PANA Working Group
Internet Draft
Document: draft-ietf-pana-ipsec-01.txt
Expires: June 2004

M. Parthasarathy
Nokia

January 2004

PANA enabling IPsec based Access Control

Status of this Memo

Copyright Notice

Abstract

The PANA (Protocol for carrying Authentication for Network Access) working group is developing protocol for authenticating clients to the access network using IP based protocols. The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client and PANA authentication agent at the end of a successful authentication. This document discusses the details for establishing an IPsec security association using the PANA security association for enabling IPsec based access control.

Table of Contents

1.0 Introduction

The PANA (Protocol for carrying Authentication for Network Access) working group is developing protocol for authenticating clients to the access network using IP based protocols. The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client and PANA authentication agent at the end of successful authentication. The PANA authentication agent (PAA) indicates the results of the authentication using the PANA-Bind-Request message wherein it can indicate the access control method enforced by the access network. The PANA protocol [PANA-PROT] does not discuss any details of IPsec [IPSEC] SA establishment, when IPsec is used for access control. This document discusses the details of establishing an IPsec security association between PANA client and the enforcement point. When the IPsec SA is successfully established, it can be used for access control and specifically used to prevent the service theft mentioned in [PANA-THREATS].

Please refer to [PANAREQ] for terminology and definitions of terms used in this document. The following picture illustrates what is being protected with IPsec. As shown in Figure 1, PANA Authentication Agent (PAA), Enforcement Point (EP) and the Access Router (AR) are co-located. The IPsec security association protects the traffic between PaC and EP. In IPsec terms, EP is a security gateway (therefore a router) and forwards packets coming from the PaC to other nodes.

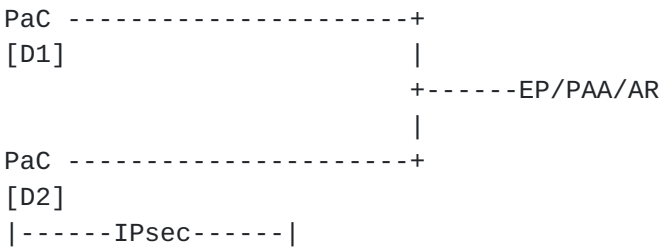

Figure 1

First, this document discusses some of the pre-requisites for IPsec SA establishment. Next, it gives details on what should be communicated between PAA and EP. Then, it gives the details of IKE/IPsec exchange with packet formats and SPD entries. Finally, it discusses the issues when IPsec is used for remote access together with local access.

2.0 Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

3.0 Pre-requisites for IPsec SA establisment

This document assumes that the following have already happened before the IPSEC SA is established.

1) PANA client (PaC) and PAA mutually authenticate each other using EAP methods that derive Master Session Key (MSK).

2) PaC learns the IP address of the Enforcement point (EP) during the PANA exchange.

3) PaC learns that the network uses IPsec [IPSEC] for securing the link between PaC and EP during the PANA exchange.

4) PaC configures a link-local address before the PANA protocol begins. At the end of authentication, it either acquires a globally reachable address using [DHCP][DHCPV6] or using IKE or auto-configures an address using stateless auto-configuration [IPV6-ND] if IPv6 is being used.

In the case of DHCP and IKE, EP can trivially learn the address allocated to the client. In the case of auto-configuration (which includes global address or addresses configured as in [PRIV]), EP may not know the address assigned to the PaC. Thus, it may not be able to setup the SPD entries appropriately before IKE exchange starts. As most of the IKE implementations assume that the SPD can be consulted during the SA negotiation, it may require slightly a different behavior from IKE in the auto-configuration case. In the case of auto-configuration, IKE should be able to setup the SAs for the traffic selectors specified by the PaC without consulting the SPD entry. If there is already an SA for the same address, then the SA request MUST be rejected with INVALID-ID-INFORMATION [IKE]. If PaC authenticates itself successfully, EP should add the SPD entry for protecting the subsequent data packets.

