Configuring a Site to Site IPsec between the SBC Gateways

This article describes the steps necessary to configure the Sonus SBC 1000/2000 for IPsec.

On this Page

Related Articles

- Creating and Modifying IPsec Tunnel Entries

Overview

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. The IPsec enabled SBC gateway secures data transmission between the subnets behind the branch remote offices and the corporate headsquarters (HQ). IPsec tunnels are established and maintained to provide for data privacy, integrity, authenticity, and anti-replay protection for network traffic over Internet-based connections.

Site to Site IPsec Settings in a Nutshell

The procedures outlined in this document are best practice recommendations and guidelines for the steps requires to set up an IKEv2 connection between Sonus SBC 1000/2000 gateways with IPSec Tunnel Tables.

First, determine how to authenticate both SBC IPsec enabled peers to each other. Configure a preshared key as a strong pass-phrase or install a digital RSA certificate with a stronger 2048-bit key option. This is used for authentication and to ensure the IPsec gateways are authorized by proving their identities to each other. Both gateways must use the same type of credentials – either preshared keys or digital certificates. Preshared keys are shared with the gateway peer, therefore both keys must match.

The tunnel connection definition is configured and negotiated in two phases. In phase 1, set up a secure and encrypted channel (required to protect the phase 2 negotiations). In phase 2, establish the IPSec Security Association (SA) to tell the gateway what traffic is being sent over the tunnel, and how to encrypt and authenticate it.

Phase 1 Settings

- Specify both SBC gateway addresses. Specify the address of the local SBC gateway and the address of the remote SBC gateway as an IP address or a Fully Qualified Domain Name(FQDN).
- Specify the authentication mode as preshared key or certificate. When using the digital certificate, specify the subject Distinguished Name (DN) field or the Subject Alternative Name (x509v3 Extension SAN field) of the peer's certificate. If certificates is not used, as recommended for larger deployments where security measures are of concern, then specify a long and complex preshared key. The preshared key must be a strong password or a pass-phrase represented as hexadecimal or Base64 encoded binary values.
- Choose a transform set, which includes the type of encryption, authentication and how long the security association will last. Select Sha256 if required to use a stronger authentication algorithm. Select either 3DES or AES 128, 256 bit key strength for encryption. Select AES 256 as this is the strongest encryption protocol. Specify a Diffie-Hellman key group, usually 1, 2, 5 or 14 (14 is the most secure group).
- Specify an IKE lifetime for the IKE SA, which adds more security to SBC gateway if the keys have been hacked. Although this will also have a slight affect on performance as well.

Phase 2 Settings

- Specify what traffic will go across the tunnel using the IP address, Network address, or IP address range. This is access to the SBC gateway's internal network, so either remote users from home, or the peer office can have access to resources behind the SBC IPsec enabled gateway.
- Choose whether to use Perfect Forward Secrecy (PFS), for optional and an extra layer of security. When enabling PFS, both SBC gateway peers must support and use PFS. Select which Diffie-Hellman group to use for new keying material. The higher the group selected such as DH Group 14, the stronger the key.
- Specify the encryption and authentication algorithms, securing the data in the IPsec SA (Phase 2 Proposal). The only type of proposal supported on the SBC gateway is ESP to provide authentication and encryption. Specify the authentication and encryption algorithm and protocol which will be the same as ones chosen for Phase 1 settings as to simplify the configuration steps when establishing the tunnel with another SBC gateway peer.
- Specify the IPsec lifetime for the IPsec SA. This ensures that the encryption keys change over a period of time and have them recreated, adding more security, as well as having a slight affect on performance.

Final steps

- Create policies or rules that allow the tunneled traffic in and out of the firewall based on the topology firewalling requirements. The option to either enable or disable the firewall policy rules on SBC IPsec enabled gateway will automatically insert the policy based match traffic rules.

- Configure the SBC gateway peer with the exactly the same settings and/or the reverse of its peer's settings as configured on the local gateway for some of the fields. If the peer settings are not reversed, this will result in a failure to establish a tunnel and it's service status will appear as **Down**.

