

Cyberoam appliance can be deployed in a network in two modes:

- Gateway mode. Popularly known as Route mode
- Bridge mode. Popularly known as Transparent mode

Article provides step-by-step procedure to configure Cyberoam in Gateway mode. Configuration steps are provided assuming that you have not configured Cyberoam appliance and are using factory default settings of the appliance. If your appliance has any custom settings, [rollback to factory default setting](#) before following the steps provided in the article.

We are going to consider a hypothetical network example with firewall serving as a Gateway. We will replace the existing firewall with Cyberoam without changing the existing network LAN schema. Article covers:

- [Features supported in gateway mode](#)
- [Deployment steps](#)
- [How to verify configuration](#)
- [Advance configuration](#)

Overview

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.

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 Detection and Prevention Services, Gateway Anti Virus, and Gateway Anti spam. If you do not have Cyberoam security modules subscriptions, you may register for free trial.

Features supported in Gateway mode

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

VLAN support in Gateway mode

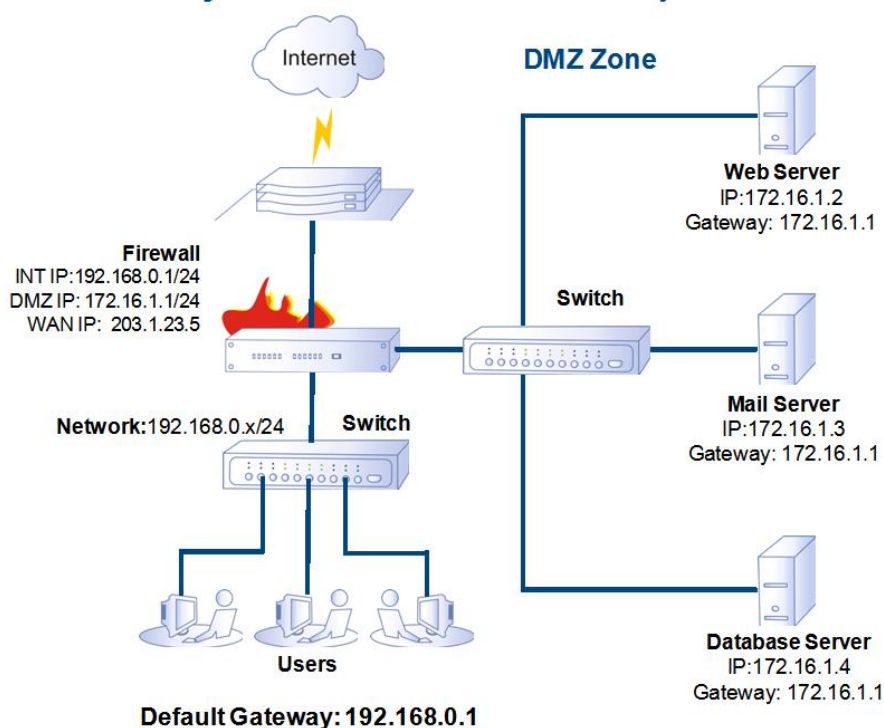
While the network depicted in the example is simple, it is not uncommon for large networks to use VLANs for segmentation of traffic. If the existing firewall was configured for VLAN, refer [Virtual LAN Configuration Guide](#) for configuring VLAN in Cyberoam.

High Availability support in Gateway mode

HA, refer High Availability Guide for configuring HA cluster in Cyberoam

Sample Schema

Throughout the article we will use the network parameters displayed in the below given network diagram.

