



Firewalls

By Carlos Gerez Garcia, Christopher Ditto, and Mark Riley Slik

cit470

Task: Diagram

team 10 Layer 3: outside zones' public IPv4 address assignments

public space (IPv4 subnet ID)	router	firewall (dynamic NAT)	static NAT	(broadcast)
157.201.22.72/29	157.201.22.73	157.201.22.74 470t10ra.cit.byui.edu	157.201.22.75- 157.201.22.78	157.201.22.79

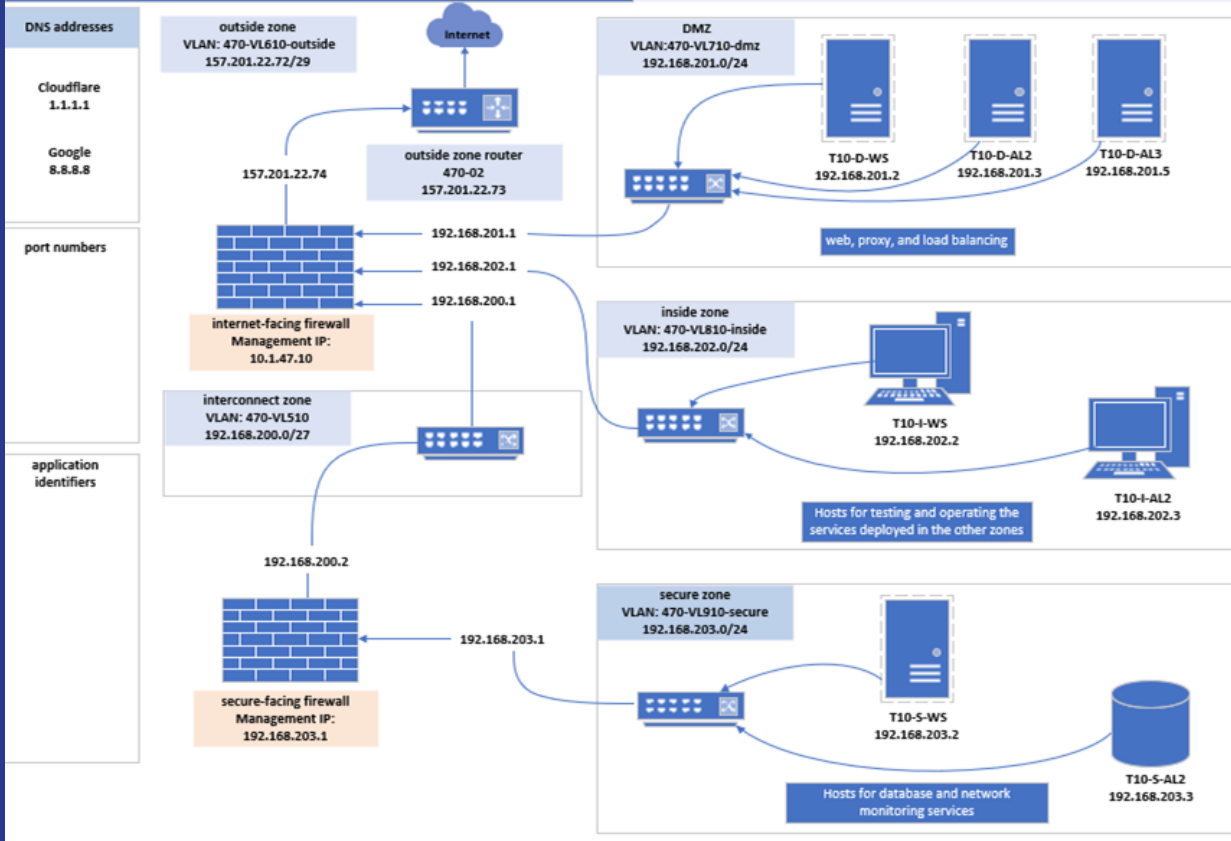
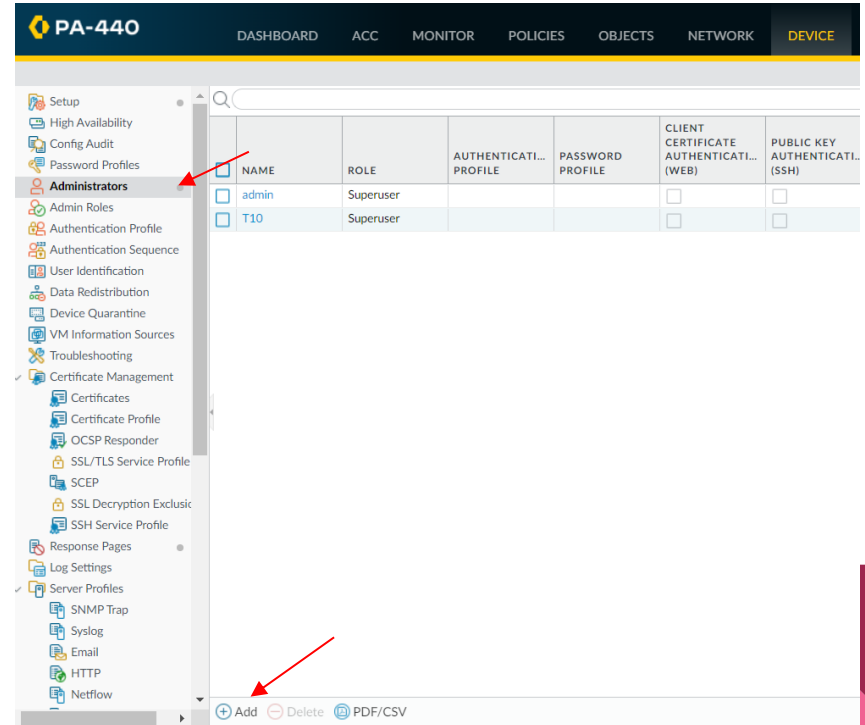


Diagram Outline for Team 10

Palo Alto PA-440 Configuration

Log into Palo Alto GUI, using the credentials given by the course instructor.

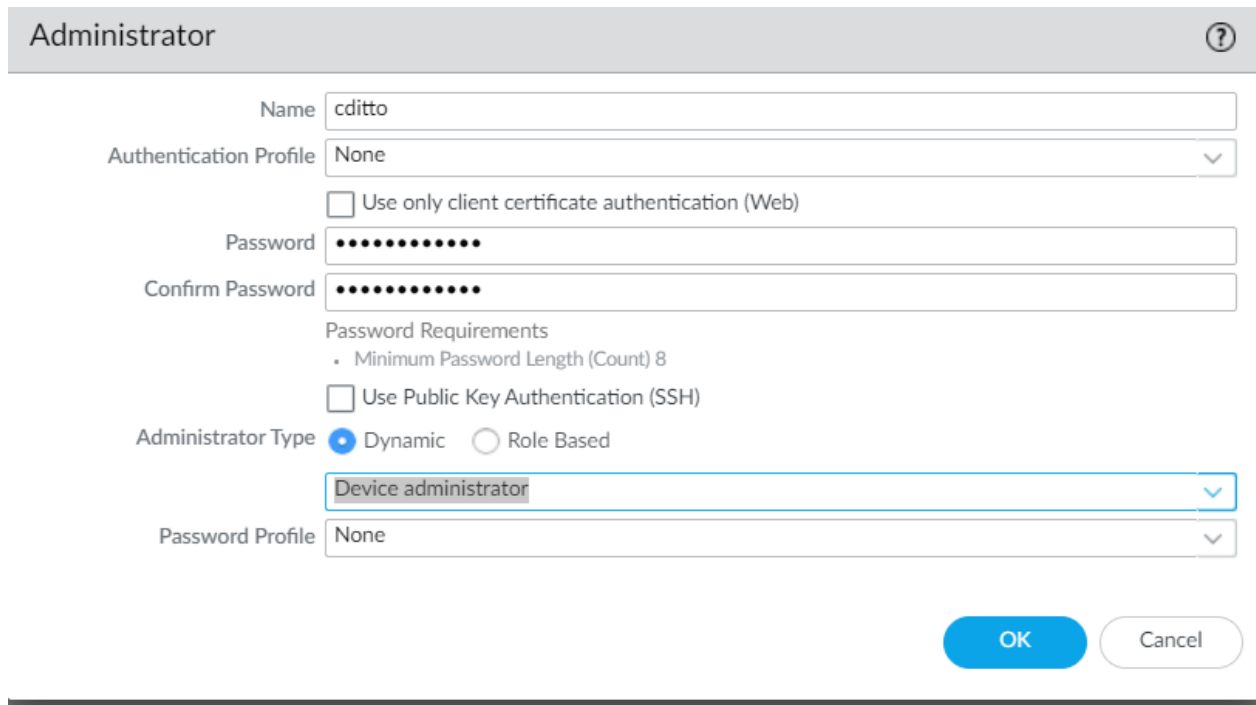
Once inside the GUI click on 'Administrators' and then on 'Add' at the bottom of the page



Palo Alto PA-440 Configuration

Create a new administrative account.

Each member off the team should create their own administrative account.



The screenshot shows the 'Administrator' configuration window in the Palo Alto PA-440 configuration interface. The window has a title bar with a question mark icon. The form contains the following fields and options:

- Name:** A text field containing 'cditto'.
- Authentication Profile:** A dropdown menu set to 'None'.
- ☐ Use only client certificate authentication (Web)
- Password:** A text field with masked characters (dots).
- Confirm Password:** A text field with masked characters (dots).
- Password Requirements:**
 - Minimum Password Length (Count) 8
- ☐ Use Public Key Authentication (SSH)
- Administrator Type:** Two radio buttons: 'Dynamic' (selected) and 'Role Based'.
- Role:** A dropdown menu set to 'Device administrator'.
- Password Profile:** A dropdown menu set to 'None'.

At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (white with a grey border).

Palo Alto PA-440 Configuration

After Creating the new account commit your changes, log out using the button at the bottom left corner.

The screenshot shows the Palo Alto PA-440 configuration interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The 'DEVICE' tab is active, and a red arrow points to the 'Commit' button in the top right corner. Below the navigation bar is a search bar and a table of users. The table has columns for NAME, ROLE, AUTHENTICATI... PROFILE, PASSWORD PROFILE, CLIENT CERTIFICATE AUTHENTICATI... (WEB), PUBLIC KEY AUTHENTICATI... (SSH), PROFILE, and LOCKED USER. The users listed are admin (Supervisor), T10 (Supervisor), and cdlto (Device administrator). Below the table, a red box highlights the 'System Resources' section, which shows Management CPU at 4%, Data Plane CPU at 0%, and Session Count at 0 / 199998. A red arrow points to the 'Session Count' text. At the bottom, a status bar shows 'cdlto | Logout | Last Login Time: 01/20/2024 22:11:00 | Session Expire Time: 02/19/2024 22:11:00 |'. To the right of the 'System Resources' section, a 'successfull' message is visible, along with 'User T10 a' and 'Commit job JobId=12.0'.

NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE	LOCKED USER
admin	Supervisor			<input type="checkbox"/>	<input type="checkbox"/>		
T10	Supervisor			<input type="checkbox"/>	<input type="checkbox"/>		
cdlto	Device administrator			<input type="checkbox"/>	<input type="checkbox"/>		

Device Certificate Status: Valid

System Resources

- Management CPU: 4%
- Data Plane CPU: 0%
- Session Count: 0 / 199998

cdlto | Logout | Last Login Time: 01/20/2024 22:11:00 | Session Expire Time: 02/19/2024 22:11:00 |

successfull

User T10 a

Commit job JobId=12.0

The screenshot shows the 'Commit' dialog box. The title bar says 'Commit'. The main text states: 'Doing a commit will overwrite the running configuration with the commit scope.' Below this, there are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) T10'. The dialog is divided into two sections: 'COMMIT SCOPE' and 'LOCATION TYPE'. The 'COMMIT SCOPE' section contains a table with one row: 'device-and-network'. The 'LOCATION TYPE' section is empty. At the bottom, there are three buttons: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these buttons is a checkbox labeled 'Group By Location Type' which is checked. Below the buttons, there is a text area labeled 'Description'. A red arrow points to the 'Commit' button at the bottom right. The 'Cancel' button is also visible.

Commit

Doing a commit will overwrite the running configuration with the commit scope.