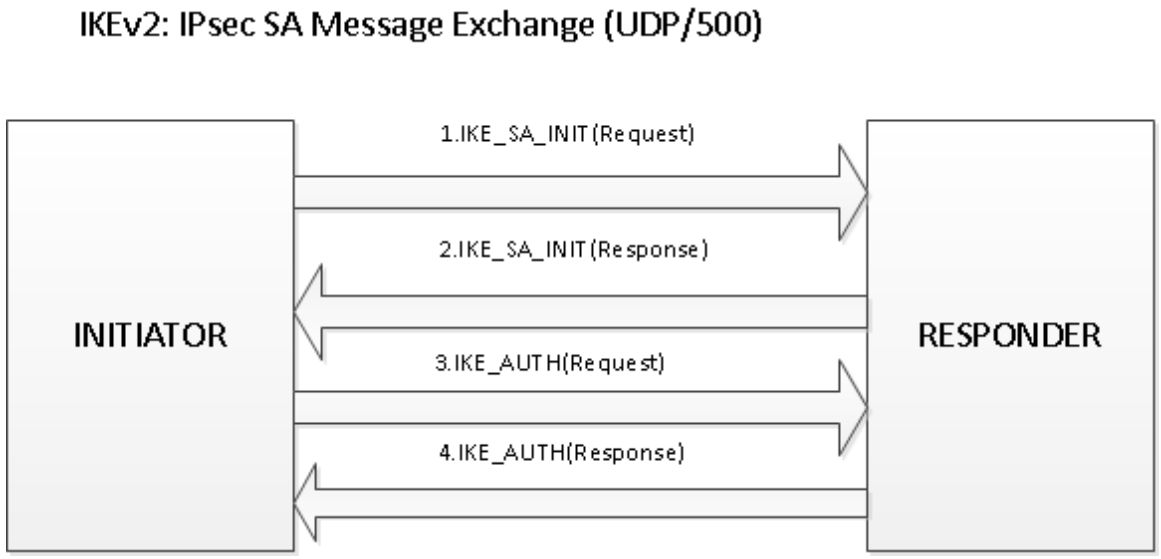
IKEv2 SA Message Exchange Flow

Internet Key Exchange (IKE) is accessed via UDP port 500. IP port 50 must be used for the Encapsulating Security Payload (ESP). The NAT Traversal is assigned to UDP port 4500.

When NAT is present, UDP port 4500 is used in the tunnel path.

IKE SA

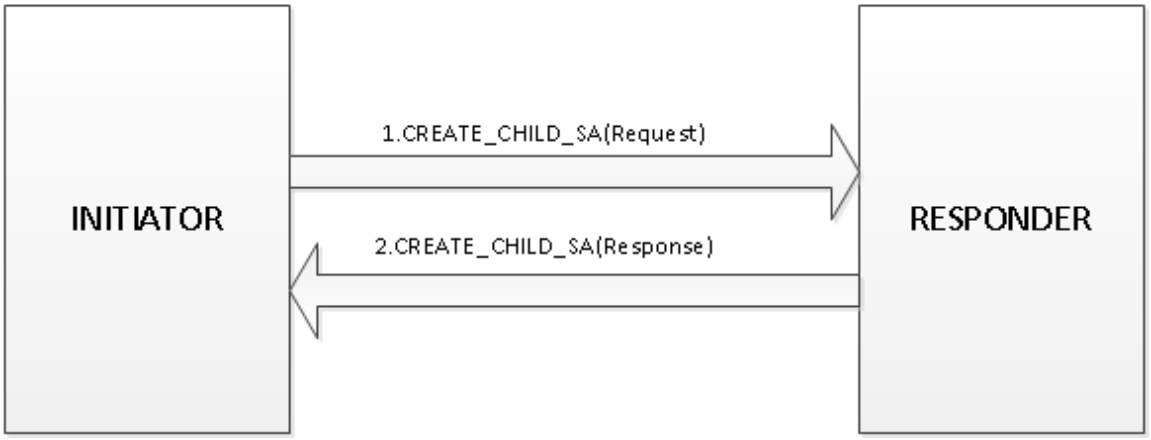
The establishment of a single IKE SA using the IKEv2 protocol requires an exchange of four UDP datagrams as shown in the illustration below. The task of resending messages falls to the initiator only. The IKE_SA_INIT message carries the selection of cryptographic transforms for the IKE SA, the derivation of a common Diffie-Hellman secret and the nonces into a single exchange. The IKE_AUTH message authenticates the peers using the pre-shared keys(PSK)or the RSA signatures supported by the SBC to create the first so-called Child SA by defining the traffic selectors and cryptographic transforms for the IPsec connection.



IPsec SA

The establishment of a single or multiple Child SA using the IKEv2 protocol requires an exchange of a CREATE_CHILD_SA request/response pair as shown in the following illustration. The message carries the cryptographic transforms, a pair of fresh nonces, an optional Diffie-Hellman exchange if PFS is desired and the additional traffic selectors.

