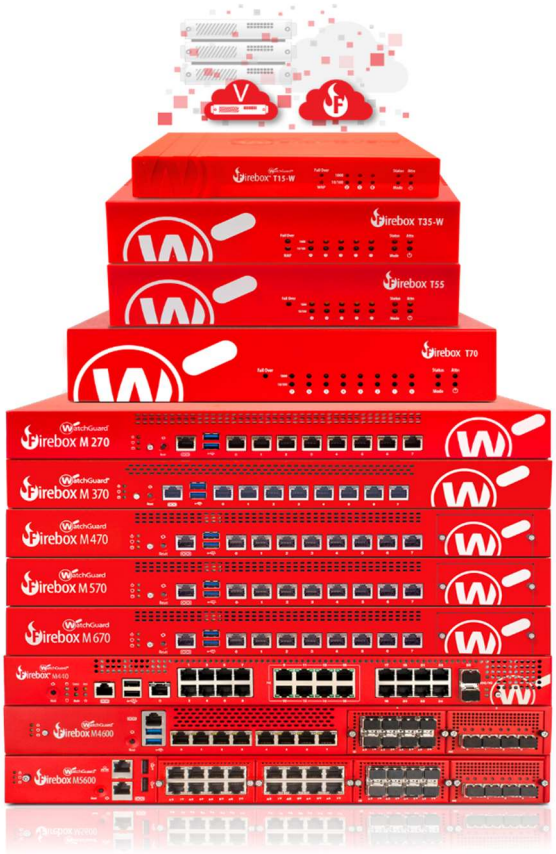
Firebox WebUI ガイド



ウォッチガード・テクノロジー・ジャパン株式会社

2019 年 8 月 Rev-5

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 WSM 基本設定ガイドの姉妹版です。基本設定ガイドにおいて WSM で設定した内容を、WebUI で設定するというコンセプトで解説しています。

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、Firebox 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、2019 年 5 月時点での最新バージョン Fireware OS v12.4 のものです。

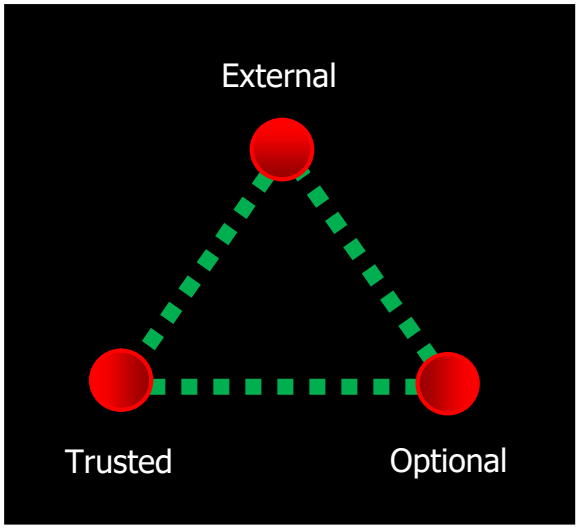
このガイドが、Firebox を自在に使いこなす一助になれば幸いです。

第一章 Firebox のセキュリティ概念

Firebox のネットワーク概念

Firebox 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



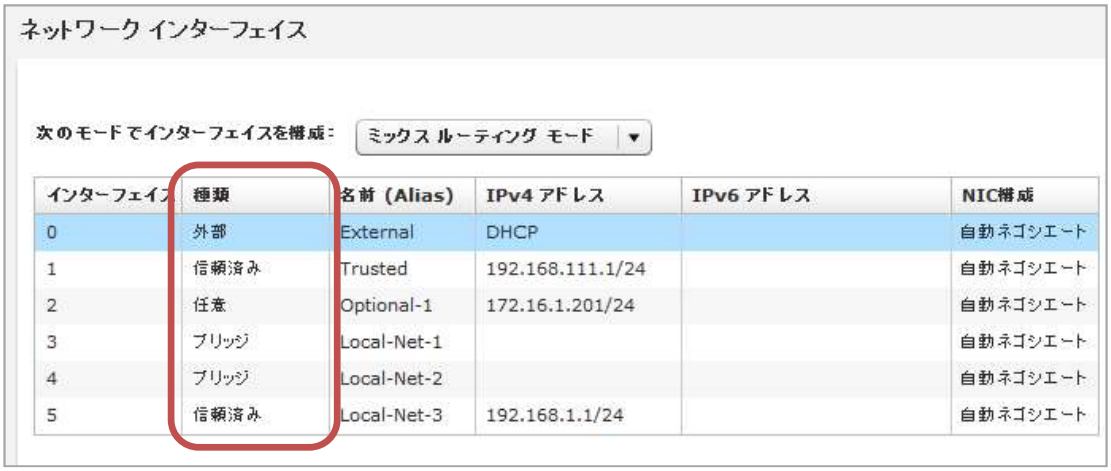
この「三角関係」、すなわち 3 種類のネットワークのゾーンを意識するなら、Firebox の設定は非常に容易です。

WebUI のネットワーク設定に見る Firebox の概念

Firebox 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

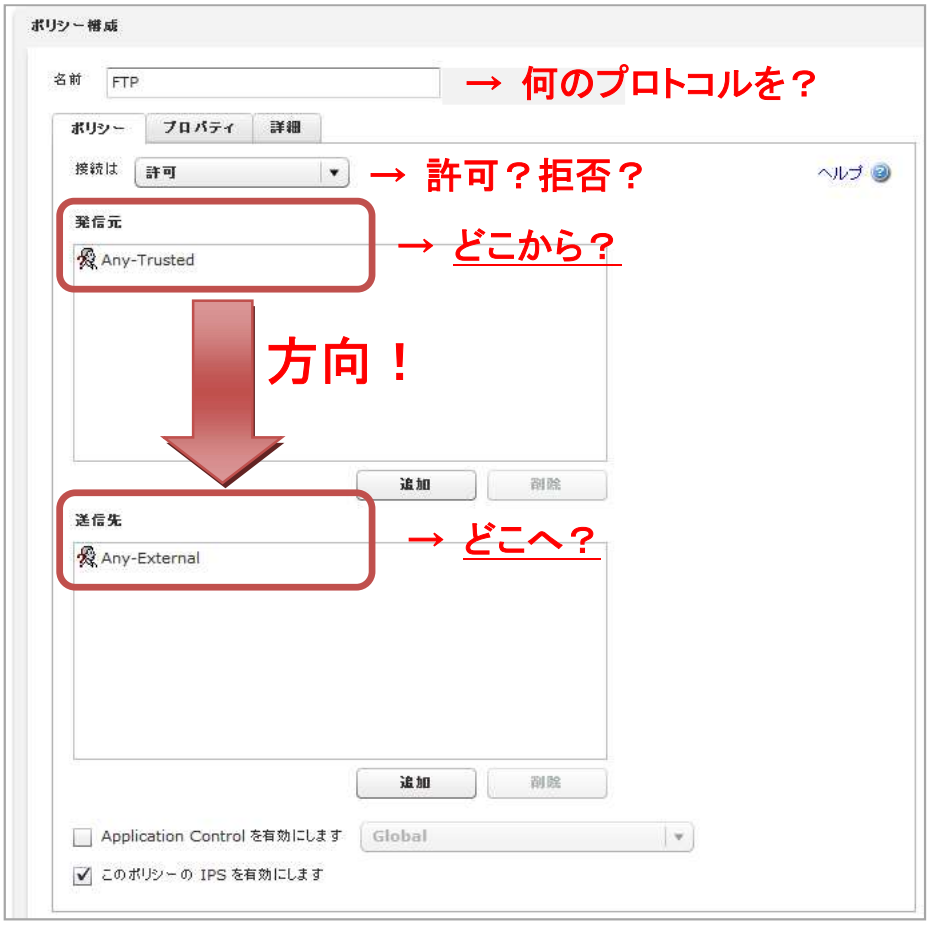
（一部ブリッジですがこれも Trusted です。ブリッジの構成は後述します）

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

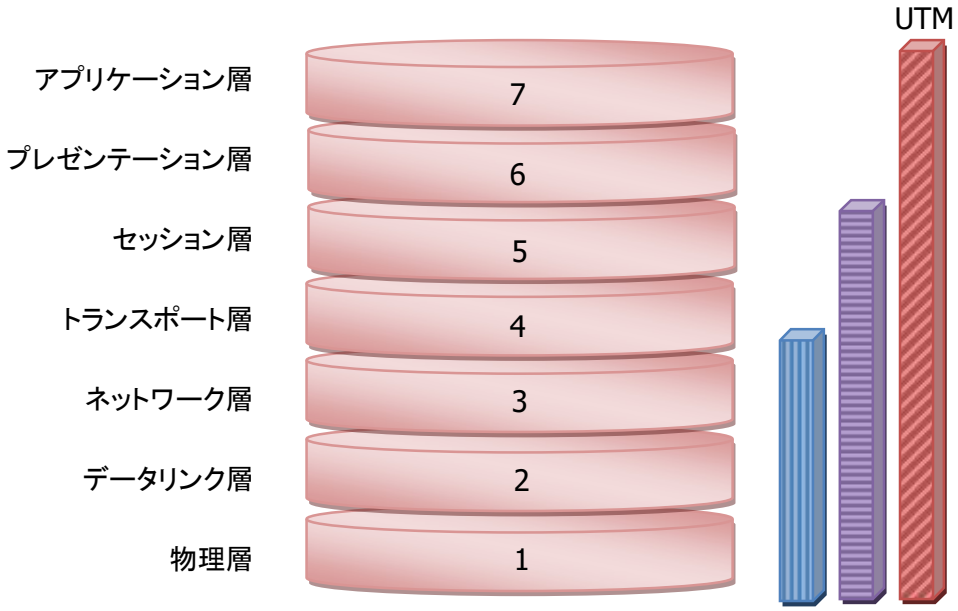
以下は実際のポリシー構成画面です。（第四章で詳しく解説します）

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。



Firebox で実現可能なセキュリティ範囲

Firebox 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

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、 Firebox 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 Web ブラウザです。

これは、ブラウザでアクセスする環境があれば、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 Firebox 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。デバイスに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(Fireware 11.9.4 時点)。

- 既定のパケット処理オプションのログ記録の変更
- 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
- 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
- セカンダリの PPPoE インターフェイスを追加・編集する

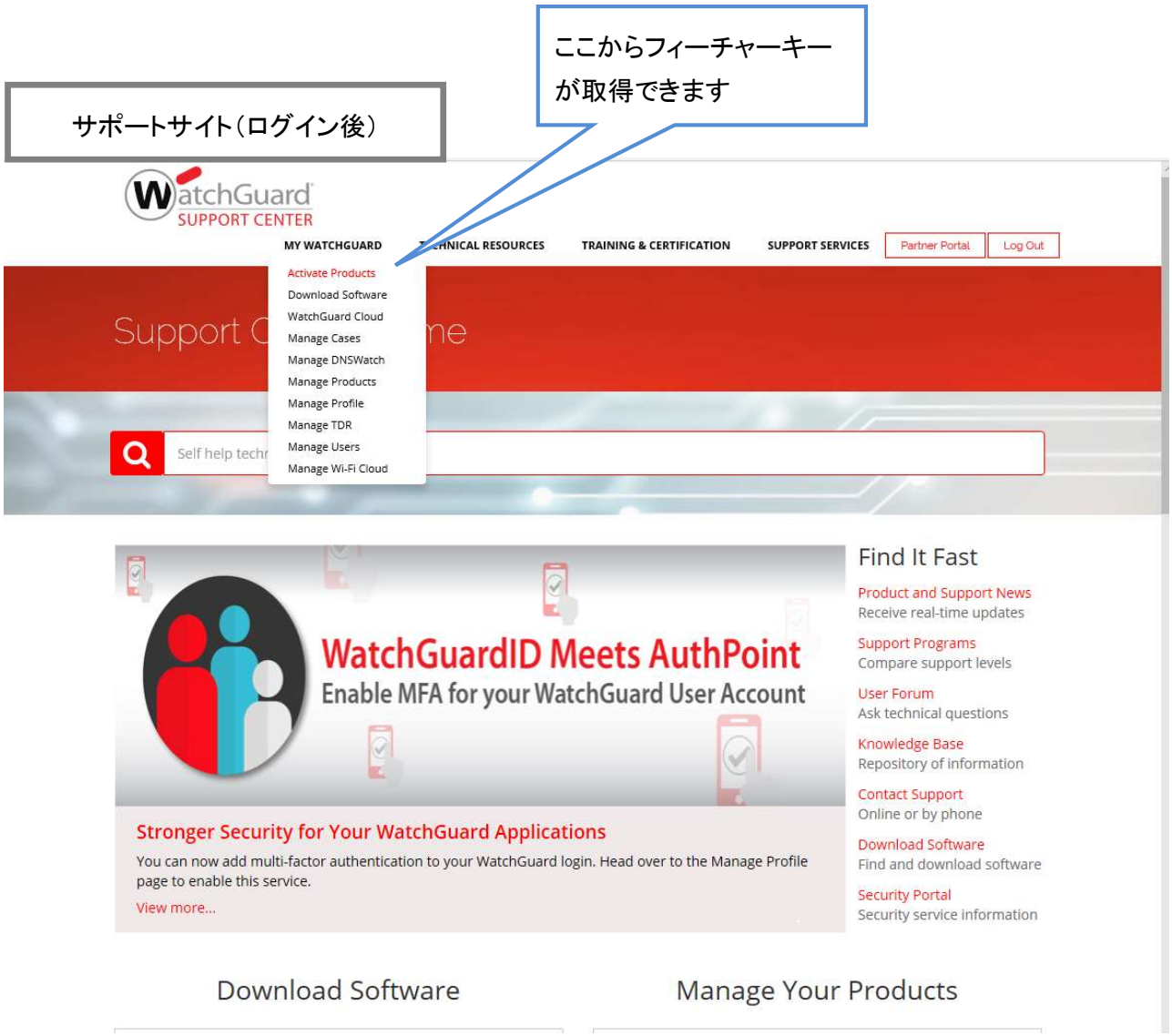
WatchGuard System Manager に付属している各種ツールの一部も WebUI では利用できません。

第二章　初期設定

事前準備

事前準備として、セットアップするデバイスのフィーチャーキー(ライセンスキー)の取得を行います。
WatchGuard サポートサイトにログインし、『My Products』から、該当機器のフィーチャーキーを取得し、テキストファイルなどで保存しておきます。

WatchGuard　サポート(US)　：　https://watchguard.force.com/customers/CustomerCommunityHome

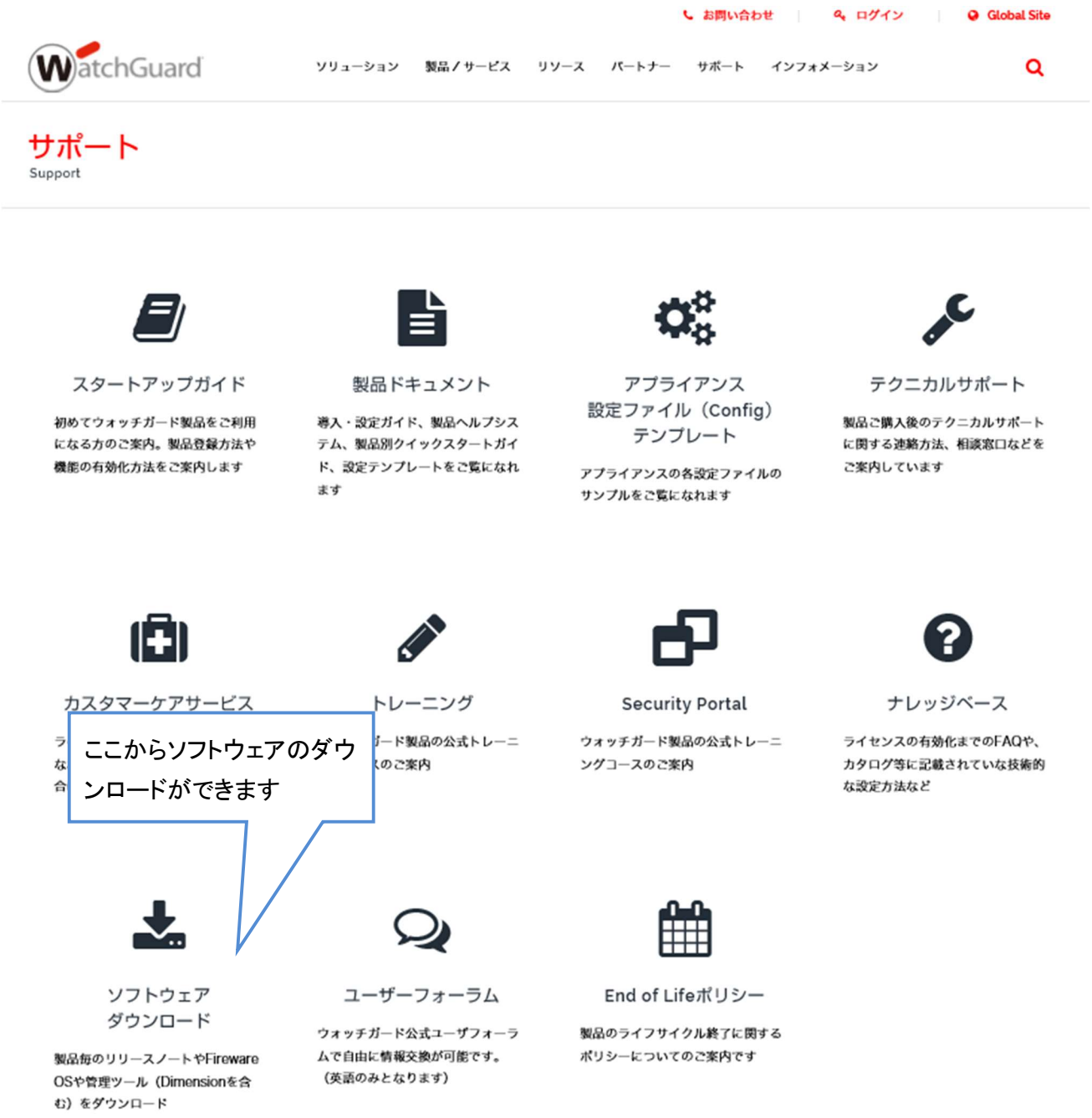


WatchGuard サポート（US）： https://www.watchguard.co.jp/support

また、必要なソフトウェアもインストールしておきましょう。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、管理者の方は WSM を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。Fireware は最新バージョンにアップグレードする際に必須となります。

- WatchGuard System Manager ： 管理ツール
- Fireware ： ファームウェア(機器のシリーズに対応したものを選択)

サポートサイト（ログイン後）



ソフトウェアがダウンロードできたら、WatchGuard System Manager のインストールを行います。
インストーラーはすべてデフォルトで進めます。

次に Fireware も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。
以上で準備は完了です。

ファクトリーリセット

購入した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、Firebox 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 Firebox 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 Firebox は「セーフモード」というモードで動作します。

リセット後にはセットアップ ウィザードを実行できますので、設定する本体と PC を LAN ケーブルで結線しておきましょう。

結線

どのモデルも 1 番ポートがデフォルトで設定可能な Trusted ポートとなりますので、PC と Firebox の 1 番ポートを LAN ケーブルで接続しておきます。

Firebox M シリーズ

Firebox T シリーズ

次にシリーズごとのリセット方法を解説します。

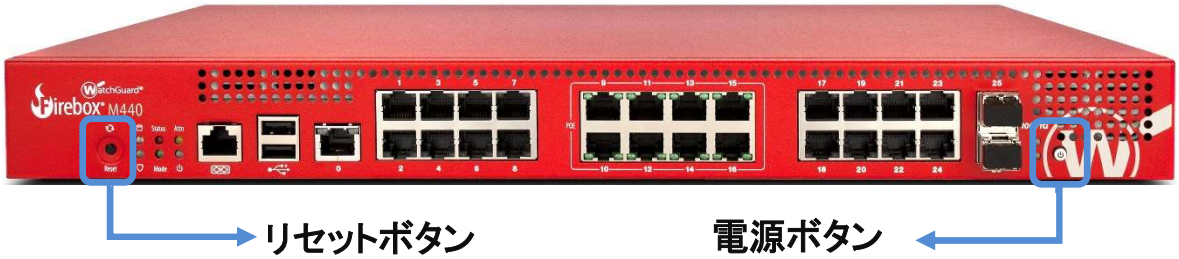
Firebox M440 のリセット

1. 本体背面の電源スイッチを入れ、電源を投入します

2. デバイス前面の電源ボタンを 3 秒間長押しして、一旦電源を切ります

3. デバイス前面のリセットボタンを押した状態で、電源ボタンを短く押して電源を入れます

M440 の電源ボタンとリセットボタンの位置



4. リセットボタンを押し続け、Attn インジケーターが点滅したら手を離します

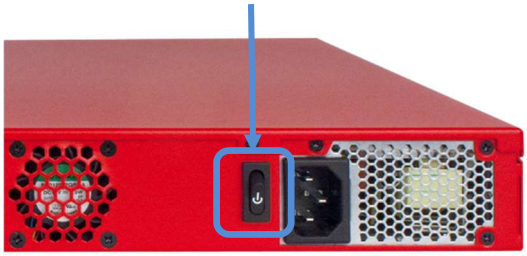
5. Attn インジケーターが点滅から点灯に変わるまで待ちます

Attn インジケーターが点灯になったらリセットされたことを意味します

6. 電源ボタンを短く押して電源を入れます

Firebox M440 リセット

1. 本体背面の電源スイッチを入れ、電源を投入します



2. デバイス前面の電源ボタンを 3 秒間長押しして、一旦電源を切ります

3. デバイス前面のリセットボタンを押した状態で、電源ボタンを短く押して電源を入れます

M440 の電源ボタンとリセットボタンの位置

4. Arm インジケーターが赤い間、リセットボタンを押し続けます

5. Arm インジケーターがゆっくり緑色に点滅している間も押し続けます

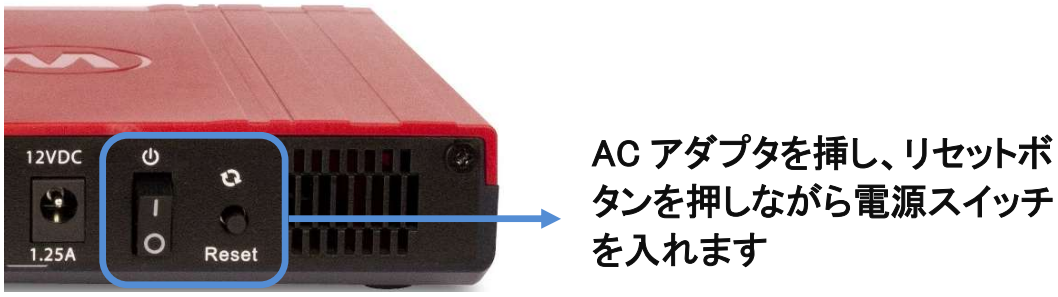
6. 緑色の点滅が早くなったら手を離し、点滅が赤になるまで待ちます

   Arm インジケーターが赤の点滅になったらリセットされたことを意味します。

Firebox T シリーズ

1. 電源を投入します。

Firebox T シリーズは電源スイッチがあるので、AC アダプタを挿し、Reset ボタンを押しながら電源スイッチを入れます。Reset ボタンは押したままにします。



2. Attn インジケーターが点滅し始めたらリセットボタンを離します。

点滅は 30 秒から 60 秒続きます(機種によっては点滅しないものもあります)。

3. Attn インジケーターが点滅しない場合は、点灯するまでリセットボタンを押し続けます。点灯したらリセットボタンを離します

4. 点灯した状態がリセットされたことを表わします。

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

設定後、PC 側から 10.0.1.1 に ping コマンドを実行して、疎通を確認して下さい。

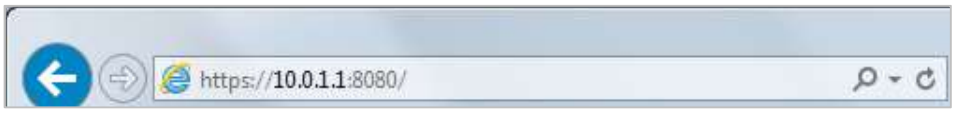
【豆知識】どんなときに初期化が必要？

- ✓ 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一から設定したい
- ✓ ある拠点から Firebox を引き上げてきて、別の拠点で使うために一から設定したい
- ✓ 雷による停電。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
- ✓ Fireware をアップグレードしたが、元のバージョンに戻したい

Web Setup Wizard

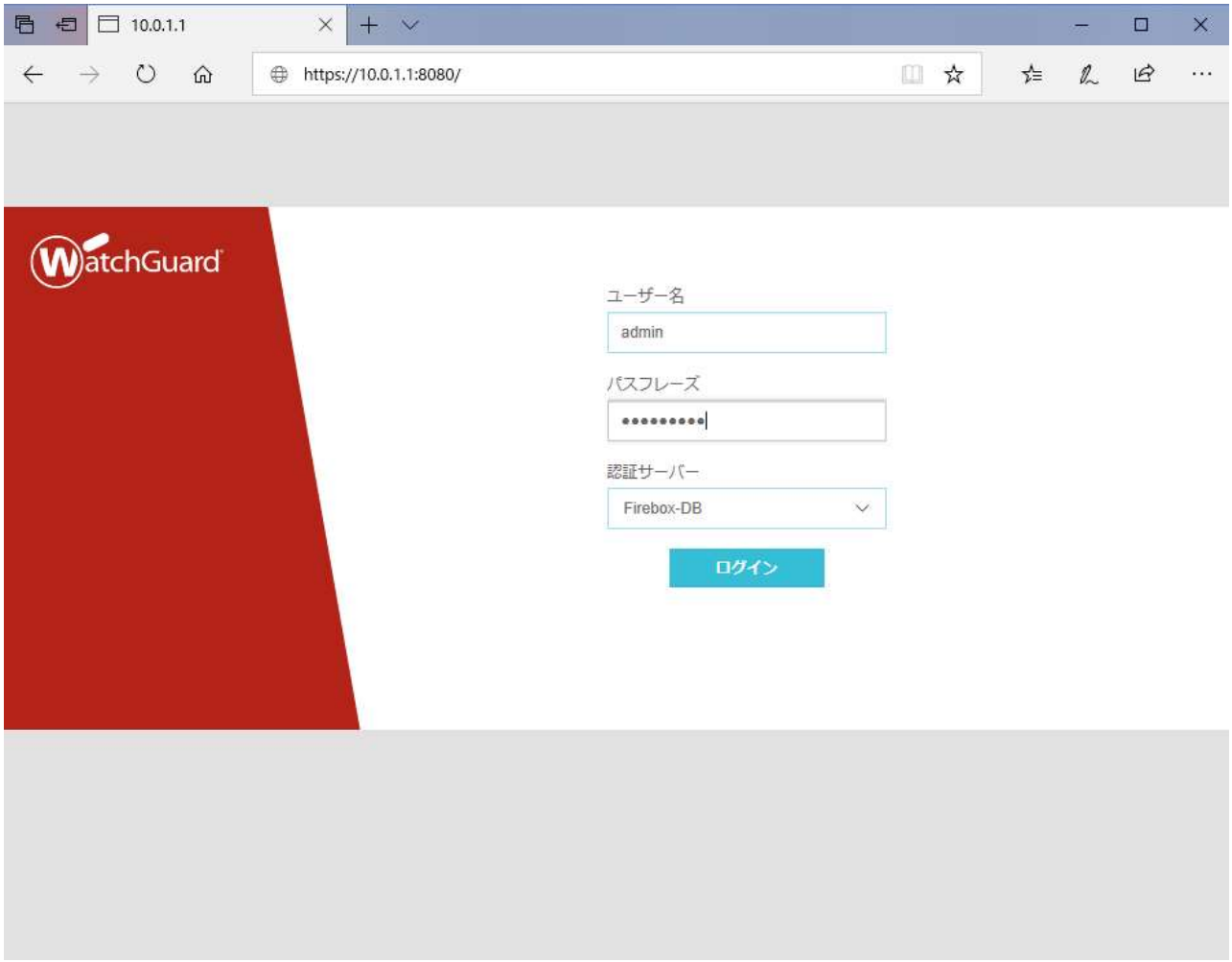
機器をセーフモードで起動したら、Web Setup Wizard で初期設定を行なうことができます。

