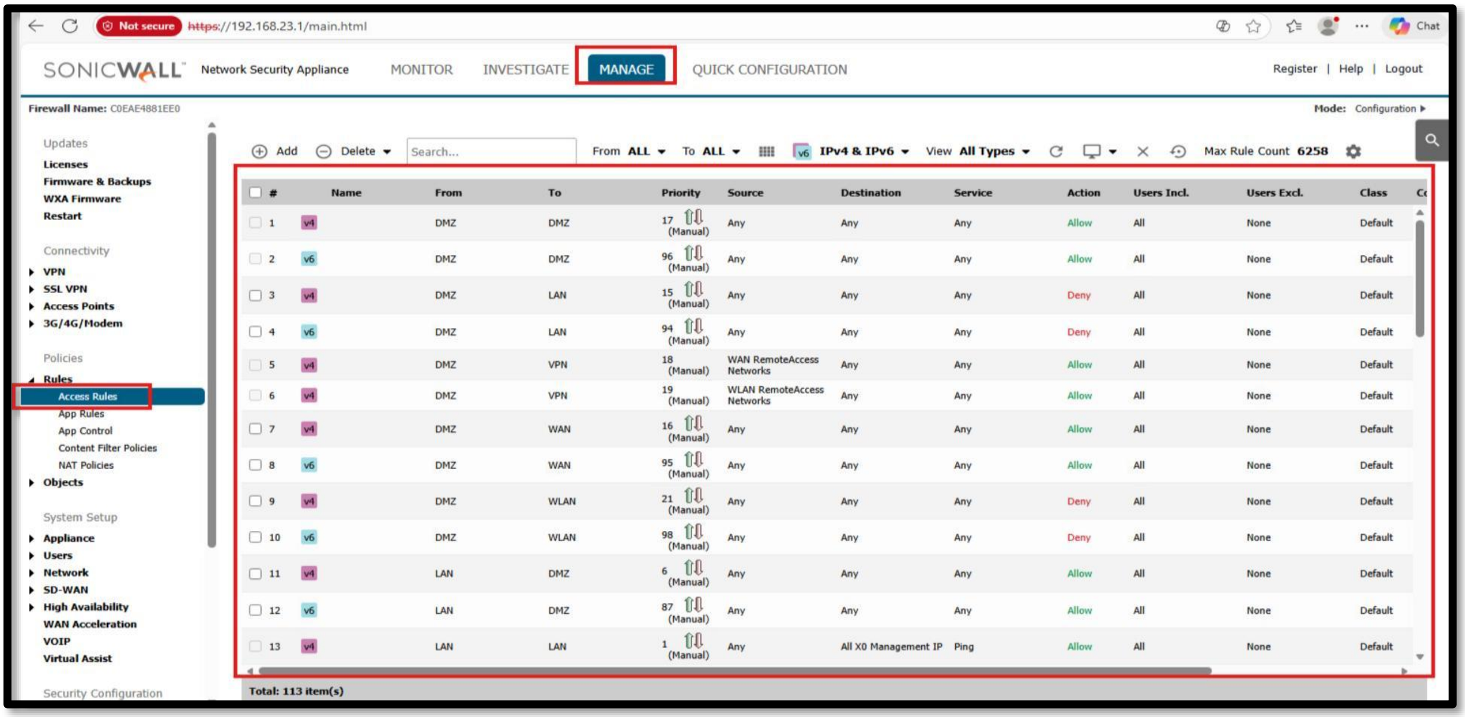
SonicWall Firewall

Project Summary: This project document provides a step-by-step procedure for configuring firewall rules on a SonicWall device to test specific network restrictions. The tests cover blocking access to a website, disabling ping (ICMP) requests, restricting Remote Desktop Protocol (RDP) traffic, and blocking DNS queries. Each test includes detailed setup instructions, rule configuration steps, and procedures to verify that the restrictions are working as intended. This guide is intended for network administrators, security engineers, or anyone looking to understand and implement granular network control and firewall testing in a controlled environment. By following this document, users will gain hands-on experience with SonicWall firewall rule creation, policy enforcement, and network traffic testing.

Firewall Rule: A firewall rule acts like a road sign for network traffic, indicating whether specific traffic is allowed or blocked between zones, such as WAN to LAN or LAN to WAN. Each rule defines the type of traffic, source and destination IPs, ports, and protocols that are permitted or denied. Properly configured firewall rules are essential for protecting sensitive resources, preventing unauthorized access, and maintaining compliance with security policies. Beyond simply allowing or blocking traffic, firewall rules also help in traffic segmentation, monitoring network activity, prioritizing critical applications, and mitigating threats like malware or unauthorized remote access. Understanding how to design and implement effective firewall rules demonstrates practical network security skills that are highly valuable for enterprise IT environments. To create or manage a firewall rule, you define the conditions under which network traffic is allowed or denied, including the source and destination IP addresses, ports, protocols, and zones. Effective rule management ensures secure communication, prevents unauthorized access, and maintains network performance. Regular monitoring and updates to firewall rules are essential to adapt to changing network requirements and emerging security threats.

To create or manage a firewall rule in SonicWall simply go to:
SonicWall Dashboard > Manage > Rules > Access Rules > You can see all the rules below:



□ #	Name	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Class	Co
□ 1	v4	DMZ	DMZ	17 (Manual)	Any	Any	Any	Allow	All	None	Default	
□ 2	v6	DMZ	DMZ	96 (Manual)	Any	Any	Any	Allow	All	None	Default	
□ 3	v4	DMZ	LAN	15 (Manual)	Any	Any	Any	Deny	All	None	Default	
□ 4	v6	DMZ	LAN	94 (Manual)	Any	Any	Any	Deny	All	None	Default	
□ 5	v4	DMZ	VPN	18 (Manual)	WAN RemoteAccess Networks	Any	Any	Allow	All	None	Default	
□ 6	v4	DMZ	VPN	19 (Manual)	WLAN RemoteAccess Networks	Any	Any	Allow	All	None	Default	
□ 7	v4	DMZ	WAN	16 (Manual)	Any	Any	Any	Allow	All	None	Default	
□ 8	v6	DMZ	WAN	95 (Manual)	Any	Any	Any	Allow	All	None	Default	
□ 9	v4	DMZ	WLAN	21 (Manual)	Any	Any	Any	Deny	All	None	Default	
□ 10	v6	DMZ	WLAN	98 (Manual)	Any	Any	Any	Deny	All	None	Default	
□ 11	v4	LAN	DMZ	6 (Manual)	Any	Any	Any	Allow	All	None	Default	
□ 12	v6	LAN	DMZ	87 (Manual)	Any	Any	Any	Allow	All	None	Default	
□ 13	v4	LAN	LAN	1 (Manual)	Any	All X0 Management IP	Ping	Allow	All	None	Default	

