

# 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 2019 年 5 月 Rev-5

# 目次

| はじめに                                      |
|---|
| 第一章 Firebox のセキュリティ概念 ~ Firebox マニアになろう!6 |
| Firebox のネットワーク概念6                        |
| ネットワーク設定に見る Firebox の概念7                  |
| ポリシーマネージャに見る XMT の概念8                     |
| Firebox で実現可能なセキュリティ範囲9                   |
| WatchGuard System Manager の概要10           |
| WatchGuard System Manager11               |
| ポリシーマネージャ(Policy Manager)12               |
| Firebox System Manager13                  |
| 第二章 初期設定 ~ Firebox を一から設定しよう!14           |
| 事前準備14                                    |
| ファクトリーリセット17                              |
| 結線17                                      |
| Firebox T シリーズ18                          |
| Firebox M470/570 のリセット19                  |
| Firebox M440 のリセット20                      |
| ファクトリーリセット後の設定21                          |
| Quick Setup Wizard22                      |
| 第三章 ネットワークの設定 ~ まずはルーターとして構成しよう!          |
| 設定の保存                                     |
| DNS/WINS 設定                               |
| DNSの設定31                                  |
| WINSの設定31                                 |
| 外部ネットワークの設定                               |
| インターフェイス名                                 |
| 固定 IP の設定33                               |
| DHCP の設定34                                |

| PPPoE の設定                      | 35 |
|--------------------------------|----|
| 複数の固定 IP がある場合                 | 36 |
| 内部ネットワークの設定                    | 37 |
| Trusted インターフェイスの設定            | 38 |
| DHCP サーバーの使用                   | 38 |
| ブリッジの構成                        | 41 |
| DMZ を設定する                      | 44 |
| NAT 設定(1-1NAT)                 | 44 |
| ルーティング設定                       | 46 |
| 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! | 48 |
| ポリシーマネージャついて                   | 48 |
| ポリシーマネージャの画面構成                 | 48 |
| ポリシーの変更/追加/保存                  | 49 |
| ポリシーの保存                        | 49 |
| ポリシーの追加                        | 50 |
| ポリシー追加 (内側から外側へ)               | 50 |
| ポリシー追加 (外側から内側へ)               | 52 |
| ポリシー追加 (SNAT で外側から内側へ)         | 57 |
| テンプレートにないポリシーを追加する             | 60 |
| ポリシーの編集                        | 63 |
| 一時的に無効にする                      | 63 |
| ログを記録する                        | 64 |
| 運用スケジュールを設定する                  | 65 |
| ポリシー以外のファイアウォール設定              | 66 |
| Default Threat Protection      | 66 |
| Blocked Sites                  | 67 |
| Blocked Ports                  | 67 |
| 第五章 UTM の設定 ~ あらゆる脅威に対応しよう     | 68 |
| プロキシポリシーの追加                    | 69 |

| Web Blocker の設定              |
|------------------------------|
| Web Blocker を有効にする72         |
| Web Blocker を構成する75          |
| Gateway Anti-Virus の設定80     |
| Gateway Anti-Virus を有効にする80  |
| Gateway Anti-Virus を構成する82   |
| spamBlocker の設定              |
| POP-Proxy を追加する              |
| spamBlocker を有効にする90         |
| spamBlocker を構成する92          |
| Intrusion Prevention Service |
| 構成例                          |
| IPS の設定95                    |
| ポリシー設定98                     |
| IPS の調整                      |
| 例外の設定104                     |
| Reputation Enabled Defense   |
| RED 構成時の注意点106               |
| ポリシーの追加107                   |
| RED の構成108                   |
| おわりに                         |

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、WatchGuard Firebox 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、 Fireboxの日常的な管理は難なくできるようになるでしょう。

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 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、Firebox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。

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。



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 Optional、1-3 が Trusted、4,5 を External として設定しています。

| Eードでイン | ターフェイスを構成: ミック | スルーティング モード |             |           | #M\$3 \$22 0 0 0 7 4 3 . |   |
|--------|----------------|-------------|-------------|-----------|--------------------------|---|
| ターフェ   | 名前 (エイリアス)     | 種類          | IPv4 アドレス   | IPv6 アドレス | NIC 構成                   | 相 |
| 0      | Optional       | 任意          | 10.0.0.1/24 |           | 自動ネゴシエート                 | - |
| 1      | Trusted-1      | 信頼済み        | 10.0.1.1/24 |           | 自動ネゴシエート                 |   |
| 2      | Trusted-2      | 信頼済み        | 10.0.2.1/24 |           | 自動ネゴシエート                 |   |
| 3      | Trusted-3      | 信頼済み        | 10.0.3.1/24 |           | 自動ネゴシエート                 |   |
| 4      | External-1     | 外部          | DHCP        |           | 自動ネゴシエート                 |   |
| 5      | External-2     | 外部          | DHCP        |           | 自動ネゴシエート                 |   |
| 6      | Optional-5     | 無効          |             |           | 自動ネゴシエート                 |   |
| 7      | Optional-6     | 無効          |             |           | 自動ネゴシエート                 |   |
|        |                |             |             |           |                          |   |

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。

| 前: FTP   | → 何のプロトコルを?  |                     |
|--|--|---------------------|
| ポリシー プロパティ 詳細  |  |                     |
| FTP 接続を…   |  |                     |
| 許可 🗸   | → 許可?拒否?   | Ŷ                   |
| 送信元  |  |                     |
| Any-Trusted  | → どこから?  |                     |
|  |  |                     |
|  | _  |                     |
| 一 万间   |  | 追加 编集 削除            |
|  |  | Marchal con Marchal |
| Any-External   | 10   |                     |
|  | → <u>どこへ?</u>  |                     |
|  |  |                     |
|  |  |                     |
|  |  |                     |
|  |  | <b>追加</b> 編集 削除     |
| Route outbound traffic using SD-V  | VAN Based Routing VAN Based Routing VAN Based Routing  | <b>追加</b> 編集 削除     |
| Route outbound traffic using SD-V SD-WAN Action  | VAN Based Routing (Fireware OS v12.3 or higher)  | <b>追加</b> 編集 削除     |
| Route outbound traffic using SD-V SD-WAN Action  | WAN Based Routing (Fireware OS v12.3 or higher)  | <u>追加</u> 編集 削除     |
| Route outbound traffic using SD-V SD-WAN Action  | VAN Based Routing (Fireware OS v12.3 or higher)  | <b>追加</b> 編集 削除     |
| <ul> <li>Route outbound traffic using SD-V</li> <li>SD-WAN Action</li> <li>Application Control を有効にします:</li> </ul>   | VAN Based Routing (Fireware OS v12.3 or higher)  | <u>追加</u> 調集 削除     |
| <ul> <li>□ Route outbound traffic using SD-V</li> <li>SD-WAN Action</li> <li>□ Application Control を有効にします:</li> <li>☑ Geolocation を有効化する</li> </ul>   | WAN Based Routing (Fireware OS v12.3 or higher)  | 3 <b>2 加</b> 編集 削除  |
| <ul> <li>□ Route outbound traffic using SD-V</li> <li>SD-WAN Action</li> <li>□ Application Control を有効にします:</li> <li>☑ Geolocation を有効化する</li> <li>☑ このポリシーの IPS を有効にします</li> </ul>  | VAN Based Routing (Fireware OS v12.3 or higher)  | <u>追加</u> 翻集        |
| <ul> <li>□ Route outbound traffic using SD-V</li> <li>SD-WAN Action</li> <li>□ Application Control を有効にします:</li> <li>☑ Geolocation を有効化する</li> <li>☑ このポリシーの IPS を有効にします</li> <li>□ 帯域幅と時間クォータを有効化する (</li> </ul>                      | WAN Based Routing (Fireware OS v12.3 or higher)  Kan Based Routing (Fireware OS v12.3 or higher)  Global  Global  Fireware OS v11.10 以降) | <u>追加</u> 翻柴 削除     |
| <ul> <li>□ Route outbound traffic using SD-V</li> <li>SD-WAN Action</li> <li>□ Application Control を有効にします:</li> <li>☑ Geolocation を有効化する</li> <li>☑ このポリシーの IPS を有効にします</li> <li>□ 帯域幅と時間クォータを有効化する (</li> <li>ブロキシ アクション:</li> </ul> | WAN Based Routing 《Fireware OS v12.3 or higher)<br>Clobal<br>Clobal<br>Fireware OS v11.10 以降)  | <u>追加</u> 編集 削除     |
| <ul> <li>□ Route outbound traffic using SD-V</li> <li>SD-WAN Action</li> <li>□ Application Control を有効にします:</li> <li>☑ Geolocation を有効化する</li> <li>☑ このポリシーの IPS を有効にします</li> <li>□ 帯域幅と時間クォータを有効化する (</li> <li>プロキシアクション:</li> </ul>  | VAN Based Routing (Fireware OS v12.3 or higher)  Global  Global  Fireware OS v11.10 以降)  | <u>追加</u> 鋼集 削除     |

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。

| / /· | ペケットフィルタ | : 7 | ポートベー | マ |
|------|----------|-----|-------|---|
|------|----------|-----|-------|---|

**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

## 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、Firebox でネットワーク管 理とセキュリティ設定を、容易に且つ効率的に行なうためのソフトウェアです。

WSM の基本コンポーネントは、Firebox を管理するためのクライアントソフトウェアと、Firebox と連携して動作するサーバーソフトウェアに分かれています。

クライアントソフトウェアは、WatchGuard System Manager ウィンドウであり、そこから Firebox デバイスに 接続したり、Policy Manager などの設定ツールや FSM(Firebox System Manager)などのモニタリングツー ルを起動できます。



サーバーソフトウェアは Firebox を複数台まとめて管理できる Management Server、可視化ツールの Log Server および Report Server、メールの隔離ができる Quarantine Server などを含んでいます。

#### WatchGuard System Manager

WatchGuard System Manager (以下 WSM) は、Firebox 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 Firebox 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 Web UI も用意されています。通常の設定管理業務では、この Web UI で問題なく行なえます。しかし Firebox 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。 Web UI には設定する上での制約がいくらかあるのに対して WSM ではすべての設定が可能です。加えて WSM には設定やモニタリングする上で役立つ、数々の有用なツールと連携できるからです。

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 Firebox へ接続します
- 2. メニューの ツール 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。

ポリシーマネージャ上で設定した内容は Firebox 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。

またコンフィグファイルを後から Firebox に流し込むことも可能です。

### Firebox System Manager

Firebox System Manager は、Firebox をリアルタイムでモニタリングするためのインターフェイスです。この ツールから、Firebox 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 Firebox 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 ~ Firebox を一から設定しよう!

#### 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『ソフトウェアダウンロード』より必要なソフトウェアを取得します。

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

WatchGuard サポートセンター(US)のログイン後、MY WATCHGUARD からドロップダウンリストで Download Software のページにアクセスできます。

| サポートサイト(ロ<br>・ ・ ・ い 命 https://<br>・ ・ い か 合 https:// | Iグイン後)<br>Software Home<br>vatchguard.force.com/custome   | + v<br>ers/CustomerComm | からソフトウェアダ<br>・ジにアクセスできま  | ウンロードの<br>ます     | - □ ×<br>☆ ☆ & ピ …                                    |
|---|---|-------------------------|--------------------------|------------------|---|
| Soft on CENTER  | MY WATCHGUARD   | TECH RESOURCES          | TRAINING & CERTIFICATION | SUPPORT SERVICES | Partner Portal Log Out                                |
| Support Cente   | Activate Peroducts<br>Download Software<br>WatchGuard Cloud<br>Manage Cases<br>Manage DNSWatch<br>Manage Products<br>Manage Profile<br>Manage TDR<br>Manage Users<br>Manage Wi-Fi Cloud | al search               |                          |                  |   |
|   | (A)   | F                       | 1                        |                  | Find It Fast  |
|   |   |                         |                          |                  | Product and Support News<br>Receive real-time updates |
|   | Watch   | GuardID I               | <b>Meets</b> Auth        | Point            | Support Programs<br>Compare support levels            |
|   | Enable M  | FA for your Wa          | atchGuard User /         | Account          | User Forum<br>Ack technical questions                 |

必要なソフトウェアは、以下の2つです。

- WatchGuard System Manager
- Fireware

Fireware はモデルに対応したものをダウンロードしてください。また WSM は Fireware と同じか上位のバー ジョンをお使いください。 Software Download のページで、WSM とモデルに対応した Fireware をダウンロードします。

| Software Downloads  |                    |   |
|---|--------------------|---|
| Show downloads for:<br>Select a device<br>Or type the first four digits of the serial number: | モデルごとの<br>Fireware | Welcome!<br>Latest Software Releases:<br>- Fireware v12.1.1<br>- WatchGuard Dimension v2.1.1 Update 2<br>- WatchGuard XCS v10.2                                 |
| Or, choose your device and family model:<br>Firebox and XTM                                   | WatchGuard AP      | 最新のWSM<br>Quick Link<br>Fireware v1 cta<br>Help us test of Fireware! Click here<br>to join the V. SM/Fireware v12.2 Beta Program.                               |
| WatchGuard XCS  | WatchGuard SSL     | WSM v12.1.1<br>Download the latest release of WatchGuard System<br>Manager.<br>Dimension v2.1.1 Update 2<br>Find the latest installation, and upgrade files for |

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 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。 合わせてライセンスキー(Feature Key) も取得しておきます。上記 URL の『Manage 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。



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

| CirchGuard* |  | 17 9 17 22<br>17 9 17 12<br>17 9 17 9 17 12<br>17 9 17 12<br>1 |  |
|-------------|--|--|--|

└─→ 1 番ポート: Trusted

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 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。

## Firebox M470/570 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

#### M470/570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
- 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 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

# 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      |

Firebox の1番ポートとPCを接続しておいてください。

リセット後、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。

| Girebox* M500 | :  |              |
|---------------|----|--------------|
|               | 1番 | ポート 10.0.1.1 |
|               |    | 10.0.1.2     |

【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
- ✓ Fireware をアップグレードしたが、元のバージョンに戻したい

初期化をすればいつでも新品を箱から出したのと同じ状態からセットアップできます。

# 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、<u>ツール</u> — <u>Quick Setup Wizard</u>をクリックします。

| 💐 WatchGuard Sys    | m Manager  |                     | -05 |        | ×   |
|---------------------|--|---------------------|-----|--------|-----|
| ファイル(F) 編集(E)       | リール(m) ウィンドウ(w)  | ) <u>ヘルブ(h)</u>     |     |        |     |
| ∢ 🜌 🎞 ≟             | 崔 Quick Setup Wizard   | d(Q)                |     |        |     |
| テバイス ステータス          | Policy Manager(P)  | inager(M)           |     |        |     |
|                     | 管理レポートの生成<br>構成レポートの生成<br>CA Manager<br>Log Manager(L)<br>Report Manager(R)<br>Quarantine Server ( | 成<br>成<br>Client(U) |     |        |     |
|                     |  |                     |     |        |     |
| uick Setup Wizard を | 日朝します  |                     | C   | AP NUM | SCR |

# 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]。



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

|                           | フェイスを選択し      | てください。                                  |
|---------------------------|---------------|---|
| 名前                        | IPアドレス        | 說明                                      |
| ローカル エリア接続                | 10.0.1.3      | Intel(R) 82579LM Gigabit Network Conne. |
| Wifi                      | 10.254.252.48 | Intel(R) Centrino(R) Advanced-N 6205    |
| VMware Network Adapter VM | 192.168.80.1  | VMware Virtual Ethernet Adapter for V   |
| VMware Network Adapter VM | 192.168.23.1  | VMware Virtual Ethernet Adapter for V   |
|                           |               |   |

デバイスが発見されたら次へ。



※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

# 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& ペーストするか、[参照]をクリックし、保存しておいた Feature Key を指定して読み込みます。

| WatchGuard Quick Setup Wizard  |                                |
|--|--------------------------------|
| デバイスのソフトウェアをアクティベートします。  | WatchGuard                     |
| デバイスを機能キーでアクティベートする必要があります。 機能<br>ルドに貼り付けるか、[参照] をクリックしてファイルから機能キ  | キーのテキストをこのフィー<br>-をインストールできます。 |
| Feature: VPN_USER#25<br>Feature: VPA_SPEED#0<br>Feature: VPA_SPEED#0<br>Feature: WEBBLOCKER@Feb-10-2017<br>Feature: XTM_PR0<br>Expiration: never   | ···· 参照                        |
| Signature: 302c02140a47de40-88a19324fa16c818-b5a2a04952df  | c7e1-02147                     |
| <ul> <li>              ・             が能キーがない場合は、<u>LiveSecurity</u> Web サイトを参照し<br/><del>詳細情報 <u>機能キー</u>             ・          </del></li> </ul> | 、て入手します。                       |
| <戻る  | 次へ > キャンセル                     |

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。ステータスパスフレーズと構成パスフレーズに同 ー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。

| WatchGuard Quick Setu           | p Wizard                              |                   |
|---------------------------------|---------------------------------------|-------------------|
| デバイス用のパスフレー                     | ズを作成します。                              | WatchGuard        |
| デバイス用の新しいステータ<br>カして、正しく入力されてい  | スおよび構成のパスフレーズを<br>るかを確認します。           | 5入力します。 パスフレーズを再入 |
| ステータス パスフレーズ<br>(読み取り専用アクセス)    | •••••                                 |                   |
| パスフレーズの再入力:                     | •••••                                 |                   |
| 構成パスフレーズ:<br>(読み書きアクセス)         | •••••                                 |                   |
| パスフレーズの再入力:                     | •••••                                 |                   |
| (1) パスフレーズには、最<br>次の項目の作成方法の詳細強 | 低 8 文字を使用する必要があ<br>カなパ <u>スフレーズ</u> . | ります。              |
|                                 |                                       | 5 次へ 5 キャンセル      |
|                                 |                                       |                   |

「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」の画面になれば初期設定の 完了です。



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。

# 第三章 ネットワークの設定 ~ まずはルーターとして構成しよう!

それでは前章で初期設定を施した Firebox 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、[Login]をクリックします。

|         | onnect to Firebox                                     | ×                                   |  |
|---------|---|-------------------------------------|--|
| イスステータス | Please enter the user lo<br>of your Firebox.          | gin information                     |  |
|         | IP Address or Name:<br>User Name:<br>Passphrase:      | 10.0.1.1         ▼           status |  |
|         | Authentication Server:<br>Domain:<br><u>Ti</u> meout: | Firebox-DB<br>25<br>seconds         |  |
| L       |   | Login Cancel Help                   |  |

以下のように接続した Firebox が表示されます。

| WatchGuard System Manager   |              |
|---|--------------|
| ファイルビ 編集回 ツールロ ウィンドウ(1) ヘルプ(1)  |              |
|   |              |
| デバイスステータス   |              |
| ■ TSO-Minatoku-Branch (10.0.1.1) - T30 [Fireware XTM v11.10.5.B495245] ● 示 Firebox のステータス ● 証明書 ● 認明書 ● Mobile VPN with IPSecトンネル ● Mobile VPN with SSLトンネル ● Mobile VPN with SSLトンネル ● Mobile VPN with PTPトンネル ● Mobile VPN with L2TP トンネル |              |
|   | CAP NUM SCRL |

