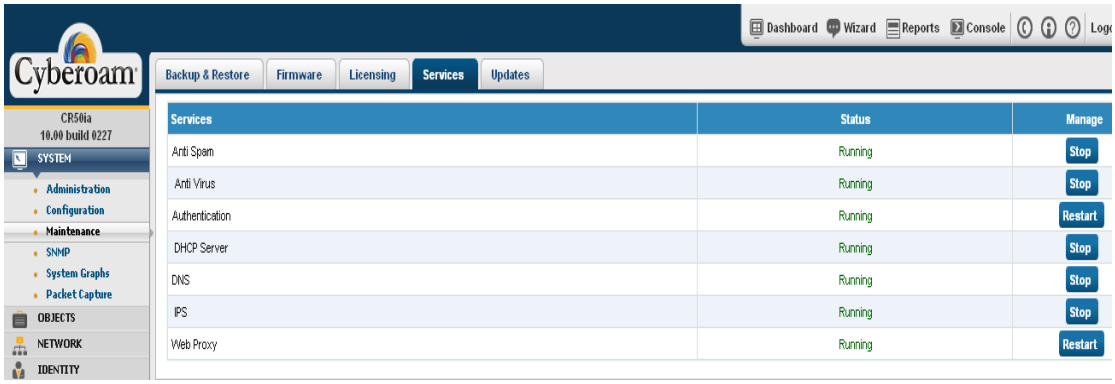
Analytical Tool checks the health of the System in a single shot. It is used for troubleshooting and diagnosing problems found in the System.

Analytical Tool is like a periodic health check up that helps to identify the impending System related problems. After identifying the problem, appropriate actions can be taken to solve the problems and keep the System running smoothly and efficiently.

Analytical Tool shows the status of System. Based on the status, Administrator can judge whether the respective System component is working fine (OK Status), is facing a minor problem (Warning Status) or is having a major problem (Critical Status).

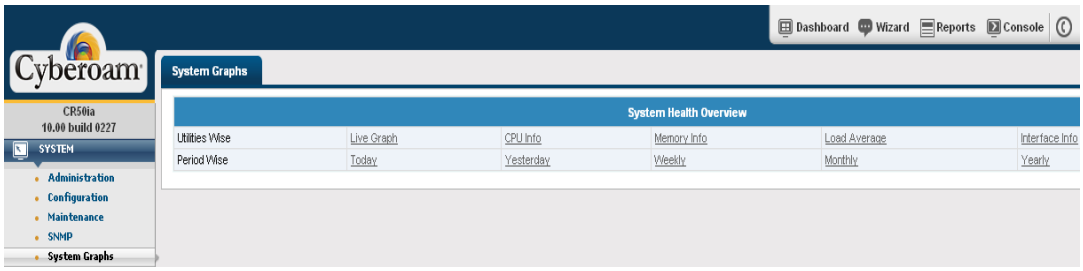
Diagnostic Tools: Services Status

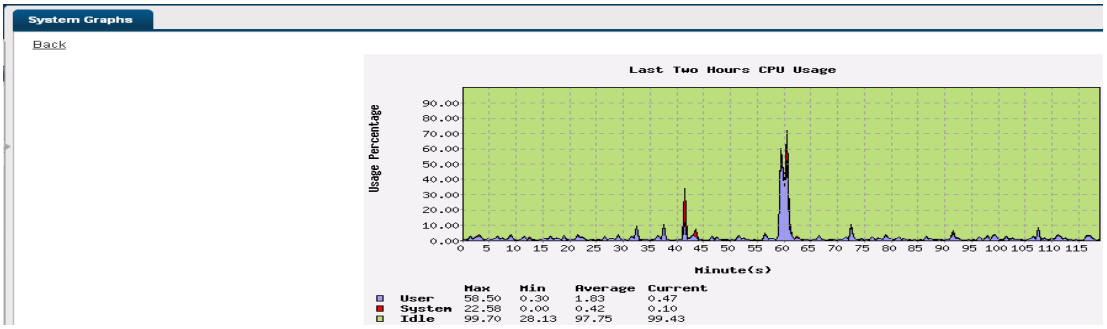
System → Maintenance → Services



Diagnostic Tools: System health graphs

System → System Graphs





Troubleshooting: Event Viewer

Shows live logs for IPS, Web & application filter, IM, Antivirus.

