



CHAPTER 9

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, page 9-1](#)
- [Configuring ACLs on the Tunnel Interface, page 9-2](#)
- [Verifying ACLs are Applied to a Tunnel, page 9-2](#)

Mobile-User ACLs in Packet Filtering

The Home Agent supports per user packet filtering. Packet filtering 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 applies to traffic from the user leaving the tunnel. An output ACL applies to traffic sent to the user using the tunnel. The attributes are synced to the standby HA during normal sync and bulksync operation. Here are some additional conditions associate with this feature:

- The **show ip mobile binding** command displays ACLs applied to a mobility binding. Only the ACLs downloaded at the time of initial authentication are applied. An ACL downloaded at the time of mobile re-authentication, for lifetime renewal, is not 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

Performance is significantly degraded 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 ip access-group 150 in -----> apply access-list 150	Configures a tunnel template.
access-list 150 deny any 10.10.0.0 0.255.255.255 access-list permit any any -----> permit all but traffic to 10.10.0.0 network	Configures the ACL.
ip mobile home-agent template tunnel 10 address 10.0.0.1	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 44.0.0.1
Mobility Binding List:
44.0.0.1:
  Care-of Addr 55.0.0.11, Src Addr 55.0.0.11
  Lifetime granted 00:01:30 (90), remaining 00:00:51
  Flags sbDmg-T-, Identification C661D5A0.4188908
  Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
Tunnel1 Input ACL: inaclname
Tunnel1 Output ACL: outaclname - Empty list or not configured.
  MR Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
  Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
  Mobile Networks: 111.0.0.0/255.0.0.0 (S)
  Acct-Session-Id: 0
  Sent on tunnel to MN: 0 packets, 0 bytes
  Received on reverse tunnel from MN: 0 packets, 0 bytes
```

```
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
```