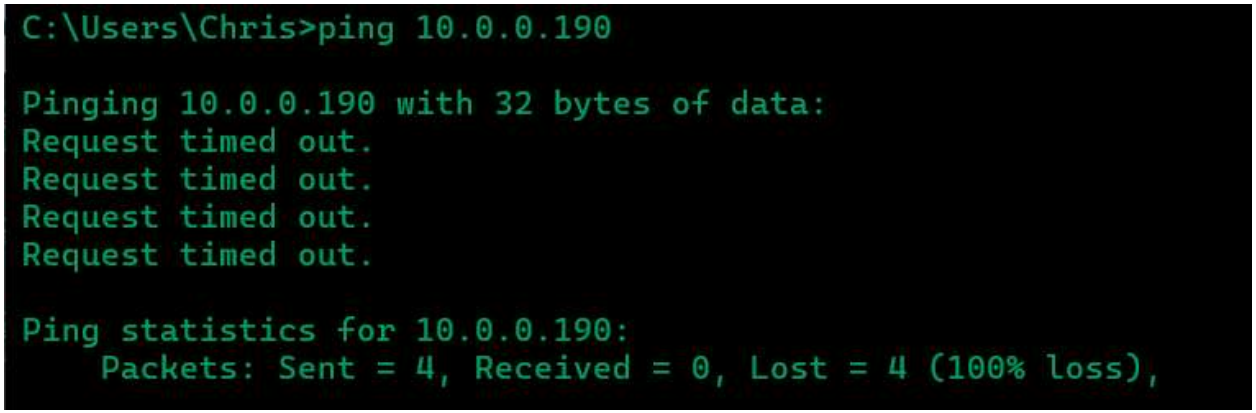
Firewalls and how to work with them and not get burned...

Lets first ping our Windows server. Interesting, result as I am timing out on my server.



Ok, lets try a different approach...

Nmap time

First I try a stealth scan (-sS), but no luck. Though, Nmap tells me try -Pn so lets try that next. This is saying scan don’t ping and just scan, but again no luck. Well, maybe -sA which can help map out firewall rulesets. Ok, at a loss lets just try a simple nmap scan.

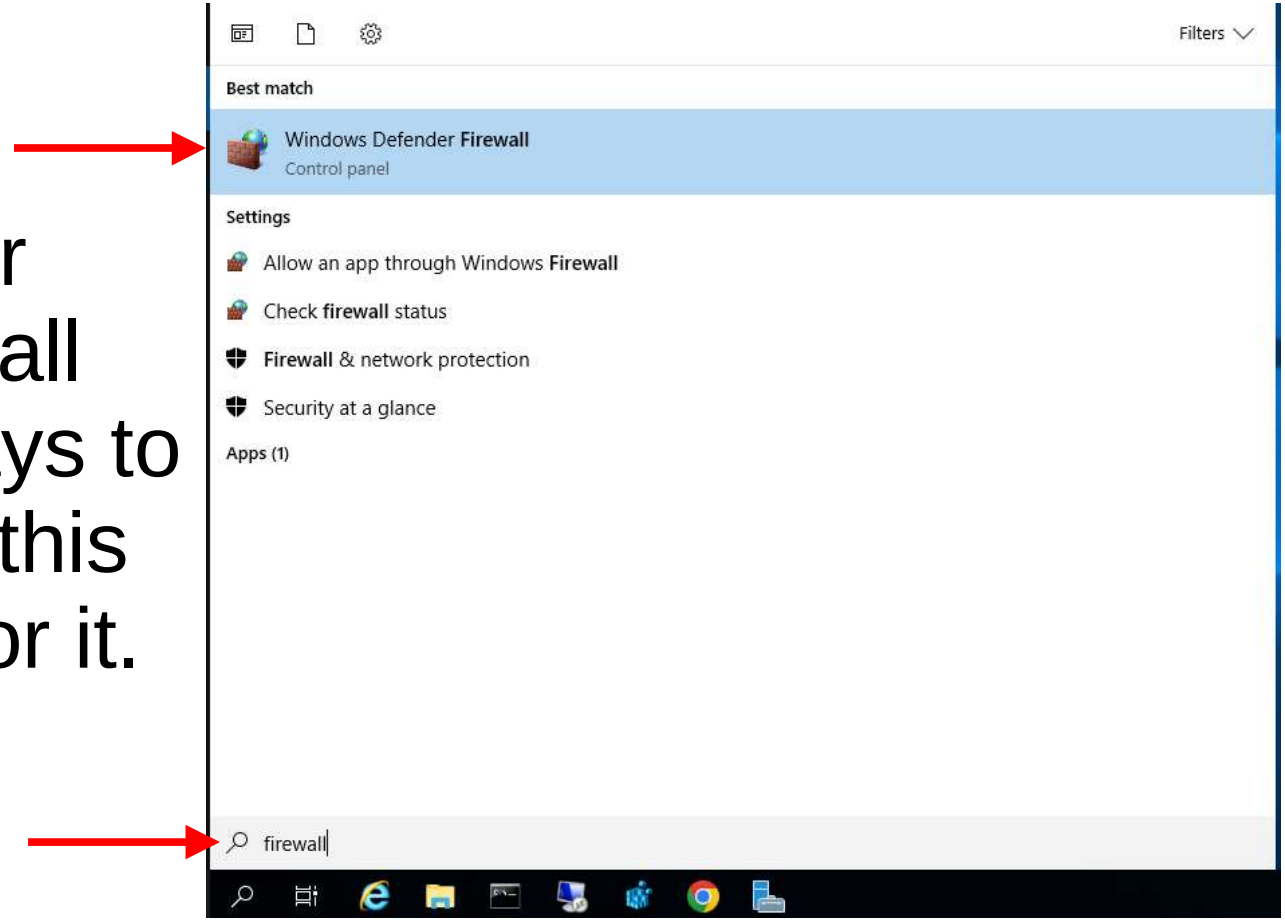
```
C:\Users\Chris>nmap -sS 10.0.0.190
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-02 19:59 Mountain Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 7.22 seconds

C:\Users\Chris>nmap -Pn 10.0.0.190
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-02 20:00 Mountain Daylight Time
Nmap done: 1 IP address (0 hosts up) scanned in 3.88 seconds

C:\Users\Chris>nmap -sA 10.0.0.190
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-02 20:00 Mountain Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.37 seconds

C:\Users\Chris>nmap 10.0.0.190
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-02 20:00 Mountain Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.76 seconds
```

Well, does 10.0.0.190 even exist on our network? We should be able to check the ARP table (arp -a) to find out.

