WSM
WatchGuard System Manager
基本設定ガイド

ウォッチガード・テクノロジー・ジャパン株式会社

2014 年 7 月 Rev-03

目次

はじめに

この度はウォッチガード製品を選定していただきありがとうございます。

本書は、XTM を設定するための強力なツールである WSM (WatchGuard System Manager) による設定方法を解説するものです。

具体的なケースに基づき、手順を追いながら解説していますので、本書に沿って一通り設定してみるなら、XTM の日常的な管理は難なくできるようになるに違いありません。

なお、本書で使用されている設定画面は、2014 年 7 月時点での最新バージョン Fireware XTM OS v11.9 のものです。

このガイドが、XTM を自在に使いこなす一助になれば幸いです。

第一章　XTM のセキュリティ概念　～　XTM マニアになろう！

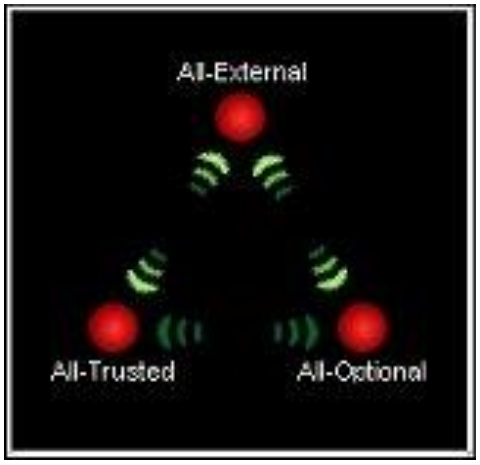
この章では、WatchGuard 伝統のネットワーク概念と設定ツールの特徴を説明します。これらを知っておくなら、設定の習得は容易になり、製品に対する理解も深まるでしょう。

このガイドをお読みの方には、XTM の設定について理解を深めていただき、ぜひマニアの域にまで足を踏み入れていただきたいと思います。

XTM のネットワーク概念

XTM はネットワークの設定をする上で、基本的に以下の 3 つのゾーンが定義されています。

エイリアス	日本語標記	意味
External	外部	WAN、インターネット側
Trusted	信頼済み	内部ネットワーク、LAN 側
Optional	任意	DMZ など



この「三角関係」、すなわち 3 種類のネットワークのゾーンを意識するなら、XTM の設定は非常に容易です。

【豆知識】「三角形」は WatchGuard の象徴だった

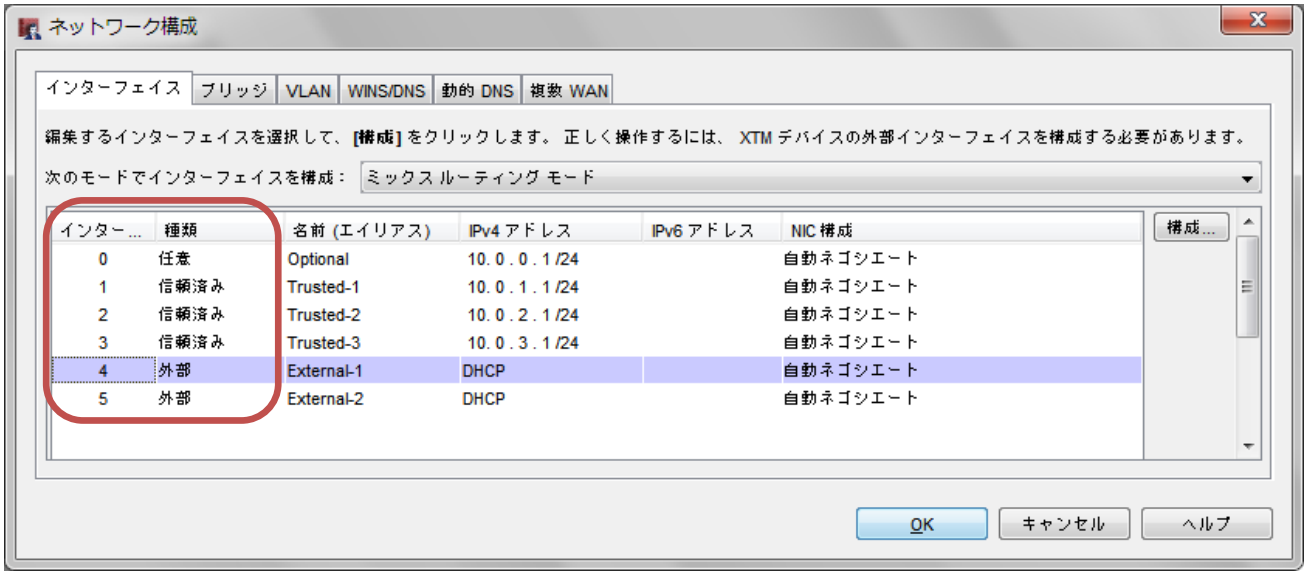
初期の製品 WatchGuard Firebox II には、このネットワークの概念がフロントパネルに具象化されていました。古くからの WatchGuard ファンには馴染み深いものです。

ネットワーク設定に見る XTM の概念

XTM は、物理ポートごとに External/Trusted/Optional を設定します。

またそれらは固定ではなく自由に設定できます。

以下のネットワーク構成画面では、0 が Optional、1-3 が Trusted、4,5 を External として設定しています。

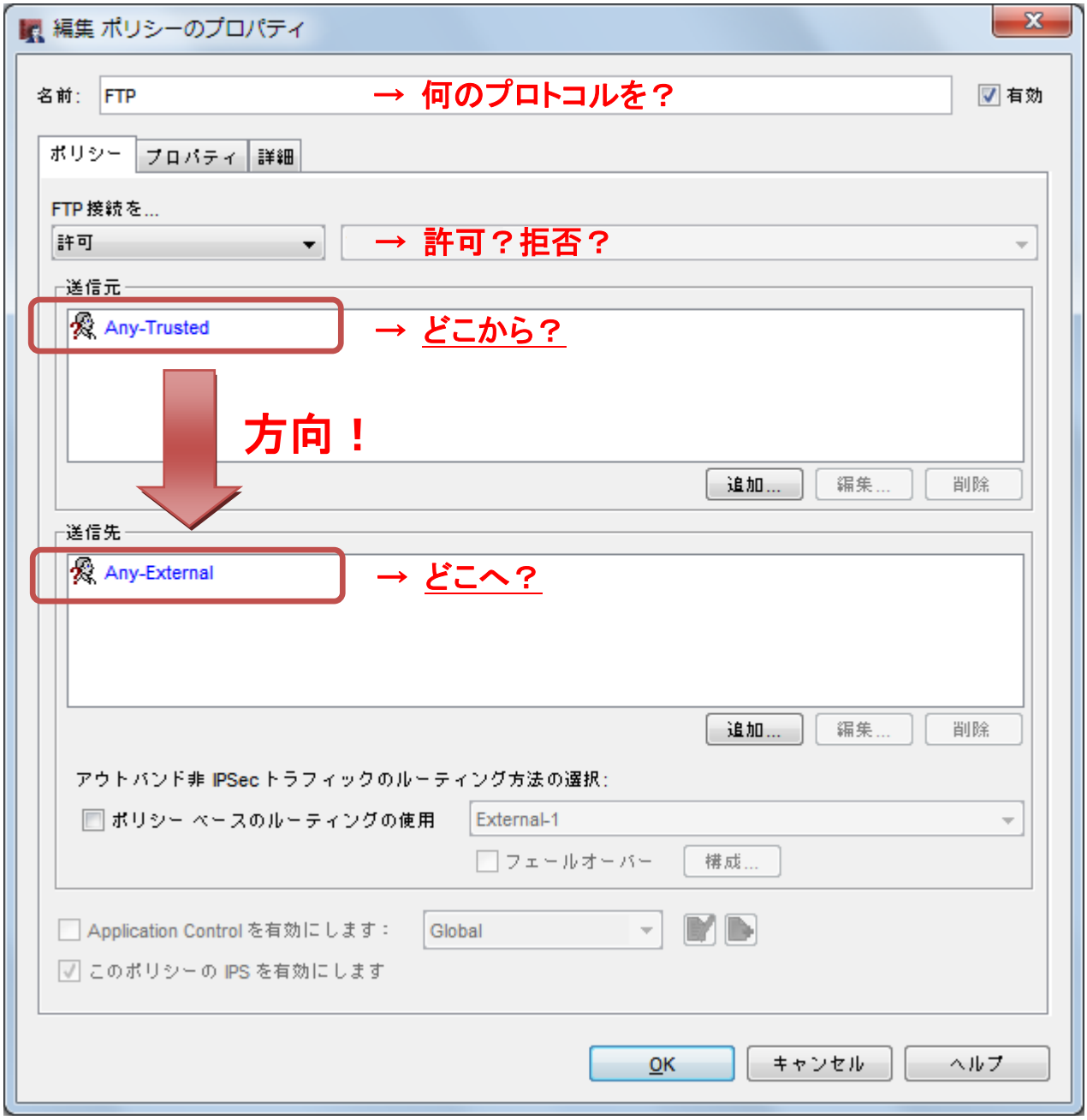


初期設定の External は 0 番ポートですが、それにとらわれる必要はまったくない、ということです。

ポリシーマネージャに見る XMT の概念

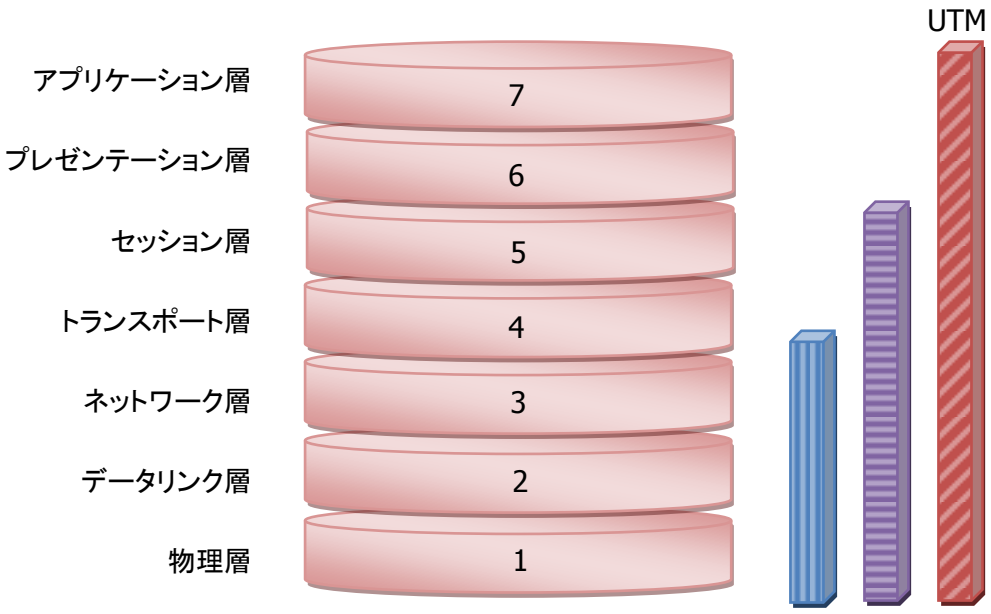
以下はポリシーマネージャのポリシー編集実際の画面です。(後ほど詳しく解説します)

前述のネットワークの方向に従って設定されることが分かるでしょう。



XTM で実現可能なセキュリティ範囲

XTM は通常のファイアウォールで実現可能な L3 までのセキュリティに加え、L7 までの高レイヤーまでのセキュリティを提供する UTM アプライアンスです。



レイヤー7 までカバーするのが UTM です。

パケットフィルタ　：ポートベース

ファイアウォール　：ステートフルパケットインスペクション

UTM　：コンテンツフィルタリング、IPS、アンチウイルスなどのプロキシ機能

【豆知識】XTM とは

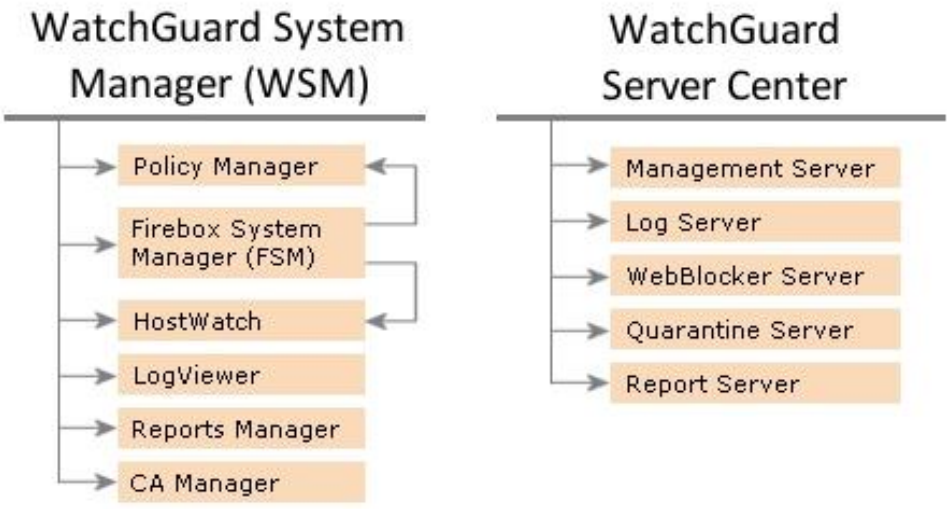
製品名“XTM”は、UTM(Unified Threat Management)の次世代拡張版を意味する“Extensible Threat Management”の頭文字を取ったものです。

WatchGuard System Manager の概要

WatchGuard System Manager (WSM<ダブリュエスエム>と呼んでください) は、XTM でネットワーク管理とセキュリティ維持を、容易に且つ効率的に行なうためのソフトウェアです。

WatchGuard System Manager の基本コンポーネントは、WatchGuard System Manager ウィンドウと、5 つの WSM サーバー ソフトウェアからなります。WatchGuard System Manager からは、他の WatchGuard ツールにアクセスすることができます。

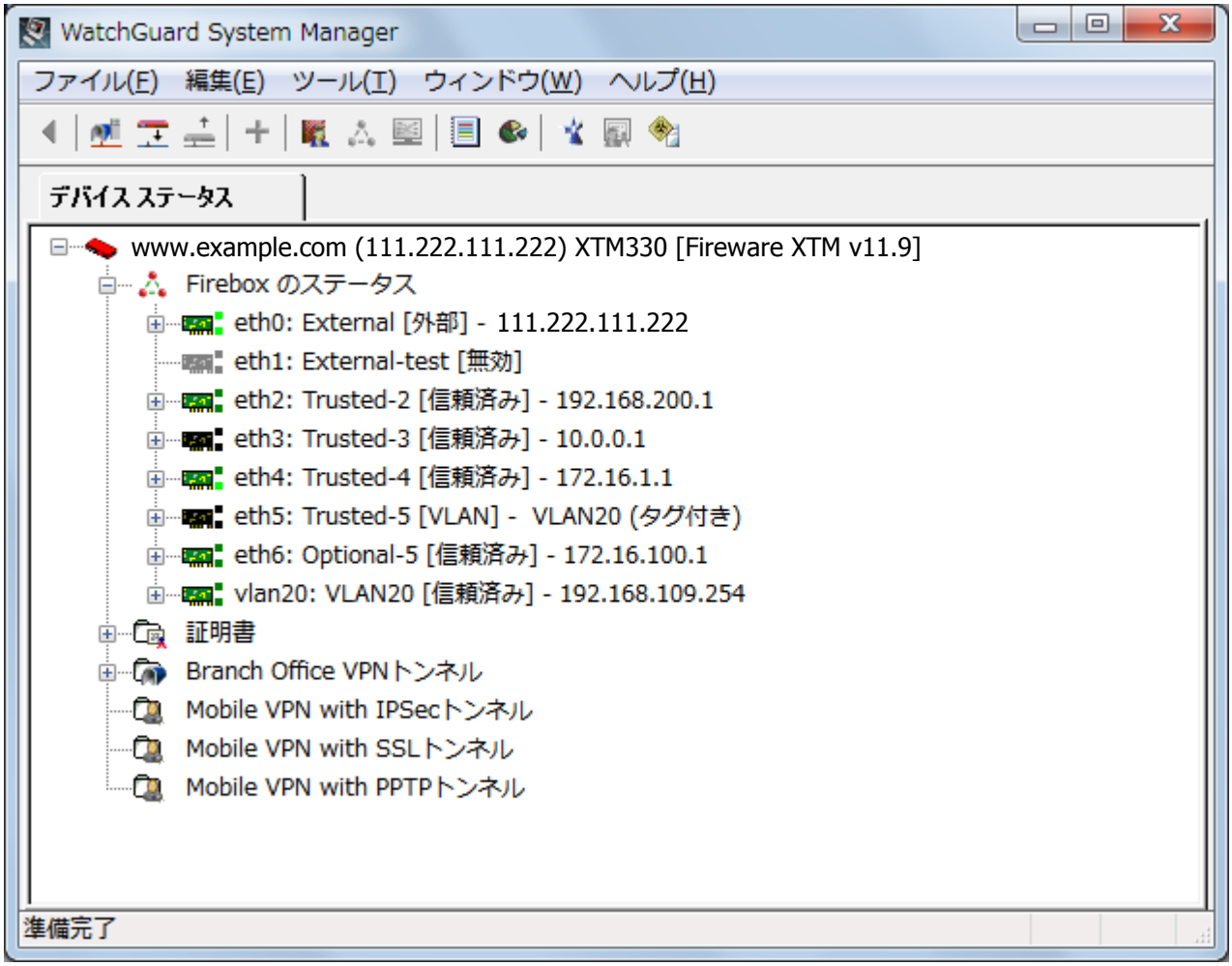
次の図は、WatchGuard System Manager の各ツール/サーバーソフトウェアへのアクセス方法、および、切り替え方法を示したものです。



WatchGuard System Manager

WatchGuard System Manager (以下 WSM) は、XTM および WatchGuard Management Server に接続し、管理するためのアプリケーションです。

WSM は後方互換性をサポートしており、異なるバージョンのファームウェアの XTM も一括管理できます。



管理用のインターフェイスとしては WebUI も用意されています。日常の設定変更くらいでしたらそれでもよいのですが、XTM マニアの方には是非この WSM を使っていただきたいと思います。なぜなら WSM は数々の有用なツール群にアクセスするためのインターフェイスでもあるからです。

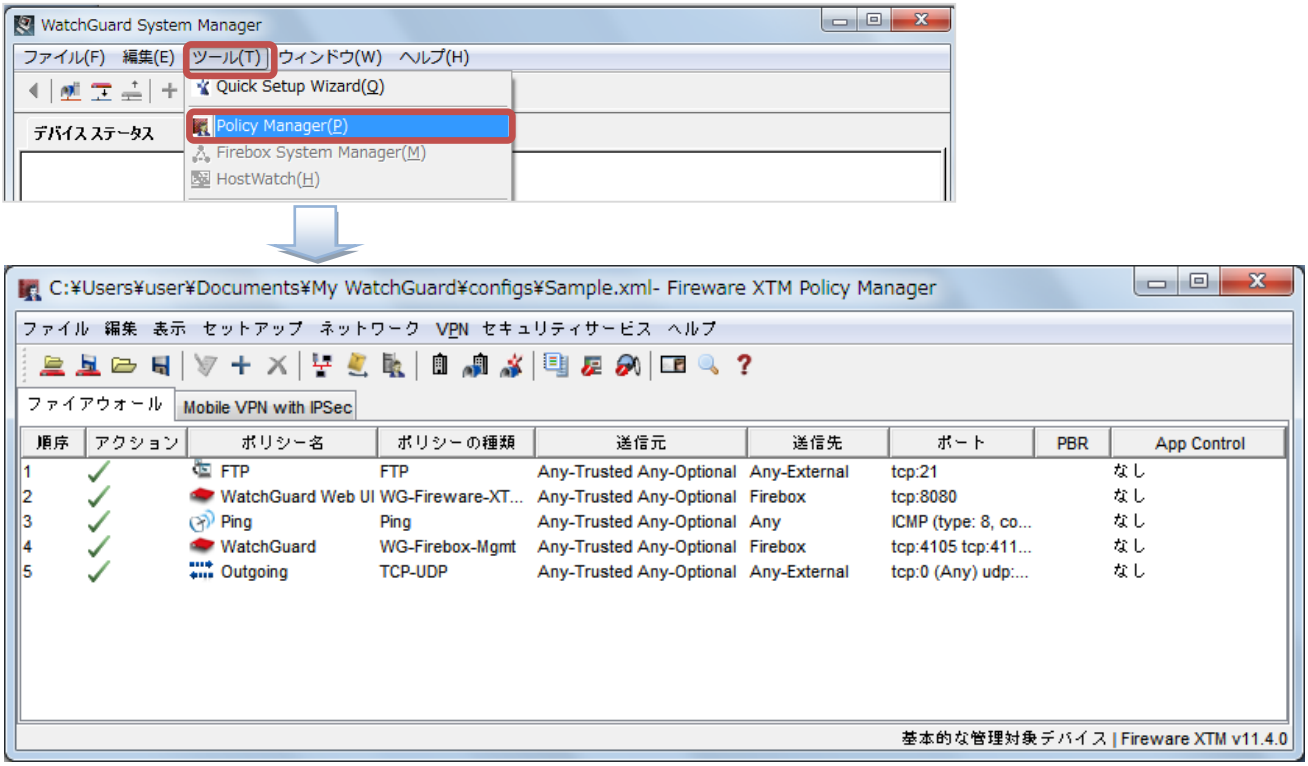
以下にそのツールのいくつかをご紹介します。

ポリシーマネージャ(Policy Manager)

Policy Manager は、ファイアウォールおよび UTM の構成に使用するインターフェイスです。実際、設定時の大半はこのツールを使うことになります。

Policy Manager には、デフォルトで様々なプロトコルのパケットフィルタおよびプロキシのテンプレートが含まれています。また、カスタムでポート、プロトコル、およびその他のパラメータを指定して任意のフィルタを作成することもできます。起動方法は、

1. WSM で XTM へ接続します
2. メニューの ツール より Policy Manager をクリックします



詳細表示で表示された上から順番にポリシーが評価されます。[1]

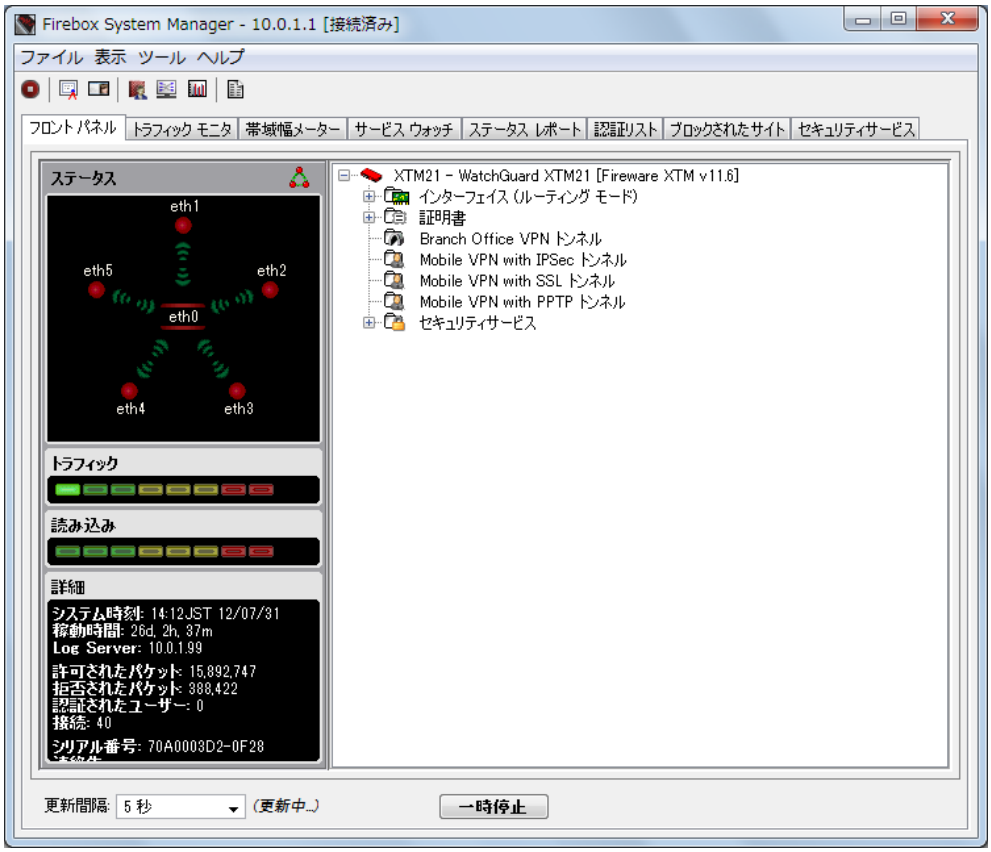
ポリシーマネージャ上で設定した内容は XTM へ保存するまで反映されません。そのため、実機がない環境でも事前に PC でコンフィグを作成しファイルとして保存しておくことが可能です。

また、このコンフィグファイルは後で XTM に流し込むことも可能です。

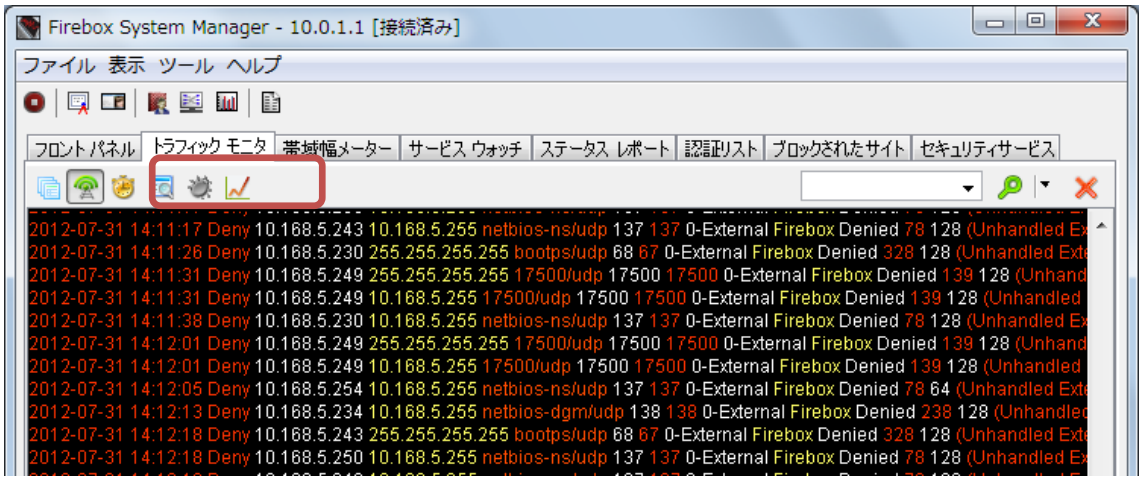
[1] WSM インストール後は標準で大きなアイコン表示です。ポリシーの評価順序を正確に把握するためにも、表示メニューから詳細表示を選んでください

Firebox System Manager

Firebox System Manager は、XTM のリアルタイム監視用のインターフェイスです。このツールから、XTM の構成と状態をリアルタイムで確認することができます。



たとえばトラフィックモニタータブをクリックすると、リアルタイムで XTM を通過するパケットのログを見ることができます。



第二章　初期設定　～　XTM をーから設定しよう！

事前準備

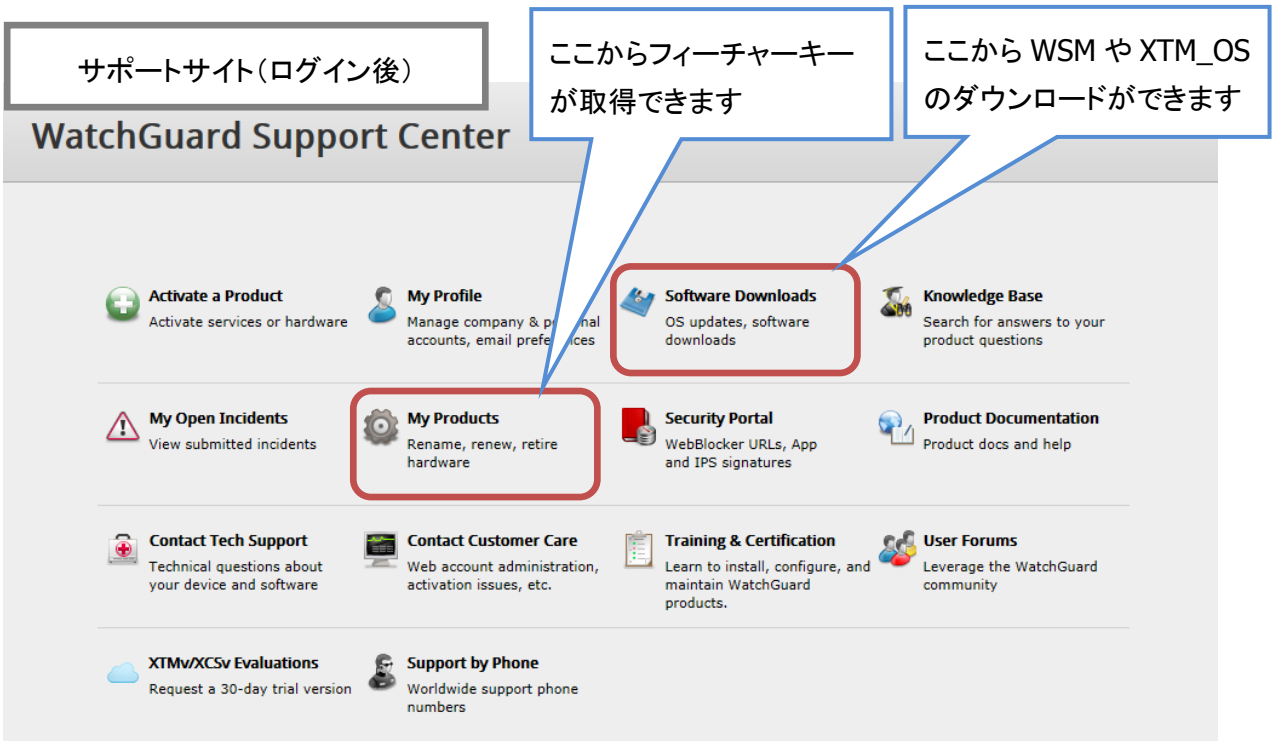
事前準備としてセットアップに必要なソフトウェアをインストールします。製品アクティベート後、WatchGuard Support (US)サイト内の『Articles & Software』より必要なソフトウェアを取得します（ログインが必要）。

WatchGuard サポート (US) ： https://www.watchguard.com/support/index.asp

必要なソフトウェアは、以下の 2 つです。

- WatchGuard System Manager
- Fireware XTM OS (XTM のシリーズに対応したものを選択)

また、合わせてライセンス(Feature Key)の取得を行います。上記 URL の『My Products』から、該当機器の Feature Key を取得し、テキストファイルなどで保存しておきます。



ソフトウェアがダウンロードできたら、まず WatchGuard System Manager のインストールを行います。

初期セットアップではデフォルトでインストールします。途中、インストールするソフトウェアを選択する画面が表示されますが、追加せずそのまま進めます。

次に Fireware XTM OS をインストールします。こちらのインストールウィザードもすべてデフォルトで進めてください。

以上でソフトウェア側の準備は完了です。

ファクトリーリセット

デフォルト状態からの設定手順を記述するのが普通のマニュアルですが、XTM マニアの皆さんにはこのファクトリーリセットのステップからマスターしていただきたいと思います。

これは XTM を、工場出荷時の既定の設定に戻す手段です。リセットして起動すると XTM は「セーフモード」というモードで動作します[2]。

手順については機種によって 2 通りあります。

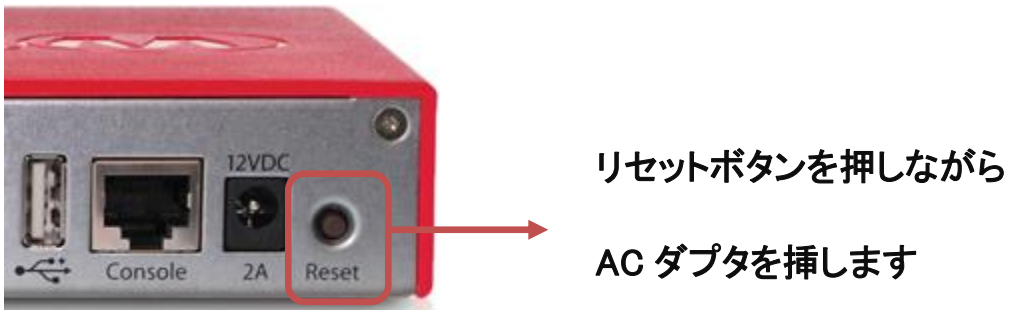
XTM2/3 シリーズ(330 除く)

1. XTM と接続

XTM との接続は、1 番ポートがデフォルトで Trusted となりますので、PC と XTM の 1 番ポートを LAN ケーブルで接続しておきます。

2. 電源の投入

リセットするためには特殊な方法で電源を投入します。機器の背面、右端の Reset ボタンを押しながら、AC アダプタの電源を挿します。Reset ボタンは起動中、ずっと押したままにします。



[2] SYS-B Mode とも言います。ちなみに正常起動の場合は SYS-A Mode になります

3.　起動の確認

フロントパネル　右端上の Attn(アテンション)ランプがオレンジ色に点灯したら、セーフモードで起動したことが分かります。

起動途中に点滅したりしますが、Reset ボタンはずっと押し続けます。

点灯状態になったら、それがセーフモード起動を意味します。

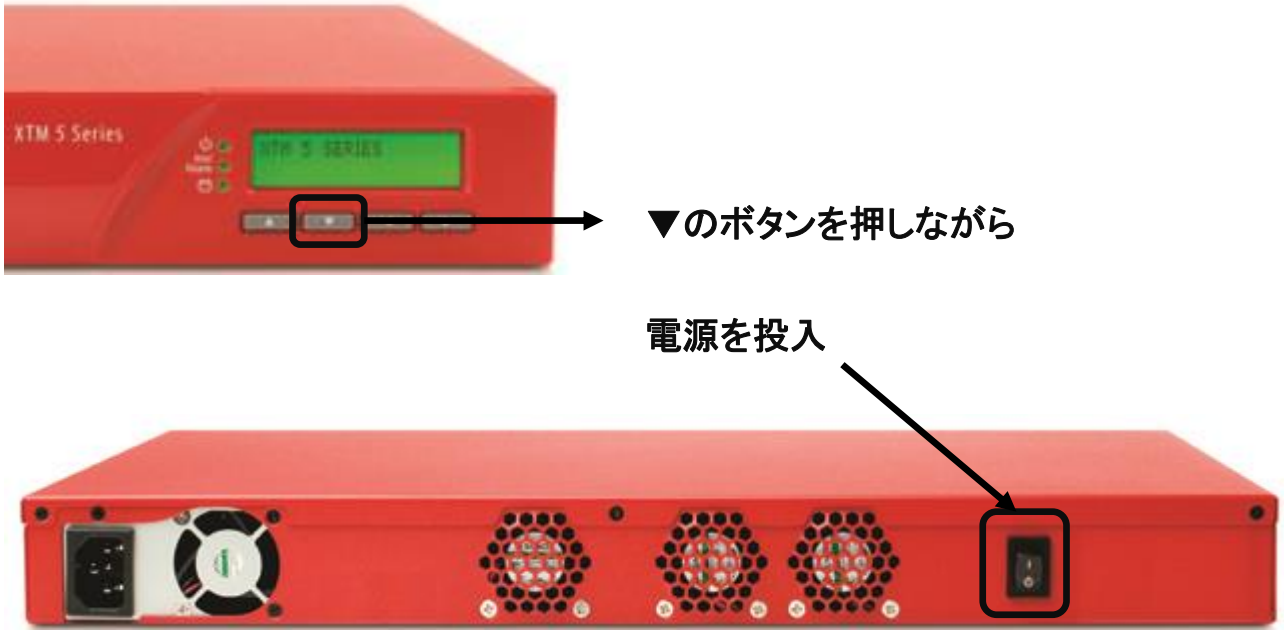
XTM330/5/8/10/20 シリーズ

1. XTM と接続

2/3 シリーズと同様にどの機種でも 1 番ポートが Trusted となります。PC と 1 番ポートを LAN ケーブルで接続しておきます。

2. 電源の投入

フロントパネル 右方、液晶パネルの下に上下左右の矢印ボタンがあります。この中の下向き▼のボタンを押しながら、背面の電源スイッチを ON にします。



3. 起動の確認

フロントパネルの表示が以下のように遷移します。(機種によって若干の違いがあります)

① Safe Mode で起動する旨の表示

② しばらくすると社名の表示

③ 最後に Uptime の表示

Uptime が表示されたら起動完了です。ここまできたら▼ボタンから手を離しても大丈夫です。

ファクトリーリセット後の設定

以下のデフォルト設定になります。設定する PC は Trusted のネットワークにあわせます。

External(0 番ポート)の IP アドレス	DHCP
Trusted(1 番ポート)の IP アドレス	10.0.1.1

設定する PC 側の設定は、以下のように固定 IP アドレスを設定しておいてください。

IP アドレス	10.0.1.2
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.0.1.1

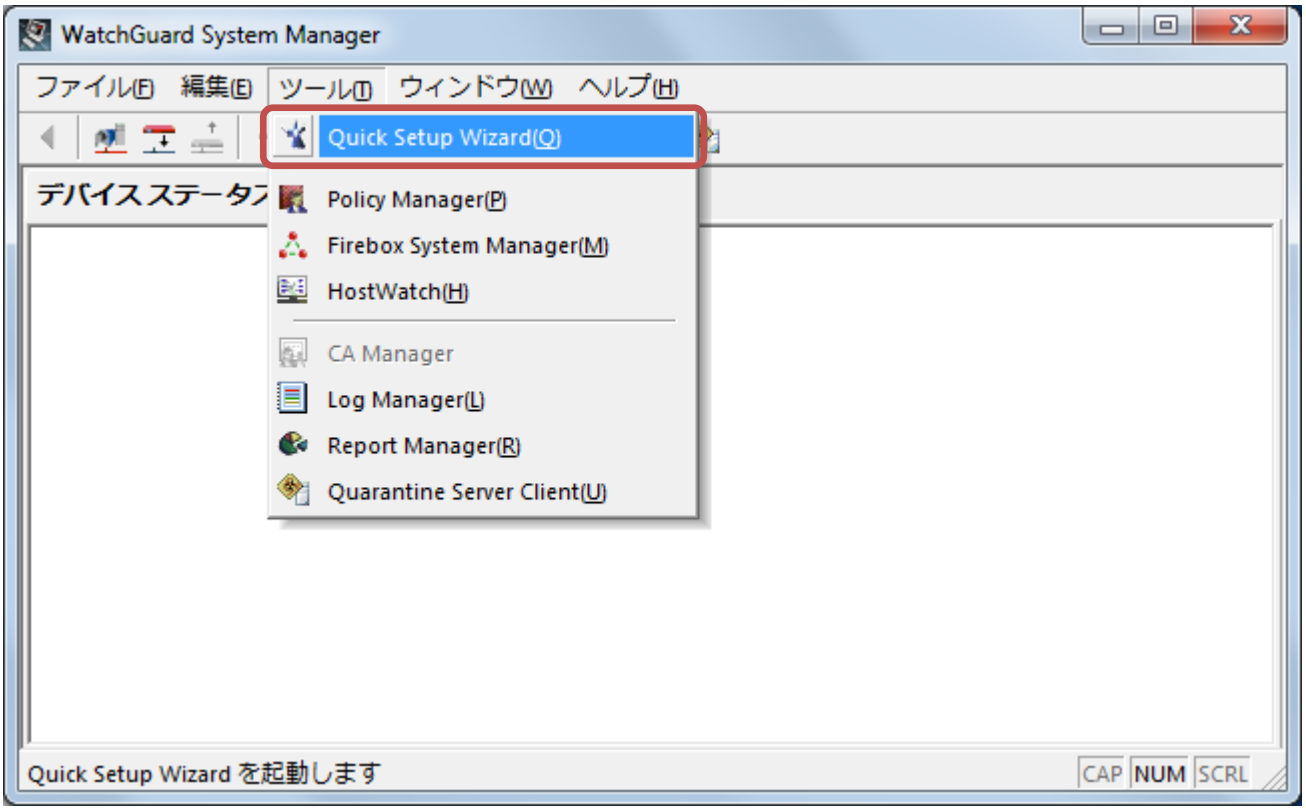
【豆知識】どんなときに初期化が必要？

- ✓ 構成パスフレーズを忘れてしまった
- ✓ 検証フェーズ終了後、本番設置前にきれいにーから設定したい
- ✓ ある拠点から XTM を引き上げてきて、別の拠点で使うためにーから設定したい
- ✓ 雷で停電。復帰後、起動したらコンフィグが壊れていた(稀ですが過去の事例にありました)。
  きれいな状態に戻してから、バックアップしていたコンフィグを読み込ませたい
- ✓ XTM_OS をアップグレードしたが、元のバージョンに戻したい（Recovery Mode）

