IPsec in VoIP Networks

Newport networks

IPSEC IN VOIP NETWORKS

IPsec is widely used to provide secure access to corporate private networks. IPsec is specified by TISPAN and 3GPP for both access, core and interconnect applications. However, IPsec and the current range of corporate network edge Network Address and Port Translators (NAPTs) are not compatible with the Next Gen services provided by VoIP architectures. This technical note describes the problems and the solution defined by TISPAN.

Background

IP does not have any in-built security capabilities, thus IPsec was introduced to provide the required security services. These include: encryption, authentication, integrity validation and anti-replay. IPsec operates at the network layer (layer 3) making it more flexible than TLS since it can encapsulate both UDP and TCP. However, IPsec assumes that the end-to-end connection does not have to traverse intermediate devices such as NATs which alter the authenticated packets.

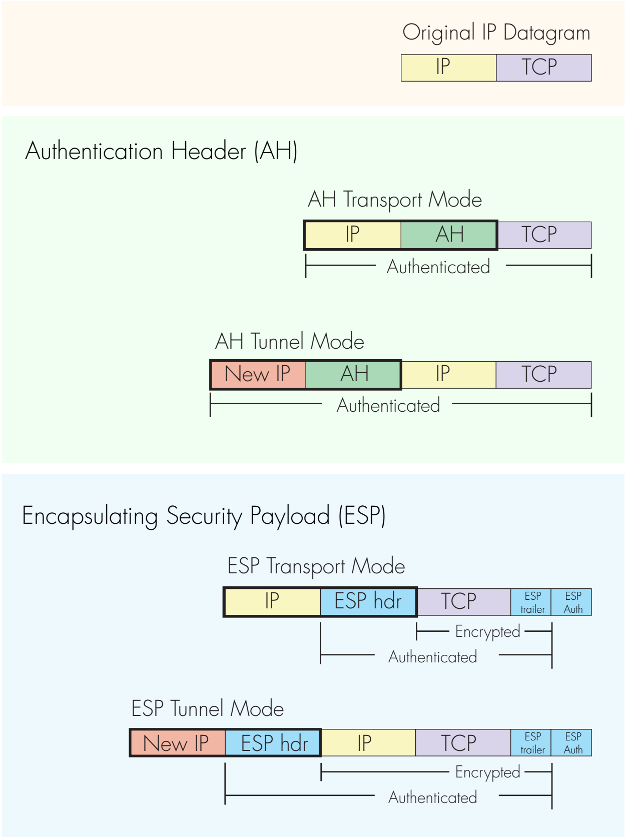
NATs are widely deployed throughout the business world (near 100% of all business networks) and also by many domestic IP users; since about 50% of domestic network edge devices have NAT functionality in them (e.g. ADSL modems). More correctly these devices should be call NAPTs – Network Address *and Port* Translators – unfortunately, as we shall see, IPsec obscures some of this information.

IPsec Details

IPsec has several different modes of operation: Authentication Header (AH) and Encapsulating Security Payload (ESP). These in turn have two connection modes, tunnel mode and transport mode. ETSI and 3GPP specify the use of IPsec ESP tunnel mode in TS 33.210 (interconnect and core) and ESP transport mode in TS 33.203 (access).

AH or ESP?

IPsec Authentication Header (AH) provides authentication of origin, message integrity checking and prevention of replay attacks. In AH mode there is no encryption of the payload, only the header is involved.



IPsec Encapsulating Security Payload (ESP] offers message integrity, data confidentiality, prevention of replay attacks and optionally authentication.

Transport or Tunnel?

In general transport mode is used to secure end-to-end communications between two devices, whilst tunnel mode is used to connect two networks. This is reflected in the 3GPP selection of ESP transport mode for access and tunnel for interconnect.

In transport mode IPsec AH protects both the payload and the IP header fields and inserts a new header between the original IP header and the payload. In tunnel mode the whole IP packet is encapsulated within an AH and new IP header.

