



Pocket Guide

Establish Site-to-Site VPN Connection using RSA Keys

For Customers with Sophos Firewall

Document Date: November 2016

Contents

Overview	3
Scenario	3
Site A Configuration.....	4
Step 1: Create IPsec Connection	4
Step 2: Activate Connection	7
Site B Configuration.....	7
Step 1: Create IPsec Connection	7
Step 2: Activate and Establish Connection	10
Copyright Notice.....	11

Overview

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It is used in protecting data flows 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).

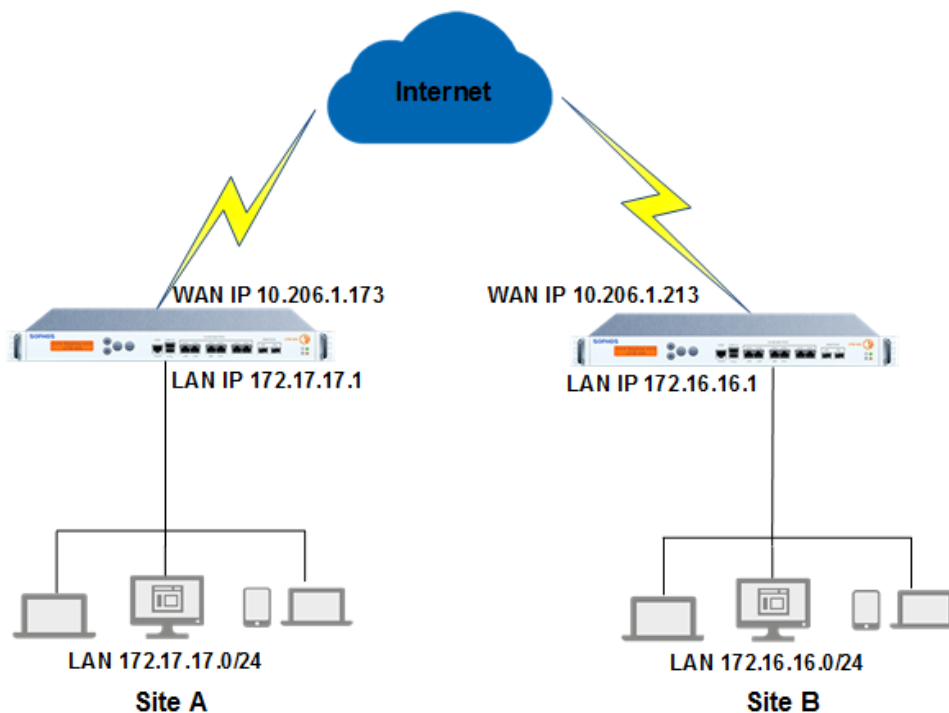
Sophos Firewall's IPsec VPN offers site-to-site VPN with cost-effective site-to-site remote connectivity, eliminating the need for expensive private remote access networks like leased lines, Asynchronous Transfer Mode (ATM) and Frame Relay. The mechanisms used to authenticate VPN peers are Preshared Key, Digital Certificate and RSA Keys.

This article describes a detailed demonstration of how to set up a site-to-site IPsec VPN connection between the two networks using RSA Keys 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.

Network Parameters	
Site A Network details	Local Server (WAN IP address) – 10.206.1.173
	Local LAN address –172.17.17.17/24
	Local ID – john@sophos.com
	<RSA Key for Site A>
Site B Network details	Remote VPN server (WAN IP address) – 10.206.1.213
	Remote LAN Network –172.16.16.16/24
	Remote ID – dean@sophos.com
	<Remote RSA Key for Site B >



Site A Configuration



The configuration is to be done from Site A’s Sophos Firewall Admin Console using profile having read-write administrative rights for relevant feature(s).

Step 1: Create IPsec Connection

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

Parameters	Value	Description
General Settings		
Name	SiteA_to_SiteB	Enter a unique name to identify IPsec Connection.
Description	SiteA to SiteB IPsec	Enter a description for the 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.

Establish Site-to-Site IPsec Connection using RSA Keys

Action on VPN Restart	Respond Only	<p>Select the Action to be taken on the connection when VPN services or Device restarts.</p> <p>Available Options</p> <ul style="list-style-type: none"> - 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	RSA Key	Select Authentication Type. Authentication of user depends on the type of connection.
Local RSA Key	<Site A RSA Key>	Mention the Local RSA Key.
Remote RSA key	<Site B RSA Key>	Mention the Remote RSA Key.
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	<p>Select IP family to configure IPsec VPN tunnels with mixed IP families.</p> <p>Available Options:</p> <ul style="list-style-type: none"> - IPv4 - IPv6 <p>By default, IPv4 will be selected.</p> <p>Four types of IPsec VPN tunnels can be created:</p> <ul style="list-style-type: none"> 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.