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。

| ファイア       | ウォール Mobile | e VPN with IPSec              |                       |                           |              |                            |    |
|------------|-------------|-------------------------------|-----------------------|---------------------------|--------------|----------------------------|----|
| - <u>-</u> |             | 1                             | 1                     |                           | フィルタ:な       | L v 🍞                      | 7  |
| 順序 /       | アクション       | ポリシー名                         | ポリシーの種類               | 送信元                       | 送信先          | ボート                        | P  |
| 1          | V           | ETP-proxy                     | FTP-proxy             | Any-Trusted, Any-Optional | Any-External | tcp:21                     |    |
| 2          | V 🖉 🥘       | W HTTP-proxy                  | HTTP-proxy            | Any-Trusted, Any-Optional | Any-External | tcp:80                     |    |
| 3          | 🖉 🖉 🍘       | HTTPS-proxy                   | HTTPS-proxy           | Any-Trusted, Any-Optional | Any-External | tcp:443                    |    |
| 4          | V 🔘         | WatchGuard Certificate Portal | WG-Cert-Portal        | Any-Trusted, Any-Optional | Firebox      | tcp:4126                   |    |
| 5          | 10          | WatchGuard Web UI             | WG-Fireware-XTM-WebUI | Any-Trusted, Any-Optional | Firebox      | tcp:8080                   |    |
| 6          | 🗸 🌄 🔘 🖳     | Ping 💮                        | Ping                  | Any-Trusted, Any-Optional | Any          | icmp (type: 8, code: 255)  |    |
| 7          | 🗸 🌄 🔘 🖳     | DNS                           | DNS                   | Any-Trusted, Any-Optional | Any-External | tcp:53 udp:53              |    |
| 8          | Ø 🌑         | POP3-proxy                    | POP3-proxy            | Any-Trusted               | 172.16.1.51  | tcp:110 tcp:995 (tis)      |    |
| 9          | 10          | WatchGuard                    | WG-Firebox-Mgmt       | Any-Trusted, Any-Optional | Firebox      | tcp:4105 tcp:4117 tcp:4118 |    |
| 10         | V 🖓 🕲 🖳     | Cutgoing                      | TCP-UDP               | Any-Trusted, Any-Optional | Any-External | tcp:0 (Any) udp:0 (Any)    |    |
|            |             |                               |                       |                           |              |                            |    |
|            |             |                               |                       |                           |              |                            |    |
|            |             |                               |                       |                           |              |                            |    |
|            |             |                               |                       |                           |              |                            |    |
| <          |             |                               |                       |                           |              |                            |    |
|            |             |                               |                       |                           |              | Fireware OS v              | 11 |

| ファイアウォール     Mobile VPN with     モデム       順序 / アクション     ワイヤレス     フィルタ: なし     アイレス: なし       順序 / アクション     ARPエントリ     ARPエントリ     Any-Trusted, Any-Optional     Any-External       ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・   | フィイアウォール       Mobile VPN with       モデム         ワイヤレス       ワイヤレス         NAT       ARPエントリ         ME序 / アクション       アクション         ● HTTP-       ルート         ● HTTP-       助的ルーティング         ● HTTP-       動的ルーティング         ● HTTP-       動的ルーティング         ● Watch       ゲートウェイワイヤレスコントローラ         ● DNS       DNS         ● Watch       WG-Firebox-Mgmt         ● DNS       DNS         ● Watch       WG-Firebox-Mgmt         ● Outgoing       TCP-UDP  |             | / 十 入   筆 構成   |  | . ?  |  |
|---|---|-------------|--|--|--|--|
| 開発・アクジョン ARPエントリ… ARPエントリ… ルート… か Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Firebox Any-Trusted, Any-Optional Firebox Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Firebox Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Firebox Any-Trusted, Any-Optional Any-External Any-External Any-Trusted, Any-Optional Any-External Any-External Any-Trusted, Any-Optional Any-External Any-External Any-Trusted, Any-Optional Any-External | ARPエントリ…<br>ルート…<br>動的ルーティング…<br>Watch<br>シートウェイワイヤレスコントローラ…<br>マルチキャスト…<br>DNS<br>WatchGuard WG-Firebox-Mgmt TCP-UDP<br>ARPエントリ…<br>ルート…<br>動的ルーティング…<br>マルチキャスト…<br>DNS<br>ARPエントリ…<br>ルート…<br>動的ルーティング…<br>スルチキャスト…<br>DNS<br>ARPエントリ…<br>ルート…<br>動的ルーティング…<br>マルチキャスト…<br>DNS<br>ARPエントローラ…<br>スルチートウェイワイヤレスコントローラ…<br>マルチキャスト…<br>DNS<br>ARPエントローラ…<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Firebox<br>Any-Trusted, Any-Optional Any<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Any-External<br>Any-Trusted, Any-Optional Any-External | ファイアウォール Mo | bile VPN with I モデム<br>ワイヤレス<br>NAT  |  | フィルタ: なし   | ~ 7 7  |
| V Dutgoing TCP-UDP Any-Trusted, Any-Optional Any-External   | V Dutgoing TCP-UDP Any-Trusted, Any-Optional Any-External   |             | <ul> <li>ARPエント</li> <li>● FTP-pr<br/>● HTTP-<br/>● HTTP-</li> <li>財的ルーテ</li> <li>Watch</li> <li>ゲートウェ</li> <li>● Watch</li> <li>マルチキャ</li> <li>④ DNS</li> <li>● WatchGuard</li> </ul> | リ<br>イング<br>イワイヤレスコントローラ<br>スト<br>DNS<br>WG-Firebox-Mgmt | изтат<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional | Any-External<br>Any-External<br>Any-External<br>Firebox<br>Firebox<br>Any<br>Any-External<br>Firebox |
|   |   |             | Outgoing   | TCP-UDP  | Any-Trusted, Any-Optional  | Any-External   |

# ネットワークの構成画面が開きます。

| <b>リモートでイン</b> | ターフェイスを構成: ミック | スルーティング モード |             |           |          |    | 1 |
|----------------|----------------|-------------|-------------|-----------|----------|----|---|
| インターフェ         | 名前 (エイリアス)     | 種類          | IPv4 アドレス   | IPv6 アドレス | NIC 構成   | 構成 |   |
| 0              | External       | 外部          | DHCP        |           | 自動ネゴシエート |    |   |
| 1              | Trusted        | 信頼済み        | 10.0.1.1/24 |           | 自動ネゴシエート |    |   |
| 2              | Optional-1     | 無効          |             |           | 自動ネゴシエート |    |   |
| 3              | Optional-2     | 無効          |             |           | 自動ネゴシエート |    |   |
| 4              | Optional-3     | 無効          |             |           | 自動ネゴシエート |    |   |
| 5              | Optional-4     | 無効          |             |           | 自動ネゴシエート |    |   |
| 6              | Optional-5     | 無効          |             |           | 自動ネゴシエート |    | 1 |

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。

| 順序 / アクション ポリシー名 ポ<br>② こ ③ ② 二 ④ CFTP-proxy FTP-proxy<br>② こ ● FTP-proxy HTTP-proxy<br>● HTTP-proxy HTTP-proxy<br>● HTTPS-prox HTTPS-prox<br>● WGC-Cert-Po   | シーの種類<br>Any-Trusted, Any-Opi<br>Any-Trusted, Any-Opi     | フィルタ:<br>送信先<br>rtional Any-External | なし ~ ア<br>ポート              |
|---|---|--------------------------------------|----------------------------|
| 順序 / アクション ポリシー名 ポ  | シーの種類 送信元<br>Any-Trusted, Any-Opi<br>Any-Trusted, Any-Opi | itional Any-External                 | ポート                        |
| Image: System | Any-Trusted, Any-Op<br>Any-Trusted, Any-Op                | tional Any-External                  | 4                          |
| Image: Solution of Solut  | Any-Trusted, Any-Opt                                      |                                      | ICp.21                     |
|   |   | tional Any-External                  | tcp:80                     |
| VatchGuard Certificate Portal WG-Cert-Po  | Any-Trusted, Any-Opt                                      | tional Any-External                  | tcp:443                    |
|   | Any-Trusted, Any-Opt                                      | tional Firebox                       | tcp:4126                   |
| 🗸 🌑 🛛 🗢 WatchGuard Web Ul 🛛 🛛 WG-Firewar  | -XTM-WebUI Any-Trusted, Any-Opt                           | utional Firebox                      | tcp:8080                   |
| 🗸 🌄 🕘 🖳 🔗 Ping  Ping  | Any-Trusted, Any-Opt                                      | utional Any                          | icmp (type: 8, code: 255)  |
| 🗸 🌄 🕘 🖳 🖨 DNS 🛛 DNS   | Any-Trusted, Any-Opt                                      | tional Any-External                  | tcp:53 udp:53              |
| 👰 🌒 💋 РОРЗ-ргоху РОРЗ-ргоху   | Any-Trusted   | 172.16.1.51                          | tcp:110 tcp:995 (tls)      |
| VG-Firebox 🖤 🖉 🖉  | Igmt Any-Trusted, Any-Opt                                 | tional Firebox                       | tcp:4105 tcp:4117 tcp:4118 |
| V 💭 🌑 🖳 🗰 Outgoing TCP-UDP  | Any-Trusted, Any-Opt                                      | itional Any-External                 | tcp:0 (Any) udp:0 (Any)    |
|   |   |                                      |                            |
|   |   |                                      |                            |
|   |   |                                      |                            |

構成パスフレーズを入力して[OK]をクリックします。

| 管理者権限を持つユーザ<br>ださい。 | ~のユーザー名とパスフレーズを指定してく | ОК    |
|---------------------|----------------------|-------|
| ₽ アドレスまたは名前:        | 10.0.1.1             | キャンセル |
| 管理者のユーザー名:          | admin                |       |
| 管理者のパスフレーズ:         | ••••••               |       |
| 認証サーバー:             | Firebox-DB ~         |       |

コンフィグをファイルに保存するためのダイアログも開きます。



設定のバックアップのため、ファイルも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。

| <ul> <li>C:¥Users¥eueda¥Documen</li> <li>ファイル 編集 表示 セットアップ</li> <li>二 回 回 日 マー ×</li> <li>ファイアウオール Mobile VPN w</li> </ul> | ts¥My WatchGuard¥configs¥T30-Minatoku-Branch.xml- Fireware XTM Policy Manager<br>7 ネットワーク FireCluster VPN セキュリティサービス ヘルプ<br>  操 💐 🐘   🗈 🦛 🎉   💷 🖉 🌮   🗔 🔍 ?  |  |
|--|--|--|
| J順序 ✓ アクション<br>1 ✓ ● ℃ FTF<br>2 ✓ ◆ Wa<br>3 ✓ ↔ Wa<br>5 ✓ ☆ Out  | 管理者権限を持つユーザーのユーザー名とパスフレーズを指定してくたさい。       OK         アドレスまたは名前:10.0.1.1       ・         管理者のユーザー名: admin       ・         管理者のパスフレーズ:       ・         認証サーバー: Firebox-DB       ・         構成をアップロードしています       ・ | ▼ ア.<br>送信先<br>Any-External<br>Firebox<br>Any<br>Firebox<br>Any-External |
| •  | m  | Fireware XTM v11.10.5  |

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。1

<sup>1</sup> 保存された構成ファイルは[ファイル] [開く] [構成ファイル]から読み込ませることができます。

#### 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 Firebox 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
- Wi-Fi Cloud や TDR の Threat Sync のクラウドにアクセスする際の名前解決
- 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

#### DNS の設定

ポリシーマネージャの <u>ネットワーク</u> — <u>構成</u> をクリックし、ネットワーク構成の 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、<u>追加</u>ボタンをクリックで追加できます。

| ネットワーク構成            |                                 |             |             |                  |             |               |              |              |                         |
|---------------------|---------------------------------|-------------|-------------|------------------|-------------|---------------|--------------|--------------|-------------------------|
| ンターフェイス リン          | ンクアグリゲーション                      | ブリッジ VLAN   | ループバック      | Bridge Protocols | WINS/DNS 動約 | DNS 複数 WAN    | Link Monitor | SD-WAN PPPoE |                         |
| DNS (Domain Name S  | ystem) サーバー                     |             |             |                  |             |               |              |              |                         |
| ドメイン名:              |                                 |             |             |                  |             |               |              |              |                         |
| DNS サーバー: 8.8.      | 8.8                             |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             | - 11-0 ID 751 | フをコカオる       |              | $\overline{\mathbf{v}}$ |
|                     |                                 | 20 km       | <b>1</b> 44 | 20184            | DINS 9      |               | X2/132       |              |                         |
|                     |                                 | 36.00       | · · · · · · | 目引以先             | Pアドレ        | 2             |              |              |                         |
| DNS 転送を有効           | i化する <mark>(</mark> Fireware OS | v11.12.2以降) |             |                  |             | (IPv4または)     | Pv6アドレス)     |              | -                       |
| 選択したインター            | フェイスをリッスンす                      | 3           | $\sim$      | 選択               |             |               |              |              |                         |
| 条件付き転送              |                                 |             |             |                  |             |               | ОК           | キャンセル        |                         |
| ドメイン                |                                 | DNS サーバー    |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 | 18 hD       | 编集          | 晋山殷全             |             |               |              |              |                         |
|                     | 1 A3 at at at 11 at 7           | ALC: N      | *m / C      | PIZZO            |             |               |              |              |                         |
| DNS 転送 ロ ク it       | 録を有効化する                         |             |             |                  |             |               |              |              |                         |
| WINS (Windows Inter | net Naming Service) サ           | - //-       |             |                  |             |               |              |              |                         |
| WINS サーバー:          |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             |               |              |              |                         |
|                     |                                 |             |             |                  |             | (             | or +         | a 2147 II.   | ヘルプ                     |

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。

| 2.292 |  |  |
|-------|--|--|
|       |  |  |

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]をクリックします。

| するインター | フェイスを選択して、構成をク           | ? リックします。 正しく操<br>マールーティング チード | 作するには、 XTM デバイス・ | の外部インターフェイスを制 | #成する必要があります。 |    |
|--------|--------------------------|--------------------------------|------------------|---------------|--------------|----|
|        | メージェイバビョス。<br>名前 (エイリアス) | 通知                             | Pv4 7 FL 7       | PV67FLZ       | NIC 建成       | 標成 |
| 0      | Ontional                 | 任音                             | 10 0 0 1/24      |               | 自動ネゴシェート     |    |
| 1      | Trusted-1                | 信頼済み                           | 10 0 1 1/24      |               | 自動ネゴシエート     |    |
| 2      | Trusted-2                | 信頼済み                           | 10.0.2.1/24      |               | 自動ネゴシエート     |    |
| 3      | Trusted-3                | 信頼済み                           | 10.0.3.1/24      |               | 自動ネゴシエート     |    |
| 4      | External-1               | 外部                             | DHCP             |               | 自動ネゴシエート     |    |
| 5      | External-2               | 你都                             | DHCP             |               | 目動ネコジェート     |    |
| 6      | Optional-5               | 無効                             |                  |               | 自動ネゴシエート     |    |
| 7      | Optional-6               | 無効                             |                  |               | 自動ネゴシエート     |    |
|        |                          |                                |                  |               |              |    |
|        |                          |                                |                  |               |              |    |

インターフェイスの詳細を設定できる画面が開きます。

| ] IPv6 セカンダリ MAC | アクセス制御 ¥田           |            |        |      |
|------------------|---------------------|------------|--------|------|
| ンターフェイス名 (エイリア   | アス): External       |            |        |      |
| ンターフェイスの説明:      |                     |            |        |      |
| ンターフェイスの種類:      | 外部                  |            |        | ~    |
| ◯ 静的 ₽の使用        |                     |            |        |      |
| <b>Pアドレス</b> :   |                     |            |        |      |
| デフォルト ゲートウェ      | 1 : [               |            |        |      |
| の DHCP クライアントの様  | E用                  |            |        |      |
| クライアント           |                     |            |        |      |
| ホスト名             |                     |            |        |      |
| ホスト P            |                     |            |        |      |
| □リース時間: 8時       | акн.<br>Ш           |            |        |      |
| □ DHCP 強制更新を有    | :効化する (Fireware OS) | v11.8.1以降) |        |      |
| 共有 = ~ :         |                     |            |        |      |
| ◯ PPPoE の使用      |                     |            |        |      |
| ③ Pアドレスの自動取      | 御                   |            |        |      |
| 〇 次の IP アドレスを使   | (用:                 |            |        |      |
| ユーザー名:           |                     |            |        |      |
| パスワード:           |                     |            |        |      |
| パスワードの再入力:       |                     |            |        |      |
|                  |                     |            | 1 乙四苯基 | コパティ |
|                  |                     |            |        |      |

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。

| インターフェイス名 <mark>(</mark> エイリア | A): External |   |
|-------------------------------|--------------|---|
| インターフェイスの説明:                  |              |   |
| インターフェイスの種類:                  | 外部           | ~ |
|                               |              |   |
| ● 静的 IP の使用                   |              |   |
| <ul> <li>静的 Pの使用</li> </ul>   |              |   |

# 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。

| ホスト名             |  |
|------------------|--|
| ホスト IP           |  |
| ● IP アドレスの自動取得   |  |
| ◯ 次の IP アドレスを使用: |  |
| □ リース時間: 8時間     |  |
|                  |  |

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。

| ● IP アトレスの自動取得  |  |        |
|---|--|--------|
| ○次の IP アドレスを使用:   |  | $\sim$ |
| ユーザー名:  | username@provider.name   |        |
| パスワード:  | •••••  |        |
| パスワードの再入力・  |  |        |
|   | I¥\$   | プロパティ  |
| の指定によってはより詳細な   | い設定が必要になることがあります。  |        |
|   |  |        |
| 細プロパティ]をクリックし、指   | 定の項目を設定してください。   |        |
| PPPoE プロパティ   | ×  |        |
| 接統設定  |  |        |
| ■ PPPoE検出パケット内でのホスト固有タグの使用  |  |        |
| ● 常にオン  |  |        |
| PPPoE の初期化を再試行する間隔  | 60 <b>↓</b> 秒  |        |
| ○ ダイヤルオンデマンド  | Manual ( 1997  |        |
| アイドル タイムアウトまでの時間  | 20 🌩 😚   |        |
|   | ана ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (  |        |
| └─」LCPエコー要求を使用して、大われたPPPoE接続を持  |  |        |
| ✓ LCPエコー要求を使用して、矢和れたPPPeb接続を把<br>LCPエコーを再試行する回数   | 6 🗘 🗆  |        |
| ▲ LCPエコー委家を使用して、大われたPPPoL38旅を作<br>LCPエコーを再試行する回数<br>LCPエコー タイムアウトまでの時間  | 6 💭 🛛<br>10 🜩 秒  |        |
| ▲ LCPエコー委束を使用して、矢われたPPPoL28前を#<br>LCPエコーを再試行する回数<br>LCPエコータイムアウトまでの時間           □ 自動再起動が設定された時間         日曜日         :         0   | 6 	 □<br>10 	 ₱₽<br>↓ : 0 	 0 	 (HH:MM)  |        |
| <ul> <li>└ LCPエコーを再試行する回数</li> <li>LCPエコーを再試行する回数</li> <li>LCPエコーを有試行する回数</li> <li>LCPエコータイムアウトまでの時間</li> <li>自動再起動が設定された時間</li> <li>日曜日 : 0</li> <li>認証設定</li> </ul>   | 6 → □<br>10 → ₽₽<br>+ : 0 + (HH:MM)  |        |
| <ul> <li>✓ LCPエコー要求を使用して、大われたPPPoL2(数約を作<br/>LCPエコーを再試行する回数<br/>LCPエコータイムアウトまでの時間</li> <li>□ 自動再起動が設定された時間</li> <li>□ 日曜日</li> <li>: 0</li> <li>2証設定</li> <li>サービス名:</li> </ul>   | 6 	 □<br>10 	 ₩<br>÷ : 0 	 (HH:MM)   |        |
| ▲ LCPエコー要求を使用して、矢われたPPPoL26(前を作<br>LCPエコーを再試行する回数<br>LCPエコータイムアウトまでの時間<br>自動再起動が設定された時間 日曜日 : 0<br>8証設定<br>サービス名:<br>アクセスコンセントレータの名前:   | 6 	 □<br>10 	 ↓<br>÷ : 0 	 ↓ (HH:MM)   |        |
| <ul> <li>■ LCPエコー委家を使用して、矢われたPPPoL投版を作<br/>LCPエコーを再試行する回数</li> <li>■ 自動再起動が設定された時間</li> <li>□ 自動再起動が設定された時間</li> <li>□ 回転</li> <li>□ の</li> <li>□ 0</li> <li>□ 0</li></ul> | 6 € □<br>10 € ₩<br>↓ : 0 \$ (HH:MM)  |        |
| CLCPエコー委束を使用して、矢われたPPPoL26(取を用<br>LCPエコーを再試行する回数<br>LCPエコーを再試行する回数<br>自動再起動が設定された時間 日曜日 : 0 認証設定<br>サービス名:<br>アクセスコンセントレータの名前:<br>認証の再試行 3<br>認証の気イムアウト: 20   | 6 € □<br>10 € ₩<br>÷ : 0 \$ (HH:MM)  |        |
| <ul> <li>✓ LCPエコー要求を使用して、矢われたPPPoL投資を指<br/>LCPエコーを再試行する回数     </li> <li>▲動再起動が設定された時間 日曜日 : 0</li> <li>認証設定         <ul> <li>サービス名:</li> <li>アクセスコンセントレータの名前:</li> <li>認証のタイムアウト:</li> <li>20</li> </ul> </li> <li>その他</li> </ul>   | 6 - □<br>10 - +><br>+ : 0 + (HH:MM)  |        |
| <ul> <li>✓ LCPエコー要求を使用して、大われたPPPoL投版を構<br/>LCPエコーを再試行する回数</li> <li>▲ 自動再起動が設定された時間 日曜日 ●: 0</li> <li>8証設定</li> <li>サービス名:</li> <li>アクセスコンセントレータの名前:</li> <li>認証の項試行</li> <li>3 認証のタイムアウト: 20</li> <li>その他</li> <li>● PPPoE ネゴシエージョンの間に PPPoE クライアント</li> </ul>  | 6 🛫 🖬<br>10 € 秒<br>↓ : 0 ÷ (HH:MM)<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●<br>●   |        |
| <ul> <li>▲ LCPエコー委家を使用して、矢われたPPPoL28前を相<br/>LCPエコーを再試行する回数</li> <li>▲ 自動再起動が設定された時間 日曜日 : 0</li> <li>認証設定</li> <li>サービス名:</li> <li>アクセス コンセントレータの名前:</li> <li>認証の承ば行</li> <li>認証のタイムアウト:</li> <li>20</li> <li>その他</li> <li>● PPPoE ネゴジエーションの間に PPPoE クライアント</li> <li>● PPPoE ネゴジエーションの間に PPPoE クライアント</li> </ul>  | <ul> <li>6 → □</li> <li>10 → 秒</li> <li>÷ ・ 秒</li> <li>の酔的 Pアドレスを送信する</li> <li>の酔的 Pアドレスを送信しない</li> </ul>  |        |
| ▲ LCPエコーを再試行する回数         LCPエコーを再試行する回数         上CPエコーを再試行する回数         自動再起動が設定された時間         日曜日         ・         御話設定         サービス名:         アクセスコンセントレータの名前:         認証の算試行         認証のタイムアウト:         20         その他         ● PPPoE ネゴシエーションの間に PPPoE クライアント         ● PPPoE ネゴシエーションの間に PPPoE クライアント         ● PPPoE ネゴシエーションの間に PPPoE クライアント   | <ul> <li>6 → □</li> <li>10 → 秒</li> <li>÷ : 0 ÷ (HH:MM)</li> <li>◆</li> <li>◆</li> <li>か</li> <li>秒</li> <li>の締め Pアドレスを送信する</li> <li>の締め Pアドレスを送信しない</li> <li>アンドの締め Pアドレスの送信および強制 (Fireware OS v11.8.1 以降)</li> </ul> |        |

