NAT traversal for IPsec

Heikki Ollikainen
Helsinki University of Technology
heikki.v.ollikainen@nokia.com

Abstract

Network Address Translator (NAT) is a technology that is used for allowing multiple computers in the network to share a single public IP address for accessing the Internet. The basic reason for NAT usage is the limited number of IPv4 addresses. NAT is widely used in the current networks where it is also used as cloaking service for computers in internal network, since all computers behind the NAT router are hidden from external networks i.e. Internet. In the same time, this may cause connectivity problems (e.g. P2P) for terminals and applications since connections to outside has only one public IP address - depending on the mode how NAT is handling the address translation. Therefore, in order to guarantee smooth and feasible traffic pass-through, several NAT traversal mechanisms has been designed and deployed. IPsec is a security protocol that is used for securing the IP (L3) level traffic. The key functionality of IPsec is to protect the confidentiality of the data, assure the authenticity of the sender, and the integrity of the data that it has not been changed in transition. Internet Key Exchange (IKE) protocol uses IPsec for embedding the IP address of sending computer into its payload. When the IKE packet - that contains the embedded IPsec address - is sent through NAT, the sender IP address is changed to match the address of NAT box. Therefore, when the receiver notifies that the IP address of the IKE packet do not match to sender’s original IP address, it drops the packet. The key problem of NAT with IPsec is that NAT must change information in the packet headers in order to perform the packet pass-through. This feature in NAT causes a conflict with IPsec, and the packets will be dropped. This paper discusses of existing method related to IPsec NAT traversal and the problematics regarding the IPsec NAT traversal. The goal of this paper is to present the mainstream solution how to provide NAT traversal for IPsec.

1 Introduction

This paper is organized as follows:

- The first part 1 provides an introduction to related topics such as NAT, IPsec, the problematics of IPsec with NAT.
- The second part 2 presents the current solution NAT-T, and the NAT-T encapsulation/decapsulation mechanisms.
- The third part 3 present NAT-T solutions for problems.
- The fourth part 4 presents a discussion.
- The last part 5 summarizes the paper, concludes the work and describes the further work.

The following sections presents an introduction to related topics.

1.1 Network Address Translator (NAT)

NAT is an Internet standard [7] that enables a Local Area Network (LAN) to use a set of IP addresses for internal traffic, and a second set of IP addresses for external traffic. NAT is located at the border of the internal network (e.g. LAN) and external network (e.g. Internet) where IP address translation is needed. The main reasons for NAT usage are as follows:

- Save IP addresses - The address space of IPv4 is limited. NAT provides an easy way to hold down the demand for IP addresses through IP address reuse. NAT enables service provider to use more internal IP addresses that are non-conflicting with the IP addresses used by other service providers.
- Cloaking service - NAT hides internal IP addresses, increasing security for end-users.

Network address translation can be performed in different manner that depends on the features of NAT implementation, but the main modes for execution of the address translation are as follows:

Static NAT provides a service where a private IP address is mapped to a public IP address. The public IP address is always the same IP address for all connections. This allows an internal host, such as a Web server, to have an unregistered/private IP address and still be reachable over the Internet.

- For example, we can use a static mapping if we want an internal network device with a private IP address of 11.0.0.193 to always use a public IP
address of 172.21.55.68. Therefore, whenever a internal device with 11.0.0.193 address initiates a transaction with the Internet, NAT router will replace the private IP address (11.0.0.193) with the public IP address (172.21.55.68).

Dynamic NAT provides a service where a private IP address is mapped to a public IP address that is fetched from a pool of registered/public IP addresses. Typically, the NAT router in a network keeps a table of registered IP addresses. Moreover, when a connection (with a private IP address) requests the access to Internet, router chooses an IP address from the table (that is not at the time being used by another connection). Dynamic NAT increases the security of a network as it cloaks the internal configuration of a private network, and makes it difficult for someone in external network to monitor individual usage patterns. Furthermore, dynamic NAT allows a private network to use private IP addresses that are invalid on the Internet but useful as internal addresses.

