H3C Firewall 製品
セキュリティポリシーの設定例

New H3C Technologies Co., Ltd.
http://www.h3c.com

ソフトウェアバージョン:Release 1118、Release 1118P07
文書バージョン: 6W101-20180821

商標

H3C,  ,H3CS,H3CIE,H3CNE,Aolynk,  ,H³Care,  ,IRF,NetPilot,Netflow,SecEngine,
SecPath,SecCenter,SecBlade,Comware,ITCMM および HUASAN は,New H3C Technologies Co.,Ltd.の商標です。

その他のすべての商標は、各所有権者の財産です。

注意

このドキュメントの情報は、予告なく変更されることがあります。このドキュメントのすべての内容(説明、情報、推奨事項を含む)は正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提示されます。H3C は、このドキュメントに含まれる技術的または編集上の誤りや脱落について責任を負いません。

はじめに

このコンフィギュレーションガイドでは、スイッチの導入に役立つ次の機能と作業について説明します。

この Web 構成ガイドでは、H3C ファイアウォール製品のソフトウェア機能について説明し、これらの機能の Web 構成例を示します。

この序文には、ドキュメントに関する次のトピックが含まれています。

- 対象者
- 表記法
- 文書のフィードバック

対象者

このマニュアルの対象者:

- ネットワークプランナー。
- フィールドテクニカルサポート/サービスエンジニア
- ネットワーク管理者

表記法

ここでは、マニュアルで使用されている表記法について説明します。

コマンドの表記法

規約	説明
太字	**太字のテキストは、文字どおりに入力したコマンドとキーワードを示します。**
イタリック体	*斜体のテキストは、実際の値に置き換える引数を表します。*
[]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x | y | ... }	中カッコは、必要な構文の選択肢を縦棒で区切って囲みます。この中から1つを選択します。
[x | y | ...]	角カッコは、オプションの構文選択のセットを縦棒で区切って囲みます。この中から1つまたは何も選択しません。
{ x | y | ... } *	アスタリスクの付いた中括弧は、必須構文の選択肢を縦棒で区切って囲みます。この中から少なくとも1つを選択します。
[x | y | ...] *	アスタリスクの付いた角括弧は、オプションの構文選択肢を縦棒で区切って囲みます。選択肢は1つ、複数、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	シャープ記号(#)で始まる行はコメントです。

GUI のルール

規約	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニューアイテムは太字で表示されます。たとえば、New Userウィンドウが開き、OKをクリックします。
>	マルチレベルメニューは、 File Create > Folderのように、山かっこで区切られています。

シンボル

規約	説明
⚠警告!	重要な情報を理解していない場合や、その情報に従っていない場合に、けがをするおそれがある場合に注意を促す警告。
△注意:	重要な情報が理解されていない場合、または情報が理解されていない場合に、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性がある場合に、注意を促す警告。
ⓘ重要:	重要な情報への注意を喚起するアラート。
注:	追加情報または補足情報を含むアラート。
ヒント:	役立つ情報を提供するアラート。

ネットワークトポロジーアイコン

規約	説明
	ルーター、スイッチ、ファイアーウォールなどの汎用ネットワークデバイスを表します。
	ルーターまたはレイヤー3スイッチなどのルーティング対応デバイスを表します。
	レイヤー2スイッチやレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2および他のレイヤー2機能をサポートするルーターを表します。
	アクセスコントローラー、Unified Wired-WLANモジュール、またはUnified Wired-WLANスイッチ上のアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向信号を表します。
	指向性信号を表します。
	ファイアーウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。
	ファイアーウォール、ロードバランシング、NetStream、SSL VPN、IPS、またはACGモジュールなどのセキュリティモジュールを表します。

本書に記載されている例

このドキュメントの例では、ハードウェアモデル、設定、またはソフトウェアバージョンがデバイスと異なるデバイスを使用している場合があります。通常、例のポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイスの内容とは異なります。

文書のフィードバック

製品マニュアルに関するコメントは、info@h3c.com まで電子メールでお送りください。

ご意見をお寄せください。

内容

セキュリティポリシーの設定例

はじめに

次に、セキュリティポリシーの設定例を示します。

前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、セキュリティポリシー機能に関する基本的な知識があることを前提としています。

制限事項とガイドライン

パケットフィルタリング(設定されている場合)は、どのセキュリティポリシールールにも一致しないパケットに対してのみ実行されます。ベストプラクティスとして、セキュリティポリシーには、パケットフィルタリングよりも厳しいフィルタリング基準が設定されていることを確認してください。これにより、一致しないパケットはパケットフィルタリングによってフィルタリングできます。

