ITCorporation

SONICWALL®

SecureFirst

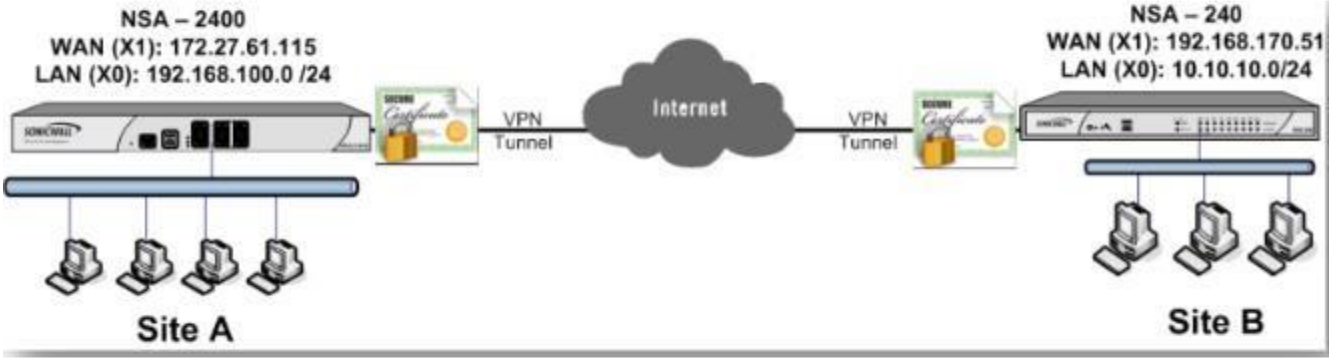
Site to Site VPN Using Certificates

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 : **How to obtain a Certificate from a Windows Certificate Authority (CA)**
- Refer this KB article to obtain a signed certificate from a public CA: **How to Request and Import a Signed Certificate from Thawte**

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.

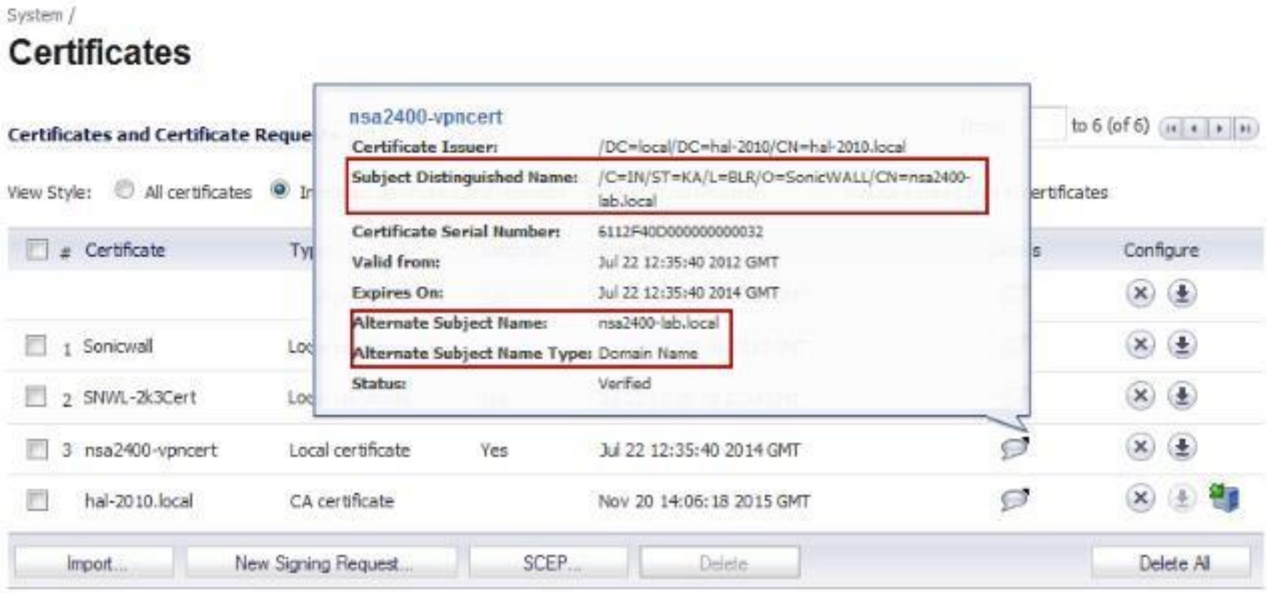
- Login to the SonicWall management GUI
- Navigate to the VPN page.
- Click on **Add** to open to the **General** tab of the **VPN Policy** window.
- The **General** tab is where most of the certificate specific information is entered.
- **Policy Type**: Site to Site
- **Authentication Method**: IKE 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 (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.