設定する PC とリセットしたデバイスの 1 番ポートを結線し、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。

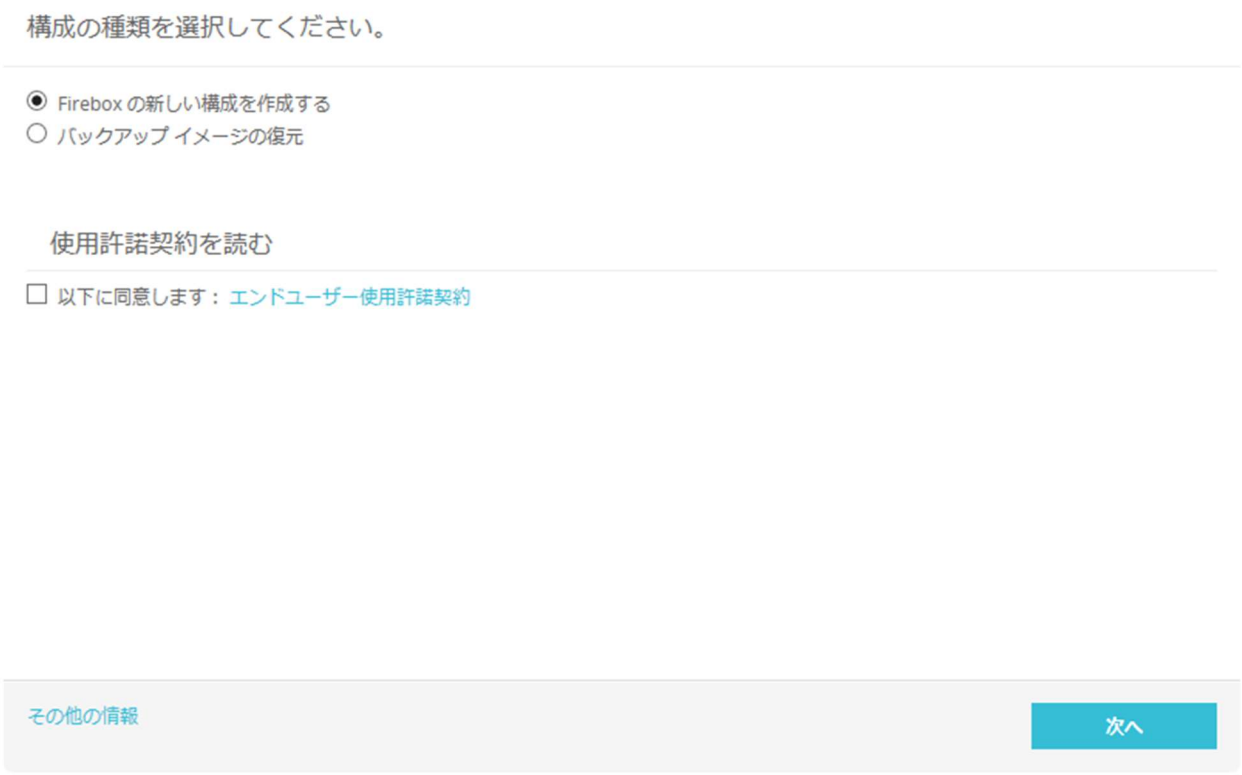


証明書のセキュリティ警告が出てもそのまま続行します。

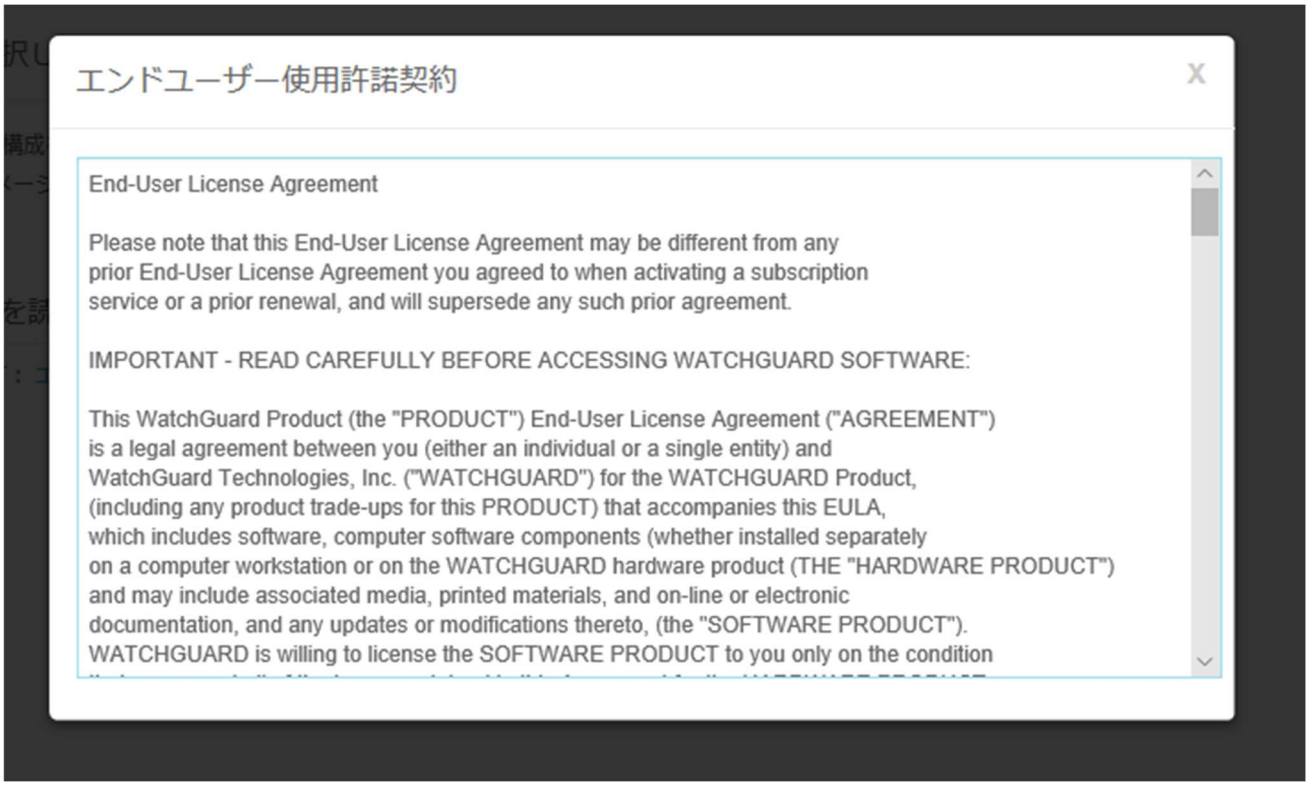
ログイン画面が表示されたらユーザー名に「admin」、パスフレーズに「readwrite」を入力し[ログイン]をクリックします。



Wizard が始まります。初期設定が目的なので「Firebox の新しい構成を作成する」にチェックして[次へ]。



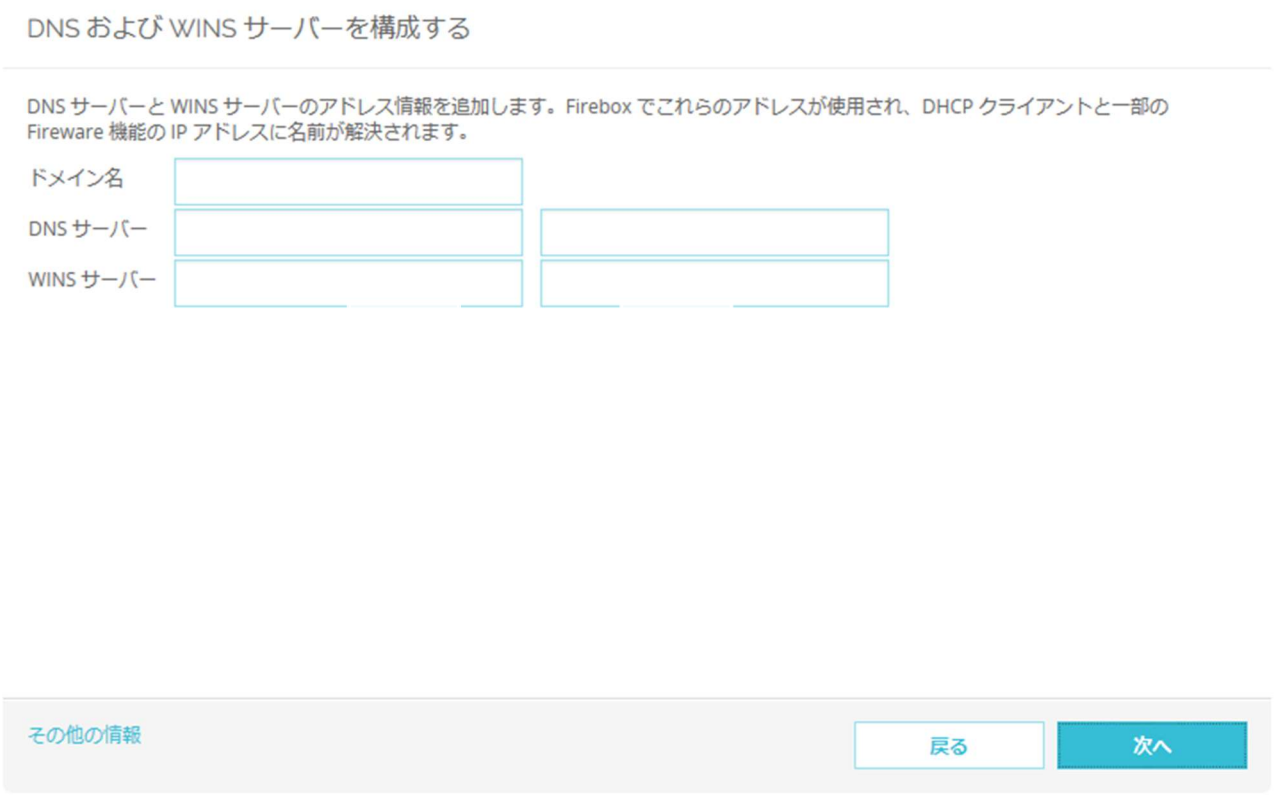
使用許諾契約の条項に同意して[次へ]。



以降、各種ネットワークやポリシーをできる画面になりますが、すべての設定項目は初期セットアップ後に変更可能ですので、設定が決まっていなくてもデフォルトのまま進んでいただいて構いません。

外部インターフェイスは DHCP(デフォルトのまま)を選択し[次へ]。

DNS サーバーの指定です。後から設定できますが、プロバイダもしくはシステム部門指定の IP アドレス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イス(現在接続しているポート)の設定です。

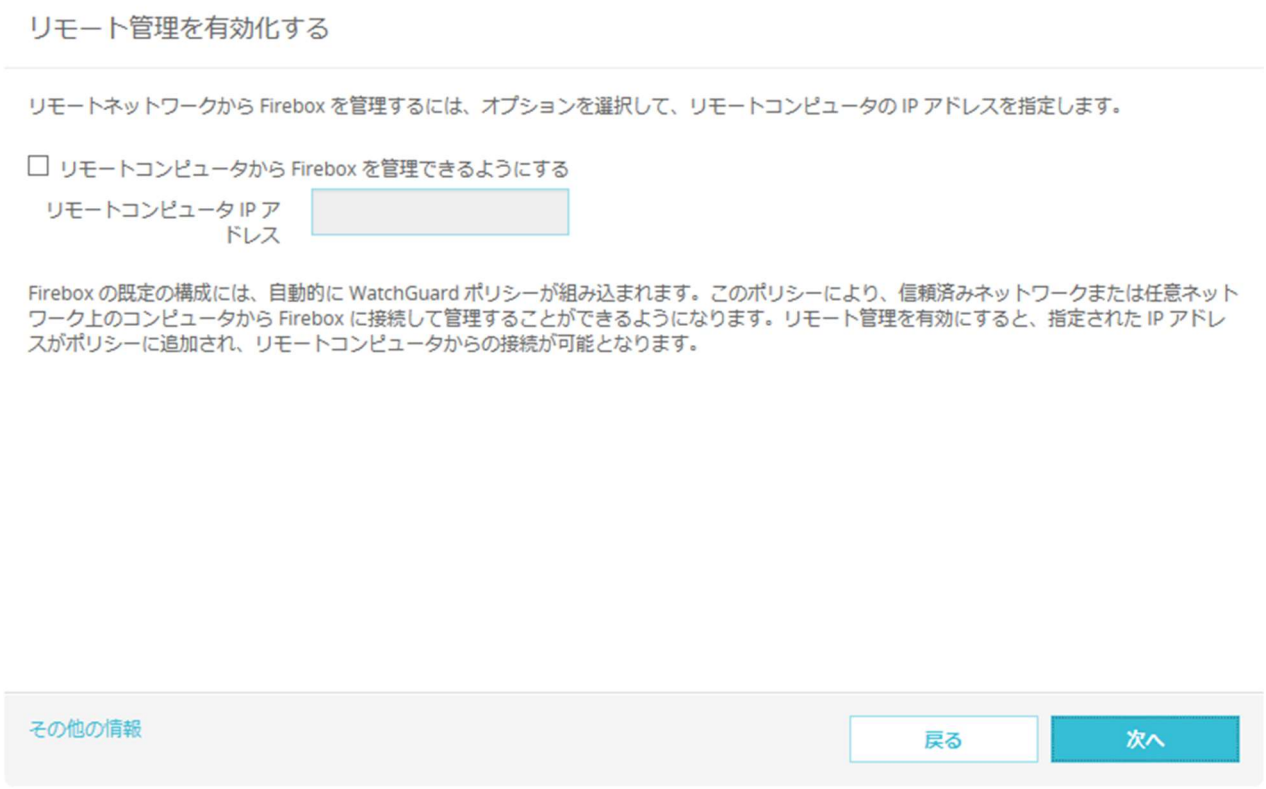
DHCP を有効にしてよければこのまま次へ。開始/終了 IP を変更しても構いません。

DHCP を有効にしたくない場合はチェックを外して[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。

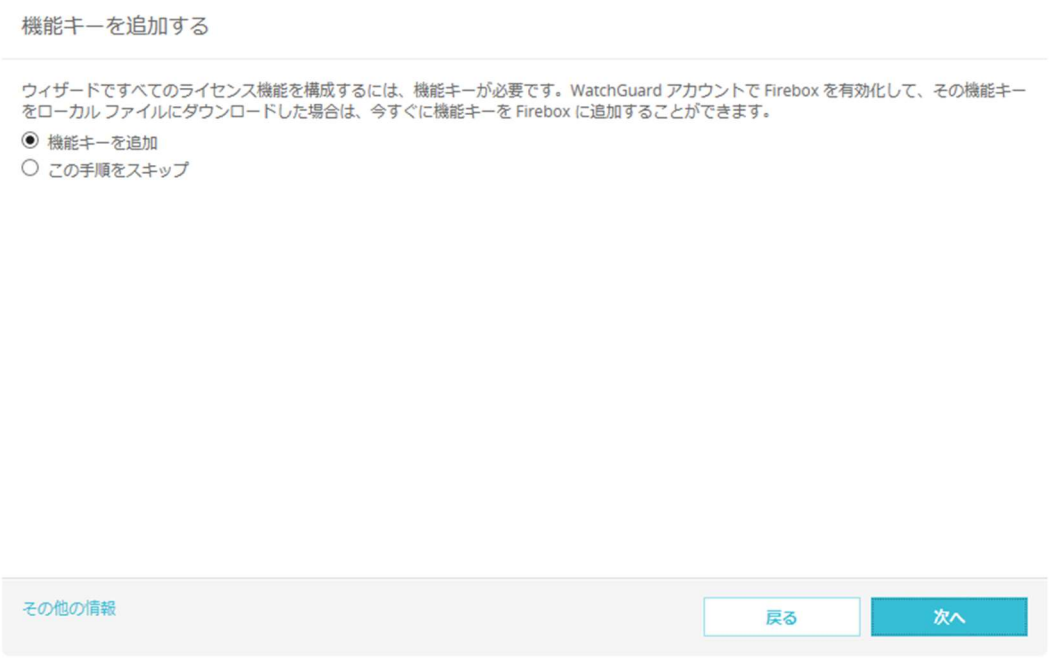
リモート管理の有効化はしないで[次へ]。（後からポリシーの編集画面で変更できます）



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]。

有効化の画面になります。[1]機能キーを追加 を選んで[次へ]。

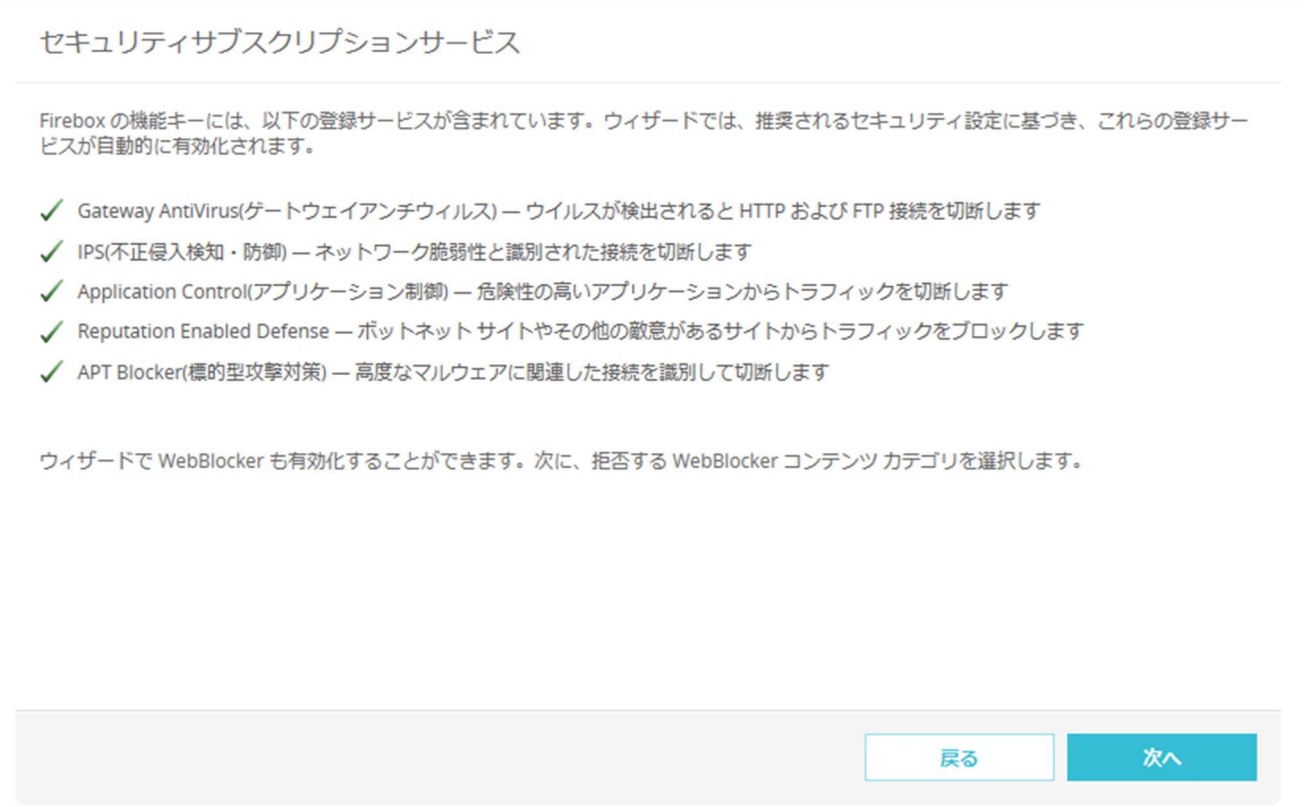


あらかじめ取得しておいた機能キーをテキストボックスに貼り付けて [次へ]。

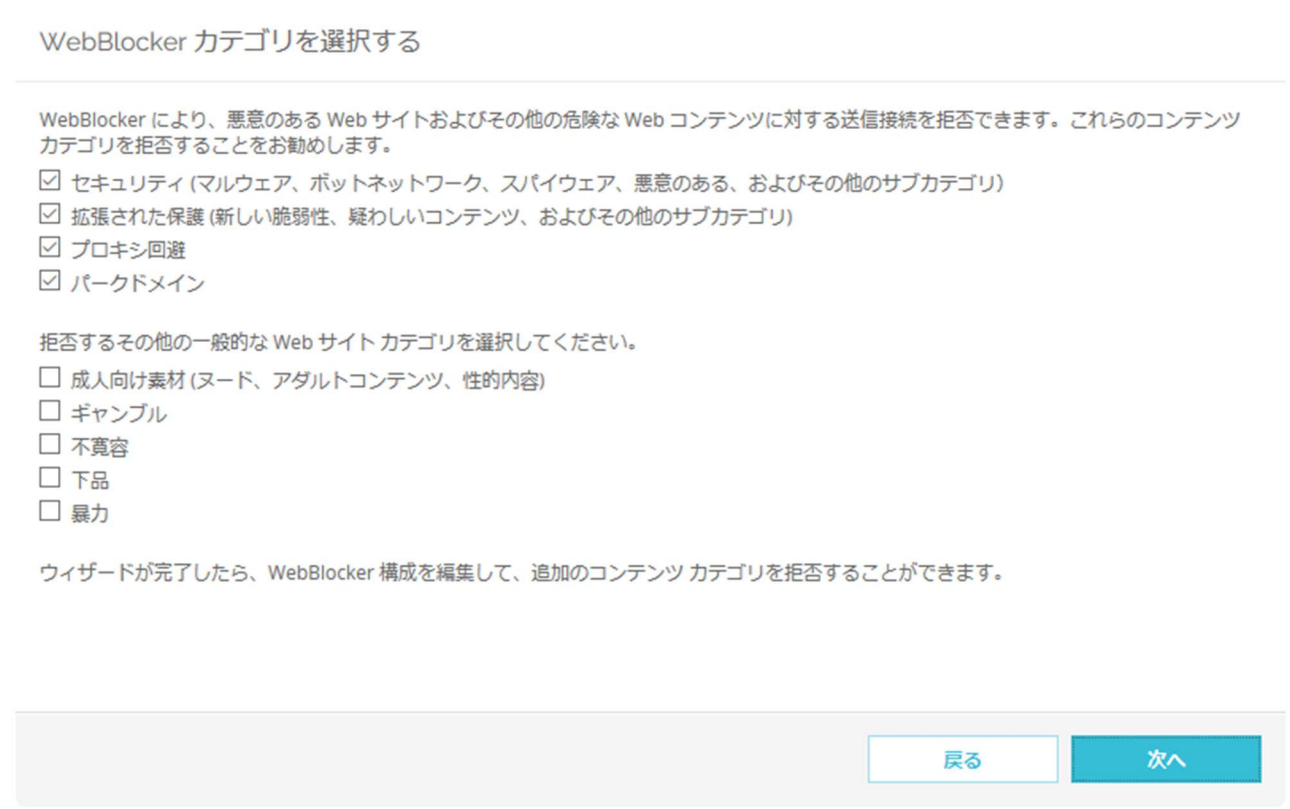
有効化された登録サービスを確認し、[次へ]。

---

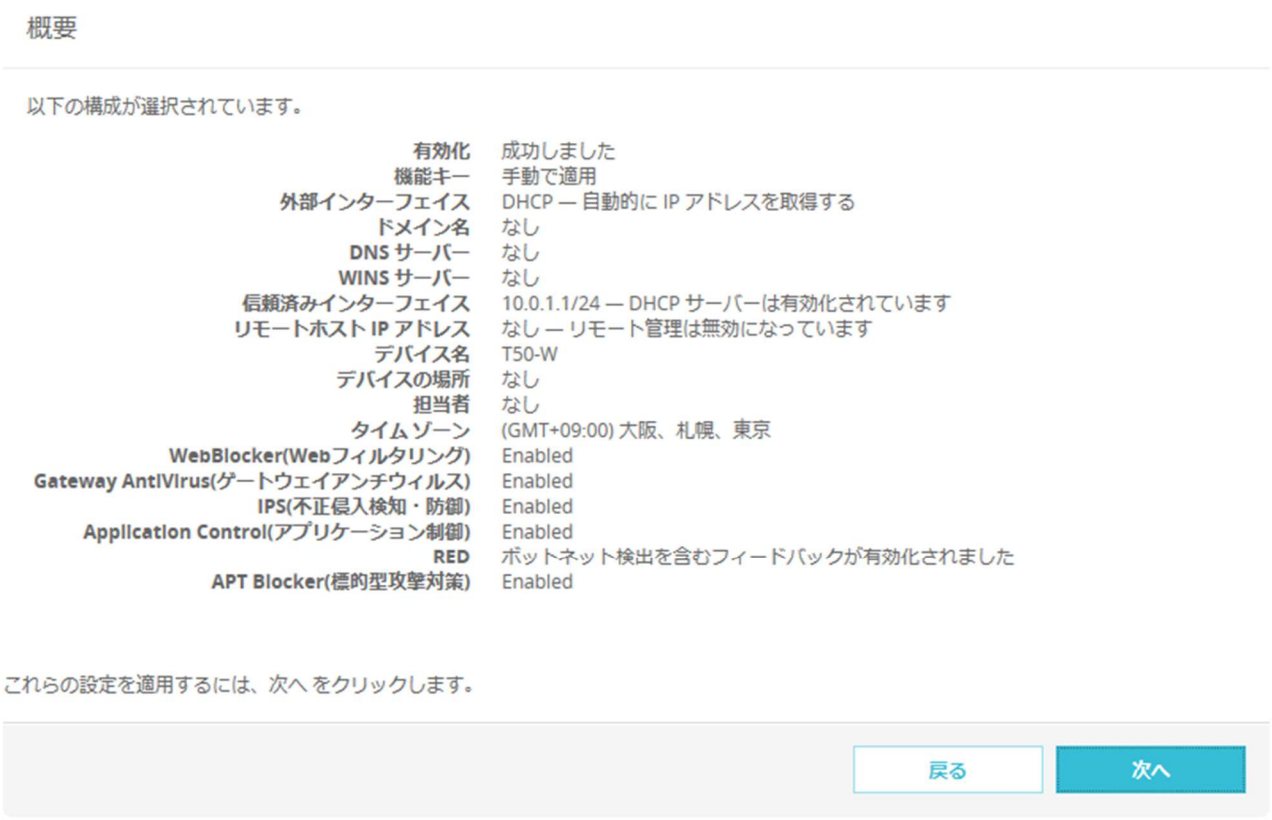
[1] オンラインになっている場合は「機能キーを追加する」画面がスキップされクラウドから自動的にキーが追加されます。



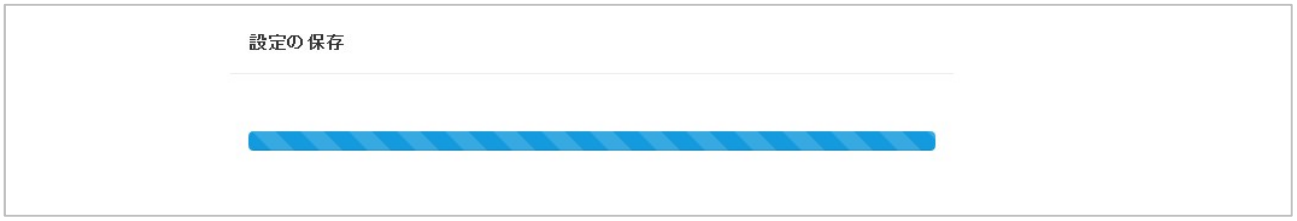
WebBlocker カテゴリを選択します。あらかじめ危険なサイトは禁止対象になっていますが、追加で禁止したい項目があればここでチェックします。