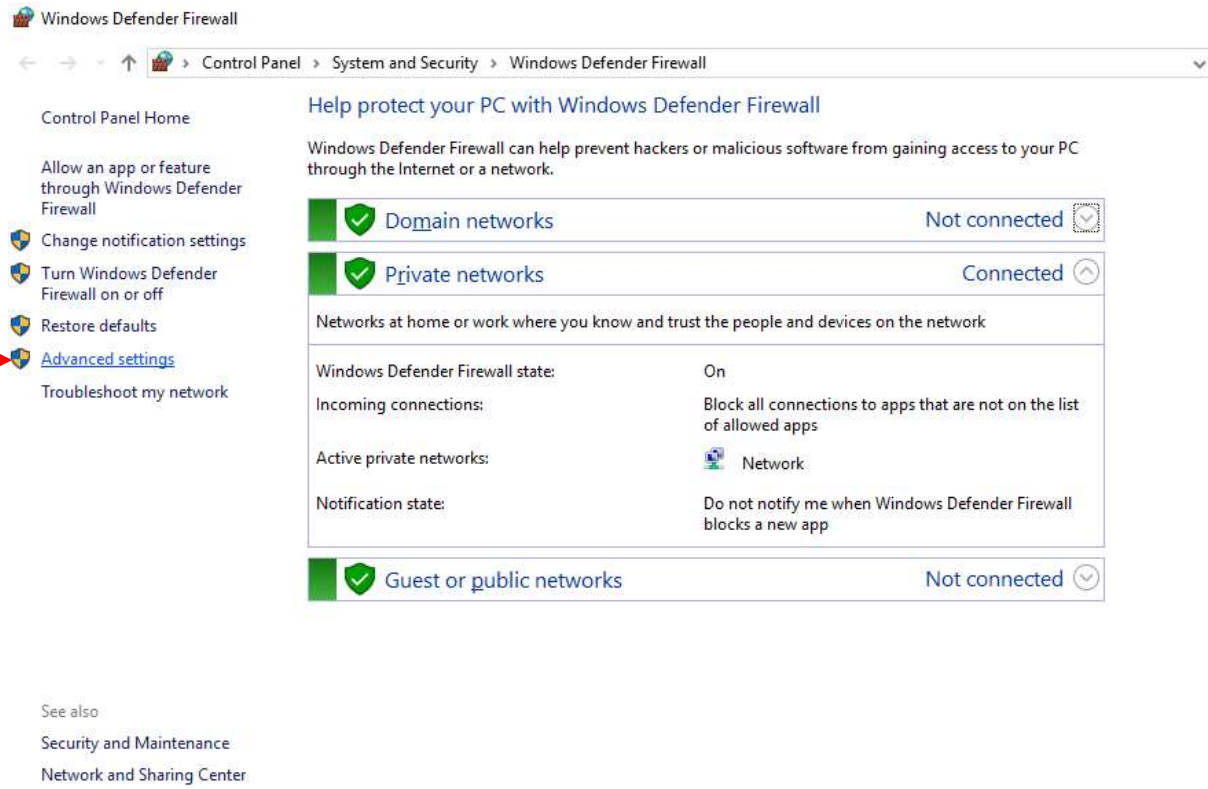
Ok, so we know it actually is an assigned IP but otherwise we can't seem to find it.

```
C:\Users\Chris>arp -a

Interface: 192.168.56.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.0.0.170 --- 0xd
  Internet Address      Physical Address      Type
  10.0.0.1              80-da-c2-91-35-d7     dynamic
  10.0.0.92             a4-5d-36-1b-b6-b6     dynamic
  10.0.0.108            24-fc-e5-83-a3-6f     dynamic
  10.0.0.136            80-0c-f9-1a-18-35     dynamic
  10.0.0.159            34-25-be-51-b7-f3     dynamic
  10.0.0.161            08-00-27-2a-8d-e9     dynamic
  10.0.0.190            08-00-27-b0-65-65     dynamic
  10.0.0.228            d8-80-83-5d-e5-6d     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.113           01-00-5e-00-00-71     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

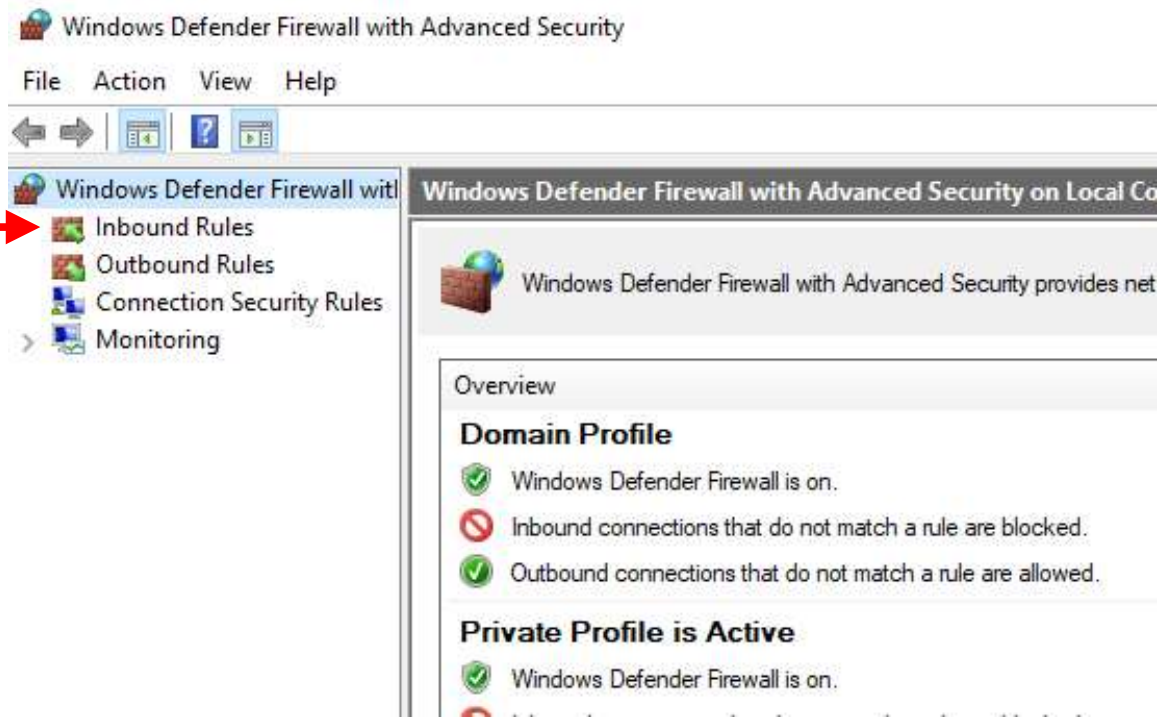
Lets check our Windows Firewall settings. Many ways to get there but for this lets just search for it.



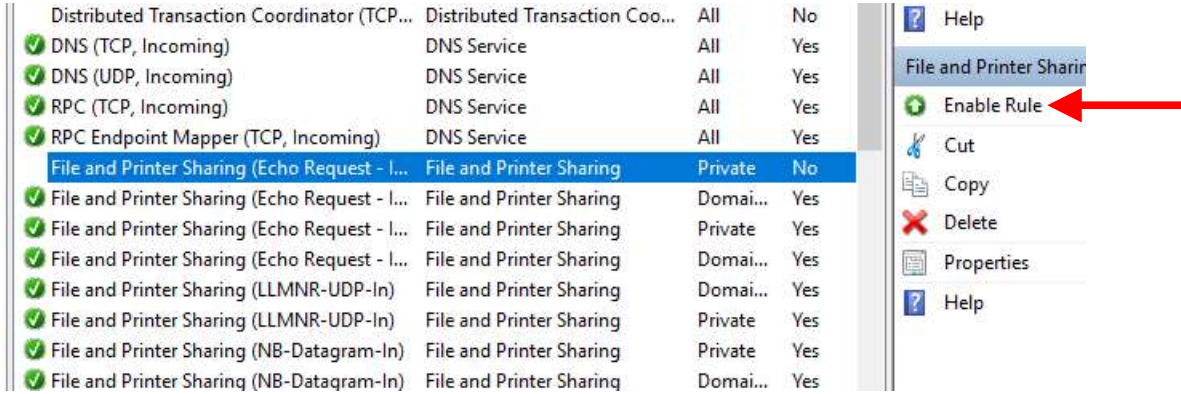
Next select Advanced



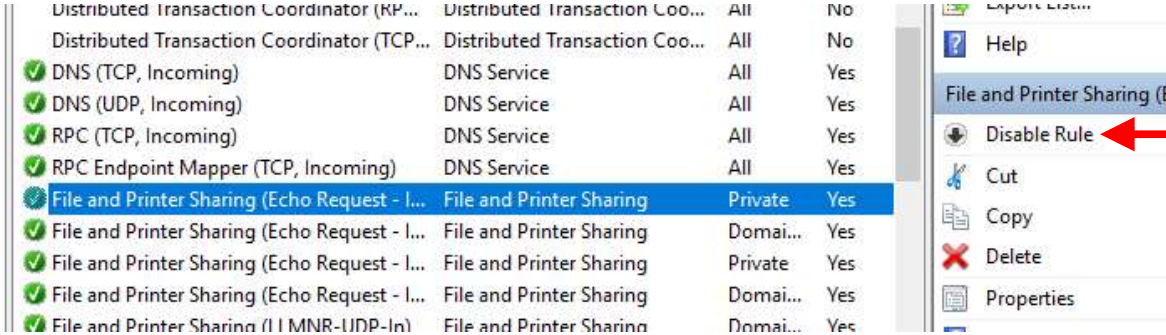
