

DEPLOYMENT GUIDE

セキュアSDブランチ 7.4設定ガイド

FortiSwitch 接続編

Version 1.00 2024年1月



免責事項

本ドキュメントに関する著作権は、フォーティネットジャパン合同会社へ帰属します。 フォーティネットジャパン合同会社が事前に承諾している場合を除き、形態及び手段を 問わず本ドキュメントまたはその一部を複製する事は禁じられています。 また本内容は参考例となります。個別のセキュリティ対策に関する要件を満たすには、 ご利用者様ごとにプランニングおよび設定の調整が必要となりますので、予めご了承 下さい。尚、本ドキュメントの作成にあたっては細心の注意を払っておりますが、その 記述内容は予告なしに変更される事があります。

目次

第一章:はじめに	<u>4</u>
第二章:FortiLinkの設定	<u>5</u>
第三章:FortiSwitchの接続、設定	<u>9</u>
Appendix : FortiGate GUIアクセス	<u>15</u>
改定履歴	<u>16</u>

1. はじめに

現代のネットワーク環境では、効率的かつ安全な運用管理が求められています。その中心となるのが、FortiLink を使用したFortiSwitchの管理ソリューション「セキュアSDブランチ」です。このガイドでは、FortiLinkを利用 してFortiSwitchを遠隔で管理する方法であるセキュアSDブランチについて詳しく解説していきます。

FortiLinkは、FortiGateをスイッチコントローラーとして使用し、ディストリビューションFortiSwitchに接続す ることで、ネットワークの各エッジまで安全性を拡張し、統一されたアクセス制御を提供します。この設定を通 じて、異なるVLANの作成・管理や802.1X認証、ファイアウォールポリシーなど、FortiOSの包括的なセキュリ ティ機能を活用することが可能になります。

このガイドでは、FortiLinkを使ったFortiSwitchの基本的な設定手順をステップバイステップで説明し、セキュ アSDブランチの構築の方法を提供します。

1-1. 利用機器と OS バージョン

FortiGate-100F	7.4.2
FortiSwitxh-224E-POE	7.4.2

1-2. 構成



1-3. 参考資料

本ガイドで紹介している設定は公式な設定ガイドに基づいています。より詳細な情報が必要な場合は以下も合わせてご参照ください。

https://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/173270/fortiswitch-management

2. FortiLink の設定

以下の手順でFortiLink を設定します。

- 1.FortiGate のスイッチコントローラーの有効化
- 2.FortiLinkインターフェースの設定
- 3.FortiSwitchポートの自動検出

1.FortiGate のスイッチコントローラーの有効化

FortiGateにログインし、CLIで以下を入力します。

config system global

set switch-controller enable

end

GUIで行う場合、「System」>「表示機能設定」のコア機能「スイッチコントローラー」を有効にします。



2.FortiLinkインターフェースの設定

FortiLinkで使用するインターフェースを設定します。この設定はGUIを用いることを推奨します。 FortiGateはモデルによりデフォルトのFortiLink用インターフェースが設定されている場合があります。ご利用 になるモデルのデータシートをご参照ください。FortiGate-100Fの場合、X1/X2 がそれに該当します。本ガイ ドではポート20をFortiLink用に構成します。





「ネットワーク」>インターフェースの「802.3ad アグリゲート」下の「FortiLink」をクリック、編集をクリッ クしFortiLinkインターフェースの設定を行います。

FG100F_Marketing	• ≡ Q		
 	➤ Image: Second s	13 15 17 19 	
DNS IPAM FortiExtenders	+ 新規作成 ● 削除 ● インターフェイスを統合 名前 ◆ タイプ ◆	検索 メンバー ◆	IP/ネットマスク◆
SD-WAN	🔲 🖶 802.3ad アグリゲート 🔞		
スタティックルート ポリシールート	■ D fortilink D 802.3ad アグリゲート	. x1 . x2	FortiSwitch専用
RIP	■ 言 LANの拡張 ①		
	2-3 FortiLinkインターフェース設定		

インターフェースの編集画面で、インターフェースメンバーの項の「+」をクリックし、FortiLinkで使用する物 理ポートの設定を行います。ここでは、X1/X2を削除し、ポート20を追加します。

