

# Configuring InterVLAN Routing with a Layer 3 Switch and pfSense

Posted on [August 19, 2019](#) by [Greig Mitchell](#) — [24 Comments ↓](#)

Recently I was tasked with deploying a Layer 3 managed network switch alongside an existing pfSense firewall appliance for a relatively small network.

As a quick bit of a background the network consisted of around 10 VLANs which were all being terminated and routed on a pfSense firewall connected to an existing Layer 2 switch via a single 1Gbps trunk link (Router on a stick). There was then a requirement to swap out the existing Layer 2 switch and put a Layer 3 switch in its place to handle interVLAN routing between the VLANs to save resources on the firewall whilst increasing performance.

So to start this off I began documenting and making a high-level list of the steps:

1. Remove the VLAN interfaces off PfSense
2. Create the SVIs for each VLAN interface on the Layer 3 switch
3. Enable IP Routing on the Layer 3 switch
4. Configure the uplink port to pfSense LAN interface as a Routed Port
5. Add static routes on pfSense back to the Layer 3 switch for each network
6. Add firewall/NAT rules on pfSense for each network
7. Add a default route on Layer 3 switch to PfSense

**Note:** I'm not going to go into detail on removing interfaces on PfSense or creating VLANs, I already assume you are familiar with this. In this example the switch configuration is based off a Cisco Catalyst 3560X, the steps may be different for other switch vendors. For Cisco you will need an IOS image and/or license which enables routing features.

First is to create the SVIs for each VLAN interface on Layer 3 switch:

```
Switch(config)# interface Vlan3
Switch(config-if)# ip address 172.16.3.1 255.255.255.0
```

```
Switch(config)# interface Vlan4
Switch(config-if)# ip address 172.16.4.1 255.255.255.0
```

Then we enable IP Routing globally on the switch:

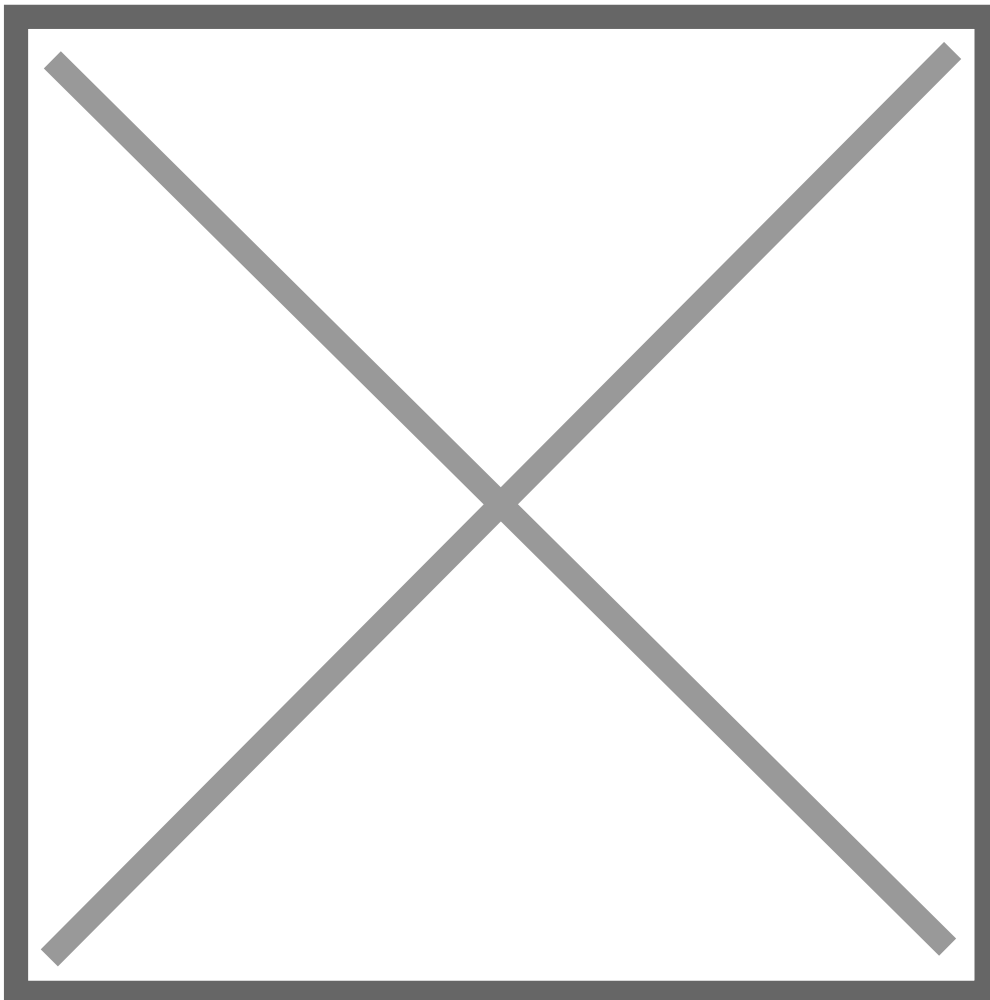
```
Switch(config)# ip routing
```

The next stage is to configure the physical uplink going from the switch to the pfSense LAN interface. This can be referred to as a “Transit” network for traffic leaving the Layer 3 switch i.e. to the Internet. There are a few ways this can be achieved, either by creating a dedicated VLAN interface with an SVI or configuring a physical switch port as a Routed Port using the “no switchport” command then giving it a dedicated IP address – I will be using this method but in most cases it is normally recommended to use a small subnet mask such as a /30 for the transit network.

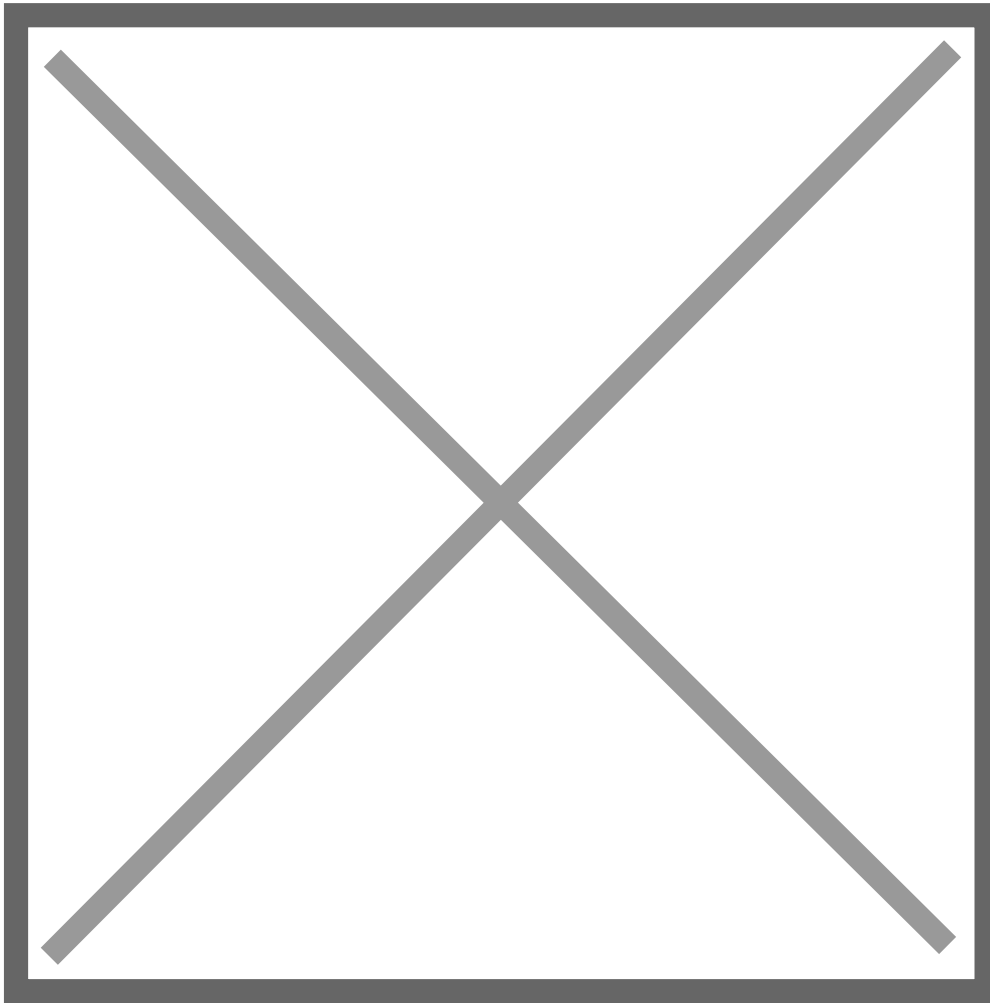
In this example 172.16.1.1 will be the routed port IP address and 172.16.1.2 will be the pfSense LAN interface address.

```
Switch(config)# interface GigabitEthernet1/4  
Switch(config-if)# description Routed Port to pfSense LAN Interface  
Switch(config-if)# no switchport  
Switch(config-if)# ip address 172.16.1.1 255.255.255.252
```

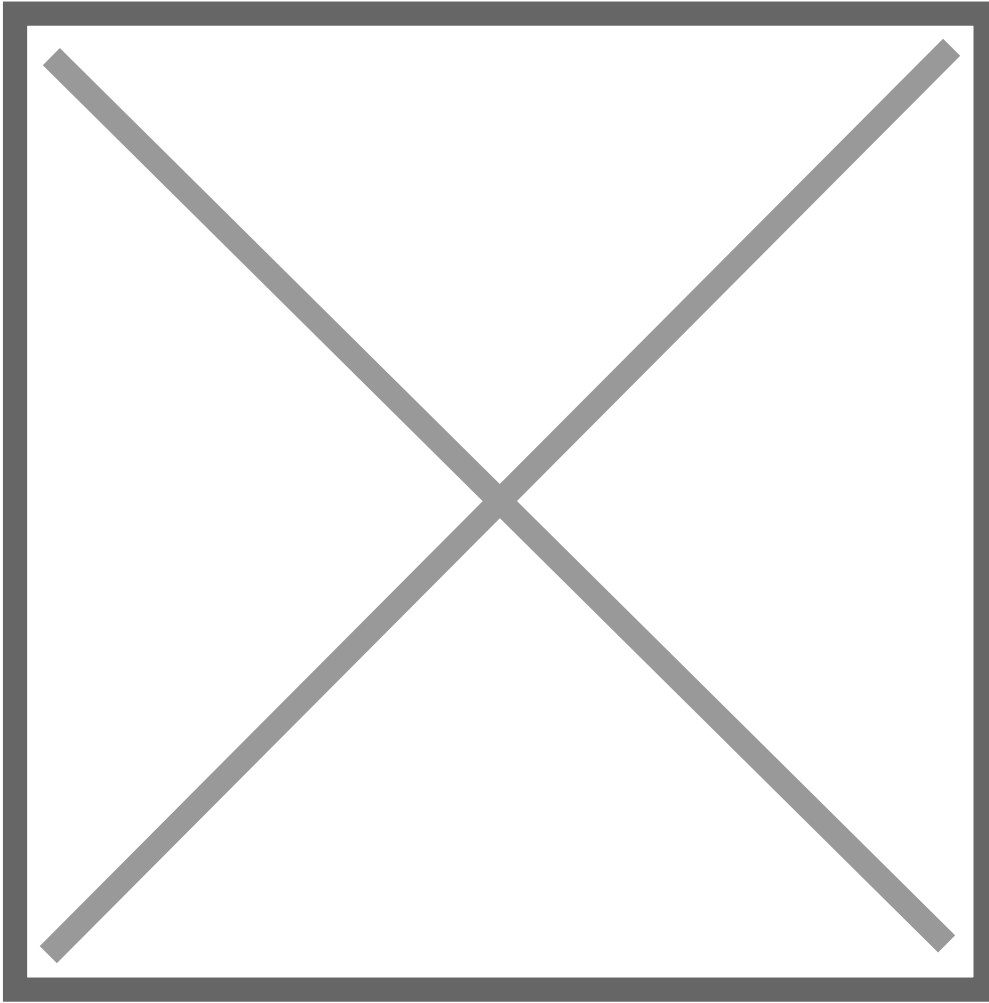
For pfSense to know about the networks we need add static routes back to Layer 3 switch. First to go System > Routing > Gateways and click “Add” and enter the IP address of the Layer 3 switch routed port.



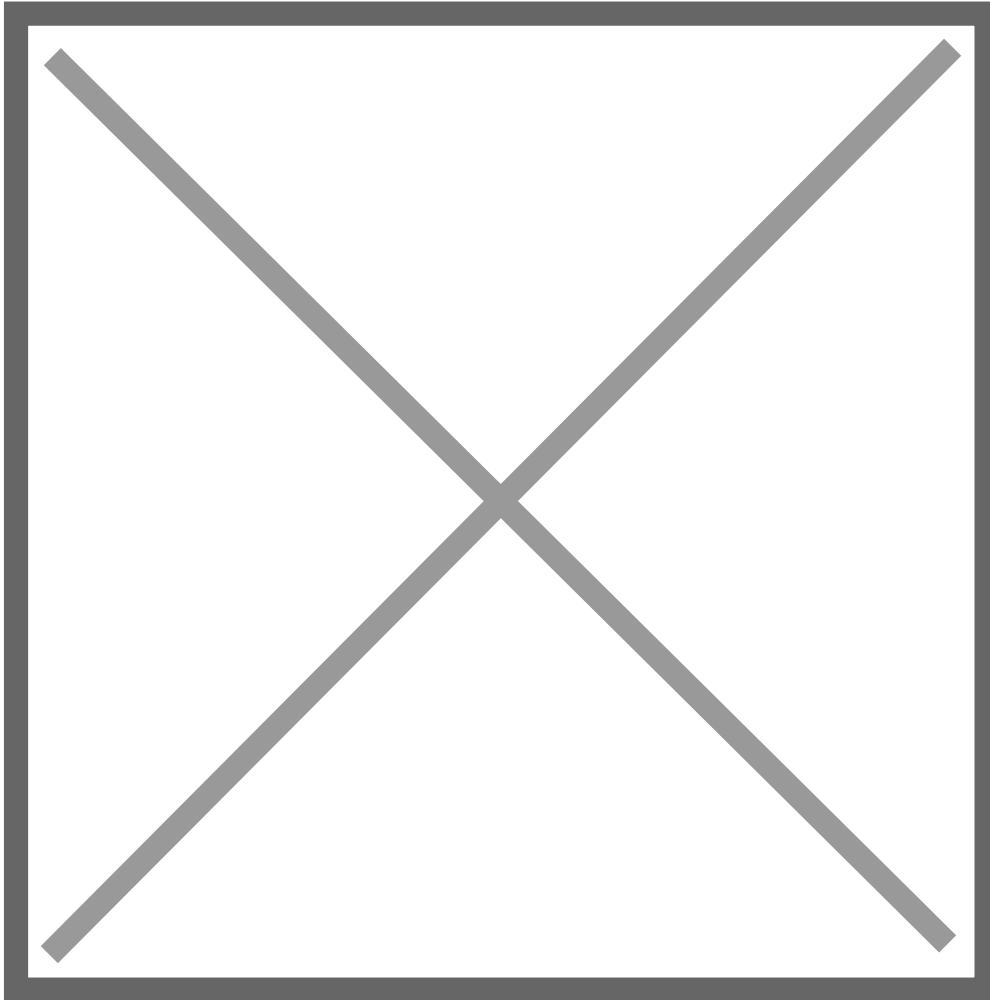
Under System > Routing > Static Routes click “Add” and add each of the networks for the various VLANs on the Layer 3 switch, selecting the Layer 3 Switch as the gateway.



For hosts in each of the various VLANs to get out to the internet Firewall and Outbound NAT rules must be created for each network on pfSense. Firstly, navigate to Firewall > NAT > Outbound and check the existing rules - if using automatic outbound NAT pfSense will have already added in the required rules for the networks otherwise these will need to be added manually.



Next navigate to Firewall > Rules > LAN and add pass rules for the various networks.



At this point pfSense is now aware of each of the networks on the Layer 3 switch and is configured to route their traffic outbound to the Internet. The last and final stage is to add a default route for all traffic not destined for the Layer 3 switch to pfSense - this will provide each of the VLANs with Internet access.

To do this login to the Layer 3 Switch and enter the following command:

```
Switch(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

Now InterVLAN routing should be working successfully on the Layer 3 switch and the hosts on each of those networks should have Internet access through the pfSense firewall.

With this setup there are couple of things to keep in mind...

- Restricting traffic between each of the VLANs must be performed by creating ACLs (Access Control Lists) on the Layer 3 switch as opposed to using Firewall rules on pfSense - this can be less flexible and user friendly.
- Adding additional VLAN SVIs on the Layer 3 switch will require adding the appropriate static routes and Firewall/NAT rules to pfSense for those networks to enable Internet access if needed.

I hope this helps anyone looking to configure InterVLAN routing with a Layer 3 switch and pfSense.

---

Revision #1

Created 2023-11-11 02:17:19 UTC by Ryan

Updated 2025-02-12 01:12:27 UTC by Ryan