

WSM WatchGuard System Manager 詳細設定ガイド



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

目次

はじめに4
第一章 ネットワーク構成5
ブリッジモードでの運用5
構成例6
ネットワークの設定7
spamBlocker の設定10
ドロップインモードでの運用16
構成例17
ネットワークの設定18
LAN の構成19
ポリシーの設定
第二章 負荷分散と冗長構成
サーバー負荷分散
構成例24
ネットワークの設定25
負荷分散用 SNAT の作成26
ポリシーの追加
FireCluster (HA 構成)
FireCluster の要件
構成例
ネットワークの設定34
FireCluster の設定
クラスタの起動
複数 WAN
要件
構成例
ネットワークの設定
複数 WAN の設定

動作確認41
第三章 UTM 機能
Application Control
ポリシーと Application Control アクションの紐付け42
ファイル転送サービスを制御する44
APT Blocker
APT Blocker の有効化51
ポリシーへの適用
第四章 ユーザーインターフェイス54
CLI
接続方法55
設定手順
WebUI
接続方法
Fireware のアップグレード/ダウングレード64
コンフィグファイルの保存とレポート表示69
クライアント側の UI カスタマイズ73
終わりに

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 基本設定ガイドで触れることのできなかった詳細な設定、大規模ネットワークや高負荷な環境に対応するための方法などを、具体的なケースを交えながら解説しています。

前提として WSM 基本設定ガイド レベルの知識が必要ですので、まだお読みになっていない方はご一読されることをお勧めいたします。

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 XTM 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 ネットワーク構成

WSM 基本設定ガイドでは、Firebox のデフォルトの動作モードである「ルーティングモード」での設定を一通り解説しました。

この詳細設定ガイドでは Firebox を透過的に使用するための「ブリッジモード」(トランスペアレントモードとも 言います)で運用するケースとそのための設定方法、さらには Firebox のもう一つの動作モードであるドロッ プインモードでの設定方法についても解説します。

ブリッジモードでの運用

ブリッジモードで構成する場合 Firebox は管理用の IP アドレスのみで運用されます。この場合の Firebox は透過的に動作し、既存のネットワークの構成を変更することなく UTM 機能を適用することが可能になります。

ただしブリッジモードはその名のとおりL2(レイヤー2)で動作するので、下記の機能は使用できなくなります。

- マルチ WAN
- VLAN
- FireCluster (HA 構成)
- セカンダリネットワーク
- DHCP および DHCP リレー
- 1to1NAT およびダイナミック NAT
- ダイナミックルーティング(OSPF,BGP,RIP)
- すべての VPN 機能

構成例

ブリッジモードを利用する実際的な例として、ここではサーバーを保護する UTM として構成する手順をご紹介します。

この例では、既存のファイアウォールと DMZ にあるサーバーの間に Firebox を挟み込む形で設置していま す。ブリッジモードで動作させることにより、既存のファイアウォールやサーバーの設定を変更せずに spamBlocker(アンチスパム)や IPS などの UTM 機能を追加することができます。



設定するにあたり、このネットワークの設定を以下のように想定します。

ファイアウォールの DMZ 側の IP アドレス	172.16.1.1
Firebox に設定する IP アドレス	172.16.1.254
メールサーバーの IP アドレス	172.16.1.51

ネットワークの設定

ポリシーマネージャのメニューにある<u>ネットワーク</u> – <u>構成</u> をクリックし、ネットワーク構成の画面を開きます。

インターフェイスのモードを指定するリストからブリッジモードを選択します。

ターフェイス	リンクアグリゲーシ					
オスインター		S JUND VLAN NEJAS	ック Bridge Protocols N	WINS/DNS 動的 DNS	複数 WAN Link Monitor SD-WA	N PPPoE
	コーイコキ、深切して	様式をクリックします エレノ操作			イコを様式すると言がたります	
t-rc105	メーノエイスを構成:	ミックスルーティング モート				
ンターフェ	名前 (エイリアス)	ドロップイン モード				
0	External	ミックス ルーティング モード				
1	Trusted	信頼済み	10.0.1.1/24		自動ネゴシエート	
2	Optional-1	無効			自動ネゴシエート	
3	Optional-2	無効			自動ネゴシエート	
4	Optional-3	無効			自動ネゴシエート	
5	Optional-4	無効			自動ネゴシエート	
6	Optional-5	無効			自動ネゴシエート	
					0K ±++2.171	L 0.11.7

IPv4 アドレスは XMT に設定する IP アドレスである 172.16.1.254/24 を入力します。これが WSM で接続 する際の管理 IP アドレスになります。

ゲートウェイの欄には上位のファイアウォールの DMZ 側ポートの 172.16.1.1 を指定します。

のモードでインターフェー	イスを構成:	ブリッジモード			
		── VLAN ID を使用した管理	アクセス用の VLAN タグを記	許可する 1 ≑	
rebox IP アドレス					
重類		IPv4アドレス		ゲートウェイ	
tatic IP		172.16.1.254		172.16.1.1	【構成
咸済みインターフェイス					▲
インターフェイス	名前 (エ-	(リアス)	種類	NIC 構成	用成
0	External		外部	自動ネゴシエート	
1	Trusted		信頼済み	自動ネゴシエート	
2	Optional-1		無効	自動ネゴシエート	
3	Optional-2		無効	自動ネゴシエート	
4	Optional-3		無効	自動ネゴシエート	
5	Optional-4		無効	自動ネゴシエート	
6	Optional-5		無効	自動ネゴシエート	

その横の[構成]ボタンをクリックすると、ブリッジモードのプロパティを設定できます。

とはいえ、設定できる項目はそれほど多くありません。

Firebox は接続されているデバイスの MAC アドレスを自動的に登録し、ルーティングテーブルに保存してゆ きますが、それを有効にするチェックが「自動ホストマッピング」です。基本的にはどれもチェックを入れてお くべきでしょう。

「関連ホスト」の項では、手動でデバイスの接続を構成する場合、または自動ホスト マッピング機能が正常 に動作しない場合、関連するホスト エントリを追加できます。

関連ホスト エントリは、1 つのホストの IP アドレスと 1 つのネットワークインターフェイスの間に静的ルート を作成します。 デフォルトでは Firebox の外部インターフェイスとデフォルトゲートウェイとなっているファイア ウォールの IP アドレスが関連付けられています。

ドロップイン/ブリッジ モード プロバ	71		
NA - /- +	251/7		
リターフェイス ポストメン			
110/07/14/22/2			
このインターフェイスに接続す MACアドレスがFireboxで自動が ト マッピングを有効にします。 Fireboxでは関連ホスト リスト	"るホスト デバイスの 肉に検出されるように、各ネットワー 自動ホスト マッピングが有効にな にないデバイスからの接続は無視され	・ク インターフェイスの っていない場合、 1.ます。	自動ホス
🗹 External	Optional-3		
✓ Trusted	Optional-4		
Optional-1	Optional-5		
Ontinnal 2			
1連ホスト	インターフェイス名	128-7	追加
172. 16. 1 . 1	External	0	削除

[OK]をクリックし、設定を保存します。

次にポリシーを設定します。

spamBlocker の設定

WSM 基本設定ガイドでは、UTM 機能を有効にする際にウィザードを使っていましたが、ここでは手動でポリシーを追加し、spamBlocker を有効にしてみましょう。

ポリシーマネージャで[ポリシー追加]ボタンをクリックし、以下の追加画面で SMTP-proxy を選択し、[追加] ボタンをクリックします。

🌄 ポリシーを追加する		×
新しいポリシーに対して事前定義済みまたは □	カスタム ポリシーを選択し. ポリシー テンプレー POP3-proxy	ます。 ・ト プロパティ
H323-ALG H323-ALG HTTP-proxy HTTPS-proxy	POP3 ボート 110	プロトコル TCP
POP3-proxy SIP-ALG	POP3S ポート 995	プロトコル TCP
● SMTP-proxy ● TCP-UDP-proxy ● ● バケット フィルタ	Fireware OS v12.2↓ 説明	以降。
bb	ポスト オフィス ブ	□ F ⊐ /k V3
カスタムを管理する		
	ポリシ	ッーを追加する キャンセル ヘルブ

ポリシーの新規作成画面が開きます。

SMTP-proxy は基本的に Incoming のポリシーなので、送信元は Any-External、送信先は未設定の状態になっています。

送信先の[追加]ボタンをクリックし、設定しましょう。

CUTD assure		
. Smir-proxy		P #
リシー プロパティ 詳細		
(TD provy 控結ち		
·미···································	TCPDSTの送信	
- 		
Sサホート: 有効	✓ (Fireware US v12.2 k/k#)	
差信元		
Any-External		
	i	1加 編集 削除
*信先		
差信先 		
美信先 粲 None		
送信先 <mark> 祭 None</mark>		
≚信先 <mark> ≪ None</mark>		
差信先 <mark>桑 None</mark>		
≚信先 <mark>桑 None</mark>		
≚信先 <mark>& None</mark>		1加 編集 削除
≚信先 餐 None	ED WALL Desire Daution	110 編集 削除
盖信先 餐 None □ Route outbound traffic using	SD-WAN Based Routing (Fireware OS v12.3 or higher)	<u>1 ho</u> 網集 削除
≚信先 Route outbound traffic using SD-WAN Action	SD-WAN Based Routing (Fireware OS v12.3 or higher)	<u>】加</u> 編集 削除
≚信先	SD-WAN Based Routing (Fireware OS v12.3 or higher)	<u>】加</u> 稱集 削除
≚信先 None None Route outbound traffic using SD-WAN Action	SD-WAN Based Routing (Fireware OS v12.3 or higher)	<u>1.10</u> 新在 新加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加
▲信先 None Route outbound traffic using SD-WAN Action	SD-WAN Based Routing (Fireware OS y12.3 or higher)	<u>} 加</u> 稱失 削除
▲信先 None None None SD-WAN Action Application Control を有効にし	SD-WAN Based Routing (Fireware OS v12.3 or higher) 한 한 호 3 : Global 한 한	<u>3 加</u> 嗣除
送信先 None None Route outbound traffic using SD-WAN Action Application Control を有効にし Geolocation を有効にする	SD-WAN Based Routing (Fireware OS v12.3 or higher) Image: SD-WAN Based Routing Image: SD-WAN Based Routing Image: SD-WAN Based Routi	<u>a ho</u> 御朱 削除
送信先 None ○ Route outbound traffic using SD-WAN Action ○ Application Control を有効にし ○ Geolocation を有効化する ○ オニのポリシーの IPS を有効にし	SD-WAN Based Routing (Fireware OS v12.3 or higher) 호 한 환 호 호 : Global 환 환 (Jit 국	<u>1.10</u> 編集 削除
≚信先 None Route outbound traffic using SD-WAN Action Application Control を有効にし Geolocation を有効化する Conポリシーの IPS を有効にし	SD-WAN Based Routing ♥ (Fireware OS v12.3 or higher) ■ ■ ■ ます: Global ■ ■ Global ♥ ■ *ます	<u>3. 加</u> 鋼柴
▲信先 None Route outbound traffic using SD-WAN Action Application Control を有効にし Geolocation を有効化する このポリシーの IPS を有効にし 常域幅と時間フォータを有効()	ます: Global ノます: Clobal ノます にする (Fireware OS v11.10 以降)	<u>3 加</u>
送信先 None Route outbound traffic using SD-WAN Action Application Control を有効にし Geolocation を有効化する このポリシーの IPS を有効にし 常域幅と時間クォータを有効1 'ロキシアクション: SMTP-Inco	SD-WAN Based Routing (Fireware OS v12.3 or higher) ます: Global Global (Fireware OS v11.10 以降) ごする (Fireware OS v11.10 以降) mino.Standard	<u>a</u> 加 和殊 判除

アドレスの追加画面からその他の追加をクリックします。

Any Firebox Any-External			
Any-Trusted Any-Optional			
ANY-DOVPN			
追加 追加	SNAT の追加	ユーザーの追加	その他の追加
_{& Any-DOVPN} 追加 訳されたメンバーとア	SNATの追加 "ドレス:	ユーザーの追加	その他の追加 削除
_{&} Any-DOVPN 追加 択されたメンバーとア	SNATの追加 ?ドレス:	ユーザーの追加	その他の追加 副除

送信先はメールサーバーの IP アドレスを指定します。

. Contribution					☑ 有効	
リシー プロパティ 詳細						
MTP-proxy 授颖を	TOD BOTO	4 / 5				
reg ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		(Fireware OS v1	2.2以降)		~	
送信元	75.70.81	1				
Any-External	(使用可能な	×ンバー:				
		一の追加				
		種類の選択:	ホスト IPv4			~
¥/##		値:	172. 16. 1.51			
None None	- <u>R</u>					
	選択					
Route outbound traffic us	ing					
SD-WAN Action						
SD-WAN Action						
SD-WAN Action	:LIII:					
SD-WAN Action Application Control を有効! Geolocation を有効化する	:133:					
SD-WAN Action Application Control を有効1 Geolocation を有効化する このポリシーの IPS を有効	こします :					
SD-WAN Action Application Control を有効に Geolocation を有効化する このポリシーの IPS を有効 常知個と時間フォータを有効	こします : にします 効化する (
SD-WAN Action Application Control を有効に Geolocation を有効化する このポリシーの IPS を有効 常地幅と時間クォータを有 プロキシ アクション: SMTP-1	こします: にします 効化する(ncoming.S					OK キャンセル

