SOPHOS
Security made simple.

Pocket Guide

Establish Site-to-Site VPN Connection using Digital Certificates

For Customers with Sophos Firewall

Document Date: November 2016

Contents

Overview

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.

Just like a passport, a digital certificate provides identifying information, is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

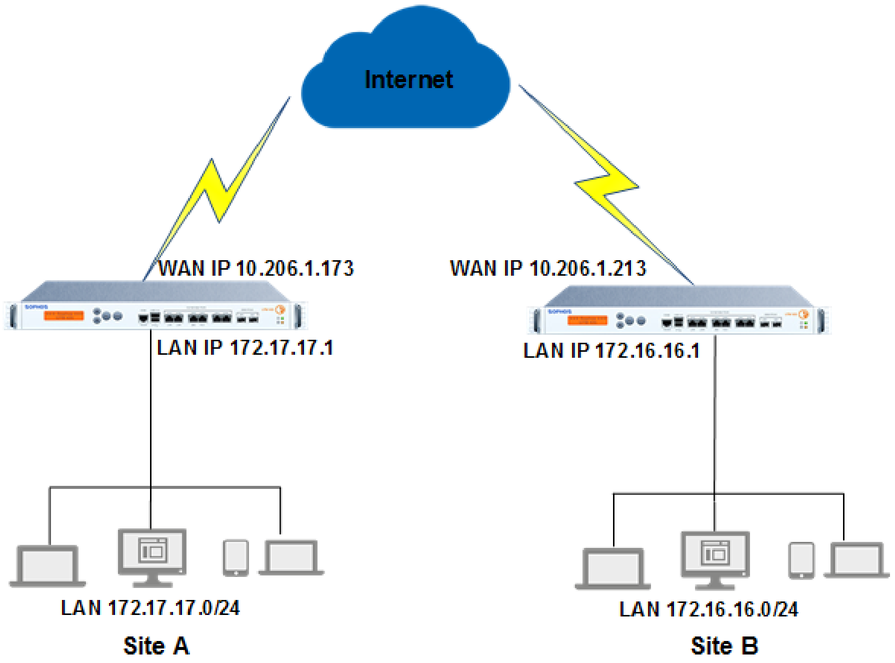
Prerequisites

Exchange Certificate Authority (CA) and Digital Certificates between a Head Office (HO) and Branch Office (BO) and, then, configure and establish an IPsec connection between them.

Scenario

Configure a site-to-site IPsec VPN connection between Site A and Site B by following the steps given below. In this article, we have used the following parameters to create the VPN connection.

Network Parameters	
HO Network details	Local WAN IP address – 10.206.1.173
	Local LAN address –172.17.17.0/24
BO Network details	Remote WAN IP address – 10.206.1.213
	Remote LAN Network –172.16.16.0/24



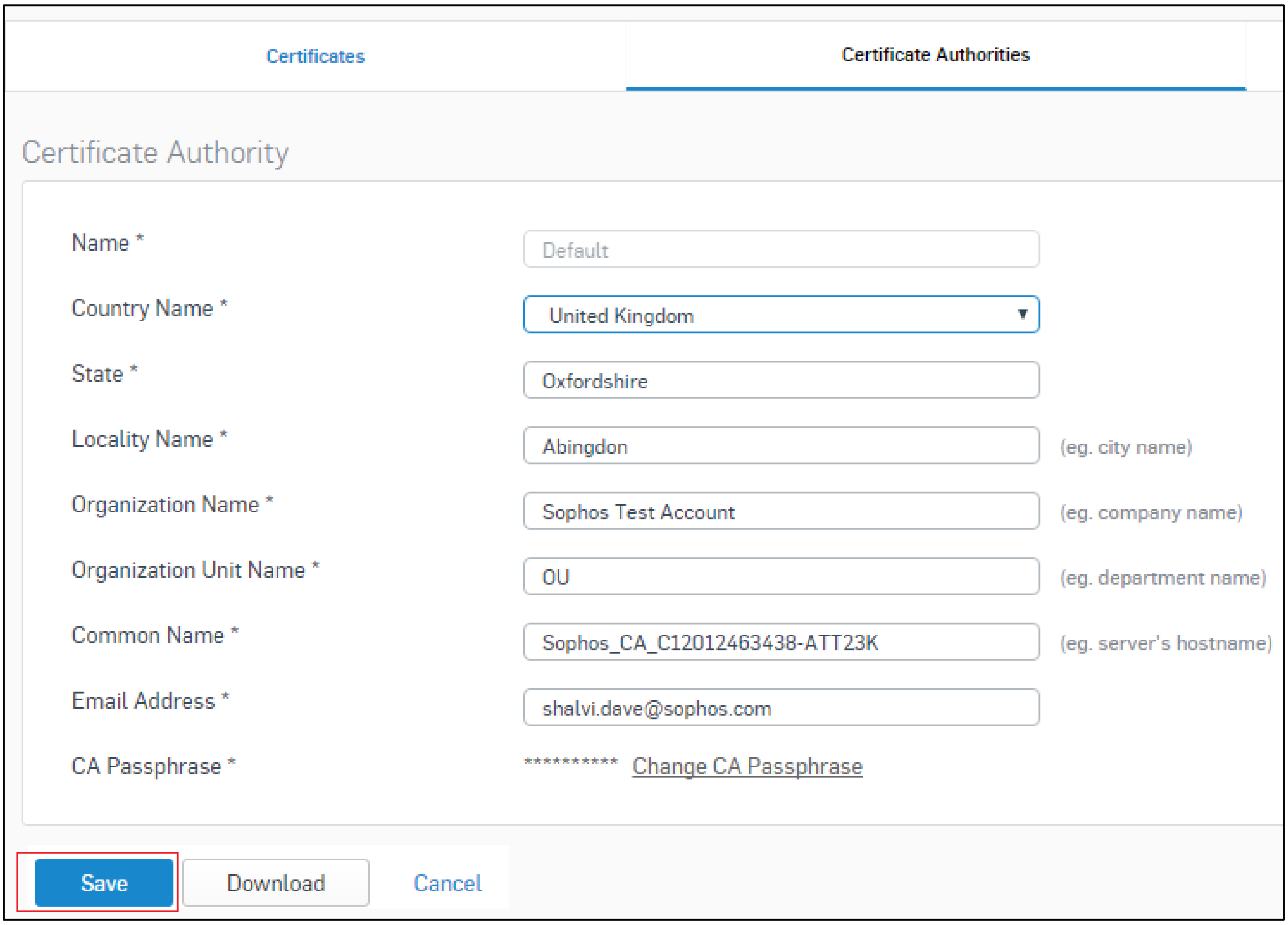
Configuration

You must be logged on to the Admin Console of both HO and BO SF as an administrator with Read-Write permission for relevant feature(s).