Then lets take a look at the Inbound Rules

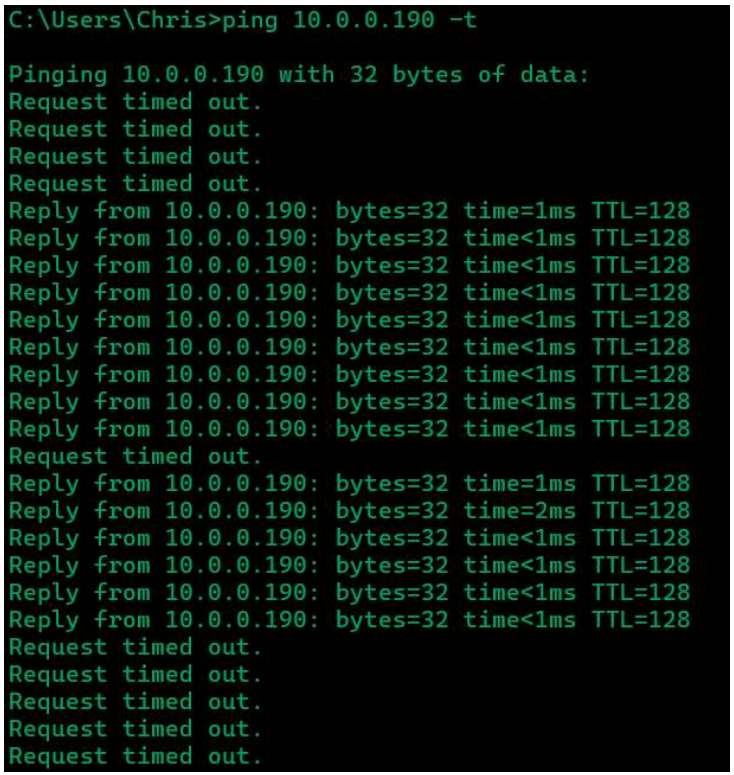


Scroll to File and Printer Sharing (Echo Request ICMPv4) Notice there are two but the key is the profile and for my server the Firewall is active on the Private network.



Lets continuously ping (-t) from our host and then on the server firewall enable/disable and see what happens.

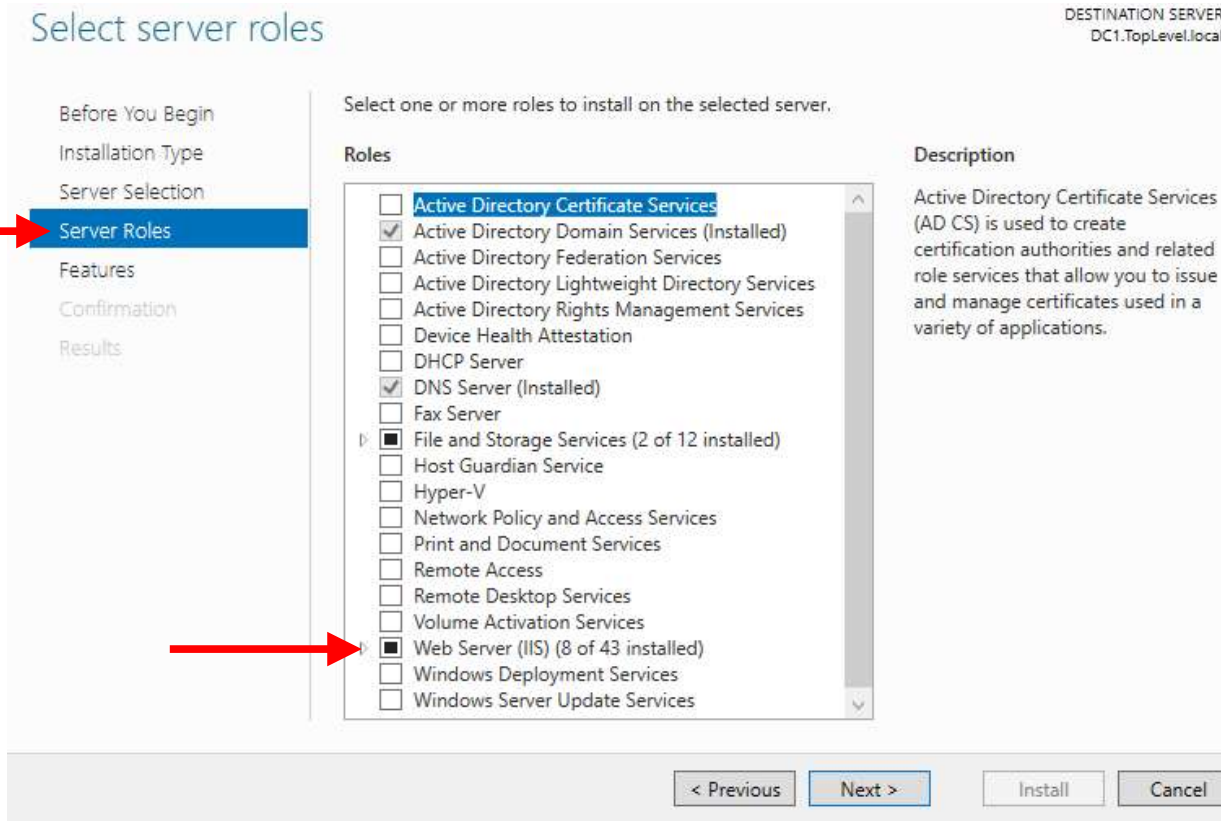




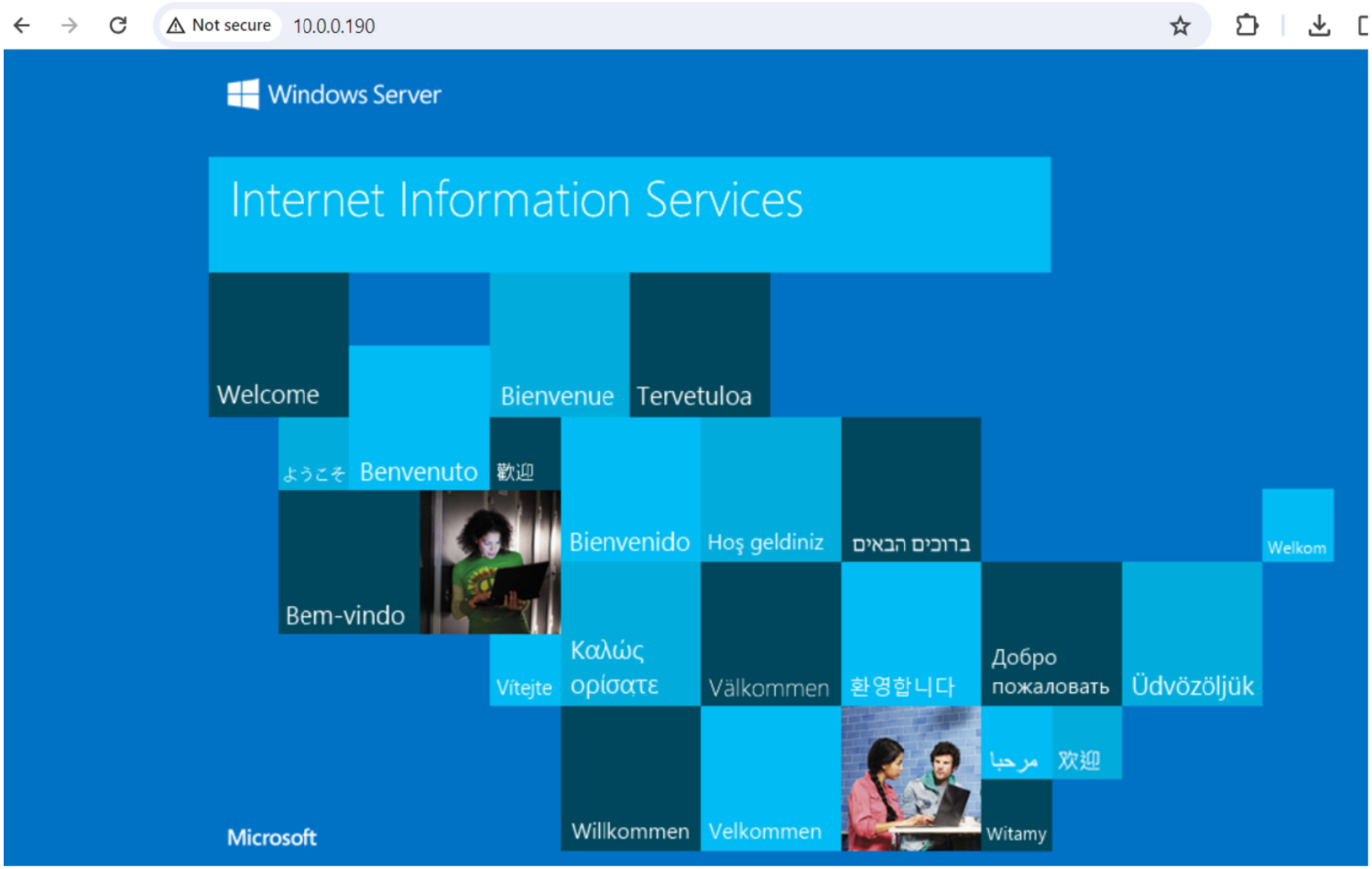
Switch back to our host and as you enable/disable watch for changes.

Looks like we figured it out and as we disable the firewall the ping requests go through.

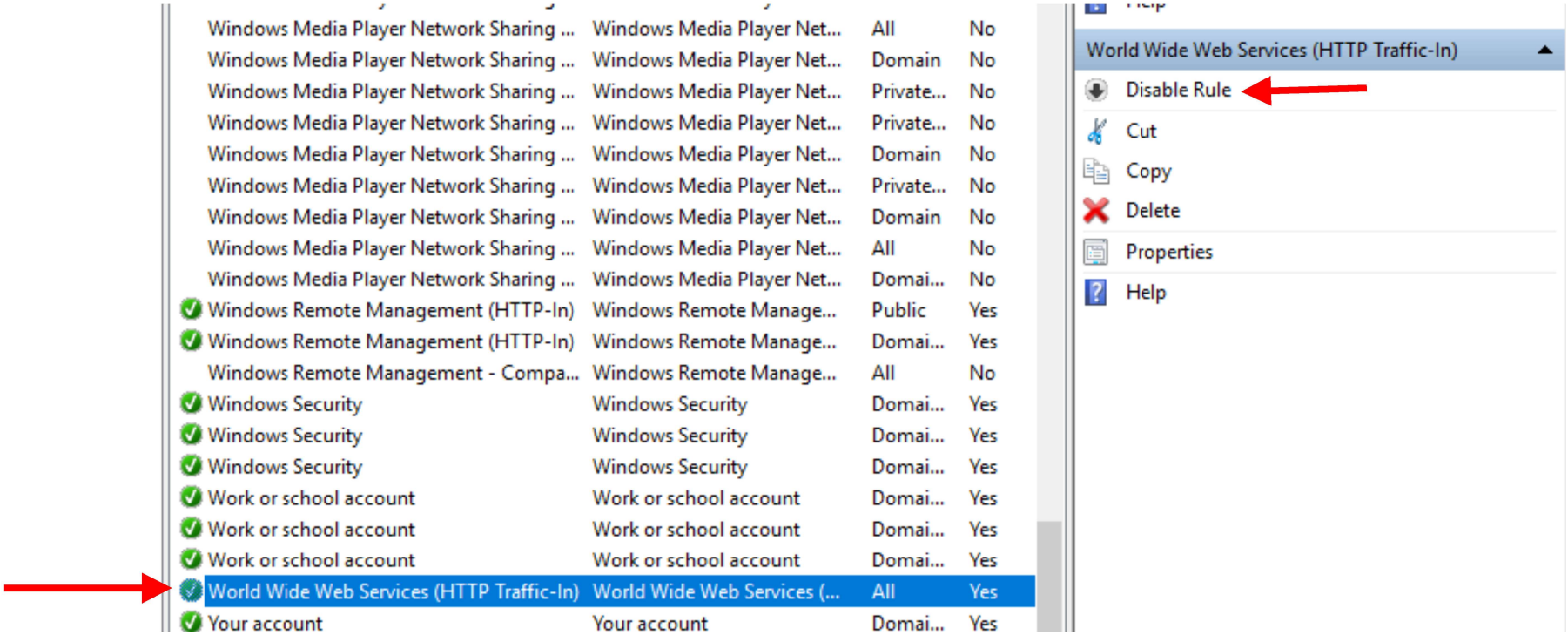
Next lets turn on the Microsoft Web Server (IIS)



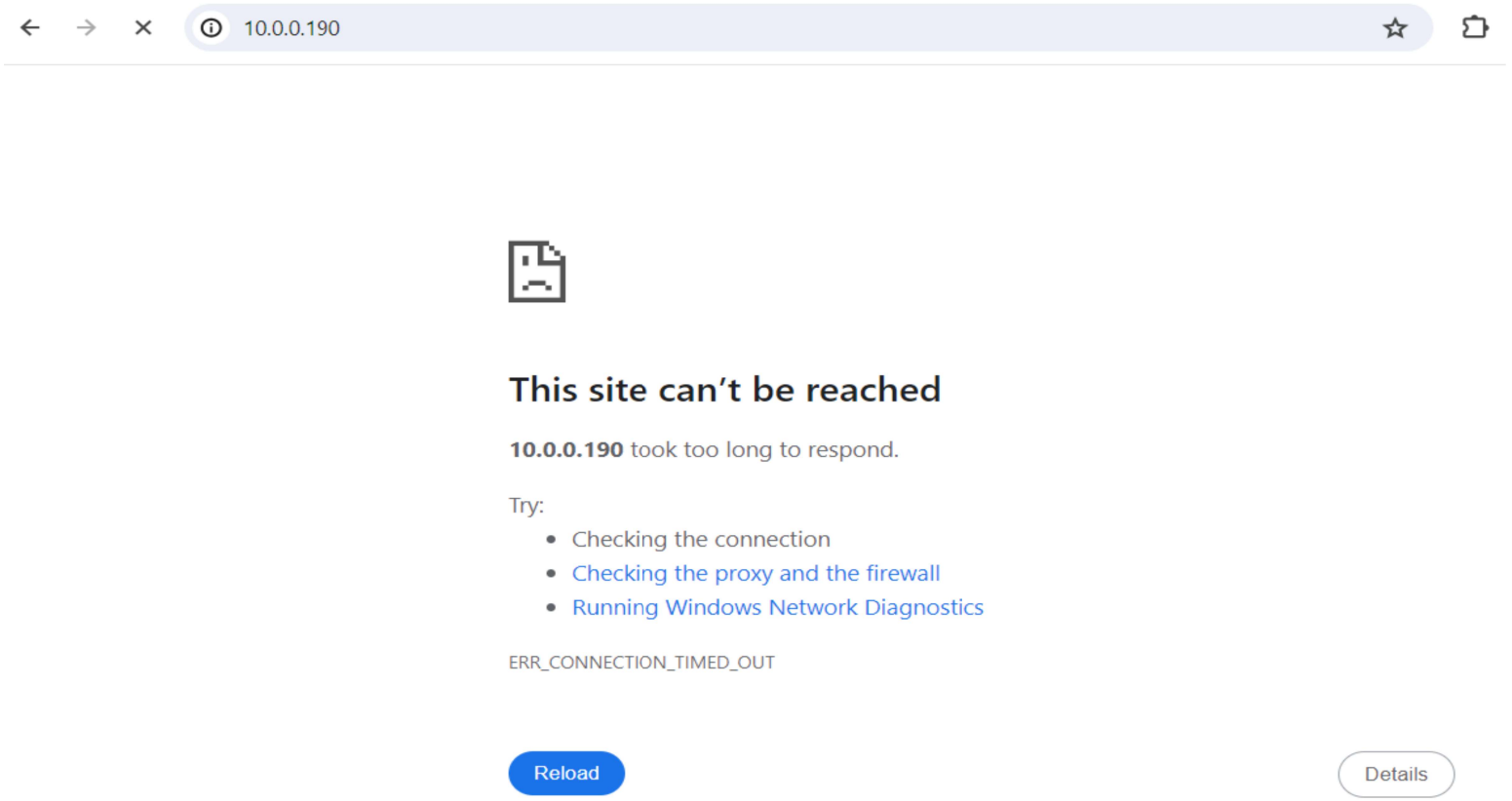
You should be able to check by trying to access from your host web browser.



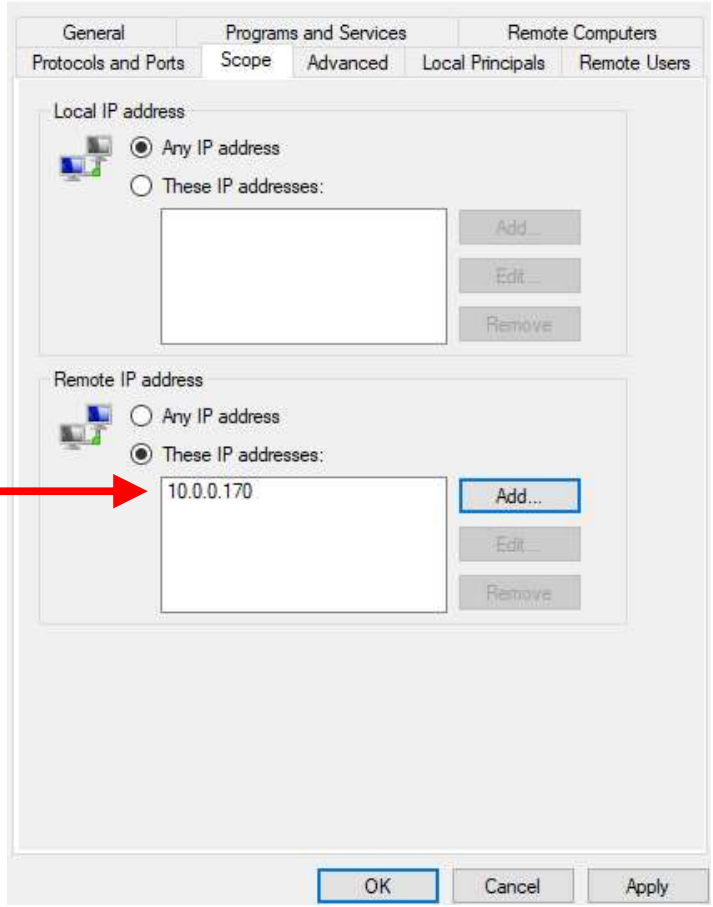
Lets scroll to the World Wide Web Services and Disable the Rule



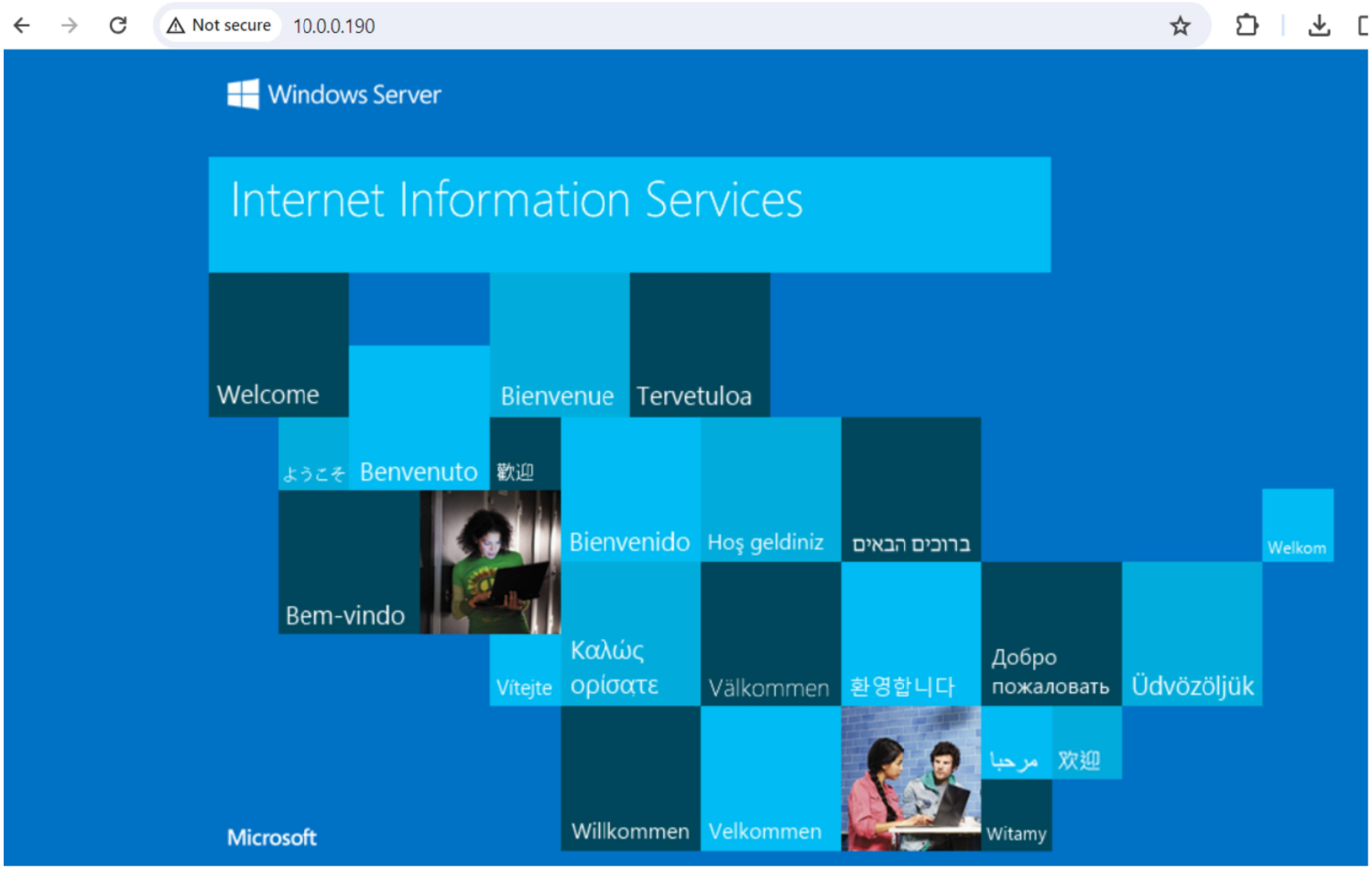
I’m sure as you guessed, if you check from your host the site is down.

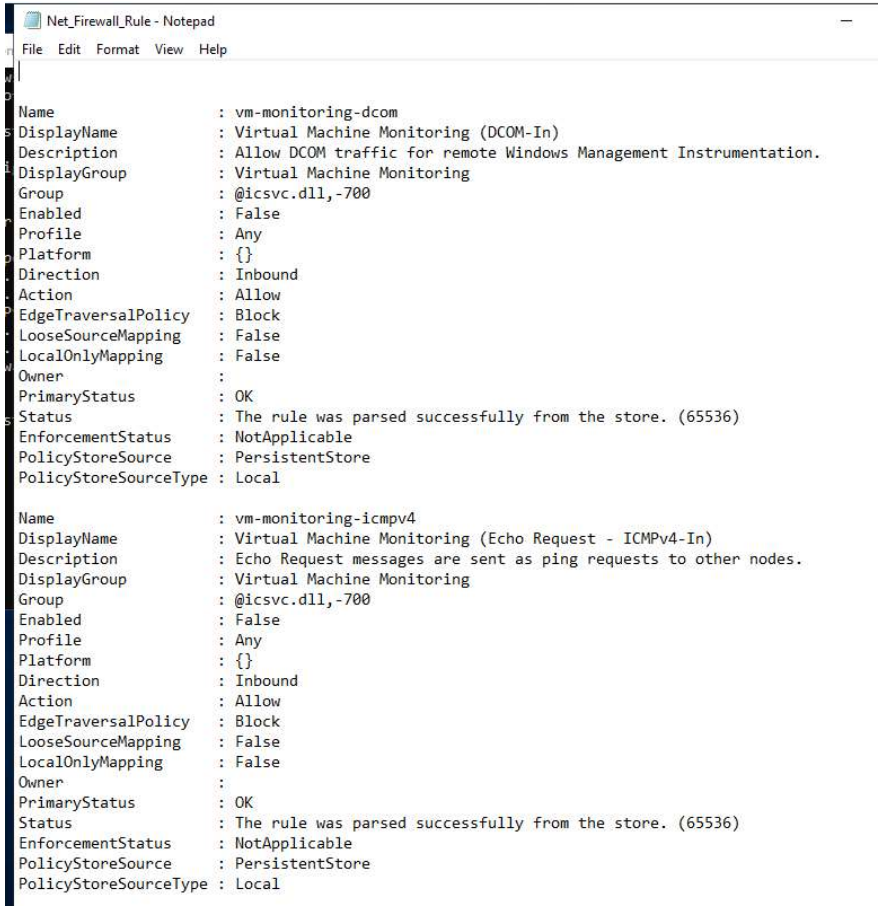