OK をクリックして抜けるとポリシーマネージャに SMTP-proxy が追加されています。

	B 8 V	+ × ¥ 🖲 🗽 🗈 🦛	😹 🗚 🖳 🖉 🔗 🗖 🗖	?				
ファイア	ウォール Mobil	e VPN with IPSec						
					7	イルタ:なし	~	77
順序 /	アクション	ポリシー名	ポリシーの種類	送信元	送信先	ポート	PBR	SD-WA
1 2 3 4 5 6 7 8 9 10		 FTP-proxy HTTP-sproxy HTTP-sproxy WatchGuard Certificate Portal WatchGuard Web UI Ping DNS SMTP-proxy WatchGuard Outgoing 	FTP-proxy HTTP-proxy HTTPS-proxy WG-Cert-Portal WG-Fireware-XTM-WebUI Ping DNS SMTP-proxy WG-Firebox-Mgmt TCP-UDP	Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-Trusted, Any-Optional	Any-External Any-External Any-External Firebox Firebox Any Any-External 172.16.1.51 Firebox Any-External	tcp:21 tcp:80 tcp:443 tcp:4126 tcp:8080 icmp (type: 8, code: 255) tcp:53 udp:53 tcp:25 tcp:455 (tls) tcp:24105 tcp:4117 tcp:4118 tcp:0 (Any) udp:0 (Any)		
<						11	Firewar	e OS

このプロキシに spamBlocker を有効にし、アクションを設定しましょう。

再度 SMTP-proxy のポリシーを開きます。

[プロキシアクションの複製]ボタンをクリックします。

	>
前: SMTP-proxy	「有効
ポリシー プロパティ 詳細	
SMTD.orovy 接訪友	
許可 v TCP RS	1の送信
しらサポート: 有効	✓ (Fireware OS v12.2 以降)
送信元	
🛠 Any-External	
	追加 . 福朱 削強
送信先	
-	注血加 《編集 前川余
Route outbound traffic using SD-W SD-WAN Action	S& MD 福後 副除 AN Based Routing (Fireware OS v12.3 or higher)
□ Route outbound traffic using SD-W SD-WAN Action □ Application Control を有効にします:	注加 福年 副除 AN Based Routing (Fireware OS v12.3 or higher)
 □ Route outbound traffic using SD-W SD-WAN Action □ Application Control を有効にします: ☑ Geolocation を有効化する 	注意加 海疾 副除 AN Based Routing (Fireware OS v12.3 or higher) Global Global Global W 予
 Route outbound traffic using SD-W SD-WAN Action Application Control を有効にします: Geolocation を有効化する エのポリシーの IPS を有効にします 	注意加 海疾 副除 AN Based Routing (Fireware OS v12.3 or higher) Global Global 「新 論 」 「新 論 」
 Route outbound traffic using SD-W SD-WAN Action Application Control を有効にします: Geolocation を有効化する ごのポリシーの IPS を有効にします 帯転幅と時間クォータを有効化する (F 	注意加 編集 副除 AN Based Routing V (Fireware OS v12.3 or higher) Global M M M M M M M M M M M M M M M M M M M
Route outbound traffic using SD-W SD-WAN Action Application Control を有効にします: Geolocation を有効にする ごのポリシーの IPS を有効にします 帝城幅と時間クォータを有効にする (F プロキシ アクション: SMTP-Incoming.State	

プロキシアクション構成の左メニューの「spamBlocker」をクリックします。

まだ有効になっていないので、spamBlockerを有効にするのチェックを入れます。

前:	SMTP-Incoming.Standard		
明:	ard recommended standard	onfiguration for SMTP-Incoming with logging enabled	
カテ	1V		
	全般 →全般設定 → グリーティング ルール ESMTP → ESMTP 設定 → STARTTLS Encryption	spamBlocker	
	└─認証 添付ファイル └──コンテンツの種類 └──ファイル名 マドレコ		
	Mail From Rept To ヘッダー ゲートウェイ AV		
	Data Loss Prevention <mark>spamBlocker</mark> 拒否メッセージ ブロキッと AV アラーム		
	APT Blocker TLS		

するとSMTP 通信を許可する際のアクションを設定する画面が表示されます。

例として2通りの設定を以下に挙げます。

例-1:スパムは拒否、広告メールなどのバルクはタグ付け、未確認(疑わしい)は許可の設定

SMTP-Incoming.Standard				
ard recommended standard o	onfiguration for SMTP-Inco	ming with logging enabled		
- JU				
全般 全般設定 − (1) - ティング 山 - 山	spamBlocker			
ESMTP ESMTP設定	🗹 spamBlocker を有効	りにする		
STARTTLS Encryption	アクション 例外 Vi	rus Outbreak Detection		
☆付ファイル コンテンツの種類	各スパム カテゴリ	のアクションを選択してくだ;	5い。	
ファイル名	確認されたスパム:	拒否	~	🗹 ログ メッセージの送信
ーアドレス Mail From	バルク:	サブジェクト タグの追加	~ ***BULK***	🔽 ログ メッセージの送信
L-Rept To ヘッダー	未確認:	許可	~	🗹 ログ メッセージの送信
ゲートウェイ AV Data Loss Prevention	spamBlocker サーノ	いーが使用できない場合の、S	/TP 電子メールへのアクセ	スの処理方法: 許可 🗸
"spamblocker "拒否メッセージ "プロキシと AV アラーム "APT Blocker	□ スパムでないと	:分類された電子メールごとに	ログ メッセージを送信	

例-2:スパム、バルク、未確認(疑わしい)のどれもタグ付けの設定

ard recommended standard	configuration for SMTP-Inco	ming with logging enabled		
- I U				
全般	spamBlocker			
全般設定				
ーグリーティング ルール	anom Pleaker 5 5 d	hI- T Z		
ESMIP FONTD BY T		11- 9 %		
STARTTLS Encryption	アクション 例外 Vir	rus Outbreak Detection		
1.21E				
添付ファイル	各スパム カテゴリ(のアクションを選択してください。		
ーコンテンツの種類		[]		
「ファイル名	確認されたスパム:	サブジェクト タグの追加 🗠	***SPAM***	└ ログメッセージの送信
ーアトレス LMail From	パルク:	サブジェクト タグの追加 🔷	***BULK***	🔽 ログ メッセージの送信
Rcpt To	土础闭。	サブジェクト タガのieta	***CUSDECT***	
ヘッダー	The VEC BAD .	555151 X 5654	SUSPECT	
ゲートウェイ AV	enamBlocker tt – /	くっか使用できかい場合の SMTD	勇子マー 山へのアクセン	2.000理方法· 許可 。
Data Loss Prevention	spaniblocker 5 7	i priemicerative dot Simir	-BIX 10.007.7.07	(0)25±1)2.
spamBlocker				
拒否メッセージ	☑ スパムでないと	:分類された電子メールごとに口ク	「メッセージを送信	

設定を Firebox に保存し、動作を確認してください。

ドロップインモードでの運用

ドロップインモードはブリッジモードに似ていますが、より柔軟な運用が可能です。

具体的には、以下のように動作します

- Firebox のすべてのインターフェイス (外部、信頼済み、および任意) に、同じプライマリ IP アドレス が割り当てられます
- どのインターフェイスにもセカンダリ ネットワークを割り当てることができます。
- 信頼済みネットワークおよび任意ネットワークのホストでは、同じ IP アドレスおよびデフォルト ゲート ウェイを保持したまま、セカンダリ ネットワーク アドレスを追加できるため、Firebox はこれらのネット ワーク上のホストにトラフィックを正しく送信できます。
- Firebox 配下のパブリック サーバーは、引き続きパブリック IP アドレスを使用できます。ネットワークの外部からパブリック サーバーにトラフィックをルーティングするときに、ネットワーク アドレス変換 (NAT) は使用されません。

構成例

前述の特長を利用すれば、一例として Unnumbered PPPoE を使ったグローバル IP を持つネットワークを 構成することができます。

この例では、Unnumbered PPPoE 対応のルーターの下に Firebox を設置し、グローバル IP アドレスの DMZ 領域を作成します。

同時に Trusted インターフェイスにセカンダリ IP アドレスを設定することにより、クライアント用のセグメント も構成します。



設定するにあたり、このネットワークの設定を仮に以下のように想定します。

固定のグローバル IP 8 個のネットワーク	203.0.113.0 (0-7)/29
PPPoE ルーターの IP アドレス	203.0.113.1
Firebox に設定する IP アドレス	203.0.113.2
サーバーに割り当てる IP アドレス	203.0.113.3~6
LAN 側のネットワーク	192.168.1.0/24

Firebox のインターフェイスは、あらかじめ0番ポートはExternal、1番ポートはTrusted、2番ポート以降 は Optional で設定しておいてください。(IP アドレスはデフォルトで結構です)

ネットワークの設定

ネットワーク構成の画面のインターフェイスのモードを「ドロップインモード」にします。

集するインター	フェイスを選択して、 構成 を	クリックします。正しく擁	作するには、 XTM デバイスの外	部インターフェイスを構成する必要があります。	
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			
(ンターフェ	名前 (エイリアス) につ	u sì エード(牧教 WAN SA u ブイン エード(牧教 WAN	(ボーナ) (スレキけ無効)	٦	
0	External-1	ソノイン ビード (機能)(A)			
1	External-2	外部	DHCP	自動ネゴシエート	
2	LAN1	プリッジ		自動ネゴシエート	
3	LAN2	ブリッジ		自動ネゴシエート	
4	LAN3	ブリッジ		自動ネゴシエート	
5	Optional-4	無効		自動ネゴシエート	
6	Optional-5	無効		自動ネゴシエート	

すると以下のような画面になります。

IPv4 アドレスは前述の設定表どおり、203.0.113.2を設定します。

ゲートウェイは PPPoE ルーターの内側のアドレスである 203.0.113.1 を指定します。

インターフェ	Bridge Protocols イス	WINS/DNS 動的 DI リンクアグリン	NS 複数 WAN デージョン	Link Monitor プリッ	SD-WAN	VLAN
集するインターフェイス [;] のモードでインターフェ	を選択して、 構成 をクリック イスを構成: ドロップイン	フします。正しく操作する ・モード	こは、 XTM デバイスの外部	インターフェイス	を構成する必要	きがあります。
irebox IP アドレス						1
重類 itatic IP	IPv4アドレス 203.0.113.2		ゲートウェイ 203.0.113.1			構成
アドレスの範囲を最大	6つまで設定できます。					
アドレスの範囲を最大 アドレス ブール:	:6 つまで設定できます。					
アドレスの範囲を最大 アドレス ブール: 開始 IP	、6 つまで設定できます。	終了 P			追加	
アドレスの範囲を最大 アドレスブール: 開始 IP	c 6 つまで設定できます。	終了 P			」 這加 編集	
アドレスの範囲を最大 アドレスブール: 開始 IP	c 6 つまで設定できます。	¥¥了₽				
アドレスの範囲を最大 アドレス ブール: 開始 IP 予約 アドレス:	c 6 つまで設定できます。	終了 IP			道加 編集 削除	
アドレスの範囲を最大 アドレス ブール: 開始 IP 子約 アドレス: 子約 ろ	c 6 つまで設定できます。	¥7 ₽	MAC 7 F V 3			
アドレスの範囲を最大 アドレスブール: 開始 IP 予約 アドレス: 予約 スドレス:	c 6 つまで設定できます。	終了 IP 1P	MAC 7 F L Z		道加 編集 削除 違加 編集	

サーバーからは Firebox に割り当てた 203.0.113.2 がゲートウェイアドレスになります。

アドレス欄の横にある構成を開くと、ブリッジモードと同様、自動ホストマッピングの有効/無効および関連ホ ストのエントリの設定をする画面になります。詳しくはブリッジモードの項をご覧ください。

動ホストマッピング				
このインターフェイスに接続す	るホスト デパイスの			
IACアドレスがFireboxで自動的 トマッピングを有効にします。	aに検出されるように、各キ 自動ホスト マッピングが	ミットワーク 有効になって	インターフェイス(いない場合、	り自動ホス
Fireboxでは関連ホスト リストに	こないデバイスからの接続!	は無視されま	₫ .	
External-1	2 L	AN3		
External-2	2	ptional-4		
LAN1		ptional-5		
LAN2				
連ホストーーーーー				
/ ホスト	インターフェイス	(名	インターフ	追加
203. 0 .113. 1	External-1		0	削除

OK ボタンをクリックし、ネットワーク構成の画面に戻ります。

LAN の構成

ネットワーク構成の画面をスクロールバーで下に下がると、インターフェイスの一覧があります。

LAN 側のネットワークを構成するために、インターフェイス1を選択し、[構成]をクリックします。

W-2000	Bridge Protocols	WINS/DNS	動的 DNS	複数 WAN	Link Monitor	SD-WAN	PPPo
インター	-7=12		ンクアグリゲーシ	97 97	プリック	2	VLAN
集するインターフェ・	イスを選択して、 構成 をクリ・	ックします。正しく	操作するには、 X	TMデバイスの外部イ	ンターフェイスを構成	はする必要があり	します。
のエードアインター・	フェイフを構成・「ドロップイ	N # ~ K					
or (4)2.	7 1 7 214 A8 - 1 H 7 7 1	201					
成済みインターフェ	17						
インターフェイス	名前 (エイリアス)	ŧ	ŧXĄ	NIC構成			構成
0	External-1	外	部	自動ネゴシ	ドート		
1	Trusted	信	頼済み	自動ネゴシ	エート		
2	LAN1	無	効	自動ネゴシ	I∼ ŀ		
3	LAN2	無	効	自動ネゴシ	エート		
4	LAN3	無	効	自動ネゴシ	エート		
5	Optional-4	無	効	自動ネゴシ	L-F		
6	Optional-5	無	効	自動ネゴシ	I ~ h		

