



WebUI ガイド



目次

第一章 XTM のセキュリティ概念	5
XTM のネットワーク概念	5
WebUI のネットワーク設定に見る XTM の概念	6
WebUI のポリシー設定画面に見る XMT の概念	7
XTM で実現可能なセキュリティ範囲	8
WebUI の概要	9
WebUI の制限事項	9
第二章 初期設定	10
事前準備	10
ファクトリーリセット	11
XTM2/3 シリーズ(330 除く)	11
XTM330/5/8/10/20 シリーズ	13
ファクトリーリセット後の設定	14
Web Setup Wizard.....	15
機能キーの追加.....	22
第三章 ネットワークの設定	24
外部ネットワークの設定	26
固定 IP の設定	28
DHCP の設定	28
PPPoE の設定	29
DNS/WINS 設定	30
DNS の設定	30
WINS の設定	31
内部ネットワークの設定	32
Trusted インターフェースの設定	32
DHCP サーバーの使用	33
ブリッジの構成	35
DMZ を設定する	39

NAT 設定 (1-to-1NAT).....	40
ルーティング設定	42
第四章 ファイアウォールの設定	44
ポリシー設定画面.....	44
画面構成.....	44
ポリシーの変更/追加/保存.....	46
ポリシーの追加.....	47
ポリシー追加 (内側から外側へ)	47
ポリシー追加 (外側から内側へ)	50
ポリシー追加 (SNAT で外側から内側へ).....	53
テンプレートにないポリシーを追加する	57
ポリシーの編集.....	60
一時的に無効にする	60
ログを記録する.....	61
運用スケジュールを設定する	62
ポリシー以外のファイアウォール設定	64
規定のパケット処理.....	64
ブロックされたサイト	65
ブロックされたポート	65
第五章 UTM の設定.....	66
プロキシポリシーの追加	67
プロキシアクションの追加	67
プロキシポリシーの追加.....	69
Web Blocker の設定.....	71
Web Blocker を構成する.....	71
Gateway AntiVirus の設定	78
Gateway AntiVirus を有効にする	78
Gateway AntiVirus を構成する.....	80
spamBlocker の設定	83

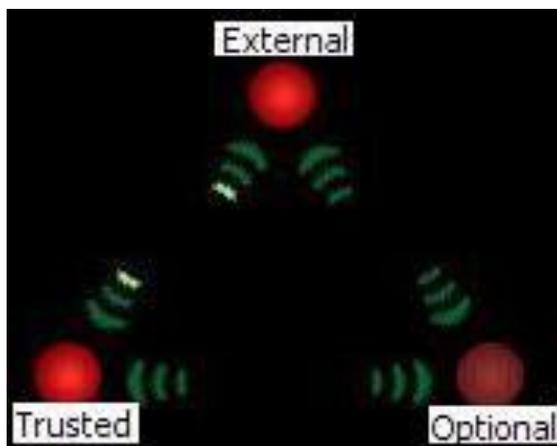
POP-Proxy アクションを追加する	83
POP3-proxy ポリシーを追加する	85
spamBlocker を構成する.....	87

第一章 XTM のセキュリティ概念

XTM のネットワーク概念

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

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



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

WebUI のネットワーク設定に見る XTM の概念

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

またそれらは固定ではなく自由に設定できます。

以下のネットワーク構成画面では、0 が External(外部)、3 が Optional(任意)、それ以外は Trusted(信頼済み)として設定しています。

ネットワーク インターフェイス

次のモ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 ▼

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

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

初期設定の External は 0 番ポートですが、それにとられる必要はありません。

WebUI のポリシー設定画面に見る XMT の概念

以下は実際のポリシー構成画面です。(後ほど詳しく解説します)

前述のネットワークの方向に従って設定されることが分かるでしょう。

The screenshot shows the 'ポリシー構成' (Policy Configuration) web interface. The policy name is 'FTP'. The action is set to '許可' (Allow). The source is 'Any-Trusted' and the destination is 'Any-External'. A large red arrow points from the source to the destination, labeled '方向!' (Direction!).

Annotations in red text:

- 名前: FTP → 何のプロトコルを?
- 接続は: 許可 → 許可? 拒否?
- 発信元: Any-Trusted → どこから?
- 方向! (indicated by a large red arrow pointing from source to destination)
- 送信先: Any-External → どこへ?

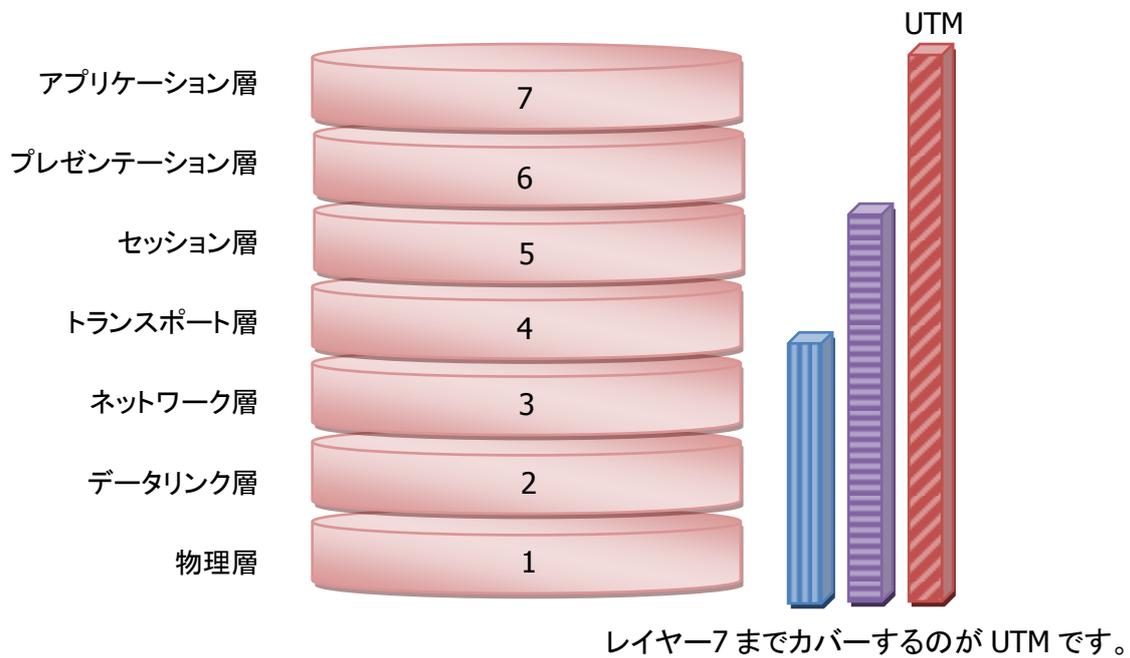
Buttons: 追加 (Add), 削除 (Delete) are present for both source and destination lists.

Options at the bottom:

- Application Control を有効にします
- このポリシーの IPS を有効にします
- Global (dropdown menu)

XTM で実現可能なセキュリティ範囲

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



-  パケットフィルター : ポートベース
-  ファイアウォール : ステートフルパケットインスペクション
-  UTM : コンテンツフィルタリング、IPS、アンチウイルスなどのプロキシ機能

WebUI の概要

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

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

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

WebUI の制限事項

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

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

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

第二章 初期設定

事前準備

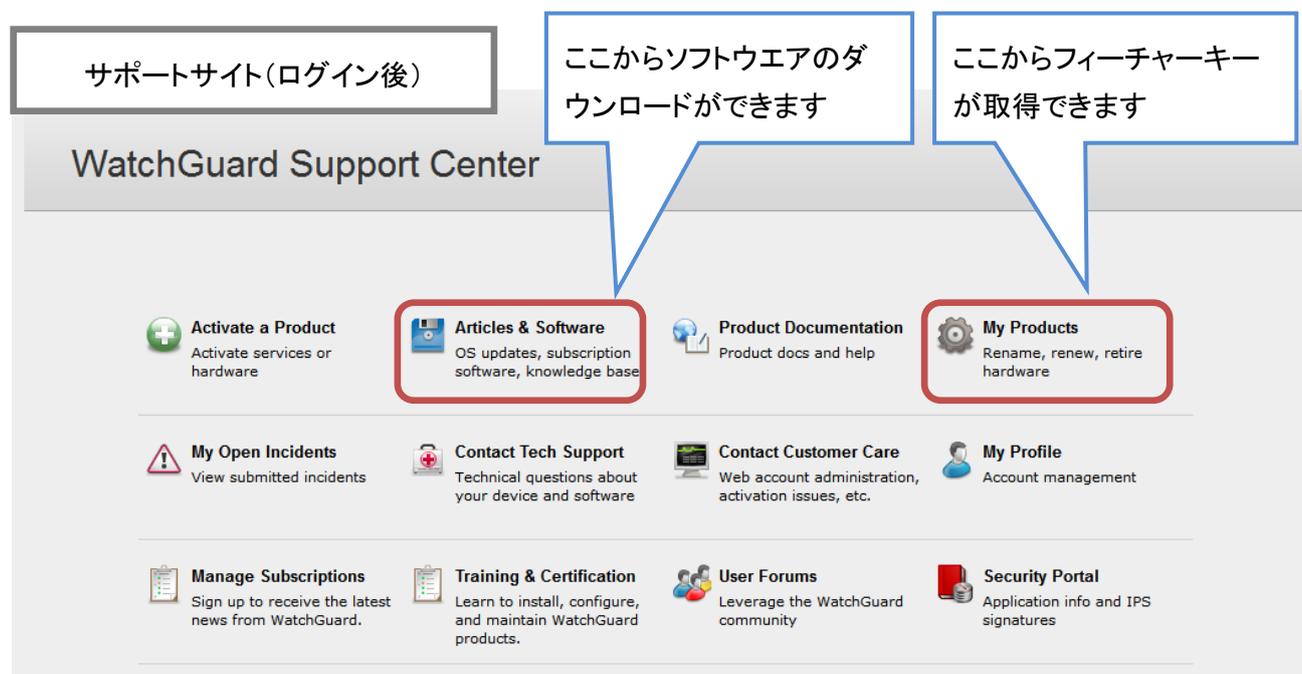
事前準備としてセットアップに必要なソフトウェアをインストールします。製品アクティベート後、WatchGuard Support (US)サイト内の『Articles & Software』より必要なソフトウェアを取得します(ログインが必要)。

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

必要なソフトウェアは、以下の 2 つです。

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

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



ソフトウェアがダウンロードできたら、まず WatchGuard System Manager のインストールを行います。前述のとおり、WebUI には WSM と比較して若干の制限事項がありますので、すぐに使わないとしても、管理者の方にはあらかじめインストールしておくことをおすすめします。

インストーラーはすべてデフォルトで進めます。途中、インストールするソフトウェアを選択する画面が表示されますが、追加せずそのまま進めます。

次に Fireware XTM OS をインストールします。こちらのインストールウィザードもすべてデフォルトで進めてください。以上でソフトウェア側の準備は完了です。

ファクトリーリセット

ファクトリーリセットとは XTM を、工場出荷時の既定の設定に戻す手段です。リセットして起動すると XTM は「セーフモード」というモードで動作します¹。

手順については機種によって 2 通りあります。

XTM2/3 シリーズ(330 除く)

1. XTM と接続

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



1 番ポート: Trusted

2. 電源の投入

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



リセットボタンを押しながら

AC アダプタを挿します

¹ SYS-B Mode とも言います。ちなみに正常起動の場合は SYS-A Mode になります

3. 起動の確認

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



起動途中に点滅したりしますが、Reset ボタンはずっと押し続けます。

点灯状態になったら、それがセーフモード起動を意味します。

XTM330/5/8/10/20 シリーズ

1. XTM と接続

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



2. 電源の投入

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



▼のボタンを押しながら

電源を投入



3. 起動の確認

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

- ① Safe Mode で起動する旨の表示



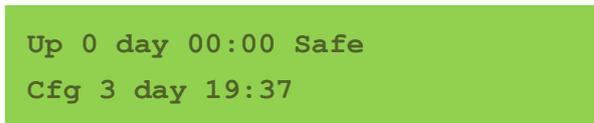
Safe Mode
Starting...

