FortiNAC

Juniper EX Switch 802.1x-MAC-Authentication Device Integration

Version: 8.x

Date: April 29, 2020

Rev: D

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

Contents

Overview

The information in this document provides guidance for configuring the Juniper EX switch to be managed by FortiNAC when configured for RADIUS (802.1x or MAC Authentication). This document details the items that must be configured.

If the Juniper switch will not be configured for RADIUS, *do not use this document*. Configure the switch and see section **Add or Modify a Device** of the **Administration Guide** in the Fortinet Document Library for instructions on modeling the device in Topology.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

FortiNAC provides network visibility (where endpoints connect) and manages network access for hosts connecting to the Juniper EX using RADIUS authentication.

How it Works

Visibility

FortiNAC learns where endpoints are connected on the network using the following methods:

- RADIUS communication
- L2 Polling (MAC address table read)
- L3 Polling (ARP cache read)

Control

FortiNAC provisions an endpoint's network access by managing VLAN assignments based on the switch model configuration or an applicable network access policy and the host state of the device. The VLAN configuration is modified using the appropriate method based upon the vendor and model (see chart below).

Device Support Methods

Endpoint Connectivity Notification	Reading MAC Address Tables (L2 Poll)	Reading IP Tables (L3 Poll)	Reading VLANs	VLAN Assignment	De-auth
RADIUS (802.1x or MAC-auth)	CLI	SNMP	CLI	CLI RADIUS	RADIUS Disconnect (UDP 3799)

RADIUS Authentication

FortiNAC supports MAC and 802.1x authentication.

See **Wired RADIUS Authentication** in the Appendix for more information regarding RADIUS operation. For more FortiNAC RADIUS integration details, including switch support, see section **Wired devices and 802.1X** of the **Administration Guide** in the Fortinet Document Library.

Note: There is no immediate notification to FortiNAC of when an endpoint disconnects. FortiNAC must rely on polling the switch for L2 information to determine an endpoint has disconnected.

Requirements

- **Juniper**
  - Minimum firmware version: JUNOS 12.3
  - SNMP community or account
  - Account for SSH access
  - Static IP address (or dynamic IP addresses that are reserved). FortiNAC has no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.
- **FortiNAC**
  - Minimum version: Version 7.0
- **Host configuration (required for 802.1x authentication)**
  - Host supplicants should be configured to authenticate using user credentials, not host information, such as hostname. This will give FortiNAC the user information to associate with the host/device allowing for automatic authentication.
- **RADIUS Server (required for 802.1x authentication)**
  - The encryption method for user names and passwords passed between FortiNAC and the RADIUS server must be set to PAP. This affects the validation account created on the RADIUS server for communication with FortiNAC and entered in the RADIUS Server Profile configuration.
- **Network**
  - Do not use asymmetric routing between your device and the FortiNAC server. RADIUS requests and responses between the FortiNAC server and the wireless device must travel through the same interface on the FortiNAC server.
  - **Important:** FortiNAC's capacity for processing RADIUS requests is approximately 60 requests per second. Capacity is affected by the use of other features in the program such as the Persistent Agent or MAC Notification Traps. Any requests that are not immediately processed are placed in queue. After 5 seconds any unprocessed requests are discarded. If FortiNAC is going to be installed in an environment where it is expected to receive more than 60 RADIUS requests per second, an additional FortiNAC appliance may be required to handle the load.

Integration

Configure Juniper EX

Before integrating with FortiNAC, set the device up on your network and ensure that it is working correctly. Once working, begin the integration process with FortiNAC.

Note: When configuring security strings on network devices or names for items within the configuration, it is recommended that you use only letters, numbers and hyphens (-). Other characters may prevent FortiNAC from communicating with the device, such as #. Some device manufacturers prohibit the use of special characters. For example, Cisco prohibits the use of @ and #.

Radius Server

Define the FortiNAC Server or FortiNAC Control Server as the RADIUS server for the devices to be managed by FortiNAC.

radius-server	FortiNAC Server/Control server eth0 interface IP Address **High Availability**: IP address of primary control server (Do not use Shared IP address). Set up the secondary control server as a secondary RADIUS server using its actual IP address. (802.1x environments) consider setting up the actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.
port	UDP 1812
source-address	Switch IP address displayed in Topology
secret	**Important**: Must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.