インターフェイス1の設定画面を開いたら「セカンダリ」タブを選択し、[追加]ボタンをクリックします。 次のように、IP アドレスの欄に LAN 用のネットワークの設定をします。

■ インターフェイスの設定 - インターフェイス番号 1	\times
全般 セカンダリ MACアクセス制御 詳細	^
このインターフ フィックをルー 戦 セカンダリネットワークの追加 ×	
■ アドレス: 192.168.1.1/24 道院	<u></u>
編集	
OK キャンセル	
	~
OK キャンセル ヘル	7

この設定によって、Trusted インターフェイスに接続されるクライアントからは、192.168.1.1 をゲートウェイ とするネットワークを構成できます。

全般タブに戻って、DHCP サーバーの設定もできます。

セカンダリネットワークでの DHCP サーバーの使用にチェックを入れて、クライアントに払い出す IP アドレス プールや DNS サーバーを設定することができます。

そ セカンダリ	MACアクセス制	læn i¥\$⊞		
ンターフェイ	ス名 (エイリアス)	: Trusted		
シターフェイ	スの説明:			
ンターフェイ	スの種類:	信頼済み		
)システムロH	ICP設定の使用			
) DHCP を無效	めにする			
● セカンダリ	ネットワークでの	DHCPサーバーの使用		
アドレスの)範囲を最大 6 つま	で設定できます。		
アドレス:	ブール:			
192,168,1	.100	192.1	68.1.254	35.70
				編集
				削除
予約 アド	レス:			
予約名		予約旧	MACアドレス	1£ 10
				編集
				尚收8 注
リース時間	8時間			~
リー ス時間 DNSサー	1 8時間 - バーとWINSサー	バーを構成する	OHCPオプション	~
リース時間 DNSサー 既定のゲー	1 8時間 - バーとWINSサー - トウェイ:	バーを構成する	DHCPオブション	~
リース時間 DNSサー 既定のゲー ④ インタ	1 8時間 - バーとWINSサー - トウェイ: - フェイス IPを使	バーを構成する	DHCPオブション	×
リース時間 DNSサ〜 一 一 のゲー ④ インタ	1 8時間 - バーとWINSサー トウェイ: - フェイス IPを後 ネットロークアク	バーを構成する	DHCPオブジョン	×
リース時間 DNSサー 一 一 の ズンタ り ア た し フ フ フ の デ - () インタ り ア ち - の フ の フ し の ち - の 、 の デ - の 、 の デ - の 、 の 、 つ 、 の 、 の 、 つ 、 の 、 つ 、 の 、 つ 、 の の 、 の 、 の 、 の の 、 の 、 の の 、 の 、 の の 、 の の 、 の の 、 の の の 、 の の 、 の の 、 の の の 、 の の の 、 の の の の の の の の 、 の の の の 、 の の の の の の の の の の の の の	1 8時間 - バーとWINSサー - トウェイ: - フェイス Pを修 ネットワークでの (DHCDDH#16157	バーを構成する 此用する 〇 指定する DHCP中継の使用 DHCPログバッター	DHCP オブション ・・・・	×
リース時間 DNSサー 一 一 一 の ゲー ④ インタ り セ カンダリ ー ア ド レス り 、 の ゲー ・ 一 の 、 サー ・ 一 の 、 サー ・ 一 の 、 サー ・ 一 の 、 サー ・ 一 の 、 サー ・ 一 の 、 サー ・ の ゲー ・ の ゲー ・ の ゲー ・ の ゲー ・ の ゲー ・ の ゲー ・ の ゲー ・ の ゲー ・ の 、 の ゲー ・ の 、 の ゲー ・ の 、 の ゲー ・ の 、 の ゲー ・ の 、 の か ー の 、 の か ー の 、 の か ー の 、 の か ー の か ー の か ー の か ー の か ー の か ー の か ー の か ー の か ー の か ー の か の か ー の の か ー の か ー の か ー の の の か ー の の の の の の の の の の の の の	- パーとWINSサー トウェイ: ーフェイス Pを後 ネットワークでの (DHCP中継が有効	バーを構成する E用する 〇 指定する DHCP中継の使用 的なすべてのインターフ	DHCPオブション ・・・・ エイス用):	×
リース時間 DNSサー 一 一 の インタ り セカンダリ IPアドレス	- バーとWINSサー - バーとWINSサー トウェイ: - フェイス Pを御 ネットワークでの (DHCP中継が有対	バーを構成する 使用する 〇 指定する ・ DHCP中継の使用 力なすべてのインターフ	DHCPオブション ・・・・ エイス用):	×
リース時間 DNSサ・ 既定のゲー ● インタ)セカンダリ Pアドレス	- バーとWINSサー - バーとWINSサー - トウェイ: - フェイス Pを使 ネットワークでの (DHCP中継が有文	バーを構成する 使用する 〇 指定する ・DHCP中継の使用 的なすべてのインターフ	DHCPオブション エイス用):	×
リース時間 DNSサ・ 既定のゲー ④ インタ)セカンダリ Pアドレス	- バーとWINSサー - バーとWINSサー - トウェイ: - フェイス Pを伸 ネットワークでの (DHCP中継が有文	バーを構成する を用する 〇 指定する DHCP中継の使用 かなすべてのインターフ 違加	DHCP オフション エイス用): 削除	×
リース時間 DNSサ- 既定のゲー ④ インタ) セカンダリ Pアドレス (Fireware I	 8時間 バーとWINSサー トウェイ: フェイス Pを使 ネットワークでの (DHCP中継が有対 OS v11.10 では、1 	バーを構成する を用する () 指定する DHCP 中継の使用 かなすべてのインターフ 違加 DHCP リレーの観察の	DHCP オフション エイス用): 削除 P アドレスがサポートされています	× •)
リース時間 DNSサ- 既定のゲー ④ インタ) セカンダリ Pアドレス (Fireware II	 8時間 バーとWINSサー トウェイ: フェイス Pを使 ネットワークでの (DHCP中継が有文 OS v11.10 では、1 	バーを構成する 取用する ① 指定する DHCP 中継の使用 かなすべてのインターフ 違加 DHCP リレーの観数の	DHCP オブション エイス用): 創账 P アドレスがサポートされています	×. .)
リース時間 DNSサ・ 既定のゲー ④ インタ)セカンダリ Pアドレス (Fireware l	- バーとWINSサー - バーとWINSサー - トウェイ: - フェイス Pを伸 ネットワークでの (DHCP中継が有文 OS v11.10 では、1	バーを構成する 取用する 〇 指定する ・ DHCP 中継の使用 的なすべてのインターフ 違加 DHCP リレーの視数の	DHCP オブション エイス用): 創账 P アドレスがサポートされています	× •)
リース時間 DNSサ- 既定のゲー ④ インタ) セカンダリ) Pアドレス (Fireware l	- バーとWINSサー - バーとWINSサー - トウェイ: - フェイス P を作 ネットワークでの (DHCP中継が有文 OS v11.10 では、1	バーを構成する 使用する ① 指定する PDHCP 中継の使用 的なすべてのインターフ 通加 DHCP リレーの観数の I	DHCP オブション エイス用): 創除 P アドレスがサポートされています	× •)

[OK]をクリックします。

インターフェイス2から5は、サーバー用の Optional(任意)のポートとして設定しています。

インターフェイス	種類	名前 (エイリアス)	NIC構成	構成
0	外部	External	自動ネゴシエート	
1	信頼済み	Trusted	自動ネゴシエート	
2	任意	Optional-1	自動ネゴシエート	
3	任意	Optional-2	自動ネゴシエート	
4	任意	Optional-3	自動ネゴシエート	
5	任意	Optional-4	自動ネゴシエート	
6	任意	Optional-5	自動ネゴシエート	

下の図はメールサーバー、ウェブサーバー、DNS サーバーへの通信を許可するポリシー(フォーカス当てて いるもの)を追加した状態です。

いずれも Any-External から Any-Optional を許可するポリシーです。

フィルターなし						
順序	アクション	ポリシー名	ポリシーの種類	送信元	送信先	ポート
	1	W HTTP-Incomming	HTTP	Any-External	Any-Optional	tcp:80
	1	IMAP-Incomming	IMAP	Any-External	Any-Optional	tcp:143
	Ø	HTTPS-Incomming	HTTPS-proxy	Any-External	Any-Optional	tcp:443
	1	🗢 WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080
		(a) Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
		DNS	DNS	Any-Trusted, Any-Optional	Any-External	tcp:53 udp:53
	1	DNS-Incomming	DNS	Any-External	Any-Optional	tcp:53 udp:53
	0	POP3-Incoming	POP3-proxy	Any-External	Any-Optional	tcp:110 tcp:995 (tls)
	1	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118
		Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)

第二章 負荷分散と冗長構成

Firebox は、内部のサーバーに対して負荷分散する設定、FireCluster とよばれる HA 構成の設定、2 つの ポートに External ポートを設定して負荷分散やフェールオーバーを実現するマルチ WAN を設定すること ができます。

第二章では、これら負荷分散と冗長構成の手法を解説します。

自社のウェブサイトのレスポンス低下は、機会損失や企業の評判低下に直結します。しかし、ロードバランスの専用機器は高価なものが多く、導入時のコストは企業にとって大きな負担となります。

Firebox は、ルーター、ファイアウォール、UTM の機能に加え、低価格でロードバランスを実現します。

構成例

DMZ に Web サーバーが 3 台あり、それらに負荷分散したいというケースで説明しましょう。



ネットワーク構成は以下のとおりです。

External	PPPoE 接続
LAN 側のネットワーク	192.168.1.0/24
DMZ 側のネットワーク	172.16.1.0/24
サーバーに割り当てる IP アドレス	172.16.1.51 ~ 53

設定の流れとしては、

- 1. インターフェイスを構成
- 2. 複数サーバーへの負荷分散用の SNAT を作成する
- 3. DMZ の Web サーバーに HTTP アクセスを許可するポリシーを作成
- 4. そのポリシーの送信先を、作成した Web サーバー用の SNAT に指定

となります。

ネットワークの設定

構成にしたがって、以下のように設定します。

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				
ンターフェ	名前 (エイリアス)	種類	IPv4 アドレス	IPv6 アドレス	NIC 構成	權成
0	External	外部	PPPoE		自動ネゴシエート	
1	Trusted	信頼済み	10.0.1.1/24		自動ネゴシエート	
2	Optional-1	任意	172. 16. 1 . 1 /24		自動ネゴシエート	
3	LAN2	無効			自動ネゴシエート	
4	LAN3	無効			自動ネゴシエート	
5	Optional-4	無効			自動ネゴシエート	
6	Optional-5	無効			自動ネゴシエート	

負荷分散用 SNAT の作成

ポリシーマネージャ <u>セットアップ</u> – <u>アクション</u> – <u>SNAT</u> をクリックします。

C:#Users#tsuto#Documents#IMy WatchGuard#config	s¥T50-W-MAY29.xml *- Fireware	Policy Manager		- 0	×
ファイル 編集 表示 セットアップ ネットワーク FireClus	ter VPN セキュリティサービス	ヘルプ			
	🆇 🧚 🖳 🗶 🔗 🗖 🔍	?			
エイリアス		7	ィルタ: なし	~	P 7
順序 / アクショ 認証	ポリシーの種類	送信元	送信先	ポート	
1 2 証明書	HTTP	Any-External	Any-Optional	tcp:80	
2 3 4 5 6 7 8 9 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 ・ 10 10 10 10 10 10 10 10 10 10	トラフィック管理 ブロキシ コンテンツ TLS プロファイル 24ジュール SNAT Quotas	Any-External Any-External Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-External Any-Trusted, Any-Optional Any-Trusted, Any-Optional	Any-Optional Any-Optional Firebox Any Any-External Any-Optional Firebox Any-External	tcp:143 tcp:843 tcp:8080 icmp (type: 8, code: 2 tcp:53 udp:53 tcp:53 udp:53 tcp:110 tcp:995 (tls) tcp:4105 tcp:4117 tcp tcp:0 (Any) udp:0 (Ar	55) :4118 iy)
< OSの互換性				Fireware	> 05 v12 4 0

SNAT の画面が起動します。[追加]ボタンをクリックします。

D_Web_Server	 追加
	編集
	割除

追加画面では「SNAT 名」に分かりやすい名前をつけます。

NAT の種類として「サーバー負荷分散」を選択します。

SNAT名:	WebServ	rer		
2月:				
○ 静的 N	AT 💽 🕂	ーバー負荷な	分散	
NAT X V	15-:			
				追加
				編集
				削除