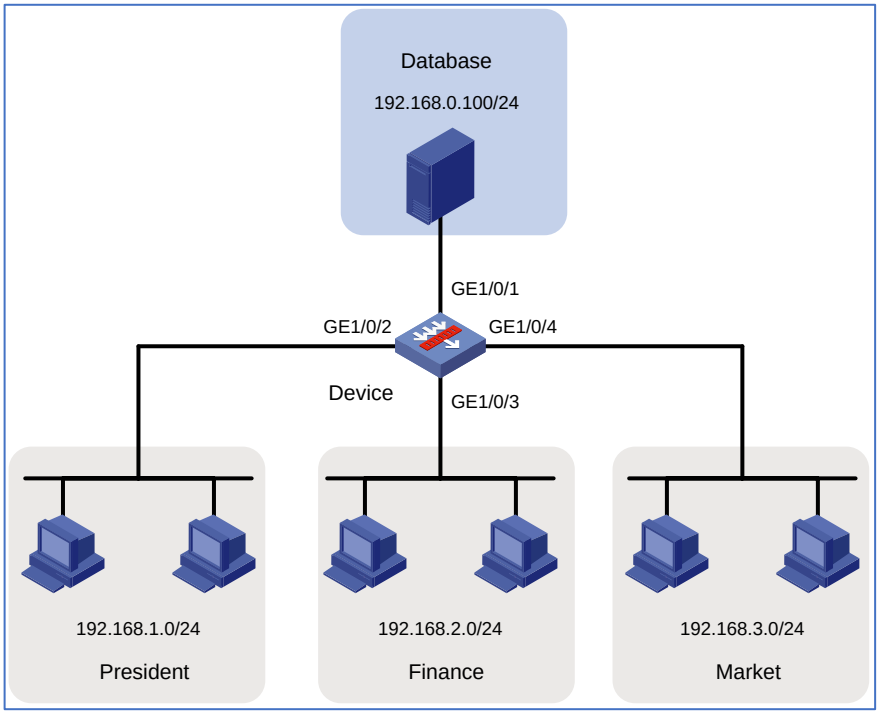
例:基本セキュリティポリシーの設定

ネットワーク構成

図 1 に示すように、次の目標を達成するようにセキュリティポリシーを設定します。

- **President** オフィスは、HTTP を通じていつでも **financial** データベースサーバーにアクセスできる。
- **financial** オフィスは、平日の 8:00～18:00 に HTTP 経由で **financial** データベースサーバーにアクセスできます。
- **marketing** オフィスは、HTTP を介して **financial** データベースサーバーにいつでもアクセスできません。

図1 ネットワーク図



使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

   #トップナビゲーションバーで、**Network** をクリックします。

   #ナビゲーションペインで **Interface Configuration > Interfaces** を選択します。

   #GE1/0/1 の **Edit** アイコンをクリックします。

   #開いたダイアログボックスで、インターフェイスを設定します。

   A) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、192.168.0.1/24と入力します。

   B) **Ok**をクリックします。

   #GE1/0/2、GE1/0/3、GE1/0/4の//3、GE1/0/4のIPアドレスをそれぞれ192.168.1.1/24、192.168.2.1/24、192.168.3.1/24に設定します。

2. セキュリティゾーンを作成します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Security Zones** を選択します。

#次のタスクを実行します。

- **database** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/1 を追加します。
- **president** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/2 を追加します。
- **finance** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/3 を追加します。
- **market** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/4 を追加します。

3. 時間範囲を作成します。

#トップナビゲーションバーで、**Object** をクリックします。

#ナビゲーションペインで、**Object Groups > Time Ranges** を選択します。

#**Create** をクリックします。

#表示されるダイアログボックスで、名前 **work** と入力し、**Periodic time range** の **Create** をクリックします。

#表示されるダイアログボックスで、時間範囲を設定します。

- 開始時刻を **08:00** に設定します。
- 終了時刻を **18:00** に設定します。
- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、および **Friday** を選択し

#**OK** をクリックします。

4. IPv4アドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、object をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#次のタスクを実行します。

- IPv4 アドレスオブジェクトグループ **database** を作成し、サブネットアドレスが 192.168.0.0/24 の IPv4 アドレスオブジェクトをグループに設定します。

- IPv4 アドレスオブジェクトグループの **president** を作成し、サブネットアドレス 192.168.1.0/24 の IPv4 アドレスオブジェクトをグループに設定します。
- IPv4 アドレスオブジェクトグループ **finance** を作成し、サブネットアドレス 192.168.2.0/24 の IPv4 アドレスオブジェクトをグループに設定します。
- IPv4 アドレスオブジェクトグループ **market** を作成し、サブネットアドレス 192.168.3.0/24 の IPv4 アドレスオブジェクトをグループに設定します。

5. サービスオブジェクトグループを作成します。

   #トップナビゲーションバーで、**object** をクリックします。

   #ナビゲーションペインで、**Object Groups > Service Object Groups** を選択します。

   #**create** をクリックします。

   #開いたダイアログボックスで、サービスオブジェクトグループを設定します。

   A) グループ名を入力します。この例では、**web**と入力します。

   B) **add**をクリックします。

   C) 表示されるダイアログボックスで、オブジェクトグループ**http**を選択します。

   D) **ok**をクリックします。

6. セキュリティゾーン **president** からセキュリティゾーン **database** へのセキュリティポリシーを作成し、president オフィスがいつでも HTTP を介してデータベースにアクセスできるようにします。

