Configuring IPsec NAT-Traversal

Restrictions for IPsec NAT-Traversal

- When using a static NAT policy to change both source IP address and source port, you need to set NAT rules for both port 500 and port 4500. When NAT is detected IPsec traffic is shifted to port 4500. If there is no NAT rule for port 4500, traffic will not reach tunnel destination and IPsec NAT-Traversal will remain down.
- Dynamic NAT policy for changing IP address is not supported for IPsec NAT-Traversal.
- IPsec NAT-Traversal is not supported for IPv6 traffic.
- IPsec NAT-Traversal does not work when an IP address is translated to the IP address of an existing subnet in the topology.
- IPSEC and NAT are not supported on the same device.
- When making changes to the IPsec NAT-Traversal keepalive timer, you first need to remove the tunnel mode and tunnel protection configurations from the SVTI. Then, you need to reconfigure the tunnel mode and tunnel protection along with the changes to the IPsec NAT-Traversal keepalive timer.
- Traffic through an IPsec tunnel will not work when IPsec NAT-Traversal sessions and other IPsec sessions have the same tunnel destination.
- IPsec NAT-Traversal will not work when MACsec is enabled on the underlay interfaces.
- All the limitations that apply to IPsec also apply to IPsec NAT-Traversal.

Information About IPsec NAT-Traversal

The following sections provide information about IPsec NAT-Traversal.

Feature Design of IPsec NAT-Traversal

The IPsec NAT-Traversal feature introduces support for IPsec traffic to travel through NAT or PAT points in the network by encapsulating IPsec packets in a User Datagram Protocol (UDP) wrapper, which allows the packets to travel across NAT devices. The following sections define the details of NAT-Traversal:

IKE Phase 1 Negotiation NAT Detection

During Internet Key Exchange (IKE) phase 1 negotiation, two types of NAT detection occur before IKE Quick Mode begins--NAT support and NAT existence along the network path.

To detect NAT support, you should exchange the vendor identification (ID) string with the remote peer. During Main Mode (MM) 1 and MM 2 of IKE phase 1, the remote peer sends a vendor ID string payload to its peer to indicate that this version supports NAT traversal. Thereafter, NAT existence along the network path can be determined.

Detecting whether NAT exists along the network path allows you to find any NAT device between two peers and the exact location of NAT. A NAT device can translate the private IP address and port to public value (or from public to private). This translation changes the IP address and port if the packet goes through the device. To detect whether a NAT device exists along the network path, the peers should send a payload with hashes of the IP address and port of both the source and destination address from each end. If both ends calculate the hashes and the hashes match, each peer knows that a NAT device does not exist on the network path between them. If the hashes do not match (that is, someone translated the address or port), then each peer needs to perform NAT traversal to get the IPsec packet through the network.

The hashes are sent as a series of NAT discovery (NAT-D) payloads. Each payload contains one hash; if multiple hashes exist, multiple NAT-D payloads are sent. In most environments, there are only two NAT-D payloads--one for the source address and port and one for the destination address and port. The destination NAT-D payload is sent first, followed by the source NAT-D payload, which implies that the receiver should expect to process the local NAT-D payload first and the remote NAT-D payload second. The NAT-D payloads are included in the third and fourth messages in Main Mode and in the second and third messages in Aggressive Mode (AM).

IKE Phase 2 Negotiation NAT-Traversal Decision

While IKE phase 1 detects NAT support and NAT existence along the network path, IKE phase 2 decides whether or not the peers at both ends will use NAT-Traversal. Quick Mode (QM) security association (SA) payload in QM1 and QM2 is used to for NAT-Traversal negotiation.

Because the NAT device changes the IP address and port number, incompatibilities between NAT and IPsec can be created. Thus, exchanging the original source address bypasses any incompatibilities.

UDP Encapsulation of IPsec Packets for NAT- Traversal

In addition to allowing IPsec packets to traverse across NAT devices, UDP encapsulation also addresses many incompatibility issues between IPsec and NAT and PAT. The resolved issues are as follows:

Incompatibility Between IPsec ESP and PAT is resolved as follows:

If PAT found a legislative IP address and port, it would drop the Encapsulating Security Payload (ESP) packet. To prevent this scenario, UDP encapsulation is used to hide the ESP packet behind the UDP header. Thus, PAT treats the ESP packet as a UDP packet, processing the ESP packet as a normal UDP packet.

