Palo Alto Networks

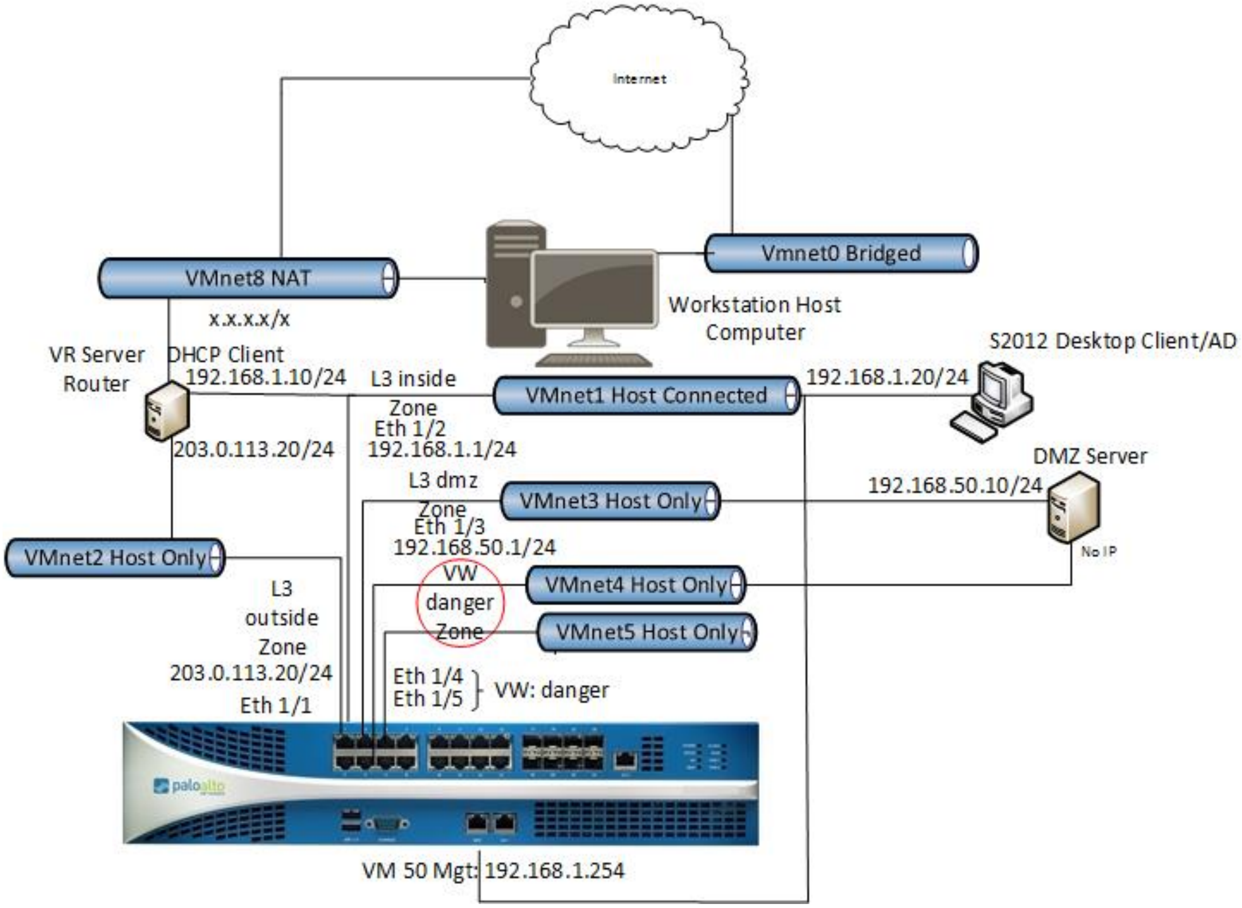
Academy Labs

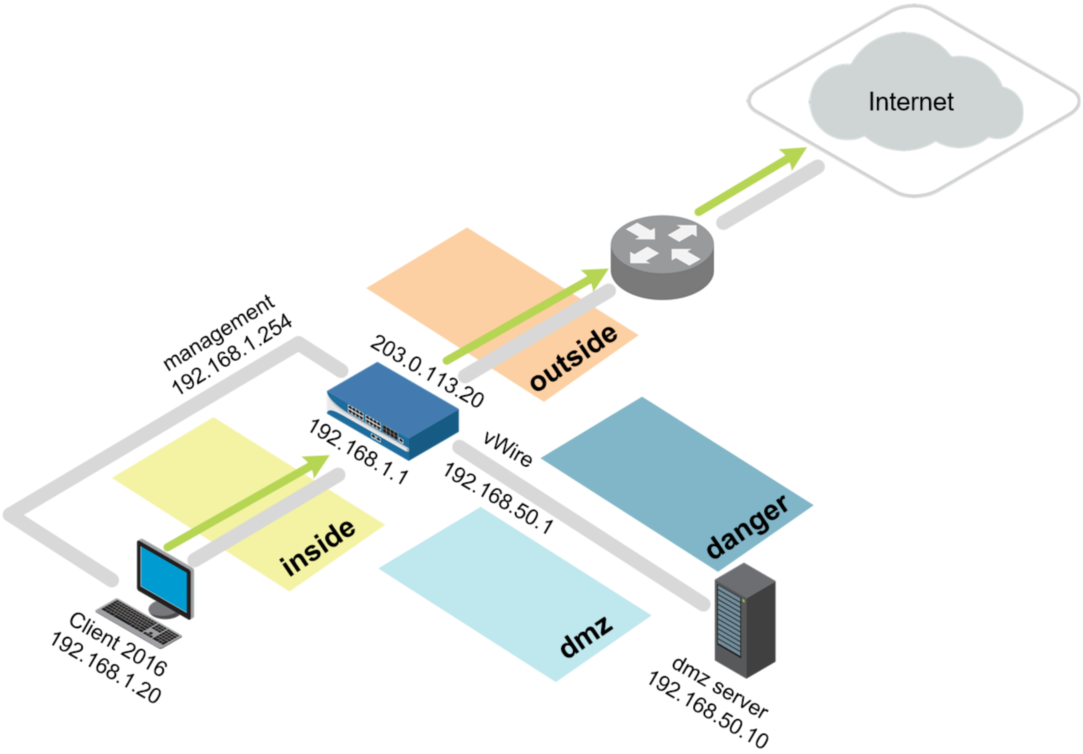
Lab 3 Security and NAT Policies

Document Version: 2018-11-10

www.paloaltonetworks.com

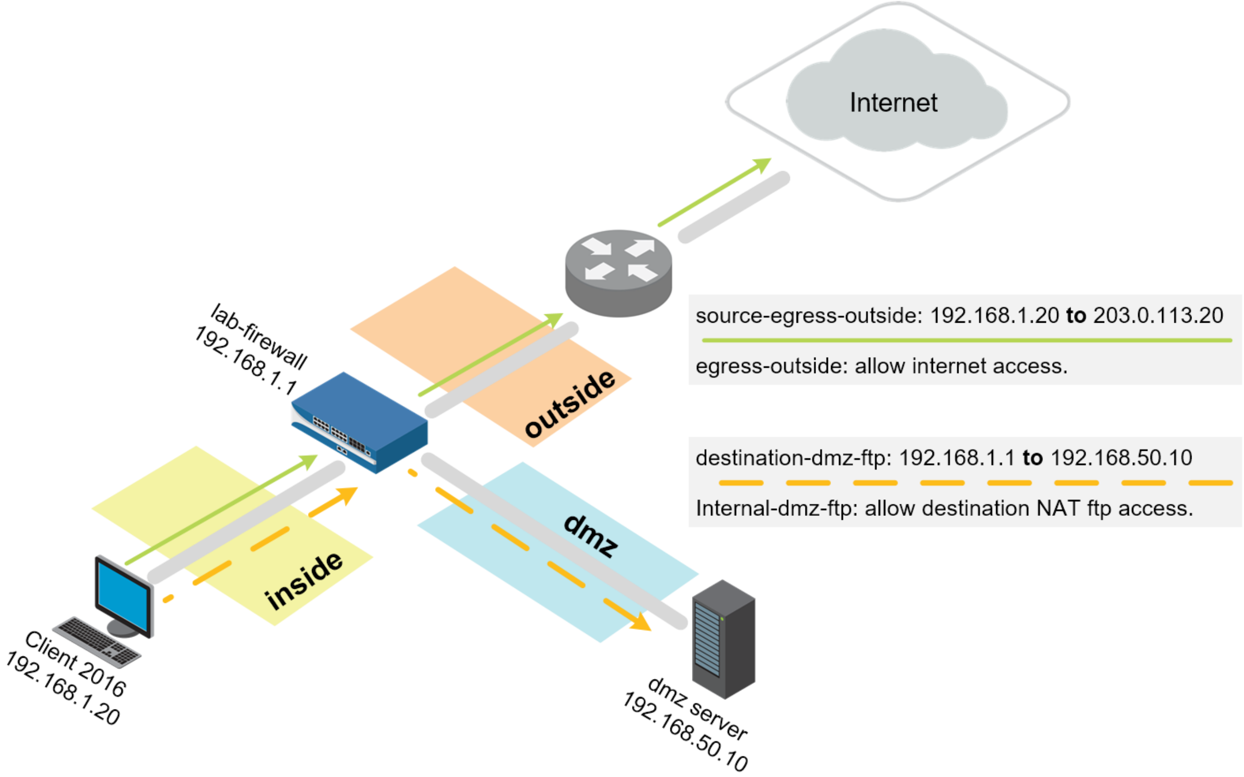
Lab Topology





Virtual Machine	Username	Password
Firewall	admin	admin
Server 2012	lab-user	Pal0Alt0
Centos AAC DMZ	root	Pal0Alt0
Centos Virtual Router	root	Pal0Alt0

Lab 3: Security and NAT Policies

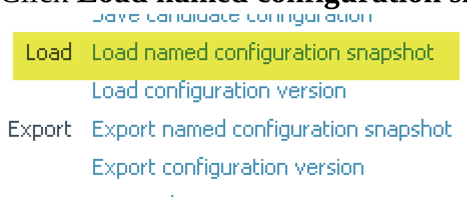

Internet
lab-firewall
192.168.1.1
outside
source-egress-outside: 192.168.1.20 **to** 203.0.113.20
egress-outside: allow internet access.
destination-dmz-ftp: 192.168.1.1 **to** 192.168.50.10
Internal-dmz-ftp: allow destination NAT ftp access.
inside
dmz
Client 2016
192.168.1.20
dmz server
192.168.50.10

Lab Objectives

- Create tags for later use with Security policy rules.
- Create a basic source NAT rule to allow outbound access and an associated Security policy rule to allow the traffic.
- Create a destination NAT rule for the FTP server and an associated Security policy rule to allow the traffic.

3.0 Load Lab Configuration

1. In the web interface select **Device** > **Setup** > **Operations**.
2. Click **Load named configuration snapshot**:


Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version

3. Select **edu-210-lab-03** and click **OK**.
4. Click **Close**.
5. Commit all changes.

3.1 Create Tags

Tags enable you to group, sort, and filter objects using keywords or phrases. Tags can be applied to Address objects, Address Groups (static and dynamic), services, Service Groups, and policy rules. Tags can be assigned a color that makes the results of a search easier to find in the web interface. In the following steps, you will assign a description to a tag, assign the tag a color, and apply the tag to different policies.