The AH header allows the recipient to detect out of sequence packets, and authenticate the sender. It also protects the integrity of the payload and header, the recipient recalculates the hash and a mismatch indicates data tampering or incorrect key, the packet it therefore discarded.

For this reason IPsec AH is incompatible with NATs of any type since the function of a NAT is to alter the packet header, specifically the IP address. The AH mechanism will then cause the packet to be discarded as the calculation of the data integrity will indicate that the packet has been altered.

ESP in both transport and tunnel modes encapsulates and encrypts the required data and appends it to the original IP header (only changing the protocol field), therefore ESP is more 'NAT friendly'. Transport mode ESP encapsulates just the payload, i.e. the UDP or TCP part, whilst tunnel mode encapsulates the whole IP packet. There is no check that the encrypted portion matches the non-encrypted portion, and so NATs can be readily traversed.

In order to provide a secure path for VoIP signalling applications it can be seen that ESP with authentication provides the required security and authentication combination. However, 3GPP have assumed this will operate in a NAT free network.

The Problem with IPsec and NATs

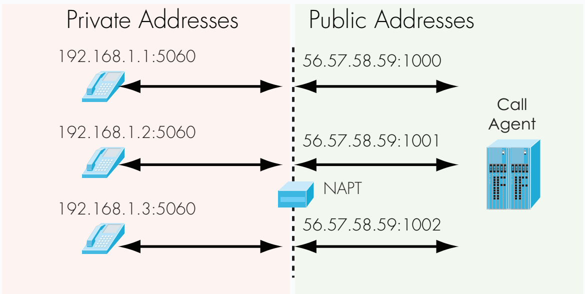
Most NAT devices are used to provide a mapping of many devices on a private network onto a single public IP address. They do this by mapping ports as well as IP addresses. This means they alter the contents of the transport layer protocol, i.e UDP or TCP. When a NAPT device encounters an IPsec ESP packet it no longer has access to the transport layer ports and will usually revert to NAT-only operation.

If there is only one IPsec device behind the NAT this is not a problem, since the NAT will simply translate the private IP address to the public IP address. This enables the single device to communicate through the NAT to the far end.

However, there is a problem where there are multiple IPsec sources behind a NAPT communicating with a single server. For example, several VoIP phones located on a business network talking to the same SIP server in the hosting Service Provider's network.

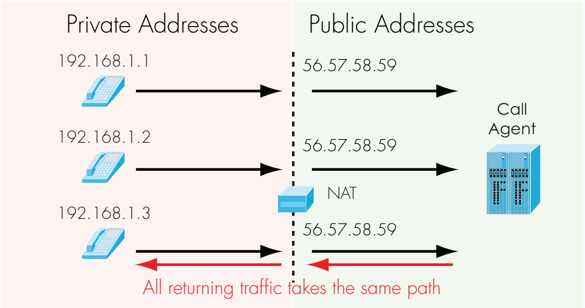
As we have seen, IPsec encapsulates and obscures the transport layer port information which the NAPT needs to create unique bindings between source IP address and port and destination IP address and port. This behaviour is more correctly termed symmetric Network Address and Port Translator, and is by far the most widely used NAPT mechanism in access networks.

Normal NAPT operation with IP traffic



IP address and Port Numbers mapped from private to public addresses. Each source/destination pair is unique.

NAPT operation with IPsec traffic



IPsec obscures port number, NAPT reverts to NAT. Private address translated to Public address. No unique identifier for returning traffic