If we want we can also adjust the Scope of the rule. I decided to only allow my host OS to access the site.



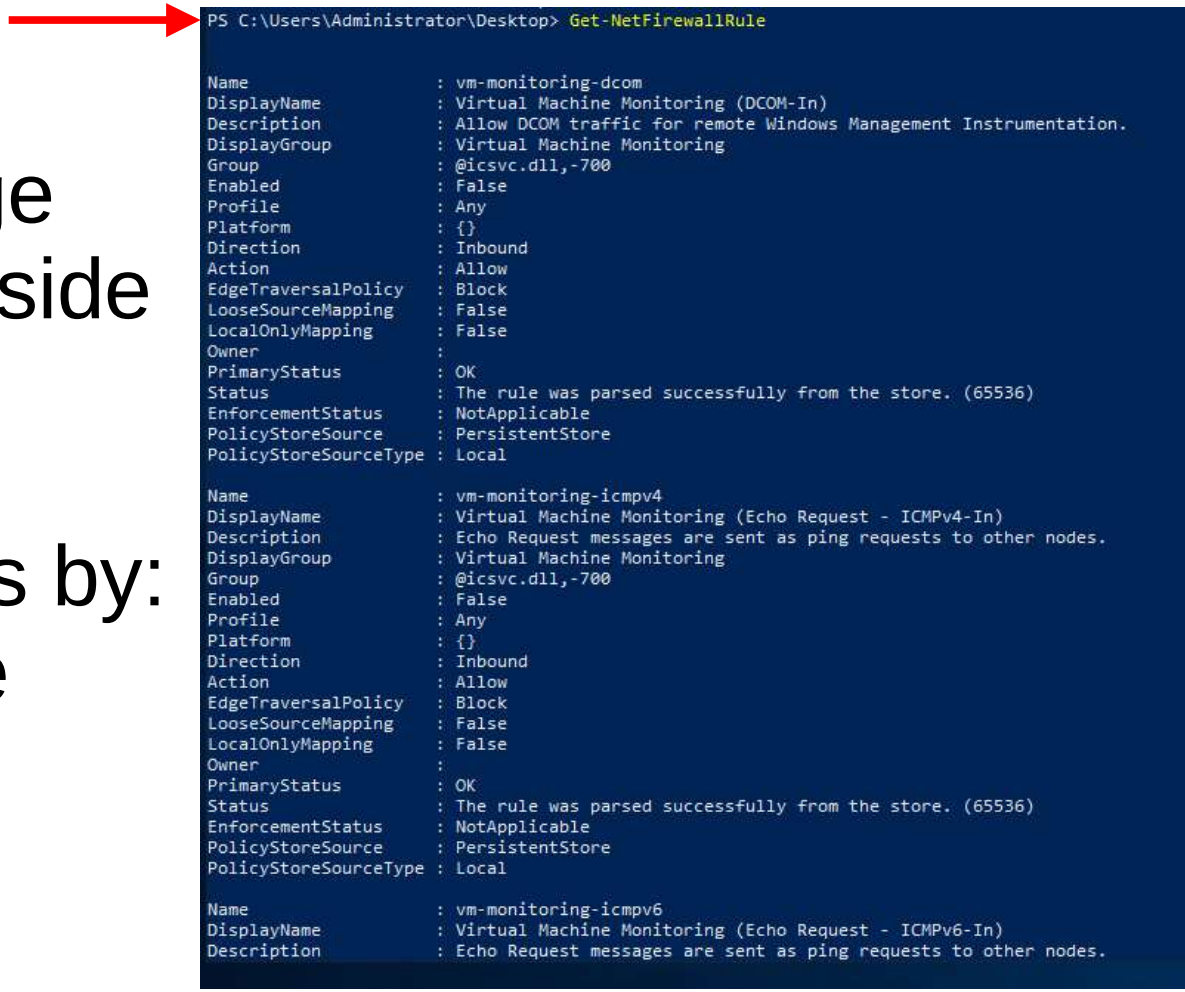
And, back up but now only allowed from the host OS



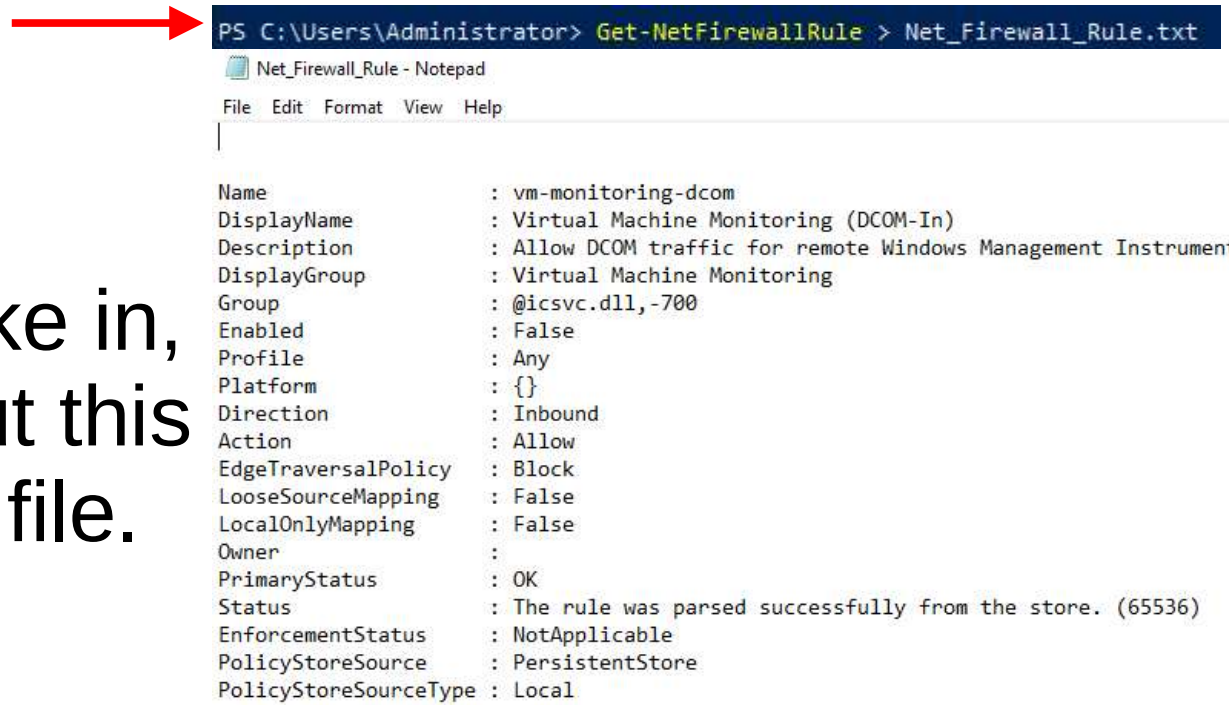

Net_Firewall_Rule - Notepad
File Edit Format View Help
Name : vm-monitoring-dcom
DisplayName : Virtual Machine Monitoring (DCOM-In)
Description : Allow DCOM traffic for remote Windows Management Instrumentation.
DisplayGroup : Virtual Machine Monitoring
Group : @icsvc.dll,-700
Enabled : False
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
Name : vm-monitoring-icmpv4
DisplayName : Virtual Machine Monitoring (Echo Request - ICMPv4-In)
Description : Echo Request messages are sent as ping requests to other nodes.
DisplayGroup : Virtual Machine Monitoring
Group : @icsvc.dll,-700
Enabled : False
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

Lets now try to change Firewall settings from inside Powershell.

First, lets check the rules by: Get-NetFirewallRule



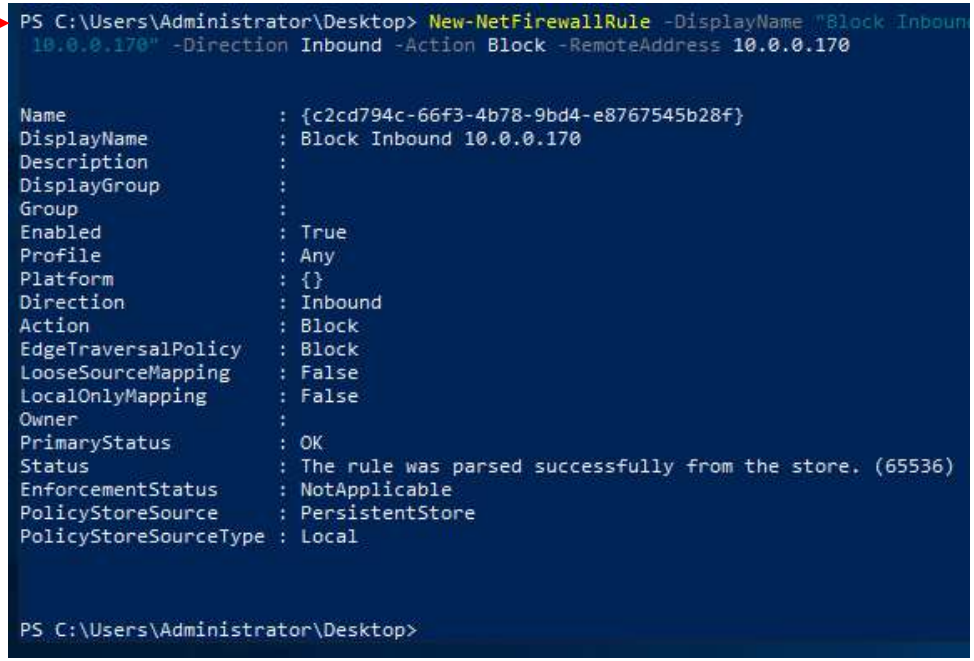
Ok, a bit much to take in, so lets do it again but this time redirect it to a file.

