CHAPTER 6

グローバル オブジェクトの追加

Objects ペインでは、FWSM にポリシーを組み込む際に不可欠な再利用コンポーネントの設定、表示、修正がすべてできます。たとえば、セキュリティ ポリシーの対象ホストやネットワークを定義すると、ホストやネットワークを選択するだけで機能を適用でき、適用対象を何度も定義する必要がなくなります。そのため、時間を短縮できると同時に、一貫性のあるセキュリティ ポリシーを高い精度で実現できます。ホストやネットワークの追加、削除が必要な場合、Objects ペインを利用して 1 箇所から変更できます。

この章には、次の項があります。

ネットワーク オブジェクトおよびグループの使用

この項では、ネットワーク オブジェクトおよびグループを使用する方法について説明します。次の項目を取り上げます。

ネットワーク オブジェクトの概要

ネットワーク オブジェクトに、ホストおよびネットワークの IP アドレスをあらかじめ定義しておくと、以後の設定がスムーズになります。アクセス ルールや AAA ルールなどのセキュリティ ポリシーを設定するだけで、手動で入力する代わりに事前定義済みのアドレスをクリックすることができます。さらに、オブジェクトの定義を変更すると、そのオブジェクトを使用するルールでその変更が自動的に継承されます。

ネットワーク オブジェクトを手動で追加することもできますが、アクセス ルールや AAA ルールなどの既存のコンフィギュレーションから ASDM で自動的にオブジェクトを作成することもできます。これらの取得済みオブジェクトのいずれかを編集すると、このオブジェクトを使用するルールを後で削除しても、そのオブジェクトは残っています。それ以外の場合、取得済みオブジェクトを更新すると、現在のコンフィギュレーションのみが反映されます。

複数のホストやネットワークをグループ化しておくと、アドレス グループにルールを簡単に適用できます。複数のネットワーク オブジェクト グループをネストして「グループのグループ」にすると、単一のグループとして参照できます。

ルールの設定時に、ASDM ウィンドウの右側の Addresses サイド ペインにも使用可能なネットワーク オブジェクトやネットワーク オブジェクト グループが表示されます。このサイド ペインから直接オブジェクトを追加、編集、削除できます。また、サイド ペインから選択したアクセス ルールの送信元または宛先に追加するネットワーク オブジェクトおよびグループをドラッグすることもできます。

ネットワーク オブジェクトの設定

ネットワーク オブジェクトを設定するには、次の手順を実行します。

ステップ 1　Configuration > Global Objects > Network Objects/Group ペインで **Add > Network Object** をクリックして新しいオブジェクトを追加するか、またはオブジェクトを選択してから **Edit** をクリックします。

ルールを追加する場合、ルール ウィンドウの Addresses サイド ペインからもネットワーク オブジェクトを追加または編集できます。

リストにあるオブジェクトを検索するには、Filter フィールドに名前または IP アドレスを入力し、**Filter** をクリックします。ワイルドカード文字としてアスタリスク (*) と疑問符 (?) を使用できます。

Add/Edit Network Object ダイアログボックスが表示されます。

ステップ 2　次の値を入力します。

- Name：（オプション）オブジェクト名。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、およびアンダースコア（_）です。64 文字以内で指定します。
- IP Address：ホストまたはネットワークの IP アドレス。
- Netmask：IP アドレスのサブネット マスク。
- Description：（オプション）ネットワーク オブジェクトの説明。

ステップ 3　**OK** をクリックします。

これで、ルールの作成時にこのネットワーク オブジェクトを使用できるようになります。編集済みオブジェクトの場合、このオブジェクトを使用するルールで変更が自動的に継承されます。

（注）　使用中のネットワーク オブジェクトを削除することはできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループを設定するには、次の手順を実行します。

ステップ 1　Configuration > Global Objects > Network Objects/Group ペインで **Add > Network Object Group** をクリックして新しいオブジェクト グループを追加するか、またはオブジェクト グループを選択してから **Edit** をクリックします。

ルールを追加する場合、ルール ウィンドウの Addresses サイド ペインからもネットワーク オブジェクト グループを追加または編集できます。

リストにあるオブジェクトを検索するには、Filter フィールドに名前または IP アドレスを入力し、**Filter** をクリックします。ワイルドカード文字としてアスタリスク (*) と疑問符 (?) を使用できます。

Add/Edit Network Object Group ダイアログボックスが表示されます。

ステップ 2　Group Name フィールドにグループ名を入力します。

使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、およびアンダースコア（_）です。64 文字以内で指定します。

ステップ 3　（オプション）Description フィールドに説明を最大 200 文字で入力します。

ステップ 4　既存のオブジェクトまたはグループを新しいグループに追加したり（ネストされたグループを許可する）、新しいアドレスを作成してグループに追加したりできます。

- 既存のネットワーク　オブジェクトまたはグループを新しいグループに追加するには、Existing Network Objects/Groups ペインでオブジェクトを右クリックします。

  また、オブジェクトを選択してから **Add** ボタンをクリックすることもできます。オブジェクトまたはグループは右側の Members in Group ペインに追加されます。
- 新しいアドレスを追加するには、Create New Network Object Member 領域に値を入力して **Add** をクリックします。

  オブジェクトまたはグループは右側の Members in Group ペインに追加されます。アドレスは、ネットワーク オブジェクトのリストにも追加されます。

オブジェクトを削除するには、Members in Group ペインでオブジェクトをダブルクリックするか、または **Remove** ボタンをクリックします。

ステップ 5　メンバー オブジェクトをすべて追加したら、**OK** をクリックします。

これで、ルールの作成時にこのネットワーク オブジェクト グループを使用できるようになります。編集済みオブジェクト グループの場合、このグループを使用するルールで変更が自動的に継承されます。

（注）　使用中のネットワーク オブジェクト グループを削除することはできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ルールでのネットワーク オブジェクトおよびグループの使用

ルールを作成すると、IP アドレスを手動で入力するか、あるいはネットワーク オブジェクトまたはグループを参照してルールで使用できます。

（注）　アクセス ルールの場合のみ、ネットワーク オブジェクトおよびグループを、Addresses ペインから、選択したアクセス ルールの送信元または宛先にドラッグ アンド ドロップできます。

ネットワーク オブジェクトまたはグループをルールで使用するには、次の手順を実行します。

ステップ 1　ルールのダイアログボックスで、送信元または宛先アドレスのフィールドの隣にある参照ボタン **...** をクリックします。

Browse Source Address または Browse Destination Address ダイアログボックスが表示されます。

ステップ 2　新しいネットワーク オブジェクトまたはグループを追加するか、あるいは既存のネットワーク オブジェクトまたはグループをダブルクリックして選択します。

リストにあるオブジェクトを検索するには、Filter フィールドに名前または IP アドレスを入力し、**Filter** をクリックします。ワイルドカード文字としてアスタリスク (*) と疑問符 (?) を使用できます。

