Security Parancsok

Security K9 license aktiválása PT-ben, ha a router alapból nem támogatja:

1. go to the global privilege level (enable, config t) and type

```
Router(config)#license boot module c1900 technology-package securityk9

ezt a parancsot néha 2x kell kiadni egymás után...
```

2. and once the IOS will ask for acceptance type Yes

```
ACCEPT? [yes/no]: yes
```

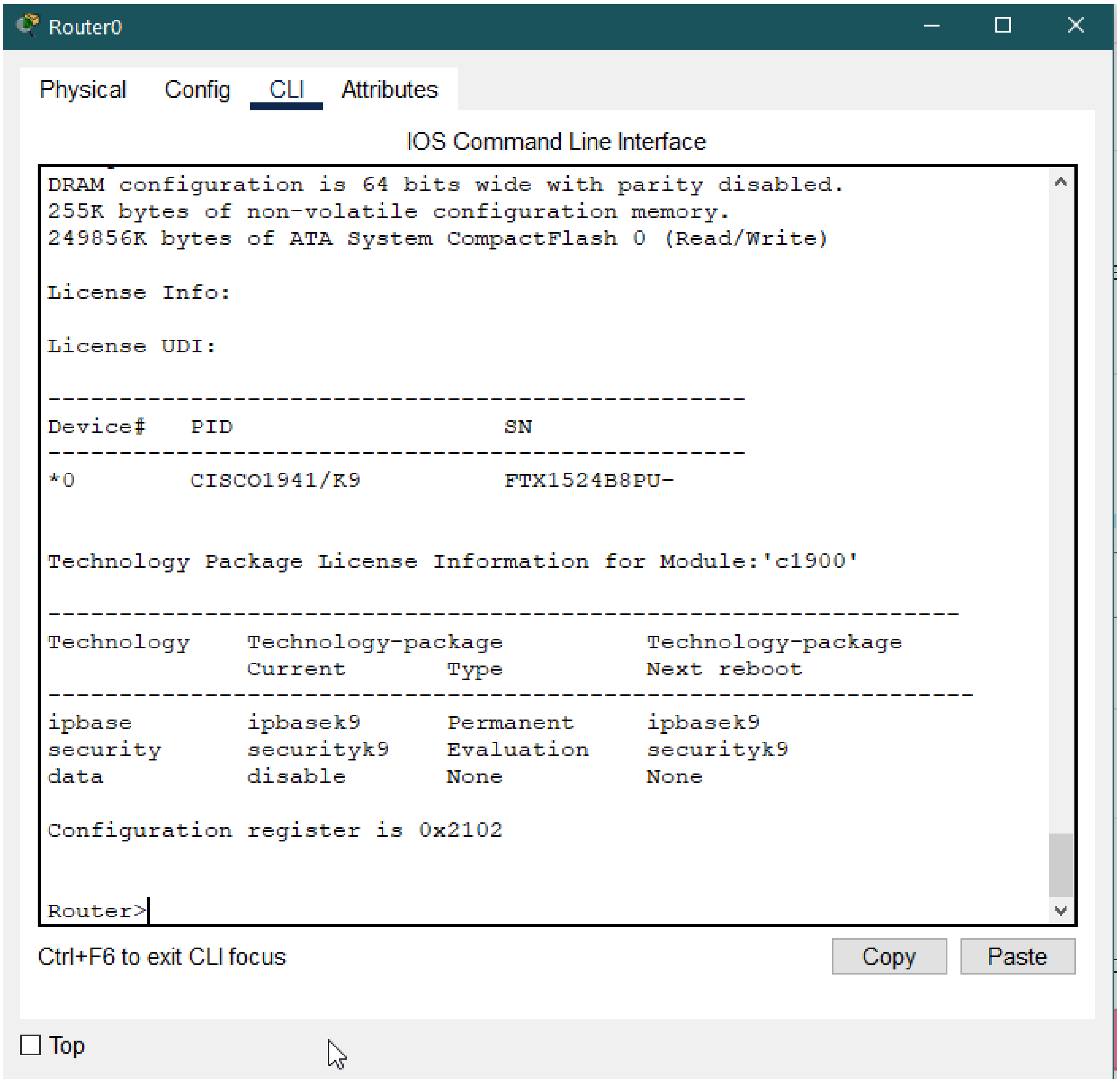
3. then jump to privilege using “End” or Ctrl Z
4. Save the config using

```
Router# Copy run startup
```

