A05 – Host Based Firewalls

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

**Overview**

In this lab you will be configuring host-based firewalls on both Linux and Windows machines.

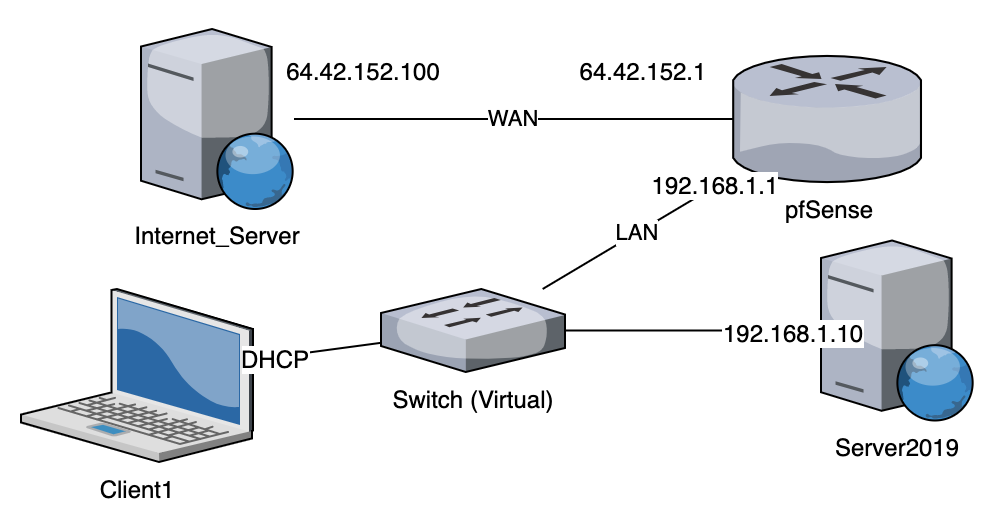
**Credentials:**

* Server2019
  + Administrator
  + Password1!
* Internet\_Server
  + root
  + Password1!
* Client1 and Client2
  + DSU
  + Password1!

**The Network**

The network consists of two client computers (Windows 10) and an internal webserver (Windows Server 2019) as well as a webserver on the “internet” (CentOS 7). The pfsense machine at the core is already configured, you will not need to configure it for this lab.

On the LAN, Servers will be in the range from 192.168.1.2 – 192.168.1.49. Clients will use DHCP and be in the range 192.168.1.50 – 192.168.1.199.



**Your Task**

Your task for this lab is to secure the host-based firewalls on all three systems (Internet\_Server, Client1, Server2019) based on the following requirements:

* From the standpoint of the Internet\_Server, all addresses must be able to access the website hosted on Internet\_Server. This server is HTTP only.
* The Internet\_Server does not need to initiate any outbound connections.
* Only internal clients within the internal DHCP Range need to access the website hosted on Server2019. This server is HTTP only.
  + Create a rule on the Client that only allows firefox.exe outbound over port 80.
* Only the following internal addresses need to be able to access the Client machine over RDP: 192.168.1.2 – 192.168.1.15
  + This can be tested from Server2019

Make sure you do not create other rules on any system that will allow additional traffic through the firewall. All firewalls should be a default deny in all directions.

Note: You may need to include the following rules on the Linux machine to allow related and established connections (stateful)…