☒ Commit All Changes ☐ Commit Changes Made By: (1) T10

COMMIT SCOPE	LOCATION TYPE
device-and-network	

☒ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit Cancel

Palo Alto PA-440 Configuration

Log back in using the new
credentials

The image shows a login interface for Palo Alto Networks. At the top, there is the Palo Alto Networks logo, which consists of an orange diamond-shaped icon made of four smaller diamonds, followed by the text "paloalto" in a bold, black, sans-serif font, with "NETWORKS" in a smaller, black, sans-serif font below it. Below the logo, there are two input fields. The first field contains the text "cditto". The second field contains a series of ten dots, indicating a password. Below these fields is a blue, rounded rectangular button with the text "Log In" in white. The entire login interface is enclosed in a yellow border.

 **paloalto**[®]
NETWORKS

cditto

.....

Log In

Palo Alto PA-440 Configuration

Select 'Virtual Router' from the left menu.

Use the default router unless instructed otherwise.

Select 'Interfaces', find the physical port labeled 'ethernet1/3' and click the label

The screenshot shows the Palo Alto PA-440 configuration interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', and 'NETWORK'. The left sidebar lists various configuration options: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers (highlighted with a red arrow), IPsec Tunnels, and GRE Tunnels. The main content area displays a table with columns: NAME, INTERFACES, CONFIGURATION, and RIP. The 'default' virtual router is selected, indicated by a red arrow pointing to the 'default' entry in the NAME column.

NAME	INTERFACES	CONFIGURATION	RIP
default		ECMP status: Disabled	

The screenshot shows the Palo Alto PA-440 configuration interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', and 'NETWORK'. The left sidebar lists various configuration options: Interfaces (highlighted with a red arrow), Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, and GlobalProtect. The main content area displays a table with columns: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, and IP ADDRESS. The 'ethernet1/3' interface is selected, indicated by a red arrow pointing to the 'ethernet1/3' entry in the INTERFACE column.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Virtual Wire		Link State: Down	none
ethernet1/2	Virtual Wire		Link State: Down	none
ethernet1/3			Link State: Up	none

Palo Alto PA-440 Configuration

Change the
'Interface Type' to
'Layer3'.

Click OK.

Ethernet Interface

Interface Name

ethernet1/3

Comment

Interface Type

Layer3

Netflow Profile

None

Config

IPv4

IPv6

SD-WAN

Advanced

Assign Interface To

Virtual Router

None

Security Zone

None

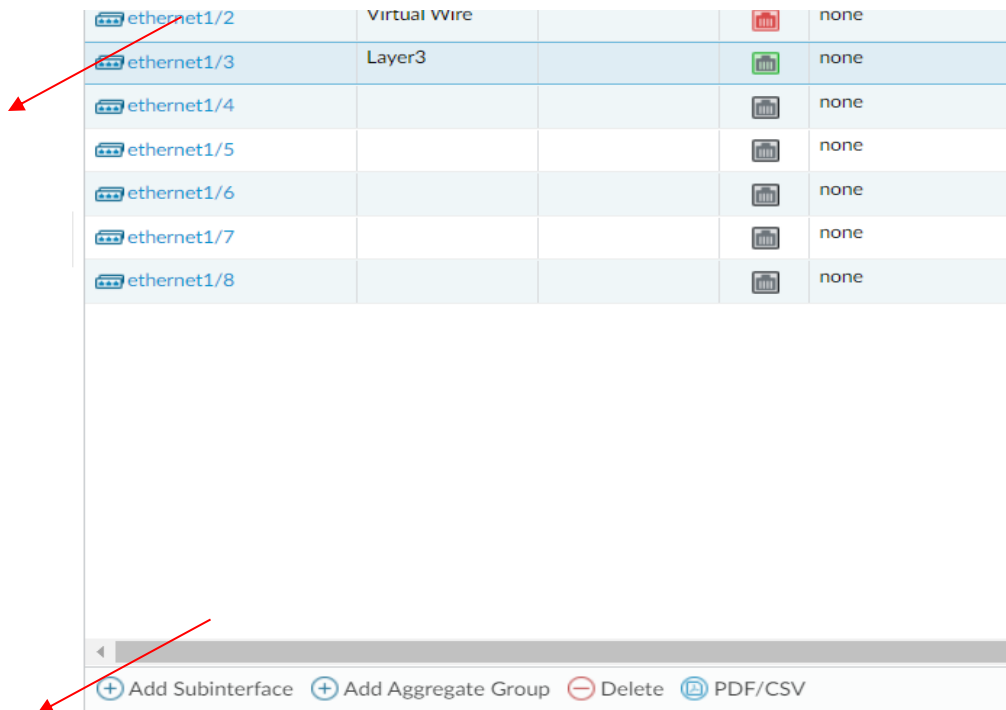
OK

Cancel

ethernet1/2	Virtual Wire			none
ethernet1/3	Layer3			none
ethernet1/4				none
ethernet1/5				none
ethernet1/6				none
ethernet1/7				none
ethernet1/8				none

Palo Alto PA-440 Configuration

Highlight
'ethernet1/3' then
click on 'Add
Subinterfaces'



The screenshot shows a configuration table with 5 columns. The first column contains interface names (ethernet1/2 to ethernet1/8), the second contains their types (Virtual Wire, Layer3, and empty), and the fifth contains their status (none). A red arrow points to the 'ethernet1/3' row. Below the table is a toolbar with four buttons: '+ Add Subinterface', '+ Add Aggregate Group', '- Delete', and 'PDF/CSV'. A second red arrow points to the '+ Add Subinterface' button.

ethernet1/2	Virtual Wire			none
ethernet1/3	Layer3			none
ethernet1/4				none
ethernet1/5				none
ethernet1/6				none
ethernet1/7				none
ethernet1/8				none

+ Add Subinterface + Add Aggregate Group - Delete PDF/CSV

Palo Alto PA-440 Configuration

Click on the 'Config' tab

Add the subinterface number and duplicate for the tag as per best practice.

Add default to the 'Virtual Router' and then click on the dropdown in the Security Zone and add New Zone.

Change zone to 'inside'.

Layer3 Subinterface

Interface Name: ethernet1/3 . 810

Comment:

Tag: 810

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: None

None

New Zone

Layer3 Subinterface

Interface Name: ethernet1/3 . 810

Comment:

Tag: 810

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

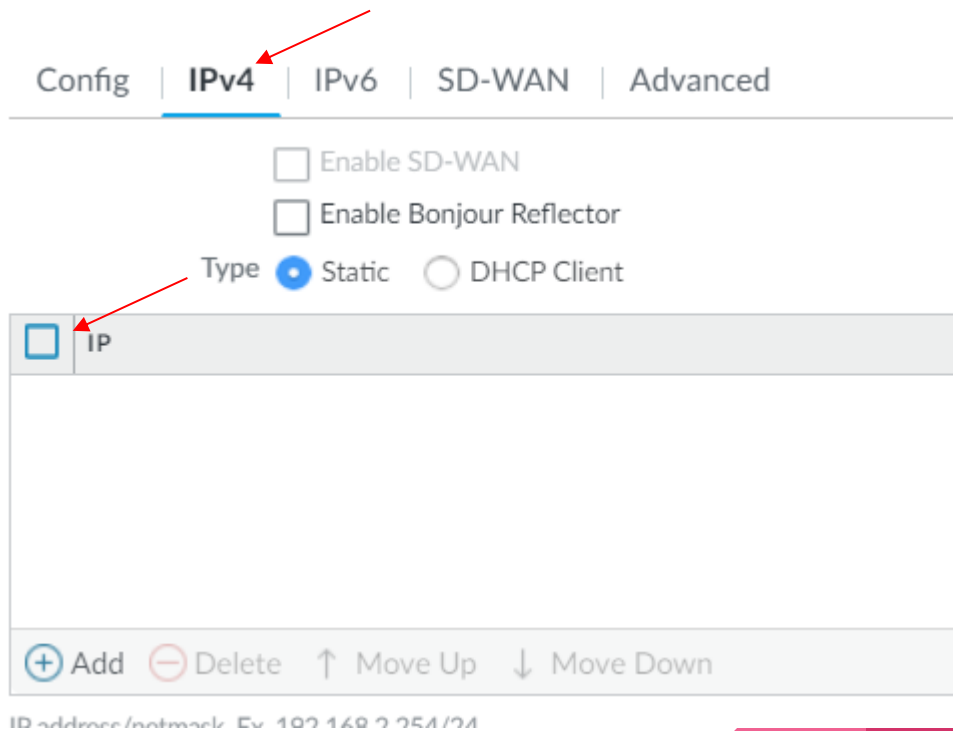
Security Zone: inside

OK Cancel

Palo Alto PA-440 Configuration

Select the 'IPv4' tab.

Select IP and add the IP address reserved for your teams firewall. Be sure to include the subnet mask suffix in CIDR notation.



The screenshot displays the Palo Alto PA-440 configuration interface. At the top, there are tabs for 'Config', 'IPv4', 'IPv6', 'SD-WAN', and 'Advanced'. The 'IPv4' tab is selected, indicated by a red arrow. Below the tabs, there are checkboxes for 'Enable SD-WAN' and 'Enable Bonjour Reflector', both of which are unchecked. Under the 'Type' section, the 'Static' radio button is selected, and the 'DHCP Client' radio button is unselected. Below this, there is a table with a single row labeled 'IP'. The 'IP' column has a red arrow pointing to it. At the bottom of the interface, there are buttons for '+ Add', '- Delete', '↑ Move Up', and '↓ Move Down'. Below these buttons, there is a text field for 'IP address/netmask' with the example '192.168.2.254/24'.

Config | **IPv4** | IPv6 | SD-WAN | Advanced

☐ Enable SD-WAN

☐ Enable Bonjour Reflector

Type ☒ Static ☐ DHCP Client

IP

+ Add - Delete ↑ Move Up ↓ Move Down

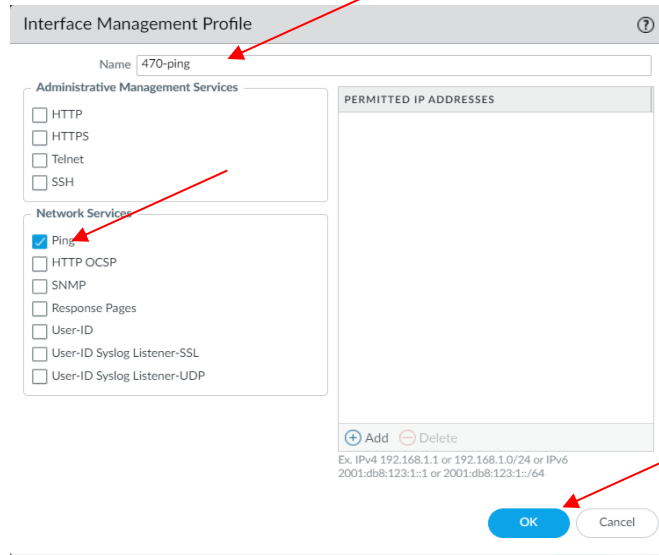
IP address/netmask Ex 192.168.2.254/24

Palo Alto PA-440 Configuration

Select the 'Advanced' tab then select 'Management Profile'











Create a profile named '470 pin' and enable the ping option in that new profile.

Click OK.



Palo Alto PA-440 Configuration

Check your work in the interface table and adjust any misconfigurations.

 ethernet1/3	Layer3			none	none	Untagged	none	none
 ethernet1/3.510	Layer3	470-ping		192.168.200.1/24	default	510	none	interconnect
 ethernet1/3.610	Layer3	470-ping		157.201.22.72/29	default	610	none	outside
 ethernet1/3.710	Layer3	470-ping		192.168.201.1/24	default	710	none	dmz
 ethernet1/3.810	Layer3	470-ping		192.168.202.1/24	default	810	none	inside

Palo Alto PA-440 Configuration

Select 'Virtual Routers' again then select the teams virtual router.

Click the 'Static Route' subtab, then create a new static route.

Name the route after your teams number and the word default.

The default route should be 0.0.0.0/0 which is the network ID for the whole internet.

The IP address of the next hop should be set to your teams assigned gateway router.

The screenshot shows the Palo Alto Networks configuration interface. On the left, the 'Virtual Routers' section is selected. On the right, a table lists the virtual routers. Below this, the 'Static Route - IPv4' configuration window is open, showing the following settings:

NAME	INTERFACES
default	ethernet1/3.810 ethernet1/3.710 ethernet1/3.610 ethernet1/3.510

Virtual Router - Static Route - IPv4						
Name	T10-default					
Destination	0.0.0.0/0					
Interface	None					
Next Hop	IP Address					
	157.201.22.73/29					
Admin Distance	10 - 240					
Metric	10					
Route Table	Unicast					
<input type="checkbox"/> Path Monitoring						
Failure Condition <input checked="" type="radio"/> Any <input type="radio"/> All Preemptive Hold Time (min) 2						
<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
<input type="button" value="Add"/> <input type="button" value="Delete"/>						

At the bottom right, there are 'OK' and 'Cancel' buttons.

