

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.

```
C:\Users\Chris>ping 10.0.0.190

Pinging 10.0.0.190 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.190:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

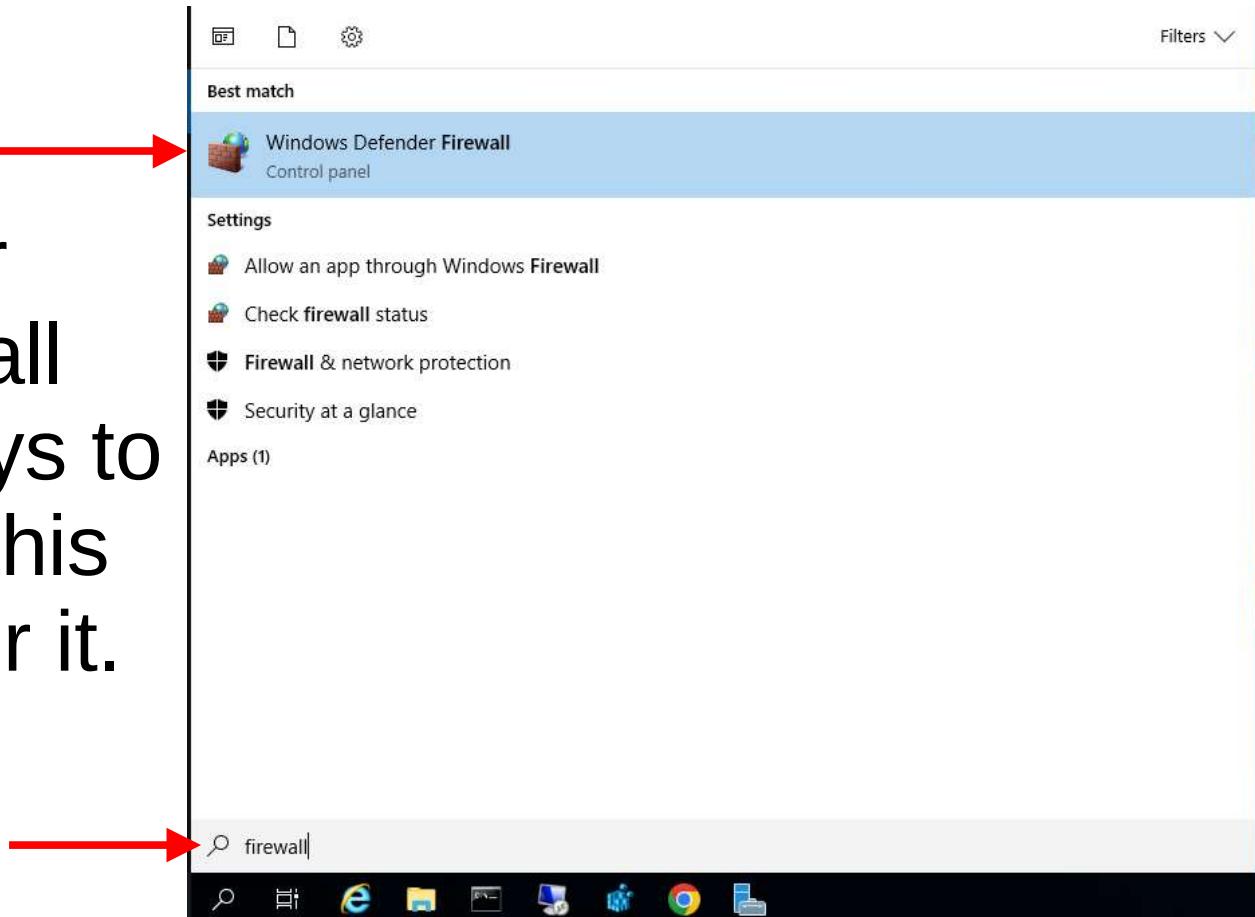
C:\Users\Chris>nmap 10.0.0.190
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-02 20:00 Mountain Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.76 seconds
```

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:	Internet Address	Type
192.168.56.1 --- 0x5		
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		
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

The screenshot shows the Windows Defender Firewall settings in the Control Panel. On the left, there's a sidebar with links like 'Allow an app or feature through Windows Defender Firewall', 'Change notification settings', 'Turn Windows Defender Firewall on or off', 'Restore defaults', and 'Advanced settings'. A red arrow points from the text 'Next select Advanced' to the 'Advanced settings' link. The main pane displays network protection settings for 'Domain networks', 'Private networks', and 'Guest or public networks'. It shows that 'Private networks' is connected and 'Domain networks' is not connected. The 'Windows Defender Firewall state' is set to 'On'. Under 'Incoming connections', it says 'Block all connections to apps that are not on the list of allowed apps'. Under 'Active private networks', it lists 'Network'. Under 'Notification state', it says 'Do not notify me when Windows Defender Firewall blocks a new app'.

Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Network Type	Status	Action
Domain networks	Not connected	<input type="checkbox"/>
Private networks	Connected	<input checked="" type="checkbox"/>
Guest or public networks	Not connected	<input type="checkbox"/>

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network

Notification state: Do not notify me when Windows Defender Firewall blocks a new app

See also

[Security and Maintenance](#)

[Network and Sharing Center](#)

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.

Distributed Transaction Coordinator (TCP... ✓ DNS (TCP, Incoming) ✓ DNS (UDP, Incoming) ✓ RPC (TCP, Incoming) ✓ RPC Endpoint Mapper (TCP, Incoming)	Distributed Transaction Co... DNS Service DNS Service DNS Service DNS Service	All All All All All	No Yes Yes Yes Yes
File and Printer Sharing (Echo Request - I... ✓ File and Printer Sharing (LLMNR-UDP-In) ✓ File and Printer Sharing (LLMNR-UDP-In) ✓ File and Printer Sharing (NB-Datagram-In) ✓ File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing File and Printer Sharing	Private Domai... Private Domai... Domai... Private Private Domai...	No Yes Yes Yes Yes Yes Yes Yes
File and Printer Sharing (Echo Request - I... ✓ File and Printer Sharing (LLMNR-UDP-In) ✓ File and Printer Sharing (LLMNR-UDP-In) ✓ File and Printer Sharing (NB-Datagram-In) ✓ File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing File and Printer Sharing	Private Domai... Private Domai... Domai... Private Private Domai...	No Yes Yes Yes Yes Yes Yes Yes

