**A picture containing text, screenshot, font, operating system

Description automatically generated**

**ASA – Default configuration and licenses**

**Note: Por default ASA no tiene password y hay que crear una**

Verification commands

1. Show run
2. Show version
3. Show license

**ASA Basic configuration:**

Show run interface

Step 1: hostname and domain name

Configuration terminal

!

Hostname ASA2023

!

Domain-name sageit.com

!

Step 1: Configure interfaces.

Interfaces

* Inside
* Outside
* DMZ
* Management

**int gi0/3**

nameif inside

!security-level 100 - Optional

ip address 10.1.1.1 255.255.255.0

no shut

!

**Int gi0/2**

Nameif outside

ip address 192.1.20.1 255.255.255.0

no shut

!

**Int gi0/0**

Nameif DMZ

security-level 50

ip address 192.168.4.1 255.255.255.0

no shut

!

**Int management0/0**

Nameif mgmt.

security-level 100

ip address 192.3.20.1 255.255.255.0

no shut

Verification Commands

1. Show run interface: Display the running config for an interface
2. Show interface ip brief: Similar to show ip int br
3. Show nameif: Display interfaces, names and security levels

Step 2: Configure PCs

Configure PCs (No Windows)

ifconfig <interface\_name> <ip\_address> netmask <netmask\_address>

password for pcs:cisco/cisco

Management PC

sudo hostname managementPC

sudo ifconfig eth0 192.3.20.2 netmask 255.255.255.0

sudo route add default gw 192.3.20.1 eth0

Outside PC

sudo hostname OutsidePC

sudo ifconfig eth0 10.2.2.2 netmask 255.255.255.0

sudo route add default gw 10.2.2.1 eth0

Inside PCs (Windows)

Username: IEUser

Password: Passw0rd!

Use Ethernet (not Ethernet 2)

IP 10.20.20.2

Default Gateway: 10.20.20.1

sudo hostname InsidePC1

sudo ifconfig eth0 10.20.20.5 netmask 255.255.255.0

sudo route add default gw 10.20.20.1 eth0

sudo hostname InsidePC2

sudo ifconfig eth0 10.20.20.6 netmask 255.255.255.0

sudo route add default gw 10.20.20.1 eth0

Outside Router:

Default route to ASA

ip route 0.0.0.0 0.0.0.0 192.1.20.1

DMZ Router

Default route to ASA

ip route 0.0.0.0 0.0.0.0 192.168.4.1

Step 3: Enable ICMP to the ASA

**Policy-map global policy config: to allow icmp traffic**

Policy-map global\_policy

Class inspection\_default

Inspect icmp

**ASA Management:**

Step 1: Configure Telnet from inside

1. telnet source ip/mask
2. interface
3. password
4. local database (LOCAL is case sensitive)

telnet 10.1.1.0 255.255.255.0 inside

!

Enable password sageit123

!

username admin password cisco123

!

Aaa authentication telnet console LOCAL

!

**Verification:** From Router INSIDE telnet to 10.1.1.1

R\_INSIDE#telnet to 10.1.1.1

On ASA execute the command **who**

Step 4: Configure SSH

Domain-name sageit.com

crypto key generate rsa general-keys modulus 2048

username **testuser** password **testpass**

aaa authentication ssh console LOCAL

ssh version 2

!

ssh 192.3.20.0 255.255.255.0 mgmt

ssh timeout 5

Verification: SSH from Management PC

ssh [testuser@192.3.20.1](mailto:testuser@192.3.20.1)