SNAT メンバーの[追加]をクリックし、SNAT のメンバーを追加します。

するとサーバー負荷分散 NAT の設定画面が開きます。

 ■ サーバー負荷分散 NAT を追加します ■ アドレスまたはインターフェイス ■ 発信元 IP を設定する 	X	負荷分散方法では、「ラウンドロビン」 と「最小構成」を選択できます。 <u>ラウンドロビン</u> :
方法: サーバー: IPアドレス	ラウンドロビン ✓ 重み 編集	接続が順番に (ラウンドロビンで) 割 り振られます。 最初の接続は、重みで 指定された 1 番目のサーバーに送信 されます。
☑固定接続を有効にする		最小接続 : 新しいセッション発生時、現時点でオー プンな接続数が最も少ないサーバーに 送信されます。
(FQDN の静的 NAT の場合は、 Firew	'are v1/2 以降加必要です) <u>K</u> キャンセル	

負荷分散方法を選択したら、[追加]ボタンをクリックし、サーバーを追加しましょう。

[追加]ボタンをクリックすると、サーバーの追加画面が開きます。

サーバーの IP アドレスを入力します。



重みは負荷分散の重み付けの設定で、接続の優先順位を表わします。

[OK]をクリックし追加したら、同じように残り2台のサーバーを追加します。 以下のような画面になるでしょう。

Pアドレスまたはインターフェイス	Any-External	~
🦳 発信元 IP を設定する	1/1/12	
方法:	ラウンド ロビン	×
サーバー:	- - -	
IF アトレス 172.16.1.51	_里み 1	追加
172.16.1.52	1	編集
172.16.1.53	1	省归取完
-		
✓ 固定接続を有効にする	8 🝨 时間 🗸	1
		ミアオン

「固定接続を有効にする」のチェックは、指定の期間、継続的に同じサーバーを使用する接続のことです。 接続を固定すると、ある発信元アドレスと宛先アドレス ペア間のすべてのパケットは、指定した期間、同じ サーバーに送信されます。

	TTODOGITOI	
说明:		
()静的	NAT 🖲 サーバー負荷分散	
SNAT X	ンパー:	
ታ-	パーの負荷分散:ラウンドロビン	這加
440 / 447 /	ny-External> 172.16.1.52 [1]	編集
,	vny-External> 172.16.1.53 [1]	削除

3 台分のサーバーを設定し、負荷分散 NAT 画面を OK で抜けると、SNAT 画面は次のようになっています。

この画面で[OK]をクリックし設定を保存しましょう。

SNAT 画面に設定が追加されたことが分かります。

VebServer	追加
	編集
	削除

ポリシーの追加

ポリシーの追加から、HTTP の許可ポリシーを追加します。

ポリシー名は分かりやすいように「HTTP-Incoming」としておきましょう。送信元は Any-External です。

送信先のデフォルト設定を削除し、送信先の[追加]ボタンをクリックし追加します。

新規作成 ポリシーのプロパティ				
前: HTTP-Incomming				☑有
ペリシー プロパティ 詳細				
TTP-proxy 接続を				
許可 v TCP RS	Tの送信			
送信元				
₩ Any-Trusted				
Å.			追加 編集	出的余
遂信先 ————————————————————————————————————				
送信先 Any-External Route outbound traffic using SD-W SD-WAN Action	AN Based Routing V (Firew)	are OS v12.3 or high	〕追加… 」 編集… er)	削除
送信先 Any-External Route outbound traffic using SD-W SD-WAN Action	AN Based Routing (Firew)	are OS v12.3 or high	〕追加… 」 ar)	副除
送信先 Any-External Route outbound traffic using SD-W SD-WAN Action Application Control を有効にします:	AN Based Routing (Firew)	are OS v12.3 or high	〕追加… 」編集。 er)	副蜂
送信先 Any-External Route outbound traffic using SD-W SD-WAN Action Application Control を有効にします: Geolocation を有効にする	AN Based Routing V (Firewa Global Global V	are OS v12.3 or high	注度加 編集。 er)	削除
送信先 Any-External Route outbound traffic using SD-W SD-WAN Action Application Control を有効にします: Geolocation を有効化する ごのポリシーの IPS を有効にします 常期幅と時間クォータを有効化する に	AN Based Routing (Firewa Global Global V irewate OS v11 10. 2(85)	are OS v12.3 or high	〕注 如… 」 (注 加 …) ()	

SNAT の追加ボタンをクリックします。

Firebox Any-External			
Any-Trusted Any-Optional Any-BOVPN			
3皇为日	SNAT の追加	ユーザーの追加…	その他の追加…
択されたメンバーとこ	アドレス:		削除

SNAT 画面で、先ほど作成した負荷分散 NAT である「WebServer」を選択し、OK ボタンをクリックします。

NATまたはサーバー負荷分散アクションを追加、	編集、削除します。
/ebServer	······································
	編集
	削除

以下のアラートが出たら[はい]をクリックします。(他の送信先が入っていると削除されます)

Fireware	Policy Manager	×
	サーバー負荷分散はその他のアドレスと一緒に使用する。 これらのアドレスを削除しますか?	ことはできません。
	はい(Y) いいえ(N)	

送信先が選択できたので OK ボタンをクリックします。

■ R R R R R R R	kny irebox kny-External kny-Trusted			Í
	kny-Optional kny-BOVPN			
	3皇 700	SNAT の追加	ユーザーの追加	その他の追加
選択 さ	ちれたメンバーと	アドレス:		間限
N +++ ++	VebServer (サー Any-External Any-External Any-External	バーの負荷分散: ラウンド) -> 172.6.1.51 [1] -> 172.6.1.52 [1] -> 172.6.1.52 [1]	ロビン)	

ポリシーは以下のようになります。

f: HTTP-Incomming	
リジー プロパティ 詳細	
TTP-proxy 接続を	n n 164 ALL
	10)选择
送信元	
🔆 Any-Trusted	
	追加… 羅集 削除
	- AND - RANK
WebServer (サーハーの具荷分散: -	7926HE2)
Any-External> 1/2.16.1.51 [1]	
Any-External> 172.16.1.52 [1]	
Any-External> 172.16.1.53 [1]	
Any-External> 172.16.1.53 [1]	
Any-External> 172.16.1.53 [1]	2.8.10 調節 副修會
Any-External> 172.16.1.53 [1]	<u>追加</u> 爾莱 削除
Any-External> 172.16.1.53 [1]	LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
Any-External> 172.16.1.53 [1]	<u>追加</u> 福集 削除 AN Based Routing → (Fireware OS v12.3 or higher)
Any-External> 172.16.1.53 [1]	追加】 頭集 對除 AN Based Routing → (Fireware OS v12.3 or higher)
Any-External> 172.16.1.53 [1]	AN Based Routing 🧹 (Fireware OS v12.3 or higher)
Any-External> 172.16.1.53 [1]	<u>追加</u> 爾集 對除 AN Based Routing → (Fireware OS v12.3 or higher)
Any-External> 172.16.1.53 [1]	AN Based Routing (Fireware OS v12.3 or higher)
Any-External> 172.16.1.53 [1] Route outbound traffic using SD-WAN Action Application Control を有効にします:	AN Based Routing 《Fireware OS v12.3 or higher)
Any-External> 172.16.1.53 [1] Route outbound traffic using SD-W, SD-WAN Action Application Control を有効にします: Geolocation を有効化する	AN Based Routing 《Fireware OS v12.3 or higher) AN Based Routing 《Fireware OS v12.3 or higher) Global Global M M M M M M M M M M M M M
Any-External> 172.16.1.53 [1] □ Route outbound traffic using SD-WAN Action □ Application Control を有効にします: □ Geolocation を有効化する □ このポリシーの IPS を有効にします	AN Based Routing 《Fireware OS v12.3 or higher) AN Based Routing 《Fireware OS v12.3 or higher) Global Global M M M M M M M M M M M M M
Any-External →> 172.16.1.53 [1] Route outbound traffic using SD-WAN Action Application Control を有効にします: Geolocation を有効化する このポリシーの IPS を有効にします 帯域幅と時間クォータを有効化する (F	AN Based Routing 《Fireware OS v12.3 or higher) M M M M M M M M M M M M M M M M M M M
Any-External →> 172.16.1.53 [1] Route outbound traffic using SD-WA SD-WAN Action Application Control を有効にします: Geolocation を有効化する Conポリシーの IPS を有効にします 常城幅と時間クォータを有効化する (F	AN Based Routing (Fireware OS v12.3 or higher) AN Based Routing (Fireware OS v12.3 or higher) Global Global W D W D W D V = 212: HTTP-Client Standard
Any-External →> 172.16.1.53 [1] Route outbound traffic using SD-WAN Action Application Control を有効にします: Geolocation を有効化する このポリシーの IPS を有効にします 帯域幅と時間クォータを有効化する (F プロキシ アクションまたはコンテンツ ア・	AN Based Routing (Fireware OS v12.3 or higher) AN Based Routing (Fireware OS v12.3 or higher) Global Global W M M M M M M M M M M M M M

必要なら HTTPS ポリシーも同様に設定します。

ポリシーマネージャでは、追加された設定が以下のように表示されています。

ファイア	?ァイアウォール Mobile VPN with IPSec フィルタ:なし				~ 77	
順序 🗸	アクション	ポリシー名	ポリシーの種類	送信元	送信先	- - - - -
	0	TE FTB prover	ETD prove	Any Trusted, Any Optional	Any External	top:21
9	1	Mr HTTP-Incomming	HTTP	Any-External	Any-External	. tcp:80
8	Ø	HTTPS-Incommina	HTTPS-proxy	Anv-Trusted	Anv-External	tcp:443
	~	WatchGuard Certificate Portal	WG-Cert-Portal	Any-Trusted, Any-Optional	Firebox	tcp:4126
	~	🗢 WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080
	V 🖓 🖳	(c) Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
	V 🖓 🖳	DNS	DNS	Any-Trusted, Any-Optional	Any-External	tcp:53 udp:53
	Ø	POP3-proxy	POP3-proxy	Any-Trusted	Any-External	tcp:110 tcp:995 (tls)
	~	Search Watch Guard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118
D	V 🔎 🖳	Cutgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)
					445-1 5 5776381438444	

以上で負荷分散の設定は完了です。

複数 WAN

Firebox は外部ポートを複数(最大で4つのインターフェイス)構成することにより、負荷分散、可用性の向 上を図ることができます。

たとえば、

- インターネット閲覧の際のもたつきを解消したい
- VPN 接続のスループットの向上を図りたい
- 外部インターフェイスの接続が切れた際に別のインターフェイスにフェールオーバーしたい
- 片方のインターフェイスを外部からサーバーへのアクセスにし、もう片方を社内用と分けたい

といった場合のソリューションになります。

要件

- 複数 WAN に割り当てる外部インターフェイスにそれぞれの接続先があること
 2つ(以上)の ISP 接続契約、IP アドレスなど
- ミックスルーティングモードで構成すること

構成例

2 社の ISP(インターネット・サービス・プロバイダー)と契約し、Firebox のインターフェイス1と2を外部ポートとして複数 WAN を構成します。

動作モードはラウンドロビンで、負荷分散を行ないます。



ネットワークの設定

まずは構成例に基づいて、一つ目の外部インターフェイスを設定します。

インターフェイス名に他の外部インターフェイスと区別がつくように命名します。

インターフェイスの設定 - インター	7ェイス番号 0	;
IPv4 IPv6 セカンダリ MACア	·クセス制御 i¥細	
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	~

インターフェイス設定画面の下方に PPPoE 設定の箇所がありますので、PPPoE の使用にチェックを入れ、 ISP から提供された接続情報を入力します。

◉次の IP アドレスを使用:	203.0.113.1	
ユーザー名:	abc123@isp-01.net	
パスワード:	******	
パスワードの再入力:	*******	

インターフェイス1に2つ目の外部インターフェイスを同様に設定します。

ソターフェイス名 (エイリアス)・		
	External-2	
ンターフェイスの説明:		
ンターフェイスの種類:	外部	v
● PPPoE の使用		
○₽アドレスの自動取得		
⑤ 次の IP アドレスを使用:	203.0.114.1	~
ユーザー名:	xyz789@isp-02.net	
パスワード:	******	
パフロードの再しか。	******	
1.X.2 T 0HXD.		
MAY TOMAN.		詳細プロパティ
AXY TOHAD.		詳細プロパティ
TrustedとOptionalも設定すると、ネットワーク構成の画面は次のようになります。

上記の設定で外部インターフェイスも2つ構成されています。

ンターフェ	名前 (エイリアス)	種類	IPv4 アドレス	IPv6 アドレス	NIC 構成	構成
0	External-1	外部	PPPoE		自動ネゴシエート	
1	External-2	外部	PPPoE		自動ネゴシエート	
2	LANT	無効			自動ネコジエート	
3	LAN2	無効			自動ネゴシエート	
4	LAN3	無効			自動ネゴシエート	
5	Optional-4	無効			自動ネゴシエート	
6	Optional-5	無効			自動ネゴシエート	

