Post 8

Thursday, January 24, 2019 11:25 PM

ASA 5505'S P1

ASA FW Models:
SOHO:

ASA 5505/Security Plus	Up to 150 Mbps
ASA 5506-X/Security Plus	750 Mbps
ASA 5512-X/Security Plus ASA 5515-X	1 Gbps 1.2 Gbps

Internet edge: Medium/large businesses:

ASA 5525-X	2 Gbps
ASA 5545-X	3 Gbps
ASA 5555-X	4 Gbps

Large enterprises/data centers

ASA 5585-X SSP10	4 Gbps
ASA 5585-X SSP20	10 Gbps
ASA 5585-X SSP40	20 Gbps
ASA 5585-X SSP60	40 Gbps
ASA Service Module	20 Gbps

All models provide advanced stateful firewall features/VPN functionality

- **Biggest diff:** Max throughput/number/types of ints

Cisco ASAv: Adaptive Security Virtual Appliance

- Virtual domain: Server hypervisor can create virtual switch capable of supporting many types of VM's
- Ops as VM using server's ints to process traffic
- Also supports site-to-site/remote-access VPN/clientless VPN
- Doesn't support clustering/multiple contexts

Avail in 3 models:

1. **ASAv5:** 2GB mem: 100 Mbps throughput
2. **ASAv10:** 2GB mem: 1Gbps throughput
3. **ASAv30:** 8GB mem: 2Gbps throughput

ASA Next-Generation FW Apps: SW combines: FW/VPN concentrator/intrusion prevention into 1 img

Advanced ASA FW 4 features:

Virtualization	Single ASA: Partitioned into multiple virtual devices • Security context: Each virtual device • Each context independent device w/own sec policy/ints/admins • Multiple contexts: Similar to having multiple standalone devices Features supported in multiple context modes: Routing tables/FW features/IPS/Mgmt Features not supported: VPN/Dynamic routing protocols
High avail w/failover	2 identical ASAs: Paired into active/standby failover config: Redundancy • Both platforms must be identical: SW/license/mem/ints incl/SSM: Sec Services Module
ID FW	Optional: Granular access control based on association of IP's to Win AD login info • Client attempts to access server: Must auth using AD ID-based FW • Enhance access control/sec policy allowing usrs/groups/specified in place of source IP's • ID-based sec policies can be interleaved w/out restriction bet traditional IP-based rules

Threat control/containment	All ASA's support IPS: Advanced IPS only provided by integrating HW modules w/ASA arch • IPS capability avail using AIP: Advanced Inspection/Prevention modules • Anti-MW can be deployed by integrating CSC: Content Sec/Control module • AIP-SSM: Advanced Inspection/Prevention Sec Services Module • AIP-SSC: Advanced Inspection/Prevention Sec Services Card ○ Deliver protection against thousands of known exploits ○ Also protect against millions of unknown exploit variants using IPS engines/sigs

FW's in Network Design

Outside	Network/zone outside protection of FW
Inside	Network/zone protected/behind FW
DMZ	Demilitarized Zone: Allows both inside/outside usrs access to protected network resources

How zones interact for permitted traffic:

- Traffic from inside: Going outside: Permitted
- Traffic from inside: Going to DMZ: Permitted
- Traffic from outside: Going to DMZ: Selectively permitted

How zones interact for denied traffic:

- Traffic from outside: Going inside: Denied
- Traffic from DMZ: Going inside: Denied

ISRs: Can provide FW features by using ZPF: Zone-Based Policy FW or CBAC: Context-Based Access Control

ASA: Same features, but config differs from IOS rtr config of ZPF

- Dedicated FW appliance
- Default: Treats defined inside int as trusted network/any defined outside ints as untrusted
- Each int: Associated sec lvl
- Sec lvls enable it implement sec policies (AKA trust levels)

2 ASA Modes of Op:

Routed	2/more ints separate L3 networks [domains] • Supports multiple ints • Each int on diff subnet/req an IP on that subnet • ASA applies policy to flows as they transit FW
Transparent	**AKA: Bump in the wire/Stealth FW** • Functions like L2 device/not considered router hop • Useful to simplify network config/when existing addressing can't be altered **Drawbacks:** No support for dynamic routing protocols/VPNs/QoS/DHCP Relay

License: Specifies options enabled on given ASA

- Most come pre-installed w/either Base or Security Plus license
- **ASA 5505:** Base license/option to upgrade to Sec Plus license
  - **Security Plus**: Enables 5505 to scale to support higher connection capacity/up to 25 IPsec VPN usrs
  - Adds full DMZ support/integrates into switched network envs through VLAN trunking support
  - Enables support for redundant ISP connections/stateless active/standby high-avail services

