Configuring DMZ on the RV34x Series Router

Objective

The objective of this document is to show you how to configure Demilitarized Zone (DMZ) Host and Hardware DMZ on RV34x series routers.

Introduction

A DMZ is a location on a network that is open to the internet while securing your Local Area Network (LAN) behind a firewall. Separating the main network from either a single host or an entire sub-network, or “subnet” ensures that people visiting your service such as Internet gaming, video conferencing, web, or email servers via the DMZ, won’t have access to your LAN. Cisco offers two methods of using DMZs which is DMZ Host and Hardware DMZ. DMZ Host allows one host on the LAN to be exposed to the internet while Hardware DMZ (subnet/range) is a subnetwork that is open to the public.

In planning your DMZ you may consider using either a private or public IP address. A private IP address will be unique to you, only on your LAN. A public IP address will be unique to your organization and is assigned by your Internet Service Provider (ISP). To procure a public IP address you will need to contact your ISP.

Most users would use Hardware DMZ because it automatically sets up a VLAN and its own network segment. For “Hardware DMZ” we are using subnet or range option. DMZ host is simpler to configure as you don’t have to configure access rules, but it is less secure.

WAN-to-DMZ is the most popular use case, as well as LAN-to-DMZ. DMZ-to-WAN is also allowed, as DMZ machines might need operating system patches or updates, but DMZ-to-LAN should be blocked because it could be a potential security hole. For example, hackers on the Internet use DMZ as the jumper server.

The difference between DMZ host and Hardware DMZ in terms of use case is:

If you want to expose something to the Internet, but you have an all-in-one server, or you don’t have spare public IP addresses, you should use DMZ Host. Place the server in one of your VLANs and set it up as the DMZ Host. Then the external user can access the server by the router’s WAN IP.

If you want to expose something to the Internet, and you have several servers (each with a specific service) and the same amount of public IP addresses, you should use Hardware DMZ. Connect these servers to the specified DMZ port (i.e. LAN 4 for RV340) and configure them with the same public IP addresses you configure in the router or subnet). Then the external user can access each of the servers by those IP addresses.

DMZ	Compare	Contrast
Host	Segregates traffic	Single host, fully

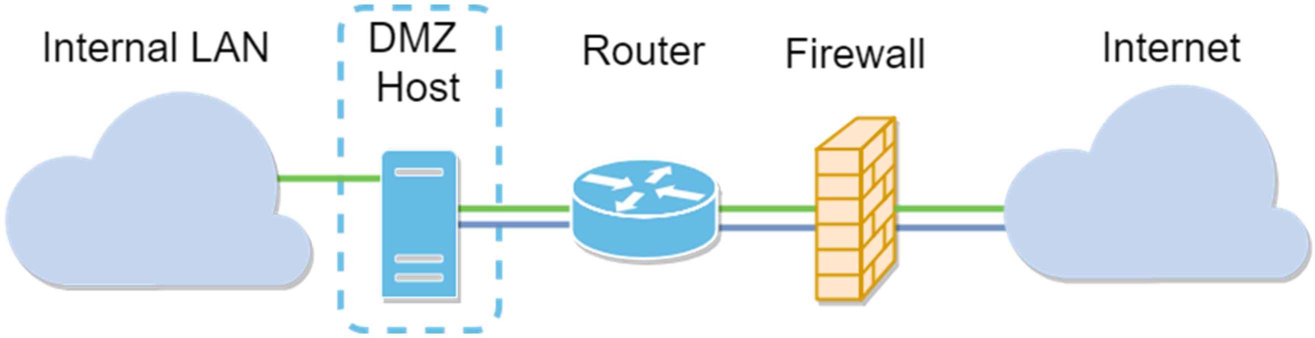
		open to the internet
Subnet/Range	Segregates traffic	Multiple devices and types, fully open to the internet.

Note: In this example, we will have a switch plugged into the DMZ port of the router when configuring DMZ Subnet.

To learn how to enable SSH on a switch, please refer to this article: Enabling SSH service on 300/500 Series Managed Switches.

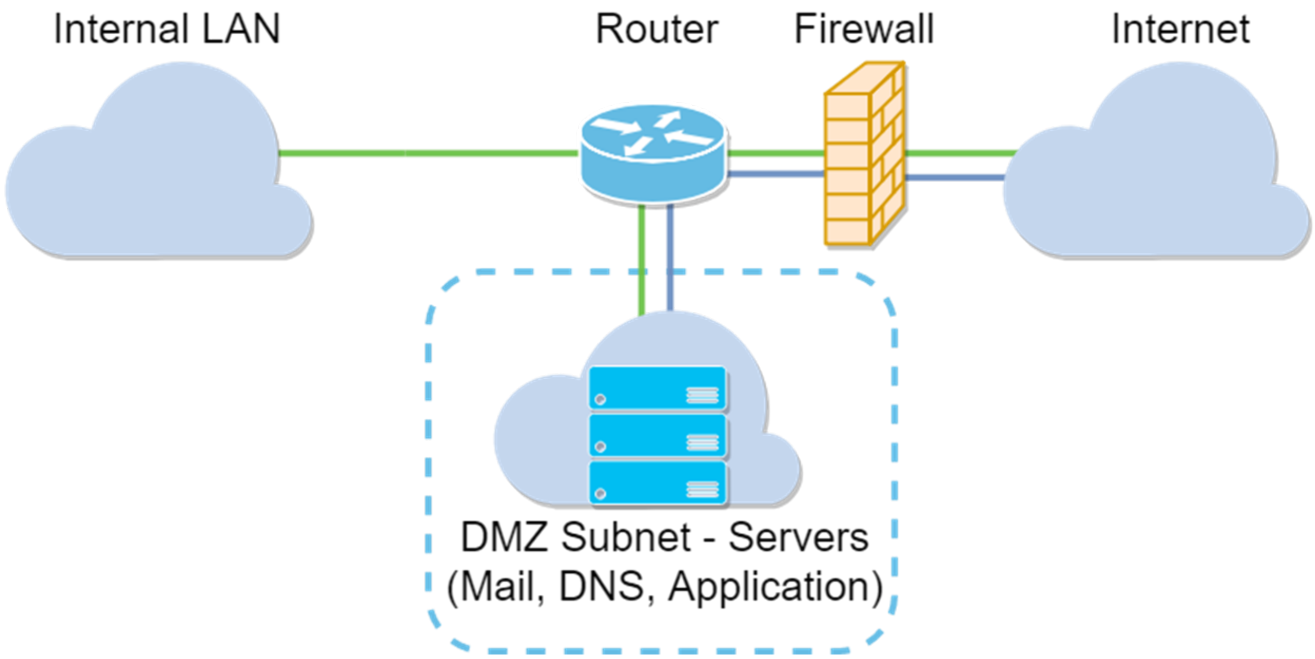
To learn how to configure DMZ on the RV160/RV260, please see this article: DMZ Options for RV160/RV260 Routers.

Host DMZ Topology



Note: When using a host DMZ, if the host is compromised by a bad-actor your internal LAN may be subject to further security intrusion.

Subnet DMZ Topology



Applicable Devices

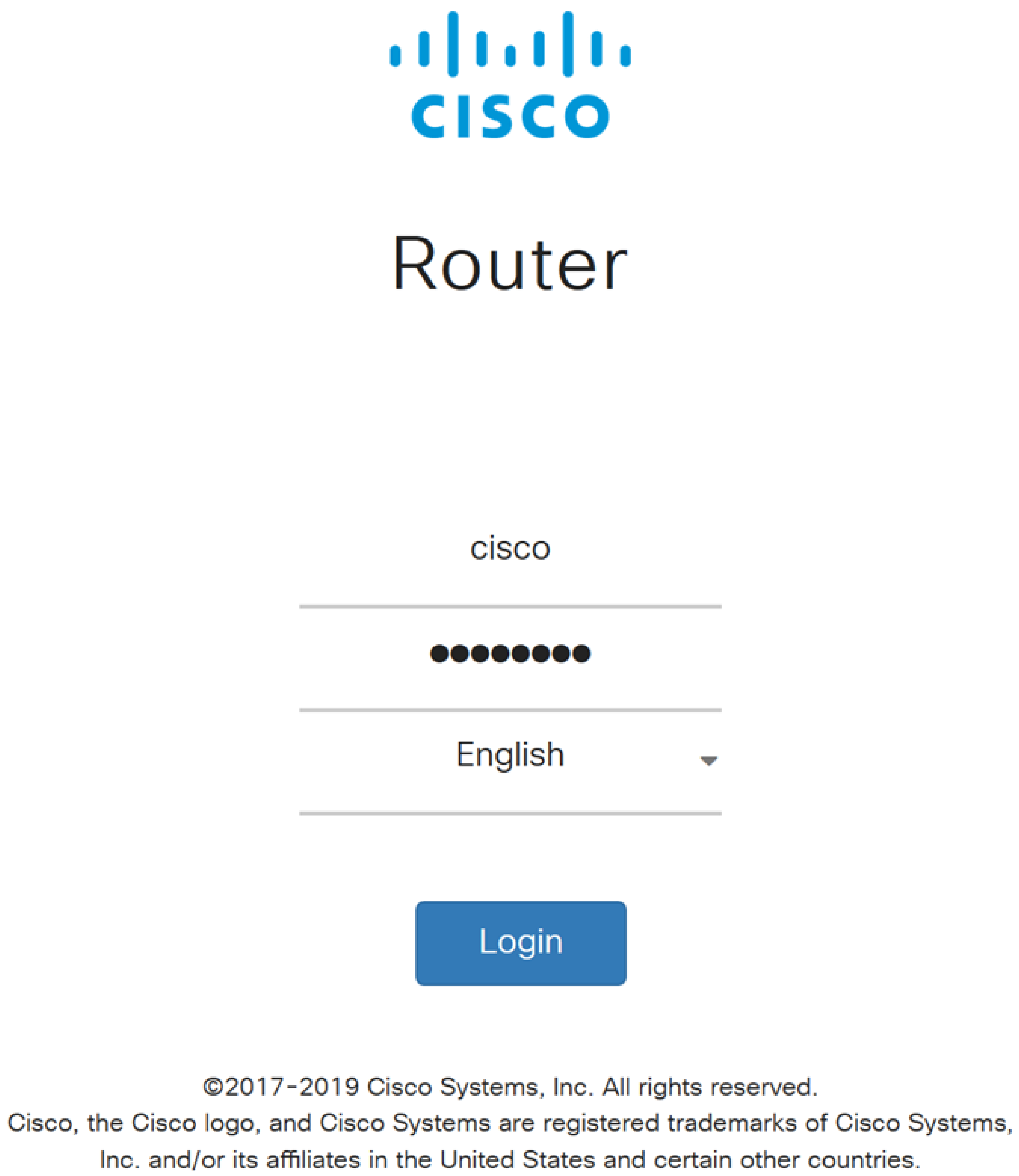
RV34x

Software Version

1.0.02.16

Configuring DMZ Host

Step 1. Log in to the web configuration page of your router.



Router

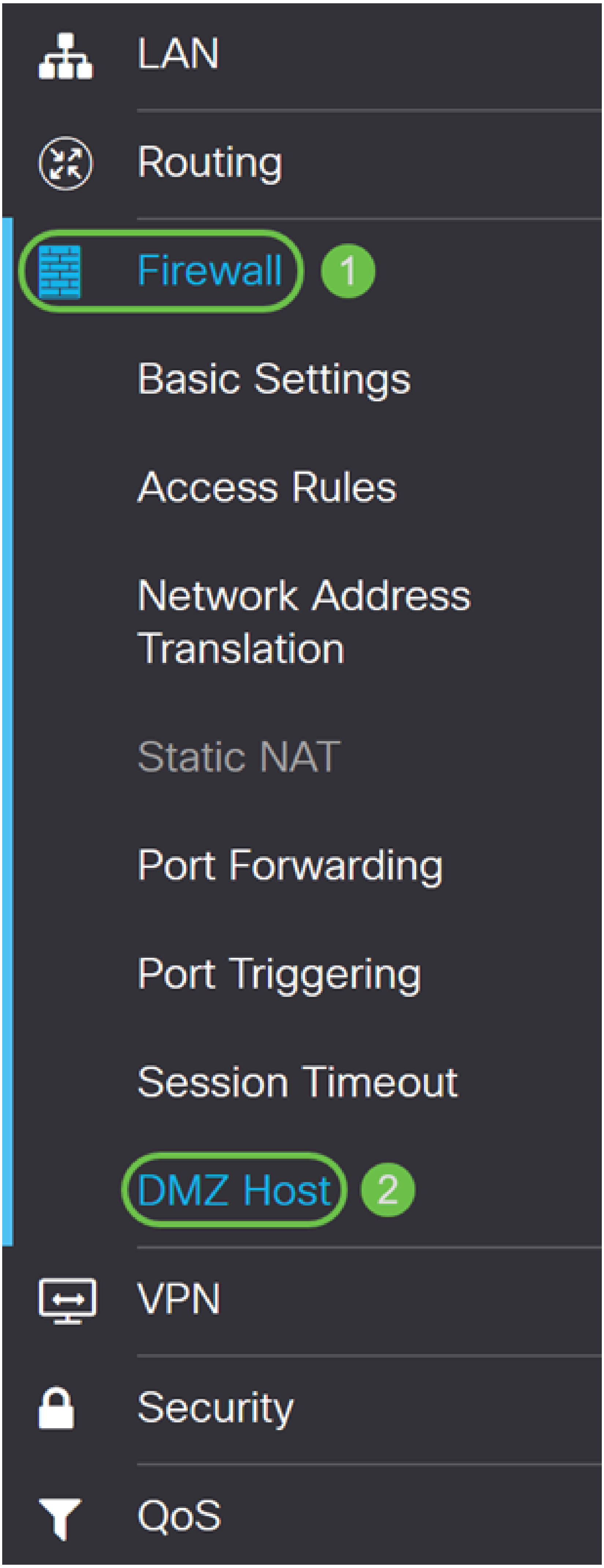
cisco

●●●●●●●●

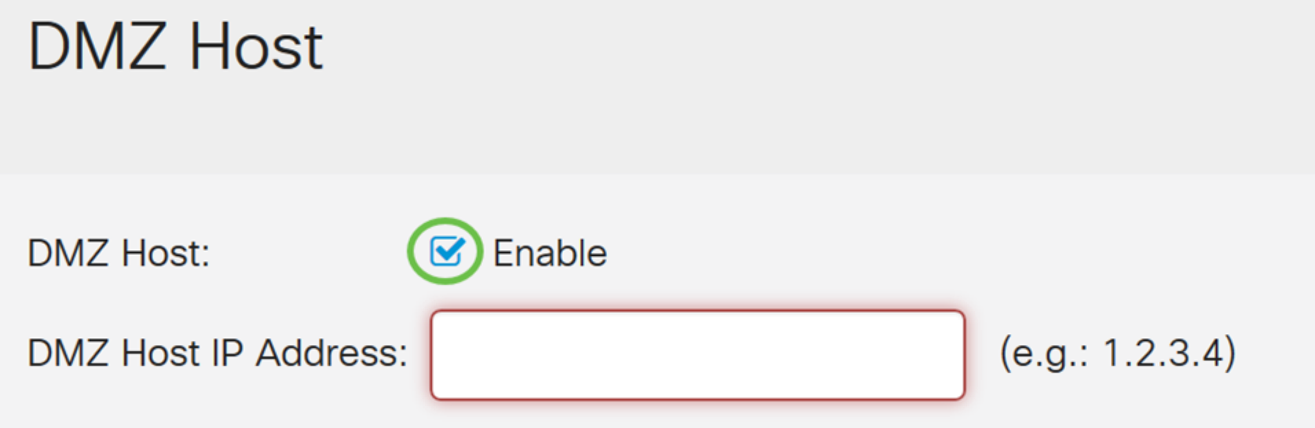
English

©2017-2019 Cisco Systems, Inc. All rights reserved.
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 2. Navigate to **Firewall > DMZ Host**.


