

# SecureFirst

Site to Site VPN between a SonicWall firewall and a Cisco IOS device

KNOWLEDGE DATABASE



# Site to Site VPN between a SonicWall firewall and a Cisco IOS device

## **Technical Notes:**

SonicWall has tested VPN interoperability with Cisco IOS SonicOS Standard and Enhanced using the following VPN Security Association information: Keying Mode: IKE IKE Mode: Main Mode with No PFS (perfect forward secrecy) SA Authentication Method: Pre-Shared key Keying Group: DH (Diffie Hellman) – Group 1 ID\_Type: IP Encryption and Data Integrity: ESPDES with MD5 ESP 3DES with MD5 ESP DES with SHA1 ESP 3DES with SHA1

## EXAMPLE setup:

The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with MD5 and without PFS.

SonicWall WAN: IP 10.0.31.102 LAN: 192.168.170.1/24

Cisco IOS WAN: 10.0.31.132 LAN: IP 192.168.132.1/24

#### SonicWall Configuration

First, on the SonicWall, you must create an address object for the remote network.

- 1. Log into the SonicWall.
- 2. Browse to Network, then Address Objects
- 3. Create a new Address Object for the network on the Cisco end you wish to reach (Cisco LAN).





VALL   N	etwork Security Applia	nce				U Wizards	Rep Logout
m	Network /						
ork	Address Obje	cts					
allover & LB	Address Crowns					Rems 1 to 1	(of 1) (14 4 5 51)
	View Style: C All Address	Objects Custom Address Object	s C Default Address Objects			Go to A	ddress Objects 🐔
s Objects						1	
	Add Group	Delete				L	Delete All
icies	□ ► # Name		Address Detail	Туре	Zone	Configure	Comments
	Add Addres	s Object - Mozilla Firefox	<u>X</u>	Group		ØØ	ø
ਸ	Add G SONICWALL	Network Security Appli	ance			T	Delete All
/	Name:	CiscoNetwork					
ii. Uno	Address 0 Zone Assignme	nt: VPN	-			Items 1 to 2	(of 2) ((( * ( * ( * ( *
e	Type:	Network	-			Go to a	Address Groups 🐖
	Ad Network:	192.168.132.0			Refresh All	Purge All	Delete All
Firewall	F # Netmask	255.255.255.0		Туре	Zone	Configure	Comments
	E 1 Ready			Host	WAN	00	ø
labilty	□ 2		Add Close	Network	VPN	Ø	ø
Services	Ad				Refresh All	Purge All	Delete All

Next, on the SonicWall you must create an SA.

- 1) Browse to VPN, then Settings (default view for VPN).
- 2) Ensure that "Enable VPN" is selected.
- 3) Click Add.
- 4) Change the Authentication Method to "IKE using pre-shared secret".
- 5) Name the SA, in this example "CiscolOS".
- 6) Enter the WAN IP of the Cisco for "IPSec Primary Gateway Name or Address:".
- 7) Enter your shared secret, in this example "password"