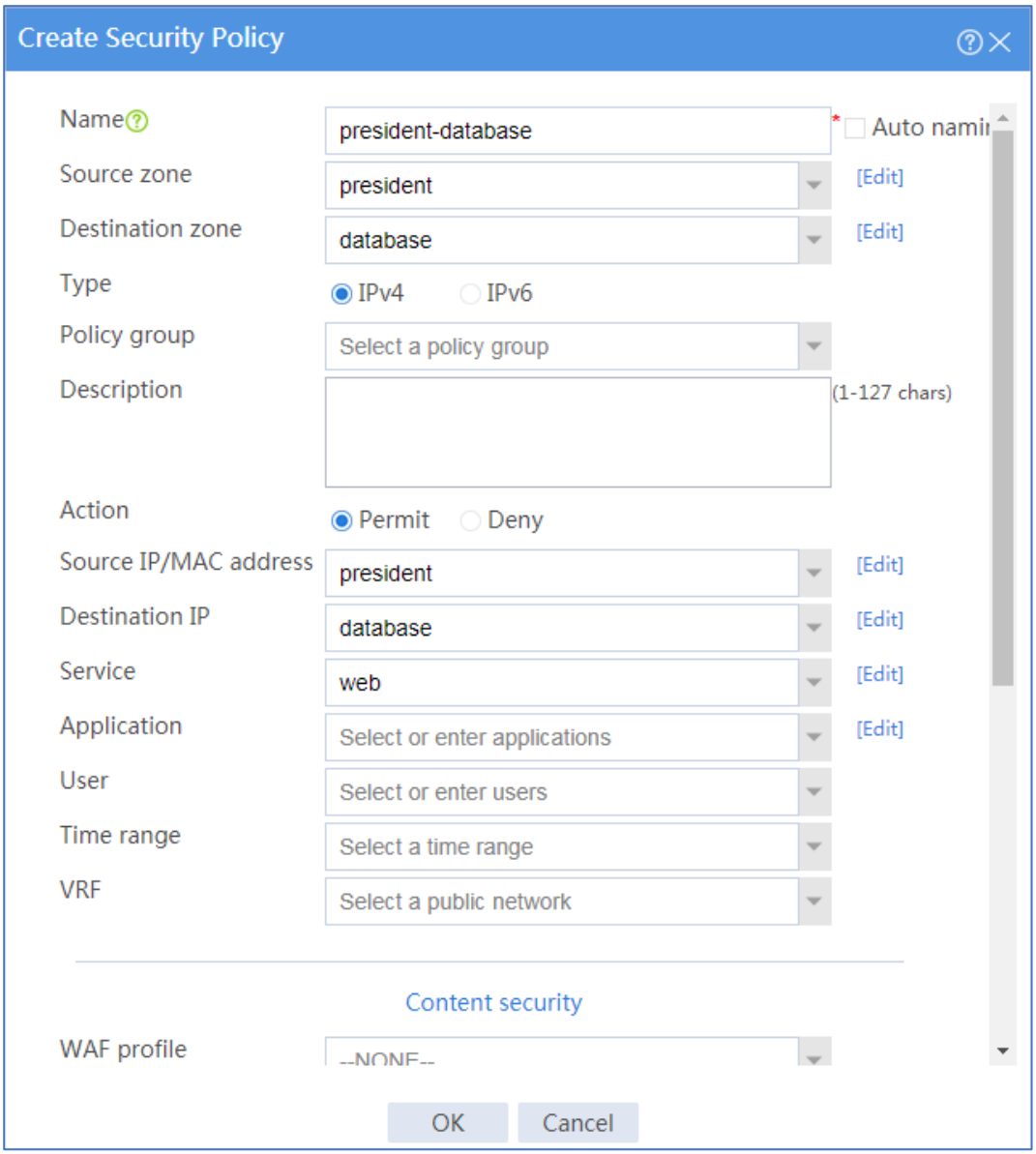
   #トップナビゲーションバーで、**Policies** をクリックします。

   #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

   #**create** をクリックします。

   #開いたダイアログボックスで、図 2 に示すセキュリティポリシーを作成します。

図2 presidentオフィスのセキュリティポリシーを作成する



#**OK** をクリックします。

7. セキュリティゾーン **finance** からセキュリティゾーン **database** へのセキュリティポリシーを作成し、平日の 8:00 から 18:00 まで、財務オフィスが HTTP を介してデータベースにアクセスできるようにします。

