SOPHOS
Security made simple.

Pocket Guide

Establish Site-to-Site VPN Connection using Preshared Key

For Customers with Sophos Firewall

Document Date: November 2016

Contents

Overview

IPsec is an end-to-end security technology operating in the Internet Layer of the Internet Protocol Suite. It is used in protecting data transfer between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

The **IPsec VPN** feature in Sophos Firewall (SF) offers site-to-site VPN with cost-effective site-to-site remote connectivity, eliminating the need for expensive private remote access technologies like leased lines, Asynchronous Transfer Mode (ATM) and Frame Relay. This article describes a detailed configuration example that demonstrates how to set up a site-to-site IPsec VPN connection between the two networks using preshared key to authenticate VPN peers.

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.

Site A (Local) Network Details:

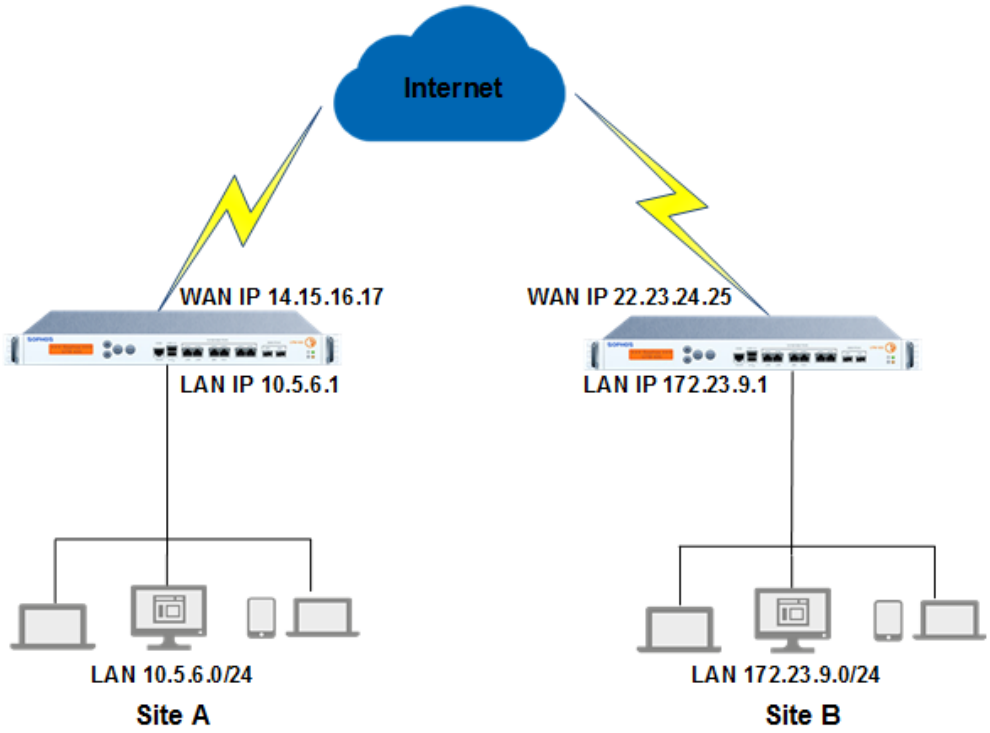
WAN IP Address - 14.15.16.17

LAN - 10.5.6.0/24

Site B (Remote) Network Details:

WAN IP Address - 22.23.24.25

LAN - 172.23.9.0/24



Site A Configuration

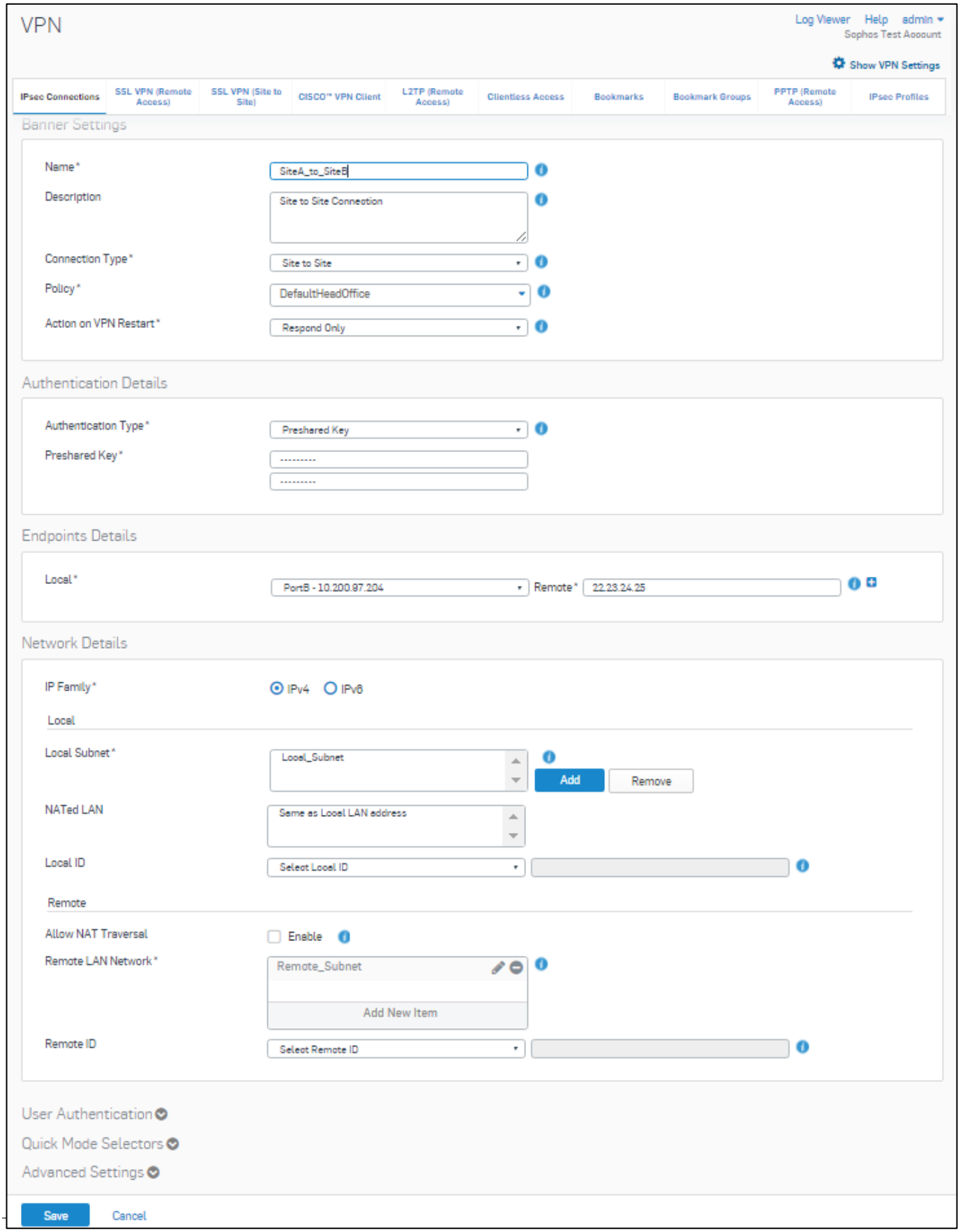
You must be logged on to the Admin Console using Device Access Profile which has read/write administrative rights over relevant features.

Step 1: Create IPsec Connection

Go to **Configure > VPN** and click **Add** under **IPsec Connections**. Create a Connection as per following parameters.

