



**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).

Network /

Address Objects

Address Groups Items 1 to 1 (of 1)

View Style: All Address Objects Custom Address Objects Default Address Objects

Go to Address Objects

Add Group... Delete Delete All

Name	Address Detail	Type	Zone	Configure	Comments
CiscoNetwork		Group			

Items 1 to 2 (of 2)

Go to Address Groups

Refresh All Purge All Delete All

Type	Zone	Configure	Comments
Host	WAN		
Network	VPN		

Refresh All Purge All Delete All

Done [AS n/a | 10.61.240.1]

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"

VPN /

VPN Policy

Settings

VPN Group

Unique

VPN Policy

Site T

Group

Current

No En

No Ad

Ready

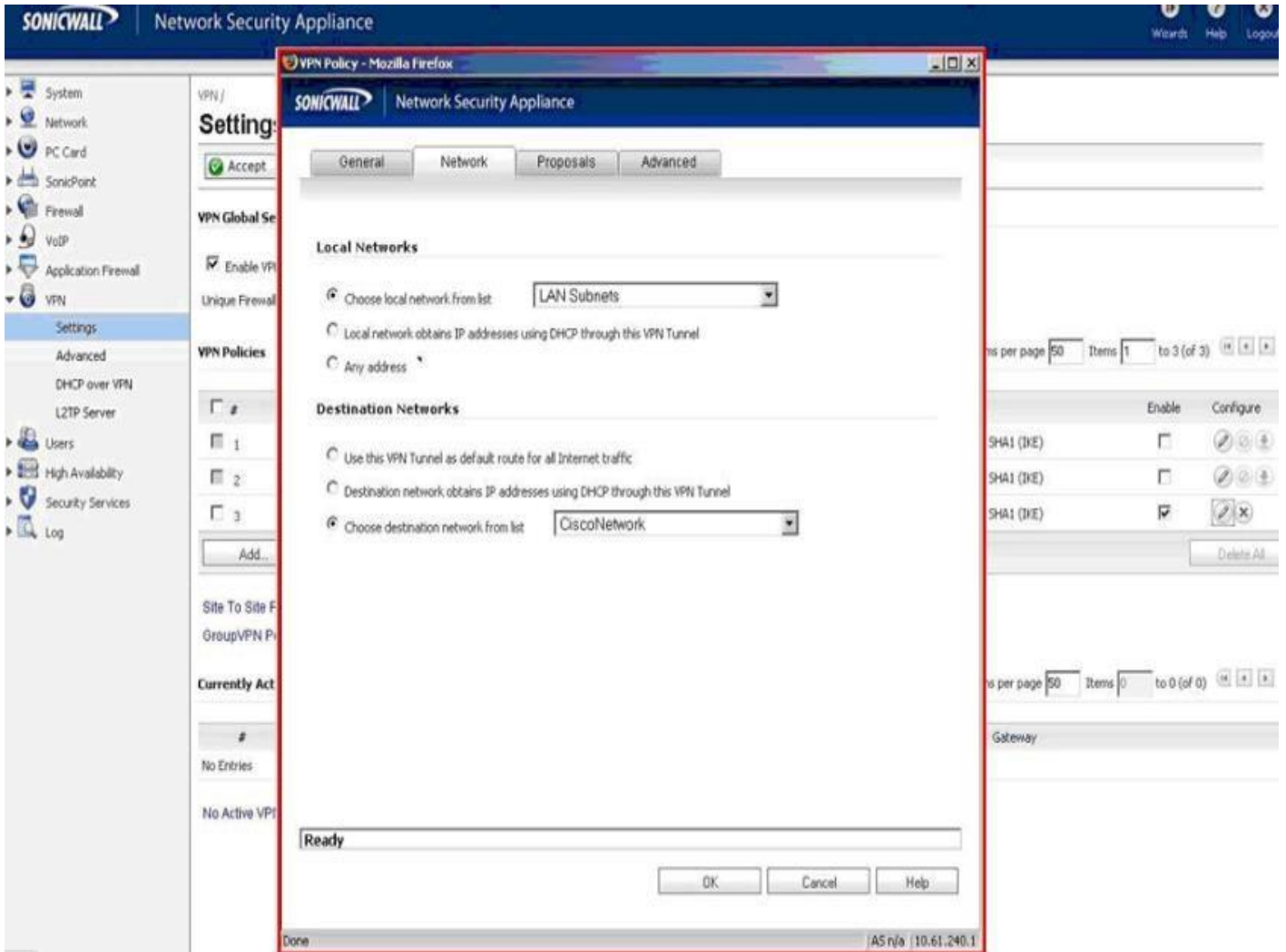
OK Cancel Help

Items per page 50 Items 1 to 2 (of 2)

Items per page 50 Items 0 to 0 (of 0)

Gateway

- 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.