6. Select **Objects** > **Tags**. Tags
7. Click Add to define a new tag.
8. Configure the following:

Parameter	Value
Name	Select **danger**
Color	**Purple**

9. Click **OK** to close the **Tag** configuration window.
10. Click Add again to define another new tag.
11. Configure the following:

Parameter	Value
Name	`egress`
Color	**Blue**

12. Click **OK** to close the **Tag** configuration window.
13. Click Add again to define another new tag.
14. Configure the following:

Parameter	Value
Name	Select **dmz**
Color	**Orange**

15. Click **OK** to close the **Tag** configuration window.
16. Click Add again to define another new tag.
17. Configure the following:

Parameter	Value
Name	`internal`
Color	**Yellow**

18. Click **OK** to close the **Tag** configuration window.

3.2 Create a Source NAT Policy

19. Select **Policies** > **NAT**. NAT

20. Click Add to define a new source NAT policy.

21. Configure the following:

Parameter	Value
Name	`source-egress-outside`
Tags	**egress**

22. Click the **Original Packet** tab and configure the following:

Parameter	Value
Source Zone	**inside**
Destination Zone	**outside**
Destination Interface	**ethernet1/1**

23. Click the **Translated Packet** tab and configure the following:

Parameter	Value
Translation Type	**Dynamic IP And Port**
Address Type	**Interface Address**
Interface	**ethernet1/1**
IP Address	Select **203.0.113.20/24** (Make sure to *select* the interface IP address, do not *type* it.)

24. Click **OK** to close the **NAT Policy Rule** configuration window.

You will not be able to access the internet yet because you still need to configure a Security policy to allow traffic to flow between zones.

3.3 Create Security Policy Rules

Security policy rules reference Security zones and enable you to allow, restrict, and track traffic on your network based on the application, user or user group, and service (port and protocol).

25. Select **Policies** > **Security**. Security

26. Click Add to define a Security policy rule.

27. Configure the following:

Parameter	Value
Name	`egress-outside`
Rule Type	**universal (default)**
Tags	**egress**

28. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	**inside**
Source Address	**Any**

29. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	**outside**
Destination Address	**Any**

30. Click the **Application** tab and verify that ☑ Any is selected.

31. Click the **Service/URL Category** tab and verify that application-default ▾ is selected.

32. Click the **Actions** tab and verify the following:

Parameter	Value
Action Setting	**Allow**
Log Setting	**Log at Session End**

33. Click **OK** to close the **Security Policy Rule** configuration window.

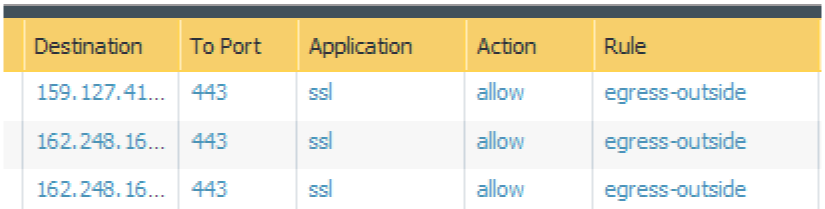
34. Commit all changes.

3.4 Verify Internet Connectivity

35. Test internet connectivity by opening a different browser in private/incognito mode and browse to `msn.com` and `shutterfly.com`.

36. In the web interface select **Monitor** > **Logs** > **Traffic**. Traffic

37. Traffic log entries should be present based on the internet test. Verify that there is allowed traffic that matches the Security policy rule egress-outside. This process may take a minute or two for the log files to be updated:



Destination	To Port	Application	Action	Rule
159.127.41...	443	ssl	allow	egress-outside
162.248.16...	443	ssl	allow	egress-outside
162.248.16...	443	ssl	allow	egress-outside

3.5 Create an FTP Service

When you define Security policy rules for specific applications, you can select one or more services that limit the port numbers that the applications can use.

38. In the web interface select **Objects** > **Services**. Services
39. Click Add to create a new service using the following:

Parameter	Value
Name	`service-ftp`
Destination Port	`20-21`

40. Click **OK** to close the **Service** configuration window.

3.6 Create a Destination NAT Policy

You are configuring destination NAT in the lab to get familiar with how destination NAT works, not because it is necessary for the lab environment. (No outside host will attempt to connect to an internal server.)

