Cisco ASA Firewall Commands – Cheat Sheet

In this post I have gathered the most useful Cisco ASA Firewall Commands and created a Cheat Sheet list that you can download also as PDF at the end of the article.

I have been working with Cisco firewalls since 2000 where we had the legacy PIX models before the introduction of the ASA 5500 and the newest ASA 5500-X series. The biggest changes in command syntax happened of course at the transition between PIX and ASA models and also after the changes in ASA version 8.3 and later (especially on NAT configuration commands).

From ASA versions 8.3 and later (including 9.x) the command syntax does change a little bit on some commands at every new version update but the majority of core configurations remain the same.

There are hundreds of commands and configuration features of the Cisco ASA firewall. The official Cisco command reference guide for ASA firewalls is more than 1000 pages. Therefore it's not possible to cover the whole commands' range in a single post. For this reason I have selected the most important commands and the ones used most frequently from ASA administrators to set up the firewall appliance.

You can download the commands cheat sheet in PDF format at the end of this post.

Also, if you are interested for Cisco Routers and Switches Commands Cheat Sheet documents, have a look at the links below:

Cisco Switch Commands Cheat Sheet

Cisco Router Commands Cheat Sheet

Most Important Cisco ASA Firewall Commands - Cheat Sheet

Start Configuring the firewall

ciscoasa> enable
Password:

[Enter into "Privileged Mode". This will require to enter the "enable" password]

ciscoasa# configure terminal
ciscoasa(config)#

[Enter into "Global Configuration Mode" to start configuring the device]

Viewing and Saving the configuration

ciscoasa# show running-config

[Show the currently running configuration]

ciscoasa# show startup-config

[Show the configuration which is stored on the device. This is the one which will be loaded if you reboot the firewall]

ciscoasa# copy run start
or
ciscoasa# write memory

[Save the running configuration so it won't be lost if you reboot]

Image Software Management

ciscoasa# copy tftp flash

[Copy image file from TFTP to Flash of ASA]

ciscoasa#config term
ciscoasa(config)# boot system flash:/asa911-k8.bin

[At next reboot, the firewall will use the software image "asa911-k8.bin" from flash]

Passwords and Users

ciscoasa(config)# enable password *Gh4w7$-s39fg#(!*

[You must create a strong "enable" password which gives access to the configuration mode of the device]

ciscoasa(config)#username *ciscoadmin* password *adminpassword* privilege 15

[Create a local user account and assign privilege level 15 which means administrator access]

Change Device Hostname

ciscoasa(config)# hostname DATA-CENTER-FW
DATA-CENTER-FW(config)#

Configure Secure Management Access to the Firewall

ciscoasa(config)# crypto key generate rsa modulus 2048

[Create SSH keys]

ciscoasa(config)#aaa authentication ssh console LOCAL

[The device will authenticate SSH user access from the LOCAL user database]

ciscoasa(config)#username *admin* password *adminpassword* privilege 15

[Create local administrator user]

ciscoasa(config)#ssh 192.168.1.10 255.255.255.255 inside

[Allow SSH access only from host 192.168.1.10 from the "inside" interface]

Interface Configuration and Security Levels

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif DMZ
ciscoasa(config-if)# ip address 192.168.1.2 255.255.255.0
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# no shutdown

The absolutely necessary Interface Sub-commands that you need to configure in order for the interface to pass traffic are the following:

- ***nameif "interface name":*** *Assigns a name to an interface*
- ***ip address "ip_address" "subnet_mask" :*** *Assigns an IP address to the interface*
- ***security-level "number 0 to 100" :*** *Assigns a security level to the interface*
- ***no shutdown :*** *By default all interfaces are shut down, so enable them.*

Static and Default Routes

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 100.1.1.1

[Configure a default route via the "outside" interface with gateway IP of 100.1.1.1]

ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 192.168.1.1

[Configure a static route via the "inside" interface. To reach network 192.168.2.0/24 go via gateway IP 192.168.1.1]

