A method for configuration of IPsec clients using DHCP
draft-richardson-ipsec-dhcp-over-ike-00.txt

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 August 17, 2003.

Copyright Notice

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

1. Introduction ................................................. 4
2. Time sequence diagram .................................... 5
3. Comparisons with mode-cfg ................................. 6
4. Comparisons with DHCP-over-IPsec .......................... 7
   References ................................................. 8
   Author’s Address .......................................... 8
   Full Copyright Statement ................................. 9
Abstract

IPsec technology is frequently used for remote access scenarios. A tunnel is established from a mobile node (such as a laptop) and an IPsec gateway located at the Enterprise. The mobile node’s tunnel outer address is potentially any IP address on the Internet. The mobile node’s tunnel inner address should be an address from within the enterprise. The assignment of this address should ideally be done dynamically.

This document specifies a configuration mode called "DHCP over IKE". The document specifies that the payload of a DHCP exchange should be carried over an IKE phase 1 exchange.
1. Introduction

Intro about problem space for configuring clients with addresses. We use [1] to with [2].
2. Time sequence diagram

The setup consists of:

```
+--------+                 +---------+         +--------+
| client |=================| Security|---------|  DHCP  |
+--------+                 | gateway |         | server |
```

HDR, SAi1, KEi, Ni -->
<-- HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, DHCP(disc)}) -->

---DHCP Discovery->
<--DHCP Offer------

<-- HDR, SK {IDr, [CERT,] AUTH, DHCP(offer))

HDR, SK{SAi2, TSi, TSr, DHCP(request)}-->

---DHCP request-->
<--DHCP ACK------

<-- HDR, SK {SAr2, TSi, TSr, DHCP(ack)}

later, upon rekey, one does:

HDR, SK {SAi2, TSi, TSr, DHCP(request)}-->

---DHCP request-->
<--DHCP ACK------

<-- HDR, SK {SAr2, TSi, TSr, DHCP(ack)}
3. Comparisons with mode-cfg

From the point of view of the IKE implementor, this proposal is very similar to mode configuration. There are two major differences: inclusion of a DHCP client state machine into the client IKE, and the IKEv2 gateway must encapsulate the DHCP payloads into a UDP packet and relay them to a DHCP server. The gateway SHOULD also append DHCP relay options to the end to signal to the DHCP server that it came via IKEv2.

The major advantage of DHCP-over-IKE vs mode-cfg is that it leverages all of the DHCP protocol infrastructure for configuration of the end host. Further, it naturally interacts with the DHCP infrastructure at the enterprise end.
4. Comparisons with DHCP-over-IPsec

The DHCP-over-IKE situation appears more complicated due to the inclusion of the DHCP state machines into IKEv2. The major complexity appears to be on the client. Note that this is an illusion - in the DHCP-over-IPsec, the IKE on the client needs to know what state the DHCP client it is so that it may act accordingly. As such, the states are simply represented twice. Unless the implementor is able to take advantage of an existing DHCP client present on the OS, there is little savings in actual code.

DHCP-over-IPsec requires that a very strange IPsec SA be configured for: 0.0.0.0:udp/67 <->0.0.0.0:udp/68. Note that extreme care must be taken to make sure that this does not also catch packets destined to the DHCP server on the physical wire. This SA MUST be torn down before any traffic is mis-directed on it. Further, it is very difficult to configure a mobile system that must maintain tunnels to two enterprises.
References


Author’s Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

EMail: mcr@sandelman.ottawa.on.ca
URI: http://www.sandelman.ottawa.on.ca/
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 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.

Acknowledgement

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