

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	
Step 2: Activate Connection	
Site B Configuration	
Step 1: Create IPsec Connection	7
Step 2: Activate and Establish Connection	10
Copyright Notice	11
Step 2: Activate Connection Site B Configuration Step 1: Create IPsec Connection	7 7 7 10

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).

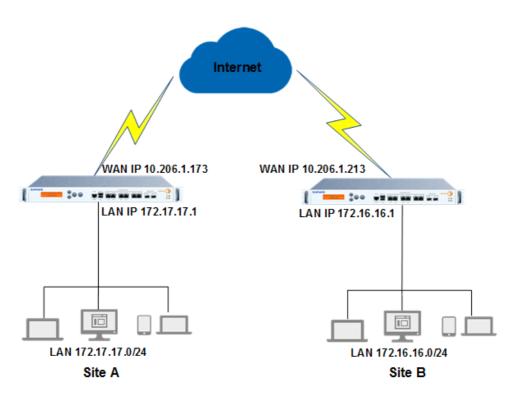
Sophos Firewall's IPsec VPN offers site-to-site VPN with cost-effective site-to-site remote connectivity, eliminating the need for expensive private remote access networks like leased lines, Asynchronous Transfer Mode (ATM) and Frame Relay. The mechanisms used to authenticate VPN peers are Preshared 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 a="" for="" key="" site=""></rsa>
Site B Network details	Remote VPN server (WAN IP address) – 10.206.1.213
	Remote LAN Network –172.16.16.16/24
	Remote ID – <u>dean@sophos.com</u>
	<remote b="" for="" key="" rsa="" site=""></remote>



Site A Configuration

The configuration is to be done from Site A's Sophos Firewall Admin Console using profile having readwrite 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.					

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	5	
Authentication Type	RSA Key	Select Authentication Type. Authentication of user depends on the type of connection.
Local RSA Key	<site a="" key="" rsa=""></site>	Mention the Local RSA Key.
Remote RSA key	<site b="" key="" rsa=""></site>	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	 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.

Psec Connections SSL VPN Acc	(Remote SSL VPN (Site to ess) Site)	CISCO''' VPN Client	L2TP (Remote Access)	Clientless	Access	Bookmarks	Bookmark Groups	PPTP (Remote Access)	Show VPN Settin
eneral Settings									
Name *		SiteA_to_SiteB]	0				
Description		SiteA to SiteB IPsec			0				
Connection Type *		Site to Site		// •	0				
Policy *	[DefaultHeadOffice			0				
Action on VPN Restart		Respond Only		•	0				
uthentication Detail	S								
Authentication Type *		RSA Key		•	0				
Local RSA Key *		DsAQPP+1Rt9HE9wtGfxt DNA6l0iM5lWqbDw7DoY Qi26ekKutFBuSl7GWM0i ww1yiMhq6FJZxDQb2dz	BxIQlob09r5yZY6F Wkl5/243gbWyMb aeVkdFCgzQS1V2g F9+tcq4N+XhBha2	e9Ym ansdb kke7 ▼ uPrP					
Remote RSA Key *		DsAQN/K0M66z4/3J/Yw LtFxNBloBv7++sz/H2tJw 22PaJpSFYQ6klf9PUCYY 5IIO6LttRyVUMhnQJg8T (mi1zEXxK1w0a38cbXau	yosERK8On8+hrM vyYDgYWb0+iK3tA /bPByxU4FaPvkJS Zx5hyYD808xo1Xz uCL5IPNMH27cd2l	urLrq A OdUK SoZn V uCS1					
ndpoints Details									
Local *	[PortB - 10.206.1.173		¥	Remote *	10.206.1.213			00
letwork Details									
IP Family *	G	IPv4 O IPv6							
Local									
Local Subnet *				*	Add	Remo	ive		
NATed LAN		Same as Local LAN addr	ress	*					
Local ID		Select Local ID		۲				0	
Remote									
Allow NAT Traversal		🛾 Enable 🕧							
Remote LAN Network		172.16.16.16/24		10	0				
Remote ID			New Item					0	
. and the	Ļ	Select Remote ID		*					
Jser Authentication	0								
uick Mode Selector									
Advanced Settings	2								

November 2016

Version: 01092016AHM

Click Save to create IPSec connection.