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Troubleshooting: Event Viewer

Logs & Reports → Event Viewer

Event Viewer page allows to view the live logs for event modules like:

- IPS
- Web Filter
- Anti Spam
- Anti Virus
- Firewall
- IM

This page gives concentrated information about all the events that occurred under respective modules.

Event Viewer: Web Filter

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Event Viewer

Logs & Reports → Event Viewer → Web Filter

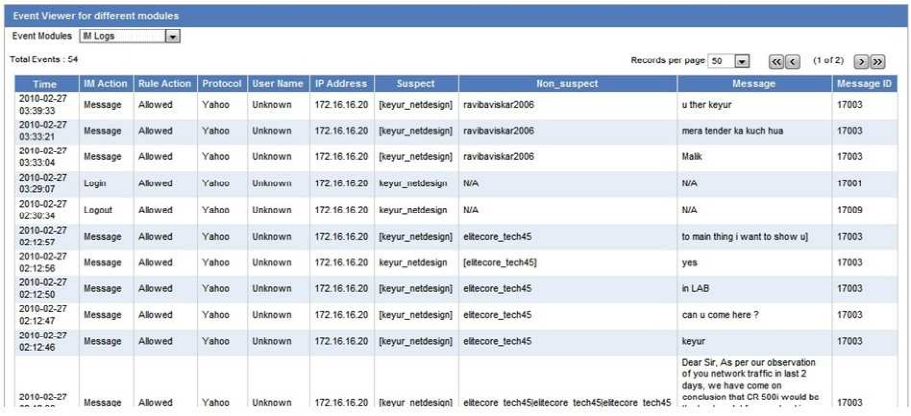
Time	Action	User Name	Source IP	Destination IP	Category	URL	Bytes Transfer	Message ID
2010-02-27 04:07:45	Allowed		172.16.16.50 :55985	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:07:13	Allowed		172.16.16.50 :43359	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:06:41	Allowed		172.16.16.50 :36464	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:06:09	Allowed		172.16.16.50 :38876	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:06:04	Allowed		172.16.16.20 :38865	212.58.226.79 :80	NewsAndMedia	http://newsrss.bbc.co.uk /rss/newsonline_world_editio...	27393	16001
2010-02-27 04:05:37	Allowed		172.16.16.50 :55478	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:05:04	Allowed		172.16.16.50 :56074	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:04:32	Allowed		172.16.16.50 :52195	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	1462	16001
2010-02-27 04:04:00	Allowed		172.16.16.50 :59125	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:03:13	Allowed		172.16.16.50 :60390	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001
2010-02-27 04:02:54	Allowed		172.16.20.25 :51079	74.220.207.169 :80	None	http://congaro.com/spm/page.php	92	16001
2010-02-27 04:02:41	Allowed		172.16.16.50 :60994	64.191.223.35 :80	IPAddress	http://64.191.223.35/SpamResolverNG /SpamResolverNG.d...	58	16001

Event Viewer: IM

Cyberoam | Cyberoam Certified Network & Security Professional (CCNSP)

