

Firebox WebUI ガイド



ウォッチガード・テクノロジー・ジャパン株式会社 2019 年 8 月 Rev-5

目次

はじめに
第一章 Firebox のセキュリティ概念6
Firebox のネットワーク概念6
WebUI のネットワーク設定に見る Firebox の概念7
WebUI のポリシー設定画面に見る XMT の概念8
Firebox で実現可能なセキュリティ範囲9
WebUI の概要10
WebUI の制限事項10
第二章 初期設定11
事前準備
ファクトリーリセット14
結線14
Firebox M440 のリセット15
Firebox M400/500 のリセット16
Firebox T シリーズ17
ファクトリーリセット後の設定18
Web Setup Wizard19
機能キーの追加
第三章 ネットワークの設定33
外部ネットワークの設定
固定 IP の設定
DHCP の設定
PPPoE の設定40
DNS/WINS 設定
DNS の設定42
WINS の設定
内部ネットワークの設定45
Trusted インターフェイスの設定45

[)HCP サーバーの使用	6
_	ブリッジの構成	9
[MZを設定する	6
٦	IAT 設定(1-to-1NAT)	8
j	レーティング設定	2
第四章	☞ ファイアウォールの設定	4
ポリ	シー設定画面	4
Ī	回面構成64	4
7	ポリシーの変更/追加/保存	6
ポリ	シーの追加	7
7	ポリシー追加 (内側から外側へ)6	7
7	、 ポリシー追加 (外側から内側へ)	0
7	ペリシー追加 (SNAT で外側から内側へ)75	5
-	-ンプレートにないポリシーを追加する	9
ポリ	シーの編集	3
-	-時的に無効にする	3
Γ	コグを記録する	4
i	デ こ ジュールを設定する	5
ポリ	シー以外のファイアウォール設定	8
ţ	見定のパケット処理	8
-	$\ddot{\nu}$	9
-	ブロックされたポート	9
第五章	を UTMの設定 の	0
プロ	キシポリシーの追加	0
-	ッシュンクションの追加	1
-	プロキシポリシーの追加 94	4
We	h Blocker の設定	7
		7
Gat	eway AntiVirusの設定	5
	/	~

Gateway AntiVirus を有効にする	105
Gateway AntiVirus を設定する	107
spamBlocker の設定	113
POP-Proxy アクションを追加する	113
POP3-proxy ポリシーを追加する	116
spamBlocker を構成する	
おわりに	123

はじめに

この度はウォッチガード製品を選定していただきありがとうございます。

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

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

なお、本書で使用されている設定画面は、2019 年 5 月時点での最新バージョン Fireware OS v12.4 のものです。

このガイドが、Fireboxを自在に使いこなす一助になれば幸いです。

第一章 Firebox のセキュリティ概念

Firebox のネットワーク概念

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

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



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

WebUI のネットワーク設定に見る Firebox の概念

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

またそれらは固定ではなく自由に設定できます。

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

ヾのモードでイン	ターフェイスを構	#成: ミックスルー	ティング モード 🛛 💌		
インターフェイン	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
1	信頼済み	Trusted	192.168.111.1/24		自動ネゴシエー
2	任意	Optional-1	172.16.1.201/24		自動ネゴシエー
3	ブリッジ	Local-Net-1			自動ネゴシエー
4	ブリッジ	Local-Net-2			自動ネゴシエー
5	信頼済み	Local-Net-3	192.168.1.1/24		自動ネゴシエー

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

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

WebUI のポリシー設定画面に見る XMT の概念

以下は実際のポリシー構成画面です。(第四章で詳しく解説します) 前述のネットワークの方向に従って設定されることが分かるでしょう。



Firebox で実現可能なセキュリティ範囲

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



レイヤー7までカバーするのが UTM です。

パケットフィルタ: ポートベース

ファイアウォール : ステートフルパケットインスペクション

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

WebUI の概要

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

これは、ブラウザでアクセスする環境があれば、Windows、Linux、Mac OS、また他のどんなプラットフォームのコンピュータからでも Firebox デバイスを管理できることを意味します。

Web UI は、リアルタイム管理ツールです。デバイスに行なった変更はすぐに反映されます。

WebUI の制限事項

すべての設定は、WSM に含まれる Policy Manager で完了できますが、WebUI では制限事項があります。 完了できないタスクは以下のとおりです(Fireware 11.9.4 時点)。

- 既定のパケット処理オプションのログ記録の変更
- ポリシーの名前を変更する
- カスタム アドレスをポリシーに追加する
- ホスト名 (DNS 参照) を使用してポリシーに IP アドレスを追加する
- FireCluster のメンバーであるデバイスの構成を表示または変更する
- セカンダリの PPPoE インターフェイスを追加・編集する

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

第二章 初期設定

事前準備

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

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



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

また、必要なソフトウェアもインストールしておきましょう。前述のとおり、WebUI には WSM と比較して若干の制限事項がありますので、すぐに使わないとしても、管理者の方は WSM をあらかじめインストールしておくことをおすすめします。Fireware は最新バージョンにアップグレードする際に必須となります。

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



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

次に Fireware もインストールします。こちらのインストールウィザードもすべてデフォルトで進めてください。 以上で準備は完了です。 ファクトリーリセット

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

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

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

結線

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

Firebox M シリーズ



Firebox T シリーズ



次にシリーズごとのリセット方法を解説します。

Firebox M440 のリセット

1. 本体背面の電源スイッチを入れ、電源を投入します



- 2. デバイス前面の電源ボタンを3秒間長押しして、一旦電源を切ります
- 3. デバイス前面のリセットボタンを押した状態で、電源ボタンを短く押して電源を入れます

M440 の電源ボタンとリセットボタンの位置



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



5. Attn インジケーターが点滅から点灯に変わるまで待ちます

Attn インジケーターが点灯になったらリセットされたことを意味します

6. 電源ボタンを短く押して電源を入れます

Firebox M440 リセット

1. 本体背面の電源スイッチを入れ、電源を投入します



M440の電源ボタンとリセットボタンの位置

- 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

WitchGuard* Direbox* M440					
L	リセットァ	ドタン	電源ボタ:	י א א	

Arm インジケーター

- 4. Arm インジケーターが赤い間、リセットボタンを押し続けます
- 5. Arm インジケーターがゆっくり緑色に点滅している間も押し続けます
- 6. 緑色の点滅が早くなったら手を離し、点滅が赤になるまで待ちます

Arm インジケーターが赤の点滅になったらリセットされたことを意味します。



Firebox T シリーズ

1. 電源を投入します。

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



2. Attn インジケーターが点滅し始めたらリセットボタンを離します。



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

- 3. Attn インジケーターが点滅しない場合は、点灯するまでリセットボタンを押し続けます。点灯したらリ セットボタンを離します
- 4. 点灯した状態がリセットされたことを表わします。

ファクトリーリセット後の設定

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

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

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

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

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

【豆知識】どんなときに初期化が必要?

- ✓ 構成パスフレーズを忘れてしまった
- ✓ 検証フェーズ終了後、本番設置前にきれいに一から設定したい
- ✓ ある拠点から Firebox を引き上げてきて、別の拠点で使うために一から設定したい
- ✓ 雷による停電。復帰後、起動したらコンフィグが壊れていた(稀ですが過去の事例にありました)。 きれいな状態に戻してから、バックアップしていたコンフィグを読み込ませたい
- ✓ Fireware をアップグレードしたが、元のバージョンに戻したい

Web Setup Wizard

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

設定する PC とリセットしたデバイスの 1 番ポートを結線し、ブラウザのアドレスバーに https://10.0.1.1:8080 を入力し、アクセスします。



証明書のセキュリティ警告が出てもそのまま続行します。

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



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

構成の種類を選択してください。

Firebox の新しい構成を作成する
 バックアップ イメージの復元

使用許諾契約を読む

□ 以下に同意します: エンドユーザー使用許諾契約

その他の情報

况入

使用許諾契約の条項に同意して[次へ]。

エンドユーザー使用許諾契約	Х
End-User License Agreement	
Please note that this End-User License Agreement may be different from any prior End-User License Agreement you agreed to when activating a subscription	
service or a prior renewal, and will supersede any such prior agreement.	
IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:	
This WatchGuard Product (the "PRODUCT") End-User License Agreement ("AGREEMENT")	
is a legal agreement between you (either an individual or a single entity) and	
(including any product trade-ups for this PRODUCT) that accompanies this FULA	
which includes software, computer software components (whether installed separately	
on a computer workstation or on the WATCHGUARD hardware product (THE "HARDWARE PRODUCT") and may include associated media, printed materials, and on-line or electronic	
documentation, and any updates or modifications thereto, (the "SOFTWARE PRODUCT").	
WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition	\sim

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

外部インターフェイスは DHCP(デフォルトのまま)を選択し[次へ]。

Web Setup Wizard へようこそ

朗報です!お使いの Firebox がオンラインになり、アクティブ化されました。

既定では、Firebox では DHCP を使用して外部インターフェイスの IP アドレスが取得されます。他のネットワーク設定で外部インターフェイスを構成することもできます。

● 既定の DHCP 外部インターフェイス設定を維持する

○ 外部インターフェイス設定を構成する



DNS サーバーの指定です。後から設定できますが、プロバイダもしくはシステム部門指定の IP アドレスが 決まっていましたら入力して[次へ]。

DNS サーバーと WINS サーバーのアドレス情報を追加しま Fireware 機能の IP アドレスに名前が解決されます。	す。Firebox でこれらのアドレスが使用る	され、DHCP クライアントと一部の
ドメイン名		
DNS サーバー		
WINS サーバー		
その他の情報		戻る次へ

信頼済みインターフェイス(現在接続しているポート)の設定です。

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

DHCPを有効にしたくない場合はチェックを外して[次へ]。

信頼済みインターフェイスを構成する

信頼済みインターフェイス用に、内部のプライベート 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 アドレスは信頼済みインターフェイスとなります。

IP アドレス	10.0.1.1	1	24	
☑ このインタ	ターフェイス上で DHCP サーバ	-7	を有効に	する
IP アドレス範	囲			
開始	10.0.1.2			
終了	10.0.1.254			

信頼済みインターフェイスの IP アドレスを変更すると、ウィザードを完了した後、新しい IP アドレスを使用して Fireware Web UI に接続する 必要があります。また、コンピュータの IP アドレスがこのインターフェイス IP アドレスと同じサブネット上にあることを確認する必要があり ます。

その他の情報	戻る	次へ	

パスフレーズの設定です。status ユーザーは設定の読み取り専用のアカウント、admin ユーザーは設定が 保存できる管理者アカウントです。それぞれを8文字以上の英数字で設定します。

status と admin は同じパスフレーズを使用することはできません。

Firebox のパスフレーズを作成する

Firebox には、2つの	既定のユーザー アカウントが含まれています。	
admin — 読み書きの ステータス — 読み取	の権限。 双り専用の権限。	
各アカウントで使用す 各パスフレーズは 8 〜	るパスフレーズを入力します。 • 32 文字にする必要があります。	
ユーザー名	ステータス (読み取りのみ)	
パスフレーズ	•••••	
パスフレーズの確認	•••••	
ユーザー名	管理者(読み書き)	
パスフレーズ	••••••	
パスフレーズの確認	••••••	

その他の情報	戻る	次へ

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

リモート管理を有効化する

リモートネットワークから Firebox を管理するには、オプションを選択して、リモートコンピュータの IP アドレスを指定します。

□ リモートコンピュータから Firebox を管理できるようにする

リモートコンピュータ IP ア	
ドレス	

Firebox の既定の構成には、自動的に WatchGuard ポリシーが組み込まれます。このポリシーにより、信頼済みネットワークまたは任意ネット ワーク上のコンピュータから Firebox に接続して管理することができるようになります。リモート管理を有効にすると、指定された IP アドレ スがポリシーに追加され、リモートコンピュータからの接続が可能となります。

その他の情報	戻る	次へ

デバイス名を入力し[次へ]。

連絡先とフィードバックの設定を構成する

連絡先情報

この Firebox の情報を指定します。これにより、複数のデバイスを管理する際に Firebox を特定することができます。

デバイス名	T50-W
デバイスの場所	
担当者	

デバイスフィードバック

デバイスのフィードバックを参考に、WatchGuard は製品や機能の改善に努めています。お使いの Firebox から WatchGuard に送信される フィードバックには、Firebox の使用方法に関する情報が含まれますが、貴社または貴社のデータに関する識別情報が含まれることはありません。

☑ デバイスフィードバックを WatchGuard に送信

その他の情報	戻る	次へ
Letter and the second		

タイムゾーンは「(GMT+09:00)大阪、札幌、東京」を選択して[次へ]。



その他の情報	戻る	次へ

有効化の画面になります。¹機能キーを追加 を選んで[次へ]。

機能キーを追加する

ウィザードですべてのライセンス機能を構成するには、機能キーが必要です。WatchGuard アカウントで Firebox を有効化して、 をローカル ファイルにダウンロードした場合は、今すぐに機能キーを Firebox に追加することができます。	その機能キー
 機能キーを追加 この手順をスキップ 	

その他の情報	戻る	次へ

あらかじめ取得しておいた機能キーをテキストボックスに貼り付けて [次へ]。

機能キーを追加する

ature: MUVFN_DSER#50 ature: NETWORK_DISCOVERY@Mar-17-2022 ature: RED@Mar-17-2022 ature: SESSION#200000 ature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB ature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB ature: SSLVPN_USER#50 ature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB ature: VLAN#75 ature: VLAN#75 ature: VLAN#75 ature: VLAN#75 ature: VFN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: MUVPA_USEK#50 eature: NETWORK_DISCOVERY@Mar-17-2022 eature: RED@Mar-17-2022 eature: SESSION#200000 eature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB eature: SSLVPN_USER#50 eature: SSLVPN_USER#50 eature: VLAN#75 eature: VLAN#75 eature: VLAN#75 eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: 302d02150276586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: LIVESECURITY@Mar-17-2022	~
ature: NE I WORK_DISCOVERY@Mar-17-2022 ature: SED@Mar-17-2022 ature: SESSION#200000 ature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB ature: SSLVPN_USER#50 ature: VLNM#75 ature: VLNM#75 ature: VVPN_SPEED#0 ature: VVPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: RE1WORK_DISCOVERY@Mar-17-2022 eature: RED@Mar-17-2022 eature: SESSION#200000 eature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB eature: SSLVPN_USER#50 eature: SLVPN_USER#50 eature: TDR@Mar-17-2022;AMER eature: VPN_SPEED#0 eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: MUVPN_USER#50	
ature: REU@Mar-17-2022 ature: SESSION#200000 ature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB ature: SSLVPN_USER#50 ature: SLVPN_USER#50 ature: UAN#75 ature: VLNM#75 ature: VPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: SESGION#20000 eature: SESSION#20000 eature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB eature: SSLVPN_USER#50 eature: TDR@Mar-17-2022;AMER eature: TDR@Mar-17-2022;AMER eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: NETWORK_DISCOVERY@Mar-17-2022	
ature: SESSION#200000 ature: SESSION#200000 ature: SLVPN_USER#50 ature: SLVPN_USER#50 ature: VLAN#75 ature: VPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: SESSION#200000 eature: SESSION#200000 eature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB eature: TDR@Mar-17-2022;AMER eature: VLAN#75 eature: VPN_SPEED#0 eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: RED@Mar-17-2022	
ature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB ature: SPLVPN_USER#50 ature: TVR@Mar-17-2022;AMER ature: VLAN#75 ature: VPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB eature: SSLVPN_USER#50 eature: TDR@Mar-17-2022;AMER eature: VLAN#75 eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: SESSION#200000	
ature: SSLVFN_USER#50 ature: TDR@Mar-17-2022;AMER ature: VLN#75 ature: VVPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: SSLVPN_USER#50 eature: TDR@Mar-17-2022;AMER eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: SPAMBLOCKER@Mar-17-2022;UC17Q63WEU2Q2UGD54HB	
ature: TDR@Mar-17-2022;AMER ature: VLAN#75 ature: VPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: TDR@Mar-17-2022;AMER eature: VLAN#75 eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: SSLVPN_USER#50	
ature: VLAN#75 ature: VLAN#75 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: VLAN#75 eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: TDR@Mar-17-2022;AMER	
ature: VPN_SPEED#0 ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never ynature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: VPN_SPEED#0 eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: VLAN#75	
ature: WEBBLOCKER@Mar-17-2022 ature: XTM_PRO piration: never jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: WEBBLOCKER@Mar-17-2022 eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: VPN_SPEED#0	
ature: XTM_PRO piration: never nature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	eature: XTM_PRO xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: WEBBLOCKER@Mar-17-2022	
piration: never nature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3	xpiration: never ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	eature: XTM_PRO	
<pre>jnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- dc2d3b412adfad-9b23f736e317b3</pre>	ignature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6- 3dc2d3b412adfad-9b23f736e317b3	kpiration: never	
dc2d3b412adfad-9b23f736e317b3	3dc2d3b412adfad-9b23f736e317b3	gnature: 302d0215027e586a-40871e2ddda5bb8c-58e415a75f038b27-61021428b23fd8b6-	
		3dc2d3b412adfad-9b23f736e317b3	
			\sim

