

SuitePRO V4 / IndigoPro UTM オプション FortiGate 設定手順書

株式会社 NTTPC コミュニケーションズ 更新日:2024年11月06日



目次

1. はじめに		4
2. UTM 管理サ	イトへのログイン	4
3. UTM 管理サ	イトの管理	5
3-1	UTM 管理サイト のパスワード変更	5
3-2	UTM 管理サイト 接続元 IP アドレスの追加	5
4. ファイアウォー	・ルポリシー	6
4-1	ファイアウォールポリシー	6
4-3	プリセットされているファイアウォールポリシー	7
5. ファイアウォー	・ルアドレス	8
5-1	ファイアウォールアドレス	8
5-2	ファイアウォールアドレスの変更	8
5-3	ファイアウォールアドレスの登録	9
6. フ ァイアウォー	・ルアドレスグループ	10
6-1	ファイアウォールアドレスグループ	10
6-2	ファイアウォールアドレスグループの変更	10
7. ファイアウォー	・ルポリシーの有効化・無効化	11
7-1	ファイアウォールポリシーの有効化	11
7-2	ファイアウォールポリシーの無効化	12
8. セキュリティ	アンチウイルス	13
アンチ	ウイルスの設定	13
9. セキュリティ	アンチスパム	15
アンチ	スパムの設定	15
10. セキュリティ	IPS	17
IPS 0)設定	17
11.セキュリティ	WAF(Web アプリケーションファイアウォール)	
WAF	の設定	
12. セキュリティ	SSL/SSH インスペクション	20
12-1	SSL/SSH インスペクション設定	20
12-2	ポリシーの設定	21
12-3	SSL inspection 警告について	22
13. ロードバラン	ン サー	23
13-1	へルスチェックモニタの作成	23
13-2	バーチャルサーバの作成	23
13-3	リアルサーバの作成	25
13-4	ファイアウォールポリシーの作成	
13-5	ロードバランサー接続確認	27
14. IPsec (Fo	ortiClient リモート接続)	
14-1	ユーザの作成	
14-2	IPsecの設定	31
14-4	クライアント設定	



15. IPsec(サイト間接続)	37
15-1 IPsecトンネルの作成	37
15-2 作成された IPsec トンネルの確認	39
15-3 (参考)リモート拠点側の設定	40
16. 証明書のインポート	43
証明書のインポート	43
17.コンソール	45
17-1 コンソールからログイン	45
17-2 接続元 IP アドレスの許可設定を追加する場合	46
18. FortiGate 管理-snmp 監視設定	48
18-1 インターフェース設定	48
18-2 snmpd 設定	48
18-3 管理アカウント設定	49
19. FortiGate 管理-CPU・メモリ負荷の詳細確認	51
sys top の確認と プロセスの kill	51
20. FortiGate 管理-システムログの確認	52
システムログの確認	52
21. FortiGate 管理-オートメーション設定	53
スティッチの作成	53
22.設定例	55
22-1 設定例 1 : 国内アドレスのみを許可する	55
22-2 設定例 2 : インターネット系サービスの許可も追加する場合(ISDB の利用)	57
23. Q&A	58
24. 提供 仕様	63
24-1.仮想 UTM OS イメージの違い	63
24-2 イメージ初期設定	64



1. はじめに

本手順書では FortiGate バージョン 7.4の基本的な設定方法について解説します。

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。

2. UTM 管理サイトへのログイン

コントロールパネル SuitePRO V4(https://pro4.arena.ne.jp)または IndigoPro(https://compas.arena.ne.jp) にログインし、「セキュリティ」>「UTM/NIC4」>「基本情報」を開き、UTM 情報内の「UTM 管理サイト」の URLをクリックします。

UTM 管理サイト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。 ※初期状態では、証明書がインポートされていないため、証明書エラーの画面が表示されます。 必要に応じて、お客さまにてドメインとそのドメインの証明書を取得してください。

- +	ŧ.kz		
1-1	/ 占		
パスワ	7ード		

※ログインできない場合

コントロールパネルの UTM 管理サイトへのアクセス許可から、アクセス元の IP アドレスが許可されているか確認してください。 SuitePRO V4(https://pro4.arena.ne.jp) IndigoPro(https://compas.arena.ne.jp)

SuitePRO V4「UTM 管理サイトへのアクセス制限」 https://help.arena.ne.jp/hc/ja/articles/360039329673#chapter2

IndigoPro「UTM 管理サイトへのアクセス制限」

https://help.arena.ne.jp/hc/ja/articles/4408148218775#chapter2

UTM	管理サイト用のドメインを準備する場合、以下の作業を実施
1	ドメイン取得(FortiGate で使用するため、サーバーとは別に準備する)
2	DNS登録
	A レコードで FG 管理サイトの IP アドレスを指定(例 : fvd1111.fg.arena.ne.jp)
3	取得したドメインの証明書購入
4	FortiGate:証明書インポート ※手順「証明書のインポート」参照
(5)	FortiGate:証明書設定
	「システム」>「設定」メニュー
	「管理者設定」>「HTTPSサーバー証明書」にて対象の証明書を選択し、適用





3. UTM 管理サイトの管理

UTM 管理サイト

- 3-1 UTM 管理サイト のパスワード変更
- (1) ログイン後、UTM 管理サイト右上のユーザ名をクリックします。



「パスワードの変更」をクリックします。

✿ システム	
🗅 設定	•
≜ パスワードの	変更
● ログアウト	

(2) 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		×
現在の管理者フ		上再
▲ ログインが必要	夏になります。	
ユーザ名	username	
旧パスワード	現在のパスワード(入力)	۲
新しいパスワード	新しいパスワード(入力)	۲
パスワードの再入力	新しいパスワード(再入力)	۲

3-2 UTM 管理サイト 接続元 IP アドレスの追加

接続元アドレスの追加を行う方法です。管理サイトにログインしたうえでの作業となります。現在のアドレスが追加されていない場合は、アクセスができませんので「18.コンソール」をご確認ください

(1) システム>管理者を選択します。

	¢ >776	.*
	管理者	☆
(2)	対象の管理者をクリックします。	
	+新規作成 → 🥒 編集 💼 削除	検索
	名前♥	
	🖸 システム管理者 2	
	admin	
	🛔 username	

adminとは・・弊社管理のサポート用アカウントになります。削除や変更はお控えいただくようお願い致します。削除・変更されますと、お問い合わせの際こお客様の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。





信頼されるホストにログインを制限の欄に IP アドレスを追加し、「OK をクリックします。 (3)

管理者の編集			
ユーザ名 ዐ	useri	ame	パスワードの変更
タイプ		カルユーザ	
	リモ	ートサーバグループの単一ユー	-ザと一致
	IJŦ	ートサーバグループのすべての	ユーザと一致
	publi	c key infrastructure (PKI) グルー	- プを利用
コメント	З×	ント記入	0/255
信頼される	5ホスト	にログインを制限	
信頼されるホス	スト1	203.0.113.40/32	×
信頼されるホン	スト2	203.0.113.41/32	×
		0	
		v	
		ОК	キャンセル

- 4. ファイアウォールポリシー
- 4-1 ファイアウォールポリシー

ファイアウォールポリシーは、FortiGate ユニットを通過するトラフィックを、FortiGate インタフェース間で制御します。

- ・Incoming(外部から仮想サーバー)の通信
- ・ Outgoing (仮想サーバーから外部)の通信

トラフィックは、ファイアウォールポリシーリストの最上位にあるものから下位の項目へと順番に評価されます。 一致するポリシーが検出されると、そのポリシーで指定された処理が行われ、以降のファイアウォールポリシーは適用されません。 許可ポリシーに一致しなかったトラフィックは拒否されます。(暗黙の拒否)

ファイアウォールポリシーの表示 4-2

「ポリシー&オブジェクト」>「ファイアウォールポリシー」をクリックすると、ファイアウォールポリシーが表示されます。







4-3 プリセットされているファイアウォールポリシー

初期のファイアウォールポリシーは下記のように設定しています。 Incoming(外部から仮想サーバー)の通信 ① NTTPC:ポート監視サーバーの通信を許可(ポート監視サービスを利用するために必要) ② Preset2~7:サンプルとなるプリセットのファイアウォールポリシー (ステータス:無効) preset2:オフィス等からSSH (TCP/22) 接続を許可する際に使用 preset3:オフィス等からリモートデスクトップ (TCP/3389) 接続を許可する際に使用 preset4:DNS(TCP,UDP/53)サーバーを構築した際に使用 preset5:HTTP(TCP/80)サーバーを構築した際に使用 preset6:HTTPS(TCP/443)サーバーを構築した際に使用 preset7:メールサーバー(※)を構築した際に使用 %POP3 (TCP/110), SMTP (TCP/25), SMTP_SUBMISSION (TCP/587), IMAP (TCP/143)

Outgoing(仮想サーバーから外部)の通信

③ preset1:仮想サーバーから外部への通信はすべて許可

Incoming (外部から仮想サーバー)

ernet - SuiteP	RO_NW					
NTTPC	NTTPC_Port_Monitoring	SuitePite SuitePite	o always	ALL ALL	✓ ACCEPT	◎ 無効
preset2	I Office_Group	SuitePRO_NW	Lo always	EN SSH	✓ ACCEPT	🖸 無効
preset3	To Office_Group	SuitePRO_NW	lo always	RDP	✓ ACCEPT	😋 無効
preset4		1++++ (7=-/	カブ・4冊なけ	🔛 DNS	✓ ACCEPT	◎ 無効
preset5			7	😡 НТТР	✓ ACCEPT	◎ 無効
preset6	🔲 all	Web_Server_Group	o always	I HTTPS	✓ ACCEPT	〇 無効
preset7		Mall_Server_Group	To always		* ACCEPT	
aoin		י ע רייא (אַצ	10 mm/s	Ha contra	Contraction of the	Y may
		11-7		-		
preset1	Sute2RO_NW	1 m	Co steeps	ALL.	✓ ACCEPT	0.8.2
	NTTPC preset2 preset3 preset4 preset5 preset6 preset7 CGOIN	NTTPC INTIPC_Port_Monitoring preset2 III Office_Group preset3 III Office_Group preset4 IIII 2つつり preset5 IIIII preset6 IIIII preset6 IIII preset6 IIIII preset6 IIII preset6 IIIII preset6 IIIII preset6 IIIII preset6 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	NTTPC INTTPC Port_Monitoring SuitePRO_MW preset2 III Office_Group SuitePRO_MW preset3 III Office_Group SuitePRO_MW preset4 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	NTTPC INTTPC. Port_Monitoring SuitePRO_NW G always preset2 Goffice_Group SuitePRO_NW G always preset3 G Office_Group SuitePRO_NW G always preset4 all OCULUE SuitePRO_NW G always preset5 all COULDENT CAPPOAC : 無効 preset6 all G OULDENT Group G always preset6 all G OULDENT Group G always COULDENT G OULDENT Group G always COULDENT G OULDENT G OULDENT G OULDENT G OULDENT COULDENT G OULDENT COULDE	NTTPC INTTPC. Port_Monitoring SuitePRO_NW Galways ALL preset2 Group SuitePRO_NW Galways GROP preset4 日 10 つりしてシート (ステータス::無効) ONS preset5 日 11 のけして、Group Galways HTTPS preset6 日 11 のけして、Group Galways HTTPS preset6 日 11 ののらり合わい CODID CODID	NTTPC INTTPC_Port_Monitoring SuitePRO_NW G always ALL ✓ ACCEPT preset2 Goffice_Group SuitePRO_NW G always BRDP ✓ ACCEPT preset4 日間 ②プリセント、「ステータズ:無効」 ONS ✓ ACCEPT preset5 日間 『ひりしたい」、Web_Server_Group G always 日 HTTPS ✓ ACCEPT preset6 日間 『Web_Server_Group G always 日 HTTPS ✓ ACCEPT





5. ファイアウォールアドレス

5-1 ファイアウォールアドレス ファイアウォールポリシーに使用するアドレスです。 初期で登録されているファイアウォールアドレスの一部を紹介します。

> NTTPC_Port_Monitoring:NTTPCポート監視サーバーで使用しているため変更しないでください。 OfficeA:仮想サーバーにアクセスする拠点のアドレスを登録(※) OfficeB:仮想サーバーにアクセスする上記とは別の拠点があれば登録(※)

※初期で指定している IP アドレスは、RFC で定義されている例示用の IP アドレス(192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24) 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。

5-2 ファイアウォールアドレスの変更

ここでは例として、プリセットされているファイアウォールポリシーを使用し、オフィス等、仮想サーバーにアクセスする拠点からのみ SSH (TCP/22) 接続を許可します。

本設定の他に、仮想サーバー側での設定も必要となります。詳細はこちらをご確認ください。

- SuitePROV4 • https://help.arena.ne.jp/hc/ja/articles/360039329633 IndigoPro https://help.arena.ne.jp/hc/ja/articles/4408133780375
- ファイアウォールアドレス設定画面表示 (1)「ポリシー&オブジェクト」>「アドレス をクリックします

