How to setup Site to Site VPN with IKE2 Dynamic Client Proposal in SonicOS 6.2 and above

KNOWLEDGE DATABASE

SONICWALL
Knowledge Database

How to setup Site to Site VPN with IKE2 Dynamic Client Proposal in SonicOS 6.2 and above

Feature/Application:

SonicOS provides IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes globally rather than configure these IKE Proposal settings on an individual policy basis. This scenario could be used while one site has dynamic WAN IP address.
And then on the other site, "IPsec Primary Gateway Name or Address" in the VPN policy General tab will be filled in "0.0.0.0" or left blank.

Procedure:

Cconfiguration on the Central Office (Static WAN IP address)

Central location network configuration:

1. LAN Subnet: **192.168.136.0**
2. Subnet Mask: **255.255.255.0**
3. WAN IP: **10.103.193.114**
4. Local IKE ID SonicWall Identifier: Shanghai (This could be any string except it has to match the remote location VPN's Peer IKE ID SonicWall Identifier)

Step 1: Creating **Address Object** for **remote Site:**

- Login to the central location SonicWall appliance
- Navigate to **Network > Address Objects** page.
- Scroll down to the bottom of the page and click on **Add** button, enter the following settings.

Name – **Remote_Lan**,
Zone – **VPN**,
Type – **Network**,
Network – **192.168.126.0**,
Netmask – **255.255.255.0**

- Click **OK** when finished.

Step 2: Configuring a VPN Policy:

a. Click on ***VPN > Settings***
b. Check the box "***Enable VPN***" under Global VPN Settings.
c. Click on the "***Add***" button under VPN Policies section. The VPN Policy window pops up.

Click the **General** tab

a. Select the Authentication method as "**IKE Using Preshared Secret**"
b. Name: **To_Branch_Office**
c. IPsec Primary Gateway Name or Address: **0.0.0.0**

Note: Since the Remote WAN IP address changes frequently, it is recommended to use the 0.0.0.0 IP address as the Primary Gateway.

d. IPsec Secondary Gateway Name or Address: **0.0.0.0**
e. Shared Secret: **SonicWall** (The Shared Secret would be the same at both SonicWall's)
f. Local IKE ID: SonicWall Identifier - **Shanghai** (This could be any string except it has to match the remote location VPN's **Peer IKE ID SonicWall Identifier**)
g. Peer IKE ID: SonicWall Identifier - **San Jose** (This could be any string except it has to match the remote location VPN's **Local IKE ID SonicWall Identifier**)

Click the **Network** tab

Ø Local Networks

Select **Choose local network from list,** and select the Address Object – **X0 Subnet** (Lan subnet)

Ø Destination Networks

Select **Choose destination network from list,** and select the Address Object –**Remote_Lan**

Click the **Proposals** tab

IKE (Phase 1) Proposal

Exchange: **IKEv2 Mode**
DH Group: Group 5
Encryption: AES-256
Authentication: SHA-512
Life Time (seconds): **28800**

Note: The menu "DH Group", "Encryption" and "Authentication" will be gray-out since "IPsec Primary Gateway Name or Address" in General tab is filled in "0.0.0.0" or leaved blank. And they will be configured in step 3.

IPsec (Phase 2) Proposal

Protocol: **ESP**
Encryption: **3DES**
Authentication: **SHA1**

Enable Perfect Forward Secrecy(not checked)

Click the **Advanced** tab

Ensure that the **VPN Policy bound to: Zone WAN**

- Click **OK** when finished

Step 3: Configuring the IKEv2 Dynamic Client Proposal:

a. Click on ***VPN > Advanced***
b. Check the "***Configuration***" under IKEv2 Settings. The configuration window pops up
DH Group: Group 5
Encryption: AES-256
Authentication: SHA-512
c. Click OK when finished

Configuration on the remote location (Dynamic WAN IP address)

Network Configuration:

1. LAN Subnet: **192.168.126.0**
2. Subnet Mask: **255.255.255.0**
3. WAN IP: DHCP (As this is a Dynamic IP Address)
4. Local IKE ID SonicWall Identifier: **San**

Jose (This has to match the central location VPN's**Peer IKE ID SonicWall Identifier**)