- 新しいネットワーク オブジェクトの追加するには、P.6-2 の「ネットワーク オブジェクトの設定」を参照してください。
- 新しいネットワーク オブジェクト グループを追加するには、P.6-3 の「ネットワーク オブジェクト グループの設定」を参照してください。

新しいオブジェクトを追加するか、または既存のオブジェクトをダブルクリックすると、それらのオブジェクトは Selected Source/Destination フィールドに表示されます。アクセス ルールの場合、このフィールドで複数のオブジェクトまたはグループをカンマ区切りで追加できます。

ステップ 3　**OK** をクリックします。

ルールのダイアログボックスに戻ります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ネットワーク オブジェクトまたはグループの使用状況の表示

ネットワーク オブジェクトまたはグループを使用するルールを表示するには、Configuration > Global Objects > Network Objects/Group ペインで、拡大鏡の Find アイコンをクリックします。

Usages ダイアログボックスに、ネットワーク オブジェクトまたはグループを使用中のすべてのルールが表示されます。このダイアログボックスには、そのオブジェクトを含むネットワーク オブジェクト グループも表示されます。

サービス グループの設定

この項では、サービス グループを設定する方法について説明します。次の項目を取り上げます。

Service Groups

Service Groups ペインで、指定したグループに複数のサービスを関連付けます。1 つのグループでプロトコルとサービスの種類を指定することもできますが、次の種類ごとにサービス グループを作成することもできます。

- TCP ポート
- UDP ポート
- TCP-UDP ポート
- ICMP タイプ
- IP プロトコル

複数のサービス グループをネストして「グループのグループ」にすると、単一のグループとして参照できます。

サービス グループは、ポート、ICMP タイプ、プロトコルを識別する必要がある、ほとんどのコンフィギュレーションで使用できます。NAT ルールやセキュリティ ポリシー ルールの設定時に、ASDM ウィンドウの右側のサイド ペインにもサービス グループなど使用可能なグローバル オブジェクトが表示されます。このサイド ペインから直接オブジェクトを追加、編集、削除できます。

フィールド

- Add：サービス グループを追加します。ドロップダウン リストからサービス グループの種類を選択して追加するか、または Service Group から複数の種類を選択します。
- Edit：サービス グループを編集します。
- Delete：サービス グループを削除します。サービス グループを削除すると、使用されているすべてのサービス グループから削除されます。アクセス ルールで使用しているサービス グループは、削除しないでください。アクセス ルールで使用されているサービス グループを空にすることはできません。
- Find: フィルタして名前が一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter フィールド：サービス グループの名前を入力します。ワイルドカード文字としてアスタリスク（*）と疑問符（?）を使用できます。
  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
- Name：サービス グループ名を一覧表示します。名前の隣にあるプラス（+）アイコンをクリックすると、サービス グループが展開され、サービスを確認できます。マイナス（-）アイコンをクリックすると、サービス グループが折りたたまれます。
- Protocol：サービス グループのプロトコルを一覧表示します。
- Source Ports：プロトコルの送信元ポートを一覧表示します。
- Destination Ports：プロトコルの宛先ポートを一覧表示します。
- ICMP Type：サービス グループの ICMP タイプを一覧表示します。
- Description：サービス グループの説明を一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Service Group

Add/Edit Service Group ダイアログボックスで、サービスをサービス グループに割り当てます。このダイアログボックス名は追加するサービス グループのタイプと同じ名前になります。たとえば、追加するサービス グループが TCP の場合、Add/Edit TCP Service Group ダイアログボックスが表示されます。

フィールド

- Group Name：グループ名を 64 文字以内で入力します。重複するオブジェクト グループ名は指定できません。サービス グループの名前にネットワーク オブジェクト グループで使用した名前は使用できません。
- Description：サービス グループの説明を 200 文字以内で入力します。
- Existing Service/Service Group：サービス グループに追加可能なアイテムを識別します。定義済みのサービス グループから選択するか、よく使用されるポート、タイプ、プロトコルの名前のリストから選択します。
  - Service Groups：このテーブルのタイトルは、追加するサービス グループ タイプによって異なります。定義済みのサービス グループが含まれます。
  - Predefined：定義済みのポート、タイプ、またはプロトコルが一覧表示されます。
- Create new member：新しいサービス グループのメンバーを作成します。
  - Service Type：新しいサービス グループ メンバーのサービス タイプを選択します。サービス タイプには TCP、UDP、TCP-UDP、ICMP、およびプロトコルがあります。
  - Destination Port/Range：新しい TCP、UDP、または TCP-UDP サービス グループ メンバーの宛先ポートまたは範囲を入力します。
  - Source Port/Range：新しい TCP、UDP、または TCP-UDP サービス グループ メンバーの送信元ポートまたは範囲を入力します。
  - ICMP Type：新しい ICMP サービス グループ メンバーの ICMP タイプを入力します。
  - Protocol：新しいプロトコルのサービス グループ メンバーのプロトコルを入力します。
- Members in Group：サービス グループに追加済みのアイテムを示します。
- Add：選択したアイテムをサービス グループに追加します。
- Remove：選択したアイテムをサービス グループから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Browse Service Groups

Browse Service Groups ダイアログボックスで、サービス グループを選択します。このダイアログボックスはさまざまなコンフィギュレーション画面で使用され、その時のタスクに該当する名前で表示されます。たとえば、Add/Edit Access Rule ダイアログボックスの場合、このダイアログボックス名は「Browse Source Port」または「Browse Destination Port」になります。

フィールド

- Add：サービス グループを追加します。
- Edit：選択したサービス グループを編集します。
- Delete：選択したサービス グループを削除します。
- Find: フィルタして名前が一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter フィールド：サービス グループの名前を入力します。ワイルドカード文字としてアスタリスク（*）と疑問符（?）を使用できます。
  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
- Type：TCP、UDP、TCP-UDP、ICMP、Protocol など、表示するサービス グループのタイプを選択できます。タイプをすべて表示するには、**All** を選択します。通常、ルールのタイプを設定する場合、使用できるサービス グループのタイプは 1 つだけです。TCP のアクセス ルールに UDP のサービス グループは選択できません。
- Name：サービス グループ名を示します。アイテムの名前の隣にあるプラス（+）アイコンをクリックすると、アイテムが展開されます。マイナス（-）アイコンをクリックすると、アイテムが折りたたまれます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

