

Firewalls

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

cit470

Task: Diagram

DNS addresses

Cloudflare
1.1.1.1

Google
8.8.8.8

port numbers

application
identifiers

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.byu.edu	157.201.22.75- 157.201.22.78	157.201.22.79

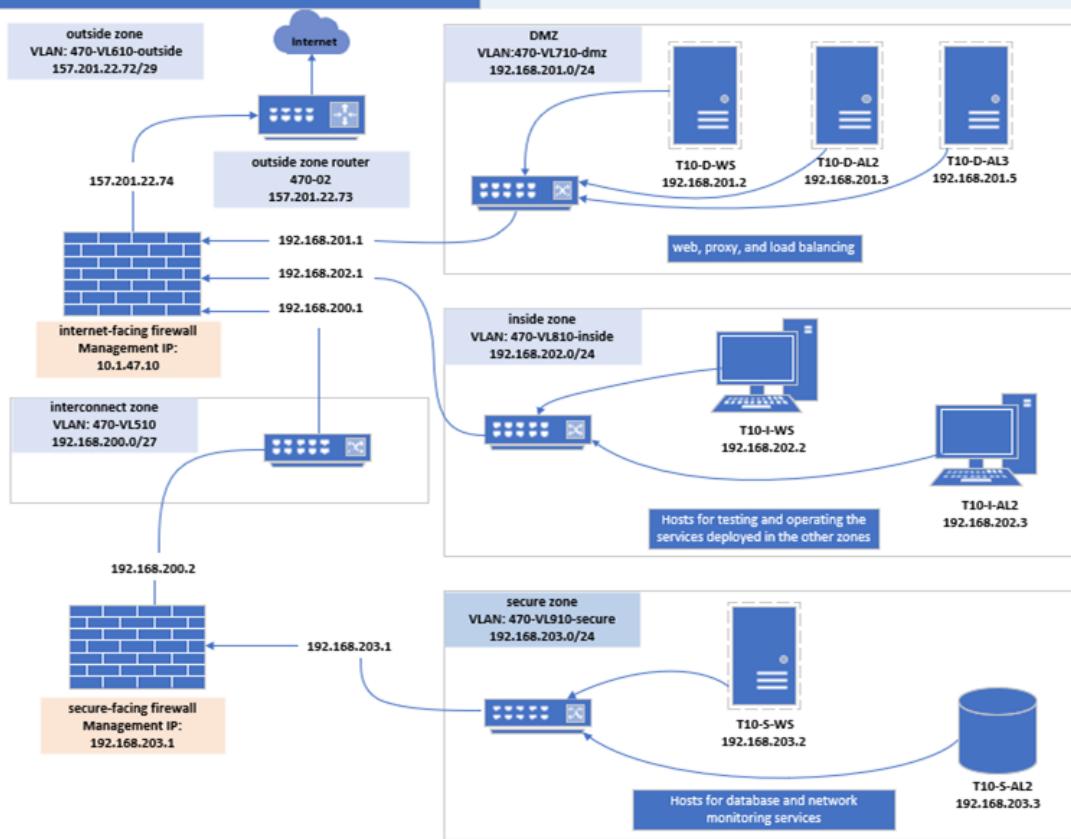


Diagram Outline for Team
10

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

The screenshot shows the Palo Alto PA-440 Device configuration interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE, with DEVICE selected. On the left, a sidebar menu lists various configuration categories such as Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management, Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusive, SSH Service Profile, Response Pages, Log Settings, Server Profiles, SNMP Trap, Syslog, Email, HTTP, and Netflow. The 'Administrators' item is expanded, showing two entries: 'admin' and 'T10', both listed as Superuser roles. A red arrow points from the text above to the 'Administrators' link in the sidebar. Another red arrow points to the 'Add' button located at the bottom right of the main content area, just above the 'Delete' and 'PDF/CSV' buttons.

NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)
admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>
T10	Superuser			<input type="checkbox"/>	<input type="checkbox"/>

Palo Alto PA-440 Configuration

Create a new administrative account.

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

Administrator

Name: cditto

Authentication Profile: None

Use only client certificate authentication (Web)

Password: [REDACTED]

Confirm Password: [REDACTED]

Password Requirements

- Minimum Password Length (Count) 8

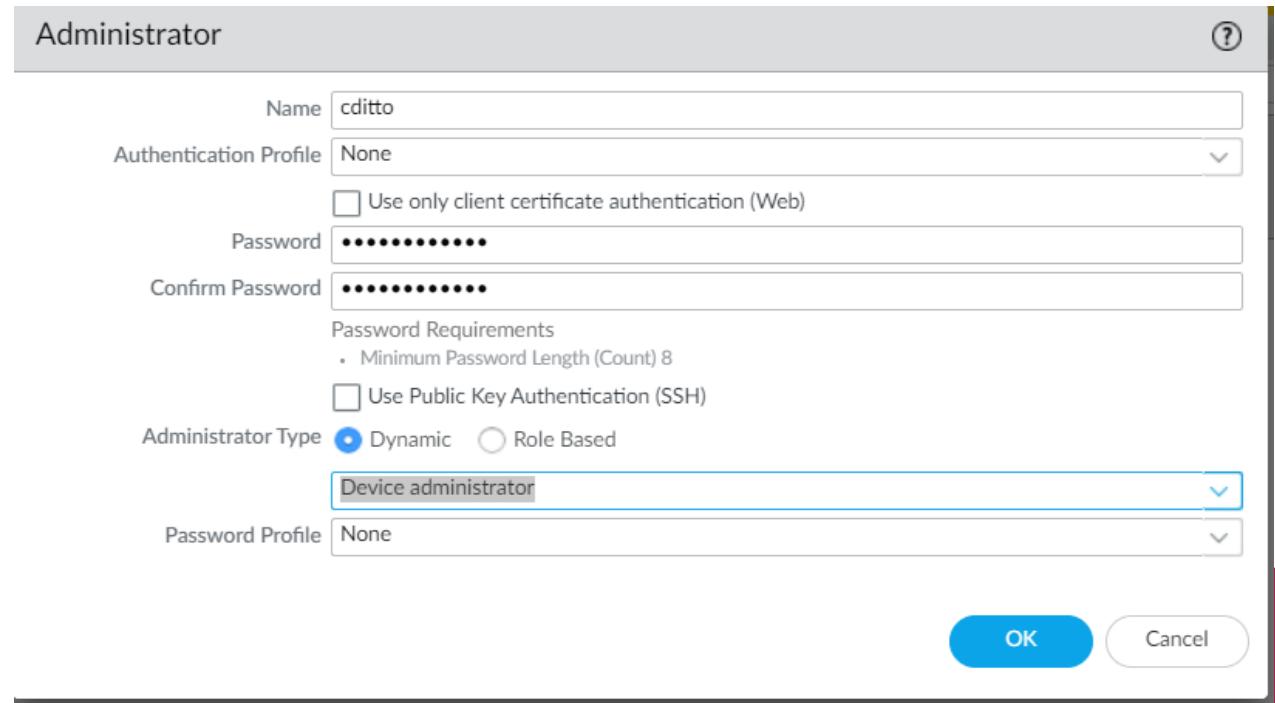
Use Public Key Authentication (SSH)

Administrator Type: Dynamic Role Based

Device administrator

Password Profile: None

OK Cancel



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 'DEVICE' tab selected in the top navigation bar. A red arrow points to the 'Commit' button in the top right corner of the main content area. Below it is a table listing user accounts:

Name	Role	Authenticati... Profile	Password Profile	Certificate Authenticati... (WEB)	Public Key Authenticati... (SSH)	Profile	Locked User
admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>		
T10	Superuser			<input type="checkbox"/>	<input type="checkbox"/>		
cditto	Device administrator			<input type="checkbox"/>	<input type="checkbox"/>		

A red box highlights the 'System Resources' section, which displays CPU usage and session counts. Another red arrow points to the 'Logout' link at the bottom left of the page.

Device Certificate Status: Valid

System Resources

- Management CPU: 4% (progress bar)
- Data Plane CPU: 0% (progress bar)
- Session Count: 0 / 199998

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

The screenshot shows the 'Commit' dialog box. A red arrow points to the 'Commit' button at the bottom right. The dialog includes fields for 'COMMIT SCOPE' (set to 'device-and-network') and 'LOCATION TYPE'.

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	

Preview Changes Change Summary Validate Commit 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



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 PA-440 interface with the 'NETWORK' tab selected. On the left, a sidebar lists various network components: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers (which is currently selected), IPSec Tunnels, and GRE Tunnels. The main pane displays a table for 'Virtual Routers'. A search bar is at the top. Below it is a table with columns: NAME, INTERFACES, CONFIGURATION, and RIP. One row is highlighted with a blue background, showing 'default' in the NAME column. A red arrow points from the sidebar's 'Virtual Routers' entry to this highlighted row.