Incompatibility Between Checksums and NAT is resolved as follows:

In the new UDP header, the checksum value is always assigned to zero. This value prevents an intermediate device from validating the checksum against the packet checksum, thereby, resolving the TCP UDP checksum issue because NAT changes the IP source and destination addresses.

Incompatibility Between Fixed IKE Destination Ports and PAT is resolved as follows:

PAT changes the port address in the new UDP header for translation and leaves the original payload unchanged.

To see how UDP encapsulation helps to send IPSec packets see the figures below.

Figure 1: Standard IPsec Tunnel Through a NAT/PAT Point (No UDP Encapsulation)

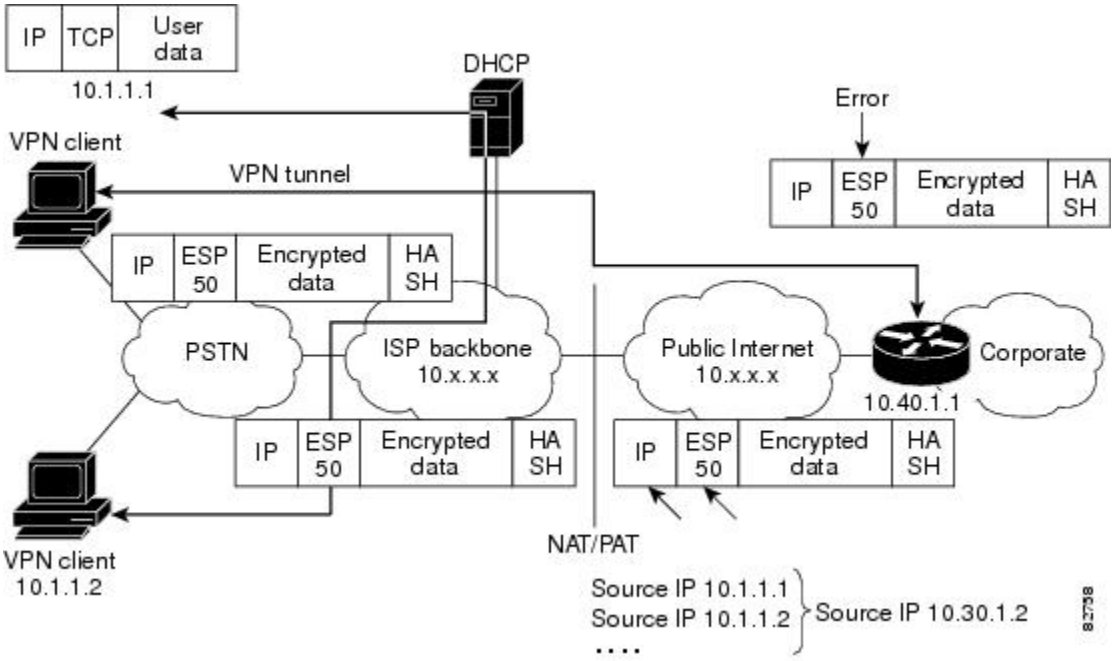
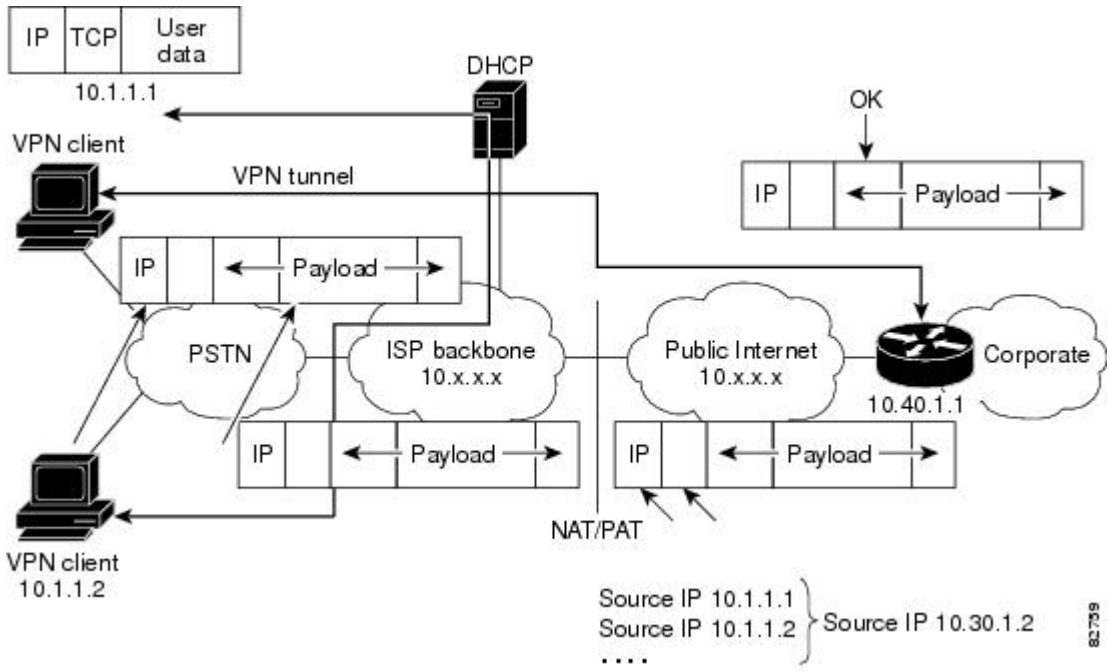


