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.

This Internet-Draft will expire on February 27, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

The DHCP Relay Agent Information Option (RFC 3046) conveys information between a DHCP relay agent and a DHCP server. This specification defines a mechanism for securing the messages exchanged between a relay agent and a server using IPsec (RFC 2401).
Table of Contents

1. Requirements Terminology .................................. 3
2. DHCP Terminology ........................................... 3
3. Introduction ................................................. 3
4. Use of IPsec to secure DHCP messages ....................... 3
5. IANA Considerations ......................................... 5
6. Security Considerations ...................................... 5
7. IPsec Considerations ......................................... 5
8. Acknowledgments ............................................... 5
   Normative references ........................................ 5
   Informative References ...................................... 5
   Author’s Address ........................................... 6
   Intellectual Property and Copyright Statements ............ 7
1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. DHCP Terminology

This document uses the terms "DHCP server" (or "server") and "DHCP client" (or "client") as defined in RFC 2131. The term "DHCP relay agent" refers to a "BOOTP relay agent" as defined in RFC 2131.

3. Introduction

DHCP (RFC 2131) provides IP addresses and configuration information for DHCP clients. It includes a relay agent capability (RFC 951, RFC 1542), in which processes within the network infrastructure receive broadcast messages from clients and forward them to servers as unicast messages. In network environments like DOCSIS data-over-cable and xDSL, for example, it has proven useful for the relay agent to add information to the DHCP message before forwarding it, using the relay agent information option, RFC 3046. The kind of information that a relay agent adds is often used in the server’s decision making about the addresses and configuration parameters that the client should receive. The way that the relay agent data is used in server decision-making tends to make that data very important, and highlights the importance of the trust relationship between the relay agent and the server.

The existing DHCP Authentication specification (RFC 3118) only secures communication between the DHCP client and server. Because relay agent information is added after the client has signed its message, the DHCP Authentication specification explicitly excludes relay agent data from that authentication.

The goals of this specification is to define a method that a relay agent can use to:

1. protect the integrity of the data that the relay adds
2. provide replay protection for that data
3. leverage the existing IPsec mechanism

4. Use of IPsec to secure DHCP messages

Relay agents and servers that exchange messages securely can use
IPsec mechanisms [3] as described in this section. If a client message is relayed through multiple relay agents, each of the relay agents must have established independent, pairwise trust relationships. That is, if messages from client C will be relayed by relay agent A to relay agent B and then to the server, relay agents A and B must be configured to use IPsec for the messages they exchange, and relay agent B and the server must be configured to use IPsec for the messages they exchange.

Relay agents and servers that support secure relay agent to server or relay agent to relay agent communication use IPsec under the following conditions:

Selectors: Relay agents are manually configured with the addresses of the relay agent or server to which DHCP messages are to be forwarded. Each relay agent and server that will be using IPsec for securing DHCP messages must also be configured with a list of the relay agents to which messages will be returned. The selectors for the relay agents and servers will be the pairs of addresses defining relay agents and servers that exchange DHCP messages on the DHCP UDP ports 67 and 68.

Mode: Relay agents and servers use transport mode and ESP [4]. The information in DHCP messages is not generally considered confidential, so encryption need not be used (i.e., NULL encryption can be used).

Key management: Because the relay agents and servers are used within an organization, public key schemes are not necessary. Because the relay agents and servers must be manually configured, manually configured key management may suffice, but does not provide defense against replayed messages. Accordingly, IKE with preshared secrets SHOULD be supported. IKE with public keys MAY be supported.

Security policy: DHCP messages between relay agents and servers should only be accepted from DHCP peers as identified in the local configuration.

Authentication: Shared keys, indexed to the source IP address of the received DHCP message, are adequate in this application.

Availability: Appropriate IPsec implementations are likely to be available for servers and for relay agents in more featureful devices used in enterprise and core ISP networks. IPsec is less likely to be available for relay agents in low end devices primarily used in the home or small office markets.
5. IANA Considerations

There are no IANA considerations for the authentication mechanisms described in this document.

6. Security Considerations

This specification describes a mechanism that can be used to provide authentication and message integrity protection to the messages between DHCP relay agents and DHCP servers.

The authentication sub-option protocol requires configuration of relay agents and servers with shared secret keys.

7. IPsec Considerations

The use of IPsec for securing relay agent options in DHCP messages requires the existence of an IPsec implementation available to the relay agents and DHCP servers. It also requires manual configuration of the participants, including manual distribution of keys.

8. Acknowledgments

The need for this specification was made clear by comments made by Thomas Narten and John Schnizlein at IETF 53.

Normative references


Informative References


Author’s Address

Ralph Droms
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA  01719
USA

Phone: +1 978.936.1674
EMail: rdroms@cisco.com
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.

Full Copyright Statement

Copyright (C) The Internet Society (2003). 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 assignees.

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.

Acknowledgment

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