IPSEC Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-ietf-ipsec-dhcp-12.txt>

Baiju Patel
Intel
Bernard Aboba
Microsoft
Scott Kelly
RedCreek Communications
Vipul Gupta
Sun Microsystems, Inc.

DHCPv4 Configuration of IPsec Tunnel Mode

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

This document is an Internet-Draft. 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.

Abstract

In many remote access scenarios, a mechanism for making the remote host appear to be present on the local corporate network is quite useful. This may be accomplished by assigning the host a "virtual" address from the corporate network, and then tunneling traffic via IPsec from the host's ISP-assigned address to the corporate security gateway. In IPv4, Dynamic Host Configuration Protocol (DHCP) provides for such remote host configuration. This draft explores the requirements for host configuration in IPsec tunnel mode, and describes how DHCPv4 may be leveraged for configuration.

Table of contents

1 Introduction..... 2
1.1 Terminology..... 2
1.2 Requirements Language..... 3
2.0 IPsec tunnel mode configuration requirements..... 3
2.1 DHCP configuration evaluation..... 3
2.2 Summary..... 4
3.0 Scenario overview..... 4
3.1 Configuration walk-through..... 5
4.0 Detailed description..... 6
4.1 DHCPDISCOVER message processing..... 7
4.2 DHCP Relay behavior..... 9
4.3 DHCPREQUEST message processing..... 10
4.4 DHCPACK message processing..... 10
4.5 Configuration policy..... 10
5.0 Security Considerations..... 11
6.0 IANA Considerations..... 11
7.0 Intellectual Property Statement..... 12
8.0 References..... 12
9.0 Acknowledgments..... 14
10.0 Author's Address..... 14
11.0 Appendix - IKECFG evaluation..... 15
12.0 Full Copyright Statement 16

1. Introduction

In many remote access scenarios, a mechanism for making the remote host appear to be present on the local corporate network is quite useful. This may be accomplished by assigning the host a "virtual" address from the corporate network, and then tunneling traffic via IPsec from the host's ISP-assigned address to the corporate security gateway. In IPv4, Dynamic Host Configuration Protocol (DHCP) [3] provides for such remote host configuration. This draft explores the requirements for host configuration in IPsec tunnel mode, and describes how DHCPv4 may be leveraged for configuration.

1.1. Terminology

This document uses the following terms:

DHCP client
: A DHCP client or "client" is an Internet host using DHCP to obtain configuration parameters such as a network address.

DHCP server
: A DHCP server or "server" is an Internet host that returns configuration parameters to DHCP clients.

1.2. 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 [1].

2. IPsec tunnel mode configuration requirements

As described in [21], the configuration requirements of a host with an IPsec tunnel mode interface include the need to obtain an IPv4 address and other configuration parameters appropriate to the class of host. In addition to meeting the basic requirements [21], the following additional capabilities may be desirable:

a. integration with existing IPv4 address management facilities
b. support for address pool management
c. reconfiguration when required
d. support for fail-over
e. maintaining security and simplicity in the IKE implementation.
f. authentication where required

2.1. DHCP configuration evaluation

Leveraging DHCP for configuration of IPsec tunnel mode meets the basic requirements described in [21]. It also provides the additional capabilities described above.

Basic configuration
: In IPv4, leveraging DHCPv4 [3] for the configuration of IPsec tunnel mode satisfies the basic requirements described in [21]. Since the required configuration parameters described in [21] are a subset of those already supported in DHCPv4 options [5], no new DHCPv4 options are required, and no modifications to DHCPv4 [3] are required.

Address management integration
: Since DHCPv4 is widely deployed for address management today, reuse of DHCPv4 for IPsec tunnel mode address management enables compatibility and integration with existing addressing implementations and IPv4 address management software.

Address pool management
: As described in [18], DHCPv4 implementations support conditional behavior so that the address and configuration parameters assigned can be dependent on parameters included in the DHCPDISCOVER. This makes it possible for the security gateway to ensure that the remote host receives an IP address assignment from the appropriate address pool, such as via the

User Class option, described in [16].

Reconfiguration
DHCP supports the concept of configuration leases, and there is a proposal for handling forced reconfiguration [14].

Fail-over support
When leveraging DHCPv4, configuration and addressing state is kept on the DHCP server, not within the IKE implementation. As a result, the loss of a tunnel server does not result in the loss of configuration and addressing state, thus making it easier to support fail-over [8].

