CHAPTER 10

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。

この章は、次の内容で構成されています。

パケット フィルタリングでのモバイル ユーザ アクセス コントロール リスト（ACL）

Home Agent（HA）は、ユーザ単位パケット 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、登録要求が正常に認証された場合、Remote Authentication Dial-In User Service（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 Access Control List（ACL; アクセス コントロール リスト）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 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 **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	トンネル テンプレートを設定します。 ACL を設定します。 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
```

ネットワーク アクセス識別子（NAI）/ レルム単位の入力/出力 アクセス リスト

HA R5.0 は、HA が Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）からの access-response メッセージで ACL 名を受け取った場合に、モバイル ユーザに対してアップストリーム/ダウンストリーム（入力/出力）ACL をサポートします。ただし、AAA が access-response で ACL 名を送信しない場合は、モバイル ユーザに対して入力/出力 ACL を適用できません。HA R5.1 は、トンネル テンプレートを使用するトンネル単位の入力/出力 ACL をサポートしますが、これはそのトンネル上のすべてのユーザに適用されます。特定のユーザまたは一連のユーザだけに ACL を適用することはできません。

- この機能では、レルム/Network Access Identifier（NAI; ネットワーク アクセス識別子）単位の入力/出力 ACL 名の設定がサポートされます。ACL 名に対応する ACL は、**ip access-list extended** *acl-name* コマンドを使用して設定します。
- ACL 名をレルム/NAI に関連付けた後で ACL を修正、更新、作成、または削除すると、その特定の ACL を使用しているモバイル ユーザに修正がただちに適用されます。
- レルム/NAI に関連付けられている入力/出力 ACL 名を変更または追加すると、そのレルム/NAI に属する現在のすべてのバインディングに新しい ACL が適用されます。
- レルム/NAI に関連付けられている入力/出力 ACL 名を削除した場合、削除された ACL は、そのレルム/NAI に属する現在のバインディングに適用されません。
- 入力/出力 ACL 名がレルム/NAI に設定されているかどうかに関係なく、HA が access-response メッセージで入力/出力 ACL 名を受け取ると、AAA から受け取った ACL 名がモバイル ユーザに適用されます。

NAI/ レルム機能単位の入力/出力アクセス リストの設定

Cisco HA Release 5.1 で NAI/ レルム機能単位の入力/出力アクセス リストをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm` *nai* `|` *realm* `in-acl` *in-acl-name* `Router(config)# [no] ip mobile realm` *nai* `|` *realm* `out-acl` *out-acl-name*	

制限事項および制約事項

- レルム/NAI 単位の入力/出力 ACL を設定する場合、名前付き拡張アクセス リストだけがサポートされます。
- セッションに対する最初の正常な access-response で受け取られた ACL 名だけが適用されます。後続の access-response の ACL 名は考慮されません。