To configure FortiNAC as the RADIUS server, use the following command:

```
# set access radius-server <FortiNAC IP Address> port 1812 source-
address <switch IP address Modeled in Topology> secret <radiusSecret>
```

Authentication Profile

Create an authentication profile which specifies to use the FortiNAC server. Use the following commands:

```
# set access profile <profileName> authentication-order radius

# set access profile <profileName> radius authentication- server
<FortiNAC eth0 IP Address> accounting-server
<FortiNAC eth0 IP Address>

# set protocols dot1x authenticator authentication-profile-name
<profileName>
```

MAC Authentication (optional)

MAC-Auth can be used to support multiple clients on a single port, and to bypass lengthy configuration commits. Juniper EX Switches do not support SNMP writes. Therefore, to configure the device FortiNAC must interact with the Juniper CLI. Committing changes via the CLI takes a very long time on these devices and the time increases significantly when the device is stacked.

MAC Authentication on a port in conjunction with RADIUS responses can be used to avoid this issue all together. In this scenario, there is no need to bring the port down or back up, and no need to switch the VLAN on the port.

In addition, using MAC-Auth removes the need for mac-notification traps. Managing the ports with MAC-Auth supports the use case where multiple hosts connect behind an IP Phone or a router. Each host is handled separately and can be given a different VLAN in the RADIUS response. This option provides more flexibility than port based VLAN assignment relied on when using MAC Notification traps.

Switch Configuration:

Basic MAC Authentication is enabled using the following commands:

```
# set protocols dot1x authenticator interface <interfaceName> supplicant
multiple

# set protocols dot1x authenticator interface <interfaceName> mac-radius
restrict

# set protocols dot1x authenticator  interface <interfaceName> mac-radius
flap-on-disconnect
```

The following commands have additional options:

supplicant:

- **single**—Only one host needs to authenticate. All other hosts piggybacks on the first host. This is not secure and is not recommended.
- **single-secure**—Only one host can authenticate. All other hosts are not allowed on the port.
- **multiple**—One or many hosts can connect to the port. Each host authenticates separately.

mac-radius restrict: This setting is required if you only want to use MAC-Auth. If this is not set the device attempts to use 802.1x first, and will only use MAC-Auth as a fallback.

flap-on-disconnect: This option is required for the FortiNAC integration. Without this the host never receives a new IP address. This is the equivalent of bringing down the port and then bringing the port back up when switching VLANs.

Wired 802.1x For Port Security (optional)

This is the standard 802.1x use case for a pure 802.1x solution. Only hosts or devices with a valid 802.1x supplicant are allowed to connect to a port.

Switch Configuration:

```
# set protocols dot1x authenticator interface <interfaceName> supplicant
multiple
```

The following commands have additional options:

supplicant:

- **single**—Only one host needs to authenticate. All other hosts piggybacks on the first host. This is not secure and is not recommended.
- **single-secure**—Only one host can authenticate. All other hosts are not allowed on the port.
- **multiple**—One or many hosts can connect to the port. Each host authenticates separately.

Note: There is no flap-on-disconnect option for 802.1x. The supplicant handles refreshing the IP address on a VLAN change.

Wired 802.1x With MAC-Auth Fallback (optional)

This option attempts an 802.1x authentication first, and only uses MAC-Auth as a fallback if 802.1x authentication fails. This is a good option for networks where 802.1x enabled devices are required to work alongside devices that don't support 802.1x.

Switch Configuration:

Similar to the MAC-Auth configuration but with no restrict option.

```
# set protocols dot1x authenticator interface <interfaceName> supplicant
multiple
```

```
# set protocols dot1x authenticator  interface <interfaceName> mac-radius
flap-on-disconnect
```

The following commands have additional options:

supplicant:

- **single**—Only one host needs to authenticate. All other hosts piggybacks on the first host. This is not secure and is not recommended.
- **single-secure**—Only one host can authenticate. All other hosts are not allowed on the port.
- **multiple**—One or many hosts can connect to the port. Each host authenticates separately.

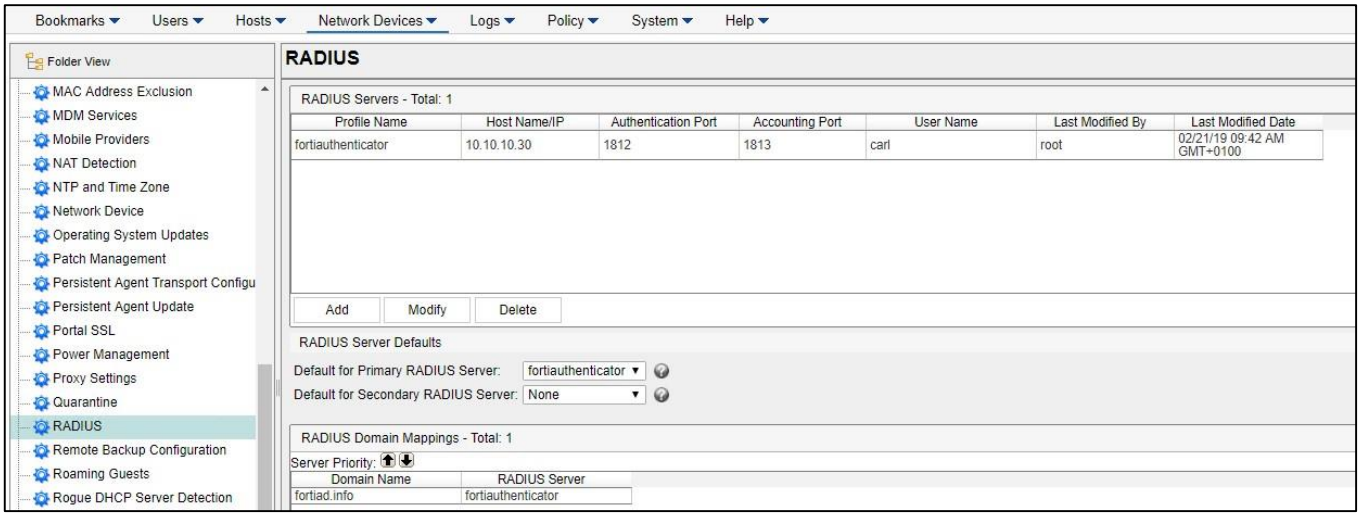
flap-on-disconnect: This option is required for the FortiNAC integration. Without this the host never receives a new IP address. This is the equivalent of bringing down the port and then bringing the port back up when switching VLANs.

Configure FortiNAC

RADIUS Server (Required for 802.1x Authentication)

FortiNAC acts as a proxy for 802.1X requests. Add a RADIUS server (such as FortiAuthenticator) to FortiNAC in order to proxy the 802.1X packets to the correct server. See **Configure RADIUS Settings** in the **Administration Guide** for instructions.

Important: The RADIUS Secret used must be exactly the same on the RADIUS server.



Note: FortiNAC does not proxy RADIUS requests when using MAC authentication.

Model the Device

1. Navigate to **Network Device > Topology**
2. Discover or add all APs. See section **Add or Modify a Device** or **Discovery** of the **Administration Guide** for instructions.

   SNMP Settings: SNMP v1 or v3 credentials

   CLI Settings: Credentials used for CLI or API access.

Note: If a "?" appears as the icon, then support needs to be added for that device. See KB article Options for Devices Unable to Be Modeled in Topology for instructions.

3. Click the **Polling** tab in the right panel of the model.
4. Set **L2 (Hosts) Polling** to 10 minutes. And click **Save**.

Model Configuration

1. After modeling the device in the Topology View, right-click on the model and click **Model Configuration**.
2. Fill in the fields as appropriate:
   - **User Name** used for CLI access
   - **Password** used for CLI access
   - **Protocol** used for CLI access
   - **Primary RADIUS Server (802.1x authentication)**: Either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
   - **Secondary RADIUS Server (802.1x authentication):** Either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
   - **RADIUS Secret**: Required for both MAC and 802.1x authentication. Must match the value entered on the device itself and the value entered on the RADIUS settings window.
3. In the **Network Access** section, click the **Read VLANs** or **Read Roles** button. This populates the drop-down lists for the different connection states, such as Registration. Data in the drop-down lists represents the roles or VLANs created on the device.
4. Select a setting in **Access Enforcement** for each host state.
5. In the **Access Value** column select a Role or VLAN for each host state desired to enforce.
6. In the **Preferred Container** field, select the Container in Topology which the Wireless Access Points should be placed as they are discovered.
7. Click **Apply**.

Validate

1. Configure test port to send RADIUS requests to FortiNAC.
2. Connect a rogue host to the newly enforced port.
3. Verify the following:
   - Host is moved to the isolation VLAN
   - Host is able to access the captive portal (if configured)
   - Register the system and make sure it gets moved to the appropriate VLAN.

If any of the above do not work as expected, refer to the Troubleshooting section of this document.

Troubleshooting

Related KB Articles

Refer to the applicable KB article(s):
Troubleshooting SNMP Communication Issues
Troubleshooting Poll Failures
Troubleshooting RADIUS clients not connecting
Troubleshooting Wireless Clients Moved to the Wrong VLAN

Debugging

FortiNAC Commands

Send a RADIUS Disconnect:
```
SendCoA -ip <devip> -mac <clientmac> -dis
```

RADIUS activity (prints to /bsc/logs/output.master):
```
CampusMgrDebug -name RadiusManager true
```

L2 related activity (prints to /bsc/logs/output.master):
```
CampusMgrDebug -name BridgeManager true
```

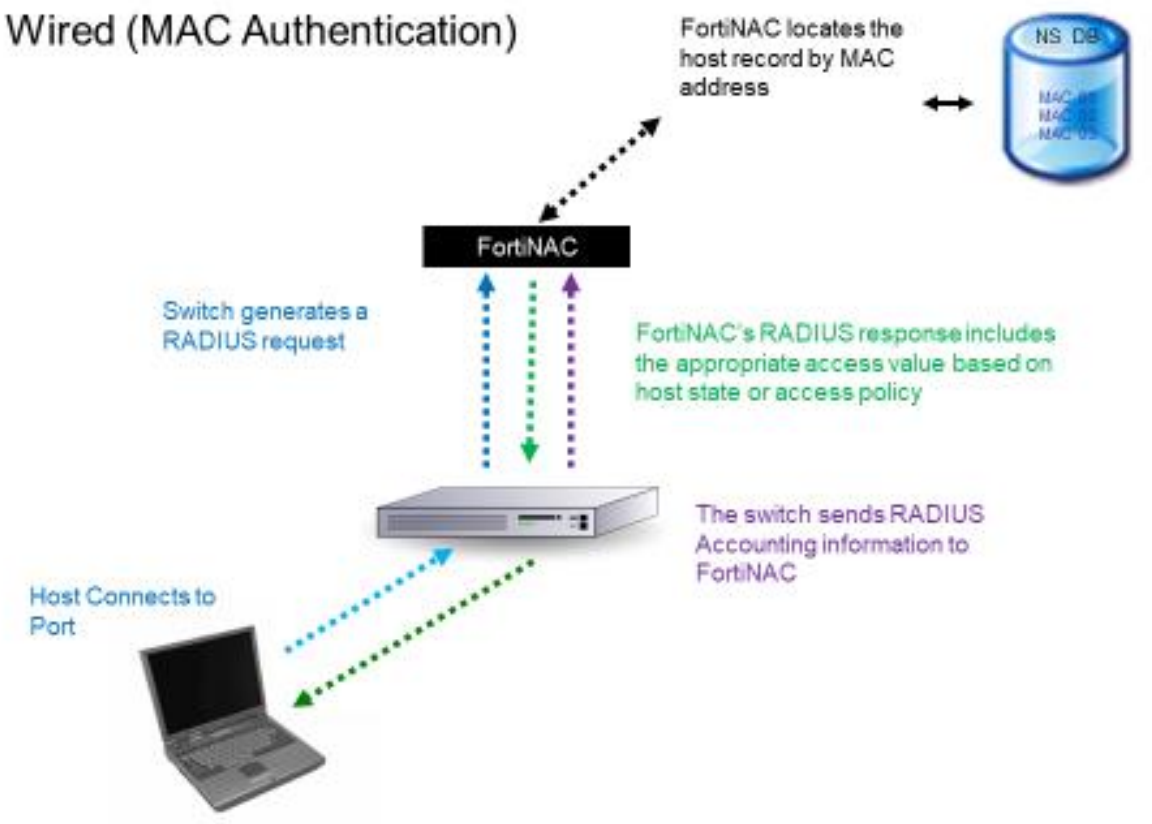
Vendor specific (prints to /bsc/logs/output.master):
```
CampusMgrDebug -name Juniper true
```

Disable debugging feature
```
CampusManagerDebug -name <value> false
```

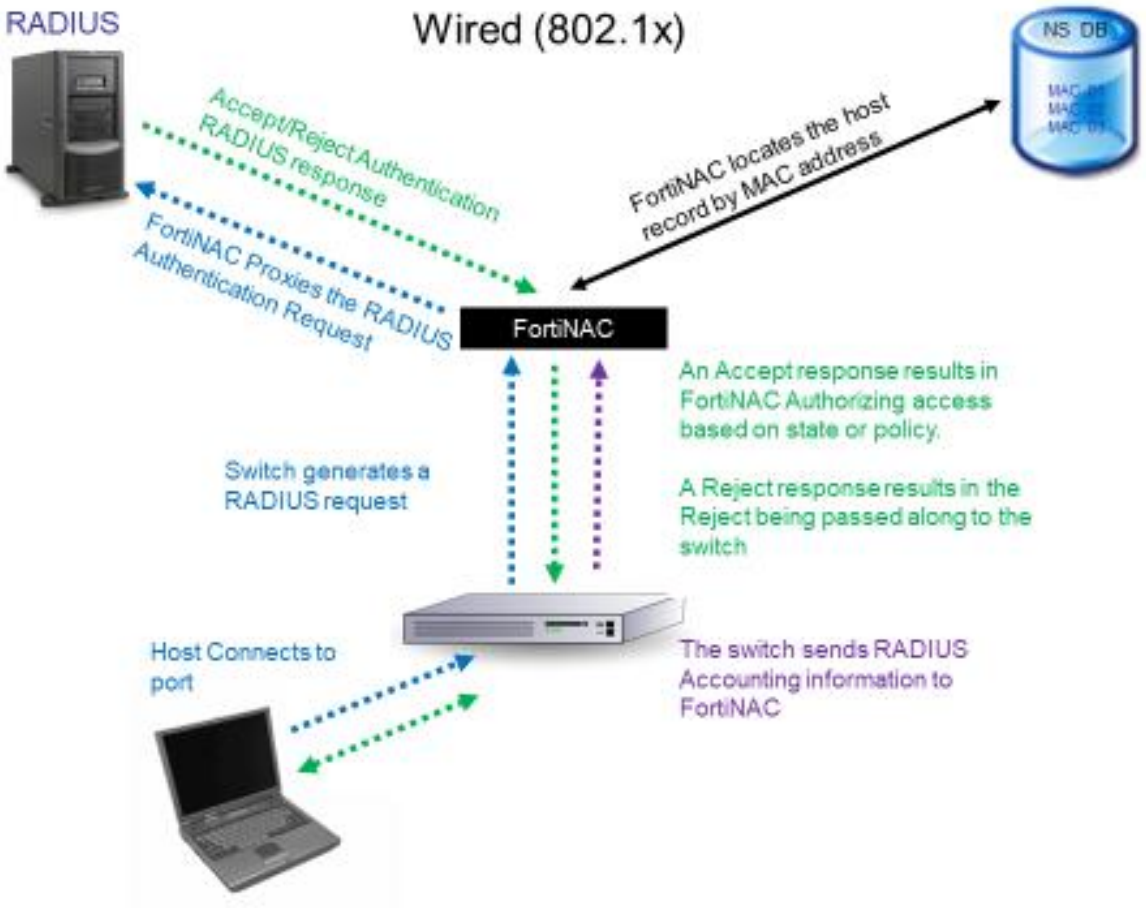
Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Appendix

Wired RADIUS Authentication



MAC Authentication: Endpoints are authenticated based on the MAC address. This requires no configuration on the endpoint.



802.1x Authentication: Endpoints are authenticated based on user information. This requires supplicant configuration on the endpoint and a third party authentication server.