Cheat Sheet

```
show ip ospf neighbour
show ip ospf interface
```

Configure the INSIDE,OUTSIDE abd DMZ interface with the following
IP address 209.165.200.253/28, nameif OUTSIDE, security-level 1, assign to G1/1
IP address 192.168.10.1/24, nameif INSIDE, security-level 100, assign to G1/2
IP address 192.168.20.1/24, nameif DMZ, security-level 70, assign to G1/3'

```
        interface g1/1
        nameif OUTSIDE <name here>
        security-level 1 <level here>
        ip address 209.165.200.253 255.255.255.240
        no shutdown
```

DHCP Service Conf for ASA which gives IP to connected PCs via DHCP

```
        dhcpd address 192.168.10.25-192.168.10.35
INSIDE
        dhcpd dns 192.168.10.10 interface INSIDE
        dhcpd option 3 ip 192.168.10.1 (option
3means default gateway)
        dhcpd enable INSIDE
```

Routing on ASA(Configure a default route)

```
                                  <ip>  <subnet>
        route OUTSIDE 0.0.0.0 0.0.0.0
209.165.200.254
```

Setting up NTP on ASA

```
        ntp authenticate
        ntp authentication-key 1 md5 corpkey<key
here>
        ntp server 192.168.10.10 <server here>
        ntp trusted-key 1
```

SSH on ASA

```
        username user01 password adminpass01
        aaa authentication ssh console LOCAL
        crypto key generate rsa modulus 1024
        yes
        ssh 192.168.10.250 255.255.255.255 INSIDE
// IF ssh from only one ip
        ssh timeout 200
                               // timeout 20 mins
```

NAT service for the ASA

```
        object network (Name of network object)
        subnet ip subnet
        nat (inside,outside) dynamic interface
        can be inside, outside or dmz,outside
depending on where and which network object
        dynamic or statíc. Static is followec by
the ip.
        exit
```

ACL On ASA to implement security policy
Configure a named extended ACL to permit inside hosts to be translated to the pool of outside IP addresses. Name the ACL NAT-IP-ALL.

```
        configure terminal
        access-list NAT-IP-ALL extended permit ip
any any
        access-list <LIST name> extended permit
<protocol>tcp <source>any host
<dest>209.165.200.241 eq 80
```

Apply NAT-IP-ALL ACL to the DMZ and OUTSIDE interfaces in the inward direction.

```
        access-group <ACL name> <in or out>
interface <interface name>
```

. Configure all unused ports in static access mode so that they will not negotiate trunks.

```
        switchport mode access
        switchport nonegotiate
```

# Switch port security

```
        switchport port-security
        switchport port-security maximum 2 <MAX 2
MAC  addresses allowed>
        switchport port-security mac-address sticky
<Sticky means they are remembered>
        switchport port-security violation restrict
        switchport nonegotiate
```

# Implement STP Security

On Switch1, implement STP security measures on the active ports that are connected to hosts.
a. Configure the switch to disable host ports that receive a BPDU.
b. Configure the ports to quickly go into STP forwarding mode without going through the STP transitional modes. Do this on a port-by-port basis, not on the entire switch.
Switch 1

```
        interface range f0/1, f0/5, f0/10, g0/1
        spanning-tree bpduguard enable
        spanning-tree portfast
```

. PortFast is a feature that speeds up the transition of a port from the blocking state to the forwarding state when it is first enabled or when a link comes up. This helps to reduce the time it takes for end devices to become operational on the network and prevents network disruptions.

Site to site vpn between HQ and Branch Routers

a.Configure ACL 120 on the HQ router to identify the interesting traffic to be sent across the VPN. The interesting traffic is all IP traffic from the HQ LAN to the Branch LAN.
HQ ROUTER

```
        access-list 120 permit ip 209.165.200.240
0.0.0.15 198.133.219.32 0.0.0.31
```

b.Configure the ISAKMP Phase 1 properties on the HQ router. The crypto ISAKMP policy is 10. Refer to the ISAKMP Phase 1 Policy Parameters Table for the specific details needed.

```
        crypto isakmp policy 10
        encryption aes 256
        hash sha
        authentication pre-share
        group 2
        lifetime 1800
        exit

        crypto isakmp key Vpnpass101 address
198.133.219.2

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

c.Configure the ISAKMP Phase 2 properties on the HQ router using 10 as the sequence number. Refer to the ISAKMP Phase 2 Policy Parameters Table for the specific details needed.

