Virtual Tunnel Interface

This chapter describes how to configure a VTI tunnel.

About Virtual Tunnel Interfaces

The ASA supports a logical interface called Virtual Tunnel Interface (VTI). As an alternative to policy based VPN, a VPN tunnel can be created between peers with Virtual Tunnel Interfaces configured. This supports route based VPN with IPsec profiles attached to the end of each tunnel. This allows dynamic or static routes to be used. Egressing traffic from the VTI is encrypted and sent to the peer, and the associated SA decrypts the ingress traffic to the VTI.

Using VTI does away with the requirement of configuring static crypto map access lists and mapping them to interfaces. You no longer have to track all remote subnets and include them in the crypto map access list. Deployments become easier, and having static VTI which supports route based VPN with dynamic routing protocol also satisfies many requirements of a virtual private cloud.

Guidelines for Virtual Tunnel Interfaces

General Configuration Guidelines

- VTIs are only configurable in IPsec mode. To terminate GRE tunnels on an ASA is unsupported.
- You can use dynamic or static routes for traffic using the tunnel interface.
- The MTU for VTIs is automatically set, according to the underlying physical interface. However, if you change the physical interface MTU after the VTI is enabled, you must disable and reenable the VTI to use the new MTU setting.
- If Network Address Translation has to be applied, the IKE and ESP packets will be encapsulated in the UDP header.
- IKE and IPsec security associations will be re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.

- Tunnel group name must match what the peer will send as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which are not IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.
- VTI and crypto map configurations can co-exist on the same physical interface, provided the peer address configured in the crypto map and the tunnel destination for the VTI are different.
- By default, all traffic through VTI is encrypted.
- By default, the security level for VTI interfaces is 0.
- Access list can be applied on a VTI interface to control traffic through VTI.
- Only BGP is supported over VTI.
- If ASA is terminating IOS IKEv2 VTI clients, disable the config-exchange request on IOS, because ASA cannot retrieve the mode-CFG attributes for this L2L session initiated by an IOS VTI client.

IPv6 Support

IPv6 is not supported.

Context Mode

Supported in single mode only.

Firewall Mode

Supported in routed mode only.

DHCP Relay

DHCP relay is not supported on Virtual Tunnel Interfaces (VTIs).

Create a VTI Tunnel

To configure a VTI tunnel, create an IPsec proposal (transform set). You will need to create an IPsec profile that references the IPsec proposal, followed by a VTI interface with the IPsec profile. Configure the remote peer with identical IPsec proposal and IPsec profile parameters. SA negotiation will start when all tunnel parameters are configured.

Note For the ASA which is a part of both the VPN VTI domains, and has BGP adjacency on the physical interface:

When a state change is triggered due to the interface health check, the routes in the physical interface will be deleted until BGP adjacency is re-established with the new active peer. This behavior does not apply to logical VTI interfaces.

Access control lists can be applied on a VTI interface to control traffic through VTI. To permit any packets that come from an IPsec tunnel without checking ACLs for the source and destination interfaces, enter the sysopt connection permit-vpn command in global configuration mode.

You can use the following command to enable IPsec traffic through the ASA without checking ACLs:

hostname(config)# sysopt connection permit-vpn

When an outside interface and VTI interface have the security level of 0, if you have ACL applied on VTI interface, it will not be hit if you do not have same-security-traffic configured.

To configure this feature, use the **same-security-traffic** command in global configuration mode with its **intra-interface** argument.

Procedure

Step 1 Add an IPsec Proposal (Transform Sets).

Step 2 Add an IPsec Profile.

Step 3 Add a VTI Tunnel.

Add an IPsec Proposal (Transform Sets)

A transform set is required to secure traffic in a VTI tunnel. Used as a part of the IPsec profile, it is a set of security protocols and algorithms that protects the traffic in the VPN.

Before you begin

- You can use either pre-shared key or certificates for authenticating the IKE session associated with a VTI. IKEv2 allows asymmetric authentication methods and keys. For both IKEv1 and IKEv2, you must configure the pre-shared key under the tunnel group used for the VTI.
- For certificate based authentication using IKEv1, you must specify the trustpoint to be used at the initiator. For the responder, you must configure the trustpoint in the tunnel-group command. For IKEv2, you must configure the trustpoint to be used for authentication under the tunnel group command for both initiator and responder.

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)**.

Step 2 Configure IKEv1 or IKEv2 to establish the security association.

