SSD-assistance
Server Specification Document Assistance

サーバー設定仕様書自動生成サービス『SSD-assistance』【生成サンプル】

1.本サンプルについて

本サンプルは、サーバー設定仕様書自動生成サービス『SSD-assistance』を使用して生成された編集可能な Microsoft Excel (.xlsx) 形式のファイルを、PDF化したものです。
実際に生成される設定仕様書は非常に情報量が多いため、繰り返しの部分などを一部省略しておりますが、出力される項目については全てご確認いただける内容となっております。

2.サーバー設定仕様書自動生成サービス『SSD-assistance』とは

セイ・テクノロジーズでは設定仕様書(パラメーターシート)を自動で作成するサービス『SSD-assistance』を提供しております。
詳しくはこちらをクリックしてください

3.お問い合わせ

SSD-assistanceに関するお問い合わせは、お気軽に以下のお問い合わせフォームからご連絡ください。
詳しくはこちらをクリックしてください

セイ・テクノロジーズ株式会社

SSD-assistance
Server Specification Document Assistance

『SSD-assistance』「FortiGate 設定仕様書」生成サンプルについて

1.FortiGate設定仕様書について

『SSD-assistance』が生成する「FortiGate 設定仕様書」は、VDOMの使用有無に関わらずご利用いただけます。
そのため、VDOMの使用状況に応じて生成される書式が異なります。

1.VDOMを使用しない構成の場合
「FortiGate 設定仕様書」が1ファイル生成されます。

2.VDOMを使用する構成の場合
「FortiGate Global 設定仕様書」が1ファイル、「FortiGate VDOM 設定仕様書」はVDOMの設定数に応じたファイルが生成されます。

2.目次

簡易セキュリティ設定チェック.....P.　3
FortiGate 設定仕様書 .....P. 10
FortiGate Global 設定仕様書.....P.110
FortiGate VDOM 設定仕様書.....P.155

セイ・テクノロジーズ株式会社

FortiGate 簡易セキュリティ設定チェック

簡易セキュリティ設定チェックについて

本チェックシートは、FortiGateのセキュリティ設定状況を確認するための参考情報として、一般的なセキュリティ観点を整理したものです。
本チェック結果は設定状況の一例を示すものであり、セキュリティの完全性や安全性を保証するものではありません。
実際の設定や運用にあたっては、お客様の環境やポリシー、最新の製品ドキュメント等を踏まえ、適切にご判断ください。
FortiGateを保護する機能および管理者を保護する機能を中心に、設定状況を確認するための参考情報としてチェック結果を表示します。

基本情報

確認日	2026/6/1 12:00
Alias	FortiGate-40F
ファームウェアバージョン	FGT40F-7.6.7-FW-build3704-260601

目次

チェック①　アカウントの管理
FortiGateの管理者アカウントおよび認証ポリシーの設定状況について確認します。
- **管理者アカウント名の変更**
- **パスワードポリシーの有効**

チェック②　管理アクセス
FortiGateの管理インターフェースへのアクセス制御および認証設定の状況について確認します。
- **USBインストール**
- **アクセス制御**
- **二要素認証**
- **ログイン免責事項**

チェック③　バージョン管理
FortiGateの管理インターフェースへのアクセス制御および認証設定の状況について確認します。
- **ファームウェア自動更新**
- **仮想パッチ**

チェック④　アクセスの抑制
未使用機能や不要なアクセス経路の無効化など、攻撃対象領域を減らすための設定状況を確認します。
- **使用していないインターフェースの無効化**
- **使用していないプロトコルの無効化**

◆商標
FortiGateおよびFortiGateの製品名は、Fortinet, Inc.の米国およびその他の国における商標または登録商標です。

・簡易セキュリティ設定チェックシート付きのデザインを選択すると、目次からチェック④までのシートが、「FortiGate 設定仕様書」および「FortiGate Global 設定仕様書」の先頭（設定仕様書表紙の

チェック①　アカウントの管理

管理者アカウント名の変更

FortiGateを含むネットワーク機器やセキュリティ機器は工場出荷された初期状態でadminという管理者アカウントが設定されています。
adminをそのまま使用し続けたり、別の管理アカウントを作成したのに削除せずに残すことによって、不正アクセスのリスクが高まります。
「admin」というアカウントが設定されている場合は項目の横は ● がついております。
該当の項目は設定内容を確認し、必要に応じて変更してください。
別の管理者アカウントにsuper_adminの管理者プロファイルを適用し、adminアカウントを削除をすることでセキュリティを強化できます。

名前	プロファイル	タイプ	コメント	
admin	super_admin	ローカル		●
guest_user01		ローカル		
guest_user02		ローカル		
guest_user03	admin_no_access	リモート		
guest_user04	admin_no_access			
guest_user05	admin_no_access	リモート+ワイルドカード		
manager	super_admin	ローカル		

パスワードポリシーの有効化

安易なパスワード（例：passw0rdなど）や推測されやすいパスワードは解読され不正アクセスされる危険があります。
パスワードポリシーにより、安全なパスワードの設定や定期的にパスワード変更を強制し、脆弱なパスワード設定を防ぎます。
初期設定ではパスワードポリシーはOff（制限なし）となっているため、パスワードポリシーを有効化し、最長文字や特殊文字の使用、
有効期限等を設定することを推奨します。
パスワードポリシーの設定が無効（disable）の場合、項目の横に ● がついております。設定内容を確認し、必要に応じて変更してください。
また、パスワード紛失時のリカバリーのため、定期的な設定バックアップを推奨します。

パスワードスコープ		●

チェック②　管理アクセス

USBインストール

一部のFortiGateではUSBポートがサポートされています。
様々な人が容易に物理的なアクセスができる状態で設置される場合、SBポートを無効化する事で物理セキュリティを強化できます。
USBインストールの設定が有効（enable）の場合、項目の横に ● がついております。設定内容を確認し、必要に応じて変更してください。

USB自動インストール	設定ファイルを検知を有効	enable	●
	ファームウェアを検知を有効	enable	●

アクセス制御

FortiGateに管理者で接続する通信を、管理者アカウント毎に制御できます。
信頼するホスト／ネットワークを登録した制御や通信プロトコルを制限することで、不正な接続を防ぐことができます。
「信頼されるホストにログインを制限」の設定が初期値の場合は ● がついております。
該当の項目は設定内容を確認し、必要に応じて変更してください。

信頼されるホストにログインを制限

ユーザー名	admin		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
	IPv6	::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●

ユーザー名	guest_user01		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
		0.0.0.0/0.0.0.0	●
	IPv6	::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
		::/0	●
	以下省略		●
			●
		::/0	●
		::/0	●

接続するプロトコルの設定

名前	wan

管理者アクセス	IPv4	■ HTTPS ■ HTTP ■ PING □ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
	IPv6	□ HTTPS □ HTTP ■ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続

名前		lan1
管理者アクセス	IPv4	□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □
	IPv6	□ □ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続

以下省略

二要素認証

FortiGateでは認証する管理者アカウント含め様々なアカウントに二要素認証が適用可能です。
管理者アカウントに二要素認証を使用する事で、パスワード漏洩に対して対策を講じる事ができるため、有効化を推奨します。
二要素認証の設定が無効（disable）の場合、項目の横に ● がついております。
該当の項目は設定内容を確認し、必要に応じて変更してください。

ユーザー名	admin		
二要素認証	設定	disable	●
	認証タイプ	disable	

ユーザー名	guest_user01		
二要素認証	設定	disable	●
	認証タイプ	disable	

ログイン免責事項

管理者アカウントでFortiGateにログインする前後に免責事項を表示できます。
免責事項に不正アクセスの禁止、刑法に関する内容を記載し、表示することで不正なログイン行為に対する抑止力になります。
ログイン免責事項の設定が無効（disable）の場合、項目の横に ● がついております。
該当の項目は設定内容を確認し、必要に応じて変更してください。

ログイン後の免責事項メッセージ	disable	●
ログイン前の免責事項メッセージ	disable	●

チェック③　バージョン管理

ファームウェア自動更新

脆弱性のリスクを低減するには、ソフトウェアを常に最新の状態に保ち、既知の脆弱性に対するパッチが適用されている必要があります。
FortiGateでは、最新のファームウェアがリリースされて利用可能になったときに、アップグレードの自動実行をスケジュールできます。
ファームウェア自動更新の設定が無効（disable）の場合、項目の横に ● がついております。
該当の項目は設定内容を確認し、必要に応じて変更してください。
ファームウェアアップグレード時はFortiGateの再起動が発生します。
FortiGateをHAクラスタで構成している場合は通信を中断することなくアップグレード可能です。
再起動による通信断の影響が懸念される場合はHAクラスタでの構成を推奨します。

パッチの自動アップグレード	disable	●

仮想パッチ

機器へのアクセスは特定の経路・ユーザー等に制限することに加え、脆弱性に対するパッチが適用されている状態にする必要があります。
FortiGateではローカルインポリシーによりファイアウォールポリシーを適用し、通信の制御ができます。
ポリシーに仮想パッチを有効にすることで、FortiGateに対する既知の脆弱性を悪用した不正アクセスをIPSエンジンで検知、
ブロックできます。
仮想パッチの設定が無効（disable）の場合、項目の横に ● がついております。
該当の項目は設定内容を確認し、必要に応じて変更してください。
仮想パッチは一部の脆弱性の悪用を軽減しますが、すべての脆弱性に対して有効ではありません。
仮想パッチが有効な脆弱性に対しては、緩和策として仮想パッチを実行しつつ、根本的な解決策として、
ファームウェアの最新化を推奨します。

着信インターフェース	仮想パッチ
lan	enable

チェック④　アクセスの抑止

使用していないインタフェースの無効化

使用していないインターフェースを無効にすることで、デバイスの攻撃対象領域を縮小することができます。
FortiGateのGUIへログインし、本チェック結果と照らし合わせて確認し、使用していないインターフェースは無効化してください。

ポート	状態	タイプ	IP設定
wan	up	physical	192.168.1.254 255.255.255.0
lan1	up	physical	
lan2	up	physical	
lan3	up	physical	192.168.1.10 255.255.255.0

以下省略

使用していないプロトコルの無効化

使用していないプロトコルを無効にすることで、攻撃者がFortiGateユニットに関する情報収集に利用する可能性のある通信を遮断します。
本チェック結果を確認し、不要なプロトコルは無効化してください。
また、本チェック対象以外のプロトコルについても、必要に応じて設定を確認してください。

確認対象プロトコル

プロトコル	説明
dhcp-relay-service	DHCPリレーを使用するインターフェースのみで有効にしてください。
pptp-client	インターフェースをPPTPクライアントとして動作させない場合は無効にしてください。
arpfoward	L3インターフェース（NATモード）を使用する場合は有効にします。
broadcast-forward	異なるネットワークセグメント間でブロードキャストトラフィックの転送を無効にします。
l2sforward	L3インターフェース（NATモード）を使用する場合は有効にします。
icmp-send-redirect	必要に応じてICMPリダイレクトを無効にできます。
icmp-accept-redirect	必要に応じてICMPリダイレクトを無効にできます。
vlanforward	L3インターフェース（NATモード）を使用する場合は有効にします。
stpforward	L3インターフェース（NATモード）を使用する場合は有効にします。
ident-accept	TCPポート113に対する応答を無効にします。
ipmac	IP/MACバッティングを無効にします。
netbios-forward	NetBIOSフォワードを無効にします。
security-mode	キャプティブポータル認証を無効にするには「none」に設定します。
device-identification	デバイスを検出する機能が不要なインターフェースに対して無効にします。
lldp-transmission	LLDPが必要なデバイスと接続される場合以外を除いて必要ありません。

物理インタフェース

ポート	wan					
プロトコル	状態	プロトコル	状態	プロトコル	状態
dhcp-relay-service	disable	icmp-send-redirect	enable	ipmac	disable
pptp-client	disable	icmp-accept-redirect	enable	netbios-forward	disable
arpfoward	enable	vlanforward	disable	security-mode	none
broadcast-forward	disable	stpforward	disable	device-identification	disable
l2sforward	disable	ident-accept	disable	lldp-transmission	vdom

ポート	lan1				
プロトコル	状態	プロトコル	状態	プロトコル	状態
dhcp-relay-service		icmp-send-redirect		ipmac	
pptp-client		icmp-accept-redirect		netbios-forward	
arpfoward		vlanforward		security-mode	
broadcast-forward		stpforward		device-identification	
l2sforward		ident-accept		lldp-transmission	

ポート	lan2				
プロトコル	状態	プロトコル	状態	プロトコル	状態
dhcp-relay-service		icmp-send-redirect		ipmac	
pptp-client		icmp-accept-redirect		netbios-forward	
arpfoward		vlanforward		security-mode	
broadcast-forward		stpforward		device-identification	
l2sforward		ident-accept		lldp-transmission	

ポート	lan3				
プロトコル	状態	プロトコル	状態	プロトコル	状態
dhcp-relay-service	disable	icmp-send-redirect	enable	ipmac	disable

pptp-client	disable	icmp-accept-redirect	enable	netbios-forward	disable
arpfoward	enable	vlanforward		ecurity-mode	none
broadcast-forward	disable	stpforward		evice-identification	disable
l2sforward	disable	ident-accept	disable	ndp-transmission	disable

以下省略

・本設定仕様書サンプルはFortiGate 40Fから採取した
"full-configuration"のファイルを使用して作成しております。
・一部固有のIPアドレスが記述された部分はマスクしております。

FortiGate 設定仕様書

仕様書商事 様

FortiGate ホスト名	FortiGate-40F
作成日	20YY年MM月DD日
作成者	セイ･テクノロジーズ

セイ･テクノロジーズ株式会社

(住所)

改訂履歴

版数	日付	内容	担当者

目次

1. システム（概要）

システムの設定、および管理者、管理者プロファイル、HA、SNMP、FortiGuard、表示機能設定の概要を記載しています。

2. システム（管理者）

システムの管理者の詳細を記載しています。

3. システム（管理者プロファイル）

システムの管理者プロファイルの詳細を記載しています。

4. システム（SNMP v1/v2c）

システムのSNMP v1/v2cの詳細を記載しています。

5. システム（SNMP v3）

システムのSNMP v3の詳細を記載しています。

6. ネットワーク（概要）

ネットワークのインターフェース、およびスタティックルートの概要、DNSを記載しています。

7. ネットワーク（物理インターフェース）

ネットワークの物理インターフェースの詳細を記載しています。

8. ネットワーク（インターフェース）

ネットワークの下記インターフェースの詳細を記載しています。
802.3ad アグリゲート
PPPoEインターフェース
SSL-VPNトンネル
VLAN
ハードウェアスイッチ
ループバックインターフェース
冗長インターフェース

9. ネットワーク（スタティックルート）

ネットワークのスタティックルートの詳細を記載しています。

10. ネットワーク（SD-WAN）（概要）

SD-WANゾーン、SD-WANルール、およびパフォーマンスSLAの概要を記載しています。

11. ネットワーク（SD-WAN ルール）

SD-WANルールの詳細を記載しています。

12. ネットワーク（SD-WAN パフォーマンスSLA）

パフォーマンスSLAの詳細を記載しています。

13. ポリシー&オブジェクト（概要）

ポリシー&オブジェクトのファイアウォールポリシー、およびアドレスグループ、アドレス、IPv6アドレステンプレート、サービス、スケジュール、DANTとバーチャルIP、IPプールの概要を記載しています。

14. ポリシー&オブジェクト（ファイアウォールポリシー）

ポリシー&オブジェクトのファイアウォールポリシーの詳細を記載しています。

15. ポリシー&オブジェクト（アドレス）

ポリシー&オブジェクトのアドレスグループ、およびアドレス、IPv6アドレステンプレートの詳細を記載しています。

16. ポリシー&オブジェクト（サービス）

ポリシー&オブジェクトのサービスの詳細を記載しています。

17. ポリシー&オブジェクト（バーチャルIP）

ポリシー&オブジェクトのバーチャルIPの詳細を記載しています。

18. ポリシー&オブジェクト（IPプール）

ポリシー&オブジェクトのIPプールの詳細を記載しています。

19. セキュリティプロファイル（アンチウイルス）

セキュリティプロファイルのアンチウイルスの詳細を記載しています。

20. セキュリティプロファイル（WEBフィルタ）

セキュリティプロファイルのWEBフィルタの詳細を記載しています。

21. 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）

セキュリティプロファイルのアプリケーションコントロールの詳細を記載しています。

22. セキュリティプロファイル（侵入防止）（概要）

セキュリティプロファイルの侵入防止の概要を記載しています。

23. セキュリティプロファイル（侵入防止）

セキュリティプロファイルの侵入防止の詳細を記載しています。

24. セキュリティプロファイル（SSL/SSHインスペクション）（概要）

セキュリティプロファイルのSSL/SSHインスペクションの概要を記載しています。

25. セキュリティプロファイル（SSL/SSHインスペクション）

セキュリティプロファイルのSSL/SSHインスペクションの詳細を記載しています。

26. VPN（概要）

IPsec VPN、およびSSL-VPNの概要を記載しています。

27. VPN（IPsecトンネル）

VPNのIPsecトンネルの詳細を記載しています。

28. VPN（ハブ&スポーク トポロジ）

ハブ＆スポーク トポロジのVPNに関連する設定の一つであるBGPについて記載しています。

29. VPN（SSL-VPN設定）

SSL-VPNの設定を記載しています。

30. VPN（SSL-VPNポータル）

VPNのSSL-VPNポータルの詳細を記載しています。

◆商標

FortiGateおよびFortiGateの製品名は、Fortinet, Inc.の米国およびその他の国における商標または登録商標です。

1. システム（概要）

機種情報

ファームウェアバージョン	FGT40F-7.4.7-FW-build2731-250120
Alias	FortiGate-40F

管理者

システム管理者

名前	プロファイル	タイプ	コメント
admin	super_admin	ローカル	
test_2	test_2	ローカル	
test04	admin_no_access	リモート	
test05_qauser	admin_no_access		
test06	admin_no_access	リモート+ワイルドカード	
manager	super_admin	ローカル	

REST API管理者

名前	プロファイル	コメント
test_3	test_1	
test_2	test_2	
test_1	test_1	

シングルサインオン管理者

名前	プロファイル
test_1	test_1

管理者プロファイル

プロファイル名	コメント
prof_admin	
test_1	
CLIcommand_on	
CLIcommand_off	
CLIcommand_custom-allon	
CLIcommand_custom-alloff	

設定

ホスト名		FortiGate-40F
システム時間		
タイムゾーン		Asia/Tokyo
時刻設定(NTP)	有効	enable
	サーバー選択	FortiGuard
	同期間隔 (分)	60
時刻設定(PTP)	有効	
	モード	
	遅延メカニズム	
	リクエスト間隔 (秒)	
	インターフェース	
デバイスをローカルNTPサーバとして設定		
リッスンするインターフェース		l2t.root
		lan
管理者設定		
HTTPポート		80
HTTPSへリダイレクト		enable
HTTPSポート		443
HTTPサーバー証明書		self-sign
SSHポート		22
Telnetポート		23
アイドルタイムアウト (分)		30
ACMEインターフェース		test_1
		test_25
シングルサインオン		
ファブリックSSO		

FortiCloud SSO	FortiCloud SSOを有効	disable
	Default admin profile	
パスワードポリシー		
パスワードスコープ		管理者
最小長		8
新規文字の最小文字数		0
キャラクタ要件	大文字	1
	小文字	1
	数字 (0-9)	1
	特殊文字	1
パスワード再利用を許可		enable
パスワード期限 (日)		90
ワークフローマネジメント		
設定保存モード		自動
タイムアウト時に元に戻す (秒)		
ポリシー変更サマリ		必須
ポリシーはデフォルトで期限切れです		enable
後に期限切れ(日)		30
設定表示		
言語		日本語
テーマ		jade
日付/時刻表示		ブラウザのタイムゾーン
VLANスイッチモード		disable
NGFWモード		プロファイルベース
セントラルNAT		disable
初期設定		
FortiConverter に設定ファイルの取得を許可する		disable
自動ファイルシステムチェック		enable
USB自動インストール	設定ファイルを検知を有効	enable
	設定ファイルを検知	fgt_system.conf
	ファームウェアを検知を有効	enable
	ファームウェアを検知	image.out
Eメールサービス		
SMTPサーバ		fortinet-xxxx.com
ポート		465
認証	認証を有効	disable
	ユーザー名	
セキュリティモード		smtps

HA

モード		アクティブ・アクティブ	
デバイスのプライオリティ		128	
優先度の効果を上げる		enable	
クラスタ設定			
グループID		0	
グループ名		test_2	
セッションピックアップ		disable	
モニタインターフェース		test_24	
		test_25	
ハートビートインターフェース			
インターフェース名		優先度	
lan3		136	
wan		90	
管理インターフェースの予約			
インターフェース	ゲートウエイ	IPv6ゲートウェイ	宛先サブネット

SNMP

システム情報	
SNMPエージェント	enable

説明	
ロケーション	
コンタクト情報	

SNMP v1/v2c

名前	クエリ	トラップ	ホスト	IPv6ホスト	イベント	ステータス
test_1	v1: enable v2: enable	v1: enable v2: enable	0.0.0.0/0.0.0.0, 0.0.0.1/255.255.255.255, 0.0.0.2/255.255.255.255, 0.0.0.3/255.255.255.255		40	disable
test_2	v1: disable v2: disable	v1: disable v2: disable	0.0.0.0/0.0.0.0, 0.0.0.1/255.255.255.255, 0.0.0.2/255.255.255.255, 0.0.0.3/255.255.255.255	fd00:xxxx:9d16::abcd/128, fd00:xxxx:9d16::abce/128	1	enable
test_ 3	v1: disable v2: enable	v1: disable v2: enable	0.0.0.0/0.0.0.0	fd00:xxxx:9d16::abcd/128	42	enable

SNMP v3

名前	セキュリティレベル	クエリ	トラップ	ホスト	IPv6ホスト	イベント	ステータス
test_2	プライベート	disable	enable	0.0.0.0, 0.0.0.0			disable
test_1	認証なし	enable	enable	0.0.0.0, 0.0.0.0, 0.0.0.0		41	disable
test_3	非プライベート	enable	disable	0.0.0.0, 0.0.0.0		21	disable
test_4	認証なし	disable	disable	0.0.0.0, 0.0.0.0	fd00:xxxx:9d16::abcd	1	enable
test_5	認証なし	enable	enable	192.10.20.0, 192.10.20.10	fd00:xxxx:9d16::abcd, fd00:xxxx:9d16::abce	41	enable

FortiGuard

FortiGuardアップデート		
スケジュールされたアップデート	有効	enable
	スケジュール	毎週
	曜日	月曜
	時間	午後 4時
IPSの品質を向上		enable
拡張IPSシグネチャパッケージを利用		enable
アンチウイルス PUP/PUA		enable
サーバロケーションの更新		米国のみ
フィルタリング		
Webフィルタキャッシュ	Webフィルタキャッシュの有効	enable
	キャッシュの有効期間(分)	60
Eメールフィルタキャッシュ	Eメールフィルタキャッシュの有効	enable
	キャッシュの有効期間(分)	30
FortiGuardフィルタリングサービス	プロトコル	https
	ポート	443

FortiGuardサーバをオーバライド	
サーバーアドレス	サーバータイプ
192.0.0.0	両方
xx::	フィルタリング
192.12.0.0	アンチウイルスとIPSのアップデート

表示機能設定

コア機能	(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります

IPsec VPN	enable	enable
IPv6	enable	disable
SSL-VPN	enable	disable
Wifiコントローラー	enable	enable
スイッチコントローラー	enable	enable
高度なルーティング	enable	enable
セキュリティ機能		
DNSフィルタ	enable	enable
Explicitプロキシ	disable	disable
Eメールフィルタ	enable	disable
Inline-CASB	enable	disable
Webアプリケーションファイアウォール	enable	disable
Webフィルタ	enable	enable
アプリケーションコントロール	enable	enable
アンチウイルス	enable	enable
エンドポイントコントロール		enable
ゼロトラストネットワークアクセス	disable	enable
データ漏洩対策	enable	disable
ビデオフィルタ	enable	enable
ファイルフィルタ	enable	enable
仮想パッチ	enable	disable
侵入防止	enable	enable
その他の機能		
DNSデータベース	enable	disable
DoSポリシー	enable	enable
Eメール収集	enable	disable
FortiExtender	enable	disable
FortiGate Cloud Sandbox	enable	disable
ICAP	enable	disable
Implicit Firewall ポリシー	enable	enable
Local Inポリシー	enable	disable
SD-WANインターフェース	enable	enable
SSL-VPNパーソナルブックマーク	enable	disable
SSL-VPNレルム	enable	disable
VoIP	enable	disable
アドバンストエンドポイントコントロール		disable
アプリケーション検知ベースのSD-WAN	enable	disable
トラフィックシェイピング	enable	enable
ポリシーの詳細オプション	enable	disable
ポリシーベース IPsec VPN	enable	disable
ポリシー免責事項	enable	disable
マルチキャストポリシー	enable	disable
ローカルアウトルーティング	enable	disable
ロードバランス	enable	disable
ワークフローマネジメント	enable	disable
ワイヤレス オープンセキュリティ	enable	disable
運用技術(OT)	enable	disable
脅威ウェイトトラッキング	enable	enable
高度なワイヤレス機能	enable	disable
差し替えメッセージグループ	enable	disable
証明書	enable	enable
動的なデバイスとOSの識別	enable	disable
複数インターフェースポリシー	enable	disable
名前なしポリシー許可	enable	disable

2. システム（管理者）

システム管理者

No. 1

ユーザー名		admin
タイプ		ローカルユーザ
コメント		
管理者プロファイル		super_admin
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 2

ユーザー名		test_2
タイプ		ローカルユーザ
コメント		
管理者プロファイル		test_2
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0

管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 3

ユーザー名		test_3
タイプ		ローカルユーザ
コメント		
管理者プロファイル		
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	192.112.0.0/255.240.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	test_1
		test_2

REST API管理者

No. 1

ユーザー名	test_3
コメント	
管理者プロファイル	test_1
APIキー	ENC SH11223344556677889900aabbccddeeffgghhiijjkkllmmnnooppqqrrsstt=
PKIグループ	tesst05_remoteusergroup
オリジン間リソース共有許可	
信頼されるホストにログインを制限	

No. 2

ユーザー名	test_2
コメント	
管理者プロファイル	test_2
APIキー	ENC
PKIグループ	
オリジン間リソース共有許可	https://192.0.2.0:80
信頼されるホストにログインを制限	

No. 3

ユーザー名	test_1
コメント	
管理者プロファイル	test_1

APIキー	ENC SH1122334455667788990 0aabbccddeeffgghhiijjkkllmmnnooppqqrrsstt=
PKIグループ	
オリジン間リソース共有許可	
信頼されるホストにログインを制限	2001:xxx::/128
	192.112.0.0/255.240.0.0
	2001:xxx::/128
	xxxx:a88::/128
	192.112.0.0/255.240.0.0
	192.112.1.0/255.240.0.0

SSO管理者

No. 1

ユーザー名	test_1
管理者プロファイル	test_1

No. 2

ユーザー名	test_2
管理者プロファイル	test_2

3. システム（管理者プロファイル）

No. 1

名前		prof_admin
コメント		
アクセス権限		
セキュリティファブリック		読み書き
FortiView		読み書き
ユーザー＆デバイス		読み書き
ファイアウォール		読み書き
	ポリシー	
	アドレス	
	サービス	
	スケジュール	
	その他	
ログ＆レポート		読み書き
	設定	
	データアクセス	
	レポートアクセス	
	脅威ウェイト	
ネットワーク		読み書き
	設定	
	パケットキャプチャ	
	ルーター	
システム		読み書き
	管理者ユーザ	
	FortiGuard更新	
	設定	
	メンテナンス	
セキュリティプロファイル		読み書き
	アンチウイルス	
	IPS	
	Webフィルタ	
	Eメールフィルタ	
	データ漏洩対策（データ漏えい防止）	
	ファイルフィルタ	
	アプリケーションコントロール	
	ICAP	
	VoIP	
	Webアプリケーションファイアウォール	
	DNSフィルタ	
	エンドポイントコントロール	
	ビデオフィルタ	
	仮想パッチ	
	Inline-CASB	
VPN		読み書き
Wifi＆スイッチ		読み書き
CLI診断コマンドの使用を許可（system-diagnostics）（FortiOS 7.4.1以前）		
CLIコマンドの使用を許可（FortiOS 7.4.2以降）	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		
アイドルタイムアウトのオーバーライド		disable
タイムアウトしない		
オフライン(分)		

No. 2

名前	test_1

コメント		
アクセス権限		
セキュリティファブリック		読み取り
FortiView		読み書き
ユーザー＆デバイス		読み取り
ファイアウォール		カスタム
	ポリシー	読み取り
	アドレス	読み書き
	サービス	読み取り
	スケジュール	読み書き
	その他	読み取り
ログ＆レポート		カスタム
	設定	読み取り
	データアクセス	読み書き
	レポートアクセス	読み取り
	脅威ウェイト	読み書き
ネットワーク		カスタム
	設定	読み取り
	パケットキャプチャ	読み書き
	ルーター	読み取り
システム		カスタム
	管理者ユーザ	読み取り
	FortiGuard更新	読み書き
	設定	読み取り
	メンテナンス	読み書き
セキュリティプロファイル		カスタム
	アンチウイルス	読み取り
	IPS	読み書き
	Webフィルタ	読み取り
	Eメールフィルタ	読み書き
	データ漏洩対策（データ漏えい防止）	なし
	ファイルフィルタ	読み書き
	アプリケーションコントロール	読み取り
	ICAP	読み書き
	VoIP	読み取り
	Webアプリケーションファイアウォール	読み書き
	DNSフィルタ	読み取り
	エンドポイントコントロール	読み書き
	ビデオフィルタ	読み取り
	仮想パッチ	なし
	Inline-CASB	なし
VPN		読み書き
Wifi＆スイッチ		読み取り
CLI診断コマンドの使用を許可（system-diagnostics）(FortiOS 7.4.1以前)		
CLIコマンドの使用を許可(FortiOS 7.4.2以降)	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		
アイドルタイムアウトのオーバーライド		enable
タイムアウトしない		enable
オフライン(分)		0

4. システム (SNMP v1v2c)

No. 1

コミュニティ名	test_1	
有効化済み	disable	
ホスト	IPアドレス	ホストタイプ
	0.0.0.0/0.0.0.0	クエリを受け入れトラップを送信する
	192.0.0.1/255.255.255.255	クエリのみ受け入れる
	192.0.0.2/255.255.255.255	トラップのみ送信する
	192.0.0.3/255.255.255.255	クエリを受け入れトラップを送信する
IPv6ホスト	IPアドレス	ホストタイプ
クエリ		
v1有効	enable	
ポート	161	
v2c有効	enable	
ポート	161	
トラップ		
v1有効	enable	
ローカルポート	162	
リモートポート	162	
v2c有効	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	enable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable
snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	disable	enable
APがアップ	enable	enable

APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

No. 2

コミュニティ名	test_2	
有効化済み	enable	
ホスト	IPアドレス	ホストタイプ
	0.0.0.0/0.0.0.0	クエリを受け入れトラップを送信する
	192.0.0.1/255.255.255.255	クエリのみ受け入れる
	192.0.0.2/255.255.255.255	トラップのみ送信する
	192.0.0.3/255.255.255.255	トラップのみ送信する
IPv6ホスト	IPアドレス	ホストタイプ
	fd00:xxxx:9d16::abcd/128	クエリを受け入れトラップを送信する
	fd00:xxxx:9d16::abce/128	クエリを受け入れトラップを送信する
クエリ		
v1有効	disable	
ポート	161	
v2c有効	disable	
ポート	161	
トラップ		
v1有効	disable	
ローカルポート	162	
リモートポート	162	
v2c有効	disable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	disable	enable
利用可能なメモリが不足	disable	enable
利用可能なログスペースが不足	disable	enable
インターフェースのIPアドレス変更	disable	enable
VPNトンネルがアップ	disable	enable
VPNトンネルがダウン	disable	enable
HAクラスタのステータスが変化	disable	enable
HAハートビートインターフェースの障害	disable	enable
IPSがアタックを検知	disable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	disable	enable
AVがオーバーサイズファイルを検知	disable	enable
AVがパターンに一致するファイルを検知	disable	enable
AVが断片化ファイルを検知	disable	enable
インターフェースIPの変更(FMトラップ)	disable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	disable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	disable	enable
HAクラスタメンバーがアップ	disable	enable
HAクラスタメンバーがダウン	disable	enable
エンティティ設定変更(RFC4133)	disable	enable
AVシステムがコンサーブモードへ移行	disable	enable

AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	disable	enable
AVがオーバーサイズファイルをブロック	disable	enable
IPSパッケージの更新	disable	enable
IPSネットワークバッファがフル	disable	enable
snmp-event::temperature-high	disable	enable
snmp-event::voltage-alert	disable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	disable	enable
FortiAnalyzerから切断	disable	enable
snmp-event::faz	disable	enable
APがアップ	disable	enable
APがダウン	disable	enable
FortiSwitchコントローラーセッションがアップ	disable	enable
FortiSwitchコントローラーセッションがダウン	disable	enable
ロードバランスリアルサーバがダウン	disable	enable
新しいデバイスを発見	disable	disable
CPU使用率が高いです。	disable	enable
DHCPアドレスの制限	disable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	disable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	disable	enable

No. 3

コミュニティ名	test_ 3	
有効化済み	enable	
ホスト	IPアドレス	ホストタイプ
	0.0.0.0/0.0.0.0	クエリを受け入れトラップを送信する
IPv6ホスト	IPアドレス	ホストタイプ
	fd00:xxxx:9d16::abcd/128	クエリを受け入れトラップを送信する
クエリ		
v1有効	disable	
ポート	161	
v2c有効	enable	
ポート	161	
トラップ		
v1有効	disable	
ローカルポート	162	
リモートポート	162	
v2c有効	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable

設定変更(FMトラップ)	enable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable
snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	enable	enable
APがアップ	enable	enable
APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	enable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

5. システム (SNMP v3)

No. 1

ユーザー名	test_2	
有効化済み	disable	
セキュリティレベル		
認証	プライベート	
認証アルゴリズム	sha	
暗号化アルゴリズム	aes	
ホスト		
IPアドレス	0.0.0.0	
	0.0.0.0	
IPv6ホスト		
IPアドレス		
クエリ		
有効化済み	disable	
ポート	161	
トラップ		
有効化済み	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	disable	enable
利用可能なメモリが不足	disable	enable
利用可能なログスペースが不足	disable	enable
インターフェースのIPアドレス変更	disable	enable
VPNトンネルがアップ	disable	enable
VPNトンネルがダウン	disable	enable
HAクラスタのステータスが変化	disable	enable
HAハートビートインターフェースの障害	disable	enable
IPSがアタックを検知	disable	enable
IPSがアノマリを検知	disable	enable
AVがウイルスを検知	disable	enable
AVがオーバーサイズファイルを検知	disable	enable
AVがパターンに一致するファイルを検知	disable	enable
AVが断片化ファイルを検知	disable	enable
インターフェースIPの変更(FMトラップ)	disable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	disable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	disable	enable
HAクラスタメンバーがアップ	disable	enable
HAクラスタメンバーがダウン	disable	enable
エンティティ設定変更(RFC4133)	disable	enable
AVシステムがコンサーブモードへ移行	disable	enable
AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	disable	enable
AVがオーバーサイズファイルをブロック	disable	enable
IPSパッケージの更新	disable	enable
IPSネットワークバッファがフル	disable	enable
snmp-event::temperature-high	disable	enable
snmp-event::voltage-alert	disable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	disable	enable
FortiAnalyzerから切断	disable	enable
snmp-event::faz	disable	enable
APがアップ	disable	enable
APがダウン	disable	enable
FortiSwitchコントローラーセッションがアップ	disable	enable
FortiSwitchコントローラーセッションがダウン	disable	enable

ロードバランスリアルサーバがダウン	disable	enable
新しいデバイスを発見	disable	disable
CPU使用率が高いです。	disable	enable
DHCPアドレスの制限	disable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	disable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	disable	enable

No. 2

ユーザー名	test_1	
有効化済み	disable	
セキュリティレベル		
認証	認証なし	
認証アルゴリズム		
暗号化アルゴリズム		
ホスト		
IPアドレス	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
IPv6ホスト		
IPアドレス		
クエリ		
有効化済み	enable	
ポート	161	
トラップ		
有効化済み	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable
設定変更(FMトラップ)	enable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	enable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable

snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	disable	enable
APがアップ	enable	enable
APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

6. ネットワーク（概要）

インターフェース

下表は次のインターフェースを記載しています。

802.3ad アグリゲート
トンネルインターフェース (PPPoEインターフェースのみ)
SSL-VPNトンネル
VLAN
ハードウェアスイッチ
ループバックインターフェース
冗長インターフェース
物理インターフェース

名前	エイリアス	タイプ	メンバー	IP/ネットマスク	ステータス	バーチャルドメイン	コメント
fortilink		802.3ad アグリゲート	a	192.1.2.254/255.255.255.0	有効化済み	root	
test_802.3ad_3	test_802.3ad_3	802.3ad アグリゲート		0.0.0.0/0.0.0.0	有効化済み	root	802.3ad test
Interface3		SSL-VPNトンネル			有効化済み	root	
dhcptest		VLAN			有効化済み	root	
Interface01	エイリアス	VLAN			有効化済み	root	
onearmtest	onearmtest01	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_1	test_1	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_11	test_11	VLAN		0.0.0.0/0.0.0.0	無効化済み	root	
test_23	test_23	VLAN		0.0.0.0/0.0.0.0	無効化済み	root	
VLAN_test_1	VLAN_test_1	VLAN		192.145.0.0/255.0.0.0	有効化済み	root	
VLAN_test_2	VLAN_test_2	VLAN			有効化済み	root	
lan		ハードウェアスイッチ	lan1, lan2	192.168.99.100/255.255.255.0	有効化済み	root	
loopback_test_3	loopback_test_3	ループバックインターフェース		0.0.0.0/0.0.0.0	有効化済み	root	
lan1		物理インターフェース			有効化済み	root	
lan2		物理インターフェース			有効化済み	root	
lan3	test	物理インターフェース		192.168.1.10/255.255.255.0	有効化済み	root	
modem		物理インターフェース			無効化済み	root	
wan	test	物理インターフェース		192.31.1.254/255.255.255.0	有効化済み	root	

DNS

プライマリDNSサーバー	192.45.45.45
セカンダリDNSサーバー	192.46.46.46
ローカルドメイン名	saytech
	saytech_2
DNSプロトコル	
DNS (UDP/53)	enable
TLS (TCP/853)	disable
HTTPS (TCP/443)	enable
SSL証明書	Fortinet_Factory_Backup
サーバホスト名	globalsdns.fortinet.net
	globalsdns2.fortinet.net
IPv6 DNS設定	
プライマリDNSサーバ	fd00:xxxx:9d16::abcd
セカンダリDNSサーバ	fd00:xxxx:9d16::abce