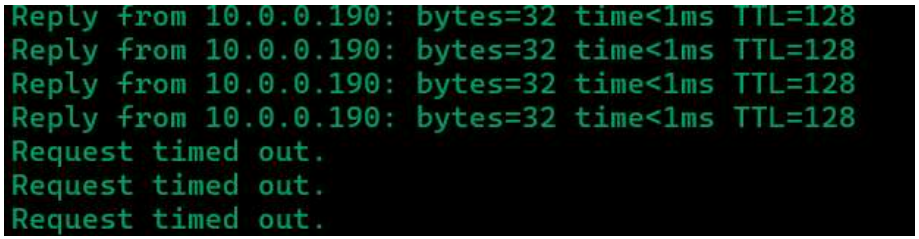


Using PS lets try to block the host. We will make a New-NetFirewallRule

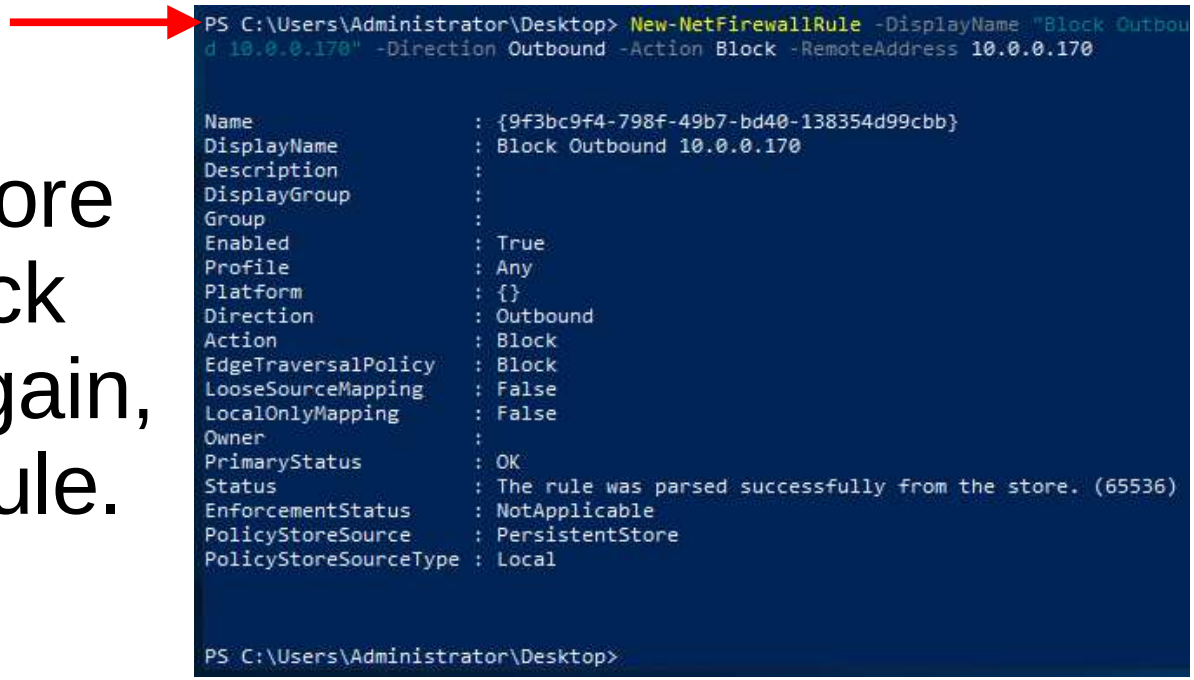
Once done properly you can go back and see if you are still receiving packets from the ping -t request.

It was successful as ping is now timing out.

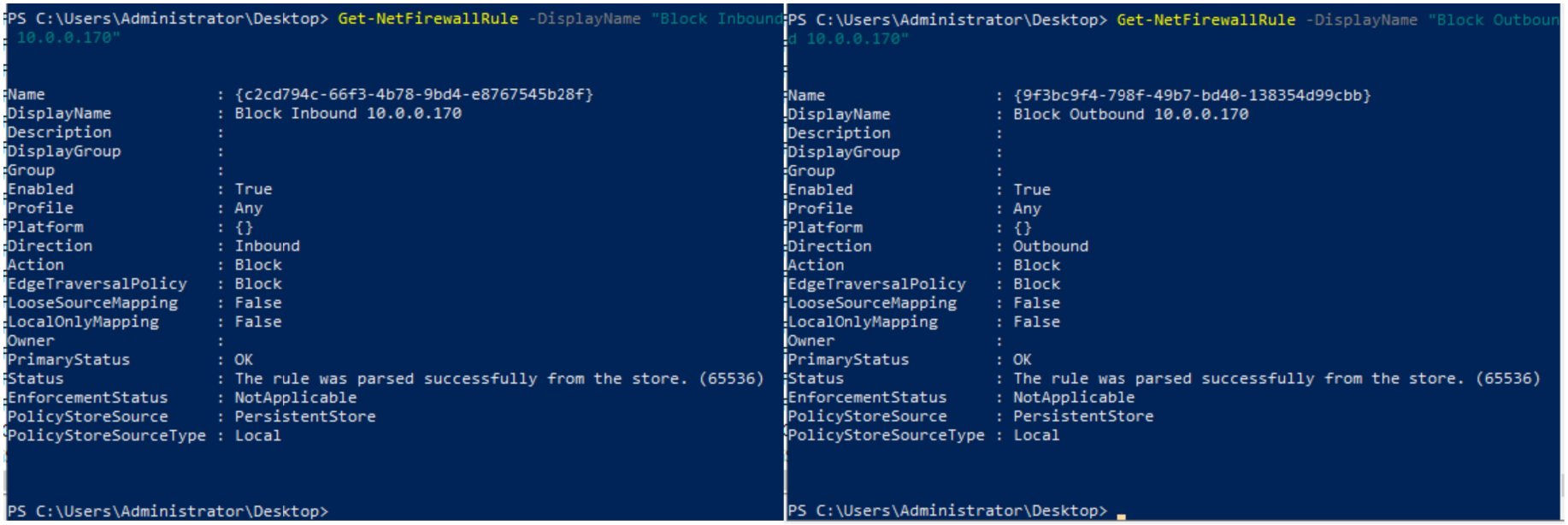




We can do a bit more and lets also Block Outbound traffic. Again, New-NetFirewallRule.

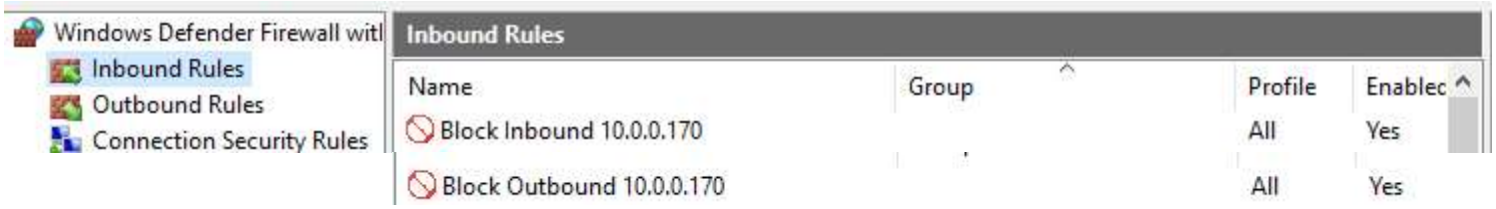


If you want to review the rules then we can Get-NetFirewallRule and you can always redirect to a file if needed.

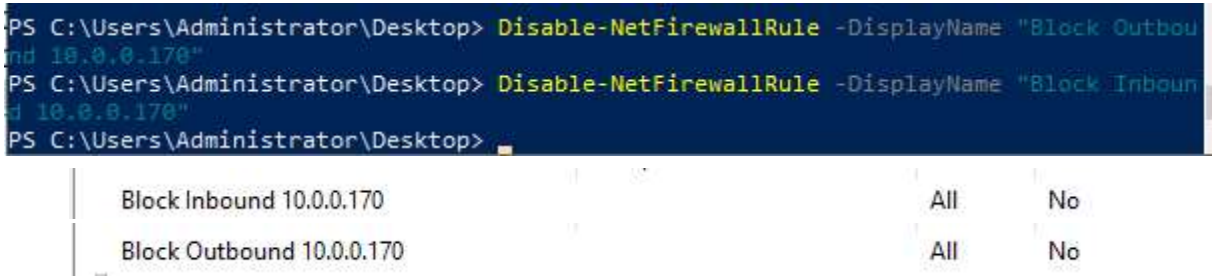


Lets check and see if the GUI Firewall has updated to reflect our changes.

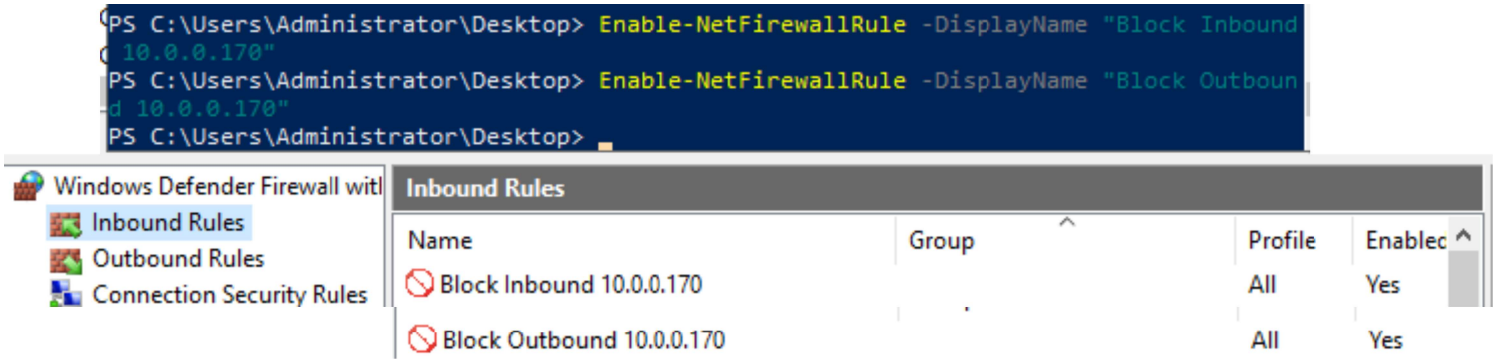
It sure has and we see instead of the green check or nothing that we now have the Block symbol.



Lets disable the rules in PS and then check back in the GUI.

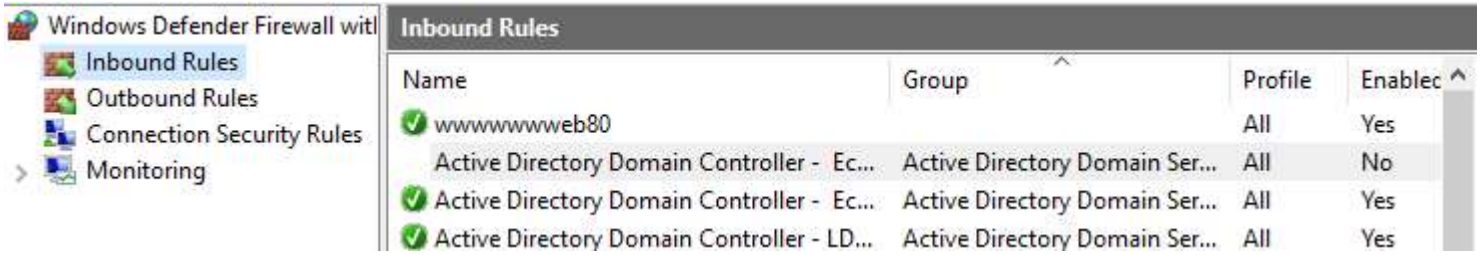


Ok, and if we enable them again we see the symbols update with our rules.



Ok, that is enough of that. Lets go ahead and remove those rules and check in the GUI as well.