その他の情報

有効化された登録サービスを確認し、[次へ]。

戻る

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

セキュリティサブスクリプションサービス

Firebox の機能キーには、以下の登録サービスが含まれています。ウィザードでは、推奨されるセキュリティ設定に基づき、これらの登録サービスが自動的に有効化されます。

- ✓ Gateway AntiVirus(ゲートウェイアンチウィルス) ウイルスが検出されると HTTP および FTP 接続を切断します
- ✓ IPS(不正侵入検知・防御) ネットワーク脆弱性と識別された接続を切断します
- ✓ Application Control(アプリケーション制御) 危険性の高いアプリケーションからトラフィックを切断します
- ✓ Reputation Enabled Defense ボットネット サイトやその他の敵意があるサイトからトラフィックをブロックします
- ✓ APT Blocker(標的型攻撃対策) 高度なマルウェアに関連した接続を識別して切断します

ウィザードで WebBlocker も有効化することができます。次に、拒否する WebBlocker コンテンツ カテゴリを選択します。

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

WebBlocker カテゴリを選択する

WebBlocker により、悪意のある Web サイトおよびその他の危険な Web コンテンツに対する送信接続を拒否できます。これらのコンテンツ カテゴリを拒否することをお勧めします。 ② セキュリティ (マルウェア、ボットネットワーク、スパイウェア、悪意のある、およびその他のサブカテゴリ) ③ 拡張された保護 (新しい脆弱性、疑わしいコンテンツ、およびその他のサブカテゴリ) ④ プロキシ回避 ④ パークドメイン 拒否するその他の一般的な Web サイト カテゴリを選択してください。 ■ 成人向け素材 (ヌード、アダルトコンテンツ、性的内容) ■ ギャンブル ■ 不寛容 ■ 下品 ■ 暴力

ウィザードが完了したら、WebBlocker 構成を編集して、追加のコンテンツ カテゴリを拒否することができます。



最後に設定のサマリーが表示されますので、内容を確認して[次へ]。

概要

以下の構成が選択されています。

有効化	成功しました
機能丰一	手動で適用
外部インターフェイス	DHCP — 自動的に IP アドレスを取得する
ドメイン名	なし
DNS サーバー	なし
WINS サーバー	なし
信頼済みインターフェイス	10.0.1.1/24 — DHCP サーバーは有効化されています
リモートホスト IP アドレス	なし — リモート管理は無効になっています
デバイス名	T50-W
デバイスの場所	なし
担当者	なし
タイムゾーン	(GMT+09:00) 大阪、札幌、東京
WebBlocker(Webフィルタリング)	Enabled
Gateway AntiVirus(ゲートウェイアンチウィルス)	Enabled
IPS(不正侵入検知・防御)	Enabled
Application Control(アプリケーション制御)	Enabled
RED	ボットネット検出を含むフィードバックが有効化されました
APT Blocker(標的型攻擊対策)	Enabled

これらの設定を適用するには、次へ をクリックします。

設定が保存されます。

設定の保存	

セットアップ完了が表示されます。

設定は完了です。

Firebox の基本構成が完了しました。これにより、アウトバウンド TCP、UDP、FTP、DNS、HTTP、HTTPS、および ping 接続が許可され、要求していないすべてのインバウンド接続がブロックされるようになります。ウィザードに表示されるライセンス付与された登録サービスは、推奨設定で有効化されています。

Firebox OS を更新する

使用可能な Firebox の Fireware OS の更新を見つけるには、Fireware Web UI で、システム > OS をアップグレードする の順に選択します。

Firebox を管理する Fireware Web UI を開く WatchGuard System Manager をダウンロードする https://10.0.1.1:8080 http://software.watchguard.com



自動的に再起動がかかり、設定した内容で起動します。3~4分お待ちください。

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

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

WatchGuard	Fireware Web UI	д— У —: admin ? 🤇
ダッシュポード	フロント バネル	C
	トップクライアント すべて表示	システム
	名前 レートキ パイト ヒット	名前 T50-W-Kamiyacho46 モデル T50-W
	10.0.1.3 203 кърз 839 кв 31	バージョン 12.4.8589964
トラフィックモニタ ゲートウェイ ワイヤレス コントローラ Geolocation(ジオロケーション)	上位宛先 すべて表示	- シリアル语う 70AF02A9669A2 システム時間 11:04 Asia/Tokyo システム日村 2019-05-10 孫御時間 0 days 00:22
	名前 レートキ パイト ヒット	サーバー
	10.0.1.1 — 110 кърз — 632 кв 6	Log Server 無効
システム ステータス	52.98.37.34 61 кърз 7 кв 2	Dimension #20
ドットワーク	40.126.12.227 С 7 кърз с 40 кв 3	WatchGuard Cloud ステータス 無効
	162.125.34.129 5 кырз 11 кв 2	
キュリティサフスクリフションサーヒス 羅	40.90.190.179 5 кърз 38 кв 5	再起動
PN	13.107.136.9 4 кырз С 56 кв 3	2677 00 (A
	8.8.8.8 2 кърз 2 кв 5	遍云 20 万 🗸
	52.114.158.50 2 кърз 19 кв 2	外部帯域幅
	40.108.227.49 — 1 кърз 13 кв 1	384 Kbps 386 Kbps
	40.91.74.57 840 bps 9 кв 1	200 KDps 128 Kbps 0 Kbps
		20 分前 現在

初期セットアップは以上で完了です。

機能キーの追加

機能キー(フィーチャーキー)とは、機能を有効にするライセンスキーのことです。

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

ですので、各種設定に入る前に、機能キーをデバイスに追加・更新する手順を解説します²。設定操作には 管理者権限でログインする必要があります。

WatchGuard	Fireware Web UI				ユーザー:admi	. ?	
ダッシュボード	機能丰一						
システム ステータス	概要						
ネットワーク	モデル	T50-W					
ファイアウォール							
セキュリティサブスクリプションサービス	シリアル番号	70AF02A966	9A2				
1212	ソフトウェア エディション	Fireware XTM	1 Pro				
VPN	-						
システム	老名	302d0215027	e586a-40871e2ddda5bb				
情報	機能						
機能中一	機能 🕈		值	有効期限	残り時	8	
NTP	モデル アップグレード		T50-W	なし			
SNMP	Application Control(アプリケー	ション制御)	Enabled	03/17/2022	有効期間	1043日	
WatchGuard Cloud	APT Blocker(標的型攻擊対策)		Enabled	03/17/2022	有効期間	1043日	
管理対象デバイス	認証済みユーザーの総数		500	なし			
ログ記録 診断ログ	Gateway AntiVirus(ゲートウェイアンチウィ ルス)		Enabled	03/17/2022	有効期間	1043日	
グローバル設定	Branch Office VPN トンネル		50	なし			
証明書(C) プロキシの自動構成	Dimension Basic		Enabled	03/17/2022	有効期間	1043日	

左側メニュー <u>システム</u> – <u>機能キー</u> からアクセスします。

機能キーの画面が表示されたら、画面の下方にある [機能キーの更新] ボタンをクリックします。

²機能キーの取得方法は「第二章 初期設定」の「事前準備」の項をご覧ください

機能キーの変	更								
機能キーの夏	「新 機能	キーの削除							
機能キーの取	得								
LiveSecurity を	通じて機能キー	をダウンロー	ドするには	機能キーの取得	l				
☑機能キーの自動同期化を有効化									
☑機能キーが失	通知								

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。

uard				
	Reputation Enabled Defense(レビュテー	Enabled	03/17/2022	
	Firebox 機能キーの追加		×	
	機能キーの内容を下記の領域に貼り付ける			
	Feature: SESSION#200000		^	
	Feature: SSLVPN_USER#50	103WEU2Q2UGD54HB	~	
		ОК	キャンセル(C)	
			03/17/2022	
	BGP ルーティング プロトコル			

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。

WatchGuard	Fireware Web UI				ユーザー:admin	?	
ダッシュボード	機能丰一						
システム ステータス	概要						
ネットワーク	モデル	T50-W					
ファイアウォール							
セキュリティサプスクリプションサービス	シリアル番号	L					
認証	ソフトウェア エディション	Fireware XTM	/ Pro				
VPN							
システム	署名	302d0215027	7e586a-40871e2ddda5bb				
情報	機能						
機能半一	機能 🗘		値	有効期限	残り時間		
	モデル アップグレード		T50-W	なし			
	Application Control(アプリケ-	-ション制御)	Enabled	03/17/2022	有効期間 1	043 日	
		22,000			19707410	_	
WatchGuard Cloud	APT Blocker(標的型攻擊対策)		Enabled	03/17/2022	有効期間 1	.043 日	
管理対象デバイス	認証済みユーザーの総数		500	なし			
ログ記録 診断ログ	Gateway AntiVirus(ゲートウェ ルス)	Gateway AntiVirus(ゲートウェイアンチウィ ルス)		03/17/2022	有効期間 1	.043 日	
グローバル設定	Branch Office VPN トンネル		50	なし			
証明霅(C)	Dimension Basic		Enabled	03/17/2022	有効期期 1	043 日	
プロキシの自動構成	Differision Dasic		LINDICU	00/1//2022		040 L	

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 Firebox に、WebUI で接続してみましょう。

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

パスフレーズは、Wizard で設定した構成パスフレーズを入力し、[ログイン]ボタンをクリックします。

6 4 10.0.1.1	×	+ ~					177		×
\leftrightarrow \rightarrow \heartsuit	the https: htttps: https: https: https: https: https:	//10.0.1.1:8080/			□ ☆	հ≡	h	Ŀ	
WatchGuard			ユーザー名 admin パスフレーズ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	~					

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

WatchGuard	Fireware Web UI	l					ユ ー ザー :	admin ?
ダッシュポード	フロント パネル							S
フロント パネル セキュリティサブスクリプションサービス	トップクライ	イアント				すべて表示	システム	
FireWatch	名前	レートキ		ለተኮ		<u></u>	名前 モデル	T50-W-Kamiyacho46 T50-W
インターフェイス	10.0.1.3	_	203 Kbps		839 кв	31	バージョン	12.4.B589964
トラフィック モニタ							シリアル番号システム時間	70AF02A9669A2 11:04 Asia/Tokyo
ゲートウェイ ワイヤレス コントローラ Geolocation(ジオロケーション)	上位宛先					すべて表示	システム日付 稼働時間	2019-05-10 0 days 00:22
モバイルセキュリティ	名前	レート≎		ለኅኮ		<mark>ዞ</mark> ット	サーバー	
ネットワークディスカバリー	10.0.1.1		110 Kbps		632 кв	6	Log Server	無効
システム ステータス	52.98.37.34	-	61 Kbps		7 кв	2	Dimension	無効
ネットワーク	40 126 12 227		7 Khos		40 KD	3	WatchGuar	rd Cloud
ファイアウォール	40.120.12.227		7 KDps		40 KB	5	ステータス	無効
セキュリティサブスクリプションサービス	162.125.34.129		5 Kbps	_	11 кв	2	雨記道	h
忍証	40.90.190.179	<	5 Kbps		38 кв	5	19/23	30
/PN	13.107.136.9		4 Kbps		56 кв	3		
\$Z₹4	8.8.8.8	_	2 Kbps	_	2 кв	5	過去 20 分	~
	52.114.158.50		2 Kbps	-	19 кв	2	外部帯域幅	
	40.108.227.49	_	1 Kbps	_	13 кв	1	384 Kbps	送偏
	40.91.74.57	_	840 bps		9 кв	1	258 Kbps 128 Kbps 0 Kbps	

20 分前

現在

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

WatchGuard	Fireware We	b UI				ユーザー:admin	?	
ダッシュボード システム ステータス	インターフェイ インターフェイ	(ス (スの構成 混合ル	ノーティング モード	~				
ネットワーク インターフェイス ARP エントリ	インター	フェイス DN	S/WINS					
リンクアグリゲーション VLAN プリッジ ループバック	イン ター フェイ ス☆	名前 (エイリア ス)	種類	IPV4 アドレス	IPV6 アドレス	NIC の構成		
複数 WAN	0	External	External	DHCP		Auto Negotiate		
リンク モニー	1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate		
動的 DNS	2	Optional-1	Disabled			Auto Negotiate		
NAT	3	Optional-2	Disabled			Auto Negotiate		
ルート	4	Optional-3	Disabled			Auto Negotiate		
マルチキャストルーティング	5	Optional-4	Disabled			Auto Negotiate		
ゲートウェイ ワイヤレス コントローラ モデム	6	Optional-5	Disabled			Auto Negotiate		
ワイヤレス	編集							
ファイアウォール セキュリティサプスクリプションサービス 2755	保存							
VPN								
システム								

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

まずは外部インターフェイスから設定しましょう。

該当のインターフェイスを選択して、[編集]をクリックします。

WatchGuard	Fireware We	eb UI			-ב	#— : admin (?)	
ダッシュポード システム ステータス	インターフェ・ インターフェ・	イス イスの構成 混合ル-	-ティング モード	~			
ネットワーク インターフェイス ARP エントリ	インター	フェイス DNS/	WINS				
リンクアグリゲーション VLAN	インター フェイス 🕈	名前 (エイリアス)	種類	IPV4 アドレス	IPV6 アドレス	NIC の構成	
プリッジ	0		External	DHCP		Auto Negotiate]
ルーノハック 複数 WAN	1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate	
SD-WAN	2	Optional-1	Disabled			Auto Negotiate	
リンク モニー	3	Optional-2	Disabled			Auto Negotiate	
動的 DNS NAT	4	Optional-3	Disabled			Auto Negotiate	
ルート	5	Optional-4	Disabled			Auto Negotiate	
動的ルーティング マルチキャスト ルーティング	6	Optional-5	Disabled			Auto Negotiate	
ゲートウェイ ワイヤレス コントローラ モデム	編集						
フィヤレス ファイアウォール	保存						

次頁のように、インターフェイスの詳細を設定できる画面が開きます。
選択したインターフェイスの詳細設定画面になります。

最初にインターフェイス名を設定することができます。

インターフェイス / 編集			
インターフェイス名(エイリ アス)	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	\checkmark	
IPv4 IPv6 tz;	カンダリ 詳細		
構成モード	DHCP	\checkmark	
クライアント名			
ホスト名			
	● IPの自動取得		
	○ この IP アドレスを使用する	3	
	リース時間 8	時間 >]
	DHCP 強制更新を有効化		
共有丰一			
保存キャン	ンセル(C)		

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

たとえば複数 WAN で2ポートの External がある場合、それぞれに External-1、External-2 というエイリア スをつけることができます。³

インターフェイス / 編集		
インターフェイス名 (エイリアス)	External-1	
インターフェイスの説明		
インターフェイスの種類	外部	
IPv4 IPv6 セカンダリ	青羊糸囲	

³ もちろんデフォルトのままでも問題ありません。

固定 IP の設定

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

インターフェイス / 編集
インターフェイス名 (エイリ アス) 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 〜
IPv4 IPv6 セカンダリ 詳細
構成モード 静的 IP ~
IPアドレス 10.0.0.1 / 24
ゲートウェイ 10.0.254 ×
保存 キャンセル(C)

DHCP の設定

構成モードで DHCP を選択するだけです。

インターフェイス / 編集	
インターフェイス名(エイリ アス)	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 ~
IPv4 IPv6 tz	カンダリ 詳細
構成モード	DHCP V
クライアント名	
ホスト名	
	 IP の自動取得
	〇 この IP アドレスを使用する
	リース時間 8 時間 ~
	□ DHCP 強制更新を有効化
共有キー	
保存 キャ	>セル(C)

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 / 編集	
インターフェイス名(エイリ アス)	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 ~
IPv4 IPv6 t	カンダリ 詳細
構成モード	PPP0E V
	 IPの自動取得 この IP アドレスを使用する
ユーザー名	signin@watchguard.com
パスワード	•••••
確認	•••••
	詳細
保存 キャン	>セル(C)