### 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。

| R インターフェイスの        | )設定 - インターフェイス番号 0<br>ンダリ ACアクセス制御 詳細                             | ^ |
|--------------------|---|---|
| このインターフ<br>クをルーティン | ェイスで使う IP アドレスを追加してください。それらのアドレスは正しいネットワークヘトラフィッ<br>グする目的で用いられます。 |   |
|                    | 通加         通加           1         1           1         1         | l |
|                    | IPアドレス: ~ ~ 編集  |   |
|                    |   |   |
|                    | OK キャンセル  |   |
|                    | OK キャンセル ヘルプ  | ~ |


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、ポリシーマネージャの*ネットワーク — 構成*の画面から行ないます。

インターフェイスー覧より、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。

| ンターフェ  | 名前 (エイリアス) | 種類             | IPv4 アドレス           | IPv6 アドレス | NIC構成    | 権成 |
|--------|------------|----------------|---------------------|-----------|----------|----|
| 0      | Optional   | 任意             | 10.0.0.1/24         |           | 自動ネゴシエート |    |
| 1      | Trusted-1  | 信頼済み           | 10.0.1.1/24         |           | 自動ネゴシエート |    |
| 2      | Trusted 2  | 信頼道の           | 10.0.2.1/24         |           | 自動ホリンエード |    |
| 3      | Futoroal 1 | 1言親()資め<br>品加2 | 10.0.3.1724<br>DHCD |           | 自動ネコンエート |    |
| 4<br>c | External 2 | 51-51          | DHCP                |           | 自動ネコンエート |    |
| 6      | Ontional-5 | 91-10<br>细动    | DITCH               |           | 自動ネゴジェート |    |
| 7      | OptionaL6  | 無効             |                     |           | 自動ネゴジェート |    |
|        |            |                |                     |           |          |    |

### 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。

| V4 IPv6 セカンダリ MACアクセ | セス制御 詳細 |   |
|----------------------|---------|---|
| インターフェイス名 (エイリアス):   | Trusted |   |
| インターフェイスの説明:         |         |   |
| インターフェイスの種類:         | 信頼済み    | ~ |
| IPアドレス: 10.0.1.1/    | 24      | ~ |

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。

| インターフェイス名 (エイリア  | 'ス):   Trusted |  |
|--|----------------|--|
| インターフェイスの説明:<br>インターフェイスの種類:                                       | 信頼済み           |  |
| IP アドレス: 10.0<br>の DHCP を無効にする                                     | .1.1/24        | <ul> <li>アドレス範囲の追加</li> </ul>                                  |
| <ul> <li>DHCPサーバーの使用<br/>アドレスの範囲を最大 6</li> <li>アドレスプール:</li> </ul> | つまで設定できます。     |  |
| 開始   |                | 開始アドレス: 10.0.1.100<br>↓<br>終了アドレス: 10.0.1.199<br>↓<br>Ⅲ除<br>Ⅲ除 |
|  |                | <u>ОК</u> キャンセル  |
| 予約 アドレス:<br>予約タ  | 子約             |  |
|  |                |  |
|  |                |  |

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]ボタンがあります。これをクリックします。

| 10.0.1.100 10.0.1.199 編編<br>声称 アドレス:<br>予約名 予約 P MAC アドレス 通路  | 開始 IP                                | <b>終了</b> | P           | ii hi   |
|---|--------------------------------------|-----------|-------------|---|
| 予約 アドレス:       予約名       予約名       予約日       MAC アドレス       通約       調約       111   | 10.0.1.100                           | 10.0.1    | .199        | 福集  |
| 予約 アドレス:<br>予約 名 予約 P MAC アドレス 編編<br>研修 研修 開設 日本 100000000000000000000000000000000000   |                                      |           |             |   |
| <del>予約 アドレス:</del><br>予約名 予約 P MAC アドレス 通道<br>編編<br>1111111111111111111111111111111111                                       |                                      |           |             |   |
| 予約 アドレス:<br>予約 A 予約 P MAC アドレス 通知<br>第5<br>11111111111111111111111111111111111  |                                      |           |             |   |
| 予約 アドレス:         通数           予約名         予約P         MAC アドレス         通数           編編         1111         1111         1111 |                                      |           |             |   |
| 予約名     予約P     MACアドレス     通註       編録     調節  | 予約 アドレフ                              |           |             |   |
| 《編 5<br>日初日   | 1.0571.05%                           |           |             |   |
|   | 子約名                                  | 予約IP      | MAC アドレス    | i£ ht   |
|   | 子約名                                  | 予約P       | MAC アドレス    | <b>) () () ()</b> () () () () () () () () () () () () ()                                      |
|   | ት በ / ት ፡፡<br>ት ክ ፡፡                 | 子約P       | MACアドレス     | <b>注血加</b><br>第二第<br>第11月<br>第11月   |
|   | <b>予約</b> 名                          | 予約IP      | MACアドレス     | <b>注度加</b><br>等請 練<br>尚刊 PA   |
|   | 子約名                                  | 子約P       | MACアドレス     |   |
|   | 子約名                                  | <b>平約</b> | MAC アドレス    | <b>注 血 如</b>  |
| 」 2時間 8時間   | 子約名<br>子約名                           | 予約IP      | MAC 7 F L ス | ()<br>)<br>)<br>)<br>()<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>)<br>) |
|   | 子約名<br>リース時間 8時間<br>Paiの社、15、199010社 |           | MAC 7 F L Z | <b>4</b><br>全部<br>(1)<br>(1)<br>(1)<br>(1)<br>(1)<br>(1)<br>(1)<br>(1)<br>(1)<br>(1)          |

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。

| ドメイン名:  | ļ          |              |          |          |            |
|---------|------------|--------------|----------|----------|------------|
| 6       | CDNS サーバー  |              | <u>د</u> | <b>3</b> | 10         |
| ſ       |            |              |          |          | 兼          |
|         | 🚔 DNS サーバ・ | 一の IP アドレスを指 | 定        | 百        | 川路余        |
| WINS サー | DNS サーバー   | 10.0.100.100 | Ŧ        | ]<br>    | <u>र</u> ) |
|         |            |              |          | ji ji    | 10         |
|         |            |              |          | \$       | 躾          |
|         |            | ОК           | キャンセル    |          | 唯          |

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。

| SD-WAN PPPOE | 4    |
|--------------|------|
|              |      |
| -フェイス        | 追加   |
|              | 编集   |
|              |      |
|              | 削除   |
|              | 7113 |

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。

|                       | & U            |             |          |  | ٦Ē |
|-----------------------|----------------|-------------|----------|--|----|
| 名前(Alias):            | Trusted-Bridge |             |          |  |    |
| 說明:                   |                |             |          |  |    |
| セキュリティ ゾー             | ン: 信頼済み        |             |          | -  |    |
| ₽アドレス:                | 10.0.11.1/24   |             |          | ◄]   |    |
| 🔘 DHCP を無効I           | こする            |             |          |  |    |
| OHCP サーバー             | - の使用          |             |          |  |    |
| アドレスの範                | 囲を最大6つまで設定     | できます。       |          |  | Ξ  |
| アドレスプ                 | - 1V :         | p.          |          |  |    |
| 開始旧                   |                | <b>终</b> 了  | P        | <u>نڈ میں</u>                                      |    |
| 10.0.11.100           |                | 10.0.1      | 11.199   | 1  |    |
|                       |                |             |          | 編集   |    |
|                       |                |             |          | 編集<br>削除   |    |
|                       |                |             |          | 編集<br>削除   |    |
|                       |                |             |          |  |    |
|                       |                |             |          |  |    |
|                       |                |             |          | 編集<br>肖明除  | 11 |
|                       | 7.             |             |          | 《編集<br>肖·]除  |    |
| <u>予約 アドレ</u><br>子約 タ | 7:             | 子約回         | MAC PELZ | 編集<br>肖明除  |    |
| 子約 アドレ:<br>子約名        | 7:             | ታኑን<br>P    | MAC アドレス | 編集<br>肖明除<br>〕<br>〕<br>注加                          |    |
| <u>予約 アドレ:</u><br>予約名 | 7:             | <br> 予約₽    | MAC アドレス | 編集<br>肖明除  |    |
| <u>予約 アドレ</u><br>子約名  | 7:             | <u>ት</u> ዩን | MAC アドレス | 第編集<br>肖以除       肖以除       「追加」       編集       肖以除 |    |

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。

| /ターフェイス      | リンクアグリゲー  | ション ブリッジ VLAI | N ループバック Bridge P | otocois WINS/DNS | 動的 DNS 複数 WAN | Link Monitor SD-WAN F | PPoE |
|--------------|-----------|---------------|-------------------|------------------|---------------|-----------------------|------|
| ーカル エリア      | ネットワークのブリ | ッジの設定         |                   |                  |               |                       |      |
| 前 (Alias)    | ソーン       | IPv4 アドレス     | IPv6 アドレス         | DHCP             | Secondary     | インターフェイス              | 追加   |
| usted-Bridge | 信頼済み      | 10.0.11.1/24  |                   | Local            |               |                       | 福集   |
|              |           |               |                   |                  |               |                       | 削除   |
|              |           |               |                   |                  |               |                       |      |

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。

| There is a second state | (2,2, -2, )   (4- | en sterright 19440 |              |              |       |       |
|-------------------------|-------------------|--------------------|--------------|--------------|-------|-------|
| インターフェ                  | イス名:              | Trusted-2          |              |              |       |       |
| インターフェ                  | イスの説明:            |                    |              |              |       |       |
| インターフェ                  | イスの種類             | ブリッジ               |              |              |       | *     |
| 選択したブ                   | リッジ インター          | -フェイスでのトラフ・        | ィックの送受信      |              |       |       |
| メンバー                    | ソーン               | 名前                 | IPv4 Address | IPv6 Address | DHCP  | セカンダリ |
| ۲                       | 言頼済み              | Trusted-Bridge     | 10.0.11.1/24 |              | Local |       |
|                         |                   |                    |              |              |       |       |

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、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。

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。

| <sup>PV4</sup>   IPv6   セカンタ | 「リ MACアクセス制御 詳細     |   |
|------------------------------|---------------------|---|
| インターフェイス名                    | 5 (エイリアス): Optional |   |
|                              |                     |   |
| インターフェイスの                    | )說明:                |   |
| インターフェイスの                    | D種類: 任意             |   |
| IPアドレス:                      | 10.100.10.1/24      | <b>•</b>                                |
|                              |                     | 17 - 17 - 17 - 17 - 17 - 17 - 17 - 17 - |

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 (1-1 NAT)

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 1-1 NAT(ワントゥワンナット)です。

ポリシーマネージャの <u>ネットワーク</u> — <u>NAT</u> 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「単ー IP」(NAT するサーバーが一台)を例にします。

| 🌉 1-1マッピングの追加                                      | ×                        |                   |
|--|--------------------------|-------------------|
| 種類<br>マップの種類: 単一 IP 〜<br>単一の IP アドレスを別の IP アドレスにマッ | プします                     |                   |
| 構成<br>インターフェイスと相互に変換する 2 つの IP ア                   | ドレスを選択します。               |                   |
| インターフェイス: External 〜<br>NAT ベース: 10.0.0.1          | Real ベース: 10.100. 10.101 | サーバーのローカル IP アドレス |
| ◆<br>外部インターフェイスの IP アドレス                           | <u></u>                  |                   |

インターフェイス:Firebox 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

1-1 NATを設定したら、それに合致したポリシーでアドレス変換の対象となります。たとえば内部の Web サーバーに外部からアクセスさせるような HTTP-Incoming ポリシーを作成し、それに合致し たトラフィックに適用されます。ファイアウォールの章で「ポリシー追加 (外側から内側へ)」をご覧くだ さい。

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

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。



ポリシーマネージャの <u>ネットワーク</u> — <u>ルート</u> 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。

| ーティング先 | ゲートウェイ | メトリッ | インターフェイス | 追加     |
|--------|--------|------|----------|--------|
|        |        |      |          | 編集     |
|        |        |      |          | 置则形余   |
|        |        |      |          | インボート  |
|        |        |      |          | エクスポート |
|        |        |      |          |        |
|        |        |      |          |        |
|        |        |      |          |        |
|        |        |      |          |        |
|        |        |      |          |        |

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。

| ルートタイプ:      | 静的ルート ジョン・ション・ション・ション・ション・ション・ション・ション・ション・ション・シ |
|--------------|---|
| 宛先タイプ:       | ネットワーク⊫Pv4 〜                                    |
| ルーティング先:     | 192.168.111.0 /24                               |
| ゲートウェイ:      | 10. 0 . 1 .254                                  |
| メトリック:       | 1   |
| □ インターフェイスの排 | iz: 📃 🗸 🗸                                       |

## 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 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

| 7 7 4 1 | / 補来 表示 セッ<br>▲ 🗁 🖶   🦁 ·<br>?ウォール Mobile | + X   ¥ 🗶 🗽   🗈 🦛 💰           | A 🗐 🖉 🔗 🗖 🔍 1              | ?                           |                      |                           |
|---------|---|-------------------------------|----------------------------|-----------------------------|----------------------|---------------------------|
|         |   |                               |                            | 2                           | フィルタ: なし             | ~ 7                       |
| 順序 /    | アクション                                     | ポリシー名                         | ポリシーの種類                    | 送信元                         | 送信先                  | ポート                       |
| 1       | 1   | ETP FTP                       | FTP                        | Any-Trusted                 | Any-External         | tcp:21                    |
| 2       | Ø 🔊 🛄                                     | HTTP-proxy                    | HTTP-proxy                 | Any-Trusted                 | Any-External         | tcp:80                    |
| 3       | Ø 🌄 🛄                                     | HTTPS-proxy                   | HTTPS-proxy                | Any-Trusted                 | Any-External         | tcp:443                   |
| 4       | 1   | WatchGuard Gateway Wireless   | WG-Gateway-Wireless-Contr. | . Any-Trusted, Any-Optional | Firebox              | udp:2529                  |
| 5       | 1   | WatchGuard Authentication     | WG-Auth                    | Any-Trusted, Any-Optional   | Firebox              | tcp:4100                  |
| 6       | 1   | WG-Auth-WebBlocker            | WG-Auth                    | Any-Trusted, Any-Optional   | Firebox              | tcp:4100                  |
| 7       | 1   | WatchGuard Certificate Portal | WG-Cert-Portal             | Any-Trusted, Any-Optional   | Firebox              | tcp:4126                  |
| 8       | 1   | WatchGuard Web UI             | WG-Fireware-XTM-WebUI      | Any-Trusted, Any-Optional   | Firebox              | tcp:8080                  |
| 9       |   | (c) Ping                      | Ping                       | Any-Trusted, Any-Optional,  | Any                  | icmp (type: 8, code: 255) |
| 10      | 1   | WatchGuard                    | WG-Firebox-Mgmt            | Any-Trusted, Any-Optional,  | Firebox              | tcp:4105 tcp:4117 tcp:41. |
| 11      |   | WG-Cloud-Managed-WiFi         | WG-Cloud-Managed-WiFi      | Any-Trusted                 | *.mojonetworks.com,  | tcp:80 tcp:443 udp:3851   |
| 12      | 15  | Any-External                  | Any                        | Any-Trusted                 | Any-External         | any                       |
| 13      | 1   | Any-Optional                  | Any                        | Any-Optional                | Any-Trusted, Any-Ext | any                       |
| 14      | 1   | Any-Trusted                   | Any                        | Any-Trusted                 | Any-Trusted          | any                       |

ポリシーー覧の主な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      |

| 既存のオ  | ポリシーを変<br>をクリックし             | 更する際には、該当のポリ<br>ます。  | 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                           |
|---|------------------------------|--|--|--|
| ペリシー<br>□ IP> (+ =                                      | -の追加は                        | + ボタンをクリックしま   |  |  |
| ■【 C:¥U<br>ファイル<br>■ 加<br>ファイア                          | İsers¥tsuto¥Doci<br>編集 表示 セ: | uments¥My WatchGuard¥configs<br>ットアップ ネットワーク FireClust<br>・ X  | ¥T50-W-kamiyacho-46.xml *-<br>ter V <u>P</u> N セキュリティサービス<br><b>ぶ ぷ   □] <i>足 බ</i>   □ </b>   | Fireware Policy ー ロ ×<br>ペルプ<br><b>、 ?</b> |
| /////   | 24 70 MODILE                 | e VPN with IPSec   |  |  |
|   |                              |  | フィルタ:  | al 🗸 🕅 🗸                                   |
| 順序 左  | アクション                        | ポリシー名  | フィルタ:<br>  ポリシーの種類   | なし         ア 了.           送信元         送信元  |
| J順序 /<br>1<br>2<br>3<br>4<br>5<br>5<br>7<br>3<br>3<br>9 | アクション                        | # 비 シー名<br>출 FTP-proxy<br>₩ HTTP-proxy<br>♥ HTTPS-proxy<br>₩ WatchGuard Certificate Portal<br>♥ WatchGuard Web UI<br>♥ Ping<br>➡ DNS<br>♥ WatchGuard<br>₩ Outgoing | フィルタ:<br>ポリシーの種類<br>FTP-proxy<br>HTTP-proxy<br>HTTPS-proxy<br>WG-Cert-Portal<br>WG-Fireware-XTM-WebUI<br>Ping<br>DNS<br>WG-Firebox-Mgmt<br>TCP-UDP | なし   |



<sup>2</sup> 保存の手順は、第三章の「設定の保存」の節をご覧ください

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)

ー例として、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。

| Finger            | ^ | ポリシー テンプ  | レート プロパティ                                     |                        |
|-------------------|---|-----------|---|------------------------|
| Gopher            |   | HTTP      |   |                        |
| HBCI              |   | ボート       | プロトコル   |                        |
| TTPS              |   | 80        | TCP   |                        |
| IDENT             |   |           |   |                        |
| IGMP              |   |           |   |                        |
| IPSec             |   | 說明        |   |                        |
| IRC               |   | HTTP パケット | フィルタを使用しても、トラフィッ                              | クに HTTP プロ 🥢           |
| Intel-Video-Phone |   | キシルールセ    | ットは適用されません。HTTPトラフ                            | イックにプロキ                |
| Kerberos-V4       |   | シを通用するに   | には、 HTTP プロキシ ポリシーを使用<br>、パブリック HTTP サーバーに対して | します。VPN の<br>のA 注意のオステ |
| Kerberos-V5       |   | とをお勧めしま   | オ。外部ホストはスプーフィングの                              | )可能性がありま               |
| BO I DAP          |   | す。正しい場所   | fから送信されたパケットかどうか、                             | WatchGuard It          |
| LDAP-SSL          |   | 確認できません   | 。HTTP 接続着信が拒否されたとき                            | に、ブロックさ                |
| and I also blacks | ~ | れたサイトのし   | ストに発信元 IP アドレスを追加する                           | 513 🕚                  |

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。

| f: HTTP-Outgoing $\rightarrow 2\pi$   | いりやすい名前を付ける   |
|---|---|
|   |   |
| リジュ ブロパティ 詳細  |   |
| FTP接続を…<br>た可しての「TP   |   |
| ¥@#   |   |
| Any-Trusted -   | → どこから  |
|   |   |
|   |   |
|   | AN LM   |
|   | <b>站道加山…</b> 納来 自如死   |
| 送信先   |   |
|   | 1.4   |
| 🙊 Any-External 📃  | → どこへ   |
| 🙊 Any-External —  | → どこへ   |
| X Any-External  | → どこへ   |
| 🛠 Any-External —  | → どこへ   |
| X Any-External —  | → どこへ   |
| X Any-External —  | → どこへ<br>追加<br>追知<br>調集<br>削除   |
| Route outbound traffic using  | → どこへ<br>i追加 編集 削除<br>SD-WAN Based Routing → (Fireware OS v12.3 or higher)  |
| Route outbound traffic using  | → どこへ<br>i 追加 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)   |
| Route outbound traffic using SD-WAN Action  | → どこへ<br>i追加 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>■ ■   |
| Route outbound traffic using SD-WAN Action  | → どこへ<br>i追加 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>■ ■ ■   |
| Route outbound traffic using SD-WAN Action  | → どこへ<br>i追加 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>■ ■ ■<br>F : Ginbal   |
| ※ Any-External Route outbound traffic using SD-WAN Action Application Control を有効にします Geolocation を有効化する  | → どこへ<br>i 追加 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>ぼ III (Fireware OS v12.3 or higher)<br>ぼ IIII (Fireware OS v12.3 or higher)<br>IIIII (Fireware OS v12.3 or higher)   |
| ※ Any-External Route outbound traffic using SD-WAN Action Application Control を有効にします Geolocation を有効化する このポリシーの IPS を有効にします  | → どこへ<br>i & 10 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>F : Global (Global ) ( |
| <ul> <li>Route outbound traffic using SD-WAN Action</li> <li>Application Control を有効にします</li> <li>Geolocation を有効化する</li> <li>このポリシーの IPS を有効にしま</li> </ul>                                     | → どこへ<br>i 追加… 編集… 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>す: Global ● ●<br>す<br>2 (Fireware OS v11.10 比)<br>す<br>2 (Fireware OS v11.10 比)<br>ま)  |
| <ul> <li>Route outbound traffic using SD-WAN Action</li> <li>Application Control を有効にします</li> <li>Geolocation を有効化する</li> <li>このポリシーの IPS を有効にしま</li> <li>帯域幅と時間クォータを有効化す</li> </ul>            | → どこへ<br>iù カロ 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)  |
| <ul> <li>Route outbound traffic using S</li> <li>SD-WAN Action</li> <li>Application Control を有効にします</li> <li>Geolocation を有効化する</li> <li>このポリシーの IPS を有効にしま</li> <li>帯域幅と時間クォータを有効化す</li> </ul> | → どこへ<br>i 追加… 編集 削除<br>SD-WAN Based Routing (Fireware OS v12.3 or higher)<br>f : Global ●<br>Global ●<br>f : Global ●<br>f : Market CS v11.10 以降)  |