NAME	INTERFACES	CONFIGURATION	RIP
default		ECMP status: Disabled	

The screenshot shows the PA-440 interface with the 'NETWORK' tab selected. On the left, a sidebar lists various network components: Interfaces (which is currently selected), Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, and GlobalProtect. The main pane displays a table for 'Interfaces'. At the top, there is a navigation bar with tabs: Ethernet (which is selected and highlighted in blue), VLAN, Loopback, Tunnel, and SD-WAN. Below the navigation bar is a search bar. The main table has columns: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, and IP ADDRESS. Three entries are listed: 'ethernet1/1' (Virtual Wire, Link State: up, IP Address: none), 'ethernet1/2' (Virtual Wire, Link State: up, IP Address: none), and 'ethernet1/3' (Virtual Wire, Link State: up, IP Address: none). A red arrow points from the 'Ethernet' tab in the navigation bar to the 'ethernet1/3' entry in the table.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Virtual Wire		up	none
ethernet1/2	Virtual Wire		up	none
ethernet1/3	Virtual Wire		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

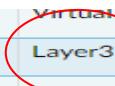
Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: None

Security Zone: None

OK  Cancel

Interface	Virtual Wire	Action
ethernet1/2		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'

ethernet1/2	Virtual VWire			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

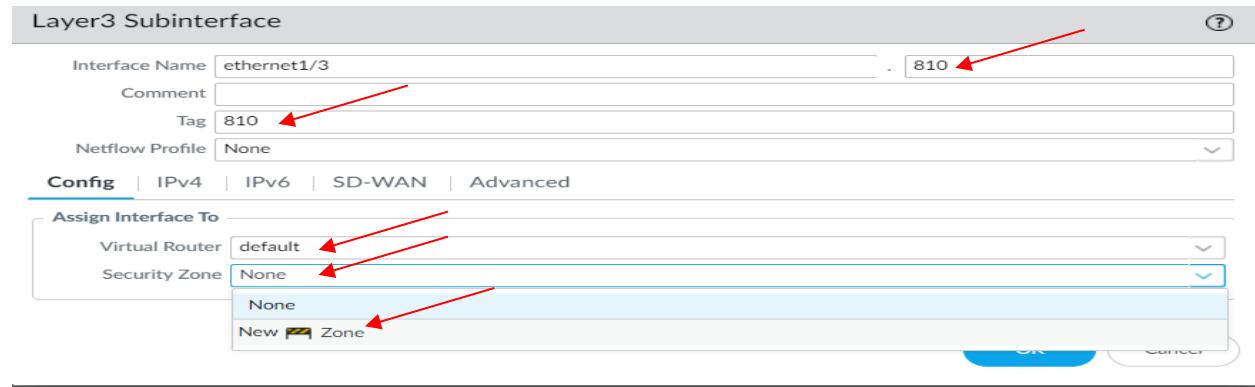
Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: None

New Zone



Layer3 Subinterface

Interface Name: ethernet1/3 . 810

Comment:

Tag: 810

Netflow Profile: None

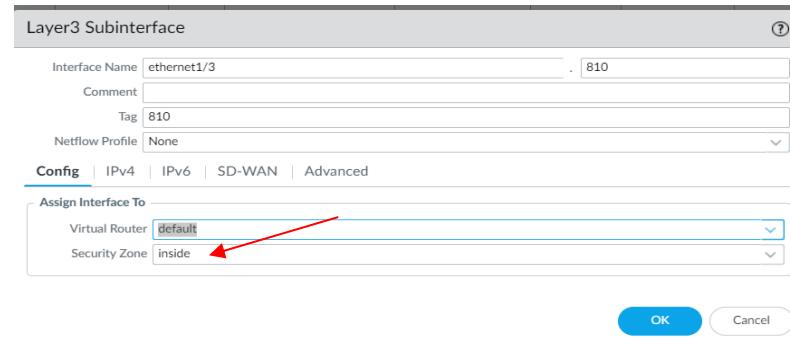
Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default

Security Zone: inside

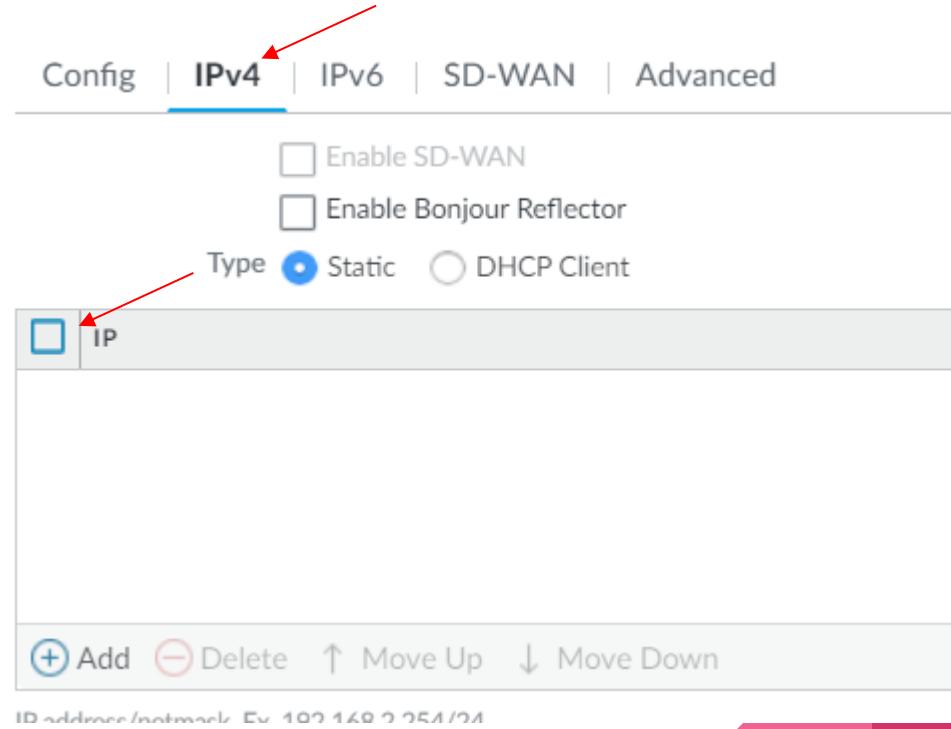
OK Cancel



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.

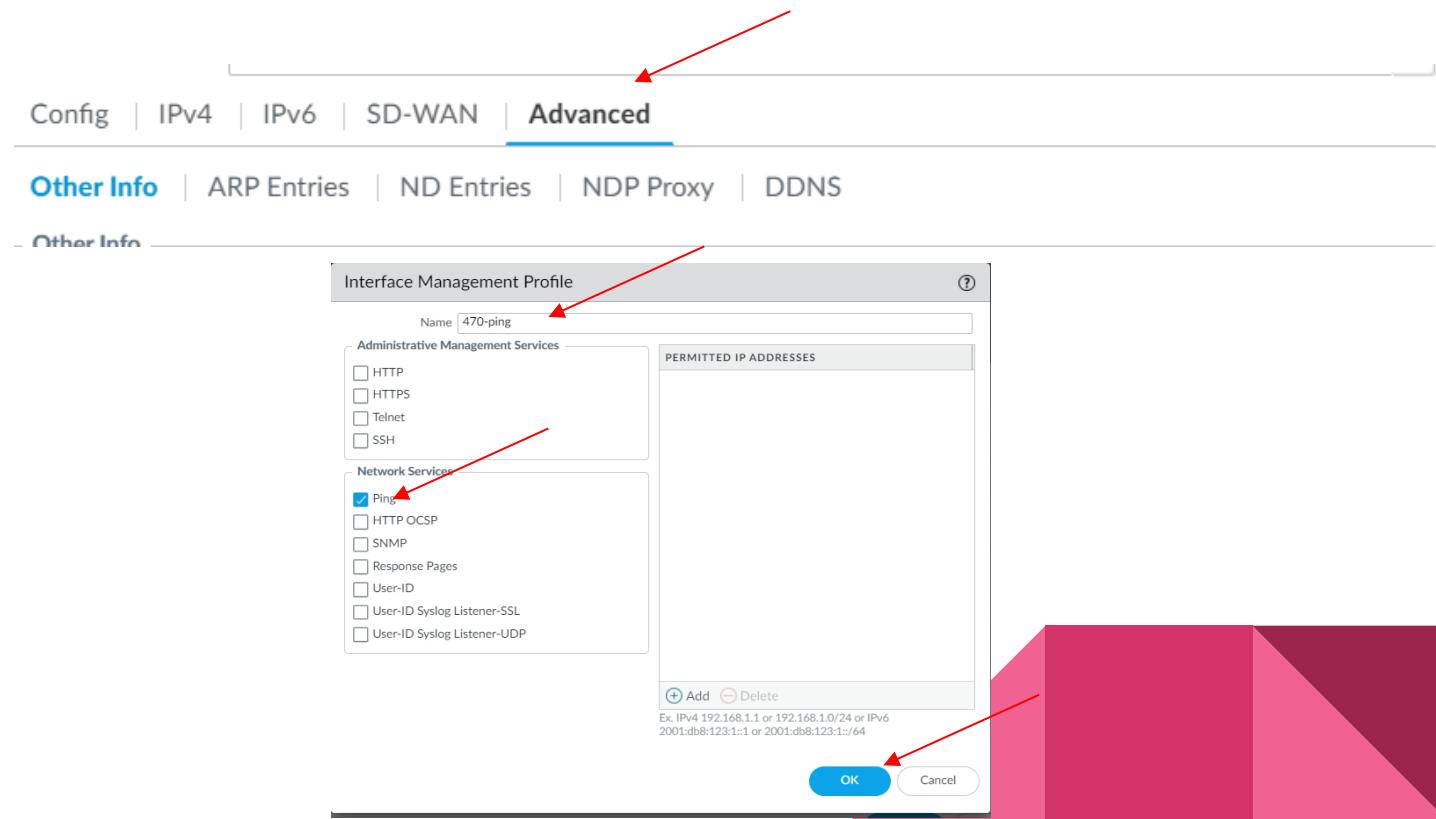


Palo Alto PA-440 Configuration

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 PA-440 configuration interface. On the left, a sidebar lists various networking components: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers (selected), IPSec Tunnels, GRE Tunnels, and DHCP. Below the sidebar, a table lists existing virtual routers, each associated with one or more interfaces. The 'default' router is selected. At the bottom, a modal dialog box titled 'Virtual Router - Static Route - IPv4' is open, showing fields for Name (T10-default), Destination (0.0.0.0), Interface (None), Next Hop IP Address (157.201.22.73/29), Admin Distance (10 - 240), Metric (10), and Route Table (Unicast). A red arrow points to the 'Name' field, and another red arrow points to the 'Next Hop IP Address' field. At the bottom right of the modal 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

	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

+ Add - Delete

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.

