

IP Security Protocol Working Group (IPSEC)  
INTERNET-DRAFT  
[draft-ietf-ipsec-dhcp-over-ike-dhcpd-00.txt](#)  
Expires: 2 October 2003

T. Kivinen  
2 April 2003

## Using DHCP server/client backend for DHCP over IKE

### Status of This Memo

This document is a submission to the IETF IP Security Protocol (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list ([ipsec@lists.tislabs.com](mailto:ipsec@lists.tislabs.com)) or to the editor.

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/lid-abstracts.txt>

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

### Abstract

This document describes method of using dynamic host configuration protocol (DHCP) as a backend for the internet key exchange (IKE) version 2 host configuration protocol.

INTERNET-DRAFT

2 April 2003

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Using existing DHCP client . . . . .	<a href="#">2</a>
<a href="#">3.</a>	Using existing DHCP server . . . . .	<a href="#">2</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">7.</a>	Non-Normative References . . . . .	<a href="#">5</a>
<a href="#">8.</a>	Authors' Addresses . . . . .	<a href="#">5</a>

[1.](#) Introduction

The IKEv2 [[IKEV2](#)] offers way to put DHCP [[RFC2131](#)] packets inside the IKE packet exchange to do the host configuration for the remote access clients. This protocol describes how to use existing DHCP client and/or server with IKEv2 host configuration protocol.

[2.](#) Using existing DHCP client

The host configuration protocol in IKEv2 is defined so that it can be easily be used with currently existing DHCP client. All packets normally sent by the DHCP client are simply intercepted and put inside the DHCP payload. If this is during the initial IKE SA creation phase, the the DHCP payloads are sent inside the IKE\_AUTH packets. If the DHCP packet is intercepted when the IKE SA is already ready, then the DHCP payloads are sent as informational exchange. Informational exchanges MUST NOT be used before the IKE SA creation is finished.

The reason for the interception and sending DHCP packets inside IKE is that the IPsec SAs created between the client and security gateway might not allow DHCP traffic, and also because replies to the DHCP packets might come as broadcast in some cases (DHCPNAK), and to get those working we MUST use DHCP relay processing in the security gateway end. Also the actual configuration backend on the other end might not be DHCP server, but for example RADIUS [[RFC2865](#)] server.

Note, that the reply to the information exchange having DHCP payload, might not contain the reply to the actual DHCP request, i.e it might be empty, and the reply might be sent as separate informational exchange initiated by the security gateway when the reply packet is available or during the next reply to IKE\_AUTH if the IKE SA is not yet ready.

### 3. Using existing DHCP server

If the security gateway wants to use existing DHCP server(s) it MUST act as a DHCP relay. When it receives DHCP payload from the client it MUST set the giaddr field to contain one of its own IP addresses, and it SHOULD add DHCP Relay Agent Information Option [[RFC3046](#)] (DHCP option code 82) as last DHCP option just before end option. The Agent Circuit ID Sub-option (sub-option code 1) is filled with the security gateways

I. Kivinen

[page 2]

---

INTERNET-DRAFT

2 April 2003

IKE SPI value.

In some cases the security gateway might put this DHCP relay to its own IP alias and use that address in the giaddr field. This is especially useful if the security gateway already has DHCP server or DHCP relay running.

Where 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 IKE SA in order to route the DHCP server response to the appropriate IKE SA. Note that this is particularly undesirable in large VPN servers where the resulting state will be substantial.

After sending the request out (either to the configured DHCP server(s) or to broadcast address), the security gateway should wait for configurable time (default should be few seconds) and collect replies received during that. The security gateway might reply immediately when the first reply is received, or it might wait for the full time and send all packets received during that time. It normally is not useful to wait for multiple DHCPACK packets, as there should only be exactly one of those. On the other hand when waiting for the DHCPOFFER packets in environment where there are multiple DHCP servers available (load balancing, high availability cases etc) it might be better to wait for more than one DHCPOFFER packet.