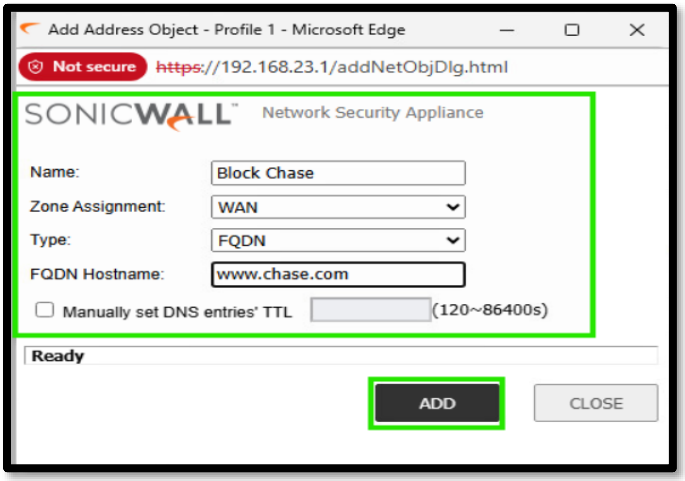
Total: 113 item(s)

SonicWall Firewall

Test 1: Block access to the website chase.com while allowing access to all other websites.

Step 1: Create Address Object

- SonicWall Dashboard > Manage > Objects > Click Address Objects > Add



Add Address Object - Profile 1 - Microsoft Edge

Not secure https://192.168.23.1/addNetObjDlg.html

SONICWALL Network Security Appliance

Name: Block Chase

Zone Assignment: WAN

Type: FQDN

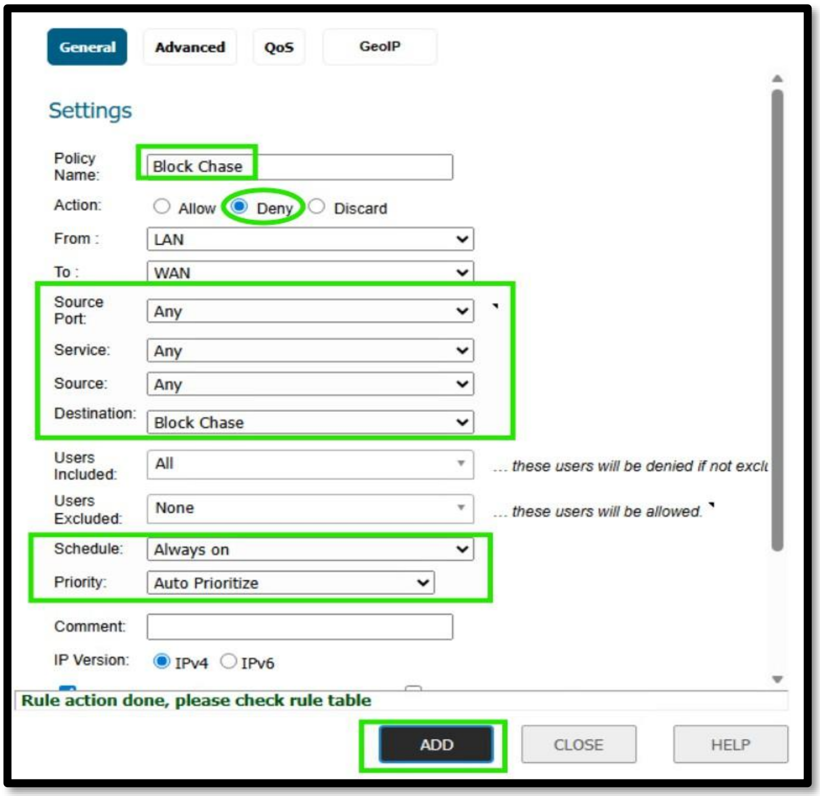
FQDN Hostname: www.chase.com

□ Manually set DNS entries' TTL (120~86400s)

Ready

Step 2: Create Firewall Rule

- Go to > Policies > Rules > Access Rules > Select From: LAN > To: WAN > Click Add
  - Policy Name: Block Chase
  - Action: Deny
  - Source Port: Any
  - Destination: Block Chase (the one that was created in address object)
  - Service: Any



Settings

Policy Name: Block Chase

Action: ○ Allow ● Deny ○ Discard

From : LAN

To : WAN

Source Port: Any

Service: Any

Source: Any

Destination: Block Chase

Users Included: All ... these users will be denied if not excl

Users Excluded: None ... these users will be allowed.

Schedule: Always on

Priority: Auto Prioritize

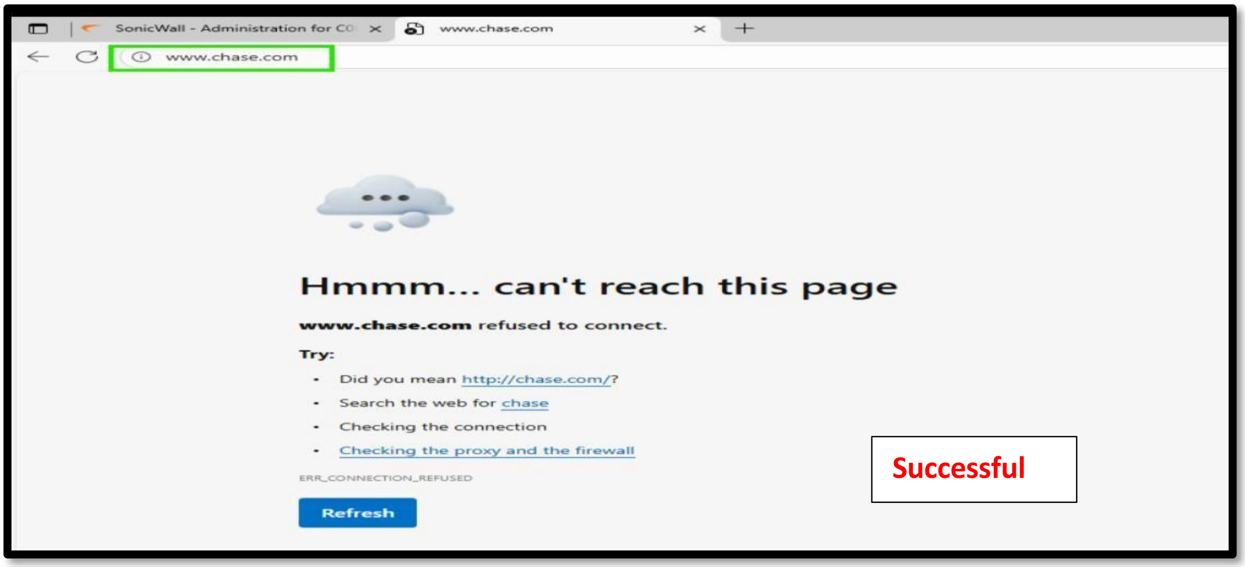
Comment:

IP Version: ● IPv4 ○ IPv6

Rule action done, please check rule table

Step 3: Test and Verify

- Open a browser from a PC > Go to www.chase.com



Hmmm... can't reach this page

www.chase.com refused to connect.