ダイナミックDNS

ドメイン	パブリックIPアドレスを使用	インターフェース
saytech.xxxx.com	enable	fortilink
		Interface01
		Interface2

xxxx.float-zone.com	disable	test_1

スタティックルート

IPv4

宛先	ゲートウェイIP	インターフェース	ステータス	コメント
0.0.0.0/0.0.0.0	192.168.99.2	lan	enable	
0.0.0.0/0.0.0.0		l2t.root	enable	
Adobe-Adobe.Experience.Cloud (ID: 917640)	0.0.0.0	test_1	enable	インターネットサービステスト
Amazon-AWS (ID: 393320)	192.168.99.1	lan	enable	インターネットサービステスト 2
0.0.0.0/0.0.0.0	192.168.99.2	test_1	enable	
Zuora-Web (ID: 4063233)	0.0.0.0	test_1	enable	
192.20.20.0/255.255.255.0	0.0.0.0	lan	enable	
サイト 2 _remote		サイト 2	enable	VPN: サイト 2 (Created by VPN wizard)
サイト 2 _remote			enable	VPN: サイト 2 (Created by VPN wizard)
N1_remote			enable	VPN: N1 (Created by VPN wizard)
xcvbnm_remote		xcvbnm	enable	VPN: xcvbnm (Created by VPN wizard)
xcvbnm_remote			enable	VPN: xcvbnm (Created by VPN wizard)
pojpoj,_remote		pojpoj,	enable	VPN: pojpoj, (Created by VPN wizard)
pojpoj,_remote			enable	VPN: pojpoj, (Created by VPN wizard)
サイト全埋_remote			enable	VPN: サイト全埋 (Created by VPN wizard)

IPv6

宛先	ゲートウェイIP	インターフェース	ステータス	コメント
12:xx::/128	12:xx::	test_1	enable	
12:xx::/128	12:xx::	test_1	enable	

7. ネットワーク（物理インターフェース）

本章では、一部の設定値を次の凡例に従い表記しています。

凡例

チェックボックス形式の設定値の表記

■：設定がenable（有効）になっていることを示しています。

□：設定がdisable（無効）になっていること、または未設定を示しています。

物理インターフェース

No. 1

名前		wan
エイリアス		test
タイプ		物理インターフェース
VRF ID		10
バーチャルドメイン		root
ロール		未定義
推定帯域幅	アップストリーム（kbps）	10
	ダウンストリーム（kbps）	10
アドレス		
アドレッシングモード		IPAMによる自動管理
IPAMによる自動管理 - ネットワークサイズ		256
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		10
PPPoE - 初期PADTタイムアウト		5
IP/ネットマスク		192.31.1.254/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
ワンスアームスニファー		
セキュリティプロファイル	アンチウイルス	
	Webフィルタ	
	アプリケーションコントロールセンサー	
	IPS	
	ファイルフィルタ	
ロギングオプション	許可トラフィックをログ	
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント		ID： プレフィックスヒント：
セカンダリIPアドレス		enable
IP/ネットマスク		管理者アクセス
		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING □ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ セキュリティファブリック接続
LLDP受信		VDOM設定を使用

LLDP送信	VDOM設定を使用
DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	

アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

No. 2

名前		lan1
エイリアス		
タイプ		物理インターフェース
VRF ID		
バーチャルドメイン		root
ロール		未定義
推定帯域幅	アップストリーム (kbps)	
	ダウンストリーム (kbps)	
アドレス		
アドレッシングモード		
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		
PPPoE - 初期PADTタイムアウト		
IP/ネットマスク		
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		
ワンスアームスニファー		
セキュリティプロファイル	アンチウイルス	
	Webフィルタ	
	アプリケーションコントロールセンサー	
	IPS	
	ファイルフィルタ	
ロギングオプション	許可トラフィックをログ	
IPv6アドレッシングモード		
IPv6アドレス/プレフィックス		
IPv6アドレスの自動設定		
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		
IP/ネットマスク	管理者アクセス	
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト	
管理者アクセス		
IPv4	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト	
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続	
LLDP受信		
LLDP送信		
DHCPサーバ (サーバモード)		
DHCPステータス		
アドレス範囲 (開始 - 終了)		-

ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)			
一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)					
一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	
Explicit Webプロキシ	
セキュリティモード	
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	
その他	
コメント	

ステータス	有効化済み

8. ネットワーク（インターフェース）

本章では次のインターフェースの詳細を記載しています。

802.3ad アグリゲート　　ハードウェアスイッチ
PPPoEインターフェース　　ループバックインターフェース
SSL-VPNトンネル　　冗長インターフェース
VLAN

本章では一部の設定値を次の凡例に従い表記しています。

凡例

チェックボックス形式の設定値の表記

■ : 設定がenable (有効)になっていることを示しています。

□ : 設定がenable (無効)になっていること、または未設定を示しています。

802.3ad アグリゲート

No. 1

名前		fortilink
エイリアス		
タイプ		802.3ad アグリゲート
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		a
ロール		未定義
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		IPAMによる自動管理
IPAMによる自動管理 - ネットワークサイズ		256
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		192.1.2.254/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		□ HTTPS　□ HTTP　□ PING　□ FMGアクセス □ SSH　□ SNMP　□ FTM □ RADIUSアカウンティング　□ セキュリティファブリック接続 □ スピードテスト
管理者アクセス		
IPv4		□ HTTPS　□ HTTP　■ PING　□ FMGアクセス □ SSH　□ SNMP　□ FTM □ RADIUSアカウンティング　■ セキュリティファブリック接続 □ スピードテスト
IPv6		□ HTTPS　□ HTTP　□ PING　□ FMGアクセス □ SSH　□ SNMP　□ セキュリティファブリック接続
LLDP受信		enable
LLDP送信		enable
DHCPサーバ (サーバモード)		

DHCPステータス	disable
アドレス範囲 (開始 - 終了)	-
ネットマスク	0.0.0.0
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	0.0.0.0
DNSサーバー	システムDNSと同じ
DNSサーバー (指定)	
リース時間 (秒)	604800
高度な設定	
タイプ	レギュラー
NTPサーバ	システムNTPと同じ
NTPサーバ (指定)	
無線コントローラー	指定
無線コントローラー (指定)	0.0.0.0
	0.0.0.0
	0.0.0.0
タイムゾーン	disable
次のブートストラップサーバ	0.0.0.0
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	

アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

No. 2

名前		test_802.3ad_3
エイリアス		test_802.3ad_3
タイプ		802.3ad アグリゲート
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		IPAMによる自動管理
IPAMによる自動管理 - ネットワークサイズ		65536
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		0.0.0.0/0.0.0.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		委任済
IPv6アドレス/プレフィックス		
IPv6アドレスの自動設定		
アイデンティティアソシエーション識別子		1
IPv6アップストリームインターフェース		test_802.3ad_3
IPv6サブネット		::/0
DHCPv6プレフィックス委任		enable
IAPDプレフィックスヒント	ID	プレフィックスヒント
	49	::/0
	2	::/0
	1	::/0
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
IPv6		■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ セキュリティファブリック接続
LLDP受信		enable
LLDP送信		enable
DHCPサーバ (サーバモード)		
DHCPステータス		enable
アドレス範囲 (開始 - 終了)		-
ネットマスク		255.255.0.0
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ		192.1.255.254
DNSサーバー		インターフェースIPと同じ
DNSサーバー (指定)		

リース時間 (秒)	604800
高度な設定	
タイプ	レギュラー
NTPサーバ	ローカル
NTPサーバ (指定)	
無線コントローラー	インターフェースIPと同じ
無線コントローラー (指定)	
タイムゾーン	disable
次のブートストラップサーバ	0.0.0.0
TFTPサーバ	192.123.123.0
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	::/0
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	test_802.3ad_3
サブネット	::/0
RDNSSサービス	指定
RDNSSサービス (指定)	xx:a1::
DHCPv6サーバ	
DHCPv6ステータス	enable
IPv6サブネット	::/0
DNSサービス	指定

委任済	アップストリームインターフェース	
指定	DNSサーバ	xx:a1::
		xx:a2::
		xx:a3::
		::

ステートフルサーバ - IPモード	IP範囲

IP範囲	アドレス範囲 (開始 - 終了)	-

ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	802.3ad test
ステータス	有効化済み

PPPoEインターフェース

設定はありません。

SSL-VPNトンネル

No. 1

名前		Interface3
エイリアス		
タイプ		SSL-VPNトンネル
VRF ID		0
バーチャルドメイン		root
インターフェース		lan
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
管理者アクセス		
IPv4		■ HTTPS ■ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 ■ スピードテスト
IPv6		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続
ネットワーク		
Explicit Webプロキシ		
セキュリティモード		
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		
ポータルメッセージのカスタマイズ		
送信元を除外		
宛先/サービスを除外		
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		
アウトバウンド帯域幅 (kbps)		10000
その他		
コメント		comment
ステータス		有効化済み

VLAN

No. 1

名前		Interface01
エイリアス		エイリアス
タイプ		VLAN
VRF ID		0
バーチャルドメイン		root
VLANプロトコル		802.1Q
インターフェース		fortilink
VLAN ID		1
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		DHCP
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1

PPPoE - 初期PADTタイムアウト	1
IP/ネットマスク	
サーバーからデフォルトゲートウェイを取得	enable
ディスタンス	5
内部DNSを上書き	enable
IPv6アドレッシングモード	マニュアル
IPv6アドレス/プレフィックス	::/0
IPv6アドレスの自動設定	disable
アイデンティティアソシエーション識別子	
IPv6アップストリームインターフェース	
IPv6サブネット	
DHCPv6プレフィックス委任	disable

IAPDプレフィックスヒント	ID	プレフィックスヒント

セカンダリIPアドレス	
IP/ネットマスク	管理者アクセス
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト

管理者アクセス

IPv4	■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続

DHCPサーバ (サーバモード)

DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	

高度な設定

タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)

リレーモード	disable
タイプ	
DHCPサーバIP	

ステートレスアドレス自動設定(SLAAC)

IPv6プレフィックス		
DHCPv6サーバ		
DHCPv6ステータス		
IPv6サブネット		
DNSサービス		
委任済	アップストリームインターフェース	
指定	DNSサーバ	
ステートフルサーバ - IPモード		
IP範囲	アドレス範囲 (開始 - 終了)	-
ネットワーク		
デバイスの検知		enable
Explicit Webプロキシ		
セキュリティモード		none
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		
ポータルメッセージのカスタマイズ		
送信元を除外		
宛先/サービスを除外		
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		Traffic Shaping Profile 1
アウトバウンド帯域幅 (kbps)		1000
その他		
コメント		コメント
ステータス		有効化済み

No. 2

名前		Interface2
エイリアス		
タイプ		VLAN
VRF ID		0
バーチャルドメイン		root
VLANプロトコル		802.1Q
インターフェース		wan
VLAN ID		2
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		DHCP
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		
サーバーからデフォルトゲートウェイを取得		enable
ディスタンス		5
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		

IP/ネットマスク	管理者アクセス
	□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □ スピードテスト

管理者アクセス	
IPv4	■ HTTPS ■ HTTP ■ PING □ FMGアクセス ■ SSH ■ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 ■ スピードテスト
IPv6	□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続

DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 アップストリームインターフェース	
指定 DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	enable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス ※ユーザーグループを指定しない場合は、すべて許可	

ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL) ※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

ハードウェアスイッチ

No. 1

名前		lan
エイリアス		
タイプ		ハードウェアスイッチ
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		lan1
		lan2
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		192.168.99.100/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ■ セキュリティファブリック接続 ☐ スピードテスト
IPv6		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
LLDP受信		VDOM設定を使用

LLDP送信	VDOM設定を使用
DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
STP	enable
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	

SPAN(ポートミラーリング)	
有効	enable
送信元ポート	lan2
宛先ポート	lan1
方向	両方
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

ループバックインターフェース

No. 1

名前		loopback_test_3
エイリアス		loopback_test_3
タイプ		ループバックインターフェース
VRF ID		0
バーチャルドメイン		root
ロール		WAN
推定帯域幅	アップストリーム (kbps)	27
	ダウンストリーム (kbps)	22
アドレス		
IP/ネットマスク		0.0.0.0 0.0.0.0
IPv6アドレス/プレフィックス		
IPv6アドレスの自動設定		
DHCPv6プレフィックス委任		
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		enable
IP/ネットマスク		管理者アクセス
0.0.0.0 0.0.0.0		■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
0.0.0.0 0.0.0.0		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □ スピードテスト
0.0.0.0 0.0.0.0		■ HTTPS □ HTTP □ PING □ FMGアクセス ■ SSH □ SNMP □ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
管理者アクセス		
IPv4		■ HTTPS □ HTTP ■ PING □ FMGアクセス ■ SSH □ SNMP □ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続
ネットワーク		
Explicit Webプロキシ		
セキュリティモード		キャプティブポータル
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		Guest-group
		test_1
ポータルメッセージのカスタマイズ		test_1
送信元を除外		Interface03 address

	Interface2 address
	test_11 address
宛先/サービスを除外	test_10 address
	test_1
	test_23 address
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	http://xxxx.com
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	85
その他	
コメント	ループバックインターフェース＆セカンドIPテスト
ステータス	有効化済み

No. 2

名前		loopback_test_4	
エイリアス		loopback_test_4	
タイプ		ループバックインターフェース	
VRF ID		10	
バーチャルドメイン		root	
ロール		LAN	
推定帯域幅	アップストリーム (kbps)	0	
	ダウンストリーム (kbps)	0	
アドレス			
IP/ネットマスク		192.155.1.0 255.255.0.0	
IPv6アドレス/プレフィックス			
IPv6アドレスの自動設定			
DHCPv6プレフィックス委任			
IAPDプレフィックスヒント		ID	プレフィックスヒント
セカンダリIPアドレス		disable	
IP/ネットマスク		管理者アクセス	
		☐ HTTPS　☐ HTTP　☐ PING　☐ FMGアクセス ☐ SSH　☐ SNMP　☐ FTM ☐ RADIUSアカウンティング　☐ セキュリティファブリック接続 ☐ スピードテスト	
管理者アクセス			
IPv4		■ HTTPS　■ HTTP　■ PING　☐ FMGアクセス ■ SSH　■ SNMP　■ FTM ■ RADIUSアカウンティング　■ セキュリティファブリック接続 ■ スピードテスト	
IPv6		■ HTTPS　■ HTTP　■ PING　■ FMGアクセス ■ SSH　■ SNMP　■ セキュリティファブリック接続	
ネットワーク			
Explicit Webプロキシ			
セキュリティモード		none	
認証ポータル (外部) ※指定しない場合はローカル			
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可			
ユーザーグループ			
ポータルメッセージのカスタマイズ			
送信元を除外			
宛先/サービスを除外			
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト			
トラフィックシェイピング			
アウトバウンドシェイピングプロファイル			
アウトバウンド帯域幅 (kbps)		0	
その他			
コメント			
ステータス		有効化済み	

冗長インターフェース

No. 1

名前		test_24
エイリアス		test_24
タイプ		冗長インターフェース
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		
ロール		DMZ
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		0.0.0.0/0.0.0.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ☐ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
LLDP受信		enable
LLDP送信		enable
DHCPサーバ (サーバモード)		
DHCPステータス		
アドレス範囲 (開始 - 終了)		-
ネットマスク		
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ		
DNSサーバー		
DNSサーバー (指定)		
リース時間 (秒)		
高度な設定		
タイプ		
NTPサーバ		
NTPサーバ (指定)		
無線コントローラー		

無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)			
一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)					
一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	qwertyuiop
ステータス	有効化済み

9. ネットワーク（スタティックルート）

IPv4

No. 1

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	
ゲートウェイアドレス		192.168.99.2
インターフェース		lan
アドミニストレーティブ・ディスタンス		255
コメント		
ステータス		enable
高度な設定		
プライオリティ		1

No. 2

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	
ゲートウェイアドレス		
インターフェース		l2t.root
アドミニストレーティブ・ディスタンス		255
コメント		
ステータス		enable
高度な設定		
プライオリティ		9999

No. 3

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	Adobe-Adobe.Experience.Cloud (ID: xxxx)
ゲートウェイアドレス		0.0.0.0
インターフェース		test_1
アドミニストレーティブ・ディスタンス		
コメント		インターネットサービステスト
ステータス		enable
高度な設定		
プライオリティ		

No. 4

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	Amazon-AWS (ID: xxxx)
ゲートウェイアドレス		192.168.99.99
インターフェース		lan
アドミニストレーティブ・ディスタンス		
コメント		インターネットサービステスト 2
ステータス		enable
高度な設定		
プライオリティ		

IPv6

No. 1

宛先	12:xx::/128
ゲートウェイアドレス	12:xx::
インターフェース	test_1
アドミニストレーティブ・ディスタンス	10
コメント	
ステータス	enable
高度な設定	
プライオリティ	1024

No. 2

宛先	12:xx::/128
ゲートウェイアドレス	12:xx::
インターフェース	test_1
アドミニストレーティブ・ディスタンス	20
コメント	
ステータス	enable
高度な設定	
プライオリティ	1050

10. SD-WAN（概要）

SD-WANゾーン

ゾーン	インタフェース	ゲートウェイ	IPv6ゲートウェイ	コスト	ステータス	プライオリティ
virtual-wan-link						
SD-WAN_zone1						
SD-WAN_zone	DHCPv6サーバ	0.0.0.0	::	0	有効	1
SD-WAN_zone2	test_01	0.0.0.0	::	1	有効	1
	test_02	0.0.0.0	::	0	無効	65535
	capture_vlan	0.0.0.0	::	3	有効	1

SD-WANルール

ID	名前	IPバージョン	送信元 ※1	宛先 ※1	基準	メンバー ※1	パフォーマンスSLA ※1	ポート	プロトコル	ステータス
1	SD-WAN_rule1	ipv4	xxxxx.xxx	xxxxx.xxx		test_8		開始： 1 終了： 65535	TCP	有効
2	SD-WAN_rule2	ipv4	xxxxx.xxx	all	latency	test_8, test_9	test_SLA	開始： 1 終了： 65535	UDP	無効
3	SD-WAN_rule3	ipv4	xxxxx.xxx	xxxxx.xxx	jitter	test_8	Default_FortiGuard	開始： 終了：	ANY	有効
4	SD-WAN_rule4	ipv6	xxxxx.xxx	xxxxx.xxx	packet-loss	test_9	test_SLA2	開始： 終了：	10	有効
5	SD-WAN_rule5	ipv6	xxxxx.xxx	xxxxx.xxx	inbandwidth	test_8, test_9	test_SLA4	開始： 終了：	ANY	有効

※1 記入欄に記載する設定値が多い場合は一部省略しています。

パフォーマンスSLA

名前	サーバ検知	インターフェース ※1	故障しきい値	リカバリしきい値
Default_DNS			5	10
Default_Office_365	xxxxx.xxx		5	10
Default_Gmail	xxxxx.xxx		5	10
Default_Google Search	xxxxx.xxx		5	10
Default_FortiGuard	xxxxx.xxx		5	10
test_SLA	xxxxx.xxx		5	5
test_SLA2	test	test_8	5	5
test_SLA3	test1, test2	test3, test4	5	5

※1 記入欄に記載する設定値が多い場合は一部省略しています。

11. SD-WAN（ルール）

暗黙のルール

ロードバランスアルゴリズム		usage-based		
メンバー	ウェイト	Ingress Spillover Threshold (kbps)	Egress Spillover Threshold (kbps)	Priority
test_3		16776000	4	1
test_4		10000	16776000	65535
capture_vlan		1	0	1
DHCPv6サーバ		10	1	1

プライオリティルール

No. 1

ID	1
名前	SD-WAN_rule1
ステータス	有効
IPバージョン	ipv4
送信元	
アドレス	xxxxx.xxx
ユーザグループ	01_remoteusergroup
宛先	
アドレス	xxxxx.xxx
プロトコル (※ 指定の場合はプロトコル番号を表示)	TCP
ポート範囲	1 - 65535
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	manual
インタフェースリファレンス	test_8
ゾーンプリファレンス	SD-WAN_zone1
計測されたSLA	
必要なSLAターゲット	
ロードバランシング	有効
クオリティ基準	
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	有効
転送DSCPタグ	000000
逆方向DSCP	有効
リバースDSCPタグ	000000

No. 2

ID	2
名前	SD-WAN_rule2
ステータス	無効
IPバージョン	ipv4
送信元	
アドレス	all
ユーザグループ	demo, test_2
宛先	

アドレス	all
プロトコル (※ 指定の場合はプロトコル番号を表示)	UDP
ポート範囲	1 - 65535
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_8
	test_9
ゾーンプリファレンス	SD-WAN_zone1, virtual-wan-link
計測されたSLA	test_SLA
必要なSLAターゲット	
ロードバランシング	
クオリティ基準	latency
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	無効
転送DSCPタグ	
逆方向DSCP	無効
リバースDSCPタグ	

No. 3

ID	3
名前	SD-WAN_rule3
ステータス	有効
IPバージョン	ipv4
送信元	
アドレス	login.xxxxx.xxx, Interface2 address, test_ダイナミック_ファブリック6, Microsoft Office 365
ユーザグループ	guest, vpnuser1, tesst02_remoteusergroup
宛先	
アドレス	wildcard.xxxxxxx.xxxx, Interface2 address, トンネル 1 サイト間_remote, サイト 3_remote
プロトコル (※ 指定の場合はプロトコル番号を表示)	ANY
ポート範囲	-
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_8
ゾーンプリファレンス	SD-WAN_zone1
計測されたSLA	Default_FortiGuard
必要なSLAターゲット	

ロードバランシング	
クオリティ基準	jitter
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	無効
転送DSCPタグ	
逆方向DSCP	無効
リバースDSCPタグ	

No. 4

ID	4
名前	SD-WAN_rule4
ステータス	有効
IPバージョン	ipv6
送信元	
アドレス	test1_IPv6_address_FQDN
ユーザグループ	test_ 3
宛先	
アドレス	SSLVPN_TUNNEL_IPv6_ADDR1
プロトコル (※ 指定の場合はプロトコル番号を表示)	10
ポート範囲	-
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	0x11
ビットマスク	0x12
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_9
ゾーンプリファレンス	testQA1
計測されたSLA	test_SLA2
必要なSLAターゲット	
ロードバランシング	
クオリティ基準	packet-loss
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	
転送DSCPタグ	
逆方向DSCP	
リバースDSCPタグ	

No. 5

ID	5
名前	SD-WAN_rule5
ステータス	有効
IPバージョン	ipv6
送信元	
アドレス	test2_IPv6, test_IPv6group
ユーザグループ	vpnuser1, tesst05_remoteusergroup
宛先	

アドレス	xxxxx.xxx
プロトコル (※ 指定の場合はプロトコル番号を表示)	ANY
ポート範囲	-
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_8
	test_9
ゾーンプリファレンス	SD-WAN_zone1, virtual-wan-link
計測されたSLA	test_SLA4
必要なSLAターゲット	
ロードバランシング	
クオリティ基準	inbandwidth
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	
転送DSCPタグ	
逆方向DSCP	
リバースDSCPタグ	

12. SD-WAN (パフォーマンスSLA)

No. 1

名前	Default_DNS		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル			
サーバ			
DNSサーバ	システムDNSと同じ		
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	1000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 2

名前	Default_Office_365		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	https		
サーバ	xxx.xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	120000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 3

名前	Default_Gmail		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	ping		
サーバ	xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	2
リンクステータス			
チェック間隔 (ms)	1000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 4

名前	Default_Google Search		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	https		
サーバ	xxx.xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	120000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 5

名前	Default_FortiGuard		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	https		
サーバ	xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	120000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

13. ポリシー&オブジェクト（概要）

ファイアウォールポリシー

名前	from ※1	to ※1	送信元（アドレス）※1	宛先（アドレス）※1	アクション
test01_FWpolicy	Interface03	loopback_test_3	IPv4: login.xxxx.com IPv6:	IPv4: login.xxxx.com IPv6:	許可
SSL-VPN-Access-Policy	ssl.root	lan	IPv4: SSLVPN_TUNNEL_ADDR1 IPv6:	IPv4: all IPv6:	許可
SSL-VPN-Access-Policy-New	ssl.root	lan	IPv4: SSLVPN_TUNNEL_ADDR1 IPv6:	IPv4: all IPv6:	許可
vpn_サイト2_local_0	test_24	サイト2	IPv4: サイト2_local IPv6:	IPv4: サイト2_remote IPv6:	許可
vpn_サイト2_remote_0	サイト2	test_24	IPv4: サイト2_remote IPv6:	IPv4: サイト2_local IPv6:	許可
vpn_サイト2_share_internet	サイト2	loopback_test_3	IPv4: サイト2_remote IPv6:	IPv4: all IPv6:	許可
vpn_xcvbnm_local_0	Interface2	xcvbnm	IPv4: xcvbnm_local IPv6:	IPv4: xcvbnm_remote IPv6:	許可
vpn_xcvbnm_remote_0	xcvbnm	Interface2	IPv4: xcvbnm_remote IPv6:	IPv4: xcvbnm_local IPv6:	許可
vpn_xcvbnm_share_internet	xcvbnm	loopback_test_3	IPv4: xcvbnm_remote IPv6:	IPv4: all IPv6:	許可
vpn_pojpoj,_local_0	test_24	pojpoj,	IPv4: pojpoj,_local IPv6:	IPv4: pojpoj,_remote IPv6:	許可
vpn_pojpoj,_remote_0	pojpoj,	test_24	IPv4: pojpoj,_remote IPv6:	IPv4: pojpoj,_local IPv6:	許可
vpn_pojpoj,_share_internet	pojpoj,	loopback_test_3	IPv4: pojpoj,_remote IPv6:	IPv4: all IPv6:	許可

※1 記入欄に記載する設定値が多い場合は一部省略しています。

アドレスグループ

IPv4グループ

名前	タイプ	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。	ルーティング可能
G Suite	グループ	xxxx.com wildcard.xxxx.com	
Microsoft Office 365	グループ	login.xxxx.com login.xxxx.com login.xxxx.net	
test1_IPv4group	フォルダ	FIREWALL_AUTH_PORTAL_ADDRESS SSLVPN_TUNNEL_ADDR1	
test1_IPv4_addressgroup	グループ		
test2_IPv4_addressgroup	グループ		enable
test3_IPv4_addressgroup	フォルダ		enable
トンネル1サイト間_local	グループ	トンネル1サイト間_local_subnet_1 トンネル1サイト間_local_subnet_2	enable
トンネル1サイト間_remote	グループ	トンネル1サイト間_remote_subnet_1 トンネル1サイト間_remote_subnet_2	enable
リモートアクセス1_split	グループ	dhcptest address	
サイト2_local	グループ		enable
サイト2_remote	グループ	サイト2_remote_subnet_1	enable
サイト3_local	グループ	サイト3_local_subnet_1	enable
サイト3_remote	グループ	サイト3_remote_subnet_1	enable
N1_local	グループ	N1_local_subnet_1	enable
N1_remote	グループ	N1_remote_subnet_1	enable
xcvbnm_local	グループ	xcvbnm_local_subnet_1	enable

xcvbnm_remote	グループ	xcvbnm_remote_subnet_1	enable
pojpoj,_local	グループ	pojpoj,_local_subnet_1	enable
pojpoj,_remote	グループ	pojpoj,_remote_subnet_1	enable

IPv6グループ

名前	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
test_IPv6group	SSLVPN_TUNNEL_IPv6_ADDR1
test2_IPv6group	SSLVPN_TUNNEL_IPv6_ADDR1 test2_IPv6 test_IPv6group

アドレス

アドレス

名前	タイプ	インターフェース	詳細	IP	コメント	ルーティング可能
EMS_ALL_UNKNOWN_CLIENTS	ダイナミック					
EMS_ALL_UNMANAGEABLE_CLIENTS	ダイナミック					
none	サブネット			0.0.0.0/255.255.255.255		disable
login.xxxx.com	FQDN		login.xxxx.com			disable
login.xxxx.com	FQDN		login.xxxx.com			disable
login.xxxx.net	FQDN		login.xxxx.net			disable
xxxxl.com	FQDN		xxxx.com			disable
wildcard.xxxx.com	FQDN		*.xxxx.com			disable
xxxx.com	FQDN		*.xxxx.com			disable
all	サブネット			0.0.0.0/0.0.0.0		disable
FIREWALL_AUTH_PORTAL_ADDRESS	サブネット			0.0.0.0/0.0.0.0		disable
FABRIC_DEVICE	サブネット			0.0.0.0/0.0.0.0	IPv4 addresses of Fabric Devices	
SSLVPN_TUNNEL_ADDR1	IP範囲			192.212.134.200 - 192.212.134.210		
lan	インターフェイス サブネット	lan		192.168.99.0/255.255.255.0		disable
FCTEMS_ALL_FORTICLOUD_SERVERS	ダイナミック					
Interface01 address	インターフェイス サブネット	Interface01		0.0.0.0/255.255.255.255		disable
Interface2 address	インターフェイス サブネット	Interface2		0.0.0.0/255.255.255.255		disable
Interface03 address	インターフェイス サブネット	Interface03		0.0.0.0/255.255.255.255		disable
test_1 address	インターフェイス サブネット	test_1		0.0.0.0/255.255.255.255		disable
test_IPMA_3 address	インターフェイス サブネット	test_IPMA_3		192.31.0.0/255.255.255.0		disable
VLAN_test_2 address	インターフェイス サブネット	VLAN_test_2		0.0.0.0/255.255.255.255		disable
VLAN_test_1 address	インターフェイス サブネット	VLAN_test_1		192.0.0.0/255.0.0.0		disable
test_802.3ad_3 address	インターフェイス サブネット	test_802.3ad_3		0.0.0.0/255.255.255.255		disable
test1_address	ジオグラフィ		JAPAN			

test1_IPv4_address_IPhani	IP範囲			192.123.0.0 - 192.123.0.10		
test_wildcard_address_1	ワイルドカード			192.168.0.56/255.255.0.255		
onearmtest address	インターフェイス サブネット	onearmtest		0.0.0.0/255.255.255.255		disable
dhcptest address	インターフェイス サブネット	dhcptest		0.0.0.0/255.255.255.255		disable
VPN_to_Opponent_local_subnet_1	サブネット			192.168.10.0/255.255.255.0		enable
VPN_to_Opponent_remote_subnet_1	サブネット			192.168.20.0/255.255.255.0		enable
IPsec_Tunnel_Pool	IP範囲			192.250.250.1 - 192.250.250.254		
トンネル１サイト間_local_subnet_1	サブネット			192.168.99.0/255.255.255.0		enable
トンネル１サイト間_remote_subnet_1	サブネット			192.20.20.0/255.255.255.0		enable
ハブアンドスポーク_local_subnet_1	サブネット			192.0.0.0/192.0.0.0		enable
リモートアクセス1_range	IP範囲			192.168.1.10 - 192.168.1.250	VPN: リモートアクセス1 (Created by VPN wizard)	
N1_local_subnet_1	サブネット			192.168.99.0/255.255.255.0		enable
xcvbnm_local_subnet_1	サブネット			192.168.8.0/255.255.252.0		enable
pojpoj,_local_subnet_1	サブネット			192.96.0.0/255.224.0.0		enable

IPv6アドレス

名前	タイプ	詳細	IP
SSLVPN_TUNNEL_IPv6_ADDR1	サブネット		fdff:xxxx::/120
all	サブネット		::/0
none	サブネット		::/128
test2_IPv6	IPv6範囲		xx:a1:: - xx:a10::
test1_IPv6_address_FQDN	FQDN	aaa.aa	
test1_IPv6_address_region	IPv6地域	JAPAN	
test1_IPv6_address_template	IPv6テンプレート	test1_IPv6_template	2001:xxx:0:cd30::/60
test1_IPv6_address_MAC	デバイス(MACアドレス)	"11:22:33:44:55:66" "00:11:22:33:44:55" "22:33:44:55:66:77"	
test2_IPv6_address_template	IPv6テンプレート	test2_IPv6_template	xxxx:db8:0:cd30::/60
test2_IPv6_address_MAC	デバイス(MACアドレス)	"00:11:22:33:44:55" "11:22:33:44:55:66" "22:33:44:55:66:77" "33:44:55:66:77:88-33:44:55:66:77:99"	
test20250312_geography_Japan	IPv6地域	JAPAN	
test20250312_geography_Bulgaria	IPv6地域	BULGARIA	
test20250312_geography_China	IPv6地域	CHINA	

マルチキャストアドレス

名前	タイプ	インターフェース	IP
all	マルチキャストIP範囲		192.0.0.0 - 192.255.255.255
all_hosts	マルチキャストIP範囲		192.0.0.1 - 192.0.0.1
all_routers	マルチキャストIP範囲		192.0.0.1 - 192.0.0.1
Bonjour	マルチキャストIP範囲		192.0.0.1 - 192.0.0.1
EIGRP	マルチキャストIP範囲		192.0.0.1 - 192.0.0.1
OSPF	マルチキャストIP範囲		192.0.0.1 - 192.0.0.1
test1_multiaddress	ブロードキャストサブネット		0.0.0.0 0.0.0.0

IPv6マルチキャストアドレス

名前	IPv6アドレス
all	xxxx::/8
test1_IPV6_multicast	xxxx::/8
test2_IPV6_multicast	xxxx::/8

IPv6アドレステンプレート

名前	IPv6アドレスプレフィックス
test1_IPv6_template	2001:xxx:0:cd30::/60
test2_IPv6_template	xxxx:db8:0:cd30::/60

サービス

名前	サービスタイプ	詳細				IP/FQDN	カテゴリ	プロトコル
		TCP	UDP	ICMP	SCTP			
ALL	ファイアフォール						一般	IP
FTP	ファイアフォール	21				0.0.0.0	file access	TCP/UDP/SCTP
FTP_GET	ファイアフォール	21				0.0.0.0	file access	TCP/UDP/SCTP
FTP_PUT	ファイアフォール	21				0.0.0.0	file access	TCP/UDP/SCTP
DNS	ファイアフォール	53	53			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
HTTP	ファイアフォール	80				0.0.0.0	web access	TCP/UDP/SCTP
HTTPS	ファイアフォール	443				0.0.0.0	web access	TCP/UDP/SCTP
IMAP	ファイアフォール	143				0.0.0.0	Eメール	TCP/UDP/SCTP
IMAPS	ファイアフォール	993				0.0.0.0	Eメール	TCP/UDP/SCTP
LDAP	ファイアフォール	389				0.0.0.0	認証	TCP/UDP/SCTP
DCE-RPC	ファイアフォール	135	135			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
POP3	ファイアフォール	110				0.0.0.0	Eメール	TCP/UDP/SCTP
POP3S	ファイアフォール	995				0.0.0.0	Eメール	TCP/UDP/SCTP
SAMBA	ファイアフォール	139				0.0.0.0	file access	TCP/UDP/SCTP
SMTP	ファイアフォール	25				0.0.0.0	Eメール	TCP/UDP/SCTP
SMTPS	ファイアフォール	465				0.0.0.0	Eメール	TCP/UDP/SCTP
KERBEROS	ファイアフォール	88 464	88 464			0.0.0.0	認証	TCP/UDP/SCTP
LDAP_UDP	ファイアフォール		389			0.0.0.0	認証	TCP/UDP/SCTP
SMB	ファイアフォール	445				0.0.0.0	file access	TCP/UDP/SCTP
ALL_TCP	ファイアフォール	1-65535				0.0.0.0	一般	TCP/UDP/SCTP
ALL_UDP	ファイアフォール		1-65535			0.0.0.0	一般	TCP/UDP/SCTP
ALL_ICMP	ファイアフォール						一般	ICMP
ALL_ICMP6	ファイアフォール						一般	ICMP6
GRE	ファイアフォール						tunneling	IP
AH	ファイアフォール						tunneling	IP
ESP	ファイアフォール						tunneling	IP
AOL	ファイアフォール	5190-5194				0.0.0.0		TCP/UDP/SCTP
BGP	ファイアフォール	179				0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
DHCP	ファイアフォール		67-68			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
FINGER	ファイアフォール	79				0.0.0.0		TCP/UDP/SCTP
GOPHER	ファイアフォール	70				0.0.0.0		TCP/UDP/SCTP
H323	ファイアフォール	1720 1503	1719			0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
IKE	ファイアフォール		500 4500			0.0.0.0	tunneling	TCP/UDP/SCTP
Internet-Locator-Service	ファイアフォール	389				0.0.0.0		TCP/UDP/SCTP
IRC	ファイアフォール	6660-6669				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
L2TP	ファイアフォール	1701	1701			0.0.0.0	tunneling	TCP/UDP/SCTP
NetMeeting	ファイアフォール	1720				0.0.0.0		TCP/UDP/SCTP
NFS	ファイアフォール	111 2049	111 2049			0.0.0.0	file access	TCP/UDP/SCTP
NNTP	ファイアフォール	119				0.0.0.0		TCP/UDP/SCTP

NTP	ファイアフォール	123	123			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
OSPF	ファイアフォール						ネットワークサービス	IP
PC-Anywhere	ファイアフォール	5631	5632			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
PING	ファイアフォール						ネットワークサービス	ICMP
TIMESTAMP	ファイアフォール							ICMP
INFO_REQUEST	ファイアフォール							ICMP
INFO_ADDRESS	ファイアフォール							ICMP
ONC-RPC	ファイアフォール	111	111			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
PPTP	ファイアフォール	1723				0.0.0.0	tunneling	TCP/UDP/SCTP
QUAKE	ファイアフォール		26000 27000 27910 27960			0.0.0.0		TCP/UDP/SCTP
RAUDIO	ファイアフォール		7070			0.0.0.0		TCP/UDP/SCTP
REXEC	ファイアフォール	512				0.0.0.0		TCP/UDP/SCTP
RIP	ファイアフォール		520			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
RLOGIN	ファイアフォール	513:512-1023				0.0.0.0		TCP/UDP/SCTP
RSH	ファイアフォール	514:512-1023				0.0.0.0		TCP/UDP/SCTP
SCCP	ファイアフォール	2000				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
SIP	ファイアフォール	5060	5060			0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
SIP-MSNmessenger	ファイアフォール	1863				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
SNMP	ファイアフォール	161-162	161-162			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
SSH	ファイアフォール	22				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
SYSLOG	ファイアフォール		514			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
TALK	ファイアフォール		517-518			0.0.0.0		TCP/UDP/SCTP
TELNET	ファイアフォール	23				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
TFTP	ファイアフォール		69			0.0.0.0	file access	TCP/UDP/SCTP
MGCP	ファイアフォール		2427 2727			0.0.0.0		TCP/UDP/SCTP
UUCP	ファイアフォール	540				0.0.0.0		TCP/UDP/SCTP
VDOLIVE	ファイアフォール	7000-7010				0.0.0.0		TCP/UDP/SCTP
WAIS	ファイアフォール	210				0.0.0.0		TCP/UDP/SCTP
WINFRAME	ファイアフォール	1494 2598				0.0.0.0		TCP/UDP/SCTP
X-WINDOWS	ファイアフォール	6000-6063				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
PING6	ファイアフォール							ICMP6
MS-SQL	ファイアフォール	1433 1434				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
MYSQL	ファイアフォール	3306				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
RDP	ファイアフォール	3389				0.0.0.0	リモートアクセス	TCP/UDP/SCTP

VNC	ファイアフォール	5900				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
DHCP6	ファイアフォール		546 547			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
SQUID	ファイアフォール	3128				0.0.0.0	tunneling	TCP/UDP/SCTP
SOCKS	ファイアフォール	1080	1080			0.0.0.0	tunneling	TCP/UDP/SCTP
WINS	ファイアフォール	1512	1512			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
RADIUS	ファイアフォール		1812 1813			0.0.0.0	認証	TCP/UDP/SCTP
RADIUS-OLD	ファイアフォール		1645 1646			0.0.0.0		TCP/UDP/SCTP
CVSPSERVER	ファイアフォール	2401	2401			0.0.0.0		TCP/UDP/SCTP
AFS3	ファイアフォール	7000-7009	7000-7009			0.0.0.0	file access	TCP/UDP/SCTP
TRACEROUTE	ファイアフォール		33434-33535			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
RTSP	ファイアフォール	554 7070 8554	554			0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
MMS	ファイアフォール	1755	1024-5000			0.0.0.0		TCP/UDP/SCTP
NONE	ファイアフォール	0				0.0.0.0		TCP/UDP/SCTP
webproxy	Explicitプロキシ	0-65535:0-65535				0.0.0.0	web proxy	ALL

