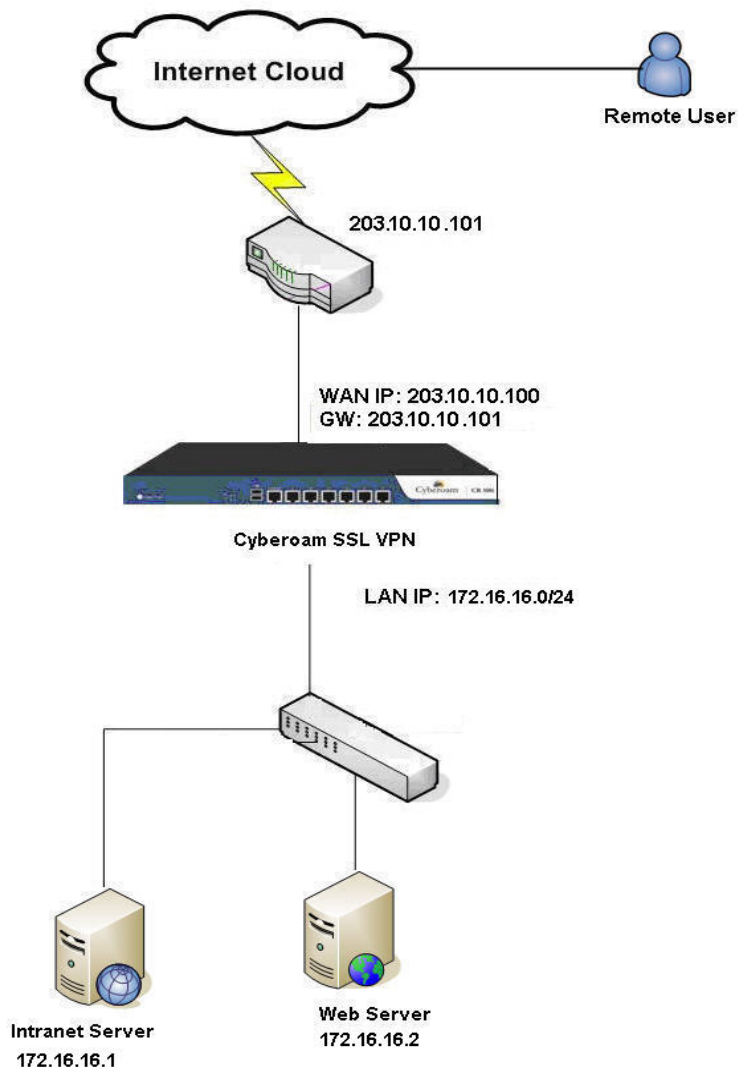


SSL (Secure Socket Layer) VPN provides simple-to-use and implement secure access for the remote users. It allows access to the corporate network from anywhere, anytime and provides the ability to create point-to-point encrypted tunnels between remote user and company's internal network, requiring combination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

Depending on the access requirement, remote users can access corporate network through SSL VPN Client or End user Web Portal (clientless access).

This document describes procedure to configure SSL VPN in Cyberoam:

Network Diagram



Configuration Table

Configuration Parameter	Value
Cyberoam WAN IP	203.10.10.100
Cyberoam LAN IP	172.16.16.0/24
Intranet Server IP	172.16.16.1
Web Server IP	172.16.16.2
IP Range Leased to user after successful connection through SSL VPN	10.1.1.1 to 10.1.1.254

Following are the steps to configure SSL VPN in Cyberoam.

1. [Global Configuration](#)
2. [Access Resource Configuration](#)
3. [Policy Configuration](#)
4. [Portal Settings](#)
5. [SSL-VPN Client Installation for Full Access Mode](#)

Step 1: Global Configuration

a. Create Certificate Authority

1. Go to System → Certificate Management → Manage Certificate Authority
2. Click **Default** certificate authority.
3. Update certificate authority as per following screen shot.