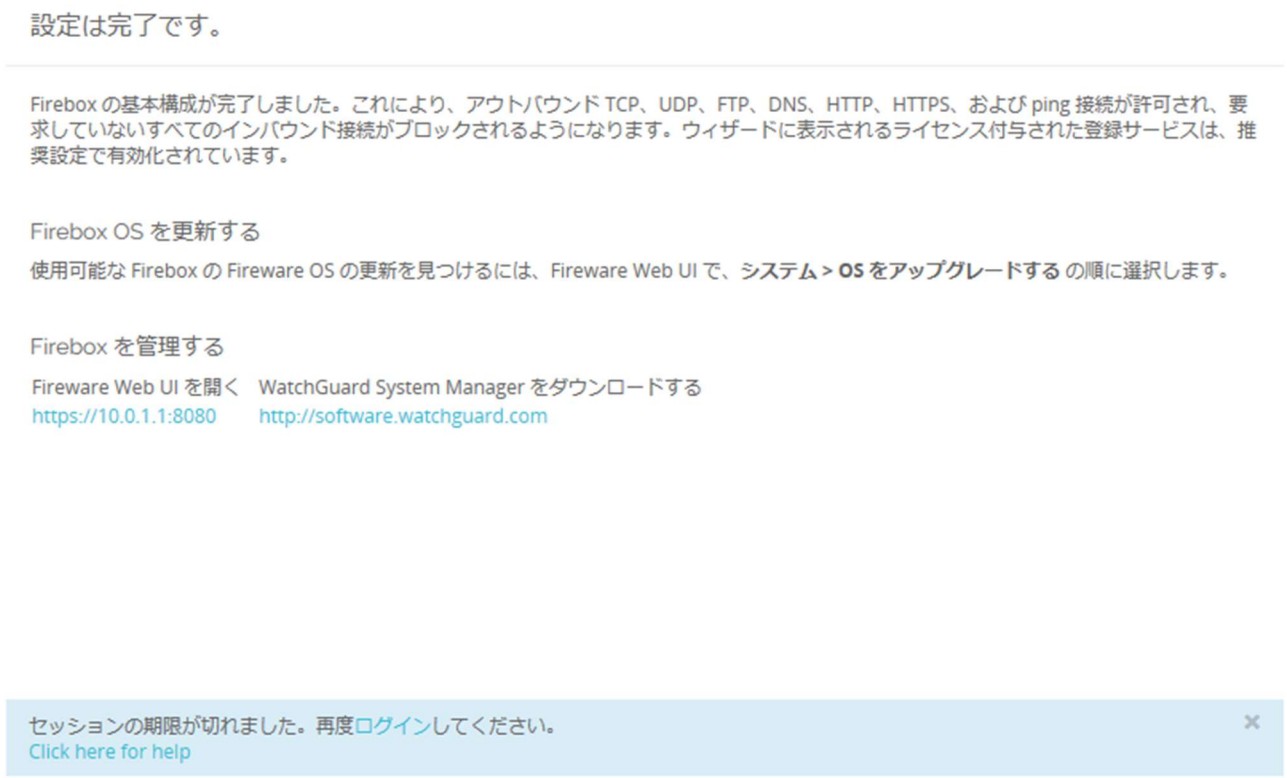
最後に設定のサマリーが表示されますので、内容を確認して[次へ]。



設定が保存されます。



セットアップ完了が表示されます。



自動的に再起動がかかり、設定した内容で起動します。3～4 分お待ちください。

再度 https://10.0.1.1:8080 にアクセスし、ウィザードで設定したパスワードでログインしてください。

以下のように Web UI のダッシュボードが表示されれば問題なく設定できています。

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)とは、機能を有効にするライセンスキーのことです。

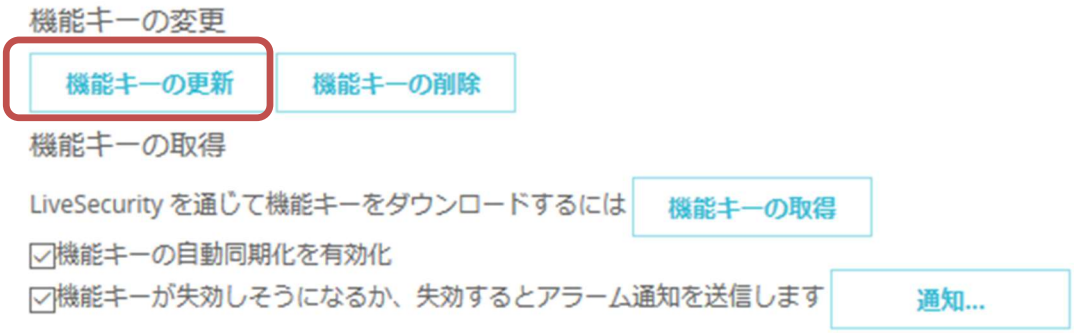
これをデバイスに追加しない間は、Firebox は限定的な状態で動作します。また、新たに追加で購入した機能も、アップデートされた新しい機能キーを追加しなければ有効になりません。

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・更新する手順を解説します[2]。設定操作には管理者権限でログインする必要があります。

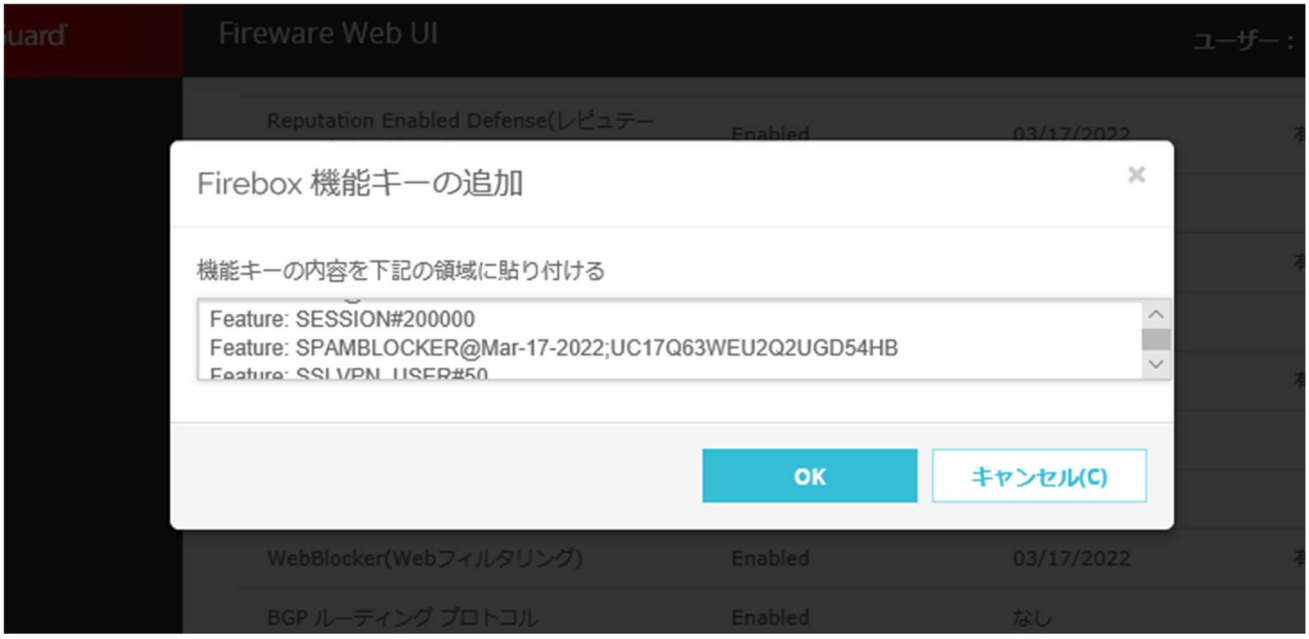
左側メニュー *システム* ー *機能キー* からアクセスします。

機能キーの画面が表示されたら、画面の下方にある [機能キーの更新] 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。



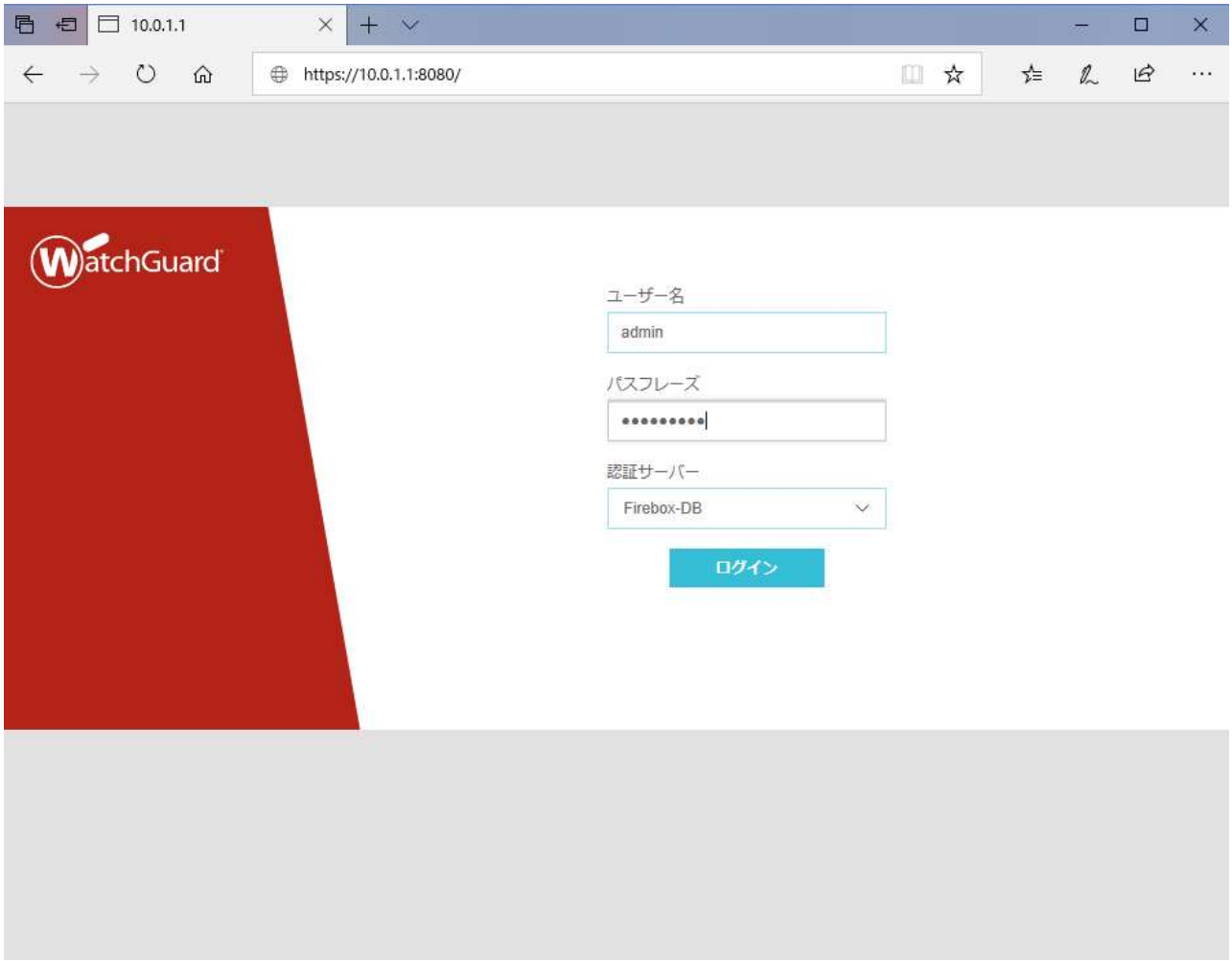
貼り付けたら保存ボタンをクリックします

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。

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

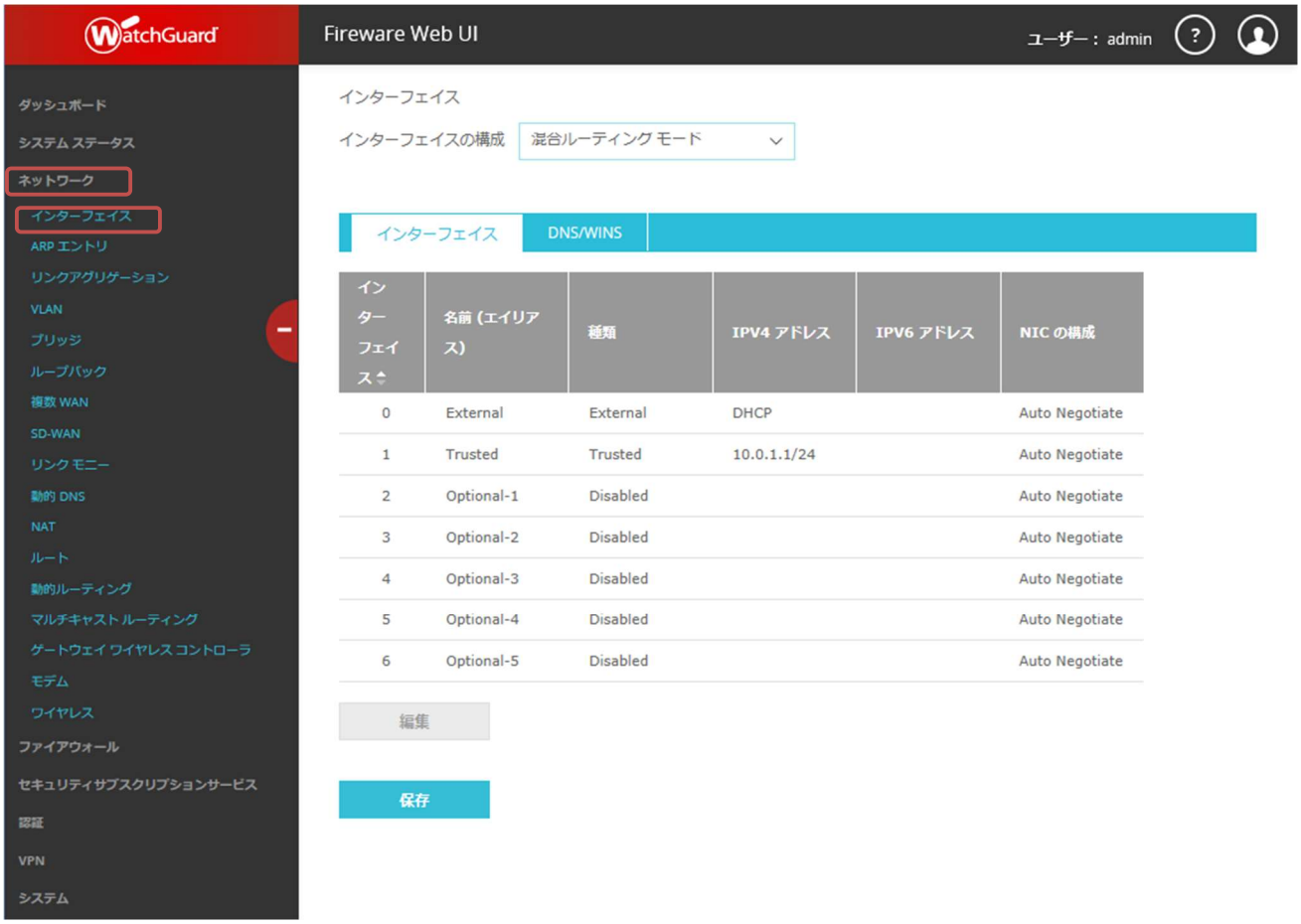
ブラウザで https://10.0.1.1:8080 に再び接続します。
パスフレーズは、Wizard で設定した構成パスフレーズを入力し、[ログイン]ボタンをクリックします。



ログインすると最初に Firebox の状態を表わすダッシュボードが表示されます。


WatchGuard
Fireware Web UI
ユーザー：admin
ダッシュボード
フロント パネル
セキュリティサブスクリプションサービス
FireWatch
インターフェイス
トラフィック モニタ
ゲートウェイ ワイヤレス コントローラ
Geolocation(ジオロケーション)
モバイル セキュリティ
ネットワークディスカバリー
システム ステータス
ネットワーク
ファイアウォール
セキュリティサブスクリプションサービス
認証
VPN
システム
フロント パネル
トップクライアント
すべて表示
名前 レート バイト ヒット
10.0.1.3 203 Kbps 839 KB 31
上位宛先
すべて表示
名前 レート バイト ヒット
10.0.1.1 110 Kbps 632 KB 6
52.98.37.34 61 Kbps 7 KB 2
40.126.12.227 7 Kbps 40 KB 3
162.125.34.129 5 Kbps 11 KB 2
40.90.190.179 5 Kbps 38 KB 5
13.107.136.9 4 Kbps 56 KB 3
8.8.8.8 2 Kbps 2 KB 5
52.114.158.50 2 Kbps 19 KB 2
40.108.227.49 1 Kbps 13 KB 1
40.91.74.57 840 bps 9 KB 1
システム
名前 T50-W-Kamiyacho46
モデル T50-W
バージョン 12.4.B589964
シリアル番号 70AF02A9669A2
システム時間 11:04 Asia/Tokyo
システム日付 2019-05-10
稼働時間 0 days 00:22
サーバー
Log Server 無効
DNSWatch 無効
Dimension 無効
WatchGuard Cloud
ステータス 無効
再起動
過去 20 分
外部帯域幅
512 Kbps
384 Kbps
256 Kbps
128 Kbps
0 Kbps
送信
受信
20 分前
現在

インターフェイスを設定するには、左側メニュー *ネットワーク* ー *インターフェイス* をクリックします。

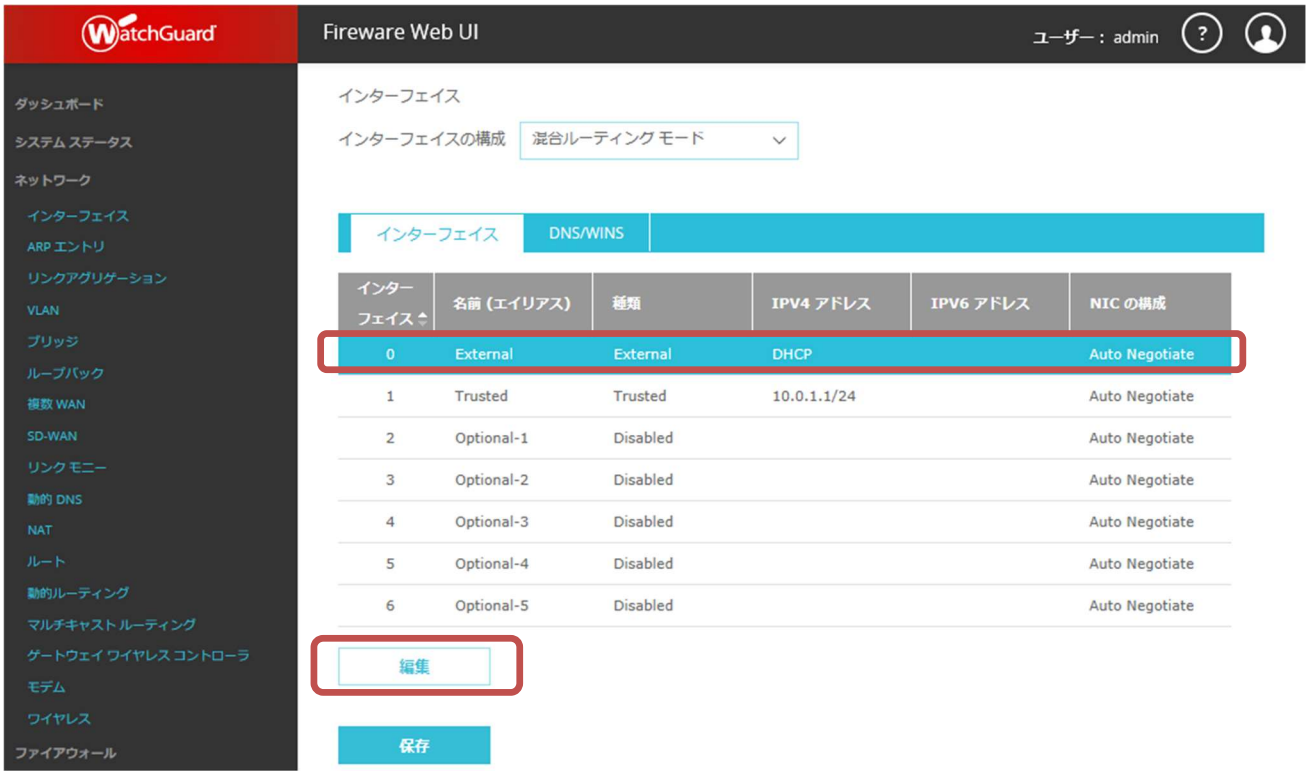


このネットワークインターフェイス画面から、各インターフェイスの設定ができます。

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。

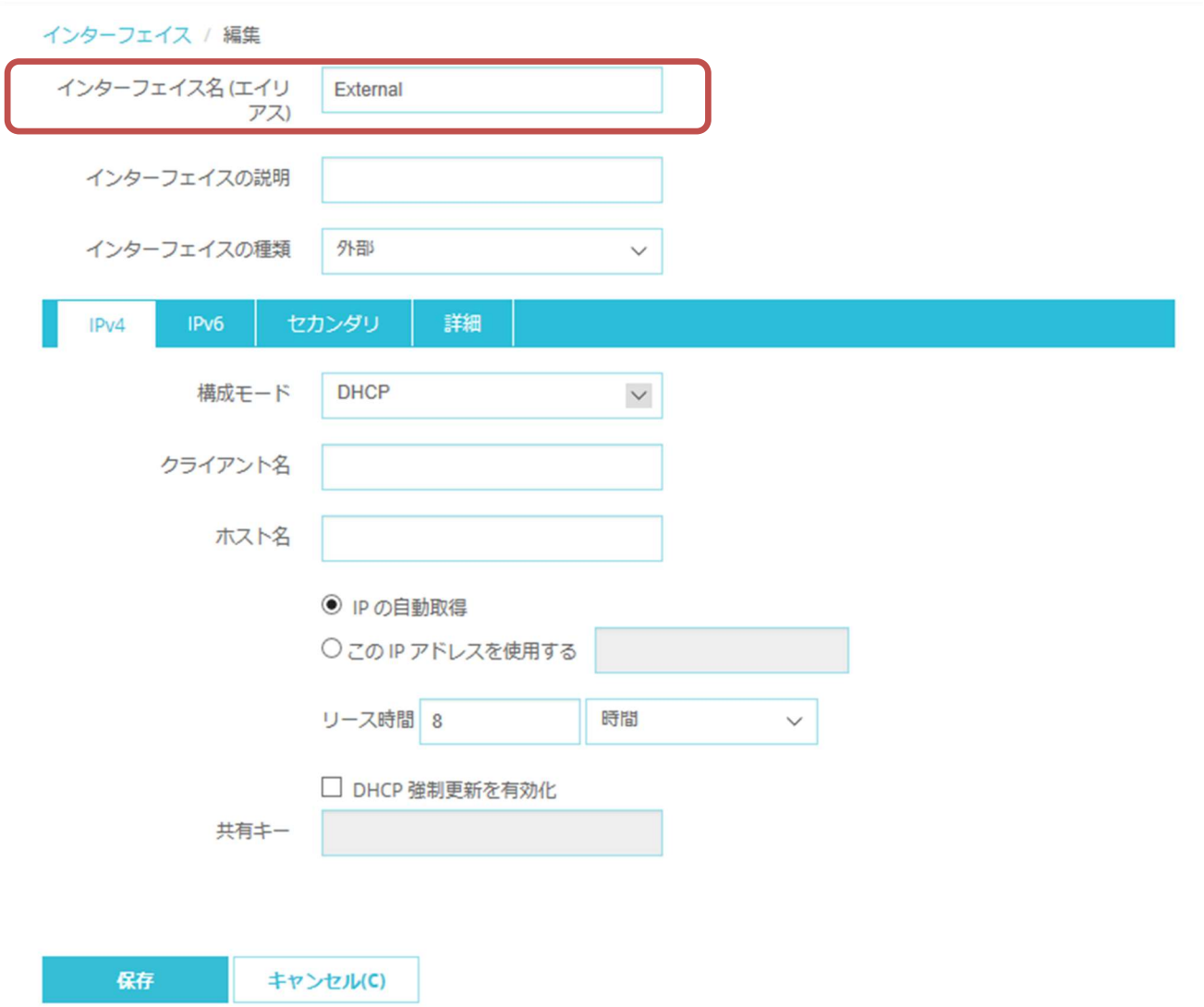
該当のインターフェイスを選択して、[編集] をクリックします。



次頁のように、インターフェイスの詳細を設定できる画面が開きます。

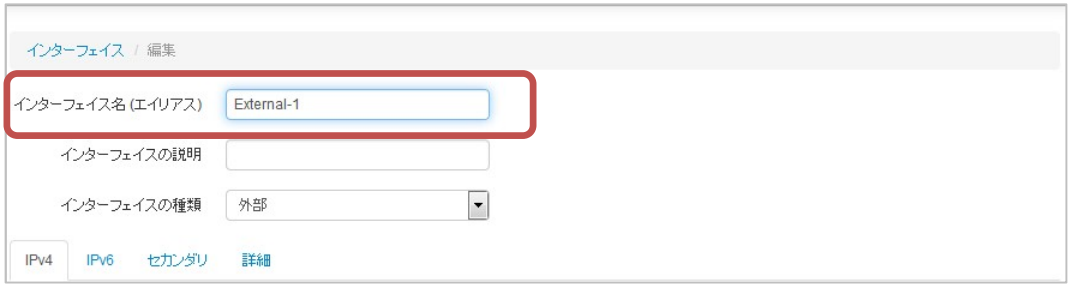
選択したインターフェイスの詳細設定画面になります。

最初にインターフェイス名を設定することができます。



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。[3]