**Show commands:**

show ssh sessions

show asdm session

Step 5: Configure ASDM

Configure routing between INSIDE Router and ASA

ip route 0.0.0.0 0.0.0.0 10.1.1.1

Configure routing between ASA and INSIDE Router

route inside 10.20.20.0 255.255.255.0 10.1.1.2

http server enable

http 10.20.20.0 255.255.255.0 inside

username asdmuser password cisco123 privilege 15

aaa authentication http console LOCAL

Access to ASDM https://<ASA-Address>/admin

https://10.1.1.1/admin

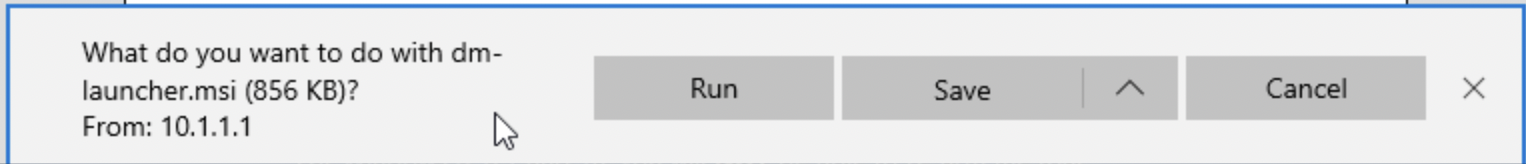
A screenshot of a computer error

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generatedA screenshot of a computer security

Description automatically generated with low confidence



A screenshot of a computer error

Description automatically generated with medium confidenceA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated with medium confidence

A blue sign with white text

Description automatically generated with low confidence

On ASAv on Csslab, we need to specify a route with specific VPN ip, example:

http 10.209.207.234 255.255.255.255 inside

A screenshot of a computer

Description automatically generated

A screenshot of a computer error message

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated

Upload ASDM Image in ASA:

FTP Without password:

Copy ftp flash

10.52.14.227

asdm-7151.bin

FTP with Password (global configuration mode): copy ftp://cisco:cisco@10.52.14.227/asdm-7151.bin flash:/asdm-7151.bin

asdm image flash:asdm-7151.bin

http server enable

http 10.52.14.227 255.255.255.255 inside

username asdmuser password cisco123 privilege 15

aaa authentication http console LOCAL

**ASA NAT:**

*Static NAT*

**DMZ Router**

!

ip route 0.0.0.0 0.0.0.0 192.168.4.1

!

restconf

ip http secure-server

ip http authentication local

username cisco password C1sco123

enable password cisco

!

line vty 0 4

transport input telnet

password cisco

login

!

Verification

**show platform software yang-management process**

**show ip int br**

**OUTSIDE Router**

ip route 192.168.4.0 255.255.255.0 192.1.20.1

**ASA**

Object Network telnet

Host 192.1.20.2

nat (outside,DMZ) static 192.168.4.10

!

Access-list OUT permit tcp any 192.168.4.2 255.255.255.255 eq telnet

!

Access-group OUT in interface outside

!

**Verification: telnet from OUTSIDE Router to DMZ Router**

telnet 192.168.4.2

pwd cisco

**On ASA**

Show nat

Show access-list

***Dynamic NAT***

**On INSIDE Router**

ip route 0.0.0.0 0.0.0.0 10.1.1.1

!

**On DMZ Router**

**!**

ip route 0.0.0.0 0.0.0.0 192.168.4.1

**!**

***ASA***

*!access-list traffic\_in\_DMZ permit icmp any any*

*!access-group traffic\_in\_DMZ in interface inside*

*!*

*object network inside\_nat*

*subnet 10.20.20.0 255.255.255.0*

*exit*

*!*

*object network NAT\_pool*

*range 192.168.4.20 192.168.4.25*

*exit*

*nat (inside,DMZ) source dynamic inside\_nat NAT\_pool*

*!*

**Verification**

**From inside PC ping to DMZ router on 192.168.4.2**

**Show nat**

**Show xlate**

!!!Access-list OUT permit tcp any 192.168.4.2 255.255.255.255 eq www

**Final Configurations:**

**ASA**

ASA2# show run

: Saved

:

: Serial Number: 9A2T29UEPX6

: Hardware: ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz

:

ASA Version 9.16(2)

!

hostname ASA2

domain-name sageit.com

enable password \*\*\*\*\* pbkdf2

service-module 0 keepalive-timeout 4

service-module 0 keepalive-counter 6

names

no mac-address auto

!

interface GigabitEthernet0/0

nameif DMZ

security-level 50

ip address 192.168.4.1 255.255.255.0

!

interface GigabitEthernet0/1

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/2

nameif outside

security-level 0

ip address 192.1.20.1 255.255.255.0

!