Figure 2: IPsec Packet with UDP Encapsulation



UDP Encapsulated Process for Software Engines Transport Mode and Tunnel Mode ESP Encapsulation

After the IPsec packet is encrypted by a hardware accelerator or a software crypto engine, a UDP header and a non-IKE marker (which is 8 bytes in length) are inserted between the original IP header and ESP header. The total length, protocol, and checksum fields are changed to match this modification. The first figure below shows an IPsec packet before and after transport mode is applied; the second figure below shows an IPsec packet before and after tunnel mode is applied.

Figure 3: Transport Mode--IPsec Packet Before and After ESP Encapsulation

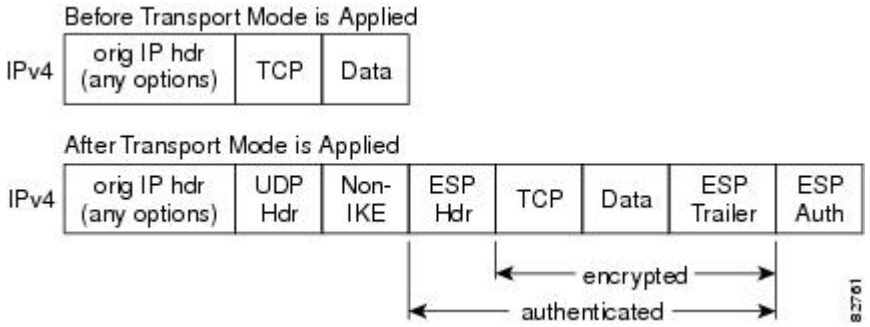
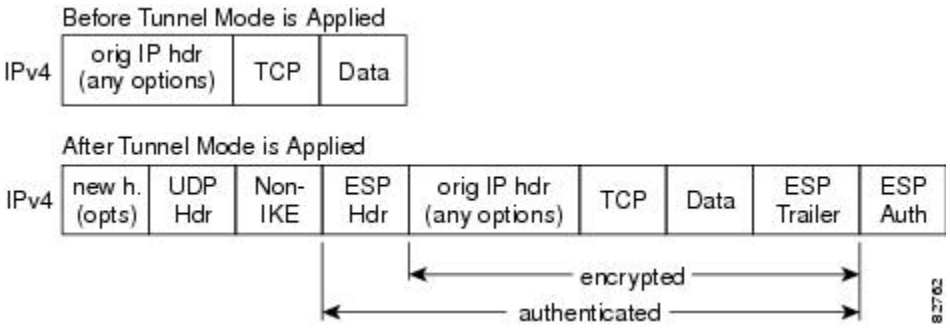


Figure 4: Tunnel Mode--IPsec Packet Before and After ESP Encapsulation



You should consider the following points when using IPsec NAT-Traversal.