LAN
Routing
Firewall
1
Basic Settings
Access Rules
Network Address Translation
Static NAT
Port Forwarding
Port Triggering
Session Timeout
DMZ Host
2
VPN
Security
QoS

Step 3. In the *DMZ Host* field, check the **Enable** checkbox to enable DMZ Host.



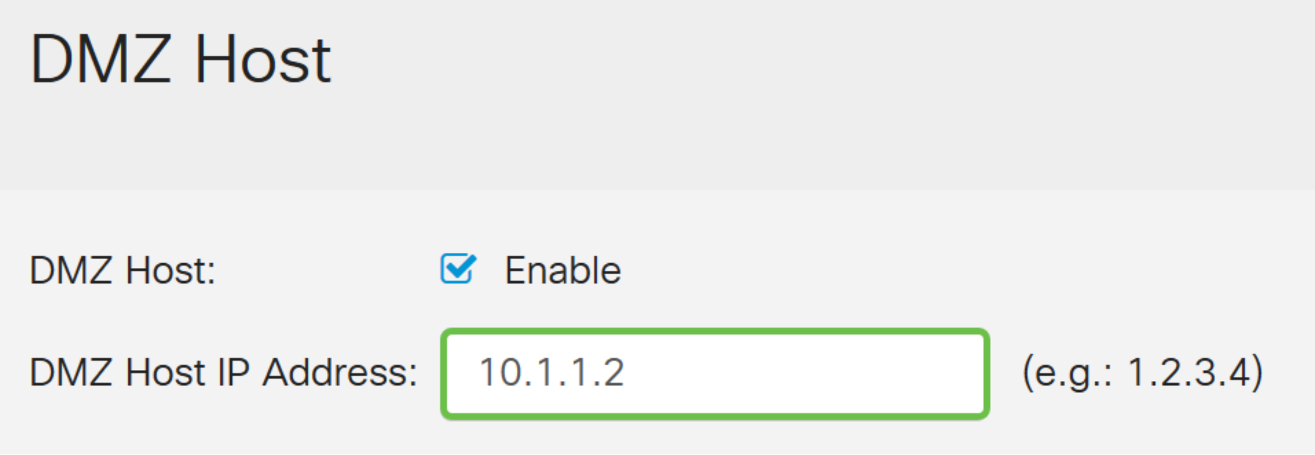
DMZ Host

DMZ Host: ☑ Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

Step 4. Enter the IP address of the host in the *DMZ Host IP address* that will be exposed to the Internet to use services such as Internet gaming, video conferencing, web, or email servers.

Note: The LAN DMZ host needs to be given a fixed or static IP address for the DMZ host feature to work properly. Make sure it is on the same network as your router. You can also configure this when the DMZ is in another VLAN.

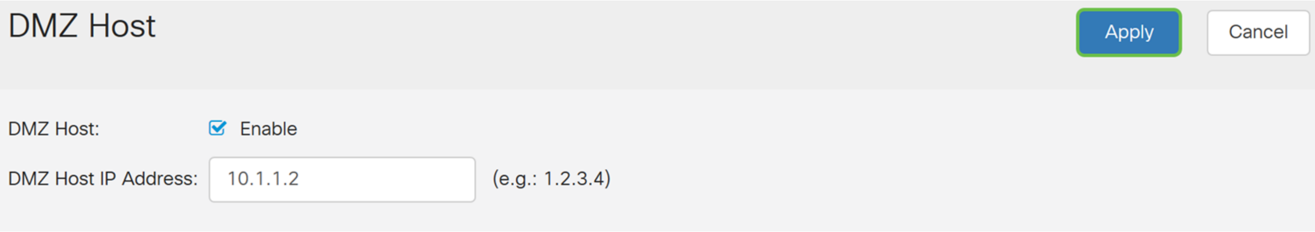


DMZ Host

DMZ Host: ☑ Enable

DMZ Host IP Address: 10.1.1.2 (e.g.: 1.2.3.4)

Step 5. Click **Apply** save your configuration.



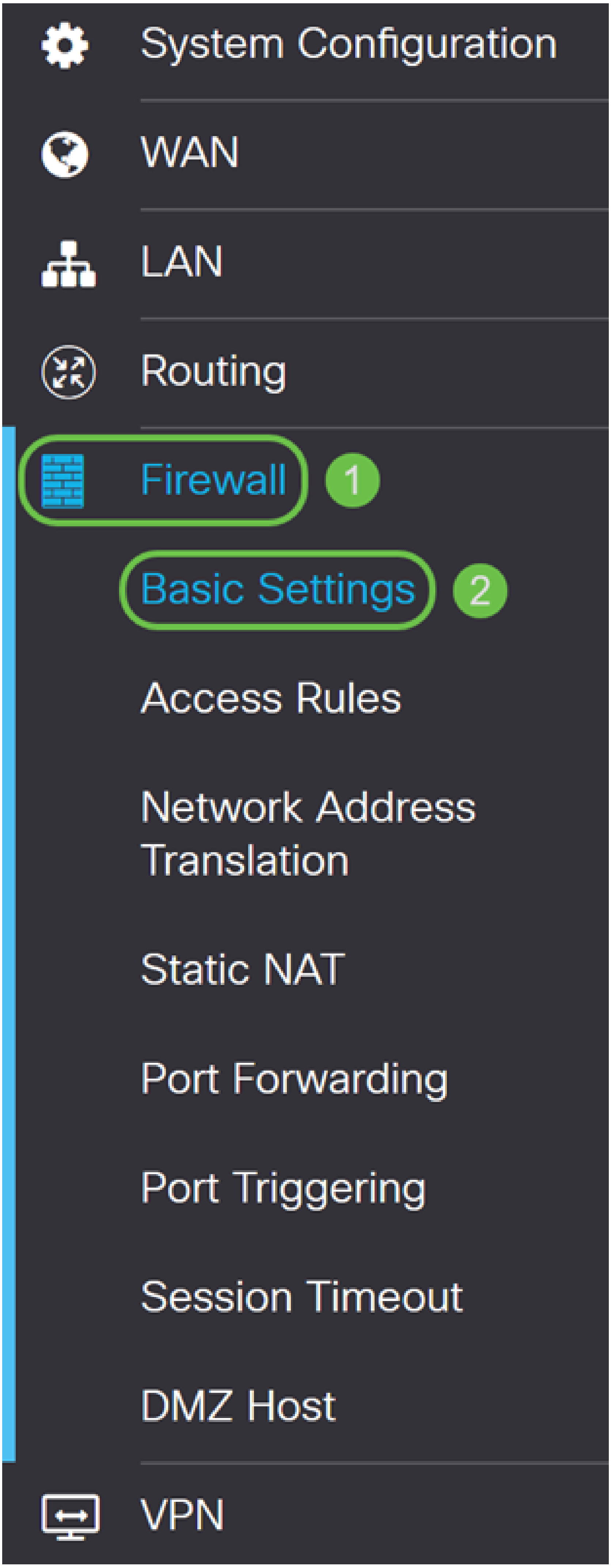
DMZ Host

DMZ Host: ☑ Enable

DMZ Host IP Address: 10.1.1.2 (e.g.: 1.2.3.4)

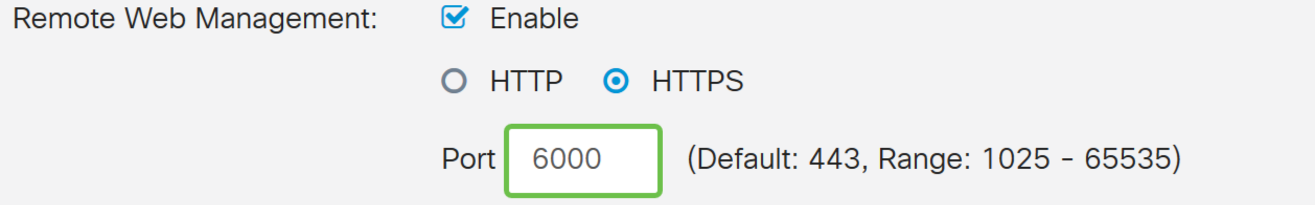
You should now have successfully enabled DMZ host.

Step 6. (Optional) In the next few steps, we will be showing you one way to verify DMZ host. Navigate to **Firewall > Basic Settings**.


System Configuration
WAN
LAN
Routing
Firewall
1
Basic Settings
2
Access Rules
Network Address Translation
Static NAT
Port Forwarding
Port Triggering
Session Timeout
DMZ Host
VPN

Step 7. (Optional) In this example, *Remote Web Management* is enabled with **HTTPS** selected. This is to log in to the web configuration page remotely via the WAN IP address. In this step, we will be adjusting the port number to **6000**. The range is from **1025-65535**.

Note: If you have configured this while accessing the web management page remotely, your page may hang at the loading screen. This means that the port has changed to what you have adjusted.



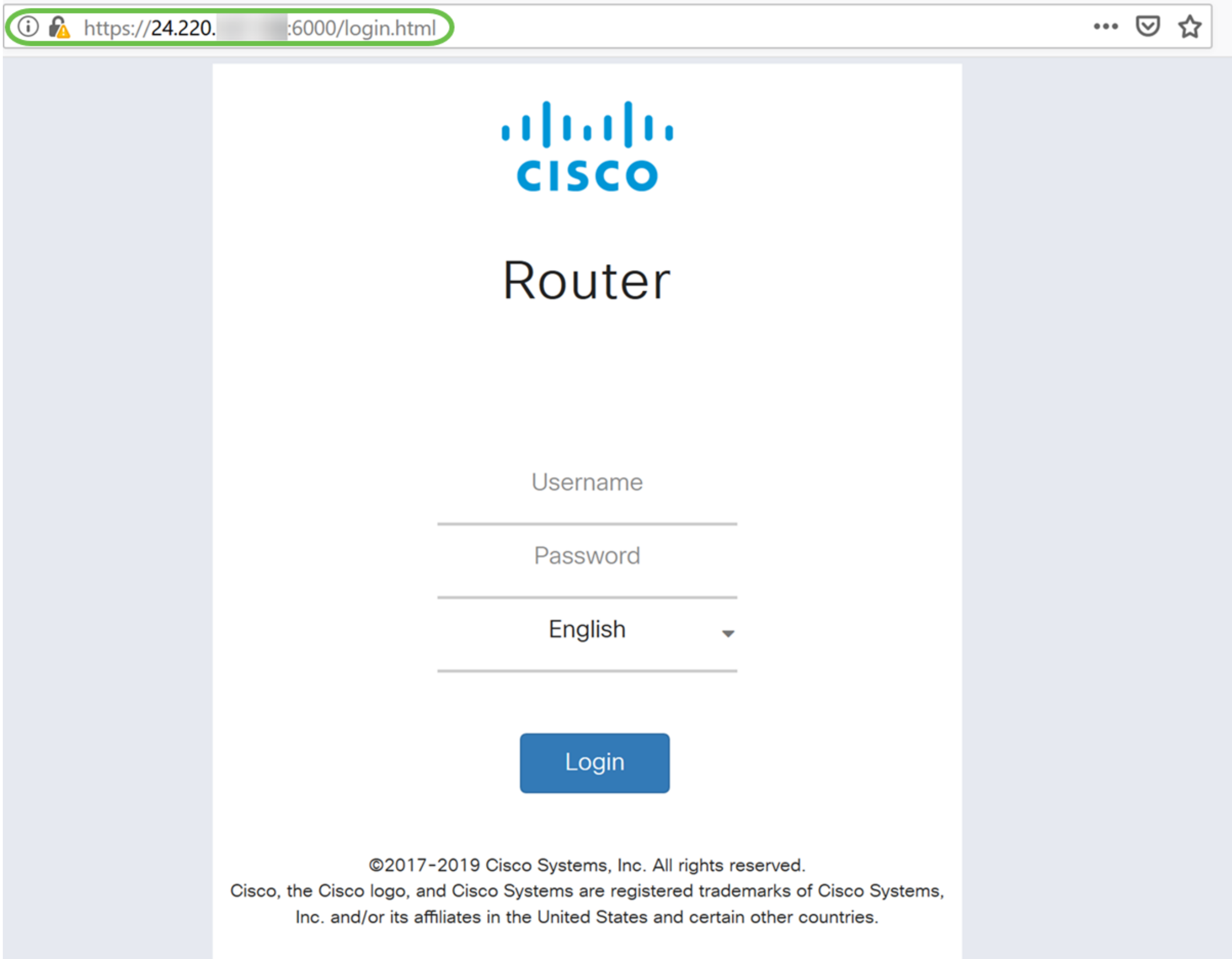
Remote Web Management: ☑ Enable

○ HTTP ● HTTPS

Port 6000 (Default: 443, Range: 1025 - 65535)

Step 8. Verify that you can access the web configuration page of your router by typing **https://[*WANIPaddress*]:port**, where the WAN IP address is your actual WAN IP address of the router and then the **:port** for the port number that you have set in step 5 for this section. In this example, we entered **https://24.220.x.x:6000**, but you would include the actual numbers and not **x**. The x is to hide our public WAN IP address.

Note: Make sure you are off the VPN, sometimes being on the VPN will not allow you to access the web configuration page.



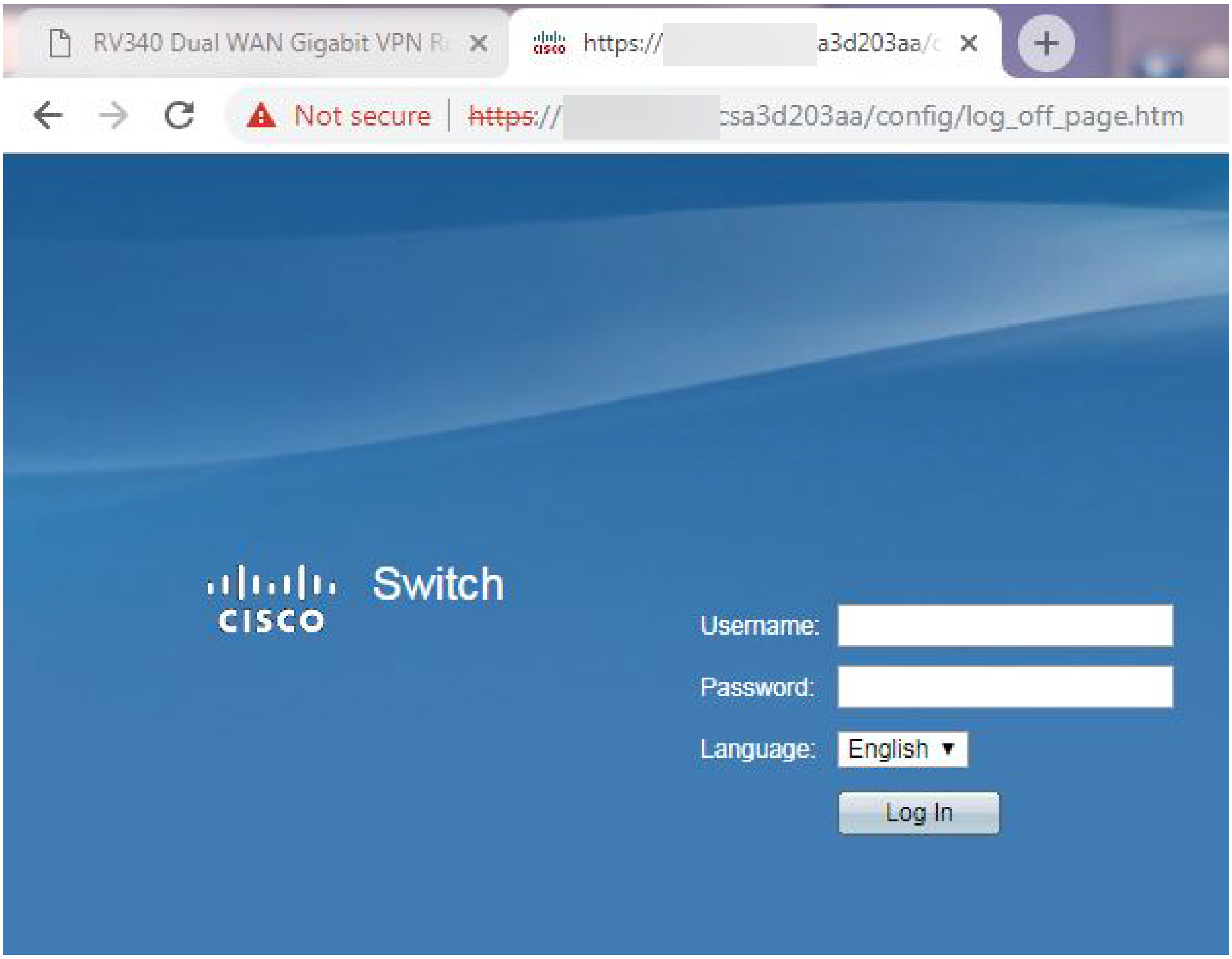
https://24.220.[redacted]:6000/login.html

©2017-2019 Cisco Systems, Inc. All rights reserved.
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 9. You should now be able to access the web configuration page of your device that is in the DMZ port by using the WAN IP address without adding the port number.

https://24.220.x.x:6000 – will display the web configuration page of the router.