Security and simplicity
Leveraging DHCPv4 also makes it easier to maintain security in the IKE implementation since no IKE modifications are required to support configuration.

Authentication
Where DHCPv4 authentication [6] is required, this can be supported on an IPsec tunnel mode interface as it would be on any other interface.

2.2. Summary

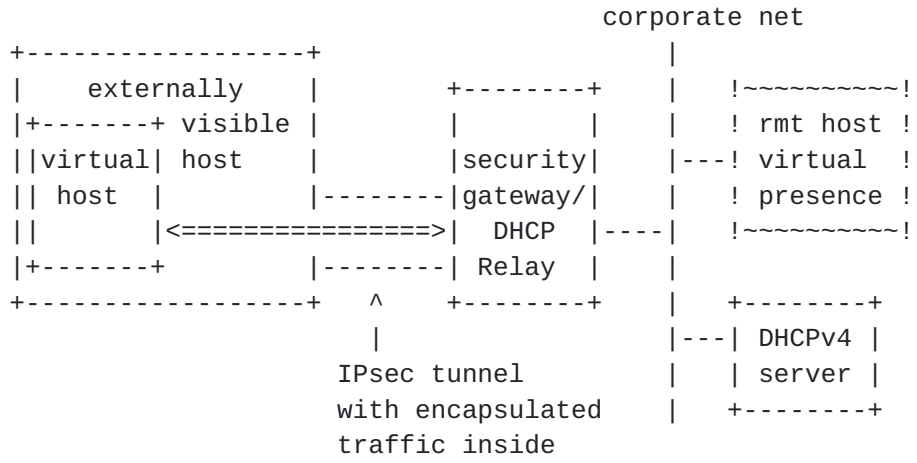
As described, DHCPv4 [3] meets the IPsec tunnel mode configuration requirements [21], as well as providing additional capabilities. As described in the Appendix, IKECFG [13] does not meet the basic requirements, nor does it provide the additional capabilities. As a result, DHCPv4 is the superior alternative for IPsec tunnel mode configuration.

3. Scenario overview

IPsec [2], [9]-[12] is a protocol suite defined to secure communication at the network layer between communicating peers. Among many applications enabled by IPsec, a useful application is to connect a remote host to a corporate intranet via a security gateway, using IPsec tunnel mode. This host is then configured in such a manner so as to provide it with a virtual presence on the internal network. This is accomplished in the following manner:

A remote host on the Internet will connect to the security gateway and then establish an IPsec tunnel to it. The remote host then interacts via the IPsec tunnel with a DHCPv4 server which provides the remote host with an address from the corporate network address space. The remote host subsequently uses this as the source address for all interactions with corporate resources. Note that this implies that the corporate

security gateway continues to recognize the host's original, routable IP address as the tunnel endpoint. The virtual identity assumed by the remote host when using the assigned address appears to the corporate network as though it were situated behind a security gateway bearing the original routable IP address. All the traffic between the remote host and the intranet will be carried over the IPsec tunnel via the security gateway as shown below:



This scenario assumes that the remote host already has Internet connectivity and the host Internet interface is appropriately configured. The mechanisms for configuration of the remote host's address for the Internet interface are well defined; i.e., PPP IP control protocol (IPCP), described in [4], DHCPv4, described in [3], and static addressing. The mechanisms for auto-configuration of the intranet are also standardized. It is also assumed that the remote host has knowledge of the location of the security gateway. This can be accomplished via DNS, using either A, KX [23], or SRV [24] records.

A typical configuration of the remote host in this application would use two addresses: 1) an interface to connect to the Internet (Internet interface), and 2) a virtual interface to connect to the intranet (intranet interface). The IP address of the Internet and intranet interfaces are used in the outer and inner headers of the IPsec tunnel mode packet, respectively.