以上で複数 WAN を設定する準備ができました。

複数 WAN の設定

同じくネットワーク構成の「複数 WAN」のタブを選択します。

		22 VIAN	一ルーフバック	Bridge Protoco	IS WINS/DNS	; 動的 DNS	複数 WAN	Link Monitor	SD-WAN	PPPoF
的 WAN 接 rt						-				
◎∞ いつい 117∞ 複数の外部インターフェイスの間で≢	≢ IPSec トラ	フィックを川	ーティングす	る方法を選択しま	す。[構成] を2	フリックする	と、その他の	つプロパティを	を設定できまう	す。
ルーティング テーブル	→ 構成									
スティッキ-接続										
FCP、UDP、およびその他の (非 TCP	非 UDP) ブ	ロトコルのス	ティッキー接筆	抗間隔を設定しま	₫.					
TCP スティッキ-接続:	3 🌲	分 🕹								
JDP スティッキ-接続:	3 🗘	分 ~								
その他のスティッキ-接続:	3 🗘	分 ~								
复数 WAN フェールオーバー イベン フェイスに自動的に送信されます。D	トが発生し、 Pクティブな	元のインター (非 IPSec 接	フェイスが再。 たについては、	度使用できるよう Firebox で使用す	になった場合 るオプション	は、 Firebox を選択します	によって新し 、	、い接続すべて	てが元のイン	9-
即時フェールバック:アクティブな	接続のすべる	でを直ちに停	とします。			~				
⊣ン=1.5ax cxaa≫ すべての複数 WAN イベントがログド	自動的に記録	まされます。	(通知] をクリッ	クすると、複数	WANイベント	の通知設定	を構成できま	す.		
通知										

複数 WAN 構成のセクションでラウンドロビンを選択します。

/ダーフェイス	リンクアグリゲーショ	ノ ブリッジ	VLAN	ループバック	Bridge Protocols	WINS/DNS	動的 DNS	複数 WAN	Link Monitor	SD-WAN	PPPoE

ラウンドロビンの振る舞いを設定するために、構成ボタンをクリックします。

VLAN ループバック	Bridge Protocols	22.00 Alexandra					
	minade i transionio	WINS/DNS	動的 DNS	複数 WAN	Link Monitor	SD-WAN	PPPoE
		mitorento	2747 0110		Entre informed	00-11/41	TITOL
クをルーティングする	方法を選択します。	[構成]をクリ	リックする.	と、その他の	プロパティを	設定できま	す。
	ゥクをルーティングする	・クをルーティングする方法を選択します。	・クをルーティングする方法を選択します。[構成]]をク!	・クをルーティングする方法を選択します。[構成] をクリックする	- クをルーティングする方法を選択します。[構成] をクリックすると、その他の	・ クをルーティングする方法を選択します。[構成]をクリックすると、その他のプロパティを	・ クをルーティングする方法を選択します。[構成]をクリックすると、その他のブロバティを設定できま

複数 WAN ラウンドロビン構成が開きます。ここではインターフェイスの重み付けの設定ができます。

構成ボタンをクリックします。

きめる	インターフェイス	重み付け	構成
	External-1 (0)	1	-

ラウンドロビンの重み付けの画面が開きます。

ます。
, 11,

重み付けの計算方法は以下のとおりです。

- 1. 構成例ですと一つは 100Mbps、もう一つは 1Gbps なので、整数にならして単位をそろえます
 - ➤ インターフェイス 0 は 100Mbps、インターフェイス 1 は 1000Mbps です
- 2. 比例式で最小通信速度を1とした比率を割り出します
 - ▶ [100:1000]なので[1:10]という比率になります
- 3. 重み付けは External-1 が 1、External-2 が 10 になります

External-1 の重み付け



External-2 の重み付け

🔩 ラウンドロビンの重み付け			×
インターフェイス External-	2のラウンドロ	モンの重	みを入力します。
10 🜩			
	0	К	キャンセル

設定後、ラウンドロビンの構成は以下のようになっています。

₿める	インターフェイス	重み付け	構成
	External-1 (0)	1	
	External-2 (1)	10	

動作確認

Firebox System Manager のトラフィックモニタで確認することができます。

http でフィルタリングして、クライアント PC から Web アクセスします。下の図は負荷テストツールで大量の HTTP アクセスを生成した際のログです。

パケットが通過する際に、外部インターフェイスの External-1 と External-2 の両方が使用されていることが 分かります。

Firebox System Manager	10.0.1.1 [接続済み]				1	- 0	×
	1						
プロックされたサイト フロントパネル	ヤキュリティサードス トラフィック モニタ	ゲートウェイ ワイヤレス コント 帯域幅メーター	ローラ S サービス ウォッチ	D-WAN	トラフィック管理 ステータス レポート	ユーザー ク 認証	ォータ リスト
💽 😤 😕 🖾 💥 📈				htt	p	~ 👂 •	×
2019-06-21 15:54:37 Allow 1 2019-06-21 15:54:40 Allow 1 2019-06-21 15:54:40 Allow 1 2019-06-21 15:54:44 Allow 1 2019-06-21 15:54:46 Allow 1 2019-06-21 15:54:51 Allow 1 2019-06-21 15:54:51 Allow 1 2019-06-21 15:54:53 Allow 1 2019-06-21 15:54:53 Allow 1 2019-06-21 15:54:56 Allow 1 2019-06-21 15:55:00 Allow 1 2019-06-21 15:55:00 Allow 1 2019-06-21 15:55:10 Allow 1 2019-06-21 15:55:27 Allow 1 2019-06-21 15:55:36 Allow 1 2019-06-21 15:55:36 Allow 1 2019-06-21 15:55:37 Allow 1 2019-06-21 15:55:37 Allow 1 2019-06-21 15:55:36 Allow 1	0.0.1.2 20.184.14.47 http 0.0.1.2 13.107.136.9 http 0.0.1.2 13.107.136.9 http 0.0.1.2 13.107.42.12 http 0.0.1.2 05.52.108.76 http 0.0.1.2 20.190.141.193 h 0.0.1.2 13.107.42.12 http 0.0.1.2 13.107.43.26 http 0.0.1.2 104.47.43.26 http 0.0.1.2 104.47.43.26 http 0.0.1.2 104.47.93.16 http 0.0.1.2 13.107.136.9 http 0.0.1.2 52.114.158.91 htt 0.0.1.2 52.114.158.91 htt 0.0.1.2 52.114.158.91 htt 0.0.1.2 13.107.136.9 http 0.0.1.2 13.107.136.9 http 0.0.1.2 13.107.136.9 http 0.0.1.2 13.107.136.9 http 0.0.1.2 52.114.158.91 htt 0.0.1.2 52.114.158.91 htt 0.0.1.2 52.114.158.91 htt 0.0.1.2 52.98.64.50 https 0.0.1.2 52.98.64.50 https 0.0.1.2 52.98.64.50 https	sitcp 4352 443 2-Trusted sitcp 4355 443 2-Trusted sitcp 4358 443 2-Trusted sitcp 4380 443 2-Trusted sitcp 4381 443 2-Trusted sitcp 4381 443 2-Trusted sitcp 4384 443 2-Trusted sitcp 4386 443 2-Trusted sitcp 4386 443 2-Trusted sitcp 4388 443 2-Trusted sitcp 4389 443 2-Trusted sitcp 4392 443 2-Trusted sitcp 4396 443 2-Trusted sitcp 4397 443 2-Trusted sitcp 4397 443 2-Trusted sitcp 4397 443 2-Trusted sitcp 4392 443 2-Trusted sitcp 4394 443 2-Trusted sitcp 4426 443 2-Trusted sitcp 4426 443 2-Trusted sitcp 4426 443 2-Trusted sitcp 4432 443 2-Trusted 1 itcp 4463 443 2-Trusted 1	D-External-1 A D-External-1 A D-External-1 A D-External-1 A D-External-1 A D-External-1 A D-External-2 A D-External-2 A D-External-2 A D-External-2 A D-External-1 A D-External-2 Ap External-2 Ap	pication ider oplication ider	tified 1500 112 (Ou tified 2744 127 (Ou tified 291 127 (Our tified 1500 118 (Ou tified 1500 118 (Ou tified 1500 118 (Ou tified 1500 118 (Ou tified 291 127 (Our tified 2445 127 (Our tified 2445 127 (Our tified 254 127 (Our tified 1500 118 (Our tified 1454 63 (Our tified 1454 63 (Our tified 1500 117 (Our tified 1454 63 (Our t	utgoing-00) utgoing-00) going-00) ytgoing-00) utgoing-00) ytgoing-00) going-00) ytgoing-00) <	proc ^ proc _ proc _
更新間隔: 5秒		一時停止					

第三章 UTM 機能

WSM 基本設定ガイドでは WebBlocker、Gateway Anti-Virus、spamBlocker、Intrusion Prevention Service(IPS)、Reputation Enabled Defense (RED) について解説しましたが、本書では Application Control の設定方法について紹介します。

Application Control

アプリケーション・コントロールは、文字通り、社内で使用される可能性があるアプリケーションを制御しま す。プロトコルは何か、ブラウザベースか否かに関係なく、アプリケーションの振る舞いや特徴を検知して、 その利用方法を細かく管理することができます。これにより、私的目的のネットワーク利用を制限したり、情 報漏洩を防いだりすることができます。

このセクションでは、ファイル転送サービスの制御を想定し、設定方法を解説します。

ポリシーと Application Control アクションの紐付け

ポリシーマネージャから Outgoing ポリシーをダブルクリックして開きます。

建し ファイア	L 🗁 🖷 🛛 🏹 ウォール Mobil	+ 🗙 🖞 💐 🍇 🏛 🚚 le VPN with IPSec	***	?				
				7	ィルタ:なし		~ 7	7
順序/	アクション	ポリシー名	ポリシーの種類	送信元		送信先		
1 2 3 4 5 6 7 8 9		 FTP-proxy HTTP-Incomming HTTPS-Incomming WatchGuard Certificate Portal WatchGuard Web UI Ping DNS POP3-proxy WatchGuard 	FTP-proxy HTTP HTTPS-proxy WG-Cert-Portal WG-Fireware-XTM-WebUI Ping DNS POP3-proxy WG-Eirebox Mont	Any-Trusted, Any-Optional Any-External Any-Trusted Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted, Any-Optional Any-Trusted	Any-External Any-Trusted Any-Trusted Firebox Firebox Any Any-External Any-External Eirebox			
10		Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External			

「Application Control を有効にします」のチェックを入れます(①)。

このポリシーに、後で作成する Application Control のアクションを横のドロップダウンリスト(②)をから選択 することによってポリシーとアクションが紐付き、目的のアプリケーションを制御ようになります。

前:Outgoing	
ポリシー フロオニス 5米細	
TCP-UDP接続を…	-
計 り V TCP RSTの送信	ä
送信元	
Any-Trusted	
2 Any-Optional	
	追加 編集
A2 18 76	
Anv-External	
Any-External	
Any-External	
Any-External	<u>注血加</u> 編集
Any-External	<u>追加</u> 猫集 崔明殊 sed Routing 《Fireware OS v12.3 or higher)
Any-External Route outbound traffic using SD-WAN Base SD-WAN Action	〕追加 編集 削除 sed Routing (Fireware OS v12.3 or higher)
Any-External Route outbound traffic using SD-WAN Bat SD-WAN Action	追加 編集 HUD 余 sed Routing (Fireware OS v12.3 or higher)
Any-External Route outbound traffic using SD-WAN Base SD-WAN Action	这加 編集 尚明 sed Routing (Fireware OS v12.3 or higher)
Any-External Any-External Route outbound traffic using SD-WAN Base SD-WAN Action C	追加 編集 肖明 sed Routing (Fireware OS v12.3 or higher)
Any-External Route outbound traffic using SD-WAN Base SD-WAN Action 2 Application Control を有効にします: Glob	追加 編集 削除 sed Routing (Fireware OS v12.3 or higher)
Any-External Route outbound traffic using SD-WAN Bat SD-WAN Action 2 Application Control を有効にします: Glob Glob Glob	道加 編集 謝除 sed Routing (Fireware OS v12.3 or higher) aal () 》 》
 Any-External Route outbound traffic using SD-WAN Bas SD-WAN Action ② ② ✓ Application Control を有効にします: Glob ✓ Geolocation を有効化する ✓ このポリシーの IPS を有効にします 	注意加 編集
 Any-External Route outbound traffic using SD-WAN Bas SD-WAN Action Application Control を有効にします: Glob Geolocation を有効化する Glob このポリシーの IPS を有効にします 帯域幅と時間クォータを有効化する (Firewar 	建加 編集 前除 sed Routing (Fireware OS v12.3 or higher) al pal Pal
 Any-External Route outbound traffic using SD-WAN Bar SD-WAN Action Application Control を有効にします: Glob Geolocation を有効化する Glob このポリシーの IPS を有効にします 帯域幅と時間クォータを有効化する (Firewar 	注血加 編集 前明 sed Routing (Fireware OS v12.3 or higher) ① al · · · · · · · · · · · · · · · · · · ·
Any-External Route outbound traffic using SD-WAN Base SD-WAN Action ② ② Application Control を有効にします: Glob Geolocation を有効化する Glob ご このポリシーの IPS を有効にします 常転幅と時間クォータを有効化する (Firewar プロキシ アクション:	iù 加 編集 前明 sed Routing (Fireware OS v12.3 or higher) al 《 節 節 al 《 節 節 al 《 節 節

Outgoing ポリシーと紐付けるのは、Application Control の機能がプロトコル(ポート番号)に関係なく、全通 信を対象にしてアプリケーションを判別し、制御するからです。

どのプロトコルか確定していれば、その特定のポリシーで Application Control を有効にすることもできます。

特に Outgoing よりも上位に定義されているポリシーがあれば、そのポリシーでも Application Control を有 効にする必要があります。

では実際に Application Control のアクションを作成してみましょう。

ファイル転送サービスを制御する

ファイル転送サービスは便利ですが、情報漏えいにつながるリスクもあります。

この項では、ファイル転送サービスは原則禁止、しかし顧客とのファイルのやりとりに Dropbox を使うという ことになり、それだけを許可するケースを想定し、設定します。

