**basic router security**

en

conf t

security passwords min-length 10

service password-encryption

enable secret ciscoenapa55

line con 0

password ciscoconpa55

exec-timeout 15 0

login

logging sync

exit

line vty 0 4

password ciscovtypa55

exec-timeout 15 0

login

exit

banner motd cWarning unauthorized access is prohibited!c

----------------------------------------------------------------

**basic switch security**

service password-encryption

enable secret ciscoenapa55

line con 0

password ciscoconpa55

exec-timeout 15 0

login

logging sync

line vty 0 4

password ciscovtypa55

exec-timeout 15 0

login

exit

banner motd cWarning unauthorized access is prohibited!c

int fa/01

switchport mode trunk

switchport trunk native vlan 99

switchport nonegotiate

storm-control broadcast level 50

int fa0/6

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

switchport port-security

switchport port-security mac-address sticky

no shutdown

int range

shutdown

----------------------------------------------------------------

**AAA Local Authentication**

username Admin01 privilege 15 secret Admin01pa55

aaa new-model

aaa authentication login default local enable

line con 0

login authentication default

aaa authentication login <nama> local

line vty 0 4

login authentication <nama AAA>

end

--------------------------

TACACS+

en

conf t

<config username and secret>

Tacacs-server host <server ip>

Tacacs-server key <key>

Aaa new-model

Aaa authentication login default group tacacs+ local

RADIUS

en

conf t

<config username and secret>

radius-server host <ip server>

radius-server key <key>

Aaa new-model

Aaa authentication login default group tacacs+ local

----------------------------------------------------------------

SSH

ip domain-name ccnasecurity.com

ip ssh version 2

line vty 0 4

transport input ssh

----------------------------------------------------------------

**ACL**

ACL Standard Numbered

En

Conf t

Access-list <num> permit <ip address/network addr.> <wildcard>

Line vty 0 4

Access-class 10 in

Int <int>

Ip access-group 120 in/out

ACL Extended Numbered

En

Conf t

Access-list <num> permit/deny

Interface <int>

Ip access-group <num> in/out

IPv6 ACL

Ipv6 access-list <nama>

Deny/permit

Int <int>

Ipv6 traffic-filter <nama> in/out

----------------------------------------------------------------

**Secure Against Login Attacks**

- If a user fails to log in twice within a 30-second time span, then disable logins for one minute

- Log all failed login attempts

login block-for 60 attempts 2 within 30

login on-failure log

----------------------------------------------------------------

**Configure Site-to-Site IPsec VPNs**

R1

conf t

- ACL to identify interesting traffic on R1

- ACL 101 to allow traffic from R1 lo1 network to R3 fa0/1 LAN

- explicitly deny other traffic

access-list 101 permit ip 172.20.1.0 0.0.0.255 172.30.3.0 0.0.0.255

- configure isakmp policy 10 phase 1

- key distribution method: isakmp

- encrypton ase 256

- authentication method: pre-shared

- hash sha-1

- key exchange: DH group 5

- IKE SA lifetime: 3600

- ISAKMP key: ciscovpnpa55 at receiver: on S3 s0/0/1

crypto isakmp policy 10

encryption aes 256

authentication pre-share

hash sha

group 5

lifetime 3600

exit

crypto isakmp key ciscovpnpa55 address 10.20.20.1

- Create the transform set VPN-SET to use esp-aes 256 and esp-sha-hmac.

- Then create the crypto map CMAP that binds all of the Phase 2 parameters together.

- Use sequence number 10 and identify it as an ipsec-isakmp map. - Transform Set: VPN-SET

- Transform Encryption: esp-aes 256

- Transform Authentication: esp-sha-hmac

- set receiver end: on R3 s0/0/1

- Perfect Forward Secrecy (PFS): group5

- Crypto Map name: CMAP

- SA Establishment: ipsec-isakmp

- Bind the crypto map CMAP to the outgoing interface

crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac

crypto map CMAP 10 ipsec-isakmp

set peer 10.20.20.1

set pfs group5

set transform-set VPN-SET

match address 101

exit

interface S0/0/0

crypto map CMAP

end R1 - repeat similar things on the other side (change address and interface)

----------------------------------------------------------------

**Zone-Based Pair Policy (on R3)**

- create zones

zone security IN-ZONE

zone security OUT-ZONE

create an ACL, permit all IP protocols from source network to any destination

access-list 110 permit ip 172.30.3.0 0.0.0.255 any

create a class map, that uses the match-all option and ACL 110

class-map type inspect match-all INTERNAL-CLASS-MAP

match access-group 110

exit

create a policy map, that uses the class map to inspect

policy-map type inspect IN-2-OUT-PMAP

class type inspect INTERNAL-CLASS-MAP

inspect

- create a zone pair, with source and destination

- specify the policy map to be used to inspect traffic between two zones

zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE

service-policy type inspect IN-2-OUT-PMAP

exit

assign interface to the zones

interface fa0/1

zone-member security IN-ZONE

exit

interface s0/0/1

zone-member security OUT-ZONE

exit

----------------------------------------------------------------

**IPS**

- Create a directory in flash named ipsdir and set it as the location for IPS signature storage

- Create an IPS rule named IPS-RULE.

- Retire the all signature category with the retired true command (all signatures within the signature release). o

- Unretire the IOS\_IPS Basic category with the retired false command.

- Apply the rule inbound on the S0/0/1 interface

mkdir ipsdir

conf t

ip ips config location flash:ipsdir

//at this stage, copy paste crypto key file

ip ips name IPS-RULE

ip ips signature-category

category all

retired true

exit

category ios\_ips basic

retired false

exit

exit

<Enter>

interface s0/0/1

ip ips IPS-RULE in

----------------------------------------------------------------

**ASA**

conf t

interface vlan 1

nameif inside

security-level 100

ip address 192.168.10.1 255.255.255.0

exit

interface vlan 2

nameif outside

security-level 0

no ip address dhcp

ip address 209.165.200.234 255.255.255.248

exit

hostname CCNAS-ASA1

domain-name ccnasecurity.com

enable password ciscoenapa55

config AAA on ASA

- Configure AAA to use the local ASA database for Telnet and SSH user authentication

username Admin01 privilege 15 secret Admin01pa55

username admin password adminpa55

aaa authentication ssh console LOCAL

aaa authentication telnet console LOCAL

- Allow Telnet access from the inside 192.168.10.0/24 network with a timeout of 10 minutes.

- Allow SSH access from the outside host 172.30.3.3 with a timeout of 10 minutes

telnet 192.168.10.0 255.255.255.0 inside

telnet timeout 10

ssh 172.30.3.3 255.255.255.255 outside

ssh timeout 10

Configure the ASA as a DHCP server using the following settings: - Assign IP addresses to inside DHCP clients from 192.168.10.5

- Enable DHCP to listen for DHCP client requests

dhcpd address 192.168.10.5-192.168.10.30 inside

dhcpd enable inside

Create a static default route to the next hop router (R1) IP address

route outside 0.0.0.0 0.0.0.0 209.165.200.233

Create a network object named inside-net and assign attributes to it using the subnet and nat commands.

object network inside-net

subnet 192.168.10.0 255.255.255.0

nat (inside,outside) dynamic interface

Create a dynamic NAT translation to the outside interface

nat (inside,outside) dynamic interface

exit

Modify the Cisco Modular Policy Framework (MPF) on the ASA using the following settings:

- Configure class-map inspection\_default to match default-inspection-traffic, and then exit to global configuration mode.

class-map inspection\_default

match default-inspection-traffic

exit

- Configure the policy-map list, global\_policy. Enter the class inspection\_default and enter the command to inspect icmp. Then exit to global config mode.

policy-map global\_policy

class inspection\_default

inspect icmp

exit

- Configure the MPF service-policy to make the global\_policy apply globally

service-policy global\_policy global

----------------------------------------------------------------

**Syslog**

Syslog (Client)

en

conf t

logging <ip addr. of syslog server>

Syslog (Server)

From the **Services** tab of the **Syslog Server**’s dialogue box, select the **Syslog** services button. Observe the logging messages received from the routers.

----------------------------------------------------------------

**NTP**

NTP Client

en

conf t

set ntp server <ip addr>

set ntp client enable

ntp update-calendar

NTP Server

En

Conf t

ntp master

* + - 1. On **PC-A**, click **NTP** under the Services tab to verify NTP service is enabled.
      2. To configure NTP authentication, click **Enable** under Authentication. Use key **1** and password **NTPpa55** for authentication.

NTP Authentication

ntp authenticate

ntp trusted-key <key>

ntp authentication-key <key> md5 <password>

----------------------------------------------------------------

OSPF MD5 Authentication

en

conf t

Router ospf 1

Area 0 authentication message-digest

Int s0/0/0

Ip ospf message-digest-key 1 md5 <password>