Managing a FortiSwitch unit with a FortiGate
Administration Guide
Managing a FortiSwitch unit with a FortiGate

April 30, 2014.

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.
# Change Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr. 30, 2014</td>
<td>Added models FS-1024D and FS-1048D.</td>
</tr>
<tr>
<td>Nov. 20, 2013</td>
<td>Initial Release.</td>
</tr>
</tbody>
</table>
Introduction

Welcome and thank you for selecting Fortinet products for your network configuration and protection. This document is intended to provide an understanding of how to manage a FortiSwitch unit with a FortiGate unit, also known using a FortiSwitch unit in Fortilink mode.

Supported Models

FortiSwitch Models

This guide was written for FortiSwitch units running FortiSwitchOS 2.0.3.

The following models are currently supported:

- FortiSwitch-28C
- FortiSwitch-324B-POE
- FortiSwitch-348B
- FortiSwitch-448B

FortiGate Models

This document was written for FortiGate units running FortiOS 5.0.5.

Only FortiGate models that have the Switch Controller feature can be used to manage a FortiSwitch unit. This feature is available on the following FortiGate units:

- FortiGate-100D
- FortiGate-140D
- FortiGate 200D
- FortiGate 240D
- FortiGate-600C
- FortiGate-800C
- FortiGate-1000C

A FortiGate unit that is operating in HA mode cannot manage a FortiSwitch.

Before You Begin

Before you start administrating your FortiSwitch unit, certain assumptions have been made in the writing of this manual:

- You have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch unit’s model and have administrative access to the FortiSwitch web-based manager and CLI.
- You have installed a FortiGate unit on your network and have administrative access to the FortiGate web-based manager and CLI.

How this Guide is Organized

This guide has two sections: Set-up and Scenarios. Set-up describes how to set up the FortiSwitch unit to be managed by a FortiGate unit. Scenarios contains practical examples of how to use the FortiSwitch unit to manage a network.
Set-up

This chapter contains information on some initial information and set-up that is required to manage a FortiSwitch unit with a FortiGate unit.

- Connecting the FortiSwitch and FortiGate units
- Creating Virtual Local Area Networks (VLANs)

**Connecting the FortiSwitch and FortiGate units**

Before the FortiSwitch and FortiGate units can be connected, the FortiSwitch unit’s management mode must be set to allow remote management and the FortiGate unit must have the Switch Controller menu enabled.

**Changing the FortiSwitch unit’s management mode**

The FortiSwitch unit’s management mode can be changed either from the FortiSwitch’s web-based manager or from the CLI.

**Using the web-based manager**

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Beside **Operation Mode**, select **Change**.
3. Change **Management Mode** to **FortiGate Remote Management**.
4. Select **OK**.
5. A warning will appear, asking if you wish to continue. Select **OK**.

The FortiSwitch unit is now ready to be connected to the FortiGate unit.

**Using the CLI**

Using the following command to change the FortiSwitch unit’s management mode:

```
config system global
    set switch-mgmt-mode fortilink
end
```

**Enabling the FortiGate’s Switch Controller**

The FortiGate unit’s Switch Controller may need to be enabled before the FortiSwitch unit can be connected and managed. This can be done using either the web-based manager or the CLI.

**Using the web-based manager**

1. Go to **System > Config > Features**.
2. Turn on the **WiFi & Switch Controller** feature.
3. Select **Apply**.

The menu option **WiFi & Switch Controller** now appears in the web-based manager.
Using the CLI

Using the following command to enable the Switch Controller:

```
cfg system global
  set switch-controller enable
end
```

Authorizing the FortiSwitch unit as a managed switch

Use an Ethernet cable to connect the MGMT port of the FortiSwitch unit to an internal port on the FortiGate unit. Next, the FortiSwitch addressing must be set so that the FortiGate unit will recognize the FortiSwitch unit, after which point the FortiSwitch unit can be authorized as a managed switch.

Using the web-based manager

1. Go to System > Network > Interfaces and edit the internal port.
2. Set Addressing mode to Dedicate to FortiAP/FortiSwitch.
3. Set the IP address and netmask to use.
4. Select OK.
5. Go to WiFi & Switch Controller > Managed Devices > Managed FortiSwitch. Right click on the switch and select Authorize.

A icon with a checkmark now appears in the Status column.