スケジュール

繰り返し

名前	日	時間 (開始と終了どちらも"00:00"の場合は"終日"です。)	
		開始	終了
always	日曜, 月曜, 火曜, 水曜, 木曜, 金曜, 土曜	00:00	00:00
none	none	00:00	00:00
default-darrp-optimize	日曜, 月曜, 火曜, 水曜, 木曜, 金曜, 土曜	01:00	01:30

ワンタイム

名前	開始日	終了日	有効期限切れ前イベントログ	期限までの日数
onetime_test	00:00 2024/10/09	00:00 2024/10/29	disable	0

スケジュールグループ

名前	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
test_schedule_01	onetime_test always default-darrp-optimize none onetime_test_2
test_schedule_02	always

バーチャルIP

IPv4

名前	インターフェース	マッピング元	マッピング先	ステータス
test1_IPv4_IP	test_1	192.123.0.0	192.123.0.0 xxx:a1::	
test2_IPv4_FQDN	any	xxxx.com	xxxx.com	
TestVirtualIp_20250225_01	any	123.111.111.111	xxxx.com	

IPv6

名前	マッピング元	マッピング先	
		IPv4アドレス/範囲	IPv6アドレス/範囲
test1_IPv6	123:a1::	disable	124:b1::
test1_IPv6	123:a1::	disable	124:b1::
test1_IPv6	123:a1::	disable	124:b1::

IPv4 バーチャルIPグループ

名前	インターフェース	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
test1_IPv4_VIP	fortilink	test2_IPv4_FQDN
VIPgroup_02	test_10	test2_IPv4_FQDN

IPv6 バーチャルIPグループ

名前	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
VIPgroup_IPv6_01VIPgroup_02	test1_IPv6
VIPgroup_IPv6_02VIPgroup_02	test1_IPv6 test1_IPv6_2

IPプール

IPv4

名前	外部IP範囲	タイプ	ARPリプライ
test1_IPv4	192.123.0.0 - 192.123.0.0	オーバーロード	enable
test2_IPv4	192.123.0.0 - 192.123.0.0	1対1	enable
test3_IPv4	192.123.0.0 - 192.123.0.0	固定ポート範囲	enable
test4_IPv4	192.123.0.0 - 192.123.0.0	ポートをブロック割り当て	disable

IPv6

名前	外部IP範囲
test1_IPv6	xx:a1:: - xx:a10::
test2_IPv6	xxxx:a1:: - xxxx:a1::
test3_IPv6	xxxx:a11:: - xxxx:a100::

14. ポリシー&オブジェクト（ファイアウォールポリシー）

No. 1

ID	1
名前	test01_FWpolicy
着信インターフェース	Interface03
発信インターフェース	loopback_test_3
送信元	
アドレス (IPv4)	login.xxxx.com
アドレス (IPv6)	
ユーザー	
ユーザーグループ	
インターネットサービス	
IPv6インターネットサービス	
送信元の無効化 (送信元をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
IP/MACベースアクセスコントロール	
宛先	
アドレス (IPv4)	login.xxxx.com
アドレス (IPv6)	
インターネットサービス	
IPv6インターネットサービス	
宛先の無効化 (宛先をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
スケジュール	always
サービス	ALL
アクション	許可
インスペクションモード	
プロキシHTTP(S) トラフィック	
ファイアウォール/ネットワークオプション	
NAT / NAT46 / NAT64	NAT
プロトコルオプション	default
免責事項オプション	
免責事項を表示	disable
ブロック通知	disable
認証メッセージをカスタマイズ	
セキュリティプロファイル	
アンチウイルス	
Webフィルタ	
ビデオフィルタ	
DNSフィルタ	
アプリケーションコントロール	
IPS	
ファイルフィルタ	
Eメールフィルタ	
VoIP	
ICAP	
Webアプリケーションファイアウォール	
DLPプロファイル	
SSLインスペクション	custom-deep-inspection
復号トラフィックミラー	
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
違反トラフィックをログ	utm
高度な設定	

WCCP	disable
キャプティブポータルから除外	disable
ワークフローマネジメント	
ポリシーの有効期限	enable
有効期限日	2025-03-27 18:29:00
コメント	
このポリシーを有効化	enable

No. 2

ID	4
名前	SSL-VPN-Access-Policy
着信インターフェース	ssl.root
発信インターフェース	lan
送信元	
アドレス (IPv4)	SSLVPN_TUNNEL_ADDR1
アドレス (IPv6)	
ユーザー	
ユーザーグループ	tesst04_remoteusergroup
	tesst05_remoteusergroup
インターネットサービス	
IPv6インターネットサービス	
送信元の無効化 (送信元をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
IP/MACベースアクセスコントロール	
宛先	
アドレス (IPv4)	all
アドレス (IPv6)	
インターネットサービス	
IPv6インターネットサービス	
宛先の無効化 (宛先をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
スケジュール	always
サービス	ALL
アクション	許可
インスペクションモード	
プロキシHTTP(S) トラフィック	
ファイアウォール/ネットワークオプション	
NAT / NAT46 / NAT64	disable
プロトコルオプション	default
免責事項オプション	
免責事項を表示	
ブロック通知	disable
認証メッセージをカスタマイズ	
セキュリティプロファイル	
アンチウイルス	
Webフィルタ	
ビデオフィルタ	
DNSフィルタ	
アプリケーションコントロール	
IPS	
ファイルフィルタ	
Eメールフィルタ	
VoIP	
ICAP	

Webアプリケーションファイアウォール	
DLPプロファイル	
SSLインスペクション	no-inspection
復号トラフィックミラー	
ロギングオプション	
許可トラフィックをログ	すべてのセッション
違反トラフィックをログ	all
高度な設定	
WCCP	disable
キャプティブポータルから除外	
ワークフローマネジメント	
ポリシーの有効期限	disable
有効期限日	
コメント	
このポリシーを有効化	enable

15. ポリシー&オブジェクト（アドレス）

IPv4 アドレスグループ

No. 1

グループ名	G Suite
タイプ	グループ
メンバー	xxxx.com
	wildcard.xxxx.com
メンバーの除外	disable
メンバーの除外 メンバー	
スタティックルート設定	
コメント	

No. 2

グループ名	Microsoft Office 365
タイプ	グループ
メンバー	login.xxxx.com
	login.xxxx.com
	login.xxxx.com
メンバーの除外	disable
メンバーの除外 メンバー	
スタティックルート設定	
コメント	

IPv6 アドレスグループ

No. 1

グループ名	test_IPv6group
メンバー	SSLVPN_TUNNEL_IPv6_ADDR1
コメント	test_IPv6group

No. 2

グループ名	test2_IPv6group
メンバー	SSLVPN_TUNNEL_IPv6_ADDR1
	test2_IPv6
	test_IPv6group
コメント	

IPv4 アドレス

No. 1

名前	EMS_ALL_UNKNOWN_CLIENTS
タイプ	ダイナミック
IP/ネットマスク	
IP範囲	
FQDN	
IP/ワイルドカードマスク	
国/地域	
サブタイプ	ems-tag
SPT(System Posture Token)	
FSSOグループ	
MACアドレス	
インターフェース	
スタティックルート設定	
コメント	

No. 2

名前	EMS_ALL_UNMANAGEABLE_CLIENTS
タイプ	ダイナミック
IP/ネットマスク	
IP範囲	
FQDN	
IP/ワイルドカードマスク	
国/地域	

サブタイプ	ems-tag
SPT(System Posture Token)	
FSSOグループ	
MACアドレス	
インターフェース	
スタティックルート設定	
コメント	

IPv6 アドレス

No. 1

名前	SSLVPN_TUNNEL_IPv6_ADDR1	
タイプ	サブネット	
IPv6アドレス	fdff:xxxx::/120	
IP範囲		
FQDN		
国/地域		
IPv6アドレステンプレート		
サブネットプレフィックス		
セグメント名	タイプ	値
ホストタイプ		
ホスト		
MACアドレス		
コメント		

No. 2

名前	all	
タイプ	サブネット	
IPv6アドレス	::/0	
IP範囲		
FQDN		
国/地域		
IPv6アドレステンプレート		
サブネットプレフィックス		
セグメント名	タイプ	値
ホストタイプ		
ホスト		
MACアドレス		
コメント		

No. 3

名前	none	
タイプ	サブネット	
IPv6アドレス	::/128	
IP範囲		
FQDN		
国/地域		
IPv6アドレステンプレート		
サブネットプレフィックス		
セグメント名	タイプ	値
ホストタイプ		
ホスト		
MACアドレス		
コメント		

IPv4 マルチキャストアドレス

No. 1

名前	all
タイプ	マルチキャストIP範囲

マルチキャストIP範囲	192.0.0.0 - 192.255.255.255
ブロードキャストサブネット	
インターフェース	
コメント	

No. 2

名前	all_hosts
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.1 - 192.0.0.1
ブロードキャストサブネット	
インターフェース	
コメント	

No. 3

名前	all_routers
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.2 - 192.0.0.2
ブロードキャストサブネット	
インターフェース	
コメント	

No. 4

名前	Bonjour
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.251 - 192.0.0.251
ブロードキャストサブネット	
インターフェース	
コメント	

No. 5

名前	EIGRP
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.10 - 192.0.0.10
ブロードキャストサブネット	
インターフェース	
コメント	

No. 6

名前	OSPF
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.5 - 192.0.0.6
ブロードキャストサブネット	
インターフェース	
コメント	

IPv6マルチキャストアドレス

No. 1

名前	all
IPv6アドレス	ff00::/8
コメント	

IPv6アドレステンプレート

No. 1

名前	test1_IPv6_template
IPv6アドレスプレフィックス	2001:xxx:0:cd30::/60

サブネットセグメント

セグメント名	ビット	排他	定義された値
country	4	disable	0x4
			0b0111
state	4	disable	
city	4	disable	
site	4	disable	

lan	4	disable	
vlan	4	disable	

No. 2

名前		test2_IPv6_template	
IPv6アドレスプレフィックス		2001:xxx:0:cd30::/60	
サブネットセグメント			
セグメント名	ビット	排他	定義された値
country	4	disable	0b0011
state	4	disable	
city_test_1	4	enable	0b0011
site_test_1	4	disable	0b0111
lan	4	disable	
vlan_test_4	4	enable	0b0111

16. ポリシー&オブジェクト（サービス）

No. 1

名前		ALL
サービスタイプ		ファイアフォール
コメント		
カテゴリ		一般
プロトコルオプション		
プロトコルタイプ		IP
タイプ		
コード		
アドレス	IP範囲	
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 2

名前		FTP
サービスタイプ		ファイアフォール
コメント		
カテゴリ		file access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
21		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 3

名前		FTP_GET
サービスタイプ		ファイアフォール
コメント		
カテゴリ		file access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
21		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 4

名前		FTP_PUT
サービスタイプ		ファイアフォール
コメント		
カテゴリ		file access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
21		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 5

名前		DNS
サービスタイプ		ファイアフォール
コメント		
カテゴリ		ネットワークサービス
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
53		
宛先ポート(UDP)		
宛先ポート		送信元ポート
53		
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 6

名前		HTTP
サービスタイプ		ファイアフォール
コメント		
カテゴリ		web access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
80		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 7

名前		HTTPS
サービスタイプ		ファイアフォール
コメント		
カテゴリ		web access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
443		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

17. ポリシー&オブジェクト（バーチャルIP）

IPv4

No. 1

名前			test1_IPv4_IP
コメント			
ステータス			
ネットワーク			
	インターフェース		test_1
	タイプ		スタティックNAT
	送信元インターフェースフィルタ		
	スタティックNAT	外部IPアドレス/範囲	192.123.0.0
		マップ	
		IPv4アドレス/範囲	192.123.0.0
		IPv6アドレス/範囲	xxx:a1::
	FQDN	外部 IP	
		外部 FQDN	
		マップされたアドレス	
オプションのフィルタ			
	送信元アドレス		192.123.123.0
			192.123.123.1
	サービス		"ALL_ICMP" "ALL_TCP" "test1_IP"
ポートフォワード			
	ポートフォワードが有効		enable
	プロトコル		
	ポートマッピングタイプ		
	外部サービスポート		
	IPv4ポートへマップ		65535
	IPv6ポートへマップ		65535

No. 2

名前			test2_IPv4_FQDN
コメント			
ステータス			
ネットワーク			
	インターフェース		any
	タイプ		FQDN
	送信元インターフェースフィルタ		
	スタティックNAT	外部IPアドレス/範囲	
		マップ	
		IPv4アドレス/範囲	
		IPv6アドレス/範囲	
	FQDN	外部 IP	0.0.0.0
		外部 FQDN	xxxx.com
		マップされたアドレス	xxxx.com
オプションのフィルタ			
	送信元アドレス		
	サービス		
ポートフォワード			
	ポートフォワードが有効		enable
	プロトコル		udp
	ポートマッピングタイプ		多対多
	外部サービスポート		65535
	IPv4ポートへマップ		65535
	IPv6ポートへマップ		

IPv6

No. 1

名前	test1_IPv6

コメント	
ネットワーク	
外部IPアドレス/範囲	xxx:a1::
マップ	
IPv6アドレス/範囲	xxx:b1::
IPv4アドレス/範囲	disable
オプションのフィルタ	
送信元アドレス	xxx:c1::
	xxx:d1::
	xxx:b1::
ポートフォワード	
ポートフォワードが有効	enable
プロトコル	tcp
外部サービスポート	65535
IPv6ポートへマップ	65535
IPv4ポートへマップ	65535

IPv4 バーチャルIPグループ

No. 1

名前	test1_IPv4_VIP
コメント	
インターフェース	fortilink
メンバー	test2_IPv4_FQDN

IPv6 バーチャルIPグループ

No. 1

名前	VIPgroup_IPv6_01
コメント	
メンバー	test1_IPv6

18. ポリシー&オブジェクト（IPプール）

IPv4

No. 1

名前	test1_IPv4
コメント	
タイプ	オーバーロード
外部IP範囲	192.123.0.0 - 192.123.0.0
ブロックサイズ	
Internal IP範囲	
ユーザあたりのブロック	
ユーザあたりのポート	
NAT64	enable
ARP リプライ	enable

No. 2

名前	test2_IPv4
コメント	
タイプ	1対1
外部IP範囲	192.123.0.0 - 192.123.0.0
ブロックサイズ	
Internal IP範囲	
ユーザあたりのブロック	
ユーザあたりのポート	
NAT64	
ARP リプライ	enable

No. 3

名前	test3_IPv4
コメント	
タイプ	固定ポート範囲
外部IP範囲	192.123.0.0 - 192.123.0.5
ブロックサイズ	
Internal IP範囲	192.123.0.0 - 192.123.0.5
ユーザあたりのブロック	
ユーザあたりのポート	32
NAT64	
ARP リプライ	enable

No. 4

名前	test4_IPv4
コメント	
タイプ	ポートをブロック割り当て
外部IP範囲	192.123.0.0 - 192.123.0.7
ブロックサイズ	568
Internal IP範囲	
ユーザあたりのブロック	111
ユーザあたりのポート	
NAT64	disable
ARP リプライ	disable

IPv6

No. 1

名前	test1_IPv6
コメント	
外部IP範囲	xx:a1:: - xx:a10::
NAT46	disable

No. 2

名前	test2_IPv6
コメント	
外部IP範囲	xxxx:a1:: - xxxx:a1::
NAT46	enable

No. 3

名前	test3_IPv6
コメント	
外部IP範囲	xxxx:a11:: - xxxx:a100::
NAT46	disable

19. セキュリティプロファイル（アンチウイルス）

No. 1

名前	default
コメント	Scan files and block viruses.
機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	disable	disable	—	
SMTP	ブロック	disable	disable	enable	
POP3	ブロック	disable	disable	enable	
IMAP	ブロック	disable	disable	enable	
FTP	ブロック	disable	disable	—	—
CIFS	disable	disable	disable	—	—
MAPI					—
SSH				—	—

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

No. 2

名前	sniffer-profile
コメント	Scan files and monitor viruses.

機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	モニタ	enable	ー	
SMTP	ブロック	モニタ	enable	enable	
POP3	ブロック	モニタ	enable	enable	
IMAP	ブロック	モニタ	enable	enable	
FTP	ブロック	モニタ	enable	ー	ー
CIFS	disable	disable	disable	ー	ー
MAPI					ー
SSH				ー	ー

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

20. セキュリティプロファイル (WEBフィルタ)

No. 1

名前	default
コメント	Default web filtering.
機能セット	フローベース

FortiGuardカテゴリベースのフィルタ

ID	グループ	カテゴリ名	アクション
12	g01 Potentially Liable	Extremist Groups	ブロック
2	g02 Adult/Mature Content	Alternative Beliefs	ブロック
7	g02 Adult/Mature Content	Abortion	ブロック
8	g02 Adult/Mature Content	Other Adult Materials	ブロック
9	g02 Adult/Mature Content	Advocacy Organizations	ブロック
11	g02 Adult/Mature Content	Gambling	ブロック
13	g02 Adult/Mature Content	Nudity and Risque	ブロック
14	g02 Adult/Mature Content	Pornography	ブロック
15	g02 Adult/Mature Content	Dating	ブロック
16	g02 Adult/Mature Content	Weapons (Sales)	ブロック
57	g02 Adult/Mature Content	Marijuana	ブロック
63	g02 Adult/Mature Content	Sex Education	ブロック
64	g02 Adult/Mature Content	Alcohol	ブロック
65	g02 Adult/Mature Content	Tobacco	ブロック
66	g02 Adult/Mature Content	Lingerie and Swimsuit	ブロック
67	g02 Adult/Mature Content	Sports Hunting and War Games	ブロック
26	g05 Security Risk	Malicious Websites	ブロック
61	g05 Security Risk	Phishing	ブロック
86	g05 Security Risk	Spam URLs	ブロック
88	g05 Security Risk	Dynamic DNS	ブロック
90	g05 Security Risk	Newly Observed Domain	ブロック
91	g05 Security Risk	Newly Registered Domain	ブロック
0	g21 Unrated	Unrated	ブロック

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	
オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分

サーチエンジン

Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	

スタティックURLフィルタ

無効なURLをブロック	
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック	disable
コンテンツフィルタ	

パターンタイプ	パターン	言語	アクション	ステータス

レーティングオプション

Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)	
ドメインまたはIPアドレスでURLをレーティング	

プロキシオプション

HTTP POST アクション	許可
Javaアプレットを削除	
ActiveXの削除	
Cookieを削除	

No. 2

名前	sniffer-profile
コメント	Monitor web traffic.
機能セット	フローベース

FortiGuardカテゴリベースのフィルタ

ID	グループ	カテゴリ名	アクション
1	g01 Potentially Liable	Drug Abuse	モニタ
3	g01 Potentially Liable	Hacking	モニタ
4	g01 Potentially Liable	Illegal or Unethical	モニタ
5	g01 Potentially Liable	Discrimination	モニタ
6	g01 Potentially Liable	Explicit Violence	モニタ
12	g01 Potentially Liable	Extremist Groups	モニタ
59	g01 Potentially Liable	Proxy Avoidance	モニタ
62	g01 Potentially Liable	Plagiarism	モニタ
83	g01 Potentially Liable	Child Sexual Abuse	モニタ
96	g01 Potentially Liable	Terrorism	モニタ
98	g01 Potentially Liable	Crypto Mining	モニタ
99	g01 Potentially Liable	Potentially Unwanted Program	モニタ
2	g02 Adult/Mature Content	Alternative Beliefs	モニタ
7	g02 Adult/Mature Content	Abortion	モニタ
8	g02 Adult/Mature Content	Other Adult Materials	モニタ
9	g02 Adult/Mature Content	Advocacy Organizations	モニタ
11	g02 Adult/Mature Content	Gambling	モニタ
13	g02 Adult/Mature Content	Nudity and Risque	モニタ
14	g02 Adult/Mature Content	Pornography	モニタ
15	g02 Adult/Mature Content	Dating	モニタ
16	g02 Adult/Mature Content	Weapons (Sales)	モニタ
57	g02 Adult/Mature Content	Marijuana	モニタ
63	g02 Adult/Mature Content	Sex Education	モニタ
64	g02 Adult/Mature Content	Alcohol	モニタ
65	g02 Adult/Mature Content	Tobacco	モニタ
66	g02 Adult/Mature Content	Lingerie and Swimsuit	モニタ
67	g02 Adult/Mature Content	Sports Hunting and War Games	モニタ
19	g04 Bandwidth Consuming	Freeware and Software Downloads	モニタ
24	g04 Bandwidth Consuming	File Sharing and Storage	モニタ
25	g04 Bandwidth Consuming	Streaming Media and Download	モニタ
72	g04 Bandwidth Consuming	Peer-to-peer File Sharing	モニタ
75	g04 Bandwidth Consuming	Internet Radio and TV	モニタ
76	g04 Bandwidth Consuming	Internet Telephony	モニタ
26	g05 Security Risk	Malicious Websites	モニタ
61	g05 Security Risk	Phishing	モニタ
86	g05 Security Risk	Spam URLs	モニタ
88	g05 Security Risk	Dynamic DNS	モニタ
90	g05 Security Risk	Newly Observed Domain	モニタ
91	g05 Security Risk	Newly Registered Domain	モニタ
17	g06 General Interest - Personal	Advertising	モニタ
18	g06 General Interest - Personal	Brokerage and Trading	モニタ
20	g06 General Interest - Personal	Games	モニタ
23	g06 General Interest - Personal	Web-based Email	モニタ
28	g06 General Interest - Personal	Entertainment	モニタ
29	g06 General Interest - Personal	Arts and Culture	モニタ
30	g06 General Interest - Personal	Education	モニタ
33	g06 General Interest - Personal	Health and Wellness	モニタ
34	g06 General Interest - Personal	Job Search	モニタ
35	g06 General Interest - Personal	Medicine	モニタ
36	g06 General Interest - Personal	News and Media	モニタ

37	g06 General Interest - Personal	Social Networking	モニタ
38	g06 General Interest - Personal	Political Organizations	モニタ
39	g06 General Interest - Personal	Reference	モニタ
40	g06 General Interest - Personal	Global Religion	モニタ
42	g06 General Interest - Personal	Shopping	モニタ
44	g06 General Interest - Personal	Society and Lifestyles	モニタ
46	g06 General Interest - Personal	Sports	モニタ
47	g06 General Interest - Personal	Travel	モニタ
48	g06 General Interest - Personal	Personal Vehicles	モニタ
54	g06 General Interest - Personal	Dynamic Content	モニタ
55	g06 General Interest - Personal	Meaningless Content	モニタ
58	g06 General Interest - Personal	Folklore	モニタ
68	g06 General Interest - Personal	Web Chat	モニタ
69	g06 General Interest - Personal	Instant Messaging	モニタ
70	g06 General Interest - Personal	Newsgroups and Message Boards	モニタ
71	g06 General Interest - Personal	Digital Postcards	モニタ
77	g06 General Interest - Personal	Child Education	モニタ
78	g06 General Interest - Personal	Real Estate	モニタ
79	g06 General Interest - Personal	Restaurant and Dining	モニタ
80	g06 General Interest - Personal	Personal Websites and Blogs	モニタ
82	g06 General Interest - Personal	Content Servers	モニタ
85	g06 General Interest - Personal	Domain Parking	モニタ
87	g06 General Interest - Personal	Personal Privacy	モニタ
89	g06 General Interest - Personal	Auction	モニタ
31	g07 General Interest - Business	Finance and Banking	モニタ
41	g07 General Interest - Business	Search Engines and Portals	モニタ
43	g07 General Interest - Business	General Organizations	モニタ
49	g07 General Interest - Business	Business	モニタ
50	g07 General Interest - Business	Information and Computer Security	モニタ
51	g07 General Interest - Business	Government and Legal Organizations	モニタ
52	g07 General Interest - Business	Information Technology	モニタ
53	g07 General Interest - Business	Armed Forces	モニタ
56	g07 General Interest - Business	Web Hosting	モニタ
81	g07 General Interest - Business	Secure Websites	モニタ
84	g07 General Interest - Business	Web-based Applications	モニタ
92	g07 General Interest - Business	Charitable Organizations	モニタ
93	g07 General Interest - Business	Remote Access	モニタ
94	g07 General Interest - Business	Web Analytics	モニタ
95	g07 General Interest - Business	Online Meeting	モニタ
97	g07 General Interest - Business	URL Shortening	モニタ
100	g07 General Interest - Business	Artificial Intelligence Technology	モニタ
101	g07 General Interest - Business	Cryptocurrency	モニタ
0	g21 Unrated	Unrated	モニタ

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	
オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分

サーチエンジン

Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	

スタティックURLフィルタ

無効なURLをブロック	

URLフィルタ					
URL	タイプ	アクション	ステータス		
FortiSandboxにより検知された悪意のあるURLをブロック		disable			
コンテンツフィルタ					
パターンタイプ	パターン	言語	アクション	ステータス	
レーティングオプション					
Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)					
ドメインまたはIPアドレスでURLをレーティング					
プロキシオプション					
HTTP POST アクション		許可			
Javaアプレットを削除					
ActiveXの削除					
Cookieを削除					

No. 3

名前		wifi-default	
コメント		Default configuration for offloading WiFi traffic.	
機能セット		フローベース	
FortiGuardカテゴリベースのフィルタ			
ID	グループ	カテゴリ名	アクション
12	g01 Potentially Liable	Extremist Groups	ブロック
2	g02 Adult/Mature Content	Alternative Beliefs	ブロック
7	g02 Adult/Mature Content	Abortion	ブロック
8	g02 Adult/Mature Content	Other Adult Materials	ブロック
9	g02 Adult/Mature Content	Advocacy Organizations	ブロック
11	g02 Adult/Mature Content	Gambling	ブロック
13	g02 Adult/Mature Content	Nudity and Risque	ブロック
14	g02 Adult/Mature Content	Pornography	ブロック
15	g02 Adult/Mature Content	Dating	ブロック
16	g02 Adult/Mature Content	Weapons (Sales)	ブロック
57	g02 Adult/Mature Content	Marijuana	ブロック
63	g02 Adult/Mature Content	Sex Education	ブロック
64	g02 Adult/Mature Content	Alcohol	ブロック
65	g02 Adult/Mature Content	Tobacco	ブロック
66	g02 Adult/Mature Content	Lingerie and Swimsuit	ブロック
67	g02 Adult/Mature Content	Sports Hunting and War Games	ブロック
26	g05 Security Risk	Malicious Websites	ブロック
61	g05 Security Risk	Phishing	ブロック
86	g05 Security Risk	Spam URLs	ブロック
88	g05 Security Risk	Dynamic DNS	ブロック
90	g05 Security Risk	Newly Observed Domain	ブロック
91	g05 Security Risk	Newly Registered Domain	ブロック
0	g21 Unrated	Unrated	ブロック
カテゴリ使用クォータ			
カテゴリ		クォータ合計	
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			
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を有効			
オーバーライドできるグループ			
プロファイル名			
切り替え先		ユーザ	
切り替え期間 モード		事前定義	
切り替え期間		15分	
サーチエンジン			
Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制			
YouTubeへのアクセスを制限する			

すべての検査キーワードをログ	
スタティックURLフィルタ	
無効なURLをブロック	enable
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック	disable
コンテンツフィルタ	

パターンタイプ	パターン	言語	アクション	ステータス

レーティングオプション	
Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)	
ドメインまたはIPアドレスでURLをレーティング	
プロキシオプション	
HTTP POST アクション	許可
Javaアプレットを削除	disable
ActiveXの削除	disable
Cookieを削除	disable

21. 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）

No. 1

名前		block-high-risk
コメント		
ネットワークプロトコルの強制		disable
ポート	プロトコルの強制	違反アクション

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細			アクション
1	アプリケーション (ID):			ブロック
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:	P2P (2), Proxy (6)	
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	
2	アプリケーション (ID):			許可
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:		
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	disable
DNSトラフィックの許可とログ	enable
HTTPベースアプリケーションの差し替えメッセージ	enable

No. 2

名前		test1_applicationcontrol_monitor
コメント		
ネットワークプロトコルの強制		enable
ポート	プロトコルの強制	違反アクション
21	http ssh telnet ftp dns smtp pop3 imap snmp nntp https	モニタ
22	http dns	ブロック

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細	アクション

1	アプリケーション (ID):		38614, 29025, 17534, 17535, 52798, 16284, 16616, 35760, 34742, 44606, 44607, 38923, 17045, 16554, 23345, 35963, 42324, 16413, 31529, 30220, 25379, 44391, 31030, 25939, 36983, 16313, 1, 15819, 24256, 28887, 17168, 31374, 16078, 34647, 16688, 16620, 16240, 16410, 45998, 16692, 26617, 36666, 17038, 16398, 38993, 38995, 38994, 23217, 42902, 43286, 25959, 36481, 26886, 30156, 27754, 36931, 32257, 36975, 36953, 36960, 35982, 35983, 35984, 16683, 26806, 15951, 30061, 43928, 31252, 25238, 38100, 39107, 32165, 33238, 23662, 16789, 16491, 52516, 30169, 44033, 32343, 43713, 27210, 37172, 36740, 35944, 47432, 47433, 56258, 56259, 56260, 51269, 43349, 45138, 48970, 46289, 38075, 45300, 26875, 35598 26873, 16492, 28046, 38540, 17840, 49555, 31605, 46934, 54312, 45628, 47772, 38266, 39164, 40123, 37518, 38981, 38997, 36718, 43468, 24305, 37591, 38109, 35151, 35229, 41680, 39243, 37619, 42662, 16171, 38900, 46178, 25953, 25903, 38547, 31498, 27508, 33383, 30074	隔離 有効期限(364日23時間59分)
	フィルター	ビヘイビア:		
		アプリケーションカテゴリ:		
		ポピュラリティ:		
		プロトコル:		
		リスク:		
		テクノロジー:		
		ベンダー:		
2	アプリケーション (ID):		38614, 29025, 17534, 17535, 52798, 16284, 16616	ブロック
	フィルター	ビヘイビア:		
		アプリケーションカテゴリ:		
		ポピュラリティ:		
		プロトコル:		
		リスク:		
		テクノロジー:		
		ベンダー:		
3	アプリケーション (ID):		30796, 18119, 30098, 28843, 17419, 47964, 53799, 53798, 109051910, 54708, 54701, 54700, 54702, 53580, 16638, 42806, 48692, 35824, 16858, 17020, 30159, 46402, 46403, 46405, 46404, 46406, 39541, 52515, 11933, 51247, 43590, 38768, 35163, 37659, 37676, 17459, 36313, 35421, 44019, 35420, 38542, 38959, 38960, 38975, 38974, 38958, 30127, 38778, 17039, 45464, 45465, 52075, 46931, 38337, 31019, 16235, 16389, 16241, 16404, 45686, 39101, 16312, 25886, 16403, 36185, 40269	許可
	フィルター	ビヘイビア:		
		アプリケーションカテゴリ:		
		ポピュラリティ:		
		プロトコル:		
		リスク:		
		テクノロジー:		
		ベンダー:		

	4	アプリケーション (ID):	38614, 29025, 17534, 17535, 52798, 16284, 16616, 35760, 34742, 44606, 44607, 38923, 17045, 16554, 23345, 35963, 42324, 16413, 31529, 30220, 25379, 44391, 31030, 25939, 36983, 16313, 1, 15819, 24256, 28887, 17168, 31374, 16078, 34647, 16688, 16620, 16240, 16410, 45998, 16692, 26617, 36666, 17038, 16398, 38993, 38995, 38994, 23217, 42902, 43286, 25959, 36481, 26886, 30156, 27754, 36931, 32257, 36975, 36953, 36960, 35982, 35983, 35984, 16683, 26806, 15951, 30061, 43928, 31252, 25238, 38100, 39107, 32165, 33238, 23662, 16789, 16491, 52516, 30169, 44033, 32343, 43713, 27210, 37172, 36740, 35944, 47432, 47433, 56258, 56259, 56260, 51269, 43349, 45138, 48970, 46289, 38075, 45300, 26875, 35598 26873, 16492, 28046, 38540, 17840, 49555, 31605, 46934, 54312, 45628, 47772, 38266, 39164, 40123, 37518, 38981, 38997, 36718, 43468, 24305, 37591, 38109, 35151, 35229, 41680, 39243, 37619, 42662, 16171, 38900, 46178, 25953, 25903, 38547, 31498, 27508, 33383, 30074, 12183, 11768, 48454, 31251, 30340, 26563, 36933, 36468, 20922, 26583, 27507, 55579, 36891, 36596, 16425, 43465, 39546, 35202, 48798, 51546, 31989, 42831, 24265, 50444, 36205, 30238, 16062, 34244, 16237, 50758, 35928, 16701, 28622, 16311, 16665, 16250, 16377, 52120, 24735, 16189, 24924, 35800, 38990, 38991, 38992, 26193, 39484, 35972, 35981, 35977, 16784, 33881, 31079, 37722, 23432, 39062, 34927, 38005, 31279, 31281, 42904, 16086 42297, 36576, 36577, 36578, 17521, 35968, 35969, 35971, 39071, 28885, 26286, 45760, 40766, 16653, 48964, 44306, 53243, 28889, 16664, 32357, 53352, 31910, 17482, 41601, 6, 36557, 44289, 25649, 52685, 17042, 38732, 43691, 29307, 31104, 36139, 46764, 30073, 30079, 36217, 43967, 38063, 52118, 17731, 50800, 35584, 35586, 43966, 35585, 38654, 27238, 36134, 38952, 34816, 17573, 25833, 16234, 16365, 25471, 16675, 16243, 16613, 17048, 38350, 43425, 39380, 18090, 17049, 16663, 16374, 16373, 38247, 39102, 16451, 16452, 30175, 37084, 16610, 16075, 25907, 16955, 39350, 50736, 48425, 16153, 53531, 50137, 34301, 37706, 44422, 36410, 54505, 37536, 16220, 38324, 29610, 35459, 16985, 33000, 29867, 34339 27948, 43356, 21114, 33178, 41954, 16067, 34859, 34736, 55810, 39676, 16646, 39651, 26185, 25282, 42300, 39684, 30274, 48062, 36574, 25952, 26628, 50719, 32259, 15962, 30165, 16416, 26821, 16666, 37166, 39244, 47578, 33661, 43597, 30090, 20923, 35814, 35812, 47957, 46938, 36460, 46158, 50413, 32641, 28588, 16338, 37585, 27147, 16282, 16254, 16287, 16436, 16387, 16214, 28198, 34616, 34517, 34516, 34515, 34514, 34512, 34507, 34506, 34505, 34503, 16993, 16994, 16195, 47816, 50869, 39624, 17763, 31496, 12634, 33704, 10357, 43707, 24923, 16310, 37050, 52427, 16072, 26035, 25242, 28125, 36136, 42500, 38966, 16625, 16450, 16349, 16040, 31160, 46837, 46832, 30796, 18119, 30098, 28843, 17419, 47964	許可

53799, 53798, 109051910, 54708, 54701, 54700, 54702, 53580, 16638, 42806, 48692, 35824, 16858, 17020, 30159, 46402, 46403, 46405, 46404, 46406, 39541, 52515, 11933, 51247, 43590, 38768, 35163, 37659, 37676, 17459, 36313, 35421, 44019, 35420, 38542, 38959, 38960, 38975, 38974, 38958, 30127, 38778, 17039, 45464, 45465, 52075, 46931, 38337, 31019, 16235, 16389, 16241, 16404, 45686, 39101, 16312, 25886, 16403, 36185, 40269, 16614, 33764, 35764, 35763, 17165, 37197, 36302, 27314, 36790, 47681, 45728, 43738, 39017, 26380, 44028, 36484, 25465, 39212, 39211, 39210, 25453, 39492, 30147, 16546, 16458, 38223, 16447, 28389, 38344, 23638, 15896, 152305673, 24426, 15832, 23813, 17735, 15722, 38517, 24318, 29210

38468, 40934, 40935, 40933, 39381, 43448, 22922, 23260, 35523, 17399, 46510, 24468, 44139, 16018, 43712, 16049, 30164, 16709, 16761, 18123, 17182, 16802, 44500, 16264, 16983, 24912, 46717, 17550, 30709, 15890, 40768, 27459, 16041, 30953, 38685, 38910, 34256, 16490, 42803, 41908, 25561, 16524, 49806, 17678, 50610, 45488, 27946, 43273, 47019, 37364, 25195, 26631, 40319, 39283, 41692, 34305, 47834, 50890, 42334, 37085, 39109, 16771, 45485, 37053, 34455, 30213, 42242, 16723, 29309, 32280, 32282, 31554, 49654, 16514, 16210, 16557, 42774, 16405, 15851, 18288, 16329, 23973, 17004, 16999, 46719, 16309, 38387, 26487, 17540, 16799, 18175, 30728, 37952, 51995, 25174, 40424, 36817, 38382, 25936, 55481

45623, 35767, 45622, 38662, 35766, 16013, 15817, 16170, 38726, 38725, 43322, 41694, 43323, 8, 26346, 31380, 16354, 16395, 43440, 36660, 39491, 38953, 38131, 42537, 16035, 34552, 16053, 43334, 42769, 43335, 49384, 41703, 37402, 50537, 43308, 43605, 43292, 43296, 43312, 43303, 43299, 43298, 43305, 43306, 43301, 43309, 43304, 43297, 43307, 43302, 43295, 43300, 46205, 43313, 16541, 32123, 40489, 38653, 23756, 43326, 44020, 43327, 32121, 35434, 32417, 32122, 43324, 43325, 16593, 30269, 16698, 52849, 56204, 56208, 54662, 53327, 17154, 43332, 43333, 36249, 24818, 36853, 48983, 48981, 43190, 42768, 33053, 45064, 28428, 43714, 23094, 32003, 36963, 13586, 41600, 16804, 42533, 43294, 50363, 11203

15849, 24473, 55600, 50906, 38467, 43315, 43316, 16260, 37454, 47601, 36818, 36203, 27218, 39449, 25906, 52636, 17901, 16649, 25875, 16647, 28697, 51699, 52642, 16941, 17917, 37644, 31563, 36628, 16465, 34500, 16255, 16624, 39393, 36504, 17372, 33487, 15879, 15893, 34039, 40469, 34050, 34038, 34041, 41392, 34040, 38996, 33224, 152305668, 17136, 16695, 15880, 40568, 38782, 17850, 32559, 15887, 44131, 28283, 50471, 30341, 38336, 49779, 36209, 42496, 44659, 16356, 38509, 42822, 44301, 43454, 37958, 31608, 37212, 39284, 32844, 26789, 16787, 36774, 38016, 30192, 16167, 25380, 43959, 16706, 47058, 43582, 42312, 36999, 36072, 36079, 36077, 37985, 16097, 38474, 38483, 16478, 36387, 24739, 16314, 38249

