Network Working Group
Request for Comments: 2709
Category: Informational

P. Srisuresh
Lucent Technologies

October 1999

Security Model with Tunnel-mode IPsec for NAT Domains

Status of this Memo

Copyright Notice

Abstract

There are a variety of NAT flavors, as described in [Ref 1]. Of the domains supported by NATs, only Realm-Specific IP clients are able to pursue end-to-end IPsec secure sessions. However, all flavors of NAT are capable of offering tunnel-mode IPsec security to private domain hosts peering with nodes in external realm. This document describes a security model by which tunnel-mode IPsec security can be architected on NAT devices. A section is devoted to describing how security policies may be transparently communicated to IKE (for automated KEY exchange) during Quick Mode. Also outlined are applications that can benefit from the Security Model described.

1. Introduction and Overview

NAT devices provide transparent routing to end hosts trying to communicate from disparate address realms, by modifying IP and transport headers en-route. This solution works best when the end user identifier (such as host name) is different from the address used to locate end user.

End-to-end application level payload security can be provided for applications that do not embed realm-specific information in payloads that is meaningless to one of the end-users. Applications that do embed realm-specific information in payload will require an application level gateway (ALG) to make the payload meaningful in both realms. However, applications that require assistance of an ALG en-route cannot pursue end-to-end application level security.

All applications traversing a NAT device, irrespective of whether they require assistance of an ALG or not, can benefit from IPsec tunnel-mode security, when NAT device acts as the IPsec tunnel end point.

Section 2 below defines terms specific to this document.

Section 3 describes how tunnel mode IPsec security can be recognized on NAT devices. IPsec Security architecture, format and operation of various types of security mechanisms may be found in [Ref 2], [Ref 3] and [Ref 4]. This section does not address how session keys and policies are exchanged between a NAT device acting as IPsec gateway and external peering nodes. The exchange could have taken place manually or using any of known automatic exchange techniques.

Section 4 assumes that Public Key based IKE protocol [Ref 5] may be used to automate exchange of security policies, session keys and other Security Association (SA) attributes. This section describes a method by which security policies administered for a private domain may be translated for communicating with external nodes. Detailed description of IKE protocol operation may be found in [Ref 5] and [Ref 6].

Section 5 describes applications of the security model described in the document. Applications listed include secure external realm connectivity for private domain hosts and secure remote access to enterprise mobile hosts.

2. Terminology

Definitions for majority of terms used in this document may be found in one of (a) NAT Terminology and Considerations document [Ref 1], (b) IP security Architecture document [Ref 2], or (c) Internet Key Enchange (IKE) document [Ref 5]. Below are terms defined specifically for this document.

2.1. Normal-NAT

The term "Normal-NAT" is introduced to distinguish normal NAT processing from the NAT processing used for secure packets embedded within an IPsec secure tunnel. "Normal-NAT" is the normal NAT processing as described in [Ref 1].

2.2. IPsec Policy Controlled NAT (IPC-NAT)

The term "IPsec Policy Controlled NAT" (IPC-NAT, for short) is defined to describe the NAT transformation applied as an extension of IPsec transformation to packets embedded within an IP-IP tunnel, for

which the NAT node is a tunnel end point. IPC-NAT function is essentially an adaptation of NAT extensions to embedded packets of tunnel-mode IPsec. Packets subject to IPC-NAT processing are beneficiaries of IPsec security between the NAT device and an external peer entity, be it a host or a gateway node.

IPsec policies place restrictions on what NAT mappings are used. For example, IPsec access control security policies to a peer gateway will likely restrict communication to only certain addresses and/or port numbers. Thus, when NAT performs translations, it must insure that the translations it performs are consist with the security policies.

Just as with Normal-NAT, IPC-NAT function can assume any of NAT flavors, including Traditional-NAT, Bi-directional-NAT and Twice-NAT. An IPC-NAT device would support both IPC-NAT and normal-NAT functions.

3. Security model of IPC-NAT

The IP security architecture document [Ref 2] describes how IP network level security may be accomplished within a globally unique address realm. Transport and tunnel mode security are discussed. For purposes of this document, we will assume IPsec security to mean tunnel mode IPsec security, unless specified otherwise. Elements fundamental to this security architecture are (a) Security Policies, that determine which packets are permitted to be subject to Security processing, and (b) Security Association Attributes that identify the parameters for security processing, including IPsec protocols, algorithms and session keys to be applied.

Operation of tunnel mode IPsec security on a device that does not support Network Address Translation may be described as below in figures 1 and 2.

