Network Configuration Example

Employee and Guest Access for wired devices with Juniper EX and Impulse SafeConnect NAC

Modified: 2017-02-20

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring MC-LAG on EX9200 Switches in the Core for Campus Networks

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Network Configuration Example

This network configuration example describes the different components and configurations required to enable Employee and Guest access for wired endpoints using Impulse's SafeConnect Network Access Control Offering.

This network configuration example is based on a validated topology. Juniper Networks validated network configuration examples are extensively tested using both simulation and live network elements to ensure comprehensive validation of all published solutions. Customer use cases, common domain examples, and field experience are combined to generate prescriptive configurations to guide customer and partner implementations of Juniper Networks solutions.

Use Case Overview

Juniper Networks EX Series switches are designed to meet the demands of today's high-performance businesses. EX Series Ethernet switches allow companies to grow their networks at their own pace, minimizing large up-front investments. Based on open standards, EX Series switches provide the carrier-class reliability, security risk management, virtualization, application control, and lower total cost of ownership (TCO) that businesses need today while allowing them to scale in an economically sensible way for years to come.

Impulse's SafeConnect solution is a policy management platform that provides role- and device-based network access control for IoT and user devices across any wired, wireless and VPN infrastructure. Enterprises which also deploy EX Series switches in these environments can leverage the extensive RADIUS capabilities on the EX Series switches to integrate with SafeConnect. This enables customers to deploy consistent security policy across wired and wireless infrastructure.

Multiple use cases can be addressed with Juniper EX Series and SafeConnect. This document describes an example of how to configure a Juniper EX4300 switch and SafeConnect for Wired Employee and Guest access.

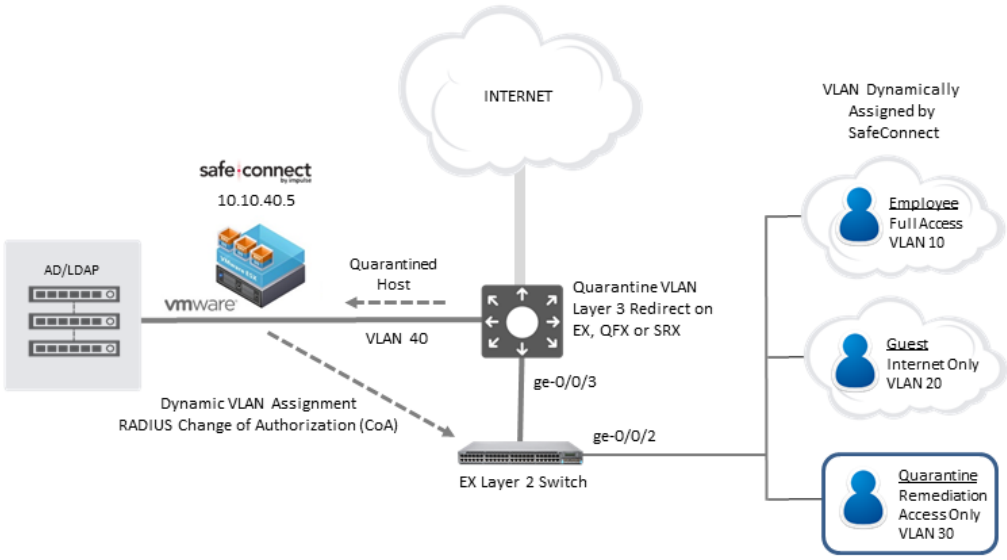
Related Documentation

- Configuring EX switches for 802.1X Authentication
- Configuring EX switches for MAC Authentication
- SafeConnect RADIUS Server Configuration Guide

Use Case Details

In addition to Employees, enterprises typically have visitors, contractors or guests who would require access to the network. Especially in scenarios where contractors are working in campus, they would need temporary access to the network or to the Internet. It is common for these users to use wired network for access. Enterprises that have port control enabled on access ports can use Impulse SafeConnect to provide the necessary access to these temporary users. Guest users are redirected to a guest self-enrollment portal where the user can submit a request for guest credentials to authenticate to the guest network without involving help desk personnel. After the guest authentication is successful, the guest user gets limited access to the network. Juniper EX series switches enable this workflow by providing support for MAC authentication, Dynamic VLAN Assignment and RADIUS Change of Authorization capabilities.

Figure1: Use Case Topology



In this case, ge-0/0/2 is configured for port authentication. In EX switches by default the authentication order is 802.1x -> MAC Radiius -> Captive portal. In this example, an Employee or Guest laptop is connected to port ge-0/0/2. The laptop may or may not be configured for 802.1X authentication.

For an Employee laptop with 802.1X configured, EAPoL packets are received by the switch and 802.1X authentication will be performed. After authentication takes place, the SafeConnect RADIUS server will dynamically assign the port to the Employee VLAN (10).

For a Guest laptop that does not have 802.1X configured, EAPoL packets are not received by the switch and MAC authentication is performed. The MAC authentication will initially place the port in the Quarantine VLAN (30) for Captive Portal user authentication. The Layer 3 device (EX / QFX / SRX) will redirect traffic received in the Quarantine VLAN to SafeConnect. After authentication takes place, a RADIUS Change of Authorization (CoA) will be sent from the SafeConnect RADIUS server to the EX Layer 2 switch and the port will be placed in the Guest VLAN (20).

Components

- Juniper EX Series Layer 2 Switch
  - 15.1R3 or later
- Juniper EX / QFX / SRX for Layer 3
  - 15.1R3 or later
- Impulse SafeConnect
  - 6.4 or later

Configuration

Configuring the EX Layer 2 Switch

On EX for port authentication, you must configure the following.

- Access Profile and provide RADIUS server details
- Dot1X protocol configuration
- VLAN configuration
- Access Port configuration

Configure SafeConnect RADIUS Server and Access Profile

```
}
access {
   radius-server {
       10.10.40.5 {
            port 1812;
            accounting-port 1813;
            dynamic-request-port 3799;
            secret "XXXXX";
     }
        }
 profile SC-RADIUS {
        accounting-order radius;
        authentication-order radius;
        radius {
            authentication-server 10.10.40.5;
            accounting-server 10.10.40.5;
            }
        }
        accounting {
            order radius;
            accounting-stop-on-failure;
            accounting-stop-on-access-deny;
            coa-immediate-update;
            address-change-immediate-update;
            update-interval 10;
        }
    }
}
```

Configure Dot1X protocol

```
protocols {
    dot1x {
        authenticator {
            authentication-profile-name SC-RADIUS;
            interface {
                ge-0/0/2.0 {
                    supplicant multiple;
                    mac-radius {
                        restrict;
                    }
                }
            }
        }
    }
}
```

Configure VLANs

Note – it is assumed the remainder of the VLAN configurations are in place for routing, etc.

```
vlans {
    employee-vlan {
        vlan-id 10;
    }
     guest-vlan {
        vlan-id 20;
    }
     quarantine-vlan {
        vlan-id 30;
    }
     Safeconnect-enforcer-vlan {
        vlan-id 40;
    }

}
```

Configure Access Port

```
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
```

Configuring the EX/QFX/SRX Layer 3 Quarantine VLAN Redirect

On EX for port authentication, you must configure the following.

- Routing Instance
- Firewall Filter
- Apply Filter to Quarantine VLAN Layer 3 Interface

Configure Routing Instance

```
routing-instances {
    TEST-VR {
        instance-type virtual-router;
    }
    quarantine-table {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.10.40.5;
            }
        }
    }
}
```

Configure Firewall Filter for Redirect

```
firewall {
    filter REDIRECT {
        term NO_REDIRECT {
            from {
                destination-port [ 67 53 ];
            }
            then accept;
        }
        term REDIRECT_ALL {
            then {
                routing-instance quarantine-table;
            }
        }
    }
}
```

Apply Filter to Quarantine VLAN Layer 3 Interface

```
interfaces {
    ge-0/0/3 {
        vlan-tagging;
        unit 30 {
            description "Quarantine VLAN";
            vlan-id 30;
            family inet {
                filter {
                    input REDIRECT;
                }
                address 10.10.30.1/24;
            }
        unit 40 {
            description "SafeConnect Enforcer";
            vlan-id 40;
            family inet {
                address 10.10.40.1/24;

        }
    }
}
```

This completes the configuration required on the Juniper wired network infrastructure. The next steps will be to configure the SafeConnect RADIUS Server.

SafeConnect RADIUS Server Configuration

Refer to the SafeConnect RADIUS Server Configuration Guide to complete the integration with SafeConnect. Login to the SafeConnect management interface at https://portal.myweblogon.com:8443/manage. If this does not work, you can replace 'portal.myweblogon.com' with the IP address of your SafeConnect appliance. In a SafeConnect cluster environment, this must be the manager node. If a branded URL is configured, replace 'portal.myweblogon.com' with the branded URL chosen. Once Logged in, choose Configuration Manger > Enforcement Setup > RADIUS Configuration > RADIUS Configuration to complete the configuration for the instructions in the guide.