Quick Setup Wizard

機器を Safe Mode で起動したら、Quick Setup Wizard で初期設定を行ないます。

スタートメニューから WatchGuard System Manager を起動し、ツールメニューから Quick Setup Wizard をクリックします。

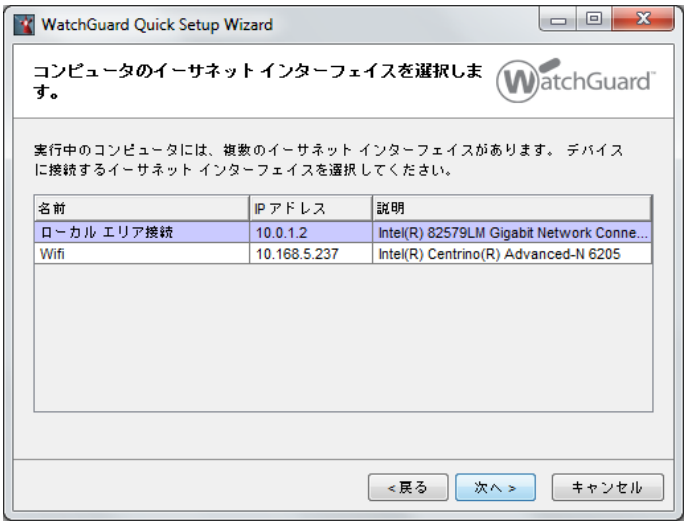


ようこそ、の画面は次へ。

「はい、デバイスは認識される準備ができています」を選び次へ。

※他のオプションは機種の選択やセーフモード起動の方法を指示してくれるウィザードになります

インターフェイスが複数あるとリストが表示されます。XTM と接続しているインターフェイスを選んで次へ。



デバイスが発見されたら次へ。

デバイス名を任意で入力します。

デバイスの外部インターフェイス、内部インターフェイス、DNS、Management Server、リモート管理　の画面ではデフォルトのまま次へ進みます。

デバイスのアクティベートの画面では、あらかじめ取得しておいた Feature Key をテキストボックスにコピー&ペーストして有効化します。もしくは参照ボタンをクリックし、保存しておいたテキスト形式の Feature Key を指定して読み込みます。

次にパスワードを設定します。8 文字以上が要求されます。テータスパスフレーズと構成パスフレーズに同一のものは設定できません。

ステータスパスフレーズはユーザー権限で、設定の閲覧や通信のリアルタイムモニタリングに使用します。構成パスフレーズは管理者用で、主に設定の保存時に使用します。

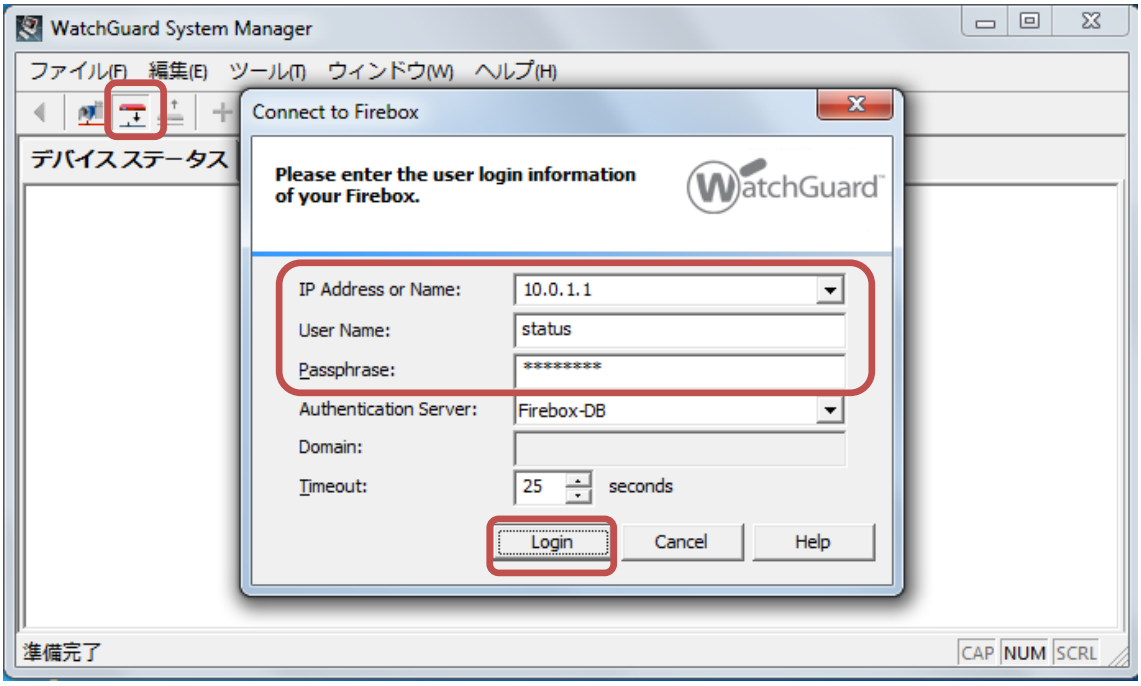
「デバイスの構成を確認します」画面で設定のサマリーが表示されたら、そのまま次へ。

ウィザードがデバイスを構成しています」の画面の後に、正常に完了しましたの画面になれば OK です。

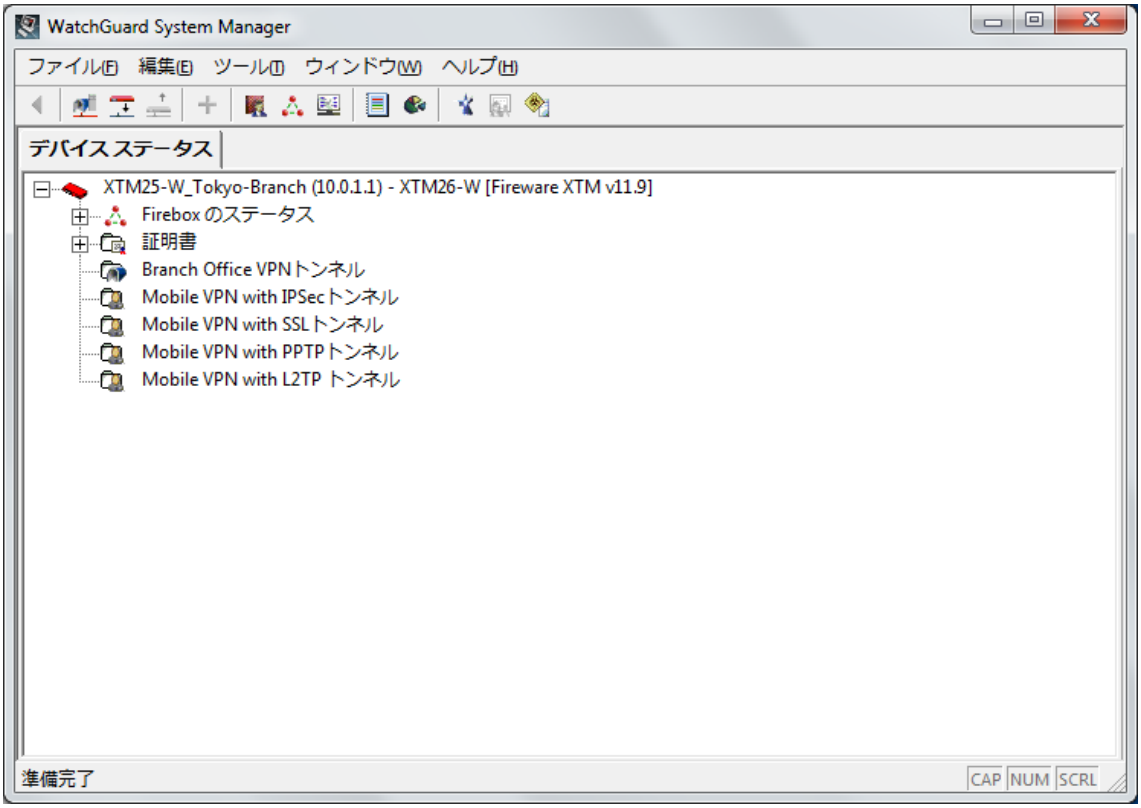
このあと自動的に再起動がかかり、通常モードで起動します。

それでは前章で初期設定を施した XTM に、WSM で接続してみましょう。

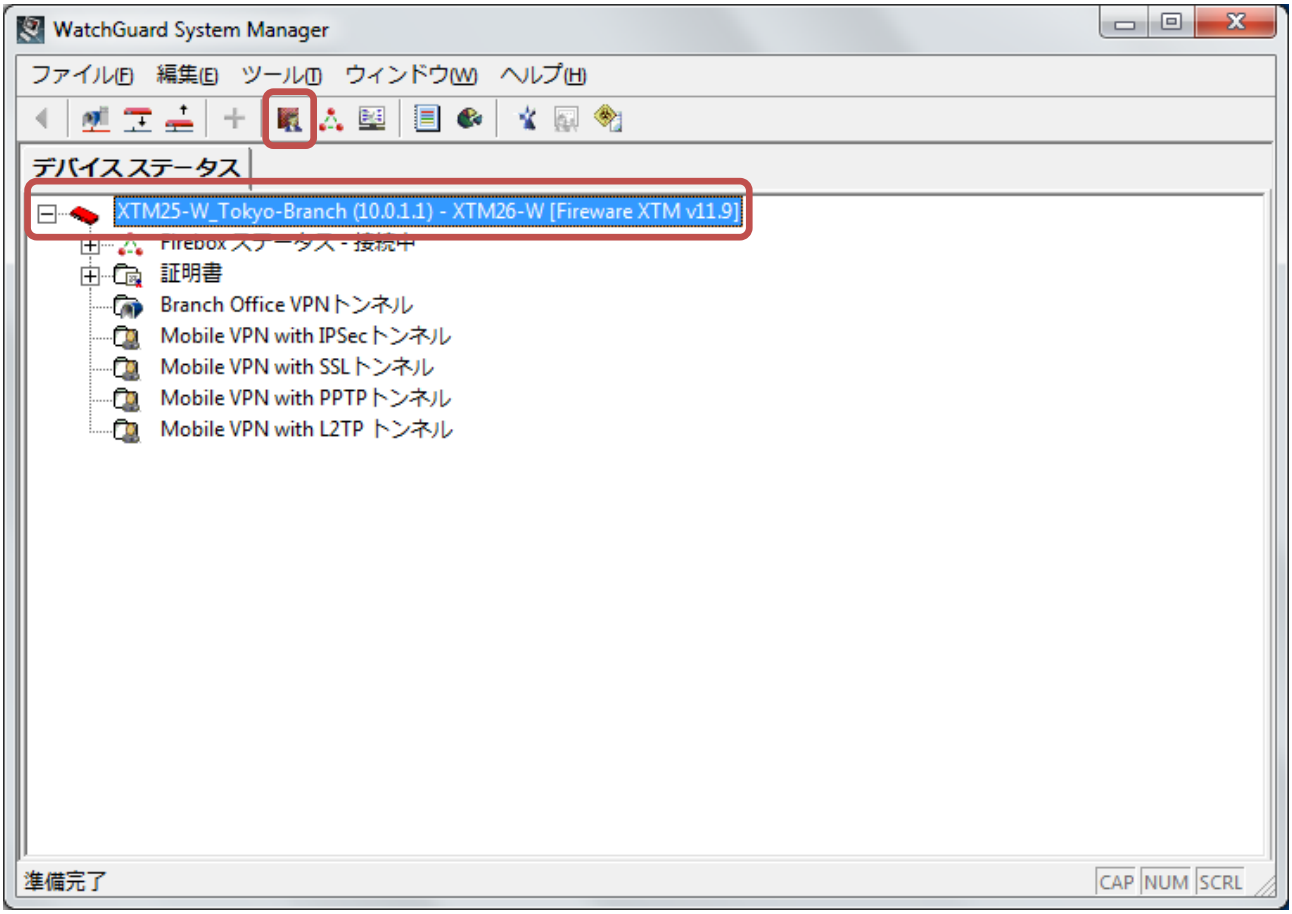
ツールバーの接続ボタンをクリックすると接続のダイアログが表示されます。IP Address は Trusted ポートのアドレス、Passphrase はステータスパスフレーズを入力し、ログインボタンをクリックします。



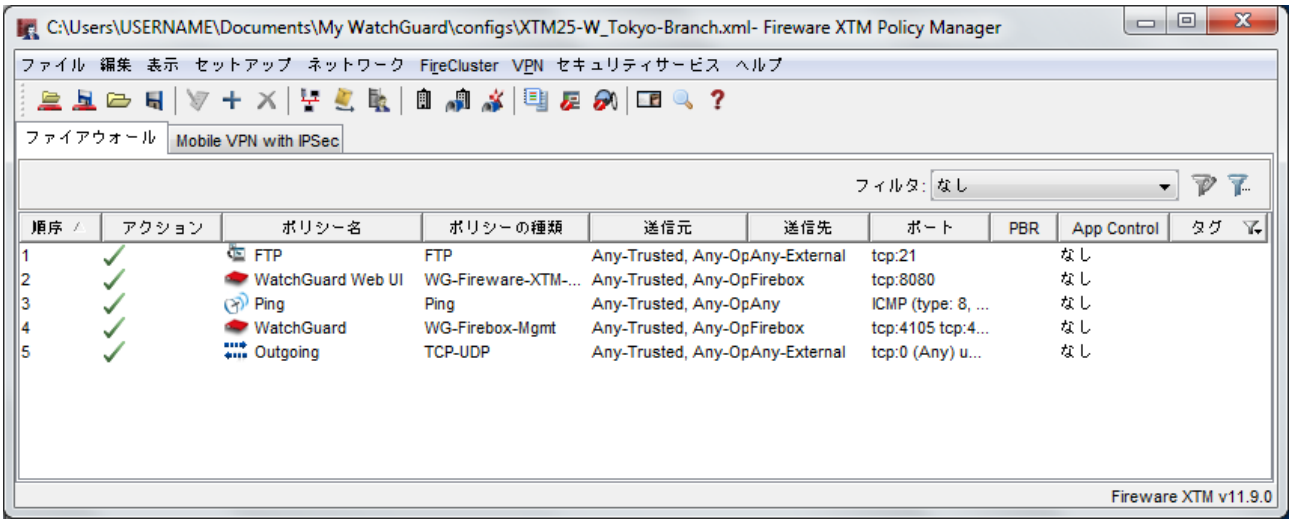
以下のように接続した XTM が表示されます。



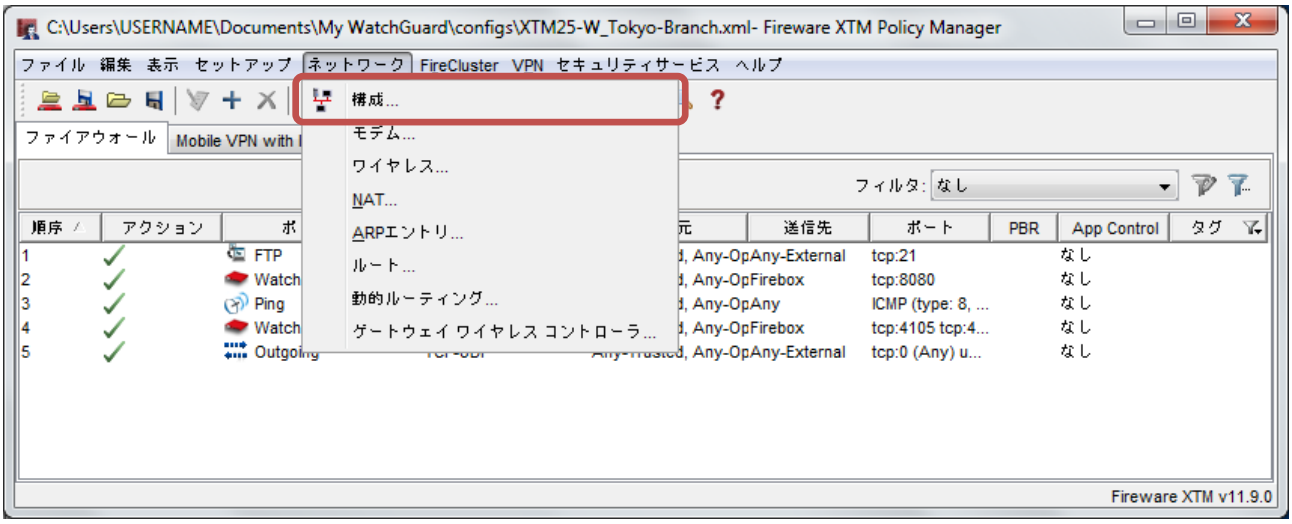
ネットワーク インターフェイスの構成はすべてポリシーマネージャから行ないます。機器を選択した状態でツールバーの Policy Manager ボタンをクリックします。



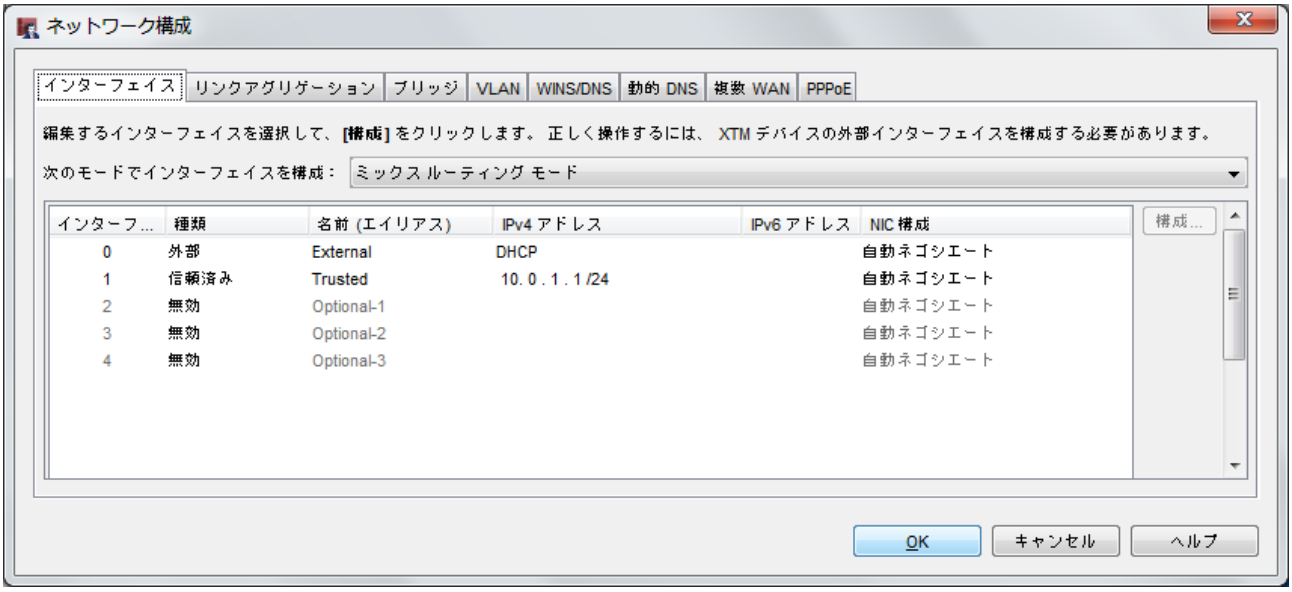
ポリシーマネージャが起動します。



インターフェイスを設定するには、ネットワークメニューの構成をクリックします。



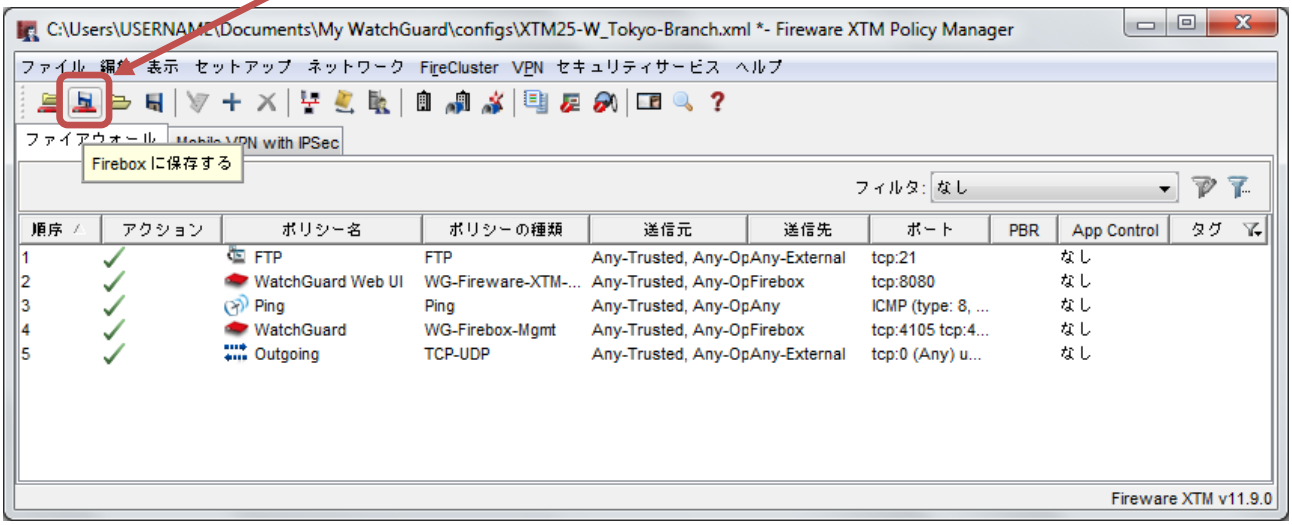
ネットワークの構成画面が開きます。



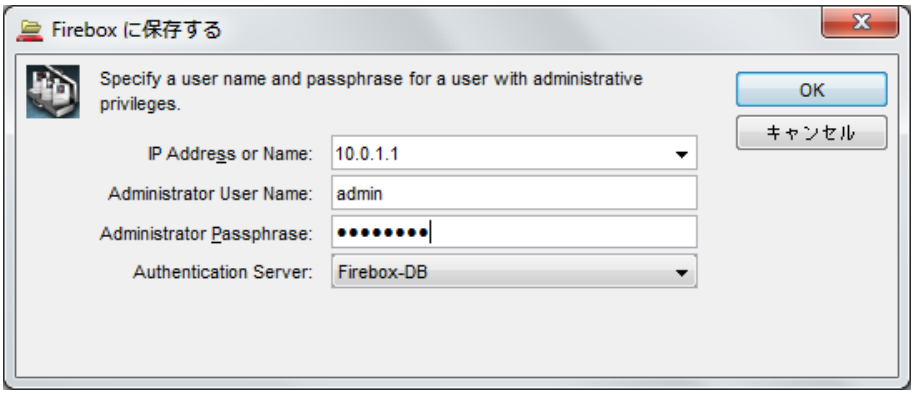
設定の保存

先に設定の保存方法を説明しておきます。

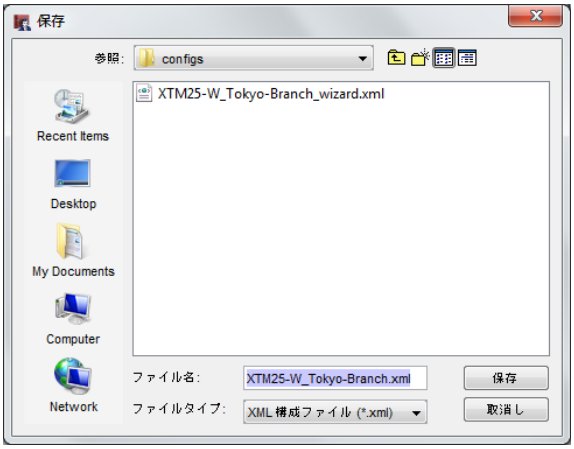
ポリシーマネージャの Firebox に保存するボタンをクリックします。



構成パスフレーズを入力して OK をクリックします。



ファイルに保存するためのダイアログも開きます。

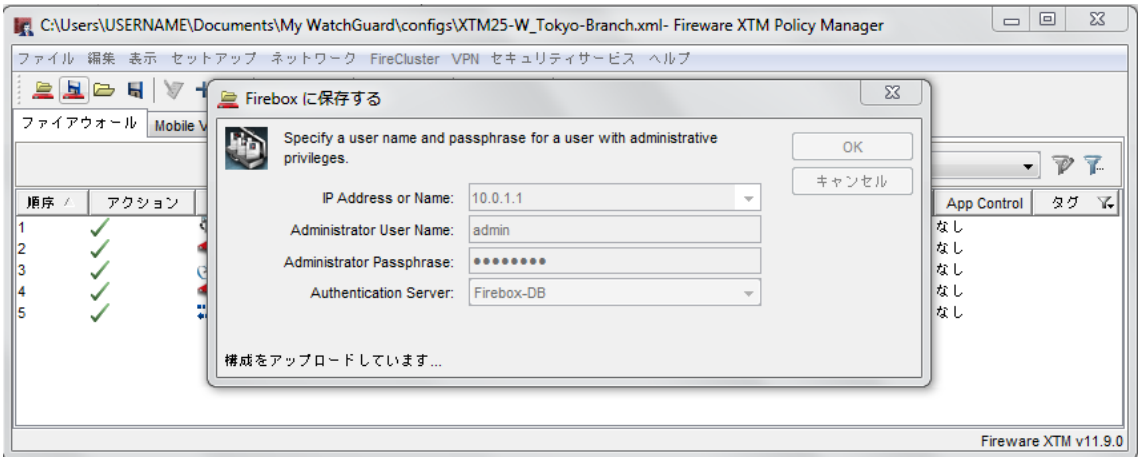


ここでデフォルトのファイル名で保存すれば、一つ前の設定に戻すことができます。

また、タイムスタンプをファイル名の末尾に付けて保存すれば、何世代も前に戻すことも可能になります。（例：XTM25_TokyoBranch-20140123.xml　など）

設定のバックアップのため、ファイルとして保存しておくことをおすすめします。

保存をクリックすると、設定が本体に反映されます。



最後にダイアログが出て完了です。

以降は設定したらその都度、この方法で保存してください。

DNS/WINS 設定

ネットワーク設定の手始めに DNS の設定をしてみましょう。

しかし何故、ネットワーク機器である XTM 自身に DNS を設定する必要があるのでしょうか？以下のような理由があります。

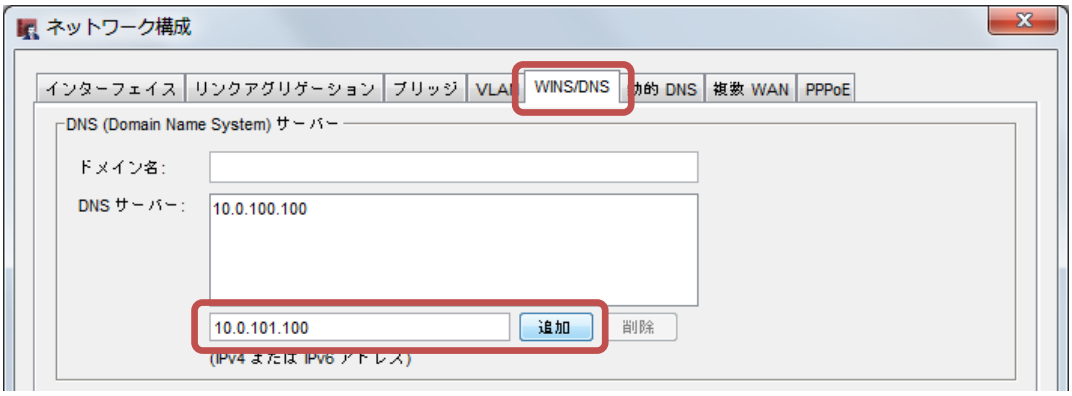
- ゲートウェイアンチウィルスや IPS のシグネチャ更新時の名前解決
- スパムブロッカーサーバーへの問い合わせの際の名前解決
- NTP サーバーを FQDN で設定した際の名前解決
- Branch Office VPN(拠点間 VPN)でドメイン名を使用した場合の名前解決

※ 注意：XTM は DNS リレーを行ないません。内部ノードが DNS のサーバーアドレスを XTM の IP アドレスに指定しても名前解決ができないので注意してください
（但し CLI で設定可能。実施方法はお問い合わせください）

DNS の設定

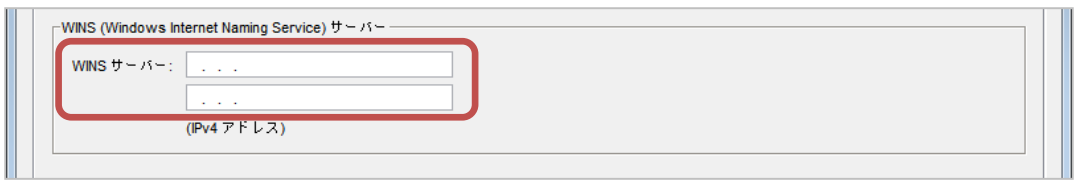
ポリシーマネージャの ネットワーク メニューから 構成 → WINS/DNS タブを選択します。

囲みのテキストエリアに DNS サーバーの IP アドレスを入力して、追加ボタンをクリックで追加できます。



WINS の設定

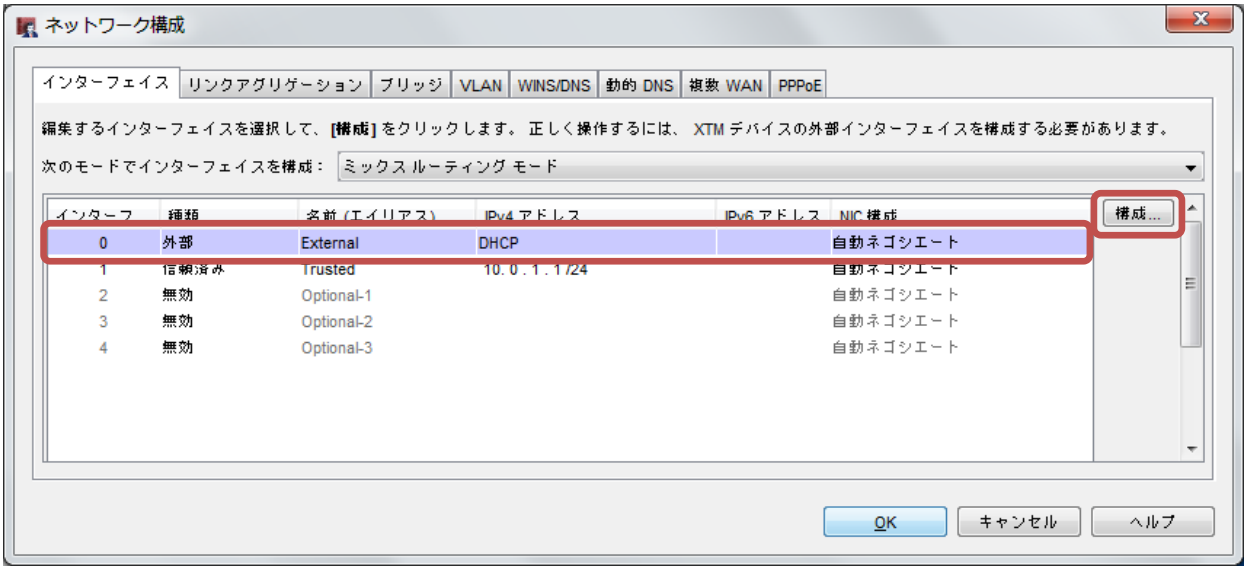
社内に WINS サーバーがあれば、下にある WINS サーバーの欄に IP アドレスを入力します。



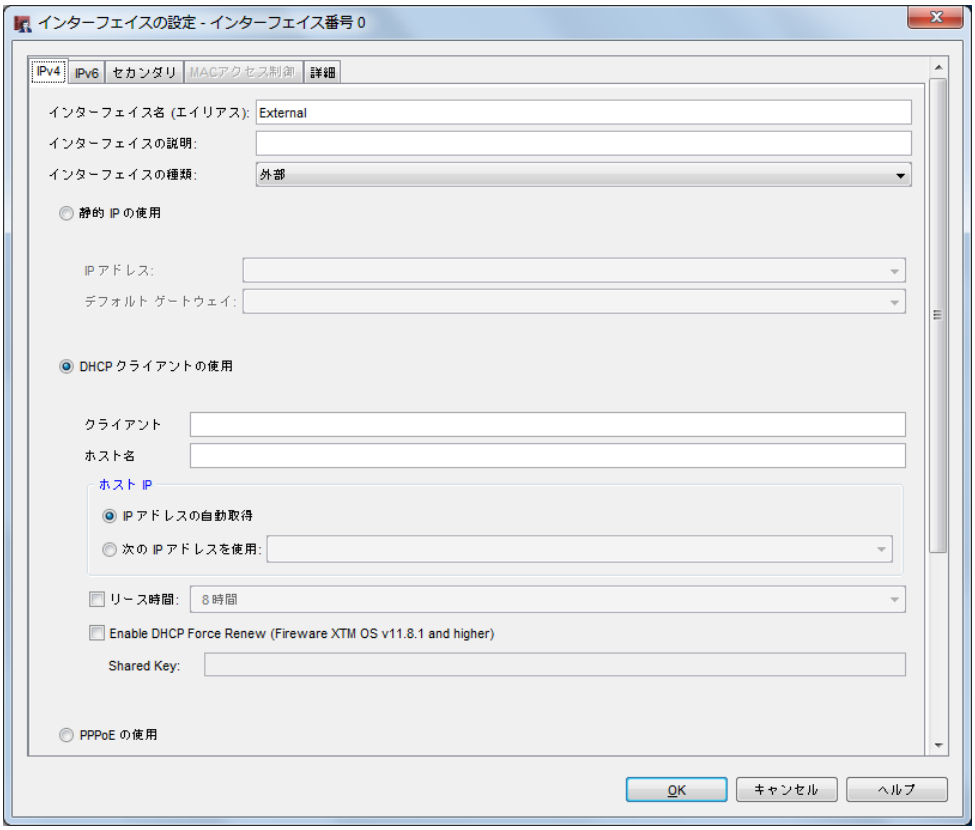
外部ネットワークの設定

次にインターフェイスの設定です。まずは外部インターフェイスから設定しましょう。

該当のインターフェイスを選択して、右の構成ボタンをクリックします。



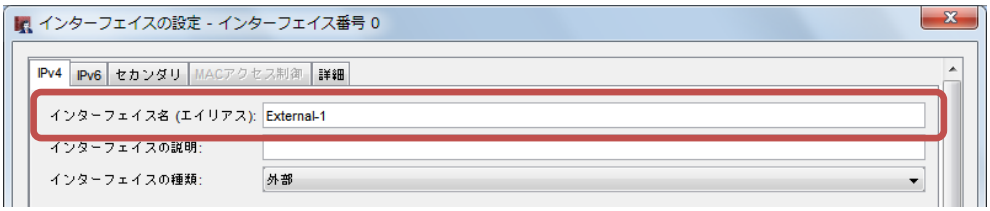
インターフェイスの詳細を設定できる画面が開きます。



インターフェイス名

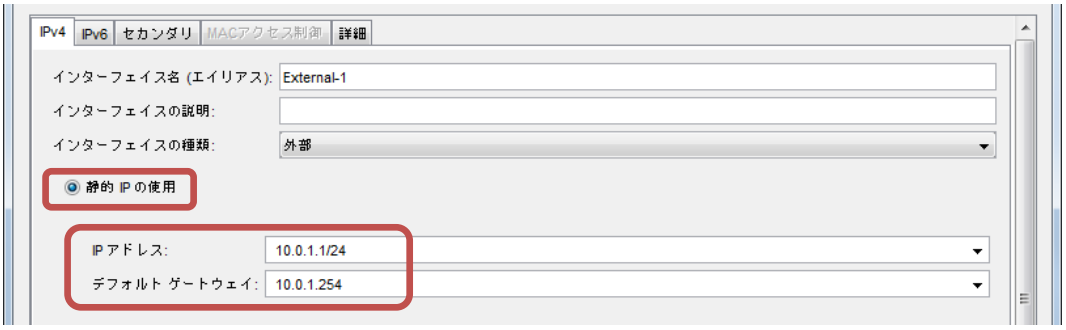
すべてのインターフェイス名(エイリアス)は任意で命名できます。外部インターフェイスだからといって必ず External でなければならない、というわけではありません。

たとえばマルチ WAN で 2 ポートの External がある場合、それぞれに External-1、External-2 というエイリアスをつけることができます。



固定 IP の設定

静的 IP の使用にチェックを入れ、IP アドレスにスラッシュ区切りでサブネットマスクのビット数、デフォルトゲートウェイを入力します。



DHCP の設定

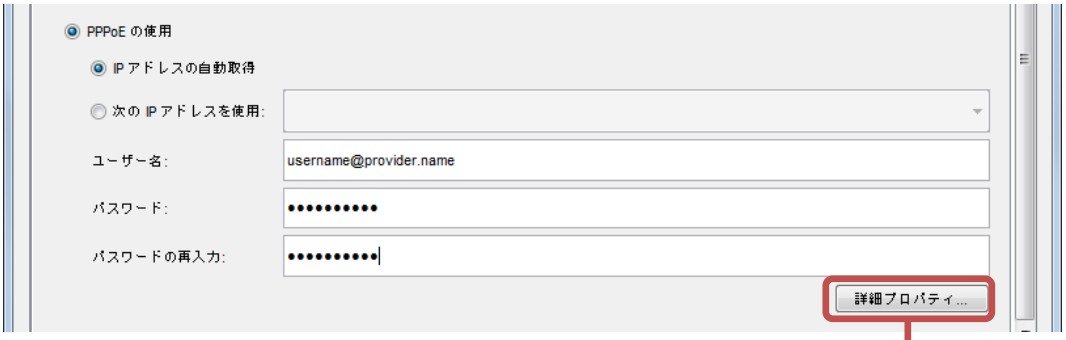
DHCP クライアントの使用にチェックを入れるだけです。

ISP 又は DHCP サーバーがクライアントを識別するために、MAC アドレスやホスト名の情報が必要になる場合があります。その際には、指示に従ってクライアント/ホスト欄に入力してください。

