

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	4
第二章：FortiLinkの設定	5
第三章：FortiSwitchの接続、設定	9
Appendix：FortiGate GUIアクセス	15
改定履歴	16

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

FortiSwitch-224E-POE 7.4.2

1-2. 構成

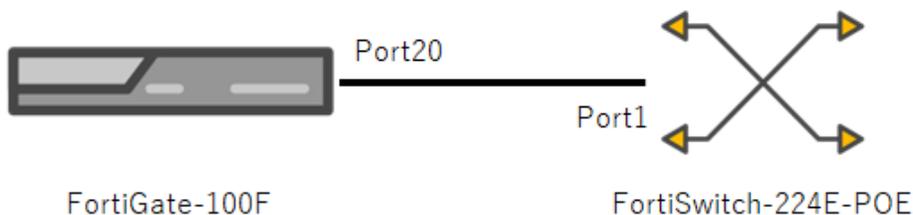


図1 構成概要

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。

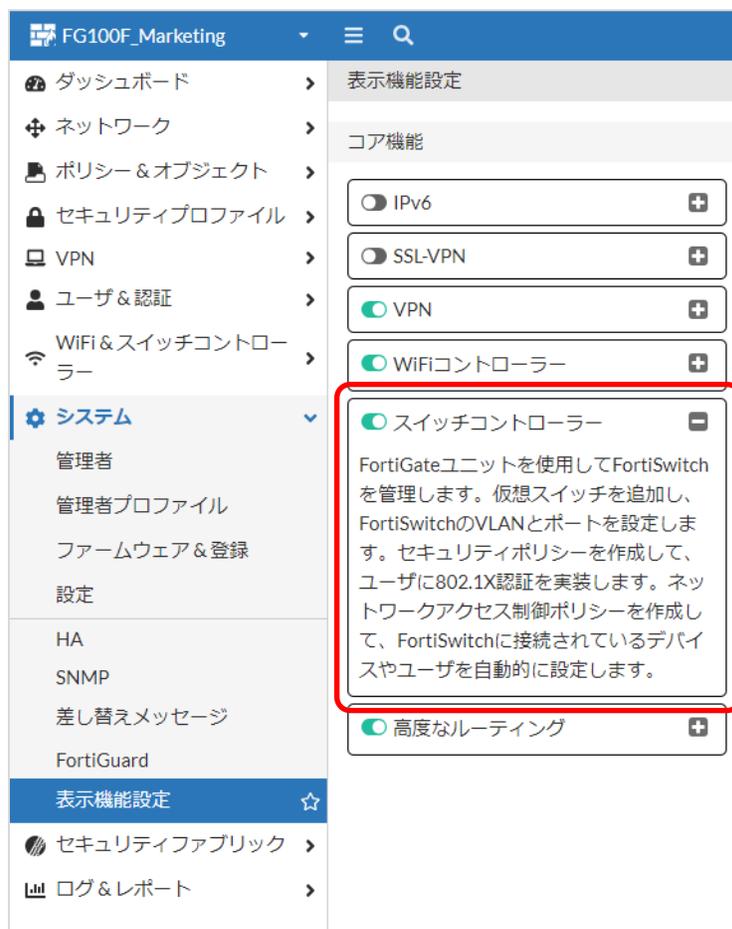


図2-1 スイッチコントローラー有効化

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。

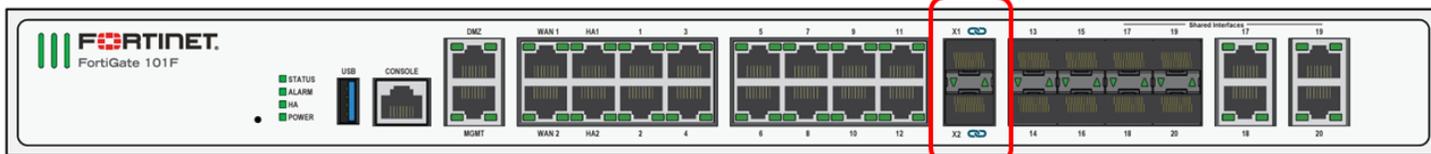


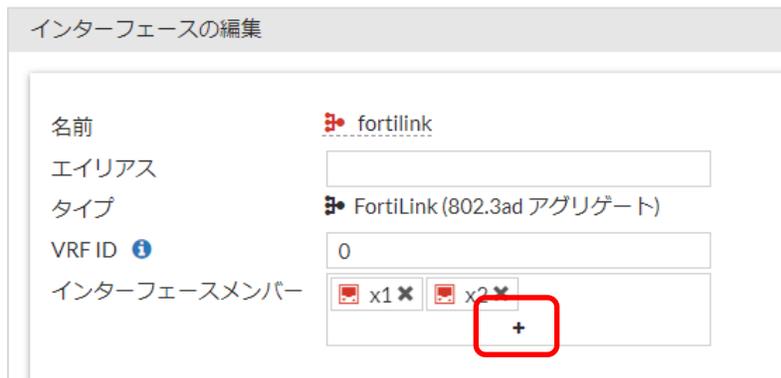
図2-2 デフォルトFortiLinkポート (FortiGate-100F)