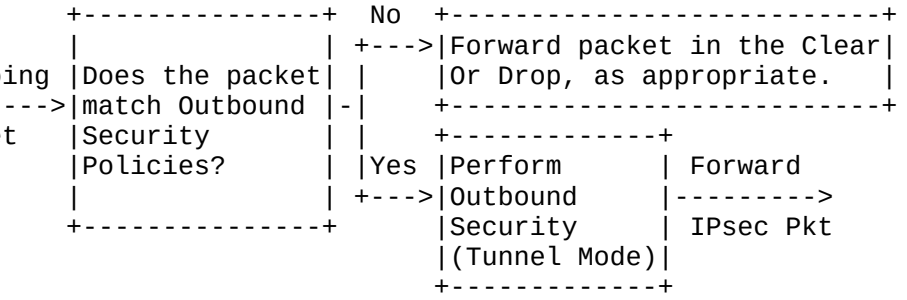

Figure 1. Operation of Tunnel-Mode IPsec on outgoing packets.

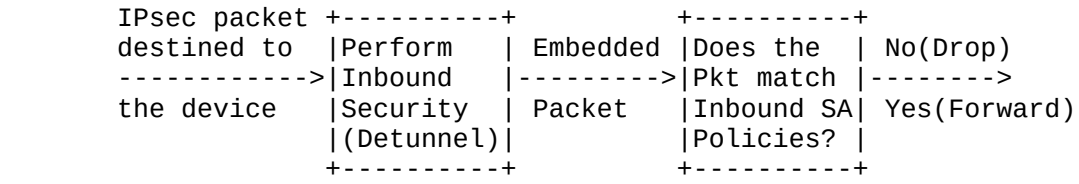

Figure 2. Operation of Tunnel-Mode IPsec on Incoming packets

A NAT device that provides tunnel-mode IPsec security would be required to administer security policies based on private realm addressing. Further, the security policies determine the IPsec tunnel end-point peer. As a result, a packet may be required to undergo different type of NAT translation depending upon the tunnel end-point the IPsec node peers with. In other words, IPC-NAT will need a unique set of NAT maps for each security policy configured. IPC-NAT will perform address translation in conjunction with IPsec processing differently with each peer, based on security policies. The following diagrams (figure 3 and figure 4) illustrate the operation of IPsec tunneling in conjunction with NAT. Operation of an IPC-NAT device may be distinguished from that of an IPsec gateway that does not support NAT as follows.

(1) IPC-NAT device has security policies administered using private realm addressing. A traditional IPsec gateway will have its security policies administered using a single realm (say, external realm) addressing.

(2) Elements fundamental to the security model of an IPC-NAT device includes IPC-NAT address mapping (and other NAT parameter definitions) in conjunction with Security policies and SA attributes. Fundamental elements of a traditional IPsec gateway are limited only to Security policies and SA attributes.

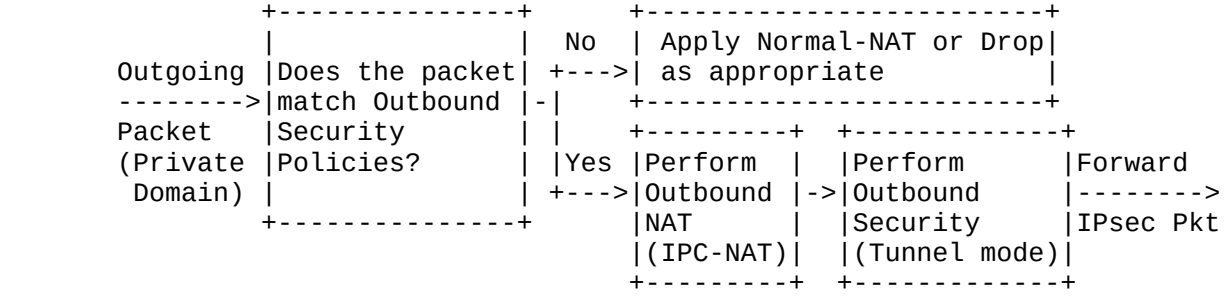

Figure 3. Tunnel-Mode IPsec on an IPC-NAT device for outgoing pkts

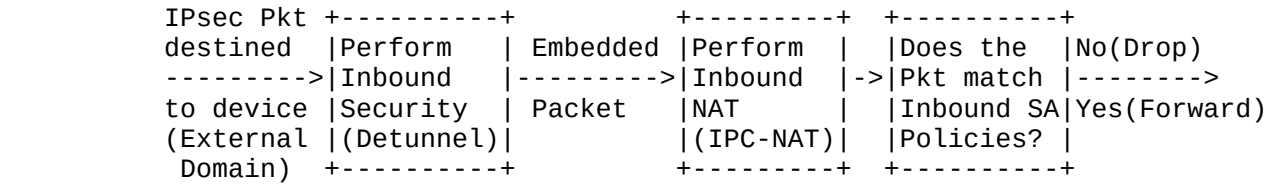

Figure 4. Tunnel-Mode IPsec on an IPC-NAT device for Incoming pkts

Traditional NAT is session oriented, allowing outbound-only sessions to be translated. All other flavors of NAT are Bi-directional. Any and all flavors of NAT mapping may be used in conjunction with the security policies and secure processing on an IPC-NAT device. For illustration purposes in this document, we will assume tunnel mode IPsec on a Bi-directional NAT device.