3.1. Configuration walk-through

The configuration of the intranet interface of the IPsec tunnel mode host is accomplished in the following steps:

a. The remote host establishes an IKE security association with the security gateway in a main mode or aggressive mode exchange. This IKE SA then serves to secure additional quick mode IPsec SAs.

b. The remote host establishes a DHCP SA with the IPsec tunnel mode server in a quick mode exchange. The DHCP SA is an IPsec tunnel mode SA established to protect initial DHCPv4 traffic between the security gateway and the remote host. The DHCP SA MUST only be used for DHCP traffic. The details of how this SA is set up are described in Section 4.1.

c. DHCP messages are sent back and forth between the remote host and the DHCPv4 server. The traffic is protected between the remote host and the security gateway using the DHCP SA established in step b. After the DHCP conversation completes, the remote host's intranet interface obtains an IP address as well as other configuration parameters.

d. The remote host MAY request deletion of the DHCP SA since future DHCP messages will be carried over a new IPsec tunnel. Alternatively, the remote host and the security gateway MAY continue to use the same SA for all subsequent traffic by adding temporary SPD selectors in the same manner as is provided for name ID types in [2].

e. If a new IPsec tunnel is required, the remote host establishes a tunnel mode SA to the security gateway in a quick mode exchange. In this case, the new address assigned via DHCPv4 SHOULD be used in the quick mode ID.

At the end of the last step, the remote host is ready to communicate with the intranet using an IPsec tunnel. All the IP traffic (including future DHCPv4 messages) between the remote host and the intranet are now tunneled over this IPsec tunnel mode SA.

Since the security parameters used for different SAs are based on the unique requirements of the remote host and the security gateway, they are not described in this document. The mechanisms described here work best when the VPN is implemented using a virtual interface.

4. Detailed description

This section provides details relating to the messages exchanged during the setup and teardown of the DHCP SAs.

4.1. DHCPDISCOVER message processing

The events begin with the remote host intranet interface generating a DHCPDISCOVER message. Details are described below:

FIELD	OCTETS	DESCRIPTION
op	1	Message op code / message type. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Hardware address type. Set to value (TBD) signifying an IPsec tunnel mode virtual interface.
hlen	1	Hardware address length
hops	1	Client sets to zero, optionally used by relay agents when booting via a relay agent.
xid	4	Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server.
secs	2	Filled in by client, seconds elapsed since client began address acquisition or renewal process.
flags	2	Flags. Broadcast bit MUST be set to zero.
ciaddr	4	Client IP address; only filled in if client is in BOUND, RENEW or REBINDING state.
yiaddr	4	'your' (client) IP address.
siaddr	4	IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK by server.
giaddr	4	Security gateway interface IPv4 address, used in booting via a relay agent.
chaddr	16	Client hardware address. Should be unique.
sname	64	Optional server host name, null terminated string.
file	128	Boot file name, null terminated string; "generic" name or null in DHCPDISCOVER, fully qualified directory-path name in DHCPOFFER.
options	var	Optional parameters field.

Table 1: Description of fields in the DHCP message

The htype value is set to the value TBD, signifying a virtual IPsec tunnel mode interface, in order to enable the DHCP server to differentiate VPN from non-VPN requests. The chaddr field of the DHCPDISCOVER MUST include an identifier unique to the virtual subnet. The client MUST use the same chaddr field in all subsequent messages within the same DHCPv4 exchange. In addition, the chaddr SHOULD be persistent between reboots so that the DHCP server will be able to re-assign the same address if desired.

The hlen and chaddr fields SHOULD be determined as follows:

a. If one or more LAN interfaces are available, the hlen and chaddr fields SHOULD be determined from the active LAN interface with the lowest interface number. If no active LAN interface is available, then the parameters SHOULD be determined from the LAN interface with the lowest interface number. This enables the chaddr to be persistent between reboots, as long as the LAN interface hardware is not removed.

b. If there is no LAN interface, the chaddr field SHOULD be determined by concatenating x'4000', the IPv4 address of the interface supplying network connectivity, and an additional octet. The x'4000' value indicates a locally administered unicast MAC address, thus guaranteeing that the constructed chaddr value will not conflict with a globally assigned value.

   The additional octet (which MAY represent an interface number) SHOULD be persistent between reboots, so that the chaddr value will be persistent across reboots if the assigned IPv4 address remains consistent.

If the above prescription is followed, then the chaddr will always be unique on the virtual subnet provided that the remote host only brings up a single tunnel to the security gateway. Where a LAN interface is available, the chaddr will be globally unique. When a non-LAN interface is available and a unique Internet address is assigned to the remote host, the chaddr will also be globally unique. Where a private IP address [22] is assigned to a non-LAN interface, it will not be globally unique. However, in this case packets will not be routed back and forth between the remote host and the security gateway unless the external network and corporate network have a consistent addressing plan. In this case the private IP address assigned to the remote host will be unique on the virtual subnet.