Network Address Translation (NAT)

ciscoasa(config)# object network internal_lan
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface

[Configure PAT for internal LAN (192.168.1.0/24) to access the Internet using the outside interface]

ciscoasa(config)# object network obj_any
ciscoasa(config-network-object)# subnet 0.0.0.0 0.0.0.0
ciscoasa(config-network-object)# nat (any,outside) dynamic interface

[Configure PAT for all ("any") networks to access the Internet using the outside interface]

ciscoasa(config)# object network web_server_static
ciscoasa(config-network-object)# host 192.168.1.1
ciscoasa(config-network-object)# nat (DMZ , outside) static 100.1.1.1

[Configure static NAT. The private IP 192.168.1.1 in DMZ will be mapped statically to public IP 100.1.1.1 in outside zone]

ciscoasa(config)# object network web_server_static
ciscoasa(config-network-object)# host 192.168.1.1
ciscoasa(config-network-object)# nat (DMZ , outside) static 100.1.1.1 service tcp 80 80

[Configure static Port NAT. The private IP 192.168.1.1 in DMZ will be mapped statically to public IP 100.1.1.1 in outside zone only for port 80]

Access Control Lists (ACL)

ciscoasa(config)# access-list OUTSIDE_IN extended permit tcp any host 192.168.1.1 eq 80

[Create an ACL to allow TCP access from "any" source IP to host 192.168.1.1 port 80]

ciscoasa(config)# access-group OUTSIDE_IN in interface outside

[Apply the ACL above at the "outside" interface for traffic coming "in" the interface]

ciscoasa(config)# access-list INSIDE_IN extended deny ip host 192.168.1.1 any
ciscoasa(config)# access-list INSIDE_IN extended permit ip any any
ciscoasa(config)# access-group INSIDE_IN in interface inside

[Create an ACL to deny all traffic from host 192.168.1.1 to any destination and allow everything else. This ACL is then applied at the "inside" interface for traffic coming "in" the interface]

Object Groups

ciscoasa(config)# object-group network WEB_SRV
ciscoasa(config-network)# network-object host 192.168.1.1
ciscoasa(config-network)# network-object host 192.168.1.2

[Create a network group having two hosts (192.168.1.1 and 192.168.1.2). This group can be used in other configuration commands such as ACLs]

ciscoasa(config)# object-group network DMZ_SUBNETS
ciscoasa(config-network)# network-object 10.1.1.0 255.255.255.0
ciscoasa(config-network)# network-object 10.2.2.0 255.255.255.0

[Create a network group having two subnets (10.1.1.0/24 and 10.2.2.0/24). This group can be used in other configuration commands such as ACLs]

ciscoasa(config)# object-group service DMZ_SERVICES tcp
ciscoasa(config-service)# port-object eq http
ciscoasa(config-service)# port-object eq https
ciscoasa(config-service)# port-object range 21 23

[Create a service group having several ports. This group can be used in other configuration commands such as ACLs]

ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp any object-group DMZ_SUBNETS object-group DMZ_SERVICES

[Example of using object groups in ACLs]

Subinterfaces and VLANs

ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# no nameif
ciscoasa(config-if)# no security-level
ciscoasa(config-if)# no ip address
ciscoasa(config-if)# exit

ciscoasa(config)# interface gigabitethernet 0/1.1
ciscoasa(config-subif)# vlan 10
ciscoasa(config-subif)# nameif inside1
ciscoasa(config-subif)# security-level 80
ciscoasa(config-subif)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface gigabitethernet 0/1.2
ciscoasa(config-subif)# vlan 20
ciscoasa(config-subif)# nameif inside2
ciscoasa(config-subif)# security-level 90
ciscoasa(config-subif)# ip address 192.168.2.1 255.255.255.0

[In example above we have a physical interface (GE0/1) which is split into two subinterfaces (GE0/1.1 and GE0/1.2) belonging to two different VLANs with different IPs and security levels]