PPPoE の設定

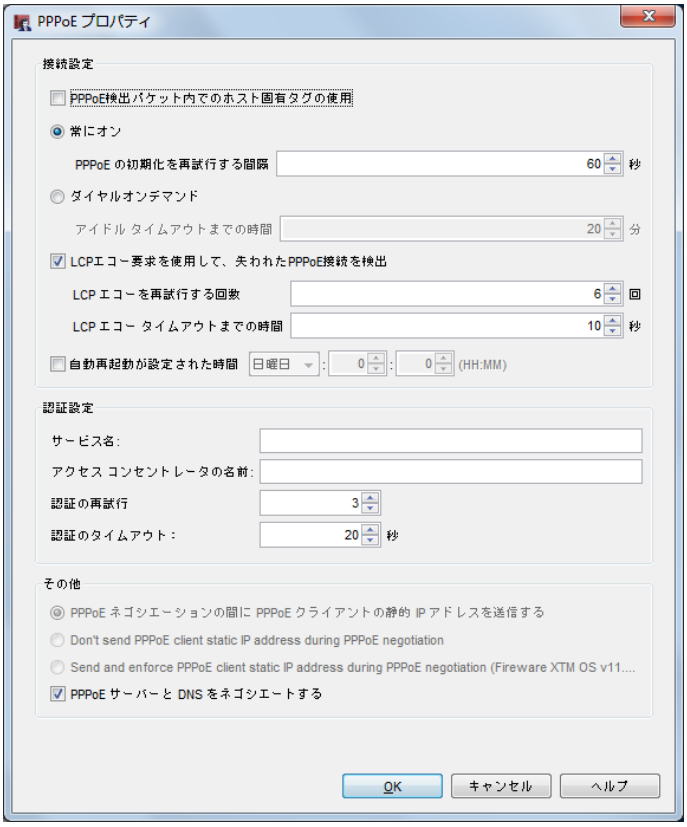
「PPPoE の使用」にチェックを入れます。ユーザー名とパスワードは、ISP から指定されたものを入力します。

IP アドレスが固定であれば「次の IP アドレスを使用」にチェックを入れて、指定の IP アドレスを入力します。



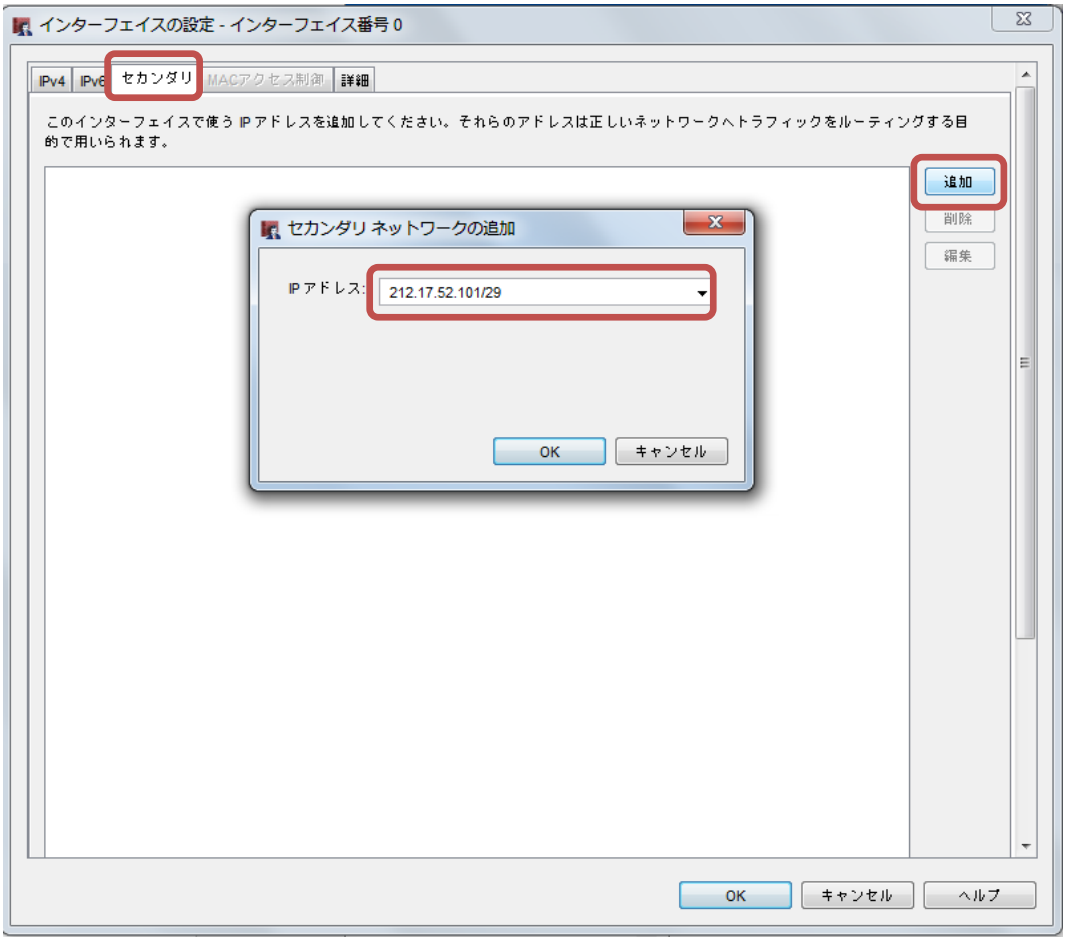
ISP の指定によってはより詳細な設定が必要になることがあります。

詳細プロパティボタンをクリックし、指定の項目を設定してください。

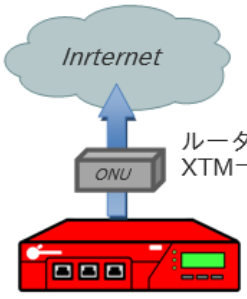


複数の固定 IP がある場合

固定 IP でも PPPoE でも、固定 IP アドレスが 2 つ以上ある場合は、インターフェイス設定画面の「セカンダリ」タブから追加します。



【豆知識】PPPoE は日本法人のリクエストで実現！



今となっては当たり前の PPPoE の機能も、ブロードバンドの回線が広まった当初は搭載されていませんでした。

しかし市場でのニーズを鑑み、日本法人として機能をリクエストした結果、PPPoE が実装されることとなりました。

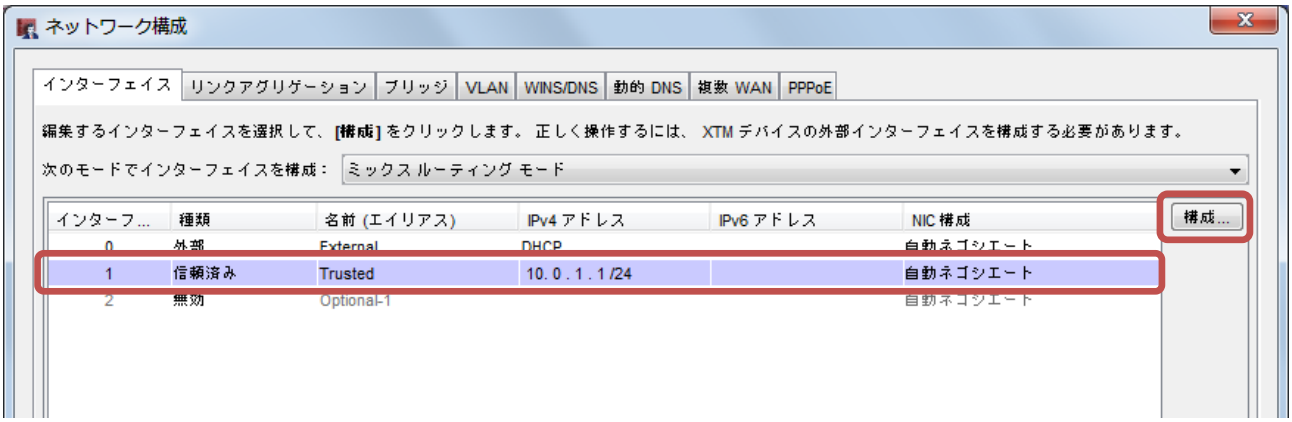
WatchGuard はお客様のニーズを速やかに実現する体制を持っているのです。

内部ネットワークの設定

XTM では内部ネットワークを Trusted(信頼済み)と Optional(任意)として設定します。

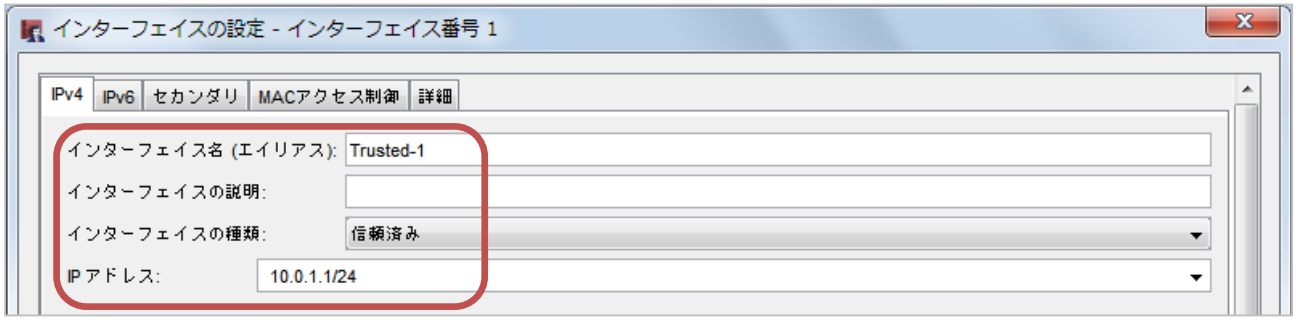
設定は外部インターフェイス同様、ポリシーマネージャから ネットワーク メニュー → 構成 の画面から行ないます。

インターフェイス一覧より、信頼済みインターフェイスを選択して、ダブルクリックもしくは構成ボタンをクリックすることで、インターフェイスの設定画面を開きます。



Trusted インターフェイスの設定

設定画面は外部インターフェイスと同様です。インターフェイス名(エイリアス)は任意に設定できます。インターフェイスの種類は「信頼済み」を選択し、このポートに割り当てる IP アドレスと、スラッシュ区切りでサブネットマスクのビット数を入力し設定します。

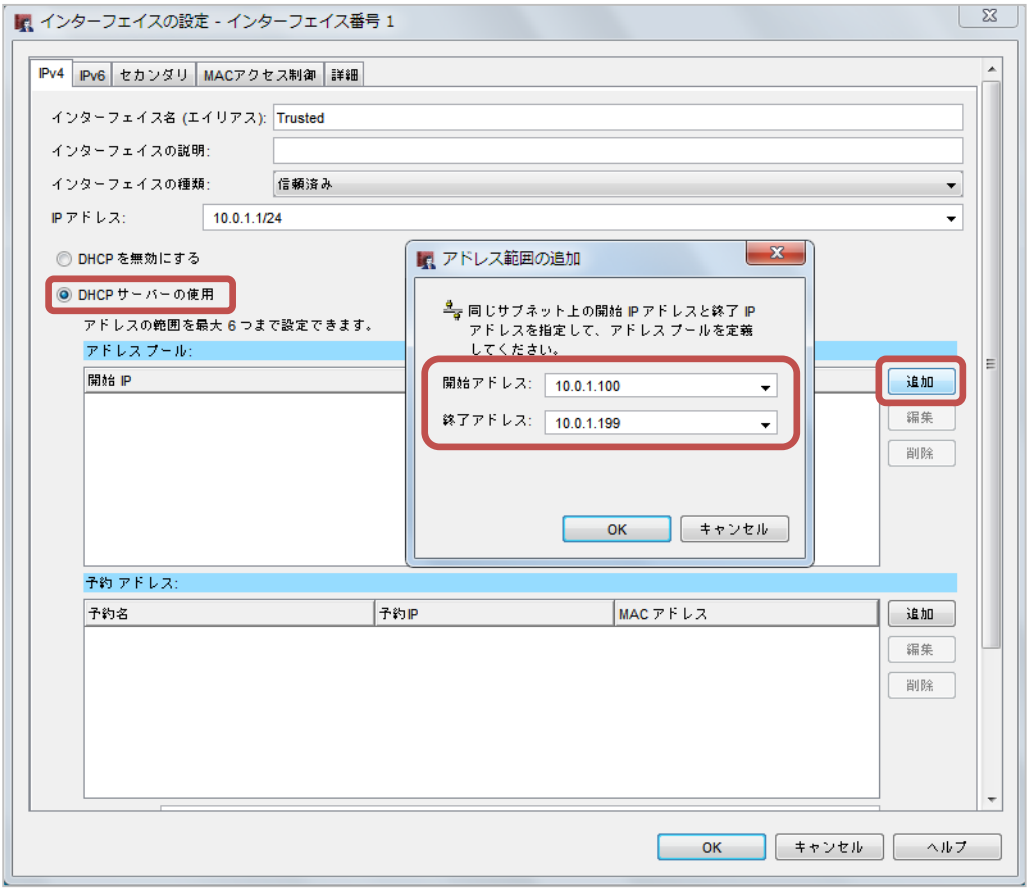


DHCP サーバーの使用

内部ネットワーク下のクライアント PC に IP アドレスを配布したい場合、DHCP サーバーの使用にチェックを入れます。

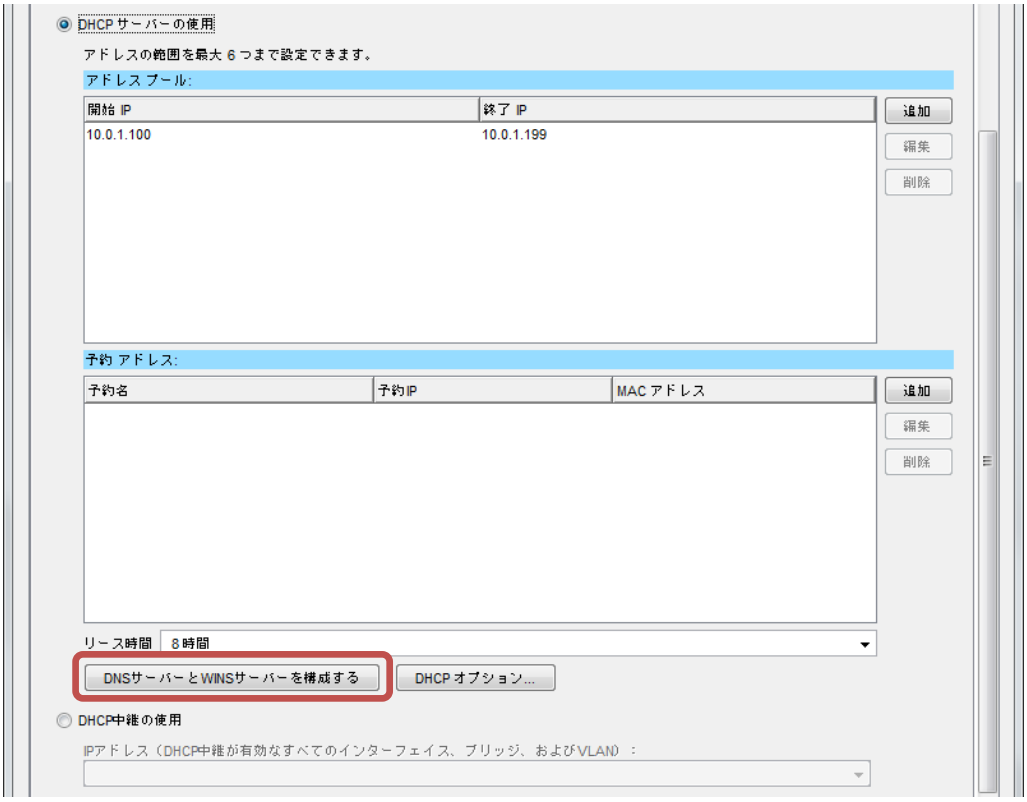
アドレスプールの追加ボタンをクリックし、配布する IP アドレスの範囲を入力します。

例ではセグメント 4 オクテット目の 100 台をクライアントに割り当てる範囲として設定しています。

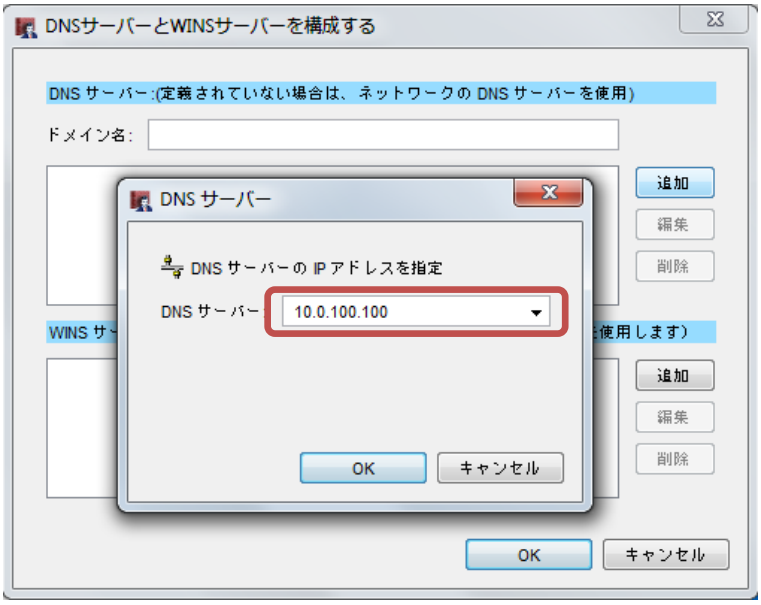


さらに、クライアントは IP アドレスだけでなく名前解決も必要なので、DNS サーバーの情報も配布します。
(次頁)

インターフェイスの設定画面をスクロールバーで下がると、下方に「DNS サーバーと WINS サーバーを構成する」のボタンがあります。これをクリックします。



クライアントに設定したい DNS サーバーの情報を入力します。

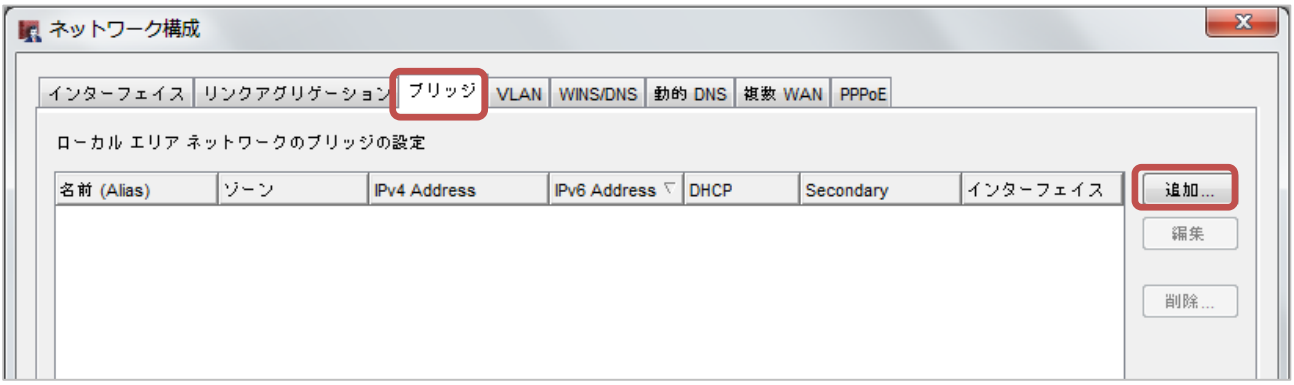


以上で DHCP サーバーが構成できました。

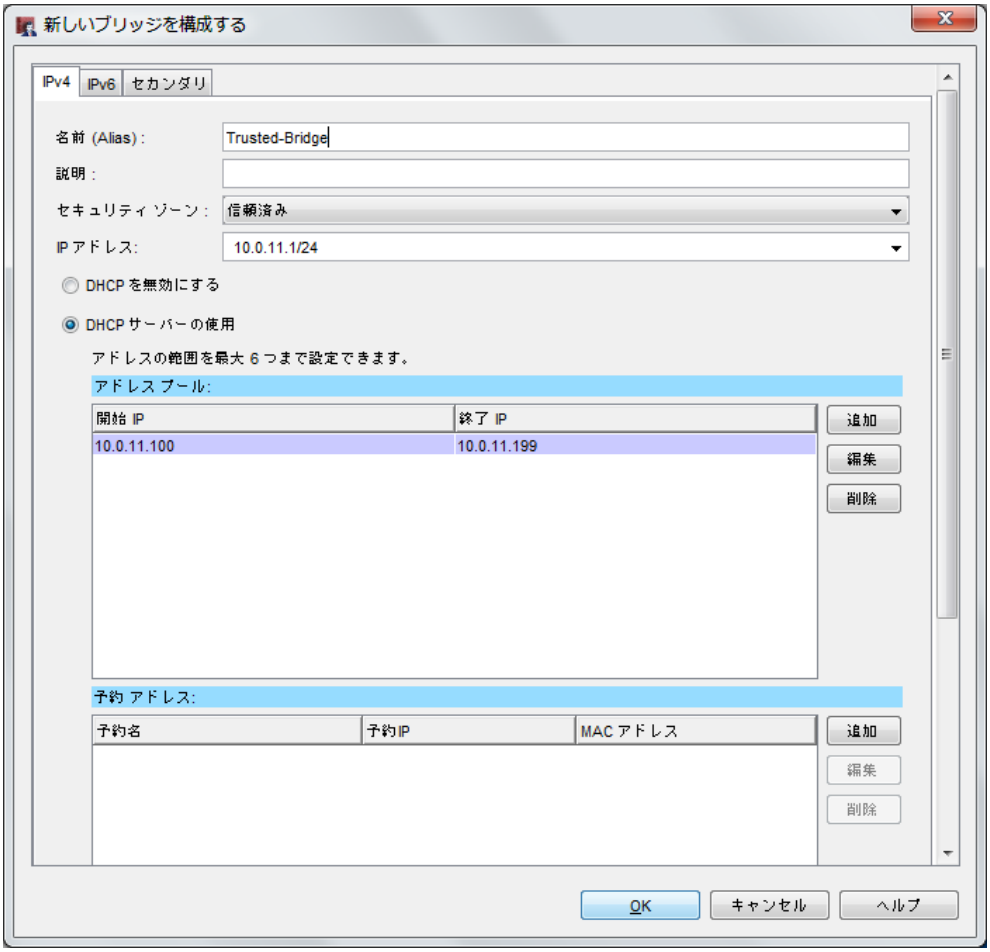
ブリッジの構成

内部ネットワークを、空いているポートの数だけサブネットを分割しても、管理上複雑になる、クライアントの数がそれほどない、同じサブネットでポートを複数使用し負荷を分散させたい・・・といった場合、複数ポートをブリッジで束ねることができます。

ネットワーク構成の画面で「ブリッジ」タブから設定することができます。追加ボタンをクリックします。

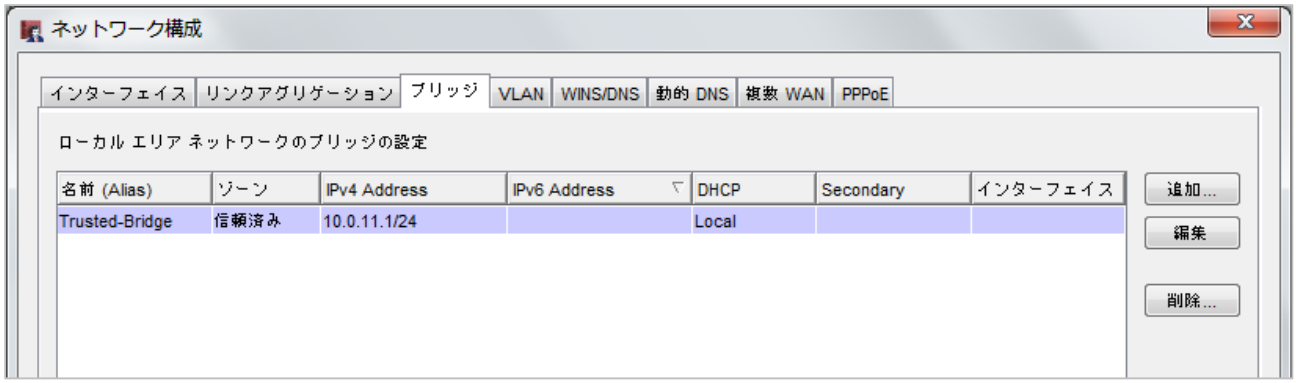


エイリアスや IP アドレス、DHCP サーバーを、Trusted インターフェイスと同じように設定します。



一通り設定したら OK をクリックします。

以上でブリッジが定義されました。

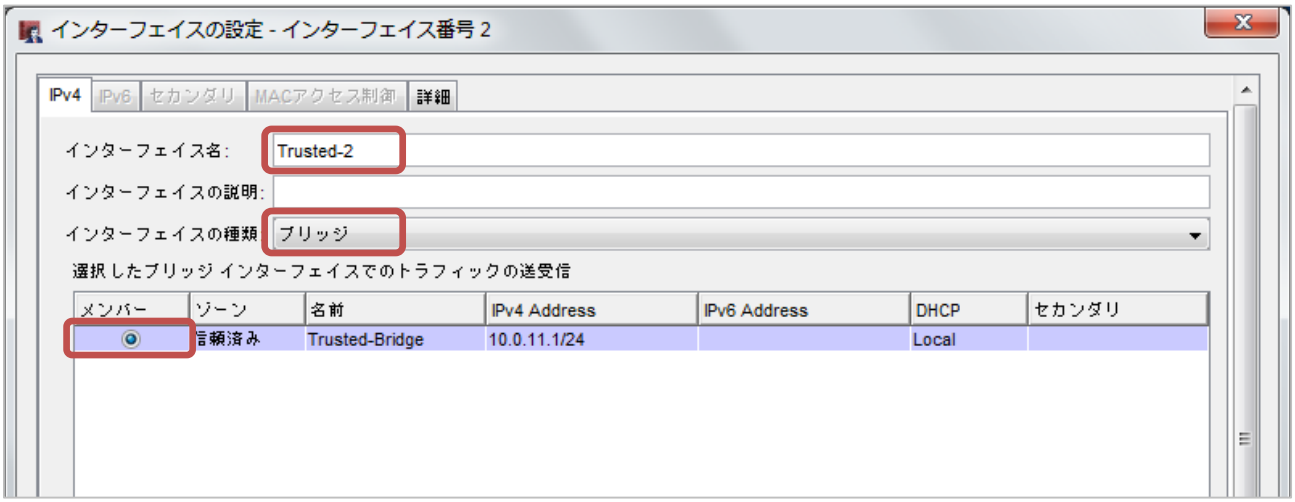


それでは 2 番ポート以降のインターフェイスをブリッジに加えてゆきましょう。

インターフェイス 2 の設定を開き、任意のインターフェイス名をつけます。

インターフェイスの種類は「ブリッジ」にします。

ブリッジの一覧が表示されますので、メンバーになるブリッジにチェックを入れます。



この設定を保存すると 2 番ポートはブリッジのメンバーとなります。

以上の設定を施すと、Trusted は 1 番ポートの「Trusted-1」と、ブリッジに設定した「Trusted-Bridge」の、2 種類が存在することになります。これではポリシーを設定する際に面倒だと思われるかもしれません。しかし、XTM には Any-Trusted というビルトインのエイリアスが存在します。

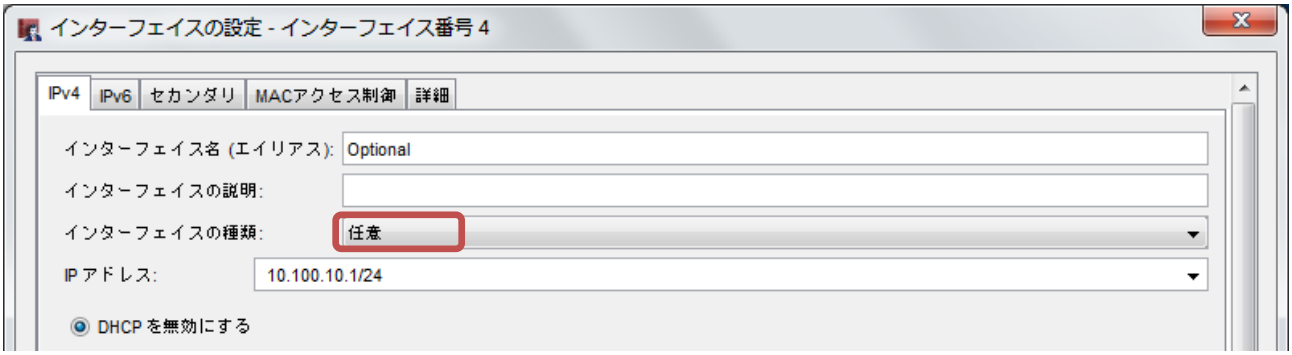
これまでの設定でできた 2 つの Trusted ネットワークはこの Any-Trusted で表わされます。

同様に External や Optional が複数あっても、Any-External や Any-Optional を用いてポリシーを適用することができます。

DMZ を設定する

メールサーバーやウェブサーバーを Trusted とは別の内部ネットワークに設置する場合、Optional ネットワークを定義することができます。

インターフェイスの設定画面の「インターフェイスの種類」を「Optional」(ローカライズされた表記ですと「任意」)を選択します。こうすることによって、Trusted とは違う文字通り任意のネットワーク設定やポリシーを適用することができます。



エイリアスや IP アドレスの設定方法は Trusted の設定と同様です。

NAT 設定 (1-1NAT)

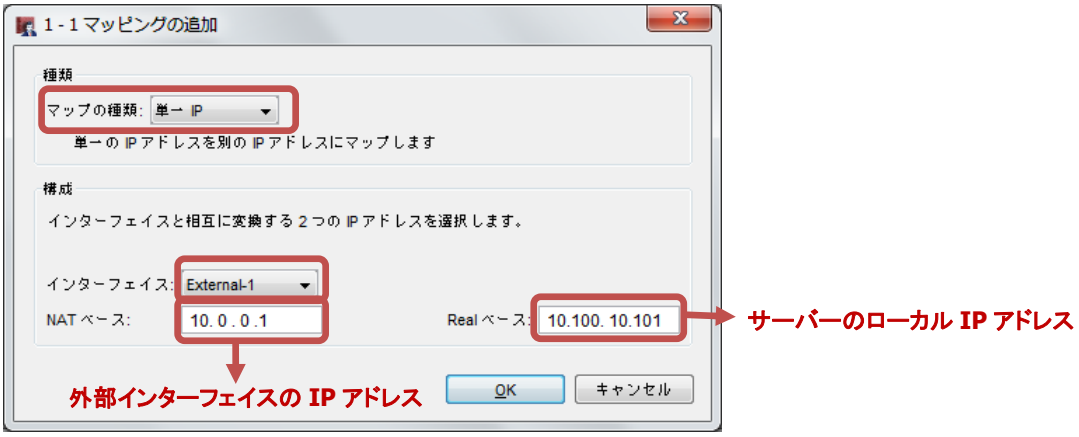
DMZ を設定したら、サーバーへの NAT 設定をしたいと思われるでしょう。その場合、よく用いられるのが 1-1NAT(ワントゥワンナット)です。

ポリシーマネージャのメニュー ネットワーク → NAT をクリックすると、NAT のセットアップ画面が開きます。

1-1NAT タブを選択し、追加ボタンをクリックしてください。

マッピングの追加画面で NAT を設定します。

マップの種類は「単一 IP」(NAT するサーバーが一台)を例にします。



インターフェイス:XTM の外部インターフェイスのエイリアスを選択します。

NAT ベース: 外部インターフェイスの IP アドレス

Real ベース: サーバーのローカル IP アドレス

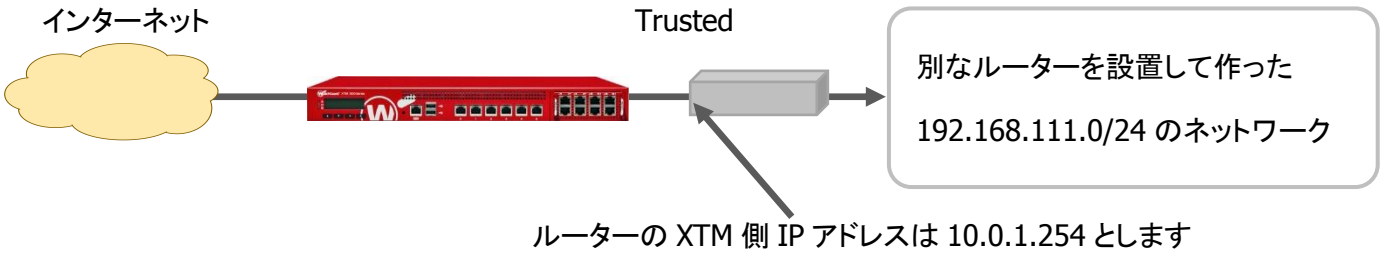
他にもポートフォワーディングも可能な SNAT (Static Nat)の設定もあります。こちらはポリシーの追加時に設定しますので、ファイアウォールの章で取り上げます。

ルーティング設定

XTM の Trusted の背後に別なルーターを置いて、新たにネットワークを構成した場合、そのままでは XTM はそのネットワークの存在を知らないままです。

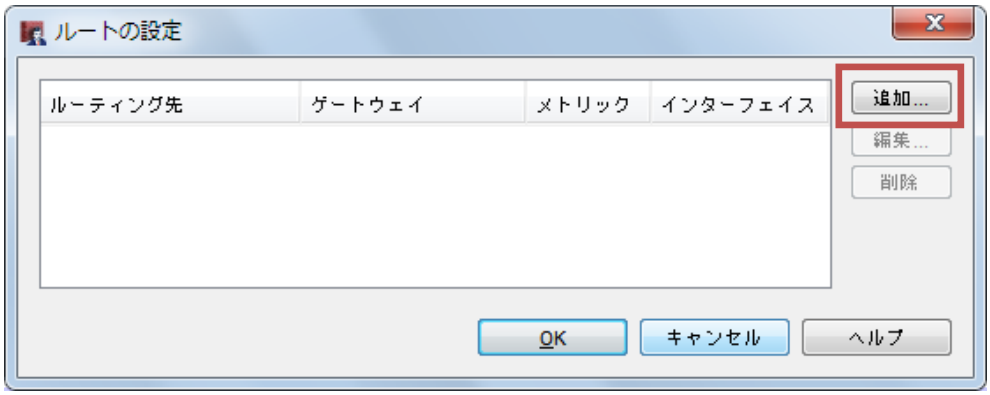
その場合、明示的にルートを設定する必要があります。

例:

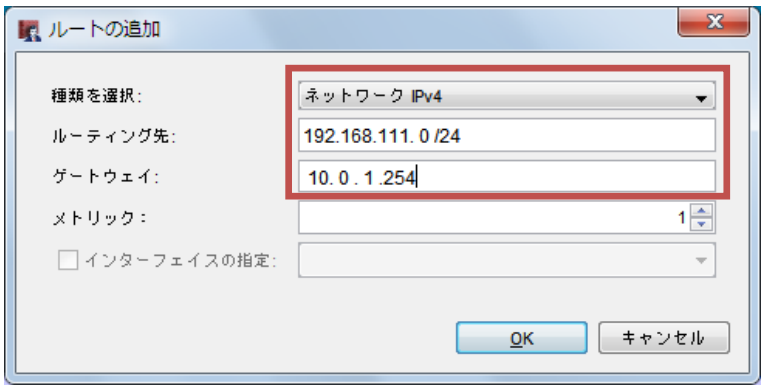


ポリシーマネージャからメニュー ネットワーク → ルート をクリックします。

ルートの設定画面が開くので、追加ボタンをクリックします。



ルートの追加画面で、ルーティング先のネットワークとそこに到達するためのゲートウェイとなる IP アドレスを入力します。



第四章　ファイアウォールの設定　～　パケットを自在に操ろう！

基本的なネットワークが設定できたら、今度は XTM をファイアウォールとして構成してゆきましょう。

ファイアウォールとしての観点から、ポリシーマネージャの画面をあらためて解説します。

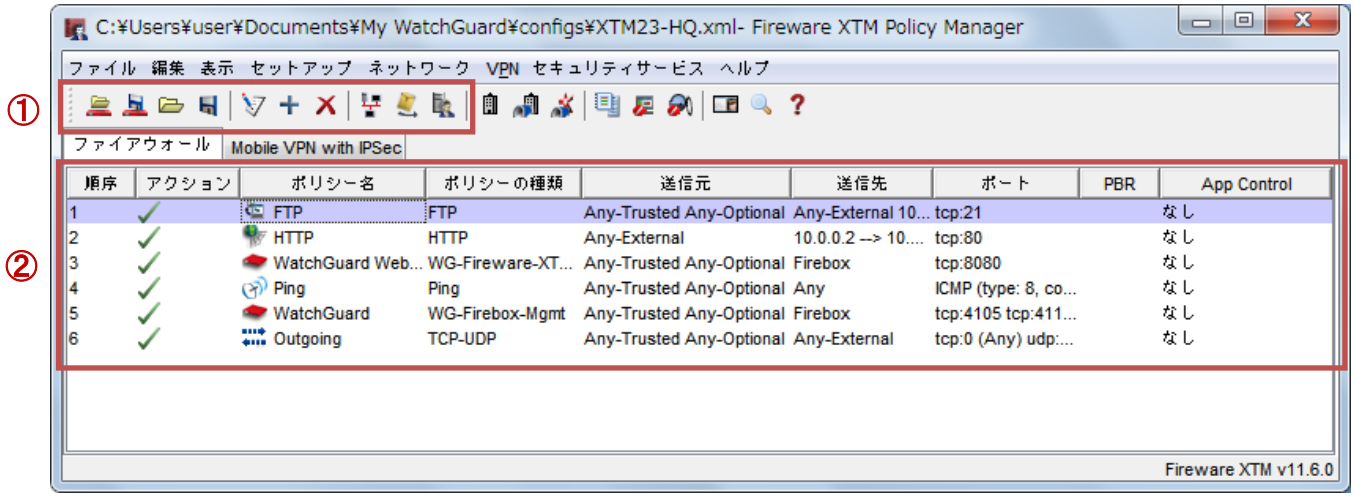
ポリシーマネージャついて

ポリシーマネージャの画面構成

ファイアウォールおよびプロキシのルールは、すべてこのポリシーマネージャから設定します。

① ツールバー　：よく使うメニューは、このツールバーにアイコンで配置されています。

② ポリシー一覧　：設定されたファイアウォールおよびプロキシポリシーはすべて表示されます



ポリシー一覧の各カラムの意味を以下に説明しておきます。

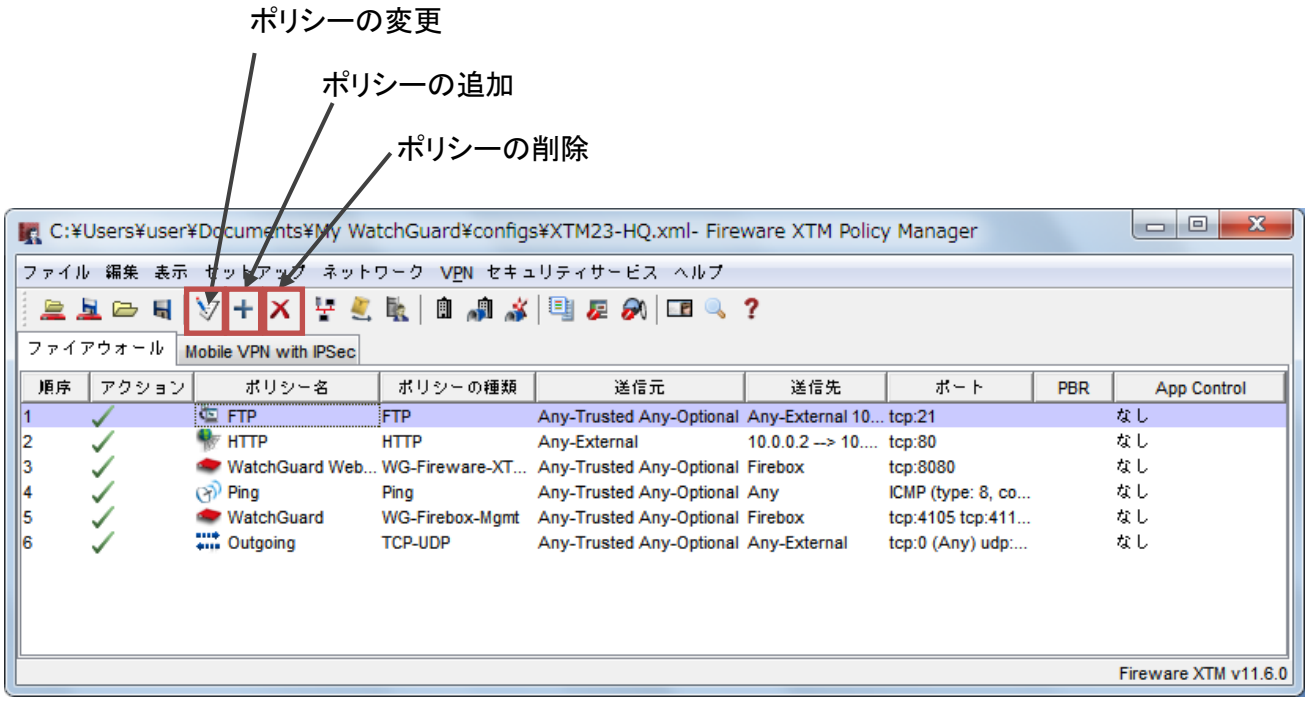
順序	ポリシーの評価順序です。上から順に評価され、マッチしたルールが適用されます
アクション	ポリシーの有効/無効、ログ記録、スケジュールなどが表示されます
ポリシー名	ポリシー作成時、任意で命名できます。後から変更することも可能です
ポリシーの種類	プロトコルまたは通信の種類です
送信元/送信先	送信元/先がエイリアス、IP/ネットワークアドレス、SNAT、ユーザーなどで表示されます
ポート	プロトコルとポート番号で表示されます。ポートの 0 はすべてのポート番号が対象です
App Control	アプリケーションコントロールの有効/無効が表示されます