interface GigabitEthernet0/3

nameif inside

security-level 100

ip address 10.1.1.1 255.255.255.0

!

interface Management0/0

no management-only

nameif mgmt.

security-level 100

ip address 192.3.20.1 255.255.255.0

!

ftp mode passive

dns server-group DefaultDNS

domain-name sageit.com

object network telnet

host 192.1.20.2

object network inside\_nat

subnet 10.20.20.0 255.255.255.0

object network NAT\_pool

range 192.168.4.20 192.168.4.25

access-list OUT extended permit tcp any host 192.168.4.2 eq telnet

pager lines 23

mtu DMZ 1500

mtu outside 1500

mtu inside 1500

mtu mgmt. 1500

no failover

no failover wait-disable

no monitor-interface service-module

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

arp rate-limit 8192

nat (inside,DMZ) source dynamic inside\_nat NAT\_pool

!

object network telnet

nat (outside,DMZ) static 192.168.4.10

access-group OUT in interface outside

route inside 10.20.20.0 255.255.255.0 10.1.1.2 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

timeout conn-holddown 0:00:15

timeout igp stale-route 0:01:10

user-identity default-domain LOCAL

aaa authentication telnet console LOCAL

aaa authentication ssh console LOCAL

aaa authentication login-history

no snmp-server location

no snmp-server contact

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpoint \_SmartCallHome\_ServerCA