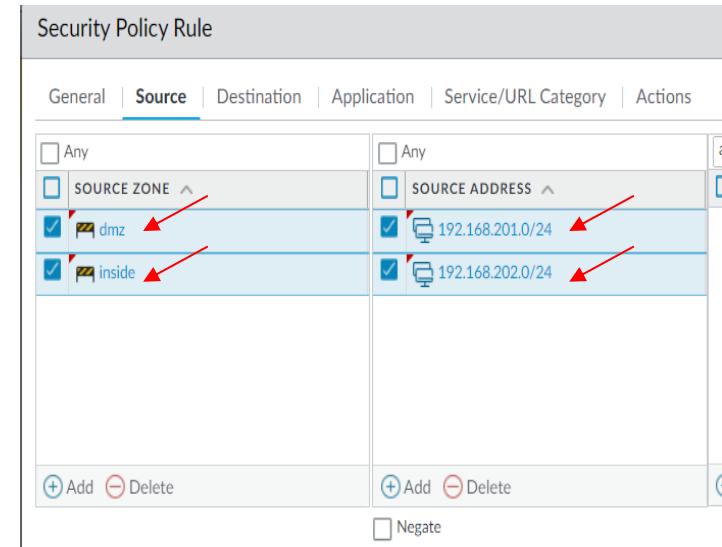
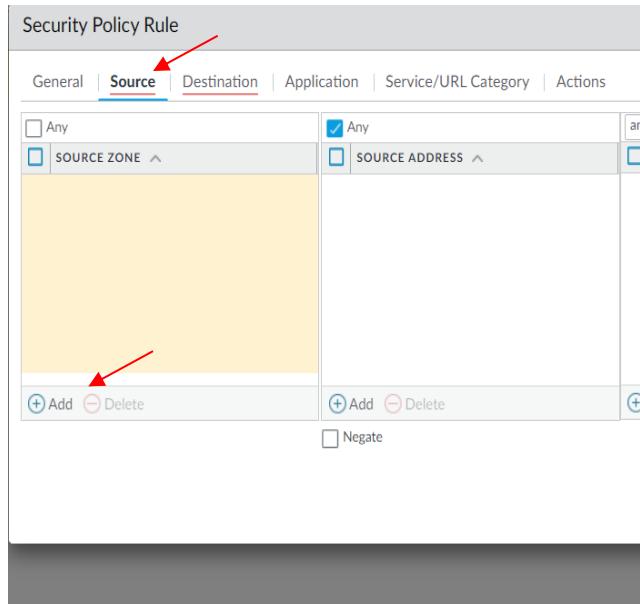
The screenshot shows the Palo Alto Networks management interface. At the top, there's a navigation bar with tabs: Dashboard, ACC, Monitor, Policies (which is highlighted in blue), Objects, Network, and Device. Below the navigation bar is a secondary header with a 'Security' icon and the word 'Security'. The main content area is titled 'Security Policy Rule' and contains several tabs: General (which is active, indicated by a blue underline), Source, Destination, Application, Service/URL Category, and Actions. Under the General tab, there are fields for Name (containing 'T10-outbound'), Rule Type (set to 'universal (default)'), Description, Tags, Group Rules By Tag (set to 'None'), Audit Comment, and an Audit Comment Archive section. Red arrows from the surrounding text blocks point to the 'Destination' tab in the header, the 'Name' field in the configuration window, and the 'Destination' tab in the detailed view.

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.

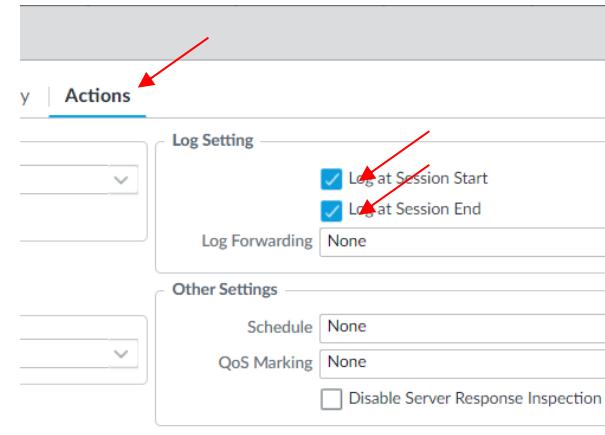
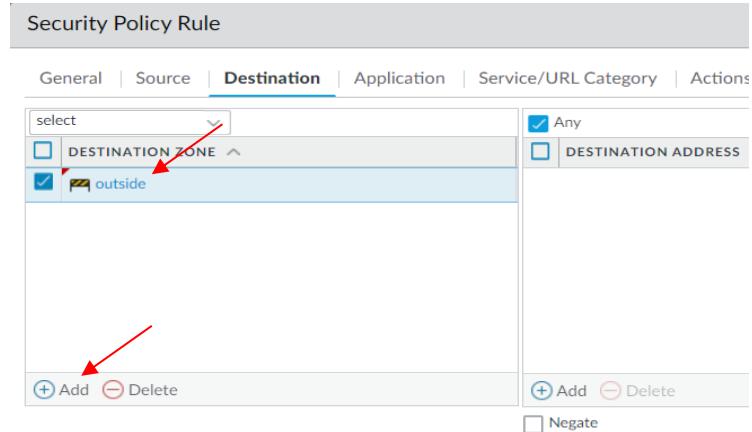
Under 'Source Addresses' click 'Add' and enter your teams DMZ subnet and the repeat with your inside zone subnet.



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.



Palo Alto PA-440 Configuration

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

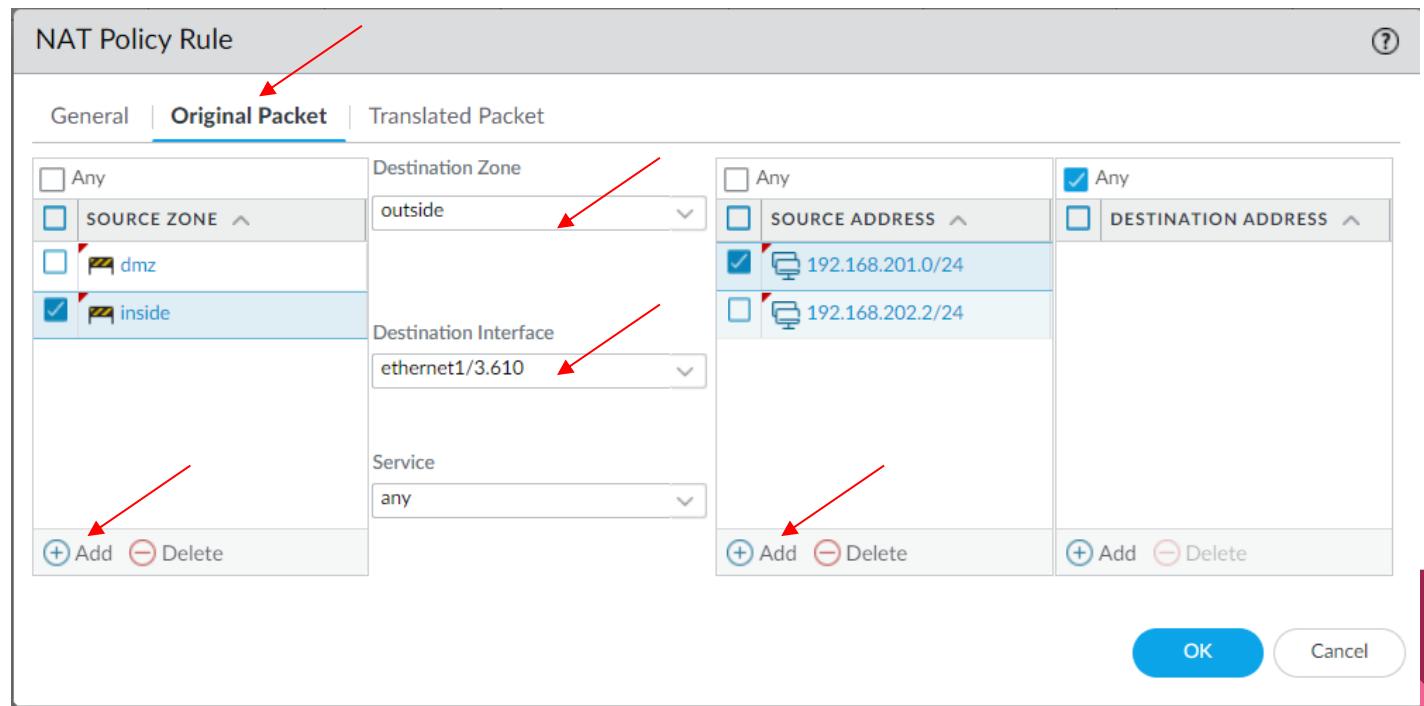
Under the 'General' tab name the new policy after your team name and the word dynamic.

The screenshot shows the Palo Alto PA-440 web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', and 'POLICIES'. On the left sidebar, under 'Security', the 'NAT' option is selected, indicated by a red arrow. The main content area displays a table with columns 'NAME', 'TAGS', and 'SOURCE ZONE'. Below the table, a modal dialog is open titled 'NAT Policy Rule'. The 'General' tab is active, shown by a blue underline. Inside the dialog, the 'Name' field contains the value 'T10-dynamic', which is also highlighted with a red arrow. Other fields visible include 'Description', 'Tags', 'Group Rules By Tag' (set to 'None'), 'NAT Type' (set to 'ipv4'), and an 'Audit Comment' field. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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.



Palo Alto PA-440 Configuration

Select the 'Translated Packet' tab.