Step 1: Upload HO Sophos Firewall's Default CA to BO Sophos Firewall (SF)

Head Office

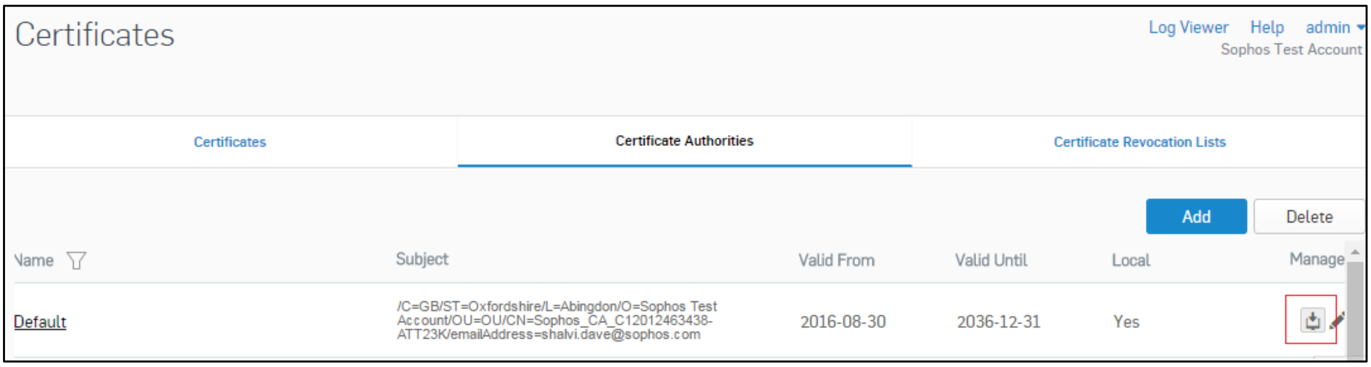
Go to **System** > **Certificates** > **Certificate Authorities** and select **Default** CA. Specify the details of the CA, as shown below and click **Save**.



Certificate Authority

Name *	Default	
Country Name *	United Kingdom ▾	
State *	Oxfordshire	
Locality Name *	Abingdon	(eg. city name)
Organization Name *	Sophos Test Account	(eg. company name)
Organization Unit Name *	OU	(eg. department name)
Common Name *	Sophos_CA_C12012463438-ATT23K	(eg. server's hostname)
Email Address *	shalvi.dave@sophos.com	
CA Passphrase *	********** Change CA Passphrase	

Once CA is generated, download the CA to your local computer by clicking the **Download Button.**



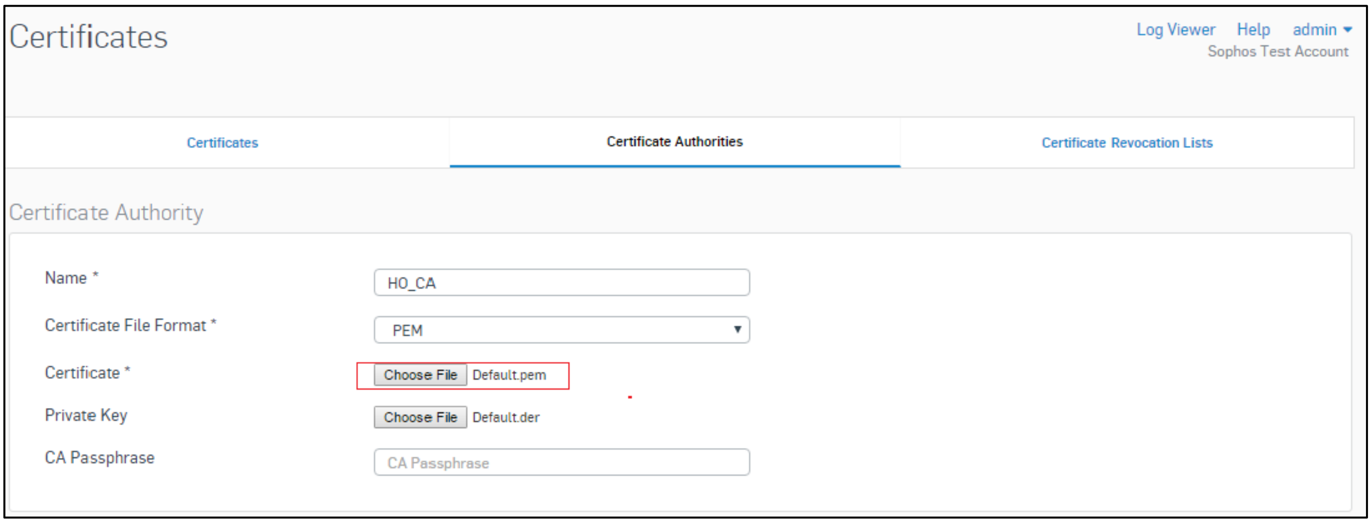
Name	Subject	Valid From	Valid Until	Local	Manage
Default	/C=GB/ST=Oxfordshire/L=Abingdon/O=Sophos Test Account/OU=OU/CN=Sophos_CA_C12012463438-ATT23K/emailAddress=shalvi.dave@sophos.com	2016-08-30	2036-12-31	Yes	

A file named local_certificate_authority.tar.gz is downloaded. Store the uncompressed file. The file contains the CA Root Certificate in two file formats:

- Default.pem (PEM File)
- Default.der (Security Certificate)

Branch Office

Upload the CA Certificates (downloaded from HO) to BO SF. To upload CA, go to **System > Certificates > Certificate Authorities** and click **Add**. Upload the CA Root Certificate in either PEM or DER format.



Name * HO_CA

Certificate File Format * PEM

Certificate * Choose File Default.pem

Private Key Choose File Default.der

CA Passphrase CA Passphrase

Click **Save** to save the HO Default CA in BO Sophos Firewall.