no validation-usage

crl configure

crypto ca trustpoint \_SmartCallHome\_ServerCA2

no validation-usage

crl configure

crypto ca trustpool policy

auto-import

crypto ca certificate chain \_SmartCallHome\_ServerCA

certificate ca 0a0142800000014523c844b500000002

30820560 30820348 a0030201 0202100a 01428000 00014523 c844b500 00000230

0d06092a 864886f7 0d01010b 0500304a 310b3009 06035504 06130255 53311230

10060355 040a1309 4964656e 54727573 74312730 25060355 0403131e 4964656e

54727573 7420436f 6d6d6572 6369616c 20526f6f 74204341 2031301e 170d3134

30313136 31383132 32335a17 0d333430 31313631 38313232 335a304a 310b3009

06035504 06130255 53311230 10060355 040a1309 4964656e 54727573 74312730

25060355 0403131e 4964656e 54727573 7420436f 6d6d6572 6369616c 20526f6f

74204341 20313082 0222300d 06092a86 4886f70d 01010105 00038202 0f003082

020a0282 020100a7 5019de3f 993dd433 46f16f51 6182b2a9 4f8f6789 5d84d953

dd0c28d9 d7f0ffae 95437299 f9b55d7c 8ac142e1 315074d1 810d7ccd 9b21ab43

e2acad5e 866ef309 8a1f5a32 bda2eb94 f9e85c0a ecff98d2 af71b3b4 539f4e87

ef92bcbd ec4f3230 884b175e 57c453c2 f602978d d9622bbf 241f628d dfc3b829

4b49783c 93608822 fc99da36 c8c2a2d4 2c540067 356e73bf 0258f0a4 dde5b0a2

267acae0 36a51916 f5fdb7ef ae3f40f5 6d5a04fd ce34ca24 dc74231b 5d331312

5dc40125 f630dd02 5d9fe0d5 47bdb4eb 1ba1bb49 49d89f5b 02f38ae4 2490e462

4f4fc1af 8b0e7417 a8d17288 6a7a0149 ccb44679 c617b1da 981e0759 fa752185

65dd9056 cefbaba5 609dc49d f952b08b bd87f98f 2b230a23 763bf733 e1c900f3

69f94ba2 e04ebc7e 93398407 f744707e fe075ae5 b1acd118 ccf235e5 494908ca

56c93dfb 0f187d8b 3bc113c2 4d8fc94f 0e37e91f a10e6adf 622ecb35 0651792c

c82538f4 fa4ba789 5c9cd2e3 0d39864a 747cd559 87c23f4e 0c5c52f4 3df75282

f1eaa3ac fd49341a 28f34188 3a13eee8 deff991d 5fbacbe8 1ef2b950 60c031d3

73e5efbe a0ed330b 74be2020 c4676cf0 08037a55 807f464e 96a7f41e 3ee1f6d8

09e13364 2b63d732 5e9ff9c0 7b0f786f 97bc939a f99c1290 787a8087 15d77274

9c557478 b1bae16e 7004ba4f a0ba68c3 7bff31f0 733d3d94 2ab10b41 0ea0fe4d

88656b79 33b4d702 03010001 a3423040 300e0603 551d0f01 01ff0404 03020106

300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414 ed4419c0

d3f0068b eea47bbe 42e72654 c88e3676 300d0609 2a864886 f70d0101 0b050003

82020100 0dae9032 f6a64b7c 44761961 1e2728cd 5e54ef25 bce30890 f929d7ae

6808e194 0058ef2e 2e7e5352 8cb65c07 ea88ba99 8b5094d7 8280df61 090093ad

0d14e6ce c1f23794 78b05f9c b3a273b8 8f059338 cd8d3eb0 b8fbc0cf b1f2ec2d

2d1bccec aa9ab3aa 60821b2d 3bc3843d 578a961e 9c75b8d3 30cd6008 8390d38e

54f14d66 c05d7403 40a3ee85 7ec21f77 9c06e8c1 a7185d52 95edc9dd 259e6dfa

a9eda33a 34d0597b daed50f3 35bfedeb 144d31c7 60f4daf1 879ce248 e2c6c537

fb0610fa 75596631 4729da76 9a1ce982 aeef9ab9 51f78823 9a699562 3ce55580

36d75402 fff1b95d ced4236f d845844a 5b65ef89 0cdd14a7 20cb18a5 25b40df9

01f0a2d2 f400c874 8ea12a48 8e65db13 c4e22517 7debbe87 5b172054 51934a53

030bec5d ca33ed62 fd45c72f 5bdc58a0 8039e6fa d7fe1314 a6ed3d94 4a4274d4

c3775973 cd8f46be 5538effa e89132ea 97580422 de38c3cc bc6dc933 3a6a0a69

3fa0c8ea 728f8c63 8623bd6d 3c969e95 e0494caa a2b92a1b 9c368178 edc3e846

e2265944 751ed975 8951cd10 849d6160 cb5df997 224d8e98 e6e37ff6 5bbbaecd

ca4a816b 5e0bf351 e1742be9 7e27a7d9 99494ef8 a580db25 0f1c6362 8ac93367

6b3c1083 c6addea8 cd168e8d f0073771 9ff2abfc 41f5c18b ec00375d 09e54e80

effab15c 3806a51b 4ae1dc38 2d3cdcab 1f901ad5 4a9ceed1 706cccee f457f818

ba846e87

quit

crypto ca certificate chain \_SmartCallHome\_ServerCA2

certificate ca 0509

308205b7 3082039f a0030201 02020205 09300d06 092a8648 86f70d01 01050500

3045310b 30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164

6973204c 696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f

6f742043 41203230 1e170d30 36313132 34313832 3730305a 170d3331 31313234

31383233 33335a30 45310b30 09060355 04061302 424d3119 30170603 55040a13

1051756f 56616469 73204c69 6d697465 64311b30 19060355 04031312 51756f56

61646973 20526f6f 74204341 20323082 0222300d 06092a86 4886f70d 01010105

00038202 0f003082 020a0282 0201009a 18ca4b94 0d002daf 03298af0 0f81c8ae

4c19851d 089fab29 4485f32f 81ad321e 9046bfa3 86261a1e fe7e1c18 3a5c9c60

172a3a74 8333307d 615411cb edabe0e6 d2a27ef5 6b6f18b7 0a0b2dfd e93eef0a

c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633 e62496f7 3fba5b2b 1c7a35c2

d667feab 66508b6d 28602bef d760c3c7 93bc8d36 91f37ff8 db1113c4 9c7776c1

aeb7026a 817aa945 83e205e6 b956c194 378f4871 6322ec17 6507958a 4bdf8fc6

5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2 e9fe5c98 8cf573af 6bb47ecd

d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c 13f1dedd f6c4f889 3fd175f5

92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03 fd9cbf5b 16ac92db eafe797c

adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53 0c48e60e bdc9b476 0652e611

