WebUI ガイド

REV 2.0

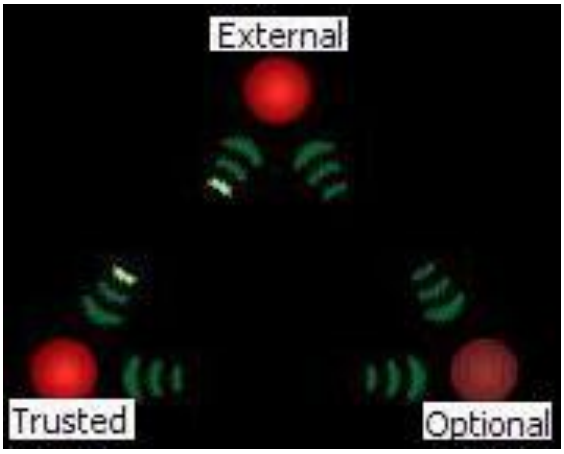
目次

第一章　XTM のセキュリティ概念

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



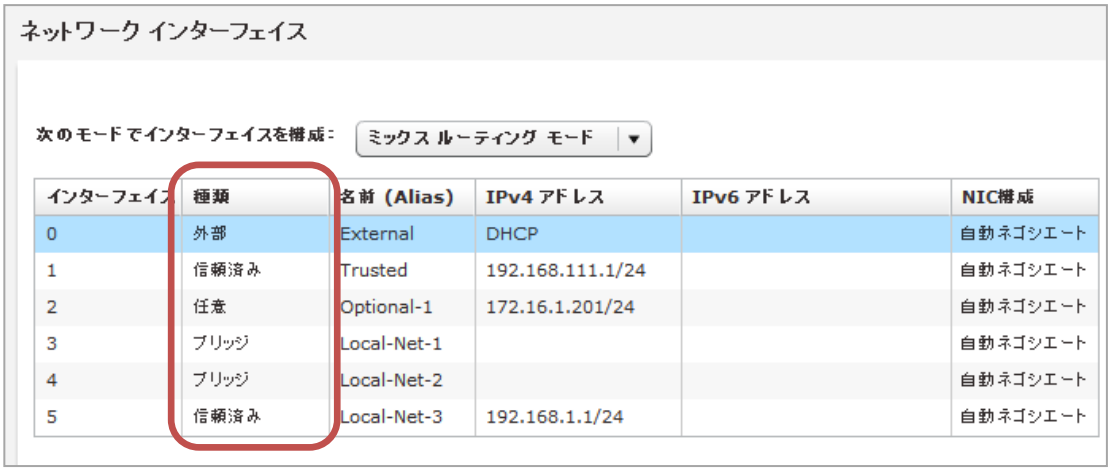
この「三角関係」、すなわち 3 種類のネットワークのゾーンを意識するなら、XTM の設定は非常に容易です。

WebUI の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 External(外部)、3 が Optional(任意)、それ以外は Trusted(信頼済み)として設定しています。



インターフェイス	種類	名前 (Alias)	IPv4 アドレス	IPv6 アドレス	NIC構成
0	外部	External	DHCP		自動ネゴシエート
1	信頼済み	Trusted	192.168.111.1/24		自動ネゴシエート
2	任意	Optional-1	172.16.1.201/24		自動ネゴシエート
3	ブリッジ	Local-Net-1			自動ネゴシエート
4	ブリッジ	Local-Net-2			自動ネゴシエート
5	信頼済み	Local-Net-3	192.168.1.1/24		自動ネゴシエート

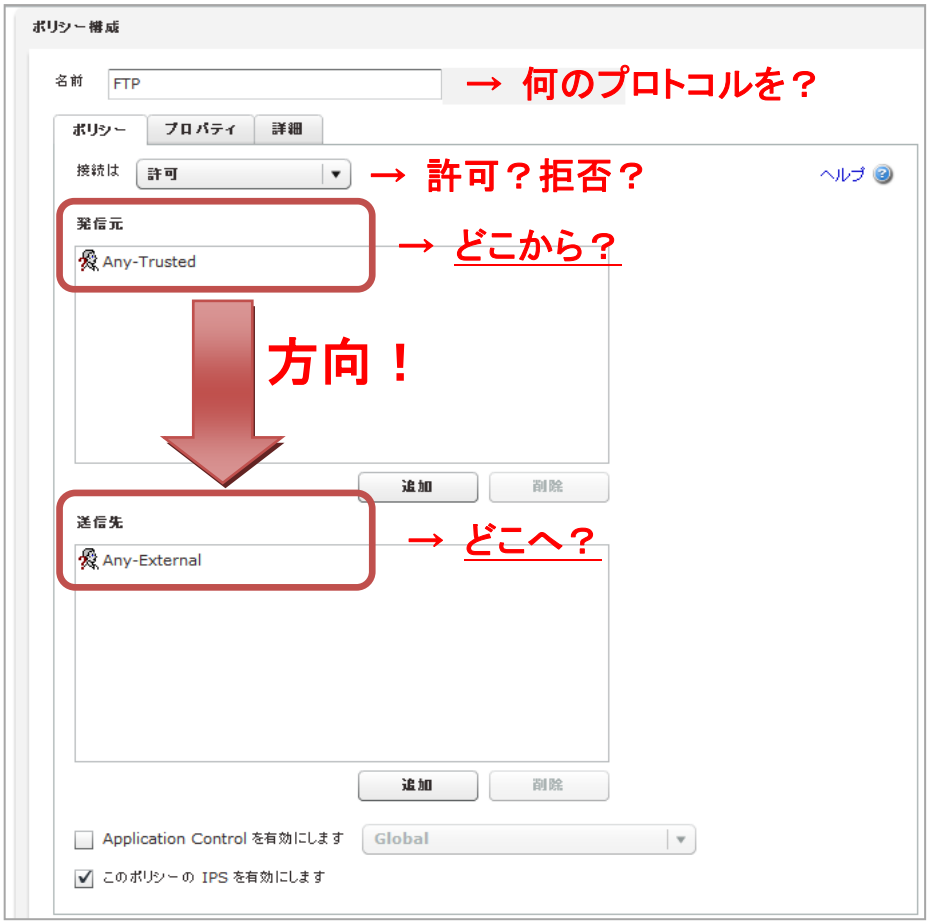
（一部ブリッジですがこれも Trusted です。ブリッジの構成は後述します）

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ありません。

WebUI のポリシー設定画面に見る XMT の概念

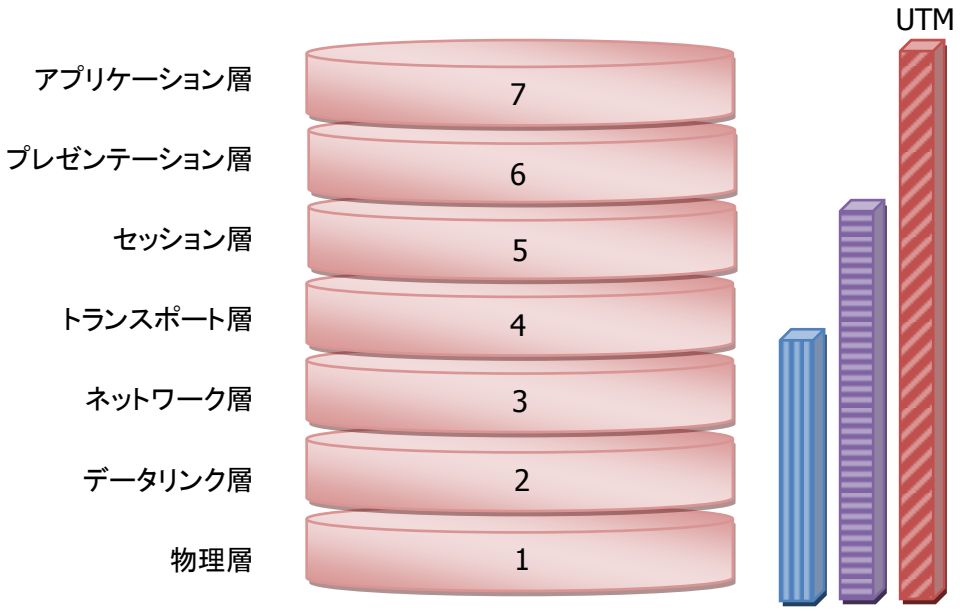
以下は実際のポリシー構成画面です。(後ほど詳しく解説します)

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。

パケットフィルター　：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

WebUI の概要

WebUI は、管理 PC に追加のソフトウェアをインストールせずに、 XTM デバイスを管理および監視することができます。 必要となる唯一のソフトウェアは、Adobe Flash に対応しているブラウザです。

これは、Adobe Flash 9 対応ブラウザとネットワーク接続さえできれば、Windows、Linux、Mac OS、また他のどんなプラットフォームのコンピュータからでも XTM デバイスを管理できることを意味します。

Web UI は、リアルタイム管理ツールです。 これは、デバイスに変更を行うために Web UI を使用する場合、行なった変更はすぐに反映されます。

WebUI の制限事項

すべての設定は、WSM に含まれる Policy Manager で完了できますが、WebUI では制限事項があります。完了できないタスクは以下のとおりです(XTM_OS 11.6.1 時点)。

- 証明書のエクスポートまたは証明書の詳細表示 (証明書のインポートのみ可能)
- 診断ログ記録の開始と診断ログのレベル変更
- 既定のパケット処理オプションのログ記録の変更
- Branch Office VPN イベントの通知の有効化または無効化
- デバイスの ARP テーブルに対する、静的 ARP エントリの追加と削除
- 手動での Mobile VPN with SSL 構成ファイルを取得する
- 暗号化された Mobile VPN with IPSec エンドユーザー用クライアント構成 (.wgx ファイル) の取得 (同様な非暗号化 .ini ファイルの取得のみ可能)
- ポリシーの名前を変更する
- カスタム アドレスをポリシーに追加する
- ホスト名 (DNS 参照) を使用してポリシーに IP アドレスを追加する
- ロールに基づいた管理を行う (ロールベース アクセスコントロールまたは RBAC とも呼ばれます)
- FireCluster のメンバーであるデバイスの構成を表示または変更する

WatchGuard System Manager に付属しているアプリケーションのグループには、監視機能とレポーティング機能など、多くのツールがあります。HostWatch、Log andReport Manager、および WSM で提供される各種ツールの一部も WebUI では利用できません。

第二章　初期設定

事前準備

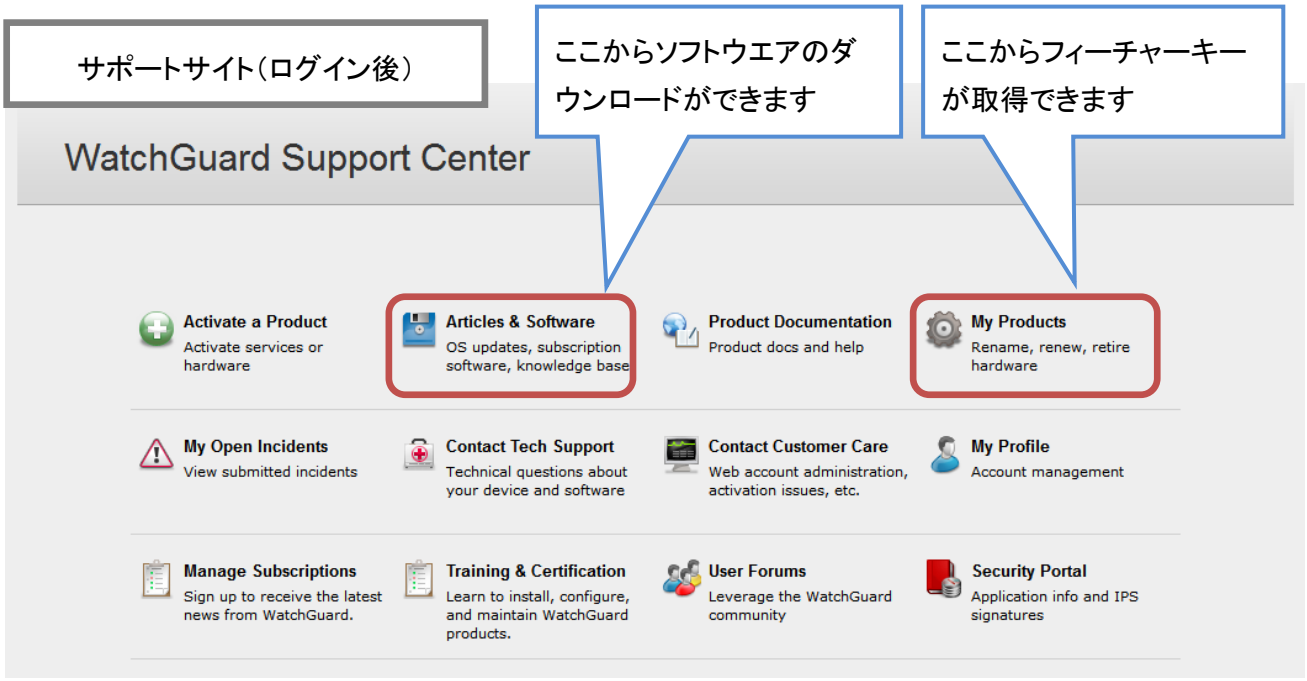
事前準備としてセットアップに必要なソフトウェアをインストールします。製品アクティベート後、WatchGuard Support (US)サイト内の『Articles & Software』より必要なソフトウェアを取得します（ログインが必要）。

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。前述のとおり、WebUI には WSM と比較して若干の制限事項がありますので、すぐに使わないとしても、管理者の方にはあらかじめインストールしておくことをおすすめします。

インストーラーはすべてデフォルトで進めます。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

ファクトリーリセットとは 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[1]。

手順については機種によって 2 通りあります。

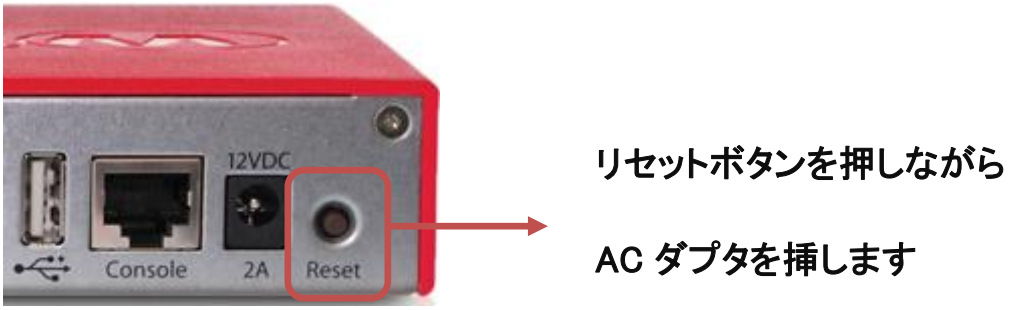
XTM2/3 シリーズ(330 除く)

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。



[1] 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

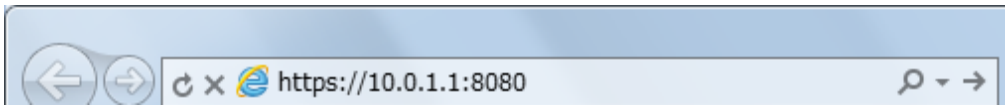
設定する PC 側の設定は、以下のように固定 IP アドレスを設定しておいてください。

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

Web Setup Wizard

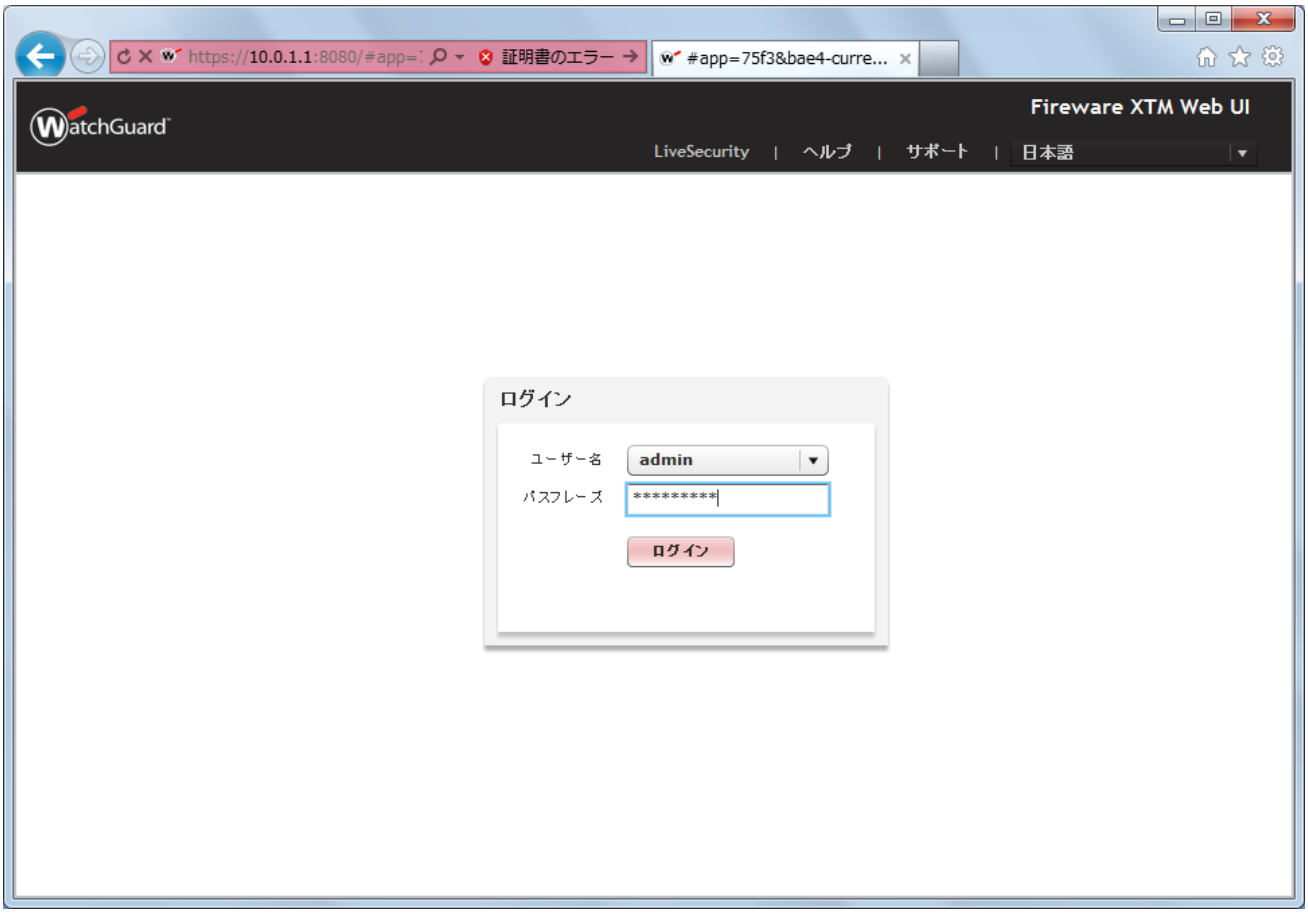
機器を Safe Mode で起動したら、Web Setup Wizard で初期設定を行ないます。

設定する PC と Safe Mode で起動した XTM のインターフェース 1 を LAN ケーブルで接続し、ブラウザのアドレスバーに https://10.0.1.1:8080 を入力し、アクセスします。



証明書のセキュリティ警告が出てもそのまま続行します。

するとログイン画面が表示されますのでパスフレーズに「readwrite」を入入力します。



Wizard が始まりますので「次へ」ボタンをクリックします。

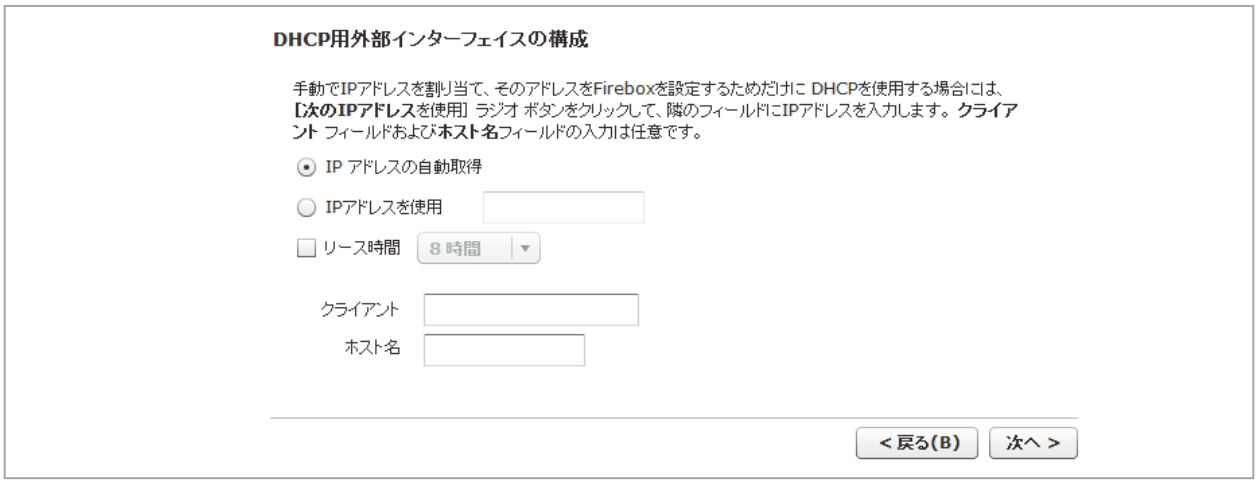
初期設定が目的なので「新しい Firebox 構成を作成します」にチェックして次へ。