[3] もちろんデフォルトのままでも問題ありません。

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。

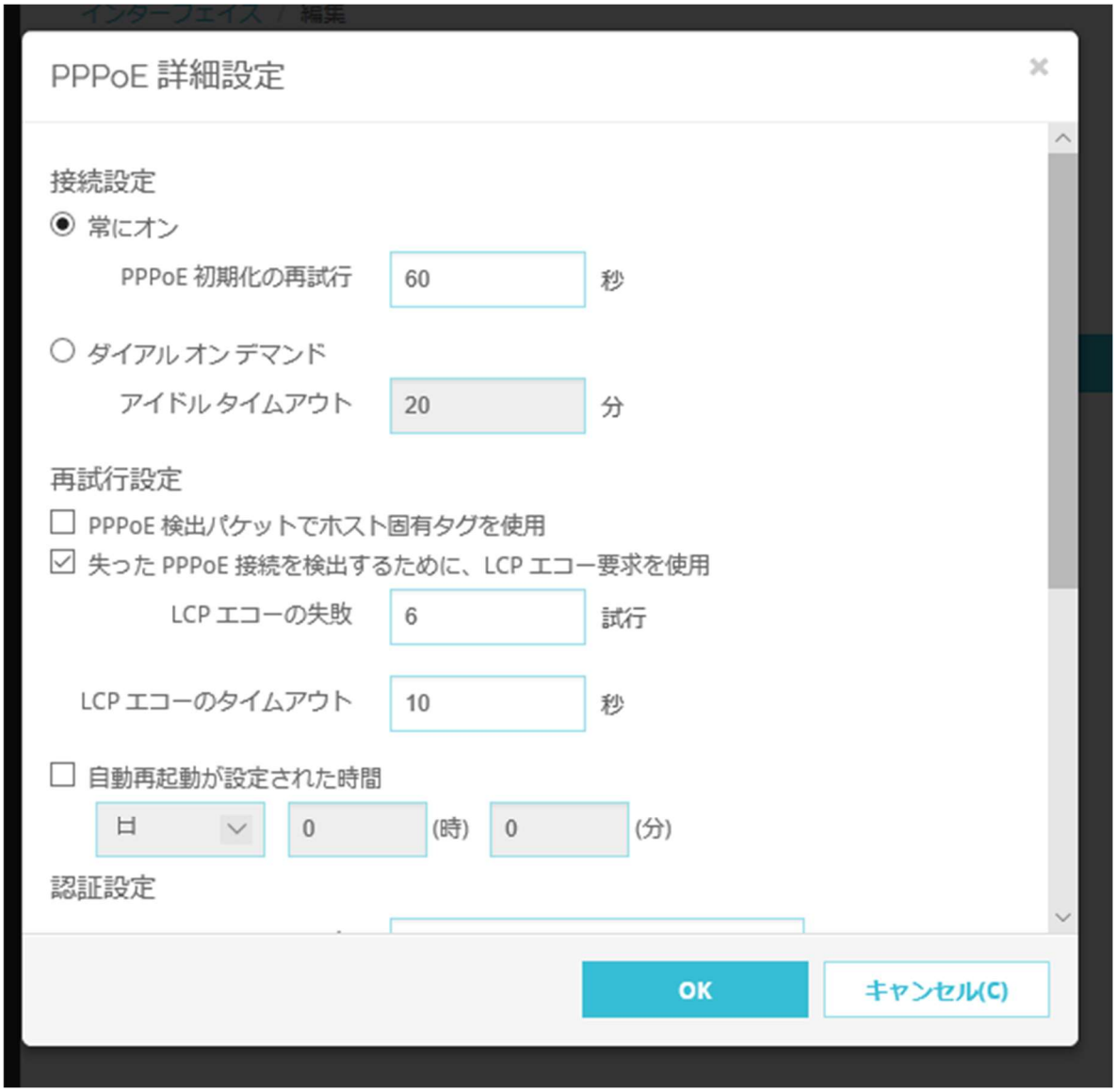
PPPoE の設定

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]ボタンをクリックし、ISP 指定の項目を設定してください。


インターフェイス / 編集
PPPoE 詳細設定
接続設定
常にオン
PPPoE 初期化の再試行
60
秒
ダイアル オン デマンド
アイドル タイムアウト
20
分
再試行設定
PPPoE 検出パケットでホスト固有タグを使用
失った PPPoE 接続を検出するために、LCP エコー要求を使用
LCP エコーの失敗
6
試行
LCP エコーのタイムアウト
10
秒
自動再起動が設定された時間
日
0
(時)
0
(分)
認証設定
OK
キャンセル(C)

DNS/WINS 設定

ネットワーク機器である Firebox 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。

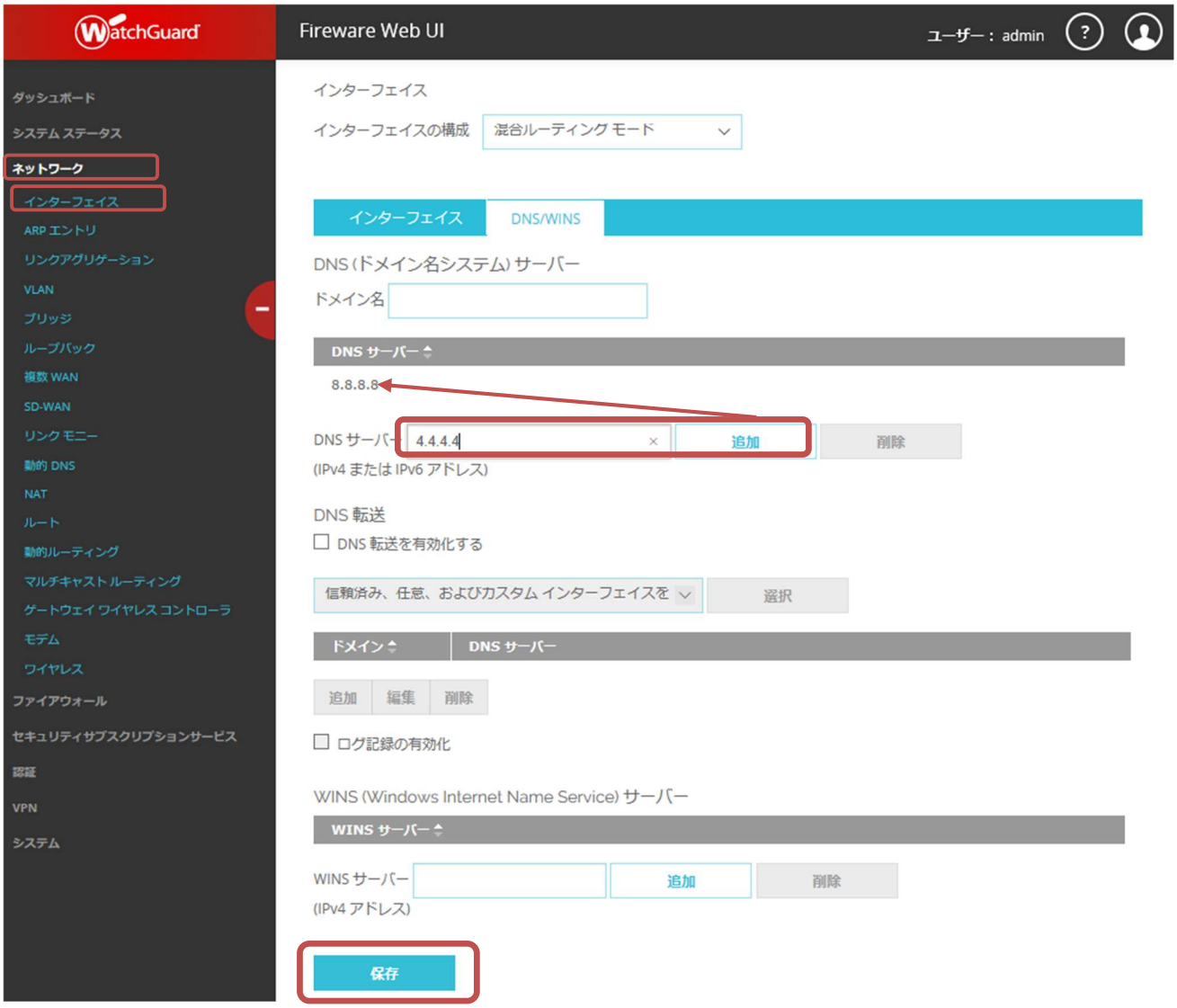
- ゲートウェイアンチウィルスや IPS のシグネチャ更新時の名前解決
- スパムブロッカーサーバーへの問い合わせの際の名前解決
- NTP サーバーを FQDN で設定した際の名前解決
- 拠点間 VPN でドメイン名を使用した場合の名前解決

※ 注意：Firebox 側で 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 Firebox の IP アドレスに指定しても名前解決しませんので注意してください

DNS の設定

左側メニューの*ネットワーク* － *インターフェイス*をクリックし、ネットワークインターフェイス画面のインターフェイス一覧を表示します。
DNS サーバーの欄に DNS サーバーのアドレスを入力し、[追加]ボタンをクリックします。するとドメイン名一覧に DNS サーバーが追加されます。

下方にある [保存] ボタンをクリックして設定を保存します。


WatchGuard
Fireware Web UI
ユーザー：admin
ダッシュボード
システム ステータス
ネットワーク
インターフェイス
ARP エントリ
リンクアグリゲーション
VLAN
ブリッジ
ループバック
複数 WAN
SD-WAN
リンク モニー
動的 DNS
NAT
ルート
動的ルーティング
マルチキャスト ルーティング
ゲートウェイ ワイヤレス コントローラ
モデム
ワイヤレス
ファイアウォール
セキュリティサブスクリプションサービス
認証
VPN
システム
インターフェイス
インターフェイスの構成
混合ルーティング モード
インターフェイス
DNS/WINS
DNS (ドメイン名システム) サーバー
ドメイン名
DNS サーバー
8.8.8.8
DNS サーバー
4.4.4.4
追加
削除
(IPv4 または IPv6 アドレス)
DNS 転送
DNS 転送を有効化する
信頼済み、任意、およびカスタム インターフェイスを
選択
ドメイン
DNS サーバー
追加
編集
削除
ログ記録の有効化
WINS (Windows Internet Name Service) サーバー
WINS サーバー
WINS サーバー
追加
削除
(IPv4 アドレス)
保存

WINS の設定

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

[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

Firebox 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、左側メニューの*ネットワーク* ー *インターフェイス* の画面から行ないます。

インターフェイス一覧より、設定したいインターフェイスを選択し、構成ボタンをクリックし、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。

ここでは Trusted-1 というインターフェイ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、インターフェイスの設定画面の中央にあるドロップダウンリストから、「DHCP サーバー」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 1xx の IP アドレスをクライアントに割り当てる設定をしています。

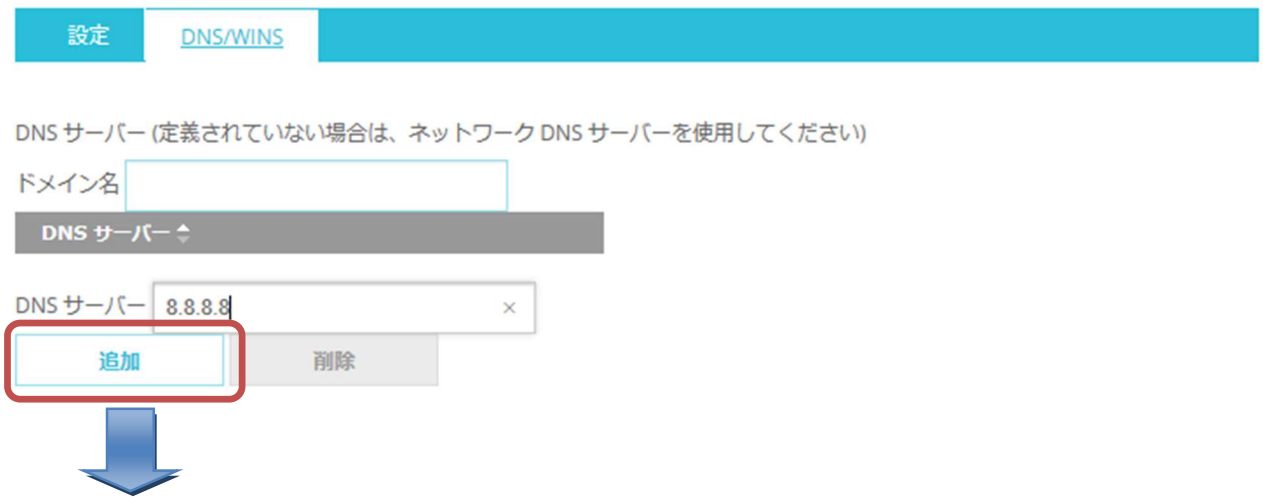
追加すると一覧に表示されます

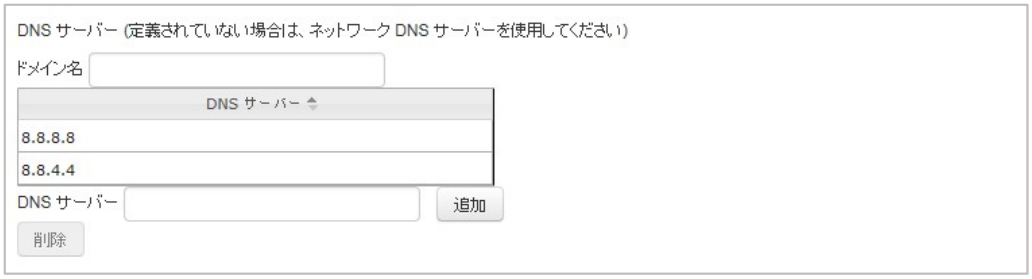
さらに、クライアントは IP アドレスだけでなく名前解決も必要なので、DNS サーバーの情報も配布します。

(次頁)

「DHCP サーバー」のドロップダウンリストの下の[DNS/WINS]のタブをクリックします。

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。

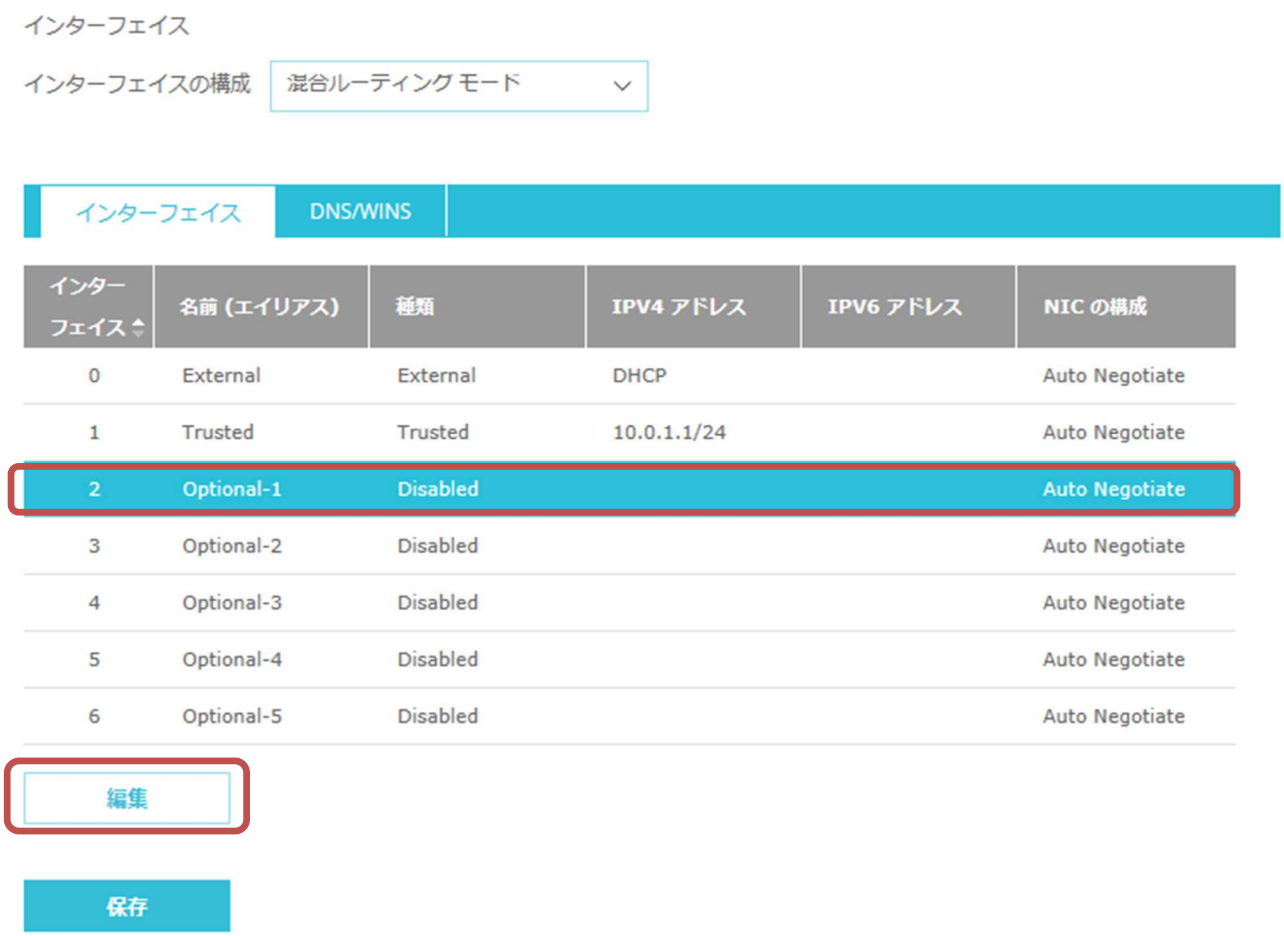
以上で DHCP サーバーが構成できました。

ブリッジの構成

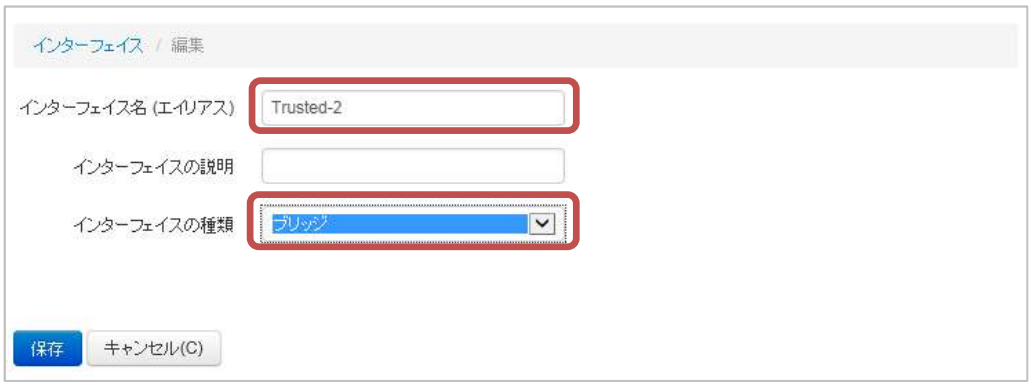
内部ネットワークを、空いているポートの数だけサブネットを分割しても、管理上複雑になる、クライアントの数がそれほどない、同じサブネットでポートを複数使用し負荷を分散させたい・・・といった場合、複数ポートをブリッジで束ねることができます。

例として 2, 3 番のインターフェイスをブリッジとして構成しましょう。

インターフェイス一覧の画面でブリッジにしたいものを選んで[編集]ボタンをクリックします。



インターフェイス名を入力し、インターフェイ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イスが、次のようにブリッジに変更されました。

残りのインターフェイスも同じように設定していきます。

以上で指定のインターフェイスをブリッジとして設定できました。

次にブリッジを定義します。左側メニュー *ネットワーク* - *ブリッジ* より、ブリッジの構成画面を開きます。

[追加]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、インターフェイスに設定する 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イ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」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、Firebox 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 インターフェイ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)

先程はブリッジの設定タブで設定作業をしましたが、その横の 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。[追加]ボタンをクリックします。

アドレス範囲の開始と終了 IP を入力し、[OK]をクリックします。

アドレスプールを追加したら、下にある DNS も追加します。DNS の IP アドレスを入力して[追加]ボタンをクリックします。


ブリッジ / ブリッジの設定の追加
ブリッジの設定
DHCP
セカンダリ
IPv6
ブリッジ プロトコル
DHCP モード
DHCP サーバー
ドメイン名
リース時間
8
時間
アドレス プール
開始 IP
終了 IP
10.0.1.100
10.0.1.199
追加
編集
削除
予約済みアドレス
IP アドレス
予約名
MAC ADDRESS
追加
編集
削除
DNS サーバー
DNS サーバー
10.100.100.101
10.100.100.102
追加
削除

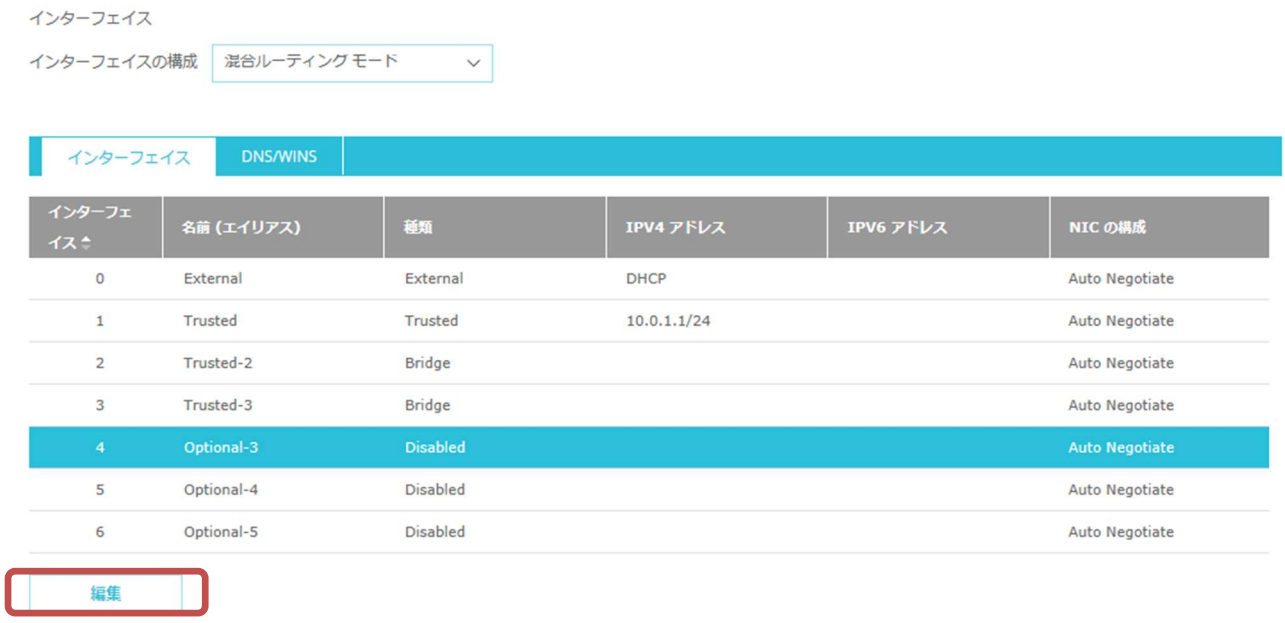
最後に[保存]ボタンをクリックし、設定を反映させます。

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。

インターフェイスの設定画面の「インターフェイスの種類」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。

Optional に設定したいインターフェイスを選択して[編集]をクリックします。



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

インターフェイス名と IP アドレスを設定しましょう

ここまでの設定でインターフェイスは以下のようになりました。

インターフェイス	名前 (エイリアス)	種類	IPV4 アドレス	IPV6 アドレス	NIC の構成
0	External	External	DHCP		Auto Negotiate
1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate
2	Trusted-2	Bridge			Auto Negotiate
3	Trusted-3	Bridge			Auto Negotiate
4	DMZ	Optional	10.0.4.1/24		Auto Negotiate
5	Optional-4	Disabled			Auto Negotiate
6	Optional-5	Disabled			Auto Negotiate

編集

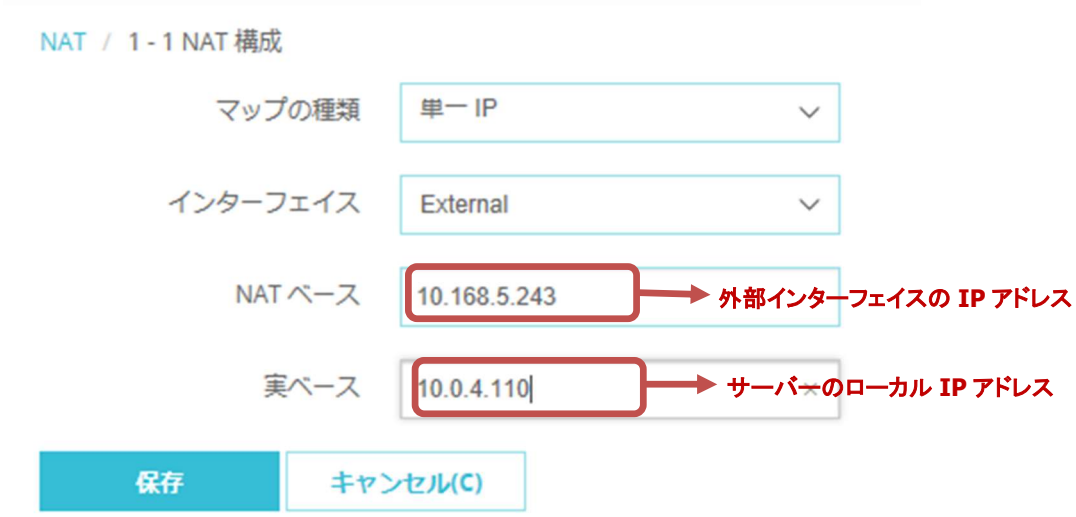
NAT 設定 (1-to-1NAT)

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」、インターフェイスは External を指定します。

NAT ベースには外部インターフェイスの 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。

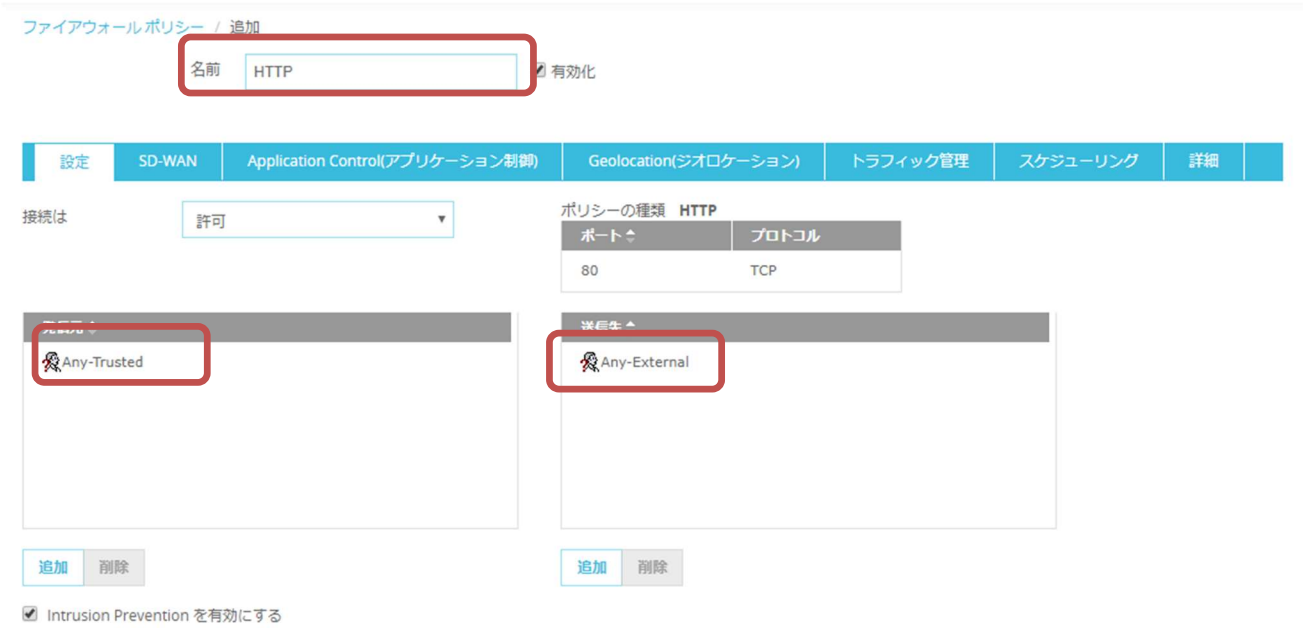
実際に 1-1 NAT を利用するには、ポリシーによって許可されている必要があります。