System /

Certificates

Certificates and Certificate Reque

View Style: ○ All certificates ● I ertificates

to 6 (of 6)

nsa2400-vpncert

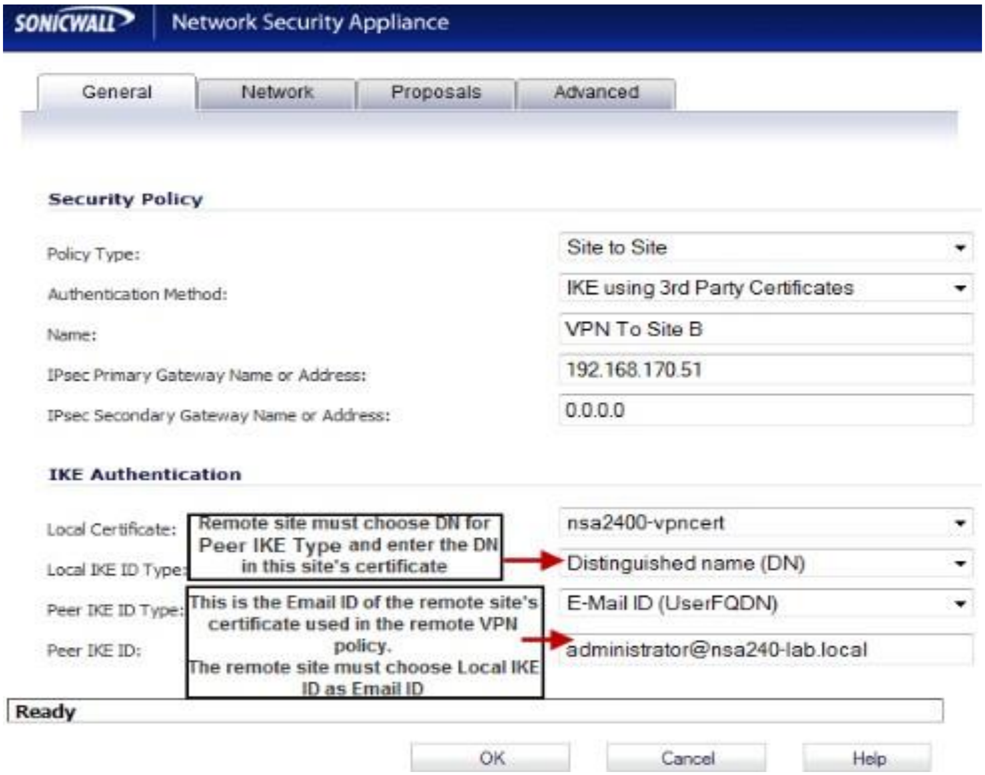
Certificate Issuer:	/DC=local/DC=hal-2010/CN=hal-2010.local
Subject Distinguished Name:	/C=IN/ST=KA/L=BLR/O=SonicWALL/CN=nsa2400-lab.local
Certificate Serial Number:	6112F40D000000000032
Valid from:	Jul 22 12:35:40 2012 GMT
Expires On:	Jul 22 12:35:40 2014 GMT
Alternate Subject Name:	nsa2400-lab.local
Alternate Subject Name Type:	Domain Name
Status:	Verified

□ #	Certificate	Ty			s	Configure
						☒ ⬇
□ 1	Sonicwall	Lo				☒ ⬇
□ 2	SNWL-2k3Cert	Lo				☒ ⬇
□ 3	nsa2400-vpncert	Local certificate	Yes	Jul 22 12:35:40 2014 GMT	💬	☒ ⬇
□	hal-2010.local	CA certificate		Nov 20 14:06:18 2015 GMT	💬	☒ ⬇

- **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.