- ② しばらくすると社名の表示



WatchGuard
Technologies

- ③ 最後に Uptime の表示



Up 0 day 00:00 Safe
Cfg 3 day 19:37

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

ファクトリーリセット後の設定

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

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

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

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

Web Setup Wizard

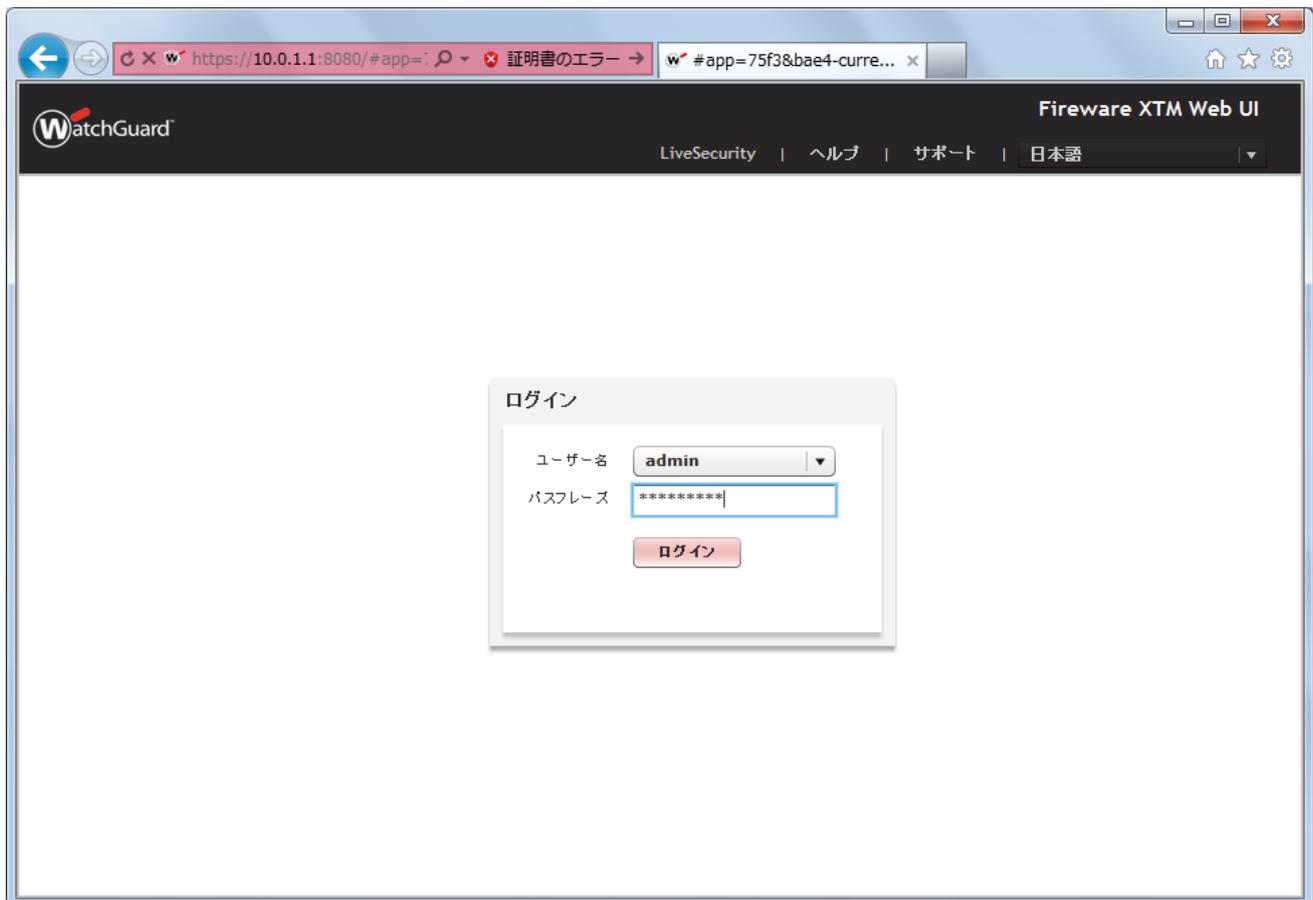
機器を Safe Mode で起動したら、Web Setup Wizard で初期設定を行ないます。

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



証明書のセキュリティ警告が出てもそのまま続行します。

するとログイン画面が表示されますのでパスワードに「readwrite」を入力します。



Wizard が始まりますので「次へ」ボタンをクリックします。



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



使用許諾契約の条項に同意していただき次へ。



外部インターフェースはまだ構成がはっきり決まっていない場合はそのまま次へ。

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

Fireboxの外部インターフェイスの構成

IP アドレスを設定するときインターネット サービス プロバイダが使用している方法を選択してください。

DHCP
 PPPoE
 静的

外部インターフェイスは、インターネットまたはワイド エリア ネットワーク (WAN) に接続するインターフェイスです。外部インターフェイスが正しく動作するには、IPアドレスが割り当てられている必要があります。インターネット サービス プロバイダは、次の方法のうち 1 つを使って IP アドレスを設定します。

[DHCP]
ISP が、DHCP(動的ホスト設定プロトコル)を使用して IP アドレスを割り当てている場合は、このオプションを選択します。DHCPは、ネットワーク上のコンピュータが、IPアドレスやその他の情報(既定のゲートウェイなど)を取得するために使用する、インターネット プロトコルです。利用者がインターネットに接続すると、ISP側で DHCPサーバーとして構成されたコンピュータによって、自動的に IPアドレスが割り当てられます。そのアドレスは以前に割り当てられたものと同じ場合もあれば、新しいアドレスの場合もあります。

次へ。

DHCP用外部インターフェイスの構成

手動でIPアドレスを割り当て、そのアドレスをFireboxを設定するためのだけに DHCPを使用する場合には、**[次のIPアドレスを使用]** ラジオ ボタンをクリックして、隣のフィールドにIPアドレスを入力します。クライアント フィールドおよびホスト名フィールドの入力は任意です。

IP アドレスの自動取得
 IPアドレスを使用
 リース時間
クライアント
ホスト名

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

DNSサーバーおよびWINSサーバーの構成

Fireboxのいくつかの機能では、Windows Internet Name Service (WINS)および Domain Name System (DNS) サーバーのIPアドレスを共有します。これらのサーバーへのアクセスは、Fireboxの信頼済みインターフェイスから行える必要があり、次の目的で使用されます：

- * Fireboxは、spamBlocker、Gateway AV、およびIPS機能を正しく動作させるためにIPSec VPNIに対してIPアドレスへの名前解決を提供しますが、ここに示すDNSサーバーを使用します。
- * WINSおよびDNSエントリは、信頼済みネットワークまたはオプション ネットワーク上のDHCPクライアントによって使用されます。また、Mobile VPNユーザーがDNSクエリを解決するためにも使用されます。

Domain Name	<input type="text"/>	
DNSサーバー	<input type="text" value="8.8.8.8"/>	<input type="text" value="8.8.4.4"/>
WINSサーバー	<input type="text"/>	<input type="text"/>

信頼済みインターフェイス(現在接続しているポート)の設定です。次へ。

信頼済みインターフェイスの構成

信頼済みインターフェイスで使用できるように、内部プライベート ネットワークから利用可能なIPアドレスを入力します。このIPアドレスが信頼するインターフェイスのアドレスになります。

IPアドレス /

このインターフェイス上でのDHCPサーバーの有効化

開始IP

終了IP

信頼済みインターフェイスのIPアドレスを変更した場合は、ブラウザのアドレスバーの新しいIPアドレスを使用して、Fireware XTM Web UIに接続する必要があります。例えば、信頼済みインターフェイスのIPアドレスを172.16.0.1に変更した場合は、接続には、https://172.16.0.1:8080を使用する必要があります。コンピュータが新しい信頼済みネットワークのIPサブネットの範囲内に存在するように、コンピュータのIPアドレスも変更する必要があります。

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

デバイス用のパスワードを作成します。

ご使用のデバイスには、次の2つの組み込みユーザー アカウントがあります：

- *admin には読み書き権限があります。
- *status には読み取り専用権限があります。

各アカウントと一緒に使用するパスワードを入力します。
パスワードの文字数は 8 文字以上 32 文字以下です。

ユーザー名 status (読み取り専用)
パスワード *****
パスワードの確認 *****

ユーザー名 admin (読み書き)
パスワード *****
パスワードの確認 *****

< 戻る(B) 次へ >

リモート管理の有効化はしないで次へ。(ポリシーの画面で変更できます)

リモート管理を有効にします。

このデバイスのリモート コンピュータからの管理を許可する

リモート ホストIPアドレス

Web Setup Wizardを使用してFireboxを構成する場合には、WatchGuard という名前のポリシーが自動的に作成されます。このポリシーによって、信頼済みネットワークまたは任意ネットワーク上の任意のコンピュータからFireboxに接続して管理することが許可されます。リモート ロケーション(Firebox 外部の任意の場所) から Fireboxを管理する場合は、ここでリモートIPアドレスを追加して、このポリシーを変更できます。

< 戻る(B) 次へ >

デバイス名を入力し次へ。

デバイスの連絡先情報の追加

デバイスの連絡先情報は、複数のデバイスを管理する場合にこのデバイスを特定するのに役に立ちます。

デバイス名

デバイスの場所

連絡先

< 戻る(B) 次へ >

タイムゾーンは「(GMT+09:00)大阪、札幌、東京」を選択して次へ。

タイムゾーンを設定します。

Fireboxで使用するタイムゾーンを選択してください。この設定によって、ログファイルおよびツール (LogViewer、WatchGuard Reports、WebBlocker など) に表示される日付と時刻が制御されます。

タイムゾーン

最後に設定のサマリーが表示されます。次へ。

概要

以下の構成の確認

アクティベーション: 成功

外部インターフェイス: IP アドレスの自動取得
-DHCPを使用しています

信頼済みインターフェイス: 10.0.1.1/24
-DHCPを使用していません

タイムゾーン: (GMT+09:00) 大阪、札幌、東京

これらの設定を適用するには、[次へ] をクリックします。

設定が反映されます。

XTM へようこそ > 構成 > アクティベーション > 完了

セットアップが進行中です.....

セットアップ完了が表示されます。完了ボタンをクリックします。



初期セットアップは以上で完了です。

機能キーの追加

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

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

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

左側メニュー **システム** - **機能キー** からアクセスします。

機能キーの画面が表示されたら、アップデート ボタンをクリックします。

ダッシュボード
システム ステータス
ネットワーク
ファイアウォール
セキュリティサービス
認証
VPN
システム
システム
機能キー
NTP
SNMP
管理対象のデバイス
ログ記録
診断ログ
グローバル設定
証明書
アップグレード OS
バックアップ イメージ
イメージの復元
USBドライブ
パスフレーズ
コンフィグレーションファイル

機能キー

ヘルプ ⓘ

概要

モデル XTM530 **アップデート**

シリアル番号 **削除**

ソフトウェア エディション

有効期限

署名

機能

機能	値	有効期限	残り時間
モデル アップグレード	無効	なし	
認証ドメインの総数	15	なし	
認証されたユーザーの総数	2500	なし	
Branch Office VPNトンネル	600	なし	
最大ファイアウォール ポリシー	有効	なし	
フィルタ ポリシーの最大スループット	2300	なし	
アウトバウンドアクセスが許可されたIPアドレス	有効	なし	
Mobile VPNユーザー	400	なし	
最大QoSアクション	100	なし	
最大同時セッション	700000	なし	

この機能キーが期限切れになった場合、一部の機能および容量が既定値に戻る可能性があります。

機能キーの取得

LiveSecurityから機能キーをダウンロードするには、次をクリックしてください **機能キーを取得**

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

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

Firebox機能キーの追加
機能キーの内容を、下の領域に貼り付けてください。

```

Serial Number:
License ID: 80
Name: 10-02-2012_21:17
Model: XTM530
Version: 1
Feature: APP_CONTROL@Apr-05-2013
Feature: AUTH_DOMAIN#15
Feature: AUTHENTICATED_USER#2500
Feature: AV@Apr-05-2013
Feature: AV_TRIAL@May-20-2010
Feature: BOVPN_TUNNEL#600
Feature: FIREWARE_XTM
Feature: FW_SPEED#0
Feature: IPS@Apr-05-2013
Feature: IPS_TRIAL@May-20-2010
Feature: LIVESECURITY@May-19-2013
Feature: MUVPN_USER#400
Feature: RED@Apr-05-2013
Feature: SESSION#700000
Feature: SPAMBLOCKER@Apr-05-
    
```

保存 リセット キャンセル

貼り付けたら保存ボタンをクリックします

正規のライセンスを追加できると、以下のような画面になります。

機能キー

概要

モデル XTM530

シリアル番号

ソフトウェア エディション Fireware XTM Pro

番名 302d0215029f326a-9ebb668f1fdb3fd4-bbe7cf3d713c9217-1d02147ccd6b9ebb-ddb73973e2329279-09432

機能

機能	値	有効期限	残り時間
モデル アップグレード	無効	なし	
Application Control	有効	2013-04-05	有効期間 184 日
認証ドメインの総数	15	なし	
認証されたユーザーの総数	2500	なし	
Gateway AntiVirus (AV)	有効	2013-04-05	有効期間 184 日
Branch Office VPNトンネル	600	なし	
Fireware XTM	有効	なし	
フィルタ ポリシーの最大スループット	有効	なし	
Intrusion Prevention (IPS)	有効	2013-04-05	有効期間 184 日
LiveSecurity Service	有効	2013-05-19	有効期間 228 日
Mobile VPNユーザー	400	なし	
Reputation Enabled Defense	有効	2013-04-05	有効期間 184 日

