FortiVoice - LLDP and Manual VLAN Technical Note

Version 6.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 4, 2020
FortiVoice 6.4.0 LLDP and Manual VLAN Technical Note
26-640-584067-20200904

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-09-04	Initial release of the LLDP and Manual VLAN Technical Note.

Introduction

Virtual local area networks (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. Smaller broadcast domains reduce traffic and increase network security.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

Another key use of VLANs is its ability to prioritize FortiFone voice traffic over PC data traffic. Prioritizing voice traffic is achieved by segregating connections through the use of VLAN IDs, and then assigning a higher priority for the voice VLAN over the data VLAN. Prioritizing the voice VLAN is critical for businesses that rely on phone calls not dropping due to other network traffic.

VLAN IDs can also be utilized over the Link Layer Discovery Protocol (LLDP), which is used by network devices for advertising their identity and capabilities over a local area network. LLDP data units are exchanged in the format of Type, Length, Value (TLV). This data contains information such as the system name and description, port number, VLAN name and ID, IP management address, and other system capabilities including router, bridge, telephone, and access point information.

Unlike the Cisco Discovery Protocol (CDP), LLDP is vendor-neutral, and can carry out its functions in a more standardized way.

The Media Endpoint Discovery (MED) is an enhancement of LLDP, known as LLDP-MED, that provides the following facilities:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and Differentiated services (DiffServ) settings), enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), enhanced emergency services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (such as manufacturer, software and hardware versions, and serial or asset number).

This document includes the following topics:

Configuring FortiFone VLAN using LLDP and FortiGate

In the following FortiFone VLAN configuration example, the network switch must support LLDP-MED. FortiSwitch 108D POE and Cisco Catalyst 2960X LAN base switches have been tested. This configuration covers the configuration of both switches to achieve the goal outlined in the scenario.

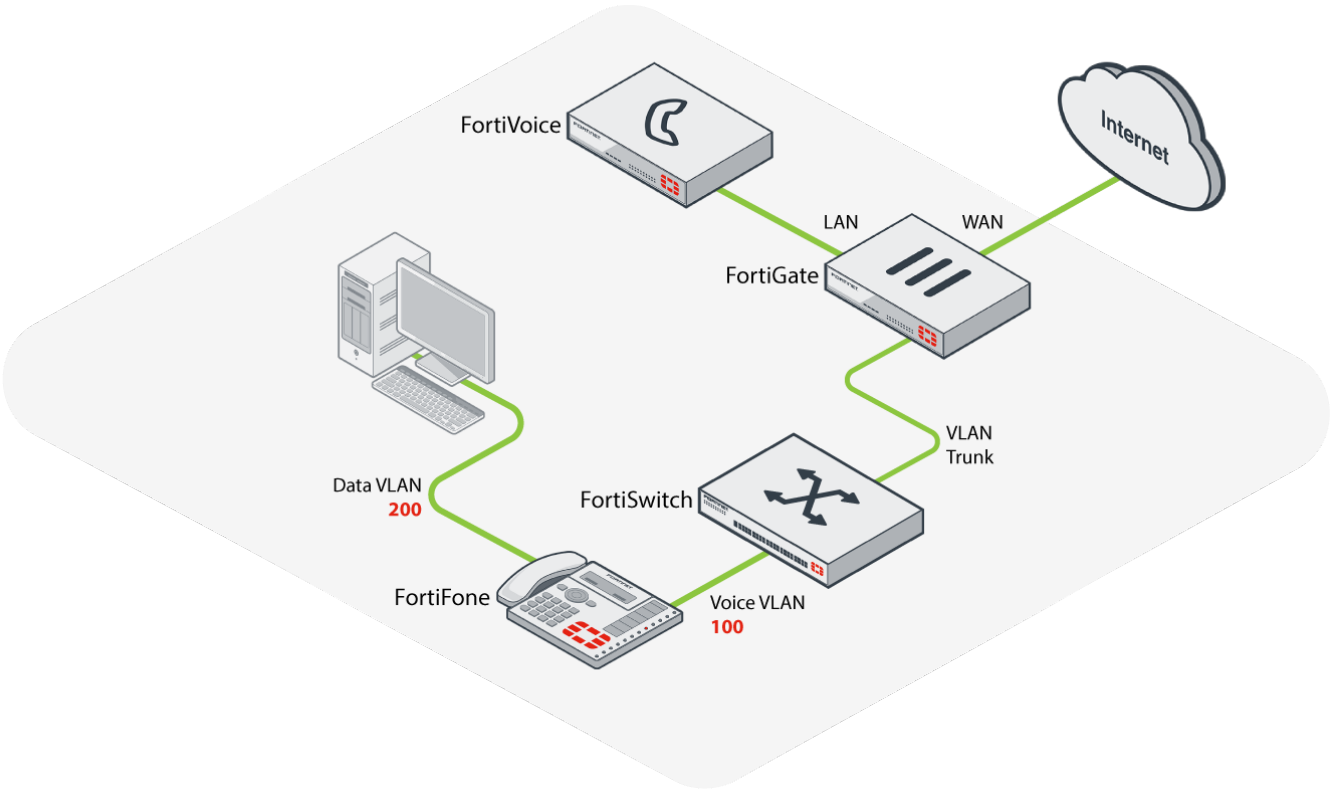
You may need to deploy phones using the existing IT infrastructure which only has one network drop for each employee. In addition, you may need to implement this solution using either FortiSwitch or a Cisco LAN base switch, both of which support 802.1Q VLAN tagging and LLDP-MED. Some phones such as FortiFone have two network ports: LAN and PC.

The recommended solution is to connect FortiFone to the switch using the LAN port and connect the computer to the PC port of FortiFone.

FortiVoice, FortiGate, and FortiSwitch devices depicted in this guide are all running firmware version 6.4.

Address topology

Procedures in this document use the following address topology. Larger deployments (that may require the deployment of thousands of extensions) require FortiVoice to have its own dedicated subnet and VLAN.