Security Policy

Policy Type:	Site to Site
Authentication Method:	IKE using 3rd Party Certificates
Name:	VPN To Site B
IPsec Primary Gateway Name or Address:	192.168.170.51
IPsec Secondary Gateway Name or Address:	0.0.0.0

IKE Authentication

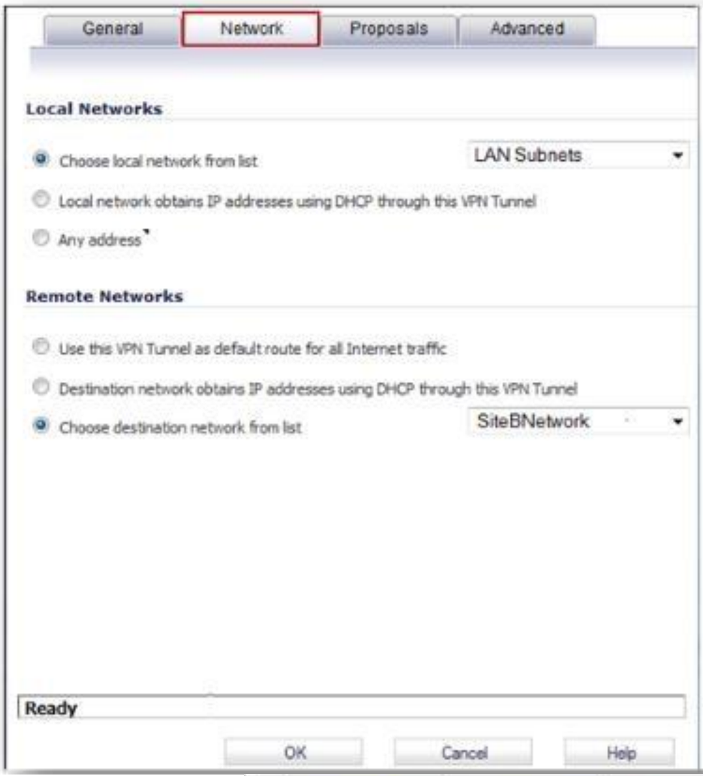
Local Certificate:	nsa2400-vpncert
Local IKE ID Type:	Distinguished name (DN)
Peer IKE ID Type:	E-Mail ID (UserFQDN)
Peer IKE ID:	administrator@nsa240-lab.local

Remote site must choose DN for Peer IKE Type and enter the DN in this site's certificate

This is the Email ID of the remote site's certificate used in the remote VPN policy. The remote site must choose Local IKE ID as Email ID

Ready

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 :



Local Networks

● Choose local network from list: LAN Subnets

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

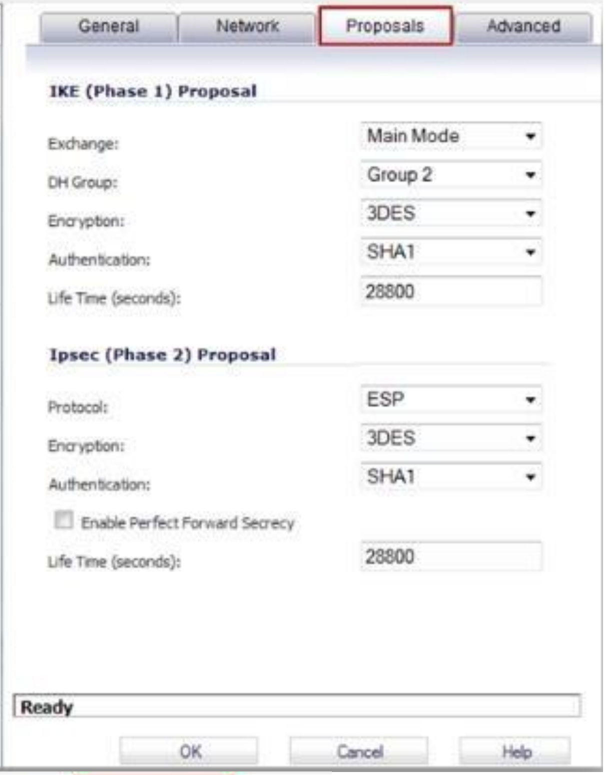
Remote Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list: SiteBNetwork