ISP の指定によってはより詳細な設定が必要になることがあります。

[詳細]ボタンをクリックし、ISP 指定の項目を設定してください。

PPPoE 詳細設定				×
接続設定 ● 常にオン				^
PPPoE 初期化の再試行	60	秒		
○ ダイアルオンデマンド				
アイドル タイムアウト	20	分		
再試行設定 □ PPPoE 検出パケットでホスト ☑ 失った PPPoE 接続を検出する LCP エコーの失敗	固有タグを使用 ために、LCP エコ・ 6	要求を使用 試行		ļ
LCP エコーのタイムアウト	10	秒		
 □ 自動再起動が設定された時間 □ □ □ □	(時) 0	(分)		
認証設定				~
		ОК	キャンセル(C)	

DNS/WINS 設定

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

- ゲートウェイアンチウィルスや IPS のシグネチャ更新時の名前解決
- スパムブロッカーサーバーへの問い合わせの際の名前解決
- NTP サーバーを FQDN で設定した際の名前解決
- 拠点間 VPN でドメイン名を使用した場合の名前解決
 - ※ 注意: Firebox 側で DNS リレーは行いません。内部ノードが DNS のサーバーアドレスを Firebox の IP アドレスに指定しても名前解決しませんので注意してください

DNS の設定

を側メニューの<u>ネットワーク</u> - <u>インターフェイス</u>をクリックし、ネットワークインターフェイス画面のインター フェイス一覧を表示します。

DNS サーバーの欄に DNS サーバーのアドレスを入力し、[追加]ボタンをクリックします。するとドメイン名ー 覧に DNS サーバーが追加されます。

下方にある [保存] ボタンをクリックして設定を保存します。

	Fireware Web UI	ユーザー:admin	?	
ダッシュボード	インターフェイス			
システム ステータス	インターフェイスの構成 混合ルーティング モード 🗸			
ネットワーク				
インターフェイス				
ARP エントリ	インターフェイス DNS/WINS			
	DNS (ドメイン名システム) サーバー			
VLAN	ドメイン名			
プリッジ				_
	DNS サーバー \$			
複数 WAN	8.8.8.8			
SD-WAN				
500 E	DNS サーバー 4.4.4.4 × 追加 削除			
NAT	(IPV4 または IPV6 アトレス)			
	DNS 転送			
動的ルーティング	□ DNS 転送を有効化する			
ゲートウェイ ワイヤレス コントローラ	信頼店の、住意、およびJJスダムインダーフェイスを V 選択			
モデム	ドメイン \$ DNS サーバー			
ファイアウォール	追加 編集 削除			
セキュリティサブスクリプションサービス	□ ログ記録の有効化			
器紙				
VPN	WINS (Windows Internet Name Service) サーバー			
*776	WINS サーバー 🌩			
2274				
	WIN5 サーバー 追加 削除			
	Rt			
	14.15			

WINS の設定

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

インターフェイス
インターフェイスの構成 混合ルーティング モード 🗸
インターフェイス DNS/WINS
DNS (ドメイン名システム) サーバー
ドメイン名
DNS サーバー 🗧
8.8.8.8
(IPv4 または IPv6 アドレス)
DNS 転送
□ DNS 転送を有効化する
信頼済み、任意、およびカスタム インターフェイスを 🗸 選択
ドメイン \$ DNS サーバー
追加 編集 削除
□ログ記録の有効化
WINS (Windows Internet Name Service) ± -1
WINS サーバー ≎
10.0.1.220
WINS サーバー 10.0.1.221 × 追加 削除
(IPv4 アドレス)
保存

[保存] ボタンをクリックし、設定を保存します。

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

設定は外部インターフェイス同様、左側メニューの*ネットワーク – インターフェイス*の画面から行ないます。

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

WatchGuard	Fireware We	b UI			-ב	ザー: admin (?)	
ダッシュボード システム ステータス	インターフェィ インターフェィ	イス	-ティングモード	~			
ネットワーク インターフェイス ARP エントリ	インター	フェイス DNS/	WINS				
リンクアグリゲーション VLAN プリッジ	インター フェイス \$ 0	名前 (エイリアス) External	種類 External	IPV4 アドレス DHCP	IPV6 アドレス	NIC の構成 Auto Negotiate	
ループバック 複数 WAN	1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate	
SD-WAN	2	Optional-1	Disabled			Auto Negotiate	

Trusted インターフェイスの設定

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

ここでは Trusted-1 というインターフェイス名を付けています。

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

インターフェイス / 編集				
インターフェイス名(エ 〕	イリ アス)			
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		\checkmark	
IPv4 IPv6	セカンダリ	MAC アクセス制御	詳細	
IP アドレス 10.0.1.1	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、インターフェイスの設定画面の中央 にあるドロップダウンリストから、「DHCP サーバー」を選択します。

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

例ではセグメント4オクテット目の1xxのIPアドレスをクライアントに割り当てる設定をしています。

DHCP サーバー V	
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	
10.0.1.2 10.0.1.254	
追加 編集 削除	
アドレス範囲の追加	×
開始 IP 10.0.1.100	
終了 IP 10.0.1.128	×
ок	キャンセル(C)

追加すると一覧に表示されます

アドレス ブール		
	開始 IP 💲	終了 IP
10.0.1.100		10.0.1.199
追加 編集	削除	

さらに、クライアントは IP アドレスだけでなく名前解決も必要なので、DNS サーバーの情報も配布します。 (次頁) 「DHCP サーバー」のドロップダウンリストの下の[DNS/WINS]のタブをクリックします。

インターフェイス / 編集			
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	~	
IPv4 IPv6 セカ	ンダリ MAC アク	セス制御 詳細	
IP アドレス 10.0.1.1	/ 24		
DHCP サーバー	\checkmark		
設定 DNS/WINS			

DNS サーバー (定義されていない場合は、ネットワーク DNS サーバーを使用してください)

ドメイン名	
DNS サーバー 💲	
DNSサーバー	追加
削除	

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。

設定 <u>DNS/WINS</u>
DNS サーバー (定差されていない場合は、ネットワーク DNS サーバーを使用してください)
ドメイン名
DNS サーバー \$
DNS サーバー 8.8.8.8 ×
追加

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
ドメイン名	
DNS サーバー	÷
8.8.8.8	
8.8.4.4	
DNS サーバー	追加
肖耶余	

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

保存

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

例として 2,3番のインターフェイスをブリッジとして構成しましょう。

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

インターフェ・	イス				
インターフェー	イスの構成 混合ルー	ティング モード	\sim		
インター	-フェイス DNS/V	VINS			
インター フェイスキ	名前 (エイリアス)	種類	IPV4 アドレス	IPV6 アドレス	NIC の構成
0	External	External	DHCP		Auto Negotiate
1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate
2	Optional-1	Disabled			Auto Negotiate
3	Optional-2	Disabled			Auto Negotiate
4	Optional-3	Disabled			Auto Negotiate
5	Optional-4	Disabled			Auto Negotiate
6	Optional-5	Disabled			Auto Negotiate
編集					

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

インターフェイス / 編集	
インターフェイス名 (エイリアス)	Trusted-2
インターフェイスの説明	
インターフェイスの種類	
保存 キャンセル(C)	

無効だったインターフェイスが、次のようにブリッジに変更されました。

混合ルーティング モード インターフェイスの構成 \sim インターフェイス 13 IPV4 アドレス IPV6 アドレス 名前 (エイリアス) 種類 NIC の構成 DHCP 0 External External Auto Negotiate Trusted Trusted 10.0.1.1/24 1 Auto Negotiate Trusted-2 3 Optional-2 Disabled Auto Negotiate Optional-3 Disabled 4 Auto Negotiate Optional-4 Disabled 5 Auto Negotiate 6 Optional-5 Disabled Auto Negotiate 編集



インターフェイス

残りのインターフェイスも同じように設定していきます。

以上で指定のインターフェイスをブリッジとして設定できました。

インターフェイス

インターフェ	イスの構成 混合	ルーティング モード	~		
インター	-717 DN	IS/WINS			
イン ター フェイ ス \$	名前 (エイリア ス)	種類	IPV4 アドレス	IPV6 アドレス	NIC の構成
0	External	External	DHCP		Auto Negotiate
1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate
2	Trusted-2	Bridge			Auto Negotiate
3	Trusted-3	Bridge			Auto Negotiate
4	Optional-3	Disabled			Auto Negotiate
5	Optional-4	Disabled			Auto Negotiate
6	Optional-5	Disabled			Auto Negotiate
拒 隹					
ग्धाःसः					
保存					

次にブリッジを定義します。左側メニュー <u>ネットワーク</u> - <u>ブリッジ</u>より、ブリッジの構成画面を開きます。 [追加]ボタンをクリックし、ブリッジを追加しましょう。

WatchGuard	Fireware Web UI	ユーザー:admin	?
ダッシュボード	プリッジ		
システム ステータス	使用可能なブリッジ インターフェイス		
ネットワーク インターフェイス ARP エントリ リンクアグリゲーション	名前 (エイリアス) Trusted-2 Trusted-3 構成		
VLAN	ブリッジの設定		
プリッジ	名前 シ リーン IPV4 プ	アドレス IPV6 アドレス インターフェイス	
ループバック 複数 WAN	追加 編集 削除		
SD-WAN			

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。



ブリッジ / ブリッジの設定の追加

選択したブリッジ インターフェイスのトラフィックの選択および受信

プ リッ ジ◆	インターフェース名	インターフェイス番号	
	Trusted-2	2	ブリッジになるインターフェイ
	Trusted-3	3	スをチェックします
	保存 キャンセル(C)		

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 カします。そしてブリッジにするインターフェイスにチェックを入れます。

以上で保存してください。

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

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

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

ブリッジでも Trusted インターフェイスで設定したように DHCP サーバーを構成することができます。 (次頁) 先程はブリッジの設定タブで設定作業をしましたが、その横の DHCP タブに移り、DHCP モードで「DHCP サーバー」を選択します。

IP アドレスプールを指定します。[追加]ボタンをクリックします。

ブリッジ / ブリッジの設定の追加	1		
ブリッジの設定 DHCR	セカンダリ	IPv6 ブリッジプロトコル	
DHCP モード	DHCP サーバー	×	
ドメイン名			
リース時間	8	時間 🗸	
アドレスプール			
開始 IP \$		終了 IP	
追加 編集 削除			

アドレス範囲の開始と終了 IP を入力し、[OK]をクリックします。

1		Х
10.1.1.100		
10.1.1.199	×	
	ок ++	・ンセル(C)
	10.1.1.100	10.1.1.100 10.1.1.199 ×

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

ブリッジ / ブリッジの設定の追加

<u>ブリッジの設定</u>	DHCP	セカンダリ	IPv6	ブリッジプロ	⊐ト⊐ル		
DHCP E	-r Dh	CP サーバー		\checkmark			
ドメイ	ン名						
リース	時間 8			時間	\sim		
アドレスプール							
開始 IP 💲				終了 IP			
10.0.1.100			1	10.0.1.199			
追加 編集 削除							
IP アドレス 🗧		予約名			MAC AD	DRESS	
追加 編集 削除							
DNS サーバー							
DNS サーバー 💲							
10.100.100.101							
10.100.100.102	× 追加	1 削除					

最後に[保存]ボタンをクリックし、設定を反映させます。

アドレスプール

開始 IP \$	終了 IP	
10.0.1.100	10.0.1.199	
<u>追加</u> 編集 削除 予約済みアドレス		
IP アドレス ◆ 予約名	MAC ADDRESS	
追加 編集 削除		
DNS サーバー		
DNS サーバー 💲		
10.100.101		
10.100.100.102		
追加削除		
WINS サーバー		
WINS サーバー 💲		
<u>追加</u> 削除 DHCP オプション		
□-ド ◆ 名前 種類 種類	値	
追加 編集 削除		
 既定のゲートウェイ ● インターフェイス IP アドレスを使用する ○ IP アドレスを指定する 		

DMZを設定する

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

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

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

インターフェイス					
インターフェイスの	湖城 混合ルーティングモー	К ∨			
インターフェ	イス DNS/WINS				
インターフェ イスキ	名前 (エイリアス)	種類	IPV4 アドレス	IPV6 アドレス	NIC の構成
0	External	External	DHCP		Auto Negotiate
1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate
2	Trusted-2	Bridge			Auto Negotiate
3	Trusted-3	Bridge			Auto Negotiate
4	Optional-3	Disabled			Auto Negotiate
5	Optional-4	Disabled			Auto Negotiate
6	Optional-5	Disabled			Auto Negotiate
編集					

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

インターフェイス名と IP アドレスを設定しましょう

インターフェイス / 編集		
インターフェイス名 (エイリ アス)	DMZ	
インターフェイスの説明		
インターフェイスの種類	任意	\checkmark
IPv4 IPv6 tz	カンダリ MAC アクセス制御	〕 詳細
IPアドレス 10.0.4.1	/ 24	
DHCP を無効にする	~	
保存 キャン	>セル(C)	

ここまでの設定でインターフェイスは以下のようになりました。

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

編集

NAT 設定 (1-to-1NAT)

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

左側メニュー <u>ネットワーク</u> → <u>NAT</u> 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	NAT	
システム ステータス	動的 NAT	
ネットワーク	動的 NAT では、パケットの発信元 IP を書き換えることで、送信インターフ	ェイスの IP アドレスを使用します。
インターフェイス	発信元 ◆	送信先
ARP エントリ	192.168.0.0/16	Any-External
リンクアグリゲーション	172.16.0.0/12	Any-External
VLAN	10.0.0.0/8	Any-External
<i>ว</i> ีป _ั งชั	10.0.0/0	
ループバック	治100 XIII9 上/一轮前 丁/一轮前	
複数 WAN	1月1日本 1日本 1日本 1日本 1日本 1日本 1日本 1日本 1日本 1日本	
SD-WAN	1 - 1 NAT	
リンクモニー	いい・ 1 - 1 NAT は 1 つの IP アドレスの範囲に送信されたパケットを書き換え、別	のアドレス範囲にリダイレクトします。
動的 DNS NAT	インターフェイス \$	ホストの数
ルート 動的ルーティング	追加 編集 削除	
マルチキャストルーティング	保存	
ゲートウェイ ワイヤレス コントローラ		

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



保存をクリックすると 1-to-1 NAT の一覧に追加されます。

NAT

動的 NAT

動的 NAT では、パケットの発信元 IP を書き換えることで、送信インターフェイスの IP アドレスを使用します。

発信元 🗣	送信先		ソース IP	
192.168.0.0/16	Any-External			
172.16.0.0/12	Any-External			
10.0.0/8	Any-External			
追加 削除 上に移動 下に 1-1 NAT	移動			
1 - 1 NAT は 1 つの IP アドレスの範囲に	送信されたパケットを書き換え、別のフ	アドレス範囲にリダイレクト	します。	
インターフェイス 🗢	ホストの数	NAT ペース	実ペース	
External	1	10.168.5.243	10.0.4.110	
追加編集 削除				

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

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

を側メニューの <u>ファイアウォール</u> – <u>ファイアウォールポリシー</u> をクリックし、ポリシーの[追加]ボ タンをクリックします。

ダッシュボード	ポリシ	/-									
システムステータス	70	フション・	7	ポリシーの追加						5	マイルタ なし ・
ネットワーク			7								
ファイアウォール										100	GEOLOCATIO
ファイアウォール ポリシー		Ral R≩≜			種類	発信元	送信先		SD-WAN	CONTROL	オロケーショ タグ
Mobile VPN IPSec ポリシー											>)
エイリアス			>								
プロキシ アクション		1	0	FTP-proxy	FTP-proxy	Any-Trusted, An	Any-External	tcp:21		Global	Global
コンテンツ アクション		2	07	HTTP-proxy	HTTP-proxy	Any-Trusted, An	Any-External	tcp:80		Global	Global
TLS プロファイル	_		~				12 12 12 12				20 x 12
トラフィック管理		3	0	HTTPS-proxy	HTTPS-proxy	Any-Trusted, An	Any-External	tcp:443		Global	Global
スケジューリング		4	10	WatchGuard	WG-Cert-Portal	Any-Trusted, An	Firebox	tcp:4126			Global
SNAT		5	10	WatchGuard	WG-Fireware-X1	Any-Trusted, An	Firebox	tcp:8080			Global
既定のパケット処理				~							
ブロックされたサイト		6	~ 0	(g))Ping	Ping	Any-Trusted, An	Any	ICMP (type: 8,		Global	Global
フロックされたホート		7	10	DNS	DNS	Any-Trusted, An	Any-External	tcp:53 udp:53		Global	Global
クオーダ		8	/0	WatchGuard	WG-Firebox-Mg	Any-Trusted, An	Firebox	tcp:4105 tcp:41			Global
24197197299999999-62	-	0		Outaoina	TCP-UDP	Any-Trusted An	Any-External	top:0.udp:0		Global	Global
1311		-	v 10	eneoutgoing		Any masted, An	any external	copie adpie		0.000	010001
VPN	ポリ	ノシー自動	順序指定	キードを無効にする	5						
システム	ポリシ	ノー チェッ	カーを表	長示する							

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

ファイアウォール ポリシー / ファイアウォール ポリシーの追加

ポリシーの種類を選択する							
◉ パケットフィルタ	НТТР	•					
◎ プロキシ	プロキシを選択します	٣	プロキ	テシ アクシ	ションを道	醒択	*
カスタム	Select a policy type	٣	追加	編集	削除		
ポート 🕈	プロトコル						
80	ТСР						
HTTP パケット フィルタを使用し に適用されることはありません。 リシーを使用します。WatchGua サーバーのみに許可することを推 す。WatchGuard はこれらのパめ 信 HTTP 接続が拒否された時はい に追加するように、Firebox を設	しても、HTTP プロキシのルールセットが任 HTTP トラフィックをプロキシするには、 ard は、受信 HTTP を Firebox の配下にある 課します。 外部ホストはなりすましである rットが正しい場所から送信されたことを確 いつでも、ソース IP アドレスを [ブロックさ 定することができます。 通常のログオプショ	意のトラ HTTP プ パブリッ 部できま れたサイ ョンのす	フィック ロキシポ クHTTP ありま ぜん。 受 イトリスト べては	*			



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

ファイアウォールポリシー / 追	<u>自力口</u>				
名前	HTTP 2	有効化			
設定 SD-WAN	Application Control(アプリケーション制御)	Geolocation(ジオロケーション)	トラフィック管理	スケジューリング	詳細
接続は 許可	Y	ポリシーの種類 HTTP ポート☆ プロトコル 80 TCP			
Any-Trusted	(¥E⊈ ▲ &Any-External			
追加 削除		追加削除			

☑ Intrusion Prevention を有効にする

設定が済んだら接続テストをしてみましょう。

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

(← (=) (≦) http://10.168.5.243/ (> ~ ℃) (≦) NATのテスト	×	6 🖒 😳
DMZ		
このページはDMZに設置されているWebサーバーです。		
ExternalからHTTP接続してこのページが表示されているなら、		
NATは正常に設定されています。		
		€ 100% ▼

この他に、ポートフォワーディングも可能な SNAT (Static Nat)の設定もあります。 こちらはファイアウォールの章で取り上げます。

ルーティング設定

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

その場合、明示的にルートを設定する必要があります。



左側メニュー <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。

ダッシュボード	ルート			
システムステータス	ルート ≎	グートウェイ	メトリック	インターフェイス
ネットワーク	追加 續集 削除	インポート(1) エクスポート		
インターフェイス	AELOH WENC DOPA			
ARPエントリ	ROVAN 仮相インターフェイフ	に対してリートをインポート/エクフポートできま	=++ 4	
リンクアグリゲーション	BOVEN 1024 29-214X			
VLAN				
プリッジ	保存			
ループバック				
複数 WAN				
SD-WAN				
リンクモニー				
動的 DNS				
NAT ルート 動的ルーティング				
マルチキャストルーティング				
ゲートウェイ ワイヤレス コントローラ				
モデム				
ワイヤレス				

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	トの種類	静的ルート	$\overline{\mathbf{v}}$	
宛分	もの種類	ネットワーク IPv4		_
13	ルート先	192.168.111.0	/ 24	
ゲー	-トウェイ	10.0.1.254	×	
	メトリック	1],	

[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。

ルートキ ゲートウェイ メトリック インターフェイス 192.168.111.0 10.0.1.254 1 道加 編集 削除 インボート(I) エクスボート	ルートキ ゲートウェイ メトリック インターフェイス 192.168.111.0 10.0.1.254 1 追加 編集 削除 インボート(I) エクスボート SOVPN 仮想インターフェイスに対してルートをインボート/エクスボートできません	レート			
192.168.111.0 10.0.1.254 1 追加 編集 削除 インポート(I) エクスポート	192.168.111.0 10.0.1.254 1 追加 編集 削除 インボート(I) エクスボート BOVPN 仮想インターフェイスに対してルートをインボート/エクスポートできません	ルートキ	グートウェイ	አኮሀック	インターフェイス
追加 編集 削除 インボート(I) エクスボート	追加 編集 削除 インポート(I) エクスポート BOVPN 仮想インターフェイスに対してルートをインポート/エクスポートできません	192.168.111.0	10.0.1.254	1	
	BOVPN 仮想インターフェイスに対してルートをインポート/エクスポートできません	追加 編集 削除 -	(ンポート(I) エクスポート		
	OVPN 仮想インターフェイスに対してルートをインボート/エクスポートできません				
		保存			

pingを実行して、ルートを追加したネットワークに疎通すれば OK です。



第四章 ファイアウォールの設定

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

ファイアウォールとしての観点から、ポリシー設定画面をあらためて解説します。

ポリシー設定画面

画面構成

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

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

ダッシュボード システムステータス	ポリシー	- ション ・	ポリシー	の追加		ポ	ノシーー	覧			フィルタ なし	×
ネットワーク ファイアウォール	•	顧序 💲	アクション	ポリシー名	種類	発伝元	送后先	<i>ж</i> -ь	SD-WAN	APP CONTROL	GEOLOCATION(ジオ ロケーション)	91
ファイアウォールポリシー		1	0 60	TTP-proxy	FTP-proxy	Any-Trusted, Any-Optior	Any-External	tcp:21		Global	Global	
Mobile VPN IPSec ポリシー エイリアス	8	2	0.00	HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Optior	Any-External	tcp:80		Global	Global	
プロキシ アクション		3	~	ST HTTP	HTTP	Any-Trusted	Any-External	tcp:80			Global	
コンテンツアクション	•	4	0 60	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Optior	Any-External	tcp:443		Global	Global	
TLS プロファイル トラフィック管理	•	5	V	WatchGuard Certifica	WG-Cert-Portal	Any-Trusted, Any-Option	Firebox	tcp:4126			Global	
スケジューリング		6	~	WatchGuard Web UI	WG-Fireware-XTM-Webl	Any-Trusted, Any-Optior	Firebox	tcp:8080			Global	
SNAT		7	V 601	Sybing	Ping	Any-Trusted, Any-Optior	Any	ICMP (type: 8, code: 2		Global	Global	
既定のパケット処理 ブロックされたサイト	0	8	√ 60 €	DNS	DNS	Any-Trusted, Any-Optior	Any-External	tcp:53 udp:53		Global	Global	
ブロックされたポート	•	9	10	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optior	Firebox	tcp:4105 tcp:4117 tcp:			Global	
クォータ		10	1000	Outgoing	TCP-UDP	Any-Trusted, Any-Option	Any-External	tcp:0 udp:0		Global	Global	
セキュリティサブスクリプションサービス 認証 VPN	ポリ	シー自動順序 - チェッカ-	¥指定モート→	を無効にする								

ポリシーー覧の各カラムの意味は以下のとおりです。

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

ポリシーの変更/追加/保存

ポリシーの新規追加は、ポリシーの追加 ボタンをクリックします。

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

<u>ポリシーの追加</u>

ポリシ	/- /ション▼	7	パリシーの述れ]					フィリ	レタ なし *
-	順序≑			種類	発信元	送信先		SD-WAN	APP CONTROL	GEOLOCATIO オロケーショ タグ ン)
•		00	🔄 FTP-proxy						Global	Global
	2	00	HTTP-proxy	HTTP-proxy	Any-Trusted, Ar	Any-External	tcp:80		Global	Global
	3	~	Р ТТР	НТТР	Any-Trusted	Any-External	tcp:80			Global
	4	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Ar	Any-External	tcp:443		Global	Global
	5	√0	WatchGuard	WG-Cert-Portal	Any-Trusted, Ar	Firebox	tcp:4126			Global
	6	√●	WatchGuard	WG-Fireware-X	Any-Trusted, Ar	Firebox	tcp:8080			Global
	7	√ 👩	Ping	Ping	Any-Trusted, Ar	Any	ICMP (type: 8,		Global	Global
	8	√ ि	DNS	DNS	Any-Trusted, Ar	Any-External	tcp:53 udp:53		Global	Global
	9	√●	WatchGuard	WG-Firebox-Mg	Any-Trusted, Ar	Firebox	tcp:4105 tcp:4			Global
	10	10	Cutgoing	TCP-UDP	Any-Trusted, Ar	Any-External	tcp:0 udp:0		Global	Global

ポリシー自動順序指定モードを無効にする

ポリシー チェッカーを表示する

ポリシーの編集・削除

ポリシ	-											
アク	ション	7	リシーの	追加						フィ	ルタ なし	,
ポ ポ タ	リシーの リシーの グをポリ	編集 削除 シーに追		8	種類	発信元	送信先	ポート	SD-WAN	APP CONTROL	GEOLOCATIO オロケーショ タグ ン)	7
9	グをポリ	シーから	削除 ▹ ᠈-		FTP-proxy	Any-Trusted, Ar	Any-External	tcp:21		Global	Global	
			r:	P-proxy	HTTP-proxy	Any-Trusted, Ar	Any-External	tcp:80		Global	Global	
9	グを管理		FF	P	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	4	00	🔶 НТТІ	PS-proxy	HTTPS-proxy	Any-Trusted, Ar	Any-External	tcp:443		Global	Global	
	5	10	Wato	chGuard	WG-Cert-Portal	Any-Trusted, Ar	Firebox	tcp:4126			Global	
	6	10	● Wato	chGuard	WG-Fireware-X	Any-Trusted, Ar	Firebox	tcp:8080			Global	
	7	10	Ping		Ping	Any-Trusted, Ar	Any	ICMP (type: 8,		Global	Global	
	8	√ ि	DNS		DNS	Any-Trusted, Ar	Any-External	tcp:53 udp:53		Global	Global	
	9	~	● Wato	chGuard	WG-Firebox-Mg	Any-Trusted, Ar	Firebox	tcp:4105 tcp:4	E		Global	
	10	√ 💿	Outg	joing	TCP-UDP	Any-Trusted, Ar	Any-External	tcp:0 udp:0		Global	Global	

ポリシー自動順序指定モードを無効にする

ポリシー チェッカーを表示する

ポリシーの編集、もしくは削除をクリックします。

ポリシーの追加

それでは実際にポリシーを追加してみましょう。

ポリシー追加 (内側から外側へ)

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。[ポリシーの追加]ボタンをクリックします。

※ デフォルトでは「Outgoing」ポリシーがあるため、HTTP の許可ポリシーがなくても Web の閲覧はできま す。もし Outgoing を無効にして、許可する通信を手動で設定する場合などに必要です。

アク	ション・	7	「リシーの追加						フィ	ルタ なし
	順序≑			種類	発信元	送信先		SD-WAN	APP CONTROL	GEOLOCATIO オロケーショ タグ ン)
		00	C FTP-proxy						Global	
D	2	00	HTTP-proxy	HTTP-proxy	Any-Trusted, Ar	Any-External	tcp:80		Global	Global
	3	~	9 НТТР	НТТР	Any-Trusted	Any-External	tcp:80			Global
	4	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Ar	Any-External	tcp:443		Global	Global
	5	√●	WatchGuard	WG-Cert-Portal	Any-Trusted, Ar	Firebox	tcp:4126			Global
	6	√⊜	WatchGuard	WG-Fireware-X	Any-Trusted, Ar	Firebox	tcp:8080			Global
	7	√ 6	Ping	Ping	Any-Trusted, Ar	Any	ICMP (type: 8,		Global	Global
0	8	10	DNS	DNS	Any-Trusted, Ar	Any-External	tcp:53 udp:53		Global	Global
	9	√●	WatchGuard	WG-Firebox-Mg	Any-Trusted, Ar	Firebox	tcp:4105 tcp:4	E		Global
	10	10		TCP-UDP	Any-Trusted, Ar	Any-External	tcp:0 udp:0		Global	Global

ポリシー チェッカーを表示する

ポリシーの種類を選択します。

O NO OF JAILO	HTTP	Y	
○ ブロキシ ○ カスタム	プロキシを選択します Select a policy type	 ▼ブロキシアクションを選択 ▼ 追加 編集 削除 	Ŧ
ポート \$ 80	プロトコル TCP		

送信元と送信先を指定します。今回は内側から外側への許可ポリシーなのでデフォルトのままで結構です。 基本的には、ポリシーの設定項目は、どのプロトコルが許可/拒否か、どこから(From)どこに(To)対する ルールかを明示します。最後に設定を反映させるため、下方にある「保存]ボタンをクリックします。



WebUI ではポリシー名は変更できませんのでご注意ください。(もちろん WSM からなら変更できます)

設定が保存されるとポリシー一覧に戻ります。

設定したポリシーが表示されていることを確認してください。

ポリシ	_										
アク	ション・	ボ	リシーの追加						7	フィルタ なし	٣
-	順序≑	ア ク シ ョ ン	ポリシー名	種類	発信元	送信先	ボート	SD-WAN	APP CONTROL	GEOLOCATION オロケーショ タイ ン)	ġ
	1	00	FTP-proxy	FTP-proxy	Any-Trusted, Any	Any-External	tcp:21		Global	Global	
	2	00	HTTP-proxy	HTTP-proxy	Any-Trusted, Any	Any-External	tcp:80		Global	Global	
	3	10	9 // НТТР	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	4	√⊜	State of the second sec	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	5	0	🟓 HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any	Any-External	tcp:443		Global	Global	
	6	~	WatchGuard C	WG-Cert-Portal	Any-Trusted, Any	Firebox	tcp:4126			Global	
	7	√●	WatchGuard W	WG-Fireware-XT	Any-Trusted, Any	Firebox	tcp:8080			Global	

ポリシー追加 (外側から内側へ)

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

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

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

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

◎ バケットフィルタ	HTTP	٣			
○ ブロキシ	プロキシを選択します	×	プロキシアク	フションを選択	
) カスタム	Select a policy type	Ŧ	追加 編集	削除	
ポート \$ 80	プロトコル TCP 期日しても、HTTP プロキシのルールセット	∽が任意のトラ	シブィック		
ITTP パケット フィルタを		-/+ UTTD 7	「ロキシ ポ		

送信元は Any-External、送信先は Web サーバーなので、送信元の Any-Trusted を削除します。名前は 分かりやすいものをつけます。すでに同じ HTTP で内→外のポリシーを追加したので、外→内は HTTP-Incoming など区別がつくように命名するとよいでしょう。

ファイアウォール	ルポリシー / ;	追加						
	名前	HTTP-incoming	☑ 有効化					
設定	SD-WAN	Application Control(アプリケーション制御) Geolocatio	on(ジオロケーション)	トラフィック管理	スケジューリング	詳細	
接続は	許可	v	ポリシーの種類 ポート ♠ 80	HTTP לובאם איבור באויי דכף				
登伝元 Any-Truste	ed		XGt ↑ Any-Extern	゚゚゚ <mark>゚</mark> b サーバ-	ーを指定す	るので、今ま	あるもの	を削除し
Salit Drait			追加 削除					

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

[追加]ボタンをクリック

メンバーの種類	エイリアス	•	
	Any		
	Firebox		
	Any-Trusted		
	Any-Optional Any-BOVPN		
	External	*	

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

ファイアウォール ポリシー / 👔	自加				
名前	HTTP-incoming	☑ 有効化			
設定 SD-WAN	Application Control(アプリケーション制徒	印) Geolocation(ジオロケーション)	トラフィック管理	スケジューリング	詳細
接続は 許可	٣	ポリシーの種類 HTTP ポート * プロトコル 80 TCP			
発信元 🛊		☆ 厚生 ▲			
追加 削除		iê.bu iink			

削除したら新しい送信先を追加します。[追加]ボタンをクリックします。

メンバーの追加画面では、メンバーの種類にホスト IPv4 を選択します。

メンバーの追加		×
メンバーの種類	市スト IPv4	•
ſ	<u>ま (リフス</u> ホスト IPv4	
聚信元 1 梁Any-External	ホスト範囲 IPv4 ホスト範囲 IPv6 ネットワーク IPv6 ホスト範囲 IPv6 Firewall ユーザー Firewall グルーブ PPTP ユーザー PPTP グルーブ SSLVPN ユーザー SSLVPN グルーブ トンネル アドレス カスタム アドレス 大級的 NAT)K キャンセル(C) 送信先 ±
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]。

メンバーの追加		×
メンバーの種類	ホスト IPv4 ~ 10.0.0.1	
	ОК	キャンセル(C)