検査マップの設定

ここでは、次の項目について説明します。

検査マップの概要

検査マップでは、専用のプロトコル検査エンジンの検査マップを作成できます。検査マップを利用して、プロトコル検査エンジンのコンフィギュレーションを保存します。それから、グローバル セキュリティ ポリシーや特定のインターフェイスのセキュリティ ポリシーを使用して特定のトラフィック タイプにマップを関連付け、検査マップのコンフィギュレーション設定をイネーブルにします。

Security Policy ペインの Service Policy Rules オプションから検査マップをトラフィックに適用すると、サービス ポリシーで指定した基準に従って照合が行われます。サービス ポリシーは、FWSM の特定のインターフェイスまたはすべてのインターフェイスに適用することができます。

FWSM のステートフル アプリケーション検査にアルゴリズムを適用して、アプリケーションのセキュリティとサービスを保証します。アプリケーションの中には特別な処理を必要とするものがあり、専用の検査エンジンでそのような場合に対応します。特別なアプリケーション検査エンジンを必要とするのは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むか、またはダイナミックに割り当てられたポートでセカンダリ チャネルを開くアプリケーションです。

アプリケーション検査エンジンは NAT と連携し、アドレッシング情報が埋め込まれている場所の識別をサポートします。これによって NAT では、それらの埋め込まれたアドレスを変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートしたりできます。

各アプリケーション検査エンジンはセッションを監視して、セカンダリ チャネルのポート番号も確認します。多くのプロトコルは、パフォーマンスを向上させるために、TCP または UDP のセカンダリ ポートを開きます。ウェルノウン ポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。アプリケーション検査エンジンは、この初期セッションを監視し、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポート上でのデータ交換を許可します。

また、ステートフル アプリケーション検査により、検査中のプロトコルの過程で発行されたコマンドと応答の有効性を監査します。FWSM は攻撃を確実に防御するため、トラフィックが検査されるプロトコルごとに RFC 仕様に準拠しているかどうかチェックします。

表 6-1 に、検査マップ機能でサポートされているプロトコルの概要を示します。

表 6-1　検査マップ

DCERPC	DCERPC オプションで、DCERPC 検査マップを作成、表示、管理します。DCERPC は、Microsoft のクライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。
FTP	FTP オプションで、FTP 検査マップを作成、表示、管理します。インターネットなど、TCP/IP ネットワークを介してファイルを転送する通信プロトコルです。FTP マップを使用して、セキュリティ アプライアンスを通過したり FTP サーバに到達したりする FTP PUT などの、特定の FTP プロトコル方式をブロックできます。
GTP	GTP オプションで、GTP 検査マップを作成、表示、管理します。GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、セキュリティ アプライアンスを通過する GTP バージョンを制御できます。
H.225	H.225 オプションで、H.225 検査マップを作成、表示、管理します。H.225 は、H.323 接続でコントロールおよびセットアップの呼び出しに使用するプロトコルです。
HTTP	HTTP オプションで、HTTP 検査マップを作成、表示、管理します。HTTP はワールドワイド ウェブのクライアントとサーバ間の通信で使用されるプロトコルです。HTTP マップを使用して、RFC 準拠の HTTP ペイロード コンテンツ タイプを設定できます。また、特定の HTTP 方式をブロックし、一部のトンネル アプリケーションによる HTTP 転送を防止できます。
MGCP	MGCP オプションで、MGCP 検査マップを作成、表示、管理します。MGCP は、VoIP デバイスと MGCP コール エージェント間の接続を管理するためのプロトコルです。
SIP	SIP オプションで、SIP 検査マップを作成、表示、管理します。SIP は、VoIP 電話などのエンドポイントと SIP ゲートウェイまたはプロキシ サーバの間で VoIP 接続を確立するためのプロトコルです。
SNMP	SNMP オプションで、SNMP の検査マップを作成、表示、管理します。SNMP は、ネットワーク管理デバイスとネットワーク管理ステーション間の通信に利用されるプロトコルです。SNMP マップを使用して、SNMP v1、2、2c、3 など特定の SNMP バージョンをブロックできます。

DCERPC

DCERPC ペインで、DCERPC アプリケーションの事前に設定された検査マップを表示します。DCERPC マップでは、DCERPC アプリケーション検査のデフォルト設定値を変更できます。

DCERPC は、Microsoft のクライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

DCERPC 検査マップは、TCP のウェルノウン ポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。サーバの埋め込まれた IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポート番号で複数の接続を確立する可能性があるので、ピンホールを複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

フィールド

- Map Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Pinhole Timeout：DECRPC ピンホールのタイムアウト。デフォルト値は 2 分です。
- EPM Service：バインディング中にエンドポイント マッパー サービスの適用を強制するかどうかを一覧表示します。
- EPM Service Lookup : エンドポイント マッパー サービスのルックアップをイネーブルにするかどうかを一覧表示します。
- Add：Add DCERPC ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit DCERPC ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit DCERPC Map

Add/Edit DCERPC Map ダイアログボックスで、DCERPC のアプリケーション検査を制御する DCERPC マップを新規作成できます。

フィールド

- Name：DCERPC マップを追加する場合、DCERPC マップの名前を入力します。DCERPC マップを編集する場合、すでに設定されている DCERPC マップの名前が表示されます。
- Pinhole Timeout：ピンホール タイムアウトを設定します。クライアントが使用するサーバ情報は、複数の接続のエンドポイント マッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルト値は 2 分です。
- Enforce endpoint-mapper service：バインディング中はエンドポイント マッパー サービスの適用を強制します。
- Enable endpoint-mapper service lookup：エンドポイント マッパー サービスのルックアップをイネーブルにします。ディセーブルの場合、ピンホール タイムアウトが適用されます。
  - Enforce Service Lookup Timeout：指定されたサービス ルックアップのタイムアウトを適用します。

    Service Lookup Timeout：ルックアップでピンホールした場合のタイムアウトを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

FTP

FTP ペインで、FTP アプリケーションの事前に設定された検査マップを表示します。FTP マップでは、FTP アプリケーション検査のデフォルト設定値を変更できます。FTP ペインでは、新しい FTP マップを追加するか、または既存のマップを変更または削除できます。

フィールド

- Map　Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Mask reply to system command : クライアントが、クライアントからの FTP 要求を含む FTP システム コマンドへのサーバ応答を表示できないようにします。
- Denied Request Commands : 特定のアプリケーション検査マップで禁止されている FTP コマンドを一覧表示します。これらのコマンドを含む FTP 要求を受信すると、要求がドロップされます。
- Add：Add FTP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit FTP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit FTP Map

Add/Edit FTP Map ダイアログボックスで、FTP アプリケーションの検査マップを定義します。FTP マップでは、FTP アプリケーション検査のデフォルト設定値を変更できます。