Parameters	Value	Description
General Settings		
Name	SiteA_to_SiteB	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.
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	Preshared Key	Select Authentication Type. Authentication of user depends on the type of connection.
Preshared Key	*<Key>*	Enter the Preshared Key. The same is to be used in the Site B SF Device.
Endpoint Details		
Local	PortB-14.15.16.17	Select Local WAN port from the list. IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.
Remote	22.23.24.25	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		

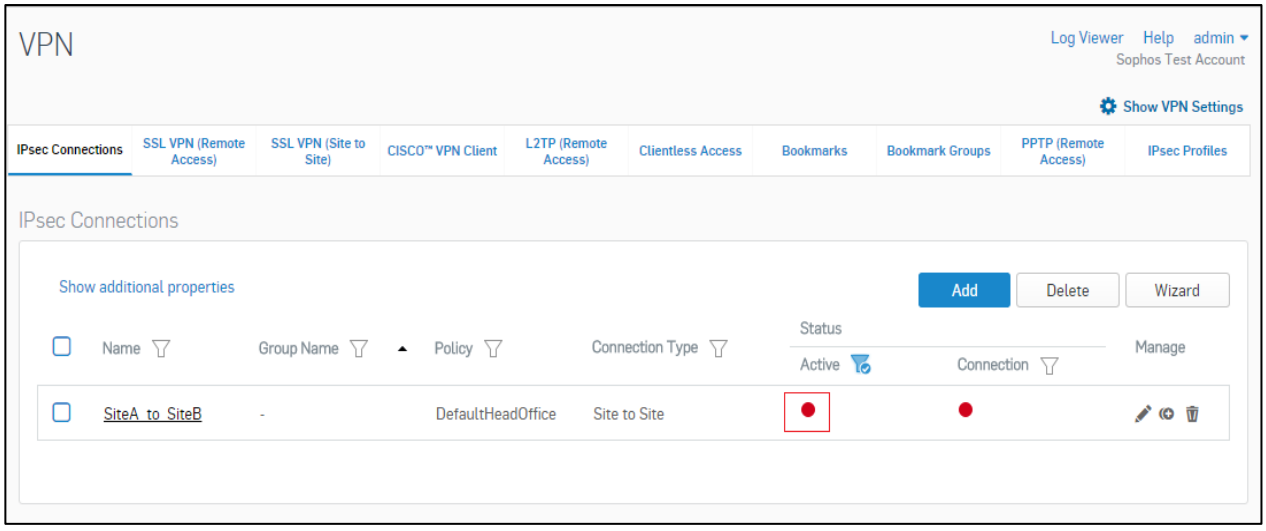
IP Family	IPv4	Select IP family to configure IPsec VPN tunnels with mixed IP families. Available Options: - IPv4 - IPv6 By default, IPv4 will be selected. Four types of IPsec VPN tunnels can be created: 4 in 4 (IPv4 subnets with IPv4 gateway) 6 in 6 (IPv6 subnets with IPv6 gateway) 4 in 6 (IPv4 subnets with IPv6 gateway) 6 in 4 (IPv6 subnets with IPv4 gateway)
Local Subnet	10.5.6.0/24	Select Local LAN Address of Site A. Add and Remove LAN Address using Add Button and Remove Button.
Remote LAN Network	172.23.9.0/24	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.


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 *
SiteA_to_SiteB
Description
Site to Site Connection
Connection Type *
Site to Site
Policy *
DefaultHeadOffice
Action on VPN Restart *
Respond Only
Authentication Details
Authentication Type *
Preshared Key
Preshared Key *
Endpoints Details
Local *
PortB - 10.200.97.204
Remote *
22.23.24.25
Network Details
IP Family *
IPv4
IPv6
Local
Local Subnet *
Local_Subnet
Add
Remove
NATed LAN
Same as Local LAN address
Local ID
Select Local ID
Remote
Allow NAT Traversal
Enable
Remote LAN Network *
Remote_Subnet
Add New Item
Remote ID
Select Remote ID
User Authentication
Quick Mode Selectors
Advanced Settings
Save
Cancel