インターフェースの編集	
名前	₽ fortilink
エイリアス	
タイプ	➡ FortiLink (802.3ad アグリゲート)
VRFID 🚯	0
インターフェースメンバ・	- x1 × = x2 × +
2-4 イン	ターフェースメンバー編集

エントリ編集画面では、ポート名をクリックするたびに、選択→非選択に表示が遷移します。必要なポートが選 択された状態になるようにし、「クローズ」をクリックし終了します。

エントリを選択 🗙
Q検索
im port20
🛗 ha1
🗎 ha2
📃 x1
📃 x2
クローズ

2-5 エントリ選択画面

インターフェースの編集					
名前	Be fortilink				
エイリアス					
タイプ	➡ FortiLink (802.3ad アグリゲート)				
VRF ID 🚯	0				
インターフェースメンバー	m port20 ×				
	+				

2-6 インターフェースメンバー編集

「デバイスを自動的に承認」オプションを有効化、それ以外の項目はデフォルト設定のまま「OK」をクリックし、設定を保存します。

インターフェースの編集	
アドレス	
アドレッシングモード	マニュアル IPAM DHCP PPPoE ワンアームスニファー FortiSwitch専用
IP/ネットマスク	169.254.1.1/255.255.255.0
接続デバイス	FortiSwitch
デバイスを自動的に承認 🚯	
FortiLinkスプリットインターフェース	
ロックタウンISL	
OHCPサーバ	
DHCPステータス O 4	国効化済み 🔮 無効化済み
アドレス範囲 169.	254.1.2-169.254.1.254
	•
ネットマスク 255.	255.255.0
デフォルトゲートウェイ イン	ターフェースIPと同じ 指定
DNSサーバ シス	テムDNSと同じ インターフェースIPと同じ 指定
リース時間 🚯 🔹 6048	800 秒
FortiClient On-Netステータス 🌑	
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	
アウトバウンド帯域幅	0
その他	
	OK キャンセル
2	-7 インターフェースメンバー編集(続)

3.FortiSwitchポートの自動検出設定

FortiSwitchOS 7.2.0以降では、デフォルトですべてのポートで自動検出が有効になっているため、スイッチ側の設定は不要です。また、FortiSwitchOS 3.4.0以降では、最後の4つのポートがデフォルトで自動検出が有効になっています。いずれのポートも手動でFortiLink用に設定することができます。

3. FortiSwitch の接続、設定

FortiSwitchの接続

FortiGate-100Fのポート20とFortiSwitch224E-POEのポート1をイーサネットケーブルで接続します。

「WiFi&スイッチコントローラー」>「マネージドFortiSwitch」をクリックしトポロジ画面を開きます。

FG100F_Marketing	- ≡	۹			
● セキュリティプロファイ ル	, Î	▶新規作成	¤ ステッチアクション▼	2 リフレッシュ	◆ 並び替え 検索
UPN	>			FortiLinkス	タック: fortilink
▲ ユーザ&認証	>	5 FG100F	Marketing		10000750
☆ WiFi & スイッチコント ローラー	•	✤ fortilink		szz4EPTF fort1	18000037
・ マネージドFortiAP					
WiFiクライアント					
WiFiマップ					
SSID					
FortiAPプロファイル					
WIDSプロファイル					
WiFi設定					
FortiLinkインターフェー ス					
マネージドFortiSwitch	☆				
		図3-1	FortiSwitch管理画	画面	