```
PS C:\Users\Administrator\Desktop> Remove-NetFirewallRule -DisplayName "Block Outboun
d 10.0.0.170"
PS C:\Users\Administrator\Desktop> Remove-NetFirewallRule -DisplayName "Block Inbound
 10.0.0.170"
PS C:\Users\Administrator\Desktop>
```

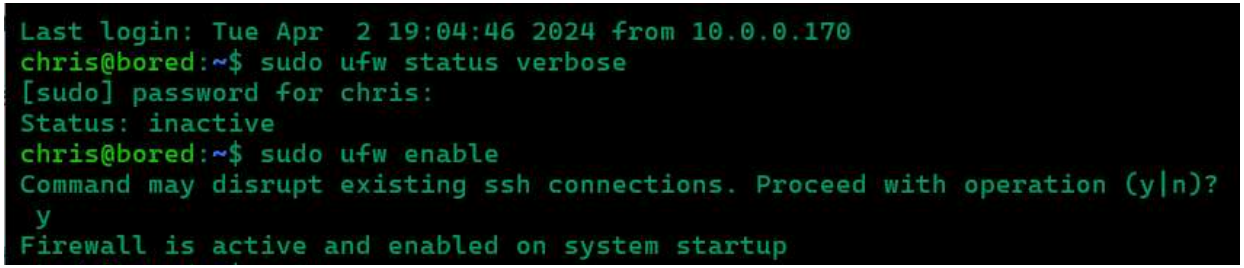


Well, hopefully we have learned a little about Windows Firewall settings and how to adjust them.

Now, what about Linux? Lets keep this wild ride going...

First up do we have an **u**buntu **f**ire**w**all (ufw) up? Check the status but we need to elevate privilages so enter “sudo ufw status” (we can use verbose for a bit more also)

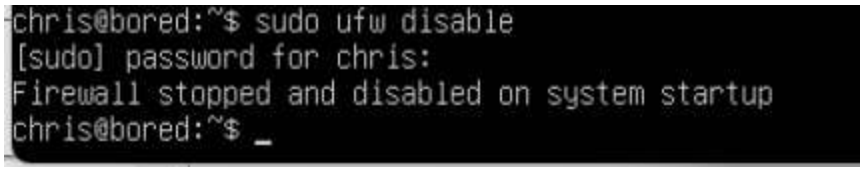
Status: Inactive tells us the ufw is currently off so lets enable with “sudo ufw enable”



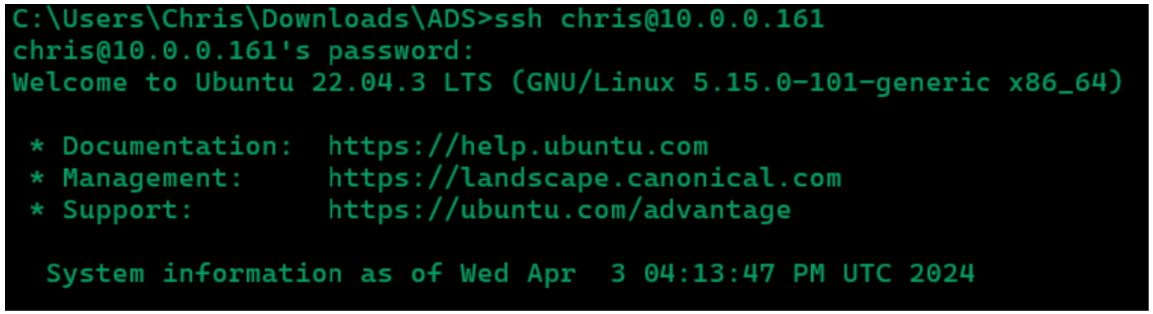
Now that we have turned it on lets exit and try to SSH back in...