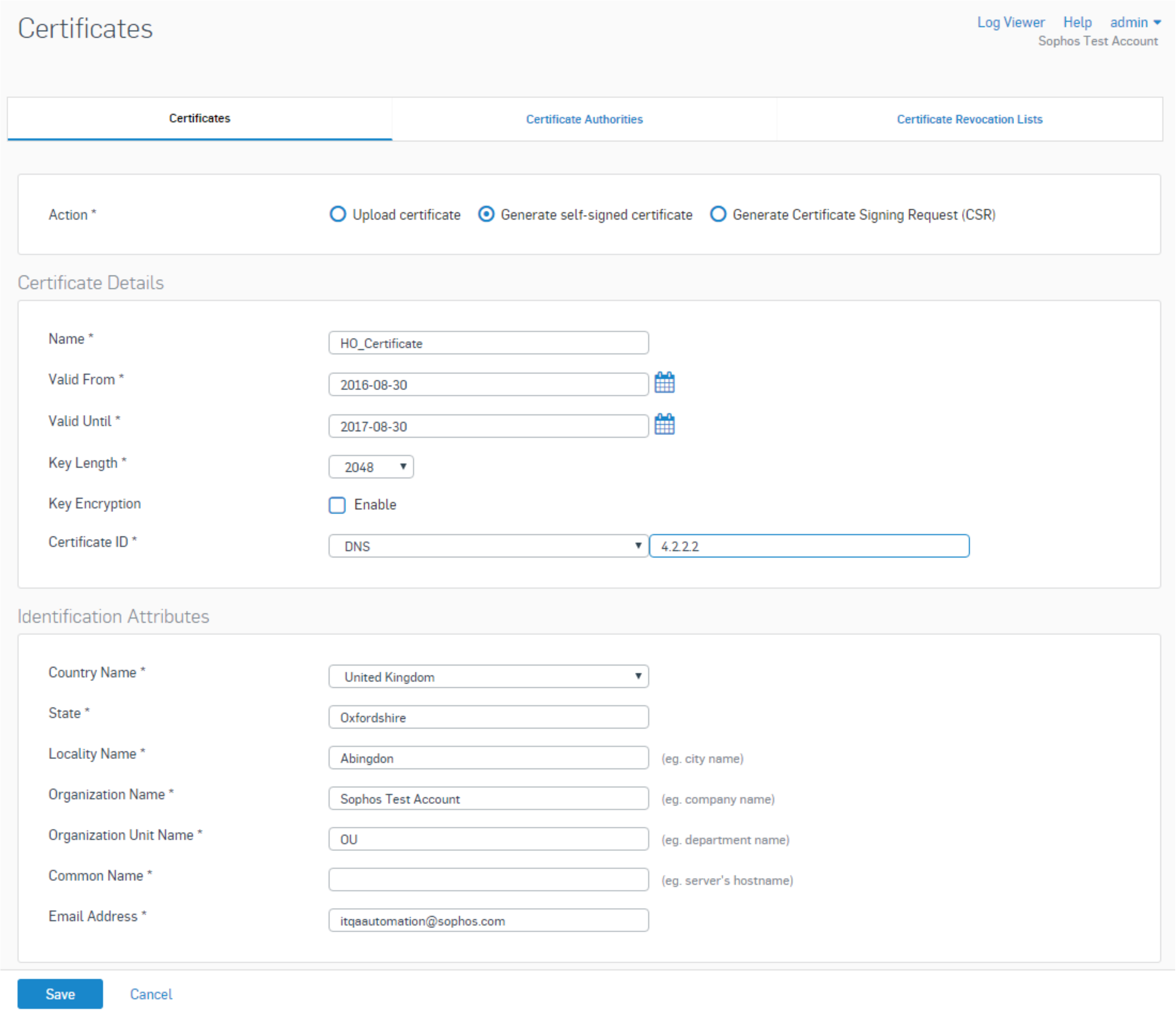
Step 2: Upload BO Sophos Firewall’s Default CA to HO Sophos Firewall

Configure and download the Default CA in BO SF and upload it on HO SF using similar steps as shown in step 1.

Step 3: Upload HO Sophos Firewall’s Digital Certificate to BO Sophos Firewall

Head Office

Create a Self-Signed Certificate in HO SF. Go to **System > Certificates > Certificates** and click **Add** to create a new certificate. Select **Generate Self Signed Certificate** and specify the details as shown below.



Certificates

Action * ○ Upload certificate ● Generate self-signed certificate ○ Generate Certificate Signing Request (CSR)

Certificate Details

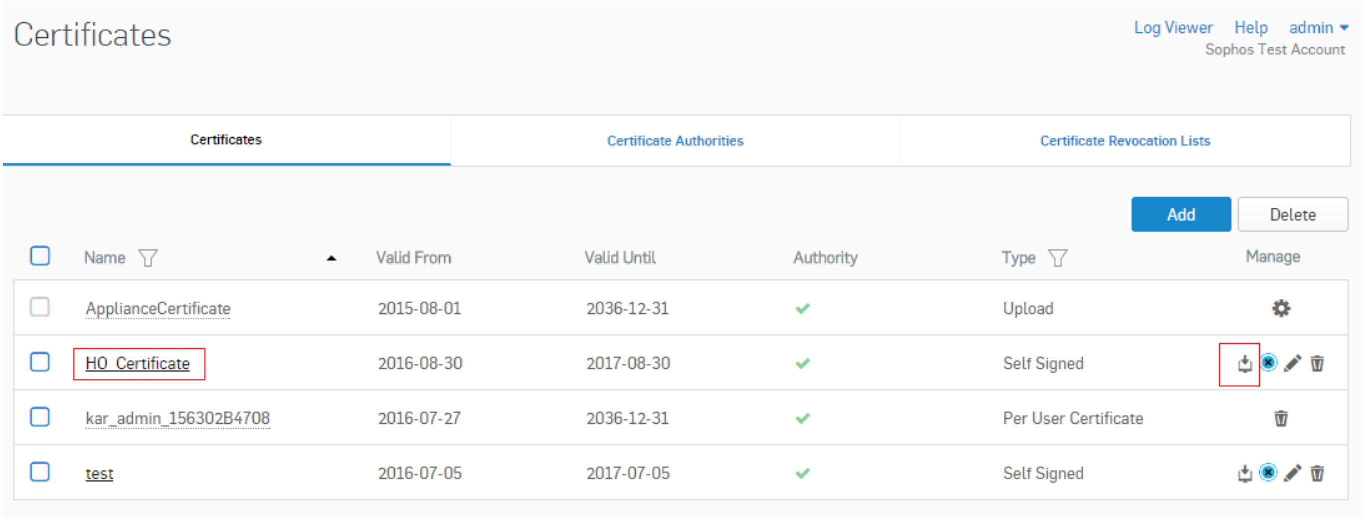
Name *	HO_Certificate
Valid From *	2016-08-30
Valid Until *	2017-08-30
Key Length *	2048
Key Encryption	□ Enable
Certificate ID *	DNS 4.2.2.2

Identification Attributes

Country Name *	United Kingdom	
State *	Oxfordshire	
Locality Name *	Abingdon	(eg. city name)
Organization Name *	Sophos Test Account	(eg. company name)
Organization Unit Name *	OU	(eg. department name)
Common Name *		(eg. server's hostname)
Email Address *	itqaautomation@sophos.com	

Click **Save** to save certificate.

