

Managed SD-WAN セキュアインターネット接続 vUTM ユーザ設定マニュアル

第2. 2版



目次

1	はじ	こめに	. 5
2	vUTI	M カスタマコントロールへの接続	. 6
	2. 1	vUTM カスタマコントロールへのログインについて	. 6
	2. 2	vUTM カスタマコントロールのパスワード変更	. 6
3	プリ	リセット設定	. 8
	3. 1	ファイアウォールポリシー	. 8
	3. 2	セキュリティプロファイル	13
4	ファ	· イアウォールポリシーの設定方法	17
	4. 1	ファイアウォールポリシーの追加	17
	4. 2	ファイアウォールポリシーの変更	19
	4. 3	ファイアウォールポリシーの削除	20
5	アト	・レスの設定方法	21
	5. 1	アドレスの追加	21
	5. 2	アドレスの変更	24
	5.3	アドレスの削除	25
6	アト	・レスグループの設定方法	26
	6. 1	アドレスグループの追加	26
	6. 2	アドレスグループの変更	27
	6.3	Private List、Src Black List、Skip List、Dst Black Listの設定方法	28
	6. 4	アドレスグループの削除	32
7	サー	- ビスの設定方法	33
	7. 1	サービスの追加	33
	7. 2	サービスの変更	34
	7. 3	サービスの削除	35
8	サー	- ビスグループの設定方法	36
	8. 1	サービスグループの追加	36
	8. 2	サービスグループの変更	37
	8.3	サービスグループの削除	38
9	ファ	ィイアウォールポリシーの有効化・無効化	39
	9. 1	ファイアウォールポリシーの有効化	39
	9. 2	ファイアウォールポリシーの無効化	40
10) セキ	-ュリティプロファイル:アンチウイルス	41
	10. 1	アンチウイルスの設定	41
	I.	インスペクションされるプロトコル	.42
	II.	APT プロテクションオプション	.43



III.	ウイルスアウトブレイク防止	43
10. 2	アンチウイルスの有効化・無効化	44
11 セキ	-ュリティプロファイル:Web フィルタ	45
11.1	Web フィルタの設定	45
I.	FortiGuard カテゴリベースのフィルタ	46
II.	カテゴリ使用クォータ	48
III.	ユーザにブロックされたカテゴリのオーバーライドを許可する	50
IV.	サーチエンジン	50
V.	スタティック URL フィルタ	50
VI.	レーティングオプション	52
VII.	プロキシオプション	52
11. 2	Web フィルタの有効化・無効化	53
12 セキ	-ュリティプロファイル:アプリケーションコントロール	54
12. 1	アプリケーションコントロールの設定	54
I.	カテゴリ	56
II.	ネットワークプロトコルの強制	57
III.	アプリケーションとフィルタのオーバーライド	58
IV.	オプション	60
12. 2	アプリケーションコントロールの有効化・無効化	61
13 セキ	-ュリティプロファイル:侵入防止(IPS)	62
13. 1	侵入防止(IPS)の設定	62
I.	悪意のある URL をブロック	63
II.	IPS シグネチャとフィルタ	63
III.	ボットネット C&C	65
13. 2	侵入防止(IPS)の有効化・無効化	66
14 ファ	· イルフィルタ	68
14. 1	ファイルフィルタの設定	68
I.	ルール	69
14. 2	ファイルフィルタの有効化・無効化	71
15 セキ	-ュリティプロファイル:E メールフィルタ	72
15. 1	E メールフィルタプロファイルの設定	72
I.	プロトコルごとのスパム検知数	73
II.	FortiGuard スパムフィルタリング	73
III.	ローカルスパムフィルタリング	74
15. 2	E メールフィルタの有効化・無効化	76
16 ダッ	,シュボード	77
16. 1	ステータス	77



16. 2	2 LAN/DMZ 上位利用	77
16. 3	3 セキュリティ、システムイベント	78
17 Fc	prtiView	78
18 □	グ&レポート	79
19 /	ージョン差分により削除・移動された設定	81
19. 1	V6. 2. 7→v7. 2. 5	81
20 Q8	A	82



1 はじめに

本手順書では NTT 東日本「Managed SD-WAN セキュアインターネット接続サービス」の vUTM カスタマコントロールについて、お客さまアカウントにて設定できる項目を解説します。

本手順で使用している IP アドレスは、RFC で定義されている例示用の IP アドレスとなりますので、設定の際はお客さまの環境に応じて指定してください。

お客さまアカウントにて閲覧、変更できる一覧は表 1-1. の通りです。

表 1-1. お客さまアカウント権限一覧.

内容	権限	
ダッシュボード (FortiView※)	変更可能	
ポリシー&オブジェクト	ファイアウォール	設定可能
	アドレス	設定可能
	サービス	設定可能
セキュリティプロファイル	アンチウイルス	設定可能
	Web フィルタ	設定可能
	アプリケーションコントロール	設定可能
	侵入防止 (IPS)	設定可能
	ファイルフィルタ	設定可能
	Eメールフィルタ	設定可能
システム	閲覧可能	
セキュリティファブリック	閲覧可能	
ログ&レポート		閲覧可能

※FortiView はダッシュボード配下にあります。

「ネットワーク」「システム」「セキュリティファブリック」メニューは、一部閲覧/変更できる箇所 もありますが、本マニュアルの記載事項以外を変更することで意図しない動作が発生する可能性があ る為、変更しないようお願いいたします。



- 2 vUTM カスタマコントロールへの接続
 - 2.1 vUTM カスタマコントロールへのログインについて

vUTM カスタマコントロールへのアクセスは、CPE 配下の端末のブラウザから URL に直接 IP アドレスを指定することでログインできます。

接続先 URL: https://10.128.180.5

※ インターネット経由でのアクセスはできません。vUTM カスタマコントロールへはお客さま LAN 環境からのみアクセスが可能となります。

vUTM カスタマコントロールのログイン画面が表示されますので、ユーザ名、パスワードを入力し、ログインをクリックします。

※ 初期アクセスにおいて、証明書エラーの画面が表示されますが、サイト自体の問題はございません。



図 2-1. vUTM カスタマコントロール・ログイン画面.

2.2 vUTM カスタマコントロールのパスワード変更

ログイン後、vUTMカスタマコントロール右上のユーザ名「User」をクリックします。



図 2-2. vUTM カスタマコントロール・右上表示.

表示されたプルダウンから「パスワードの変更」をクリックします。



図 2-2. vUTM カスタマコントロール・パスワード変更表示.



現在のパスワード、新しいパスワードを 2 回入力し、「OK」をクリックします。

	パスワードの編集					
■ 現在の管理者アカウントのパスワードを変更すると再ログインが必要 になります。						
ユーザ名 User						
旧パスワード						
新しいパスワード						
パスワードの再入力						
OK キャンセル						

図 2-3. vUTM カスタマコントロール・パスワード変更画面.



3 プリセット設定

セキュアインターネット接続サービスにてプリセットされたファイアウォールポリシーやセキュリティプロファイルの設定概要について記載します。

プリセットのファイアウォールポリシーを利用することで、様々な通信要件に対して簡易な設定変更により、セキュリティ機能の有効化・無効化を実現することが可能です。

実際の設定方法については、各章をご覧ください。

3.1 ファイアウォールポリシー

セキュアインターネット接続サービスでは、カスタムルールを除いた 5 つのファイアウォールポリシーがプリセットされています。

- ① 送信元ブラックルール(Src Black Rule)
- ② スキップルール(Skip Rule)
- ③ 宛先ブラックルール(Dst Black Rule)
- ④ カスタムルール(Custom Rule) ※vUTM 設定変更依頼時のみ設定・変更
- (5) LAN→WAN JレーJレ (LAN→WAN Rule)
- ⑥ 暗黙の拒否ルール

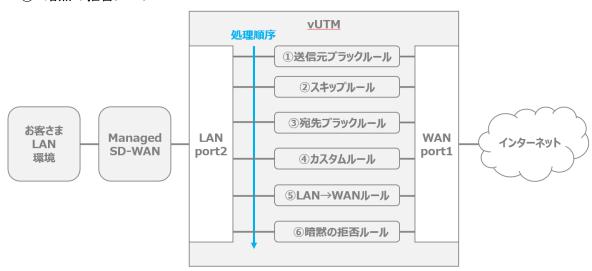


図 3-1. プリセットのファイアウォールポリシー概要図.

ポリシーは、記載順に処理され、通信要件に合致するポリシーにて通信が制御されます。 プリセットされたファイアウォールポリシーのパラメータの追加・変更にて運用して頂くこと を推奨します。

vUTM 設定変更のご依頼を申し付け頂くことによりカスタムルールによって、お客さま LAN 環境におけるセグメント単位でのポリシーの作成等ができ、上記の⑤「LAN→WAN ルール」ポリシーにおいては、インターネット向けの通信に対して、きめ細かくセキュリティ機能を適用することが可能です。

HTTPS、SMTPS、POP3S など SSL/TLS により暗号化された通信に対してセキュリティ機能を働かせることはできません。



表 3-1. プリセットのファイアウォールポリシー一覧.

	ポリシー名	用途	デフォルト 設定
1	送信元ブラックル ール	 アドレスグループ(Src Black List)に送信元 IP アドレスを追加することにより、当該通信を拒否することが可能です。 初期設定時、Src Black List は、空の状態で提供いたします。 感染した端末の IP アドレスを Src Black List に適用することで、インターネットの通信を拒否することが可能です。 	有効
2	スキップルール	 アドレスグループ(Skip List)に宛先 IP アドレスを追加することにより、当該通信の全セキュリティ機能を無効化することが可能です。 初期設定時、Skip List は、空の状態で提供いたします。 信頼のある宛先 IP アドレスを Skip List に適用することで、セキュリティ機能を無効化することが可能です。 	有効
3	宛先ブラックルー ル	 アドレスグループ(Dst Black List)に宛先 IP アドレスを追加することにより、当該通信を拒否することが可能です。 初期設定時、Dst Black List は、空の状態で提供いたします。 明らかに悪性な WEB サイト等を Dst Black List に適用することで、対象の通信を拒否することが可能です。 	有効
4	カスタムルール	- vUTM 設定変更依頼時のみに作成されるポリシーです。 - VPN 内のプライベートアドレス (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16) を送信元 IP アドレスとする範囲内において、お客さま LAN 環境におけるセグメント単位でのポリシーの作成においてセキュリティ機能の適用を個別に設定が可能です。	無効(未作成)
5	LAN→WAN JレーJレ	 基本となるファイアウォールポリシーとなります。 VPN内のプライベートアドレス(10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)を送信元 IP アドレスとして、全てのインターネット接続の通信を対象にセキュリティ機能を適用します。 	有効
6	暗黙の拒否ルール	上記①~⑤に合致しない通信を明示的に拒否します。	有効



各ファイアウォールポリシーの設定項目に関しては以下の通りとなります。

※ 灰色の網掛け部分に関してはできないパラメータとなります。

表 3-2. ファイアウォールポリシーの設定項目.