```
chris@bored:~$ exit
logout
Connection to 10.0.0.161 closed.

C:\Users\Chris\Downloads\ADS>ssh chris@10.0.0.161
ssh: connect to host 10.0.0.161 port 22: Connection timed out
```

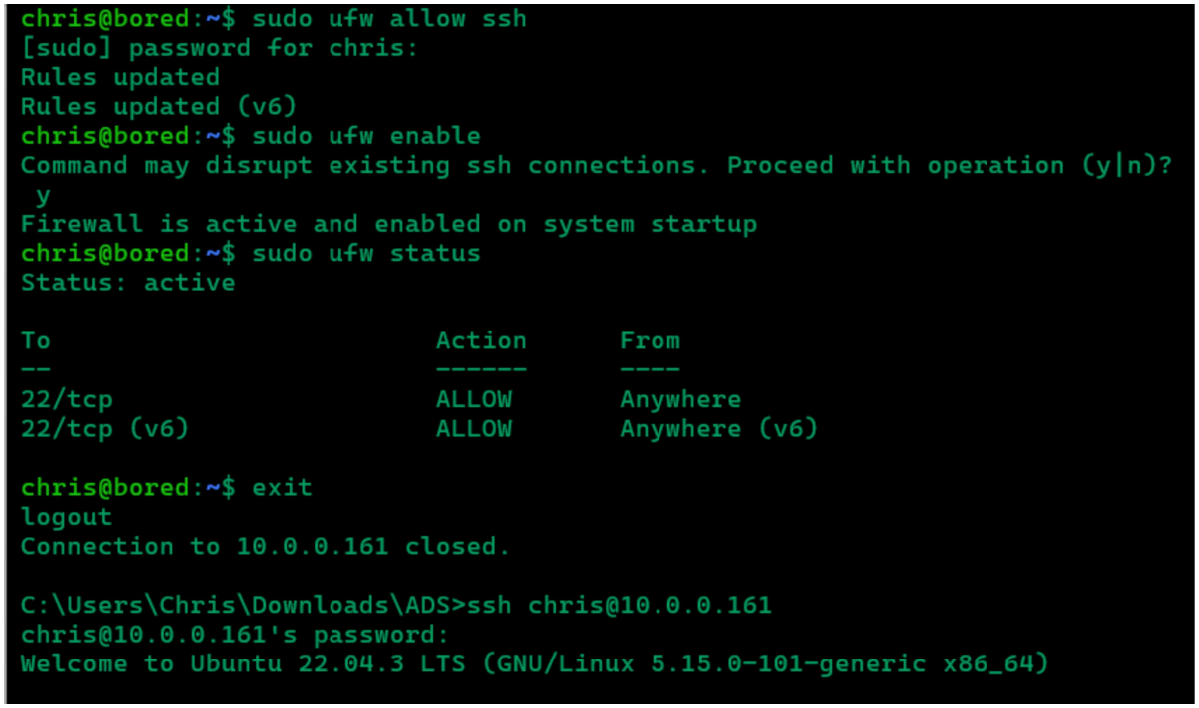
No worries, but we just have to swap over to the VM and disable the ufw.



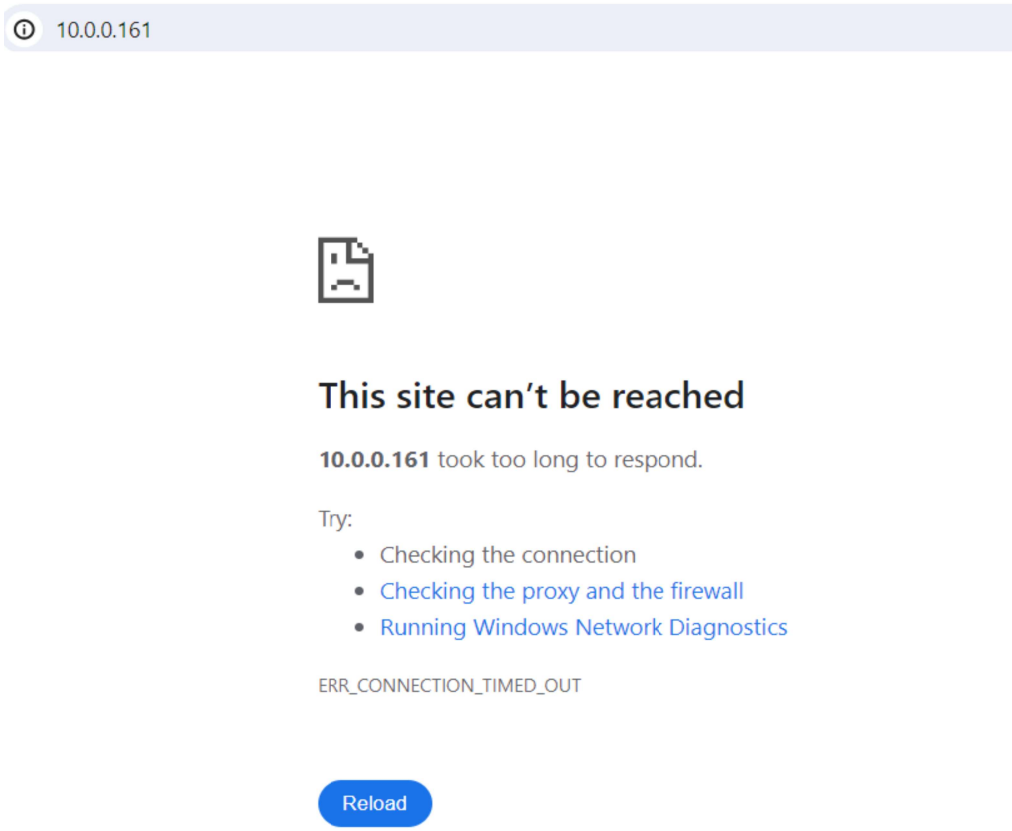
Back in, so now lets enable but not kill the SSH ability.



We can just allow SSH “sudo ufw allow ssh” and then enable it “sudo ufw enable”. A quick status check, “sudo ufw status” shows us ssh is allowed. We can then verify by exiting and see if we can remove back in.

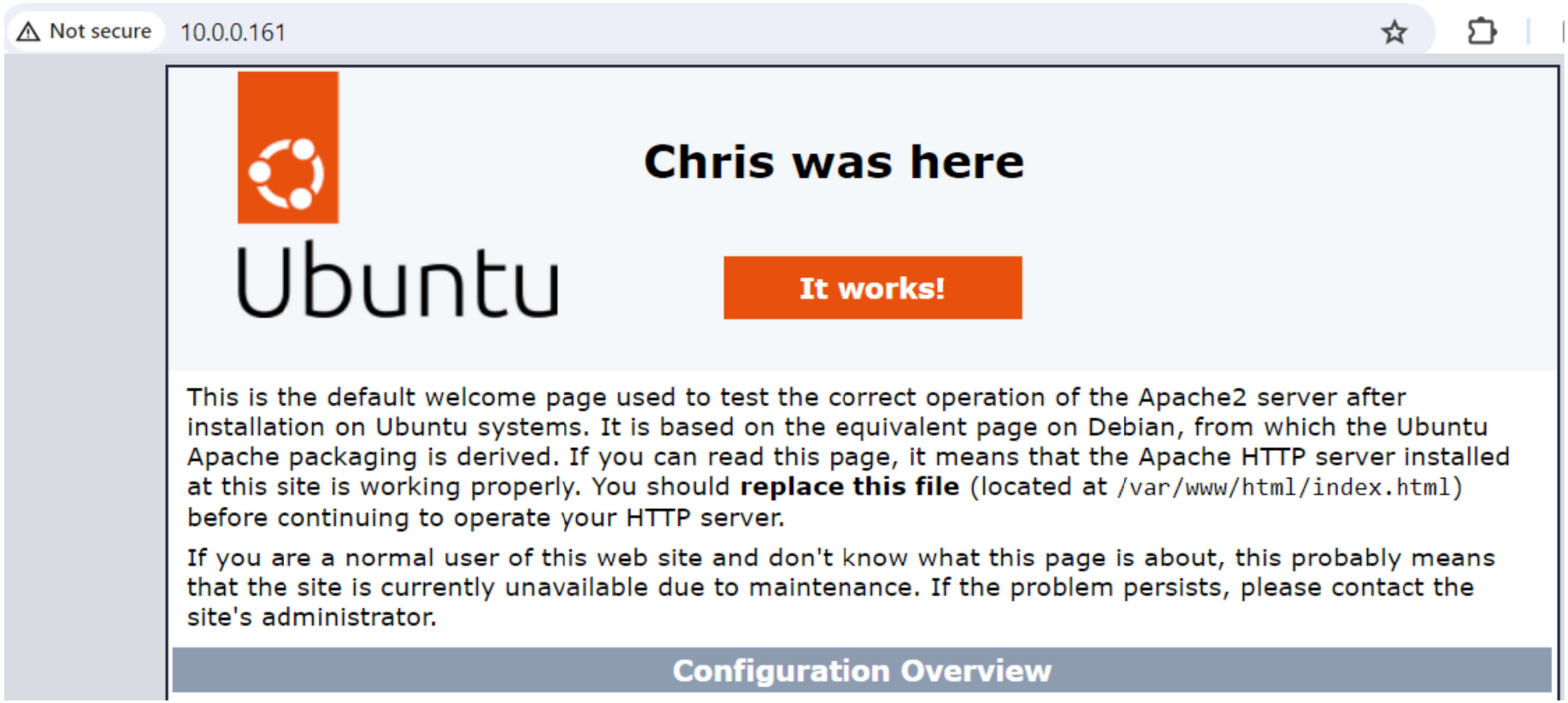


We have now turned on the firwall and enabled SSH but what about our server? Doh, looks like we are blocked.



Ok, I guess a quick disable should fix (temporarily)