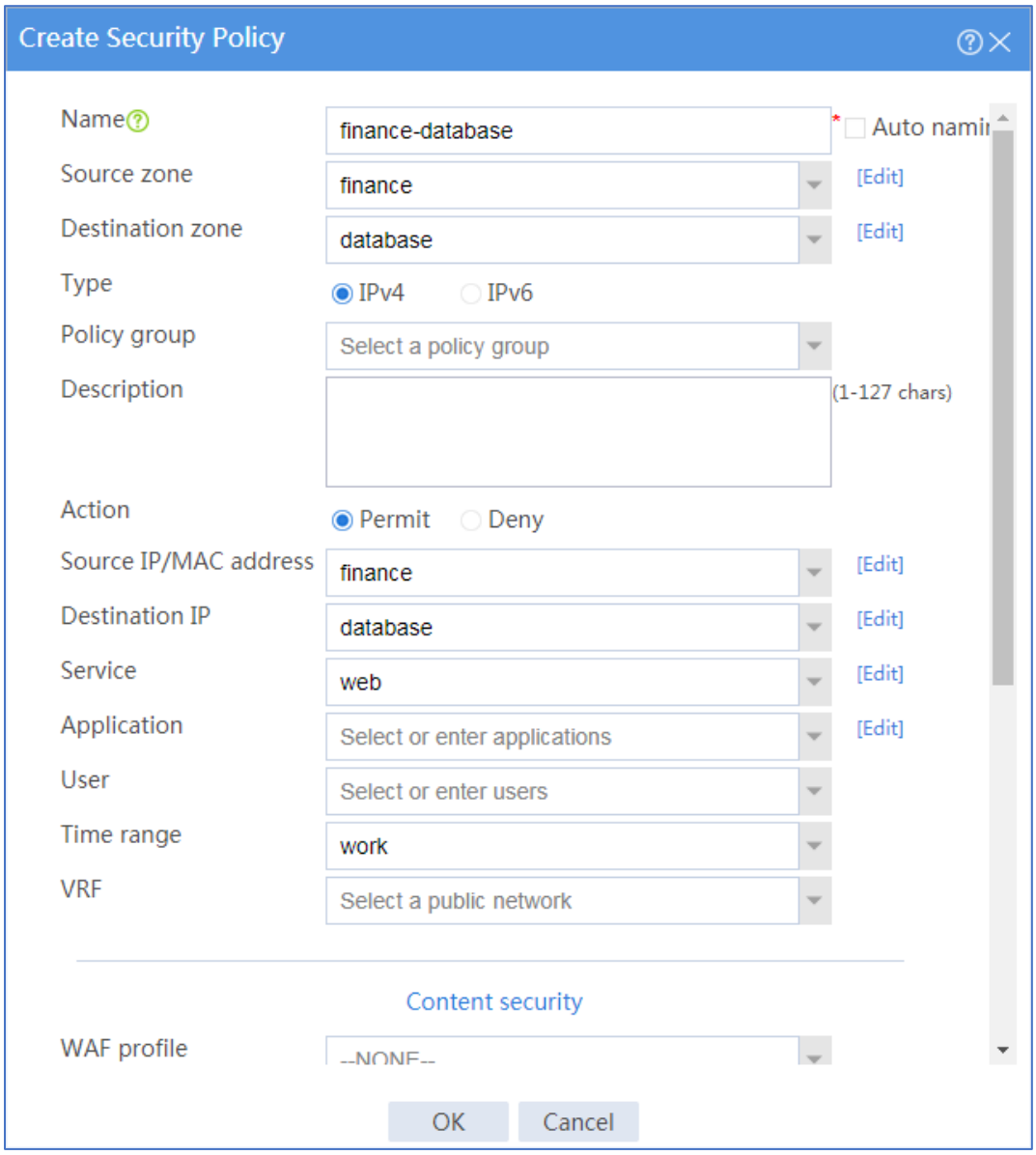
#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、図 3 に示すセキュリティポリシーを作成します。

図3 financeオフィスのセキュリティポリシーを作成する



#**OK** をクリックします。

8. セキュリティゾーン **market** からセキュリティゾーン **database** のセキュリティポリシーを作成し、**marketing** オフィスがいつでも HTTP を介してデータベースにアクセスできないようにします。