	設定項目	設定内容		参考項目
1	名前	任意:ポリシー名を記載		
2	着信インターフェース	固定:LAN (port2) ※他インターフェースでは動作化	呆証不可	
3	発信インターフェース	固定:WAN(port1) ※他インターフェースでは動作の	呆証不可	
4	送信元	任意 IP アドレス:予め設定され レスもしくはアドレスグループを		5 章: アドレス 6 章: アドレスグループ
5	宛先	同上		同上
6	サービス	任意:制御対象のプロトコルター (UDP, TCP) 及び宛先ポート番号を		7章:サービス 8章:サービスグループ
7	アクション	許可/拒否:当該通信の許容/打	巨否を指定	
8	NAT	固定:有効		
9	IP プール設定	発信インターフェースの IP アドレスを使用 ※ 帯域専有タイプのみ「ダイナミック IP プ ールを使用」を使用		サービス種別により設定値が異なり ます
10	プロトコルオプション	固定:default2		
11	セキュリティ プロファイル	 アンチウイルス Web フィルタ DNS フィルタ アプリケーションコントロール 侵入防止(IPS) ファイルフィルタ Eメールフィルタ SSL インスペクション* 	有効/無効 有効/無効 有効/無効 有効/無効効 有効/無効効 有効/無効 有効/無効	10章:アンチウイルス 11章:Web フィルタ - 12章:アプリケーションコントロール 13章:侵入防止(IPS) 14章:ファイルフィルタ 15章:E メールフィルタ
12	ロギングオプション	アクション:許可の場合 許可トラフィックのログ:有効/無効 許可トラフィックの記録設定: セキュリティイベント/すべてのセッション アクション:拒否の場合 違反トラフィックのログ:有効/無効		アクションの設定内容により表示内 容が異なります
13	有効化設定	│ファイアウォールポリシーの有效 │を指定	动化/無効化	9章:ファイアウォールポリシー

※ SSL インスペクション:有効化の際は「certificate-inspection2」を利用

「deep-inspection」機能はサービス提供外



プリセットされているファイアウォールポリシーの設定内容は以下の通り。

- ※ 橙色の網掛け部分に関しては変更しないことを推奨としております。変更後の問合せはサービス 提供外とさせていただきます。
- ※ 灰色の網掛け部分に関しては変更できないパラメータとなります。変更することで予期しない 動作を起こす可能性があります。
- ※ 濃い灰色の網掛け部分に関しては非表示・非活性のパラメータとなります。

表 3-3. ファイアウォールポリシーの設定項目(1/2).

	我 0 0. ファイテラオールパラン の政定項目 (1/2).						
	設定項目	①送信元ブラックルール	②スキップルール	③宛先ブラックルール			
1	名前	Src Black Rule	Skip Rule	Dst Black Rule			
2	着信インター フェース	LAN(port2)	LAN(port2)	LAN(port2)			
3	発信インター フェース	WAN(port1)	WAN(port1)	WAN (port1)			
4	送信元	Src Black List*	all	all			
5	宛先	all	Skip List*	Dst Black List*			
6	サービス	ALL	ALL	ALL			
7	アクション	拒否	許可	拒否			
8	NAT		有効				
9	IP プール設定		発信インターフェースの IP ア ドレス or ダイナミック IP プ ール				
10	プロトコルオ プション		default2				
			アンチウイルス:無効				
			Web フィルタ:無効				
	セキュリティ		DNS フィルタ:無効				
11			アプリケーションコントロー ル: 無効				
'	プロファイル		侵入防止(IPS):無効				
			ファイルフィルタ:無効				
			E メールフィルタ:無効				
			SSL インスペクション: 無効 (no-inspection)				
12	ロギングオプ ション	違反トラフィックをログ∶有 効	許可トラフィックをログ∶無効	違反トラフィックをログ∶有効			
13	有効化設定	有効	有効	有効			



表 3-4. ファイアウォールポリシーの設定項目(2/2).

	設定項目	④カスタムルール [†]	⑤LAN→WAN ルール	⑥暗黙の拒否ルール
1	名前	Custom Rule	LAN→WAN Rule	暗黙の拒否
2	着信インター フェース LAN (port2)		LAN(port2)	any
3	発信インター フェース	WAN(port1)	WAN(port1)	any
4	送信元	 任意:申込内容に準じる 	Private List [‡]	all
5	宛先	任意:申込内容に準じる	All	all
6	サービス	任意:申込内容に準じる	ALL	
7	アクション	許可/拒否	許可	拒否
8	NAT	有効	有効	
9	発信インターフェース IP プール設定 アドレス or ダイナミ プール		発信インターフェースの IP ア ドレス or ダイナミック IP プ ール	
10	プロトコルオ プション	default2	default2	
	セキュリティ プロファイル	アンチウイルス:任意	アンチウイルス:無効	
		Web フィルタ:任意	Web フィルタ:無効	
		DNS フィルタ:無効	DNS フィルタ:無効	
11		アプリケーションコントロー ル: 任意	アプリケーションコントロー ル: 無効	
' '		侵入防止(IPS) :任意	侵入防止(IPS) :無効	
		ファイルフィルタ:任意	ファイルフィルタ:無効	
		E メールフィルタ:任意	E メールフィルタ:無効	
		SSL インスペクション:有効 (certificate-inspection2)	SSL インスペクション:有効 (certificate-inspection2)	
12	ロギングオプ ション 任意:申込内容に準じる		許可トラフィックをログ:有 効 許可トラフィックの記録設 定:セキュリティイベント	違反トラフィックをログ:有 効
13	有効化設定	無効	有効	有効

† ④カスタムルールについては vUTM 設定変更依頼時のみに作成されるポリシーとなります。 初期設定においてはプリセットされているファイアウォールポリシーには含まれていません。 上記はアクション:許可の場合に設定ができる場合の設定項目となります。

許可/拒否の設定によって設定できる項目は異なります。

‡ 初期設定時は、プライベート IP アドレスのリスト(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)を提供します。



3.2 セキュリティプロファイル

ファイアウォールポリシー ⑤LAN \rightarrow WAN ルールのセキュリティプロファイルにおいては、一般的な 0A 端末がインターネットでの通信を実施する際のセキュリティ脅威を検知・ブロック可能とするようにプリセットされています。

なお、以下に該当する機能については、サービス提供外としております。

- I. 通常想定しない通信要件
- II. 負荷により安定サービスが損なわれる懸念がある機能
- III. 過検知による業務影響の恐れがある機能
- IV. 未提供な機能

各セキュリティプロファイルにおける設定概要は以下の通りです。

※ 灰色の網掛け部分に関してはサービス提供外のパラメータとなります。

表 3-5. セキュリティプロファイル概要(1/4).

	設定項目	設定内容	デフォルト設定	備考
		アンチウイルスプロ ファイル	機能セット:プロキシベース	理由IVにより フローベース は未提供
			HTTP:有効	
			SMTP:有効	
			P0P3:有効	
		インスペクションさ	IMAP:有効	
		れるプロトコル	FTP:有効	
			CIFS:無効	**** *
	アンチウイルス		MAPI: 無効	理由Iにより 無効化
1			SSH:無効	
1		ATP プロテクションオ プション ウイルスアウトブレ イク防止	コンテンツ無害化:無効	理由皿により 無効化
			E メール添付の Windows 実行ファイルをウイルス として扱う:有効	
			Forti Sandbox に検査の為ファイルを送信:無効 Forti NDR に検査のためファイルを送信:無効	理由Ⅳにより 無効化
			モバイルマルウェアプロテクションを含める:有効	
			隔離:無効	理由Ⅲにより 無効化
			Forti Guard アウトブレイク防止データベースを使用:無効	理由Ⅲにより 無効・非推奨
			外部マルウェアブロックリストを使用:無効	理由Ⅳにより
			EMS 脅威フィードの使用: 無効	無効化



表 3-6. セキュリティプロファイル概要 (2/4).

	設定項目	設定内容	デフォルト設定	備考
		Web フィルタ	機能セット:プロキシベース	理由Ⅳによりフロ
		プロファイル	成化とグド・プロインベース	ーベースは未提供
			セキュリティリスクの高いサイト: ブロック	
		FortiGuard カ	(悪意のある web サイト, フィッシング詐欺, スパム URL,	
		テゴリベース	ダイナミック DNS, 新たに観察されたドメイン, 新たに登	理由Ⅳにより未
		のフィルタ	録されたドメイン)	提供
		0)) 1 / 10 /	ローカルカテゴリ:許可	
			上記以外のカテゴリ:モニタ	
		カテゴリ使用	未設定	
		クォータ		
		ユーザにブロ	無効	
		ックされたカ		理由Ⅳにより無
		テゴリのオー		効化
		バーライドを		<i>33</i> .15
		許可する		
	Web フィルタ	サーチエンジン	Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制:無効	理由Ⅳにより無
			YouTube へのアクセスを制限する:無効	→ 効化
2			すべての検査キーワードをログ:無効	
			無効な URL をブロック:有効	
			URL フィルタ:無効	利用する際は
		スタティック		有効にすること
		URL フィルタ	FortiSandbox により検知された悪意のある URL をブロ	理由Ⅱにより無
			ック:無効	効化
			コンテンツフィルタ:無効	利用する際は
				有効にすること
		1= <i>.</i> \. \. \. \. \. \. \. \. \. \. \. \. \.	レーティングエラー発生時に Web サイトを許可:有効	
		レーティング	ドメインまたは IP アドレスで URL をレーティング:無	理由Ⅲにより効
		オプション	効	化
			Google アカウントの使用を特定のドメインに制限:無	理由Ⅳにより未
			効	提供
		プロキシオプ	HTTP POST アクション:許可	
		ション	Java アプレットを削除:無効	
			ActiveX の削除:無効	理由Iにより無 効化
			Cookie を削除:無効	ᄽᆙ



表 3-7. セキュリティプロファイル概要(3/4).

	設定項目	設定内容	デフォルト設定	備考
		1>	P2P: ブロック	
		カテゴリ	上記以外のカテゴリ:モニタ	
		ネットワーク	無効	md = m/- k
		プロトコルの		理由Ⅱ、Ⅲによ
		強制		り無効化
		アプリケーシ	有効	
3	アプリケーション	ョンとフィル		
3	コントロール	タのオーバー		
		ライド		
			デフォルト以外のポートで検出されたアプリケーショ	理由Ⅱ、Ⅲによ
			ンをブロック:無効	り無効化
		オプション	DNS トラフィックの許可とログ:有効	
			HTTP ベースアプリケーションの差し替えメッセージ:	理由Ⅳにより未
			無効	提供
		悪意のある		
		URL をブロッ	有効	
		ク		
			タイプ:フィルタ	初期設定のシグ
4	 侵入防止 (IPS)	IPS シグネチ	アクション: デフォルト	ネチャ設定
7	及人例正(113)	ヤとフィルタ	パケットロギング:無効	理由Ⅱにより無
		() 1 // //	ステータス: デフォルト	対化
			フィルタ:重大度 3 以上	777.10
		ボットネット	ボットネットサイトへの発信接続をスキャン:ブロッ	
		C&C	ク	



表 3-8. セキュリティプロファイル概要 (4/4).

	設定項目	設定内容	デフォルト設定	備考
	ファイルフィルタ	ファイルフィ		理由Ⅳによりフ
		ルタプロファ	機能セット:プロキシベース	ローベースは未
		イル		提供
5		アーカイブの		
		コンテンツを	有効	
		スキャン		
		ルール	未作成	
		Eメールフィ		理由Ⅳによりフ
		ルタプロファ	機能セット:プロキシベース	ローベースは未
		イル		提供
			IMAP:スパムアクション:タグ、タグ挿入箇所:サブ	
		プロトコルご	ジェクト、タグ形式:Spam	
	Eメールフィルタ	ノロトコルこ とのスパム検	POP3:スパムアクション:タグ、タグ挿入箇所:サブ	
		知数	ジェクト、タグ形式:Spam	
		川奴	SMTP:スパムアクション:タグ、タグ挿入箇所:サブ	
6			ジェクト、タグ形式:Spam	
0			IP アドレスチェック:有効	
		FortiGuard ス	URL チェック:有効	
		パムフィルタ	E メール内のフィッシング URL を検知:有効	
		リング	E メールチェックサムのチェック: 有効	
			スパム報告:有効	
			HELO DNS ルックアップ:無効	理由Iにより無
		ローカルスパ	リターン E メール DNS チェック:無効	効化
		ムフィルタリ ング	ブラック/ホワイトリスト:無効	利用する際は
				有効にすること



- 4 ファイアウォールポリシーの設定方法 本章では、ファイアウォールルールの追加、変更、削除設定方法について解説しています。
 - 4.1 ファイアウォールポリシーの追加
 - ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



図 4-1. ファイアウォールポリシーの選択表示.