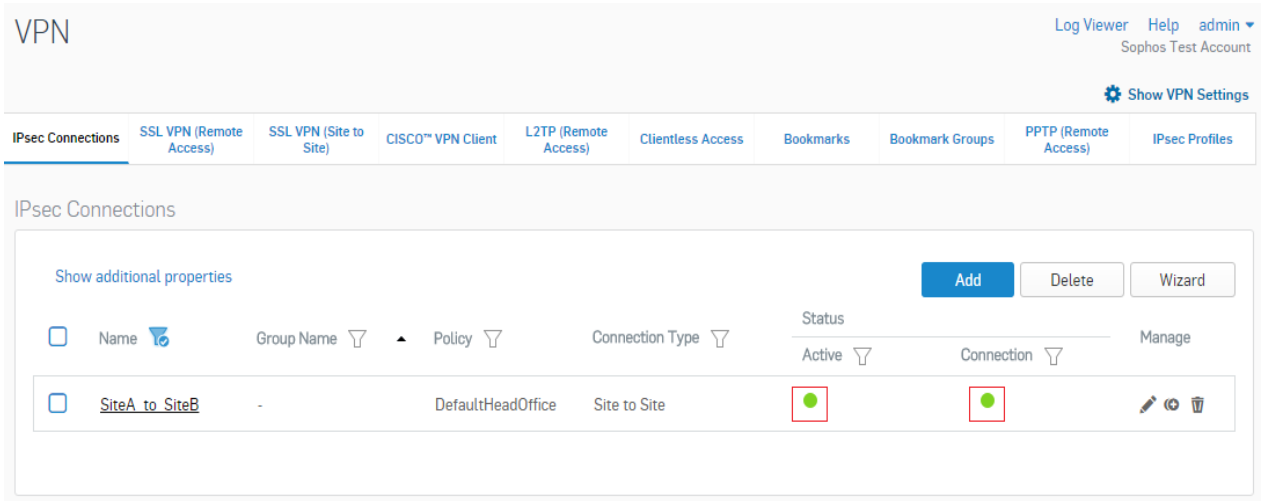
Click **Save** to create IPSec connection.

Step 2: Activate Connection

On clicking **Save**, the following screen is displayed showing the connection created above.



Click  under Status (Active) and Status (Connection) to activate the connection.