System       VWV       SOMCAULTY Network Security Appliance         Network       Som Advanced         PC Card       General Network       Proposals Advanced         Network       Security Policy         Acposation Pierwall       WN B         Network       Security Policy         Advanced       Name:         Disc Primary Gateway Name or Address:       100.031.132         Disc Primary Gateway Name or Address:       100.031.132         Users       IKE Authentication         Socurity Perices       Internation         Disc Primary Gateway Name or Address:       Internation         Disc Primary Gateway Name or Address:       Internation         Disc Primary Gateway Name or Address:       Internation         Socurity Perices       Internation         Disc Primary Gateway Name or Address:       Internation         Disc Primary Gateway Name or Address:       Internation         Socurity Services       Internation         Disc Primary Gateway Name or Address       Internation         Socurity Services       Internation         Disc Primary Gateway Name or Address       Internation         Sheed Servicet       Disc Primary Gateway Name or Address       Internation         Disc Primary Gateway Name or Address<		0	VPN Policy - Mozilla Firefox	21	-		_OX			
Society of the second of the seco	System Network PC Card	VPN / Set	SONICWALL Network S	ecurity Appliance	s Advanced	1				
DHCP over VPN   L2TP Server   Users   Hgh Availability   Security Services   Log   Stile 1   Log   Site 1   Log   No En   No En   No En	SonicPoint Firewall VIP Application Firewall VIN Settings Advanced	VPN GI	Security Policy Authentication Method: Name:		IKE using Prest	ared Secret	10	Items per page 50	Items 1 to 2 (of	2) (11 + 1 + 1
Users IKE Authentication   High Availability   Security Services   Confirm Shared Secret:   password   Confirm Shared Secret:   password   Confirm Shared Secret:   password   Confirm Shared Secret:   Peer IXE ID:   IP Address   Peer IXE ID:   IP Address   No En   No En   No En	DHCP over VPN L2TP Server	Г.	IPsec Primary Gateway Nami IPsec Secondary Gateway N	e or Address: ame or Address:	[10.0.31.132		uite		Enable	Configure
Security Services Log Shared Secret: password Confirm Shared Secret: password Confirm Shared Secret: password Confirm Shared Secret: password Confirm Shared Secret: password Delote AL De	🐸 Users 🔛 High Availability	п	IKE Authentication				ES/HP	IAC SHA1 (IKE) IAC SHA1 (IKE)	C	00£
Site T Local IKE ID: IP Address  Peer IKE ID: IP Address  Curres No En No An	Security Services		Shared Secret: Confirm Shared Secret:	password		Mask Shared Secret				Delete All
Peer IXE ID:     IP Address       Current       No Ent       No Ant		Site T Group	Local IKE ID:	IP Address						
No Erv No Ar		Currei	Peer IKE ID:	IP Address	<u>ا</u> ا		10	Items per page 50	Items 0 to 0 (of 0	
No Ar		No Enf						Gateway		
		No Ac								

**ITCorporation**<sup>®</sup> Visit our Website: www.itclatam.com Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290 / +57 318 4914652 sales@itclatam.com/tss@itclatam.com REV1.01



- 1) Select the "Network" tab.
- 2) Select "Lan Subnets" for Local Networks from the drop down box. Select the address object previously created for the destination network.

		VPN Policy - Mo	ozilla Firefox			-101×	1	Supris 1	1990 - 1990
▶ 🐺 System ▶ 🧟 Network	ven/ Setting:	SONICWALL	Network Security Ap	pliance					
PC Card     SonicPoint	Accept	General	Network	Proposals Adv	anced				
Prewal     Prewal     OUP     VolP     Pocation Frewal     OV     VFN     Settings	VPN Global Se	Chocsel Netw Chocsel	<b>vorks</b> local network from list twork obtains 1P addresses (	LAN Subnets	Turnel		ns per page 50 Terris 1	to 3 (of	3) (# + )
DHCP over VPN	THEFT	C Any add	dress *				a ta tat tat	to a fer	**
L2TP Server	I # II I Z Add Site To Site F GroupVPN Pi Currently Act # No Entries	C Use this	n Networks	for all Internet traffic ssees using DHCP through th CiscoNetwork	is VPN Tunnel	l	SHA1 (IKE) SHA1 (IKE) SHA1 (IKE) Is per page S0 Rems 0 Gsteway	Enable	Contigure © © ± © © ± Delate Al
	NO ACINE VPT	Ready		[	0K	Cancel Help			
		Done				AS n/a 10.61.240.1			

- 1) Select the "Proposals" tab.
- 2) Change DH group under IKE Phase 1 to "Group 1".
- 3) Change authentication for IKE Phase 1 to "MD5".
- 4) Change the authentication for IPSec Phase 2 to "MD5"
- 5) Do not enable Perfect Forward Secrecy.



System	VPN/	🕏 VPN Policy - Mozilla Firefox 💷					
Network.	Settings	SONICWALL Network Security	Appliance				
PC Card	Accept						
Frewall	VPN Global Sett	General Network	Proposals Advan	ced			
Application Frewall VPN	Enable VPN	IKE (Phase 1) Proposal					
Settings		Exchange:	Main Mode				3-00 <b>200 - 00</b> - 00
Advanced	VPN Policies	DH Group:	Group 1	2	s per page 50 Items	1 to 3 (of	3) (18 [4] [8
DHCP over VPN	E.,	Encryption:	3DES			Enable	Configure
Users	E 1	Authentication:	MD5	×	HAT (IKE)		00 L
tigh Availability	Π 2	Life Time (seconds):	28800		HA1 (IKE)		000
iecurity Services	E 3	Ipsec (Phase 2) Proposal			HA1 (IKE)	4	2×
og	Add	1 - <b>*</b> - 2,20, <b>*</b> - 5 - 22,20, <b>*</b> - 10 - <b>*</b> - 12,20,	(mar				Diciote All
		Protocol	ESP	<u>×</u>			
	Site To Site Po	Encryption:	3DES	<u> </u>			
		Authentication:	MD5	<u> </u>			
	Currently Activ	Enable Perfect Forward Secrecy			per page 50 Items	to 0 (of	0) (2) (2) (2
	, c	DH Group:	Group 2	<u>×</u>	Sateway		
	No Entries	Life Time (seconds):	28800		a protocol vi		
	the second se						