41. In the web interface select **Policies** > **NAT**. NAT
42. Click Add to define a new destination NAT policy rule.
43. Configure the following:

Parameter	Value
Name	`destination-dmz-ftp`
Tags	**internal**

44. Click the **Original Packet** tab and configure the following:

Parameter	Value
Source Zone	**inside**
Destination Zone	**inside**
Destination Interface	**ethernet1/2**
Service	**service-ftp**

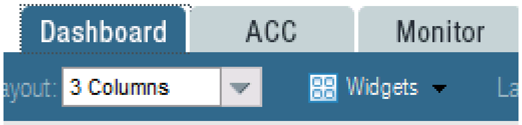
Parameter	Value
Destination Address	`192.168.1.1`

45. Click the **Translated Packet** tab and configure the following:

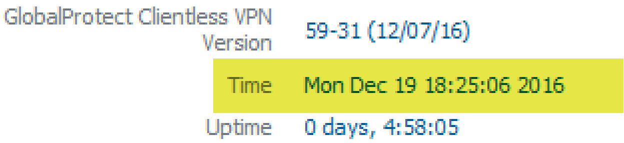
Parameter	Value
Destination Address Translation Type	**Static IP**
Translated Address	`192.168.50.10` (address of DMZ server)

46. Click **OK** to close the **NAT Policy** configuration window.

3.7 Create a Security Policy Rule

47. Click the **Dashboard** tab. 

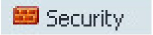
48. Note the current time referenced by the firewall:



GlobalProtect Clientless VPN Version 59-31 (12/07/16)

Time Mon Dec 19 18:25:06 2016

Uptime 0 days, 4:58:05

49. Select **Policies** > **Security**. 

50. Click to define a new Security policy rule.

51. Configure the following:

Parameter	Value
Name	`internal-dmz-ftp`
Rule Type	**universal (default)**
Tags	**internal**

52. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	**inside**

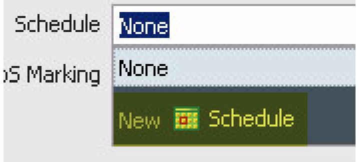
53. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	**dmz**
Destination Address	`192.168.1.1`

54. Click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	**service-ftp**

55. Click the **Actions** tab and verify that **Allow** is selected.
56. Locate the **Schedule** drop-down list and select **New Schedule**:



By default, Security policy rules always are in effect (all dates and times). To limit a Security policy to specific times, you can define schedules and then apply them to the appropriate policy rules.

57. Configure the following:

Parameter	Value
Name	`internal-dmz-ftp`
Recurrence	**Daily**
Start Time	5 minutes from the time noted in Step 48 (firewall time)
End time	2 hours from the current firewall time.

Note: Input time in a 24-hour format.

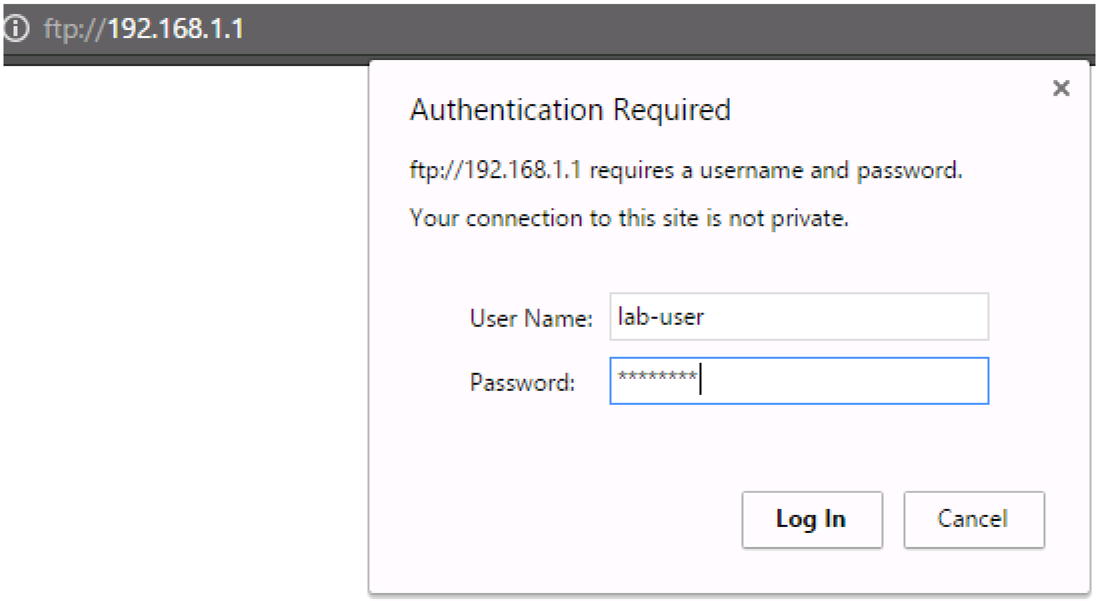
58. Click **OK** to close the **Schedule** configuration window.
59. Click **OK** to close the **Security Policy Rule** configuration window.
60. Commit all changes.