Try:

- Did you mean http://chase.com/?
- Search the web for chase
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

Refresh

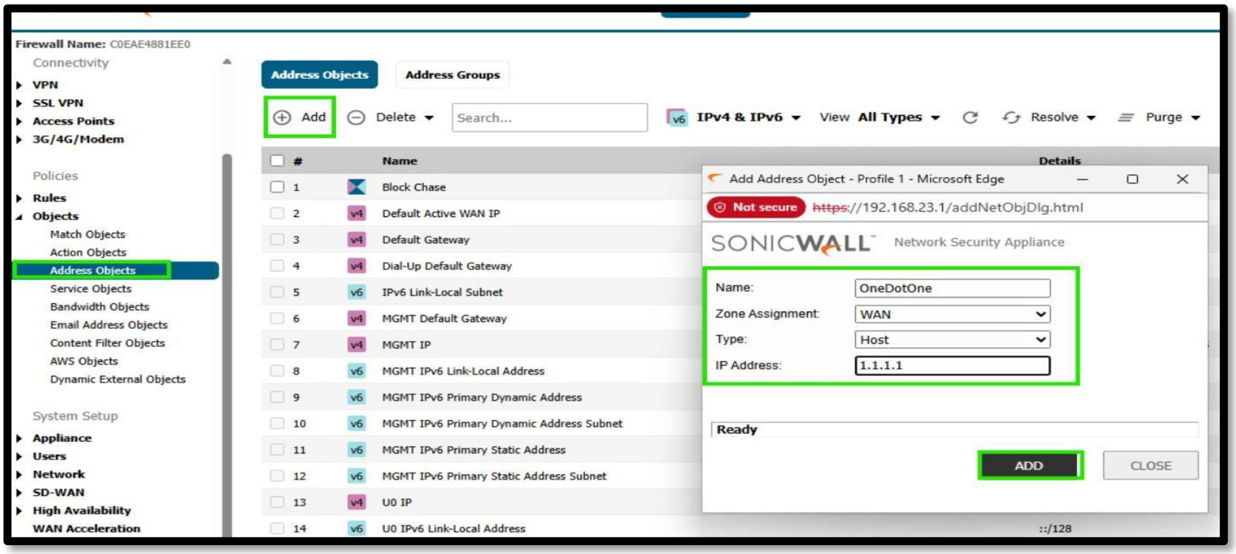
Successful

Conclusion: Because of the enforcement of the firewall rule and policy created to block access to chase.com, the user is unable to access the website from their browser within the company network, as the firewall actively blocks the request. This demonstrates the effectiveness of firewall policies in controlling network traffic, enforcing company security guidelines, and preventing access to unauthorized or potentially risky websites. The test also highlights the importance of properly defining rules, applying them to the correct zones, and verifying that traffic restrictions work as intended without impacting access to other websites or services.

Test 2: Block ICMP (ping) request to a specific IP (1.1.1.1) while allowing all other traffic.

Step 1: Create Address Object

- SonicWall Dashboard > Manage > Objects > Click Address Objects > Add



Firewall Name: C0EAE4881EE0

Connectivity
- VPN
- SSL VPN
- Access Points
- 3G/4G/Modem

Policies
- Rules
- Objects
  - Match Objects
  - Action Objects
  - Address Objects
  - Service Objects
  - Bandwidth Objects
  - Email Address Objects
  - Content Filter Objects
  - AWS Objects
  - Dynamic External Objects

System Setup
- Appliance
- Users
- Network
- SD-WAN
- High Availability
- WAN Acceleration

Address Objects | Address Groups

Add | Delete | Search... | IPv4 & IPv6 | View All Types | Resolve | Purge

#		Name	Details
1		Block Chase	
2	v4	Default Active WAN IP	
3	v4	Default Gateway	
4	v4	Dial-Up Default Gateway	
5	v6	IPv6 Link-Local Subnet	
6	v4	MGMT Default Gateway	
7	v4	MGMT IP	
8	v6	MGMT IPv6 Link-Local Address	
9	v6	MGMT IPv6 Primary Dynamic Address	
10	v6	MGMT IPv6 Primary Dynamic Address Subnet	
11	v6	MGMT IPv6 Primary Static Address	
12	v6	MGMT IPv6 Primary Static Address Subnet	
13	v4	U0 IP	
14	v6	U0 IPv6 Link-Local Address	::/128

Add Address Object - Profile 1 - Microsoft Edge

Not secure | ~~https~~://192.168.23.1/addNetObjDlg.html

SONICWALL Network Security Appliance

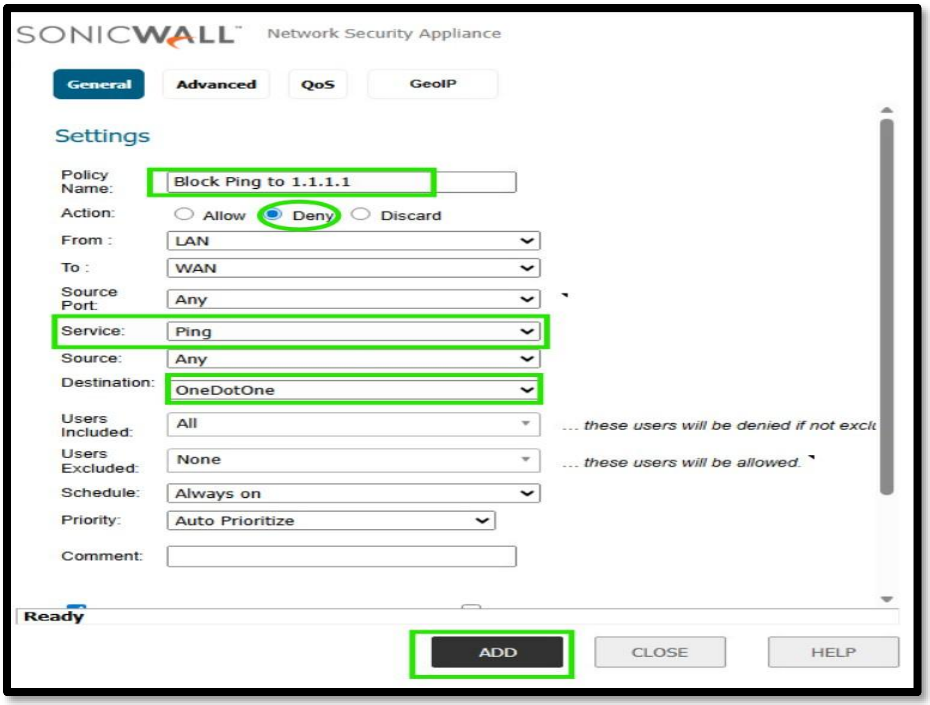
Name:	OneDotOne
Zone Assignment:	WAN
Type:	Host
IP Address:	1.1.1.1

