ASA (Adaptive Security Appliance)

ASA Terminology

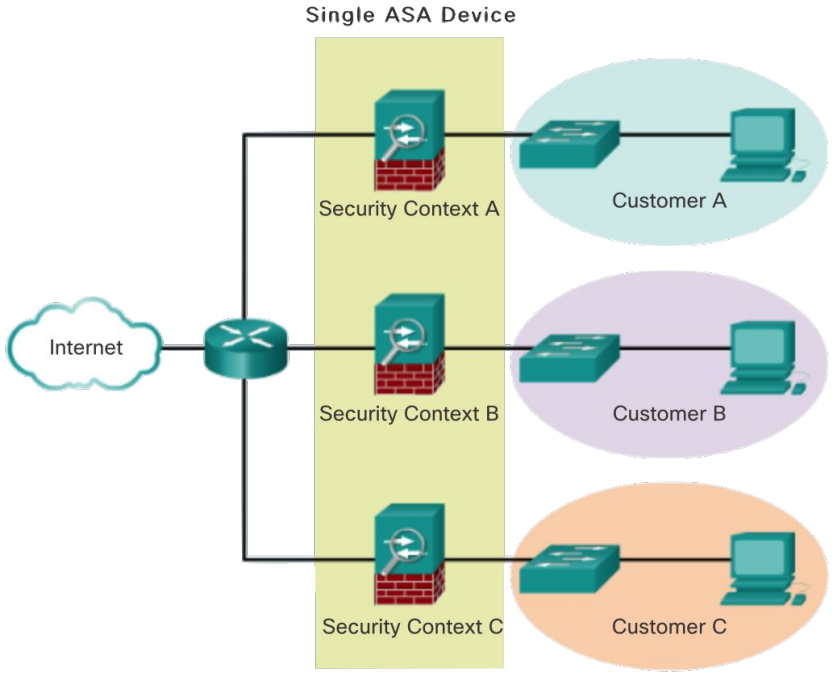
- ASDM: GUI tool for configuring ASA over HTTP
- Partition: virtual “device” created by virtually separating a device
- Packet state: describes if traffic is part of an existing connection or not
- License: software purchased from Cisco to expand an ASA’s capacities
- SVI: a layer 2 physical port encapsulated by a VLAN into a layer 3 interface

What is an ASA?

- Edge router that acts as a firewall
- Uses a different operating system
- Used in larger networks
- Uses SVIs
- Includes other features such as NAT, DHCP, and VPN software
- Additional “modules” can be connected to add additional security features

Partitioning

- An ASA can be partitioned, meaning it acts as if it is multiple separate devices
- Each partition has a different “security context”
- This allows the ASA to have different configurations for different groups



ZBF (Zone-Based Firewall)

- Typically includes 3 basic zones
  - inside (trusted by default)
  - outside (untrusted by default)
  - DMZ (limited outside access allowed)
- A trusted zone allows incoming connections, while an outside zone blocks them

Stateful Firewall

- Tracks (inspects) the state of a packet
- Allows incoming “replies”, but not incoming packets from unestablished connections
- Inspection occurs at the session management path, which is part of the management plane
- Packets from an established connection are not rechecked