- 1) Select "Advanced" tab.
  - 2) Ensure that keep alive is enabled on <u>only</u> one end of the tunnel.
  - 3) Select "Enable Windows Networking (NetBIOS) Broadcast" if you would like to pass NetBIOS across the VPN.

#### COMMANDS FOR CISCO IOS

Do not forget to issue the command "write memory" or "copy running-config startup-config" when configuration is complete.

#### Task: Set ACCESS LIST

Command: Access-list 101 permit ip 192.168.132.0 0.0.0.255 192.168.170.0 0.0.0.255 Description: Specify the inside and destination networks. This permits the IP network traffic you want to protect to pass through the router.

#### Task: Define IKE parameters

Command: crypto isakmp policy 1 5 Description: Identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) (This command puts you into the config-isakmp command mode.)





*Command:* encryption 3des *Description:* To specify the encryption algorithm

Command: hash md5 Description: To specify the hash algorithm

*Command:* authentication pre-share *Description:* To specify theauthentication

Command: group 1 Description: To specify the Diffe-Hellman group identifier

*Command:* lifetime 3600 *Description:* Specify the security association's lifetime

Command: exit Description: To exit the config-isakmp command mode

*Command:* crypto isakmp key password address 10.0.31.102 *Description:* To configure a pre-shared authentication key. In this case the pre-shared secret is "password"

#### Task: Define IPSEC parameters

*Command:* crypto ipsec transform-set strong esp-3des esp-md5-hmac *Description:* Configure a transform-set. This identifies the encryption and authentication methods you want to use.

Command: crypto map tosonicwall 15 ipsec-isakmp Description: Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)





*Command:* match address 101 *Description:* To specify an extended access list for a crypto map entry

Command: set transform-set strong Description: To specify which transform sets can be used with the crypto map entry

Command: set peer 10.0.31.102 Description: To specify an IPSec peer in a crypto map entry

Command: exit Description: To exit the crypto map command mode

#### Task: Apply Crypto Map to an Interface

Command: interface fastethernet0/1 Description: Specify an interface on which to apply the crypto map. (This command puts you into the interface command mode). Please note, you need to specify the interface that you have defined as external (your WAN interface).

Command: crypto map tosonicwall Description: Apply the previously defined crypto map set to an interface

Command: exit Description: Exit the interface command mode

*Command:* exit *Description:* Exit the global configuration mode





# **RESOLUTION FOR SONICOS 6.5 AND LATER**

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

#### Technical Notes:

SonicWall has tested VPN interoperability with Cisco IOS SonicOS Standard and Enhanced using the following VPN Security Association information:

Keying Mode: IKE IKE Mode: Main Mode with No PFS (perfect forward secrecy) SA Authentication Method: Pre-Shared key Keying Group: DH (Diffie Hellman) – Group 1 ID\_Type: IP Encryption and Data Integrity: ESPDES with MD5 ESP 3DES with MD5 ESP DES with SHA1

ESP 3DES with SHA1

## **EXAMPLE setup:**

The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with MD5 and without PFS.

SonicWall *WAN:* IP 10.0.31.102 *LAN:* 192.168.170.1/24

Cisco IOS WAN: 10.0.31.132 LAN: IP 192.168.132.1/24





#### SonicWall Configuration

First, on the SonicWall, you must create an address object for the remote network.

- 1. Log into the SonicWall.
- 2. Browse to Manage > Objects > Address Objects
- 3. Create a new Address Object for the network on the Cisco end you wish to reach (Cisco LAN).

Updates	Address O	bjects	C Edit Address Object	t - Google Chrome		
Licenses			A Not secure	://192.168.198.	1/addNetObjDlg	.html?objType Q
Firmware & Backups	Add	Θ	CONICIALA	II. Natural Const	u Appliance	
WXA Firmware		_	SONICWA	LL Network Securit	у мррналсе	
Restart	·	Name				
Connectivity	1	CiscoN	Name:	CiscoNetwork		
Connectivity			Zone Assignment:	VPN	•	
SSI VPN			Туре:	Range	•	
Access Points			Starting IP Address:	192.168.132.1		
3G/4G/Modem			Ending IP Address:	255.255.255.0		
Policies			Ready			
Rules					6	
Objects					OK	CANCEL
Match Objects					1. C.	al al di
Action Objects						
Address Objects						
Service Objects						
Bandwidth Objects			L			
Email Address Objects						

Next, on the SonicWall you must create an SA.