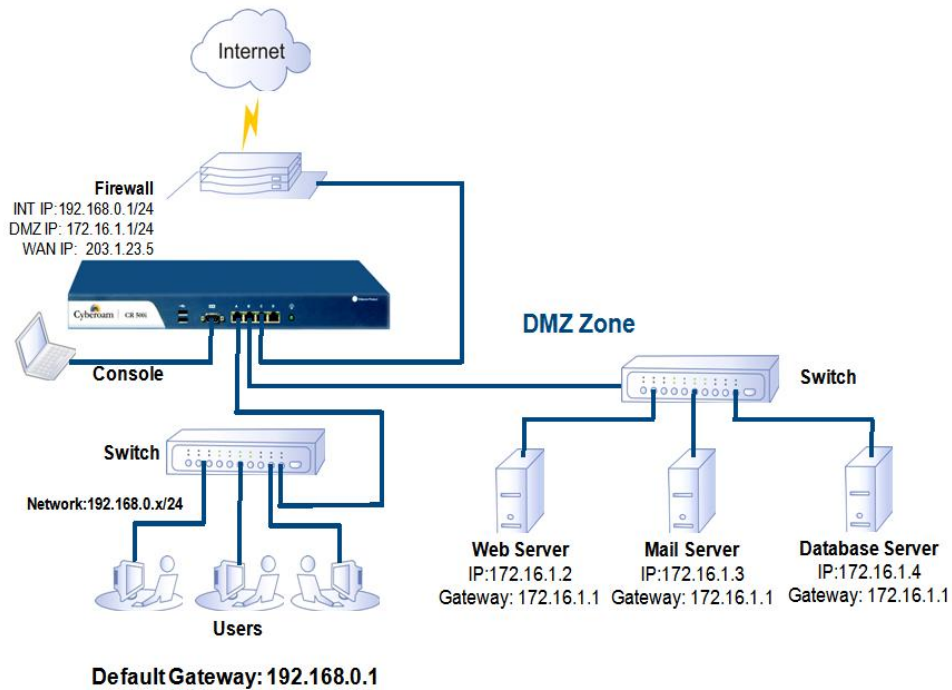
Before Cyberoam Scenario - Gateway

The below given network diagram depicts a network where Cyberoam is added to the perimeter for the purpose of providing security services.

Traffic from hosts connected to the LAN would be permitted outbound through the Cyberoam to the gateways, while traffic from the WAN would, by default, not be permitted inbound.

The public servers, a mail, web and database server, on the DMZ, an access Rule allowing WAN-to-LAN traffic for the appropriate IP addresses and services will be added to allow inbound traffic to those servers.

Cyberoam in Gateway Mode



Preparing to configure

Cyberoam Appliance is shipped with the following default configuration:

Port A IP address (LAN zone): 172.16.16.16/255.255.255.0

Port B IP address (WAN zone): 192.168.2.1/255.255.240.0

Gather DNS IP address, date and time zone and well as administrator email address.

Deployment steps

Connecting Appliance

Connect port A of the Appliance to a management computer's Ethernet interface. You can use a cross-over Ethernet cable to connect directly or use straight-through Ethernet cable to connect through hub or switch. Both the cables are provided along with the Appliance.

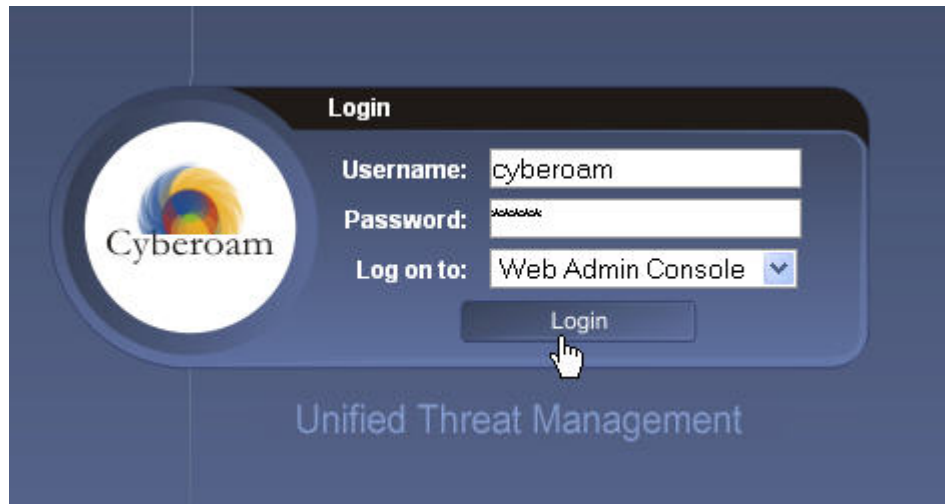
By connecting management computer to port A, we are assigning port A to LAN zone.