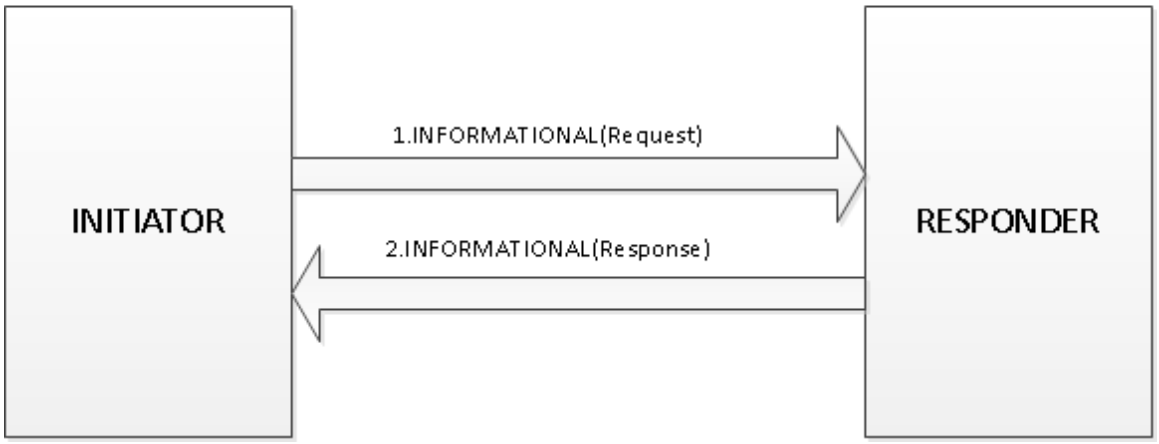
IKEv2: CREATE_CHILD_SA Message Exchange (UDP/500)



Dead Peer Detection Keep-Alive

The SBC gateway defines a hard-coded time interval of 30s with which keep-alive INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. All connections with a dead peer are stopped and unrouted. The gateway also defines a hard-coded timeout interval of 60s, after which all connections to a peer are deleted and the IKE and Child Security Associations(SA) are cleared in case of inactivity.

IKEv2: INFORMATIONAL Message Exchange (UDP/500)