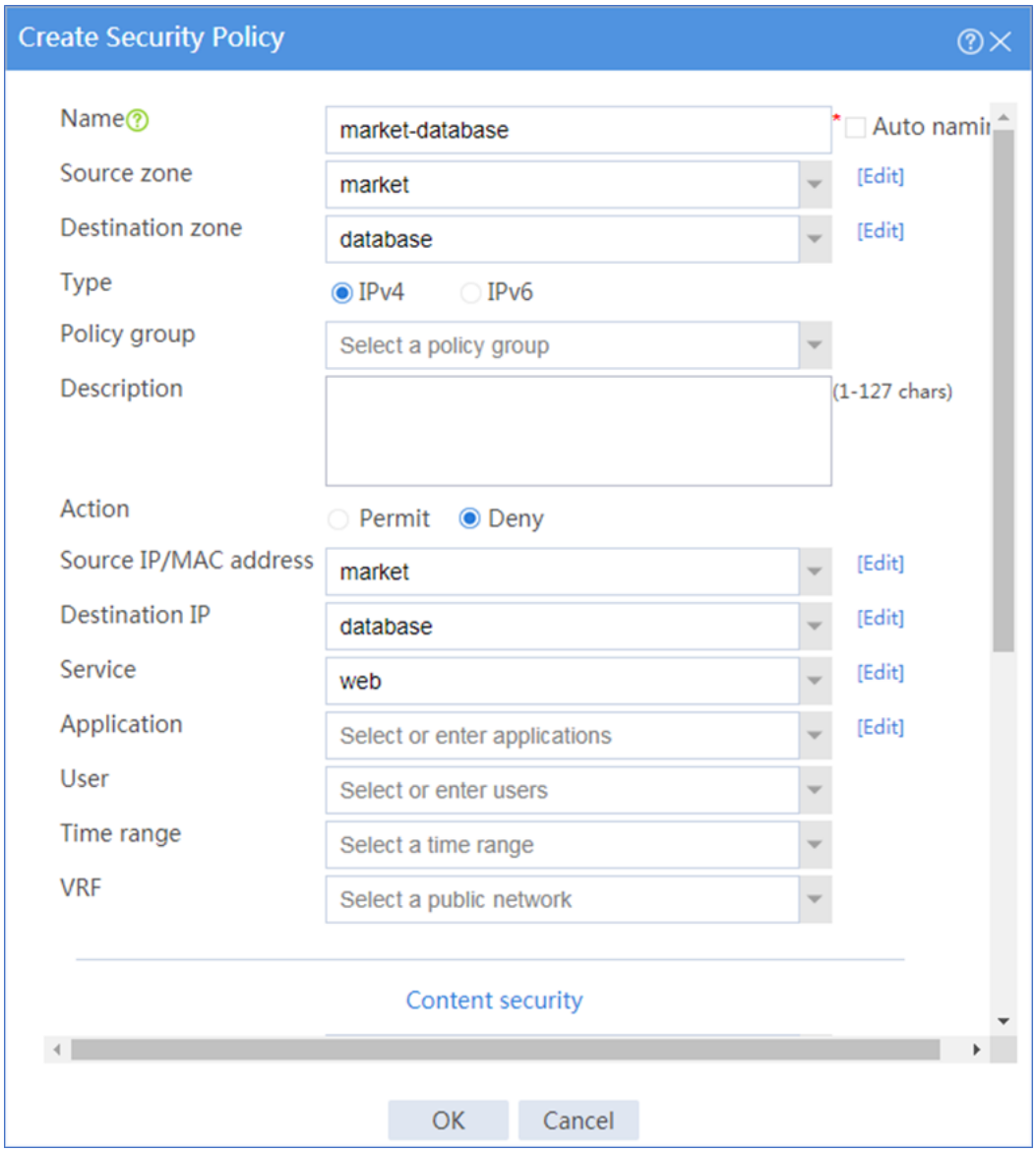
#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、図 4 に示すセキュリティポリシーを作成します。

図4 marketingオフィスのセキュリティポリシーを作成する



#**OK** をクリックします。

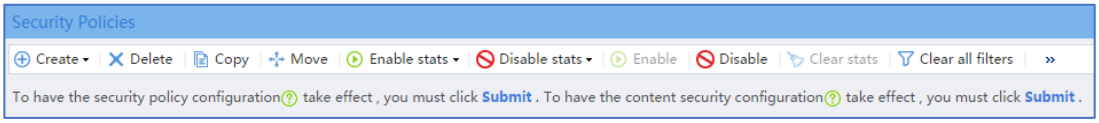
9. セキュリティポリシーをすぐに有効にするには、セキュリティポリシー一致アクセラレーションをアクティブにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Activate**(この例では最初の **Submit**)をクリックします。

図 5 セキュリティポリシーマッチングアクセラレーションを有効にする

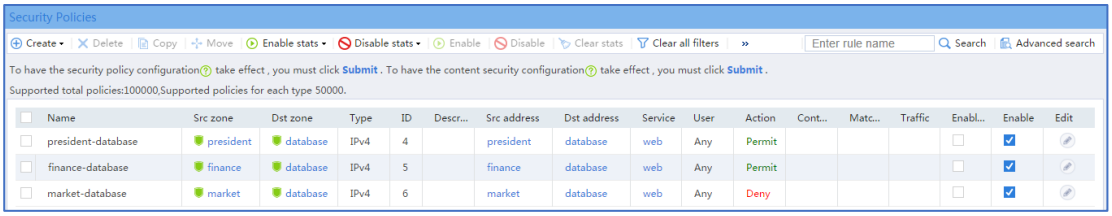


設定の確認

#各オフィスの PC を使用して、ブラウザから財務データベースサーバーの Web サービスにアクセスします。

#セキュリティポリシーが正しく設定されていることを確認します(図 6 を参照)。

図6 セキュリティポリシーの設定



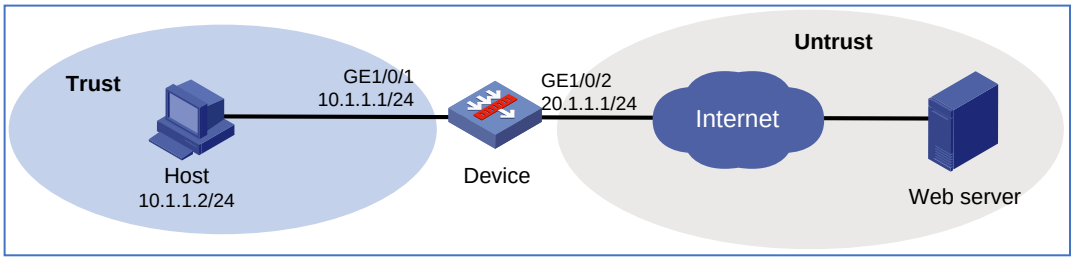
例:セキュリティポリシーとDPIの設定

ネットワーク構成

図 7 に示すように、内部ネットワーク内のホストはデバイスを介してインターネットにアクセスします。次の設定でデバイスのセキュリティポリシーと DPI を設定します。