「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。



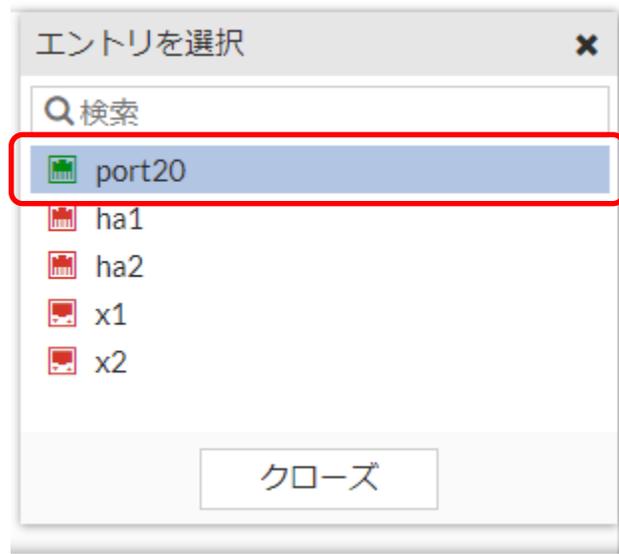
2-3 FortiLinkインターフェース設定

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。

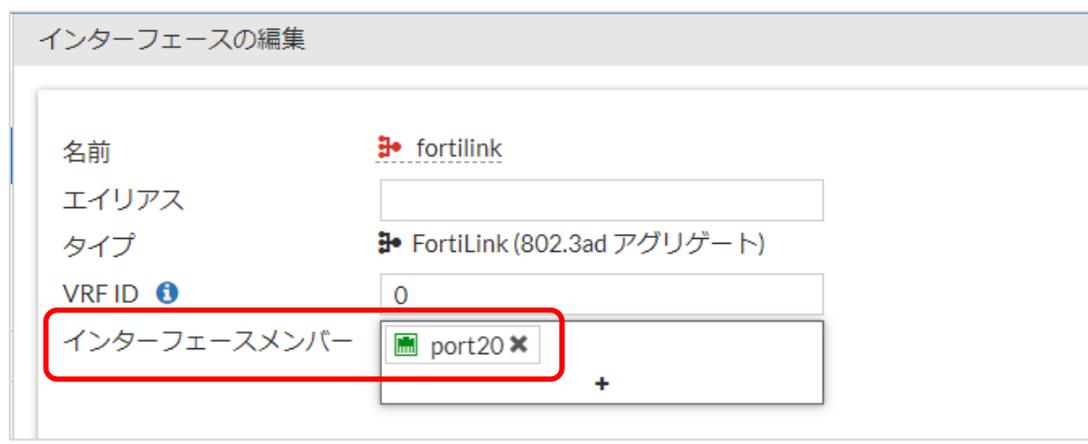


2-4 インターフェースメンバー編集

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。



2-5 エントリ選択画面



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ア FortiSwitch専用

IP/ネットマスク

接続デバイス

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 ⓘ

ロックダウンISL

DHCPサーバ

DHCPステータス 有効化済み 無効化済み

アドレス範囲

