Cyberoam
A SOPHOS Company

Cyberoam Reviewer's Guide

Document Version 10.6.1-25-07-2014

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

General Information

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640: www.cyberoam.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-66065777
Email: support@cyberoam.com
Web site: www.cyberoam.com
Visit www.cyberoam.com for the regional and latest contact information.

Additional Resources

Visit following links for more information to configure Cyberoam

Technical Documentation - http://docs.cyberoam.com
Cyberoam Knowledge Base - http://kb.cyberoam.com
Cyberoam Security Center - http://csc.cyberoam.com
Cyberoam Upgrades - http://customer.cyberoam.com

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Important Notice

Cyberoam Technologies Pvt. Ltd. has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Cyberoam Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Cyberoam Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

Use of this product and document is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam UTM Appliances. You will find the copy of the EULA at http://www.cyberoam.com/documents/EULA.html and the Warranty Policy for Cyberoam UTM Appliances at http://kb.cyberoam.com.

RESTRICTED RIGHTS

Copyright 1999 - 2014 Cyberoam Technologies Pvt. Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

Corporate Headquarters

Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640 Website: www.cyberoam.com

Contents

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Preface

Thank you for purchasing the award-winning, future-ready Cyberoam Security Appliance.

Welcome to Cyberoam Reviewer’s Guide! This document is designed to ensure that you are easily able to use the basic features of Cyberoam. It contains configuration guidelines on the simplest and commonest use-case scenarios to be performed after a Cyberoam appliance is up and running in your network.

In addition to this guide, you can access online help by clicking **More Options >** **Help** located on the right most corner of every page of GUI. Please ensure that the management computer is connected to the Internet to access On-Cloud Context Sensitive Online Help. The entire Cyberoam documentation set is available at http://docs.cyberoam.com and http://kb.cyberoam.com.

The configuration given in the document is to be performed from Web Admin Console (GUI) of Cyberoam unless specified.

Cyberoam - Future-ready Security Appliances

Cyberoam’s NG Series of Security Appliances offer high-speed security to organizations through their unique, user identity-based policy controls. They enable organizations to keep stride with the current and future IT trends which include Internet of Things, data moving at 100 times the current speeds, super-fast wireless connections, critical business applications and services moving to the Web, Internet access devices multiplying per user and a tremendous increase in data usage. The gargantuan performance leap in Cyberoam ensures that while a company’s growth and productivity increases in leaps and bounds, its security follows close at their heels.

This Reviewer’s Guide has been written with respect to CR 2500iNG-XP, which is part of Cyberoam’s NG Series. It brings with it a whole new range of features: an intuitive next-generation GUI and a revamped reporting mechanism.

The all-new Firmware – CyberoamOS: The NG series appliances are based on CyberoamOS – the most intelligent and powerful Cyberoam firmware till date. The new firmware tightly integrates with the hardware for network and crypto acceleration to deliver high performance. The CyberoamOS also extracts the highest level of performance from a multi-core platform, along with offering minimum latency and improved processing speed with use of optimized Interrupt Rates and Fast Path technology. Its Next Generation security features offer protection against newly evolving threats.

FleXi Ports: The FleXi Ports (XP) available in the XP series of appliances offer flexible network connectivity with I/O slot that allows additional Copper/Fiber 1G/10G ports on the same security appliance. To organizations who want to shift to Fiber 1GbE/10GbE connectivity, FleXi Ports give freedom from forced purchase of higher end security appliances to get desired I/O interfaces. FleXi Ports consolidate the number of devices in a network, offering benefits of power efficiency, reduced network complexity and reduced OPEX.

Powerful Hardware: Cyberoam comes with a powerful hardware consisting of Gigahertz processors for nanosecond security processing along with Gigabit Ethernet ports and high port density. A complete overhaul of the appliance design has resulted in an unmatched performance gain with Next Generation memory and more storage capacity.

Superior Quality: The unique design and robust components used in the Cyberoam support high speed I/O throughputs for better performance as well as protect against tough environmental conditions, including power surge and fluctuations.

Next Generation GUI: Cyberoam's state-of-the-art GUI leverages Web 2.0 technology to minimize security errors and simplify navigation. It is aimed at removing the clutter from managing Security appliances. Feature inputs include accordion menus and tabs, easy access top panel, static status bar, unsubscribed modules visibility, direct appliance actions for reboot and shutdown, Web 2.0 pop-ups and the use of TAB and SPACE keys for easy and effective navigation.

Extensible Security Architecture: Cyberoam's extensible security architecture has been designed to grow with the future security needs of an organization without degrading system performance, in order to support newer feature enhancements with minimum effort. This is in sharp contrast to fixed configuration ASIC architecture-based appliances whose capability cannot be upgraded as quickly.

IPv6 Managed Security and Services: Cyberoam further holds up its future-ready claim by securing IPv6 traffic. Cyberoam Security Appliance has been awarded the "IPv6 Ready Gold Logo".

Enhanced Feature Set – More bang for the buck: Cyberoam consists of the full Cyberoam Security Appliance feature set which delivers great value-for-money.

- Firewall delivers effective protection over IPv6 and IPv4 traffic with stateful and deep packet inspection, access control, user authentication, Network and Application layer protection.
- IPS, with its large signature database, as well as support for custom signatures, delivers intelligent protection against DoS attacks, backdoor activity, blended threats and more.
- Web Application Firewall (WAF) secures websites and web-based applications in organizations against Application Layer (Layer 7) attacks like SQL injection, cross-site scripting (XSS), URL parameter tampering, session hijacking, buffer overflows, and more.
- Cyberoam's content filtering controls indiscriminate surfing with a highly comprehensive and rapidly-updated URL categorization database with 90+ categories.
- Application Layer Management controls applications based on user, time and bandwidth to control their availability to users. It also offers benefits of productivity and cost containment by optimizing bandwidth consumed within the organization.
- Cyberoam's Mixed Mode of Deployment provides an ideal solution for an organization's network that already have an existing firewall or router acting as a Gateway and the organization does not want to replace the firewall, but still wishes to take advantage of NGFW security features using Cyberoam. Cyberoam Mixed Mode supports Multi-link Management (MLM), Multiple Bridge Pairs, VPN and HA.
- Multi-link Management and Link Aggregation maximizes connectivity and reliability by managing Internet traffic over multiple ISP links, while supporting failover.
- With Inbound DNS Load Balancing, inbound traffic can be distributed over multiple WAN links to achieve load balancing for the internally hosted servers like mail server, web server. Cyberoam balances incoming load and provides redundancy by allowing the hosted servers to be accessible through multiple links
- Anti Malware offers protection from viruses, worms, spyware and more across the web, Email protocols (HTTP, FTP, SMTP, POP3, IMAP) and IM traffic.
- Anti Spam with signature-less RPD technology, delivers content-agnostic spam protection from both inbound as well as outbound spam. This is on top of a user-based spam digest and Virus Outbreak Detection technology. Sender IP Reputation technology is employed to

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

combat forged mail signatures.

- Support of ICAP to Integrate Third-Party DLP, Web Filtering and AV Applications. Internet Content Adaption Protocol (ICAP) offloads the primary server by redirecting specific Internet based content to dedicated ICAP Servers. Thus, Cyberoam can be deployed in heterogeneous enterprise environments and can hand over HTTP traffic to ICAP Server for malware scanning, content filtering and Data Loss Prevention (DLP) scanning or other processing.
- Cyberoam's VPN offerings allow secure, remote connectivity across IPSec, PPTP and L2TP along with SSL VPN.
- 3G/4G/WiMAX support offers secure high-speed continuous connectivity with failover and load balancing capabilities.

Revamped Cyberoam iView Reporting Tool: Cyberoam has an integrated Cyberoam iView logging and reporting tool to offer visibility into activities within the organization for ensuring security, data confidentiality and regulatory compliance. With 1200+ drilldown reports, its bifurcated dashboard facilitates better presentation of reports with one dashboard displaying all traffic-related information while the other displays security-related reports. Cyberoam has also introduced enhancements in the form of Chart Preferences, Records per Page Control, Inline Charts, Animated Charts and Report Group Dashboard to increase visibility and improve the presentation of the reports. The reports can be exported in PDF, MS Excel and HTML formats.

Data Leakage Prevention: Put together, Cyberoam's Content Filtering, Application Layer Management and control, WAF and Instant Messenger Control features form a powerful data leakage prevention suite against insider threats.

Quick Deployment and Easy Setup: Cyberoam is very simple to operate and readily deployable in any networking environment. While the Quick Start Guide gives step-by-step deployment instructions, the Getting Started manual gives initial configuration guidelines on Cyberoam's Web Admin Console (GUI).

Customer Support and Documentation: Cyberoam appliances offer several levels of paid customer support, as shown in http://www.cyberoam.com/mcontracts.html**.** All of them include Web, Telephone, Email and Chat Support along with firmware upgrades, hardware warranty and RMA fulfillment. They also include access to the knowledge base (kb.cyberoam.com), Customer Support Portal (http://customer.cyberoam.com**)** and the Cyberoam Security Center (www.cyberoamsecuritycenter.com).

The Cyberoam Product Documentation website http://docs.cyberoam.com provides the latest Release Notes, Installation and Product Guides for all Cyberoam products. Also, Cyberoam Knowledge Database, http://kb.cyberoam.com/ contains an exhaustive array of information related to upgrades and troubleshooting guidelines.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam Deployment

If Cyberoam is not already deployed in your network, refer to the Quick Start Guide to get step-by-step deployment help.

Customer Account and Appliance Registration

A Customer Account is required for Appliance registration. If you have not created an account or registered your appliance already, refer to Registration and Subscription Guide, which provides a walk-through of the entire process.

Access Cyberoam GUI Console

Web Admin Console

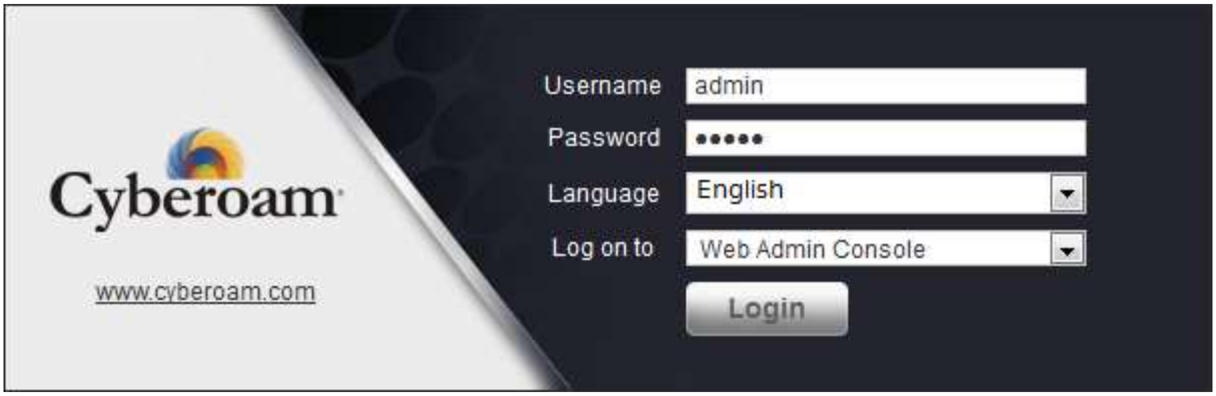
Cyberoam supports Web 2.0 based easy-to-use graphical interface - Web Admin Console, to configure and manage your Cyberoam appliance. While many of the GUI elements display the embedded information tool tip on mouse hover, the Status bar at the bottom of each window displays the status of actions executed in the Web Admin Console.