```
        crypto map VPN-MAP 10 ipsec-isakmp
        match address 120
        set transform-set VPN-SET
        set peer 198.133.219.2
        set pfs group2
        set security-association lifetime seconds
1800
        exit
```

d.Bind the VPN-MAP crypto map to the outgoing interface.

```
        int s0/0/0
        crypto map VPN-MAP
```

e.Configure IPsec parameters on the Branch router using the same parameters as on the HQ router. Note that interesting traffic is defined as the IP traffic from the Branch LAN to the LAN that is attached to HQ.

f.Save the running-config, then reload both the HQ and Branch routers.

```
        end
        copy running-config startup-config
```

Now on BRANCH ROUTER

```
        access-list 120 permit ip 198.133.219.32 0.0.0.31 209.165.200.240 0.0.0.15

        crypto isakmp policy 10
        encryption aes 256
        hash sha
        authentication pre-share
        group 2
        lifetime 1800
        exit

        crypto isakmp key Vpnpass101 address 209.165.200.226

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

        crypto map VPN-MAP 10 ipsec-isakmp
        match address 120
        set transform-set VPN-SET
        set peer 209.165.200.226
        set pfs group2
        set security-association lifetime seconds 1800
        exit

        int s0/0/0
        crypto map VPN-MAP
        end
        copy running-config startup-config
```

HTTP server on ASA

. Configure the ASA to allow HTTPS connections from any host on the INSIDE network (192.168.1.0/24) using the http server enable command in global configuration mode. This allows access to the ASA GUI (ASDM).

```
NETSEC-ASA(config-if)# exit
NETSEC-ASA(config)# http server enable
NETSEC-ASA(config)# http 192.168.1.0 255.255.255.0 INSIDE
```

R1 basic conf

```
        security passwords min-length 10
        enable secret algorithm-type scrypt cisco12345
        username admin01 algorithm-type scrypt secret cisco12345
        crypto key generate rsa general-keys modulus 1024
        ip http server // not needed
        line con 0
        exec-timeout 5 0
        logging synchronous
        login local
        line vty 0 4
        exec-timeout 5 0
        login local
        transport input ssh
        end
```

Site to Síte VPN (ROUTERs)

Conf as normal then enable router ospf

On R1, use the following commands:

```
        R1(config)# router ospf 101
        R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
        R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

b. On R2, use the following commands:

```
        R2(config)# router ospf 101
        R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
        R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

c. On R3, use the following commands:

```
        R3(config)# router ospf 101
        R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
        R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

1. Enable isakmp by installing security9k and reloading router if req

```
        R1(config)# crypto isakmp enable
```

2. Configure IKE Phase 1 ISAKMP policy on R1 and R3

```
        R1(config)# crypto isakmp policy 10
        R1(config-isakmp)# hash sha
        R1(config-isakmp)# authentication pre-share
        R1(config-isakmp)# group 24
        R1(config-isakmp)# lifetime 3600
        R1(config-isakmp)# encryption aes 256
        R1(config-isakmp)# end
```

3. Configure pre shared keys

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

Configure the same policy on R3. Add address of R1 on R3 conf

4. Cónfigure the IPsec transform set and lifetime

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

and on R3 as well

5. Define interesting traffic on R1 and R3

```
        R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

6. Create and apply a crypto map

```
        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 group24
        R1(config-crypto-map)# set transform-set R1-R3
        R1(config-crypto-map)# set security-association lifetime seconds 900
        R1(config-crypto-map)# exit
```

Similarly on R3 then with changed ip

7. Finally apply the map to interface.

```
        R1(config)# interface G0/0/0
        R1(config-if)# crypto map CMAP
```