Palo Alto PA-440 Configuration

Virtual Router - Static Route - IPv4

Name

T10-default

Destination

0.0.0.0/0

Interface

None

Next Hop

IP Address

157.201.22.73/29

Admin Distance

10 - 240

Metric

10

Route Table

Unicast

☐ Path Monitoring

Failure Condition

☒ Any ☐ All

Preemptive Hold Time (min)

2

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
<div><div>+ Add</div><div>- Delete</div></div>						

OK

Cancel

Palo Alto PA-440 Configuration

Click the 'Policy' tab.

Select 'Security' then click 'Add' at the bottom corner to set a new security rule.

You will set an outbound 'client' server that will allow inside zones to access Internet servers via your outside zone.

Set the name to your team name-Outbound and the rule type to universal.

The screenshot displays the Palo Alto Networks configuration interface. At the top, the 'Policies' tab is selected, indicated by a red arrow. Below the navigation bar, the 'Security' tab is also selected, with another red arrow pointing to it. The main configuration area shows the 'Security Policy Rule' page. The 'General' tab is active, and the 'Name' field is set to 'T10-outbound'. The 'Rule Type' is set to 'universal (default)', also indicated by a red arrow. The 'Description' field is empty. The 'Tags' field is empty. The 'Group Rules By Tag' is set to 'None'. The 'Audit Comment' field is empty, with a link to 'Audit Comment Archive' below it. The 'Destination' tab is also visible, with a red arrow pointing to it.

General	Source	Destination	Application	Service/URL Category	Actions
Name	T10-outbound				
Rule Type	universal (default)				
Description					
Tags					
Group Rules By Tag	None				
Audit Comment					

[Audit Comment Archive](#)

Palo Alto PA-440 Configuration

Select the 'Source' tab and then click on Add.

Add your DMZ, then click 'Add' then add your inside zone.

Under 'Source Addresses' click 'Add' and enter your teams DMZ subnet and the repeat with your inside zone subnet.

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input type="checkbox"/> Negate	

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions

<input type="checkbox"/> Any	<input type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/> dmz	<input checked="" type="checkbox"/> 192.168.201.0/24
<input checked="" type="checkbox"/> inside	<input checked="" type="checkbox"/> 192.168.202.0/24
<input type="checkbox"/> Negate	

Palo Alto PA-440 Configuration

Select the 'Destination' tab then use the same procedure to add the outside zone

Select 'Actions' tab then check the 'Log at Session Start' and 'Log at Session End' boxes.

The screenshot shows the 'Security Policy Rule' configuration page with the 'Destination' tab selected. The 'DESTINATION ZONE' dropdown is set to 'outside'. A red arrow points to the 'outside' zone. The 'Add' button at the bottom is also highlighted with a red arrow. The 'Any' checkbox is checked.

General	Source	Destination	Application	Service/URL Category	Actions
select					
<input type="checkbox"/> DESTINATION ZONE ^					
<input checked="" type="checkbox"/> outside					
<input type="checkbox"/> DESTINATION ADDRESS					
<input checked="" type="checkbox"/> Any					
<input type="checkbox"/> Negate					
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>					

The screenshot shows the 'Security Policy Rule' configuration page with the 'Actions' tab selected. The 'Log at Session Start' and 'Log at Session End' checkboxes are checked. The 'Log Forwarding' is set to 'None'. The 'Schedule' and 'QoS Marking' are set to 'None'. The 'Disable Server Response Inspection' checkbox is unchecked. A red arrow points to the 'Actions' tab.

Log Setting
<input checked="" type="checkbox"/> Log at Session Start
<input checked="" type="checkbox"/> Log at Session End
Log Forwarding: None

Other Settings
Schedule: None
QoS Marking: None
<input type="checkbox"/> Disable Server Response Inspection

Palo Alto PA-440 Configuration

Select 'NAT' on the left and then select 'Add'.

Under the 'General' tab name the new policy after your team name and the word dynamic.

The screenshot shows the Palo Alto PA-440 configuration interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', and 'POLICIES'. The left sidebar lists various configuration categories: Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, and Authentication. The 'NAT' category is selected, and a red arrow points to it. The main content area displays a table with columns 'NAME', 'TAGS', and 'SOURCE ZONE'. Below the table, the 'NAT Policy Rule' configuration page is shown. The 'General' tab is active, and a red arrow points to the 'Name' field, which contains the text 'T10-dynamic'. Other fields include 'Description', 'Tags', 'Group Rules By Tag' (set to 'None'), 'NAT Type' (set to 'ipv4'), and 'Audit Comment'. The 'Audit Comment Archive' link is visible below the 'Audit Comment' field. At the bottom right, there are 'OK' and 'Cancel' buttons.

NAME	TAGS	SOURCE ZONE
------	------	-------------

NAT Policy Rule

General | Original Packet | Translated Packet

Name: T10-dynamic

Description:

Tags:

Group Rules By Tag: None

NAT Type: ipv4

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

Palo Alto PA-440 Configuration

Click the 'Original Packet' tab.

Specify the teams DMZ and inside zones as source zones and specify the correct numbered subinterface for the teams outside zone.

The screenshot shows the 'NAT Policy Rule' configuration window with the 'Original Packet' tab selected. The configuration is as follows:

General	Original Packet	Translated Packet
SOURCE ZONE		
<input type="checkbox"/> Any		
<input type="checkbox"/> SOURCE ZONE ^		
<input type="checkbox"/> dmz		
<input checked="" type="checkbox"/> inside		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>		
Destination Zone		
outside		
Destination Interface		
ethernet1/3.610		
Service		
any		
SOURCE ADDRESS		
<input type="checkbox"/> Any		
<input checked="" type="checkbox"/> SOURCE ADDRESS ^		
<input checked="" type="checkbox"/> 192.168.201.0/24		
<input type="checkbox"/> 192.168.202.2/24		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>		
DESTINATION ADDRESS		
<input checked="" type="checkbox"/> Any		
<input type="checkbox"/> DESTINATION ADDRESS ^		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>		

At the bottom right, there are 'OK' and 'Cancel' buttons.

Palo Alto PA-440 Configuration

Select the 'Translated Packet' tab.

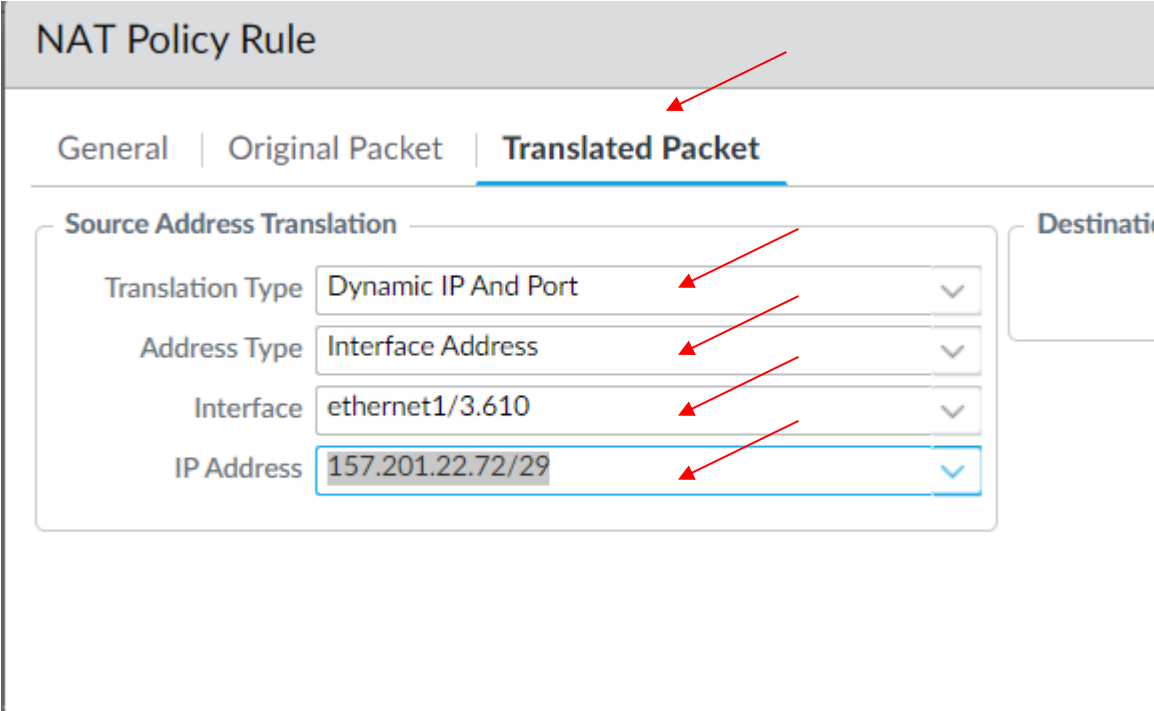
Change the 'Translation Type' to 'Dynamic IP and Port'

Change the 'Address' to 'Interface'

Specify the numbered subinterface of your outside zone Address'

Finally, select the IP address that was assigned to that subinterface.

Click OK



The screenshot displays the 'NAT Policy Rule' configuration interface. The 'Translated Packet' tab is selected, indicated by a red arrow. The 'Source Address Translation' section contains four fields, each with a red arrow pointing to it: 'Translation Type' is set to 'Dynamic IP And Port', 'Address Type' is set to 'Interface Address', 'Interface' is set to 'ethernet1/3.610', and 'IP Address' is set to '157.201.22.72/29'. The 'Destination' section is partially visible on the right.

NAT Policy Rule		
General	Original Packet	Translated Packet
Source Address Translation		
Translation Type	Dynamic IP And Port	▼
Address Type	Interface Address	▼
Interface	ethernet1/3.610	▼
IP Address	157.201.22.72/29	▼
Destination		

Palo Alto PA-440 Configuration

Review your
new NAT rule

Commit your
changes.

	NAME	TAGS	Original Packet					Translated Packet		
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	T10-dynamic	none	dmz inside	outside	ethernet1/3.610	192.168.201.0... 192.168.202.2...	any ✓	any	dynamic-ip-and-port ethernet1/3.610 157.201.22.72/29	none

Commit

Doing a commit will overwrite the running configuration with the commit scope.
☐ Commit All Changes ☒ Commit Changes Made By:(1) cdlitto

COMMIT SCOPE	LOCATION TYPE	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>
device-and-network		<input checked="" type="checkbox"/>

Preview Changes Change Summary Validate Commit ☒ Group By Location Type

Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit.
Description

Commit

Cancel

Commit Status

Operation Commit
Status Completed
Result Successful
Details Partial changes to commit: changes to configuration by administrators: cdlitto
Changes to configuration in device and network
Changes to policy and objects configuration
Configuration committed successfully

Commit

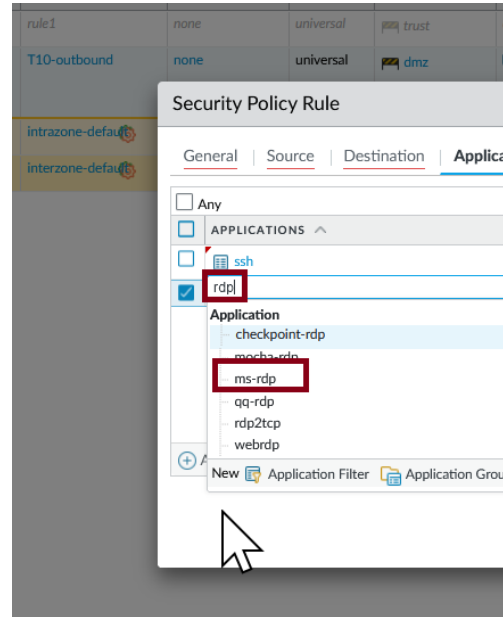
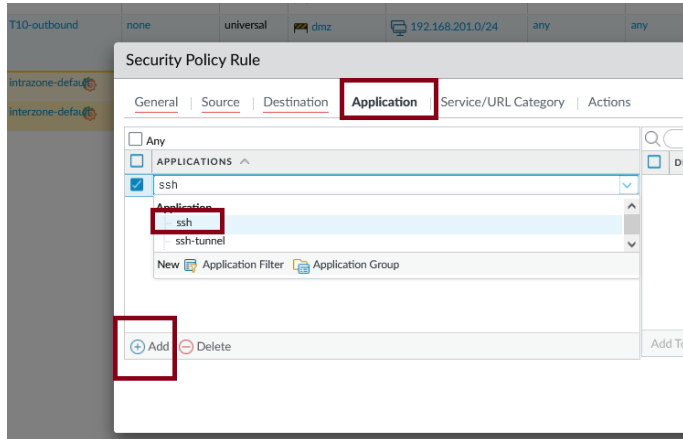
Close

Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.

