Policy-Based Forwarding

CDT Matthew Driver
CDT Jack Sadle

Integrated Information Technology
ROTC
University of South Carolina

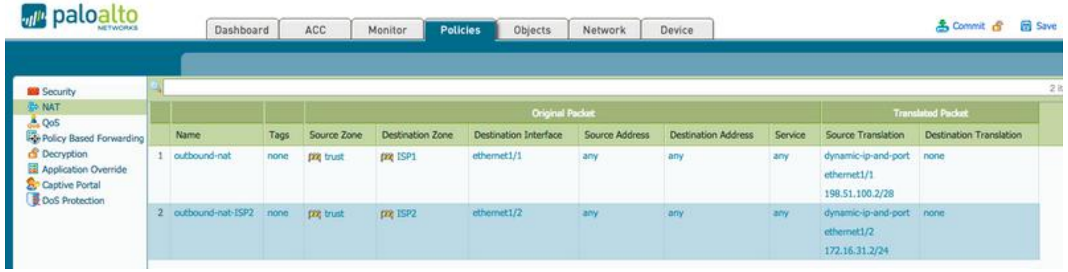
April 22nd, 2021

Agenda

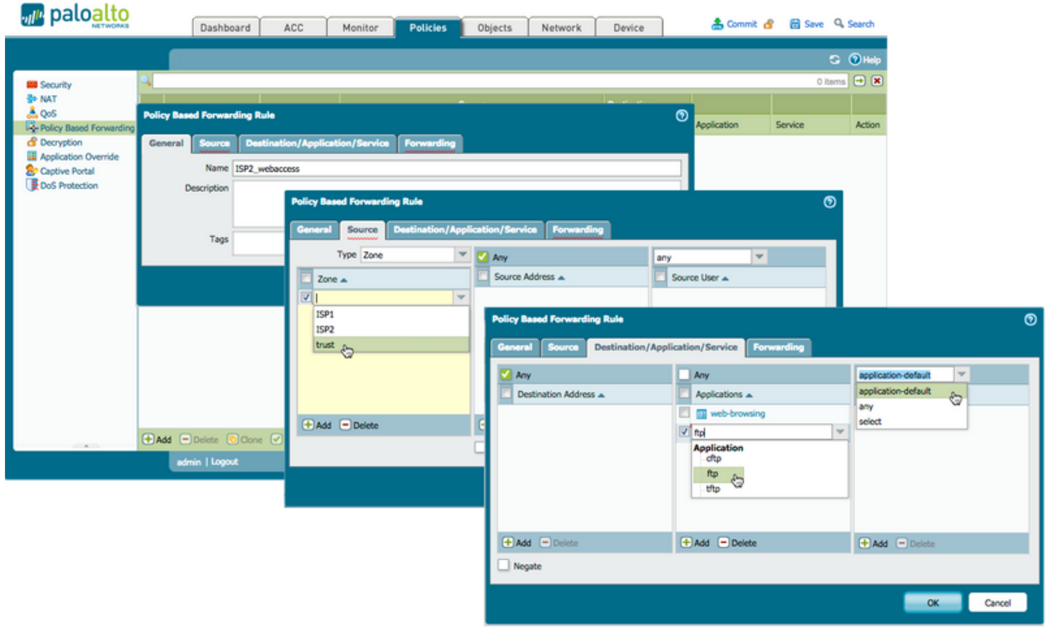
- Introduction
- Policy Based Forwarding
- Scenario Description
- Solution
- Conclusion

Policy Based Forwarding

Under normal circumstances, a security device (firewall, Next-generation Firewall (NGFW)) uses the destination IP address in the packet header to determine the egress interface. Policy-based Forwarding (PBF) allows a network / security engineer to override the routing table, and to specify the egress interface based on specific parameters such as source or destination IP address, or type of traffic.



			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	outbound-nat	none	trust	ISP1	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 198.51.100.2/28	none
2	outbound-nat-ISP2	none	trust	ISP2	ethernet1/2	any	any	any	dynamic-ip-and-port ethernet1/2 172.16.31.2/24	none



Policy Based Forwarding Rule

Name: ISP2_webaccess

Description:

Tags:

Policy Based Forwarding Rule

Type: Zone

□ Zone

☑ Any

□ Source Address

any

□ Source User

Policy Based Forwarding Rule

☑ Any

□ Destination Address

□ Any

□ Applications

□ web-browsing

☑ ftp

application-default

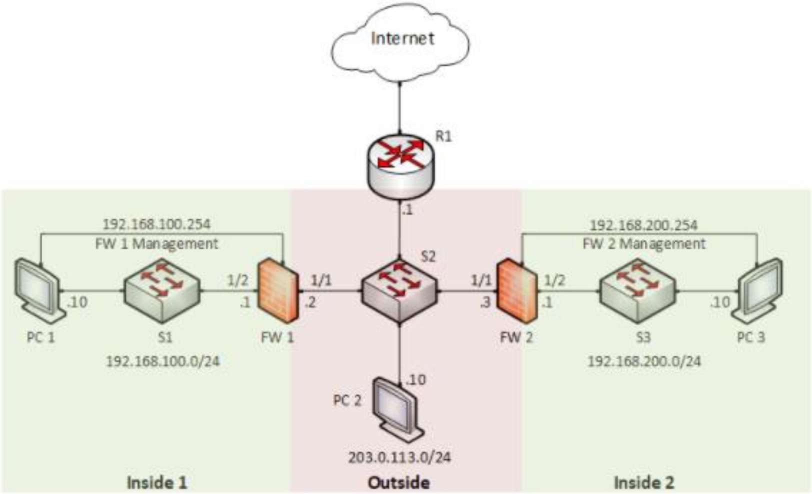
□ Negate

Scenario Description

- Large company infrastructure with high traffic volumes
- Company has access to two ISP’s
- Company uses FTP to transfer files between locations
- Company accesses an offsite FTP server
- Company would like to utilize the second ISP to securely transport FTP traffic

Proposed Solution and Implementation

- Establish a Policy-based Forwarding rule to separate the FTP traffic
- Non-FTP traffic will continue through ISP 1 which is the default route
- Verify connectivity to the external FTP server throughout



Conclusion

- Policy-Based Forwarding is utilized to filter traffic at the NGFW
- Establishing a Policy-Based Forwarding rule will allow a company to separate traffic by type of traffic and or source or destination
- This strategy will allow the company to utilize Policy-Based Forwarding to increase security of FTP traffic to their external server