Before LLDP-MED is enabled on FortiFone, the phone is placed in VLAN 200, along with the PC. Some newer FortiFone models have LLDP enabled by default. As a result, these phones lease an IP address from the voice VLAN and are automatically placed in VLAN100 instead.

The FortiFone VLAN configuration example uses the following settings:

- **VLAN 100**: The voice network (FortiFone) is on 192.168.100.0/24 subnet, with the FortiVoice 200D IP VLAN interface on 192.168.100.99.
- **VLAN 200**: The data network (PC) is on 192.168.200.0/24 subnet, with the FortiVoice 200D IP VLAN interface on 192.168.200.99.
- **Native VLAN**: Untagged traffic is on the 192.168.1.0/24 subnet, with the FortiVoice 200D physical port IP on 192.168.1.199.
- FortiGate is used as the DHCP server.

Configure FortiSwitch

Steps to configure FortiSwitch are shown using the CLI only because you cannot complete all the steps using the GUI.

1. On FortiSwitch, open the *CLI Console* and enter the following commands to create the LLDP profile:

```
config switch lldp profile
   edit fortifone
      config med-network-policy
         edit "voice"
            set status enable
            set vlan 100
         next
         edit "voice-signaling"
            set status enable
            set vlan 100
      end
end
```

2. Configure the allowed and native VLANs to allow voice VLAN on the ports connecting to FortiFone. The VLAN ID specified for the native VLAN will be used for when FortiFone first boots up, with LLDP disabled.
   Enter the following commands for the FortiSwitch port that FortiFone will be connecting to (in this example, *port1*):

```
config switch interface
   edit port1
      set allowed-vlans 100
      set native-vlan 200
   next
end
```

3. Apply the newly created LLDP profile to the port connecting to FortiFone. This is the port that FortiFone connects directly to on the switch (in this example, *port1*):

```
config switch physical-port
   edit port1
      set lldp-profile fortifone
      set speed auto
   next
end
```

4. Create the VLAN trunk. This port (in this example, *port10*) is the physical connection between FortiSwitch and FortiGate:

```
config switch trunk
   edit "Gate_Trunk"
      set members "port10"
      set description "Gate Trunk"
   next
end
```

5. To allow the configured trunk to carry traffic for different VLANs, set the allowed VLANs on the trunk interface connecting to FortiGate:

```
config switch interface
   edit "Gate_Trunk"
      set allowed-vlans 1,100,200
   next
end
```

Configure Cisco switch

1. Enable LLDP globally (disabled by default):

```
Switch(Config)# lldp run
```

2. Create a network policy assigning VLAN ID 100 for voice traffic:

```
Switch(Config)# network-policy profile 1
Switch(Config-network-policy)# voice vlan 100
```

3. Apply the network policy to the interface connecting to FortiFone:

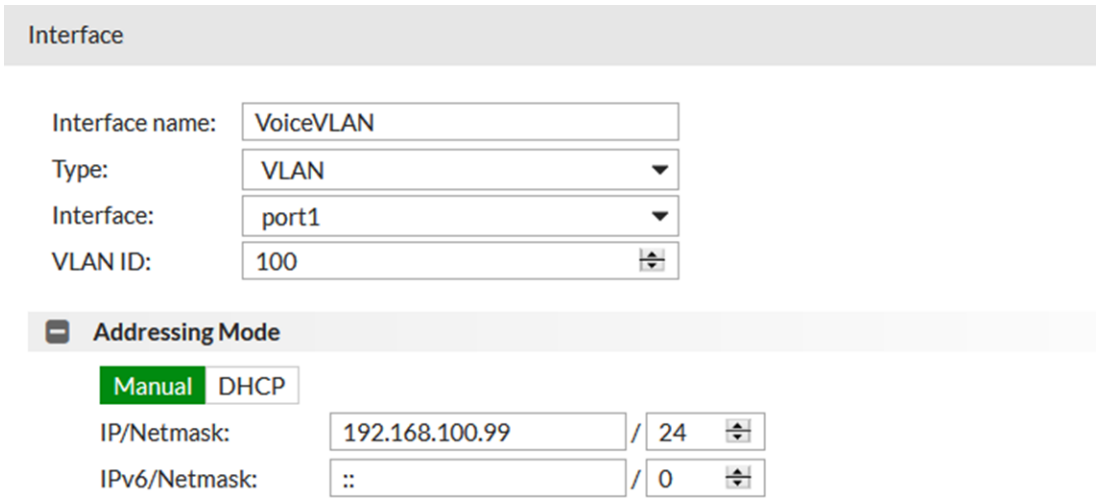
```
Switch(Config)# interface giga 1/0/24
Switch(Config-Interface)# switchport mode access
Switch(Config-Interface)# switchport access vlan 200
Switch(Config-Interface)# lldptransmitl
Switch(Config-Interface)# lldp receive
Switch(Config-Interface)# network-policy 1
```