Event Viewer

Logs & Reports → Event Viewer → IM



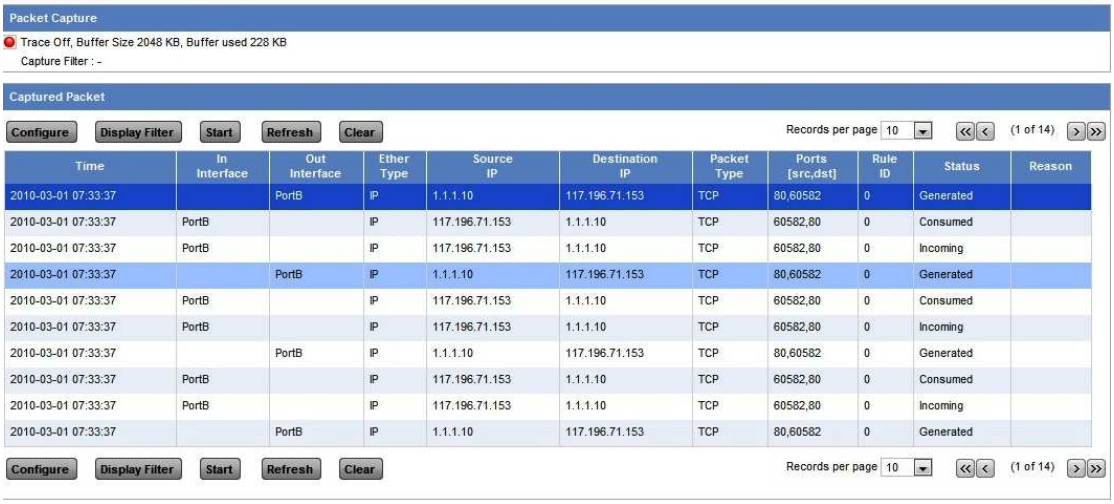
Time	IM Action	Rule Action	Protocol	User Name	IP Address	Suspect	Non_suspect	Message	Message ID
2010-02-27 03:39:33	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	ravibaviskar2006	u ther keyur	17003
2010-02-27 03:33:21	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	ravibaviskar2006	mera tender ka kuch hua	17003
2010-02-27 03:33:04	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	ravibaviskar2006	Malik	17003
2010-02-27 03:29:07	Login	Allowed	Yahoo	Unknown	172.16.16.20	keyur_netdesign	N/A	N/A	17001
2010-02-27 02:30:34	Logout	Allowed	Yahoo	Unknown	172.16.16.20	keyur_netdesign	N/A	N/A	17009
2010-02-27 02:12:57	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	elitecore_tech45	to main thing i want to show u]	17003
2010-02-27 02:12:56	Message	Allowed	Yahoo	Unknown	172.16.16.20	keyur_netdesign	[elitecore_tech45]	yes	17003
2010-02-27 02:12:50	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	elitecore_tech45	in LAB	17003
2010-02-27 02:12:47	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	elitecore_tech45	can u come here ?	17003
2010-02-27 02:12:46	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	elitecore_tech45	keyur	17003
2010-02-27	Message	Allowed	Yahoo	Unknown	172.16.16.20	[keyur_netdesign]	elitecore_tech45[elitecore_tech45[elitecore_tech45	Dear Sir, As per our observation of you network traffic in last 2 days, we have come on conclusion that CR 500i would be	17003

Event Viewer: Anti Virus

Logs & Reports → Event Viewer → Anti Virus

Packet Capture:

Packet capture displays dropped packets details on the specified interface. It will provide connection details and details on which module is dropping packets e.g. firewall, IPS along with information like firewall rule number, user, Web and Application Filter policy number etc. This will help Cyberoam administrators to troubleshoot errant firewall rule.



Trace On - packet capturing is on
Trace Off - packet capturing is off.

Captured packets fill the buffer up to a size of 2048 KB. While the packet capturing is on, if the buffer used exceeds the stipulated buffer size, packet capturing stops automatically. In such a case, you would have to manually clear the buffer for further use.

Capture Filter – There are various filter conditions for capturing the packets. The BPF String is used for filtering the packet capture.

For example, Capture Filter - host 192.168.1.2 and port 137

Configure Button
Open a popup window to configure following general settings for capturing:

•Number of Bytes to Capture (per packet)
•Wrap Capture Buffer Once Full

Enter BPF String - BPF (Berkeley Packet Filter) sits between link-level driver and the user space. BPF is protocol independent and use a filter-before-buffering approach. It includes a machine abstraction to make the filtering efficient. e.g. host 192.168.1.2 and port 137

Display Filter Button
Log can be filtered as per the following criteria: Interface Name, Ether Type, Packet Type, Source IP Address, Source Port, Destination IP Address, Destination Port

Troubleshooting and Debugging Tools

Majority of the real time troubleshooting commands are available on Cyberoam CLI.