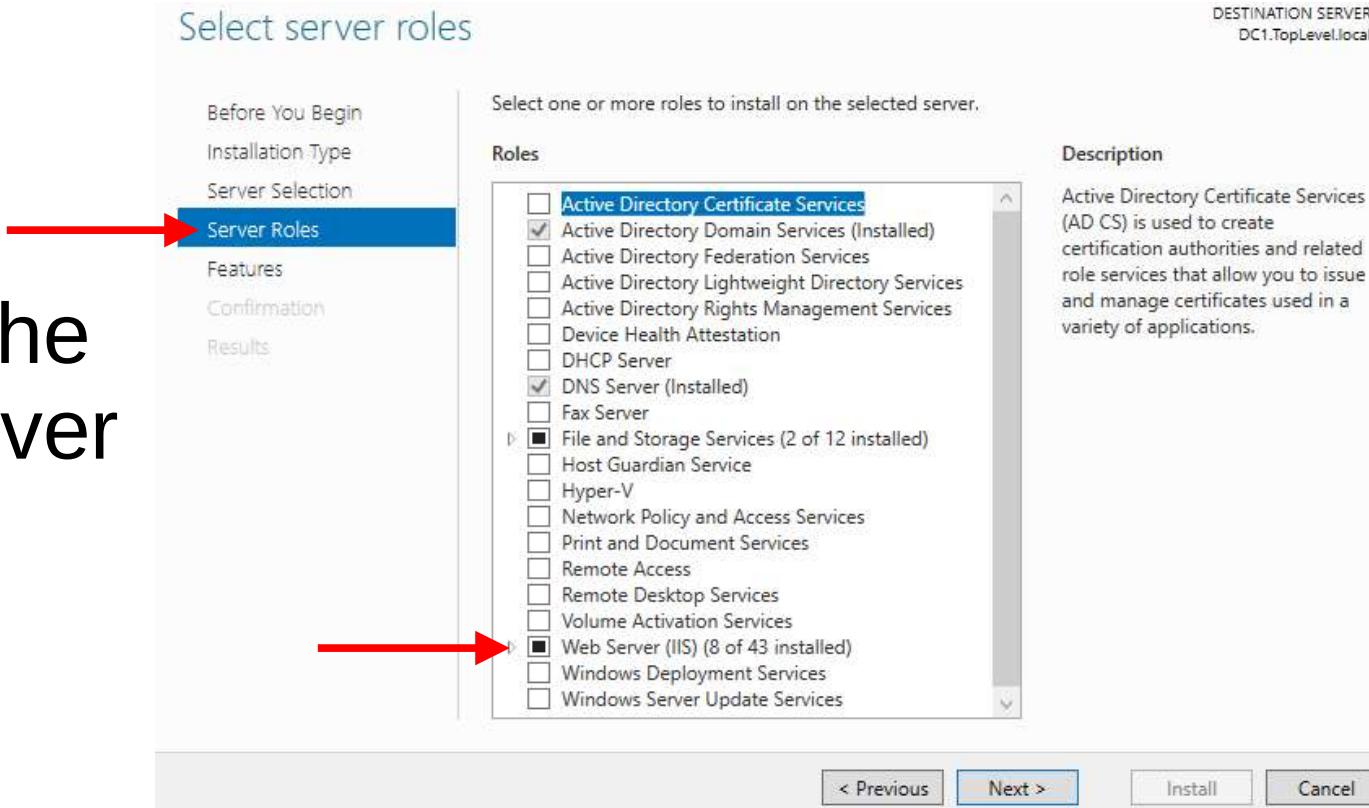
Distributed Transaction Coordinator (RP... ✓ DNS (TCP, Incoming) ✓ DNS (UDP, Incoming) ✓ RPC (TCP, Incoming) ✓ RPC Endpoint Mapper (TCP, Incoming)	Distributed Transaction Co... DNS Service DNS Service DNS Service DNS Service	All All All All	No Yes Yes Yes
File and Printer Sharing (Echo Request - I... ✓ File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing	Private Domai... Private Domai... Domai...	Yes Yes Yes Yes Yes
File and Printer Sharing (Echo Request - I... ✓ File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing	Private Domai... Private Domai... Domai...	Yes Yes Yes Yes Yes

```
C:\Users\Chris>ping 10.0.0.190 -t  
  
Pinging 10.0.0.190 with 32 bytes of data:  
Request timed out.  
Reply from 10.0.0.190: bytes=32 time=1ms TTL=128  
Reply from 10.0.0.190: bytes=32 time<1ms TTL=128  
Request timed out.  
Reply from 10.0.0.190: bytes=32 time=1ms TTL=128  
Reply from 10.0.0.190: bytes=32 time=2ms TTL=128  
Reply from 10.0.0.190: bytes=32 time<1ms TTL=128  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```

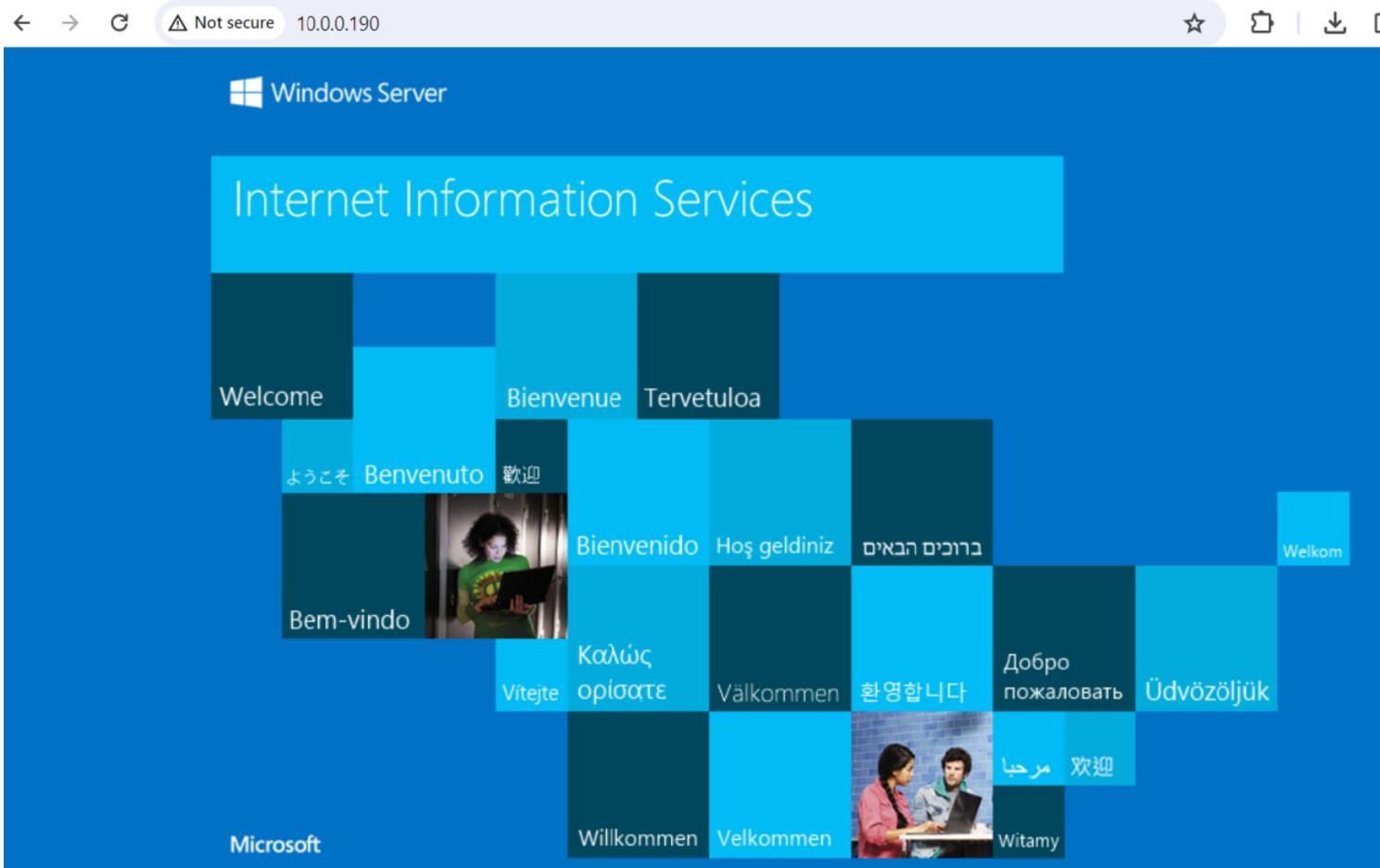
Switch back to our host and as you enable/disable watch for changes.