※ルールの表示がされていない場合は+ボタンをクリックして表示させてください。



図 4-2. ファイアウォールポリシーの表示画面.

② プリセットルールの LAN \rightarrow WAN Rule を右クリックし、空のポリシーを挿入 \rightarrow 上へをクリックします。



図 4-3. 空のポリシー挿入画面.



③ 挿入した空のポリシーをダブルクリックし開く。

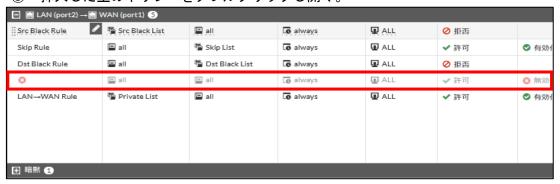


図 4-4. ポリシー選択画面.

④ 以下の設定項目をもとに設定を行い、設定完了後「OK」をクリックする。 表 4-1. ファイアウォールポリシーの設定項目.

	設定項目	変更内容	備考
1	名前	任意	
2	着信インターフェース	LAN(port2)	LAN(port2)以外を選択した場合、動作保証はできません
3	発信インターフェース	WAN (port1)	WAN(port1)以外を選択した場合、動作保証はできません
4	送信元	任意	アドレスの作成方法は 6.2 項参照
5	宛先	任意	アドレスの作成方法は 6.2 項参照
6	サービス	任意	サービスの作成方法は8.2項参照
7	アクション	許可/拒否	
8	NAT	有効	
9	IP プール設定	発信インターフェースの IP アドレスを使用 ※ 帯域専有タイプのみ「ダイナミック IP プール を使用」を使用	サービス種別により設定値が異なります
10	プロトコルオプション	default2	
		アンチウイルス:有効/無効	※有効の場合、default のみ選択可
	セキュリティプロファイル	Web フィルタ:有効/無効	※有効の場合、default のみ選択可
		DNS フィルタ:無効	
		アプリケーションコントロール: 有効/無効	※有効の場合、default のみ選択可
11		侵入防止(IPS):有効/無効	※有効の場合、default のみ選択可
		ファイルフィルタ:有効/無効	※有効の場合、default のみ選択可
		E メールフィルタ∶有効/無効	※有効の場合、default のみ選択可
		SSL インスペクション: 有効	※有効の場合、certificate-
		(certificate-inspection2)	inspection2のみ選択可能 ※無効の場合、ログは取得されませ
12	ロギングオプション	任意	人
13	有効化設定	有効/無効	

- ※ 上記以外の設定をした場合、動作保証はできません。
- ※ 灰色の網掛け部分に関してはサービス提供外のパラメータとなります。



- 4.2 ファイアウォールポリシーの変更
 - ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。

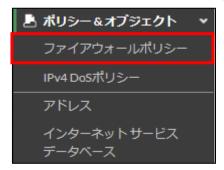


図 4-5. ファイアウォールポリシーの選択表示.

② 変更するポリシーをダブルクリックする。



図 4-6. 変更対象のポリシー選択画面.

③ 表 4-1 を参照し設定変更を行い、変更完了後「OK」をクリックする。



図 4-7. 設定変更画面.



- 4.3 ファイアウォールポリシーの削除
 - ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。

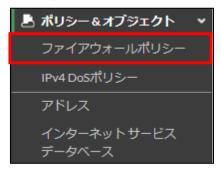


図 4-8. ファイアウォールポリシーの選択表示.

② 削除したいポリシーを選択し、画面上部の削除ボタンをクリックする。



図 4-9. 削除対象ポリシー選択画面.



5 アドレスの設定方法

本章では、Src Black List、Skip List、Dst Black List、ファイアウォールルールの送信元、宛 先などに設定するアドレスについて解説しています。

※詳細が表示されていない場合、左の+ボタンをクリックすることによって展開されます。



図 5-1. アドレス・アドレスグループ選択画面.

5.1 アドレスの追加

① 左のメニューからポリシー&オブジェクト->アドレスを選択する。

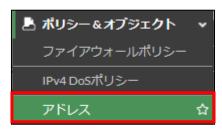


図 5-2. アドレス選択画面.

② 新規作成->アドレスをクリックする。

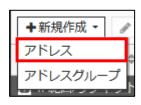


図 5-3. アドレス選択画面.



③ 名前を記載しタイプにて使用するタイプを選択する。

※タイプについては、サブネット、IP範囲、FQDNのいずれかをご使用ください。

I. サブネットの場合、下記のように記載して OK をクリックする。

例:140.227.17.254/32を追加する場合

名前:140.227.17.254/32

タイプ:サブネット

IP/ネットマスク: 140.227.17.254/32

新規アドレス	
名前	140.227.17.254/32
カラー	国 変更
タイプ	サブネット ▼
IP/ネットマスク	140.227.17.254/32
インターフェース	□ any ▼
スタティックルート設定 🖜	
コメント	コメント記入 /// 0/255
	h. s. tari
	OK キャンセル

図 5-4. 新規アドレス設定画面(サブネット).

II. IP範囲の場合、下記のように記載して OK をクリックする。

例:192.168.1.100-192.168.1.200 を追加する場合

名前:192.168.1.100-192.168.1.200

タイプ: IP 範囲

IP 範囲: 192.168.1.100-192.168.1.200



図 5-5. 新規アドレス設定画面(IP 範囲).



III. FQDN の場合、下記のように記載して OK をクリックする。

例: https://www.ntt-east.co.jp を追加する場合

名前:ntt-east.co.jp

タイプ:FQDN

FQDN: www.ntt-east.co.jp



図 5-6. 新規アドレス設定画面(FQDN).



5.2 アドレスの変更

① 左のメニューからポリシー&オブジェクト->アドレスを選択する。



図 5-7. アドレス選択画面.

② 変更対象のアドレスをダブルクリックする。

+ 新規作成 ▼ / 編集 >_ CLIで編集 「 クローン								
名前 ♦	詳細◆	インターフェース◆	タイプ ♦	参照◆				
□ IP範囲/サブネット 8								
1 0.0.0.0/8	10.0.0.0/8		アドレス	1				
172.16.0.0/12	172.16.0.0/12		アドレス	1				
192.168.0.0/16	192.168.0.0/16		アドレス	1				
☐ FABRIC_DEVICE	0.0.0.0/0		アドレス	0				
FIREWALL_AUTH_PO	0.0.0.0/0		アドレス	0				
SSLVPN_TUNNEL_AD	10.212.134.200 - 10.212.1		アドレス	2				
□ all	0.0.0.0/0		アドレス	20				
∅ none	0.0.0.0/32		アドレス	3				
☐ FQDN 6	□ FQDN 🔞							

図 5-8. 変更対象アドレスの選択画面.

③ 変更箇所を変更し、OK をクリックする。



図 5-9. 変更対象アドレスの設定画面.



5.3 アドレスの削除

① 左のメニューからポリシー&オブジェクト->アドレスを選択する。

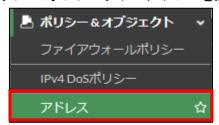


図 5-10. 変更対象アドレスの選択画面.

② 削除したいアドレスを選択し削除をクリックする。



図 5-11. 削除対象アドレスの選択画面.

③ 確認ウィンドウがでるので、OK をクリックします。



図 5-12. 削除アドレスの確認画面.



6 アドレスグループの設定方法

本章では、5章で作成したアドレスをグルーピングする方法、Private List、Src Black List、 Skip List、Dst Black Listでの設定方法を解説しています。

- 6.1 アドレスグループの追加
 - ① 左のメニューからポリシー&オブジェクト->アドレスを選択する。

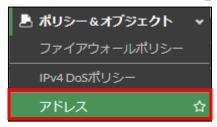


図 6-1. アドレス選択画面.

② 新規作成をクリックし、アドレスグループを選択する。

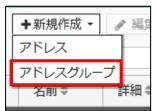


図 6-2. アドレスグループ選択画面.

③ グループ名、メンバー、(必要であれば) コメントを記載して、OK をクリックします。



図 6-3. 新規アドレスグループ設定画面.

例: 192.168.0.0/24 と 192.168.2.0/24 のようなセグメントが異なるアドレスをメンバーに設定することにより1グループとして利用することが可能となります。

※メンバーは 5.1 項で登録したファイアウォールアドレスを使用します。アドレスグループが登録されていることを確認します。



6.2 アドレスグループの変更

① 左のメニューからポリシー&オブジェクト->アドレスを選択する。

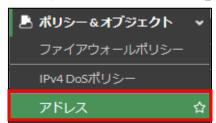


図 6-4. アドレス選択画面.

② 変更したいアドレスグループをダブルクリックします。

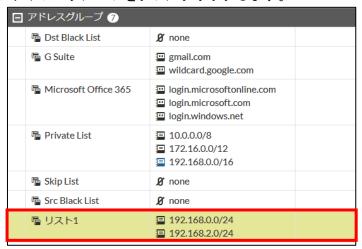


図 6-5. 変更対象アドレスグループ選択画面.

③ 変更したい項目を変更し、OK をクリックする。

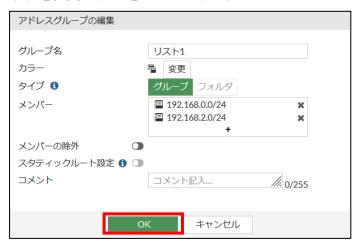


図 6-6. 変更対象アドレスグループ設定画面.

※ 既存アドレスグループ Private List、Skip List、Src Black List、Dst Black Listのアドレスが変更可能です。



- 6.3 Private List、Src Black List、Skip List、Dst Black List の設定方法 ※ 事前に 5.1 項で登録したファイアウォールアドレスが必要となります。
 - ① Private List への設定方法
 - ※セキュリティチェックをしながらインターネットへ通信を行うリストになります。
 - I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループ にある Private List をダブルクリックする。

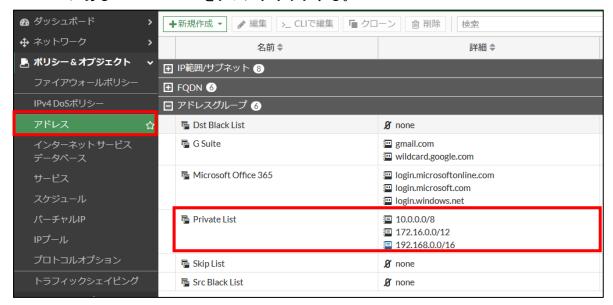
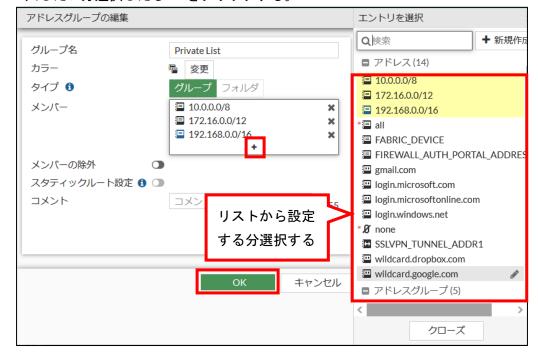


図 6-7. Private List 選択画面.

