Remediating UDP Source Port Pass Firewall Vulnerability on ESXi servers

ESXi uses a stateless firewall. Consequently, it has a rule to allow incoming DNS traffic (UDP) through source port 53. The easiest way to fix this vulnerability is to restrict the access on this port to the local DNS server IP addresses.

You can restrict access either using the vSphere Web Client or VMware PowerCLI. Instructions for each method are below.

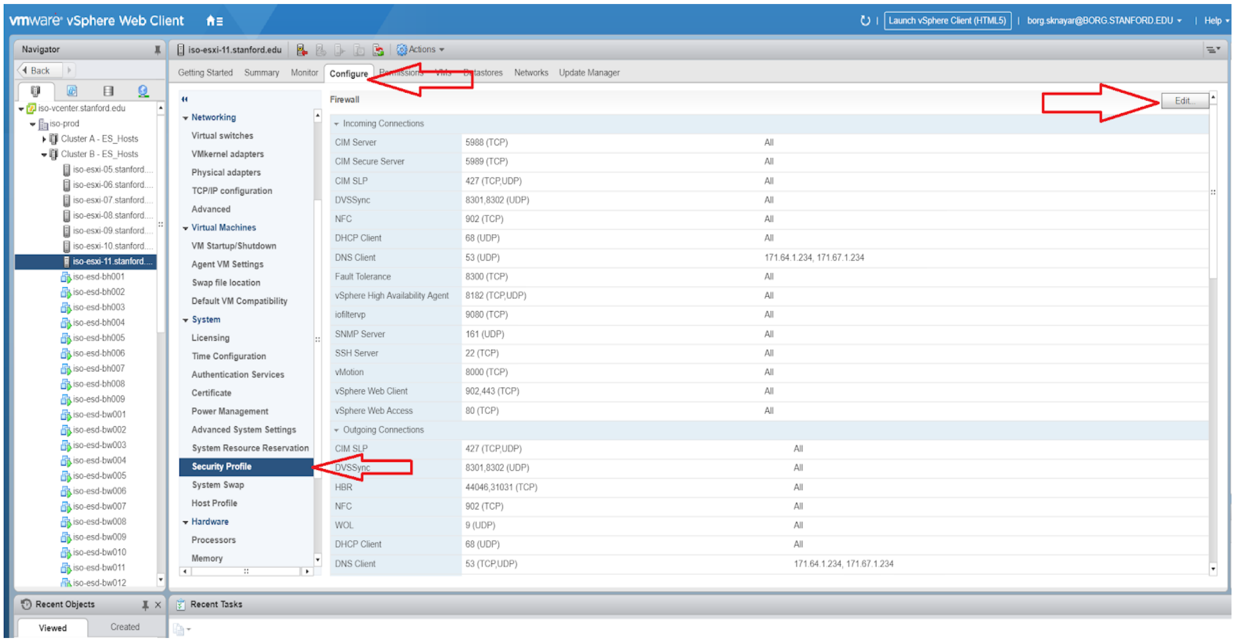
Using the vSphere Web Client

1. Access the vSphere web client.

2. Login into vCenter and navigate to the **Hosts and Cluster** view.

3. In the left hand navigation panel, click on the host you would like to update.

4. Click the **Configure** tab and select **Security Profile.**

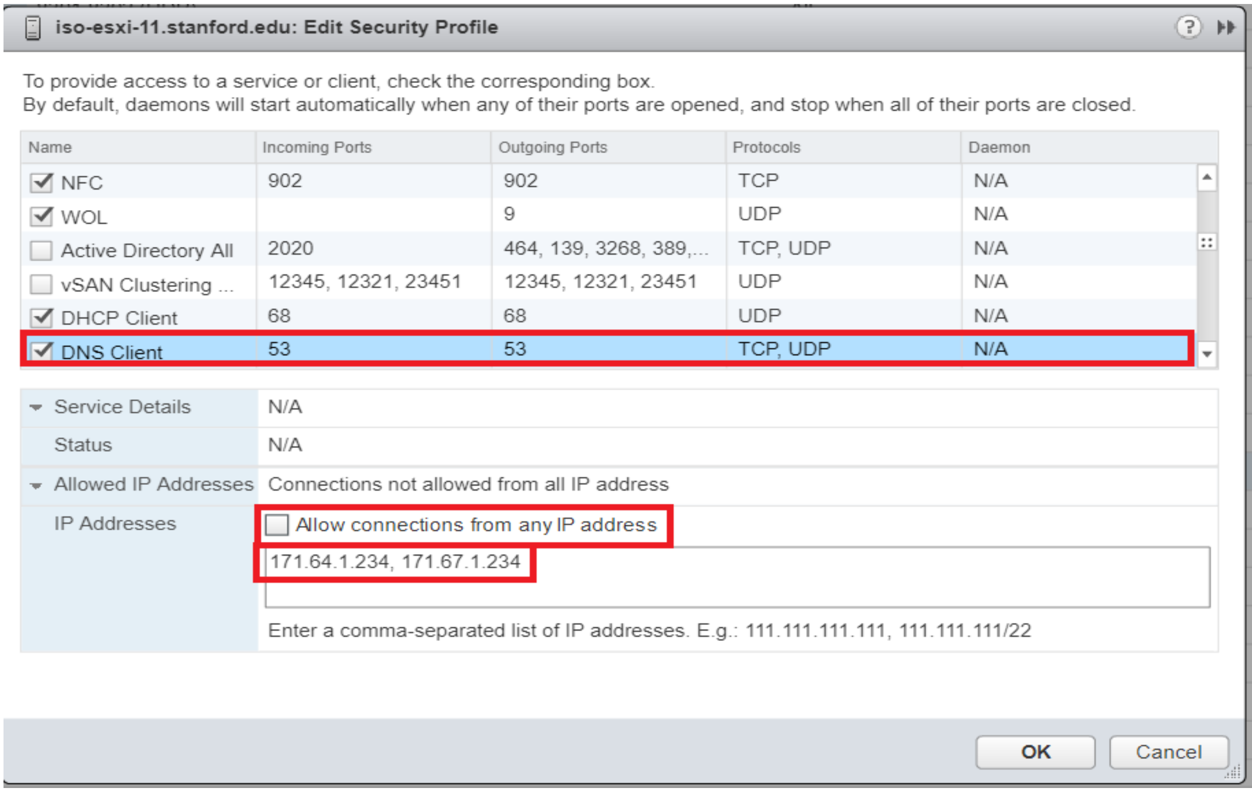


Firewall

Incoming Connections		
CIM Server	5988 (TCP)	All
CIM Secure Server	5989 (TCP)	All
CIM SLP	427 (TCP,UDP)	All
DVSSync	8301,8302 (UDP)	All
NFC	902 (TCP)	All
DHCP Client	68 (UDP)	All
DNS Client	53 (UDP)	171.64.1.234, 171.67.1.234
Fault Tolerance	8300 (TCP)	All
vSphere High Availability Agent	8182 (TCP,UDP)	All
iofiltervp	9080 (TCP)	All
SNMP Server	161 (UDP)	All
SSH Server	22 (TCP)	All
vMotion	8000 (TCP)	All
vSphere Web Client	902,443 (TCP)	All
vSphere Web Access	80 (TCP)	All
Outgoing Connections		
CIM SLP	427 (TCP,UDP)	All
DVSSync	8301,8302 (UDP)	All
HBR	44046,31031 (TCP)	All
NFC	902 (TCP)	All
WOL	9 (UDP)	All
DHCP Client	68 (UDP)	All
DNS Client	53 (TCP,UDP)	171.64.1.234, 171.67.1.234

5. Scroll up and click on **Edit** to edit the firewall.

6. In the popup window, make the following changes.
   - Select **DNS Client**
   - If it is selected, deselect **Allow connections from any IP address**
   - Enter a comma separated list of DNS server IP addresses



iso-esxi-11.stanford.edu: Edit Security Profile

To provide access to a service or client, check the corresponding box.
By default, daemons will start automatically when any of their ports are opened, and stop when all of their ports are closed.

Name	Incoming Ports	Outgoing Ports	Protocols	Daemon
☑ NFC	902	902	TCP	N/A
☑ WOL		9	UDP	N/A
□ Active Directory All	2020	464, 139, 3268, 389,...	TCP, UDP	N/A
□ vSAN Clustering ...	12345, 12321, 23451	12345, 12321, 23451	UDP	N/A
☑ DHCP Client	68	68	UDP	N/A
☑ DNS Client	53	53	TCP, UDP	N/A

Service Details	N/A
Status	N/A
Allowed IP Addresses	Connections not allowed from all IP address
IP Addresses	□ Allow connections from any IP address 171.64.1.234, 171.67.1.234 Enter a comma-separated list of IP addresses. E.g.: 111.111.111.111, 111.111.111/22

7. Click **Ok**.

Using VMware PowerCLI

You can use the following PowerCLI commands to automate the updating of all of your ESXi servers. You will need to add a few additional lines of code to fetch ESXi hostnames and such.

```
$ESXfw = (get-esxcli -vmhost <ESXiHOST>).network.firewall
$ESXfw.ruleset.set($false,$true,"dns")
$ESXfw.ruleset.allowedip.add("171.64.1.234","dns")
$ESXfw.ruleset.allowedip.add("171.67.1.234","dns")
```