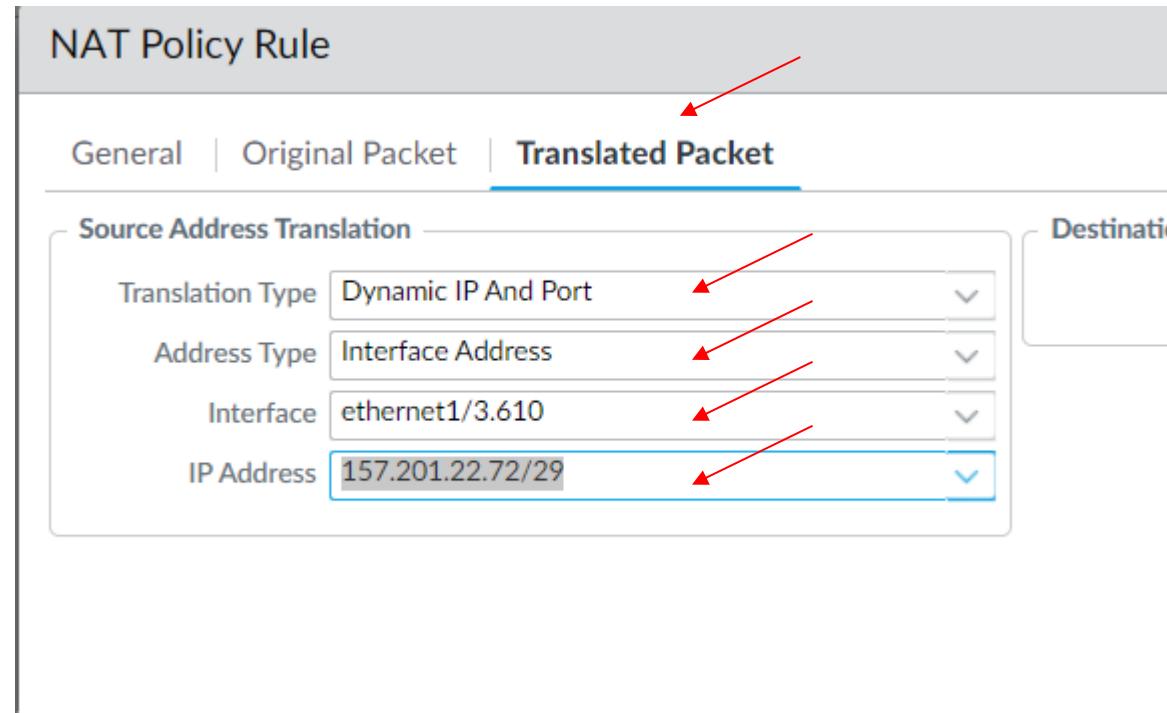
Change the 'Transition Type' to 'Dynamic IP and Port'

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



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) cditto

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

Commit Status

Operation Commit
Status Completed
Result Successful

Details Partial changes to commit: changes to configuration by administrators: cditto
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 a network management interface for a PA-440 device. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box), OBJECTS, NETWORK, and DEVICE. On the left, a sidebar lists various policy-based forwarding options like NAT, QoS, and Application Override. A central table displays existing security rules:

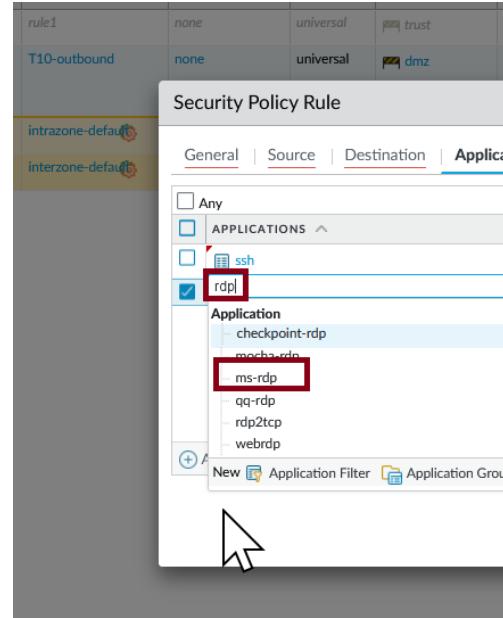
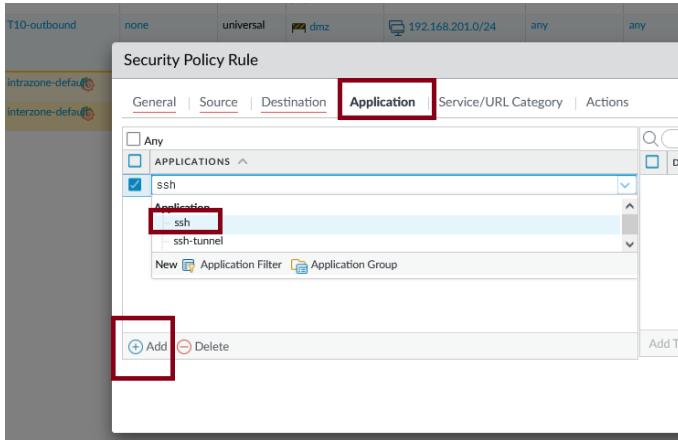
	Name	Tags	Type	Zone	Address	User	Device	Zone	Address	Device	Action	Profile	Options
1	rule1	none	universal	DMZ trust	any	any	any	DMZ untrust	any	any	Allow	none	...
2	T10-outbound	none	universal	DMZ	192.168.201.0/24	any	any	outside	any	any	Allow	none	...
3	intrazone-default	none	universal	DMZ	any	any	any	any	any	any	Allow	none	...
4	interzone-default	none	universal	DMZ	any	any	any	any	any	any	Deny	none	...

A modal window titled "Security Policy Rule" is open, also highlighted with a red box. It contains tabs for General, Source, Destination, Application, Service/URL Category, and Actions. The General tab shows the following fields:

- Name:
- Rule Type: universal (default)
- Description:
- Tags:
- Group Rules By Tag: None
- Audit Comment:

At the bottom of the modal are "OK" and "Cancel" buttons.

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.

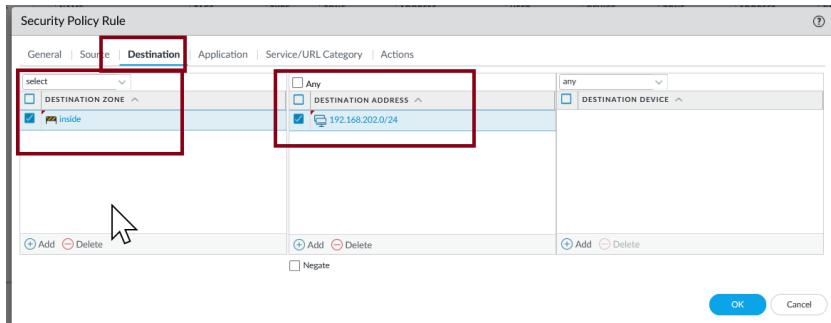
The screenshot shows the Fortinet GUI with the 'POLICIES' tab selected. A 'Security Policy Rule' dialog box is open, with the 'General' tab selected. The rule name is 'T10-dmz-to-inside-remote-access'. The 'Source' tab is highlighted with a red box. The 'Name' field contains 'T10-dmz-to-inside-remote-access'. The 'Rule Type' is 'universal (default)'. The 'Description' and 'Tags' fields are empty. The 'Group Rules By Tag' field shows 'None'. The 'Audit Comment' field is empty. At the bottom, there is an 'Audit Comment Archive' link.

The screenshot shows the 'Source' tab of the 'Security Policy Rule' dialog box. The 'Source' tab is highlighted with a red box. The configuration includes:

- Source Zone: 'dmz' (selected)
- Source Address: '192.168.201.0/24' (selected)
- Source User: 'any'
- Source Device: 'any'

Below the table, there are 'Add' and 'Delete' buttons for each row, and a 'Negate' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

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



	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	192.168.201.0/24	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	192.168.202.0/24	any	ms-rdp ssh	application-...	Allow	none
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
5	interzone-default	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.

The screenshot displays two side-by-side windows for configuring a security policy rule.

Left Window (General Tab):

- General:** The active tab.
- Name:** T10-inside-to-dmz-all
- Description:** universal (default)
- Tags:** None
- Group Rules By Tag:** None
- Audit Comment:** Audit Comment Archive

Right Window (Source Tab):

- Source Tab:** Active tab.
- Source Zone:** Any, SOURCE ZONE, inside (selected).
- Source Address:** Any, SOURCE ADDRESS, 192.168.202.0/24 (selected).
- Source User:** SOURCE USER (disabled).
- Buttons:** OK, Cancel, Add, Delete, Negate.

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

The image displays two side-by-side screenshots of a 'Security Policy Rule' configuration interface, likely from a network management tool like Cisco ASA or similar.

Left Screenshot (Destination Tab):

- The tab bar at the top includes General, Source, **Destination**, Application, Service/URL Category, and Actions.
- The Destination section shows a 'SELECT' dropdown with 'DESTINATION ZONE' and 'dmz' (selected) highlighted with a red box.
- Below it are sections for 'DESTINATION ADDRESS' (with 'Any' and '192.168.201.0/24' options) and 'DESTINATION DEVICE' (with 'any' selected).
- At the bottom are 'Add' and 'Delete' buttons, and an 'OK' button.

Right Screenshot (Application Tab):

- The tab bar at the top includes General, Source, Destination, **Application**, Service/URL Category, and Actions.
- The Application section shows a 'SELECT' dropdown with 'Any' (selected) highlighted with a red box.
- Below it is a 'DEPENDS ON' field with a search icon and a list of 0 items.
- At the bottom are 'Add' and 'Delete' buttons, and an 'OK' button.

