Cyberoam

Unified Threat Management

QUICK START GUIDE

CR 50i
CR 100i
CR 250i
CR 500i
Appliances

F000000116

Version: QSG 50-500i/9410-1.0-17/01/2007

1 DEFAULTS

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

Telnet Console (SSH/Serial Connection)	
*Password:	admin

* Username and Password are case sensitive

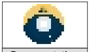
Package Contents

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

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

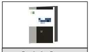
Serial Cable

Blue Straight-through Ethernet Cable


Documentation CD

Power Cable

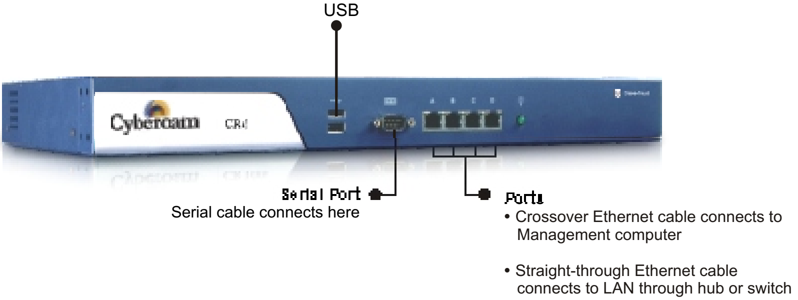
Red Crossover Ethernet Cable


Quick Start Guide

If any items from the package are missing. please contact Cyberoam Support at support@cyberoam.com

2 UNDERSTANDING THE APPLIANCE

▶ FRONT PANEL



USB

Serial Port
Serial cable connects here

Ports
- Crossover Ethernet cable connects to Management computer
- Straight-through Ethernet cable connects to LAN through hub or switch

- **Serial Port** - Use to connect to the Management computer
- **USB port** - Provided for future use
- **Ports# A,B,C,D,E,F** - Use these ports to connect the Appliance to the Ethernet network

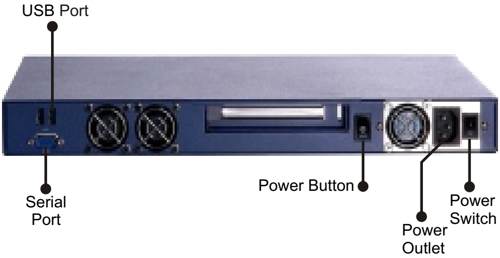
CR 250i and CR 500i - If you want to bypass Cyberoam incase of power or Appliance failure when deployed as Bridge, use C and D ports.

CR 50i and CR 100i - Hardware Bypass option is not available**.**

As Cyberoam does not pre-configure any ports for LAN, WAN, DMZ networks, it is not necessary to use any particular port for them. Usage of ports depends on how the physical connection is required or planned.

Total number of ports are appliance specific

▶ BACK PANEL



**Serial Port - **Provided for future use

**Power button - **Keep the button pressed for 5 seconds to power off. Press to power on.

3 PLANNING THE CONFIGURATION

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

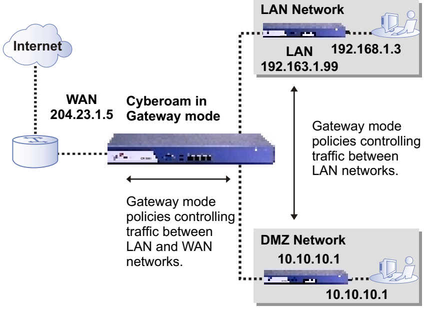
To control the Internet access through Cyberoam the entire Internet bound traffic from the LAN network should pass through Cyberoam.

Gateway Mode

Configure as Gateway if you want to use Cyberoam as

1. A firewall or replace an existing Firewall
2. A gateway for routing traffic
3. Deploy Cyberoam's Gateway failover with link load balancing

Apart from configuring Gateway IP address (IP address through which all the traffic will be routed), you must also configure LAN and WAN IP addresses.


LAN Network
Internet
LAN 192.168.1.3
192.163.1.99
WAN
204.23.1.5
Cyberoam in Gateway mode
Gateway mode policies controlling traffic between LAN networks.
Gateway mode policies controlling traffic between LAN and WAN networks.
DMZ Network
10.10.10.1
10.10.10.1

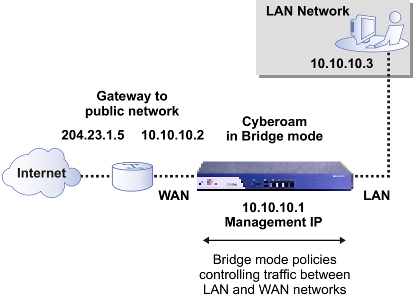
Bridge Mode

Configure as Bridge if

1. You have a private network behind an existing firewall or behind a router and you do not want to replace the firewall.

2. You are already masquerading outgoing traffic.

   Cyberoam can be bypassed only if deployed as Bridge.



You will be able to manage and monitor the entire Internet traffic passing through Cyberoam, control web access and apply bandwidth and application restrictions, apply virus and spam scanning policy and IDP policy in either of the modes.