使用許諾契約の条項に同意していただき次へ。

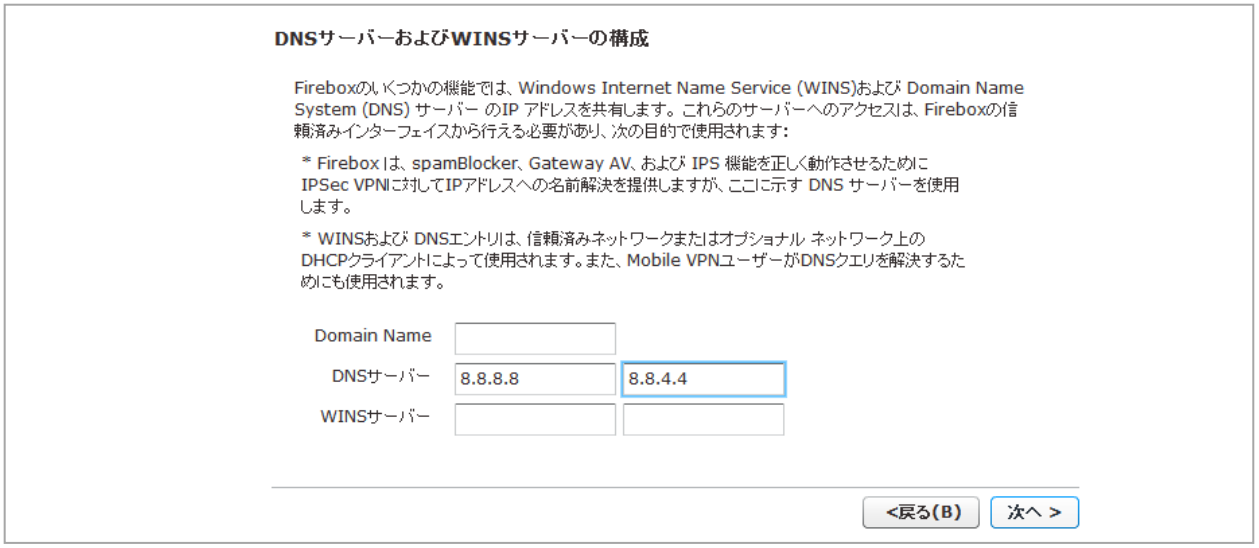
外部インターフェースはまだ構成がはっきり決まっていない場合はそのまま次へ。

構成が決まっている場合でも、後から WebUI で設定できますので、このまま進んで構いません。

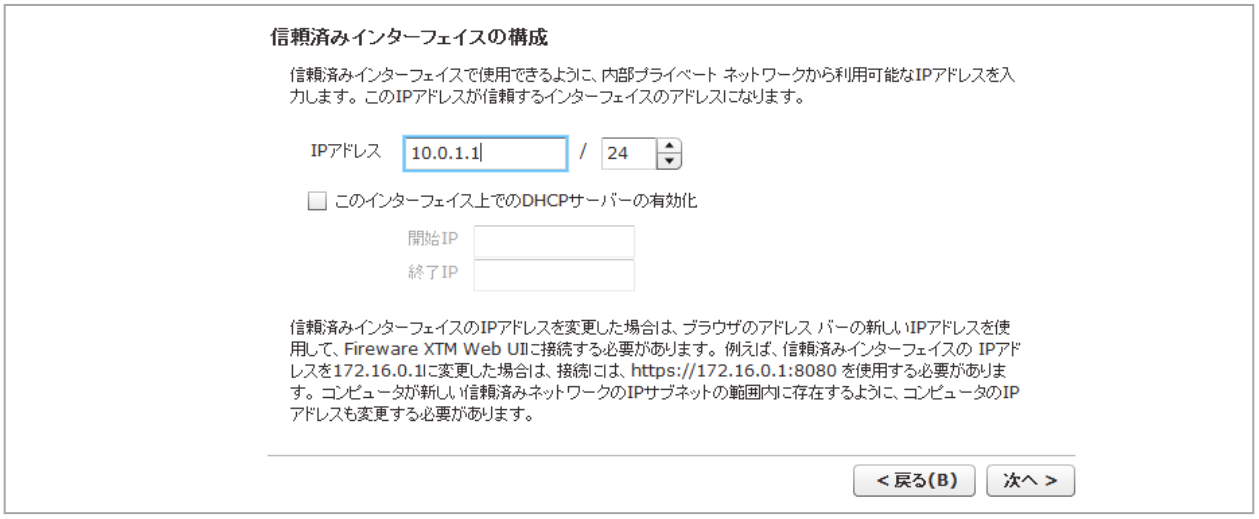
次へ。



DNS サーバーの指定です。後から設定できますが、決まっていましたら入力して次へ。

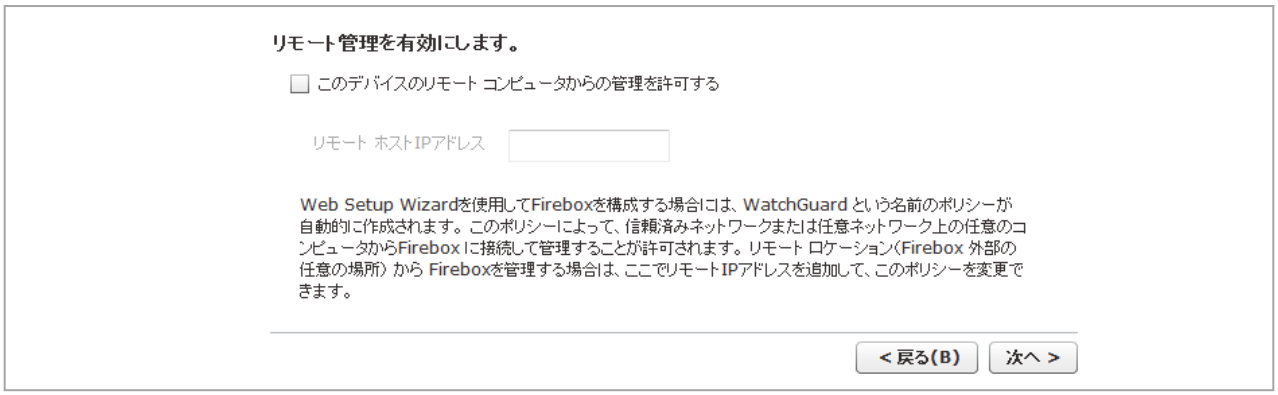


信頼済みインターフェース(現在接続しているポート)の設定です。次へ。

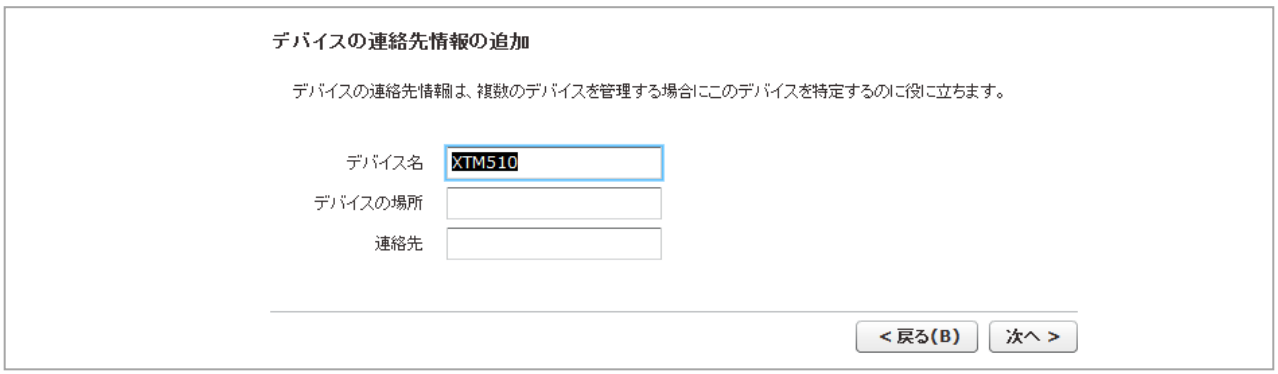


パスフレーズの設定です。status ユーザーは設定の読み取り専用のアカウント、admin ユーザーは設定が保存できる管理者アカウントです。それぞれを 8 文字以上の英数字で設定します。
status と admin は同じパスフレーズを使用することはできません。

リモート管理の有効化はしないで次へ。（ポリシーの画面で変更できます）



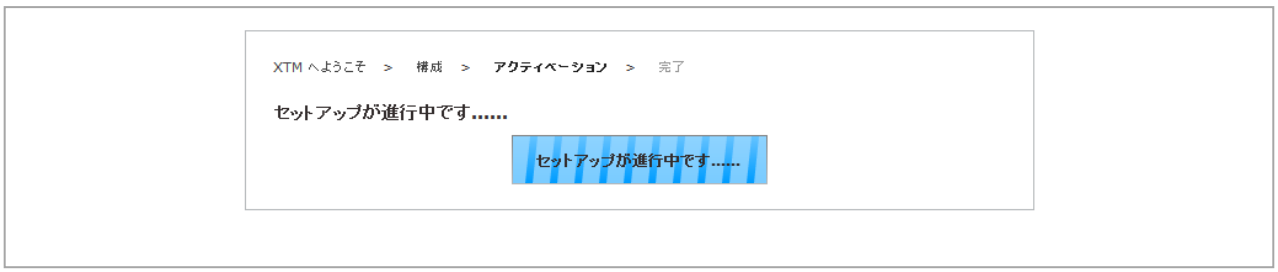
デバイス名を入力し次へ。



タイムゾーンは「(GMT+09:00)大阪、札幌、東京」を選択して次へ。

最後に設定のサマリーが表示されます。次へ。

設定が反映されます。



セットアップ完了が表示されます。完了ボタンをクリックします。

初期セットアップは以上で完了です。

機能キーの追加

機能キー(フィーチャーキー)は簡単に言えば、機能を有効にするライセンスキーです。

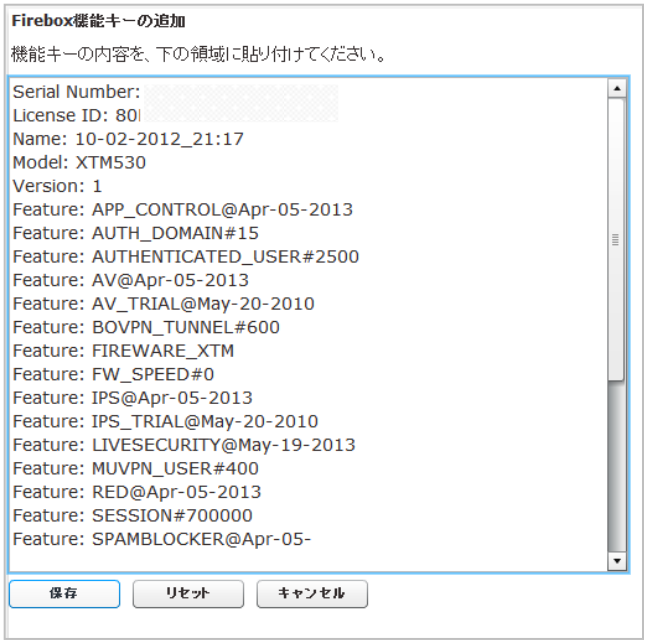
これをデバイスに追加しない間は、XTM は限定的な状態で動作します。また、新たに追加で購入した機能も、アップデートされた新しい機能キーを追加しなければ有効になりません。

ですので、各種設定に入る前に、機能キーをデバイスに追加する方法を解説します[2]。

左側メニュー システム ー 機能キー からアクセスします。
機能キーの画面が表示されたら、アップデート ボタンをクリックします。

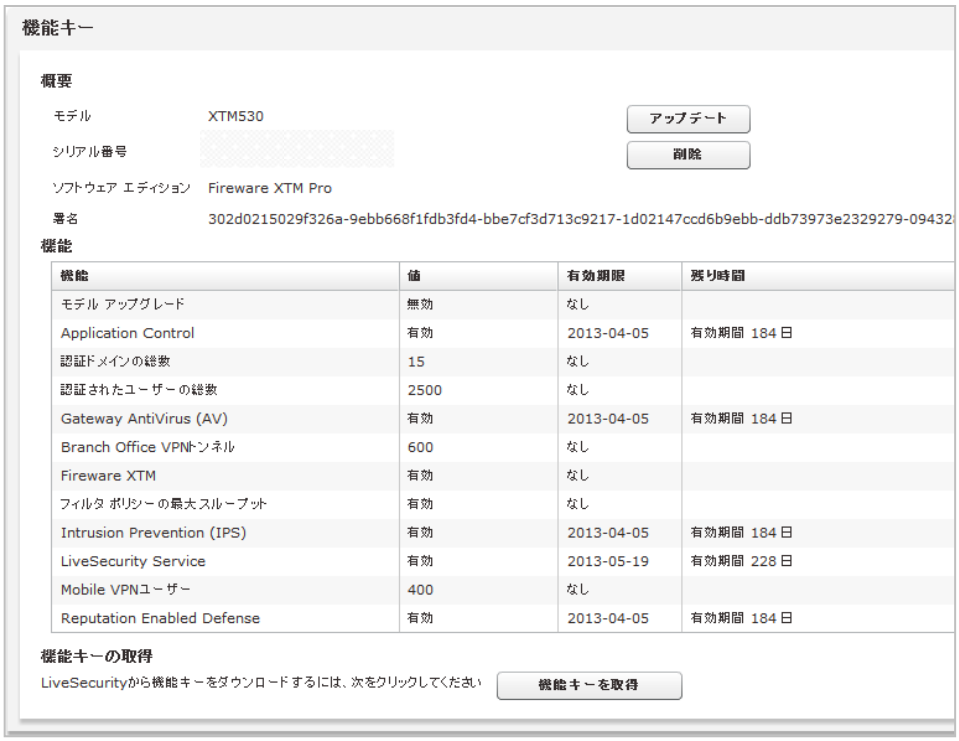
[2] 機能キーの取得方法は「第二章 初期設定」の「事前準備」の項をご覧ください

機能キーを入力するテキストボックスに、あらかじめ取得した機能キーをコピー＆ペーストします。



貼り付けたら保存ボタンをクリックします

正規のライセンスを追加できると、以下のような画面になります。



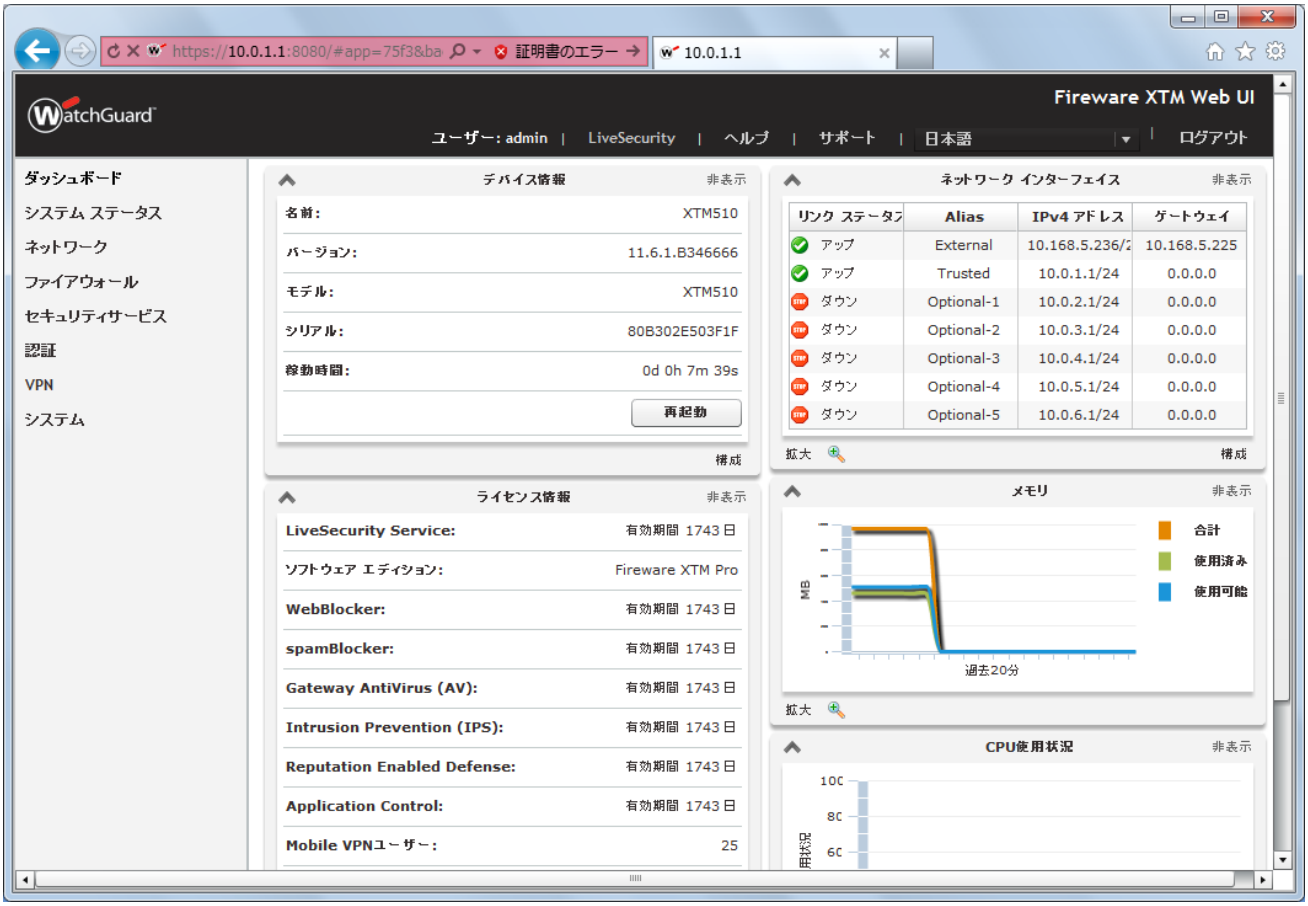
機能が有効になり、有効期限と残りの日数が表示されます。

第三章　ネットワークの設定

それでは前章で初期設定を施した XTM に、WebUI で接続してみましょう。

ブラウザで https://10.0.1.1:8080 に再び接続します。
パスフレーズは、Wizard で設定した構成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。

ログインすると最初に XTM の状態を表わすダッシュボードが表示されます。



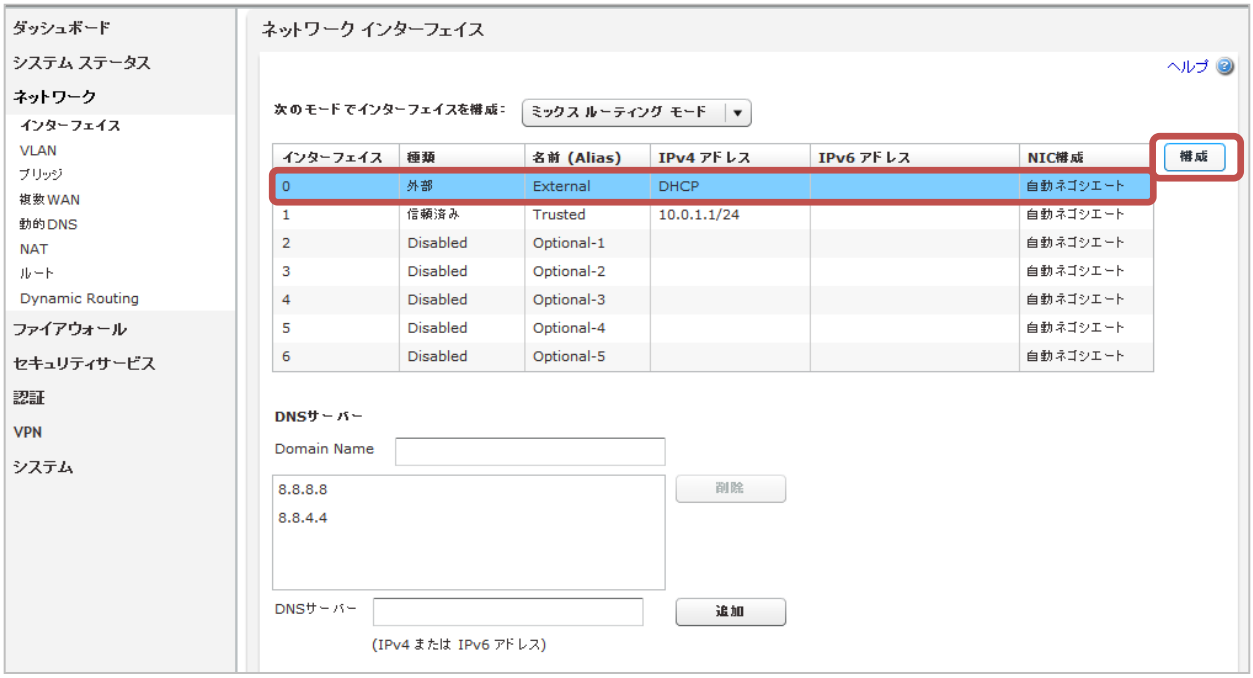
インターフェースを設定するには、左側メニュー ネットワークのインターフェースをクリックします。

このネットワークインターフェース画面から、各インターフェースの設定ができます。

外部ネットワークの設定

まずは外部インターフェースから設定しましょう。

該当のインターフェースを選択して、右の構成ボタンをクリックします。



次頁のように、インターフェースの詳細を設定できる画面が開きます。

選択したインターフェースの詳細設定画面になります。

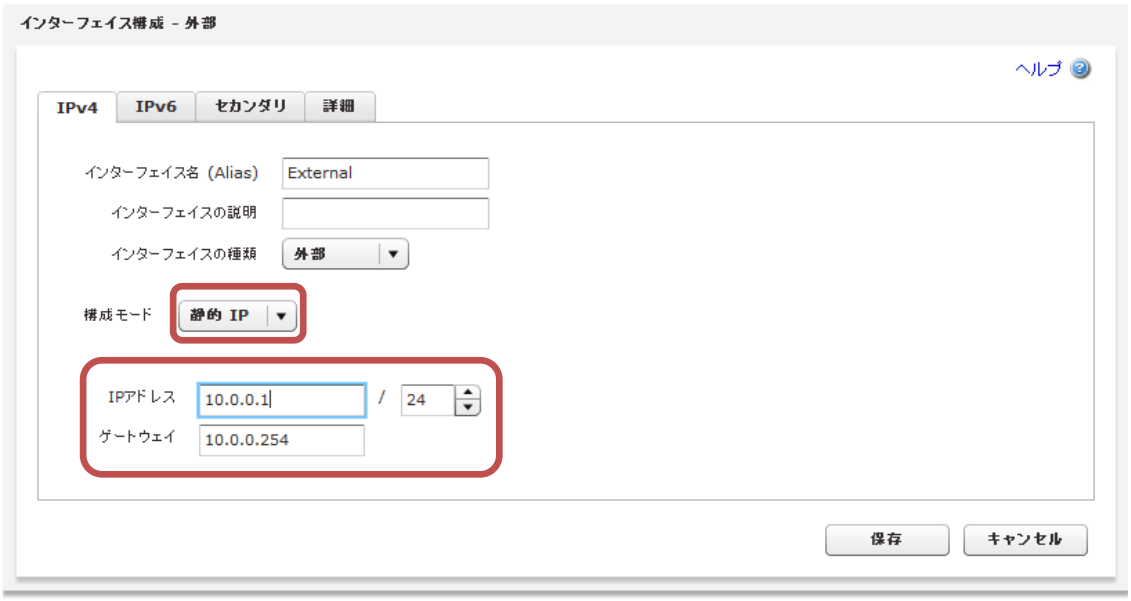
最初にインターフェース名を設定することができます。

すべてのインターフェース名(エイリアス)は任意で命名できます。外部インターフェー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。

たとえば複数 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。

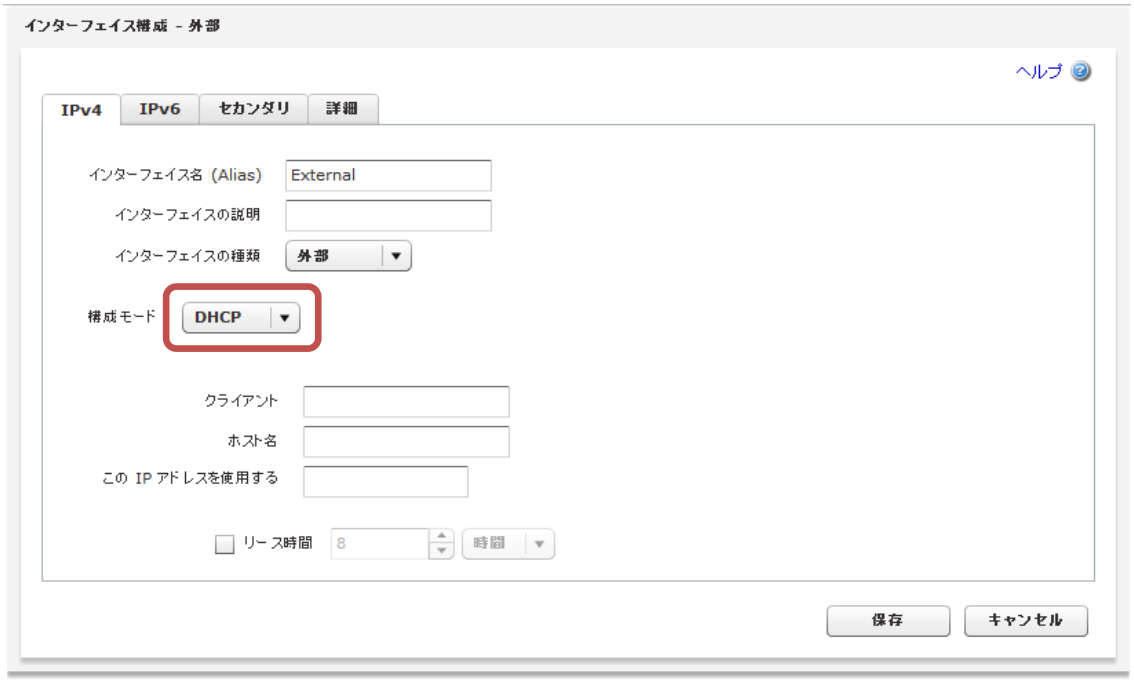
固定 IP の設定

構成モードで静的 IP を選択し、IP アドレス、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

構成モードで DHCP を選択するだけです。

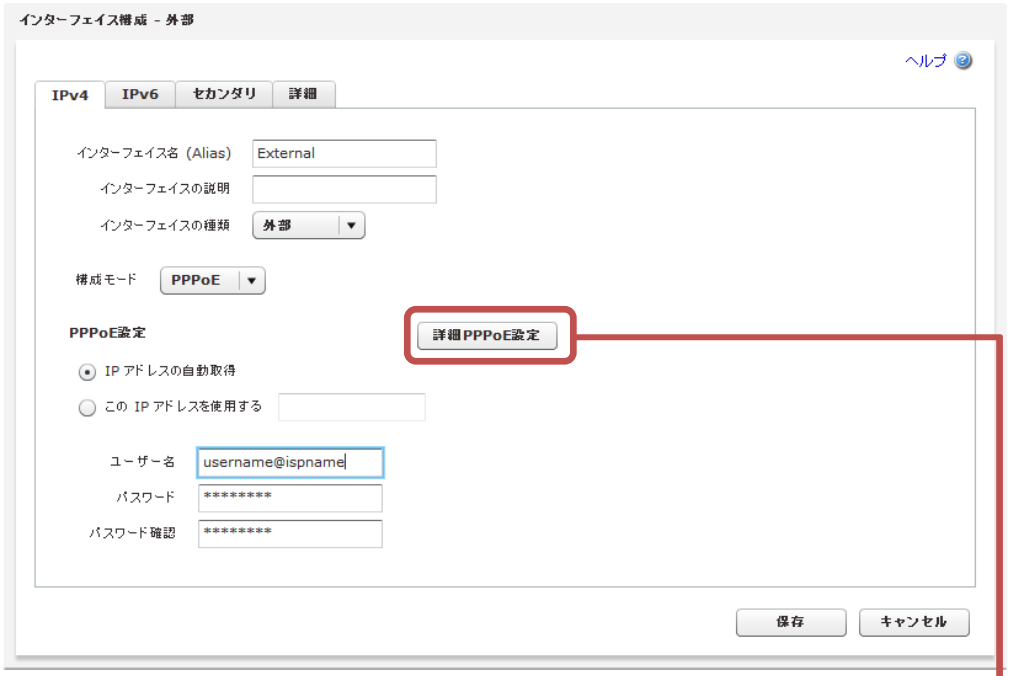


ISP 又は DHCP サーバーがクライアントを識別するために、MAC アドレスやホスト名の情報が必要になる場合があります。その際には、指示に従ってクライアント、ホスト名の欄に入力してください。