自動承認によってFortiLinkが確立すると、FortiGateとFortiSwitchが黒実線で接続します。

同画面にある状態の凡例を参考に状態を確認してください。



図3-2 状態の凡例

VLAN設定

FortiGateから管理対象のFortiSwitchのVLANを一元的に設定、管理できます。

「WiFi&スイッチコントローラー」>「FortiSwitch VLAN」をクリック、「+新規作成」をクリックし、「新規 インターフェース作成画面」を開きます。



図3-3 FortiSwitch VLAN画面

以下の通り設定し、「OK」をクリックし保存します。お客様の環境に合わせて設定してください。

名前: vlan200

VLAN ID: 200

アドレス

アドレッシングモード:マニュアル

IP/ネットマスク: 172.16.0.1/24

新規インターン	フェース	
名前	vlan 200	
エイリアス		
タイプ	3冊 VLAN	
インターフュ	ェース 🗜 fortilink	
VLAN ID	200	
VRF ID 🚯	0	
カラー	■ 変更	
ロール 🕚	LAN	•
アドレス		
アドレッシン	ングモード	マニュアル IPAM DHCP PPPoE ワンアームスニファー
IP/ネットマン	スク	172.16.0.1/24
アドレスオン	ブジェクトに一致するサブネ	ットの作成
名前		vlan 200 address
宛先		172.16.0.0/24
セカンダリル	Pアドレス	
管理者アクセ	セス	
IDv4	□ HTTPS	□ HTTP 1 □ PING
11 V-1	□ FMGアクセス	SSH SNMP
	G FTM	□ RADIUSアカウンティン □ セキュリティファブリッ
		グ ク接続 🕄
	□ スピードテスト	
О ПНСР	ナーノベ	
ネットワーク	ク	
		OK キャンセル
	 図	3-4 新規インターフェース作成画面

FortiSwitch VLAN画面にて、作成したVLANを確認することができます。

-	•新規作成	Q		
	名前♥	VLAN ID ≑	IP 🗢	
	📲 quarantine.fortilink (quarantine)	4093	169.254.11.1/255.255.255.0	
	제품 rspan.fortilink (rspan)	4092	169.254.14.1/255.255.255.0	
	¤₿ default.fortilink (_default)	1	0.0.0/0.0.0.0	
۰	x≌ nac segment.fortilink (nac segment)	4088	10.255.11.1/255.255.2	
l	≭≣ vlan 200	200	172.16.0.1/255.255.255.0	

図3-5 FortiSwitch VLAN画面

スイッチポートの設定

スイッチのポート10から20を vlan200に設定します。

「WiFi&スイッチコントローラー」>「FortiSwitchポート」をクリックし、スイッチポート画面を開きます。

式 FG100F_Marketing		≡ વ				
▲ セキュリティプロファイ	`	➡ 新規作	成▼ 《 編	創 前 前 除	検索	
- <i>n</i>		ポート	トランク	モード	ポートポリシー	有効な機i
U VPN	>	S224FP	TF18000659	(28)		
💄 ユーザ&認証	>	C port1				
^{♥ WiFi & スイッチコント} [●] ローラー	~	G port2		スタティック		♥ エッジポート
マネージドFortiAP	- 1	(nort?		7 5 - 100 5		
WiFiクライアント		V ports		スタティック		 ▼ エッシホート ◆ スパニングツリ
WiFiマップ		🔮 port4		スタティック		● エッジポート
SSID		- (F				
FortiAPプロファイル	. 1	G/ port5		スタテイツク		 ▼ エッジホート ◆ スパニングツリ
WIDSプロファイル	お	気に入り追加	I	スタティック		⊘ エッジポート
WiFi設定	Û					♥ スパニングツリ
FortiLinkインターフェー ス		🔮 port7		スタティック		 ♥ エッジポート ♥ スパニングツリ
マネージドFortiSwitch		🕑 port8		スタティック		 ♥ エッジポート ♥ スパニングツリ
FortiSwitchクライアント		🔮 port9		スタティック		⊘ エッジポート
FortiSwitch VLAN						♥ スパニングツリ
FortiSwitchポート	☆	🔮 port10		スタティック		 ✓ エッジポート ✓ スパニングツリ
FortiSwitchポートポリシ		🔮 port11		スタティック		⊘ エッジポート
		図3-6	FortiSwitc	h ポート画面	ī	

ポート表示になっていない場合、右上の表示切替ボタンの「ポート」をクリックし、ポート表示に切り替えます。



ポート10をクリックして選択状態にし、Shiftキーを押した状態でポート20をクリックすることで、複数ポートを選 択することができます。この状態でネイティブVLANカラム上にマウスオーバーし、表示された編集マークをクリッ ク、VLAN選択画面を表示させます。