3.8 Test the Connection

61. Wait for the scheduled time to start for the internal-dmz-ftp Security policy rule.
62. Open a new Chrome browser window in private mode and browse to `ftp://192.168.1.1`.
63. At the prompt for login information, enter the following:

Parameter	Value
User Name	`lab-user`

Parameter	Value
Password	`paloalto`



ftp://192.168.1.1

Authentication Required

ftp://192.168.1.1 requires a username and password.

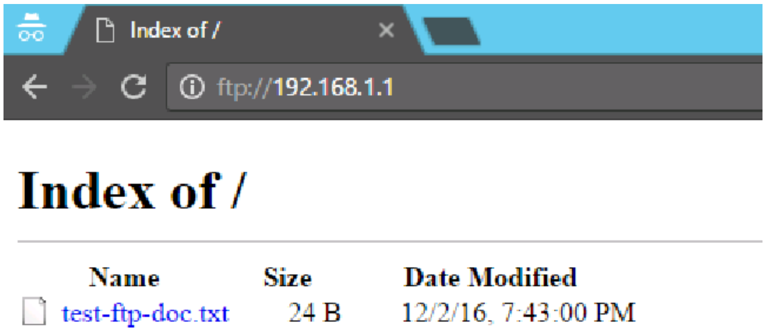
Your connection to this site is not private.

User Name: lab-user

Password: ********

192.168.1.1 is the inside interface address on the firewall. The firewall is not hosting the FTP server. The fact that you were prompted for a username indicates that FTP was allowed through the firewall using the destination NAT.

64. Verify that you can view the directory listing, and then close the Chrome browser window:

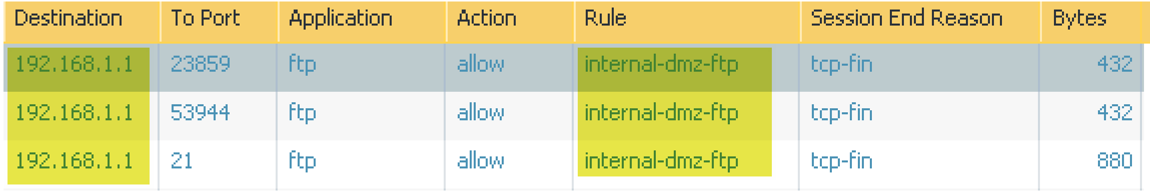


Index of /

Name	Size	Date Modified
test-ftp-doc.txt	24 B	12/2/16, 7:43:00 PM

65. In the web interface select **Monitor** > **Logs** > **Traffic**. Traffic

66. Find the entries where the application ftp has been allowed by rule internal-dmz-ftp. Notice the **Destination** address and rule matching:



Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
192.168.1.1	23859	ftp	allow	internal-dmz-ftp	tcp-fin	432
192.168.1.1	53944	ftp	allow	internal-dmz-ftp	tcp-fin	432
192.168.1.1	21	ftp	allow	internal-dmz-ftp	tcp-fin	880

Stop. This is the end of the Security and NAT Policies lab.