- II. メンバーの+をクリックしリストから対象のアドレスを選択し、投入する。
- III. 入したい分選択したら OK をクリックする。





- ② Src Black List への設定方法
 - I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループ にある Src Black List をダブルクリックする。

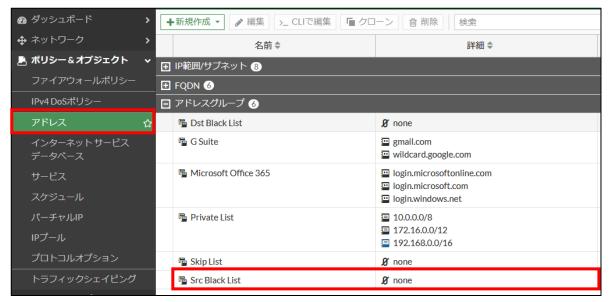


図 6-9. Src Black List 選択画面.

- II. メンバーの+をクリックしリストから対象のアドレスを選択し、投入する。
- III. 投入したい分選択したら OK をクリックする。

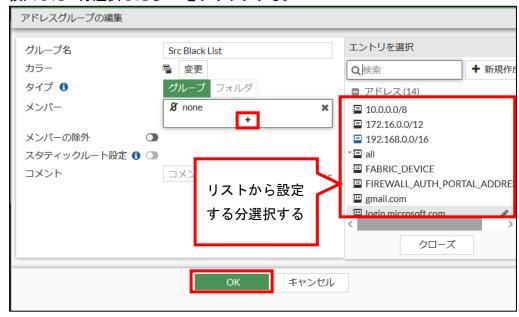


図 6-10. Src Black List 設定画面.



- ③ Skip List への設定方法
 - I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループ にある Skip List をダブルクリックする。

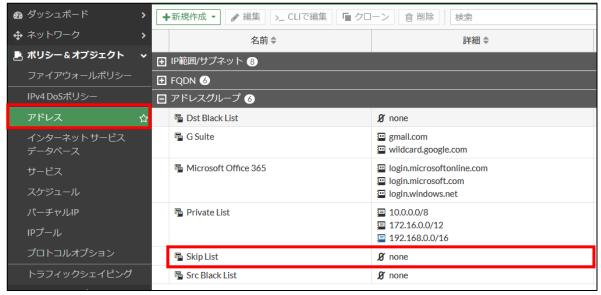


図 6-11. Skip List 選択画面.

- Ⅱ. メンバーの+をクリックしリストから対象のアドレスを選択し、投入する。
- III. 投入したい分選択したら OK をクリックする。



図 6-12. Skip List 設定画面.



- ④ Dst Black List への設定方法
 - I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループ にある Dst Black List をダブルクリックする。

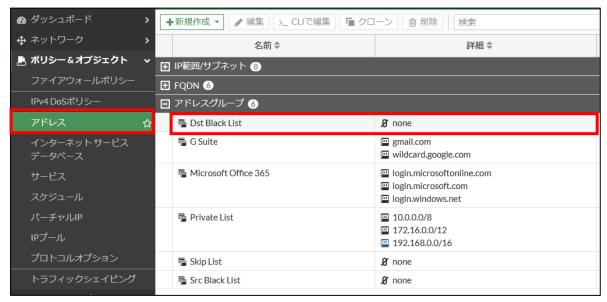


図 6-13. Dst Black List 選択画面.

- II. メンバーの+をクリックしリストから対象のアドレスを選択し、投入する。
- III. 投入したい分選択したら OK をクリックする。



図 6-14. Dst Black List 設定画面.



6.4 アドレスグループの削除

① 左のメニューからポリシー&オブジェクト->アドレスを選択する。



図 6-15. アドレス選択画面.

② 削除したいアドレスグループをクリックし、削除をクリックします。

+新規作成▼ → 編集 >_ CLIで編集 「 クローン						
名前◆	詳細◆	インターフェース \$	タイプ ♦	参照◆		
FQDN 6						
□ アドレスグループ ⑦						
□ Dst Black List	Ø none		アドレスグループ	1		
₲ G Suite	gmail.com wildcard.google.com		アドレスグループ	0		
Microsoft Office 365	☐ login.microsoftonline.com ☐ login.microsoft.com ☐ login.windows.net		アドレスグループ	0		
Private List	10.0.0.0/8 172.16.0.0/12 172.168.0.0/16		アドレスグループ	1		
■ Skip List	Ø none		アドレスグループ	1		
😼 Src Black List	Ø none		アドレスグループ	1		
% リスト1	□ 192.168.0.0/24 □ 192.168.2.0/24		アドレスグループ	0		

図 6-16. 削除対象アドレスグループの選択画面.

③ 確認ウィンドウがでるので、OK をクリックします。

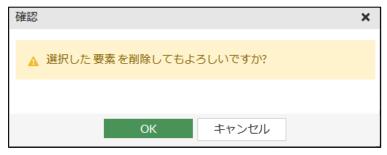


図 6-17. 削除アドレスの確認画面.

※ファイアウォールポリシーの送信元、宛先に設定されているアドレスグループは削除することができません。



7 サービスの設定方法

本章では、ファイアウォールルールで設定するサービス (TCP や UDP など) の設定方法について解説しています。

7.1 サービスの追加

① 左のメニューからポリシー&オブジェクト->サービスを選択する。

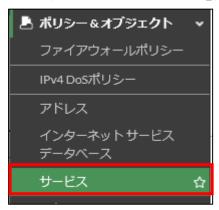


図 7-1. サービス選択画面.

- ② 新規作成をクリックし、名前の記載、プロトコルタイプを選択する。 ※プロトコルタイプは3種類ありますが、TCP/UDP/SCTPを使用することを推奨します。
 - I. プロトコルタイプ TCP/UDP/SCTP を選択した場合、アドレス、宛先ポートを記載し、 OK をクリックする。

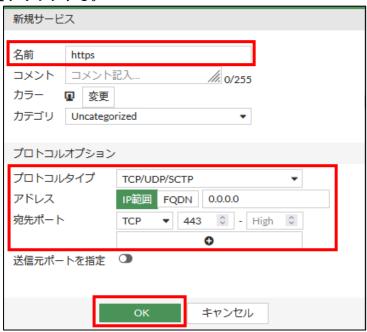


図 7-2. サービス設定画面.



7.2 サービスの変更

① 左のメニューから「ポリシー&オブジェクト->サービス」を選択する。

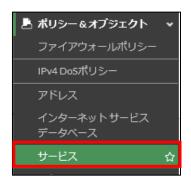


図 7-3. サービス選択画面.

② 変更対象のサービスをダブルクリックする。

≡ Q				>_ 0 - 1	ሷ1 → 9 nt	tpc •
+ 新規作成 / 編集	■ クローン 前 削除			サービス	サービスグル・	ープ
○ Q 検索						Q
名前◆	詳細 🗢	IP/FQDN \$	カテゴリ 🕏	プロトコル 🗘	参照 🕏	
№ нттр	TCP/80	0.0.0.0	Web Access	TCP/UDP/SCTP	1	-
■ HTTPS	TCP/443	0000	Web Access	TCP/UDP/SCTP	2	
https	TCP/443	0.0.0.0	未分類	TCP/UDP/SCTP	0	ŀ
Ū IKE	UDP/500 UDP/4500	0.0.0.0	Tunneling	TCP/UDP/SCTP	0	
☑ IMAP	TCP/143	0.0.0.0	Eメール	TCP/UDP/SCTP	1	
☑ IMAPS	TCP/993	0.0.0.0	Eメール	TCP/UDP/SCTP	1	
INFO ADDRESS	ICMP/ANY		未分類	ICMP	0	

図 7-4. 変更対象サービスの選択画面.

③ 変更する項目を変更し、OKをクリックする。

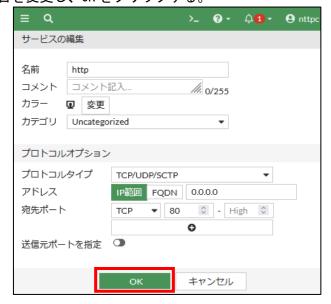


図 7-5. 変更対象サービスの設定画面.



7.3 サービスの削除

① 左のメニューからポリシー&オブジェクト->サービスを選択する。

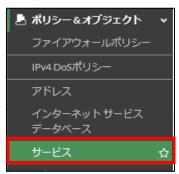


図 7-6. サービス選択画面.

② 削除対象のサービスを選択し、削除をクリックする。

≡ Q				>_ ?·	△1 - 9 nttpo
★ 新規作成 📝 編集				Q J -E	ス サービスグループ
名前 ♣	詳細◆	IP/FQDN \$	カテゴリ 🕏	プロトコル 🕏	参照章
□ FTP_GET	TCP/21	0.0.0.0	File Access	TCP/UDP/SCTP	0
■ FTP_PUT	TCP/21	0.0.0.0	File Access	TCP/UDP/SCTP	0
■ GOPHER	TCP/70	0.0.0.0	未分類	TCP/UDP/SCTP	0
■ GRE	IP/47		Tunneling	IP	0
■ H323	TCP/1720 TCP/1503 UDP/1719	0.0.0.0	VoIP, Messaging & Other Appl	TCP/UDP/SCTP	0
■ HTTP	TCP/80	0.0.0.0	Web Access	TCP/UDP/SCTP	1
■ HTTDS	TCD/M/3	0000	Web Access	TCD/HDD/SCTD	2
🖳 https	TCP/443	0.0.0.0	未分類	TCP/UDP/SCTP	0
⊋ IKE	UDP/500 UDP/4500	0.0.0.0	Tunneling	TCP/UDP/SCTP	0
■ IMAP	TCP/143	0.0.0.0	Eメール	TCP/UDP/SCTP	1
■ IMAPS	TCP/993	0.0.0.0	Eメール	TCP/UDP/SCTP	1
INEO ADDRESS	ICMD/ANIV		土八湘	ICMD	0
セキュリティレーティン	グ問題				25%

図 7-7. 削除対象サービス選択画面.

③ 確認ウィンドウがでるので、OK をクリックする。

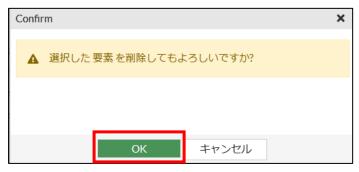


図 7-8. 削除サービスの確認画面.



8 サービスグループの設定方法

本章では、7章で作成したサービスをグルーピングする方法を解説しています。

- ※ 事前に7.1項で登録したサービスの作成が必要となります。
- 8.1 サービスグループの追加
 - ① 左のメニューからポリシー&オブジェクト->サービスを選択する。

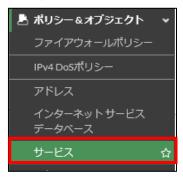


図 8-1. サービス選択画面.

② 右の選択肢からサービスグループを選択し、新規作成をクリックする。



図 8-2. サービスグループ新規作成選択画面.

③ 名前を任意で記載、メンバーで対象のサービスをエントリから選択し OK をクリックする。



図 8-3. サービスグループ新規作成画面.



- 8.2 サービスグループの変更
 - ① 左のメニューからポリシー&オブジェクト->サービスを選択する。

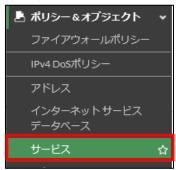


図 8-4. サービス選択画面.

② 右の選択肢からサービスグループを選択し、変更したいサービスグループをダブルクリックする。



図 8-5. サービスグループ選択画面.

③ 変更したい項目を変更し、OKをクリックする。



図 8-6. サービスグループ変更画面.