- 内部ネットワークからのデータパケットに対してアンチウイルス検出を実行し、パケットのウイルスをドロップします。
- ウイルス例外として ID90321 のウイルスを指定します。
- アプリケーション例外として RenMinWang を指定します。システムがウイルスを含むパケットを RenMinWang に許可し、アラームを生成できるようにします。

図7 ネットワーク図



使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

   #トップナビゲーションバーで、**network** をクリックします。

   #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

   #GE1/0/1 の **edit** アイコンをクリックします。

   #開いたダイアログボックスで、インターフェイスを設定します。

   A) **basic configuration**タブで、**Trust**セキュリティゾーンを選択します。

   B) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。

   C) **ok**をクリックします。

   #GE1/0/GE1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。

2. IPv4アドレスオブジェクトグループを作成します。

   #トップナビゲーションバーで、**object** をクリックします。

   #ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

   #**create** をクリックします。

   #開いたダイアログボックスで、サービスオブジェクトグループを設定します。

   A) グループ名**private**を入力します。

   B) **add**をクリックします。

   C) 表示されるダイアログボックスで、**network segment**オブジェクトを選択し、IPv4アドレスと

マスク長10.1.1.0/24を入力します。

D) **OK**をクリックします。

E) **Create IPv4 Object Group**ページで、**ok**をクリックします。

3. アンチウイルスプロファイルを作成します。

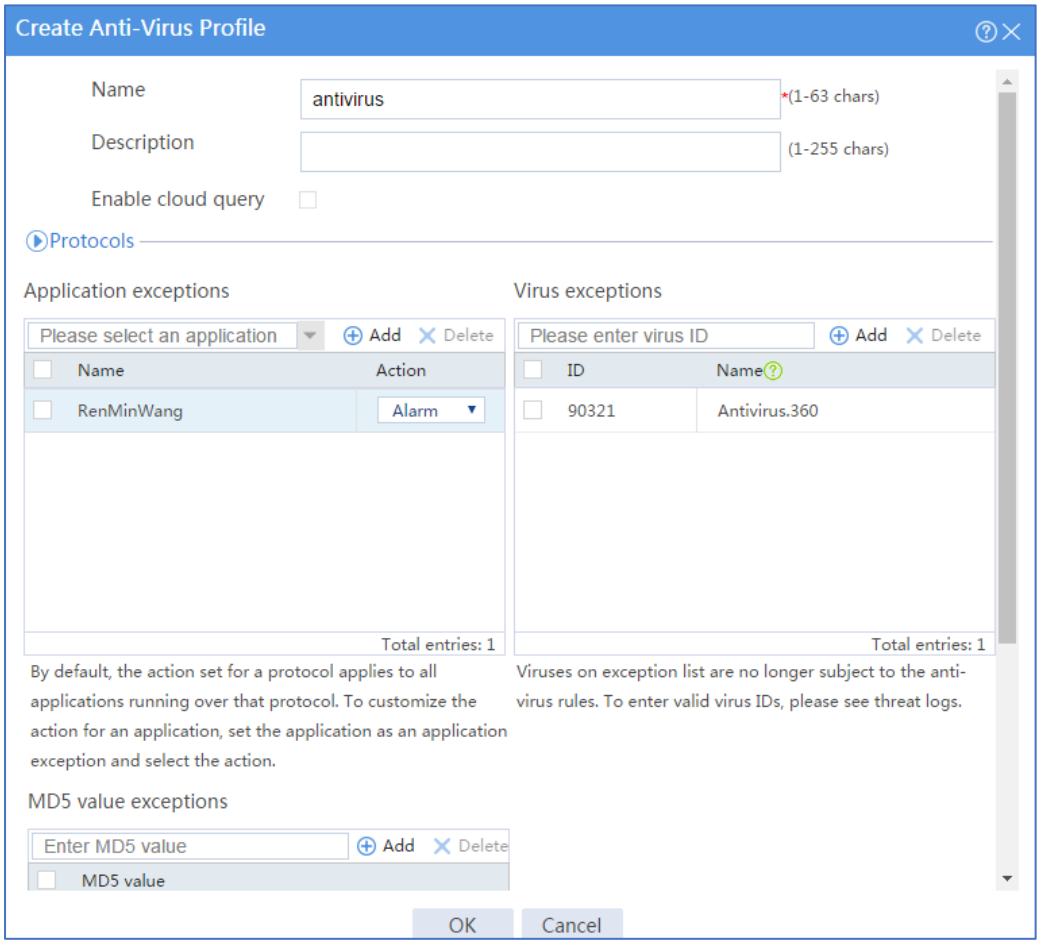
#トップナビゲーションバーで、**objects** をクリックします。

#ナビゲーションペインで、**APPSecurity> Anti-Virus** > **Profile** を選択します。

#**Create** をクリックします。

#表示されるダイアログボックスで、アンチウイルスプロファイルを作成します(図 8 を参照)。

図 8 ウイルス対策プロファイルを作成する



A) **ok**をクリックします。

4. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#図 9 と図 10 に表示されるダイアログボックスで、およびに示すセキュリティポリシーを作成します。