Using the CLI

1. Configure the interface for port 1.
   ```
   cfg system interface
     edit port1
       set ip 172.20.120.10 255.255.255.0
       set allowaccess capwap
     end
   end
   ```
2. Authorize the FortiSwitch unit as a managed switch.
   ```
   cfg switch-controller managed-switch
     edit FS324P3W11000127
       set fsw-wan1-admin enable
     end
   ```

Creating Virtual Local Area Networks (VLANs)

Using Virtual Local Area Networks (VLANs) allows you to get the most out of using your FortiSwitch unit by using ID tags to logically separate a LAN into smaller broadcast domains. A single LAN can contain many unique VLANs, which allows different policies to be created for different types of users and segments traffic so that it is only sent to and from the intended VLAN.

For example, if a company has one LAN which is to be used for both the marketing and the accounting department, this LAN can be segmented into two VLANs. This allows the traffic from each department to be isolated, so information packets sent to the marketing department are only sent on the marketing VLAN. It also allowed different policies to be created, so that security
can be increased for the accounting department without also increasing it for the marketing department.

Now that your FortiSwitch unit is managed by your FortiGate unit, a VLAN can be configured on the FortiSwitch, using the FortiGate.

The following instructions will create a VLAN to be used by the marketing team for network and Internet access. The PCs used by the marketing team will connect to ports 3-6 on the FortiSwitch unit.

Setting up a VLAN requires:

- Creating the VLAN.
- Assigning ports on the FortiSwitch unit to the VLAN.

**Using the web-based manager**

**Creating the VLAN**

1. Go to WiFi & Switch Controller > Switch Network > Virtual Switch and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td></td>
</tr>
<tr>
<td>IP/Network Mask</td>
<td>172.20.120.10/255.255.255.0</td>
</tr>
</tbody>
</table>

2. Enable DHCP Server. Set the IP range to 172.20.120.11-172.20.120.254.

3. Select OK.

The entry marketing is now shown on the list of Virtual Switches. A marketing interface has also been added, which can be seen by going to System > Network > Interfaces.
Assigning FortiSwitch Ports to the VLAN

1. Go to WiFi & Switch Controller > Managed Devices > Managed FortiSwitch
2. Highlight the FortiSwitch unit and select Edit Managed FortiSwitch.
3. Click and drag a box around ports 3-6 to select them.
4. Select marketing from the Assign to list.

Ports 3-6 on the FortiSwitch have now been assigned to the marketing VLAN and will appear in red.

Using the CLI

1. Create the marketing VLAN.
   ```
   config switch-controller vlan
   edit marketing
     set color 32
   end
   ```

2. Set the VLAN’s IP address.
   ```
   config system interface
   edit marketing
     set ip 172.20.120.14 255.255.255.0
   end
   ```

3. Enable a DHCP Server.
   ```
   config system dhcp server
   edit 1
     set default-gateway 172.20.120.10
     set dns-service default
     set interface marketing
       config ip-range
         set start-ip 172.20.120.11
         set end-ip 172.20.120.254
       end
       set netmask 255.255.255.0
   end
   ```
4. Assign ports 3-6 to the VLAN.

```plaintext
config switch-controller managed-switch
edit FS324P3W11000127
config ports
edit port3
   set vlan marketing
next
edit port4
   set vlan marketing
next
edit port5
   set vlan marketing
next
edit port6
   set vlan marketing
end
end
```

Setting up a security policy for the VLAN

The following instructions configure a basic security policy for the marketing VLAN that will allow all traffic from the marketing VLAN to have access to the Internet.

**Using the web-based manager**

1. Go to **Policy > Policy > Policy** and select **Create New**. Change the following settings:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Subtype</td>
<td>Address</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>marketing</td>
</tr>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ALL</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Enable</td>
</tr>
<tr>
<td>Logging Options</td>
<td>Log all Sessions</td>
</tr>
</tbody>
</table>

2. Select **OK**.

With this security policy in place, all computers connected to the marketing VLAN can now access the Internet.
Using the CLI

Create a security policy for the marketing VLAN.

```
config security policy
  edit 2
    set srcintf marketing
    set dstintf wan1
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
    set logtraffic all
    set nat enable
end
```
Scenarios

This chapter contains practical examples of how to use the FortiSwitch unit to manage a network. The scenarios are as follows:

- Scenario 1: Allowing access to specific users on the marketing VLAN
- Scenario 2: Adding a specific device to the marketing VLAN
- Scenario 3: Accessing the marketing VLAN remotely using an SSL VPN
- Scenario 4: Configuring the accounting VLAN using an SFP port
- Scenario 5: Connecting a VoIP phone to the FortiSwitch
- Scenario 6: Connecting a FortiAP unit to the FortiSwitch

The Example Network

All the scenarios are interrelated and are used to manage an example network with the following attributes:

- The FortiSwitch unit used is a FortiSwitch-324B, serial number FS324P3W11000127.
- The FortiSwitch unit’s MGMT port connects to port1 on the FortiGate unit.
- The LAN is divided into two distinct VLANs, configured as follows:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP</th>
<th>Device(s)</th>
<th>Port(s)</th>
<th>Policy ID(s)</th>
<th>GUI Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>marketing</td>
<td>172.20.120.10/255.255.255.0</td>
<td>marketing PCs, marketing laptop</td>
<td>3-6</td>
<td>2, 3</td>
<td></td>
</tr>
<tr>
<td>accounting</td>
<td>172.20.130.10/255.255.255.0</td>
<td>accounting PCs</td>
<td>21</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>voip</td>
<td>172.20.140.10/255.255.255.0</td>
<td>VoIP phone</td>
<td>10</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>access_point</td>
<td>172.20.150.10/255.255.255.0</td>
<td>FortiAP</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

- There are six devices that connect directly to the FortiSwitch unit’s ports using Ethernet cables: the 3 marketing PCs, the marketing laptop, the VoIP phone, and the FortiAP unit.
- The accounting VLAN connects to the FortiSwitch using an SFP port.
- There are three marketing employees (Jane Smith, Tom Brown, Bob Lee) who will use the marketing VLAN using the marketing PCs.
- The MAC address of the marketing laptop is 01:23:45:67:89:ab.
- The IP range for the VoIP phone is 10.10.10.10-10.10.10.50.
- The FortiAP unit is a FortiAP-11C, serial number FAP11C3X12000412.
Scenario 1: Allowing access to specific users on the marketing VLAN

In Scenario 1, the policy for the marketing VLAN will be altered so that different users have different access. The firewall policy will be created so that all three marketing employees (Jane Smith, Tom Brown, Bob Lee) have user accounts. These accounts will be put into one of two groups: full-time and part-time. Full-time employees will always have network access, while part-time employees will only have access on Mondays, Wednesdays and Fridays. This policy will apply to each user when they use any of the PCs that connect to the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch.

Creating a policy to match scenario 1 requires:
- Creating users.
- Creating groups.
- Creating a schedule.
- Configuring the firewall policy.
Using the web-based manager

Creating a User Group
2. Name the user group part-time.
3. Set Type as Firewall.
4. Select OK.

The entry part-time will now appear on the user group list. Repeat these steps to create another user group, named full-time.

Creating a User
2. Use the User Creation Wizard to create a user. In part 1, select Local User.
3. In part 2, change the following settings:

<table>
<thead>
<tr>
<th>User Name</th>
<th>blee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>password</td>
</tr>
</tbody>
</table>

4. In part 3, enter the email address blee@example.com
5. In part 4, select Enable and User Group. Set part-time as the group.
6. Select Done.

The entry blee will now appear in the user list. Repeat these steps to create user accounts tbrown and jsmith and add both of these accounts to the full-time group.

Creating a Schedule
1. Go to Firewall Objects > Schedule > Schedules. Select Create New and then select Recurring.
2. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>part-time_schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day of the Week</td>
<td>Monday, Wednesday, Friday</td>
</tr>
</tbody>
</table>

3. Select OK.

The entry part-time schedule will now appear on the schedules list.

Configuring the Firewall Policy
1. Go to Policy > Policy > Policy and select the policy for the marketing VLAN. Select Edit.
2. Set Policy Subtype as User Identity.
4. Change the following settings to set access for part-time employees:

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group(s)</td>
<td>part-time</td>
</tr>
<tr>
<td>Schedule</td>
<td>part-time_schedule</td>
</tr>
<tr>
<td>Service</td>
<td>ALL</td>
</tr>
</tbody>
</table>
5. Select OK.
7. Change the following settings to set access for full-time employees:

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group(s)</td>
<td>full-time</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ALL</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

| Logging Options | Log all Sessions |

8. Select OK.
9. Select OK.

You have now finished creating a policy that matches scenario 1. This policy will apply to all three users when they use any of the PCs that connect to the marketing VLAN.