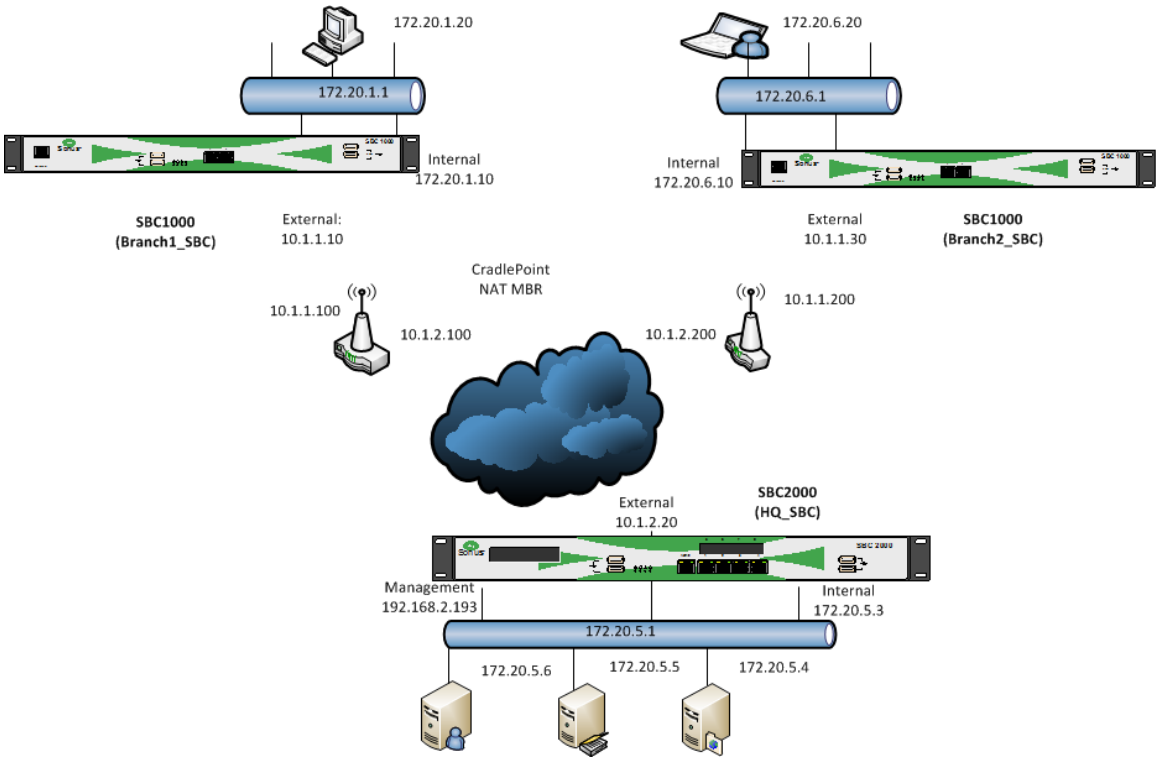
Prerequisites

- An IPsec license is required to manage IPsec tunnels.
- A Sonus SBC Certificate and Trusted CA Certificate must be obtained and imported to the SBC when Certificate is selected from the Authentication Mode list box in the Authentication Parameters panel. Refer to Working with Certificates for information about configuring certificates on the SBC.
- When upgrading to version 3.0 existing Sonus SBC Certificates will fail authentication due to key integrity verification errors when used to bring up the IPsec tunnel in the Certificate authentication mode. Before beginning to manage an IPsec tunnel for Certificate authentication, must generate a new Certificate Signing Request (CSR), re-sign, and re-import a new Sonus SBC Certificate.

Related Documentation

Network Topology Diagram

The configuration settings and examples in following sections are based on network a topology comprising a single SBC gateway at two different branch sites, behind an external NAT accessing the corporate gateway or the servers in the subnet behind the corporate gateway over public internet access.



General Configuration Notes

The following information refers to the Create IPsec Tunnel Entry page of the SBC 1000/2000 user interface.
For more information see: Managing IPsec Tunnels and Creating and Modifying IPsec Tunnel Entries.

Networking Properties

- Specify the local and remote site peer address (outside interface IP of the SBC gateway).
- Configure the local host internal subnet to allow traffic to and from the selected hosts/networks at the remote site.

> **Information Note:**
> Any or all IP traffic (0.0.0.0/0) subnets is not a supported configuration for the Local Subnet Addresses attribute. It is supported for the Remote Subnet Addresses attribute as the peer needs to define the specific host addresses in properly establishing the IPsec SA traffic selector policies.

- A maximum of 10 subnet addresses can be configured per tunnel connection entry.
- When specifying the local and/or remote site peer address as an FQDN address type, the DNS Server must be configured to resolve the FQDN.

Important Note:
The local and remote site peer address type selected as either IP or FQDN on the branch office SBC, must be the same address type configured on the headquarters SBC. The address type on both peers must be the same type (e.g., IP or FQDN). For example, the **Local Address** configured with an IP on branch office SBC will not be able match the peer config that has the **Remote Address** configured as FQDN address type on the headquarters SBC. This can be addressed by one of two possible ways: 1) Configure the **Remote Address** as FQDN on the headquarters SBC which is the same address type configured on the peer SBC. or 2) Enable **Allow any Remote Address** field on the headquarters SBC to match either address type.

Operating Mode

- **Initiator**
  Either an SBC 1000 or an SBC 2000 IPsec enabled gateway can be deployed at branch offices sites which will negotiate the tunnel in an active mode of operation.
- **Responder**
  An SBC 2000 IPsec enabled gateway must be deployed at the corporate site premises and waits, in a passive mode, for tunnels to be initiated by the branch office IPsec enabled gateway peer(s).

Tunnel Activation

This setting is applicable for the IPsec enabled gateway configured in an **Initiator** mode of operation.

- **Always**
  It is used to activate a permanent and/or stand-alone tunnel establishment. This setting should be used mainly for the purposes of confirming that the tunnel is being established with the proper configurations and/or troubleshooting the connection failures in the field.
- **Link Monitor Action**
  This is the default recommended setting for the tunnel to be activated and negotiated with the peer in an on-demand mode. The on-demand tunnel activation is performed by the branch survivability 3G4G fail-over feature. Refer to Configuring 3G4G Failover guidelines which covers configuration of the 3G4G fail-over feature on the Sonus SBC 1000/2000 under the Working with Branch Survivability section.

Branch1_SBC Tunnel Connection Definition

1. **Tunnel Name**: Branch1_SBC
2. **Local Address**: Ethernet 2 IP(10.1.1.10)

   Note:
   Alternatively configured as FQDN (eg: branch1sbc.uxdev.com), when the **Remote Address** is also configured the same on the headquarters SBC. Another alternative is to enable the **Allow Any Local Address** which automatically selects any local or outside interface IP.