Ready



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

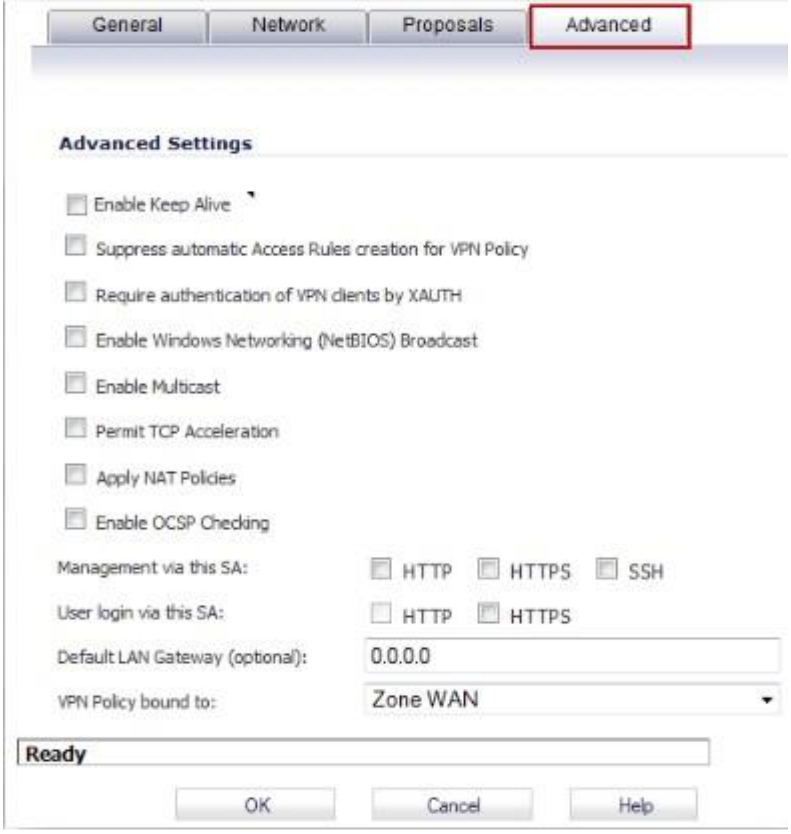
Encryption: 3DES

Authentication: SHA1

□ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Ready



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Require authentication of VPN clients by XAUTH

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Permit TCP Acceleration

□ Apply NAT Policies

□ Enable OCSP Checking

Management via this SA: □ HTTP □ HTTPS □ SSH

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Zone WAN

Ready

Site B (NSA 240) configuration

Obtain a signed certificate

- Refer this KB article to obtain a signed certificate from a Microsoft CA : **UTM: How to obtain a Certificate from a Windows Certificate Authority (CA)**
- Refer this KB article to obtain a signed certificate from a public CA: **UTM: How to Request and Import a Signed Certificate from Thawte**

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.

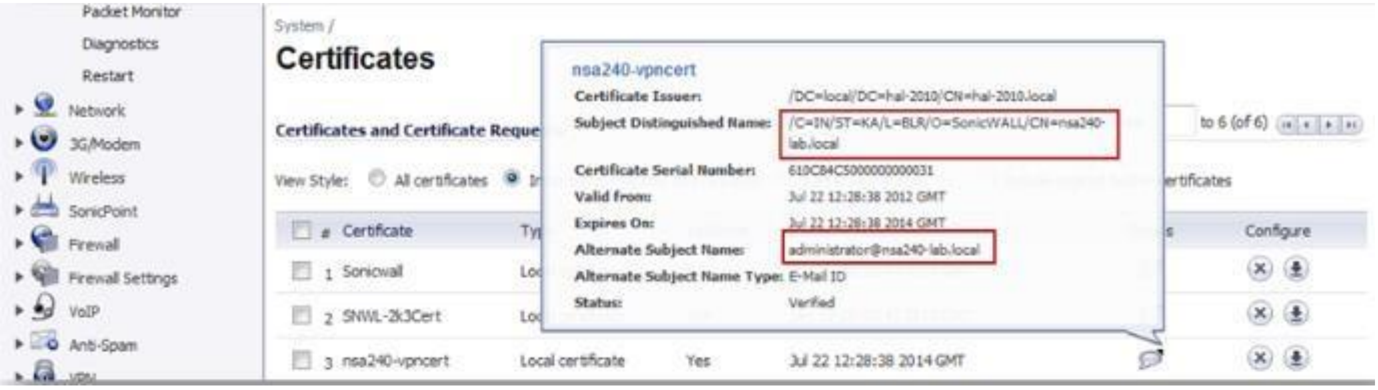
- Login to the SonicWall management GUI
- Navigate to the VPN page.
- Click on **Add** to open to the **General** tab of the **VPN Policy** window.
- The **General** tab is where most of the certificate specific information is entered.
- **Policy Type**: Site to Site
- **Authentication Method**: IKE 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.