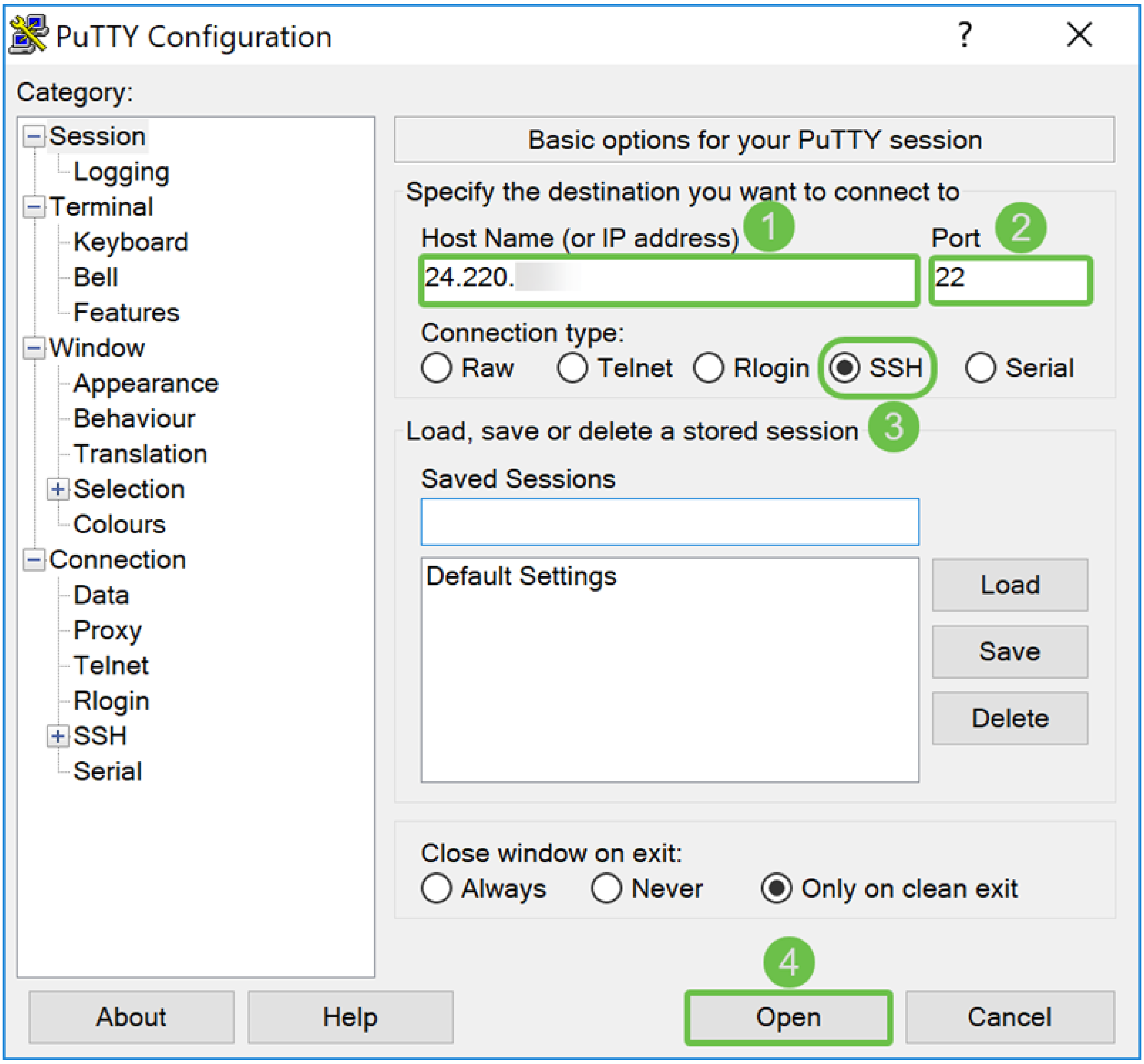
https://24.220.x.x – will display the web configuration page of the switch.


RV340 Dual WAN Gigabit VPN R
https://[redacted]a3d203aa/c
Not secure
https://[redacted]csa3d203aa/config/log_off_page.htm
cisco Switch
Username:
Password:
Log In

Language: English

Step 10. We will be using PuTTY to SSH into the switch. Enter the **public IP address** of your device under the *Host Name (or IP address)* field. Ensure port **22** is entered and **SSH** is selected. Click **Open** to start your connection.

Note: If you want to SSH into the switch, remember to enable SSH on the switch first. In most switches, you can navigate to **Security > TCP/UDP Services** to enable **SSH Service**. To SSH using Windows, you can download PuTTY. Check this document for more information on: How to Access an SMB Switch CLI using SSH or Telnet. SSH is recommended and Telnet is not as SSH is more secure.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 24.220.[redacted]

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

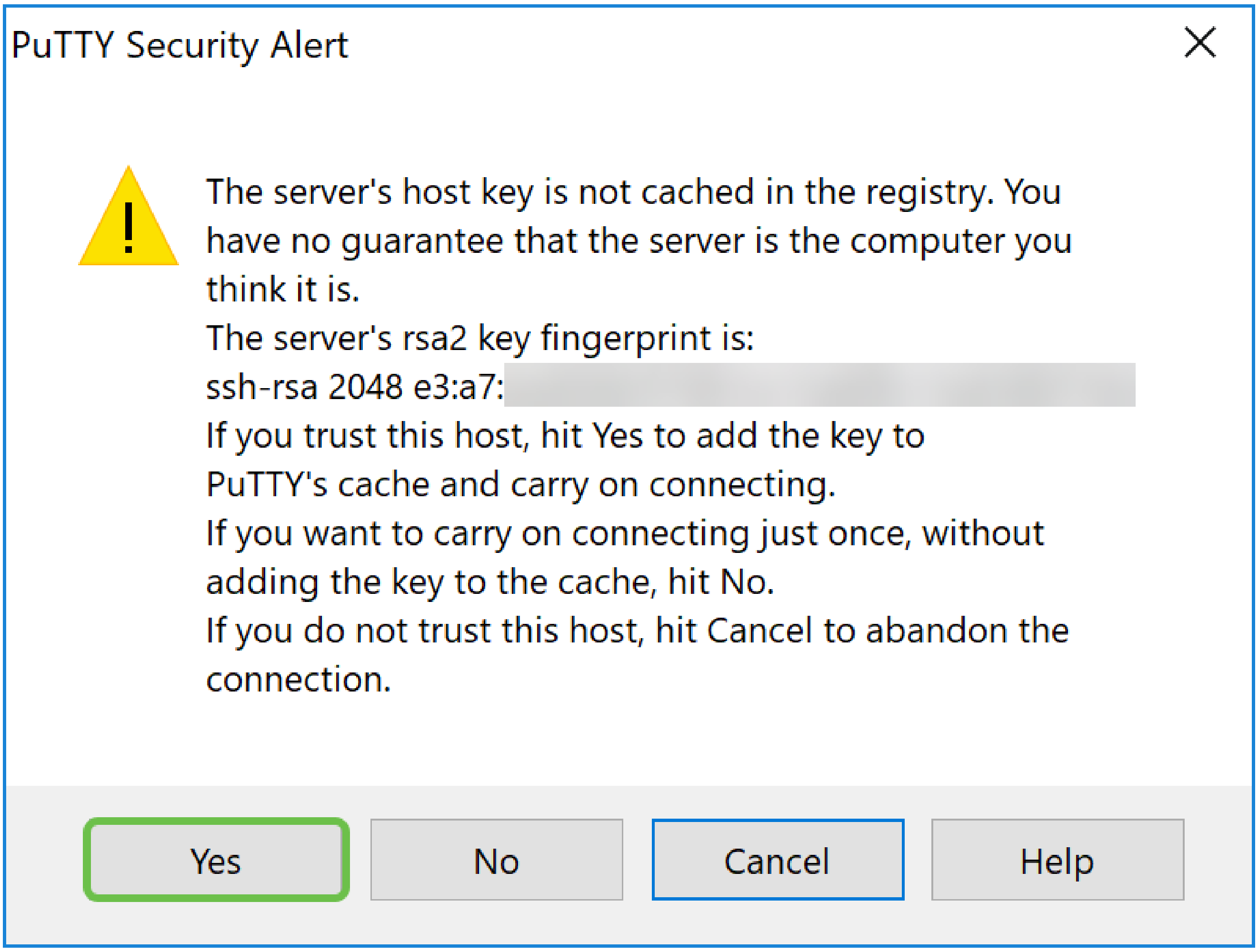
Load, save or delete a stored session

Saved Sessions

Default Settings

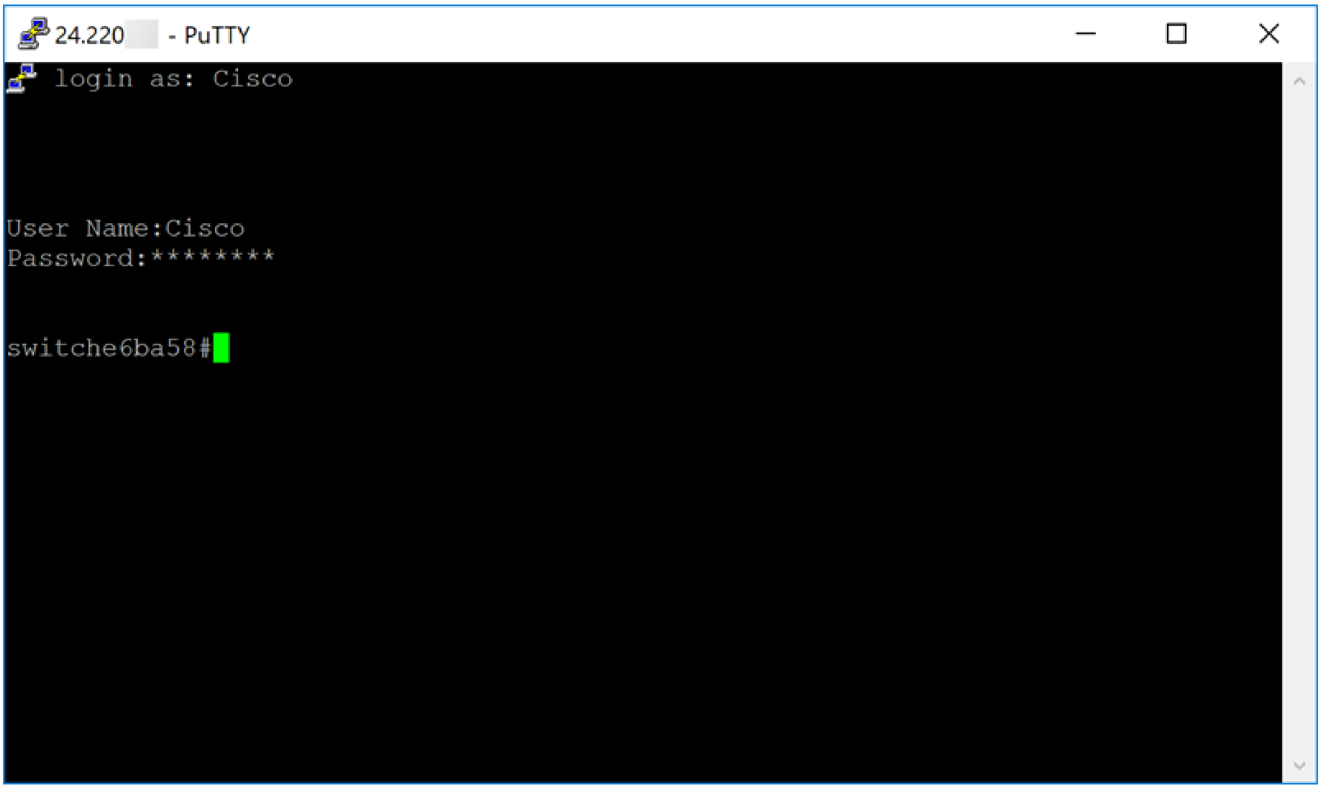
Close window on exit: ○ Always ○ Never ● Only on clean exit

Step 11. A *PuTTY Security Alert* may appear. Click **Yes** to continue to connect.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 e3:a7:[redacted]
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Step 12. If your connection is successful, you will be prompted to log in with your credentials.

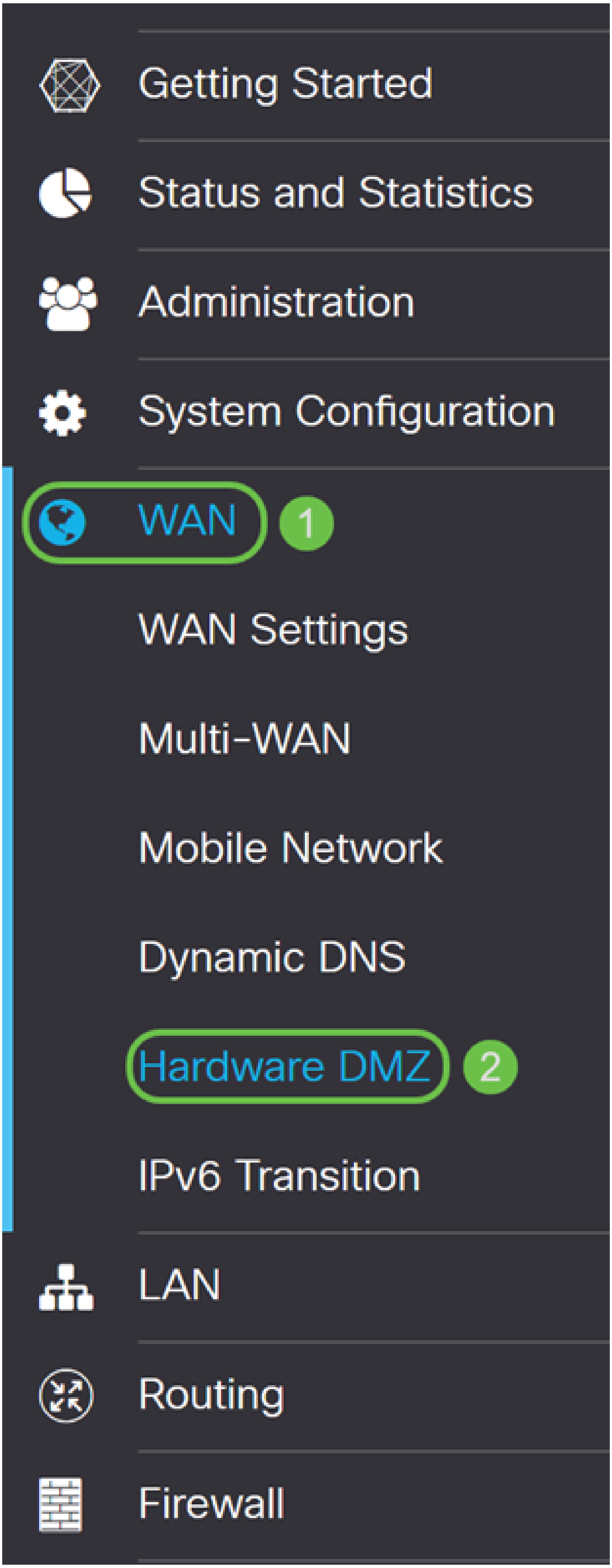


```
login as: Cisco



User Name:Cisco
Password:********


switche6ba58#
```