機能キーの取得
LiveSecurityから機能キーをダウンロードするには、次をクリックしてください

機能が有効になり、有効期限と残りの日数が表示されます。

第三章 ネットワークの設定

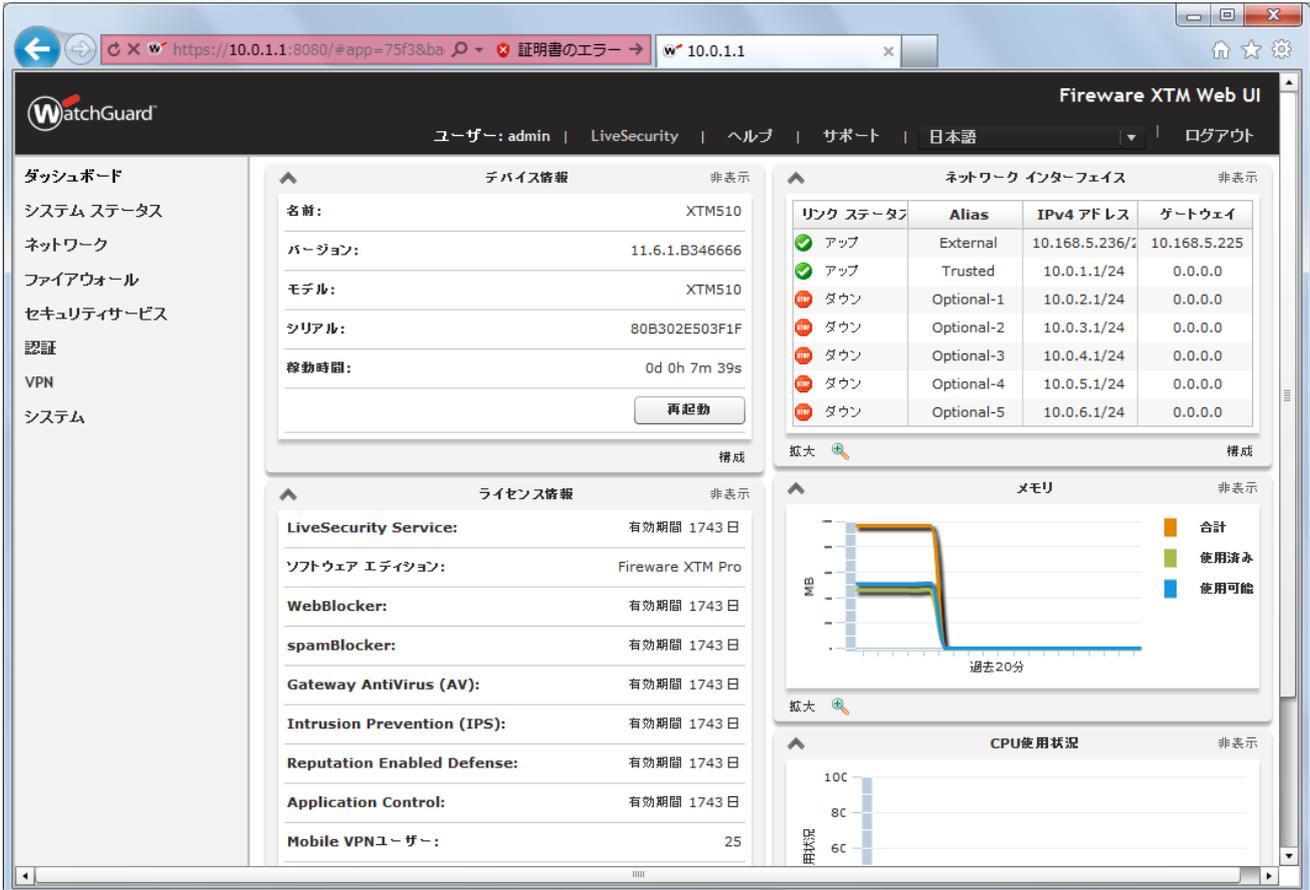
それでは前章で初期設定を施した XTM に、WebUI で接続してみましょう。

ブラウザで <https://10.0.1.1:8080> に再び接続します。

パスワードは、Wizard で設定した構成パスワードを入力し、ログインボタンをクリックします。



ログインすると最初に XTM の状態を表わすダッシュボードが表示されます。



The dashboard displays the following information:

- Device Information:** Name: XTM510, Version: 11.6.1.B346666, Model: XTM510, Serial: 80B302E503F1F, Uptime: 0d 0h 7m 39s. Includes a '再起動' (Restart) button.
- Network Interfaces:** A table showing the status of various interfaces.
- Licensing Information:** LiveSecurity Service (1743 days), Software Edition (Fireware XTM Pro), WebBlocker (1743 days), spamBlocker (1743 days), Gateway AntiVirus (AV) (1743 days), Intrusion Prevention (IPS) (1743 days), Reputation Enabled Defense (1743 days), Application Control (1743 days), and Mobile VPN Users (25).
- Memory Usage:** A line graph showing memory usage over the last 20 minutes, with categories for total, used, and available memory.
- CPU Usage:** A bar chart showing CPU usage across different components.

リンク	ステータス	Alias	IPv4 アドレス	ゲートウェイ
アップ	アップ	External	10.168.5.236/24	10.168.5.225
アップ	アップ	Trusted	10.0.1.1/24	0.0.0.0
ダウン	ダウン	Optional-1	10.0.2.1/24	0.0.0.0
ダウン	ダウン	Optional-2	10.0.3.1/24	0.0.0.0
ダウン	ダウン	Optional-3	10.0.4.1/24	0.0.0.0
ダウン	ダウン	Optional-4	10.0.5.1/24	0.0.0.0
ダウン	ダウン	Optional-5	10.0.6.1/24	0.0.0.0

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

ネットワーク インターフェース

次のモードでインターフェースを構成: ミックス ルーティング モード

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

ヘルプ

作成

DNSサーバー

Domain Name

8.8.8.8

8.8.4.4

DNSサーバー

(IPv4 または IPv6 アドレス)

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

外部ネットワークの設定

まずは外部インターフェースから設定しましょう。

該当のインターフェースを選択して、右の構成ボタンをクリックします。

ネットワーク インターフェイス

次のモ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

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

DNSサーバー

Domain Name

8.8.8.8
8.8.4.4

削除

DNSサーバー

追加

(IPv4 または IPv6 アドレス)

次頁のように、インターフェースの詳細を設定できる画面が開きます。

選択したインターフェースの詳細設定画面になります。

最初にインターフェース名を設定することができます。

インターフェース構成 - 外部

ヘルプ

IPv4 IPv6 セカンダリ 詳細

インターフェース名 (Alias) External

インターフェースの説明

インターフェースの種類 外部

構成モード DHCP

クライアント

ホスト名

この IP アドレスを使用する

リース時間 8 時間

保存 キャンセル

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

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

IPv4 IPv6 セカンダリ 詳細

インターフェース名 (Alias) External-1

インターフェースの説明

インターフェースの種類 外部

固定 IP の設定

構成モードで静的 IP を選択し、IP アドレス、サブネットマスクのビット数、デフォルトゲートウェイを入力します。

The screenshot shows the 'External Interface Configuration' window. The 'IPv4' tab is selected. The 'Interface Name (Alias)' is 'External'. The 'Interface Type' is 'External'. The 'Configuration Mode' is set to 'Static IP'. The 'IP Address' is '10.0.0.1' with a subnet mask of '24'. The 'Gateway' is '10.0.0.254'. The 'Save' and 'Cancel' buttons are at the bottom right.

DHCP の設定

構成モードで DHCP を選択するだけです。

The screenshot shows the 'External Interface Configuration' window. The 'IPv4' tab is selected. The 'Interface Name (Alias)' is 'External'. The 'Interface Type' is 'External'. The 'Configuration Mode' is set to 'DHCP'. The 'Client' field is empty. The 'Host Name' field is empty. The 'Use this IP address' field is empty. The 'Lease Time' is set to '8' hours. The 'Save' and 'Cancel' buttons are at the bottom right.

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

PPPoE の設定

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

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

インターフェイス構成 - 外部

IPv4 IPv6 セカンダリ 詳細

ヘルプ

インターフェイス名 (Alias) 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

構成モード PPPoE

PPPoE設定

IP アドレスの自動取得

この IP アドレスを使用する

ユーザー名 username@ispname

パスワード *****

パスワード確認 *****

保存 キャンセル

詳細 PPPoE 設定

ISP の指定によってはより詳細な設定が必要になることがあります。

「詳細 PPPoE 設定」ボタンをクリックし、指定の項目を設定してください。

構成モード PPPoE

詳細 PPPoE 設定 <- PPPoE のメイン設定に戻る

接続設定

PPPoE 抽出 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 秒

ダイアルオンデマンド

アイドル タイムアウトまでの時間 20 分

LCPI コー 要求を使用して、失われた PPPoE 接続を検出

LCPI コーを再試行する回数 6 試行数

LCPI コー タイムアウトまでの時間 10 秒

自動再起動が設定された時間 日曜日 : 0 : 0 (HH:MM)

認証設定

サービス名

アクセス コンセントレータの名前

認証の再試行 3

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 クライアントの静的 IP アドレスを送信する

PPPoE サーバーと DNS をネゴシエートする

DNS/WINS 設定

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

- ゲートウェイアンチウィルスや IPS のシグネチャ更新時の名前解決
- スпамブロッカーサーバーへの問い合わせの際の名前解決
- 内部 DHCP クライアントへの DNS サーバーアドレスの配布
- NTP サーバを FQDN で設定した際の名前解決
- 拠点間 VPN でドメイン名を使用した場合の名前解決

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

DNS の設定

左側メニューの「ネットワーク」→「インターフェイス」をクリックし、ネットワークインターフェイス画面のインターフェイス一覧を表示します。

一覧の下にある DNS サーバーの欄に入力し、追加ボタンをクリックして追加します。

The screenshot shows the 'ネットワーク インターフェイス' (Network Interfaces) configuration page. On the left, the 'ネットワーク' (Network) menu is expanded to 'インターフェイス' (Interfaces). The main content area shows a table of interfaces and a 'DNSサーバー' (DNS Servers) section.

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

DNSサーバー

Domain Name:

8.8.8.8

DNSサーバー:
(IPv4 または IPv6 アドレス)

スクロールして画面右下にある「保存」ボタンをクリックして設定を保存します。

WINS の設定

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

DNSサーバー

Domain Name

8.8.8.8

DNSサーバー
(IPv4 または IPv6 アドレス)

WINSサーバー

WINSサーバー
(IPv4 アドレス)

画面右下の「保存」ボタンをクリックし、設定を保存します。

内部ネットワークの設定

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

設定は外部インターフェース同様、左側メニューの「ネットワーク」→「インターフェース」の画面から行ないます。

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

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

Trusted インターフェースの設定

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

ここでは Trusted-1 というインターフェース名を付けています。

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

インターフェース構成 - 信頼済み/任意

ヘルプ

IPv4 IPv6 セカンダリ MACアクセス制御 詳細

インターフェース名 (Alias) Trusted-1

インターフェースの説明

インターフェースの種類 信頼済み

IPアドレス 10.0.1.1 / 24

DHCPを無効にする

保存 キャンセル

DHCP サーバーの使用

内部ネットワーク下のクライアント PC に IP アドレスを配布したい場合、インターフェースの設定画面の下方にあるドロップダウンリストから、「DHCP サーバーの使用」を選択します。

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

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

DHCPサーバーの使用 ▼

設定 | DNS/WINS

リース時間 8 時間 ▼

アドレスプール

開始IP	終了IP	削除
10.0.1.100	10.0.1.254	

予約アドレス

予約IP	予約名	MACアドレス	削除
------	-----	---------	----

予約名 追加

予約IP

MACアドレス



追加すると一覧に表示されます

アドレスプール

開始IP	終了IP	削除
10.0.1.100	10.0.1.254	

開始IP 追加

終了IP

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

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

The screenshot shows the DHCP server configuration interface. At the top, there are fields for 'インターフェイス名 (Alias)' (Trusted), 'インターフェイスの説明', and 'インターフェイスの種類' (信頼済み). Below that is the 'IPアドレス' field (10.0.1.1 / 24). A dropdown menu 'DHCPサーバーの使用' is open, and the 'DNS/WINS' option is highlighted with a red box. Underneath, there is a 'リース時間' (8) and a '時間' dropdown. A table titled 'アドレスプール' shows a range from '開始IP' 10.0.1.100 to '終了IP' 10.0.1.254. Below the table are input fields for '開始IP' and '終了IP' with an '追加' button.

クライアントに設定したい DNS サーバーの情報を入力し、追加します。

This screenshot shows the 'DNS/WINS' configuration page. It has a 'DNSサーバー (定義されていない場合は、ネットワークDNSサーバーを使用します)' section with a 'Domain Name' field and a list of servers. One server, '8.8.8.8', is already listed with a '削除' button. A new 'DNSサーバー' '8.8.4.4' is being entered into the input field, and the '追加' button is highlighted with a red box. Below is a 'WINSサーバー (定義されていない場合は、ネットワークWINSサーバーを使用します)' section with an empty list and a '削除' button. At the bottom, there is a 'WINSサーバー' input field and an '追加' button.

WINS サーバーがあれば同じ要領で追加できます。

以上で DHCP サーバーが構成できました。

ブリッジの構成

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

例として 2-5 番のインターフェースをブリッジとして構成しましょう。

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

ネットワーク インターフェイス

ヘルプ

次のモ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

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

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

インターフェイス構成 - ブリッジ

ヘルプ

ブリッジ 設定

インターフェイス名 (Alias) 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**

保存 キャンセル

無効だったインターフェースが、次のようにブリッジに変更されました。

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

残りのインターフェースも同じように設定してゆきます。

以上でどのインターフェースをブリッジにするか指定できました。

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

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

新規作成ボタンをクリックし、ブリッジを追加しましょう。

The screenshot shows the 'ブリッジ' (Bridge) configuration page. On the left sidebar, 'ネットワーク' (Network) and 'インターフェイス' (Interface) are highlighted. The main content area is titled 'ブリッジ' and includes a 'ヘルプ' (Help) link. Under '使用可能なブリッジ インターフェイス' (Available Bridge Interfaces), there is a list of interfaces: '名前 (Alias)' with values 'Trusted-2', 'Trusted-3', 'Trusted-4', and 'Trusted-5', and a '構成' (Configure) button. Below this is the 'ブリッジ設定' (Bridge Settings) section, which contains a table with columns: '名前' (Name), 'ゾーン' (Zone), 'IPアドレス' (IP Address), and 'インターフェイス' (Interface). To the right of the table is a '新規作成' (New Creation) button, which is highlighted with a red box. Below the table are '構成' (Configure) and '削除' (Delete) buttons.

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

The screenshot shows the 'ブリッジ' (Bridge) configuration window. It has tabs for 'ブリッジ設定', 'DHCP', and 'セカンダリ'. Under 'ブリッジ設定', there are fields for '名前' (Name) set to 'Trusted-Bridge', '説明' (Description), 'セキュリティゾーン' (Security Zone) set to '信頼済み' (Trusted), and 'IPアドレス' (IP Address) set to '10.0.11.1 / 24'. Below these is a table titled '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' (Selected Bridge Interfaces for Traffic Forwarding). The table has columns for 'ブリッジ' (Bridge), 'インターフェイス名' (Interface Name), and 'インターフェイス番号' (Interface Number). The rows are: 'Trusted-2' (2), 'Trusted-3' (3), 'Trusted-4' (4), and 'Trusted-5' (5). The 'Trusted-5' row is highlighted. At the bottom are '保存' (Save) and 'キャンセル' (Cancel) buttons. Three blue callout boxes point to the '名前' field, the 'IPアドレス' field, and the 'Trusted-5' row.