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

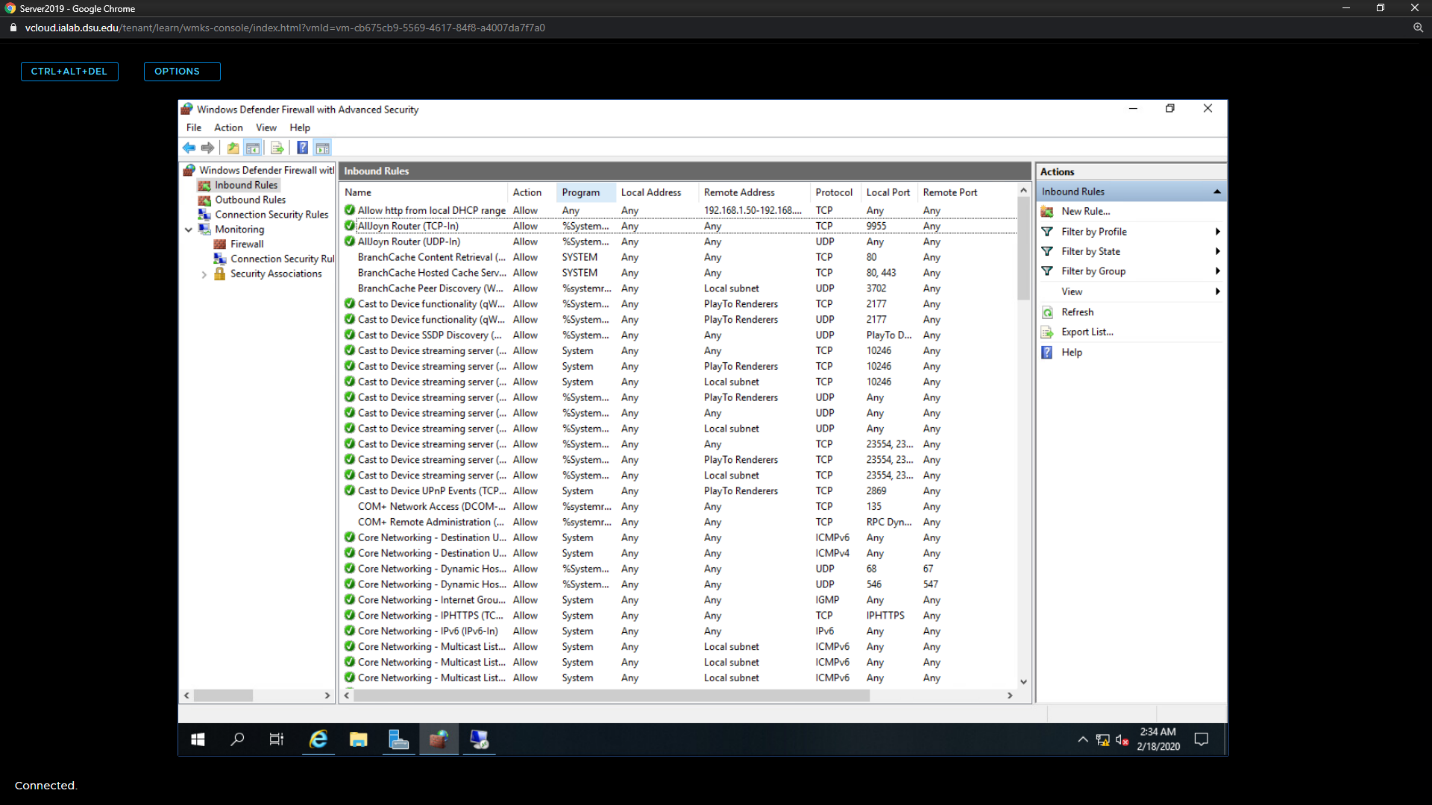
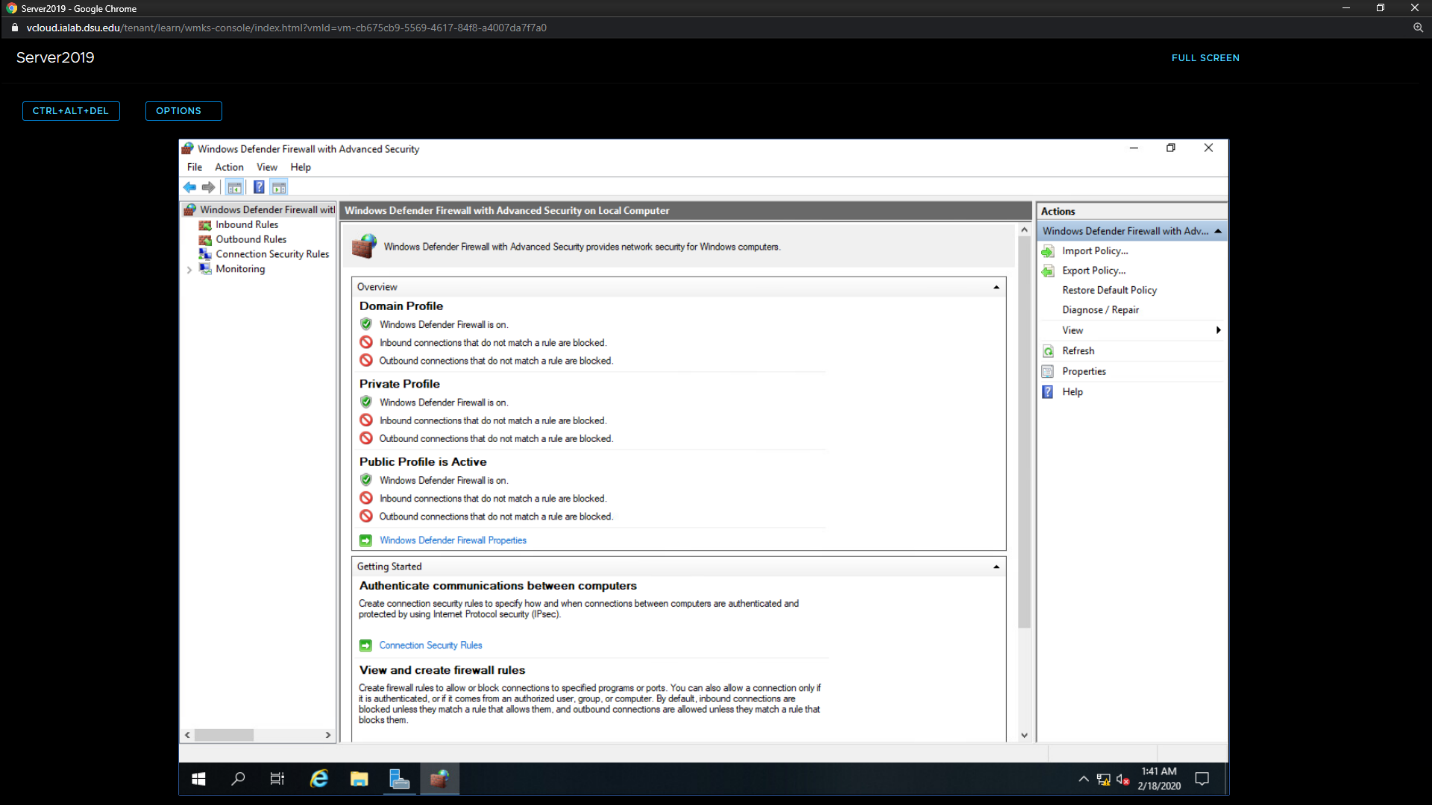
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