3. **Remote Address**: 10.1.2.20

   Note:
   Alternatively configured as FQDN (eg: hqsbc.uxdev.com), when the **Local Address** is also configured the same on the headquarters SBC.

4. **Local Subnet Addresses**: 172.20.1.10/32,172.20.1.20/32

   Note:
   Alternatively configured as subnet address range such as 172.20.1.0/24.

5. **Remote Subnet Addresses**: 172.20.5.0/24

Note:

Alternatively configured as specific host addresses with CIDR mask value 32. Also, can be configured as 0.0.0.0/0 to accept all IP traffic which the HQ SBC peer specifically defines in the **Local Subnet Addresses**.

Branch2_SBC Tunnel Connection Definition

1. **Tunnel Name**: Branch2_SBC
2. **Local Address**: branch2sbc.uxdev.com
3. **Remote Address**: hqsbc.uxdev.com
4. **Local Subnet Addresses**: 172.20.6.0/24
5. **Remote Subnet Addresses**: 172.20.5.3/32,172.20.5.4/32,172.20.5.5/32,172.20.5.6/32

HQ_SBC Tunnel Connection Definitions

The networking configuration must be the exact opposite of those configured on each branch office sites, that is, reverse the **Local Address**, **Remote Address**, **Local Subnet Addresses** and **Remote Subnet Addresses** used on the branch office when setting up a one-to-one tunnel connection entry on the headquarters SBC.

- Tunnel ID 1

1. **Tunnel Name**: HQ_to_Branch1_SBC
2. **Local Address**: Ethernet 2 IP(10.1.2.20)

   Note:

   Alternatively configured as FQDN (eg: hqsbc.uxdev.com), when the **Remote Address** is also configured the same on the branch office SBC.

3. **Remote Address**: 10.1.1.10

   Note:

   Alternatively configured as FQDN (eg: branch1sbc.uxdev.com), when the **Remote Address** is also configured the same on the branch office SBC. Another alternative is to enable the **Allow Any Remote Address** to accept any remote external interface required in case of the remote host behind NAT.

4. **Local Subnet Addresses**: 172.20.5.3/32,172.20.5.4/32,172.20.5.5/32,172.20.5.6/32
5. **Remote Subnet Addresses**: 172.20.1.0/24

   Note:

   Alternatively configured as specific host addresses with CIDR mask value 32. Also, can be configured as 0.0.0.0/0 to accept all IP traffic which the Branch SBC peer specifically defines in the **Local Subnet Addresses**.

- Tunnel ID 2

1. **Tunnel Name**: HQ_to_Branch2_SBC
2. **Local Address**: hqsbc.uxdev.com
3. **Remote Address**: branch2sbc.uxdev.com

   Note:

Another alternative is to enable the **Allow Any Remote Address** to accept any remote external interface required in case of the remote host behind NAT.

4. **Local Subnet Addresses**: 172.20.5.0/24
5. **Remote Subnet Addresses**: 172.20.6.0/24

Firewall and Policy Based Routing

Policy-based Firewall Rules

The **Apply Policy Rules** field is enabled by default and automatically inserts bi-directional FORWARD rules on gateways or an INPUT and OUTPUT rule on single hosts, and adds an INPUT and OUTPUT rule to reach the gateway itself when the tunnel is established. Likewise, these rules are deleted when the tunnel is disconnected.

Use of the policy module depends on how the rest of the firewall is configured and the exact requirements.
When the forwarding-firewalling feature is enabled, the iptables policy module rules-matches packets based on their relation to IPsec policies which will do everything related to only allow traffic from/to the tunneled subnet and not the whole subnet via the IPsec tunnels. The **Apply Policy Rules** fiel d can be disabled if there is a business case requirement to configure custom IPsec ACCEPT/DROP rules which take precedence in relation to the automatically created IPsec rules.

Policy-based Source Routing Table

In a simple network topology with no nexthop gateway between the subnet and the local internal network interface on the SBC gateway, the policy-based source routing entries are created automatically.

To enable the policy-based source routing capabilities: the source address must be the local internal network interface. The **Local Subnet Addresses** list must include the local internal network address, and the **Remote Subnet Addresses** must contain the peer's internal network address.