4. To allow traffic to be carried across different VLANs, set the interface connecting to FortiVoice to trunk mode:

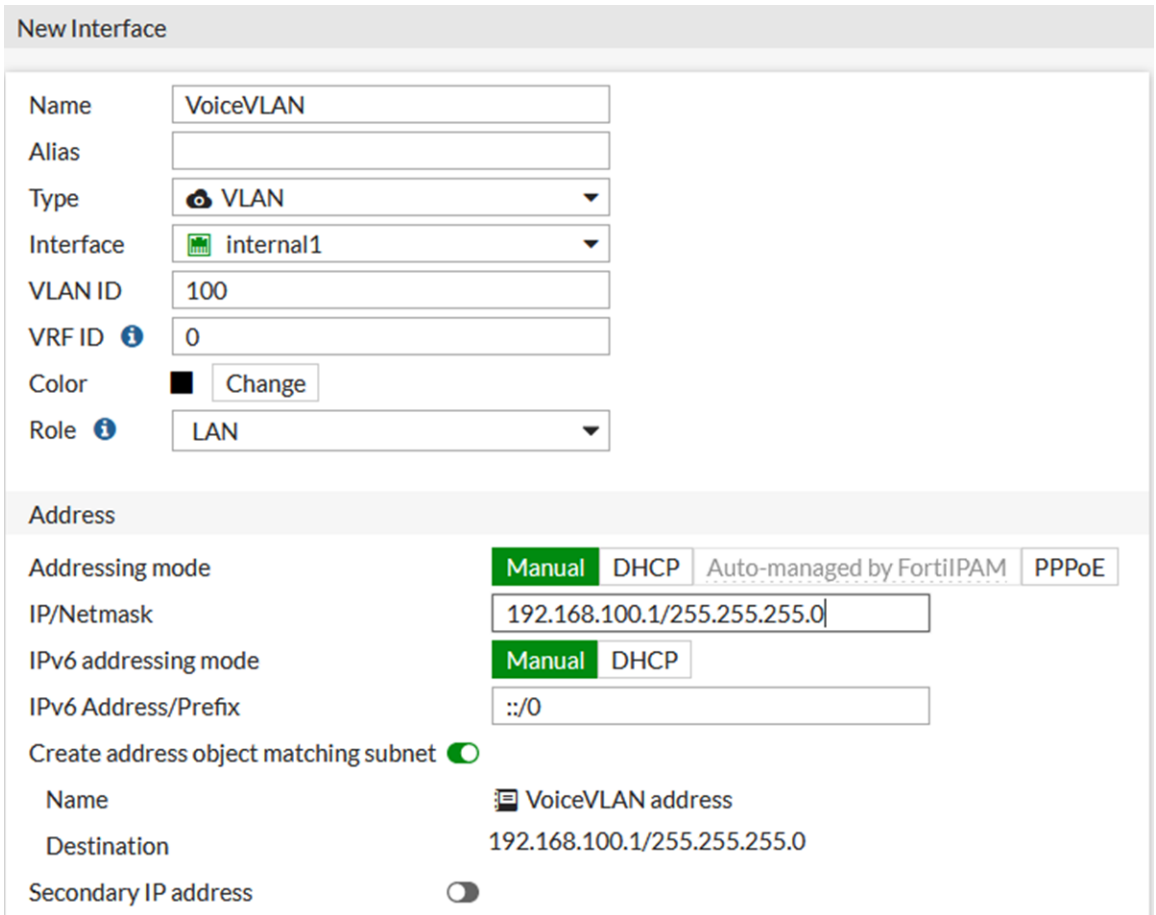
```
Switch(Config)# interface giga 1/0/1
Switch(Config-Interface)# switchport mode trunk
```

Configure the VLAN interfaces on FortiVoice and FortiGate

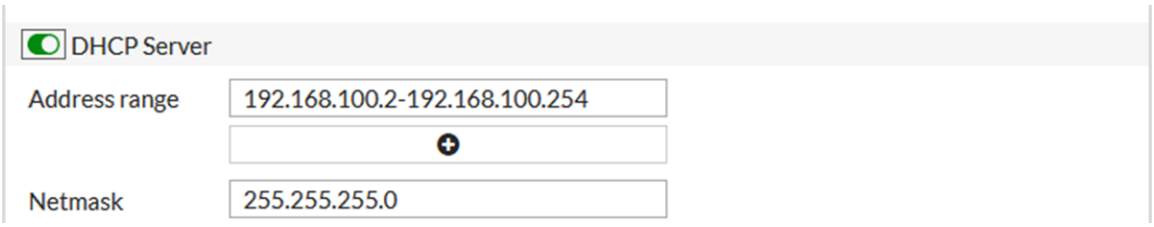
1. On FortiVoice, go to *System* > *Network* > *Network* and click *New*.
2. Enter an *Interface name*.
3. Set *Type* to *VLAN*.
4. Set *Interface* to *port1*.
5. Set a *VLAN ID* of *100*.
6. Under *Addressing Mode*, enter an *IP/Netmask* of *192.168.100.99/24*, and click *Create*.



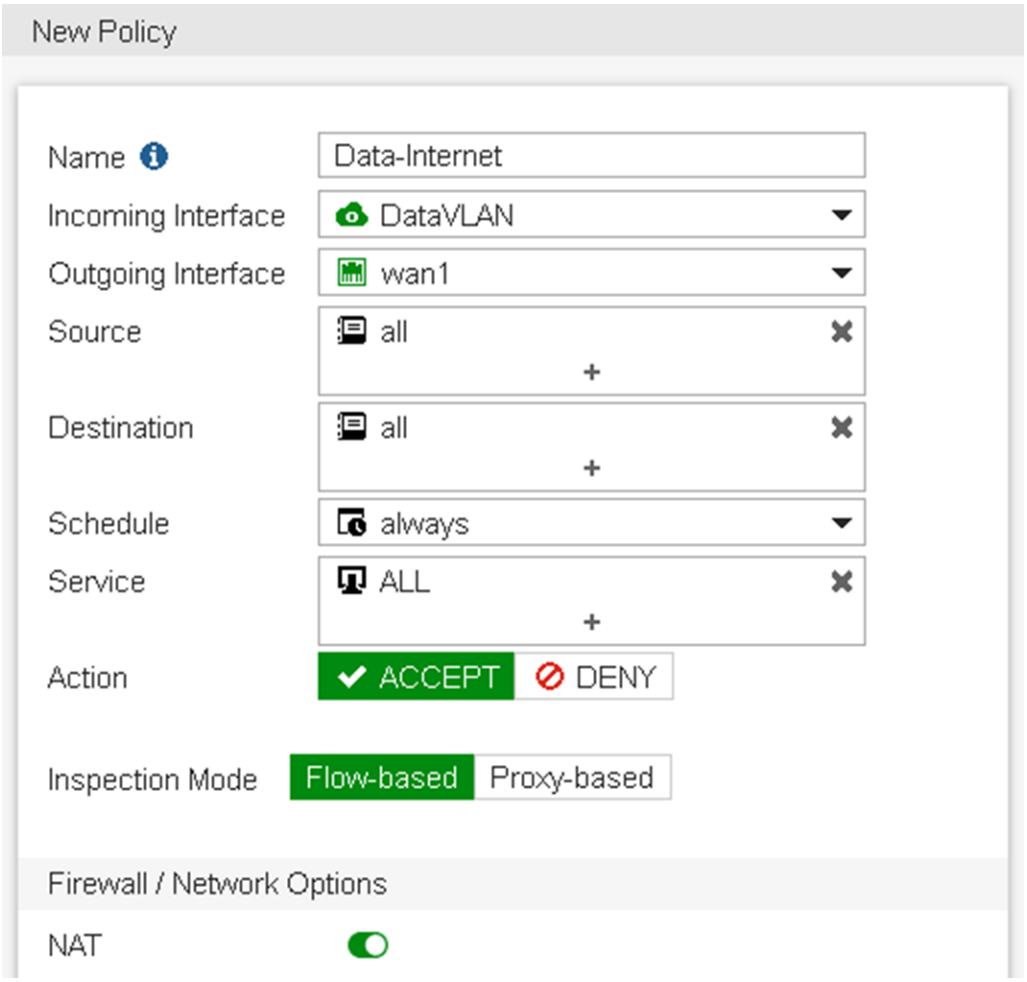
7. Create another entry for the data VLAN on the same interface, this time setting the *VLAN ID* to *200* and an *IP/Netmask* of *192.168.200.99/24*.
8. On FortiGate, go to *Network* > *Interfaces* and click *Create New* > *Interface*.
9. On the internal port, configure VLAN interfaces for both voice and data VLANs, but set their IP/netmasks to 192.168.100.1/24 and 192.168.200.1/24 respectively.