- 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.

- 1) Select “Advanced” tab.
- 2) Ensure that keep alive is enabled on only 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 15
```

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 the authentication

Command:

group 1

Description:

To specify the Diffie-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).

The screenshot displays the SonicWall management interface. The top navigation bar includes 'SONICWALL Network Security Appliance', 'MONITOR', 'INVESTIGATE', 'MANAGE', and 'QUICK CONFIGURATION'. The left-hand menu shows various configuration categories, with 'Address Objects' selected under the 'Objects' section. The main content area shows a table with one entry: '# 1 CiscoN'. A dialog box titled 'Edit Address Object - Google Chrome' is overlaid on the screen. The dialog contains the following fields: Name: CiscoNetwork, Zone Assignment: VPN, Type: Range, Starting IP Address: 192.168.132.1, and Ending IP Address: 255.255.255.0. The status bar at the bottom of the dialog says 'Ready'. There are 'OK' and 'CANCEL' buttons at the bottom right.

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.

SONICWALL® Network Security Appliance MONITOR INVESTIGATE **MANAGE** QUICK CONFIGURATION Help | Logout

Mode: Configuration

Updates
Licenses
Firmware & Backups
WXA Firmware
Restart

Connectivity
VPN
Base Settings
Advanced Settings
DHCP over VPN
LTP Server
SSL VPN
Access Points
3G/4G/Modem

Policies
Rules
Objects

System Setup

VPN Global Settings

Enable VPN
Unique Firewall Identifier: 18B1697D0FC0

View IP Version: IPv4 IPv6

VPN Policies

Refresh Interval (secs) 10 Items per page 50 Items 1 to 5 (of 5)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
3	VPN to NSA 2650 Site	2.2.2.2	10.10.10.0 - 10.10.10.255	ESP: AES-256/HMAC SHA256 (IKE)	<input checked="" type="checkbox"/>	
4	To_400w	10.103.20.200		ESP: 3DES/HMAC SHA1 (IKEv2)	<input checked="" type="checkbox"/>	
5	To_3600	10.103.20.94		ESP: 3DES/HMAC SHA1 (IKEv2)	<input checked="" type="checkbox"/>	

Site To Site Policies: 3 Policies Defined, 3 Policies Enabled, 1000 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 1 Policies Enabled, 12 Maximum Policies Allowed

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

SONICWALL® Network Security Appliance

General **Network** Proposals Advanced

Security Policy

Policy Type: Site to Site
Authentication Method: IKE using Preshared Secret
Name: CiscoIOS
IPsec Primary Gateway Name or Address: 10.0.31.132
IPsec Secondary Gateway Name or Address:

IKE Authentication

Shared Secret:
Confirm Shared Secret: Mask Shared Secret
Local IKE ID: IPv4 Address
Peer IKE ID: IPv4 Address

Ready

- 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).

The screenshot shows the SonicWall Network Security Appliance configuration interface. At the top, there are four tabs: General, Network (selected), Proposals, and Advanced. Below the tabs, the 'Local Networks' section has two radio buttons: 'Choose local network from list' (selected) and 'Any address'. A dropdown menu next to 'Choose local network from list' is set to 'LAN Subnets'. The 'Remote Networks' section has three radio buttons: 'Use this VPN Tunnel as default route for all Internet traffic', 'Choose destination network from list' (selected), and 'Use IKEv2 IP Pool'. A dropdown menu next to 'Choose destination network from list' is set to 'CiscoNetwork'. Below that, there is another dropdown menu labeled '--Select IP Pool Network--'. At the bottom of the window, there is a status bar that says 'Ready' and three buttons: OK, CANCEL, and HELP.

- 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.

SONICWALL™ Network Security Appliance

General Network **Proposals** Advanced

IKE (Phase 1) Proposal

Exchange: IKEv2 Mode ▼

DH Group: Group 1 ▼

Encryption: 3DES ▼

Authentication: MD5 ▼

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP ▼

Encryption: 3DES ▼

Authentication: MD5 ▼

Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Ready

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

SONICWALL™ Network Security Appliance

General

Network

Proposals

Advanced

Advanced Settings

- Enable Keep Alive
- Suppress automatic Access Rules creation for VPN Policy
- Disable IPsec Anti-Replay
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- WXA Group:
- 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:

IKEv2 Settings

- Do not send trigger packet during IKE SA negotiation

Ready

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 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 the router.

Task: Define IKE parameters

Command:

```
crypto isakmp policy 15
```

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 the authentication

Command:

```
group 1
```

Description:

To specify the Diffie-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.