- Configure IKEv1.

a) In the IKEv1 IPsec Proposals (Transform Sets) panel, click **Add**.
b) Enter the **Set Name**.
c) Retain the default selection of the **Tunnel** check box.
d) Select **ESP Encryption** and **ESP Authentication**.
e) Click **OK**.

- Configure IKEv2.

a) In the IKEv2 IPsec Proposals panel, click **Add**.

b) Enter the **Name**, and **Encryption**.
c) Choose the **Integrity Hash**.
d) Click **OK**.

Add an IPsec Profile

An IPsec profile contains the required security protocols and algorithms in the IPsec proposal or transform set that it references. This ensures a secure, logical communication path between two site-to-site VTI VPN peers.

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)**.

Step 2 In the **IPsec Profile** panel, click **Add**.

Step 3 Enter the IPsec profile **Name**.

Step 4 Enter the **IKE v1 IPsec Proposal** or the **IKE v2 IPsec Proposal** created for the IPsec profile. You can choose either an IKEv1 transform set or an IKEv2 IPsec proposal.

Step 5 If you need an end of the VTI tunnel to act only as a responder, check the **Responder only** check box.

- You can configure one end of the VTI tunnel to perform only as a responder. The responder-only end will not initiate the tunnel or rekeying.
- If you are using IKEv2, set the duration of the security association lifetime greater than the lifetime value in the IPsec profile in the initiator end. This is to facilitate successful rekeying by the initiator end and ensure that the tunnels remain up.
- If the rekey configuration in the initiator end is unknown, remove the responder-only mode to make the SA establishment bi-directional, or configure an infinite IPsec lifetime value in the responder-only end to prevent expiry.

Step 6 (Optional) Check the **Enable security association lifetime** check box, and enter the security association duration values in **kilobytes** and **seconds**.

Step 7 (Optional) Check the **PFS Settings** check box to enable PFS, and select the required Diffie-Hellman Group.

Perfect Forward Secrecy (PFS) generates a unique session key for each encrypted exchange. This unique session key protects the exchange from subsequent decryption. To configure PFS, you have to select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key. The key derivation algorithms generate IPsec security association (SA) keys. Each group has a different size modulus. A larger modulus provides higher security, but requires more processing time. You must have matching Diffie-Hellman groups on both peers.

This establishes the strength of the of the encryption-key-determination algorithm. The ASA uses this algorithm to derive the encryption and hash keys.

Step 8 (Optional) Check the **Enable sending certificate** check box, and select a **Trustpoint** that defines the certificate to be used while initiating a VTI tunnel connection. Check the **Chain** check box, if required.

Step 9 Click **OK**.

Step 10 In the **IPsec Proposals (Transform Sets)** main panel, click **Apply**.

Step 11 In the **Preview CLI Commands** dialog box, click **Send**.

Add a VTI Interface

To create a new VTI interface and establish a VTI tunnel, perform the following steps:

Note Implement IP SLA to ensure that the tunnel remains up when a router in the active tunnel is unavailable. See Configure Static Route Tracking in the ASA General Operations Configuration Guide in http://www.cisco.com/go/asa-config.

Procedure

Step 1 Choose **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Step 2 Choose **Add** > **VTI Interface**. The **Add VTI Interface** window appears.

Step 3 In the **General** tab, enter the **VTI ID**. This can be any value from 0 to 10413. Up to 100 VTI interfaces are supported.

Note If you will be migrating configurations from other devices to ASA 5506 devices, use the tunnel ID range of 1 - 100. This is to ensure compatibility of tunnel range of 1 - 100 available in ASA 5506 devices.

Step 4 Enter the **Interface Name**.

Ensure the Enable Interface checkbox is checked.

Step 5 Enter the source **IP Address** of the tunnel and the **Subnet Mask**.

Step 6 Click the **Advanced** tab.

All the fields need to have valid values or selections for the tunnel to be displayed in the VPN Wizard.

Step 7 Enter the **Destination IP** address.

Step 8 Select the **Source Interface**.

Step 9 Select the IPsec profile in the **Tunnel Protection with IPsec Profile** field.

Step 10 Check the **Ensure the Enable Tunnel Mode IPv4 IPsec** check box.

Step 11 Click **OK**.

Step 12 In the **Interfaces** panel, click **Apply**.

Step 13 In the **Preview CLI Commands** dialog box, click **Send**.

After the updated configuration is loaded, the new VTI appears in the list of interfaces. This new VTI can be used to create an IPsec site-to-site VPN.