

SecureFirst

Site to Site VPN Using Certificates KNOWLEDGE DATABASE



Site to Site VPN Using Certificates

Using digital certificates for authentication instead of pre-shared keys in a site-to-site VPN configuration is considered more secure. This KB article describes the method to configure a site-to-site VPN using digital certificates.

Although the devices depicted in this article are an NSA 2400 (Site A) and an NSA 240 (Site B) running SonicOS Ehanced 5.8.1.7 firmware, all SonicWall UTM appliances running either SonicOS Enhanced or Standard firmware support this configuration.

A valid certificate from a third party Certificate Authority (CA) must be installed in the SonicWall UTM appliance. The CA could either be a public CA or a Microsoft CA. For the purpose of this article, certificates issued by Microsoft CA are used.



Site A:

X1 (WAN) Interface IP: 172.27.61.115 X0 Subnet: 192.168.100.0/24

Site B:

X1 (WAN) Interface IP: 192.168.170.51 X0 Subnet: 10.10.10.0/24

RESOLUTION:

Site A (NSA 2400) configuration

Obtain a signed certificate

• Refer this KB article to obtain a signed certificate from a Microsoft CA : <u>How to obtain a Certificate</u> from a Windows Certificate Authority (CA)

• Refer this KB article to obtain a signed certificate from a public CA: <u>How to Request and Import a</u> <u>Signed Certificate from Thawte</u>

When obtaining a signed certificate the following must be borne in mind:

- Wild card characters (* or ?) are not supported in Email ID, Distinguished Name or Domain Name
- Email ID and Domain Name can be used only when it is specified in the Subject Alternative Name of the cortificate







Create a site-to-site VPN policy.

- Login to the SonicWall management GUI
- Navigate to the VPN page.
- Click on Add to open to the General tab of the VPN Policy window.
- The General tab is where most of the certificate specific information is entered.
- Policy Type: Site to Site
- Authentication Method: IKE using 3rd Party Certificates.
- Name: Enter a name for this VPN policy.
- **IPsec Primary Gateway Name or Address**: Enter the name or IP address of the Site B (NSA 240) SonicWall.
- **IPsec Secondary Gateway Name or Address**: Enter the name or IP address of the secondary WAN of the Site B (NSA240) SonicWall.
- IKE Authentication
- Local Certificate: Select the certificate obtained earlier from a CA
- Local IKE ID Type: Choose anyone of the following depending on the information in the signed certificate:

Distinguished Name (DN): Based on the certificate's Subject Distinguished Name field, which is contained in all certificates by default. As with the E-Mail ID and Domain Name below, the entire Distinguished Name field must be entered for site-to-site VPNs - Wild card characters are not supported. To find the certificate details (Subject Alternative Name, Distinguished Name, etc.), navigate to the **System > Certificates** page and click on the **Details** icon. DNs are separated by the forward slash character, for example: /C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub

Email ID (UserFQDN): Based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name in Email ID format, that value must be used. If obtaining a new certificate from a CA, you could specify an E-mail ID in the Subject Alternative Name. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the E-Mail ID must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect. For example, *administrator@sonic-lab.local*

Domain Name: Based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name in Domain Name format, that value must be used. If obtaining a new certificate from a CA, you could specify a Domain Name in the Subject Alternative Name. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the Domain Name must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect. For example, *sonic-lab.com*

IP Address (IPv4): If the Common Name (CN) or the Subject Alternative Name in the certificate is an IP address, enter the IP address here.

ITCorporation® 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



System /

Certifi	cates and Certificate	Reque	nsa2400-vj Certificate I	ssuer:	/DC=local/DC=hal	-2010/CN=hal-2010.local	t	o 6 (of 6) (+++++
View St	yle: 🔘 All certificates	• Ir	Subject Dist	inguished Name:	/C=IN/ST=KA/L=E lab.local	BLR/O=SonicWALL/CN=nsa2400-	ertifica	ates
	# Certificate	Ту	Certificate S Valid from:	ierial Number:	6112F40D00000000 Jul 22 12:35:40 201	0032 2 GMT	s	Configure
	1 Sonicwall	Loc	Alternate Su	ubject Name: ubject Name Type	nsa2400-lab.local s Domain Name			× ±
	2 SNWL-2k3Cert	Loc	Status:	10	Verified			⊗ 🕭
	3 nsa2400-vpncert	Local	certificate	Yes	Jul 22 12:35:40 2	1014 GMT	10	۵ ک
	hal-2010.local	CA ce	rtificate		Nov 20 14:06:18	2015 GMT	ø	🛞 街 🎒
1	Import Ne	w Signing	Request	SCEP.	Dele	ie		Delete Al

• **Peer IKE ID Type**: This must be the **Local IKE ID Type** selected in the VPN policy of Site B (NSA 240) SonicWall. The following can be selected:

- Distinguished Name (DN) Email ID (UserFQDN) Domain Name IP Address (IPv4)
- Peer IKE ID: Enter the value of what is selected above.