**Using the CLI**

1. Create the 3 users.

   ```
   config user local
   edit blee
   set type password
   set passwd password
   next
   edit tbrown
   set type password
   set passwd password
   next
   edit jsmith
   set type password
   set passwd password
   end
   ```
2. Create the 2 user groups and add the users to them.

```plaintext
config user group
edit part-time
  set group-type firewall
  set member blee
next
edit full-time
  set group-type firewall
  set member tbrown jsmith
end
```

3. Create the schedule for part-time employees.

```plaintext
config firewall schedule recurring
edit part-time_schedule
  set day monday wednesday friday
end
```

4. Add user authentication to the firewall policy for the marketing VLAN.

```plaintext
config firewall policy
edit 2
  set identity-based enable
  config identity-based-policy
    edit 1
      set schedule part-time_schedule
      set logtraffic all
      set groups part-time
      set dstaddr all
      set service ALL
    next
    edit 2
      set schedule always
      set logtraffic all
      set groups full-time
      set dstaddr all
      set service ALL
end
```

**Scenario 2: Adding a specific device to the marketing VLAN**

In Scenario 2, a new policy will be created for the marketing VLAN that will be used by the marketing laptop. This policy will affect the marketing laptop that is used periodically for tasks such as boardroom presentations or for guests, tasks for which the laptop requires Internet access. The laptop will access the Internet by connecting to the marketing VLAN through ports
3, 4, 5 or 6 on the FortiSwitch. Adding a new policy for the laptop will allow it to connect without requiring user authentication and will also limit the scope of the device’s access.

Creating a policy to match scenario 2 requires:
- Assigning a reserve IP to the laptop.
- Creating a firewall address for the reserve IP.
- Creating a firewall policy that uses the reserve IP.

**Using the web-based manager**

**Assigning a Reserve IP to the Laptop**
1. Go to **System > Network > Interfaces** and select **marketing**.
2. Under **DHCP Server**, expand the **Advanced** options.
3. In the **MAC Address Access Control List** and select **Create New**.
4. Change the following settings:

<table>
<thead>
<tr>
<th>MAC</th>
<th>01:23:45:67:89:ab</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>172.20.120.254</td>
</tr>
<tr>
<td>Action</td>
<td>Reserve IP</td>
</tr>
</tbody>
</table>

**Creating a Firewall Address for the Reserve IP**
1. Go to **Firewall Objects > Address > Addresses** and select **Create New**.
2. Change the following settings:

<table>
<thead>
<tr>
<th>Category</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>marketing_laptop</td>
</tr>
<tr>
<td>Type</td>
<td>Subnet</td>
</tr>
<tr>
<td>Subnet/IP Range</td>
<td>172.20.120.254</td>
</tr>
<tr>
<td>Interface</td>
<td>marketing</td>
</tr>
</tbody>
</table>

**Configuring a Firewall Policy**
1. Go to **Policy > Policy > Policy** and select **Create New**.
2. Change the following settings:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Subtype</td>
<td>Address</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>marketing</td>
</tr>
<tr>
<td>Source Address</td>
<td>marketing_laptop</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>HTTP HTTPS DNS</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Enabled</td>
</tr>
<tr>
<td>Logging Options</td>
<td>Log all Sessions</td>
</tr>
</tbody>
</table>

3. Select OK.
4. In the policy list, select the Seq. # column of the new policy and drag the policy above the previous policy for the marketing VLAN. This will ensure that the laptop will be identified through this policy.

You have now finished creating a policy that matches scenario 2. This policy will apply to anyone who uses the laptop to connect to the marketing VLAN using an Ethernet cable.