Cyberoam appliances are shipped with two "Administrator" Users as:

Username	Password	Console Access	Privileges
admin	admin	Web Admin console CLI console	Full privileges for both the consoles or read-write permission for the entire configuration performed through either of the consoles.
cyberoam	cyber	Web Admin console only	Full privileges or read-write permission for the entire configuration performed through Web Admin console

We recommend you to change the password of both the users immediately on deployment.

If you are accessing Cyberoam appliance for the first time after deployment and have not changed the default IP scheme, browse to http://172.16.16.16, or http://<LAN IP address of Cyberoam>, and log on with default credentials. LAN IP Address of Cyberoam is the IP Address configured through the Network Configuration Wizard at the time of deployment.



Username: admin
Password: •••••
Language: English
Log on to: Web Admin Console

Screen - Login

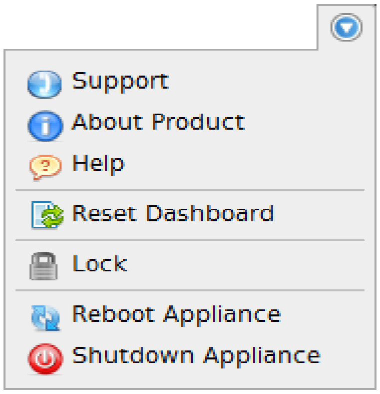
© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

The Dashboard is displayed upon successful authentication to the appliance.

The Dashboard provides a quick and fast overview of all the important parameters of Cyberoam Appliance including the current operating status of the appliance. It groups the information in drag-and-drop doclets, which makes it easy to re-position, navigate and locate the required information.

Dashboard displays automatically upon successful authentication to a Cyberoam Appliance, and can be viewed at any time by pressing F10 key or clicking Dashboard icon in the topmost icon bar. This icon bar on the upper rightmost corner of every page provides access to several commonly used functions like:

- Dashboard – Click to view the Dashboard
- Wizard – Network Configuration Wizard guides you through a step-by-step configuration of the network parameters like IP Address, subnet mask and default gateway for your appliance.
- Reports – Redirects to the Integrated Logging and Reporting solution – Cyberoam iView, which offers a wide spectrum of unique user identity-based reports across applications and protocols, and provides in-depth network visibility to help organizations take corrective and preventive measures.
- Console – It provides immediate access to Command Line Interface (CLI) by initiating a Telnet connection with CLI without closing Web Admin Console.
- Logout Logout – Click to log out from the Web Admin Console.
- More Options – Click to view all the other options available for assistance. On clicking, the following menu is displayed.



The available options are:

- Support is used to open the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
- About Product is used to open the appliance registration information page.
- Help is used to open the context – sensitive help for the page. Each appliance includes a Web-based online help, which can be viewed from any of the page of Web Admin Console. It is deployed automatically with the software.
- Reset Dashboard is used to reset the Dashboard to factory default settings.
- Lock is used to lock the Web Admin Console. Cyberoam automatically locks the Web Admin

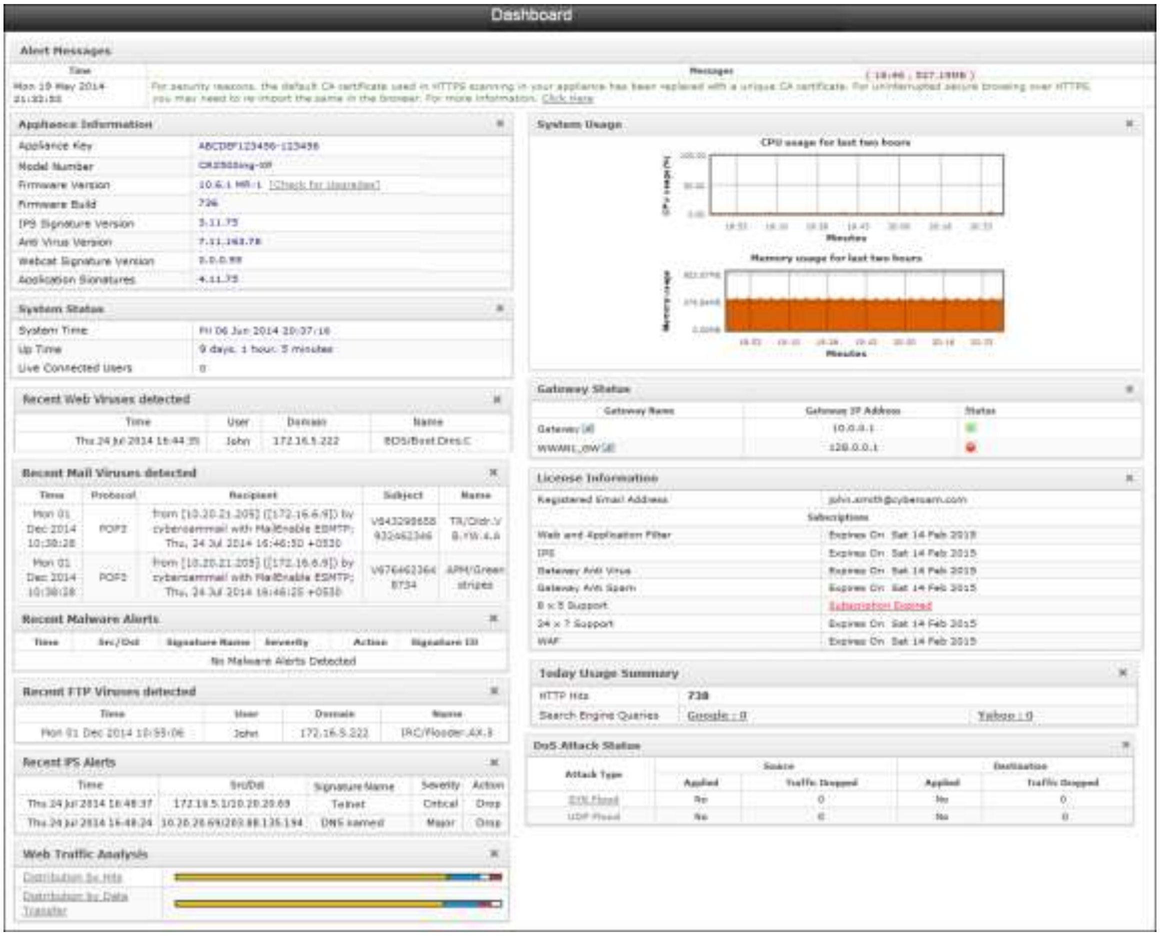
Console if the appliance is in an inactive state for more than 3 minutes. Provide administrator credentials to unlock the Web Admin Console.

- By default, Lock functionality is disabled. Enable Admin Session Lock from **System > Administration > Settings**.
- Reboot Appliance 🔄 is used to reboot the appliance.
- Shutdown Appliance ⏻ is used to shutdown the appliance.

> Note
>
> CLI Console can be accessed via remote login utility – TELNET or SSH client.

Dashboard Tools and Management

Cyberoam Dashboard consists of a number of re-arrange able doclets. Each doclet displays essential information about the appliance such as the Gateway Status, System Status, Recent Viruses Detected, Recent IPS Alerts, Web Traffic Analysis, etc. You can drag and drop the doclets in the desired position on the Dashboard. You can also remove or close the less often used doclets from the dashboard by clicking × icon on the upper right corner on each doclet.



Dashboard

Alert Messages

Time	Messages (18:46 , 527.1986)
Mon 19 May 2014 21:32:55	For security reasons, the default CA certificate used in HTTPS scanning in your appliance has been replaced with a unique CA certificate. For uninterrupted secure browsing over HTTPS, you may need to re-import the same in the browser. For more information, Click Here

Appliance Information

Appliance Key	ABCDEF123456-123456
Model Number	CR2500ing-XP
Firmware Version	10.6.1 MR-1 [Check for Upgrades]
Firmware Build	726
IPS Signature Version	3.11.75
Anti Virus Version	7.11.163.78
Webcat Signature Version	3.0.0.99
Application Signatures	4.11.75

System Status

System Time	Fri 06 Jun 2014 20:37:16
Up Time	9 days, 1 hour, 5 minutes
Live Connected Users	0

Recent Web Viruses detected

Time	User	Domain	Name
Thu 24 Jul 2014 16:44:35	John	172.16.5.222	BDS/Bset.Dns.C

Recent Mail Viruses detected

Time	Protocol	Recipient	Subject	Name
Mon 01 Dec 2014 10:38:28	POP3	from [10.20.21.205] ([172.16.6.9]) by cyberoammail with MailEnable ESMTP; Thu, 24 Jul 2014 16:46:30 +0530	V843298658 932462346	TR/Dldr.V B.YW.4.A
Mon 01 Dec 2014 10:38:28	POP3	from [10.20.21.205] ([172.16.6.9]) by cyberoammail with MailEnable ESMTP; Thu, 24 Jul 2014 16:46:25 +0530	V676462364 8734	APM/Green stripes

Recent Malware Alerts

Time	Src/Dst	Signature Name	Severity	Action	Signature ID
No Malware Alerts Detected					

Recent FTP Viruses detected

Time	User	Domain	Name
Mon 01 Dec 2014 10:55:06	John	172.16.5.222	IRC/Flooder.AX.3

Recent IPS Alerts

Time	Src/Dst	Signature Name	Severity	Action
Thu 24 Jul 2014 16:48:37	172.16.5.1/10.20.20.69	Telnet	Critical	Drop
Thu 24 Jul 2014 16:48:24	10.20.20.69/203.88.135.194	DNS named	Major	Drop

Web Traffic Analysis

Distribution by Hits

Distribution by Data Transfer

System Usage

Gateway Status

Gateway Name	Gateway IP Address	Status
Gateway	10.0.0.1	🟩
WWAN1_GW	128.0.0.1	🔴

License Information

Registered Email Address	john.smith@cyberoam.com
Subscriptions	
Web and Application Filter	Expires On Sat 14 Feb 2015
IPS	Expires On Sat 14 Feb 2015
Gateway Anti Virus	Expires On Sat 14 Feb 2015
Gateway Anti Spam	Expires On Sat 14 Feb 2015
8 x 5 Support	Subscription Expired
24 x 7 Support	Expires On Sat 14 Feb 2015
WAF	Expires On Sat 14 Feb 2015

Today Usage Summary

HTTP Hits	738	
Search Engine Queries	Google : 0	Yahoo : 0

DoS Attack Status

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	No	0	No	0
UDP Flood	No	0	No	0

Screen - Dashboard

Maintenance

Synchronize Licenses

Navigate to **System > Maintenance > Licensing** and click Synchronize to synchronize licenses. This fetches the license details from the Cyberoam Registration Server and updates the Appliance.