13857263 0304e004 362b2019 02e874a7 1fb6c956 66f07525 dc67c10e 616088b3

3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1 b222b653 1cdf351d dca1772a

31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f ba2c1515 ea97b3d2 a2b5bef2

8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d 82a44c81 e2a1d1ba 675f9507

a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51 ce506a08 31f991da 0c8f645c

03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc 61dc8b33 77d34432 35096204

921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001 a381b030 81ad300f 0603551d

130101ff 04053003 0101ff30 0b060355 1d0f0404 03020106 301d0603 551d0e04

1604141a 8462bc48 4c332504 d4eed0f6 03c41946 d1946b30 6e060355 1d230467

30658014 1a8462bc 484c3325 04d4eed0 f603c419 46d1946b a149a447 3045310b

30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164 6973204c

696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f 6f742043

41203282 02050930 0d06092a 864886f7 0d010105 05000382 0201003e 0a164d9f

065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026 0c0db547 645df8b4 72c946a5

03182755 89787d76 ea963480 1720dce7 83f88dfc 07b8da5f 4d2e67b2 84fdd944

fc775081 e67cb4c9 0d0b7253 f8760707 4147960c fbe08226 93558cfe 221f6065

7c5fe726 b3f73290 9850d437 7155f692 2178f795 79faf82d 26876656 3077a637

78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d a256d5a7 2fbc561f cf39c1e2

fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a f890d257 a21951a5 2d9741da

074fa950 da908d94 46e13ef0 94fd1000 38f53be8 40e1b46e 561a20cc 6f588ded

2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f d0f8e4c6 39e90488 3cc3baeb

557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1 77680d35 6423acb8 55a103d1

4d4219dc f8755956 a3f9a849 79f8af0e b911a07c b76aed34 d0b62662 381a870c

f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808 3fe95ef9 3507e4c9 626e577f

a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c e1b9825c 5da0c3e9 d848bd19

a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7 ef276208 e291195c d2f121dd

ba174282 97718153 31a99ff6 7d62bf72 e1a3931d cc8a265a 0938d0ce d70d8016

b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0 01506943 9ef4b2ef 6df8ecda

f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5 8210eac2 31cd2e

quit

telnet 10.1.1.0 255.255.255.0 inside

telnet timeout 5

ssh stricthostkeycheck

ssh timeout 5

ssh version 2

ssh key-exchange group dh-group14-sha256

ssh 192.3.0.0 255.255.0.0 mgmt.

ssh 192.3.20.0 255.255.255.0 mgmt.

console timeout 0

console serial

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

dynamic-access-policy-record DfltAccessPolicy

username testuser password \*\*\*\*\* pbkdf2

username admin password \*\*\*\*\* pbkdf2

!

class-map inspection\_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

parameters

message-length maximum client auto

message-length maximum 512

no tcp-inspection

policy-map global\_policy

class inspection\_default

inspect ip-options

inspect netbios

inspect rtsp

inspect sunrpc

inspect tftp

inspect dns preset\_dns\_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect rsh

inspect esmtp

inspect sqlnet

inspect sip

inspect skinny

inspect snmp

inspect icmp

policy-map type inspect dns migrated\_dns\_map\_2

parameters

message-length maximum client auto

message-length maximum 512

no tcp-inspection

policy-map type inspect dns migrated\_dns\_map\_1

parameters

message-length maximum client auto

message-length maximum 512

no tcp-inspection

!

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

call-home

profile CiscoTAC-1

no active

destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService

destination address email callhome@cisco.com

destination transport-method http

subscribe-to-alert-group diagnostic

subscribe-to-alert-group environment

subscribe-to-alert-group inventory periodic monthly

subscribe-to-alert-group configuration periodic monthly

subscribe-to-alert-group telemetry periodic daily

profile License

destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService

destination transport-method http

Cryptochecksum:6622c1a84ca55eeaac817fdc450fe47e

: end

ASA2#

**Inside Router**

**inside#show run**

Building configuration...

Current configuration : 6060 bytes

!