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。

| C:¥             | Users¥user <sup>3</sup> | ¥Documents¥My Wa                      | atchGuard¥config     | s¥XTM23-HQ.xml *- Fi     | reware XTM Po   | olicy Manager     | l   | - 0 <b>X</b> |
|-----------------|-------------------------|---------------------------------------|----------------------|--------------------------|-----------------|-------------------|-----|--------------|
| ファイト            | レ 編集 表示                 | セットアップ ネット                            | ワーク V <u>P</u> N セキュ | ュリティサービス ヘルプ             |                 |                   |     |              |
| <b>注</b><br>ファイ | 星 🗁 🔙  <br>アウォール        | V7 + X   ₩ 🧶<br>Mobile VPN with IPSec | k 🗈 🎝 🕉              | 1 🗐 🖉 🔗 🗖 🔍              | ?               |                   |     |              |
| 順序              | アクション                   | ポリシー名                                 | ポリシーの種類              | 送信元                      | 送信先             | ポート               | PBR | App Control  |
|                 | 1                       | TTP FTP                               | FTP                  | Anv-Trusted Anv-Ontional | Anv-External 10 | ten 21            | な   |              |
|                 | 1                       | W HTTP-Outgoing                       | НТТР                 | Any-Trusted              | Any-External    | tcp:80            | な   | L            |
|                 | ~                       | watchGuard web                        | wG-Fireware-XI       | Any-Trusted Any-Optional | Firebox         | тер:виви          | 4   | C .          |
|                 | 1                       | Ping                                  | Ping                 | Any-Trusted Any-Optional | Any             | ICMP (type: 8, co | な   | L            |
|                 | 1                       | WatchGuard                            | WG-Firebox-Mgmt      | Any-Trusted Any-Optional | Firebox         | tcp:4105 tcp:411  | な   | L            |
|                 | 1                       | Cutgoing                              | TCP-UDP              | Any-Trusted Any-Optional | Any-External    | tcp:0 (Any) udp:  | な   | L            |

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。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、ポリシーを追加する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。

| GRE                        | ^ | ポリシー テンプ                         | レート プロパティ  |                                       |                          |
|----------------------------|---|----------------------------------|--|---------------------------------------|--------------------------|
| HBCI                       |   | HTTP                             |  |                                       |                          |
|                            |   | ボート                              | プロトコル  |                                       |                          |
| IDENT                      |   | 80                               | TCP  |                                       |                          |
| IPSec                      |   | 説明                               |  |                                       |                          |
| Kerberos-V4<br>Kerberos-V5 |   | HTTP パケット<br>キシ ルール セ<br>シを適用するに | フィルタを使用しても、<br>ットは適用されません。<br>は、HTTP プロキシ ポ <sup>1</sup> | トラフィックに H<br>HTTP トラフィック<br>Jシーを使用します | TTP ブロ<br>にブロキ<br>、VPN の |
| L2TP                       |   | 内側に保持する<br>とをお勧めしま<br>す。正しい場所    | パブリック HTTP サーノ<br>す。外部ホストはスプ<br>から送信されたパケッ               | いーに対してのみ許<br>ーフィングの可能性<br>トかどうか、Watch | 可するこ<br>がありま<br>Guard は  |
| Lotus-Notes                | ~ | 確認できません<br>れたサイトのリ               | 。日日P接続着信が把き<br>ストに発信元 IP アドレ                             | rされたときに、ノー<br>スを追加するよう                | 1993                     |

ポリシー名は分かりやすいものを付けるようおすすめします。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。

|  | 同じプロトゥルの他のポルシート区別がつくら   | 51- |
|--|---|-----|
|  | 向しノロトコルの地のホリン一と区別がってよ   | л-  |
| リシー プロパティ 詳細   |   |     |
| TTP接続を   |   | _   |
| 年可 ~│ TCF  | PRST的送信   |     |
| 送信元<br><sup>1</sup> Any External   |   |     |
| Any-External   | → 外部から  |     |
|  |   |     |
|  |   |     |
|  | 追加… 編集 削除   |     |
| 送信先  |   |     |
|  |   |     |
|  | 加ボタンをクリック →<br>追加…<br>編集<br>副除  |     |
| 追<br>Route outbound traffic using St   | 加ボタンをクリック →<br>追加… 編集 削除<br>D-WAN Based Routing (Fireware OS v12.3 or higher)                                   |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action  | <mark>加ボタンをクリック →<br/>14 加… 編集… 削除</mark><br>D-WAN Based Routing → (Fireware OS v12.3 or higher)<br><b>●</b>    |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action  | <mark>加ボタンをクリック →<br/>ILE 加… 編集 副除</mark><br>D-WAN Based Routing → (Fireware OS v12.3 or higher)<br><b>I</b>    |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action  | 加ボタンをクリック →<br>追加… 編集 削除<br>D-WAN Based Routing (Fireware OS v12.3 or higher)                                   |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action<br>Application Control を有効にします<br>Geolocation を有効化する   | 加ボタンをクリック →<br>追加… 編集… 削除<br>D-WAN Based Routing (Fireware OS v12.3 or higher)<br>ご 図 M M<br>ご Global<br>Global |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action<br>Application Control を有効にします<br>Geolocation を有効化する<br>このポリシーの IPS を有効にします                                    | 加ボタンをクリック →<br>追加… 編集 削除<br>D-WAN Based Routing (Fireware OS v12.3 or higher)                                   |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action Application Control を有効にします Geolocation を有効化する このポリシーの IPS を有効にします 常城幅と時間フォータを有効化する                            | 加ボタンをクリック →<br>追加 編集  |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action<br>Application Control を有効にします<br>Geolocation を有効化する<br>このポリシーの IPS を有効にします<br>帯域幅と時間クォータを有効化する<br>7ロキシ アクション: | 加ボタンをクリック →<br>追加… 編集 削除<br>D-WAN Based Routing (Fireware OS v12.3 or higher)                                   |     |
| 追<br>Route outbound traffic using St<br>SD-WAN Action<br>Application Control を有効にします<br>Geolocation を有効化する<br>このポリシーの IPS を有効にします<br>帯域幅と時間ウォータを有効化する<br>7ロキシ アクション: | 加ボタンをクリック →<br>追加 編集  |     |

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。

| Firebox<br>Any-External<br>Any-Trusted<br>Any-Optional<br>Any-BOVPN |               |         |         |
|---|---------------|---------|---------|
| 追加  | SNAT の追加      | ユーザーの追加 | その他の追加… |
| されたメンバーとフ   | <b>^</b> ドレス: |         | 削除      |
| されたメンバーとう   | パレス:          |         | 用引取条    |

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]。

| メンバ | 一の追加         |                      | ×     |
|-----|--------------|----------------------|-------|
|     | 種類の選択:<br>値: | ホスト IPv4<br>10.0.0.1 | ~     |
|     |              |                      |       |
|     |              |                      |       |
|     |              |                      |       |
|     |              |                      |       |
|     |              | <u>о</u> к           | キャンセル |

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。

| 許可 v TCP RSTの送信<br>送信元<br>Any-External | ×          |
|--|------------|
| 送信元<br><mark> 梁</mark> Any-External    |            |
| Any-External                           |            |
|  | <b>追加…</b> |
| 送信先                                    |            |
| ♥ 10.0.0.1                             |            |

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

| 1. T. T. T. C.   | テ╶┥┋╪╪╨  |                    |           |
|--|--|--------------------|-----------|
| スケジュール:  | Always On 🔍  |                    |           |
| - ラフィック管理  | #アクション   |                    |           |
|  | 順方向 (送信元 >送信先);                                    | 既定 (制限なし)          |           |
|  | 逆方向 (送信先 >送信元):                                    | (期限なし)             |           |
| ŧ號速度 (bps)   |  |                    |           |
| 制限なし   |  |                    | ~         |
| 🗌 容重を超えた   | とらアラームで知らせる  |                    | <b>通知</b> |
| MPエラー処理  |  |                    |           |
|  | の使用 〜 ICMPの  | 設定                 |           |
| クローバル設定  |  |                    |           |
| クローバル設定<br>AT QoS  |  |                    |           |
| クローバル設定<br>IAT QoS<br>ī方のルールでト   | ·ラフィックが制限される場合に                                    | t 1-1 NAT が優先されます。 |           |
| クローバル設定<br>IAT QoS<br>i方のルールでト<br>I-1 NAT (ネ:                          | ・ラフィックが制限される場合に<br>ットワーク NAT設定の使用)                 | t 1-1 NAT が優先されます。 |           |
| クローバル設定<br>IAT QoS<br>i方のルールでト<br>ゴ 1-1 NAT (ネ:<br>ご 動的 NAT            | ・ラフィックが制限される場合に<br>ットワーク NAT設定の使用)                 | t 1-1 NAT が優先されます。 |           |
| クローバル設定<br>IAT QoS<br>前方のルールでト<br>☑ 1-1 NAT (ネ:<br>☑ 動的 NAT<br>④ ネットワ・ | ・ラフィックが制限される場合に<br>ットワーク NAT設定の使用)<br>- ク NAT設定の使用 | t 1-1 NAT が優先されます。 |           |

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。

| <b>IR</b> C:¥ | Users¥eueda¥Docu | iments¥My WatchGuard¥configs¥SE-   | VERIFIER-T50W.xml *- Firewar | e Policy Manager            |                     | - 0                       | ×       |
|---------------|------------------|------------------------------------|------------------------------|-----------------------------|---------------------|---------------------------|---------|
| ファイル          | / 編集 表示 セッ       | トアップ ネットワーク Fi <u>r</u> eCluster V | PN セキュリティサービス へ              | ルプ                          |                     |                           |         |
|               | 🖬 📾 🖷 🕅 🖓 🚽      | F 🗙 🔤 💐 🗽 🐘 🔒 🚙 🏄                  | * 🗐 🖉 🔗 🖬 🔍 1                | ?                           |                     |                           |         |
| ファイフ          | アウオール Mobile \   | /PN with IPSec                     |                              |                             |                     |                           |         |
|               |                  |                                    |                              |                             | フィルタ: なし            | ~ V                       | 7       |
| 順序 ≠          | アクション            | ポリシー名                              | ポリシーの種類                      | 送信元                         | 送信先                 | <b>ポ</b> ∽ト               | T       |
| 1             | /                | OT FTB                             | FTD                          | Any Trueted                 | Any External        | ton:21                    | and an  |
| 2             | 1                | W HTTP-Incoming                    | НТТР                         | Any-External                | 10.0.0.1            | tcp:80                    |         |
| 3             | Ŷ                | nite-proxy                         | птте-ргоху                   | Any-musted                  | Any-External        | tcp.ou                    | _       |
| 4             | 1                | WatchGuard SSLVPN                  | SSL-VPN                      | Any-External, Any-Trusted   | Firebox             | tcp:443                   |         |
| 5             | 0                | HTTPS-proxy                        | HTTPS-proxy                  | Any-Trusted                 | Any-External        | tcp:443                   |         |
| 6             | 1                | WatchGuard Gateway Wireless        | WG-Gateway-Wireless-Contr.   | . Any-Trusted, Any-Optional | Firebox             | udp:2529                  |         |
| 7             | 1                | WatchGuard Authentication          | WG-Auth                      | Any-Trusted, Any-Optional   | Firebox             | tcp:4100                  |         |
| 8             | 1                | WG-Auth-WebBlocker                 | WG-Auth                      | Any-Trusted, Any-Optional   | Firebox             | tcp:4100                  |         |
| 9             | 1                | WatchGuard Web UI                  | WG-Fireware-XTM-WebUI        | Any-Trusted, Any-Optional   | Firebox             | tcp:8080                  |         |
| 10            |                  | Ping Ping                          | Ping                         | Any-Trusted, Any-Optional,  | Anv                 | icmp (type: 8, code: 255) |         |
| 11            | 1                | WatchGuard                         | WG-Firebox-Momt              | Any-Trusted, Any-Optional,  | Firebox             | tcp:4105 tcp:4117 tcp:41. |         |
| 12            |                  | WG-Cloud-Managed-WiFi              | WG-Cloud-Managed-WiFi        | Anv-Trusted                 | *.moionetworks.com  | tcp:80 tcp:443 udp:3851 . |         |
| 13            | 1                | Any-External                       | Any                          | Any-Trusted                 | Anv-External        | anv                       |         |
| 14            | 1                | Any-Optional                       | Any                          | Any-Optional                | Any-Trusted Any-Ext | any                       |         |
| 15            | 1                | Any Trijetad                       | Λον                          |                             | Any Trueted         | anv                       | ~       |
| <             |                  |                                    |                              |                             |                     |                           | >       |
|               |                  |                                    |                              |                             |                     | Fireware OS v             | /12.4.0 |

次はポートフォワーディングも可能な SNAT (Static NAT)の設定方法について解説します。

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 の追加]ボタンをクリックします。

| Any           |          |         |        |
|---------------|----------|---------|--------|
| Firebox       |          |         |        |
| Any-External  |          |         |        |
| Any-Trusted   |          |         |        |
| Any-BOVPN     |          |         |        |
| <u>نۇ</u> ئەر | SNAT の追加 | ユーザーの追加 | その他の追加 |
|               |          |         | RidRó  |
| 択されたメンバーとフ    | Pトレス:    |         | HARP   |
|               |          |         |        |
|               |          |         |        |
|               |          |         |        |
|               |          |         |        |

SNAT の追加画面で SNAT 名を入力し、[追加]ボタンをクリックします。

| SNAT名: TO_Web_Se | rver |             |
|------------------|------|-------------|
| 20月:             |      |             |
| SNAT メンバー:       |      |             |
|                  |      | <b>通加</b> . |
|                  |      | 編集          |
|                  |      | 直的除         |
|                  |      |             |
|                  |      |             |
|                  |      |             |
|                  |      |             |

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。

| External/Optional IP Address                        | External-1                    | ٠          |
|---|-------------------------------|------------|
| 🥅 発信元 IP を設定する                                      | 10 E F                        |            |
| 内部 IP アドレス:   | 10.100.10.101                 |            |
| 🥅 内部ボートを別のボート                                       | こ設定する                         | 0          |
| (Static NAT for an Option<br>XTM OS v11.8.1 or high | nal IP address require<br>er) | s Fireware |

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。

|            | さい。          |     |        |
|------------|--------------|-----|--------|
| NAT名:      | TO_Web_Serve | er  |        |
| .明: [      |              |     |        |
| אמד ציצאי  | - :          |     |        |
| External-1 | > 10.100.10. | 101 | ie ho. |
|            |              |     | 編集     |
|            |              |     | 直除     |
|            |              |     |        |
|            |              |     |        |
|            |              |     |        |
|            |              |     |        |

# 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。

| A CONTRACTOR OF |  |
|---|--|
| f: HTTP-Incomming   |  |
| リシー プロパティ 詳細  |  |
|   |  |
| TIP接統を<br>4可 ー TCD DST  | の送信  |
|   | v/xs1a   |
|   |  |
| 2 Any-External  |  |
|   |  |
|   |  |
|   |  |
|   | <b>追加…</b> 神乐… <b>則防</b>   |
| 送信先   |  |
| TO_Web_Server (Static NAT)  |  |
| External-1> 10.100.10.101   |  |
|   |  |
|   |  |
|   |  |
|   | <u>追加</u> 編集 削除  |
|   | <u>追加</u> 編集 削除  |
| Application Control を有効にします:  | 道加 御除<br>Global 🔹 💽  |
| ■ Application Control を有効にします: ⑦ このポリシーの IPS を有効にします  | 追加 編集 削除<br>Global 👻 💽   |
| <ul> <li>Application Control を有効にします:</li> <li>このポリシーの IPS を有効にします</li> </ul>   | 道加 編集 削除<br>Global   |
| ■ Application Control を有効にします: ☑ このポリシーの IPS を有効にします ブロキシ アクション:  | 注加 編集 肖明隆<br>Global  |
| ■ Application Control を有効にします:<br>■ このポリシーの IPS を有効にします<br>プロキシ アクション:  | 道加) 編集 削除<br>Global • ) ●  |
| <ul> <li>□ Application Control を有効にします:</li> <li>□ このポリシーの IPS を有効にします</li> <li>ブロキシ アクション:</li> </ul>  | <u>追加) 編集) 削除</u><br>Giobal • <b>》 》</b>                         |
| ■ Application Control を有効にします: ■ このポリシーの IPS を有効にします プロキシ アクション:  | 送加 編集 肖明徐<br>Global - 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一        |
| <ul> <li>□ Application Control を有効にします:</li> <li>□ このポリシーの IPS を有効にします</li> <li>プロキシ アクション:</li> </ul>  | <u>追加</u> 編集 削除<br>Giobal • I III III III III III III III III II |

## 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[カスタムを管理する]ボタンをクリックします。

| 🌄 ポリシーを追加する  |                                    |                              |       | ×   |
|--|------------------------------------|------------------------------|-------|-----|
| 新しいポリシーに対して事前定競済みまたはカスク<br>フロキシ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ<br>シ | Rム ポリシーを選<br>ポリシー テン:<br>ポート<br>説明 | 択します。<br>7レート プロパティ<br>プロトコル |       |     |
| カスタムを管理する  |                                    | ドリシーを追加する                    | キャンセル | ヘルプ |

[カスタムポリシーテンプレートを管理する]画面で[新規作成]ボタンをクリックします。

| 新規作成   |
|--------|
| 福朱     |
| 当时很余   |
| インボート  |
| エクスポート |
|        |

[カスタムポリシーテンプレートを管理する]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。

| 明:            |           |         |      |     |
|---------------|-----------|---------|------|-----|
| 類: ③ア         | 「ケット フィル・ | 9 0     | ブロキシ |     |
| нг 470;       |           |         |      | 追加  |
|               |           |         |      | [編集 |
|               |           |         |      | 削除  |
|               |           |         |      |     |
|               |           |         |      |     |
| <b>1</b> +-4/ | マイドルカイ    | . ምግኑ በ | し地学  |     |

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。

| 明:<br>類: ④ パケットフィルタ ⑦ プロキシ<br>ロトコル:<br>CP:2000 追加. | 明:<br>頤: ④ パケット フィルタ ⑦ ブロキシ<br>ロトコル:<br>IP:2000<br>編集。 | 前:       | Internal_System   |
|--|--|----------|-------------------|
| ロトコル:<br>CP:2000 (追加)                              | ロトコル:<br>1P:2000 通加。<br>編集。                            | 明:<br>類: | ◎ パケットフィルタ ◎ プロキシ |
| CP:2000  | P:2000 追加.<br>編集。                                      |          | 0.000             |
|  | 編集   | 마        | םµ:               |

[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。

| ー <mark>ー</mark> フロキシ<br>ー 二章 DMS provo   | ポリシー テンプ        | レート プロパティ    |  |
|---|-----------------|--------------|--|
| Explicit-proxy  | Internal_System |              |  |
| <ul> <li>FTP-proxy</li> <li>H323-ALG</li> <li>HTTP-proxy</li> <li>HTTPS-proxy</li> <li>MAP-proxy</li> <li>POP3-proxy</li> <li>POP3-proxy</li> </ul> | ポート<br>2000     | プロトコル<br>TCP |  |
| SIF-ALG<br>SMTP-proxy<br>TCP-UDP-proxy<br>バケットフィルタ<br>カスタム<br>Internal_System   |                 |              |  |
| カスタムを管理する   |                 |              |  |

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。

| ドリシー プロパチ     | F⊣ ≣¥≇⊞ |           |  |
|---------------|---------|-----------|--|
| FCP-UDP 接続を   | 100 A   |           |  |
| 許可            |         | TCPRSTの送信 |  |
| 送信元           |         |           |  |
| Any-Trusted   |         |           |  |
| 🙊 Any-Optiona |         |           |  |

### するとポリシーー覧でも無効になったことが分かります。

| ファイル<br>🚊 💂<br>ファイアウ                            | 編集 表示 セ<br>🗁 喝   🏹<br>フォール Mobile | ットアップ ネットワーク FireClust<br>🛨 🗙   🏆 💐 🍡   🏛 劇<br>s VPN with IPSec   | ter VPN セキュリティサービス<br>🂰 ෯   📑 💋 🔗   🖬 🍕  | 、ヘルブ<br><mark>人 ?</mark>  |
|---|-----------------------------------|---|--|---|
|   |                                   |   | フィルタ:  | al 🗸 🖓 🕇  |
| 順序 左  | アクション                             | ポリシー名   | ポリシーの種類  | 送信元   |
| 1<br>2<br>3<br>4<br>5<br>6<br>7<br>8<br>9<br>10 |                                   | <ul> <li>FTP-proxy</li> <li>HTTP-Incoming</li> <li>HTTP-Outgoing</li> <li>HTTPS-proxy</li> <li>WatchGuard Certificate Portal</li> <li>WatchGuard Web UI</li> <li>Ping</li> <li>DNS</li> <li>WatchGuard</li> <li>Outgoing</li> </ul> | FTP-proxy<br>HTTP<br>HTTP<br>HTTPS-proxy<br>WG-Cert-Portal<br>WG-Fireware-XTM-WebUI<br>Ping<br>DNS<br>WG-Firebox-Mgmt<br>TCP-UDP | Any-Trusted, Any-Optional<br>Any-External<br>Any-Trusted<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional, HQ<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional<br>Any-Trusted, Any-Optional |
| <   |                                   |   |  | Fireware OS v12   |

