How do Network Address Translator (NAT) applications work with PCoIP?

Answer:

The PCoIP protocol is compatible with Network Address Translation (NAT) based on the following table:

PCoIP Deployment Environment				Supported NAT Implementations		
Host	**Client**	**View Security Server**	**VPN Tunnel**	**Static NAT**	**Dynamic NAT**	**Port-based NAT**
Software Host	Software Client	Optional	Optional	Yes	Yes	Yes
	Zero Client	Optional	Optional	Yes*	Yes*	Yes*
Hardware Host	Software Client	Optional	Optional	Yes	Yes	Yes*
	Zero Client	Yes	Optional	Yes*	Yes*	Yes*
	Zero Client	No	Yes	Yes	Yes	Yes
	Zero Client	No	No	Yes	Yes	No

* See What encryption algorithm and bandwidth metrics are used for various setups of zero clients, soft clients, soft and hard hosts? (15134-281) for notes on network bandwidths supported.

If The PCoIP traffic is encapsulated in a tunnelling protocol such as VPN, equipment that implements NATs is then compatible with PCoIP technology.

The PCoIP technology supports both IPSec ESP and UDP encapsulated IPSec. The encapsulation depends on your deployment environment (the type of PCoIP host used and if a VMware View Security Server is used).

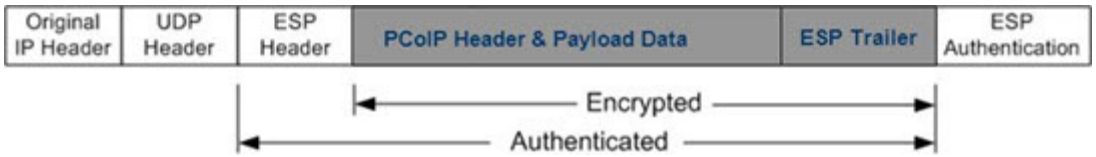
- **PCoIP Software:** When using PCoIP software on the host or client, the UDP/ESP encapsulation mode is used.
- **PCoIP hardware host with VMware View Security Server**: When connecting PCoIP zero clients to remote workstations using PCoIP host cards through the View Security Server, the UDP/ESP encapsulation mode is used.
- **PCoIP Hardware Host:** This applies to Tera 1 and Tera 2 host cards using firmware prior to 4.1. When using PCoIP hardware hosts, IPsec ESP encapsulation mode is used. Since IPsec ESP encrypts the entire packet outside of the IP SA/DA and ESP header, there are no port numbers for the NAT to use. However, since PCoIP does not use the IP

Authentication Header, the NAT can manipulate the IP address information in the IP header.

PCoIP Packet Encapsulation Options

Option 1: UDP/ESP (works with Static, Dynamic, Port-Based NATs)

During a session, the PCoIP payloads are encapsulated inside UDP packets with which the NATs can freely work.

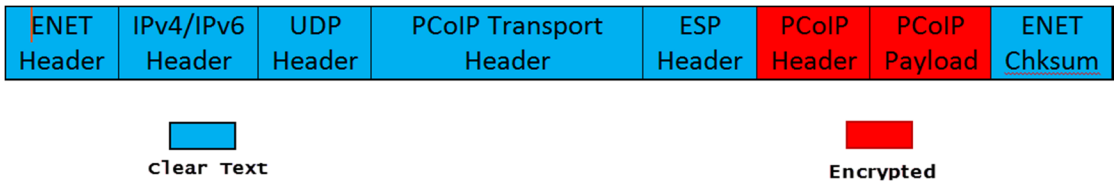


Option 2: IPSec ESP (works with Static and Dynamic NATs unless a VPN encapsulation is used)

During a session, the PCoIP packets do not have a UDP header so that NAT has no UDP ports to work with.

Option 3: UDP/ESP with PCoIP Transport Header (works with View 5.1 +/ Arch and with Static, Dynamic, and Port-Based NATs)

During a session, the PCoIP payloads are encapsulated inside UDP packets with which the NATs can freely work. Additionally the packet contains the PCoIP Transport Header which can be is used by certified network equipment.

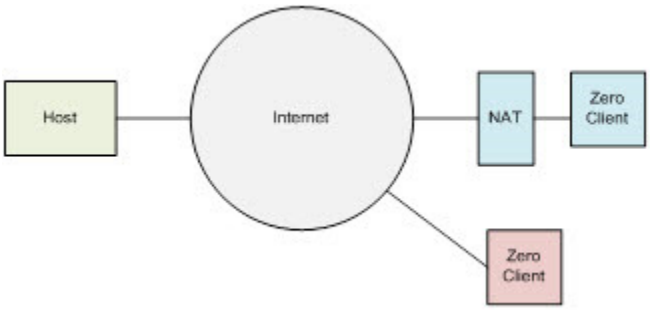


Configuring your NAT

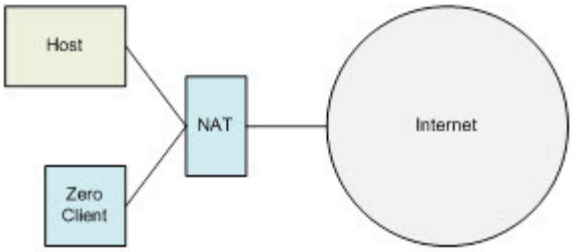
To configure your NAT to allow a zero client to establish a session with a host:

- **Host card that is not connected to a NAT:** Generally, the only NAT setting you must enable is "IPsec Passthrough". (This is often enabled by default.) ***A key limitation is that since there are no port numbers, there can be only one active zero client-to-hard host session traversing the NAT at once***. The NAT device forwards all incoming IPsec-ESP packets to the internal device that sent the last outgoing IPsec-ESP packet. When there is more than one sender (more than one active zero client-to-hard host session), the NAT

device ends up forwarding incoming IPsec-ESP packets to the wrong zero client and one of the sessions times out and fails.



- **Host card is connected to the same NAT as the zero client:** There are no special configuration steps to start a session for this scenario.



- **Host card is connected to a different NAT than the zero client:** Enable "IPsec Passthrough," and then configure the NAT to port forward TCP port 4172 to the host card IP address. To start the session, the zero client's peer address is the NAT's public IP address. (If there is an option to forward ESP packets to the host card's internal IP address, enable this setting. This setting is not commonly available, so we rely on "IPsec Passthrough".)

  You must also change the NAT port-forwarding configuration to have a different host card establish a NAT-traversing PCoIP session.