ポート	トランク	モード	ポートポリシー	有効な機能	ネイティブVLAN	許可するVLAN	4
🖤 port8		スタティック		 ♥ エッジボート ♥ スパニングツリープロトコル 	≍∦ default.fortilink (_default)	x quarantine.fortilink (quarantine)	
🔮 port9		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	≭¦ default.fortilink (_default)	🛪 quarantine.fortilink (quarantine)	
🔮 port10		スタティック		 ● エッジポート ● スパニングツリープロトコル 	제월 default.fortilink (_lefau	📲 quarantine.fortilink (quarantine)	
🕑 port11		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	쳐 default.fortilink (_default)	📲 quarantine.fortilink (quarantine)	
🚭 port12		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	≍∦ default.fortilink (_default)	📲 quarantine.fortilink (quarantine)	
🔮 port13		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	제품 default.fortilink (_default)	≍ quarantine.fortilink (quarantine)	
🔮 port14		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	쳐울 default.fortilink (_default)	¤∰ quarantine.fortilink (quarantine)	
🔮 port15		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	쳐 default.fortilink (_default)	¤∰ quarantine.fortilink (quarantine)	
🔮 port16		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	제를 default.fortilink (_default)	¤∰ quarantine.fortilink (quarantine)	
🔮 port17		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	제를 default.fortilink (_default)	¤∰ quarantine.fortilink (quarantine)	
🔮 port18		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	≍∰ default.fortilink (_default)	≍ quarantine.fortilink (quarantine)	
🔮 port19		スタティック		 ● エッジポート ● スパニングツリープロトコル 	제품 default.fortilink (_default)	≍∰ quarantine.fortilink (quarantine)	
🔮 port20		スタティック		 ♥ エッジポート ♥ スパニングツリープロトコル 	제를 default.fortilink (_default)	¤∰ quarantine.fortilink (quarantine)	
🔮 port21		スタティック		 ▼エッジポート スパニングツリープロトコル 	≭ default.fortilink (_default)	📲 quarantine.fortilink (quarantine)	

図3-8 編集マーク表示

作成済みのvlan 200を選択、適用をクリックします。

エントリを選択	×		
Q検索	➡ 新規作成		
端 default.fortilink (_default) 端 rspan.fortilink (rspan)			
≭≣ vlan 200			
適用	キャンセル		
図3-9 VLANエントリ画面			

選択したすべてのポートにvlan200の割当が完了しました。

🕑 port10	スタティック	 ● エッジポート ● スパニングツリープロトコル 	≭∦ vlan 200
🔮 port11	スタティック	 ▼エッジポート スパニングツリープロトコル 	¤≣ vlan 200
🔮 port12	スタティック	 ● エッジポート ● スパニングツリープロトコル 	¤≣ vlan 200
🔮 port13	スタティック	 ♥ エッジポート ♥ スパニングツリープロトコル 	≭≣ vlan 200
🔮 port14	スタティック	 ♥ エッジポート ♥ スパニングツリープロトコル 	¤∄ vlan 200
🔮 port15	スタティック	 ♥ エッジポート ♥ スパニングツリープロトコル 	¤∄ vlan 200
🔮 port16	スタティック	 ♥ エッジポート ♥ スパニングツリープロトコル 	¤∄ vlan 200
🔮 port17	スタティック	 ♥ エッジポート ♥ スパニングツリープロトコル 	¤∄ vlan 200
🔮 port18	スタティック	 ● エッジポート ● スパニングツリープロトコル 	¤∄ vlan 200
🔮 port19	スタティック	 ♥ エッジボート ♥ スパニングツリープロトコル 	¤∄ vlan 200
🔮 port20	スタティック	 ♥ エッジポート ♥ スパニングツリープロトコル 	¤∄ vlan 200

図3-10 適用されたVLAN

Appendix FortiGate GUI アクセス

工場出荷状態ログインおよび環境設定

コンソールPCのIPアドレスを192.168.1.0/24のネットワーク(ホストアドレスは99以外)に設定し、FortiGate-100FのMGMTポートに接続します。

Webブラウザで「http://192.168.1.99」にアクセスすると、FortiGateのログイン画面が表示されます。

	•	
1	Username	
1	Password	
	Login	
	20011	
	図Ap-1.ログイン画面	

以下のデフォルトクレデンシャル情報を入力し、「Login」をクリックします。

ユーザ名:admin

パスワード:なし

初回のみ、パスワードの変更を促す画面が表示されます。新しいパスワードを設定します。

Change Password		
A You are required to change the default password.		
Old Password		
•••••		
ОК		
Logout		
図Ap-2.パスワード変更画面		

環境設定を行います。

左ペイン「System」>「Setting」を選択、以下の通り設定のうえ「Apply」をクリックし、設定を保存します。 Time zone : (GMT+9:00) Asia/Tokyo

Language : Japanese

表示が日本語に切り替わります。

改定履歴

バージョン	リリース日	改定履歴
1.0.0	2024.1	初版発行