PPPoE の設定

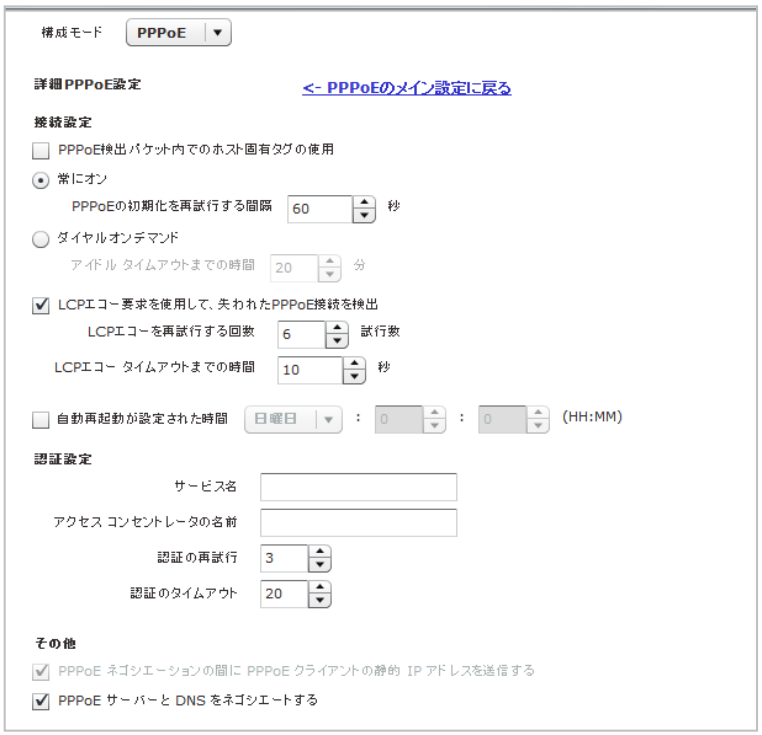
構成モードで「PPPoE」を選択します。ユーザー名とパスワードは、ISP から指定されたものを入力します。

IP アドレスが固定であれば「この 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 PPPoE 設定」ボタンをクリックし、指定の項目を設定してください。



DNS/WINS 設定

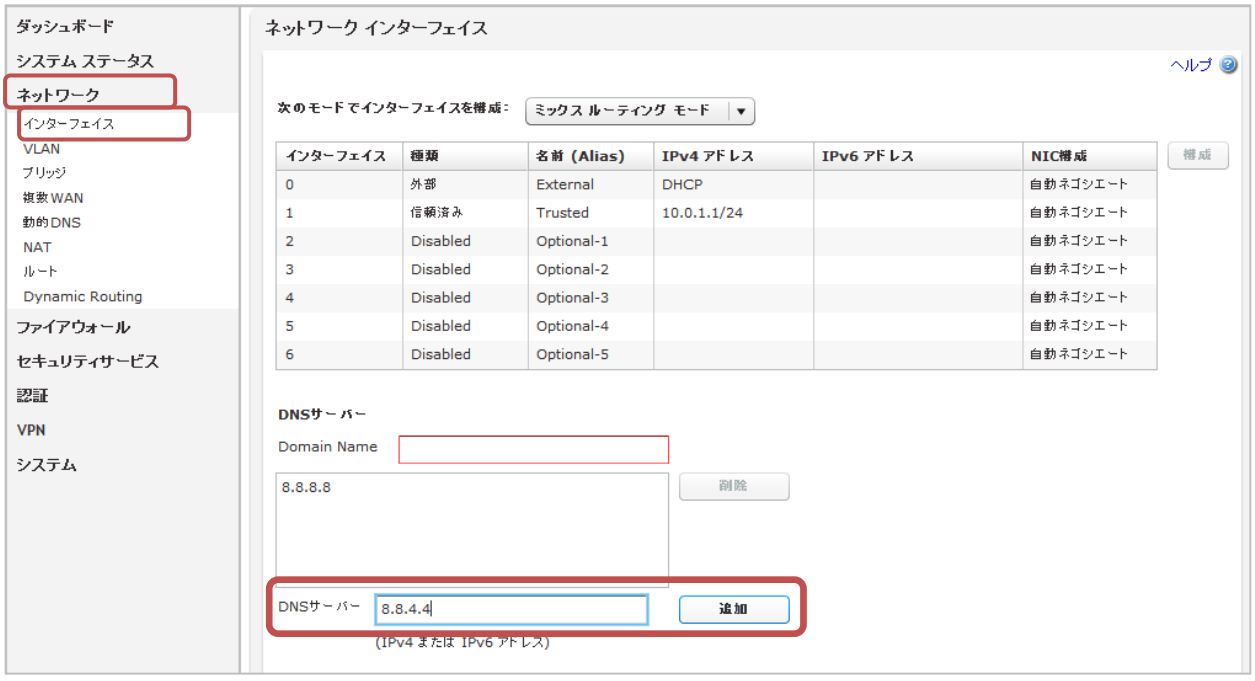
ネットワーク機器である XTM 自身になぜ DNS を設定する必要があるのでしょうか？以下のような理由があります。

- 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
- 内部 DHCP クライアントへの DNS サーバーアドレスの配布
- NTP サーバを FQDN で設定した際の名前解決
- 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 リレーは行いません。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

左側メニューのネットワーク－インターフェースをクリックし、ネットワークインターフェース画面のインターフェース一覧を表示します。
一覧の下にある DNS サーバーの欄に入力し、追加ボタンをクリックして追加します。



スクロールして画面右下にある「保存」ボタンをクリックして設定を保存します。

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。

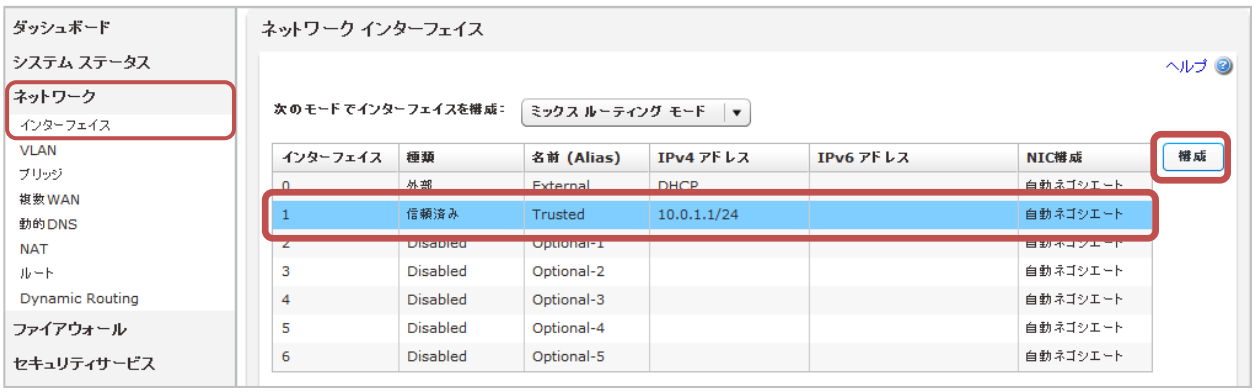
画面右下の「保存」ボタンをクリックし、設定を保存します。

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ース同様、左側メニューの[ネットワーク]－[インターフェース] の画面から行ないます。

インターフェース一覧より、設定したいインターフェースを選択し、構成ボタンをクリックすることで、インターフェースの設定画面を開きます。



Trusted インターフェースの設定

設定画面は外部インターフェースと同様です。インターフェース名(エイリアス)は任意に設定できます。

ここでは Trusted-1 というインターフェース名を付けています。

そして、このポートに割り当てる IP アドレスとサブネットマスクのビット数を入力し、保存します。

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、インターフェースの設定画面の下方にあるドロップダウンリストから、「DHCP サーバーの使用」を選択します。

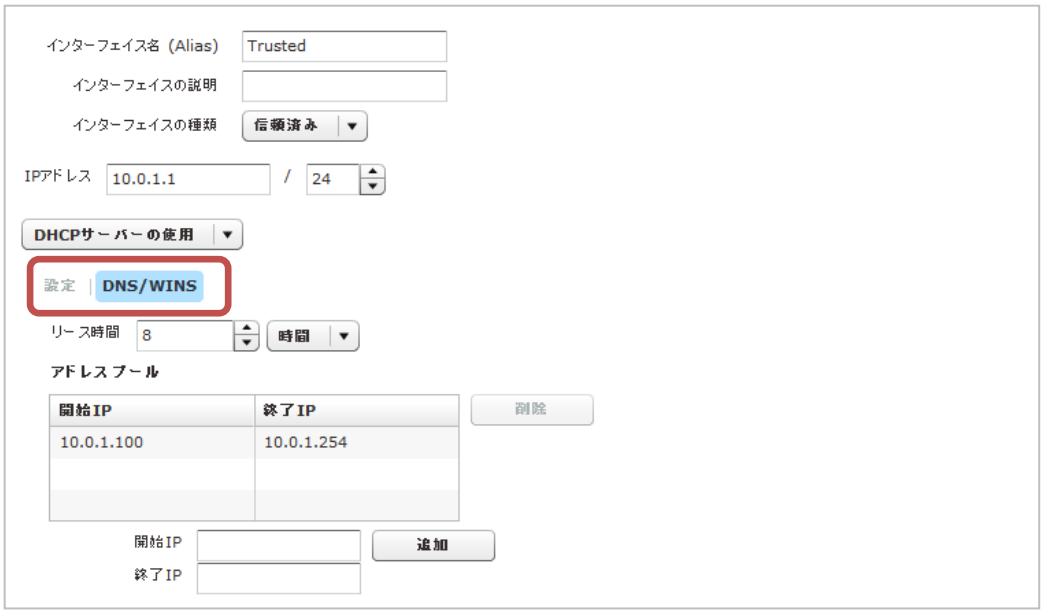
アドレスプールの追加ボタンをクリックし、配布する IP アドレスの範囲を入力します。

例ではセグメント 4 オクテット目の 100 以降の IP アドレス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。

追加すると一覧に表示されます

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)

「DHCP サーバーの使用」のドロップダウンリストの下の「DNS/WINS」のリンクをクリックします。



クライアントに設定したい DNS サーバーの情報を入力し、追加します。

WINS サーバーがあれば同じ要領で追加できます。

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。

例として 2-5 番のインターフェースをブリッジとして構成しましょう。

インターフェース一覧の画面でブリッジにしたいものを選んで構成ボタンをクリックします。

インターフェース名を入力し、インターフェースの種類でブリッジを選択し、保存します。

無効だったインターフェースが、次のようにブリッジに変更されました。

インターフェイス	種類	名前 (Alias)	IPv4 アドレス	IPv6 アドレス	NIC構成
0	外部	External	DHCP		自動ネゴシエート
1	信頼済み	Trusted-1	10.0.1.1/24		自動ネゴシエート
2	ブリッジ	Trusted-2			自動ネゴシエート
3	Disabled	Optional-2			自動ネゴシエート
4	Disabled	Optional-3			自動ネゴシエート
5	Disabled	Optional-4			自動ネゴシエート
6	Disabled	Optional-5			自動ネゴシエート

残りのインターフェースも同じように設定してゆきます。

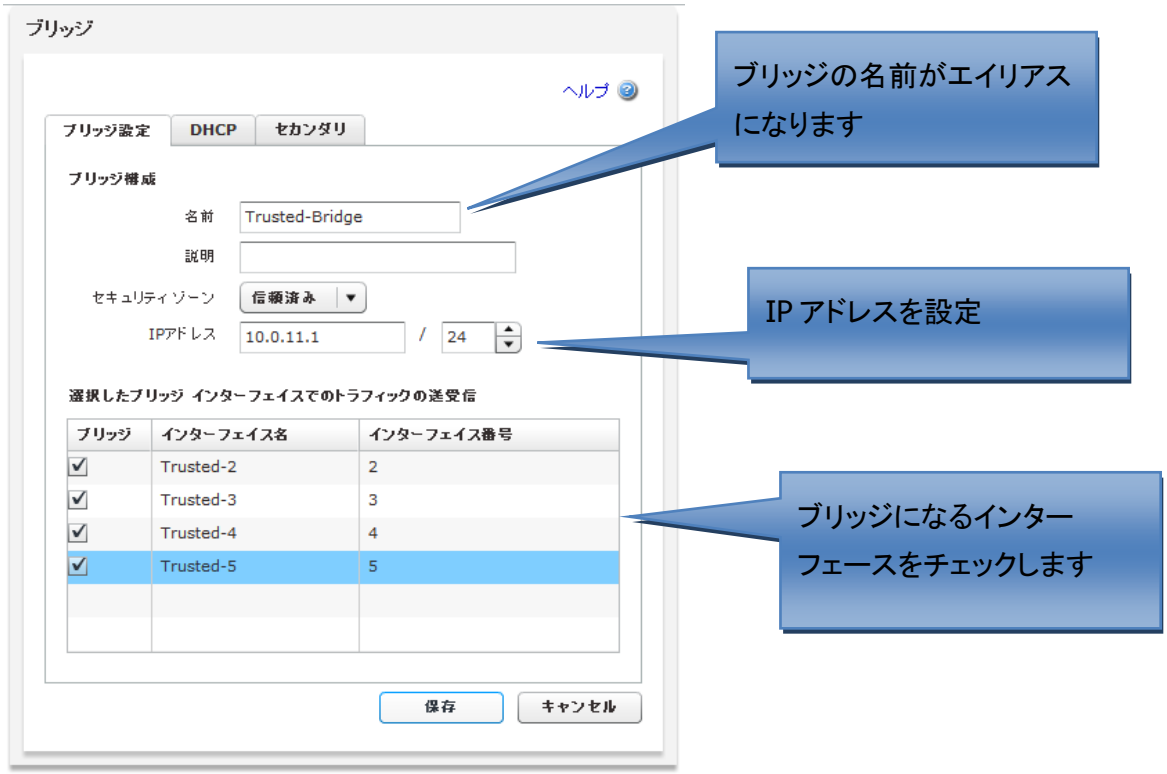
以上でどのインターフェースをブリッジにするか指定できました。

インターフェイス	種類	名前 (Alias)	IPv4 アドレス	IPv6 アドレス	NIC構成
0	外部	External	DHCP		自動ネゴシエート
1	信頼済み	Trusted-1	10.0.1.1/24		自動ネゴシエート
2	ブリッジ	Trusted-2			自動ネゴシエート
3	ブリッジ	Trusted-3			自動ネゴシエート
4	ブリッジ	Trusted-4			自動ネゴシエート
5	ブリッジ	Trusted-5			自動ネゴシエート
6	Disabled	Optional-5			自動ネゴシエート

次にブリッジを定義します。左側メニュー インターフェース－ブリッジより、ブリッジの構成画面を開きます。

新規作成ボタンをクリックし、ブリッジを追加しましょう。

ブリッジの追加画面では、まず、ブリッジにつける名前を入力します。これがエイリアスになります。



セキュリティゾーンは「信頼済み」を選択し、インターフェースに設定する IP アドレスとサブネットマスクを入力します。そしてブリッジにするインターフェースにチェックを入れます。

以上で保存してください。

以上の設定を施すと、Trusted(信頼済み)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。これを用いて設定をすれば、複数のエイリアスにも一括してポリシーを適用できるというわけです。

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。

ブリッジでも Trusted インターフェースで設定したように DHCP サーバーを構成することができます。
(次頁)

DHCP タブに移り、DHCP モードで「DHCP サーバー」を選択します。

IP アドレスプールを指定します。

画面の下方にスクロールすると、DNS サーバーを指定することができます。

最後に保存ボタンをクリックし、設定を反映させます。

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。

インターフェースの設定画面の「インターフェースの種類」を「Optional」(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。

インターフェース名(エイリアス)や IP アドレスの設定方法は Trusted と同様です。

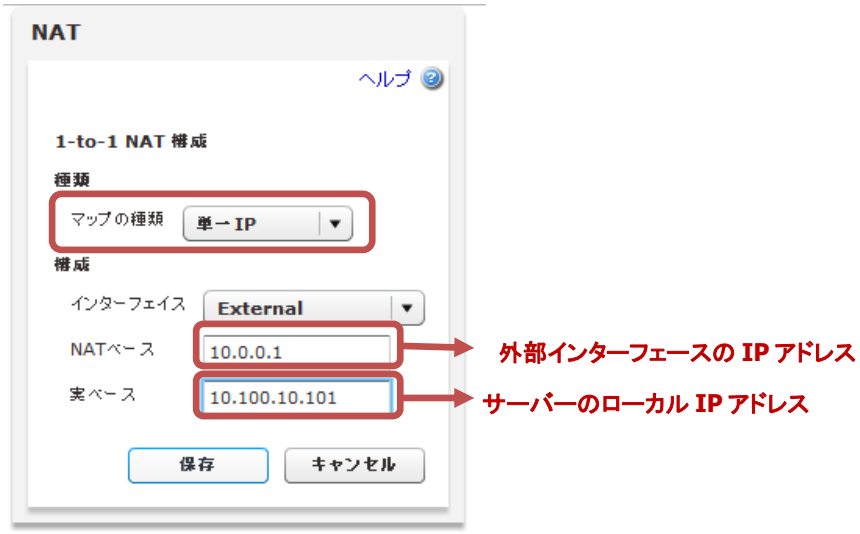
NAT 設定 (1-to-1NAT)

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-to-1NAT(ワントゥワンナット)です。

左側メニュー ネットワーク → NAT をクリックすると、NAT の構成画面になります。
下方の 1-to-1 NAT の追加ボタンをクリックします。

NAT の追加画面になりますので、マップの種類は「単一 IP」、インターフェースは External を指定します。

NAT ベースには外部インターフェースの IP アドレス、Real ベースにはサーバーのローカル IP アドレスを指定します。



保存をクリックすると 1-to-1 NAT の一覧に追加されます。

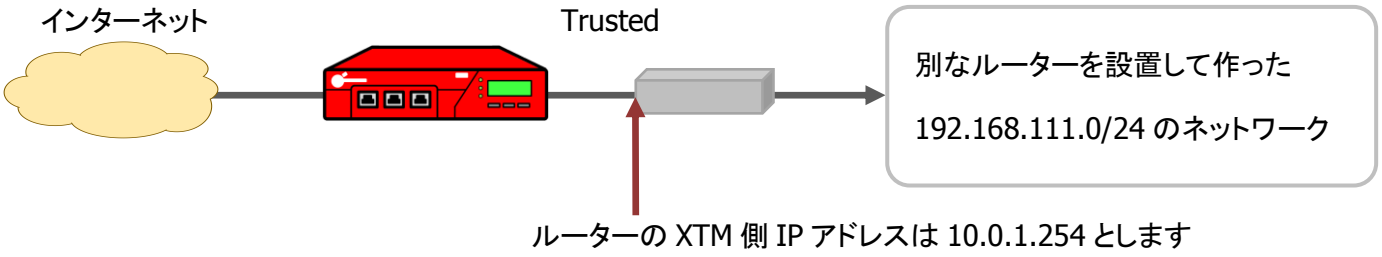
他にもポートフォワーディングも可能な SNAT (Static Nat)の設定もあります。こちらはポリシーの追加時に設定しますので、ファイアウォールの章で取り上げます。

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。

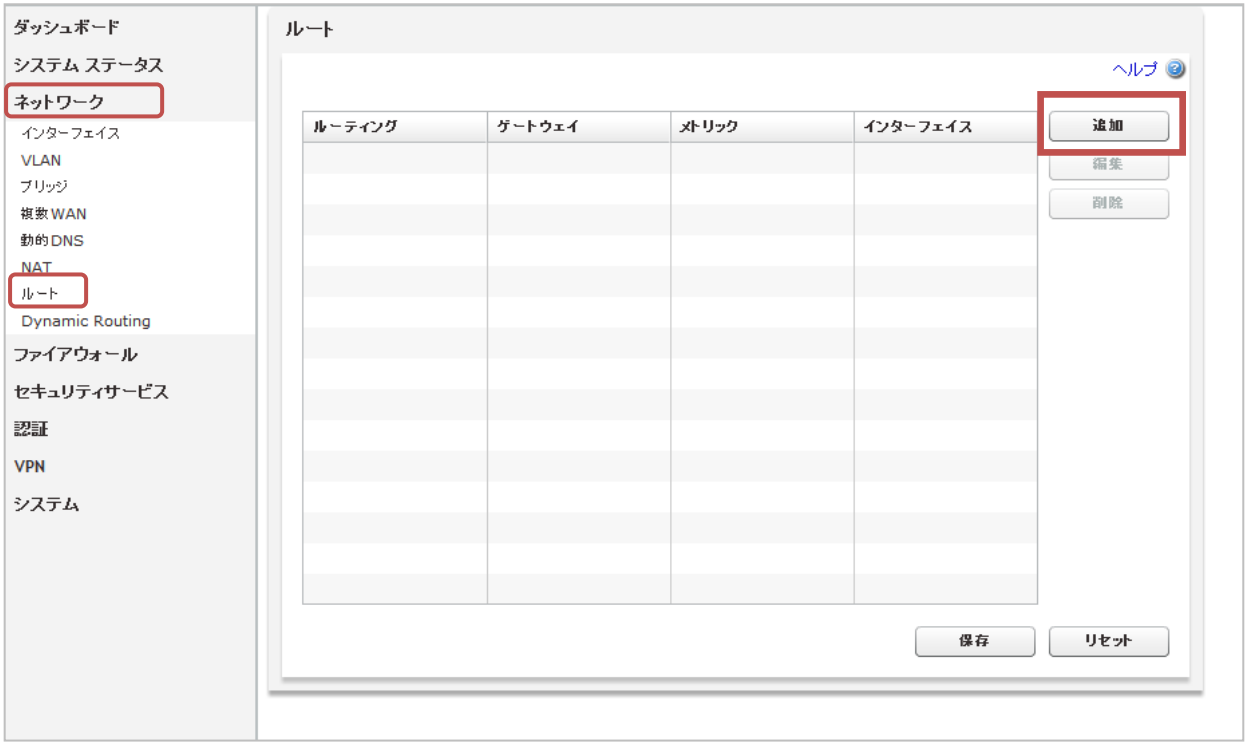
その場合、明示的にルートを設定する必要があります。

例:

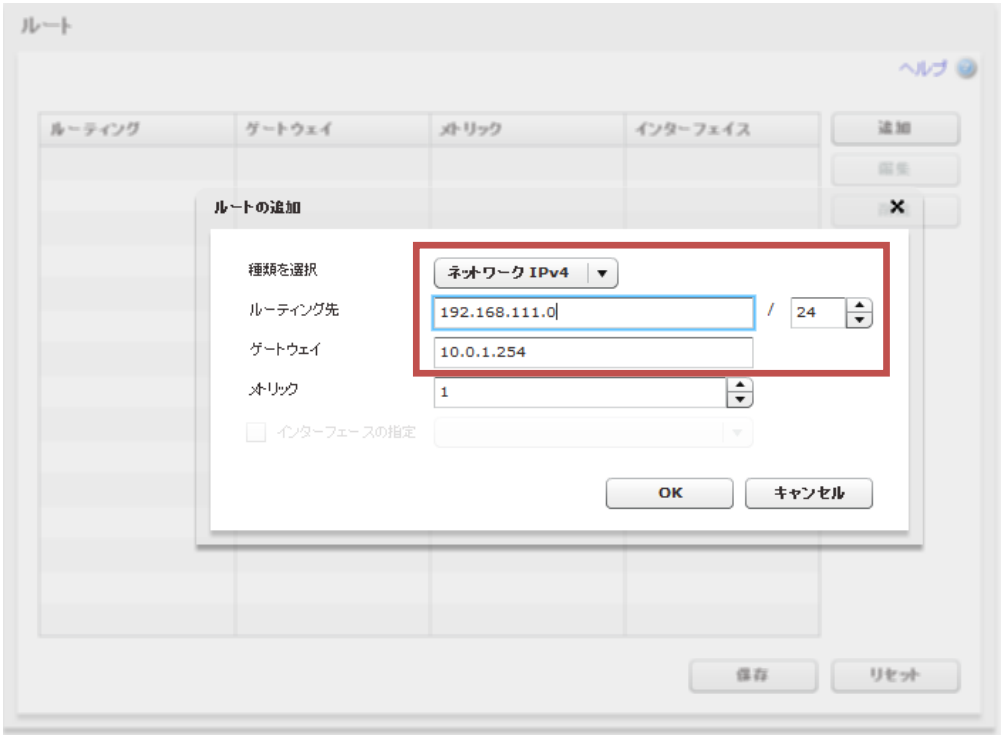


左側メニュー[ネットワーク] → [ルート] をクリックします。

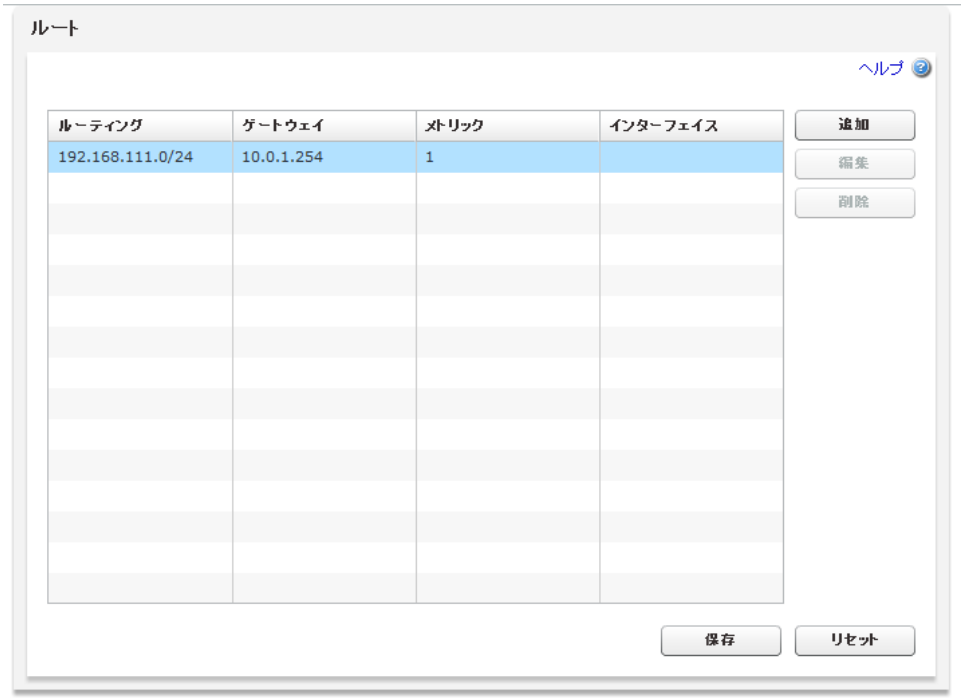
ルートの設定画面が開くので、追加ボタンをクリックします。



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。



OK ボタンをクリックすると一覧に追加されますので、保存します。



第四章　ファイアウォールの設定

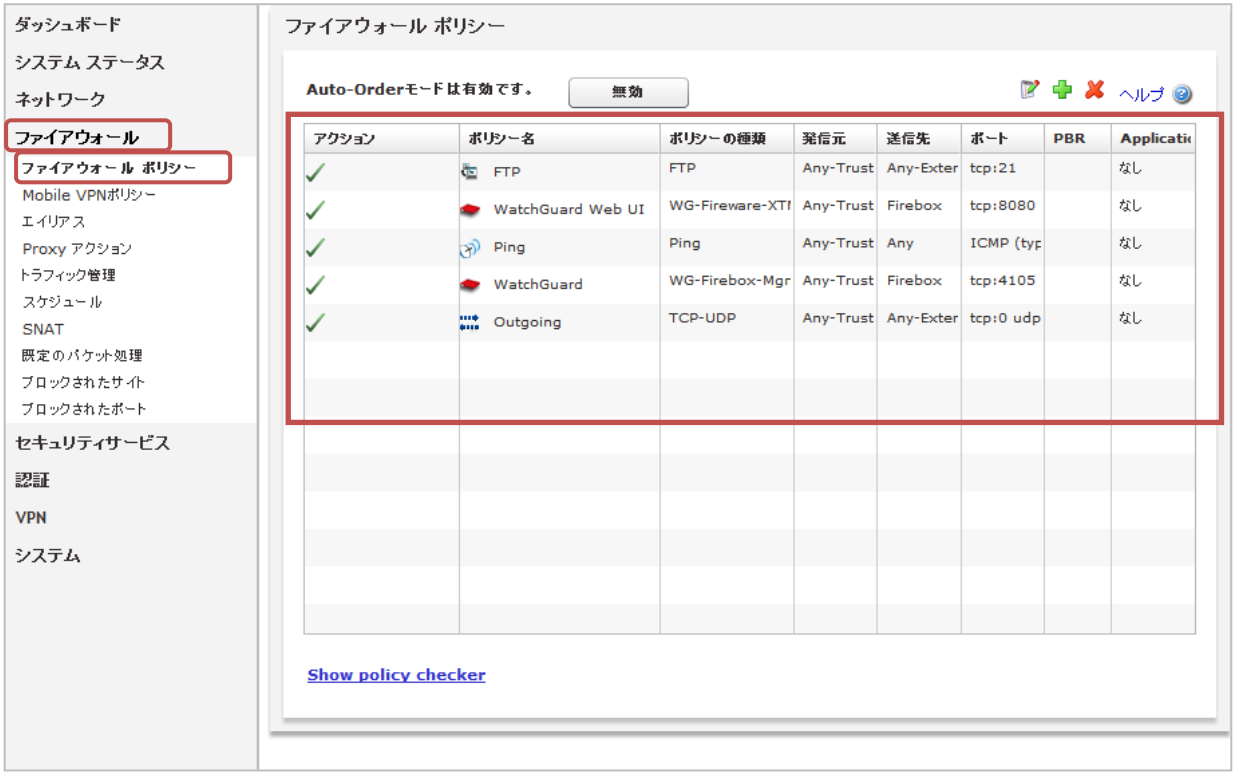
基本的なネットワークが設定できたら、今度は XTM をファイアウォールとして構成してゆきましょう。

ファイアウォールとしての観点から、ポリシー設定画面をあらためて解説します。

ポリシー設定画面

画面構成

ポリシー設定画面は、左側メニューの ファイアウォール ー ファイアウォールポリシー をクリックして表示します。ポリシーの一覧が表示されます。



表示順序は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

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。

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、ポリシーの編集ボタン をクリックします。

ポリシーの新規追加は 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

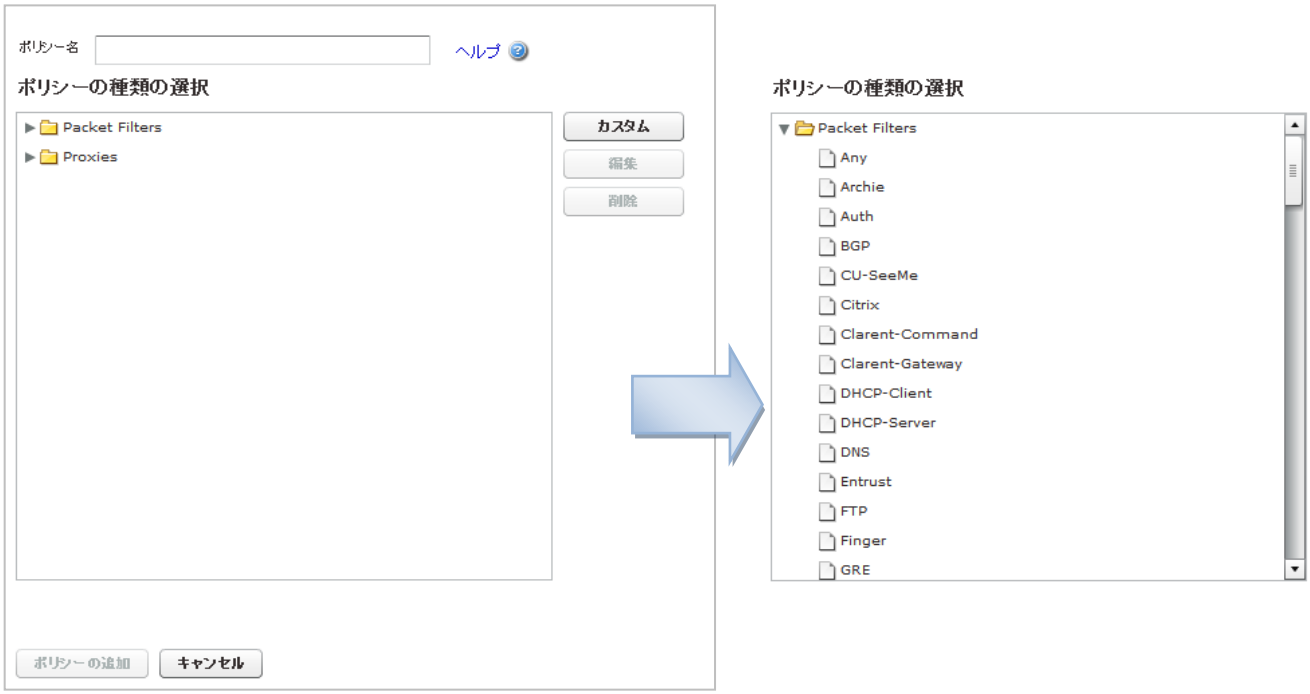
それでは実際にポリシーを追加してみましょう。

ポリシー追加 （内側から外側へ）

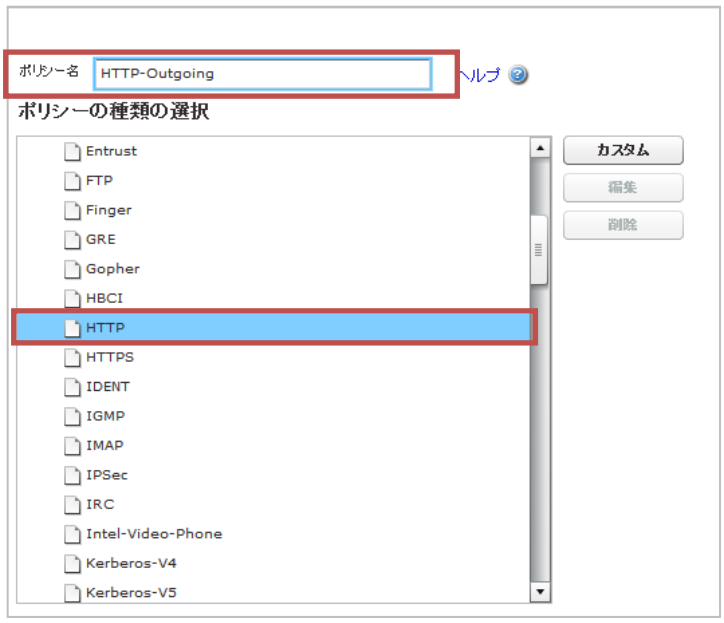
一例として、LAN 側から外にインターネットを見に行けるよう、HTTP 通信を許可するポリシーを作成してみます。ポリシーの追加ボタンをクリックします。

※ 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

追加ボタンをクリックすると、ポリシーの種類の選択画面になります。
Packet Filters のツリーを展開すると、代表的なプロトコルのポリシーテンプレートがあります。



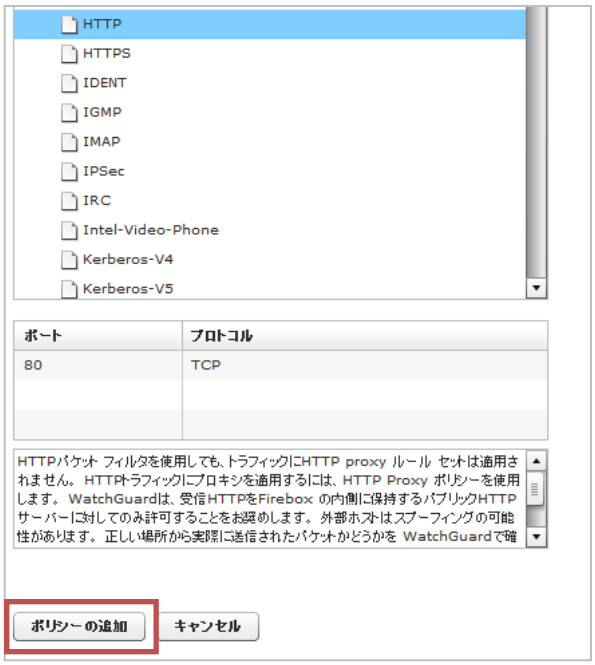
ポリシーテンプレートの中から目的のプロトコルを選択し、ポリシー名を入力します。



WebUI ではポリシー名は後から変更できませんのでご注意ください。

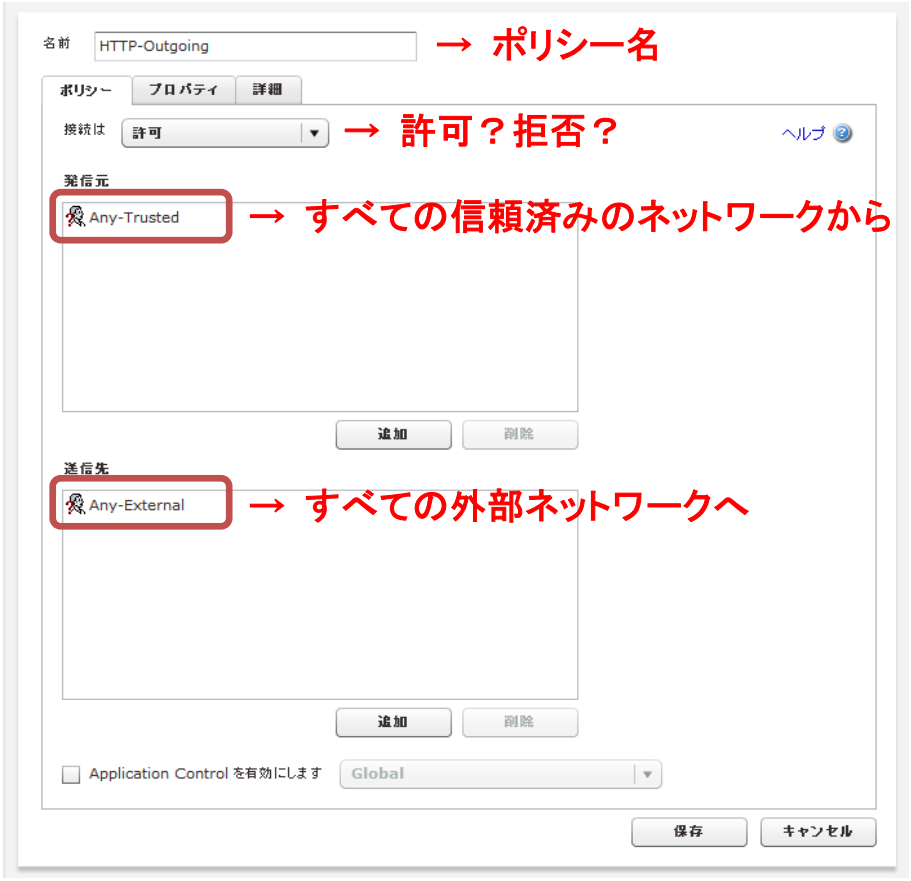
(もちろん WSM からなら変更できます)

下方の追加ボタンをクリックします。

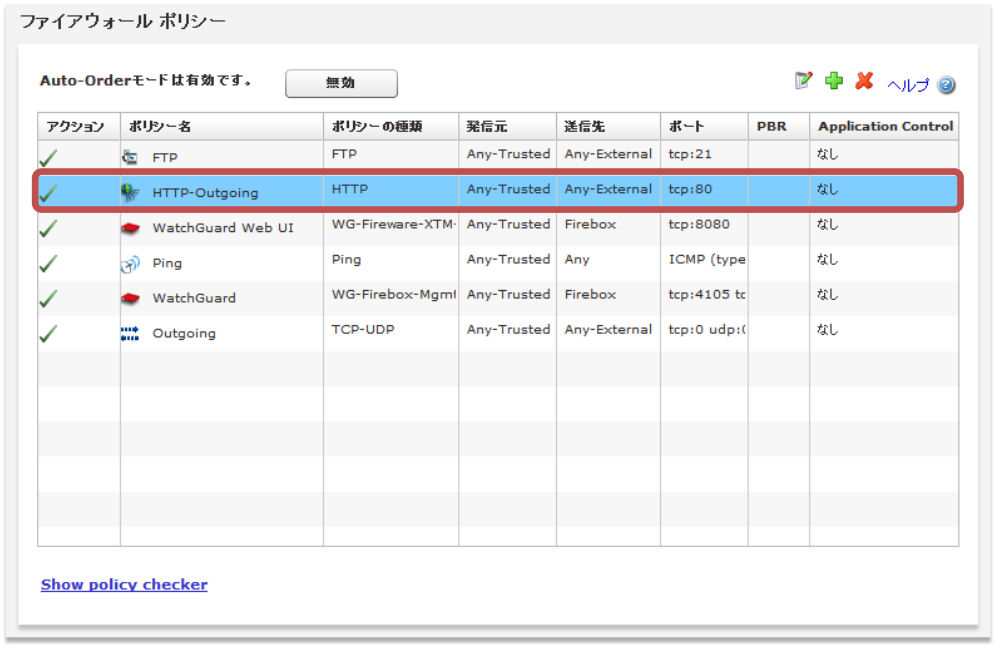


すると、新規作成ポリシーのプロパティが開きます（次頁）。

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保存ボタンをクリックします。



ポリシーー一覧に戻り、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）

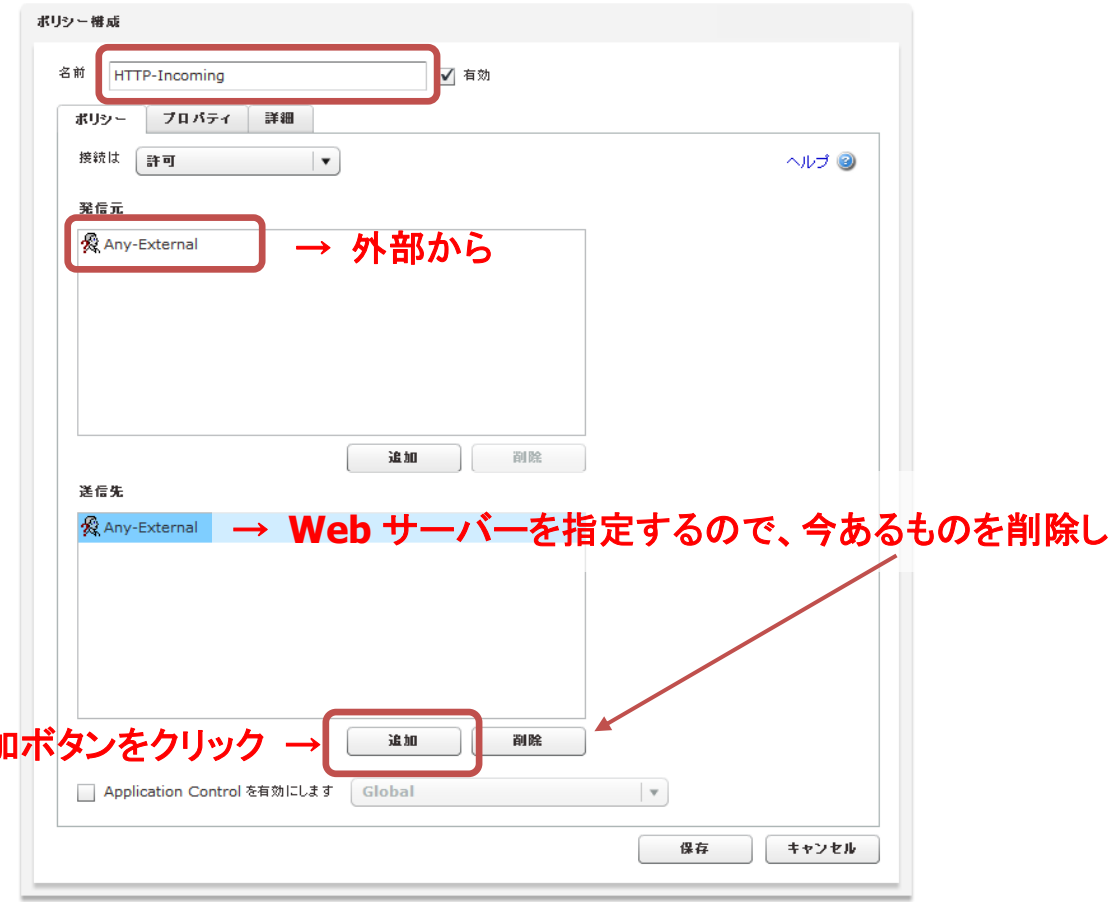
ネットワーク設定の章では DMZ を作るため、最後のポートを Optional にして設定しました。
そこに Web サーバーがある前提で、外側からのアクセスを許可する設定をしてみましょう。

Web サーバーは 10.100.10.110 とします。

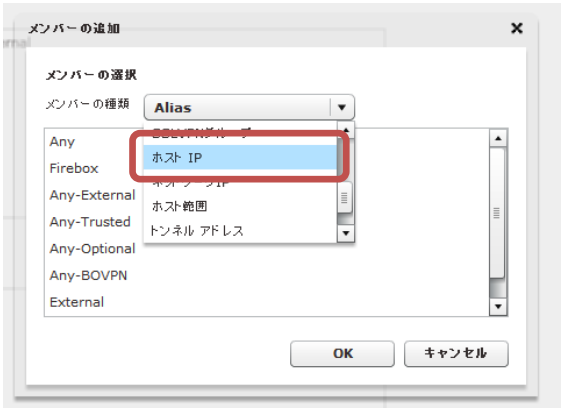
前項と同じようにポリシーの追加ボタンで HTTP を選び、ポリシー名を入力し、追加ボタンをクリックします。