ポリシーの変更/追加/保存

既存のポリシーを変更する際には、該当のポリシーを選択しダブルクリック、もしくはポリシーの変更ボタン  をクリックします。

ポリシーの追加は  ボタンをクリックします。

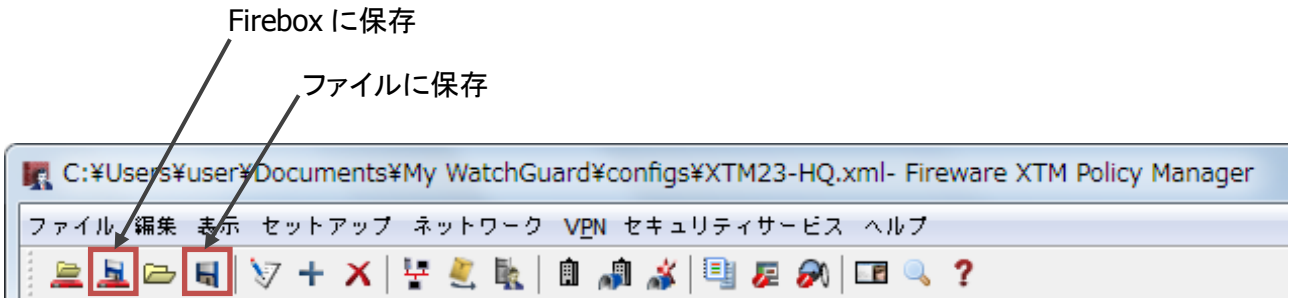
削除は該当のポリシーを選択して  ボタンをクリックします。



ポリシーの保存

設定したポリシーを本体に反映させたい場合は、Firebox に保存ボタン  をクリックします。[3]

ポリシーをファイルで保存したい場合は、ファイルとして保存するボタン  をクリックします。



[3] 保存の手順は、第三章の「設定の保存」の節をご覧ください

ポリシーの追加

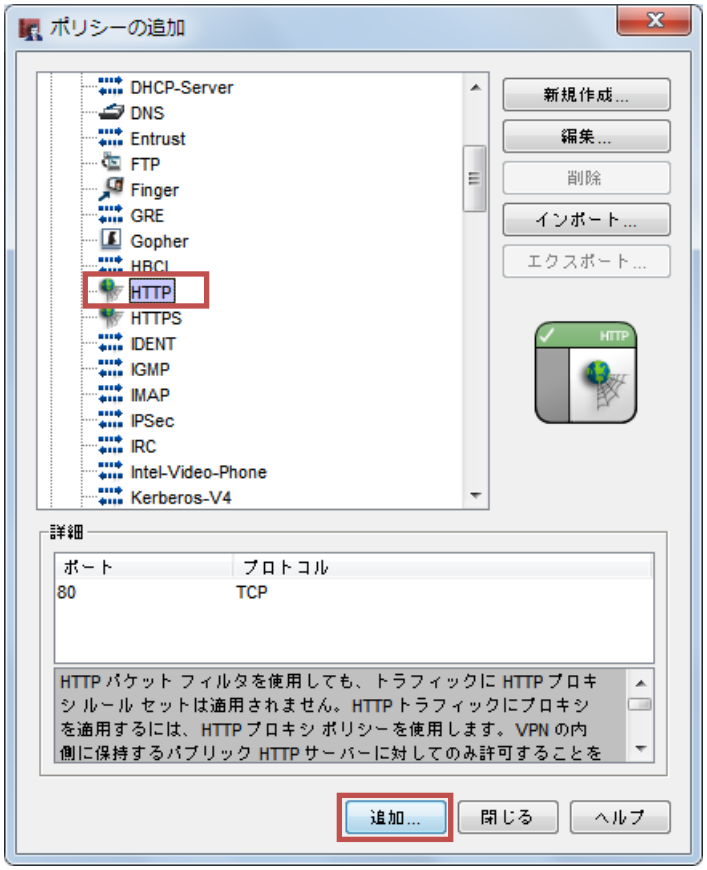
それでは実際にポリシーを追加してみましょう。

ポリシー追加 （内側から外側へ）

一例として、LAN 側から外にインターネットを見に行けるよう、HTTP 通信を許可するポリシーを作成してみます。ツールバーの「ポリシーの追加」ボタンをクリックします。

※ 実際は「Outgoing」ポリシーがあるため、HTTP の許可ポリシーがなくても Web の閲覧はできます

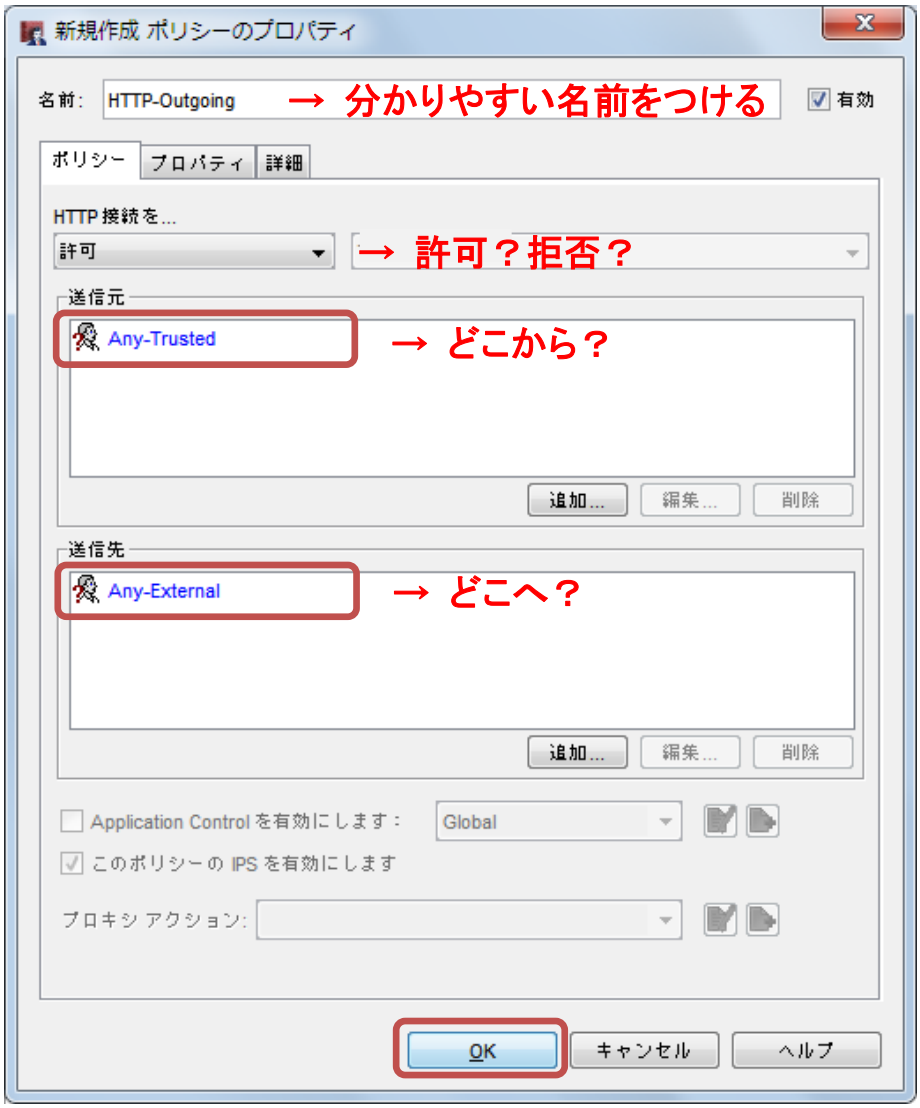
ポリシーの追加画面が開いたら、目的のプロトコルを選択し、下方の追加ボタンをクリックします。



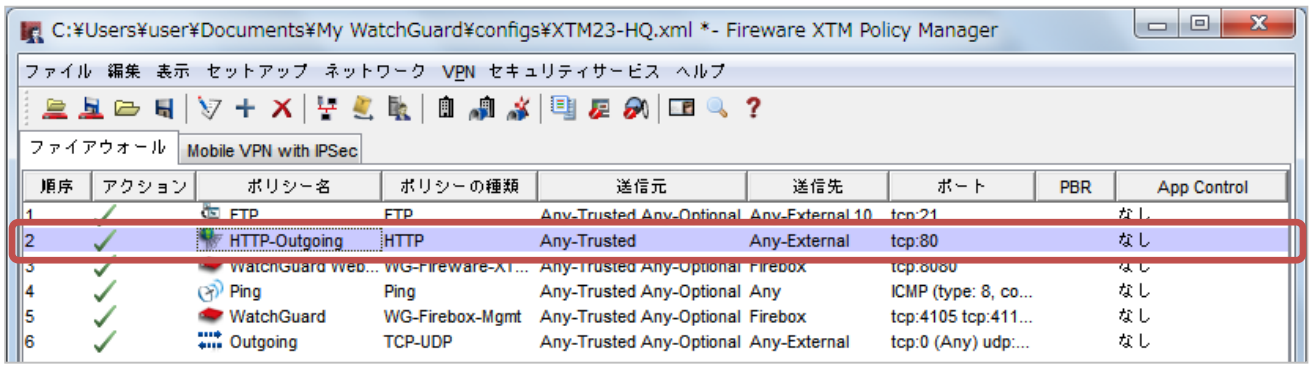
すると、新規作成ポリシーのプロパティが開きます（次頁）。

ポリシーの名前は分かりやすいものをつけることができます。

内側から外側への HTTP アクセスを許可するので、以下のデフォルト状態で OK をクリックします。



ポリシーの追加画面を閉じ、ポリシーマネージャに戻ってみると、新しいポリシーが追加されています。



ポリシー追加 （外側から内側へ）

ネットワーク設定の章では DMZ を作るため、最後のポートを Optional にして設定しました。

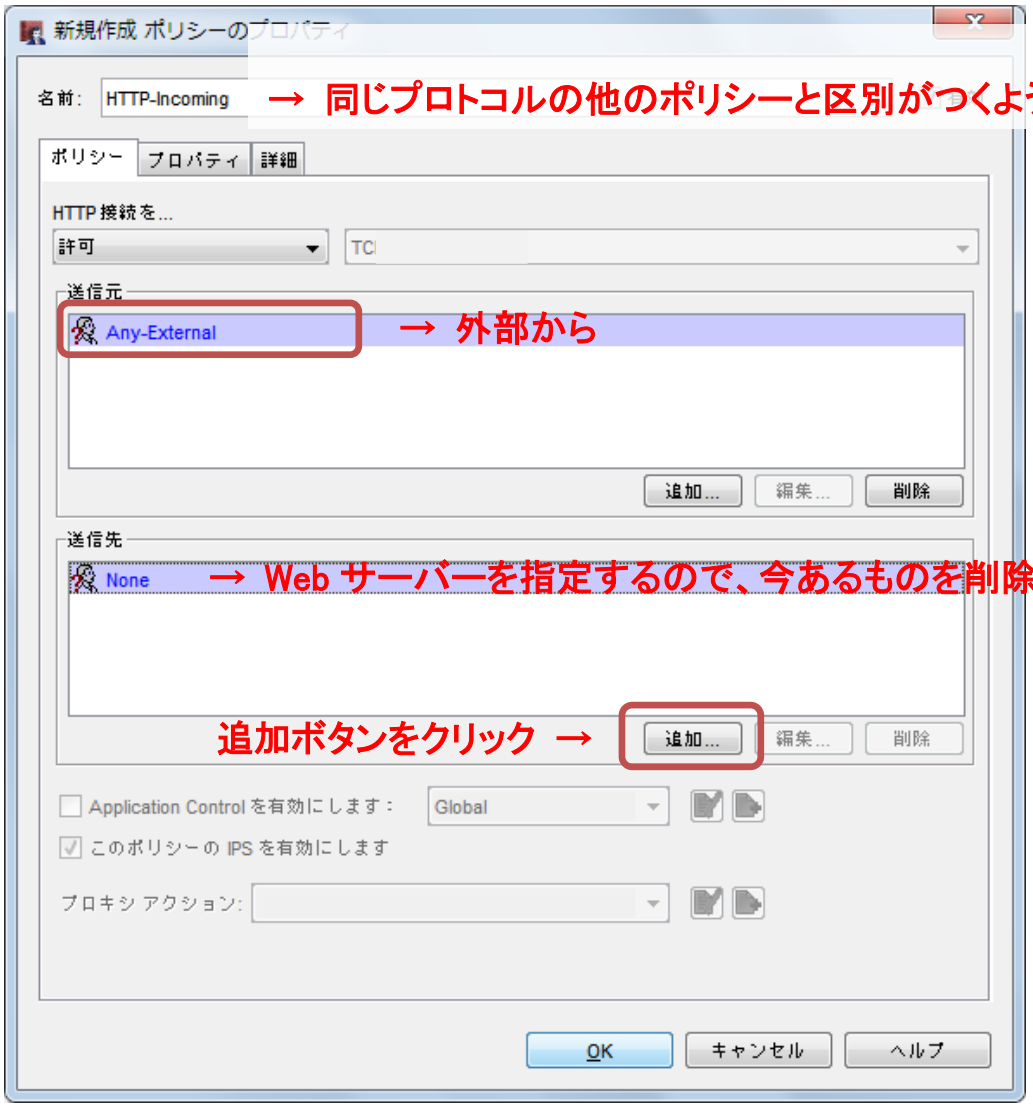
そこに Web サーバーがある前提で、外側からのアクセスを許可する設定をしてみましょう。

Web サーバーは 10.100.10.110 とします。

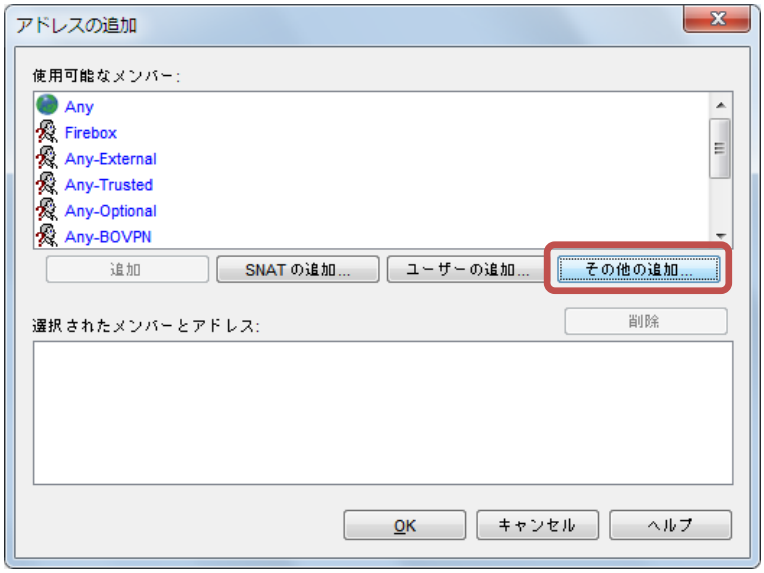
前項と同じようにポリシーの追加画面で HTTP を選び追加ボタンをクリックし、ポリシーの新規作成画面を開きます。

名前は分かりやすいものをつけます。すでに同じ HTTP で内→外のポリシーを追加したので、外→内は HTTP-Incoming など区別がつくように命名するとよいでしょう。

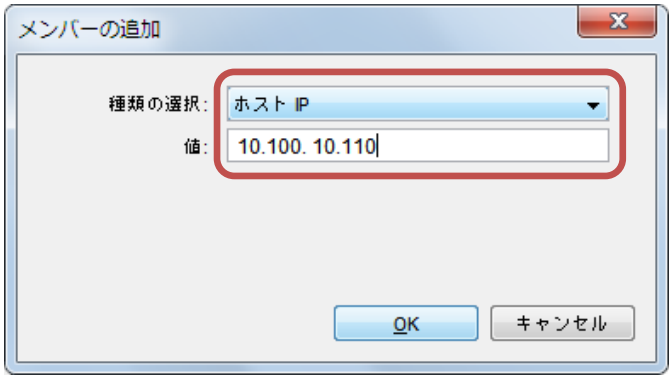
送信元は Any-External、送信先は Web サーバーなので、追加ボタンをクリックして、IP アドレスで指定します。



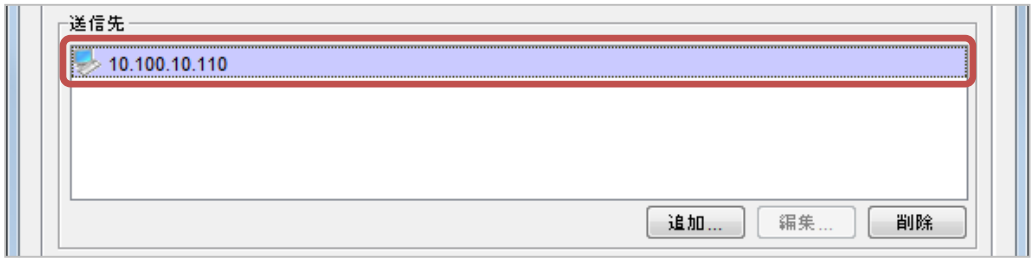
アドレスの追加画面では、その他の追加ボタンをクリックします。



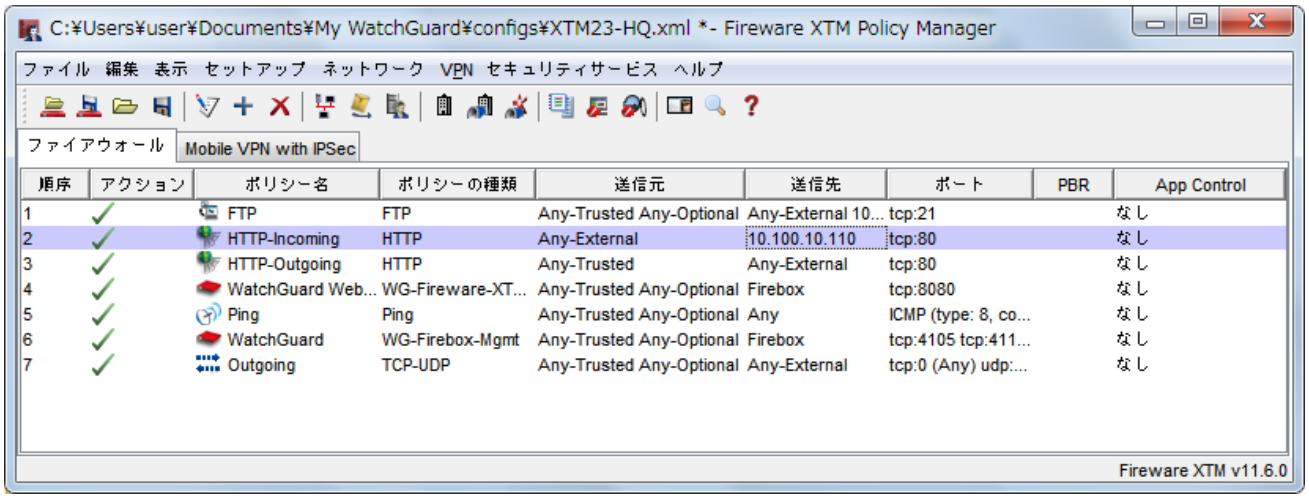
メンバーの追加画面では種類の選択ではホスト IP、値は Web サーバーの IP アドレスを入力して OK。



OK で抜けてポリシーの新規作成画面に戻ると、以下のように送信先が設定されます。



ウェブサーバーにアクセス許可するポリシーが作成されました。



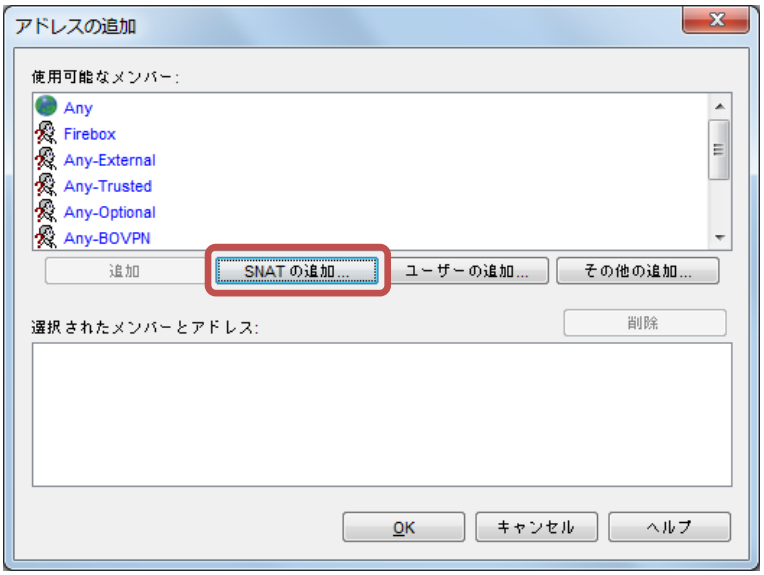
ポリシー追加 （SNAT で外側から内側へ）

前述の設定は、1-1 NAT が前提の設定でしたが、ポリシー単体で NAT を設定することもできます。

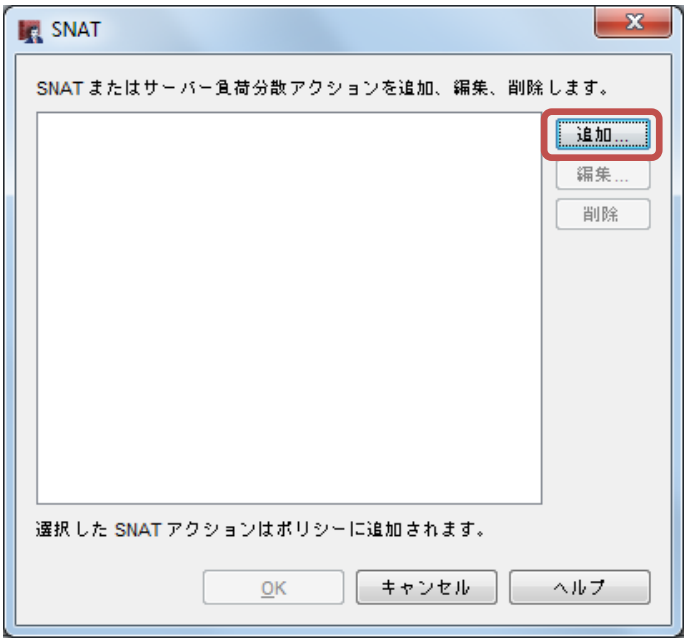
それが SNAT(Static NAT)と呼ばれ、ポートフォワーディングも設定できます。

ポリシーの追加ボタンをクリックし、前項同様に名前や送信元を設定します。

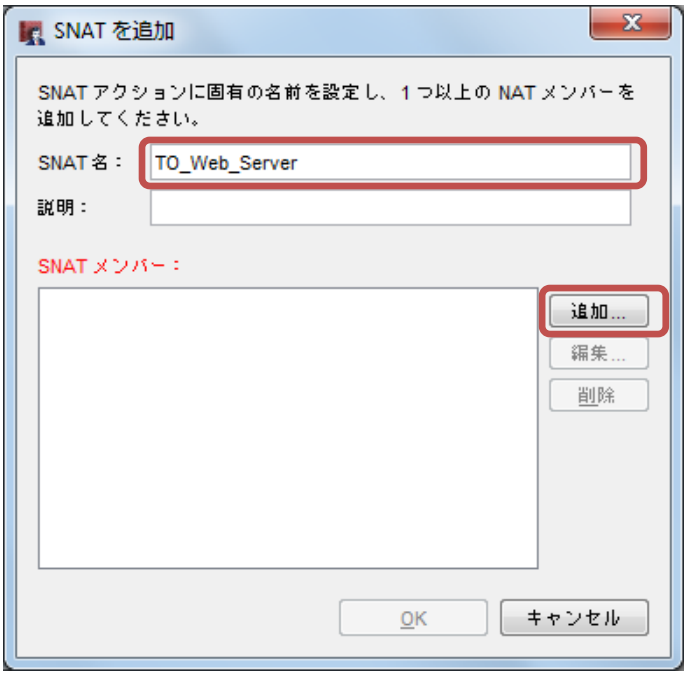
送信先の追加ボタンをクリックし、SNAT ボタンをクリックします。



SNAT 画面で追加ボタンをクリックします。

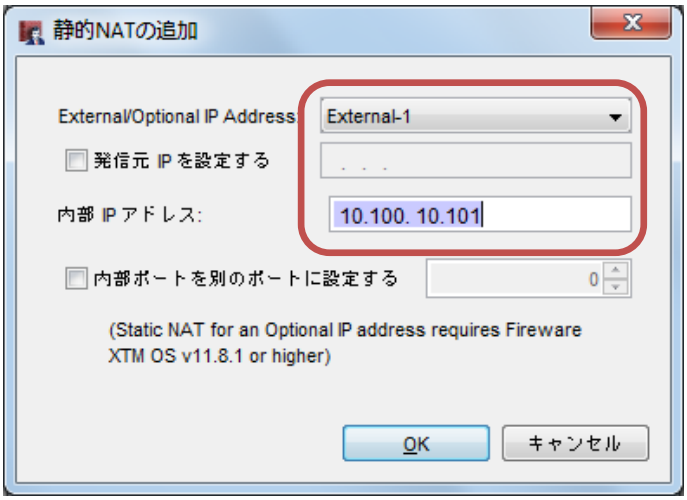


SNAT を追加画面で SNAT 名を入力し、追加ボタンをクリックします。



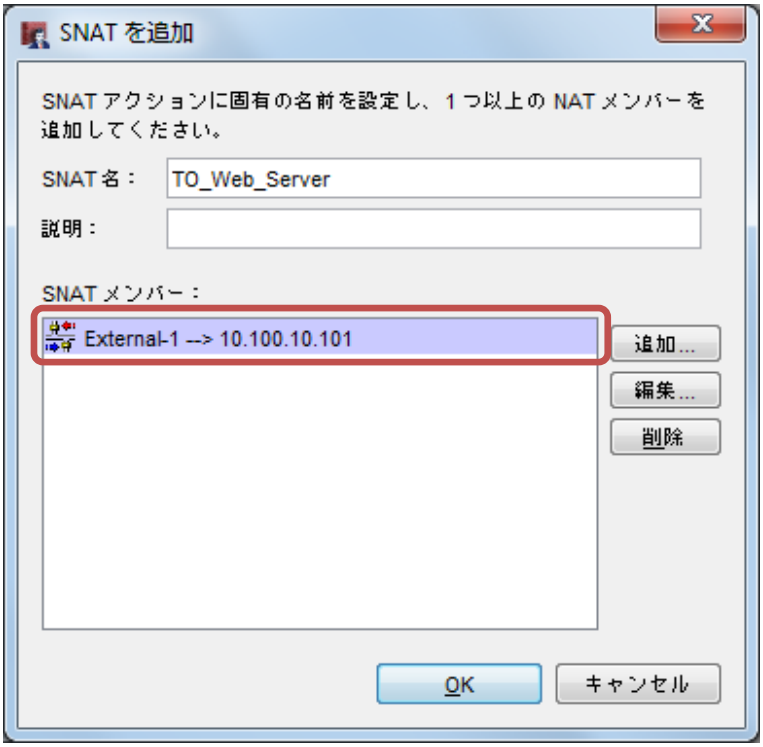
外部 IP アドレスは IP アドレスかエイリアスを選択します。

内部 IP アドレスは Web サーバーの IP アドレスを入力します。

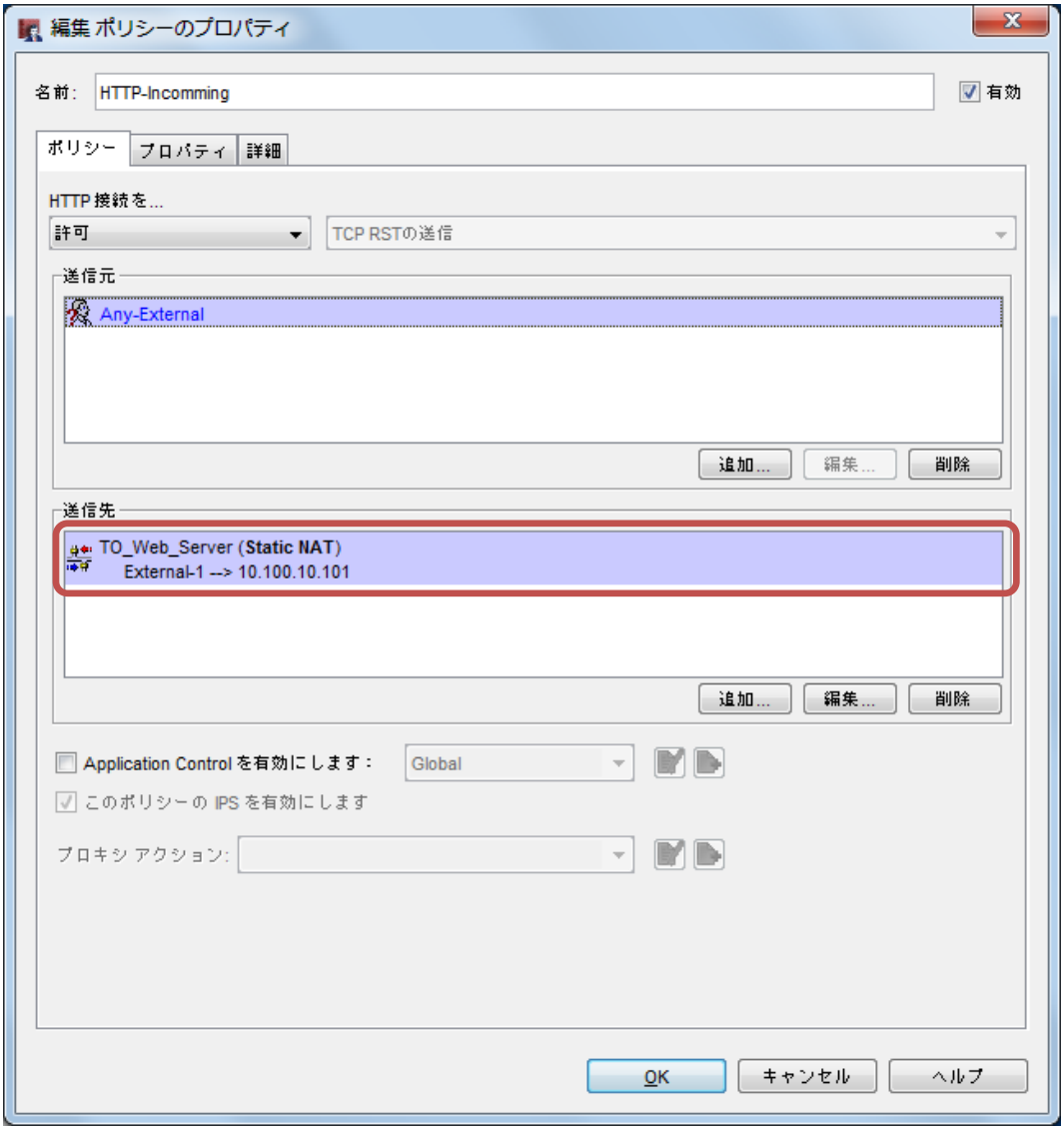


ポートフォワーディングをしたい場合は「内部ポートを別のポートに設定する」にチェックを入れ、変換後のポートを指定します。(例:80 番ポートで受けて 8080 にフォワーディングするなど)

OK をクリックし、SNAT を追加の画面に戻ると以下のように SNAT メンバーが追加されています。



OK で抜けてポリシー新規作成の画面に戻ると以下のように送信先が設定されます。

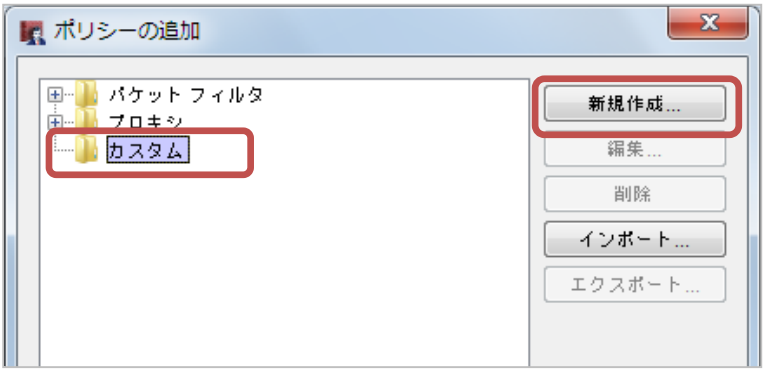


テンプレートにないポリシーを追加する

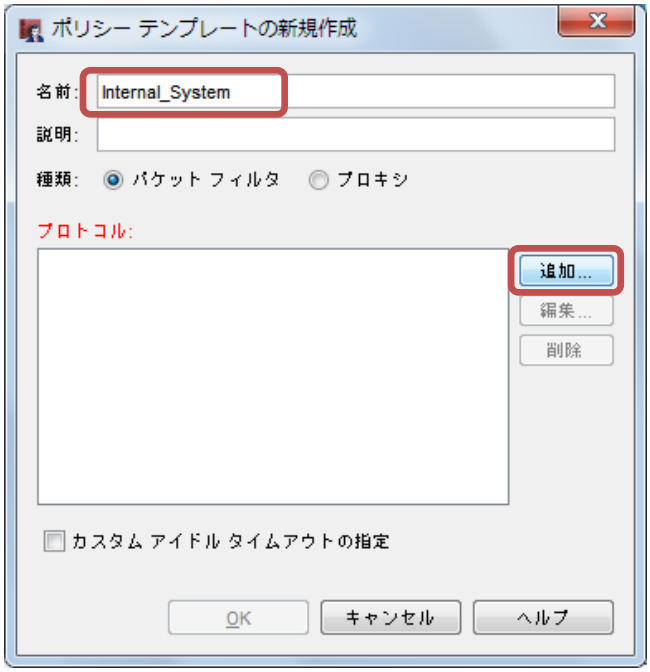
ポリシーの追加画面では、パケットフィルタの下の代表的なプロトコルテンプレートを元にポリシーを作成しました。しかし、内製の社内システムで使うポート番号での通信を制御する場合など、独自のポリシーを作成しなければならないことがあります。

その場合、カスタムでテンプレートを作成することができます。

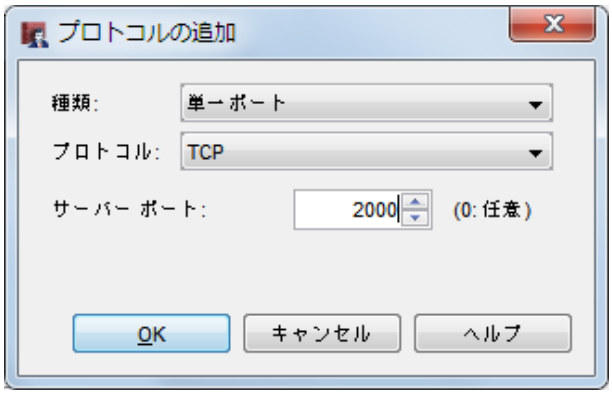
ポリシーの追加画面で、「カスタム」にフォーカスを当てて新規作成ボタンをクリックします。



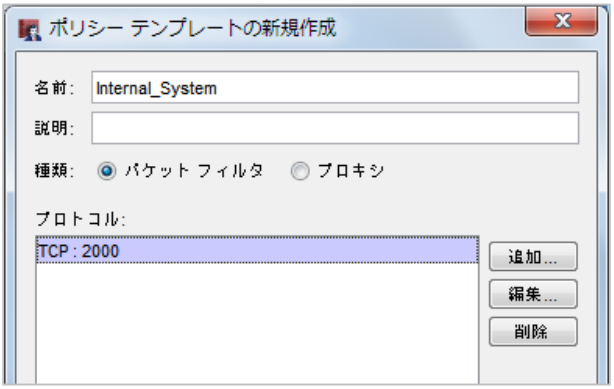
ポリシーテンプレートの新規作成で名前を入力し、追加ボタンをクリックします。



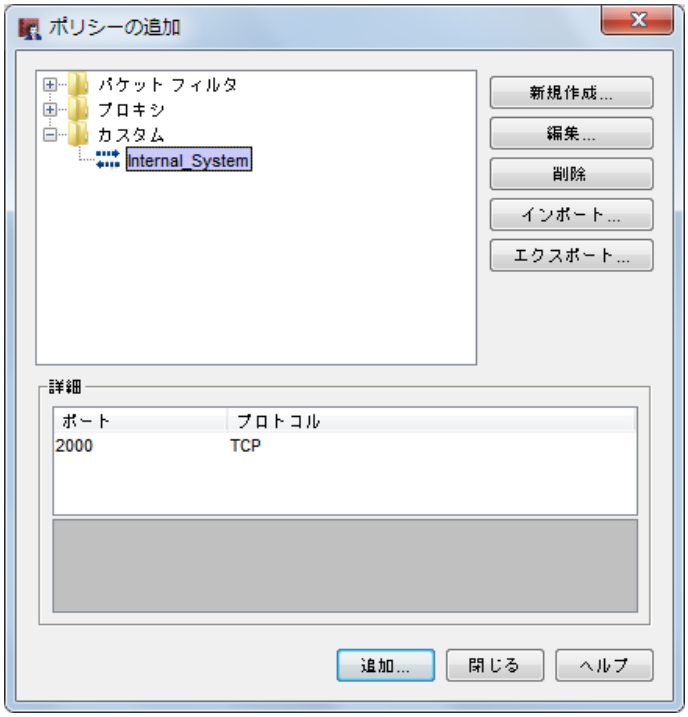
プロトコルの追加で種類とプロトコル、サーバーポートを指定して OK をクリックします。