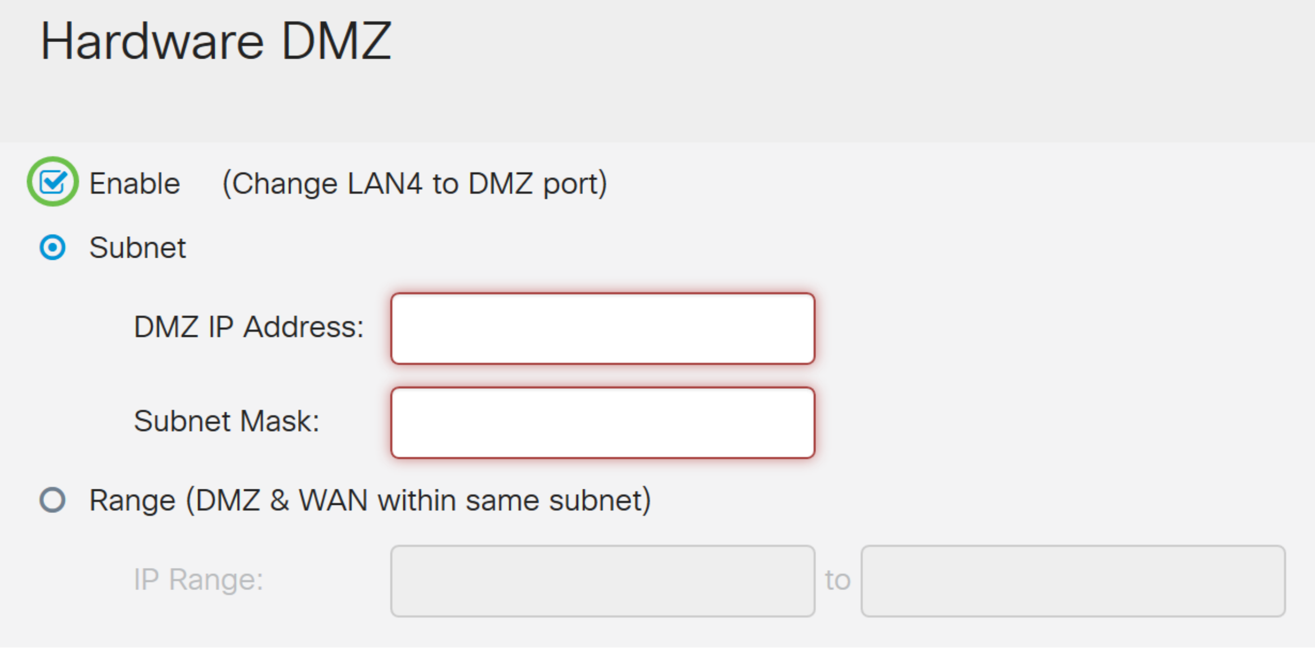
Configuring Hardware DMZ

Step 1. If you want to configure Hardware DMZ instead of DMZ Host, navigate to **WAN >**

Hardware DMZ.


Getting Started
Status and Statistics
Administration
System Configuration
WAN
1
WAN Settings
Multi-WAN
Mobile Network
Dynamic DNS
Hardware DMZ
2
IPv6 Transition
LAN
Routing
Firewall

Step 2. Check **Enable** checkbox to change LAN4 to DMZ port.



Hardware DMZ

☑ Enable (Change LAN4 to DMZ port)

● Subnet

DMZ IP Address:

Subnet Mask:

○ Range (DMZ & WAN within same subnet)

IP Range: to

Step 3. A warning message will appear. Click **Yes** to accept the changes that the router would make to the DMZ port (LAN4) or **No** to deny the changes.

When DMZ is set at enable, the DMZ Port (LAN4) configuration will be changed automatically as follows:

Remove from LAG port (Section “LAN > Port Settings”)

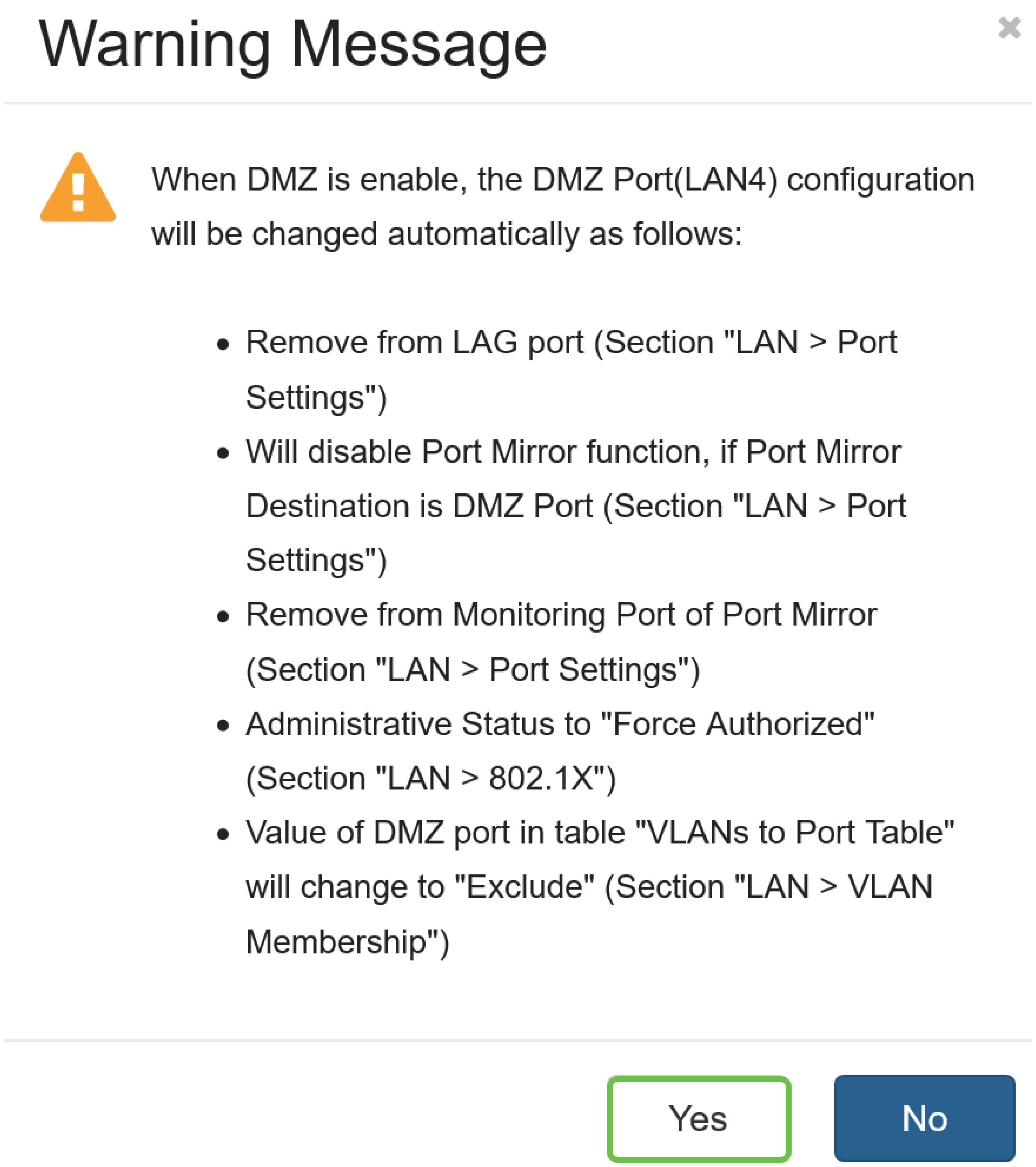
Will disable Port Mirror function, if Port Mirror Destination is DMZ Port (Section “LAN > Port Settings”)

Remove from Monitoring Port of Port Mirror (Section “LAN > Port Settings”)

Administrative Status to “Force Authorized” (Section “LAN > 802.1X”)

Value of DMZ port in table “VLANs to Port Table” will change to “Exclude” (Section “LAN > VLAN Membership”)

In this example, we will be clicking **Yes**.

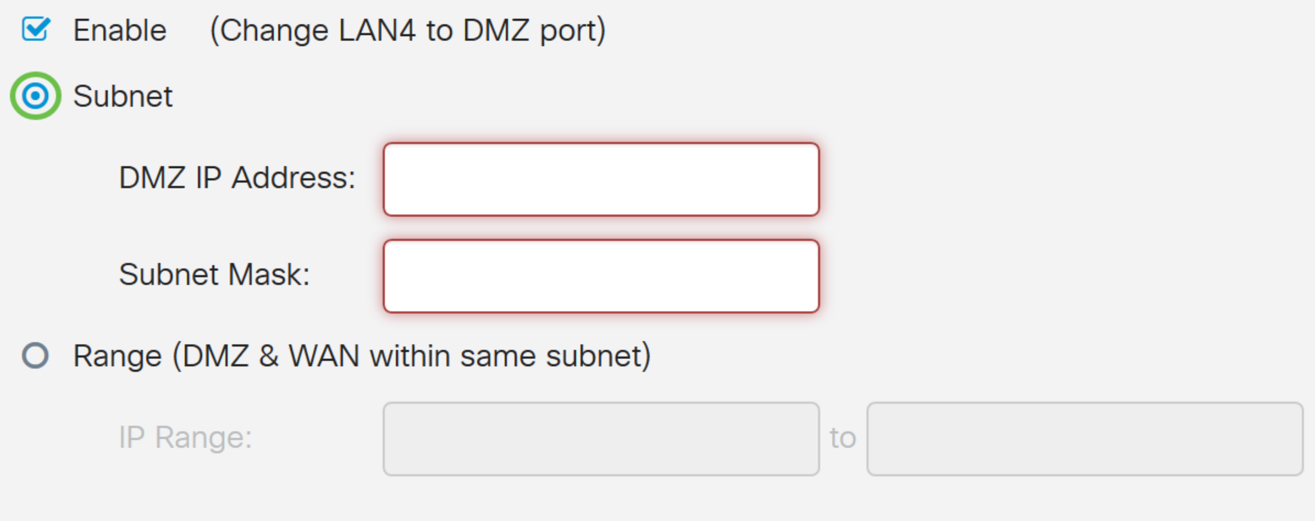


Warning Message

When DMZ is enable, the DMZ Port(LAN4) configuration will be changed automatically as follows:

- Remove from LAG port (Section "LAN > Port Settings")
- Will disable Port Mirror function, if Port Mirror Destination is DMZ Port (Section "LAN > Port Settings")
- Remove from Monitoring Port of Port Mirror (Section "LAN > Port Settings")
- Administrative Status to "Force Authorized" (Section "LAN > 802.1X")
- Value of DMZ port in table "VLANs to Port Table" will change to "Exclude" (Section "LAN > VLAN Membership")

Step 4. Select either **Subnet** or **Range (DMZ & WAN within same subnet)**. In this example, we will be selecting **Subnet**.



☑ Enable (Change LAN4 to DMZ port)

● Subnet

DMZ IP Address:

Subnet Mask:

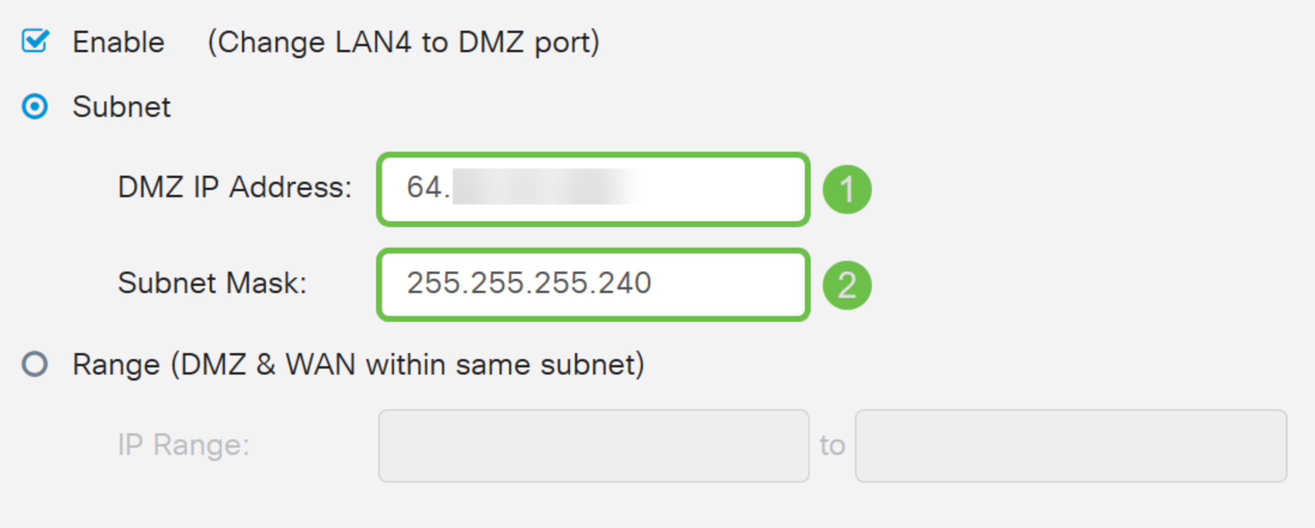
○ Range (DMZ & WAN within same subnet)

IP Range: to

Step 5. Enter in the **DMZ IP Address** and **Subnet Mask**. Anything that is plugged into the LAN4 segment must be in this network.

Note: Make sure that the device connected to the DMZ port has that static IP address. This IP address may need to be outside of your WAN subnet.

In this example, we will be using a public IP address for the DMZ.



☑ Enable (Change LAN4 to DMZ port)

● Subnet

DMZ IP Address: 64.[redacted] 1

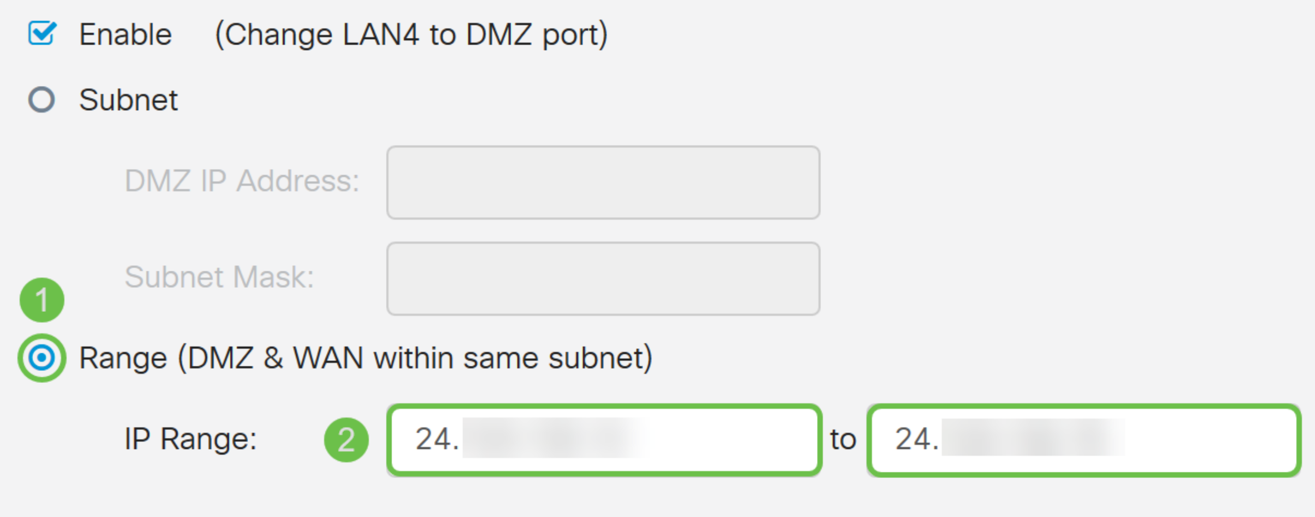
Subnet Mask: 255.255.255.240 2

○ Range (DMZ & WAN within same subnet)

IP Range: to

Note: If you intend to use the *Range* method, then you will need to click the **Range** radio button, then enter the range of IP addresses assigned by your ISP. This is usually used when you have multiple public IP address from your ISP for multiple devices that are in your DMZ network.