For use in DHCPv4 configuration of IPsec tunnel mode, the client-identifier option MUST be unique within the virtual subnet and SHOULD be persistent across reboots. Possibilities include:

a. The htype/chaddr combination. If assigned as described above, this will be unique on the virtual subnet. It will be persistent across reboots for a LAN interface. If a non-LAN interface is used, it may not be persistent across reboots if the assigned IP address changes.

b. The machine FQDN concatenated with an interface number. Assuming that the machine FQDN does not conflict with that of another machine, this will be unique on the virtual

subnet as well as persistent across reboots.

c. The user NAI concatenated with an interface number. Assuming that the user is only connected to the VPN at one location, this will be unique on the subnet as well as persistent across reboots.

In order to deliver the DHCPDISCOVER packet from the intranet interface to the security gateway, an IKE Phase 1 SA is established between the Internet interface and the security gateway. A phase 2 (quick mode) DHCP SA tunnel mode SA is then established. The key lifetime for the DHCP SA SHOULD be on the order of minutes since it will only be temporary. The remote host SHOULD use an IDci payload of 0.0.0.0/UDP/port 68 in the quick mode exchange. The security gateway will use an IDcr payload of its own Internet address/UDP/port 67 The DHCP SA is established as a tunnel mode SA with filters set as follows:

From remote host to security gateway: Any to Any, destination: UDP port 67
From security gateway to remote host: Any to Any, destination: UDP port 68

Note that these filters will work not only for a client without configuration, but also with a client that has previously obtained a configuration lease, and is attempting to renew it. In the latter case, the DHCP SA will initially be used to send a DHCPREQUEST rather than a DHCPDISCOVER message. The initial DHCPv4 message (DHCPDISCOVER or DHCPREQUEST) is then tunneled to the security gateway using the tunnel mode SA. Note that since the DHCPDISCOVER packet has a broadcast address destination, the IPsec implementations on both the remote host and the security gateway must be capable of handling this.

4.2. DHCP Relay behavior

While other configurations are possible, typically the DHCPv4 server will not reside on the same machine as the security gateway, which will act as a DHCPv4 relay, inserting its address in the "giaddr" field. In this case, the security gateway relays packets between the client and the DHCPv4 server, but does not request or renew addresses on the client's behalf. While acting as a DHCP Relay, the security gateway MAY implement DHCP Relay load balancing as described in [19].

Since DHCP Relays are stateless, the security gateway SHOULD insert appropriate information in the DHCP message prior to forwarding to one or more DHCP servers. This enables the security gateway to route the corresponding DHCPOFFER message(s) back to the remote host on the correct IPsec tunnel, without having to keep state gleaned from the DISCOVER, such as a table of the xid, chaddr and tunnel.

If the security gateway maintains a separate subnet for each IPsec tunnel, then this can be accomplished by inserting the appropriate interface address in the giaddr field. Alternatively, the security gateway can utilize the DHCP Relay Agent Information Option [17]. In this case, the virtual port number of the tunnel is inserted in the Agent Circuit ID Sub-option (sub-option code 1).

To learn the internal IP address of the client in order to route packets to it, the security gateway will typically snoop the yiaddr field within the DHCPACK and plumb a corresponding route as part of DHCP Relay processing.

Where allocating a separate subnet for each tunnel is not feasible, and the DHCP server does not support the Relay Agent Information Option, stateless Relay Agent behavior will not be possible. In such cases, implementations MAY devise a mapping between the xid, chaddr, and tunnel in order to route the DHCP server response to the appropriate tunnel endpoint. Note that this is particularly undesirable in large VPN servers where the resulting state will be substantial.

4.3. DHCPREQUEST message processing

After the Internet interface has received the DHCPOFFER message, it forwards this to the intranet interface after IPsec processing. The intranet interface then responds by creating a DHCPREQUEST message, which is tunneled to security gateway using the DHCP SA.

4.4. DHCPACK message processing

The DHCPv4 server then replies with a DHCPACK or DHCPNAK message, which is forwarded down the DHCP SA by the security gateway. The remote host Internet interface then forwards the DHCPACK or DHCPNAK message to the intranet interface after IPsec processing.