- For example, we use a dynamic mapping with a pool of public IP addresses available from the range of 172.21.50.1 to 172.21.50.100. Therefore, when a device with a private IP address (11.0.0.193) sends a request to access the Internet, the NAT would replace the private IP address (11.0.0.193) with one of the public IP addresses in the pool between 172.21.50.1-172.21.50.100. Furthermore, dynamic NAT router needs to monitor the state of responses, and translate them back to device with private IP address (11.0.0.193). Finally, at the end of the session, dynamic NAT releases the public IP address, and returns it back to the pool, so the public IP address would be again available for other connections and private IP addresses.

As summary of basic NAT functionality that applies for both static and dynamic NAT:

- An internal machine connects to an external machine.
- The NAT router checks the NAT table, when the first packet arrives from the internal machine.
- If no static match has been found the NAT router performs the IP address translation of the internal IP address to an external (public) IP address from the available pool of external IP addresses by replacing the source IP address.
- The external machine receives the packet and replies to the external IP address given by the NAT table.
- The NAT router executes a lookup in its table of internal to external IP address mappings, and forwards the packet to the machine with the internal address.

- The packet is received and the rest of the communication session uses the NAT table.

1.2 Internet Protocol Security (IPsec)

IPsec is an Internet standard [1] and a security framework for securing the network layer (L3) traffic by extending the IP packet header with additional protocol numbers. IPsec allows encryption of any higher layer protocol, including the arbitrary TCP and UDP sessions. However, even IPsec is conceptually simple and provides a excellent flexibility, it is a complex protocol to setup e.g. key management and configuration of encryption of addresses and ports using IPsec options.

IPsec provides following features as key functionality: the confidentiality of data, authenticity of the sender and the integrity of data. In addition, IPsec provides a replay protection prevents acceptance of a packet that has been captured and re-sent.

As disadvantage, IPsec requires operating systems to support direct manipulation of IP headers. For example, Linux IPsec support is not a standard feature in the kernel, the support must be compiled into it separately. Furthermore, putting the cryptography feature in the kernel isolates it from the application making it more difficult to code crypto-aware software. On the contrary, for example, SSL support simply requires linking a SSL library into the application that allows it to query easily certificates that have been used to authenticate a client. Similarly, same thing with IPsec requires application to query kernel using some kind of API.

Security Association (SA) is a fundamental concept in IPsec. SA is a relationship between source and destination network entities that describe how the entities will use security services to communicate with each other. An SA is defined by packet’s destination IP address and a Security Parameter Index (SPI) - 32-bit value - that allows multiple SAs to single destination IP address. IPsec provides many options for performing network encryption, authentication and integrity for each connection. When the SA is determined, the source and destination entities must determine exactly the algorithms that are to be used for communication - for example, DES or 3DES for encryption, MD5 or SHA-1 for integrity. Furthermore, after deciding on the algorithms, the network entities must share session keys. SA is the method that IPsec uses to track all concerns related to communications session between source and destination entities. SAs can operate in transport mode or tunnel mode. In transport mode the IPsec data field begins with upper level packet headers i.e. TCP, UDP, ICMP. In tunnel mode the IPsec data field begins with an new IP packet headers [9].
IPsec consists of two protocols: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH protects the integrity of the IP packet by protecting/encrypting the whole IP packet. The AH protocol headers and parameters are presented in Fig. 2:

- Security Parameter Index (SPI) that specifies the SA to use for decapsulation of the packet.
- Sequence number that protects against replaying attacks
- Hash Message Authentication Code (HMAC) that guarantees the integrity of the data, since only IPsec peers (initiating/receiving) can create and check the HMAC value.

AH protects the IP datagram including immutable parts of the IP header like the IP addresses. Therefore, the AH protocol does not allow NAT traversal where NAT replaces an IP address in the IP header by its own IP address. This exchange causes HMAC value become invalid when receiver peer checks it.

ESP ensures the integrity of data using HMAC, and the confidentiality with encryption. HMAC value is only calculated over the payload, and the IP header is not included into calculation process. The ESP protocol headers and parameters are presented in Fig. 3:

- Security Parameter Index (SPI) that specifies the SA to use for decapsulation of the ESP packet.
- Sequence number that protects against replaying attacks

Since the HMAC value is only calculated over payload, NAT does not break the ESP. NAT-T [6] uses this ESP based solution for allowing the traffic between IPsec peers.