The screenshot shows the Palo Alto Networks PA-440 Security Policy configuration interface. The 'POLICIES' tab is selected in the top navigation bar. On the left, the 'Security' section is expanded, showing various security features. The main table lists existing security policies, including 'T10-outbound' and 'Intrazone-default'. A 'Security Policy Rule' dialog box is open, showing the 'General' tab. The 'Name' field is empty, and the 'Rule Type' is set to 'universal (default)'. The 'Description' field is empty. The 'Tags' field is empty. The 'Group Rules By Tag' is set to 'None'. The 'Audit Comment' field is empty. The 'Audit Comment Archive' link is visible. The 'OK' and 'Cancel' buttons are at the bottom right of the dialog box. At the bottom of the interface, the 'Add' button is highlighted in the bottom left corner.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIC
1 nat1	none	universal	any	trust	any	any	any	any	any	any	any	Allow	none	
2 T10-outbound	none	universal	any	192.168.201.0/24	any	any	outside	any	any	application...	any	Allow	none	
3 Intrazone-default	none	universal	any	trust	any	any	any	any	any	any	any	Allow	none	
4 Interzone-default	none	universal	any	trust	any	any	any	any	any	any	any	Deny	none	

Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.



Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

Name: **T10-dmz-to-inside-remote-access**

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions

Any	Any
<input checked="" type="checkbox"/> SOURCE ZONE ^	<input checked="" type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/> dmz	<input checked="" type="checkbox"/> 192.168.201.0/24

[Add](#) [Delete](#) [Add](#) [Delete](#)

☐ Negate

[OK](#) [Cancel](#)

Add a Security Policy for Applications ssh and remote access to give access from DMZ to inside Zone.

The screenshot shows the 'Security Policy Rule' configuration page. The 'Destination' tab is selected. The 'Destination Zone' dropdown is set to 'inside'. The 'Destination Address' dropdown is set to '192.168.202.0/24'. The 'Destination Device' dropdown is set to 'any'. The 'Add' and 'Delete' buttons are visible at the bottom of each column.

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow	none
2	T10-outbound	none	universal	dmz outside	192.168.201.0/24 192.168.202.0/24	any	any	outside	any	any	any	application-...	Allow	none
3	T10-dmz-to-inside-r...	none	universal	dmz	192.168.201.0/24	any	any	inside	192.168.202.0...	any	ms-rdp ssh	application-...	Allow	none
4	intrazone-defau...	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
5	interzone-defau...	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

Add a Policy Rule to allow all traffic from inside towards DMZ.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

Name: T10-inside-to-dmz-all

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

Security Policy Rule

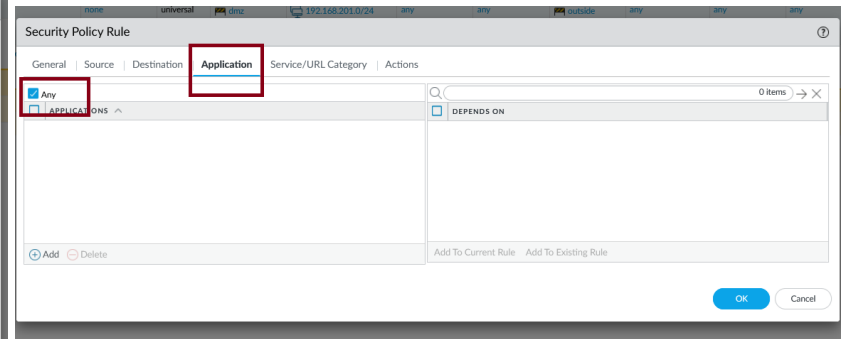
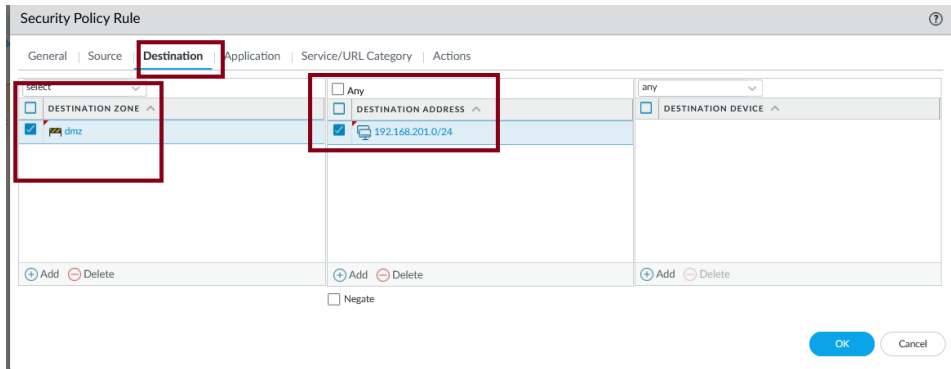
General | **Source** | Destination | Application | Service/URL Category | Actions

Any	Any	any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER
<input checked="" type="checkbox"/> inside	<input checked="" type="checkbox"/> 192.168.202.0/24	

+ Add - Delete + Add - Delete + Add - Delete

☐ Negate

Add a Policy Rule to allow all traffic from inside towards DMZ.



The new rules created for Remote Desktop and for the intern zone.

PA-440 DASHBOARD ACC MONITOR **POLICIES** OBJECTS NETWORK DEVICE

Consent

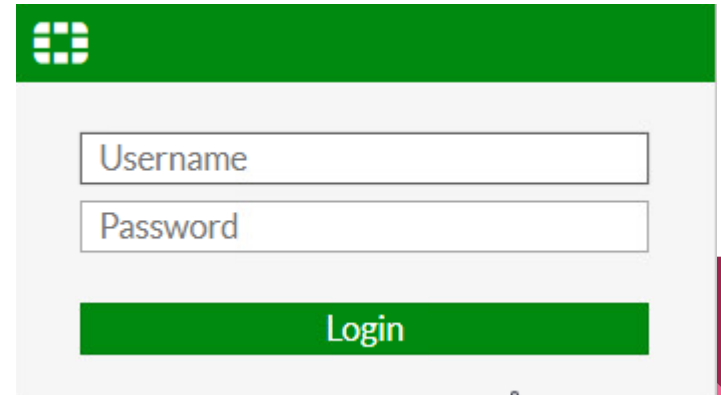
Security 6 items

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow
2	T10-outbound	none	universal	dmz	192.168.201.0/24	any	any	outside	any	any	any	application-...	Allow
3	T10-dmz-to-inside-remote-access	none	universal	dmz	192.168.201.0/24	any	any	inside	192.168.202.0/24	any	ms-rdp	application-...	Allow
4	T10-inside-to-dmz-all	none	universal	inside	192.168.202.0/24	any	any	dmz	192.168.201.0/24	any	ssh	application-...	Allow
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Policy Optimizer

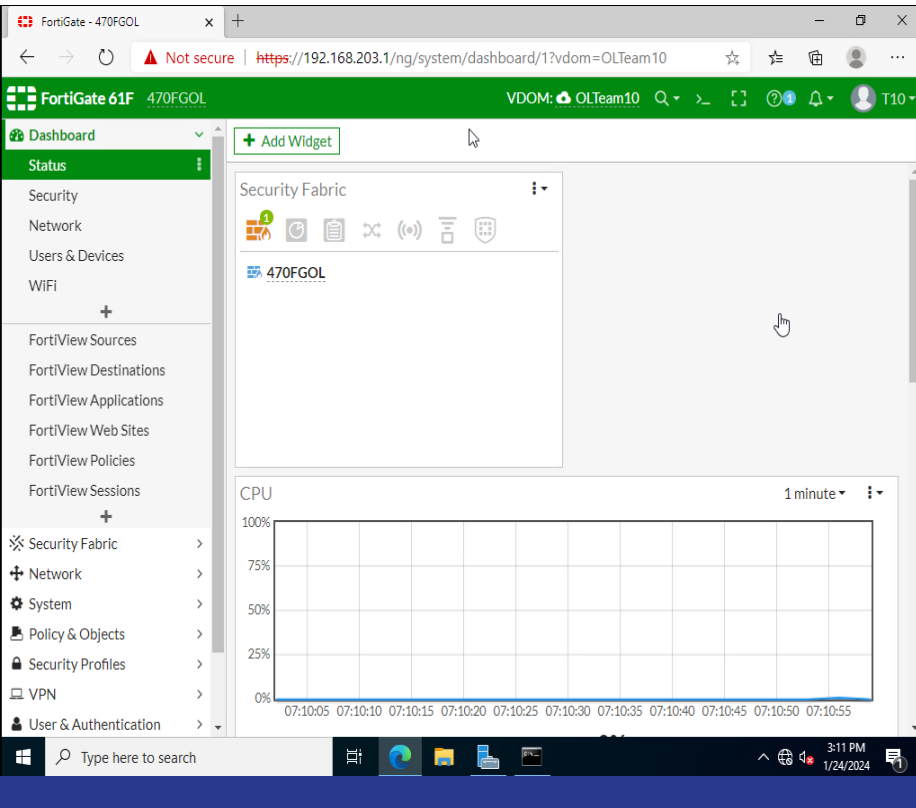
Fortigate Configurations

Connect to your windows secure server and connect to Fortigate by using a web browser and entering the ip address for your gateway. You should have the login credentials



The image shows a screenshot of the Fortigate web interface. At the top is a green header bar with the Fortigate logo on the left. Below the header is a light gray login box. Inside this box, there are two white input fields: the top one is labeled 'Username' and the bottom one is labeled 'Password'. Below these fields is a green button with the word 'Login' in white text. The entire interface is set against a white background with a decorative pink and purple geometric shape at the bottom right.

Go to System Administrator and make new Admin account for yourself



New Administrator

Username	<input type="text" value="Riley"/>
Type	<div><div>Local User</div><div>Match a user on a remote server group</div><div>Match all users in a remote server group</div><div>Use public key infrastructure (PKI) group</div></div>
Password	<input type="password" value="••••••••"/> <input type="checkbox"/>
Confirm Password	<input type="password" value="••••••••"/> <input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Administrator Profile	<div></div>

☐ Two-factor Authentication

☐ Restrict login to trusted hosts

☐ Restrict admin to guest account provisioning only

Go to Interface and make new one for the interconnect Zone making sure to fill out the vlan and Ip info and enabling ping

FortiGate - 470FGOL

Not secure | <https://192.168.203.1/ng/interface/edit?vdom=OLTeam10>

FortiGate 61F 470FGOL VDOM: OLTeam10

Dashboard > Security Fabric > Network > Interfaces

New Interface

Address

Addressing mode: Manual DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask: 192.168.200.2/24

Create address object matching subnet: ☒

Name: Interconnect address

Destination: 192.168.200.2/24

Secondary IP address: ☐

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection

☒ DHCP Server

Network

Device detection: ☒

Security mode: ☐

OK Cancel

FortiGate - 470FGOL

Not secure | <https://192.168.203.1/ng/interface/edit?vdom=OLTeam10>

FortiGate 61F 470FGOL VDOM: OLTeam10

Dashboard > Security Fabric > Network > Interfaces

New Interface

Name: Interconnect

Alias:

Type: VLAN

Interface:

VLAN ID: 510

Virtual domain: OLTeam10

Role: LAN

Addressing mode: Manual DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask: 192.168.200.2/24

Create address object matching subnet: ☒

Name: Interconnect address

Destination: 192.168.200.2/24

Secondary IP address: ☐

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☒ PING

OK Cancel

Make a Static route going to the Palo Alto Firewall in the interconnect zone

The image shows two side-by-side browser windows of the FortiGate 61F 470FGOL web interface. The left window displays the 'Static Routes' configuration page, which is currently empty with the message 'No results'. The right window shows the 'New Static Route' configuration form. In this form, the 'Destination' is set to 'Subnet' with the value '0.0.0.0/0.0.0.0'. The 'Gateway Address' is '192.168.200.1' and the 'Interface' is 'Interconnect'. The 'Administrative Distance' is '10'. The 'Status' is 'Enabled'. At the bottom of the form are 'OK' and 'Cancel' buttons. The interface includes a green top bar with the device name and VDOM, and a left sidebar with navigation menus for Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report.