! Last configuration change at 19:43:28 UTC Sat Jun 10 2023

!

version 17.3

service timestamps debug datetime msec

service timestamps log datetime msec

service call-home

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

platform console serial

!

hostname inside

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

!

!

!

!

!

!

!

!

!

!

login on-success log

!

!

!

!

!

!

!

subscriber templating

!

!

!

!

!

!

multilink bundle-name authenticated

!

!

!

!

crypto pki trustpoint SLA-TrustPoint

enrollment pkcs12

revocation-check crl

!

crypto pki trustpoint TP-self-signed-3707587885

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-3707587885

revocation-check none

rsakeypair TP-self-signed-3707587885

!

!

crypto pki certificate chain SLA-TrustPoint

certificate ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030

32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363

6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934

3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305

43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720

526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030

82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D

CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520

1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE

4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC

7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188

68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7

C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191

C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44

DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201

06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85

4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500

03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905

604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B

D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8

467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C

7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B

5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678

80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB

418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0

D697DF7F 28

quit

crypto pki certificate chain TP-self-signed-3707587885

certificate self-signed 01

30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 33373037 35383738 3835301E 170D3233 30363130 31333532

35305A17 0D333330 36303931 33353235 305A3031 312F302D 06035504 03132649

4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37303735

38373838 35308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201

0A028201 0100C325 9C3E1B4B 4BC5D7AA AB7B6D65 DB4E26FC 108CA4D7 E8F981CA

89D65CCE 6FD5D2FD 954E035A B4087DD5 FA04D866 DDC24F54 8410D3BA 36E89ABB

45734C24 943A39B9 4686B34D 074FB057 FB5F0345 43065BC7 36694E99 DD9A10E5

932FFB1A E91E77D5 0D15A825 3C1CD942 BF10D8CF EAEA0338 220ED4C2 6D699BED

84D32D52 DAD3816B CBFDC168 924B6142 0ED070C3 06CF07DA 4DCA0B48 A37E4F48

6DB7F834 E26B215A 75455F56 923EFA1E F61A78E9 8E4C7202 B87B7BE9 F1A6A8CE

5A4EC543 6E5DEE88 466B37CF B149F8F0 DAA18982 C838B28C 6B596EA6 64342703

0E748F5A 3ABCA2BA 49AA1519 A04F68E3 EFD631C8 9F8E524F 529C2518 27B07A78

4DD376A3 BF0D0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF

301F0603 551D2304 18301680 143379CF 85B71200 2E35AF28 CDB97A1B 4AAC26C1

23301D06 03551D0E 04160414 3379CF85 B712002E 35AF28CD B97A1B4A AC26C123

300D0609 2A864886 F70D0101 05050003 82010100 8FFD37C4 46652D33 80522982

A6717D7D 08D5C72E D1DC1C7F 88A3292F 7CAE857E 396CF0F7 FD766D8C 02417D41

E6C1FC06 94AED304 494A4407 3CD76A2E 96E59C67 DC9BD131 7BF495B1 3DA477DB

EE9FF636 F961663C 19FEEE23 5B917245 6CE42C26 DDA4302C 47CC1087 E3FAE08E

C12305CD F806C5AB B7C79F96 45A78FD1 BBDD54CA 9132BD49 C9DA40D6 4C8BEF58

591BE86D 529E61D8 EEB98AE7 D51968D4 76E136C0 013016AB B5AF99FA 166483CA

8E31085D B08B2265 3B034BE6 05888D97 1EB18E47 485BE556 EF7081B2 74F5854E

DDB91DB2 A70BE5F5 46D7061A AFBA864C 9E90A710 3D7C9E51 5AED8E4F ACA8593B

BB11BCF3 FAD40887 7CCBA255 FAC11E77 9D95717A

quit

!

license udi pid CSR1000V sn 9KE8X1VBF4T

diagnostic bootup level minimal

memory free low-watermark processor 71489

!

!

spanning-tree extend system-id

!

!

redundancy

!

!

!

!