Ready

ADD | CLOSE

Step 2: Create Firewall Rule

- Go to > Policies > Rules > Access Rules > LAN >WAN > Click Add > Policy Name: Block Ping
  - Action: Deny
  - Source Port: Any
  - Destination: OneDotOne (the one that was created in address object)
  - Service: Ping



SONICWALL Network Security Appliance

General | Advanced | QoS | GeoIP

Settings

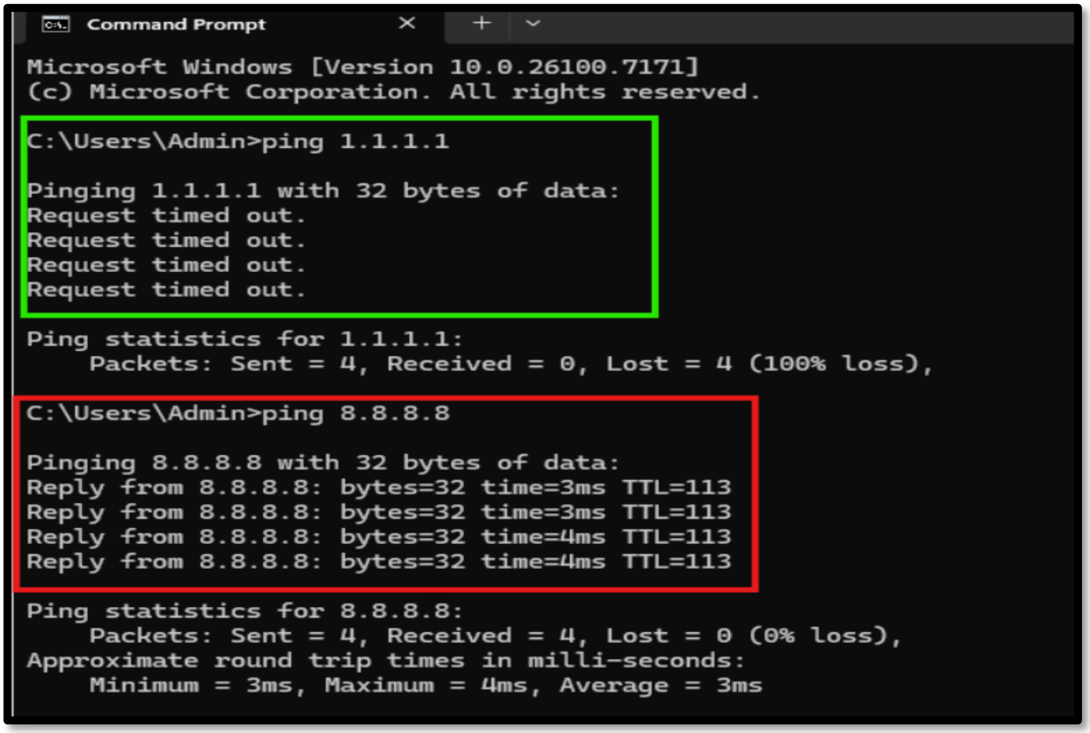
Policy Name:	Block Ping to 1.1.1.1
Action:	○ Allow ● Deny ○ Discard
From :	LAN
To :	WAN
Source Port:	Any
Service:	Ping
Source:	Any
Destination:	OneDotOne
Users Included:	All … these users will be denied if not excl
Users Excluded:	None … these users will be allowed.
Schedule:	Always on
Priority:	Auto Prioritize
Comment:	