5. and reload the router

```
Router# reload
```

6. After reload the Security feature is activated



```
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524B8PU-


Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None

Configuration register is 0x2102


Router>
```

ADMINISTRATIVE ACCESS

```
R1(config)# security passwords min-length 10
R1(config)# enable algorithm-type scrypt secret cisco12345

R1(config)# line console 0
R1(config-line)# password ciscocon
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous

R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# transport input telnet
R1(config-line)# login

R1(config)# service password-encryption

R1(config)# banner motd $Unauthorized access strictly prohibited!$

R1(config)# username user01 algorithm-type scrypt secret user01pass
R1(config)# username admin privilege 15 algorithm-type scrypt secret cisco12345
```

SSH

```
R1(config)# ip domain-name ccnasecurity.com

R1(config)# username admin privilege 15 algorithm-type scrypt secret cisco12345

R1(config)# crypto key zeroize rsa
R1(config)# crypto key generate rsa general-keys modulus 1024
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2


R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Accept only SSH connections:

```
KECSKEMET(config)# line vty 0 4
KECSKEMET(config-line)# transport input ssh
```

PCs attached to FastEthernet interfaces:

```
KECSKEMET(config)# interface FastEthernet0/1
KECSKEMET(config-if)# ip access-group 101 in
KECSKEMET(config)# access-list 101 permit tcp <PC-IP-address> <PC-subnet-mask> any eq 22
KECSKEMET(config)# access-list 101 deny tcp any any eq 22
```

ADMINISTRATIVE ROLES

```
R1(config)#enable secret cisco12345
R1(config)#aaa new-model
```

Belépés “root view”-ba

```
R1# enable view
Password: cisco12345
```

Pl.:

```
R1(config)# parser view admin1
R1(config-view)# secret admin1pass
R1(config-view)# commands exec include all show
R1(config-view)# commands exec include all config terminal
R1(config-view)# commands exec include all debug
R1(config-view)# end
```

Belépés:

```
R1# enable view admin1
Password:  admin1pass
R1# show parser view
Current view is ‘admin1’

R1(config)#parser view alladminok superview
R1(config-view)# view admin1
R1(config-view)# view admin2
```

```
parser view INTERFACE_CONFIG
secret PASSWORD
commands interface
exit

parser view ROUTER_CONFIG
secret PASSWORD
commands router
exit

parser view LINE_CONFIG
secret PASSWORD
commands line vty
exit

username SIMPLE_USER privilege 7 secret PASSWORD
username SUPER_ADMIN privilege 15 secret PASSWORD
```

NTP

Master

```
R2# clock set 20:12:00 Dec 17 2014
R2(config)# ntp authentication-key 1 md5 NTPpassword
R2(config)# ntp trusted-key 1
R2(config)# ntp authenticate
R2(config)# ntp master 3
```

Clients

```
R1(config)# ntp authentication-key 1 md5 NTPpassword
```

```
R1(config)# ntp trusted-key 1
R1(config)# ntp authenticate
R1(config)# ntp server 10.1.1.2
R1(config)# ntp update-calendar

R1# show ntp associations
R1# debug ntp all
```

SYSLOG

(Tftpd32 includes a TFTP server)

```
R1(config)# service timestamps log datetime msec (ajánlott hozzá az ntp server)
R1(config)# logging host 192.168.1.3 (a server IP címe)
```

Severity Level	Keyword	Meaning
0	emergencies	System is unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

```
Pl.:
R1(config)# logging trap warnings    (ebben az esetnem a 0. 1. 2. 3. 4 szintűeket fogja logolni)

R1# show logging
```

OSPF authentication

Plain text

```
R2(config)# interface serial 0/0/1
R2(config-if)# ip ospf authentication
R2(config-if)# ip ospf authentication-key cisco