Set the IP address of the management system 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.



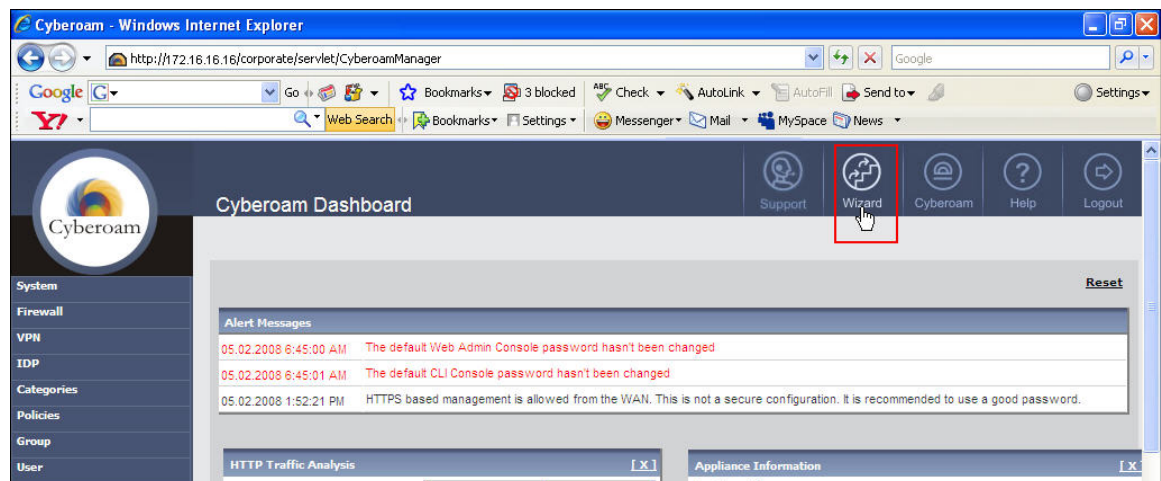
Internet Explorer 5.5+ or Mozilla Firefox 1.5+ is required to access Web Admin Console.

If you cannot log on, verify the following configurations:

- Did you plug your management workstation into the port A on the appliance? - Deployment can only be performed through port A.
- Is the link light glowing on both the management computer and the Appliance? – If not, check and replace the cable
- Is your management 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?

Starting Network Configuration Wizard

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





Configuring deployment mode and IP addresses

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

The diagram illustrates the Gateway Mode deployment. A CYBEROAM device is connected to a Router, which is connected to the PUBLIC INTERNET. The CYBEROAM device is also connected to a Console (laptop). The CYBEROAM device is connected to a Switch, which is connected to a DMZ Zone containing a Web Server, Mail Server, and Database Server. The Switch is also connected to a group of desktop computers.

Deployment Mode Zone & Network Configuration Access Configuration Mail Settings Date & Time Configuration Summary


Navigation buttons: Previous, Next (highlighted), Cancel

javascript:submitForm();