Verify license info on ASA
R1# show version
R1# show activation-key

Base License	Security Plus License
FW Conns, Concurrent: 10,000	FW Conns, Concurrent: 25,000
VPN Licenses	VPN Licenses
Combined VPN sessions of all types, Max: 25	Combined VPN sessions of all types, Max: 25
Other VPN (sessions): 10	Other VPN (sessions): 25

Overview of ASA 5505

- **Default DRAM**: 256 MB (up to 512 MB)
- **Default flash**: 128 MB

- **Failover config:** 2 units must be identical models w/same HW config/number/types of ints/RAM

Front Panel:
- USB 2 port
- Speed/Link Activity LEDs: Solid green indicates 100 Mb/s: LED off? Indicates 10 Mb/s
- Power/Status/Active/VPN tunnel LEDs
- Sec Services Slot LED: Indicates SSC card present

Back Panel:
- 48 VDC power connector
- 2 10/100 PoE ports
- 6 10/100 Fast Ethernet ports: Can be dynamically grouped to create 3 separate VLANs/zones: Network segmentation/sec
- 2 USB 2 ports
- Reset button/Lock slot/Serial/Con port
- **Sec Service Card Slot:** Adds AIP-SSC card: Intrusion prevention services

ASA Sec Lvls
- Assigns sec lvls to distinguish bet inside/outside networks
- **Sec lvls:** Define the lvl of trustworthiness of an int
- Higher lvl? More trusted int
- #'s range from 0: untrustworthy-100: very trustworthy
- **Each int must have a name/sec lvl from 0-100**
- **Lvl 100:** Assigned to most sec network (inside): Can be assigned to outside

DMZs/other networks can be assigned sec lvl bet 0-100
- Traffic from int w/higher lvl to lower lvl int: Outbound traffic
- Traffic from int w/lower lvl to higher lvl int: Inbound traffic

Default: Outbound traffic: Allowed/inspected
- Returning traffic allowed b/c of stateful packet inspection
- Traffic from outside/going into either DMZ/inside: Denied: Default
- Return traffic: Inside/returning via outside int: Allowed
- Any exception req ACL to explicitly permit traffic from int w/lower lvl to int w/higher lvl

ASA 5505 Deployment Scenarios
- Edge sec device: Small business to ISP device (DSL/Cable modem)
- Inside network (VLAN 1) w/sec lvl 100: Outside network (VLAN 2) w/sec lvl 0

Config includes 2 preconfig VLANs:
1. **VLAN 1:** For inside network
2. **VLAN 2:** For outside network

IOS cmd	ASA cmd
enable secret [password]	**enable password** [password]
line vty 0 – 4 **password** [password] **login**	**passwd** [password]
ip route	**route** if_name
sh ip int br	**sh int ip br**
sh ip route	**sh route**
sh vlan	**sh switch vlan**
sh ip nat translations	**sh xlate**
copy run start	**write** [memory]
erase startup-config	**write erase**

ASA: Restore factory default
configure factory-default [global]

ASA Setup Wiz: Displayed when ASA erased/rebooted using **write erase/reload** [priv]
- When device rebooted: Wiz asks "Pre-config FW now through interactive prompts [yes]?"
- Default ASA prompt **ciscoasa>**

Enter priv EXEC

enable user EXEC mode
NTP: Set date/time
clock set [priv]
Legal notification
banner motd
Priv EXEC passwd auto encrypted using MD5: Stronger encryption using AES should be enabled
Change master passphrase
key config-key password-encryption
Determine if password encryption enabled
show password encryption
Basic Config Cmds
hostname name
domain-name name
enable password password
banner motd message
key config-key password-encryption [new-pass | old-pass]
password encryption aes

Config Logical VLAN Ints: Config ints on 5505 diff from other 5500 series ASA models

- Other ASAs: Phys port can be assigned L3 IP directly
- ASA 5505: 8 integrated switch ports are L2

2 kinds of ints that need to be config:

1. Logical VLAN ints: Config w/L3 info including name/sec lvl/IP
2. Phys switch ports: L2 switch ports assigned to logical VLAN ints

L3 params config on logical VLAN int SVI: Switch Virtual Int

- Requires name/int sec lvl/IP
- L2 switch ports are assigned specific VLAN
- Switch ports on same VLAN can comm w/each other using HW switching
- Switch port on VLAN 1 wants to comm w/port on VLAN 2?
    - ASA applies sec policy to traffic/routes bet 2 VLANs