図 9 基本セキュリティポリシー設定を作成する

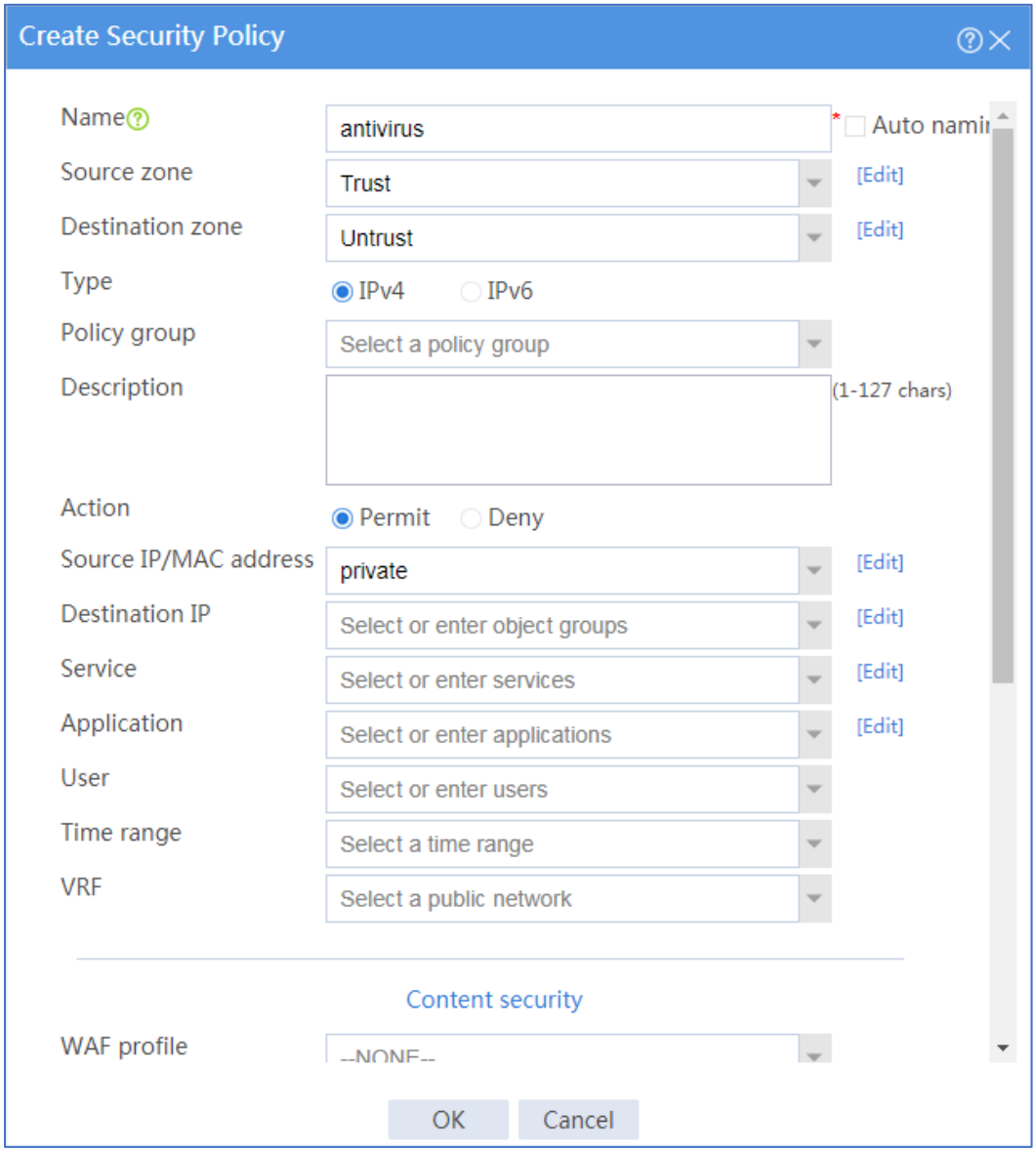
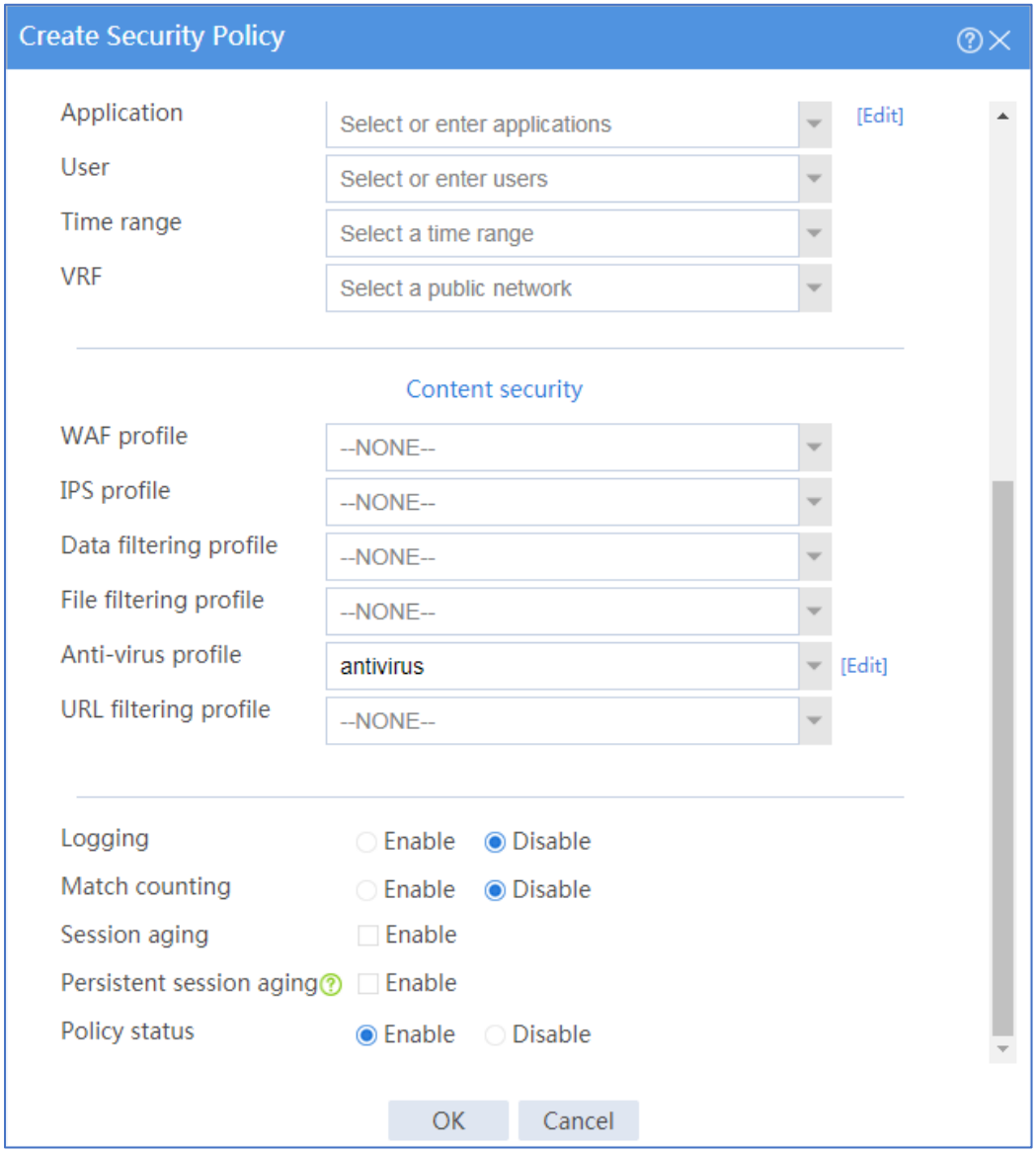