### 1.3 Problems of IPsec over NAT

- **NATs cannot update upper-layer checksums.** TCP and UDP headers contains a checksum that incorporates the values of the source and destination IP addresses, and port numbers. When NAT changes the IP address and/or the port number of a packet, it normally updates the TCP or UDP checksum. When the TCP checksum (mandatory) and UDP checksum (optional) are encrypted with ESP, it cannot be updated. Therefore, since NAT has been changing the IP addresses and ports, the checksum verification fails at the destination.

- **IKE UDP port number cannot be changed.** Some implementations of IPsec use UDP port 500 as both the source and destination UDP port number. However, for an IPsec peer located behind a NAT, the NAT changes the source address of the initial IKE packet (main mode). Furthermore, IKE traffic may be discarded depending on the implementation.

- **NATs cannot multiplex IPsec data streams.** ESP protected IPsec traffic does not contain a visible TCP or UDP header. The ESP header is between the IP header and the encrypted TCP and UDP.
header. Therefore, the TCP and UDP port numbers cannot be used to multiplex traffic to different private network hosts. The ESP header contains a field named the Security Parameter Index (SPI) where it is used to identify an IPsec Security Association (SA).

The destination IP address must be mapped to a private IP address for inbound traffic to the NAT. The destination IP address of inbound traffic for multiple IPsec ESP data streams is the same address. Therefore, the destination IP address and SPI must be tracked or mapped to the private destination IP address and SPI to distinguish one IPsec ESP data stream from another. The change of using the same SPI value between multiple private network clients is low, since the SPI is a 32-bit number. The problem us that it is difficult to determine which outbound SPI value corresponds to which inbound SPI value. NATs cannot map the SPI value, since the ESP trailer contains Hashed Message Authentication Code (HMAC) that verifies the integrity of the ESP protocol data unit (PDU). The SPI cannot be changed without invalidating the HMAC value.

- **NAT timeout of IKE UDP port mapping can cause problems.** UDP mappings in NAT are often deleted very quickly. The initiator’s IKE traffic creates a UDP port mapping in the NAT that is used for the duration of the initial **main mode** and **quick mode** IKE negotiations. However, if the responder later sends IKE messages to the initiator and the UDP port mapping is not present, it is discarded by the NAT. Furthermore, this can cause SAs to time out and be removed by the responder.

- **Identification IKE payload contains embedded IP addresses.** Each IPsec peer sends an identification payload that includes an embedded IP address for the sending IP address for the sending IPsec peer for the main and quick mode negotiations. Since the source address of the sending node has been changed by a NAT, the embedded address does not match the IP address of the IKE packet. An IPsec peer that validates the IP address of the identification IKE payload discards the packet. An IPsec peer that validates IP address of the identification IKE payload discards the packet ad abandon the IKE negotiation.

## 2 UDP Encapsulation of IPsec ESP Packets

This section provides an overview to functionality of IPsec NAT-T, and to changes that are mandatory for NAT-T protocol. The original protocol specification is described in [6]. IPsec NAT-T adds a UDP header that encapsulates the Encapsulating Security Payload (ESP) header. This gives the NAT router a UDP header containing UDP ports that can be used for multiplexing IPsec data streams. Furthermore, NAT-T puts the original IP address into a NAT-0A (Original Address) payload. This gives the receiving IPsec peer access to required information so that the source and destination IP addresses and ports can be checked and the checksum validated. Therefore, this solves the problem of the embedded source IP address not matching the source address on the packet.

ESP encapsulation can be used for both IPv4 and IPv6 protocols. Encapsulation is used with IKE whenever negotiated, and the UDP port numbers are the same as used by IKE traffic [6].

The IPsec NAT-T functions basically as follows: First, NAT-T peer determines in initial IPsec negotiation, i) if both IPsec peers (initiating/responding) can perform IPsec NAT-T ii) if there is a NAT router in the path between them. Moreover, if both of the conditions are true, the peers automatically use IPsec NAT-T to send IPsec traffic across the NAT. If either IPsec peer does not support IPsec NAT-T, then normal IPsec negotiation(s) and protection is performed. If both peers support IPsec NAT-T and there are no NATs between them, normal IPsec protection is performed.