ASA 5505 w/Base license: Doesn't allow 3 fully functioning VLAN ints to be created
3rd "limited" VLAN int can be created if 1st config w/
no forward interface vlan

- Cmd limits int from initiating contact w/another VLAN
- When inside/outside VLAN ints config: no forward interface vlan # entered before **nameif**entered on 3rd int
- # arg specifies VLID to which int can't initiate traffic
- Security Plus license required to achieve full functionality

IP of int can be config using 1 of following:
Manually: Assign IP/mask to int
DHCP: When int connecting to upstream device providing DHCP services

- Int can be DHCP client/discover its IP/DHCP-related info from upstream device

PPPoE: When int connecting to upstream DSL device point-to-point connectivity over Ethernet services

- Int can be PPPoE client/discover IP from upstream DSL device

Logical VLAN int Cmds

int vlan vlan-number	VLAN int config mode
nameif if_name	Names int using txt str
security-level value	Sets sec lvl 0-100

Config IP on VLAN ints

manually	**ip address ip/netmask**
DHCP	**ip address dhcp** **ip address dhcp setroute**
PPPoE	**ip address pppoe** **ip address pppoe setroute**

ASA(config)# int vlan 1
ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default
ASA(config-if)# security-level 100

ASA(config-if)# ip address 192.168.1.1 255.255.255.0
ASA(config-if)# exit

ASA(config)# int vlan 2
ASA(config-if)# nameif outside
INFO: Security level for "inside" set to 100 by default
ASA(config-if)# security-level 0
ASA(config-if)# ip address 209.165.200.226 255.255.255.248
ASA(config-if)# exit

Assigning L2 Ports to VLANs
- Default: All L2 switch ports assigned to VLAN 1
- To change default VLAN L2 port must be config using **switchport access vlan vlan-id**

ASA(config)# int e0/0
ASA(config-if)# switchport access vlan 2
ASA(config-if)# no shut
ASA(config-if)# exit

ASA(config)# int e0/1
ASA(config-if)# switchport access vlan 1
ASA(config-if)# no shut
ASA(config-if)# exit

Running config only displays switchport access vlan cmd for ints whose VLAN changed from 1
- Ints in default VLAN 1 don't display cmd

show switch vlan Verify VLAN settings
show interface / **show interface ip brief** Display status of all ASA ints
show ip address Display info for L3 VLAN ints

Config Default Static Route
- If ASA config as a DHCP client: Can receive/install default route from upstream device
- Otherwise: Default static route must be config using:
    - route int-name 0.0.0.0 0.0.0.0 next-hop-ip cmd

ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
ASA(config)# show route | begin Gateway Verify route

Config Remote Access Services
- Telnet/SSH req to manage ASA 5505 remotely
- **aaa authentication telnet console LOCAL** Overrides passwd set w/passwd cmd
    - Auth's Telnet access against local db

Telnet Config
ASA(config)# password cisco
ASA(config)# telnet 192.168.1.3 255.255.255.255 inside
ASA(config)# telnet timeout 3
ASA(config)# show run telnet
telnet 192.168.1.3 255.255.255.255 inside
telnet timeout 3

ASA Cmd	Description
passwd | password *password*	Sets login pass up to 80 chars in length
telnet { *ipv4/mask* **|** *ipv6/prefix***}** *ifname*	ID's which inside host/network can telnet to ASA
telnet timeout *minutes*	Default: Idle 5+ min closed by ASA: Alters default
aaa authentication telnet console LOCAL	Configs Telnet to refer to local db for auth
clear configure telnet	Removes telnet connection from config

Config SSH Access
ASA(config)# username ADMIN password class
ASA(config)# aaa authentication ssh console LOCAL
ASA(config)# crypto key generate rsa modulus 2048

ASA(config)# ssh 192.168.1.3 255.255.255.255 inside
ASA(config)# ssh 192.168.1.4 255.255.255.255 inside
ASA(config)# ssh 172.16.1.3 255.255.255.255 outside
ASA(config)# ssh version 2
ASA(config)# show ssh
show ssh Verify SSH config