Internet 100%

Network Configuration Wizard - Windows Internet Explorer

http://172.16.16.16/corporate/webpages/wizard/routeInterfaceMgmt.jsp



Network Configuration



Port A As per network diagram

☐ Obtain an IP from DHCP

☐ Obtain an IP from PPPoE

☒ Use Static IP

IP Address

192.168.0.1

Subnet Mask

255.255.240.0

Zone

LAN

Gateway Details

ISP Name

IP Address

PPPoE Details

User Name

Password

DNS Configuration

☐ Obtain DNS from DHCP

Primary DNS

203.88.135.194

Secondary DNS

192.168.1.254

Previous

Next

Deployment Mode

Zone & Network Configuration

Access Configuration

Mail Settings

Date & Time Configuration

Summary

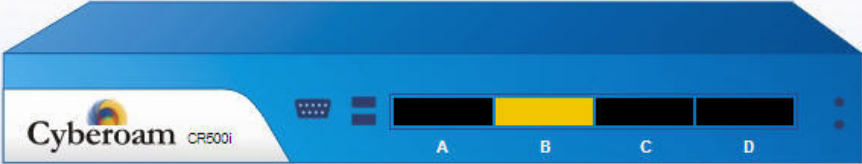
Internet

100%

Network Configuration Wizard - Windows Internet Explorer

http://172.16.16.16 /corporate/webpages/wizard/routeInterfaceMgmt.jsp

Cyberoam Network Configuration



Port B

☐ Obtain an IP from DHCP
☐ Obtain an IP from PPPoE
☒ Use Static IP

IP Address: 203.1.23.5
Subnet Mask: 255.255.255.240
Zone: WAN

Gateway Details

ISP Name: elitecore
IP Address: 192.168.0.1

PPPoE Details

User Name:
Password:

DNS Configuration

☐ Obtain DNS from DHCP
Primary DNS: 203.88.135.194
Secondary DNS: 192.168.1.254

Previous Next

Deployment Mode Zone & Network Configuration Access Configuration Mail Settings Date & Time Configuration Summary

Internet 100%

Network Configuration Wizard - Windows Internet Explorer

http:// 172.16.16.16 /corporate/webpages/wizard/routeInterfaceMgmt.jsp

Cyberoam | Network Configuration

Port C

☐ 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: DMZ

Gateway Details:
 ISP Name:
 IP Address:
 PPPoE Details:
 User Name:
 Password:

DNS Configuration:
☐ Obtain DNS from DHCP
 Primary DNS: 203.88.135.194
 Secondary DNS: 192.168.1.254

Previous Next

Deployment Mode | **Zone & Network Configuration** | Access Configuration | Mail Settings | Date & Time Configuration | Summary

javascript:submitForm()

Internet 100%

Configuring default Internet Access policy (IAP)

For your convenience, Cyberoam provides 3 pre-defined Internet Access policy. Based on the Internet Access policy, Cyberoam decided which outbound traffic is to be allowed or dropped.

