CHAPTER 9

ユーザ単位パケット フィルタリング

この章では、ユーザ単位パケット フィルタリング、および Cisco IOS Mobile Wireless Home Agent ソフトウェアでのこの機能の実装について説明します。

この章の内容は、次のとおりです。

パケット フィルタリングでのモバイル ユーザ ACL

Home Agent（HA）は、ユーザ単位のパケット フィルタリングをサポートしています。この機能を使用すると、レジストレーション要求が正常に認証された場合、RADIUS サーバから HA に戻されるアクセス応答に、「inACL」および「outACL」アトリビュートが含まれます。「inACL」および「outACL」アトリビュートは、モビリティ バインディングに適用される HA 上の設定済み ACL を識別します。入力 ACL は、ユーザからトンネル経由で発信されたトラフィックに適用されます。出力 ACL は、トンネル経由でユーザ宛てに送信されたトラフィックに適用されます。これらのアトリビュートは、標準同期およびバルク同期処理により、スタンバイ HA に同期化されます。

モビリティ バインディングに適用された ACL は、**show ip mobile binding** コマンドによって表示できます。初回認証時にダウンロードされた ACL だけが適用されます。ライフタイム更新用のモバイル再認証時にダウンロードされた ACL は、適用されません。

HA は、各ユーザについて、1 つの入力 ACL 名と 1 つの出力 ACL 名を受け入れます。

この機能でサポートされるのは、名前付き拡張アクセスリストだけです。

（注） 多数のモビリティ バインディングにモバイル ユーザ ACL を適用すると、パフォーマンスが著しく劣化します。

HA では、外部データ ネットワークからの出力パケット、および Foreign Agent（FA; 外部エージェント）または Mobile Node（MN; モバイル ノード）の IP アドレスに基づく入力データ パケットの両方をフィルタリングできます。

トンネル インターフェイス上での ACL の設定

テンプレート トンネル機能を使用して特定のトラフィックをブロックする ACL を設定するには、次の作業を実行します。

コマンド	目的
`Router(config)# interface tunnel 10` `ip access-group 150 in -------> apply access-list 150`	トンネル テンプレートを設定します。

`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`
	ACL を設定します。

`ip mobile home-agent template tunnel 10  address 10.0.0.1`	テンプレート トンネルを使用する HA を設定します。

トンネルへの ACL 適用の確認

次に、**show ip mobile binding** コマンドの出力例を示します。

モビリティ バインディングに適用された ACL、アカウンティング セッション ID、およびアカウンティング カウンタ

```
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
```