Establish Site-to-Site IPsec Connection using RSA Keys

VPN Log Viewer Help admin ▾

[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](#)

General Settings

Name * ⓘ

Description ⓘ

Connection Type * ⓘ

Policy * ⓘ

Action on VPN Restart * ⓘ

Authentication Details

Authentication Type * ⓘ

Local RSA Key * ⓘ

Remote RSA Key * ⓘ

Endpoints Details

Local * Remote * ⓘ

Network Details

IP Family * IPv4 IPv6

Local

Local Subnet * ⓘ

NATed LAN

Local ID ⓘ

Remote

Allow NAT Traversal Enable ⓘ

Remote LAN Network * ⓘ

Remote ID ⓘ

User Authentication ▾

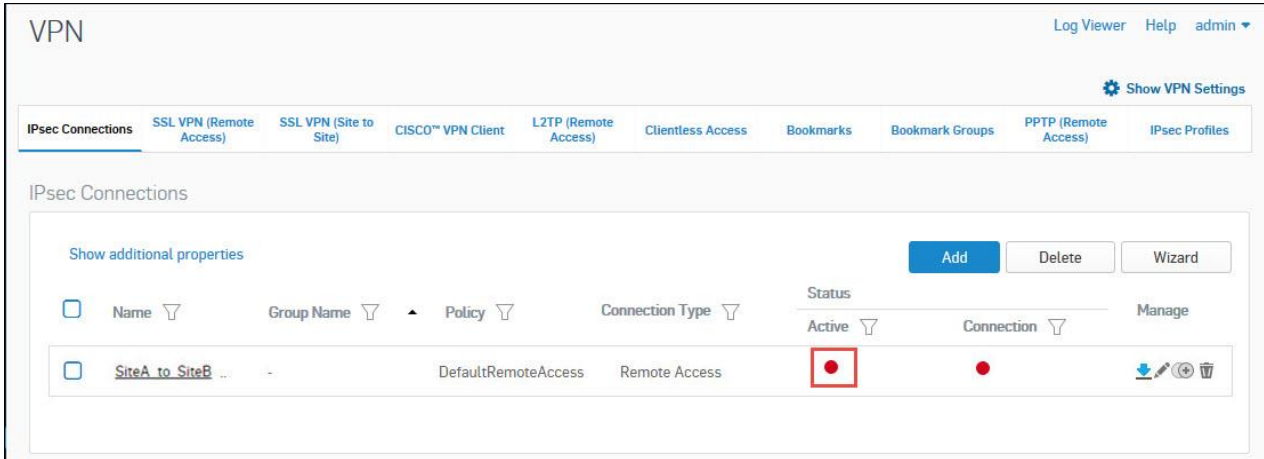
Quick Mode Selectors ▾


Advanced Settings ▾

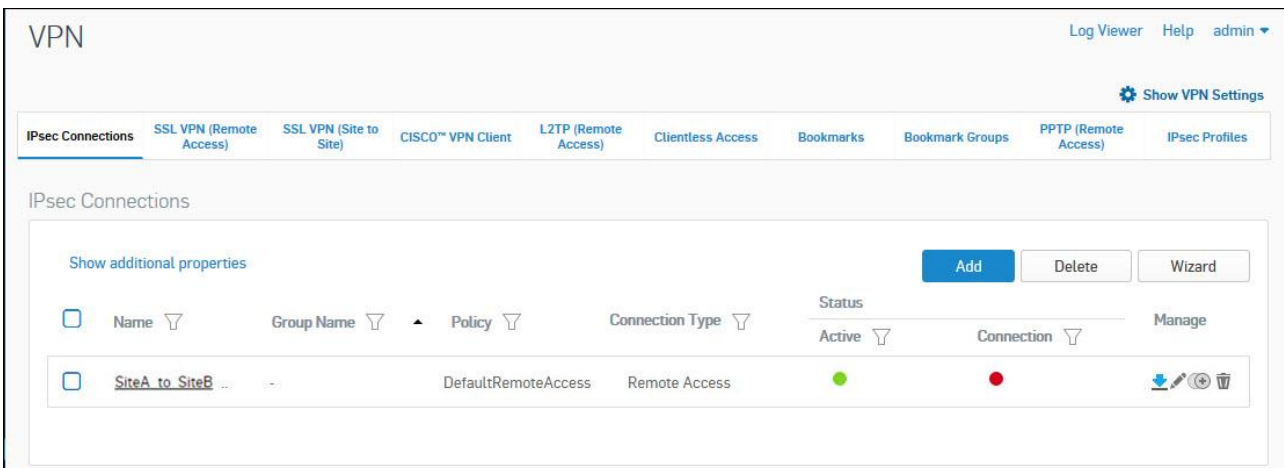
Click **Save** to create IPsec connection.

Step 2: Activate Connection

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



Click  under Status (Active) 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 > IPsec** and click **Add** under IPsec Connections. Create a Connection as per following parameters.

Parameters	Value	Description
General Settings		
Name	SiteB_to_SiteA	Enter a unique name to identify IPsec Connection.