Notice however that a NAT device capable of providing security across IPsec tunnels can continue to support Normal-NAT for packets that do not require IPC-NAT. Address mapping and other NAT parameter definitions for Normal-NAT and IPC-NAT are distinct. Figure 3 identifies how a NAT device distinguishes between outgoing packets that need to be processed through Normal-NAT vs. IPC-NAT. As for packets incoming from external realm, figure 4 outlines packets that may be subject to IPC-NAT. All other packets are subject to Normal-NAT processing only.

4. Operation of IKE protocol on IPC-NAT device.

IPC-NAT operation described in the previous section can be accomplished based on manual session key exchange or using an automated key Exchange protocol between peering entities. In this section, we will consider adapting IETF recommended Internet Key Exchange (IKE) protocol on a IPC-NAT device for automatic exchange of security policies and SA parameters. In other words, we will focus on the operation of IKE in conjunction with tunnel mode IPsec on NAT devices. For the reminder of this section, we will refer NAT device to mean IPC-NAT device, unless specified otherwise.

IKE is based on UDP protocol and uses public-key encryption to exchange session keys and other attributes securely across an address realm. The detailed protocol and operation of IKE in the context of IP may be found in [Ref 3] and [Ref 4]. Essentially, IKE has 2 phases.

In the first phase, IKE peers operate in main or aggressive mode to authenticate each other and set up a secure channel between themselves. A NAT device has an interface to the external realm and is no different from any other node in the realm to negotiate phase I

with peer external nodes. The NAT device may assume any of the valid Identity types and authentication methodologies necessary to communicate and authenticate with peers in the realm. The NAT device may also interface with a Certification Authority (CA) in the realm to retrieve certificates and perform signature validation.

In the second phase, IKE peers operate in Quick Mode to exchange policies and IPsec security proposals to negotiate and agree upon security transformation algorithms, policies, keys, lifetime and other security attributes. During this phase, IKE process must communicate with IPsec Engine to (a) collect secure session attributes and other parameters to negotiate with peer IKE nodes, and to (b) notify security parameters agreed upon (with peer) during the negotiation.

An IPC-NAT device, operating as IPsec gateway, has the security policies administered based on private realm addressing. An ALG will be required to translate policies from private realm addressing into external addressing, as the IKE process needs to communicate these policies to peers in external realm. Note, IKE datagrams are not subject to any NAT processing. IKE-ALG simply translates select portions of IKE payload as per the NAT map defined for the policy match. The following diagram illustrates how an IKE-ALG process interfaces with IPC-NAT to take the security policies and IPC-NAT maps and generates security policies that IKE could communicate during quick mode to peers in the external realm.

Policies in quick mode are exchanged with a peer as a combination of IDci and IDcr payloads. The combination of IDs (policies) exchanged by each peer must match in order for the SA parameters on either end to be applied uniformly. If the IDs are not exchanged, the assumption would be that the Quick mode negotiated SA parameters are applicable between the IP addresses assumed by the main mode.

Depending on the nature of security policies in place(ex: end-to-end sessions between a pair of nodes vs. sessions with an address range), IKE-ALG may need to request NAT to set up address bindings and/or transport bindings for the lifetime (in seconds or Kilo-Bytes) the sessions are negotiated. In the case the ALG is unable to setup the necessary address bindings or transport bindings, IKE-ALG will not be able to translate security policies and that will result in IKE not pursuing phase II negotiation for the effected policies.

When the Negotiation is complete and successful, IKE will communicate the negotiated security parameters directly to the IPC-NAT gateway engine as described in the following diagram.