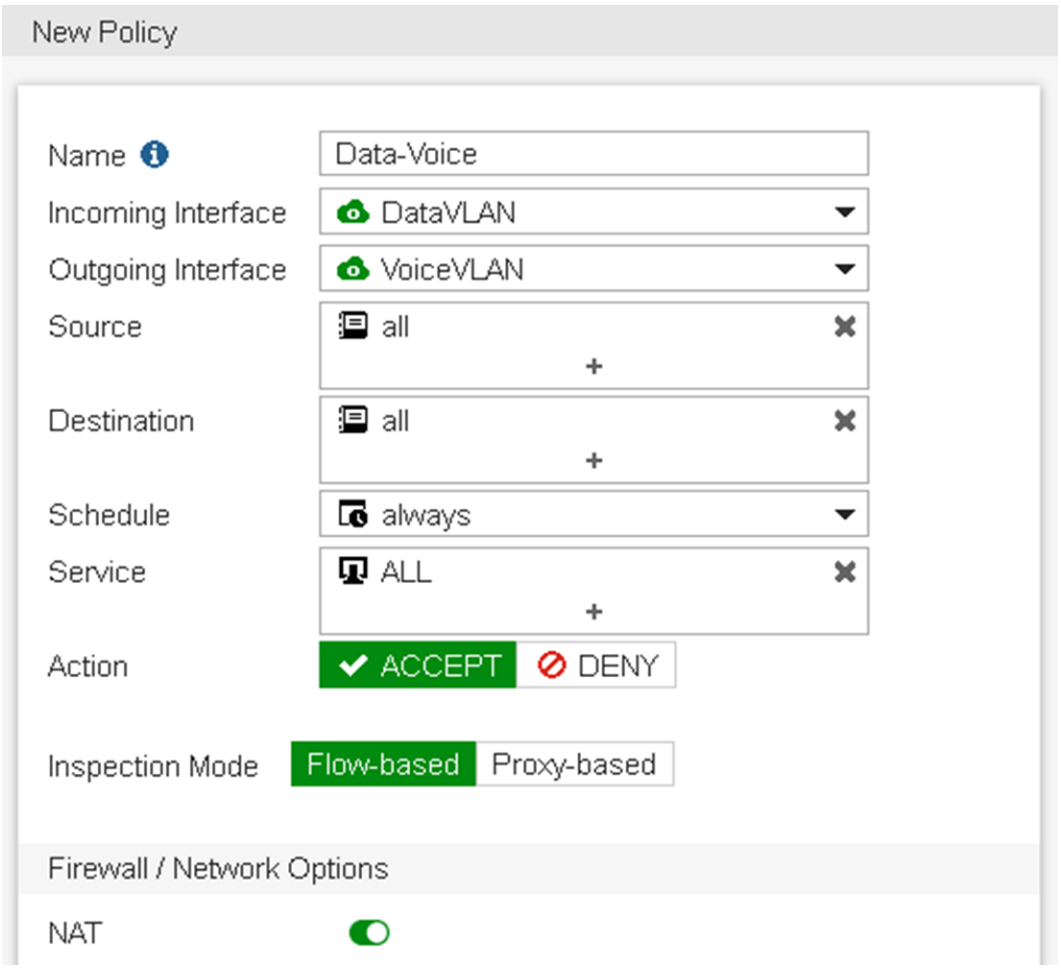
10. In the configuration of the new VLAN interface, enable *DHCP Server* so both VLAN interfaces have an IP *Address Range*.



11. Go to *Policy & Objects* > *Firewall Policy* and create an outbound policy for the data VLAN so the PC connected to FortiFone can access the internet.

