

Applicable Version: 10.00 onwards

Overview

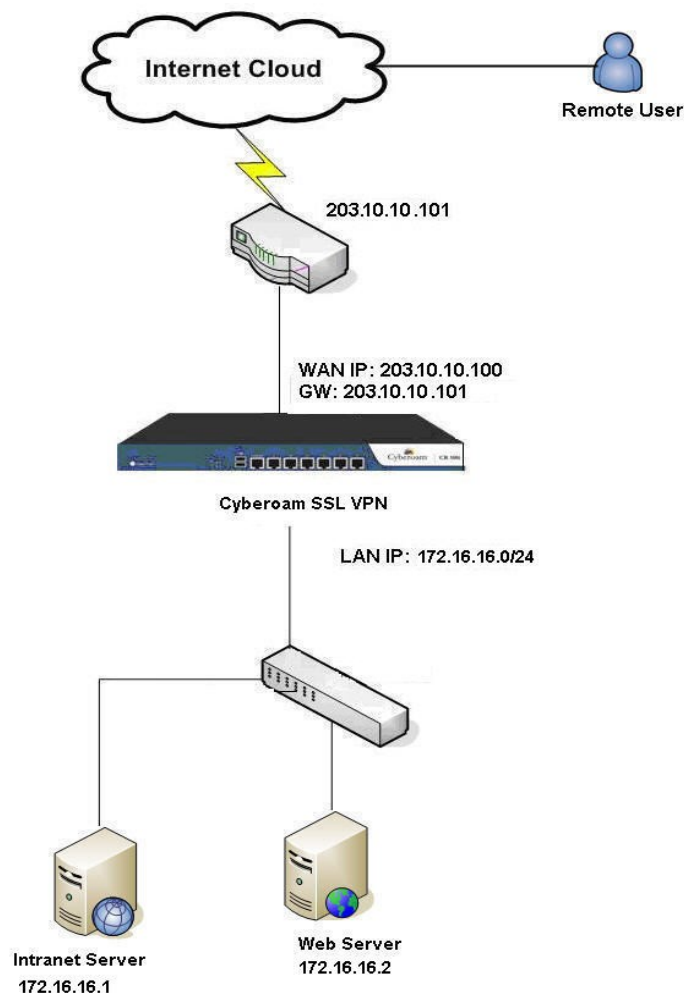
SSL (Secure Socket Layer) VPN provides simple-to-use, secure access for remote users to the corporate network from anywhere, anytime. It enables creation of point-to-point encrypted tunnels between remote user and company's internal network, requiring combination of SSL certificates and a username/password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

Cyberoam allows remote users access to the corporate network in 3 Modes:

- **Tunnel Access Mode:** User gains access through a remote SSL VPN Client.
- **Web Access Mode:** Remote users can access SSL VPN using a web browser only, i.e., clientless access.
- **Application Access Mode:** users can access web applications as well as certain enterprise applications through a web browser, i.e., clientless access.

Scenario

Configure SSL VPN in Cyberoam such that the remote user shown in the diagram below is able to access the Web and Intranet Servers in the company's internal network. The user is to have Full Access, i.e., Tunnel, Web and Application Access. The network particulars given below are used as an example throughout this article.



Network Parameters

Configuration Parameter	Value
Cyberoam WAN IP	203.10.10.100
LAN Network	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	10.10.10.1 to 10.10.10.254

Configuration

Configure SSL VPN in Cyberoam by following the steps given below. You must be logged on to the Web Admin Console as an administrator with Read-Write permission for relevant feature(s).

Step 1: Generate Default Certificate Authority

To generate the default Certificate Authority, go to **System > Certificate > Certificate Authority** and click **Default CA**.

Update the Default CA as shown below.

The screenshot shows the 'Certificate Authority' configuration page. The 'Name' field is set to 'Default'. The 'Country Name' is set to 'United States', 'State' to 'Florida', 'Locality Name' to 'Tampa', 'Organization Name' to 'Cyberoam Technologies', 'Organization Unit Name' to 'Marketing', 'Common Name' to 'Cyberoam', and 'Email Address' to 'administrator@cyberoam'. The 'CA Passphrase' field is masked with asterisks and has a 'Change CA Passphrase' link. At the bottom, there are three buttons: 'OK', 'Download', and 'Cancel'. The 'OK' button is highlighted with a red box.

Click **OK** to generate Default Certificate Authority.

Note:

If you are using an external certificate authority, you can upload the same by following steps mentioned in the article [Add an External Certificate Authority \(CA\) in Cyberoam](#).

Step 2: Create self-signed Certificate

To create a self-signed Certificate, go to **System > Certificate > Certificate** and click **Add**. Generate a Self Signed Certificate as shown below.