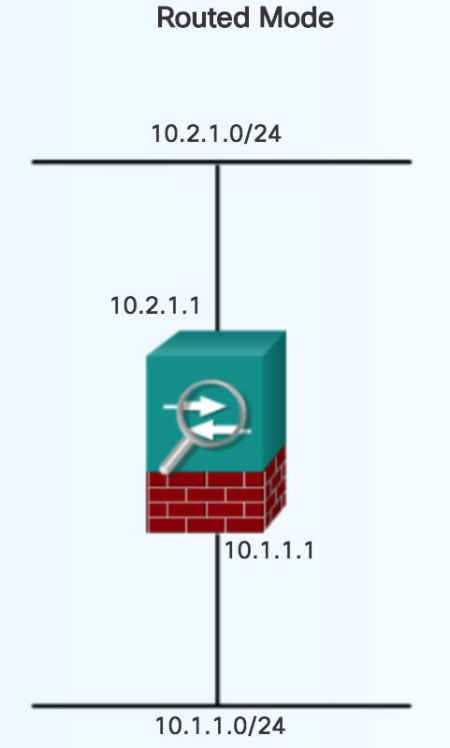
Layer 7 Inspection

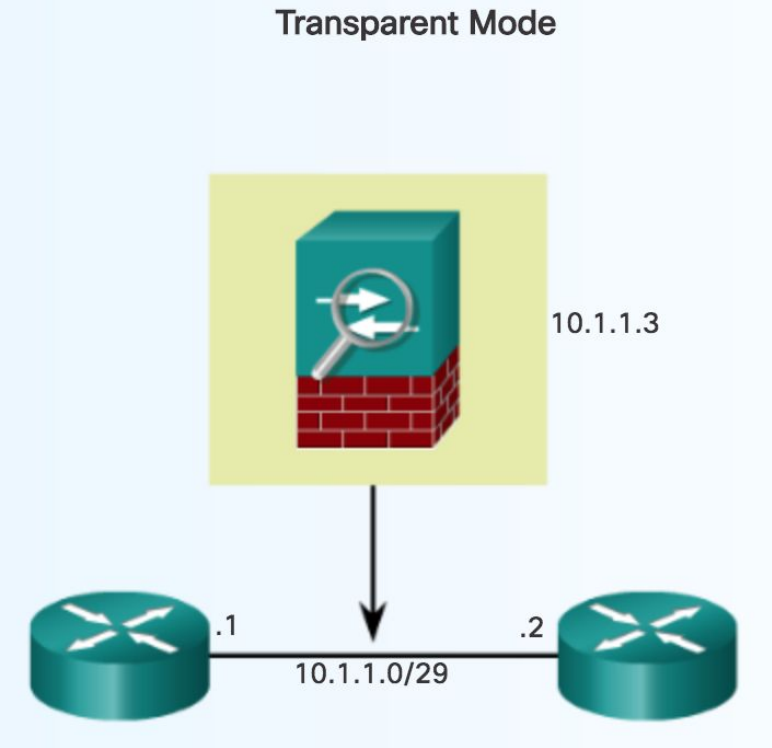
- Filters based on the data itself, not headers
- Can be configured to filter malware, viruses, certain users, illegal activity, etc
- Can be used unethically for large-scale censorship
- Can be circumvented by a VPN or other types of encryption
- Certain protocols require layer 7 inspection due to embedded data (FTP, SNMP, H.323)

Firewall Modes

- Routed mode
  - ASA is considered a router/"hop" in the network
  - Can perform layer 3 services
  - Each interface is on a different subnet
- Transparent mode
  - ASA is considered a layer 2 switch
  - Invisible to attackers
  - Cannot perform layer 3 services

Firewall Modes





Security Levels

- Define the level of trustworthiness
- 0–100 (100 is most trusted)
- Traffic from an interface with a higher security level sent to an interface with a lower security level is considered outbound traffic and vice versa for inbound
- Help control network access, inspection engines, and filtering

OS Differences

- Does not require “do” before “show” commands
- Does not have an “enable secret” command
- Has a “help [command]” command that shows command syntax and a description
- Uses security levels to apply access control by default

OS Differences (cont.)

IOS Router Command	Equivalent ASA Command
`erase startup-config`	`write erase`
`enable secret`	`enable password`

`line con 0`
`password password`
`login`
	`passwd password`

`show ip interfaces brief`	`show interfaces ip brief`
`show ip route`	`show route`
`show ip nat translations`	`show xlate`
`show vlan`	`show switch vlan`
`ip route`	`route outside`
`Ctrl+C`	`Q`

Configuring Remote Access

Step Description	Placement	Command	Category	Notes
configure the telnet/ssh password	ASA config	passwd [password]	requirement	equivalent to "password" command in a regular router's vty line config
identify 1+ clients allowed to use telnet/SSH to connect to the router	ASA config	[telnet/ssh] [client ip] [client subnet mask] [vlan name]	requirement	
set a telnet/SSH login timeout	ASA config	[telnet/ssh] timeout [minutes]	optional	default is 5 minutes
create a user account for authentication	ASA config	username [name] password [password]	optional	required for SSH
use the local database for authentication	ASA config	aaa authentication [ssh/telnet] console LOCAL	optional	required for SSH "LOCAL" is caps-sensitive
generate crypto keys for SSH	ASA config	crypto key generate rsa modulus 1024	optional	required for SSH "crypto key zeroize rsa" to reverse the command