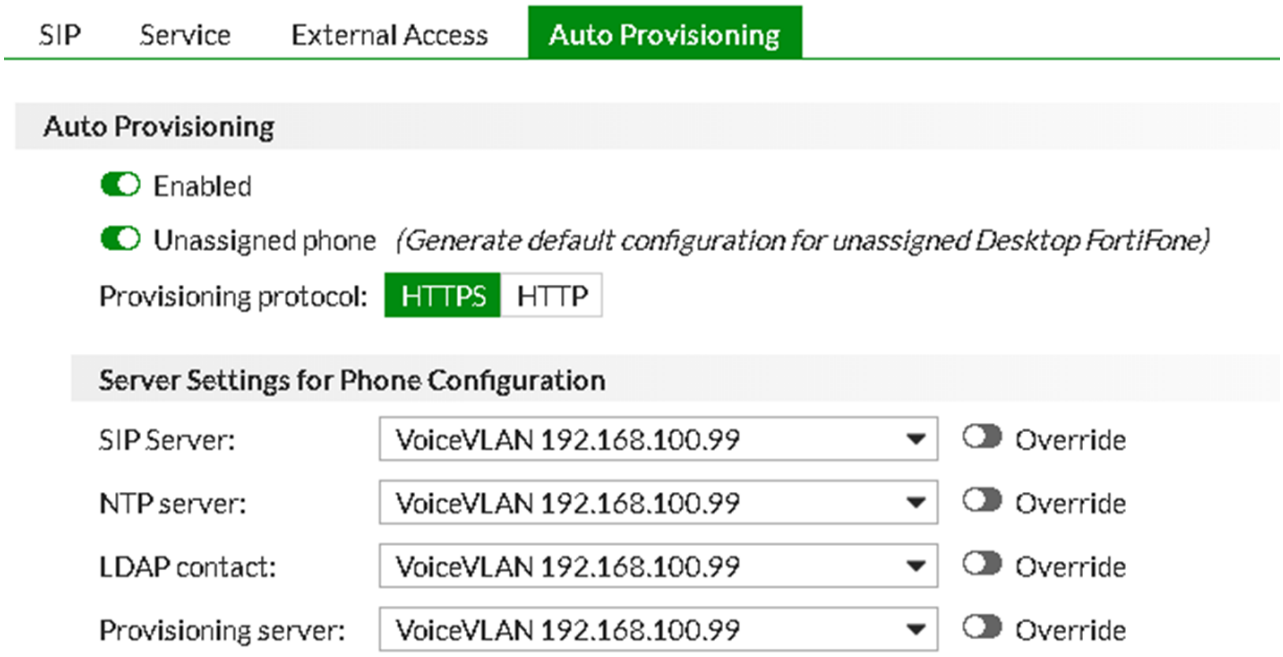


12. To allow FortiFone to auto provision with FortiVoice, create another policy between the voice and data VLANs.



Configure auto provisioning and HTTPS server settings on FortiVoice

1. Back on FortiVoice, go to *System* > *Advanced* > *Auto Provisioning*.
2. Enable the feature and configure the HTTP or HTTPS settings accordingly.



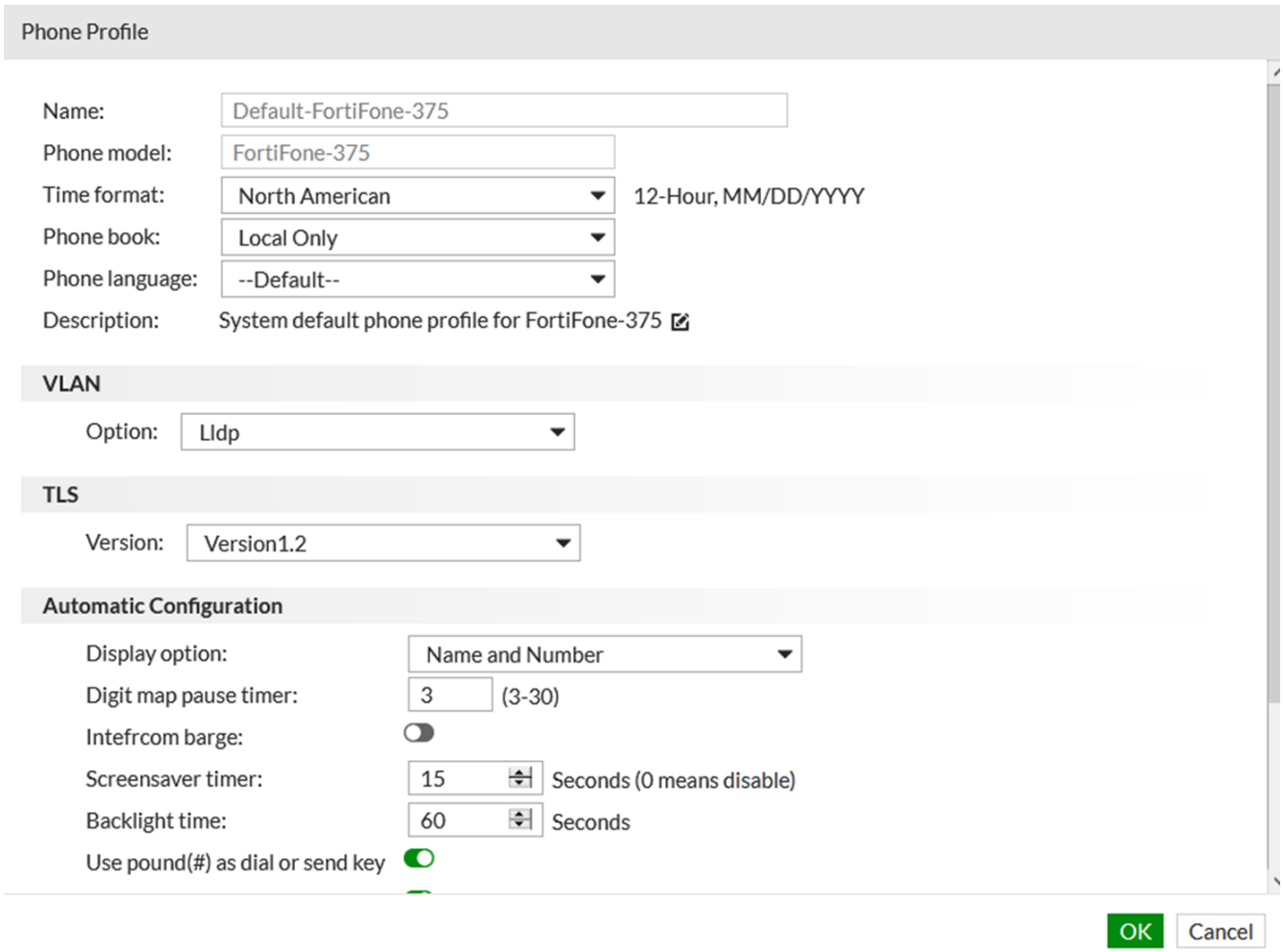
Edit the default LLDP phone profile on FortiVoice

Since some FortiFone models have LLDP disabled by default, make sure that LLDP is enabled to allow FortiFone to auto-discover the voice VLAN configuration.