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

PA-440

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Commit

Security

NAT QoS Policy Based Forwarding Decryption Tunnel Inspection Application Override Authentication DoS Protection SD-WAN

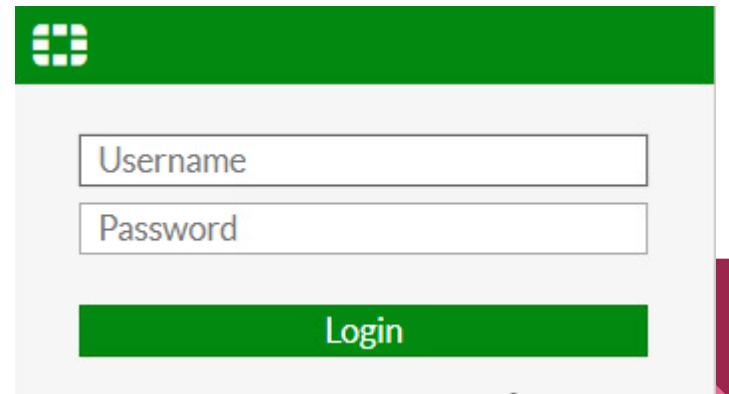
NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow	
T10-outbound	none	universal	dmz	192.168.201.0/24	any	any	outside	any	any	any	any	application-...	Allow
T10-dmz-to-inside-remote-access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



Go to System Administrator and make new Admin account for yourself

The screenshot shows the FortiGate Management Interface. On the left, there's a navigation sidebar with various tabs like Dashboard, Status, Security, Network, Users & Devices, WiFi, and several FortiView sections. A CPU usage chart is also visible. On the right, a modal window titled "New Administrator" is open. It has fields for "Username" (set to "Riley"), "Type" (set to "Local User", which is highlighted in green), "Password" (a masked password), "Confirm Password" (another masked password), "Comments" (a text input field with placeholder "Write a comment..."), and "Administrator Profile" (a dropdown menu). Below these fields are three toggle buttons: "Two-factor Authentication", "Restrict login to trusted hosts", and "Restrict admin to guest account provisioning only". The status bar at the bottom shows the date and time as 3:11 PM 1/24/2024.

FortiGate - 470FGOL

FortiGate 61F 470FGOL

Dashboard

Status

Security Fabric

470FGOL

CPU

1 minute

100%

75%

50%

25%

0%

Type

Username

Riley

Local User

Match a user on a remote server group

Match all users in a remote server group

Use public key infrastructure (PKI) group

Password

Confirm Password

Comments

Write a comment... 0/255

Administrator Profile

Two-factor Authentication

Restrict login to trusted hosts

Restrict admin to guest account provisioning only

3:11 PM 1/24/2024

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

The image shows two side-by-side screenshots of the FortiGate 61F web interface, both titled "FortiGate - 470FGOL" and "Not secure | https://192.168.203.1/ng/interface/edit/?vdom=OLTeam10". The left window shows the initial configuration of a new interface, while the right window shows the completed configuration.

Left Window (Initial Configuration):

- Address:**
 - Addressing mode: Manual (selected)
 - IP/Netmask: 192.168.200.2/24
 - Create address object matching subnet: Enabled (radio button)
 - Name: Interconnect address
 - Destination: 192.168.200.2/24
 - Secondary IP address: Disabled (radio button)
- Administrative Access:**
 - IPv4:
 - HTTPS
 - FMG-Access
 - FTP
 - HTTP:
 - SSH
 - RADIUS Accounting
 - PING
 - SNMP
 - Security Fabric Connection
- DHCP Server:** Enabled
- Network:**
 - Device detection: Enabled (radio button)
 - Security mode: Disabled (radio button)

Right Window (Completed Configuration):

- Address:**
 - Name: Interconnect
 - Alias:
 - Type: VLAN (selected)
 - Interface:
 - VLAN ID: 510
 - Virtual domain: OLTTeam10
 - Role: LAN (selected)
- Address Object:** Address (selected)
 - Addressing mode: Manual (selected)
 - IP/Netmask: 192.168.200.2/24
 - Create address object matching subnet: Enabled (radio button)
 - Name: Interconnect address
 - Destination: 192.168.200.2/24
 - Secondary IP address: Disabled (radio button)
- Administrative Access:**
 - HTTPS
 - HTTP
 - PING (selected)
 - SSH
 - RADIUS Accounting
 - SNMP
 - Security Fabric Connection

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

The screenshot shows two browser windows for the FortiGate 61F management interface. Both windows are connected to the same VDOM, OLTTeam10.

Left Window (Main View):

- URL: https://192.168.203.1/ng/routing/static?vdom=OLTeam10
- Header: FortiGate - 470FGOL
- Left sidebar:
 - Dashboard
 - Security Fabric
 - Network** (selected)
 - Interfaces
 - Packet Capture
 - SD-WAN Zones
 - SD-WAN Rules
 - Performance SLA
- Content area:
 - Static Routes (selected)
 - System
 - Policy & Objects
 - Security Profiles
 - VPN
 - User & Authentication
 - WiFi & Switch Controller
 - Log & Report

No results

Right Window (Create New Route):

- URL: https://192.168.203.1/ng/routing/static/edit?vdom=OLTeam10
- Header: FortiGate - 470FGOL
- Left sidebar:
 - Dashboard
 - Security Fabric
 - Network** (selected)
 - Interfaces
 - Packet Capture
 - SD-WAN Zones
 - SD-WAN Rules
 - Performance SLA
- Content area:
 - Static Routes (selected)
 - System
 - Policy & Objects
 - Security Profiles
 - VPN
 - User & Authentication
 - WiFi & Switch Controller
 - Log & Report
- Form:

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	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

New Static Route

Advanced Options

OK Cancel

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

The screenshot shows the FortiGate 61F 470FGOL web interface. The left sidebar navigation menu includes: Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy, Addresses (selected), 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 top bar shows the title 'FortiGate - 470FGOL', a warning 'Not secure | https://192.168.203.1/ng/firewall/address/edit?vdom=OLTeam10', and a user profile for 'Riley'. The main content area displays a 'New Address' configuration dialog with the following fields: Name (DMZ), Color (Change), Type (Subnet), IP/Netmask (192.168.201.0/24), Interface (any), Static route configuration (disabled), and Comments (Write a comment...). Below the dialog are 'OK' and 'Cancel' buttons. To the right of the dialog is a sidebar titled 'FortiGate 470FGOL' with sections for 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, and Video Tutorials.

FortiGate - 470FGOL

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

VDOM: OLTeam10

Riley

New Address

Name: DMZ

Type: Subnet

IP/Netmask: 192.168.201.0/24

Interface: any

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

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

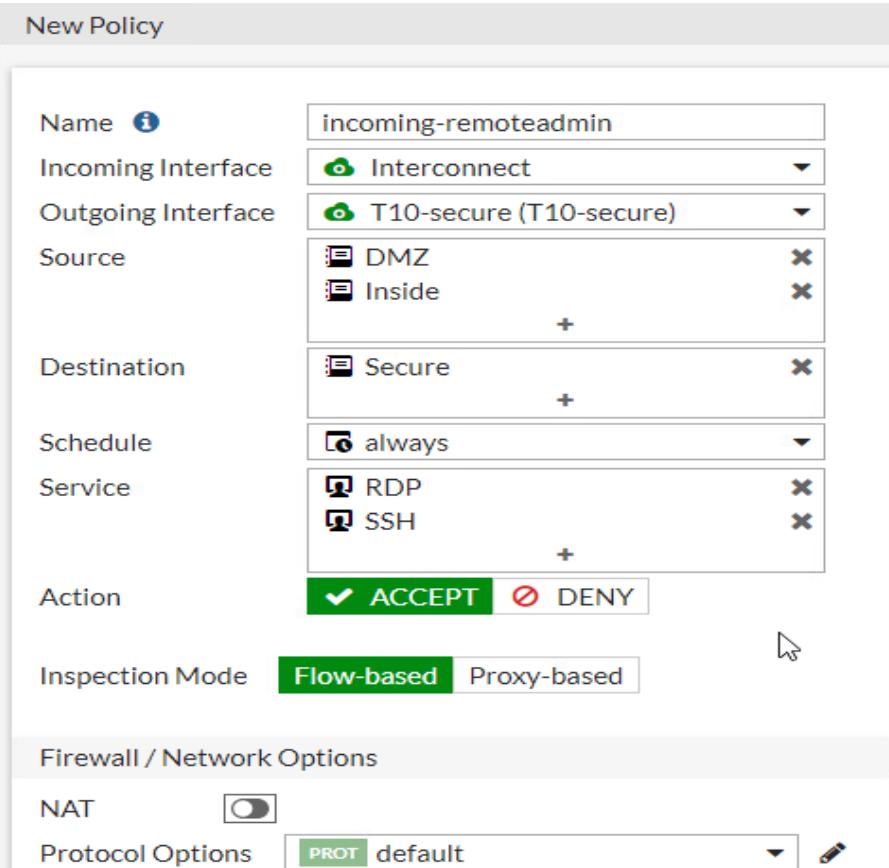
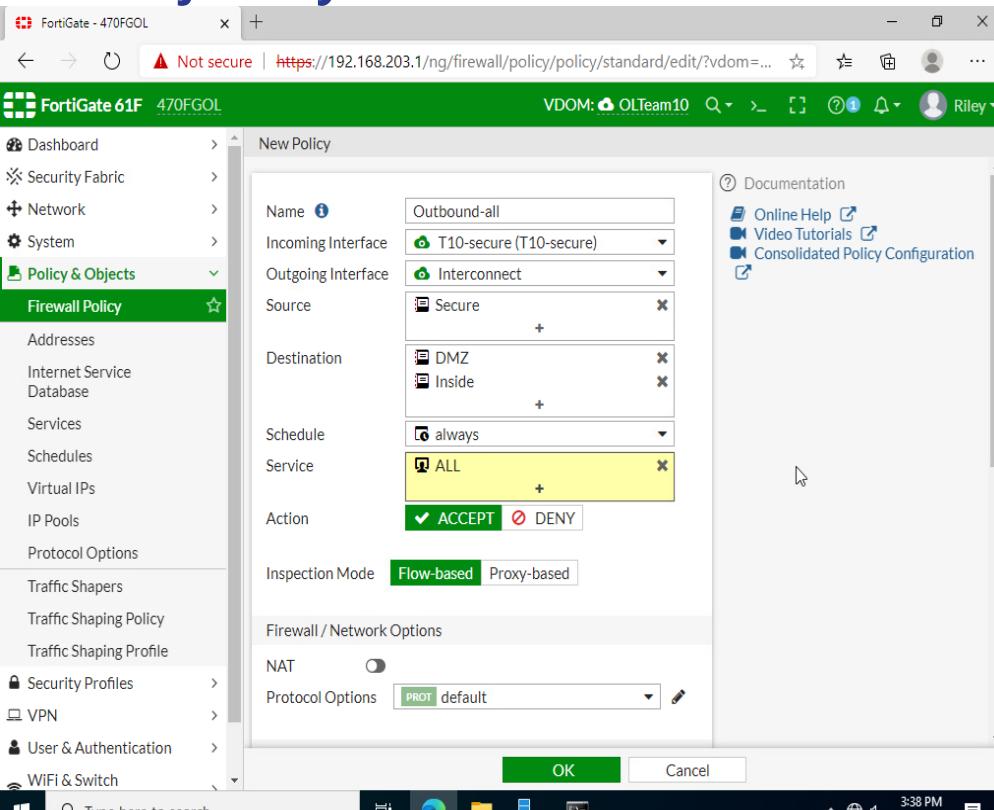
User & Authentication