Step 1: Creating **Address Object** for **remote site:**

- Login to the Remote location SonicWall appliance
- Navigate to **Network > Address Objects** page.
- Scroll down to the bottom of the page and click on **Add** button, enter the following settings.
Name – **Central_Lan**
Zone – **VPN**
Type – **Network**
Network – **192.168.136.0**
Netmask – **255.255.255.0**
- Click **OK** when finished

Step 2: Configuration VPN Policy:

a. Click on ***VPN > Settings***
b. Check the box "***Enable VPN***" under Global VPN Settings.
c. Click on the "***Add***" button under the VPN Policies section. The VPN Policy window pops up.

Click the **General** tab

a. Select the Authentication method as "**IKE Using Preshared Secret**"
b. Name: **To_Central_Office**
c. IPsec Primary Gateway Name or Address: **10.103.193.114**
d. IPsec Secondary Gateway Name or Address: **0.0.0.0**
e. Shared Secret: **SonicWall**
f. Local IKE ID: SonicWall Identifier - **San**
Jose (This has to match the central location VPN's **Peer IKE ID SonicWall Identifier**)
g. Peer IKE ID: SonicWall Identifier – **Shanghai** (This has to match the central location VPN's **Local IKE ID SonicWall Identifier**)

Click the **Network** tab

Ø Local Networks

Select **Choose local network from list,** and select the Address Object – **LAN Primary Subnet**

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com

Ø Destination Networks

Select **Choose destination network from list**, and select the Address Object – **Central_Lan**

Click the **Proposals** tab

IKE (Phase 1) Proposal

Exchange: **IKEv2 Mode**
DH Group: **Group 5**
Encryption: **AES-256**
Authentication: **SHA-512**
Life Time (seconds): **28800**

IPsec (Phase 2) Proposal

Protocol: **ESP**
Encryption: **3DES**
Authentication: **SHA1**

Enable Perfect Forward Secrecy (not checked)

Click the **Advanced** tab

Enable Keep Alive box should be checked
VPN Policy bound to: **Zone WAN**
- Click **OK** when finished

How to Test:

From the remote location try to ping an IP address on the central location.
Note: Before receiving successful replies, you might see couple of "Request Timed Out" messages while the VPN tunnel is still establishing.

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.

Feature/Application:
SonicOS provides IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes globally rather than configure these IKE Proposal settings on an individual policy basis. This scenario could be used while one site has dynamic WAN IP address.
And then on the other site, "IPsec Primary Gateway Name or Address" in the VPN policy General tab will be filled in "0.0.0.0" or left blank.

Procedure:

Cconfiguration on the Central Office (Static WAN IP address)

- **Central location network configuration**:

1. LAN Subnet: **192.168.136.0**
2. Subnet Mask: **255.255.255.0**
3. WAN IP: **10.103.193.114**
4. Local IKE ID SonicWall Identifier: Shanghai (This could be any string except it has to match the remote location VPN's Peer IKE ID SonicWall Identifier)

Step 1: Creating **Address Object** for **remote Site:**

- Login to the central location SonicWall appliance
- Navigate to **Manage > Policies >Objects > Address Objects** page.
- At the top of the page and click on **Add** button, enter the following settings.

Name – **Remote_Lan**,
Zone – **VPN**,
Type – **Network**,
Network – **192.168.126.0**,
Netmask – **255.255.255.0**

- Click **OK** when finished.

Step 2: Configuring a VPN Policy:

a. Click on ***Manage > Connectivity > VPN > Base Settings***
b. Check the box "***Enable VPN***" under Global VPN Settings.
c. Click on the "***Add***" button under VPN Policies section. The VPN Policy window pops up.

