

Overview

The Palo Alto Networks Next-Generation Firewall is capable of performing destination Network Address Translation (NAT) to allow multiple services to reside behind a single IP address if networking space is limited. This could allow the use of single IP address to host many internal services behind it, depending on the destination port specified in the incoming packet destined to the firewall interface. This feature is most commonly used on internet facing interfaces as a means to conserve public IP space provided by the ISP.

The Scenario

You've successfully deployed your Palo Alto Networks firewall into a layer 3 (L3) mode where the firewall is participating in source and destination NAT for inbound and outbound traffic. However, your IP space given by your ISP is either limited or is running out due to usage by other sources. Utilizing DNAT (Destination NAT) you can utilize a single IP address for multiple services. This lab will walk through how you would enable a web server (port 80, and 443), a DNS server (port 53), and a SMTP gateway (port 25) behind a single IP address on the internet.

IP Addresses for this Example

- Web Server:
 - Internal: 10.10.10.20
 - External: 70.50.30.10
- DNS Server:
 - Internal 10.10.10.30
 - External 70.50.30.10
- SMTP Gateway:
 - Internal 10.10.10.40



Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 2

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- External 70.50.30.10

Getting Started

Once you have access to your firewall, login with administrative rights to make changes to the candidate configuration.

Basic Setup

1. Login to your Palo Alto Networks firewall device

The default credentials are:

username: **admin**

password: **admin**



2. (Optional) Navigate to the "Objects" to create address objects for your policies
 - a. Select "Addresses" on the left-hand side navigation.
 - b. Select "Add" at the bottom to create a new Address object.
 - c. Enter the information for Name and IP address, hit "OK" when you are finished.
 - d. Create a single address object for the IP addresses to be used for all services.

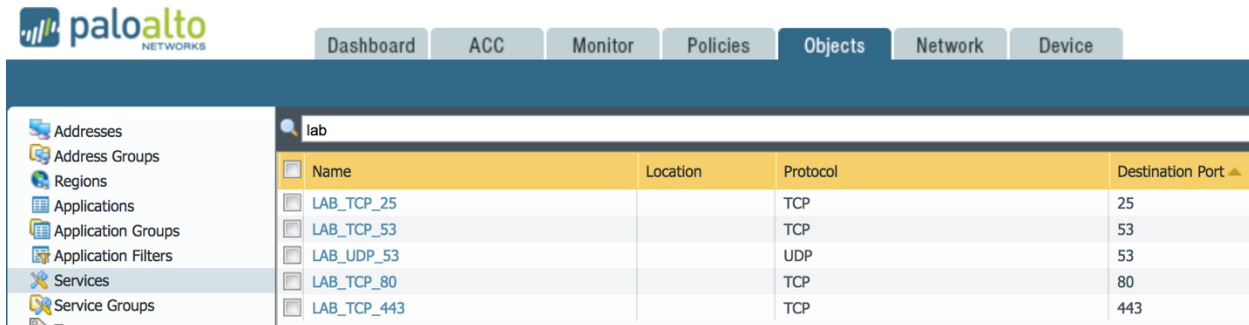


3. Create Service Objects for each service you plan to host behind the IP single IP address

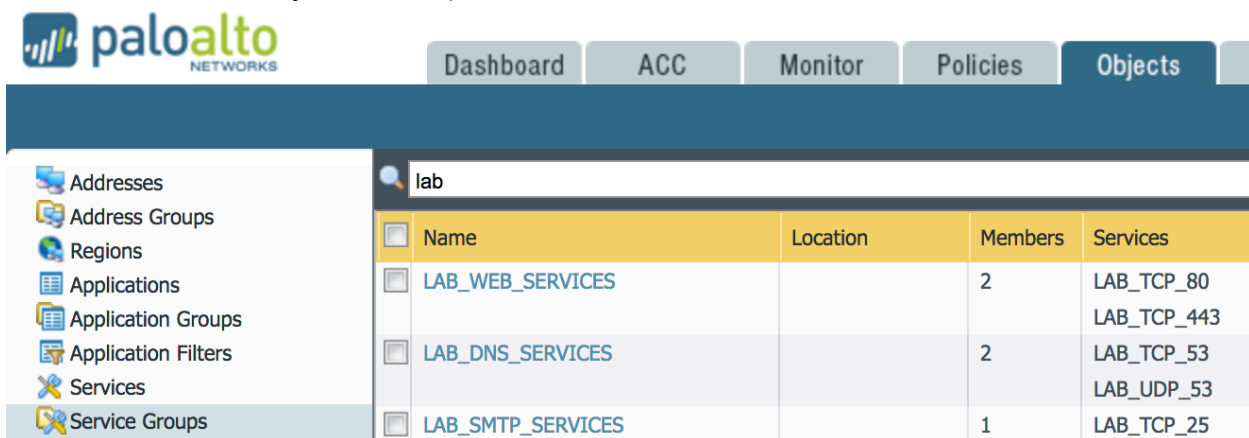
Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 3