フィールド

- FTP Map Name：アプリケーション検査マップの名前を定義します。
- Mask reply to system command : クライアントが、クライアントからの FTP 要求を含む FTP システム コマンドへのサーバ応答を表示できないようにします。
- Denied Request Commands
  - APPE：ファイルに追加するコマンドを禁止します。
  - CDUP：現在の作業ディレクトリの親ディレクトリに移動するコマンドを禁止します。
  - DELE：ファイルを削除するコマンドを禁止します。
  - GET：ファイルを取得するコマンドを禁止します。
  - HELP：ヘルプ情報を提供するコマンドを禁止します。
  - MKD：ディレクトリを作成するコマンドを禁止します。
  - PUT：ファイルを送信するコマンドを禁止します。
  - RMD：ディレクトリを削除するコマンドを禁止します。
  - RNFR：変更元ファイル名を指定するコマンドを禁止します。
  - RNTO：変更先ファイル名を指定するコマンドを禁止します。

- SITE：サーバ システム固有のコマンドを禁止します。通常、リモート管理に使用します。
- STOU：一意のファイル名を使用してファイルを保存するコマンドを禁止します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

GTP

GTP ペインで、GTP アプリケーションの事前に設定された検査マップを表示します。GTP マップでは、GTP アプリケーション検査のデフォルト設定値を変更できます。GTP ペインでは、新しい GTP マップを追加するか、または既存のマップを変更または削除できます。

（注） GTP 検査は、特別なライセンスがなければ使用できません。

フィールド

- GTP Map Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Description：GTP マップごとに説明をテキストで表示します。
- Fields：選択した GTP マップでイネーブルにするフィールドを個々に表示します。
- Values：選択した GTP マップでイネーブルにするフィールドごとの値を表示します。
- Add：Add GTP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit GTP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map > IMSI Prefix タブ

IMSI Prefix タブで、GTP 要求の中で使用できるように IMSI プレフィックスを定義します。

フィールド

- **GTP Map Name**：アプリケーション検査マップの名前を識別します。
- **Description**：アプリケーション検査マップの説明をテキストで入力します。
- **IMSI Prefix to Allow**
  - **Country Code**：0 以外の 3 桁の値でモバイル カントリ コードを定義します。1 桁または 2 桁の値を指定すると、先頭に 0 が付加されて 3 桁になります。
  - **Network Code**：2 桁または 3 桁の数字でネットワーク コードを定義します。
  - **Add**：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - **Delete**：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map > Bounds タブ

Bounds タブでは、GTP アプリケーション検査がイネーブルの場合、メッセージの長さ、キュー サイズ、トンネル数の許容範囲を定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- Message Length：許可される UDP ペイロードの、メッセージの長さのデフォルト最大値を変更できます。
- Minimum：UDP ペイロードの最小バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
- Maximum：UDP ペイロードの最大バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
- Queue Size：許容される要求キュー サイズのデフォルト最大値を変更できます。最大要求キュー サイズのデフォルト値は 200 です。
- Queue Size：キューで応答待ちができる GTP 要求数の最大値を指定します。1 ～ 9999999 の範囲で指定できます。
- Maximum Tunnels Count：許容されるトンネル数のデフォルト最大値を変更できます。デフォルトのトンネル制限値は 500 です。
- Maximum Tunnel Count：許容するトンネル数の最大値を指定します。グローバルなトンネル全体の制限値を 1 ～ 9999999 の範囲で指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map > Timeouts タブ

Timeouts タブでは、GTP アプリケーション検査がイネーブルの場合の、GSN、PDP コンテキスト、要求キュー、シグナリング、および GTP トンネルで許可される非アクティブ期間の最大値を定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- GSN：GSN を削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。
- GSN：タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
- PDP-Context：GTP セッションで PDP コンテキストを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。
- PDP Context：タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
- Request Queue：GTP セッション中に GTP メッセージを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 分です。
- Request Queue：タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
- Signaling：GTP シグナリングを削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。
- Signaling：タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
- Tunnel：GTP トンネルの非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 時間です。
- Tunnel：タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map > APN タブ

APN タブでは、GTP アプリケーション検査がイネーブルの場合にドロップするアクセスポイントを定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- Access Points to Drop
  - Name：ドロップするアクセスポイントの名前を指定します。デフォルトでは、有効な APN のメッセージをすべて検査します。すべての APN が指定できます。
  - Add：指定した APN を Access Point Name テーブルに追加します。
  - Delete：選択した APN を Access Point Name テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit GTP Map > Action タブ

Action タブでは、GTP アプリケーション検査がイネーブルの場合に実行する特定のアクションを定義できます。

フィールド

- GTP Map Name：アプリケーション検査マップの名前を識別します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- Permit packets with errors：無効なパケットまたは検査時にエラーが見つかったパケットを、ドロップしないで FWSM から送信します。デフォルトでは、無効なパケットや解析中に失敗したパケットはドロップされます。
- GTP Versions to Drop
  - GTP Version：ドロップするメッセージの GTP バージョンを指定します。有効な指定範囲は 0 ～ 255 です。0 は Version 0、1 は Version 1 を示します。GTP の Version 0 はポート 3386 を使用し、Version 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが対象です。
  - Add：指定した GTP バージョンを Version テーブルに追加します。
  - Delete：選択した GTP バージョンを Version テーブルから削除します。
- Message IDs to Drop
  - Message ID：ドロップするメッセージの数値識別子を指定します。有効な指定範囲は 1 ～ 255 です。デフォルトでは、すべての有効なメッセージ ID が対象です。
  - Add：指定した Message ID を Message ID テーブルに追加します。
  - Delete：選択した Message ID を Message ID テーブルから削除します。

- Permit Response：GSN プールにある GSN が SGSN 要求に応答して、GGSN のロードバランシングを達成できるようにします。無効な GTP パケットや解析中に失敗したパケットはドロップされます。
  - Object Groups to Add：別のオブジェクト グループから応答を受信できるオブジェクト グループを指定します。

    From Object Group：応答を送信するオブジェクト グループの名前を指定します。

    Browse：定義済みオブジェクト グループの一覧を参照します。

    To Object Group：要求を送信するオブジェクト グループの名前を指定します。

    Browse：定義済みオブジェクト グループの一覧を参照します。
  - Add：指定した Object Group を Object Group テーブルに追加します。
  - Delete：選択した Object Group を Object Group テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

H.225

H.225 ペインで、事前に設定された H.225 アプリケーションの検査マップ（H.225 マップ）を表示します。H.225 ペインでは、新しい H.225 マップを追加するか、または既存のマップを変更または削除できます。

H.225 マップでは、Cisco CallManager が HSI から取得した情報に基づいて H.323 エンドポイント間の接続を確立しようとすると、FWSM がポート固有のダイナミック ピンホールを開いて H.323 接続をイネーブルにすることができます。H.225 マップは HSI とその関連エンドポイントに関する情報を提供します。この情報は、FWSM で保護されているネットワークのセキュリティを侵害することなくこのような接続を確立するために必要です。