After processing of the DHCPACK, the intranet interface is configured and the Internet interface can establish a new IPsec tunnel mode SA to the security gateway. The remote host may now delete the DHCP tunnel mode SA. All future DHCP messages sent by the client, including DHCPREQUEST, DHCPINFORM, DHCPDECLINE, and DHCPRELEASE messages will use the newly established VPN SA. Similarly, all DHCP messages subsequently sent by the DHCPv4 server will be forwarded by the security gateway (acting as a DHCP Relay) using the IPsec tunnel mode SA, including DHCPOFFER, DHCPACK, and DHCPNAK messages.

It SHOULD be possible to configure the remote host to forward all Internet-bound traffic through the tunnel. While this adds overhead to round-trips between the remote host and the Internet, it provides some added security in return for this, in that the corporate security

gateway may now filter traffic as it would if the remote host were physically located on the corporate network.

4.5. Configuration policy

Several mechanisms can be used to enable remote hosts to be assigned different configurations. For example, clients may use the User Class Option [16] to request various configuration profiles. The DHCPv4 server may also take a number of other variables into account, including the htype/chaddr; the host name option; the client-identifier option; the DHCP Relay Agent Information option [17]; the vendor-class-identifier option; the vendor-specific information option; or the subnet selection option [15].

Conditional configuration of clients, described in [18], can be used to solve a number of problems, including assignment of options based on the client operating system; assignment of groups of clients to address ranges subsequently used to determine quality of service; allocation of special address ranges for remote hosts; assignment of static routes to clients [20], etc. As noted in the security considerations, these mechanisms, while useful, do not enhance security since they can be evaded by a remote host choosing its own IP address.

5. Security Considerations

This protocol is secured using IPsec, and as a result the DHCP packets flowing between the remote host and the security gateway are authenticated and integrity protected.

However, since the security gateway acts as a DHCP Relay, no protection is afforded the DHCP packets in the portion of the path between the security gateway and the DHCP server, unless DHCP authentication is used.

Note that authenticated DHCP cannot be used as an access control mechanism. This is because a remote host can always set its own IP address and thus evade any security measures based on DHCP authentication.

As a result, the assigned address MUST NOT be depended upon for security. Instead, the security gateway can use other techniques such as instantiating packet filters or quick mode selectors on a per-tunnel basis.

As described in [17], a number of issues arise when forwarding DHCP client requests from untrusted sources. These include DHCP exhaustion attacks, and spoofing of the client identifier option or client MAC address. These issues can be partially addressed through use of the DHCP

Relay Information Option [17].

6. IANA Considerations

This draft requires that an htype value be allocated for use with IPsec tunnel mode, as described in section 4.1. Note that DHCP relies on the arp-parameters registry for definition of both the hrd parameter in ARP and the htype parameter in BOOTP/DHCP. As a result, an assignment in the arp-parameters registry is required, even though IPsec-DHCP will never use that parameter for ARP purposes, since conceptually BOOTP/DHCP and ARP share the arp-parameters registry.

This draft does not create any new number spaces for IANA administration.

7. 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.

8. References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[3] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[4] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[5] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[6] Droms, R., Arbaugh, W., "Authentication for DHCP Messages", Internet draft (work in progress), draft-ietf-dhc-authentication-16.txt, January 2001.

[7] Cobb, S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", RFC 1877, December 1995.

[8] Droms, R., Kinnear, K., Stapp, M., Volz, B., Gonczi, S., Rabil, G., Dooley, M., Kapur, A., "DHCP Failover Protocol", Internet draft (work in progress), draft-ietf-dhc-failover-08.txt, July 2000.

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

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

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

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

[13] Dukes, D., Pereira, R., "The ISAKMP Configuration Method", Internet draft (work in progress), draft-dukes-ike-mode-cfg-00.txt, October 2000.

[14] De Schrijver, P., T'Joens, Y., Hublet, C., "Dynamic host configuration : DHCP reconfigure extension", Internet draft (work in progress), draft-ietf-dhc-pv4-reconfigure-04.txt, April 2001.

[15] Waters, G., "The IPv4 Subnet Selection Option for DHCP", RFC 3011, November 2000.

[16] Stump, G., Droms, R., Gu, Y., Vyaghrapuri, R., Demirtjis, A., Beser, B., Privat, J., "The User Class Option for DHCP", RFC 3004, November 2000.

[17] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[18] Droms, R., and Lemon, T., The DHCP Handbook, Macmillan, Indianapolis, Indiana, 1999.