For example:
1) On the Branch1_SBC gateway (Refer to Network Topology Diagram section), the Ethernet 1 IP(172.20.1.10) is the local internal network interface. This address should be added to the **Local Subnet Addresses** as 172.20.1.10/32 or automatically included when specifying the address range such as 172.20.1.0/24. Likewise, on the Branch1_SBC gateway, the Ethernet 1 IP(172.20.5.3) which is the remote internal network interface configured on the HQ_SBC gateway should be added to the **Remote Subnet Addresses** as 172.20.5.3/32 or automatically included when specifying the address range such as 172.20.5.0/24.

2) On the HQ_SBC gateway (Refer to Network Topology Diagram), the networking configuration must be the exact opposites of the ones configured on each branch office sites. Reverse the **Local Subnet Addresses** and **Remote Subnet Addresses** used on the branch office when setting up a one-to-one tunnel connection entry on the headquarters SBC.

Note:
With a complex network topology involving one or multiple nexthop gateways, may need to create static default gateway routes on the SBC gateways (**Protocols** navigation pane -> **IP** -> **Static Routes**).

Tunnel Setup using Preshared Key Authentication

Specify either the peer address of the remote site (outside interface IP of the peer SBC gateway) or the remote identifier when enabling the **Allow Any Remote Address** field in case of the remote host behind NAT. Use either an existing or new pre-shared key to be configured the same between the SBC gateway peers.

Using the Same Secret Key Between All Sites

Branch1_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key

2. **New Preshared Secret**: Testing123@#

Branch2_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: Testing123@#

HQ_SBC Tunnel Connection Definitions

Tunnel connection definitions on headquarters SBC gateway can be configured in two possible ways as indicated by the examples below.

Single Tunnel Connection for all Branch Sites

A single tunnel ID can be configured on the headquarters SBC to negotiate the traffic selectors from any branch office by specifying *any* remote address as an identifier selector.

> **(!) Caution:**
> At present, the IPsec Statistics table does not report the statistics details for all the branch CHILD_SAs created over a single IKE_SA tunnel connection. This is known limitation and will be supported in future releases. Therefore, it is recommended to configure the one-to-one tunnel connection per the example provided below in the **Multiple Tunnel Connections for Specific Branch Sites** section.

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24,172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **Remote Identifier**: 0.0.0.0
5. **New Preshared Secret**: Testing123@#

Multiple Tunnel Connections for each Branch Site

The need to create multiple tunnels on the headquarters SBC as one-to-one mapping with branch sites is highly recommended when there is a greater interest in maintaining separate tunnels and/or analyzing the **IPsec Statistics** data corresponding to each branch sites.

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local address such as 10.1.1.10 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Authentication Mode**: Preshared Key
4. **New Preshared Secret**: Testing123@#

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**

Alternatively configured as an FQDN such as branch2sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local address such as 10.1.1.30 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **New Preshared Secret**: Testing123@#

Using Different Secret Keys at Each Branch Site

Branch1_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: ABC123

Branch2_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: XYZ456

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local interface address such as 10.1.1.10 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Authentication Mode**: Preshared Key
4. **New Preshared Secret**: ABC123

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
> Alternatively configured as an FQDN such as branch2sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local interface address such as 10.1.1.30 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Authentication Mode**: Preshared Key

4. **New Preshared Secret**: XYZ456

Tunnel Setup Using Certificate Key Authentication

As a best practice where security is of concern for multiple branch office SBC deployments, generating a new Certificate Signing Request, acquiring and installing a digital signed certificate and Trusted Certificate Authority (CA) root chain is recommended.

The CA file(s) which signed the **Sonus SBC Certificate** must be exported from each branch office SBC (if these are different CA vendors) and imported on the headquarters SBC.
Likewise, the CA file(s) which signed the **Sonus SBC Certificate** must be exported from the headquarters SBC and imported on each of the branch office SBC gateways.
The CA file(s) must be imported/exported under the Web UI **Security** navigation pane * > Certificates > Trusted CA* folder.

> **Warning:**
> With the current release (version 3.0), when replacing an existing **Sonus SBC Certificate and/or *Trusted CA Certificates**, the SBC gateway must be rebooted for the tunnels to be re-established with the new certificate installments and/or replacements. This is a known limitation and will be supported in future releases.