NAT-T makes several changes to IPsec:

- **UDP header is placed between the outer IP header and the ESP header encapsulation the ESP Packet Data Unit (PDU).** The same ports that are used for IKE are used for UDP encapsulated ESP traffic.

- **The IPsec NAT-T IKE header contains a new non-ESP marker (see figure 4) field that allows a recipient to distinguish between a UDP-encapsulated ESP PDU and an IKE message.** IPsec NAT-T peer begins to use the new IKE header after determined that there is an intermediate NAT.

- **UDP message that uses the same ports as IKE traffic, contains a single byte (0xFF), and it is used to refresh the UDP port mapping in a NAT for IKE and UDP encapsulated ESP traffic to a private network host.**

- **New vendor ID IKE payload contains a well-known hash value, which indicates that the peer is capable of performing IPsec NAT-T.**

- **NAT discovery IKE payload contains a has value that incorporates an address and port number.** An IPsec peer includes two NAT discovery payloads.
during the main mode negotiation - one for destination IP address/port and one source IP address/port. The recipient uses NAT discovery payloads to discover whether a NAT translated addresses or port numbers are located behind NATs.

- New encapsulation mode for 'UDP encapsulated ESP transport mode and tunnel mode' are specified during quick mode negotiation to inform the IPsec peer that UDP encapsulation for ESP PDUs should be using.

- New IKE payload for NAT original address (NAT-OA) that contains the original IP address of the IPsec peer. Each peer sends the NAT-OA IKE payload during the quick mode negotiation for UDP encapsulated ESP transport. The recipient stores this IP address in the parameters for the SA.

Non-ESP marker field - presented in figure 4 - must be in align with the SPI field in ESP packet. The following sub sections (2.2-2.5)will clarify the NAT-T tunneling solution and procedures in more detailed level.

2.1 Auxiliary procedure

NAT-T presents two separate auxiliary procedures. Both of them are introduces in the following sections.

2.1.1 Tunnel mode decapsulation NAT procedure

In the tunnel mode, the inner IP header can contain addresses that are not suitable for the current networks. This procedure defines how these addresses are to be converted to suitable addresses:

The tunnel mode decapsulation NAT procedure contains following steps [6]:

1. First, check that the source IP addresses of the inner packet is valid according to local policy, if a valid source IP address space has been defined in the local policy for the encapsulated packets from the peer.

2. Second, check that the source IP address used in the inner packet is the assigned IP addresses, if an IP address has been assigned for the remote peer.

3. Third, perform the network address translation for the packet, and make it suitable for transport in the local communication network.

2.1.2 Transport mode decapsulation NAT procedure

When a transport mode has been used to transmit packets, the contained TCP and UDP headers will have incorrect checksums since the change of parts of the inner IP header during the NAT transit. Therefore, this procedure here presents how to fix the checksums.

The transport mode decapsulation NAT procedure contains following steps [6]:

1. First, if the the protocol header after ESP header is a TCP or UDP header, the procedure must incrementally recompute the TCP/UDP checksum:
   i) Subtract the source IP address in the received packet from the checksum
   ii) Add the real source IP address received via IKE to the checksum that is included in IKE payload (NAT-OA)
   iii) Subtract the destination IP address in the received packet from the checksum
   iii) Add the real destination IP address received via IKE to the checksum (IKE NAT-OA payload).

2. Second, recompute the checksum field in the UDP/TCP checksum field, if the protocol header after ESP header is a TCP or UDP header.

3. Third, set the checksum field to zero in the UDP header, if the protocol header after ESP header is a UDP header. If the protocol header

4. Fourth, if the protocol header after ESP header is TCP header, and if there is an option to flag to the stack that the TCP checksum does not need to be computed, then the flag can be used. However, in order to used flag with TCP checksum, this should be used only in transport mode when integrity is protected. Furthermore, for tunnel mode TCP checksums must be verified.

2.2 Transport mode ESP encapsulation

Fig. 5 presents the transport mode ESP encapsulation.