WiFi & Switch

Type here to search

3:31 PM
1/24/2024

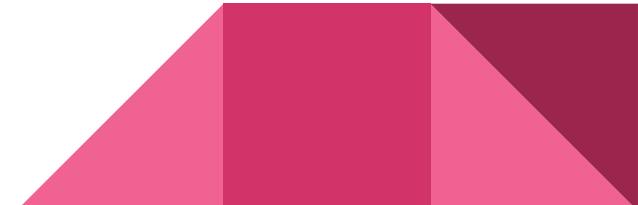
Inside of Policy & Objects select Firewall policies and make an outbound and rdp/ssh policies using the new object you made.



Review all the Policies and enable ALL for logging

						Create New	Edit	Delete	Policy Lookup	<input type="text"/> 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.

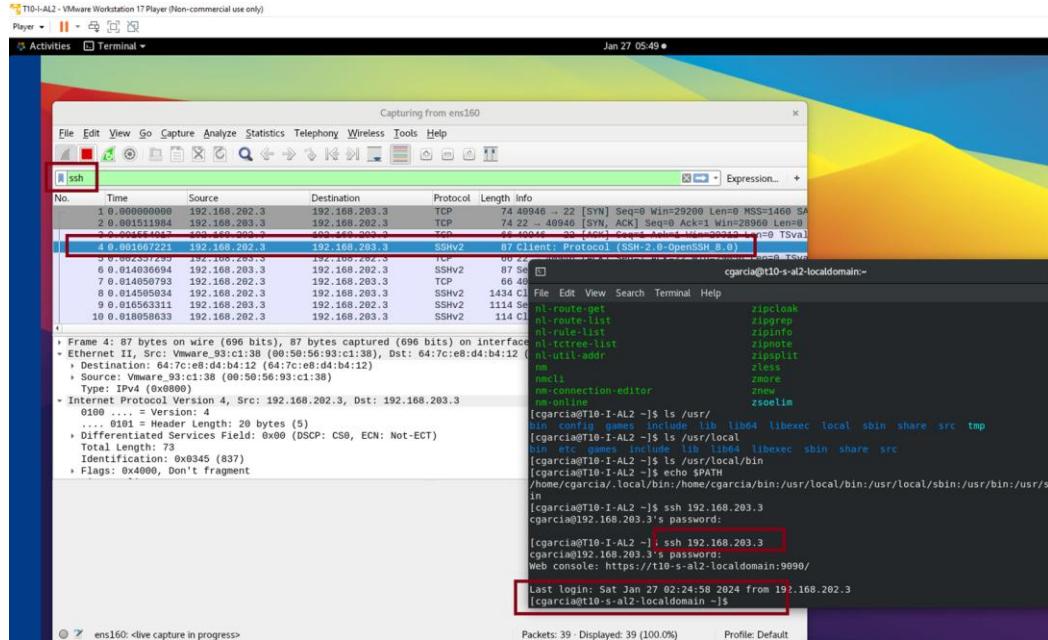
Was corrected from 192.168.200.0/24 to 192.168.203.0/24.

The screenshot shows the Palo Alto PA-440 Policy Manager interface. The main window displays a list of 8 security policies under the 'POLICIES' tab. The policies are listed in the following order:

NAME	TAGS	TYPE	Source	Destination	APPLICATION	SERVICE	ACTION	PROFILE
rule1	none	universal	trust any	any untrust	any	any	Allow	none
T10-outbound	none	universal	dmz 192.168.201.0/24	any outside	any	any	Allow	none
T10-dmz-to-inside-remote-access	none	universal	dmz 192.168.201.0/24	any inside	any	any	Allow	none
T10-inside-to-dmz-all	none	universal	inside 192.168.202.0/24	any dmz	any 192.168.201.0/24	any	Allow	none
T10-secure-to-dmz-inside	none	universal	interconnect 192.168.200.0/24	any dmz	any 192.168.201.0/24	any	Allow	none
T10-to-Secure-Remote-Admin	none	universal	dmz 192.168.201.0/24	any interconnect	any 192.168.200.0/24	any	Allow	none
intrazone-default	none	intrazone	any inside	(intrazone) any	any	any	Allow	none
interzone-default	none	interzone	any any	any any	any	any	Deny	none

The policies highlighted with red boxes are T10-secure-to-dmz-inside and T10-to-Secure-Remote-Admin. Both policies have their source and destination IP ranges highlighted. A cursor is visible at the bottom right corner of the highlighted area.

Linux SSH connections \$PATH problems.



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.

*ens160

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

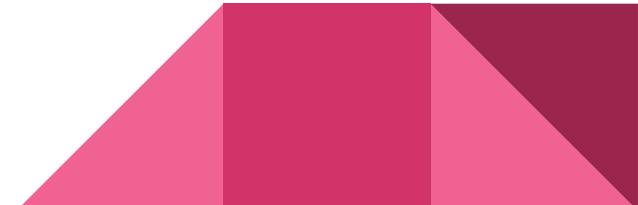
ssh Expression... + 192.168.202.3

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=1460
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

T10-D-WS - VMware Workstation 17 Player (Non-commercial use only)

Player

Recycle Bin

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

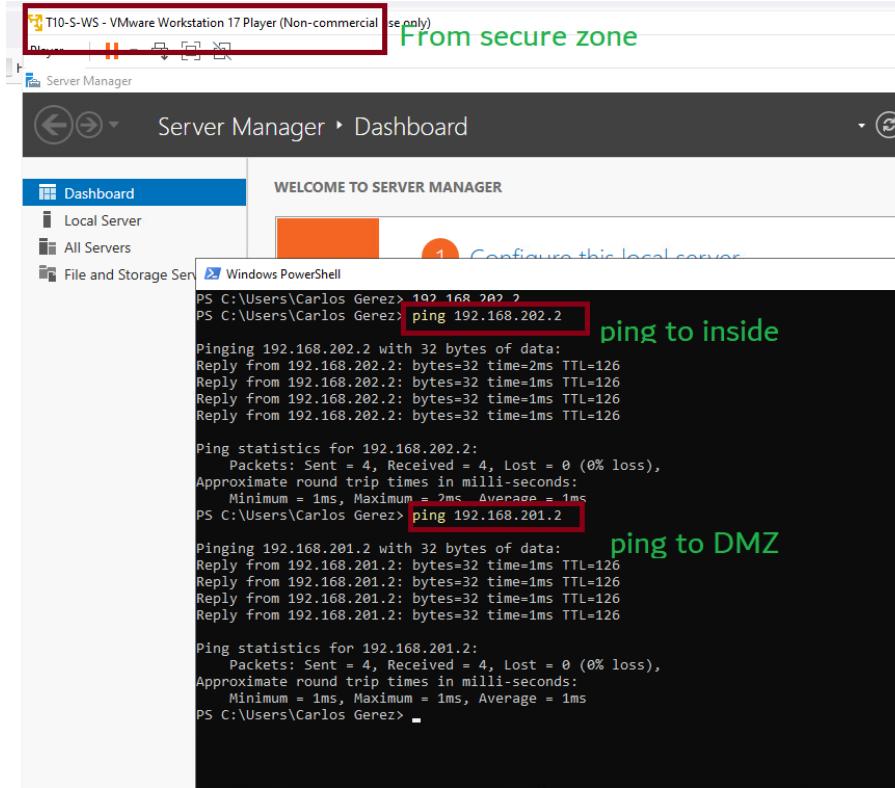
```
PS C:\Users\cgarcia> ping 192.168.201.2 Inside to DMZ
Pinging 192.168.201.2 with 32 bytes of data:
Reply from 192.168.201.2: bytes=32 time=1ms TTL=127

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 Inside to secure
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



From secure zone

