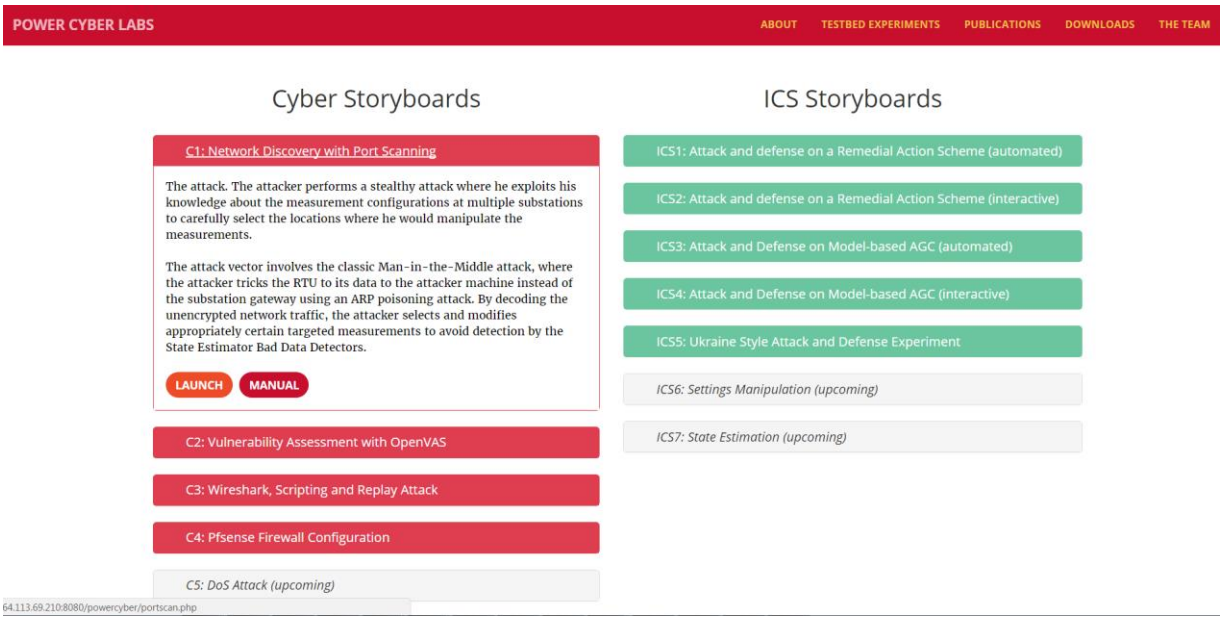
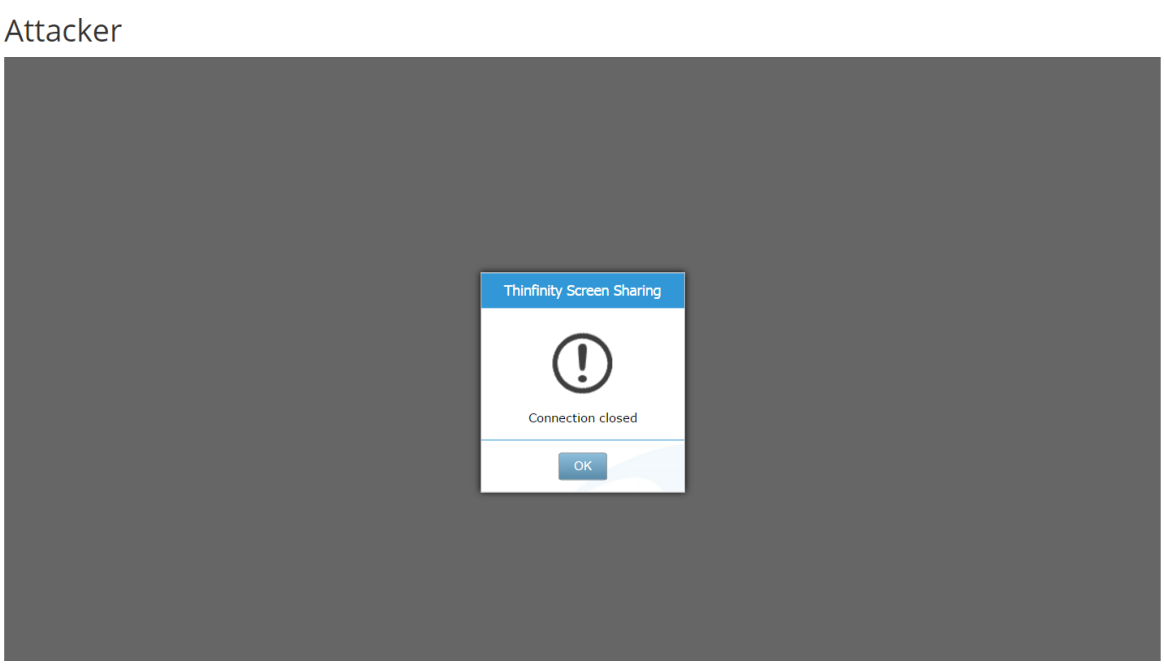
Preliminary steps before starting the experiment:

1) Click the Launch button to start the experiment.