## 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。

| 編集 ポリシーのプロパティ                                      |   | ×        |
|--|---|----------|
| 5前: Ping<br>ポリシー プロパティー詳細                          |   | 有効       |
| ボリシーの種類: Ping<br>ポート                               | プロトコル<br>ICMP (type: 8, code: 255)  |          |
| コメント<br>Policy added on 2019-04-03T14:12:27+09:00. |   |          |
| 97:  | ■ ログ記録と通知<br>カテゴリ:<br>■ ■ ■ = わていろがな == ト == ト == + = + = + = + = + = = = =                     |          |
| ポリシータグ   | ■ 13 A CUSATION ● ログメッセージを送信する ○ レポートのログメッセージを送信する (Fireware OS 11. ○ SNMPトラップを送信 ○ SNMPトラップを送信 | 10.5 以降) |
| ログ記録<br>接続を試みたサイトを自動的にブロックする                       | <ul> <li>● 電子メール</li> <li>● ボッブアップウィンドウ</li> </ul>  |          |
|  | 起動間隔: 15 🔹 分<br>繰り返し回数: 10 🔹  |          |
|  | OK  | ヘルフ      |
|  |   |          |

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。

| 前: HTTP-Outgoing  |   | ☑ 有效 |
|---|---|------|
| ポリシー フロバティ 詳細   |   |      |
|   |   |      |
| スケジュール: Always On   |   |      |
| スケジュール: Always On ・   |   |      |
| スケジュール: Always On ・<br>Traffic Management Actions<br>Forward (From > To): | <ul> <li>         ・</li> /ul> |      |

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。

| 前: 1  | Busir | nes | sHo | urs |   |     |   |          |          |
|-------|-------|-----|-----|-----|---|-----|---|----------|----------|
| 明: [  |       |     |     |     |   |     |   |          |          |
| 時間    | П     | д   | ×   | *   | * | 金   | ± |          | モード: 1時間 |
| 06:00 | 1     |     |     |     |   |     |   |          | :稼働時間    |
| 07:00 | 1     |     |     |     |   |     |   | 1        | □→非窃働時間  |
| 08:00 |       |     |     |     |   |     | _ |          |          |
| 09:00 |       |     |     |     |   |     | 1 |          |          |
| 10:00 |       |     |     |     |   | - 6 | 5 | <b>.</b> |          |
| 11:00 |       |     |     |     |   |     |   | 1        |          |
| 12:00 |       |     |     |     |   |     |   | 1        |          |
| 13:00 |       |     |     |     |   |     | 1 |          |          |
| 14:00 |       |     |     |     |   |     |   | _        |          |
| 15:00 |       |     |     |     |   |     | - | =        |          |
| 16:00 |       |     |     |     |   |     |   |          |          |
| 17:00 |       |     |     |     |   |     | 1 |          |          |
| 18:00 |       |     |     |     |   |     | 1 |          |          |
| 19:00 |       | A   | 2 1 |     |   |     |   |          |          |
| 20:00 |       |     |     |     |   |     |   |          |          |
| 21:00 |       |     |     |     |   |     |   | -        |          |
|       |       |     |     |     |   |     |   |          |          |

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<u>セットアップ</u> — <u>Default Threat Protection</u> — <u>規定のパケット処理</u> をクリックします。

| 【 C:\Users\USERNA ファイル 編集 表示 | ME\Documents\My W                    | /atchGuard\configs\XTM25-<br>フーク FireCluster VPN セキ | W_Tokyo-Branch<br>ニュリティサービス               | i.xml- Fireware XT<br>いへルプ                        | M Policy Manag                               | er  |                |       | X      |
|------------------------------|--------------------------------------|---|---|---|--|-----|----------------|-------|--------|
| 🚊 🖣 🗁 🖏  <br>ファイアウオール M      | システム<br>機能キー                         | 💰   🖳 🖉   | Ø 🖬 🔍 '                                   | ?   |  |     |                |       |        |
|                              | エイリアス                                |   |   | (3  | フィルタ: なし                                     |     | Ý              | ] 🍞   | 7      |
| 順序 / アクショ                    |                                      | シーの種類   | 送信元                                       | 送信先   | ポート  | PBR | App Control    | タグ    | 7.     |
|                              | Bolair<br>アクション<br>Default Threat Dr | otection ) と 既定の                                    | Any-Trusted, An<br>Any Etternal<br>パケット処理 | y-OpAny-External<br>External-1> '<br>Any-External | tcp:21<br>10tcp:80<br>tcp:80                 |     | なし<br>なし<br>なし |       |        |
|                              | NTP<br>SNMP                          | レーマー<br>フロッ・<br>分 ブロッ・                              | クされたサイト<br>クされたポート                        | pFirebox<br>DpAny<br>DpFirebox                    | tcp:8080<br>ICMP (type: 8,<br>tcp:4105 tcp:4 |     | なし<br>なし<br>なし |       |        |
| 7 🗸                          | 管理対象のデバー                             | イス設定 M  | Any-musted, An                            | y-OpAny-External                                  | tcp:0 (Any) u                                |     | なし             |       |        |
|                              | グローバル設定。<br>OS Compatibility.        |   |   |   |  |     |                |       |        |
|                              |                                      |   |   |   |  |     | Fireware       | XTM v | 11.9.0 |

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。

|                       |        |                     | ОК        |
|-----------------------|--------|---------------------|-----------|
| ▼ ステーティンク収撃の防御        |        |                     | = + + 171 |
| 📝 IP ソース ルーティングの防御    |        |                     | 41707     |
| 📝 ポート空間プローブのブロック      | 10 🌲   | 宛先ボート/ソース IP (しきい値) | ログ記録。     |
| 📝 アドレス空間ブローブのブロック     | 10 🌲   | 宛先 IP/ソース IP (しきい値) | ~117      |
| 📝 IPSec フラッド攻撃の防御     | 1500 🌲 | パケット/秒 (しきい値)       |           |
| 📝 KE フラッド攻撃の防御        | 1000 🌲 | パケット/秒 (しきい値)       |           |
| 📝 ICMP フラッド攻撃の防御      | 1000 🌲 | パケット/秒 (しきい値)       |           |
| 📝 SYN フラッド攻撃の防御       | 5000 🌲 | パケット/秒 (しきい値)       |           |
| ☑ UDP フラッド攻撃の防御       | 1000 🔹 | パケット/秒(しきい値)        |           |
| 未処理パケット               |        |                     | 1         |
| 🥅 未処理パケットのソースの自動ブロック  |        |                     |           |
| 🥅 接続が無効のクライアントにエラー メッ | セージを送信 |                     |           |
| 分散サービス拒否(DDoS)攻撃の防止   |        |                     | 1         |
| 📝 サーバー クォータ当たり        |        | 100 🜩 接続数 /秒        |           |
|                       |        | 100 ********        |           |

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 $\underline{vvPv}$  — <u>Default Threat Protection</u> — <u>ブロックされたサイト</u> 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。

| ロックされたサイト<br>ブロックされたサイト                          | ブロックされたサイトの例外 | 自動ブロック |
|--|---------------|--------|
| 9.22.156.197<br>183.181.168.52<br>183.181.172.62 |               |        |
|  |               |        |

### **Blocked Ports**

ポリシーマネージャの セットアップ — Default Threat Protection — <u>ブロックされたポート</u>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。

| /ロックされたホート |             | ок      |
|------------|-------------|---------|
| 1          | <u>^</u>    | (       |
| 111        |             | キャンセル   |
| 513        | E           | n /TERM |
| 514        |             |         |
| 2049       |             | ヘルプ     |
| 6000       |             |         |
| 6001       |             |         |
| 6002       |             |         |
| ポート:       | 1 🚔 🔒 10 前除 |         |

# 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。

※ 現時点の Fireware v12.4 では、初期セットアップウィザードを実行すると基本的なセキュリティ設定 はすべて済んだ状態になっており、手動で設定する必要はほとんどありませんが、この章の情報は ご自身でポリシーの追加や設定済みのポリシーを変更する際に役立ちます。





セキュリティ機能を有効にするためのライセンスは、現在 Basic Security Suite と Total Security Suite の 2 種類が存在します。

Basic は AV や IPS などの従来型の脅威に対応するもの、Total はマルウェアやラ ンサムウェアなど未知の脅威、DNS セキュリティ、エンドポイント、クラウドサービス までカバーする全部入りとなっています。 ぜひ Total Security Suite をご選択くださ い。※ 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、 [ポリシーを追加する]ボタンをクリックします。

| 🔣 ポリシーを追加する  |   | ×  |
|--|---|--|
| 新しいポリシーに対して事前定義済<br>プロキシ<br>プロキシ<br>Explicit-proxy<br>Explicit-proxy<br>H323-ALG<br>HTTP-proxy<br>HTTP-proxy<br>POP3-proxy<br>SIP-ALG<br>SMTP-proxy<br>TCP-UDP-proxy | タム ポリシーを選;<br>ポリシー テンプ<br>HTTP-proxy<br>ポート<br>80<br>説明<br>HTTP はハイパ<br>使ってインター | 択します。<br>イレート プロパティ<br>プロトコル<br>TCP<br>ーテキスト転送プロトコルです。World Wide Webを ▲<br>-ネット上で情報をやり取りするときに使用しま  |
| カスタムを管理する  | す。WatchGua<br>キシとは異なり<br>のキャッシュか<br>る場合、ポリシ<br>する必要があり<br>は正常に動作し               | rd ホリジー "HTTP Proxy" は HTTP キャッジュ プロ<br>Jます。HTTP キャッシュ プロキシでは Web データ<br>証制御されます。外部キャッシュ プロキシを使用す<br>ハーを追加して、組織に必要な送信ポリシーを有効に<br>Jます。そのようにしない場合、外部への TCP 接続<br>Jません。 V |

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。

| 、新規作成 ポリシーのプロパティ                   | 2                                       | >  |
|------------------------------------|---|--|
| 前: HTTP-proxy                      |   | ☑ 有効   |
| ポリシー プロパティ 詳細                      |   |  |
|                                    |   |  |
| 11 IP-proxy 授初を<br>許可 V TCP RS7    | の送信                                     | ~  |
| 送信元                                |   |  |
| R Any-Trusted                      |   |  |
|                                    |   | <b>追加</b> 羅集 削除  |
| 送信先                                |   |  |
|                                    |   | <b>追加</b> 編集 削除  |
| Route outbound traffic using SD-W/ | N Based Routing 🥪 (Fireware OS v12.3 or | higher)  |
| SD-WAN Action                      |   |  |
| Application Control を有効にします:       | Global M D                              |  |
| ☑ Geolocation を有効化する               | Global 🗸 📝 🂽                            |  |
| ✓ このポリシーの IPS を有効にします              | provide the second stand                |  |
| ── 帯域幅と時間クォータを有効化する (Fi            | eware OS v11.10 以降)                     |  |
| プロキシ アクションまたはコンテンツ ア?              | ション: HTTP-Client.Standard               | <ul> <li>Image: Image: Ima</li></ul> |
|                                    | [                                       | OK キャンセル ヘルブ   |

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。<sup>3</sup>

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。

| プロキシ アクションまたはコンテンツ アクション: | HTTP-Client.Standard | ~ |  |
|---------------------------|----------------------|---|--|
|                           |                      |   |  |

<sup>3</sup> 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<u>セキュリティサービス</u> — <u>WebBlocker</u> — <u>アクティブにする</u> をクリックします。

| 🔣 C:¥Users¥tsuto¥Documents¥My WatchGuard¥configs¥T50-W-MAY29.xml- Fireware Policy Manager |          |  |  |  |   | - 🗆   | ×   |
|---|----------|--|--|--|---|---|---|
| ファイル 編集 表示 セットアップ ネットワーク FireCluster VPN セキュリティサービス ヘルプ                                   |          |  |  |  |   |   |   |
| ファイア<br>アイア<br>順序 /<br>1<br>2<br>3<br>4<br>5<br>6<br>7<br>8<br>9<br>10<br>11              | 補業 表示 セ: | + X I シー名<br>* VPN with IPSec<br>* VPN with IPSec<br>* FTP-proxy<br>* HTTP-Incomming<br>* HTTP-proxy<br>* HTTP-proxy<br>* HTTP-proxy<br>* HTTP-proxy<br>WatchGuard Web UI<br>* Ping<br>DNS<br>Ø POP3-proxy<br>* WatchGuard<br>WatchGuard<br>* Outgoing | FTP-pro<br>HTTP-pr<br>HTTP-pr<br>HTTPS-<br>WG-Fire<br>Ping<br>DNS<br>POP3-p<br>WG-Fire<br>TCP-UD | Application Control<br>APT Blocker<br>ボットネット検出<br>Data Loss Prevention<br>DNSWatch<br>Gateway AntiVirus >><br>Geolocation<br>Intrusion Prevention<br>モバイル セキュリティ<br>Quarantine Server<br>Reputation Enabled Defense<br>spamBlocker >><br>Threat Protection | なし<br>送信元<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional | 送信先<br>Any-External<br>External-1> 1<br>Any-External<br>Firebox<br>Firebox<br>Any<br>Any-External<br>Any-External<br>Firebox<br>Any-External<br>Firebox<br>Any-External | tcp:21<br>tcp:80<br>tcp:44<br>tcp:41<br>tcp:53<br>tcp:11<br>tcp:52<br>tcp:11<br>tcp:0 ( |
|   |          |  |  | WebBlocker   | 省 アクティブにす   | ·る  |   |
|   |          |  |  |  | 🥹 11FA8   |   |   |
|   |          |  |  |  |   |   |   |
| Fireware 0S v12.4.0   |          |  |  |  |   |   |   |

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



アクションを識別するための名前を指定します。
| Activate WebBlocker Wizard                   | ×                   |
|--|---------------------|
| WebBlocker アクションの名前を選択する                     | WatchGuard          |
| 名前は、プロキシ アクションの後のアプリケーションにおけるこの WebBlocker ア | クションを特定するために使用されます。 |
| 名前: WebBlocker.1                             |                     |
|  |                     |
|  |                     |
|  |                     |
|  |                     |
|  |                     |
|  |                     |
|  |                     |
|  |                     |
|  |                     |

# 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。

| 19.110.000    | Fゴリを表示する 🗸 す/ | べてのカテゴリ 🗸 検索:       |      | ウイック アクション   | 34 |
|---------------|---------------|---------------------|------|--------------|----|
| Action        | カテゴリ          | サブカテゴリ              | アラーム | ログ           |    |
| 許可            | π             | T .                 |      | $\checkmark$ | -  |
| 許可            | π             | Web and Email Spam  |      | $\checkmark$ |    |
| 許可            | π             | Webおよび電子メール・マーケティング |      | $\checkmark$ |    |
| 許可            | π             | Webサイト翻訳            |      | $\checkmark$ |    |
| 許可            | п             | Webホスティング           |      | $\checkmark$ |    |
| 許可            | п             | Web分析               |      | $\checkmark$ |    |
| 許可            | п             | ウェブ・コラボレーション        |      | $\checkmark$ |    |
| 許可            | π             | コンピュータセキュリティ情報      |      | $\checkmark$ |    |
| 許可            | п             | ハッカー関連              |      | $\checkmark$ |    |
| 許可            | π             | プロキシによるブロック回避       |      | $\checkmark$ |    |
| 許可            | п             | 検索エンジンおよびポータル       |      | $\checkmark$ |    |
| 許可            | п             | 未承認の携帯市場            |      | $\checkmark$ |    |
| 許可            | アダルト          | アダルト                |      | $\checkmark$ |    |
| 許可            | アダルト          | アダルト・コンテンツ          |      | $\checkmark$ |    |
| 許可            | アダルト          | セックス                |      | $\checkmark$ |    |
| ≣≄ <b>च</b> ⊺ | マガルト          | z = k               |      |              | ~  |

先に作成した WebBlocker アクションと結びつくプロキシポリシーを選択します

| Activate WebBlocker Wizard                             | ×             |
|--|---------------|
| 新しいプロキシ ポリシーを作成する                                      | (WatchGuard   |
| 作成するプロキシボリシーを選択します。<br>✓ HTTP クライアント<br>✓ HTTPS クライアント |               |
|  |               |
|  |               |
|  |               |
| ヘルフ  | <戻る 次へ> キャンセル |

Wizard が終了します。「WebBlocker の中央構成に進みます」にチェックが入ったまま[完了]をクリック。



# Web Blocker を構成する

項目を選択し、[編集]をクリックします。

| ッロー<br>(編集<br>当)(R |  | 0.0555 |  |
|--------------------|--|--------|--|
| ******<br>前道       |  |        |  |
|                    |  |        |  |
| 1 241              |  |        |  |
| エクスポ               |  |        |  |
|                    |  |        |  |
|                    |  |        |  |
|                    |  |        |  |
|                    |  |        |  |
|                    |  |        |  |
|                    |  |        |  |
|                    |  |        |  |
|                    |  |        |  |

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。

| 时: Default-WebB     | locker                               |                       |      |              |
|---------------------|--------------------------------------|-----------------------|------|--------------|
| 明: Default config   | uration for WebBlocker               |                       |      |              |
| テゴリ ᅰ外 詳            | 細 アラーム サーバー                          |                       |      |              |
| すべてのカテゴリ?           | を表示する 〜 すべてのカテゴリ                     | ✓ 検索:                 |      | クイック アクション   |
| Action              | カテゴリ                                 | サブカテゴリ                | アラーム | П <i>7</i>   |
| F可                  | п                                    | п                     | 1    |              |
| F可                  | п                                    | Web and Email Spam    |      |              |
| F可                  | π                                    | Webおよび電子メール・マーケティング   |      |              |
| F可                  | π                                    | Webサイト翻訳              |      |              |
| F可                  | Π                                    | Webホスティング             |      |              |
| F可                  | π                                    | Web分析                 |      |              |
| F可                  | π                                    | ウェブ・コラボレーション          |      |              |
| F可                  | π                                    | コンピュータセキュリティ情報        |      |              |
| F可                  | π                                    | ハッカー関連                |      |              |
| 否                   | π                                    | プロキシによるブロック回避         |      |              |
| F可                  | π                                    | 検索エンジンおよびボータル         |      |              |
| F ण                 | π                                    | 未承認の携帯市場              |      |              |
| F可                  | アダルト                                 | アダルト                  |      |              |
| F可                  | アダルト                                 | アダルト・コンテンツ            |      |              |
| F可                  | アダルト                                 | セックス                  |      |              |
| F可                  | アダルト                                 | ヌード                   |      |              |
| F可                  | アダルト                                 | ランジェリー&水着             |      |              |
| F可                  | アダルト                                 | 性数育                   |      |              |
| F可                  | インターネット・ コミュニケー                      | シ インターネット・ コミュニケーション  |      |              |
| F可                  | インターネット・ コミュニケー                      | シ Web チャット            |      |              |
| F可                  | インターネット・ コミュニケー                      | シ テキストとメディアによるメッセージ配信 |      |              |
| F可                  | インターネット・ コミュニケー                      | シ一般の電子メール             |      |              |
| F可                  | インターネット・ コミュニケー                      | シ 組織の電子メール            |      |              |
| F可                  | エンターテイメント                            | エンターテイメント             |      |              |
| F可                  | エンターテイメント                            | メディアファイル ダウンロード       |      |              |
| F可                  | ギャンブル                                | ギャンブル                 |      |              |
| F可                  | ゲーム                                  | ゲーム                   |      |              |
| F可                  | コラボレーション - Office                    | コラボレーション - Office     |      | $\checkmark$ |
| F可                  | ショッピング                               | ショッピング                |      |              |
| FIJ                 | ショッピング                               | インターネット・オークション        |      |              |
| RLが未分類の場合           | a 許可 🗸 🗌 アラーム 🗹 ·                    | このアクションを記録する          |      |              |
| ote: Warn action is | s supported in Fireware OS v12.4 and | higher.               |      |              |

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

| Defa    | ault-WebBloc       | ker                                |                                |  |                   |                   |
|---------|--------------------|------------------------------------|--------------------------------|--|-------------------|-------------------|
| 月: Defa | ault configura     | tion for WebBlocker                |                                |  |                   |                   |
| テゴリ     | 例外 詳細              | アラーム サーバー                          | -1                             |  |                   |                   |
|         |                    |                                    |                                | 1  | h ( h 7 h 21 - 21 | 1                 |
|         | 1                  | 11 11.555                          | 1.0000000                      | 22011  | 0100700BJ         | 1040              |
| 10 V    |                    |                                    |                                | Dettern  |                   |                   |
| nabled  | Action             | Name                               | Match Type                     | Pattern  | Alarm Log         | 15.00             |
| nabled  | Action<br>許可       | Name<br>WatchGuard                 | Match Type<br>正規表現             | ^{0-9a-zA-Z \]{1,256}\.watchguard\.com/                      | Alarm Log         | 1 <u>5川</u><br>選挙 |
| nabled  | Action<br>許可<br>許可 | Name<br>WatchGuard<br>amazon.co.jp | Match Type<br>正規表現<br>パターン マッチ | ^[0-9a-zA-Z \]{1,256}\.watchguard\.com/<br>*.*amazon.co.jp/* |                   | <u>通加</u><br>現集   |