Establish Site-to-Site IPsec Connection using RSA Keys

Description	SiteB to SiteA IPsec	Enter a description for the 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 <ul style="list-style-type: none"> - 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	RSA Key	Select Authentication Type. Authentication of user depends on the type of connection.
Local RSA Key	<Site B RSA Key>	Mention the Local RSA Key.
Remote RSA Key	<Site A RSA Key>	Mention the Remote RSA Key.
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: <ul style="list-style-type: none"> - 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	172.16.16.0/24	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.

Establish Site-to-Site IPsec Connection using RSA Keys

VPN Log Viewer Help admin

[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](#)

General Settings

Name * ⓘ

Description ⓘ

Connection Type * ⓘ

Policy * ⓘ

Action on VPN Restart * ⓘ

Authentication Details

Authentication Type * ⓘ

Local RSA Key * ⓘ

Remote RSA Key * ⓘ

Endpoints Details

Local * Remote *

Network Detail

IP Family * IPv4 IPv6

Local

Local Subnet * ⓘ

NATed LAN

Local ID ⓘ

Remote

Allow NAT Traversal Enable ⓘ

Remote LAN Network * ⓘ

Remote ID ⓘ

User Authentication

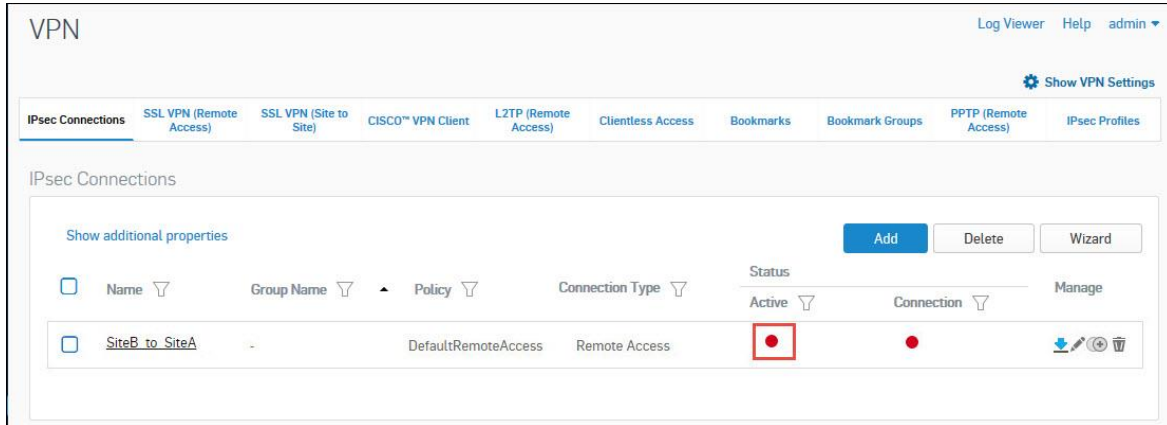
Quick Mode Selectors

Advanced Settings

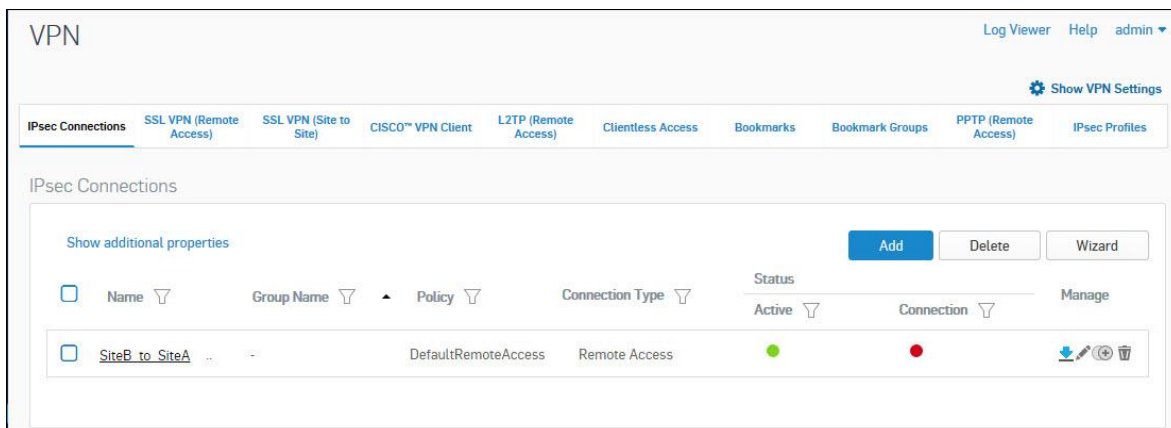
Click **Save** to create IPsec connection.

Step 2: Activate and Establish Connection

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



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



The above configuration establishes an IPsec connection between Two (2) 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 **Policies** 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 practise that Branch Offices retries the connection instead of the Head Office retrying all the branch office connections.

Copyright Notice

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.