Update Certificate Authority Dashboard W

Certificate Authority

Certificate Authority Name* Default

Country Name* United States

State/Province Name* Texas

Locality Name* Houston (eg. city name)

Organization Name* Elitecore (eg. company name)

Organization Unit Name* Elitecore Pvt Ltd (eg. department name)

Common Name* elitecore (eg. server's hostname)

Email Address* elitecore@cyberoam.com

CA Password* ***** [Change Password](#)

4. Click **Re-Generate**

If the customer is using an external certificate authority, then upload the external certificate authority as follows:

Go to System → Certificate Management → Upload CA.

b. Create Local Certificate

1. Go to System → Certificate Management → New Certificate
2. Check option to **Generate Self Signed Certificate**

3. Generate local certificate with following values:

Parameter	Value
Action	Generate Self Signed Certificate
Certificate Name	Certificate_1
Valid upto	Jul 30, 2010 (change the date from given calendar, if required)
Key length	1024 (change Key length from the drop down, if required)
Password	Specify password (at least 10 characters long)
Confirm Password	Re-enter the password for confirmation. Password is case sensitive.
Certificate ID	E-mail: cyber@cyberoam.com

4. Click **Generate**

c. **Configure SSL Global Parameters**

1. Go to SSL VPN → Global settings
2. Configure global settings with following values:

Parameter	Value
Global Settings	
Protocol	TCP
Port	8443
SSL Server Certificate	Certificate_1(created in Step 1.b)
SSL Client Certificate	Certificate_1(created in Step 1.b)
Full Access Settings	
IP Lease Range	10.1.1.1-10.1.1.254
Subnet Mask	255.255.255.0
Primary DNS	4.2.2.2 (change, if required)
Secondary DNS	203.1.3.194(change, if required)
Primary WINS	Specify IP address of primary WINS, if required
Secondary WINS	Specify IP address of primary WINS, if required
Enable DPD	Select option to detect dead peers. <ul style="list-style-type: none"> • Check Peer after every: 60 seconds (change, if required) • Disconnect after:300 seconds(change, if required)
Idle Time Out	10 Minutes (change, if required)
Web Access Settings	
Idle Time Out	10 Minutes(change, if required)

Global Settings		Dashboard	Wizard	Console	Support	Cyber
General Settings						
Protocol*	TCP	(Select UDP for better performance)				
Port*	8443					
SSL Server Certificate*	Certificate 1					
SSL Client Certificate*	Certificate 1					
Full Access Settings						
IP Lease Range*	10.1.1.1	-	10.1.1.254	(Should be from Private IP ranges. First IP in the range will be used by the server.)		
Subnet Mask*	255.255.255.0					
Primary DNS	4.2.2.2	Secondary DNS	203.1.3.194			
Primary WINS						
Secondary WINS						
Enable DPD*	<input checked="" type="checkbox"/>					
Check Peer after every*	60	Seconds				
Disconnect after*	300	Seconds				
Idle Timeout*	15	Minutes				
Web Access Settings						
Idle Timeout*	10	Minutes				
Save						

Step 2: Access Resource Configuration

Cyberoam SSL VPN can be configured in two modes.

- **Full Access Mode :**
Full Access mode provides access to the corporate network with the help of SSL VPN client. Remote user has to download and install SSL VPN client from end user web portal.
- **Web Access Mode**
Web Access mode provides access of corporate network through web browser only.

Full Access Mode Pre-Requisite:

Add Hosts/Networks

Host and networks are internal corporate resources, which are available to a remote user in Full Access mode while bookmark is a URL which remote user can access in Web access mode.

Full Access mode supports two tunnel types

- **Split tunnel :** In split tunnel mode, only the traffic for the private network is tunneled and encrypted
- **Full tunnel:** In full tunnel mode, private network traffic as well as other Internet traffic is also tunneled and encrypted.

In case of split tunnel, you need to add host and networks in Cyberoam.

Please note that Cyberoam does not support host groups in SSL VPN policy.

To add Host

1. Go to Firewall → Host → Add

2. Add host with following values:

Parameter	Value
Host Name	Host_1
Host Type	IP/Subnet (change host type to Range, IP List, MAC Address, MAC List , if required)
Network	172.16.16.1/255.255.255.255
Select Host Group	host_group_1

The screenshot shows the 'Add Host' configuration page. It includes a title bar with 'Add Host' and navigation links for 'Dashboard' and 'Wizard'. Below the title bar, there's a sub-header 'Add Host'. The form fields are: 'Host Name*' with the value 'host_1'; 'Host Type*' with radio buttons for 'IP/Subnet' (selected), 'Range', 'IP List', 'MAC Address', and 'MAC List'; 'Network*' with two input fields containing '172.16.16.1' and '255.255.255.255' separated by a slash; and 'Select Host Group' with a dropdown menu showing 'host_group_1'. At the bottom right, there are 'Create' and 'Cancel' buttons.

3. Click **Create** to add new host

Web Access Mode Pre-Requisite

Create Bookmarks/ Bookmark Groups

Bookmark is a URL which remote user can access in Web access mode and a bookmark group is a logical grouping of several bookmarks based on user's access requirements.