ASA Cmd	Description
username name password password	Creates local db entry
aaa authentication ssh console LOCAL	Configs SSH to refer to local db for auth • LOCAL is a predefined server tag
crypto key generate rsa modulus size	Generates RSA key req for SSH encryption: Modulus size: 512/768/1024/2048
ssh ipv4/mask | ipv6/prefix ifname	ID's which inside host/network can SSH to ASA int: Multiples allowed • If ifname not specified: SSH enabled on all ints except outside int
ssh version #	Default: ASA allows v1/v2: Restrict connections to specific version
ssh timeout minutes	Alters default exec timeout of 5 min
clear configure ssh	Removes SSH connection from config

Config NTP Services

- **NTP: Network Time Protocol:** Can be enabled on ASA to obtain date/time from NTP server

ASA(config)# ntp authenticate
ASA(config)# ntp trusted-key 1
ASA(config)# ntp authentication-key 1 md5 cisco123
ASA(config)# ntp server 192.168.1.254

ASA Cmd	Description
ntp authenticate	Enables auth w/NTP server
ntp trusted-key *key_id*	Specifies auth key ID to be trusted key: Req for auth w/NTP server
ntp authentication-key *key_id***md5** *key*	Sets key to auth w/NTP server
ntp server IP key *key_id*	ID's NTP server

Verify NTP config/status: show ntp status and **show ntp associations**
Config DHCP Services

- ASA can config to be DHCP/provide IP's/DHCP-related info to hosts
- ASA 5505: Base license can provide IP config info for up to 32 DHCP clients
- Base license: 10-usr license: It will permit up to 10 concurrent internal IP's to comm to outside int/VLAN
    - 50-user license: Max 128 clients
    - UL: Unrestricted License: Max 256: Same as all other ASA's
    - If ASA outside int config as DHCP client:
    - dhcpd auto_config outside [global] used to pass DHCP-obtained info to inside clients

Verify DHCP settings:

show dhcpd state	DHCP state for inside/outside ints
show dhcpd binding	DHCP bindings of inside usrs
show dhcpd statistics	DHCP statistics
clear dhcpd binding **clear dhcpd statistics**	Clear bindings/statistics

ASA(config)# dhcpd address 192.168.1.10-192.168.1.41 inside
ASA(config)# dhcpd lease 1800

ASA Cmd	Description
dhcpd address IP1-IP2 ifname	Creates DHCP addr pool: IP1 is start and IP2 is end: Pool must be on same subnet as ASA int

dhcpd dns dns1 dns2	Specifies IP of DNS servers (optional)
dhcpd lease lease-length	Granted to client: Amt of time in sec that client can use allocated IP before lease expires Default: 3600 (1hr): Can be 0-1,048,575
dhcpd domain name	Specifies domain name assigned to client
dhcpd enable ifname	Enables DHCP server service on int (inside typically) of ASA

Intro to Objects/Object Groups

- ASA supports objects/object groups
- Objects created/used by ASA in place of inline IP in any given config
- An object can be defined w/particular IP/entire subnet/range of addr/protocol/specific port range
- Can be re-used in 7 configs

Advantage: When an object is mod: Change auto applied to all rules that use the object: Easy to maintain configs

- Objects can be attached/detached from 1/more object groups when needed,
  - Ensures objects not duplicated, but re-used where needed
  - Can be used in NAT/ACL's/object groups: Network objects are a vital part of config NAT

2 types of objects that can be config:

Network	Contains single IP/mask: 3 types: Host/subnet/range: **object network cmd**
Service	Contains protocol/optional source/dest port: **object service cmd**

Config Network Objects
Create a network object:
object network object-name [global]

- Name can contain only 1 IP/mask pair
- Can only be 1 statement in network object
- Entering a 2nd replaces config

Can be defined using 1 of 3 methods

ASA Cmd	Description
host	Assign IP to named object
subnet	Assigns subnet to named object
range	Assigns range of IP's to named object

clear config object network Erase all network objects

Config Network Object
ASA(config)# object network EXAMPLE-1
ASA(config-network-object)# host 192.168.1.3
ASA(config-network-object)# exit

ASA(config)# show running-config object

ASA(config)# object network EXAMPLE-1
ASA(config-network-object)# host 192.168.1.4
ASA(config-network-object)# range 192.168.1.10 192.168.1.20
ASA(config-network-object)# exit

ASA(config)# show running-config object

Config Service Objects

- **object service object-name** [global]
- Service object config mode: Service object can contain a protocol: ICMP/ICMPv6/TCP/UDP port/port ranges

Ops such as eq (equal), neq (not equal), lt (less than), gt (greater than) and range, support config port for given protocol

- If no op specified: Default op is eq

Service object name can only be associated with 1 protocol/port(s)

- If an existing service object is config w/diff protocol/port: New config replaces existing protocol/port w/new ones