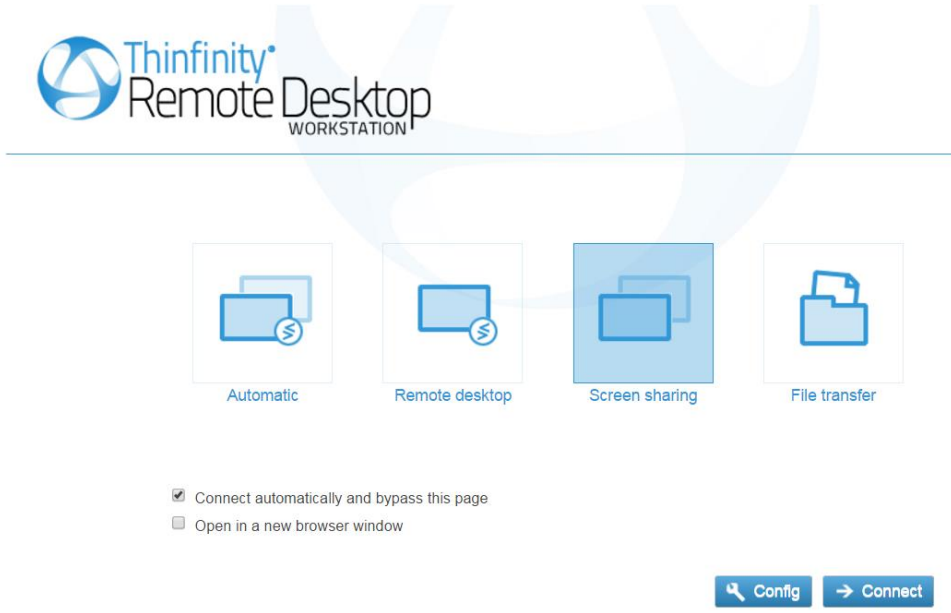


2) Click OK to create a new session



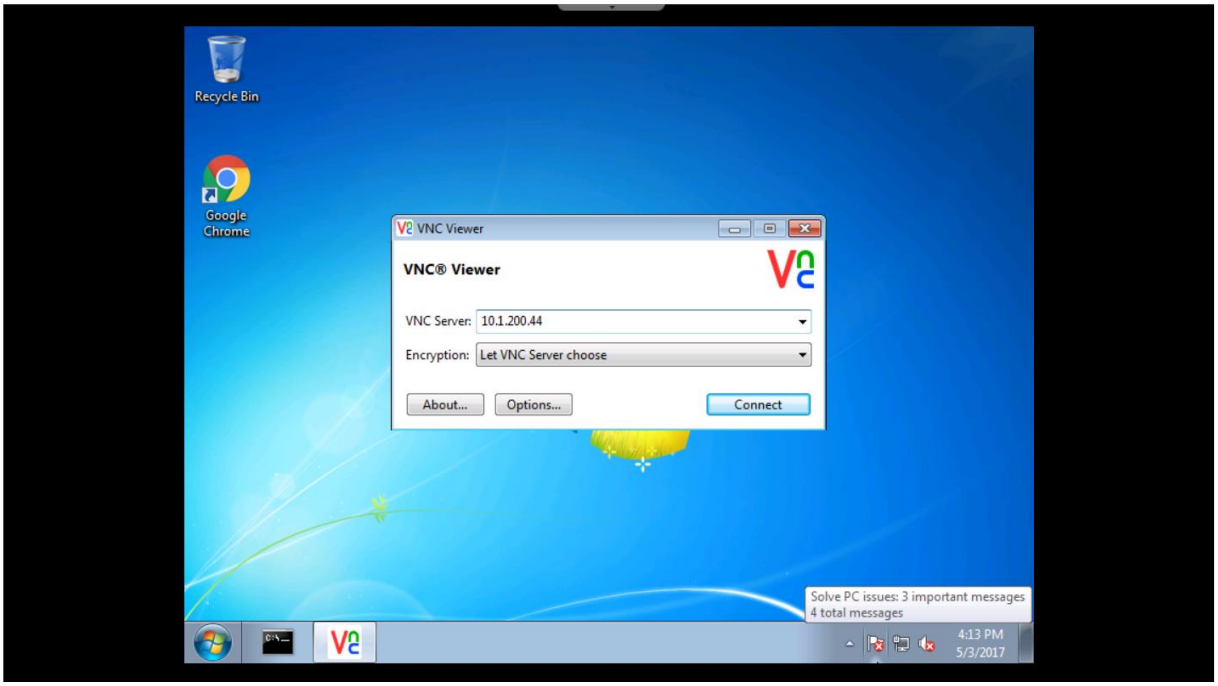
3) Click the **Screen Sharing** option and click connect to establish the session

