1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

2. Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

3. Abstract

Perhaps the most common use of IPSEC is in providing virtual private networking capabilities. One very popular use of VPNs is to provide tele-commuter access to the corporate Intranet. With NATs being increasingly deployed in home gateways, NAT-IPSEC incompatibilities have become a major barrier to deployment of IPSEC in one of its principal uses. This draft describes known incompatibilities between NAT and IPSEC and discusses alternatives for addressing them.

4. Requirements language

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [2].
5. Introduction

Perhaps the most common use of IPSEC [6] is in providing virtual private networking capabilities. One very popular use of VPNs is to provide tele-commuter access to the corporate Intranet. With NATs [8]~[9] being increasingly deployed in home gateways, NAT-IPSEC incompatibilities have become a major barrier to deployment of IPSEC in one of its principal uses. This draft describes known incompatibilities between NAT and IPSEC and discusses alternatives for addressing them.

6. Known incompatibilities between NAT and IPSEC

The incompatibilities between NAT and IPSEC are numerous, ranging from the obvious to the subtle. Some of the known incompatibilities include:

a) Incompatibility between IPSEC AH [3] and NAT. Since the AH header incorporates the IP source and destination addresses in the keyed message integrity check, NAT or reverse NAT devices making changes to address fields will invalidate the message integrity check. Since IPSEC ESP [4] does not incorporate the IP source and destination addresses in its keyed message integrity check, this issue does not arise for ESP.

b) Incompatibility between checksums and NAT. TCP/UDP/SCTP checksums have a dependency on the IP source and destination addresses through inclusion of the "pseudo-header" in the calculation. As a result, where checksums are calculated and checked on receipt, they will be invalidated by passage through a NAT or reverse NAT device.

As a result, IPSEC ESP will only pass unimpeded through a NAT if TCP/UDP/SCTP protocols are not involved (as in IPSEC tunnel mode or IPSEC/GRE), or checksums are not calculated (as is possible with UDP). As described in [13], TCP checksum calculation and verification is required.

c) Incompatibility between IKE address identifiers and NAT. Where IP addresses are used as identifiers in IKE MM [7] or QM, modification of the IP source or destination addresses by NATs or reverse NATs will result in a mismatch between the identifiers and the addresses in the IP header. As described in [7], IKE implementations are required to discard such packets.

While use of userIDs or FQDNs as identifiers is possible within IKE, there are usage scenarios (e.g. SPD entries describing subnets) that cannot be accommodated this way.
d) Incompatibility between fixed IKE destination ports and NAPT. Where multiple hosts behind the NAPT initiate IKE SAs to the same responder, a mechanism is needed to allow the NAPT to demultiplex the incoming IKE packets. This is typically accomplished by translating the IKE UDP source port. While it is permissible to float the IKE UDP source port, this can result in unpredictable behavior during rekeys. Unless the floated source port is used as the destination port for the rekey, the NAT may not be able to send the re-key packets to the correct destination.

Alternatives to source port de-multiplexing, such as IKE cookie de-multiplexing, also result in problems with rekeying, since re-keys typically will not use the same cookies as the earlier traffic.

e) Incompatibilities between overlapping SPD entries and NAT. Where hosts behind a NAT negotiate overlapping SPD entries with the same destination in IKE QM, packets may be sent down the wrong IPSEC SA. This occurs because to the sender, the IPSEC SAs appear to be equivalent, since they exist between the same endpoints and can be used to pass the same traffic.

f) Incompatibilities between IPSEC SPI selection and NAT. Since IPSEC ESP traffic is encrypted and thus opaque to the NAT, the NAT must use elements of the IP and IPSEC header to demultiplex incoming IPSEC traffic. The combination of the source IP address, security protocol (AH/ESP) and IPSEC SPI is typically used for this purpose.