Firmware Upgrades

Navigate to **System > Maintenance > Firmware** to install latest firmware. Refer Upgrade Firmware of Cyberoam Appliance for instructions to download and use latest firmware.

Updates

Navigate to **System > Maintenance > Updates** to update the Antivirus Definition, IPS Signatures and Application Signatures.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam Configuration

Network

Zones

Zones are logical grouping of Interfaces, each with its own set of usage rules, services and policies that includes:

- Predefined zones - LAN, WAN, DMZ, LOCAL, VPN
- Custom zones

LOCAL zone is the grouping of the entire set of physical ports on the Cyberoam Appliance, including their configured aliases. In other words, IP Addresses assigned to all the ports fall under the LOCAL zone.

To create an additional LAN, DMZ and VPN zone types, refer Cyberoam User Guide.

Interfaces

The appliance is shipped with a number of physical interfaces/ports and number of interfaces depends on the appliance model. The physical interfaces can be configured as:

- Alias – Alias allows binding multiple IP Addresses onto a single physical interface. It is another name for the interface that will easily distinguish this interface from another interface.
- Bridge Pair – Bridge pair enables to configure transparent subnet gatewaying.
- LAG – Link Aggregation Group (LAG) is a method by which multiple network connections can be combined into a single connection. It is also known as trunking, NIC teaming, NIC bonding and Ether Channel. LAG is mostly used for handling LAN traffic.
- VLAN – Virtual LAN is a broadcast domain configured on switch on a port-by-port basis.
- WLAN – Wireless Local Area Network (WLAN) is used to associate devices through wireless distribution method and connection to the Internet is provided through an access point.
- WWAN – Wireless WAN is wide area network (WAN) for data that is typically provided by the cellular carriers to transmit a wireless signal over a range of several miles to a mobile device.

To configure interface alias, bridge pair, LAG, VLAN, WLAN or WWAN navigate to **Network > Interfaces/Wireless LAN / Wireless WAN. Refer** Cyberoam User Guide for detailed configuration steps.

Publish Web and Mail Servers

To configure Cyberoam for providing access to internal resources such as mail and web server hosted in LAN/DMZ, you need to create:

- Virtual Host from (**Firewall > Virtual Host > Add**)
- WAN to LAN Firewall Rule for the respective Virtual Host to allow the inbound traffic (when servers are hosted in LAN)
- WAN to DMZ Firewall Rule for respective Virtual Host to allow the inbound traffic (when servers are hosted in DMZ)

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

You may refer the article Publish Internal Server over Internet for step-by-step configuration to publish internal web/mail/other servers over LAN. For other similar articles, please refer http://kb.cyberoam.com.

Users

Users are identified by an IP Address or a user name and assigned to a user group. All the users in a group inherit the policies defined for that group.

User Registration

Cyberoam appliance supports five types of Users:

- Normal
- Clientless
- Single Sign on
- Thin Client User
- WWAN User

To register or create users, refer Cyberoam User Guide for detailed configuration steps.

Import Users through CSV file or AD

User can be imported to Cyberoam through a CSV file containing user records. For CSV file particulars, refer Import Users from CSV file. Active Directory users/groups/OUs can be imported after integrating Cyberoam with the Active Directory. Importing user groups or OUs can be conveniently done through the Import Group Wizard, refer Import Active Directory OUs and Groups.

User Authentication

When the user attempts to access the Internet, the appliance requests a user name and password and authenticates the user's credentials before giving access. User authentication can be performed using the Cyberoam local database or the external authentication servers after integration.

Cyberoam can be integrated with AD, LDAP/S or Radius server for authentication. To configure the external authentication servers, navigate to **Identity > Authentication > Authentication Server**.

Objects

Objects are logical entities which are integrated with firewall rules or policies. Objects can be:

- Hosts – IP Host, MAC Host, FQDN Host, Country Host.
- Services- Represents specific protocol and port combination.
- Schedule- Used to define time/duration for rules or policies.
- File Types- Grouping of particular file extension or MIME headers.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Basic Security

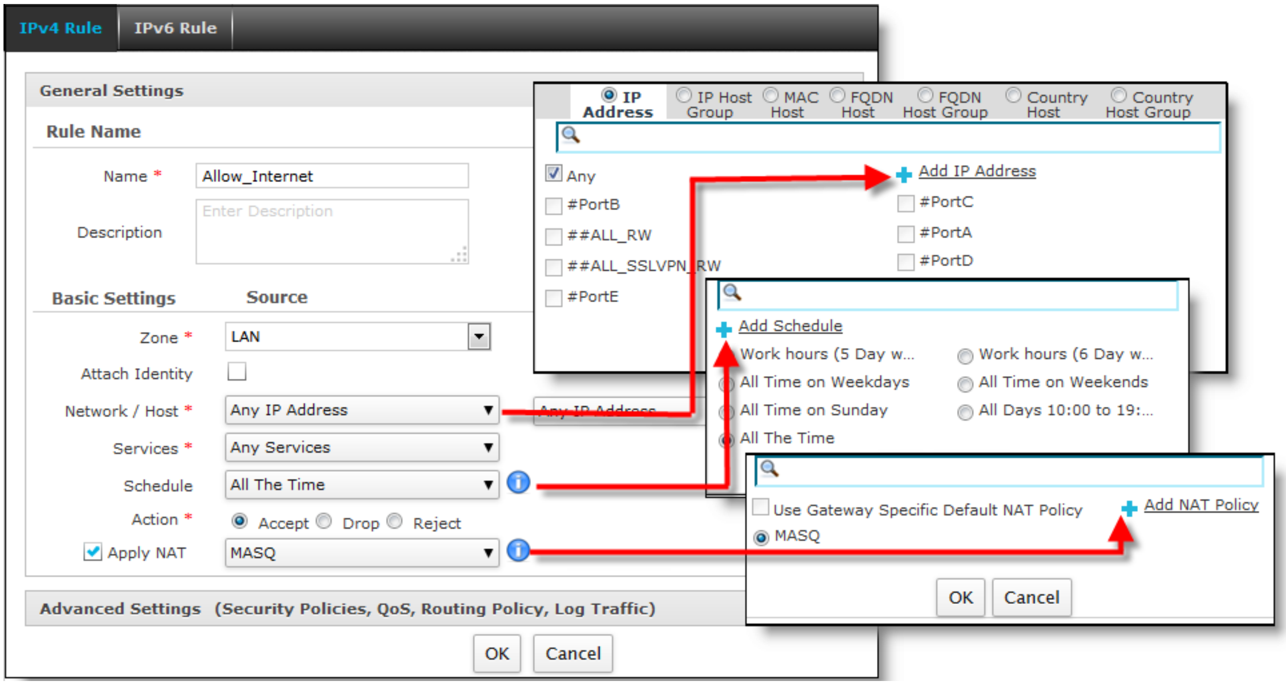
Firewall Rules

Firewall Rule is a centralized network management tool that allows defining inbound and outbound access policy and configuring the entire set of security policies of the Cyberoam security appliance.

The Firewall Rule page is a sortable rule management interface, designed to make rule management a simpler and more intuitive process. The rule components referenced by the firewall can be configured from the Firewall Rule page itself, and thus, eliminating the need to navigate from page-to-page to create the rule components from this single page itself:

Following rule components can be configured using the Firewall Rule page:

- Entire set of Cyberoam security policies – Virus and Spam scanning, IPS, Web filter policy, Application filter policy, Web Application Firewall policy, IM control policy, QoS policy and routing policy.
- All the Objects – IP Address, MAC Address, Virtual Host, FQDN and Country hosts, services, schedule


IPv4 Rule
IPv6 Rule
General Settings
Rule Name
Basic Settings
Source
Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)
OK
Cancel

Name * Allow_Internet

Description Enter Description

Zone * LAN

Attach Identity □

Network / Host * Any IP Address

Services * Any Services

Schedule All The Time

Action * ● Accept ○ Drop ○ Reject

☑ Apply NAT MASQ

● IP Address ○ IP Host Group ○ MAC Host ○ FQDN Host ○ FQDN Host Group ○ Country Host ○ Country Host Group

☑ Any
□ #PortB
□ ##ALL_RW
□ ##ALL_SSLVPN_RW
□ #PortE

Add IP Address
□ #PortC
□ #PortA
□ #PortD

Add Schedule
○ Work hours (5 Day w...
○ All Time on Weekdays
○ All Time on Sunday
● All The Time
○ Work hours (6 Day w...
○ All Time on Weekends
○ All Days 10:00 to 19:...