nsa240-vpncert

Certificate Issuer: /DC=local/DC=hal-2010/CN=hal-2010.local

Subject Distinguished Name: /C=IN/ST=KA/L=BLR/O=SonicWALL/CN=nsa240-lab.local

Certificate Serial Number: 610C84C5000000000031

Valid from: Jul 22 12:28:38 2012 GMT

Expires On: Jul 22 12:28:38 2014 GMT

Alternate Subject Name: administrator@nsa240-lab.local

Alternate Subject Name Type: E-Mail ID

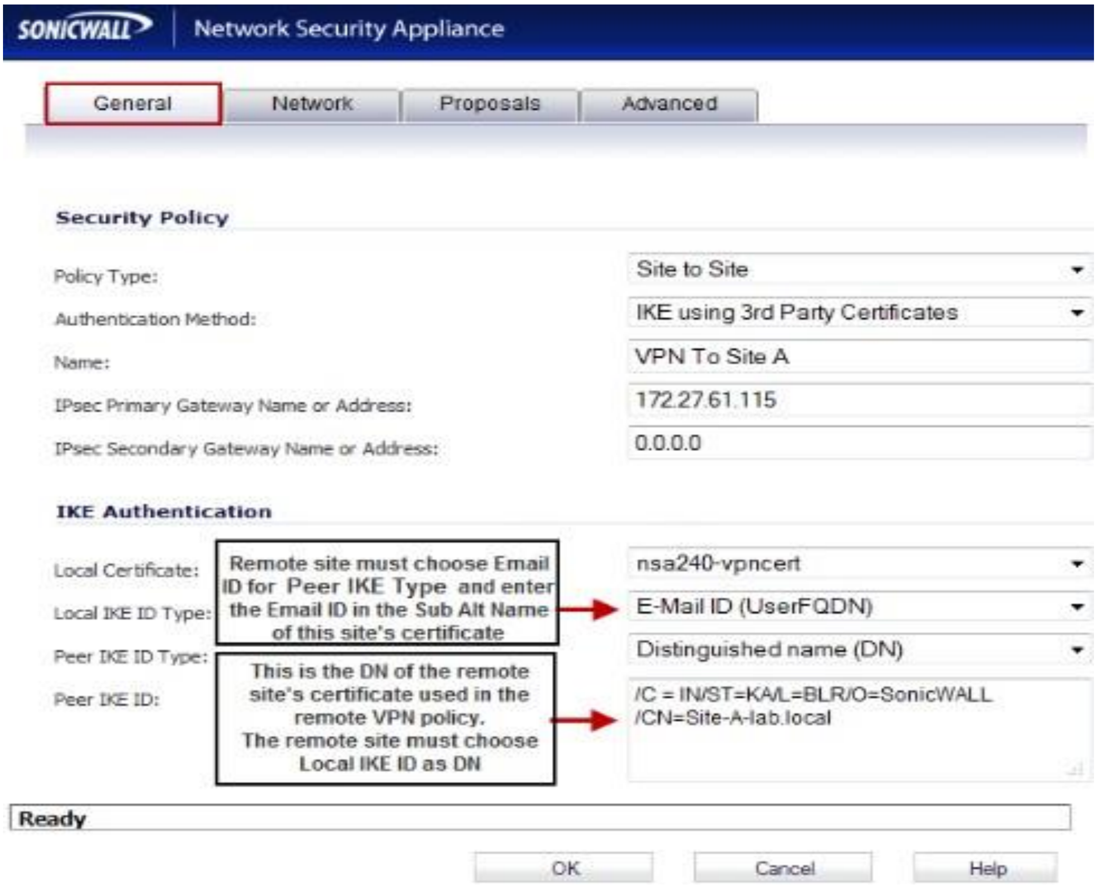
Status: Verified

	#	Certificate	Type		
□	1	Sonicwall	Loc		
□	2	SNWL-2k3Cert	Loc		
□	3	nsa240-vpncert	Local certificate	Yes	Jul 22 12:28:38 2014 GMT

- **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.