Attacker



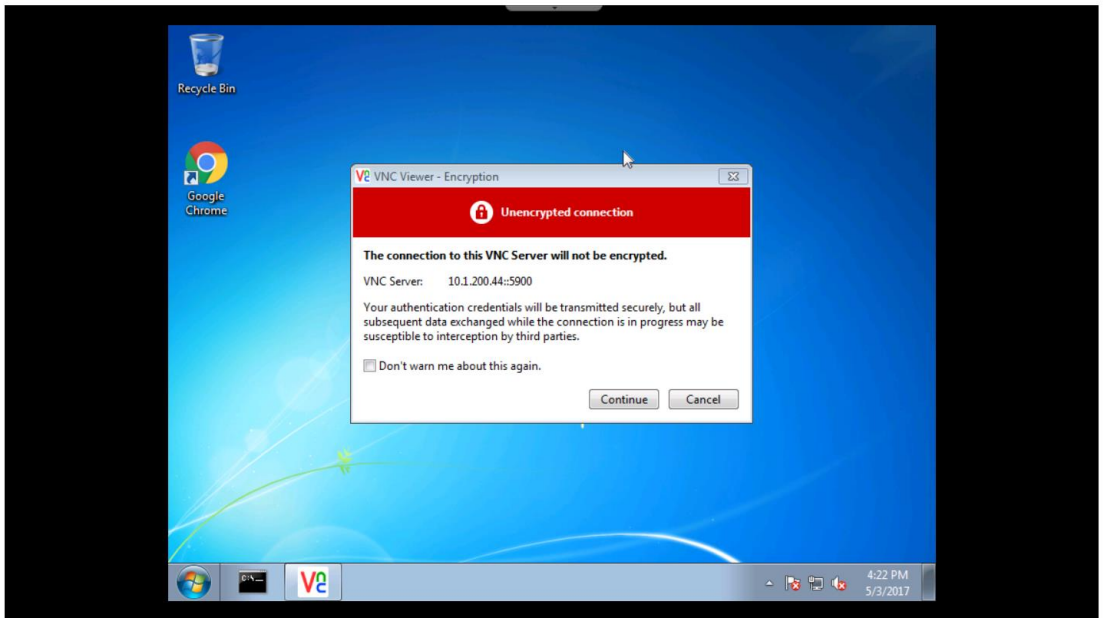
4) Click the **VNC viewer** button on the taskbar of the Windows 7 host that opens soon after and enter **10.1.200.44** as the ip address of the VNC server. Click connect to establish the session

Attacker



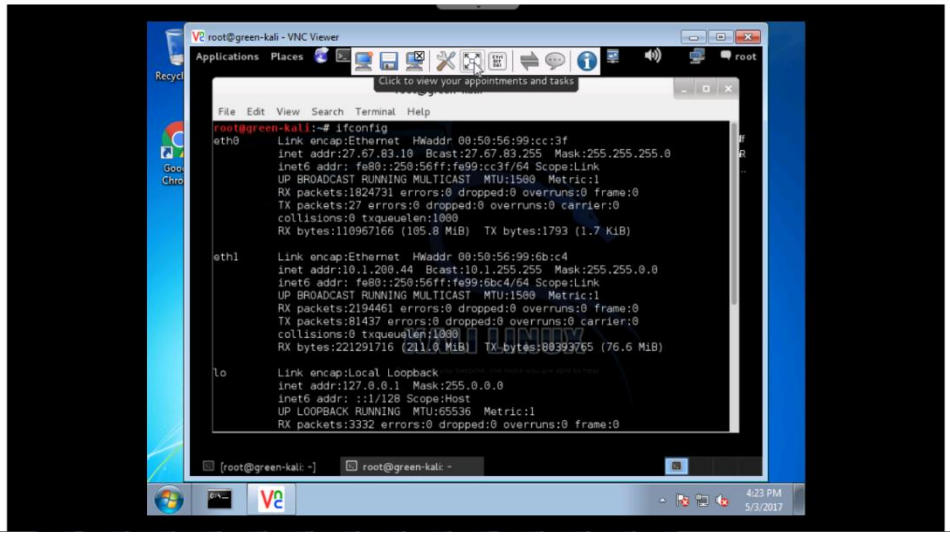
5) Click Continue to connect to the kali box.