プロトコルに設定が入ります。



OK で抜けてポリシーの追加画面に戻ると、カスタムポリシーがテンプレートとして登録されています。



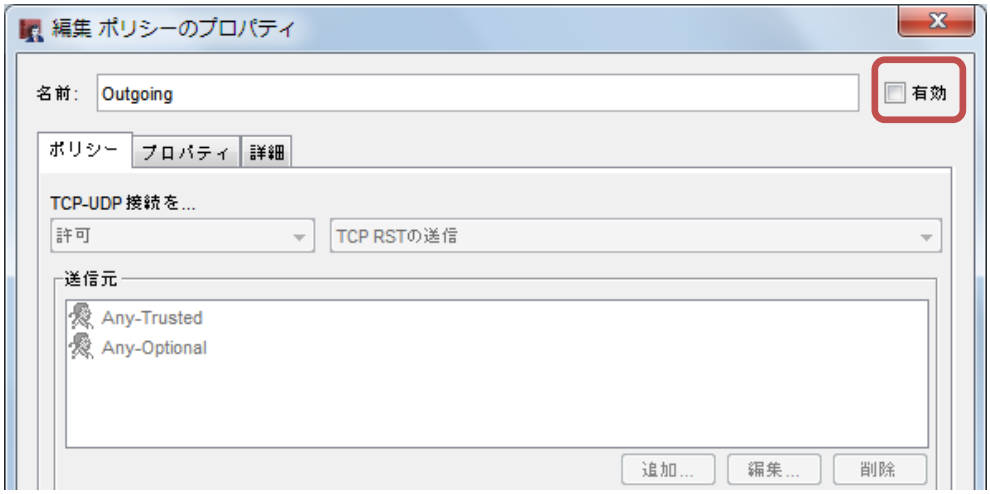
あとはこのテンプレートを使って、前述の手順でポリシーを追加することができます。

ポリシーの編集

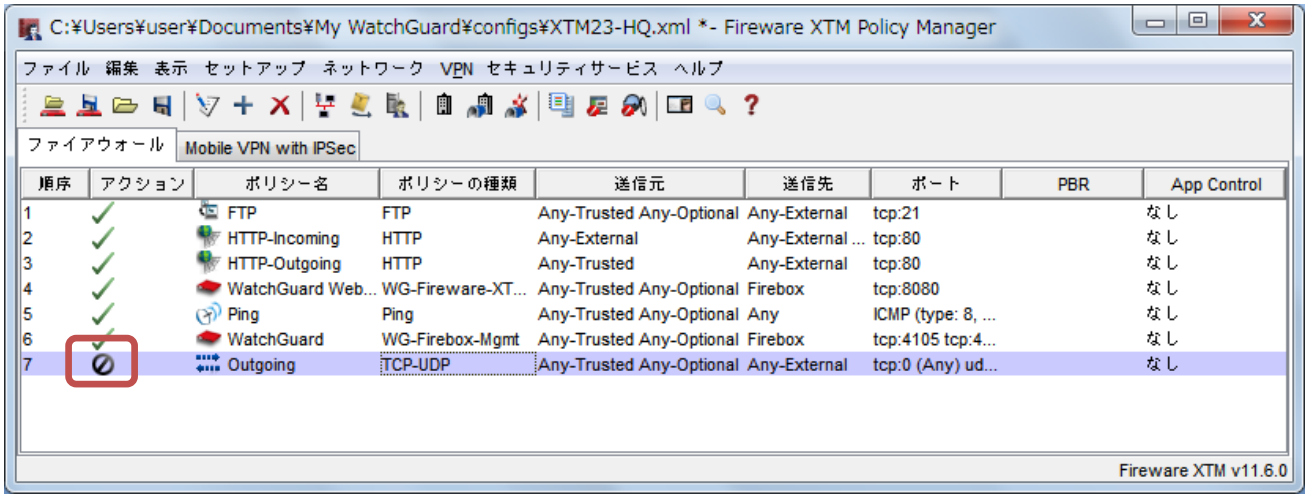
ポリシーの新規作成手順で触れなかった詳細な設定について、いくつかご紹介します。

一時的に無効にする

特定のポリシーを一時的に効かせないようにするには、削除するのではなく、一時的に無効にすることができます。ポリシーのプロパティ画面の右上にある、有効のチェックを外します。



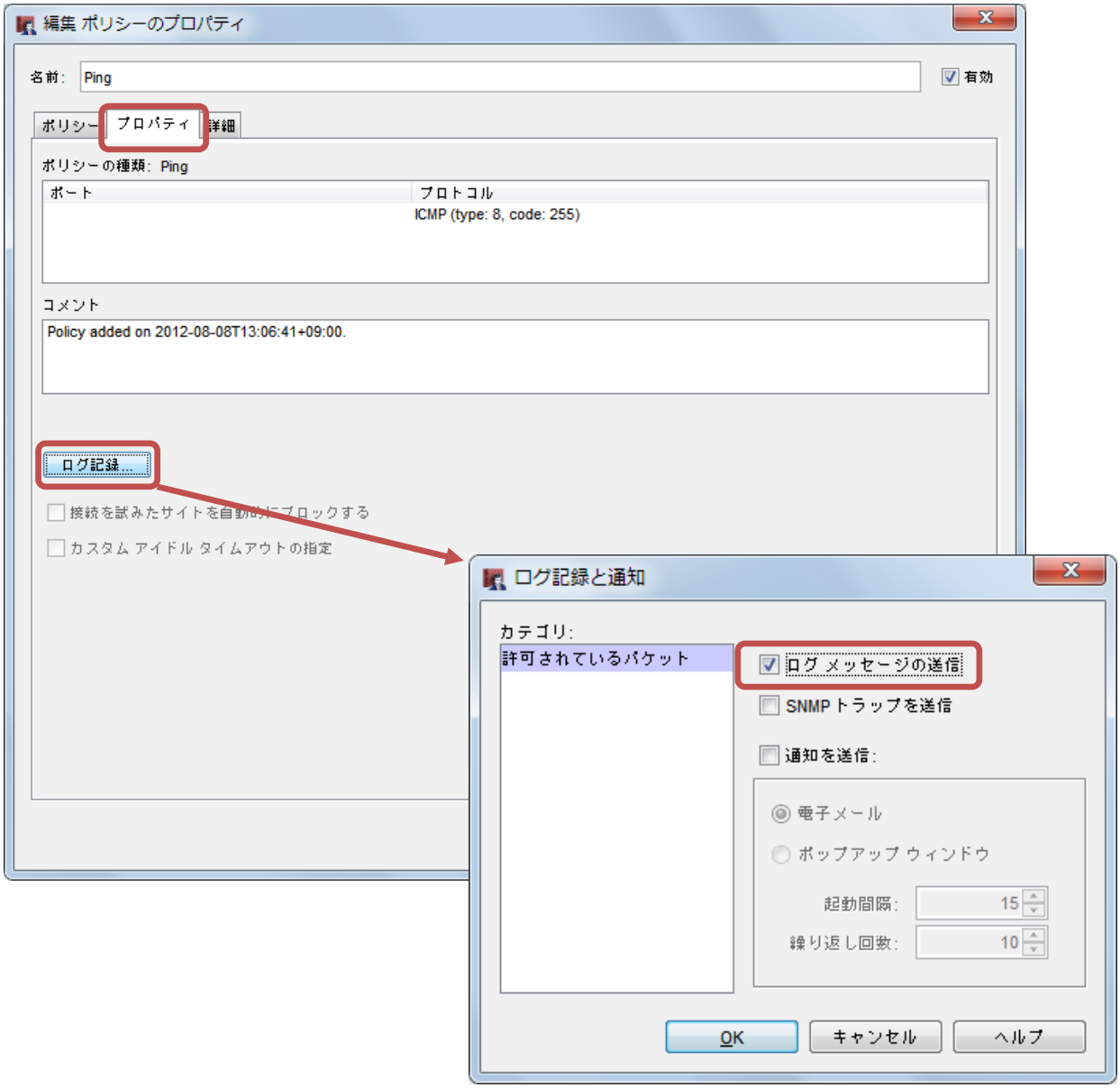
するとポリシー一覧でも無効になったことが分かります。



ログを記録する

ポリシーを設定しても、ログ記録を有効にしないとのログは出力されません。たとえば ICMP を制御するポリシー「ping」がデフォルトで入っていますが、このままでは ping コマンドを実行してもログは残りません。

ログ記録を有効にするにはポリシーのプロパティの「プロパティ」タブにあるログ記録ボタンをクリックします。



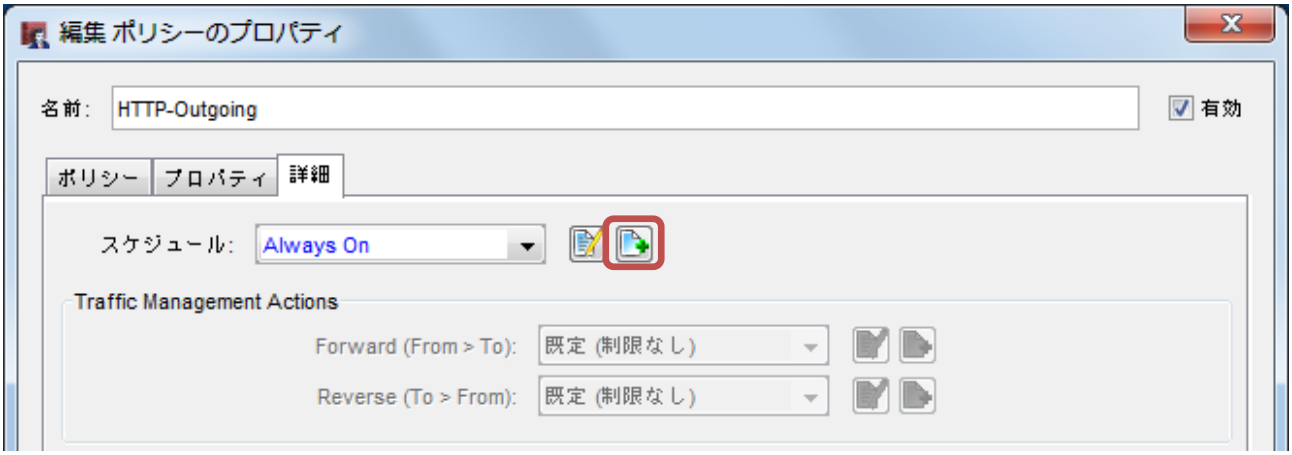
ログ記録と通知画面で「ログメッセージの通信」にチェックを入れます。

この設定により、トラフィックモニターやログサーバーでこのポリシーのログを見ることができるようになります。

運用スケジュールを設定する

指定の時間にのみポリシーが有効となるように、ポリシーの運用スケジュールを設定することができます。

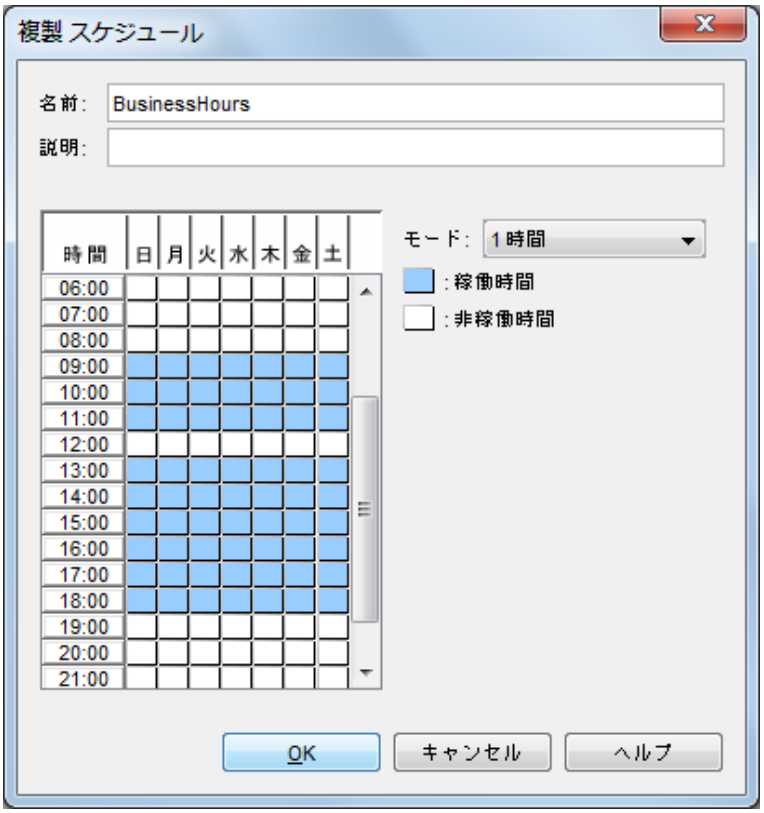
ポリシーのプロパティの「詳細」タブを選択し、スケジュールの新規作成/複製ボタンをクリックします。



名前にはスケジュールの内容が分かるようなスケジュール名を入力します。

稼働時間は「ポリシーが有効な場合」を意味し、非稼働時間は「ポリシーが有効でない場合」を意味します。

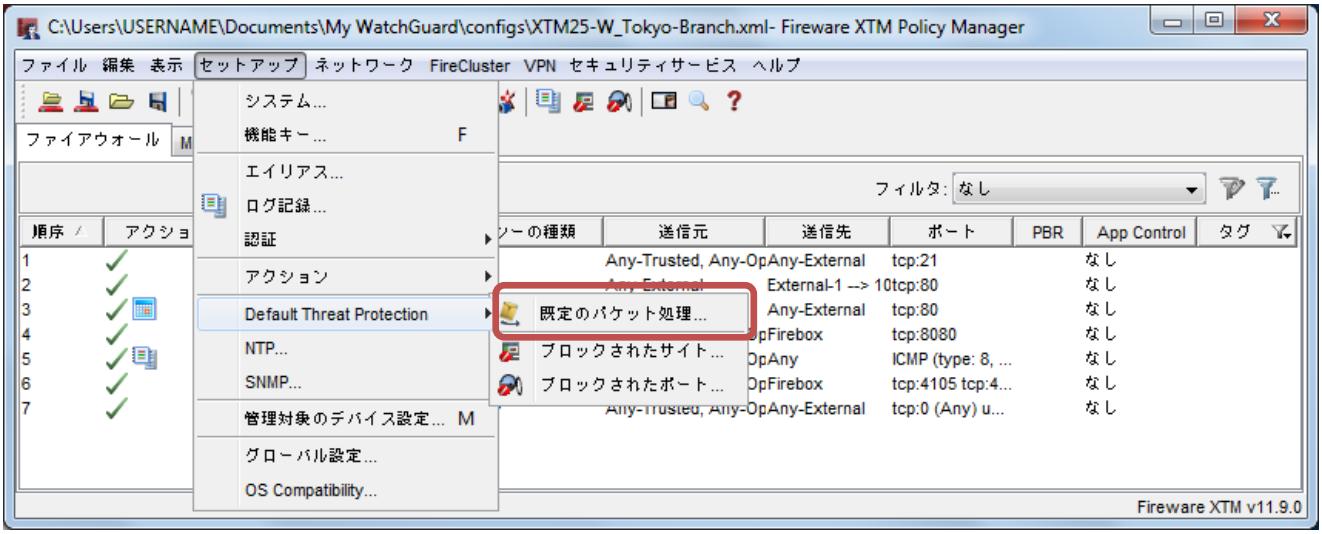
青色/白色をクリックまたはドラッグで反転させて、ポリシーの有効/無効の時間帯を設定します。



作成したスケジュールは、複数のポリシーで利用できます。

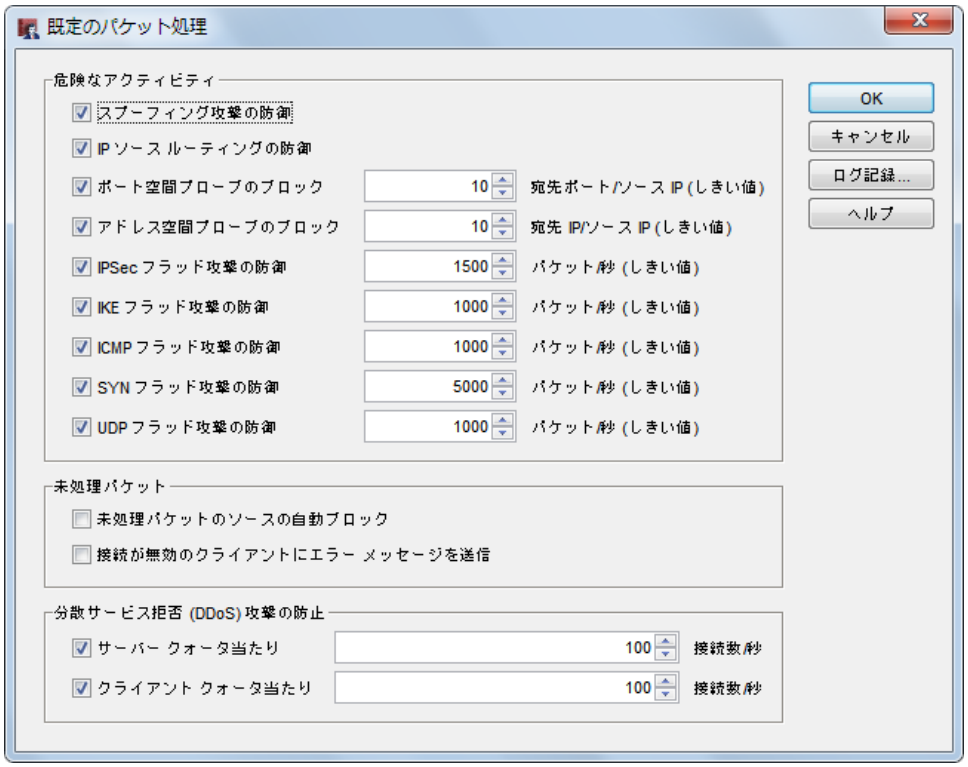
Default Threat Protection

ポリシーマネージャの セットアップ メニューの Default Threat Protection → 規定のパケット処理 をクリックします。



XTM はデフォルトで、DDoS、スプーフィング攻撃または SYN フラッド攻撃の一部である可能性のあるパケットなど、セキュリティ リスクとなる可能性のあるパケットを拒否設定になっています。

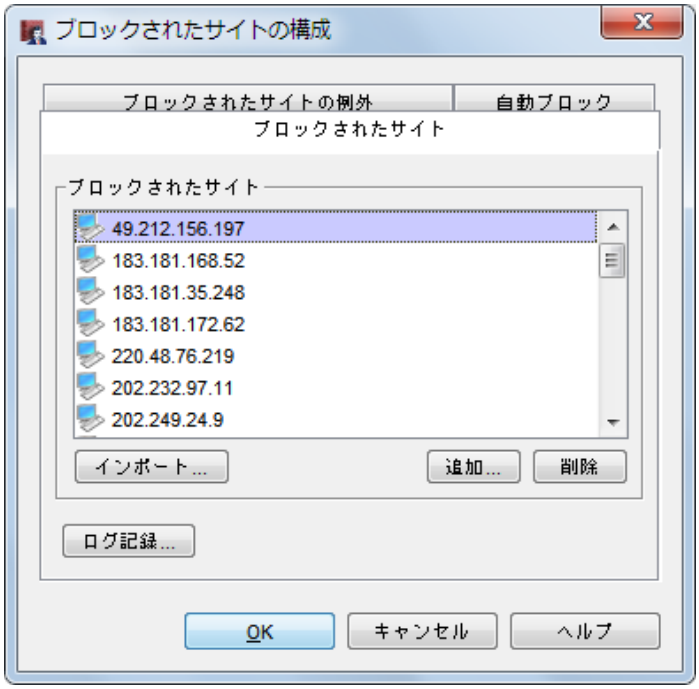
既定のパケット処理の画面からは、攻撃と判断する閾値が設定できます。



Blocked Sites

ポリシーマネージャの セットアップ メニューの Default Threat Protection → ブロックされたサイト をクリックします。

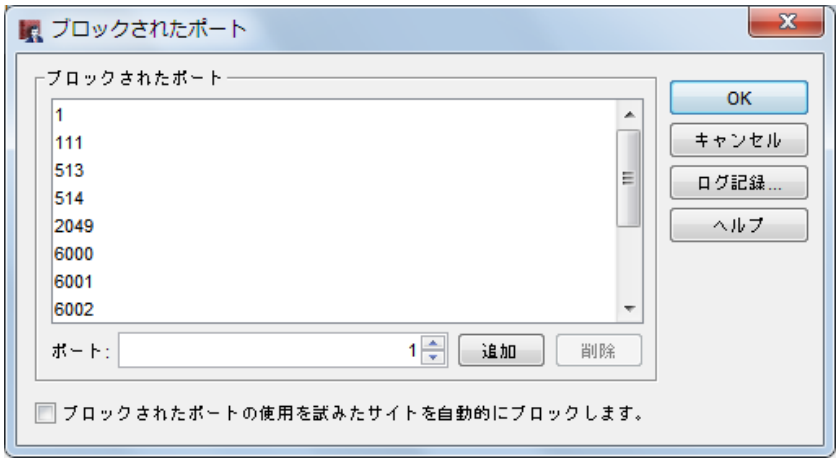
この画面から特定のサイトを登録し、そのサイトへのアクセスをブロックすることができます。



Blocked Ports

ポリシーマネージャの セットアップ メニューの Default Threat Protection → ブロックされたポート をクリックします。

この画面から特定のポートをブロックする設定ができます。なお、ここで設定されているポートでもポリシー上で許可すればポリシー側の設定が優先されます。



第五章　UTM の設定　～　あらゆる脅威に対応しよう

コンテンツフィルタリングやアンチウイルスなど、アプリケーションレベルの脅威に対応する機能を UTM (Unified Threat Management)といいます。

この章では代表的な UTM の機能である、Web Blocker(コンテンツフィルタリング)、Gateway Anti-Virus、spamBlocker の設定方法を解説します。

【豆知識】お得な UTM ライセンスの購入方法

UTM を有効にするためのライセンスは、機能ごとに購入することが可能です。

しかし、もし 2 機能以上(WebBlocker と Anti-Virus の組み合わせ等)のご利用をお考えでしたら、Security Bundle のご購入がお勧めです。およそ 2 機能分のライセンス料ですべての機能を有効にできます。

※　販売価格は販売店にお問い合わせください

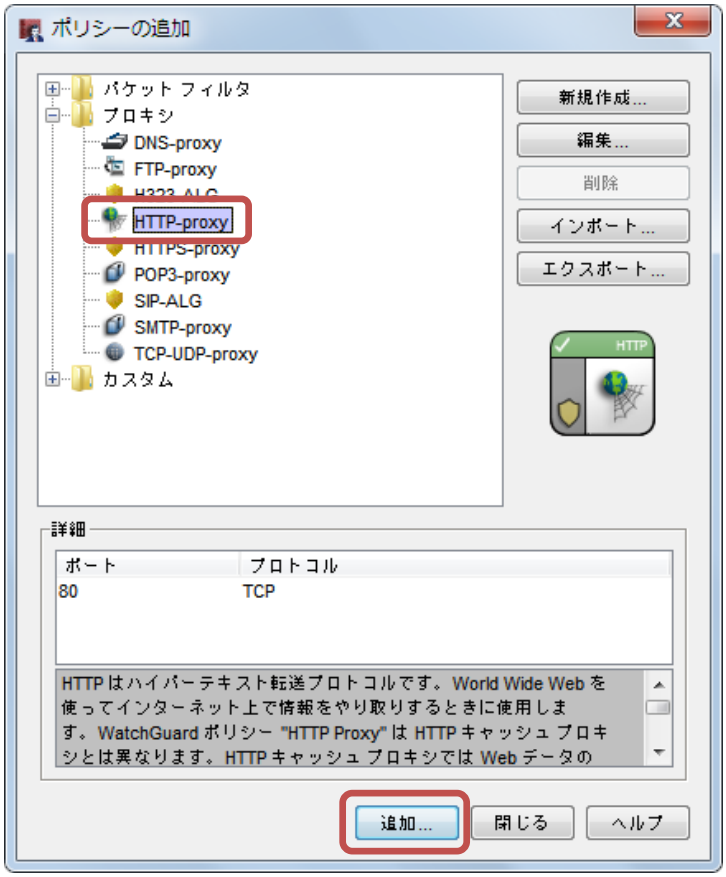
プロキシポリシーの追加

UTM の設定といっても、ポリシー自体はファイアウォール(パケットフィルタ)と同じです。

ポリシーマネージャの追加ボタンをクリックし、ポリシーの追加画面を表示します。

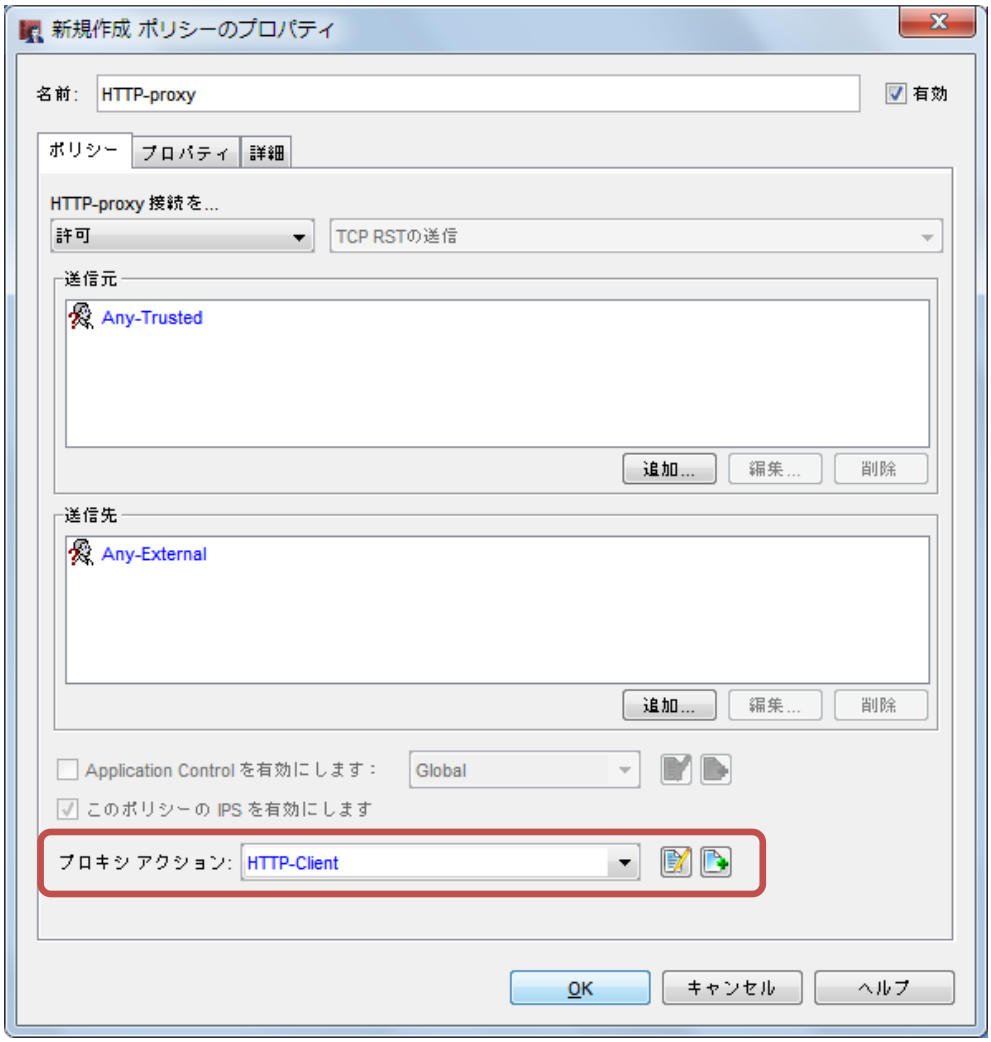
これまでは「パケットフィルタ」ツリーにあるプロトコルを選択していましたが、UTM を設定する場合は「プロキシ」 ツリーにあるテンプレートを選択します。

たとえば、コンテンツフィルタリングを設定する場合は、HTTP 通信上の制御なので、HTTP-proxy を選択し、追加ボタンをクリックします。



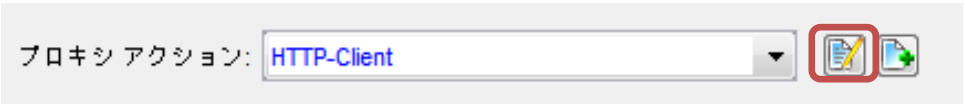
するとファイアウォール設定と同様のポリシーのプロパティ画面が開きます。

ファイアウォールとプロキシの唯一の違いは、プロパティ画面下方の「プロキシ アクション」です。



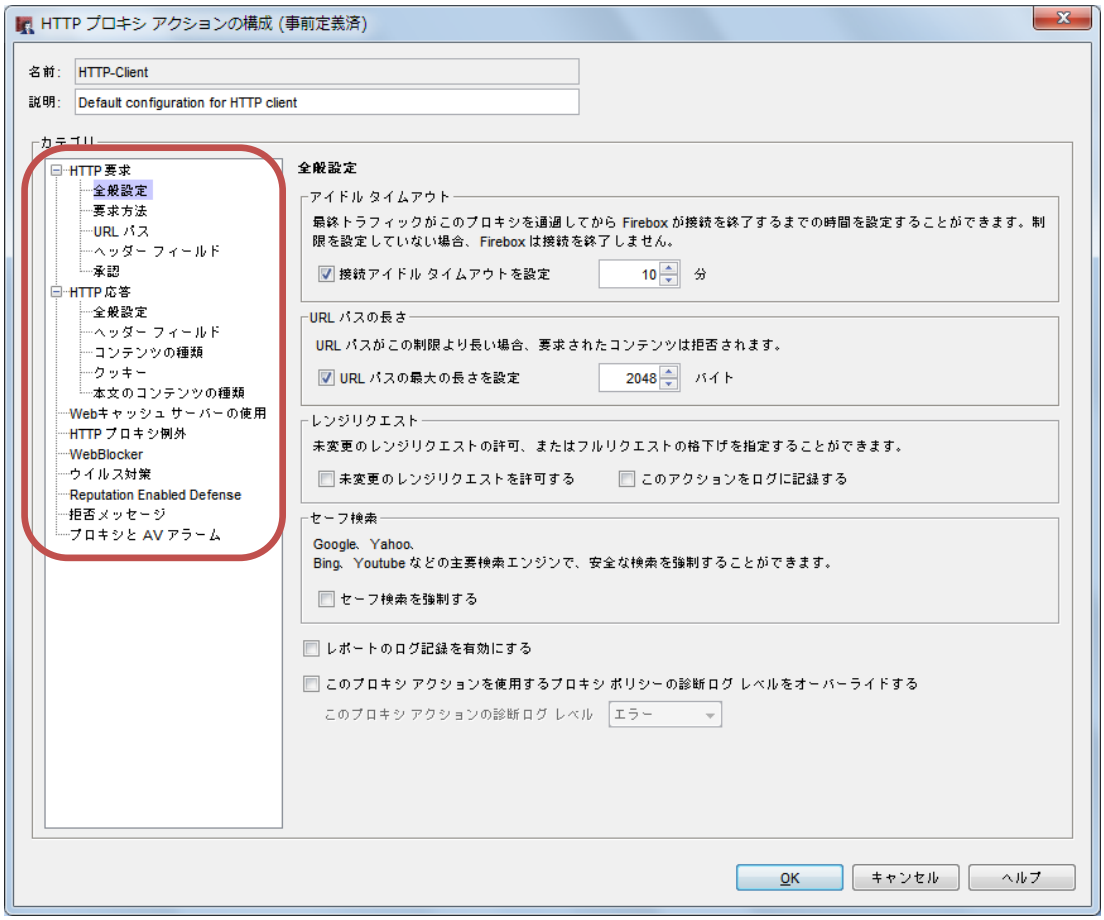
つまり、このプロトコルについては基本的には許可ポリシーですが、通過する際には設定されたアクション(すなわちコンテンツフィルタリングやアンチウイルス)を効かせます、という意味になります。[4]

プロキシアクションの右側の「プロキシの表示/編集」ボタンをクリックすると、それがよく分かります。



[4] プロキシという呼び名ですが、キャッシュサーバーのように機能するわけではありません

プロキシアクションの構成画面が開きますが、左側のメニューには WebBlocker やウイルス対策などの項目があり、このポリシーが適用されたときに、UTM の各機能のアクションが働くことが分かります。

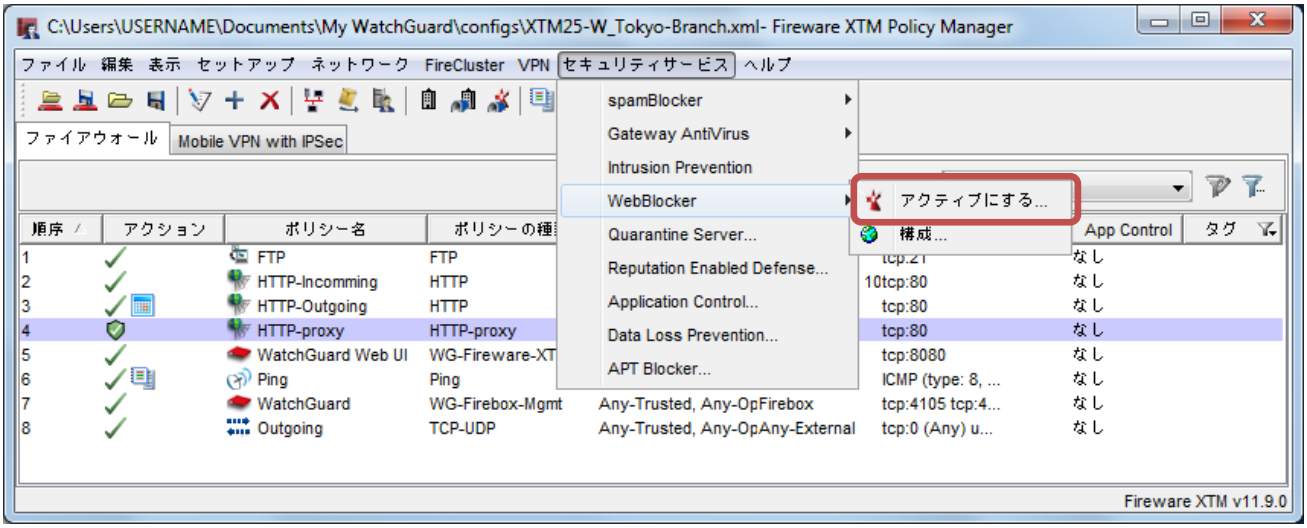


HTTP-proxy ポリシーを追加しただけでは、UTM は有効になりません。

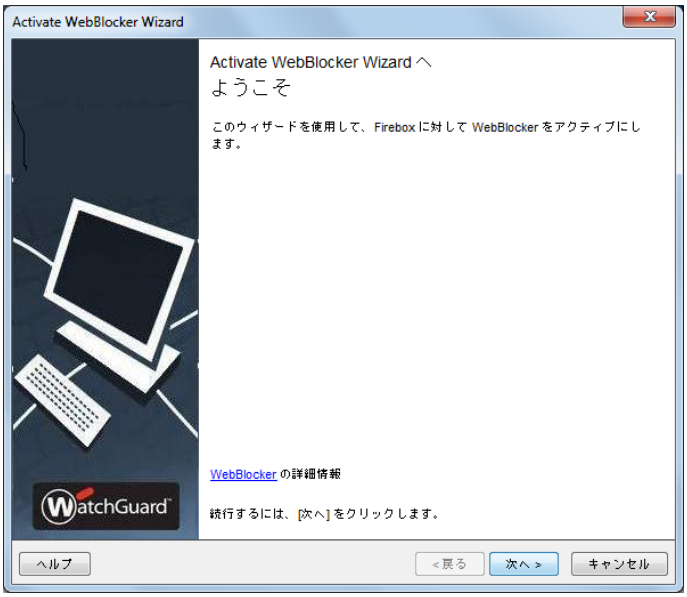
次に、Web Blocker の機能を有効にし、設定してみましょう。

Web Blocker を有効にする

ポリシーマネージャの セキュリティサービス メニュー → WebBlocker → アクティブにする をクリックします。

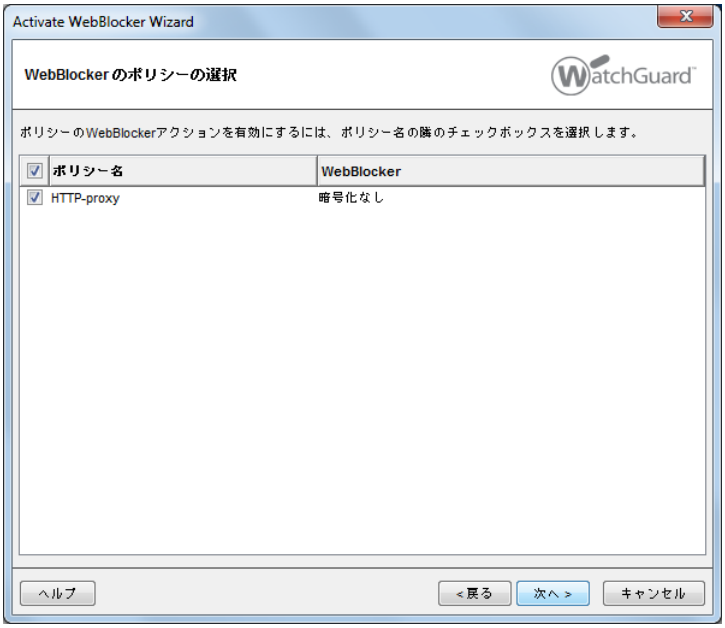


WebBlocker を構成するためのウィザードが始まりますので、次へボタンをクリックします。



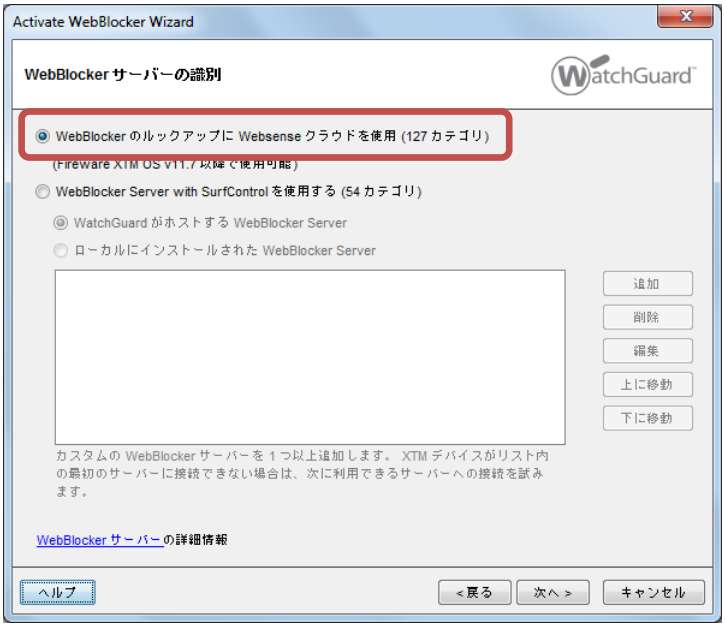
先に追加しておいた HTTP-proxy にチェックが入っています。

このチェックが入ったプロキシポリシーの中で WebBlocker が有効になります。次へ をクリックします。



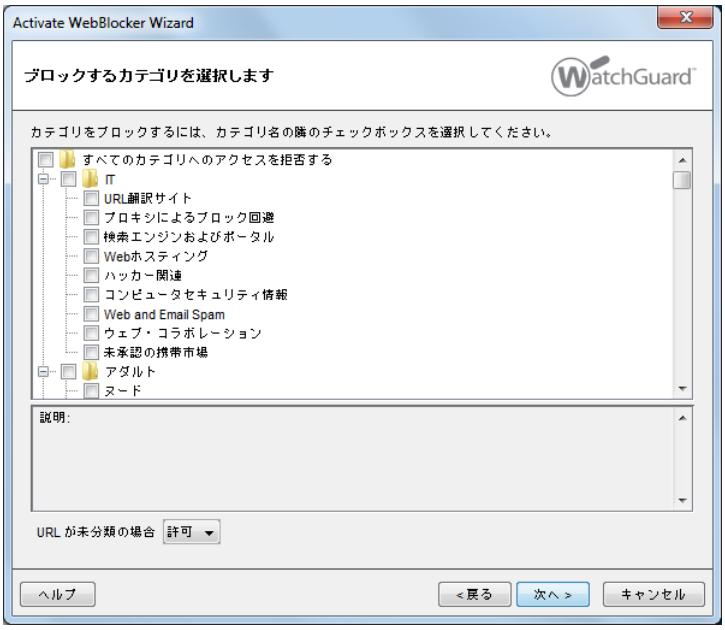
WebBlocker サーバーを指定します。XTM OS v11.7 以降では、Websence クラウドを指定でき、自社で WebBlocker サーバーを設置する必要がなくなりました。