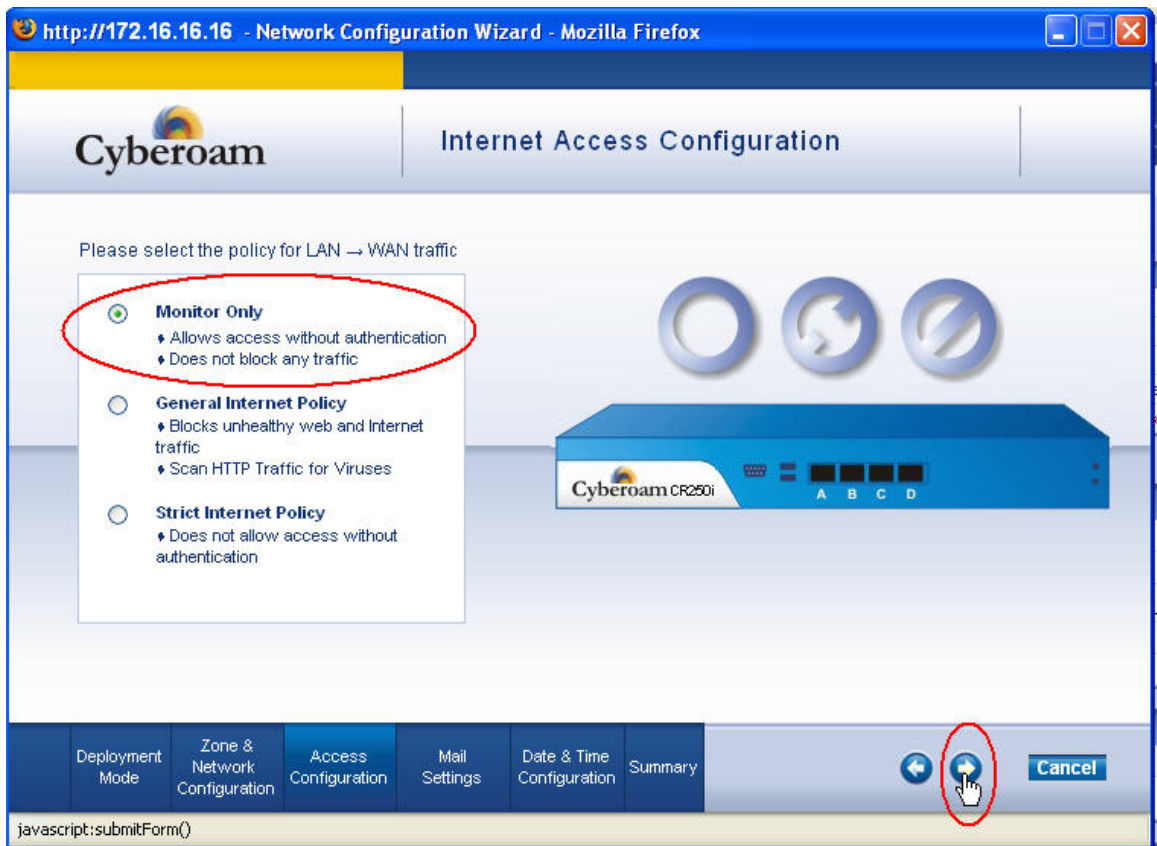
Monitor Only policy allows entire outbound traffic i.e. all the sessions origination from LAN to WAN.

General Internet policy allows entire authenticated outbound traffic after scanning HTTP traffic for virus. But, blocks traffic from the URLs categorized under following Web categories: Porn, Nudity, AdultContent, URL TranslationSites, Drugs, CrimeandSuicide, Gambling, MilitancyandExtremist, PhishingandFraud, Violence, Weapons categories

Strict Internet policy allows only authenticated outbound traffic i.e. all the sessions origination from LAN to WAN after user is authenticated.

As IAP can altogether disable protection or block all access to the Internet, hence it is recommended to apply Monitor Only policy.

Please note, if you apply General Internet policy, certain access to certain URLs will be blocked.




Configuring 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.

Network Configuration Wizard - Windows Internet Explorer

http:// 172.16.16.16 /corporate/webpages/wizard/notificationConf.jsp



Configure Mail Settings



Configure Email and Mail Server settings for System Notifications

Send Notifications to Email Address

margaret@elitecore.com

Mail Server IP Address - Port

203.88.135.194 - 25

From Email Address

anthony@elitecore.com

Deployment Mode

Zone & Network Configuration

Access Configuration

Mail Settings

Date & Time Configuration

Summary

←

→


Cancel

javascript:submitForm()


Internet 100%

Configuring Date and Time zone


http://172.16.16.16 - Network Configuration Wizard - Microsoft Internet Explorer



Date & Time Configuration



Date & Time	
Time Zone	GMT+05:30 - Asia/Calcutta
Set Date	06 YY 05 MM 30 DD
Set Time	19 HH 38 MM 47 SS