Configuring DHCP

Step Description	Placement	Command	Category	Notes
enables the DHCP server service on the inside interface	ASA config	dhcpd enable inside	requirement	
define the pool of IP addresses and assign the pool to inside users	ASA config	dhcpd address [low ip address] - [high ip address] inside	requirement	
define a domain name	ASA config	dhcpd domain [domain name]	optional	
add a DNS server	ASA config	dhcpd dns [ip of dns server]	optional	
add a WINS server address	ASA config	dhcpd wins [wins ip address]	optional	
change the lease time	ASA config	dhcpd lease [seconds]	optional	default is 3600 seconds (1 hour)
pass settings obtained by outside interface to the interface and connected clients	ASA config	dhcpd auto_config outside	optional	passes DNS, WINS, and domain information
show assigned IP addresses	anywhere in an ASA	do show dhcpd binding	optional	

Objects

- Once created, can be used in place of an inline IP address in any ASA configuration
- Can be defined with an IP address/netmask or a protocol/port
- Can be reused
- When an object is modified, the change is automatically applied to all rules using it

Types of Objects

- Network object (**`object network`** command)
  - contains a single IP address/mask pair
  - can be a host, subnet, or range
  - required in NAT
- Service object (**`object service`** command)
  - contains a protocol and optional source and/or destination port

Object Config

Process	Step Description	Placement	Command	Category	Notes
Network object	create a network object/access the network object config	ASA config	object network [name]	requirement	
	define the network object	network object config	host [ip address] subnet [subnet address] [subnet mask] range [low ip address] [high ip address]	requirement	only 1 of the 3 options may be used per object entering a second option replaces the first
Service object	create a service object/access the service object config	ASA config	object service [name]	requirement	
	define the service object	service object config	service [protocol] (optional: [source/destination] [operator] [port]) service [icmp/icmp6] [type]	requirement	only 1 of the 2 options may be used per object entering a second option replaces the first operators include lt, gt, eq, neq, range default operator is eq

Object Groups

- A group of similar objects
- Cannot share a name with objects
- 4 types: network, service (to define port numbers), protocol, ICMP-type
- Cannot be removed or emptied if used in a command
- Cannot be used for NAT

Object Group Config

Step Description	Placement	Command	Category	Notes
create/configure a network group	ASA config	object-group [network/service/protocol/icmp-type] [name]	requirement	"tcp/udp/tcp-udp" is added to the end if using a service group
add a description	group config	description [description]	optional	
add a pre-existing group to the group	group config	group-object [group name]	optional	
add an object to a group	group config	[port/network/protocol/icmp/service]-object [arguments]	optional	use "?" to view list of arguments to use

ACLs

- Configured the same way as an extended ACL, but with a name instead of a number
- Standard ACLs filter based on destination (instead of source); typically only used for OSPF
- Extended ACLs are also used in AAA, VPN, and MPF config
- Use netmask instead of wildcard
- ASAs also have a webtype ACL (used for VPNs) and an EtherType ACL (used in transparent mode)
- Configured similarly to IOS ACLs
- Arguments can be objects/object groups

Types of ACL Filtering

- Through-traffic filtering
  - applies to traffic passing through the ASA from one interface to another
  - normal ACL configuration
    - Set up an ACL
    - Apply ACL to an interface
- To-the-box-traffic filtering
  - aka management access rules
  - applies to traffic that terminates on the ASA
  - requires an additional set of rules to implement access control

Applying ACLs

- Uses the “access-group” command like in IOS
- “access-group” command is used in global config mode
- Interface is then specified by name
- "per-user-override" can be added to the end to allow downloadable ACLs to override the entries on the interface
- "control-plane" can be added to the end to apply the ACL to the management plane

ACL Config Example

```
access-list ACL-IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
access-list ACL-IN extended permmit ip any any
access-group ACL-IN in interface inside
```

Not my typo -_-

```
CCNAS-ASA(config)# access-list ACL-IN extended permit object-
group TCP
object-group Internet-Hosts object-group Internal-Servers object-
group HTTP-SMTP
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
```

NAT

- Configured using objects
- Can use dynamic/static NAT or PAT
- Commands are entered within network object configuration mode
- Many more commands outside of Packet Tracer

NAT Config

Step Description	Placement	Command	Category	Notes
create/configure a network object	ASA config	object network [name]	requirement	
identify a range of inside addresses to be mapped	network object config	host [ip address] subnet [subnet address] [subnet mask] range [low ip address] [high ip address]	requirement	only 1 of the 3 options may be used per object entering a second option replaces the first
configure dynamic nat	network object config	nat ([inside int name],[outside int name]) dynamic [network object]	optional	network object can be replaced with the keyword "interface" to enable PAT
configure static NAT	network object config	nat ([inside int name],[outside int name]) static [outside address]	optional	keyword "any" can be used instead of the outside interface name to allow translation between multiple interfaces
show translations	anywhere in an ASA	show xlate	optional	