📕 ポリシー&オブジェクト	•
ファイアウォールポリシー	
Local Inポリシー	
DoSポリシー	
アドレス	☆





(2) プリセットのアドレス変更

プリセットのアドレス「Office_A」を右クリックし「編集」を選択し、名前とアドレスを変更します。

(例) 名前:「Office_A」から「Office_Tokyo」と変更 ※お客さまのオフィス拠点名等分かりやすい名前を指定してください。 アドレス: 203.0.113.40/29と変更

		新規アドレス	
名前	タイプ	名前 カラー インターフェース タイプ	Office_Tokyo 回 変更 □ any ・ サブネット ・
4 Office_B	 ▼ 名前 ぐフィルタ ・ ✔ 編集 	IP/ネットマスク スタティックルート設定 O コメント	203.0.116.40/29
		ОК	→ → → → → → → → → → → → → → → → → → →

内容を確認し、「OK」をクリックします。

5-3 ファイアウォールアドレスの登録

IP アドレスを新しく登録する場合は「アドレス」を新規作成します。「新規作成」をクリックし、「アドレス」を選択します。

≣ Q			
Address	Address Gr	oup	
+ 新規作成	∥ 編集	ク ローン	創除
	名前		

アドレス: 203.0.113.41/32と入力

(例)

名前:「Office_Osaka」と入力 ※お客さまのオフィス拠点名等分かりやすい名前を指定してください。

名前	Office_Osaka
カラー	■ 変更
インターフェース	🗆 any 💌
タイプ	サブネット 🗸
IP/ネットマスク	203.0.113.41/32
スタティックルート	設定 🖸
コメント	コメント記入

内容を確認し、「OK」をクリックします。



6. ファイアウォールアドレスグループ

6-1 ファイアウォールアドレスグループ

ファイアウォールポリシーに使用するアドレスグループです。ファイアウォールアドレスをグループでまとめることができます。 初期で登録しているファイアウォールアドレスグループを使用して変更してみます。

例 Office Group: Office A, Office B

- ファイアウォールアドレスグループの変更 6-2 登録した「アドレス」を「ファイアウォールアドレスグループ」でグループ化します。 ここでは例として、プリセットのアドレスグループ「Office_Group」の編集を行います。
- (1) アドレスグループ編集

「ポリシー&オブジェクト」>「アドレス」の上部メニューの「Address Group」を選択します。

≡ ۹			
Address	Address Gr	roup	
+ 新規作成	/ 福集	<i>∎ 2</i> □->	俞 削除

「Office Group」を右クリックし、「編集」をクリックします。

名前	タイプ	メンバー
🖥 G Suite	グループ	Image: gmail.com ▼ タイプ でフィルタ ・
🖷 Microsoft Office 365	グループ	 ✓ 編集 ■ クローン
The Office_Group	グループ	 前除 >_ CLIで編集

アドレスグループから除外 (2)

「メンバ」をクリックすると画面右側にアドレス一覧が表示されます。

「Office_A」のみ使用する場合は、メンバの「Office_B」の右横の×をクリックして削除します。

「OK」をクリックします。	
---------------	--

カテゴリ	IPv4グループ	エントリを選択	×
久前	Office Group	検索	+
タイプ 🕕	グループ フォルダ	アドレス・	
カラー	撮 変更する ▼	ー アドレス 図 NTTPC Part Monitoring	
メンバー	Office_A	SuitePRO_NW	
	Office_B	X Office_A	
	· · ·	Office_B	
メンバーの除外	•	Japan_Segment	
スタティックルート設定 0 0		Dipsec_range	
1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -		= 7K1.7H17	
コメント	コメント記入	クローズ	





(3) アドレスグループに追加

新たなアドレスをグループに追加する場合は、「+」をクリックし、右側のエントリから対象アドレスを選択します。 色が反転し、メンバにが加つったことを確認し、OKをクリックします。

カテゴリ		IPv4グループ	エントリを選択	×
名前		Office Group	検索	Q +
タイプ 0		グループ フォルダ	アドレス・	
カラー		看 変更する ▼	ー アドレス	5
メンバー		Office_A	X SuitePRO_NW	
		Office_B +	X Office_A	
メンバーの除外	0		Japan_Segment	
スタティックルート設定 🚯	0		ipsec_range	
コメント		コメント記入	- マドレフガルーブ クロ-	- <i>X</i>

7. ファイアウォールポリシーの有効化・無効化

7-1 ファイアウォールポリシーの有効化

ファイアウォールポリシーを使用するには、ポリシーを有効化する必要があります。 ここでは例として、preset2:オフィス等からSSH(TCP/22)接続を許可するポリシーを有効化し、サーバーへのSSH通信を 許可します。

(1) IPv4 ポリシーの選択

「ポリシー&オブジェクト」>「ファイアウォールポリシー」をクリックします。



(2) プリセットのポリシーの確認

プリセットされている「preset 2」を確認します。

送信元:「Office_Group」(お客さまのオフィス) 送信先:「SuitePRO_NW」(お客さまの/反想サーバーが属しているネットワークアドレス) サービス:「SSH」

アクション:「ACCEPT」

ID	▼名前	▼ 送信元	▼ 宛先	▼ スケジュール	▼ サービス	▼ アクション	T NAT
	nternet (por	rt8) - SuitePRO_NW1812 (port1)	(1 - 7)				
1	NTTPC	NTTPC_Port_Monitoring	SuitePRO_NW	Co always	🔽 ALL	✓ ACCEPT	🖸 無効
23	preset2	Te Office_Group	SuitePRO_NW	lo always	<u> I</u> SSH	✓ ACCEPT	🖸 無効
30	preset3	Te Office_Group	SuitePRO_NW	Co always	😨 RDP	ACCEPT	🕲 無効



(3) ステータスポリシーの変更

対象の ID[2]を選択し、「有効」をクリックします。

ポリシー		ID	名前	
🗄 Internet (port2	:) → 📓 S	uitePR	O_NW (port1) 7	
NTTPC (2)		2	NTTPC	
Opreset2 (3)		3	preset2	
	🥒 編集	日掲	■入 • 🔷 有効	前前
🕴 preset3 (4)		4.	preset3	
😳 preset4 (5)		5	preset4	
O▲ preset5 (6)		6	preset5	

(4) 有効化の確認

ID 横の×が消え、ポリシーが有効化されたことを確認してください。

NTTPC (2)	2	NTTPC	MTTPC_Port_Monitoring
preset2 (3)	3	preset2	P Office_Group
😢 preset3 (4)	4	preset3	Page Office_Group

7-2 ファイアウォールポリシーの無効化

有効化したポリシーを無効化する場合はステータスを無効に変更します。 ここでは例として、preset2:オフィス等からSSH(TCP/22)接続を許可するポリシーを無効化し、サーバーへのSSH通信 許可を取り消します。

(1) ポリシーの無効化

対象のIDを右クリックし、「ステータス」>「無効」をクリックします。



(2) 無効化の確認

ID 横に×が追加され、無効化されたことを確認してください。

NTTPC (2)	2	NTTPC	4 NTTPC_Port_Monitoring
🙁 preset2 (3)	3	preset2	Group



8. セキュリティ アンチウイルス

アンチウイルスの設定

アンチウイルスとは、サーバーの通信を監視し、不正なウイルスを検知し感染を未然に防ぐシステムです。アンチウイルスは初期状態では OFF になっています。ここでは preset7(MAIL 通信を許可するポリシー)に作成済みアンチウイルスプロファイルの設定を行います。

(1) IPv4 ポリシーの選択

「ポリシー&オブジェクト」>「IPv4 ポリシー」をクリックします。



(2) ポリシーの編集

プリセットされている「preset 7」を選択し、「編集」をクリックします。

8	preset7 🖪 all	Mail_Server_Group	Co always	MAIL	✓ ACCEPT	◎ 無効	+
---	---------------	-------------------	-----------	------	----------	------	---

(3) アンチウイルスの有効化

下記のように設定し、最後に「OK」をクリックします。

アンチウイルス:「ON」に変更し、プルダウンから「AV_MAIL」を選択

SSL インスペクション:任意のプロファイルを指定します。例では「certificate-inspection」を指定しています。

このポリシーを有効:有効になっていない場合は「ON」

セキュリティプロファイル		
アンチウイルス		
ビデオフィルタ		0
IPS		0
ファイルフィルタ		0
Eメールフィルタ		0
Webアプリケーションファイアウ	オール	•
SSLインスペクション		55L certificate-inspection
ロギングオプション		
許可トラフィックをログ	0	セキュリティイベント すべてのセッション
セッション開始時にログを生成	0	
パケットのみをキャプチャ	0	
		0/1023
このポリシーを有効化 🔹 🜑		
		OK キャンセル

(※SSL インスペクションの警告については 12-3「SSL インスペクション警告について」を参照ください。)



(4) preset7のセキュリティプロファイルに「AV」が追加されました。

preset7	all	🖥 Mail Server Group	o always	✓ ACCEPT	3 無効化済み	PRX default	AV AV MAIL	
							SSL certificate-inspec	ction

サービス「MAIL」で許可されるサービスは「SMTP」、「Submission」、「POP3」、「IMAP」です。

※ ウイルスが検知された場合の動作

■ POP3 / IMAP

受信したメールにウイルスが発見された場合は、ウイルスを含む添付ファイルのみが削除され、添付ファイルは 次のメッセージに置き換えられます。送信元へウイルス検知の通知は行われません。

>シャセージ

Dangerous Attachment has been Removed. The file "<ファイル名>" has been removed because of a virus. It was infected with the "ウイルス名" virus. File guarantined as: ""."ウイルス 情報 URL"

■ SMTP / SMTP SUBMISSION

メール送信時にウイルスメールが発見された場合は、メールは送信されません。 送信元には、次のメッセージを含むエラーメッセージの表示またはエラーメールが配送されます。

送信メールのログ

Dangerous Attachment has been Removed. The file "<ファイル名>" has been removed because of a virus. It was infected with the "ウイルス名" virus. File guarantined as: ""."ウイルス情 報 URL"

※ ポリシーに「アンチウイルス」と「アンチスパム」両方を設定し、「アンチスパム」の設定で SMTP のアクションに「タグ」を指定し ている場合

メール送信時にウイルスを検知した場合、ウイルスを含む添付ファイルのみが取り除かれ、メールが送信されます。 取り除かれた添付ファイルは次のメッセージに置き換えられます。

>シャセージ

Dangerous Attachment has been Removed. The file "<ファイル名>" has been removed because of a virus. It was infected with the "ウイルス名" virus. File quarantined as: ""."ウイルス 情報 URL"



9. セキュリティ アンチスパム

アンチスパムの設定

アンチスパムとは、サーバーの通信を監視し、迷惑メールを検知するシステムです。アンチスパムは初期状態では OFF になっていま す。ここでは preset7 (MAIL 通信を許可するポリシー) にアンチスパムの設定を行います。

(1) IPv4 ポリシーの選択

「ポリシー&オブジェクト」>「IPv4 ポリシー」をクリックします。

💄 ポリシー&オブジェクト	*
ファイアウォールポリシー	슙
DoSポリシー	

(2) ポリシーの編集

プリセットされている「preset 7」を選択し、「編集」をクリックします。

	preset7 (8)	8	4 all	4 SuitePRO_NW		✔ 許可	o always
--	-------------	---	-------	---------------	--	------	----------

アンチスパムの有効化 (3)

下記のように設定し、最後に「OK」をクリックします。

アンチスパム:「ON」に変更し、プルダウンから任意のプロファイルを選択。例では「ANTISPAM」を選択 SSL インスペクション:任意のプロファイルを指定します。例では「certificate-inspection」を指定しています。

このポリシーを有効:有効になっていない場合は「ON」

セキュリティブロファイル		
アンチウイルス	0	
ビデオフィルタ	0	
IPS	0	
ファイルフィルタ	0	
Eメールフィルタ	•	email ANTISPAM -
Webアプリケーションファイアウ	ォール 🗿	
SSLインスペクション		ssi certificate-inspection
ロギングオプション		
許可トラフィックをログ	• tz‡	ニリティイベント すべてのセッション
セッション開始時にログを生成	0	
パケットのみをキャプチャ	•	
ーイメント		
		0/1023
このポリシーを有効化 💽		
		OK キャンセル





(4) preset7のセキュリティプロファイルに「EMAIL(アンチスパム)」が追加されました。

preset7(8)	8	4 all	4 SuitePRO_NW	🔓 MAIL	✔ 許可	🙁 無効化済み	EMAIL ANTISPAM
							ss. certificate-inspection

※ 迷惑メールが検知された場合の動作

■ POP3 / IMAP*

受信したメールに迷惑メールが発見された場合は、該当メールの件名に[SPAM] と追記されます。

※IMAPはご利用のメールソフトによって挙動が異なることがあります

メールヘッダ

X-SpamInfo: FortiGuard - AntiSpam ase, X-ASE-REPORT: (略)

■ SMTP / SMTP_SUBMISSION

メール送信時に迷惑メールと判定された場合は、メールは送信されません。 送信元には、次のメッセージを含むエラーメッセージの表示またはエラーメールが配送されます。

送信メールのログ

554 5.7.1 This message has been blocked because ASE reports it as spam. (in reply to end of DATA command))

メール送信時に迷惑メールと判断された場合は、該当メールの件名に[SPAM] と追記されます。

メールヘッダ

X-SpamInfo: FortiGuard - AntiSpam ase, X-ASE-REPORT: (略)



10. セキュリティ IPS

IPSの設定

IPS(侵入防止システム)とは、サーバーの通信を監視し、不正なアクセスを検知して攻撃を未然に防ぐシステムです。IPS は初期状態では OFF になっています。ここでは preset5(HTTP 通信を許可するポリシー)に IPS の設定を行います。

IPv4 ポリシーの選択

「ポリシー&オブジェクト」>「IPv4 ポリシー」をクリックします。



(2) ポリシーの編集

プリセットされている「preset 7」を選択し、「編集」をクリックします。

preset7 (8)	8	4 all	4 SuitePRO_NW	✔ 許可	always

(3) IPS の選択

下記のように設定し、最後に「OK」をクリックします。

IPS:「ON」に変更し、プルダウンから「IPS_HTTP」を選択

SSL インスペクション:任意のプロファイルを指定します。例では「certificate-inspection」を指定しています。 このポリシーを有効:有効になっていない場合は「ON」

セキュリティブロファイル	
アンチウイルス	0
ビデオフィルタ	0
IPS	
ファイルフィルタ	0
Eメールフィルタ	0
Webアプリケーションファイアウ:	
SSLインスペクション	ssL certificate-inspection 🗸
ロギングオプション	
許可トラフィックをログ	• セキュリティイベント すべてのセッション
セッション開始時にログを生成	
パケットのみをキャプチャ	•
	0/1023
このポリシーを有効化 🔹 🔘	
	ОК =+>>tл

Preset7のセキュリティプロファイルに「IPS」が追加されました。

※HTTPS などの SSL 通信を監視する場合は別途「証明書インポート」、「SSL/SSH インスペクション」の設定が必要です。





11.セキュリティ WAF (Web アプリケーションファイアウォール)

WAF の設定

WAFとは、サーバーの通信を監視し、Webアプリケーションの脆弱性を悪用した攻撃を検知するシステムです。WAFは初期状 態では OFF になっています。ここでは preset5(HTTP 通信を許可するポリシー)に WAF の設定を行います。

(1) IPv4 ポリシーの選択

「ポリシー&オブジェクト」>「ファイアウォールポリシー」をクリックします。



(2) ポリシーの編集

プリセットされている「preset 6」を選択し、「編集」をクリックします。

Opreset6(7) 7 4 all	4 SuitePRO_NW	HTTPS	✔ 許可	lo always
---------------------	---------------	-------	------	-----------

(3) インスペクションモード:「プロキシ」を選択



Web アプリケーションファイアウォール:「ON」に変更

SSL インスペクション:任意のプロファイルを指定します。例では作成した SSL インスペクションプロファイルを指定しています。 このポリシーを有効:有効になっていない場合は「ON」

セキュリティプロファイル	
アンチウイルス	0
ビデオフィルタ	0
IPS	0
ファイルフィルタ	•
Eメールフィルタ	0
Webアプリケーションファイアウォール	♥ WAF default
SSLインスペクション 🛆	sst example
復号トラフィックミラー	0
ロギングオプション	
許可トラフィックをログ 🔹 🔘	セキュリティイベント すべてのセッション
セッション開始時にログを生成 🛛 🕥	
パケットのみをキャプチャ 🔹 🔿	
	0/1023
このポリシーを有効化 🔹 🔘	
	ОК ====================================





(4) preset5のセキュリティプロファイルに「WAF」が追加されました。

preset6 (7)	7	4 all	4 SuitePRO_NW	HTTPS	✔ 許可	lo always	WAF default
							ss. example

※HTTPS などの SSL 通信を監視する場合は別途「証明書インポート」、「SSL/SSH インスペクション」の設定が必要です。

※ Web アプリケーションの脆弱性を悪用した攻撃が検知された場合の動作

ブラウザに以下のメッセージが表示され、アクセスがブロックされます。

Web Application Firewall This transfer is blocked by a Web Application Firewall. This transfer is blocked.



12. セキュリティ SSL/SSH インスペクション

SSL/SSH インスペクション

暗号化された通信において UTM 機能を利用するための設定です。SSL/SSH インスペクションは初期状態では検査しない「noinspection」が指定されています。ここでは preset6(HTTPS 通信を許可するポリシー)に SSL/SSH インスペクションの設定 を行います。事前に「16.証明書のインポート」を実施ください。

- 12-1 SSL/SSH インスペクション設定
- (1)SSL/SSH インスペクションの新規作成

「セキュリティプロファイル」>「SSL/SSH インスペクション」をクリックします。



SSL/SSH インスペクションプロファイルの作成 (2) 画面上の「新規作成」をクリックし、新しいプロファイルを作成します。

> ✔ 編集 「 クローン 」 自 削除 +新規作成

下記のように設定し、最後に「OK」をクリックします。

名前:任意の名前を入力

SSL インスペクションの有効: SSL サーバー保護

サーバー証明書:「16.証明書のインポート」でインポートした証明書を選択

SSL/SSH-1	ンスペクションプロファイルの編集
名前	example
コメント	コメント記入 // 0/255
SSLインス	ペクションオプション
いずれかめ	XSSLインスペクションを有効化 複数のサールに接続する複数のクライアント SSLサーバ保護
サーバ証明	re fullchain × よ ダウンロード +
プロトコル	ルポートマッピング
すべてのオ	ペートを検査する 🕥
HTTPS	443
HTTP/3	Inspect バイパス ブロック
DNS over (QUIC Inspect バイバス ブロック
SSLインス	ペクションから除外
アドレス	+
SSL除外の	ログを記録する 🕥
	OK キャンセル





12-2 ポリシーの設定

(1) IPv4 ポリシーの選択

「ポリシー&オブジェクト」>「ファイアウォールポリシー」をクリックします。

💄 ポリシー&オブジェクト ~

ファイアウォールポリシー

(2) ポリシーの編集

プリセットされている「preset 6」を選択し、「編集」をクリックします。

preset6 (7) 7 preset6 4 all SuitePRO_NW	🚺 always 🖬 HTTPS
---	------------------

(3) SSL インスペクションの有効化

下記のように設定し、最後に「OK」をクリックします。

SSL インスペクション: プルダウンから「先ほど作成したプロファイル」を選択

このポリシーを有効:有効になっていない場合は「ON」

SSLインスペクション 🗛		ss. example 🗸
復号トラフィックミラー		0
ロギングオプション		
許可トラフィックをログ	C	セキュリティイベント すべてのセッション
セッション開始時にログを生成	•	
パケットのみをキャプチャ	•	
4<%		
		0/1023
このポリシーを有効化 🛛 🜑		
	ſ	

・SSL inspection フルインスペクションの注意アイコンについて

以下は FortiGate に設定した証明書はユーザのブラウザにインストールが必要という注意です。

証明書がパブリックな証明書発行期間から入手した CA 証明書をご利用であれば、問題ありません。自己証明書などをご利用 の場合はエンドユーザーのブラウザに証明書のインストールが必要です。

このSSLノロノアイル 書をインストールした	はフルSSLインスへクションを使用 Wいとエンドユーザに証明書の警告;	しています。フラワリに証明 が表示されます。
SSLインスペクション 🛕	example	•
		_
確認		
This SSL profile uses full SSL inspection. En warnings unless the certificate is installed	id users will likely see certificate in their browser.	
OK ≠	センセル	



12-3 SSL inspection 警告について

SSL インスペクションは初期状態で「no-inspection(※SSLを監査しない)」セキュリティプロファイルが指定されています。 セキュリティプロファイルを設定して「no-inspection」が選択されている場合以下の警告が表示されます。

証明書をご利用の場合は、「16.証明書のインポート」、「12.SSL/SSH インスペクション」の設定を行うか その他プリセットされている「certificate-inspection」等のプロファイルを選択してください。 手順例では「certificate-inspection」を選択し、SNIのチェックを行っています。 SSLを使用しない場合は、このまま OK を押して問題ありません。

	確	10月 日本
4	The no-inspection profile doesn't pe selected with other UTM profiles or	erform SSL inspection, so it shouldn't be r features that require SSL inspection.
	ОК	キャンセル

「no-inspection」を選択した場合、次のようにファイアウォール一覧で注意アイコンが表示されます

A preset7 (8)	8	4 all	
---------------	---	-------	--

ポリシーID 8

ポリシー名 preset7

このポリシーには次の問題があります。

 no-inspectionのプロファイルはSSLインスペクションを実行しないため、SSLイ ンスペクションを必要とする他のUTMプロファイルや機能とは一緒に選択で きません。

このエラーメッセージに関する詳細は次をご参照ください

https://community.fortinet.com/t5/Customer-Service/Technical-Tip-How-to-resolve-the-warning-message-The-no/ta-p/244152





13. ロードバランサー

ロードバランサーの設定

FortiGate は L4 レベルで負荷分散を行うことができます。ここでは HTTP サーバー2 台をラウンドロビン方式で負荷分散する設定を行います。ロードバランサーではバーチャル IP の設定が必要です。



13-1 ヘルスチェックモニタの作成

「ポリシー&オブジェクト」>「ヘルスチェック」をクリックします。「新規作成」をクリックし、「ヘルスチェックモニタ」を編集します。





ヘルスチェックモニタの設定を行います。

名前	ヘルスチェック名を指定(例は、「HTTPS」と指定)
タイプ	タイプを指定(例は、「HTTPS」を指定)
間隔	チェック間隔を指定
タイムアウト	タイムアウトこなるまでの時間を指定
再試行	再試行の回数を指定

ヘルスチェック	7モニタ	の編集				
名前	HTTP	S				
タイプ	Ping	TCP	HTTP	HTTPS	DNS	
間隔	10					秒
タイムアウト	2					秒
再試行	3					武行

内容を確認し、「OK」をクリックします。

13-2 バーチャルサーバの作成

「ポリシー&オブジェクト」>「バーチャルサーバ」をクリックします。「新規作成」をクリックし、「バーチャルサーバ」を編集します。





ポリシー&オブジェクト ファイアウォールポリシー	*
バーチャルサーバ ヘルスチェック	
+新規作成	

バーチャルサーバの設定を行います。

名前	バーチャルサーバ名を指定(例は、「WebServer_VIP」)
タイプ	タイプを指定(例は、「HTTPS」)
バーチャルサーバ IP	NIC4のNW帯からサーバーで使用していないものを指定
	※コントロールパネルにログインし、「セキュリティ」>「UTM/NIC4」>「基本情報」のゲートウェイを確認します。
	(SuitePRO V4 <u>https://pro4.arena.ne.jp</u> または IndigoPro <u>https://compas.arena.ne.jp/</u>)
	仮こゲートウェイが 203.0.113.1 の場合、203.0.113.2 から 203.0.113.6 の 5 個の範囲でアドレスを選択で
	きます。 例えば、 サーバーで 203.0.113.2と203.0.113.3を使用している場合、 バーチャルサーバ IP に最後の
	203.0.113.6を指定します。
バーチャルサーバポート	ポート番号を指定(例は、「443」)
ロードバランス方法	ロードバランスの方法を選択(例は、「ラウンドロビン」)
ヘルスチェック	ヘルスチェック方法を選択。ヘルスチェック選択可の中から選択し、⊜をクリックして右側に移動さ
	せる。(例は、「HTTPS」を指定)
クライアント IP の保持	必要に応じて ON/OFF してください。
	「クライアント IP の保持」を ON にすると、クライアント IP アドレスは X-Forwarded-For ヘッダ
	ーに記録されます。(X-Forwarded-Forのロギングは別途 Web サーバーなどの設定が必要
	です。)
モード	SSLオフロードの範囲を選択します。例では「フル」を選択します。
証明書	Webサーバーの証明書を指定します「証明書のインポート」でアップロードします





新規バーチャルサーバ			
タイプ IPv4 名前 WebServer_V コメント コメント記入 カラー 및 変更	IP ∅0/255		
ネットワーク			
タイプ インターフェース バーチャルサーバIP バーチャルサーバポート ロードパランス方式 パーシステンス ヘルスチェック HTTP多重化 ① ① クライアントIPの保持 ①	HTTPS ▼ □ any ▼ 203.0.113.6 443 スタティック ▼ None HTTP クッキー SSLセッション @ HTTPS ★	(例) N] D	C4 の NW 帯からサーバーで使用していないものを拮
SSLオフロード モード クライアント <-	>FortiGate フル		
証明書 🔽 fullchain	-		

13-3 リアルサーバの作成

そのまま画面の下へ移動し、リアルサーバーの「新規作成」をクリックします。

リアルサーバ			
+ 新規作成	✔ 編集	 削除	
IPアドレスポー	トウェイ	最大接続数	モード
マッチするエン	トリーはあ	ぅりません。	

リアルサーバの設定を行います。

IP アドレス	サーバーの IP アドレスを指定(例は、203.0.113.2と203.0.113.3)
ポート	ポート番号を指定(例は、「80」を指定 HTTPS の場合は「443」を指定)
モード	対象サーバーの状態を指定(例は、「アクティブ」を指定)