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

送信先 🗘			

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。

設定	SD-WAN	Application Control(アプリケーション制御)	Geolocation(ジオロケーション)	トラフィック管理	スケジューリング	詳細
接続は		許可 >	ポリシーの種類 HTTP ポート ≎ 80	プロトコル TCP		
発信元 ✿	ternal		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

ファイアウォ	ールポリシー /	編集					
	名前	HTTP-Incommin	ng 🗹 i	有効化			
						_	
設定	SD-WAN	Application Con	trol(アプリケーション制御)	Geolocation(ジオロケーション)	トラフィック管理	スケジューリング	詳細
コメント							
Policy addee	d on 2019-08-008	T09:13:17+09:00.					
NAT							
トラフィック	か両方のルールは	三対して有効の場合、	1-t NAT ルールが優先されま	9.			
✓ 1 - 1 NAT	(ネットワーク N	AI 設定で使用 9 る)					
● ネット	フーク NAT 設定を	E 使用する					
0 このポリ	リシーのすべての	トラフィック					
□ 発信元	IP を設定する	0.0.0.0					

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。

ポリシ	_									
アク	ション・	ポ	リシーの追加						5	フィルタなし ~
•	順序≑	ア ク シ ヨ ン	ポリシー名	種類	発信元	送信先	ボート	SD-WAN	APP CONTROL	GEOLOCATIONI オロケーション)
	1	0	FTP-proxy	FTP-proxy	Any-Trusted, Any	Any-External	tcp:21		Global	Global
	2	√●	HTTP-Incomm	HTTP	Any-External	10.0.0.1	tcp:80			Global
	3	0	HTTP-proxy	HTTP-proxy	Any-Trusted, Any	Any-External	tcp:80		Global	Global
	4	0	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any	Any-External	tcp:443		Global	Global
	5	√●	WatchGuard C	WG-Cert-Portal	Any-Trusted, Any	Firebox	tcp:4126			Global
	6	√●	WatchGuard V	WG-Fireware-XTI	Any-Trusted, Any	Firebox	tcp:8080			Global
	7	10	NPing	Ping	Any-Trusted, Any	Any	ICMP (type: 8, co		Global	Global
	8	√ [⊚		DNS	Any-Trusted, Any	Any-External	tcp:53 udp:53		Global	Global
	9	√)	WatchGuard	WG-Firebox-Mgm	Any-Trusted, Any	Firebox	tcp:4105 tcp:411	L		Global
	10	10	Outgoing	TCP-UDP	Any-Trusted, Any	Any-External	tcp:0 udp:0		Global	Global
	11	√●	Allow IKEv2-U	Any	IKEv2-Users (Any	Any	Any			Global

ポリシー追加 (SNAT で外側から内側へ)

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

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

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



SNAT の名前を入力します。何に対する NAT か分かりやすいものがよいでしょう。 名前の入力後、NAT のメンバーを作成するため、SNAT 画面で[追加]ボタンをクリックします。

SNAT / 追加			
名前	WebServer		
記印			
種類	 静的 NAT サーバー負荷分散 		
	SNAT メンバー 🌲		
追加 編集 削除			
保存 キャンセル(C)			

メンバーの追加の画面で、外部 IP アドレスは Any-External、種類は内部 IP アドレスを選択し、ホストは Web サーバーの 10.0.4.110 を入力して[OK]をクリックします。

メンバーの追加	
インターフェイスの IP アド レス	Any-External
種類を選択	内部 IP アドレス *
ホスト	10.0.4.110
	□ 発信元 IP を設定する
	□ 内部ポートを別のポートに設定する 1
	OK キャンセル(C)

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

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

[保存]ボタンをクリックして設定を反映させます。

名前	WebServer		
言兑日月	[
種類	 静的 NAT サーバー負荷分散 		
	SNAT メンバー 🌻	_	
hy-External> 10.0.4.110 追加 編集 削除			

SNAT が追加されました。

SNAT				
NAT ‡;	たはサーノ	(一負荷分散アクジ 名前 *	コンを追加、編集または削除します。 種類	說明
WebSer	ver		SNAT	

それでは新しく定義した SNAT をポリシーに適用してみましょう。

HTTP-Incoming ポリシーをクリックして編集します。

-	顧序拿	ア ク ション	ポリシー名	種類	発信元	送信先	ボート	SD-WAN	арр Control	GEOLOCATIO オロケーショ ン)	タヴ
	1	00	FTP-proxy	FTP-proxy	Any-Trusted, Ar	Any-External	tcp:21		Global	Global	
	2	√⊜	HTTP-incomi	НТТР	Any-External	10.168.5.233	tcp:80			Global]
	3	00	HTTP-proxy	HTTP-proxy	Any-Trusted, Ar	Any-External	tcp:80		Global	Global	
	4	√●	W HTTP	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	5	√⊜	HTTP.Outgoi	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	6	0	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Ar	Any-External	tcp:443		Global	Global	
	7	√●	WatchGuard	WG-Cert-Portal	Any-Trusted, Ar	Firebox	tcp:4126			Global	
	8	√●	WatchGuard	WG-Fireware-X	Any-Trusted, Ar	Firebox	tcp:8080			Global	
	9	√ 👩	Ding	Ping	Any-Trusted, Ar	Any	ICMP (type: 8,		Global	Global	
	10	√ 🔽	DNS	DNS	Any-Trusted, Ar	Any-External	tcp:53 udp:53		Global	Global	
	11	√●	WatchGuard	WG-Firebox-Mg	Any-Trusted, Ar	Firebox	tcp:4105 tcp:4	ŧ.		Global	
	12	√ 👩	Outgoing	TCP-UDP	Any-Trusted, Ar	Any-External	tcp:0 udp:0		Global	Global	

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。

メンバーの追加			×
メンバーの種類	青鉤 NAT	•	
	WebServer		
		~	
		ОК	キャンセル(C)
	1		

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。

ファイアウォール	ポリシー /	編集		
	名前	HTTP-incoming	☑ 有効化	
設定S	D-WAN	Application Control(アプリケーション制御	I) Geolocation(ジオロケーション) トラフィック管理 スケジューリング 詳細	8
接続は	許可	v	ポリシーの理類 HTTP ポート ↑ プロト⊐ル 80 TCP	
発信元 ≜			送信先	
🛠 Any-Externa			<pre>\$\$ 10.168.5.233 \$\$ WebServer (SNAT) Any-External> 10.0.4.110</pre>	
			See Am some	

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。

ポリシ	-									
アク	ション・	ポリ	リシーの追加						フィルタ	なし
•	順 序≑	アク ショ ン	ポリシー名	種類	発信元	送信先	ポート	SD-WAN	APP CONTROL	GEOLOCATION(オロケーション)
	1	0 6	EFTP-proxy	FTP-proxy	Any-Trusted, Any-	Any-External	tcp:21		Global	Global
	2	√●	WHTTP-incoming	HTTP	Any-External	Any-External> 10.0.4.110	cp:80			Global
	3	0 0	HTTP-proxy	HTTP-proxy	Any-Trusted, Any-	Any-External	tcp:80		Global	Global
	4	~0	Р ИТТР	HTTP	Any-Trusted	Any-External	tcp:80			Global
	5	10	HTTP. Outgoing	НТТР	Any-Trusted	Any-External	tcp:80			Global
	6	0	븢 HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-	Any-External	tcp:443		Global	Global
	7	V	WatchGuard Ce	WG-Cert-Portal	Any-Trusted, Any-	Firebox	tcp:4126			Global
	8	~0	HatchGuard We	WG-Fireware-XTM	Any-Trusted, Any-	Firebox	tcp:8080			Global
	9	√ ⊚ (Ping	Ping	Any-Trusted, Any-	Any	ICMP (type: 8, co	1	Global	Global
	10	100	DNS	DNS	Any-Trusted, Any-	Any-External	tcp:53 udp:53		Global	Global
	11	√)	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-	Firebox	tcp:4105 tcp:411	5		Global
	12	100	Outgoing	TCP-UDP	Any-Trusted, Any-	Any-External	tcp:0 udp:0		Global	Global
4										•

テンプレートにないポリシーを追加する

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

その場合、カスタムでテンプレートを作成することができます。

ポリシー一覧で[ポリシーの追加]ボタンをクリックします。

ポリシ	-										
アク	ション・		リシーの追加						5	イルタなし	٣
-	順序拿	アクション	ポリシー名	種類	発信元	送信先	ポート	SD-WAN	APP CONTROL	GEOLOCATION オロケーショ ン)	<i>91</i>
	1	0	FTP-proxy	FTP-proxy	Any-Trusted, Any	Any-External	tcp:21		Global	Global	
	2	00	HTTP-proxy	HTTP-proxy	Any-Trusted, Any	Any-External	tcp:80		Global	Global	
	3	√●	9 /7 НТТР	HTTP	Any-Trusted	Any-External	tcp:80			Global	
	4	√ 🎱	HTTP.Outgoing	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	5	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any	Any-External	tcp:443		Global	Global	
	6	~	WatchGuard C	WG-Cert-Portal	Any-Trusted, Any	Firebox	tcp:4126			Global	
	7	√●	WatchGuard V	WG-Fireware-XTM	Any-Trusted, Any	Firebox	tcp:8080			Global	

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

種類を選択する	
ットフイルタ Calast a peakst filter -	
Delect a packet inter	
+>Select a proxy ▼	•
Select a policy type ▼ 追加 編集 削除	
ポート 🆘 プロトコル	

新しいポリシーの名前を入力します。

そしてプロトコル(ポート番号)を定義するために[追加]ボタンをクリックします。

名前	Internal_Production_System			
ii 兑8月				
種類	💿 パケット フィルタ 🔘 プロキジ	DNS	•	
プロトコル 🄝				
肖·J『余				
ヌム アイドル タイムアウト	の指定 180 秒			

プロトコルを単一ポートで追加します。

種類	[単一ポート]	•
プロトコル	ТСР	•]
サーバーボート	2000	
	〔範囲; 0	-65535

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	ポート範囲	•	
プロトコル	UDP	•	
開始サーバー ポート	2000		
終了サーバー ポート	2010		
		OK ++	ンセル(C)

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。

名前 説明	Internal_Prod_System		
種类則	 パケット フィルタ () プロキシ 	DNS	¥
プロトコル 今 TCP:2000 TCP:2000-2010 3週70 自印家			
Dス3ム アイドル タイムアウト(保存 キャンセル(C)	り指定 180 秒		

これで新しいテンプレートとして登録されます。

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

プロキシを選択します	Ŧ				
			トシアクラ	ションを選択	*
Select a policy type	¥	追加	編集	削除	
Select a policy type					
nternal_Production_System		ר			
		_	1		
	Select a policy type Select a policy type iternal_Production_System	Select a policy type Select a policy type Iternal_Production_System	Select a policy type	Select a policy type ternal_Production_System	Select a policy type ternal_Production_System

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

ポリシーの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。

ファイアウォール ポリシー 名前	/編集 前 HTTP.Outgoing	效化			
設定 SD-WAN	Application Control(アプリケーション制御)	Geolocation(ジオロケーション)	トラフィック管理	スケジューリング	詳細
接続は ファイアウォール ポリシー 名	許可 、 / 編集 前 HTTP.Outgoing 目有	ポリシーの種類 HTTP ポート ◆ 80	プロトコル TCP		
設定 SD-WAN	Application Control(アプリケーション制御)	Geolocation(ジオロケーション)	トラフィック管理	スケジューリング	詳細
接続は	許可 ▼	ポリシーの種類 HTTP ポート ✿ 80	プロトコル TCP	1	

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。

-	順 序 ≎	アク ショ ン	ポリシー名	種類	発信元	送信先	ボート
	1	00	FTP-proxy	FTP-proxy	Any-Trusted, Any-	Any-External	tcp:21
	2	√)	WHTTP-incoming	HTTP	Any-External	Any-External>	tcp:80
	3	00	WHTTP-proxy	HTTP-proxy	Any-Trusted, Any-	Any-External	tcp:80
	4	√0	9 7 НТТР	нттр	Any-Trusted	Any-External	tcp:80
	5	0	HTTP.Outgoing	нттр	Any-Trusted	Any-External	tcp:80
	6	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-	Any-External	tcp:443

ログを記録する

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

ログで確認したい場合は、ログ記録の「ログメッセージの送信」にチェックを入れます。

ファイアウォー	-ル ポリシー / 編集			
	名前 Ping		☑ 有効化	
設定	SD-WAN Application スケジューリング 詳	n Control(アプリケーション) 細	別御) Geolocation(ジオロケーシ	マヨン) トラフィック管理
接続は	許可	▼ ポリシ ポー	ーの種類 Ping ト☆ プロトコル ICMP (type: 8, code: 255)	
発信元 🕈		送信	先 🌻	
🙊 Any-Trus	ted	۵	ny	
R Any-Opti	onal			
追加 削降	ŝ	追加	削除	
 Intrusion P 帯域幅と時 	revention を有効にする 間クォータを有効化する			
 接続を試み 	たサイトを自動的にブロックで	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	2ージの送信 のログ メッセージを送信する			

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

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

運用スケジュールを設定する

指定の時間にのみポリシーが有効となるように、ポリシーの運用スケジュールを設定することができます。 左側メニュー <u>ファイアウォール</u> ー <u>スケジュール</u> をクリックします。

新しいスケジュールを作成するため、[追加]ボタンをクリックします。



週中の日中帯のみ適用したい場合、以下のようにドラッグして緑色に反転させます。 名前にはスケジュールの内容が分かるようなスケジュール名を入力します。

スケジュー	スケジューリング / スケジュールの追加									
スケジュール	設定									
名前Week	名前 Weekday-Daytime						,			
時間	日曜日	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日			
00:00										
01:00										
02:00										
03:00										
04:00										
05:00										
06:00										
07:00		1								
08:00										
09:00										
10:00										
11:00										
12:00										
13:00										
14:00										
16:00										
16:00										
17:00										
18:00										
19:00										
20:00										
21:00										

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

設定したら保存してください。

作成したスケジュールが一覧に載り、その下のスケジュールポリシーで適用したいポリシーにチェックを入 れ、アクションの選択 ドロップダウンリストから、作成したスケジュールを選択します。

	名前 💲			
ays On				
0700-1900				
ekday-Daytime				
加複製編集削除				
ポリシー名	スケジュール設定する			
	フムジョンルジャン			
FTP	Always On			
HTTP-incoming	Always On			
HTTP-Outgoing	Always On			
WatchGuard Web UI	Always On			
Ping	, lways On			
	Always On			
WatchGuard	Always On			
WatchGuard Outgoing	Always on			
WatchGuard Outgoing クションの選択 - 保存 復元	Always Of			
WatchGuard Outgoing クションの選択 、 保存 復元	Always Off			

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

ポリシー名	スケジュール設定する
FTP	Always On
HTTP-incoming	Always On
HTTP-Outgoing	Always On
WatchGuard Web UI	Alwaye On
Ping	Weekday-Daytime
WatchGuard	Always On
Outgoing	Always On

規定のパケット処理

左側メニュー<u>ファイアウォール</u> – <u>規定のパケット処理</u>をクリックします。

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

ダッシュボード	既定のパケット処理		
システムステータス	危険なアクティビティ		
ネットワーク	☑ スプーフィング攻撃の防御		
ファイアウォール	IP ソースルーティングの廃棄		
ファイアウォール ボリシー Mobile VPN IPSec ポリシー	☑ ブロックポートのスキャン	10	destination ports/source IP per second
エイリアス			
プロキシ アクション	IP スキャンをブロックする	10	destination IPs/source IP per second
コンテンツ アクション			
TLSプロファイル	☑ IPSEC フラッド攻撃の防御	1500	packets per second
トラフィック管理			
スケジューリング	☑ IKE フラッド攻撃の防御	1000	packets per second
SNAT		4000	
既定のパケット処理	■ ICMP ノフット以学の防御	1000	packets per second
ブロックされたサイト	✓ SVN フラッド攻撃の防御	5000	packets per second
ブロックされたポート			
クォータ	☑ UDP フラッド攻撃の防御	1000	packets per second
セキュリティサブスクリプションサービス			
認証			
VPN	未処理バケット		
システム	□ 未処理の外部パケットの発信元	P を自動的にブロッ	クする
	□ 接続が無効のクライアントにエラ	ラー メッセージを送	
	分散サービス拒否攻撃の防御		
	☑ サーバー クォータ当たり	100	秒あたりの接続数
	✓ クライアント クォータ当たり	100	秒あたりの接続数
	保存		

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

ブロックされたサイト

ブロ	コックされたサイト	ブロック	されたサイトの例	191
ブロック	クされたサイト			
	ブロックされたサイ	`		
	115.230.126.151			
	115.239.228.4			
	78.23.181.243			
	140.114.70.36			
追加	インポート(I)	エクスポート	削除	
	1.5.11			