TCPDUMP

Tcpdump is a packet capture tool that allows intercepting and capturing packets passing through a network interface, making it useful for understanding and troubleshooting network layer problems.

Usage

Use from Cyberoam Telnet Console, option 4 Cyberoam Console

How to view traffic of the	tcpdump command	Example
specific host	tcpdump 'host <ipaddress>'	tcpdump 'host 10.10.10.1'
specific port	tcpdump 'port <port-number>'	tcpdump 'port 21'
specific host for the particular port	tcpdump 'host <ipaddress> and port <port-number>'	tcpdump 'host 10.10.10.1 and port 21'
the specific host for all the ports except SSH	tcpdump 'host <ipaddress> and port not <port-number>'	tcpdump 'host 10.10.10.1 and port not 22'
specific protocol	tcpdump 'proto ICMP' tcpdump 'proto UDP' tcpdump 'proto TCP' tcpdump 'arp'	

Note: Expression can be combined using logical operators AND or OR and with NOT also. Make sure to use different combinations within single quotes.

Analysing tcpdump output

corporate> tcpdump 'port 21'
Kernel filter, protocol ALL, datagram packet socket
tcpdump: listening on all devices

12:29:33.860721 eth0 < 172.16.16.81.1633 > 161.114.22.105.ftp: S 4023323694:4023323694(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)

12:29:33.860769 eth1 > 192.168.13.40.1633 > 161.114.22.105.ftp: S 4023323694:4023323694(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)

12:29:33.861293 eth1 < 161.114.22.105.ftp > 192.168.13.40.1633: S 1587918290:1587918290(0) ack 4023323695 win 5840 <mss 1460> (DF)

12:29:33.861324 eth0 > 161.114.22.105.ftp > 172.16.16.81.1633: S 1587918290:1587918290(0) ack 4023323695 win 5840 <mss 1460> (DF)

12:29:33.861530 eth0 < 172.16.16.81.1633 > 161.114.22.105.ftp: . 1:1(0) ack 1 win 65535 (DF)

12:29:33.861567 eth1 > 192.168.13.40.1633 > 161.114.22.105.ftp: . 1:1(0) ack 1 win 65535 (DF)

1st line:
Brown color shows timestamp of the packet
Green color shows the incoming interface

Blue color shows source address who originates the request

Red color shows destination IP address

Orange color shows services which is being accessed

Pink color shows flag of particular packet. This is new connection originated by 172.16.16.81 IP address & destined for 161.114.22.105 to access FTP services. This is first packet so flag is set to Sync "S"

3rd line: As three ways handshaking needs to be complete, second packet is the response coming back from server with "Ack" for Sync packet. This is nothing but "Syn-Ack" packet.

4th Line: "Ack" packet sent by source for "Syn-Ack". For any tcp connection first three lines are like

Source to Destination-- Sync

Destination to Source-- Sync-Ack

Source to Destination—Ack

Generate binary file of traffic log generated with custom parameters

Cyberoam also supports to save and download the tcpdump output in a binary file from Telnet Console.

File tcpdump contains the troubleshooting information useful to analyse the traffic with advanced tool like ethereal for Cyberoam Support team.