**Deliverable**

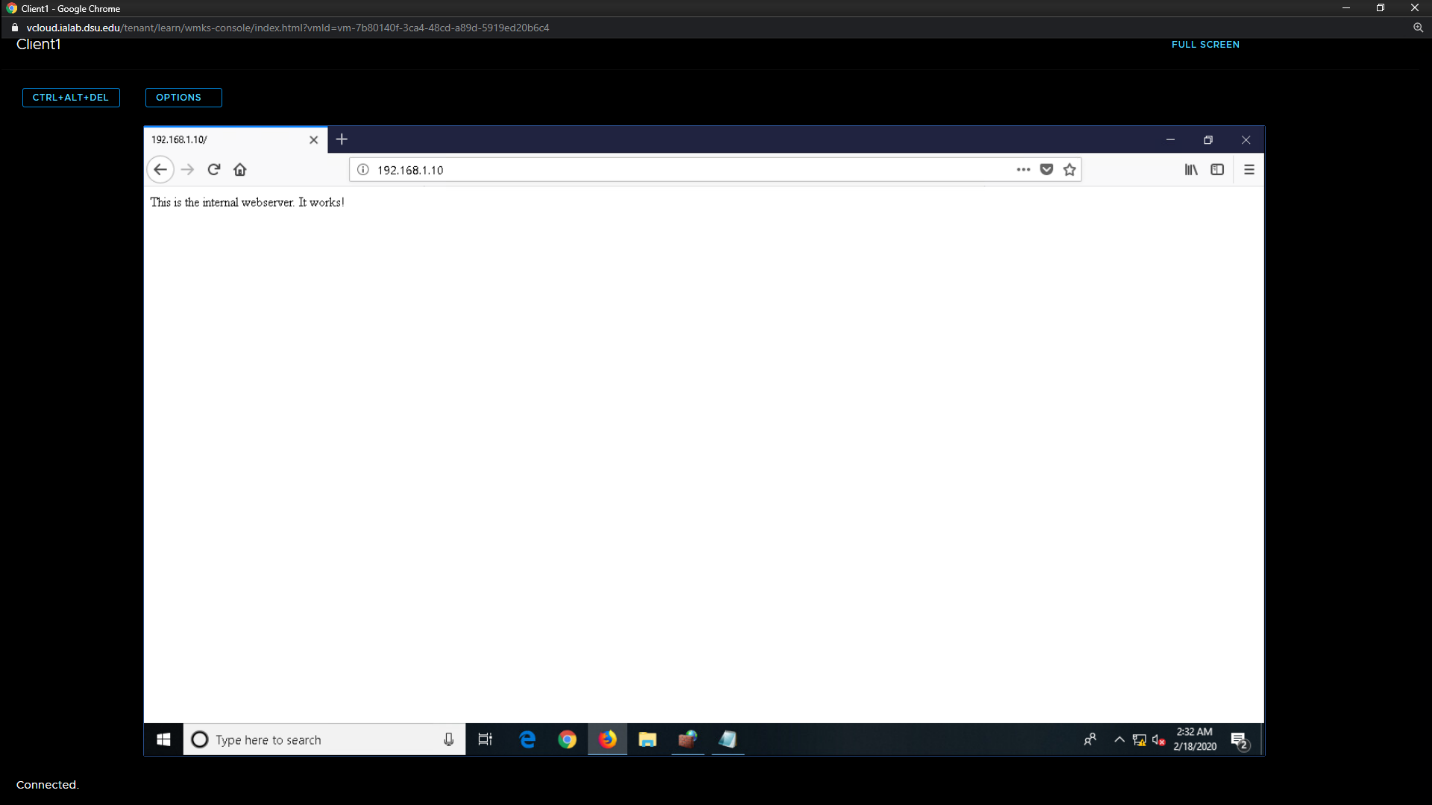
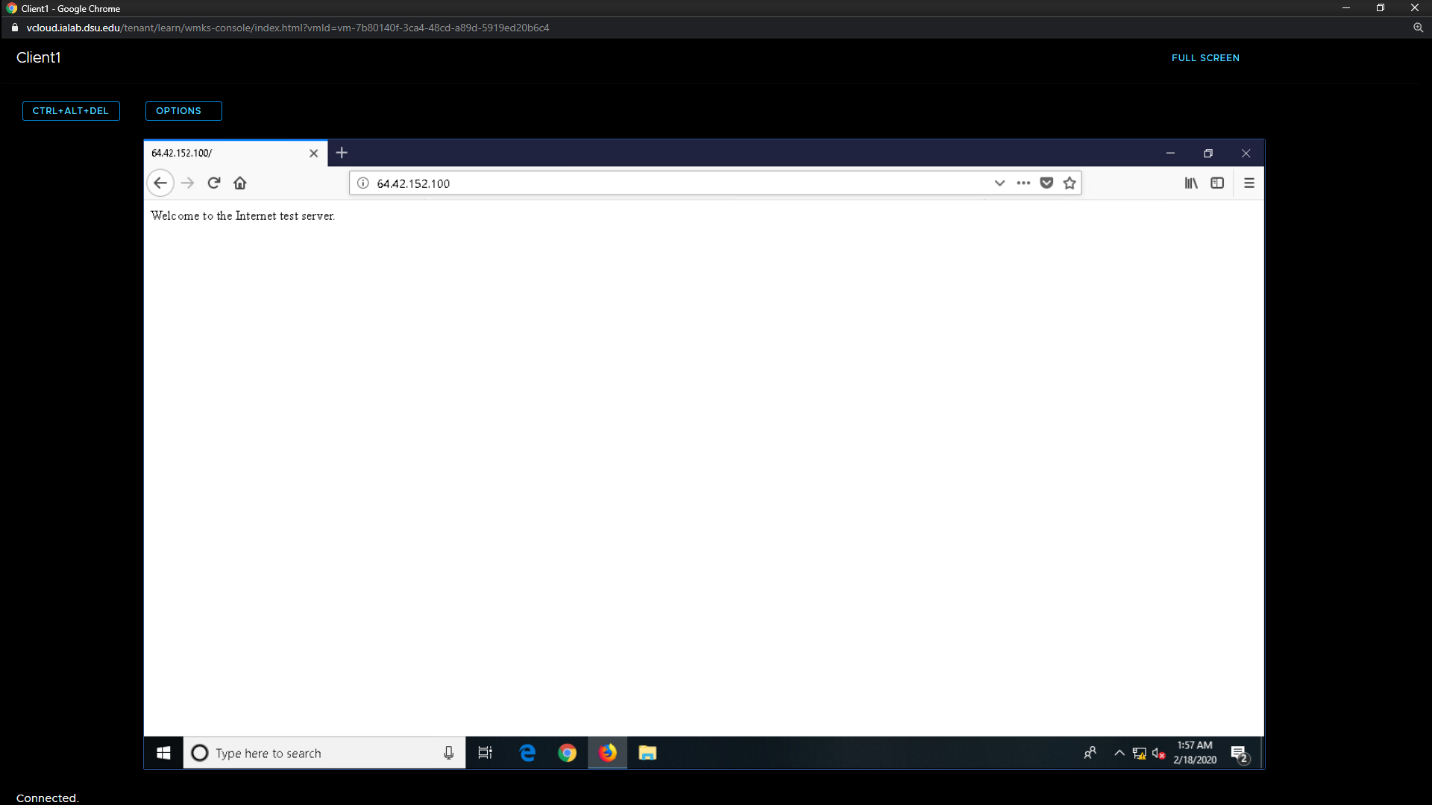