ブロックされたポート

左側メニューファイアウォール – <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。

ブロックされたボート	
1	
111	
513	
514	
2049	
6000	
6001	
6002	
6003	
6004	
6005	
7100	
8000	

第五章 UTM の設定

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

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

プロキシポリシーの追加

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

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



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

プロキシアクションの追加

<u>ファイアウォール</u> – <u>Proxy アクション</u> をクリックします。そして、HTTP プロトコルで UTM を有効にしたい 場合は HTTP-Client(事前定義済み)を選択し、[複製]ボタンをクリックします。

ダッシュポード	プロキシ アクション		
システム ステータス	7⊓≢≈,▲	道商	
ネットワーク	HTTP-Client Standard (事前定美语)	HTTP	^
ファイアウォール			
ファイアウォール ポリシー Mobile VPN IPSec ポリシー	HTTP-Server.Standard (爭則定義済) HTTP-Client (事前定義済)	нттр	
ביושד 🧲	Explicit-Web.Standard (爭刖定義済)	Explicit	
プロキシ アクション コンテンツ アクション	HTTP-Server (事前定義済)	нттр	
ヿ゙゙゙゙゙゙゙゙゙ゞプロファイル	Default-HTTP-Client	HTTP	
トラフィック管理	SMTP-Incoming.Standard (事前定義済)	SMTP	
スケジューリング	SMTP-Outgoing.Standard (事前定義済)	SMTP	
SNAT 歴定のパケット処理	SMTP-Incoming (事前定義済)	SMTP	
プロックされたサイト	SMTP-Outgoing (事前定義済)	SMTP	
プロックされたポート	FTP-Client.Standard (事前定義済)	FTP	
クォータ セキュリティサブスクリプションサービス	FTP-Server.Standard (事前定義済)	FTP	
認証	FTP-Client (事前定義済)	FTP	
VPN	FTP-Server(事前定義済)	FTP	
システム	Default-FTP-Client	FTP	
	DNS-Outgoing (事前定義済)	DNS	
	DNS-Incoming (事前定義済)	DNS	
	TCP-UDP-Proxy.Standard (事前定義済)	TCP-UDP	
	TCP-UIP-Proxy (御前字義済) 接載 編集 削除	TCP-UDP	v

Proxy アクションの詳細設定画面になります。

まずはアクションの内容を表わす名前を入力します。

名前を入力したら、下方の[保存]ボタンをクリックして、アクションを保存します。

プロキシアクション / 複製
HTTP プロキシ アクション設定
名前 HTTP-Client-Security ×
説明 Default configuration for HTTP client
HTTP 要求 ▼ HTTP 応答 ▼ Web キャッシュ サーバーの使用 HTTP プロキシの例外 拒否メッセージ (deny message) DLP(情報漏えい対策)
WebBlocker(Webフィルタリング) Gateway AV Reputation Enabled Defense(レピュテーションセキュリティ) プロキシおよび AV アラーム
APT Blocker(標的型攻擊対策)
全般設定
☑ クライアント接続のアイドルタイムアウトを以下 に設定する: 10 分
☑ URL のパス最大長の設定 2048 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記録する
Google、Yahoo、Bing、YouTube などの主要検索エンジンで、SafeSearch を強制することができます。YouTube の強制レベルを選択することもできます。
□ SafeSearch を強制する
YouTube の SafeSearch 強制レベル
□ レポートのログ記録を有効にする
□ このプロキシ アクションを使用するプロキシ ポリシーの診断ログ レベルをオーバーライドする
[このプロキシアクションの診断ログレベル] エラー マ
保存 キャンセル(C)

保存すると、プロキシアクション一覧に戻ります。

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

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

次に、このアクションと紐づいたプロキシポリシーを追加してみましょう。

プロキシポリシーの追加

<u>ファイアウォール</u> – <u>ファイアウォールポリシー</u>からポリシーー覧を表示し、通常のポリシーと同様、 [ポリシーの追加]ボタンをクリックし、ポリシーの追加画面を表示します。

ダッシュボード	ポリシ	-									
システムステータス	PS	ション・	ボ	リシーの追加						フ.	イルタなし ~
ネットワーク			P								
ファイアウォール ファイアウォールポリシー Mobile VPN IPSec ポリシー		順 序¢	ク ショ ン	ポリシー名	種類	発信元	送信先	ボート	SD-WAN	APP CONTROL	GEOLOCATION (ジオロケー タグ ション)
דלטדג		1	00	ETP-proxy	FTP-proxy	Any-Trusted, An	Any-External	tcp:21		Global	Global
プロキシアクション		2	√●	WHTTP-incomir	НТТР	Any-External	Any-External>	tcp:80			Global
コンテンシテンション TLSプロファイル		3	00	HTTP-proxy	HTTP-proxy	Any-Trusted, An	Any-External	tcp:80		Global	Global
トラフィック管理		4	√⊜	9 / НТТР	нттр	Any-Trusted	Any-External	tcp:80			Global
スケジューリング		5	00	HTTP.Outgoin	HTTP	Any-Trusted	Any-External	tcp:80			Global
SNAT 歴定のパケット処理		6	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, An	Any-External	tcp:443		Global	Global
プロックされたサイト		7	~	WatchGuard (WG-Cert-Portal	Any-Trusted, An	Firebox	tcp:4126			Global
ブロックされたポート クォータ		8	√●	ال WatchGuard ا	WG-Fireware-XT	Any-Trusted, An	Firebox	tcp:8080			Global
セキュリティサブスクリプションサービス		9	√ 👩	Ping	Ping	Any-Trusted, An	Any	ICMP (type: 8, c		Global	Global
121E		10	10	DNS	DNS	Any-Trusted, An	Any-External	tcp:53 udp:53		Global	Global
VPN		11	√●	WatchGuard	WG-Firebox-Mgr	Any-Trusted, An	Firebox	tcp:4105 tcp:41			Global
システム		12	10	Cutgoing	TCP-UDP	Any-Trusted, An	Any-External	tcp:0 udp:0		Global	Global
	ボリミ	リシー自動	加字指定 -	Eードを無効にする							

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

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

最後に[ポリシーの追加]ボタンをクリックします。

ファイアウォール ポリシー / ファイ	イアウォール ポリシーの追加					
ポリシーの種類を選択する						
○ パケットフィルタ	-バケット フィルタを選択	\sim				
● プロキシ	HTTP-proxy	~	HTTP-0	Client-Se	curity	\sim
	Select a policy type	\leq	追加	編集	削除	
ボート 🗢	プロトコル					
80	ТСР					
HTTP (ハイパーテキスト転送プロ)	ארבא).					
ポリシーの追加キャンセ	ıμ(C)					

するとファイアウォール設定と同様の、ポリシーの構成画面になります。ポリシー名は分かりやすいものを 任意に入力してください。

ファイアウォールとプロキシの違いは、「プロキシ アクション」タブです。

ファイアウォール ポリシー / 追加				
名前 HTTP-pi	roxy-Outgoing	□有効化		
設定 SD-WAN Applicati スケジューリング	on Control(アプリケーション制御) 詳細	Geolocation(ジオロケーション)	トラフィック管理	プロキシ アクション
接続は	~	ポリシーの種類 HTTP-proxy ポート☆ プロトコル 80 TCP		
発信元 ✿ 餐Any-Trusted		送信先 🛊		
追加削除		<u>追加</u> 削除		
 ☑ Intrusion Prevention を有効にする □ 帯域幅と時間クォータを有効化する 				
□ 接続を試みたサイトを自動的にブロック	フする			
□ カスタム アイドル タイムアウトの指定	180 秒			

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

最後に下方の[保存]ボタンを押してポリシーを追加しましょう。

	タグ 🗢		
編集			

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

プロキシ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。

ポリシ	リシー										
70	ション・	-	ポリシーの追加						5	フィルタなし ~	
•	順 序 \$	ア ク ショ ン	ポリシー名	種類	発信元	送信先	ボート	SD-WAN	APP CONTROL	GEOLOCATIOI (ジオロケー タグ ション)	
	1	0	FTP-proxy	FTP-proxy	Any-Trusted, Ar	Any-External	tcp:21		Global	Global	
	2	√●	HTTP-incomi	НТТР	Any-External	Any-External	tcp:80			Global	
	3	0	HTTP-proxy	HTTP-proxy	Any-Trusted, Ar	Any-External	tcp:80		Global	Global	
	4	00	HTTP-proxy-	HTTP-proxy	Any-Trusted	Any-External	tcp:80			Global	
	5	~	WHTTP	НТТР	Any-Trusted	Any-External	tcp:80			Global	
	6	00	WHTTP.Outgoin	HTTP	Any-Trusted	Any-External	tcp:80			Global	
	7	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Ar	Any-External	tcp:443		Global	Global	
	8	~	WatchGuard	WG-Cert-Portal	Any-Trusted, Ar	Firebox	tcp:4126			Global	
	9	/0	WatchGuard	WG-Fireware-X	Any-Trusted, Ar	Firebox	tcp:8080			Global	
	10	√ [6	MPing	Ping	Any-Trusted, Ar	Any	ICMP (type: 8,	i i	Global	Global	
	11	√ [6		DNS	Any-Trusted, Ar	Any-External	tcp:53 udp:53		Global	Global	
	12	~	WatchGuard	WG-Firebox-Mg	Any-Trusted, Ar	Firebox	tcp:4105 tcp:42	1		Global	
	13	10	Outgoing	TCP-UDP	Any-Trusted, Ar	Any-External	tcp:0 udp:0		Global	Global	

ポリシー自動順序指定モードを無効にする

ポリシー チェッカーを表示する

Web Blocker の設定

WebBlocker はコンテンツフィルタリングの役割をし、業務時間中の無秩序な Web ブラウジングを規制する ことができます。フィルタリング用のデータベースは実績のある FORCEPOINT のものを利用しており、ユー ザーが Web サイトにアクセスしようとしたとき、Firebox はそのサイト情報を照合します。規制対象であれば アクセスをブロックし、警告画面を表示します。

Web Blocker を構成する

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



まずアクション名を入力します。

サーバータブでは、「WebBlocker クラウド」を選択します。

WebBlocker(Webフィルタリング) / WebBlocker アクションの追加								
アクション名 Unrelated with Business								
カテゴリ 例外 詳細 アラーム サーバー(S)								
● V(ebBlocker クラウド								
●オンプレミス WebBlocker Server								
オンプレミス WebBlocker Server を選択するには、まずそれを WebBlocker グローバル設定に追加する必要があります。								
保存 キャンセル(C)								

5

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

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

「サーバータイムアウト」と「ライセンスのバイパス」の設定をご確認ください。

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

WebBlocker(Webフィルタリング) / WebBlocker アクションの追加
アクション名
カテゴリ 例外 詳細 アラーム サーバー(S)
ローカルを優先
□ WebBlocker のローカル優先を有効化する
WebBlocker ローカル優先パスフレーズおよび非アクティブ タイムアウトを指定する
パスフレーズ
確認
非アクティブ タイムアウト 5 分
□ このアクションをログ記録する
サーバー タイムアウト どちらも許可
次の時間内にサーバーに接続できない場合 6 秒 アラーム このアクションをログ記録する
かに ・ ・ ・ ・ い ab サイトの表示を許可する
〇 Web サイトへのアクセスを拒否する \Box アラーム \Box このアクションをログ記録する
ライセンスのハイバス
WebBlocker ライセンスが期限切れの場合、すべてのサイトへのアクセスを 許可
保存 キャンセル(C)

運用方針にもよりますが、これらの設定を「許可」にしておき、WebBlocker サーバーのタイムアウト時やラ イセンス更新を忘れてしまった場合に、業務に影響が出ないように設定を検討してください。

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

アクラ	ション名 unrela	ated with business				
	カテゴリ	例外 詳細 アラー	-ム サーバー(S)			
র	べてのカテゴリる	を マベてのカテゴリ	✓ 検索(S)	2-	イック アクション	•
	アクション	カテゴリ	サプカテゴリ	アラーム	ログ	
	許可	Abortion	Abortion			
	許可	Abortion	Pro-Choice			
	許可	Abortion	Pro-Life			1
	許可	Adult Material	Adult Content			
	許可	Adult Material	Adult Material		\checkmark	
	許可	Adult Material	Lingerie and Swimsuit			
	許可	Adult Material	Nudity			
	許可	Adult Material	Sex			
	許可	Adult Material	Sex Education			
	許可	Advocacy Groups	Advocacy Groups			
	許可	Bandwidth	Bandwidth			
	許可	Bandwidth	Educational Video		\checkmark	
	許可	Bandwidth	Entertainment Video		\checkmark	
	許可	Bandwidth	Internet Radio and TV		\checkmark	
	許可	Bandwidth	Internet Telephony		\checkmark	
	許可	Bandwidth	Peer-to-Peer File Sharing		\checkmark	
-		e 1.10		_	`	1

WebBlocker(Webフィルタリング) / WebBlocker アクションの追加

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

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

Adult Material カテゴリで項目をフィルタします。

	カテゴリ	例外詳細	アラーム	サーバー(S)			
বৃশ	、てのカテゴリを	a 🗸 🖂	al	▲ 検索(3)	クイック アクション・		
	アクション	עבלמ		ערבוורה		アラーム	ログ
	許可	Adult Material		Adult Content			\checkmark
	許可	Adult Material		Adult Material	Adult Material		
	許可	Adult Material		Lingerie and Swimsuit			\checkmark
	許可	Adult Material		Nudity			\checkmark
	許可	許可 Adult Material		Sex	Sex		
	許可	Adult Material		Sex Education			\checkmark

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



すべての Adult Material カテゴリが拒否されます

	カテゴリ	例外	詳細	アラーム	サー	-/(—(S)							
व.	すべてのカデゴリをき ~ Adult Material ~ 検索(S)									クイ	クイック アクション 🗸		
	アクション	カラ	-ゴリ		t	ナブカテゴリ			2	アラーム	ログ		
	拒否	Adult Material			A	Adult Content					\checkmark		
	拒否	Ad	Adult Material			Adult Material							
	拒否	Ad	ult Material		L	Lingerie and Swimsuit							
	拒否	Ad	ult Material		١	ludity							
	拒否	Adult Material			S	Sex					\square		
	拒否	Ad	ult Material		S	Sex Educati	ion				\checkmark		
-													

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。

クション・									
ログ									

一通り設定したら、画面下方にある保存ボタンをクリックし設定を反映させます。

新しい WebBlocker のアクションが登録されました。

WebBlocker(Webフィルタリング)

WebBlocker のアクション

アクシ	'∋>≎				CATEGORIES DENIED	例外	GLOBAL EXCEPTIONS	アラーム	ログ
Defau	lt-WebBl	ocker			21	1	No	0	22
Unrela	Unrelated with Business			6	4	No	0	131	
追加	複製	編集	削除						

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

下の WebBlocker ポリシーに、あらかじめ作成したアクション「HTTP-Client-Security」には何も関連付けら れず「なし」になっています。

アクションの選択のドロップダウンリストで WebBlocker のプロファイル「Unrelated with Business」を指定します。

١	NebBlocker(Webフィルタリング)						
١	WebBlocker のアクション						
	アクション 🕈	CATEGORIES DENIED	例外		GLOBAL EXCEPTIONS	アラーム	D17
	Default-WebBlocker	21 1			No	0	22
	Unrelated with Business	6	4		No	0	131
[追加 複製 編集 削除						
	WebBlocker ポリシー		_				
	■ プロキシアクション	ファイアウォール ボリシー		種類		WEBBLOCKER アク	クション
	Default-HTTP-Client	HTTP-proxy		НТТР		Default-WebBlocker	
	Default-HTTPS-Client	HTTPS-proxy		HTTPS		Default-WebBlocker	
	HTTP-Client-Security	HTTP-proxy-Outgoing		нттр		Unrelated with Business	
	アクションの選択- 保存 復元 なし Default-WebBlocker						
	Unrelated with Business		ta/-				
4	_のフィリードを使用して、ナバイスの WebBlocker	を構成しますウィザードを	美行				

この状態で保存ボタンをクリックし、設定を保存します。

WebBlocker(Webフィルタリング)	VebBlocker(Webフィルタリング)									
WebBlocker のアクション										
アクション 🗘	CATEGORIES DENIED	例外		GLOBAL EXCEPTIONS	アラーム	לים				
Default-WebBlocker	21 1		No		0	22				
Unrelated with Business		4				131				
追加 複製 編集 削除 WebBlocker ポリシー										
プロキシ アクション	ファイアウォール ポリシー		種類		WEBBLOCKER アクション					
Default-HTTP-Client	HTTP-proxy		НТТР		Default-WebBlocker					
Default-HTTPS-Client	HTTPS-proxy		HTTPS		Default-WebBlocker					
HTTP-Client-Security	HTTP-Client-Security HTTP-proxy-Outgoing				Unrelated with Business					
アクションの選択 ▼ 保存 復元										

設定を保存したら、試しにショッピングサイトにアクセスしてみてください。

WebBlocker が機能し、以下のように拒否画面が表示されます。

Request denied by WatchG × +					
🕙 www.rakuten.co.jp	∀ C	Q 楽天	÷	÷	♠
	Request denied by WatchGuard HTTP Prop	xy.			
Reason: Ca	ategory 'Shopping' denied by WebBlocker policy 'Unrelated with	h Business'.			
Please con	tact your administrator for assistance.				
More Detail	s:				
Method: G	ET				
Host: www.	rakuten.co.jp				
Path: /					
	WatchGuard Technologies, Inc.				