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、



メンバーの選択で、メンバーの種類を「ホスト IP」にします。



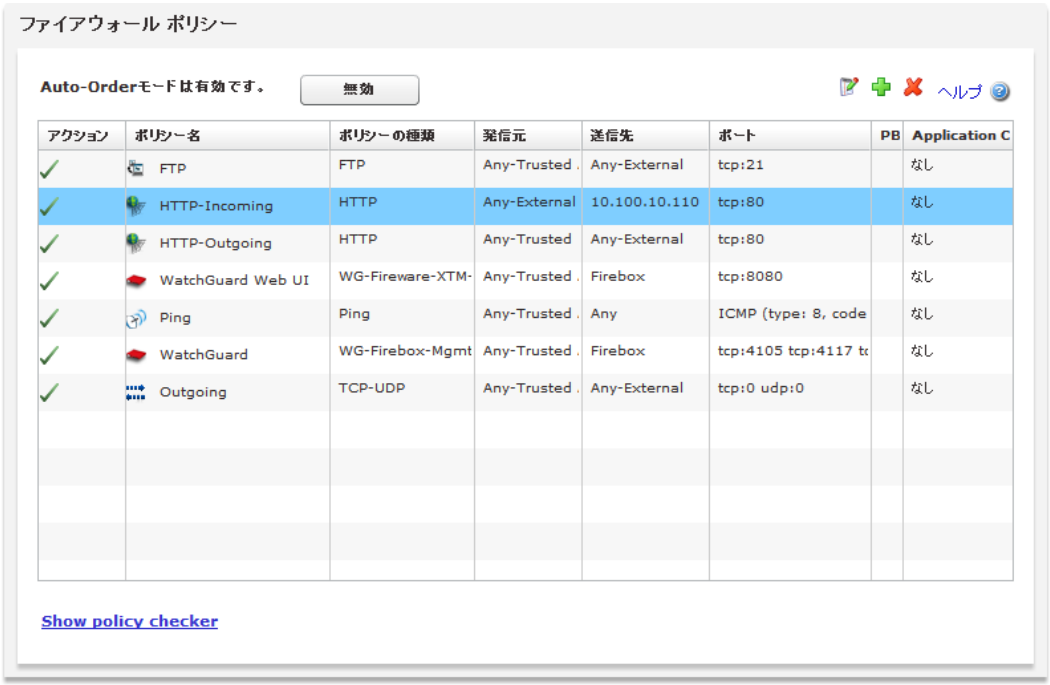
IP アドレスを入力できるようになるので、Web サーバーの IP アドレスを入力し、OK をクリックします。

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。

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ています。

下方の保存ボタンをクリックし、設定を反映させます。

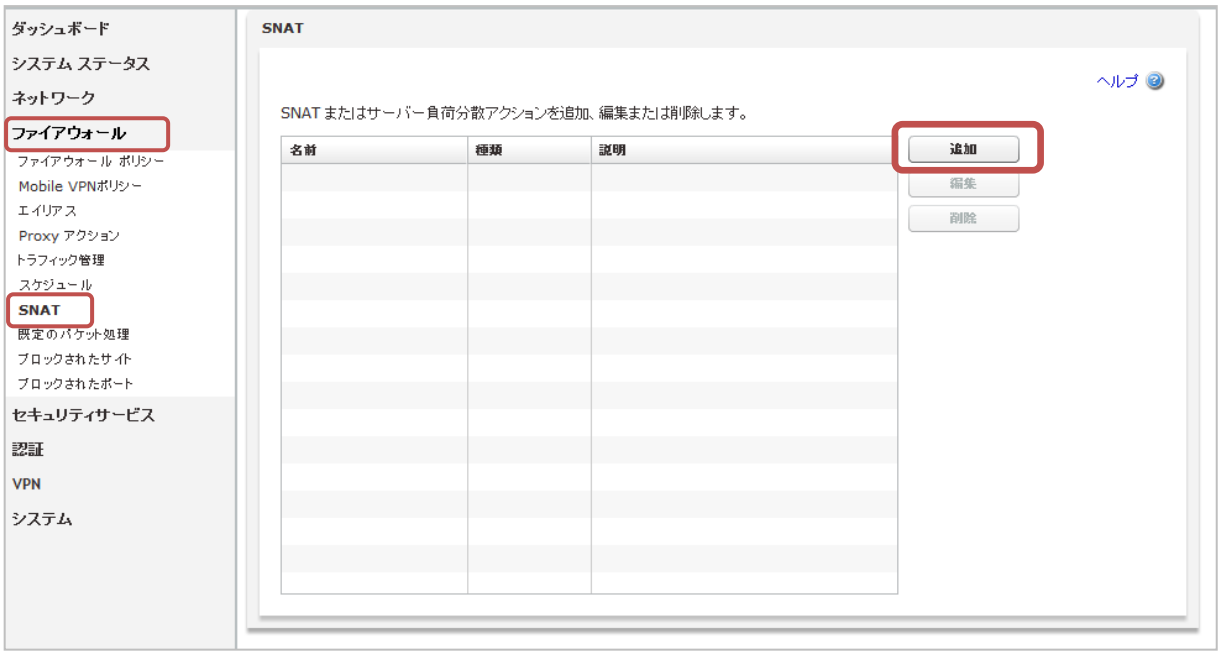
一覧に戻り、ウェブサーバーにアクセス許可するポリシーが作成されました。



ポリシー追加 （SNAT で外側から内側へ）

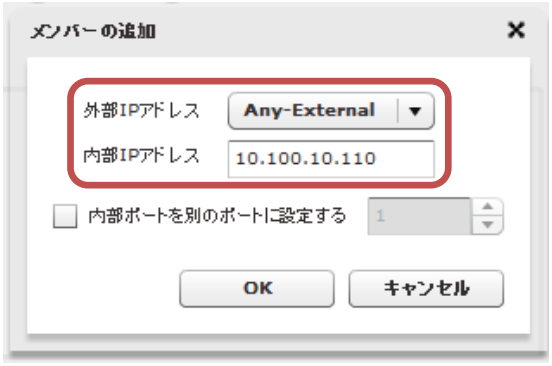
前述の Web サーバーへの許可ポリシーは、1-to-1 NAT が前提の設定でしたが、ポリシー単体で NAT を適用することもできます。
それが SNAT(Static NAT)と呼ばれ、1-to-1 NAT と違い、ポートフォワーディングも設定できます。

左側メニューのファイアウォール －SNAT をクリックすると SNAT 画面になります。
追加ボタンをクリックし、新しい SNAT を定義しましょう。



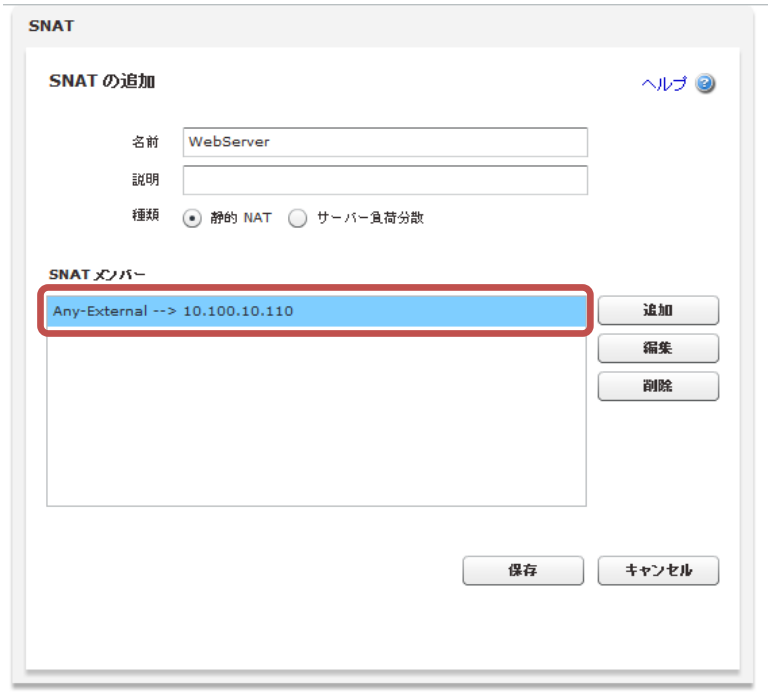
SNAT の名前を入力します。何に対する NAT か分かりやすいものがよいでしょう。
SNAT 画面で追加ボタンをクリックします。

メンバーの追加の画面で、外部 IP アドレスは Any-External、内部 IP アドレスは Web サーバーの 10.100.10.110 を入力して OK をクリックします。



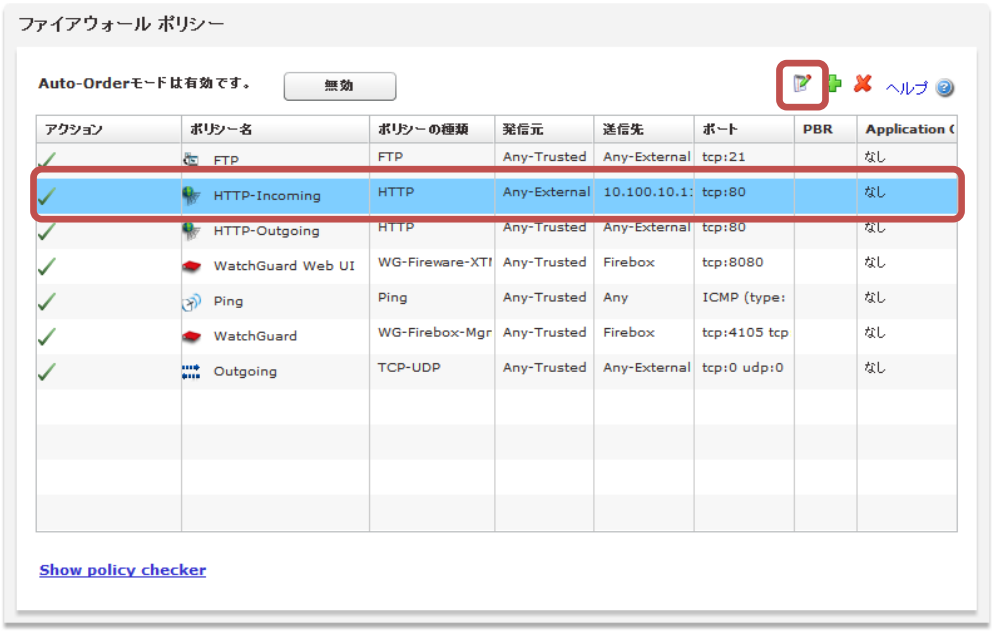
ポートフォワーディングをしたい場合は「内部ポートを別のポートに設定する」にチェックを入れ、変換後のポートを指定します。(例：80 番ポートで受けて 8080 にフォワーディングするなど)

SNAT メンバーが追加されましたので、保存ボタンをクリックして設定を反映させます。

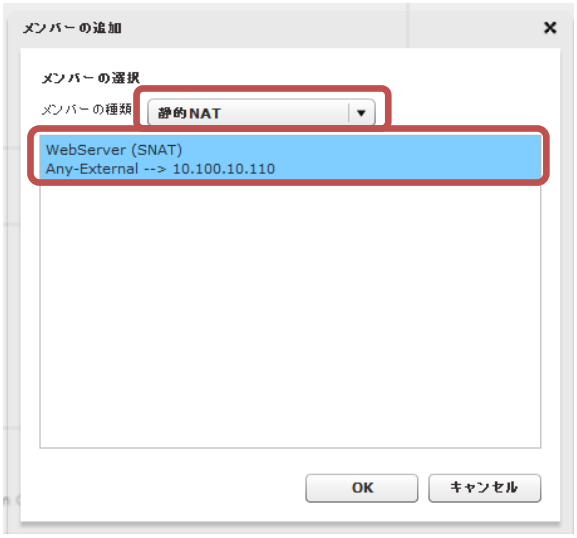


それでは新しく定義した SNAT をポリシーに適用してみましょう。

HTTP を Web サーバーに許可するポリシーを選択し、編集ボタンをクリックします。

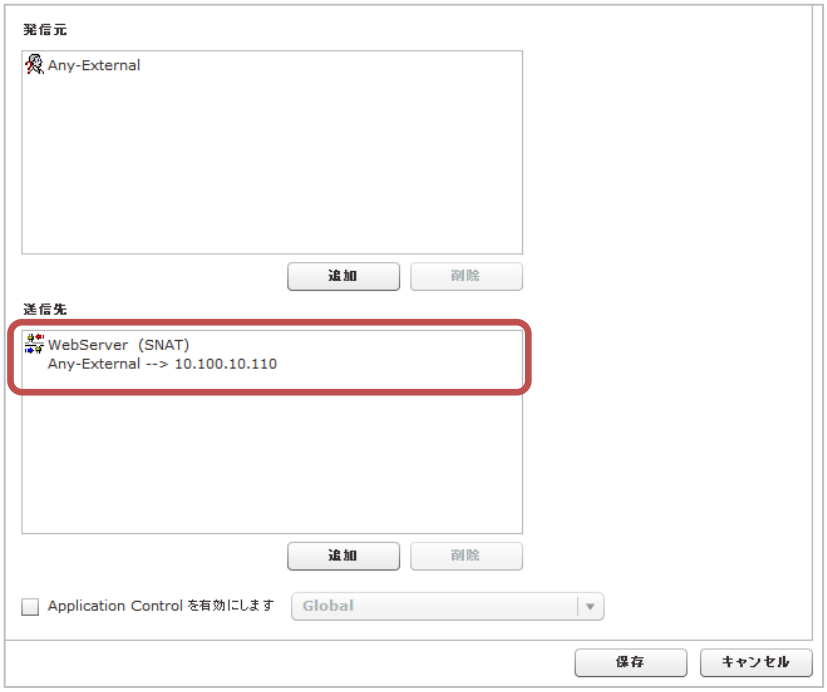


既存の送信先を削除し、追加ボタンをクリックしたら、送信先のメンバーの選択で、メンバーの種類に「静的 NAT」を選択します。



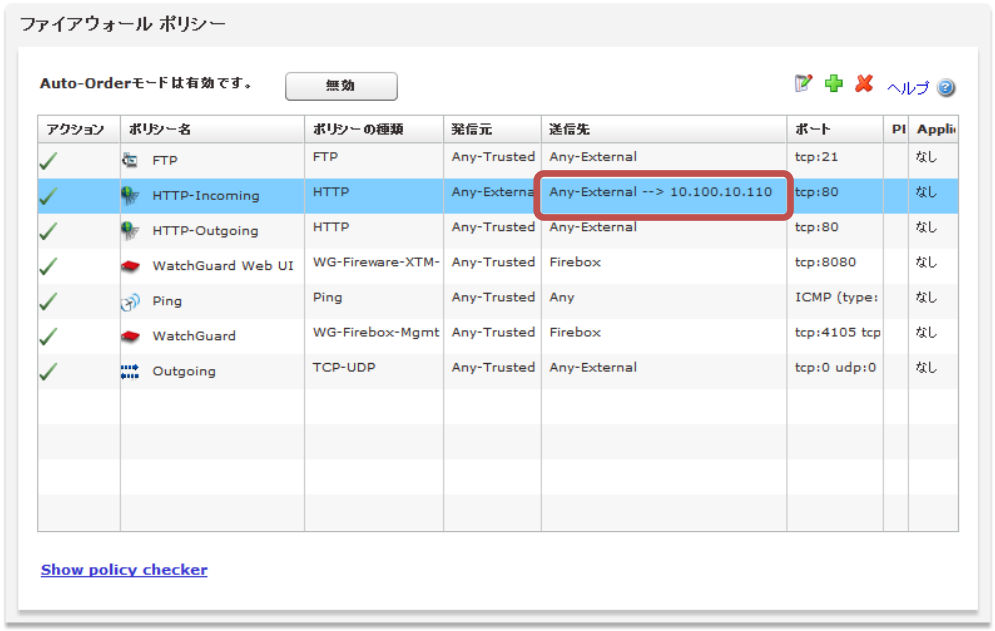
事前に定義した SNAT を選択し、OK ボタンをクリックします。

ポリシー設定画面に戻ると以下のように送信先が設定されます。



保存ボタンをクリックし、設定を反映させます。

ポリシー一覧に戻ると、HTTP-Incoming の送信先が SNAT の定義になっていることが分かります。



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。

ポリシー一覧で新規追加ボタンをクリックします。

次の画面でカスタムボタンをクリックします。

プロトコル(ポート番号)を定義するために追加ボタンをクリックします。

プロトコルを単一ポートで追加します。

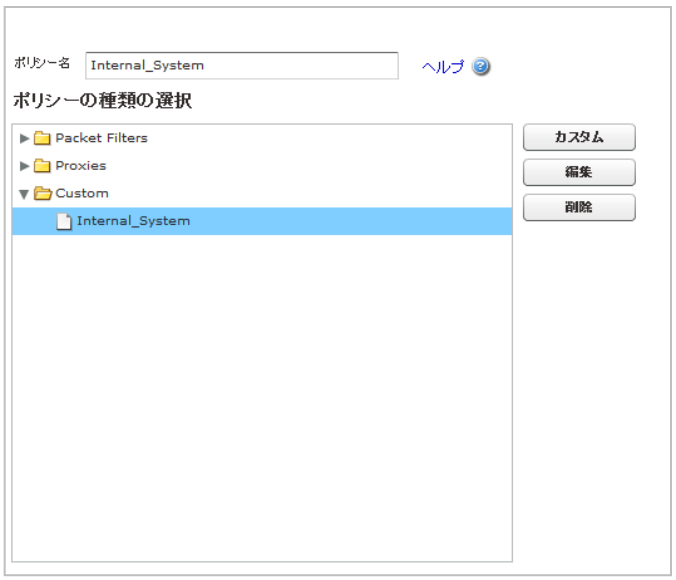
プロトコルを複数追加でき、ポート範囲も指定できます。

新しいポリシーテンプレートの画面に、プロトコルが追加されたことが確認できます。

保存ボタンをクリックします。

新しいテンプレートとして登録されました。

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。

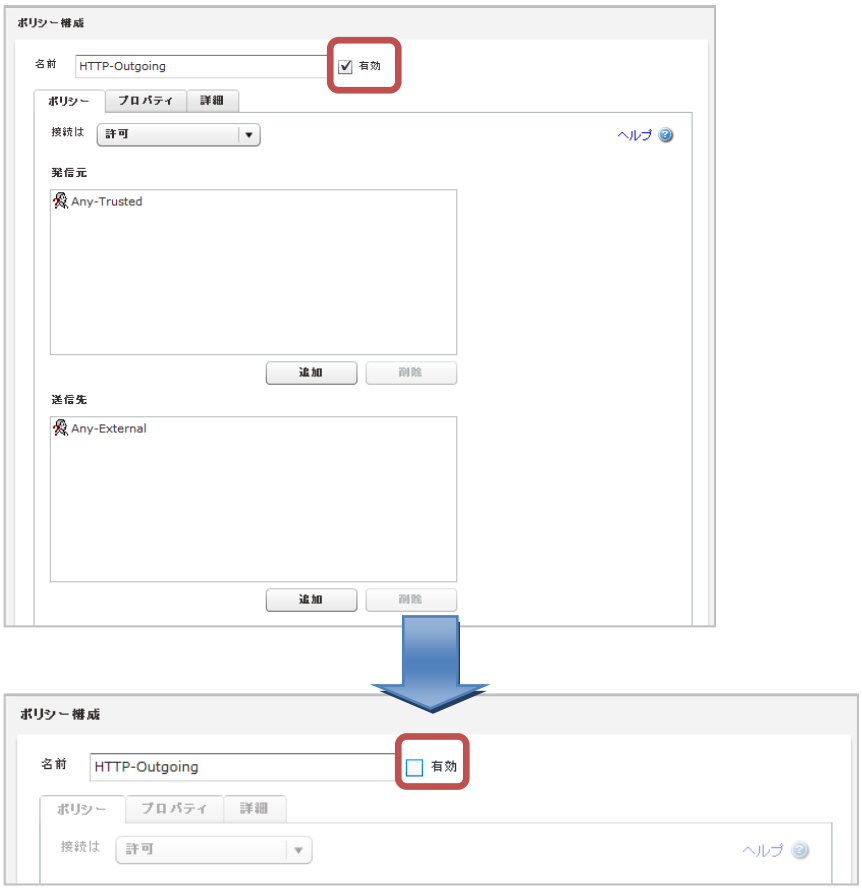


ポリシーの編集

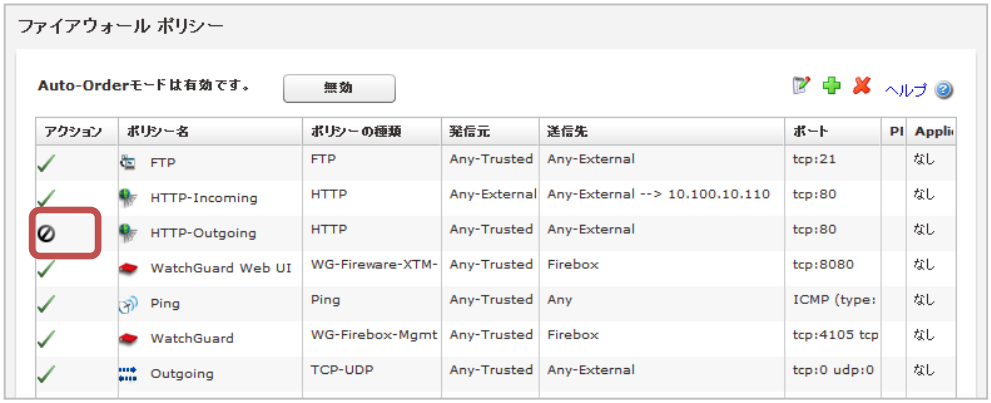
ポリシーの新規作成手順で触れなかった詳細な設定について、いくつかご紹介します。

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。



保存して一覧に戻ると、ポリシー一覧でも無効になったことが分かります。

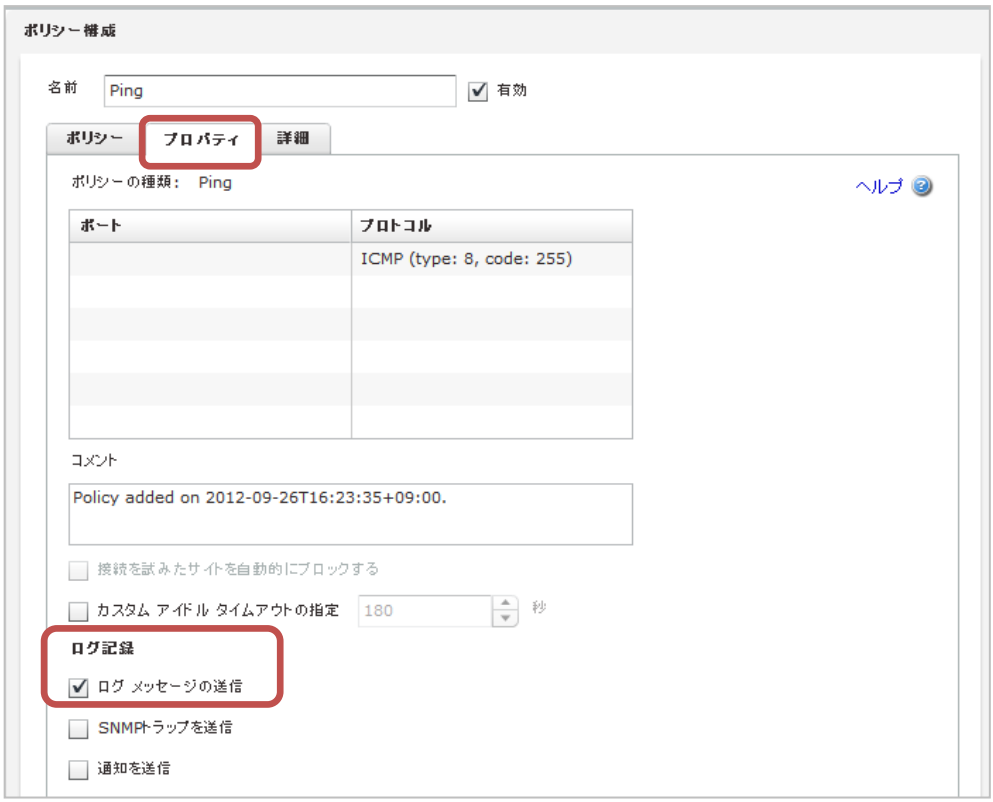


ログを記録する

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 を許可するポリシー「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」タブで設定します。