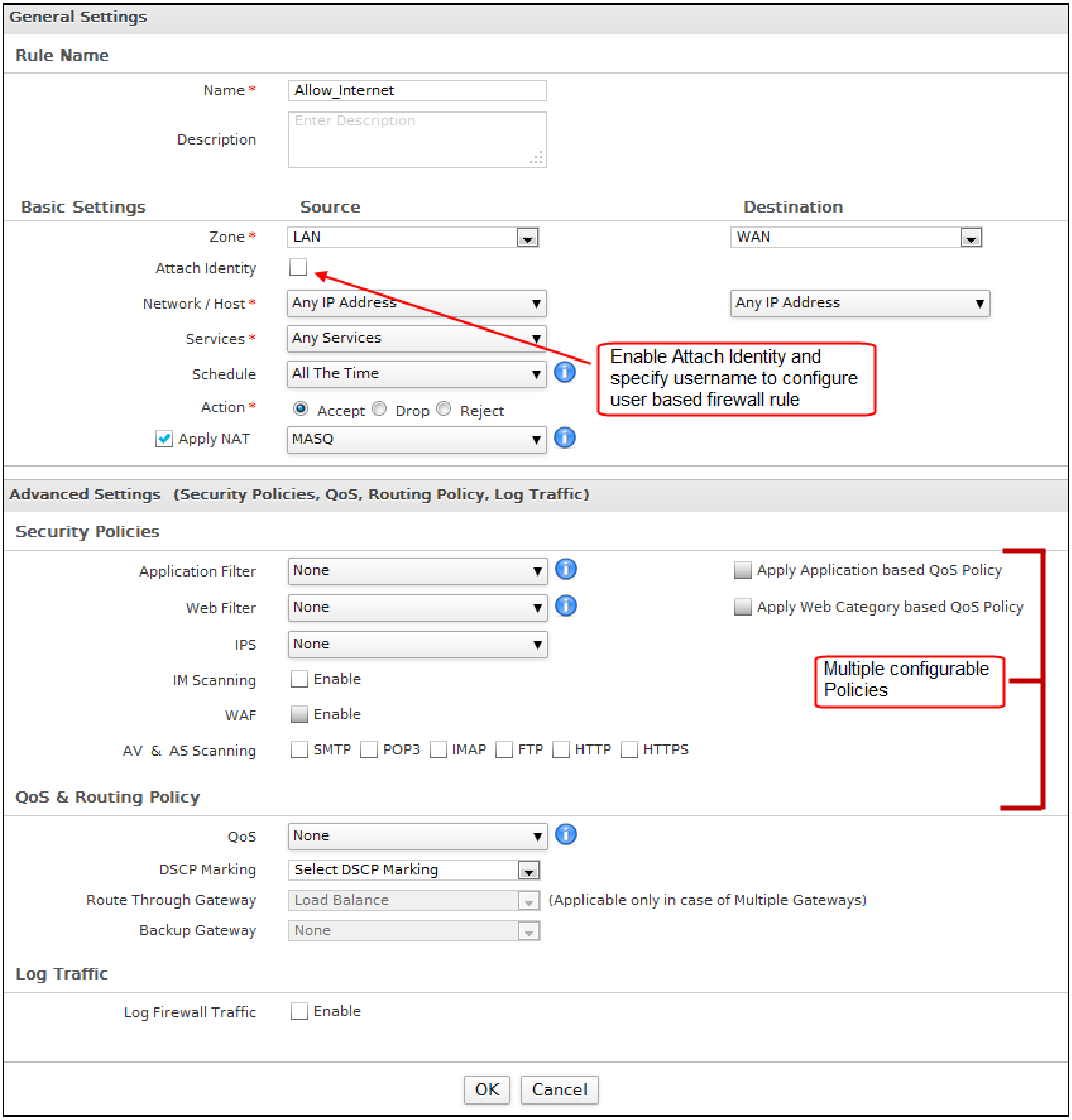
□ Use Gateway Specific Default NAT Policy
Add NAT Policy
● MASQ
OK Cancel

Screen – Firewall Rule

By default, Cyberoam allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN.

To manage firewall rule, go to **Firewall > Rule > IPv4 Rule**.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.



General Settings

Rule Name

Name * Allow_Internet

Description Enter Description

Basic Settings	Source	Destination
Zone *	LAN	WAN
Attach Identity	□	
Network / Host *	Any IP Address	Any IP Address
Services *	Any Services	
Schedule	All The Time	
Action *	● Accept ○ Drop ○ Reject	
☑ Apply NAT	MASQ	

Enable Attach Identity and specify username to configure user based firewall rule

Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)

Security Policies

Application Filter	None	□ Apply Application based QoS Policy
Web Filter	None	□ Apply Web Category based QoS Policy
IPS	None	
IM Scanning	□ Enable	
WAF	□ Enable	
AV & AS Scanning	□ SMTP □ POP3 □ IMAP □ FTP □ HTTP □ HTTPS	

Multiple configurable Policies

QoS & Routing Policy

QoS	None
DSCP Marking	Select DSCP Marking
Route Through Gateway	Load Balance (Applicable only in case of Multiple Gateways)
Backup Gateway	None

Log Traffic

Log Firewall Traffic □ Enable

Screen – Firewall Rule

Web Filtering

Use Web filtering to limit the access to the contents available to the user based on a combination of categories, keywords, URLs, domain names and file types. Cyberoam filters web traffic based on categories and policies. Fine-tune the default policies for controlling access as per your requirement.

You may refer the article Configure Web Filter Policy to create a Web Filter Policy such that it denies access to all the websites falling under “Games” web category. For other similar articles, please refer

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

http://kb.cyberoam.com.

Application Filter

Application Filter Policy controls access to applications and specifies which user can access which applications and/or when. Fine-tune the default policy for controlling access as per your requirement.

Scenario: Create Application Filter Policy DenyProxy to Block Proxies

Create a custom policy named "DenyProxy" from **Application Filter > Policy > Policy > Add** based on the template "Allow All".

Update "DenyProxy" policy to add a rule:

- Category - "Proxy"
- Application – Freegate, Ultrasurf
- Action – "Deny"
- Schedule – "Work hours (5 Day week)"

When the above policy is applied to a firewall rule, all the users will be denied access to "Freegate" and "Ultrasurf" during the working hours.

Scenario: Allow 'FacebookVideoChat' for specific user-group only (while explicitly blocking it for others).

Step 1: Create a custom policy "Block_FacebookVideoChat" from **Application Filter > Policy > Policy > Add** based on the template "Deny All".

Update policy add a rule to deny Facebook chat:

- Category – Social Networking
- Application – Facebook Video Chat
- Action – Deny
- Schedule – All the Time

Step 2: Apply the Application filter policy created in Step 1 in the required firewall rule.

With the above policy applied through firewall rule, all the users will be denied access to Facebook Video chat application.

Step 3: Create another custom policy ''Allow_FacebookVideoChat'' based on the template ''Allow All'' to allow access to specific user-group only.

- Category – Social Networking
- Application – Facebook Video Chat
- Action – Allow
- Schedule – All the Time

Update policy add a rule to allow Facebook video chat:

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

- Category – Social Networking
- Application – Facebook Video Chat
- Action – Allow
- Schedule – All the Time

Step 4: Apply the Application filter policy created in Step 3 to the specific user group from **Identity > Groups > Groups**.

With this policy applied on the group, only specific group will be able to access Facebook Video chat application while all other users will be denied access

Scenario: Block P2P applications for a user – John Pitt

Step 1: Create a custom policy “BlockP2P” from **Application Filter > Policy > Policy > Add** based on the template “Allow All”. Update policy to add a rule with the following parameters:

- Category - P2P
- Applications – Select All
- Action - Deny
- Schedule – All the Time

Step 2: Go to **Identity > Users > Users**, edit the details of user – John Pitt and attach Application Filter Policy created in step 1.

Step 3: Create Identity-based Firewall Rule from **Firewall > Rule > Add**

- Source: LAN, Any Host
- Click “Check Identity” to enable Identity-based Firewall rule and select the user “John Pitt“
- Destination: WAN, Any Host
- Service: All Services

With the above configuration, User – John Pitt will not be able to access any of the P2P Applications included in the category during the time specified in the schedule.

WAF Protection

Web Application Firewall Module enables protection of your Web Servers from Application Layer (Layer 7) attacks such as SQL injection, cross-site scripting (XSS), URL parameter tampering.

Scenario: Protect Domain www.test.com publicly hosted on Web Server 202.134.168.208

Configure Web Server in Cyberoam from **WAF > Web Servers > Web Server > Add** according to following parameters:

Zone: DMZ

Web Server Hosted On: Public IP/FQDN

Public IP/FQDN: 202.134.168.208

Domains to Protect: Specific Domains Hosted (www.test.com)

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

IPS settings and Policies

To reduce the chances of excessive false positives and the number of alerts, Cyberoam IPS Policy Tuner allows creation of perfect-fit IPS scanning policy. The administrator can fine-tune the default policies or create custom policies to reduce the false positives.

The appliance provides following pre-defined policies. You can directly use policies 1 to 6 without any modifications while policies 7 to 10 can either be used directly or, can be modified as per your requirements:

1. DMZ TO LAN
2. DMZ TO WAN
3. LAN TO DMZ
4. LAN TO WAN
5. WAN TO DMZ
6. WAN TO LAN
7. generalpolicy
8. lantowan strict policy
9. lantowan general policy
10. dmzpolicy

Create Identity-based IPS Policy

In order to provide a high level of granularity, Cyberoam allows implementing IPS scanning for individual user also. This additionally reduces the network load as the traffic for the rest of the users will not be scanned.

To configure Identity-based IPS Policy:

Step 1: Define IPS policy from **IPS > Policy** and click **Add**.

Step 2: Configure Firewall Rule for the user and attach IPS Policy created in step 1.

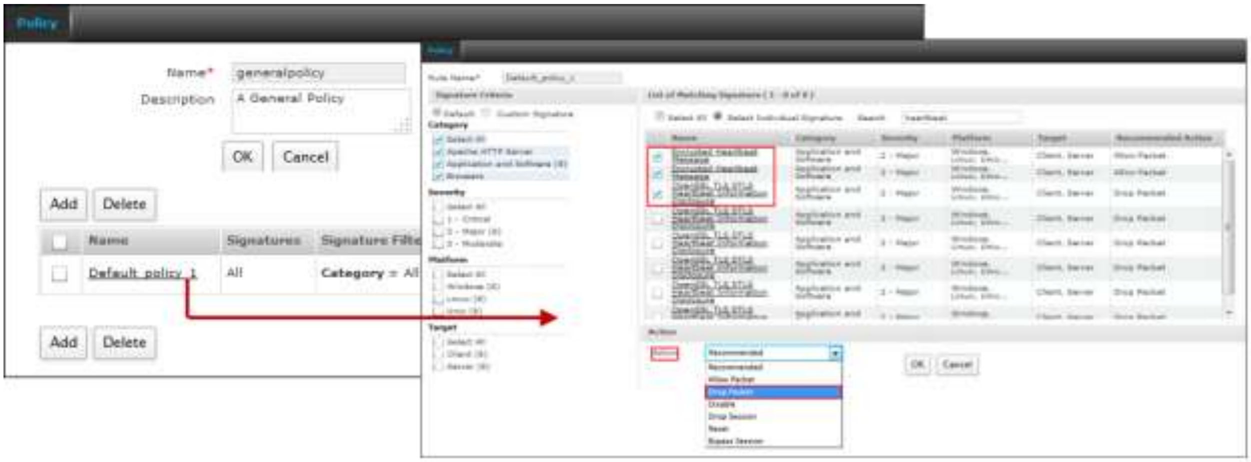
Signature-based Protocol Anomaly Detection

Step 1: Go to **IPS > Policy > Policy** and update/modify the default “generalpolicy” policy.

Step 2: Click “Default_Policy_1” category to view signatures included in this category.

Step 3: Select “Allow Packet”, “Drop Packet”, “Drop Session”, “Reset”, “Bypass Session” as required for the appropriate signatures.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.