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

The screenshot shows a list of firewall rules in Windows Firewall with Advanced Security. A red arrow points to the last rule in the list, which is highlighted with a blue selection bar. The rule details are shown in a context menu on the right side of the screen.

Action	Name	Profile	Enabled
Windows Media Player Network Sharing ...	Windows Media Player Net...	All	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Domain	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Private...	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Private...	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Domain	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Private...	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Domain	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	All	No
Windows Media Player Network Sharing ...	Windows Media Player Net...	Domai...	No
✓ Windows Remote Management (HTTP-In)	Windows Remote Manage...	Public	Yes
✓ Windows Remote Management (HTTP-In)	Windows Remote Manage...	Domai...	Yes
Windows Remote Management - Compa...	Windows Remote Manage...	All	No
✓ Windows Security	Windows Security	Domai...	Yes
✓ Windows Security	Windows Security	Domai...	Yes
✓ Windows Security	Windows Security	Domai...	Yes
✓ Work or school account	Work or school account	Domai...	Yes
✓ Work or school account	Work or school account	Domai...	Yes
✓ Work or school account	Work or school account	Domai...	Yes
✓ World Wide Web Services (HTTP Traffic-In)	World Wide Web Services (...	All	Yes
✓ Your account	Your account	Domai...	Yes

Context menu options for the selected rule:

- Disable Rule (highlighted with a red arrow)
- Cut
- Copy
- Delete
- Properties
- Help

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

A screenshot of a web browser window. The address bar at the top shows the URL `10.0.0.190`. Below the address bar, there's a large, stylized icon of a sad face inside a square. The main content area has the following text:

This site can't be reached

10.0.0.190 took too long to respond.

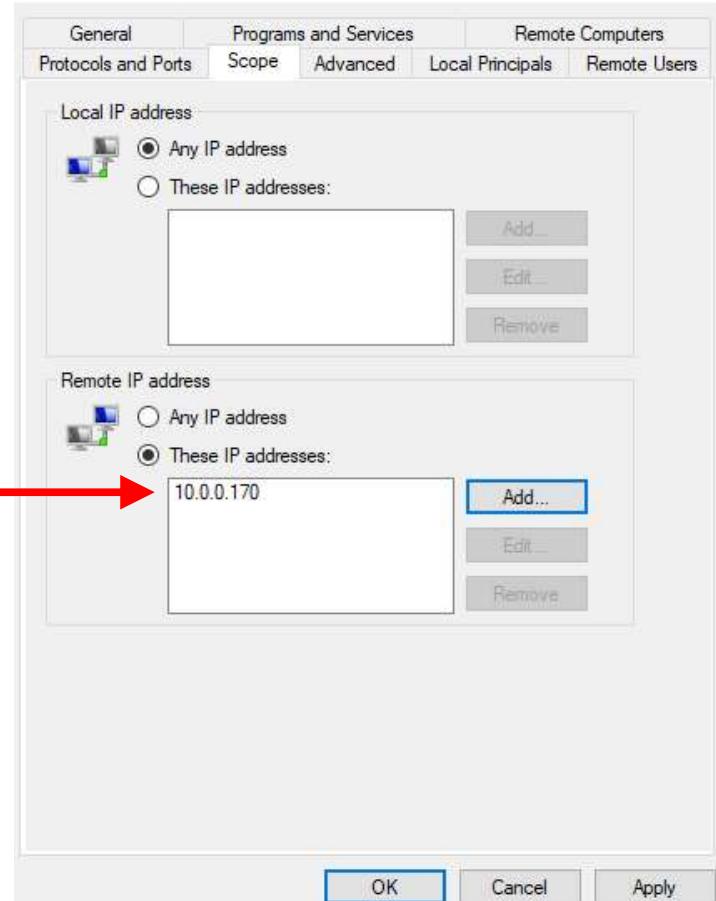
Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

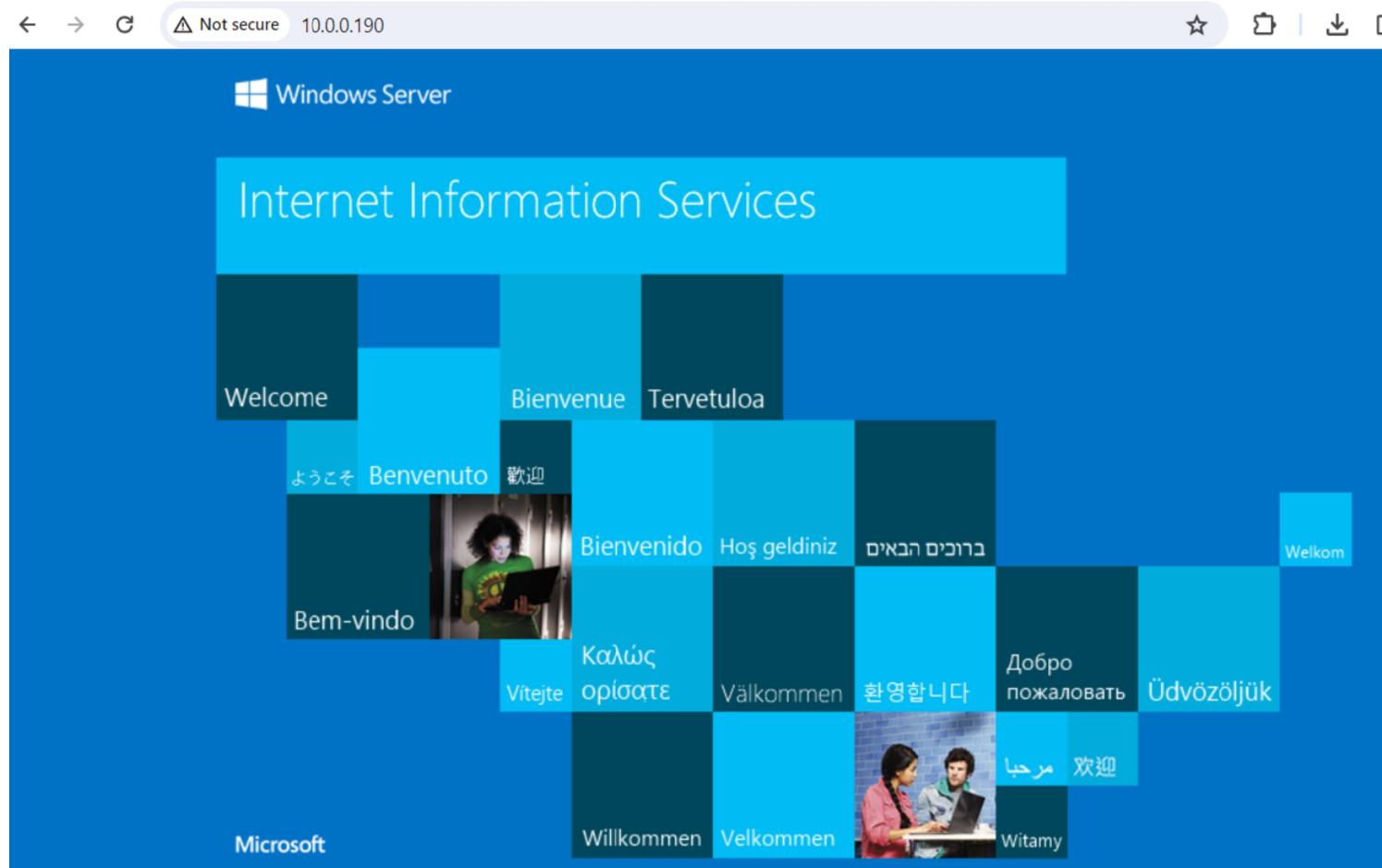
ERR_CONNECTION_TIMED_OUT

At the bottom of the page, there are two buttons: a blue "Reload" button on the left and a white "Details" button with a thin border on the right.

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