Ready

ADD | CLOSE | HELP

Step 3: Test

- ➢ Open Command Prompt > Ping 1.1.1.1 > Verify



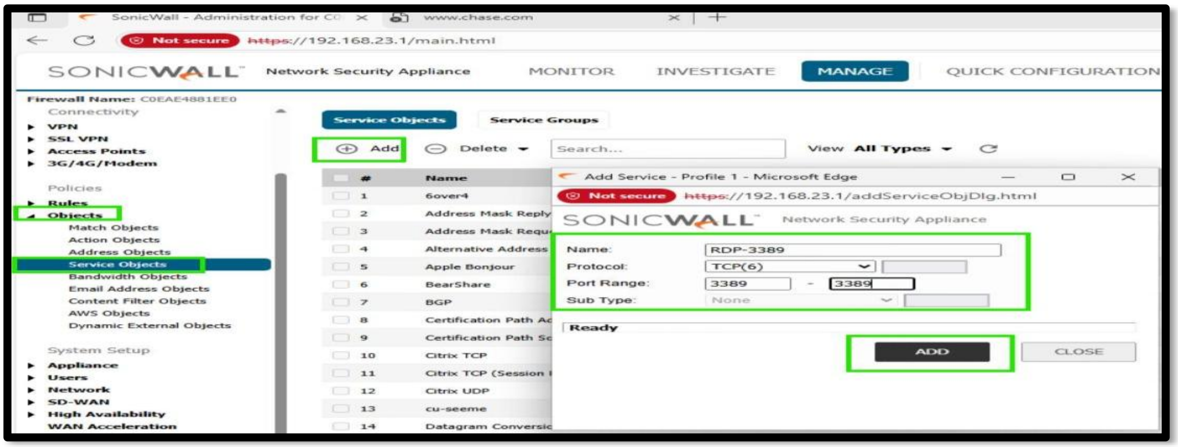
```
Microsoft Windows [Version 10.0.26100.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=3ms TTL=113
Reply from 8.8.8.8: bytes=32 time=3ms TTL=113
Reply from 8.8.8.8: bytes=32 time=4ms TTL=113
Reply from 8.8.8.8: bytes=32 time=4ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Conclusion: The user is unable to ping 1.1.1.1 because the firewall policy enforces the ICMP block rule. This demonstrates that the firewall is actively controlling network traffic, preventing unauthorized or unwanted requests while allowing all other types of traffic to function normally. It highlights practical skills in configuring and testing firewall rules for security and network management.

Test 3: Block RDP (Remote Desktop Protocol) traffic on port 3389 from LAN to WAN while allowing other traffic.

Step 1: Create Service

- ➢ Go to Objects > Click Service Objects > Add



Firewall Name: C0EAE4881EE0

#	Name
1	6over4
2	Address Mask Reply
3	Address Mask Requ
4	Alternative Address
5	Apple Bonjour
6	BearShare
7	BGP
8	Certification Path Ac
9	Certification Path Sc
10	Citrix TCP
11	Citrix TCP (Session I
12	Citrix UDP
13	cu-seeme
14	Datagram Conversic

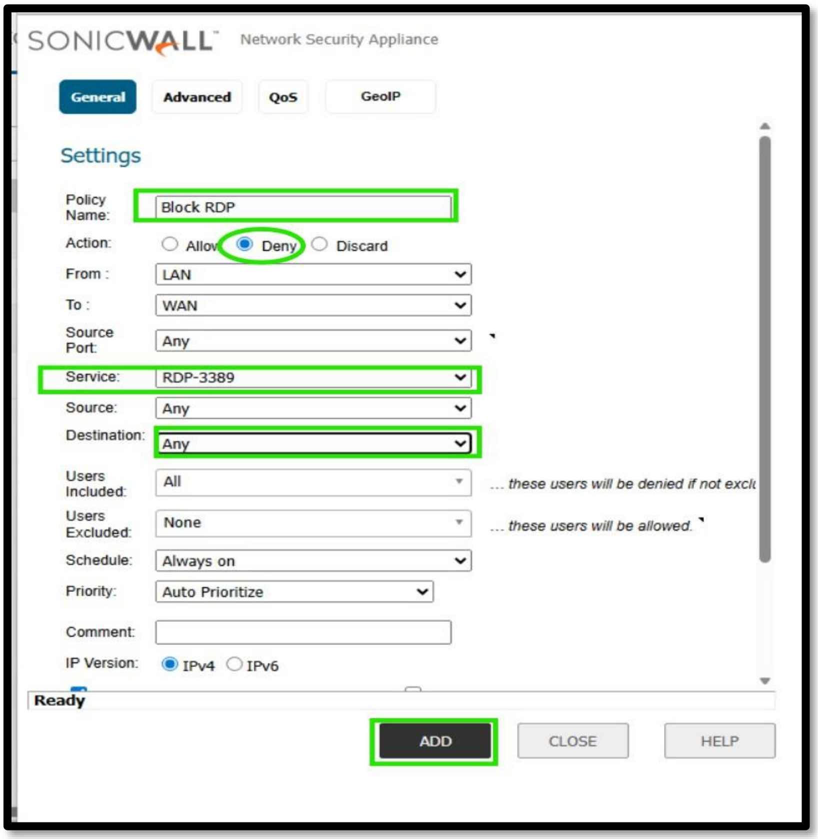
Name: RDP-3389
Protocol: TCP(6)
Port Range: 3389 - 3389
Sub Type: None

Ready

SonicWall Firewall

Step 2: Create Firewall Rule

- Go to > Policies > Rules > Access Rules > LAN >WAN > Click Add
  - Policy Name: Block RDP
  - Action: Deny
  - Source Port: Any
  - Service: RDP-3389
  - Destination: Any



Settings

Policy Name: Block RDP

Action: ○ Allow ● Deny ○ Discard

From : LAN

To : WAN

Source Port: Any

Service: RDP-3389

Source: Any

Destination: Any

Users Included: All ... these users will be denied if not excl

Users Excluded: None ... these users will be allowed.

Schedule: Always on

Priority: Auto Prioritize

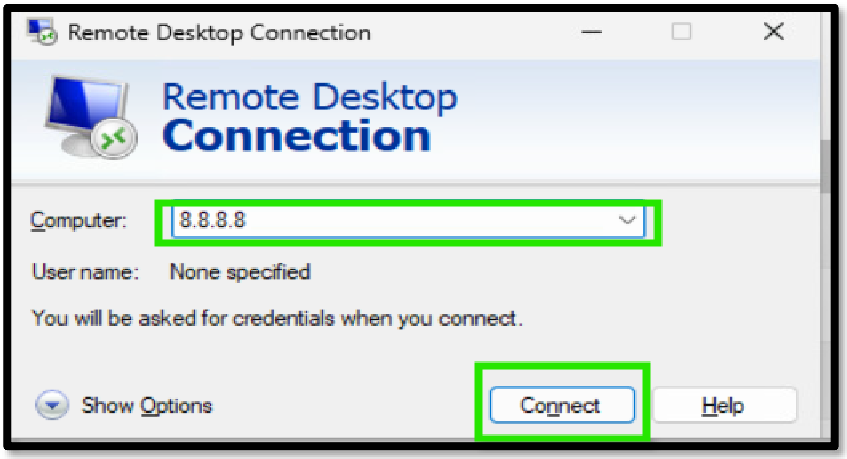
Comment:

IP Version: ● IPv4 ○ IPv6

Ready

Step 3: Test and Verify

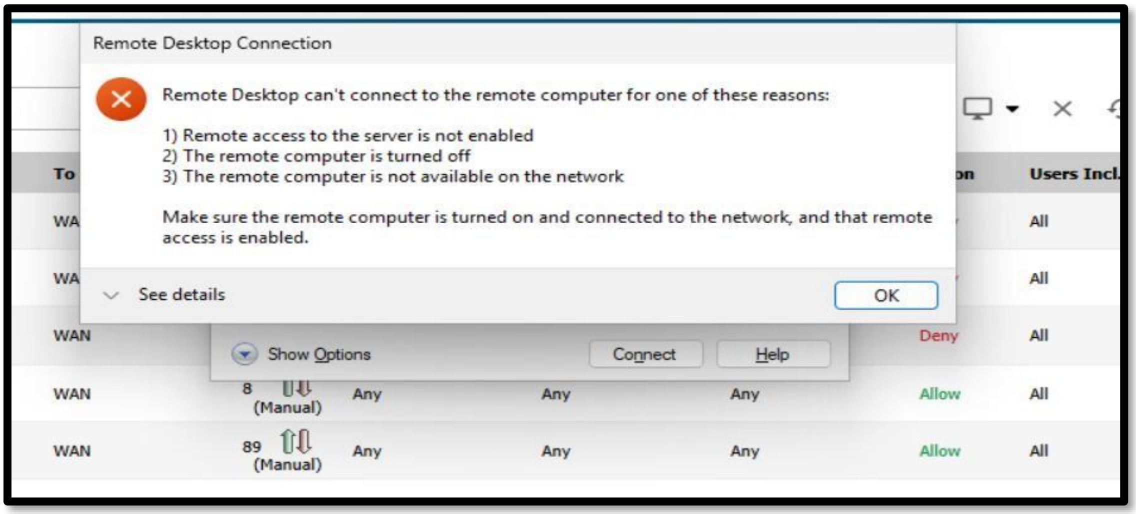
Open Remote Desktop (mstsc.exe) and attempt to connect to any public IP. The connection should fail, confirming that the firewall rule blocking RDP traffic from LAN to WAN is functioning correctly.



Computer: 8.8.8.8

User name: None specified

You will be asked for credentials when you connect.



Remote Desktop Connection