「WebBlocker のルックアップに Websence クラウドを使用」にチェックを入れます。



次へ をクリックします。

カテゴリの指定は後で設定できますので、そのまま次へ進みます。



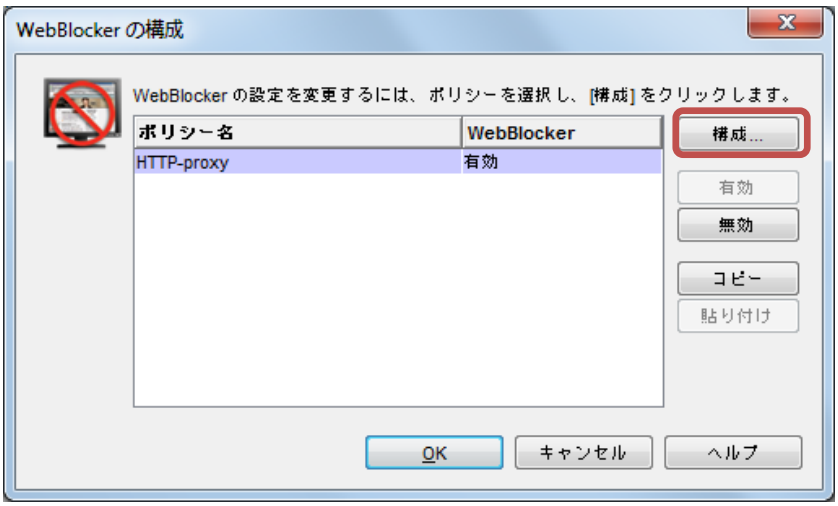
Wizard が完了します。

「WebBlocker の中央構成に進みます」にチェックが入ったまま完了ボタンをクリックします。[5]

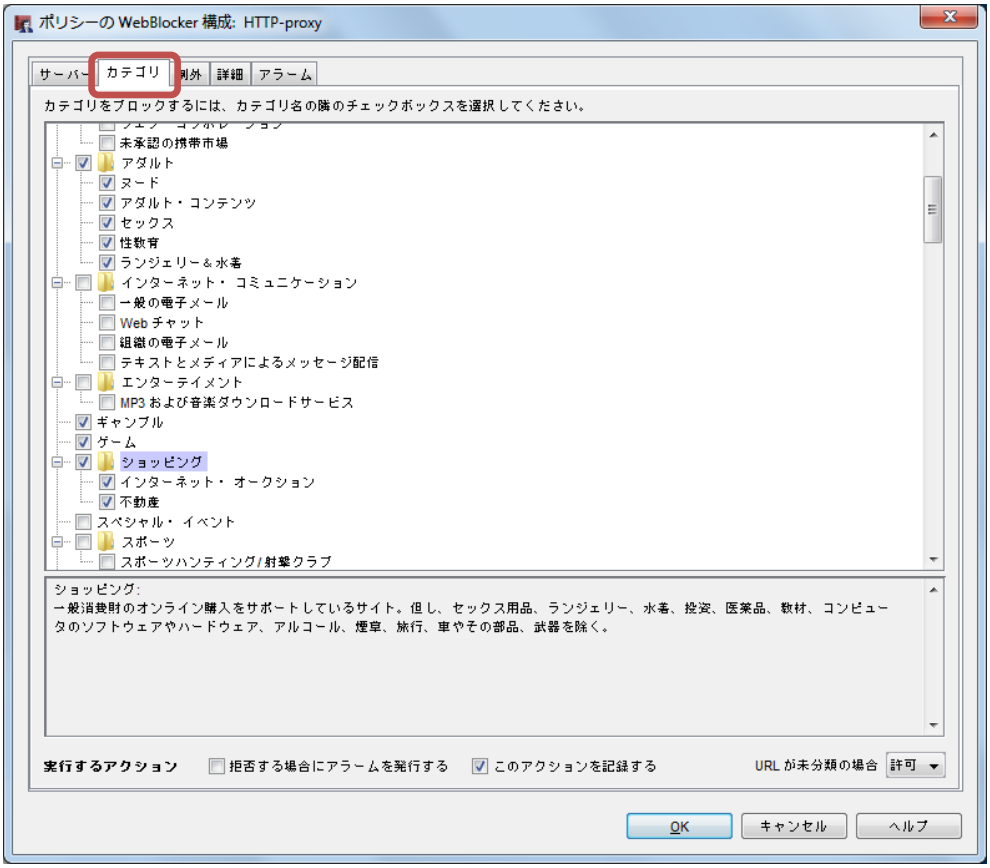
[5] チェックをつけなくても、後からポリシーマネージャのセキュリティサービス→WebBlocker→構成で開くことができます。

Web Blocker を構成する

構成ボタンをクリックします。



カテゴリタブをクリックします。アダルト、犯罪、ショッピングなど、仕事中に規制したいカテゴリにチェックを入れます。

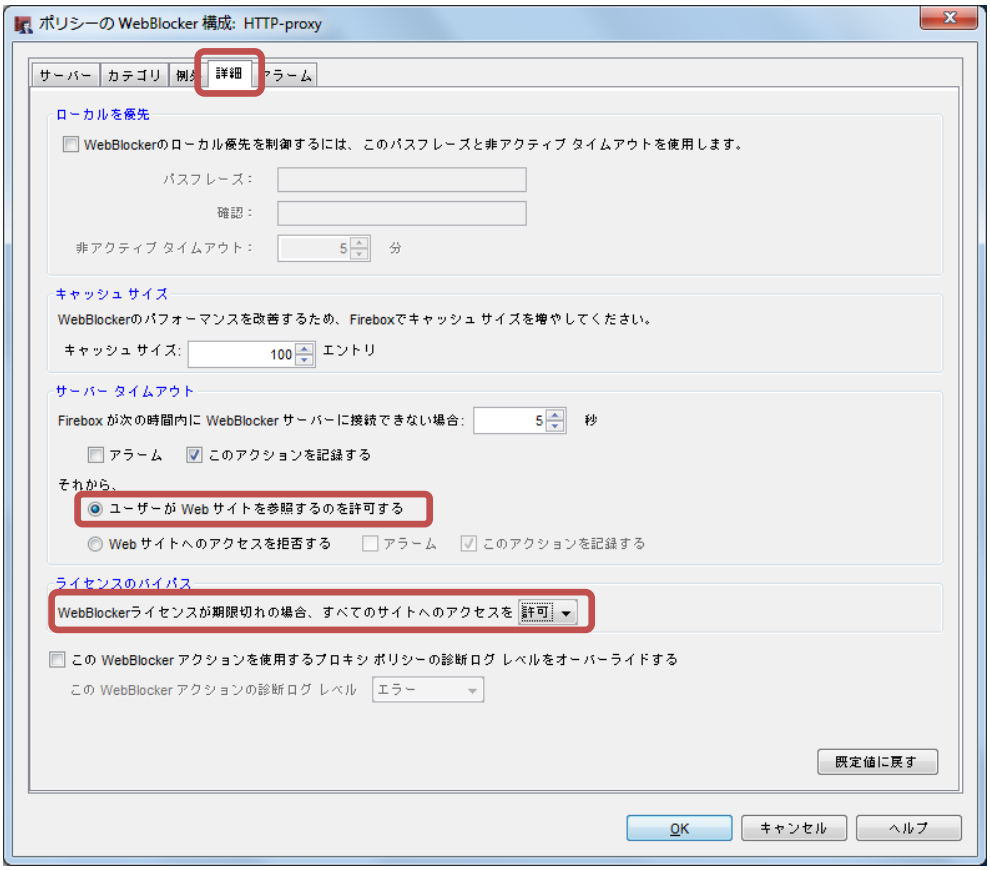


例外タブでは、規制対象から外したいサイトを登録できます。

例：ショッピングサイトはカテゴリで一律規制するが、Amazon だけは許可する

注意すべき点として、デフォルトではサーバーにアクセスできない時や UTM のライセンスが切れた時に、ユーザーに Web サイトの閲覧を拒否する設定になっています。

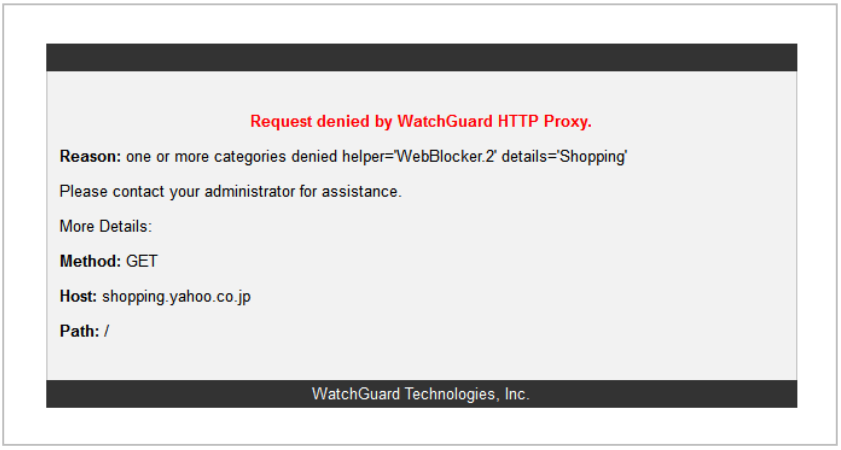
それが不都合であれば、詳細タブの「サーバータイムアウト」と「ライセンスバイパス」の項は許可する設定にしておきます。



以上で WebBlocker の設定は完了です。OK で抜けて設定を保存してください。

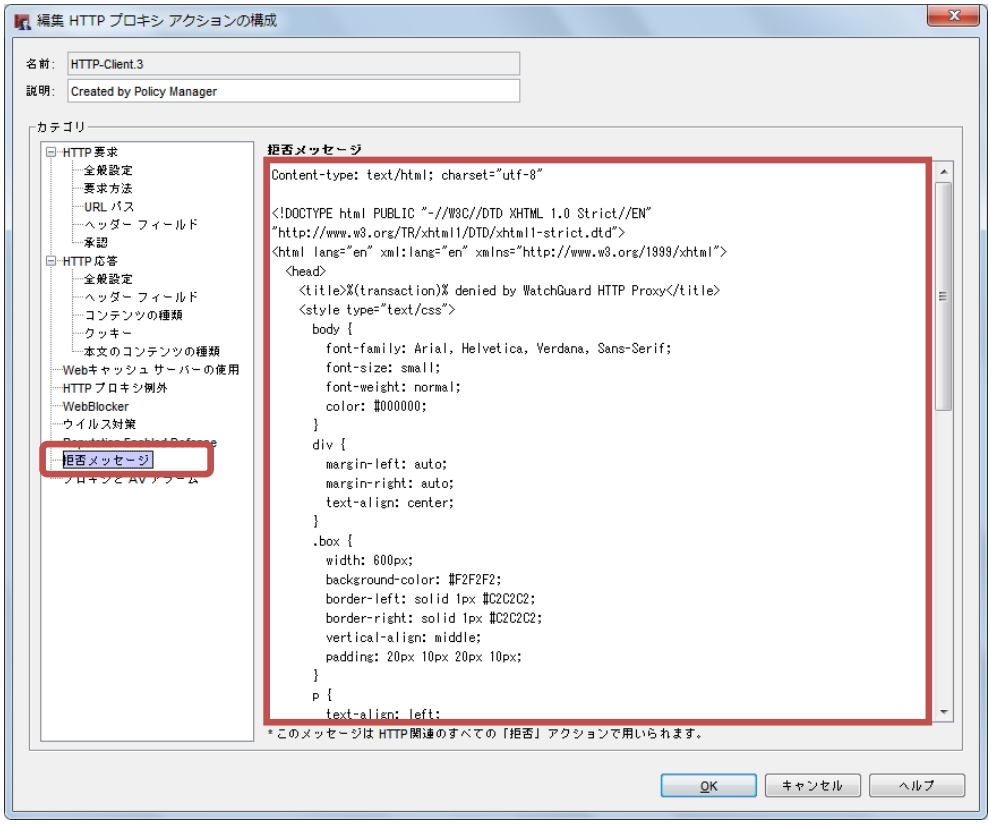
設定を保存したら、試しにショッピングサイトにアクセスしてみてください。

以下のように拒否画面が表示されます。



この拒否画面は、以下の方法で日本語にカスタマイズすることが可能です。

HTTP-proxy のプロキシの表示/編集画面の左メニュー下方にある「拒否メッセージ」で自由に HTML を記述できます。



※%(reason)%など、%記号で囲われた変数部分は日本語化できません

以下が日本語化した画面です。

【豆知識】コンテンツフィルタリングのデータベースは Websence のもの

WebBlocker のフィルタリング用データベースは、Websence 社より供給を受けています。その他の UTM 機能のシグネチャやエンジンも他社製であることを、WatchGuard ははばかることなく公表しています。

それは、自社で中途半端なものを開発するよりも、優秀な専門ベンダーから供給を受けることで最高のセキュリティを確保できると確信しているからです。

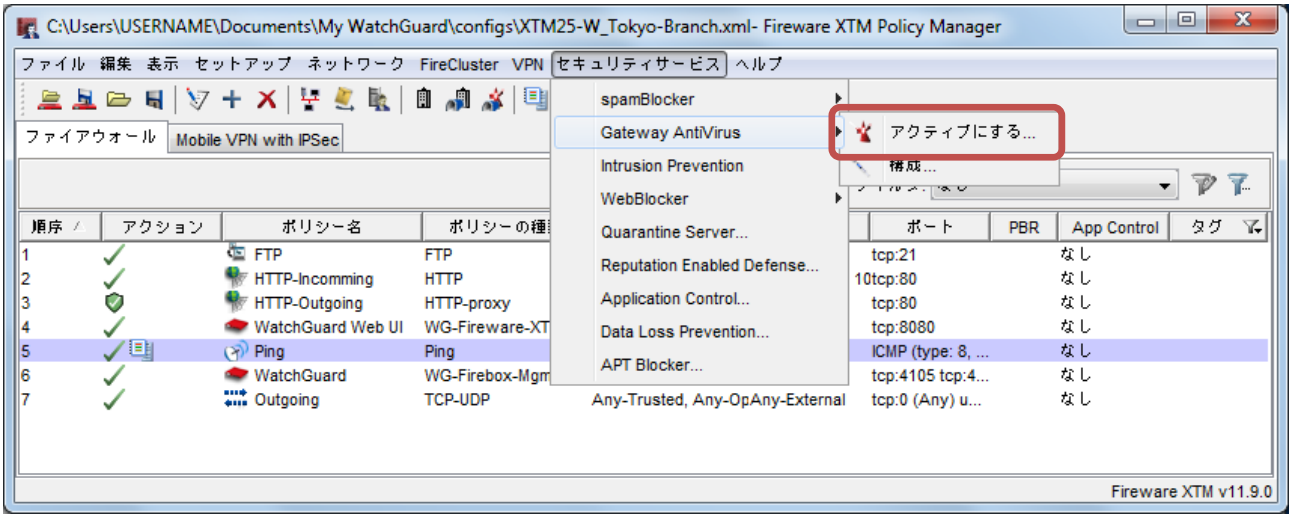
WatchGuard はそれを Best-in-Class Security もしくは BEST-OF-BREED と表現しています。

Gateway Anti-Virus の設定

XTM はネットワークを介して侵入しようとするウイルスを検知し、防御することができます。

Gateway Anti-Virus を有効にする

WebBlocker と同様、ポリシーマネージャの セキュリティサービス → Gateway Anti-Virus → アクティブにする をクリックします。

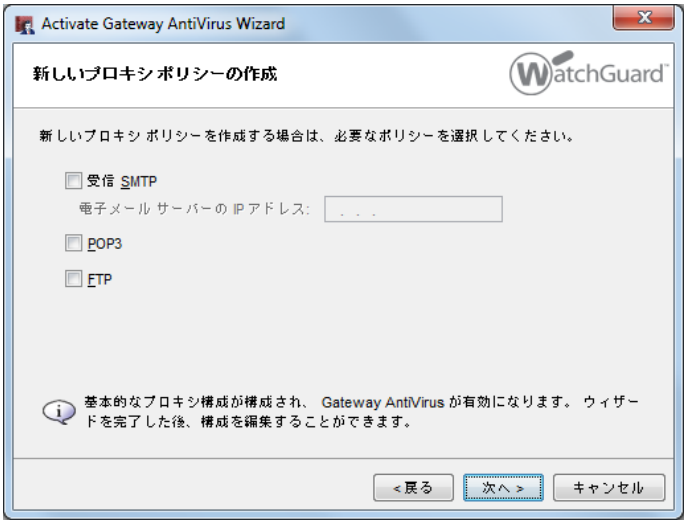


Gateway Anti-Virus を構成するためのウィザードが始まりますので、次へボタンをクリックします。

先に作成してあった HTTP-proxy にチェックが入っています。

このチェックが入ったプロキシポリシーの中で Anti-Virus が有効になります。次へ をクリックします。

他のプロトコルで Anti-Virus 機能を働かせたい場合はチェックを入れることができます。次へ進みます。

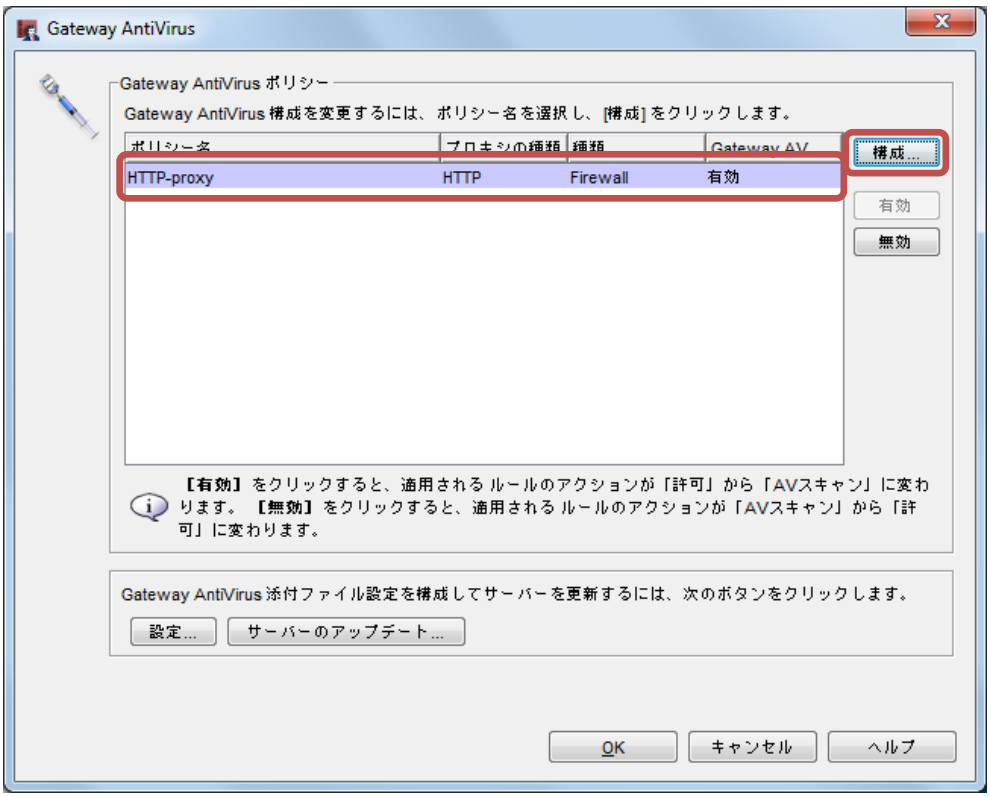


以上で Gateway Anti-Virus が有効になり、ウィザードが完了します。

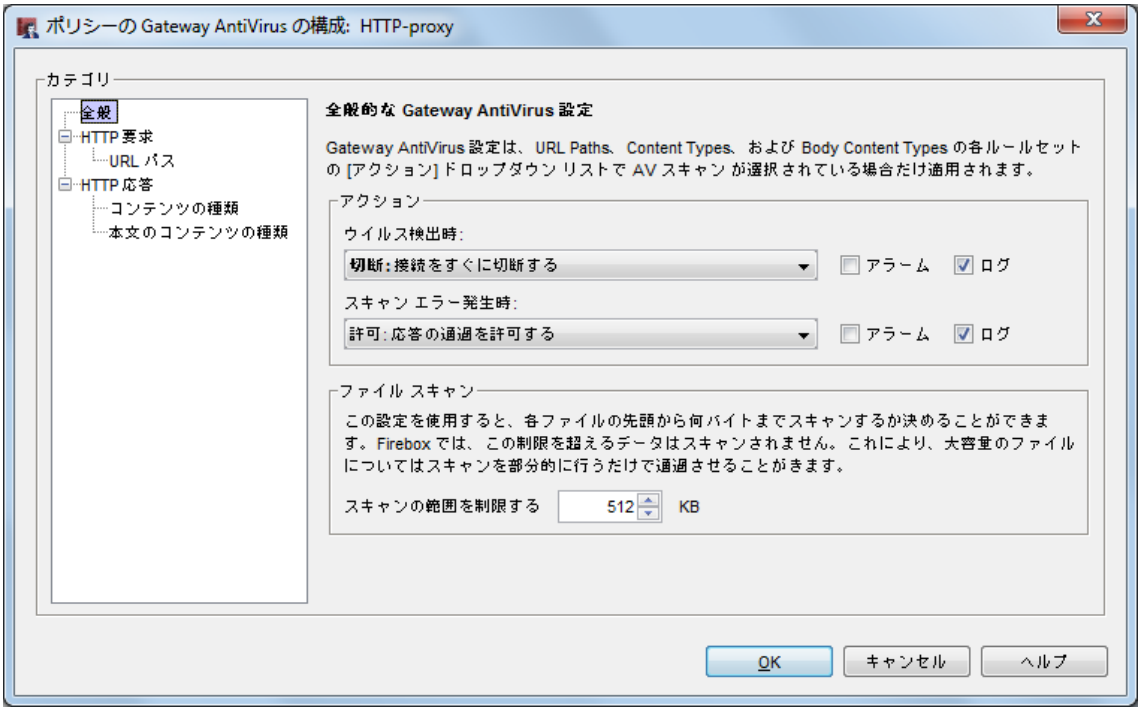
Gateway Anti-Virus を構成する

ポリシーマネージャの セキュリティサービス → Gateway Anti-Virus → 構成 で中央構成画面を開きます。

中央構成画面では、該当のプロキシポリシーを選択し、構成ボタンをクリックします。

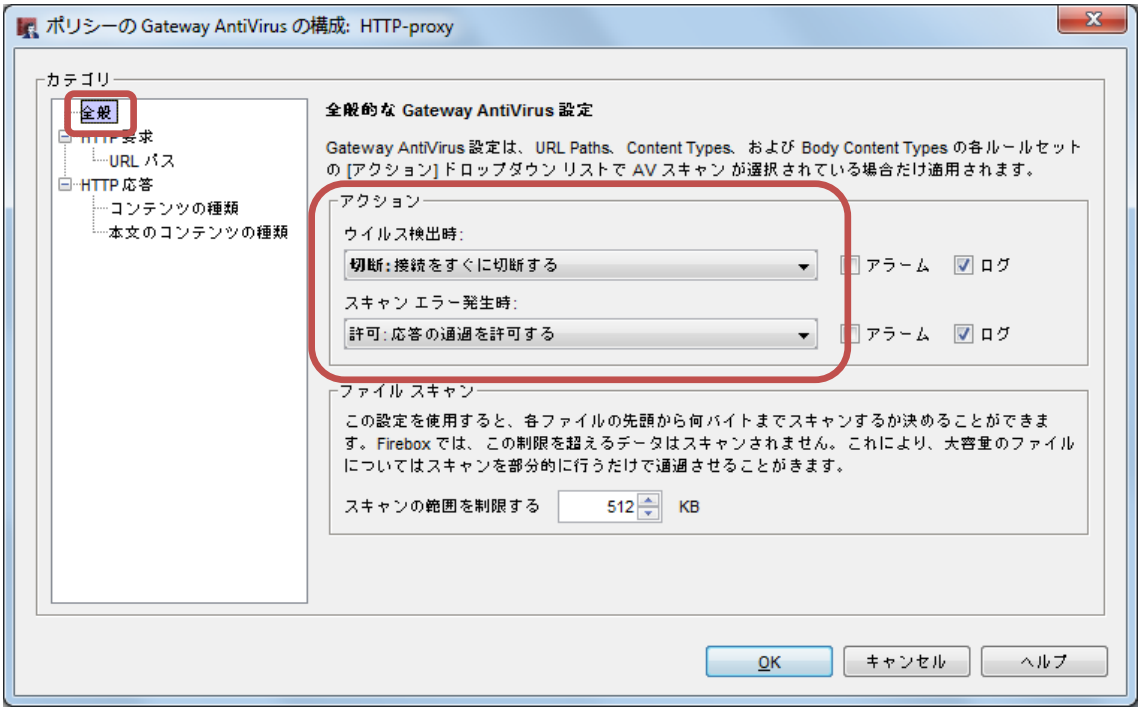

Gateway AntiVirus
Gateway AntiVirus ポリシー
Gateway AntiVirus 構成を変更するには、ポリシー名を選択し、[構成] をクリックします。
ポリシー名
プロキシの種類
種類
Gateway AV
HTTP-proxy
HTTP
Firewall
有効
構成...
有効
無効
【有効】をクリックすると、適用される ルールのアクションが「許可」から「AVスキャン」に変わります。【無効】をクリックすると、適用される ルールのアクションが「AVスキャン」から「許可」に変わります。
Gateway AntiVirus 添付ファイル設定を構成してサーバーを更新するには、次のボタンをクリックします。
設定...
サーバーのアップデート...
OK
キャンセル
ヘルプ

構成画面が開きます。


ポリシーの Gateway AntiVirus の構成: HTTP-proxy
カテゴリ
全般
HTTP 要求
URL パス
HTTP 応答
コンテンツの種類
本文のコンテンツの種類
全般的な Gateway AntiVirus 設定
Gateway AntiVirus 設定は、URL Paths、Content Types、および Body Content Types の各ルールセットの [アクション] ドロップダウン リストで AV スキャン が選択されている場合だけ適用されます。
アクション
ウイルス検出時:
切断: 接続をすぐに切断する
アラーム
ログ
スキャン エラー発生時:
許可: 応答の通過を許可する
アラーム
ログ
ファイル スキャン
この設定を使用すると、各ファイルの先頭から何バイトまでスキャンするか決めることができます。Firebox では、この制限を超えるデータはスキャンされません。これにより、大容量のファイルについてはスキャンを部分的に行うだけで通過させることができます。
スキャンの範囲を制限する
512
KB
OK
キャンセル
ヘルプ

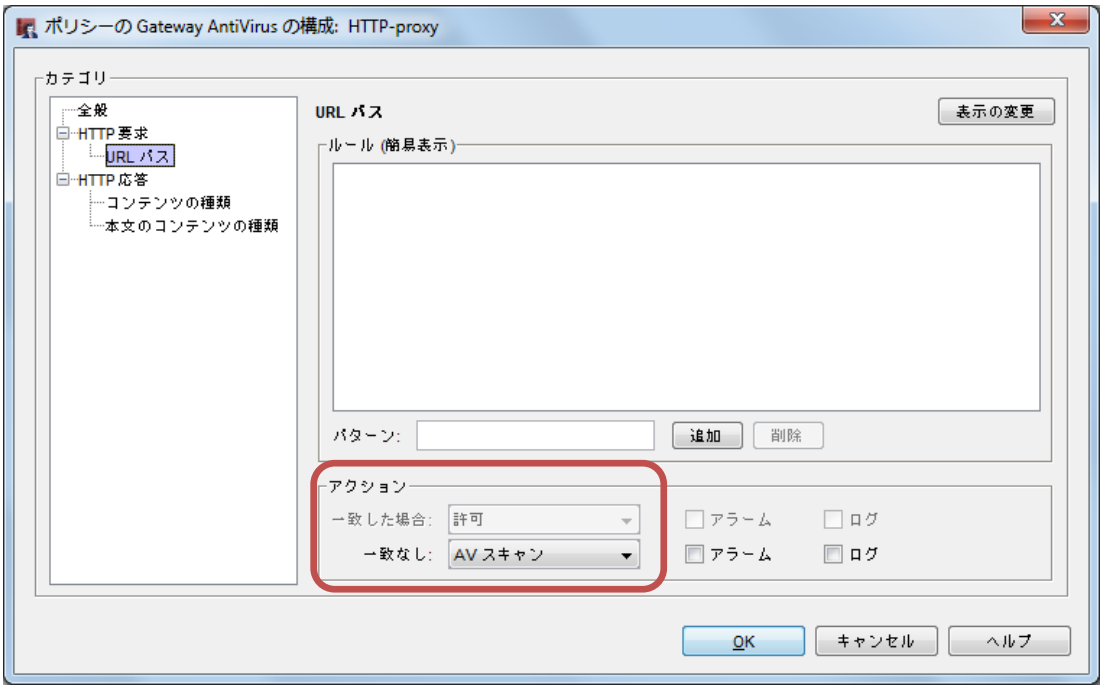
全般設定では、ウイルス検出時の基本動作について設定します。

デフォルトでは、ウイルス検出時は「切断」、スキャンエラー発生時は「許可」となっています。



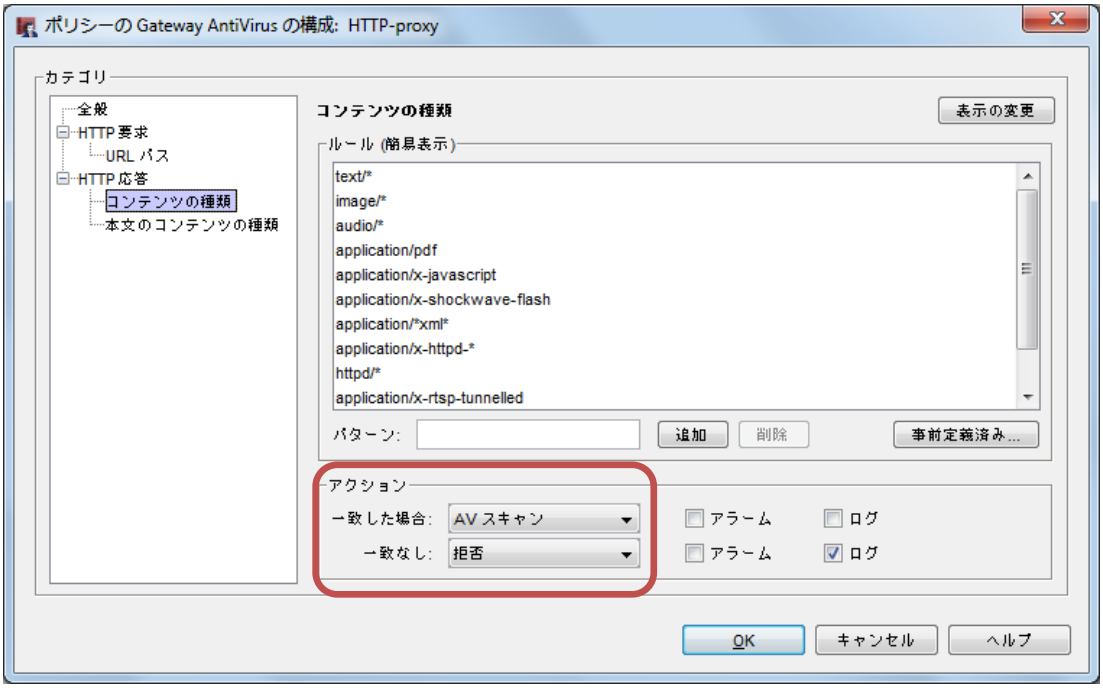
ウイルスを検出する条件を設定するところが、URL パス、コンテンツの種類、本文のコンテンツの種類の 3 箇所あります。

URL パスでは、指定した URL のパターンにマッチする又はしないときのアクションを定義します。



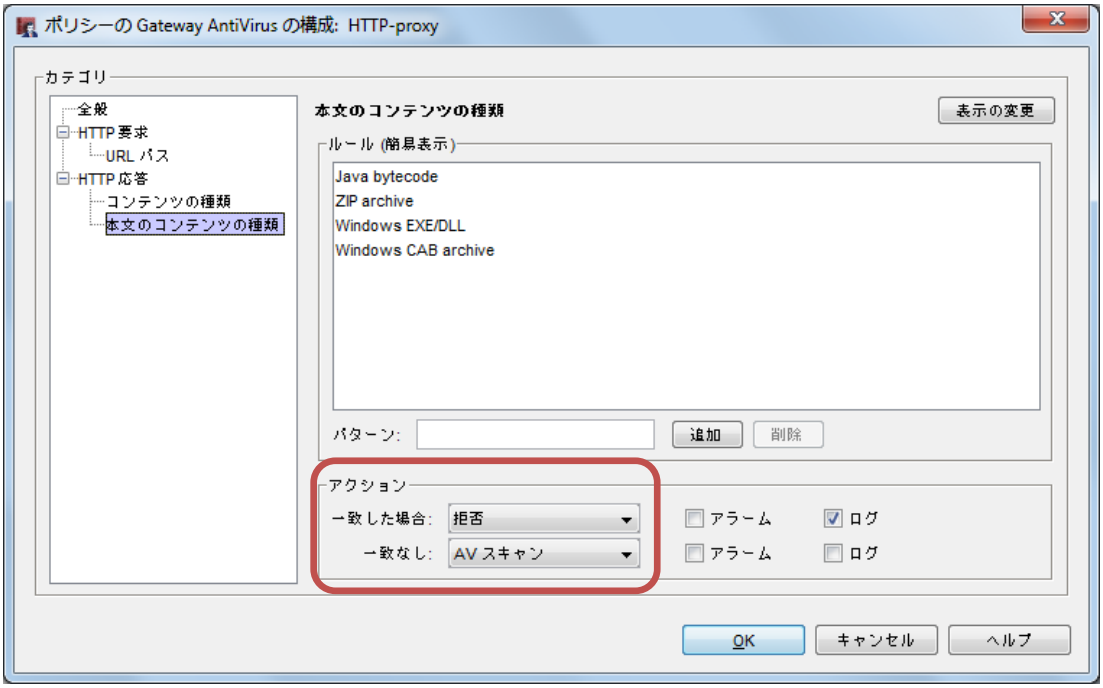
通常は、URL パスでフィルタ処理を行う場合よりも、ヘッダーまたは本文のコンテンツの種類に基づいてフィルタ処理を行う方が簡単であり、精度も向上します。

コンテンツの種類では、HTTP 通信のヘッダーで判断できるコンテンツの種類により、一致しないものは拒否、一致するものは許可するが AV スキャンをかけるというアクションになっています。



もちろんどんなヘッダーであっても、一致してもしなくても AV スキャンをするという選択肢も現実的です。前述の URL パスと同じように、ルールを空にして、一致なしで AV スキャンという設定です。

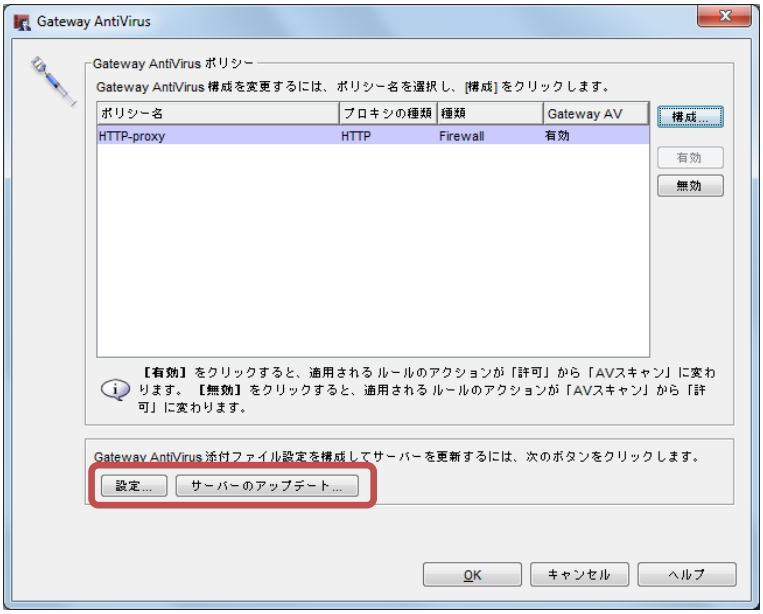
本文のコンテンツの種類では、デフォルトで一致なしが拒否、それ以外を AV スキャンになっています。しかし、現実的には ZIP ファイルのダウンロード、ソフトウェアのインストーラー(.exe)のダウンロードなどが発生しますので、一致する場合もしない場合も AV スキャンを選択しておくとよいでしょう。