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

WebBlocker(Webフィルタリング)

WebBlocker のアクション									
アクション		CATEGORIES DENIED	例外		GLOBAL EXCEPTIONS	アラーム	לים		
Default-WebBlocker	3	21	1		No	0	131		
unrelated with business		0 1		No		0	131		
追加 複製 編集 肖	除								
WebBlocker ポリシー									
■ プロキシアクション	77	ファイアウォール ポリシー				WEBBLOCKE	WEBBLOCKER アクション		
Default-HTTP-Client	HTT	P-proxy		HTTP		Default-WebBl	ocker		
Default-HTTPS-Client	нтт	PS-proxy		HTTPS		Default-WebBl	ocker		
アクションの選択・	存復元								
◆ 設定									
WebBlocker Activation Wi	zard	_							
このウィザードを使用して、デバイスの WebBlocker を構成します ウィザードを実行									
			104						

Gateway AntiVirus の設定

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

Gateway AntiVirus を有効にする

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

その上でメニュー<u>セキュリティサブスクリプションサービス</u> - <u>Gateway AV</u> をクリックします。

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

ダッシュポード	Gateway AV			
システム ステータス	Gateway AntiVirus のアクション			
ネットワーク	プロキシ アクション 💲	ファイアウォール ポリシー	種類	ステータス
ファイアウォール	HTTP-Client.Standard		НТТР	無効 (事前定義済み)
セキュリティサブスクリプションサービス	HTTP-Server.Standard		HTTP	無効 (事前定義済み)
Application Control	HTTP-Client		НТТР	無効 (事前定義済み)
(アプリケーション制御)	Explicit-Web.Standard		Explicit	無効 (事前定義済み)
APT Blocker(標的型攻撃対策) ポットネット検出	HTTP-Server		НТТР	無効 (事前定義済み)
DLP(情報漏えい対策)	Default-HTTP-Client	HTTP-proxy	НТТР	Enabled
DNSWatch Gateway AV	HTTP-Client-Security	HTTP-proxy-Outgoing	нттр	無効
Geolocation(ジオロケーション)	SMTP-Incoming.Standard		SMTP	無効 (爭則正義済み)
IPS(不正侵入検知・防御)	SMTP-Outgoing.Standard		SMTP	無効 (事前定義済み)
モバイルセキュリティ	SMTP-Incoming		SMTP	無効 (事前定義済み)
Quarantine Server	SMTP-Outgoing		SMTP	無効 (事前定義済み)
Reputation Enabled Defense	FTP-Client.Standard		FTP	無効 (事前定義済み)
Reputation Enabled Defense (レビュテーションセキュリティ)	FTP-Client.Standard		FTP	無効 (事前定義済み)
Reputation Enabled Defense (レピュテーションセキュリティ) spamBlocker(述感メール対策) Threat Detection	FTP-Client.Standard		FTP	無効 (事前定義済み)

「Gateway AntiVirus を有効にする」にチェックを入れます。

Gateway AV / HTTP-Client-Sect	urity			
Proxy HTTP-Client-Security				
🖸 Gateway AnitVirus の有効化]			
Gateway AntiVirus 構成				
ウイルスが検出された場合	切断	~ [コアラーム	
スキャン エラーが起こった場合	計可	~ [コアラーム	
コンテンツがスキャン サイズ 制限を超えた場合	許可	~ [コアラーム	
コンテンツが暗号化されてい る場合	許可	~ [コアラーム	
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 you set the Gateway AntiVirus scan limit to higher than 10 MB, APT Blocker analyzes files only up to 10 MB in size.

スキャン サイズの制限		1024	キロバイト
段友	+7	ر ا ت الـ (٦)	
PKIT	モアノビル(い)		

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

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

以上で保存します。GAV は有効になります。

Gateway AntiVirus を設定する

プロキシアクションの一覧に戻ったら、再度、定義したアクションを選択し、今度は[サーバーの更新]ボタン をクリックします。

Gateway AV

Gateway AntiVirus のアクション

プロキシ アクション 🕈	ファイアウォール ポリシー	種類	ステータス
HTTP-Client.Standard		HTTP	無効 (事前定義済み)
HTTP-Server.Standard		НТТР	無効 (事前定義済み)
HTTP-Client		НТТР	無効 (事前定義済み)
Explicit-Web.Standard		Explicit	無効 (事前定義済み)
HTTP-Server		НТТР	無効 (事前定義済み)
Default-HTTP-Client	HTTP-proxy	НТТР	Enabled
HTTP-Client-Security	HTTP-proxy-Outgoing	нттр	Enabled
HTTP-Client-Security SMTP-Incoming.Standard	HTTP-proxy-Outgoing	HTTP SMTP	Enabled 無効 (事前定義済み)
HTTP-Client-Security SMTP-Incoming.Standard SMTP-Outgoing.Standard	HTTP-proxy-Outgoing	HTTP SMTP SMTP	Enabled 無効 (事前定義済み) 無効 (事前定義済み)
HTTP-Client-Security SMTP-Incoming.Standard SMTP-Outgoing.Standard SMTP-Incoming	HTTP-proxy-Outgoing	HTTP SMTP SMTP SMTP	Enabled 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み)
HTTP-Client-Security SMTP-Incoming.Standard SMTP-Outgoing.Standard SMTP-Incoming SMTP-Outgoing	HTTP-proxy-Outgoing	HTTP SMTP SMTP SMTP SMTP	Enabled 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み)
HTTP-Client-Security SMTP-Incoming.Standard SMTP-Outgoing.Standard SMTP-Incoming SMTP-Outgoing FTP-Client.Standard	HTTP-proxy-Outgoing	HTTP SMTP SMTP SMTP SMTP FTP	Enabled 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み) 無効 (事前定義済み)

構成	
サーバーの更新	ファイル例外

Gateway AntiVirus アクティブ化ウィザード

このウィザードを使用して、デバイスの Gatway AntiVirus 設定を構成します ウィザードを実行

GAV の全体的な設定になります。

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

Gateway AV / 署名の更新

自動署名更新		
☑ 自動更新を有効にする		
間隔	1	時間
	 ✓ Intrusion Prevention および Applica ✓ Gateway AntiVirus の署名 □ Data Loss Prevention の署名 	tion Control の署名
	✓ ボットネット検出サイトデータベーフ	z
	☑ Geolocation データベース	
サーバーの更新		
サーバー URL の更新	https://services.watchguard.com]
HTTP プロキシ サーバー		
□ 接続 サーバーの更新 HTTP ブ	ロキシ サーバーを使用	
サーバー アドレス	サーバー アドレス	
		1
サーバーボート	8080	
サーバー認証	なし >	
保存 キャン	rセル(C)	

以上で設定を保存してください。
HTTP ヘッダーやファイルの種類によって GAV をどう適用するかなどの詳細な設定は、プロキシアクション 側で指定します。

メニューのファイアウォール – 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。

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
プロキシ アクション
עבעמיז שעדעב
トラフィック管理
セキュリティサブスクリプションサー
認証
VPN
システム

プロキシ アクション

プロキシ 🕈	種類	
HTTP-Client.Standard (事前定義済)	НТТР	^
HTTP-Server.Standard (事前定義済)	НТТР	
HTTP-Client (事前定義済)	HTTP	
Explicit-Web.Standard (事前定義済)	Explici HTTP	
HTTP-Server (事前定義済)	НТТР	
Default-HTTP-Client	HTTP	
HTTP-Client-Security	нттр	
SMTP-Incoming.Standard (事前定義済)	SMTP	
SMTP-Outgoing.Standard (事前定義済)	SMTP	
SMTP-Incoming (事前定義済)	SMTP	
SMTP-Outgoing (事前定義済)	SMTP	
FTP-Client.Standard (事前定義済)	FTP	
FTP-Server.Standard (事前定義済)	FTP	
FTP-Client (事前定義済)	FTP	
FTP-Server (事前定義済)	FTP	
Default-FTP-Client	FTP	
DNS-Outgoing (事前定義済)	DNS	
DNS-Incoming (事前定義済)	DNS	
TCP-UDP-Proxy.Standard (事前定義済)	TCP-UDP	~



HTTP 応答 - コンテンツの種類

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

プロキシ アクション	/ 編集						
HTTP プロキシア	クション誘	设定					
	名前	HTTP-Client-Se	ecurity				
	説明	Default configu	ration for HTTP client				
HTTP 要求 ▼	HTTP 応答	š▼ Web ≠1	ャッシュ サーバーの使用	HTTP ;	プロキシの例外	拒否メッセージ (deny me	ssage)
DLP(情報漏えい)	全般設定		フィルタリング) G	ateway AV	Reputation Ena	abled Defense(レピュテーシ	ョンセキュリティ)
プロキシおよび			r(標的型攻擊対策)				
全般設定	ヘッダー	フィールド					
✓ クライアント接続	コンテン	ツの種類	10	分			
トに設定9る: VIIIIのパフ長大手	クッキー						
□ 変更されていない	本文コン	テンツの種類	2048	ハイト			
□ このアクション	レをログ記録	する	6				

次の図のように、HTTP 通信のヘッダーで判断できるコンテンツの種類により、一致しないものは拒否、一致するものは AV スキャンをかけるという設定になっています。

ただ、すべてのコンテンツの種類を把握して設定するにも限界がありますので、このドロップダウンリストで 「AV スキャン」を選択するのも現実的です(つまりすべて AV スキャン対象に)。

コンテンツの	の種類						
ENAE 7	クション	名前	マッチタイプ	68	7 5- 4	ロ グ	
	AV スキャン	HTTP-tunnelled RTSP stream types	完全一致	application/x-rtsp- tunnelled			^
	AV スキャン	WatchGuard application types	完全一致	application/x-watchguard- locked			
	AV スキャン	All XML application types	パターン一致	application/*xml*			
	AV スキャン	All application types	パターン一致	application/*			
	AV スキャン	All audio types	パターン一致	audio/*			
	AV スキャン	All font types	パターン一致	font/*			
	AV スキャン	All image types	パターン一致	image/*			
	AV スキャン	All encapsulated message types	パターン一致	message/*			
	AV スキャン	All model types	パターン一致	model/*			
	AV スキャン	All multipart types	パターン一致	multipart/*			~
追加複	製 編集 削除	上に移動 下に移動					

ROULEUNT AV スキャン マログ

保存

キャンセル(C)

HTTP 応答 - 本文のコンテンツの種類

説明

次に同じく HTTP 応答のリストから「本文のコンテンツの種類」をクリックします。

Default configuration for HTTP client



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。

HTTP 要求▼ HTTP 応答▼ Web キャッシュ サーバーの使用 HTTP プロキシの例外 拒否メッセージ (deny message) DLP(情報漏えい対策) WebBlocker(Webフィルタリング) Gateway AV Reputation Enabled Defense(レピュテーションセキュリティ) プロキシおよび AV アラーム APT Blocker(標的型攻撃対策)

本文コンテンツの種類

ENAE アクション		名前	マッチタイプ	G	ア ラー ム	ログ
	拒否	Java bytecode	パターン一致	%0xcafebabe%*		\checkmark
	拒否	ZIP archive	パターン一致	%0x504b0304%*		
	拒否	Windows EXE/DLL	パターン一致	%0x4d5a%*		
	拒否	Windows CAB archive	パターン一致	%0x4d53434600000000%*		

追加 複製 編集 削除 上に移動 下に移動

前記のルールが一致しなかった場合に実行するアクション AV スキャン v ロアラーム ログ しかし、現実的には ZIP ファイルやソフトウェアのインストーラー(.exe)のダウンロードなどが発生しますので、一致する場合もしない場合も AV スキャンを選択しておくとよいでしょう。

Enabl	アクション	名前	マッチタイプ	値	アラー。	ログ
1	AV スキャン	Java bytecode	パターンー致	%0xcafebabe%*		1
	AV スキャン	ZIP archive	パターン一致	%0x504b0304%*		
	AV スキャン	Windows EXE/DLL	パターン一致	%0x4d5a%*		1
	AV スキャン	Windows CAB archive	パターン一致	%0x4d534346000000		1

最後に下方の保存ボタンをクリックして、設定を反映させます。

以上で Gateway AntiVirus の設定が完了しました。

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

Response denied by WatchGuard HTTP Proxy.
Reason: virus matched signature name='EICAR_Test'
Please contact your administrator for assistance.
More Details:
Method: GET
Host: www.eicar.org
Path: /download/eicar.com
WatchGuard Technologies, Inc.

spamBlocker の設定(手動)

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

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

spamBlocker アクティブ化ウィザードを実行して POP-Proxy アクションを追加する

WebBlocker で Proxy ポリシーの HTTP-proxy が必要だったように、spamBlocker では POP3-proxy が必要です。また、それと紐づく Proxy アクションが必要です。では、まずウィザードを実行して Proxy アクションを定義しましょう。トップページから次へをクリックします。



プロクシ―ポリシーから POP3 を選択し、次へをクリックします。

新しいプロキシポリシーの作成	
追加のプロキシ ポリシーを作成する場合、1 つ選択します。	
 □ Incoming SMTP ・ 電子メールサーバー IP アドレス □ POP3 □ IMAP 	
スキップ	戻る次へ

終了をクリックし、spamBlockerのアクションを表示します。

spamBlocker(迷惑メール対策)

変更の保存に成功しました。

spamBlocker アクティブ化ウィザードが完了しました。

[終了] をクリックして、spamBlocker 構成に進みます。



×

spamBlocker(迷惑メール対策)

spamBlocker のアクション

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

次に、このアクションと紐づいたプロキシポリシーを追加してみましょう。

POP3-proxy ポリシーを追加する

ファイアウォール ポリシー / ファイアウォール ポリシーの追加

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* でポリシーー覧を表示し、ポリシーの新規[追加]ボタンをクリックします。

ポリシーの種類の選択画面になりますので、POP3-Proxyを選択します。

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

ポリシーの種類を選択する 〇 パケットフィルタ	-バケット ノイルタを選択	\sim				
◎ プロキシ	POP3-proxy	\sim	POP3-0	Client.Sta	ndard.1	\sim
О カスタム	Select a policy type	\sim	追加	編集	削除	
POP3 ポート 🅈	プロトコル					
110	ТСР					
POP3S ポート 🕈	プロトコル					
995	ТСР					
Post Office Protocol V3 •						

ポリシーの追加

キャンセル(C)

ポリシーの[追加]ボタンをクリックします。

ポリシー構成の画面になるので、画面下の保存ボタンをクリックして保存します。

ファイアウォールオ	ペリシー / 追加					
	名前 POP3-C	lient.Standard.1	☑有	劝化		
設定 SD プ)-WAN Applicat	ion Control(アプリケ- スケジューリング	-ション制御) 詳細	Geolocation(ジオロケ-	-ション)	トラフ・
接続は	許可	~	ポリシーの種類	POP3-proxy		
TLS サポート	Enabled	~	110	тср		
			POP3S ポート	◆ プロトコル		
			995	тср		
発信元 💲			送信先 💲			
Any-Trusted			🙊 Any-Extern	nal		
追加 削除			追加 削除			
Intrusion Preve	ntion を有効にする					