ポリシーマネージャのメニュー <u>セキュリティサービス</u> – <u>Application Control</u> をクリックします。

C:¥U	sers¥tsuto¥Doc	uments¥My WatchGuard¥configs	¥T50-W-MA	Y29.xml- Fireware Policy Manage	r		-		×
ファイル	編集 表示 セ	ットアップ ネットワーク FireClust	ter VPN 🛧	キュリティサービス ヘルプ	_				
2	🖻 🖷 🕅 🕅	+ 🗙 🐺 🧶 🍇 🗈 🚚	💰 🍯 🛛	Application Control					
ファイア	ウォール Mobile	VPN with IPSec		APT Blocker					
				ボットネット検出		(11-75), 45-1			. 7
				Data Loss Prevention		11/2. 40			.
順序 △	アクション	ポリシー名		DNSWatch	送信元		送信先		
1	Ø 🔊	EFTP-proxy	FTP-pro	Gateway AntiVirus	Any-Optional	Any-External			
2	ó	HTTPS-Incomming	HTTPS-	Geolocation		Any-Trusted			
4	1	WatchGuard Certificate Portal	WG-Cer	Intrusion Prevention	Any-Optional	Firebox			
5		WatchGuard Web UI	WG-Fire	モバイル セキュリティ	Any-Optional	Firebox			
6			DNS	Quarantine Server	Any-Optional	Any Any-External			
8	0	POP3-proxy	POP3-p	Reputation Enabled Defense		Any-External			
9	1	WatchGuard	WG-Fire	anamBlacker	Any-Optional	Firebox			
10	V 🖓 🖳	Outgoing	TCP-UD	spamblocker	Any-Optional	Any-External			
				Threat Protection					
<				WebBlocker	>				>
							Fir	eware OS	v12.4.0

アクションの一覧画面が開きます。[追加]をクリックして、アクションを作成しましょう。

アクション	アプリケーション	ポリシー DNC ETD account Output	追加
510081	Crypto Admin Bypass F	-1 DNS, FTP-proxy, Outgol	複製…
			編集

ここではファイル共有サービスすべてが対象になりますので、カテゴリ別の表示に切り替えます。

名前: AppControl.1					
光明 :					
~					
● すべてのアプリケー	ションを表示			17 V.	
◯ 構成済みアプリケー	ションのみを表示 カテゴリ:	すべて	~	検索:	
カテゴリ	アプリケーション	動作	アクション		
Business tools	Aspera FASP	Transfer			
Business tools	Citrix	Authority, Access			
Business tools	Directi	Access			
Business tools	Docker	Access			
Business tools	Eastmoney	Authority, Access			
Business tools	IBM HTTP	Access			
Business tools	Microsoft Office	Access			
Business tools	Microsoft Office 2013 license	Access			
Business tools	Microsoft Office 365	Authority			
Business tools	Microsoft OS license	Access			
Business tools	Microsoft Remote Web Workpla	ice Access			
Business tools	Microsoft Store	Access			
Business tools	Radacct RADIUS	Access			
Business tools	Skype for Business	Access			
Business tools	WatchGuard Authentication Ac	Access			
Business tools	WatchGuard CLI	Access			
Business tools	WatchGuard external Webbloc	k Access			
Business tools	WatchGuard Security Event Pro	o Access			
Business tools	WatchGuard Web Management	UIAccess			
Business tools	WatchGuard Webblocker datab	Access			
	WatchGuard W/SM Mananemen	t Access	_		
カテゴリ別で選択			アクショ	ンをクリアする	編集
アプリケーションが一致	しない場合: グローバルアクションな	を使用 🗸 🗸			
	1.:				

カテゴリで File Sharing services and tools をチェックし、切断を選択します。

Business tools	切断	~	Database tools	切断	
Email messaging services	切断	4	File sharing services and tools	切断	~
Instant messengers	切断	4	Investment platforms	切断	÷
Management tools and protocols	切断	~	Media streaming services	切断	с. У
Network Protocols(1)	切断	×.	Network Protocols(2)	切断	~
Network Protocols(3)	切断	\sim	Online games	切断	~
Peer-to-peer networks	切断	~	Private protocols	切断	~
Remote access terminals	切断	с.	Security update tools	切断	
] Social networks	切断	~	Tunneling and proxy services	切断	~
VoIP services	切断	4	Web instant messengers	切断	*
Web services	切断	4			

OKをクリックして、新規アクションの追加画面に戻ります。

構成済みのアプリケーションのみを表示 をクリックすると、ファイル転送サービス関連のアプリケーションす べてが切断になっていることが確認できます。

名前はアクションの内容を表わすわかりやすいものに編集してください。ここでは「FileTransferCtrl」とします。

各前: FireSharingCtrl			
# 8A +			
○ すべてのアプリケーションを	·表示		
● 構成済みアプリケーションの)みを表示 カテゴリ	: রম্ব	→ 検索:
カテゴリ	アプリケーション	動作	アクション
File sharing services and tools	0zz0	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	BIZHARD	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	Box	Authority, Transfer, Acces	as切断 (カテゴリ別)
File sharing services and tools	DBank	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	Dropbox	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	FTP Applications	Authority, Communicate, T.	切断 (カテゴリ別)
File sharing services and tools	GetRight	Transfer	切断 (カテゴリ別)
File sharing services and tools	Google Drive	Access	切断 (カテゴリ別)
File sharing services and tools	iCloud	Authority, Transfer, Acces	ss切断 (カテゴリ別)
File sharing services and tools	Kuaipan	Authority	切断 (カテゴリ別)
File sharing services and tools	Mediafire	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	MEGA	Access	切断 (カテゴリ別)
File sharing services and tools	Naver Cloud	Authority, Transfer, Acces	ss切斷 (カテゴリ別)
File sharing services and tools	NextCloud	Access	切断 (カテゴリ別)
File sharing services and tools	NFS	Access	切断 (カテゴリ別)
File sharing services and tools	OneDrive	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	Sugarsync	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	TeamBeam	Access	切断 (カテゴリ別)
File sharing services and tools	UPlusBox	Authority, Access	切断 (カテゴリ別)
File sharing services and tools	WD My Cloud	Access	切断 (カテゴリ別)
File sharing services and tools	Web File Transfer	Transfer	切断 (カテゴリ別)
File sharing services and tools	Wetransfer	Authority, Transfer, Acces	ss切断 (カテゴリ別)
カテゴリ別で選択			アクションをクリアする 編集
アプリケーションが一致したい地	合: グローバルアクショ	つを使用 🗸	
//////////////////////////////////////		a chemi a a	

では、Dropbox だけ使用可能にしましょう。Dropbox をダブルクリックし、構成画面を開きます。

「すべての動作にアクションを設定する」にチェックを入れ、許可を選択します。

マフリケーション	Dropbox	
カテゴリ	File sharing services ar	nd tools
● すべての動作にな	アクションを設定する	許可
		+ z
○すべくの指定の譬	の1年にアクションを設定 9	10
) g へ c の相定の Authority	切断	10 V
) すべての相定の Authority	切断	с. С

この画面では更に細かい制御も可能で、例えば「ファイルのアップロードは禁止し、受け取り(ダウンロード) のみ許可する」といった設定もできます。

Authority を許可するとフィアルのアップロードが可能になってしまいますので切断、そしてダウンロードは可能にするため、Access を許可の設定にします。

アプリケーション	Dropbox	
カテゴリ	File sharing services a	nd tools
○すべての動作にな	アクションを設定する	許可
o + w +		
● すべての指定の語	b作にアクションを設定?	する
● すべての指定の ■ Authority	助作にアクションを設定 ? 切断	f 3 ~
● すべての相定のま ✓ Authority ✓ Access	か作にアクションを設定: 切断 許可	f 3 ~ ~

このように必要に応じて、きめ細かな制御をすることが可能です。

すべて OK で抜けて、ポリシーマネージャの画面に戻ります。

アクションのカラムに Application Control が有効になったことを示すアイコンが表示されています。

この状態で Outgoing ポリシーをダブルクリックして開きます。

注 ファイア	. 🗁 🖷 🛛 🏹 ウォール 🛛 Mobi	+ 🗙 💱 🗶 🗽 🗊 🚚 le VPN with IPSec	🏄 🤲 🖳 🖉 🖾 🖉	?				
				7	ィルタ:なし		×	P 7
順序/	アクション	ポリシー名	ポリシーの種類	送信元		送信先		
1	0 💭	ETP-proxy	FTP-proxy	Any-Trusted, Any-Optional	Any-External	1000 CARANTONIS		
2	1	WTTP-Incomming	HTTP	Any-External	Any-Trusted			
3	0	HTTPS-Incomming	HTTPS-proxy	Any-Trusted	Any-Trusted			
4	1	WatchGuard Certificate Portal	WG-Cert-Portal	Any-Trusted, Any-Optional	Firebox			
5	1	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox			
6		(c) Ping	Ping	Any-Trusted, Any-Optional	Any			
7		DNS	DNS	Any-Trusted, Any-Optional	Any-External			
8	0	POP3-proxy	POP3-proxy	Any-Trusted	Any-External			
9	1	🗢 WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox			
10		Cutoping	TCP-UDP	Any-Trusted Any-Optional	Any-External			

Application Control を有効にします のチェックの横のドロップダウンリストで、先ほど作成したアクションを 選択します。

編集 ポリシーのプロパティ				×
前: Outgoing				☑ 有効
files and starting				
パリシー フロバティ 詳細				
TCP-UDP 接続を	TOP DOT ON WAT			
***	TCP RS10)透信			~
Any-Trusted				
			追加 編集	削除
送信先				
Route outbound traffic using	SD-WAN Based Routing \lor (Firew	vare OS v12.3 or higher)	追加 福朱	削除
SD-WAN Action	 Image: Second sec			
☑ Application Control を有効にし ☑ Geolocation を有効化する ☑ このポリシーの IPS を有効にし 常磁幅と時間クォータを有効に	ます: FireSharingCtrl マ Global FireSharingCtrl まする (Fireware OS v11.10 以降)			
プロキシ アクション:	~			
		ОК	キャンセル	ヘルブ

[OK]で抜けてポリシーマネージャに戻ると Outgoing ポリシーの App Control の列に選択したアクション名 が表示されています。この状態で設定を保存すると、ファイル転送サービスに対する制御が動作します。

🚊 🛓 ファイア	🕻 🗁 🖷 🛛 🏹 'ウォール Mobi	+ 🗙 🖞 💐 🎼 🛍 🚚 le VPN with IPSec	🎄 🍂 🖳 🧶 🔗 🗖 🖓	. ?				
						フィルタ: なし		~ 77
順序 ニ	アクション	ポリシー名	ポリシーの種類	送信元	递信先	ポート	PBR SD-WAN	App Contro
	0 💭	E FTP-proxy	FTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:21		Global
	1	W HTTP-Incomming	HTTP	Any-External	Any-Trusted	tcp:80		なし
	0	HTTPS-Incomming	HTTPS-proxy	Any-Trusted	Any-Trusted	tcp:443		なし
	1	WatchGuard Certificate Portal	WG-Cert-Portal	Any-Trusted, Any-Optional	Firebox	tcp:4126		なし
	1	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080		なし
		Ping Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)		Global
	V 🎝 🛄	DNS	DNS	Any-Trusted, Any-Optional	Any-External	tcp:53 udp:53		Global
	0	POP3-proxy	POP3-proxy	Any-Trusted	Any-External	tcp:110 tcp:995 (tls)		なし
	1	🗢 WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118		なし
0		Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)		FireSharingCtr