```
PS C:\Users\Administrator\Desktop> Get-NetFirewallRule

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

Name          : vm-monitoring-icmpv6
DisplayName   : Virtual Machine Monitoring (Echo Request - ICMPv6-In)
Description   : Echo Request messages are sent as ping requests to other nodes.
```

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



```
PS C:\Users\Administrator> Get-NetFirewallRule > Net_Firewall_Rule.txt
```

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
```

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.

```
PS C:\Users\Administrator\Desktop> New-NetFirewallRule -DisplayName "Block Inbound 10.0.0.170" -Direction Inbound -Action Block -RemoteAddress 10.0.0.170

Name : {c2cd794c-66f3-4b78-9bd4-e8767545b28f}
DisplayName : Block Inbound 10.0.0.170
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Block
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
```

```
PS C:\Users\Administrator\Desktop>
```

```
Reply from 10.0.0.190: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Request timed out.
```

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



```
PS C:\Users\Administrator\Desktop> New-NetFirewallRule -DisplayName "Block Outbound 10.0.0.170" -Direction Outbound -Action Block -RemoteAddress 10.0.0.170

Name          : {9f3bc9f4-798f-49b7-bd40-138354d99cbb}
DisplayName   : Block Outbound 10.0.0.170
Description   :
DisplayGroup :
Group         :
Enabled       : True
Profile       : Any
Platform      : {}
Direction     : Outbound
Action        : Block
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

PS C:\Users\Administrator\Desktop>
```

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

```
PS C:\Users\Administrator\Desktop> Get-NetFirewallRule -DisplayName "Block Inbound 10.0.0.170"
Name          : {c2cd794c-66f3-4b78-9bd4-e8767545b28f}
DisplayName   : Block Inbound 10.0.0.170
Description   :
DisplayGroup :
Group        :
Enabled       : True
Profile       : Any
Platform      : {}
Direction    : Inbound
Action        : Block
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

PS C:\Users\Administrator\Desktop> Get-NetFirewallRule -DisplayName "Block Outbound 10.0.0.170"
Name          : {9f3bc9f4-798f-49b7-bd40-138354d99cbb}
DisplayName   : Block Outbound 10.0.0.170
Description   :
DisplayGroup :
Group        :
Enabled       : True
Profile       : Any
Platform      : {}
Direction    : Outbound
Action        : Block
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

PS C:\Users\Administrator\Desktop>
```

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.

```
PS C:\Users\Administrator\Desktop> Disable-NetFirewallRule -DisplayName "Block Outbound 10.0.0.170"
PS C:\Users\Administrator\Desktop> Disable-NetFirewallRule -DisplayName "Block Inbound 10.0.0.170"
PS C:\Users\Administrator\Desktop>
```

Name	Group	Profile	Enabled
Block Inbound 10.0.0.170	All	No	
Block Outbound 10.0.0.170	All	No	

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

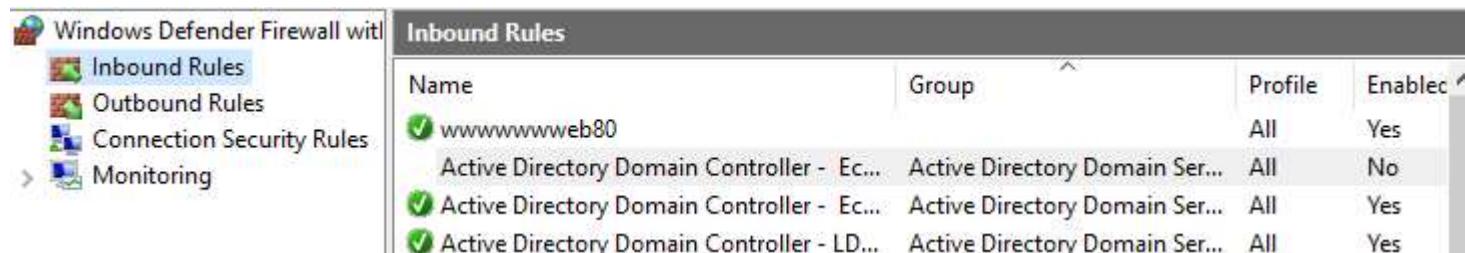
```
PS C:\Users\Administrator\Desktop> Enable-NetFirewallRule -DisplayName "Block Inbound 10.0.0.170"
PS C:\Users\Administrator\Desktop> Enable-NetFirewallRule -DisplayName "Block Outbound 10.0.0.170"
PS C:\Users\Administrator\Desktop>
```