Once Certificate is generated, download it to your local computer by clicking the **Download Icon** against it.



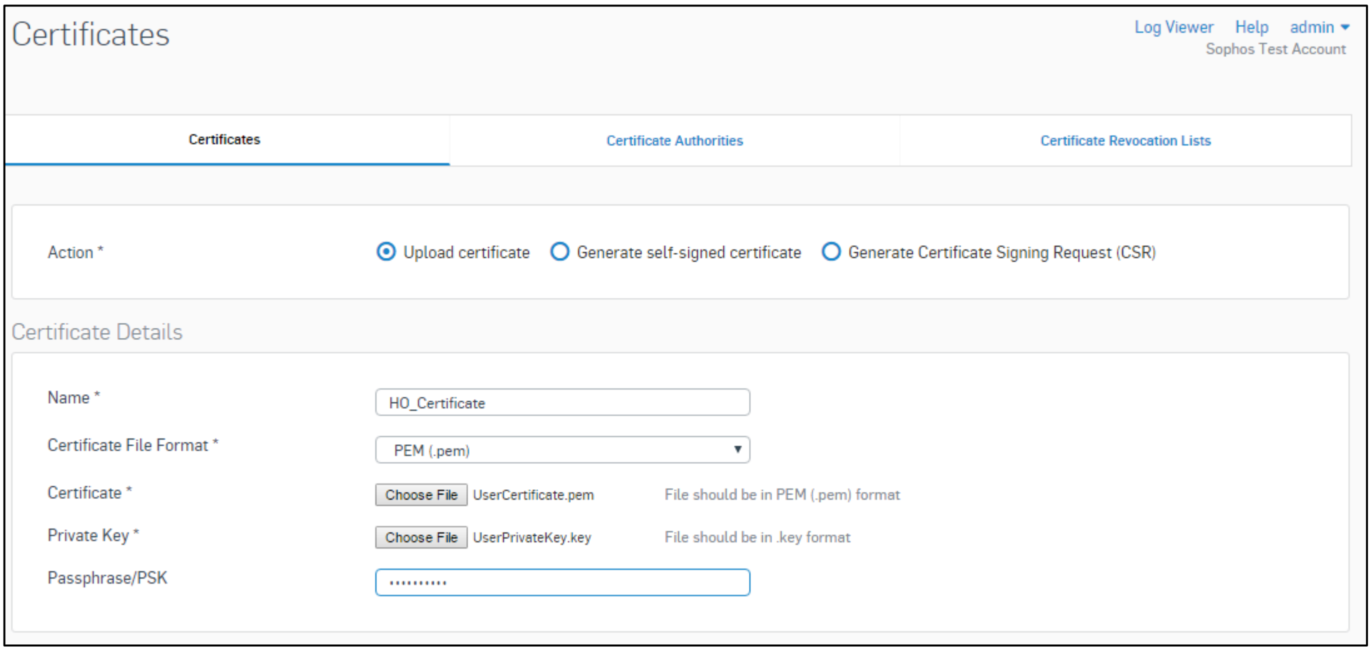
□	Name	Valid From	Valid Until	Authority	Type	Manage
□	ApplianceCertificate	2015-08-01	2036-12-31	✓	Upload	⚙
□	HO_Certificate	2016-08-30	2017-08-30	✓	Self Signed	
□	kar_admin_156302B4708	2016-07-27	2036-12-31	✓	Per User Certificate	
□	test	2016-07-05	2017-07-05	✓	Self Signed	

A file named HO_Certificate.tar.gz is downloaded. Store the uncompressed file. The file contains the following certificate files:

- UserPrivateKey.key (KEY File)
- UserCertificate.pem (PEM File)
- RootCertificate (PEM File)
- Password.txt (Passphrase if Key Encryption is enabled)
- HO_Certificate.p12 (Personal Information Exchange)

Branch Office

Upload the Certificate (downloaded from HO Sophos Firewall) to BO Sophos Firewall. To upload certificate, go to **System > Certificates > Certificates** and click **Add**. Select **Certificate** as **UserCertificate.pem**, **Private Key** as **UserPrivateKey.pem** and specify the **Passphrase**.



Certificates

Action * ● Upload certificate ○ Generate self-signed certificate ○ Generate Certificate Signing Request (CSR)

Certificate Details

Name * HO_Certificate

Certificate File Format * PEM (.pem)

Certificate * Choose File UserCertificate.pem File should be in PEM (.pem) format

Private Key * Choose File UserPrivateKey.key File should be in .key format

Passphrase/PSK ••••••••••

Click **Save** to save the certificate.

Step 4: Upload BO Sophos Firewall’s Digital Certificate to HO Sophos Firewall

Configure and download the Self-signed certificate in BO SF and upload it on HO SF using similar steps as shown in step 3.