If you have a single public IP address and subnet does not work for you, enter the single public IP address in both fields under the *IP Range* field. The IP address needs to be a different free IP from the WAN IP subnet, it cannot use the WAN IP address. For example, if you are given a single public IP address of 24.100.50.1 which is within the same subnet as your WAN IP address then enter in **24.100.50.1** to **24.100.50.1** in the *IP Range* field.



☑ Enable (Change LAN4 to DMZ port)

○ Subnet

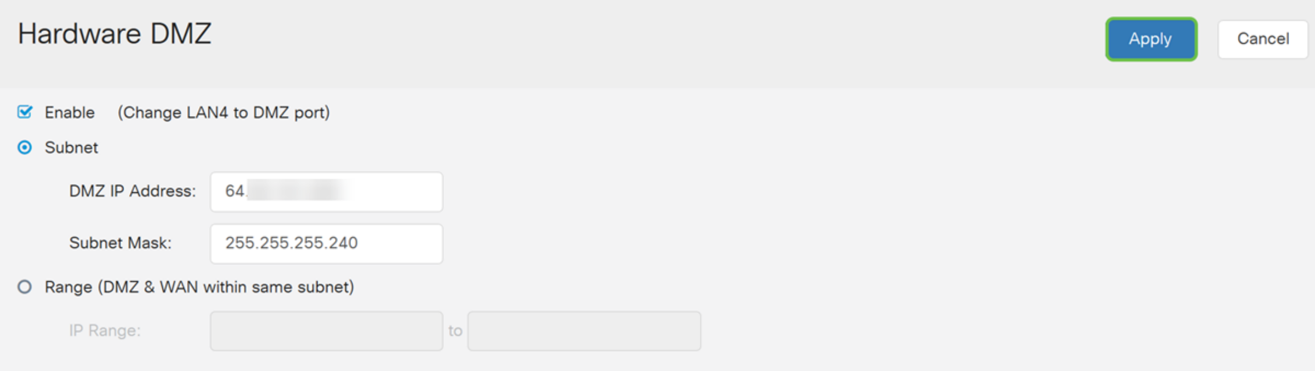
DMZ IP Address:

Subnet Mask:

● Range (DMZ & WAN within same subnet)

IP Range: 24.[redacted] to 24.[redacted]

Step 6. Click **Apply** in the upper right hand corner to accept the DMZ settings.



Hardware DMZ

☑ Enable (Change LAN4 to DMZ port)

● Subnet

DMZ IP Address: 64[redacted]

Subnet Mask: 255.255.255.240

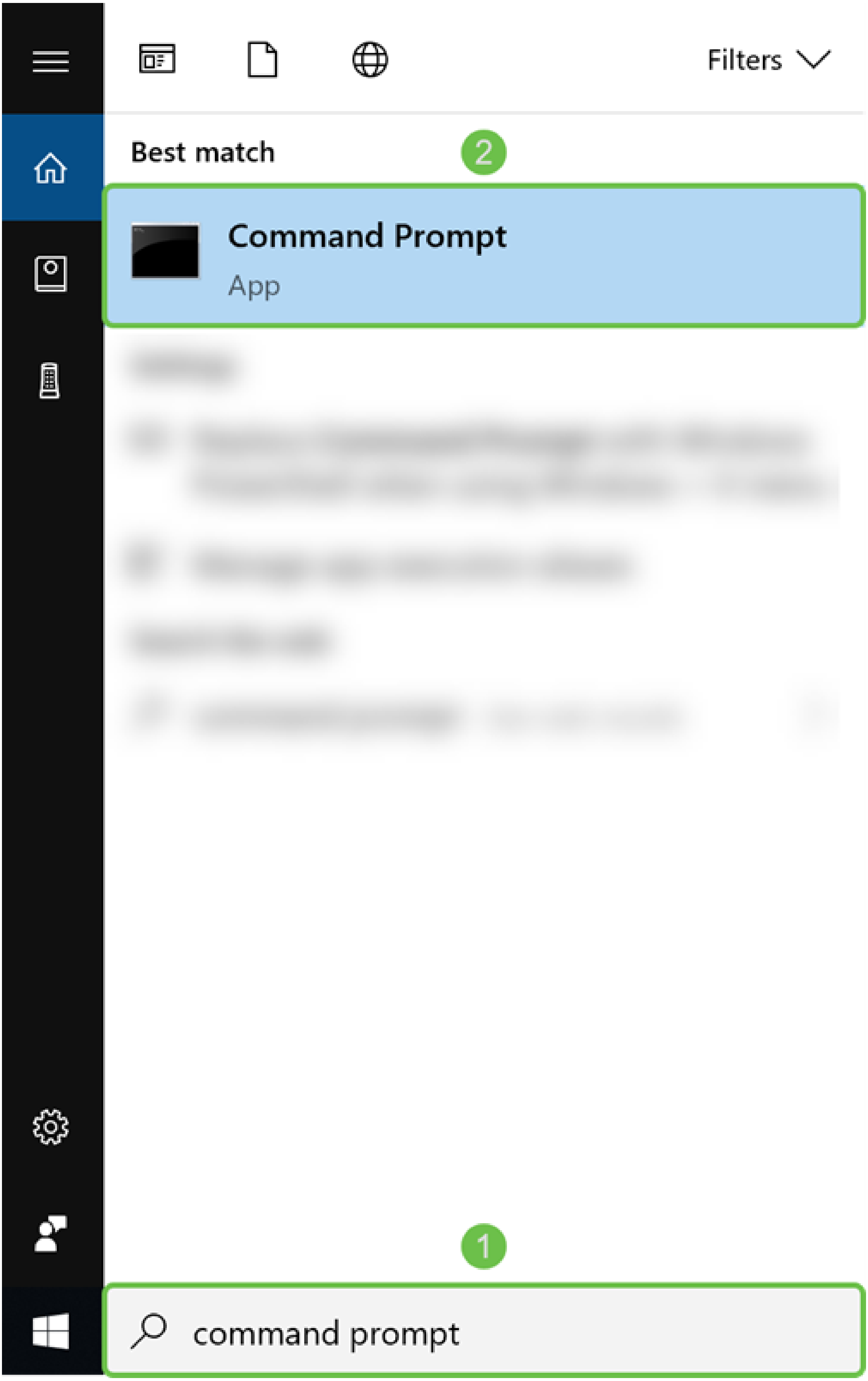
○ Range (DMZ & WAN within same subnet)

IP Range: to

You should have successfully enabled Hardware DMZ.

Step 7. (Optional) To verify this, open command prompt on your PC by navigating to the search bar at the bottom left and typing in **command prompt**. Click the **command prompt** application when it appears.

Note: We are using Windows 10 for this example.

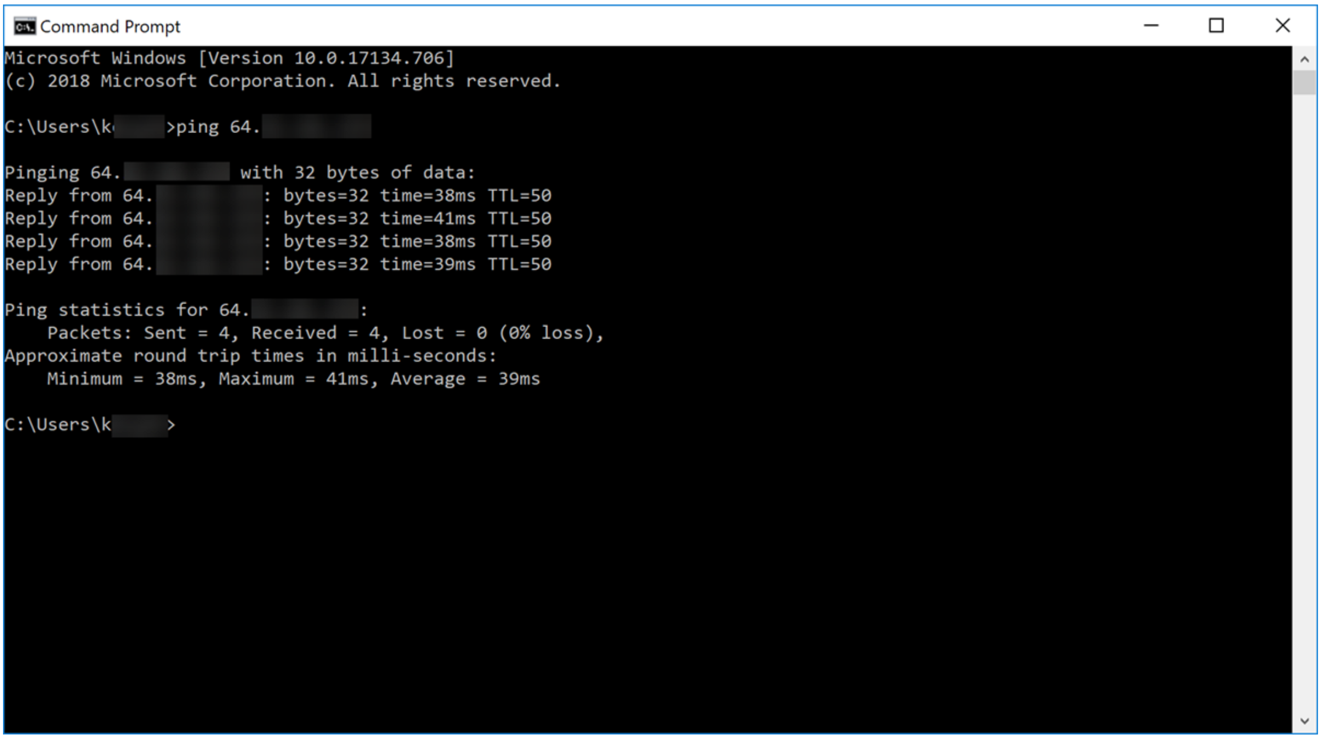


command prompt

Step 8. (Optional) A *Command Prompt* window will open. We will be executing a ping command to the DMZ IP address to see if there is any connectivity. Use the **ping** *DMZ_IP_Address* command. Hit the **enter** key when you want to start the ping. If you got replies from that IP address, it means you have connectivity between you and the DMZ. If you received any sort of messages like “Request timed out” or “Destination host unreachable” then you should check your configuration and connections.

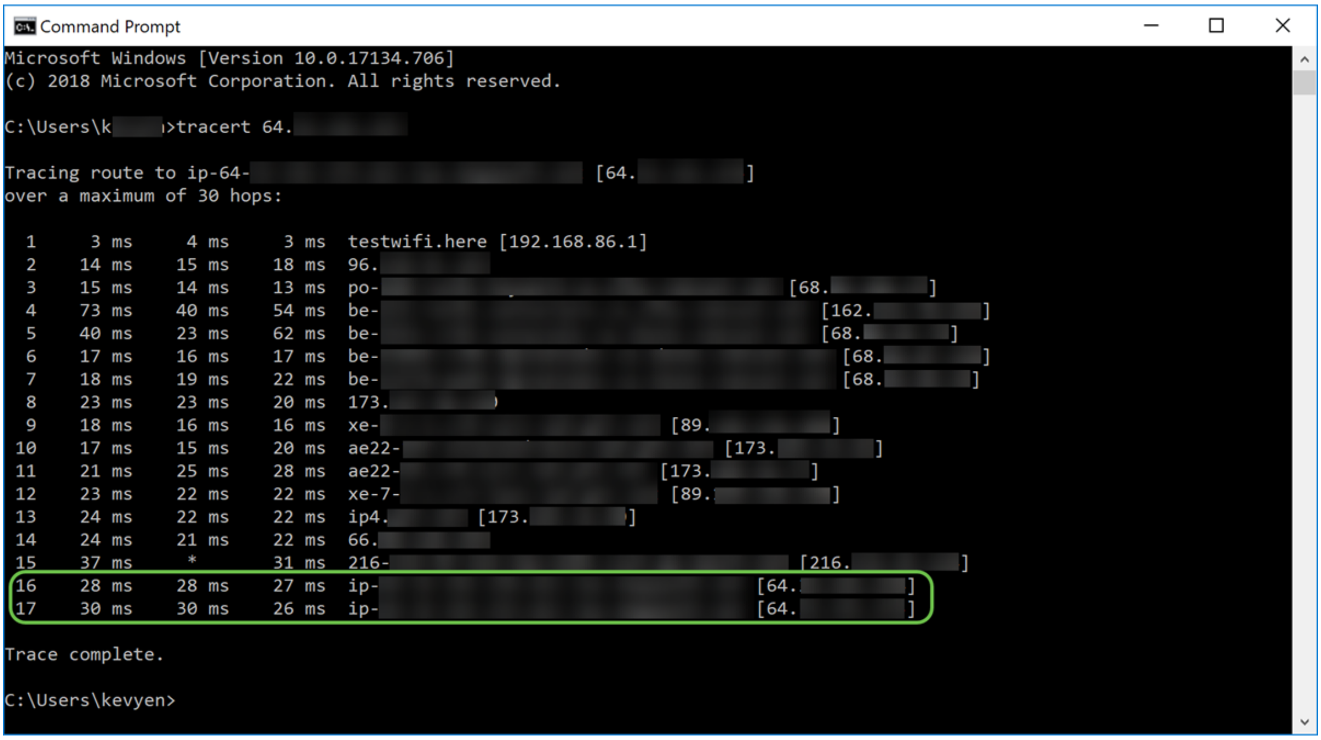
In this example, we will be typing in ping **64.x.x.x.x**. 64.x.x.x is our public IP address for the DMZ.

Note: Check out this great document: [Troubleshooting on RV160 and RV260 Routers](). This troubleshooting document will cover some of the areas to analyze when troubleshooting connectivity. Even though this document is for the RV160 and RV260, you may be able to use some similar troubleshooting steps in there.



```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\k[redacted]>ping 64.[redacted]

Pinging 64.[redacted] with 32 bytes of data:
Reply from 64.[redacted]: bytes=32 time=38ms TTL=50
Reply from 64.[redacted]: bytes=32 time=41ms TTL=50
Reply from 64.[redacted]: bytes=32 time=38ms TTL=50
Reply from 64.[redacted]: bytes=32 time=39ms TTL=50

Ping statistics for 64.[redacted]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 41ms, Average = 39ms

C:\Users\k[redacted]>
```

Step 9. (Optional) We can also execute a traceroute command to see the path that the packets take to get to the destination. Use the **tracert** *DMZ_IP_Address* command and hit the **enter** key to start the process. In this example, we can see that the trace is complete when it hits the DMZ IP address at the end. It will also display “Trace complete” once it hits the destination.