- 1) Browse to Manage > VPN > Base Settings.
- 2) Ensure that "Enable VPN" is selected.
- 3) Click Add.





Mode: Configuration					
lew IP Version: ⊛ IPv4 ⊚ IPv6	V	(II) (a) Refeath Ini	0	VPN Global Settings Enable VPN Unique Firewall Identifier: 188169700F0 V/DN Dollicion	Updates Licenses Firmware & Backups WXA Firmware Restart Connectivity
tems 1 to 5 (of 5) 1 5	erikar (seca) 10 secura her haße 20 s	III C Reitest In		VPN POlicies	Date California
Enable Configure	Crypto Suite	Destinations	Gateway	S # Name	Base Settings Advanced Settings
Enable Configure	Crypto Suite ESP: 30ES/HMAC SHA1 (IKE)	Destinations	Gateway	WIN POILCIES	Base Settings Advanced Settings DHCP over VPN L2TP Server
tems 1 to 5 (of 5) 1 1 Enable Configure . 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Crypto Suite ESP: 3DES/HMAC SHA1 (IXE) ESP: 3DES/HMAC SHA1 (IXE)	Destinations	Gateway	WAN GroupVPN     2 WLAN GroupVPN	Base Settings Advanced Settings DHCP over VPN L2TP Server SSL VPN
Enable         Configure           ℓ         ∅ ∞ ⊕           ∅         ⊕           ∅         ⊕           ∅         ⊕           ∅         ⊕	Crypto Suite ESP: 3DES/HMAC SHA1 (IXE) ESP: 3DES/HMAC SHA1 (IXE) ESP: 3DES/HMAC SHA1 (IXE) ESP: 4ES-256/HMAC SHA15 (IXE)	Destinations 10.10.10.0 - 10.10.10.255	Gateway		Base Settings Advanced Settings DHCP over VPN L2TP Server SSL VPN Access Points 30/46/Modem
Enable         Configure           Ø         Ø           Ø         Ø           Ø         Ø           Ø         Ø           Ø         Ø           Ø         Ø	Crypto Suite         20         xxmm per page         20         x           ESP: 3DES/HMAC SHA1 (IXE)         ESP: 3DES/HMAC SHA1 (IXE)         ESP: 4ES-256/HMAC SHA1 (IXE)         ESP: 4ES-256/HMAC SHA1 (IXE)           ESP: 3DES/HMAC SHA1 (IXE)         ESP: 3DES/HMAC SHA1 (IXE)         ESP: 4ES-256/HMAC SHA1 (IXE)	Destinations 10.10.10.0 - 10.10.10.255	Gateway 2.2.2.2 10.103.20.200		Base Settings Advanced Settings DHCP over VPN L2TP Server SSL VPN Access Points 3G/4G/Modem
Enable         Configure           ∅         ∅         ⊕           ∅         ∅         ⊕           ∅         ∅         ⊕           ∅         ∅         ⊕           ∅         ∅         ⊕           ∅         ∅         ⊕           ∅         ∅         ⊗           ∅         ∅         ⊗           ∅         ∅         ⊗           ∅         ∅         ⊗	Crypto Suite         20         xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Destinations 10.10.10.0 - 10.10.10.255	Gateway 2.2.2.2 10.103.20.200 10.103.20.34		Ease Settings Advanced Settings DHCP over VPN L2TP Server SSL VPN Access Points 3G/4G/Modem Policies

- 4) Select Authentication Method to "IKE using pre-shared secret".
- 5) Name the SA, in this example "CiscolOS".
- 6) Enter the WAN IP of the Cisco for "IPSec Primary Gateway Name or Address:".
- 7) Enter your shared secret, in this example "password"

Policy Type:		Site to Si	te	•	
Authentication Method:		IKE using	Preshared Secret	•	
Name:		CiscoIOS			
Psec Primary Gateway	Name or Address:	10.0.31.1	32		
Psec Secondary Gatew	ay Name or Address:				
Shared Secret: Confirm Shared Secret:			Mask Shared Secret		
Local IKE ID:	IPv4 Address	•			
Peer IKE ID:	IPv4 Address	•			





- 1) Select the "Network" tab.
- 2) Select "Lan Subnets" for Local Networks from the drop down box. Select the address object previously created for the destination network (CiscoNetwork).