Service Object Cmds

ASA Cmd	Description
service protocol [source [*op port* **] destination [***op port* **]]**	Specifies IP protocol/name/number
service tcp [source [*op port***] destination [***op port***]]**	Specifies service object for TCP
service udp [source [*op port***] destination [***op port***]]**	Specifies service object for UDP
service icmp icmp-type	Specifies service object for ICMP
service icmp6 icmp6-type	Specifies service object for ICMPv6

Syntax:
ASA(config)# object service SERV-1
ASA(config-service-object)# service tcp destination eq ftp
ASA(config-service-object)# service tcp destination eq www
ASA(config-service-object)# exit

ASA(config)# show running-config object service Verify service object configs

Object Groups: Can be grouped together to create an object group: By doing so: Object group can be used in ACE entry

- Instead of having to enter ACE for each object separately
- Protocol object group can also be created: Not recommended: service object-group should be used instead

Guidelines/Limitations to object groups:

- Objects/object groups share same name space
- Object groups must have unique names
- Object group can't be rem/emptied if used in cmd
- ASA doesn't support IPv6 nested object groups

Types of Group Objects

Network	Specifies list of IP/host/subnet/network addr
Service	Used to group TCP/UDP/TCP/UDP ports into an object: • ASA enables creation of service object group that can contain mix of TCP/UDP/ICMP services • +Any protocol: ESP/GRE/TCP
Sec	Can be used in features that support Cisco TrustSec by including: • Group in an extended ACL: In turn: Used in an access rule
ICMP-Type	Uses unique types to send control msgs: RFC 792: • Can group necessary types req to meet org's sec needs • Example: Create object group ECHO to group echo/echo-reply
Usr	Locally created: Imported AD usr groups can be defined for use in features that support ID FW

Config Common Object Groups
object-group network grp-name [global]

- After: Add network objects to network group using **network-object** | **group-object** cmds
- Network object group can't be used to implement NAT: Network object req to implement NAT

Config ICMP object group:
object-group icmp-type grp-name [global]
icmp-object | **group-object** Add ICMP objects to ICMP object group
Config service object group:
object-group service grp-name [global]

- Can define mix of TCP/UDP/ICMP-type services/any protocol

service-object | **group-object**
Config service object group for TCP/UDP/:

- Specify option in **object-group service grp-name** [**tcp** | **udp** | **tcp-udp**]
- When tcp, udp, or tcp-udp is optionally specified on CLI:
  - Service defines standard service object group of TCP/UDP port specifications
  - Example: eq smtp/range 2000 2010
- Add port objects to service group w/**port-object** | **group-object**

clear configure object-group [global] Remove all object groups from config
show running-config object-group Verify group object configs

Network Object group:
ASA(config)# object-group network ADMIN-HOST
ASA(config-network-object-group)# description Administrative hosts
ASA(config-network-object-group)# network-object host 192.168.1.3
ASA(config-network-object-group)# network-object host 192.168.1.4
ASA(config-network-object-group)# exit

ASA(config)# object-group network ALL-HOSTS
ASA(config-network-object-group)# description ALL inside hosts
ASA(config-network-object-group)# network-object 192.168.1.32 255.255.255.240
ASA(config-network-object-group)# group-object ADMIN-HOST
ASA(config-network-object-group)# exit

ASA(config)# show run object-group

ICMP-Type Object Groups:
ASA(config)# object-group icmp-type ICMP-ALLOWED
ASA(config-network-object-group)# icmp-object echo
ASA(config-network-object-group)# icmp-object time-exceeded
ASA(config-network-object-group)# exit

ASA(config)# show running-config object-group id ICMP-ALLOWED

Services Object Groups:
ASA(config)# object-group service SERVICES-1
ASA(config-network-object-group)# service-object tcp destination eq www
ASA(config-network-object-group)# service-object tcp destination eq https
ASA(config-network-object-group)# service-object tcp destination eq pop3
ASA(config-network-object-group)# service-object udp destination eq ntp
ASA(config-network-object-group)# exit

ASA(config)# object-group service SERVICES-2 tcp
ASA(config-network-object-group)# port-object eq www
ASA(config-network-object-group)# port-object eq smtp
ASA(config-network-object-group)# exit

ASA(config)# object-group service SERVICES-3 tcp
ASA(config-network-object-group)# group-object SERVICES-2
ASA(config-network-object-group)# port-object eq ftp
ASA(config-network-object-group)# port-object range 2000 2005
ASA(config-network-object-group)# exit