General	Network	Proposals	Advanced	
	M			
Security Polic	v			
Policy Type:			Site to Site	
Authentication Me	thod:		IKE using 3rd Party Certificates	
Name:			VPN To Site B	
IPsec Primary Gab	eway Name or Address		192.168.170.51	
IPsec Secondary (Sateway Name or Addr	ess:	0.0.0.0	
IKE Authentic	ation			
Local Certificate:	Remote site must	choose DN for	nsa2400-vpncert	
Local IKE ID Type:	in this site's o	certificate	Distinguished name (DN)	
Peer IKE ID Type:	e: This is the Email ID of the remote site's		s E-Mail ID (UserFQDN)	
Peer IKE ID: policy. The remote site must choose Local IKE ID as Email ID		administrator@nsa240-lab.local		





The configuration in the General tab is over. The remaining tabs, Network, Proposals and Advanced, can be configured in the same way as a normal VPN :

General Network Proposals Advan	Ced General Network Proposals A	vance
Local Networks	IKE (Phase 1) Proposal	
TANS	boete Exchange: Main Mode	٠
Choose local network from list	DH Group: Group 2	•
Local network obtains IP addresses using DHCP through this VPN Tunnel	Encryption: 3DES	•
Any address	Authentication: SHA1	٠
Remote Networks	Life Time (seconds): 28800	
🗇 Use this VPN Tunnel as default route for all Internet traffic	Ipsec (Phase 2) Proposal	
O Destination network obtains IP addresses using DHCP through this VPN	Tunnel ESP	•
Choose destination network from list SiteBN	etwork · · · · · · · · · · · · · · · · · · ·	
	Authorstration: SHA1	+
	Enable Perfect Forward Secrecy	
	Life Time (seconds): 28800	
OK Cancel	Help OK Cancel	Help
OK Cancel General Netw	Heip OK Cancel	Help
OK Cancel General Netw Advanced Settings	Heip OK Cancel	Help
OK Cancel General Netw Advanced Settings	Help OK Cancel	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive	Help OK Cancel	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Suppress automatic Acces Require authentication of	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Suppress automatic Access Require authentication of Enable Windows Networka	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Suppress automatic Access Require authentication of Enable Windows Networka Enable Multicast	Heip OK Cancel rork Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast	Help
OK Cancel General Netw Advanced Settings Enable Keep Aive Suppress automatic Access Require authentication of Enable Windows Networka Enable Multicast Permit TCP Acceleration	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Suppress automatic Access Require authentication of Enable Windows Networka Enable Multicast Permit TCP Acceleration Apply NAT Policies	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast	Help
OK Cancel General Netw Advanced Settings Character Settings Ch	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast	Help
OK Cancel General Netw Advanced Settings Character Settings Ch	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast HTTP HTTPS SSH	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Suppress automatic Access Require authentication of Enable Windows Networki Enable Multicast Permit TCP Acceleration Apply NAT Policies Enable OCSP Checking Management via this SA: User login via this SA:	Heip OK Cancel Iorik Proposals Advanced Is Rules creation for VPN Policy VPN clients by XAUTH Ing (NetBIOS) Broadcast Image: HTTP HTTPS Image: HTTP HTTPS	Help
OK Cancel General Netw Advanced Settings	Heip OK Cancel Iorik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ing (NetBIOS) Broadcast Image: HTTP HTTPS	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Enable Keep Alive Suppress automatic Access Require authentication of Enable Windows Networks Enable Multicast Permit TCP Acceleration Apply NAT Policies Enable OCSP Checking Management via this SA: User login via this SA: Default LAN Gateway (optional VPN Policy bound to:	Heip OK Ork Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast HTTP HTTPS SSH HTTP HTTP HTTPS 0.0.0.0 Zone WAN	Help
OK Cancel General Netw Advanced Settings Enable Keep Alive Suppress automatic Access Require authentication of Enable Windows Networki Enable Multicast Permit TCP Acceleration Apply NAT Policies Enable OCSP Checking Management via this SA: User login via this SA: Default LAN Gateway (optional VPN Policy bound to:	Heip OK Orik Proposals Advanced s Rules creation for VPN Policy VPN clients by XAUTH ng (NetBIOS) Broadcast Image: HTTP HTTP </td <td>Help</td>	Help



Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290/ +57 318 4914652 sales@itclatam.com/tss@itclatam.com REV1.01



Site B (NSA 240) configuration

Obtain a signed certificate

- Refer this KB article to obtain a signed certificate from a Microsoft CA : <u>UTM: How to obtain a</u> <u>Certificate from a Windows Certificate Authority (CA)</u>
- Refer this KB article to obtain a signed certificate from a public CA: <u>UTM: How to Request and</u> <u>Import a Signed Certificate from Thawte</u>
- When obtaining a signed certificate the following must be borne in mind:
 - Wild card characters (* or ?) are not supported in Email ID, Distinguished Name or Domain Name
 - Email ID and Domain Name can be used only when it is specified in the Subject Alternative Name of the certificate.

Create a site-to-site VPN policy.

- Login to the SonicWall management GUI
- Navigate to the VPN page.
- Click on Add to open to the General tab of the VPN Policy window.
- The **General** tab is where most of the certificate specific information is entered.
- Policy Type: Site to Site
- Authentication Method: IKE using 3rd Party Certificates.
- Name: Enter a name for this VPN policy.
- IPsec Primary Gateway Name or Address: Enter the name or IP address of the Site B (NSA 240) SonicWall.

• **IPsec Secondary Gateway Name or Address**: Enter the name or IP address of the secondary WAN of the Site B (NSA 240) SonicWall.

- IKE Authentication
- Local Certificate: Select the certificate obtained earlier from a CA
- Local IKE ID Type: Choose anyone of the following depending on the information in the signed certificate:

Distinguished Name (DN): Based on the certificate's Subject Distinguished Name field, which is contained in all certificates by default. As with the E-Mail ID and Domain Name below, the entire Distinguished Name field must be entered for site-to-site VPNs - Wild card characters are not supported. To find the certificate details (Subject Alternative Name, Distinguished Name, etc.), navigate to the **System > Certificates** page and click on the **Details** icon. DNs are separated by the forward slash character, for example: /C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub

Email ID (UserFQDN): Based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name in Email ID format, that value must be used. If obtaining a new certificate from a CA, you could specify an E-mail ID in the Subject Alternative Name. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the E-Mail ID must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect. For example, *administrator@sonic-lab.local*

Domain Name: Based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name in Domain Name format, that value must be used. If obtaining a new certificate from a CA, you could specify a Domain Name in the Subject Alternative Name. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the Domain Name must be entered. This is





because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect. For example, *sonic-lab.com*

IP Address (IPv4): If the Common Name (CN) or the Subject Alternative Name in the certificate is an IP address, enter the IP address here.

Packet Monitor Diagnostics Restart	System / Certificates	nsa240-vpncert Certificate Issuers	/DC=local/DC=hal-2010/CN=hal-2010.local	
SG/Modem	Certificates and Certificate Reque	Subject Distinguished Name:	/C=IN/ST=KA/L=BLR/O=SonicWALL/CN=nsa240- lab.local	to 6 (of 6)
► ¶ Wireless	View Style: 🔿 All certificates 💌 Ir	Certificate Serial Numbers Valid from:	619C84C500000000031 Jul 22 12-28-38 2012 GMT	ertificates
SonoPoint General	🔄 # Certificate Typ	Expires On:	3ui 22 13-28-38 2014 GMT	s Configure
Frewall Settings	🗐 1 Sonicwall Loc	Alternate Subject Name Alternate Subject Name Type	administratori@nsa240-lab.local n. E-Mail ID	× (*)
VoIP	2 SNWL-2k3Cert Lot	Status:	Verfied	× 🛃
Anti-Spam Anti-Spam	🔄 3 nsa240-vpncert Local	certificate Yes	3ul 22 12:28:38 2014 GMT	8

• **Peer IKE ID Type**: This must be the **Local IKE ID Type** selected in the VPN policy of Site B (NSA 2400) SonicWall. The following can be selected:

Distinguished Name (DN) Email ID (UserFQDN) Domain Name

IP Address (IPv4)

Peer IKE ID: Enter the value of what is selected above.

