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 discusses the incompatibilities between NAT and IPSEC and suggests how IPSEC might be made more NAT friendly.

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 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 discusses the incompatibilities between NAT and IPSEC and suggests how IPSEC might be made more NAT friendly.

6. NAT/IPSEC incompatibilities

The known incompatibilities between NAT and IPSEC are as follows:

a) IPSEC AH [3] will not go through the NAT, because the AH header incorporates the IP source and destination fields in the authentication hash.

b) IPSEC ESP [4] does not incorporate the IP source and destination fields in its authentication hash. However, there is an implicit dependency on source and destination addresses within TCP/UDP/SCTP checksums which cover the "pseudo-header." Therefore IPSEC ESP will only go through the NAT if TCP/UDP/SCTP protocols are not involved (as in IPSEC tunnel mode or IPSEC/GRE), UDP checksums are turned off (TCP checksums are required), or if TCP/UDP/SCTP checksums are ignored by the receiving party.

c) Where IP addresses are used as identifiers in IKE MM [7] or QM, IKE will only go through the NAT if the parties do not check or use IP addresses in IKE MM identifiers (several current implementations don’t do this) AND if in addition they don’t check or use IP addresses in IKE QM identifiers (most implementations DO use addresses and check them).

d) Because of IKE re-keying behavior, it is necessary for implementations to float their IKE source port in order to enable NATs to de-multiplex incoming re-keys which may not use the same cookies as the earlier traffic. Otherwise it is possible for the re-key to be sent to the wrong SA by the NAT.

e) In order to enable an IPSEC implementation to send traffic down the correct IPSEC SA, it is necessary for those SAs to be differentiated in some way. In practice this implies negotiation of non-overlapping SPD entries. For example, if two clients behind a NAT were to negotiate the same SPD entries, then there would be no way to decide which SA
to use to protect a given packet.

f) Since 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 and IPSEC SPI is typically used for this purpose. If the initiator is behind a NAT then since the responder chooses the SPI, the combination of source address and SPI will be unique. However, if the responder is behind a NAT then it is possible (though unlikely) that the same SPI value will be chosen by two or more responders. In this case the NAT could send the IPSEC packets to the wrong destination.

7. Recommendations

It is recommended that the following actions be taken to improve the NAT-friendliness of IPSEC:

a) Since IPSEC ESP null provides much the same security services as IPSEC AH, but without explicitly covering the IP header in its authentication hash, it is recommended that IPSEC ESP null be used instead of AH.

b) Since transport mode IPSEC traffic is integrity protected and authenticated using strong cryptography, there is little to gained by having the receiver check TCP/UDP/SCTP checksums on traffic protected by IPSEC transport mode SAs. It is therefore recommended that checksum verification be made optional in this case.

c) Since proper de-multiplexing of IKE re-keys is dependent on initiators floating their IKE source ports, it is recommended that IKE implementations float their source ports.

d) It is recommended that IP addresses not be used as identifiers in IKE MM. Where user authentication is done, a network access identifier (user@realm) can be used instead. In the case of machine authentication, an FQDN can be used. In practice use of IP address identifiers in IKE MM provides little security value, since assuming that the integrity of the IKE packets is verified, it can be assumed that the correspondent has possession of the correct keys.

e) In tele-commuter scenarios, it is expected that both IPSEC transport mode (for L2TP/IPSEC as well as other UDP and TCP) and IPSEC tunnel mode will be commonly used. In these cases, the SFD entries typically only need to protect traffic
between the two endpoints. In such circumstances, use of an FQDN (machine identifier) or NAI (user identifier) should be permitted within the SPD negotiation in IKE QM.

8. Security considerations

It is not believed that the changes described above will impact IPSEC security adversely. 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.

9. Acknowledgments

Thanks to William Dixon of Microsoft for many useful discussions of this problem space.

10. References


11. Authors’ Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
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-00.txt>, and expires January 1, 2001.