POP3 プロキシポリシーがポリシー一覧に追加されました。

WatchGuard	Firew	are We	eb UI								ユーザー:admin (? (
	ポリシ	2-										
テムステータス	7	クション・	- 7	パリシーの追加						7	イルタ なし	\sim
			7									
アウォール		_									GEOLOCATIO	
		履き			種類	発信元	送信先		SD-WAN	CONTROL	オロケーショ	タヴ
				6 ETT		Anu Trusted Au	Any Determed			Clabel		
シアクション		1	0.0	C PTP-proxy	PTP-proxy	Any-Trusted, Ar	Any-External	tcp:21		Global	Giobai	
		2	~ •	HTTP-Incom	HTTP	Any-External	10.0.0.1	tcp:80			Global	
イック管理		3	00	HTTP-proxy	HTTP-proxy	Any-Trusted, Ar	Any-External	tcp:80		Global	Global	
		4	00	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Ar	Any-External	tcp:443		Global	Global	
		5	/0	WatchGuard	WG-Cert-Portal	Any-Trusted, Ar	Firebox	tcp:4126			Global	
パケット処理		6	/0	WatchGuard	WG-Fireware-X	Any-Trusted, Ar	Firebox	tcp:8080			Global	
ックされにサイト ックされたポート		7		Ping	Ping	Any-Trusted, Ar	Any	ICMP (type: 8.	r.	Global	Global	
		0		ADMC	DNS	Any Trusted Ar	Any External	ton E2 udn E2		Clobal	Clobal	
ティサブスクリプションサービス		0	V 10	-DNS	DINS	Any-Trusted, Ar	Any-External	tcp:55 uup:55		Giobal	Giobai	
		9		POP3-proxy	POP3-proxy	Any-Trusted	Any-External	tcp:110 tcp:99	5		Global	
		10	√)	WatchGuard	WG-Firebox-Mg	Any-Trusted, Ar	Firebox	tcp:4105 tcp:4	t		Global	
		11	√ 💿	Outgoing	TCP-UDP	Any-Trusted, Ar	Any-External	tcp:0 udp:0		Global	Global	
		12	10	Allow IKEv2-	Any	IKEv2-Users (Ai	Any	Any			Global	

spamBlocker を構成する

メニューの<u>セキュリティサブスクリプションサービス</u> – <u>spamBlocker(迷惑メール対策)</u>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。

samelocker(短泉メール)第 5 2 3 2 - 0 - 2 3 2 5 2 5 2 5 2 5 2 5 2 5 2 5 2 5 2 5	WatchGuard	Fireware Web UI			ユーザー:admin (?)
spanBlocker のグククション Totaシ アクション Totav Portav Totav T		spamBlocker(迷惑メール対策)			
トウーク ブロもシアクションナ ブロイアクショント 秋川P 板川 ブブークス パアウィール SMTP-Incoming.Standard SMTP	テムステータス	spamBlocker のアクション			
RPPO+-ル SMTP-Incoming.Standard SMTP 無効(申前定義系か) Rule SMTP-Outgoing.Standard SMTP 服効(申前定義系か) PU/D-253780) SMTP-Outgoing.Standard SMTP 服効(申前定義系か) SMTP-Outgoing.Standard SMTP 医効(申前定義系か) SMTP-Outgoing.Standard POP3 Exb(申前定義系か) SMTP-Outgoing SMTP Exb(申前定義系か) SMTP-Outgoing POP3 Exb(申前定義系か) POP3-Client.Standard POP3 Exb(申前定義系か) POP3-Client.Standard POP3 Exb(申前定義系か) POP3-Client.Standard POP3 Exb(申前定義系か) POP3-Server.Standard POP3 Exb(申前定義系か) POP3-Client.Standard POP3-proxy POP3 Exb(申前定義系か) POP3-Client.Standard IMAP Exb(申前定義系か) IMAP-Client.Standard IMAP Exb(申前定義系か) IMAP-Server.Standard IMAP Exb(申前定義系か) IMaker(Eigs /- ルルが) Fig Fig Fig Pop3-Client.Standard IMAP Exb(申前定義系か) Fig IMaker(Eigs /- ルルが) Fig Fig Fig Pop3-Client.Standard IMAP		プロキシ アクション 🕈	ファイアウォール ポリシー	種類	ステータス
NUCROTORY NOT CONTROL NUCROTORY NOT CONTROL NUCROTORY NOT CONTROL NUCROTORY NOT CONTROL NUCROTORY NOT CONTROL NUTP-Outgoing,Standard SMTP - Outgoing,Standard SMTP - Bill (中部定義규어) SMTP - Outgoing,Standard POP3 Bill (中部定義규어) POP3-Client.Standard POP3 Bill (中部定義규어) POP3-Server.Standard POP3 Bill (中部定義규어) POP3-Client.Standard POP3 Bill (中部定義규어) POP3-Client.Standard POP3 Bill (中部定義규어) POP3-Server POP3 Bill (中部定義규어) POP3-Server POP3 Bill (中部定義규어) POP3-Client.Standard POP3-proxy POP3 Enabled POP3-Client.Standard POP3-proxy POP3 Enabled POP3-Client.Standard INAP Bill (中部定義규어) IMAP-Client.Standard INAP Bill (中部定義규어) IMAP-Server.Standard INAP Bill (中部定義규어) IMAP-Server.Standard INAP Bill (中部定義규어) POP3-Server POP5-f-f/t/Clpf-fF TOP (FE) FE/F	(アウォール	SMTP-Incoming.Standard		SMTP	無効 (事前定義済み)
Nutcion Control SMTP-Incoming SMTP 用効 (申前定義系か) 19(ウレーションがめ) 19(ウレーションがの) SMTP-Outgoing SMTP 用効 (申前定義系か) 19(ウレーションがの) 19(ウロ-ションがの) POP3-Client.Standard POP3 用効 (申前定義系か) 10(クロ-フーション) POP3-Client.Standard POP3 用効 (申前定義系か) 10(クロ-フージョン) POP3-Client.Standard.1 POP3-Server POP3 用効 (申前定義系か) 10(クロ-フージョン) POP3-Client.Standard.1 POP3-proxy POP3 Enabled 11(AP-Client.Standard.1 POP3-proxy POP3 Enabled 11(AP-C	リティサブスクリプションサービス	SMTP-Outgoing.Standard		SMTP	無効(事前定義済み)
PUP->323080 SMTP-Outgoing SMTP 無効 (特前定義系み) Bioder(陽が加減事が為) POP3-Client.Standard POP3 無効 (特前定義系み) POP3-Client.Standard POP3 無効 (特前定義系み) POP3-Client.Standard POP3 無効 (特前定義系み) POP3-Client.Standard POP3 無効 (特前定義系み) POP3-Client.Standard. POP3-Server POP3 無効 (特前定義系み) POP3-Server POP3-Server POP3 Emb(中前定義系み) POP3-Client.Standard.1 POP3-proxy POP3 Emb(中前定義系み) POP3-Client.Standard.1 POP3-proxy POP3 Emb(中前定義系み) POP3-Client.Standard.1 POP3-proxy POP3 Emb(中前定義系み) IMAP-Client.Standard IMAP Emb(中前定義系み) IMAP-Server.Standard IMAP Emb(中前定義系み) IMAP-Server.Standard IMAP Emb(中前定義系み) Imblocker(WE37-JU/P)-// IMB Imb(F) Emb(F) Imblocker(WE37-JU/P)-// IMB Imblocker アクライブ化ウィザード Emb(F) Imblocker アクライボ化ウィザード Emblocker アクライボ化ウィザード Emblocker アクライボルウィザード	lication Control	SMTP-Incoming		SMTP	無効 (事前定義済み)
Bioker(勝例型放撃対策) トマット検出 「開催温えい対策) POP3-Client.Standard POP3 開効(特前定義系分) POP3-Client、Standard POP3 開効(特前定義系分) POP3-Client POP3 開効(特前定義系分) POP3-Client POP3 開効(特前定義系分) POP3-Server POP3 開効(特前定義系分) POP3-Server POP3 開効(特前定義系分) POP3-Server POP3 開効(特前定義系分) POP3-Client.Standard.1 POP3-proxy POP3 Enabled IMAP-Client.Standard IMAP 開効(特前定義系分) POP3-Client.Standard IMAP 開効(特前定義系分) IMAP-Server.Standard IMAP 開効(特前定義系分) IMAP-Server.Standard IMAP 開効(特前定義系分) IMAP-Server.Standard IMAP 開効(特前定義系分) IMAP-Server.Standard IMAP 開効(特前定義系分) IMAP-Server.Standard IMAP 開効(特前定義系分) SpamBlocker(アクティブ化ウィザード TOP5 イポードで大変使用して、同じくTOP pompBlocker を提供します。Pot Martington		SMTP-Outgoing		SMTP	無効(事前定義済み)
Fx-59 Form Fx-60 Mark CFMILELINFT (#ME3LXU3Ma) POP3-Server.Standard POP3 無効 (特前定義系か) POP3-Client POP3 無効 (特前定義系か) POP3-Client.Standard.1 POP3-Server POP3 FX-0 POP3-Client.Standard.1 POP3-Server POP3-Client.Standard.1 POP3-proxy POP3 FX-0 FX-0 FX-0 FX-0 FX-0 FX-0 FX-0 POP3 FX-0 FX-0 FX-0 POP3 FX-0 FX-0 FX-0 FX-0 <td>Blocker(標的型攻擊対策)</td> <td>POP3-Client, Standard</td> <td></td> <td>POP3</td> <td>無効(事前定美済み)</td>	Blocker(標的型攻擊対策)	POP3-Client, Standard		POP3	無効(事前定美済み)
Markan Marka	トネット検出 情報温えい対策)	POP2 Sequer Standard		0002	每% (中部中学文z)
Map Avion POP3-Client POP3 用効 (甲卵定気水か) xxxtor(ジオロケーション) POP3-Client POP3 用効 (甲卵定気水か) POP3-Client POP3-Client POP3 用効 (甲卵定気水か) POP3-Client POP3-Client POP3 用効 POP3-Client.Standard.1 POP3-proxy POP3 Enabled IMAP-Client.Standard.1 POP3-proxy POP3 Enabled IMAP-Client.Standard IMAP 目効 (甲前定気水か) Imap IMAP-Server.Standard IMAP 目効 (甲前定気水か) Imap IMAP-Server.Standard IMAP 目効 (甲前定気水か) Imap IMAP-Server.Standard IMAP 目効 (甲前定気水か) Imap Imap:Server.Standard Imap Imap Imap Imap:Server.Standard Imap Imap Im		POP3-Server.Standard		POP3	無約(学用)上我(資 の)
POP3-Server POP3 無効(単前定義系か) 小正覚入彼山・防助) (小ビキュリティ トワーグディスか/U- antine Server POP3-groxy POP3 Enabled IMAP-Client.Standard.1 POP3-groxy POP3 Enabled IMAP-Client.Standard.1 POP3-groxy POP3 Enabled IMAP-Server.Standard IMAP E30 (単前定義系か) IMAP-Server.Standard IMAP E30 (単向定義系の) Image:Server.Standard Image:Server.Standard Image:Server.Standard Image:Server.Standard Image:Server.St		POP3-Client		POP3	無効(事則定義済み)
www.ck.k/m ・ が助う (ル セキュリティ トワークディスカ/バリー antime Server tation Enabled Defense ユテーションセキュリティ) Bioker(派急メールが策) at Detection Bioker(アクラィブ化ウィザード このウンゲードを売用して、モリバクの complicitient を提供します、 ウング いちだだ		POP3-Server		POP3	無効 (事前定義済み)
イルセキュリティ トワークディスカパリー rantine Server Atation Enabled Defense ビュテーションセキュリティ) nBlocker(Webフィルタリング) Blocker(Webフィルタリング) spamBlocker アクティブ化ウィザード		POP3-Client.Standard.1	POP3-proxy	POP3	Enabled
トワークディスカバリー antine Server tation Enabled Defense ユデーションとキュリティ) Biocker(派急メールが強) ar Detection Biocker(アクティブ化ウィザード スのウィビードを売用して、デビノスの pomplic/core を掲載します。 ウィビード かまままた		IMAP-Client.Standard		IMAP	無効(事前定義済み)
anne Sever azon Enabled Defense コテーションだキュリティ) Biocker(Webフィルタリング) Biocker(Webフィルタリング) Biocker(Webフィルタリング)		IMAP-Server.Standard		IMAP	無効(事前定義済み)
attorn Endoled Deretes ユテーションセキュリティ) Blocker(派遣メール対策) II Detection SpamBlocker アクティブ化ウィザード スロウィザードを使用リース デビイスの completeder を提供します 合い折 いちまた	antine server				non (2-magnet)
at Detection Blocker(速数メールが病) at Detection Blocker(Webフィルタリング) spamBlocker アクティブ化ウィザード このウィザードを使用して、デビイスの nomPloyler を提供します。 かいたいたまで	ration enabled befense	概成			
	Blocker(迷惑メール対策)				
siocker(Webフィルタリング) spamBlocker アクティブ化ウィザード	at Detection	◆ 設定			
apparticulations / ジェイン 10ション ジー		spamBlocker アクティブ化ウィ	ザード		
			シーI	+ 151/-	

spamBlocker(迷惑メール対策) / POP3-Client.Seucrity

Proxy POP3-Client.Standard.1

☑ spamBlockerの有効化

spamBlocker のアクション	例外について	Virus Outbre	ak Detection		
各スパム カテゴリのアクション	を選択する				
確認済み	サフジェクト タグの述	らうちょう しょうしん しんしょう しんしょ しんしょ	***SPAM***		☑ ログ メッセージの送信
バレク	サフジェクト タグの道	5加 ~	***BULK***		🗹 ログメッセージの送信
疑わしい	許可 サブジェクト タグの過	自加	☑ ログメッセ-	-ジの送信	
spamBlocker サービスが利用でる	きない場合、評り		~ 電子	子メール	
スパムではないと分類された	電子メールごとに、ログ	メッセージを送信	言する		
保存 キャン	ンセル(C)				

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

カテゴリは、「確認済み」のスパム、「バルク」(主に広告メールなど)、「疑わしい」の3種類です。

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

「例外について」タブでは、ホワイトリストの追加削除が行なえます。

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

spamBlocker(迷惑メール対策) / POP3-Client.Seucrity
Proxy POP3-Client.Standard.1
☑ spamBlocker の有効化
spamBlocker のアクション 例外について Virus Outbreak Detection
次のいずれかの送信者および受信者ルールに一致する電子メールのトラフィックは spamBlocker を迂回します。 プロキシに関連するその他の ルールは構成された通りに適用されます。
アクション 🗢 送信者
追加 編集 削除 上に移動 下に移動
☑ 上記の例外のいずれかと一致する各電子メールに、ログ メッセージを送信する
保存 キャンセル(C)

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

*(アスタリスク)@ドメイン名の形で、ドメインを指定することもできます。

アクション	許可	•
送信者	*@watchguard.com	

この例では*@watchgaurd.comをホワイトリストに入れています。

spamBlocker 0		例外について	
連するその他のル	ールは構成され	た通りに適用され	Usia Control C
	アクション	2.\$	送信者
許可			*@watchguard.com
追加 削除	上に移動	下に移動	
25月11 前小市	」」これかと一致	する各電子メーノ	Uこ、ログ メッセージを送信する

[保存]ボタンをクリックして、設定を反映させましょう。

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

spamBlocker(迷惑メール対策)

spamBlocker のアクション

保存

プロキシ アクション 🕈	ファイアウォール ポリシー	種類	ステータス
SMTP-Incoming.Standard		SMTP	無効 (事前定義済み)
SMTP-Outgoing.Standard		SMTP	無効(事前定義済み)
SMTP-Incoming		SMTP	無効 (事前定義済み)
SMTP-Outgoing		SMTP	無効(事前定義済み)
POP3-Client.Standard		POP3	無効(事前定義済み)
POP3-Server.Standard		POP3	無効(事前定義済み)
POP3-Client		POP3	無効(事前定義済み)
POP3-Server		POP3	無効(事前定義済み)
POP3-Client.Security	POP3-proxy-Outgoing	POP3	Enabled
IMAP-Client.Standard		IMAP	無効(事前定義済み)
IMAP-Server.Standard		IMAP	無効(事前定義済み)
IMAP-Client.Standard.1	IMAP-proxy	IMAP	Enabled
構成			
◎ 設定			
spamBlocker(迷惑メール対策) / 設定		
設定 HTTP プロキ	⊧シサーバー Virus Outi	preak Detection	
Virus Outbreak Detectior	n		
Virus Outbreak Detection	n (VOD) の有効化		
VOD でスキャンする最大ファ	イルサイズ 100		キロバイト

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。

キャンセル(C)

POP3-Client-Security		
Blocker の有効化		
Blocker のアクション	例外について Virus O	utbreak Detection
0.1.1.0.1		
Uutbreak Detection	2	
イルスが検出された場合	肖耶余	 アラーム 🕑 ログ
ャン エラーが起こった場合	計可	🔻 🔲 75-4 🕑 ФУ

設定を保存してください。

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

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

以上で spamBlocker の設定は完了です。

おわりに

WebUI ガイドをご参照いただきありがとうございました。

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

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

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