When the security gateway gets DHCP replies back from the network it should use the DHCP Relay Agent Information to associate the reply to

specific IKE SA. The security gateway MUST remove the DHCP Relay Agent Information Option and set the giaddr to 0 before encoding the DHCP packet inside the IKE DHCP payload.

If during the IKE SA creation phase the security gateway receives DHCP replies during the time it does not have request to be replied (i.e it has replied to last IKE request from the client, and the client has not yet sent a next request), it MUST keep at least the last DHCP reply it has received, and send it to the client when possible (i.e when the client makes next IKE request). Security gateway cannot during the IKE SA creation phase initiate exchanges to the client itself, it must wait for the client to drive the exchange.

After the IKE SA is created then the security gateway can send replies back to the client as separate informational exchanges.

When security gateway sees DHCPACK it must get the yiaddr from the payload and configure that to be the clients IP address. This clients IP address is used during the IKE\_AUTH exchange to narrowing the TS<sub>i</sub> selector down to only include clients IP address. Security gateway MUST also make sure that if the same client IP address is given out to two different entities (== clients IKE SA authenticated IKE identity are different) the older one of those IPsec SAs is deleted.

I.e if DHCPACK is received to address which is already associated with

some other entity, then the old entities IPsec SAs are deleted.

The DHCP server should be sending the reply packets to the Relay address, i.e to the security gateway, but in some cases the DHCP server might also try to send the packet directly to the client's IP address (DHCP renewing state, or replies to DHCPINFORMs). The security gateway SHOULD try to intercept all DHCP packets going directly to clients IP address and encapsulate them inside the DHCP payload in the IKE SA. This is never needed for the IKE\_AUTH state as the DHCP server will not try to send packets directly to the client (the client is either in DHCP init or DHCP init-reboot state, it cannot be in DHCP renewing state).

The reason for the interception is to make sure the DHCP requests gets back to the client even if the IPsec SA created between client and security gateway does not allow DHCP traffic in it, or the client might not be actually using DHCP client to do the configuration. As any of those packets going directly to the client cannot have effect to the security gateway operations, there is no mandatory requirement for the

security gateway to intercept those packets.

Only packet that could affect the security gateway operations are the DHCPACKs which have different IP address than given in previous case, and those packets cannot be sent to the client directly.

If client never gets DHCPACK back (which might be sent by the DHCP server directly to the client) when in DHCP renewing state, it moves to DHCP rebinding state, which uses broadcasts, and the client will get packets through.

The client MUST NOT use DHCPINFORM packets, but use normal DHCP address allocation instead. The security gateway does need to support DHCPINFORM processing.

#### [4.](#) Security Considerations

If real DHCP server is used, then the DHCP protocol between security gateway and the DHCP server might be vulnerable to different kind of attacks. If the DHCP server is inside the security gateway itself then such attacks are not possible.

#### [5.](#) IANA Considerations

This document does not have any actions for IANA.

#### [6.](#) Normative References

[IKEV2]

Kaufman C., "Internet Key Exchange (IKEv2) Protocol", [draft-ietf-ipsec-ikev2-05.txt](#), February 2003

[RFC3046]

Patrick M., "DHCP Relay Agent Information Option", January 2001

[I.](#) Kivinen

[page 4]

---

INTERNET-DRAFT

2 April 2003

[RFC2131]

Droms R., "Dynamic Host Configuration Protocol", March 1997

#### [7.](#) Non-Normative References

[RFC2865]

Rigney, C., S. Willens, A. Rubens, and Simpson W., "Remote Authentication Dial In User Service (RADIUS)", June 2000.

[RFC1533]

Alexander S., and Droms R., "DHCP Options and BOOTP Vendor Extensions", October 1993.

## 8. Authors' Addresses

Tero Kivinen  
SSH Communications Security Corp  
Fredrikinkatu 42  
FIN-00100 HELSINKI  
Finland  
E-mail: [kivinen@ssh.fi](mailto:kivinen@ssh.fi)

SSH Communications Security  
SSH IPSEC Toolkit

<http://www.ssh.fi/>  
<http://www.ssh.fi/ipsec/>