**Using the CLI**

1. Assign a reserve IP to the laptop.
   ```
   config system dhcp server
   edit 2
   config reserved-address
   edit 1
   set action reserved
   set ip 172.20.120.254
   set mac 01:23:45:67:89:ab
   end
   end
   ```

2. Create a firewall address for the reserve IP.
   ```
   config firewall address
   edit marketing_laptop
   set subnet 172.20.120.254
   end
   ```
3. Create a firewall policy for the marketing VLAN that uses the reserve IP.

```fortigate
config firewall policy
edit 3
  set srcintf marketing
  set dstintf wan1
  set srcaddr marketing_laptop
  set dstaddr all
  set action accept
  set schedule always
  set service HTTP HTTPS DNS
  set logtraffic all
  set nat enable
end
```

4. Place the new firewall policy at the top of the policy list.

```fortigate
config firewall policy
move 2 after 3
end
```

**Scenario 3: Accessing the marketing VLAN remotely using an SSL VPN**

In Scenario 4, a policy is created to allow remote access to the marketing VLAN, using a virtual private network (VPN) tunnel. This policy will allow marketing employee Tom Brown to connect to the marketing VLAN remotely from his home. The default IP Pool, `SSLVPN_TUNNEL_ADDR1`, will be used to configure the SSL VPN web portal. The computer Tom Brown is using to access the network remotely has a dynamic IP address and will be using the FortiClient application to auto connect to the VPN tunnel. To maintain security, split tunneling will be disabled. This policy will be used whenever Tom Brown accesses the marketing VLAN remotely.

Creating a policy to match scenario 2 requires:

- Creating a user group.
- Creating a firewall address for the marketing VLAN.
- Creating an SSL VPN web portal.
- Creating a SSL VPN firewall policy for the marketing VLAN.

**Using the web-based manager**

**Creating a User Group**

2. Name the Group `remote access`.
3. Set Type as Firewall.
4. Highlight `tbrown` on the Available Users list.
5. Select the right-pointing arrow to move `tbrown` to the Members list.
6. Select OK.

The entry `remote access` will now appear on the Group list, with `tbrown` listed under Members.
Creating a Firewall Address for the marketing VLAN

1. Go to Firewall Objects > Address > Addresses and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>marketing VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet</td>
</tr>
<tr>
<td>Subnet/IP Range</td>
<td>172.20.120.14/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>marketing</td>
</tr>
</tbody>
</table>

2. Select OK.

Creating an SSL VPN Web Portal

1. Go to VPN > SSL > Portals and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>marketing-remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Tunnel Mode</td>
<td>Enable</td>
</tr>
<tr>
<td>Enable Split Tunneling</td>
<td>Disable</td>
</tr>
<tr>
<td>IP Pools</td>
<td>SSLVPN_TUNNEL_ADDR1</td>
</tr>
<tr>
<td>Client Options</td>
<td>Auto Connect</td>
</tr>
<tr>
<td>Enable Web Mode</td>
<td>Enable</td>
</tr>
<tr>
<td>Applications</td>
<td>HTTP/HTTPS, FTP, SSH</td>
</tr>
</tbody>
</table>

2. Select Apply.

Creating a Firewall Policy

1. Go to Policy > Policy > Policy and select Create New.
2. Change the following settings:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Remote Address</td>
<td>all</td>
</tr>
<tr>
<td>Local Interface</td>
<td>marketing</td>
</tr>
<tr>
<td>Local Protected Subnet</td>
<td>marketing VLAN</td>
</tr>
</tbody>
</table>

4. Change the following settings:

<table>
<thead>
<tr>
<th>Group(s)</th>
<th>remote access</th>
</tr>
</thead>
<tbody>
<tr>
<td>User(s)</td>
<td>tbrown</td>
</tr>
</tbody>
</table>
5. Select OK.
6. Select OK.

You have now finished creating a policy that matches scenario 4. This policy will be used whenever Tom Brown accesses the marketing VLAN remotely.

**Using the CLI**

1. Create the user group for remote users.
   ```
   config user group
   edit remote-access
   set group-type firewall
   set member tbrown
   end
   ```

2. Create a firewall address for the marketing VLAN.
   ```
   config firewall address
   edit marketing_VLAN
   set associated-interface marketing
   set subnet 172.20.120.14 255.255.255.0
   end
   ```

3. Create the SSL VPN web portal.
   ```
   config vpn ssl web portal
   edit marketing-remote
   set allow-access web ftp ssh
   config widget
   edit 1
   set type tunnel
   set split-tunneling disable
   set ip-pools SSLVPN_TUNNEL_ADDR1
   set auto-connect enable
   end
   ```
4. Create a firewall policy to allow remote access to the marketing VLAN.

```fortigate
config firewall policy
edit 3
set srcintf wan1
set dstintf marketing
set dstaddr marketing_VLAN
set action ssl-vpn
set identity-based-policy
config identity-based-policy
set schedule always
set groups remote_access
set users tbrown
set sslvpn-portal marketing-remote
end
end
```

**Scenario 4: Configuring the accounting VLAN using an SFP port**

The SFP ports should only be used to connect UL-listed optical transceiver products, rated Laser Class 1.33V DC.