一例として Web サーバーを公開していて、HTTP のアクセスをこの DMZ にあるサーバーにリダイレクトするには以下のようにポリシーを追加します。

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、ポリシーの[追加]ボタンをクリックします。

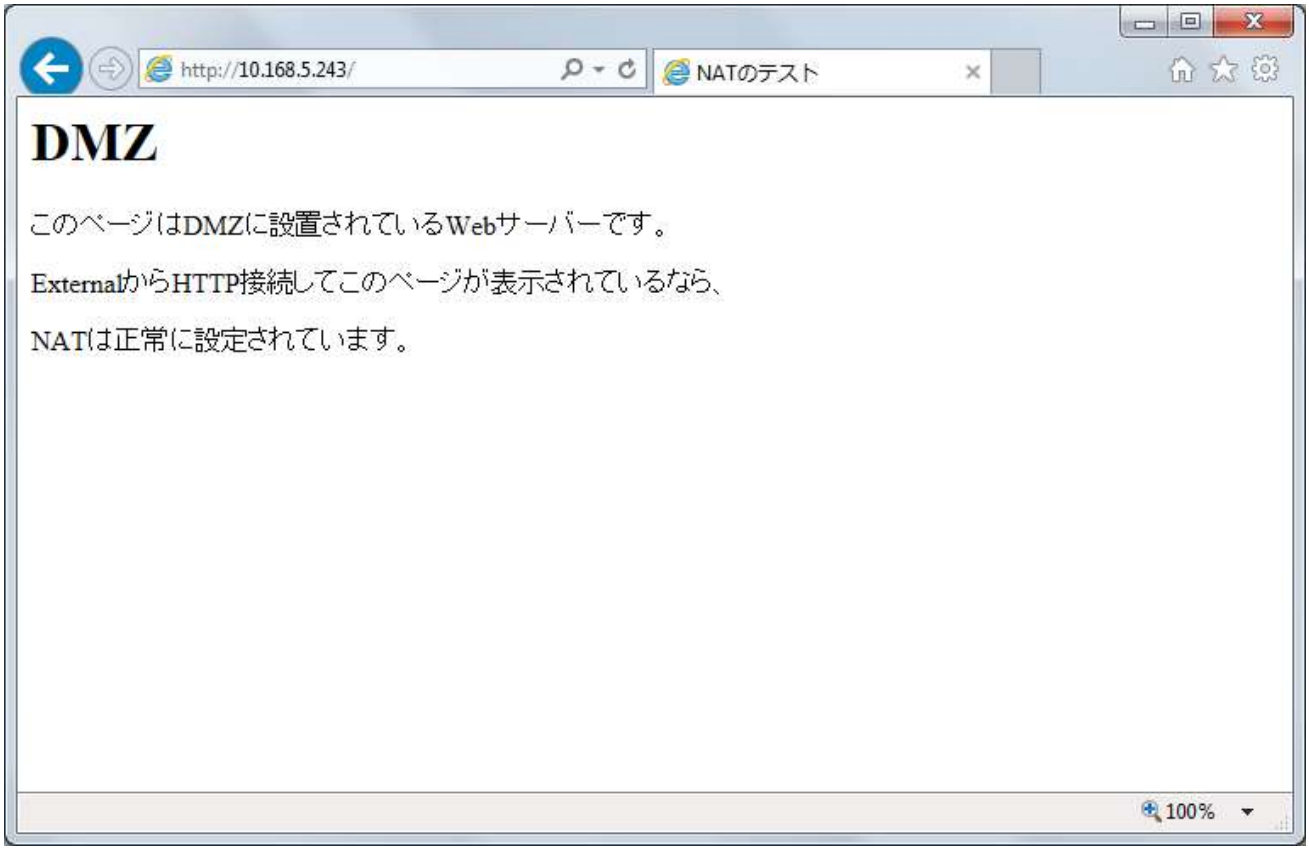
ポリシーの種類はパケットフィルタで HTTP を選択し、[ポリシーの追加]ボタンをクリックします。

次のポリシーの画面でポリシー名を入力、、発信元に Any-External、送信先に NAT ベースの IP アドレスを指定します。※画面の詳しい解説や発信元/送信先の追加削除の方法は、第四章で解説しています



設定が済んだら接続テストをしてみましょう。

ブラウザで External ポートにアクセスし、DMZ にある WEB サーバーのページを表示できれば 1-to-1 NAT の設定は成功です。(表示はテストページの例)



この他に、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。

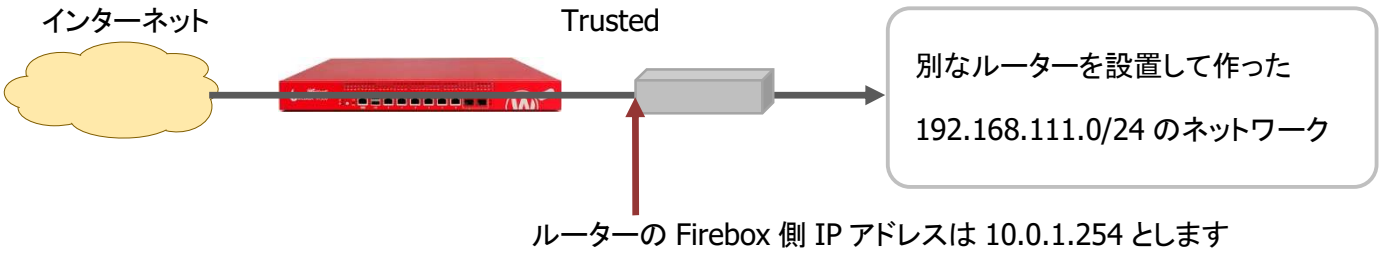
こちらはファイアウォールの章で取り上げます。

ルーティング設定

Firebox 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 Firebox 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：



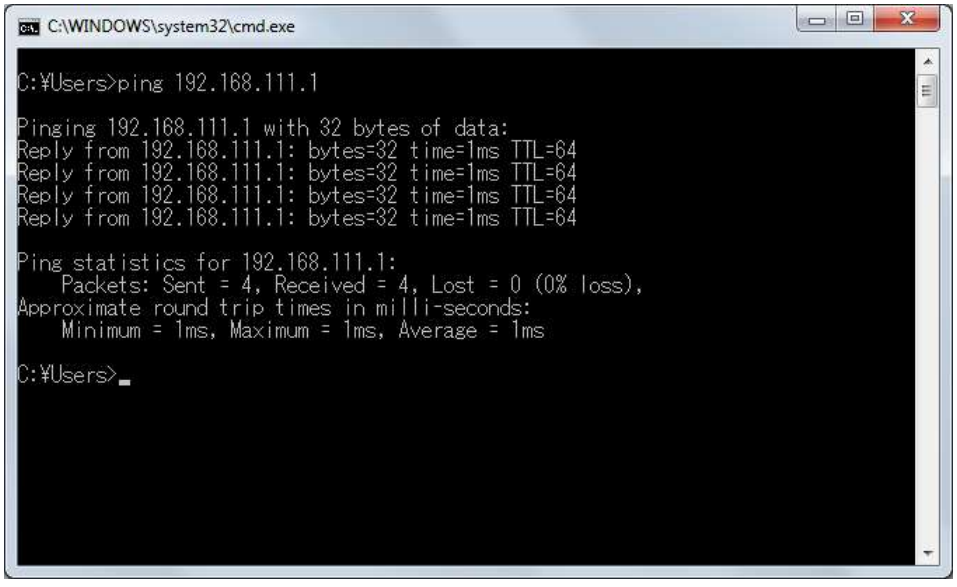
左側メニュー *ネットワーク* — *ルート* をクリックします。

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。

ping を実行して、ルートを追加したネットワークに疎通すれば OK です。



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 Firebox 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、先に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は以下のとおりです。

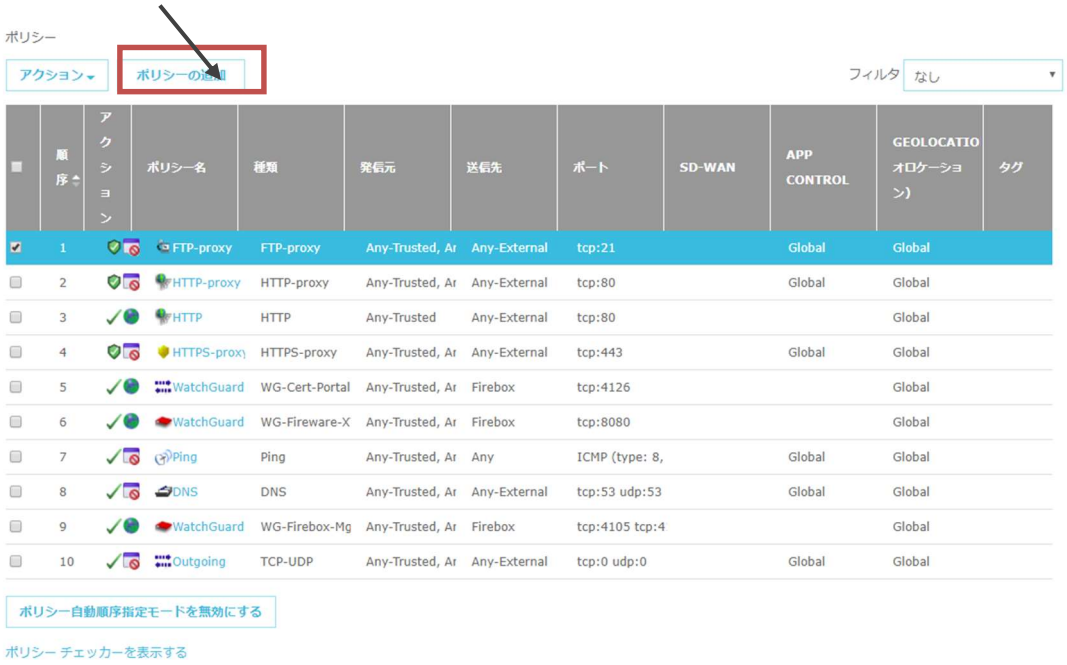
アクション	ポリシーの有効/無効、ログ記録、スケジュールなどが表示されます
ポリシー名	ポリシー作成時、任意で命名できます
種類	プロトコルまたは通信の種類です
送信元/送信先	送信元/先のエイリアス、IP/ネットワークアドレス、SNAT、ユーザーが表示されます
ポート	プロトコルとポート番号で表示されます。ポートの 0 はすべてのポート番号が対象です
App Control	アプリケーションコントロールの有効/無効が表示されます

ポリシーの変更/追加/保存

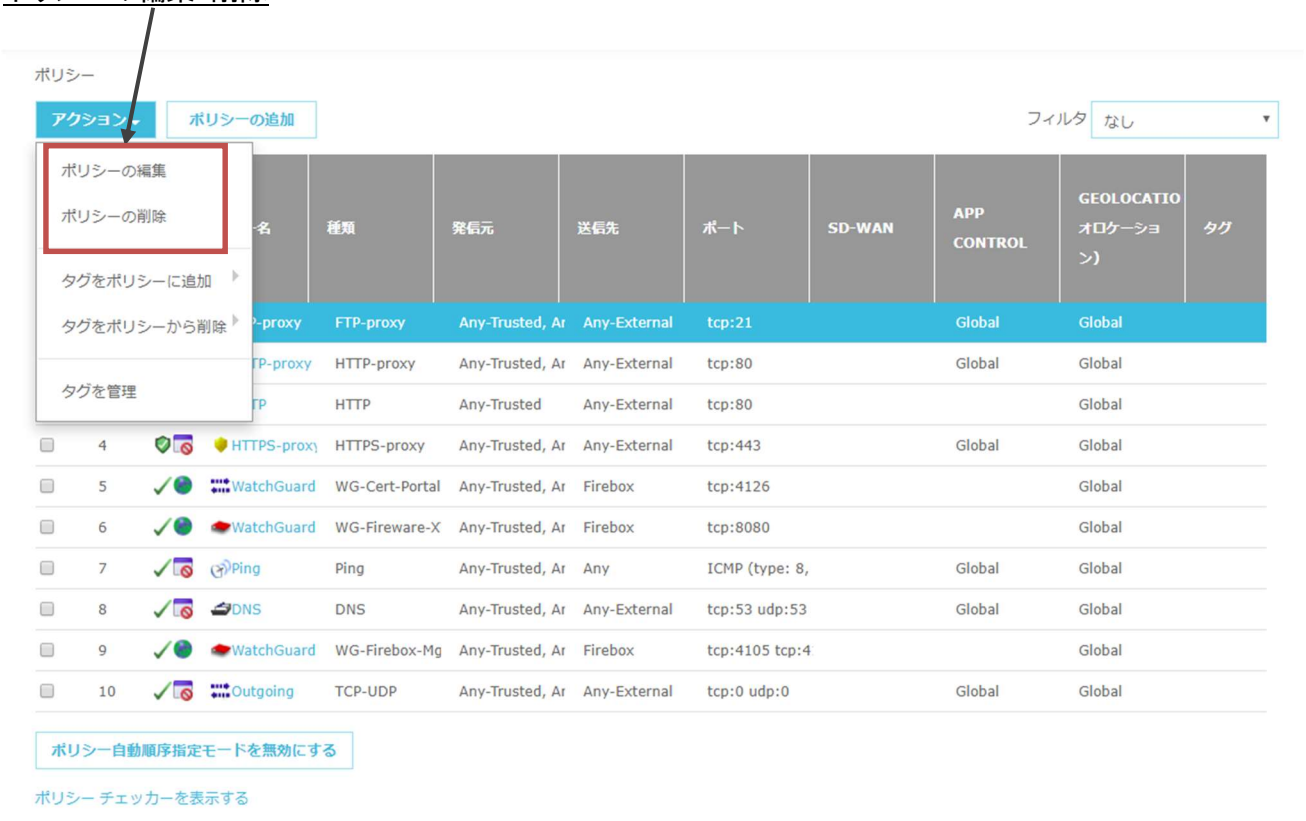
ポリシーの新規追加は、ポリシーの追加 ボタンをクリックします。

既存のポリシーを変更・削除するには、目的のポリシーをチェックして選択した上で、アクションボタンをクリックします。

ポリシーの追加



ポリシーの編集・削除



ポリシーの編集、もしくは削除をクリックします。

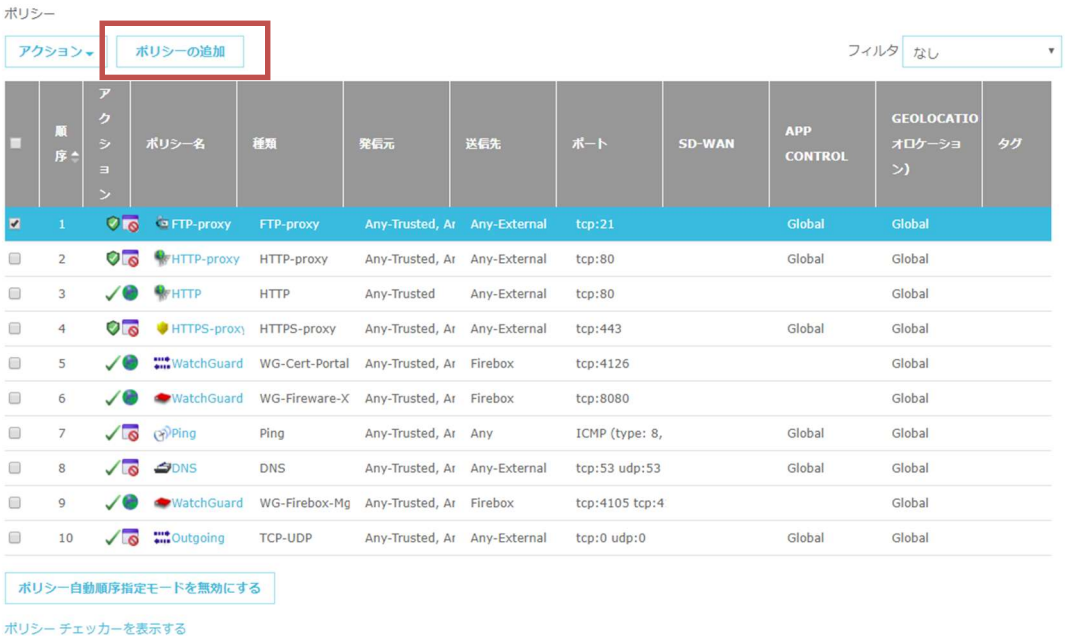
ポリシーの追加

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。

※ デフォルトでは「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。もし Outgoing を無効にして、許可する通信を手動で設定する場合などに必要です。



ポリシーの種類を選択します。

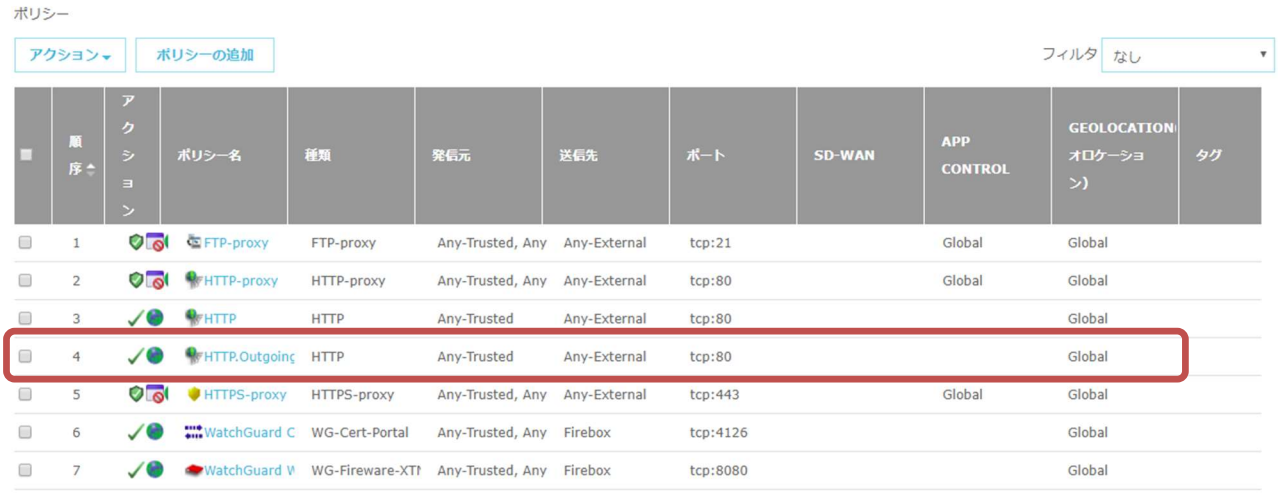
送信元と送信先を指定します。今回は内側から外側への許可ポリシーなのでデフォルトのままで結構です。

基本的には、ポリシーの設定項目は、どのプロトコルが許可/拒否か、どこから(From)どこに(To)対するルールかを明示します。最後に設定を反映させるため、下方にある[保存]ボタンをクリックします。

WebUI ではポリシー名は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)

設定が保存されるとポリシー一覧に戻ります。

設定したポリシーが表示されていることを確認してください。



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 10.0.4.110 とします。こちらは 1-1 NAT が設定されていることによって内部のサーバーにアドレス変換してアクセスが行なわれます。

前項と同じようにポリシーの追加画面で HTTP を選び、ポリシーの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。

送信元は Any-External、送信先は Web サーバーなので、送信元の Any-Trusted を削除します。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。

削除したら、隣にある[追加]ボタンをクリックします。メンバーの追加画面で Any-External を選択して[OK]をクリックします。

[追加]ボタンをクリック

発信元が Any-External になります。同様に送信先も削除して、設定し直します。

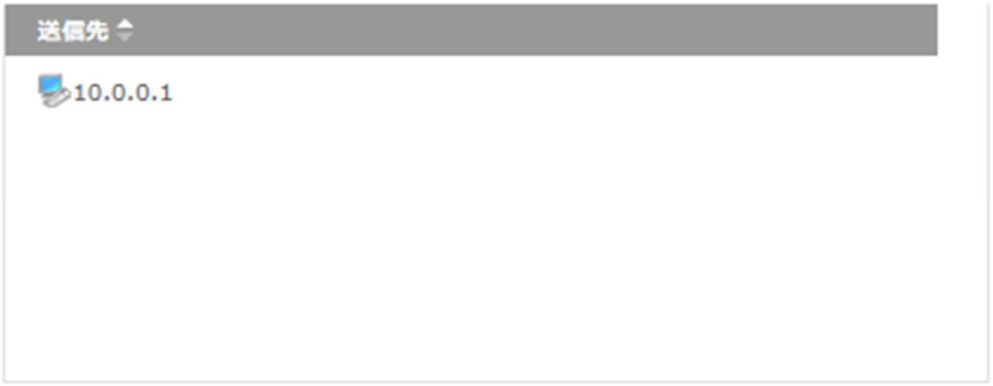
削除したら新しい送信先を追加します。[追加]ボタンをクリックします。

メンバーの追加画面では、メンバーの種類に ホスト IPv4 を選択します。

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

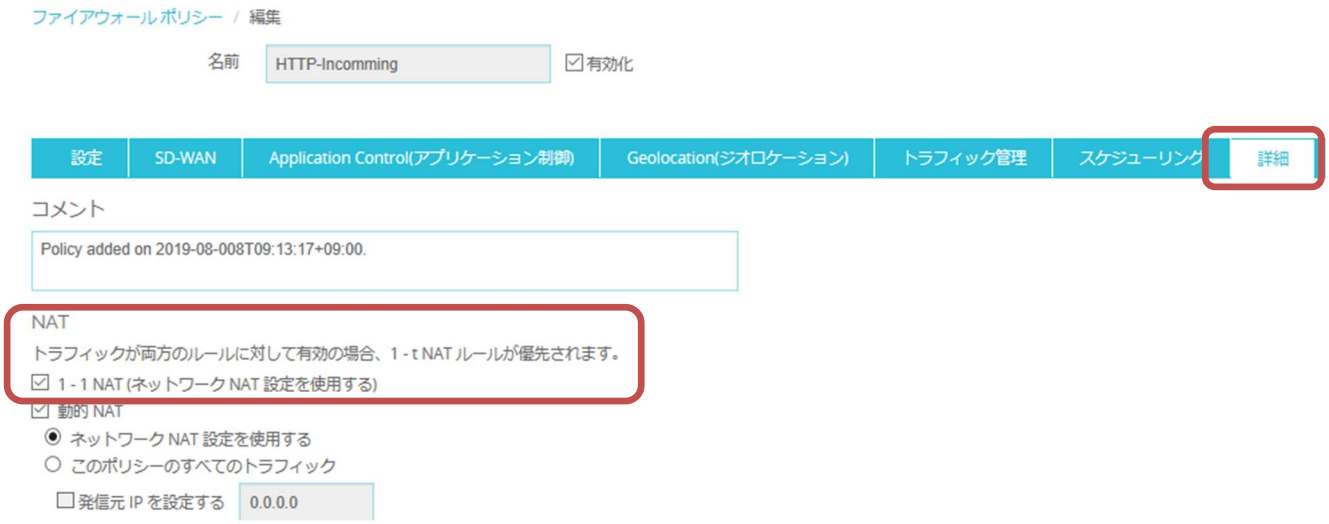
1-to-1 NAT でいう NAT ベースのアドレスを指定します。(Real ベースのアドレスではありません)

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。

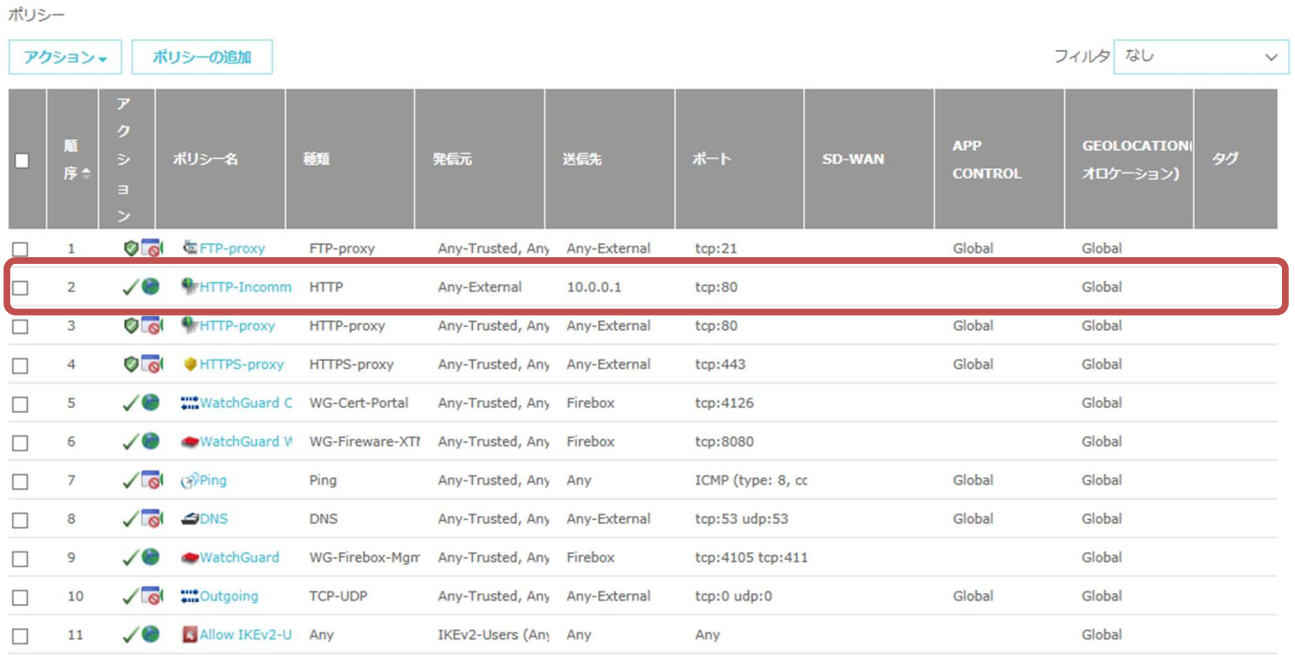


ではこの状態でなぜ内部のサーバーに NAT されるのでしょうか。

詳細タブを選択すると、下方に NAT の項目があり、デフォルトで 1-1 NAT が有効になるようにチェックが付いています。つまりあらかじめ設定しておいた 1-1 NAT の設定に合致するポリシーが存在する場合のみ、内部サーバーへのアドレス変換が行なわれます



OK で抜けて Policy Manager に戻ると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ています。



	順序	アクション	ポリシー名	種類	発信元	送信先	ポート	SD-WAN	APP CONTROL	GEOLOCATION(オロケーション)	タグ
☐	1		FTP-proxy	FTP-proxy	Any-Trusted, Any	Any-External	tcp:21		Global	Global	
☐	2		HTTP-Incomm	HTTP	Any-External	10.0.0.1	tcp:80			Global	
☐	3		HTTP-proxy	HTTP-proxy	Any-Trusted, Any	Any-External	tcp:80		Global	Global	
☐	4		HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any	Any-External	tcp:443		Global	Global	
☐	5		WatchGuard C	WG-Cert-Portal	Any-Trusted, Any	Firebox	tcp:4126			Global	
☐	6		WatchGuard W	WG-Fireware-XTI	Any-Trusted, Any	Firebox	tcp:8080			Global	
☐	7		Ping	Ping	Any-Trusted, Any	Any	ICMP (type: 8, cc		Global	Global	
☐	8		DNS	DNS	Any-Trusted, Any	Any-External	tcp:53 udp:53		Global	Global	
☐	9		WatchGuard	WG-Firebox-Mgm	Any-Trusted, Any	Firebox	tcp:4105 tcp:411			Global	
☐	10		Outgoing	TCP-UDP	Any-Trusted, Any	Any-External	tcp:0 udp:0		Global	Global	
☐	11		Allow IKEv2-U	Any	IKEv2-Users (Any	Any	Any			Global	

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。
名前の入力後、NAT のメンバーを作成するため、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、種類は内部 IP アドレスを選択し、ホストは Web サーバーの 10.0.4.110 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)

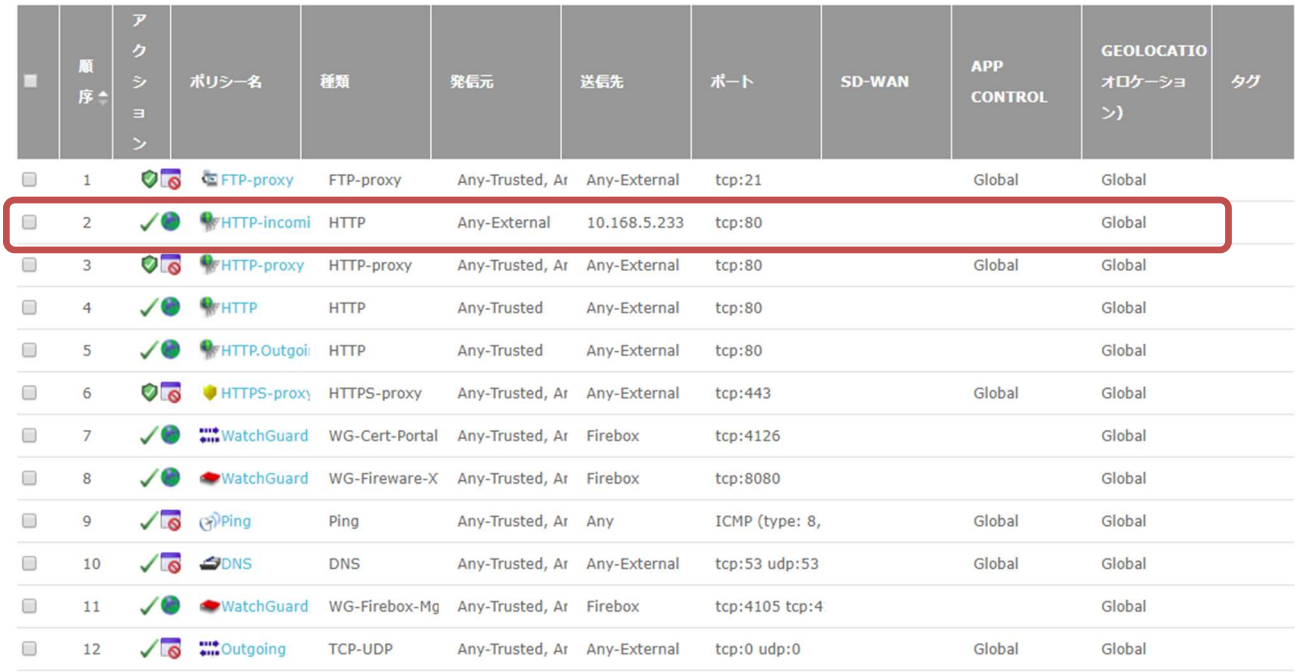
OK ボタンをクリックすると SNAT の追加画面に戻り、SNAT メンバーが追加されたことを確認できます。

[保存]ボタンをクリックして設定を反映させます。

SNAT が追加されました。

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。

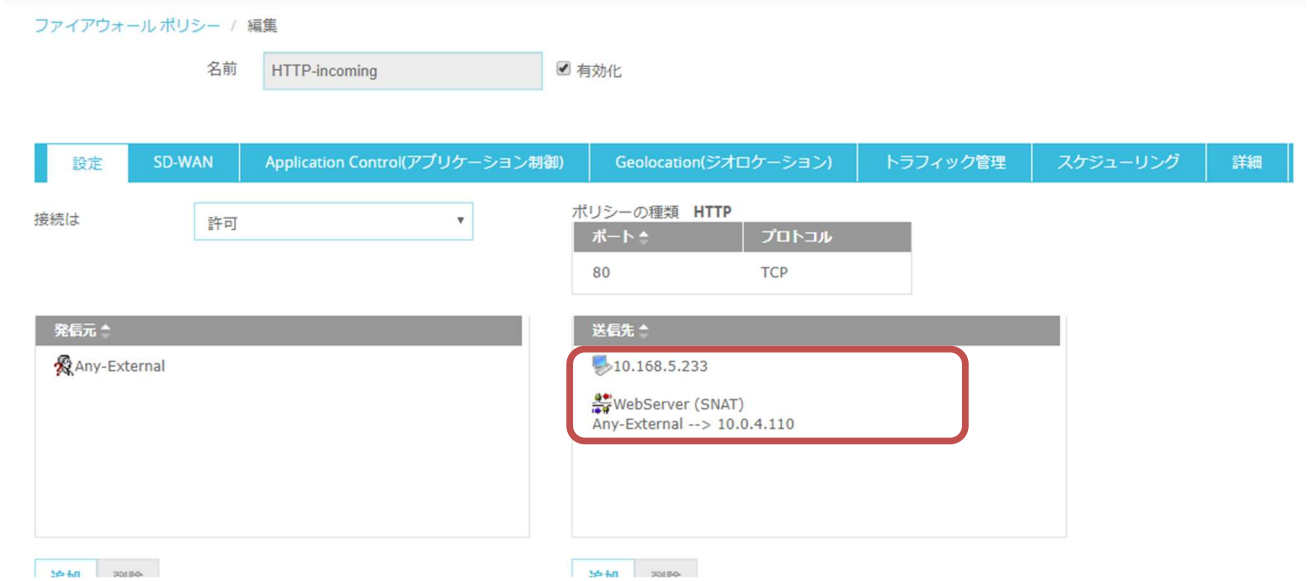
HTTP-Incoming ポリシーをクリックして編集します。



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。

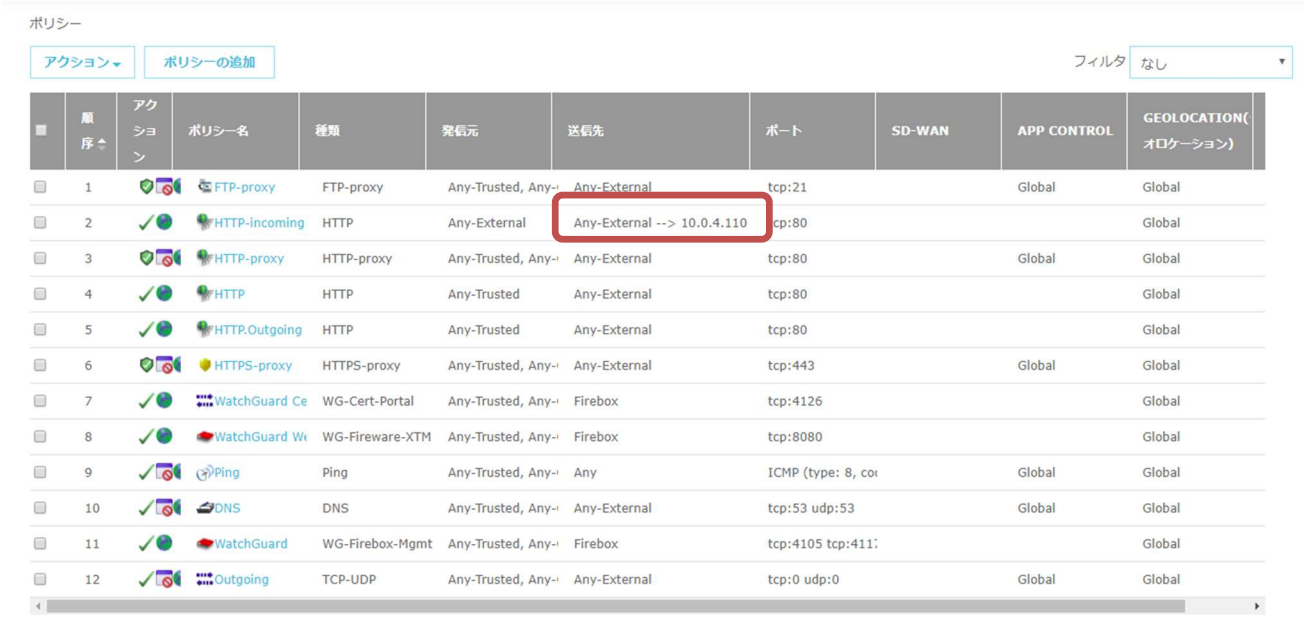
事前に定義した SNAT を選択し、[OK]ボタンをクリックします。

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。

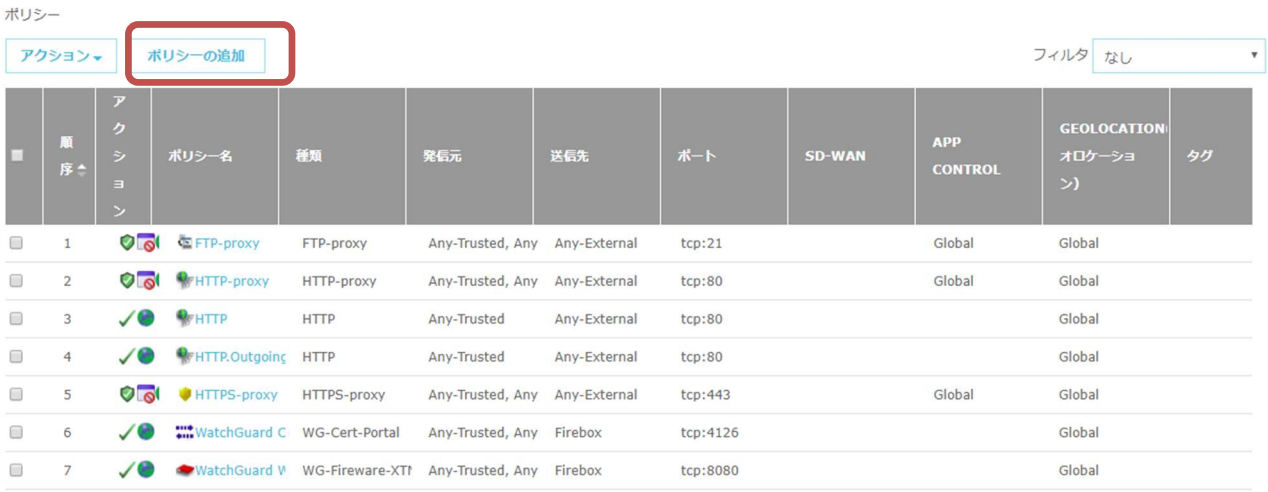


テンプレートにないポリシーを追加する

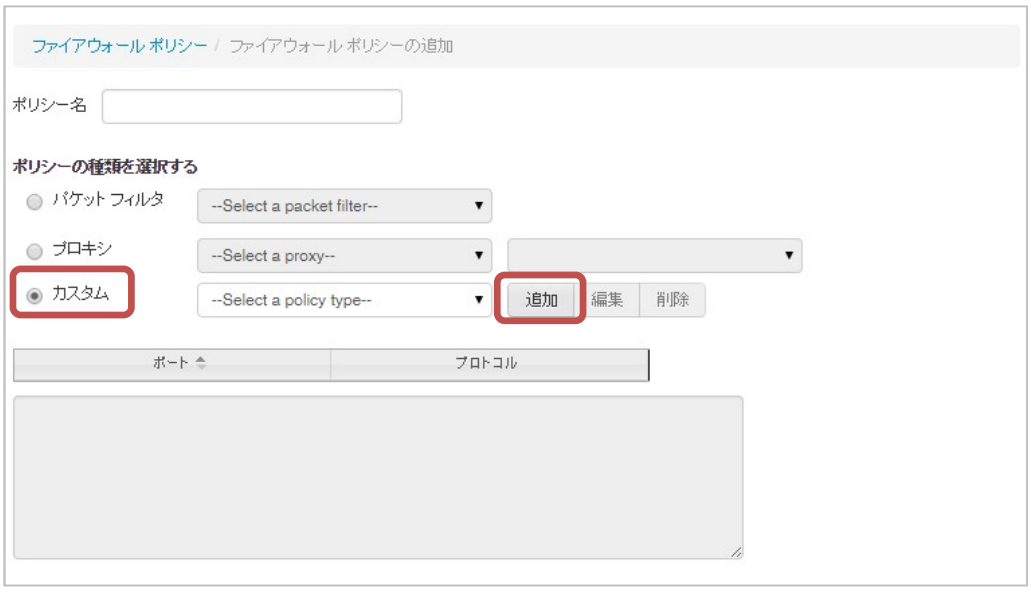
ポリシーの追加画面では、パケットフィルタのプロトコルテンプレートを元にポリシーを作成しました。しかし、内製の社内システムで使うポート番号での通信を制御する場合など、独自のポリシーを作成しなければならないことがあります。

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[ポリシーの追加]ボタンをクリックします。



次の画面でポリシーの種類を「カスタム」を選択し、[追加]ボタンをクリックします。



新しいポリシーの名前を入力します。

そしてプロトコル(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。

これで新しいテンプレートとして登録されます。

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。

ポリシーの種類をカスタムにし、作成した名前のポリシーテンプレートを選んで追加します。

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

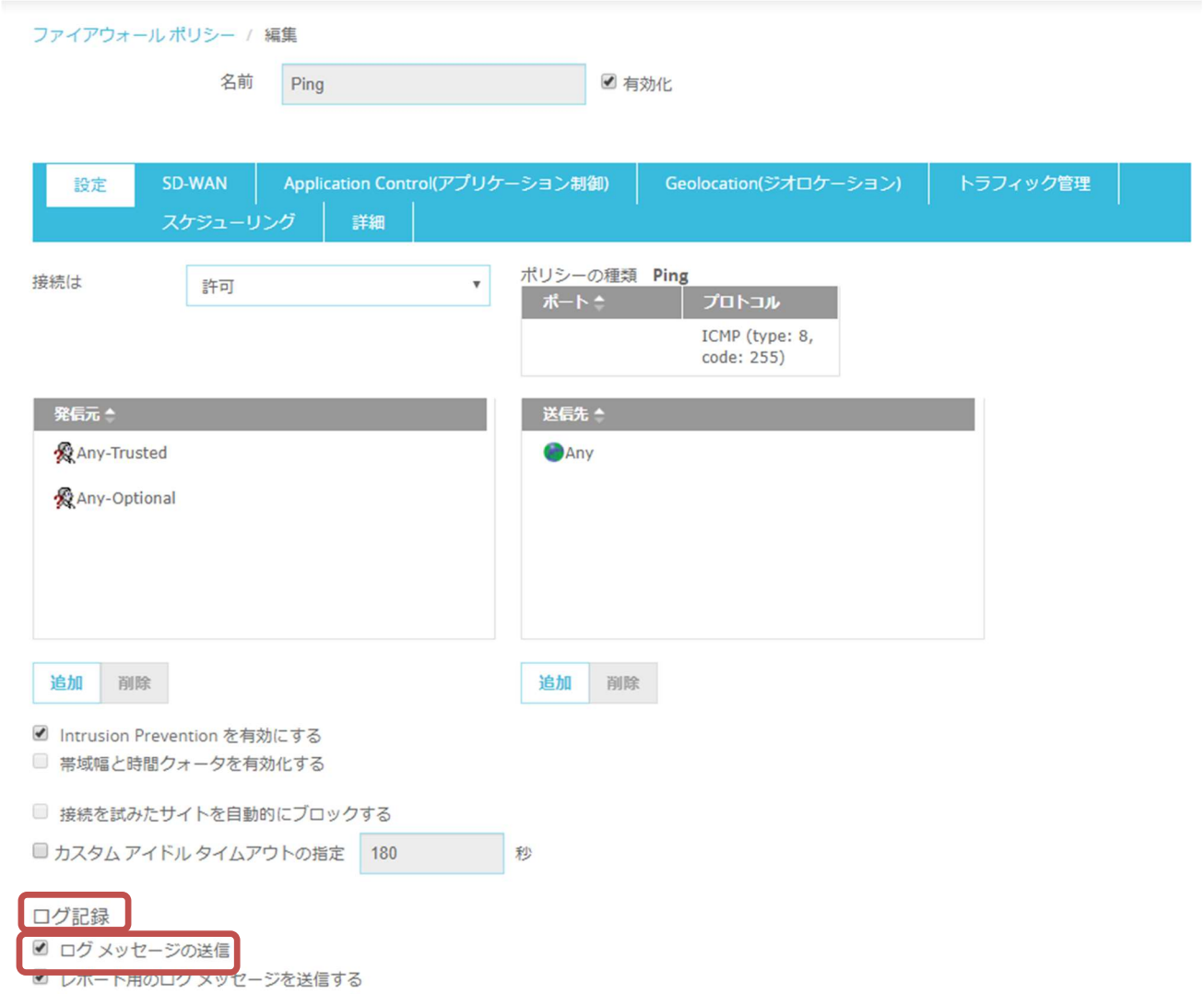
特定のポリシーを一時的に効かせないようにするには、削除するのではなく、一時的に無効にすることができます。ポリシーのプロパティ画面の右上にある、有効のチェックを外します。

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。

ログで確認したい場合は、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。

※ログサーバーは別途設定が必要です。詳しくは「ログ&レポート設定ガイド」でご確認ください

運用スケジュールを設定する

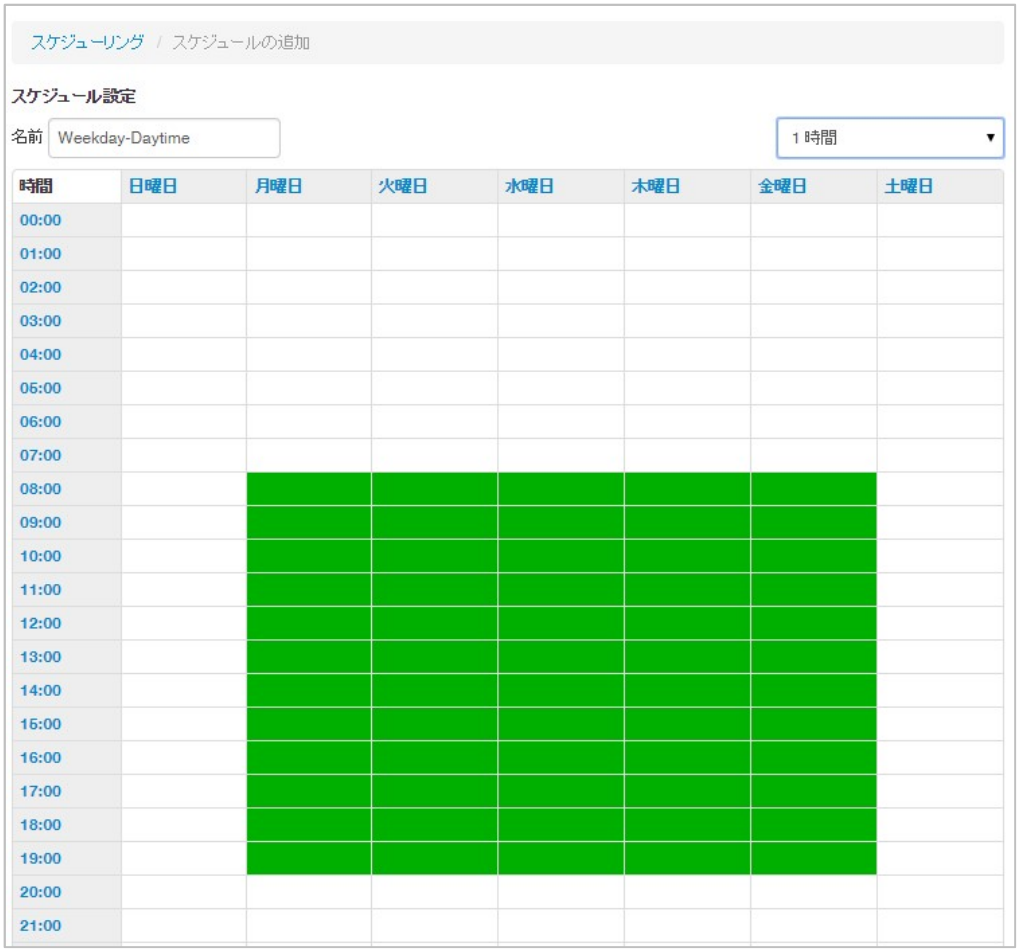
指定の時間にのみポリシーが有効となるように、ポリシーの運用スケジュールを設定することができます。

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。

週中の日中帯のみ適用したい場合、以下のようにドラッグして緑色に反転させます。

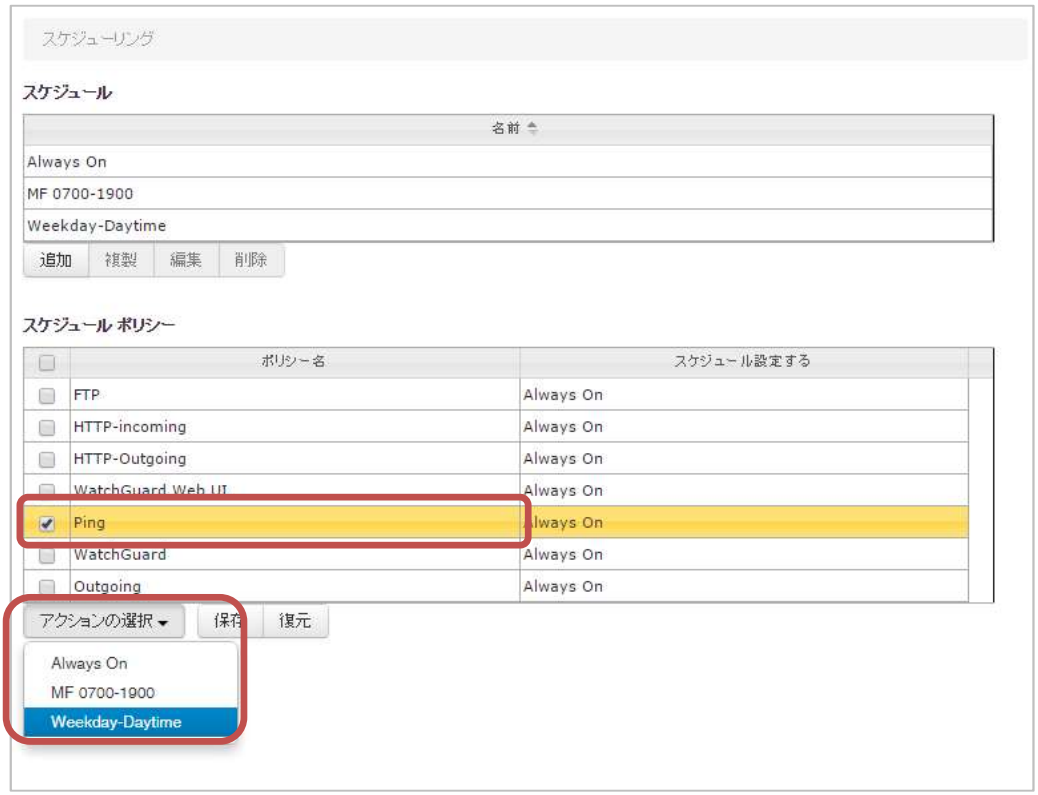
名前にはスケジュールの内容が分かるようなスケジュール名を入力します。



右上の時間単位を 1 時間にして色を反転させ、微調整が必要なら 30 分または 15 分に切り替えると楽にできます。

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ポリシーで適用したいポリシーにチェックを入れ、アクションの選択 ドロップダウンリストから、作成したスケジュールを選択します。



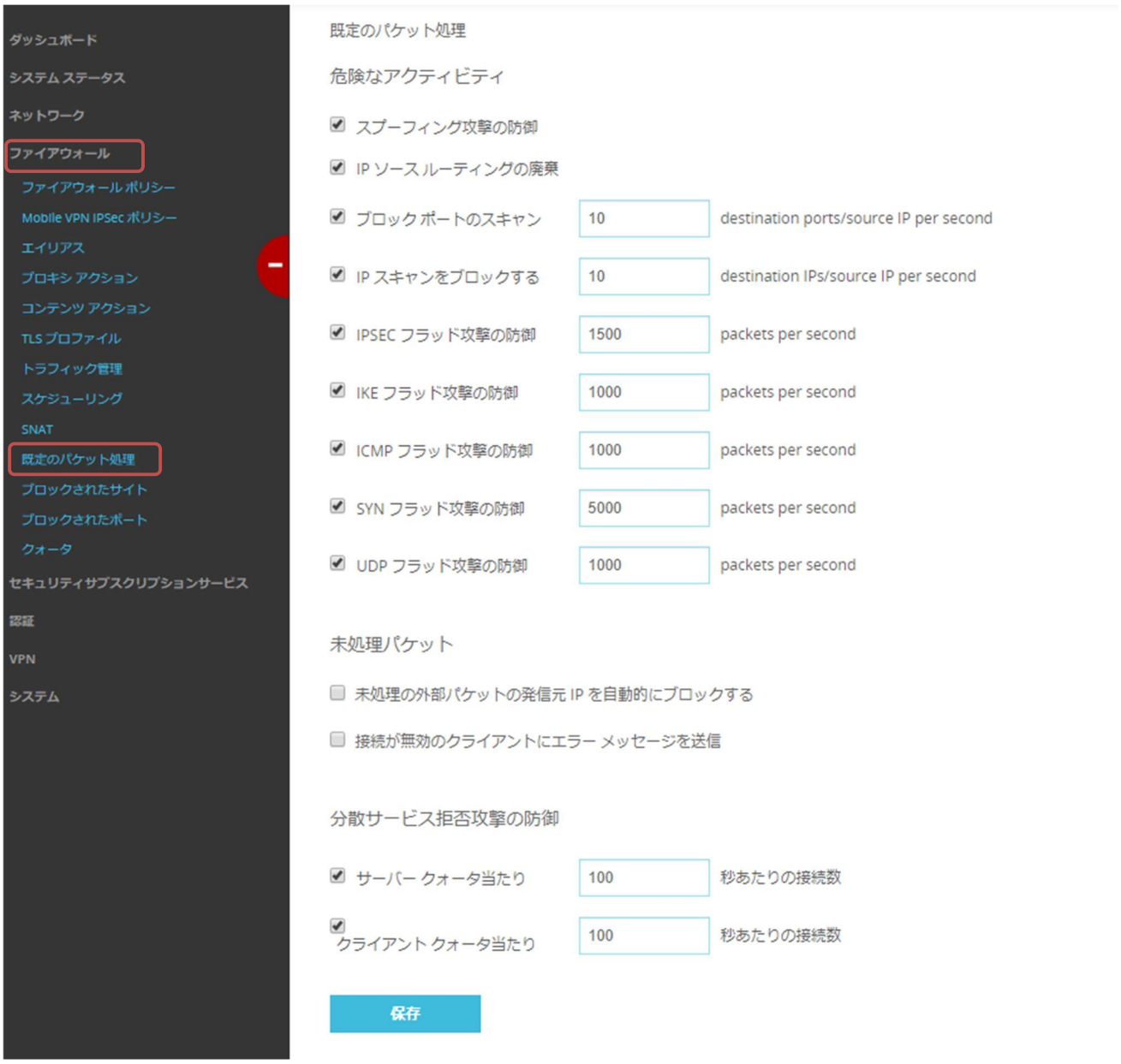
適用するスケジュールが設定されますので、保存ボタンをクリックして有効にします。

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。

Firebox 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、そのサイトへの通信をブロックすることができます。テキストファイル1行に1サイトを記述してファイルからインポートすることもできます。

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

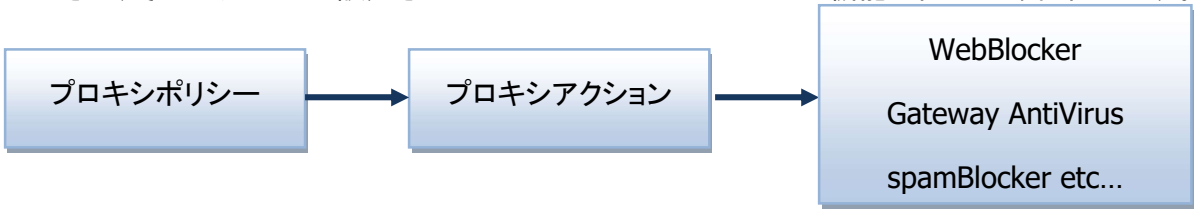
アンチウイルスやコンテンツフィルタリングなど、アプリケーションレベルの様々な脅威に対し、総合的に対応するセキュリティ機能を UTM (Unified Threat Management)といいます。