ネットマスク

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 ⓘ 秒

FortiClient On-Netステータス

高度な設定

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

その他

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」をクリックしてポロジ画面を開きます。

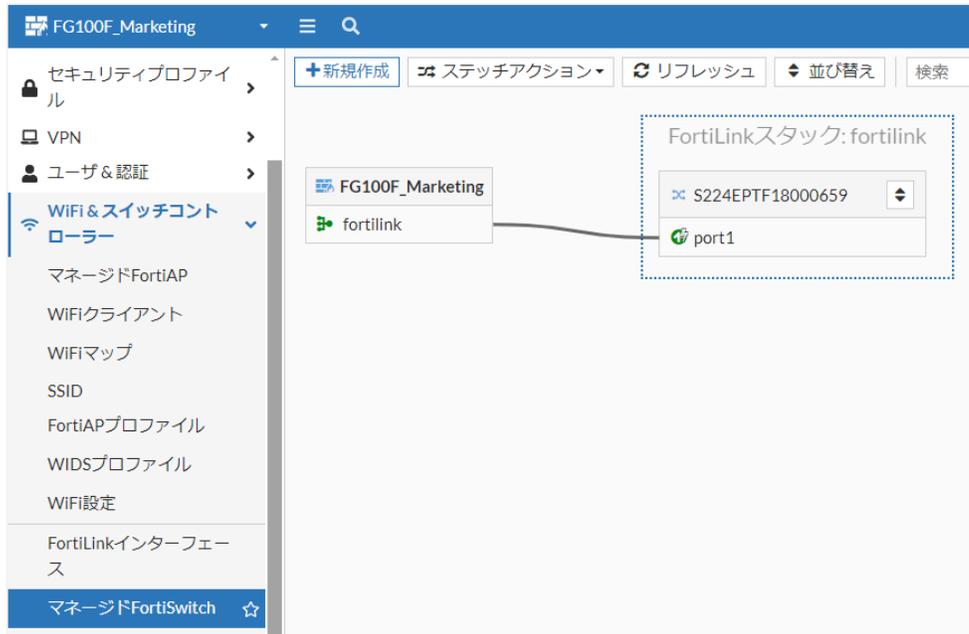


図3-1 FortiSwitch管理画面

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。

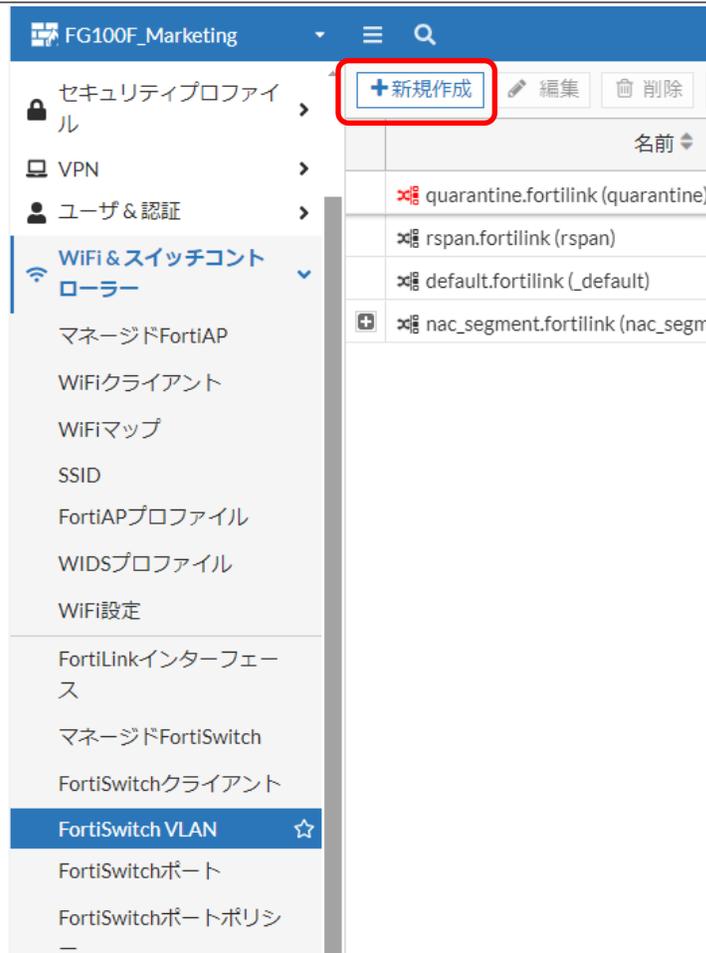


図3-3 FortiSwitch VLAN画面

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

新規インターフェース

名前: vlan 200

エイリアス:

タイプ: VLAN

インターフェース: fortilink

VLAN ID: 200

VRF ID: 0

カラー: 変更

ルール: LAN

アドレス

アドレスリングモード: マニュアル IPAM DHCP PPPoE ワンアームスニフアー

IP/ネットマスク: 172.16.0.1/24

アドレスオ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IPアドレス:

管理者アクセス

IPv4

HTTPS HTTP PING

FMGアクセス SSH SNMP

FTM RADIUSアカウントインテグレーション セキュリティファブリック接続

スピードテスト

DHCPサーバ

ネットワーク

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。

名前	VLAN ID	IP
quarantine.fortilink (quarantine)	4093	169.254.11.1/255.255.255.0
rspan.fortilink (rspan)	4092	169.254.14.1/255.255.255.0
default.fortilink (_default)	1	0.0.0.0/0.0.0.0
nac_segment.fortilink (nac_segment)	4088	10.255.11.1/255.255.255.0
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。

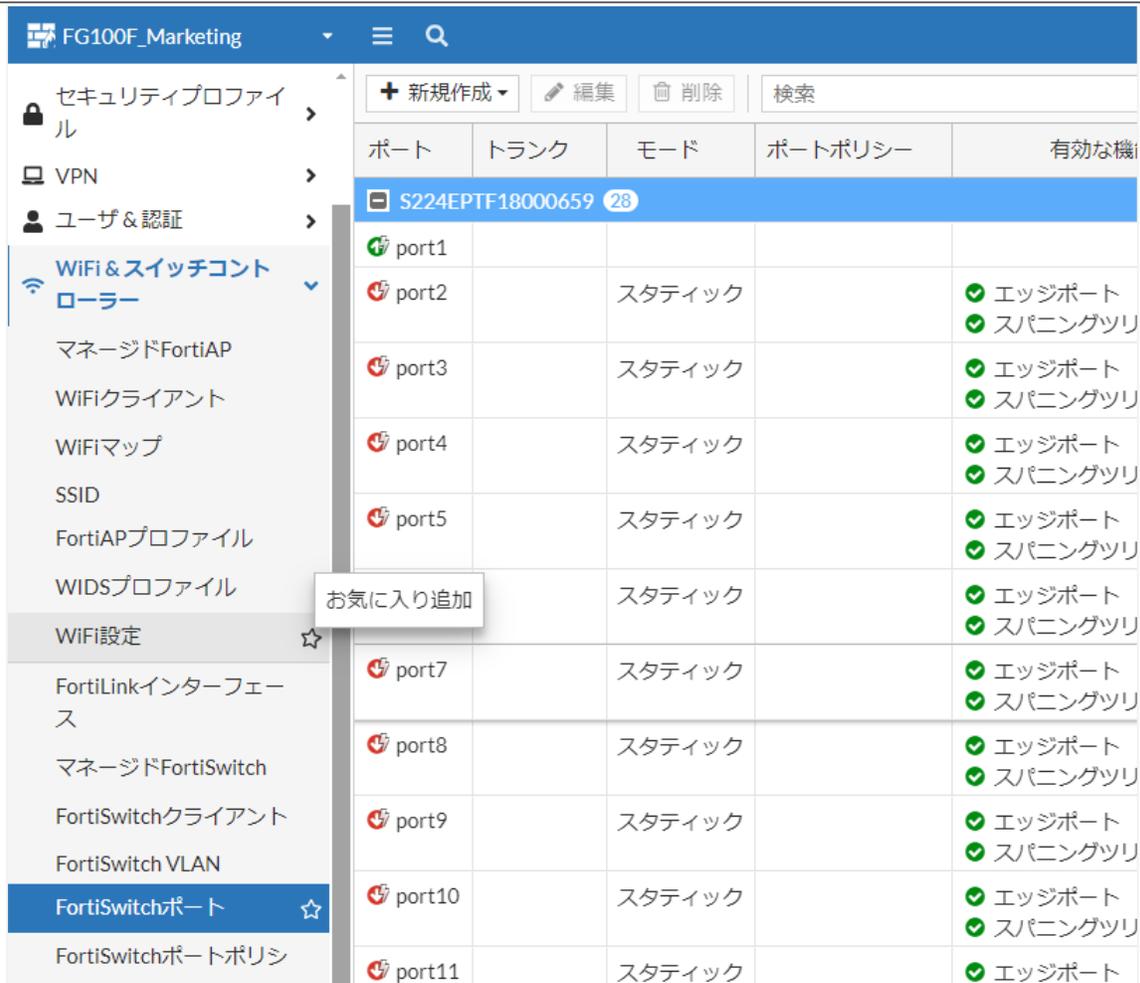


図3-6 FortiSwitch ポート画面

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。

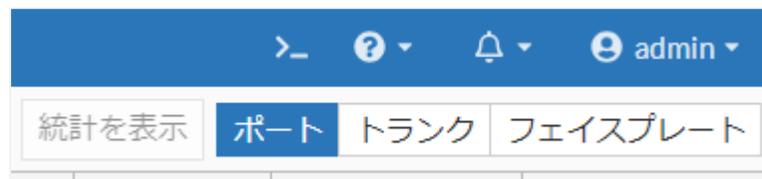


図3-7 FortiSwitch VLAN画面 (右上部)

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	タ
port8		スタティック		<ul style="list-style-type: none"> 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)	
port9		スタティック		<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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)	
port11		スタティック		<ul style="list-style-type: none"> 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)	
port12		スタティック		<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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)	