Security Policy

Policy Type: Site to Site

Authentication Method: IKE using 3rd Party Certificates

Name: VPN To Site A

IPsec Primary Gateway Name or Address: 172.27.61.115

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

Local Certificate: nsa240-vpncert

Local IKE ID Type: E-Mail ID (UserFQDN)

Peer IKE ID Type: Distinguished name (DN)

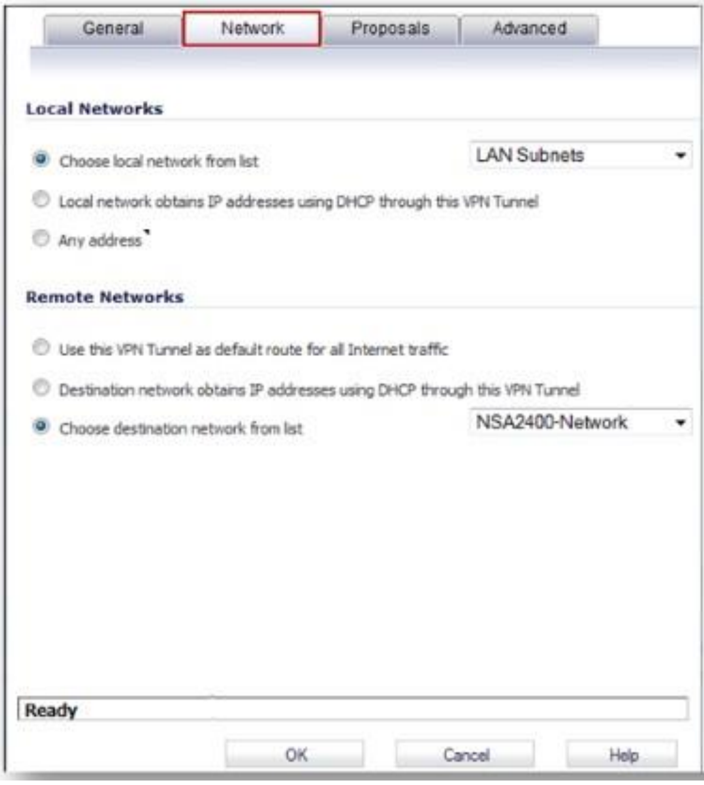
Peer IKE ID: /C = IN/ST=KA/L=BLR/O=SonicWALL /CN=Site-A-lab.local

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

This is the DN of the remote site's certificate used in the remote VPN policy. The remote site must choose Local IKE ID as DN

Ready

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 :