R3(config)# interface serial 0/0/1
R3(config-if)# ip ospf authentication
R3(config-if)# ip ospf authentication-key cisco
```

MD5

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 cisco

R2(config)# interface serial 0/0/0
R2(config-if)# ip ospf authentication message-digest
R2(config-if)# ip ospf message-digest-key 1 md5 cisco
```

SHA256 Hashing

```
R1(config)# key chain NetAcad
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string CCNASkeystring
R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256
```

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain NetAcad
```

AAA

local

```
R3(config)# aaa new-model
R3(config)# aaa authentication login default local-case none
R3(config)# aaa authentication login TELNET_LINES local
```

```
R3(config)# line vty 0 4
R3(config-line)# login authentication TELNET_LINES
```

verification

```
R3(config)# service timestamps debug datetime msec
R3# debug aaa authentication
```

Server-based

```
R1(config)# aaa new-model
R1(config)# aaa authentication login default group radius none
R1(config)# aaa accounting exec default start-stop group radius
```

```
CEGLED(config)# aaa authentication login TELNET_LINES group radius
local CEGLED(config)# line vty 0 4 CEGLED(config-line)# login
authentication TELNET_LINES
```

```
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.3 auth-port [port] acct-port [port]
R1(config-radius-server)# key radiuspass
```

```
R1(config)# tacacs server SERVER-T
R1(config-radius-server)# address ipv4 192.168.1.3
R1(config-radius-server)# single-connection
R1(config-radius-server)# key tacacspass
```

Régebbi ios-en

```
R1(config)# radius-server host [IP]
R1(config)# radius-server key [pw]
```

```
R1(config)# tacacs-server host [IP] single-connection
R1(config)# tacacs-server key [pw]
```

ZPF

```
R3(config)# zone security INSIDE
R3(config)# zone security INTERNET
```

```
R3(config)# class-map type inspect match-any INSIDE_PROTOCOLS
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp
```

```
R3(config)# policy-map type inspect INSIDE_TO_INTERNET
R3(config-pmap)# class type inspect INSIDE_PROTOCOLS
R3(config-pmap-c)# inspect
```

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET
R3(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET
R3(config)# interface g0/1
R3(config-if)# zone-member security INSIDE
R3(config)# interface s0/0/1
R3(config-if)# zone-member security INTERNET
```

```
R3#show zone-pair security
R3#show policy-map type inspect zone-pair
R3# show zone security
```

L2 security

The default priority for S1 and S2 is 32769 (32768 + 1 with System ID Extension). Set S1 priority to **0** so that it becomes the root switch.

```
S1(config)# spanning-tree vlan 1 priority 0
S1# show spanning-tree
```

Note: You can also use the **spanning-tree vlan 1 root primary** command to make S1 the root switch for VLAN 1.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport nonegotiate

S1#show interfaces f0/1 switchport


S2(config)# interface f0/18
S2(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
S2(config-if)# spanning-tree bpduguard enable
```

Note: PortFast and BPDU guard can also be enabled globally with the **spanning-tree portfast default** and **spanning-tree portfast bpduguard** commands in global configuration mode.

Note: BPDU guard can be enabled on all access ports that have PortFast enabled. These ports should never receive a BPDU. BPDU guard is best deployed on user-facing ports to prevent rogue switch network extensions by an attacker. If a port is enabled with BPDU guard and receives a BPDU, it is disabled and must be manually re-enabled. An **err-disable timeout** can be configured on the port so that it can recover automatically after a specified time period.

```
S1# show spanning-tree interface f0/6 detail
```

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. Having all ports in forwarding state will result in forwarding loops. If a port enabled with loopguard stops hearing BPDUs from the designated port on the segment, it goes into the loop inconsistent state instead of transitioning into forwarding state. Loop inconsistent is basically blocking, and no traffic is forwarded. When the port detects BPDUs again it automatically recovers by moving back into blocking state.

Loop guard should be applied to non-designated ports. Therefore, the global command can be configured on non-root switches.

```
S2(config)# spanning-tree loopguard default
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

```
S2(config-if)# switchport port-security maximum 3
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security aging time 120
```

```
R1(config)# ip dhcp pool CCNAS
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.4
```

Enable DHCP snooping globally.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping information option
```

Enable DHCP snooping for VLAN 1 and 20.