Name* generalpolicy

Description A General Policy

	Name	Signatures	Signature Filte
□	Default_policy_1	All	Category = All

Screen – Modify ‘generalpolicy’

VPN – Secure Remote Connectivity

Cyberoam can be used to establish VPN connection and supports following protocols to authenticate and encrypt traffic:

- Internet Protocol Security (IPsec)
- Layer Two Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Layer (SSL)

Configure Site-to-Site IPSec VPN connection between Head Office and Branch Office

To make VPN connection configuration task easier, Cyberoam provides six preconfigured VPN policies for the frequently used VPN deployment scenarios:

- DefaultL2TP
- DefaultHeadOffice
- DefaultBranchOffice
- AES128_MD5
- Default Policy

The administrator can directly use “DefaultHeadOffice“ or “DefaultBranchOffice” default policies for the most common scenario to establish site-to-site connection using preshared key to authenticate peers.

You may refer the article Establish Site-to-Site IPSec Connection using Preshared key for step-by-step configuration to configure site-to-site IPSec connection. For other similar articles, please refer http://kb.cyberoam.com.

Configure remote access VPN on Cyberoam

This is commonly called a "road warrior" configuration, because the client is typically a laptop, PDA, Mobile Phone or Tablet being used from remote locations, and connected over the Internet using service providers and dialup connections. Cyberoam provides clients for Windows, Linux, Macintosh platforms as well as inbuilt clients. The most common use of this scenario is when you are at home or on the road and

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

want access to the corporate network.

You may refer the article Setup Cyberoam VPN Client to connect to a Cyberoam for the remote access using preshared key for step-by-step configuration of Remote VPN connection. For other similar articles, please refer http://kb.cyberoam.com.

If you are using Cyberoam IPSec VPN Client for the first time, download Client from http://www.cyberoam.com/vpnhelp.html.

Configure VPN failover

You will need to configure VPN failover condition to keep your VPN connection always ON. Cyberoam allows you to configure failover conditions at the time of creating IPSec connection. Alternately, configure connection failover as follows:

- Create Connection Group from VPN **>** IPSec **>** Failover Group **and click Add**. Failover Group is the grouping of all the connections that are to be used for failover. The order of connections in the Group defines fail over priority of the connection.
- Define Failover condition in the Group.

Your primary VPN connection will failover to the next active Connection in the Group if Connection Group is created including the primary connection. For example, if the connection established using 4th Connection in the Group is lost then 5th Connection will take over provided the 5th Connection is active.

Configure SSL VPN

SSL (Secure Socket Layer) VPN allows access to the organization network from anywhere, anytime and provides the ability to create point-to-point encrypted tunnels between remote employees and company's internal network, requiring a combination of SSL certificates and a username/password for authentication to enable access to the internal resources.

For details on how to configure SSL VPN, refer to SSL VPN User Guide.

QoS and Bandwidth Management

Bandwidth prioritization and control depends on efficient QoS. The primary objective of QoS (Quality of Service) policy is to manage and distribute the total bandwidth on certain parameters and user attributes. QoS policy allocates & limits the maximum bandwidth usage of the user and controls the web and network traffic. Additionally, with the rapid increase in the number of deployed enterprise application, application traffic takes a particular toll on bandwidth. The idea is to streamline bandwidth usage and give priority to business critical traffic and throttle unproductive traffic.

Navigate to **QoS > Policy** to define QoS filters and settings. Cyberoam QoS policy can be defined based on the following parameters:

Define for whom you want to create policy – User/Firewall Rule/Web Category/Application

Define Type of policy - Strict/Committed

Define the Implementation strategy of the policy - Total/Individual Upload and Download

Define Bandwidth Usage – Individual/Shared

You may refer the article Bandwidth Shaping using QoS Policies for step-by-step configuration of QoS.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

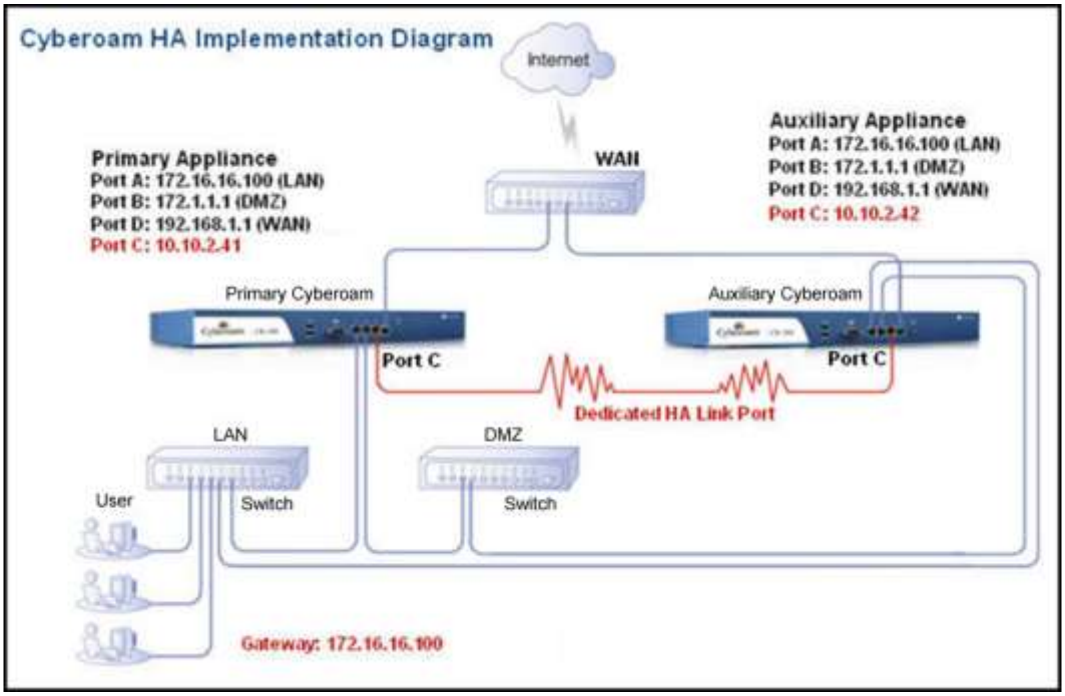
For other similar articles, please refer http://kb.cyberoam.com.

High Availability

Hardware failure such as a failure of the power supply, hard disk, or processor is the main reason behind the failure of Internet security system and/or a Firewall. To provide a reliable and continuous connection to the Internet and security services such as Firewall, VPN, Intrusion Detection and Prevention, Virus Scanning, Web Filtering, and Spam Filtering services, two appliances can be configured to function as a single appliance and provide High Availability.

Clustering Technology is used to ensure the High Availability. In a cluster, two appliances are grouped together and instructed to work as a single entity.

To configure HA between Cyberoam Primary and Auxiliary appliances, navigate to the **System > HA**.



Refer Cyberoam High Availability Configuration Guide for detailed steps and explanation.

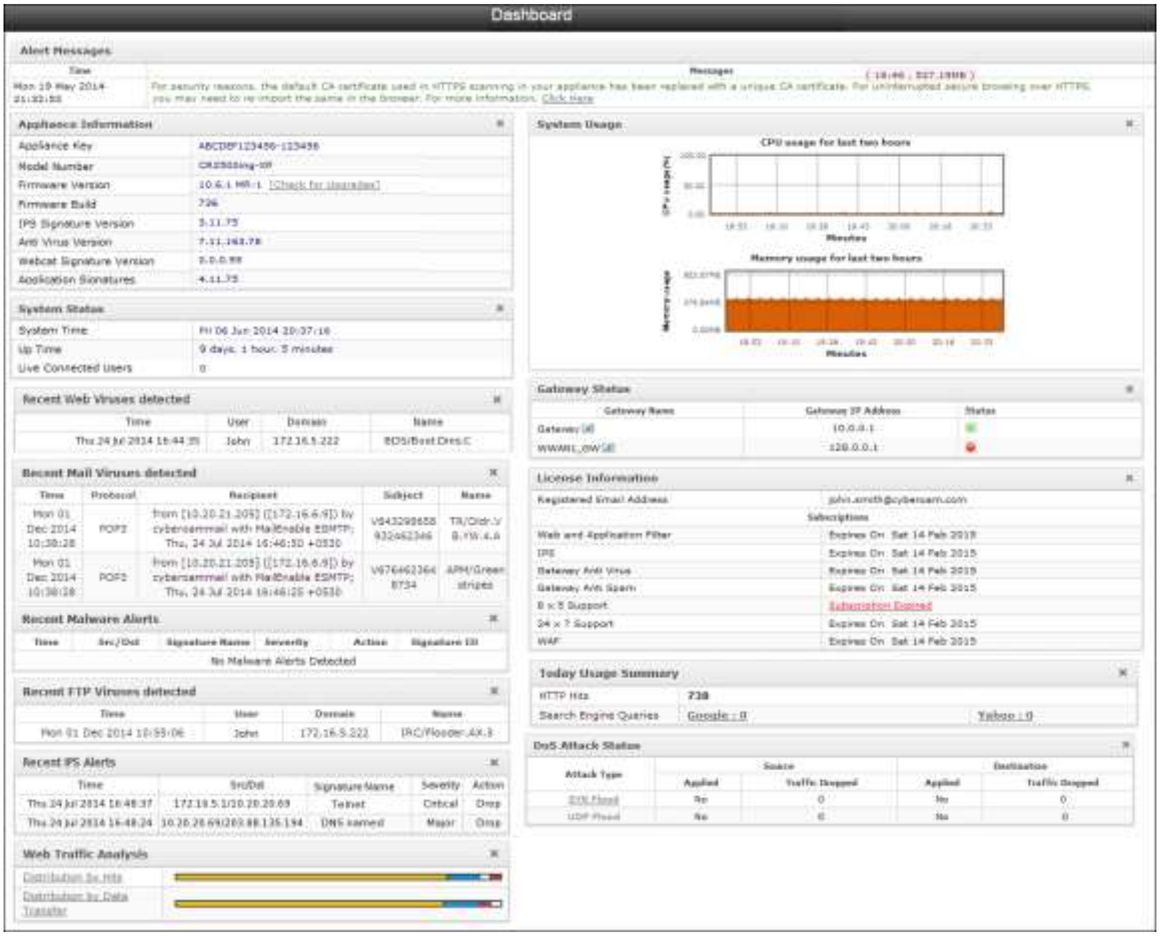
© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam Administration: Monitoring and Optimization

Monitoring

Dashboard

Dashboard serves the purpose of a ready-reference providing instant visibility into network resource usability as well as alerts providing attack vs. user information without in-depth search.