16437, 16841, 28493, 30719, 31929, 31935, 31936, 31933, 30712, 17149, 28845, 24218, 16727, 26182, 16206, 2, 30256, 27728, 11414, 16285, 16288, 16307, 16406, 35641, 16209, 16236, 24755, 25434, 16290, 25798, 16103, 27783, 152305671, 30138, 39592, 16055, 16211, 25459, 32609, 33907, 16399, 16372, 16414, 32075, 16454, 28632, 16297, 16369, 16417, 16295, 16321, 16291, 16363, 16364, 16294, 28938, 28936, 28940, 16277, 16445, 16996, 17603, 16381, 16278, 16827, 16528, 38693, 25198, 35793, 30273, 34527, 39188, 39187, 41698, 42669, 16643, 35656, 35678, 47020, 47021, 38885, 33826, 26043, 46718, 36028, 46930, 42719, 25878, 16031, 24429, 51216, 23971, 16926, 16928, 16932, 38855, 36050, 36052, 36051, 43186
39696, 42004, 45499, 45500, 27082, 21668, 36463, 37763, 26061, 43941, 17567, 36237, 17196, 54651, 16604, 16367, 37056, 38903, 38902, 17145, 54720, 52121, 43528, 43526, 33494, 38512, 43347, 38064, 35813, 38419, 16648, 51945, 17147, 9, 38861, 16265, 24484, 35894, 46939, 38380, 37499, 31614, 17163, 16517, 34881, 30531, 17146, 17164, 16537, 16590, 27104, 16435, 16392, 16173, 16300, 46218, 31755, 16302, 16612, 38942, 25388, 43531, 53242, 16778, 32752, 39467, 31486, 16261, 16262, 31037, 35614, 38905, 56257, 16864, 16331, 40318, 40317, 38645, 23257, 25196, 31021, 17354, 16355, 36590, 38964, 15891, 31988, 27977, 36442, 54561, 16464, 16229, 16281, 16280, 16670, 16401, 44782, 38332, 32836, 16317
36572, 16463, 43715, 37200, 25960, 16299, 16135, 48410, 48413, 47687, 16197, 16397, 16252, 37485, 36483, 52661, 17458, 42850, 26352, 27209, 25670, 35799, 35801, 36171, 38860, 46578, 30161, 27775, 48426, 36974, 30207, 48568, 15878, 36511, 16958, 16654, 16793, 35583, 35517, 25452, 23398, 26683, 38854, 38853, 34962, 52514, 33313, 49860, 37253, 30447, 39621, 24970, 39505, 55822, 23698, 37500, 33182, 43280, 43278, 41468, 43279, 43281, 43277, 42000, 43289, 43288, 41475, 38924, 48002, 53340, 54064, 47996, 41470, 47962, 24623, 16807, 36194, 36202, 53335, 24703, 16767, 27304, 48100, 50829, 54507, 39482, 16711, 42644, 39458, 40175, 43276, 15816, 24747, 16162, 38709, 38708, 41702, 41701, 48099, 41469
50364, 43566, 33759, 50589, 15897, 152305667, 52166, 16190, 18216, 16100, 16191, 16192, 43950, 54548, 43947, 16095, 15999, 40503, 47961, 41516, 43541, 54418, 47822, 54419, 41471, 48109, 47966, 53336, 16009, 38550, 24009, 47562, 27922, 44026, 27103, 16175, 34060, 17113, 45727, 16461, 38150, 40858, 46913, 44016, 33002, 27821, 33900, 16830, 16676, 17011, 28846, 15886, 16304, 28391, 16316, 44504, 38670, 25877, 23689, 16912, 16279, 16303, 56214, 56211, 16213, 152305672, 17041, 16386, 17613, 16270, 33728, 18215, 16238, 37718, 16089, 24731, 28247, 38690, 36055, 42501, 17144, 34164, 36390, 39057, 25069, 39485, 50684, 31908, 37306, 39021, 25076, 36222, 41660, 38003, 52439, 39020, 39019, 25077, 36232, 36233

37994, 52471, 54733, 24483, 17017, 16208, 15837, 27839, 30141, 24744, 38044, 45114, 26013, 18155, 38500, 35444, 30184, 28844, 25456, 25457, 35757, 35758, 36371, 43426, 37401, 50376, 17333, 30295, 54502, 32295, 50737, 17409, 16151, 44677, 36629, 34426, 25562, 25843, 39108, 48384, 16390, 26951, 28851, 28638, 28754, 56118, 25950, 25447, 38929, 54923, 32843, 36109, 23382, 35419, 42006, 35418, 16003, 24727, 52618, 53322, 53323, 37186, 35657, 35659, 35658, 17244, 38848, 38849, 22933, 16986, 45477, 15888, 32442, 30955, 54976, 39280, 30185, 35033, 16434, 16408, 16456, 16407, 36998, 16104, 27561, 152305670, 16800, 15843, 16714, 16174, 16256, 16444, 45751, 36191, 16239, 16376, 11726, 25143, 17197, 30966

25566, 25958, 16179, 49459, 38258, 50604, 16831, 37535, 29081, 36384, 34757, 29143, 37606, 39309, 36370, 16686, 40661, 31291, 38291, 53201, 24466, 23184, 37299, 52437, 36536, 31349, 35705, 35707, 38759, 35699, 41683, 18033, 34998, 36206, 36208, 38321, 17599, 38797, 44635, 35003, 35298, 42766, 16267, 16513, 56053, 36448, 45738, 31753, 35728, 35737, 39082, 52821, 25426, 44044, 35325, 43611, 36098, 35938, 43816, 26728, 26966, 56016, 107347980, 32384, 38846, 25853, 32642, 20806, 33561, 25078, 39100, 42333, 40842, 16412, 108855300, 46940, 36854, 18096, 18095, 16133, 38845, 38817, 15969, 25192, 40702, 16178, 16129, 32317, 34114, 35244, 40169, 16832, 42498, 16431, 16305, 36635, 35297, 15859, 24834, 47431

28631, 16172, 16245, 25622, 15511, 41536, 16652, 37382, 16296, 16626, 16246, 35961, 25439, 39549, 29902, 16595, 16308, 16460, 38734, 16939, 16677, 25376, 16027, 16667, 15894, 152305678, 16368, 31594, 16051, 44657, 17896, 39172, 32242, 50347, 36381, 16596, 15861, 17006, 32246, 34554, 39637, 10854, 38386, 16276, 46612, 37455, 16942, 49540, 27510, 27509, 27505, 35348, 38340, 16915, 16684, 31013, 42635, 46962, 17040, 16275, 32842, 50739, 41474, 17209, 16899, 16657, 18218, 30958, 16719, 30222, 16777, 30191, 46480, 16680, 55883, 16442, 16594, 32443, 54381, 40776, 49809, 40791, 50978, 25039, 49751, 24968, 16366, 16370, 38051, 16402, 16411, 16457, 16293, 16383, 24800, 34640, 38938, 26180, 26179, 30251

16320, 16274, 16443, 37000, 44611, 44623, 44624, 16441, 28608, 16074, 27559, 152305669, 28992, 29265, 28991, 16906, 34797, 34795, 34789, 34793, 16642, 16196, 31613, 31618, 16415, 37272, 16730, 17428, 17429, 16691, 38944, 16455, 37206, 16439, 16453, 16060, 39079, 45336, 15895, 40417, 41543, 41542, 41541, 41540, 47013, 34964, 16212, 43342, 16438, 16573, 16378, 24887, 43708, 36656, 27081, 16920, 38575, 35704, 38574, 35263, 47376, 38314, 37332, 44458, 29600, 16393, 38269, 38570, 30707, 30708, 16837, 16919, 31379, 44238, 16096, 36575, 28695, 42551, 43983, 17338, 34165, 35014, 35013, 30254, 36591, 18167, 39083, 24882, 45632, 37054, 43847, 39073, 38883, 16134, 46959, 35978, 35980, 35979, 16535, 15815

24530, 24531, 23759, 25056, 45145, 17945, 10, 28554, 43540, 28587, 29350, 39917, 28597, 43345, 42770, 43346, 30734, 34951, 34950, 35762, 16679, 28875, 43464, 34560, 24624, 12290, 24626, 27937, 35563, 16539, 49696, 49721, 39194, 34391, 16150, 16637, 16152, 11421, 35284, 28944, 35748, 35741, 24532, 45625, 38171, 29248, 43462, 17405, 16391, 36192, 17740, 16025, 24284, 43463, 49573, 16967, 16518, 38338, 29810, 11767, 25565, 16497, 43592, 16092, 16687, 16907, 24534, 36053, 36054, 56054, 16201, 152305666, 48915, 43584, 52130, 38174, 50301, 40194, 31645, 38999, 47011, 37845, 51219, 27410, 17141, 16763, 16655, 36489, 54326, 25654, 39506, 16283, 16232, 24888, 16550, 16216, 16217, 16388, 34641, 38327
16186, 16253, 16319, 16289, 28696, 37064, 16385, 38259, 30795, 31615, 28752, 38878, 49887, 17498, 51457, 17195, 33988, 39454, 32640, 16946, 32171, 31205, 16936, 49748, 36049, 40823, 15985, 15921, 39632, 39630, 38098, 50776, 24767, 16091, 55966, 46953, 36056, 48839, 42903, 16538, 35305, 35191, 35196, 16632, 37095, 38862, 42358, 43598, 38834, 39590, 45746, 14797, 16182, 46280, 37055, 16786, 44419, 54409, 54399, 54402, 54387, 16627, 35692, 43045, 38104, 20910, 26519, 53549, 36167, 16094, 16446, 15565, 30452, 44589, 30233, 38683, 17236, 33912, 41733, 41678, 48800, 32304, 34067, 27750, 34051, 46603, 36722, 41718, 41717, 34111, 52305, 34201, 16669, 31295, 31832, 16927, 34425, 39213, 16258, 16259
16533, 26282, 24750, 28570, 39201, 28572, 34860, 28571, 33607, 42313, 43467, 43729, 36723, 39771, 16001, 44719, 38466, 43351, 23919, 16462, 36445, 36446, 47633, 34257, 16083, 16440, 16105, 42640, 40565, 36420, 41614, 38965, 48424, 109051912, 18007, 56014, 38857, 44023, 43520, 26376, 55564, 32014, 36486, 36488, 36487, 16487, 15973, 16384, 16371, 25455, 33284, 16382, 30028, 17174, 15510, 27700, 52654, 52653, 17324, 43958, 46721, 44067, 40793, 52420, 44658, 44052, 50014, 16418, 55895, 16896, 34815, 16774, 51741, 54255, 48427, 16908, 16909, 17153, 38130, 16588, 16660, 26178, 16029, 35047, 25360, 36418, 38471, 38472, 38473, 37537, 35141, 46720, 24630, 25627, 28511, 49859, 17204, 16080, 47809, 16997
36900, 31944, 16380, 16379, 16923, 17247, 16247, 16788, 25879, 46482, 46483, 46486, 46487, 36375, 16375, 43604, 51136, 51137, 51138, 43427, 31078, 51478, 19796, 35169, 33760, 52488, 47379, 44274, 54485, 54484, 36743, 52599, 36730, 52600, 36741, 36648, 36742, 39523, 49387, 54517, 54516, 54518, 54481, 54480, 54483, 54482, 46932, 29410, 35432, 35433, 30209, 34397, 27084, 15862, 26363, 36968, 16350, 31848, 31845, 39113, 31846, 39112, 39111, 32948, 31847, 16662, 35962, 38783, 28057, 37371, 40698, 39999, 49971, 49970, 48961, 35360, 27538, 36869, 39174, 16911, 17179, 16661, 16503, 11836, 16973, 31287, 17143, 43625, 17162, 27457, 31824, 32007, 31885, 31871, 31884, 31843, 24258, 31834, 34236, 31833

			16940, 39537, 40304, 52452, 52165, 11, 43965, 46495, 31182, 32149, 46224, 43449, 48801, 48803, 37261, 16530, 36721, 37052, 45763, 44117, 43539, 16929, 16198, 16215, 16704, 15997, 17185, 16242, 16257, 16286, 34492, 16137, 30036, 34993, 37738, 36441, 49405, 36117, 52517, 53522, 30158, 24939, 31175, 16707, 38463, 43355, 27604, 17476, 30210, 17191, 34491, 31197, 15839, 39077, 16169, 38522, 38521, 41691, 41689, 33571, 27609, 17194, 17210, 13624, 42670, 39483, 31232, 16623, 28076, 39159, 39158, 39157, 41681, 42899, 39481, 35031, 35617, 39342, 28106, 39712, 34638, 32261, 41785, 32262, 43969, 38394, 35828, 38507, 43975, 16180, 42620, 35635, 31077, 33321, 49282, 41598, 48989, 44956, 31076, 33104 55756, 23397, 30201, 16420, 17396, 49969, 38569, 25564, 39191, 35943, 16531, 35285, 18148, 16922, 16635, 44027, 16619, 44132, 26054, 47974, 30536, 34791, 40821, 36653, 28877, 43287, 44295, 36006, 55465, 16499, 46933, 16486, 36075, 17466, 36241, 36137, 36119, 24533, 16469, 54547, 40471, 40470, 16467, 38514, 17693, 24559, 16477, 24561, 36238, 16475, 36116, 37065, 47383, 47382, 48958, 47385, 49830, 31200, 50535, 39304, 16419, 26793, 34646, 16507, 16690, 40818, 16225, 49626, 29880, 41644, 35600, 35599, 34499, 38164, 31161, 26630, 26633, 34435, 17057, 16042, 31167, 17007, 30415, 17008, 34613, 17009, 17010, 52159, 16618, 40316, 36462, 26914, 17172, 15963, 37323, 27415, 40866, 16315, 56200, 23399 42658
	フィルター	ビヘイビア:	
		アプリケーションカテゴリ:	
		ポピュラリティ:	
		プロトコル:	
		リスク:	
		テクノロジー:	
		ベンダー:	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	enable
DNSトラフィックの許可とログ	enable
HTTPベースアプリケーションの差し替えメッセージ	enable

22. セキュリティプロファイル（侵入防止）（概要）

IPSセンサー

名前	コメント
all_default	All predefined signatures with default setting.
all_default_pass	All predefined signatures with PASS action.
protect_http_server	Protect against HTTP server-side vulnerabilities.
protect_email_server	Protect against email server-side vulnerabilities.
protect_client	Protect against client-side vulnerabilities.
high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities
wifi-default	Default configuration for offloading WiFi traffic.
sniffer-profile	Monitor IPS attacks.
default	Prevent critical attacks.

カスタムIPSシグネチャ

ID	名前	シグネチャ	コメント

23. セキュリティプロファイル（侵入防止）

IPSセンサー

No. 1

名前	all_default
コメント	All predefined signatures with default setting.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト　（隔離時間　日　時間　分）
	Action：default　Log：enable　Quarantine：none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	all
プロトコル	all
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間（秒）	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

No. 2

名前	all_default_pass
コメント	All predefined signatures with PASS action.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	モニター　（隔離時間　日　時間　分）
	Action：pass　Log：enable　Quarantine：none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	all
プロトコル	all
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	

レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間 (秒)	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

No. 3

名前	protect_http_server
コメント	Protect against HTTP server-side vulnerabilities.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト (隔離時間 日 時間 分)
	Action : default Log : enable Quarantine : none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	サーバー
重大度	■■■□□ (medium) ■■■■□ (high) ■■■■■ (critical)
プロトコル	HTTP
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間 (秒)	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
30316	
10174	
26815	
27309	
40361	
15186	
17866	
17868	
38015	
40473	
37624	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

24. セキュリティプロファイル（SSL/SSHインスペクション）（概要）

SSL/SSHインスペクションプロファイル

SSL/SSHインスペクションプロファイルを下表に示します。

なお、次の3つは読み取り専用の標準プロファイルです。

・certificate-inspection

・deep-inspection

・no-inspection

名前	コメント
deep-inspection	Read-only deep inspection profile.
custom-deep-inspection	Customizable deep inspection profile.
no-inspection	Read-only profile that does no inspection.
certificate-inspection	Read-only SSL handshake inspection profile.
test01_SSL	
test02_SSL	
test03_SSL	
test04_SSL	
test05_SSL	
test06_SSL	
test07_SSL	
test08_SSL	
test09_SSL	
test10_SSL	
test11_SSL	
test12_SSL	SSH deep inspection (all ports)
test13_SSL	

25. セキュリティプロファイル (SSL/SSHインスペクション)

SSL/SSHインスペクションプロファイル

注記
本節では、SSLインスペクションオプションおよび共通オプションの一部の設定について、CLIおよび設定ファイル上の構成に基づき、プロトコルごとに記載しています。
そのため、FortiGate GUI（Web管理画面）上の表示項目と、本節の記載項目が一対一で対応しない場合があります。

No. 1

名前	deep-inspection						
コメント	Read-only deep inspection profile.						
SSLインスペクションオプション							
いずれかのSSLインスペクションを有効化	複数のサーバに接続する複数のクライアント						
インスペクション方式	フルSSLインスペクション						
CA証明書	Fortinet_CA_SSL						
悪意のある証明書	ブロック						
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
信頼されないSSL証明書		許可	許可	許可	許可	許可	許可
サーバ証明書SNIチェック		有効					
SSL暗号の準拠を強制	無効	無効	無効	無効	無効	無効	無効
SSLネゴシエーションの準拠を強制	無効	無効	無効	無効	無効	無効	無効
RPC over HTTPS							
HTTPS 経由の MAPI							
サーバ証明書							
プロトコルポートマッピング							
すべてのポートを検査する	無効						
プロトコルごとの設定							
	ステータス	ポート					
HTTPS	有効	443					
	暗号化されたクライアントHello :						
SMTPS	有効	465					
POP3S	有効	995					
IMAPS	有効	993					
FTPS	有効	990					
DNS over TLS	無効	853 (固定値)					
HTTP/3							
DNS over QUIC							
SSLインスペクションから除外							
著名なWebサイト	無効						
SSL除外のログを記録する	無効						
WEBカテゴリ							
ID	名前						
31	Finance and Banking						
33	Health and Wellness						
アドレス							
adobe							
Adobe Login							
android							
apple							
appstore							
mzstatic-apple							
SSHインスペクション							
SSH deep scan							
SSH port							
共通オプション							
無効なSSL証明書							
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
期限切れの証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
失効した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック

検証がタイムアウトした証明書		信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可
検証に失敗した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
SSLアノマリのログを記録する	有効						

No. 2

名前	custom-deep-inspection						
コメント	Customizable deep inspection profile.						
SSLインスペクションオプション							
いずれかのSSLインスペクションを有効化	複数のサーバに接続する複数のクライアント						
インスペクション方式	フルSSLインスペクション						
CA証明書	Fortinet_CA_SSL						
悪意のある証明書	ブロック						
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
信頼されないSSL証明書		許可	許可	許可	許可	許可	許可
サーバ証明書SNIチェック		有効					
SSL暗号の準拠を強制	無効	無効	無効	無効	無効	無効	無効
SSLネゴシエーションの準拠を強制	無効	無効	無効	無効	無効	無効	無効
RPC over HTTPS							
HTTPS 経由の MAPI							
サーバ証明書							
プロトコルポートマッピング							
すべてのポートを検査する	無効						
プロトコルごとの設定							
	ステータス			ポート			
HTTPS	有効			443			
	暗号化されたクライアントHello :						
SMTPS	有効			465			
POP3S	有効			995			
IMAPS	有効			993			
FTPS	有効			990			
DNS over TLS	無効			853 (固定値)			
HTTP/3							
DNS over QUIC							
SSLインスペクションから除外							
著名なWebサイト	無効						
SSL除外のログを記録する	無効						
WEBカテゴリ							
ID	名前						
31	Finance and Banking						
33	Health and Wellness						
アドレス							
android							
fortinet							
google-play							
icloud							
itunes							
microsoft							
skype							
SSHインスペクション							
SSH deep scan							
SSH port							
共通オプション							
無効なSSL証明書							
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
期限切れの証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
失効した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
検証がタイムアウトした証明書		信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可

検証に失敗した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
SSLアノマリのログを記録する	有効						

No. 3

名前	no-inspection						
コメント	Read-only profile that does no inspection.						
SSLインスペクションオプション							
いずれかのSSLインスペクションを有効化							
インスペクション方式	フルSSLインスペクション						
CA証明書	Fortinet_CA_SSL						
悪意のある証明書	ブロック						
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
信頼されないSSL証明書		許可	許可	許可	許可	許可	許可
サーバ証明書SNIチェック		有効					
SSL暗号の準拠を強制	無効	無効	無効	無効	無効	無効	無効
SSLネゴシエーションの準拠を強制	無効	無効	無効	無効	無効	無効	無効
RPC over HTTPS							
HTTPS 経由の MAPI							
サーバ証明書							
プロトコルポートマッピング							
すべてのポートを検査する	無効						
プロトコルごとの設定							
	ステータス			ポート			
HTTPS	無効						
	暗号化されたクライアントHello :						
SMTPS	無効						
POP3S	無効						
IMAPS	無効						
FTPS	無効						
DNS over TLS	無効			853 (固定値)			
HTTP/3							
DNS over QUIC							
SSLインスペクションから除外							
著名なWebサイト							
SSL除外のログを記録する							
WEBカテゴリ							
ID	名前						
アドレス							
SSHインスペクション							
SSH deep scan							
SSH port							
共通オプション							
無効なSSL証明書							
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
期限切れの証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
失効した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
検証がタイムアウトした証明書		信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可
検証に失敗した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
SSLアノマリのログを記録する	有効						

26. VPN（概要）

IPsecトンネル

トンネル名	インターフェースバインディング
VPN_to_Opponent	lan
トンネル 1	loopback_1
ハブアンド	lan
リモートア	loopback_1
カスタム	ssl.root
サイト 2	ssl.root
サイト3	loopback_1

IPsecアグリゲート

名前	アルゴリズム
aguri	weighted-round-robin

IPsecコンセントレーター

名前	メンバー

SSL-VPNポータル

名前	トンネルモード	Webモード
full-access		有効
test1	有効	有効
test2	有効	有効

SSL-VPNレルム

URLパス	バーチャルホスト	最大同時ユーザー数
test		0
corp-realm	vpn.xxxx.com	50

SSL-VPNクライアント

トンネル	インターフェース	サーバ	ポート	コメント
test	Interface3	testtest	443	

27. VPN (IPsecトンネル)

No. 1

名前	VPN_to_Opponent
トンネルテンプレート (空白の場合はカスタム)	カスタム
ネットワーク	
インターフェースバインディング	lan
システムDNSを使用する	
IPアドレス	192.2.2.2
IPv4モード設定	
クライアントアドレス範囲	-
サブネットマスク	
DNSサーバ	
IPv4スプリットトンネルを有効化	
アクセス可能ネットワーク	
IPv6モード設定	
クライアントアドレス範囲	-
プレフィックス	
DNSサーバ	
IPv6スプリットトンネルを有効化	
アクセス可能ネットワーク	
デッドピア検知	オンデマンド
DPD再試行回数	3
DPD再試行間隔	20
前方誤り訂正	
イーグレス	無効
イングレス	無効
高度な設定	
ルートの追加	
オートディスカバリ送信側	無効
オートディスカバリ受信側	無効
インターフェースIPの交換	無効
デバイスの作成	無効
認証	
リモートデバイス/ダイナミックDNS	リモートデバイス
リモートIPアドレス	192.2.2.2
FQDN	
認証方式	事前共有鍵
事前共有鍵	********
証明書名	
ピアオプション	
受け入れるタイプ	any
ピアID	

フェーズ2セレクタ		
名前	ローカルアドレス	リモートアドレス
新規フェーズ 2	192.0.0.0 - 192.255.255.255	192.1.1.1

XAUTH	
クライアント	
ユーザ名	
パスワード	********
ユーザグループ *未記入の場合はポリシーから継承	

No. 2

名前	トンネル 1
トンネルテンプレート (空白の場合はカスタム)	サイト間 - FortiGate
ネットワーク	
インターフェースバインディング	loopback_test_3
システムDNSを使用する	
IPアドレス	192.1.1.1
IPv4モード設定	
クライアントアドレス範囲	-

サブネットマスク	
DNSサーバ	
IPv4スプリットトンネルを有効化	
アクセス可能ネットワーク	
IPv6モード設定	
クライアントアドレス範囲	-
プレフィックス	
DNSサーバ	
IPv6スプリットトンネルを有効化	
アクセス可能ネットワーク	
デッドピア検知	オンデマンド
DPD再試行回数	3
DPD再試行間隔	20
前方誤り訂正	
イーグレス	無効
イングレス	無効
高度な設定	
ルートの追加	
オートディスカバリ送信側	無効
オートディスカバリ受信側	無効
インターフェースIPの交換	無効
デバイスの作成	無効
認証	
リモートデバイス/ダイナミックDNS	リモートデバイス
リモートIPアドレス	192.1.1.1
FQDN	
認証方式	事前共有鍵
事前共有鍵	********
証明書名	
ピアオプション	
受け入れるタイプ	any
ピアID	

フェーズ2セレクタ

名前	ローカルアドレス	リモートアドレス
トンネル１サイト間	トンネル１サイト間_local	トンネル１サイト間_remote

XAUTH	
クライアント	
ユーザ名	
パスワード	
ユーザグループ *未記入の場合はポリシーから継承	

28. VPN（ハブ&スポーク トポロジ）

BGP

ネイバー

トンネルIP	AS
192.10.10.2	65001
192.10.10.1	65001

ネイバー範囲

プレフィックス	ネイバーグループ
192.10.10.0 255.255.255.0	HUB-GROUP
192.20.20.0 255.255.255.0	HUB-GROUP

29. VPN (SSL-VPN設定)

SSL-VPNステータス	有効

接続設定

リッスンするインターフェース	loopback_test_4
	test_10
リッスンするポート	443
サーバ証明書	Fortinet_Factory_Backup
HTTPをSSL-VPNにリダイレクト	無効
アクセスを制限 *特定ホストへアクセス制限未設定の場合は、任意のホストからのアクセスを許可	
特定ホストへアクセス制限	
ホスト (IPv4アドレス)	all
ホスト (IPv6アドレス)	all
送信元をネゲート	無効
アイドルログアウト	
非アクティブ (秒)	0
クライアント証明書を要求	無効

トンネルモードクライアント設定

アドレス範囲	
IPv4アドレス	SSLVPN_TUNNEL_ADDR1
IPv6アドレス	SSLVPN_TUNNEL_IPv6_ADDR1
DNSサーバ *DNSサーバ未設定の場合はクライアントシステムのDNSと同じ	
DNSサーバ #1	0.0.0.0
DNSサーバ #2	0.0.0.0
Ipv6 DNSサーバ #1	::
Ipv6 DNSサーバ #2	::
WINSサーバ	
WINSサーバ #1	0.0.0.0
WINSサーバ #2	0.0.0.0
IPv6 WINSサーバ #1	::
IPv6 WINSサーバ #2	::

WEBモードの設定

言語	ブラウザの設定

認証/ポータルマッピング

ユーザ	グループ	レルム	ポータル
QA	Guest-group	corp-realm	test1
guest	IPsec_Users	corp-realm	test2

30. VPN (SSL-VPNポータル)

No.1

名前	full-access
ユーザを一度に単一のSSL-VPN接続に制限する	無効
トンネルモード	
スプリットトンネリング	
ルーティングアドレスの上書き	
送信元IPプール	
Ipv6トンネルモード	
IPv6スプリットトンネリング	
IPv6ルーティングアドレスの上書き	
送信元IPv6プール	
トンネルモードクライアントオプション	
クライアントがパスワードを保存することを許可する	
クライアントの自動接続を許可する	
クライアントが接続をキープすることを許可する	
DNSスプリットトンネリング　(SplitDns)	

ドメイン	プライマリDNSサーバ	セカンダリDNSサーバ	プライマリDNSIpv6サーバ	セカンダリDNSIpv6サーバ

ホストチェックタイプ	
特定のOSバージョンに制限	

バージョン	アクション	トレランス	パッチレベル

WEBモード	有効
ランディングページ	カスタム
ポータルメッセージ	
テーマ	
デフォルトプロトコル	
セッション情報を表示	
接続ランチャーを表示	
ログイン履歴を表示	
ユーザブックマーク	
定義済みブックマークを表示	
ブックマークにフォーカス	
コンテンツIP/UIを書き換え	有効
RDP/VNCクリップボード	
定義済みブックマーク	
名前	
タイプ	
説明	
ホスト	
ポート	
URL	
シングルサインオン	
ユーザ名	
パスワード	
SSOフォームデータ	

フォームキー	フォーム値

フォルダー	
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	

制限付き管理者モード	
ユーザ名	
パスワード	
URL	testTest
SSOクレデンシャル	SSL-VPNログイン
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
FortiClientダウンロード	
ダウンロード方法	
ダウンロードロケーションのカスタマイズ	
Windows	
Mac	

・本設定仕様書サンプルはFortiGate 40Fから採取した
"full-configuration"のファイルを使用して作成しております。
・一部固有のIPアドレスが記述された部分はマスクしております。

FortiGate Global 設定仕様書

仕様書商事 様

FortiGate ホスト名	FortiGate-40F
作成日	20YY年MM月DD日
作成者	セイ･テクノロジーズ

セイ･テクノロジーズ株式会社

(住所)

改訂履歴

版数	日付	内容	担当者

目次

1. システム（概要）

システムの設定、および管理者、管理者プロファイル、HA、SNMP、FortiGuard、表示機能設定の概要を記載しています。

2. システム（管理者）

システムの管理者の詳細を記載しています。

3. システム（管理者プロファイル）

システムの管理者プロファイルの詳細を記載しています。

4. システム（SNMP v1/v2c）

システムのSNMP v1/v2cの詳細を記載しています。

5. システム（SNMP v3）

システムのSNMP v3の詳細を記載しています。

6. システム（VDOM）

システムのVDOMの詳細を記載しています。

7. ネットワーク（概要）

ネットワークのインターフェース、およびスタティックルートの概要、DNSを記載しています。

8. セキュリティプロファイル（アンチウイルス）

セキュリティプロファイルのアンチウイルスの詳細を記載しています。

9. セキュリティプロファイル（WEBフィルタ）

セキュリティプロファイルのWEBフィルタの詳細を記載しています。

10. 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）

セキュリティプロファイルのアプリケーションコントロールの詳細を記載しています。

11. セキュリティプロファイル（侵入防止）（概要）

セキュリティプロファイルの侵入防止の概要を記載しています。

12. セキュリティプロファイル（侵入防止）

セキュリティプロファイルの侵入防止の詳細を記載しています。

◆商標

FortiGateおよびFortiGateの製品名は、Fortinet, Inc.の米国およびその他の国における商標または登録商標です。

1. システム（概要）

機種情報

ファームウェアバージョン	FGT40F-7.4.7-FW-build2731-250120
Alias	FortiGate-40F

管理者

システム管理者

名前	プロファイル	タイプ	コメント
admin	super_admin	ローカル	
test_user	test_user	ローカル	
test_manager		ローカル	

REST API管理者

名前	プロファイル	コメント
test_3	test_1	
test_2	test_2	
test_1	test_1	

シングルサインオン管理者

名前	プロファイル
test_1	test_1
test_2	test_2

管理者プロファイル

プロファイル名	コメント
prof_admin	
test_1	
test_2	
CLIcommand_on	
CLIcommand_off	
CLIcommand_custom-allon	
CLIcommand_custom-alloff	

設定

ホスト名		FortiGate-40F
システム時間		
タイムゾーン		Asia/Tokyo
時刻設定(NTP)	有効	enable
	サーバー選択	FortiGuard
	同期間隔 (分)	60
時刻設定(PTP)	有効	
	モード	
	遅延メカニズム	
	リクエスト間隔 (秒)	
	インターフェース	
デバイスをローカルNTPサーバとして設定		
リッスンするインターフェース		l2t.root
		lan
管理者設定		
HTTPポート		80
HTTPSへリダイレクト		enable
HTTPSポート		443
HTTPサーバー証明書		self-sign
SSHポート		22
Telnetポート		23
アイドルタイムアウト (分)		30
ACMEインターフェース		test_1
		test_25
シングルサインオン		
ファブリックSSO		
FortiCloud SSO	FortiCloud SSOを有効	disable

	Default admin profile	
パスワードポリシー		
パスワードスコープ		管理者
最小長		8
新規文字の最小文字数		0
キャラクタ要件	大文字	1
	小文字	1
	数字 (0-9)	1
	特殊文字	1
パスワード再利用を許可		enable
パスワード期限 (日)		90
ワークフローマネジメント		
設定保存モード		自動
タイムアウト時に元に戻す (秒)		
ポリシー変更サマリ		
ポリシーはデフォルトで期限切れです		
後に期限切れ(日)		
設定表示		
言語		日本語
テーマ		jade
日付/時刻表示		ブラウザのタイムゾーン
VLANスイッチモード		disable
NGFWモード		
セントラルNAT		
初期設定		
FortiConverter に設定ファイルの取得を許可する		disable
自動ファイルシステムチェック		enable
USB自動インストール	設定ファイルを検知を有効	enable
	設定ファイルを検知	fgt_system.conf
	ファームウェアを検知を有効	enable
	ファームウェアを検知	image.out
Eメールサービス		
SMTPサーバ		fortinet-notifications.com
ポート		465
認証	認証を有効	disable
	ユーザー名	
セキュリティモード		smtps

HA

モード		アクティブ・アクティブ	
デバイスのプライオリティ		128	
優先度の効果を上げる		enable	
クラスタ設定			
グループID		0	
グループ名		test_2	
セッションピックアップ		disable	
モニタインターフェース		test_24	
		test_25	
ハートビートインターフェース			
インターフェース名		優先度	
lan3		136	
wan		90	
管理インターフェースの予約			
インターフェース	ゲートウエイ	IPv6ゲートウェイ	宛先サブネット

SNMP

システム情報	
SNMPエージェント	enable
説明	

ロケーション	
コンタクト情報	

SNMP v1/v2c

名前	クエリ	トラップ	ホスト	IPv6ホスト	イベント	ステータス
test_1	v1: enable v2: enable	v1: enable v2: enable	0.0.0.0/0.0.0.0, 0.0.0.1/255.255.255.255, 0.0.0.2/255.255.255.255, 0.0.0.3/255.255.255.255		40	disable
test_2	v1: disable v2: disable	v1: disable v2: disable	0.0.0.0/0.0.0.0, 0.0.0.1/255.255.255.255, 0.0.0.2/255.255.255.255, 0.0.0.3/255.255.255.255	fd00:xxxx:9d16::abcd/128, fd00:xxxx:9d16::abce/128	1	enable
test_ 3	v1: disable v2: enable	v1: disable v2: enable	0.0.0.0/0.0.0.0	fd00:xxxx:9d16::abcd/128	42	enable

SNMP v3

名前	セキュリティレベル	クエリ	トラップ	ホスト	IPv6ホスト	イベント	ステータス
test_2	プライベート	disable	enable	0.0.0.0, 0.0.0.0			disable
test_1	認証なし	enable	enable	0.0.0.0, 0.0.0.0, 0.0.0.0		41	disable
test_3	非プライベート	enable	disable	0.0.0.0, 0.0.0.0		21	disable
test_4	認証なし	disable	disable	0.0.0.0, 0.0.0.0	fd00:xxxx:9d16::abcd	1	enable
test_5	認証なし	enable	enable	192.168.20.0, 192.168.30.10	fd00:xxxx:9d16::abcd, fd00:e670:9d16::abce	41	enable

FortiGuard

FortiGuardアップデート		
スケジュールされたアップデート	有効	enable
	スケジュール	毎週
	曜日	月曜
	時間	午後 4時
IPSの品質を向上		enable
拡張IPSシグネチャパッケージを利用		enable
アンチウイルス PUP/PUA		
サーバロケーションの更新		米国のみ
フィルタリング		
Webフィルタキャッシュ	Webフィルタキャッシュの有効	enable
	キャッシュの有効期間(分)	60
Eメールフィルタキャッシュ	Eメールフィルタキャッシュの有効	enable
	キャッシュの有効期間(分)	30
FortiGuardフィルタリングサービス	プロトコル	https
	ポート	443

FortiGuardサーバをオーバライド	
サーバーアドレス	サーバータイプ
123.0.0.0	両方
12::	フィルタリング
123.12.0.0	アンチウイルスとIPSのアップデート
aaaxxxx	フィルタリング

表示機能設定

コア機能	(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります

IPsec VPN		enable
IPv6	enable	disable
SSL-VPN		disable
Wifiコントローラー		enable
スイッチコントローラー		enable
高度なルーティング		enable
セキュリティ機能		
DNSフィルタ		enable
Explicitプロキシ		disable
Eメールフィルタ		disable
Inline-CASB		disable
Webアプリケーションファイアウォール		disable
Webフィルタ		enable
アプリケーションコントロール		enable
アンチウイルス		enable
エンドポイントコントロール		enable
ゼロトラストネットワークアクセス		enable
データ漏洩対策		disable
ビデオフィルタ		enable
ファイルフィルタ		enable
仮想パッチ		disable
侵入防止		enable
その他の機能		
DNSデータベース		disable
DoSポリシー		enable
Eメール収集		disable
FortiExtender		disable
FortiGate Cloud Sandbox	enable	disable
ICAP		disable
Implicit Firewall ポリシー		enable
Local Inポリシー		disable
SD-WANインターフェース		enable
SSL-VPNパーソナルブックマーク		disable
SSL-VPNレルム		disable
VoIP		disable
アドバンストエンドポイントコントロール		disable
アプリケーション検知ベースのSD-WAN	enable	disable
トラフィックシェイピング		enable
ポリシーの詳細オプション		disable
ポリシーベース IPsec VPN		disable
ポリシー免責事項		disable
マルチキャストポリシー		disable
ローカルアウトルーティング	enable	disable
ロードバランス		disable
ワークフローマネジメント	enable	disable
ワイヤレス オープンセキュリティ	enable	disable
運用技術(OT)		disable
脅威ウェイトトラッキング		enable
高度なワイヤレス機能		disable
差し替えメッセージグループ	enable	disable
証明書	enable	enable
動的なデバイスとOSの識別		disable
複数インターフェースポリシー		disable
名前なしポリシー許可		disable

2. システム（管理者）

システム管理者

No. 1

ユーザー名		admin
タイプ		ローカルユーザ
コメント		
管理者プロファイル		super_admin
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 2

ユーザー名		test_2
タイプ		ローカルユーザ
コメント		
管理者プロファイル		test_2
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0

管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 3

ユーザー名		test_3
タイプ		ローカルユーザ
コメント		
管理者プロファイル		
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	192.112.0.0/255.240.0.0
		192.112.10.0/255.240.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	test_1
		test_2

No. 4

ユーザー名		test04
タイプ		リモートサーバグループの単一ユーザと一致
コメント		
管理者プロファイル		admin_no_access
パスワード変更を強制		
リモートユーザーグループ		tesst01_remoteusergroup
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0

		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 5

ユーザー名		test05_qauser
タイプ		public key infrastructure(PKI)グループを利用
コメント		
管理者プロファイル		admin_no_access
パスワード変更を強制		
リモートユーザーグループ		
PKIグループ		tesst05_remoteusergroup
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 6

ユーザー名		test06
タイプ		リモートサーバグループのすべてのユーザと一致
コメント		
管理者プロファイル		admin_no_access
パスワード変更を強制		
リモートユーザーグループ		tesst01_remoteusergroup
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0

		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

No. 7

ユーザー名		manager
タイプ		ローカルユーザ
コメント		デモ・ハンズオン用
管理者プロファイル		super_admin
パスワード変更を強制		disable
リモートユーザーグループ		
PKIグループ		
信頼されるホストにログインを制限	IPv4	0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
		0.0.0.0/0.0.0.0
	IPv6	::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
		::/0
管理者をゲストアカウントのプロビジョニングのみに制限	ゲストグループ	

REST API管理者

No. 1

ユーザー名	test_3
コメント	
管理者プロファイル	test_1
APIキー	ENC SH11223344556677889900aabbccddeeffgghhiijjkkllmmnnooppqqrrsstt=
PKIグループ	tesst05_remoteusergroup
オリジン間リソース共有許可	
信頼されるホストにログインを制限	

No. 2

ユーザー名	test_2
コメント	
管理者プロファイル	test_2
APIキー	ENC
PKIグループ	
オリジン間リソース共有許可	https://192.xxx.40.0:80
信頼されるホストにログインを制限	

No. 3

ユーザー名	test_1
コメント	
管理者プロファイル	test_1

APIキー	ENC SH1122334455667788990 0aabbccddeeffgghhiijjkkllmmnnooppqqrrsstt=
PKIグループ	
オリジン間リソース共有許可	
信頼されるホストにログインを制限	2001:a66::/128
	192.112.0.0/255.240.0.0
	2001:a77::/128
	2001:a88::/128
	192.113.0.0/255.240.0.0
	192.114.0.0/255.240.0.0