However, since the outgoing and incoming SPIs are chosen independently, there is no way for the NAT to determine what incoming SPI corresponds to what destination host merely by inspecting outgoing traffic. Thus, were two hosts behind the NAT to attempt to bring up IPSEC SAs to the same destination simultaneously, it is possible that the NAT will send the incoming IPSEC packets to the wrong destination.

g) Incompatibilities between embedded IP addresses and NAT. Since the payload is integrity protected, any IP addresses enclosed within IPSEC packets will not be translatable by a NAT. Protocols that utilize embedded IP addresses include FTP, IRC, SNMP, LDAP, H.323, SIP and many games.
7. Alternatives

The following alternatives have been proposed for addressing the incompatibilities between NAT and IPSEC:

- UDP encapsulation
- RSIP
- Changes to IKE

We discuss the pros and cons of each alternative in turn.

7.1. UDP encapsulation

In this approach, IKE and IPSEC packets are encapsulated in UDP prior to being sent. The receiver then discards the outer IP header and UDP encapsulation, thus disregarding any changes that may have been made by intervening NAPTs.

This approach has several advantages. It does not require any changes to either the IKE or IPSEC protocols, and is compatible with all IPSEC protocols (AH/ESP) and modes (transport/tunnel), although some changes to IKE implementations are required. Since it relies only on NAPT support for UDP, this approach is likely to work with the vast majority of existing NAT implementations.

In terms of disadvantages, this proposal requires changes to existing hosts, and adds 28 octets of additional overhead. By adding a NAT compatibility mode to IKE/IPSEC, the total time to negotiate an IPSEC SA may be increased significantly. For example, when an IKE initiator fails to receive a response, it will typically need to try again using UDP encapsulation, since the lack of response may have been due to the presence of intervening NATs.

7.2. RSIP

RSIP, described in [10]-[11], includes mechanisms for IPSEC traversal, as described in [12]. By enabling host-gateway communication, RSIP addresses issues of IPSEC SPI de-multiplexing as well as SPD overlap. It is thus suitable for use in enterprise as well as home networking scenarios.

By tunneling IKE and IPSEC packets, RSIP avoids changes to the IKE and IPSEC protocols, although major changes are required to IKE and IPSEC implementations to retrofit them for RSIP-compatibility. It is thus compatible with all existing protocols (AH/ESP) and modes (transport and tunnel).
In order to handle de-multiplexing of IKE re-keys, RSIP requires floating of the IKE source port, as well as re-keying to the floated port. As a result, interoperability with existing IPSEC implementations is not assured.

Disadvantages of RSIP include that it requires major changes to both host implementations as well as to gateways. As a result, an RSIP-enabled host requires a corresponding RSIP-enabled gateway in order to establish an IPSEC SA with another host.

7.3. IKE and checksum processing changes

In this approach, a number of changes are made in IKE usage and checksum processing. The advantage of this approach is that it does not add additional overhead as does the encapsulation approach. In addition, minimal changes are required to the IKE or IPSEC protocols.

However, this approach offers only limited compatibility with IPSEC tunnel mode (only enabling negotiation of "me" and "any" SPD entries), and may only be used to allow transport of IPSEC ESP through a NAT, not AH.

This approach also requires changes to host implementations as well as modest changes to existing NATs. As a result, it can be expected to work with a substantial fraction of existing NATs, although by no means all of them.

Another disadvantage of this approach is that it does not address issues of SPD conflict or incoming IPSEC SPI de-multiplexing. As a result, unless it is combined with a host-gateway communication protocol such as RSIP, this approach cannot be applied to enterprise scenarios where multiple hosts behind the NAT may establish IPSEC SAs to the same destination.