1. First, ordinary ESP encapsulation procedure is used.

2. Second, a properly formatted UDP header is inserted where shown.
ESP
TCP
PAYLOAD
UDP
IP
(ORIGINAL)
IPv4
IPv4
BEFORE APPLYING ESP/UDP
AFTER APPLYING ESP/UDP
ESP TRAILER
ESP AUTH
ENCRIPTED
AUTHENTICATED
Figure 5: The transport mode ESP encapsulation

IPv4
IPv4
BEFORE APPLYING ESP/UDP
AFTER APPLYING ESP/UDP
ESP TRAILER
ESP AUTH
ENCRIPTED
AUTHENTICATED
Figure 6: The tunnel mode ESP encapsulation procedure.

3. Third, the total length, protocol and the header checksum fields are edited to match the resulting IP packet.

2.3 Transport mode ESP decapsulation

1. First, the UDP header is removed from the IP packet.

2. Second, the total length, protocol, header checksum fields in the new IP header are edited to match the resulting IP packet.

3. Third, ordinary ESP decapsulation procedure is used.

4. Fourth, transport mode decapsulation NAT procedure will be performed as described in (2.1.2)

2.4 Tunnel mode ESP encapsulation

Fig. 6 presents the tunnel mode ESP encapsulation.

1. First, ordinary ESP encapsulation procedure is used.

2. Second, a properly formatted UDP header is inserted where shown.

3. Third, the total length, protocol and header checksum fields in the new IP header are edited to match the resulting IP packet.

2.5 Tunnel mode ESP decapsulation

1. First, the UDP header is removed from the packet.

2. Second, the total length, protocol, header checksum fields in the new IP header are edited to match the resulting IP packet.

3. Third, ordinary ESP decapsulation procedure is used.

4. Fourth, tunnel mode decapsulation procedure is used.

3 NAT-T solutions for problems

NAT-T provides solutions to some issues that were listed in the chapter 1.3. We present a summary of the solutions that NAT-T provides [6], [2], [3], [5]:

Problem: **NATs can not update the upper-layer checksum(s)**

- A receiving IPsec peer has all required information (source/destination IP address and port number) that it needs for verification of the upper-layer checksum, when it has received the original IP address in IKE payload (NAT-OA).

Problem: **Identification IKE payload contains embedded IP addresses**

- A receiving IPsec peer has the original IP address where it can verify the contents of the identification IKE payload during the IKE quick mode negotiation, after sending the original IP address in the IKE NAT-OA payload.

Problem: **IKE UDP port number cannot be changed**

- IPsec peers can accept IKE messages from different source port than 500. IPsec NAT-T peers changes the IKE UDP port of 500 to the port 4500 during the IKE main mode negotiation in order to prevent an IKE-aware NAT from modifying the IKE packets.

Problem: **NATs can not multiplex IPsec data streams**

- The NAT router uses the UDP port(s) for multiplexing of the IPsec data streams, when encapsulating the ESP PDU within the UDP header.

Problem: **NAT timeout of IKE UDP port mapping may cause problems**

- NAT-T has a mechanism for sending NAT keep alive packets (detailed description in [6]).
4 Discussion

The NAT router conceals the original source IP address and replaces it by its own (static) or one of its own (dynamic) IP address(es). Moreover, this make the IPsec AH protocol immediately unusable, but IPsec ESP can still be used if both IPsec peers are configured correctly. The problem of NAT traversal mechanism for IPsec is tricky: the main purpose of IPsec protocol is to protect the confidentiality of data, assure the authenticity of sender and the integrity of data. Therefore, when IPsec packet is traversing the NAT router, the main purpose of IPsec is to prevent exactly the activity NAT router is performing to IP packets - IPsec AH/ESP assures that the data has not been changed during the transition. Furthermore, when processing the IPsec packet, only the sender and receiver can create and check the IPsec header values (e.g. HMAC) since the encryption - NAT can only see the outer IP header.

NAT router maintains an internal table where all connections are stored, in order to keep track of outgoing and incoming connections. For example if a terminal in internal network connects to external web server in Internet, NAT conceals the original address with its own and inputs a notification to internal table that indicates all packets coming back on the chosen terminal port will be forwarded to original address/terminal. Furthermore, when another terminal connects to web server in Internet, NAT handles the connection identically, or NAT will modify the port for unambiguity. Therefore, it works well with protocols that provide ports such as UDP and TCP.