- In IPsec the payload is integrity protected. Hence, any IP address enclosed within IPsec packets cannot be translated by NAT. Protocols that use embedded IP addresses include FTP, Internet Relay Chat (IRC), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), H.323, and Session Initiation Protocol (SIP). These protocols cannot be directly translated by NAT.
- NAT is incompatible with IPsec when IP addresses are used as a search key to find a preshared key. Modification of the IP source or destination addresses by NAT or reverse NAT results in a mismatch between the IP address and the preshared key.

Starting with the Cisco IOS XE Cupertino 17.9.2 release, the following changes apply to IPsec NAT-Traversal.

- When one of the IPsec NAT-Travesal tunnels sharing a destination IP address goes down the other tunnels will remain functional.
- You can ping the tunnel destination IP address for a IPsec NAT-Traversal session.

Starting with the Cisco IOS XE Cupertino 17.9.3 release, the following changes apply to IPsec NAT-Traversal.

- IPsec NAT-Traversal is supported on a Switched Virtual Interface (SVI).
- IPsec NAT-Traversal is supported even when the tunnel source is used as a physical port.
- IPsec NAT-Traversal is supported on a VRF.
- You can configure IPsec NAT-Traversal via a subinterface.

NAT Keepalives

NAT keepalives are enabled to keep the dynamic NAT mapping alive during a connection between two peers. NAT keepalives are UDP packets with an unencrypted payload of 1 byte. Although the current dead peer detection (DPD) implementation is similar to NAT keepalives, there is a slight difference: DPD is used to detect peer status, while NAT keepalives are sent if the IPsec entity did not send or receive the packet at a specified period of time--valid range is between 5 to 3600 seconds.

If NAT keepalives are enabled, users should ensure that the idle value is shorter than the NAT mapping expiration time, which is 20 seconds.

How to Configure IPsec NAT-Traversal

The following sections provide information about configuring IPsec NAT-Traversal.

Configuring NAT-Traversal

NAT-Traversal is a feature that is auto detected by VPN devices. If both VPN devices are NAT-Traversal capable, NAT-Traversal is auto detected and auto negotiated.

Disabling NAT-Traversal

You may wish to disable NAT-Traversal if you already know that your network uses IPsec-awareness NAT (spi-matching scheme). To disable NAT-Traversal, perform the following procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**no crypto ipsec nat-transparency udp-encapsulation**
	Example:
	`Device(config)#`
	`no crypto ipsec nat-transparency udp-encapsulation`
		Disables NAT-Traversal.

Configuring NAT Keepalives

To configure your device to send NAT keepalives, perform the following procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ikev2 nat keepalive** *seconds* **Example:** `Device(config)# crypto ikev2 nat keepalive 20`	Allows an IPsec node to send NAT keepalive packets. • *seconds* --The number of seconds between keepalive packets; range is between 5 to 3,600 seconds. **Note** A five-percent jitter mechanism value is applied to the timer to avoid security association rekey collisions. If there are many peer routers, and the timer is configured too low, then the router can experience high CPU usage.

Verifying IPsec Configuration

To verify your configuration, perform the following optional steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password, if prompted.
Step 2	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail** **Example:** `Device# show crypto ipsec sa`	Displays the settings used by current SAs.

Configuration Examples for IPsec NAT-Traversal

The following sections show examples of IPsec NAT-Traversal configuration.

NAT Keepalives Configuration Example

The following example shows how to enable NAT keepalives to be sent every 20 seconds.

```
Device> enable
Device# configure terminal
Device(config)crypto ikev2 nat keepalive 20
```

Feature History for IPsec NAT-Traversal

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	IPsec NAT-Traversal	The IPsec NAT-Traversal feature introduces support for IPsec traffic t or PAT points in the network by addressing many known incompatibi and IPsec. Support for this feature was introduced on the Cisco Catalyst 9300X S

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to Cisco Feature Navigator.