```
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

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>
```

From secure zone.

Testing connectivity with ssh between zones

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

WS

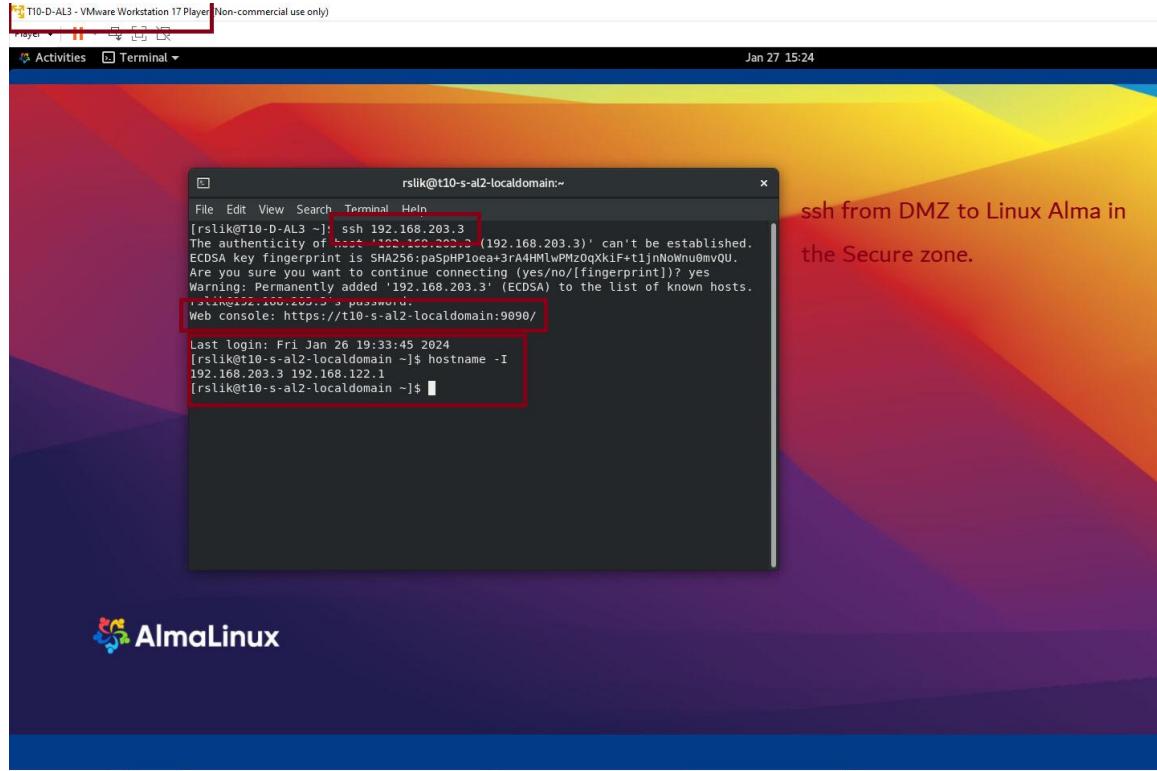
Activities Terminal Jan 27 03:26

```
[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's password:  
Web console: https://t10-s-al2-localhost:9090/  
  
