Network Working Group
Expires May 20th, 1997
Internet Draft

J. O'Hara
New Oak Communications
November 20, 1997

Configuration of Tunnel Mode Ipsec Endpoint Parameters

<draft-ohara-ipsecparam-00.txt>

Status of this Memo

Abstract

This document describes the assignment of configuration parameters to IPsec tunnel mode client endpoints. Single user computers that are connecting into corporations via Internet Service Providers, ISP's, using Tunnel mode IPsec may need to have configuration information supplied to them, such as inner ip address, DNS server addresses, WINS server addresses, etc.

This document describes a method utilized by New Oak Communications to pass these parameters between it's Extranet Access Switch and it's IPsec client software.

TABLE OF CONTENTS

1. Introduction

Traditional use of Tunnel Mode IPsec has been focused at firewall to firewall connections with state configured at each end. This is well suited for branch office routing, but is less appropriate for internet remote access, where a single user system, such as a home computer or laptop is connected to an Internet Service Provider's Point of Presence, POP. In this model the end system will have it's IP configuration initially configured through IPCP in the dial up case or via DHCP in the case of a cable modem or ADSL. It is desirable for the IPsec tunnel parameters and policy to be downloaded to the end user's system in similar, but secure manner.

Tunnel mode IPsec is well suited to allow traveling or home users the opportunity to tunnel directly from their systems into corporate sites. In doing so the user would first connect to a ISP's POP. Then the user would initiate a connection with a access server on the edge of their network that would serve as the other end of the IPsec tunnel.

Establishment of a secure tunnel hides the corporation's network topology and allows the end users system to operate just as if it were an internal system. The end users system will need to be assigned a new end node address for use inside the IPsec tunnel and other addresses such as those of DNS and WINS servers. In this draft the terms "end node" read as a home or traveling user's PC, and "access server" as the device that exists between the corporate Intranet and the Internet terminates IPsec tunnel connections.

This document assumes that the reader is familiar with the related documents "The resolution of ISAKMP with Oakley" [Hark97], and "Dynamic Host Configuration Protocol, RFC 2131" [Drom97], that provide important background for this specification.

In this document, the key words "MAY", "MUST", "recommended", "required", and "SHOULD", are to be interpreted as described in [RFC-2119].

2. IP ADDRESS ASSIGNMENT

Assignment of a Inner IP address is accomplished by using the access server supplied Proxy ID responder, IDur, supplied by the initiator (server) as part of the Quick Mode exchange undertaken in ISAKMP phase 2. To utilize the proxy ID's in this way requires that the phase 2 initiator is the server and that the responder (the end node) accepts that address as it's inner, or tunneled address.

ISAKMP usage [Hark97] and [Pip97] describe the 2 stage process for establishment of a Security Association, SA. Phase 1 establishes a secure connection for SA negotiation. During Phase 2 this negotiation is accomplished within the authenticated and protected channel constructed in phase 1. Phase 2 is characterized by 1 or more Quick mode exchanges.

When the end node initiates the IPsec tunnel it will be the Phase 1 initiator. During Phase 2 the access server MUST be the initiator, as shown below.

Quick Mode is defined as follows from [Hark97]:

```
 Initiator (server)                Responder (end node)
--------------------              ----------------------
HDR*, HASH(1), SA, Ni
  [, KE ] [, IDui, IDur ] -->
                          <--    HDR*, HASH(2), SA, Nr
                                      [, KE ] [, IDui, IDur ]
HDR*, HASH(3)              -->
```

Where the contents of IDui are specified as follows:

Identification Type for IDui and IDur will be: ID_IPV4_ADDR   1

The ID_IPV4_ADDR type specifies a single four (4) octet IPv4 address.

Summary:

By reversing the Phase 1 and Phase 2 initiator roles and using the supplied IDur as the tunneled source address the problem of how to supply a remote user a tunneled, inner address can be resolved. This reversal of roles is within the scope of the draft [Hark97] and provides secure assigment method protected by the ISAKMP SA.

3. DNS and WINS ADDRESS ASSIGNMENT

When the end node has received its tunnelled address and the IPsec tunnel has been established, the end node may require the addresses for DNS and WINS servers inside the corporate network. To obtain these addresses, the end node uses the Dynamic Host Configuration Protocol (DHCP) [Drom97] as follows:

The end node sends a tunnelled unicast DHCPINFORM message under the protection of the just-established IPsec SA. The source address inside the tunnel is the IPv4 address received from the server in IDur (as described in section 2), while the destination address is the server's IPv4 address on the corporate network, as provided in IDui. The "ciaddr" field in the DHCPINFORM message MUST be the same as the end node's source address inside the tunnel. If the end node requires DNS server configuration, the end node SHOULD provide DHCP option 55 (Parameter Request List) as specified in RFC 2132, and include DHCP option 6 (Domain Name Server option) in the list. If the end node requires WINS server configuration, it SHOULD provide a parameter request list that includes DHCP option **44 (NetBIOS over TCP/IP Server option).**

The server responds by sending a tunnelled unicast DHCPACK message to the end node's tunnelled address. The DHCPACK MAY include one or more DNS servers, provided by DHCP option 6, and MAY include one or more WINS servers, provided by DHCP option 44.

4. Security Considerations

Protection of corporate network topology is of concern and it should be observed that tunnel addresses assigned with this method are transmitted under the protection of the ISAKMP SA, while the DNS and WINS server addresses are protected by the IPsec SAs. Thus, the information is no more (and no less) secure than the SAs themselves.

5. References

[Alex97] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997

[Bra97] Bradner, S., "Key Words for use in RFCs to indicate Requirement Levels", RFC2119, March 1997.

[Drom97] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, Bucknell University, March 1997.

[Hark97] Harkins, D., Carrel, D., "The resolution of ISAKMP with Oakley", draft-ietf-ipsec-isakmp-oakley-04.txt.

[MSST96] Maughhan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", version 8, draft-ietf-ipsec-isakmp-08.{ps,txt}.

[Orm96] Orman, H., "The Oakley Key Determination Protocol", version 1, TR97-92, Department of Computer Science Technical Report, University of Arizona.

[Pip97] Piper, D., "The Internet IP Security Domain Of Interpretation for ISAKMP", version 5, draft-ietf-ipsec-ipsec-doi-05.txt.

6. Author's Address

John O'Hara
New Oak Communications, Inc.
125 Nagog Park
Acton, Massachusetts, 01720

johara@newoak.com

(978) 266 1011 voice