How to configure IPv6 support for IPSec on AR450S routers

About this document

This document describes how to configure IPv6 support for IP Security (IPSec) on your AR450S router, and provides a configuration example, illustrating how to configure IPSec with IPv6 using ISAKMP/IKE key management.

Hardware and software used

- Allied Telesyn AR450S routers.
- Software release 2.5.2 patch 02.

Allied Telesyn feature licences may be required to enable IPv6, as well as 3DES and AES. Contact your nearest authorised Allied Telesyn distributor or reseller for details.

IPv6 Security

IPv6 provides built-in support for IP Security. The support is through the implementation of IPv6 extension headers - the Authentication Header (AH) and Encapsulating Security Payload (ESP) Header. These extension headers are mandatory in IPv6 and must be supported by all IPv6 nodes.

The Authentication Header is identified by protocol 51. It provides authentication and integrity (without confidentiality) services for the IPv6 packets.

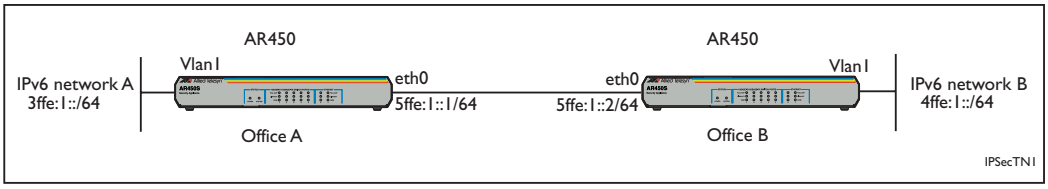
The Encapsulating Security Payload Header is identified by protocol 50. It provides integrity, confidentiality and authentication services for the IPv6 packets.

The Authentication Header and the Encapsulating Security Payload Header can be applied alone or together to provide the desired set of security services for the selected IPv6 packets. For more information about AH and ESP, see RFC 2402 "*IP Authentication Header*", and RFC 2406 "*IP Encapsulating Security Payload (ESP)*".

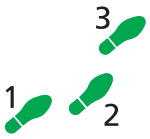
How to configure the routers

This section describes the steps for configuring the AR450 router with IPv6/IPSec using ISAKMP/IKE key management and AES encryption for the scenario illustrated in Figure 1.

Figure 1: Configuration setup for AR450 routers



Configuration for AR450 in Office A



1. **Configure the system**

```
set system name=Office_A
```

2. **Set up the user**

```
add user=secoff pass=secoff priv=securityofficer login=yes
login secoff
enable system security_mode
set user securedelay=600
create enco key=1 type=general value=123456789
```

3. **Configure IP**

```
enable ipv6
add ipv6 int=eth0 ip=5ffe:1::1/64
add ipv6 int=vlan1 ip=3ffe:1::1/64
add ipv6 rou=::/0 next=5ffe:1::2 int=eth0
```

4. **Configure ISAKMP**

```
create isakmp pol=test1 ipversion=6 pe=5ffe:1::2 enc=aes128 key=1
```

Note that in this example, AES128 bit encryption is used. AES on the AR450S also supports 192 bit and 256 bit encryption.

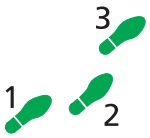
```
set isakmp pol=test1 sendd=true setc=true
enable isakmp
```

5. Configure IPSec

```
create ipsec sas=1 key=isakmp prot=esp enc=aes128 hasha=null

create ipsec sas=2 key=isakmp prot=ah hasha=sha

create ipsec bund=1 key=isakmp string="1 and 2"

create ipsec pol=isakmp1 int=eth0 ac=permit ipversion=6

set ipsec pol=isakmp1 lp=500 rp=500

create ipsec pol=test2 int=eth0 ac=ipsec ipversion=6
   key=isakmp bund=1 peer=5ffe:1::2

set ipsec pol=test2 lad=3ffe:1::/64 rad=4ffe:1::/64

create ipsec pol=ndc int=eth0 ac=permit ipv=6 icmptype=ndall
   ** see note

enable ipsec
```

*** An IPSEC policy is required to permit the ICMPv6 packet types 133-136 for IPv6 neighbour discovery on the Ethernet0 interface.*

Configuration for AR450 in Office B



1. Configure the system

```
set system name=Office_B
```

2. Configure the user.

```
add user=secoff pass=secoff priv=securityofficer login=yes

login secoff

enable system security_mode

set user securedelay=600

create enco key=1 type=general value=123456789
```

3. Configure IP

```
enable ipv6

add ipv6 int=eth0 ip=5ffe:1::2/64

add ipv6 int=vlan1 ip=4ffe:1::1/64

add ipv6 rou=::/0 next=5ffe:1::1 int=eth0
```

4. Configure ISAKMP

```
create isakmp pol=test1 ipversion=6 pe=5ffe:1::1 enc=aes128 key=1

set isakmp pol=test1 sendd=true setc=true

enable isakmp
```

5. Configure IPSec

```
create ipsec sas=1 key=isakmp prot=esp enc=aes128 hasha=null

create ipsec sas=2 key=isakmp prot=ah hasha=sha

create ipsec bund=1 key=isakmp string="1 and 2"

create ipsec pol=isakmp1 int=eth0 ac=permit ipversion=6

set ipsec pol=isakmp1 lp=500 rp=500

create ipsec pol=test2 int=eth0 ac=ipsec ipversion=6
   key=isakmp bund=1 peer=5ffe:1::1

set ipsec pol=test2 lad=4ffe:1::/64 rad=3ffe:1::/64

create ipsec pol=ndc int=eth0 ac=permit ipv=6 icmptype=ndall
   ** see note

enable ipsec
```

*** An IPSEC policy is required to permit the ICMPv6 packet types 133-136 for IPv6 neighbour discovery on the Ethernet0 interface.*

SHOW Command Outputs

The following command outputs are captured from the routers after successful Security Association negotiation between the peers.

Figure 2: Output of the SHOW ENCO KEY command for AR450 of Office A

```
SecOff Office_A> sh enco key

   ID  Type      Length Digest   Description                 Mod    IP
   ------------------------------------------------------------------
    1  GENERAL        9 8955F7B8 -                           -      -
```

Figure 3: Output of the SHOW ISA SA command for AR450 of Office A

```
SecOff Office_A> sh isa sa
                                  Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-------------------------------------------------------------------------
1    5ffe:0001::0002
                       AES    SHA   -/-/-                86400/75600/2360
```

Figure 4: Output of the SHOW IPS SA command for AR450 of Office A

```
SecOff Office_A> sh ips sa

SA Id Policy                Bundle  State     Protocol    OutSPI        InSPI
-------------------------------------------------------------------------------
    0 test2                      1  Valid     ESP     4176016067   3181970551
    1 test2                      1  Valid     AH       208077695    511686139
```

Figure 5: Output of the SHOW ENCO KEY command for AR450 of Office B

```
SecOff Office_B> sh enco key

   ID  Type      Length Digest   Description              Mod      IP
   ---------------------------------------------------------------------
    1  GENERAL        9 8955F7B8 -                        -        -
```

Figure 6: Output of the SHOW ISA SA command for AR450 of Office B

```
SecOff Office_B> sh isa sa
                                  Expiry Limits - hard/soft/used
SA Id PeerAddress    EncA.  HashA. Bytes Seconds
-------------------------------------------------------------------------------
1     5ffe:0001::0001
                     AES    SHA   -/-/- 86400/75600/2522
```

Figure 7: Output of the SHOW IPS SA command for AR450 of Office B

```
SecOff Office_B> sh ips sa

SA Id Policy                 Bundle  State     Protocol     OutSPI      InSPI
-------------------------------------------------------------------------------
   0  test2                      1  Valid     ESP      3181970551 4176016067
   1  test2                      1  Valid     AH        511686139  208077695
```