タイプ	IP ダイナミックアドレス
Pv4アドレス	203.0.113.2 (例)
ペート	443 (例)
最大接続数	0
E− *	アクティブ スタンバイ 無効

内容を確認し、「OK」をクリックします。

同様に、もう1台リアルサーバを作成します。(例:203.0.113.3)





追加したリアルサーバを確認して「OK」をクリックします

◆新規作成	● 編集	向 削除	
アドレス	ポート	最大接続数	₹-ĸ
03.0.113.2	443	0	アクティブ
03.0.113.3	443	0	アクティブ
			0

13-4 ファイアウォールポリシーの作成

「ポリシー&オブジェクト」>「IPv4 ポリシー」をクリックし、「preset6」を選択した状態で右クリックし、「コピー」をクリックします。

(HTTPS の場合は「preset6」)					
	7	ポリシー	送信元	宛先	スケジュール
ポリシー&オブジェクト v	🖬 🕅 Int	ternet (port2)	\rightarrow \blacksquare SuitePRO NW (port1) (8)		
ファイアウォールポリシー 🕁		TPC (2)	4 NTTPC_Port_Monitoring	4 SuitePRO_NW	To always
DoSポリシー	_ pre	set2 (3)	Japan_Segment	SuitePRO_NW	lo always
アドレス		preset3 (4)	Group	A SuitePRO_NW	lo always
インターネットサービスデ ータベース		preset4 (5)	4 all	SuitePRO_NW	lo always
サービス	0	preset5 (6)	4 all	4 SuitePRO_NW	💽 always
スケジュール	v 😮	preset6 (7)	4 all	4 SuitePRO_NW	Co always
バーチャルP		ø	編集 🛛 挿入 🗸 🖉 有効 🗌 🕻] 削除 🛛 🗸 さらに	
IPプール	0	preset7 (8)	4 all	⊿ Su C ⊐ピー	

次に「ペースト」を選択し、「上へ」をクリックします。「preset6」の上に新しいポリシーが作成されます。

 ▼ さらに 	
0 ⊐Ľ−	551
	▲上へ
🗋 逆方向ポリシーを作成	▼ 下へ
🐻 一致するログを表示	
🔺 FortiViewで表示する	
>_ CLIで編集	

新しいポリシーを選択した状態で「編集」をクリックします。

<mark>8</mark> 9	9	4 all			4 SuiteP	RO_NW	🚺 always	
			▲ 編集	司挿入▼	⊘ 有効	向 削除	▼ さらに	



ファイアウォールポリシーを編集します。

名前	ポリシーの名前を入力(例は、LB-HTTPS)
送信元	送信元を指定します。(例は、all)
宛先アドレス	送信先を指定します。(例は、WebServer_VIP)
サービス	対象のサービスを選択(例は、HTTP)リアルサーバに設定したプロトコルに合わせて設定し
	ます。



13-5 ロードバランサー接続確認

先ほど、手順「バーチャルサーバの作成」で作成したバーチャル IP に接続できることをブラウザで確認する。 例の場合 https://203.0.113.6

※バーチャルサーバの VIP(もしくはドメイン名)に対してアクセスします。

<ヘルスチェックの状態を確認する>

ヘルスチェックを確認する場合はダッシュボード>ステータスで「ウイジェット追加」します



[「]ロードバランス」を選択します





	■ ネットワーク	
DHCP DHCPクライアントをモニタします。	DNS 現在接続しているDNSサーバのレイテンシをモニタ します。	IPsec IPsec VPN扱続をモニタします。
IPプール使用率 IPプール使用率のモニタ.	インターフェース帯域幅 選択した新聞枠での選択したインターフェースのリ アルタイムの寿信および発信トラフィック帯環境。	ルーティング 現在のルーティングテーブルをモニタします。
ロードバランス 負荷分散の状態をモニタします。	割り当てられたIPによる上位IPプール 別り当てられたIPによって無約された上位IPプール。	

ダッシュボードに「ロードバランス」が追加されます。ダブルクリックで展開します



リアルサーバのヘルスチェック状況が確認できます

ステータスが「アップ」になっていることを確認してください。(モードが無効の場合、ステータスは常に「ダウン」になります)







14. IPsec(FortiClient リモート接続)

IPSecVPNの設定

FortiClient をインストールしたパソコンから、FortiGate へ IPsec 接続することができます。

- 14-1 ユーザの作成
- (1) ユーザグループを作成します。
 - 「ユーザ&認証」>「ユーザグループ」をクリックします。「新規作成」をクリックし、「ユーザグループ」を作成します。



ユーザグループ名を入力します。(例: IPsec_group)

タイプは「ファイアウォール」を選択し、「OK」をクリックします。

新規ユーサ	fグループ				
名前	IPsec_group				
タイプ	ファイアウォール		٦ - ١		
	Fortinetシングルサイン	ンオン(FSSO)			
	RADIUSシングルサイン	ンオン(RSSO)			
	ゲスト				
メンバー	+				
62.5 (50354) 845 -					
	ОК	キャンセル			
次にユーザ	定義を作成します。「ユ	ーザ&デバイス_	>「ユーザ定義	劇を選択し、「新規	北市成」をクリック
	/ユホート >	+新規作成	● 編集 「	クローン 官削	除検索
🕂 ネット	・ワーク >	名前:	タイプキ	二要素認証 🕈	グループ
島 ポリシ	/−&オブジェクト ゝ				
	.IJ , , [/] ,				
	>				
נ–ב ≗	· ▲認証 →				
ש-ב	定義 ☆				
ユーサ	「グループ				
ゲスト	管理				
I DAP	サーバ				



0



(3) ユーザタイプで「ローカルユーザ」を選択し、「次へ」をクリックします。

ユーザ/グループ作成ウィザ-	- ^K
1 ユーザタイプ 🔪 🛛 🗅	ヴインクレデンシャル 🄰 3 コンタクト情報 🎽 🛿 エキストラ情報 🏷
ローカルユーザ	
リモートRADIUSユーザ	
リモートTACACS+ユーザ	
リモートLDAPユーザ	
FSSO	
FortiNACユーザ	

(4) ログイン クレデンシャルの設定: 認証用のユーザ名(例: ipsec_user)、パスワードを入力して「次へ」をクリックします。

S = - (15)	☆ ブ ▶ 2 ログインクレデンシャル ▶ 3 コンタクト情報 ▶ 4 エキストラ情報
ユーザ名	ipsec_user
パスワード	

(5) コンタクト情報の設定:必要に応じて二要素認証を有効にし、「次へ」をクリックします。

🗸 ユージタイプ 📐	🔮 ログインクレデン	5en 🔪 3 🗆	ッタクト情報 🔰 🕢 エキストラ情報
) 二要素認証			
	. = 2	*^	++>.+71

(6) エキストラ情報:「ユーザグループ」をONに設定し、ユーザグループに先ほど作成したグループを指定して「作成」をクリックします。

🜒 ユーザタイプ 🔰 🕲 ログ	インクレデンシャル 🔰 🗸 コンタクト 💷 🎽 🕘 エキストラ情報
ューザアカウントステータス	ஏ 有効化済み
ューザグループ 🔹 🔘	IPsec_group ★





14-2 IPsecの設定

「IPsec」の設定をします。

(1) VPN セットアップの設定

「VPN」>「IPsec ウィザード」をクリックします。任意の「名前」を入力、「リモートアクセス」を選択し、「次へ」をクリックします。



VPN作成ウィザード	
1 VPNセットアップ	2 認証 🔰 🕄 ボリシー&ルーティング 🗋 🚭 クライアントオプション 🔰 🕄 設定の確認 🔪
名前	FortiClient
テンプレートタイプ	サイト間 ハブアンドスボーク リモートアクセス カスタム
リモートデバイスタイプ	クライアントペース ネイティブ
	FortiClient Cisco

(2) 認証 設定

下記のように設定します。本手順では【事前共通鍵】を選択します。

着信インターフェース	「Internet(port2)」を指定
認証方式	選択します。例では事前共通鍵を指定
事前共通鍵	(任意の文字列)※FortiClient 設定時に私用します
ユーザグループ	IPsecの接続を許可するユーザーグループを指定します。
	※ここでは手順「14-1」で作成した「IPsec_group」を指定

VPN作成ウィザード			
🜒 VPNセットアップ	2 認証 2 3 ボリシー&ルー	ーティング	🄰 🚯 クライアントオプション 🔰 🕤 設定の確認 🍃
着信インターフェース	🔚 Internet (port2)	•	
認証方式	事前共有鍵 シグネチャ		
事前共有鍵	•••••	۲	
ユーザグループ	IPsec_group	•	

(3) ポリシー&ルーティング

「VPN」>「SSL-VPN 設定」をクリックします。ポリシーの作成画面に移り、設定します。

ローカルインターフェース	「SuitePRONW(port1)」を指定
ローカルアドレス	IPsec 接続を許可する 接続先 を選択。例は「SuitePRO_NW」
クイアントアドレス範囲	クライアントに割り当てるアドレス帯を指定します。
	例は「192.168.100.10-192.168.100.20」
゙サブネットマスク	クライアントに割り当てるサブネットマスクを指定します
	例は「255.255.255」





※DNS サーバー :システム DNS を使うを選択すると Fortinetの DNS が設定されます。

指定の DNS がある場合は「指定」を選択してアドレスを入力してください。

※IPv4 スプリットトンネル:

ON にした場合「ローカルアドレス」で指定した宛先の通信のみが IPsecVPN 経由になります。OFF にした場合、接続元クライア ントの通信はすべて IPsecVPN 経由となります。接続元のネットワーク環境が大きく変わりますのでご注意ください。

VPN作成ウィザード		
🖉 VPNセットアップ 🔰 🕄 芝麻 🔪 🕄	ポリシー&ルーティング 🎽 🖪 クライア	ントオプション 🔰 5 設定の確認 🔪
ローカルインターフェース	SuitePRO_NW (port1)	
	+	
ローカルアドレス	SuitePRO_NW X	
	+	
クライアントアドレス範囲	192.168.100.10-192.168.100.20	
サブネットマスク	255.255.255.255	
DNSサーバ	システムDNSを使う 指定	
IPv4スプリットトンネリングを有効化 🜑		
エンドポイント登録を許可		

(4) クライアントオプション

設定を選択し、「次へ」をクリックします。

VPN作成ウィザード		
🖉 VPNセットアッ	ブ 🎽 🕼 認証 🔰 🕼 ポリシームルーティ	>/) ▶ ④ クライアントオプション ▶ ⑤ 設定の確認 ▶
パスワード保存	0	
オートコネクト	0	
常にアップ(Keep Aliv	e) 🜑	

(5) 設定の確認

設定の一覧が表示されますので確認します。

VPN作成ウィザード	
🕢 VPNセットアップ 🔰 🖉 認証	🔪 ボリシー &ルーティング 💟 🐼 クライアントオブション 🔰 🗿 設定の確認 🔪
● VPNを作成する前に、以下の	設定を確認してください。
オブジェクトの概要	
スプリット <mark>トンネル</mark> グループ	FortiClient_split
フェーズ1インターフェース	FortiClient
フェーズ2インターフェース	FortiClient
アドレス	Fo <mark>rtiClient_range</mark>
リモートからローカルへのポリシー	vpn_FortiClient_remote
エンドポイント登録	FortiClient





(6) 結果確認

結果が示されます。

VPN作成ウィザード	
✓ VPNセットアップ	えび ポリシー&ルーティング 🔰 🖉 クライアントオプション 🔰 🖉 製造の確認 〉
♥ VPNが設定されました	
オブジェクトの概要	
スプリットトンネルグループ	◎ ℡ FortiClient_split 🖋 編集
フェーズ1インターフェース	♥ O FortiClient ✔ 編集
フェーズ2インターフェース	FortiClient
アドレス	◎ 囧 FortiClient_range
リモートからローカルへのポリシー	vpn_FortiClient_remote_0 (9)
エンドポイント登録	◎ 有効

14-3 ファイアウォールポリシーの設定

IPsec 用のポリシーが新たに作成されていますので内容を確認します

「ポリシー&オブジェクト」>「ファイアウォールポリシー」を選択します。対象の IPsec トンネル名のポリシーを選択します。

🕞 fvd 🔹	=	۹			
🛉 お気に入り 🔹 👌	+新	規作成 🖋 編集 🗠 CL	.で編集 💿 削除	Q ポリシーのルックアップ	検索
🙆 ダッシュボード 💦 👌	ÐI	クスポート・ インターフ	フェースペアビュー シ	ーケンス別	
	10	夕前	洋信寺立ちにつ	肉生 マドレフ	7.4
🛃 ポリシー&オブジェクト 🔷				3077 PDX	~ ~ ~ ~
ファイアウォールポリシー 🌣		Forticient M Suterko	TARA (Botta)	*************	
IPv4 DoSポリシー	19	vpn_FortiClient_remote_0	FortiClient_range	SuitePRO_NW	0

