PANA Working Group
Internet Draft
Document: draft-mohanp-pana-ipsec-00.txt
Expires: October 2003

<M. Parthasarathy>
<Tahoe Networks>

May 2003

Securing the first hop in PANA using IPsec

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. But it does not specify any mechanism for preventing service theft. This document discusses the details for establishing an IPsec security association for securing

the link between PANA client and the enforcement point, which can be used to prevent service theft.

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 protocol itself stops here and does not discuss any methods for preventing service theft in the access network. The service theft can be prevented by simple IP address and MAC address filters, if the link between PANA client and PANA agent is a non-shared medium. In the case of shared links, filters are not sufficient to prevent service theft as it can be easily spoofed [PANA-THREATS]. This document discusses the details for establishing an IPsec security association for securing the link between PANA client and the enforcement point, which can be used to prevent service theft.

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. But it does not affect the details in this draft. 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.

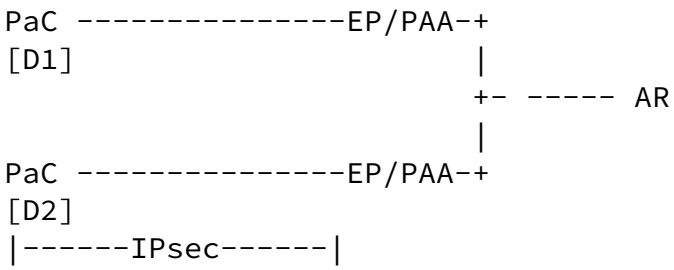

Figure 1

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 establishment

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 PAA (and hence EP) knows about the IP address of the PaC, before the IKE exchange

starts.

4.0 Communication between PAA and EP

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]. IKE pre-shared key is derived from the PANA SA, which is

established when PaC and PAA successfully authenticate to each other. Pre-shared key is derived from the PANA SA using a prf (e.g. SHA-1).

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. or aggressive mode with pre-shared key. PaC and EP SHOULD use its IP address as the client 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.

After Phase I SA is established, quick mode exchange is performed to establish an ESP transport mode IPsec SA for protecting the traffic between PaC and EP. The packets are still tunneled between PaC and EP as described later. But there is just one SA on the PaC for all the traffic flow between PaC and EP. The next few sections discuss about 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
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 that does not need protection.

7.1 IPv4 SPD entries

PaC's SPD OUT:

```
            IF source = PAC-ADDR  & destination = EP-ADDR &
             protocol = IP-in-IP
             THEN USE ESP TRANSPORT SA
```

```
PaC's SPD IN:
          IF source = EP-ADDR & destination = PAC-ADDR &
           protocol = IP-in-IP
           THEN USE ESP TRANSPORT SA
```

```
EP's SPD OUT:
          IF source = EP-ADDR & destination = PAC-ADDR &
           protocol = IP-in-IP
           THEN USE ESP TRANSPORT SA
```

```
EP's SPD IN:
          IF source = PAC-ADDR & destination = EP-ADDR &
           protocol = IP-in-IP
           THEN USE ESP TRANSPORT SA
```

PaC configures an IP-in-IP tunnel [IP-TUN] interface and configures a default route entry pointing at the IP-IP tunnel interface. There are only two routes to other nodes. There is a direct route to EP and a default route pointing at the tunnel interface. We denote the tunnel interface by PAC-EP-TUN interface in the following discussion. This

tunnel interface adds the encapsulating header <SRC=PAC-ADDR, DST=EP-ADDR>. Similarly, EP configures IP-IP tunnel interface for each PaC and there is one route for each PaC pointing at the right tunnel interface. The tunnel interface in EP adds the encapsulating header <SRC=EP-ADDR, DST=PAC-ADDR>.

It is assumed that PaC has two interfaces. First one represents the actual physical attachment to the network e.g., Ethernet interface and the second one is the tunnel interface PAC-EP-TUN interface. Following steps describe the packet processing in detail on a PaC.

1. An IPv4 packet is sent to destination "DEST".

2. None of the SPD rules matches the packet. Note that even if "DEST" is EP-ADDR, the protocol normally does not match unless the application is using raw sockets.