The screenshot shows the Windows Defender Firewall with Advanced Security interface. On the left, there's a navigation pane with three options: 'Inbound Rules' (selected), 'Outbound Rules', and 'Connection Security Rules'. The main area is titled 'Inbound Rules' and contains a table with the following data:

Name	Group	Profile	Enabled
Block Inbound 10.0.0.170	All	Yes	
Block Outbound 10.0.0.170	All	Yes	

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 Outbound  
id 10.8.0.170"  
PS C:\Users\Administrator\Desktop> Remove-NetFirewallRule -DisplayName "Block Inbound  
10.8.0.170"  
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 **ubuntu firewall** (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**”

```
Last login: Tue Apr  2 19:04:46 2024 from 10.0.0.170
chris@bored:~$ sudo ufw status verbose
[sudo] password for chris:
Status: inactive
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
```

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.

```
chris@bored:~$ sudo ufw disable
[sudo] password for chris:
Firewall stopped and disabled on system startup
chris@bored:~$ _
```

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

```
C:\Users\Chris\Downloads\ADS>ssh chris@10.0.0.161
chris@10.0.0.161's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information as of Wed Apr  3 04:13:47 PM UTC 2024
```

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.

```
chris@bored:~$ sudo ufw allow ssh
[sudo] password for chris:
Rules updated
Rules updated (v6)
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 status
Status: active

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

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

C:\Users\Chris\Downloads\ADS>ssh chris@10.0.0.161
chris@10.0.0.161's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-101-generic x86_64)
```

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

① 10.0.0.161



This site can't be reached

10.0.0.161 took too long to respond.

Try:

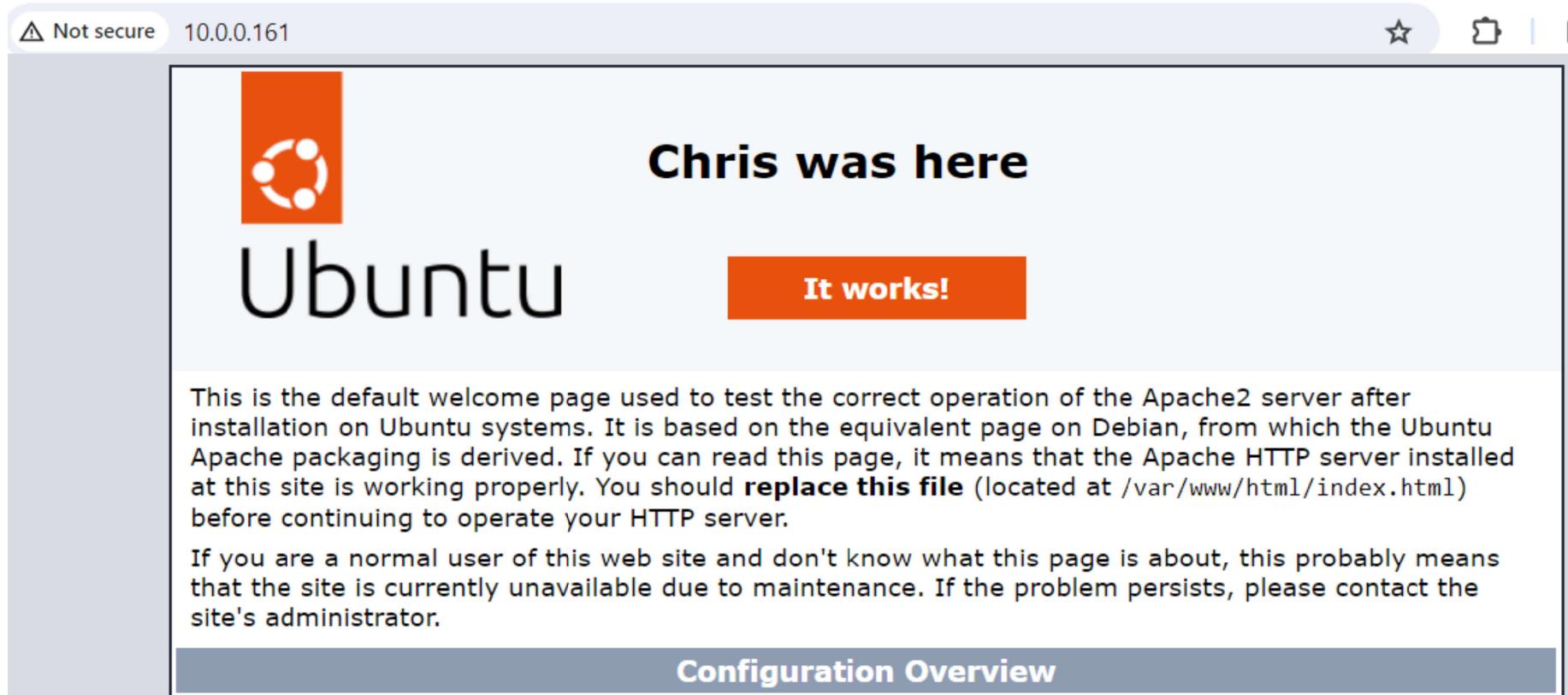
- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