NAT 設定は最初「ON」になっております。ON になっていると、IPsec を経由するすべての接続元のアドレスが FortiGate のイン スタフェースになります。接続元アドレスをクライアントアドレスにする場合は「NAT」の設定を「OFF」にしてください。

NAT			
IPプール設定	発信インターフェース	のアドレスを	使用
	ダイナミックIPプール	を使う	
送信元ポートの保持			
プロトコルオプシ=	2 PRot default	•	





14-4 クライアント設定

クライアント端末に FortiClient のインストールを行います。

- (1) ダウンロード https://www.forticlient.com/downloads にアクセスします。 「FortiClient VPN」をダウンロードし、クライアント端末にインストールします。
- (2) FortiClientの設定

インストールした FortiClient を起動し、リモートアクセス> IPsec VPN を選択します。



(3) FortiClientの設定

インストールした FortiClient を起動し、リモートアクセス> IPsec VPN を選択します。

以下の情報を入力し「適用」をクリックします。

接続名	任意の名前を入力(例は、「ipsec vpn」)
リモートGW	FG 管理サイトのホスト名(例は、fvd0000.fg.arena.ne.jp)
	※お客さまにて、FG 管理サイト用のドメインを別途取得している場合はそち
	らを指定する
認証方法	指定した認証方法を設定します。(例 事前共通鍵の場合 : 事前共通鍵を
	指定し、「14-2(2)認証 設定」で設定したパスワード
	設定したパスワードを入力します)





FortiClient Zero Trust Fabric Agent ファイル ヘルブ			-	×
8	VPN接続の編集 VPN 技統名	SSE-VPN Exercision XML		×
🔆 ゼロトラストアクセス	説明 リモートGW	fvd0000.fg.arena.ne.jp		
□ リモートアクセス	認疑方法	◆+リモートゲートウェイを追加 ■前共有鍵 ・	1	
 お知らせ 	認証(XAuth)	 □ ユーザ名入力 ○ ユーザ名を保存 ○ 無効 	J	
₿ () () () () () () () () () ()	Failover SSL VPN	[なし] ~		
() (144)	+詳細設定			
		キャンセル 保存		
■ ロック解除設定				

(4) 接続

※14-1 ログイン (4) クレデンシャルの設定で作成したユーザ PortiClient -- Zero Trust Fabric Agen
ファイル ヘルブ UNLICENSED Q A 🖵 リモートアクセス お知らせ Please contact your administrator or connect to EMS for license activation. Unlicensed VPN access is available until 2023年9月28日 17:29:26 VPN名称 - ≡ ipsec ユーザ名 ipsec_user パスワード □ パスワードを保存 接続

ユーザ名、パスワードを入力し「接続」をクリックし、接続します。





(5) 接続状態確認

VPN 接続済みになったことが確認できます。

FortiClient Zero Trust Fabric Agent		- 🗆 🗙
27416 ALT	VPN接続済み	UNLICENSED
※ ゼロトラストアクセス		
具 リモートアクセス		
① お知らせ	VPN名称 int	sec
〇 設定	IPアドレス 19	22.168.100.10
◎ 情報	ユーザ名 (4) 期間 00	3ec_user1 0:00:07
	受信バイト 0) 送信バイト 2:	KB 21 KB
	切断	ŕ
ロック解除設定		

代表的なエラー

エラー表示	対処
不正なクレデンシャル	ユーザ ID とパスワードを再度確認します。
VPN connection failed. Please check your	FortiClientのポリシーGW に指定したホストと通信がで
configuration and network connection, then try	きません。もしくは事前共通鍵などに誤りがあります。
your connection. If the problem persists, contact	FortiClientの設定を確認してください。
your network administrator for help	
トンネルゲートウエイ/ポリシーサーバーと疎通できません。	FortiClientのポリシーGWに指定したホストと通信がで
	きません。FortiClientの設定を確認してください。





15. IPsec(サイト間接続)

IPsec の設定

FortiGateや Cisco などの機器から IPsec トンネルを使用した VPN 接続をすることができます。 ここでは、例として FortiGate を使用したリモート拠点との接続について説明します。 また、拠点側 FortGgate に固定の WAN 側 IP アドレスが設定されている場合について解説します。

- 15-1 IPsec トンネルの作成
- (1) IPsec トンネルの作成

[VPN]>[IPsec ウィザード]をクリックします。



以下のように設定します。

名前	任意の名前を設定します(例は「IPsec_Tunnel」)
テンプレートタイプ	サイト間
NAT 設定	サイト間に NAT なし
リモートデバイスタイプ	FortiGate

VPN作成ウィザード					
1 VPNセットアップ	2 認証 2 3 ポリシー & ルーティング	ブ 🔰 🗿 設定の確	認		
名前	IPsec_Tunnel	サイ	卜間 - FortiGate		
テンプレートタイプ	サイト間 ハブアンドスポーク				~
1 / 4 7 = 1 - 1	リモートアクセスカスタム	2		Internet	
NAT設定	サイト間にNAIなし このサイトはNAT越し		and the second second	Internet	ALL REAL
	リモートサイトはNAT越し		This FortiGate		Remote FortiGate
リモートデバイスタイプ	Forti Gate				
	diala Cisco				
	<戻る	次へ >	キャンセル		

[次へ]を押下します。





リモートデバイス	IP アドレス
IP アドレス	リモート拠点 FortiGateの wan 側 IP アドレスを指定
	します。(例では「198.51.100.5」としています)
発信インターフェース	Internet(port2) 自動的に選択されます
認証方式	例では「事前共通鍵」を選択します
事前共通鍵	任意の文字列を入力します
	後程リモート拠点側の IPsec 設定でも使用しますの
	で必ず控えておきます。

[リモートデバイス]を『IP アドレス』とし、[IP アドレス]欄ヘリモート拠点 FortiGate の wan 側 IP アドレスを [xxx.xxx.xxx]の形式で入力します。([出力インターフェース]は自動的に選択されます) [認証方式]を『事前共有鍵』とし、[事前共有鍵]欄に任意の文字列を入力します。 **この『事前共有鍵』は後程リモート拠点側の IPsec 設定でも使用しますので必ず控えておきます。**

VPN作成ウィザード			
🔮 VPNセットアップ	🔰 2 認証 🔰 🕄 ポリシー & ルーティング	▶ ④ 設定の確認 ▶	
リモートデバイス	IPアドレス ダイナミックDNS	サイト間 - FortiGate	
リモートIPアドレス	198.51.100.5		
発信インターフェース	🔳 Internet (port2) 🔹		
認証方式	事前共有鍵シグネチャ		Internet
事前共有鍵	••••••	This FortiGate	Remote FortiGate
		mistoridate	hemote i onidate
		50 50 50	
	< 戻る	次へ> キャンセル	

[次へ]を押下します。

[ローカルインターフェース]にて『SuitePRO_NW(port1))を選択します。

[ローカルサブネット]にはお客様の環境に応じて自動的に入力が行われますので、

[リモートサブネット]欄にリモート拠点側のLAN 側セグメントを[xxx.xxx.xxx.xxx/xx]の形式で入力してください。

VPN作成ウィザード			
🖉 venteo トアップ ∑ 🧭	認証 🔰 🕄 ポリシー &ルーティング 🎽 🕘	設定の確認	
ローカルインターフェース	SuitePRO_NW (port1) ×	サイト間 - FortiGate	
ローカルサブネット	203.0.113.0/29		
リモートサブネット	192.0.2.0/24		nternet
インターネットアクセス 0	● None ローカル共有 リモート使用	This FortiGate	Remote FortiGate
	< 戻る 次/	>> キャンセル	

[作成]を押下します。



IPsec トンネルが作成されました。

WebARENA

♥ VPNが設定されました		
作成したオブジェクトのサマリ	j	
フェーズ1インターフェース	IPsec_tunnel	
ローカルアドレスグループ	IPsec_tunnel_local	
リモートアドレスグループ	IPsec_tunnel_remote	
フェーズ2インターフェース	IPsec_tunnel	
スタティックルート	4	
ブラックホールルート	5	
リモートへの許可ポリシー	17	
リモートからローカルポリシー	- 18	

- 15-2 作成された IPsec トンネルの確認
- (1) 自動追加されたリソースの確認

正常に作成されると、以下の項目が自動で追加、設定されます。

[ネットワーク]>[インターフェース]に IPsec トンネルが追加されます。





609	FortiGate VM64-KVM 1	5 7 9 11 13 15 17 19 21 23 6 8 10 12 14 16 18 20 22 24]	
+ 亲	所規作成・ 🧳 編集 🏻 🖮 🎽	□除 ▶ インターフェイスを統	合検索	٩
	名前≑	タイプキ	キーハイト	IP/ネットマスクキ
⊕ ≯	802.3ad アグリゲート ①			12
⊕	トンネルインターフェース	1		
	物理インターフェース 3			
	SuitePRO_NW (port1)	■ 物理インターフェース		
	🖷 Internet (port2)	■ 物理インターフェース		
L	IPsec_Tunnel	⊙ トンネルインターフェース		0.0.0/0.0.0.0

[ネットワーク]>[スタティックルート]にルールが2つ追加されます。

宛先♀	ゲートウェイIP‡	インターフェースキ	ステータスキ	גאב <mark>+</mark>
0.0.0/0	=_=	🔳 Internet (port2)	◎ 有効化済み	
🐴 IPsec_Tunnel_remote		IPsec_Tunnel	● 有効化済み	VPN: IPsec_Tunnel (Created by VPN wizard)
📮 IPsec Tunnel_remote		0 ブラックホール	● 有効化済み	VPN: IPsec_Tunnel (Created by VPN wizard)

[ポリシー&オブジェクト]>[IPv4 ポリシー]に以下のポリシーが追加されます。

	ポリシー	ID	送信元	宛先	サービス	アクション	スケジュール	
Internet (port2) → I SuitePRO_NW (port1) ③								
) IPsec_Tunnel → 🔚 SuitePRO_N	IW (port	1) 1					
	vpn_IPsec_Tunnel_remote_0 (11)	11	🖥 IPsec_Tunnel_remote	Pipec Tunnel local	🔽 ALL	✔ 許可	to always	
Image: SuitePRO_NW (port1) → Image: Internet (port2)								
	\square \blacksquare SuitePRO_NW (port1) \rightarrow \bigcirc IPsec_Tunnel \bigcirc							
	vpn_IPsec_Tunnel_local_0 (10)	10	Pierec_Tunnel_local	🖥 IPsec_Tunnel_remote	🔽 ALL	✔ 許可	🚺 always	

デフォルトでは拠点間の通信は全て許可となりますので、必要に応じてお客様側でポリシーの設定をお願いします。

[ポリシー&オブジェクト]>[アドレス]に以下のアドレスが追加されます。

\$	名前	タイプ	インターフェース	詳細	IP	参照
4 FAB	RIC_DEVICE	サブネット			0.0.0.0/0	0
4 FIRE	WALL_AUTH_PORTAL_ADDRES	S サブネット			0.0.0.0/0	0
4 IPsec	c_Tunnel_local_subnet_1	サブネット			203.0.113.0/29	1
4 IPsec	c_Tunnel_remote_subnet_1	サブネット			192.0.2.0/24	1

15-3 (参考)リモート拠点側の設定

参考として、リモート拠点側 FortiGate の設定例を示します。





IPsec トンネルの作成
 [VPN]>[IPsec ウィザード]をクリックします。

🖵 VPN	~
IPsecトンネル	
IPsecウィザード	☆
IPsecトンネルテンプレー ト	

[名前]に任意の名前を入力します(ここで指定する名前は [15-1]で入力したものと同一でなくて構いません)。

例) Site1l

[テンプレートタイプ]を『サイト間』、

[リモートデバイスのタイプ]を『FortiGate』、

[NAT 設定]を『サイト間に NAT なし』とします。

VPN作成ウィザード			
1 VPNセットアップ	🕑 認証 🕽 🕄 ポリシー&ルーティング 🚺	④ 設定の確認	
名前	Site1	サイト間 - FortiGate	
テンプレートタイプ	サイト間 ハブアンドスボーク		6451
	リモートアクセス カスタム		
NAT設定	サイト間にNATなし		Internet
	このサイトはNAT越し リモートサイトはNAT越し	This FortiGate	Remote FortiGate
リモートデバイスタイプ	# FortiGate		
	India Cisco		
	〈戻る	次へ> キャンセル	

[次へ]を押下します。

[リモートデバイス]を「IP アドレス」

[IP アドレス]へ対象 UTM の wan 側 IP アドレスを入力します。

[発信インターフェース]はリモート側のインターネット側インターフェースを指定します。

[認証方式]を『事前共有鍵』とし、[事前共有鍵]欄に[15-1]で UTM 側作業時に設定したものと

同一の事前共有鍵を入力します。

VPN作成ウィザード			
🕑 VFNセットアップ	🔪 🙆 認証 🔪 🚳 ポリシームルーティング	7 🔰 ● 設定の確認	
リモートデバイス	IPアドレス ダイナミックDNS	サイト間 - FortiGate	
リモートIPアドレス			
発信インターフェース			
認証方式	事前共有鍵 シクネチャ		Internet
事前共有鍵	·····	This FortiGate	Remote FortiGate
	〈戻る	次へ> キャンセル	