Editing a pre-existing profile is strongly recommended.

If you decide to create a new phone profile instead of editing a default profile, then you must remember to apply the new profile across the whole deployment.

1. On FortiVoice, go to *Phone System* > *Profile* > *Phone* and select a default profile specific to your FortiFone model.
2. Under *VLAN*, set *Option* to LLDP.
3. Click *OK*.



Perform the initial provisioning of FortiFone

1. Connect FortiFone to the configured VLAN port on the switch. Perform a factory reset on the phone if it currently has an old configuration.
   After the phone reboots, FortiVoice assigns an IP address in the data VLAN (in this example, VLAN 200, 192.168.200.x/24) to FortiFone. This IP address assignment is performed because FortiFone has not received its configuration file (with LLDP enabled) from FortiVoice yet. This can be confirmed by going to *Monitor* > *Extension & Device* > *Phone*.
   Again, be aware that some FortiFone models do have LLDP enabled. These phones appear as unassigned, but have an assigned IP address from the voice VLAN (in this example, VLAN 100, 192.168.100.x/24).
2. Assign the unassigned FortiFone to a new or existing extension. When provisioning the extension, select the custom LLDP phone profile created earlier (in this example, *LLDP-Enable*).
   If there is a large number of FortiFone devices to provision, you can export the extension configurations to a CSV file and then import that file into FortiVoice. For details about exporting and importing IP extensions, see the Configuring IP extensions section in the FortiVoice Phone System Administration Guide.
3. When the extension provisioning is complete, FortiFone reboots automatically, auto-provisions to the configured voice VLAN (in this example, VLAN 100, 192.168.100.x/24), and registers with FortiVoice.

This step may take a few minutes. Once FortiFone registers successfully, make an inbound and outbound test call to verify that FortiFone is configured properly.

Connect the PC to the VLAN port on FortiFone

1. Using a standard Ethernet cable, connect the PC (corporate NIC) to the PC port on FortiFone.
2. Verify that the PC leases an IP address from the data VLAN 192.168.200.x subnet, allowing the PC access to the internet.
3. To confirm that the PC is able to successfully browse the internet, open the PC's command prompt and enter `ipconfig /all`.

Configuring the FortiFone manual VLAN

The following example shows how to create a manual VLAN port trunk configuration, that is specific to manual-VLANs. A gate trunk is configured to connect FortiSwitch to FortiGate. This connection allows VLAN Real-Time Transport Protocol (RTP) traffic between the two devices, and enables VLAN IP addresses to be received from the VLAN DHCP server on FortiGate. Manual trunks are also configured to support multiple VLAN tags.

The key advantage of having a manually configured VLAN over one that uses LLDP is that voice traffic can be prioritized over PC data traffic. The logical VLAN interfaces, each assigned a VLAN ID, can be used to separate more business-critical traffic from less-critical traffic. These interfaces are then referenced in phone system profiles. VLAN tagging must be enabled to segregate the FortiFone voice network and PC data network.

Prior to starting the procedures in this section, make sure to complete the tasks in Configuring FortiFone VLAN using LLDP and FortiGate.

Release and renew IP addresses on the PC

It is a good practice to make sure that a new IP address has been assigned by the PC port of a manual-VLAN FortiFone. To renew all DHCP IP addresses, enter the following commands in the PC's command prompt:

```
ipconfig /release
ipconfig /renew
```

Configure gate and manual VLAN trunks

1. On FortiSwitch, go to *Switch* > *Port* > *Trunk* and create the following four static trunks:
   a. One on port 1 (*Gate-trunk*)
   b. Three on the remaining ports 2, 3, and 4 (*Manual-Trunk-Portx*)
2. Go to *Switch* > *Interface* > *Trunk* and configure the trunk's native and allowable VLAN settings:
   a. Set the *Native VLAN* for each trunk to 1.
   b. Assign each trunk the native, voice, and data VLAN (1, 100, and 200).

Define the port as manual VLAN specific

Open the FortiSwitch CLI console and enter the following commands, specifying port 1 as a manual-only VLAN port.

The `lldp-profile` entry is set to `default`, which means that no LLDP configuration has been applied to the port, leaving it in a manual-only VLAN state:

```
config switch physical-port
   edit "port1"
      set cdp-status disable
```

```
        set description ''
        set dmi-status global
        set flow-control rx
        set l2-learning enable
        set lldp-profile "default"
        set lldp-status tx-rx
        set max-frame-size 9216
        set poe-status enable
        set speed auto
        set status up
    next
end
```