図 10 コンテンツセキュリティ設定を構成する



#**OK** をクリックします。

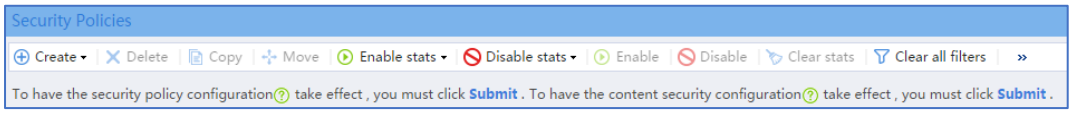
5. セキュリティポリシーをすぐに有効にするには、セキュリティポリシー一致アクセラレーションをアクティブにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Activate**(この例では最初の **Submit**)をクリックします。

図 11 Acceleration に合致するセキュリティポリシーを Activate させる



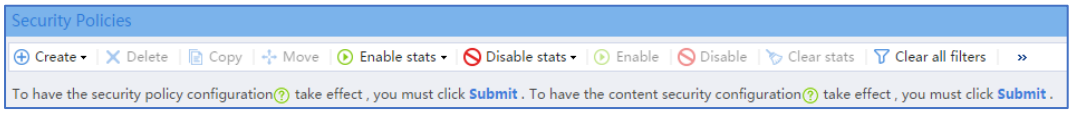
6. 設定を有効にするには、コンテンツセキュリティ設定を送信します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Submit**(この例では 2 番目の **Submit**)をクリックします。

図 12 コンテンツセキュリティ設定の送信



設定の確認

#セキュリティポリシーが正しく設定されていることを確認します。

図13 セキュリティポリシーの設定