Last login: Sat Jan 27 02:18:07 2024  
[cgarcia@t10-s-al2-localhost ~]$ hostname -I  
192.168.203.3 192.168.122.1  
[cgarcia@t10-s-al2-localhost ~]$
```

AlmaLinux

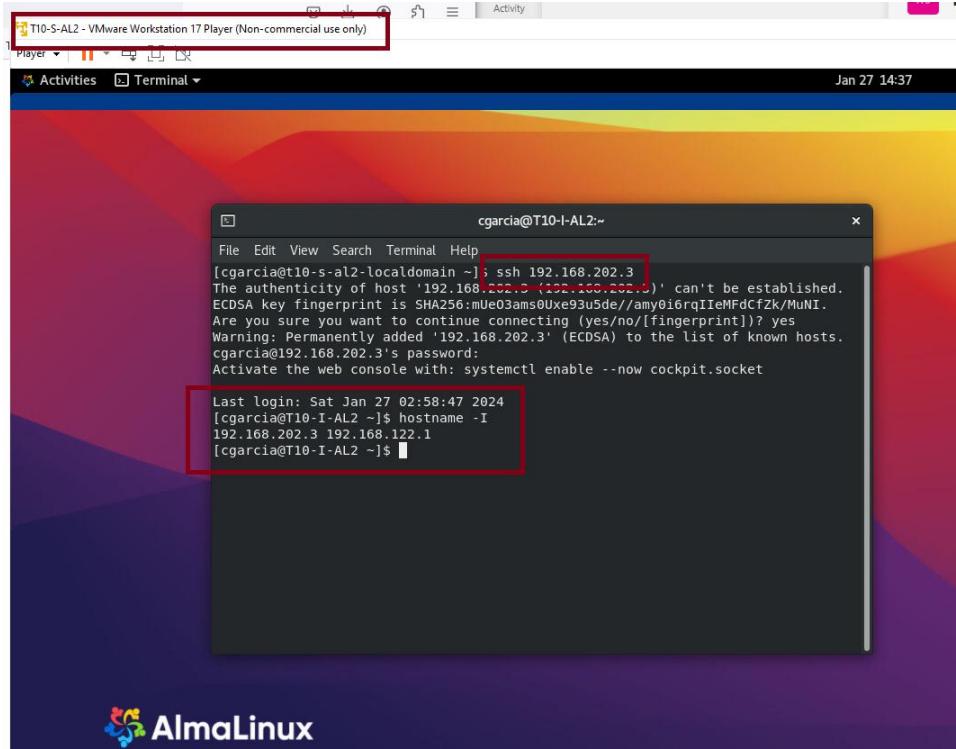
From inside to secure ssh.

Testing connectivity with ssh between zones



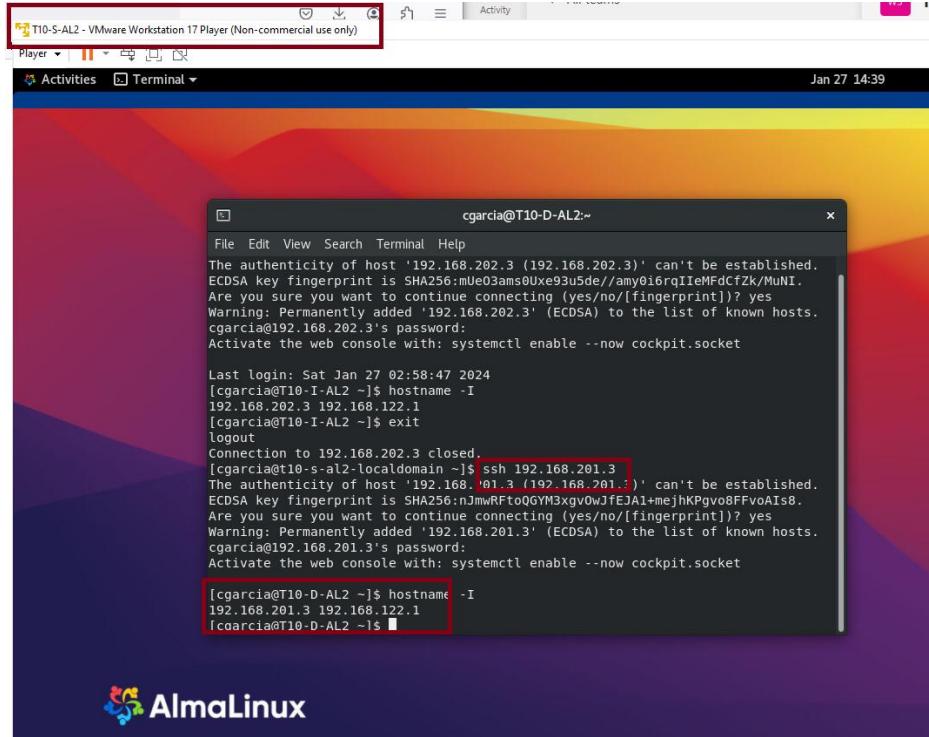
From DMZ to secure
ssh

Testing connectivity with ssh between zones



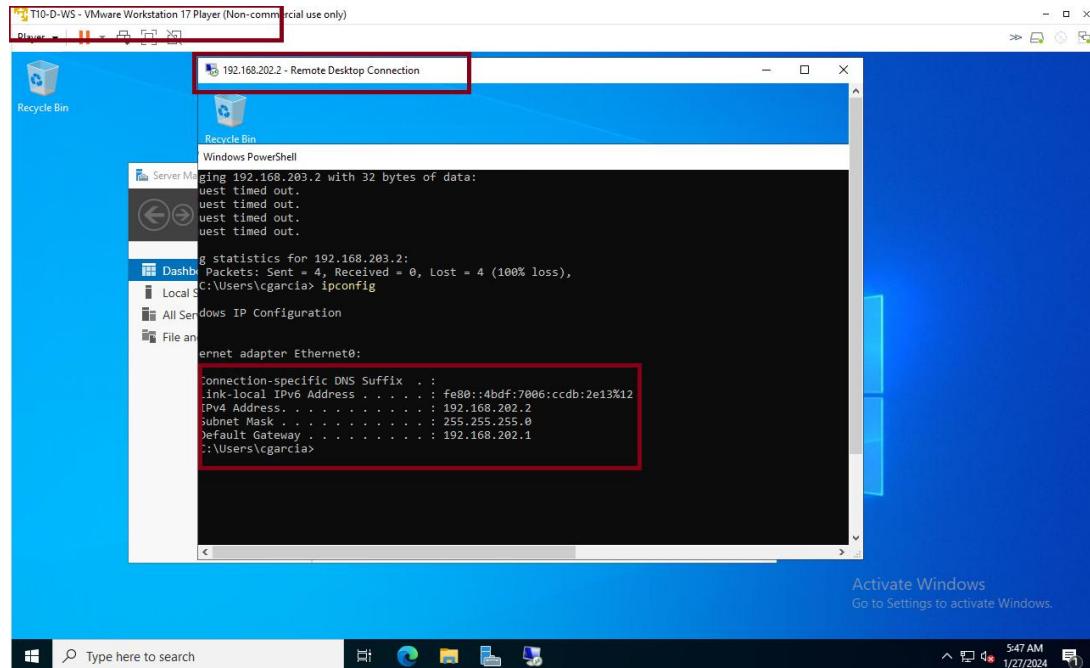
From secure to
inside ssh

Testing connectivity with ssh between zones



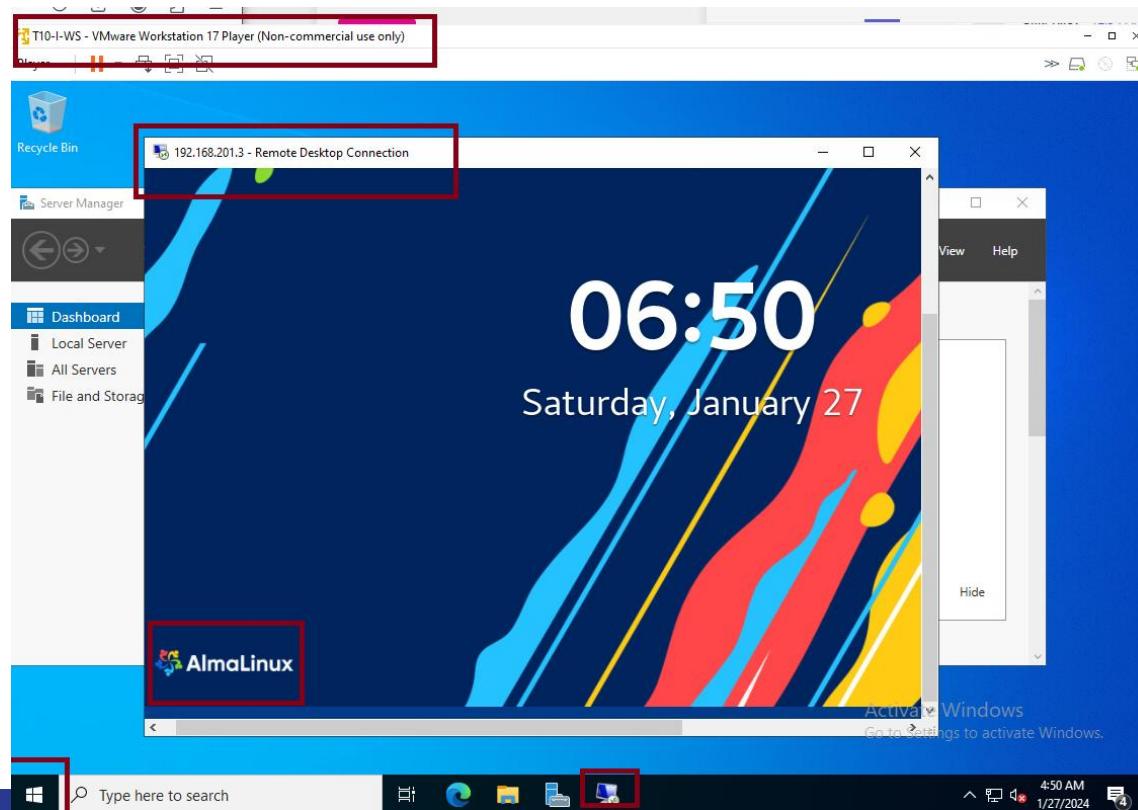
From secure
to DMZ ssh

Testing Remote Desktop connectivity between zones



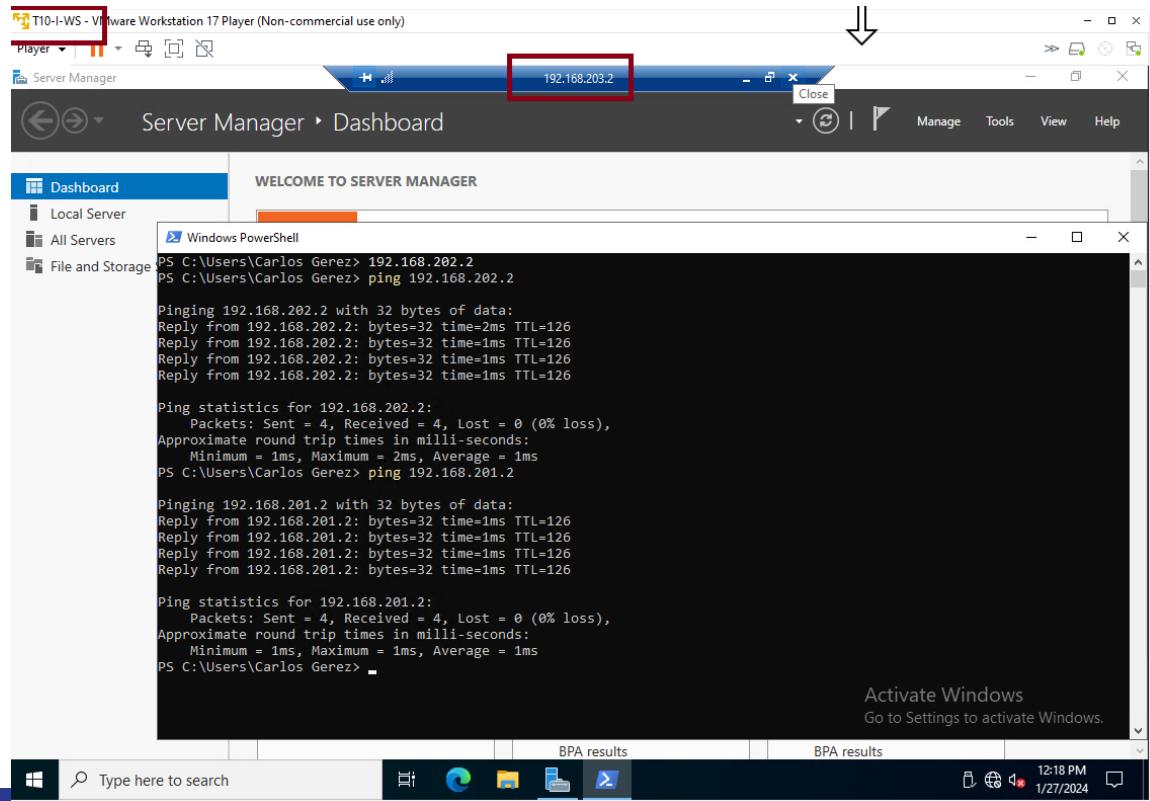
DMZ to inside zone.

Testing Remote Desktop connectivity between zones



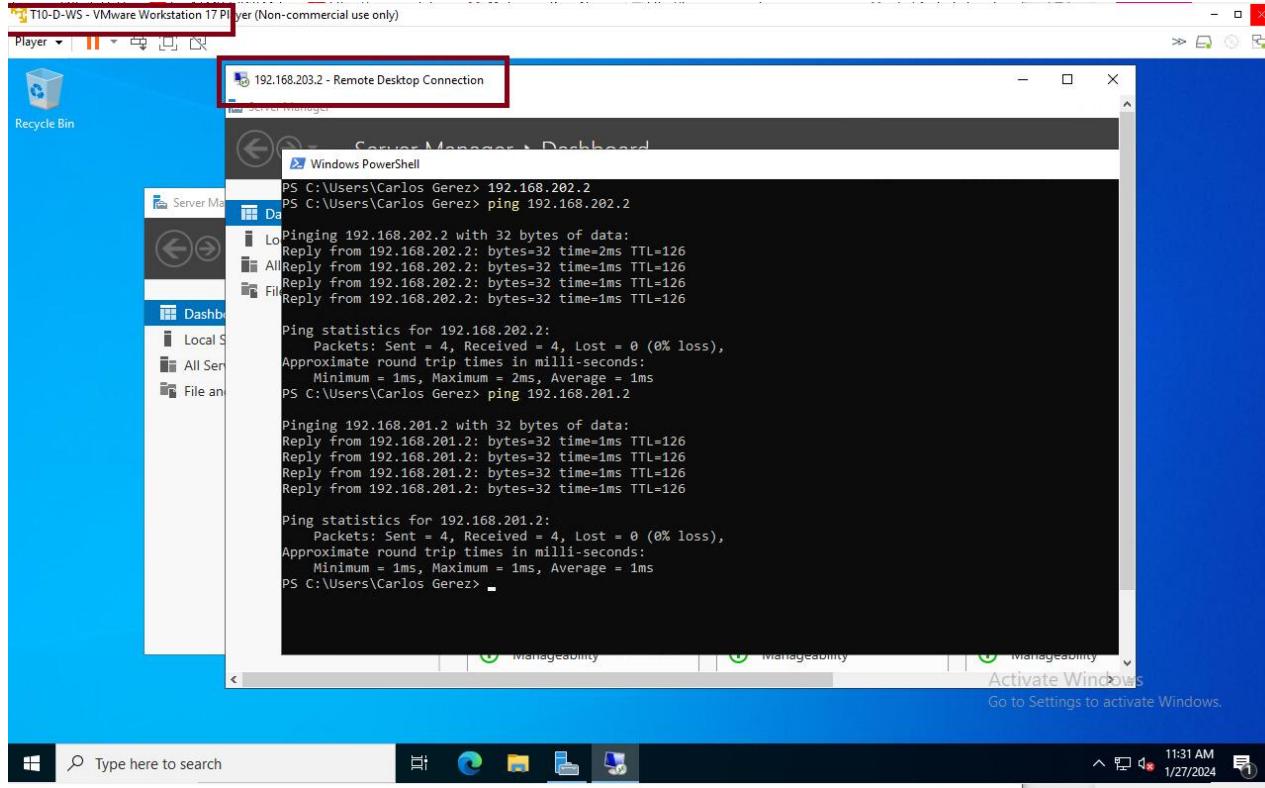
Inside to DMZ zone.

Testing Remote Desktop connectivity between zones



Inside to secure zone.

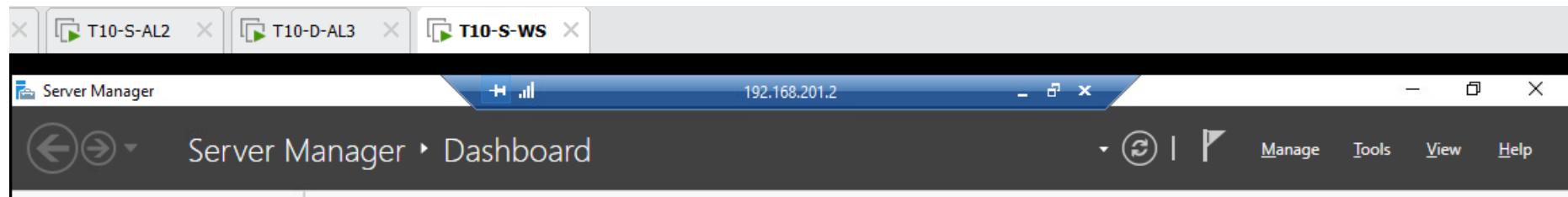
Testing Remote Desktop connectivity between zones



DMZ to secure zone.

Testing Remote Desktop connectivity between zones

Secure to DMZ.



Testing Remote Desktop connectivity between zones

Secure to Inside.