Remote Desktop can't connect to the remote computer for one of these reasons:

1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network

Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.

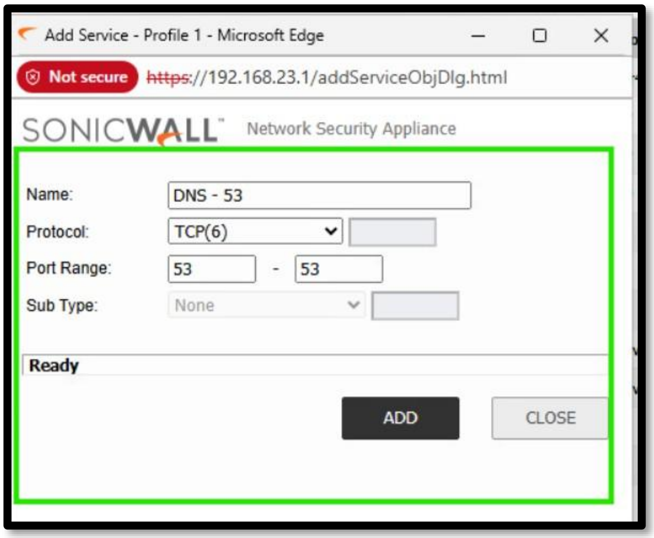
To						Users Incl.
WA						All
WA						All
WAN					Deny	All
WAN	8 (Manual)	Any	Any	Any	Allow	All
WAN	89 (Manual)	Any	Any	Any	Allow	All

Conclusion: This test demonstrates that RDP traffic from the LAN to the WAN can be successfully blocked using a firewall rule on port 3389, while allowing all other network traffic to function normally. It highlights the importance of properly defining firewall policies to secure remote access, prevent unauthorized connections, and maintain network integrity. The exercise reinforces practical skills in configuring, enforcing, and verifying firewall rules in a controlled enterprise environment.

Test 4: Block all DNS (Port 53) queries from a PC to prevent domain name resolution, while allowing other network traffic.

Step 1: Create Service Object

- ➢ Go to Objects > Click Service Objects > Add



Add Service - Profile 1 - Microsoft Edge

Not secure https://192.168.23.1/addServiceObjDlg.html

SONICWALL Network Security Appliance

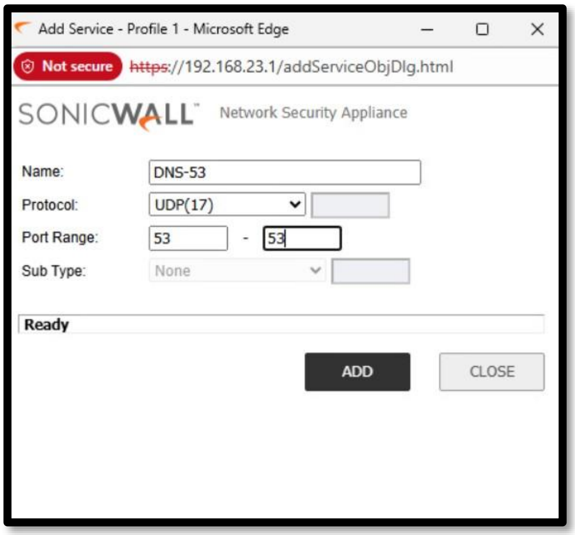
Name: DNS - 53

Protocol: TCP(6)

Port Range: 53 - 53

Sub Type: None

Ready



Add Service - Profile 1 - Microsoft Edge

Not secure https://192.168.23.1/addServiceObjDlg.html

SONICWALL Network Security Appliance

Name: DNS-53

Protocol: UDP(17)

Port Range: 53 - 53

Sub Type: None

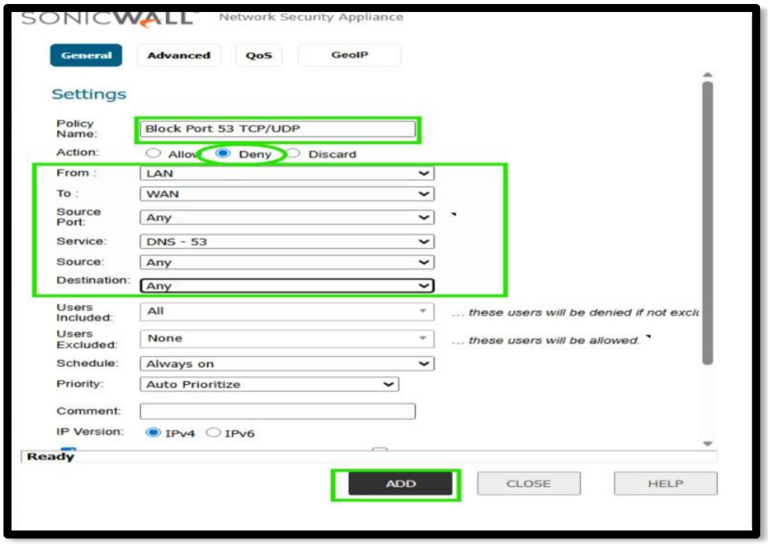
Ready

SonicWall Firewall

Step 2: Create Firewall Rule

- Go to > Policies > Rules > Access Rules > LAN >WAN > Click Add
    - Policy Name: Block Port 53 TCP/UDP
    - Action: Deny
    - Source Port: Any
    - Service: DNS-53
    - Source: Any
    - Destination: Any

- Important: Place this rule at the top of the LAN→WAN rules list to ensure it is evaluated first and effectively blocks DNS queries before other rules are applied.



Settings

Policy Name: Block Port 53 TCP/UDP

Action: ○ Allow ● Deny ○ Discard

From : LAN

To : WAN

Source Port: Any

Service: DNS - 53

Source: Any

Destination: Any

Users Included: All ... these users will be denied if not excl

Users Excluded: None ... these users will be allowed.

Schedule: Always on

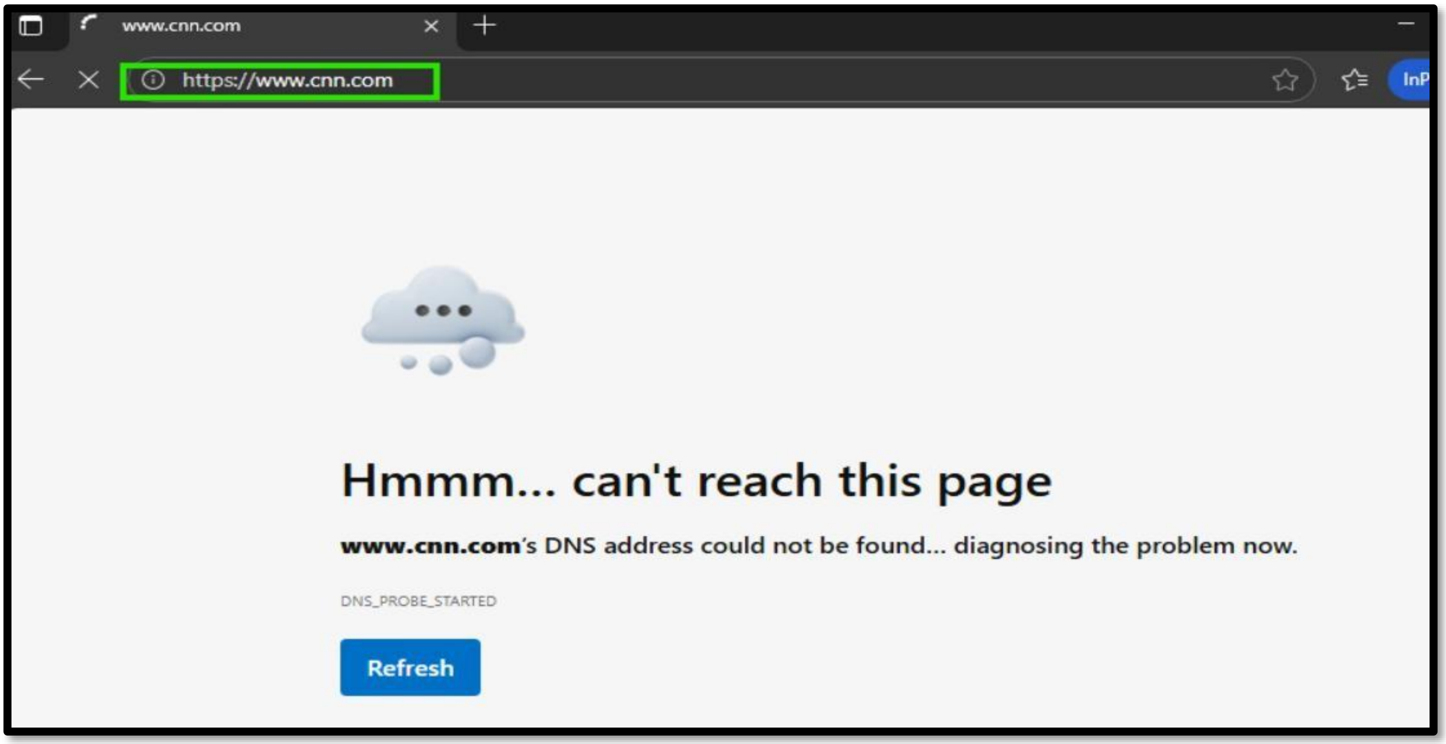
Priority: Auto Prioritize

Comment:

IP Version: ● IPv4 ○ IPv6