3. IP stack looks up the route. The default route matches and the route points at the PAC-EP-TUN interface. The tunnel encapsulates

the packet and the encapsulated packet re-enters IP stack.

4. Now, the packet matches the above SPD rule and the packet is protected using ESP transport mode SA. If an ESP transport mode SA is not found, IKE is triggered to setup the SA.

Similar steps happen on the EP also.

7.2 IPv6 SPD entries

The IPv6 SPD entries are slightly different from IPv4 to prevent the neighbor discovery [IPV6-ND] packets from being protected with IPsec. Due to the current limitation in specifying the proper selectors for neighbor discovery packets, the following selectors, bypasses 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.

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-LINK-LOCAL & destination = EP-LINK-LOCAL
```



```
           & protocol = IPv6-in-IPv6
           THEN USE ESP TRANSPORT SA
```

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 = EP-LINK-LOCAL & destination = PAC-LINK-LOCAL
             & protocol = IPv6-in-IPv6
                THEN USE ESP TRANSPORT SA
```

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 = EP-LINK-LOCAL & destination = PAC-LINK-LOCAL
             & protocol = IPv6-in-IPv6
                THEN USE ESP TRANSPORT SA
```

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-LINK-LOCAL & destination = EP-LINK-LOCAL
             & protocol = IPv6-in-IPv6
                THEN USE ESP TRANSPORT SA
```


PaC configures an IPv6-in-IPv6 tunnel [IPV6-TUN] interface and configures a default route entry pointing at the tunnel interface. We denote this by PAC-EP-TUN6 interface in the following discussion. The tunnel interface adds the encapsulating header <SRC=PAC-LINK-LOCAL, DST=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 EP and entries for link-local addresses of other PaC's on the link.
2) Destination Cache : This contains the entry for EP and entries for link-local addresses of other PaC's on the link.
3) Prefix List : This list contains the link-local prefix alone.
4) Default Router List : This list contains the EP alone.

Similarly, EP configures IPv6-in-IPv6 tunnel interface for each PaC and there is one route for each PaC pointing at the right tunnel interface. The tunnel interface in EP adds the encapsulating header <SRC=EP-LINK-LOCAL, DST=PAC-LINK-LOCAL>. 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. Following steps describe the packet processing in detail.

It is assumed that PaC has two interfaces. First one represents the actual physical attachment to the network e.g., Ethernet interface and the second one is the tunnel interface PAC-EP-TUN6 interface. Following steps describe the packet processing in detail on a PaC.

1. An IPv6 packet is sent to destination "DEST6".

2. If the packet has a source address of all zeroes e.g. duplicate address detection, then IPsec is bypassed irrespective of the destination address. These packets are sent out directly on the physical interface.

3. If source or DEST6 is link-local unicast or multicast, then IPsec is bypassed. Route lookup will return a route pointing at the physical interface through which the packets will be sent out.

4. At this step, none of the SPD rules match the packet. Note that even if "DEST" is "EP-ADDR", the protocol normally does not match unless the application is using raw sockets.

5. IP stack looks up the route. The default route matches and the route points at the PAC-EP-TUN6 interface. The tunnel encapsulates the packet and the encapsulated packet re-enters IP stack.

6. Now, the packet matches the SPD rule <SRC=PAC-LINK-LOCAL, DST=EP-

LINK-LOCAL, protocol = IPv6-in-IPv6> and the packet is protected using ESP transport mode SA. If an ESP transport mode SA is not found, IKE is triggered to setup the SA.

Similar steps happen on the EP also.

8.0 Double IPsec

If the PaC uses IPsec for secure remote access, there will be separate SPD entries protecting the traffic to/from remote network. In this case, IPsec needs to be applied twice, once for protecting the remote access and once for protecting the local access. Following are the differences when IPsec is used for remote access.