!

interface GigabitEthernet1

ip address 10.1.1.2 255.255.255.0

negotiation auto

no mop enabled

no mop sysid

!

interface GigabitEthernet2

ip address 10.20.20.1 255.255.255.0

negotiation auto

no mop enabled

no mop sysid

!

interface GigabitEthernet3

no ip address

shutdown

negotiation auto

no mop enabled

no mop sysid

!

interface GigabitEthernet4

no ip address

shutdown

negotiation auto

no mop enabled

no mop sysid

!

ip forward-protocol nd

no ip http server

ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 10.1.1.1

!

!

!

!

!

!

!

control-plane

!

!

!

!

!

!

line con 0

stopbits 1

line vty 0

login

transport input ssh

line vty 1

login

length 0

transport input ssh

line vty 2 4

login

transport input ssh

!

call-home

! If contact email address in call-home is configured as sch-smart-licensing@cisco.com

! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH notifications.

contact-email-addr sch-smart-licensing@cisco.com

profile "CiscoTAC-1"

active

destination transport-method http

!

!

!

!

!

end

inside#

**Pre-Configuration**

**Configure SSH in ASA**

Domain-name cisco.com

crypto key generate rsa general-keys modulus 2048

username testuser password testpass

aaa authentication ssh console LOCAL

ssh version 2

ssh 10.60.0.0 255.255.0.0 outside

ssh 10.60.0.0 255.255.0.0 dmz

ssh 10.60.0.0 255.255.0.0 inside

ssh timeout 5

Int gi0/0

Nameif outside

ip address 192.168.10.254 255.255.255.0

no shut

int gi0/3

nameif inside

ip address 10.10.10.254 255.255.255.0

no shut

**ACL to allow icmp traffic from PC1 to PC2**

Access-list INOUT extended permit ip host 192.168.10.10 host 10.10.10.10

access-group INOUT in interface outside

ASA Fundamentals – Session 2

**Scenario 1: Static Routes**

**Pre-config**

**ASA:**

**int gi0/3**

nameif inside

#security-level 100 - Optional

ip address 10.1.1.1 255.255.255.0

no shut

!

**Int gi0/2**

Nameif outside

ip address 192.1.20.1 255.255.255.0

no shut

!

**Int gi0/0**

Nameif DMZ

security-level 50

ip address 192.168.4.1 255.255.255.0

no shut

!

**Int management0/0**

Nameif mgmt.

security-level 100

ip address 192.3.20.1 255.255.255.0

no shut

!

Configure PCs

Configure PCs (No Windows)

ifconfig <interface\_name> <ip\_address> netmask <netmask\_address>

password for pcs:cisco/cisco

Management PC

sudo hostname managementPC

sudo ifconfig eth0 192.3.20.2 netmask 255.255.255.0

sudo route add default gw 192.3.20.1 eth0

Outside PC

sudo hostname OutsidePC

sudo ifconfig eth0 10.2.2.2 netmask 255.255.255.0

sudo route add default gw 10.2.2.1 eth0

Inside PCs (Windows)

Username: IEUser

Password: Passw0rd!

Use Ethernet (not Ethernet 2)

IP 10.20.20.2

Default Gateway: 10.20.20.1

sudo hostname InsidePC1

sudo ifconfig eth0 10.20.20.5 netmask 255.255.255.0

sudo route add default gw 10.20.20.1 eth0

sudo hostname InsidePC2

sudo ifconfig eth0 10.20.20.6 netmask 255.255.255.0

sudo route add default gw 10.20.20.1 eth0

**InsideRouter:**

interface GigabitEthernet1

ip address 10.1.1.2 255.255.255.0

no shut

!

**OutsideRouter:**

interface GigabitEthernet1

ip address 192.1.20.2 255.255.255.0

no shut

!

Int Loopback 90

Ip address 10.2.2.2 255.255.255.0

**DMZRouter:**

interface GigabitEthernet1

ip address 192.168.4.2 255.255.255.0

no shut

!

Ip route 0.0.0.0 0.0.0.0 192.168.4.1

!

Step 3: Enable ICMP to the ASA

**Policy-map global policy config: to allow icmp traffic**

Policy-map global\_policy

Class inspection\_default

Inspect icmp

OSPF

ASA

Router ospf 1

router-id 10.10.10.10

network 192.1.20.0 255.255.255.0 area 0

network 192.168.4.0 255.255.255.0 area 0

!

Interface Gig 0/2

ospf authentication message-digest

ospf message-digest-key 1 md5 cisco555

OutsideRouter

Router ospf 1

router-id 2.2.2.2

network 10.2.2.0 0.0.0.255 area 0

network 192.1.20.0 0.0.0.255 area 0

!

Interface Gi1

ip ospf authentication message-digest

ip ospf message-digest-key **1** md5 **cisco555**

verification

ASA

Show ospf neighbor

Router

Show ip ospf neighbor

Test: Ping

RouterDMZ to 10.2.2.2

Failover

A diagram of a computer network

Description automatically generated with low confidence

ASA Failover (A/S):

<https://networkwizkid.com/2017/09/14/cisco-configuring-asav-activestandby-failover/>

<https://www.youtube.com/watch?v=KfwekVfTkJ0>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/general/asa-98-general-config/ha-failover.html#ID-2107-00000429>

PC – Internal

sudo hostname Internal

sudo ifconfig eth0 192.168.2.50 netmask 255.255.255.0

sudo route add default gw 192.168.2.1 eth0

PC – External

sudo hostname External

sudo ifconfig eth0 192.168.1.50 netmask 255.255.255.0

sudo route add default gw 192.168.1.1 eth0

Step 2: Enable ICMP to the ASA

Policy-map global\_policy

Class inspection\_default

Inspect icmp

end

Step 3: Configure Failover on ASAs

**Primary ASA**

Hostname ASA1

!

interface g0/0

nameif outside

ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2

no shut

!

interface g0/3

nameif inside

ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2

no shut

!

Int gi0/1

No shut

!

Int gi0/2

No shut

!

Failover lan unit primary

Failover lan interface FOLINK gi0/1

Failover link STATE Gi0/2

Failover interface ip FOLINK 1.1.1.1 255.255.255.252 standby 1.1.1.2

Failover interface ip STATE 2.2.2.1 255.255.255.252 standby 2.2.2.2

Failover

Prompt hostname state priority

**Secondary ASA**

Hostname ASA2

Failover lan unit secondary

!

Int gi0/1

No shut

!

Int gi0/2

No shut

!

Failover lan unit secondary

Failover lan interface FOLINK gi0/1

Failover link STATE Gi0/2

Failover interface ip FOLINK 1.1.1.1 255.255.255.252 standby 1.1.1.2

Failover interface ip STATE 2.2.2.1 255.255.255.252 standby 2.2.2.2

Failover

Prompt hostname state priority

verification

**Show run int gi0/2**

**Show failover**

**Show failover history**

**!failover active:** Change standby to active node

Step 4: PC Test

From PC internal try Ping 192.168.1.50.

From PC external try to Ping 192.168.2.50 should fail based on security levels

Step 5: Configuring Access list

access-list OUT\_IN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

access-group OUT\_IN in interface outside

Step 6: Failover

Perform test again and shutdown ASA1, failover occurs

Windows Credentials

* User: **IEUser**.
* **Password**: Passw0rd!

route inside 0.0.0.0 0.0.0.0 default\_gateway

ASA Automation

Step 1: Enable basic auth for ASDM

http server basic-auth-client ASDM

Step 2: create username

username cisco password cisco privilege 15

Step 3: Enable HTTP authentication using the local database.

aaa authentication http console LOCAL

Step 4: Enable the HTTP server and allow access from a network.

http server enable

http 0.0.0.0 0.0.0.0 inside or specific ip address

To run CURL: go to cd Desktop/Devnet/scripts

chmod +x ASA.sh

./ASA.sh

#GET ALL CONFIG

#curl -k -A ASDM https://cisco:cisco@10.52.14.140/admin/config

#Execute a command

curl -k -A ASDM https://cisco:cisco@10.52.14.140/admin/exec/show+version

#curl -k -A ASDM https://cisco:cisco@10.52.14.140/admin/exec/show+int+ip+br

A screenshot of a computer

Description automatically generated

List of curl options

<https://gist.github.com/eneko/dc2d8edd9a4b25c5b0725dd123f98b10>

Los router cisco requieren licencia especial para vpn´s? Gracias