General	Network Proposals	Advanced	
Security Polic	-y		
Policy Type:		Site to Site	3
Authentication Me	thod:	IKE using 3rd Party Certificates	- ĵ
Name:		VPN To Site A	
IPsec Primary Gat	eway Name or Address:	172.27.61.115	
IPsec Primary Gat IPsec Secondary (eway Name or Address: Sateway Name or Address:	172.27.61.115 0.0.0.0	
IPsec Primary Gat IPsec Secondary (IKE Authentic Local Certificate: Local IKE ID Type:	eway Name or Address: Sateway Name or Address: Cation Remote site must choose Email ID for Peer IKE Type and enter the Email ID in the Sub Alt Name of this site's certificate	172.27.61.115 0.0.0.0 nsa240-vpncert E-Mail ID (UserFQDN)	
IPsec Primary Gat IPsec Secondary (IKE Authentic Local Certificate: Local IKE ID Type: Peer IKE ID Type:	eway Name or Address: Sateway Name or Address: Sation Remote site must choose Email ID for Peer IKE Type and enter the Email ID in the Sub Alt Name of this site's certificate	172.27.61.115 0.0.0.0 nsa240-vpncert E-Mail ID (UserFQDN) Distinguished name (DN)	
IPsec Primary Gat IPsec Secondary (IKE Authentic Local Certificate: Local IKE ID Type: Peer IKE ID Type: Peer IKE ID:	eway Name or Address: Sateway Name or Address:	172.27.61.115 0.0.00 nsa240-vpncert E-Mail ID (UserFQDN) Distinguished name (DN) /C = IN/ST=KA/L=BLR/O=SonicWALL /CN=Site-A-lab.local	

ITCorporation[®] 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



The configuration in the General tab is over. The remaining tabs, Network, Proposals and Advanced, can be configured in the same way as a normal VPN :

Choose local network from list Local network obtains IP addre Any address	sses using DHCP through thi	LAN Subnets s VPN Tunnel	•	IKE (Phase 1) Exchange: DH Group:	Proposal	Main Mode Group 2	•
Choose local network from list Local network obtains IP addre Any address	sses using DHCP through thi	LAN Subnets s VPN Tunnel	•	Exchange: DH Group:		Main Mode Group 2	•
Choose local network from list Local network obtains IP addre Any address	sses using DHCP through thi	LAN Subnets	•	DH Group:		Group 2	-
Cocal network obtains IP addre Any address Comote Networks	sses using DHCP through thi	s VPN Tunnel		erraioep.			•
D Any address				Complete		3DES	
emote Networks				End ypbon:	SHA1	_	
emote Networks				Authentication:	28800		
			-	Life Time (seconds):			
D Use this VPN Tunnel as default	route for all Internet traffic			Ipsec (Phase 2) Proposal		
Destination network obtains IP	addresses using DHCP throu	ugh this VPN Tunnel	_	Dentacals		ESP	
Choose destination network from the second secon	om list.	NSA2400-Network	•	Protocol		3DES	•
				Encryption:		SHA1	
				Authentication:		SHAT	•
				Enable Perfect	Forward Secrecy		
				Life Time (seconds):		28800	
leady			Re	eady			C. Linese
	ОК С	ancel Help			OK	Cancel	Help
[General	Network Prop	sals	Advanced			

Advanced Settings

-				
\checkmark	Enable	Кеер	Alive	1

-

- Suppress automatic Access Rules creation for VPN Policy
- Require authentication of VPN dients by XAUTH
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast

Perm	IT TO	'ΡΔ	nnel	era	tion
 1.200.000	** **			~ ~	- and

Apply NAT Policies

Enable OCSP Checking

Management via this SA:

НТТР НТТР5 User login via this SA:

OK.

Default LAN Gateway (optional):	0.0.0.0	
VPN Policy bound to:	Zone WAN	

🗏 HTTP 🛄 HTTPS 📃 SSH

Cancel

Ready	

Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290/+57 318 4914652 sales@itclatam.com/tss@itclatam.com REV1.01

-

Help

ITCorporation[®] Visit our Website: www.itclatam.com



The check box **Enable OCSP Checking** can be optionally enabled if an OCSP responder is available in the network. Click on OK to complete the configuration.

Testing:

Initiate a ping from Site B (NSA 240) to an internal IP address in Site A (NSA 2400) should bring the tunnel come up. A green button alongside the VPN policies will indicate the tunnel is up.

If the tunnel does not come up due to mis-configuration in the Local or Remote IKE ID, the logs will clearly indicate where the error is. For example the following log message appears in the initiator (Site B in this scenario):

Warning VPN IKE IKE Responder: Proposed IKE ID mismatch 172.27.61.115, 500 192.168.170.51, 500 VPN Policy: VPN to Site A; ID Type Mismatch. Local: UserFQDN; Peer: DN

The above message indicates that there is a mismatch in the Local and Peer IKE IDs in either of the VPN policies. The Peer IKE ID in this side's (Site B) VPN policy has been set to Email Address but the Local IKE ID in Site A has been set to Distinguished DN.