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。

| 』WebBlocker アクション の編集  | 3       |
|--|---------|
| 名前: Default-WebBlocker   |         |
| 說明: Default configuration for WebBlocker   |         |
| カテゴリ 例外 詳細 アラーム サーバー   |         |
| サーバータイムアウト<br>Firebox が次の時間内に WebBlocker サーバーに接続できない場合: 5 ÷ 秒<br>☑ アラーム ☑ このアクションを記録する<br>それから                       |         |
| <ul> <li>● ユーザーが Web サイトを参照するのを許可する</li> <li>○ Web サイトへのアクセスを拒否する</li> <li>○ アラーム</li> <li>○ このアクションを記録する</li> </ul> |         |
| 5422201412   |         |
|  |         |
|  | 既定値に戻す  |
|  | <u></u> |

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。

|                    | Request denied by WatchGuard HTTP Proxy.                       |  |
|--------------------|--|--|
| Reason: one or m   | ore categories denied helper='WebBlocker.2' details='Shopping' |  |
| Please contact you | ur administrator for assistance.                               |  |
| More Details:      |  |  |
| Method: GET        |  |  |
| Host: shopping.yal | hoo.co.jp  |  |
| Path: /            |  |  |

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。

| Default-HTTP-Client  |   |
|--|---|
| Created by Policy Manager  |   |
| ≠1U  |   |
| HTTP 要求           全般設定           要求方法           URL パス           ヘッダーフィールド           -条記           HTTP 応答           -2 検説定           ヘッダーフィールド           コンテンツの種類           クッキー           本文のコンテンツの種類           Webキャッシュサーバーの使用           HTTP ブロキシ例外           Oata Loss Prevention           WebBlocker           ゲートウェイ AV           Ponutation Explored Datense           把否 スッセージ           メッセージ           APT Blocker | <pre>HEES.vyt-9<br/>Content-type: text/html; charset="utf-8"<br/>(!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"<br/>"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"&gt;<br/>Chtml lang="en" xml1ang="en" xmlns="http://www.w3.org/1939/xhtml"&gt;<br/>Chead<br/>(title&gt;%(transaction)% denied by WatchGuard HTTP Proxy<br/>(style type="text/css"&gt;<br/>body {<br/>font-family: Arial, Helvetica, Verdana, Sans-Serif;<br/>font-size: small;<br/>font-weight: normal;<br/>color: #D00000;<br/>}<br/>div {<br/>margin-left: auto;<br/>margin-right: auto;<br/>text-align: center;<br/>}<br/>}<br/>.box {<br/>width: 600px;<br/>background-color: #F2F2F2;<br/>border-left: solid 1px #C2C2C2;<br/>vertical-align: middle;<br/>padding: 20px 10px 20px 10px;<br/>}<br/>}<br/>cate: align: left;<br/>} </pre> |

※%(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。

|                    | 警告  |
|--------------------|---|
|                    | セキュリティ機制こよってこの通信(Request)が拒否されました!  |
|                    | このサイトの閲覧が業務上必要な場合、またはこの結果について問い合わせたい場合は<br>以下の情報をメール本文に貼り付けて、 <u>情報システム課</u> までご連絡ください。 |
| 理由: Ca             | tegory 'Shopping' denied by WebBlocker policy 'WebBlocker.1'.                           |
| メノッド:              | GET   |
| 接続先 <mark>U</mark> | RL: t.nissen.co.jp  |
| 137.100            | //p/r? site=5& article=144& link=521484656& image=7746121                               |

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



WebBlocker のフィルタリング用データベースは、FORCEPOINT 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

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 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 —

#### <u>アクティブにする</u>をクリックします。

| <u>津</u> 🛓<br>ファイア・   | 🔁 🖶   🦻<br>ウオール Mobi | + X   ¥ 💐 🗽   🖻 劇<br>e VPN with IPSec   | <b>*</b> *   | Application Control<br>APT Blocker<br>ボットネット検出<br>Data Loss Prevention  | -   | フィルタ: なし  | ~ 77  |
|---|----------------------|---|--|---|---|---|---|
| )順序 //<br>1<br>2<br>3<br>4<br>5<br>6<br>6<br>7<br>8<br>9<br>9 |                      | ポリシー名<br>を FTP-proxy<br>・ HTTP-proxy<br>・ HTTP-proxy<br>・ WatchGuard Certificate Portal<br>・ WatchGuard Web UI<br>・ Ping<br>つ DNS<br>・ WatchGuard<br>・ WatchGuard<br>・ Outgoing | FTP-pro<br>HTTP-pri<br>HTTPS-<br>WG-Cet<br>WG-Fire<br>Ping<br>DNS<br>WG-Fire<br>TCP-UD | DNSWatch<br>Gateway AntiVirus<br>Geolocation<br>Intrusion Prevention<br>モバイルセキュリティ<br>Quarantine Server<br>Reputation Enabled Defense<br>spamBlocker<br>Threat Protection<br>WabBlocker | 送信元<br>構成<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional | 送信先<br>ternal<br>ternal<br>Firebox<br>Firebox<br>Any<br>Any-External<br>Firebox<br>Any-External | ポート           tcp:21           tcp:80           tcp:443           tcp:5080           icmp (type: 8, code: 255)           tcp:53 udp:53           tcp:4105 tcp:4117 tcp:4118           tcp:0 (Any) udp:0 (Any) |

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。

| ateway          | / AntiVirus の設定をポリ                   | シーに適用します                      | U                    | atchGua              |
|-----------------|--------------------------------------|-------------------------------|----------------------|----------------------|
| このリス<br>Gateway | トにはアクティブなポリシ<br>y AntiVirus が有効になってし | - が含まれていますが、そ<br>いません。アクティブなポ | れらのポリシ<br>リシーに対応     | ーに対応する<br>する Gateway |
| antiVirus<br>選択 | sをアクティブにするには、<br>ポリシー名               | [選択] チェック ホックス・<br>  プロキシの。   | をオンにして・<br>. 種類      | Gateway AV           |
| $\checkmark$    | FTP-proxy<br>HTTP-proxy              | FTP<br>HTTP                   | Firewall<br>Firewall | 有効<br>無効             |
|                 |                                      |                               |                      |                      |
|                 |                                      |                               |                      |                      |
|                 |                                      |                               |                      |                      |

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。

| K Activate Gateway AntiVirus Wizard |             |       | ×         |
|-------------------------------------|-------------|-------|-----------|
| 新しいプロキシポリシーの作成                      |             | W     | atchGuard |
| 新しいプロキシ ポリシーを作成する場合は、必要なポリ          | リシーを選択      | してくだき | ·L\.      |
| □受信 SMTP                            |             |       |           |
| 電子メール サーバーの ドアドレス:                  |             |       |           |
| П РОРЗ                              |             |       |           |
| ☑ 明示的 (Fireware OS v11.11 以降)       |             |       |           |
| □ MAP (Fireware OS v12.0 以降)        |             |       |           |
|                                     |             |       |           |
| 👔 基本的なブロキシ構成が構成され、 Gateway Ar       | itiVirus が有 | 効になりま | す。ウィザー    |
| ── ドを完了した後、構成を編集することができます           | *           |       |           |
|                                     | 戻る          | 次へ>   | キャンセル     |

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<u>セキュリティサービス</u> — <u>Gateway Anti-Virus</u> — <u>構成</u>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。

| r-proxy rife rifewall 편정<br>TP-proxy HTTP Firewall 無効  |
|--|
| niir radwaii <del>m</del> .vi  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| □ 【有効】をクリックすると、適用されるルールのアクジョンが「計可」から「AVスキャン」に変わりま。   |
| 💞 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。   |
|  |
|  |
|  |
|  |
| configure the Gateway AntiVirus attachment settings undate server, and file exceptions, click the following but  |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following buth  |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butt  |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butt<br>サーバーのアップデート File Exceptions   |
| <ul> <li>&gt;</li></ul>  |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butt  |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butt  |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butter $t = x = 0$ and $\tau = 1$ .   |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following buth<br>サーバーのアップデート File Exceptions   |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butt<br>$\psi - \kappa - \sigma \mathcal{P} \vee \mathcal{I} \mathcal{F} - h$ File Exceptions                       |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following buttors $\psi - \mathcal{N} = \mathfrak{O} \mathcal{P} \vee \mathcal{I} \mathcal{F} = \mathbb{N}$ . File Exceptions |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following buth<br>サーバーのアップデート File Exceptions   |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following butt<br>サーバーのアップデート File Exceptions   |
| configure the Gateway AntiVirus attachment settings, update server, and file exceptions, click the following buth<br>サーバーのアップデート   File Exceptions   |

#### 構成画面が開きます。

| <ul> <li>全般のな G</li> <li>HTTP 要求</li> <li>→ URL / X</li> <li>→ HTTP 応答</li> <li>→ コンテンツの種類</li> <li>本文のコンテンツの種類</li> <li>アクション</li> <li>デパンジンジンジンの種類</li> <li>アクション</li> <li>デパンジンジンジン</li> <li>研断: 統</li> <li>スキャン</li> <li>許可: 応:</li> <li>コンテン</li> <li>許可: 応:</li> <li>コンテン</li> <li>許可: 応:</li> </ul> | ateway AntiVirus 設定<br>ntiVirus 設定は、URL Paths、Content Ty<br>リップダウン リストで AV スキャン が遠<br>ay AntiVirus を有効化する<br>ノー<br>検出時:<br>読をすぐに切断する<br>エラー発生時:<br>客の通過を許可する<br>かがスキャン サイズの制限を超過したね<br>客の通過を許可する | ypes、および Boo<br>諸択されている場合<br>く            | dy Content Type<br>含だけ適用され.          | sの各ル〜ルセットの (ア・<br>ます。               |
|--|--|---|--------------------------------------|-------------------------------------|
| ウイルス<br><b>切断:接</b><br>スキャン<br>許可:応:<br>コンテン<br>許可:応:<br>アテン<br>許可:応:  | 検出時:<br>読をすぐに切断する<br>エラー発生時:<br>客の通過を許可する<br>ツがスキャン サイズの制限を超過した%<br>客の通過を許可する<br>へが使見化されてしる根本でについての  | 〜<br>〜<br>幕合 (Fireware OS                 | ☑ アラーム<br>☑ アラーム<br>S v12.0.1 以降):   |                                     |
| スキャン<br>許可:応3<br>コンテン<br>許可:応3<br>コンテン<br>許可:応3  | エラー発生時:<br>答の道過を許可する<br>ツがスキャンサイズの制限を超過した。<br>客の通過を許可する<br>いが使見化されている根本でについての  | 〜<br>≜合 (Fireware OS<br>〜                 | ☑ アラーム<br>S v12.0.1以降):              | ☑ nº                                |
| 許可:応<br>コンテン<br>許可:応<br>コンテン<br>許可:応<br>に  | 客の通過を許可する<br>ツがスキャン サイズの制限を超過した。<br>客の通過を許可する  | 〜<br>集合 (Fireware 05<br>〜                 | ☑ アラーム<br>S v12.0.1 以降):             | M 02                                |
| コンテン<br>許可:応:<br>コンテン<br>許可:応:   | ツがスキャン サイズの制限を超過した。<br>客の通過を許可する<br>2.5555日の1000000000000000000000000000000000   | 場合 (Fireware OS<br>〜                      | S <mark>v</mark> 12.0.1 以降):         |                                     |
| 計可:応:<br>コンテン<br>許可:応:   | 各の通過を許可する  | ~   |                                      |                                     |
| コンテン<br>許可:応 <sup>3</sup>  | いち成ワルナヤアリス担合(ビュー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・   |   | ✓ アラーム                               | M 00                                |
| ET "J : AG-  | ッか噌ちにされている場合 (Fireware O   | IS v12.0.1 以降):                           |                                      |                                     |
|  | 50/8/8/201-19-2  | *   |                                      |                                     |
| ファイル<br>Set the m<br>This scar<br>AntiVirus<br>スキャン  | スキャン<br>aximum file size to scan.<br>size limit also limits the maximum size o<br>scan limit to higher than 10 MB, APT Blo<br>サイズの制限 5120 🗼 KB   | f files analyzed by<br>cker analyzes file | y APT Blocker, I<br>is only up to 10 | fyou set the Gateway<br>MB in size. |

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。

| 7 <u>1</u> ∪<br>[⊊#]               | 全般的な Gateway AntiVirus 設定  |                            |                       |  |
|------------------------------------|--|----------------------------|-----------------------|--|
| ■ HTTP 要求<br>■ URL パス<br>■ HTTP 広答 | Gateway AntiVirus 設定は、URL Paths、 Content Types、および Boo<br>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 | dy Content Type<br>含だけ適用され | sの各ルールセットの [アク<br>ます。 |  |
|                                    | ☑ Gateway AntiVirus を有効化する   |                            |                       |  |
| └──本文のコンテンツの種類                     | 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                     | ☑ ¤∅                  |  |
|                                    | コンテンツがスキャン サイズの制限を超過した場合 (Fireware Of  | sv1201以隆):                 |                       |  |
|                                    | 許可:応答の通過を許可する ✓  | 「アラーム                      |                       |  |
|                                    | コンニンンが成果化されている根金(ジョン・マック・ペク・ペイン・パート  |                            |                       |  |
|                                    | コンテンツが暗ちにされている場合 (Fireware US V12.0.1 以降)-<br>注意: 広気の通過を注意する                                   |                            |                       |  |
|                                    | al J. Abarovaniz dal 13 5  |                            |                       |  |
|                                    | ファイルスキャン   |                            |                       |  |
|                                    | Set the maximum file size to scan.   |                            |                       |  |
|                                    | This scan size limit also limits the maximum size of files analyzed by                         | APT Blocker. If            | fyou set the Gateway  |  |
|                                    | Antivirus scan limit to higher than 10 MB, APT Blocker analyzes file                           | is only up to TU           | MB IN SIZE.           |  |
|                                    | スキャンサイズの制限 5120 🔶 KB   |                            |                       |  |
|                                    |  |                            |                       |  |
|                                    |  |                            |                       |  |
|                                    |  |                            |                       |  |
|                                    |  |                            |                       |  |
|                                    | 1  |                            |                       |  |

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。

| ──全般   | URL パス 表示の変更                               |
|--|--|
| カテゴリ<br>- 全<br>HTTP 東求<br>- URL パス<br>- HTTP 応答<br>- コンテンツの種類<br>- 本文のコンテンツの種類 | ルール(簡易表示)         表示の変更                    |
|  | バターン:<br>アクション<br>一致した場合: 許可<br>アラーム<br>ログ |

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。

| 全般  | コンテンツの種類   | 表示の変    |
|---|--|---------|
| □ HTTP 要求   | 「ルール (簡易表示)  |         |
| 日 HTTP 5ま<br>↓ ↓ URL バス<br>日 HTTP 応答<br>↓ コンデンツの種類<br>↓ 本文のコンデンツの種類 | HTTP-tunnelled RTSP stream types<br>All XML application types<br>All application types<br>All audio types<br>All font types<br>All inage types<br>All encapsulated message types<br>All model types<br>All model types<br>All wideo types<br>All video types<br>Missing or empty |         |
|   | バターン: 違加 副務<br>アクション   | 事前定競演み  |
|   | →致した場合: AVスキャン 🗸 🗌 アラー   | L 🗌 🛛 🖓 |

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。

|   | 本文のコンテンツの種類  | 表示の変更        |
|---|--|--------------|
| HTTP 要求                                 | - ルール (簡易表示)   |              |
| HTTP になる<br>→ コンテンツの種類<br>→ 本文のコンテンツの種類 | Java bytecode<br>ZIP archive<br>Windows EXE/DLL<br>Windows CAB archive |              |
|   |  | 18 hn Ballfa |

[OK]をクリックして、中央構成の画面に戻ります。

[File Exceptions]ボタンからは各ファイルに、ファイルのスキャンを許可するかドロップするかを指定します。 [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。

|   | フロキシの種類                              | 種類<br>Finanuall       | Gateway AV                    | 槽    |
|---|--------------------------------------|-----------------------|-------------------------------|------|
| HTTP-proxy  | HTTP                                 | Firewall              | 有効                            |      |
|   |                                      |                       |                               |      |
| 〔1)<br>「1)<br>「1)<br>「1)<br>「1)<br>「1)<br>「1)<br>「1)<br>「 | i用される ルールのアクションが<br>ールのアクションが「AVスキャン | 「許可」から「A、<br>ン」から「許可」 | /スキャン」に変わります<br>に変わります。       | . [# |
| To configure the Gateway AntiVirus atta                   | achment settings, update server, a   | and file exceptions   | s, click the following buttor | 15.  |

File Exceptions ボタンをクリックすると、スキャンするファイルの例外リストが表示されます。例外ファイルとし てファイルの MD5 ハッシュ値を指定します。

| イル MD5 ハッシュ |   | 說明                   |    | アクション    | п <i>7</i> | j <u>e</u> t |
|-------------|---|----------------------|----|----------|------------|--------------|
|             | ■ ファイル例外を追加する<br>ファイル MDS ハッシュ<br>説明:<br>アクション: | :  <br> <br>   में ग | ри | Ø<br>:‡₹ | ×          | 546 2        |
| l           |   |                      |    |          |            |              |

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。

| ☑ 自動アップデートを   | 自効にする 間隔:  |   | 1 🔶 時間                        |
|---|--|---|-------------------------------|
| Intrusion Prever  | ntion と Application Contro   | ol 署名   |                               |
| Gateway AntiV   | irus 署名  |   |                               |
| Data Loss Preve   | ention 署名  |   |                               |
| 🗹 ボットネット検   | 出サイト データベース(   | Fireware OS v11.  | 11以降)                         |
| ✓ Geolocation ¥~  | - タベース (Fireware OS  | v11.12以降)   |                               |
| # = 16 =  |  |   |                               |
| ッーハー<br>アップデート サーバーの  | URLを入力   |   |                               |
|   |  |   |                               |
| https://services.watchgu  | uard.com   |   |                               |
| https://services.watchgu  | ard.com  |   |                               |
| https://services.watchgu<br>HTTP ブロキシ サーバー -  | uard.com   |   |                               |
| https://services.watchgu<br>HTTP ブロキシ サーバー<br>□ HTTP ブロキシ サーバ   | uard.com<br>バーを使ってアップデー  | トサーバーに接続  | する                            |
| https://services.watchgu<br>HTTP フロキシ サーパーー<br>□ HTTP フロキシ サーノ<br>IPv4 または IPv6 ア  <br>Firebox fi Freewate  | uard.com<br>パーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11 12 以路を実行し                                  | ト サーバーに接続<br>指定します。IPv6<br>アロろ必要があり                         | <b>する</b><br>アドレスを使用<br>! = す |
| https://services.watchgu<br>HTTP ブロキシ サーバー -<br>□ HTTP ブロキシ サー /<br>IPv4 または IPv6 ア I<br>Firebox か Fireware   | uard.com<br>Nーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し                                  | ト サーバーに接続<br>指定します。 IPv6<br>, ている必要があり                      | <b>する</b><br>アドレスを使用<br>!ます。  |
| https://services.watchgu<br>HTTP ブロキシ サーバー<br>□ HTTP ブロキシ サーバ<br>IPv4 または IPv6 ア<br>Firebox か Fireware<br>サーバー アドレス:  | uard.com<br>パーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>IPv4 アドレス                     | ト サーバーに接続<br>自定します。IPv6<br>でいる必要があり                         | <b>する</b><br>アドレスを使用!<br>!ます。 |
| https://services.watchgu<br>HTTP プロキシ サーバー<br>HTTP プロキシ サーバ<br>IPv4 または IPv6 ア<br>Firebox が Fireware<br>サーバー アドレス:<br>サーバー ボート:   | uard.com<br>N ー を使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>IPv4 アドレス<br>8080 ↓         | ト サーバーに接続<br>指定します。IPv6<br>ている必要があり                         | する<br>アドレスを使用<br>!ます。         |
| https://services.watchgu<br>HTTP プロキシ サーパー<br>□ HTTP プロキシ サーパ<br>IPv4 または IPv6 ア I<br>Firebox が Fireware<br>サーバー アドレス:<br>サーバー ボート:<br>サーバー認証:                                | uard.com<br>N ~ を使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>Pv4 アドレス<br>8080<br>*<br>なし | ト サーバーに接続<br>指定します。 IPv6<br>、ている必要があり<br>                   | <b>する</b><br>アドレスを使用<br>!ます。  |
| https://services.watchgu HTTP ブロキシ サーバー   | uard.com<br>パーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>PV4 アドレス<br>8080<br>なし        | ト サーバーに接続<br>指定します。IPv6<br>.ている必要があり<br> <br> <br>          | <b>する</b><br>アドレスを使用<br>!ます。  |
| https://services.watchgu<br>HTTP プロキシ サーバー<br>日 HTTP プロキシ サーバ<br>IPv4 または IPv6 ア I<br>Firebox が Fireware<br>サーバー アドレス:<br>サーバー ボート:<br>サーバー認証:<br>ユーザー名:<br>ドメイン:             | uard.com<br>パーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>IPv4 アドレス<br>8080<br>なし       | ト サーバーに接続<br>自定します。IPv6<br>ている必要があり<br> <br> <br>           | する<br>アドレスを使用<br>!ます。         |
| https://services.watchgu ITTP ブロキシ サーバー   | uard.com<br>パーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>PV4 アドレス<br>8080<br>なし        | ト サー バー に接続<br>指定します。 IPv6<br>. ている必要があり<br> <br> <br> <br> | <b>する</b><br>アドレスを使用:<br>!ます。 |
| https://services.watchgu<br>ITTP プロキシ サーバー -<br>□ HTTP プロキシ サーバ<br>IPv4 または IPv6 ア I<br>Firebox が Fireware<br>サーバー アドレス:<br>サーバー ポート:<br>サーバー認証:<br>ユーザー名:<br>ドメイン:<br>パスワード: | uard.com<br>パーを使ってアップデー<br>ドレスまたはホスト名を打<br>OS v11.12 以降を実行し<br>PV4 アドレス<br>私し                | ト サーバーに接続<br>指定します。IPv6<br>、ている必要があり                        | する アドレスを使用 します。               |