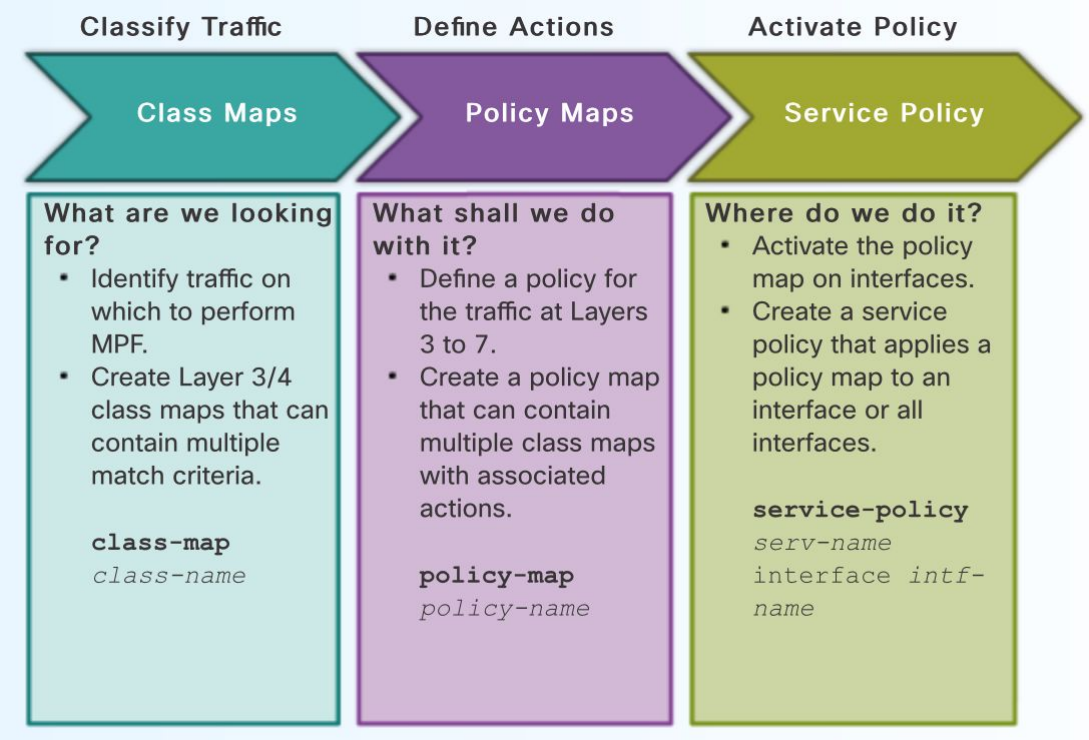
NAT Config Examples

```
ıfig)# object network DMZ-SERVER
ıfig-network-object)# host 192.168.2.3
ıfig-network-object)# nat (dmz,outside) static 209.165.200.227
ıfig-network-object)# exit
ıfig)#
ıfig)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
ıfig)# access-group OUTSIDE-DMZ in interface outside
ıfig)#
```

```
ıfig)# object network PUBLIC-IP
ıfig-network-object)# range 209.165.200.240 255.255.255.240
ıfig)# object network INSIDE-NET
ıfig-network-object)# subnet 192.168.1.0 255.255.255.224
ıfig-network-object)# nat (inside,outside) dynamic PUBLIC-IP
ıfig-network-object)# end
```

MPF

- Modular Policy Framework
- Defines a set of rules for applying firewall features
- Can be used to filter based on layers 5–7



MPF Config Steps

1. (Optional) Configure extended ACLs to identify specific traffic
2. Configure the class map to identify traffic
3. Configure a policy map to apply actions to the class maps
4. Configure a service policy to attach the policy map to an interface

MPF Config Steps

Step Description	Placement	Command	Category	Notes
create/configure a map	ASA config	class-map [name]	requirement	
add a preconfigured ACL to use	map config	match access-list [acl name]	requirement	"match any" can be used to match all traffic
add a description	map config	description [description]	optional	
enter class map config mode	map config	class [name]	optional	allows configuration of inspect and other commands
inspect traffic using a protocol	class map config	inspect [application]	optional	
apply the policy map	ASA config	service-policy [map name] interface [int name]	requirement	replace "interface [int name]" with "global" to apply it to all interfaces

MPF Config Example

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

Packet Tracer Lab

CCNA 9.4.1.5

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash