CHAPTER 10

# Per User Packet Filtering

This chapter discusses Per-User Packet Filtering and its implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:



## Mobile-User ACLs in Packet Filtering

The Home Agent supports per user packet filtering. This feature provides that for a successfully authenticated registration request, the RADIUS server will return “inACL” and “outACL” attributes in an access response to the HA. “inACL” and “outACL” attributes identify the pre-configured ACLs on the HA that are applied to mobility bindings. An input ACL will apply to traffic from the user leaving the tunnel. An output ACL will apply to traffic sent to the user using the tunnel. The attributes will be synched to the standby HA during normal sync and bulksync operation.

ACLs applied to a mobility binding can be displayed by **show ip mobile binding** command. Only the ACLs downloaded at the time of initial authentication will be applied. An ACL downloaded at the time of mobile re-authentication, for lifetime renewal, will not be applied.

The HA will accept one input ACL name and one output ACL name for each user.

Only named extended access-lists are supported for this feature

**Note** There is significant performance degradation when mobile user ACLs are applied to a large number of mobility bindings.

The Home Agent can filter both egress packets from an external data network and ingress data packets based on the Foreign Agent IP address or the Mobile Node IP address.

## Configuring ACLs on the Tunnel Interface

To configure ACLs to block certain traffic using the template tunnel feature, perform the following task:

| Command | Purpose |
|---|---|
| `Router(config)# interface tunnel 10`<br>`ip access-group 150 in -------> apply access-list 150`<br>`access-list 150 deny any 10.10.0.0 0.255.255.255`<br>`access-list permit any any`<br>`------> permit all but traffic to 10.10.0.0 network`<br><br>`ip mobile home-agent template tunnel 10 address 10.0.0.1` | Configures a tunnel template.<br>Configures the ACL.<br><br>Configures a Home Agent to use the template tunnel. |

## Verifying ACLs are Applied to a Tunnel

Here is example output of the **show ip mobile binding** command:

### ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
user1-flow8@abc.com (Bindings 1):
    Home Addr 30.0.0.5
    Care-of Addr 7.0.0.2, Src Addr 7.0.0.1
    Lifetime granted 00:03:20 (200), remaining 00:03:03
    Flags sBdmg-T-, Identification CB32792C.A7E22A29
    Tunnel0 src 7.0.0.242 dest 7.0.0.2 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Acct-Session-Id: 0x0000009D
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Radius Disconnect Enabled

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes
```

## In/Out Access List Per NAI/Realm

HA R5.0 supports upstream/downstream (in/out) ACLs for a mobile user if the HA receives the ACL names in the access-response message from AAA. But, if AAA does not send ACL names in the access-response, it is not possible to have in/out ACL applied for a mobile user. HA R5.1 supports in/out ACLs per tunnel using tunnel template, but this is applied on all users on the tunnel. It is not possible to apply ACLs only to specific users or to a set of users.

- This feature supports configuration of in/out ACL names per realm/NAI. The ACLs corresponding to the ACL names are configured by using the **ip access-list extended** *acl-name* command.
- If the ACL is modified/updated/created/deleted after associating the ACL name to realm/NAI, the modifications are applied immediately to the mobile users that are using this particular ACL.
- If the in/out ACL name associated with a realm/NAI is modified/added, then the new ACL will be applied to all the current bindings that belong to the realm/NAI.
- If the in/out ACL name associated with a realm/NAI is deleted, then the deleted ACL will not be applied to the current bindings that belong to the realm/NAI.
- Irrespective of whether in/out ACL name is configured for a realm/NAI, if the HA receives in/out ACL names in an access-response message, then the ACL names received from AAA are applied to the mobile user.

## Configuring the In/Out Access List Per NAI/Realm Feature

To enable the In/Out Access List per NAI/Realm feature in Cisco HA Release 5.1, perfrom the following task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Router(config)# ip mobile realm` *nai* \| *realm* `in-acl` *in-acl-name*<br>`Router(config)# [no] ip mobile realm` *nai* \| *realm* `out-acl` *out-acl-name* | |

### Limitations and Restrictions

- Only named extended ACLs are supported for configuring the in/out ACLs per realm/NAI.
- Only ACL names received in the first successful access-response for the session are applied. ACL names from the subsequent access-responses are not considered.