ログ記録の「ログメッセージの送信」にチェックを入れます。



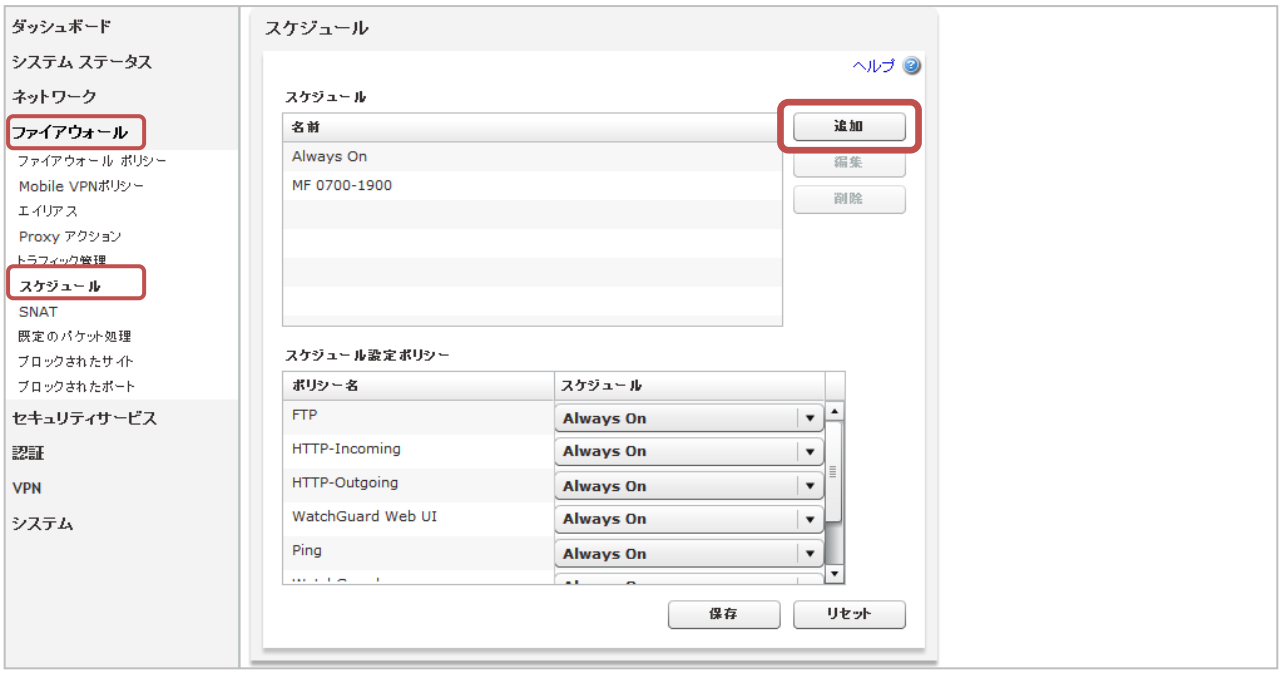
この設定により、トラフィックモニターやログサーバーでこのポリシーのログを見ることができるようになります。

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。

左側メニュー ファイアウォール ー スケジュール をクリックします。

新しいスケジュールを作成するため、追加ボタンをクリックします。



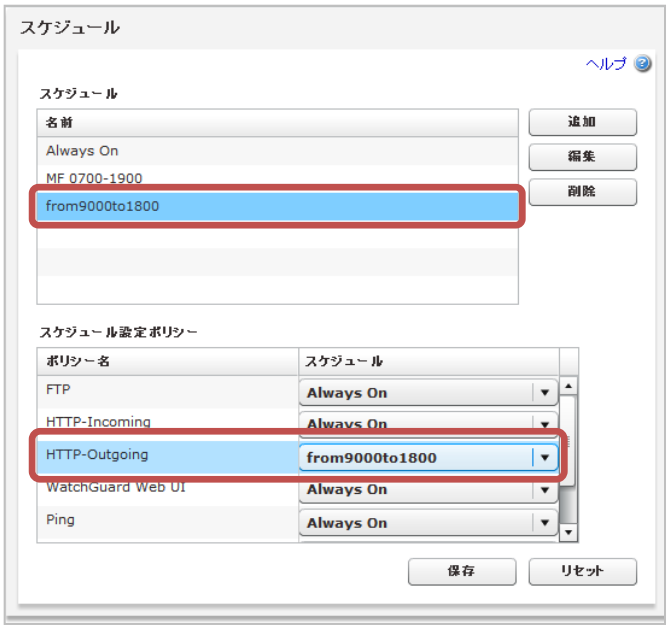
名前にはスケジュールの内容が分かるようなスケジュール名を入力します。

稼働時間は赤色で「ポリシーが有効な時間」を意味し、非稼働時間は白色で「ポリシーが有効でない時間」を意味します。

赤色/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。

設定したら保存してください。

作成したスケジュールが一覧に載り、その下のスケジュール設定ポリシー欄でスケジュールを割り当てることができます。

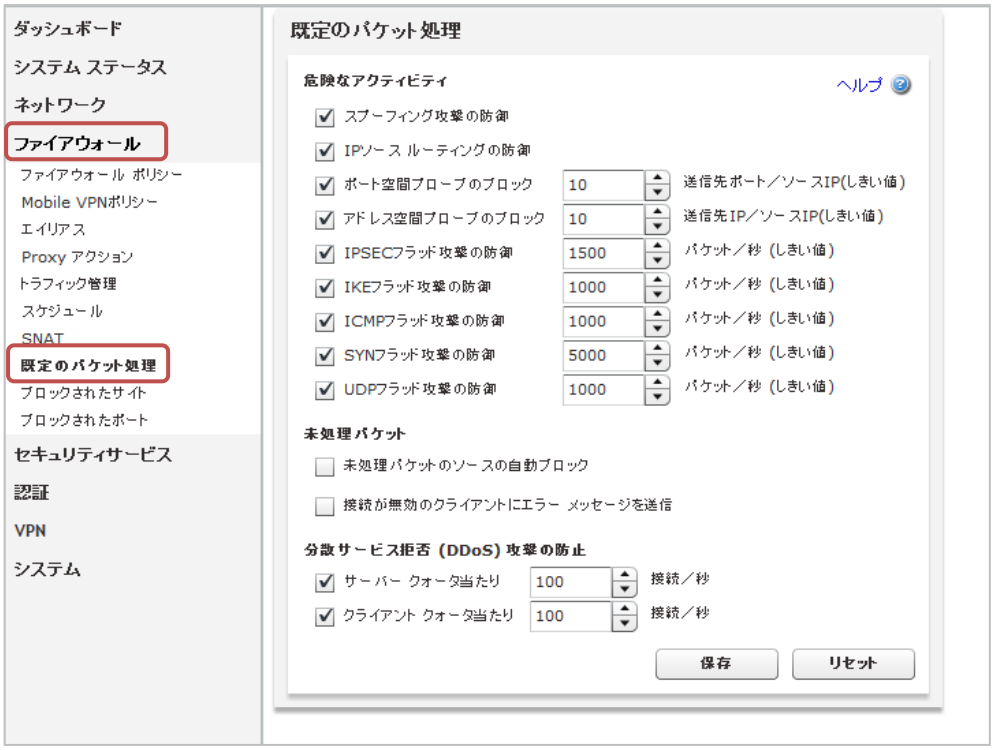


ポリシー以外のファイアウォール設定

規定のパケット処理

左側メニューファイアウォール ー 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。

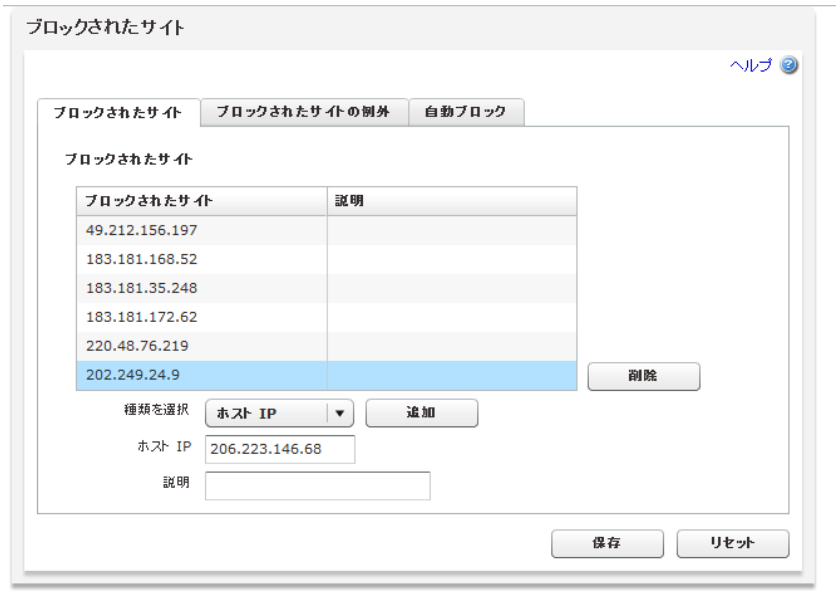


必要に応じて、攻撃と判断する閾値を変更できます。

ブロックされたサイト

左側メニュー[ファイアウォール] ー [ブロックされたサイト] をクリックします。

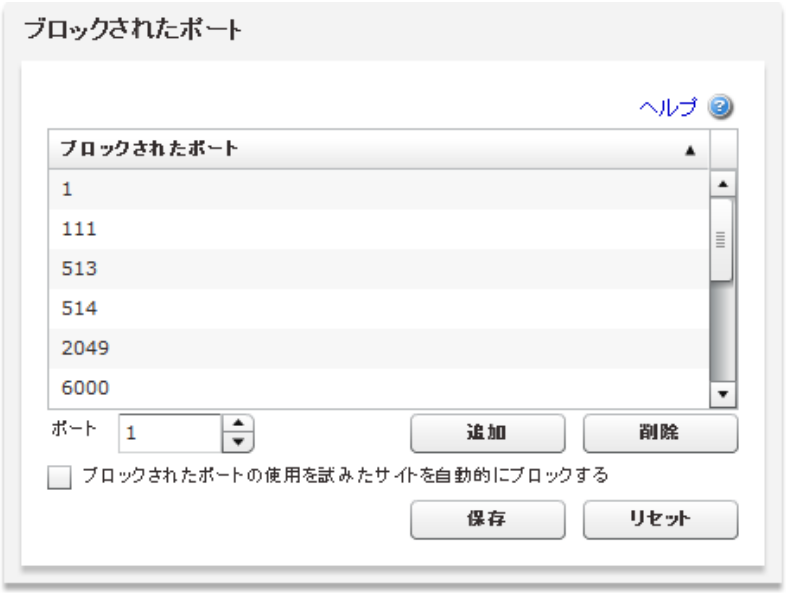
この画面から特定のサイトを登録し、そのサイトへのアクセスをブロックすることができます。



ブロックされたポート

左側メニュー[ファイアウォール] ー [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

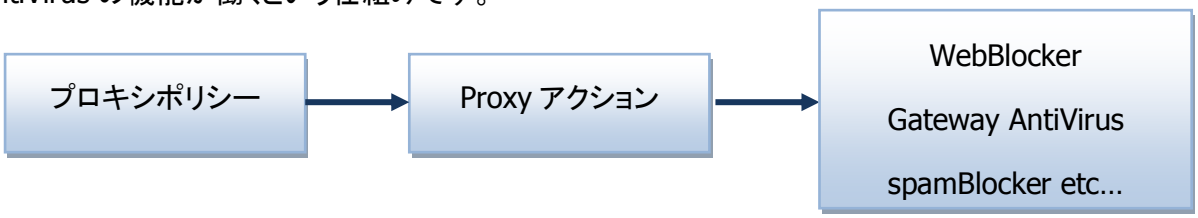
コンテンツフィルタリングやアンチウィルスなど、アプリケーションレベルの脅威に対応する機能を UTM (Unified Threat Management)といいます。

この章では UTM の代表的な機能である、webBlocker(コンテンツフィルタリング)、Gateway AntiVirurs、spamBlocker の設定方法を解説します。

プロキシポリシーの追加

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

プロキシポリシーと紐づいた Proxy アクションが呼び出され、そのアクションと紐付いた WebBlocker や AntiVirus の機能が働くという仕組みです。



ですので、UTM を有効にするには

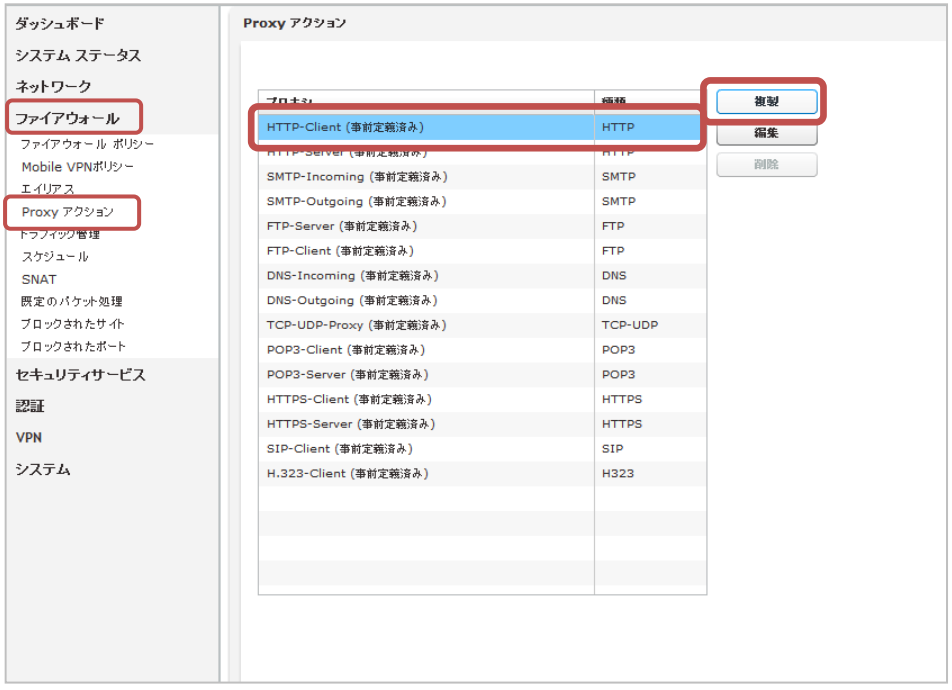
1.プロキシアクションの定義、 2.プロキシポリシーの追加、 3.各種 UTM 機能の設定

の 3 つを設定してゆきます。

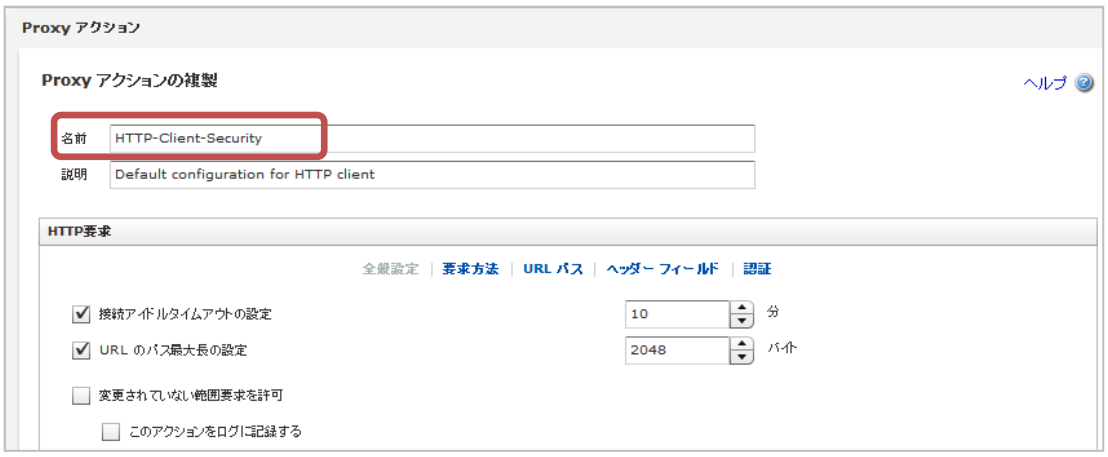
プロキシアクションの追加

ファイアウォール－Proxy アクション をクリックします。

HTTP-Client(事前定義済み)を選択し、複製ボタンをクリックします。



Proxy アクションの詳細な設定をする画面になりますが、まずはアクションの内容を表わす名前を入力します。



名前を付けたら下方の保存ボタンをクリックして、アクションを保存します。

一覧には事前定義済みのアクションの他に、新しく定義したアクションが加わりました。

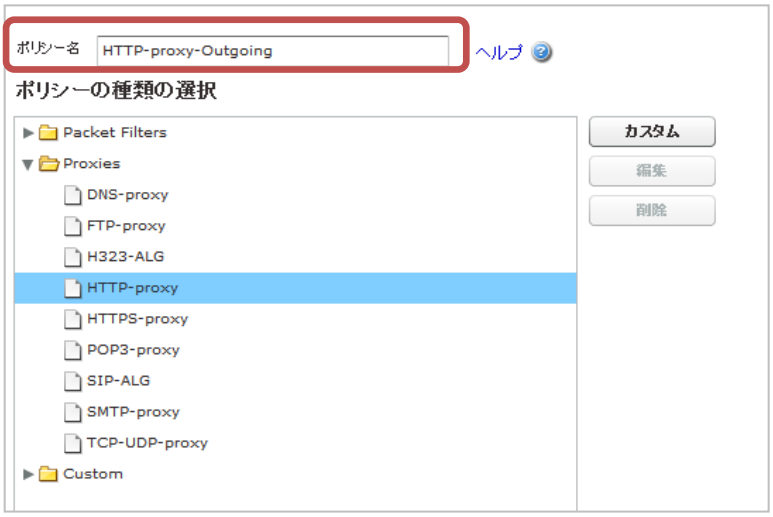
次に、このアクションと紐づいたプロキシポリシーを追加してみましょう。

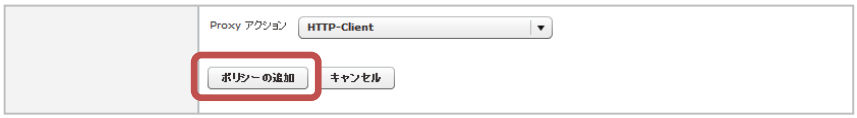
プロキシポリシーの追加

ファイアウォール ― ファイアウォールポリシー からポリシー一覧を表示し、通常のポリシーと同様、ポリシー一覧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。

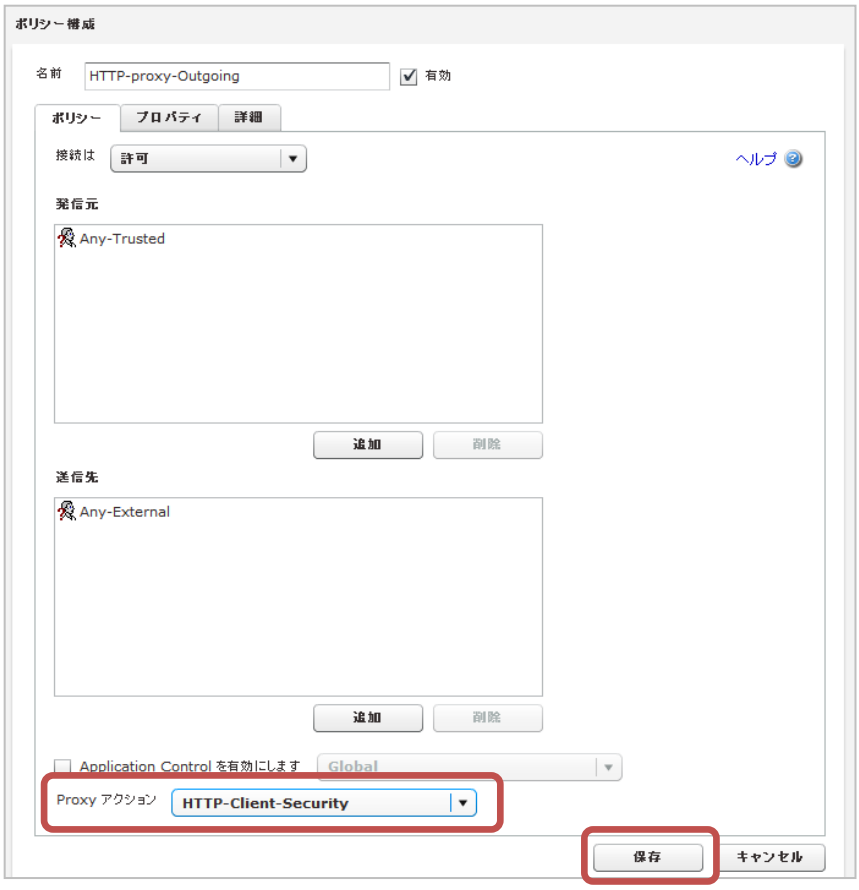
これまでは「Packet Filters」ツリーにあるプロトコルを選択していましたが、UTM を設定する場合は「Proxies」ツリーにあるテンプレートを選択します。
たとえば、コンテンツフィルタリングを設定する場合は、HTTP 通信上の制御なので、HTTP-proxy を追加します。

HTTP-proxy テンプレートを選択し、ポリシー名に名前を入力し、下方の「ポリシーの追加」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ィルス)を効かせます***、という意味になります。[3]

この Proxy アクションのドロップダウンリストで、先ほど追加しておいたアクションを選択します。

最後に保存ボタンを押してポリシーを追加しましょう。

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PE	Applica
✓	FTP	FTP	Any-Trusted	Any-External	tcp:21		なし
✓	HTTP-Incoming	HTTP	Any-External	Any-External --> 1	tcp:80		なし
✓	HTTP-proxy-Outgoing	HTTP-proxy	Any-Trusted	Any-External	tcp:80		なし
✓	HTTP-Outgoing	HTTP	Any-Trusted	Any-External	tcp:80		なし
✓	WatchGuard Web UI	WG-Fireware-XTM	Any-Trusted	Firebox	tcp:8080		なし
✓	Ping	Ping	Any-Trusted	Any	ICMP (type: 8, coc		なし
✓	WatchGuard	WG-Firebox-Mgm	Any-Trusted	Firebox	tcp:4105 tcp:4117		なし
✓	Outgoing	TCP-UDP	Any-Trusted	Any-External	tcp:0 udp:0		なし