Step 5: Configure IPsec Connection

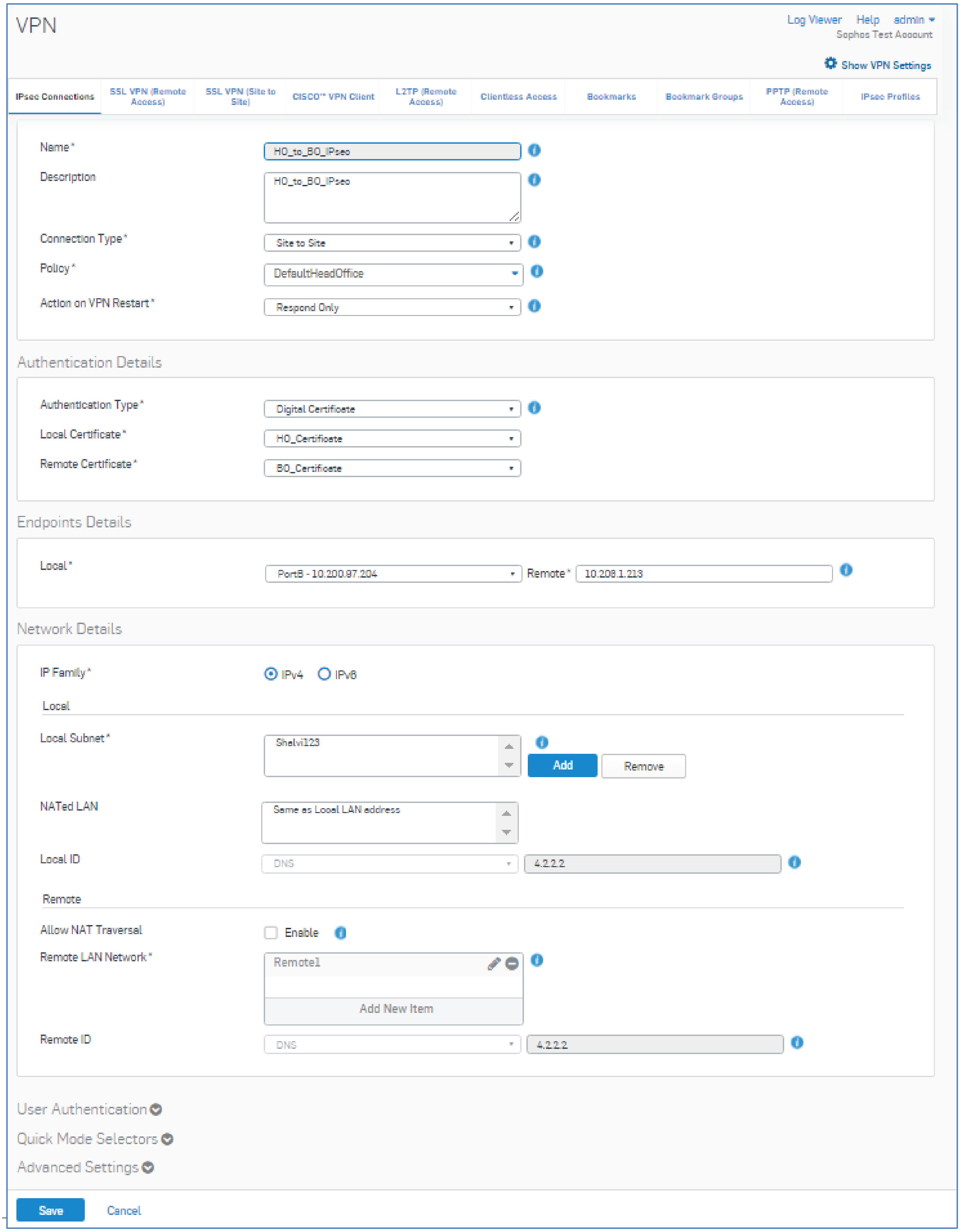
Head office

Implement the following steps on HO Sophos Firewall.

1. To create a new IPsec connection, go to **Configure > VPN > IPsec Connections** and click **Add**. Create the connection using the following parameters.

Parameters	Value	Description
General Settings		
Name	HO_to_BO_IPsec	Specify a unique name to identify IPsec Connection.
Connection Type	SitetoSite	Select SitetoSite.
Policy	DefaultHeadOffice	Select policy to be used for connection. Policy can also be added by clicking “Create New” link.

Parameters	Value	Description
Action on VPN Restart	Respond Only	Select the Action to be taken on the connection when VPN services or Device restarts. Available Options - Respond Only: Keeps connection ready to respond to any incoming request. - Initiate: Activates connection on system/service start so that the connection can be established whenever required. - Disable: Keeps connection disabled till the user activates.
Authentication Details		
Authentication Type	Digital Certificate	Select Authentication Type. Authentication of user depends on the type of connection.
Local Certificate	HO_Certificate	Select the local certificate that should be used for authentication by the device.
Remote Certificate	BO_Certificate	Select the remote certificate that should be used for authentication by remote peer.
Endpoint Details		
Local	PortB-10.206.1.173	Select Local WAN port from the list. IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.
Remote	10.206.1.213	Specify an IP Address or domain name of the remote peer. Click Add icon ⊞ against the option “Remote” to add new endpoint pairs or click Remove icon ⊟ to remove the endpoint pairs.
Network Details		
IP Family	IPv4	Select IP family to configure IPsec VPN tunnels with mixed IP families. Available Options: - IPv4 - IPv6 By default, IPv4 will be selected. Four types of IPsec VPN tunnels can be created: 4 in 4 (IPv4 subnets with IPv4 gateway) 6 in 6 (IPv6 subnets with IPv6 gateway) 4 in 6 (IPv4 subnets with IPv6 gateway) 6 in 4 (IPv6 subnets with IPv4 gateway)
Local Subnet	172.17.17.0/24	Select Local LAN Address of Site A. Add and Remove LAN Address using Add Button and Remove Button.
Remote LAN Network	172.16.16.0/24	Select IP Addresses and netmask of remote network in Site B which is allowed to connect to the Device server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.