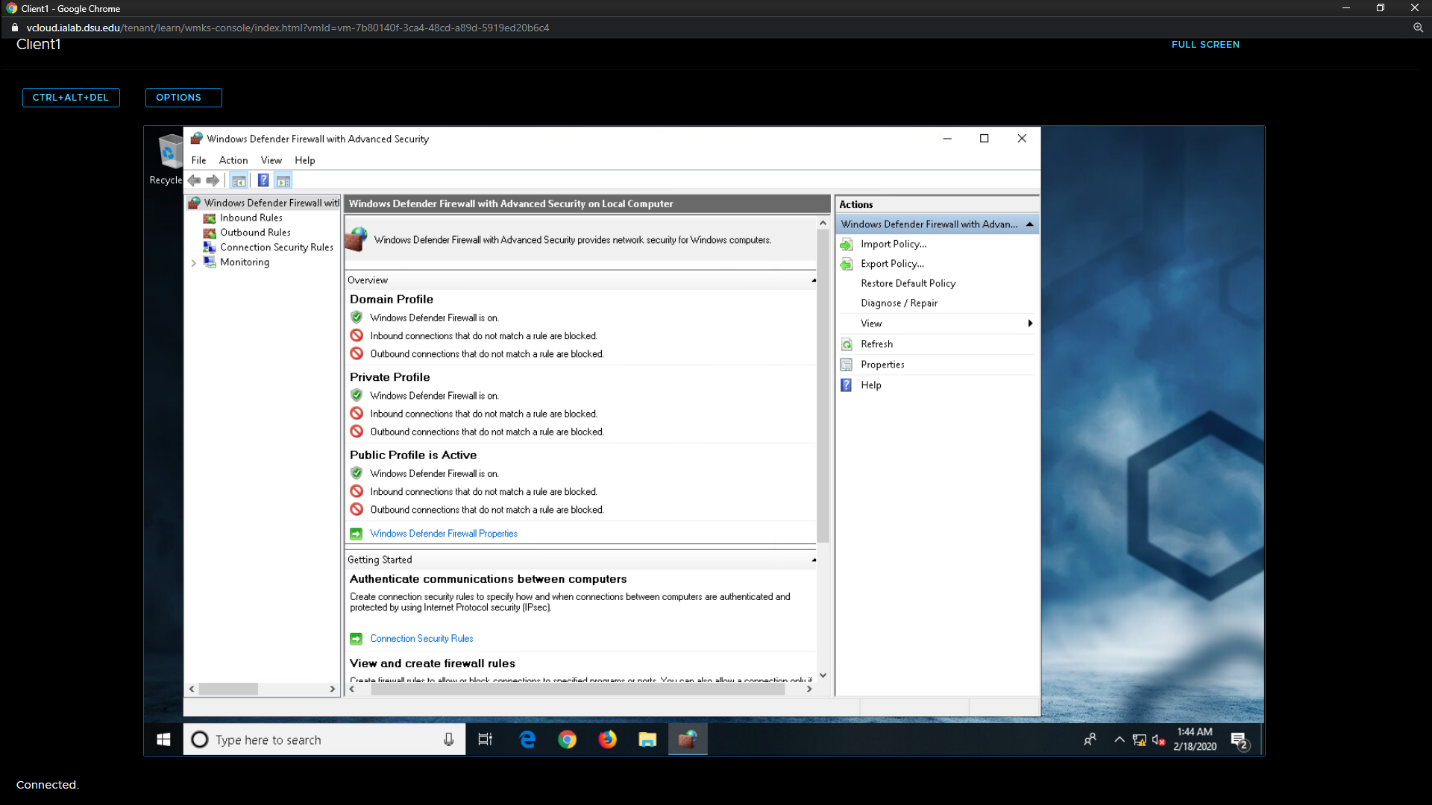
Make sure your screenshots include the title bar of the VM.

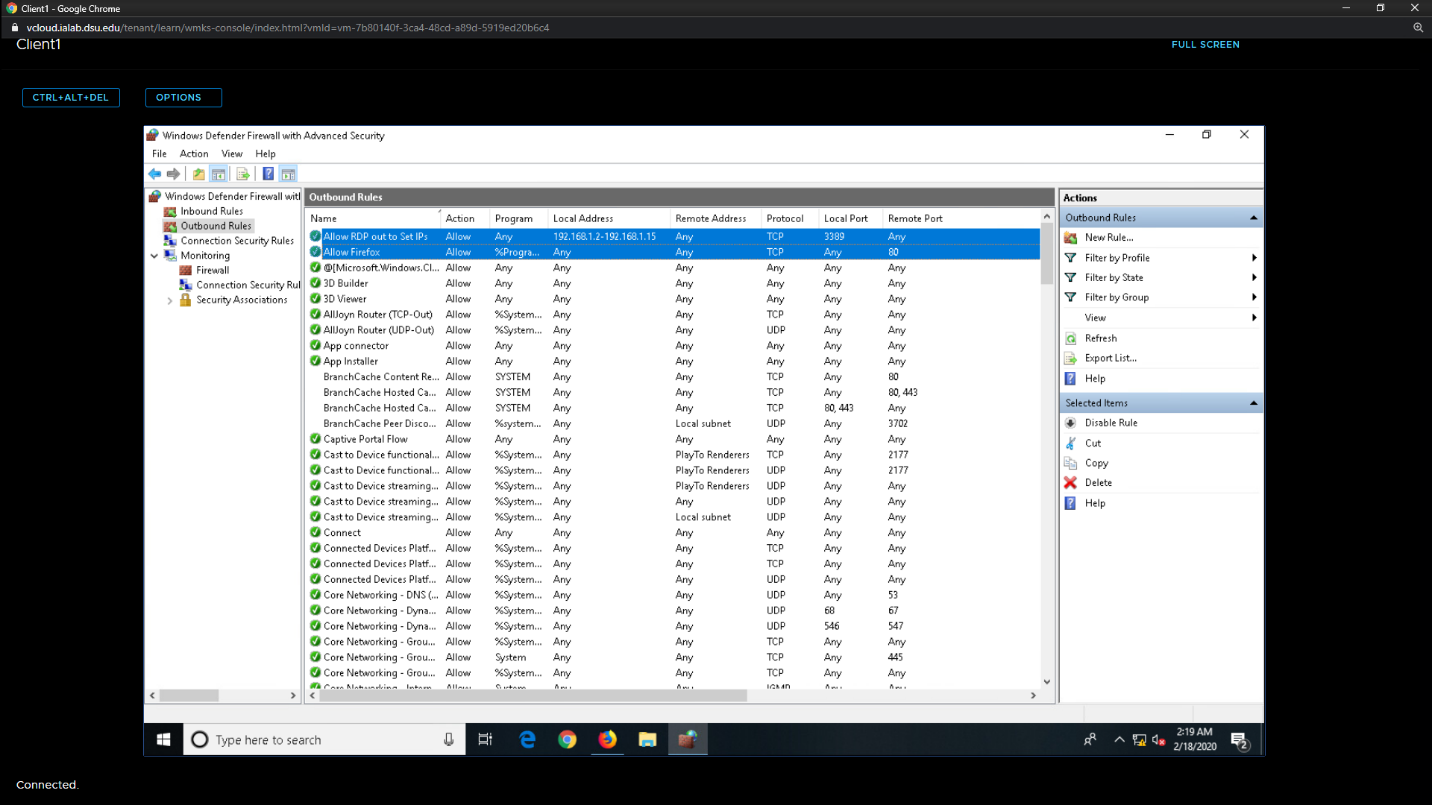
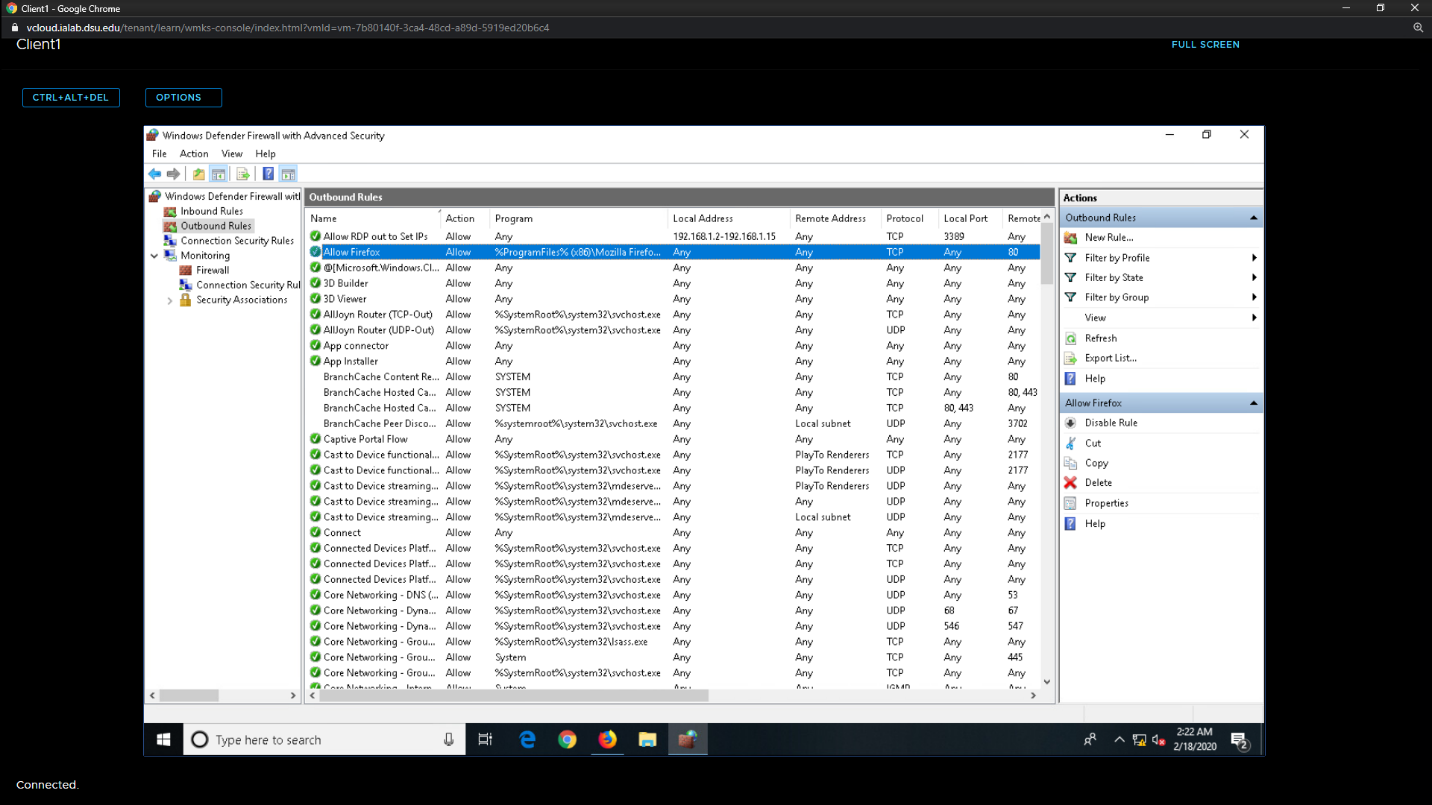
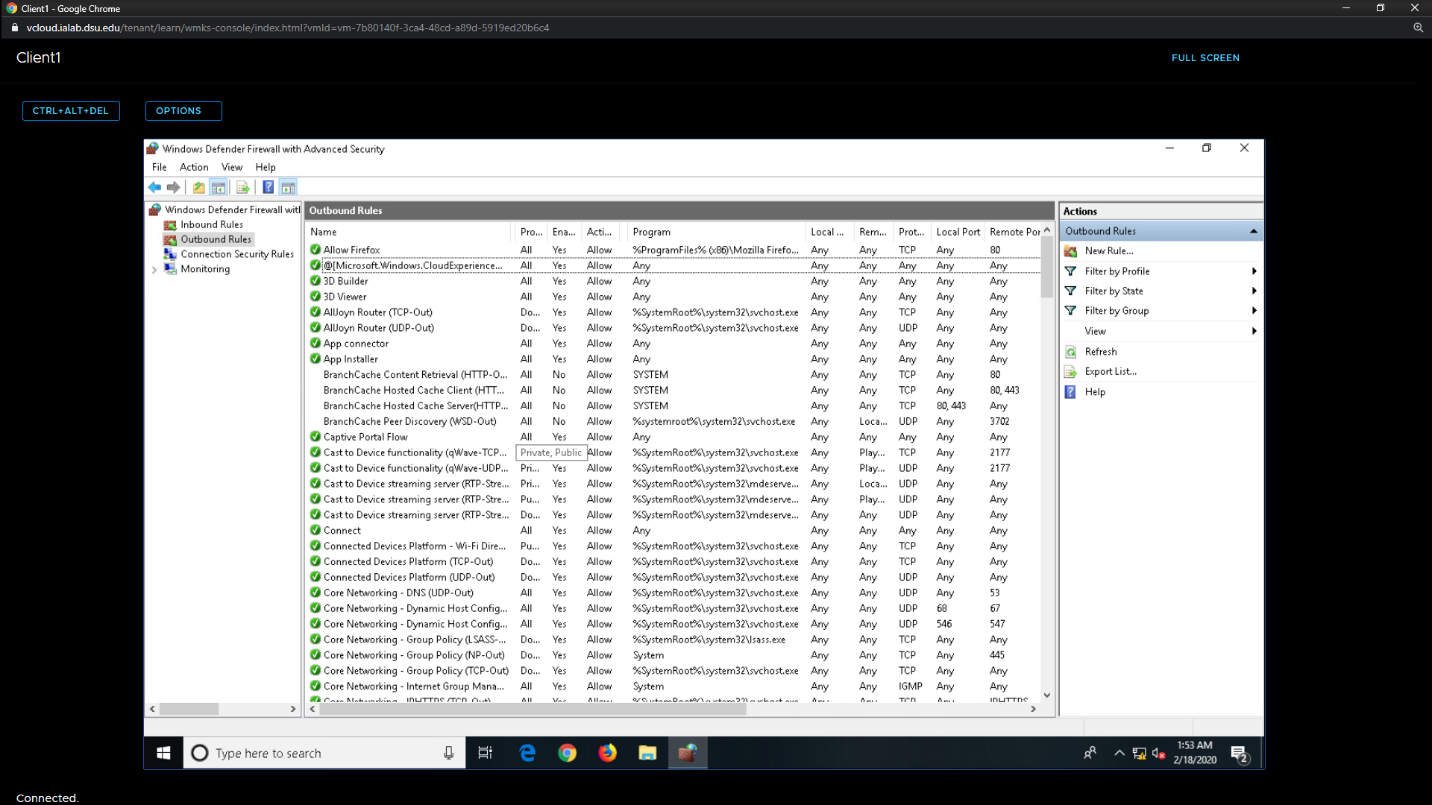
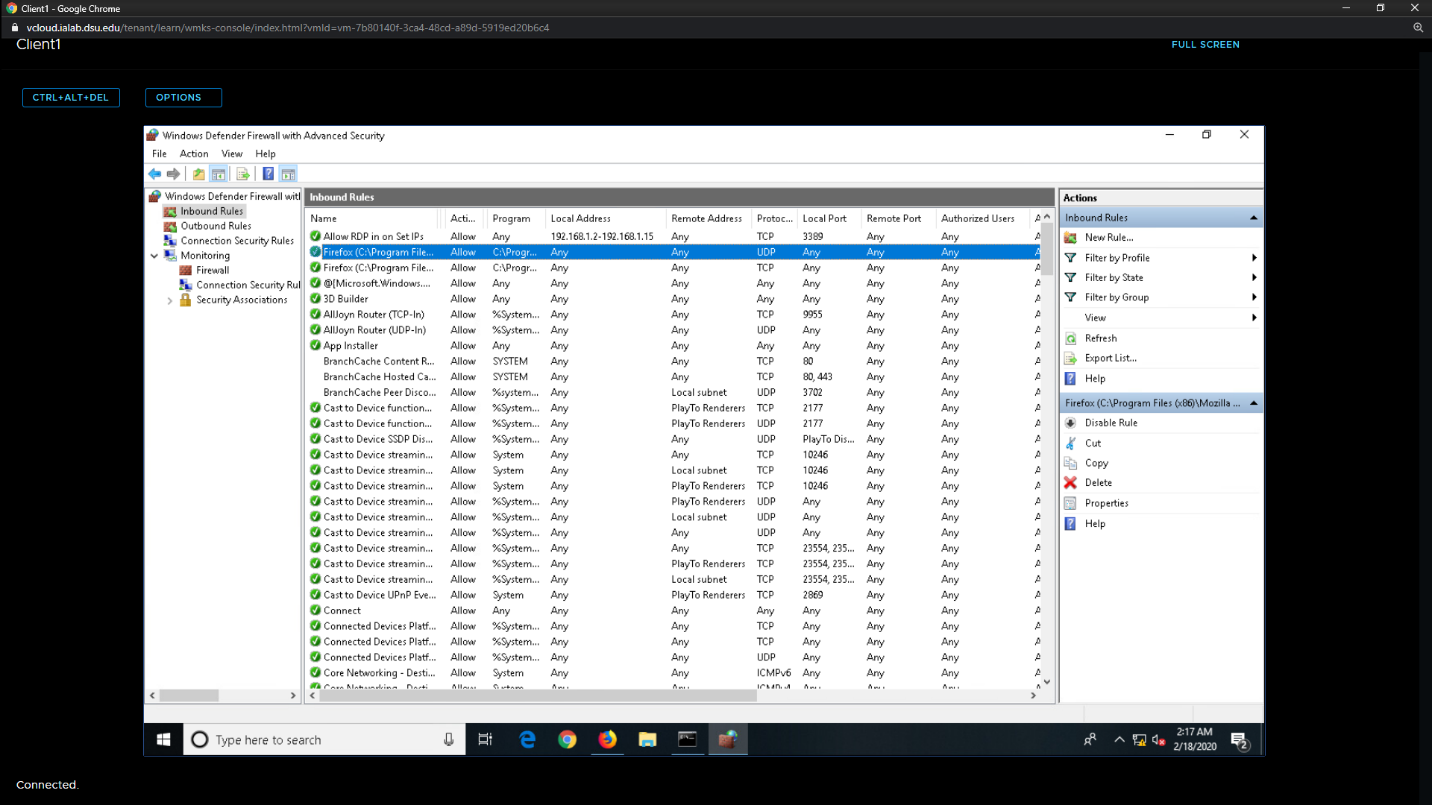
Provide the following screenshots in a Word or PDF document:

* The summary/landing page “Windows Defender Firewall with Advanced Security” on the **TWO** Windows machines
* Any firewall rules you created on the **TWO** Windows machines
  + Screenshots of Windows firewall rules MUST include: Program, Local Address, Remote Address, Protocol, Local Port, Remote Port.
* The output of iptables -L on the Internet\_Machine

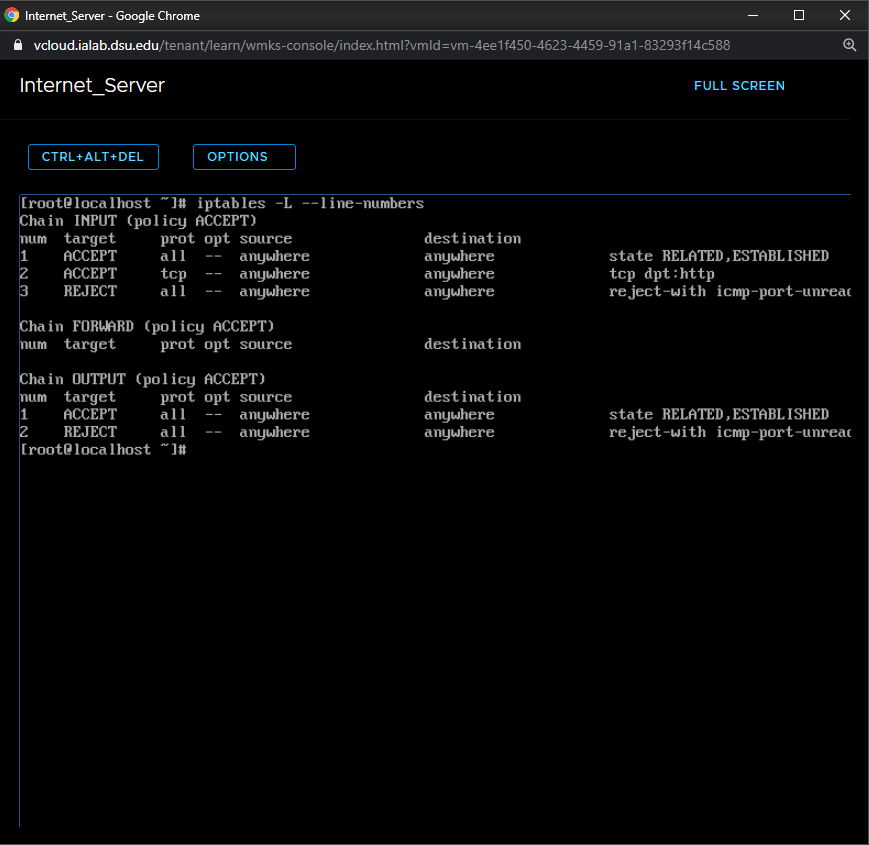
Server\_2019  


Client:

  
Client 1 Cont:  


Internet Server

  
  
I can’t seem to figure out the RDP from server2019 to Client. I am pretty sure I have it set to allow both TCP and UDP 3389 between them. The connection is failing, but the logs have stopped reporting why. I know that the connection is reaching, Client. And I know that client is responding (otherwise the response would show up in the logs). But the connection is failing, and nothing is showing on the logs for the server. I’m wondering if the edge firewall is cutting off the client from responding.