Using the Subject Alternative Names (SAN) Identifier

Specify the **Certificate Identifier** as Subject Alternative Name (**IPsec Tunnel Table** navigation pane **> Remote Attributes** panel) on the branch office SBC. To do this, copy one of the Subject Alternative Names display text (**IPsec Tunnel Table** navigation pane **> Local Attributes** read-only panel) from the headquarters SBC gateway and paste it in the **Certificate Identifier** field text box under the Remote Attributes panel of the branch office SBC. Likewise, copy the Subject Alternative Name text (**IPsec Tunnel Table** navigation pane **> Local Attributes** read-only panel) on the branch office SBC gateway and paste it in the Certificate Identifier field text box under the Remote Attributes section of the headquarters SBC. When specifying a peer certificate's SAN identifier, enable and specify the local SAN identifier under the Local Attributes section on the branch office and headquarters SBC gateways. These additional field configurations are mandatory in order to perform a successful look-up and match of an expected SAN identifier against the configured SAN identifier.

The following sections are examples for authenticating a peer gateway using the SAN identifier:

Branch1_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Enabled
2. **SAN Identifier**: branchgw1.uxdev.com
3. **Authentication Mode**: Certificate
4. **Certificate Identifier**: hqgw.uxdev.com

Branch2_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Enabled
2. **SAN Identifier**: branchgw2.uxdev.com
3. **Authentication Mode**: Certificate
4. **Certificate Identifier**: hqgw.uxdev.com

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**

Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Use SAN Identifier**: Enabled
4. **SAN Identifier**: hqgw.uxdev.com
5. **Authentication Mode**: Certificate
6. **Certificate Identifier**: branchgw1.uxdev.com

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Use SAN Identifier**: Enabled
4. **SAN Identifier**: hqgw.uxdev.com
5. **Authentication Mode**: Certificate
6. **Certificate Identifier**: branchgw2.uxdev.com

Using the Distinguished Name(DN) Identifier

Specify the **Certificate Identifier** as Subject Distinguished Name(**IPsec Tunnel Table** navigation pane -> **Remote Attributes** panel) on the branch office SBC. To do this, copy the Subject Distinguished Name display text(**IPsec Tunnel Table** navigation pane -> **Local Attributes** read-only panel) from the headquarters SBC and paste it in the **Certificate Identifier** field text box under the Remote Attributes panel of the branch office SBC. Likewise, copy the Subject Distinguished Name display text(**IPsec Tunnel Table** navigation pane -> **Local Attributes** read-only panel) from the branch office SBC gateway and paste it in the Certificate Identifier field text box under the Remote Attributes panel on the headquarters SBC gateway.

Branch1_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Disabled
2. **Authentication Mode**: Certificate
3. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testhq.uxdev.com

Branch2_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Disabled
2. **Authentication Mode**: Certificate
3. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testhq.uxdev.com

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
> Alternatively configured as FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testbranch1.uxdev.com

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
> Alternatively configured as FQDN such as branch2sbc.uxdev.com, when the **Local Address** is also configured the same on branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testbranch2.uxdev.com

Using Any Identifier

One significance of configuring 'any' certificate identifier is to simplify the configuration steps at the headquarters SBC gateway in larger deployments.

The Trusted Certificate Authority file(s) must be exported from each branch office SBC gateway and imported to the headquarters SBC gateway. This is the only configuration step required in order to perform a successful look-up and match of an expected SAN or DN dentifier against the 'any' identifier configured on the SBC gateway peer,

The configuration examples for authenticating the peer gateway using 'any' SAN or DN identifier is provided below.

HQ_SBC Tunnel Connection Definition using Any SAN Identifier

A single tunnel ID can be configured to negotiate the traffic selectors from any branch offices by specifying a local SAN identifier, 'any' remote address and 'any' peer certificate's SAN identifier.
The branch sites SBC tunnel connection is unchanged from the example provided in 'Using SAN Identifier' section above.

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24,172.20.6.0/24
3. **Use SAN Identifier**: Enabled
4. **SAN Identifier**: hqgw.uxdev.com
5. **Authentication Mode**: Certificate
6. **Certificate Identifier**: any

HQ_SBC Tunnel Connection Definition using Any DN Identifier

A single tunnel ID can be configured to negotiate the traffic selectors from any branch offices by specifying 'any' remote address and 'any' certificate DN identifier.
The branch sites SBC tunnel connection is unchanged from the example provided in 'Using DN Identifier' section above.

1. **Allow Any Remote Address**: Enabled

2. **Remote Subnet Addresses**: 172.20.1.0/24,172.20.6.0/24
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: any

Certificate and Preshared Key Using Any Identifier

Each branch office site can specify various authentication mode(Certificate or PSK) and identifier type(same secret, different secret, SAN or DN). The headquarters SBC should create a one-to-one tunnel connection mapping to match whichever authentication mode specified on the branch office SBC.