Name * HO_to_BO_IPsec

Description HO_to_BO_IPsec

Connection Type * Site to Site

Policy * DefaultHeadOffice

Action on VPN Restart * Respond Only

Authentication Details

Authentication Type * Digital Certificate

Local Certificate * HO_Certificate

Remote Certificate * BO_Certificate

Endpoints Details

Local * PortB - 10.200.97.204 Remote * 10.208.1.213

Network Details

IP Family * ● IPv4 ○ IPv6

Local

Local Subnet * Shelvi123

NATed LAN Same as Local LAN address

Local ID DNS 4.2.2.2

Remote

Allow NAT Traversal □ Enable

Remote LAN Network * Remote1

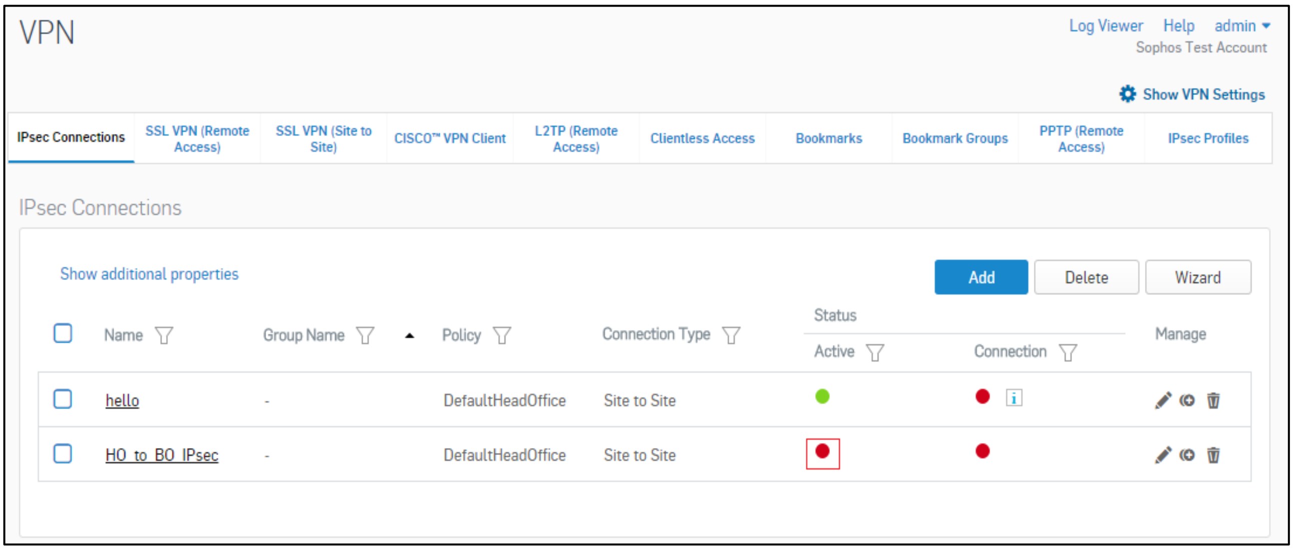
Remote ID DNS 4.2.2.2

User Authentication

Quick Mode Selectors

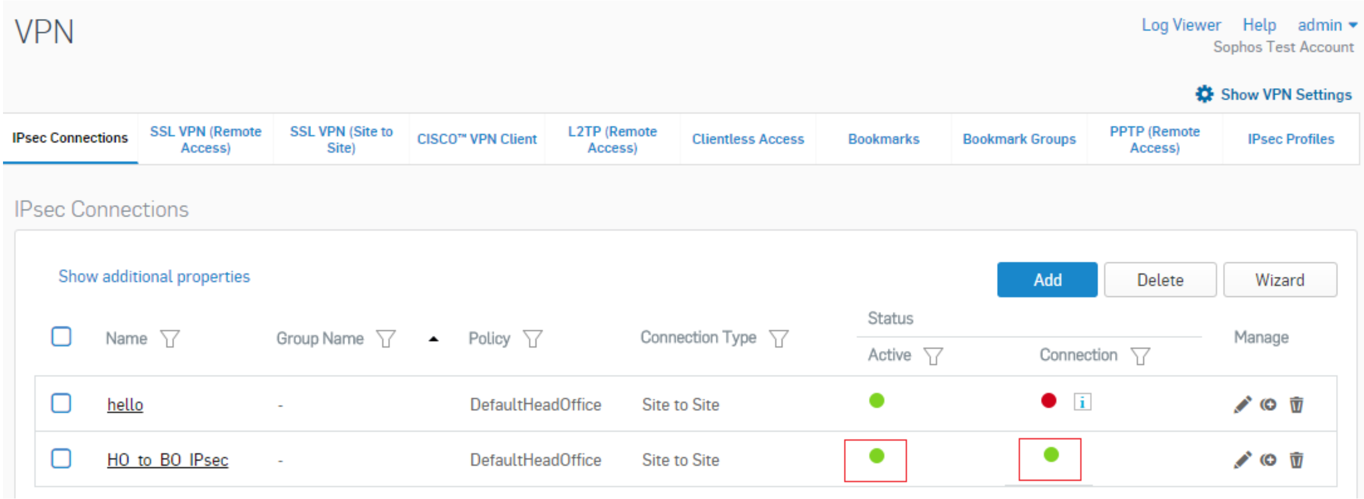
Advanced Settings

2. Click **Save** to create IPsec connection. On clicking Save, the following screen is displayed showing the connection created above.



□	Name	Group Name	Policy	Connection Type	Status		Manage
					Active	Connection	
□	hello	-	DefaultHeadOffice	Site to Site	●	●	
□	HO_to_BO_IPsec	-	DefaultHeadOffice	Site to Site	●	●	

3. Click ● under Status: Active and Connection, to activate the connection.



□	Name	Group Name	Policy	Connection Type	Status		Manage
					Active	Connection	
□	hello	-	DefaultHeadOffice	Site to Site	●	●	
□	HO_to_BO_IPsec	-	DefaultHeadOffice	Site to Site	●	●	