Step 2: Activate Connection

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

								\$	Show VPN Setting
Psec 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
Psec Conner Show addir	ctions						Add	Delete	Wizard
Nan	ne	Group Name 🖓	▲ Policy ∑	Con	nection Type 🛛	Status	Conner	tion 7	Manage
						Active	Conney	nou D	<u>₹</u> .≉ ⊕ 🛱

Click • under Status (Active) to activate the connection.

								\$	Show VPN Setting
Psec 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
Psec Connec	ional properties						Add	Delete	Wizard
_	ie 🖓	Group Name	► Policy 7	Cor	nnection Type 🏾 🖓	Status Active 🖓		tion 7	Manage
Site.	A to SiteB	(e)	DefaultRemo	teAccess F	Remote Access	•	•		👱 🖋 🛞 🗑

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.

November 2016

Version: 01092016AHM

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 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	5	
Authentication Type	RSA Key	Select Authentication Type. Authentication of user depends on the type of connection.
Local RSA Key	<site b="" key="" rsa=""></site>	Mention the Local RSA Key.
Remote RSA Key	<site a="" key="" rsa=""></site>	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: 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 (IPv4 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.

Psec Connections SSL VPN (Remote SSL V Access)	PN (Site to CISCO" VPN Client L2TP (Remote Access)	Clientless Access	Bookmarks	Bookmark Groups	PPTP (Remote Access)	Show VPN Setting
eneral Settings						
Name *	SiteB_to_SiteA	0				
Description	Site B to Site A IPsec	0				
Connection Type *	Site to Site	0				
Policy *	DefaultHeadOffice -	0				
Action on VPN Restart *	Initiate	0				
Authentication Details						
Authentication Type *	RSA Key	0				
Local RSA Key *	0sAQODxqaR3Te837si4edi/htiTEG Qk0EHzv05gvhXVdq5tWlAJPT1t XSANErNx1YFx5J91HqMPTULs0f NbcIZW70iCUvtejUWAN9x5E4m/					
Remote RSA Key *	MOyU6klbYEPSC+mZSNrfhJEqTXI sxhYfhSixoR+1yheEhr3t0qDECQdv PYX/J3j6jqtySh06u45u3nX7pMe0 +y+69e62rFZ6c8FRELME9					
ndpoints Details						
Local *	PortB - 10.206 1 213	Remote * 10	2061173]	
letwork Detail						
IP Family *	● IPv4 ● IPv6					
Local						
Local Subnet *	172.16.16.16/24	O Add	Remove			
NATed LAN	Same as Local LAN address					
Local ID Remote	Select Local ID 🔹			0		
Allow NAT Traversal	🗌 Enable 🌒					
Remote LAN Network *	172.17.17.17/24	0				
	Add New Item					
Remote ID	Select Remote ID)		0		
Jser Authentication 🛇						
Jser Authentication 🛇						
Advanced Settings 🛇						

November 2016

Version: 01092016AHM

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.

								\$	Show VPN Settin
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 Profile
IPsec Connec									
Show addit	ional properties						Add	Delete	Wizard
Nam	ie 🛛		► Policy	Cor	inection Type 🏹	Status			Manage
U Nati			- roucy []	001	incodon Type	Active 🖓	Connec	ction 🖓	Tunuge
	3 to SiteA			teAccess F	Remote Access				🛃 🎤 🛞 📆

Click

under Status (Active) and Status (Connection).

								\$	Show VPN Settin
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
IPsec Connec	tions						Add	Delete	Wizard
_	ie	Group Name 🛛	► Policy 7	Con	nection Type 🏾 🖓	Status	400000	tion 7	Manage
-	to SiteA	-	DefaultRemo	to Accord D	emote Access				👱 🖋 🛞 🗑

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.