Dashboard

Alert Messages

Time	Messages (18:46 , 527.19MB)
Mon 19 May 2014 21:32:58	For security reasons, the default CA certificate used in HTTPS scanning in your appliance has been replaced with a unique CA certificate. For uninterrupted secure browsing over HTTPS, you may need to re-import the same in the browser. For more information, Click Here

Appliance Information

Appliance Key	ABCDEF123456-123456
Model Number	CR2500ing-XP
Firmware Version	10.6.1 MR-1 [Check for Upgrades]
Firmware Build	726
IPS Signature Version	3.11.75
Anti Virus Version	7.11.162.78
Webcat Signature Version	2.0.0.88
Application Signatures	4.11.75

System Status

System Time	Fri 06 Jun 2014 20:37:16
Up Time	9 days, 1 hour, 5 minutes
Live Connected Users	0

Recent Web Viruses detected

Time	User	Domain	Name
Thu 24 Jul 2014 16:44:35	John	172.16.5.222	BDS/Bset.Dms.C

Recent Mail Viruses detected

Time	Protocol	Recipient	Subject	Name
Mon 01 Dec 2014 10:38:28	POP3	from [10.20.21.205] ([172.16.6.9]) by cyberoammail with MailEnable ESMTP; Thu, 24 Jul 2014 16:46:50 +0530	V643298658 932462346	TR/Dldr.V B.YW.4.A
Mon 01 Dec 2014 10:38:28	POP3	from [10.20.21.205] ([172.16.6.9]) by cyberoammail with MailEnable ESMTP; Thu, 24 Jul 2014 16:46:25 +0530	V676462364 8734	APM/Green stripes

Recent Malware Alerts

Time	Src/Dst	Signature Name	Severity	Action	Signature ID
No Malware Alerts Detected					

Recent FTP Viruses detected

Time	User	Domain	Name
Mon 01 Dec 2014 10:55:06	John	172.16.5.222	IRC/Flooder.AX.3

Recent IPS Alerts

Time	Src/Dst	Signature Name	Severity	Action
Thu 24 Jul 2014 16:48:37	172.19.5.1/10.20.20.69	Telnet	Critical	Drop
Thu 24 Jul 2014 16:48:24	10.20.20.69/203.88.135.194	DNS named	Major	Drop

Web Traffic Analysis

Distribution by Hits

Distribution by Data Transfer

System Usage

Gateway Status

Gateway Name	Gateway IP Address	Status
Gateway	10.0.0.1	🟩
WWAN1_GW	128.0.0.1	🟥

License Information

Registered Email Address	john.smith@cyberoam.com
Subscriptions	
Web and Application Filter	Expires On: Sat 14 Feb 2015
IPS	Expires On: Sat 14 Feb 2015
Gateway Anti Virus	Expires On: Sat 14 Feb 2015
Gateway Anti Spam	Expires On: Sat 14 Feb 2015
8 x 5 Support	Subscription Expired
24 x 7 Support	Expires On: Sat 14 Feb 2015
WAF	Expires On: Sat 14 Feb 2015

Today Usage Summary

HTTP Hits	738	
Search Engine Queries	Google : 0	Yahoo : 0

DoS Attack Status

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	No	0	No	0
UDP Flood	No	0	No	0

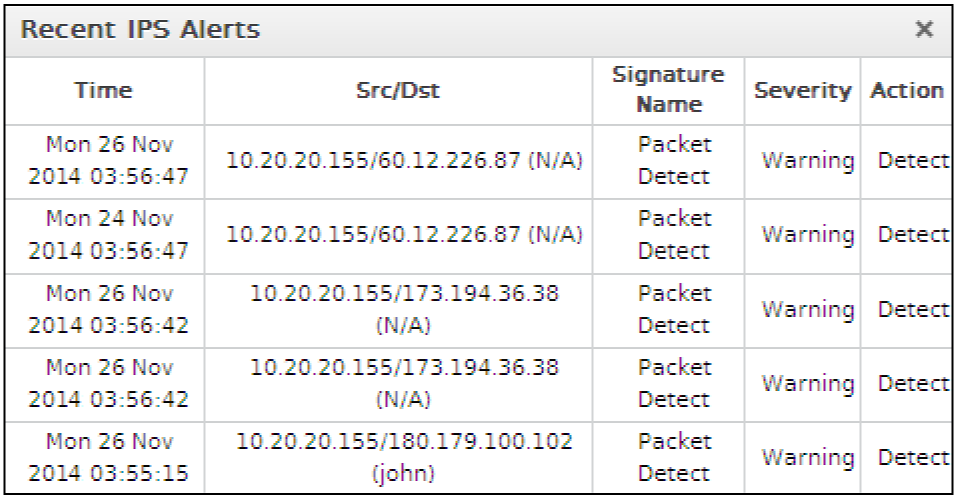
Screen - Dashboard

Drag-and-Drop Dashboard doclets can be minimized or repositioned to appropriately place doclets that require special attention for managing Cyberoam. Press F10 key to view the Dashboard from any of the pages.

User specific threats detection through dedicated Doclets

Dashboard - “Recent IPS Alerts” doclet – User-based IPS Alerts

The administrator can get the information of threat origin even in DHCP environment as username is included in the IPS alerts. In DHCP environment, where IP Address is assigned dynamically, without username it is practically impossible to track the threat origin.

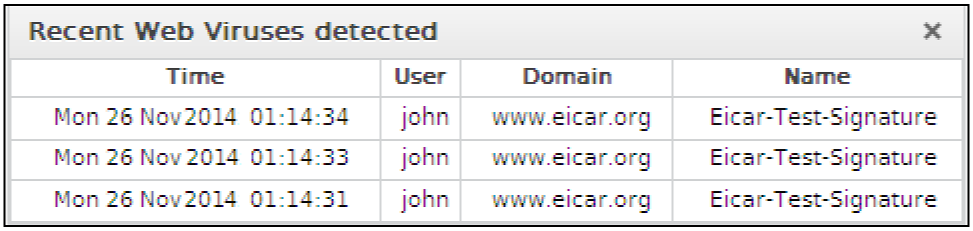


Recent IPS Alerts

Time	Src/Dst	Signature Name	Severity	Action
Mon 26 Nov 2014 03:56:47	10.20.20.155/60.12.226.87 (N/A)	Packet Detect	Warning	Detect
Mon 24 Nov 2014 03:56:47	10.20.20.155/60.12.226.87 (N/A)	Packet Detect	Warning	Detect
Mon 26 Nov 2014 03:56:42	10.20.20.155/173.194.36.38 (N/A)	Packet Detect	Warning	Detect
Mon 26 Nov 2014 03:56:42	10.20.20.155/173.194.36.38 (N/A)	Packet Detect	Warning	Detect
Mon 26 Nov 2014 03:55:15	10.20.20.155/180.179.100.102 (john)	Packet Detect	Warning	Detect

Screen – Recent IPS Alerts Doclet

Dashboard - "Recent Web Viruses detected" doclet – User-wise Web Virus detection Alert

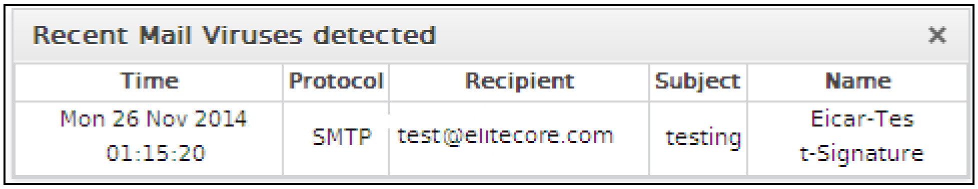


Recent Web Viruses detected

Time	User	Domain	Name
Mon 26 Nov2014 01:14:34	john	www.eicar.org	Eicar-Test-Signature
Mon 26 Nov 2014 01:14:33	john	www.eicar.org	Eicar-Test-Signature
Mon 26 Nov2014 01:14:31	john	www.eicar.org	Eicar-Test-Signature

Screen – Recent Web Viruses Detected Doclet

Dashboard - "Recent Mail Viruses detected" doclet – User-wise Mail Virus detection Alert



Recent Mail Viruses detected

Time	Protocol	Recipient	Subject	Name
Mon 26 Nov 2014 01:15:20	SMTP	test@elitecore.com	testing	Eicar-Tes t-Signature

Screen – Recent Mail Viruses Detected Doclet

Reporting

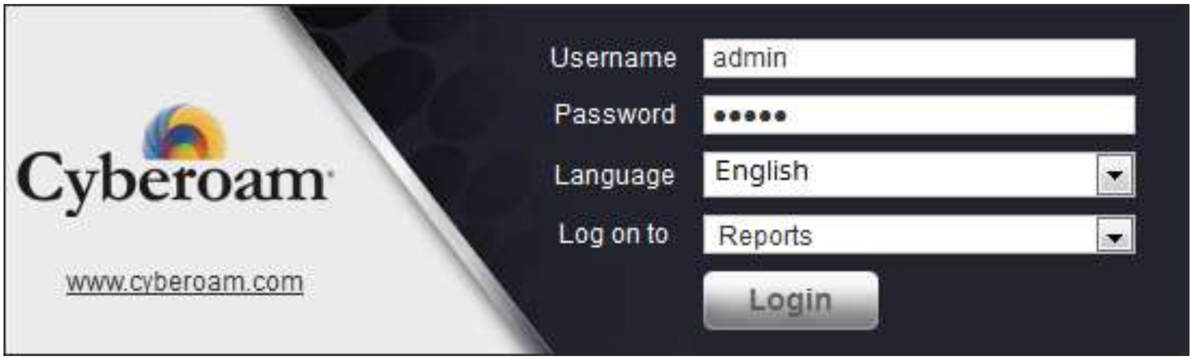
Access On-Appliance Reports

You can access On-Appliance reports in 3 ways:

Go to **Logs and Reports → View Reports** from Web Admin Console.

Click the Report icon on the upper right hand corner of the screen.

Directly login to Cyberoam iView – On-Appliance Reports from Cyberoam Login Screen. On the Login Screen, provide Administrator credentials and select “Reports” under Log on to.



Username: admin
Password: •••••
Language: English
Log on to: Reports

Screen – Login to On-Appliance Reports

Analytical Reports for Better Optimization

Analytical reports provide details on each and every activity of your network including senders and recipients of virus and spam mails, attackers and victims of IPS attacks.

Additionally, extensive reports that can help to analyze all the User activities like sites surfed, amount of data transferred and surfing time, carried out by user, group and so on are also provided to take the corrective actions by tuning the policies based on the user behavior.