Refer to the documentation CD-ROM for information on how to control traffic, and how to configure antivirus protection, content filtering, spam filtering, intrusion detection and prevention (IDP), and virtual private networking (VPN).

4 GETTING CONFIGURATION INFORMATION

Use the tables given below to gather the information you need before proceeding to deploy Appliance.

Gateway Mode

For all the required Ports

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

The LAN IP address and Subnet Mask must be valid for the respective networks.

Bridge Mode

Bridge IP address	IP address	___.___.___.___
	Subnet Mask	___.___.___.___

► GENERAL SETTINGS

IP address of the Default Gateway A default gateway is required for Cyberoam to route connections to the Internet.	___.___.___.___
DNS IP Address	___.___.___.___
System Time Zone	______________
System Date and Time	______________
Email ID of the administrator where Cyberoam Will send System Alerts	______________

5 CONNECTING CYBEROAM

Ethernet connection

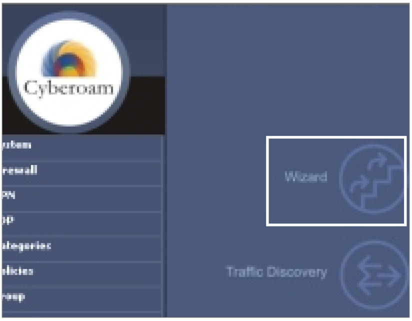
1. Connect the Cyberoam Appliance's 'Port A' to a management computer's Ethernet interface.
   Use a cross-over Ethernet cable to connect the devices directly or use straight-through Ethernet cable to connect the devices through a hub or switch.
2. Change the IP address of the management computer to172.16.16.2 and the subnet mask to 255.255.255.0.

From the management computer:

1. Browse to https://172.16.16.16
2. Log on to the Cyberoam Web Admin Console using default username 'cyberoam' and password 'cyber'.
3. Click Wizard icon to launch the Network Configuration wizard.

Prerequisite

1. Ethernet connection between management computer and Cyberoam.
2. Internet Explorer 5.5+ or Mozilla Firefox 1.5+ is required to access Cyberoam Web Admin Console.

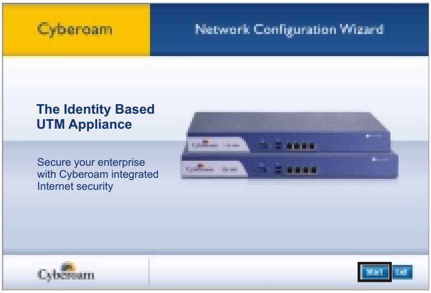


Note: If you change the LAN IP address (Gateway mode) or Bridge IP address (Bridge mode), you must use this address to reconnect to the Web Admin Console. You might also have to change the IP address of the management computer to be on the same subnet as the new IP address.

6 CONFIGURING THE CYBEROAM APPLIANCE

Network Configuration Wizard will guide you step-by-step through configuration of the network parameters like IP address, subnet mask, and default gateway for Cyberoam. Use the configuration settings you have noted in section 4.

Click **'Start'** to start the configuration.



The Identity Based UTM Appliance

Secure your enterprise with Cyberoam integrated Internet security

▶ CONFIGURE MODE

Gateway mode

To configure Cyberoam in Gateway mode, select Gateway Mode option and click ➡ button.

Follow the on screen steps to configure:

1. Configure static IP address and subnet mask
2. Provide Gateway details: ISP name and IP address or if you want to enable Interface for PPPoE, provide PPPoE details: User Name and Password (only for WAN zone)

Click **'Next'** button to repeat the above procedure for each port

3. Provide DNS IP address

Bridge mode

To configure Cyberoam in Bridge mode, select Bridge Mode option and click ➡ button.

1. Configure Bridge IP address and subnet mask.

   CR 250i and CR 500i - If you want to bypass Cyberoam incase of power or Appliance failure when deployed as Bridge, use C and D ports.

   CR 50i and CR 100i - Hardware Bypass option is not available**.**

2. Provide Gateway and DNS IP address.

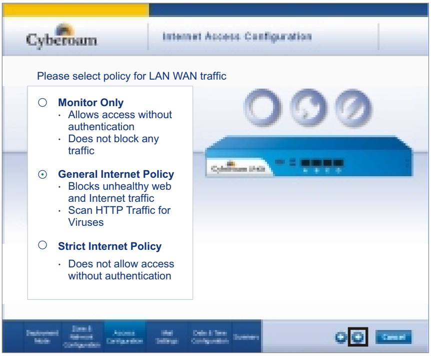
▶ CONFIGURE INTERNET ACCESS

Configure Internet access policy for LAN to WAN traffic.

'Monitor Only' policy allows LAN to WAN traffic

'General Internet' policy enables IDP[1] and Virus[2] scanning and allows LAN to WAN traffic except Unhealthy Web and Internet traffic as defined by Cyberoam. This will include sites related to Adult contents, Drugs, Crime and Suicide, Gambling, Militancy and Extremist, Violence, Weapons, Phishing and Fraud and URL Translation sites.

'Strict Internet' policy enables IDP[1] and Virus[2] scanning and allows only authenticated LAN to WAN traffic.