Step 3: Test and verify

- ➢ Open a web browser on the PC and attempt to visit cnn.com. The request should fail, confirming that DNS queries are successfully blocked by the firewall rule.

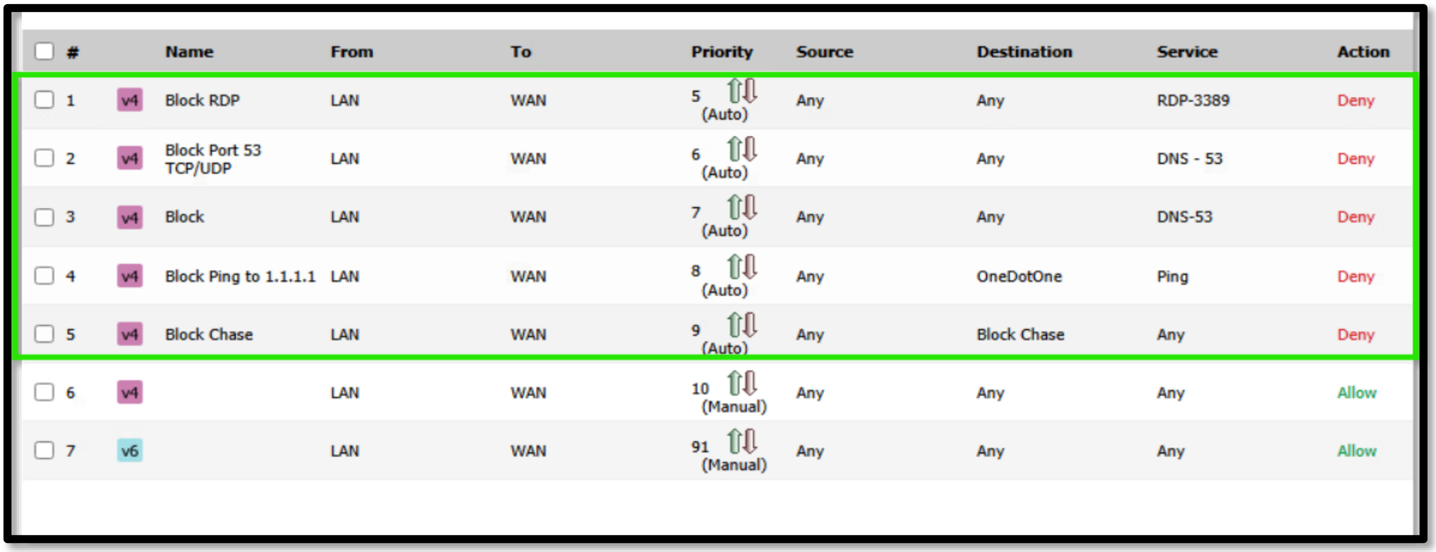


Hmmm... can't reach this page

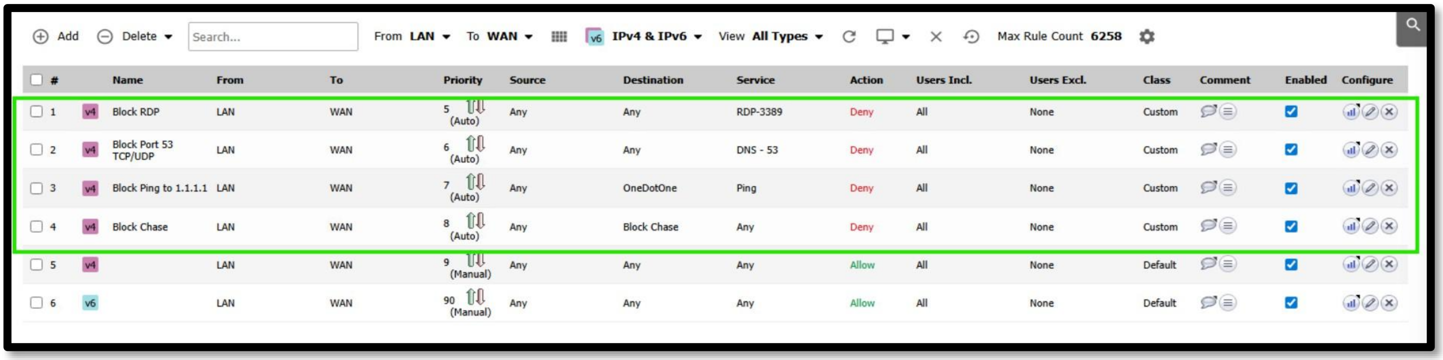
www.cnn.com's DNS address could not be found... diagnosing the problem now.

DNS_PROBE_STARTED

SonicWall Firewall



□	#		Name	From	To	Priority	Source	Destination	Service	Action
□	1	v4	Block RDP	LAN	WAN	5 (Auto)	Any	Any	RDP-3389	Deny
□	2	v4	Block Port 53 TCP/UDP	LAN	WAN	6 (Auto)	Any	Any	DNS - 53	Deny
□	3	v4	Block	LAN	WAN	7 (Auto)	Any	Any	DNS-53	Deny
□	4	v4	Block Ping to 1.1.1.1	LAN	WAN	8 (Auto)	Any	OneDotOne	Ping	Deny
□	5	v4	Block Chase	LAN	WAN	9 (Auto)	Any	Block Chase	Any	Deny
□	6	v4		LAN	WAN	10 (Manual)	Any	Any	Any	Allow
□	7	v6		LAN	WAN	91 (Manual)	Any	Any	Any	Allow



□	#		Name	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Class	Comment	Enabled	Configure
□	1	v4	Block RDP	LAN	WAN	5 (Auto)	Any	Any	RDP-3389	Deny	All	None	Custom		☑	
□	2	v4	Block Port 53 TCP/UDP	LAN	WAN	6 (Auto)	Any	Any	DNS - 53	Deny	All	None	Custom		☑	
□	3	v4	Block Ping to 1.1.1.1	LAN	WAN	7 (Auto)	Any	OneDotOne	Ping	Deny	All	None	Custom		☑	
□	4	v4	Block Chase	LAN	WAN	8 (Auto)	Any	Block Chase	Any	Deny	All	None	Custom		☑	
□	5	v4		LAN	WAN	9 (Manual)	Any	Any	Any	Allow	All	None	Default		☑	
□	6	v6		LAN	WAN	90 (Manual)	Any	Any	Any	Allow	All	None	Default		☑	

Firewall Rule Configuration and Management Best Practices

- **Place Deny Rules at the Top:** Firewall rules are processed from top to bottom. Always position deny or block rules above allow rules to ensure they are evaluated and enforced correctly.

- **Define the Source Carefully:** When creating a rule, use (Source: Any) to block traffic from all internal devices, or specify individual IP addresses or Address Objects if you want to restrict only certain PCs. Properly defining the source ensures precise control over network traffic.

- **Test Each Rule in a Controlled Environment:** After creating a rule, verify that it blocks or allows the intended traffic. Always perform testing in a staging or lab environment before applying rules to the production network. Check firewall logs to confirm the rule is matching traffic as expected and functioning correctly.