Want to know	Where to find	What Next*
Total number of Web viruses received by the user ‘Abraham’	**Dashboard > Custom Dashboard** Username Criteria – Abraham > Top Web Viruses widget	Verify Antivirus configuration from **Antivirus > HTTP/S**
IPS Attack victims	**Reports > Attacks >Top Victims** Drill down for attack category, platform or Severity-wise Break-down.	Based on the severity of the attack, ‘’Drop’’ traffic for applications with severe risks from **Application Filter > Policy**
BYOD client types	**Internet Usage > Top Client Type** Drill down for Top Groups, Top Users and Data-wise Reports.	Inspect user’s internet usage requirements and apply QoS policy based on ‘’User’’ and ‘’Schedule’’ from **QoS > Policy**
Users who access Social Networking Web Category most frequently	**Search > Web Surfing Reports** Report Type: Summary Search Type: Category Category Name: SocialNetworking	Block the Web Category for the users/group from Web Filter > Policy and apply the policy in firewall rule. Alternatively, apply Access Time /Surfing Quota/Data Transfer policy for the user/group from **Identity > Policy**

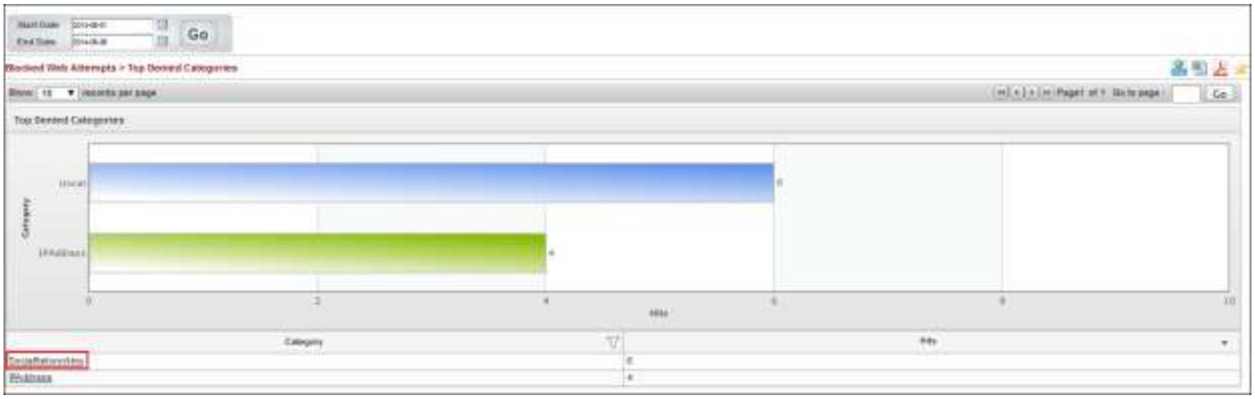
© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Top 10 Categories accessed across enterprise	**Reports > Web Usage > Top Categories** Drill down from Category name to view the list of domains, contents and users.	Apply QoS based on ''Application'' and set ''Priority'' for the applications from **QoS > Policy**
File downloaded over FTP by user John	**Dashboard > Custom Dashboard** Source Host Criteria: Username →**Top Files Downloaded via FTP**	Inspect FTP domain and block if found un-secured, from **Web Filter > Policy**
Which are the high risk application used in my network	**Reports > Application > Top Risks and drill down for Top Applications**	Inspect severity of the application and block the application from **Application Filter > Policy**
User consuming maximum bandwidth	**Reports > Top Web Users**	Apply QoS based on ''User'' and set "Priority" from **QoS > Policy**
Which Administrator accessed Cyberoam or updated configuration	**Reports > Events > Admin Events**	Identify Successful and Failed login attempt details. You can also enable role-based administration by creating different profiles for administrators from **System > Administration > Profile**

***The ''’What Next'' section provides most probable optimization steps which can be implemented on your Cyberoam. Similar optimization can be carried out based on the requirement and policies of the Enterprise.**

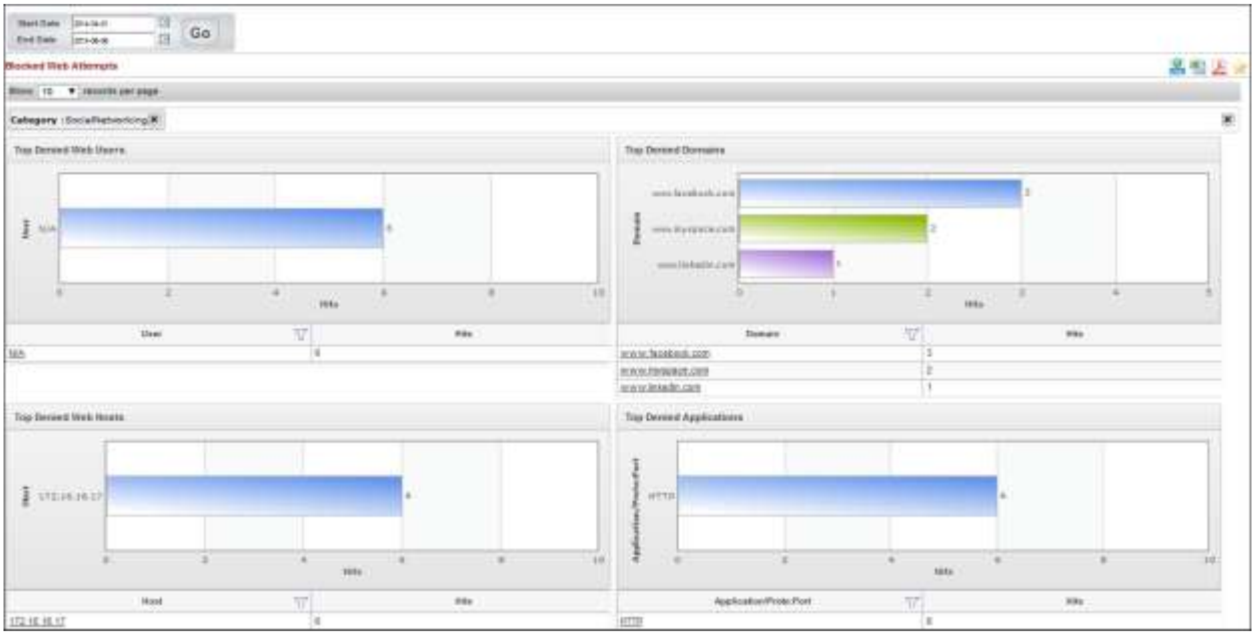
Sample Blocked Categories report

View report from **Reports > Blocked Web Attempts > Top Denied Categories** and drill down by denied categories to view user based reports



Screen – Blocked Categories Reports

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.



Start Date 2014-04-01

End Date 2014-06-06

Blocked Web Attempts

Show 10 records per page

Category : SocialNetworking

Top Denied Web Users

User	Hits
N/A	6

Top Denied Domains

Domain	Hits
www.facebook.com	3
www.myspace.com	2
www.linkedin.com	1

Top Denied Web Hosts

Host	Hits
172.16.16.17	6

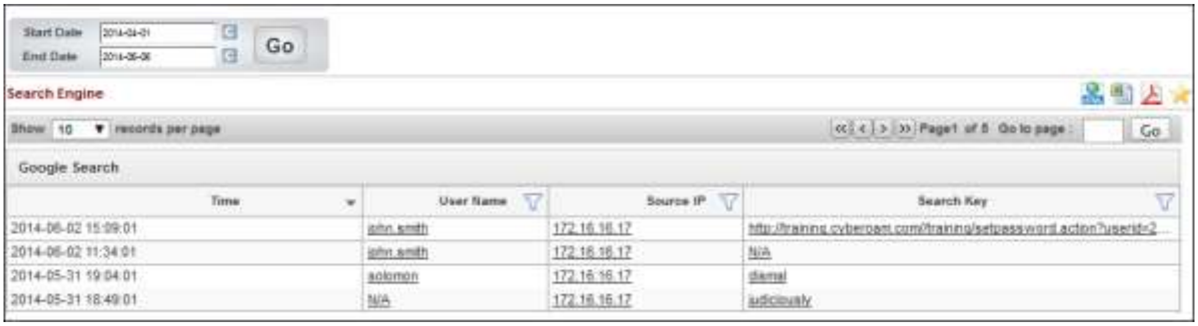
Top Denied Applications

Application/Proto:Port	Hits
HTTP	6

Screen – Blocked Categories Reports - Drilldown

Search Engine Report

Search Engine Report displays the keywords searched by using search engines including Google, Yahoo, Bing, Rediff and eBay Search. It displays username, date, time and search-keyword. View search engine reports from **Reports > Search Engine**.



Start Date 2014-04-01

End Date 2014-06-06

Search Engine

Show 10 records per page

Page1 of 5 Go to page :

Google Search

Time	User Name	Source IP	Search Key
2014-06-02 15:09:01	john.smith	172.16.16.17	http://training.cyberoam.com/training/setpassword.action?userid=2...
2014-06-02 11:34:01	john.smith	172.16.16.17	N/A
2014-05-31 19:04:01	solomon	172.16.16.17	dismal
2014-05-31 18:49:01	N/A	172.16.16.17	judiciously

Screen – Search Engine Report

Compliance reports

Many businesses and organizations require protection of their critical applications as well as customer data. For this, they need to meet regulatory requirements such as HIPAA, GLBA, SOX, FISMA and PCI. Cyberoam provides 45+ compliance reports and can be accessed from **Compliance Reports**.

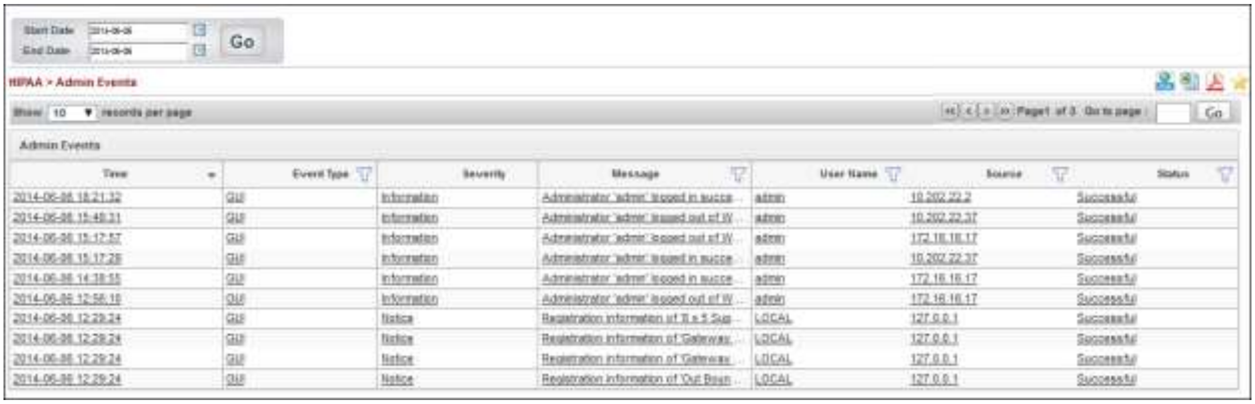
- **HIPAA** - Health Insurance Portability & Accountability Act for Health care Industry regulations i.e. Healthcare providers and insurance companies.
- **GLBA** - The Gramm-Leach-Bliley Act regulations for financial institutions including banks, mortgage brokers, lenders, credit unions, insurance and real-estate companies.
- **SOX** - Sarbanes-Oxley for publicly held companies.
- **PCI** - Payment Card Industry regulations for organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

credit card/debit card data.