- 8.3 サービスグループの削除
 - ① 左のメニューからポリシー&オブジェクト->サービスを選択する。

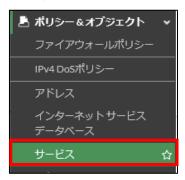


図 8-7. サービス選択画面.

② 右の選択肢からサービスグループを選択し、削除したいサービスグループを選択し削除を クリックする。



図 8-8. サービスグループ選択画面.

③ 確認画面が表示されるので OK をクリックする。

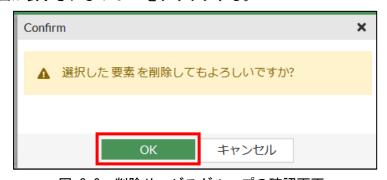


図 8-9. 削除サービスグループの確認画面.



- 9 ファイアウォールポリシーの有効化・無効化
 - 9.1 ファイアウォールポリシーの有効化
 - ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択

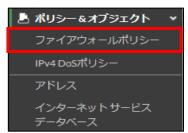


図 9-1. ファイアウォールポリシー選択画面.

② 有効化したいポリシーを右クリックし、設定ステータスから有効をクリックします。



図 9-2. ファイアウォールポリシー設定画面.



- 9.2 ファイアウォールポリシーの無効化
 - ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。

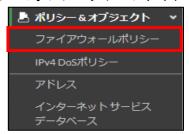


図 9-3. ファイアウォールポリシー選択画面.

② 無効化したいポリシーを右クリックし、設定ステータスから無効をクリックします。

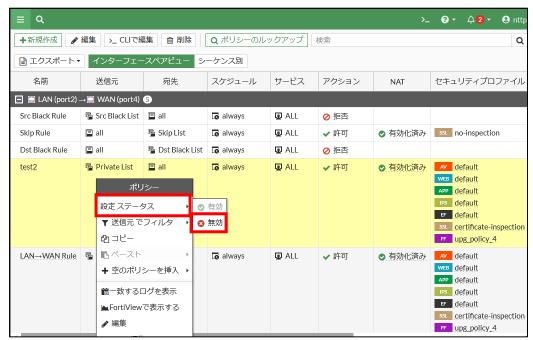


図 9-4. ファイアウォールポリシー選択画面.

- ③ 対象のポリシーが無効になったことを確認する。
 - ※対象ポリシーに赤色で×がついていることで無効化されます。
 - ※プリセットされているファイアウォールポリシーを無効化した場合、動作保証はできません。



10 セキュリティプロファイル:アンチウイルス

本章では、アンチウイルス機能の設定方法について解説しています。

アンチウイルス機能は、vUTM を通過する通信の中からマルウェア (ウイルス)をダウンロードする通信等を検知し、遮断等を行います。

マルウェアに感染した場合、端末が遠隔操作される・情報が盗まれる・データが破壊される等の 被害が発生する恐れがあります。

vUTM のアンチウイルス機能を用いることで、日々更新されるマルウェアのデータベースを用いて 通信中のマルウェアを検知し、遮断することが可能です。

アンチウイルス機能については以下のページをご参照ください。

https://www.fortiguard.com/services/antivirus

10.1 アンチウイルスの設定

① 左メニューより、ポリシー&オブジェクト→ファイアウォールポリシー -> LAN(port2) → WAN(port1) の LAN→WAN Rule をダブルクリックする。

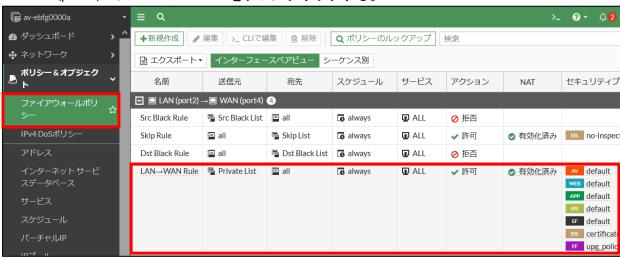


図 10-1. ファイアウォールポリシー選択画面.



② セキュリティプロファイル -> アンチウイルスにプリセットされている default にカーソルを合わせて編集をクリックします。

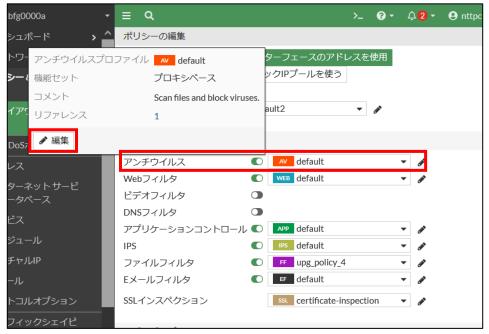


図 10-2. アンチウイルス編集選択画面.

I. インスペクションされるプロトコル監視対象にするプロトコルを「インスペクションされるプロトコル」より選択し有効化または無効化する。

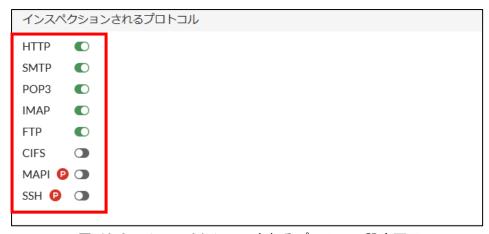


図 10-3. インスペクションされるプロトコル設定画面.



II. APT プロテクションオプション

APT プロテクションオプションでは、下記2項目の設定切り替えが行えます。

- ① Eメール添付の Windows 実行ファイルをウイルスとして扱う
- ② モバイルマルウェアプロテクションを含める



図 10-4. APT プロテクションオプション設定画面.

III. ウイルスアウトブレイク防止→サービス提供外となります。



10.2 アンチウイルスの有効化・無効化

下記のように設定されていることを確認し「OK」をクリックします。

① 有効化の場合

アンチウイルス:有効かつ、default が選択されていること このポリシーを有効化:有効になっていること



図 10-5. アンチウイルス有効設定画面.

② 無効化の場合

アンチウイルス:無効化されていること

このポリシーを有効化:有効になっていること



図 10-6. アンチウイルス無効設定画面.



11 セキュリティプロファイル: Web フィルタ

本章では、Web フィルタ機能の設定方法について解説しています。

Web フィルタ機能は、ネットワーク内の端末から Fortinet 社のデータベースによって分類された Web サイトを制限・監視します。

悪意のある Web サイトや情報漏えいリスクのある Web サイトへのアクセスを制限することで、ビジネスにおけるセキュリティリスクを大幅に低減することが可能です。

また、それぞれのカテゴリの Web サイトがどの程度利用されているかを把握することは、管理者が 組織内のネットワーク利用状況を把握する上で助けとなります。

Web フィルタ機能については以下のページをご参照ください。

https://www.fortiguard.com/services/wf

Web サイトは予め定義されたカテゴリに分類されます。またカテゴリを基に細かな Web フィルタリングポリシーの設定が可能です。

カテゴリについては以下のページをご参照ください。

https://fortiguard.com/webfilter/categories

個々のWebページがどのカテゴリに分類されているかについては以下のページからご確認いただけます。

https://fortiguard.com/webfilter

11.1 Web フィルタの設定

① 左メニューより、ポリシー&オブジェクト→ファイアウォールポリシー → LAN (port2) →WAN (port2) の LAN→WAN Rule をダブルクリックします。

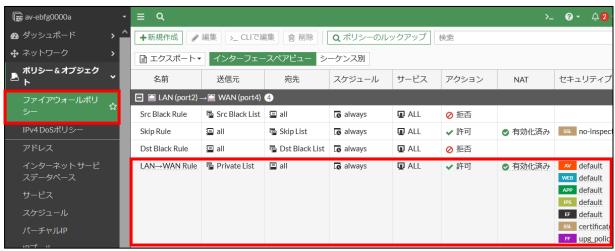


図 11-1. ファイアウォールポリシー選択画面.



② セキュリティプロファイル -> Web フィルタにプリセットされている default にカーソル を合わせて編集をクリックします。

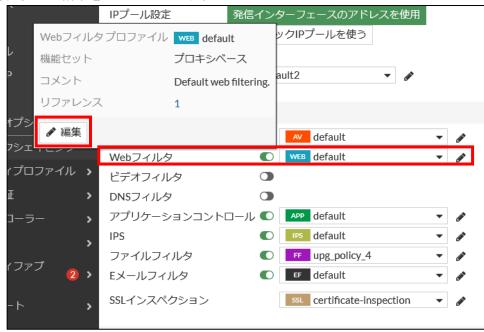


図 11-2. Web フィルタ編集画面.

I. Forti Guard カテゴリベースのフィルタ

FortiGuard カテゴリの大項目(親カテゴリ)内に表示されている小項目(子カテゴリ)を選択し、許可、モニタ、ブロックのいずれかのアクションを選択する。FortiGuard カテゴリの大項目(親カテゴリ)は、以下8項目になります。

※子カテゴリを表示させる場合は左+をクリックする。

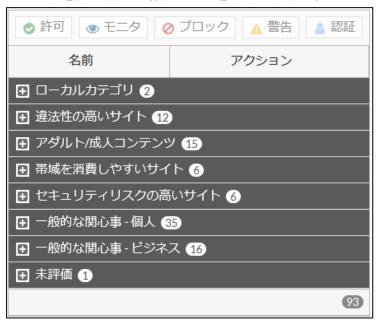


図 11-3. FortiGuard カテゴリベースのフィルタ画面.



アクションについての詳細は下記のとおりです。

許可:カテゴリ内のサイトへのアクセスを許可します。

モニタ:カテゴリ内のサイトへのアクセスを許可し、ログに記録します。

カテゴリ使用クォータの利用には「モニタ」を選択する必要があります。

ブロック:カテゴリ内のサイトへのアクセスを禁止します。

ブロックされたサイトにアクセスしようとしているユーザには、

サイトがブロックされていることを示す代替メッセージが表示されます。

※未評価についてはモニタ設定を推奨いたします。

ブロック設定にした場合、著しくスループットが落ちますのでご注意ください。

※ローカルカテゴリについてはサービス提供外となります。



II. カテゴリ使用クォータ

こちらを使用することにより対象のカテゴリに所属している URL へのアクセス制限がユーザごとにできるようになります。

制限内容としては、指定された時間内または特定の帯域幅に達した時点でサイトへのアクセスができなくなります。(ブロック画面が表示されます。)

- ※毎日深夜にリセットされるので制限に達した場合は、 翌朝再度アクセスを実施するようお願いいたします。
- ※FortiGuard カテゴリベースのフィルタでモニタ設定になっているカテゴリのみ設定可能です。

例:オンライン会議を時間制限設定する場合

① 新規作成をクリック



図 11-4. カテゴリ使用クォータ編集画面.

② カテゴリの「+」をクリックし、プルダウンリストより「オンライン会議」を選択。 クォータの種類は「時間」を選択。

クォータ合計「5分」に設定し、OKをクリック



図 11-1. クォータ編集画面.



③ カテゴリの「+」をクリックし、プルダウンリストより「オンライン会議」を選択。 クォータの種類は「時間」を選択。

クォータ合計「5分」に設定し、OKをクリック



図 11-6. カテゴリ使用クォータ編集画面.

- ※ダッシュボードに Forti Guard クォータを設定することにより、使用状況をモニタすることが可能です。
- ④ ダッシュボード->ステータスの左上部、ウィジェットの追加をクリックする。



図 11-7. ウィジェット選択画面.

⑤ ユーザ&認証にある FortiGuard クォータを選択し、ウェジェット追加をクリック する。



図 11-8. FortiGuard 選択画面.



⑥ ダッシュボードの最下部に表示されるのでユーザ単位での使用済みトラフィック クォータが確認できます。



図 11-9. FortiGuard クォータ画面.