[19] Volz, B., Gonczi, S., Lemon, T., Stevens, R., "DHC Load Balancing Algorithm", RFC 3074, February 2001.

[20] Lemon, T., "The Classless Static Route Option for DHCP", Internet draft (work in progress), draft-ietf-dhc-csr-04.txt, February 2001.

[21] Kelly, S., Ramamoorthi, S., "Requirements for IPsec Remote Access Scenarios", Internet draft (work in progress), draft-ietf-ipsra-reqmts-03.txt, January 2001.

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

[23] Atkinson, R., "Key Exchange Delegation Record for the DNS", RFC 2230, November 1997.

[24] Gulbrandsen , A., . Vixie, P., Esibov, L. "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

9. Acknowledgments

This draft has been enriched by comments from John Richardson and Prakash Iyer of Intel, Gurdeep Pall and Peter Ford of Microsoft.

10. Authors' Addresses

Baiju V. Patel
Intel Corp, JF3-206
2511 NE 25th Ave
Hillsboro, OR 97124

Phone: +1 503 264-2422
EMail: baiju.v.patel@intel.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 936-6605
EMail: bernarda@microsoft.com

Scott Kelly
RedCreek Communications

3900 Newpark Mall Road
Newark, CA 94560

Phone: +1 510 745-3969
Email: skelly@redcreek.com

Vipul Gupta
Sun Microsystems, Inc.
901 San Antonio Rd.
Palo Alto, CA 94303

Phone: +1 650 786 3614
Fax: +1 650 786 6445
EMail: vipul.gupta@eng.sun.com

11. Appendix - IKECFG evaluation

Alternatives to DHCPv4, such as ISAKMP CFG, described in [13], do not meet the basic requirements described in [21], nor do they provide the additional capabilities of DHCPv4.

Basic configuration
: While ISAKMP CFG can provide for IP address assignment as well as configuration of a few additional parameters such as the DNS server and WINS server addresses, the rich configuration facilities of DHCPv4 are not supported. Past experience with similar configuration mechanisms within PPP IPCP [7] has taught us that it is not viable merely to support minimal configuration. Eventually, either much of the functionality embodied in the DHCPv4 options [5] is duplicated or support for DHCPINFORM [3] will be required.

Address management integration
: Since IKECFG is not integrated with existing IP address management facilities, it is difficult to integrate it with policy management services that may be dependent on the user to IP address binding.

Address pool management
: IKECFG does not provide a mechanism for the remote host to indicate a preference for a particular address pool. This makes it difficult to support address pool management.

Reconfiguration
: IKECFG does not support the concept of configuration leases or reconfiguration.

Fail-over support
: Since IKECFG creates a separate pool of address state, it complicates the provisioning of network utility-class reliability, both in the IP address management system and in the security gateways themselves.

Security and simplicity
: As past history with PPP IPCP demonstrates, once it is decided to provide non-integrated address management and configuration facilities within IKE, it will be difficult to limit the duplication of effort to address assignment. Instead, it will be tempting to also duplicate the configuration, authentication and fail-over facilities of DHCPv4. This duplication will greatly increase the scope of work, eventually compromising the security of IKE.

Authentication
: While IKECFG can support mutual authentication of the IPsec tunnel endpoints, it is difficult to integrate IKECFG with DHCPv4 authentication [6]. This is because the security gateway will not typically have access to the client credentials necessary to issue an DHCPv4 authentication option on the client's behalf.

As a result, security gateways implementing IKECFG typically request allocation of an IP address on their own behalf, and then assign this to the client via IKECFG. Since IKECFG does not support the concept of an address lease, the security gateway will need to do the renewal itself. This complicates the renewal process.

Since RFC 2131 [3] assumes that a DHCPREQUEST will not contain a filled in giaddr field when generated during RENEWING state, the DHCPACK will be sent directly to the client, which will not be expecting it. As a result, it is either necessary for the security gateway to add special code to avoid forwarding such packets, or to wait until REBINDING state. Since [3] does not specify that the giaddr field cannot be filled in when in the REBINDING state, the security gateway may put its own address in the giaddr field when in REBINDING state, thereby ensuring that it can receive the renewal response without treating it as a special case.

12. Full Copyright Statement

13. Expiration Date

This memo is filed as <draft-ietf-ipsec-dhcp-12.txt>, and expires November 1, 2001.