In Scenario 4, a second VLAN will be created on the FortiSwitch, to be used for the accounting department. This VLAN will connect to the FortiSwitch unit using a copper SFP receiver that has been installed in the FortiSwitch. Due to the sensitive nature of information within the accounting network, the firewall policy that controls traffic to this network uses the default profile for all security features.
Creating an interface to match scenario 4 requires:
- Creating and assigning a VLAN.
- Configuring a firewall policy.

SFP ports are only available on certain FortiSwitch models. SFP ports are also shared with Ethernet ports and so when an SFP port is used, the Ethernet port with the same number cannot be.

Using the web-based manager

Creating and Assigning the VLAN
1. Go to WiFi & Switch Controller > Switch Network > Virtual Switch and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td></td>
</tr>
<tr>
<td>IP/Network Mask</td>
<td>172.20.120.15/255.255.255.0</td>
</tr>
</tbody>
</table>

2. Select OK.
3. Go to WiFi & Switch Controller > Managed Devices > Managed FortiSwitch and assign FortiSwitch port 21 to accounting.

Configuring the Firewall Policy
1. Go to Policy > Policy > Policy and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Subtype</td>
<td>Address</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>accounting</td>
</tr>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ALL</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>
2. Enable the following Security Profiles and set them to use the default profile: AntiVirus, Web Filter, Application Control, IPS, Email Filter, DLP Sensor, and SSL/SSH Inspection.

3. Select OK.

You have now finished creating a policy that matches scenario 5. This policy will be used for all traffic on the accounting VLAN.

**Using the CLI**

1. Create the accounting VLAN.
   ```
   config switch-controller vlan
   edit accounting
   set color 32
   end
   ```

2. Set the VLAN’s IP address.
   ```
   config system interface
   edit marketing
   set ip 172.20.120.15 255.255.255.0
   end
   ```

3. Assign the accounting VLAN to port 21.
   ```
   config switch-controller managed-switch
   edit FS324P3W11000127
   config ports
   edit port21
   set vlan accounting
   end
   end
   ```
4. Create a firewall policy for the accounting VLAN that uses the default security profiles.

```plaintext
config firewall policy
edit 4
    set srcintf accounting
    set dstintf wan1
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
    set logtraffic all
    set nat enable
    set av-profile default
    set webfilter-profile default
    set spamfilter-profile default
    set dlp-sensor default
    set ips-sensor default
    set application-list default
    set profile-protocol-options default
    set deep-inspection-options default
end
```

**Scenario 5: Connecting a VoIP phone to the FortiSwitch**

In Scenario 5, an interface will be configured to use a Voice over IP (VoIP) phone. This VoIP phone will be assigned the IP range 10.10.10.10-10.10.10.50 and connect to the FortiSwitch unit through port 10 using an Ethernet cable. The FortiGate unit’s default VoIP profile will be used.
Creating an interface to match scenario 5 requires:
- Creating and assigning a VLAN.
- Creating a firewall address for the VoIP phone.
- Configuring a firewall policy.

Using the web-based manager

Creating and Assigning the VLAN
1. Go to WiFi & Switch Controller > Switch Network > Virtual Switch and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>voip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td></td>
</tr>
<tr>
<td>IP/Network Mask</td>
<td>172.20.120.16/255.255.255.0</td>
</tr>
</tbody>
</table>

2. Select OK.
3. Go to WiFi & Switch Controller > Managed Devices > Managed FortiSwitch and assign FortiSwitch port 10 to voip.

Creating a Firewall Address
1. Go to Firewall Objects > Address > Addresses and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Category</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>voip</td>
</tr>
<tr>
<td>Color</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>IP Range</td>
</tr>
<tr>
<td>Subnet/IP Range</td>
<td>10.10.10.10-10.10.10.50</td>
</tr>
<tr>
<td>Interface</td>
<td>voip</td>
</tr>
</tbody>
</table>

2. Select OK.

Create a Firewall Policy
1. Go to Policy > Policy > Policy and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Subtype</td>
<td>Address</td>
</tr>
</tbody>
</table>
2. Enable the **VoIP** Security Profile and set it to *default*.
You have now finished creating a policy that matches scenario 6.