- III. ユーザにブロックされたカテゴリのオーバーライドを許可する →サービス提供外となります。
- IV. サーチエンジン→サービス提供外となります。
- V. スタティック URL フィルタ
 - i. 無効な URL をブロック この設定を使用することにより、SSL 証明書の CN フィールドに有効なドメイン名が 含まれていない場合に Web サイトをブロックします。
 - ii. URL フィルタ

テキストと正規表現を含むパターンで特定の URL を追加することにより、指定された URL またはパターンに一致する Web ページへのアクセスを除外(exempt)、ブロック、許可、モニタにします。

URL フィルタのタイプについての詳細は下記のとおりです。

シンプル:ドメイン(完全一致)及びサブドメインを含むドメインに一致する。

正規表現/ワイルドカード:ルールに基づいたパターンに一致する。



URL フィルタのアクションについての詳細は下記のとおりです。

除外(exempt): 許可され、後続の Web フィルタ機能(Web コンテンツフィルタなど) に渡されません。

ブロック:通信をブロックし口グに記録する。

許可: 許可され、後続の Web フィルタ機能 (Web コンテンツフィルタなど) に渡されます

モニタ: 許可され、後続の Web フィルタ機能 (Web コンテンツフィルタなど) に渡された後にログに記録されます。

例:https://www.ntt-east.co.jp をタイプシンプルでブロックする場合

① URL フィルタを有効化し、新規作成をクリックする。



図 11-10. URL フィルタ新規作成画面.

② URL、タイプ、アクション、ステータスを入力し OK をクリックする。



図 11-11. URL フィルタ設定画面.



iii.FortiSandbox により検知された悪意のある URL をブロック

FortiSandbox で検知された悪意のあるファイルをブロックしたい場合はアクションを「有効」にしてください。

iv. コンテンツフィルタ

特定の単語やパターンを含む Web ページを設定することで対象の Web サイトへのアクセスを除外、ブロック等制御することが可能です。

VI. レーティングオプション

- i. レーティングエラー発生時に Web サイトを許可 FortiGuard Web Filtering サービスでレーティングにエラーが発生したサイト を許可します。
- ii. ドメインまたは IP アドレスで URL をレーティング ブロックに指定されている web サイトを、IP でもフィルタリング可能としま す。ただし、DB の更新状況によりブロックできないことがあります。

VII. プロキシオプション

- i. Google アカウントの使用を特定のドメインに制限 →サービス提供外となります。
- ii. HTTP POST アクション

HTTP POST は入力したフォームやサーバにアップロードするファイルなどの情報を送信するときにブラウザが使用するコマンドです。

iii. Java アプレット、ActiveX、Cookie を削除

Web フィルタには、Web トラフィックから Java アプレット、ActiveX、Cookie をフィルタリングする設定があります。本削除機能を有効にすると、Java アプレット、ActiveX、Cookie を使用する Web サイトが正しく機能しなくなる場合があります。



11.2 Web フィルタの有効化・無効化

下記のように設定されていることを確認し「OK」をクリックします。

① 有効化の場合

Web フィルタ:有効かつ、default が選択されていること このポリシーを有効化:有効になっていること



図 11-12. Web フィルタ有効化設定画面.

② 無効化の場合

Web フィルタ:無効化されていること

このポリシーを有効化:有効になっていること



図 11-13. Web フィルタ無効化設定画面.



12 セキュリティプロファイル:アプリケーションコントロール

本章では、アプリケーションコントロールについて解説しています。

アプリケーションコントロール機能は、ネットワーク内の通信状況から Fortinet 社のデータベースによって分類されたアプリケーションを制限・監視します。

セキュリティリスクのあるアプリケーションによる通信を制限することで、ビジネスにおけるセキュリティリスクを大幅に低減することが可能です。

また、業務に無関係なアプリケーションの利用を発見し通信を制限することで、ネットワーク帯域の最適化や業務効率化が期待できます。

アプリケーションコントロール機能については以下のページをご参照ください。

https://www.fortiguard.com/services/appcontrol

12.1 アプリケーションコントロールの設定

① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシー→LAN(port2)→WAN(port1)のLAN→WAN Rule をダブルクリックします。

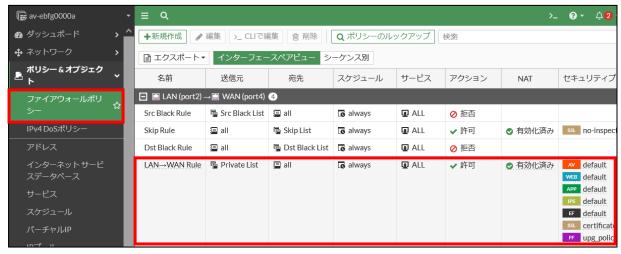


図 12-1. ファイアウォールポリシー選択画面.



② セキュリティプロファイル->アプリケーションコントロールにプリセットされている default にカーソルを合わせて編集をクリックします。



図 12-2. アプリケーションコントロール編集画面.



I. カテゴリ

カテゴリを使用すると、カテゴリタイプに基づいてシグネチャのグループを選択することが可能です。※シグネチャについては対象カテゴリにカーソルを合わせ「シグネチャを表示」をクリックすると確認可能です。



図 12-3. シグネチャ表示画面.

カテゴリより対象カテゴリを選択し、左プルダウンよりモニタ、許可、ブロックの いずれかのアクションを選択し、適用をクリックします。

カテゴリは下記 18 項目になります。

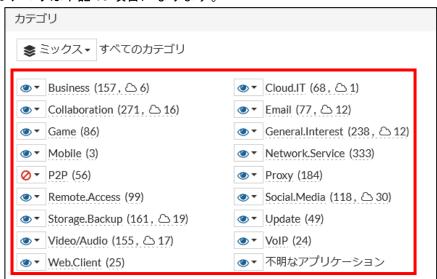


図 12-4. カテゴリ表示画面.

カテゴリに対するアクションの詳細については下記のとおりです。

モニタ:カテゴリ内のサイトへのアクセスを許可し、ログに記録します。

許可:カテゴリ内のサイトへのアクセスを許可します。

ブロック:カテゴリ内のサイトへのアクセスを禁止します。

ブロックされたサイトにアクセスしようとしているユーザには、

サイトがブロックされていることを示す代替メッセージが表示されます。

※隔離についてはサービス提供外となります。



II. ネットワークプロトコルの強制

プロトコルの設定により、既知のポート(21、80、443 など)でネットワークサービス (FTP、HTTP、HTTPS など)を構成できます。選択したポートで許可リストにないプロトコルの場合、IPS エンジンは違反アクションを実行して、そのトラフィックをブロック、許可、または監視します。

ネットワークプロトコルの強制に対する詳細については下記のとおりです。

ポート:ポートを選択します。

プロトコルの強制:強制したいプロトコルを選択します。

違反アクション:「ポート」と「プロトコルの強制」が一致しない場合のアクション

モニタ:トラフィックは通過しますが、ログ メッセージは生成されません。

ブロック:検出されたトラフィックをドロップし、ログ メッセージを生成します。

例:HTTP 通信をブロックする場合

i. ネットワークプロトコルの強制を有効化し、新規作成をクリックする。



図 12-5. ネットワークプロトコルの強制新規作成画面.

- ii.ポートにポート番号「80」を入力、プロトコルの強制については、「+」をクリックし「HTTP」を選択します。
- iii. 違反アクションで「ブロック」を選択し OK をクリックする。



図 12-6. ネットワークプロトコルの強制設定画面.



III. アプリケーションとフィルタのオーバーライド

I.カテゴリとは別に個別にアプリケーションまたはフィルタの通信の許可、ブロックなどの処理を可能とします。

個別のアプリケーションに対するタイプの詳細は下記のとおりです。

アプリケーション:既存のアプリケーションシグネチャの一覧から選択します。

フィルタ:アプリケーションカテゴリ/プロトコル/リスク等のフィルタの一覧から 選択します。

※フィルタについてはサービス提供外となります。

個別のアプリケーションに対するアクションの詳細は下記のとおりです。

モニタ:カテゴリ内のサイトへのアクセスを許可し、ログに記録します

許可:カテゴリ内のサイトへのアクセスを許可します

ブロック:カテゴリ内のサイトへのアクセスを禁止します

ブロックされたサイトにアクセスしようとしているユーザには、

サイトがブロックされていることを示す代替メッセージが表示されます

※隔離についてはサービス提供外となります。

また、一部サービス提供不可のシグネチャが存在します。

アプリケーションシグネチャの名前の右側に鍵アイコンが表示されたシグネチャは SSL インスペクション:「deep-inspection」機能が必要となります。

そのため、鍵アイコンが表示された該当のシグネチャはサービス提供外となります。 下記は Zoom の例となります。



図 12-7. 一部サービス提供不可のシグネチャの例.



例:YouTube の通信をブロックする場合

i. 新規作成をクリックする。



図 12-8. アプリケーションとオーバーライド新規作成画面.

- ii. タイプを「アプリケーション」、アクションを「ブロック」に設定します。
- iii. 検索ボックスにて「youtube」を入力し検索し、「すべての結果を追加」をクリック します。



図 12-9. アプリケーションとオーバーライド設定画面.

iv. 検索したシグネチャにチェックがついていることなどを確認し下部の「OK」をクリックする。

0	YouTube	■ Video/Audio	Browser-Based	****
•	YouTube.Downloader.YT	■ Video/Audio	Client-Server	****
•	YouTube_Category.Contr	■ Video/Audio	Browser-Based	****
0	YouTube_Channel.Access	■ Video/Audio	Browser-Based	****
0	YouTube_Channel.Contro	■ Video/Audio	Browser-Based	****
•	YouTube_Channel.ID 🛆 🔒	■ Video/Audio	Browser-Based	****

図 12-10. アプリケーションとオーバーライド確認画面.



IV. オプション

i. デフォルト以外のポートで検出されたアプリケーションをブロック モニタ及び許可アクションの場合、デフォルト以外のポート(Forti Guard アプリケーションシグネチャで定義)で検出されるとアプリケーションはブロックされます。

ブロックアクションはポートに関係なくアプリケーションの据えてのトラフィックをブロックします。

- ii. DNS トラフィックの許可とログ 有効化した場合 DNS の通信を許可し、またログへの記録をします。
- iii. HTTP ベースアプリケーションの差し替えメッセージ →サービス提供外となります。



- 12.2 アプリケーションコントロールの有効化・無効化 下記のように設定されていることを確認し「OK」をクリックします。
 - ① 有効化の場合

アプリケーションコントロール:有効かつ、default が選択されていること このポリシーを有効化:有効になっていること



図 12-11. アプリケーションコントロール有効化画面.

② 無効化の場合

アプリケーションコントロール:無効化されていること このポリシーを有効化:有効になっていること



図 12-12. アプリケーションコントロール無効化画面.



13 セキュリティプロファイル:侵入防止(IPS)

本章では、侵入防止(IPS)について解説しています。

侵入防止(IPS)機能は、外部からネットワークに侵入するための攻撃やネットワーク内部の端末・サーバが侵入されてしまった際に行われる通信を検知・遮断します。

これらは主にアプリケーションの脆弱性を狙った攻撃であり、ファイアウォール機能をすり抜ける可能性があります。

検知された通信に対し、意図しない動作をしている場合は、設定変更を検討願います。

侵入防止(IPS)機能の詳細については以下のページをご参照ください。

https://www.fortiguard.com/services/ips

13.1 侵入防止(IPS)の設定

① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシー→LAN(port2) → WAN(port1) の LAN->WAN Rule をダブルクリックします。



図 13-1. ファイアウォールポリシー選択画面.