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 AntiVirus、spamBlocker の設定方法を解説します。

プロキシポリシーの追加

UTM といっても、設定自体はファイアウォールポリシーと同様、プロキシポリシーの追加という形で行ないます。

ファイアウォールポリシーと違う点としては、プロキシポリシーが適用されると紐づいたプロキシアクションが呼び出され、そのアクションで設定された WebBlocker や AntiVirus の機能が働くという仕組みです。



ですので、UTM を設定にするには、1.プロキシアクションを定義し、 2.プロキシポリシーを追加し、 3.各種セキュリティ機能の詳細を設定していく、という手順になります。

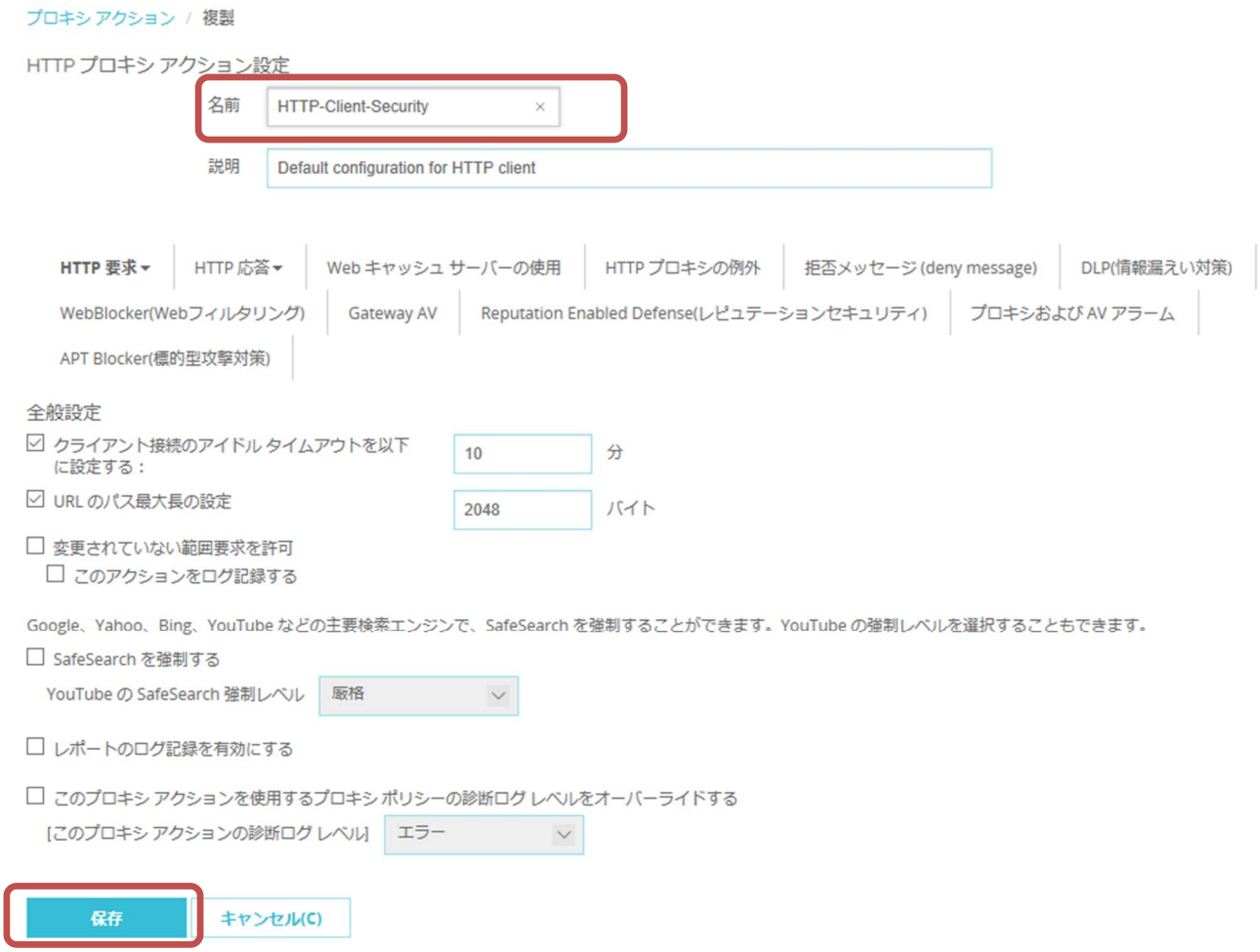
プロキシアクションの追加

ファイアウォール ー *Proxy アクション* をクリックします。そして、HTTP プロトコルで UTM を有効にしたい場合は 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 アクションの詳細設定画面になります。

まずはアクションの内容を表わす名前を入力します。

名前を入力したら、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。



保存すると、プロキシアクション一覧に戻ります。

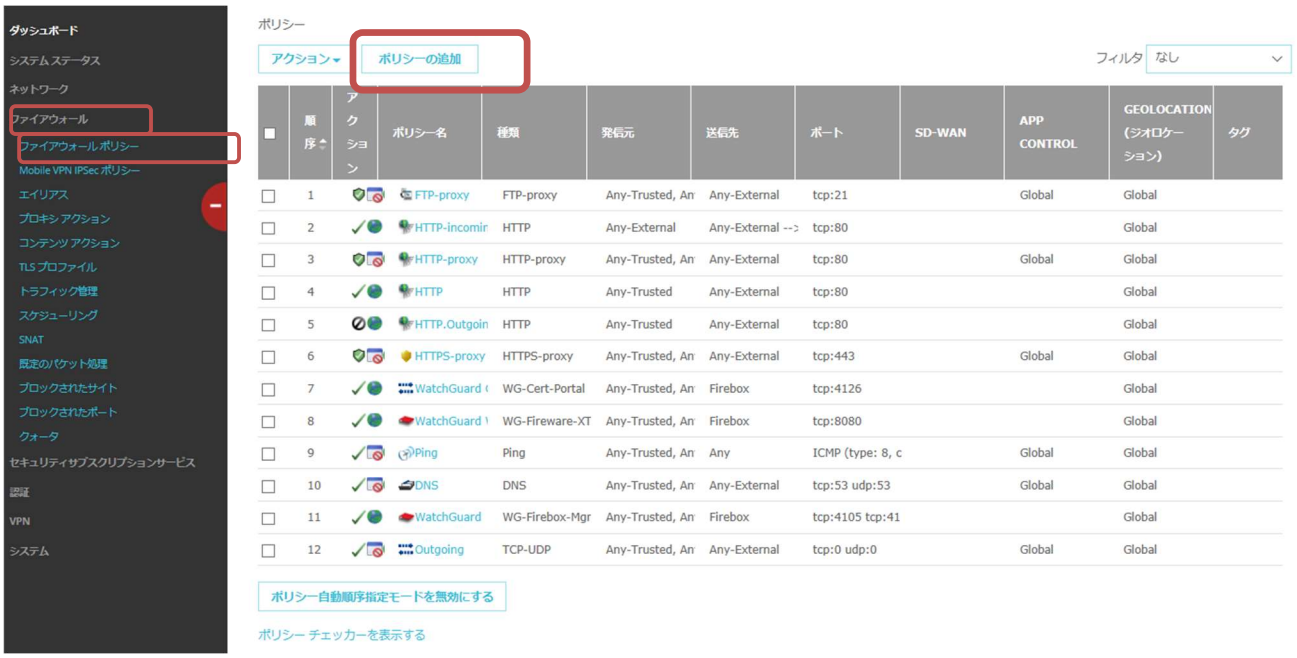
一覧には事前定義済みのアクションの他に、新しく定義したアクションが加わりました。

プロキシ	種類
DNS-Incoming（事前定義済）	DNS
DNS-Outgoing（事前定義済）	DNS
FTP-Client（事前定義済）	FTP
FTP-Client.Standard（事前定義済）	FTP
FTP-Server（事前定義済）	FTP
FTP-Server.Standard（事前定義済）	FTP
H.323-Client（事前定義済）	H323
HTTP-Client（事前定義済）	HTTP
HTTP-Client-Security	HTTP
HTTP-Client.Standard（事前定義済）	HTTP
HTTP-Server（事前定義済）	HTTP
HTTP-Server.Standard（事前定義済）	HTTP
HTTPS-Client（事前定義済）	HTTPS
HTTPS-Client.Standard（事前定義済）	HTTPS
HTTPS-Server（事前定義済）	HTTPS

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 ー *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。

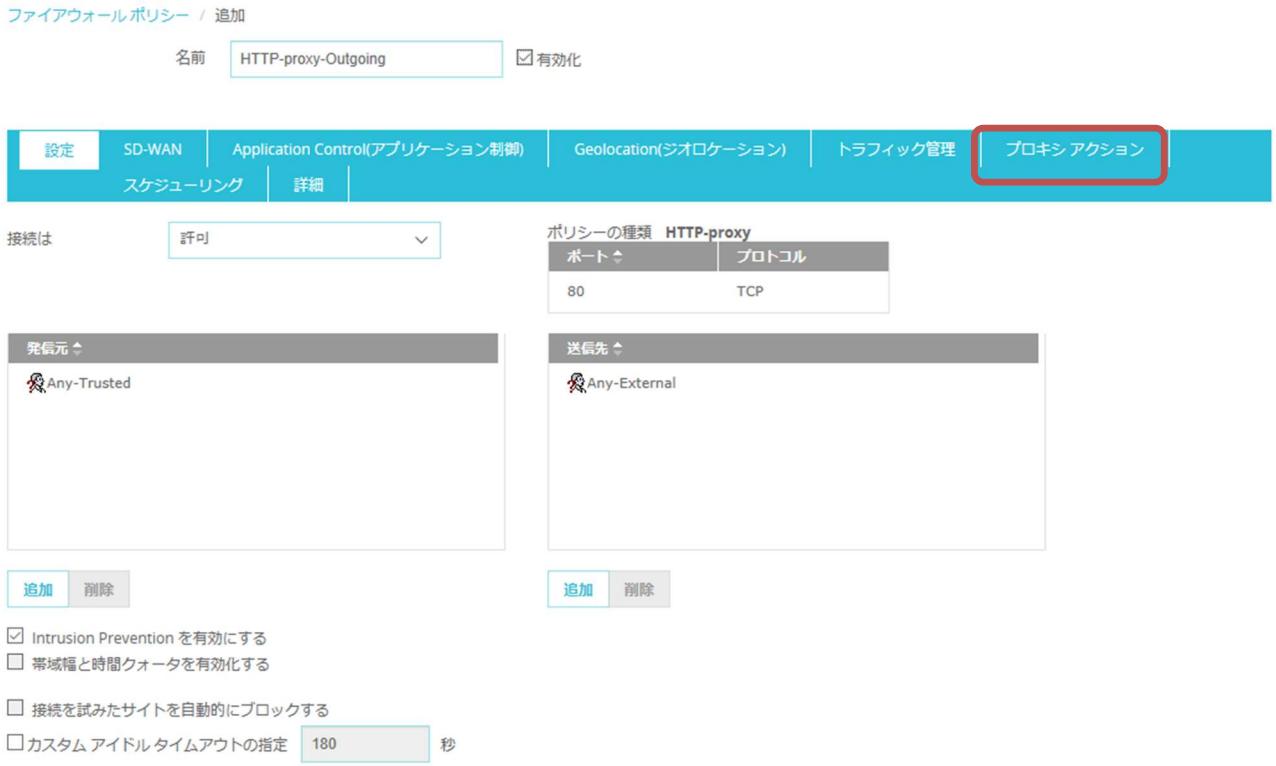


UTM を設定する場合は「プロキシ」にチェックを入れ、プロトコル(今回は HTTP-proxy)を選択します。

右隣りのプロキシアクションの欄では、あらかじめ作成したプロキシアクションを選択します。

最後に[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、ポリシーの構成画面になります。ポリシー名は分かりやすいものを任意に入力してください。
ファイアウォールとプロキシの違いは、「プロキシ　アクション」タブです。



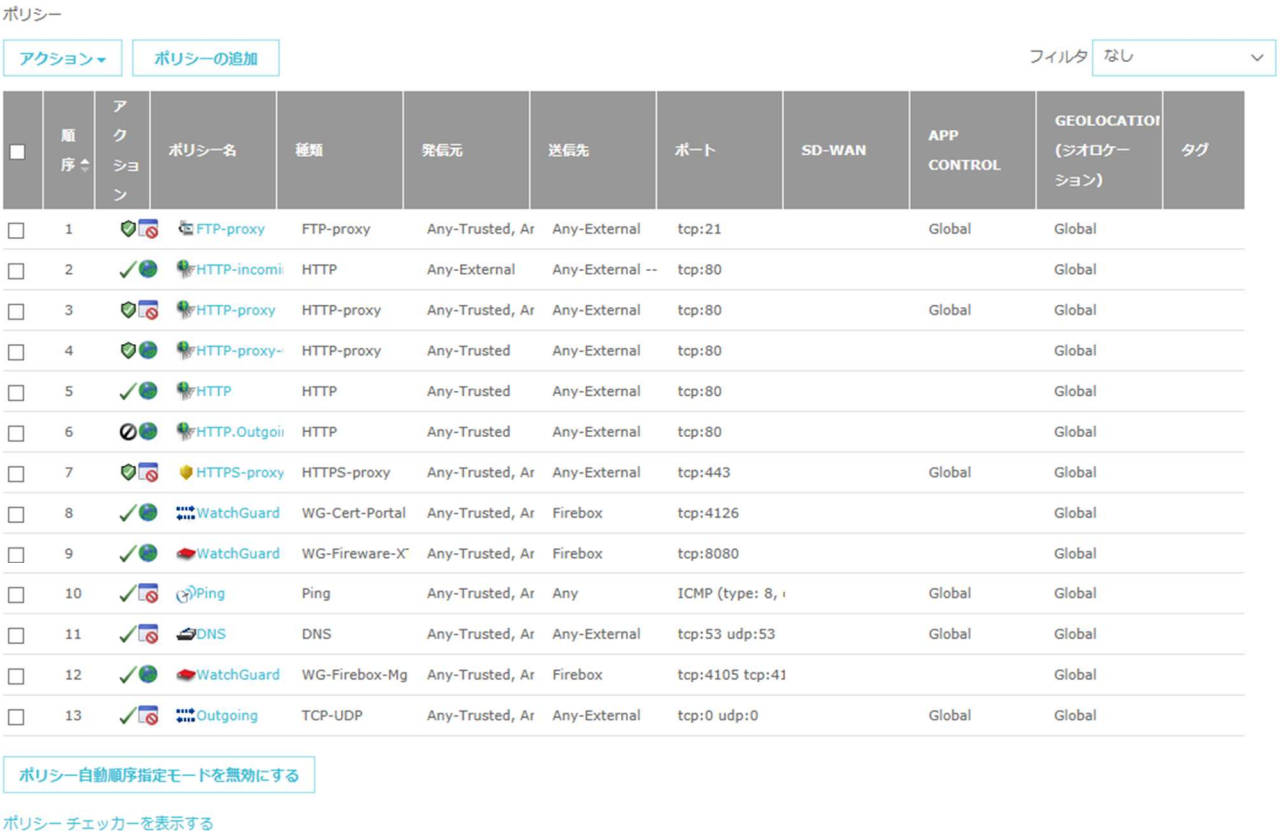
つまり、このプロトコルについては基本的には許可ポリシーですが、***通過する際には設定されたアクション(すなわちコンテンツフィルタリングやアンチウイルス)を効かせます***、という意味になります。[4]

最後に下方の[保存]ボタンを押してポリシーを追加しましょう。

[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

保存すると、ポリシー一覧に戻ります。

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。



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することができます。フィルタリング用のデータベースは実績のある FORCEPOINT 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、Firebox はそのサイト情報を照合します。規制対象であればアクセスをブロックし、警告画面を表示します。

Web Blocker を構成する

メニュー*セキュリティサブスクリプションサービス* ー *WebBlocker（Web フィルタリング）* をクリックし、WebBlocker の構成画面を開きます。
[追加]ボタンをクリックします。

まずアクション名を入力します。

サーバータブでは、「WebBlocker クラウド」を選択します。

5

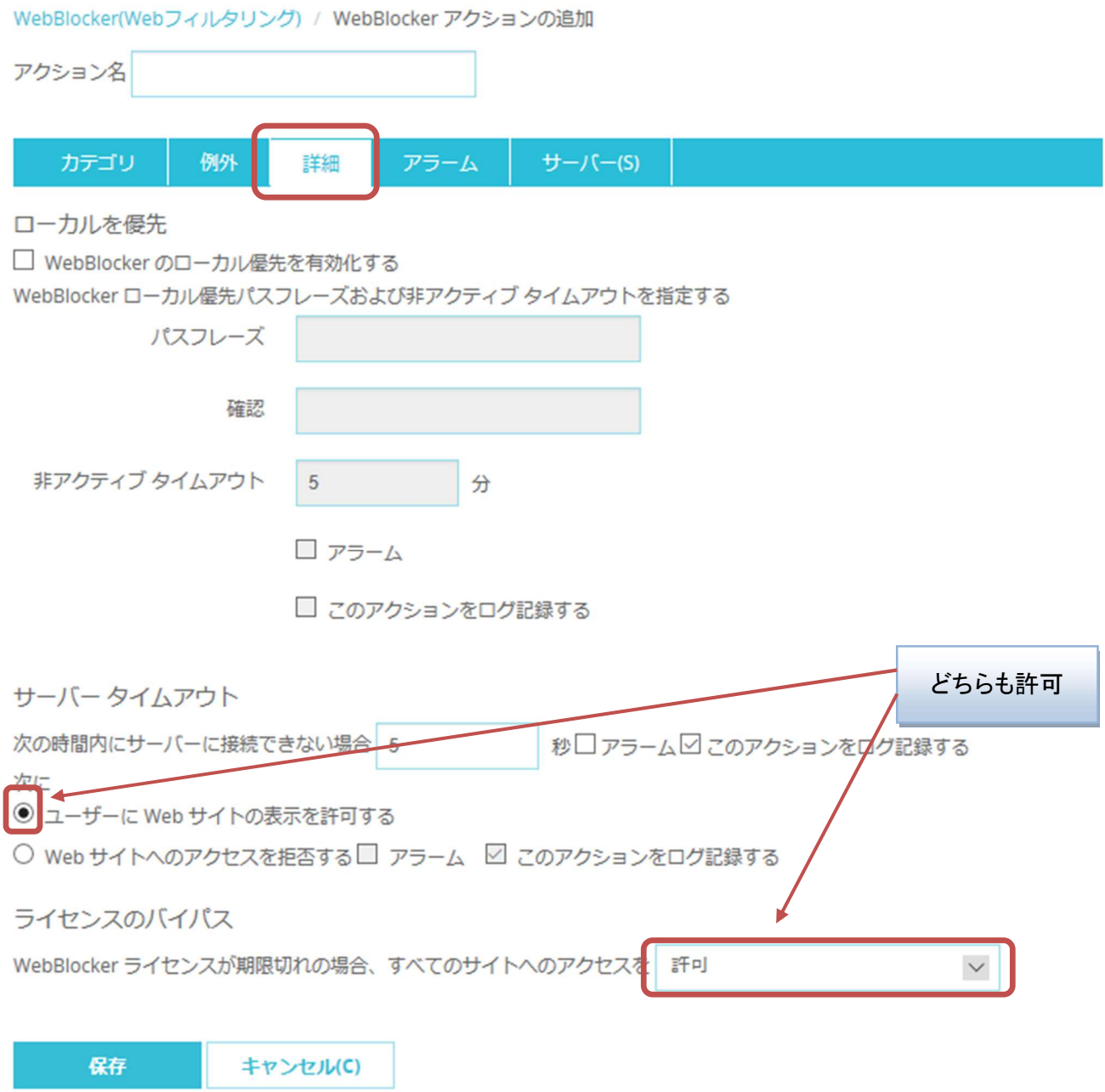
自社に WebBlocker サーバーを構築していて、そちらを使うのであれば、「オンプレミス WebBlocker Server」にチェックを入れ、サーバーの IP アドレスを追加します。

---

5 「WebBlocker グローバル設定」はセキュリティサブスクリプションサービス/WebBlocker（Web フィルタリング）メニューから 設定 ボタンをクリックで表示されます。

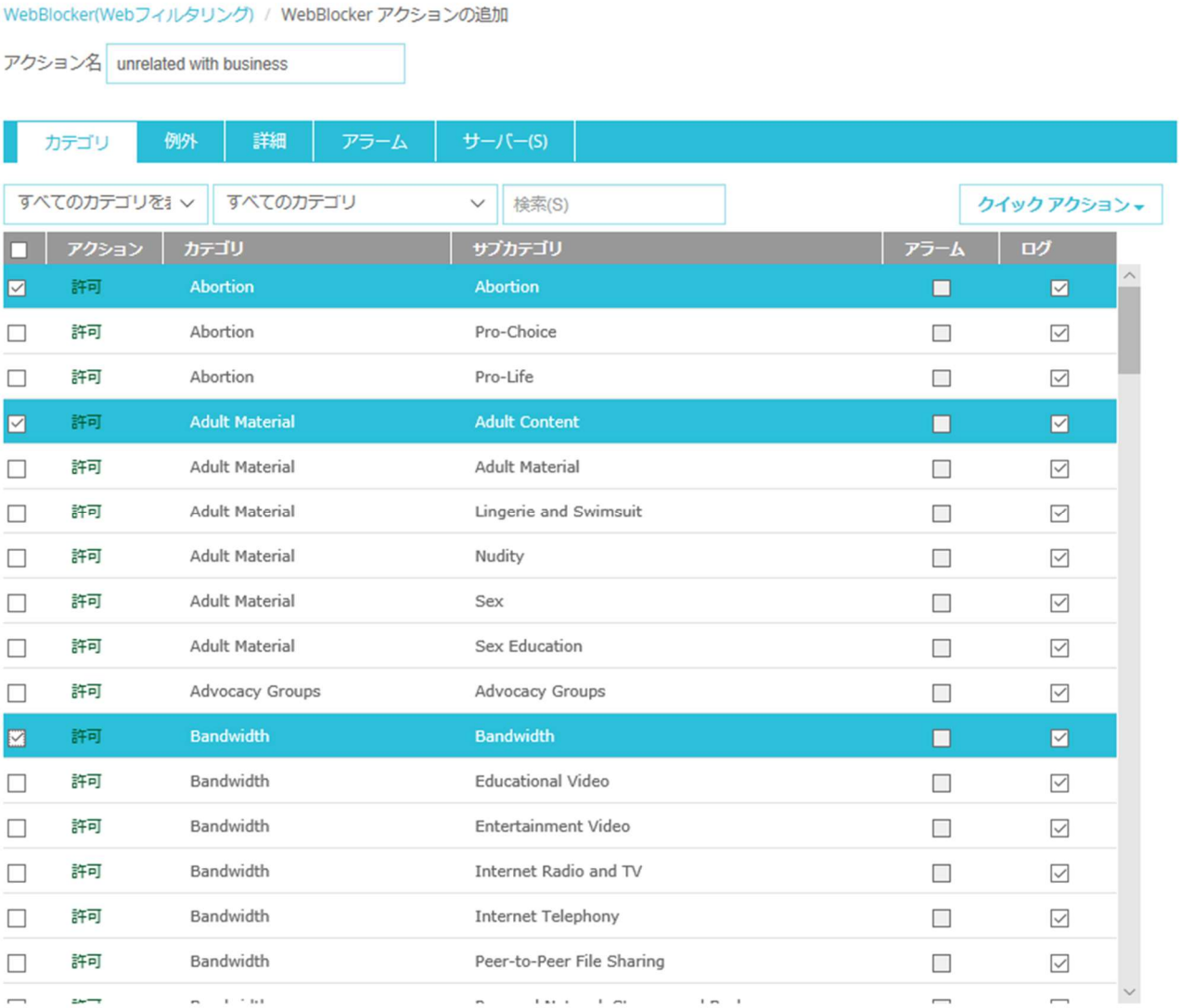
詳細タブでの設定です。

「サーバータイムアウト」と「ライセンスのバイパス」の設定をご確認ください。
もし WebBlocker 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、セキュリティを優先し、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、WebBlocker サーバーのタイムアウト時やライセンス更新を忘れてしまった場合に、業務に影響が出ないように設定を検討してください。

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にチェックを入れます。



以前のバージョンの画面ではグループ化されたカテゴリを一度に扱うことができましたが、本バージョンではユーザーインターフェースが変更され、グループ化できなくなりました。同じグループに対して同じアクションを行うにはフィルタを使い、クイックアクションでアクションを選択します。

以下の画面の例では、Adult Material でフィルタし、クイックアクションから Adult Material カテゴリに含まれるすべての項目を拒否しています。

Adult Material カテゴリで項目をフィルタします。

左上チェックボックスをチェックし、すべての Adult Material を選択します。クイックアクションから拒否を選択します。

すべての Adult Material カテゴリが拒否されます

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。

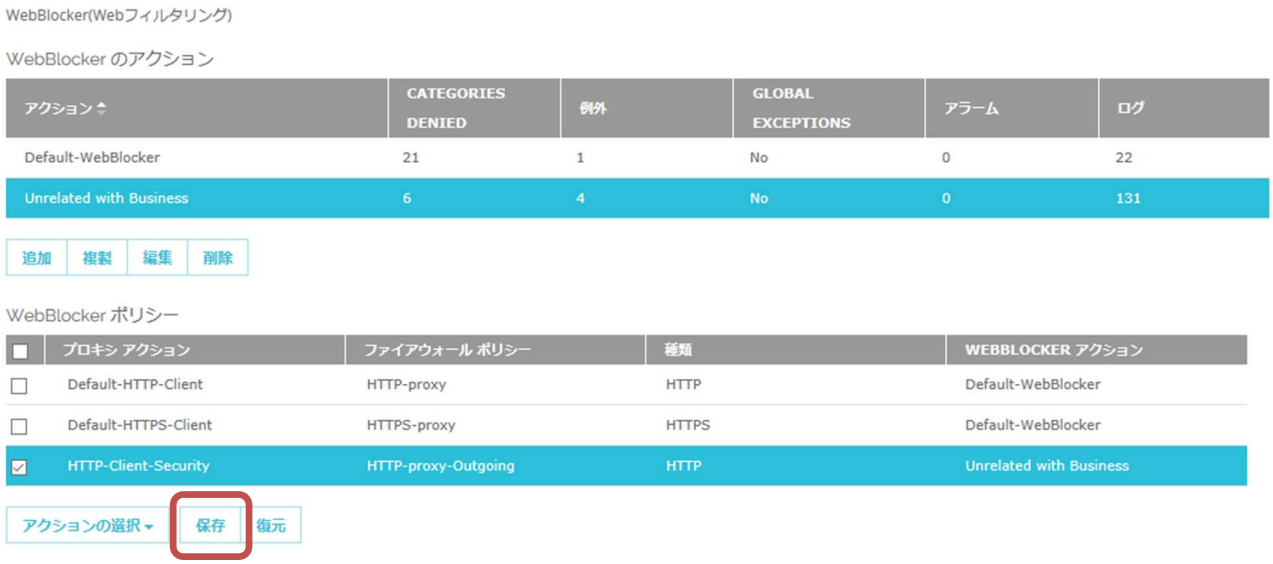
一通り設定したら、画面下方にある保存ボタンをクリックし設定を反映させます。

新しい WebBlocker のアクションが登録されました。

ではこの WebBlocker のアクションをプロキシアクションと紐付けましょう。

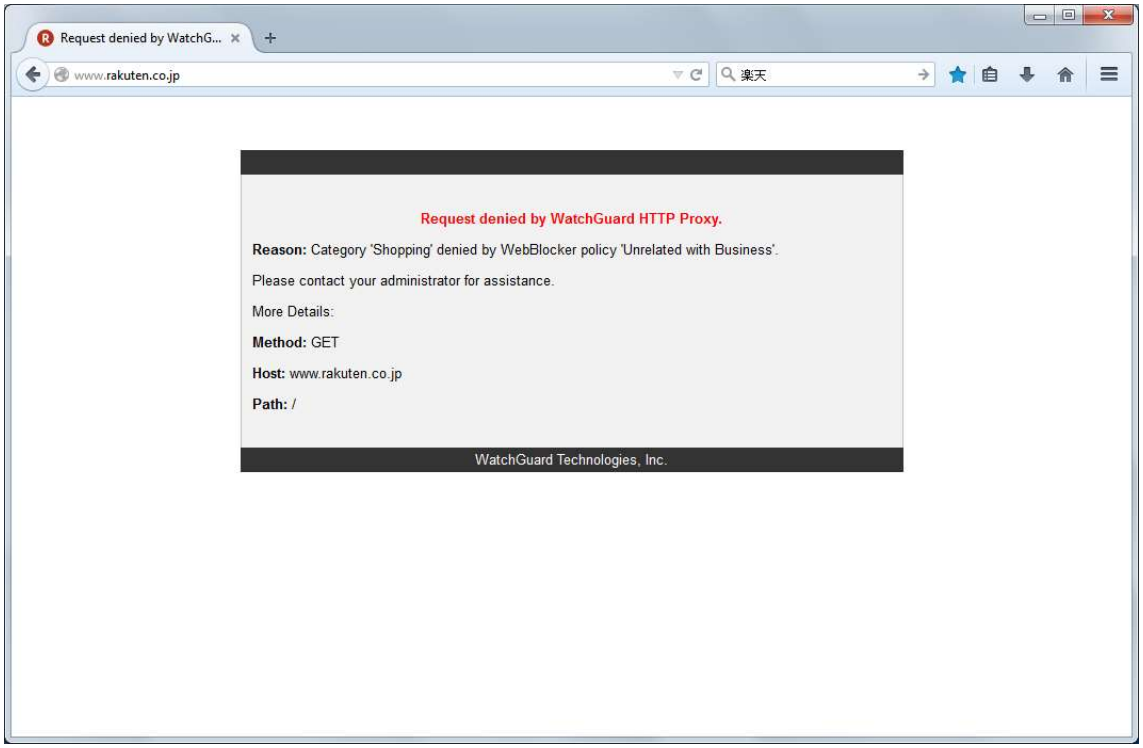
下の WebBlocker ポリシーに、あらかじめ作成したアクション「HTTP-Client-Security」には何も関連付けられず「なし」になっています。
アクションの選択のドロップダウンリストで WebBlocker のプロファイル「Unrelated with Business」を指定します。