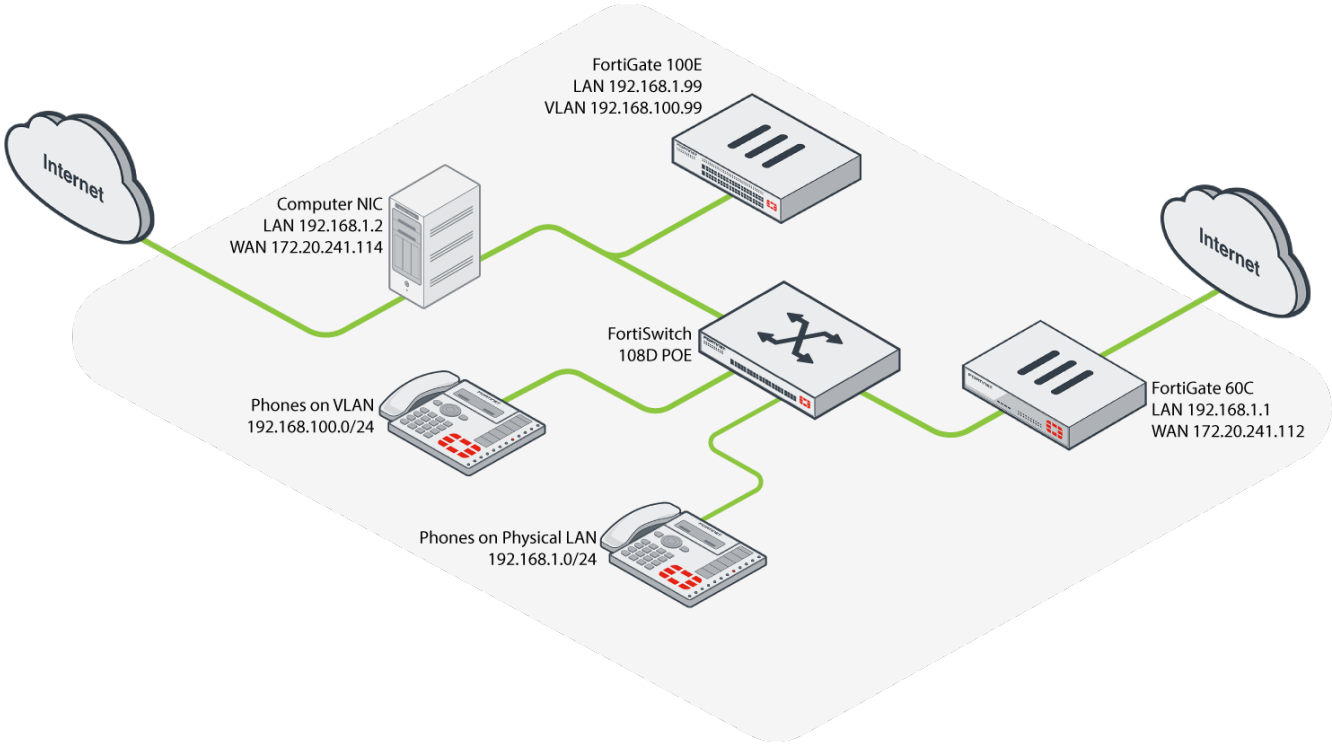
Configuring the FortiFone GUI access on a VLAN

Procedures in this section establish a new route used by the computer NIC on the on the 192.168.1.0/24 subnet to access the FortiFone GUI on the voice VLAN.

Address topology

The IP address topology in this section is similar to the addressing used for the initial FortiFone VLAN provisioning (see Configuring FortiFone VLAN using LLDP and FortiGate).

- The physical LAN is on the 192.168.1.0/24 subnet.
- The voice VLAN is on the 192.168.100.0/24 subnet.
- The data VLAN is on the 192.168.200.0/24 subnet.
- FortiGate is used as the DHCP server.



Configure routes between the NIC and the voice and data VLANs

1. On the computer NIC, open the command prompt and enter the following command to establish a new route to the voice VLAN.

Do not copy and paste this command.

```
Route –p add 192.168.100.0 mask 255.255.255.0 192.168.1.1
```

Where:

- **Route**: Establishes a new route.
- **-p**: Makes a permanent change; will not be removed if the PC is rebooted.
- **192.168.1.1**: Default gateway for this route.

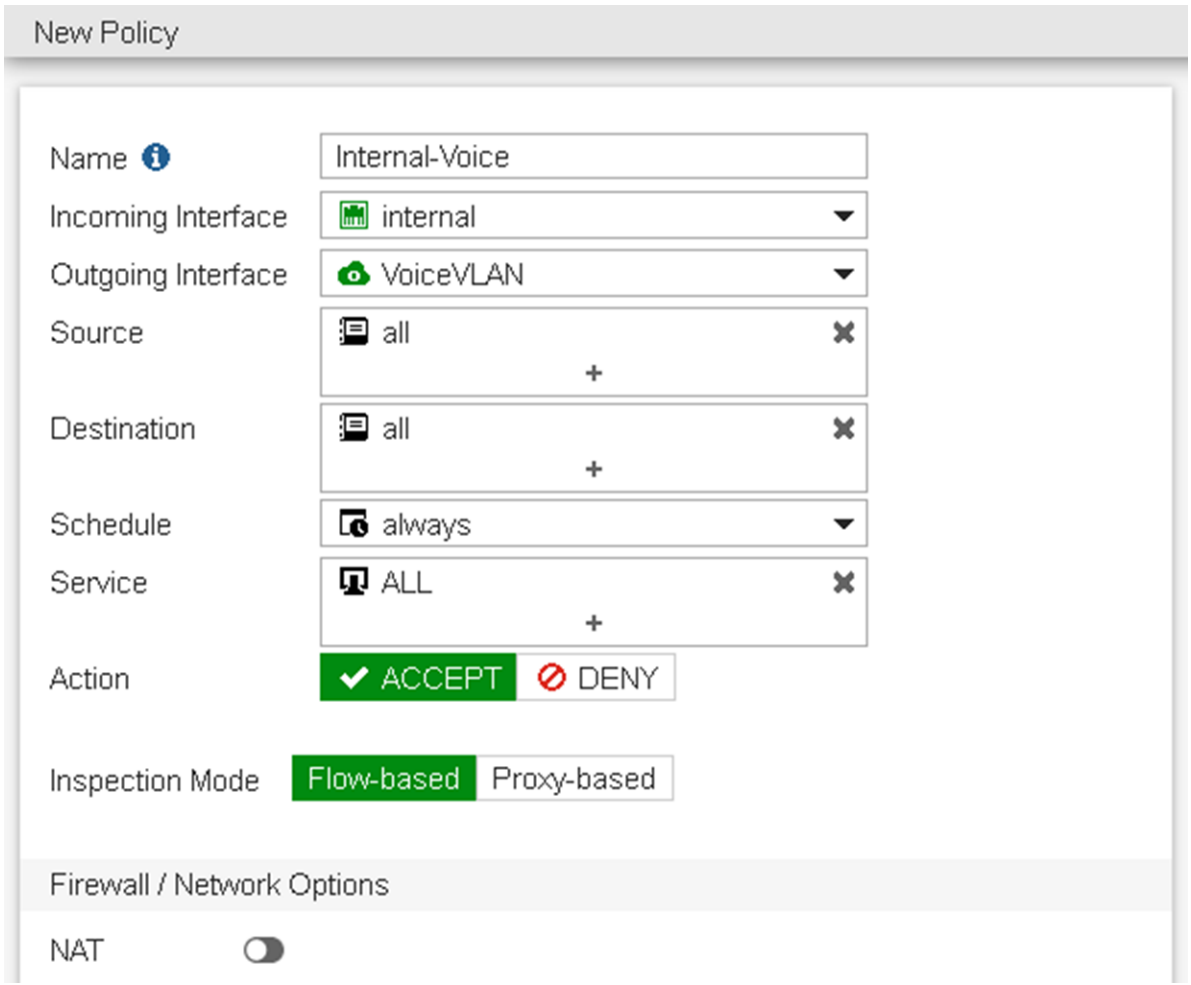
2. Enter the following command to establish a new route to the data VLAN.