FortiGate 61F 470FGOL VDOM: OLTeam10

Dashboard > **+ Create New** Edit Clone Delete Search

Destination Gateway IP Interface Status Comments

No results

FortiGate 61F 470FGOL VDOM: OLTeam10

Dashboard > New Static Route

Security Fabric >

Network >

Interfaces >

Packet Capture >

SD-WAN Zones >

SD-WAN Rules >

Performance SLA >

Static Routes >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Authentication >

WiFi & Switch Controller >

Log & Report >

Destination **Subnet** Internet Service

0.0.0.0/0.0.0.0

Gateway Address 192.168.200.1

Interface Interconnect

Administrative Distance 10

Comments Write a comment... 0/255

Status **Enabled** Disabled

Advanced Options

OK Cancel

Go to Policy & Object select address and choose new address and add an object for each zone

The screenshot displays the FortiGate 61F web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Security Fabric, Network, System, Policy & Objects (highlighted), Firewall Policy, Addresses (highlighted), Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, VPN, User & Authentication, and WiFi & Switch. The main content area is titled 'New Address' and includes the following fields: Name (DMZ), Color (Change), Type (Subnet), IP/Netmask (192.168.201.0/24), Interface (any), Static route configuration (toggle), and Comments (Write a comment...). At the bottom of the form are 'OK' and 'Cancel' buttons. The right sidebar shows the FortiGate 470FGOL status and a list of guides for configuring dynamic addresses from various cloud providers. The top of the browser window shows the URL 'https://192.168.203.1/ng/firewall/address/edit?vdom=OLTeam10' and the user 'Riley' is logged in.

FortiGate - 470FGOL

Not secure | https://192.168.203.1/ng/firewall/address/edit?vdom=OLTeam10

FortiGate 61F 470FGOL VDOM: OLTeam10 Riley

Dashboard

Security Fabric

Network

System

Policy & Objects

Firewall Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Security Profiles

VPN

User & Authentication

WiFi & Switch

New Address

Name DMZ

Color Change

Type Subnet

IP/Netmask 192.168.201.0/24

Interface any

Static route configuration

Comments Write a comment... 0/255

OK Cancel

FortiGate 470FGOL

Dynamic Address

Guides

Configuring an AWS Dynamic Address

Configuring an Azure Dynamic Address

Configuring a Google Cloud Platform Dynamic Address

Configuring an Oracle Cloud Infrastructure Dynamic Address

Configuring an OpenStack Dynamic Address

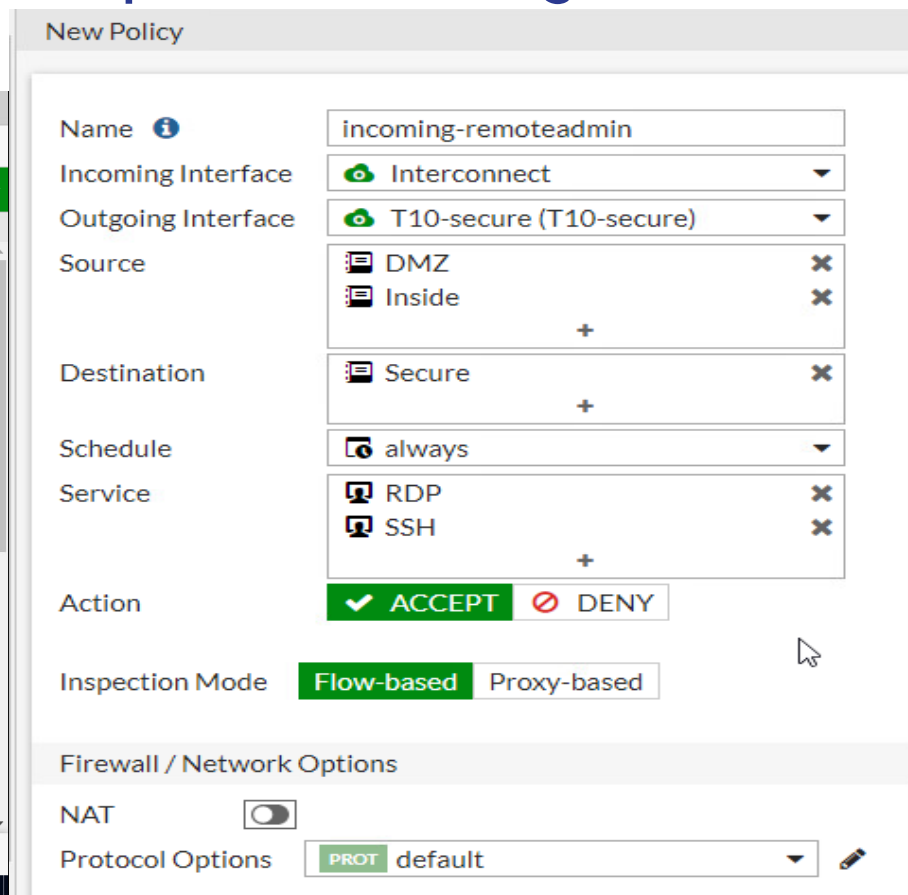
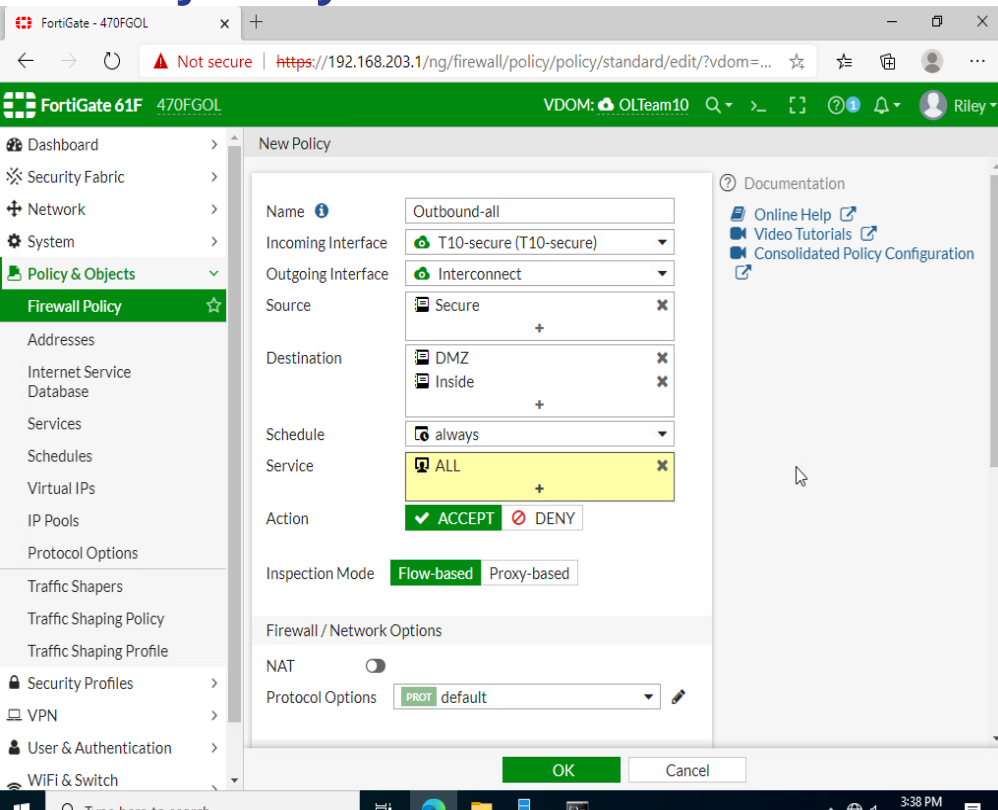
Documentation

Online Help

Video Tutorials

3:31 PM 1/24/2024

Inside of Policy & Objects select Firewall policies and make an outbound and rdp/ssh policies using the new object you made.



Review all the Policies and enable ALL for logging

+ Create New

Edit

Delete

Policy Lookup

Search

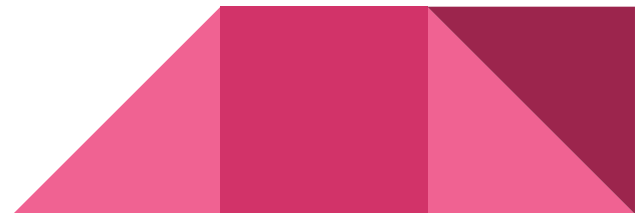
Export ▾

Interface Pair View

By Sequence

Schedule	Service	Action	NAT	Security Profiles	Log
always	RDP SSH	ACCEPT	Disabled	no-inspection	All
always	ALL	ACCEPT	Disabled	no-inspection	All
always	ALL	DENY			Enabled

Challenges we faced



Misconfiguration in Palo Alto firewall.

We didn't have connections from the secure zone since we configure Palo Alto policy with the ip range from the firewall instead of the secure zone. We find the problem when we review our diagram and tested the change.

Was corrected from 192.168.200.0/24 to 192.168.203.0/24.

[illegible]

Linux SSH connections \$PATH problems.

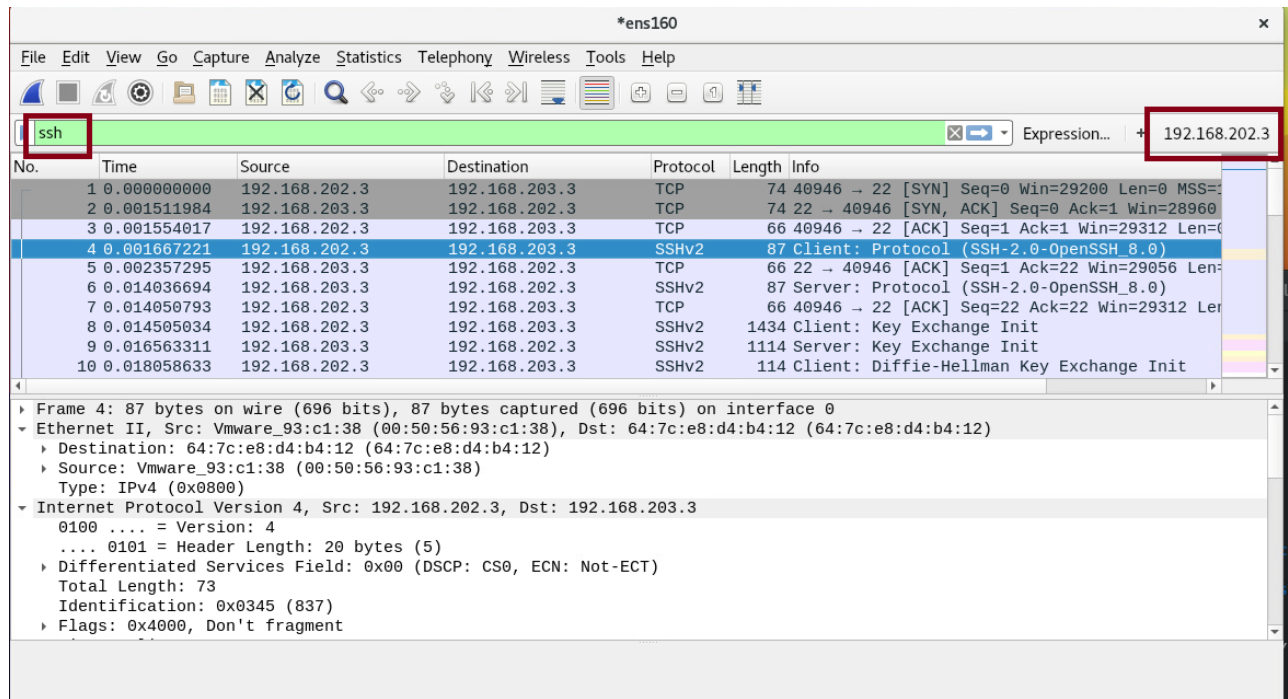
T10-I-AL2 - VMware Workstation 17 Player (Non-commercial use only)

The screenshot displays a VMware Workstation 17 Player interface. The main window shows a terminal session on a Linux VM named T10-I-AL2. The terminal output shows the user 'cgarcia' running commands to check the \$PATH environment variable. The commands 'ls /usr/bin' and 'ls /usr/local/bin' both return empty results. The user then attempts to connect to a remote host '192.168.202.3' using 'ssh'. The terminal output shows a successful SSH connection to the host '192.168.202.3' with the last login on Jan 27 02:24:58 2024. The packet capture window, titled 'Capturing from ens160', shows a list of network packets. Packet 49 is highlighted, showing an SSH client protocol connection from 192.168.202.3 to 192.168.202.3. The file explorer at the top shows the contents of the '/usr/bin' directory, which is empty.