4.0 IKE Pre-shared key derivation

If the network chooses IPsec to secure the link between PaC and EP, PAA should communicate the IKE pre-shared key, the IP address of the PaC and the PANA session ID to EP before the IKE exchange begins. As EP and PAA are assumed to be co-located,this might be just an API call.

The IKE exchange between PaC and PAA is equivalent to the 4-way handshake in [IEEE80211i] following the EAP exchange. The IKE exchange establishes the IPsec SA similar to the pair-wise transient keys (PTK) established in [IEEE80211i]. The IKE exchange provides both key confirmation and protected cipher-suite negotiation.

IKE pre-shared key is derived as follows.

```
IKE Pre-shared Key = HMAC-SHA-1 (MSK, "IKE-preshared key" |
                        Session ID | MSK-ID)
```

The values have the following meaning:

MSK: The Master Session Key (MSK) is provided by the EAP method as part of the PANA/EAP protocol execution. Please refer to [EAP-KEY] for details.

Session ID: The value as defined in the PANA protocol [PANA-PROT], identifies a particular session of a client.

MSK-ID: This identifies the MSK within a given session. During the lifetime of the PANA session, there could be multiple EAP re-authentications. As EAP re-authentication changes the MSK, MSK-ID is used to identify the right MSK. This AVP is yet to be defined in [PANA-PROT].

The character "|" denotes concatenation as defined in [IKE].

During EAP re-authentication, the MSK changes. Whenever the MSK changes, a new value of MSK-ID is established between the PaC and PAA/EP. If there is already an IKE SA established, it can continue to be used till it expires. A change in the value of MSK need not result in re-negotiating a new IKE SA or IPsec SA immediately. But any new negotiation of IKE SA should use the new pre-shared key derived from the latest MSK and is indicated by the MSK-ID in the above equation.

5.0 IKE and IPsec details

IKE [IKE] MUST be used for establishing the IPsec SA. The details specified in this document would work with IKEv2 [IKEV2] also. Any difference between them would be explicitly noted. PANA authenticates the client and derives the keys to protect the traffic. Hence, manual keying cannot be used. Aggressive mode with pre-shared key MUST be supported. PaC and EP SHOULD use its PANA session ID [PANA-PROT] as the payload of ID_KEY_ID in aggressive mode for establishing the phase I SA. IP addresses cannot be used as identifier as the PaC may be re-authenticated multiple times and hence may not uniquely identify the pre-shared key. For the same reason, main mode of IKE cannot be used as it requires addresses to be used as identifiers.

After Phase I SA is established, quick mode exchange is performed to establish an ESP tunnel mode IPsec SA for protecting the traffic between PaC and EP. The identities used during Phase II are explained below. The next few sections discuses the packet formats and SPD entries.

6.0 Packet Formats

Following acronyms are used throughout this document.

PaC's link-local address is denoted by PAC-LINK-LOCAL.

PaC's global address (which could be either auto-configured or assigned using [DHCP][DHCPv6][IKE][IKEv2] or addresses specified in [PRIV] if IPv6 is being used) is denoted by PAC-GLOBAL-ADDR.

EP's link-local address is denoted by EP-LINK-LOCAL.

The node with which the PaC is communicating is denoted by END-ADDR.

The link-local address is used as the outer header of the tunneled packet as mentioned below.

Following is the packet format on the wire for packets sent from PaC to EP:

```
IPv4/IPv6 header (source = PAC-LINK-LOCAL,
                  destination = EP-LINK-LOCAL)
ESP header
IPv4/IPv6 header (source = PAC-GLOBAL-ADDR,
                  destination = END-ADDR)
```

Following is the packet format on the wire for packets sent from EP to PaC:

```
IPv4/IPv6 header (source = EP-LINK-LOCAL,
                  destination = PAC-LINK-LOCAL)
ESP header
IPv4/IPv6 header (source = END-ADDR,
                  destination = PAC-GLOBAL-ADDR)
```

7.0 IPsec SPD entries

The SPD entries for IPv4 and IPv6 are specified separately as they are different.