Site B Configuration

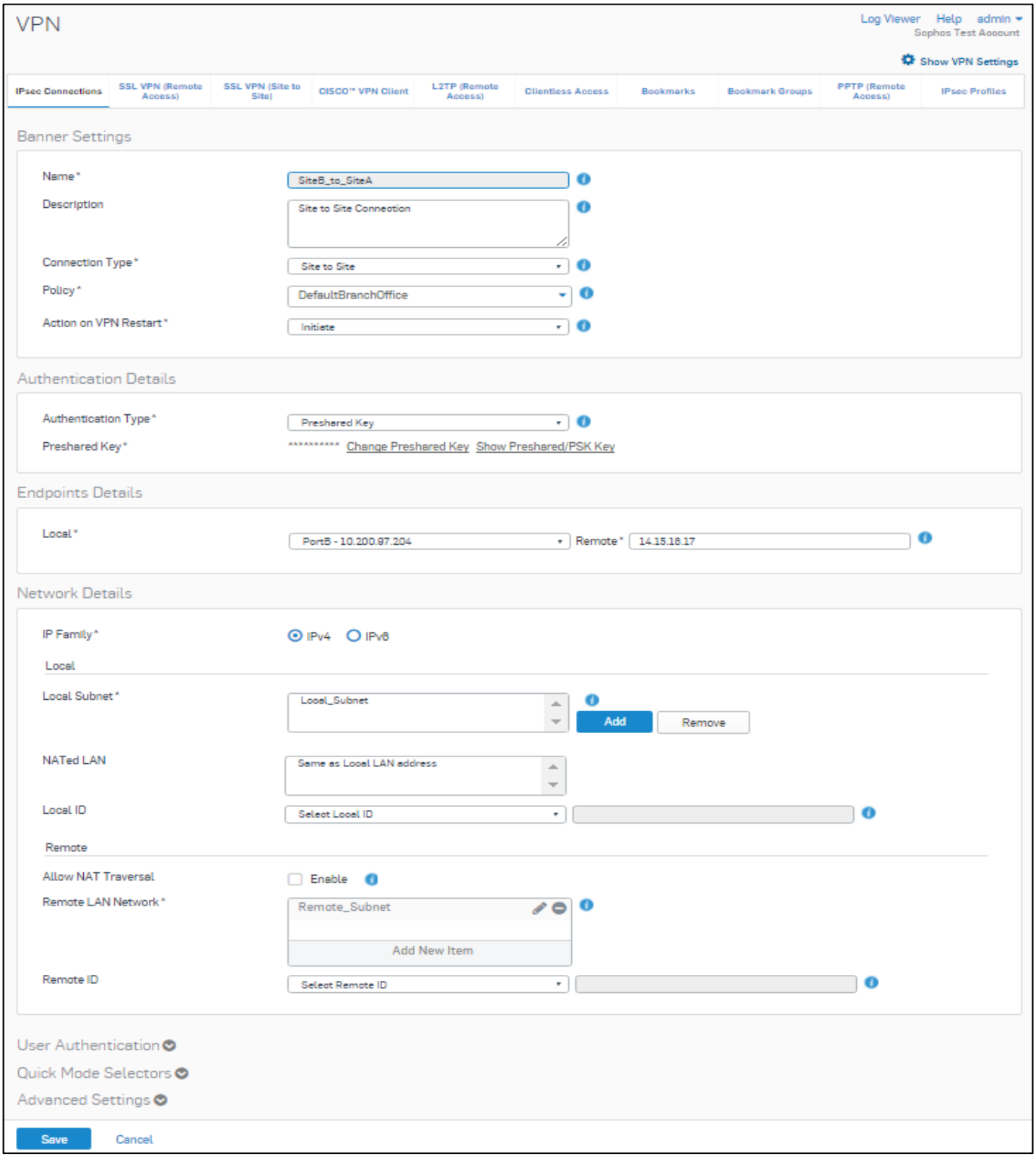
All configurations are to be done from Admin Console of Site B's SF Device using Device Access Profile having read/write administrative rights over relevant features.

Step 1: Create IPsec Connection

Go to **Configure > VPN** and click **Add** under **IPsec Connections**. Create a Connection as per following parameters.

Parameters	Value	Description
General Settings		
Name	SiteB_to_SiteA	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	Preshared Key	Select Authentication Type. Authentication of user depends on the type of connection.
Preshared Key	*<Key>*	Enter the Preshared Key. The same is to be used in the Site B SF Device.
Endpoint Details		
Local	PortB-22.23.24.25	Select Local WAN port from the list. IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.
Remote	14.15.16.17	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)