フィールド

- Name : すでに設定されている H.225 アプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- HSI Group ID：H.225 マップに関連付けられる HSI のグループ ID。

  HSI グループには、HSI とその関連エンドポイントが含まれています。H.225 マップ内の HSI グループの最大数は 5 です。
- IP Address：H.225 マップに関連付けられる IP アドレス。
- Endpoints：H.225 マップに関連付けられるエンドポイント。
- Add：Add H.225 Map ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit H.225 Map ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit H.225 Map

Add/Edit H.225 Map ダイアログボックスで、H.225 のアプリケーション検査を制御する H.225 マップを新規作成できます。

Cisco CallManager が HSI から取得した情報に基づいて H.323 エンドポイント間の接続を確立しようとしたときに、FWSM がポート固有の中継ピンホールを開いて H.323 接続をイネーブルにできるようにするには、H.225 マップが必要です。H.225 マップは HSI とその関連エンドポイントに関する情報を提供します。この情報は、FWSM で保護されているネットワークのセキュリティを侵害することなくこのような接続を確立するために必要です。

フィールド

- HSI Group ID：H.225 マップに関連付けられる HSI のグループ ID。

  HSI グループには、HSI とその関連エンドポイントが含まれています。H.225 マップ内の HSI グループの最大数は 5 です。
- IP Address：H.225 マップに関連付けられる IP アドレス。
- Endpoints：H.225 マップに関連付けられるエンドポイント。

  HSI に関連付けることができるエンドポイントの最大数は 10 です。
- Add：Add HSI Group ダイアログボックスが表示され、新規の HSI グループを定義できます。
- Edit：Edit HSI Group ダイアログボックスが表示され、HSI Group テーブルで選択した HSI グループを修正できます
- Delete：HSI Group テーブルで選択した HSI グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HSI Group

Add/Edit HSI Group ダイアログボックスで、Cisco CallManager が HSI から取得した情報に基づいて H.323 エンドポイント間の接続を確立しようとしたときに、H.323 接続をイネーブルにするための HSI グループを新規作成できます。

フィールド

- Group ID：H.225 マップに関連付けられる HSI のグループ ID。

  HSI グループには、HSI とその関連エンドポイントが含まれています。H.225 マップ内の HSI グループの最大数は 5 です。
- IP Address：HSI グループに関連付けられる IP アドレス。
- Endpoints：HSI グループ内のエンドポイントの最大数は 10 です。
  - IP Address：エンドポイントの IP アドレス。
  - Interface：エンドポイントに接続されるインターフェイス。
  - Add：HSI グループに関連付けられるエンドポイントを追加します。
  - Delete：エンドポイント テーブルで選択したエンドポイントを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

HTTP

HTTP ペインで、HTTP アプリケーションの事前に設定された検査マップを表示します。HTTP マップでは、HTTP アプリケーション検査のデフォルト設定値を変更できます。HTTP ペインでは、新しい HTTP マップを追加するか、または既存のマップを変更または削除できます。

フィールド

- Map Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Checks Enabled：選択した HTTP マップでイネーブルにする検証およびチェックを識別します。
- Add : Add HTTP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit : Edit HTTP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。
- Field：HTTP アプリケーション検査でサポートされる検査の種類を名前で一覧表示します。
- Enabled：特定の種類の検査がイネーブルかどうかを識別します。
- Value：RFC Compliance フィールドと Content Type フィールドがイネーブルの場合、これらのフィールドの値を表示します。
- Action：特定の種類のアプリケーション検査に応じて実行するアクションを識別します。
- Generate Syslog：特定の種類のアプリケーション検査に応じてシステム ログのエントリを生成するかどうかを指定します。
- Edit：Edit HTTP ダイアログボックスが表示され、選択したフィールドを修正できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map > General タブ

General タブでは、コンテンツ タイプの検査をイネーブルにするために、準拠していない HTTP 要求を受信した場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- Description：アプリケーション検査マップの説明をテキストで入力します。
- RFC Compliance
  - Action：FWSM が RFC 2616 に準拠しないトラフィックを受信した場合に実行するアクションを指定します。RFC 2616 では、許可される HTTP 方式とサポートされる拡張方式が定義されています。次のアクションを実行できます。

    Allow Packet：パケットが準拠していない方式を使用していても、FWSM はそのパケットを通過させます。

    Drop Packet：FWSM は準拠していない方式を使用するパケットを破棄します。

    Reset Connection：FWSM が準拠していない方式を使用するパケットを受信すると、TCP 接続をリセットします。
  - Generate Syslog：FWSM が準拠していない方式を使用するパケットを受信すると、システム ログ メッセージを生成します。
- コンテンツ タイプの検証
  - Verify Content-type field belongs to the supported internal content-type：HTTP 応答内のコンテンツ タイプのフィールドと、サポートされるコンテンツ タイプの事前設定リストの比較に基づいて、コンテンツ検証をイネーブルにします。イネーブルの場合、FWSM は HTML メッセージの本文とコンテンツ タイプが一致するかどうかも検証します。要求で受信したタイプが応答で送信したコンテンツ タイプと一致するかどうかを検証します。サポートされるコンテンツ タイプは次のとおりです。

audio/* |	audio/basic |	application/x-msn-messenger
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-java-xm	application/x-gzip
image |	image/cgf |	application/zip
image/jpeg |	image/png |	image/gif |
image/x-3ds |	image/x-bitmap |	image/tiff |
image/x-portable-bitmap |	image/x-portable-greymap |	image/x-niff |
text/* |	text/css	image/x-xpm |
text/plain |	text/richtext |	text/html |
text/xmcd	text/xml	text/sgml

video/-flc	video/mpeg	video/*
video/sgi	video/x-avi	video/quicktime
video/x-mng	video/x-msvideo	video/x-fli

- Verify Content-type field for response matches the Accept field of request：HTTP 応答内のコンテンツ タイプのフィールドと、HTTP 要求内の Accept フィールドで指定されているタイプの比較に基づいて、コンテンツ検証をイネーブルにします。
- Action：コンテンツ検証がイネーブルの場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：コンテンツ検証に失敗した場合でも、FWSM は HTTP 要求を許可します。

  Drop Packet：FWSM がコンテンツ検証に失敗したパケットを破棄します。

  Reset Connection：FWSM がコンテンツ検証に失敗したパケットを受信すると、TCP 接続をリセットします。
- Generate Syslog：FWSM がコンテンツ検証に失敗したパケットを受信すると、システム ログ メッセージを生成します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map > Entity Length タブ

