Network Working Group P. Hoffman
Internet-Draft VPN Consortium
Expires: February 25, 2008 D. McGrew
Cisco Systems
August 24, 2007

An Authentication-only Profile for ESP with an IP Protocol Identifier
draft-hoffman-esp-null-protocol-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on February 25, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

It is desirable to allow firewalls and intrusion detection systems to be able to inspect the payload of an ESP packet that has been encrypted with the NULL cipher. This would allow a firewall to read the contents and apply the normal policies to it. However, a device in the network cannot reliably determine which ESP packets are NULL encrypted, and cannot easily determine other ESP format parameters such as the ICV length. These issues can cause misclassification of

packets and wasted computational resources.

This document solves this problem by defining an authentication-only profile of ESP and reserving IP protocol numbers for it.

Table of Contents

1. Introduction 3
2. Using New IP Protocol Numbers 4
  2.1. Marking ESP NULL Packets 4
  2.2. Negotiating ESP NULL in IKE 4
  2.3. Firewalls and the New Protocol Numbers 5
3. IANA Considerations 5
4. Security Considerations 5
5. Normative References 5
Authors' Addresses 6
Intellectual Property and Copyright Statements 7

1. Introduction

The ESP protocol can be used with NULL encryption to provide authentication and integrity protection, but not confidentiality. This use of ESP is beneficial when access control and integrity are needed, but confidentiality is not. A good example is the case in which it is desirable to use authentication and integrity protection to prevent the spread of worms, or to prevent unauthorized access to network resources. In these scenarios, one of the benefits of authentication-only ESP is that devices in the network can inspect the ESP-protected traffic to help them meet their security goals.

Unfortunately, the ESP packet format cannot be unambiguously parsed except by the sender and receiver(s). Heuristic methods to parse ESP packets can be used, but these methods are not robust and they fail when their assumptions about ESP parameters and algorithms are wrong.

When using IPsec [RFC4301] for integrity but not encryption, a system administrator needs to decide whether to use AH [RFC4302], or to use ESP [RFC4303] with NULL encryption. The ability for systems that do ESP to support NULL encryption is mandated by [RFC4835]. Many IPsec system vendors do not support AH, making ESP with NULL encryption the natural choice for interoperable IPsec that provides only integrity.

Many firewalls can inspect the contents of the packets they process; such firewalls are often called "content-inspecting firewalls" or CIFs. CIFs often allow the firewall administrator to set policies such as "do not allow packets that cannot be inspected". Packets whose contents are encrypted (where the encryption is not performed by the firewall itself) would fall into that category.

A CIF can inspect the contents of every packet, but if some of the packets are known to be encrypted ESP packets, such inspection is wasteful. On the other hand, because ESP with NULL encryption is allowed, a CIF might need to inspect the content of every ESP packet in case it is encrypted with NULL encryption.

Some firewalls are also used for access control. Like CIFs, these ACL-enforcing firewalls sometimes also need to inspect the contents of packets when enforcing some access rules. Firewalls that act as intrusion detection systems and intrusion prevention systems (IDS/IPS) also often need to inspect packet contents, and thus have the same problems as CIFs when handling ESP traffic with NULL encryption.

This document defines a way to mark ESP packets as being encrypted with NULL encryption so that a firewall can know that it should inspect the contents. The marking is done with new IP protocol numbers. This document does not mandate such marking. Because the

marking is not mandated, the firewall may still want to inspect ESP packets that are not marked. However, by marking the ESP packets that are sure to use NULL encryption, it frees resources in the firewall. Using this marking method allows full interoperability with unchanged IKE v1 and IKE v2 implementations.

[[NOTE: the values TBD1 and TBD2 throughout this document need to be changed with the values are assigned by IANA.]]

2. Using New IP Protocol Numbers

2.1. Marking ESP NULL Packets

There are multiple ways to use NULL encryption in ESP. The method described in [RFC2410] causes the content of the ESP packet to appear just as it did in the plaintext message. The method described in [RFC4543] prepends an eight-octet initialization vector (IV) to the beginning of the content of every ESP packet. In order to enable unambiguous parsing of ESP packets, each profile fixes the length of the Integrity Check Value (ICV) and Initialization Vector (IV).

An ESP implementation that uses NULL encryption based on RFC 2410 may mark a packet with IP protocol number TBD1 instead of the normal protocol number of 50 that was assigned by IANA for ESP. The length of the IV is zero, and the length of the ICV is zero. [[NOTE FOR FUTURE DRAFT: determine what ICV length is commonly deployed here.]]

An ESP implementation that uses NULL encryption based on RFC 4543 may mark a packet with IP protocol number TBD2 instead of the normal protocol number of 50 that was assigned by IANA for ESP. The length of the IV is 8 octets, and the length of the ICV is 16 octets.

Future ESP authentication methods that do not change the plaintext message before putting it in the content can also use IP protocol TBD1. Similarly, future ESP ESP authentication methods that add exactly eight octets to the beginning of the content but leaves the rest of the plaintext alone can also use IP protocol TBD2.

2.2. Negotiating ESP NULL in IKE

When initiating IKE (either v1 or v2), the initiator can include two proposed transforms: one with the new IP protocol number, and one with IP protocol 50 (ESP). If the responder understands the new protocol numbers, it can accept and use them in the resulting ESP traffic; otherwise, the responder can still accept the older protocol numbers and use 50 as the protocol number.

2.3. Firewalls and the New Protocol Numbers

A firewall that sees one of the new protocol numbers can be assured that it can inspect the content of the ESP packets. In specific, a firewall that sees a packet with IP protocol number TBD1 can reliably determine the starting point and the length of the plaintext, and a packet with IP protocol number TBD2 has eight octets of IV (that the firewall can ignore) and then the plaintext.

A possible downside to adopting this marking method is that firewalls that block unknown IP protocols will need to be updated to handle IP protocol numbers TBD1 and TBD2. Fortunately, many (possibly most) firewalls allow such updating as policy settings by the firewall's administrator; such firewalls would not need a firmware update.

3. IANA Considerations

IANA is requested to assign the following from the "Protocol Numbers" registry:

TBD1	ESP-AUTH-ONLY-NO-IV	[This document]
TBD2	ESP-AUTH-ONLY-8-OCTET-IV	[This document]

4. Security Considerations

An attacker who can modify packets between the originator and a firewall that understands the new protocol numbers can change the protocol number on encrypted ESP packets from 50 to either of the new values. If the firewall is a CIF, this might cause the firewall to spend more resources than it would on unaltered packets.

5. Normative References

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

Authors' Addresses

Paul Hoffman
VPN Consortium
127 Segre Place
Santa Cruz, CA 95060
US

Phone: 1-831-426-9827
Email: paul.hoffman@vpnc.org

David McGrew
Cisco Systems
San Jose, CA 95134
US

Email: mcgrew@cisco.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).