WIDE Technical-Report in 2006

Configuring IPsec for SHISA

wide-tr-nautilus6-configuring-ipsec-for-shisa-00.pdf

WIDE Project : http://www.wide.ad.jp/

If you have any comments on this document, please contact to ad@wide.ad.jp

Configuring IPsec for SHISA

Keiichi Shima <keiichi@iijlab.net>

April 14, 2006

Abstract

In this memo, we describe the step-by-step configuration of IPsec database for SHISA Mobility Stack.

1 Introduction

It is always said that IPsec is awful. Regardless of the fact, we use IPsec in various places to provide security and privacy. Mobile IPv6 [1] is one of such protocols. To configure the IPsec parameters when using Mobile IPv6, you need to understand what traffic should be protected and how to set necessary parameters on your operating system. In this document, we will explain the procedure in the step-by-step manner. The target implementation is SHISA [2] that is built on top of the KAME IPv6 stack and works on FreeBSD and NetBSD.

2 Sample Network Configuration

Figure 1 is the sample network we assume in this document.

The home network prefix is `2001:db8:0:1000::/64`, the address of the home agent (HA) is `2001:db8:0:1000::1` and the home address (HoA) of the mobile node (MN) is `2001:db8:0:1000::4649`.

3 Protection Level

We can have several protection levels when using IPsec with Mobile IPv6. The following traffic can be protected.

1. Binding Update/Binding Acknowledgment messages
2. Mobile Prefix Solicitation (MPS)/Mobile Prefix Advertisement messages (MPA)
3. Normal traffic between MN and HA
4. Home Test Init (HoTI)/Home Test messages (HoT)
5. All tunneled normal traffic between MN and a correspondent node (CN)

In this memo, we will show the sample configuration to protect 1, 2 and 4.

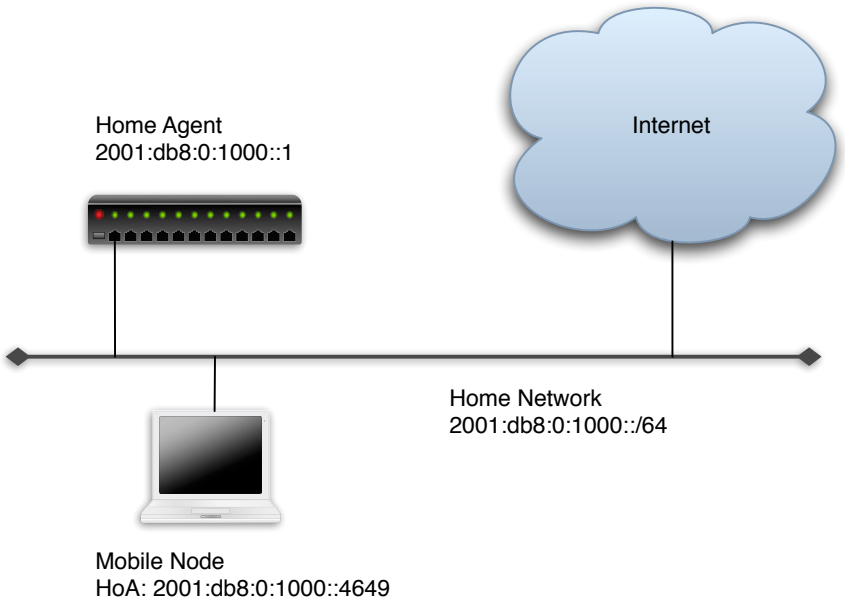

Figure 1: The sample network

4 Implementation Assumption

In this document we use the following implementation:

- FreeBSD5.4-RELEASE or NetBSD2.0
- The KAME snap kit that matches the above OSes

Although we use the above systems, the general description of how we should configure IPsec may be applied to other operating systems.

5 Security Parameters

In this memo, we use the following configuration.

IPsec protection mode We use the transport mode IPsec between MN and HA to protect Binding Update/Binding Acknowledgment messages and Mobile Prefix Solicitation/Advertisement messages.

We use the tunnel mode IPsec between MN and HA to protect Home Test Init/Home Test messages.

Security Association Security Association (SA) represents a secure data path from one node to the other node. In this example, we use 4 SAs, 2 for transport mode communication and 2 for tunnel mode communication. Table 1 shows the parameters for transport mode SAs and Table 2 shows those of tunnel mode SAs. The unique identifier defined in the tunnel mode SA is used to bind to the security policy to protect HoTI and HoT.

Transport mode: MN to HA

Source	`2001:db8:0:1000::4649` (HoA)
Destination	`2001:db8:0:1000::1` (HA)
IPsec protocol	`esp` (Encapsulating Security Payload)
SPI	`1000`
Encryption Algorithm	`des-cbc`
Encryption Key	`MNHAtran`
Authentication Algorithm	`hmac-sha1`
Authentication Key	`MNHAtransportMNHAtra`

Transport mode: HA to MN

Source	`2001:db8:0:1000::1` (HA)
Destination	`2001:db8:0:1000::4649` (HoA)
IPsec protocol	`esp` (Encapsulating Security Payload)
SPI	`1001`
Encryption Algorithm	`des-cbc`
Encryption Key	`HAMNtran`
Authentication Algorithm	`des-cbc`
Authentication Key	`HAMNtransportHAMNtra`

Table 1: Parameters of transport mode SAs

The encryption algorithms and the authentication algorithms can be chosen from all available algorithms which kernel supports (see the **setkey(8)** manual page). Each algorithm has a restriction in its key length. In `des-cbc` case, the key length is 64 bits. The key length of `hmac-sha1` is 160 bits. When using other algorithms, you have to take care the restriction of the key length.

In theory, we can use different algorithms for each SA. However, in this example we use the same encryption and authentication algorithms for all SAs.

SPI value is a 32 bits integer which is bound to a particular SA. The value must be unique in a node. Note that the value from 0 to 254 is reserved by IANA for future use. We cannot use the reserved range.

Security Policy Security Policy (SP) specifies the packet template to decide whether the incoming/outgoing packet should be processed by the IPsec stack. In this example, we protect all Mobility Header (MH) messages exchanged, MPS/MPA messages, and tunneled HoTI and HoT messages between MN and HA.

Table 3 shows the parameters of SP entries to protect MH messages on MN.

Table 4 shows the parameters of SP entries to protect MPS/MPA messages on MN.

Table 5 shows the parameters of SP entries to protect HoTI/HoT messages on MN.

The similar policies should be installed on HA. We omit the description of these SP entries for HA, since it is easy to understand by looking at the actual configuration file provided in Section 6

Tunnel mode: MN to HA

Source	`2001:db8:0:1000::4649` (HoA)
Destination	`2001:db8:0:1000::1` (HA)
IPsec protocol	`esp` (Encapsulating Security Payload)
SPI	`1002`
Unique Identifier	`1002`
Encryption Algorithm	`des-cbc`
Encryption Key	`MNHAtunn`
Authentication Algorithm	`hmac-sha1`
Authentication Key	`MNHAtunnelMNHAtunnel`

Tunnel mode: HA to MN

Source	`2001:db8:0:1000::1` (HA)
Destination	`2001:db8:0:1000::4649` (HoA)
IPsec protocol	`esp` (Encapsulating Security Payload)
SPI	`1003`
Unique Identifier	`1003`
Encryption Algorithm	`des-cbc`
Encryption Key	`HAMNtunn`
Authentication Algorithm	`hmac-sha1`
Authentication Key	`HAMNtunnelHAMNtunnel`

Table 2: Parameters of tunnel mode SAs

6 Configuration Files

In this section, we show the actual configuration file for the **setkey(8)** command based on the parameters discussed in previous sections.

The configuration file described in Figure2 installs SAs. These SAs must be installed on both MN and HA.

The configuration file described in Figure3 installs SPs on MN.

The configuration file described in Figure4 installs SPs on HA.

References

[1] David B. Johnson, Charles E. Perkins, and Jari Arkko. Mobility Support in IPv6. Technical Report RFC3775, IETF, June 2004.

[2] WIDE project. SHISA. Web page. http://www.mobileip.jp/.

Protection of outgoing MH messages

Source	`2001:db8:0:1000::4649` (HoA)
Destination	`2001:db8:0:1000::1` (HA)
Upper Layer Protocol	`135` (MH)
Direction	`out` (Outbound)
IPsec protocol	`esp`
IPsec mode	`transport`
IPsec processing level	`require` (Must be protected)

Protection of incoming MH messages

Source	`2001:db8:0:1000::1` (HA)
Destination	`2001:db8:0:1000::4649` (HoA)
Upper Layer Protocol	`135` (MH)
Direction	`in` (Inbound)
IPsec protocol	`esp`
IPsec mode	`transport`
IPsec processing level	`require` (Must be protected)

Table 3: SP parameters to protect MH messages for MN

Protection of outgoing MPS messages

Source	`2001:db8:0:1000::4649` (HoA)
Destination	`2001:db8:0:1000::1` (HA)
Upper Layer Protocol	`ipv6-icmp` or `58` (ICMPv6)
ICMPv6 type	`146` (MPS)
Direction	`out` (Outbound)
IPsec protocol	`esp`
IPsec mode	`transport`
IPsec processing level	`require` (Must be protected)

