PANA Working Group
Internet Draft
Document: draft-ietf-pana-ipsec-00.txt
Expires: March 2004

<M. Parthasarathy>

October 2003

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. In Figure 1, it is assumed that PAA and EP are co-located. It is also possible that they are not 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.

```
PaC ---------------EP/PAA-+
[D1]                      |
                          +- ----- AR
                          |
PaC ---------------EP/PAA-+
[D2]
|------IPsec------|

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

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

3) PaC has already acquired an IP address and EP knows about the IP address of the PaC, before the IKE exchange starts. If IPv6 is being used, the EP needs to know both the global address and the link-local address of the PaC.

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. This might be just an API call, if PAA and EP are co-located. It is

assumed that the communication between PAA and EP is already secured [PANA-REQ].

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)
```

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: This value is a 128-bit value as defined in the PANA protocol [PANA-PROT], which identifies a particular session of a client.

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

5.0 IKE and IPsec details

IKE [IKE] MUST be used for establishing the IPsec SA. Manual keying may not be possible, as the network does not know all the PaCs that will be authenticating to the network, a priori. Main mode with pre-shared key SHOULD be supported. Aggressive mode with pre-shared key MUST be supported. PaC and EP SHOULD use its IP address as the phase I identifier in main mode and PANA session ID [PANA-PROT] as the payload of ID_KEY_ID in aggressive mode for establishing the phase I SA. An IP address would also work well as an identifier in aggressive mode. But session ID was chosen to avoid potential problems with link-local addresses in IPv6, which are guaranteed to be unique only within the scope of a link.

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 next few sections discusses the packet formats and SPD entries.

6.0 Packet Formats

Following acronyms are used in this section.

EP's address is denoted by EP-ADDR.
PaC's address is denoted by PAC-ADDR.
The node with which the PaC is communicating is denoted by END-ADDR.

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

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

In case of IPv6, the outer IP header's addresses SHOULD be the link-local address of PaC and EP.

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

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

In case of IPv6, the outer IP header's addresses SHOULD be the link-local address of PaC and EP.

7.0 IPsec SPD entries

Following acronyms are used in this section.

EP's address is denoted by EP-ADDR.
PaC's address is denoted by PAC-ADDR.
PaC's link-local address is denoted by PAC-LINK-LOCAL
PaC's global address is denoted by PAC-GLOBAL-ADDR
EP's link-local address is denoted by EP-LINK-LOCAL

The SPD entries given below affect the traffic destined to EP-ADDR. If PAA and EP share the same IP address, then the traffic destined to PAA will also be affected. This implies that some of the control traffic, which is already protected using PANA SA will be protected with IPsec also. This can be avoided (if needed) by configuring bypass IPsec policy for packets, which are not shown below.

7.1 IPv4 SPD entries

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

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

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

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

During the IPsec SA setup, PaC uses PAC-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/router discovery [IPV6-ND] packets from being protected with IPsec. Due to the current limitation in specifying the proper selectors for neighbor discovery packets, separate set of selectors are added for bypassing IPsec for link-local traffic. All traffic destined to global address is always sent to the default router i.e, the global prefix is not considered to be on-link. In the future, when the IPsec [IPSEC] allows selectors to be based on ICMPv6 types, we just need an entry to bypass IPsec for neighbor/router discovery packets and the rest of the entries will be similar to IPv4 SPD entries.

```
   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
```

Following the conceptual model in section 5.1 of [IPV6-ND], PaC would maintain the following.

1) Neighbor Cache: This contains the entry for the link-local address of EP.
2) Destination Cache: This contains the entry for all on-link and off-link destinations.
3) Prefix List: This list contains the link-local prefix alone.
4) Default Router List: This list contains the EP alone.

Note that there are no entries for link-local addresses of other PaCs as it is assumed that communications with other PaCs use global addresses. All packets that are not destined to a link-local address are sent to the default router (EP). This can be achieved by turning off the "L" bit in the router advertisement.

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. This issue of configuring SPD entries for IKE packets is being currently discussed in the IPsec mailing list [IPSEC-ML].

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

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

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

[IPSEC-ML] https://roundup.machshav.com/ipsec/, RFC2401bis, Issue 67.

[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 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

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.