A04 – Multiple Firewalls

15 points
Turn in a Word or PDF document to the D2L Dropbox

Overview

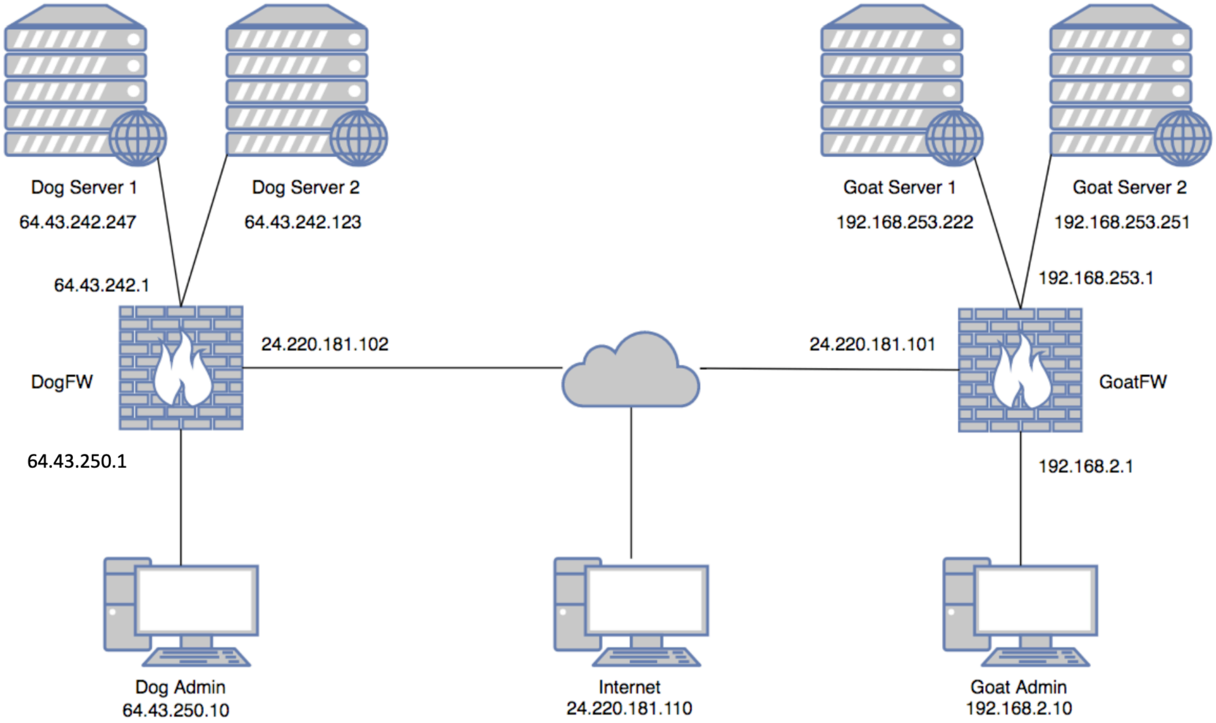
In this lab, you will configure two commercial firewalls, one with NAT and one without NAT.

Credentials:

- Palo Alto
  - admin
  - admin
- Juniper
  - root
  - Password1!

The Network

You have two separate networks in the lab, one called Goat and the other called Dog. Each network has two web servers on the DMZ, and an admin workstation on the LAN. Please note: The machine labeled "Internet" represents a computer on the internet. The IP address or subnet this machine is on does not accurately represent the machines or addresses on entire internet.



Dog (Palo Alto)

The dog network does not use NAT. A license for their firewall is already applied, and the firewall's management interface to be 64.43.250.23

- Configure each interface on Dog's firewall
    - Interface 1 is connected to the LAN, and should be configured with an appropriate IP in the subnet 64.43.250.0/24
    - Interface 2 is connected to the internet and needs to be configured with a static IP of 24.220.181.102/24
    - Interface 3 is connected to Dog's DMZ and needs to be configured with an appropriate IP within the 64.43.242.0/24 subnet
- Server1 at dog, within the DMZ, is on 64.43.242.247
- Server2 at dog, within the DMZ, is on 64.43.242.123

Goat (Juniper)

The Goat company's firewall does not have any interfaces configured. Since this network is using private IPs, is requires NAT.

- Configure each interface on Goat's firewall
    - ge-0/0/0 is on the LAN, and should have an appropriate IP set in the 192.168.2.0/24 subnet
    - ge-0/0/1 is on the DMZ, and should have an appropriate IP set in the 192.168.253.0/24 subnet
    - ge-0/0/2 is on the internet, and needs to be configured with a static IP of 24.220.181.101/24
- Server1 at goat, within the DMZ, is on 192.168.253.222
- Server2 at goat, within the DMZ, is on 192.168.253.251

- With the Goat firewall, you must also configure a route for the 64.43.0.0/16 network with a next hop of 24.220.181.102

Firewall Rules

Each firewall needs to have some rules created to allow certain activity. Be sure the rules you create are the most restrictive as possible and do not let any additional traffic not specified here through the firewall.

Dog's Rules

- Allow the internet to access the website hosted on the dog network’s server1. **Take a screenshot showing that you can get to server 1 from the Internet machine.**
- Only allow the goat network to access the website hosted on the dog network’s server2. **Take a screenshot showing you can access server2 from the goat admin machine.**
- You may need to create additional outbound rules to allow goat to browse the site. **Take a screenshot of all rules on the goat machine, showing you didn’t create any unnecessary rules.**

Goat's Rules

- Create NAT and firewall rules to allow anyone on the internet to access server1 on port 80, but do not allow any machine on the Dog network to access server1. **Take a screenshot showing the internet connected machine browsing the site on port 80.**
- Create NAT and firewall rules to allow only the Dog network to access server2's web server over port 8080. **Take a screenshot showing the Dog admin machine browsing the site on port 8080.**
- You may need to configure appropriate outbound rules from the Dog network to browse the sites. **Take a screenshot showing all of the rules on the dog network, showing you didn't create any unnecessary rules.**

Deliverable

Submit a word or PDF document to the D2L dropbox before the due date containing the **six** screenshots prescribed above - no more, no less. Make sure your screenshots include the title bar of the VM.