Entity Length タブでは、URI、HTTP ヘッダー、および HTTP 本文で許可される長さを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- URI の最大長
  - Inspect URI Length：FWSM が HTTP 要求の URI 長を検査します。
  - Maximum bytes：HTTP 要求で URI 長に許可される最大バイト数を指定します。許容範囲は 1 ～ 65535 です。
  - Action：URL の長さの検査に失敗した場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：HTTP 要求に許可されている最大長を超える URI が含まれていても、FWSM はその HTTP 要求を許可します。

    Drop Packet：HTTP 要求に許可されている最大長を超える URI が含まれている場合、FWSM はその HTTP 要求をドロップします。

    Reset Connection：許可されている最大長を超える URI が含まれている HTTP 要求を受信すると、FWSM は TCP 接続をリセットします。
  - Generate Syslog：FWSM が許可されている最大長を超える URI が含まれている HTTP 要求を受信すると、システム ログ メッセージを生成します。
- ヘッダーの最大長
  - Inspect Maximum Header Length：FWSM が HTTP 要求または応答にあるヘッダー長を検査します。
  - Request bytes：HTTP 要求でヘッダー長として許可される最大バイト数を指定します。許容範囲は 1 ～ 65535 です。

- Response bytes：HTTP 応答でヘッダー長として許可される最大バイト数を指定します。許容範囲は 1 ～ 65535 です。
- Action：HTTP ヘッダー長の検査に失敗した場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：HTTP 要求に許可されている最大長を超えるヘッダーが含まれていても、FWSM はその HTTP 要求を許可します。

  Drop Packet：HTTP 要求に許可されている最大長を超えるヘッダーが含まれている場合、FWSM はその HTTP 要求をドロップします。

  Reset Connection：許可されている最大長を超えるヘッダーが含まれている HTTP 要求を受信すると、FWSM は TCP 接続をリセットします。
- Generate Syslog：許可されている最大長を超えるヘッダーが含まれている HTTP 要求を受信すると、FWSM はシステム ログ メッセージを生成します。

• 本文の長さ
- Inspect Body Length：FWSM が HTTP 要求の本文の長さを検査します。
- Maximum bytes : HTTP メッセージで本文の長さとして許可される最小バイト数を指定します。許容範囲は 1 ～ 65535 です。
- Maximum bytes : HTTP メッセージで本文の長さとして許可される最大バイト数を指定します。許容範囲は 1 ～ 50000000 です。
- Action：HTTP 本文の長さの検査に失敗した場合に FWSM が実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：メッセージの本文が最大長よりも長い、または最小長よりも短い場合でも、FWSM はその HTTP 要求を許可します。

  Drop Packet : メッセージの本文が最大長よりも長い、または最小長よりも短い場合、FWSM はその HTTP 要求をドロップします。

  Reset Connection：メッセージの本文が最大長よりも長い、または最小長よりも短い場合、FWSM は TCP 接続をリセットします。
- Generate Syslog：メッセージの本文が最大長よりも長い、または最小長よりも短い場合、FWSM はシステム ログ メッセージを生成します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map > RFC Request Method タブ

RFC Request Method タブでは、HTTP 要求で特定の要求方式を使用するときに実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- 方式固有のアクション
  - Method to be Added : FWSM が異なる方式を使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に使用可能な方式を一覧表示します。
  - Add：選択したアクションを実行する方式を、指定した方式のテーブルに追加します。

- Remove：選択した方式を、指定した方式のテーブルから削除します。
- Action：選択した要求方式に対するアクションを指定します。選択した方式を含む HTTP メッセージを FWSM が受信すると、このアクションが実行されます。選択した方式ごとにアクションを指定できます。次のアクションを実行できます。

  Allow Packet：FWSM が HTTP 要求を許可します。

  Drop Packet：FWSM が HTTP 要求をドロップします。

  Reset Connection：FWSM が TCP 接続をリセットします。
- Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

• デフォルトのアクション
- Action：指定した方式のテーブルに含まれていない方式を含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

  Allow Packet：FWSM が HTTP 要求を許可します。

  Drop Packet：FWSM が HTTP 要求をドロップします。

  Reset Connection：FWSM が TCP 接続をリセットします。
- Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map > Extension Request Method タブ

Extension Request Method タブでは、HTTP 要求で特定の拡張方式を使用する場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- 方式固有のアクション
  - Method to be Added：FWSM が異なる方式を使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に使用可能な方式を一覧表示します。
  - Add：選択したアクションを実行する方式を、指定した方式のテーブルに追加します。
  - Remove：選択した方式を、指定した方式のテーブルから削除します。
  - Action：選択した要求方式に対するアクションを指定します。選択した方式を含む HTTP メッセージを FWSM が受信すると、このアクションが実行されます。選択した方式ごとにアクションを指定できます。次のアクションを実行できます。

    Allow Packet：FWSM が HTTP 要求を許可します。

    Drop Packet：FWSM が HTTP 要求をドロップします。

    Reset Connection：FWSM が TCP 接続をリセットします。

- Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

- デフォルトのアクション
  - Action：指定した方式のテーブルに含まれていない方式を含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定した方式のテーブルに含まれない方式を含む HTTP 要求を FWSM が許可します。

    Drop Packet：指定した方式のテーブルに含まれない方式を含む HTTP 要求を FWSM がドロップします。

    Reset Connection：指定した方式のテーブルに含まれない方式が HTTP メッセージに含まれている場合、FWSM が TCP 接続をリセットします。
  - Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択した方式を含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択した方式ごとに異なるオプションを指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map > Application Category タブ

Application Category タブでは、HTTP 要求に特定のアプリケーション タイプが含まれている場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- カテゴリ固有のアクション
  - Category to be Added：FWSM が、異なるアプリケーション カテゴリを使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に、使用可能なアプリケーション カテゴリを一覧表示します。
  - Add：選択したアクションを実行するアプリケーション カテゴリを、指定したカテゴリのテーブルに追加します。
  - Remove：選択したアプリケーション　カテゴリを、指定したカテゴリのテーブルから削除します。
  - Action：選択したアプリケーション カテゴリに対するアクションを指定します。選択したアプリケーション カテゴリを含む HTTP メッセージを FWSM が受信すると、このアクションが実行されます。選択したアプリケーション カテゴリごとに異なるアクションを指定できます。次のアクションを実行できます。

    Allow Packet：FWSM が HTTP 要求を許可します。

    Drop Packet：FWSM が HTTP 要求をドロップします。

    Reset Connection：FWSM が TCP 接続をリセットします。
  - Generate Syslog：FWSM がシステム ログ メッセージを生成します。選択したアプリケーション カテゴリを含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択したアプリケーション カテゴリごとに異なるオプションを指定できます。