[次へ]を押下します。

[ローカルインターフェース]にて IPsec 接続をするお客様環境の LAN 側インターフェースを選択します。 [ローカルサブネット]が IPsec 接続をするお客様環境の LAN 側セグメントになっていることを確認の上、 [リモートサブネット]欄にサーバー側セグメント(SuitePRO_NW(port1)のセグメント) を[xxx.xxx.xxx.xxx/xx]の形式で入力してください。



[作成]を押下します。

IPsec トンネルが作成されました。

VPN作成ウィザード	
🔮 VPNセットアップ 🔰 🕑 副証	◊ ポリシー ムルーティング ▶ ◆ 読の寝 ▶
♥ VPNが設定されました	
オブジェクトの概要	
フェーズ1インターフェース	O Site1
ローカルアドレスグループ	Site1_local 編集
リモートアドレスグループ	◎ 醖 Site1_remote 🕜 編集
フェーズ2インターフェース	Site1
スタティックルート	◎ 4 🖋 編集
ブラックホールルート	◎ 5 🖋 編集
ローカルからリモートへのポリシー	✓ ypn_Site1_local_0 (12)
リモートからローカルへのポリシー	vpn_Site1_remote_0(13)
	その他の追加トンネルリストを表示

作成後は、[15-2]を参考に適直設定内容の確認を行ってください。





16. 証明書のインポート

証明書のインポート

FortiGate で利用する証明書をインポートします。

(1) 証明書の選択

「システム」>「証明書」をクリックします。

🏟 システム	~
管理者	
証明書	☆

(2) 「インポート」>「ローカル証明書」をクリックします。

◆ 作成/インポート・
証明書
CSRの生成
CA証明書
リモート
CRL

「証明書をインポート」をクリックします。

- } 11	明書をインポート
	既存の証明書をファイルアップロードでインポートします。
	証明書をインポート

(3) 証明書・キーファイルの選択

下記のように指定し、最後に「OK」をクリックします。

タイプ:証明書

証明書ファイル:証明書ファイルを選択

キーファイル:秘密鍵ファイルを選択

パスワード:鍵ファイルにパスワードを設定している場合のみ入力

証明書名:ファイル名に合わせて自動的に設定されます。書き換えることもできます。





♪ 証明書を~	インポート		
タイプ	ローカル証明書	PKCS12証明書 証明書	
証明書ファイ	λ	example.pem 3.47 KiB	
キーファイル		example.key 1.66 K1B	
パスワード			
パスワード確	570 PrO1		
証明書名	example	2	
	作成	戻る	

(4) 証明書インポート確認

証明書の一覧に新しく証明書が追加されたことを確認します。

example C = JP, CN = example.com, L = Minato-ku, O = Example Corp., ST = Tokyo, OU = r45011704591760

ステータスも「OK」になっていることを確認します。







17.コンソール

コントロールパネルからコンソールに接続し、FortiGate にログインすることができます。

- 17-1 コンソールからログイン
- (1) コントロールパネルにログインして「セキュリティ」メニューをクリックし、プルダウンから「UTM/NIC4」を選択します。

SuitePRO V4 (https://pro4.arena.ne.jp) IndigoPro (https://compas.arena.ne.jp)



(2) 「基本情報」タブの「UTM 情報」 > 仮想 UTM サーバー管理」にある、「仮想 UTM サーバー」をクリックします。

基本情報	情報 管理サイトアクセス許可IP設定		
UTM情報			
仮想UTMサーバー管理		仮想UTMサーバー	

(3) 右側のコンソール「開く」をクリックするとコンソール画面が開きます。



(4) ログインアカウントとパスワードを入力し、ログインします。

fvd0000 login : username Password: Welcome!

コマンドの詳細は Fortinet 社の CLI reference を参照ください。(使用中のバージョンを選択してください) Fortinet Document Library https://docs.fortinet.com/product/fortigate/



17-2 接続元 IP アドレスの許可設定を追加する場合

ここでは FortiGate に接続元のアドレス許可設定を行います。UTM 管理サイトにアクセスするには、接続元のアドレスを許可設 定が必要です。接続元のアドレス許可設定は UTM 管理サイトまたはコンソールで行えます。

アカウント名	(例) username
追加するアドレス	(例)203.0.113.41

(1)「config system admin」と入力し、管理者アカウントの設定に移動します。続いて「get」と入力し、現在のアカウントの一覧を表 示し、アカウント名を確認します。

fvd0000 # config system admin

fvd0000 (admin) # get == [username] name: username

(2) 「edit アカウント名」で対象のアカウントの設定に移ります。「show」と入力すると現在の設定が表示されます。 「trusthost」が何番まで使われているか確認します。例では"trusthost1"が使われています。

fvd0000 (admin) # edit username fvd0000 (username) # show config system admin edit "username" set trusthost1 203.0.113.40 255.255.255.255 set accprofile "super_admin" set vdom "root" set password ENC SH2EGMYy5NOQsZ+YqoNFzxROnlY6utMjhQLlOKHB next

trusthost2 にアドレスを追加します。(例)「set trusthost2 203.0.113.41 255.255.255.255」と入力します。 (3) 「trusthost」は1から10まで使用可です。追加の場合は、元の設定を上書きしないよう使われていない番号を選択してくださ L۱°

現在の設定を書き換えたい場合は対象と同じ番号を指定します。

fvd0000 (username) # set trusthost2 203.0.113.41 255.255.255.255





(4) 追加後、「show」コマンドで現在の設定を確認します。trusthost2に「203.0.113.41」が追加されています。

fvd0000 (username) # show config system admin edit "username" set trusthost1 203.0.113.40 255.255.255.255 set trusthost2 203.0.113.41 255.255.255.255 ←追加されている set accprofile "prof_admin" set vdom "root" set password ENC SH2EGMYy5NOQsZ+YqoNFzxROnlY6utMjhQLlO next end

(5) 「next」で設定を終了します。ここで設定が保存・反映されます。続いて「end」「exit」で FortiGate からログオフします。

fd0000(user name) # next fvd0000(admin) #end #exit





18. FortiGate 管理-snmp 監視設定

FortiGate 自身を外部の監視サーバーから監視するための設定です。

18-1 インターフェース設定

(1) ネットワーク>インターフェースを開き、port1 (SuitePRO_NW)を選択し、色を反転させ、編集をクリックします。

🖃 🖩 物理インターフェース 2				
SuitePRO_NW (port1)	■ 物理インターフェース			
🖮 Internet (port2)	■ 物理 ハーク・フェース ステータスを設定 ・			
	✔ 編集			
	前 削除			
	▶ インターフェイスを統合			

(2) 管理者アクセスのSNMPをONにします。

管理者アク	セス		
IPv4	 ☑ HTTPS □ FMGアクセス □ FTM 	 HTTP ① SSH RADIUSアカウ ンディング 	 ✓ PING ✓ SNMP □ セキュリティフ ァブリック接続 ()

- (3) 中央下の「OK」をクリックします。
- 18-2 snmpd 設定

システム> snmpd を選択します

(1) SNMP エージェントの設定を ON にして説明やロケーションなど任意の情報を入力します。コミュニティを作成します。 「新規作成」をクリックします。

🛓 FortiGa	ite MIB ファイ	(ルのダウンロード	🕹 Fortin	et Core MIB ファ-	イルのダウン <mark>ロ</mark> ード
システム情報	ą				
SNMPエージ	エント 💽	Product			
ロケーショ: コンタクト	ン 情報	Токуо			
SNMP v1/v2c	c				
+新規作	成 🖋 編集	自削除ス	テータス・		
	The states	42. 33	14 14 14	1 2 3 4	2 2





(2) ホストの項目に監視サーバーの設定を入力します。 コミュニティ名:監視サーバーと同じコミュニティ名を入力します。 IP アドレス: 監視サーバーの IP アドレス ホストタイプ: クエリやトラップ等の種別を選択

i規SNMPコミ.	1_71					
コミュニティタ	5 monitor					
自动化溶血						
HANGH07						
ホスト						
Pアドレス	192.168.1.1	15	3	6		
ホストタイプ	クエリを受	け入れトラッ	プを送信す ▼			
Pアドレス	192.168.5.1	í.	\$	¢		
たストタイプ	クエリを受	け入れトラッ	プを送信す ▼			
		0				
\sim	2 1	\sim	-	\sim	\sim	
\sim	\sim	\sim	\leq	~~	\sim	\searrow
1有効	0		\sim	\sim		\sim
ローカルポー	h 162					
リモートポー	h 162					
/2c有効	O					
ローカルポー	h 162					
ッモートポー 	ト 162	とを確認	烈「適田	をクリッグ	フレ,ます。	
リモートボー 3)作成 をFortiGate N	ト 162 されたこ	とを確認 ^{かンロード}	記「適用」	レントン・100000000000000000000000000000000000	<i>1</i> します。 >===	
リモートボー 3) 作成 を FortiGate N システム信報	ト 162 されたこ	とを確認 ^{かンロード} [記し「適用」	をクリック 5ファイルのダウ:	ルます。	
リモートポー 3) 作成で を FortiGate N システム情報 SNMPエージェン	ト 162 されたこ 118 ファイルのち	とを確認 ^{17フレード}	記[適用] ▲ Fortinet Core MI	をクリック 8ファイルのダウ:	します。 >ロード	
リモートポー 3) 作 成で ▲ FortiGate M システム情報 SNMPエージェン 説明	ト 162 されたこ 118 ファイルのち ハト © Produk	とを確認 ^{*ウンロード} 」[*	忍し「適用」 ▲ Fortinet Core MI	をクリッグ ^{8 ファイルのダウ:}	7 します。 >□-ド	
リモートポー 3) 作 成で ▲ FortiGate N システム情報 SNIMPエージェン 説明 ロケーション	ト 162 されたここ 118 ファイルのら パト © Produc Tokyo	とを確認 ^{(カンロード}) (1	記「適用」 ▲ Fortinet Core MI	をクリック 8 ファイルのダウ:	ルます。 >□-ド	
リモートポー 3) 作 成 ▲ FortiGate N システム 信報 NIMPエージェン 説明 ロケーション コンタクト 信報	ト 162 されたここ HIB ファイルのタ Produc Tokyo	とを確認 ^{カンロード}	記「適用」 ≥ Fortinet Core MI	&クリッグ סיד רוגסאיס:	<i>1</i> します。 >□-ド	
リモートポー 3) (作 氏 て 3) (作 氏 て 3) (作 氏 て 5) () () () () () () () () () () () () ()	ト 162 118 ファイルのら パト © Produc Tokyo	とを確認 ウンロード a	恕し「適用」 ▲ Fortinet Core MI	をクリック 8 ファ・ハルのダウ:	<i>1</i> します。 >□-ド	
リモートボー 3) /(下方広。 ▲ FortiGate M SNMPエージェン 説明 ロケーション コンタクト情報 NNMP v1/v2c	ト 162 されたここ HB ファイルのタ Produc Tokyo	とを確認 	記し「適用」 ▲ Fortinet Core MI	をクリック ファイルのダウ:	<u>します。</u> >ロード	
リモートボー 3) / 「F」5人で 3) / 「F」5人で 4) / 「F」5人で 3) / 「F」5人で 4) / 「F」5 / 「」5 / 「」	Image: https://www.image: https://wwwww.image: https://www.image: htttps://wwww.image: https://www.image: https://www.image: htt	とをび曲訳 rヮンロード [rt n the admin trus	Qし「適用」 ▲ Fortinet Core MI	をクリック 8 ファイルのダウ:	<i></i> します。 >===	
リモートボー 3) / Fp5に 3) / Fp5に 500000000000000000000000000000000000	ト 162 されたここ IIB ファイルの分 Product Tokyo are missing from マ 編集 自	とを確認。 かつンロード [.t. 前除 [ステー	2し「適用」 ▲ Fortinet Core MI ted hosts. 管理書の 夕ス-	をクリック 3 ファイルのダウ:	7 ∪ ます。 ∞×	
リモートボー 3) / Fp5Cc ▲ FortiGate N システム債報 SNMPエージェンシ 加明 ロケーション コンタクト債報 SNMP v1/v2c ▲ Server IP: ▲ Server IP: 名前 ©	ト 162 ト 162 ト 162 ト ○ Produc Produc Produc マ 福島 章 クエリキ	とを確認 が つンロード	記し「適用」 ▲ Fortinet Core MI ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	をクリック 3 ファイルのダウ: 第 篇集 Pvottスト®	7 035 .	ステータス *
リモートボー 3)/(Fp5)に ▲ FortiGate M システム(情報 SNMPエージエン 説明 ロケーション コンタクト(朝朝 SNMP v1/v2c ▲ Server IP) ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	ト 162 されたここ HB ファイルのS Produc Tokyo are missing from ● 4編集 音 クエリキ ● v1有効 ● v2有効	とを確E;; オ オ n the admin trus 削除 ステー トラップ [↓] ● v1有効 ● v2有効	CL「適用」 Lorinet Core MI Led hosts. 管理者の タス- ホスト ⁶ 192168.1.15/32 192168.5.1/32	をクリック 8 ファイルのダウ: 第 ファイルのダウ: 第 ファイルのダウ: 1 Pvoホスト®	7します。 >ロード イベントキ 41	ステータス↓ ● 有効
リモートボー 3) / Fp5Ca ▲ FortiGate N システム(情報 SNMPエージェン 説明 ロケーション コンタクト(情報 SNMP v1/v2c ▲ Server IP: ▲ Server IP: 名前 © ▲ monitor	ト 162 ト 162 ト 162 ト 0 Produc Tokyo are missing from ↓ 編集 自 クエリキ ○ v1有効 ○ v2有効	とを確認。 かつ>ロード tt 前除 ステー トラップ [↑] ◎ v1有効 ◎ v2有効	CL「適用」 Ed hosts. 管理書の 5/2- オスト章 192168.5.1/32	をクリック 3 ファイルのダウ: 3 ファイルのダウ: 1 Pvottスト®	7します。 >ロード イベントキ 41	ステータス * ② 有効