## Using the CLI

1. Create the voip VLAN.
   ```
   config switch-controller vlan
   edit voip
   set color 25
   end
   ```
2. Set the VLAN's IP address.
   ```
   config system interface
   edit marketing
   set ip 172.20.120.16 255.255.255.0
   end
   ```
3. Assign the voip VLAN to port 10.
   ```
   config switch-controller managed-switch
   edit FS324P3W11000127
   config ports
   edit port10
   set vlan voip
   end
   ```
   ```
   end
   ```
4. Configure the firewall policy.
   
   ```
   config firewall policy
   edit 5
   set srcintf voip
   set dstintf wan1
   set srcaddr voip_phone
   set dstaddr all
   set action accept
   set schedule always
   set service SIP
   set logtraffic all
   set nat enable
   set voip-profile default
   end
   ```

**Scenario 6: Connecting a FortiAP unit to the FortiSwitch**

In Scenario 6, an interface will be configured to use a FortiAP unit that will provide wireless Internet access.

Creating an interface to match scenario 6 requires:

- Creating and assigning a VLAN.
- Authorizing the FortiAP unit.
- Creating an SSID.
- Creating a firewall address.
- Configuring a firewall policy.

The WiFi network provided by the access point will use the marketing schedule and allow HTTP and HTTPS traffic.
Using the web-based manager

Creating and Assigning the VLAN
1. Go to WiFi & Switch Controller > Switch Network > Virtual Switch and select Create New. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>access_point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td></td>
</tr>
<tr>
<td>IP/Network Mask</td>
<td>172.20.120.17/255.255.255.0</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enable</td>
</tr>
</tbody>
</table>

2. Select OK.
3. Go to WiFi & Switch Controller > Managed Devices > Managed FortiSwitch and assign FortiSwitch port1 to access_point.

Authorizing the FortiAP unit
1. Go to WiFi & Switch Controller > Managed Devices > Managed FortiAPs.
2. Right-click on the FortiAP unit and select Authorize.

A icon with a checkmark now appears in the Status column.

Creating an SSID
1. Go to WiFi & Switch Controller > WiFi Network > SSIDs and select Create New.
2. Change the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>WiFi SSID</td>
</tr>
<tr>
<td>Traffic Mode</td>
<td>Tunnel to Wireless Controller</td>
</tr>
<tr>
<td>IP/Network Mask</td>
<td>172.20.120.17/255.255.255.0</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>SSID</td>
<td>wireless</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>password</td>
</tr>
</tbody>
</table>

3. Select OK.

Create a Firewall Policy
1. Go to Policy > Policy > Policy and select Create New.
2. Change the following settings:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Subtype</td>
<td>Address</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>access_point</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>HTTP HTTPS DNS</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Enabled</td>
</tr>
<tr>
<td>Logging Options</td>
<td>Log all Sessions</td>
</tr>
</tbody>
</table>

3. Select OK.

4. Go to WiFi & Switch Controller > Managed Devices > Managed FortiAPs. The Status icon now appears in green, showing that the FortiSwitch unit is online.

You have now finished creating a policy that matches scenario 7.

**Using the CLI**

1. Create the access_point VLAN.
   ```
   config switch-controller vlan
   edit access_point
   set color 7
   end
   ```

2. Assign the access_point VLAN to port 1.
   ```
   config switch-controller managed-switch
   edit FS324P3W11000127
   config ports
   edit port1
   set vlan access_point
   end
   ```

3. Set the interface IP and enable CAPWAP.
   ```
   config system interface
   edit access_point
   set ip 172.20.120.17
   set allowaccess capwap
   end
   ```
4. Enable the FortiAP unit.
   ```
   config wireless-controller wtp
   edit FAP11C3X13000412
   set admin enable
   end
   ```

5. Create an SSID for the FortiAP unit.
   ```
   config wireless-controller vap
   edit WLAN
   set ssid wireless
   set passphrase password
   end
   ```

6. Configure the firewall policy.
   ```
   config firewall policy
   edit 6
   set srcintf access_point
   set dstintf wan1
   set srcaddr all
   set dstaddr all
   set action accept
   set schedule always
   set service HTTP HTTPS DNS
   set logtraffic all
   set nat enable
   end
   ```