Attacker

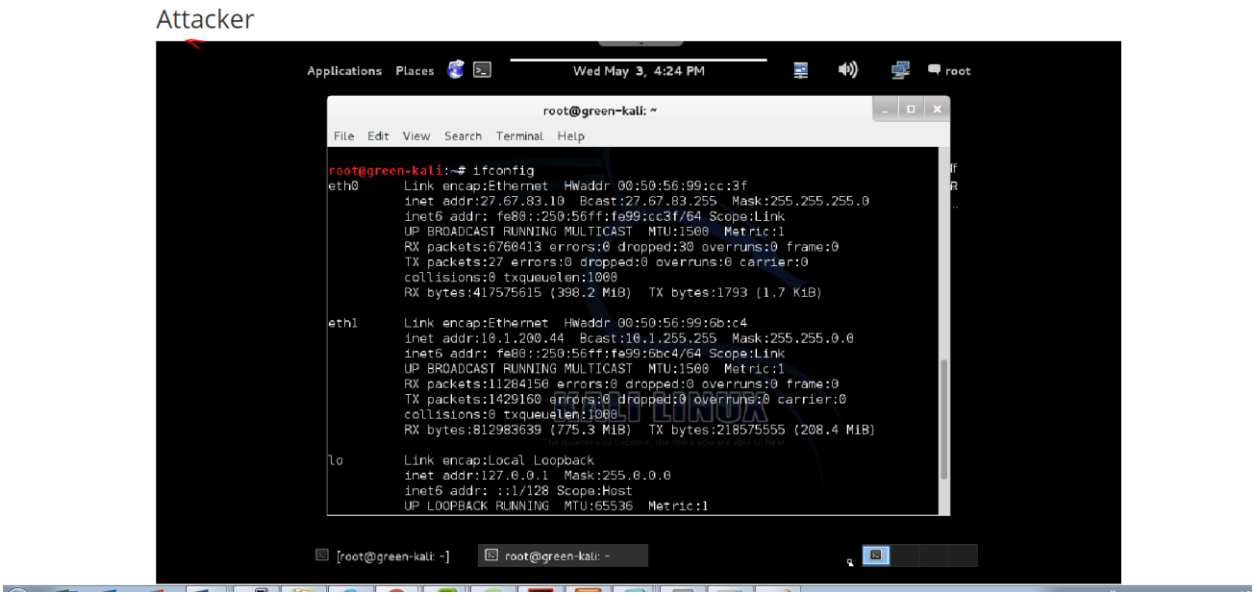


6) Gently hover over the center of the VNC viewer window to find the menu with options. Click the **Full Screen View** button (fifth from the left) for a better experience.

Attacker



7) This is how a full screen Kali box looks like.



Repeat steps 2 and 3 for the Control Center virtual machine, the Substation-RTU virtual machine and the Substation-Workstation virtual machine respectively.

Actual Experiment:

pfsense Firewall Configuration

Learning Outcomes

- Learn to configure firewall rules to meet certain security requirements.
- Learn how to restrict access to various devices connected based on the requirements.

Accessing the pfsense Firewall

pfsense uses a web-based interface to configure the various settings on the firewall. This web interface can only be accessed from the LAN side of the firewall.

We have created a workstation machine inside each network, that is running Windows 7, for the purpose of configuring each firewall.

To configure a certain pfsense firewall, first access the workstation machine that is on the same network as the firewall. (e.g.) If one wants to manage the firewall in the **Substation** network, he would access the workstation named **team**X**_substation-workstation3-win7**.

The login credentials for that machine are:

Username: alice
Password: whoami

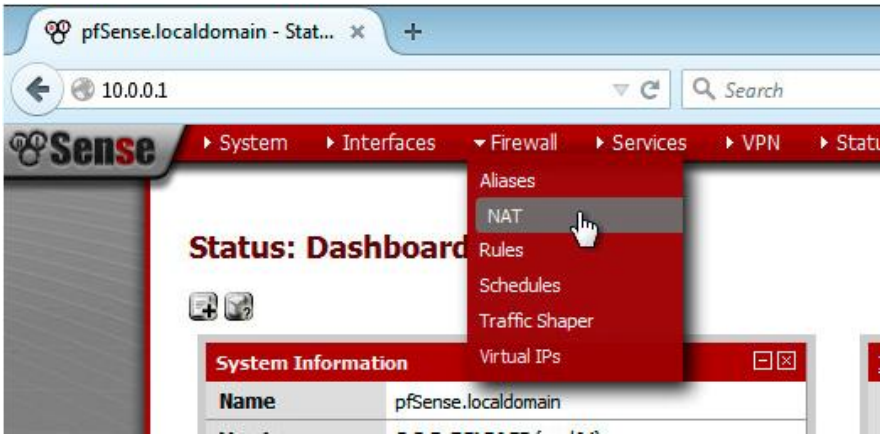
On the workstation, open a web browser and enter the IP Address of the LAN side of the pfsense firewall. (e.g.) to access the pfsense firewall on the corporate network enter the IP "10.0.0.1".