他トラップを選択し、「OK」をクリックします

- 18-3 管理アカウント設定
- (1) システム>管理者を開きます。







(2) 管理者設定を入力します

項目	値
名前	任意(例では「snmp」)
パスワード	任意
管理者プロファイル	admin_no_access
信頼されるホストにログインを制限	ON
信頼されるホスト	SNMP 監視サーバーのアドレスを入力

7 _+++-7		
ユーリ名	snmp	
タイプ	ローカルユーサ	
	リモートサーバグループの単一ユーザと一致	
	リモートサーバグループのすべてのユーザと一致	¥
	public key infrastructure (PKI) グループを利用	
パスワード	••••••	
パスワードの再入力	•••••••	
コメント	コメント記入)/25
管理者プロファイル	admin no access	1120
 二要素認証 		
 二要素認証 信頼されるホスト 	-にログインを制限	
 二要素認証 信頼されるホスト 信頼されるホスト1 	-にログインを制限 192.168.1.15/32	
 二要素認証 信頼されるホスト1 信頼されるホスト2 	にログインを制限 192.168.1.15/32 192.168.5.1/32	
 二要素認証 信頼されるホスト 信頼されるホスト1 信頼されるホスト2 	にログインを制限 192.168.1.15/32 × 192.168.5.1/32 ×	
 二要素認証 信頼されるホスト 信頼されるホスト1 信頼されるホスト2 	にログインを制限 192.168.1.15/32 192.168.5.1/32 C	
 二要素認証 信頼されるホスト1 信頼されるホスト2 管理者をだてして、 	にログインを制限 192.168.1.15/32 192.168.5.1/32 マカウントのブロビジュニングのみに生肥	





19. FortiGate 管理-CPU・メモリ負荷の詳細確認

負荷状況の詳細を確認します

sys top の確認と プロセスの kill

- (1) CLIコンソールを開きます。画面右上のメニューをクリックします
 - CLIコンソール



(2) CLI ウインドウが表示されます

「diagnose sys top」と入力し、実行します。コマンドを入力してソートすることができます。

c: CPU 使用率の順にソートして表示

m: メモリ使用率の順にソートして表示

q:表示を終了

左から、プロセス名、プロセス ID,現在のステータス、CPU 使用率(%)、メモリ使用率(%)を示します。

例「updated」プロセスはシグネチャ・DB などのアップデートプロセスです。 処理中は一時的に CPU を消費します

Run Time: 0 da	ys, 4 hours	and 1 m	inutes		
9U, 0N, 2S,	85I, 4WA, (OHI, OSI,	0ST; 199	92T, 855F	:
updated	32630	RN	92.8	0.2	
node	254	5 <	1.9	0.3	
sslvpnd	404	S	0.5	0.1	
slbrpcd	372	S	0.5	0.0	
forticldd	343	S	0.1	0.2	
httpsd	25525	S	0.1	0.1	
initXXXXXXXXXXXXX	1	S	0.1	0.0	
newcli	32641	R	0.1	0.0	





20. FortiGate 管理-システムログの確認

FortiGate のログを確認します

システムログの確認

(1) ログ&レポート>システムイベントを開きます。



(2) ログをクリックし、「一般的なシステムイベント」を選択し、「メモリ」(またはディスク)をそれぞれ選択します。

サマ	IJ	ログ			
C	*	¢ -	-般的なシステムイベント・	🕞 メモリ 🗸	□詳細

ログ出力例1: CPU usage statics (CPU 使用量)

	Notice	CPU usage reaches: 93	CPU usage statistics
l	コグ出力例2: FortiGate u	pdate succeeded(アップデート完了)	
	Notice	Fortigate scheduled update fcni=yes fdni=yes	FortiGate update succeeded

・ログの保存期間について

メモリ上のログは再起動後残りません。

ディスクログの保存期間は初期設定では7日間となっています。期間の変更を行う場合はCLIコンソールで 「maximum-log-age」の値を変更してください。0-3650までの数字が指定できます。

CLIコンソール









21. FortiGate 管理-オートメーション設定

動作を自動化する機能です。トリガーとアクションの2つをまとめたスティッチを作成します。ここでは例として Conserve mode に移行し たときに指定のアドレスにメールを送信する設定を行います。

Conserve mode…メモリ使用率が高い時に移行する自己防衛モード

スティッチの作成

(1)セキュリティファブリック>オートメーションを開きます。



(2) スティッチを作成します。新規作成を開きます。



(3) 名前を入力し、まずトリガーを追加します



※トリガーを選択します

エントリを選択	×
Q検索	◆ 新規作成
Anomaly Logs	
ウイルスログ(1)	
🚯 Virus Logs	
コンサーブモード(1)	
* Conserve Mode	Ø
スケジュール(1)	
Weekly Trigger	
セキュリティレーティング	ブサマリ (2)
🔆 Any Security Rati	ng Notification
🔆 Security Rating N	otification -
適用	キャンセル





(3) その次に「アクションを追加」を選択します



(4) 「Email Nortification」を選択します。

エントリを選択	×
Q 検索	◆ 新規作成
CLIスクリプト (1) >_ CLI Script - System Statu Eメール (4)	15
Email Notification	Ø
 ✓ HAFallover_email ✓ Network Down_email ✓ Reboot_email FortiExplorerの通知(4) ジ FortiAnalyzer Connection 	on Down_ios-n
∢ 適用 キ	ャンセル

To 宛先、サブジェクト、本文などを指定します。

名前	Email N	otification		
最小インターバル 0	0		秒	•
说明	Send a c specifie	custom email to the d recipient(s).	2 // 51	0/255
Eメール				
From				
FortiCareのEメールに	送信 🔿			
Го		sample@examp	le.com	
		N.	0	
			v	
サブジェクト		%%log.logdesc%	6%	
サブジェクト 本文		%%log.logdesc% 日時 : %%log.da	5% ate%% %	%log.time%%
サブジェクト 本文		%%log.logdesc% 日時 : %%log.da devname : %%	i% ate%% % log.devn	%log.time%%

From は指定が無い場合 DoNotReply@fortinet-notifications.com になります。

※「FortiCare の E メールに送信」は OFF のままご利用ください。

(5)完成したら「OK」をクリックします。アクションは複数追加できます。





前	Conserve mode
テータス クションの実行 ① 明	 ○ 有効 ○ 無効 シーケンシャル パラレル /0/255
テッチ * トリナ Conserv	y ve Mode
	😮 遅延の追加
Market Ac	tion ×
• 7	クションを追加

以上は設定の一例になります。このほかの設定や詳細に関しては Fortinet 社のコミュニティやフォーラム、ドキュメントを参照ください。

22.設定例

ここでは過去にお問い合わせいただいた設定方法についてまとめました。

22-1 設定例1:国内アドレスのみを許可する

- ファイアウォールポリシーは上から順に評価され、一致したポリシーがあればそのポリシーで通信します。お客様のポリシー構成に応じて、移動が必要な場合はドラッグして順番を変更してください。
- 許可されていない通信は、「暗黙の拒否」ポリシーによって拒否されますので、基本的に拒否ポリシーの作成は必要ありません。(ポリシー構成に応じて拒否ポリシーが必要な場合は設定してください)

Japan_RDP_Accept (1)	4 SuitePRO_NW	Co always	RDP	✔ 許可	許可
----------------------	---------------	-----------	-----	------	----

(1) 許可ポリシーの作成 国内限定の通信許可設定を行います。事前にプリセットされている「Japan_Segment」(ジオグラフィアドレス)を使用します。

新規ファイアウォールポリシーの作成

「新規作成」>「ファイアウォールポリシー」をクリックすると、ポリシー作成画面が表示されます。

▶ ファイアウォールポリシーの表示

「ポリシー&オブジェクト」>「ファイアウォールポリシー」をクリックすると、ファイアウォールポリシーが表示されます。 「新規作成」>「ファイアウォールポリシー」をクリックすると、ポリシー作成画面が表示されます。

下記のように設定します。

着信インターフェース	「Internet(port2)」を指定
発信インターフェース	「SuitePRO_NW(port1)」を指定





送信元	[Japan_Segment]
宛先	「SuitePRO_NW」(例)
サービス	RDP
アクション	許可
NAT	無効(例)
セキュリティプロファイル	(例 ここでは指定しません。)任意の設定を追加してください

VVII VIII VIII VIII VIII VIII VIII VII		
前 0	Japan_RDP_Accept	
循インターフェース	Internet (port2)	×
循インターフェース	SuitePRO_NW (port1)	×
信元	Japan_Segment	×
洗	SuitePRO_NW	×
くケジュール	o always	-
ナービス	RDP +	×
7クション	✔ 許可 Ø 拒否	
(ンスペクションモー	ド フローベース プロキシベ・	-ス
ファイアウォール/ネッ	v トワークオプション	
IAT C		
プロトコルオプション	PROT default	* #
?キュリティプロファ	イル	
シチウイルス 0	•	
Vebフィルタ O	•	
os a	•	
アイルフィルタ 0	•	
メールフィルタ 0)	

▶ 無効化設定

「このポリシーを有効化」を無効にし、「OK」をクリックして、ポリシー作成を完了します。



ポリシーリストの一番下に「×」が付いた状態(無効化されている)で表示されます。この段階では、まだこのポリシーは反映されていません。

25	😢 Japan_RDP	Japan_Segment	4 SuitePRO_NW	C always	RDP	✔ 許可
----	-------------	---------------	---------------	----------	-----	------

(3) ポルシーの有効化

ポリシー位置に問題ないことを確認し、有効化します。

対象ポリシーを選択し、「有効」をクリックし有効化します。ポリシーの設定が反映されます。

🖋 編集 🖥 挿入 🔹	⊘ 有効	前 削除	▼ さらに
---------------	------	-------------	-------





22-2 設定例2: インターネット系サービスの許可も追加する場合(ISDBの利用)

日本国内の許可に加えて、インターネット系のサービスも許可したい場合は、インターネットサービスデータベースのを使用します。イ ンターネットサービスの指定はアドレスオブジェクトと一緒に指定できませんので専用にポリシーを作成します。

Create New Policy エントリを選択 × 名前 🛛 検索 Q + 着信インターフェース Internet (port2) 4 インターネットサービス・ 発信インターフェース SuitePRO_NW (port1) - インターネットサービス (277) + 👩 GitHub-GitHub 送信元 & GoDaddy-Other + GoodData-Other 宛先 4 SuitePRO_NW M Google-Gmail 💪 Google-Google.Bot always スケジュール 👩 Google-Google.Cloud サービス SMTP G Google-Other G- GTHost-Dedicated.Instant.Servers Hadrian-Scanner ✓ 許可 ◎ 拒否 アクション Hetzner-Hetzner.Hosting.Service インスペクションモード フローベース プロキシベ th HP-Other ファイアウォール/ネットワークオプション 🤞 HubSpot-Other Mulu-Other NAT 0 () Hurricane.Electric-Hurricane.Electric.Internet.Servi. PROT default プロトコルオプション 🖮 IBM-Other セキュリティプロファイル クローズ

送信元(もしくは宛先)の選択で「インターネットサービス」を選択し、一覧から追加したいアドレスを選択します。

● インターネットサービスの種類の確認

ポリシー&オブジェクト>インターネットサービスデータベース のメニューを開き、内容を確認してください。宛先。送信元などの方向に よって使用できるサービスに違いがあります。

インターネットサービス ネット	フークサービス		
+新規作成 ・ / 編集 / 幅 クローン	× [>_ CLIで編集] @ 削随		
● IPアドレスルックアップ 検索		Q	
名前 🕈	方向章	エントリ数 🌣	参照 🕈
👷 Redhat-Other	両方	970	0
Redhat-Outbound_Email	宛先	970	o
👷 Redhat-RTMP	宛先	970	0
e Redhat-SSH	宛先	970	0
👷 Redhat-Web	宛先	970	0
RedShield-RedShield.Cloud	両方	37	0
Restream-Restream.Platform	宛先	1,024	0
RingCentral-RingCentral	宛先	2,353	0
- Salesforce-DNS	宛先	10,996	0