To create Book Mark

1. Go to SSL VPN → Bookmark → Add Bookmark.
2. Add bookmark with following values:

Parameter	Value
Bookmark Name	SSLVPN_1
Type	HTTP (change to HTTPS, as per requirement)
URL	http://msn.com
Description	Description of bookmark, if required

3. Click **Create** to add new bookmark

To create Bookmark Group

1. Go to SSL VPN → Bookmark → Add Bookmark Group
2. Create a Bookmark Group with following values

Parameter	Value
Bookmark Group Name	BMG_1
Description	Description of bookmark group, if required
Select Bookmark	SSLVPN_1 (created in above step)

3. Click **Create** to add a new bookmark group

Step 3: Policy Configuration

To create policy for SSL VPN

1. Go to SSL VPN → SSL VPN Policy → Add SSL VPN Policy
2. Configure SSL VPN policy using following values:

Parameter	Value
SSL VPN Settings	
Name	SSL_VPN_1
Description	Description of SSL VPN policy, if required
Access Mode	<ul style="list-style-type: none"> • Full Access Mode • Web Access Mode
Full Access Settings	
Tunnel Type	Split Tunnel
Accessible Resources	172.16.16.1 (host created in Step 2)
DPD Settings	Use Global Settings (change, if required)
Idle Time out	Use Global Settings (change, if required)
Web Access Settings	
Accessible Resources	<ul style="list-style-type: none"> • Click “Enable Custom URL Access” to enable the access to the custom URLs not defined as Bookmarks. • BMG_1 (Bookmarks Group created in Step 2)
Idle Time out	Use Global Settings (change, if required)

The screenshot shows the 'Create SSL VPN Policy' configuration page. The 'SSL VPN Settings' section includes fields for Name (SSL_VPN_1), Description (New SSL VPN policy), and Access Mode (Full Access Mode and Web Access Mode checked). The 'Full Access Settings' section shows Tunnel Type (Split Tunnel), Available Hosts/Networks (172.50.50.79, SIBOLSA, 172.50.50.121), and Selected Hosts/Networks (172.16.16.1, 172.50.50.60). The 'Web Access Settings' section shows Available Bookmarks/Bookmarks Groups (Test_2) and Selected Bookmarks/Bookmarks Groups (BMG_1, SSLVPN). The 'Create' button is highlighted at the bottom.

3. Click **Create** to create SSL VPN policy

Step 4: Portal Settings

To customize SSL VPN Web Access portal view

1. Go to SSL VPN → Portal Settings
2. In General Settings select your logo or keep it as default
3. Enter Window title, login page message and home page message.
4. Select appropriate color scheme from Color Scheme section
5. Click **Save** to save to the changes

Step 5: SSL-VPN Client Installation for Full Access Mode

1. Browse <https://WANIPaddressofcyberoam:8443>. Port number will be changed as per **Step 1.c** configuration
2. Logon to SSL VPN portal with the help of username and password of SSL VPN policy member

3. Portal home page for Web Access mode will display list of available bookmarks
4. Portal home page for Full Access mode will display option to download SSL VPN client.
5. Click **Download SSL VPN Client** to download and install SSL VPN client

6. Click **Download SSL VPN Client Configuration** to download configuration of SSL VPN client.

The screenshot shows the 'SSL VPN User Portal' interface. At the top left is the Cyberoam logo, and at the top right are 'Help' and 'Logout' links. Below the logo is a welcome message: 'Welcome, cyberoam!'. The main content area is titled 'SSL VPN Client (Full Access Mode)'. It contains five numbered steps: Step 1: Download SSL VPN Client; Step 2: Run SSL VPN Client installer and install client; Step 3: Download SSL VPN Client Configuration; Step 4: Right click on the CRSSL VPN icon on the system tray and import the configuration; Step 5: Login to CRSSL VPN Client. A red box highlights steps 1, 3, and 4. An arrow points from step 1 to the text 'For Full Access Mode Users'. Another arrow points from the text 'For Web Access Mode Users' to step 4. Below the steps is a 'Configured Bookmarks' section with a table containing two entries.

Sr. No.	Bookmark Name	Bookmark URL	Service
1	SSLVPN_test	http://msn.com/	HTTP
2	Test_2	https://yahoo.com/	HTTPS

7. Right click on the CRSSL VPN icon on the system tray and import the configuration
8. Login to CRSSL VPN Client

Document version:1.0-02/07/2009