1) PaC's SPD OUT entry will have the following additional rules.

```
IF source = REMOTE-PAC-ADDR and DST = REMOTE-NET
 THEN USE ESP TUNNEL SA
 endpoints: REMOTE-PAC-ADDR  REMOTE-GW

 where <REMOTE-PAC-ADDR> is the address in remote network.
       <REMOTE-NET> is the subnet representing the remote
        network.
       <REMOTE-GW> is the external address of the remote
        security gateway.
 There is a corresponding entry in the security gateway
 of the remote network, which is not shown here.
```

2) There is a route for reaching REMOTE-NET through the PAC-EP-TUN/PAC-EP-TUN6 interface (see section 7.0).

Following steps describe the SA establishment and packet processing in detail.

1) PaC completes the PANA authentication exchange successfully and creates the PANA SA.

2) PaC initiates the IKE exchange with the EP and establishes a ESP transport mode IPSec SA.

3) PaC sends packet to destination DEST. If DEST is part of remote network, the SPD rule <SRC=REMOTE-PAC-ADDR,DST=REMOTE-NET> will match which in turn triggers the SA establishment process.

4) If SA does not exist, it will trigger the IKE packet to be sent to the REMOTE-GW. If SA exists go to step (9)

5) IKE packets enter IP and IPsec is bypassed using socket options or explicit bypass rules. The route entry for <REMOTE-NET> matches and hence gets encapsulated through the tunnel. The tunnel adds an extra IP header.

6) The tunneled packet gets protected using the IPsec SA created in step (2). Note that it is possible that the transport mode SA does not exist at this stage. In that case, IKE will be triggered and the packet will be sent to the EP address. This packet will not get encapsulated and will bypass IPsec and establish the IPsec SA with EP.

7) EP on receiving the packet from PaC, will decapsulate the packet and match with the selectors. As it will match successfully, the packet will be forwarded to the remote network.

8) Step (4) to step (6) will happen till the IPsec SA for the remote network is established.

9) Any packet to the remote network will follow the same path as the IKE packet described above. The packet will be protected using ESP tunnel mode SA and then a transport mode SA.

In IPv4, the packet sent by PaC on the wire has the following format.

```
IP [source = PAC-ADDR, destination = EP-ADDR]
ESP [Transport mode SA to EP]
IP [source = PAC-ADDR, destination = EP-ADDR]
ESP [Tunnel mode SA to REMOTE-NET]
IP [source = REMOTE-PAC-ADDR, destination = REMOTE-NET]
TCP/UDP
```

In IPv6, the final packet will be similar except the final IP header on the packet will use link-local address.

9.0 Security Considerations

This document discusses the use of IPsec in the context of PANA to prevent service theft in the access network. As IPsec cannot specify traffic selectors based on ICMP code types, the selectors defined in this document will bypass IPsec for all link-local traffic. This may be a problem in some cases. EP should be configured with an SPD rule to bypass IPsec for IKE traffic destined from PAC-ADDR to EP-ADDR and PAC-LINK-LOCAL to EP-LINK-LOCAL. It may give rise to some vulnerabilities as any node can send traffic to port 500 (which need not be IKE traffic) and EP will not enforce IPsec for such packets.

Note that there are no rules to bypass IPsec policy for IKE packets

destined to remote network on EP, as they are protected by the SA between PaC and EP.

10.0 Normative References

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

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

3. [PANA-PROT] D.Fosberg et al., "Protocol for Carrying Authentication for Network Access", draft-ietf-pana-00.txt

4. [PANA-THREATS] M.Parthasarathy, "PANA Threat analysis and security requirements", draft-ietf-pana-threats-eval-03.txt

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

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

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

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

8. [IP-TUN] C. Perkins, "IP Encapsulation within IP", RFC 2003, October 1996

9. [IPV6-TUN] A. Conta, "Generic Packet Tunneling in IPv6 specification", RFC 2473, December 1998.

12.0 Acknowledgments

Thanks to Francis Dupont for the interesting discussions and comments on this draft.

14.0 Author's Addresses

Mohan Parthasarathy
Tahoe Networks
3052 Orchard Drive

San Jose, CA 95134

Phone: 408-944-8220
Email: mohanp@tahoenetworks.com

15.0 Full Copyright Statement

Acknowledgement

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