SSO管理者

No. 1

ユーザー名	test_1
管理者プロファイル	test_1

No. 2

ユーザー名	test_2
管理者プロファイル	test_2

3. システム（管理者プロファイル）

No. 1

名前		prof_admin
コメント		
アクセス権限		
セキュリティファブリック		読み書き
FortiView		読み書き
ユーザー＆デバイス		読み書き
ファイアウォール		読み書き
	ポリシー	
	アドレス	
	サービス	
	スケジュール	
	その他	
ログ＆レポート		読み書き
	設定	
	データアクセス	
	レポートアクセス	
	脅威ウェイト	
ネットワーク		読み書き
	設定	
	パケットキャプチャ	
	ルーター	
システム		読み書き
	管理者ユーザ	
	FortiGuard更新	
	設定	
	メンテナンス	
セキュリティプロファイル		読み書き
	アンチウイルス	
	IPS	
	Webフィルタ	
	Eメールフィルタ	
	データ漏洩対策（データ漏えい防止）	
	ファイルフィルタ	
	アプリケーションコントロール	
	ICAP	
	VoIP	
	Webアプリケーションファイアウォール	
	DNSフィルタ	
	エンドポイントコントロール	
	ビデオフィルタ	
	仮想パッチ	
	Inline-CASB	
VPN		読み書き
Wifi＆スイッチ		読み書き
CLI診断コマンドの使用を許可（system-diagnostics）(FortiOS 7.4.1以前)		
CLIコマンドの使用を許可(FortiOS 7.4.2以降)	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		disable
タイムアウトしない		
オフライン(分)		

No. 2

名前	test_1

コメント		
アクセス権限		
セキュリティファブリック		読み取り
FortiView		読み書き
ユーザー＆デバイス		読み取り
ファイアウォール		カスタム
	ポリシー	読み取り
	アドレス	読み書き
	サービス	読み取り
	スケジュール	読み書き
	その他	読み取り
ログ＆レポート		カスタム
	設定	読み取り
	データアクセス	読み書き
	レポートアクセス	読み取り
	脅威ウェイト	読み書き
ネットワーク		カスタム
	設定	読み取り
	パケットキャプチャ	読み書き
	ルーター	読み取り
システム		カスタム
	管理者ユーザ	読み取り
	FortiGuard更新	読み書き
	設定	読み取り
	メンテナンス	読み書き
セキュリティプロファイル		カスタム
	アンチウイルス	読み取り
	IPS	読み書き
	Webフィルタ	読み取り
	Eメールフィルタ	読み書き
	データ漏洩対策（データ漏えい防止）	なし
	ファイルフィルタ	読み書き
	アプリケーションコントロール	読み取り
	ICAP	読み書き
	VoIP	読み取り
	Webアプリケーションファイアウォール	読み書き
	DNSフィルタ	読み取り
	エンドポイントコントロール	読み書き
	ビデオフィルタ	読み取り
	仮想パッチ	なし
	Inline-CASB	なし
VPN		読み書き
Wifi＆スイッチ		読み取り
CLI診断コマンドの使用を許可（system-diagnostics）（FortiOS 7.4.1以前）		
CLIコマンドの使用を許可（FortiOS 7.4.2以降）	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		enable
タイムアウトしない		enable
オフライン(分)		0

No. 3

名前		test_2
コメント		
アクセス権限		
セキュリティファブリック		読み取り

FortiView		読み取り
ユーザー＆デバイス		読み取り
ファイアウォール		カスタム
	ポリシー	読み取り
	アドレス	読み取り
	サービス	読み取り
	スケジュール	読み取り
	その他	読み取り
ログ & レポート		カスタム
	設定	読み取り
	データアクセス	読み取り
	レポートアクセス	読み取り
	脅威ウェイト	読み取り
ネットワーク		カスタム
	設定	読み取り
	パケットキャプチャ	読み取り
	ルーター	読み取り
システム		カスタム
	管理者ユーザ	読み取り
	FortiGuard更新	読み取り
	設定	読み取り
	メンテナンス	読み取り
セキュリティプロファイル		カスタム
	アンチウイルス	読み取り
	IPS	読み取り
	Webフィルタ	読み取り
	Eメールフィルタ	読み取り
	データ漏洩対策 (データ漏えい防止)	なし
	ファイルフィルタ	読み取り
	アプリケーションコントロール	読み取り
	ICAP	読み取り
	VoIP	読み取り
	Webアプリケーションファイアウォール	読み取り
	DNSフィルタ	読み取り
	エンドポイントコントロール	読み取り
	ビデオフィルタ	読み取り
	仮想パッチ	なし
	Inline-CASB	なし
VPN		読み取り
Wifi＆スイッチ		読み取り
CLI診断コマンドの使用を許可 (system-diagnostics) (FortiOS 7.4.1以前)		
CLIコマンドの使用を許可 (FortiOS 7.4.2以降)	設定 (cli-config)	enable
	診断 (cli-diagnose)	disable
	実行 (cli-exec)	enable
	取得 (cli-get)	enable
	表示 (cli-show)	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		enable
タイムアウトしない		disable
オフライン(分)		10

No. 4

名前	CLIcommand_on
コメント	
アクセス権限	
セキュリティファブリック	読み取り
FortiView	読み取り
ユーザー＆デバイス	読み取り
ファイアウォール	カスタム

	ポリシー	読み取り
	アドレス	読み取り
	サービス	読み取り
	スケジュール	読み取り
	その他	読み取り
ログ & レポート		カスタム
	設定	読み取り
	データアクセス	読み取り
	レポートアクセス	読み取り
	脅威ウェイト	読み取り
ネットワーク		カスタム
	設定	読み取り
	パケットキャプチャ	読み取り
	ルーター	読み取り
システム		カスタム
	管理者ユーザ	読み取り
	FortiGuard更新	読み取り
	設定	読み取り
	メンテナンス	読み取り
セキュリティプロファイル		カスタム
	アンチウイルス	読み取り
	IPS	読み取り
	Webフィルタ	読み取り
	Eメールフィルタ	読み取り
	データ漏洩対策（データ漏えい防止）	読み取り
	ファイルフィルタ	読み取り
	アプリケーションコントロール	読み取り
	ICAP	読み取り
	VoIP	読み取り
	Webアプリケーションファイアウォール	読み取り
	DNSフィルタ	読み取り
	エンドポイントコントロール	読み取り
	ビデオフィルタ	読み取り
	仮想パッチ	なし
	Inline-CASB	なし
VPN		読み取り
Wifi＆スイッチ		読み取り
CLI診断コマンドの使用を許可（system-diagnostics）(FortiOS 7.4.1以前)		
CLIコマンドの使用を許可(FortiOS 7.4.2以降)	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		enable
タイムアウトしない		enable
オフライン(分)		0

No. 5

名前		CLIcommand_off
コメント		
アクセス権限		
セキュリティファブリック		読み書き
FortiView		読み書き
ユーザー＆デバイス		読み書き
ファイアウォール		カスタム
	ポリシー	読み書き
	アドレス	読み書き
	サービス	読み書き

	スケジュール	読み書き
	その他	読み書き
ログ & レポート		カスタム
	設定	読み書き
	データアクセス	読み書き
	レポートアクセス	読み書き
	脅威ウェイト	読み書き
ネットワーク		カスタム
	設定	読み書き
	パケットキャプチャ	読み書き
	ルーター	読み書き
システム		カスタム
	管理者ユーザ	読み書き
	FortiGuard更新	読み書き
	設定	読み書き
	メンテナンス	読み書き
セキュリティプロファイル		カスタム
	アンチウイルス	読み書き
	IPS	読み書き
	Webフィルタ	読み書き
	Eメールフィルタ	読み書き
	データ漏洩対策（データ漏えい防止）	読み書き
	ファイルフィルタ	読み書き
	アプリケーションコントロール	読み書き
	ICAP	読み書き
	VoIP	読み書き
	Webアプリケーションファイアウォール	読み書き
	DNSフィルタ	読み書き
	エンドポイントコントロール	読み書き
	ビデオフィルタ	読み書き
	仮想パッチ	なし
	Inline-CASB	なし
VPN		読み書き
Wifi＆スイッチ		読み書き
CLI診断コマンドの使用を許可（system-diagnostics）(FortiOS 7.4.1以前)		
CLIコマンドの使用を許可（FortiOS 7.4.2以降）	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		enable
タイムアウトしない		disable
オフライン(分)		10

No. 6

名前		CLIcommand_custom-allon
コメント		
アクセス権限		
セキュリティファブリック		なし
FortiView		なし
ユーザー＆デバイス		なし
ファイアウォール		なし
	ポリシー	
	アドレス	
	サービス	
	スケジュール	
	その他	
ログ & レポート		なし

	設定	
	データアクセス	
	レポートアクセス	
	脅威ウェイト	
ネットワーク		なし
	設定	
	パケットキャプチャ	
	ルーター	
システム		なし
	管理者ユーザ	
	FortiGuard更新	
	設定	
	メンテナンス	
セキュリティプロファイル		なし
	アンチウイルス	
	IPS	
	Webフィルタ	
	Eメールフィルタ	
	データ漏洩対策（データ漏えい防止）	
	ファイルフィルタ	
	アプリケーションコントロール	
	ICAP	
	VoIP	
	Webアプリケーションファイアウォール	
	DNSフィルタ	
	エンドポイントコントロール	
	ビデオフィルタ	
	仮想パッチ	
	Inline-CASB	
VPN		なし
Wifi＆スイッチ		なし
CLI診断コマンドの使用を許可（system-diagnostics）(FortiOS 7.4.1以前)		
CLIコマンドの使用を許可(FortiOS 7.4.2以降)	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		disable
タイムアウトしない		
オフライン(分)		

No. 7

名前		CLIcommand_custom-alloff
コメント		
アクセス権限		
セキュリティファブリック		なし
FortiView		なし
ユーザー＆デバイス		なし
ファイアウォール		なし
	ポリシー	
	アドレス	
	サービス	
	スケジュール	
	その他	
ログ＆レポート		なし
	設定	
	データアクセス	
	レポートアクセス	

	脅威ウェイト	
ネットワーク		なし
	設定	
	パケットキャプチャ	
	ルーター	
システム		なし
	管理者ユーザ	
	FortiGuard更新	
	設定	
	メンテナンス	
セキュリティプロファイル		なし
	アンチウイルス	
	IPS	
	Webフィルタ	
	Eメールフィルタ	
	データ漏洩対策（データ漏えい防止）	
	ファイルフィルタ	
	アプリケーションコントロール	
	ICAP	
	VoIP	
	Webアプリケーションファイアウォール	
	DNSフィルタ	
	エンドポイントコントロール	
	ビデオフィルタ	
	仮想パッチ	
	Inline-CASB	
VPN		なし
Wifi＆スイッチ		なし
CLI診断コマンドの使用を許可（system-diagnostics）(FortiOS 7.4.1以前)		
CLIコマンドの使用を許可（FortiOS 7.4.2以降）	設定（cli-config）	enable
	診断（cli-diagnose）	disable
	実行（cli-exec）	enable
	取得（cli-get）	enable
	表示（cli-show）	enable
スコープ		バーチャルドメイン
アイドルタイムアウトのオーバーライド		disable
タイムアウトしない		
オフライン(分)		

4. システム (SNMP v1v2c)

No. 1

コミュニティ名	test_1	
有効化済み	disable	
ホスト	IPアドレス	ホストタイプ
	0.0.0.0/0.0.0.0	クエリを受け入れトラップを送信する
	192.0.0.1/255.255.255.255	クエリのみ受け入れる
	192.0.0.2/255.255.255.255	トラップのみ送信する
	192.0.0.3/255.255.255.255	クエリを受け入れトラップを送信する
IPv6ホスト	IPアドレス	ホストタイプ
クエリ		
v1有効	enable	
ポート	161	
v2c有効	enable	
ポート	161	
トラップ		
v1有効	enable	
ローカルポート	162	
リモートポート	162	
v2c有効	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	enable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable
snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	disable	enable
APがアップ	enable	enable

APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

No. 2

コミュニティ名	test_2	
有効化済み	enable	
ホスト	IPアドレス	ホストタイプ
	0.0.0.0/0.0.0.0	クエリを受け入れトラップを送信する
	192.0.0.1/255.255.255.255	クエリのみ受け入れる
	192.0.0.2/255.255.255.255	トラップのみ送信する
	192.0.0.3/255.255.255.255	トラップのみ送信する
IPv6ホスト	IPアドレス	ホストタイプ
	fd00:xxxx:9d16::abcd/128	クエリを受け入れトラップを送信する
	fd00:xxxx:9d16::abce/128	クエリを受け入れトラップを送信する
クエリ		
v1有効	disable	
ポート	161	
v2c有効	disable	
ポート	161	
トラップ		
v1有効	disable	
ローカルポート	162	
リモートポート	162	
v2c有効	disable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	disable	enable
利用可能なメモリが不足	disable	enable
利用可能なログスペースが不足	disable	enable
インターフェースのIPアドレス変更	disable	enable
VPNトンネルがアップ	disable	enable
VPNトンネルがダウン	disable	enable
HAクラスタのステータスが変化	disable	enable
HAハートビートインターフェースの障害	disable	enable
IPSがアタックを検知	disable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	disable	enable
AVがオーバーサイズファイルを検知	disable	enable
AVがパターンに一致するファイルを検知	disable	enable
AVが断片化ファイルを検知	disable	enable
インターフェースIPの変更(FMトラップ)	disable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	disable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	disable	enable
HAクラスタメンバーがアップ	disable	enable
HAクラスタメンバーがダウン	disable	enable
エンティティ設定変更(RFC4133)	disable	enable
AVシステムがコンサーブモードへ移行	disable	enable

AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	disable	enable
AVがオーバーサイズファイルをブロック	disable	enable
IPSパッケージの更新	disable	enable
IPSネットワークバッファがフル	disable	enable
snmp-event::temperature-high	disable	enable
snmp-event::voltage-alert	disable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	disable	enable
FortiAnalyzerから切断	disable	enable
snmp-event::faz	disable	enable
APがアップ	disable	enable
APがダウン	disable	enable
FortiSwitchコントローラーセッションがアップ	disable	enable
FortiSwitchコントローラーセッションがダウン	disable	enable
ロードバランスリアルサーバがダウン	disable	enable
新しいデバイスを発見	disable	disable
CPU使用率が高いです。	disable	enable
DHCPアドレスの制限	disable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	disable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	disable	enable

No. 3

コミュニティ名	test_ 3	
有効化済み	enable	
ホスト	IPアドレス	ホストタイプ
	0.0.0.0/0.0.0.0	クエリを受け入れトラップを送信する
IPv6ホスト	IPアドレス	ホストタイプ
	fd00xxxx:9d16::abcd/128	クエリを受け入れトラップを送信する
クエリ		
v1有効	disable	
ポート	161	
v2c有効	enable	
ポート	161	
トラップ		
v1有効	disable	
ローカルポート	162	
リモートポート	162	
v2c有効	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable

設定変更(FMトラップ)	enable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable
snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	enable	enable
APがアップ	enable	enable
APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	enable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

5. システム (SNMP v3)

No. 1

ユーザー名	test_2	
有効化済み	disable	
セキュリティレベル		
認証	プライベート	
認証アルゴリズム	sha	
暗号化アルゴリズム	aes	
ホスト		
IPアドレス	0.0.0.0	
	0.0.0.0	
IPv6ホスト		
IPアドレス		
クエリ		
有効化済み	disable	
ポート	161	
トラップ		
有効化済み	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	disable	enable
利用可能なメモリが不足	disable	enable
利用可能なログスペースが不足	disable	enable
インターフェースのIPアドレス変更	disable	enable
VPNトンネルがアップ	disable	enable
VPNトンネルがダウン	disable	enable
HAクラスタのステータスが変化	disable	enable
HAハートビートインターフェースの障害	disable	enable
IPSがアタックを検知	disable	enable
IPSがアノマリを検知	disable	enable
AVがウイルスを検知	disable	enable
AVがオーバーサイズファイルを検知	disable	enable
AVがパターンに一致するファイルを検知	disable	enable
AVが断片化ファイルを検知	disable	enable
インターフェースIPの変更(FMトラップ)	disable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	disable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	disable	enable
HAクラスタメンバーがアップ	disable	enable
HAクラスタメンバーがダウン	disable	enable
エンティティ設定変更(RFC4133)	disable	enable
AVシステムがコンサーブモードへ移行	disable	enable
AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	disable	enable
AVがオーバーサイズファイルをブロック	disable	enable
IPSパッケージの更新	disable	enable
IPSネットワークバッファがフル	disable	enable
snmp-event::temperature-high	disable	enable
snmp-event::voltage-alert	disable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	disable	enable
FortiAnalyzerから切断	disable	enable
snmp-event::faz	disable	enable
APがアップ	disable	enable
APがダウン	disable	enable
FortiSwitchコントローラーセッションがアップ	disable	enable
FortiSwitchコントローラーセッションがダウン	disable	enable

ロードバランスリアルサーバがダウン	disable	enable
新しいデバイスを発見	disable	disable
CPU使用率が高いです。	disable	enable
DHCPアドレスの制限	disable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	disable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	disable	enable

No. 2

ユーザー名	test_1	
有効化済み	disable	
セキュリティレベル		
認証	認証なし	
認証アルゴリズム		
暗号化アルゴリズム		
ホスト		
IPアドレス	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
IPv6ホスト		
IPアドレス		
クエリ		
有効化済み	enable	
ポート	161	
トラップ		
有効化済み	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable
設定変更(FMトラップ)	enable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	enable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable

snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	disable	enable
APがアップ	enable	enable
APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

No. 3

ユーザー名	test_3	
有効化済み	disable	
セキュリティレベル		
認証	非プライベート	
認証アルゴリズム	sha256	
暗号化アルゴリズム		
ホスト		
IPアドレス	0.0.0.0	
	0.0.0.0	
IPv6ホスト		
IPアドレス		
クエリ		
有効化済み	enable	
ポート	161	
トラップ		
有効化済み	disable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	disable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	disable	enable
VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	disable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	disable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	disable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	disable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	disable	enable
インターフェースIPの変更(FMトラップ)	enable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	disable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	disable	enable

エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	disable	enable
AVバイパスの発生	enable	enable
AVがオーバーサイズファイルをパス	disable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	disable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	disable	enable
snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	disable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	disable	enable
APがアップ	disable	enable
APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	disable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	disable	enable
新しいデバイスを発見	enable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	disable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	disable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

No. 4

ユーザー名	test_4	
有効化済み	enable	
セキュリティレベル		
認証	認証なし	
認証アルゴリズム		
暗号化アルゴリズム		
ホスト		
IPアドレス	0.0.0.0	
	0.0.0.0	
IPv6ホスト		
IPアドレス	fd00:xxxx:9d16::abcd	
クエリ		
有効化済み	disable	
ポート	161	
トラップ		
有効化済み	disable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	disable	enable
利用可能なメモリが不足	disable	enable
利用可能なログスペースが不足	disable	enable
インターフェースのIPアドレス変更	disable	enable
VPNトンネルがアップ	disable	enable
VPNトンネルがダウン	disable	enable
HAクラスタのステータスが変化	disable	enable
HAハートビートインターフェースの障害	disable	enable
IPSがアタックを検知	disable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	disable	enable
AVがオーバーサイズファイルを検知	disable	enable
AVがパターンに一致するファイルを検知	disable	enable

AVが断片化ファイルを検知	disable	enable
インターフェースIPの変更(FMトラップ)	disable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	disable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	disable	enable
HAクラスタメンバーがアップ	disable	enable
HAクラスタメンバーがダウン	disable	enable
エンティティ設定変更(RFC4133)	disable	enable
AVシステムがコンサーブモードへ移行	disable	enable
AVバイパスの発生	disable	enable
AVがオーバーサイズファイルをパス	disable	enable
AVがオーバーサイズファイルをブロック	disable	enable
IPSパッケージの更新	disable	enable
IPSネットワークバッファがフル	disable	enable
snmp-event::temperature-high	disable	enable
snmp-event::voltage-alert	disable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	disable	enable
FortiAnalyzerから切断	disable	enable
snmp-event::faz	disable	enable
APがアップ	disable	enable
APがダウン	disable	enable
FortiSwitchコントローラーセッションがアップ	disable	enable
FortiSwitchコントローラーセッションがダウン	disable	enable
ロードバランスリアルサーバがダウン	disable	enable
新しいデバイスを発見	disable	disable
CPU使用率が高いです。	disable	enable
DHCPアドレスの制限	disable	enable
IPプールの利用について (About IP pool usage)	disable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	disable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	disable	enable

No. 5

ユーザー名	test_5	
有効化済み	enable	
セキュリティレベル		
認証	認証なし	
認証アルゴリズム		
暗号化アルゴリズム		
ホスト		
IPアドレス	192.168.20.0	
	192.168.20.10	
IPv6ホスト		
IPアドレス	fd00:xxxx:9d16::abcd	
	fd00:xxxx9d16::abce	
クエリ		
有効化済み	enable	
ポート	161	
トラップ		
有効化済み	enable	
ローカルポート	162	
リモートポート	162	
SNMP イベント		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
CPU負荷の高騰	enable	enable
利用可能なメモリが不足	enable	enable
利用可能なログスペースが不足	enable	enable
インターフェースのIPアドレス変更	enable	enable

VPNトンネルがアップ	enable	enable
VPNトンネルがダウン	enable	enable
HAクラスタのステータスが変化	enable	enable
HAハートビートインターフェースの障害	enable	enable
IPSがアタックを検知	enable	enable
IPSがアノマリを検知	enable	enable
AVがウイルスを検知	enable	enable
AVがオーバーサイズファイルを検知	enable	enable
AVがパターンに一致するファイルを検知	enable	enable
AVが断片化ファイルを検知	enable	enable
インターフェースIPの変更(FMトラップ)	enable	enable
設定変更(FMトラップ)	disable	disable
BGP FSMが Established ステートに移行	enable	enable
BGP FSMが高ナンバーから低ナンバーのステートに移行	enable	enable
HAクラスタメンバーがアップ	enable	enable
HAクラスタメンバーがダウン	enable	enable
エンティティ設定変更(RFC4133)	enable	enable
AVシステムがコンサーブモードへ移行	enable	enable
AVバイパスの発生	enable	enable
AVがオーバーサイズファイルをパス	enable	enable
AVがオーバーサイズファイルをブロック	enable	enable
IPSパッケージの更新	enable	enable
IPSネットワークバッファがフル	enable	enable
snmp-event::temperature-high	enable	enable
snmp-event::voltage-alert	enable	enable
snmp-event::power-supply-failure	disable	
snmp-event::power-supply	enable	enable
FortiAnalyzerから切断	enable	enable
snmp-event::faz	enable	enable
APがアップ	enable	enable
APがダウン	enable	enable
FortiSwitchコントローラーセッションがアップ	enable	enable
FortiSwitchコントローラーセッションがダウン	enable	enable
ロードバランスリアルサーバがダウン	enable	enable
新しいデバイスを発見	disable	disable
CPU使用率が高いです。	enable	enable
DHCPアドレスの制限	enable	enable
IPプールの利用について (About IP pool usage)	enable	enable
仮想OSPF以外のネイバーの状態に変化があった場合、トラップ送信	enable	enable
OSPF仮想ネイバーの状態に変化があった場合、トラップを送信	enable	enable

6. システム (VDOM)

No. 1

バーチャルドメイン	root		
タイプ	トラフィック		
NGFWモード	プロファイルベース		
セントラルNAT	disable		
WiFiの国/地域	UnitedStates		
コメント			
ワークフローマネジメント			
ポリシー変更サマリ	必須		
ポリシーはデフォルトで期限切れです	enable		
後に期限切れ	30		
リソース割り当て			
リソース	グローバルの最大値 (参考) FortiOS ver. 7.2.8 の既定値	最大値のオーバーライド	保証
アクティブセッション	制限設定なし	0	0
ポリシー & オブジェクト			
ファイアウォールポリシー	11024	0	0
ファイアウォールアドレス	16024	0	0
ファイアウォールアドレスグループ	5000	0	0
ファイアウォール カスタムサービス	制限設定なし	0	0
ファイアウォール サービスグループ	制限設定なし	0	0
ファイアウォール ワンタイムスケジュール	制限設定なし	0	0
ファイアウォール繰り返しスケジュール	制限設定なし	0	0
ユーザ & デバイス			
ユーザ	制限設定なし	0	0
ユーザグループ	制限設定なし	0	0
同時Explicitプロキシユーザ	1000	0	0
VPN			
SSL-VPN	制限設定なし	0	0
VPN IPsec フェーズ1 トンネル	200	0	0
VPN IPsec フェーズ2 トンネル	200	0	0
VPN IPsec フェーズ1 インターフェーストンネル	制限設定なし	0	0
VPN IPsec フェーズ2 インターフェーストンネル	制限設定なし	0	0
ダイヤルアップ トンネル	制限設定なし	0	0
ログ & レポート			
ログディスククォータ (MiB)	制限設定なし (MiB)		

7. ネットワーク (概要)

インターフェース

下表は次のインターフェースを記載しています。

802.3ad アグリゲート
トンネルインターフェース (PPPoEインターフェースのみ)
SSL-VPNトンネル
VLAN
ハードウェアスイッチ
ループバックインターフェース
冗長インターフェース
物理インターフェース

名前	エイリアス	タイプ	メンバー	IP/ネットマスク	ステータス	バーチャルドメイン	コメント
fortilink		802.3ad アグリゲート	a	192.1.2.254/255.255.255.0	有効化済み	root	
test_802.3ad_3	test_802.3ad_3	802.3ad アグリゲート		0.0.0.0/0.0.0.0	有効化済み	root	802.3ad test
Interface3		SSL-VPNトンネル			有効化済み	root	
dhcptest		VLAN			有効化済み	root	
Interface01	エイリアス	VLAN			有効化済み	root	
Interface2		VLAN			有効化済み	root	
onearmtest	onearmtest01	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_1	test_1	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_9	test_9	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_IPMA_3	test_IPMA_3	VLAN		192.2.0.254/255.255.255.0	有効化済み	root	
VLAN_test_1	VLAN_test_1	VLAN		192.3.0.0/255.0.0.0	有効化済み	root	
lan		ハードウェアスイッチ	lan1, lan2	192.168.3.4/255.255.255.0	有効化済み	root	
loopback_test_4	loopback_test_4	ループバックインターフェース		192.168.5.6/255.255.0.0	有効化済み	root	
test_25	test_25	冗長インターフェース			有効化済み	root	
lan1		物理インターフェース			有効化済み	root	
lan2		物理インターフェース			有効化済み	root	
lan3	test	物理インターフェース		192.168.1.10/255.255.255.0	有効化済み	root	
modem		物理インターフェース			無効化済み	root	
wan	qa.test	物理インターフェース		192.168.11.22/255.255.255.0	有効化済み	root	

DNS

プライマリDNSサーバー	192.45.45.45
セカンダリDNSサーバー	192.46.46.46
ローカルドメイン名	saytech
	saytech_2
DNSプロトコル	
DNS (UDP/53)	enable
TLS (TCP/853)	disable
HTTPS (TCP/443)	enable
SSL証明書	Fortinet_Factory_Backup
サーバホスト名	xxxx.fortinet.net
	xxxx2.fortinet.net
IPv6 DNS設定	
プライマリDNSサーバ	fd00:xxxx:9d16::abcd
セカンダリDNSサーバ	fd00:xxxx:9d16::abce

ダイナミックDNS

ドメイン	パブリックIPアドレスを使用	インターフェース
saytech.xxxx.com	enable	fortilink
		Interface01
		Interface2

abcde.xxxx-zone.com	disable	test_1

スタティックルート

IPv4

宛先	ゲートウェイIP	インターフェース	ステータス	コメント

IPv6

宛先	ゲートウェイIP	インターフェース	ステータス	コメント

8. セキュリティプロファイル（アンチウイルス）

No. 1

名前	g-default
コメント	Scan files and block viruses.
機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	disable	disable	ー	
SMTP	ブロック	disable	disable	enable	
POP3	ブロック	disable	disable	enable	
IMAP	ブロック	disable	disable	enable	
FTP	ブロック	disable	disable	ー	ー
CIFS	disable	disable	disable	ー	ー
MAPI					ー
SSH				ー	ー

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

No. 2

名前	g-sniffer-profile
コメント	Scan files and monitor viruses.

機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	disable	disable	—	
SMTP	ブロック	disable	disable	enable	
POP3	ブロック	disable	disable	enable	
IMAP	ブロック	disable	disable	enable	
FTP	ブロック	disable	disable	—	—
CIFS	disable	disable	disable	—	—
MAPI					—
SSH				—	—

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

No. 3

名前	g-wifi-default
コメント	Default configuration for offloading WiFi traffic.
機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	disable	disable	—	
SMTP	ブロック	disable	disable	enable	
POP3	ブロック	disable	disable	enable	
IMAP	ブロック	disable	disable	enable	
FTP	ブロック	disable	disable	—	—
CIFS	disable	disable	disable	—	—
MAPI					—
SSH				—	—

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

9. セキュリティプロファイル (WEBフィルタ)

No. 1

名前	g-default
コメント	Default web filtering.
機能セット	フローベース

FortiGuardカテゴリベースのフィルタ

ID	グループ	カテゴリ名	アクション
1	g01 Potentially Liable	Drug Abuse	モニタ
3	g01 Potentially Liable	Hacking	モニタ
4	g01 Potentially Liable	Illegal or Unethical	モニタ
5	g01 Potentially Liable	Discrimination	モニタ
6	g01 Potentially Liable	Explicit Violence	モニタ
12	g01 Potentially Liable	Extremist Groups	モニタ
59	g01 Potentially Liable	Proxy Avoidance	モニタ
62	g01 Potentially Liable	Plagiarism	モニタ
83	g01 Potentially Liable	Child Sexual Abuse	ブロック
96	g01 Potentially Liable	Terrorism	ブロック
98	g01 Potentially Liable	Crypto Mining	ブロック
99	g01 Potentially Liable	Potentially Unwanted Program	ブロック
2	g02 Adult/Mature Content	Alternative Beliefs	ブロック
7	g02 Adult/Mature Content	Abortion	ブロック
8	g02 Adult/Mature Content	Other Adult Materials	ブロック
9	g02 Adult/Mature Content	Advocacy Organizations	ブロック
11	g02 Adult/Mature Content	Gambling	ブロック
13	g02 Adult/Mature Content	Nudity and Risque	ブロック
14	g02 Adult/Mature Content	Pornography	ブロック
15	g02 Adult/Mature Content	Dating	ブロック
16	g02 Adult/Mature Content	Weapons (Sales)	ブロック
57	g02 Adult/Mature Content	Marijuana	ブロック
63	g02 Adult/Mature Content	Sex Education	ブロック
64	g02 Adult/Mature Content	Alcohol	ブロック
65	g02 Adult/Mature Content	Tobacco	ブロック
66	g02 Adult/Mature Content	Lingerie and Swimsuit	ブロック
67	g02 Adult/Mature Content	Sports Hunting and War Games	ブロック
26	g05 Security Risk	Malicious Websites	ブロック
61	g05 Security Risk	Phishing	ブロック
86	g05 Security Risk	Spam URLs	ブロック
88	g05 Security Risk	Dynamic DNS	ブロック
90	g05 Security Risk	Newly Observed Domain	ブロック
91	g05 Security Risk	Newly Registered Domain	ブロック
0	g21 Unrated	Unrated	ブロック

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	
オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分

サーチエンジン

Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	

スタティックURLフィルタ

無効なURLをブロック	
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック		disable		
コンテンツフィルタ				
パターンタイプ	パターン	言語	アクション	ステータス
レーティングオプション				
Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)				
ドメインまたはIPアドレスでURLをレーティング				
プロキシオプション				
HTTP POST アクション		許可		
Javaアプレットを削除				
ActiveXの削除				
Cookieを削除				

No. 2

名前		g-sniffer-profile	
コメント		Monitor web traffic.	
機能セット		フローベース	
FortiGuardカテゴリベースのフィルタ			
ID	グループ	カテゴリ名	アクション
1	g01 Potentially Liable	Drug Abuse	モニタ
3	g01 Potentially Liable	Hacking	モニタ
4	g01 Potentially Liable	Illegal or Unethical	モニタ
5	g01 Potentially Liable	Discrimination	モニタ
6	g01 Potentially Liable	Explicit Violence	モニタ
12	g01 Potentially Liable	Extremist Groups	モニタ
59	g01 Potentially Liable	Proxy Avoidance	モニタ
62	g01 Potentially Liable	Plagiarism	モニタ
83	g01 Potentially Liable	Child Sexual Abuse	モニタ
96	g01 Potentially Liable	Terrorism	モニタ
98	g01 Potentially Liable	Crypto Mining	モニタ
99	g01 Potentially Liable	Potentially Unwanted Program	モニタ
2	g02 Adult/Mature Content	Alternative Beliefs	モニタ
7	g02 Adult/Mature Content	Abortion	モニタ
8	g02 Adult/Mature Content	Other Adult Materials	モニタ
9	g02 Adult/Mature Content	Advocacy Organizations	モニタ
11	g02 Adult/Mature Content	Gambling	モニタ
13	g02 Adult/Mature Content	Nudity and Risque	モニタ
14	g02 Adult/Mature Content	Pornography	モニタ
15	g02 Adult/Mature Content	Dating	モニタ
16	g02 Adult/Mature Content	Weapons (Sales)	モニタ
57	g02 Adult/Mature Content	Marijuana	モニタ
63	g02 Adult/Mature Content	Sex Education	モニタ
64	g02 Adult/Mature Content	Alcohol	モニタ
65	g02 Adult/Mature Content	Tobacco	モニタ
66	g02 Adult/Mature Content	Lingerie and Swimsuit	モニタ
67	g02 Adult/Mature Content	Sports Hunting and War Games	モニタ
19	g04 Bandwidth Consuming	Freeware and Software Downloads	モニタ
24	g04 Bandwidth Consuming	File Sharing and Storage	モニタ
25	g04 Bandwidth Consuming	Streaming Media and Download	モニタ
72	g04 Bandwidth Consuming	Peer-to-peer File Sharing	モニタ
75	g04 Bandwidth Consuming	Internet Radio and TV	モニタ
76	g04 Bandwidth Consuming	Internet Telephony	モニタ
26	g05 Security Risk	Malicious Websites	モニタ
61	g05 Security Risk	Phishing	モニタ
86	g05 Security Risk	Spam URLs	モニタ
88	g05 Security Risk	Dynamic DNS	モニタ
90	g05 Security Risk	Newly Observed Domain	モニタ
91	g05 Security Risk	Newly Registered Domain	モニタ

17	g06 General Interest - Personal	Advertising	モニタ
18	g06 General Interest - Personal	Brokerage and Trading	モニタ
20	g06 General Interest - Personal	Games	モニタ
23	g06 General Interest - Personal	Web-based Email	モニタ
28	g06 General Interest - Personal	Entertainment	モニタ
29	g06 General Interest - Personal	Arts and Culture	モニタ
30	g06 General Interest - Personal	Education	モニタ
33	g06 General Interest - Personal	Health and Wellness	モニタ
34	g06 General Interest - Personal	Job Search	モニタ
35	g06 General Interest - Personal	Medicine	モニタ
36	g06 General Interest - Personal	News and Media	モニタ
37	g06 General Interest - Personal	Social Networking	モニタ
38	g06 General Interest - Personal	Political Organizations	モニタ
39	g06 General Interest - Personal	Reference	モニタ
40	g06 General Interest - Personal	Global Religion	モニタ
42	g06 General Interest - Personal	Shopping	モニタ
44	g06 General Interest - Personal	Society and Lifestyles	モニタ
46	g06 General Interest - Personal	Sports	モニタ
47	g06 General Interest - Personal	Travel	モニタ
48	g06 General Interest - Personal	Personal Vehicles	モニタ
54	g06 General Interest - Personal	Dynamic Content	モニタ
55	g06 General Interest - Personal	Meaningless Content	モニタ
58	g06 General Interest - Personal	Folklore	モニタ
68	g06 General Interest - Personal	Web Chat	モニタ
69	g06 General Interest - Personal	Instant Messaging	モニタ
70	g06 General Interest - Personal	Newsgroups and Message Boards	モニタ
71	g06 General Interest - Personal	Digital Postcards	モニタ
77	g06 General Interest - Personal	Child Education	モニタ
78	g06 General Interest - Personal	Real Estate	モニタ
79	g06 General Interest - Personal	Restaurant and Dining	モニタ
80	g06 General Interest - Personal	Personal Websites and Blogs	モニタ
82	g06 General Interest - Personal	Content Servers	モニタ
85	g06 General Interest - Personal	Domain Parking	モニタ
87	g06 General Interest - Personal	Personal Privacy	モニタ
89	g06 General Interest - Personal	Auction	モニタ
31	g07 General Interest - Business	Finance and Banking	モニタ
41	g07 General Interest - Business	Search Engines and Portals	モニタ
43	g07 General Interest - Business	General Organizations	モニタ
49	g07 General Interest - Business	Business	モニタ
50	g07 General Interest - Business	Information and Computer Security	モニタ
51	g07 General Interest - Business	Government and Legal Organizations	モニタ
52	g07 General Interest - Business	Information Technology	モニタ
53	g07 General Interest - Business	Armed Forces	モニタ
56	g07 General Interest - Business	Web Hosting	モニタ
81	g07 General Interest - Business	Secure Websites	モニタ
84	g07 General Interest - Business	Web-based Applications	モニタ
92	g07 General Interest - Business	Charitable Organizations	モニタ
93	g07 General Interest - Business	Remote Access	モニタ
94	g07 General Interest - Business	Web Analytics	モニタ
95	g07 General Interest - Business	Online Meeting	モニタ
97	g07 General Interest - Business	URL Shortening	モニタ
100	g07 General Interest - Business	Artificial Intelligence Technology	モニタ
101	g07 General Interest - Business	Cryptocurrency	モニタ
0	g21 Unrated	Unrated	モニタ

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	

オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分
サーチエンジン	
Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	
スタティックURLフィルタ	
無効なURLをブロック	
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック	disable
コンテンツフィルタ	

パターンタイプ	パターン	言語	アクション	ステータス

レーティングオプション	
Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)	Block all websites (disable)
ドメインまたはIPアドレスでURLをレーティング	disable
プロキシオプション	
HTTP POST アクション	許可
Javaアプレットを削除	
ActiveXの削除	
Cookieを削除	

No. 3

名前	g-wifi-default
コメント	Default configuration for offloading WiFi traffic.
機能セット	フローベース
FortiGuardカテゴリベースのフィルタ	

ID	グループ	カテゴリ名	アクション
1	g01 Potentially Liable	Drug Abuse	モニタ
3	g01 Potentially Liable	Hacking	モニタ
4	g01 Potentially Liable	Illegal or Unethical	モニタ
5	g01 Potentially Liable	Discrimination	モニタ
6	g01 Potentially Liable	Explicit Violence	モニタ
12	g01 Potentially Liable	Extremist Groups	モニタ
59	g01 Potentially Liable	Proxy Avoidance	モニタ
62	g01 Potentially Liable	Plagiarism	モニタ
83	g01 Potentially Liable	Child Sexual Abuse	ブロック
96	g01 Potentially Liable	Terrorism	ブロック
98	g01 Potentially Liable	Crypto Mining	ブロック
99	g01 Potentially Liable	Potentially Unwanted Program	ブロック
2	g02 Adult/Mature Content	Alternative Beliefs	ブロック
7	g02 Adult/Mature Content	Abortion	ブロック
8	g02 Adult/Mature Content	Other Adult Materials	ブロック
9	g02 Adult/Mature Content	Advocacy Organizations	ブロック
11	g02 Adult/Mature Content	Gambling	ブロック
13	g02 Adult/Mature Content	Nudity and Risque	ブロック
14	g02 Adult/Mature Content	Pornography	ブロック
15	g02 Adult/Mature Content	Dating	ブロック
16	g02 Adult/Mature Content	Weapons (Sales)	ブロック
57	g02 Adult/Mature Content	Marijuana	ブロック
63	g02 Adult/Mature Content	Sex Education	ブロック
64	g02 Adult/Mature Content	Alcohol	ブロック
65	g02 Adult/Mature Content	Tobacco	ブロック
66	g02 Adult/Mature Content	Lingerie and Swimsuit	ブロック

67	g02 Adult/Mature Content	Sports Hunting and War Games	ブロック
26	g05 Security Risk	Malicious Websites	ブロック
61	g05 Security Risk	Phishing	ブロック
86	g05 Security Risk	Spam URLs	ブロック
88	g05 Security Risk	Dynamic DNS	ブロック
90	g05 Security Risk	Newly Observed Domain	ブロック
91	g05 Security Risk	Newly Registered Domain	ブロック
0	g21 Unrated	Unrated	ブロック

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	
オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分

サーチエンジン

Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	

スタティックURLフィルタ

無効なURLをブロック	enable
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック	disable
コンテンツフィルタ	

パターンタイプ	パターン	言語	アクション	ステータス

レーティングオプション

Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)	
ドメインまたはIPアドレスでURLをレーティング	

プロキシオプション

HTTP POST アクション	許可
Javaアプレットを削除	disable
ActiveXの削除	disable
Cookieを削除	disable

10. 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）

No. 1

名前		g-default
コメント		Monitor all applications.
ネットワークプロトコルの強制		disable
ポート	プロトコルの強制	違反アクション

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細			アクション
1	アプリケーション (ID):			許可
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:		
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	disable
DNSトラフィックの許可とログ	enable
HTTPベースアプリケーションの差し替えメッセージ	enable

No. 2

名前		g-sniffer-profile
コメント		Monitor all applications.
ネットワークプロトコルの強制		disable
ポート	プロトコルの強制	違反アクション

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細			アクション
1	アプリケーション (ID):			許可
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:		
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	disable
DNSトラフィックの許可とログ	
HTTPベースアプリケーションの差し替えメッセージ	enable

No. 3

名前		g-wifi-default
コメント		Default configuration for offloading WiFi traffic.
ネットワークプロトコルの強制		disable
ポート	プロトコルの強制	違反アクション

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細			アクション
1	アプリケーション (ID):			許可
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:		
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	disable
DNSトラフィックの許可とログ	enable
HTTPベースアプリケーションの差し替えメッセージ	enable

11. セキュリティプロファイル（侵入防止）（概要）

IPSセンサー

名前	コメント
g-default	Prevent critical attacks.
g-sniffer-profile	Monitor IPS attacks.
g-wifi-default	Default configuration for offloading WiFi traffic.

カスタムIPSシグネチャ

ID	名前	シグネチャ	コメント

12. セキュリティプロファイル（侵入防止）

IPSセンサー

No. 1

名前	g-default
コメント	Prevent critical attacks.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト　（隔離時間　日　時間　分） Action : default　Log : enable　Quarantine : none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	■■■□□ (medium) ■■■■□ (high) ■■■■■ (critical)
プロトコル	all
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間（秒）	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

No. 2

名前	g-sniffer-profile
コメント	Monitor IPS attacks.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト　（隔離時間　日　時間　分） Action : default　Log : enable　Quarantine : none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	■■■□□ (medium) ■■■■□ (high) ■■■■■ (critical)
プロトコル	all
OS	all
アプリケーション	all
ステータス	all

アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間 (秒)	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

No. 3

名前	g-wifi-default
コメント	Default configuration for offloading WiFi traffic.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト (隔離時間 日 時間 分)
	Action : default Log : enable Quarantine : none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	■■■□□ (medium) ■■■■□ (high) ■■■■■ (critical)
プロトコル	all
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間 (秒)	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

・本設定仕様書サンプルはFortiGate 40Fから採取した
"full-configuration"のファイルを使用して作成しております。
・一部固有のIPアドレスが記述された部分はマスクしております。

FortiGate VDOM 設定仕様書

仕様書商事 様

FortiGate ホスト名	FortiGate-40F (VDOM root)
作成日	20YY年MM月DD日
作成者	セイ･テクノロジーズ

セイ･テクノロジーズ株式会社

(住所)

改訂履歴

版数	日付	内容	担当者

目次

1. システム（概要）

ファームウェアバージョン、表示機能設定を記載しています。

2. ネットワーク（概要）

ネットワークのインターフェース、およびスタティックルートの概要、DNSを記載しています。

3. ネットワーク（物理インターフェース）

ネットワークの物理インターフェースの詳細を記載しています。

4. ネットワーク（インターフェース）

ネットワークの下記インターフェースの詳細を記載しています。
802.3ad アグリゲート
PPPoEインターフェース
SSL-VPNトンネル
VLAN
ハードウェアスイッチ
ループバックインターフェース
冗長インターフェース

5. ネットワーク（スタティックルート）

ネットワークのスタティックルートの詳細を記載しています。

6. ネットワーク（SD-WAN）（概要）

SD-WANゾーン、SD-WANルール、およびパフォーマンスSLAの概要を記載しています。

7. ネットワーク（SD-WAN ルール）

SD-WANルールの詳細を記載しています。

8. ネットワーク（SD-WAN パフォーマンスSLA）

パフォーマンスSLAの詳細を記載しています。

9. ポリシー&オブジェクト（概要）

ポリシー&オブジェクトのファイアウォールポリシー、およびアドレスグループ、アドレス、IPv6アドレステンプレート、サービス、スケジュール、DANTとバーチャルIP、IPプールの概要を記載しています。

10. ポリシー&オブジェクト（ファイアウォールポリシー）

ポリシー&オブジェクトのファイアウォールポリシーの詳細を記載しています。

11. ポリシー&オブジェクト（アドレス）

ポリシー&オブジェクトのアドレスグループ、およびアドレス、IPv6アドレステンプレートの詳細を記載しています。

12. ポリシー&オブジェクト（サービス）

ポリシー&オブジェクトのサービスの詳細を記載しています。

13. ポリシー&オブジェクト（バーチャルIP）

ポリシー&オブジェクトのバーチャルIPの詳細を記載しています。

14. ポリシー&オブジェクト（IPプール）

ポリシー&オブジェクトのIPプールの詳細を記載しています。

15. セキュリティプロファイル（アンチウイルス）

セキュリティプロファイルのアンチウイルスの詳細を記載しています。

16. セキュリティプロファイル（WEBフィルタ）

セキュリティプロファイルのWEBフィルタの詳細を記載しています。

17. 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）

セキュリティプロファイルのアプリケーションコントロールの詳細を記載しています。

18. セキュリティプロファイル（侵入防止）（概要）

セキュリティプロファイルの侵入防止の概要を記載しています。

19. セキュリティプロファイル（侵入防止）

セキュリティプロファイルの侵入防止の詳細を記載しています。

20. セキュリティプロファイル（SSL/SSHインスペクション）（概要）

セキュリティプロファイルのSSL/SSHインスペクションの概要を記載しています。

21. セキュリティプロファイル（SSL/SSHインスペクション）

セキュリティプロファイルのSSL/SSHインスペクションの詳細を記載しています。

22. VPN（概要）

IPsec VPN、およびSSL-VPNの概要を記載しています。

23. VPN（IPsecトンネル）

VPNのIPsecトンネルの詳細を記載しています。

24. VPN（ハブ&スポーク トポロジ）

ハブ＆スポーク トポロジのVPNに関連する設定の一つであるBGPについて記載しています。

25. VPN（SSL-VPN設定）

SSL-VPNの設定を記載しています。

26. VPN（SSL-VPNポータル）

VPNのSSL-VPNポータルの詳細を記載しています。

◆商標

FortiGateおよびFortiGateの製品名は、Fortinet, Inc.の米国およびその他の国における商標または登録商標です。

1. システム（概要）

機種情報

ファームウェアバージョン	FGT40F-7.4.7-FW-build2731-250120
Alias	FortiGate-40F

表示機能設定

コア機能		(参考) FortiOS ver. 7.4.7 の既定値 ※モデルによって異なる場合があります
IPsec VPN	enable	enable
SSL-VPN	enable	disable
Wifiコントローラー	enable	enable
スイッチコントローラー	enable	enable
高度なルーティング	enable	enable
セキュリティ機能		
DNSフィルタ	enable	enable
Explicitプロキシ	disable	disable
Eメールフィルタ	enable	disable
Inline-CASB	enable	disable
Webアプリケーションファイアウォール	enable	disable
Webフィルタ	enable	enable
アプリケーションコントロール	enable	enable
アンチウイルス	enable	enable
ゼロトラストネットワークアクセス	disable	enable
データ漏洩対策	enable	disable
ビデオフィルタ	enable	enable
ファイルフィルタ	enable	enable
仮想パッチ	enable	disable
侵入防止	enable	enable
その他の機能		
DNSデータベース	enable	disable
DoSポリシー	enable	enable
Eメール収集	enable	disable
FortiExtender	enable	disable
ICAP	enable	disable
Implicit Firewall ポリシー	enable	enable
Local Inポリシー	enable	disable
SD-WANインターフェース	enable	enable
SSL-VPNパーソナルブックマーク	enable	disable
SSL-VPNレルム	enable	disable
VoIP	enable	disable
トラフィックシェイピング	enable	enable
ポリシーの詳細オプション	enable	disable
ポリシーベース IPsec VPN	enable	disable
ポリシー免責事項	enable	disable
マルチキャストポリシー	enable	disable
ロードバランス	enable	disable
運用技術(OT)	enable	disable
脅威ウェイトトラッキング	enable	enable
高度なワイヤレス機能	enable	disable
動的なデバイスとOSの識別	enable	disable
複数インターフェースポリシー	enable	disable
名前なしポリシー許可	enable	disable

2. ネットワーク (概要)

インターフェース

下表は次のインターフェースを記載しています。

802.3ad アグリゲート
トンネルインターフェース (PPPoEインターフェースのみ)
SSL-VPNトンネル
VLAN
ハードウェアスイッチ
ループバックインターフェース
冗長インターフェース
物理インターフェース

名前	エイリアス	タイプ	メンバー	IP/ネットマスク	ステータス	バーチャルドメイン	コメント
fortilink		802.3ad アグリゲート	a	192.168.2.3/255.255.255.0	有効化済み	root	
test_802.3ad_3	test_802.3ad_3	802.3ad アグリゲート		0.0.0.0/0.0.0.0	有効化済み	root	802.3ad test
Interface3		SSL-VPNトンネル			有効化済み	root	
dhcptest		VLAN			有効化済み	root	
Interface01	エイリアス	VLAN			有効化済み	root	
Interface2		VLAN			有効化済み	root	
onearmtest	onearmtest01	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_1	test_1	VLAN		0.0.0.0/0.0.0.0	有効化済み	root	
test_11	test_11	VLAN		0.0.0.0/0.0.0.0	無効化済み	root	
test_23	test_23	VLAN		0.0.0.0/0.0.0.0	無効化済み	root	
test_IPMA_3	test_IPMA_3	VLAN		192.168.0.254/255.255.255.0	有効化済み	root	
VLAN_test_1	VLAN_test_1	VLAN		192.168.0.0/255.0.0.0	有効化済み	root	
VLAN_test_2	VLAN_test_2	VLAN			有効化済み	root	
lan		ハードウェアスイッチ	lan1, lan2	192.168.99.100/255.255.255.0	有効化済み	root	
loopback_test_3	loopback_test_3	ループバックインターフェース		0.0.0.0/0.0.0.0	有効化済み	root	
loopback_test_4	loopback_test_4	ループバックインターフェース		192.168.1.0/255.255.0.0	有効化済み	root	
test_24	test_24	冗長インターフェース		0.0.0.0/0.0.0.0	有効化済み	root	
lan1		物理インターフェース			有効化済み	root	
lan2		物理インターフェース			有効化済み	root	
lan3	test	物理インターフェース		192.168.1.2/255.255.255.0	有効化済み	root	
modem		物理インターフェース			無効化済み	root	
wan	test	物理インターフェース		192.168.1.254/255.255.255.0	有効化済み	root	

DNS

プライマリDNSサーバー	
セカンダリDNSサーバー	
ローカルドメイン名	
DNSプロトコル	
DNS (UDP/53)	
TLS (TCP/853)	
HTTPS (TCP/443)	
SSL証明書	
サーバホスト名	
IPv6 DNS設定	
プライマリDNSサーバ	
セカンダリDNSサーバ	

ダイナミックDNS

ドメイン	パブリックIPアドレスを使用	インターフェース

スタティックルート

IPv4

宛先	ゲートウェイIP	インターフェース	ステータス	コメント
0.0.0.0/0.0.0.0	192.168.99.100	lan	enable	
0.0.0.0/0.0.0.0		l2t.root	enable	
917640	0.0.0.0	test_1	enable	インターネットサービステスト
393320	192.168.99.1	lan	enable	インターネットサービステスト 2
0.0.0.0/0.0.0.0	192.168.99.2	test_1	enable	
4063233	0.0.0.0	test_1	enable	
10.20.20.0/255.255.255.0	0.0.0.0	lan	enable	
サイト 2 _remote		サイト 2	enable	VPN: サイト 2 (Created by VPN wizard)
サイト 2 _remote			enable	VPN: サイト 2 (Created by VPN wizard)
N1_remote			enable	VPN: N1 (Created by VPN wizard)
xcvbnm_remote		xcvbnm	enable	VPN: xcvbnm (Created by VPN wizard)
xcvbnm_remote			enable	VPN: xcvbnm (Created by VPN wizard)
pojpoj,_remote		pojpoj,	enable	VPN: pojpoj, (Created by VPN wizard)
pojpoj,_remote			enable	VPN: pojpoj, (Created by VPN wizard)
サイト全埋_remote			enable	VPN: サイト全埋 (Created by VPN wizard)

IPv6

宛先	ゲートウェイIP	インターフェース	ステータス	コメント
12:xx::/128	12:xx::	test_1	enable	

3. ネットワーク（物理インターフェース）

本章では、一部の設定値を次の凡例に従い表記しています。

凡例

チェックボックス形式の設定値の表記

■ : 設定がenable（有効）になっていることを示しています。

□ : 設定がenable（無効）になっていること、または未設定を示しています。

物理インターフェース

No. 1

名前		wan
エイリアス		test
タイプ		物理インターフェース
VRF ID		10
バーチャルドメイン		root
ロール		未定義
推定帯域幅	アップストリーム（kbps）	10
	ダウンストリーム（kbps）	10
アドレス		
アドレッシングモード		IPAMによる自動管理
IPAMによる自動管理 - ネットワークサイズ		256
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		10
PPPoE - 初期PADTタイムアウト		5
IP/ネットマスク		192.168.1.254/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
ワンスアームスニファー		
セキュリティプロファイル	アンチウイルス	
	Webフィルタ	
	アプリケーションコントロールセンサー	
	IPS	
	ファイルフィルタ	
ロギングオプション	許可トラフィックをログ	
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント		ID / プレフィックスヒント
セカンダリIPアドレス		enable
IP/ネットマスク		管理者アクセス
		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING □ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ セキュリティファブリック接続
LLDP受信		VDOM設定を使用

LLDP送信	VDOM設定を使用
DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	

アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

No. 2

名前		lan1
エイリアス		
タイプ		物理インターフェース
VRF ID		
バーチャルドメイン		root
ロール		未定義
推定帯域幅	アップストリーム (kbps)	
	ダウンストリーム (kbps)	
アドレス		
アドレッシングモード		
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		
PPPoE - 初期PADTタイムアウト		
IP/ネットマスク		
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		
ワンスアームスニファー		
セキュリティプロファイル	アンチウイルス	
	Webフィルタ	
	アプリケーションコントロールセンサー	
	IPS	
	ファイルフィルタ	
ロギングオプション	許可トラフィックをログ	
IPv6アドレッシングモード		
IPv6アドレス/プレフィックス		
IPv6アドレスの自動設定		
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		
IP/ネットマスク	管理者アクセス	
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト	
管理者アクセス		
IPv4	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト	
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続	
LLDP受信		
LLDP送信		
DHCPサーバ (サーバモード)		
DHCPステータス		
アドレス範囲 (開始 - 終了)		-

ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)			
一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)					
一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	
Explicit Webプロキシ	
セキュリティモード	
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	
その他	
コメント	

ステータス	有効化済み

No. 3

名前		lan2
エイリアス		
タイプ		物理インターフェース
VRF ID		
バーチャルドメイン		root
ロール		未定義
推定帯域幅	アップストリーム (kbps)	
	ダウンストリーム (kbps)	
アドレス		
アドレッシングモード		
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		
PPPoE - 初期PADTタイムアウト		
IP/ネットマスク		
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		
ワンスアームスニファー		
セキュリティプロファイル	アンチウイルス	
	Webフィルタ	
	アプリケーションコントロールセンサー	
	IPS	
	ファイルフィルタ	
ロギングオプション	許可トラフィックをログ	
IPv6アドレッシングモード		
IPv6アドレス/プレフィックス		
IPv6アドレスの自動設定		
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		
IP/ネットマスク	管理者アクセス	
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト	
管理者アクセス		
IPv4	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト	
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続	
LLDP受信		
LLDP送信		
DHCPサーバ (サーバモード)		
DHCPステータス		
アドレス範囲 (開始 - 終了)		-
ネットマスク		
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ		
DNSサーバー		

DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)			
一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)					
一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	
Explicit Webプロキシ	
セキュリティモード	
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	
その他	
コメント	
ステータス	有効化済み

No. 4

名前	lan3

エイリアス		test
タイプ		物理インターフェース
VRF ID		3
バーチャルドメイン		root
ロール		LAN
推定帯域幅	アップストリーム (kbps)	5
	ダウンストリーム (kbps)	7
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		192.168.1.10/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
ワンスアームスニファー		
セキュリティプロファイル	アンチウイルス	
	Webフィルタ	
	アプリケーションコントロールセンサー	
	IPS	
	ファイルフィルタ	
ロギングオプション	許可トラフィックをログ	
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		enable
IAPDプレフィックスヒント	ID	プレフィックスヒント
	8	::/0
	3	2001:db8:20:3:1000:100:20:3/128
	2	2001:db8:20:3:1000:100:20:3/128
	1	2001:db8:20:3:1000:100:20:3/128
セカンダリIPアドレス		enable
IP/ネットマスク		管理者アクセス
192.168.10.1 255.255.255.0		■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
192.168.10.2 255.255.255.0		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP □ PING □ FMGアクセス ■ SSH ■ SNMP □ FTM □ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		□ HTTPS □ HTTP ■ PING ■ FMGアクセス □ SSH □ SNMP ■ セキュリティファブリック接続
LLDP受信		VDOM設定を使用
LLDP送信		enable
DHCPサーバ (サーバモード)		
DHCPステータス		enable
アドレス範囲 (開始 - 終了)		192.168.1.2 - 192.168.1.252

	192.168.1.253 - 192.168.1.255
ネットマスク	255.255.255.0
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	192.168.1.10
DNSサーバー	指定
DNSサーバー (指定)	192.168.1.255
	192.168.1.255
	192.168.1.255
	0.0.0.0
リース時間 (秒)	604800

高度な設定

タイプ	レギュラー
NTPサーバ	指定
NTPサーバ (指定)	192.168.1.255
	192.168.1.255
	192.168.1.255
無線コントローラー	指定
無線コントローラー (指定)	192.168.1.255
	192.168.1.255
	192.168.1.255
タイムゾーン	disable
次のブートストラップサーバ	0.0.0.0
TFTPサーバ	192.168.1.255
	192.168.1.10

その他のDHCPオプション

コード	タイプ	値
4	16進数	1a
5	文字列	abc
7	16進数	1a

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント
00:00:xx:00:xx:01	IPの予約	192.168.1.254	
00:00:xx:00:xx:02	IPの予約	192.168.1.255	

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			
文字列	test	文字列	test	192.168.1.252	
文字列	abc	文字列	abc	192.168.1.253	

DHCPサーバ (リレーモード)

リレーモード	disable
タイプ	
DHCPサーバIP	

ステートレスアドレス自動設定(SLAAC)

IPv6プレフィックス	2001:xxx:20:3:1000:100:20:3/128
	2001:xxx:20:3:1000:100:20:0/123

IPv6で委任されたプレフィックスリスト

アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	

DHCPv6サーバ

DHCPv6ステータス		enable
IPv6サブネット		::/0
DNSサービス		指定
委任済	アップストリームインターフェース	
指定	DNSサーバ	::
		::
		::
		::
ステートフルサーバ - IPモード		IP範囲

IP範囲	アドレス範囲 (開始 - 終了)	-
ネットワーク		
デバイスの検知		enable
Explicit Webプロキシ		
セキュリティモード		キャプティブポータル
認証ポータル (外部) ※指定しない場合はローカル		xxxx.com
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		test_1
		test_2
ポータルメッセージのカスタマイズ		
送信元を除外		xxxx.com
		Interface01 address
		Interface2 address
宛先/サービスを除外		Interface03 address
		login.microsoft.com
		login.windows.net
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		http://xxxx.com
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		Traffic Shaping Profile 1
アウトバウンド帯域幅 (kbps)		0
その他		
コメント		
ステータス		有効化済み

4. ネットワーク（インターフェース）

本章では次のインターフェースの詳細を記載しています。

802.3ad アグリゲート　　ハードウェアスイッチ
PPPoEインターフェース　　ループバックインターフェース
SSL-VPNトンネル　　冗長インターフェース
VLAN

本章では一部の設定値を次の凡例に従い表記しています。

凡例

チェックボックス形式の設定値の表記

■ : 設定がenable (有効)になっていることを示しています。

□ : 設定がenable (無効)になっていること、または未設定を示しています。

802.3ad アグリゲート

No. 1

名前		fortilink
エイリアス		
タイプ		802.3ad アグリゲート
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		a
ロール		未定義
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		IPAMによる自動管理
IPAMによる自動管理 - ネットワークサイズ		256
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		192.1.2.3/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		□ HTTPS　□ HTTP　□ PING　□ FMGアクセス □ SSH　□ SNMP　□ FTM □ RADIUSアカウンティング　□ セキュリティファブリック接続 □ スピードテスト
管理者アクセス		
IPv4		□ HTTPS　□ HTTP　■ PING　□ FMGアクセス □ SSH　□ SNMP　□ FTM □ RADIUSアカウンティング　■ セキュリティファブリック接続 □ スピードテスト
IPv6		□ HTTPS　□ HTTP　□ PING　□ FMGアクセス □ SSH　□ SNMP　□ セキュリティファブリック接続
LLDP受信		enable
LLDP送信		enable
DHCPサーバ (サーバモード)		

DHCPステータス	disable
アドレス範囲 (開始 - 終了)	-
ネットマスク	0.0.0.0
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	0.0.0.0
DNSサーバー	システムDNSと同じ
DNSサーバー (指定)	
リース時間 (秒)	604800
高度な設定	
タイプ	レギュラー
NTPサーバ	システムNTPと同じ
NTPサーバ (指定)	
無線コントローラー	指定
無線コントローラー (指定)	0.0.0.0
	0.0.0.0
	0.0.0.0
タイムゾーン	disable
次のブートストラップサーバ	0.0.0.0
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	

アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

No. 2

名前		test_802.3ad_3
エイリアス		test_802.3ad_3
タイプ		802.3ad アグリゲート
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		IPAMによる自動管理
IPAMによる自動管理 - ネットワークサイズ		65536
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		0.0.0.0/0.0.0.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		委任済
IPv6アドレス/プレフィックス		
IPv6アドレスの自動設定		
アイデンティティアソシエーション識別子		1
IPv6アップストリームインターフェース		xxxx_802.3ad_3
IPv6サブネット		::/0
DHCPv6プレフィックス委任		enable
IAPDプレフィックスヒント	ID	プレフィックスヒント
	49	::/0
	2	::/0
	1	::/0
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
IPv6		■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ セキュリティファブリック接続
LLDP受信		enable
LLDP送信		enable
DHCPサーバ (サーバモード)		
DHCPステータス		enable
アドレス範囲 (開始 - 終了)		-
ネットマスク		255.255.0.0
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ		192.1.2.254
DNSサーバー		インターフェースIPと同じ
DNSサーバー (指定)		

リース時間 (秒)	604800
高度な設定	
タイプ	レギュラー
NTPサーバ	ローカル
NTPサーバ (指定)	
無線コントローラー	インターフェースIPと同じ
無線コントローラー (指定)	
タイムゾーン	disable
次のブートストラップサーバ	0.0.0.0
TFTPサーバ	192.123.123.0
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	::/0
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	test_802.3ad_3
サブネット	::/0
RDNSSサービス	指定
RDNSSサービス (指定)	12:a1::
DHCPv6サーバ	
DHCPv6ステータス	enable
IPv6サブネット	::/0
DNSサービス	指定
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	xx:a1::
	xx:a2::
	xx:a3::
	::
ステートフルサーバ - IPモード	IP範囲
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	802.3ad test
ステータス	有効化済み

PPPoEインターフェース

設定はありません。

SSL-VPNトンネル

No. 1

名前		Interface3
エイリアス		
タイプ		SSL-VPNトンネル
VRF ID		0
バーチャルドメイン		root
インターフェース		lan
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
管理者アクセス		
IPv4		■ HTTPS ■ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 ■ スピードテスト
IPv6		□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続
ネットワーク		
Explicit Webプロキシ		
セキュリティモード		
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		
ポータルメッセージのカスタマイズ		
送信元を除外		
宛先/サービスを除外		
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		
アウトバウンド帯域幅 (kbps)		10000
その他		
コメント		comment
ステータス		有効化済み

VLAN

No. 1

名前		Interface01
エイリアス		エイリアス
タイプ		VLAN
VRF ID		0
バーチャルドメイン		root
VLANプロトコル		802.1Q
インターフェース		fortilink
VLAN ID		1
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		DHCP
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1

PPPoE - 初期PADTタイムアウト	1
IP/ネットマスク	
サーバーからデフォルトゲートウェイを取得	enable
ディスタンス	5
内部DNSを上書き	enable
IPv6アドレッシングモード	マニュアル
IPv6アドレス/プレフィックス	::/0
IPv6アドレスの自動設定	disable
アイデンティティアソシエーション識別子	
IPv6アップストリームインターフェース	
IPv6サブネット	
DHCPv6プレフィックス委任	disable

IAPDプレフィックスヒント	ID	プレフィックスヒント

セカンダリIPアドレス	
IP/ネットマスク	管理者アクセス
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト

管理者アクセス

IPv4	■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続

DHCPサーバ (サーバモード)

DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	

高度な設定

タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)

リレーモード	disable
タイプ	
DHCPサーバIP	

ステートレスアドレス自動設定(SLAAC)

IPv6プレフィックス		
DHCPv6サーバ		
DHCPv6ステータス		
IPv6サブネット		
DNSサービス		
委任済	アップストリームインターフェース	
指定	DNSサーバ	
ステートフルサーバ - IPモード		
IP範囲	アドレス範囲 (開始 - 終了)	-
ネットワーク		
デバイスの検知		enable
Explicit Webプロキシ		
セキュリティモード		none
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		
ポータルメッセージのカスタマイズ		
送信元を除外		
宛先/サービスを除外		
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		Traffic Shaping Profile 1
アウトバウンド帯域幅 (kbps)		1000
その他		
コメント		コメント
ステータス		有効化済み

No. 2

名前		Interface2
エイリアス		
タイプ		VLAN
VRF ID		0
バーチャルドメイン		root
VLANプロトコル		802.1Q
インターフェース		wan
VLAN ID		2
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		DHCP
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		
サーバーからデフォルトゲートウェイを取得		enable
ディスタンス		5
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		

IP/ネットマスク	管理者アクセス
	□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 □ スピードテスト

管理者アクセス	
IPv4	■ HTTPS ■ HTTP ■ PING □ FMGアクセス ■ SSH ■ SNMP □ FTM □ RADIUSアカウンティング □ セキュリティファブリック接続 ■ スピードテスト
IPv6	□ HTTPS □ HTTP □ PING □ FMGアクセス □ SSH □ SNMP □ セキュリティファブリック接続

DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 アップストリームインターフェース	
指定 DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	enable
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス ※ユーザーグループを指定しない場合は、すべて許可	

ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL) ※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

No. 3

名前		test_1
エイリアス		test_1
タイプ		VLAN
VRF ID		0
バーチャルドメイン		root
VLANプロトコル		802.1Q
インターフェース		fortilink
VLAN ID		10
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		0.0.0.0/0.0.0.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		enable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
DHCPサーバ (サーバモード)		
DHCPステータス		enable
アドレス範囲 (開始 - 終了)		192.123.0.0 - 192.123.0.0

	192.123.0.2 - 192.123.0.254
ネットマスク	255.255.255.0
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	192.123.0.0
DNSサーバー	システムDNSと同じ
DNSサーバー (指定)	
リース時間 (秒)	604800

高度な設定

タイプ	レギュラー
NTPサーバ	指定
NTPサーバ (指定)	0.0.0.0
	0.0.0.0
	0.0.0.0
無線コントローラー	指定
無線コントローラー (指定)	0.0.0.0
	0.0.0.0
	0.0.0.0
タイムゾーン	disable
次のブートストラップサーバ	0.0.0.0
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)

リレーモード	disable
タイプ	
DHCPサーバIP	

ステートレスアドレス自動設定(SLAAC)

IPv6プレフィックス	

DHCPv6サーバ

DHCPv6ステータス		
IPv6サブネット		
DNSサービス		
委任済	アップストリームインターフェース	
指定	DNSサーバ	
ステートフルサーバ - IPモード		
IP範囲	アドレス範囲 (開始 - 終了)	-

ネットワーク

デバイスの検知	enable
Explicit Webプロキシ	
セキュリティモード	キャプティブポータル
認証ポータル (外部) ※指定しない場合はローカル	xxxx.com

ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可

ユーザーグループ	test_1
	test_2
	test_ 3
ポータルメッセージのカスタマイズ	
送信元を除外	FABRIC_DEVICE
	xxxx.com
宛先/サービスを除外	FABRIC_DEVICE
	gmail.com
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	http://xxxx,com

トラフィックシェイピング

アウトバウンドシェイピングプロファイル	Traffic Shaping Profile 1
アウトバウンド帯域幅 (kbps)	999999
その他	
コメント	
ステータス	有効化済み

No. 4

名前		test_9
エイリアス		test_9
タイプ		VLAN
VRF ID		0
バーチャルドメイン		root
VLANプロトコル		802.1Q
インターフェース		fortilink
VLAN ID		21
ロール		未定義
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		0.0.0.0/0.0.0.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
DHCPサーバ (サーバモード)		
DHCPステータス		
アドレス範囲 (開始 - 終了)		-
ネットマスク		
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ		
DNSサーバー		
DNSサーバー (指定)		
リース時間 (秒)		
高度な設定		

タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	
その他のDHCPオプション	

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 アップストリームインターフェース	
指定 DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
セキュリティモード	キャプティブポータル
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

ハードウェアスイッチ

No. 1

名前	lan
エイリアス	
タイプ	ハードウェアスイッチ
VRF ID	0
バーチャルドメイン	root
インターフェースメンバー	lan1
	lan2

ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		192.168.99.100/255.255.255.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント		ID / プレフィックスヒント
セカンダリIPアドレス		disable
IP/ネットマスク		管理者アクセス
		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス		
IPv4		■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ■ セキュリティファブリック接続 ☐ スピードテスト
IPv6		☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
LLDP受信		VDOM設定を使用
LLDP送信		VDOM設定を使用
DHCPサーバ (サーバモード)		
DHCPステータス		
アドレス範囲 (開始 - 終了)		-
ネットマスク		
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ		
DNSサーバー		
DNSサーバー (指定)		
リース時間 (秒)		
高度な設定		
タイプ		
NTPサーバ		
NTPサーバ (指定)		
無線コントローラー		
無線コントローラー (指定)		
タイムゾーン		
次のブートストラップサーバ		
TFTPサーバ		
その他のDHCPオプション		
コード	タイプ	値
IPアドレスの割り当てルール (MACアドレス)		

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	
委任済 / アップストリームインターフェース	
指定 / DNSサーバ	
ステートフルサーバ - IPモード	
IP範囲 / アドレス範囲 (開始 - 終了)	-
ネットワーク	
デバイスの検知	disable
Explicit Webプロキシ	
STP	enable
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
SPAN(ポートミラーリング)	
有効	enable
送信元ポート	lan2
宛先ポート	lan1
方向	両方
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

ループバックインターフェース

No. 1

名前		loopback_test_3
エイリアス		loopback_test_3
タイプ		ループバックインターフェース
VRF ID		0
バーチャルドメイン		root
ロール		WAN
推定帯域幅	アップストリーム (kbps)	27
	ダウンストリーム (kbps)	22

アドレス				
IP/ネットマスク	0.0.0.0 0.0.0.0			
IPv6アドレス/プレフィックス				
IPv6アドレスの自動設定				
DHCPv6プレフィックス委任				
IAPDプレフィックスヒント	ID	プレフィックスヒント		
セカンダリIPアドレス	enable			
IP/ネットマスク	管理者アクセス			
0.0.0.0 0.0.0.0	■ HTTPS	■ HTTP	■ PING	■ FMGアクセス
	■ SSH	■ SNMP	■ FTM	
	■ RADIUSアカウンティング		■ セキュリティファブリック接続	
	■ スピードテスト			
0.0.0.0 0.0.0.0	□ HTTPS	□ HTTP	□ PING	□ FMGアクセス
	□ SSH	□ SNMP	□ FTM	
	□ RADIUSアカウンティング		□ セキュリティファブリック接続	
	□ スピードテスト			
0.0.0.0 0.0.0.0	■ HTTPS	□ HTTP	□ PING	□ FMGアクセス
	■ SSH	□ SNMP	□ FTM	
	■ RADIUSアカウンティング		■ セキュリティファブリック接続	
	■ スピードテスト			
管理者アクセス				
IPv4	■ HTTPS	□ HTTP	■ PING	□ FMGアクセス
	■ SSH	□ SNMP	□ FTM	
	■ RADIUSアカウンティング		■ セキュリティファブリック接続	
	■ スピードテスト			
IPv6	□ HTTPS	□ HTTP	□ PING	□ FMGアクセス
	□ SSH	□ SNMP	□ セキュリティファブリック接続	
ネットワーク				
Explicit Webプロキシ				
セキュリティモード	キャプティブポータル			
認証ポータル (外部) ※指定しない場合はローカル				
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可				
ユーザーグループ	Guest-group			
	test_1			
ポータルメッセージのカスタマイズ	test_1			
送信元を除外	Interface03 address			
	Interface2 address			
	test_11 address			
宛先/サービスを除外	test_10 address			
	test_1			
	test_23 address			
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	http://xxxx.com			
トラフィックシェイピング				
アウトバウンドシェイピングプロファイル				
アウトバウンド帯域幅 (kbps)	85			
その他				
コメント	ループバックインターフェース＆セカンドIPテスト			
ステータス	有効化済み			

No. 2

名前		loopback_test_4
エイリアス		loopback_test_4
タイプ		ループバックインターフェース
VRF ID		10
バーチャルドメイン		root
ロール		LAN
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		

IP/ネットマスク	192.168.1.0 255.255.0.0
IPv6アドレス/プレフィックス	
IPv6アドレスの自動設定	
DHCPv6プレフィックス委任	
IAPDプレフィックスヒント	ID / プレフィックスヒント
セカンダリIPアドレス	disable
IP/ネットマスク	管理者アクセス
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス	
IPv4	■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6	■ HTTPS ■ HTTP ■ PING ■ FMGアクセス ■ SSH ■ SNMP ■ セキュリティファブリック接続
ネットワーク	
Explicit Webプロキシ	
セキュリティモード	none
認証ポータル (外部) ※指定しない場合はローカル	
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可	
ユーザーグループ	
ポータルメッセージのカスタマイズ	
送信元を除外	
宛先/サービスを除外	
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト	
トラフィックシェイピング	
アウトバウンドシェイピングプロファイル	
アウトバウンド帯域幅 (kbps)	0
その他	
コメント	
ステータス	有効化済み

冗長インターフェース

No. 1

名前		test_24
エイリアス		test_24
タイプ		冗長インターフェース
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		
ロール		DMZ
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		マニュアル
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		0.0.0.0/0.0.0.0
サーバーからデフォルトゲートウェイを取得		
ディスタンス		
内部DNSを上書き		enable

IPv6アドレッシングモード	マニュアル
IPv6アドレス/プレフィックス	::/0
IPv6アドレスの自動設定	disable
アイデンティティアソシエーション識別子	
IPv6アップストリームインターフェース	
IPv6サブネット	
DHCPv6プレフィックス委任	disable

IAPDプレフィックスヒント	ID	プレフィックスヒント

セカンダリIPアドレス	disable
IP/ネットマスク	管理者アクセス
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト

管理者アクセス	
IPv4	■ HTTPS ■ HTTP ■ PING ☐ FMGアクセス ■ SSH ■ SNMP ☐ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
LLDP受信	enable
LLDP送信	enable

DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	

高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	

ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	

IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	

サブネット		
RDNSSサービス		
RDNSSサービス (指定)		
DHCPv6サーバ		
DHCPv6ステータス		
IPv6サブネット		
DNSサービス		
委任済	アップストリームインターフェース	
指定	DNSサーバ	
ステートフルサーバ - IPモード		
IP範囲	アドレス範囲 (開始 - 終了)	-
ネットワーク		
デバイスの検知		disable
Explicit Webプロキシ		
セキュリティモード		none
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		
ポータルメッセージのカスタマイズ		
送信元を除外		
宛先/サービスを除外		
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		
アウトバウンド帯域幅 (kbps)		0
その他		
コメント		qwertyuiop
ステータス		有効化済み

No. 2

名前		test_25
エイリアス		test_25
タイプ		冗長インターフェース
VRF ID		0
バーチャルドメイン		root
インターフェースメンバー		
ロール		DMZ
推定帯域幅	アップストリーム (kbps)	0
	ダウンストリーム (kbps)	0
アドレス		
アドレッシングモード		DHCP
IPAMによる自動管理 - ネットワークサイズ		
PPPoE - ユーザ名		
PPPoE - Unnumbered IP接続		
PPPoE - 初期Discタイムアウト		1
PPPoE - 初期PADTタイムアウト		1
IP/ネットマスク		
サーバーからデフォルトゲートウェイを取得		enable
ディスタンス		255
内部DNSを上書き		disable
IPv6アドレッシングモード		マニュアル
IPv6アドレス/プレフィックス		::/0
IPv6アドレスの自動設定		disable
アイデンティティアソシエーション識別子		
IPv6アップストリームインターフェース		
IPv6サブネット		
DHCPv6プレフィックス委任		disable
IAPDプレフィックスヒント	ID	プレフィックスヒント
セカンダリIPアドレス		

IP/ネットマスク	管理者アクセス
	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUSアカウンティング ☐ セキュリティファブリック接続 ☐ スピードテスト
管理者アクセス	
IPv4	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ■ SNMP ■ FTM ■ RADIUSアカウンティング ■ セキュリティファブリック接続 ■ スピードテスト
IPv6	☐ HTTPS ☐ HTTP ☐ PING ☐ FMGアクセス ☐ SSH ☐ SNMP ☐ セキュリティファブリック接続
LLDP受信	disable
LLDP送信	VDOM設定を使用
DHCPサーバ (サーバモード)	
DHCPステータス	
アドレス範囲 (開始 - 終了)	-
ネットマスク	
デフォルトゲートウェイ ※未指定の場合はインターフェースIPと同じ	
DNSサーバー	
DNSサーバー (指定)	
リース時間 (秒)	
高度な設定	
タイプ	
NTPサーバ	
NTPサーバ (指定)	
無線コントローラー	
無線コントローラー (指定)	
タイムゾーン	
次のブートストラップサーバ	
TFTPサーバ	

