CHAPTER 45

Cisco IOS ファイアウォール フィーチャ セットの設定

この章では、Catalyst 6500 シリーズ スイッチで Cisco IOS ファイアウォール フィーチャ セットを設定する手順について説明します。この章で説明する内容は、次のとおりです。

Cisco IOS ファイアウォール フィーチャ セットのサポートの概要

ファイアウォール フィーチャ セット イメージは、次の Cisco IOS ファイアウォール機能をサポートします。

- Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）— PFC は、CBAC が MSFC ソフトウェアに適用されている MSFC に対して CBAC を必要とするフローを方向付ける NetFlow テーブルにエントリを追加します。
- 認証プロキシ — MSFC での認証後、PFC は認証ポリシー用の TCAM サポートを提供します。
- Port-to-Application Mapping（PAM; ポート ツー アプリケーション マッピング）— PAM は MSFC のソフトウェアで実行されます。

Cisco IOS ファイアウォール機能については、次のマニュアルを参照してください。

- 『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」の章および次のセクション
  - 次の URL の「Cisco IOS Firewall Overview」
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scffiwl.htm
  - 次の URL の「Configuring Context-Based Access Control」
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfcac.htm
  - 次の URL の「Configuring Authentication Proxy」
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfahp.htm
- 次の URL の『*Cisco IOS Security Command Reference*』
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

Cisco IOS ファイアウォール イメージを使用するかどうかに関係なく、次の機能がサポートされます。

- 標準アクセス リストおよびスタティック拡張アクセス リスト
- Lock-and-Key（ダイナミック アクセス リスト）
- IP セッション フィルタリング（再帰アクセス リスト）
- TCP インターセプト
- セキュリティ サーバ サポート
- Network Address Translation（NAT; ネットワーク アドレス変換）
- 近接ルータ認証
- イベント ログ機能
- ユーザ認証および許可

（注）　Catalyst 6500 シリーズ スイッチは、Intrusion Detection System Module（IDSM）（WS-X6381-IDS）をサポートします。Catalyst 6500 シリーズ スイッチは、Cisco IOS ファイアウォール IDS 機能をサポートしません。この機能を設定するには、**ip audit** コマンドを使用します。

Cisco IOS ファイアウォールの注意事項および制約事項

Cisco IOS ファイアウォール機能を設定する場合は、次の注意事項および制約事項に従ってください。

- 他のプラットフォームで、特定のポートに関して **ip inspect** コマンドを入力すると、CBAC は、検査されたトラフィックがネットワーク装置を通過できるように、他のポートの Access Control List（ACL; アクセス制御リスト）を変更します。他のポート経由のトラフィックを拒否する ACL で、トラフィックの通過を許可するには、Catalyst 6500 シリーズ スイッチ上で、**mls ip inspect** コマンドを入力する必要があります。詳細については、「追加の CBAC 設定」（p.45-4）を参照してください。
- 再帰 ACL および CBAC には、矛盾するフロー マスク要件があります。再帰 ACL は、MSFC のソフトウェアで処理されます。
- CBAC は VACL と互換性がありません。CBAC および VACL はスイッチ上に設定できますが、同じサブネット（VLAN［仮想 LAN］）内には設定できません。

（注） IDSM は、VACL を使ってトラフィックを選択します。CBAC が設定されているサブネット内で IDSM を使用するには、**mls ip ids** *acl_name* インターフェイス コマンドを入力します。*acl_name* は、IDSM のトラフィックを選択する場合に設定します。

- Microsoft NetMeeting（2.0 以降）のトラフィックを検査するには、**h323** および **tcp** の両方の検査をオンにします。
- Web トラフィックを検査するには、**tcp** 検査をオンにします。パフォーマンスの低下を回避するには、**http** 検査をオフにして、Java をブロックします。
- Quality of Service（QoS; サービス品質）および CBAC は相互に作用したり、干渉したりすることはありません。
- CBAC は、レイヤ 3 インターフェイスとして設定された物理ポート、および VLAN インターフェイスに設定できます。
- 同じインターフェイスに VACL と CBAC を設定することはできません。