② セキュリティプロファイル->IPS にプリセットされている default にカーソルを合わせて編集をクリックします。

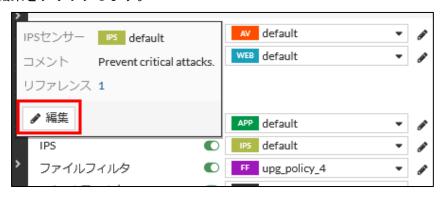


図 13-2. IPS 編集画面.

I. 悪意のある URL をブロック FortiGate 上のローカルの悪意のある URL データベースに基づいて悪意のある

URL をブロックし、ドライブバイ エクスプロイトの検出を支援します。

II. IPS シグネチャとフィルタ 侵入防止(IPS)は脆弱性をつく攻撃を検出し、保護されたデバイスを含むネットワークへの脅威の侵害を防ぎます。



図 13-3. IPS 初期設定.



IPS シグネチャに対するタイプの詳細は下記のとおりです。

フィルタ: ターゲット/重大度/プロトコル/OS/アプリケーション等のフィルタの一覧から選択します。

シグネチャ:既存の IPS シグネチャの一覧から選択します。

※フィルタについてはサービス提供外となります。

IPS シグネチャに対するアクションの詳細は下記のとおりです。

許可:トラフィックが宛先に到達し続けることを許可します。

モニタ:トラフィックが宛先に到達し続け、アクティビティを記録できるようにします。 ブロック:シグネチャに一致するトラフィックをドロップします。

デフォルト: シグネチャのデフォルトのアクションを使用します。[IPS シグネチャ] ペインでシグネチャを検索して、デフォルトのアクションを表示します。

※リセット、隔離についてはサービス提供外となります。

IPS シグネチャに対するステータスの詳細は下記のとおりです。

有効:シグネチャを有効にします。

無効:シグネチャを無効にします。

デフォルト: シグネチャのデフォルトのステータスを使用します。[IPS シグネチャ]ペインでシグネチャを検索して、デフォルトのステータスを表示します。

例: EICAR の通信をブロックする場合

i. 新規作成をクリックする。



図 13-4. IPS シグネチャとフィルタ新規作成画面.



ii. タイプを「フィルタ」→「シグネチャ」、アクションを「デフォルト」→「ブロック」に設定します。

※パケットロギング、レートベースの設定、除外 IP はサービス提供外となります。

iii. 検索ボックスにて「eicar」を入力し検索し、「すべての結果を追加」をクリック します。



図 13-5. IPS シグネチャとフィルタ設定画面.

iv. 検索したシグネチャにチェックがついていることなどを確認し、下部の「OK」を クリックする。



図 13-6. IPS シグネチャとフィルタ確認画面.

III. ボットネット C&C

ボットネットを始めとする脅威とコマンド&コントロールサーバ(C&C)の通信を遮断することで、データの不正取得やマルウェアのダウンロードを回避します。

ボットネット C&C に対するアクションの詳細は下記のとおりです。

無効:ボットネットサーバへの接続をスキャンしません。

ブロック:ボットネットサーバへの接続をブロックします。

モニタ:ボットネットサーバへの接続をログに記録します。



13.2 侵入防止(IPS)の有効化・無効化

下記のように設定されていることを確認し「OK」をクリックします。

① 左メニューよりポリシー&オブジェクト->ファイアウォールポリシー->LAN(port2) → WAN(port1)のLAN->WAN Rule をダブルクリックします。



図 13-7. ファイアウォールポリシー選択画面.

② 有効化の場合

IPS:有効かつ、defaultが選択されていること このポリシーを有効化:有効になっていること



図 13-8. IPS 有効化画面.



③ 無効化の場合

IPS:無効化されていること

このポリシーを有効化:有効になっていること



図 13-9. IPS 無効化画面.



14 ファイルフィルタ

本章では、ファイルフィルタについて解説しています。

ファイルフィルタを使用することにより、vUTM を通過する様々な種類のファイルを許可またはブロックすることが可能となります。

ファイアウォールポリシーに直接適用でき、様々なトラフィックプロトコルをサポートできます。

14.1 ファイルフィルタの設定

① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシー→LAN(port2)→WAN(port1)のLAN→WAN Rule をダブルクリックします。



図 14-1. ファイアウォールポリシー選択画面.

② セキュリティプロファイル->ファイルフィルタにプリセットされている default にカー ソルを合わせて編集をクリックします。

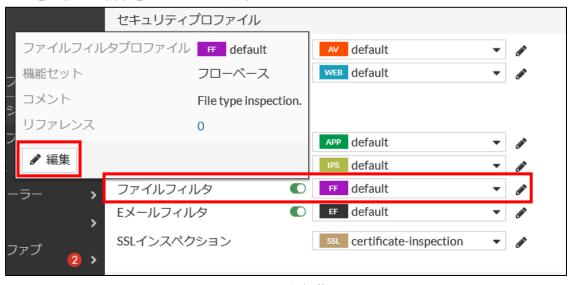


図 14-2. ファイルフィルタ編集画面.



I. ルール

ルールを使用することにより、プロトコル、トラフィック、ファイルタイプ別に対象のファイルを許可またはブロックすることが可能です。

ルールに対するトラフィックの詳細は下記のとおりです。

着信:セッションの応答方向に送信されたファイルと一致します。 発信:セッションの発信方向に送信されたファイルと一致します。

両方:セッションの発信方向と応答方向で送信されたファイルに一致します。

ルールに対するアクションの詳細は下記のとおりです。

モニタ:コンテンツを許可し、ログ メッセージを書き込みます

ブロック:コンテンツをブロックし、ログ メッセージを書き込みます

例:メールで zip ファイルを受信できなくする場合

i. 新規作成をクリックする。



図 14-3. ファイルフィルタ新規ルール作成画面.

- ii. 名前を記載する。
- iii. プロトコルで「POP3 以外をすべて×をクリックして削除する。
- iv. トラフィックで着信をクリックする。
- v. ファイルタイプの+をクリックし、zip を選択する。



vi. アクションでブロックを選択し、OK をクリックする。



図 14-4. 新規ルール設定画面.

※パスワードで保護されている場合のみについて、有効の場合、 パスワードで保護されたファイルの照合を有効にします。 設定が有効になっていない場合は、どのファイルでも一致します。



14.2 ファイルフィルタの有効化・無効化

下記のように設定されていることを確認し「OK」をクリックします。

① ファイルフィルタの有効化

ファイルフィルタ:有効かつ、default であること

このポリシーを有効化:有効になっていること



図 14-5. ファイルフィルタ有効化設定画面.

② ファイルフィルタの無効化

ファイルフィルタ:無効化されていること

このポリシーを有効化:有効になっていること



図 14-6. ファイルフィルタ無効化設定画面.



15 セキュリティプロファイル: Eメールフィルタ本章では、Eメールフィルタについて解説しています。Eメールフィルタとは、スパム検出とフィルタリングをする機能です。

Eメールフィルタ機能の詳細については以下のページをご参照ください。

https://www.fortiguard.com/services/antispam

15.1 Eメールフィルタプロファイルの設定

① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシー→LAN(port2)→WAN(port1)のLAN→WAN Rule をダブルクリックします。



図 15-1. ファイアウォールポリシー選択画面.

② セキュリティプロファイル->Eメールフィルタにプリセットされている「default」にカーソルを合わせて編集をクリックします。

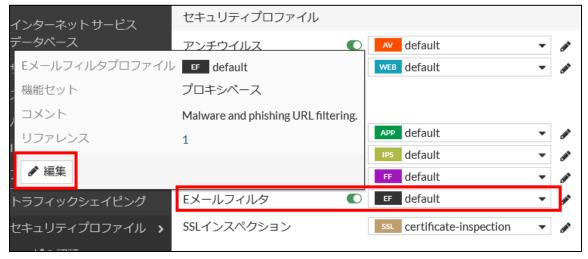


図 15-2. Eメールフィルタ編集画面.



I. プロトコルごとのスパム検知数

SMTP、POP3、IMAP プロトコルの 3 プロトコルあり、各プロトコルはセクション分けされているので各セクションでプロトコルのログを破棄 (SMTP のみ)、タグ、転送のアクションをスパムアクションより設定できます。

スパムアクションの詳細は下記のとおりです。

転送:スパムメールの送受信を許可します。

タグ:件名またはヘッダーに設定されたテキストでスパムメールにタグをつ

けます。

破棄:スパムメールを破棄(ブロック)します。

※スパムアクションでタグを選択した場合、タグの挿入箇所、タグ形式を任意で選択、記載が可能です。



図 15-3. プロトコルごとのスパム検知設定画面.

II. FortiGuard スパムフィルタリング

下記 5 つの項目を有効化または無効化することにより、スパマーの IP アドレスまたは E メール、既知のフィッシング URL、既知のスパム URL、既知のスパム E メールチェックサムなどを F Forti G Guard サーバより参照して特定します。

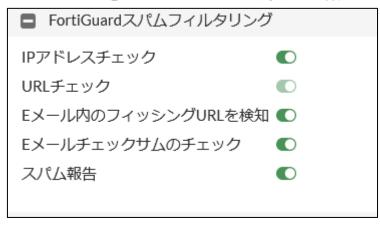


図 15-4. FortiGuard スパムフィルタリング設定画面.



III. ローカルスパムフィルタリング

電子メールまたは IP サブネットからブラックリスト/ホワイトリストを作成して、電子メールの送受信を禁止または許可することができます。

また、HELO DNS ルックアップ、リターン E メール DNS チェックを有効化することによって、Forti Gate が spam he lodns と spamraddrdns コマンドを使用して、he lo SMTP メッセージで使用されているマシン名や return-to フィールドに対して標準の DNS チェックを実行し、これらの名前が登録済みドメインに属しているかどうかを 判断します。

i. ブラック/ホワイトリスト

ブロック/許可リストは、送信者の E メールアドレスのパターンまたは IP サブネットに対して、E メールの送受信を禁止または許可することができます。E メールアドレスは正規表現またはワイルドカードで指定できます

ブラック/ホワイトリストに対するタイプの詳細は下記のとおりです。

IP/ネットマスク:送信元の IP アドレスと指定した IP アドレスを比較します。

受信者アドレス:送信者のメールアドレス内の RCPT TO エンベロープ

ヘッダーおよび To: メール ヘッダーと指定したパターンを比較します。

送信者アドレス:送信者の電子メールアドレス内の MAIL FROM エンベロープ

ヘッダー、From: メール ヘッダー、および Sender: メール ヘッダーと指定したパターンを比較します。

サブジェクト:送信者の電子メールアドレス内の Subject: メール ヘッダーの内容 と指定したパターンを比較します。

ブラック/ホワイトリストに対するアクションの詳細は下記のとおりです。

拒否としてマーク:電子メールは宛先に到達する前に破棄する。

スパムとしてマーク:電子メールの通過は許可されますが、電子メールをスパムとしてマークするインジケーターをタグ付けする。

クリアとしてマーク:電子メールは、スパムではないという前提で、宛先に到達することを許可する。



① ブラック/ホワイトリストの新規作成をクリックする。



図 15-5. ローカルスパムフィルタリング新規作成画面.

② タイプ、IP/ネットマスク・パターン、アクションを選択入力し、ステータスが 有効であることを確認し OK をクリック



図 15-6. ローカルスパムフィルタリング設定画面.



15.2 Eメールフィルタの有効化・無効化

下記のように設定されていることを確認し「OK」をクリックします。

① 有効化の場合

E メールフィルタ:有効かつ、default が選択されていること このポリシーを有効化:有効になっていること



図 15-7. Eメールフィルタ有効化設定画面.