動作確認です。OneDrive ではアップロードできません。



ログを見ればファイル転送を切断していることが分かります。

S Firebox System Manager - 10.0.1.1 [接張语み]	- П X
フロントパネル トラフィックモニタ 帯域幅メーター サービス ウォッチ ステータス レポート 認証リスト ブロックされたサイト セキュリティサービス ゲードウェイ ワイヤレス コントローラ SD-WAN トラフィッグ	管理 ユーザー クォータ
Directive 🖉 🗟 🐲 📈	v 🔎 🔻 🗙
2019-06-26 12/07/38 Dary 10.01 2 13 107 42 12 https//cp.3339 443 2-Trusted 1-External-2 Application identified 1454 119 (Outpoing-OII) proc. id="firewall" rc="101" msg. id="	3000-0149" src. ip. nat="172.16.1
2019-06-26 12:07:38 Deny 10.0.1.2 13:107.42.12 https/tcp 3340 443 2-Trusted 1-External-2 Application identified 1454 119 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3"	3000-0149" src_ip_nat="172.16.1
2019-06-26 12:07:38 Deny 10.0.1.2 13:107.42.12 https/tcp 3341 443 2-Trusted 1-External-2 Application identified 1454 119 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="172.16.1
2019-06-26 12:18:20 Deny 10.0.1.2 13:107.42.12 https://cp.4104.443.2-Trusted 1-External-2 Application identified 1454.119 (Outgoing-00) proc_id="firewall" rc="101" msg_id="	3000-0149" src_ip_nat="172.16.1
2013-06-26 12/18:20 Deny 10.01.213:107.42.12 https://doi.org/10.1117/02.12.11117/02.01117/02	2000-0149" src_ip_nat="172.16. 2000-0140" ere_ip_pat="172.16.1
	"3000-0149" src in nat="10.168
2019-06-26 12:26 21 Dem 10.0.1.2 40.90.142.230 https://co.uk/astro-feed/astro	"3000-0149" src ip nat="10.168
2019-06-26 12:26 22 Deny 10.0.1.2 40.90.142.230 https/tcp 4695 443 2-Trusted 0-External-1 Application identified 2960 101 (Outgoing-00) proc_id="firewall" rc="101" msg_id="	"3000-0149" src_ip_nat="10.168
2019-06-26 12:26:24 Deny 10.0.1.2 13.107.42.12 https/top 4697 443 2-Trusted 0-External-1 Application identified 1500 118 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="10.168.(
2019-06-26 12:26:24 Deny 10.0.1.2 13.107.42.12 https/top 4698 443 2-Trusted 0-External-1 Application identified 1500 118 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="10.168.(
2019-06-26 12:26 24 Demy 10.01.2 13:107.42.12 https/tp 4699 443 2-Trusted 0-External-1 Application identified 1500 117 (Outgoing-00) proc_id="firewall" rc="101" msg_id="2"	3000-0149" src_ip_nat="10.168.6 2000-0140" ere_in_not="10.460.4
2019-06-26122.26 /4 Demy 10.01.213.107.42.12 https://p 4/00 443 2-frusted 0-External-1 Application identified 1500 118 (Outgoing-00) proc_id="interval" rc=101" msg_od=20 0010.06.2123624 Demy 10.01.213.107.4212 https://pack.action.actio	3000-0149" src_ip_nat="10.168.5 2000-0149" erc_ip_pat="10.168.4
2019-00-2012-2024 Deny 10.01.213.017.42.12 https://provide.org/active/acti	3000-0149 src_ip_nat=10.100.
2019-06-26 12 26 24 Denv 10.0.1.2 13 107.42 12 https://commons.org/additional-additiona	3000-0149" src_ip_nat="10.168.5
2019-06-26 12:26:24 Deny 10.0.1.2 13:107.42.12 https/top 4704 443 2-Trusted 0-External-1 Application identified 1500 118 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="10.168.t
2019-06-26 12:26:24 Deny 10.0.1.2 13.107.42.12 https/top 4705 443 2-Trusted 0-External-1 Application identified 1500 117 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="10.168.(
2019-06-26 12:28:33 Deny 10.0.1.2 13.107.42.12 https/top 4836 443 2-Trusted 0-External-1 Application identified 1500 118 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="10.168.(
2019-06-26 12/28/33 Denv 10.0.1.2.13.107.42.12 https://com/doi.org/10.117/001going-000 proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="10.168.6
2019-06-26 12/28/33 Deny 10.01.213/107/42/12 https://dx.adu/2019/06/2019/2019/06/26 12/28/33 Deny 10.01.213/107/42/12 https://dx.adu/2019/06/26 12/28/33 Deny 10.01.213/107/42/12 https://dx.adu/2019/06/26 12/28/33 Deny 10.01/27/28/33 Deny 10.01/27/28/33 Deny 10.01/27/28/33 Deny 10.01/27/28/33 Deny 10.01/27/28/33 Deny 10.01/28/28/28/28/28/28/28/28/28/28/28/28/28/	3000-0149" src_ip_nat="10.168.3
2019-00-2012 31:55 Deny 10.01.213.107.42.12 https://pb.022.443.2-Trusted 1-External-2 Application Identified 1454-119 (Outgoing-00) proc_id="invariant" rc="101" msg.id="	3000-0149 sit_ip_nat=172.10. 3000-0149" src_in_nat="172.16.1
2019-06-26 12:31-53 Denv 10.0.1.2.13.107.42.12 https://doi.org/10.1213.107.42.12 https://doi.org/10.1213.107.4212 https://doi.org/10.1213.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107.4123.107	3000-0149" src ip nat="172.16.
2019-06-26 12:32:12 Deny 10.0.1.2 13:107.42.12 https/tcp 5082 443 2-Trusted 1-External-2 Application identified 1454 119 (Outgoing-00) proc_id="firewall" rc="101" msg_id="3	3000-0149" src_ip_nat="172.16.1
2019-06-26 12:32:12 Deny 10.0:1.2 13:107.42:12 https/top 5083 443 2-Trusted 1-External-2 Application identified 1454 119 (Outgoing-00) proc_id="firewal" rc="101" msg_id="3	3000-0149" src_ip_nat="172.16.1
2019-06-26 12:32:12 Deny 10:0.1.2 13:107.42.12 https/tcp 5084 443 2-Trusted 1-External-2 Application identified 1454 119 (Outgoing-00) proc_id="firewail" rc="101" msg_id="3	3000-0149" src_ip_nat="172.16.1
٤	>
更新問題 5秒 🗸 一時停止	

行末のほうを見ると、ファイル転送であると検知してブロックしていることが確認できます。

app_name= onebnike app_cat_id= o app_cat_name= internet internet		abb_
app_name="OneDrive" app_cat_id="3" app_cat_name=/File sharing services and too	ols" ap	pp_b
app_name="OneDrive" app_cat_id="3" app_cat_name="File sharing services and too	ols" ap	pp_b
" app_name="OneDrive" app_cat_id="3" app_cat_name="File sharing services and to	ols' a	app_
" app_name="OneDrive" app_cat_id="3" app_cat_name="File sharing services and to	ols' a	app_
" app_name="OneDrive" app_cat_id="3" app_cat_name="File sharing services and to	ools' a	app_
" app_name="OneDrive" app_cat_id="3" app_cat_name="File sharing services and to	ools' a	app_
" app_name="OneDrive" app_cat_id="3" app_cat_name="File sharing services and to	ools' a	app_
" ann name-"AneDrive" ann cat id-"3" ann cat name "File sharing services and to	nole i s	ann

Dropbox では設定で許可したので、ファイルのアップロードができています。

Dropbox > Documents	la ta ta 🥔	自 Q.検索	
ファイル名 エ	種类類	更新	
WSM基本設定ガイドv3.docx	ドキュメント	1 秒前	
○ いいまままのつお // っしっ オー・オー・ゴロ・コーナーナ	2**m++		
⊘ WSM基本設定ガイドv3.docxをアップロードしました。	詳細を表示		×

APT Blocker

今日、サイバー攻撃はますます複雑で巧妙になっており、特定の組織の情報や資産を狙って行なわれる攻撃は標的型攻撃と呼ばれています。攻撃方法も多様であり、攻撃に使われるウィルスやマルウェアも無数の亜種が存在します。攻撃が来た時点で未知のものであることも珍しくありません。そうした新たな脅威に対応するために、APT Blocker は非常に効果的なソリューションです。

APT Blocker の有効化

Policy Manager のメニュー <u>セキュリティサービス</u> — <u>APT Blocker</u> をクリックします。



まず、APT Blocker の有効化にチェックを入れます。

するとグレーアウトしていた画面がアクティブになるので、脅威レベルに応じたアクションを設定してください。必要に応じてログとアラームのチェックを入れます。

APT Blocker Φ ²	有効化					
骨感アクション	ポリシー 詳細					
春威レベル	アクション	アラーム	D7			
高	切断 🗸					
÷	切断 🗸		\square			
低	許可 🗸 🗸					
クリーン	許可)	-	
通知の設定	通知: なし					

図の例では、脅威レベルが高および中 の場合に通信を切断するアクションに しています。

また、切断の時にログを出力するよう にチェックを入れています。

ポリシーへの適用

どのポリシーで APT Blocker を有効にするかは、ポリシー タブで設定できます。

デフォルトでは、すべてのポリシーで無効¹になっていることが確認できます。

「感アクション」ポ	비한는 Advanced	7.02(-)10(240
ポリシー名	プロキシの種類	APT
HTTP-proxy	HTTP	無効
POP3-proxy	POP3	無効
SMTP-proxy	SMTP	無効
Q APT Blocker に	t、Gateway AntiVirus が	有効になっている;
リシーにのみ	有効にすることができま?	す。

ポリシーに適用するには、有効にしたいポリシーを選択し、右上のアクションの選択 ドロップダウンリストか ら「有効」をクリックします。

≹威アクション	ポリシー	Advanced	
			アクションの選択 🤜
ポリシー名		プロキシの種	★ アクションの選択
HTTP-proxy		HTTP	有効
POP3-proxy		POP3	無効
SMTP-proxy		SMTP	無効
SMTP-proxy		SMIP	無効

^{1 12.4.1} ではあらかじめすべて有効になっています。この例ではすべて無効になっています。

※ この一覧に表示されていないポリシーは、Proxy ポリシーが作成されていないか、Proxy ポリシーが あっても Gateway AntiVirus が有効になっていません。再度設定を見直してください

目的のポリシーで有効化したら、OK ボタンをクリックし、Policy Manager で設定を保存してください。

		アクションの選択	択
ポリシー名	プロキシの種類	APT	
TP-proxy	FTP	有効	
111Р-ргоху	IntiP	11 X/I	

設定を保存すると、APT Blocker が有効になります。

第四章 ユーザーインターフェイス

Firebox を管理するためのインターフェイスは3種類あります。管理者の方には、設定項目に制限がなく周辺ツールも充実した WSM を推奨しています。

しかし、本格的な WebUI と CLI も備えています。

この章では CLI の使い方を解説します。WebUI については、別途 WebUI ガイドをご覧いただきたいと思いますが、ここでは WebUI ガイドで触れていない Tips と便利な使い方をご紹介します。

CLI

CLI ではターミナルソフトでログイン後、それぞれのモードに入り、設定情報の取得や各種設定ができます。



次に接続方法、設定方法を解説します。

接続方法

TeraTerm、puttyなど、ターミナルソフトを以下の設定で接続することができます。

• シリアルケーブル

設定	
Port	シリアルポート(通常は COM1)
Baud Rate	115200
Date Bits	8
Stop Bits	1
Parity	No
Flow Control	None

• TCP/IP

設定	値
Host	Firebox の Trusted または Optional の IP アドレス
TCP Port	4118
Service	SSH(Version SSH2)
Protocol	IPv4

設定表どおり、ターミナルソフトで Firebox の IP アドレスとポート番号 4118 を指定して接続します。

● TCP/ <u>I</u> P	ホスト(<u>T</u>): 10.0.1.1	*
	■ ビヒストリ(0) TCPボート#(P):	4118
		- <u>-</u>
	ישראםל (<u>UN</u> C): UN	SPEC 🔻
ロシリアル	: ポート(<u>B</u>): [Ŧ

ユーザ名は admin、パスフレーズは構成パスフレーズでログインします。

SH認証		
ログイン中: 10.0.1.1 認証が必要です。		
ユーザ名(<u>N</u>):	admin	
バスフレーズ(<u>P</u>):	••••••	
	☑ バスワードをメモリ上に記憶する(M) □ エージェント転送する(Q)	
◎ ブレインテキス	トを使う(<u>L</u>)	
⑦ <u>R</u> SA/DSA鍵を	使う]
⑦ rhosts(SSH1)を	:使う ローカルのユーザ名(U) (ホスト鍵(E):)	
◎ チャレンジレス	ポンス認証を使う(キーボードインタラクティブ)	©
Pageantを使う		
	OK 接続断(<u>D</u>)	

ログインするとプロンプトが表示されます。

WG# が表示されたメインコマンドモードとなります。



ログインしている間は排他制御がかかり、他の端末から CLI のログインや WebUI のログインができなくなるので注意してください。

設定手順

では設定例として、インターフェイス1の DHCP サーバーを構成するケースを見てみましょう。

configure コマンドで Configuration Command Mode に入ります。

WG#configure

プロンプトが変わります。

WG(config)#

インターフェイスを設定する場合、Interface Command Mode に入る必要があるので interface コマンドを 入力します。interface に続いてスペースを入力し、次に何を入力してよいか分からない場合は「?」を入力し ます。

WG(config)#interface ?

FastEthernet FastEthernet IEEE 802.3

イーサネットポートを設定したいので FastEthernet を入力すればよいことが分かります。

コマンドは途中まで入力して TAB キーを押すと、補完する機能が働きます。

WG(config)#interface F<tab>

WG(config)#interface FastEthernet

エンターキーを押すと% Incomplete command.と表示されました。

WG(config)#interface FastEthernet

% Incomplete command.

これはまだ入力しなければならないパラメータがあるという意味です。

interface FastEthernet に続けて?を入力すると、インターフェイス番号を入力する必要があることが分かります。

WG(config)#interface FastEthernet ?

<int> FastEthernet interface number <0-5>

WG(config)#interface FastEthernet 1

インターフェイス1を指定していしてエンターを押します。

するとプロンプトが変わり、Interface Command Mode に入ったことが分かります。

?を入力すると、インターフェイスを設定するためのコマンド一覧が取得できます。

WG(config/if-fe1)#?	
Trusted interface confi	guration commands:
dhcp	Dynamic host configuration protocol
enable	Enable/Disable current physical interface
exit	Exit from interface configuration mode
help	Description of the interactive help system
history	Display the command history list with line numbers
ip	Internet protocol
link-speed	Link operation speed property
mac-access-control	Restrict access by MAC address
mac-ip-binding	Static MAC/IP binding in arp table
mtu	Set the interface maximum transmission unit (MTU)
name	Name of the entity
no	Negate a command or set its defaults
qos	Quality of service, be sure to enable settings by the command global-
setting	
secondary	Secondary ip address
show	Show running system information
type	Network interface type
v6	Configure the ipv6 interface

DHCP サーバーを構成するには dhcp コマンドが使えることが分かります。

それでは dhcp のあとにスペースと?を入れながら、パラメータ名を確認しつつ、設定してゆきます。

WG(config/if-fe1)#dhcp server ?