ブリッジ	インターフェイス名	インターフェイス番号
<input checked="" type="checkbox"/>	Trusted-2	2
<input checked="" type="checkbox"/>	Trusted-3	3
<input checked="" type="checkbox"/>	Trusted-4	4
<input checked="" type="checkbox"/>	Trusted-5	5

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

以上で保存してください。

以上の設定を施すと、Trusted(信頼済み)は 1 番ポートの「Trusted-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が、しかし、XTM には Any-Trusted というビルトインのエイリアスが存在します。

これまでの設定でできた 2 つの Trusted ネットワークはこの Any-Trusted で表わされます。これを用いて設定をすれば、複数のエイリアスにも一括してポリシーを適用できるというわけです。

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

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

DHCP タブに移り、DHCP モードで「DHCP サーバー」を選択します。
IP アドレスプールを指定します。

The screenshot shows a configuration window with three tabs: 'ブリッジ設定', 'DHCP', and 'セカンダリ'. The 'DHCP' tab is active. Under 'DHCP設定', the 'DHCPモード' dropdown is set to 'DHCPサーバー'. Below it are fields for 'Domain Name' and 'リース時間' (set to '8時間'). Under 'アドレスプール', a table lists an IP pool with '開始IP' 10.0.11.100 and '終了IP' 10.0.11.254. A '削除' button is next to the table. Below the table are input fields for '開始IP' and '終了IP' with an '追加' button.

画面の下方にスクロールすると、DNS サーバーを指定することができます。

The screenshot shows a configuration window for DNS and WINS servers. Under 'DNSサーバー', there is a text input field containing '8.8.8.8' and a '削除' button. Below it is another 'DNSサーバー' input field containing '8.8.4.4' and an '追加' button. Under 'WINSサーバー', there is a large empty text area and a '削除' button. Below that is a 'WINSサーバー' input field and an '追加' button. At the bottom of the window are '保存' and 'キャンセル' buttons.

最後に保存ボタンをクリックし、設定を反映させます。

DMZ を設定する

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

インターフェースの設定画面の「インターフェースの種類」を「Optional」(任意)を選択します。こうすることによって、Trusted とは違う、文字通り任意のネットワーク設定やポリシーを適用することができます。

インターフェース構成 - 信頼済み/任意

ヘルプ

IPv4 IPv6 セカンダリ MACアクセス制御 詳細

インターフェース名 (Alias) DMZ

インターフェースの説明

インターフェースの種類 任意

IPアドレス 10.100.10.1 / 24

DHCPを無効にする

保存 キャンセル

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

NAT 設定 (1-to-1NAT)

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

左側メニュー **ネットワーク** → **NAT** をクリックすると、NAT の構成画面になります。

下方の 1-to-1 NAT の追加ボタンをクリックします。

ダッシュボード
システム ステータス
ネットワーク
インターフェイス
VLAN
ブリッジ
複数 WAN
動的 DNS
NAT
ルート
Dynamic Routing
ファイアウォール
セキュリティサービス
認証
VPN
システム

NAT

ヘルプ

動的NAT

動的NATは、パケットの送信 インターフェイスのIPアドレスを使用するために、パケットのソースIPを書き換えます。

発信元	送信先
192.168.0.0/16	Any-External
172.16.0.0/12	Any-External
10.0.0.0/8	Any-External

追加
削除
上へ
下へ

1-to-1 NAT

1-to-1 NAT は、ある範囲のIPアドレスに送信されたパケットを別の範囲のアドレスに書き換えてリダイレクトします。

インターフェイス	ホストの数	NATベース	実ベース

追加
削除

保存 リセット

NAT の追加画面になりますので、マップの種類は「単一 IP」、インターフェイスは External を指定します。
NAT ベースには外部インターフェイスの IP アドレス、Real ベースにはサーバーのローカル IP アドレスを指定します。

NAT

ヘルプ ?

1-to-1 NAT 構成

種類

マップの種類 **単一 IP**

構成

インターフェイス **External**

NATベース **10.0.0.1** → 外部インターフェイスの IP アドレス

実ベース **10.100.10.101** → サーバーのローカル IP アドレス

保存 キャンセル

保存をクリックすると 1-to-1 NAT の一覧に追加されます。

1-to-1 NAT

1-to-1 NAT は、ある範囲の IP アドレスに送信されたパケットを別の範囲のアドレスに書き換えてリダイレクトします。

インターフェイス	ホストの数	NATベース	実ベース	
External	1	10.0.0.1	10.100.10.101	追加
				削除

保存 リセット

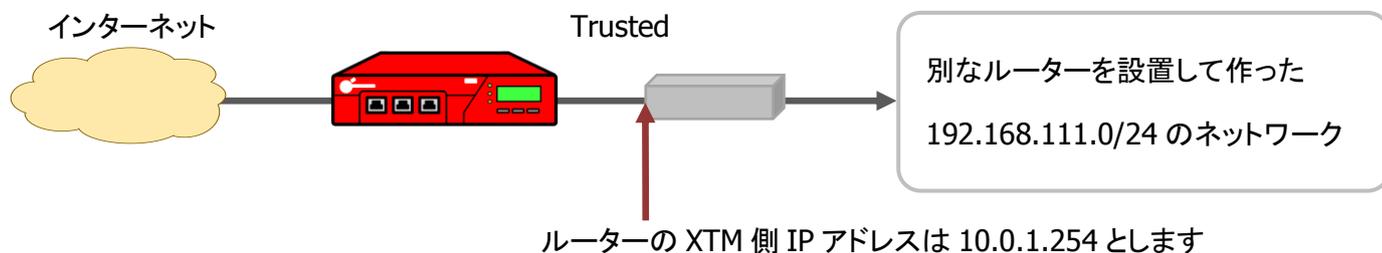
他にもポートフォワーディングも可能な SNAT (Static Nat) の設定もあります。こちらはポリシーの追加時に設定しますので、ファイアウォールの章で取り上げます。

ルーティング設定

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

その場合、明示的にルートを設定する必要があります。

例:



左側メニュー **ネットワーク** → **ルート** をクリックします。

ルートの設定画面が開くので、追加ボタンをクリックします。

ダッシュボード

システム ステータス

ネットワーク

インターフェイス

VLAN

ブリッジ

複数 WAN

動的 DNS

NAT

ルート

Dynamic Routing

ファイアウォール

セキュリティサービス

認証

VPN

システム

ヘルプ

ルーティング	ゲートウェイ	メトリック	インターフェイス

追加

編集

削除

保存

リセット

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。

ルートの追加

種類を選択: ネットワーク IPv4

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

インターフェースの指定

OK キャンセル

OK ボタンをクリックすると一覧に追加されますので、保存します。

ルートの一覧

ルーティング	ゲートウェイ	メトリック	インターフェース
192.168.111.0/24	10.0.1.254	1	

追加 編集 削除

保存 リセット

第四章 ファイアウォールの設定

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

ファイアウォールとしての観点から、ポリシー設定画面をあらためて解説します。

ポリシー設定画面

画面構成

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

ダッシュボード
システム ステータス
ネットワーク
ファイアウォール
ファイアウォール ポリシー
Mobile VPNポリシー
エイリアス
Proxy アクション
トラフィック管理
スケジュール
SNAT
既定のパケット処理
ブロックされたサイト
ブロックされたポート
セキュリティサービス
認証
VPN
システム

ファイアウォール ポリシー

Auto-Orderモードは有効です。 ヘルプ

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PBR	Applicati
✓	FTP	FTP	Any-Trust	Any-Exter	tcp:21		なし
✓	WatchGuard Web UI	WG-Fireware-XTI	Any-Trust	Firebox	tcp:8080		なし
✓	Ping	Ping	Any-Trust	Any	ICMP (typ		なし
✓	WatchGuard	WG-Firebox-Mgr	Any-Trust	Firebox	tcp:4105		なし
✓	Outgoing	TCP-UDP	Any-Trust	Any-Exter	tcp:0 udp		なし

[Show policy checker](#)

表示順序はポリシーの評価順序です。上から順に評価され、マッチしたルールが適用されます

ポリシー一覧の各カラムの意味を以下に説明しておきます。

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

ポリシーの変更 / 追加 / 保存

既存のポリシーを変更する際には、該当のポリシーを選択し、ポリシーの編集ボタン  をクリックします。

ポリシーの新規追加は  ボタンをクリックします。

削除は該当のポリシーを選択して  ボタンをクリックします。

ポリシーの編集

ポリシーの追加

ポリシーの削除

Auto-Orderモードは有効です。

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PBR	Applicati
✓	 FTP	FTP	Any-Trust	Any-Exter	tcp:21		なし
✓	 WatchGuard Web UI	WG-Fireware-XTI	Any-Trust	Firebox	tcp:8080		なし
✓	 Ping	Ping	Any-Trust	Any	ICMP (typ		なし
✓	 WatchGuard	WG-Firebox-Mgr	Any-Trust	Firebox	tcp:4105		なし
✓	 Outgoing	TCP-UDP	Any-Trust	Any-Exter	tcp:0 udp		なし

ポリシーの追加

それでは実際にポリシーを追加してみましょう。

ポリシー追加（内側から外側へ）

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

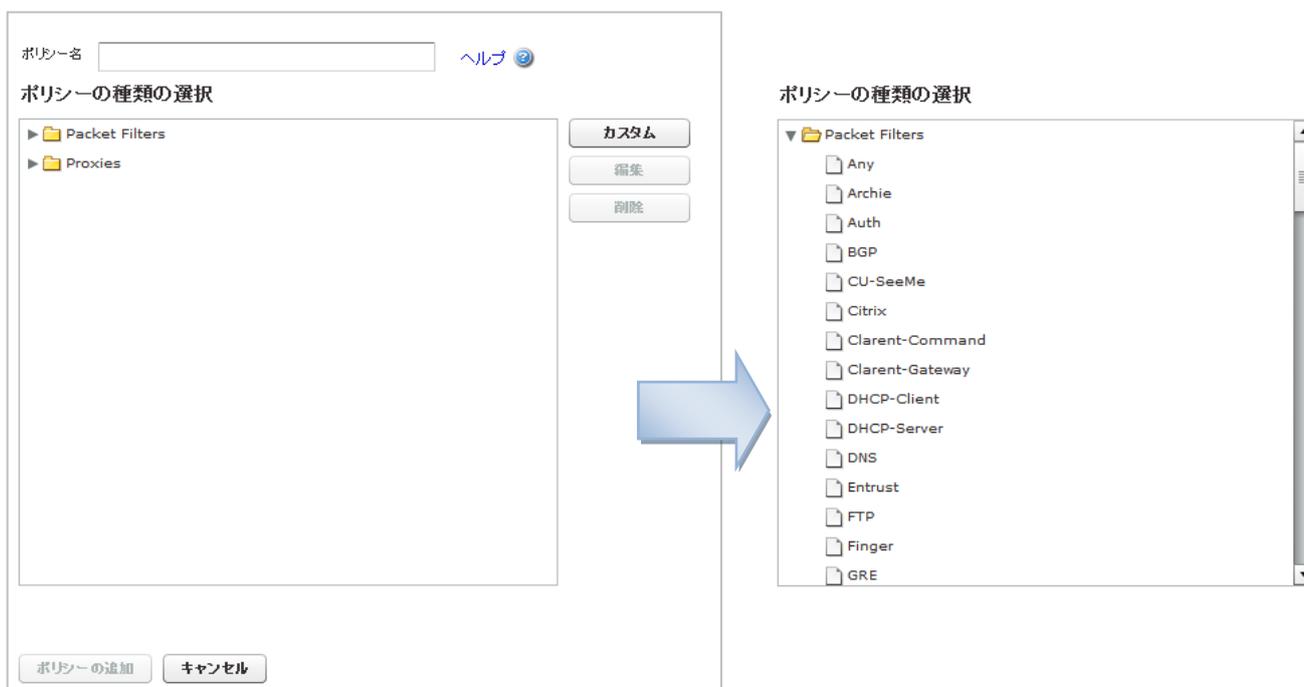
※ 実際は「Outgoing」ポリシーがあるため、HTTP の許可ポリシーがなくても Web の閲覧はできます

Auto-Orderモードは有効です。   ヘルプ 

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PBR	Applicati
✓	 FTP	FTP	Any-Trust	Any-Exter	tcp:21		なし
✓	 WatchGuard Web UI	WG-Fireware-XTI	Any-Trust	Firebox	tcp:8080		なし
✓	 Ping	Ping	Any-Trust	Any	ICMP (typ		なし
✓	 WatchGuard	WG-Firebox-Mgr	Any-Trust	Firebox	tcp:4105		なし
✓	 Outgoing	TCP-UDP	Any-Trust	Any-Exter	tcp:0 udp		なし

追加ボタンをクリックすると、ポリシーの種類の選択画面になります。

Packet Filters のツリーを展開すると、代表的なプロトコルのポリシーテンプレートがあります。



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

ポリシー名 ヘルプ

ポリシーの種類の選択

- Entrust
- FTP
- Finger
- GRE
- Gopher
- HBCI
- HTTP**
- HTTPS
- IDENT
- IGMP
- IMAP
- IPSec
- IRC
- Intel-Video-Phone
- Kerberos-V4
- Kerberos-V5

カスタム
編集
削除

WebUI ではポリシー名は後から変更できませんのでご注意ください。

(もちろん WSM からなら変更できます)

下方の追加ボタンをクリックします。

HTTP
HTTPS
IDENT
IGMP
IMAP
IPSec
IRC
Intel-Video-Phone
Kerberos-V4
Kerberos-V5

ポート	プロトコル
80	TCP

HTTPパケット フィルタを使用しても、トラフィックにHTTP proxy ルール セットは適用されません。HTTPトラフィックにプロキシを適用するには、HTTP Proxy ポリシーを使用します。WatchGuardは、受信HTTPをFirebox の内側に保持するパブリックHTTP サーバーに対してのみ許可することをお勧めします。外部ホストはスプーフィングの可能性があり、正しい場所から実際に送信されたパケットかどうかを WatchGuardで確

