# Virtual Networks
## and Secure Network Design

Hannah Pearson and Dillon Harris

August 12, 2017
Version 1.1

University of Idaho

CS 539: Applied Security Concepts

**Executive Summary**

This tutorial will imparts knowledge regarding creation of virtual networks using VyOS. Specifically, we teach readers about the steps required to establish a network with three Ethernet interfaces, and which will have three zones associated with each interface. We hope that by the end of this tutorial, the readers will see a benefit of creating virtual networks through utilization of virtual routers such as VyOS or Pfsense.

# Contents

## 1 Prerequisites: Knowledge >

Expected preparation:

- Understanding of the OSI model;
- Basic knowledge of IPv4 protocol;
- Experience with Linux systems and command line;
- Curiosity and motivation to learn.

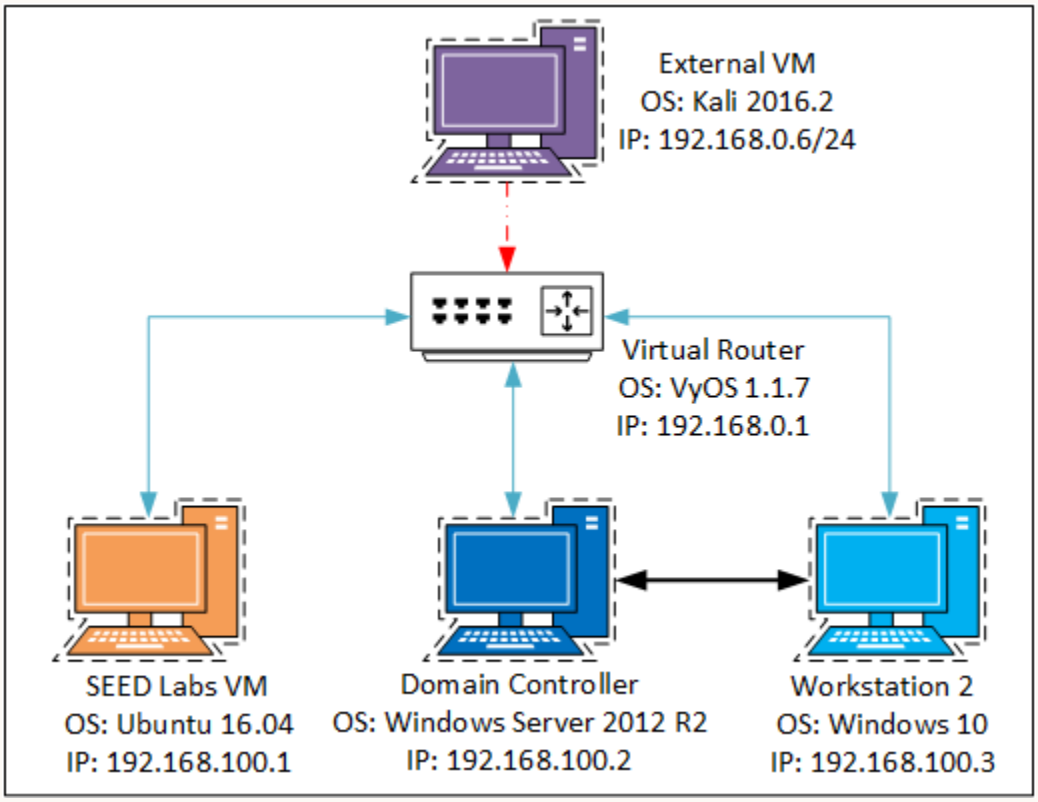
## 2 Prerequisites: VM Infrastructure <>

Using a virtualization software, set up the following VMs; all in a unique port group.

- VyOS 1.1.7 with three network adapters;
- Windows 2012 R2 Server;
- Windows 10 Workstation;
- Ubuntu Web Server;
- Kali Workstation.

Each group of VMs should be created on a distinct port group. In other words - ideally, each reader would have their own isolated network, which should be separated from other students' networks.

# 3 Network Layout



## 4 Router Overview <>

Proper network configuration is the first line of defense.
Open source routers for configuring small to mid-size networks:

- VyOS - Open source network OS.
- Pfsense - Open source firewall/router.

Both VyOS and pfSense are powerful and flexible enough to configure a secure network that accomodates a given company's unique requirements.

Properly configuring a network is the first line of defense against malicious intruders and can be accomplished by configuring a router. Two commonly used open source routers for small to mid-size networks are VyOS, which is the open source version of Vyatta, and pfSense. VyOS offers only a command line, while pfSense features both a command line and a graphical interface.