- デフォルトのアクション
  - Action：指定したカテゴリのテーブルに含まれていないアプリケーション カテゴリを含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定したカテゴリのテーブルに含まれないアプリケーション カテゴリを含む HTTP 要求を FWSM が許可します。

    Drop Packet : 指定したカテゴリのテーブルに含まれないアプリケーション カテゴリを含む HTTP 要求を FWSM がドロップします。

    Reset Connection : 指定したカテゴリのテーブルに含まれないアプリケーション カテゴリが HTTP メッセージに含まれている場合、FWSM が TCP 接続をリセットします。
  - Generate Syslog : FWSM がシステム ログ メッセージを生成します。選択したアプリケーション カテゴリを含む HTTP 要求を FWSM が受信すると、このシステム ログ メッセージが生成されます。選択したアプリケーション カテゴリごとに異なるオプションを指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Map > Transfer-Encoding タブ

Transfer-Encoding タブでは、HTTP 要求で特定の転送符号化のタイプが使用されている場合に実行するアクションを定義できます。

フィールド

- HTTP Map Name：アプリケーション検査マップの名前を定義します。
- 符号化のタイプに固有のアクション
  - Encoding-type to be Added : FWSM が異なる符号化のタイプを使用する HTTP 要求ごとに異なるアクションを実行するよう指定したい場合に使用可能な符号化のタイプを一覧表示します。
  - Add：選択した転送符号化のタイプを、指定した転送符号化のタイプのテーブルに追加します。
  - Remove : 選択した転送符号化のタイプを、指定した転送符号化のタイプのテーブルから削除します。
  - Action：指定した転送符号化のタイプのテーブルにある転送符号化のタイプを含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定した転送符号化のタイプのテーブルにある転送符号化のタイプを含む HTTP 要求を FWSM が許可します。

    Drop Packet：指定した転送符号化のタイプのテーブルにある転送符号化のタイプが HTTP 要求に含まれる場合、FWSM はその HTTP 要求をドロップします。

    Reset Connection：指定した転送符号化のタイプのテーブルにある転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM は TCP 接続をリセットします。
  - Generate Syslog：指定した転送符号化のタイプのテーブルにある転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM はシステム ログ メッセージを生成します。

- デフォルトのアクション
  - Action：指定した転送符号化のタイプのテーブルに含まれないが、サポートされている転送符号化のタイプを含む HTTP 要求を FWSM が受信した場合に実行するアクションを指定します。次のアクションを実行できます。

    Allow Packet：指定した転送符号化のタイプのテーブルに含まれていない転送符号化のタイプを含む HTTP 要求を FWSM が許可します。

    Drop Packet：指定した転送符号化のタイプのテーブルに含まれない転送符号化のタイプを含む HTTP 要求を FWSM がドロップします。

    Reset Connection：指定した転送符号化のタイプのテーブルに含まれない転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM は TCP 接続をリセットします。
  - Generate Syslog：指定した転送符号化のタイプのテーブルに含まれていない転送符号化のタイプが HTTP メッセージに含まれる場合、FWSM はシステム ログ メッセージを生成します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MGCP

MGCP ペインで、MGCP アプリケーションの事前に設定された検査マップを表示します。MGCP マップでは、MGCP アプリケーション検査のデフォルト設定値を変更できます。MGCP ペインでは、新しい MGCP マップを追加するか、または既存のマップを変更または削除できます。

フィールド

- Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Command Queue Size：MGCP コマンドの許容キュー サイズを指定します。
- Group ID：コール エージェント グループの ID を識別します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。0 ～ 2147483647 の範囲の値を指定できます。
- Gateways：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- Call Agents：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- Add：Add MGCP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit MGCP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MGCP Map の追加および編集

メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素を使用してメディア ゲートウェイを制御するには、MGCP を使用します。MGCP マップ グループ テーブルには、現在の MGCP アプリケーション検査マップに設定されているグループが一覧表示されます。既存のグループを編集するには、グループを選択してから **Edit** をクリックします。このテーブルには、次のカラムがあります。

フィールド

- MGCP Map Name：アプリケーション検査マップの名前を定義します。
- Command Queue Size：キューに入れるコマンドの最大数を指定します。1 ～ 2147483647 の範囲の値を指定できます。
- Group ID：0 ～ 2147483647 までのコール エージェント グループの ID が一覧表示されます。
- Gateways：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスが一覧表示されます。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- Call Agents：関連付けられた MGCP ゲートウェイを制御するメディア ゲートウェイ コントローラ（コール エージェント）の IP アドレスを一覧表示します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- Add：Add MGCP Group ダイアログボックスを表示します。このダイアログボックスで新しい MGCP グループを追加できます。
- Edit：Edit MGCP Group ダイアログボックスを表示します。このダイアログボックスで既存の MGCP グループのコンフィギュレーションを変更できます。
- Delete：選択した MGCP グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit MGCP Group

Add/Edit MGCP Group ダイアログボックスで、MGCP アプリケーション検査がイネーブルのときに使用される MGCP グループのコンフィギュレーションを定義します。

フィールド

- Group ID：コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。
- ゲートウェイ
  - Gateway to Be Added：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを指定します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - Add：指定した IP アドレスを IP アドレス テーブルに追加します。
  - Delete：選択した IP アドレスを IP アドレス テーブルから削除します。
  - IP Address：コール エージェント グループに設定されているゲートウェイの IP アドレスを一覧表示します。
- コール エージェント
  - Call Agent to Be Added：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを指定します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
  - Add：指定した IP アドレスを IP アドレス テーブルに追加します。
  - Delete：選択した IP アドレスを IP アドレス テーブルから削除します。
  - IP Address：コール エージェント グループに設定されているコール エージェントの IP アドレスを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SIP

SIP ペインで、SIP アプリケーションの事前に設定された検査マップを表示します。SIP マップでは、SIP アプリケーション検査に対する IP アドレス プライバシーをイネーブルにできます。SIP ペインでは、新しい SIP マップを追加するか、または既存のマップを変更または削除できます。

IP アドレスのプライバシーがイネーブルの場合、1 つの IP 電話コールまたはインスタント メッセージ セッションに参加している 2 つの SIP エンドポイントが、同じ内部ファイアウォール インターフェイスを使用して外部ファイアウォール インターフェイスの SIP プロキシ サーバに接続している場合、SIP シグナリング メッセージはすべて SIP プロキシ サーバを通過します。

TCP または UDP 経由の SIP アプリケーション検査がイネーブルの場合に、IP アドレス プライバシーをイネーブルにできます。デフォルトでは、この機能はディセーブルになっています。IP アドレス プライバシーがイネーブルの場合、FWSM は、着信 SIP トラフィックの TCP または UDP ペイロードに組み込まれた内部および外部のホスト IP アドレスを変換しません。これらの IP アドレスの変換ルールは無視されます。