```
S1(config)# ip dhcp snooping vlan 1,20
```

Limit the number of DHCP requests on an interface.

```
S1(config)# interface f0/6
S1(config-if)# ip dhcp snooping limit rate 10
S1(config-if)# exit
```

IPSEC

1.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end

show crypto isakmp policy
```

2.

```
R1(config)# crypto isakmp key cisco123 address 10.2.2.1
```

3.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#exit
```

optional:

```
R1(config)# crypto ipsec security-association lifetime seconds 1800
```

4.

ACL (érdemleges forgalom)

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set peer 10.2.2.1
R1(config-crypto-map)# set pfs group14
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
```

5.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map CMAP
```

ASA

```
ASA-Init(config)# hostname CCNAS-ASA
CCNAS-ASA(config)#domain-name ccnasecurity.com
CCNAS-ASA(config)# passwd cisco
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)# clock set 19:09:00 april 192015

CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100

CCNAS-ASA(config-if)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# no shutdown

CNAS-ASA(config)# interface vlan 3
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# no forward interface vlan 1
CCNAS-ASA(config-if)# nameif dmz
CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# no shut

CCNAS-ASA(config)# interface e0/1
CCNAS-ASA(config-if)#switchport access vlan 1
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)#interface Ethernet0/2
CCNAS-ASA(config-if)#switchport access vlan 3
CCNAS-ASA(config-if)#no shut

CCNAS-ASA(config)# show interface ip brief

CCNAS-ASA(config)# show switch vlan

CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225

CCNAS-ASA# show route
```

NAT

```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA# show nat
```

```
CCNAS-ASA# show xlate
```

Policy

```
CCNAS-ASA# class-map inspection_default
CCNAS-ASA(config-cmap)# match default-inspection-traffic

CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp

CCNAS-ASA(config)# service-policy global_policy global

CCNAS-ASA(config-pmap-c)# show run policy-map
```

DHCP

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
CCNAS-ASA(config)# dhcpd dns 209.165.201.2
```

Note:Other parameters can be specifiedfor clients, such as WINS server, lease length,and domain name.By default,the ASA sets its own IPaddress as the DHCPdefault gateway,so there is no need to configure it. However, to manually configure the default gateway, or set it to a different networking device's IPaddress,use the following command:

```
CCNAS-ASA(config)# dhcpd option 3 ip 192.168.1.1

CCNAS-ASA(config)# dhcpd enable inside
```

AAA - SSH

```
CCNAS-ASA(config)# username admin password cisco12345
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
CCNAS-ASA# write mem

CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)# ssh timeout 10
```

PAT

```
CCNAS-ASA(config)# object network dmz-server
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
```

ACL

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
```

Configure SSH Server on KECSKEMET, BUDAPEST, and SZEGED routers.

a. Configure a privileged user for login from the SSH client:

```
Router(config)# username <username> privilege 15 secret <password>
```

b. Specify privilege level 15 for the VTY lines:

```
Router(config)# line vty 0 15
Router(config-line)# privilege level 15
```

c. Use local user accounts for mandatory login and validation:

```
Router(config)# line vty 0 15
Router(config-line)# login local
Router(config-line)# transport input ssh
```

d. Configure SSH timeouts and authentication retries:

```
Router(config)# ip ssh time-out 60
Router(config)# ip ssh authentication-retries 2
```

Configure AAA using RADIUS server on BP server. On BUDAPEST and CEGLED routers.

a. Configure the authentication service and fallback:

```
Router(config)# aaa authentication login default group radius local
Router(config)# aaa authentication login no_radius none
Router(config)# aaa authorization exec default group radius if-
authenticated
```

b. Create a unique authentication method list for Telnet access on CEGLED router:

```
Router(config)# aaa authentication login TELNET_LINES group radius
local
Router(config)# line vty 0 15
Router(config-line)# login authentication TELNET_LINES
```

Configure Access List on Szeged router:

```
Router(config)# access-list 1 permit icmp any any
Router(config)# access-list 2 permit ip any
<outside_network_subnet_mask>
Router(config)# access-list 3 permit tcp host <PC4_IP> any eq 22
Router(config)# access-list 4 deny ip any any
Router(config)# interface <interface>
Router(config-if)# ip access-group 1 out
Router(config-if)# ip access-group 2 in
Router(config-if)# ip access-group 3 in
Router(config-if)# ip access-group 4 in
```

On Obuda router, configure administrative roles.

a. **Create an interface_config view:**

```
Router(config)# parser view interface_config
Router(config-view)# secret <password>
Router(config-view)# commands configure terminal interface
Router(config-view)# exit
```

b. **Create a router_config view:**

```
Router(config)# parser view router_config
Router(config-view)# secret <password>
Router(config-view)# commands configure terminal router
Router(config-view)# exit
```

c. **Create a line_config view:**

```
Router(config)# parser view line_config
Router(config-view)# secret <password>
Router(config-view)# commands configure terminal line
Router(config-view)# exit
```

d. **Create a simple user with show, debug, and ping commands:**

```
Router(config)# username <username> privilege 3 secret <password>
Router(config)# parser view line_config
Router(config-view)# commands exec include show debug ping
Router(config-view)# exit
```

e. **Create a superadmin with all commands:**

```
Router(config)# username <username> privilege 15 secret <password>
Router(config)# parser view line_config
Router(config-view)# commands all
Router(config-view)# exit
```

Configure BUDAPEST router as a DHCP server and default gateway for VLANs 10 and 20.

a. **Configure DHCP server:**

```
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router <BUDAPEST_router_IP>
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router <BUDAPEST_router_IP>
Router(dhcp-config)# exit
```

b. **Configure BUDAPEST as the DHCP server for PCs connected to CEGLED router:**

```
Router(config)# interface <interface>
Router(config-if)# ip helper-address <BUDAPEST_router_IP>
```

Configure Zone-Based Firewall (ZPF) on KECSKEMET router:

```
Router(config)# zone security inside
Router(config)# zone security outside
Router(config)# zone security dmz
Router(config)# zone-pair security inside-out source inside destination
outside
Router(config-sec-zone-pair)# service-policy type inspect INSIDE-OUT
Router(config)# zone-pair security outside-inside source outside destination
inside
Router(config-sec-zone-pair)# service-policy type inspect OUTSIDE-INSIDE
Router(config)# zone-pair security dmz-outside source dmz destination outside
Router(config-sec-zone-pair)# service-policy type inspect DMZ-OUTSIDE
Router(config)# zone-pair security inside-dmz source inside destination dmz
Router(config-sec-zone-pair)# service-policy type inspect INSIDE-DMZ
Router(config)# zone-pair security dmz-inside source dmz destination inside
Router(config-sec-zone-pair)# service-policy type inspect DMZ-INSIDE
Router(config)# class-map type inspect match-any HTTP
Router(config-cmap)# match protocol http
Router(config)# class-map type inspect match-any ICMP
Router(config-cmap)# match protocol icmp
Router(config)# class-map type inspect match-any SNMP
Router(config-cmap)# match protocol snmp
Router(config)# policy-map type inspect INSIDE-OUT
Router(config-pmap)# class type inspect HTTP
Router(config-pmap-c)# inspect
Router(config)# policy-map type inspect OUTSIDE-INSIDE
Router(config-pmap)# class type inspect HTTP
Router(config-pmap-c)# inspect
Router(config)# policy-map type inspect DMZ-OUTSIDE
Router(config-pmap)# class type inspect HTTP
Router(config-pmap-c)# inspect
Router(config)# policy-map type inspect INSIDE-DMZ
Router(config-pmap)# class type inspect HTTP
Router(config-pmap-c)# inspect
Router(config)# policy-map type inspect DMZ-INSIDE
Router(config-pmap)# class type inspect HTTP
Router(config-pmap-c)# inspect
Router(config)# interface <interface>
Router(config-if)# zone-member security inside
Router(config-if)# zone-member security outside
Router(config-if)# zone-member security dmz
```

Configure Layer 2 security:

a. Configure Basic Switch Settings:

```
Switch(config)# hostname <hostname>
Switch(config)# enable secret <password>
```

b. Configure VLAN 1 management interface on all switches:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address <ip_address> <subnet_mask>
Switch(config-if)# no shutdown
```

c. Configure SSH Server on S0 and S8:

```
Switch(config)# ip domain-name <domain_name>
Switch(config)# ip ssh version 2
Switch(config)# crypto key generate rsa
Switch(config)# line vty 0 15
Switch(config-line)# login local
Switch(config-line)# transport input ssh
```

d. Configure a privileged user for login from the SSH client:

```
Switch(config)# username <username> privilege 15 secret <password>
```

e. Configure S0 as the root switch for VLAN 10, 20, and 30:

```
Switch(config)# spanning-tree vlan 10 root primary
Switch(config)# spanning-tree vlan 20 root primary
Switch(config)# spanning-tree vlan 30 root primary
```

f. Change the native VLAN for trunk ports on S0, S5, and S6:

```
Switch(config)# interface <interface>
Switch(config-if)# switchport trunk native vlan <native_vlan>
```

g. Disable DTP on all switch ports:

```
Switch(config)# interface range <interface_range>
Switch(config-if-range)# switchport nonegotiate
```

h. Protect against STP attack:

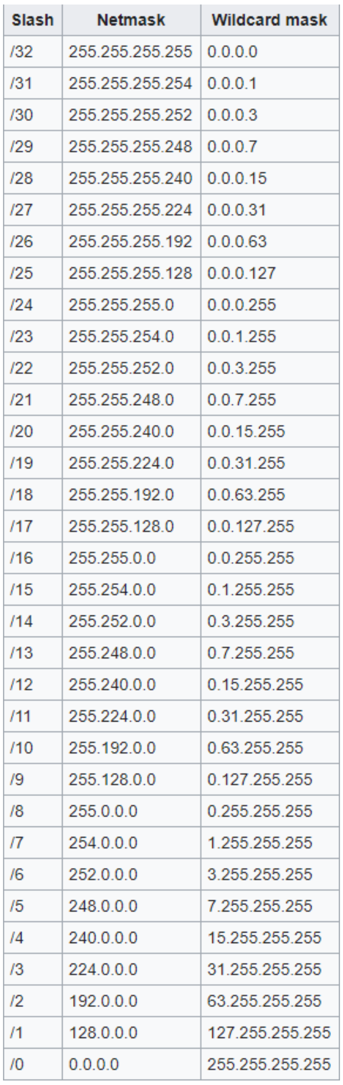
```
Switch(config)# interface range <interface_range>
Switch(config-if-range)# spanning-tree portfast
Switch(config-if-range)# spanning-tree bpduguard enable
```

i. Configure Port Security (1 MAC address, sticky) and Disable Unused Ports:

```
Switch(config)# interface range <interface_range>
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport port-security
Switch(config-if-range)# switchport port-security maximum 1
Switch(config-if-range)# switchport port-security mac-address sticky
Switch(config-if-range)# shutdown
```

j. Configure DHCP snooping:

```
Switch(config)# ip dhcp snooping
Switch(config)# interface <interface>
Switch(config-if)# ip dhcp snooping trust
Switch(config)# ip dhcp snooping limit rate
<limit_rate>
```



Slash	Netmask	Wildcard mask
/32	255.255.255.255	0.0.0.0
/31	255.255.255.254	0.0.0.1
/30	255.255.255.252	0.0.0.3
/29	255.255.255.248	0.0.0.7
/28	255.255.255.240	0.0.0.15
/27	255.255.255.224	0.0.0.31
/26	255.255.255.192	0.0.0.63
/25	255.255.255.128	0.0.0.127
/24	255.255.255.0	0.0.0.255
/23	255.255.254.0	0.0.1.255
/22	255.255.252.0	0.0.3.255
/21	255.255.248.0	0.0.7.255
/20	255.255.240.0	0.0.15.255
/19	255.255.224.0	0.0.31.255
/18	255.255.192.0	0.0.63.255
/17	255.255.128.0	0.0.127.255
/16	255.255.0.0	0.0.255.255
/15	255.254.0.0	0.1.255.255
/14	255.252.0.0	0.3.255.255
/13	255.248.0.0	0.7.255.255
/12	255.240.0.0	0.15.255.255
/11	255.224.0.0	0.31.255.255
/10	255.192.0.0	0.63.255.255
/9	255.128.0.0	0.127.255.255
/8	255.0.0.0	0.255.255.255
/7	254.0.0.0	1.255.255.255
/6	252.0.0.0	3.255.255.255
/5	248.0.0.0	7.255.255.255
/4	240.0.0.0	15.255.255.255
/3	224.0.0.0	31.255.255.255
/2	192.0.0.0	63.255.255.255
/1	128.0.0.0	127.255.255.255
/0	0.0.0.0	255.255.255.255