Deployment Mode

Zone & Network Configuration

Access Configuration

Mail Settings

Date & Time Configuration

Summary

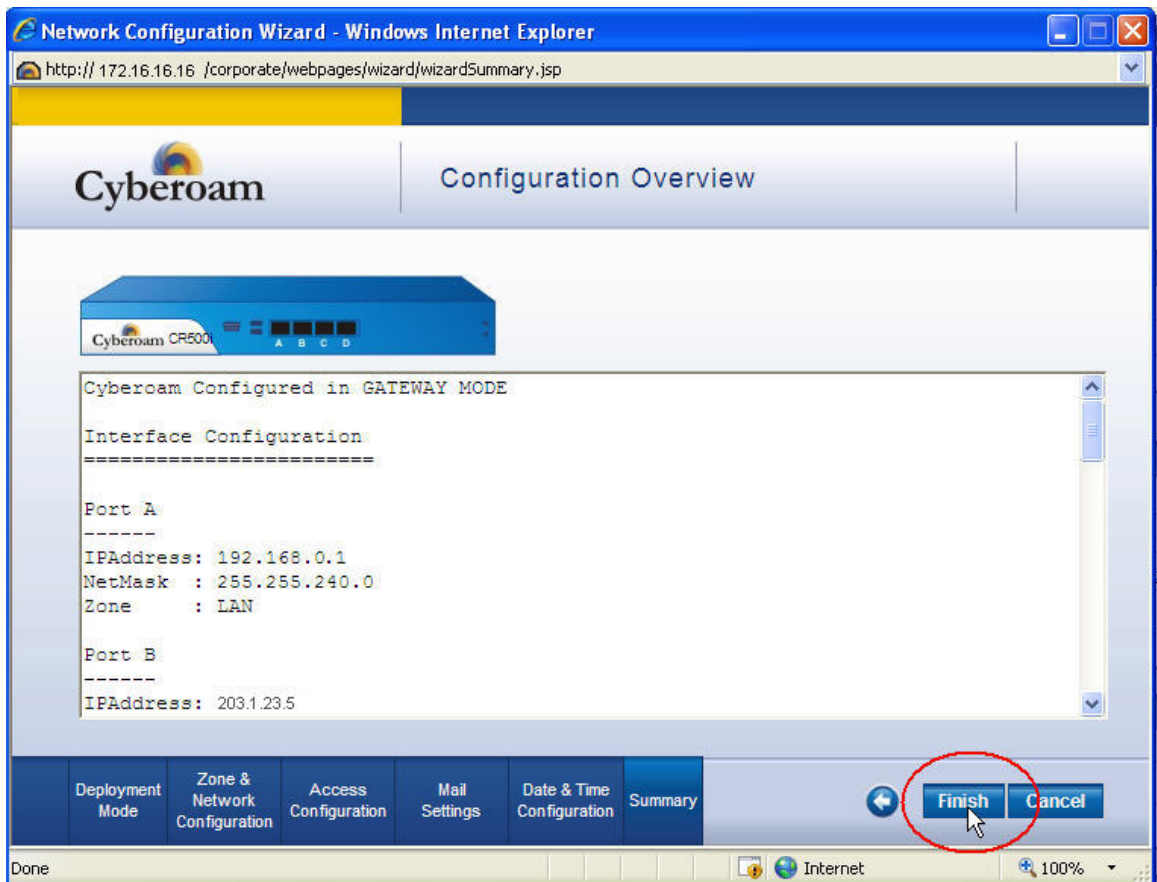
←

→

Cancel

Done

Internet



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



Note:

After changing the LAN IP address, you must use this IP address to reconnect to the web admin console. You might also have to change the IP address of the management station to be on the same subnet as the new IP address.