7.1 IPv4 SPD entries

```
PaC's SPD OUT:
          IF source = PAC-GLOBAL-ADDR & destination = any
           THEN USE ESP TUNNEL MODE SA:
           outer source = PAC-LINK-LOCAL
           outer destination = EP-LINK-LOCAL

PaC's SPD IN:
         IF source = any & destination = PAC-GLOBAL-ADDR
          THEN USE ESP TUNNEL MODE SA:
          outer source = EP-LINK-LOCAL
          outer destination = PAC-LINK-LOCAL

EP's SPD OUT:
         IF source = any & destination = PAC-GLOBAL-ADDR
          THEN USE ESP TUNEL MODE SA:
          outer source = EP-LINK-LOCAL
          outer destination = PAC-LINK-LOCAL

EP's SPD IN:
         IF source = PAC-GLOBAL-ADDR & destination = any
          THEN USE ESP TUNNEL MODE SA:
           outer source = PAC-LINK-LOCAL
```

```
            outer destination = EP-LINK-LOCAL
```

During the IPsec SA setup, PaC uses PAC-GLOBAL-ADDR as its phase 2 identity (IDci) and EP uses ID_IPV4_ADDR_RANGE or ID_IPV4_ADDR_SUBNET as its phase 2 identity. The starting address is zero IP address and the end address is all ones for ID_IPV4_ADDR_RANGE. The starting address is zero IP address and the end address is all zeroes for ID_IPV4_ADDR_SUBNET.

7.2 IPv6 SPD entries

The IPv6 SPD entries are slightly different from IPv4 to prevent the neighbor and router discovery [IPV6-ND] packets from being protected with IPsec. The first three entries of the following SPD tables bypass IPsec protection for neighbor and router discovery packets. The latest version of the IPsec [IPSEC-BIS] document allows traffic selectors to be based on ICMPv6 type and code values. In that case, the first three entries can be based on ICMPv6 type and code values.

All traffic destined to global address is always sent to the default router (EP) i.e, the global prefix is not considered to be on-link. This can be achieved by turning off the "L" bit in the router advertisement.

Pac's SPD OUT:

```
          IF source = ::/128  & destination = any
           THEN BYPASS

          IF source = fe80::/10 & destination = any
          THEN BYPASS

          IF source = any & destination = fe80::/10
           THEN BYPASS

          IF source = PAC-GLOBAL-ADDR & destination = any
           THEN USE ESP TUNNEL MODE SA:
              outer source = PAC-LINK-LOCAL
              outer destination = EP-LINK-LOCAL
```

PaC's SPD IN:

```
          IF source = ::/128 & destination = any
           THEN BYPASS

          IF source = fe80::/10 & destination = any
          THEN BYPASS

          IF source = any & destination = fe80::/10
```

```
            THEN BYPASS

           IF source = any & destination = PAC-GLOBAL-ADDR
               THEN USE ESP TUNNEL MODE SA:
                  outer source = EP-LINK-LOCAL
                  outer destination = PAC-LINK-LOCAL
```

EP's SPD OUT:

```
           IF source = ::/128 & destination = any
            THEN BYPASS

           IF source = fe80::/10 & destination = any
           THEN BYPASS

           IF source = any & destination = fe80::/10
            THEN BYPASS

           IF source = any & destination = PAC-GLOBAL-ADDR
               THEN USE ESP TUNNEL MODE SA:
                  outer source = EP-LINK-LOCAL
                  outer destination = PAC-LINK-LOCAL
```

EP's SPD IN:

```
           IF source = ::/128 & destination = any
            THEN BYPASS

           IF source = fe80::/10 & destination = any
           THEN BYPASS

           IF source = any & destination = fe80::/10
            THEN BYPASS

           IF source = PAC-GLOBAL-ADDR & destination = any
            THEN USE ESP TUNNEL MODE SA:
               outer source = PAC-LINK-LOCAL
               outer destination = EP-LINK-LOCAL
```

During the IPsec SA setup, PaC uses PAC-GLOBAL-ADDR as its phase 2 identity (IDci) and EP uses ID_IPV6_ADDR_RANGE or ID_IPV6_ADDR_SUBNET as its phase 2 identity. The starting address is zero IP address and the end address is all ones for ID_IPV6_ADDR_RANGE. The starting address is zero IP address and the end address is all zeroes for ID_IPV6_ADDR_SUBNET.