The login credentials for all the firewalls are as follows:

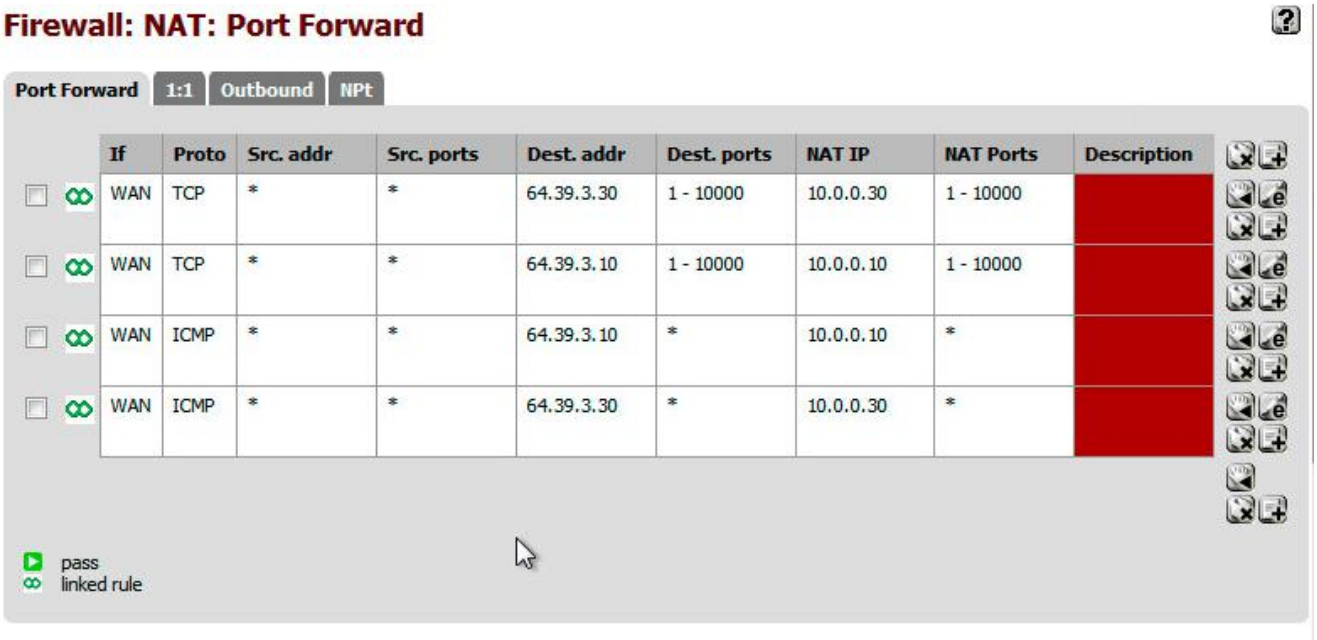
username: admin
password: pfsense

Viewing the Port Forward Configuration

From the pfsense web interface, go to Firewall → NAT

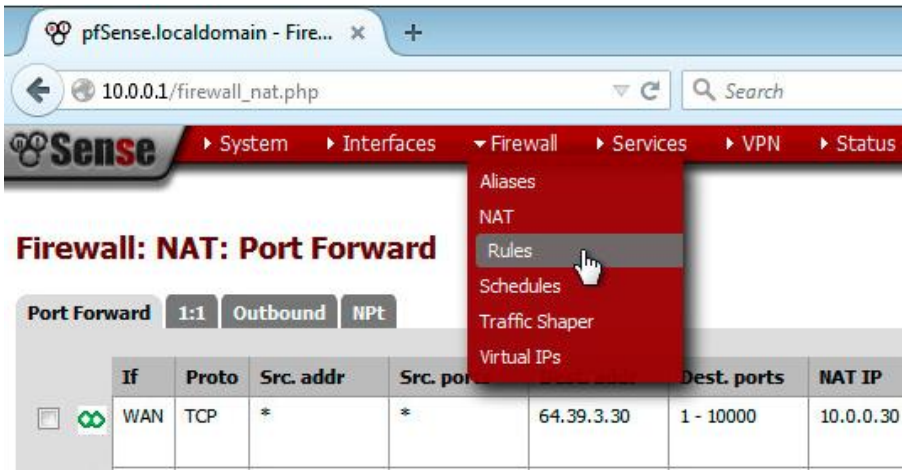


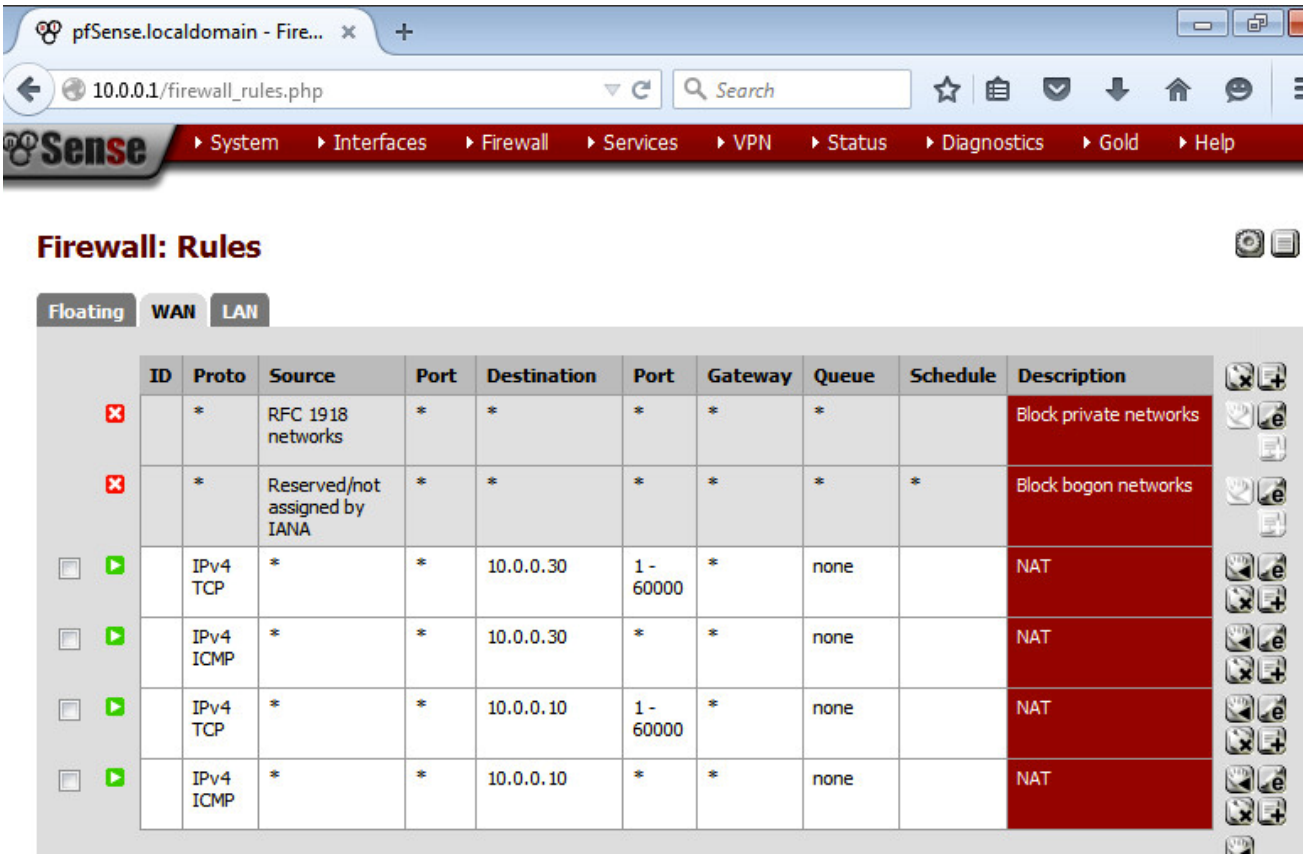
Here you will see how each of WAN IP Addresses are being forwarded to corresponding LAN IP addresses on corresponding ports.