ポリシーの追加 キャンセル

すると、新規作成ポリシーのプロパティが開きます(次頁)。

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

名前 → **ポリシー名**

ポリシー

接続は → **許可？拒否？** ヘルプ

発信元

→ **すべての信頼済みのネットワークから**

送信先

→ **すべての外部ネットワークへ**

Application Control を有効にします

ポリシー一覧に戻り、新しいポリシーが追加されています。

ファイアウォール ポリシー

Auto-Orderモードは有効です。 ヘルプ

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PBR	Application Control
✓	FTP	FTP	Any-Trusted	Any-External	tcp:21		なし
✓	HTTP-Outgoing	HTTP	Any-Trusted	Any-External	tcp:80		なし
✓	WatchGuard Web UI	WG-Fireware-XTM	Any-Trusted	Firebox	tcp:8080		なし
✓	Ping	Ping	Any-Trusted	Any	ICMP (type		なし
✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted	Firebox	tcp:4105 tc		なし
✓	Outgoing	TCP-UDP	Any-Trusted	Any-External	tcp:0 udp:(なし

[Show policy checker](#)

ポリシー追加（外側から内側へ）

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

Web サーバーは 10.100.10.110 とします。

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

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

送信元は Any-External、送信先は Web サーバーなので、

名前 有効

ポリシー **プロパティ** 詳細

接続は ヘルプ

送信元

→ 外部から

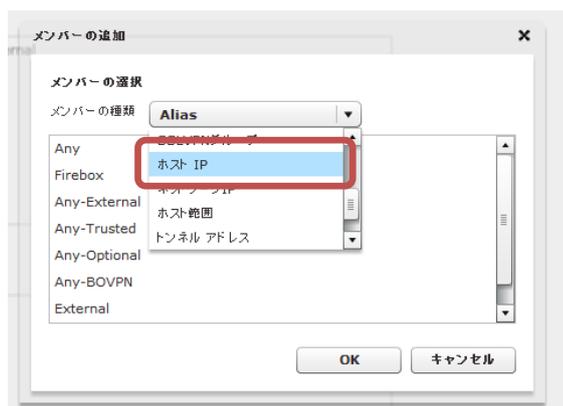
送信先

→ Web サーバーを指定するので、今あるものを削除し

追加ボタンをクリック →

Application Control を有効にします

メンバーの選択で、メンバーの種類を「ホスト IP」にします。



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



メンバーの追加画面では種類の選択ではホスト IP、値は Web サーバーの IP アドレスを入力して OK。ポリシーの新規作成画面に戻ると、以下のように送信先が設定されています。



下方の保存ボタンをクリックし、設定を反映させます。

一覧に戻り、ウェブサーバーにアクセス許可するポリシーが作成されました。

ファイアウォール ポリシー

Auto-Orderモードは有効です。    ヘルプ 

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PB	Application C
✓	 FTP	FTP	Any-Trusted	Any-External	tcp:21		なし
✓	 HTTP-Incoming	HTTP	Any-External	10.100.10.110	tcp:80		なし
✓	 HTTP-Outgoing	HTTP	Any-Trusted	Any-External	tcp:80		なし
✓	 WatchGuard Web UI	WG-Fireware-XTM-	Any-Trusted	Firebox	tcp:8080		なし
✓	 Ping	Ping	Any-Trusted	Any	ICMP (type: 8, code		なし
✓	 WatchGuard	WG-Firebox-Mgmt	Any-Trusted	Firebox	tcp:4105 tcp:4117 t		なし
✓	 Outgoing	TCP-UDP	Any-Trusted	Any-External	tcp:0 udp:0		なし

[Show policy checker](#)

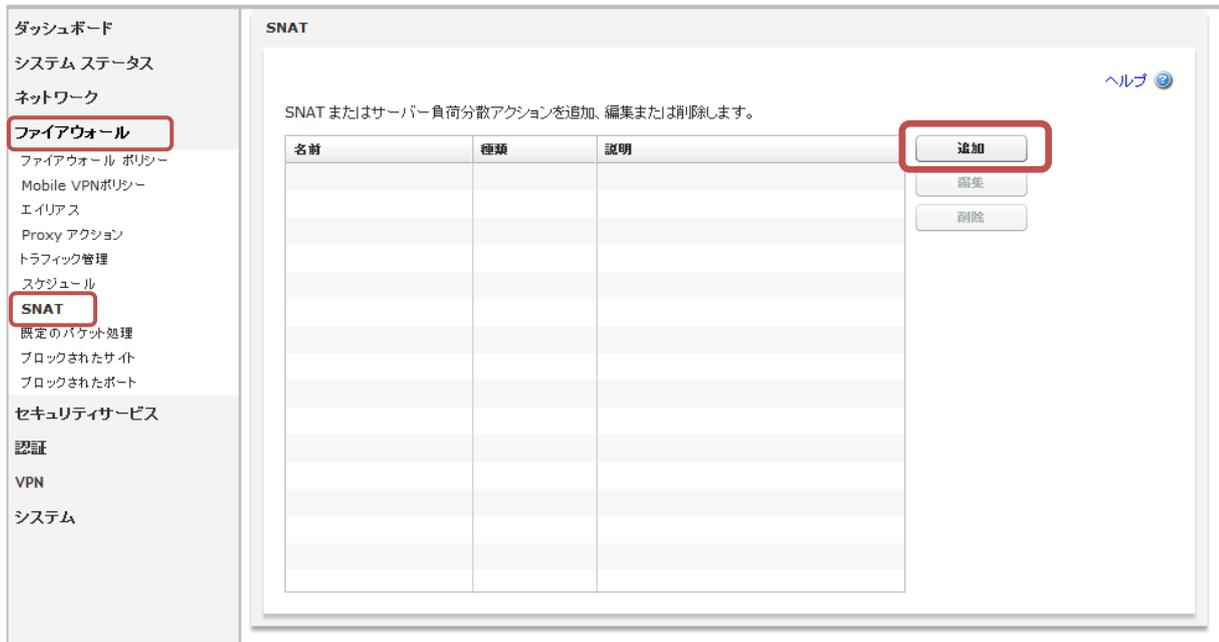
ポリシー追加 (SNAT で外側から内側へ)

前述の Web サーバーへの許可ポリシーは、1-to-1 NAT が前提の設定でしたが、ポリシー単体で NAT を適用することもできます。

それが SNAT(Static NAT)と呼ばれ、1-to-1 NAT と違い、ポートフォワーディングも設定できます。

左側メニューの「ファイアウォール」→「SNAT」をクリックすると SNAT 画面になります。

追加ボタンをクリックし、新しい SNAT を定義しましょう。

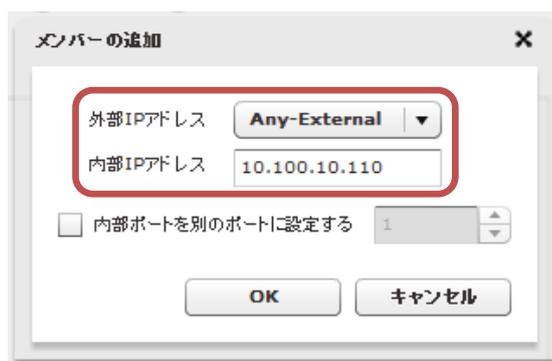


SNAT の名前を入力します。何に対する NAT が分かりやすいものがよいでしょう。

SNAT 画面で追加ボタンをクリックします。

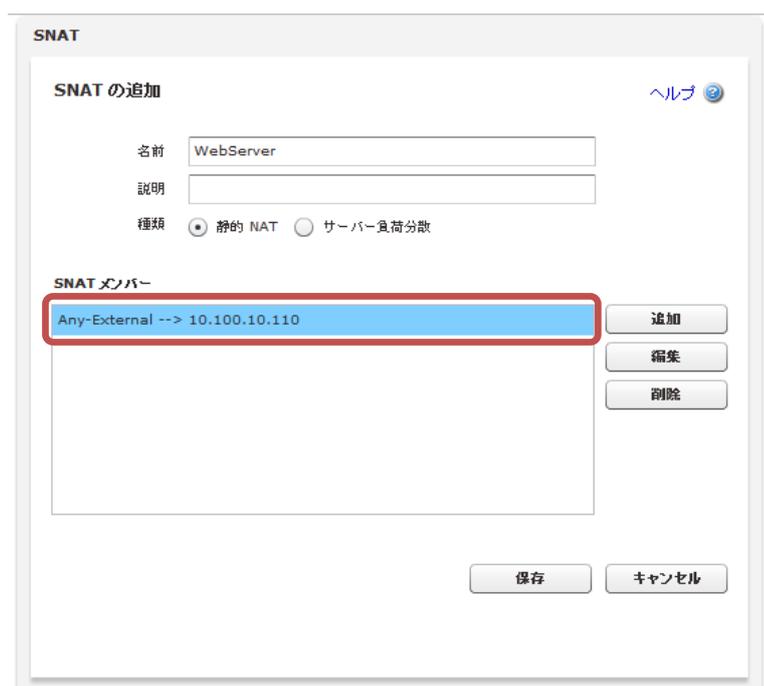


メンバーの追加の画面で、外部 IP アドレスは Any-External、内部 IP アドレスは Web サーバーの 10.100.10.110 を入力して OK をクリックします。



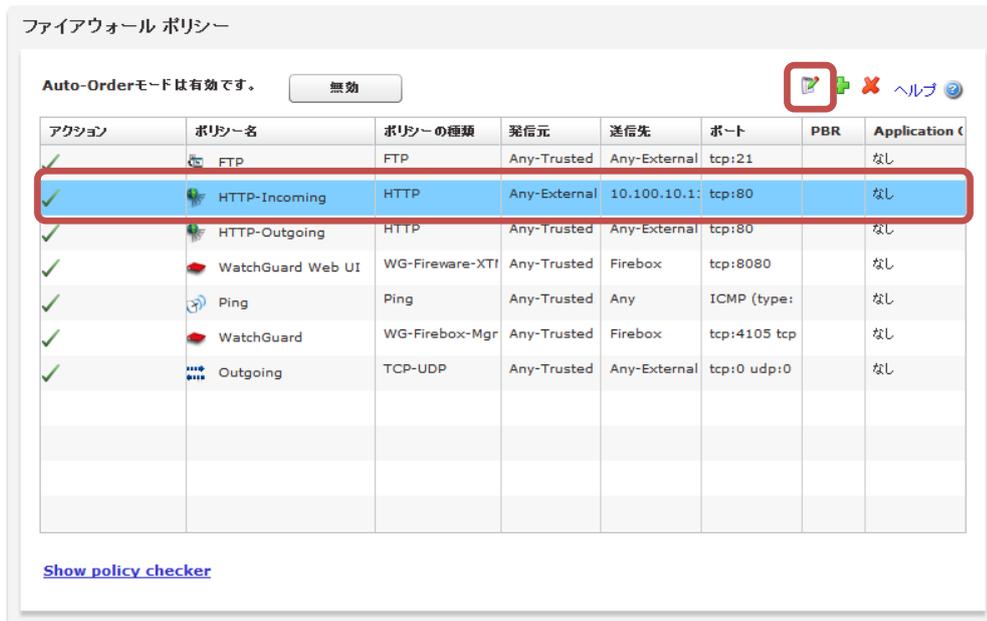
ポートフォワーディングをしたい場合は「内部ポートを別のポートに設定する」にチェックを入れ、変換後のポートを指定します。(例:80 番ポートで受けて 8080 にフォワーディングするなど)

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

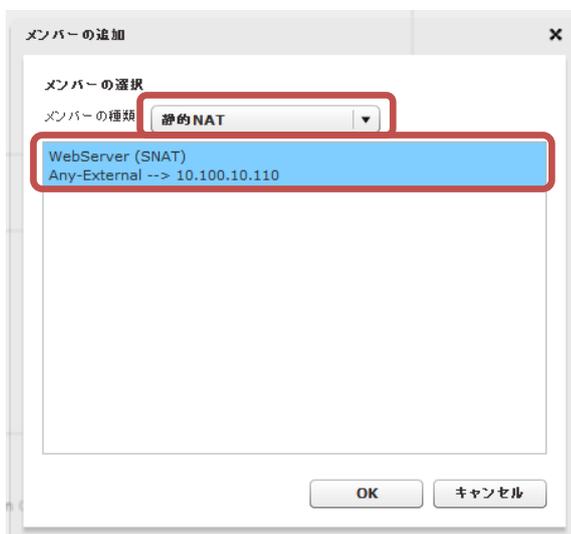


それでは新しく定義した SNAT をポリシーに適用してみましょう。

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



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



事前に定義した SNAT を選択し、OK ボタンをクリックします。

ポリシー設定画面に戻ると以下のように送信先が設定されます。

送信元

Any-External

追加 削除

送信先

WebServer (SNAT)
Any-External --> 10.100.10.110

追加 削除

Application Control を有効にします Global

保存 キャンセル

保存ボタンをクリックし、設定を反映させます。

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

ファイアウォール ポリシー

Auto-Orderモードは有効です。 無効

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PI	Appli
✓	FTP	FTP	Any-Trusted	Any-External	tcp:21		なし
✓	HTTP-Incoming	HTTP	Any-External	Any-External --> 10.100.10.110	tcp:80		なし
✓	HTTP-Outgoing	HTTP	Any-Trusted	Any-External	tcp:80		なし
✓	WatchGuard Web UI	WG-Fireware-XTM-	Any-Trusted	Firebox	tcp:8080		なし
✓	Ping	Ping	Any-Trusted	Any	ICMP (type:		なし
✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted	Firebox	tcp:4105 tcp		なし
✓	Outgoing	TCP-UDP	Any-Trusted	Any-External	tcp:0 udp:0		なし

[Show policy checker](#)

テンプレートにないポリシーを追加する

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

その場合、カスタムでテンプレートを作成することができます。

ポリシー一覧で新規追加ボタンをクリックします。

ファイアウォール ポリシー

Auto-Orderモードは有効です。  [ヘルプ](#)

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PI	Appli
✓	FTP	FTP	Any-Trusted	Any-External	tcp:21		なし

次の画面でカスタムボタンをクリックします。

ポリシー名 [ヘルプ](#)