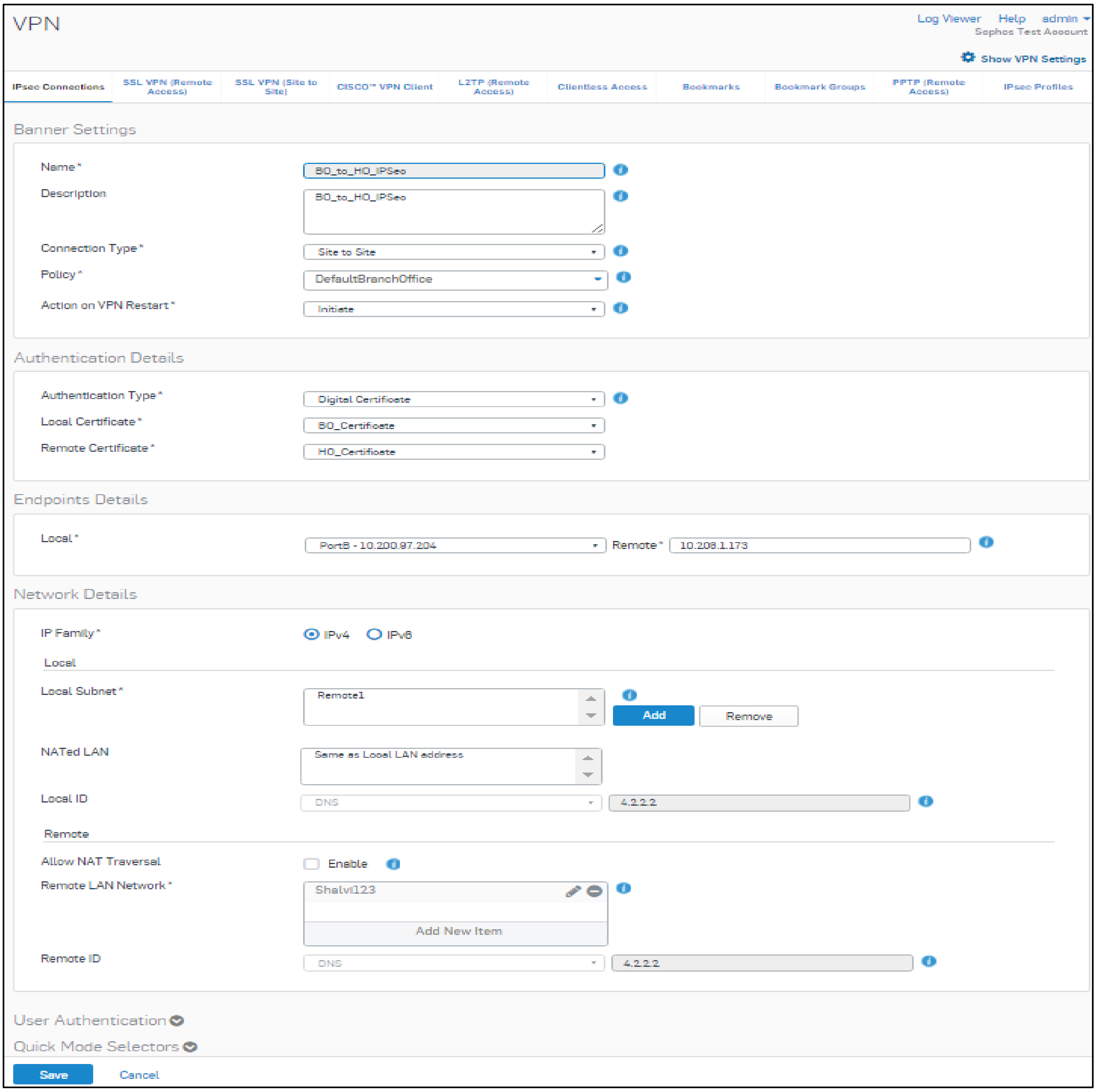
Branch Office

Implement the following steps on BO Sophos Firewall

1. To create a new IPsec connection, go to **Configure >VPN > IPsec Connections** and click **Add**. Create the connection using the following parameters.

Parameters	Value	Description
General Settings		
Name	BO_to_HO_IPSec	Specify a unique name to identify IPsec Connection.
Connection Type	SitetoSite	Select SitetoSite.
Policy	DefaultBranchOffice	Select policy to be used for connection. Policy can also be added by clicking "Create New" link.
Action on VPN Restart	Initiate	Select the Action to be taken on the connection when VPN services or Device restarts. Available Options - Respond Only: Keeps connection ready to respond to any incoming request. - Initiate: Activates connection on system/service start so that the connection can be established whenever required. - Disable: Keeps connection disabled till the user activates.
Authentication Details		
Authentication Type	Digital Certificate	Select Authentication Type. Authentication of user depends on the type of connection.
Local Certificate	BOCertificate	Select the local certificate that should be used for authentication by the device.
Remote Certificate	HOCertificate	Select the remote certificate that should be used for authentication by remote peer.
Endpoint Details		
Local	PortB-10.206.1.213	Select Local WAN port from the list. IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.
Remote	10.206.1.173	Specify an IP Address or domain name of the remote peer. Click Add icon ⊞ against the option "Remote" to add new endpoint pairs or click Remove icon ⊟ to remove the endpoint pairs.
Network Details		
IP Family	IPv4	Select IP family to configure IPsec VPN tunnels with mixed IP families. Available Options: - IPv4 - IPv6 By default, IPv4 will be selected. Four types of IPsec VPN tunnels can be created: 4 in 4 (IPv4 subnets with IPv4 gateway) 6 in 6 (IPv6 subnets with IPv6 gateway) 4 in 6 (IPv4 subnets with IPv6 gateway) 6 in 4 (IPv6 subnets with IPv4 gateway)

Parameters	Value	Description
Local Subnet	172.16.16.0/24	Select Local LAN Address of Site B. Add and Remove LAN Address using Add Button and Remove Button.
Remote LAN Network	172.17.17.0/24	Select IP Addresses and netmask of remote network in Site A which is allowed to connect to the Device server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.



VPN

Log Viewer Help admin
Sophos Test Account

Show VPN Settings

IPsec Connections | SSL VPN (Remote Access) | SSL VPN (Site to Site) | CISCO™ VPN Client | L2TP (Remote Access) | Clientless Access | Bookmarks | Bookmark Groups | PPTP (Remote Access) | IPsec Profiles