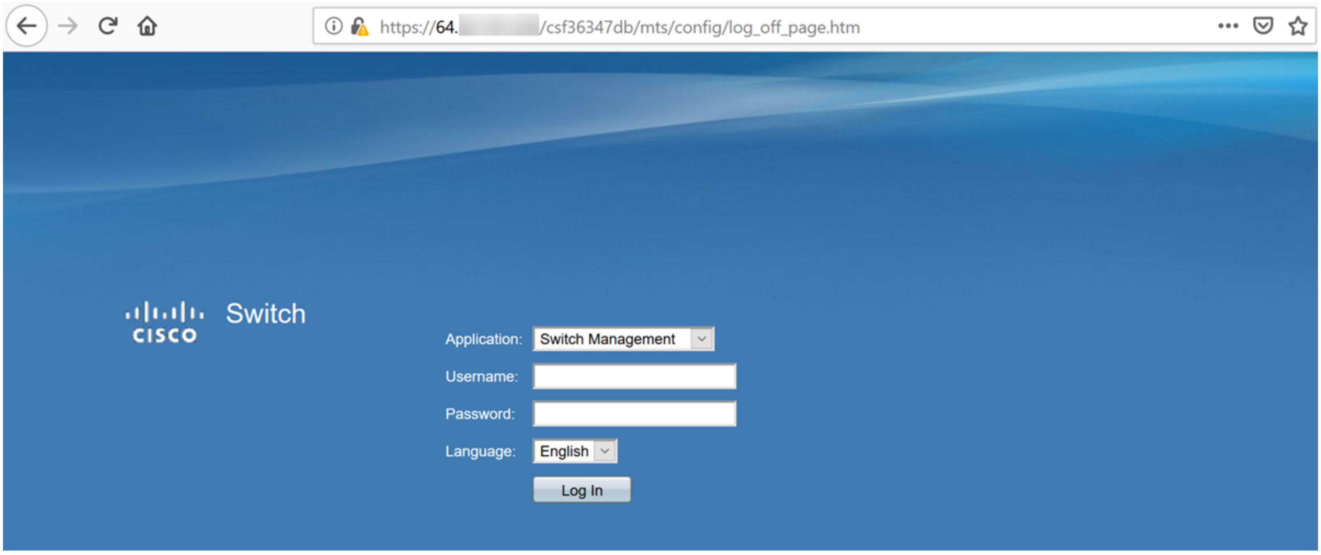


Command Prompt

```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\k[redacted]>tracert 64.[redacted]

Tracing route to ip-64-[redacted]  [64.[redacted]]
over a maximum of 30 hops:

  1     3 ms     4 ms     3 ms  testwifi.here [192.168.86.1]
  2    14 ms    15 ms    18 ms  96.[redacted]
  3    15 ms    14 ms    13 ms  po-[redacted] [68.[redacted]]
  4    73 ms    40 ms    54 ms  be-[redacted] [162.[redacted]]
  5    40 ms    23 ms    62 ms  be-[redacted] [68.[redacted]]
  6    17 ms    16 ms    17 ms  be-[redacted] [68.[redacted]]
  7    18 ms    19 ms    22 ms  be-[redacted] [68.[redacted]]
  8    23 ms    23 ms    20 ms  173.[redacted]
  9    18 ms    16 ms    16 ms  xe-[redacted] [89.[redacted]]
 10    17 ms    15 ms    20 ms  ae22-[redacted] [173.[redacted]]
 11    21 ms    25 ms    28 ms  ae22-[redacted] [173.[redacted]]
 12    23 ms    22 ms    22 ms  xe-7-[redacted] [89.[redacted]]
 13    24 ms    22 ms    22 ms  ip4.[redacted] [173.[redacted]]
 14    24 ms    21 ms    22 ms  66.[redacted]
 15    37 ms     *       31 ms  216-[redacted] [216.[redacted]]
 16    28 ms    28 ms    27 ms  ip-[redacted] [64.[redacted]]
 17    30 ms    30 ms    26 ms  ip-[redacted] [64.[redacted]]

Trace complete.

C:\Users\kevyen>
```

Step 10. (Optional) In this example, we have a switch connected to the DMZ port with the static IP address of 64.x.x.x (public IP address). We can try and access the Graphical User Interface (GUI) of the switch by entering the public IP address in the browser at the top.

We have entered **https://64.x.x.x** which brings us to the GUI page of the switch.



https://64.[redacted]/csf36347db/mts/config/log_off_page.htm

Application: Switch Management

Username:

Password:

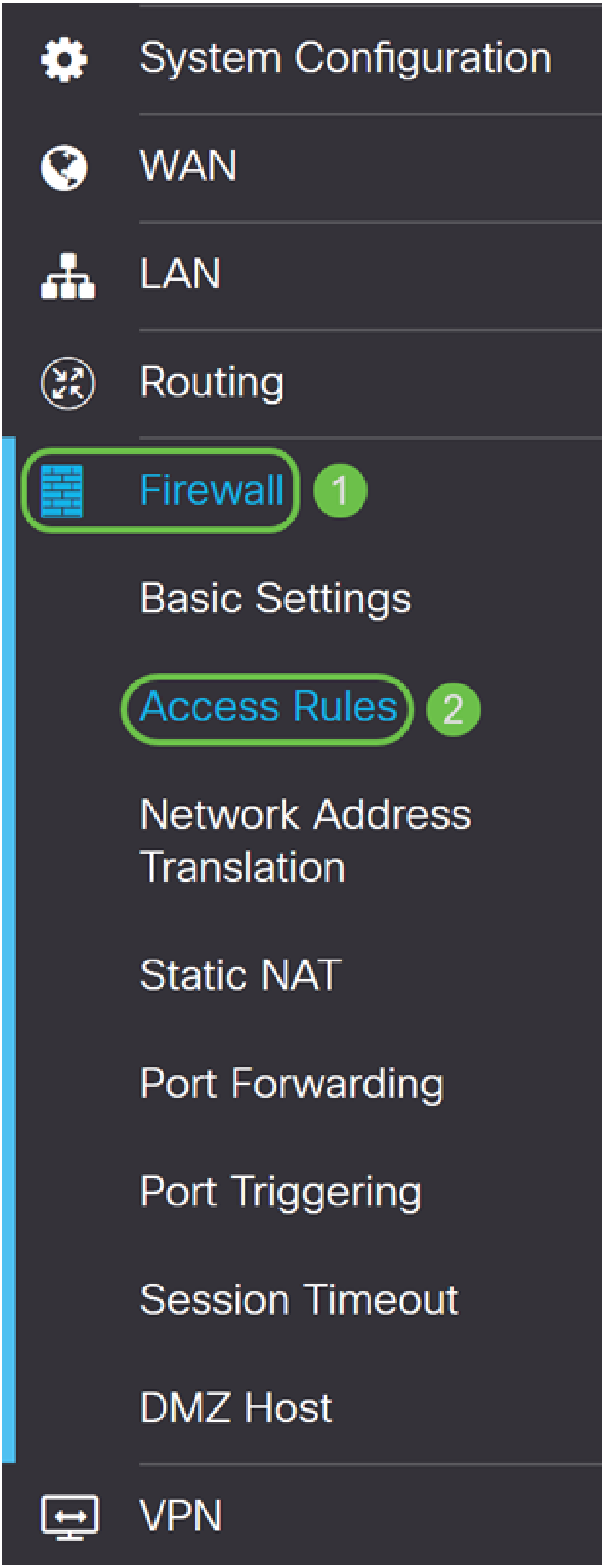
Language: English

You should now know a couple ways to verify that your DMZ is working properly.

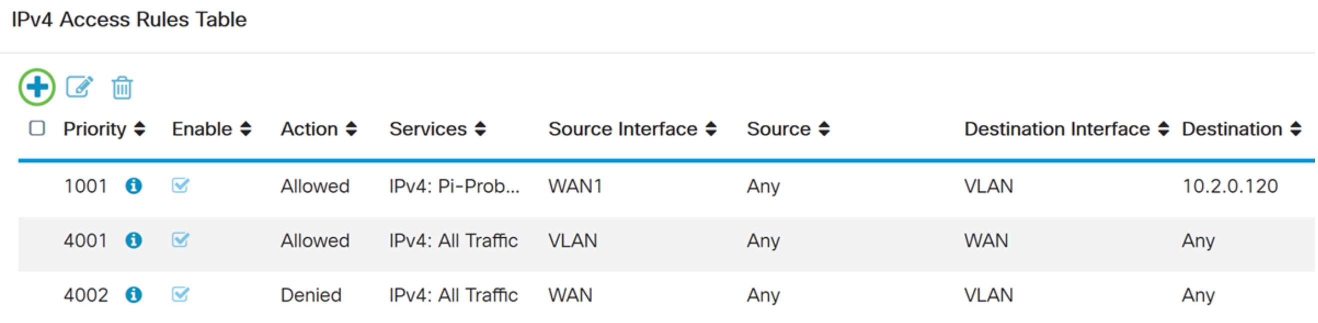
Configuring Access Rules (Optional)

If you have configured a public IP address or a range of IP address for Hardware DMZ, this section will show you an example of how to configure access rules for your DMZ. DMZ should work properly without having to configure access rules. Configuring access rules are optional but it is recommended to be configured to provide basic level of security for accessing your network. For example, if we don't configure access rules by default, all packets passing through the router could be allowed to all parts of our network. Access rules can allow one host, range of IP addresses, or a network, while preventing another host, range of IP addresses, or a network from accessing the same area (host or network). By using access rules, we can decide which types of traffic we forward or block at the router interfaces.

Step 1. Navigate to **Firewall > Access Rules**.


System Configuration
WAN
LAN
Routing
Firewall
1
Basic Settings
Access Rules
2
Network Address Translation
Static NAT
Port Forwarding
Port Triggering
Session Timeout
DMZ Host
VPN

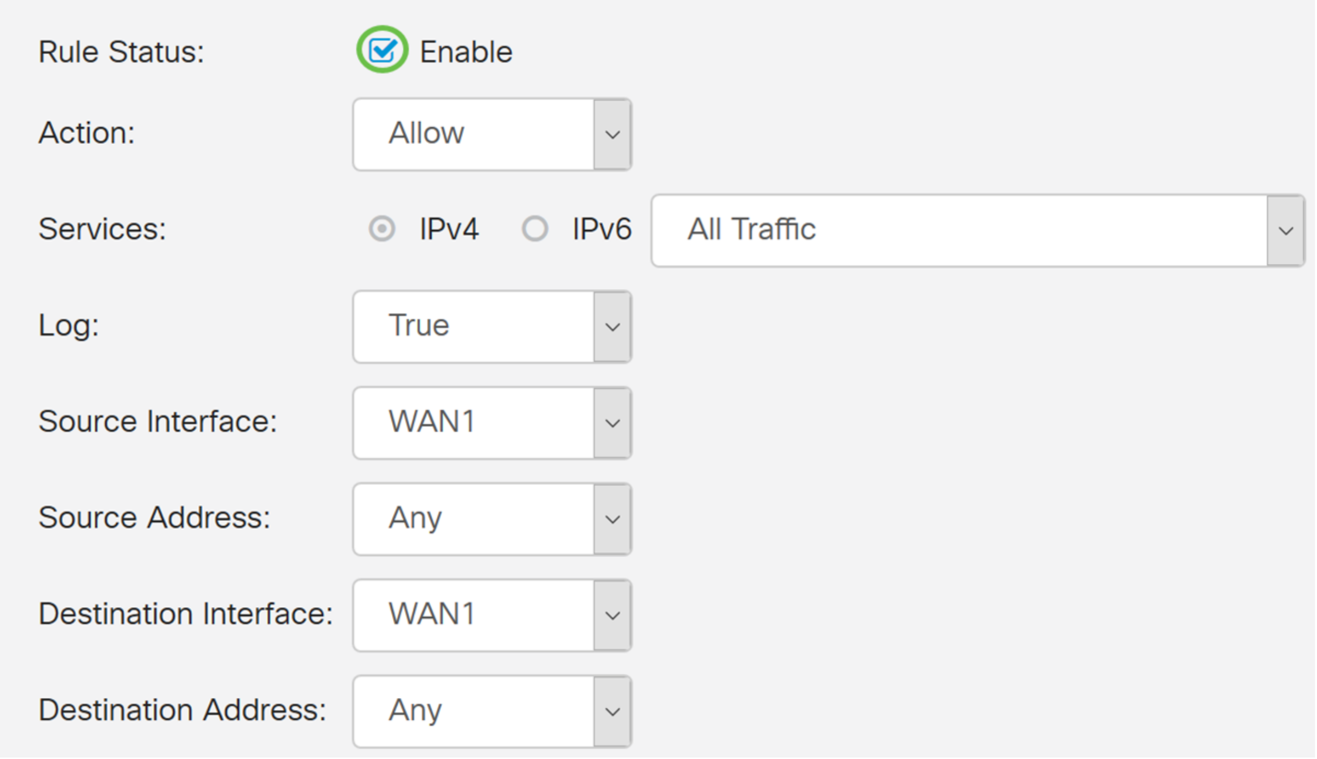
Step 2. In the *IPv4 Access Rules Table*, click the **Plus** icon to add a new IPv4 access rule.



IPv4 Access Rules Table

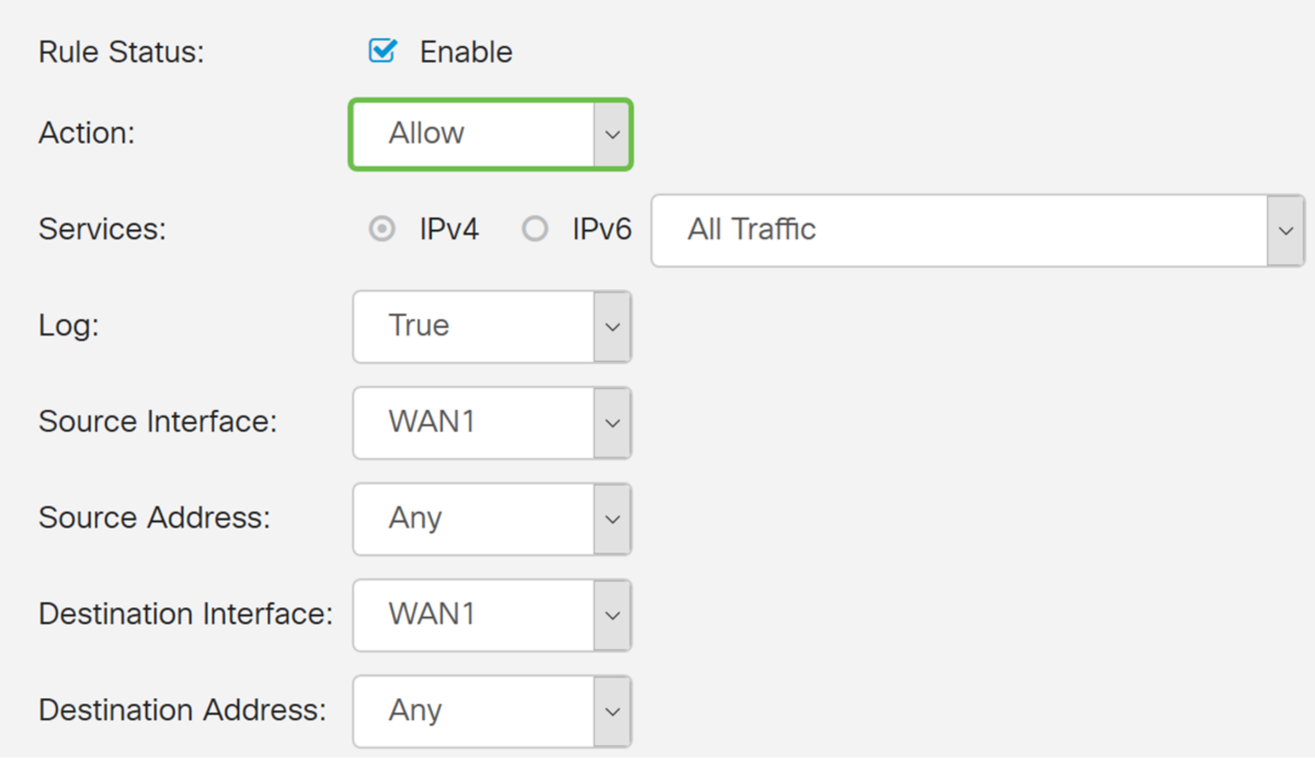
□	Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination
	1001	☑	Allowed	IPv4: Pi-Prob...	WAN1	Any	VLAN	10.2.0.120
	4001	☑	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any
	4002	☑	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any

Step 3. Ensure that the **Enable** checkbox is checked. This will enable the rule.



Rule Status:	☑ Enable
Action:	Allow
Services:	● IPv4 ○ IPv6 All Traffic
Log:	True
Source Interface:	WAN1
Source Address:	Any
Destination Interface:	WAN1
Destination Address:	Any

Step 4. In the *Action* field, select **Allow** in the drop-down list.