フィールド

- Name : すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- IP Address : IP アドレス プライバシーがイネーブルかどうかを示します。
- Add : Add SIP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit : Edit SIP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete : アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SIP Map

Add/Edit SIP Map ダイアログボックスでは、新しい SIP マップの作成、または既存のマップの修正ができます。IP アドレス プライバシーはデフォルトでディセーブルになっているので、イネーブルにするには SIP マップが必要です。

IP アドレスのプライバシーがイネーブルの場合、1 つの IP 電話コールまたはインスタント メッセージ セッションに参加している 2 つの SIP エンドポイントが、同じ内部ファイアウォール インターフェイスを使用して外部ファイアウォール インターフェイスの SIP プロキシ サーバに接続している場合、SIP シグナリング メッセージはすべて SIP プロキシ サーバを通過します。

TCP または UDP 経由の SIP アプリケーション検査がイネーブルの場合に、IP アドレス プライバシーをイネーブルにできます。デフォルトでは、この機能はディセーブルになっています。IP アドレス プライバシーがイネーブルの場合、FWSM は、着信 SIP トラフィックの TCP または UDP ペイロードに組み込まれた内部および外部のホスト IP アドレスを変換しません。これらの IP アドレスの変換ルールは無視されます。

フィールド

- SIP Map Name：アプリケーション検査マップの名前を定義します。
- IP Address Privacy：IP アドレス プライバシーをイネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP

SNMP ペインで、SNMP アプリケーションの事前に設定された検査マップを表示します。SNMP マップでは、SNMP アプリケーション検査のデフォルト設定値を変更できます。SNMP ペインでは、新しい SNMP マップを追加するか、または既存のマップを変更または削除できます。

フィールド

- Map Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップを選択して Edit をクリックすると、既存のマップの表示または変更ができます。
- Disallowed SNMP Versions：特定の SNMP アプリケーション検査マップで拒否される SNMP バージョンを識別します。
- Add：Add SNMP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit SNMP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SNMP Map

Add/Edit SNMP Map ダイアログボックスで、SNMP のアプリケーション検査を制御する SNMP マップを新規作成できます。

フィールド

- SNMP Map Name：アプリケーション検査マップの名前を定義します。
- SNMP version 1：SNMP バージョン 1 のアプリケーション検査をイネーブルにします。
- SNMP version 2 (party based)：SNMP バージョン 2 のアプリケーション検査をイネーブルにします。
- SNMP version 2c (community based)：SNMP バージョン 2c のアプリケーション検査をイネーブルにします。
- SNMP version 3：SNMP バージョン 3 のアプリケーション検査をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

グローバル プールの設定

グローバル プールの詳細については、P.21-6 の「ダイナミック NAT」を参照してください。

時間範囲の設定

Time Ranges オプションで開始時間と終了時間を定義する再利用コンポーネントを作成し、さまざまなセキュリティ機能に適用します。時間範囲を 1 回だけ定義すれば、後は時間範囲を選択して、スケジューリングが必要なさまざまなオプションに適用できます。

時間範囲機能を使用して時間の範囲を定義し、トラフィックのルールやアクションに使用できます。たとえば、アクセスリストを時間範囲に添付して、FWSM へのアクセスを制限できます。

時間範囲は、開始時間、終了時間、および繰り返し時間範囲エントリ（オプション）で構成されます。

（注）　時間範囲を作成しても、デバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- Name：時間範囲の名前を指定します。
- Start Time：時間範囲の始まる時期を指定します。
- End Time：時間範囲が終了する時期を指定します。
- Recurring Entries：指定した開始時刻と停止時刻の範囲内でアクティブな時間の追加制限を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Time Range

Add/Edit Time Range ペインで特定の日付と時刻を定義し、アクションに設定できます。たとえば、アクセスリストを時間範囲に添付して、FWSM へのアクセスを制限できます。時間範囲は FWSM のシステム クロックに依存します。ただし、最適に動作するのは NPT 同期を適用した場合です。

（注） 時間範囲を作成しても、デバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- Time Range Name：時間範囲の名前を指定します。スペースや引用符は使用できません。また、先頭にはアルファベットか数字を使用します。
- Start now/Started：時間範囲がただちに開始するか、または時間範囲がすでに始まっているかを指定します。このボタンのラベルは、追加 / 編集する時間範囲の設定状態によって変わります。時間範囲を新規追加する場合または固定の開始時間が定義された時間範囲を編集する場合、ボタンは「Start Now」になります。開始時間が非固定の時間範囲を編集する場合は、ボタンが「Started」になります。
- Start at：時間範囲の開始時刻を指定します。
  - Month：月を 1 月～ 12 月の範囲で指定します。
  - Day：日を 01 ～ 31 の範囲で指定します。
  - Year：年を 1993 ～ 2035 の範囲で指定します。
  - Hour：時間を 00 ～ 23 の範囲で指定します。
  - Minute：分を 00 ～ 59 の範囲で指定します。
- Never end：時間範囲が終了しない場合に指定します。
- End at (inclusive)：時間範囲の終了時刻を指定します。指定した終了時刻も範囲に含まれます。たとえば、指定した時間範囲が 11:30 で終了する場合、11 時 30 分 59 秒まで有効です。この場合、時間範囲は 11:31 になったとき終了します。
  - Month：月を 1 月～ 12 月の範囲で指定します。
  - Day：日を 01 ～ 31 の範囲で指定します。
  - Year：年を 1993 ～ 2035 の範囲で指定します。
  - Hour：時間を 00 ～ 23 の範囲で指定します。
  - Minute：分を 00 ～ 59 の範囲で指定します。
- Recurring Time Ranges：時間範囲を日単位または週単位で設定します。
  - Add：繰り返し時間範囲を追加します。
  - Edit：選択した繰り返し時間範囲を編集します。
  - Delete：選択した繰り返し時間範囲を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Recurring Time Range

Add/Edit Recurring Time Range ペインで時間範囲を詳細に指定し、日単位または週単位の設定を行います。

（注）　時間範囲を作成しても、デバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- Days of the week
  - Every day：週の毎日を指定します。
  - Weekdays：月曜日～金曜日を指定します。
  - Weekends：土曜日と日曜日を指定します。
  - On these days of the week：特定の曜日を指定します。
  - Daily Start Time：時間範囲が開始する時間と分を指定します。
  - Daily End Time (inclusive) エリア：時間範囲が終了する時間と分を指定します。指定した終了時刻も範囲に含まれます。
- Weekly Interval
  - From：月曜日～日曜日までの曜日を一覧表示します。
  - Through：月曜日～日曜日までの曜日を一覧表示します。
  - Hour：時間を 00 ～ 23 まで一覧表示します。
  - Minute：分を 00 ～ 59 まで一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—