In this approach, the following changes are required:

a) Use of IPSEC ESP null instead of AH.
   Since IPSEC ESP null provides integrity protection and authentication services without covering the IP header in the message integrity check, IPSEC ESP null is used in preference to IPSEC AH.

b) Optional checksum verification for IPSEC transport mode SAs.
   Since transport mode IPSEC traffic is integrity protected and authenticated using strong cryptography, modifications to the packet can be detected prior to checking UDP/TCP/SCTP checksums. Thus, checksum verification only provides assurance against errors made in internal processing. In order to
remove the incompatibility between checksum processing and NAT, checksum verification is made optional on packets covered by IPSEC transport mode SAs.

c) Floating IKE source ports.
To enable NATs to easily de-multiplex IKE traffic, it is more convenient to float IKE source ports than it is to de-multiplex using cookies. Assuming source ports are floated, to enable de-multiplexing of IKE re-keys, the initiator will need to send the re-key packets to the IKE source port used in the original negotiation. Use of floated IKE source ports is already allowed within IKE [7].

d) Use of userIDs and FQDNs as IKE MM and QM identifiers.
In order to avoid use of IP addresses as IKE MM and QM identifiers, userIDs and FQDNs are used instead. Where user authentication is desired, an ID type of ID_USER_FQDN can be used, as described in [5]. Where machine authentication is desired, an ID type of ID_FQDN can be used. In either case it is necessary to verify that the proposed identity matches that enclosed in the certificate.

8. Security considerations

Since the UDP encapsulation approach requires the additional work of decapsulation prior to IPSEC processing, it may result in increased susceptibility to denial of service attacks. However, since no changes are made in IKE or IPSEC usage, no other vulnerabilities are introduced.

The RSIP approach introduces major changes to both hosts and gateways so that it is likely that additional bugs will be introduced as a result of the scale of the required changes. However, the RSIP does not introduce changes to IPSEC and IKE processing other than the use of floating source ports, so that no new protocol vulnerabilities are created.

Changes in IKE usage and checksum processing introduce changes on both the host and gateways so that new implementation bugs may be introduced as a result. Of the usage changes, the most significant from a security point of view is the change in usage of IKE MM and QM identifiers. There is no security value to TCP/UDP/SCTP checksums, so not checking them does not decrease security. Similarly, use of IPSEC ESP null instead of AH does not introduce any security vulnerabilities.

Where certificate-based authentication is possible, it is believed that the use of ID_USER_FQDN or ID_FQDN in IKE MM instead of addresses will not introduce additional security vulnerabilities, as long as the presented identity is verified to correspond to that in the certificate.
Use of ID_FQDN or ID_USER_FQDN identifiers in IKE QM raises the issue as to what traffic will be accepted in the IPSEC SA. Since packets will be integrity protected, it is possible to verify that the source is in possession of the negotiated keys. Thus, for transport mode SAs, it may be sufficient to require that traffic originate only from a single IP address (such as as the address used in the IKE QM negotiation), and to verify packet integrity.

Things are somewhat trickier for IPSEC tunnel mode, where restricting identifiers to ID_USER_FQDN or ID_FQDN would prevent use of subnet or address range identifiers, which may be required for gateway to gateway communications. Thus this approach is not universally applicable.

However, in client to gateway communications with IPSEC tunnel mode SAs, these restrictions may be more workable. If subnet or IP address range identifiers are not used, it is reasonable to assume that only traffic from a single IP address is permitted inside the tunnel. A reasonable assumption would be that this IP address corresponds to the source address used when setting up the IKE QM SA.

9. Acknowledgments

Thanks to Steve Bellovin of AT&T Research, William Dixon of Microsoft, and Daniel Senie for useful discussions of this problem space.

10. References


[8] Srisuresh, P., and Egevang, K., "Traditional IP Network Address Translator (Traditional NAT)", Internet draft (work in progress), draft-ietf-nat-traditional-03.txt, September 1999.


11. Authors’ Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-936-6605
EMail: bernarda@microsoft.com

12. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.
The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

13. Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

14. Expiration Date

This memo is filed as <draft-aboba-ipsec-nat-02.txt>, and expires February 1, 2001.