FortiNAC

IP Phone Integration

Version 8.x

Date: 8/29/2018

Rev: C

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE

http://training.fortinet.com

FORTIGUARD CENTER

http://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Wednesday, August 29, 2018

Contents

IP Phone Integration

FortiNAC does not provide any special integration logic for different IP phone vendors. Typically, the network administrator deploys the organization's IP phone infrastructure independently of configuring the FortiNAC. Because FortiNAC's focus is on hosts daisy-chained to the phone, the type of phone that is used is unimportant.

Switch ports are usually configured for IP phones by defining some sort of tagged VLAN or special voice VLAN for the phone, which operates independently of the untagged VLAN that governs other traffic (data) on that port. FortiNAC does not involve itself with these VLANs. In fact, it is purposefully ignorant of them.

Note: Do not trunk Cisco ports that have IP Phones connected. Configure the access (untagged) VLAN and voice VLAN for the port. FortiNAC does not manage trunked ports.

Overview

The following table lists FortiNAC features applicable to IP phone support.

Feature	Description
Ignore IP phone MAC addresses when determining the appropriate VLAN for a port	As long as the device is identified as an IP phone,FortiNAC does not consider its presence when calculating the VLAN for the port. The administrator must associate the device type IP Phone with the device in FortiNAC.
Learn comings/goings of hosts daisy-chained to the phone	Traps or other notifications are needed to inform FortiNAC when hosts come and go from the phone ports, since FortiNAC cannot rely on the linkUp/linkDown traps per usual. For example: • Cisco supports a Mac Notification trap (learned and removed) that can provide this information • HP has just added a similar Mac Notification trap capability to a few of their switches • RADIUS authentication can also provide half the picture for some switches, though it is difficult to know when hosts disconnect
Automatic phone provisioning on a port	This provides ability to plug an IP phone into any port and have that port automatically configured for the phone. FortiNAC has limited support for this by leveraging the FlexCLI feature to specify the switch-specific commands to manage this process. When a phone plugs in, the configured CLI commands are applied to the port. To aid in this process, an IP phone group was added (functions as part of the Role-based CLI mapping function).

IP Phone Integration Process

1. Configure a Voice VLAN on switches to which IP phones will be connected. Typically this is a tagged VLAN. FortiNAC ignores devices on tagged VLANS and manages devices on untagged VLANs such as PCs.
2. If supported, configure MAC Notification traps on the same set of switches. FortiNAC supports MAC Notification traps on Cisco and some HP switches.
3. For Cisco switches, go to the Model Configuration View in FortiNAC and enter a comma separated list of Voice VLANs. This indicates to FortiNAC that devices on that VLAN should not be moved to any other VLAN ever. See Model Configuration.
4. Provision the phones with their proprietary configuration.
5. Add IP Phones to the FortiNAC database using one of the methods listed.
   - Import IP Phones using a .csv file. See Import Hosts, Users Or Devices.
   - Connect your phones to the network and then convert the rogue hosts to IP phones using the Register As Device tool. See Register A Host As A Device.
   - Connect your phones to the network and use the Device Profiler feature to automatically register them as IP Phones. See Device Profiler.
   - Add a new host in the host view and choose Register As A Device in the Add window, then select IP Phone as the device type. See Add Or Modify A Host.

   IP phones should be added to an IP Phone group to aid in management later. Make sure that the device type is set to IP Phone. By identifying these devices as IP Phones you indicate to FortiNAC that they should be ignored when determining the VLAN for the port.
6. Connect the PC to the phone and attempt to access the network.
7. Once an IP Phone is connected to a port, FortiNAC does not bring down the interface to change VLANs. If there is an agent installed on the connected host, the agent does a release/renew of the IP address which forces the VLAN change. If there is no agent installed, the user must wait for the IP address lease to expire. If you are not using agents on host machines, you may want to configure shorter lease times for IP addresses.

Host Connection Process Through Phone Port

1. PC connects to the port on the back of the phone.
2. If MAC Notification Traps are enabled, a trap is sent to FortiNAC.
3. If MAC Notification Traps are not enabled, the presence of the host connection is not detected until the next L2 Poll. The host will connect immediately to the network or VLAN to which the port is currently set. If the polling interval is very long, a host may have to wait before being able to register or moving to the correct VLAN.
4. FortiNAC determines the MAC Address of the PC and looks for it in the database to determine whether or not it is registered.
5. If it is not registered, the PC is placed in the Registration VLAN but the phone remains in the Voice VLAN.
6. If it is registered, the PC is placed in the Production VLAN and the phone remains in the Voice VLAN.

Additional Reading

- Solution 1498: *Voice VLAN Assigned as Default by Mistake*
- Solution 1378: VLANs Out of Sync Between Switch and FortiNAC Model Configuration
- How To: Cisco Using MAC Notification Traps For Better Performance
- Solution 1502: HP ProCurve: Configuring MAC-Notification Traps
- FortiNAC online help topics on Model Configuration and VLANs