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- a. From the top most “Objects” tab, select “Services” on the left-hand side
- b. Create service objects for search of the services that will be used based on the ports that the applications are listening on. In this case we will use:
 - i. TCP 80 and TCP 443 for Web traffic
 - ii. TCP / UDP 53 for DNS traffic
 - iii. TCP 25 for SMTP traffic



- c. Create service groups for each type of traffic so we can reduce multiple objects for each type of traffic to a single object within the firewall
 - i. Note: when selecting services for a NAT rule, each rule can only accept one firewall object (in this case you will use the Service Groups that were just created)



NAT Policies

1. Creation of Destination NAT policies for our 3 services we wish to use the 70.50.30.10 IP for
 - a. Switch to “Policies” at the top to enter the policy section of the firewall, from here switch to the NAT section to enter the NAT policy creation.
 - b. Clicking “add” at the bottom will create a new policy, in this example we will have 3 Destination NAT (DNAT) policies we will be creating.
2. The three DNAT rules will use the following logic:
 - a. Rule 1: LAB_WEB_DNAT
 - i. Original Packet
 1. Source Zone: Untrust (From internet)

Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 4

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

2. Destination Zone: Untrust (interface IP is within the Untrust zone)
 3. Destination IP Address: 70.50.30.10 (Public IP address)
 4. Service: LAB_WEB_SERVICES (the service object group created above)
 - ii. Translated Packet
 1. Leave "Source Address Translation" as "None" since we are doing Destination NAT
 2. Check the box for "Destination Address Translation"
 3. Fill the "Translated Address" field with the Address Object we created for the web servers IP within the DMZ, LAB_10.10.10.20_Webserver_DMZ.
 - b. Rule 2: LAB_DNS_DNAT
 - i. Original Packet
 1. Source Zone: Untrust (From internet)
 2. Destination Zone: Untrust (interface IP is within the Untrust zone)
 3. Destination IP Address: 70.50.30.10 (Public IP address)
 4. Service: LAB_DNS_SERVICES (the service object group created above)
 - ii. Translated Packet
 1. Leave "Source Address Translation" as "None" since we are doing Destination NAT
 2. Check the box for "Destination Address Translation"
 3. Fill the "Translated Address" field with the Address Object we created for the web servers IP within the DMZ, LAB_10.10.10.30_DNS_DMZ.
 - c. Rule 3: LAB_SMTP_DNAT
 - i. Original Packet
 1. Source Zone: Untrust (From internet)
 2. Destination Zone: Untrust (interface IP is within the Untrust zone)
 3. Destination IP Address: 70.50.30.10 (Public IP address)
 4. Service: LAB_SMTP_SERVICES (the service object group created above)
 - ii. Translated Packet
 1. Leave "Source Address Translation" as "None" since we are doing Destination NAT
 2. Check the box for "Destination Address Translation"
 3. Fill the "Translated Address" field with the Address Object we created for the web servers IP within the DMZ, LAB_10.10.10.40_SMTP_DMZ.
3. Screenshot below illustrates the created rules from the above logic

Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 5

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

paloalto

networks

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Security

NAT

QoS

Policy Based Forwarding

Decryption

Application Override

Captive Portal

DoS Protection

lab_

		Original Packet						Translated Packet	
Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1 LAB_WEB_DNAT	none	untrust	untrust	any	any	LAB_70.50.30	LAB_WEB_SERVICES	none	address: LAB_10.10.10.20_WebServer_DMZ
2 LAB_DNS_DNAT	none	untrust	untrust	any	any	LAB_70.50.30	LAB_DNS_SERVICES	none	address: LAB_10.10.10.20_WebServer_DMZ
3 LAB_SMTP	none	untrust	untrust	any	any	LAB_70.50.30	LAB_SMTP_SERVICES	none	address: LAB_10.10.10.40_SMTP_DMZ

Security Policies

- Click the “Security” tab on the left side under the “Policies” section of the firewall GUI. It is from here that the policy is created to allow the traffic that comes in via the DNAT rules that were just created.
- To add a security rule, click “Add” at the bottom of the page while in the “Security” tab of the firewall.
 - Rule 1: LAB_DNAT_WEBSITE_ACCESS
 - General
 - Use the name “LAB_DNAT_WEBSITE_ACCESS” to label this security rule
 - Rule type: Leave as “universal (default)”
 - Source
 - Source Zone: “Untrust” to designate outside access
 - Source Address: “Any” since we are allowing all internet IP addresses to access this server in this example
 - User
 - If configuring User-ID based access, this is where the settings are applied to access rules, this example does not use User-ID so the settings will be as follows:
 - Source User: “Any”
 - HIP Profile: “Any”
 - Destination
 - Note: in the following settings, the Zone and Address will not match, this is due to the processing order in the firewalls architecture, all DNAT based security policies specify the destination with the Post-NAT Zone, and it’s Pre-NAT IP, giving the mismatch seen below.
 - Destination Zone: “DMZ”
 - Destination Address: “LAB_70.50.30.10_IP”
 - Application
 - For our webserver, we will allow the SSL and web-browsing applications to ensure that no other applications are accessing our server.
 - Applications:

Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 6

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- a. SSL
- b. Web-browsing
- vi. Service/URL Category
 1. For the services, we want to be more specific, and allow only the ports specified in addition to the restricted applications so that the applications can only work on TCP 80 and TCP 443.
 2. Service: "LAB_WEB_SERVICES"
 3. URL Category: "Any"
- vii. Actions
 1. Action Setting: "Allow"
 2. Profile Setting: set your desired Security Profiles or Security Groups for the web traffic to the server.
- b. Rule: LAB_DNAT_DNS_ACCESS
 - i. General
 1. Use the name "LAB_DNAT_DNS_ACCESS" to label this security rule
 2. Rule type: Leave as "universal (default)"
 - ii. Source
 1. Source Zone: "Untrust" to designate outside access
 2. Source Address: "Any" since we are allowing all internet IP addresses to access this server in this example
 - iii. User
 1. If configuring User-ID based access, this is where the settings are applied to access rules, this example does not use User-ID so the settings will be as follows:
 2. Source User: "Any"
 3. HIP Profile: "Any"
 - iv. Destination
 1. Note: in the following settings, the Zone and Address will not match, this is due to the processing order in the firewalls architecture, all DNAT based security policies specify the destination with the Post-NAT Zone, and it's Pre-NAT IP, giving the mismatch seen below.
 2. Destination Zone: "DMZ"
 3. Destination Address: "LAB_70.50.30.10_IP"
 - v. Application
 1. For our DNS server, we will allow DNS application to ensure that no other application is accessing our server.
 2. Applications: DNS
 - vi. Service/URL Category

Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 7

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

1. For the services, we want to be more specific, and allow only the ports specified in addition to the restricted application so that the application can only work on TCP/UDP 53.
 2. Service: "LAB_DNS_SERVICES"
 3. URL Category: "Any"
- vii. Actions
1. Action Setting: "Allow"
 2. Profile Setting: set your desired Security Profiles or Security Groups for the web traffic to the server.
- c. Rule 3: LAB_DNAT_SMTP_ACCESS
- i. General
 1. Use the name "LAB_DNAT_SMTP_ACCESS" to label this security rule
 2. Rule type: Leave as "universal (default)"
 - ii. Source
 1. Source Zone: "Untrust" to designate outside access
 2. Source Address: "Any" since we are allowing all internet IP addresses to access this server in this example
 - iii. User
 1. If configuring User-ID based access, this is where the settings are applied to access rules, this example does not use User-ID so the settings will be as follows:
 2. Source User: "Any"
 3. HIP Profile: "Any"
 - iv. Destination
 1. Note: in the following settings, the Zone and Address will not match, this is due to the processing order in the firewalls architecture, all DNAT based security policies specify the destination with the Post-NAT Zone, and it's Pre-NAT IP, giving the mismatch seen below.
 2. Destination Zone: "DMZ"
 3. Destination Address: "LAB_70.50.30.10_IP"
 - v. Application
 1. For our SMTP Gateway, we will allow SMTP application to ensure that no other application is accessing our server.
 2. Application: SMTP
 - vi. Service/URL Category
 1. For the services, we want to be more specific, and allow only the ports specified in addition to the restricted applications so that the application can only work on TCP 25.

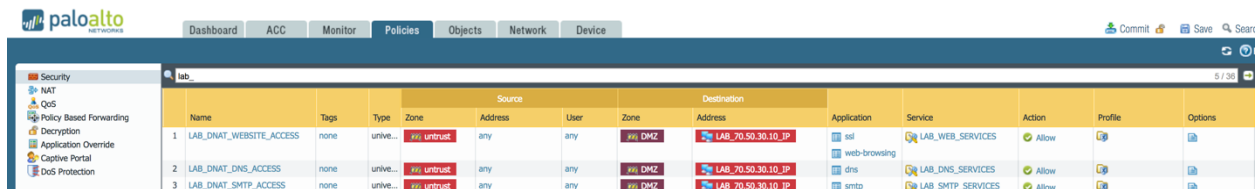
Sun Mgt Bonus Lab 7: Destination NAT multiple services behind a single IP 8

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

2. Service: "LAB_SMTP_SERVICES"
3. URL Category: "Any"

vii. Actions

1. Action Setting: "Allow"
2. Profile Setting: set your desired Security Profiles or Security Groups for the web traffic to the server.
 - a. NOTE: If applying anti-virus to a SMTP gateway, applying a "block" to incoming SMTP traffic can cause SMTP related issues as it is based on delivery assurance.



The screenshot shows the Palo Alto Networks GUI with the 'Policies' tab selected. A table lists three security policies:

Name	Tags	Type	Zone	Source Address	User	Zone	Destination Address	Application	Service	Action	Profile	Options
1 LAB_DNAT_WEBSITE_ACCESS	none	untrust	untrust	any	any	DMZ	LAB_70.50.30.10_IP	ssl	LAB_WEB_SERVICES	Allow		
2 LAB_DNAT_DNS_ACCESS	none	untrust	untrust	any	any	DMZ	LAB_70.50.30.10_IP	dns	LAB_DNS_SERVICES	Allow		
3 LAB_DNAT_SMTP_ACCESS	none	untrust	untrust	any	any	DMZ	LAB_70.50.30.10_IP	smtp	LAB_SMTP_SERVICES	Allow		

3. Commit the changes to push the candidate configuration to the running configuration to make the changes live on the Palo Alto Networks Firewall.

Conclusion

Once all security policy and NAT policies are in place, you will be able to have all 3 services available behind a single public IP address, these services are also secured using application rules and security Profiles.

The Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a couple options:

- a. Contact your Sun Management Account Rep to get pricing on a lab bundle. The newly released PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **sales@sunmanagement.net** for assistance.

- b. Reach out through the free Fuel Users Group (www.fuelusersgroup.org) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their “Virtual Test Lab,” in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their “Virtual Test Lab” at any time)
- c. For access to live Palo Alto Networks boxes for lab practice purposes please go to:
<https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>. This is a no charge service provided by Palo Alto Networks.

If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.

*Please direct any questions/comments/feedback on this lab exercise to:
education@sunmanagement.net*

Lab Author: Alex Jones, PCNSE, Network Security Engineer

Last Modified: Mar 6, 2018