- **FISMA** – The Federal Information Security Management Act regulations for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency.

Sample Admin Events Reports for Compliance Purpose



Start Date 2014-06-06
End Date 2014-06-06

HIPAA > Admin Events

Show 10 records per page

Page1 of 3 Go to page

Admin Events

Time	Event Type	Severity	Message	User Name	Source	Status
2014-06-06 18:21:32	GUI	Information	Administrator 'admin' logged in succe…	admin	10.202.22.2	Successful
2014-06-06 15:40:31	GUI	Information	Administrator 'admin' logged out of W…	admin	10.202.22.37	Successful
2014-06-06 15:17:57	GUI	Information	Administrator 'admin' logged out of W…	admin	172.16.16.17	Successful
2014-06-06 15:17:28	GUI	Information	Administrator 'admin' logged in succe…	admin	10.202.22.37	Successful
2014-06-06 14:38:55	GUI	Information	Administrator 'admin' logged in succe…	admin	172.16.16.17	Successful
2014-06-06 12:56:16	GUI	Information	Administrator 'admin' logged out of W…	admin	172.16.16.17	Successful
2014-06-06 12:29:24	GUI	Notice	Registration information of 'It s 5 Sup…	LOCAL	127.0.0.1	Successful
2014-06-06 12:29:24	GUI	Notice	Registration information of 'Gateway…	LOCAL	127.0.0.1	Successful
2014-06-06 12:29:24	GUI	Notice	Registration information of 'Gateway…	LOCAL	127.0.0.1	Successful
2014-06-06 12:29:24	GUI	Notice	Registration information of 'Out Boun…	LOCAL	127.0.0.1	Successful

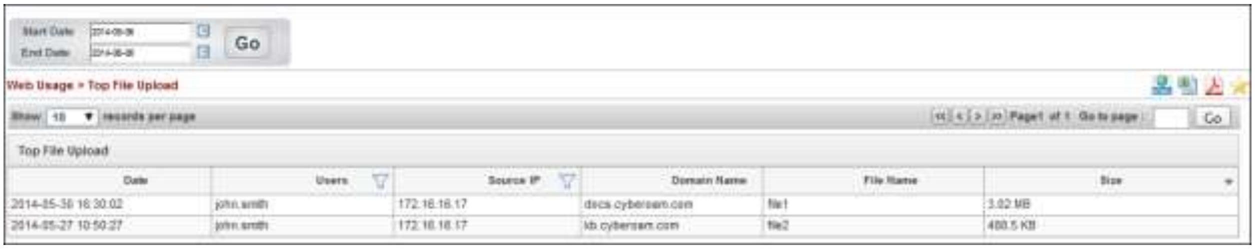
Screen – Admin Events Report

Data Leakage reports

Data leakage reveals the data loss resulting from employee behavior like lack of awareness, lack of diligence or deliberate action from the disgruntled employees, which poses a much more extensive threat than Enterprise can realize. The report provides files uploaded by the employees.

User-wise HTTP Upload

View report from **Reports > Web Usage > Top File Upload**



Start Date 2014-05-30
End Date 2014-06-06

Web Usage > Top File Upload

Show 10 records per page

Page1 of 1 Go to page

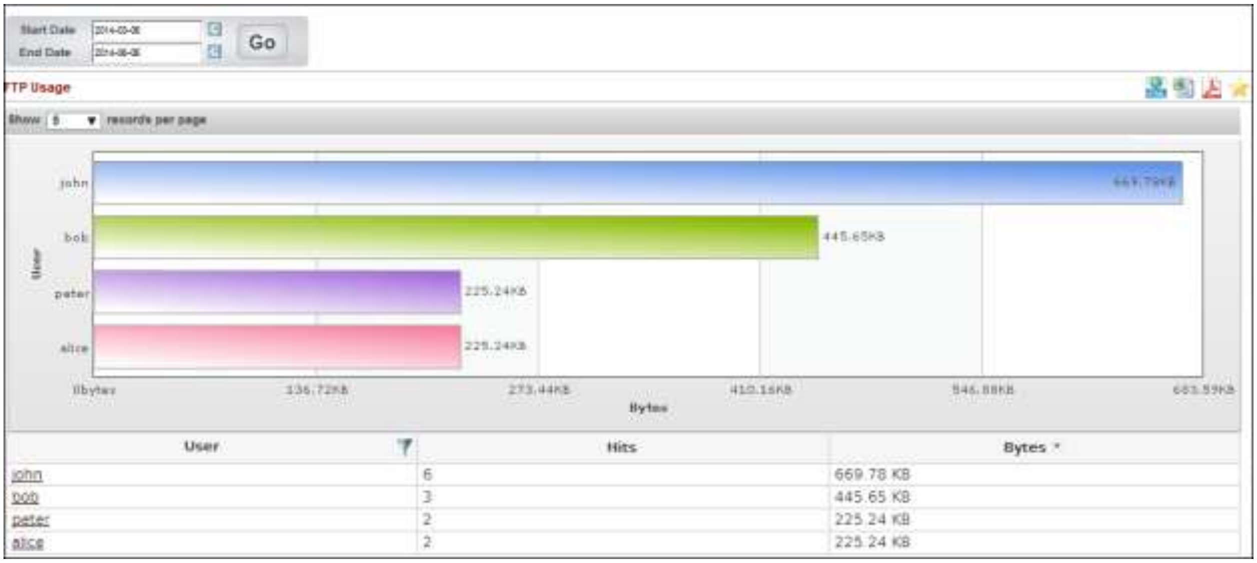
Top File Upload

Date	Users	Source IP	Domain Name	File Name	Size
2014-05-30 16:30:02	john.smith	172.16.16.17	docs.cyberoam.com	file1	3.02 MB
2014-05-27 10:50:27	john.smith	172.16.16.17	kb.cyberoam.com	file2	488.5 KB

Screen – User-wise HTTP Upload Report

User-wise FTP Upload

View from **FTP Usage > Top FTP Users (Upload)**



Start Date 2014-03-06
End Date 2014-06-06

User	Hits	Bytes
john	6	669.78 KB
bob	3	445.65 KB
peter	2	225.24 KB
alice	2	225.24 KB

Screen – User-wise FTP Upload Report

Log Viewer

Log Viewer allows administrator to view the logs for specific event modules like IPS, Web Filter, System or Anti Virus. This page gives concentrated information about all the events that occurred under respective modules.

To view logs for particular events, navigate to **Logs & Reports > Log Viewer**.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Advanced Security

Certificate Management

To use Certificates for VPN authentication or HTTPS scanning, you must have valid Certificate Authority and a certificate. Cyberoam allows you to generate a local CA to sign its own certificate. External or third-party certificates can also be used after adding the third-party provider's CA to Cyberoam.

Third Party CAs can be used for HTTPS Scanning. The certificates issued by Third Party CAs can be used for secure access of Captive Portal, Web Admin Console and My Account.

Navigate to **System > Certificate** to manage certificates. You can use default CA and can modify and re-generate it as per your requirement if you are not using any external CA. Using this CA, you can generate self-signed certificate and use it in VPN policy.

Using Third Party CA involves uploading:

- CA and root certificate (.pem or .der format)
- Certificate
- CRL (Certificate Revocation List)

Refer Add an External Certificate Authority (CA) in Cyberoam for defining external CA.

Spoof Prevention

Cyberoam's Unicast Reverse Packet Forwarding feature, also called Anti Spoofing, protects your network against IP Spoofing, and hence, all kinds of attacks that utilize IP Spoofing techniques, like DoS attacks. Cyberoam examines all incoming packets and discards all such packets that do not carry a known Source IP Address. In other words, if the source IP Address of a packet does not match with any entry on Cyberoam's routing table, or if the packet is not from a direct subnet, then Cyberoam drops that packet.

Navigate to **Firewall > Spoof Prevention** to enable spoof prevention for securing the LAN, WAN or DMZ zones.

If enabled, appliance provides 3 ways to prevent spoofing using IP-MAC trusted list:

- **IP Spoofing** – Packets will be dropped if matching route entry is not available.
- **MAC Filter** – Packets will be dropped if the MAC Addresses are not configured as trusted MAC.
- **IP-MAC Pair Filter** – Packets will be dropped if IP and MAC do not match with any entry in the IP-MAC trusted list.

Refer Does Cyberoam protect the network against IP Spoofing? for scenario specific information on Spoof Prevention.

DoS

To protect the network from DoS attacks for IPv4 and IPv6 traffic, appropriate DoS settings must be configured on Cyberoam. You can configure DoS settings by navigating to Firewall > DoS > Settings. To

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

configure attack definition for the source and destination traffic, refer **Prevent DoS and DDoS Attacks using Cyberoam**.

Cyberoam Appliance also allows you to bypass DoS rules in case you are sure that a particular source is not a threat to your network. Refer article **Create DoS Bypass Rule** for scenario specific information on bypassing DoS rule for a trusted source.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam Troubleshooting

Cyberoam provides Diagnostic Tools, System Graphs, Connection List, and Packet Capture logs to check the health of the System. They are used for troubleshooting and diagnosing problems found in the system. Cyberoam also provides the facility to generate a Consolidated Troubleshooting Report which consists of the system's current status file and log files

System Graphs

System Graphs provide 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. Go to **System > Diagnostics > System Graphs** to view graphs for different system resources including CPU utilization, interface and memory info. You can also gauge the load average on the system with the Load Average graphs. These graphs help you to understand the overall health of the system and thereby help you make changes into the system.

Packet Capture

System > Diagnostics > Packet Capture provides a Dropped Packet log, which can be to monitor the dropped packet. Refer to Monitor dropped packets on how to view and interpret the dropped packet log.

Diagnostic Tools

System > Diagnostics > Tools provide diagnostic Tools such as Ping, Trace Route, Name Lookup and Route Lookup can be used to diagnose connectivity problems, network problems and to test network communications. These assist in troubleshooting issues such as packet loss, connectivity, discrepancies in the network.

Connection List

System > Diagnostics > Connection List provides current or a live connection snapshot of your appliance in the list form. Apart from the connection details, it also provides information like Firewall Rule id, userid, connection id per connection. It is also possible to filter the connections list as per the requirement and delete the connection.

Points to remember:

- If you are integrating Cyberoam with Active Directory for authentication, use Active Directory as your DNS. You are required to define Active Directory as DNS both in Cyberoam as well as all the desktops.
- If you have configured Cyberoam as DHCP server for leasing IP Addresses, make sure DHCP server is enabled for auto-start. Else, IP Address will be leased only after rebooting Cyberoam.

© Copyright 2014 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.