ポリシーの種類の選択

- ▶ Packet Filters
- ▶ Proxies

プロトコル(ポート番号)を定義するために追加ボタンをクリックします。

新しいポリシー テンプレート

名前

説明

種類 パケット フィルタ Proxy

プロトコル

プロトコル

プロトコルを単一ポートで追加します。

プロトコルの追加

種類

プロトコル

ポート番号

プロトコルを複数追加でき、ポート範囲も指定できます。

プロトコルの追加

種類

プロトコル

最初のポート番号

最後のポート番号

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

保存ボタンをクリックします。

新しいポリシー テンプレート

名前

説明

種類 パケット フィルタ Proxy

プロトコル	操作
TCP:2000	追加
UDP:2000-2010	削除

カスタム アイドル タイムアウトの指定 秒

新しいテンプレートとして登録されました。

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

ポリシー名 ヘルプ

ポリシーの種類を選択

- Packet Filters
- Proxies
- Custom
 - Internal_System**

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。

ポリシー編集

名前: HTTP-Outgoing 有効

ポリシー: プロパティ 詳細

接続は: 許可 ヘルプ

発信元: Any-Trusted

送信先: Any-External

ポリシー編集

名前: HTTP-Outgoing 有効

ポリシー: プロパティ 詳細

接続は: 許可 ヘルプ

保存して一覧に戻ると、ポリシー一覧でも無効になったことが分かります。

ファイアウォール ポリシー

Auto-Orderモードは有効です。 ヘルプ

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PI	Appli
✓	FTP	FTP	Any-Trusted	Any-External	tcp:21		なし
✓	HTTP-Incoming	HTTP	Any-External	Any-External --> 10.100.10.110	tcp:80		なし
⊘	HTTP-Outgoing	HTTP	Any-Trusted	Any-External	tcp:80		なし
✓	WatchGuard Web UI	WG-Fireware-XTM-	Any-Trusted	Firebox	tcp:8080		なし
✓	Ping	Ping	Any-Trusted	Any	ICMP (type:		なし
✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted	Firebox	tcp:4105 tcp		なし
✓	Outgoing	TCP-UDP	Any-Trusted	Any-External	tcp:0 udp:0		なし

ログを記録する

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

ログ記録を有効にするにはポリシーのプロパティの「プロパティ」タブで設定します。

ログ記録の「ログメッセージの送信」にチェックを入れます。

ポリシー構成

名前 Ping 有効

ポリシー プロパティ 詳細

ポリシーの種類: Ping [ヘルプ](#)

ポート	プロトコル
	ICMP (type: 8, code: 255)

コメント

Policy added on 2012-09-26T16:23:35+09:00.

接続を試みたサイトを自動的にブロックする

カスタム アイドル タイムアウトの指定 180 秒

ログ記録

ログメッセージの送信

SNMPトラップを送信

通知を送信

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

運用スケジュールを設定する

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

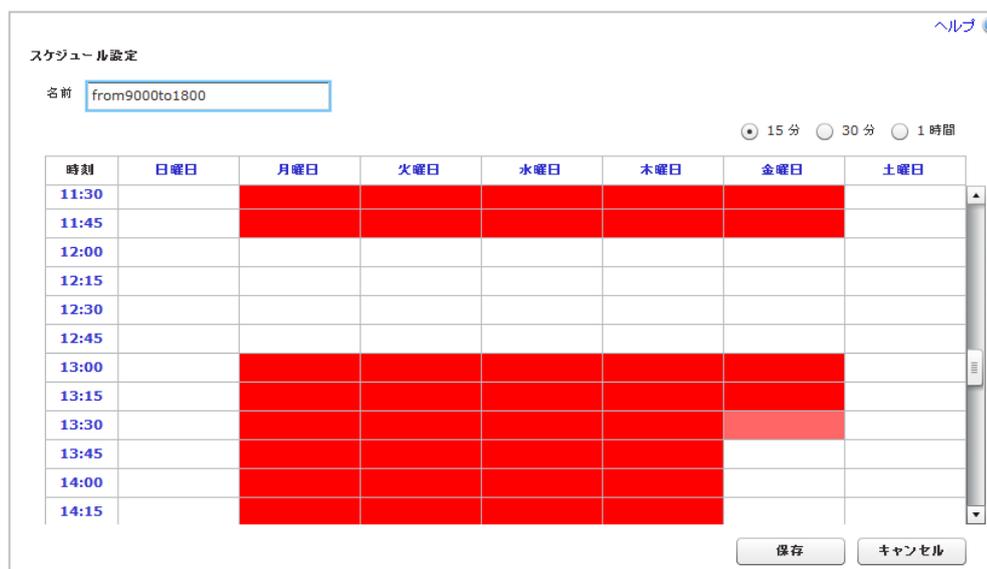
左側メニュー **ファイアウォール** - **スケジュール** をクリックします。

新しいスケジュールを作成するため、追加ボタンをクリックします。



名前にはスケジュールの内容が分かるようなスケジュール名を入力します。

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



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

設定したら保存してください。

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

スケジュール

ヘルプ

スケジュール

名前	追加
Always On	編集
MF 0700-1900	削除
from9000to1800	

スケジュール設定ポリシー

ポリシー名	スケジュール
FTP	Always On
HTTP-Incoming	Always On
HTTP-Outgoing	from9000to1800
WatchGuard Web UI	Always On
Ping	Always On

保存 リセット

ポリシー以外のファイアウォール設定

規定の packets 処理

左側メニュー **ファイアウォール** - **規定の packets 処理** をクリックします。

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

既定の packets 処理

危険なアクティビティ [ヘルプ](#)

- スプーフィング攻撃の防御
- IPソース ルーティングの防御
- ポート空間プローブのブロック 10 送信先ポート/ソースIP(しきい値)
- アドレス空間プローブのブロック 10 送信先IP/ソースIP(しきい値)
- IPSECフラッド攻撃の防御 1500 パケット/秒 (しきい値)
- IKE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 packets

- 未処理 packets 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

- サーバー クォータ当たり 100 接続/秒
- クライアント クォータ当たり 100 接続/秒

保存 リセット

必要に応じて、攻撃と判断する閾値を変更できます。

ブロックされたサイト

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

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

ブロックされたサイト

ヘルプ

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

ブロックされたサイト

ブロックされたサイト	説明
49.212.156.197	
183.181.168.52	
183.181.35.248	
183.181.172.62	
220.48.76.219	
202.249.24.9	

種類を選択 ホスト IP 追加 削除

ホスト IP 206.223.146.68

説明

保存 リセット

ブロックされたポート

左側メニュー「ファイアウォール」－「ブロックされたポート」をクリックします。

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

ブロックされたポート

ヘルプ

ブロックされたポート

1
111
513
514
2049
6000

ポート 1 追加 削除

ブロックされたポートの使用を試みたサイトを自動的にブロックする

保存 リセット

第五章 UTM の設定

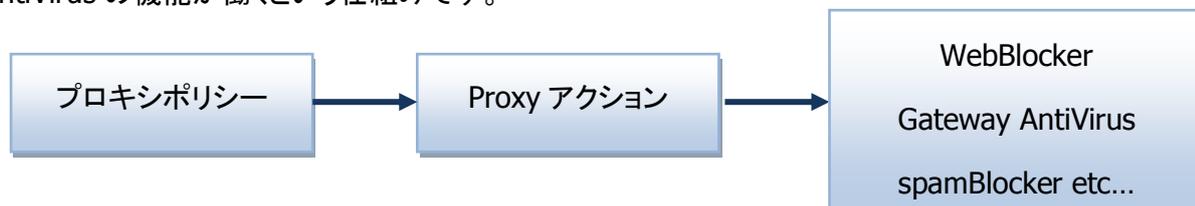
コンテンツフィルタリングやアンチウイルスなど、アプリケーションレベルの脅威に対応する機能を UTM (Unified Threat Management) といいます。

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

プロキシポリシーの追加

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

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



ですので、UTM を有効にするには

1.プロキシアクションの定義、 2.プロキシポリシーの追加、 3.各種 UTM 機能の設定
の 3 つを設定してゆきます。

プロキシアクションの追加

ファイアウォール - Proxy アクション をクリックします。

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

The screenshot shows the UTM configuration interface. On the left is a sidebar menu with categories: ダッシュボード, システム ステータス, ネットワーク, ファイアウォール, ファイアウォール ポリシー, Mobile VPNポリシー, エイリアス, Proxy アクション, トラフィック管理, スケジュール, SNAT, 既定のパケット処理, ブロックされたサイト, ブロックされたポート, セキュリティサービス, 認証, VPN, システム. The 'Proxy アクション' menu item is highlighted with a red box. The main area is titled 'Proxy アクション' and contains a table with columns '名前' and '種類'. The first row, 'HTTP-Client (事前定義済み)', is highlighted with a blue background and a red box. To the right of the table are three buttons: '複製' (highlighted with a red box), '編集', and '削除'.

名前	種類
HTTP-Client (事前定義済み)	HTTP
HTTP-Server (事前定義済み)	HTTP
SMTP-Incoming (事前定義済み)	SMTP
SMTP-Outgoing (事前定義済み)	SMTP
FTP-Server (事前定義済み)	FTP
FTP-Client (事前定義済み)	FTP
DNS-Incoming (事前定義済み)	DNS
DNS-Outgoing (事前定義済み)	DNS
TCP-UDP-Proxy (事前定義済み)	TCP-UDP
POP3-Client (事前定義済み)	POP3
POP3-Server (事前定義済み)	POP3
HTTPS-Client (事前定義済み)	HTTPS
HTTPS-Server (事前定義済み)	HTTPS
SIP-Client (事前定義済み)	SIP
H.323-Client (事前定義済み)	H323

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

Proxy アクション

Proxy アクションの複製 ヘルプ

名前

説明

HTTP要求

全般設定 | **要求方法** | URLパス | ヘッダーフィールド | 認証

接続アイドルタイムアウトの設定 分

URL のパス最大長の設定 バイト

変更されていない範囲要求を許可

このアクションをログに記録する

名前を付けたら下方の保存ボタンをクリックして、アクションを保存します。

HTTP Proxy例外

Deny Message

プロキシおよび AV アラーム

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

プロキシ	種類	複製	編集	削除
HTTP-Client (事前定義済み)	HTTP			
HTTP-Server (事前定義済み)	HTTP			
SMTP-Incoming (事前定義済み)	SMTP			
SMTP-Outgoing (事前定義済み)	SMTP			
FTP-Server (事前定義済み)	FTP			
FTP-Client (事前定義済み)	FTP			
DNS-Incoming (事前定義済み)	DNS			
DNS-Outgoing (事前定義済み)	DNS			
TCP-UDP-Proxy (事前定義済み)	TCP-UDP			
POP3-Client (事前定義済み)	POP3			
POP3-Server (事前定義済み)	POP3			
HTTPS-Client (事前定義済み)	HTTPS			
HTTPS-Server (事前定義済み)	HTTPS			
SIP-Client (事前定義済み)	SIP			
H.323-Client (事前定義済み)	H323			
HTTP-Client-Security	HTTP			

次に、このアクションと紐づいたプロキシポリシーを追加してみましょう。

プロキシポリシーの追加

ファイアウォール - ファイアウォールポリシー からポリシー一覧を表示し、通常のポリシーと同様、ポリシー一覧の追加ボタンをクリックし、ポリシーの追加画面を表示します。

ダッシュボード
システム ステータス
ネットワーク
ファイアウォール
ファイアウォール ポリシー
Mobile VPNポリシー
エリアス
Proxy アクション
トラフィック管理
スケジュール
SNAT
既定のパケット処理
ブロックされたサイト
ブロックされたポート
セキュリティサービス
認証

ファイアウォール ポリシー

Auto-Orderモードは有効です。

アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PBR	Application Contro
✓	FTP	FTP	Any-Tru	Any-Ext	tcp:21		なし
✓	HTTP-Incoming	HTTP	Any-Ext	Any-Ext	tcp:80		なし
⊘	HTTP-Outgoing	HTTP	Any-Tru	Any-Ext	tcp:80		なし
✓	WatchGuard Web UI	WG-Fireware-XTI	Any-Tru	Firebox	tcp:808		なし
✓	Ping	Ping	Any-Tru	Any	ICMP (t		なし
✓	WatchGuard	WG-Firebox-Mgr	Any-Tru	Firebox	tcp:410		なし
✓	Outgoing	TCP-UDP	Any-Tru	Any-Ext	tcp:0 ui		なし

これまでは「Packet Filters」ツリーにあるプロトコルを選択していましたが、UTMを設定する場合は「Proxies」ツリーにあるテンプレートを選択します。