Rule Status: ☑ Enable

Action: Allow

Services: ● IPv4 ○ IPv6 All Traffic

Log: True

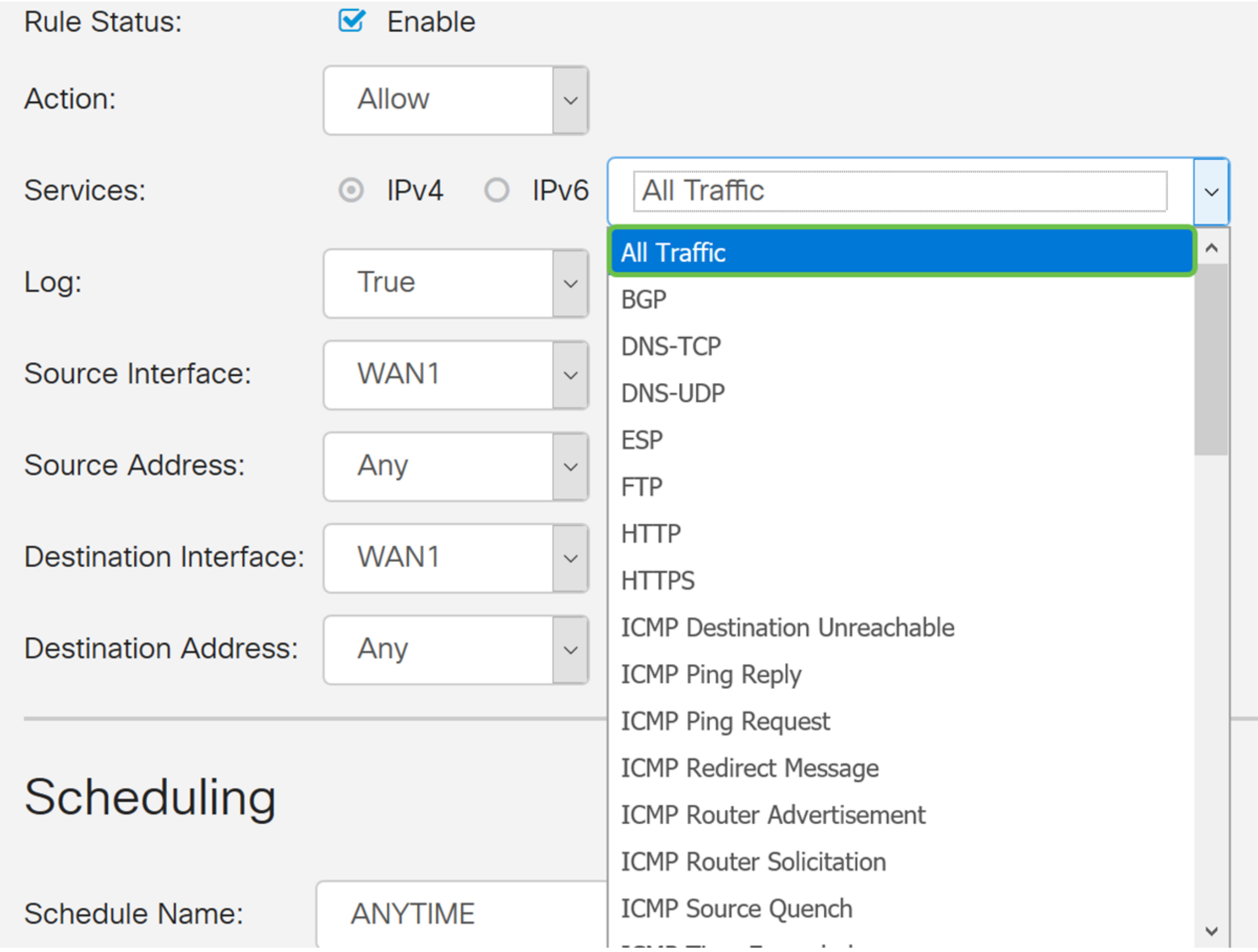
Source Interface: WAN1

Source Address: Any

Destination Interface: WAN1

Destination Address: Any

Step 5. Select a **service** in the *Services* field. We will be leaving it as **All Traffic**.



Rule Status: ☑ Enable

Action: Allow

Services: ● IPv4 ○ IPv6 All Traffic

Log: True

Source Interface: WAN1

Source Address: Any

Destination Interface: WAN1

Destination Address: Any

Scheduling

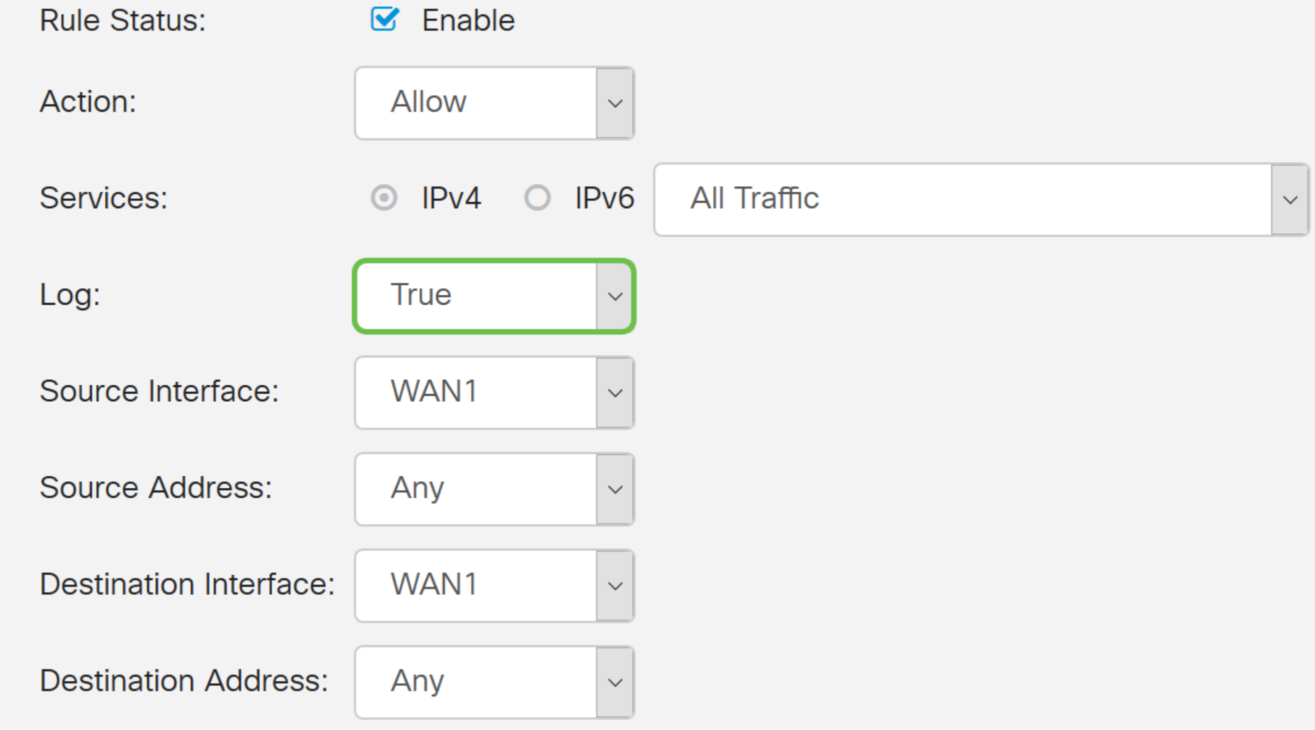
Schedule Name: ANYTIME

Step 6. Select **Never** or **True** from the drop-down list

True – Matches the rules.

Never – No log required.

In this example, we will be leaving it as **True**.



Rule Status: ☑ Enable

Action: Allow

Services: ● IPv4 ○ IPv6 All Traffic

Log: True

Source Interface: WAN1

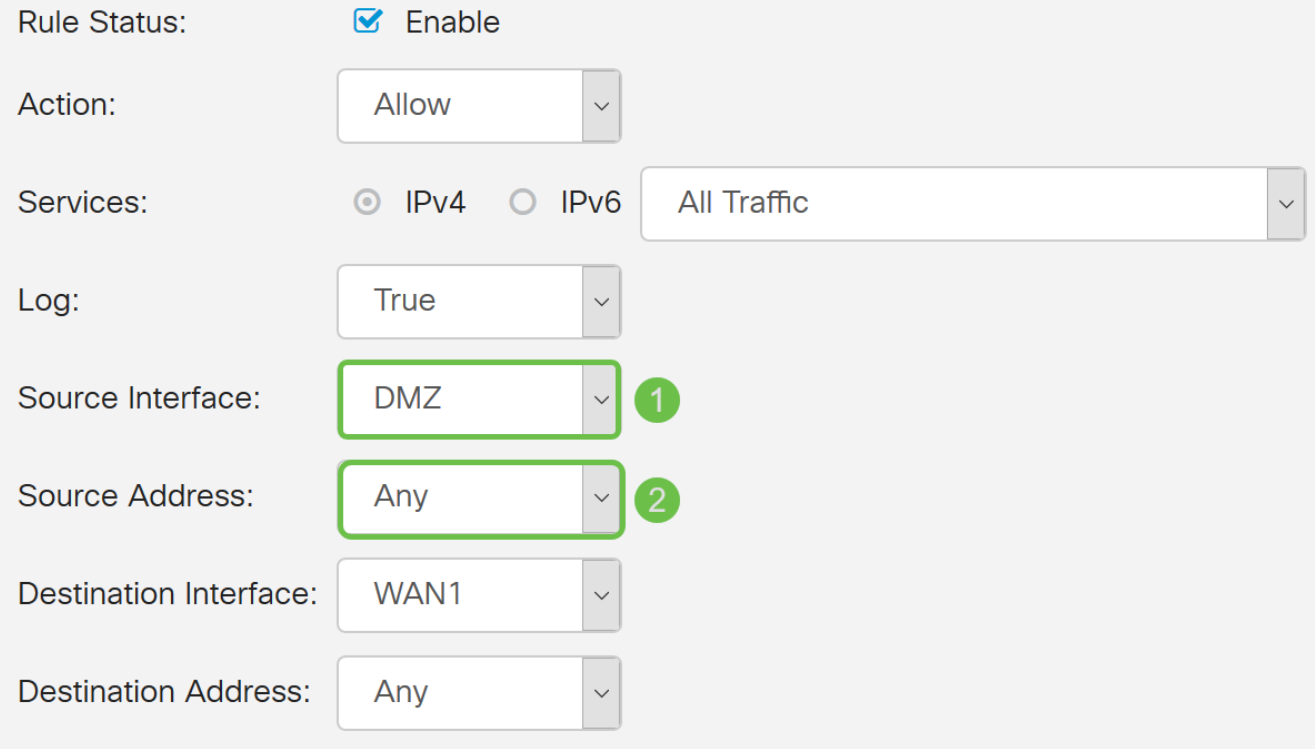
Source Address: Any

Destination Interface: WAN1

Destination Address: Any

Step 7. Select the *Source Interface* and *Source Address* from the drop-down list.

In this example, **DMZ** and **Any** was selected.



Rule Status: ☑ Enable

Action: Allow

Services: ● IPv4 ○ IPv6 All Traffic

Log: True

Source Interface: DMZ 1

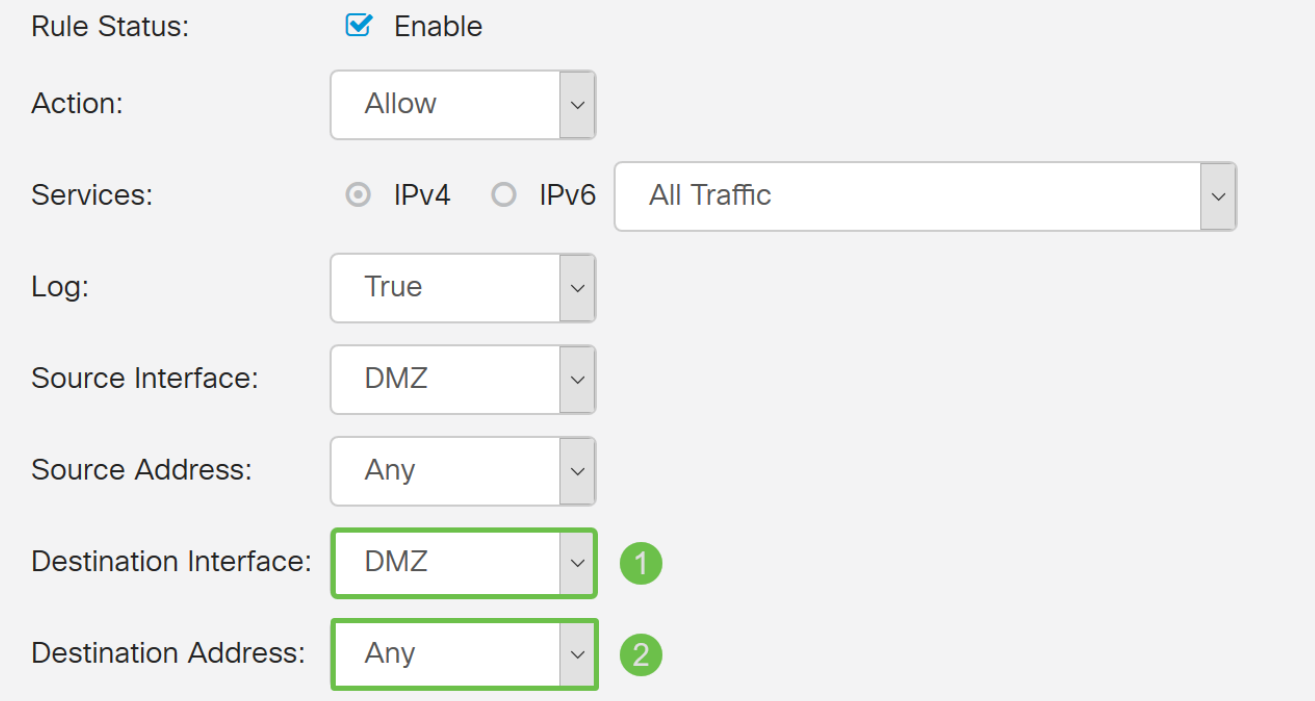
Source Address: Any 2

Destination Interface: WAN1

Destination Address: Any

Step 8. Select the *Destination Interface* and *Destination Address* from the drop-down list.

In this example, **DMZ** and **Any** was selected.