- **Clean Up Temporary Rules:** After testing, remove any temporary rules or objects to keep the firewall configuration organized. Ensure that permanent security rules remain intact to maintain network protection.

- **Use Address and Service Objects:** Wherever possible, use Address Objects and Service Objects to simplify rule management, improve readability, and reduce configuration errors.

- **Enable Logging for Critical Rules:** Logging is essential to monitor traffic patterns, detect anomalies, and troubleshoot issues effectively. Only log critical rules to avoid unnecessary log clutter.

- **Regularly Review Rules:** Periodically audit your firewall rules to remove redundant, obsolete, or conflicting entries. This ensures policies stay relevant and reduces security risks.

- **Implement the Principle of Least Privilege:** Allow only the minimum required access for users, applications, and devices. Restrict all unnecessary traffic to reduce potential attack surfaces.

- **Backup Configuration:** Before making significant changes, take a backup of the firewall configuration. This allows easy recovery in case of misconfigurations or errors.

- **Monitor and Update Firmware:** Keep your firewall firmware up to date to protect against vulnerabilities and take advantage of new security features.

- **Test Changes Before Production:** Always validate firewall rules and policies in a test or staging environment to ensure they work as intended and do not disrupt critical services before deploying to the production network.

Conclusion: This project demonstrates the practical implementation, testing, and management of firewall rules to enforce network security within an enterprise environment. By creating rules to block specific websites (Chase), ICMP (ping) traffic, Remote Desktop (RDP), and DNS queries while allowing other traffic to function normally, the project highlights the importance of precise rule definition, policy enforcement, and proper testing procedures.

Through this exercise, key skills were developed, including firewall configuration, traffic monitoring, troubleshooting, and best practices for secure rule management. Testing in a controlled environment emphasized safe deployment procedures and minimized risk to production networks. Overall, the project provides hands-on experience in securing internal networks, managing traffic policies, and applying industry-standard practices, making it a strong demonstration of practical network security and administration capabilities.