② 無効化の場合

E メールフィルタ:無効化されていること このポリシーを有効化:有効になっていること



図 15-8. Eメールフィルタ無効化設定画面.



16 ダッシュボード

16.1 ステータス

現在利用しているリソースを確認することができます。

必要に応じてダッシュボード上に表示させるウィジェットを変更することができます。 画面左上の「ウィジェット追加」を選択します。

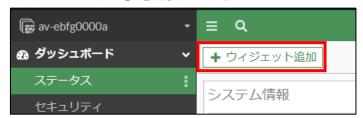


図 16-1. ウィジェット追加画面.

FortiView、セキュリティファブリック、ネットワーク、システム、リソース使用量、セキュリティの項目から必要なものを選択してください。

追加されたウィジェットは表示する時間軸を変更することができます。

変更したいウィジェットの右上にある 1 分から 24 時間で表示されている箇所を押すと、プルダウンから時間を変更できます。



図 16-2. ログ表示時間変更画面.

16.2 LAN/DMZ 上位利用

vUTMを介した通信の利用状況を確認できます。

利用容量ごとの宛先やアプリケーション、Web サイトを表示できます。

表示させる対象によってソートする項目を変更することができます。

また表示に関しても「テーブル」「バブルチャート」から選択できます。

設定する場合は各ウィジェットの右上にある縦の点々マークから「設定」を選択すると各項目を設定できる一覧が表示されます。

この設定の中から期間や利用対象、ソート対象を変更することができます。



16.3 セキュリティ、システムイベント

検知したセキュリティイベント、システムイベントを確認できます。

表示させる対象によってソートする項目を変更することができます。

設定する場合は各ウィジェットの右上にある縦の点々マークから「設定」を選択すると各項目を設定できる一覧が表示されます。

この設定の中から期間や利用対象、ソート対象を変更することができます。

17 FortiView

左メニューよりダッシュボードをクリックすることによって vUTM の通信ログを確認することができます。それぞれのメニューを選択することで「送信元」「宛先」「アプリケーション」「Web サイト」「ポリシー」「セッション」から通信のログを確認することができます。



図 17-1. FortiView 画面.

どのメニューにおいても遡る期間を「直近」「1 時間」「24 時間」「7 日」から指定することができます。



図 17-2. FortiView 表示時間変更画面.

表示させる単位を変更することができます。表示単位はメニューごとに異なります。



18 ログ&レポート

vUTMの通信ログを確認することができます。 下図の3項目より様々なログが確認可能です。



図 18-1. ログ選択画面.

転送トラフィック:vUTM を通過しようとするすべてのログが確認可能です。

システムイベントログ:vUTM上で起こったログが確認可能です。

セキュリティイベントログ:アンチウイルス、アプリケーションコントロール、Web フィルタなどのセキュリティに関するログが確認可能です。

また、表示についてメモリ、ディスク、FortiAnalyzerの3つより選択できます。



図 18-2. ログ表示選択画面.

どのメニューにおいてもログの詳細を表示し確認することができます。

対象のログをクリックし、右上にある詳細をクリックすると詳細ウィンドウが表示されます。

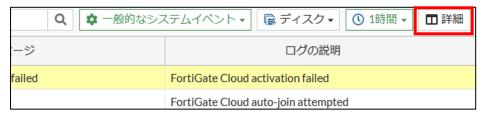


図 18-3. ログ詳細表示選択画面.



また、vUTM が保持しているログをダウンロードして確認することもできます。 左上にあるダウンロードボタンをクリックするとダウンロードができます。

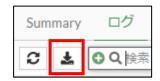


図 18-4. ログダウンロード画面.

左メニューより、ログ&レポート->ログ設定->ローカルログタブより、ディスク使用量、ディスク 使用状況の履歴が確認できます。

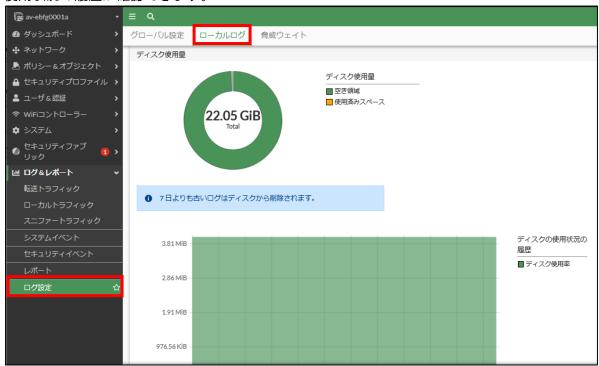


図 18-5. FortiGate ログ量確認画面.



- 19 バージョン差分により削除・移動された設定
 - 19. 1 V6. 2. 7→v7. 2. 5
 - ① Web フィルタ

ファイルフィルタ: Web フィルタから個別プロファイルメニューに昇格 プロキシオプション->YouTube へのアクセスを特定のチャンネルに制限する:設定削除 URL でイメージを評価:設定削除

② アプリケーションコントロール

オプション->QUIC:設定削除

※QUIC をブロック設定したい場合は下記手順にて設定を実施

I. アプリケーションとフィルタのオーバーライドの新規作成をクリックする。



図 19-1. アプリケーションとフィルタのオーバーライド新規作成画面.

II. タイプをアプリケーション、アクションをブロックに設定する。



図 19-2. アプリケーションとフィルタのオーダライド設定画面.

III. 検索ボックスで QUIC を検索、検索結果で出た QUIC を選択し「選択したものを追加」 をクリックし、OK をクリックする。



図 19-3. QUIC 検索画面.

③ Eメールフィルタ

ファイルフィルタ: Web フィルタから個別プロファイルメニューに昇格



20 Q&A

全般

Q:作業中にブラウザが応答しなくなった。

A: ブラウザをリロードして再読み込みをするか、別の種類のブラウザの使用をお試しください。

Q: FortiGate の詳しい仕様を知りたい。

A: Fortinet の以下のサイトをご確認ください。

FortiOS7. 2.5 クックブック

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/954635/getting-started

ファイアウォールアドレス

Q:ポリシー&オブジェクト内のアドレスを削除できない。

A: そのアドレスをグループやポリシーで使用中の場合は削除できません。

最初に使用を解除して下さい。アドレスグループ、サービス、サービスグループについても同様です。

ファイアウォールポリシー

Q:ポリシーの編集で、サービスを「HTTP」から「HTTPS」に変更したが、編集後に確認すると、「HTTP」と「HTTPS」の両方が指定されている。

A:ポリシーの編集から、サービスを変更した場合、「変更」ではなく「追加」となるため、名前の右側にある「×」をクリックしてエントリから削除してください。ポリシーのほかの項目、またはアドレスグループ、サービスグループも同様です。

Q:ポリシーが勝手に動いた。

A:ポリシーは、ドラック&ドロップで順番を変更することができます。

その順番によって優先順位が変更されるため、優先順位を変更するとき以外はポリシーを動かさないように注意してください。

Q:ポリシーで通信を拒否したはずなのに、拒否されない。

A:ポリシーは上から順番に評価されます。設定した拒否ポリシーの上側に許可ポリシーがある場合、その許可ポリシーが優先されます。

優先順位をご確認ください。



Web フィルタ

Q: Forti Guard カテゴリベースのアクションを設定するにあたり、よく利用している Web サイトが どのカテゴリに該当するのかを確認したい。

A:以下のサイトからカテゴリタイプを確認することができます。

https://www.fortiguard.com/webfilter

例:ntt-east.co.jpのカテゴリタイプを確認する場合

① 検索ボックスから「ntt-east. co.jp」を入力し検索します。





Sites sponsored by or devoted to business firms, business associations, industry groups, or business in general. Information Technology companies are excluded in this category and fall in Information Technology.

Group: General Interest - Business

Click here to see if this category is currently blocked.

Request a Review

Latest Web Filter Databases 232.20251

Protect your organization by blocking access to malicious, hacked, or inappropriate websites with FortiGuard Web Filtering. Web filtering is the first line of defense against web-based attacks. Malicious or hacked websites, a primary vector for initiating attacks, trigger downloads of malware, spyware, or risky content.

FortiGuard URL Database Categories are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families. They also take into account customer requirements for Internet management. The categories are defined to be easily manageable and patterned to industry standards.

図 20-1. Web Filter Lookup 検索画面.

② 検索結果より、「一般的な関心事-ビジネス」の「カテゴリ:ビジネス」と表示されたことを確認します。



Q: Web サイトの閲覧ができなくなった。

A: Web サイトの閲覧ができなくなった原因には vUTM の他に様々な要因が考えられます。

- ① お客さまLAN環境における故障
- ② 光アクセスサービスの故障
- ③ Managed SD-WAN の故障・設定誤り
- ④ Managed SD-WAN セキュアインターネットサービスの故障・過遮断・設定誤り
- ⑤ インターネット接続サービス (ISP) の故障
- ⑥ コンテンツプロバイダ (CP) の故障・メンテナンス

一般に、①から順番に調査を行うことによって原因特定や解決までの時間が最小限となることが知られていますが本マニュアルでは④について回答します。

- i. vUTM カスタマコントロールへ接続ができること
 - vUTM カスタマコントロールへアクセスを行いログインができることを確認します。
 - ※手順については「2.1 vUTM カスタマコントロールへのログインについて」を参照
 - ログイン画面に到達できない場合、①~③が原因の可能性があります。
- ii. サイトがブロックされていることを示す代替メッセージを確認する
 - vUTMによって通信が遮断された場合、以下の代替メッセージが表示されます。



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category ギャンブル

URL https://

To have the rating of this web page re-evaluated please click here.

図 20-2. Web フィルタによってブロックされた代替メッセージ.

- ・ 「Category」や「URL」の表示内容を確認し、Web フィルタで設定を行った内容 と比較します。
- ・ 比較の結果、必要通信と判断した場合は、Forti Guard カテゴリベースのフィル タ設定又は Skip List への登録によりブロックを回避することができます。
- ※ 手順については「6.3 Private List、Src Black List、Skip List、Dst
 Black List の設定方法」「11 セキュリティプロファイル: Web フィルタ」を参照



Q: URL フィルタタイプのシンプル、正規表現、ワイルドカードのタイプ一覧の仕様について詳しく知りたい。

A: Fortinet のコミュニティサイトにて設定方法に関するナレッジが公開されています。 以下のサイトをご確認ください。

 $https://community.\ fortinet.\ com/t5/FortiGate/Technical-Tip-URL-Filter-expressions-for-the-FortiGate/ta-p/192746$

正規表現のテストには以下のサイトにおいても確認することができます。

https://regex101.com/

※テストにはダミーデータを入れるなど、機微情報を入れないでください。



アプリケーションコントロール

Q:カテゴリのアクションを設定するにあたり、よく利用しているアプリケーションがどのカテゴリに該当するのかを確認したい。

A:以下のサイトからカテゴリタイプを確認することができます。

https://www.fortiguard.com/services/appcontrol

例:Windows Update のカテゴリタイプを確認する場合

① 検索ボックスから「Windows Update」を入力し検索します。



FortiGate next gen firewalls with FortiOS and centralized management solutions offer extensive visibility into application usage in real time, as well as trends over time through views, visualizations, and reports. You can use application control to keep malicious, risky, and unwanted applications out of your network through control points at the perimeter, in the data center, and internally between network segments.



図 20-3. Application Control Service 検索画面.

② 検索結果より、アプリケーションシグネチャ「Microsoft. Windows. Update」と表示されたことを確認します。

画面下側にカテゴリ: Update と表示されていることを確認します。

また、アプリケーションシグネチャをクリックすることで詳細を確認することができます。

Search Results

Showing results for Windows Update



Added: Dec 10, 2008 Category: Update