To save the output in the downloadable file, log on to Telnet Console:

- Go to Option 4 Cyberoam Console
- At the command prompt, issue the command:

  tcpdump <criteria> filedump

Cyberoam saves this file under the name tcpdump.out

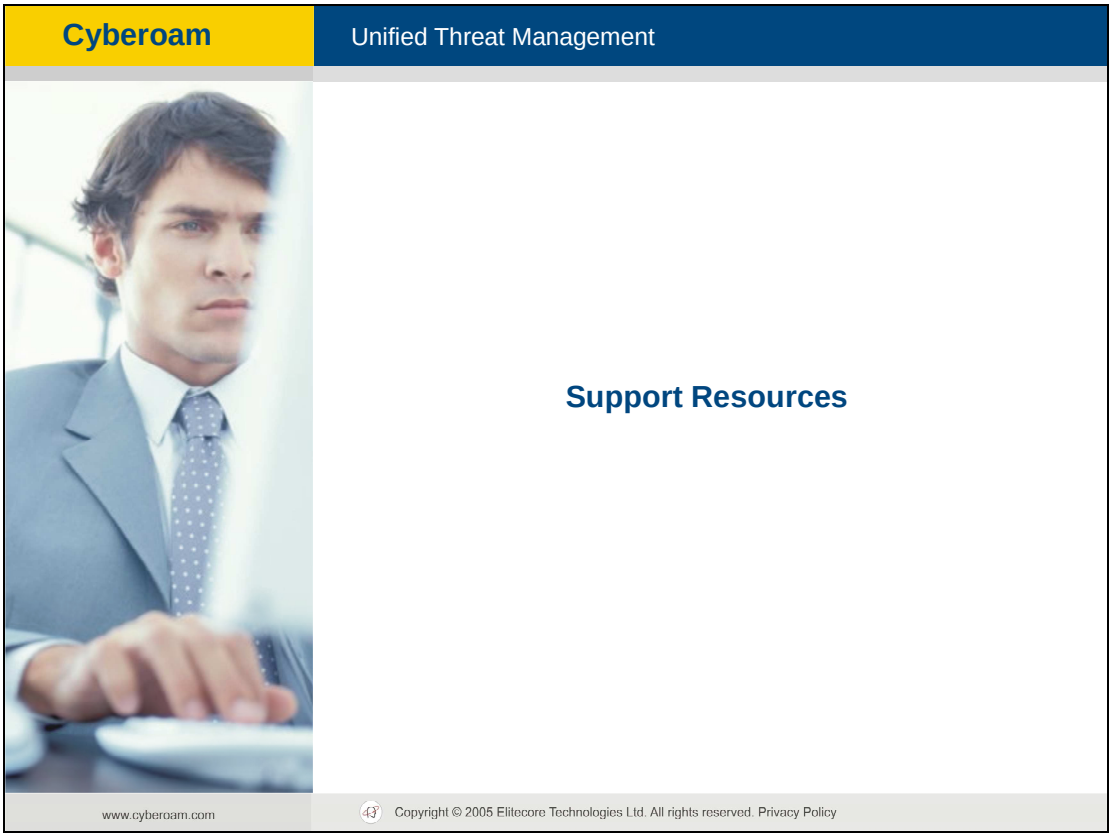
Download from http://<cyberooam_ip>/documents/tcpdump.out and mail this file to Cyberoam Support team at support@cyberoam.com

Monitoring VPN traffic

Cyberoam will automatically configure VPN IPSec interface for each WAN port configured. For example, if Port B and Port C are configured as WAN ports then Cyberoam will configure ipsec0 and ipsec1 for Port B and Port C respectively.

Use these IPSec ports to monitor VPN traffic e.g. tcpdump "-i ipsec0"