On the Linux systems on intern, the ssh connection where established towards secure zone, but the terminal just stale without showing the terminal in the secure zone we were connecting.

After checking ssh packages in that machine using Wireshark we realized that the connection exist, and that means that the problem was not in the firewalls, but in the ssh configuration on the Linux we run ssh. We run ssh with the full path (/usr/bin/ssh) and worked. The misconfiguration was in the \$PATH to ssh.

Linux SSH connections \$PATH problems.



The image shows a Wireshark network traffic capture window titled '*ens160'. The filter bar at the top contains the filter 'ssh' and a filter expression '192.168.202.3'. The packet list on the left shows a series of packets, with the selected packet (No. 4) highlighted in blue. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and SSHv2. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.202.3	192.168.203.3	TCP	74	40946 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=
2	0.001511984	192.168.203.3	192.168.202.3	TCP	74	22 → 40946 [SYN, ACK] Seq=0 Ack=1 Win=28960
3	0.001554017	192.168.202.3	192.168.203.3	TCP	66	40946 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0
4	0.001667221	192.168.202.3	192.168.203.3	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_8.0)
5	0.002357295	192.168.203.3	192.168.202.3	TCP	66	22 → 40946 [ACK] Seq=1 Ack=22 Win=29056 Len=0
6	0.014036694	192.168.203.3	192.168.202.3	SSHv2	87	Server: Protocol (SSH-2.0-OpenSSH_8.0)
7	0.014050793	192.168.202.3	192.168.203.3	TCP	66	40946 → 22 [ACK] Seq=22 Ack=22 Win=29312 Len=0
8	0.014505034	192.168.202.3	192.168.203.3	SSHv2	1434	Client: Key Exchange Init
9	0.016563311	192.168.203.3	192.168.202.3	SSHv2	1114	Server: Key Exchange Init
10	0.018058633	192.168.202.3	192.168.203.3	SSHv2	114	Client: Diffie-Hellman Key Exchange Init

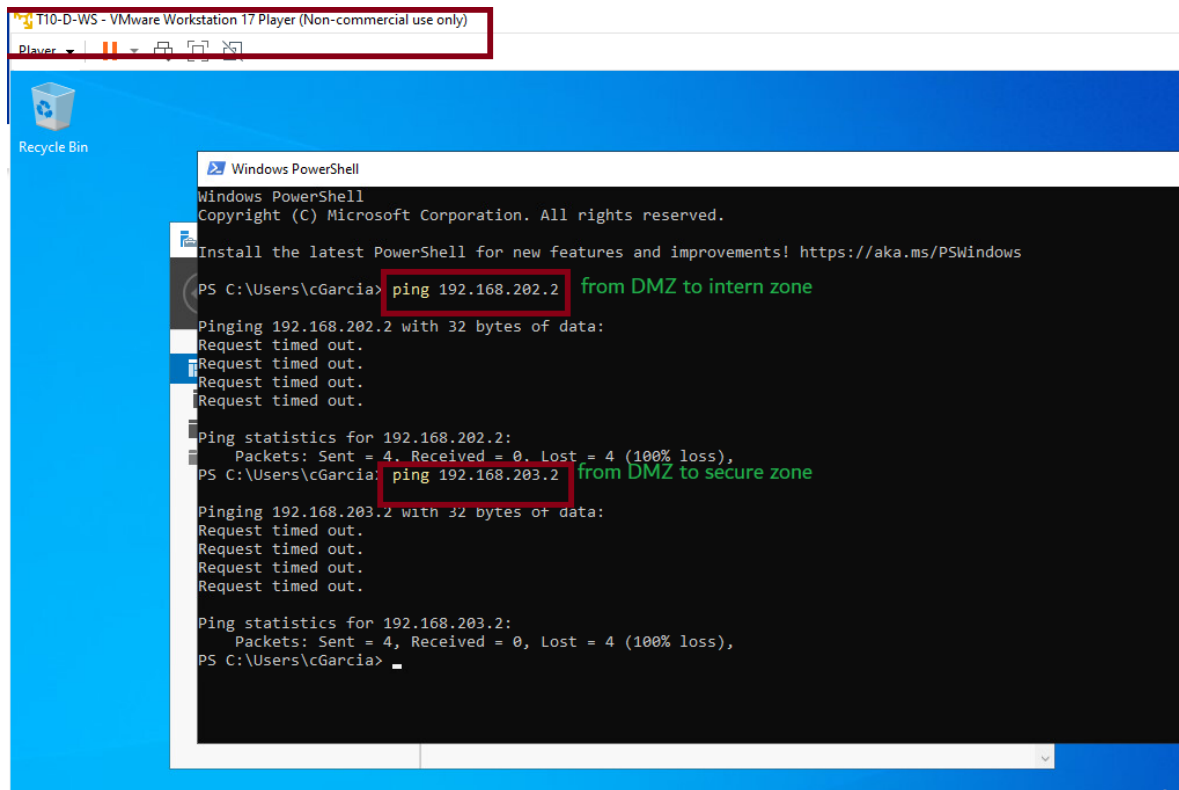
Frame 4: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
Ethernet II, Src: Vmware_93:c1:38 (00:50:56:93:c1:38), Dst: 64:7c:e8:d4:b4:12 (64:7c:e8:d4:b4:12)
Destination: 64:7c:e8:d4:b4:12 (64:7c:e8:d4:b4:12)
Source: Vmware_93:c1:38 (00:50:56:93:c1:38)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.202.3, Dst: 192.168.203.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 73
Identification: 0x0345 (837)
Flags: 0x4000, Don't fragment

Use of filters on Wireshark to isolate ssh connections.

Connectivity tests.



Testing connectivity with ping between zones



The screenshot shows a Windows PowerShell terminal window within a VMware Workstation 17 Player. The window title is "T10-D-WS - VMware Workstation 17 Player (Non-commercial use only)". The terminal output shows the following commands and results:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\cGarcia> ping 192.168.202.2 from DMZ to intern zone

Pinging 192.168.202.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.202.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\cGarcia> ping 192.168.203.2 from DMZ to secure zone

Pinging 192.168.203.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.203.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\cGarcia>
```

From DMZ zone.

Testing connectivity with ping between zones

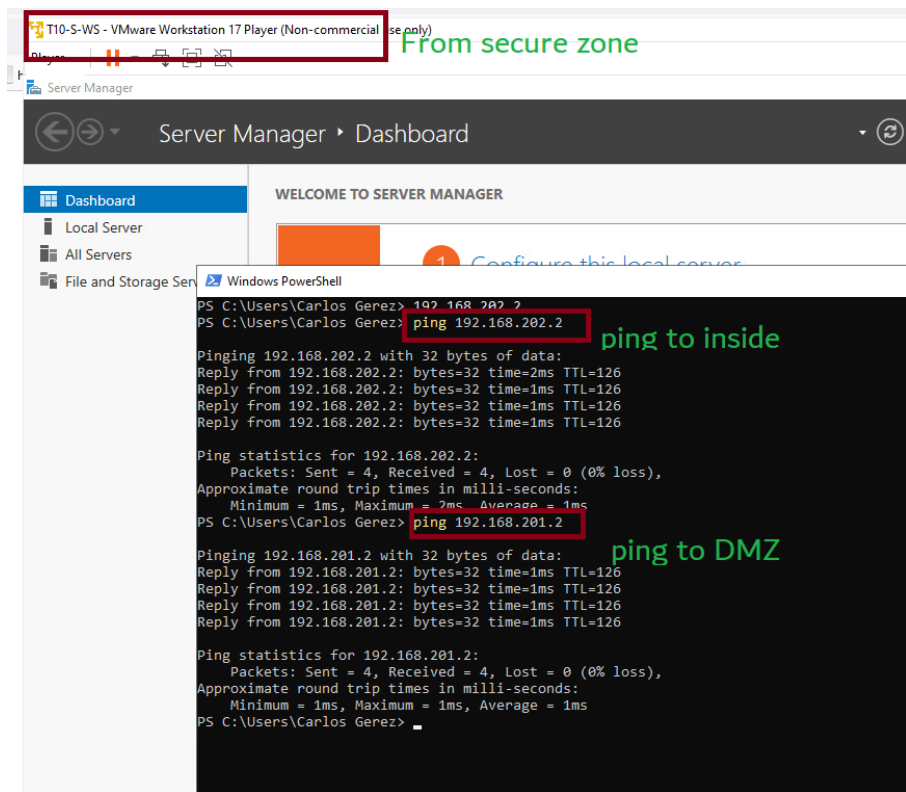
```
PS C:\Users\cgarcia> ping 192.168.201.2
Pinging 192.168.201.2 with 32 bytes of data:
Reply from 192.168.201.2: bytes=32 time<1ms TTL=127
Reply from 192.168.201.2: bytes=32 time=1ms TTL=127
Reply from 192.168.201.2: bytes=32 time=1ms TTL=127
Reply from 192.168.201.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\cgarcia> ping 192.168.203.2
Pinging 192.168.203.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.203.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\cgarcia>
```

From inside zone.

Testing connectivity with ping between zones



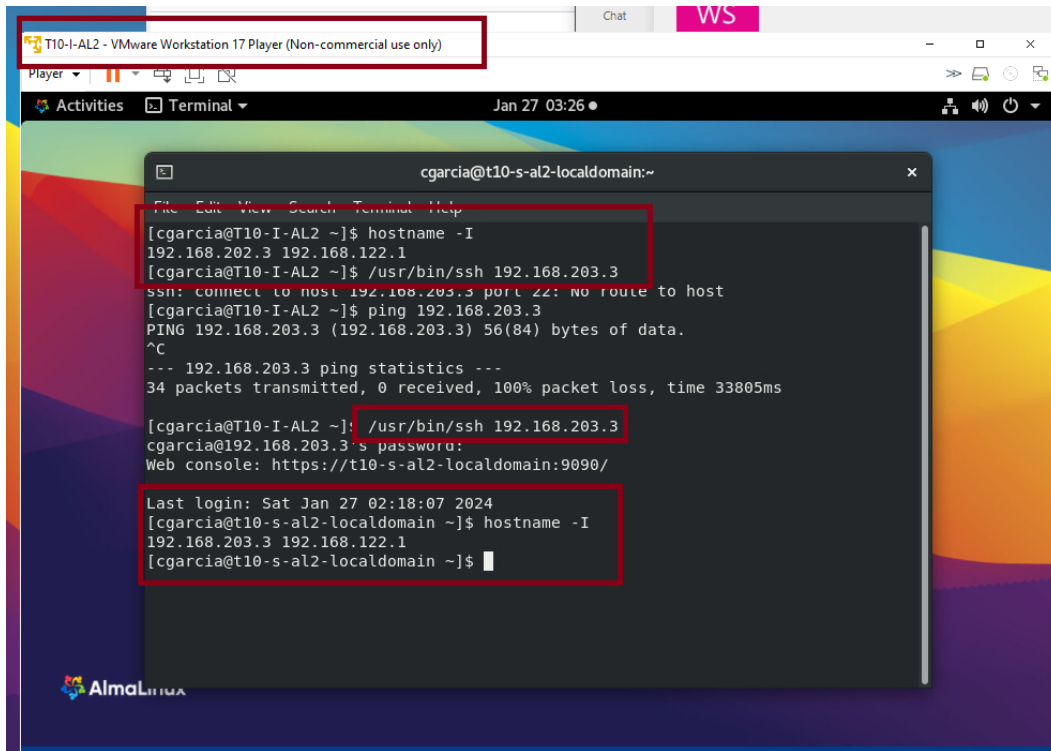
The screenshot shows a Windows PowerShell terminal window with the following content:

```
PS C:\Users\Carlos Gerez> 192.168.202.2
PS C:\Users\Carlos Gerez> ping 192.168.202.2
Pinging 192.168.202.2 with 32 bytes of data:
Reply from 192.168.202.2: bytes=32 time=2ms TTL=126
Reply from 192.168.202.2: bytes=32 time=1ms TTL=126
Reply from 192.168.202.2: bytes=32 time=1ms TTL=126
Reply from 192.168.202.2: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.202.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\Carlos Gerez> ping 192.168.201.2
Pinging 192.168.201.2 with 32 bytes of data:
Reply from 192.168.201.2: bytes=32 time=1ms TTL=126
Reply from 192.168.201.2: bytes=32 time=1ms TTL=126
Reply from 192.168.201.2: bytes=32 time=1ms TTL=126
Reply from 192.168.201.2: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Carlos Gerez>
```

Green text annotations are present: "From secure zone" at the top, "ping to inside" next to the first ping command, and "ping to DMZ" next to the second ping command. The IP addresses in the commands are highlighted with red boxes.

From secure zone.

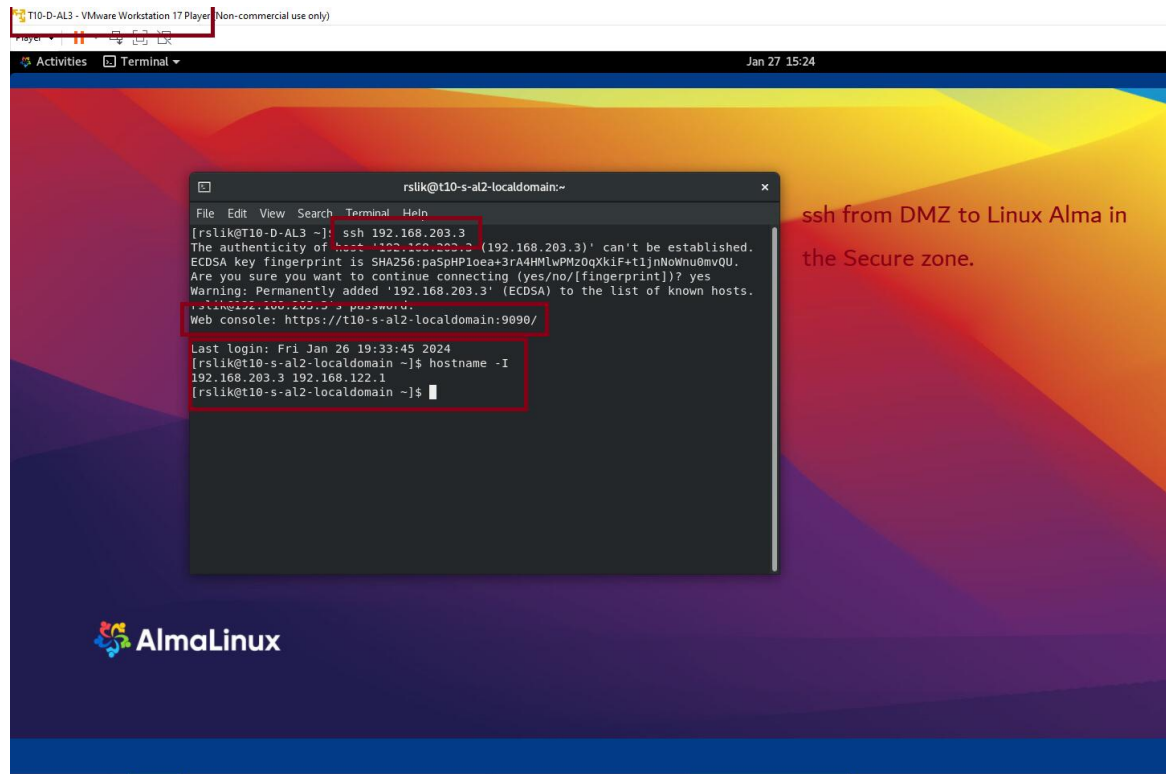
Testing connectivity with ssh between zones



```
T10-I-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities Terminal Jan 27 03:26
cgarcia@t10-s-al2-localdomain:~
File Edit View Search Terminal Help
[cgarcia@t10-I-AL2 ~]$ hostname -I
192.168.202.3 192.168.122.1
[cgarcia@t10-I-AL2 ~]$ /usr/bin/ssh 192.168.203.3
ssh: connect to host 192.168.203.3 port 22: No route to host
[cgarcia@t10-I-AL2 ~]$ ping 192.168.203.3
PING 192.168.203.3 (192.168.203.3) 56(84) bytes of data.
^C
--- 192.168.203.3 ping statistics ---
34 packets transmitted, 0 received, 100% packet loss, time 33805ms
[cgarcia@t10-I-AL2 ~]$ /usr/bin/ssh 192.168.203.3
cgarcia@192.168.203.3 ~$
Web console: https://t10-s-al2-localdomain:9090/
Last login: Sat Jan 27 02:18:07 2024
[cgarcia@t10-s-al2-localdomain ~]$ hostname -I
192.168.203.3 192.168.122.1
[cgarcia@t10-s-al2-localdomain ~]$
```

From inside to secure ssh.

Testing connectivity with ssh between zones

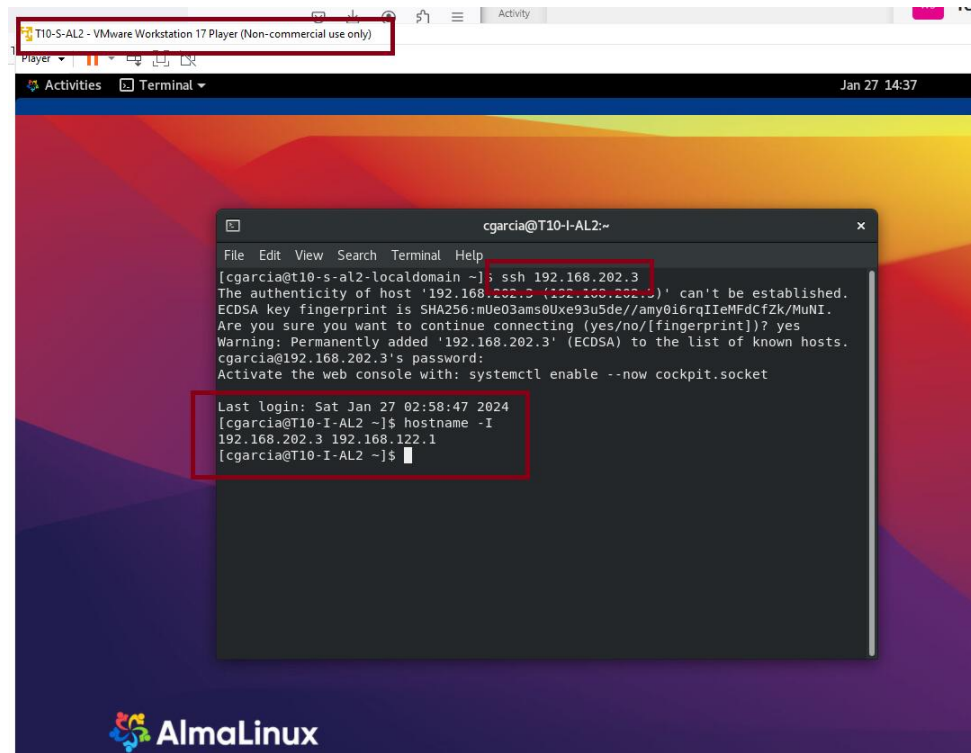


```
rslik@t10-s-al2-localdomain:~  
File Edit View Search Terminal Help  
[rslik@t10-D-AL3 ~]: ssh 192.168.203.3  
The authenticity of host '192.168.203.3' (192.168.203.3) can't be established.  
ECDSA key fingerprint is SHA256:poSPHP10es+3rA4HwPMz0gKkIF+tljnN0wmu0mvQU.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.203.3' (ECDSA) to the list of known hosts.  
Last login: Fri Jan 26 19:33:45 2024  
[rslik@t10-s-al2-localdomain ~]$ hostname -I  
192.168.203.3 192.168.122.1  
[rslik@t10-s-al2-localdomain ~]$
```

From DMZ to secure
ssh

ssh from DMZ to Linux Alma in
the Secure zone.

Testing connectivity with ssh between zones



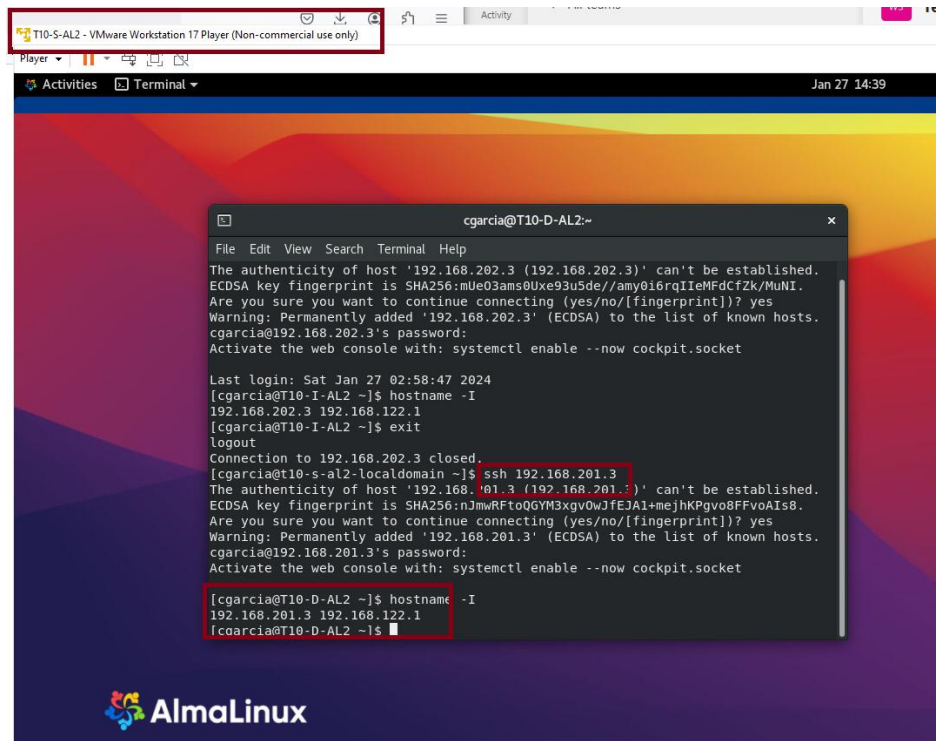
The screenshot shows a terminal window titled "cgarcia@T10-I-AL2:~" running an SSH command. The terminal output shows the SSH process starting, displaying the host's ECDSA key fingerprint, and asking for confirmation to continue connecting. The user responds "yes", and the connection is established. The terminal then shows the last login time and the output of the "hostname -I" command, which returns "192.168.202.3 192.168.122.1".

```
[cgarcia@t10-s-al2-localdomain ~]; ssh 192.168.202.3
The authenticity of host '192.168.202.3 (192.168.202.3)' can't be established.
ECDSA key fingerprint is SHA256:mUe03ams0Uxe93u5de//amy0i6rqIieMFdCfZk/MuNI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.202.3' (ECDSA) to the list of known hosts.
cgarcia@192.168.202.3's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Jan 27 02:58:47 2024
[cgarcia@T10-I-AL2 ~]$ hostname -I
192.168.202.3 192.168.122.1
[cgarcia@T10-I-AL2 ~]$
```

From secure to
inside ssh

Testing connectivity with ssh between zones



```
T10-S-AL2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities Terminal Jan 27 14:39