Viewing the Firewall Rule Configurations

To view the firewall rules that are automatically generated from the above NAT port forwarding settings, go to Firewall → Rules





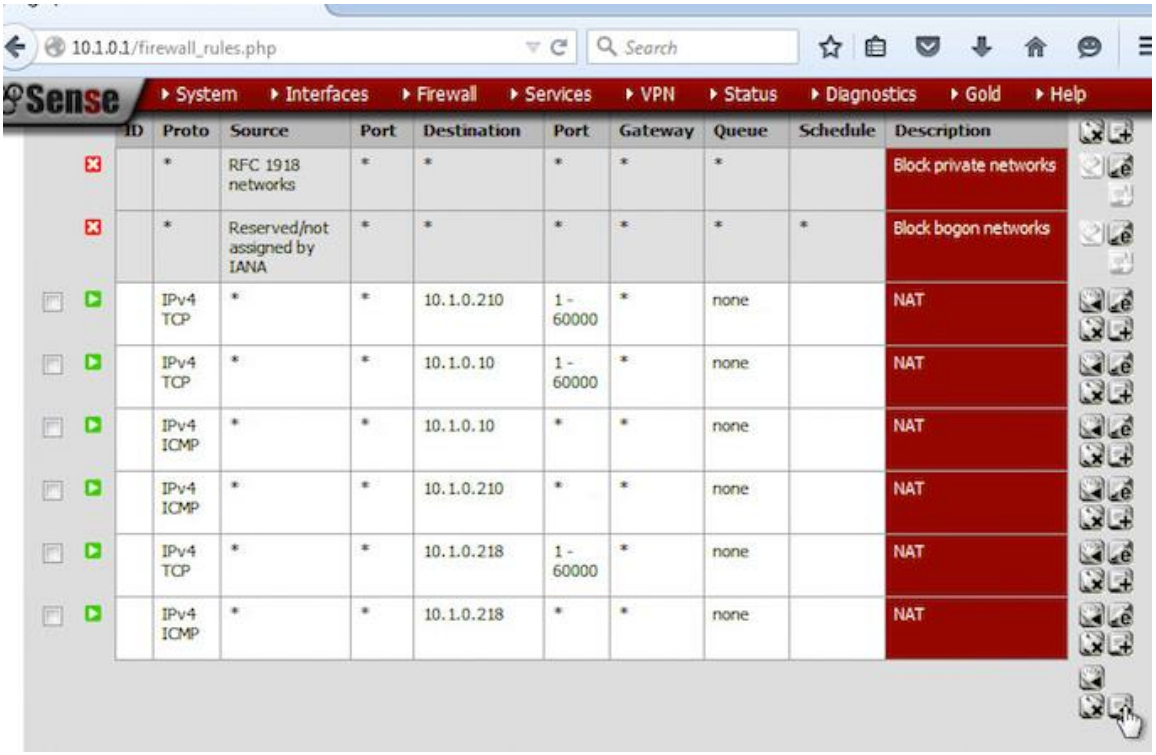
- Is there something wrong with the way we are using the firewall?
- How could these rules have been written better?