OK ボタンをクリックして、中央構成の画面に戻ります。

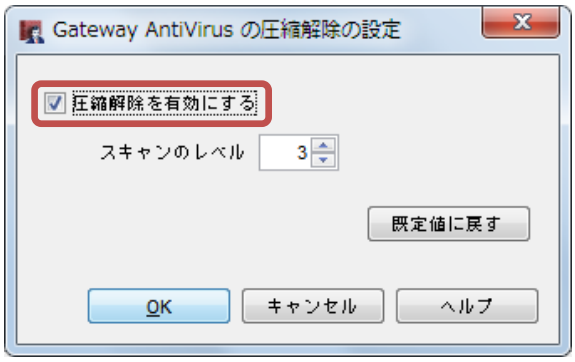
「設定」ボタンからは圧縮されたファイルのスキャンについて設定できます。

「サーバーのアップデート」ボタンからは、シグネチャの更新についての設定ができます。



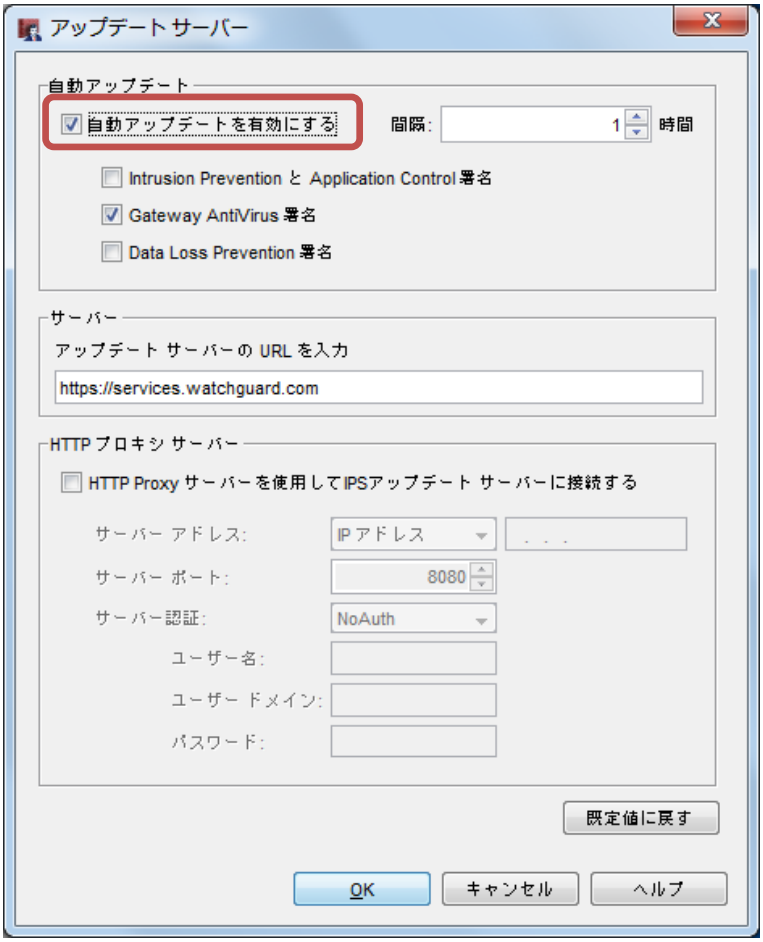
設定ボタンをクリックすると、圧縮解除の設定画面が表示されます。

「圧縮解除を有効にする」にチェックが入っていると、ZIP で圧縮されたファイルの中身もウイルスチェックするようになります。



サーバーのアップデートボタンをクリックすると、シグネチャのアップデートについての設定があります。

「自動アップデートを有効にする」に必ずチェックが入っていることを確認してください。



アップデート間隔はデフォルトで 1 時間に一回です。

以上で Gateway Anti-Virus の設定が完了しました。

しばらくするとシグネチャが更新されて、アンチウイルスが機能するようになります。

eicar テストウィルスなどで動作を確認してみてください。

【豆知識】BEST-OF-BREED を実現している ALL STAR たち

機能	提供元
Gateway Anti-Virus	AVG
WebBlocker	WebSence
spamBlocker	Cyren
IPS	Trend Micro
Application Control	Trend Micro
DLP	Sophos
APT Blocker	Lastline

spamBlocker の設定

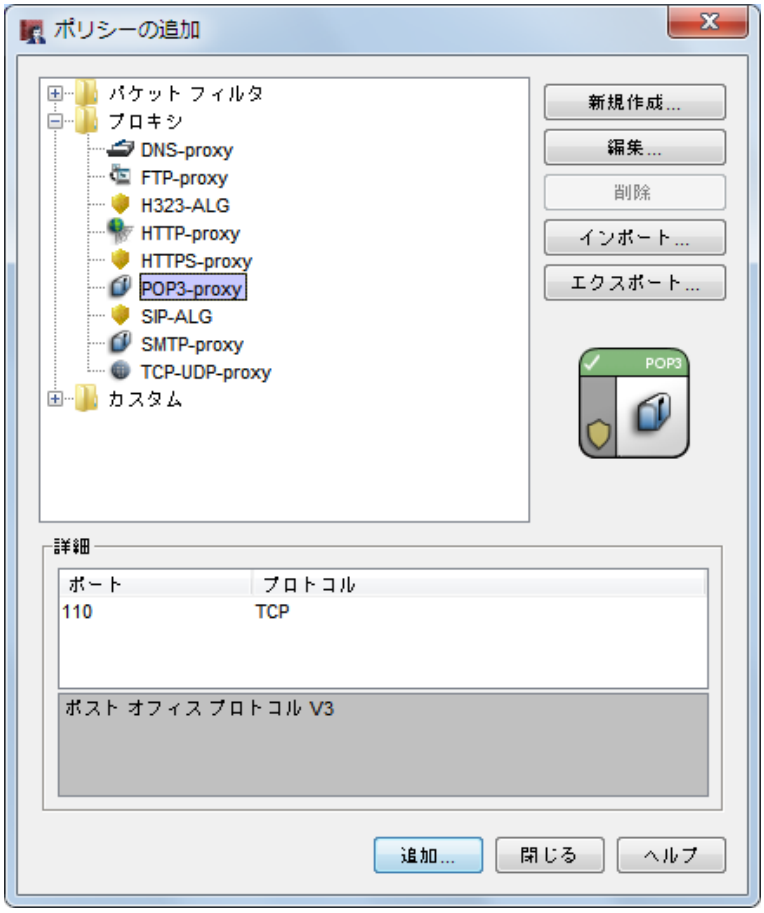
spamBlocker では、Cyren 社が開発した特許技術 RPD(Recurrent Pattern Detection)ソリューションを利用して、発見が難しいスパム攻撃を検出します。

また、オプションで VOD(Virus Outbreak Detection)を有効にし、メールを経路にして拡散される新種のウイルスに対処することもできます。

POP-Proxy を追加する

WebBlocker で HTTP-proxy が必要だったように、spamBlocker では POP3-proxy が必要です。

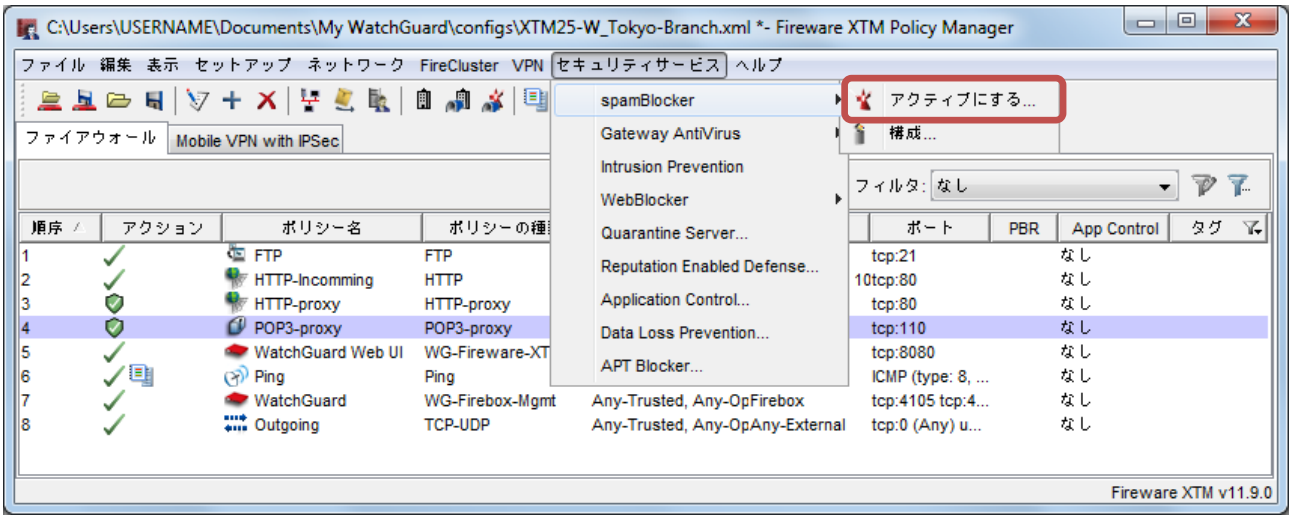
ポリシーの追加画面から、プロキシツリーの POP3-proxy を選択し、追加ボタンをクリックします。



SMTP も spamBlocker を使うことができますが、SMTP-proxy は、XTM の下に SMTP サーバーがある場合に利用します。

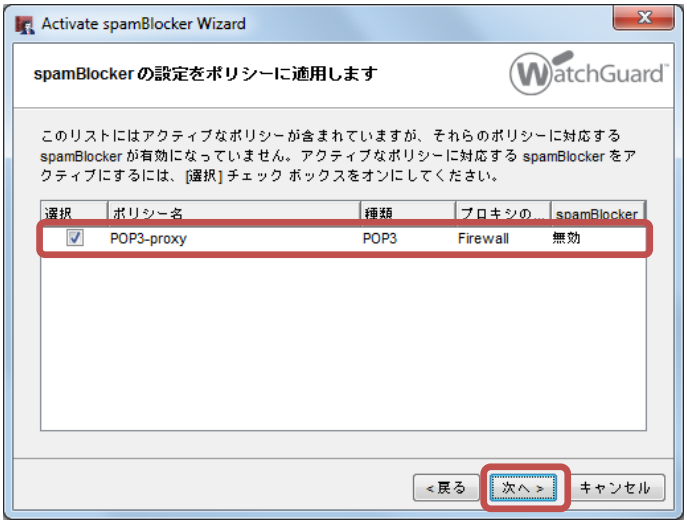
spamBlocker を有効にする

ポリシーマネージャの セキュリティサービス → spamBlocker → アクティブにする をクリックします。

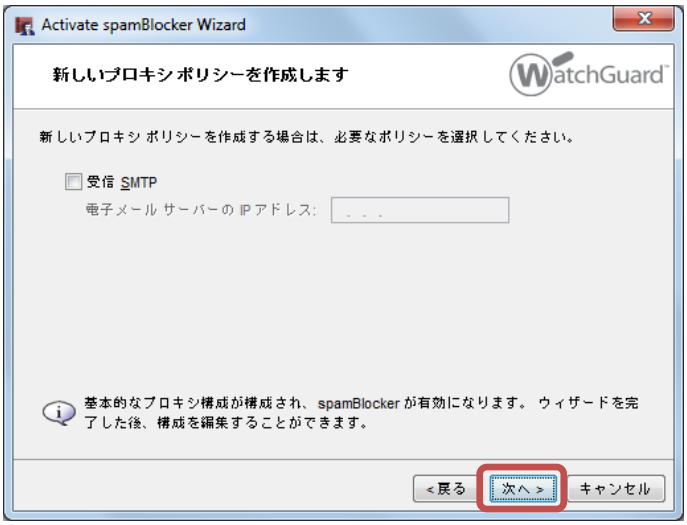


ウィザードが始まります。

POP3-proxy で有効にするよう、チェックが付いていることを確認します。



SMTP サーバーが内側にあれば、SMTP-proxy でも spamBlocker を有効にできます。次へ。

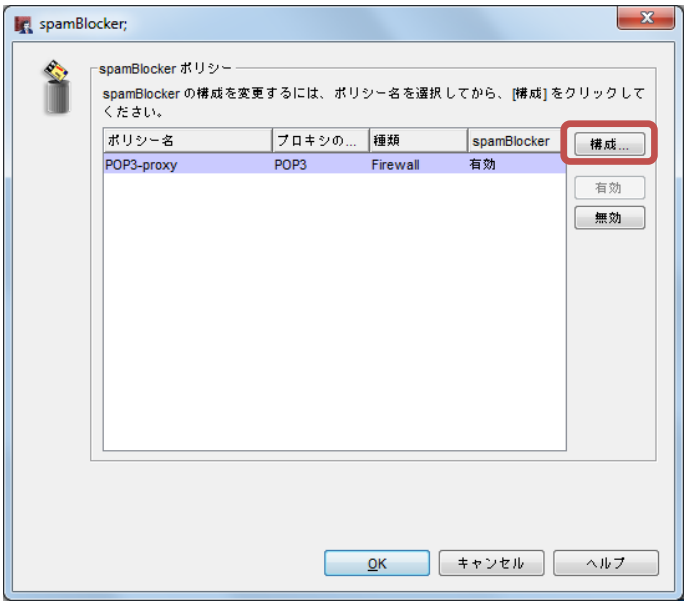


以上で POP3-proxy において spamBlocker が有効になります。

spamBlocker を構成する

ポリシーマネージャの セキュリティサービス → spamBlocker → 構成 をクリックします。

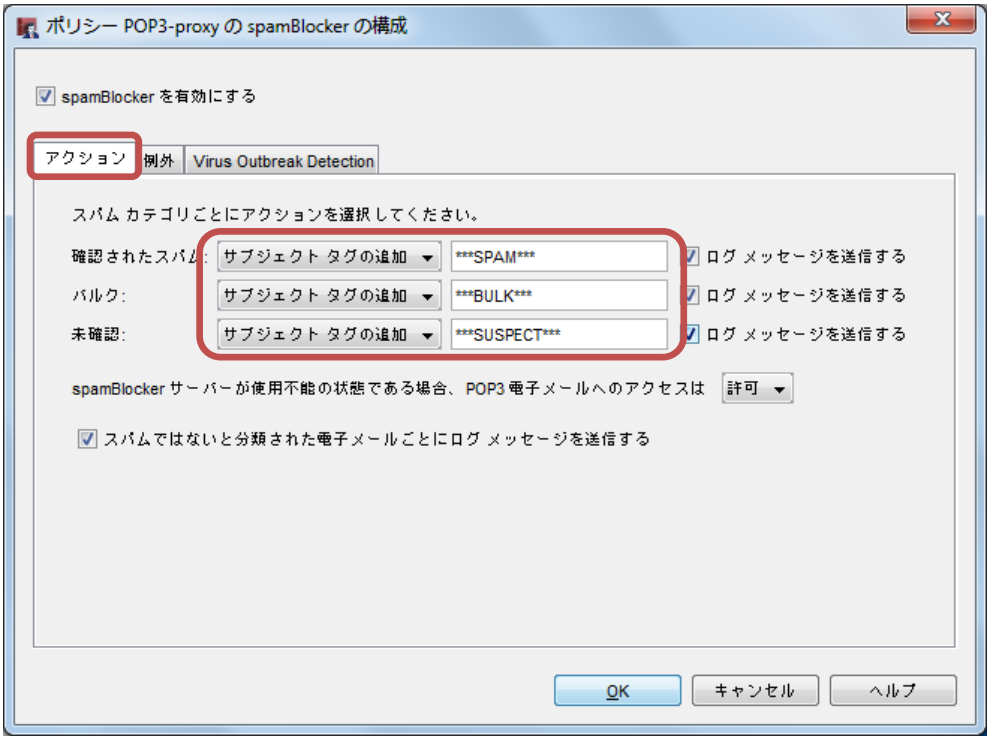
該当のポリシーを選択し、構成ボタンをクリックします。



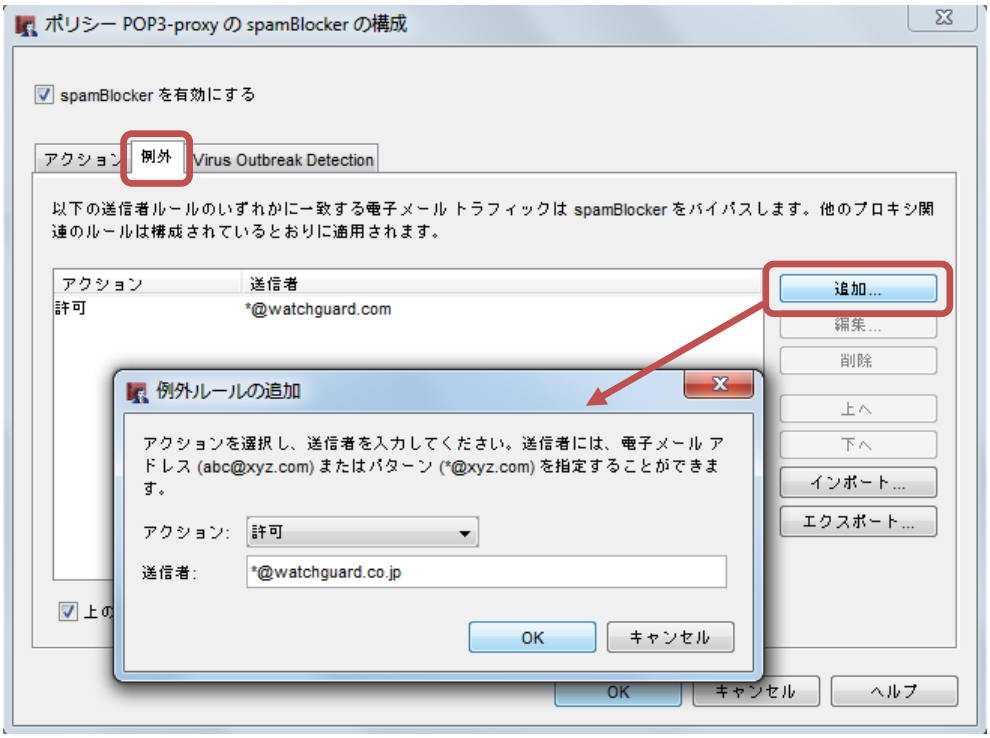
構成画面のアクションタブでは、スパムメールが検知された際の動作を定義できます。

カテゴリは、確認されたスパム、バルク(主に広告メールなど)、未確認(だが疑わしいもの)の 3 種類です。

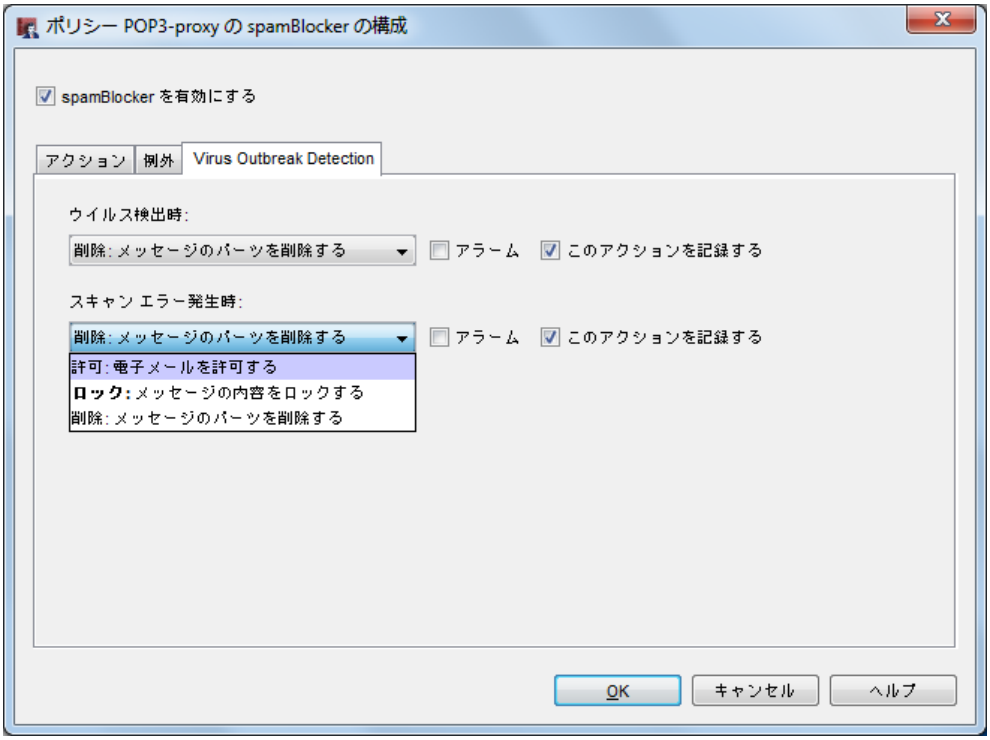
アクションは、指定の文字列(タグ)をサブジェクトに追加するか、許可するかのどちらかです。



例外タブでは、ホワイトリスト/ブラックリストの編集が行なえます。



Virus Outbreak Detection タブでは、ウイルス検出時の動作を定義できます。



ウイルス検出時は「削除」、スキャンエラー時は「許可」がよいでしょう。

設定を保存して動作を確認してください。

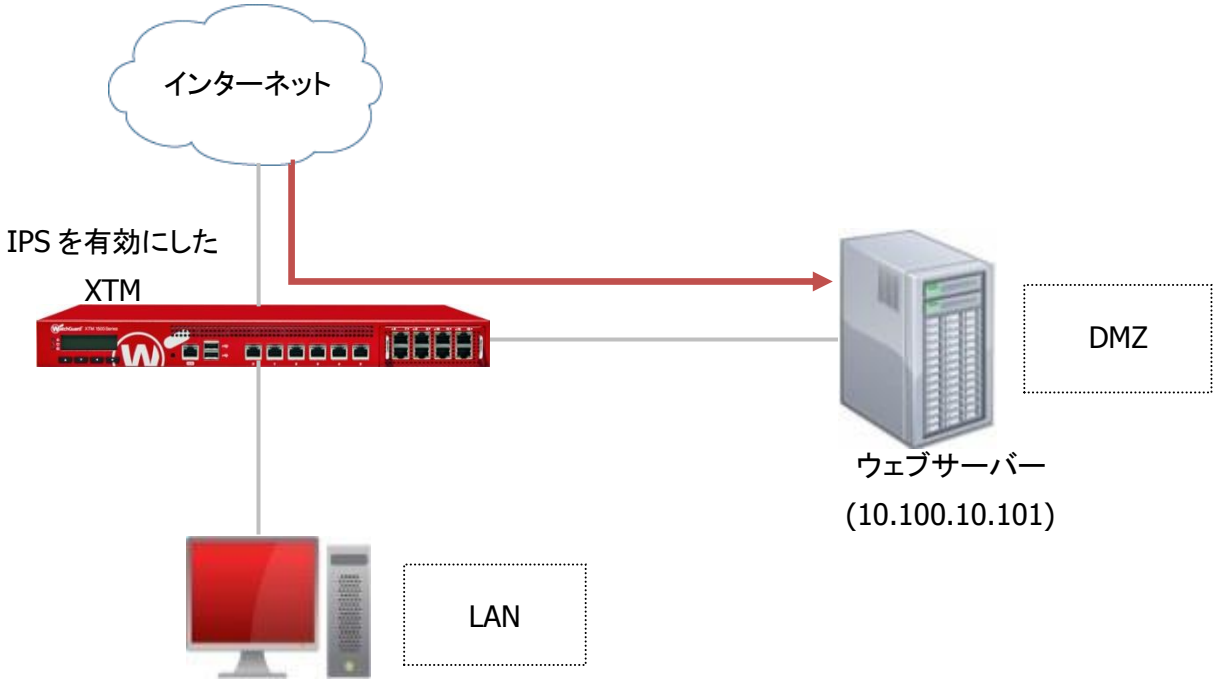
Intrusion Prevention Service

侵入攻撃は主にアプリケーションの脆弱性を利用して行なわれます。代表的なものとして、スパイウエア、SQL インジェクション、クロスサイト スクリプティング、バッファ オーバーフローなどを挙げることができます。

XTM の Intrusion Prevention Service (以下 IPS) はこれらの脅威からリアルタイムで保護します。

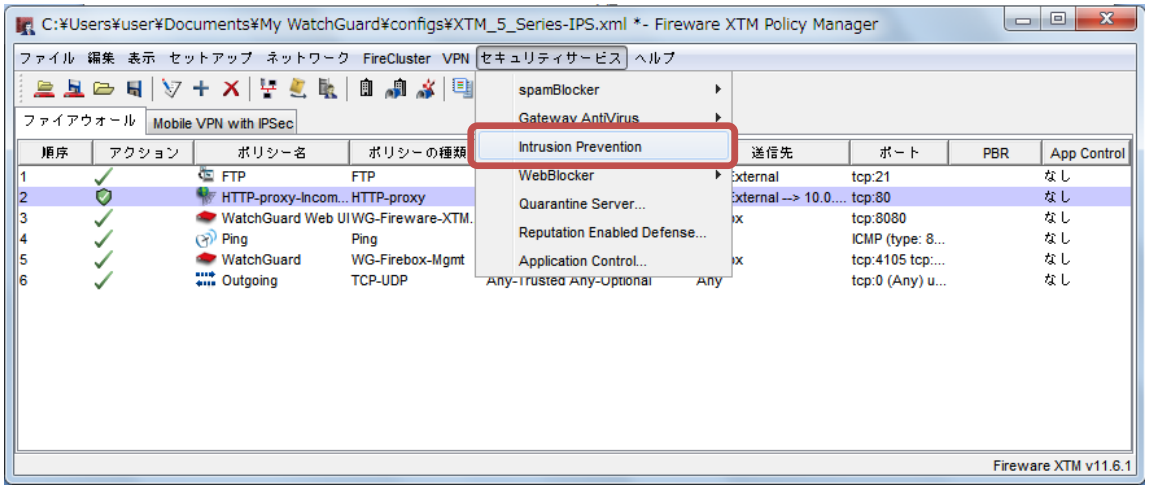
構成例

DMZ のウェブサーバーに SNAT でアクセス許可する HTTP-proxy ポリシーを設定します。そのポリシーで IPS を有効にするケースを例に解説します。



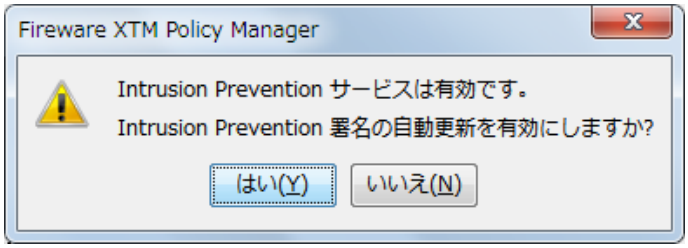
IPS の設定

ポリシーマネージャのメニュー セキュリティサービス ― Intrusion Prevention をクリックします。



IPS の構成画面がひらきますので、「Intrusion Prevention を有効にする」のチェックを入れます。

下方の OK ボタンをクリックすると、IPS シグネチャの自動更新の有効化についてのダイアログが出ますので、OK をクリックします。



※ 重要

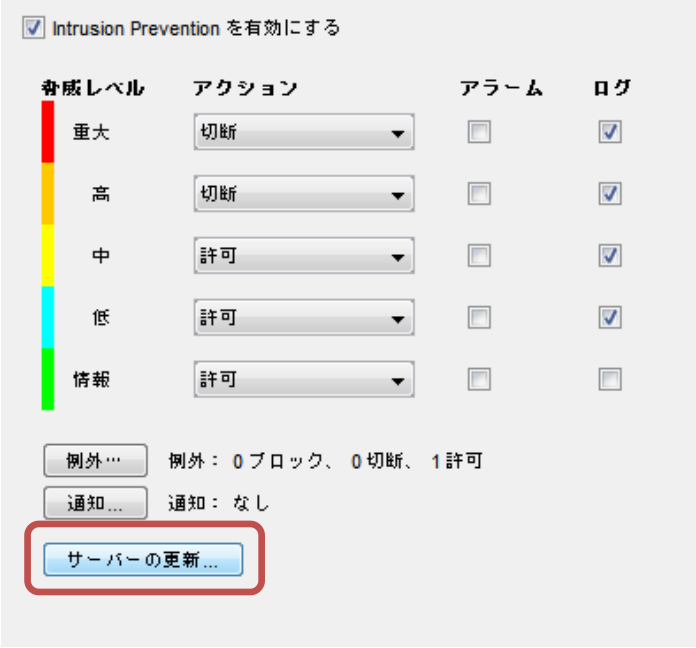
このダイアログが出なかった場合、もしくは「いいえ」をクリックしてしまった場合は、以下のように署名の自動更新を有効にしてください。

自動更新を有効にしないといつまで経ってもシグネチャが更新されず、危険にさらされることになります。

有効化についてのダイアログが出ても出なくても、自動更新が有効になっているか、必ずお確かめください。

自動更新を有効にする手順は次のとおりです。

IPS の構成画面を開き、サーバーの更新ボタンをクリックします。



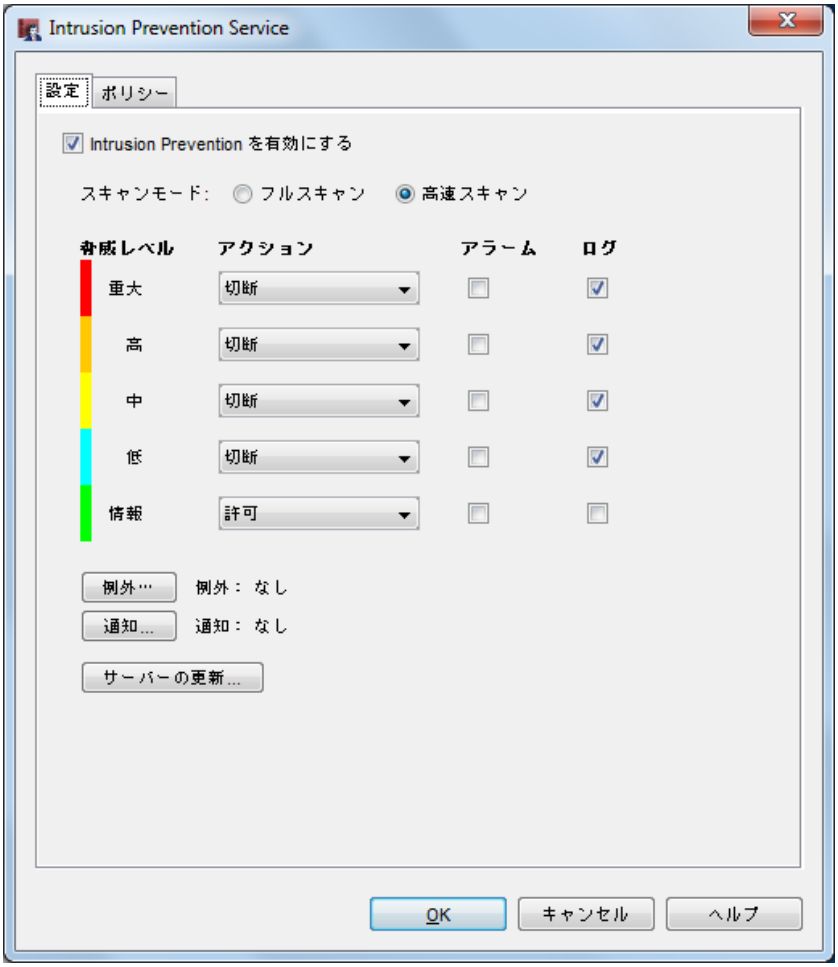
自動アップデートの欄で、「自動アップデートを有効にする」と「Intrusion Prevention と Application Control 署名」にチェックを入れます

次に侵入/攻撃を検知したときのアクションを設定します。

脅威のレベルは 5 段階になっています。

1. 情報
2. 低
3. 中
4. 高
5. 重大

デフォルトでは「低」以上の脅威レベルに一致するトラフィックを切断し、ログに記録するようになっています。



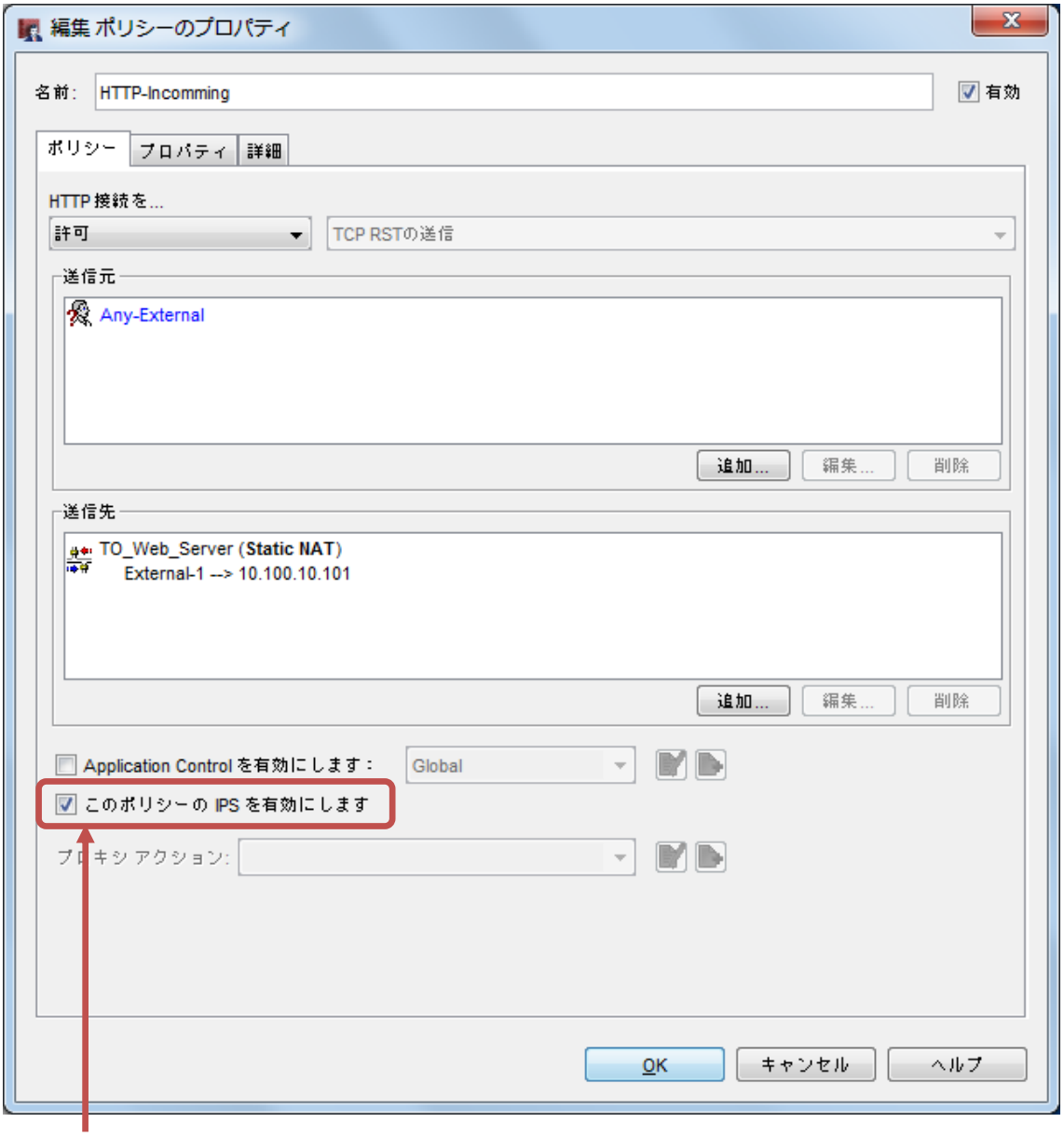
これらの脅威のレベルに対するアクションをコントロールして、自社にふさわしい設定を施します。

詳しい設定については後述します。

ポリシー設定

ポリシーの追加で、ポリシーテンプレートの HTTP から、Web サーバーへのアクセス許可ポリシーを作成します。

図は第四章のポリシー追加で SNAT を設定したものです。



「このポリシーの IPS を有効にします」にチェックが付いている状態で OK をクリックし、設定を反映させます。

このように XTM では、ポリシー単位で IPS を有効/無効に設定することができます。

IPS の設定自体は以上で有効になりました。しかし、デフォルトのアクションではかなり用心深い設定(レベル「低」で「切断」)になっており、問題ないと思える通信も切断する可能性があります。

次にアクションのレベルを調整します。

IPS の調整

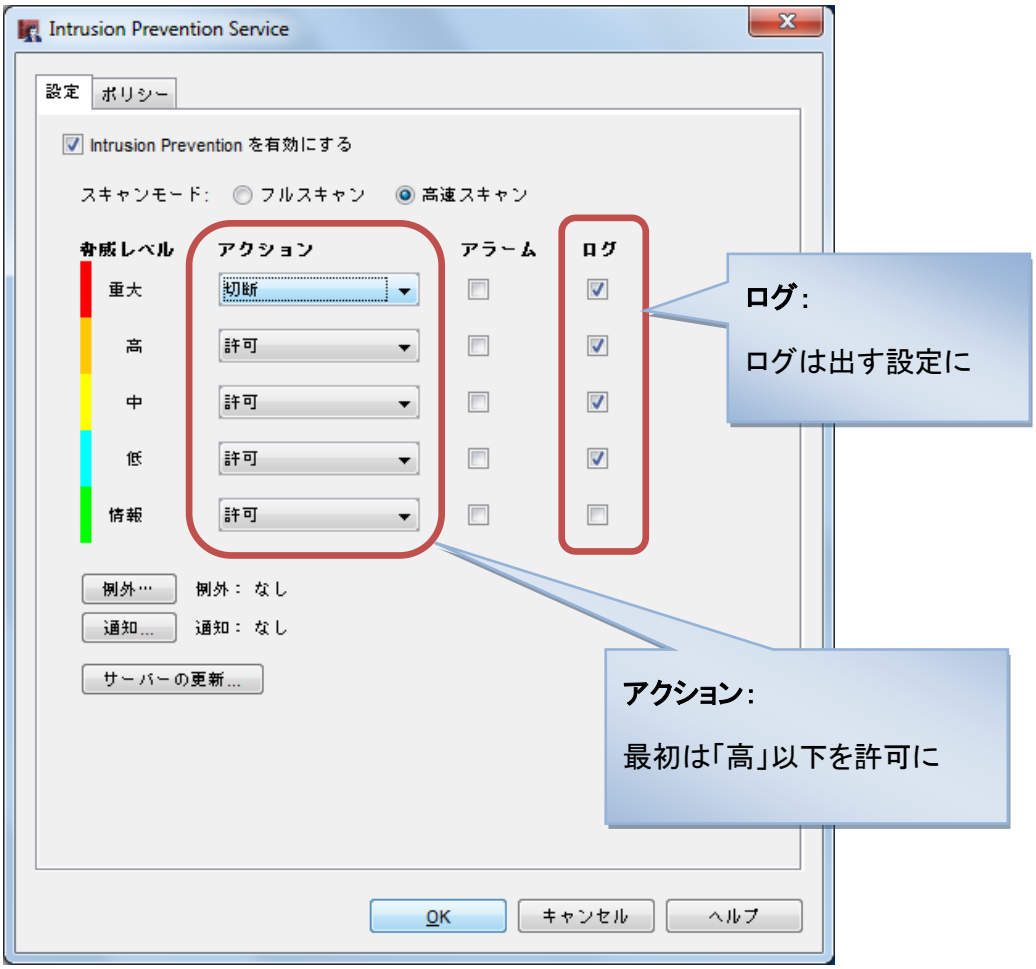
アクションを調整するためには、

1. ログを取り、どんな攻撃が多いか現状を知る
2. その攻撃に合わせたアクションを設定する
3. 特定のアクセスが攻撃として検知され不都合が生じる際には例外を設定する