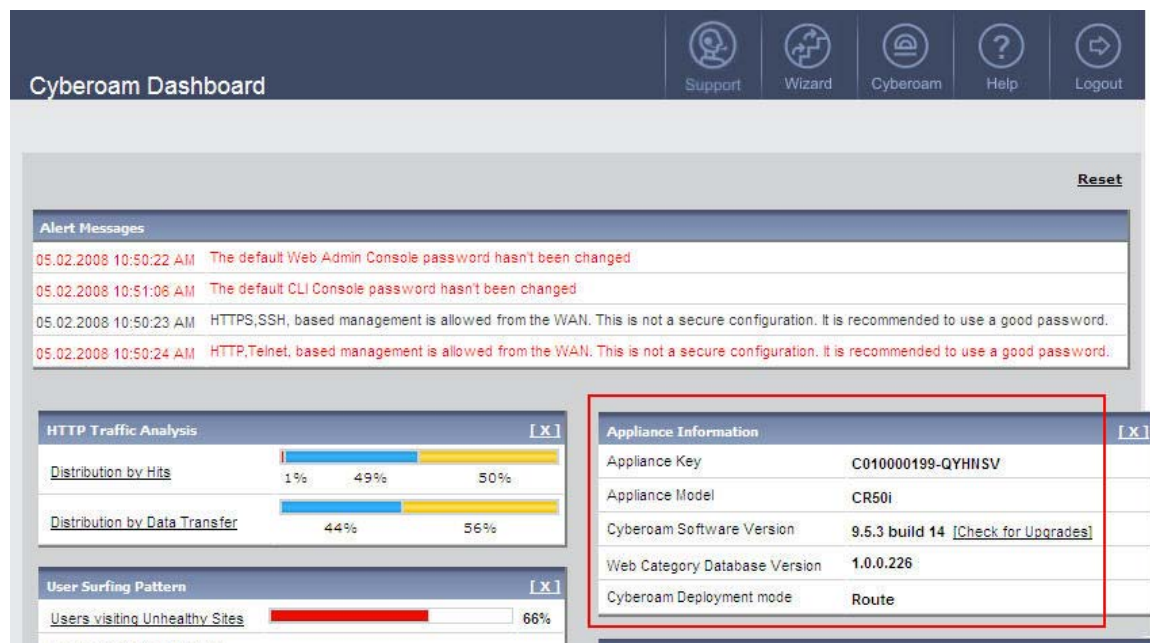
This finishes the basic configuration of Cyberoam and now you are ready to use the Appliance.

Verifying configuration using Dashboard

Browse to <https://192.168.01> 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.

Cyberoam Dashboard

Support Wizard Cyberoam Help Logout

Alert Messages [Reset](#)

05.02.2008 10:50:22 AM The default Web Admin Console password hasn't been changed

05.02.2008 10:51:06 AM The default CLI Console password hasn't been changed

05.02.2008 10:50:23 AM HTTPS,SSH, based management is allowed from the WAN. This is not a secure configuration. It is recommended to use a good password.

05.02.2008 10:50:24 AM HTTP,Telnet, based management is allowed from the WAN. This is not a secure configuration. It is recommended to use a good password.

HTTP Traffic Analysis [\[X\]](#)

Distribution by Hits

1%	49%	50%
----	-----	-----

Distribution by Data Transfer

44%	56%
-----	-----

User Surfing Pattern [\[X\]](#)

Users visiting Unhealthy Sites 66%

Users visiting Non-working Sites 100%

Users visiting Productive Sites 0%

Appliance Information [\[X\]](#)

Appliance Key C010000199-QYHNSV

Appliance Model CR50i

Cyberoam Software Version 9.5.3 build 14 [\[Check for Upgrades\]](#)

Web Category Database Version 1.0.0.226

Cyberoam Deployment mode Route

Gateway Status [\[X\]](#)

Gateway Name	Gateway IP Address	Status
elitecore	192.168.0.1	

3. Verify IP assignments

Go to System> Network Configure > Manage 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.