Banner Settings

Name*: BO_to_HO_IPSec

Description: BO_to_HO_IPSec

Connection Type*: Site to Site

Policy*: DefaultBranchOffice

Action on VPN Restart*: Initiate

Authentication Details

Authentication Type*: Digital Certificate

Local Certificate*: BO_Certificate

Remote Certificate*: HO_Certificate

Endpoints Details

Local*: Port8 - 10.200.97.204 Remote*: 10.208.1.173

Network Details

IP Family*: ● IPv4 ○ IPv6

Local

Local Subnet*: Remote1 Add Remove

NATed LAN: Same as Local LAN address

Local ID: DNS 4.2.2.2

Remote

Allow NAT Traversal: □ Enable

Remote LAN Network*: Shalvi123
Add New Item

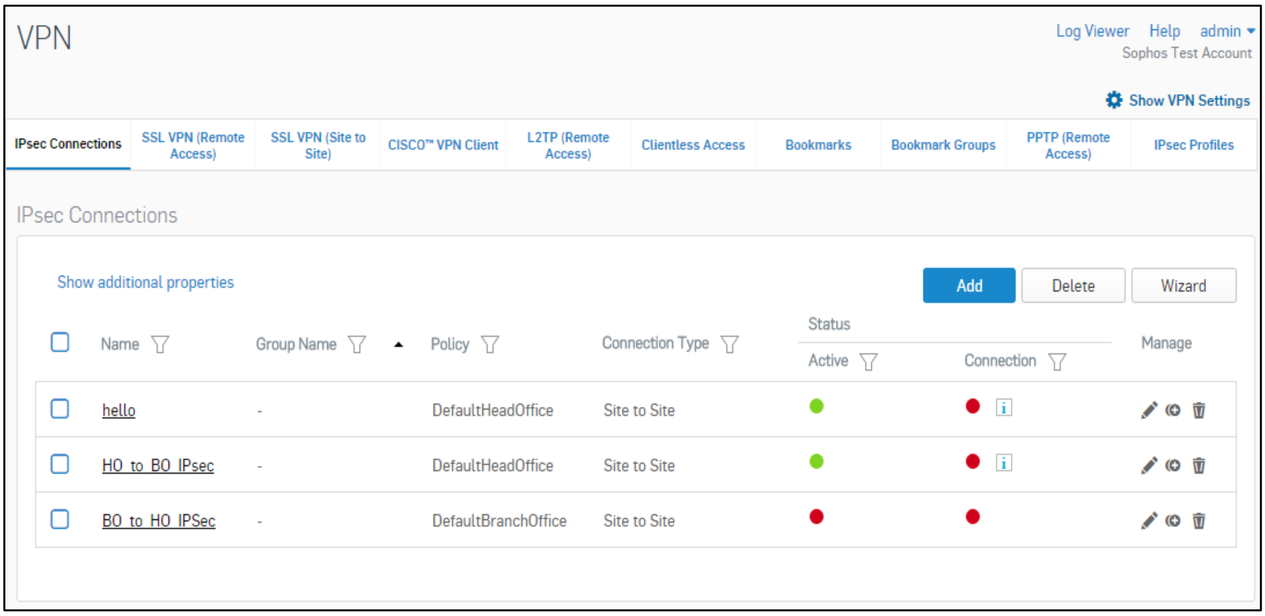
Remote ID: DNS 4.2.2.2

User Authentication

Quick Mode Selectors

Save Cancel

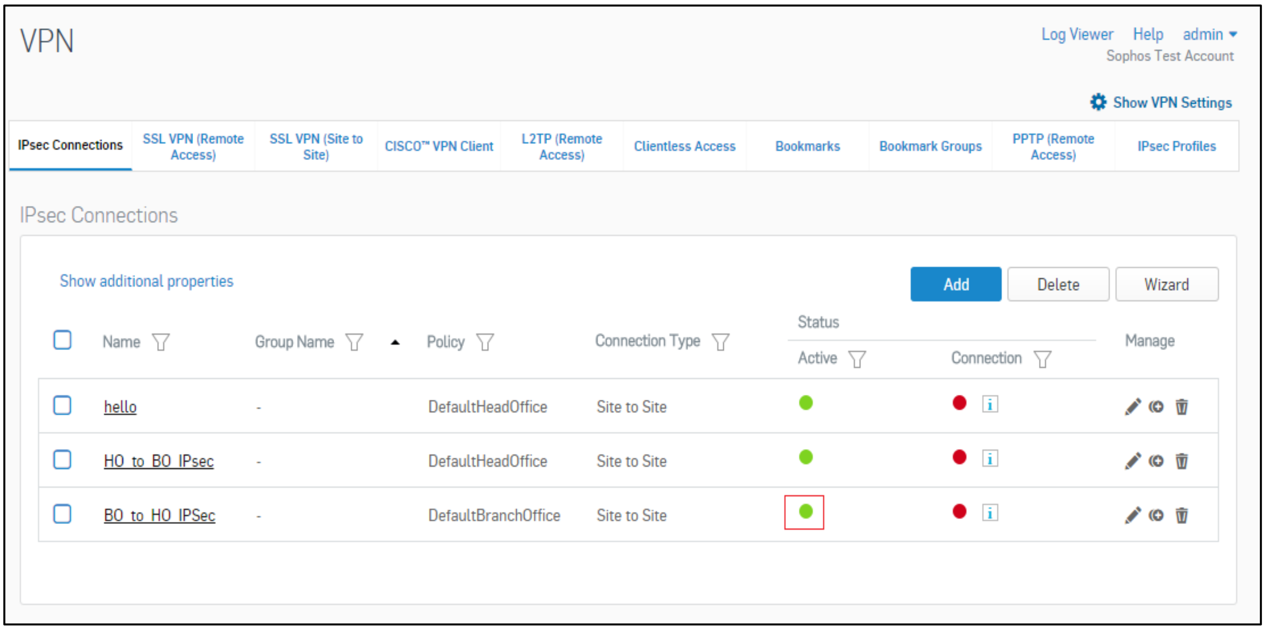
4. Click **Save** to create IPsec connection. On clicking Save, the following screen is displayed showing the connection created above.



IPsec Connections

□	Name	Group Name	Policy	Connection Type	Status: Active	Status: Connection	Manage
□	hello	-	DefaultHeadOffice	Site to Site	🟢	🔴	
□	HO_to_BO_IPsec	-	DefaultHeadOffice	Site to Site	🟢	🔴	
□	BO_to_HO_IPSec	-	DefaultBranchOffice	Site to Site	🔴	🔴	

Click ● under Status (Active) and Status (Connection).



IPsec Connections

□	Name	Group Name	Policy	Connection Type	Status: Active	Status: Connection	Manage
□	hello	-	DefaultHeadOffice	Site to Site	🟢	🔴	
□	HO_to_BO_IPsec	-	DefaultHeadOffice	Site to Site	🟢	🔴	
□	BO_to_HO_IPSec	-	DefaultBranchOffice	Site to Site	🟢	🔴	

The above configuration establishes an IPsec connection between two sites.

Note:

- Make sure that Security Policies that allow LAN to VPN and VPN to LAN traffic are configured.
- In a Head Office and Branch Office setup, usually the Branch Office acts as the tunnel initiator and Head Office acts as a responder due to following reasons:
  - Since Branch Office or other Remote Sites have dynamic IPs, Head Office is not able to initiate the connection.
  - As there can be many Branch Offices, to reduce the load on Head Office it is a good practice that Branch Offices retries the connection instead of the Head Office retrying all the branch office connections.

Copyright Notice