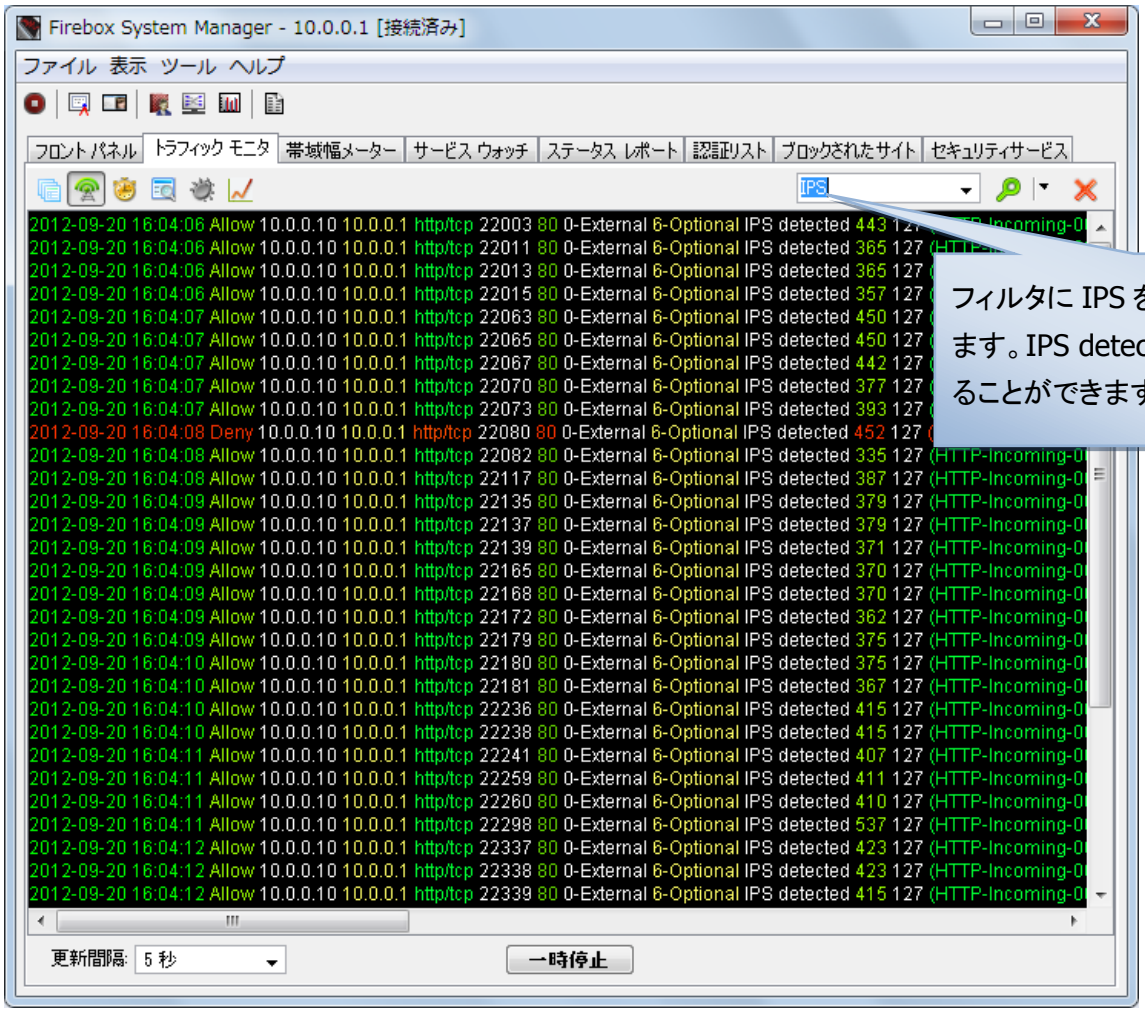
という流れで設定するとよいでしょう。

とはいえ、重大な脅威となる侵入/攻撃については最初から切断にした方がよいでしょう。

例として、高より下のレベルは許可にしながらも、ログを出す設定にしておきます。



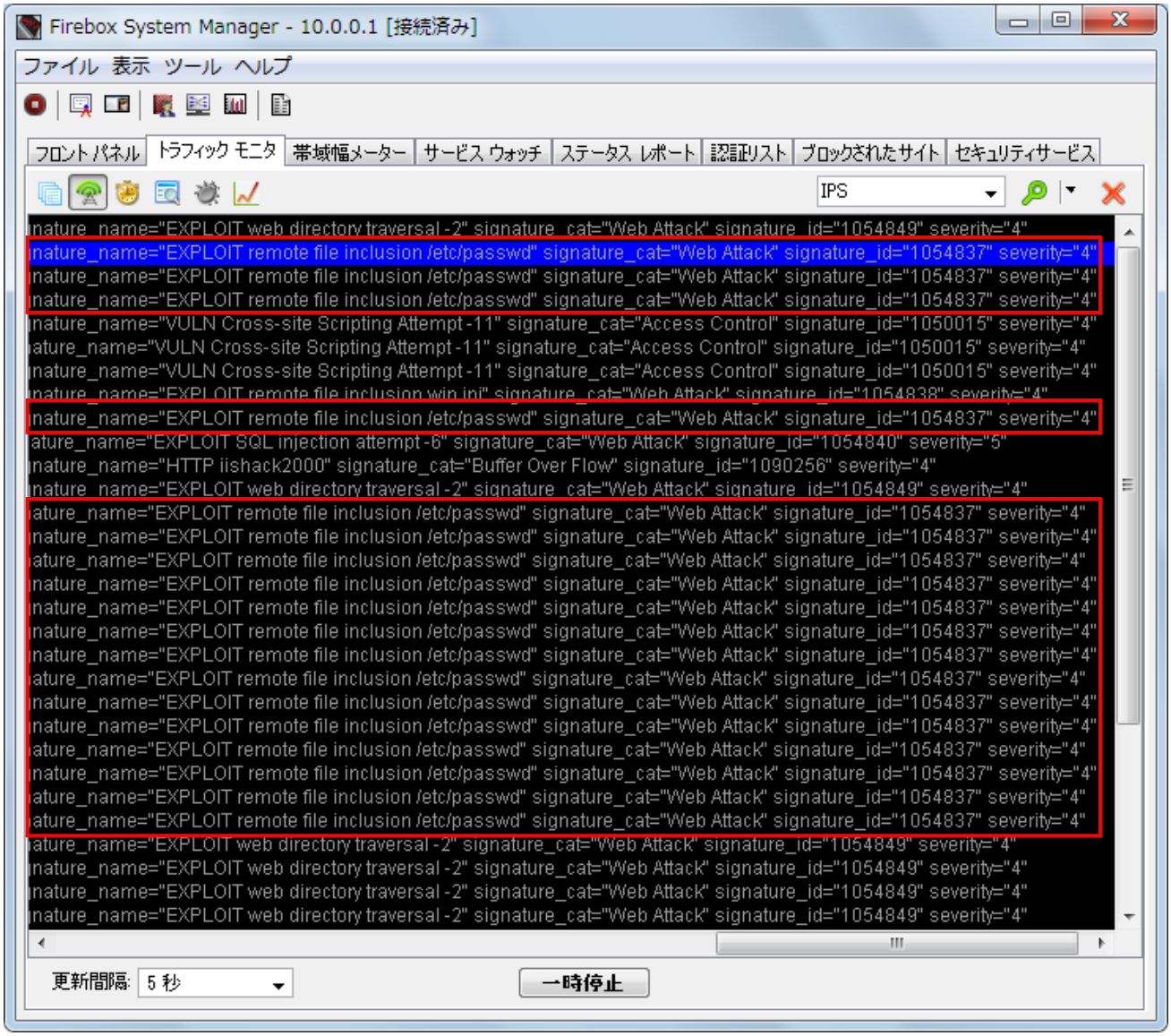
それではログを見てみましょう。Firebox System Manager のトラフィックモニターで IPS のログに絞り込んでみます。ログサーバーがあればログビューワーで同様に確認できます。



上記のログで検知している侵入/攻撃で、拒否しているものもありますが、かなり多くのものが許可されています。

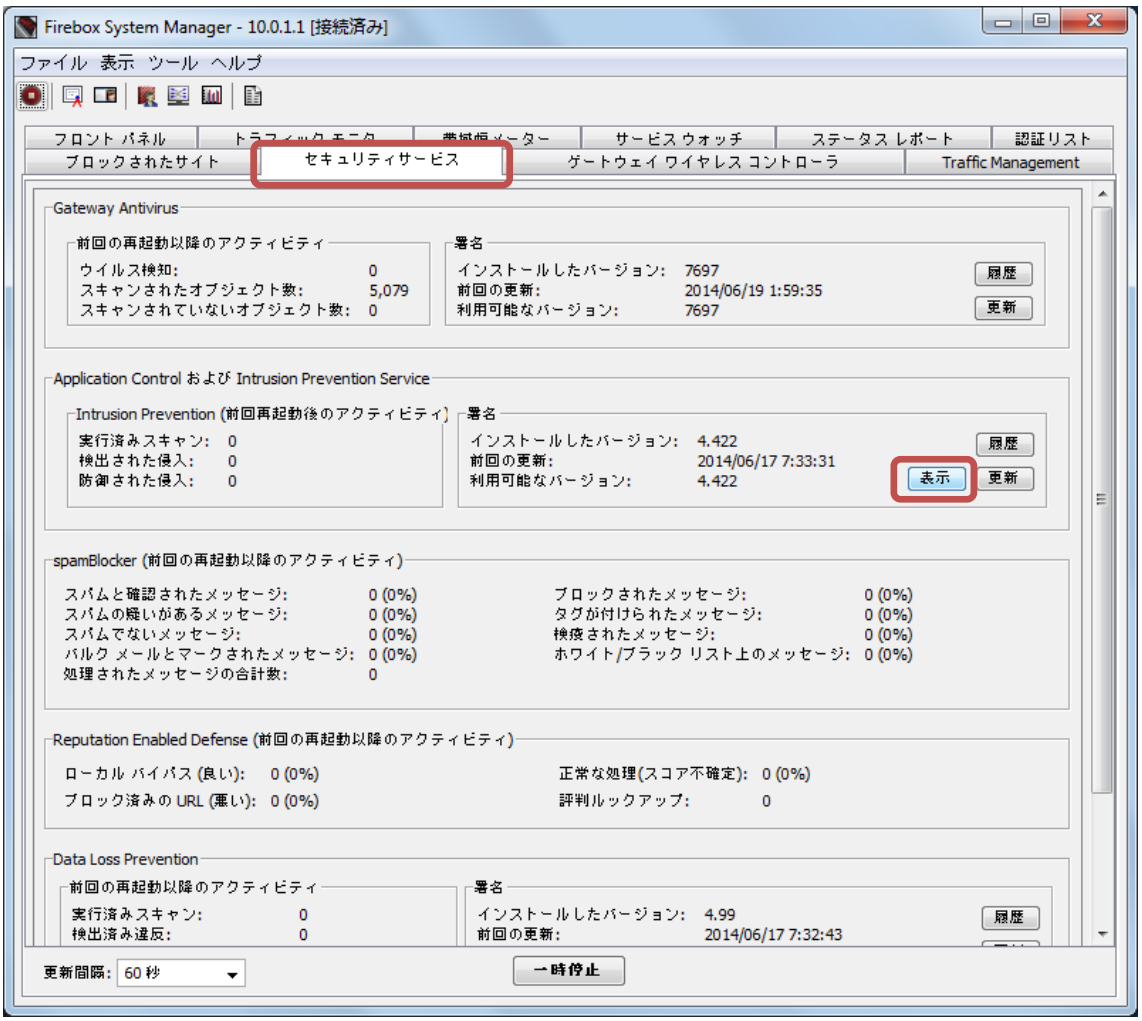
右スクロールして、ログの詳細を見てみましょう。

シグネチャ ID に注目してください。「signature id=1054837」の攻撃がかなり執拗になされていることが分かります。

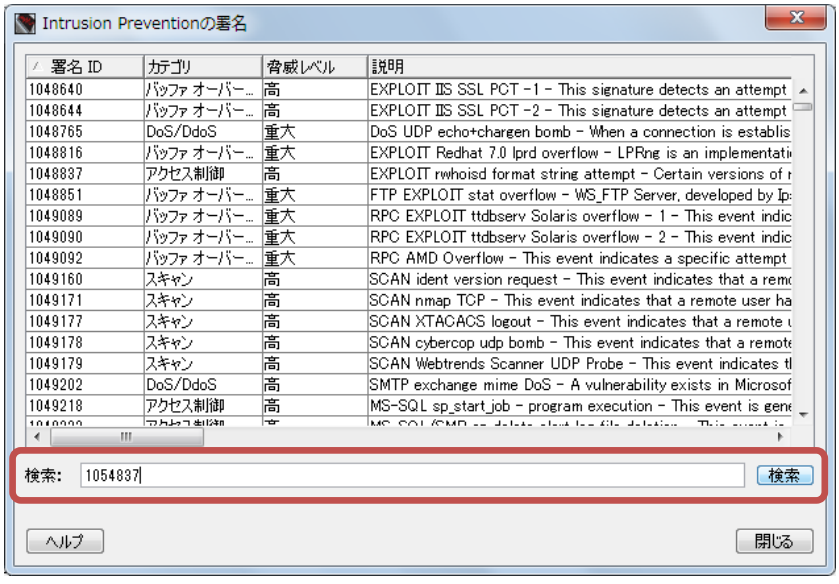


1054837 という ID をメモし、セキュリティサービスタブに移ります。

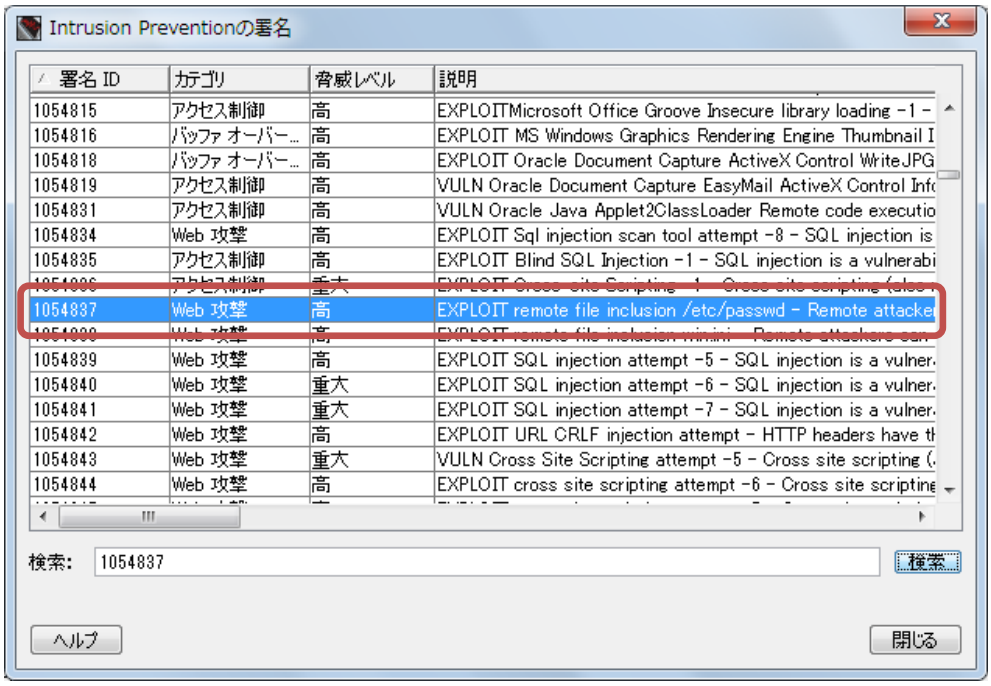
Application Control および Intrusion Prevention Service の欄の署名の表示ボタンをクリックします。



署名のダイアログが開きますので、テキストエリアに ID を入力して検索します。



検索すると、該当の行にフォーカスが当たります。

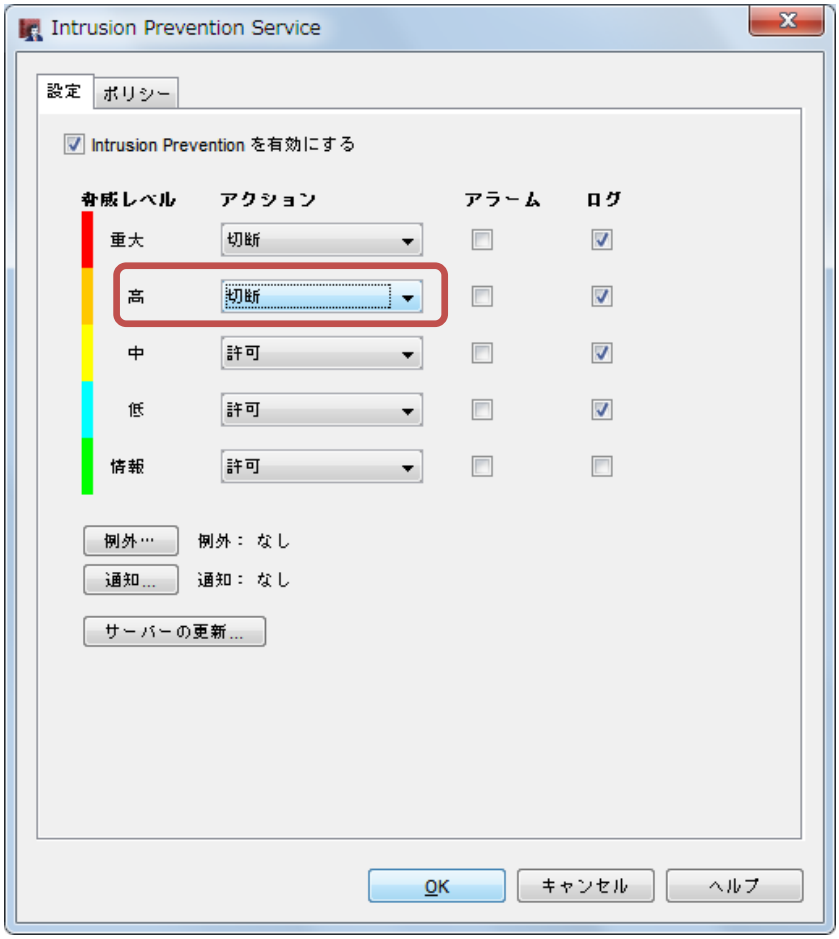


説明を読むと/etc/passwd ファイルを取り込もうとするアタックであることが分かります。Web サーバーが Unix 系の OS なら、許すわけにはいかないと思われるでしょう。

よって、脅威レベル「高」は拒否する設定にしたほうがよい、という判断になります。

IPS の構成画面を開き、アクションを調整してみましょう。

「高」のアクションを切断に変更します。



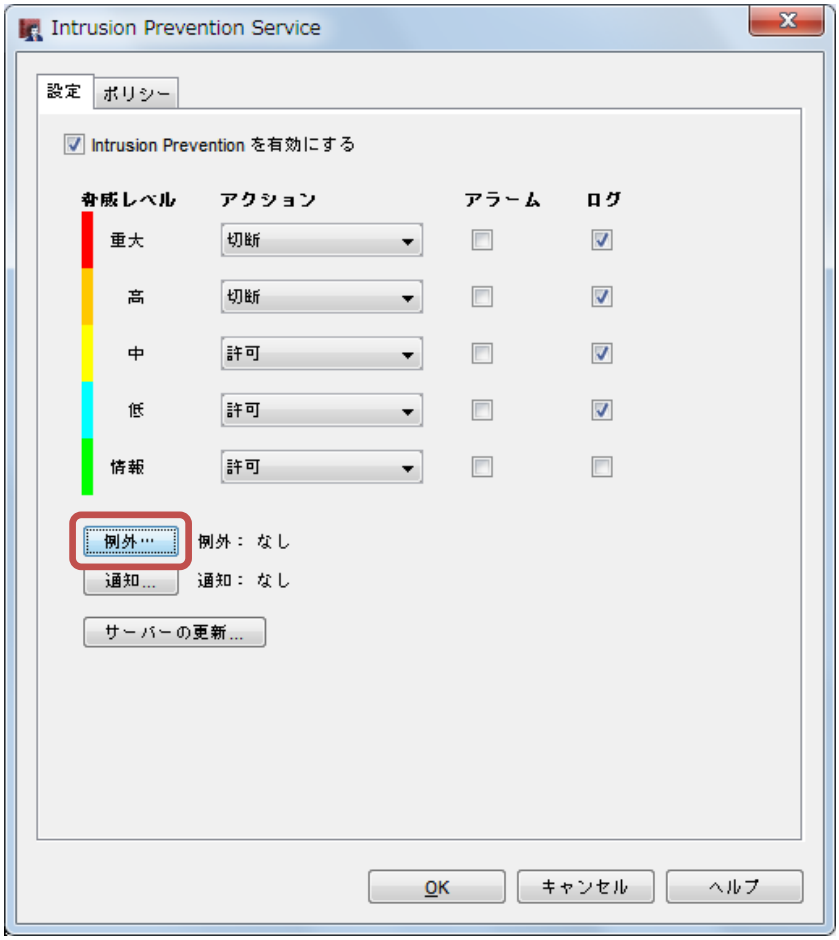
同じように「中」の脅威レベルのもので、特定の攻撃が執拗に行なわれており、それが実際に脅威になるなら、「中」のアクションも切断にした方がよいでしょう。

しかし「高」や「中」レベルを切断すると、本来通過してよいトラフィックまでが拒否される場合もあります。

その場合は例外を設定することにより、意図せずして拒否されるトラフィックを許可することができます。

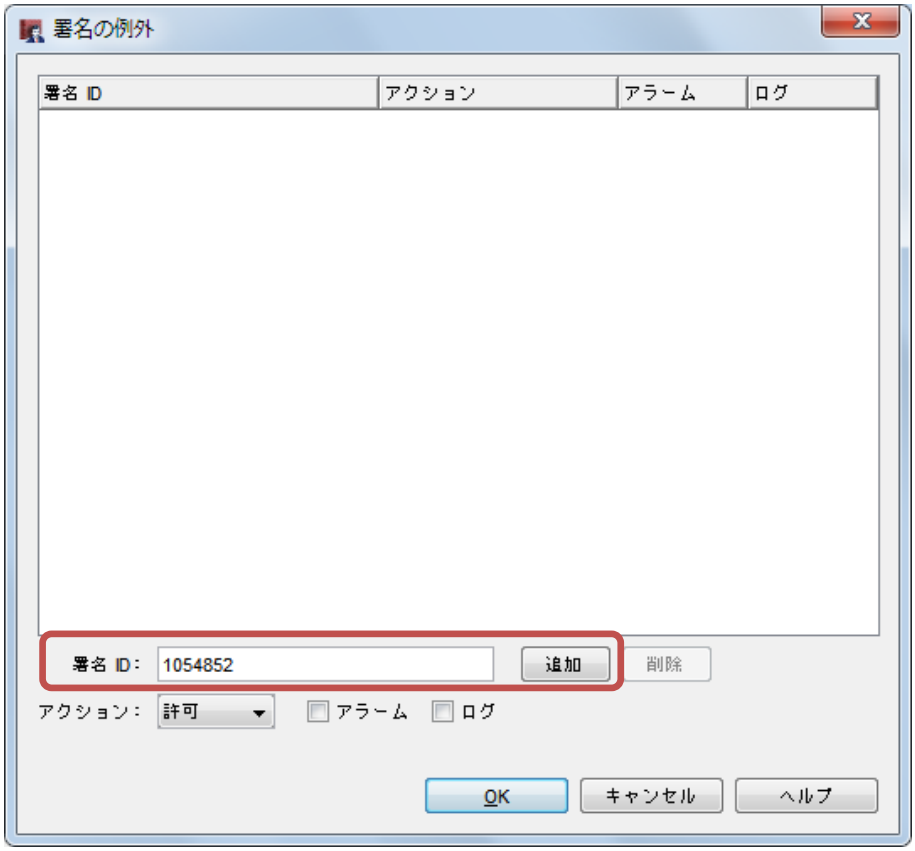
例外の設定

例外ボタンをクリックします。

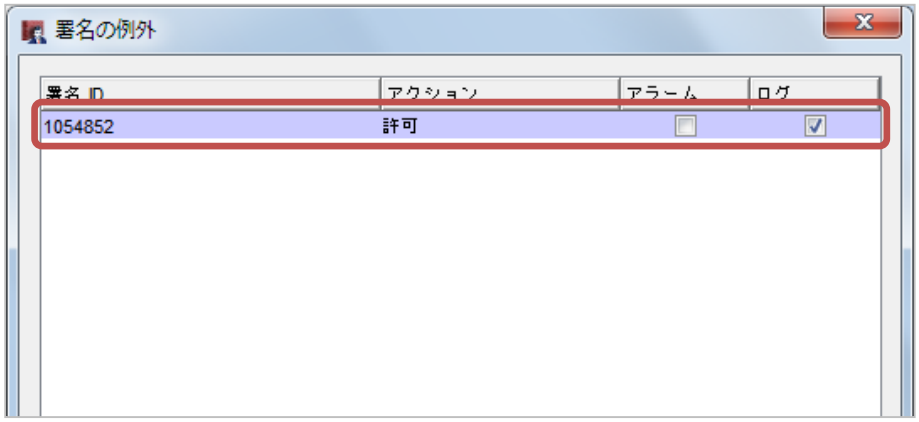


署名の例外ウィンドウが開きますので、ID を入力し、追加ボタンをクリックし、例外の一覧に加えます。

たとえば 1054852 というシグネチャ ID のトラフィックを許可しないと PHP プログラムが正常に動作しない場合(あくまでも例です)には、テキストフィールドに 1054852 を入力し、追加ボタンをクリックします。



すると、次のように一覧に追加され、この ID で検知されるトラフィックは許可されるようになります。



Reputation Enabled Defense

Reputation Enabled Defense（以下 RED）は、世界中のデバイスから収集されたレピュテーション（評判）の集合知を利用して、脅威を検知することができます。

RED はクラウドのデータベースを利用するので、ゲートウェイでのパフォーマンスを改善します。Gateway Anti-Virus を単体で使用した場合と比較すると、Web トラフィック処理の性能は 30～50%向上します。

RED 構成時の注意点

Gateway Anti-Virus が有効な HTTP-proxy ポリシーに対して RED を有効にすると、レピュテーションの良し悪しが既に分かっているサイトのウイルススキャンをスキップするため、全体的なパフォーマンスが改善します。

しかし Gateway Anti-Virus が有効でない場合に RED を有効にすると、HTTP プロキシはすべての URL でレピュテーションスコアを参照するため、RED が無効な場合と比べて当然負荷は高くなります。

効果とパフォーマンスを最大限にするために、RED と Gateway Anti-Virus の両方を有効にすることをお勧めします。

また、レピュテーションの閾値について理解しておく必要があります。

2 つのレピュテーション スコアを設定できます。

悪いレピュテーションの閾値	URL のスコアが悪いレピュテーションのしきい値より大きい場合、HTTP プロキシは検査せずにアクセスを拒否します
良いレピュテーションの閾値	URL のスコアが良いレピュテーションのしきい値より小さい場合、Gateway Anti-Virus が有効に設定されていると、HTTP プロキシによって Gateway AV スキャンがバイパスされます。

たとえば悪いレピュテーションの閾値が 90、良いレピュテーションの閾値が 20 と設定するとします。

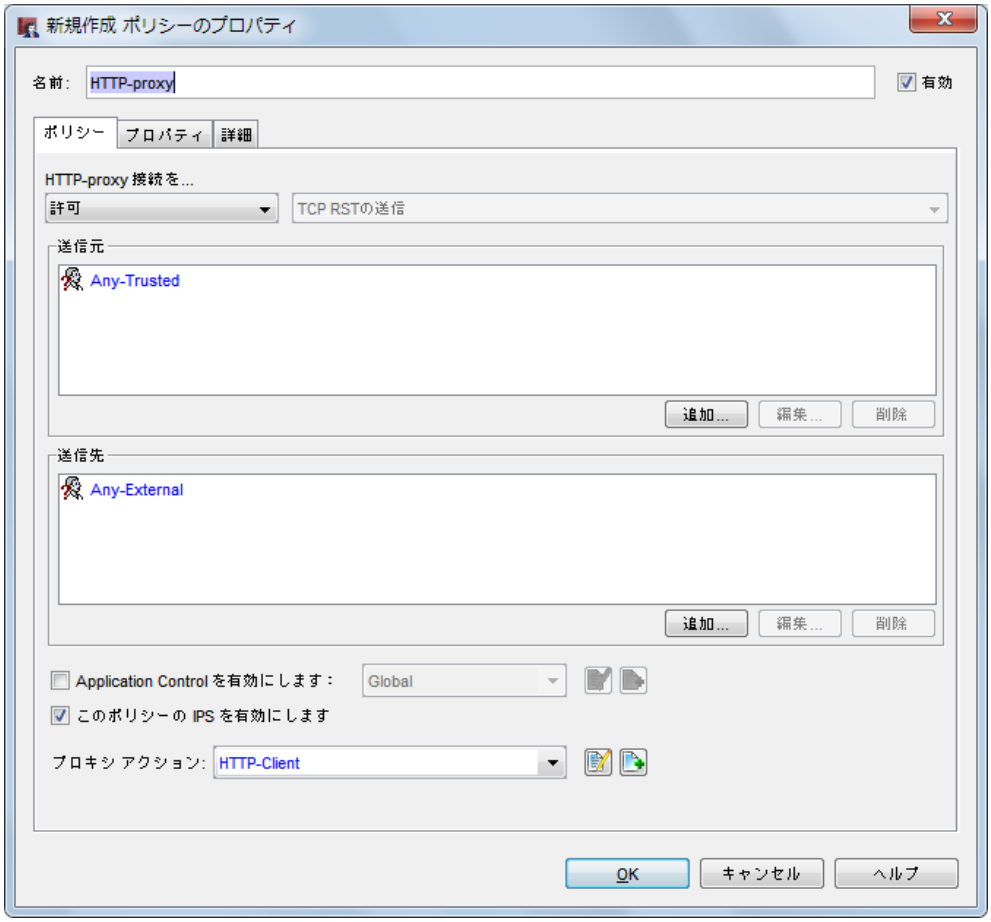
90 を越えるサイトは即座に拒否し、20 を下回るサイトはそのまま AV スキャンはバイパスされる、その中間のスコアのサイトは AV スキャンが行なわれるというわけです。

ポリシーの追加

最初に HTTP-proxy ポリシーを作成しておく必要があります。

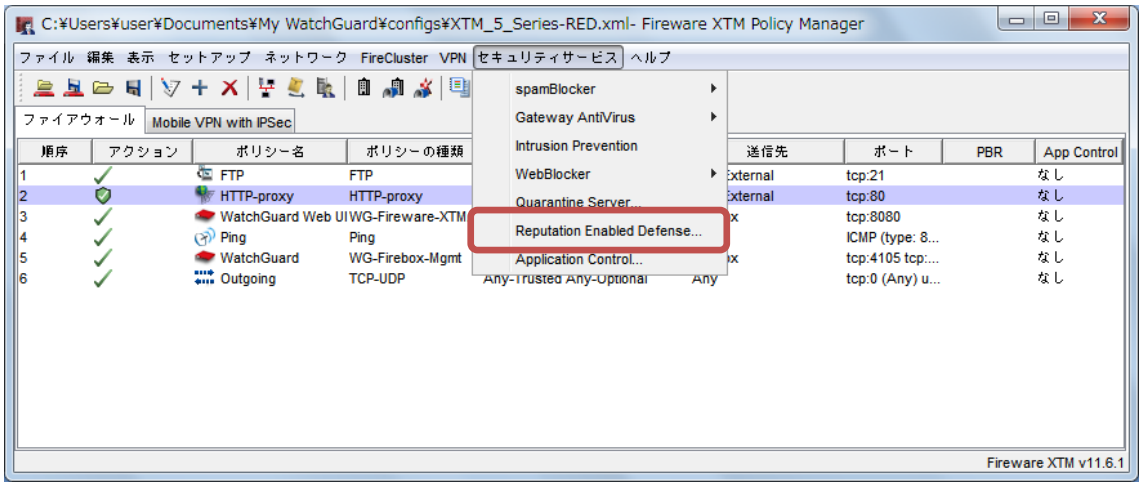
HTTP-proxy ポリシーを作成しないで RED を有効にしようとすると警告が出て設定できませんので、これまで同様、あらかじめ作成しておきます。

そのまま OK をクリックし、ポリシーを追加します。

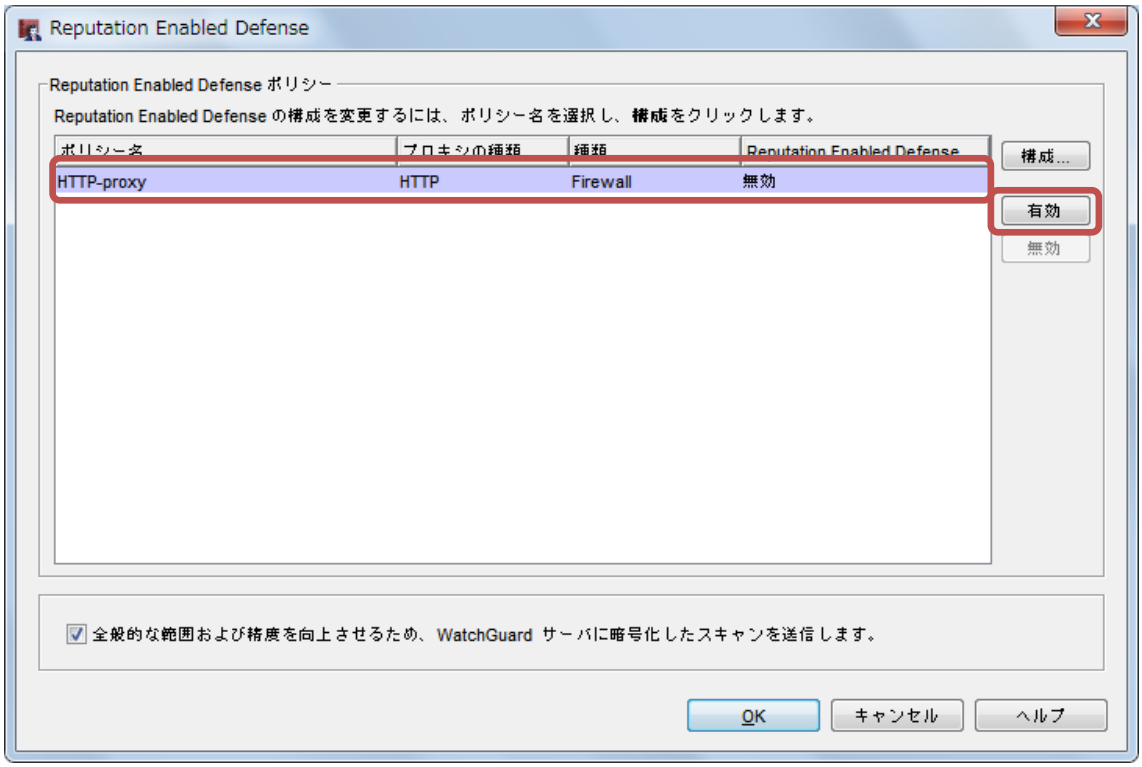


RED の構成

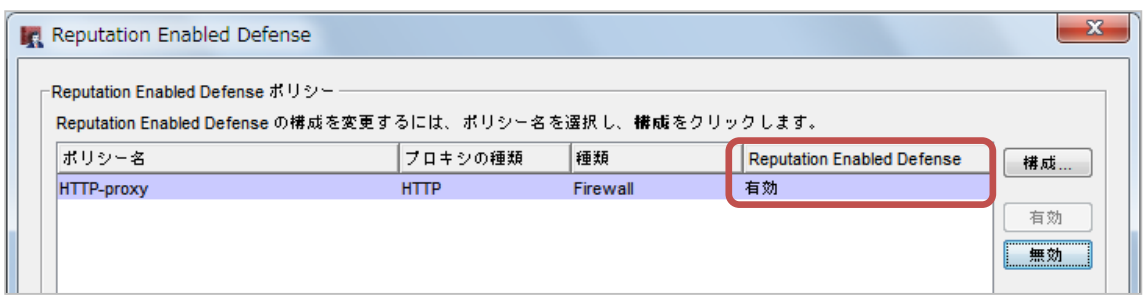
RED を有効にするために、ポリシーマネージャのメニュー セキュリティサービス ー Reputation Enabled Defense をクリックします。



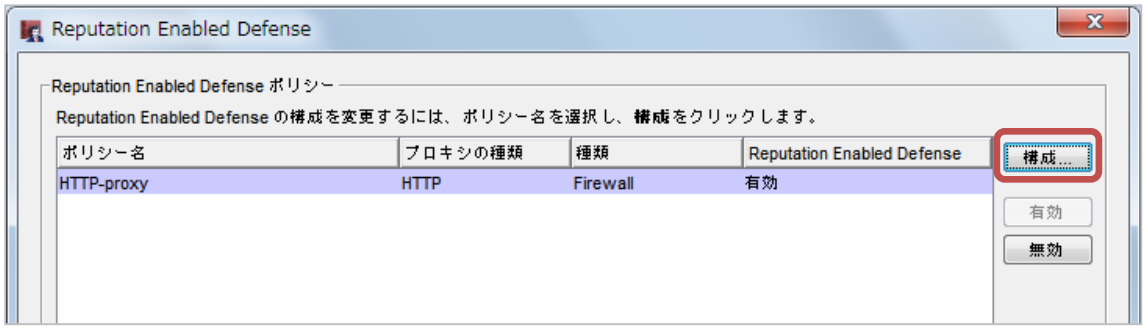
RED の構成画面で先ほど作成した HTTP-proxy ポリシーを選択し、有効ボタンをクリックします。



RED が有効になります。

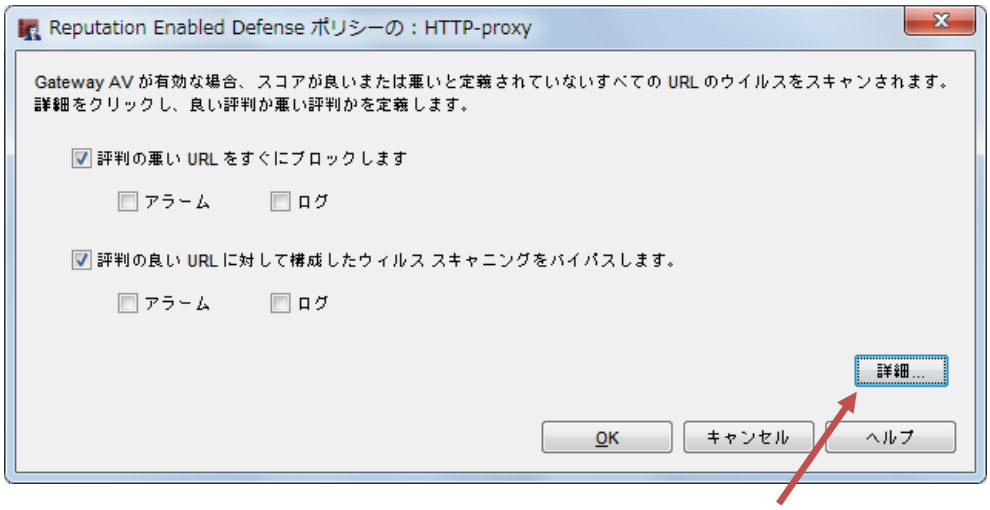


構成ボタンをクリックします。



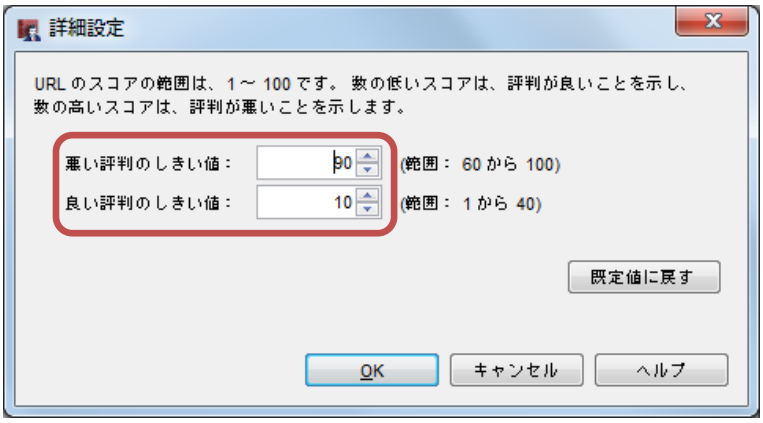
評判の悪い URL、良い URL について、それぞれアクションを設定することができます。

デフォルトで、閾値を越えた URL については、ブロックもしくはバイパスするようになっています。



悪い評判と良い評判の閾値は「詳細」ボタンから設定できます。

悪い評判は 60 以上、良い評判は 40 以下を設定できます。



あまり極端に値を上下させると、意図せずして AV スキャンをスルーしたり、問題ないと思えるサイトを拒否してしまったりする恐れがあります。ログを確認しながら少しずつ調整することをお勧めします。

Gateway Anti-Virus ではなく RED で検知された場合は、拒否画面の理由に「reputation」と表示されます。

※メッセージは日本語表示にカスタマイズしています

おわりに

WSM 基本設定ガイドは以上です。

XTM がいかに容易に導入・設定でき、且つ高度なセキュリティを確保できるか、実感していただけたかと思います。

XTM のマニアになっていただいたなら、ぜひ御社のネットワーク・セキュリティを XTM に統一していただき、最高度の機能・性能・安心を手に入れていただきたいと思います。

今後も弊社の製品が、御社のセキュリティの要としてお役に立てれば幸いです。