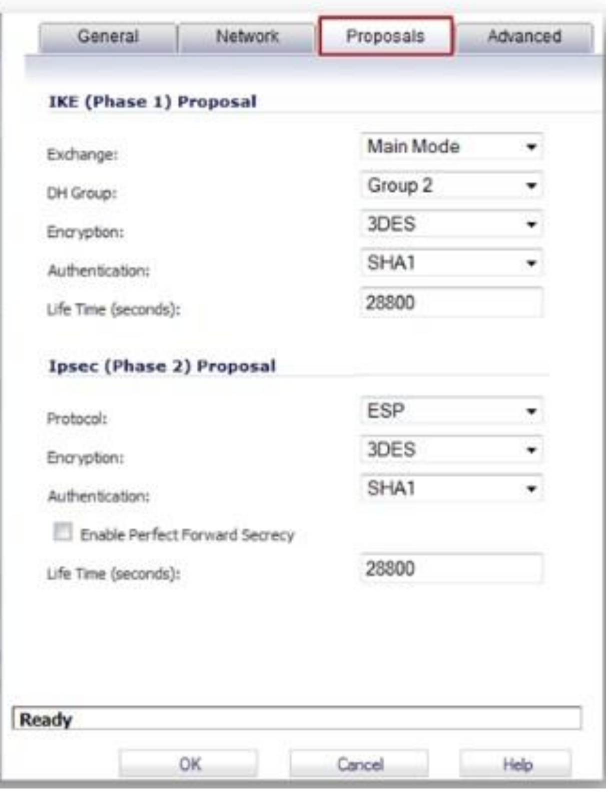
Local Networks

- ● Choose local network from list: LAN Subnets
- ○ Local network obtains IP addresses using DHCP through this VPN Tunnel
- ○ Any address

Remote Networks

- ○ Use this VPN Tunnel as default route for all Internet traffic
- ○ Destination network obtains IP addresses using DHCP through this VPN Tunnel
- ● Choose destination network from list: NSA2400-Network

Ready



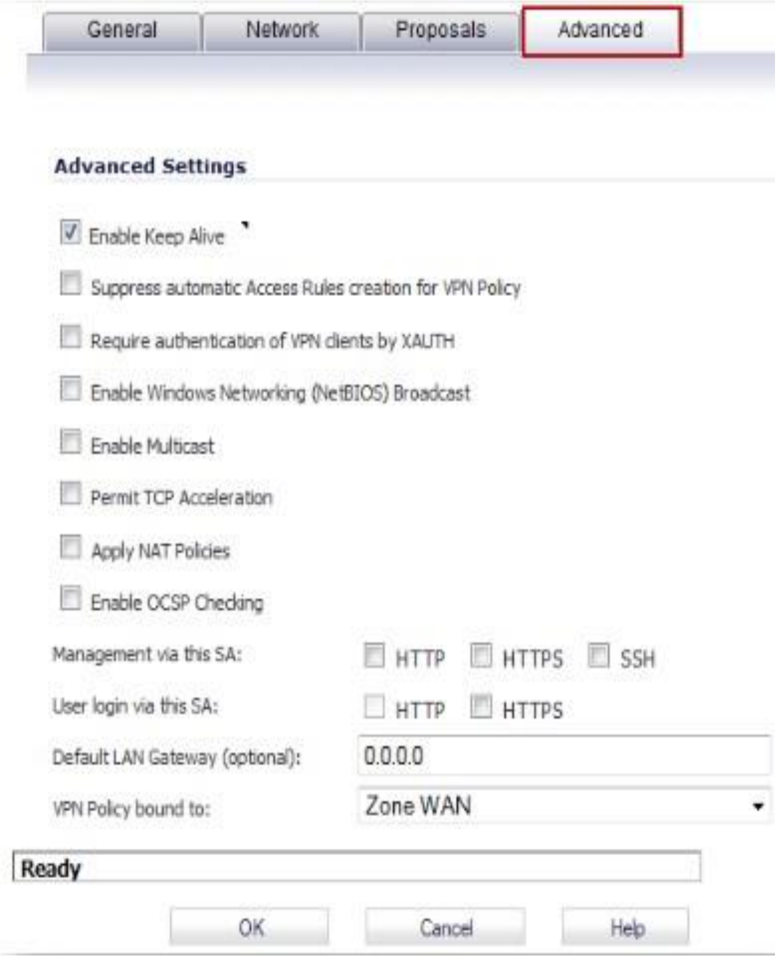
IKE (Phase 1) Proposal

Exchange: Main Mode
DH Group: Group 2
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP
Encryption: 3DES
Authentication: SHA1
□ Enable Perfect Forward Secrecy
Life Time (seconds): 28800

Ready



Advanced Settings

- ☑ Enable Keep Alive
- □ Suppress automatic Access Rules creation for VPN Policy
- □ Require authentication of VPN clients by XAUTH
- □ Enable Windows Networking (NetBIOS) Broadcast
- □ Enable Multicast
- □ Permit TCP Acceleration
- □ Apply NAT Policies
- □ Enable OCSP Checking

Management via this SA: □ HTTP □ HTTPS □ SSH
User login via this SA: □ HTTP □ HTTPS
Default LAN Gateway (optional): 0.0.0.0
VPN Policy bound to: Zone WAN

Ready

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.