Do not copy and paste this command.

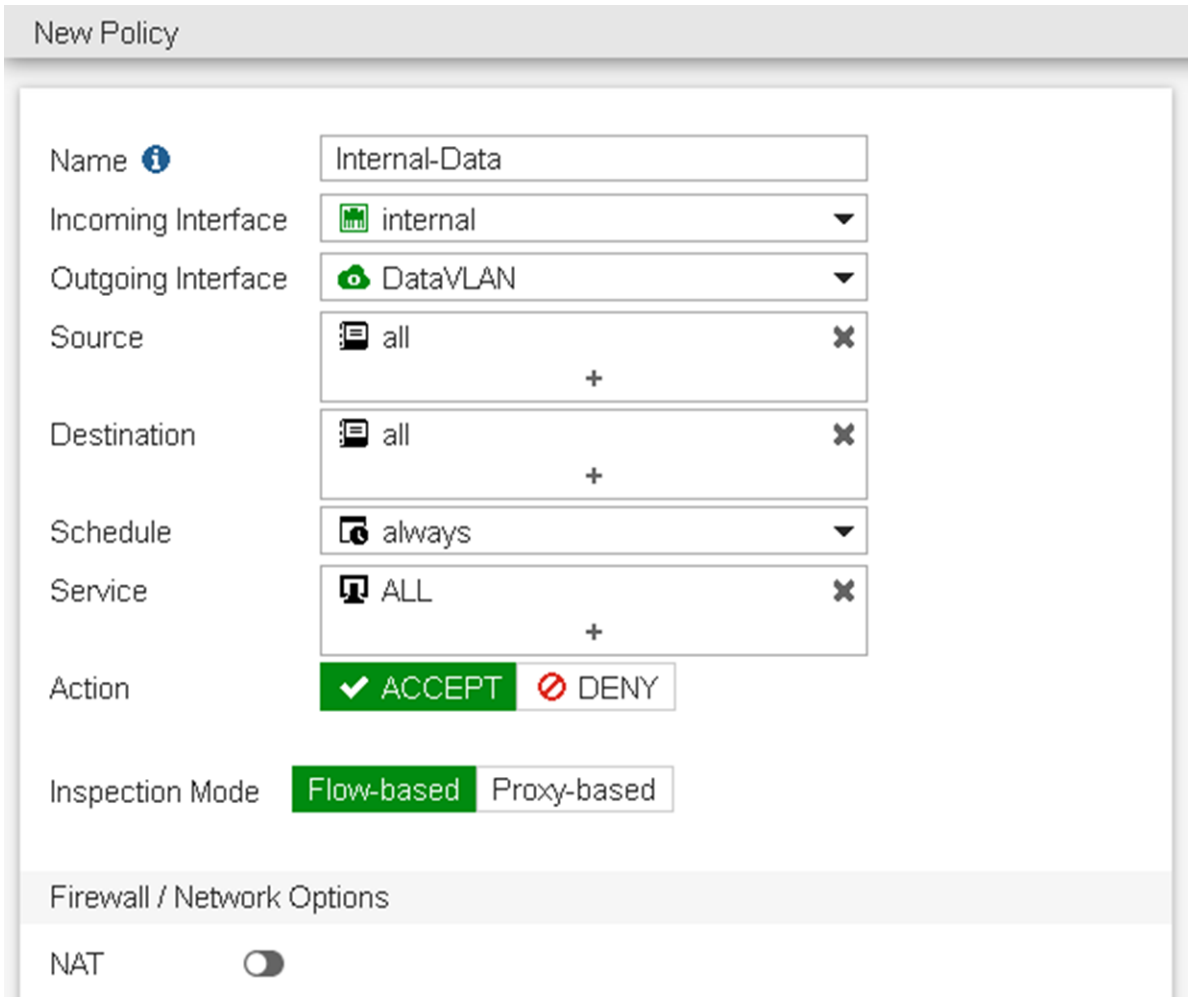
```
Route –p add 192.168.200.0 mask 255.255.255.0 192.168.1.1
```

Create policies between the LAN and the voice and data VLANs

1. On FortiGate, go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Enter a *Name*.
3. Set *Incoming Interface* to *internal*.
4. Set *Outgoing Interface* to *VoiceVLAN*.
5. For this policy, make sure to disable NAT.



6. Create another policy, allowing a connection between internal and the data VLAN.
7. Again, make sure that NAT is disabled.


New Policy
Name
Internal-Data
Incoming Interface
internal
Outgoing Interface
DataVLAN
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT