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

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 Mobile User ACLs

To configure mobile user ACLs, perform the following task:

Command	Purpose
ON PDSN-HA ---------- ... ip access-list extended mipinacl permit ip host 40.0.0.1 host 20.20.205.220 log permit ip any any log ip access-list extended mipoutacl permit ip host 20.20.205.220 host 40.0.0.1 log permit ip any any log .... **ON RADIUS** --------- **OutACL = *acl name*** This attribute specifies the ACL name to be applied to traffic sent by a correspondent node towards mobile node **InACL = *acl name*** This attribute specifies the ACL name to be applied to traffic sent by a mobile towards correspondent node	Configures mobile user ACLs.

Verifying Mobile User ACLs

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

```
router# show ip mobile binding
Mobility Binding List:
Total 1
user1-flow8@abc.com (Bindings 1):
Home Addr 40.0.0.1
Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
Lifetime granted 00:05:00 (300), remaining 00:04:21
Flags sBdmg-T-, Identification C7165AA3.10000
Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
Tunnel0 Input ACL: mipinacl
Tunnel0 Output ACL: mipoutacl
Routing Options - (B)Broadcast (T)Reverse-tunnel
Service Options:
Dynamic HA assignment
Revocation negotiated - I-bit set
Acct-Session-Id: 59
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
DNS Address primary 10.77.155.10 secondary 6.6.6.6
DNS Address Assignment enabled with entity Configured at Homeagent(3)
Dynamic DNS update to server enabled
```

Using Tunnel Templates

Tunnel templates allow configurations such as ACLs, to be applied to dynamic tunnels brought up on the Home Agent. A tunnel template is a statically configured Tunnel interface. A unique tunnel template can be specified for each of the Home Agent address configured on the Home Agent.

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`
`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`
 	
`ip mobile home-agent template tunnel 10 address 10.0.0.1`
	Configures a tunnel template.
	Configures the ACL.
	
	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
```