Clock Settings

ciscoasa# clock set 18:30:00 Aug 10 2016

[Set the time and date]

ciscoasa(config)# clock timezone MST -7

[Set the timezone to MST with -7 hours offset from UTC]

ciscoasa(config)# clock summer-time MST recurring 1 Sunday April 2:00 last Sunday October 2:00

[Set daylight saving time]

Logging Commands

ASA(config)# logging enable
[Enable logging]

ASA(config)# logging timestamp
[Attach timestamp to log messages]

ASA(config)# logging buffer-size 64000
[Set log buffer to 64kB]

ASA(config)# logging buffered warnings
[Send warning log messages to buffer log]

ASA(config)# logging asdm errors
[Send error log messages to ASDM management]

ASA(config)# logging host inside 192.168.1.30
ASA(config)# logging trap errors

[Send error log messages to syslog server 192.168.1.30]

Enable Management Access with ASDM

ASA(config)# asdm image disk0:/asdm-647.bin

[Location of ASDM image on the ASA]

ASA(config)# http server enable

[Enable the http server on the device]

ASA(config)# http 10.10.10.0 255.255.255.0 inside
[Tell the device which IP addresses are allowed to connect with HTTP (ASDM)]

ASA(config)#username admin password *adminpass*
[Configure user/pass to login with ASDM]

DHCP (Assign IP addresses to computers from the ASA device)

ciscoasa(config)# dhcpd address 192.168.1.101-192.168.1.110 inside

[Create a DHCP address pool to assign to clients. This address pool must be on the same subnet as the ASA interface]

ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
[The DNS servers to assign to clients via DHCP]

ciscoasa(config)# dhcpd enable inside
[Enable the DHCP server on the inside interface]

Permit Traffic Between Same Security Levels

ciscoasa(config)# same-security-traffic permit inter-interface

[Permits communication between different interfaces that have the same security level.]

ciscoasa(config)# same-security-traffic permit intra-interface

[Permits traffic to enter and exit the same interface.]

Useful Verification and Troubleshooting Commands

ciscoasa# show access-list OUTSIDE-IN

[Shows hit-counts on ACL with name "OUTSIDE-IN". It shows how many hits each entry has on the ACL]

Sample output:
access-list OUTSIDE-IN line 1 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0 255.255.255.0 eq telnet (hitcnt=15) 0xca10ca21

ciscoasa# show clock

[Verify that time and date are correct on the appliance]

ciscoasa# show conn

[The show conn command displays the number of active TCP and UDP connections, and provides information about connections of various types.]

ciscoasa# show conn all

[Shows all the connections through the appliance]

ciscoasa# show conn state up,http_get,h323,sip

[Shows HTTP GET, H323, and SIP connections that are in the "up" state]

ciscoasa# show conn count

54 in use, 123 most used

[Shows overall connection counts]

ciscoasa# show cpu usage

[show CPU utilization]

ciscoasa# show crypto ipsec sa

[show details about IPSEC VPNs like packets encrypted/decrypted, tunnel peers etc]

ciscoasa# show crypto isakmp sa

[show details if an IPSEC VPN tunnel is up or not. MM_ACTIVE means the tunnel is up]

ciscoasa# show disk

[List the contents of the internal flash disk of the ASA]

ciscoasa# show environment

[Displays operating information about hardware system components such as CPU, fans, power supply, temperature etc]

ciscoasa# show failover

[Displays information about Active/Standby failover status]

ciscoasa# show interface

[Shows information about Interfaces, such as line status, packets received/sent, IP address etc]

ciscoasa# show local-host

[Displays the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the ASA.]

ciscoasa# show memory

[Displays maximum physical memory and current free memory]

ciscoasa# show route

[Displays the routing table]

ciscoasa# show version

[Displays the software version, hardware configuration, license key, and related uptime data]

ciscoasa# show xlate

[Displays information about NAT sessions]