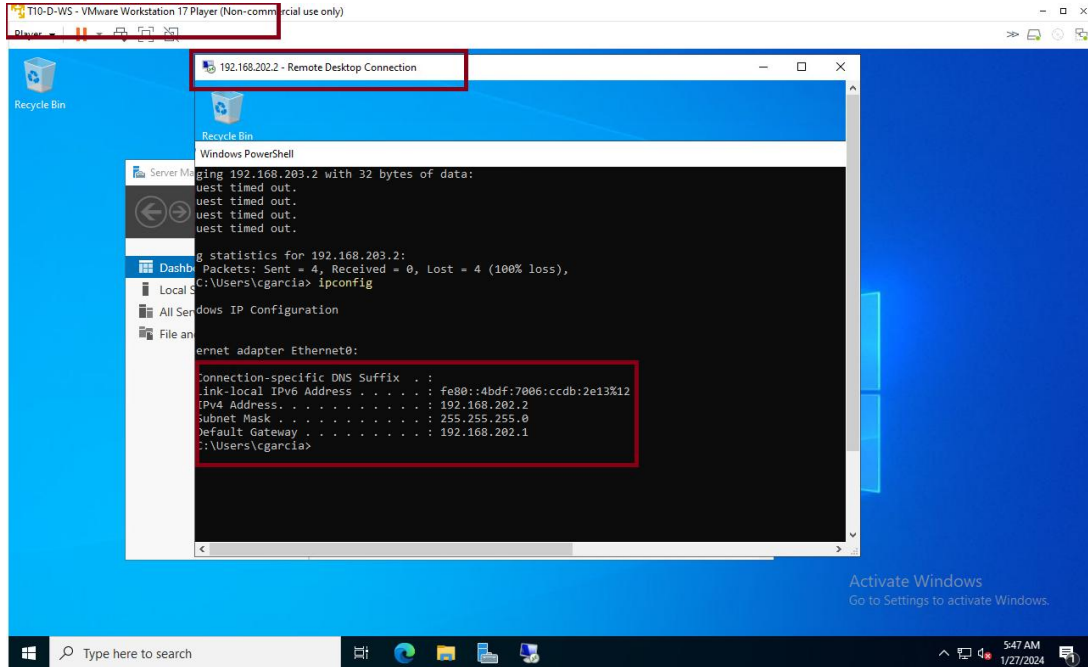
cgarcia@T10-D-AL2:~
File Edit View Search Terminal Help
The authenticity of host '192.168.202.3 (192.168.202.3)' can't be established.
ECDSA key fingerprint is SHA256:mUe03ams0Uxe93u5de/amy0i6rqIieMfdCfZk/MuNI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.202.3' (ECDSA) to the list of known hosts.
cgarcia@192.168.202.3's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Jan 27 02:58:47 2024
[cgarcia@T10-I-AL2 ~]$ hostname -I
192.168.202.3 192.168.122.1
[cgarcia@T10-I-AL2 ~]$ exit
logout
Connection to 192.168.202.3 closed.
[cgarcia@t10-s-al2-localdomain ~]$ ssh 192.168.201.3
The authenticity of host '192.168.201.3 (192.168.201.3)' can't be established.
ECDSA key fingerprint is SHA256:nJmwRFtoQGYM3xgv0wJfEJA1+mejhKpvo8FFvoAIs8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.201.3' (ECDSA) to the list of known hosts.
cgarcia@192.168.201.3's password:
Activate the web console with: systemctl enable --now cockpit.socket

[cgarcia@T10-D-AL2 ~]$ hostname -I
192.168.201.3 192.168.122.1
[cgarcia@T10-D-AL2 ~]$
```

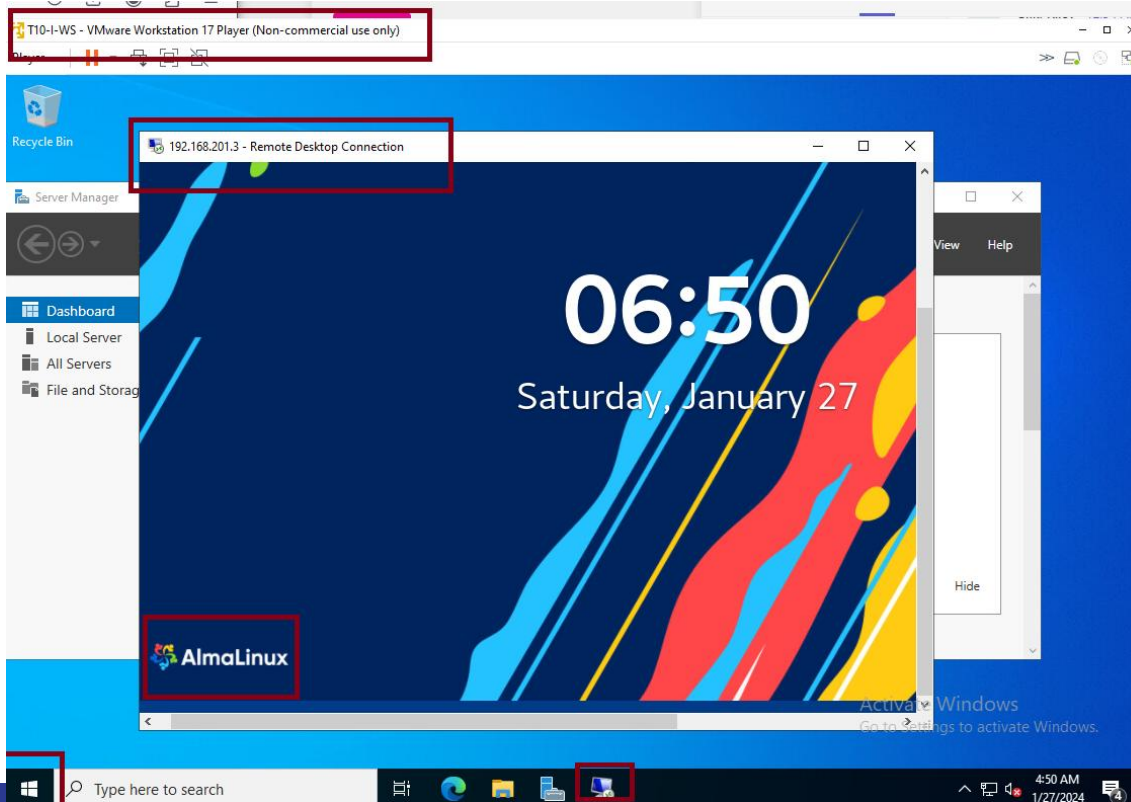
From secure
to DMZ ssh

Testing Remote Desktop connectivity between zones



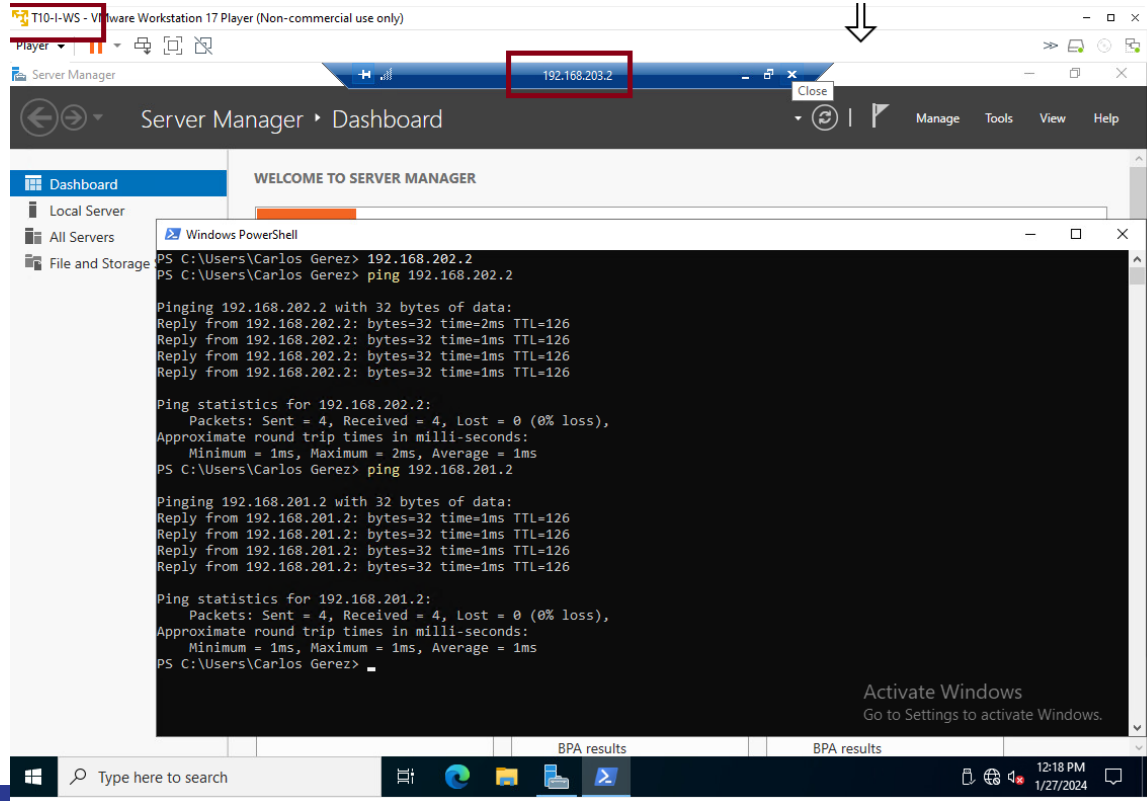
DMZ to inside zone.

Testing Remote Desktop connectivity between zones



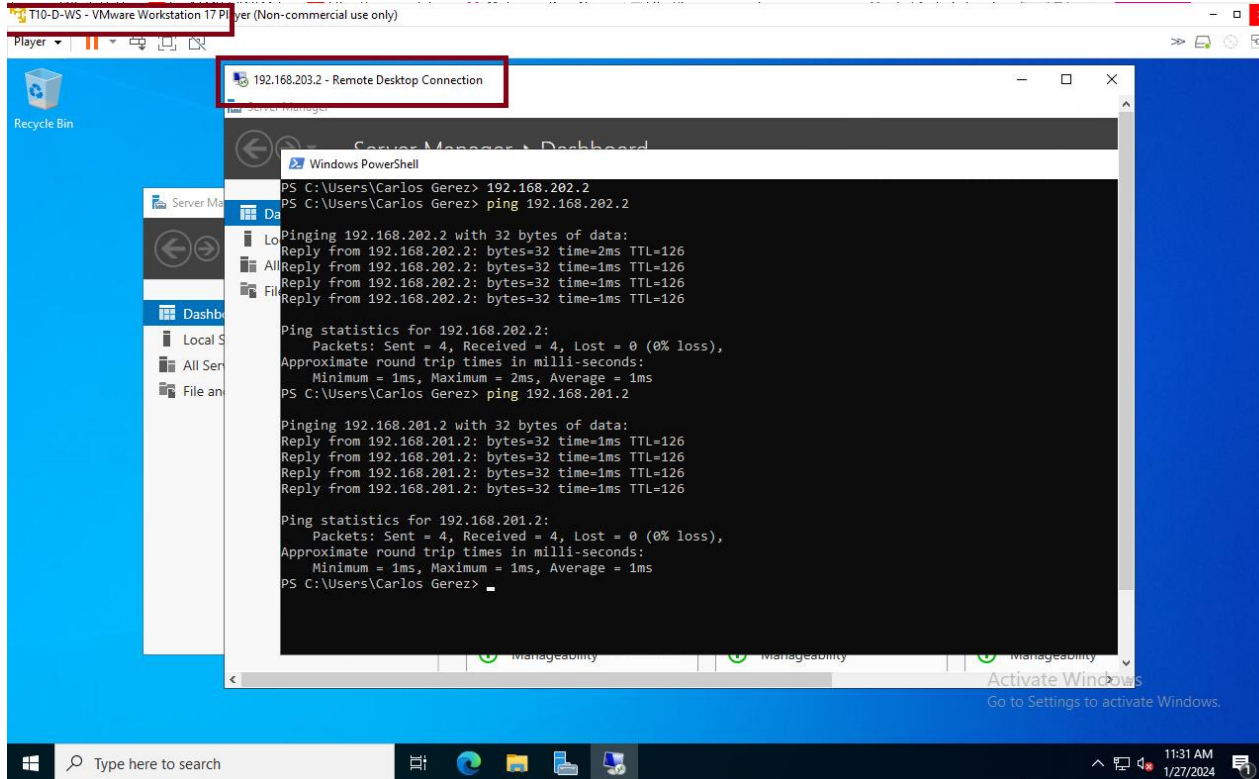
Inside to DMZ zone.

Testing Remote Desktop connectivity between zones



Inside to secure zone.

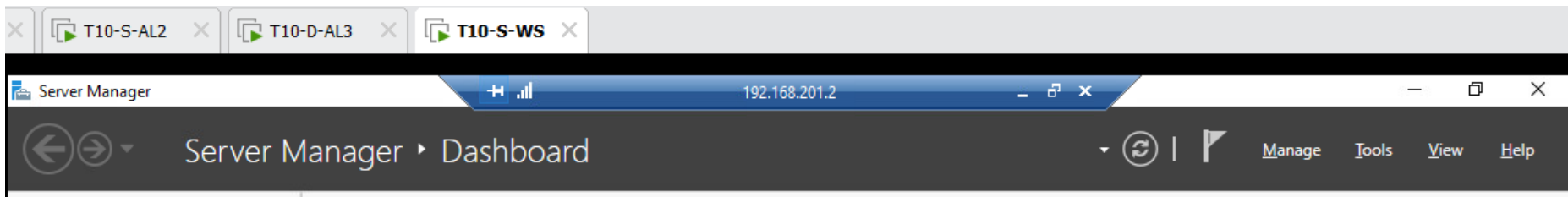
Testing Remote Desktop connectivity between zones



DMZ to secure zone.

Testing Remote Desktop connectivity between zones

Secure to DMZ.



Testing Remote Desktop connectivity between zones

Secure to Inside.