8.0 Double IPsec

If the PaC uses IPsec for secure remote access e.g., Corporate VPN access, there will be separate SPD entries protecting the traffic to/from remote network. In this case, IPsec may need to be applied twice, once for protecting the remote access and once for protecting the local access. This is the same as the iterative tunneling discussed in [IPSEC].

When the IPsec SA is established with the remote security gateway, the IKE packets from the PaC to the remote security gateway may or may not need IPsec protection on the local link depending on the configuration at the EP. If EP requires IPsec protection for all packets, then the PaC should configure SPD entries appropriately so that IKE packets destined to EP are bypassed whereas IKE packets to the remote SG are protected. If EP does not require IPsec protection for IKE packets destined to remote security gateway, it needs to configure SPD entries that would bypass them.

9.0 Security considerations

This document discusses the use of IPsec for access control when PANA is used for authenticating the clients to the access network.

If the PAA does not verify whether PaC is authorized to use an IP address, it is possible for the PaC to steal the traffic destined to some other PaC. The use of IPsec does not prevent this attack. PAA may use other mechanisms to prevent this attack.

When IPv6 is used, the SPD entries bypass all link-local traffic without applying IPsec. This should not be a limitation as the link-local address is used only by link-local services e.g. neighbor/router discovery, which uses a different mechanism to protect their traffic. Moreover, this limitation may not be there in the future if IPsec extends the SPD selectors to specify ICMP types.

10.0 Normative References

Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[IPSEC] S. Kent et al., "Security Architecture for the Internet Protocol", RFC 2401, November 1998

11.0 Informative References

[PANAREQ] A. Yegin et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", draft-ietf-pana-requirements-04.txt

[PANA-PROT] D.Fosberg et al., "Protocol for Carrying Authentication for Network Access", draft-ietf-pana-01.txt

[PANA-THREATS] M.Parthasarathy, "PANA Threat analysis and security requirements", draft-ietf-pana-threats-eval-04.txt

[KEYWORDS] S. Bradner, "Key words for use in RFCS to indicate requirement levels", RFC 2119, March 1997

[IKE] D. Harkins et al., "Internet Key Exchange", RFC 2409, November 1998

[IKEV2] Charlie Kauffman et al., "Internet Key Exchange(IKEv2) Protocol", draft-ietf-ipsec-ikev2-11.txt

[IPSEC-BIS] S.Kent, "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-00.txt

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

[DHCPV6] R. Droms et. al, "Dynamic Host Configuration Protocol for IPv6", RFC 3315, July 2003

[IPV6-ND] T. Narten et al., "Neighbor Discovery for IP version 6 (IPv6) ", RFC 2461, December 1998

[PRIV] T. Narten et al., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001

[EAP-KEY] D.Simon et al., "EAP Key Management Framework", draft-aboba-ppext-key-problem-07.txt

[IEEE80211i] IEEE Draft 802.11I/D5.0, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange between Systems LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer specifications: Specification for Enhanced Security", August 2003.

12.0 Acknowledgments

The author would like to thank Francis Dupont, Pasi Eronen, Yoshihiro Ohba, Jari Arkko, Hannes Tschofenig and other PANA WG members for their valuable comments and discussions.

13.0 Revision log

Changes between revision 00 and 01

-Specified the use of ESP tunnel mode SA instead of IP-IP transport mode SA after working group discussion.
-Specified the IKE pre-shared key derivation.

14.0 Author's Addresses

Mohan Parthasarathy
313 Fairchild Drive
Mountain View CA-94043

Phone: 408-734-8820
Email: mohanp@sbcglobal.net

15.0 Full Copyright Statement

Acknowledgement

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