追加の CBAC 設定

Catalyst 6500 シリーズ スイッチに、追加の CBAC 設定をする必要があります。Catalyst 6500 シリーズ スイッチ以外のネットワーク装置に、ポートがトラフィックを拒否するように設定されている場合、CBAC を使用すると、**ip inspect** コマンドで設定されたポートの場合、そのポートを経由してトラフィックを双方向に送信できます。同じ状況が、トラフィックが通過する必要がある別のポートにも適用されます（次の例を参照）。

```
Router(config)# ip inspect name permit_ftp ftp
Router(config)# interface vlan 100
Router(config-if)# ip inspect permit_ftp in
Router(config-if)# ip access-group deny_ftp_a in
Router(config-if)# ip access-group deny_ftp_b out
Router(config-if)# exit
Router(config)# interface vlan 200
Router(config-if)# ip access-group deny_ftp_c in
Router(config-if)# ip access-group deny_ftp_d out
Router(config-if)# exit
Router(config)# interface vlan 300
Router(config-if)# ip access-group deny_ftp_e in
Router(config-if)# ip access-group deny_ftp_f out
Router(config-if)# end
```

VLAN 100 で開始した FTP（ファイル転送プロトコル）セッションを VLAN 200 で終了する必要がある場合、CBAC を使用すると、ACL の deny_ftp_a、deny_ftp_b、deny_ftp_c、および deny_ftp_d を経由して FTP トラフィックを送信できます。VLAN 100 で開始した FTP セッションを VLAN 300 で終了する必要がある場合、CBAC を使用すると、ACL の deny_ftp_a、deny_ftp_b、deny_ftp_e、および deny_ftp_f を経由して FTP トラフィックを送信できます。

Catalyst 6500 シリーズ スイッチのポートがトラフィックを拒否するように設定されている場合、CBAC を使用すると、**ip inspect** コマンドで設定されたポートのみを経由してトラフィックを双方向に送信できます。他のポートは、**mls ip inspect** コマンドを使用して設定する必要があります。

VLAN 100 で開始した FTP セッションを VLAN 200 で終了する必要がある場合、Catalyst 6500 シリーズ スイッチ上で CBAC を使用すると、FTP トラフィックは ACL の deny_ftp_a および deny_ftp_b だけを通過します。ACL の deny_ftp_c および deny_ftp_d をトラフィックが通過するようにするには、次の例のように、**mls ip inspect deny_ftp_c** コマンドおよび **mls ip inspect deny_ftp_d** コマンドを入力する必要があります。

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)# mls ip inspect deny_ftp_d
```

VLAN 300 で FTP トラフィックを終了するには、**mls ip inspect deny_ftp_e** および **mls ip inspect deny_ftp_f** コマンドを入力する必要があります。設定を確認するには、**show fm insp** [**detail**] コマンドを入力します。

show fm insp [**detail**] コマンドを実行すると、ACL のリスト、および CBAC が設定されているポートやステータス（**ACTIVE** または **INACTIVE**）が表示されます（次の例を参照）。

```
Router# show fm insp
         interface:Vlan305(in) status :ACTIVE
         acl name:deny
           interfaces:
              Vlan305(out):status ACTIVE
```

VLAN 305 では、着信方向の検査がアクティブで、ACL は設定されていません。VLAN 305 では、ACL **deny** が発信方向に適用されていて、検査がアクティブです。

すべてのフロー情報を表示するには、**detail** キーワードを使用します。

CBAC を設定する前にポートに VACL を設定した場合は、表示されるステータスは INACTIVE となります。それ以外の場合は ACTIVE です。PFC リソースがなくなっている場合にこのコマンドを実行すると、「BRIDGE」と表示され、続いて、処理のために MSFC に送信された NetFlow 要求のうち過去に失敗したが現在アクティブな NetFlow 要求の数が表示されます。