IPsec NAT-T encapsulates the IPsec packets in UDP packets that can be easily handled by NAT router - default port number 4500 for UDP is used. Furthermore, a good feature of NAT-T is that once activated the IPsec peers can automatically use it when needed.

However, NAT-T specification also lists possible problems (known as tunnel mode conflict) for implementation of NAT-T. First, there is a possibility for remote IPsec peers to negotiate entries that overlap in a security Gateway (SGW) when IPsec tunneling mode is used. This problem may occur in the case where two separate NAT routers are connected to security gateway, and both NAT routers are having same private IP address space. Therefore, SGW may possibly see two security associations leading to destination private IP addresses which can be same, and that is what may cause some confusion in the SGW. To overcome this problem, one solution could be to make sure that private IP address spaces behind NAT routers are unique (no possibility for overlapping), if the NAT-T is supported in both private networks.

Second problem is known as transport mode conflict which is a similar problem to tunnel mode conflict. Here the problem may occur when for example two terminals behind NAT router in the same private IP address space are in secure communication with external server. In this case, if the protocol and port information for both terminals are overlapping, then simple filter lookups may not be sufficient to determine which SA has to be used to send traffic. Therefore, NAT-T implementation(s) must handle this situation either by disallowing conflicting connections or developing an alternative solution to handle the conflict. The server may see all the terminals behind the NAT router as the same IP address, therefore setting up different local policies for the same traffic descriptor is impossible in principle. The NAT-T specification lists an alternative as solution to apply best effort security: if the terminal behind the NAT router initiates security, his connection will be secured. If the same terminal sends clear text message, the external server will still accept that clear text message.

How NAT-T is used in the current computer networks? Currently, there is some controversy over whether NAT-T may cause a security risk (see transport mode conflict above) when connecting to external servers behind a NAT, and whether the default behavior of WinXP service pack 2 (SP2) creates more problems than solves them. At the moment, WinXP SP2 prevents clients to connect to server behind NAT using IPsec/NAT-T as default behavior. Furthermore, if you wish to allow such connections (IPsec/NAT-T), you can do so with a simple editing the register (0 to 1) on the WinXP client to enable it. For example Microsoft recommends that you give your VPN servers public IP addresses so WinXP clients can connect to them directly rather than through NAT. Furthermore, when using IPsec/NAT-T WinXP clients, the only supported/recommended scenario is the case where client connects to external server through path (client->NAT->Internet->server). If the external server locates behind another NAT (with private IP address), the IPsec/NAT-T will not work.

5 Conclusion and summary

This paper has been discussing NAT Traversal method (NAT-T) for IPsec. IPsec NAT-T presents an UDP based encapsulation method where the IPsec ESP is used for securing the payload. IPsec ESP encrypts only the payload of the data packet, and therefore even the NAT router changes the IP address of the packet, it does not effect to integrity check procedure that IPsec performs on receiver side to IPsec ESP HMAC value. IPsec AH remains incompatible with IPsec ESP HMAC value. The problem of NAT traversal mechanism for IPsec is tricky: the main purpose of IPsec protocol is to prevent exactly the activity NAT router is performing to IP packets - IPsec AH/ESP assures that the data has not been changed during the transition. Furthermore, when processing the IPsec packet, only the sender and receiver can create and check the IPsec header values (e.g. HMAC) since the encryption.
receiver side and the IPsec packet is dropped.

NAT-T has certain problems which are known as tunnel and transport mode conflicts. Both of the problems may occur under special circumstances and most likely in the case where networks (private or public) are in secure communications, high number of end-user using IPsec/NAT-T and NAT router must keep track of each SA that belongs to certain client. Furthermore, it is practically impossible to develop a local policy that could separate the traffic for private connections that are using same protocol and port information. Furthermore, currently the only supported mode for using NAT-T is the use scenario that uses the path (terminal->NAT->Internet->server) for communication. NAT-T does not support the scenario where external server (e.g. web server) would be located in the private network.

References


[2] IP security links and papers (IETF standards, links to related IPsec papers)
http://www.estoiie.com/links/ipsec.htmlIETF20Charters