たとえば、コンテンツフィルタリングを設定する場合は、HTTP 通信上の制御なので、HTTP-proxy を追加します。

HTTP-proxy テンプレートを選択し、ポリシー名に名前を入力し、下方の「ポリシーの追加」ボタンをクリックします。

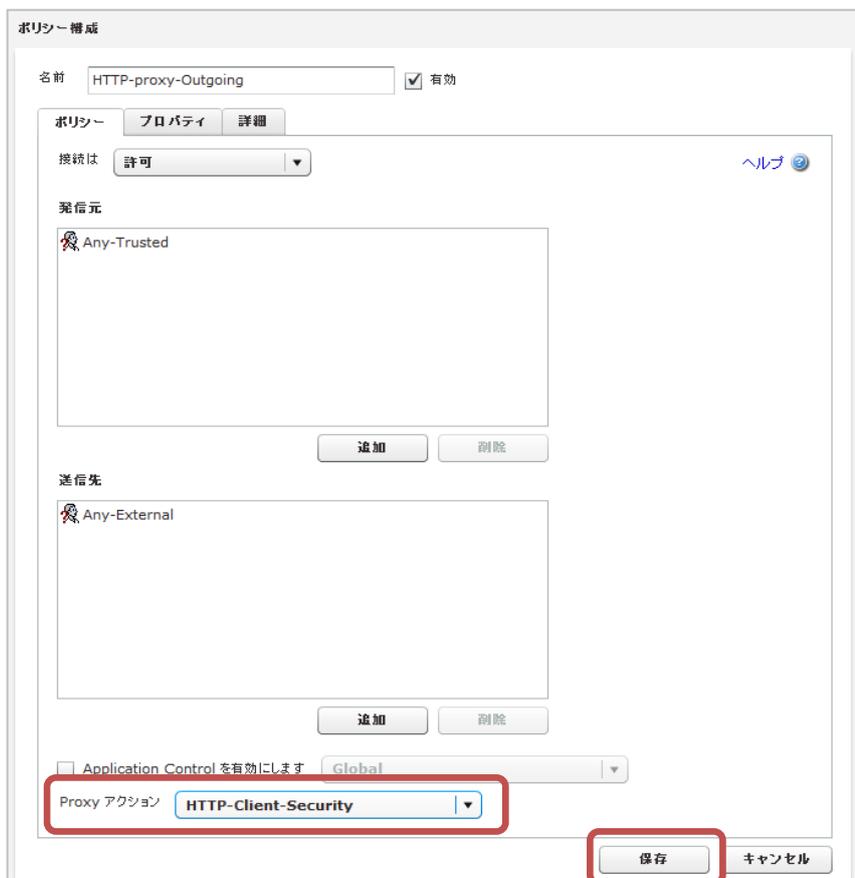
ポリシー名 ヘルプ

ポリシーの種類の選択

- Packet Filters
- Proxies
 - DNS-proxy
 - FTP-proxy
 - H323-ALG
 - HTTP-proxy**
 - HTTPS-proxy
 - POP3-proxy
 - SIP-ALG
 - SMTP-proxy
 - TCP-UDP-proxy
- Custom

Proxy アクション

するとファイアウォール設定と同様の、ポリシーのプロパティ画面が開きます。
 ファイアウォールとプロキシの唯一の違いは、プロパティ画面下方の「プロキシ アクション」です。



つまり、このプロトコルについては基本的には許可ポリシーですが、**通過する際には設定されたアクション(すなわちコンテンツフィルタリングやアンチウィルス)を効かせます**、という意味になります。³

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

最後に保存ボタンを押してポリシーを追加しましょう。

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

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

³ プロキシという呼び名ですが、キャッシュサーバーのように機能するわけではありません

Web Blocker の設定

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

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

Web Blocker を構成する

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

The screenshot shows the WebBlocker configuration interface. On the left, the navigation menu includes 'ダッシュボード', 'システム ステータス', 'ネットワーク', 'ファイアウォール', 'セキュリティサービス', and '認証'. Under 'セキュリティサービス', 'WebBlocker' is selected. The main area is titled 'WebBlocker' and features a 'WebBlockerプロフィール' section with a '新規作成' button highlighted in red. Below this is a table for 'WebBlockerのアクション' with a dropdown menu set to 'None'. At the bottom are '保存' and 'リセット' buttons.

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



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

設定タブを選択します。画面が長いので、2 つに分けて説明します。

まず、WebBlocker のプロファイル名を入力します。

注意すべき設定項目は「サーバータイムアウト」と「ライセンスのバイパス」です。

もしサーバーに一定時間以内にアクセスできない場合やライセンスが切れた場合、デフォルトでは Web の閲覧を切断する設定になっています。つまり全社の Web 利用ができなくなる可能性があります。

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

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

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

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

IP 欄に IP アドレスを入力し、追加ボタンをクリックします。

The screenshot shows the 'WebBlocker Server' configuration window. It features a table with two columns: 'IPアドレス' (IP Address) and 'ポート' (Port). The table is currently empty. To the right of the table are buttons for '上に移動' (Move Up), '下に移動' (Move Down), and '削除' (Delete). Below the table, there is an input field for 'IP' containing '10.100.10.121', a dropdown for 'ポート' (Port) set to '5003', and a blue '追加' (Add) button. The '追加' button is highlighted with a red rectangle.

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

The screenshot shows the 'WebBlocker Server' configuration window after the IP address has been added. The table now contains one row with '10.100.10.121' in the 'IPアドレス' column and '5003' in the 'ポート' column. The '追加' (Add) button is now disabled. Below the table, there is a section for '診断ログ レベル' (Diagnostic Log Level) with a checkbox and a dropdown menu set to 'エラー' (Error). At the bottom right, there are '保存' (Save) and 'キャンセル' (Cancel) buttons.

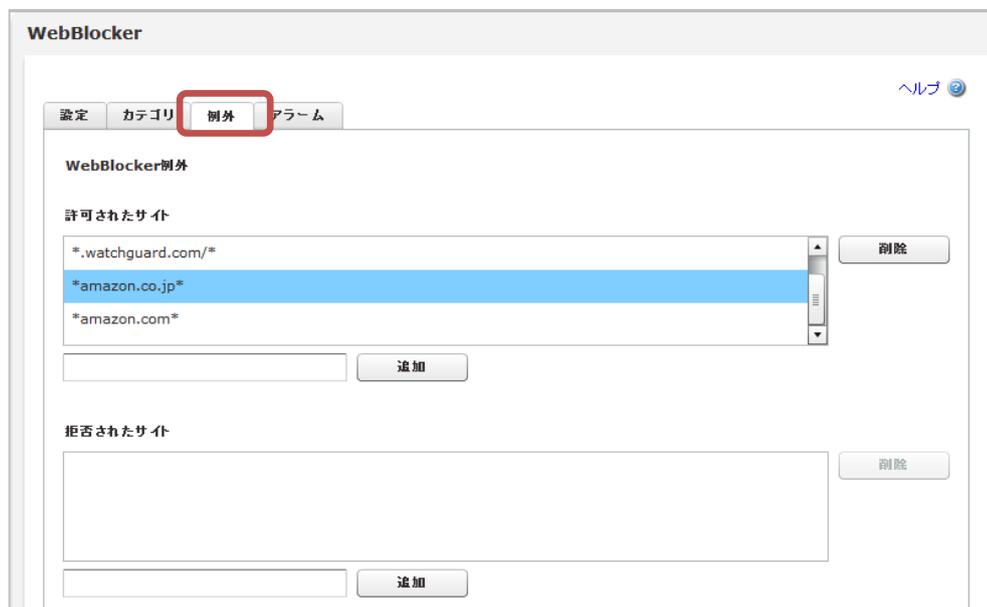
カテゴリタブをクリックします。業務中に閲覧させたくないカテゴリにチェックを入れます。

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



例外タブを選択し、許可されたサイトをパターンで設定できます。

以下は、ショッピングはカテゴリで規制しますが、Amazonは例外で許可する、という設定です。



一通り設定したら、画面下方にある保存ボタンをクリックし設定を反映させます。



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

WebBlocker

ヘルプ

WebBlocker プロファイル

プロファイル	
WebBlocker01	

新規作成
権威
削除

WebBlocker のアクション

HTTP および HTTPS のアクション	
HTTP-Client-Security	None

保存 リセット

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

下の WebBlocker のアクションの欄に、あらかじめ作成したアクション「HTTP-Client-Security」には何も関連付けられず「None」になっています。

このドロップダウンリストで WebBlocker のプロファイル「WebBlocker01」を指定します。

WebBlocker のアクション

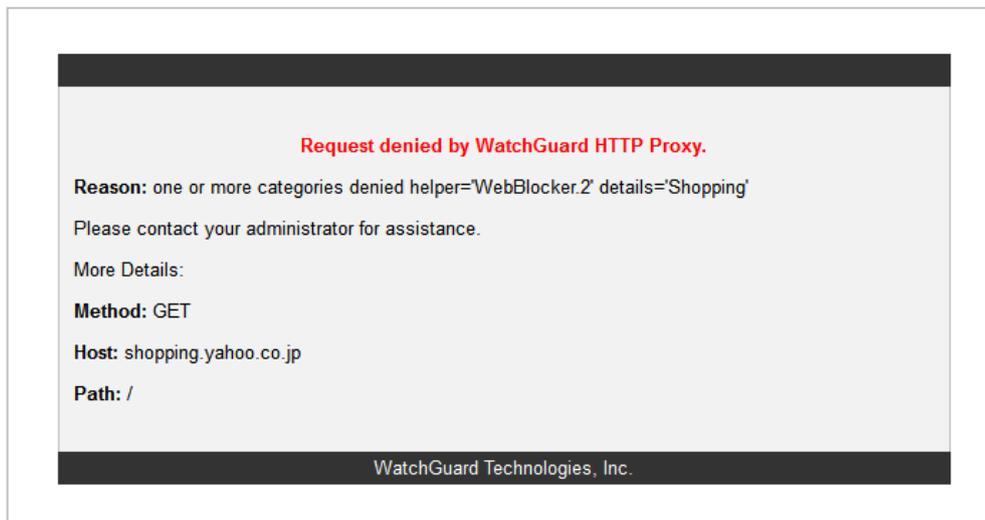
HTTP および HTTPS のアクション	
HTTP-Client-Security	WebBlocker01

保存 リセット

保存ボタンで保存します。

設定を保存したら、試しにショッピングサイトにアクセスしてみてください。

以下のように拒否画面が表示されます。



Gateway AntiVirus の設定

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

Gateway AntiVirus を有効にする

Gateway AntiVirus (以下文中では「GAV」と略します)を使用するには、前節と同様プロキシアクションの定義とプロキシポリシーを追加しておく必要があります。

その上でメニュー **セキュリティサービス** - **Gateway AV** をクリックします。

The screenshot shows the 'Gateway AV' configuration page. The left sidebar has a menu with 'セキュリティサービス' and 'Gateway AV' highlighted. The main content area shows the 'Gateway AV' configuration page with a table of actions and their statuses.

アクション	種類	ステータス
HTTP-Client	HTTP	無効 (事前定義済み)
HTTP-Server	HTTP	無効 (事前定義済み)
SMTP-Incoming	SMTP	無効 (事前定義済み)
SMTP-Outgoing	SMTP	無効 (事前定義済み)
FTP-Server	FTP	無効 (事前定義済み)
FTP-Client	FTP	無効 (事前定義済み)
POP3-Client	POP3	無効 (事前定義済み)
POP3-Server	POP3	無効 (事前定義済み)
HTTP-Client-Security	HTTP	無効

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

The screenshot shows a close-up of the 'Gateway AntiVirus のアクション' table. The 'HTTP-Client-Security' row is highlighted in blue, and the '設定' button is highlighted with a red box.

アクション	種類	ステータス
HTTP-Client	HTTP	無効 (事前定義済み)
HTTP-Server	HTTP	無効 (事前定義済み)
SMTP-Incoming	SMTP	無効 (事前定義済み)
SMTP-Outgoing	SMTP	無効 (事前定義済み)
FTP-Server	FTP	無効 (事前定義済み)
FTP-Client	FTP	無効 (事前定義済み)
POP3-Client	POP3	無効 (事前定義済み)
POP3-Server	POP3	無効 (事前定義済み)
HTTP-Client-Security	HTTP	無効

「Gateway AntiVirus を有効にする」にチェックを入れます。

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



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

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

以上で保存します。GAV は有効になります。

ヘッダーやファイルの種類でGAVをどう適用するかというより細かい設定は、プロキシアクション側で指定します。

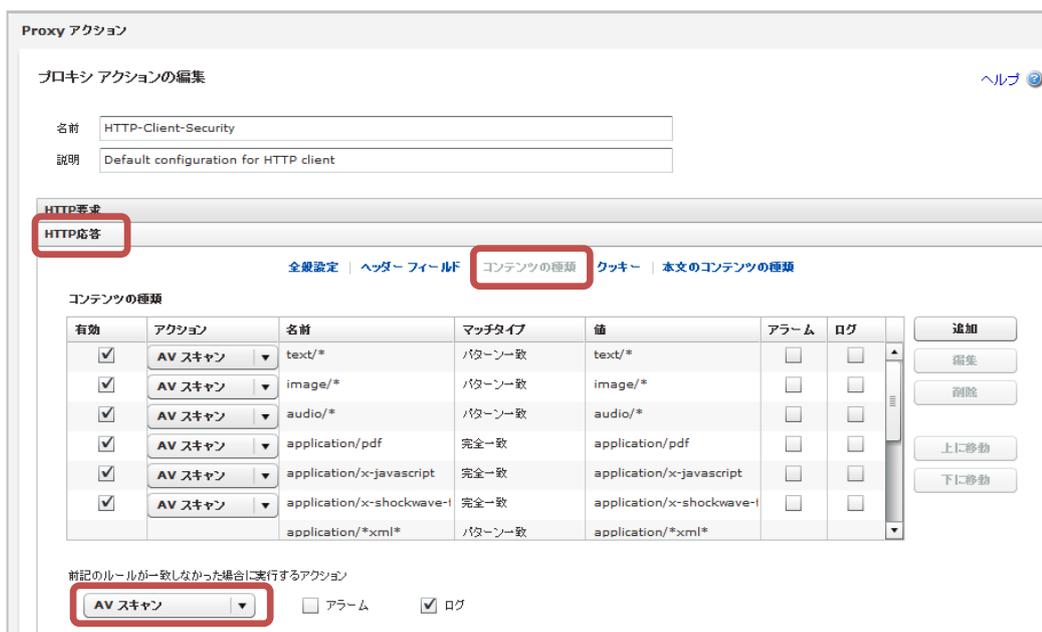
メニューのファイアウォール - Proxy アクションをクリックし、自分で定義したアクションを選択し、編集ボタンをクリックします。



プロキシアクションの編集で「HTTP 応答」のセクションを選択し、「コンテンツの種類」をクリックします。

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

ただ、すべてのヘッダーのパターンを把握して設定するにも限界がありますので、このドロップダウンリストで「AV スキャン」を選択するのも現実的です(つまりすべて AV スキャン対象に)。