プロキシポリシーが一覧に追加され、UTM 機能を有効にするための準備が整いました。

[3] 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

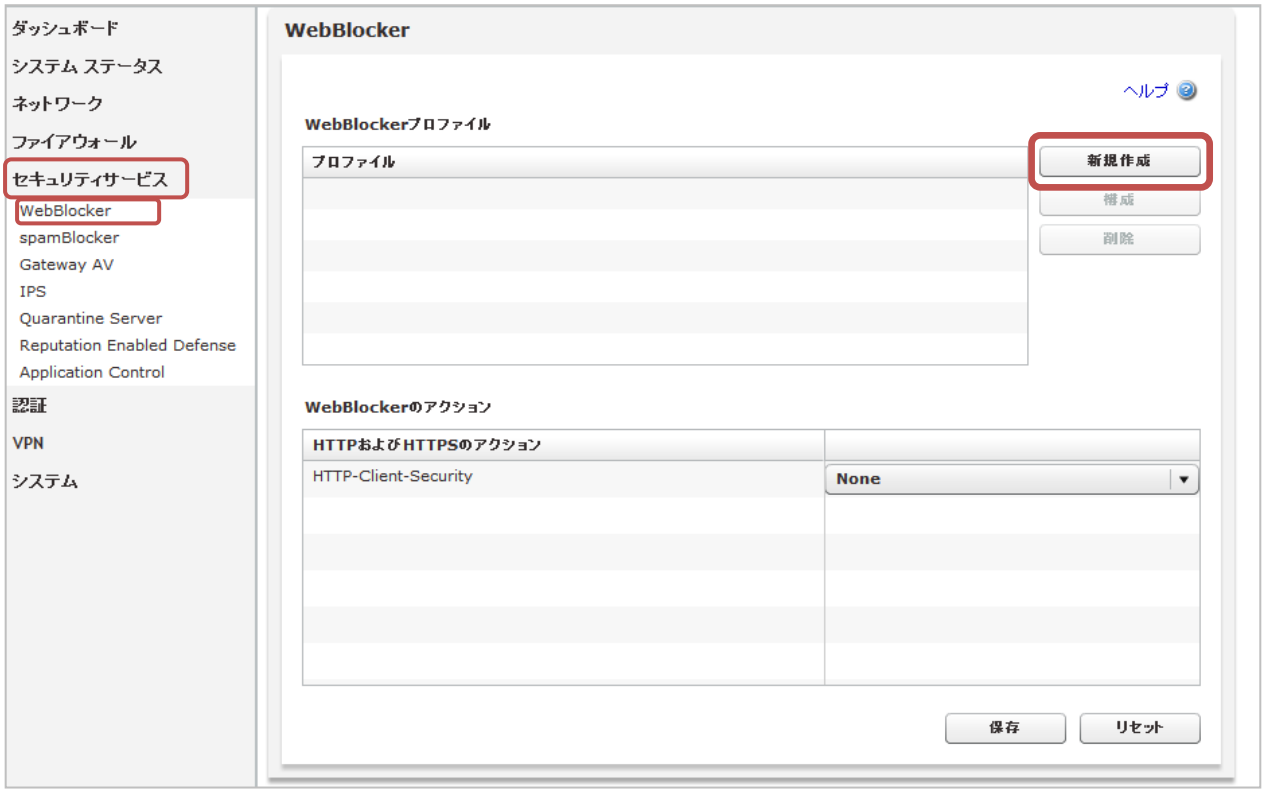
Web Blocker の設定

WebBlocker はコンテンツフィルタリングの役割をし、業務時間中の無秩序な Web ブラウジングを規制します。フィルタリング用のデータベースは実績のある WebSence のものを利用しており、ユーザーが Web サイトにアクセスしようとしたとき、XTM はそのサイト情報をデータベースに問い合わせます。

データベースにその情報がない又は規制対象でなければ、Web サイトを表示します。規制対象であればアクセスがブロックされた旨が表示され、Web サイトは表示されません。

Web Blocker を構成する

メニュー[セキュリティサービス] →[WebBlocker] をクリックし、WebBlocker の構成画面を開きます。
新規作成ボタンをクリックします。

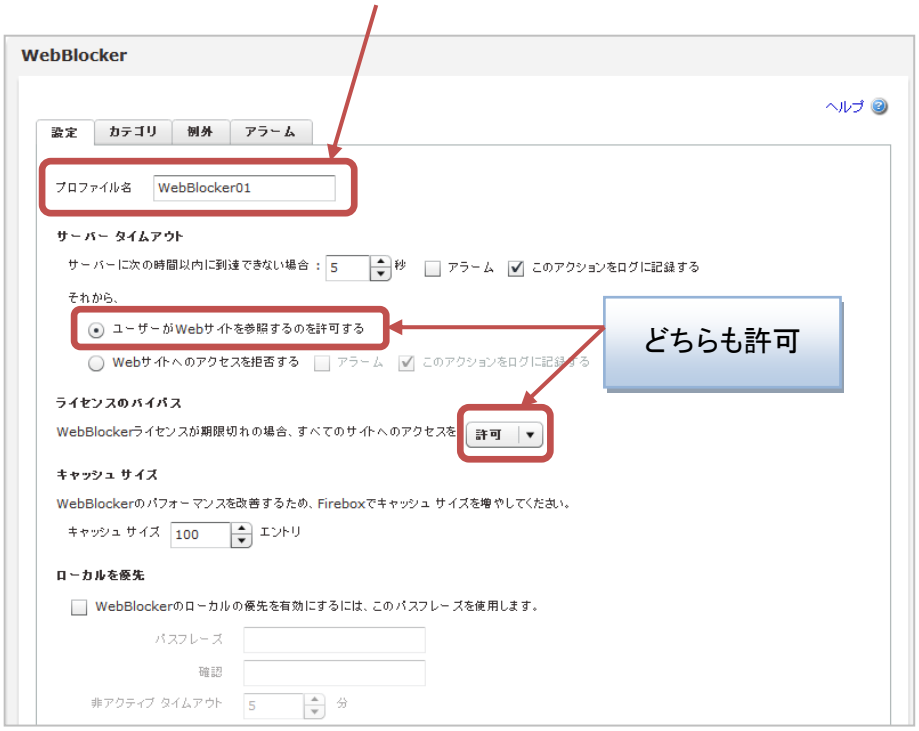


アラームタブにフォーカスが当たっていますが、ここは必須の設定項目はありません。

SNMP トラップ、又はログサーバーの設定をしている場合は通知の設定ができます。

設定タブを選択します。画面が長いので、2 つに分けて説明します。

まず、WebBloker のプロファイル名を入力します。



注意すべき設定項目は「サーバータイムアウト」と「ライセンスのバイパス」です。
もしサーバーに一定時間以内にアクセスできない場合やライセンスが切れた場合、デフォルトでは Web の閲覧を切断する設定になっています。つまり全社の Web 利用ができなくなる可能性があります。

運用方針にもよりますが、これらの設定を「許可」にしておき、業務にインパクトがないようにしておくことをおすすめします。

画面をスクロールすると、下方に WebBlocker サーバーを指定する場所があります。

2 シリーズでは WatchGuard が提供する WebBlocker サーバーを使用することができます。

330 以上の場合、自社で WebBlocker サーバーを設置していただく必要がありますので、そのサーバーの IP アドレスを指定します。

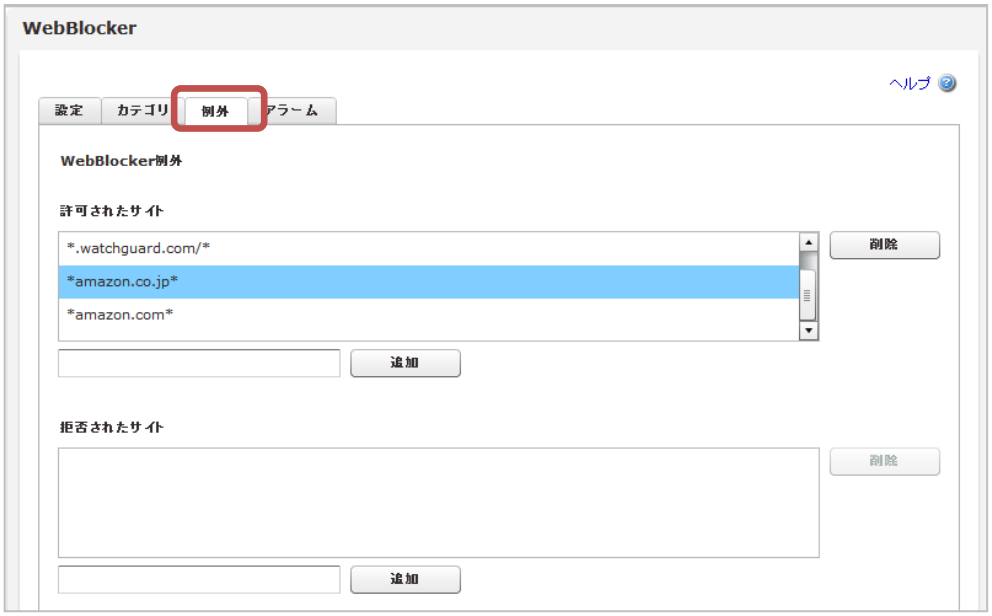
IP 欄に IP アドレスを入力し、追加ボタンをクリックします。

以下のように WebBlocker Server の一覧にサーバーの IP アドレスが追加されます。

カテゴリタブをクリックします。業務中に閲覧させたくないカテゴリーにチェックを入れます。

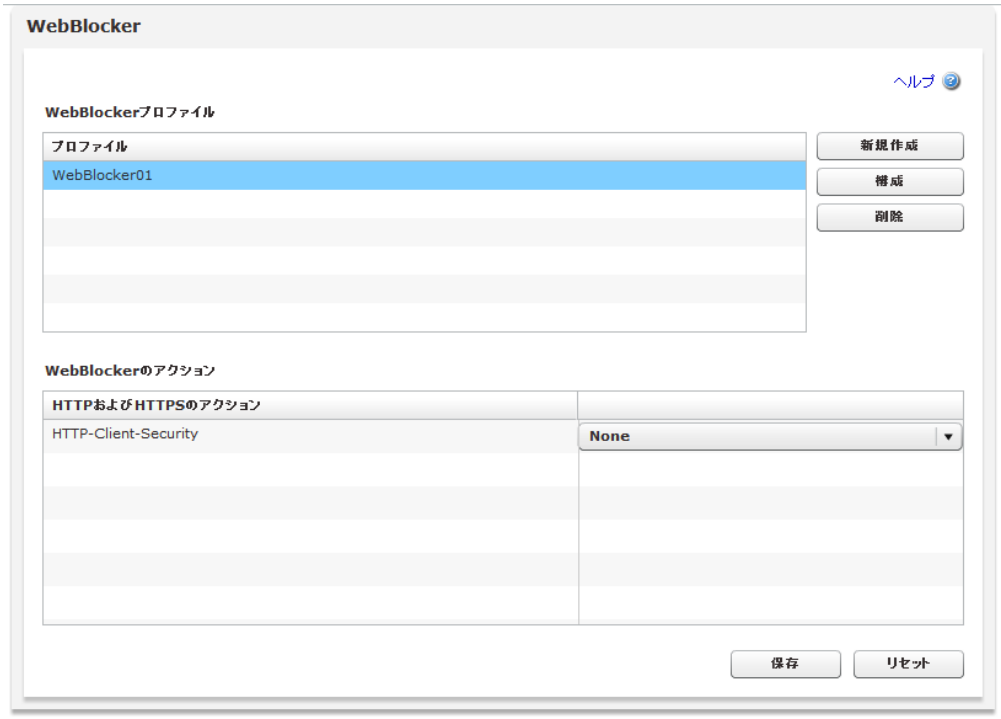
例では、アダルトや犯罪の他、動作を確認するためにショッピングも全部チェックします。

例外タブを選択し、許可されたサイトをパターンで設定できます。
以下は、ショッピングはカテゴリで規制しますが、Amazon は例外で許可する、という設定です。



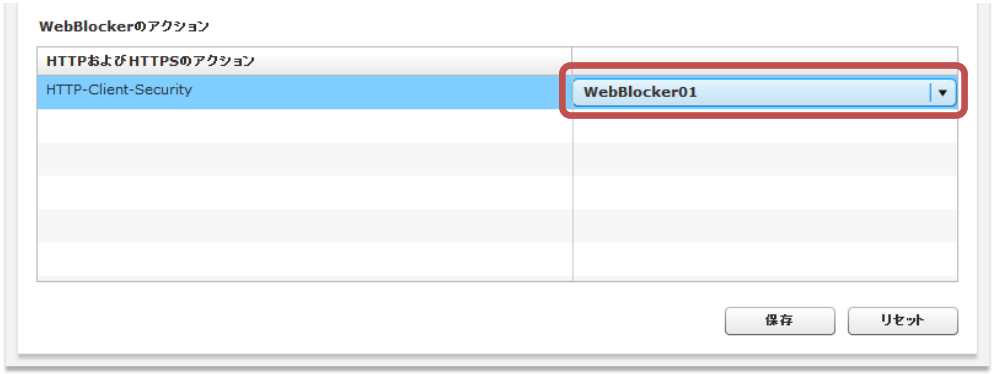
一通り設定したら、画面下方にある保存ボタンをクリックし設定を反映させます。

設定を保存すると最初の WebBlocker の画面に戻ります。
一覧には新たに定義したプロファイルがあります。



ではこの WebBlocker のプロファイルをプロキシアクションと紐付けましょう。

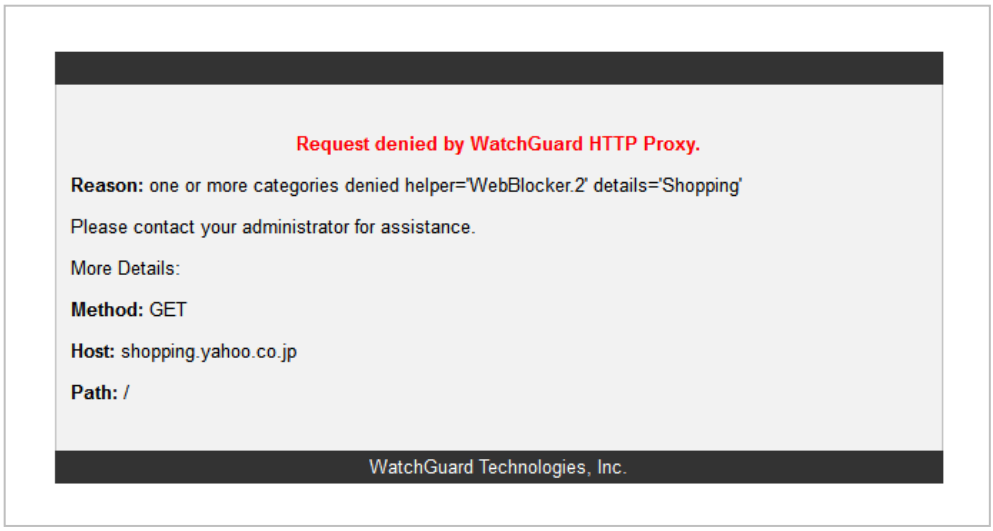
下の WebBlocker のアクションの欄に、あらかじめ作成したアクション「HTTP-Client-Security」には何も関連付けられず「None」になっています。
このドロップダウンリストで WebBlocker のプロファイル「WebBlocker01」を指定します。



保存ボタンで保存します。

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。

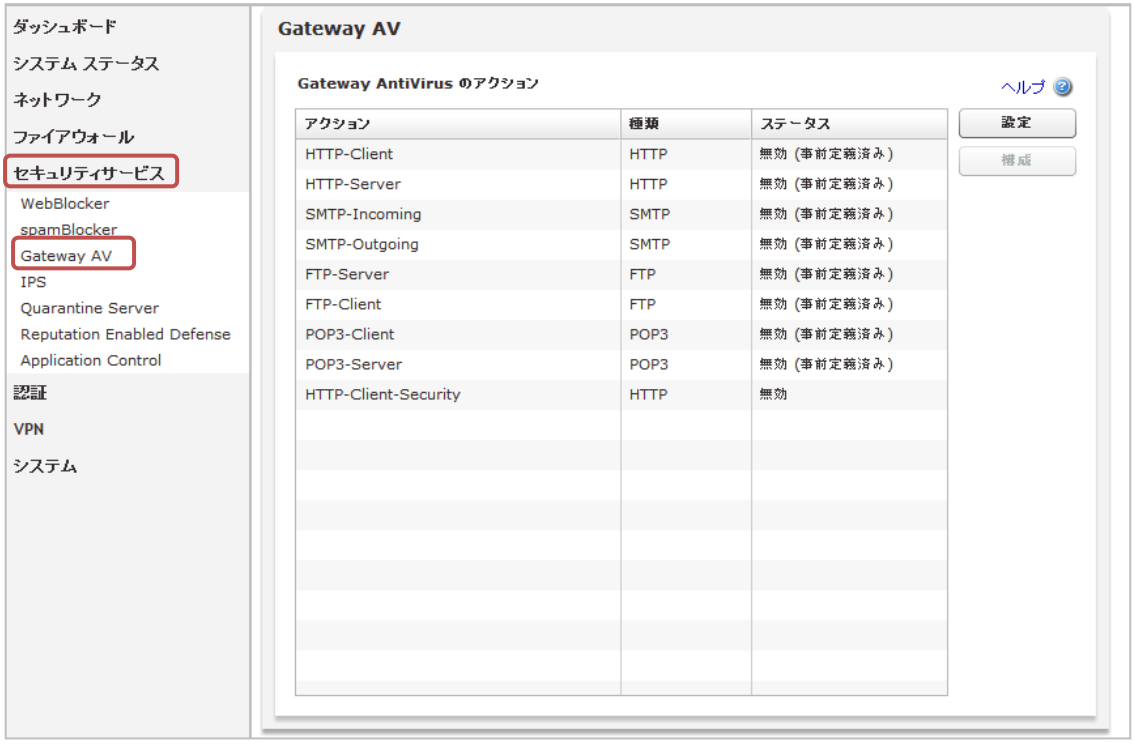


Gateway AntiVirus の設定

GatewayAntiVirus を有効にすると、XTM はネットワークを介して侵入しようとするウィルスを検知し、防御することができます。

Gateway AntiVirus を有効にする

Gateway AntiVirus (以下文中では「GAV」と略します)を使用するには、前節と同様プロキシアクションの定義とプロキシポリシーを追加しておく必要があります。
その上でメニュー セキュリティサービス ー Gateway AV をクリックします。



GAV を有効にするため、事前に定義したプロキシアクションを選択し、設定ボタンをクリックします。

「Gateway AntiVirus を有効にする」にチェックを入れます。

ウィルス検出時の動作としては「切断」を選択します。スキャンエラー発生時には「許可」が推奨されています(どちらもデフォルト)。

スキャンエラーは、パスワードがかかった ZIP ファイルなどで発生します。それを切断にしてしまうと、ZIP の受け渡しにも支障をきたすためです。

それでもそこに Virus が感染している場合はクライアント PC のアンチウィルスソフトが処理することになるでしょう。

以上で保存します。GAV は有効になります。

Gateway AntiVirus を構成する

プロキシアクションの一覧に戻ったら、再度、定義したアクションを選択し、今度は「設定」ボタンをクリックします。

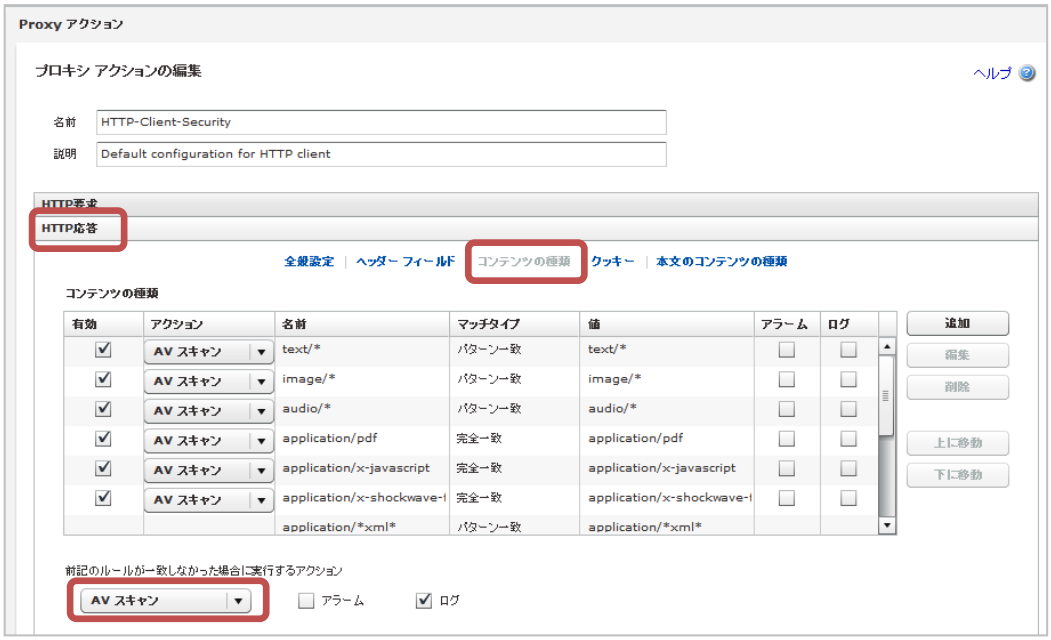
GAV の全体的な設定になります。

ZIP ファイルの中身をスキャンしたい場合は「圧縮解除を有効にする」にチェックを入れます。

AV のシグネチャが自動で更新されるため、自動シグネチャの更新の欄で「Gateway AntiVirus」にチェックを入れます。以上で設定を保存してください。

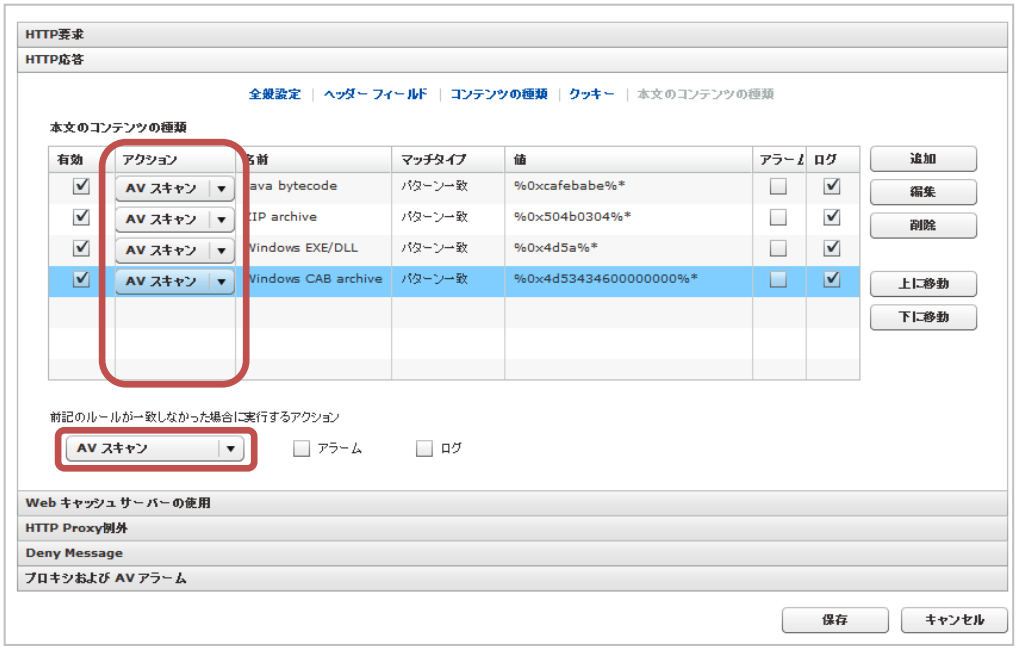
ヘッダーやファイルの種類で GAV をどう適用するかというより細かい設定は、プロキシアクション側で指定します。
メニューのファイアウォール　ー　Proxy アクションをクリックし、自分で定義したアクションを選択し、編集ボタンをクリックします。

プロキシアクションの編集で「HTTP 応答」のセクションを選択し、「コンテンツの種類」をクリックします。
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 AV スキャンをかけるというアクションがデフォルトになっています。
ただ、すべてのヘッダーのパターンを把握して設定するにも限界がありますので、このドロップダウンリストで「AV スキャン」を選択するのも現実的です(つまりすべて AV スキャン対象に)。



次に同じ画面の「本文のコンテンツの種類」リンクをクリックします。

アクションとして、デフォルトでリストにあるコンテンツが「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 ファイルやソフトウエ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。

最後に保存ボタンをクリックして、設定を反映させます。

以上で Gateway AntiVirus の設定が完了しました。
しばらく置いておく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。

spamBlocker の設定

spamBlocker では、Commtouch 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。

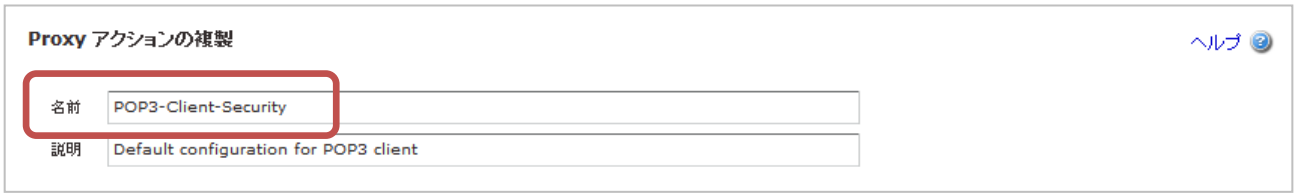
また、オプションで VOD(Virus Outbreak Detection)を有効にし、メールを経路にして拡散される新種のウイルスに対処することもできます。