(<u> </u>	· · · · · · · · · · · · · · · · · · ·
<int></int>	Lease time, in hour <1-596523>
dns-server	Dns server
domain	Domain name e.g. foo.com
reservation	Reservation name, e.g. a host name
start-addr	Start ip address
wins	Specific the wins server's ip address
WG(config/if-fe	e1)#dhcp server start
WG(config/if-fe	e1)#dhcp server start-addr 10.0.1.100 ?
<ipaddr> I</ipaddr>	End ip address <a.b.c.d></a.b.c.d>
WG(config/if-fe	e1)#dhcp server start-addr 10.0.1.100 10.0.1.199 ?
<cr></cr>	Carriage return
<int></int>	Lease time, in hour <1-596523>
dns-server	Dns server
domain	Domain name e.g. foo.com
reservation	Reservation name, e.g. a host name
start-addr	Start ip address
wins	Specific the wins server's ip address

WG(config/if-fe1)#dhcp server start-addr 10.0.1.100 10.0.1.199 WG(config/if-fe1)#

同じように DNS サーバーも設定します。

WG(config/if-fe1)#dhcp server dns WG(config/if-fe1)#dhcp server dns-server ? <ipaddr> Dns server <A.B.C.D>

WG(config/if-fe1)#dhcp server dns-server 8.8.8.8 WG(config/if-fe1)#

コマンドが成功すると、プロンプトに戻るだけです。設定し、それが即反映となる点にご注意ください。

設定が反映されていることをポリシーマネージャから確認してみてください。

CLI を終了するには、exit コマンドで各モードを抜けて終了させます。

WG(config/if-fe1)#exit

WG(config)#exit

WG#exit

CLI についてのより詳細な情報は WatchGuard(US)のサイトより得ることができます。

http://www.watchguard.com/help/documentation/xtm.asp (英語)

このページにある「Command Line Interface Reference」のリンクから、最新バージョンの CLI リファレンス を参照できます。

WebUI

WebUI についての詳しい情報は別途「WebUI ガイド」をご覧ください。

ここでは WebUI での接続方法と、WebUI ガイドには記載されていない便利な機能や使い方について解説します。

接続方法

<u>https://Firebox の IP アドレス:8080</u> で接続します。



セキュリティ証明書の警告が出ますが、「詳細」—「Webページへ移動」をクリックして閲覧を続行します。



ログインはステータスパスフレーズ(status)、構成パスフレーズ(admin)のどちらでも可能です。

ただ、admin でログインすると排他制御がかかり、他の WebUI の admin ログインや CLI から接続できなくなります。また、WSM で接続しているクライアントからも設定の保存ができなくなるので注意してください。

Passphrase	
•••••	
Authentication Serv	er
Firebox-DB	

ログインするとダッシュボードが表示され、接続した Firebox の状態のサマリーが表示されます。

🖻 🕫 🗄 Fireware Web UI (T50-V 🛛	+ ~		-			×
← → ひ 命 ▲ 証明	書エラー https://10.0.1.1:8080/dashboard/#frontpanel	□ ☆	7⁄⊒	l~	Ē	
WatchGuard	Fireware Web UI	ב- ע -:	admin (?	0)
ダッシュボード	フロントパネル				C	
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	トップクライアント すべて表示	システム				
FireWatch インターフェイス	名前 レート↓ バイト ヒッ ト	名前 モデル	T50-W-KAM JUNE28 T50-W	MIYACHO	D-	
トラフィックモニタ	10.0.1.2 🛑 1 me 55	バージョン シリアル番号 システム時間	12.4.1.859	5401 669A2 /Tokyo		
Geolocation(ジオロケーション)	10.168.5. bps 52 1	システム日付 稼働時間	2019-07-03 4 days 18:1	3 16		
モバイル セキュリティ ネットワークディスカバリー	上位宛先すべて表示	サーバー Log Server	無効			
システムステータス	名前 レートン バイト ヒッ	DNSWatch Dimension	無効			
ネットワーク	N N	WatchGuar	d Cloud			
ファイアウォール セキュリティサブスクリブションサービス	10.0.1.1 🛑 945 💼 664 6	ステータス	無効			

左側の各メニューから、インターフェイスやポリシーの設定ができます。

Fireware のアップグレード/ダウングレード

WebUI ではファームウェアのアップグレード画面から、バージョンアップはもちろんの事、ダウングレードも できるようになっています(但しファクトリーリセット状態になります)。

あらかじめ WebUI 用のファームウェア(exe 形式ではなく zip 形式のものを展開)を用意しておきます。 Software Download のページにも「Fireware 12.4 Update 2 Sysa-dl for OS updates from the Web UI」 という名称でダウンロードできるようになっています。

Fireware 12.4 Update 2

Released 04/29/2019 · SHA1 809b29cee477c8532b1f7b74c8dfb60c6cf4b979

Fireware 12.4 Update 2 Sysa-dl for OS updates from the Web UI Released 04/29/2019 · SHA1 0cf88e3f13e3df369dc20b41005ce7cbe7c76c16

WebUI 左側メニューの <u>システム</u> – <u>アップグレード OS</u> とクリックします。



ファイルの選択で [Browse...] ボタンをクリックします。

あらかじめ用意しておいたファームウェアのファイルを指定します。

Organize 🔻 🛛 New	folder)= • 🔟 🚺
🔆 Favorites	Name	Date modified	Туре
🛄 Desktop	xtm2_a6.sysa-dl	2014/05/07 16:15	SYSA-DL File
Libraries			
Libraries Libraries Documents Music Pictures Videos			

[アップグレード] をクリックします。



ボタンがアップグレード中…となるのでしばらく待ちます。

● アップグレード ファイルがあります

C:\Users\tsuto\Desktop\T30 参照...

アップグレード中...

ダウングレードの場合、Firebox が工場初期出荷状態になる旨、警告が表示されますが、Yes で進みます。

イメージがアップロードされると、再起動が促されますので、[Yes]をクリックします。

I Ein	eware X	TM Web UI	1-#~: admin < :
-EA	o os c	イメージがアップロードされました。デバイスを再起動する必要があります。再起動しますか?	X
	アッ ファ	Yes	No

ログイン画面に戻ります。

WatchGuard	
G	ユーザー名
	admin
	パスフレーズ
	•••••
	認証サーバー
	Firebox-DB ~
	ログイン

Firebox が再起動されたら、再度ログインし、動作を確認してください。

ダウングレードの場合は、Quick Setup Wizard を実施してください。

コンフィグファイルの保存とレポート表示

WSM であれば、コンフィグはポリシーマネージャの「ファイルとして保存」で保存し、設定ファイルを保存できます。しかし WebUI の場合どうすればよいでしょうか。

左側メニュー システム – 構成ファイル をクリックします。

「Download the Configuration File」のリンクをクリックすると、設定ファイルが取得できます。



保存先を指定して保存します。

名前を付けて保存				×
← → ~ ↑ 🕹 > PC > ダウンロード	~	Ū	ダウンロードの検索	Q
整理 ▼ 新しいフォルダー				0
🗊 3D オブジェクト 🔷	体売タルト むすろ酒	(F)/++	-11=++/	
➡ ダウンロード	検索条件に一致する項目はる			
デスクトップ				
● ドキュメント				
■ ピクチャ				
🎝 ミュージック				
🏪 ローカル ディスク (C				
ネットワーク				
*				
ファイル名(N): T50-W-KAMIYACHO-JUNE	28.xml.gz			 V
				100
ファイルの種類(<u>T</u>): GZ ファイル (*.gz)				ઁ

gzip 形式で保存されるので、対応した解凍ソフトで取り出します。

WebUI では、コンフィグのダウンロードだけでなく、コンフィグを分かりやすいレポート表示で閲覧することが可能です。「Firebox Configuration Report」リンクをクリックします。



別窓でレポートが表示されます。設定の閲覧や、PDF 作成ソフトなどで設定ドキュメントとして保存するなどの用途でお使いいただけます。

	× + ~							×	
\leftrightarrow \rightarrow \circlearrowright \textcircled{a}		アドレスを入	л		☆	t≡ <i>0</i> ,	L B		
Firebox 構成レポート									
目次			Firebox 構	成レポート					
<u>1ネットワーク</u>			モデル:	T50-W					
12	<u>1-1 インダーンエー</u> イス 日付: 7/3/2019								
<u>1-2 ARP エントリ</u>	構成								
<u>1-3 リンクアクリ</u> <u>ゲーション</u>	149.000								
<u>1-4 VLAN</u> 1-5 ブリッジ	1. ネ ットワーク								
1-6 Loopback	1.1 インターフェイス	ζ							
<u>1-7 候飲WAN</u> <u>1-8 SD-WAN</u>		•						_	
<u>1-9 リンクモニー</u> 1-10 動的DNS	<u>1-9 リンクモニー</u> 1 10 動のDNS								
<u>1-11 NAT</u>	構成インターノエイノ	くでミック	スルーティンク モー	Р.			40		
<u>1-12 ルート</u> 1-13 動的ルー	インターフェイス	種類	名前 (エイリアス)	IPv4 アドレス	IPv6 アド	レス	説明		
<u>1-13 動売レー</u> ティングに	0	External	External	DHCP Auto					
1-14 Multicast	1	Trusted	Trusted	10.0.1.1/24					
Routing	2	無効	Optional-1	0.0.0/24					
	3	無効	Optional-2	0.0.0/24					
	4	無効	Optional-3	0.0.0/24					
	5	無効	Optional-4	0.0.0/24					
<u>1-17 認証方法</u>	6	無効	Optional-5	0.0.0/24					
<u>2 ファイアウォール</u>	ドメイン名前な		be a		2	A.C.	1		
<u>2-1 ノアイア</u> ウォール ポリシー	DNSサーバー な	2 L							
2-2 Firewall	WINSサーバー な	2							
2-3 Mobile VPN								~	
ポリシー	<							>	
	Copyright © 2012-201	15 Watch	Guard Technologies, li	nc. All Rights Rese	erved.				
クライアント側の UI カスタマイズ

この項では管理者向けのインターフェイスではなく、クライアントがウェブブラウザで見ることになる拒否画 面のカスタマイズについて触れておきます。

WebBlocker、Gateway Anti-Virus、RED などで拒否された際に表示されるセキュリティ警告のメッセージは デフォルトで英語になっています。その警告ページのテンプレートはポリシーマネージャの HTTP-proxy ポ リシーのプロパティにあります。まず HTTP-proxy ポリシーを開きます。



[プロキシの表示/編集]ボタンをクリックします。

プロキシの表示/編集画面の「拒否メッセージ」に表示のテンプレートの設定があります。



このテンプレートの HTML を編集すれば日本語のページにすることができます。

テンプレート中で使用されている%(…)%で囲まれた Firebox のメッセージを格納する変数部分ですので、 必ず残してください。

次頁にそのままコピー&ペースとして使える HTML ソースを掲載しておきます。

(72ページで使用したセキュリティ警告画面の HTML です)

ソース中のメールアドレスや連絡先の部分は実際のものに書き換えてください

```
Content-type: text/html; charset="utf-8"
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>%(transaction)% denied by WatchGuard HTTP Proxy</title>
    <style type="text/css">
      body {
        font-family: Arial, Helvetica, Verdana, Sans-Serif;
        font-weight: normal;
        color: #000000;
      }
      div {
        margin-left: auto;
        margin-right: auto;
        text-align: center;
      }
      .box {
        width: 640px;
        background-color: #F2F2F2;
        border-left: solid 1px #C2C2C2;
        border-right: solid 1px #C2C2C2;
        vertical-align: middle;
        padding: 20px 10px 20px 10px;
      }
      р {
        text-align: left;
        font-size: small;
      }
      .red {
        font-weight: bold;
        font-size: large;
        color: Red;
        text-align: center;
      }
      .band {
        height: 20px;
        color: White;
```

```
background: #333333;
```

```
width: 640px;
      border-left: solid 1px #333333;
      border-right: solid 1px #333333;
      padding: 3px 10px 0px 10px;
    }
    div#wrap {
      margin-top: 50px;
    }
    .center{
      text-align: center;
        }
    .blue {
      font-weight: bold;
      font-size: large;
      color: blue;
      text-align: center;
    }
   </style>
 </head>
 <body>
   <div id="wrap">
    <div class="band">Security Alert !</div>
    <div class="box">
      セキュリティ機能によってアクセスは拒否されました
      お問い合わせは情報システム部(内線 1000)まで。
      アクセス許可を希望される場合は、以下のメッセージをコピーして<br/>>
      <a href="mailto:info@joho-system.domain">info@joho-system.domain</a>までメールでご連絡ください
      <hr/>
      <b> 理由: </b> %(reason)% 
      <b>アクセスメソッド:</b> %(method)%
      <b>アクセス先のサーバー:</b>%(url-host)%
      <b>URL パス:</b> %(url-path)%
    </div>
    <div class="band">WatchGuard Technologies, Inc.</div>
   </div>
 </body>
</html>
```

終わりに

WSM 詳細設定ガイドをご活用いただきありがとうございます。

WatchGuard Firebox がいかに多様なセキュリティ要件に適用できるか、実感いただけたと存じます。

今後も弊社の製品が、御社のセキュリティの要としてお役に立てれば幸いです。