The screenshot shows the 'Certificate' configuration page. The 'Action' section has three radio buttons: 'Upload Certificate', 'Generate Self Signed Certificate' (which is selected), and 'Generate Certificate Signing Request (CSR)'. Below this are several input fields: 'Name' (SSLVPN_SelfSigned), 'Valid From' (2014-07-10), 'Valid Upto' (2014-08-12), 'Key length' (512), 'Key Encryption' (checkbox, disabled), and 'Certificate ID' (Email, cyber@cyberoam.com). A section titled 'Identification Attributes' contains fields for Country Name (United States), State (Florida), Locality Name (Tampa), Organization Name (Cyberoam Technologies), Organization Unit Name (Marketing), Common Name (Cyberoam_SSLVPN), and Email Address (administrator@cyberoam.com). At the bottom, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted by a red rectangle.

Click **OK** to create the certificate.

Step 3: Configure SSL Global Parameters

To set global parameters for tunnel access, go to **VPN > SSL > Tunnel Access** and configure tunnel access settings with following values:

Parameter	Value	Description
Protocol	TCP	Select default protocol for all the SSL VPN clients.
SSL Server Certificate	SSLVPN_SelfSigned	Select SSL Server certificate from the dropdown list to be used for authentication
Per User Certificate	Disabled	SSL server uses certificate to authenticate the remote client. One can use the common certificate for all the users or create individual certificate for each user
SSL Client Certificate	SSLVPN_SelfSigned	Select the SSL Client certificate from the dropdown list if you want to use common certificate for authentication
IP Lease Range	10.10.10.1 to 10.10.10.45	Specify the range of IP addresses reserved for the SSL Clients
Subnet Mask	255.255.255.0	Specify Subnet mask
Primary DNS	4.2.2.2	Specify IP address of Primary DNS
Secondary DNS	8.8.8.8	Specify IP address of Secondary DNS
Enable DPD	Enabled	Click to enable Dead Peer Detection.

Check Peer after every	60	Specify time interval in the range of 60 to 3600 seconds after which the peer should be checked for its status.
Disconnect after	300	Specify time interval in the range of 300 to 1800 seconds after which the connection should be disconnected if peer is not live.
Idle Time Out	15	Specify idle timeout. Connection will be dropped after the configured inactivity time and user will be forced to re-login.
Data Transfer Threshold	250	Once the idle timeout is reached, before dropping the connection, appliance will check the data transfer. If data transfer is more than the configured threshold, connection will be dropped.

Tunnel Access
Web Access
Policy
Bookmark
Bookmark Group
Portal

Tunnel Access Settings

Protocol* TCP UDP (Select UDP for better performance)

SSL Server Certificate*

Per User Certificate

SSL Client Certificate *

IP Lease Range* -

Subnet Mask*

Primary DNS

Secondary DNS

Primary WINS

Secondary WINS

Dead peer detection Enable

Check Peer after every* Seconds (60-3600)

Disconnect after* Seconds (300 - 18000)

Idle Timeout* Minutes (15-60)

Data Transfer Threshold* Bytes (1-65536)

To set global Idle Time for Web Access Mode, go to **VPN > SSL > Web Access** and set Idle Time as shown below.

Tunnel Access	Web Access	Policy	Bookmark	Bookmark Group	Portal
Web Access Settings					
Idle Time*		<input type="text" value="10"/>	Minutes (10-60)		
<input type="button" value="Apply"/>					

Step 4: Create Bookmarks (Applicable for Web and Application Access Mode Only)

Bookmarks are the resources whose access is available through SSL VPN Web portal. You can also create a group of bookmarks that can be configured in SSL VPN Policy. These resources are available in Web and Application Access mode only.

To create Bookmark, go to **VPN > SSL > Bookmark** and click **Add**. Create Bookmark using following parameters.

Parameter	Value	Description
Name	Telnet	Name to identify Bookmark.
Type	TELNET	Specify type of bookmark.
URL	192.168.1.120	Specify URL at which telnet sessions are allowed to remote users.

Add Bookmark	
Name*	<input type="text" value="Telnet"/>
Type*	<input type="text" value="TELNET"/> (default port 23)
URL*	<input type="text" value="192.168.1.120"/> Example: 192.168.1.1 or 192.168.1.1:221
Description	<input type="text" value="Enter Description"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Click **OK** to create Bookmark.

Similarly, create a bookmark **Intranet** of type HTTP to allow access to the internal Intranet server.

Note:

Intranet is accessible in Web as well as Application Access Mode, while Telnet is accessible in Application Access Mode.

Step 5: Configure SSL VPN Policy

To configure SSL VPN policy, go to **VPN > SSL > Policy** and click **Add**. Create policy using parameters given below.