port14		スタティック		<ul style="list-style-type: none"> 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)	
port15		スタティック		<ul style="list-style-type: none"> 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)	
port16		スタティック		<ul style="list-style-type: none"> 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)	
port17		スタティック		<ul style="list-style-type: none"> 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)	
port18		スタティック		<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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)	
port20		スタティック		<ul style="list-style-type: none"> 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)	
port21		スタティック		<ul style="list-style-type: none"> 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。

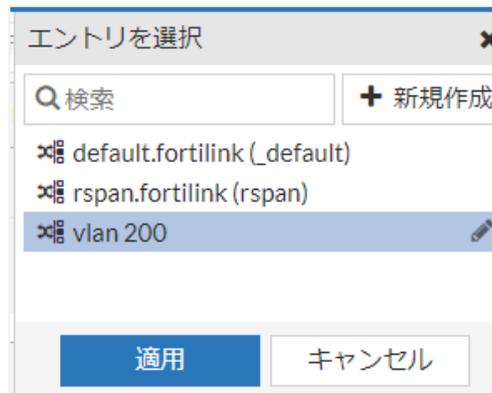


図3-9 VLANエントリー画面

選択したすべてのポートにvlan200 の割当てが完了しました。

port10	スタティック	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ エッジポート ✔ スパニングツリープロトコル 	vlan 200
port20	スタティック	<ul style="list-style-type: none"> ✔ エッジポート ✔ スパニングツリープロトコル 	vlan 200

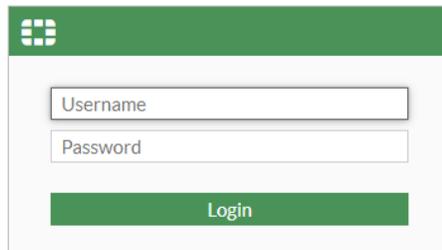
図3-10 適用されたVLAN

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。



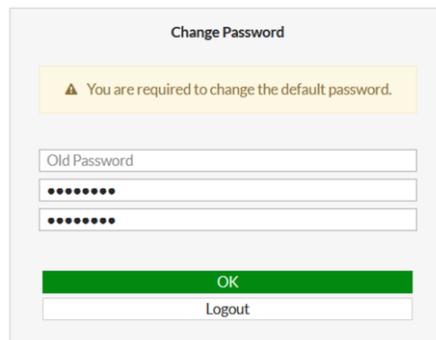
図Ap-1.ログイン画面

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。



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