Click the **General** tab

a. Select the Authentication method as "**IKE Using Preshared Secret**"
b. Name: **To_Branch_Office**
c. IPsec Primary Gateway Name or Address: **0.0.0.0**

Note: Since the Remote WAN IP address changes frequently, it is recommended to use the 0.0.0.0 IP address as the Primary Gateway.

d. IPsec Secondary Gateway Name or Address: **0.0.0.0**
e. Shared Secret: **SonicWall** (The Shared Secret would be the same at both SonicWall's)
f. Local IKE ID: SonicWall Identifier - **Shanghai** (This could be any string except it has to match the remote location VPN's **Peer IKE ID SonicWall Identifier**)
g. Peer IKE ID: SonicWall Identifier - **San Jose** (This could be any string except it has to match the remote location VPN's **Local IKE ID SonicWall Identifier**)

Click the **Network** tab

Ø Local Networks

Select **Choose local network from list,** and select the Address Object – **X0 Subnet** (LAN subnet)

Ø Destination Networks

Select **Choose destination network from list,** and select the Address Object – **Remote_Lan**

Click the **Proposals** tab

IKE (Phase 1) Proposal

Exchange: **IKEv2 Mode**
DH Group: Group 5
Encryption: AES-256
Authentication: SHA-512
Life Time (seconds): **28800**

Note: The menu "DH Group", "Encryption" and "Authentication" will be gray-out since "IPsec Primary Gateway Name or Address" in General tab is filled in "0.0.0.0" or leaved blank. And they will be configured in step 3.

IPsec (Phase 2) Proposal

Protocol: **ESP**
Encryption: **3DES**
Authentication: **SHA1**

Enable Perfect Forward Secrecy(not checked)

Click the **Advanced** tab

Ensure that the **VPN Policy bound to: Zone WAN**

- Click **OK** when finished

Step 3: Configuring the IKEv2 Dynamic Client Proposal:

a. Click on ***Manage > Connectivity > VPN > Advanced Settings***
b. Check the "***Configuration***" under IKEv2 Settings. The configuration window pops up
DH Group: Group 5
Encryption: AES-256
Authentication: SHA-512
c. Click OK when finished.

Configuration on the remote location (Dynamic WAN IP address)

Network Configuration:

1. LAN Subnet: **192.168.126.0**
2. Subnet Mask: **255.255.255.0**
3. WAN IP: DHCP (As this is a Dynamic IP Address)
4. Local IKE ID SonicWall Identifier: **San Jose** (This has to match the central location VPN's**Peer IKE ID SonicWall Identifier**)

Step 1: Creating **Address Object** for **remote site:**

- Login to the Remote location SonicWall appliance
- Navigate to **Manage > Policies >Objects > Address Objects** page.
- Scroll down to the bottom of the page and click on **Add** button, enter the following settings.

Name – **Central_Lan**
Zone – **VPN**
Type – **Network**
Network – **192.168.136.0**
Netmask – **255.255.255.0**
- Click **OK** when finished

Step 2: Configuration VPN Policy:

-Click on ***Manage > Connectivity > VPN > Base Settings.***
-Check the box "***Enable VPN***" under Global VPN Settings.
-Click on the "***Add***" button under the VPN Policies section. The VPN Policy window pops up.

Click the **General** tab

a. Select the Authentication method as "**IKE Using Preshared Secret**"
b. Name: **To_Central_Office**
c. IPsec Primary Gateway Name or Address: **10.103.193.114**
d. IPsec Secondary Gateway Name or Address: **0.0.0.0**
e. Shared Secret: **SonicWall**
f. Local IKE ID: SonicWall Identifier - **San Jose** (This has to match the central location VPN's **Peer IKE ID SonicWall Identifier**)
g. Peer IKE ID: SonicWall Identifier – **Shanghai** (This has to match the central location VPN's **Local IKE ID SonicWall Identifier**)

Click the **Network** tab

Ø Local Networks

Select **Choose local network from list,** and select the Address Object – **LAN Primary Subnet**

Ø Destination Networks

Select **Choose destination network from list**, and select the Address Object – **Central_Lan**

Click the **Proposals** tab

IKE (Phase 1) Proposal

Exchange: **IKEv2 Mode**
DH Group: **Group 5**
Encryption: **AES-256**
Authentication: **SHA-512**
Life Time (seconds): **28800**

IPsec (Phase 2) Proposal

Protocol: **ESP**
Encryption: **3DES**
Authentication: **SHA1**

Enable Perfect Forward Secrecy (not checked)

Click the **Advanced** tab

Enable Keep Alive box should be checked
VPN Policy bound to: **Zone WAN**
- Click **OK** when finished.

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com