```
chris@bored:~$ sudo ufw disable
Firewall stopped and disabled on system startup
chris@bored:~$
```



Lets try to fix a better way and try “sudo ufw allow http”

Success!

```
chris@bored:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)?
 y
Firewall is active and enabled on system startup
chris@bored:~$ sudo ufw allow http
Rule added
Rule added (v6)
chris@bored:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)

chris@bored:~$
```

Lets see if we can refine the rule set a bit more. First go ahead and delete the http rules.

```
chris@bored:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 4] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Add “numbered” to get the rule number to help you delete the correct rules.

```
chris@bored:~$ sudo ufw delete 2
Deleting:
 allow 80/tcp
Proceed with operation (y|n)? y
Rule deleted
chris@bored:~$ sudo ufw delete 3
Deleting:
 allow 80/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
chris@bored:~$
```

Confirm removal with a quick status check.

```
chris@bored:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

Next, lets restrict to our home network only for port 80 access.

```
chris@bored:~$ sudo ufw allow from 10.0.0.0/24 to any port 80
Rule added
chris@bored:~$ sudo ufw allow from 192.168.1.0/24 to any port 80
Rule added
chris@bored:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80                         ALLOW       10.0.0.0/24
80                         ALLOW       192.168.1.0/24
22/tcp (v6)                ALLOW       Anywhere (v6)

chris@bored:~$
```

We are going to allow 10.0.0.0/24 and 192.168.1.0/24

Well, how was it? Any thoughts?

Personally, I am a fan of Linux but if you put me in Windows I think GUI is for me.

However, we are cybersecurity professionals which means...we have to know it all. If weaker in an area make sure to spend a little extra time in it.