POP-Proxy アクションを追加する

WebBlocker で Proxy ポリシーの HTTP-proxy が必要だったように、spamBlocker では POP3-proxy が必要です。また、それと紐づく Proxy アクションが必要です。では、まず Proxy アクションから定義しましょう。

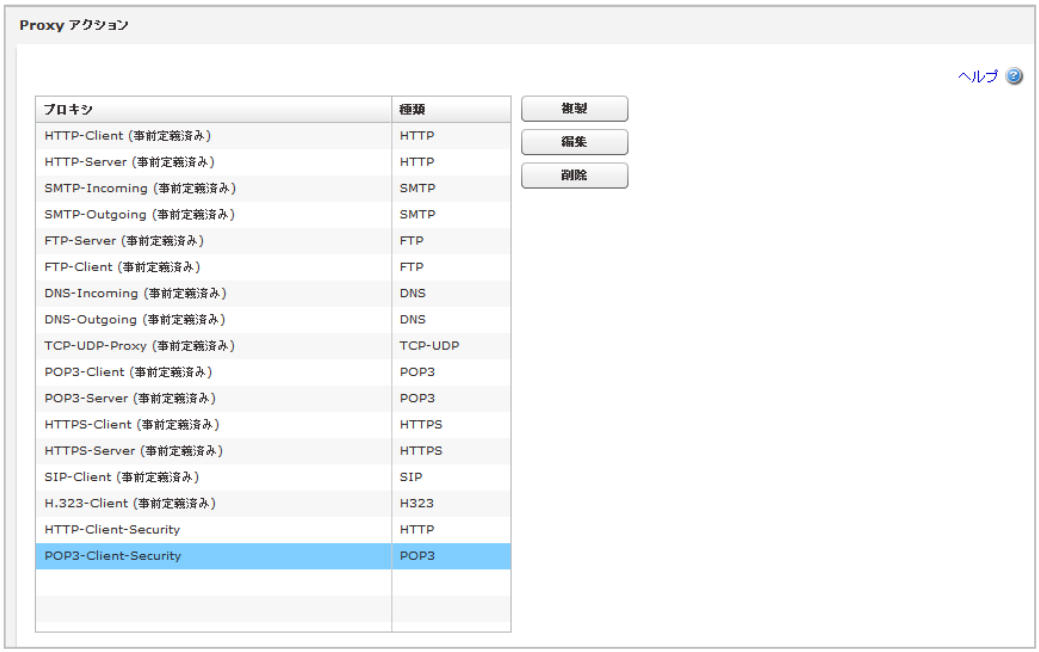
メニューのファイアウォール－Proxy アクションをクリックし、プロキシアクションの画面から、POP3-Client(事前定義済み)を選択し、複製ボタンをクリックします。

複製画面には諸々の設定項目がありますが、まずはアクションの名前を付けます。



そして画面右下の保存ボタンをクリックして、アクションを保存します。

Proxy アクションの一覧に追加されました。

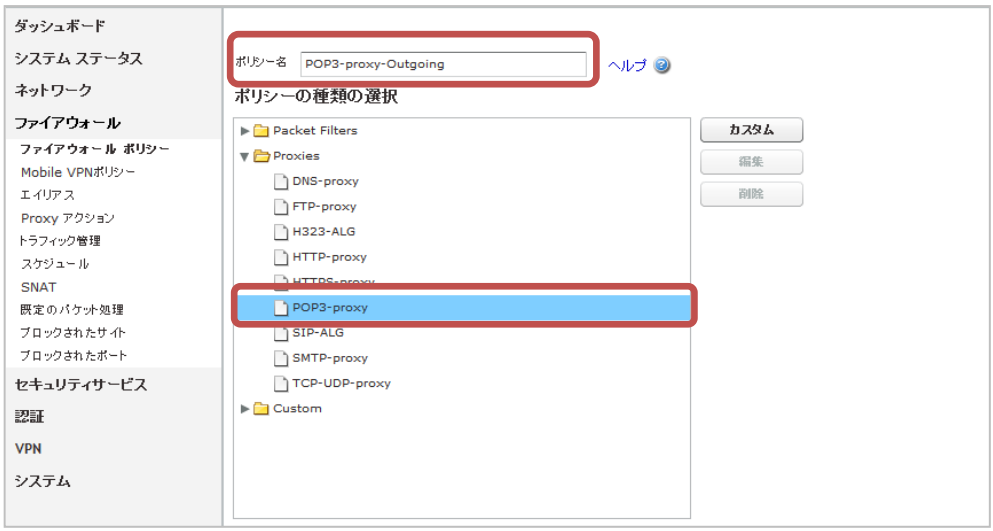


次にプロキシポリシーを追加します。

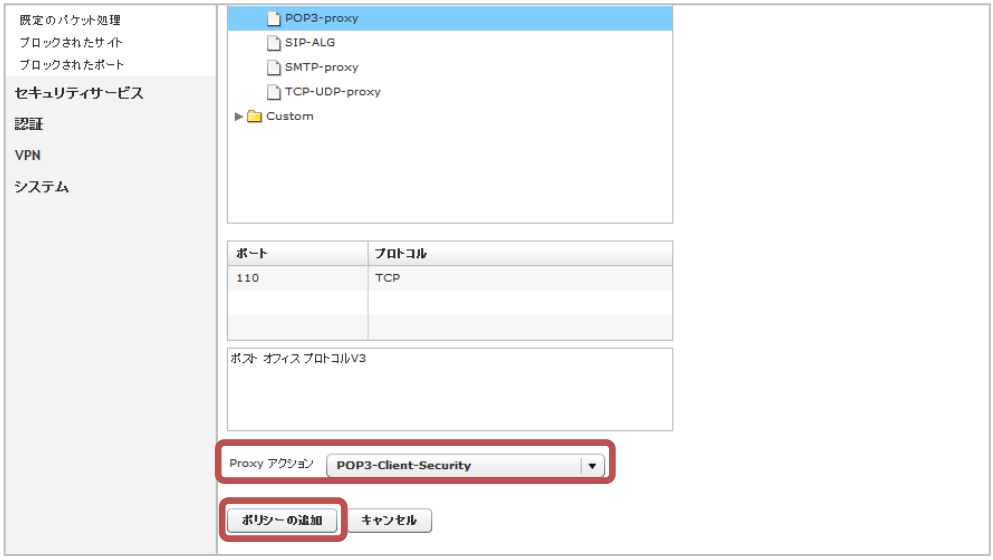
POP3-proxy ポリシーを追加する

メニューのファイアウォール ー ファイアウォールポリシー でポリシー一覧を表示し、ポリシーの新規追加ボタンをクリックします。

ポリシーの種類の選択画面になりますので、POP3-Proxy を選択します。ポリシー名も入力します。

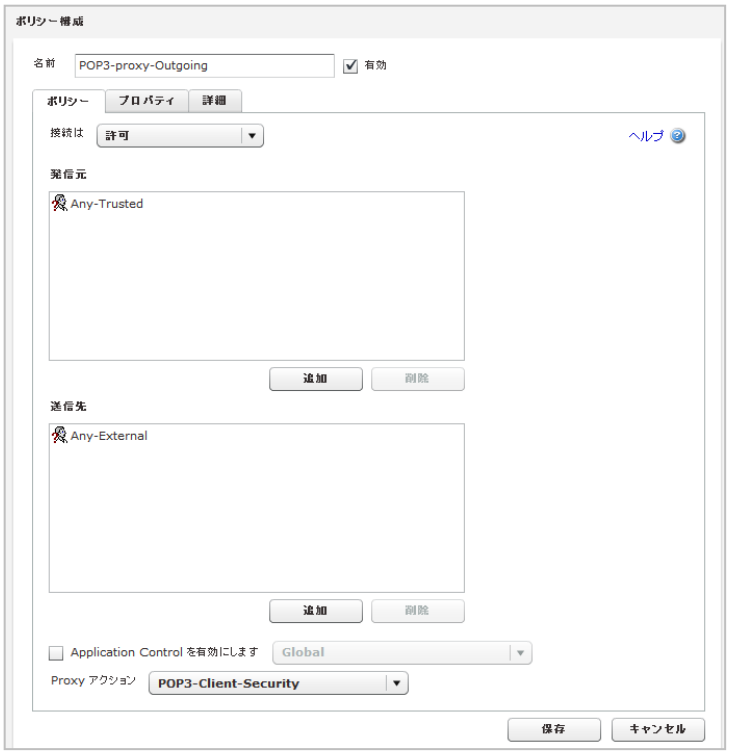


上の画面の続きです。画面下の Proxy アクションでは、先ほど事前に定義したものを選択します。

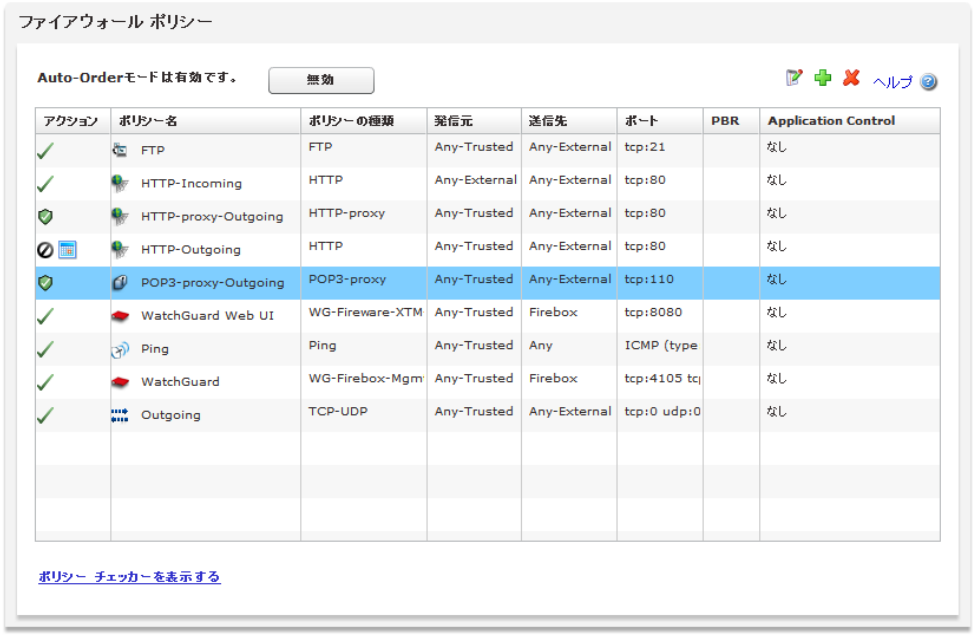


ポリシーの追加ボタンをクリックします。

ポリシー構成の画面になるので保存ボタンをクリックします。



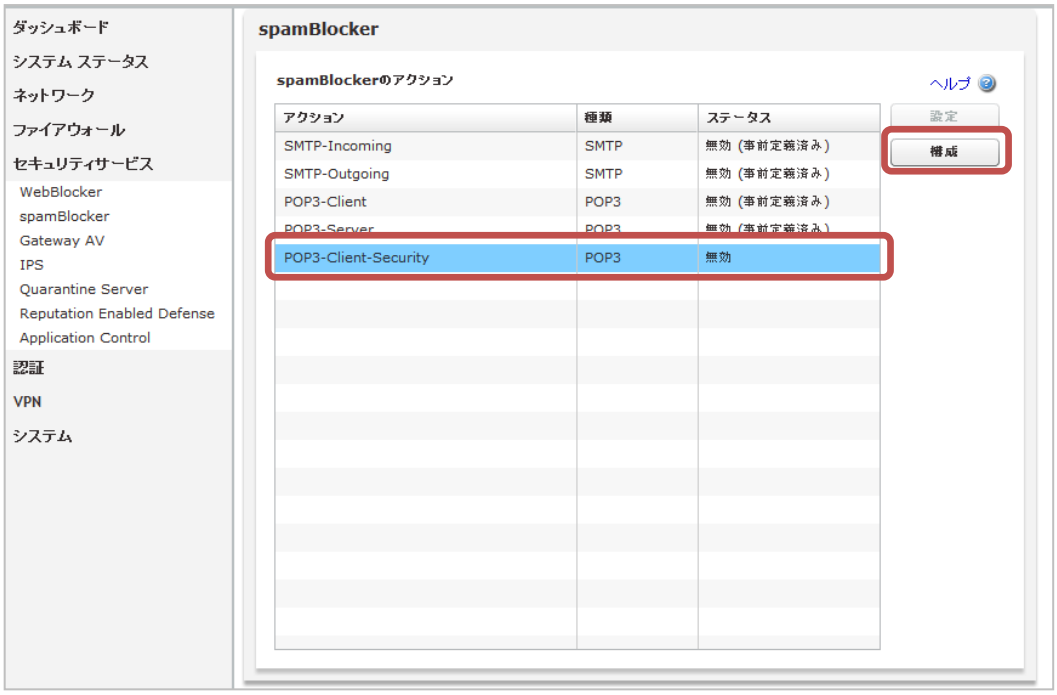
POP3 プロキシポリシーがポリシー一覧に追加されました。



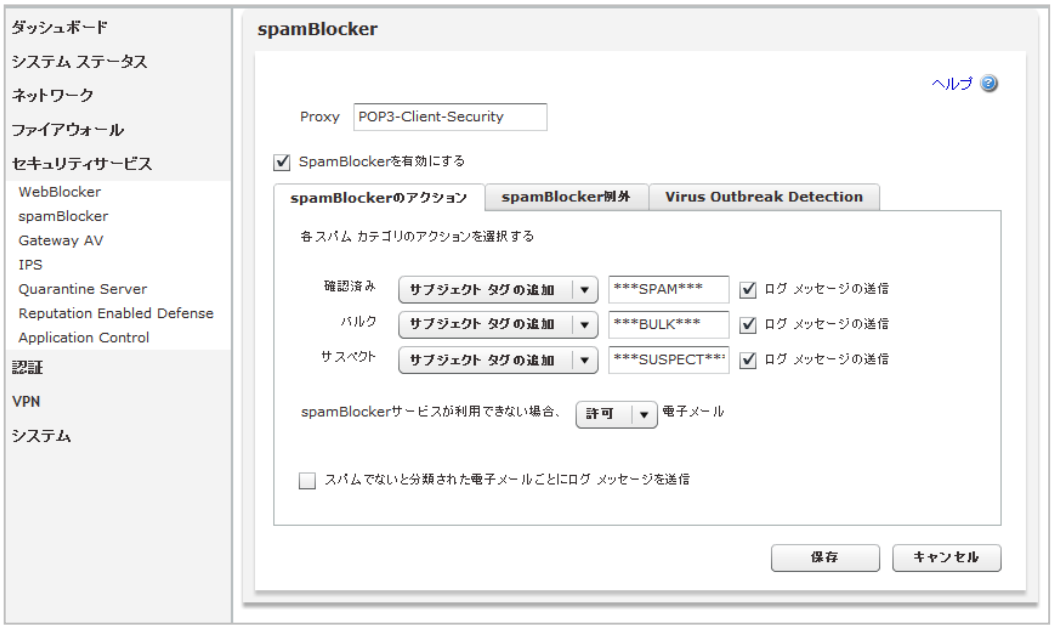
spamBlocker を構成する

メニューの[セキュリティサービス]－[spamBlocker] をクリックします。

spamBlocker アクション一覧が表示されますので、事前に作成したアクションを選択し、構成ボタンをクリックします。



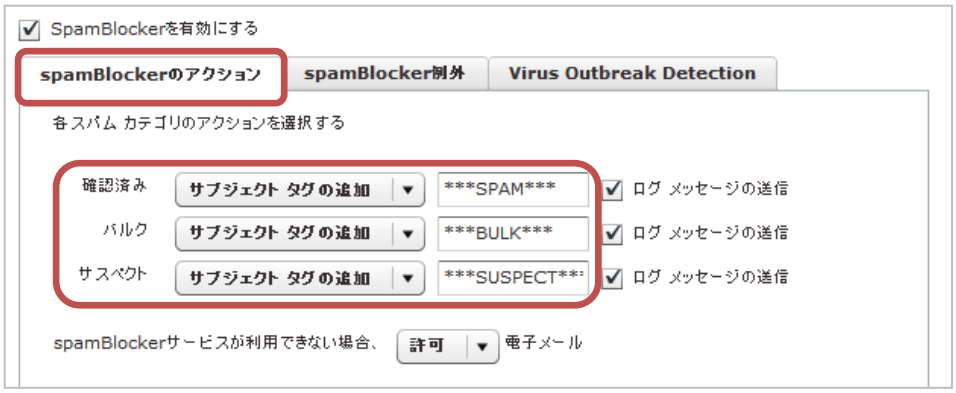
spamBlocker の設定画面で、「spamBlocker を有効にする」にチェックを入れます。



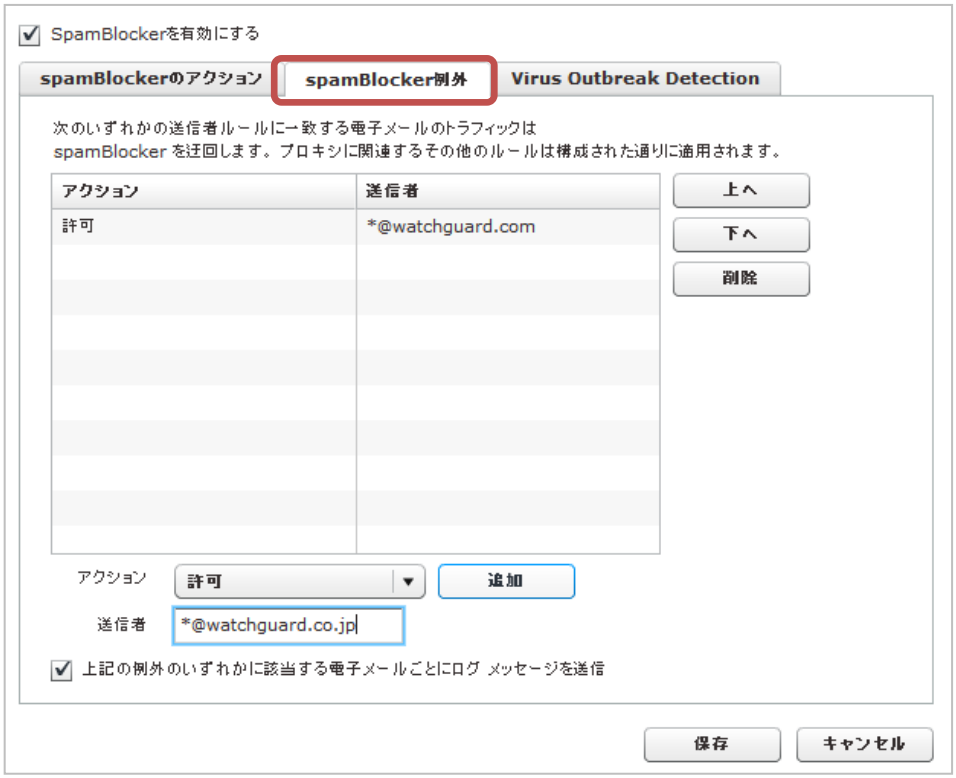
spamBlocker のアクションタブでは、スパムメールが検知された際の動作を定義できます。

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。



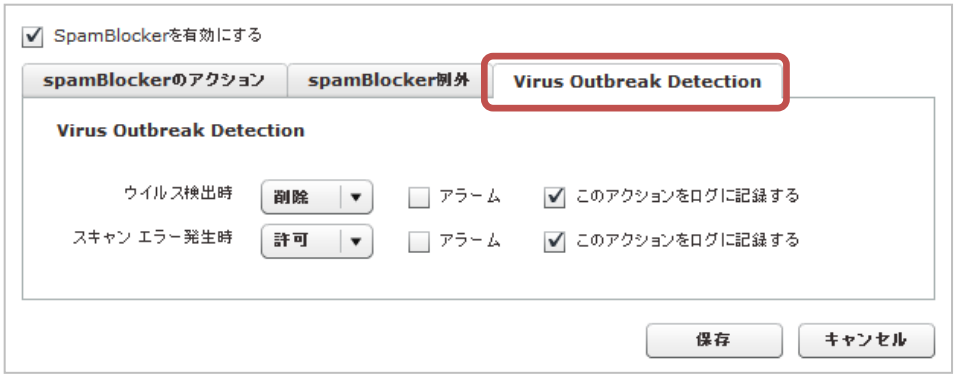
spamBlocker 例外タブでは、ホワイトリスト/ブラックリストの編集が行なえます。



この例では*@watchgaurd.com をホワイトリストに入れています。

*@watchguard.co.jp も入力し、追加ボタンを押せばホワイトリストの一覧に入ります。

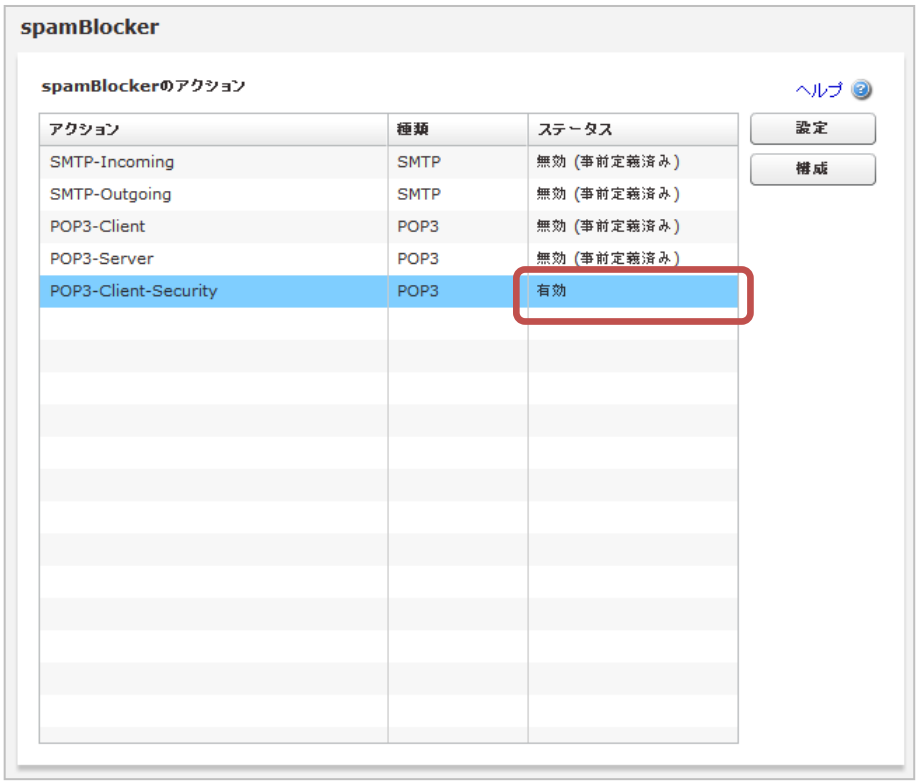
Virus Outbreak Detection タブでは、ウイルス検出時の動作を定義できます。



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。

保存するとアクションの一覧に戻ります。構成したアクションが有効になっていることが分かります。



以上で spamBlocker の設定は完了です。

WebUI 基本設定ガイドは以上です。

XTM は、UTM 機能をすべて有効にしてもスループットがよいことでご好評いただいてます。

この機会に是非、御社のルーター、ファイアウォール、UTM を WatchGuard XTM に統一していただき、強固なゲートウェイセキュリティを確保していただきたいと思います。

購入前/後のお問い合わせ先は以下のとおりです。ご不明な点がありましたら、いつでもご連絡ください。

御社のセキュリティ向上をお祈りしております！

お問い合わせ先

- 購入前のお問い合わせ
- トレーニングやこのテキストについてのお問い合わせ

電話番号	03-5456-7880
メールアドレス	JPNSales@watchguard.com

- 購入後のサポート問い合わせ

電話番号	0120-585-665
メールアドレス	JPNSupport@watchguard.com