その他のDHCPオプション

コード	タイプ	値

IPアドレスの割り当てルール (MACアドレス)

一致基準 (MACアドレス)	アクション	IP	コメント

IPアドレスの割り当てルール (DHCPリレーエージェント)

一致基準				IP (IPの予約)	コメント
サーキットID		リモートID			

DHCPサーバ (リレーモード)	
リレーモード	disable
タイプ	
DHCPサーバIP	
ステートレスアドレス自動設定(SLAAC)	
IPv6プレフィックス	
IPv6で委任されたプレフィックスリスト	
アップストリームインターフェース	
サブネット	
RDNSSサービス	
RDNSSサービス (指定)	
DHCPv6サーバ	
DHCPv6ステータス	
IPv6サブネット	
DNSサービス	

委任済	アップストリームインターフェース
指定	DNSサーバ

ステートフルサーバ - IPモード	

IP範囲	アドレス範囲 (開始 - 終了)	-
ネットワーク		
デバイスの検知		enable
Explicit Webプロキシ		
セキュリティモード		none
認証ポータル (外部) ※指定しない場合はローカル		
ユーザーアクセス　※ユーザーグループを指定しない場合は、すべて許可		
ユーザーグループ		
ポータルメッセージのカスタマイズ		
送信元を除外		
宛先/サービスを除外		
キャプティブポータル後にリダイレクト (指定のURL)　※指定しない場合は元のリクエスト		
トラフィックシェイピング		
アウトバウンドシェイピングプロファイル		Traffic Shaping Profile 1
アウトバウンド帯域幅 (kbps)		10000000
その他		
コメント		zxcvbnm
ステータス		有効化済み

5. ネットワーク（スタティックルート）

IPv4

No. 1

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	
ゲートウェイアドレス		192.168.99.2
インターフェース		lan
アドミニストレーティブ・ディスタンス		255
コメント		
ステータス		enable
高度な設定		
プライオリティ		1

No. 2

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	
ゲートウェイアドレス		
インターフェース		l2t.root
アドミニストレーティブ・ディスタンス		255
コメント		
ステータス		enable
高度な設定		
プライオリティ		9999

No. 3

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	917640
ゲートウェイアドレス		0.0.0.0
インターフェース		test_1
アドミニストレーティブ・ディスタンス		
コメント		インターネットサービステスト
ステータス		enable
高度な設定		
プライオリティ		

No. 4

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	393320
ゲートウェイアドレス		192.168.99.1
インターフェース		lan
アドミニストレーティブ・ディスタンス		
コメント		インターネットサービステスト２
ステータス		enable
高度な設定		
プライオリティ		

No. 5

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	
ゲートウェイアドレス		192.168.99.2
インターフェース		test_1
アドミニストレーティブ・ディスタンス		10
コメント		
ステータス		enable
高度な設定		
プライオリティ		1

No. 6

宛先	サブネット	0.0.0.0/0.0.0.0
	名前付きアドレス	
	インターネットサービス	4063233
ゲートウェイアドレス		0.0.0.0
インターフェース		test_1
アドミニストレーティブ・ディスタンス		
コメント		
ステータス		enable
高度な設定		
プライオリティ		

No. 7

宛先	サブネット	192.20.20.0/255.255.255.0
	名前付きアドレス	
	インターネットサービス	
ゲートウェイアドレス		0.0.0.0
インターフェース		lan
アドミニストレーティブ・ディスタンス		10
コメント		
ステータス		enable
高度な設定		
プライオリティ		1

IPv6

No. 1

宛先	xx:a1::/128
ゲートウェイアドレス	xx:a2::
インターフェース	test_1
アドミニストレーティブ・ディスタンス	10
コメント	
ステータス	enable
高度な設定	
プライオリティ	1024

No. 2

宛先	xx:a2::/128
ゲートウェイアドレス	xx:a3::
インターフェース	test_1
アドミニストレーティブ・ディスタンス	20
コメント	
ステータス	enable
高度な設定	
プライオリティ	1050

6. SD-WAN（概要）

SD-WANゾーン

ゾーン	インタフェース	ゲートウェイ	IPv6ゲートウェイ	コスト	ステータス	プライオリティ
virtual-wan-link						
testQA1						
test_SD-WAN_zone1						
test_SD-WAN_zone	DHCPv6サーバ	0.0.0.0	::	0	有効	1
test_SD-WAN_zone2	test_01	0.0.0.0	::	1	有効	1
	test_02	0.0.0.0	::	0	無効	65535
	capture_vlan	0.0.0.0	::	3	有効	1

SD-WANルール

ID	名前	IPバージョン	送信元 ※1	宛先 ※1	基準	メンバー ※1	パフォーマンスSLA ※1	ポート	プロトコル	ステータス
1	SD-WAN_rule1	ipv4	xxxxx.xxx	xxxxx.xxx		test_8		開始： 1 終了： 65535	TCP	有効
2	SD-WAN_rule2	ipv4	xxxxx.xxx	all	latency	test_8, test_9	test_SLA	開始： 1 終了： 65535	UDP	無効
3	SD-WAN_rule3	ipv4	xxxxx.xxx	xxxxx.xxx	jitter	test_8	Default_FortiGuard	開始： 終了：	ANY	有効
4	SD-WAN_rule4	ipv6	xxxxx.xxx	xxxxx.xxx	packet-loss	test_9	test_SLA2	開始： 終了：	10	有効
5	SD-WAN_rule5	ipv6	xxxxx.xxx	xxxxx.xxx	inbandwidth	test_8, test_9	test_SLA4	開始： 終了：	ANY	有効

※1 記入欄に記載する設定値が多い場合は一部省略しています。

パフォーマンスSLA

名前	サーバ検知	インターフェース ※1	故障しきい値	リカバリしきい値
Default_DNS			5	10
Default_Office_365	xxxxx.xxx		5	10
Default_Gmail	xxxxx.xxx		5	10
Default_Google Search	xxxxx.xxx		5	10
Default_FortiGuard	xxxxx.xxx		5	10
test_SLA	xxxxx.xxx		5	5
test_SLA2	test	test_8	5	5
test_SLA3	test1, test2	test3, test4	5	5

※1 記入欄に記載する設定値が多い場合は一部省略しています。

7. SD-WAN（ルール）

暗黙のルール

ロードバランスアルゴリズム		usage-based		
メンバー	ウェイト	Ingress Spillover Threshold (kbps)	Egress Spillover Threshold (kbps)	Priority
test_3		16776000	4	1
test_4		10000	16776000	65535
capture_vlan		1	0	1
DHCPv6サーバ		10	1	1

プライオリティルール

No. 1

ID	1
名前	SD-WAN_rule1
ステータス	有効
IPバージョン	ipv4
送信元	
アドレス	xxxxx.xxx
ユーザグループ	01_remoteusergroup
宛先	
アドレス	xxxxx.xxx
プロトコル (※ 指定の場合はプロトコル番号を表示)	TCP
ポート範囲	1 - 65535
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	manual
インタフェースリファレンス	test_8
ゾーンプリファレンス	SD-WAN_zone1
計測されたSLA	
必要なSLAターゲット	
ロードバランシング	有効
クオリティ基準	
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	有効
転送DSCPタグ	000000
逆方向DSCP	有効
リバースDSCPタグ	000000

No. 2

ID	2
名前	SD-WAN_rule2
ステータス	無効
IPバージョン	ipv4
送信元	
アドレス	all
ユーザグループ	demo, test_2
宛先	

アドレス	all
プロトコル (※ 指定の場合はプロトコル番号を表示)	UDP
ポート範囲	1 - 65535
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_8
	test_9
ゾーンプリファレンス	SD-WAN_zone1, virtual-wan-link
計測されたSLA	test_SLA
必要なSLAターゲット	
ロードバランシング	
クオリティ基準	latency
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	無効
転送DSCPタグ	
逆方向DSCP	無効
リバースDSCPタグ	

No. 3

ID	3
名前	SD-WAN_rule3
ステータス	有効
IPバージョン	ipv4
送信元	
アドレス	login.xxxxx.xxx, Interface2 address, test_ダイナミック_ファブリック6, Microsoft Office 365
ユーザグループ	guest, vpnuser1, tesst02_remoteusergroup
宛先	
アドレス	wildcard.xxxxxxx.xxxx, Interface2 address, トンネル 1 サイト間_remote, サイト 3_remote
プロトコル (※ 指定の場合はプロトコル番号を表示)	ANY
ポート範囲	-
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_8
ゾーンプリファレンス	SD-WAN_zone1
計測されたSLA	Default_FortiGuard
必要なSLAターゲット	

ロードバランシング	
クオリティ基準	jitter
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	無効
転送DSCPタグ	
逆方向DSCP	無効
リバースDSCPタグ	

No. 4

ID	4
名前	SD-WAN_rule4
ステータス	有効
IPバージョン	ipv6
送信元	
アドレス	test1_IPv6_address_FQDN
ユーザグループ	test_ 3
宛先	
アドレス	SSLVPN_TUNNEL_IPv6_ADDR1
プロトコル (※ 指定の場合はプロトコル番号を表示)	10
ポート範囲	-
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	0x11
ビットマスク	0x12
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_9
ゾーンプリファレンス	testQA1
計測されたSLA	test_SLA2
必要なSLAターゲット	
ロードバランシング	
クオリティ基準	packet-loss
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	
転送DSCPタグ	
逆方向DSCP	
リバースDSCPタグ	

No. 5

ID	5
名前	SD-WAN_rule5
ステータス	有効
IPバージョン	ipv6
送信元	
アドレス	test2_IPv6, test_IPv6group
ユーザグループ	vpnuser1, tesst05_remoteusergroup
宛先	

アドレス	xxxxx.xxx
プロトコル (※ 指定の場合はプロトコル番号を表示)	ANY
ポート範囲	-
サービスタイプ (※ ビットパターン、ビットマスクの両方が0x00の場合、サービスタイプは無効)	
ビットパターン	
ビットマスク	
インターネットサービス	
アプリケーション	
Apps	
Category	
Group	
発信インターフェース	
インターフェース選択戦略	priority
インタフェースリファレンス	test_8
	test_9
ゾーンプリファレンス	SD-WAN_zone1, virtual-wan-link
計測されたSLA	test_SLA4
必要なSLAターゲット	
ロードバランシング	
クオリティ基準	inbandwidth
レイテンシのウェイト	
ジッタのウェイト	
パケットロスのウェイト	
帯域幅のウェイト	
順方向DSCP	
転送DSCPタグ	
逆方向DSCP	
リバースDSCPタグ	

8. SD-WAN (パフォーマンスSLA)

No. 1

名前	Default_DNS		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル			
サーバ			
DNSサーバ	システムDNSと同じ		
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	1000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 2

名前	Default_Office_365		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	https		
サーバ	xxx.xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	120000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 3

名前	Default_Gmail		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	ping		
サーバ	xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	2
リンクステータス			
チェック間隔 (ms)	1000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 4

名前	Default_Google Search		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	https		
サーバ	xxx.xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	120000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

No. 5

名前	Default_FortiGuard		
IPバージョン	ipv4		
プローブモード	アクティブ		
プロトコル	https		
サーバ	xxxx.xxx		
DNSサーバ			
プライマリDNSサーバ			
セカンダリDNSサーバ			
参加インターフェース			
インタフェース			
SLAターゲット			
ターゲット	レイテンシしきい値 (ms)	ジッターしきい値 (ms)	パケットロスしきい値 (%)
1	250	50	5
リンクステータス			
チェック間隔 (ms)	120000		
非アクティブまでの失敗回数	5		
リンク回復までの回数 (check(s))	10		
非アクティブ時のアクション			
スタティックルートのアップデート	有効		

9. ポリシー&オブジェクト（概要）

ファイアウォールポリシー

名前	from ※1	to ※1	送信元（アドレス）※1	宛先（アドレス）※1	アクション
test01_FWpolicy	Interface03	loopback_test_3	IPv4: login.xxxx.com IPv6:	IPv4: login.xxxx.com IPv6:	許可
SSL-VPN-Access-Policy	ssl.root	lan	IPv4: SSLVPN_TUNNEL_ADDR1 IPv6:	IPv4: all IPv6:	許可
SSL-VPN-Access-Policy-New	ssl.root	lan	IPv4: SSLVPN_TUNNEL_ADDR1 IPv6:	IPv4: all IPv6:	許可
vpn_サイト２_local_0	test_24	サイト２	IPv4: サイト２_local IPv6:	IPv4: サイト２_remote IPv6:	許可
vpn_サイト２_remote_0	サイト２	test_24	IPv4: サイト２_remote IPv6:	IPv4: サイト２_local IPv6:	許可
vpn_サイト２_share_internet	サイト２	loopback_test_3	IPv4: サイト２_remote IPv6:	IPv4: all IPv6:	許可
vpn_xcvbnm_local_0	Interface2	xcvbnm	IPv4: xcvbnm_local IPv6:	IPv4: xcvbnm_remote IPv6:	許可
vpn_xcvbnm_remote_0	xcvbnm	Interface2	IPv4: xcvbnm_remote IPv6:	IPv4: xcvbnm_local IPv6:	許可
vpn_xcvbnm_share_internet	xcvbnm	loopback_test_3	IPv4: xcvbnm_remote IPv6:	IPv4: all IPv6:	許可
vpn_pojpoj,_local_0	test_24	pojpoj,	IPv4: pojpoj,_local IPv6:	IPv4: pojpoj,_remote IPv6:	許可
vpn_pojpoj,_remote_0	pojpoj,	test_24	IPv4: pojpoj,_remote IPv6:	IPv4: pojpoj,_local IPv6:	許可
vpn_pojpoj,_share_internet	pojpoj,	loopback_test_3	IPv4: pojpoj,_remote IPv6:	IPv4: all IPv6:	許可
vpn_asdfghj_remote_0	asdfghj	ssl.root	IPv4: asdfghj_range IPv6:	IPv4: IPsec_Tunnel_Pool IPv6:	許可
vpn_;jafjoewgjowg_remote_1	;jafjoewgjowg	loopback_test_4	IPv4: ;jafjoewgjowg_range IPv6:	IPv4: asdfghj_range dhcptest address IPv6:	許可
vpn_;jafjoewgjowg_remote_0	;jafjoewgjowg	loopback_test_3	IPv4: ;jafjoewgjowg_range IPv6:	IPv4: asdfghj_range dhcptest address IPv6:	許可
vpn_不具合検証_remote_0	不具合検証 test_11	loopback_test_3 loopback_test_4	IPv4: 不具合検証_range IPv6:	IPv4: loopback_test_4 address IPv6:	許可

※1 記入欄に記載する設定値が多い場合は一部省略しています。

アドレスグループ

IPv4グループ

名前	タイプ	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。	ルーティング可能
G Suite	グループ	xxxx.com wildcard.xxxx.com	
Microsoft Office 365	グループ	login.xxxx.com xxxx.com login.xxxx.net	
test1_IPv4group	フォルダ	FIREWALL_AUTH_PORTAL_ADDRESS SSLVPN_TUNNEL_ADDR1	
test1_IPv4_addressgroup	グループ		
トンネル１サイト間_local	グループ	トンネル１サイト間_local_subnet_1 トンネル１サイト間_local_subnet_2	enable
トンネル１サイト間_remote	グループ	トンネル１サイト間_remote_subnet_1 トンネル１サイト間_remote_subnet_2	enable
リモートアクセス1_split	グループ	dhcptest address	

サイト２_local	グループ		enable
サイト２_remote	グループ	サイト２_remote_subnet_1	enable
サイト3_local	グループ	サイト3_local_subnet_1	enable
サイト3_remote	グループ	サイト3_remote_subnet_1	enable
N1_local	グループ	N1_local_subnet_1	enable
N1_remote	グループ	N1_remote_subnet_1	enable
xcvbnm_local	グループ	xcvbnm_local_subnet_1	enable
xcvbnm_remote	グループ	xcvbnm_remote_subnet_1	enable
pojpoj,_local	グループ	pojpoj,_local_subnet_1	enable
pojpoj,_remote	グループ	pojpoj,_remote_subnet_1	enable
サイト全埋_local	グループ	サイト全埋_local_subnet_1	enable
サイト全埋_remote	グループ	サイト全埋_remote_subnet_1	enable

IPv6グループ

名前	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
test_IPv6group	SSLVPN_TUNNEL_IPv6_ADDR1
test2_IPv6group	SSLVPN_TUNNEL_IPv6_ADDR1 test2_IPv6 test_IPv6group

アドレス

アドレス

名前	タイプ	インターフェース	詳細	IP	コメント	ルーティング可能
EMS_ALL_UNKNOWN_CLIENTS	ダイナミック					
EMS_ALL_UNMANAGEABLE_CLIENTS	ダイナミック					
none	サブネット			0.0.0.0/255.255.255.255		disable
login.xxxx.com	FQDN		login.xxxx.com			disable
xxxx.com	FQDN		xxxx.com			disable
wildcard.xxxx.com	FQDN		*.xxxx.com			disable
all	サブネット			0.0.0.0/0.0.0.0		disable
FIREWALL_AUTH_PORTAL_ADDRESS	サブネット			0.0.0.0/0.0.0.0		disable
FABRIC_DEVICE	サブネット			0.0.0.0/0.0.0.0	IPv4 addresses of Fabric Devices	
SSLVPN_TUNNEL_ADDR1	IP範囲			192.212.134.200 - 192.212.134.210		
lan	インターフェイス サブネット	lan		192.168.1.0/255.255.255.0		disable
FCTEMS_ALL_FORTICLOUD_SERVERS	ダイナミック					
Interface01 address	インターフェイス サブネット	Interface01		0.0.0.0/255.255.255.255		disable
Interface2 address	インターフェイス サブネット	Interface2		0.0.0.0/255.255.255.255		disable
Interface03 address	インターフェイス サブネット	Interface03		0.0.0.0/255.255.255.255		disable
test_1 address	インターフェイス サブネット	test_1		0.0.0.0/255.255.255.255		disable
test_IPMA_3 address	インターフェイス サブネット	test_IPMA_3		192.31.0.0/255.255.255.0		disable
VLAN_test_2 address	インターフェイス サブネット	VLAN_test_2		0.0.0.0/255.255.255.255		disable

VLAN_test_1 address	インターフェイス サブネット	VLAN_test_1		192.0.0.0/255.0.0.0		disable
test_802.3ad_3 address	インターフェイス サブネット	test_802.3ad_3		0.0.0.0/255.255.255.255		disable
test1_address	ジオグラフィ		JAPAN			
test2_address	IP範囲			192.123.0.0 - 192.123.0.10		
test3_address	ダイナミック					
test4_address	ダイナミック					
test1_IPv4_address_IPhani	IP範囲			192.123.0.0 - 192.123.0.10		
test2_IPv4_address_giogurafi	ジオグラフィ		JAPAN			
test1_IPv4_address_dynamic	ダイナミック					
test1_IPv4_address_dynamic02	ダイナミック					
test1_IPv4_address_dynamic03	ダイナミック					
VPN_to_Opponent_local_subnet_1	サブネット			192.168.10.0/255.255.255.0		enable
VPN_to_Opponent_remote_subnet_1	サブネット			192.168.20.0/255.255.255.0		enable
IPsec_Tunnel_Pool	IP範囲			192.250.250.1 - 192.250.250.254		
トンネル１サイト間_local_subnet_1	サブネット			192.168.99.0/255.255.255.0		enable
ハブアンドスポーク_local_subnet_1	サブネット			192.0.0.0/192.0.0.0		enable
リモートアクセス1_range	IP範囲			192.16.1.1 - 192.16.1.250	VPN: リモートアクセス1 (Created by VPN wizard)	
サイト２_remote_subnet_1	サブネット			192.20.20.0/255.255.255.0		enable
N1_local_subnet_1	サブネット			192.168.99.0/255.255.255.0		enable
N1_remote_subnet_1	サブネット			192.20.20.0/255.255.255.0		enable

IPv6アドレス

名前	タイプ	詳細	IP
SSLVPN_TUNNEL_IPv6_ADDR1	サブネット		fdff:xxxx::/120
all	サブネット		::/0
none	サブネット		::/128
test2_IPv6	IPv6範囲		12:a1:: - 12:a10::
test1_IPv6_address_FQDN	FQDN	xxx.aa	
test1_IPv6_address_region	IPv6地域	JAPAN	
test1_IPv6_address_template	IPv6テンプレート	test1_IPv6_template	2001:xxxx:0:cd30::/60
test1_IPv6_address_MAC	デバイス(MACアドレス)	"11:22:33:44:55:66" "00:11:22:33:44:55" "22:33:44:55:66:77"	
test2_IPv6_address_template	IPv6テンプレート	test2_IPv6_template	2001:xxxx:0:cd30::/60
test20250312_geography_Japan	IPv6地域	JAPAN	
test20250312_geography_Bulgaria	IPv6地域	BULGARIA	
test20250312_geography_China	IPv6地域	CHINA	

マルチキャストアドレス

名前	タイプ	インターフェース	IP
all	マルチキャストIP範囲		192.0.0.0 - 192.255.255.255
all_hosts	マルチキャストIP範囲		192.0.0.1 - 192.0.0.1
all_routers	マルチキャストIP範囲		192.0.0.2 - 192.0.0.2
Bonjour	マルチキャストIP範囲		192.0.0.251 - 192.0.0.251
EIGRP	マルチキャストIP範囲		192.0.0.10 - 192.0.0.10

OSPF	マルチキャストIP範囲		192.0.0.5 - 192.0.0.6
test1_multiaddress	ブロードキャストサブネット		0.0.0.0 0.0.0.0

IPv6マルチキャストアドレス

名前	IPv6アドレス
all	xxxx::/8
test1_IPV6_multicast	xxxx::/8
test2_IPV6_multicast	xxxx::/8

IPv6アドレステンプレート

名前	IPv6アドレスプレフィックス
test1_IPv6_template	2001:xxx:0:cd30::/60
test2_IPv6_template	2001:xxx:0:cd30::/60

サービス

名前	サービスタイプ	詳細				IP/FQDN	カテゴリ	プロトコル
		TCP	UDP	ICMP	SCTP			
ALL	ファイアフォール						一般	IP
FTP	ファイアフォール	21				0.0.0.0	file access	TCP/UDP/SCTP
FTP_GET	ファイアフォール	21				0.0.0.0	file access	TCP/UDP/SCTP
FTP_PUT	ファイアフォール	21				0.0.0.0	file access	TCP/UDP/SCTP
DNS	ファイアフォール	53	53			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
HTTP	ファイアフォール	80				0.0.0.0	web access	TCP/UDP/SCTP
HTTPS	ファイアフォール	443				0.0.0.0	web access	TCP/UDP/SCTP
IMAP	ファイアフォール	143				0.0.0.0	Eメール	TCP/UDP/SCTP
IMAPS	ファイアフォール	993				0.0.0.0	Eメール	TCP/UDP/SCTP
LDAP	ファイアフォール	389				0.0.0.0	認証	TCP/UDP/SCTP
DCE-RPC	ファイアフォール	135	135			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
POP3	ファイアフォール	110				0.0.0.0	Eメール	TCP/UDP/SCTP
POP3S	ファイアフォール	995				0.0.0.0	Eメール	TCP/UDP/SCTP
SAMBA	ファイアフォール	139				0.0.0.0	file access	TCP/UDP/SCTP
SMTP	ファイアフォール	25				0.0.0.0	Eメール	TCP/UDP/SCTP
SMTPS	ファイアフォール	465				0.0.0.0	Eメール	TCP/UDP/SCTP
KERBEROS	ファイアフォール	88 464	88 464			0.0.0.0	認証	TCP/UDP/SCTP
LDAP_UDP	ファイアフォール		389			0.0.0.0	認証	TCP/UDP/SCTP
SMB	ファイアフォール	445				0.0.0.0	file access	TCP/UDP/SCTP
ALL_TCP	ファイアフォール	1-65535				0.0.0.0	一般	TCP/UDP/SCTP
ALL_UDP	ファイアフォール		1-65535			0.0.0.0	一般	TCP/UDP/SCTP
ALL_ICMP	ファイアフォール						一般	ICMP
ALL_ICMP6	ファイアフォール						一般	ICMP6
GRE	ファイアフォール						tunneling	IP
AH	ファイアフォール						tunneling	IP
ESP	ファイアフォール						tunneling	IP
AOL	ファイアフォール	5190-5194				0.0.0.0		TCP/UDP/SCTP
BGP	ファイアフォール	179				0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
DHCP	ファイアフォール		67-68			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
FINGER	ファイアフォール	79				0.0.0.0		TCP/UDP/SCTP
GOPHER	ファイアフォール	70				0.0.0.0		TCP/UDP/SCTP
H323	ファイアフォール	1720 1503	1719			0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
IKE	ファイアフォール		500 4500			0.0.0.0	tunneling	TCP/UDP/SCTP
Internet-Locator-Service	ファイアフォール	389				0.0.0.0		TCP/UDP/SCTP
IRC	ファイアフォール	6660-6669				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP

L2TP	ファイアフォール	1701	1701			0.0.0.0	tunneling	TCP/UDP/SCTP
NetMeeting	ファイアフォール	1720				0.0.0.0		TCP/UDP/SCTP
NFS	ファイアフォール	111 2049	111 2049			0.0.0.0	file access	TCP/UDP/SCTP
NNTP	ファイアフォール	119				0.0.0.0		TCP/UDP/SCTP
NTP	ファイアフォール	123	123			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
OSPF	ファイアフォール						ネットワークサービス	IP
PC-Anywhere	ファイアフォール	5631	5632			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
PING	ファイアフォール						ネットワークサービス	ICMP
TIMESTAMP	ファイアフォール							ICMP
INFO_REQUEST	ファイアフォール							ICMP
INFO_ADDRESS	ファイアフォール							ICMP
ONC-RPC	ファイアフォール	111	111			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
PPTP	ファイアフォール	1723				0.0.0.0	tunneling	TCP/UDP/SCTP
QUAKE	ファイアフォール		26000 27000 27910 27960			0.0.0.0		TCP/UDP/SCTP
RAUDIO	ファイアフォール		7070			0.0.0.0		TCP/UDP/SCTP
REXEC	ファイアフォール	512				0.0.0.0		TCP/UDP/SCTP
RIP	ファイアフォール		520			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
RLOGIN	ファイアフォール	513:512-1023				0.0.0.0		TCP/UDP/SCTP
RSH	ファイアフォール	514:512-1023				0.0.0.0		TCP/UDP/SCTP
SCCP	ファイアフォール	2000				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
SIP	ファイアフォール	5060	5060			0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
SIP-MSNmessenger	ファイアフォール	1863				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
SNMP	ファイアフォール	161-162	161-162			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
SSH	ファイアフォール	22				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
SYSLOG	ファイアフォール		514			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
TALK	ファイアフォール		517-518			0.0.0.0		TCP/UDP/SCTP
TELNET	ファイアフォール	23				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
TFTP	ファイアフォール		69			0.0.0.0	file access	TCP/UDP/SCTP
MGCP	ファイアフォール		2427 2727			0.0.0.0		TCP/UDP/SCTP
UUCP	ファイアフォール	540				0.0.0.0		TCP/UDP/SCTP
VDOLIVE	ファイアフォール	7000-7010				0.0.0.0		TCP/UDP/SCTP
WAIS	ファイアフォール	210				0.0.0.0		TCP/UDP/SCTP
WINFRAME	ファイアフォール	1494 2598				0.0.0.0		TCP/UDP/SCTP
X-WINDOWS	ファイアフォール	6000-6063				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
PING6	ファイアフォール							ICMP6
MS-SQL	ファイアフォール	1433 1434				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP

MYSQL	ファイアフォール	3306				0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
RDP	ファイアフォール	3389				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
VNC	ファイアフォール	5900				0.0.0.0	リモートアクセス	TCP/UDP/SCTP
DHCP6	ファイアフォール		546 547			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
SQUID	ファイアフォール	3128				0.0.0.0	tunneling	TCP/UDP/SCTP
SOCKS	ファイアフォール	1080	1080			0.0.0.0	tunneling	TCP/UDP/SCTP
WINS	ファイアフォール	1512	1512			0.0.0.0	リモートアクセス	TCP/UDP/SCTP
RADIUS	ファイアフォール		1812 1813			0.0.0.0	認証	TCP/UDP/SCTP
RADIUS-OLD	ファイアフォール		1645 1646			0.0.0.0		TCP/UDP/SCTP
CVSPSERVER	ファイアフォール	2401	2401			0.0.0.0		TCP/UDP/SCTP
AFS3	ファイアフォール	7000-7009	7000-7009			0.0.0.0	file access	TCP/UDP/SCTP
TRACEROUTE	ファイアフォール		33434-33535			0.0.0.0	ネットワークサービス	TCP/UDP/SCTP
RTSP	ファイアフォール	554 7070 8554	554			0.0.0.0	voip, messaging & other applications	TCP/UDP/SCTP
MMS	ファイアフォール	1755	1024-5000			0.0.0.0		TCP/UDP/SCTP
NONE	ファイアフォール	0				0.0.0.0		TCP/UDP/SCTP
webproxy	Explicitプロキシ	0-65535:0-65535				0.0.0.0	web proxy	ALL
test1_TCP_IP	ファイアフォール	1-10:1-10 1-65535	1-65535		1-65535	123.123.0.0	Eメール	TCP/UDP/SCTP
test1_TCP_FQDN	ファイアフォール	1-65535:1-10	1-65535:11-20		1-65535:21-30	0.0.0.0aaa.aa	web access	TCP/UDP/SCTP
test1_ICPM	ファイアフォール			255			一般	ICMP
test1_ICPM6	ファイアフォール			255			web proxy	ICMP6
test1_IP	ファイアフォール						web access	IP

スケジュール

繰り返し

名前	日	時間（開始と終了どちらも"00:00"の場合は"終日"です。）	
		開始	終了
always	日曜, 月曜, 火曜, 水曜, 木曜, 金曜, 土曜	00:00	00:00
none	none	00:00	00:00
default-darrp-optimize	日曜, 月曜, 火曜, 水曜, 木曜, 金曜, 土曜	01:00	01:30

ワンタイム

名前	開始日	終了日	有効期限切れ前イベントログ	期限までの日数
onetime_test	00:00 2024/10/09	00:00 2024/10/29	disable	0

スケジュールグループ

名前	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
test_schedule_01	onetime_test always default-darrp-optimize none onetime_test_2
test_schedule_02	always

バーチャルIP

IPv4

名前	インターフェース	マッピング元	マッピング先	ステータス
test1_IPv4_IP	test_1	192.123.0.0	192.123.0.0 192:xx::	

IPv6

名前	マッピング元	マッピング先	
		IPv4アドレス/範囲	IPv6アドレス/範囲
test1_IPv6	192:xx::	disable	192:xx::
test1_IPv6	192:xx::	disable	192:xx::
test1_IPv6	192:xx::	disable	192:xx::

IPv4 バーチャルIPグループ

名前	インターフェース	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
test1_IPv4_VIP	fortilink	test2_IPv4_FQDN

IPv6 バーチャルIPグループ

名前	メンバー ※記入欄に記載する設定値が多い場合は一部省略しています。
VIPgroup_IPv6_01VIPgroup_02	test1_IPv6
VIPgroup_IPv6_02VIPgroup_02	test1_IPv6 test1_IPv6_2

IPプール

IPv4

名前	外部IP範囲	タイプ	ARPリプライ
test1_IPv4	192.123.0.0 - 192.123.0.0	オーバーロード	enable
test2_IPv4	192.123.1.0 - 192.123.1.0	1対1	enable
test3_IPv4	192.123.2.0 - 192.123.2.0	固定ポート範囲	enable
test4_IPv4	192.123.3.0 - 192.123.3.0	ポートをブロック割り当て	disable

IPv6

名前	外部IP範囲
test1_IPv6	xx:a1:: - xx:a10::
test2_IPv6	xxxx:a1:: - xxxx:a1::
test3_IPv6	xxxx:a11:: - xxxx:a100::

10. ポリシー&オブジェクト（ファイアウォールポリシー）

No. 1

ID	1
名前	test01_FWpolicy
着信インターフェース	Interface03
発信インターフェース	loopback_test_3
送信元	
アドレス (IPv4)	login.xxxx.com
アドレス (IPv6)	
ユーザー	
ユーザーグループ	
インターネットサービス	
IPv6インターネットサービス	
送信元の無効化 (送信元をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
IP/MACベースアクセスコントロール	
宛先	
アドレス (IPv4)	login.xxxx.com
アドレス (IPv6)	
インターネットサービス	
IPv6インターネットサービス	
宛先の無効化 (宛先をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
スケジュール	always
サービス	ALL
アクション	許可
インスペクションモード	
プロキシHTTP(S) トラフィック	
ファイアウォール/ネットワークオプション	
NAT / NAT46 / NAT64	NAT
プロトコルオプション	default
免責事項オプション	
免責事項を表示	disable
ブロック通知	disable
認証メッセージをカスタマイズ	
セキュリティプロファイル	
アンチウイルス	
Webフィルタ	
ビデオフィルタ	
DNSフィルタ	
アプリケーションコントロール	
IPS	
ファイルフィルタ	
Eメールフィルタ	
VoIP	
ICAP	
Webアプリケーションファイアウォール	
DLPプロファイル	
SSLインスペクション	custom-deep-inspection
復号トラフィックミラー	
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
違反トラフィックをログ	utm
高度な設定	

WCCP	disable
キャプティブポータルから除外	disable
ワークフローマネジメント	
ポリシーの有効期限	enable
有効期限日	2025-03-27 18:29:00
コメント	
このポリシーを有効化	enable

No. 2

ID	4
名前	SSL-VPN-Access-Policy
着信インターフェース	ssl.root
発信インターフェース	lan
送信元	
アドレス (IPv4)	SSLVPN_TUNNEL_ADDR1
アドレス (IPv6)	
ユーザー	
ユーザーグループ	tesst04_remoteusergroup
	tesst05_remoteusergroup
インターネットサービス	
IPv6インターネットサービス	
送信元の無効化 (送信元をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
IP/MACベースアクセスコントロール	
宛先	
アドレス (IPv4)	all
アドレス (IPv6)	
インターネットサービス	
IPv6インターネットサービス	
宛先の無効化 (宛先をネゲート)	
アドレス (IPv4)	disable
アドレス (IPv6)	disable
インターネットサービス	
IPv6インターネットサービス	
スケジュール	always
サービス	ALL
アクション	許可
インスペクションモード	
プロキシHTTP(S) トラフィック	
ファイアウォール/ネットワークオプション	
NAT / NAT46 / NAT64	disable
プロトコルオプション	default
免責事項オプション	
免責事項を表示	
ブロック通知	disable
認証メッセージをカスタマイズ	
セキュリティプロファイル	
アンチウイルス	
Webフィルタ	
ビデオフィルタ	
DNSフィルタ	
アプリケーションコントロール	
IPS	
ファイルフィルタ	
Eメールフィルタ	
VoIP	
ICAP	

Webアプリケーションファイアウォール	
DLPプロファイル	
SSLインスペクション	no-inspection
復号トラフィックミラー	
ロギングオプション	
許可トラフィックをログ	すべてのセッション
違反トラフィックをログ	all
高度な設定	
WCCP	disable
キャプティブポータルから除外	
ワークフローマネジメント	
ポリシーの有効期限	disable
有効期限日	
コメント	
このポリシーを有効化	enable

11. ポリシー&オブジェクト（アドレス）

IPv4 アドレスグループ

No. 1

グループ名	G Suite
タイプ	グループ
メンバー	xxxx.com
	wildcard.xxxx.com
メンバーの除外	disable
メンバーの除外 メンバー	
スタティックルート設定	
コメント	

No. 2

グループ名	Microsoft Office 365
タイプ	グループ
メンバー	login.xxxx.com
	login.xxxx.com
	login.xxxx.com
メンバーの除外	disable
メンバーの除外 メンバー	
スタティックルート設定	
コメント	

No. 3

グループ名	test1_IPv4group
タイプ	フォルダ
メンバー	FIREWALL_AUTH_PORTAL_ADDRESS
	SSLVPN_TUNNEL_ADDR1
メンバーの除外	enable
メンバーの除外 メンバー	FIREWALL_AUTH_PORTAL_ADDRESS
スタティックルート設定	
コメント	

IPv6 アドレス

No. 1

名前	SSLVPN_TUNNEL_IPv6_ADDR1	
タイプ	サブネット	
IPv6アドレス	fdff:xxxx::/120	
IP範囲		
FQDN		
国/地域		
IPv6アドレステンプレート		
サブネットプレフィックス		
セグメント名	タイプ	値
ホストタイプ		
ホスト		
MACアドレス		
コメント		

No. 2

名前	all	
タイプ	サブネット	
IPv6アドレス	::/0	
IP範囲		
FQDN		
国/地域		
IPv6アドレステンプレート		
サブネットプレフィックス		
セグメント名	タイプ	値

ホストタイプ	
ホスト	
MACアドレス	
コメント	

IPv4 マルチキャストアドレス

No. 1

名前	all
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.0 - 192.255.255.255
ブロードキャストサブネット	
インターフェース	
コメント	

No. 2

名前	all_hosts
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.1 - 192.0.0.1
ブロードキャストサブネット	
インターフェース	
コメント	

No. 3

名前	all_routers
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.1 - 192.0.0.1
ブロードキャストサブネット	
インターフェース	
コメント	

No. 4

名前	Bonjour
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.1 - 192.0.0.1
ブロードキャストサブネット	
インターフェース	
コメント	

No. 5

名前	EIGRP
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.1 - 192.0.0.1
ブロードキャストサブネット	
インターフェース	
コメント	

No. 6

名前	OSPF
タイプ	マルチキャストIP範囲
マルチキャストIP範囲	192.0.0.1 - 192.0.0.1
ブロードキャストサブネット	
インターフェース	
コメント	

IPv6マルチキャストアドレス

No. 1

名前	all
IPv6アドレス	xxxx::/8
コメント	

No. 2

名前	test1_IPV6_multicast
IPv6アドレス	xxxx::/8

コメント	

No. 3

名前	test2_IPV6_multicast
IPv6アドレス	xxxx::/8
コメント	

IPv6アドレステンプレート

No. 1

名前		test1_IPv6_template	
IPv6アドレスプレフィックス		2001:xxx:0:cd30::/60	
サブネットセグメント			
セグメント名	ビット	排他	定義された値
country	4	disable	0x4
			0b0111
state	4	disable	
city	4	disable	
site	4	disable	
lan	4	disable	
vlan	4	disable	

No. 2

名前		test2_IPv6_template	
IPv6アドレスプレフィックス		2001:xxx:0:cd30::/60	
サブネットセグメント			
セグメント名	ビット	排他	定義された値
country	4	disable	0b0011
state	4	disable	
city_test_1	4	enable	0b0011
site_test_1	4	disable	0b0111
lan	4	disable	
vlan_test_4	4	enable	0b0111

12. ポリシー&オブジェクト（サービス）

No. 1

名前		ALL
サービスタイプ		ファイアフォール
コメント		
カテゴリ		一般
プロトコルオプション		
プロトコルタイプ		IP
タイプ		
コード		
アドレス	IP範囲	
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 2

名前		FTP
サービスタイプ		ファイアフォール
コメント		
カテゴリ		file access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
21		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 3

名前		FTP_GET
サービスタイプ		ファイアフォール
コメント		
カテゴリ		file access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
21		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 4

名前		FTP_PUT
サービスタイプ		ファイアフォール
コメント		
カテゴリ		file access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
21		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 5

名前		DNS
サービスタイプ		ファイアフォール
コメント		
カテゴリ		ネットワークサービス
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
53		
宛先ポート(UDP)		
宛先ポート		送信元ポート
53		
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 6

名前		HTTP
サービスタイプ		ファイアフォール
コメント		
カテゴリ		web access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
80		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

No. 7

名前		HTTPS
サービスタイプ		ファイアフォール
コメント		
カテゴリ		web access
プロトコルオプション		
プロトコルタイプ		TCP/UDP/SCTP
タイプ		
コード		
アドレス	IP範囲	0.0.0.0
	FQDN	
宛先ポート(TCP)		
宛先ポート		送信元ポート
443		
宛先ポート(UDP)		
宛先ポート		送信元ポート
宛先ポート(SCTP)		
宛先ポート		送信元ポート

13. ポリシー&オブジェクト（バーチャルIP）

IPv4

No. 1

名前			test1_IPv4_IP
コメント			
ステータス			
ネットワーク			
	インターフェース		test_1
	タイプ		スタティックNAT
	送信元インターフェースフィルタ		
	スタティックNAT	外部IPアドレス/範囲	192.123.0.0
		マップ	
		IPv4アドレス/範囲	192.123.0.0
		IPv6アドレス/範囲	xxx:a1::
	FQDN	外部 IP	
		外部 FQDN	
		マップされたアドレス	
オプションのフィルタ			
	送信元アドレス		192.123.1.0
			192.123.20.0
	サービス		"ALL_ICMP" "ALL_TCP" "test1_IP"
ポートフォワード			
	ポートフォワードが有効		enable
	プロトコル		
	ポートマッピングタイプ		
	外部サービスポート		
	IPv4ポートへマップ		65535
	IPv6ポートへマップ		65535

No. 2

名前			test2_IPv4_FQDN
コメント			
ステータス			
ネットワーク			
	インターフェース		any
	タイプ		FQDN
	送信元インターフェースフィルタ		
	スタティックNAT	外部IPアドレス/範囲	
		マップ	
		IPv4アドレス/範囲	
		IPv6アドレス/範囲	
	FQDN	外部 IP	0.0.0.0
		外部 FQDN	xxxx.com
		マップされたアドレス	xxxx.com
オプションのフィルタ			
	送信元アドレス		
	サービス		
ポートフォワード			
	ポートフォワードが有効		enable
	プロトコル		udp
	ポートマッピングタイプ		多対多
	外部サービスポート		65535
	IPv4ポートへマップ		65535
	IPv6ポートへマップ		

IPv6

No. 1

名前			test1_IPv6
コメント			
ネットワーク			

外部IPアドレス/範囲	123:xx::
マップ	
IPv6アドレス/範囲	124:xx::
IPv4アドレス/範囲	disable
オプションのフィルタ	
送信元アドレス	124:xx::
	xxx:d1::
	123:xx::
ポートフォワード	
ポートフォワードが有効	enable
プロトコル	tcp
外部サービスポート	65535
IPv6ポートへマップ	65535
IPv4ポートへマップ	65535

IPv4 バーチャルIPグループ

No. 1

名前	test1_IPv4_VIP
コメント	
インターフェース	fortilink
メンバー	test2_IPv4_FQDN

IPv6 バーチャルIPグループ

No. 1

名前	VIPgroup_IPv6_01
コメント	
メンバー	test1_IPv6

14. ポリシー&オブジェクト（IPプール）

IPv4

No. 1

名前	test1_IPv4
コメント	
タイプ	オーバーロード
外部IP範囲	192.123.0.0 - 192.123.0.0
ブロックサイズ	
Internal IP範囲	
ユーザあたりのブロック	
ユーザあたりのポート	
NAT64	enable
ARP リプライ	enable

No. 2

名前	test2_IPv4
コメント	
タイプ	1対1
外部IP範囲	192.123.0.0 - 192.123.0.0
ブロックサイズ	
Internal IP範囲	
ユーザあたりのブロック	
ユーザあたりのポート	
NAT64	
ARP リプライ	enable

No. 3

名前	test3_IPv4
コメント	
タイプ	固定ポート範囲
外部IP範囲	192.123.0.0 - 192.123.0.5
ブロックサイズ	
Internal IP範囲	192.123.0.0 - 192.123.0.5
ユーザあたりのブロック	
ユーザあたりのポート	32
NAT64	
ARP リプライ	enable

No. 4

名前	test4_IPv4
コメント	
タイプ	ポートをブロック割り当て
外部IP範囲	192.123.0.0 - 192.123.0.7
ブロックサイズ	568
Internal IP範囲	
ユーザあたりのブロック	111
ユーザあたりのポート	
NAT64	disable
ARP リプライ	disable

IPv6

No. 1

名前	test1_IPv6
コメント	
外部IP範囲	xx:a1:: - xx:a10::
NAT46	disable

No. 2

名前	test2_IPv6
コメント	
外部IP範囲	xx:a1:: - xx:a12::
NAT46	enable

No. 3

名前	test3_IPv6
コメント	
外部IP範囲	xx:a1:: - xx:a13::
NAT46	disable

15. セキュリティプロファイル（アンチウイルス）

No. 1

名前	g-default
コメント	Scan files and block viruses.
機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	disable	disable	ー	
SMTP	ブロック	disable	disable	enable	
POP3	ブロック	disable	disable	enable	
IMAP	ブロック	disable	disable	enable	
FTP	ブロック	disable	disable	ー	ー
CIFS	disable	disable	disable	ー	ー
MAPI					ー
SSH				ー	ー

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

No. 2

名前	g-sniffer-profile
コメント	Scan files and monitor viruses.