Protection of incoming MPA messages

Source	`2001:db8:0:1000::1` (HA)
Destination	`2001:db8:0:1000::4649` (HoA)
Upper Layer Protocol	`ipv6-icmp` or `58` (ICMPv6)
ICMPv6 type	`147` (MPA)
Direction	`in` (Inbound)
IPsec protocol	`esp`
IPsec mode	`transport`
IPsec processing level	`require` (Must be protected)

Table 4: SP parameters to protect MPS/MPA messages for MN

Protection of outgoing HoTI messages

Source	`2001:db8:0:1000::4649` (HoA)
Destination	`::/0` (any)
Upper Layer Protocol	`135` (MH)
MH type	`1` (HoTI)
Direction	`out` (Outbound)
IPsec protocol	`esp`
IPsec mode	`tunnel`
Tunnel source	`2001:db8:0:1000::4649` (HoA, which will be updated to CoA)
Tunnel destination	`2001:db8:0:1000::1` (HA)
IPsec processing level	`require` (Must be protected)
SA identifier	`1002` (Unique ID)

Protection of incoming HoT messages

Source	`::/0` (any)
Destination	`2001:db8:0:1000::4649` (HoA)
Upper Layer Protocol	`135` (MH)
MH type	`3` (HoT)
Direction	`in` (Inbound)
IPsec protocol	`esp`
IPsec mode	`tunnel`
Tunnel source	`2001:db8:0:1000::1` (HA)
Tunnel destination	`2001:db8:0:1000::4649` (HoA, which will be updated to CoA)
IPsec processing level	`require` (Must be protected)
SA identifier	`1003` (Unique ID)

Table 5: SP parameters to protect HoTI/HoT messages for MN

```
add 2001:200:db8:0:1000::4649 2001:200:db8:0:1000::1
        esp 1000
        -m transport
        -E des-cbc "MNHAtran"
        -A hmac-sha1 "MNHAtransportMNHAtra";
add 2001:200:db8:0:1000::1 2001:200:db8:0:1000::4649
        esp 1001
        -m transport
        -E des-cbc "HAMNtran"
        -A hmac-sha1 "HAMNtransportHAMNtra";
add 2001:200:db8:0:1000::4649 2001:200:db8:0:1000::1
        esp 1002
        -m tunnel
        -u 1002
        -E des-cbc "MNHAtunn"
        -A hmac-sha1 "MNHAtunnelMNHAtunnel";
add 2001:200:db8:0:1000::1 2001:200:db8:0:1000::4649
        esp 1003
        -m tunnel
        -u 1003
        -E des-cbc "HAMNtunn"
        -A hmac-sha1 "HAMNtunnelHAMNtunnel";
```

Figure 2: Configuration file to install SAs

```
spdadd 2001:db8:0:1000::4649 2001:db8:0:1000::1
        135 -P out ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::1 2001:db8:0:1000::4649
        135 -P in ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::4649 2001:db8:0:1000::1
        ipv6-icmp 146 -P out ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::1 2001:db8:0:1000::4649
        ipv6-icmp 147 -P in ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::4649 ::/0
        135 1 -P out ipsec
        esp/tunnel/2001:db8:0:1000::4649-2001:db8:0:1000::1/unique:1002;
spdadd ::/0 2001:db8:0:1000::4649
        135 3 -P in ipsec
        esp/tunnel/2001:db8:0:1000::1-2001:db8:0:1000::4649/unique:1003;
```

Figure 3: Configuration file to install SPs on MN

```
spdadd 2001:db8:0:1000::1 2001:db8:0:1000::4649
        135 -P out ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::4649 2001:db8:0:1000::1
        135 -P in ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::1 2001:db8:0:1000::4649
        ipv6-icmp 147 -P out ipsec
        esp/transport//require;
spdadd 2001:db8:0:1000::4649 2001:db8:0:1000::1
        ipv6-icmp 146 -P in ipsec
        esp/transport//require;
spdadd ::/0 2001:db8:0:1000::4649
        135 3 -P out ipsec
        esp/tunnel/2001:db8:0:1000::1-2001:db8:0:1000::4649/unique:1003;
spdadd 2001:db8:0:1000::4649 ::/0
        135 1 -P in ipsec
        esp/tunnel/2001:db8:0:1000::4649-2001:db8:0:1000::1/unique:1002;
```

Figure 4: Configuration file to install SPs on HA