この状態で保存ボタンをクリックし、設定を保存します。



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。

WebBlocker が機能し、以下のように拒否画面が表示されます。



また、WebBlocker の設定にはウィザード機能が追加されていますので、WebBlocker 初期画面から「ウィザードを実行」を選択して同様の設定をすることができます。

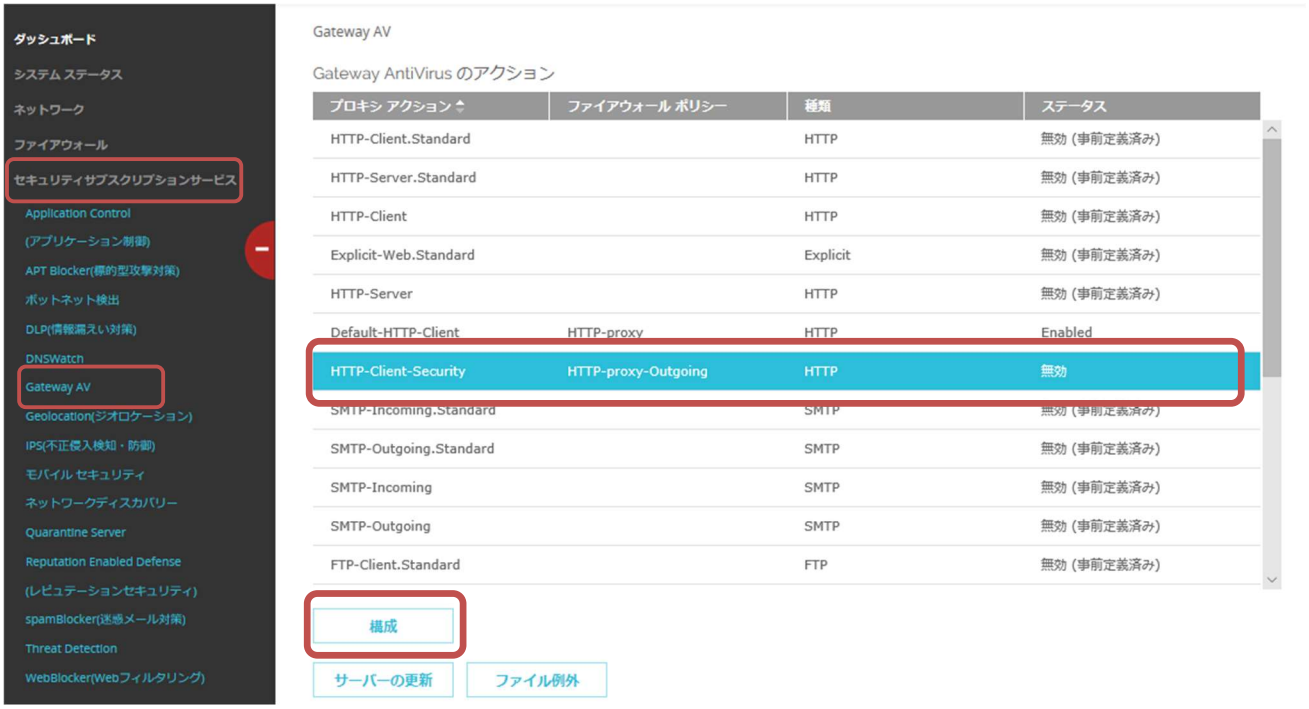
Gateway AntiVirus の設定

Gateway AntiVirus を有効にすると、Firebox 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 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*セキュリティサブスクリプションサービス* 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、構成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。

ウイ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 ファイルの受け渡しにも支障をきたすためです。

以上で保存します。GAV は有効になります。

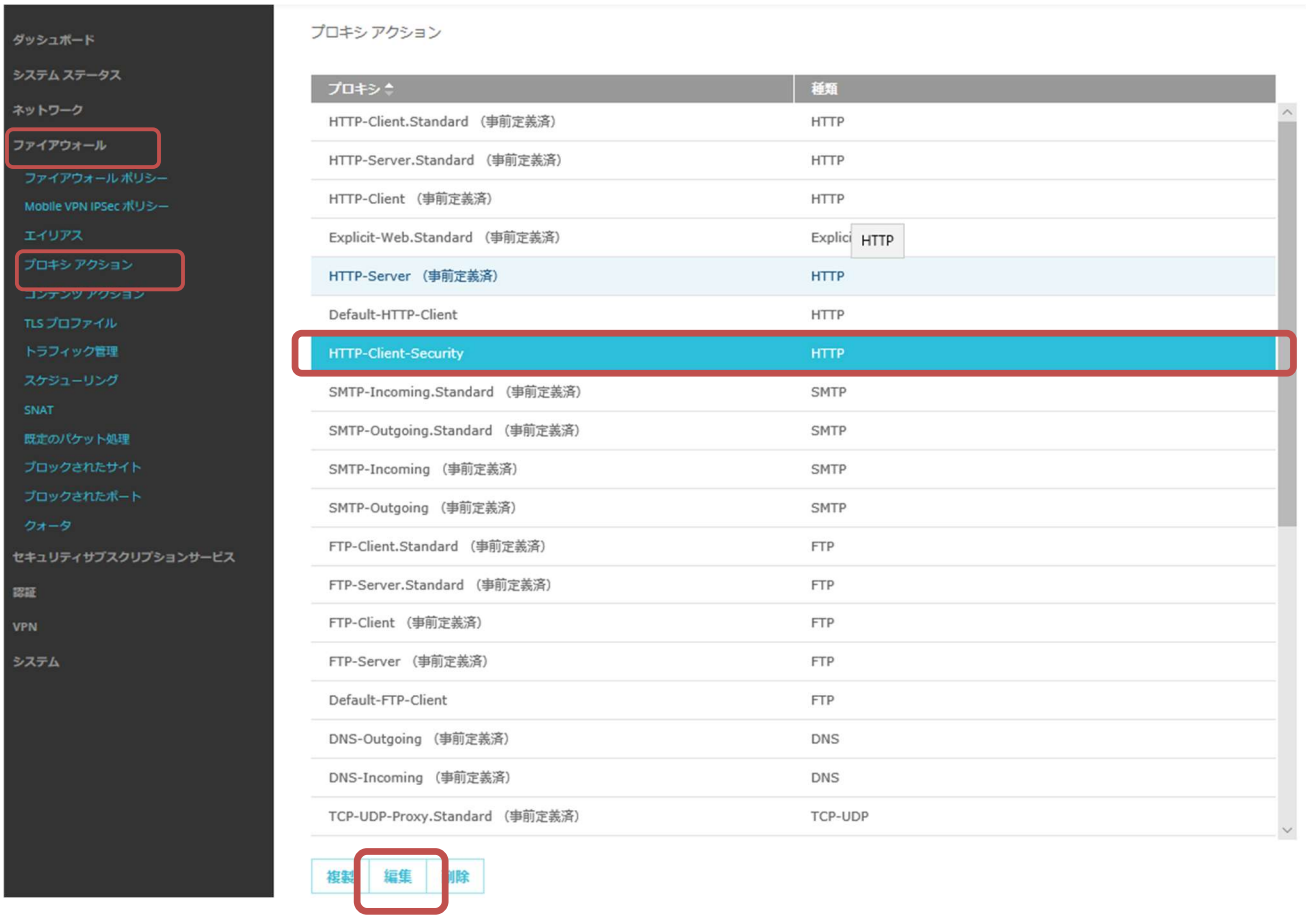
Gateway AntiVirus を設定する

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[サーバーの更新]ボタンをクリックします。

GAV の全体的な設定になります。
AV のシグネチャが確実に更新されるよう「自動更新を有効にする」に必ずチェックを入れてください。自動更新の対象として「Gateway AntiVirus の署名」にもチェックを入れます。

以上で設定を保存してください。

HTTP ヘッダーやファイルの種類によって GAV をどう適用するかなどの詳細な設定は、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。

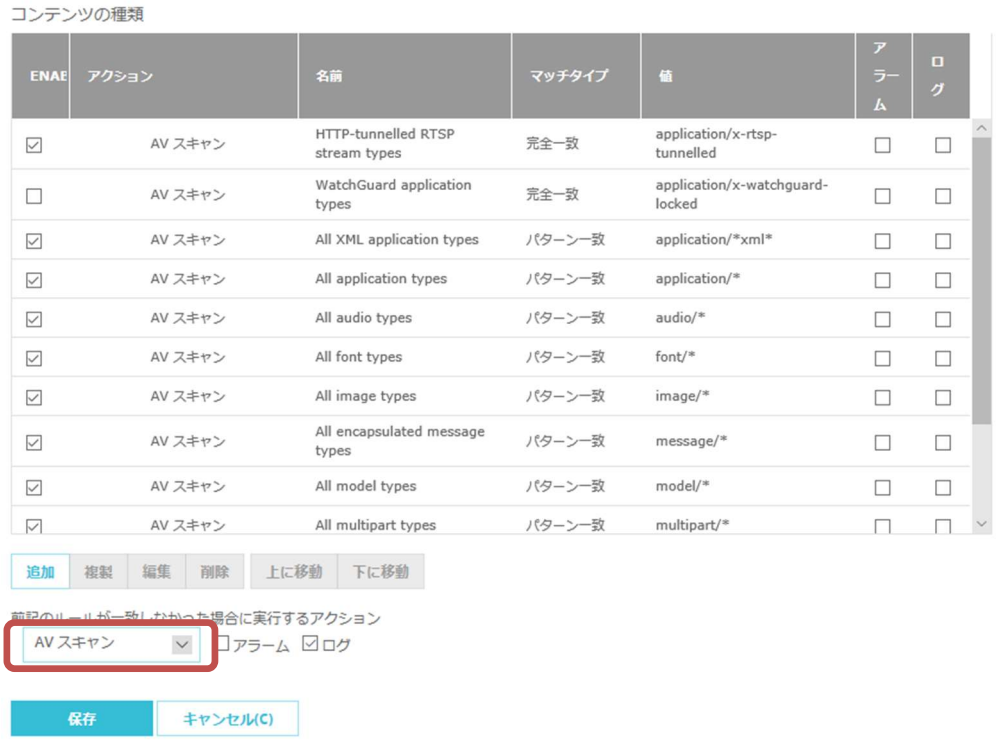


HTTP 応答 – コンテンツの種類

プロキシアクションの編集で「HTTP 応答」のドロップダウンリストで「コンテンツの種類」を選択します。

次の図のように、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設定になっています。

ただ、すべてのコンテンツの種類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)。



HTTP 応答 – 本文のコンテンツの種類

次に同じくHTTP 応答のリストから「本文のコンテンツの種類」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。

最後に下方の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（手動）

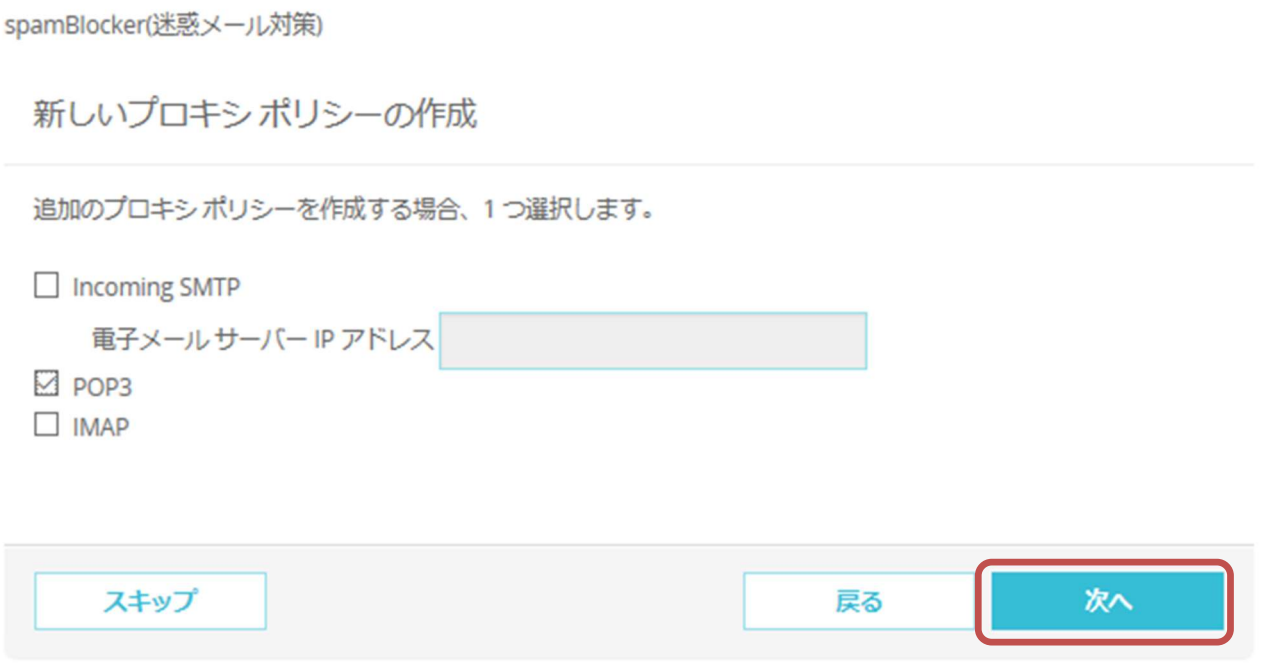
spamBlocker では、Cyren 社が持つ特許技術 RPD(Recurrent Pattern Detection)ソリューションを利用して、発見が難しいスパムを検出します。

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。

spamBlocker アクティブ化ウィザードを実行して 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、まずウィザードを実行して Proxy アクションを定義しましょう。トップページから次へをクリックします。

プロクシ―ポリシーから POP3 を選択し、次へをクリックします。



終了をクリックし、spamBlocker のアクションを表示します。

spamBlocker(迷惑メール対策)

spamBlocker のアクション

プロキシ アクション	ファイアウォール ポリシー	種類	ステータス
SMTP-Incoming.Standard		SMTP	無効 (事前定義済み)
SMTP-Outgoing.Standard		SMTP	無効 (事前定義済み)
SMTP-Incoming		SMTP	無効 (事前定義済み)
SMTP-Outgoing		SMTP	無効 (事前定義済み)
POP3-Client.Standard		POP3	無効 (事前定義済み)
POP3-Server.Standard		POP3	無効 (事前定義済み)
POP3-Client		POP3	無効 (事前定義済み)
POP3-Server		POP3	無効 (事前定義済み)
POP3-Client.Standard.1	POP3-proxy	POP3	Enabled
IMAP-Client.Standard		IMAP	無効 (事前定義済み)
IMAP-Server.Standard		IMAP	無効 (事前定義済み)

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。

POP3-proxy ポリシーを追加する

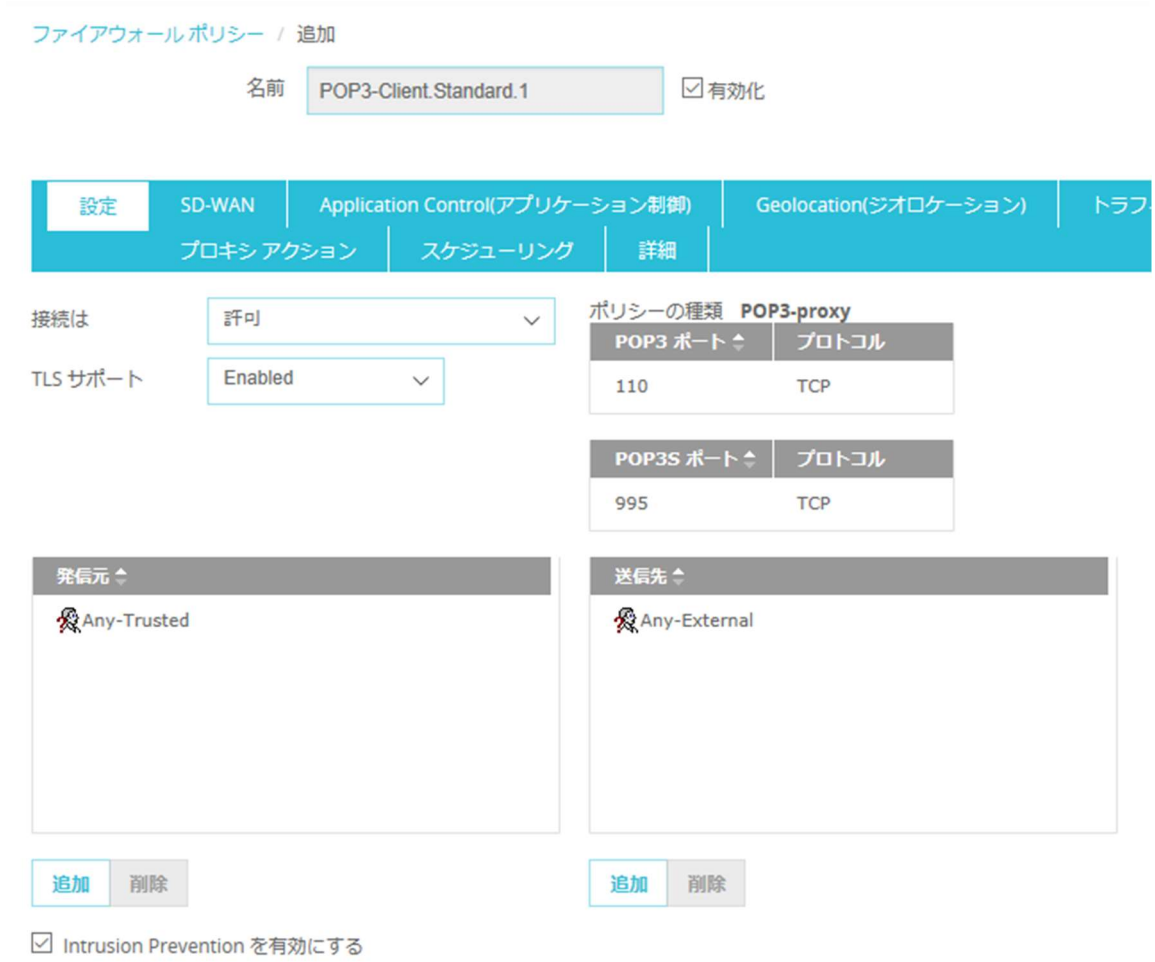
メニューの*ファイアウォール* － *ファイアウォールポリシー* でポリシー一覧を表示し、ポリシーの新規[追加]ボタンをクリックします。

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。

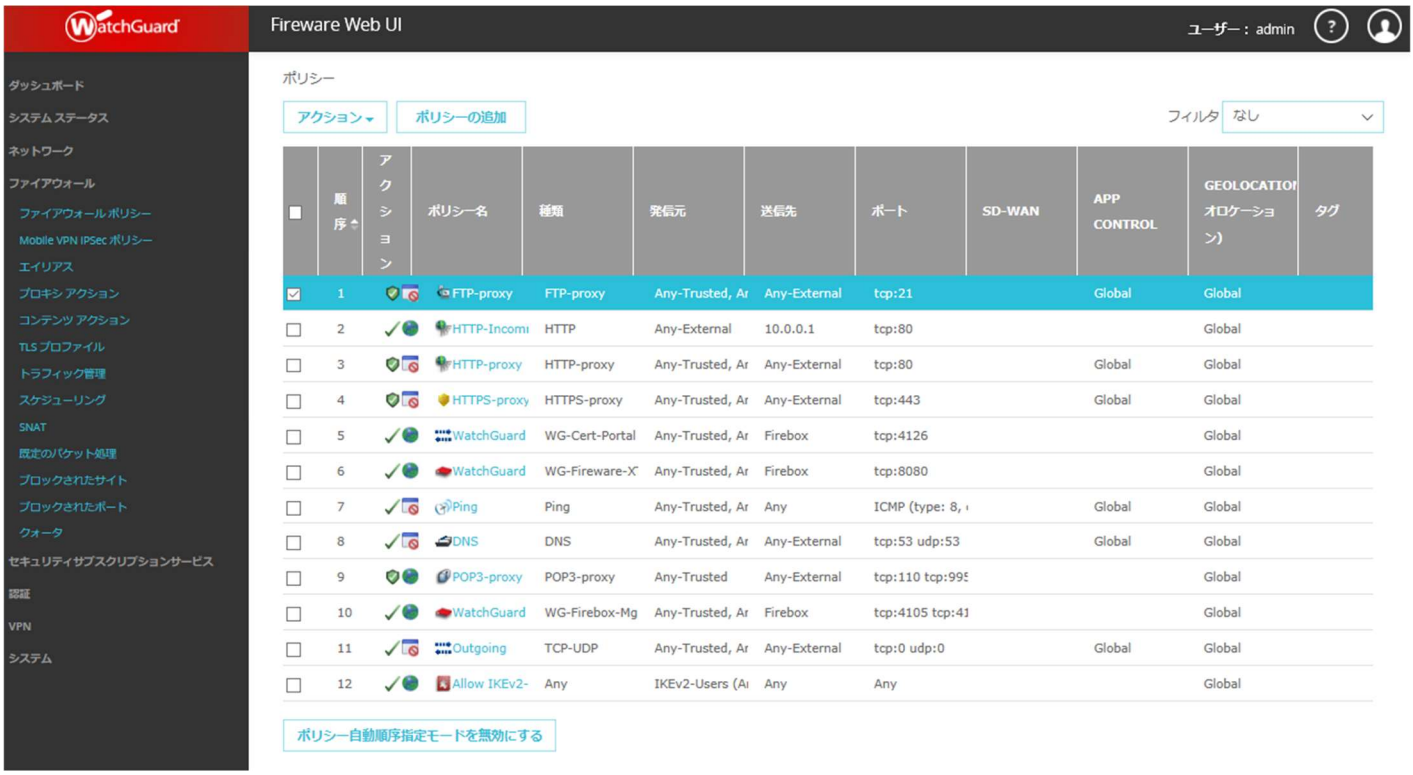
その横にはプロキシアクションのドロップダウンリストがあるので、先ほど作成したものを選択します。

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、画面下の保存ボタンをクリックして保存します。



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 *セキュリティサブスクリプションサービス* ー *spamBlocker(迷惑メール対策)* 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、「確認済み」のスパム、「バルク」(主に広告メールなど)、「疑わしい」の 3 種類です。

アクションは、そのメールを許可するか、指定の文字列(タグ)をサブジェクトに付加するか、のどちらかです。

「例外について」タブでは、ホワイトリストの追加削除が行なえます。

たとえば自社のドメインをホワイトリストに追加する場合、[追加]ボタンをクリックします。

アクションで「許可」を選択します。送信者の欄には、特定のメールアドレスを追加することもできますし、

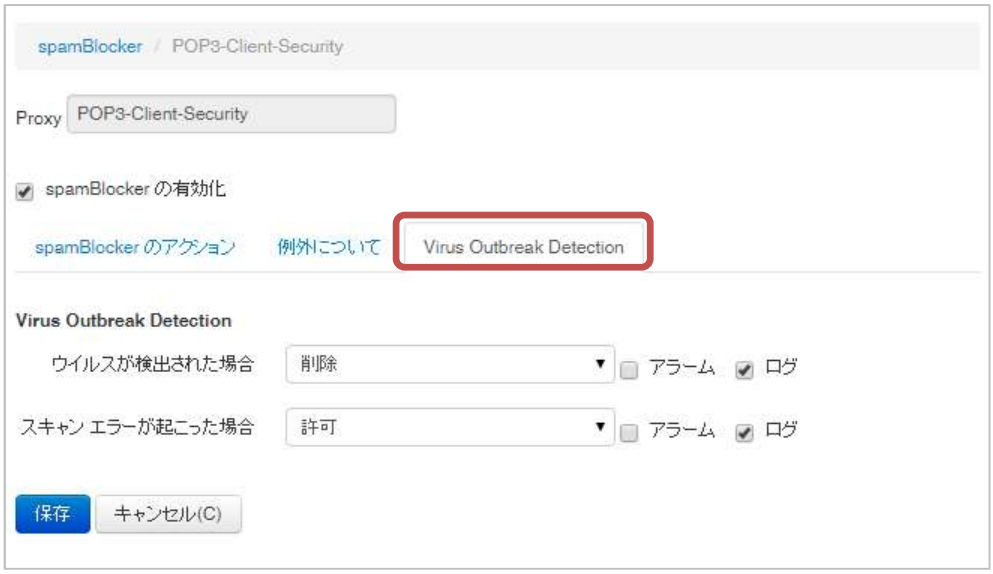
*(アスタリスク)@ドメイン名の形で、ドメインを指定することもできます。

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

[保存]ボタンをクリックして、設定を反映させましょう。

Virus Outbreak Detection タブでは、ウイルス検出時の動作を定義できます。Virus Outbreak Detection は既定で無効になっていますので、設定の[Virus Outbreak Detection（VOD）の有効化]をチェックします。

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。

おわりに

WebUI ガイドをご参照いただきありがとうございました。

WSM は強力な設定ツールですが、Web UI だけでも日常の設定管理が十分可能であることを実感していただけたかと思います。

Firebox 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います。

豊富な機能をフル活用していただき、強固なゲートウェイセキュリティを、ぜひ御社のものとしていただきたいと思います。