Adding Firewall Rules to prevent Trip Script from unauthorized host

We want to configure the firewall on the **substation network** to **only allow** DNP3 traffic from the control center network NAT (the PFSense firewall).
(IP address = x.x.x.1 where x.x.x is your control network)
(Default port for DNP3 is 20000)

On the **substation workstation**, open a web browser and enter the IP Address of the LAN side of the pfsense firewall. (e.g.) to access the pfsense firewall on the substation network enter the IP "10.1.0.1".

Then navigate to the rules tab and click the plus sign at the bottom right side of the page.

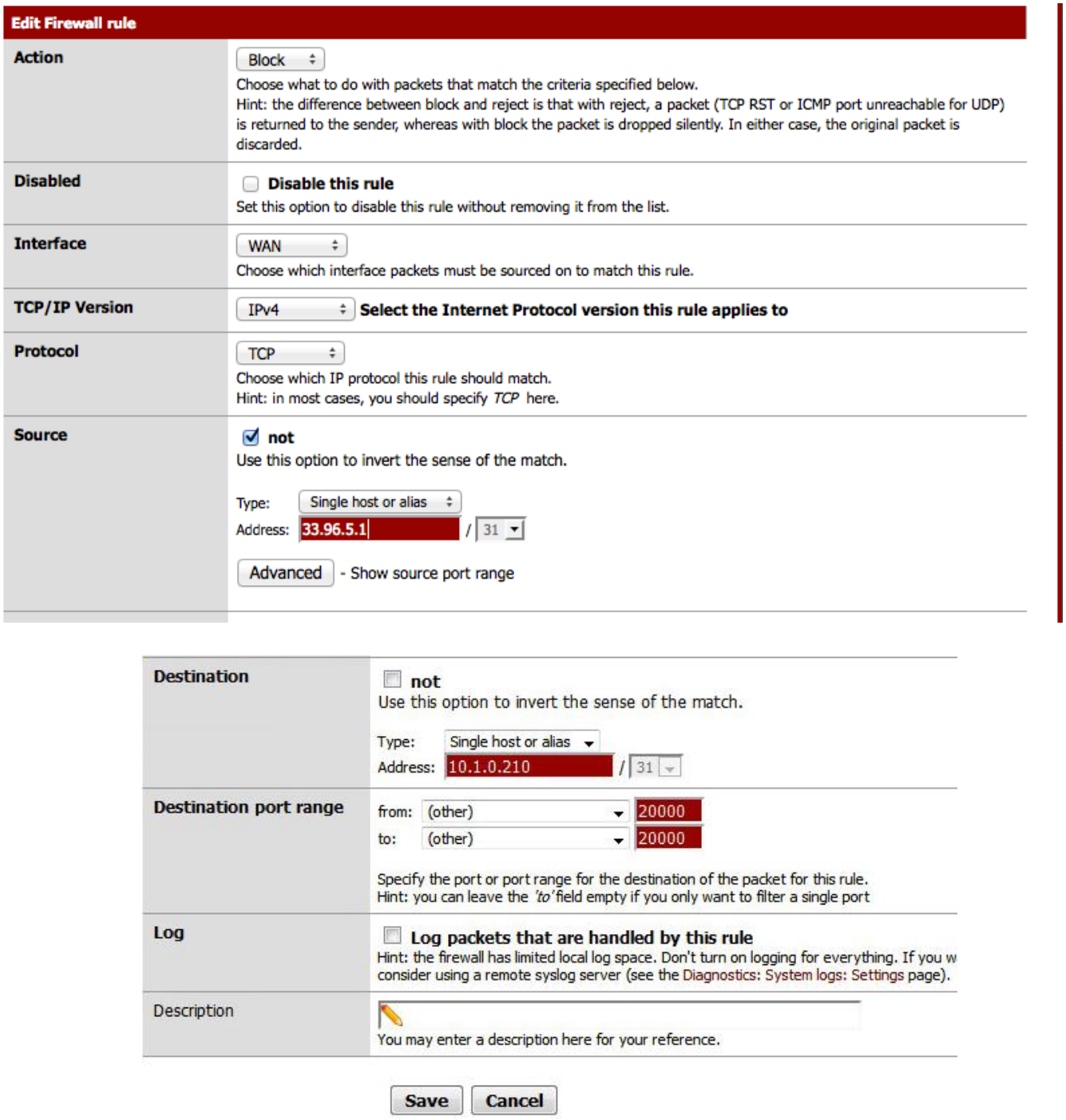


ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	RFC 1918 networks	*	*	*	*	*		Block private networks
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
	IPv4 TCP	*	*	10.1.0.210	1 - 60000	*	none		NAT
	IPv4 TCP	*	*	10.1.0.10	1 - 60000	*	none		NAT
	IPv4 ICMP	*	*	10.1.0.10	*	*	none		NAT
	IPv4 ICMP	*	*	10.1.0.210	*	*	none		NAT
	IPv4 TCP	*	*	10.1.0.218	1 - 60000	*	none		NAT
	IPv4 ICMP	*	*	10.1.0.218	*	*	none		NAT

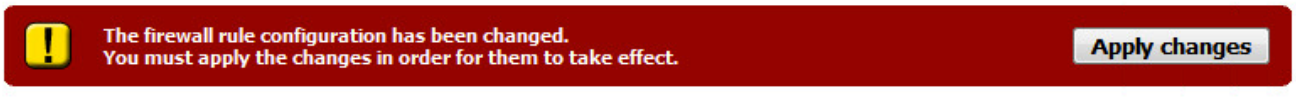
Firewall Rule – Block port 20000 from all IPs except your control center host.

Action: Block
Interface: WAN
TCP/IP version: IPv4
Protocol: TCP
Source – NOT: selected
Source – Type: Single host or alias
Source – Address: X.X.X.1
Destination – Type: Single host or alias
Destination – Address: 10.1.0.210
Destination port range: to set the destination port, select other as the port range. In the from field, enter 20000 as the port number. Leave the from field blank.