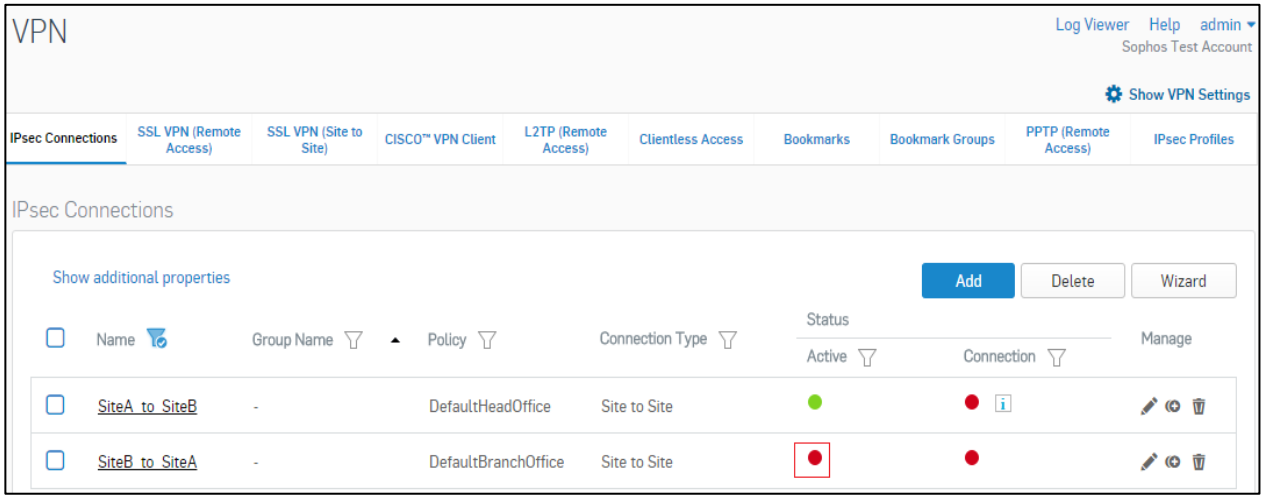
Parameters	Value	Description
Local Subnet	172.23.9.0/24	Select Local LAN Address of Site B. Add and Remove LAN Address using Add Button and Remove Button.
Remote LAN Network	10.5.6.0/24	Select IP Addresses and netmask of remote network in Site A which is allowed to connect to the Device server through 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.



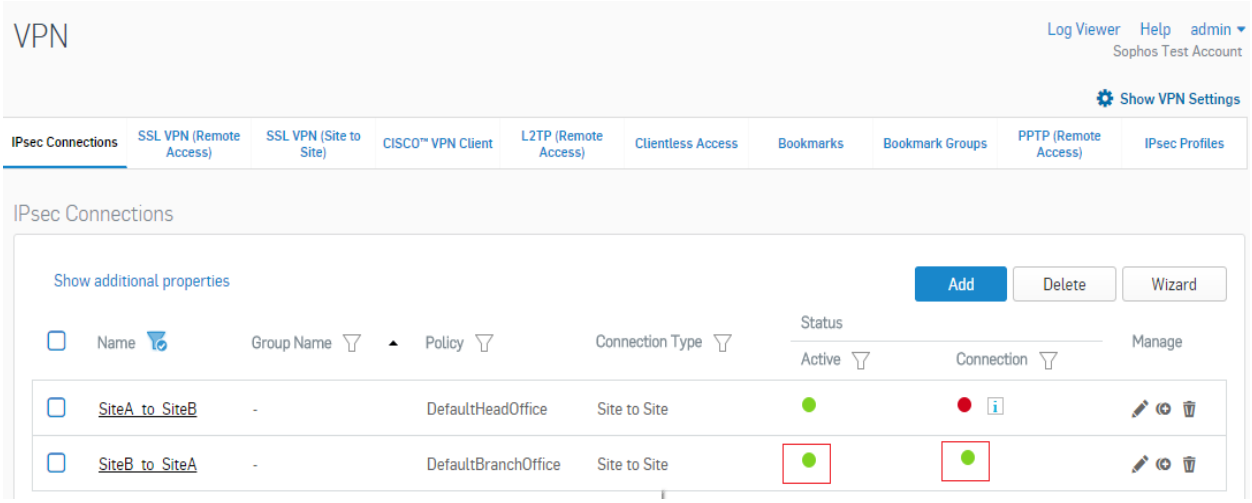
Click **Save** to create IPSec connection.

Step 2: Activate and Establish Connection

On clicking **Save**, the following screen is displayed showing the connection created in Step 1.



Click ● under Status (Active) and Status (Connection) to activate the connection.



The above configuration establishes an IPSec connection between the two sites.

Note:

Make sure that Network Policies that allow LAN to VPN and VPN to LAN traffic are configured. Network Policies can be created from **Protect > Firewall** page.

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