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

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



A screenshot of a web browser window. The address bar shows 'Not secure' and '10.0.0.161'. The page itself is the standard Apache2 'It works!' test page. It features the Ubuntu logo (a white circle icon on an orange square) and the word 'Ubuntu' in large black letters. To the right of the logo, the text 'Chris was here' is displayed. Below this, there's an orange button with the text 'It works!'. A descriptive paragraph explains the purpose of the page: 'This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.' At the bottom, there's a blue button labeled 'Configuration Overview'.

Not secure 10.0.0.161

Chris was here

Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

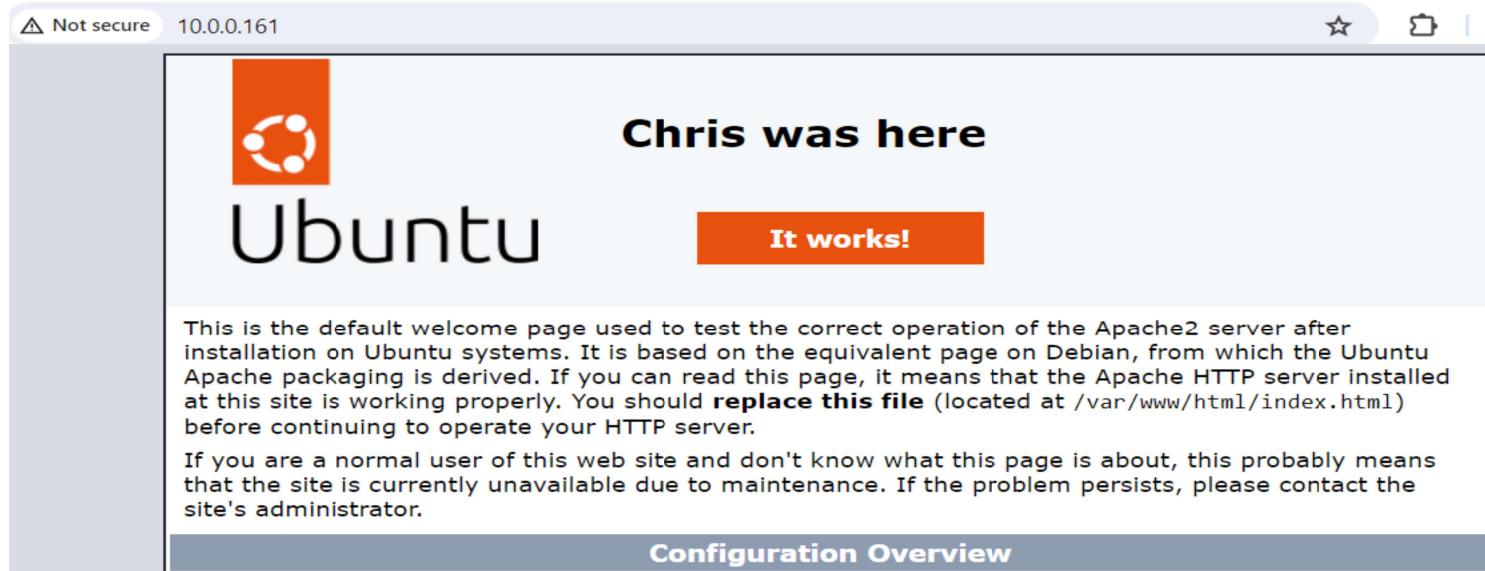
Lets try to fix a better way and try “sudo ufw allow http”

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.

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

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)

```
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)

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.

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

```
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:~$
```

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.