AAA (Authentication, Authorization, and Accounting):

Configure TACACS+ authorization:

```
Router(config)# aaa authorization exec default group tacacs+ local
Router(config)# aaa authorization commands 15 default group tacacs+ local
```

Enable accounting:

```
Router(config)# aaa accounting exec default start-stop group radius
Router(config)# aaa accounting commands 15 default start-stop group radius
```

Configure RADIUS accounting:

```
Router(config)# radius-server accounting host <RADIUS_server_IP>
Router(config)# radius-server accounting key <RADIUS_secret_key>
```

IPsec (Internet Protocol Security):

Configure IPsec site-to-site VPN:

```
Router(config)# crypto isakmp profile <profile_name>
Router(config-isakmp-profile)# match identity <remote_peer_identity>
Router(config-isakmp-profile)# keyring <keyring_name>
Router(config)# crypto keyring <keyring_name>
Router(config-keyring)# pre-shared-key address <peer_IP> key <pre
shared_key>
```

Configure IPsec remote access VPN:

```
Router(config)# crypto isakmp profile <profile_name>
Router(config-isakmp-profile)# match identity user-fqdn <domain_name>
Router(config-isakmp-profile)# client authentication list
<authentication_list_name>
Router(config)# crypto ipsec client ezvpn <ezvpn_name>
Router(config-ezvpn)# connect <connect_method>
Router(config-ezvpn)# group <group_name> key <group_key>
Router(config-ezvpn)# mode client
Router(config-ezvpn)# peer <peer_IP>
Router(config-ezvpn)# username <username> password <password>
```

Zone-Based Policy Firewall (ZPF):

Define inspection rules for specific protocols:

```
Router(config)# class-map type inspect match-all <class_map_name>
Router(config-cmap)# match protocol <protocol_name>
```

Apply service policy to interfaces:

```
Router(config)# interface <interface>
Router(config-if)# service-policy type inspect <policy_name>
```

ASA (Adaptive Security Appliance):

Enable ASDM access:

```
ASA(config)# http <inside_network_subnet_mask> <inside_network_interface>
ASA(config)# username <username> password <password> privilege
<privilege_level>
ASA(config)# http server enable
ASA(config)# http <management_network_subnet_mask>
<management_network_interface>
```

Configure PAT (Port Address Translation):

```
ASA(config)# object network <inside_network>
ASA(config-network-object)# nat (inside,<outside/dmz>) dynamic interface
```

Configure VPN group policy and tunnel group:

```
ASA(config)# group-policy <group_policy_name> internal
ASA(config-group-policy)# attributes
ASA(config-group-policy)# vpn-tunnel-protocol <protocol>
ASA(config)# tunnel-group <tunnel_group_name> type remote-access
ASA(config)# tunnel-group <tunnel_group_name> general-attributes
ASA(config-tunnel-general)# address-pool <pool_name>
ASA(config)# tunnel-group <tunnel_group_name> ipsec-attributes
ASA(config-tunnel-ipsec)# ikev1 pre-shared-key <pre-shared_key>
```

ACL (Access Control List):

Extended ACL with additional conditions:

```
Router(config)# access-list <acl_number> permit/deny <protocol> <source
_address> <source_wildcard> <destination_address> <destination_wildcard>
<additional_conditions>
```

Extended ACL with port/protocol filtering:

```
Router(config)# access-list <acl_number> permit/deny <protocol>
<source_address> <source_wildcard> eq <source_port> <destination_address>
<destination_wildcard> eq <destination_port>
```