次に同じ画面の「本文のコンテンツの種類」リンクをクリックします。

アクションとして、デフォルトでリストにあるコンテンツが「拒否」、それ以外を AV スキャンになっています。

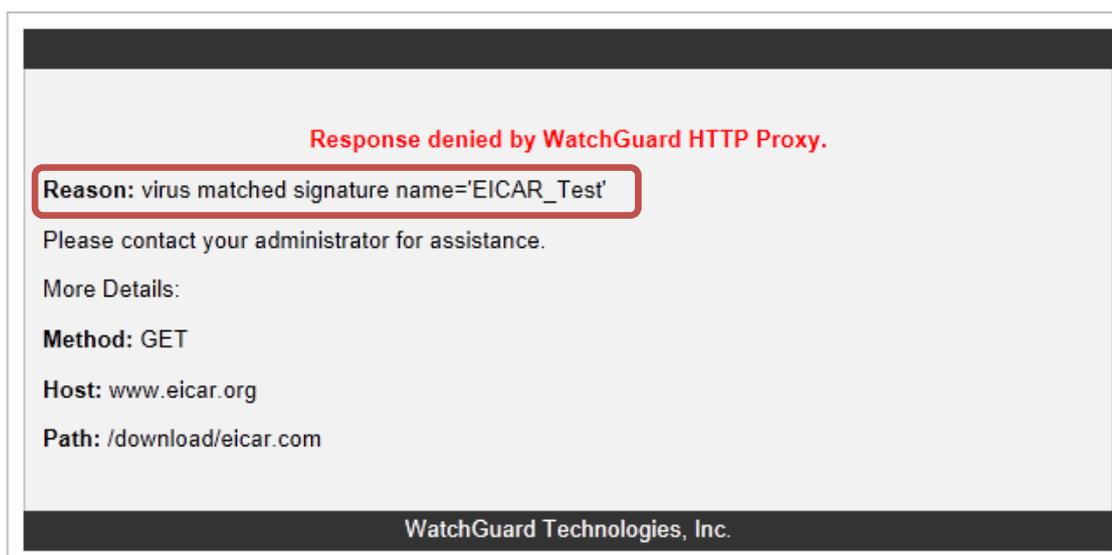
有効	アクション	名前	マッチタイプ	値	アラーム	ログ
<input checked="" type="checkbox"/>	AV スキャン	Java bytecode	パターン一致	%0xcafebabe%*	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	AV スキャン	ZIP archive	パターン一致	%0x504b0304%*	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	AV スキャン	Windows EXE/DLL	パターン一致	%0x4d5a%*	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	AV スキャン	Windows CAB archive	パターン一致	%0x4d53434600000000%*	<input type="checkbox"/>	<input checked="" type="checkbox"/>

しかし、現実的には ZIP ファイルやソフトウェアのインストーラー(.exe)のダウンロードなどが発生しますので、一致する場合もしない場合も AV スキャンを選択しておくといでしょう。

最後に保存ボタンをクリックして、設定を反映させます。

以上で Gateway AntiVirus の設定が完了しました。

しばらく置いておくとシグネチャが更新されて、アンチウイルスが機能するようになります。eicar テストウイルスなどで動作を確認してみてください。



spamBlocker の設定

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

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

POP-Proxy アクションを追加する

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

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

プロキシ	種類	
HTTP-Client (事前定義済み)	HTTP	複製
HTTP-Server (事前定義済み)	HTTP	編集
SMTP-Incoming (事前定義済み)	SMTP	削除
SMTP-Outgoing (事前定義済み)	SMTP	
FTP-Server (事前定義済み)	FTP	
FTP-Client (事前定義済み)	FTP	
DNS-Incoming (事前定義済み)	DNS	
DNS-Outgoing (事前定義済み)	DNS	
POP3-Client (事前定義済み)	POP3	
POP3-Server (事前定義済み)	POP3	
HTTPS-Client (事前定義済み)	HTTPS	
HTTPS-Server (事前定義済み)	HTTPS	
SIP-Client (事前定義済み)	SIP	
H.323-Client (事前定義済み)	H323	

複製画面には諸々の設定項目がありますが、まずはアクションの名前を付けます。

Proxy アクションの複製 ヘルプ ?

名前

説明

そして画面右下の保存ボタンをクリックして、アクションを保存します。

添付

ヘッダー

Deny Message

プロキシおよび AV アラーム

Proxy アクションの一覧に追加されました。

Proxy アクション

ヘルプ 

プロキシ	種類
HTTP-Client (事前定義済み)	HTTP
HTTP-Server (事前定義済み)	HTTP
SMTP-Incoming (事前定義済み)	SMTP
SMTP-Outgoing (事前定義済み)	SMTP
FTP-Server (事前定義済み)	FTP
FTP-Client (事前定義済み)	FTP
DNS-Incoming (事前定義済み)	DNS
DNS-Outgoing (事前定義済み)	DNS
TCP-UDP-Proxy (事前定義済み)	TCP-UDP
POP3-Client (事前定義済み)	POP3
POP3-Server (事前定義済み)	POP3
HTTPS-Client (事前定義済み)	HTTPS
HTTPS-Server (事前定義済み)	HTTPS
SIP-Client (事前定義済み)	SIP
H.323-Client (事前定義済み)	H323
HTTP-Client-Security	HTTP
POP3-Client-Security	POP3

複製
編集
削除

次にプロキシポリシーを追加します。

POP3-proxy ポリシーを追加する

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

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

ダッシュボード
システム ステータス
ネットワーク
ファイアウォール
ファイアウォール ポリシー
Mobile VPNポリシー
エリアス
Proxy アクション
トラフィック管理
スケジュール
SNAT
既定のバケット処理
ブロックされたサイト
ブロックされたポート
セキュリティサービス
認証
VPN
システム

ポリシー名 POP3-proxy-Outgoing ヘルプ

ポリシーの種類の選択

- Packet Filters
- Proxies
 - DNS-proxy
 - FTP-proxy
 - H323-ALG
 - HTTP-proxy
 - HTTPS-proxy
 - POP3-proxy**
 - SIP-ALG
 - SMTP-proxy
 - TCP-UDP-proxy
- Custom

カスタム
編集
削除

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

既定のバケット処理
ブロックされたサイト
ブロックされたポート
セキュリティサービス
認証
VPN
システム

- POP3-proxy
- SIP-ALG
- SMTP-proxy
- TCP-UDP-proxy
- Custom

ポート	プロトコル
110	TCP

ポスト オフィス プロトコルV3

Proxy アクション POP3-Client-Security

ポリシーの追加 キャンセル

ポリシーの追加ボタンをクリックします。

ポリシー構成の画面になるので保存ボタンをクリックします。

ポリシー構成

名前 有効

ポリシー **プロパティ** 詳細

接続は ヘルプ

発信元

送信先

Application Control を有効にします

Proxy アクション

POP3 プロキシポリシーがポリシー一覧に追加されました。

ファイアウォール ポリシー

Auto-Orderモードは有効です。 ヘルプ

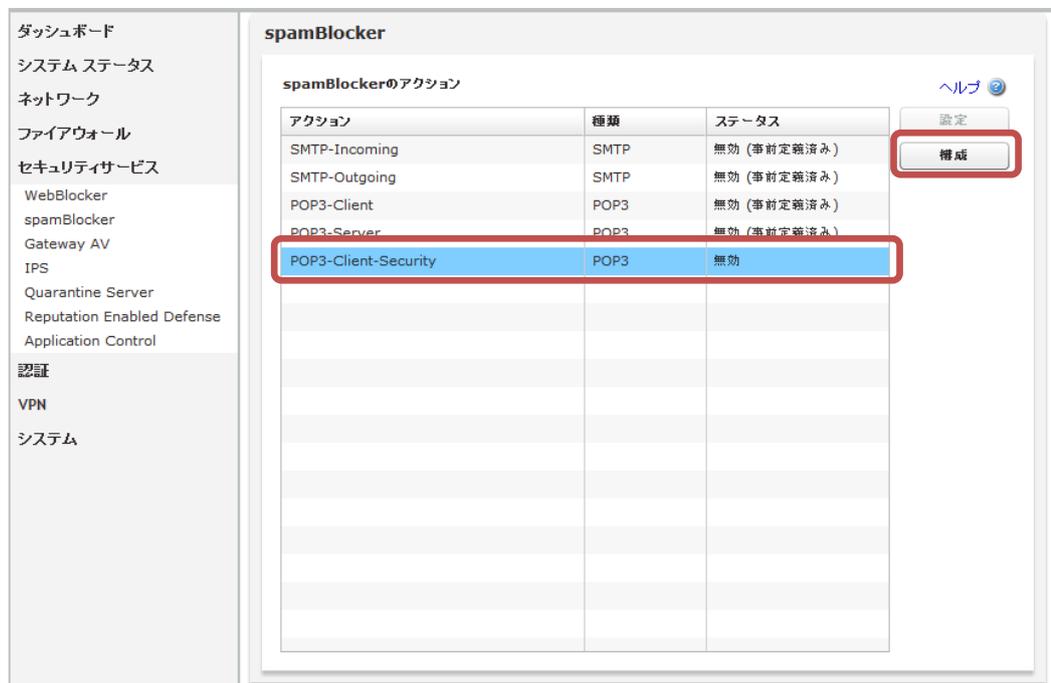
アクション	ポリシー名	ポリシーの種類	発信元	送信先	ポート	PBR	Application Control
✓	FTP	FTP	Any-Trusted	Any-External	tcp:21		なし
✓	HTTP-Incoming	HTTP	Any-External	Any-External	tcp:80		なし
✓	HTTP-proxy-Outgoing	HTTP-proxy	Any-Trusted	Any-External	tcp:80		なし
⊘	HTTP-Outgoing	HTTP	Any-Trusted	Any-External	tcp:80		なし
✓	POP3-proxy-Outgoing	POP3-proxy	Any-Trusted	Any-External	tcp:110		なし
✓	WatchGuard Web UI	WG-Fireware-XTM	Any-Trusted	Firebox	tcp:8080		なし
✓	Ping	Ping	Any-Trusted	Any	ICMP (type		なし
✓	WatchGuard	WG-Firebox-Mgm	Any-Trusted	Firebox	tcp:4105 tcp		なし
✓	Outgoing	TCP-UDP	Any-Trusted	Any-External	tcp:0 udp:0		なし

[ポリシー チェッカーを表示する](#)

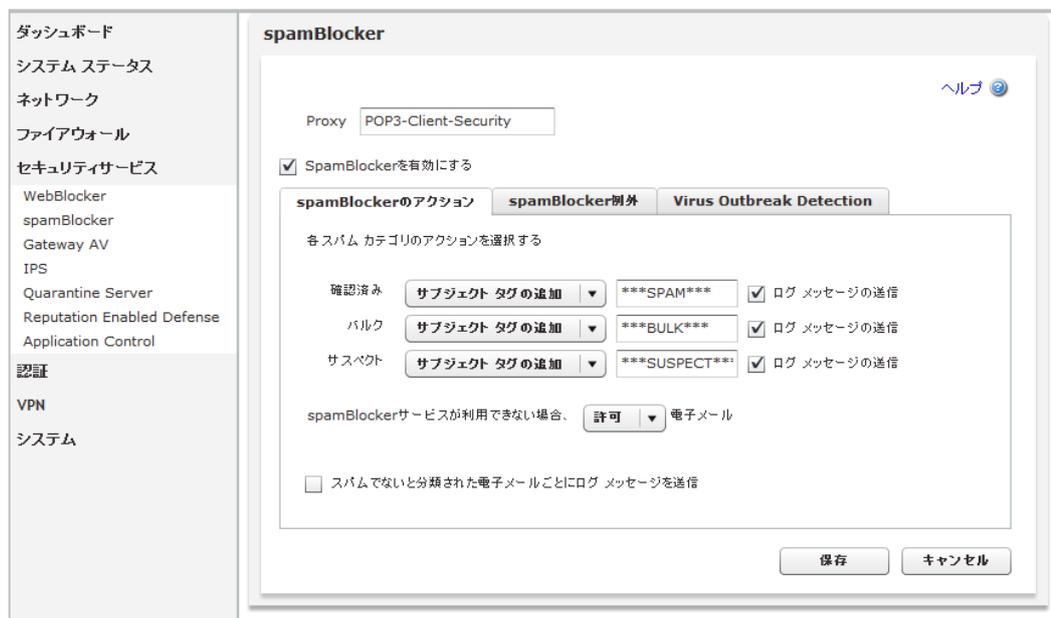
spamBlocker を構成する

メニューの「セキュリティサービス」→「spamBlocker」をクリックします。

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



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



spamBlocker のアクションタブでは、スパムメールが検知された際の動作を定義できます。
 カテゴリは、確認されたスパム、バルク(主に広告メールなど)、未確認(だが疑わしいもの)の3種類です。
 アクションは、指定の文字列(タグ)をサブジェクトに追加するか、許可するかのどちらかです。

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

この例では*@watchgaurd.com をホワイトリストに入れています。
 *@watchguard.co.jp も入力し、追加ボタンを押せばホワイトリストの一覧に入ります。

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

SpamBlockerを有効にする

spamBlockerのアクション spamBlocker例外 **Virus Outbreak Detection**

Virus Outbreak Detection

ウイルス検出時 削除 アラーム このアクションをログに記録する

スキャン エラー発生時 許可 アラーム このアクションをログに記録する

保存 キャンセル

ウイルス検出時は「削除」、スキャンエラー時は「許可」がよいでしょう。

設定を保存して動作を確認してください。

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

アクション	種類	ステータス
SMTP-Incoming	SMTP	無効 (事前定義済み)
SMTP-Outgoing	SMTP	無効 (事前定義済み)
POP3-Client	POP3	無効 (事前定義済み)
POP3-Server	POP3	無効 (事前定義済み)
POP3-Client-Security	POP3	有効

ヘルプ 設定 構成

以上で spamBlocker の設定は完了です。

WebUI 基本設定ガイドは以上です。

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

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

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

御社のセキュリティ向上をお祈りしております！

お問い合わせ先

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

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

- 購入後のサポート問い合わせ

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