Support Resources



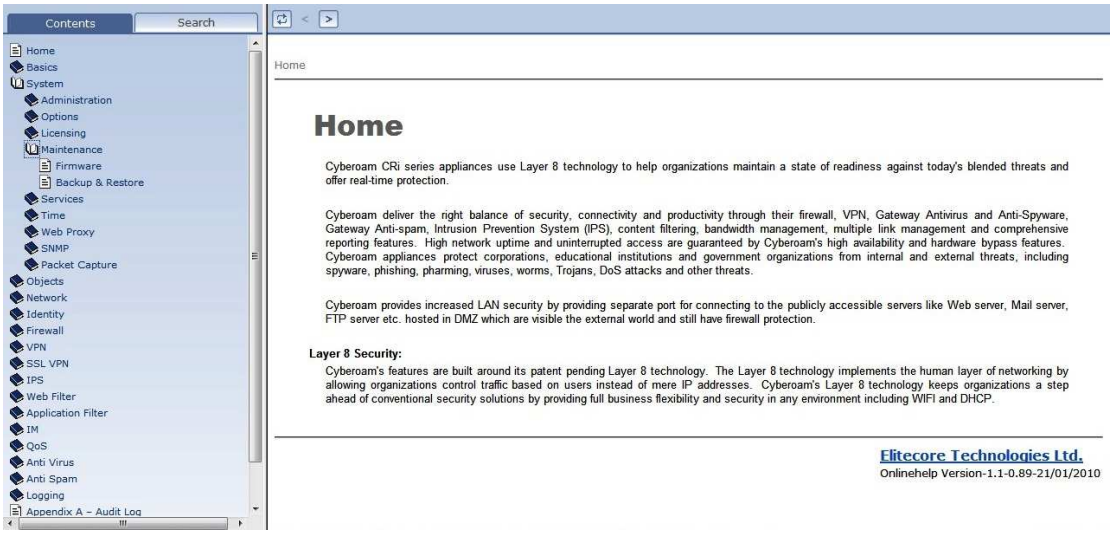
Agenda:

- On Appliance Help
- Online Resources
- Customer My Account
- Partner Portal
- Support Contact

On Appliance Help

Cyberoam appliance provides On-Appliance context sensitive help for each option. Help is just one click away from you. You just need to click on “Help” button on the top bar:

To utilise On-Appliance help there is no need of Internet connectivity as complete help is stored in appliance and available in offline mode.

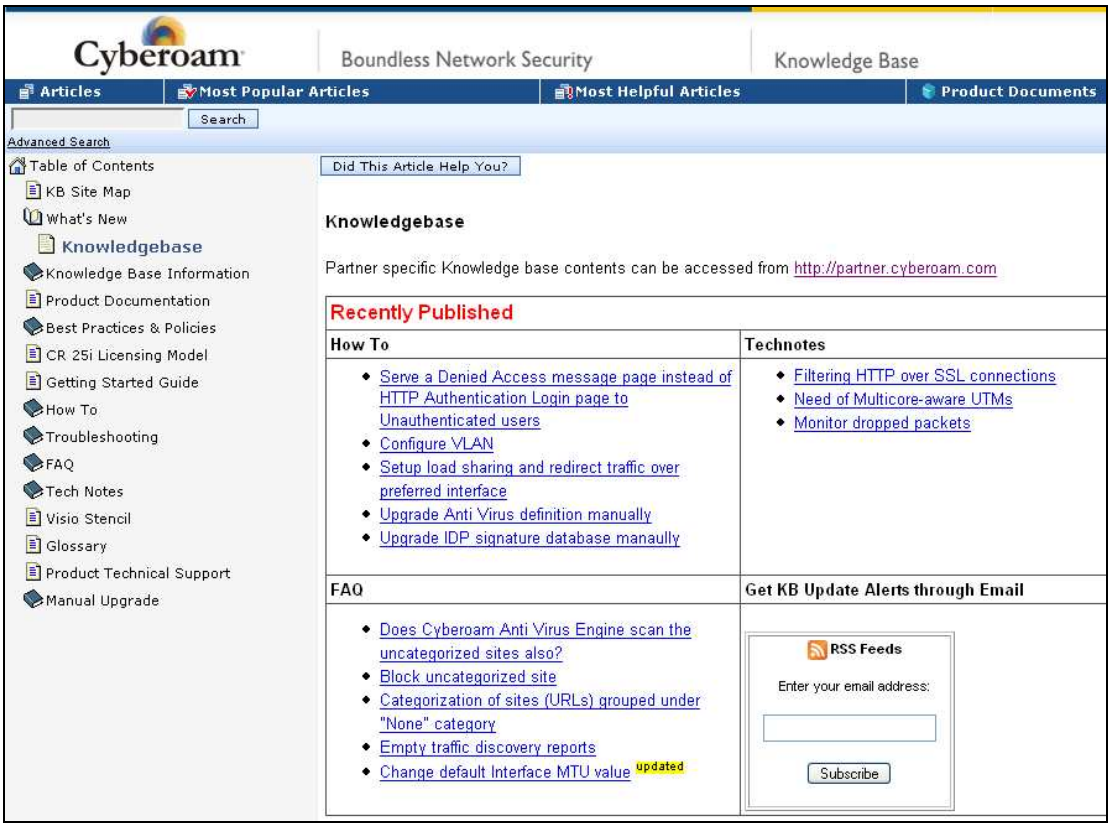


Online Resource (Web Resource)

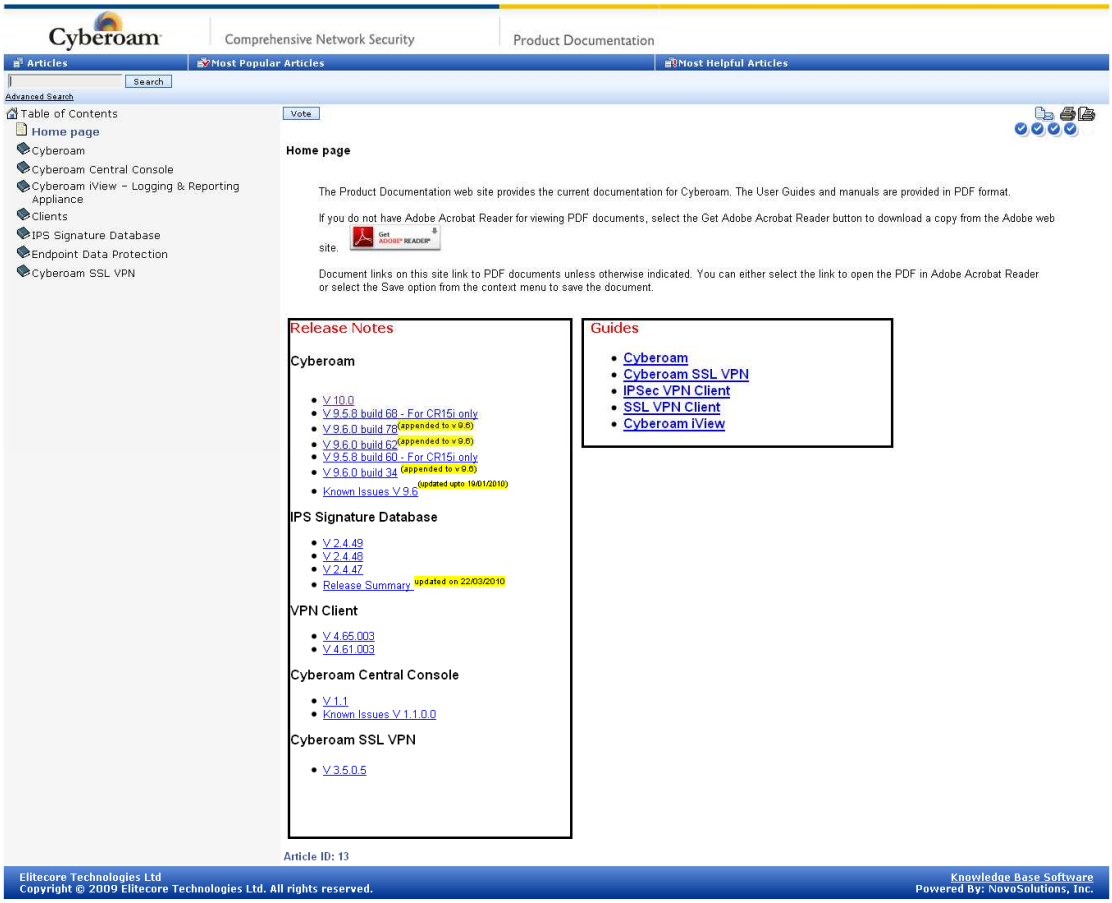
Cyberoam provides plenty of online resources to help you in Cyberoam frequent configuration and keep you updated with Cyberoam technologies, releases.

Online resource list:

Cyberoam Knowledge Base (http://kb.cyberoam.com):

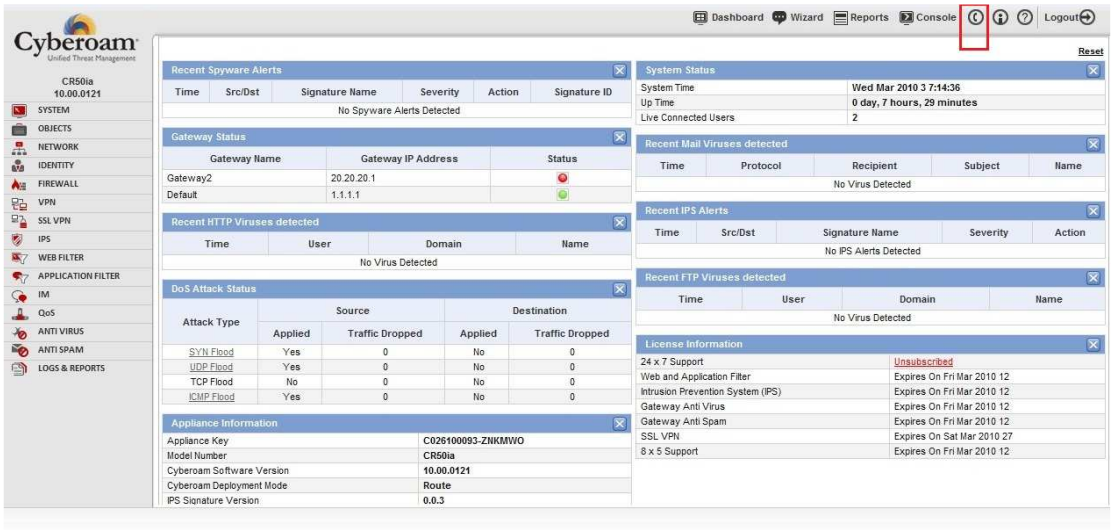


Cyberoam Product Documentation (http://docs.cyberoam.com)



Cyberoam Security Center (http://csc.cyberoam.com):

Customer My Account



Partner Portal

Partner Portal (http://partner.cyberoam.com):

Presales Contact Details:

Email Support:

EMEA	emeapartners@cyberoam.com
APAC	apacpartners@cyberoam.com
Latin America	lapartners@cyberoam.com
North America and Canada	uspresales@cyberoam.com
India	indiapresales@cyberoam.com
SAARC Countries	saarc@cyberoam.com

Chat support: http://www.cyberoam.com/presalessupport

Telephonic Presales Support:

Region	Toll Free Number	Non Toll Free Number
USA	+1-877-777-0368	+1-973-302-8446
Europe	+44-808-120-3958	+44-203-355-7917
APAC	+1-877-777-0368	+1-973-302-8446
Middle East & Africa	+1-877-777-0368	+1-973-302-8446
India	1-800-301-00013	+91-79-66065777

Support Contact

For any technical assistance, contact us through:

- Web Support:
  - Customers: http://customer.cyberoam.com
  - Partners: http://partner.cyberoam.com
- Chat Support: http://www.cyberoam.com/contactsupport.html
- Email Support: support@cyberoam.com
- Telephonic Support

Region	Toll Free Number	Non Toll Free Number
USA	+1-877-777-0368	+1-973-302-8446
Europe	+44-808-120-3958	+44-203-355-7917
APAC	+1-877-777-0368	+1-973-302-8446
Middle East & Africa	+1-877-777-0368	+1-973-302-8446
India	1-800-301-00013	+91-79-66065777