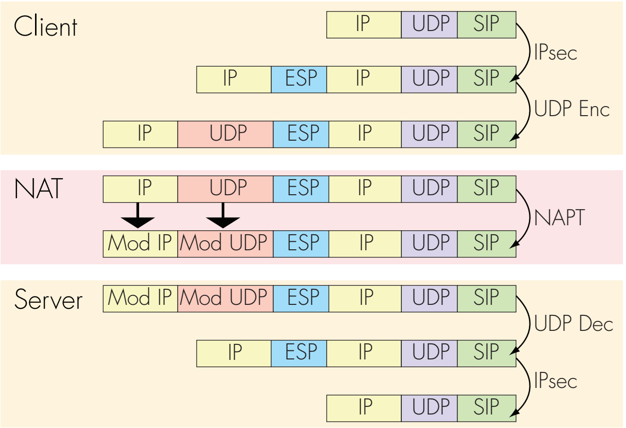
Presented with a number of IPsec streams heading out to the same destination, "VPN compatible NAPTs" change to NAT mode, thus they create a many-to-one relationship in the bindings. So, if two IPsec phones are trying to access the same server from behind the same NAPT, there is no way for the returning traffic to be steered via the appropriate binding to the correct phone.

In practice most NAPT products with a "VPN compatibility" mode use the binding created by the last outbound packet as the destination for inbound packets. Thus, one user will receive all the signalling.

TISPAN Security

In a mobile 3GPP network IPsec presents no problem because there are no NAPT devices between the phone and the server. Similarly, using IPsec ESP in tunnel mode to interconnect networks is unlikely to have to traverse NAPTs. However, to secure the signalling from phone to server in a broadband or Internet based network an alternative solution must be used.

TISPAN has recognised that NAT traversal is not possible with the IMS security solutions in TS 33.203 releases 5 and 6. It has agreed to use UDP encapsulated IPsec according to RFC 3948. TS 33.203 defines a security negotiation mechanism (RFC 3329) which includes a Mode parameter, TISPAN has extended the parameters to include "UDP-enc-tun". The encapsulation occurs in two stages: the original clear SIP/UDP message is encapsulated using IPsec ESP, then this encapsulated in another UDP header. The message is sent from port 4500 to port 4500. The intermediate NAPT device can change the source IP and port numbers without affecting the IPsec payload. De-encapsulation is the reverse process.



Conclusion

As NAPT devices are a fact of life for most broadband, WiFi and WiMax networks and IPsec is incompatible with NAPT it has been necessary for TISPAN to extend the 3GPP security mechanisms to address this crucial need. The ability to negotiate a secure signalling connection with the IMS will be crucial to the deployment of the next generation of multimedia service. TISPAN's extension of the 3GPP security framework to include UDP encapsulated IPsec means that any number of intermediate NAT or NAPT devices can be traversed. The NAT devices have access to the encapsulating UDP port numbers and can perform address and port translation in the normal way. The use of a common standard for the negotiation and delivery of a secure signalling path will greatly improve device interoperability.

Since this is an extension of the existing IMS security framework it means that other mechanisms such as key exchange remain unchanged.

There are other advantages in using IPsec as opposed to the alternative which was under consideration – TLS. TLS sits above the transport layer so port numbers are still visible to intermediate NAPTs. However, typically only the server is authenticated, and the client remains unauthenticated. TLS demands the use of TCP, whereas IPsec can use either UDP or TCP. The use of TCP in large scale deployments raises concerns about the overhead of maintaining a large number of connections with numerous UAs. Thus, TCP is not well liked by service providers since the overheads associated with its mass use are significant compared to UDP.

TISPAN's extension to the IMS security framework delivers the capability of delivering secure signalling whilst maintaining the ability to traverse intermediate NAPT devices. ■

References

RFC 4301: Security Architecture for the Internet Protocol: (obsoletes RFC 2401)

RFC 4302: IP Authentication Header: (obsoletes RFC 2402)

RFC 4303: IP Encapsulating Security Payload (ESP): (obsoletes RFC 2406)

RFC 3261: SIP: Session Initiation Protocol

RFC 3948: UDP Encapsulation of IPsec ESP Packets

RFC 3329: Security Mechanism Agreement for the Session Initiation Protocol (SIP)

ETSI TS 133 203 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services

ETSI TS 133 210 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security

Glossary

3GPP	3rd Generation Partnership Project
AH	Authentication Header
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
IPsec	IP Security
NAPT	Network Address and Port Translation
NAT	Networks Address Translation
TCP	Transmission Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
VPN	Virtual Private Network