Branch1_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Disabled
2. **Authentication Mode**: Certificate
3. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testhq.uxdev.com

Branch2_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: Testing123@#

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: any

- Tunnel ID 2

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **Remote Identifier**: 0.0.0.0
5. **New Preshared Secret**: Testing123@#

IKE/IPsec SA Cipher Suites

Proposal selection process

It is recommended that the transform data such as selection of encryption level, authentication algorithm and diffie-hellman group (DH Group) be configured the same way on the SBC gateway deployed at each branch office sites communicating with another SBC gateway at the headquarters site.

Choose the default settings: 1) IKE: aes128-sha1-modp2048 and IPSEC: aes128-sha1 or consider selecting stronger transform algorithms 2) IKE: aes256-sha256-modp2048 and IPSEC: aes256-sha256 when considering security measures.

IPsec connection can be successfully established between the SBC peers in case of non-matching Encryption, Integrity or DH Group parameters.

In case of mismatched encryption settings, the **Responder** gateway's configured cipher settings will take precedence over the proposed one received from the **Initiator** gateway. In case of a DH Group mismatch, the initiator or responder side with stronger key takes the precedence.

Performance Considerations

Selection of 3DES is supported mainly for the purpose of compatibility with non-SBC devices that do not support AES.
It is recommended to select AES encryption level since the throughput rate with the 3DES encryption will be significantly less and slower than the AES.

SA Expiry and Security Settings

IKE/IPsec SA Expiry and Protections

By default, both the **SA Expiry** and **Reauthentication** key protection measures are disabled since achieving better throughput and low latency for high call load traffic going in and out of the tunnel may be a bigger concern. Based on the business case requirements, whether a low or high degree of security measures are to be taken to protect the keys, then the **SA Expiry**, **Reauthentication**, and/or **Perfect Forward Secrecy** should be enabled under the **SA Expiry and Security Settings** panel.

The negotiation of IKE SAs and IPsec SAs can be configured to expire after a specific amount of time. By default, the **IKE Lifetime** is set to 3 hours, whereas the IPsec lifetime is set to 1 hour as to avoid collisions of these SAs expiring at same time.

Refactoring Significance Using Margin Time

The **Margin Time** field is supported to avoid collisions when the **SA Expiry** and **Reauthentication** are enabled on the SBC gateway deployed at both branch offices and the headquarters sites.
The specified margins are increased randomly(hard-coded percentage on initiator and responder gateway by which margins are randomly increased) before subtracting them from the expiration limits.
The formula shown below is used to calculate the rekey time of IKE and IPsec SAs.

Initiator Mode

```
Actual IKE rekey time = *IKE Lifetime* - (*Margin Time* + random(0, *Margin Time* * 100%))
Actual IPsec rekey time = *IPsec Lifetime* - (*Margin Time* + random(0, *Margin Time* * 100%))
```

Responder Mode

```
Actual IKE rekey time = *IKE Lifetime* - (*Margin Time* + random(0, *Margin Time* * 10%))
Actual IPsec rekey time = *IPsec Lifetime* - (*Margin Time* + random(0, *Margin Time* * 10%))
```

Example

The IPsec tunnel will attempt to rekey the IPsec SA at a random time between 40 and 50 minutes after establishing the SA.
In other words, between 10 and 20 minutes before the SA expires.
1. **IPsec Lifetime**: 1h
2. **Margin Time**: 600s(10m)

```
Actual Minimum IPsec rekey time = 1h - (10m + 10m) = 40m
Actual Maximum IPsec rekey time = 1h - (10m + 0m) = 50m
```

Other Performance Considerations

- Furthermore, for a business case where some level of security measures and performance are both of concerns, then it is recommended to enable the SA Expiry and Security Setting fields on the SBC gateways are deployed at each of the branch office sites or at the headquarters but not required at both tunnel endpoints.
- It is recommended that the **IKE Lifetime** and **IPsec Lifetime** fields be configured with different timeout value to avoid the possibility of collisions although the refactoring using **Margin Time** should prevent that.
- The rekeying of an SA needs some time, the margin values must not be too low.
- Depending on the level of security that would be required for a business case, both reauthentication and rekeying can be enabled for providing maximum security level. If **Reauthentication** is enabled, it is recommended to set the **IKE Lifetime** to a high timeout value when re-authenticating the peer where key hacking is not likely on every hour. The reauthentication unlike the rekeying protection measure not only creates the IKE_SA from scratch but also the IPsec_SAs. During the reauthentication expiry process, performance may be impacted with some packet drops as it is computationally expensive to perform the Diffie-Hellman exchange and signature verifications for reauthentication purposes.