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。

|                 | 144 54              | <b>坦</b> —           |
|-----------------|---------------------|----------------------|
| JT OUT          | (筬形                 |                      |
| WORK<br>KS WITH | Gateway Anti-Virus  | Bitdefender, Cylance |
| -               | WebBlocker          | FORCEPOINT           |
| STAR            | spamBlocker         | Cyren                |
| URITY           | 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。

| ⊒ <mark></mark> ブロキシ   | ポリシー テンプレー                | トプロパティ       |  |
|--|---------------------------|--------------|--|
| DNS-proxy Explicit-proxy   | POP3-proxy                |              |  |
| Exploit-proxy     FTP-proxy     H323-ALG     HTTP-proxy     HTTPS-proxy     MAP-proxy     POP3-proxy     SIP-ALG | POP3 ポート<br>110           | プロトコル<br>TCP |  |
|  | POP3S ポート<br>995          | フロトコル<br>TCP |  |
| ● SMTP-proxy<br>● TCP-UDP-proxy<br>● ろイルタ  | Fireware OS v12.2 J<br>說明 | 以降。          |  |
|  | ポスト オフィス ブ                | ロトコル V3      |  |
| キョウリナ酸油ナス  |                           |              |  |

SMTP も spamBlocker を使うことができますが、SMTP-proxy は、Firebox 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 <u>セキュリティサービス</u> — <u>spamBlocker</u> — <u>アクティブにする</u> をクリックします。

| द C:¥Users¥tsuto¥Documents¥My WatchGuard¥config<br>ファイル 編集 表示 セットアップ ネットワーク FireClus   | s¥T50-W-<br>ster VPN  | MAY29.xml *- Fireware Policy Manag<br>セキュリティサービス ヘルプ  | er   |  | - 0  | ×               |
|--|---|---|--|--|--|-----------------|
| アクション<br>ボリシー名<br>1<br>シー<br>イアウオール<br>Mobile VPN with IPSec<br>順序 / アクション<br>ボリシー名<br>1<br>シー<br>マイアウオール<br>Mobile VPN with IPSec<br>第月<br>・<br>アクション<br>ボリシー名<br>1<br>シー<br>、<br>第日<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・ | FTP-pro<br>HTTP-p<br>HTTP-P<br>WG-Ceir<br>WG-Firr<br>Ping<br>DNS<br>WG-Firr<br>TCP-UD | Application Control<br>APT Blocker<br>ボットネット検出<br>Data Loss Prevention<br>DNSWatch<br>Gateway AntiVirus<br>Geolocation<br>Intrusion Prevention<br>モバイルセキュリティ<br>Quarantine Server<br>Reputation Enabled Defense<br>spamBlocker<br>Threat Protection | 送信元<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>アクティブ<br>構成 | フィルタ: なし<br>送信先<br>Any-External<br>Any-External<br>Firebox<br>Firebox<br>Any<br>Any-External<br>Firebox<br>Ligto | xt - h           tcp:21           tcp:80           tcp:443           tcp:4126           tcp:8080           icmp (type: 8, code: 255)           tcp:53 udp:53           tcp:4105 tcp:4117 tcp:411           tcp:0 (Any) udp:0 (Any) | P 7-            |
| <  |   | WebBlocker 2  | •  |  | Fireware   | ><br>05 v12.4.0 |

### ウィザードが始まります。

| ようこそ。   |
|---|
| Activate spamBlocker Wizard $\Lambda$             |
| このウィザードを使用して、spamBlocker をアクティブに<br>し、基本構成を作成します。 |
|   |
| 詳細性報 snamPlocker                                  |
|   |

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。[次へ]。

| pamB           | lockerの設定をポリシー                     | に適用します                      | N                     | atchGua      |
|----------------|------------------------------------|-----------------------------|-----------------------|--------------|
| ະດຸມ           | ストにはアクティブなポリシ                      | ーが含まれていますが、                 | それらのポリシー              | - に対応する      |
| spamBl<br>フティ: | ockerが有効になっていませ<br>ブにするには、[選択] チェッ | ん。アクティブなポリシ<br>ク ポックスをオンにして | vーに対応する spi<br>てください。 | amBlocker をア |
| 選択             | ポリシー名                              | 轴颈                          | プロキシの                 | snamBlocker  |
| $\checkmark$   | POP3-proxy                         | POP3                        | Firewall              | 無効           |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |
|                |                                    |                             |                       |              |

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]。

| 🕵 Activate spamBlocker Wizard | ×               |
|-------------------------------|-----------------|
| 新しいプロキシポリシーを作成します             | WatchGuard      |
| 新しいプロキシ ポリシーを作成する場合は、必要なポリシー  | を選択してください。      |
| □ 受信 SMTP                     |                 |
| ●子メール サーバーの ℙアドレス: ┃          |                 |
| ■ IMAP (Fireware OS v12.0 以降) |                 |
|                               |                 |
|                               |                 |
|                               |                 |
|                               | 効になります。 ウィザードを完 |
|                               |                 |
|                               | (戻る 次へ) キャンセル   |
|                               |                 |

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<u>セキュリティサービス</u> — <u>spamBlocker</u> — <u>構成</u> 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。

| 41.2.2. H  | プロキシの種類 | 種類       | spamBlocker | 梯    |
|------------|---------|----------|-------------|------|
| POP3-proxy | POP3    | Firewall | 有効          | -    |
|            |         |          |             | 1.33 |
|            |         |          |             |      |
|            |         |          |             |      |

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。

| スパムカテゴリさ | とにアクションを選択してくだ   | さい。           |                 |
|----------|------------------|---------------|-----------------|
| 確認されたスパム | : サブジェクト タグの追加 ~ | ***SPAM***    | ✓ ログ メッセージを送信する |
| パルク:     | サブジェクト タグの追加 🗸   | ***BULK***    | 🚽 ログ メッセージを送信する |
| 未確認:     | サブジェクト タグの追加 🕹   | ***SUSPECT*** | 🔽 ログ メッセージを送信する |
| 🗹 スパムではな | いと分類された電子メールごとに  | こログ メッセージを送信  | する              |

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 ポリシー POP3-       | əroxy の spamBlocker の構成   | ×            |
|--------------------|---|--------------|
| ✓ spamBlocker ঠ    | 有効にする   |              |
| アクション例外            | Virus Outbreak Detection  |              |
| 以下の送信者ル<br>連のルールは構 | - ルのいずれかに一致する電子メール トラフィックは spamBlocker をバイパ<br>或されているとおりに適用されます。                      | スします。他のプロキシ関 |
| アクション              | 送信者   | 追加           |
|                    |   | 編集<br>削除     |
|                    | 列外ルールの追加 ×  | t o          |
| アク<br>ドレ<br>す。     | ションを選択し、送信者を入力してください。送信者には、モ子メール ア<br>ス (abc@xyz.com) またはパターン (*@xyz.com) を指定することができま |              |
| アク                 | ション: 許可 /   | エクスポート       |
| 送信                 | <b>#</b> :  |              |
| ☑上のι               | OK キャンセル  |              |
|                    | ОК + -  | マンセル ヘルプ     |

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

| spamBlocker を有効にする         アクション 例外 Virus Outbreak Detection         ウイルス検出時:         削除: メッセージのバーツを削除する         マラーム Cのアクションを記録する         スキャンエラー発生時:         削除: メッセージのバーツを削除する         回除: メッセージのバーツを削除する         アラーム Cのアクションを記録する | n ボリシー POP3-proxy の spamBlocker の構成  | 9         |
|--|--------------------------------------|-----------|
| アクション       例外       Virus Outbreak Detection         ウイルス検出時:       御除: メッセージのバーツを削除する       アラーム       このアクションを記録する         スキャンエラー発生時:       開除: メッセージのバーツを削除する       アラーム       このアクションを記録する                                       | ☑ spamBlocker を有効にする                 |           |
| ウイルス検出時:   | アクション 例外 Virus Outbreak Detection    |           |
| <ul> <li>■除:メッセージのパーツを削除する</li> <li>■ アラーム ○ このアクションを記録する</li> <li>スキャン エラー発生時:</li> <li>■除:メッセージのパーツを削除する</li> <li>● アラーム ○ このアクションを記録する</li> </ul>   | ウイルス検出時                              |           |
| スキャンエラー発生時:<br>副除:メッセージのバーツを副除する アラーム C このアクションを記録する<br>OK キャンケル ヘルブ   | 削除:メッセージのパーツを削除する 🚽 🗌 アラーム 🖌 このアクション | を記録する     |
| 副除:メッセージのバーツを削除する アラーム Cのアクションを記録する  | スキャン エラー発生時;                         |           |
| 0K キャンヤル ヘルブ   | 削除:メッセージのパーツを削除する 🚽 🗌 アラーム 🔽 このアクション | を記録する     |
| 0K キャンヤル ヘルブ   |                                      |           |
| 0K キャンヤル ヘルプ   |                                      |           |
| OK キャンヤル ヘルプ   |                                      |           |
| 0K キャンセル ヘルブ   |                                      |           |
| OK キャンセル ヘルブ   |                                      |           |
|  | ОК                                   | キャンセル ヘルプ |

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。

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。

Firebox 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 $\underline{t+u}$ $\underline{t+u}$ - $\underline{Intrusion Prevention}$ をクリックします。

| <u> ای</u> 🗁 🔙<br>ファイアウオール | V + X   ₩ 2 K   0 "A<br>Mobile VPN with IPSec   | <i>*</i> *  | Application Control<br>APT Blocker<br>ボットネット検出<br>Data Loss Prevention   |  | フィルタ: なし  | ~ ¥ ¥  |
|----------------------------|---|---|--|--|---|--|
| 順序 / アクシ                   | ョン ポリシー名  |   | DNSWatch   | 送信元  | 送信先   | ポート  |
| 1                          | TFP-proxy TTP-proxy TTP-proxy TTP-proxy TTP-proxy WatchGuard Certificate Portal WatchGuard Web UI TDP-proxy DNS POP3-proxy WatchGuard Utgoing Utgoing | FTP-pro<br>HTTP-pr<br>HTTP<br>WG Cer<br>WG Eire<br>Ping<br>DNS<br>POP3-p<br>WG-Fire<br>TCP-UD | Gateway AntiVirus<br>Ceolocation<br>Intrusion Prevention<br>セバイル ビチュウティ<br>Quarantine Server<br>Reputation Enabled Defense<br>spamBlocker<br>Threat Protection<br>WebBlocker | <ul> <li>Any-Optional</li> <li>Optional</li> <li>Any Optional</li> <li>Any Optional</li> <li>Any-Optional</li> <li>Any-Optional</li> <li>Any-Optional</li> <li>Any-Optional</li> <li>Any-Optional</li> <li>Any-Optional</li> </ul> | Any-External<br>Any-External<br>Any-External<br>Firebox<br>Firebox<br>Any-External<br>Firebox<br>Any-External | tcp:21<br>tcp:80<br>tcp:4126<br>tcp:5080<br>icmp (type: 8, code: 255)<br>tcp:5100;53<br>tcp:110 tcp:995 (tls)<br>tcp:4105 tcp:4117 tcp:4118<br>tcp:0 (Any) udp:0 (Any) |

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。

| 中威レベル                       | アクション:                 |        | アラーム | ログ |  |
|-----------------------------|------------------------|--------|------|----|--|
| 重大                          | 切断                     | $\sim$ |      |    |  |
| 高                           | 切断                     | ~      |      |    |  |
| ÷                           | 切断                     | ~      |      |    |  |
| 低                           | 切断                     | ~      |      |    |  |
| 情報                          | if可                    | ~      |      |    |  |
| <b>例</b> 外…<br>通知<br>サーバーのI | 例外: なし<br>通知: なし<br>更新 |        |      |    |  |

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。

| 重大 | _\$J)£h ▼ | <b>v</b> |
|----|-----------|----------|
| 高  | 切断 🗸      | <b>V</b> |
| 中  | [許可 🗸     | <b>V</b> |
| 低  | 許可 🗸      | <b>V</b> |
| 情報 | [許可 🗸     |          |

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

| 🔣 アップデート サーバー   |                  | ×      |
|---|------------------|--------|
| 自動アップデート<br>✓ 自動アップデートを有効にする  | <b>間際</b> :      | 1 💽 時間 |
| ✓ Intrusion Prevention と Applica ✓ Gateway AntiVirus 署名 □ Data Loss Prevention 署名 | ation Control 署名 |        |

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。

| 🔣 Int | rusion Preven   | tion Service     |           |            |      | ×   |
|-------|-----------------|------------------|-----------|------------|------|-----|
| 設定    | ポリシー            |                  | $\square$ |            |      |     |
|       | Intrusion Preve | ention を有効にする    |           |            |      |     |
| 3     | スキャンモード         | : ○フルスキャン        | () 高      | 速スキャン      |      |     |
| 4     | 中威レベル           | アクション:           |           | アラーム       | ۵Ő   |     |
|       | 重大              | 切断               | ~         |            |      |     |
|       | 高               | 切断               | ~         |            |      |     |
|       | ÷               | 切断               | 4         |            |      |     |
|       | 低               | 切断               | ~         |            |      |     |
|       | 情報              | 許可               | ~         |            |      |     |
| ī     |                 |                  |           |            |      |     |
| -     | 1例外···· 1       | 例外: なし<br>画知: なし |           |            |      |     |
| 1     | サーバーの夏          | 〔新…              |           |            |      |     |
| Ţ     |                 |                  |           |            |      |     |
|       |                 |                  |           |            |      |     |
|       |                 |                  |           |            |      |     |
|       |                 |                  |           |            |      |     |
|       |                 |                  | 0         | к <b>+</b> | ャンセル | ヘルブ |

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。

| f+ UTTD In a man in a   |  |  |              |                 |                |          |      |
|---|--|--|--------------|-----------------|----------------|----------|------|
| . HITP-incomming  |  |  |              |                 |                |          |      |
| リシー プロパティ   | ≣¥\$⊞  |  |              |                 |                |          |      |
|   |  |  |              |                 |                |          |      |
| TTP接続を…   | -  | DOTO WAS   |              |                 |                |          |      |
| F •J  | V ILF  | H310/3516  |              |                 |                |          |      |
| 送信元   |  |  |              |                 |                |          |      |
| 🛠 Any-External  |  |  |              |                 |                |          |      |
|   |  |  |              |                 |                |          |      |
|   |  |  |              |                 |                |          |      |
|   |  |  |              |                 |                |          |      |
|   |  |  |              |                 | `8 bo          | 伊佑       | 出口自己 |
|   |  |  |              |                 | 36.70          | \$19 5%c | 四星纪术 |
| 差信先   |  |  |              |                 |                |          |      |
| ₩ External-1>   | 10.100.10.101  |  |              |                 |                |          |      |
| External-1>   | 10.100.10.101  |  |              |                 | 追加             | 編集       | 副除   |
| External-1>   | raffic using   | WAN Resert Position  | (Fireware OS | v17 3 or hinker | <b>ìù hu</b>   | 編集       | 削除   |
| External-1>   | raffic using SI  | )-WAN Based Routing  | (Fireware OS | v12.3 or higher | <u>iê h</u> 0) | 編集       | 削除   |
| External-1> Route outbound t  | raffic using St  | )-WAN Based Routing  | (Fireware OS | v12.3 or higher | <u>追加…</u> )   | 編集       | 削除   |
| External-1> Route outbound t SD-WAN Action  | raffic using SI  | -WAN Based Routing   | (Fireware OS | v12.3 or higher | <b>i£ 10</b> ) | 編集       | 削除   |
| External-1> CROUTE OUTBOUND 1 SD-WAN Action   | raffic using SI  | -WAN Based Routing   | (Fireware OS | v12.3 or higher | 38 MD)         | 編集       | 削除   |
| External-1>     External-1>     Route outbound t     SD-WAN Action  | raffic using SI  | -WAN Based Routing   | (Fireware OS | v12.3 or higher | )              | 編集       | 削除   |
| External-1> C Route outbound t SD-WAN Action  | 10.100.10.101<br>raffic using SI<br>を有効にします  | -WAN Based Routing   | (Fireware OS | v12.3 or higher | )              | 編集       | 削除   |
| External-1> C Route outbound t SD-WAN Action Application Control  | (0.100.10.101<br>10.100.10.101<br>raffic using SI<br>を有効にします<br>化する                            | -WAN Based Routing   | (Fireware OS | v12.3 or higher | <u>追加…</u> )   | 編集       | 削除   |
| External-1> C Route outbound t SD-WAN Action Application Control Coolocation を有効 このポリシーの PP   | (0.100.10.101<br>10.100.10.101<br>raffic using SI<br>を有効にします<br>化する<br>S を有効にします               | -WAN Based Routing   | (Fireware OS | v12.3 or higher | <u>追加…</u> )   | 編集       | 削除   |
| External-1→<br>External-1→<br>Route outbound t<br>SD-WAN Action<br>Application Control<br>のたolocation を有効<br>このポリシーの IPS              | (0.100.10.101<br>10.100.10.101<br>raffic using SI<br>を有効にします<br>化する<br>S を有効にします<br>- 夕を有効にします | WAN Based Routing Global Global (Fireware OS v11.1)                            | (Fireware OS | v12.3 or higher | <u>,追加…</u> )  | 編集       | 削除   |
| ■ External-1 →<br>External-1 →<br>Route outbound t<br>SD-WAN Action<br>Conversion Control<br>Conversionを有効<br>このポリシーの PC<br>常期幅と時間クォー | 10.100.10.101<br>10.100.10.101<br>raffic using SI<br>を有効にします<br>化する<br>S を有効にします<br>- タを有効にする  | O-WAN Based Routing  Market Based Routing  Global  Global  (Fireware OS v11.1) | (Fireware OS | v12.3 or higher | <u>追加…</u> )   | 編集       | 削除.  |
| External-1→ External-1→ Route outbound t SD-WAN Action Application Control Geolocation を有効 さのポリシーの PP 常城幅と時間クォ・ 7 ロミシ アクション:          | (0.100.10.101<br>10.100.10.101<br>raffic using SI<br>を有効にします<br>化する<br>S を有効にします<br>- タを有効にする  | D-WAN Based Routing  | (Fireware OS | v12.3 or higher | <u>iê h0</u> ) | 編集       | 削除   |
| External-1→ External-1→ Route outbound t SD-WAN Action Application Control Geolocation を有効 このポリシーの PP 律域幅と時間クォー 7 ロミシアクション:           | to.100.10.101<br>10.100.10.101<br>でaffic using SI<br>を有効にします<br>化する<br>S を有効にします<br>- タを有効にする  | D-WAN Based Routing  | (Fireware OS | v12.3 or higher | <u>ie ho</u> ) | 編集       | 削除   |

「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 Firebox 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。

| 💽 Firebox System Manager - 10.0.0.1 [接続済み]   |  |
|--|--|
| ファイル 表示 ツール ヘルプ  |  |
| o   🛱 🖬   🔣 🔟   🔓  |  |
| コロントリクシル トラフィック モニタ 帯域値マーター サードス ウォッチ ステーム   | なて しまート 「四部リフト」 ブロックされたサイト」 セキュリティサービス   |
|  |  |
|  | <b>↓ / ∧</b>   |
| inature name="EXPLOIT web directory traversal -2" signature cat="\   | web Attack" signature Id="1054849" seventv="4"   |
| nature_name="EXPLOIT remote file inclusion /etc/passwd" signatur   | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| inature_name="EXPLOIT remote file inclusion /etc/passwd" signatur  | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| nature_name="VULN Cross-site Scripting Attempt -11" signature_ca   | at="Access Control" signature_id="1050015" severity="4"<br>t="#access Control" signature_id="4050045" severity="4" |
| rature_name= VOLN cross-site Scripting Attempt-11 signature_cat<br>inature_name="VULN Cross-site Scripting Attempt-11" signature_ca      | t= Access Control signature_id= 1050015 seventy= 4<br>at="Access Control" signature_id="1050015" seventy="4"       |
| inature_name="EXPLOIT remote file inclusion win ini" signature_cat   | ⊨"Web Attack" signature_id="1054838" severity="4"  |
| inature_name="EXPLOIT remote file inclusion /etc/passwd" signatur  | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| ature_name="EXPLOIT SQL injection attempt -6" signature_cat="We  | eb Attack" signature_id="1054840" severity="5"   |
| nature_name="HTTP lishack2000" signature_cat="Buffer Over Flow"  | " signature_id="1090256" seventy="4"<br>W/oh Attack" cignature_id="1054940" covority="4"                           |
| lature name="EXPLOIT web directory traversal-2" signature cal-   | cat="Web Attack" signature_id="1054645" sevent(= 4   |
| nature_name="EXPLOIT remote file inclusion /etc/passwd" signatur   | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| iature_name="EXPLOIT remote file inclusion /etc/passwd" signature  | e_cat="Web Attack" signature_id="1054837" severity="4"   |
| inature_name="EXPLOIT remote file inclusion /etc/passwd" signatur  | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| inature_name= EXPLOIT remote file inclusion letchasswd_signatur  | re_cal= vveb Allack_signature_lu= 1054837_seveniv= 4<br>re_cat="\/\eh_Attack" signature_id="1054837" severity="4"  |
| inature name="EXPLOIT remote file inclusion /etc/passwd" signatur  | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| ature_name="EXPLOIT remote file inclusion /etc/passwd" signature   | e_cat="Web Attack" signature_id="1054837" severity="4"   |
| inature_name="EXPLOIT remote file inclusion /etc/passwd" signatur  | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| inature_name="EXPLOIT remote file inclusion /etc/passwd" signatur  | re_cat="Web Attack" signature_id="1054837" severity="4"  |
| lature_name="EXPLOIT remote file inclusion /etc/passwd" signature  | re_cat="Web Attack" signature_id="1054837" seventy= 4<br>re_cat="Web Attack" signature_id="1054837" seventy="4"    |
| lature_name="EXPLOIT remote file inclusion/etc/passwd" signature   | e_cat="Web Attack" signature_id="1054837" seventy="4"  |
| ature_name="EXPLOIT remote file inclusion /etc/passwd" signature   | e_cat="Web Attack" signature_id="1054837" severity="4"   |
| iature_name="EXPLOIT web directory traversal -2" signature_cat="VV   | /eb Attack" signature_id="1054849" severity="4"  |
| nature_name="EXPLOIT web directory traversal -2" signature_cat="\  | vVeb Attack" signature_id="1054849" severity="4"   |
| nature_name= EXPLOIT web directory traversal -2" signature_cat="\<br>instruce_name="EXPLOIT web directory traversal -2" signature_cat="\ | Web Allack Signature_ld=1054849 Severity= 4"<br>Web Attack" signature_id="1054849" severity="4"                    |
| <pre>//indiaro_name= EXF_EON_web_anetiony.indversar=z_orginature_tat= 1 /</pre>  |  |
|  |  |
| 史新間場 5秒 ▼ 一時停」   |  |
|  |  |