Parameter	Value	Description
Add SSL VPN Policy		
Name	Full_Access	Name to identify the SSL VPN policy
Access Mode	Tunnel Access Mode Web Access Mode Application Access Mode	Select the access mode by clicking the appropriate option.
Tunnel Access Settings		
Tunnel Type	Split Tunnel	Select tunnel type. Tunnel type determines how the remote user's traffic will be routed.
Accessible Resources	<As required>	Select Hosts or Networks that remote user can access.
Web Access Settings		
Enable Arbitrary URL Access	Enabled	Enable to access custom URLs not defined as Bookmarks.
Accessible Resources	Intranet	Select Bookmarks/Bookmarks Group that remote user can access.
Application Access Settings		
Accessible Resources	Intranet Telnet	Select Bookmarks/Bookmarks Group that remote user can access.

Tunnel Access	Web Access	Policy	Bookmark	Bookmark Group	Portal																				
Add SSL VPN Policy																									
Name*	<input type="text" value="Full_Access"/>																								
Access Mode*	<input checked="" type="checkbox"/> Tunnel Access	<input checked="" type="checkbox"/> Web Access	<input checked="" type="checkbox"/> Application Access Mode																						
Description	<input type="text" value="Enter Description"/>																								
Tunnel Access Settings																									
Tunnel Type*	<input checked="" type="radio"/> Split Tunnel <input type="radio"/> Full Tunnel																								
Accessible Resources	<table border="1"> <thead> <tr> <th>Available Hosts/Networks</th> <th>Selected Hosts/Networks</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> 172.16.16.10</td> <td><input checked="" type="checkbox"/> 172.16.16.10</td> </tr> <tr> <td><input type="checkbox"/> #PortC</td> <td><input checked="" type="checkbox"/> 172.17.17.17/24</td> </tr> <tr> <td><input type="checkbox"/> #PortB</td> <td></td> </tr> <tr> <td><input type="checkbox"/> #PortA</td> <td></td> </tr> <tr> <td><input type="checkbox"/> #PortD</td> <td></td> </tr> <tr> <td><input type="checkbox"/> #PortE</td> <td></td> </tr> <tr> <td><input type="checkbox"/> #PortF</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.17.17.17/24</td> <td></td> </tr> <tr> <td><input type="checkbox"/> 172.16.16.0/24</td> <td></td> </tr> </tbody> </table>		Available Hosts/Networks	Selected Hosts/Networks	<input checked="" type="checkbox"/> 172.16.16.10	<input checked="" type="checkbox"/> 172.16.16.10	<input type="checkbox"/> #PortC	<input checked="" type="checkbox"/> 172.17.17.17/24	<input type="checkbox"/> #PortB		<input type="checkbox"/> #PortA		<input type="checkbox"/> #PortD		<input type="checkbox"/> #PortE		<input type="checkbox"/> #PortF		<input checked="" type="checkbox"/> 172.17.17.17/24		<input type="checkbox"/> 172.16.16.0/24				
	Available Hosts/Networks	Selected Hosts/Networks																							
<input checked="" type="checkbox"/> 172.16.16.10	<input checked="" type="checkbox"/> 172.16.16.10																								
<input type="checkbox"/> #PortC	<input checked="" type="checkbox"/> 172.17.17.17/24																								
<input type="checkbox"/> #PortB																									
<input type="checkbox"/> #PortA																									
<input type="checkbox"/> #PortD																									
<input type="checkbox"/> #PortE																									
<input type="checkbox"/> #PortF																									
<input checked="" type="checkbox"/> 172.17.17.17/24																									
<input type="checkbox"/> 172.16.16.0/24																									
<div style="border: 1px solid gray; padding: 2px;"> Advanced Settings (DPD and Idle Timeout) </div>																									
Web Access Settings																									
Accessible Resources	<input checked="" type="checkbox"/> Enable Arbitrary URL Access																								
Accessible Resources	<table border="1"> <thead> <tr> <th>Available Bookmarks/Bookmarks Groups</th> <th>Selected Bookmarks/Bookmarks Groups</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Intranet</td> <td><input checked="" type="checkbox"/> Intranet</td> </tr> </tbody> </table>		Available Bookmarks/Bookmarks Groups	Selected Bookmarks/Bookmarks Groups	<input checked="" type="checkbox"/> Intranet	<input checked="" type="checkbox"/> Intranet																			
	Available Bookmarks/Bookmarks Groups	Selected Bookmarks/Bookmarks Groups																							
<input checked="" type="checkbox"/> Intranet	<input checked="" type="checkbox"/> Intranet																								
<div style="border: 1px solid gray; padding: 2px;"> Advanced Settings (Idle Timeout) </div>																									
Application Access Settings																									
Accessible Resources																									
Accessible Resources	<table border="1"> <thead> <tr> <th>Available Bookmarks/Bookmarks Groups</th> <th>Selected Bookmarks/Bookmarks Groups</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Intranet</td> <td><input checked="" type="checkbox"/> Intranet</td> </tr> <tr> <td><input checked="" type="checkbox"/> Telnet</td> <td><input checked="" type="checkbox"/> Telnet</td> </tr> </tbody> </table>		Available Bookmarks/Bookmarks Groups	Selected Bookmarks/Bookmarks Groups	<input checked="" type="checkbox"/> Intranet	<input checked="" type="checkbox"/> Intranet	<input checked="" type="checkbox"/> Telnet	<input checked="" type="checkbox"/> Telnet																	
	Available Bookmarks/Bookmarks Groups	Selected Bookmarks/Bookmarks Groups																							
<input checked="" type="checkbox"/> Intranet	<input checked="" type="checkbox"/> Intranet																								
<input checked="" type="checkbox"/> Telnet	<input checked="" type="checkbox"/> Telnet																								
<div style="border: 1px solid gray; padding: 2px;"> Advanced Settings (Idle Timeout) </div>																									
<input type="button" value="Apply"/> <input type="button" value="Add Policy Member(s)"/> <input type="button" value="Manage Policy Member(s)"/> <input type="button" value="Cancel"/>																									