## 5 VyOS Features <>

1. VLANs;
2. Static and Dynamic routing;
3. Firewall;
4. VPN;
5. NAT;
6. DHCP.

1. VLANs - A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
2. Static/Dynamic Routing - BGP for IPv4 and IPv6.
3. Firewall - Firewall rulesets for IPv4 and IPv6 traffic you can assign to interfaces, zone-based firewall, address/network/port groups for IPv4 firewalls.
4. VPN - Site-to-site IPsec for IPv4 and IPv6, L2TP/IPsec server, PPTP server, OpenVPN for site-to-site and remote access.
5. NAT - Source NAT, port forwards, one to one, one to many, and many to many translations.
6. DHCP - DHCP and DHCPv6 server and relay.

## 6 Questions

1. What is a reason you would want to setup VLANs in a network?
2. What is the benefit of setting up a VPN?
3. What is a DMZ and why would you want to use it?
4. What does DHCP stand for?

1. VLAN's allow a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together.
2. A VPN (Virtual Private Network) is a way of adding an extra level of privacy to your online activity. VPNs encrypt your device's internet connection, allowing you to surf the web privately.
3. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.
4. Dynamic Host Configuration Protocol

## 7 Network Routing <>

1. Process of selecting a path for network traffic;
2. Packet forwarding;
3. Routing tables.

1. Routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms.
2. Packet forwarding is the transit of logically addressed network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches.
3. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations.

## 8 Introduction to VyOS <>

- Linux-based network OS;
- Free and open source;
- Network routing, firewall, and VPN;
- Started in 2013 from GPL portions of Vyatta Core 6.6R1;
- Created after community edition of Vyatta was discontinued.

VyOS is based on Debian GNU/Linux and is free and open source [2]. It was forked from parts of Vyatta, another very similar network operating system, which up until 2013 had a free community edition. When this was discontinued, VyOS was developed from Vyatta source liscenced under GPL [2].

## 9 VyOS Basics <>

- VyOS has two modes, configuration and operational;
- Configuration (prompt ends in #) for changing rules;
- Operational (prompt ends in $) for showing status;
- Enter configuration mode by typing `conf`;
- Exit configuration mode by typing `exit`;
- Save changes: `commit && save; exit`.

There are two different types of users in VyOS, admin and operator [2]. The operator user can only use operational mode, meaning they can only view existing rules and monitor the network; Operator users cannot modify the configuration. Admin users, on the other hand, have full privileges and can change the network configuration [2].

In accordance with the principle of least privilege, a user should have the privileges they need to do their job and no greater. This means that ordinary day-to-day network monitoring can (and should) be done using an operator account. For setting up and configuring a network, like we are doing today, an administrator account is necessary.

## 10 Task 1: Replace Default User Account <>

Task 1: Create a new admin user. Log out and log back in using the new user. Remove the default VyOS user (vyos).

Users can be added using the following commands [2]:

```
set system login user jsmith full-name "Johan Smith"
set system login user jsmith authentication plaintext-password
                                                        password1
set system login user jsmith level admin
```

Existing users can be viewed in configuration mode using the command [2]:

```
show system login
```

In operational mode, it is only possible to see a list of users and not the full contents of the configuration file, by using:

```
show system login users
```

To delete a user, type the following in configuration mode:

```
delete system login user [name of user to be deleted]
```

Be sure to commit changes before exiting.

## 11 VyOS Basic Commands <>

- IP Configuration - vyos@vyos$ show interfaces
- Routing - vyos@vyos$ show ip route
- Show Configuration - vyos@vyos$ show
- Show log - vyos@vyos$ monitor log, show log tail
- Configure Interfaces - vyos@vyos# set interfaces

VyOS has the great feature of hitting tab for auto complete. This will come in handy for the tasks in this presentation. When in doubt hit tab and see the command options you can use.

## 12 Introduction to Zones <>

- Useful for large or complex networks;
- Usual non-zone based approach is to specify inbound/outbound rules per interface;
- Zones can be used to combine multiple interfaces;
- Firewall rules can be set for communication between zones;
- Communication between zones is blocked by default.

Once zones have been created, they can be used to design and implement firewall rules [3]. For example:

```
set zone-policy zone INSIDE from OUTSIDE firewall name INSIDE-OUT
```

## 13 Discussion: Purpose and Application of Zones<>

- Why are zones useful? They seem like a pain...
- Answer: Well. Consider the scenario described below, drawn today for your convenience on the whiteboard.
- Discuss: How would you set up this network? What other scenarios can you envision in which zone-based firewalls might be of value?
- How is the application of firewall rules to zones similar to the application of group policy to a domain? How is it different? Is this a helpful mental analogy?

We don't have a large network set up, but you might imagine a scenario in which a large company wants to apply the principle of least privilege and limit access to specific resources to only those who need it.

For example, your company's large software development team, which is distributed across three different network interfaces, has a server they use as a software repository and the marketing team, which uses two network interfaces, has a separate server they use for storing financial records.

Both groups have access to yet another the company's internal website and employee directory as well as the external public website located on one DMZ. Only the marketing group has access to a second external website, located on DMZ_2, which is used by current clients of the software company.

## 14 Questions <>

1. What is a LAN?
2. What is a WAN?
3. What are couple of differences between the two?

1. A LAN is a local area network, usually comprised of computers, printers, and etc in a local area like a building or office.
2. A WAN is a wide area network that is made up of multiple LANs.
3. A LAN will usually have a much higher bandwidth, then a WAN. People can setup their own LAN, but they don't usually setup WANs since a typical WAN connects LANs that could be 100's, or 1000's of miles apart.

## 15 Task 1: Network Design <>

Design a network topology that separates the following hosts and servers into appropriate logical zones using the VyOS 1.1.7 Router that has been provided:

- Domain Controller - Windows 2012 Server;
- Workstation - Windows 10;
- Web Server - Ubuntu 16.04 (DMZ);
- Untrusted External Entity - Kali 2.0.

This task is a preliminary task to the technical process of actually setting up the network and can be done on paper. Consider what machines need to be accessible to whom, and use this information to divide the virtual machines into logical zones.

In an actual network, this logical separation would be mapped to actual physical separation. For the purposes of this lab, it suffices to envision the physical separation while accepting that it is not practical to actually implement.

## 16 Challenge 1: Network Setup <>

Implement the zoned network you designed earlier using subnets.

- Hint: there should be three subnets – use the three ethernet interfaces on the VyOS router. (Google is your friend!)

Note that in our configuration, due to practical constraints, these ethernet interfaces all correspond to the same VLAN (specifically, in VMWare, the same port group). In an actual network, the zones should be physically separated at this level, so try to envision this separation in your mental model of the network.

## 17 NAT Background <>

Question 1: How many possible IPv4 addresses exist?

Contrast this number with the estimated number of devices that will be connected to the Internet this year:
20 billion [1].

How is this possible? How would you solve this problem? Anyone know how this problem was solved?

See appendix for answer to Question 1.

One step to the solution was to abolish network classes (classes A, B, and C, representing networks containing 16,777,216 addresses, 65,536 addresses, and 256 addresses respectively) in favor of using more specific subnet masks, so networks that were too large for class C subnets but not large enough to use an entire class B subnet were able to free up IP addresses they did not need without an excessive strain on routers and routing tables which would otherwise have to manage mappings between multiple smaller class C networks [4].

The big breakthrough, though, was NAT. NAT, or Network Address Translation, enables one single IP address to represent an entire subnet. The following address ranges are specifically reserved for internal subnets: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 [4]. Also, by convention, the router is assigned the address ending in .1, such as 192.168.0.1 or 10.0.0.1 for example.

## 18 NAT Basics <>

- Two types of NAT;
- Source NAT (sometimes simply referred to as NAT);
- Source NAT bought time for IPv4 address problem;
- Destination NAT (Port Forward);
- Example use of port forwarding: setting up a minecraft server to use with friends on your home network.

Source NAT (also known as Port Address Translation or NAT Overload) allows an entire subnet of machines to communicate with the internet from one IP address [2]. It was invented as a solution to the dwindling number of available IPv4 addresses in relation to the number of internet connected devices several decades ago [4]. To set up a source NAT rule, the following information is required:

- Internal IP address to translate from;
- Outgoing interface through which the address is to be translated;
- External IP address to translate to.

Destination NAT, on the other hand, is used to direct *external* traffic to a specific *internal* host via a port behind a firewall. Note that setting up a Destination NAT rule requires the following things [2]:

- Interface of incoming traffic;
- Protocol and destination port;
- Internal address to forward traffic to;

## 19 Challenge 2: Source NAT Configuration <>

Challenge 1: Configure source NAT rules for both zones in your internal network.

For this task you should map "internal IP addresses" (addresses of hosts belonging to the private zone subnet) to a the external facing gateway IP address, so that your boss, who is using the Windows 10 workstation, can access the internet.

## 20 NAT Question <>

Why did we use the masquerade translation address in our NAT rules?

IP Masquerade allows other "internal" computers/machines to reach the Internet through the outward-facing gateway address.

## 21 Conclusion <

- Networking is a field in computing that everyone should be familiar with;
- VyOS is a very robust and strong open source virtual router for small and medium sized networks.

# 22 Appendix: Answers, VM information, and Changelog

## Tutorial Answers

### Task 1: Network Design and Introduction to Zones

Design a network with three zones: a private zone, for the DC and Windows 10 workstation; a DMZ, for the Ubuntu web server; and an external zone, for the Kali machine.

### Task 2: Network Implementation and Zone Configuration

Login to VyOS (user:vyos, pass:vyos) and type the following commands:

1. vyos@vyos$ `conf` or `configure`
2. vyos@vyos# `set system gateway-address 192.168.0.1`
3. vyos@vyos# `set interfaces ethernet eth0 address dhcp`
4. vyos@vyos# `set interfaces ethernet eth0 description 'OUTSIDE'`
5. vyos@vyos# `commit && save; exit` (can also type each on a separate line)

Repeat the "set interfaces..." commands for each interface you wish to configure. If you'd like to configure static IP addresses, instead of typing dhcp you can specify a subnet. For the gateway address, you can specify whichever address you'd like although the router is, by tradition, always at an address ending in .1.

### Challenge 1: Implementing Network Design

Here is an example of setting up the network design [2]:

```
set int ethernet eth0 address dhcp
set int ethernet eth0 description NAT
set int ethernet eth1 address 192.168.0.1/24
set int ethernet eth1 description PROD
set int ethernet eth2 address 192.168.1.1/24
set int ethernet eth2 description DMZ
commit
save
```

Here, `masquerade` specifies that the source address should be translated to whatever the outgoing address belonging to the gateway is [2].

### Challenge 2: Destination NAT

Here is an exammle of destination NAT configuration and firewall rules [2]:

```
set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 192.168.0.1/24
set nat source rule 10 translation address masquerade
set nat source rule 11 outbound-interface eth0
set nat source rule 11 source address 192.168.1.1/24
set nat source rule 11 translation address masquerade

set zone-policy zone NAT interface eth0
set zone-policy zone PROD interface eth1
set zone-policy zone DMZ interface eth2

set firewall name PROD-NAT default-action drop
set firewall name PROD-NAT rule 1 action accept
set firewall name PROD-NAT rule 1 state established enable
set firewall name PROD-NAT rule 1 state related enable
set firewall name PROD-NAT rule 2 action drop
set firewall name PROD-NAT rule 2 log enable
set firewall name PROD-NAT rule 2 state invalid enable
set firewall name PROD-NAT rule 9999 action drop
set firewall name PROD-NAT rule 9999 log enable
set zone-policy zone NAT from PROD firewall name PROD-NAT
```

**Answers to Questions**

1. There are 4.295 billion IPv4 addresses [4]. Some of these are reserved, making the number of available IPv4 addresses somewhat fewer.

## VM Configuration

List of VMs used in this tutorial:

- VyOS 1.1.7 (Router);
- Windows 10 (Worstation);
- Windows Server 2012 R2 (Domain Controller);
- Kali 2.0 (External, Network Scanning);
- Ubuntu 16.0.4 SEED VM (Web Server).

The VyOS machine should have three network interface cards. For the purposes of this lab and the associated practical constraints inherent in the infrastructure, it is alright if all of all network interfaces are connected to the same port group in VMWare.

## Change Log

| Virtual Networks and Security | | | |
|---|---|---|---|
| Ver. | Date | Authors | Changes |
| v1.0 | Feb. 15th 2017 | Hannah Pearson and Dillon Harris | Created Tutorial |
| v1.1 | Aug. 12th 2017 | Ananth Jillpalli | Standardization (network layout diagram edits, consistency, TeX markup cleaning, and more) |

# References


[1] Brown, Peter. 2017. *20 Billion Connected Internet of Things Devices in 2017, IHS Markit Says*. Electronics 360. Accessed February 23, 2017 from `http://electronics360.globalspec.com/article/8032/20-billion-connected-internet-of-things-devices-in-2017-ihs-markit-says`.

[2] *VyOS User Guide*. Accessed February 17, 2017 from `https://wiki.vyos.net/wiki/User_Guide`.

[3] *A Primer To Zone Based Firewall*. Accessed February 24, 2017 from `https://wiki.vyos.net/wiki/A_primer_to_Zone_Based_Firewall`.

[4] Van Beijnum, Iljitsch. 2014. *With the Americas running out of IPv4, it's official: The Internet is full*. Ars Technica. Accessed February 23, 2017 from `https://wiki.vyos.net/wiki/User_Guide`.