Then click save.

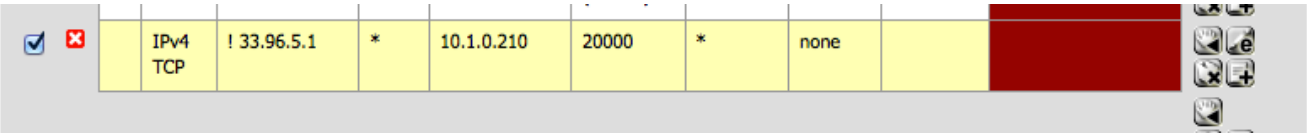


Click Apply changes to apply the firewall rule.



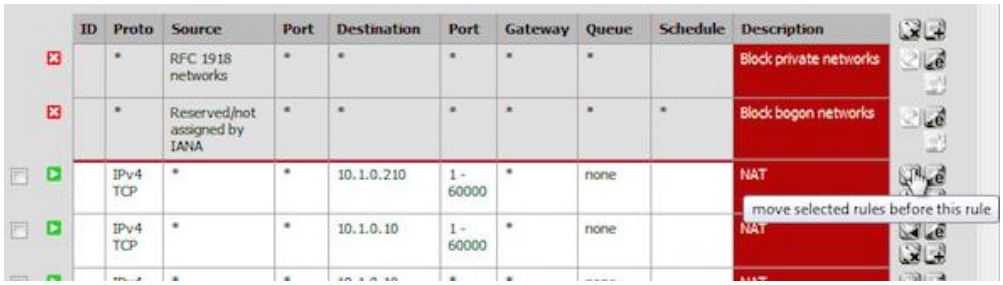
We must now move the firewall rule we created to the top of the list so it gets applied first.

Click the *check mark* on the left side of the rule you just created.



IPv4 TCP	! 33.96.5.1	*	10.1.0.210	20000	*	none		

Then scroll up and click the left arrow to insert the rule above the NAT rules but below the 2 block rules.



Then click Apply changes.

Your Task

1, Setup your whitelist in the substation firewall following above steps, and also try to create a blacklist in the similar way.

2, Once the firewall rules have been configured (either with your whitelist or blacklist enabled at one time), please verify that the changes made in pfsense does not adversely affect the normal functioning of the SCADA system. Try to switch your relay from CC and see if the controls can be done.

3, Test out whether the trip script is being blocked from the attacker Kali.

Other

Please submit the screenshots of the two firewall rules configuration. This time you should work in your own team, and the relays will be used in a time-multiplexing way. Check the following to find the two time slots when your team has a relay connected.

	03/03/2016 2pm to 5pm	03/06/2016 2pm to 5pm	03/08/2016 2pm to 5pm	03/10/2016 2pm to 5pm
Team 1	√		√	
Team 2	√		√	
Team 3	√		√	
Team 4	√		√	
Team 5		√		√
Team 6		√		√
Team 7		√		√
Team 8		√		√

* Please remember to remove all firewall rules after testing them.