Manage Interface

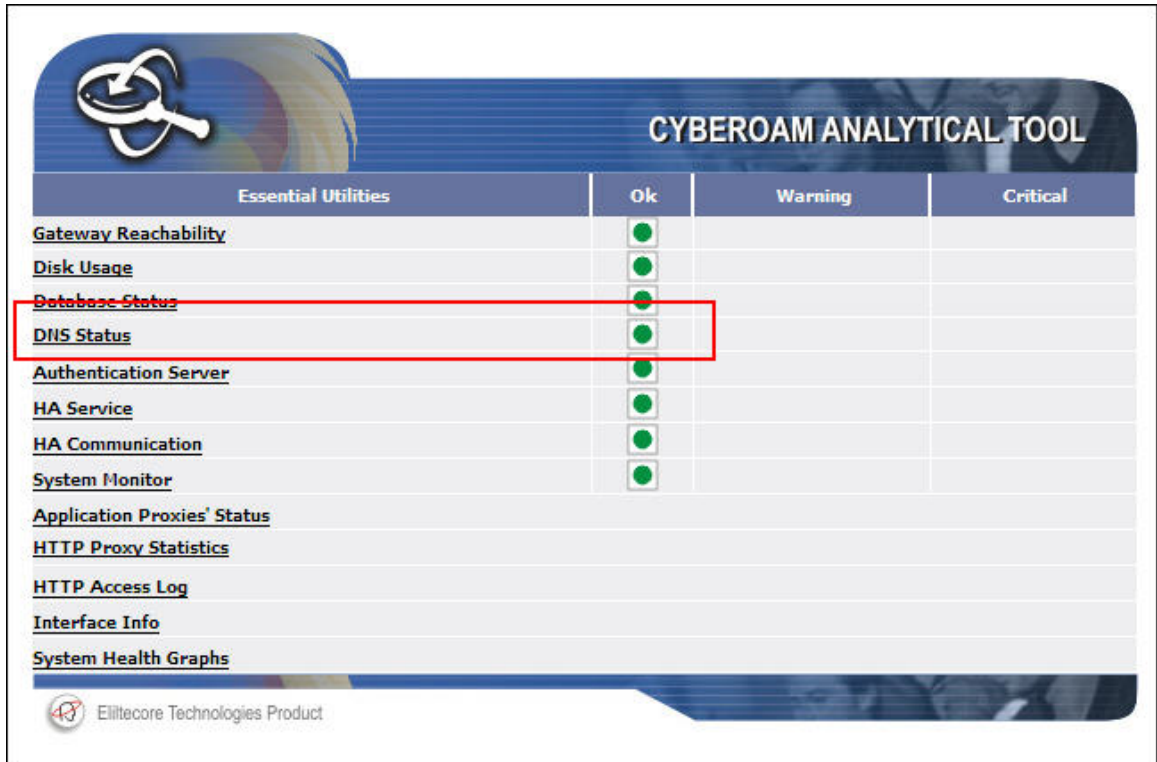
Support Wizard Cyberoam Help Logout

[Add Alias](#) [Add VLAN Subinterface](#)

+	Interface name	IP/Netmask	Status	Zone Name	Zone Type	Manage
	Port A	192.168.0.1/255.255.240.0	-	LAN	LAN	
	Port B	203.1.23.5/255.255.255.240	-	WAN	WAN	
	Port C	172.16.1.1/255.255.255.0	-	DMZ	DMZ	

4. Verify DNS status

Browse to <http://<Cyberoam IP address>/dg.html> and log on with default username and password and verify that DNS status is "Ok".



5. If due to incorrect IP address configuration, you are not able to access appliance, rollback to factory default settings and re-configure Cyberoam by repeat the entire deployment steps given in this document.

What next?

If Cyberoam is up and running, you are now ready to use the Appliance. You can now:

- Monitor network activities using Cyberoam Reports.
- Detect your network traffic i.e. applications and protocols accessed by your users.
- Configure authentication to monitor and log user activities based on User names

Rollback to factory default settings

Access Telnet Console using any of the SSH client. Start SSH client and create new Connection with the following parameters:

Hostname - <Cyberoam server IP Address>

Username – admin

Password – RESET

This will rollback Cyberoam configuration to its factory default settings.