Rule Status: ☑ Enable

Action: Allow

Services: ● IPv4 ○ IPv6 All Traffic

Log: True

Source Interface: DMZ

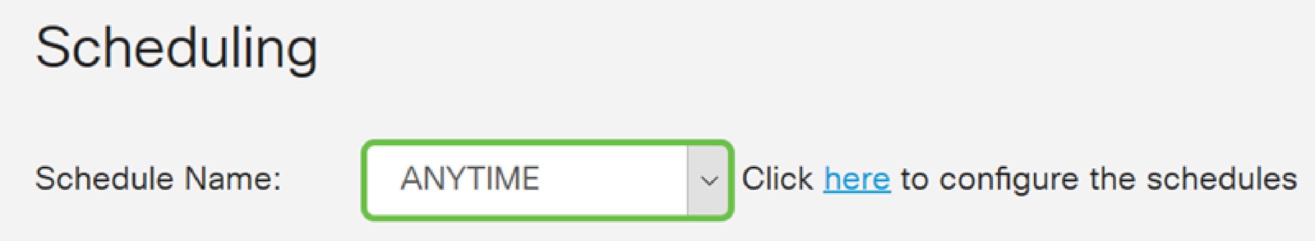
Source Address: Any

Destination Interface: DMZ

Destination Address: Any

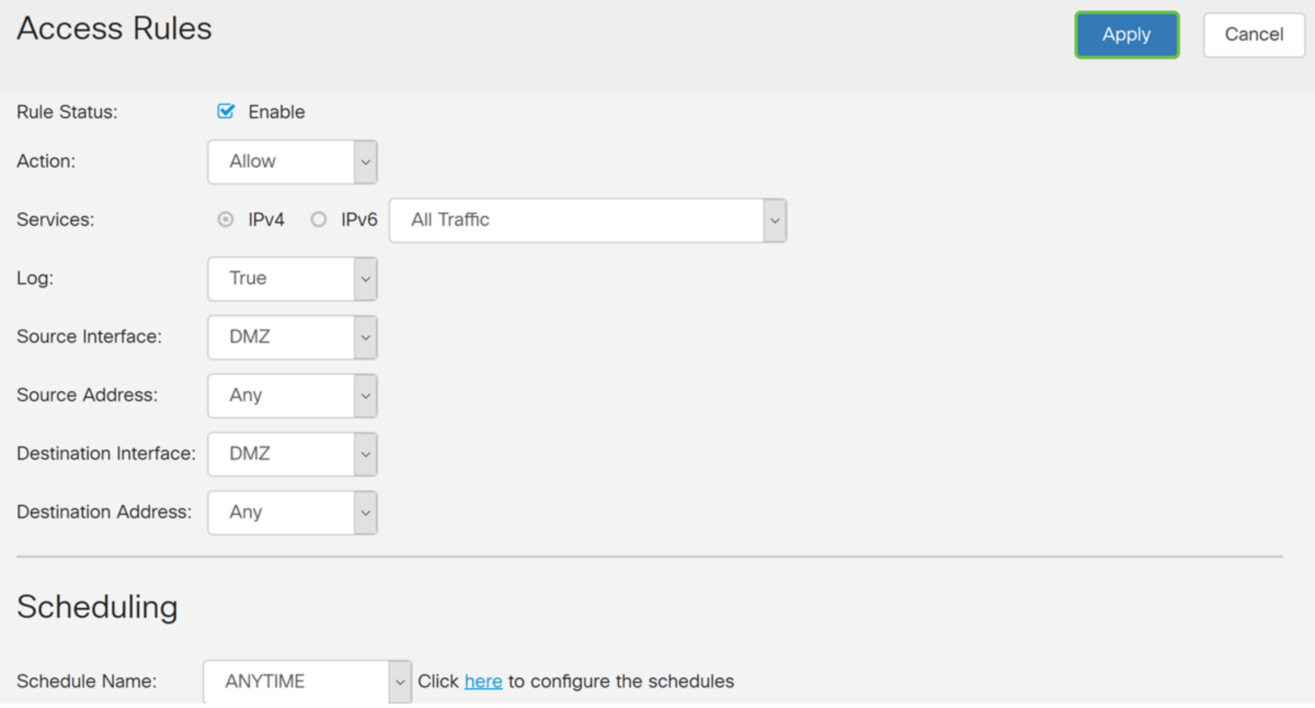
Step 9. In the *Scheduling* section, select a time from the drop-down list to apply the firewall rule. If you want to configure your own schedule, click the **here** link.

In this example, we will be using **ANYTIME** as our schedule.


Scheduling

Schedule Name: ANYTIME Click here to configure the schedules

Step 10. Click **Apply** to add the new rule. This rule says that any DMZ traffic going to any DMZ will be allowed.


Access Rules

Rule Status: ☑ Enable

Action: Allow

Services: ● IPv4 ○ IPv6 All Traffic

Log: True

Source Interface: DMZ

Source Address: Any

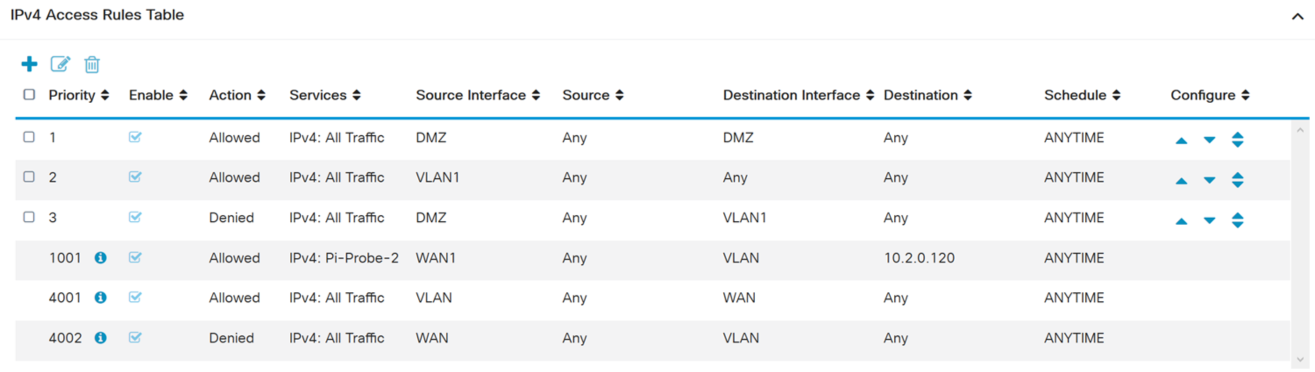
Destination Interface: DMZ

Destination Address: Any

Scheduling

Schedule Name: ANYTIME Click here to configure the schedules

Here's an example that was created. You can see that we added in a rule about DMZ not being able to communicate with any destination in VLAN 1. This is because we don't want the DMZ to be able to access anything from VLAN 1.

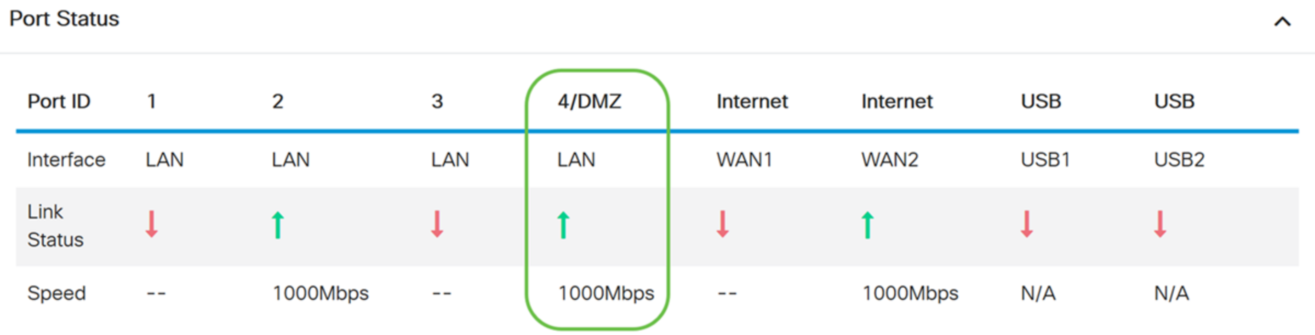


IPv4 Access Rules Table

□	Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
□	1	☑	Allowed	IPv4: All Traffic	DMZ	Any	DMZ	Any	ANYTIME	▲ ▼ ⇕
□	2	☑	Allowed	IPv4: All Traffic	VLAN1	Any	Any	Any	ANYTIME	▲ ▼ ⇕
□	3	☑	Denied	IPv4: All Traffic	DMZ	Any	VLAN1	Any	ANYTIME	▲ ▼ ⇕
	1001 ⓘ	☑	Allowed	IPv4: Pi-Probe-2	WAN1	Any	VLAN	10.2.0.120	ANYTIME	
	4001 ⓘ	☑	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any	ANYTIME	
	4002 ⓘ	☑	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any	ANYTIME	

Verifying Using the Router

Step1. To verify your device is connected in the DMZ port on the router, navigate to **Status & Statistics**, the page will load the *System Summary* page automatically. Port 4 or LAN 4 will list the status of the DMZ as "UP".

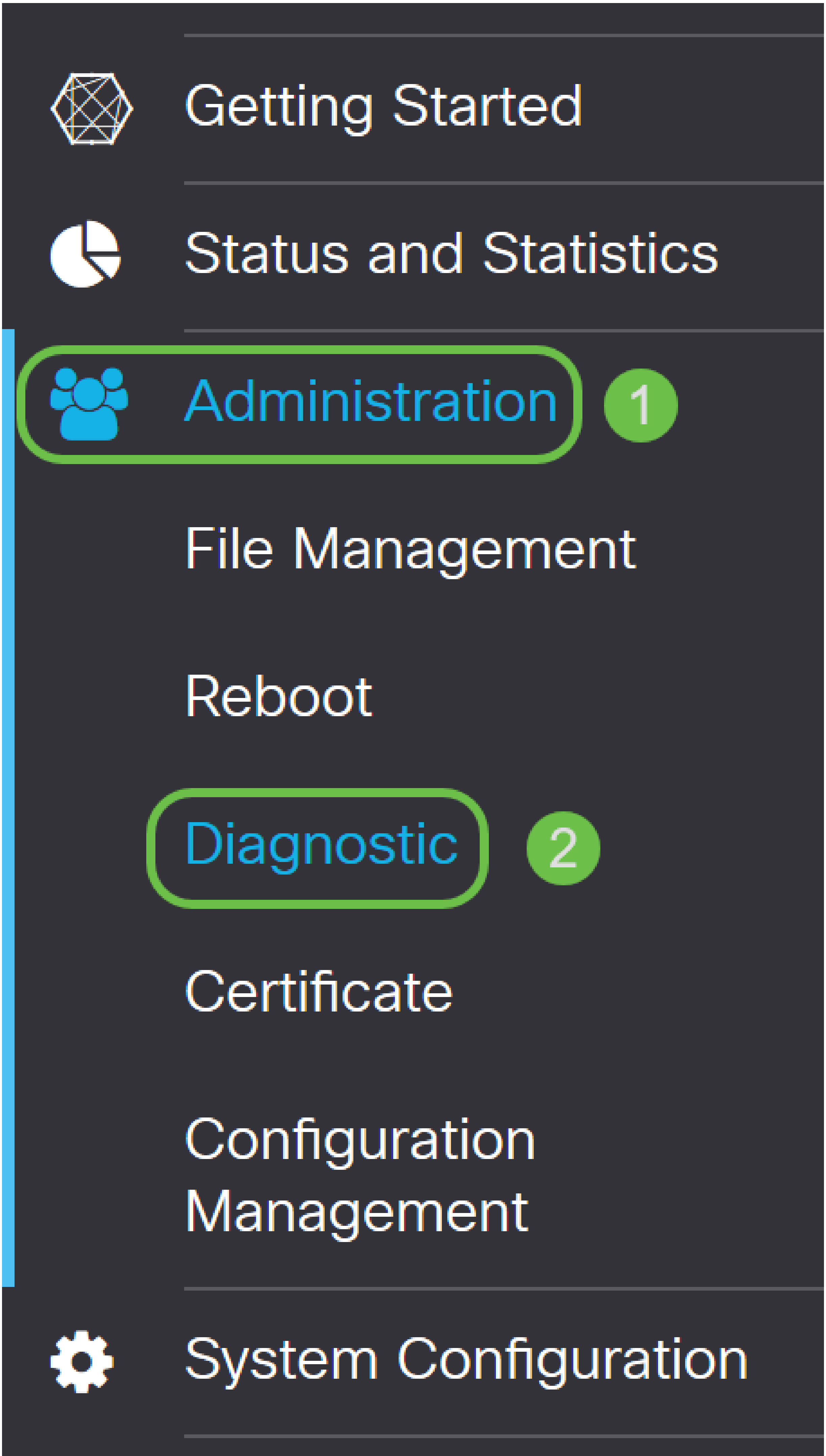


Port Status

Port ID	1	2	3	4/DMZ	Internet	Internet	USB	USB
Interface	LAN	LAN	LAN	LAN	WAN1	WAN2	USB1	USB2
Link Status	↓	↑	↓	↑	↓	↑	↓	↓
Speed	--	1000Mbps	--	1000Mbps	--	1000Mbps	N/A	N/A

Pinging the IP of the device will let us know the reachability status of the device. It will be good to verify the DMZ configuration for any specific service/port using the public IP address used.

Step 2. Navigate to **Administration > Diagnostic**.

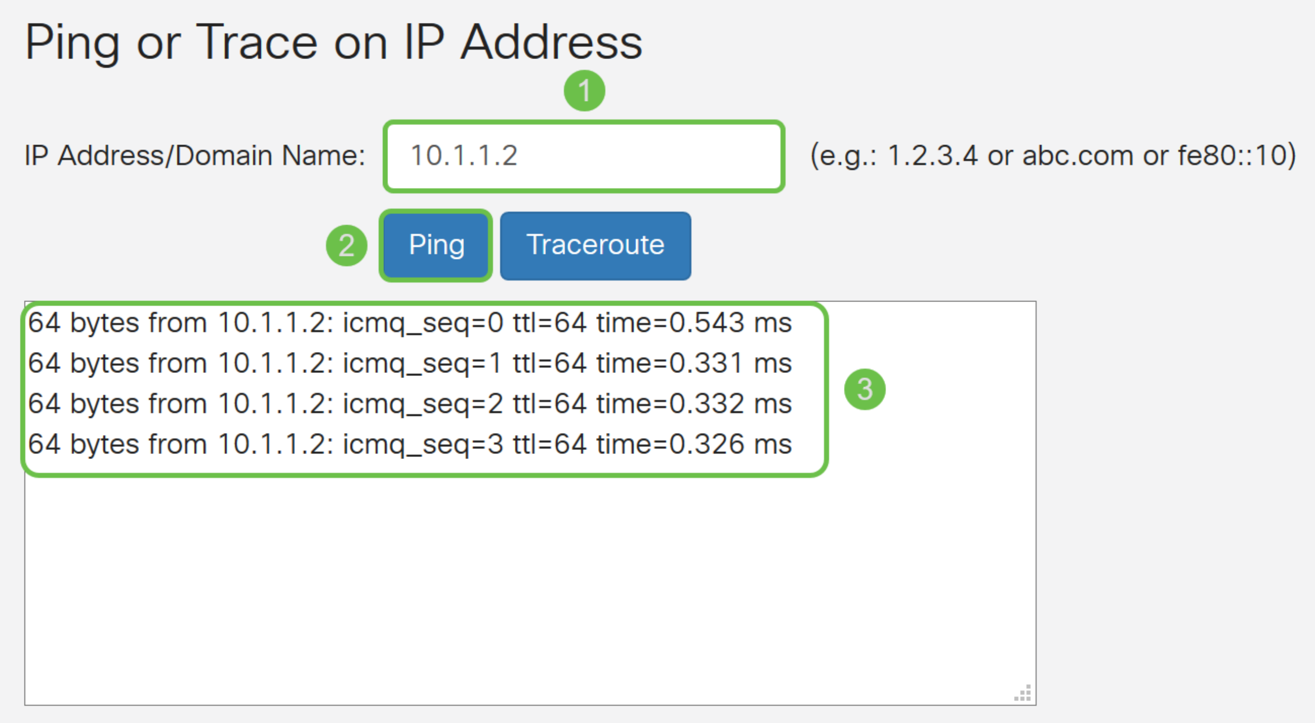


Getting Started
Status and Statistics
Administration
1
File Management
Reboot
Diagnostic
2
Certificate
Configuration Management
System Configuration

Step 3. Enter the **IP address of the DMZ** and click the **Ping** button.

In this example, we will be using the IP address of the DMZ that was configured in DMZ Host section.

Note: If the ping is successful you will see a message like shown below. If the ping fails, it means the DMZ is unable to be reached. Check your DMZ settings to ensure they are configured appropriately.


Ping or Trace on IP Address
1
IP Address/Domain Name:
10.1.1.2
(e.g.: 1.2.3.4 or abc.com or fe80::10)
2
Ping
Traceroute
3

```
64 bytes from 10.1.1.2: icmq_seq=0 ttl=64 time=0.543 ms
64 bytes from 10.1.1.2: icmq_seq=1 ttl=64 time=0.331 ms
64 bytes from 10.1.1.2: icmq_seq=2 ttl=64 time=0.332 ms
64 bytes from 10.1.1.2: icmq_seq=3 ttl=64 time=0.326 ms
```

Conclusion

Now that you have completed the setup of the DMZ, you should be able to access the services from outside the LAN.