Step 6: Apply SSL VPN Policy on User

To apply SSL VPN policy on user, follow the steps given below.

Go to **Identity > Users > User** and select the user to which policy is to be applied. Here we have applied it on user John Smith. Under Policies section, select Full_Access for SSL VPN as shown below.

Users	Clientless Users
Username*	john.smith
Name*	John Smith
Password*	***** Change Password
User Type*	<input checked="" type="radio"/> User <input type="radio"/> Administrator
Profile*	Profile
Email*	john.smith@cyberoam.com <small>Use a comma to separate multiple Email Addresses.</small>
Internet Usage Time	00:00 (HH:MM)
Policies	
Group*	Open Group
Web Filter*	Allow All
Application Filter*	Allow All
Surfing Quota*	Unlimited Internet Access
Access Time*	Allowed all the time
Data Transfer	None
QoS	None
SSL VPN*	Full_Access
L2TP*	<input type="radio"/> Enable <input checked="" type="radio"/> Disable IP Address <input type="text"/>
PPTP*	<input checked="" type="radio"/> Enable <input type="radio"/> Disable IP Address <input type="text"/>
Quarantine Digest*	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Simultaneous Logins*	<input type="checkbox"/> Unlimited <input type="text" value="1"/> (1 - 99)
MAC Binding*	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC address List	<input type="text"/> <small>Use a comma or a new line to separate multiple MAC Addresses. Example: 11:11:11:11:11:11, 22:22:22:22:22:22</small>
Login Restriction*	<input type="radio"/> Any Node <input checked="" type="radio"/> User Group node(s) <input type="radio"/> Selected Nodes <input type="radio"/> Node Range
<input type="button" value="OK"/> <input type="button" value="Reset User Accounting"/> <input type="button" value="View Usage"/> <input type="button" value="Cancel"/>	

Click **OK** to update the user's SSL VPN Policy.

Note:

Make sure that Firewall Rules allowing traffic from LAN to VPN and vice versa are present. If they are not present, create them manually. They are necessary for the VPN connections to function properly.

Step 7: Download and Install SSL VPN Client at Remote End

Remote users can login to Cyberoam SSL VPN Portal by browsing to <https://<WAN IP address of Cyberoam:port>> and logging in.

Note:

Use default port: 8443 unless customized. Access is available only to those users who have been assigned an SSL VPN policy.



Welcome to the Cyberoam SSL VPN Portal!

Username:


Password:

Language: ▼

[Login](#)

User is directed to the Main Page which displays Tunnel, Web or Application Access Mode section according to policy applied on user.

[Help](#) [Logout](#)



SSL VPN User Portal

Welcome, john.smith !

SSL VPN Client (Tunnel access mode) ▶

Download

- [Installer](#)
- [Client Configuration for Windows - IPV4 , IPV6](#)
- [Client Configuration for MAC Tunnelblick - IPV4 , IPV6](#)



Web access mode

Enter URL [Go](#)

Configured Bookmarks

Sr. No.	Bookmark Name	Bookmark URL	Service
1	Google	www.google.com	HTTPS

For Tunnel Access, user needs to access internal resources through an SSL VPN Client.

- Download the SSL VPN client from the Cyberoam website by clicking “**Installer**”.
- Download the client configuration from the Portal.
- Install the client on the remote user’s system. On complete installation, the CrSSL Client icon  appears in the system tray.
- Right-click the Client icon  and click **Import**. Import the SSL VPN configuration downloaded from the Portal.
- Login to the Client and access the company’s internal network through SSL VPN.

For Web and Application Access, user can access internal resources using web browser, i.e., clientless access. In this, user needs to browse to <https://<WAN IP address of Cyberoam:port>> and login.

Document Version: 3.1 – 24 June, 2015