Use IKEv2 IP Pool	Select IP Pool Network		
Use this VPN Tunnel as default route for all Inter     Choose destination network from list	met traffic CiscoNetwork		
Remote Networks			
Choose local network from list     Any address*	LAN Subnets	•	
Local Networks			

- 1) Select the "Proposals" tab.
- 2) Change DH group under IKE Phase 1 to "Group 1".
- 3) Change authentication for IKE Phase 1 to "MD5".
- 4) Change the authentication for IPSec Phase 2 to "MD5"
- 5) Do not enable Perfect Forward Secrecy.





KE (Phase 1) Proposal		
xchange:	IKEv2 Mode	•
H Group:	Group 1	
ncryption	3DES	Ŧ
uthentication:	MD5	
fe Time (seconds):	28800	
rotocol:	ESP	T
ncryption:	3DES	¥
uthentication:	MD5	
Enable Perfect Forward Secrecy		
ife Time (seconds):	28800	

- 1) Select "Advanced" tab.
- 2)
- Ensure that keep alive is enabled on <u>only</u> one end of the tunnel. Select "Enable Windows Networking (NetBIOS) Broadcast" if you would like to pass NetBIOS 3) across the VPN.



	[13]
SONIC	
Knowledge	Database

SONICWALL Network Security Ap	pliance	
General Network Proposals	dvanced	
Advanced Settings		Î
Enable Keep Alive		
Suppress automatic Access Rules creation fi	or VPN Policy	
Disable IPsec Anti-Replay		
Enable Windows Networking (NetBIOS) Broa	adcast	
Enable Multicast		
WXA Group: None		
Display Suite B Compliant Algorithms Only		
Apply NAT Policies		
Allow SonicPointN Layer 3 Management		
Management via this SA:	HTTPS SSH SNMP	
User login via this SA:	HTTP HTTPS	
Default LAN Gateway (optional):		
VPN Policy bound to:	Zone WAN	
IKEv2 Settings		
Do not send trigger packet during IKE SA ne	gotiation	
Ready		150

# **COMMANDS FOR CISCOIOS**

Do not forget to issue the command "write memory" or "copy running-config startup-config" when configuration is complete.

# Task: Set ACCESSLIST

Command: Access-list 101 permit ip 192.168.132.0 0.0.0.255 192.168.170.0 0.0.0.255 Description: Specify the inside and destination networks. This permits the IP network traffic you want to protect to pass through therouter.





# Task: Define IKE parameters

Command: crypto isakmp policy 1 5 Description: Identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) (This command puts you into the config-isakmp command mode.)

Command: encryption 3des Description: To specify the encryption algorithm

Command: hash md5 Description: To specify the hash algorithm

*Command:* authentication pre-share *Description:* To specify theauthentication

Command: group 1 Description: To specify the Diffe-Hellman group identifier

Command: lifetime 3600 Description: Specify the security association's lifetime

*Command:* exit *Description:* To exit the config-isakmp command mode

Command: crypto isakmp key password address 10.0.31.102 Description: To configure a pre-shared authentication key. In this case the pre-shared secret is "password"





## Task: Define IPSEC parameters

*Command:* crypto ipsec transform-set strong esp-3des esp-md5-hmac *Description:* Configure a transform-set. This identifies the encryption and authentication methods you want to use.

Command: crypto map tosonicwall 15 ipsec-isakmp Description: Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)

Command: match address 101 Description: To specify an extended access list for a crypto map entry

*Command:* set transform-set strong *Description:* To specify which transform sets can be used with the crypto map entry

Command: set peer 10.0.31.102 Description: To specify an IPSec peer in a crypto map entry

*Command:* exit *Description:* To exit the crypto map command mode





# Task: Apply Crypto Map to an Interface

Command: interface fastethernet0/1 Description: Specify an interface on which to apply the crypto map. (This command puts you into the interface command mode). Please note, you need to specify the interface that you have defined as external (your WAN interface).

Command: crypto map tosonicwall Description: Apply the previously defined crypto map set to an interface

*Command:* exit *Description:* Exit the interface command mode

*Command:* exit *Description:* Exit the global configuration mode.