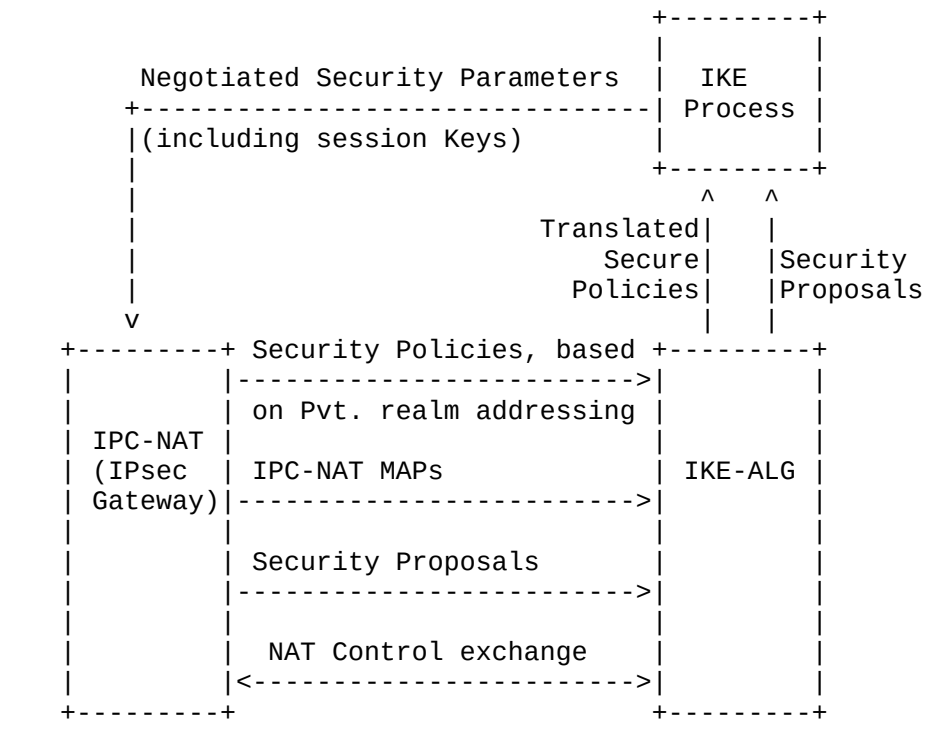

Figure 5. IKE-ALG translates Security policies, using NAT Maps.

5. Applications of IPC-NAT security model

IPC-NAT operational model described thus far illustrates how a NAT device can be used as an IPsec tunnel end point to provide secure transfer of data in external realm. This section will attempt to illustrate two applications of such a model.

5.1. Secure Extranet Connectivity

IPC-NAT Model has a direct application of being able to provide clear as well as secure connectivity with external realm using a NAT device. In particular, IPC-NAT device at the border of a private realm can peer with an IPsec gateway of an external domain to secure the Extranet connection. Extranet refers to the portion of the path that crosses the Internet between peering gateway nodes.

5.2. Secure Remote Access to Mobile Users of an Enterprise

Say, a node from an enterprise moves out of the enterprise, and attempts to connect to the enterprise from remote site, using a temporary service provider assigned address (Care-of-Address). In such a case, the mobile user could setup an IPsec tunnel session with the corporate IPC-NAT device using a user-ID and authentication mechanism that is agreed upon. Further, the user may be configured with enterprise DNS server, as an extension of authentication following IKE Phase I. This would allow the user to access enterprise resources by name.

However, many enterprise servers and applications rely on source IP address for authentication and deny access for packets that do not originate from the enterprise address space. In these scenarios, IPC-NAT has the ability (unlike a traditional IPsec gateway) to perform Network Address Translation (NAT) for remote access users, so their temporary address in external realm is translated into a enterprise domain address, while the packets are within private realm. The flavor of IPC-NAT performed would be traditional NAT (i.e., assuming mobile-user address space to be private realm and Enterprise address space to be external realm), which can either be Basic NAT (using a block of enterprise addresses for translation) or NAPT(using a single enterprise address for translation).

The secure remote access application described is pertinent to all enterprises, irrespective of whether an enterprise uses IANA registered addresses or not.

The secure remote access application described is different from Mobile-IP in that, the mobile node (described in this application) does not retain the Home-Network address and simply uses the Care-Of-address for communication purposes. It is conceivable for the IPC-NAT Gateway to transparently provide Mobile-IP type connectivity to the Mobile node by binding the mobile node’s Care-of-Address with its Home Address. Provision of such an address mapping to IPC-NAT gateway, however, is not within the scope of this document.

6. Security Considerations

If NATs and ALGs are not in a trusted boundary, that is a major security problem, as ALGs snoop end user traffic payload. Application level payload could be encrypted end-to-end, so long as the payload does not contain IP addresses and/or transport identifiers that are valid in only one of the realms. With the exception of Realm-Specific IP, end-to-end IP network level security assured by current IPsec techniques is not attainable with NATs in between. The IPC-NAT model described in this document outlines an

approach by which network level security may be obtained within external realm.

NATs, when combined with ALGs, can ensure that the datagrams injected into Internet have no private addresses in headers or payload. Applications that do not meet these requirements may be dropped using firewall filters. For this reason, it is not uncommon to find that IPC-NATs, ALGs and firewalls co-exist to provide security at the border of a private network.

REFERENCES

[1] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[2] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[3] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998

[4] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[5] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[6] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[7] Carpenter, B., Crowcroft, J. and Y. Rekhter, "IPv4 Address Behavior Today", RFC 2101, February 1997.

[8] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

Author's Address

Pyda Srisuresh
Lucent technologies
4464 Willow Road
Pleasanton, CA 94588-8519
U.S.A.

Phone: (925) 737-2153
Fax: (925) 737-2110
EMail: srisuresh@lucent.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.