23. Q&A

全般

Q: 「admin」とは何でしょうか

A: 弊社管理のサポート用アカウントになります。削除や変更はお控えいただくようお願いいたします。削除・変更されますと、お問い合わせの際にお客様の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。

- 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: 各設定画面の右側に「オンラインガイド」や「コミュニティ」のリンクがあるのでご参照ください。
 設定可能な最大値情報は Fortinet の max-values Table でご確認いただけます。
 (Model は FortiGate VM1 を選択)
 https://docs.fortinet.com/max-value-table
- Q: FortiGateの他の設定方法を知りたい。
- A: Fortinetの以下のサイトをご確認ください。 https://community.fortinet.com/ https://docs.fortinet.com/product/fortigate/
- Q: smtp(25/tcp),pop3(110/tcp),imap(143/tcp),submission(587/tcp)がオープンしているように見えるのですが。
- A: Anti Virus でメールを指定している場合、また WAF や Anti SAPM を使用している場合、FortiGate 側で応答を返します。
- Q:msrpc(135/tcp)がオープンしているように見える。
- A: Anti Virus で MAPIを指定している場合、また、Anti SAPMを使用している場合、FortiGate 側で応答を返します。
- Q: ftp(21/tcp)がオープンしているように見える。
- A: Anti Virus で FTP を指定している場合、FortiGate 側で応答を返します。
- Q: http(80/tcp・8008/tcp)がオープンしているように見える。 A: Anti Virus で HTTP を指定している場合、また WAF を使用している場合、FortiGate 側で応答を返します。
- Q: https(443/tcp)がオープンしているように見える。
- A: WAFで SSL/SSH インスペクションを使用している場合、FortiGate 側で応答を返します。
- Q: xmpp(8010/tcp)がオープンしているように見える。 A: WAF を使用している場合、FortiGate 側で応答を返します。
- Q: auth(113/tcp)がクローズされているように見える。







A: 113/TCP に関しては、FortiGate により RST パケットを返します。 パケットドロップの場合、ident 認証(RFC1413)でタイムアウトするまでクエリの再送信が行われてしまうため、FortiGate 側でクローズしています。

Q: 仮想 UTM 下のサーバー間通信は UTM でフィルタされますか。

A: 同サブネット間通信は仮想 UTM を経由せず直接アクセスしますのでフィルタされません。

Q: 古いSSL バージョンの通信がブロックされます。

コメント欄に"Read-only~"とあるプロファイルは編集できません。新規作成で新たにプロファイルを作成するか、GUIで既存

プロファイルをクローンしてから新しいプロファイルを編集し、ファイアウォールポリシーにセットしてください。

[firewall ssl-ssh-profile] Fortinet: Home> FortiGate / FortiOS 7.4.4 >CLI Reference

https://docs.fortinet.com/document/fortigate/7.4.4/cli-reference/116695140/config-firewall-ssl-ssh-profile

Q: FortiOS をアップグレードした後、Web サイトがブロックされるようになりました。

「SSL/SSH インスペクション」の既存プロファイル設定において FortiGate がアクセス先サーバーに対して 証明書の審査を実施し、この審査でエラーが発生するとトラフィックをブロックする仕様が FortiOS7.0.0 から追加されました。 このブロックを回避するには対象プロファイルの「cert-probe-failure」のアクションを「allow」に変更します。

config firewall ssl-ssh-profile

edit <certificate profile name>

config <protocol name>

set cert-probe-failure {allow | block}

end

next

end

初期状態で用意されているプロファイル「certificate-inspection」「custom-deep-inspection」「deep-inspection」の https プロトコルは block の設定になっています。





コメント欄に"Read-only~"とあるプロファイルは編集できません。新規作成で新たにプロファイルを作成するか、GUIで既存 プロファイルをクローンしてから新しいプロファイルを編集し、ファイアウォールポリシーにセットしてください。 「firewall ssl-ssh-profile」 Fortinet: Home> FortiGate / FortiOS 7.0.0 >CLI Reference https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-allow-HTTPS-port-443-traffic-when/ta-p/200844

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。使用を解除してから削除してください。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 から除外してください。ポリシーのほかの項目、またアドレスグループ、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、ドラッグ&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。優先順位をご確認べださい。
- Q: マニュアルのように、ポリシーに Internet→SuitePRO_NW の表示がない。
- A: ポリシー上部の右側に、「インタフェースペア表示」、「シーケンス順」のボタンがあります。「インタフェースペア表示」をクリックする と、マニュアルと同じ見え方になります。
- Q: マニュアルよりも、ポリシーの項目が少ない。
- A: ポリシー上部にある「ID」「名前」の行で右クリックをすると、カラムを選択できます。表示させたいカラムを選択し、下から二番目の「適用」をクリックさせるとポリシーの表示項目が増えます。
- Q: セキュリティ検査を行ったが、HTTPS 通信で IPS や WAF で検知が検知されない。
- A: HTTPS などの暗号化通信を監視するには Web サイトで使用しているキーペアをポリシーに設定する必要があります。 「証明書のインポート」を実施した後「セキュリティ SSL/SSH インスペクション」を実施してポリシーに設定を行ってください。

DoS ポリシー

Q: 着信インターフェースとは

A: ポリシーを適用するインターフェースになります。着信インターフェースによって対象の通信が異なります。

「Internet」・・・インターネットからの通信(Inbound)

「SuitePRO_NW」の場合・・・・仮想専用サーバーからの通信(Outbound)



Q:「しきい値」をどう決めたらよいのか

A: ある程度のおおまかな値を目安として設定し、一定期間モニターされることで検知状況の把握ができますので参考にされてくだ さい。ロギングを ON にした状態でアクションに「モニタ」を適用します。検知された結果はアノマリログで確認できます。

証明書エラー

Q: UTM 管理サイトヘアクセスしたときに証明書のエラーが表示される。

A: お客さまにて UTM 管理サイト用のドメインと、そのドメインの証明書を取得してください。

また、ドメインのAレコードは「UTM 管理サイト」のドメインと同じ IP アドレスを指定します。

- ① ドメイン取得 (FortiGate で使用するため、サーバーとは別に準備する)
- ② DNS 登録 A レコードで FG 管理サイトの IP アドレスを指定(例: fvd1111.fg.arena.ne.jp)
- ③ 取得したドメインの証明書購入
- ④ FortiGate:証明書インポート ※手順「証明書のインポート」参照
- 5 FortiGate:証明書設定 「システム」>「設定」メニュー 「管理者設定」>「HTTPSサーバー証明書」にて対象の証明書を選択し、適用

WAF (Web Application firewall)

O: ファイアウォール設定画面上に WAF (Web アプリケーションファイアウォール) が表示されない A:ポリシーのインスペクションモードを「プロキシベース」に変更すると表示されます。

- Q: 設定画面上に WAF が表示されない (初期 OS6.0.3 をご利用のお客様)
- A: FortiOS6.2 以降の環境では WAF の設定を GUI 上で表示させるために設定が必要となります。

(1)インスペクションモードの表示 (FortiOS 7.2 以上のみ)

画面右上に並んでいるアイコンの左端の「CLI コンソール」をクリックしコンソールを開きます。

以下のコマンドを実行して閉じます。

config system settings

set qui-proxy-inspection enable

end

(2)Web アプリケーションファイアウォールの有効化

システム>表示機能設定>Webアプリケーションファイアウォール →有効であること。無効の場合は有効にして OK をクリックする

(3)インスペクションモードの変更

ポリシー&オブジェクト>ファイアウォールポリシー WAFを設定したいポリシーを選択して、編集をクリック インスペクションモードを「プロキシモード」に設定する。 →Web アプリケーションファイアウォールが表示されますので、 ここで対象のプロファイルを選択してください。





SSLVPN

Q: SSLVPN の設定メニューが表示されない

A: FortiOS7.4.1 から SSL VPN は GUI で非表示になりました。GUI 上に表示させるためには CLI コンソールから以下の設 定を行って下さい。

----config system settings set gui-sslvpn enable end

Update SSL VPN default behavior and visibility in the GUI https://docs.fortinet.com/document/fortigate/7.4.0/new-features/233856/update-ssl-vpn-default-behavior-and-visibility-in-the-gui-7-4-1

オートメーション

Q:「Email Notification」内にある「FortiCareのEメールに送信」に記載のアドレスはどこのものですか。

A: 製品登録に使用しているメールアドレスになります。こちらの設定は OFF にしてご利用ください。





24. 提供 仕様

24-1.仮想 UTM OS イメージの違い

初期OS	FortiOS 6.0.3 2017/04 以降インストール	FortiOS 7.4.4 2024/11/08 以降インストール
お客さまアカウントのプロファイル	prof_admin ポリシーなどの設定変更が可能	super_admin すべての権限を持ちます ※プロファイルが変化したことにより「admin」アカウ ントも表示されるようになります。このアカウントは弊 社管理のサポート用になります。削除や変更はお 控えいただくようお願い致します。削除・変更されま すと、お問い合わせの際こお客様の事象が確認で きなくなり、適切なサポートが難しくなる場合がござ います。
お客様アカウントの形式	アカウント名@UTM名	アカウント名-UTM名

- そのほかの FortiGate の設定や仕様に関しては FortiOS の仕様に準じます
- 弊社変更内容については「24-2 イメージ初期設定」をご参照ください。
- 「FortiOS 6.0.3」のお客さまアカウントのプロファイルを「prof_admin」から「super_admin」に変更することも 可能です。

※ご希望の場合は、仮想 UTM のホスト名情報を添えてテクニカルサポートまでお問い合わせください。OS イン ストール時に作成したアカウントが変更対象となります。





24-2 イメージ初期設定

イメージ バージョン 7.4.4 の初期設定です。他の設定は ForiOS7.4.4 の初期設定に準じます。 これらの初期設定は CLI コンソールなどで変更可能です。

Home >FortiGate / FortiOS 7.4.4 >CLI Reference

https://docs.fortinet.com/document/fortigate/7.4.4/cli-reference/84566/fortios-cli-reference

config system global	
management-port-use-admin-sport	disable
proxy-auth-timeout	5
refresh	5
sys-perf-log-interval	0
timezone	Asia/Tokyo

config system settings		
default-voip-alg-mode	kernel-helper-based	
gui-load-balance	enable	
gui-spamfilter	enable	
gui-wireless-controller	disable	
gui-wan-load-balancing	disable	
gui-waf-profile enable	enable	
gui-allow-unnamed-policy	enable	
gui-multiple-interface-policy	enable	

config system ntp	
syncinterval	10

config system automation-action edit "Email Notification"	
forticare-email	disable



config report layout			
schedule-type	demand		

config vpn ssl settings				
port	4443			

config system admin	
admin	※弊社管理のサポート用アカウントになります。削除や管理者権限を変更はお 控えいただくようお願い致します。削除されますとお問い合わせの際こお客様 の事象が確認できなくなり、適切なサポートが難しくなる場合がございます。

config system session-ttl
set default 600
config port
edit 1
set protocol 17
set timeout 10
set start-port 53
set end-port 53
next
end
end





以下オブジェクトとして追加しています。

FW ポリシー オブジェクト

アドレス	
OfficeA	203.0.113.0 (掲示用アドレス)
OfficeB	198.51.100.5 (掲示用アドレス)
Japan_Segment	日本アドレス(タイプ geography)
SuitePRO_NW	仮想UTM ネットワーク/29
NTTPC_Port_Monitoring	203.138.84.18
アドレスグループ	
Office	OfficeA,OfficeB
サービスグループ	
MAIL	POP3/IMAP/SMTP/Submission
	•

IPS プロファイル
IPS_Mail
IPS_DNS
IPS_HTTP
IPS_HTTPS
アンチウイルスプロファイル
AV_MAIL
AV_FTP
アンチスパムプロファイル
ANTISPAM
Web Application firewall プロファイル
default
セキュリティプロファイル
custom-default





FW ポリシー(1以外すべて無効化)

ID	名前	接続元	宛先	サービス	アクション	IPS	SSL インスペクシ ヨン	プロキシ
1	preset1	SuitePRO_NW	All	All	許可	なし	no-inspection	70-
2	preset1	NTTPC_Port_ Monitoring	SuitePRO_NW	All	許可	なし	no-inspection	70-
3	preset2	Office_Group	SuitePRO_NW	SSH	許可	なし	no-inspection	70-
4	preset3	Office_Group	SuitePRO_NW	RDP	許可	なし	no-inspection	70-
5	preset4	All	SuitePRO_NW	DNS	許可	なし	no-inspection	70-
6	preset5	All	SuitePRO_NW	HTTP	許可	なし	no-inspection	70-
7	preset6	All	SuitePRO_NW	HTTPS	許可	なし	no-inspection	プロキシ
8	preset7	All	SuitePRO_NW	MAIL	許可	なし	no-inspection	プロキシ

DoS ポリシー(すべて有効化)

ID	名前	接続元	宛先	サービス
1	preset1	port1	All	All
2	preset2	port2	All	All