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

Please select 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

Click ➡ button to configure the mail settings

[1] Until Intrusion Detection and Prevention module is subscribed, IDP scanning will not be effective.
[2] Until Gateway Anti Virus module is subscribed, virus scanning will not be effective.

▶ CONFIGURE MAIL SETTINGS

1. Specify Administrator Email ID
2. Specify Mail server IP address
3. Specify email address that should be used to send the System Alerts

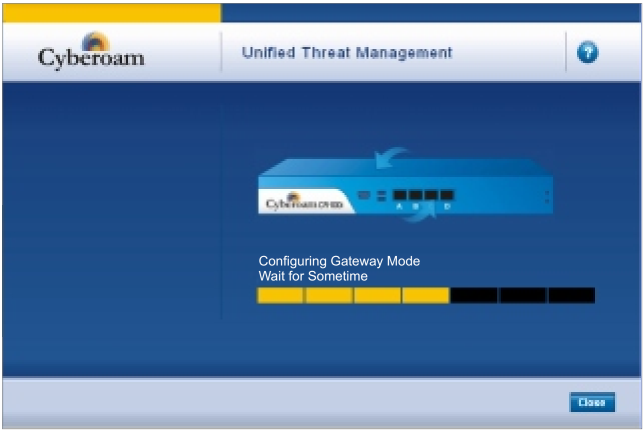
Click ➡ button for Date and Time zone configuration

▶ CONFIGURE DATE AND TIME ZONE

Set time zone and current date

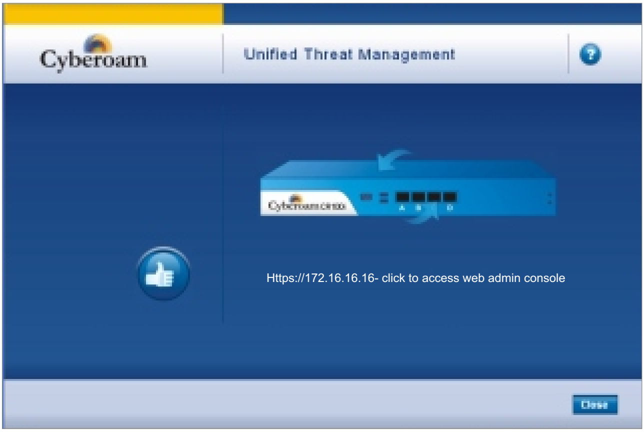
Click ➡ button to view the configured details. Copy the configured details for future use.

Click **'Finish'**. It will take few minutes to save the configuration details.



Configuring Gateway Mode
Wait for Sometime

On successful configuration following page will be displayed.



Https://172.16.16.16- click to access web admin console

Click the **URL** to access the Web Admin Console.
Click **Close** to close the Network Configuration Wizard window

Congratulations!!!

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

7 WHAT NEXT?

1. Access Cyberoam Web Admin Console

   Browse to https://<IP address of cyberoam> and log on using the default username (cyberoam) and password (cyber).

   Note: Internet Explorer 5.5+ or Mozilla Firefox 1.5+ is required to access the Cyberoam Web Admin Console

2. Create Customer Account and register Appliance
   Prerequisite: For customer account creation and appliance registration as well as module registration , Cyberoam server must be able to connect to the Internet as Cyberoam server will contact the Cyberoam's central registration site with the Appliance details

   Click 'Register Now' on the main page to create customer account and register your appliance. As soon as you register, you can avail 8 x 5 Support.

   You can go to Help → Licensing and subscribe for free 30-day trial subscription for Web and Application Filtering, IDP, Anti Virus and Anti Spam.

3. Go to Firewall → Manage Firewall page to centrally configure the Cyberoam Appliance’s UTM features. For further details refer to User Guide, Firewall section.

4. Be sure to configure the correct firewall rule for your Domain Name Server (DNS). You may not be able to access Internet if not configured properly.

5. Access Help

   For accessing online help, click the Help button or F1 key on any of the screens to access the corresponding topic's help. Use the Contents and Index options to navigate through the entire online help.

   You can go to Help → Guides and download complete documentation set.

6. Set authentication parameters

   Go to User → Authentication Settings to define the authentication parameters.

Important Notice

Elitecore 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. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

User's License

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

Limited Warranty

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and the performance thereof is under warranty provided by Kaspersky Labs. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

Disclaimer Of Warranty

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In the event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

Restricted Rights

Information supplies by Elitecore Technologies Ltd. Is believed to be accurate and reliable at the time of printing, but Elitecore Technologies assumes no responsibility for any errors that may appear in this documents. Elitecore Technologies reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice

Corporate Headquarters

Elitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

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:

Phone: +91-79-66065777
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit **www.cyberoam.com** for the regional and latest contact information.

Cyberoam
Unified Threat Management

Visit: www.cyberoam.com
Contact: info@cyberoam.com

Elitecore Technologies Limited
www.elitecore.com

USA - Tel: +1-978-465-8400, Fax: +1-978-293-0200
India - Tel: +91-79-66065606, Fax: +91-79-26407640