IP Security Protocol Working Group (IPSEC)   T. Kivinen
INTERNET-DRAFT   2 April 2003
draft-ietf-ipsec-dhcp-over-ike-radius-00.txt
Expires: 2 October 2003

Using RADIUS backend for DHCP over IKE

Status of This Memo

Abstract

This document describes method of using Remote Authentication Dial In User Service (RADIUS) as a backend for the internet key exchange (IKE) version 2 host configuration protocol.

Table of Contents

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 RADIUS [RFC2865] server to get the configuration data needed for the IKEv2 host configuration protocol.

2. Using RADIUS backend

The security gateway using the RADIUS as backend for the configuration, is acting as a protocol converted between DHCP and RADIUS. This can also be seen as if there is minimalistic DHCP server in the security gateway, and that DHCP server is then using the RADIUS server to get the actual IP address. This DCHP server is then also responsible to remembering the configuration given to client, in case client decides to request it again later (i.e when client does RENEW or REBIND).

If the client sent DHCP(DISCOVER) to the security gateway, then the security gateway MUST send the DHCP(OFFER) back with the configuration parameters found from the RADIUS attributes. The client will then reply to that with DHCP(REQUEST). The security gateway MUST then check that the paremeters are valid compared to the configuration parameters received earlier from the RADIUS and if so sent back DHCP(ACK). Note that security gateway MUST NOT leave out the DHCP(OFFER) packet, i.e it MUST NOT reply to DHCP(DISCOVER) with DHCP(ACK) even when there would not be anything for the client to do with DHCP(OFFER). This would be against the DHCP protocol.

The client may also start directly with DHCP(REQUEST), in which case security security gateway simply verifies that the parameters are valid (if there are no parameters inside then they are valid, and server can reply back immediately with full set of parameters) and replies with DHCP(ACK) with final configuration parameters. If the DHCP(REQUEST) parameters are not valid, the security gateway MUST reply with DHCP(NAK) which will cause the client to start again with DHCP(DISCOVER) payload.

3. Mapping of DHCP options to RADIUS request attributes

The mapping of the DHCP options in the DHCPDISCOVER or DHCPREQUST payload to the RADIUS attributes is following:

DHCP option	RADIUS attribute
Requested IP address (50)	Framed-IP-Address (8)
Subnet Mask (1)	Framed-IP-Netmask (9)
Domain Name Server (6)	VendorID [ID#], VSA [#]
Hostname (12)	VendorID [ID#], VSA [#]
NetBIOS Name Servers (44)	VendorID [ID#], VSA [#]
IP Address Lease Time (51)	Session-Timeout (27) or VendorID [ID#], VSA [#]

The RADIUS server may also support other DHCP options by using vendor specific attributes.

4. Mapping of RADIUS attributes to DHCP options

The mapping of the RADIUS attributes to DHCP options in the DHCPOFFER or DHCPACK payload is following:

RADIUS attribute	DHCP field
Framed-IP-Address (8)	yiaddr
Framed-IP-Netmask (9)	Subnet Mask Option (1)
VendorID [ID#], VSA [#]	Domain Name Server Option (6)
VendorID [ID#], VSA [#]	Hostname Option (12)
VendorID [ID#], VSA [#]	NetBIOS Name Servers Option (44)
Session-Timeout (27) or VendorID [ID#], VSA [#]	IP Address Lease Time (51)

The RADIUS server may also support other DHCP options by using vendor specific attributes.

The actual values for the Vendor ID and VSA (vendor specific attribute) depends on the RADIUS server vendor.

5. Security Considerations

The connection between security gateway and RADIUS server migth be vulnerable to different kind of attacks, and that connection should be protected using IPsec or some other means.

6. IANA Considerations

This document does not have any actions for IANA.

7. Normative References

[IKEV2]

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

[RFC2131]
Droms R., "Dynamic Host Configuration Protocol", March 1997

[RFC2865]
Rigney, C., S. Willens, A. Rubens, and Simpson W., "Remote Authentication Dial In User Service (RADIUS)", June 2000.

8. Non-Normative References

9. Authors' Addresses

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

--
kivinen@ssh.fi
SSH Communications Security   http://www.ssh.fi/
SSH IPSEC Toolkit   http://www.ssh.fi/ipsec/