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。

|   |                            | メーター サードフ ウォッチ フテータフ   | しポート 認証117  |
|---|----------------------------|--|-------------|
| グロックされたサイト セキュリティサービス   | ゲード                        | אין  | り管理 ユーザークォー |
| iateway Antivirus   |                            |  |             |
| 前回の再起動以降のアクティビティ<br>ウイルス検知: 0<br>スキャンされたオブジェクト数: 566<br>スキャンされていないオブジェクト数: 27 | 第名<br>  イン<br>  前回<br>  利用 | 5<br>ストールしたバージョン: 20190604.1645<br>回の更新: 2019/06/05 10:06:20 JST<br>月可能なバージョン: 20190604.1645 | 履歴          |
| pplication Control および Intrusion Prevent                                      | on Service                 |  |             |
|   |                            |  |             |
| Intrusion Prevention スキャンが実行されま<br>検出された侵入:<br>防御された侵入:                       | した: 5,898,852<br>0<br>0    | インストールしたパージョン: 4.942<br>前回の更新: 2019/06/05 2:04:44 JST<br>利用可能なパージョン: 4.942                   | 履歴<br>表示 更新 |
| アプリケーション スキャンが実行されました:<br>Applications detected:<br>Applications denied:      | 27,743<br>27,341<br>1      |  |             |
| /ebBlocker  |                            |  |             |
| Total requests: 14,697<br>Denied requests: 0                                  |                            |  |             |
| pamBlocker(前回の再起動以降のアクティビ:  | ī-л)                       |  |             |
| スパムと確認されたメッセージ: 0(0%)<br>コピーの際いがまるようた。 0(0%)                                  |                            | ブロックされたメッセージ: 0 (0%)<br>ちどがどくどうちょうよう 0 (0%)  |             |
| スパムのまたいがあるメッセージ: 0(0%) クリーンメッセージ: 0(0%)                                       |                            | 多りからいちんにメッセージ: 0(0%)<br>検疫されたメッセージ: 0(0%)  |             |
| バルク メールとマークされたメッセージ: 0 (0%)<br>処理されたメッセージの合計数: 0                              |                            | ホワイト/ブラックリスト上のメッセージ: 0(0%)   |             |
| eputation Enabled Defense (前回の再起動   | 以降のアクティビティ)                | )  |             |
| ローカル バイパス (良い): 0(0%)   |                            | 正常な処理(スコア不確定): 1,109(95.52%)   |             |
| ブロック済みの URL (悪(い): 0 (0%)   |                            | 評判リレックアップ: 1,161   |             |
| eolocation  | 10.000                     |  |             |
| 前回の再起動以降のアクティビティ  | データ                        | ベース  |             |

## 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。

| 一者治し    | カテゴリ      | 脅威レベル | 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1                      |
|---------|-----------|-------|---|
| 1049193 | バッファ オーバー | 高     | SHELLCODE x86 NOOP - 1 - The NOP allows an attacker to        |
| 1049802 | Web 攻撃    | 重大    | WEB Directory Traversal -4 - This event may indicate an atter |
| 1049945 | バッファ オーバー | 重大    | WEB Microsoft IIS Chunked Encoding Transfer Heap Overflow     |
| 1050153 | バッファ オーバー | 重大    | WEB Microsoft IIS 5.0 printer ISAPI Extension Buffer Overflow |
| 1050435 | アクセス制御    | 高     | SHELLCODE Microsoft Windows CMD.EXE Reverse Shell - Th        |
| 1050436 | バッファ オーバー | 重大    | WEB Microsoft IIS CodeRedv2 (CVE-2001-0500) - An uncheck      |
| 1050515 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Workstation Service Remote Buff     |
| 1050516 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Workstation Service Remote Buff     |
| 1050580 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Workstation Service Remote Buff     |
| 1050581 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Workstation Service Remote Buff     |
| 1050692 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Workstation Service Remote Buff     |
| 1050693 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Workstation Service Remote Buff     |
| 1050694 | Web 攻撃    | 高     | WEB SQL injection attempt -41 - SQL injection is a vulnerabil |
| 1050700 | Web 攻撃    | 重大    | WEB Cross-site Scripting (document.cookie) attempt - Cross-   |
| 1050703 | バッファ オーバー | 重大    | EXPLOIT Microsoft Windows Messenger Service Buffer Overru     |
| 1050874 | バッファ オーバー | 重大    | EXPLOIT Microsoft ASN.1 Library Bitstring Heap Overflow (CV   |
| 1051701 | 7 m/lk    | **    | WED OTTAT OF A LITTLE OF MULLET                               |

## 検索すると、該当の行にフォーカスが当たります。

| / 署名 ID | カテゴリ      | 脅威レベル |  |
|---------|-----------|-------|--|
| 1054692 | アクセス制御    | 高     | EXPLOIT Microsoft Windows Workstation Service memory corru     |
| 1054693 | アクセス制御    | 高     | TELNET Microsoft Windows Telnet Credential Reflection vulne    |
| 1054704 | DoS/DdoS  | 高     | WEB Squid strListGetItem Denial of Service (CVE-2009-2855)     |
| 1054713 | アクセス制御    | 高     | NETBIOS Microsoft Windows SMB Negotiate Request Remote         |
| 1054718 | DoS/DdoS  | 高     | DOS Microsoft Windows TCP Orphaned Connections denial of       |
| 1054778 | その他       | 重大    | FILE Microsoft Office Excel Featheader Record memory corrup    |
| 1054794 | バッファ オーバー | 重大    | WEB HTTP Accept-Language Header Buffer Overflow - The v        |
| 1051700 |           | 「王子」  | WED NTTO Host Hostor Dattor One flore The nationability is     |
| 1054837 | Web 攻撃    | 重大    | WEB Remote File Inclusion /etc/passwd - Remote attackers (     |
| 1054000 |           | 幸大    | WED Local Ella Technica missisti - 1 Damata attachana anna     |
| 1054840 | Web 攻撃    | 高     | WEB SQL injection attempt -6 - SQL injection is a vulnerabilit |
| 1054841 | Web 攻撃    | 重大    | WEB SQL injection attempt -7 - SQL injection is a vulnerabilit |
| 1054843 | Web 攻撃    | 重大    | WEB Cross-Site Scripting attempt -5.a - Cross site scripting ( |
| 1054861 | Web 攻撃    | 重大    | WEB-CLIENT JavaScript Heap Exploitation -1 - JavaScript he     |
| 1054862 | バッファ オーバー | 高     | IEC/ICCP ICS 7T Interactive Graphical SCADA System File O      |
| 1054875 | アクセス制御    | 高     | WEB-CLIENT Microsoft Internet Explorer Redirect Memory Cor     |
| <       | 1         | 1     | ······································                         |
|         | 07        |       | 1 按带   |

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。

| スキャンモート | : ○フルスキャン | ◉高速スキャン |    |  |
|---------|-----------|---------|----|--|
| 春感レベル   | アクション:    | アラーム    | ログ |  |
| 重大      | 切断        | ~       |    |  |
| 高       | 切断        | ~       |    |  |
| -       |           |         |    |  |
|         | 許可        | × 🗆     |    |  |
| 情報      | 許可        | ~       |    |  |
| 侧外…     | 側外: なし    |         |    |  |
| 通知      | 通知: なし    |         |    |  |
| サーバーの   | 更新        |         |    |  |
|         |           |         |    |  |
|         |           |         |    |  |

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。

| スキャンモー  | F: ○フルスキャ              | 、<br>シ ⑧高 | 速スキャン |    |  |
|---|------------------------|-----------|-------|----|--|
| 春威レベル   | アクション:                 |           | アラーム  | ПĴ |  |
| 重大  | 切断                     | ~         |       |    |  |
| 高   | 切断                     |           |       |    |  |
| <b>ф</b>  | 許可                     | ~         |       |    |  |
| 1E  | 許可                     | ~         |       |    |  |
| 情報  | 許可                     | ~         |       |    |  |
| <ul><li>例外…</li><li>通知…</li><li>サーパーの</li></ul> | 例外: なし<br>通知: なし<br>更新 |           |       |    |  |

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。

| 署名 ID  |         | アクション: |               | アラーム | ログ |
|--------|---------|--------|---------------|------|----|
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
|        |         |        |               |      |    |
| 署名 ID: | 1054842 |        | š <u>ê</u> ho | 削除   |    |

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。

| 🌄 署名の例外 |        |      | ×  |
|---------|--------|------|----|
| 異名 ID   | アクション: | アラーム | 07 |
| 1054842 | 許可     |      |    |
|         |        |      |    |

#### 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、<br>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、<br>Gateway Anti-Virus が有効に設定されていると、HTTP プロキシに<br>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。

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。

| 🔣 ポリシーを追加する   |  |  | × |
|---|--|--|---|
| <ul> <li>■ パリシーと注加する</li> <li>新しいポリシーに対して事前定義済みまたはカフ</li> <li>■ プロキシ</li> <li>● DNS-proxy</li> <li>● Explicit-proxy</li> <li>● FTP-proxy</li> <li>● FTP-proxy</li> <li>● SITP-proxy</li> <li>● TCP-UDP-proxy</li> <li>● TCP-UDP-proxy</li> <li>● TCP-UDP-proxy</li> <li>● カスタム</li> </ul> | スタム ポリシーを選択<br>ポリシー テンプ<br>HTTP-proxy<br>ポート<br>80<br>説明<br>HTTP はハイパー<br>使ってインター<br>す。Watch Guar<br>キシとは異なり | とします。<br>レート ブロパティ<br>ブロトコル<br>TCP<br>・テキスト転送プロトコルです。World Wide Web を<br>ネット上で情報をやり取りするときに使用しま<br>d ポリシー "HTTP Proxy" は HTTP キャッシュプロ<br>ます。HTTP キャッシュ プロキシでは Web データ |   |
|   | のキャッシュが<br>る場合、ポリシ<br>する必要があり<br>は正常に動作し   | 制御されます。外部キャッシュ プロキシを使用す<br>ーを追加して、銀織に必要な送信ポリシーを有効に<br>ます。そのようにしない場合、外部への TCP 接続<br>ません。  | ~ |

そのまま[OK]をクリックし、ポリシーを追加します。

| ti HTTP-proxy  |  |                                 |      |     |
|--|--|---------------------------------|------|-----|
|  |  |                                 |      |     |
| (リシー プロパティ 詳細  |  |                                 |      |     |
| TTP-proxy 接続を  |  |                                 |      |     |
| キ可 ✓ TCP RS  | STの送信  |                                 |      |     |
| 送信元  |  |                                 |      |     |
| XX Any-Trusted   |  |                                 |      |     |
|  |  | ie hn                           | 編集   | 街時業 |
|  |  | X8.70                           |      |     |
| 送信先<br>餐 Any-External  |  | Jā //J                          | ]    |     |
| 送信先<br>餐 Any-External  |  | <u>ند میں</u><br>ن <u>د</u> میں | 編集   | 副路  |
| 送信先<br>餐 Any-External  | VAN Based Routing VAN Based Ro | 3皇为0<br>3皇为0                    | [編集  | 削除  |
| 送信先<br>Any-External  Route outbound traffic using SD-W SD-WAN Action   | VAN Based Routing (Fireware OS v12.3 or higher)  | 32.00                           | 福集   | 削殊  |
| 送信先<br>Any-External  Route outbound traffic using SD-W SD-WAN Action   | VAN Based Routing (Fireware OS v12.3 or higher)  | 3£ h0                           | 編集   | 副時  |
| 送信先<br>Any-External<br>Route outbound traffic using SD-W<br>SD-WAN Action<br>Application Control を有効にします:  | VAN Based Routing (Fireware OS v12.3 or higher)  | 32 30                           | 福朱   | 削除  |
| 送信先<br>Any-External<br>Route outbound traffic using SD-W<br>SD-WAN Action<br>Application Control を有効にします:<br>Geolocation を有効にする  | VAN Based Routing (Fireware OS v12.3 or higher)  | 3£ h0                           | ] 編集 | 前時  |
| 送信先<br>Any-External<br>Route outbound traffic using SD-W<br>SD-WAN Action<br>Application Control を有効にします:<br>Geolocation を有効にする<br>フェのポリシン の JPS を有効にします                       | VAN Based Routing (Fireware OS v12.3 or higher)  | 3£ h0                           | ] 編集 | 副明発 |
| 送信先<br>Any-External<br>Route outbound traffic using SD-W<br>SD-WAN Action<br>Application Control を有効にします:<br>Geolocation を有効にする<br>このポリシーの IPS を有効にします<br>本知道にと時間フォータを有効にてるの   | VAN Based Routing (Fireware OS v12.3 or higher)  | 3£ 30                           | - 編集 | 副務  |
| 送信先<br>Any-External<br>Route outbound traffic using SD-W<br>SD-WAN Action<br>Application Control を有効にします:<br>Geolocation を有効化する<br>このポリシーの IPS を有効にします。<br>常報幅と時間クォータを有効化する () | VAN Based Routing (Fireware OS v12.3 or higher)  Global Global Global Fireware OS v11.10 起降)   | 3£ 50                           |      | 削除  |

#### RED の構成

RED を有効にするために、ポリシーマネージャの <u>セキュリティサービス</u> – <u>Reputation Enabled Defense</u> をクリックします。

| <b>I</b> C:¥  | Jsers¥tsuto¥Doo  | cuments¥My WatchGuard¥configs   | ¥T50-W-N   | MAY29.xml- Fireware Policy Manager   | 6  |   | -   |                         | ×       |
|---|--|---|--|--|--|---|---|-------------------------|---------|
| 7747  | 補来 表示 ゼ<br>▲ 🗁 🖷   🏹<br>?ウオール Mobil  | + X   🖞 🛃 🗽   🛍 🦛   | 🎄 👫  | Application Control<br>APT Blocker<br>ボットネット検出<br>Data Loss Prevention   |  | フィルタ:なし   |   | ~ P                     | 7.      |
| 順序 /  | アクション  | ポリシー名   |  | DNSWatch   | 送信元  | 送信先   | ポート   |                         | PI      |
| 1<br>2<br>3<br>4<br>5<br>6<br>7<br>8<br>9<br>10<br>11 | > < > < > < > <p< td=""><td><ul> <li>FTP-proxy</li> <li>HTTP-incomming</li> <li>HTTP-proxy</li> <li>HTTPS-proxy</li> <li>WatchGuard Certificate Portal</li> <li>WatchGuard Web UI</li> <li>Ping</li> <li>DNS</li> <li>POP3-proxy</li> <li>WatchGuard</li> <li>Outgoing</li> </ul></td><td>FTP-pro<br/>HTTP<br/>HTTP-pri<br/>HTTPS-<br/>WG-Cer<br/>WG-Fire<br/>Ping<br/>DNS<br/>POP3-N<br/>WG-Fire<br/>TCP-UD</td><td>Gateway AntiVirus &gt;&gt;<br/>Geolocation<br/>Intrusion Prevention<br/>モバイルセキュリティ<br/>Ouarantine Server<br/>Reputation Enabled Defense<br/>spamBlocker &gt;&gt;<br/>Threat Protection<br/>WebBlocker &gt;&gt;</td><td>Any-Optional<br/>Any-Optional<br/>Any-Optional<br/>Any-Optional<br/>Any-Optional<br/>Any-Optional<br/>Any-Optional</td><td>Any-External<br/>External-1 → 1<br/>Any-External<br/>Any-External<br/>Firebox<br/>Any<br/>Any-External<br/>Any-External<br/>Firebox<br/>Any-External</td><td>tcp:21<br/>tcp:80<br/>tcp:43<br/>tcp:443<br/>tcp:4126<br/>tcp:5080<br/>icmp (type: 8, code:<br/>tcp:53 udp:53<br/>tcp:110 tcp:995 (tls)<br/>tcp:4105 tcp:4117 tc<br/>tcp:0 (Any) udp:0 (A</td><td>255)<br/>:p:4118<br/>(ny)</td><td></td></p<> | <ul> <li>FTP-proxy</li> <li>HTTP-incomming</li> <li>HTTP-proxy</li> <li>HTTPS-proxy</li> <li>WatchGuard Certificate Portal</li> <li>WatchGuard Web UI</li> <li>Ping</li> <li>DNS</li> <li>POP3-proxy</li> <li>WatchGuard</li> <li>Outgoing</li> </ul> | FTP-pro<br>HTTP<br>HTTP-pri<br>HTTPS-<br>WG-Cer<br>WG-Fire<br>Ping<br>DNS<br>POP3-N<br>WG-Fire<br>TCP-UD | Gateway AntiVirus >><br>Geolocation<br>Intrusion Prevention<br>モバイルセキュリティ<br>Ouarantine Server<br>Reputation Enabled Defense<br>spamBlocker >><br>Threat Protection<br>WebBlocker >> | Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional<br>Any-Optional | Any-External<br>External-1 → 1<br>Any-External<br>Any-External<br>Firebox<br>Any<br>Any-External<br>Any-External<br>Firebox<br>Any-External | tcp:21<br>tcp:80<br>tcp:43<br>tcp:443<br>tcp:4126<br>tcp:5080<br>icmp (type: 8, code:<br>tcp:53 udp:53<br>tcp:110 tcp:995 (tls)<br>tcp:4105 tcp:4117 tc<br>tcp:0 (Any) udp:0 (A | 255)<br>:p:4118<br>(ny) |         |
| <   |  |   |  |  |  |   |   |                         | >       |
|   |  |   |  |  |  |   | Firev   | vare OS                 | v12.4.0 |

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。

|                         | プロキシの種類                          | 缅珀               | Reputation Enabled Defense | 構成     |
|-------------------------|----------------------------------|------------------|----------------------------|--------|
| HTTP-proxy              | HTTP                             | Firewall         | 無効                         |        |
|                         |                                  |                  |                            | 有効     |
|                         |                                  |                  |                            | 無効     |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
|                         |                                  |                  |                            |        |
| ireware OS v12 0 以路 7개ナ | Penutation Fnahled Defense ti HT | TPS # - 15 - 7 D | キシ マクションに対して仕ポート さ         | カテいません |

RED が有効になります。
| Keputation Enabled Def                                 | fense                         |           |                            | ×  |
|--|-------------------------------|-----------|----------------------------|----|
| Reputation Enabled Defens<br>Reputation Enabled Defens | e ポリシー<br>se の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        | Reputation Enabled Defense | 構成 |
| HTTP-proxy   | HTTP                          | Firewall  | 有効                         |    |
|  |                               |           |                            | 有効 |
|  |                               |           |                            | 無効 |

## [構成]ボタンをクリックします。

| 🔣 Reputa                 | ation Enabled Defense                                  |             |                     |                            |    | × |
|--------------------------|--|-------------|---------------------|----------------------------|----|---|
| Reputation<br>Reputation | on Enabled Defense ポリシー<br>on Enabled Defense の構成を変更す? | るには、ポリシー名を逃 | 選択し、 <b>構成</b> をクリッ | クします。                      |    |   |
| ポリシ                      | -名   | プロキシの種類     | 種類                  | Reputation Enabled Defense | 構成 | 1 |
| HTTP-p                   | оху  | нттр        | Firewall            | 有効                         | L  | J |
|                          |  |             |                     |                            | 有効 |   |
|                          |  |             |                     |                            | 無効 |   |

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。

| 悪い評判のしきい値: | 90 🜩 範囲: 60 から 100) |
|------------|---------------------|
| 良い評判のしきい値: | 10 🛫 範囲: 1 から 40)   |
|            |                     |

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。

|           | 酸生産の調査の設定である。   |
|-----------|---|
|           | セキュリティ機能によってこの通信(Response )が拒否されました!  |
| Ę         | のサイトの閲覧が業務上必要な場合、またはこの結果について問い合わせたい場合は<br>以下の情報をメール本文に貼り付けて、 <u>情報システム課</u> までご連絡ください。  |
| 理由: reput | lation  |
| メノッド: GE  | ET CONTRACTOR OF CONT |
|           | .: www.eicar.org  |
| パス: /dow  | nload/eicar.com   |

※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。

Firebox 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。

Firebox 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 Firebox 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。