機能セット	フローベース

インスペクションされるプロトコル　※ バックアップファイルの構成に準拠しています。

プロトコル	アンチウイルススキャン (av-scan)	ウイルスアウトブレイク防止 / 外部マルウェアブロックリストを使用 (external-blocklist)	APTプロテクションオプション / 隔離 (quarantine)	APTプロテクションオプション / Eメール添付のWindows実行ファイルをウイルスとして扱う	APTプロテクションオプション / コンテンツ無害化 (content-disarm)
HTTP	ブロック	disable	disable	ー	
SMTP	ブロック	disable	disable	enable	
POP3	ブロック	disable	disable	enable	
IMAP	ブロック	disable	disable	enable	
FTP	ブロック	disable	disable	ー	ー
CIFS	disable	disable	disable	ー	ー
MAPI					ー
SSH				ー	ー

APTプロテクションオプション	
コンテンツ無害化オプション	
エラー発生時の送信を許可	
オフィスファイルにCDRを適用	
マクロの削除の有効化 (office-macro)	
ハイパーリンクの削除の有効化 (office-hylink)	
リンクされたオブジェクトの削除の有効化 (office-linked)	
埋め込まれたオブジェクトの削除の有効化 (office-embed)	
動的なデータ交換イベントの削除の有効化 (office-dde)	
PowerPoint アクション イベントの削除を有効化 (office-action)	
PDFファイルにCDRを適用	
PDFドキュメントのJavaScript削除の有効化 (pdf-javacode)	
PDFドキュメントの埋め込みファイル削除の有効化 (pdf-embedfile)	
PDFドキュメントのハイパーリンク削除の有効化 (pdf-hyperlink)	
PDFドキュメントアクションの他ドキュメントアクセス制限の有効化 (pdf-act-gotor)	
PDFドキュメントアクションの外部アプリ起動制限の有効化 (pdf-act-launch)	
PDFドキュメントアクションのサウンド再生制限の有効化 (pdf-act-sound)	
PDFドキュメントアクションの映画再生制限の有効化 (pdf-act-movie)	
PDFドキュメントアクションのJavaScript実行制限の有効化 (pdf-act-java)	
PDFドキュメントアクションのデータ送信機能の削除の有効化 (pdf-act-form)	
CDRの後に元のファイルを保持 (元のファイル宛先)	
CDRエラーが発生した場合の送信を許可	
処理済みドキュメントにカバーページを挿入	
モバイルマルウェアプロテクションを含める	enable
ウイルスアウトブレイク防止	
EMS脅威フィードの使用	disable

16. セキュリティプロファイル (WEBフィルタ)

No. 1

名前	g-default
コメント	Default web filtering.
機能セット	フローベース

FortiGuardカテゴリベースのフィルタ

ID	グループ	カテゴリ名	アクション
1	g01 Potentially Liable	Drug Abuse	モニタ
3	g01 Potentially Liable	Hacking	モニタ
4	g01 Potentially Liable	Illegal or Unethical	モニタ
5	g01 Potentially Liable	Discrimination	モニタ
6	g01 Potentially Liable	Explicit Violence	モニタ
12	g01 Potentially Liable	Extremist Groups	モニタ
59	g01 Potentially Liable	Proxy Avoidance	モニタ
62	g01 Potentially Liable	Plagiarism	モニタ
83	g01 Potentially Liable	Child Sexual Abuse	ブロック
96	g01 Potentially Liable	Terrorism	ブロック
98	g01 Potentially Liable	Crypto Mining	ブロック
99	g01 Potentially Liable	Potentially Unwanted Program	ブロック
2	g02 Adult/Mature Content	Alternative Beliefs	ブロック
7	g02 Adult/Mature Content	Abortion	ブロック
8	g02 Adult/Mature Content	Other Adult Materials	ブロック
9	g02 Adult/Mature Content	Advocacy Organizations	ブロック
11	g02 Adult/Mature Content	Gambling	ブロック
13	g02 Adult/Mature Content	Nudity and Risque	ブロック
14	g02 Adult/Mature Content	Pornography	ブロック
15	g02 Adult/Mature Content	Dating	ブロック
16	g02 Adult/Mature Content	Weapons (Sales)	ブロック
57	g02 Adult/Mature Content	Marijuana	ブロック
63	g02 Adult/Mature Content	Sex Education	ブロック
64	g02 Adult/Mature Content	Alcohol	ブロック
65	g02 Adult/Mature Content	Tobacco	ブロック
66	g02 Adult/Mature Content	Lingerie and Swimsuit	ブロック
67	g02 Adult/Mature Content	Sports Hunting and War Games	ブロック
26	g05 Security Risk	Malicious Websites	ブロック
61	g05 Security Risk	Phishing	ブロック
86	g05 Security Risk	Spam URLs	ブロック
88	g05 Security Risk	Dynamic DNS	ブロック
90	g05 Security Risk	Newly Observed Domain	ブロック
91	g05 Security Risk	Newly Registered Domain	ブロック
0	g21 Unrated	Unrated	ブロック

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	
オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分

サーチエンジン

Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	

スタティックURLフィルタ

無効なURLをブロック	
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック		disable		
コンテンツフィルタ				
パターンタイプ	パターン	言語	アクション	ステータス
レーティングオプション				
Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)				
ドメインまたはIPアドレスでURLをレーティング				
プロキシオプション				
HTTP POST アクション		許可		
Javaアプレットを削除				
ActiveXの削除				
Cookieを削除				

No. 2

名前		g-sniffer-profile	
コメント		Monitor web traffic.	
機能セット		フローベース	
FortiGuardカテゴリベースのフィルタ			
ID	グループ	カテゴリ名	アクション
1	g01 Potentially Liable	Drug Abuse	モニタ
3	g01 Potentially Liable	Hacking	モニタ
4	g01 Potentially Liable	Illegal or Unethical	モニタ
5	g01 Potentially Liable	Discrimination	モニタ
6	g01 Potentially Liable	Explicit Violence	モニタ
12	g01 Potentially Liable	Extremist Groups	モニタ
59	g01 Potentially Liable	Proxy Avoidance	モニタ
62	g01 Potentially Liable	Plagiarism	モニタ
83	g01 Potentially Liable	Child Sexual Abuse	モニタ
96	g01 Potentially Liable	Terrorism	モニタ
98	g01 Potentially Liable	Crypto Mining	モニタ
99	g01 Potentially Liable	Potentially Unwanted Program	モニタ
2	g02 Adult/Mature Content	Alternative Beliefs	モニタ
7	g02 Adult/Mature Content	Abortion	モニタ
8	g02 Adult/Mature Content	Other Adult Materials	モニタ
9	g02 Adult/Mature Content	Advocacy Organizations	モニタ
11	g02 Adult/Mature Content	Gambling	モニタ
13	g02 Adult/Mature Content	Nudity and Risque	モニタ
14	g02 Adult/Mature Content	Pornography	モニタ
15	g02 Adult/Mature Content	Dating	モニタ
16	g02 Adult/Mature Content	Weapons (Sales)	モニタ
57	g02 Adult/Mature Content	Marijuana	モニタ
63	g02 Adult/Mature Content	Sex Education	モニタ
64	g02 Adult/Mature Content	Alcohol	モニタ
65	g02 Adult/Mature Content	Tobacco	モニタ
66	g02 Adult/Mature Content	Lingerie and Swimsuit	モニタ
67	g02 Adult/Mature Content	Sports Hunting and War Games	モニタ
19	g04 Bandwidth Consuming	Freeware and Software Downloads	モニタ
24	g04 Bandwidth Consuming	File Sharing and Storage	モニタ
25	g04 Bandwidth Consuming	Streaming Media and Download	モニタ
72	g04 Bandwidth Consuming	Peer-to-peer File Sharing	モニタ
75	g04 Bandwidth Consuming	Internet Radio and TV	モニタ
76	g04 Bandwidth Consuming	Internet Telephony	モニタ
26	g05 Security Risk	Malicious Websites	モニタ
61	g05 Security Risk	Phishing	モニタ
86	g05 Security Risk	Spam URLs	モニタ
88	g05 Security Risk	Dynamic DNS	モニタ
90	g05 Security Risk	Newly Observed Domain	モニタ
91	g05 Security Risk	Newly Registered Domain	モニタ

17	g06 General Interest - Personal	Advertising	モニタ
18	g06 General Interest - Personal	Brokerage and Trading	モニタ
20	g06 General Interest - Personal	Games	モニタ
23	g06 General Interest - Personal	Web-based Email	モニタ
28	g06 General Interest - Personal	Entertainment	モニタ
29	g06 General Interest - Personal	Arts and Culture	モニタ
30	g06 General Interest - Personal	Education	モニタ
33	g06 General Interest - Personal	Health and Wellness	モニタ
34	g06 General Interest - Personal	Job Search	モニタ
35	g06 General Interest - Personal	Medicine	モニタ
36	g06 General Interest - Personal	News and Media	モニタ
37	g06 General Interest - Personal	Social Networking	モニタ
38	g06 General Interest - Personal	Political Organizations	モニタ
39	g06 General Interest - Personal	Reference	モニタ
40	g06 General Interest - Personal	Global Religion	モニタ
42	g06 General Interest - Personal	Shopping	モニタ
44	g06 General Interest - Personal	Society and Lifestyles	モニタ
46	g06 General Interest - Personal	Sports	モニタ
47	g06 General Interest - Personal	Travel	モニタ
48	g06 General Interest - Personal	Personal Vehicles	モニタ
54	g06 General Interest - Personal	Dynamic Content	モニタ
55	g06 General Interest - Personal	Meaningless Content	モニタ
58	g06 General Interest - Personal	Folklore	モニタ
68	g06 General Interest - Personal	Web Chat	モニタ
69	g06 General Interest - Personal	Instant Messaging	モニタ
70	g06 General Interest - Personal	Newsgroups and Message Boards	モニタ
71	g06 General Interest - Personal	Digital Postcards	モニタ
77	g06 General Interest - Personal	Child Education	モニタ
78	g06 General Interest - Personal	Real Estate	モニタ
79	g06 General Interest - Personal	Restaurant and Dining	モニタ
80	g06 General Interest - Personal	Personal Websites and Blogs	モニタ
82	g06 General Interest - Personal	Content Servers	モニタ
85	g06 General Interest - Personal	Domain Parking	モニタ
87	g06 General Interest - Personal	Personal Privacy	モニタ
89	g06 General Interest - Personal	Auction	モニタ
31	g07 General Interest - Business	Finance and Banking	モニタ
41	g07 General Interest - Business	Search Engines and Portals	モニタ
43	g07 General Interest - Business	General Organizations	モニタ
49	g07 General Interest - Business	Business	モニタ
50	g07 General Interest - Business	Information and Computer Security	モニタ
51	g07 General Interest - Business	Government and Legal Organizations	モニタ
52	g07 General Interest - Business	Information Technology	モニタ
53	g07 General Interest - Business	Armed Forces	モニタ
56	g07 General Interest - Business	Web Hosting	モニタ
81	g07 General Interest - Business	Secure Websites	モニタ
84	g07 General Interest - Business	Web-based Applications	モニタ
92	g07 General Interest - Business	Charitable Organizations	モニタ
93	g07 General Interest - Business	Remote Access	モニタ
94	g07 General Interest - Business	Web Analytics	モニタ
95	g07 General Interest - Business	Online Meeting	モニタ
97	g07 General Interest - Business	URL Shortening	モニタ
100	g07 General Interest - Business	Artificial Intelligence Technology	モニタ
101	g07 General Interest - Business	Cryptocurrency	モニタ
0	g21 Unrated	Unrated	モニタ

カテゴリ使用クォータ

カテゴリ	クォータ合計

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

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を有効	

オーバーライドできるグループ	
プロファイル名	
切り替え先	ユーザ
切り替え期間 モード	事前定義
切り替え期間	15分
サーチエンジン	
Google, Yahoo!, Bing, Yandex で 'セーフサーチ' を強制	
YouTubeへのアクセスを制限する	
すべての検査キーワードをログ	
スタティックURLフィルタ	
無効なURLをブロック	
URLフィルタ	

URL	タイプ	アクション	ステータス

FortiSandboxにより検知された悪意のあるURLをブロック	disable
コンテンツフィルタ	

パターンタイプ	パターン	言語	アクション	ステータス

レーティングオプション	
Behavior when FortiGuard is unreachable (レーティングエラー発生時にWebサイトを許可)	Block all websites (disable)
ドメインまたはIPアドレスでURLをレーティング	disable
プロキシオプション	
HTTP POST アクション	許可
Javaアプレットを削除	
ActiveXの削除	
Cookieを削除	

17. 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）

No. 1

名前		g-default
コメント		Monitor all applications.
ネットワークプロトコルの強制		disable
ポート	プロトコルの強制	違反アクション

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細			アクション
1	アプリケーション (ID):			許可
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:		
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	disable
DNSトラフィックの許可とログ	enable
HTTPベースアプリケーションの差し替えメッセージ	enable

No. 2

名前		g-sniffer-profile
コメント		Monitor all applications.
ネットワークプロトコルの強制		disable
ポート	プロトコルの強制	違反アクション

アプリケーションとフィルタのオーバーライド (基本カテゴリフィルターを含む)

※ アプリケーション (ID)はアプリケーションシグネチャのIDを記載しています。IDとその詳細は、コマンド"get application name status"で確認できます。

※ 各設定値のカッコ内の数値はIDです。

プライオリティ	詳細			アクション
1	アプリケーション (ID):			許可
	フィルター	ビヘイビア:	all	
		アプリケーションカテゴリ:		
		ポピュラリティ:	★☆☆☆☆	
			★★☆☆☆	
			★★★☆☆	
			★★★★☆	
			★★★★★	
		プロトコル:	all	
		リスク:		
		テクノロジー:	all	
		ベンダー:	all	

オプション	
デフォルト以外のポートで検知されたアプリケーションをブロック	disable
DNSトラフィックの許可とログ	
HTTPベースアプリケーションの差し替えメッセージ	enable

18. セキュリティプロファイル（侵入防止）（概要）

IPSセンサー

名前	コメント
all_default	All predefined signatures with default setting.
all_default_pass	All predefined signatures with PASS action.
protect_http_server	Protect against HTTP server-side vulnerabilities.
protect_email_server	Protect against email server-side vulnerabilities.
protect_client	Protect against client-side vulnerabilities.
high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities
wifi-default	Default configuration for offloading WiFi traffic.
sniffer-profile	Monitor IPS attacks.
default	Prevent critical attacks.

カスタムIPSシグネチャ

ID	名前	シグネチャ	コメント

19. セキュリティプロファイル（侵入防止）

IPSセンサー

No. 1

名前	all_default
コメント	All predefined signatures with default setting.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト　（隔離時間　日　時間　分）
	Action：default　Log：enable　Quarantine：none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	all
プロトコル	all
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間（秒）	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

No. 2

名前	all_default_pass
コメント	All predefined signatures with PASS action.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	モニター　（隔離時間　日　時間　分）
	Action：pass　Log：enable　Quarantine：none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	all
重大度	all
プロトコル	all
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	

レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間 (秒)	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

No. 3

名前	protect_http_server
コメント	Protect against HTTP server-side vulnerabilities.
悪意あるURLをブロック	無効
IPSシグネチャとフィルタ	
No. 1	
タイプ	フィルタ
アクション	デフォルト (隔離時間 日 時間 分)
	Action : default Log : enable Quarantine : none
パケットロギング	無効
ステータス	デフォルト
フィルター	
ターゲット	サーバー
重大度	■■■□□ (medium) ■■■■□ (high) ■■■■■ (critical)
プロトコル	HTTP
OS	all
アプリケーション	all
ステータス	all
アクション	all
脆弱性タイプ	
IPSシグネチャ	
レートベースの設定 ※デフォルトの設定では「しきい値」は0に設定されます	
しきい値	
期間 (秒)	
トラック	
除外するIP	
送信元	宛先
IPSシグネチャ	
ID	
30316	
10174	
26815	
27309	
40361	
15186	
17866	
17868	
38015	
40473	
37624	
ボットネットC&C	
ボットネットサイトへの発信接続をスキャン	無効

20. セキュリティプロファイル（SSL/SSHインスペクション）（概要）

SSL/SSHインスペクションプロファイル

SSL/SSHインスペクションプロファイルを下表に示します。

なお、次の3つは読み取り専用の標準プロファイルです。

・certificate-inspection

・deep-inspection

・no-inspection

名前	コメント
deep-inspection	Read-only deep inspection profile.
custom-deep-inspection	Customizable deep inspection profile.
no-inspection	Read-only profile that does no inspection.
certificate-inspection	Read-only SSL handshake inspection profile.
test01_SSL	
test02_SSL	
test03_SSL	
test04_SSL	
test05_SSL	
test06_SSL	
test07_SSL	
test08_SSL	
test09_SSL	
test10_SSL	
test11_SSL	
test12_SSL	SSH deep inspection (all ports)
test13_SSL	

21. セキュリティプロファイル (SSL/SSHインスペクション)

SSL/SSHインスペクションプロファイル

注記
本節では、SSLインスペクションオプションおよび共通オプションの一部の設定について、CLIおよび設定ファイル上の構成に基づき、プロトコルごとに記載しています。
そのため、FortiGate GUI（Web管理画面）上の表示項目と、本節の記載項目が一対一で対応しない場合があります。

No. 1

名前	deep-inspection						
コメント	Read-only deep inspection profile.						
SSLインスペクションオプション							
いずれかのSSLインスペクションを有効化	複数のサーバに接続する複数のクライアント						
インスペクション方式	フルSSLインスペクション						
CA証明書	Fortinet_CA_SSL						
悪意のある証明書	ブロック						
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
信頼されないSSL証明書		許可	許可	許可	許可	許可	許可
サーバ証明書SNIチェック		有効					
SSL暗号の準拠を強制	無効	無効	無効	無効	無効	無効	無効
SSLネゴシエーションの準拠を強制	無効	無効	無効	無効	無効	無効	無効
RPC over HTTPS							
HTTPS 経由の MAPI							
サーバ証明書							
プロトコルポートマッピング							
すべてのポートを検査する	無効						
プロトコルごとの設定							
	ステータス	ポート					
HTTPS	有効	443					
	暗号化されたクライアントHello :						
SMTPS	有効	465					
POP3S	有効	995					
IMAPS	有効	993					
FTPS	有効	990					
DNS over TLS	無効	853 (固定値)					
HTTP/3							
DNS over QUIC							
SSLインスペクションから除外							
著名なWebサイト	無効						
SSL除外のログを記録する	無効						
WEBカテゴリ							
ID	名前						
31	Finance and Banking						
33	Health and Wellness						
アドレス							
adobe							
Adobe Login							
android							
apple							
appstore							
mzstatic-apple							
SSHインスペクション							
SSH deep scan							
SSH port							
共通オプション							
無効なSSL証明書							
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
期限切れの証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
失効した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック

検証がタイムアウトした証明書		信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可
検証に失敗した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
SSLアノマリのログを記録する	有効						

No. 2

名前	custom-deep-inspection						
コメント	Customizable deep inspection profile.						
SSLインスペクションオプション							
いずれかのSSLインスペクションを有効化	複数のサーバに接続する複数のクライアント						
インスペクション方式	フルSSLインスペクション						
CA証明書	Fortinet_CA_SSL						
悪意のある証明書	ブロック						
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
信頼されないSSL証明書		許可	許可	許可	許可	許可	許可
サーバ証明書SNIチェック		有効					
SSL暗号の準拠を強制	無効	無効	無効	無効	無効	無効	無効
SSLネゴシエーションの準拠を強制	無効	無効	無効	無効	無効	無効	無効
RPC over HTTPS							
HTTPS 経由の MAPI							
サーバ証明書							
プロトコルポートマッピング							
すべてのポートを検査する	無効						
プロトコルごとの設定							
	ステータス			ポート			
HTTPS	有効			443			
	暗号化されたクライアントHello :						
SMTPS	有効			465			
POP3S	有効			995			
IMAPS	有効			993			
FTPS	有効			990			
DNS over TLS	無効			853 (固定値)			
HTTP/3							
DNS over QUIC							
SSLインスペクションから除外							
著名なWebサイト	無効						
SSL除外のログを記録する	無効						
WEBカテゴリ							
ID	名前						
31	Finance and Banking						
33	Health and Wellness						
アドレス							
android							
fortinet							
google-play							
icloud							
itunes							
microsoft							
skype							
SSHインスペクション							
SSH deep scan							
SSH port							
共通オプション							
無効なSSL証明書							
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
期限切れの証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
失効した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
検証がタイムアウトした証明書		信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可

検証に失敗した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
SSLアノマリのログを記録する	有効						

No. 3

名前	no-inspection						
コメント	Read-only profile that does no inspection.						
SSLインスペクションオプション							
いずれかのSSLインスペクションを有効化							
インスペクション方式	フルSSLインスペクション						
CA証明書	Fortinet_CA_SSL						
悪意のある証明書	ブロック						
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
信頼されないSSL証明書		許可	許可	許可	許可	許可	許可
サーバ証明書SNIチェック		有効					
SSL暗号の準拠を強制	無効	無効	無効	無効	無効	無効	無効
SSLネゴシエーションの準拠を強制	無効	無効	無効	無効	無効	無効	無効
RPC over HTTPS							
HTTPS 経由の MAPI							
サーバ証明書							
プロトコルポートマッピング							
すべてのポートを検査する	無効						
プロトコルごとの設定							
	ステータス			ポート			
HTTPS	無効						
	暗号化されたクライアントHello :						
SMTPS	無効						
POP3S	無効						
IMAPS	無効						
FTPS	無効						
DNS over TLS	無効			853 (固定値)			
HTTP/3							
DNS over QUIC							
SSLインスペクションから除外							
著名なWebサイト							
SSL除外のログを記録する							
WEBカテゴリ							
ID	名前						
アドレス							
SSHインスペクション							
SSH deep scan							
SSH port							
共通オプション							
無効なSSL証明書							
プロトコルごとの設定	SSL	HTTPS	SMTPS	POP3S	IMAPS	FTPS	DNS over TLS
期限切れの証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
失効した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
検証がタイムアウトした証明書		信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可	信頼しないまま許可
検証に失敗した証明書		ブロック	ブロック	ブロック	ブロック	ブロック	ブロック
SSLアノマリのログを記録する	有効						

22. VPN（概要）

IPsecトンネル

トンネル名	インターフェースバインディング
VPN_to_Opponent	lan
トンネル１	loopback_test_3
ハブアンド	lan
リモートア	loopback_test_3
カスタム	ssl.root
pojpoj,	ssl.root

IPsecアグリゲート

名前	アルゴリズム
agri	weighted-round-robin

IPsecコンセントレーター

名前	メンバー

SSL-VPNポータル

名前	トンネルモード	Webモード
full-access		有効

SSL-VPNレルム

URLパス	バーチャルホスト	最大同時ユーザー数
test		0
corp-realm	vpn.xxxx.com	50

SSL-VPNクライアント

トンネル	インターフェース	サーバ	ポート	コメント
test	Interface3	testtest	443	

23. VPN (IPsecトンネル)

No. 1

名前	VPN_to_Opponent
トンネルテンプレート (空白の場合はカスタム)	カスタム
ネットワーク	
インターフェースバインディング	lan
システムDNSを使用する	
IPアドレス	192.2.2.2
IPv4モード設定	
クライアントアドレス範囲	-
サブネットマスク	
DNSサーバ	
IPv4スプリットトンネルを有効化	
アクセス可能ネットワーク	
IPv6モード設定	
クライアントアドレス範囲	-
プレフィックス	
DNSサーバ	
IPv6スプリットトンネルを有効化	
アクセス可能ネットワーク	
デッドピア検知	オンデマンド
DPD再試行回数	3
DPD再試行間隔	20
前方誤り訂正	
イーグレス	無効
イングレス	無効
高度な設定	
ルートの追加	
オートディスカバリ送信側	無効
オートディスカバリ受信側	無効
インターフェースIPの交換	無効
デバイスの作成	無効
認証	
リモートデバイス/ダイナミックDNS	リモートデバイス
リモートIPアドレス	192.2.2.2
FQDN	
認証方式	事前共有鍵
事前共有鍵	********
証明書名	
ピアオプション	
受け入れるタイプ	any
ピアID	

フェーズ2セレクタ		
名前	ローカルアドレス	リモートアドレス
新規フェーズ 2	192.0.0.0 - 192.255.255.255	192.1.1.1

XAUTH	
クライアント	
ユーザ名	
パスワード	********
ユーザグループ *未記入の場合はポリシーから継承	

No. 2

名前	トンネル 1
トンネルテンプレート (空白の場合はカスタム)	サイト間 - FortiGate
ネットワーク	
インターフェースバインディング	loopback_test_3
システムDNSを使用する	
IPアドレス	192.1.1.1
IPv4モード設定	
クライアントアドレス範囲	-

サブネットマスク	
DNSサーバ	
IPv4スプリットトンネルを有効化	
アクセス可能ネットワーク	
IPv6モード設定	
クライアントアドレス範囲	-
プレフィックス	
DNSサーバ	
IPv6スプリットトンネルを有効化	
アクセス可能ネットワーク	
デッドピア検知	オンデマンド
DPD再試行回数	3
DPD再試行間隔	20
前方誤り訂正	
イーグレス	無効
イングレス	無効
高度な設定	
ルートの追加	
オートディスカバリ送信側	無効
オートディスカバリ受信側	無効
インターフェースIPの交換	無効
デバイスの作成	無効
認証	
リモートデバイス/ダイナミックDNS	リモートデバイス
リモートIPアドレス	192.1.1.1
FQDN	
認証方式	事前共有鍵
事前共有鍵	********
証明書名	
ピアオプション	
受け入れるタイプ	any
ピアID	

フェーズ2セレクタ

名前	ローカルアドレス	リモートアドレス
トンネル１サイト間	トンネル１サイト間_local	トンネル１サイト間_remote

XAUTH	
クライアント	
ユーザ名	
パスワード	
ユーザグループ *未記入の場合はポリシーから継承	

24. VPN（ハブ&スポーク トポロジ）

BGP

ネイバー

トンネルIP	AS
192.10.10.2	65001
192.10.10.1	65001

ネイバー範囲

プレフィックス	ネイバーグループ
192.10.10.0 255.255.255.0	HUB-GROUP
192.20.20.0 255.255.255.0	HUB-GROUP

25. VPN (SSL-VPN設定)

SSL-VPNステータス	有効

接続設定

リッスンするインターフェース	loopback_test_4
	test_10
リッスンするポート	443
サーバ証明書	Fortinet_Factory_Backup
HTTPをSSL-VPNにリダイレクト	無効
アクセスを制限 *特定ホストへアクセス制限未設定の場合は、任意のホストからのアクセスを許可	
特定ホストへアクセス制限	
ホスト (IPv4アドレス)	all
ホスト (IPv6アドレス)	all
送信元をネゲート	無効
アイドルログアウト	
非アクティブ (秒)	0
クライアント証明書を要求	無効

トンネルモードクライアント設定

アドレス範囲	
IPv4アドレス	SSLVPN_TUNNEL_ADDR1
IPv6アドレス	SSLVPN_TUNNEL_IPv6_ADDR1
DNSサーバ *DNSサーバ未設定の場合はクライアントシステムのDNSと同じ	
DNSサーバ #1	0.0.0.0
DNSサーバ #2	0.0.0.0
Ipv6 DNSサーバ #1	::
Ipv6 DNSサーバ #2	::
WINSサーバ	
WINSサーバ #1	0.0.0.0
WINSサーバ #2	0.0.0.0
IPv6 WINSサーバ #1	::
IPv6 WINSサーバ #2	::

WEBモードの設定

言語	ブラウザの設定

認証/ポータルマッピング

ユーザ	グループ	レルム	ポータル
QA	Guest-group	corp-realm	test1
guest	IPsec_Users	corp-realm	test2

26. VPN (SSL-VPNポータル)

No.1

名前	full-access
ユーザを一度に単一のSSL-VPN接続に制限する	無効
トンネルモード	
スプリットトンネリング	
ルーティングアドレスの上書き	
送信元IPプール	
Ipv6トンネルモード	
IPv6スプリットトンネリング	
IPv6ルーティングアドレスの上書き	
送信元IPv6プール	
トンネルモードクライアントオプション	
クライアントがパスワードを保存することを許可する	
クライアントの自動接続を許可する	
クライアントが接続をキープすることを許可する	
DNSスプリットトンネリング　(SplitDns)	

ドメイン	プライマリDNSサーバ	セカンダリDNSサーバ	プライマリDNSIpv6サーバ	セカンダリDNSIpv6サーバ

ホストチェックタイプ	
特定のOSバージョンに制限	

バージョン	アクション	トレランス	パッチレベル

WEBモード	有効
ランディングページ	カスタム
ポータルメッセージ	
テーマ	
デフォルトプロトコル	
セッション情報を表示	
接続ランチャーを表示	
ログイン履歴を表示	
ユーザブックマーク	
定義済みブックマークを表示	
ブックマークにフォーカス	
コンテンツIP/UIを書き換え	有効
RDP/VNCクリップボード	
定義済みブックマーク	
名前	
タイプ	
説明	
ホスト	
ポート	
URL	
シングルサインオン	
ユーザ名	
パスワード	
SSOフォームデータ	

フォームキー	フォーム値

フォルダー	
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	

制限付き管理者モード	
ユーザ名	
パスワード	
URL	testTest
SSOクレデンシャル	SSL-VPNログイン
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
FortiClientダウンロード	
ダウンロード方法	
ダウンロードロケーションのカスタマイズ	
Windows	
Mac	

No.2

名前	test1
ユーザを一度に単一のSSL-VPN接続に制限する	無効
トンネルモード	有効
スプリットトンネリング	ポリシーの宛先に基づいて有効
ルーティングアドレスの上書き	test_23 address
送信元IPプール	VLAN_test_2 address
Ipv6トンネルモード	有効
IPv6スプリットトンネリング	ポリシーの宛先に基づいて有効
IPv6ルーティングアドレスの上書き	all
送信元IPv6プール	SSLVPN_TUNNEL_IPv6_ADDR1
トンネルモードクライアントオプション	
クライアントがパスワードを保存することを許可する	有効
クライアントの自動接続を許可する	有効
クライアントが接続をキープすることを許可する	無効
DNSスプリットトンネリング　(SplitDns)	

ドメイン	プライマリDNSサーバ	セカンダリDNSサーバ	プライマリDNSIpv6サーバ	セカンダリDNSIpv6サーバ
test	192.1.1.1	192.1.1.1	::1	::2

ホストチェックタイプ	ファイアーウォール
特定のOSバージョンに制限	有効

バージョン	アクション	トレランス	パッチレベル
windows-7	許可		
windows-8.1	許可		
windows-10	許可		
windows-11	許可		
macos-mojave-10.14	許可		
macos-catalina-10.15	許可		
macos-bigsur-11.0	許可		
macos-bigsur-11.1	許可		
macos-bigsur-11.2	許可		
macos-bigsur-11.3	許可		
macos-bigsur-11.4	許可		
macos-bigsur-11.5	許可		
macos-bigsur-11.6	許可		
macos-bigsur-11.7	許可		
macos-monterey-12.0	許可		
macos-monterey-12.1	許可		
macos-monterey-12.2	許可		
macos-monterey-12.3	許可		
macos-monterey-12.4	許可		
macos-monterey-12.5	許可		
macos-monterey-12.6	許可		
macos-monterey-12.7	許可		
macos-ventura-13	許可		
macos-sonoma-14	許可		

WEBモード	有効
ランディングページ	デフォルト
ポータルメッセージ	SSL-VPN Portal
テーマ	jade
デフォルトプロトコル	FTP
セッション情報を表示	有効
接続ランチャーを表示	有効
ログイン履歴を表示	無効
ユーザブックマーク	有効
定義済みブックマークを表示	有効
ブックマークにフォーカス	無効
コンテンツIP/UIを書き換え	無効
RDP/VNCクリップボード	有効
定義済みブックマーク	
名前	ブックマーク
タイプ	HTTP/HTTPS
説明	
ホスト	
ポート	
URL	test
シングルサインオン	無効
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	
パスワード	
名前	test2
タイプ	FTP
説明	
ホスト	
ポート	
URL	
シングルサインオン	SSL-VPNログイン
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	test3
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	

Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	
パスワード	
名前	test4
タイプ	RDP
説明	
ホスト	bbbb
ポート	3389
URL	
シングルサインオン	無効
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	
ドメイン	
色深度	16
画面の幅	1
画面の高さ	3
キーボードレイアウト	en-us
セキュリティ	any
Preconnection IDを送信	有効
Preconnection ID	1
Preconnection Blob	test6
ロードバランシング情報	test7
制限付き管理者モード	有効
ユーザ名	test5
パスワード	********
名前	test8
タイプ	SFTP
説明	
ホスト	
ポート	
URL	
シングルサインオン	無効
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	test9
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	
パスワード	
名前	test10
タイプ	SMB/CIFS

説明	
ホスト	
ポート	
URL	
シングルサインオン	無効
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	test11
ドメイン	test12
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	
パスワード	
名前	test13
タイプ	SSH
説明	
ホスト	192.168.1.10
ポート	
URL	
シングルサインオン	
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	
パスワード	********
名前	test14
タイプ	TELNET
説明	
ホスト	192.168.1.10
ポート	0
URL	
シングルサインオン	
ユーザ名	
パスワード	
SSOフォームデータ	

フォームキー	フォーム値
フォルダー	
ドメイン	
色深度	
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	
パスワード	
名前	test16
タイプ	VNC
説明	
ホスト	192.168.1.10
ポート	5900
URL	
シングルサインオン	
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
フォルダー	
ドメイン	
色深度	16
画面の幅	
画面の高さ	
キーボードレイアウト	
セキュリティ	
Preconnection IDを送信	
Preconnection ID	
Preconnection Blob	
ロードバランシング情報	
制限付き管理者モード	
ユーザ名	test17
パスワード	********
URL	
SSOクレデンシャル	
ユーザ名	
パスワード	
SSOフォームデータ	
フォームキー	フォーム値
FortiClientダウンロード	有効
ダウンロード方法	direct
ダウンロードロケーションのカスタマイズ	無効
Windows	
Mac	