Cheat Sheet for comprehensive Cisco Certified Network Professional (CCNP) - Security

Network Security Fundamentals

Security Threats and Vulnerabilities

- **Common Threats**: Malware, Phishing, DDoS, Man-in-the-Middle (MitM)

- **Vulnerabilities**: Software bugs, misconfigurations, weak passwords

Security Policies and Procedures

- **Zero Trust Model**: Assume breach, verify explicitly, least privilege

- **Access Control**: Role-based access control (RBAC), mandatory access control (MAC)

Firewalls and Intrusion Prevention Systems (IPS)

Firewall Configuration

- **Types**: Packet filtering, stateful inspection, next-gen firewalls (NGFW)

- **Basic Commands**:

```
conf t
access-list 101 permit tcp any any eq 80
access-list 101 deny ip any any
```

- **Zone-Based Policy Firewall (ZBF)**:

```
zone security IN
zone security OUT
policy-map type inspect IN_TO_OUT
class type inspect IN_TO_OUT_CLASS
inspect
```

Intrusion Prevention Systems (IPS)

- **Signature-Based Detection**: Pre-defined patterns of known attacks

- **Anomaly-Based Detection**: Behavioral analysis to detect deviations

- **Configuration**:

```
ip ips name IPS_POLICY
ip ips IPS_POLICY in
```

VPN and Remote Access

Site-to-Site VPN

- **IPsec Configuration**:

```
crypto isakmp policy 10
encryption aes
hash sha
group 2
lifetime 86400
crypto ipsec transform-set MY_SET esp-aes esp-sha-hmac
crypto map MY_MAP 10 ipsec-isakmp
set peer 192.168.1.1
set transform-set MY_SET
match address 101
```

Remote Access VPN

- **AnyConnect Configuration**:

```
webvpn
enable outside
tunnel-group-list enable
group-policy GROUP_POLICY internal
group-policy GROUP_POLICY attributes
vpn-tunnel-protocol ssl-client
```

Secure Routing and Switching

Secure Routing

- **Router Hardening**:

```
no ip source-route
no ip proxy-arp
service password-encryption
```

- **Secure Management**:

```
line vty 0 4
login local
transport input ssh
```

Secure Switching

- **Port Security**:

```
interface GigabitEthernet0/1
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
```

- **VLAN Security**:

```
vlan 10
name SECURE_VLAN
interface range GigabitEthernet0/1 - 4
switchport mode access
switchport access vlan 10
```

Identity and Access Management

AAA Configuration

- **RADIUS/TACACS+**:

```
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 192.168.1.2 key SECRET
```

Identity Services Engine (ISE)

- **Roles and Permissions**:

```
create authorization profile ALLOW_SSH
match condition User-Role == "Admin"
action permit
```

- **Posture Assessment**:

```
create posture policy ANTIVIRUS_CHECK
match condition Endpoint-Antivirus == "Compliant"
action permit
```

Secure Wireless Networking

Wireless Security Protocols

- **WPA2/WPA3**: AES encryption, 802.11i standard
- **WPA Enterprise**: RADIUS authentication

Wireless Controller Configuration

- **Basic Setup**:

```
wlan name SECURE_WLAN
ssid SECURE_SSID
security wpa wpa2
key-management wpa-enterprise
```

- **Guest Access**:

```
wlan name GUEST_WLAN
ssid GUEST_SSID
security wpa wpa2
key-management wpa-personal
```

Security Monitoring and Logging

Syslog Configuration

- **Remote Logging**:

```
logging host 192.168.1.3
logging trap debugging
```

- **Log Levels**:

```
logging console 7
logging monitor 5
```

NetFlow and IP SLA

- **NetFlow Configuration**:

```
interface GigabitEthernet0/1
ip flow ingress
ip flow egress
```

- **IP SLA Configuration**:

```
ip sla 1
icmp-echo 192.168.1.1
frequency 60
ip sla schedule 1 life forever start-time now
```

Advanced Security Topics

Network Address Translation (NAT)

- **Static NAT**:

```
ip nat inside source static 192.168.1.10 203.0.113.10
```

- **Dynamic NAT**:

```
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool POOL 203.0.113.10 203.0.113.20 netmask 255.255.255.0
ip nat inside source list 1 pool POOL
```

IPv6 Security

- **Basic Configuration**:

```
ipv6 unicast-routing
interface GigabitEthernet0/1
ipv6 address 2001:db8::1/64
```

- **Access Control**:

```
ipv6 access-list ACL6
permit tcp any any eq 80
deny ipv6 any any
```

Troubleshooting and Best Practices

Common Issues

- **Firewall Rules**: Check ACLs and ZBF policies

- **VPN Connectivity**: Verify IPsec tunnels and certificates

- **AAA Failures**: Ensure RADIUS/TACACS+ servers are reachable

Best Practices

- **Regular Updates**: Apply patches and updates promptly

- **Monitoring**: Use tools like Cisco Stealthwatch for continuous monitoring

- **Documentation**: Maintain detailed network diagrams and configuration backups

Useful Commands and Shortcuts

General Commands

- **Show Running Config**: `show running-config`

- **Show Interfaces**: `show interfaces`

- **Show IP Routing**: `show ip route`

Security-Specific Commands

- **Show Access Lists**: `show access-lists`

- **Show IPS Signatures**: `show ip ips signature`

- **Show VPN Sessions**: `show vpn-sessiondb`

Examples and Use Cases

Example: Secure Remote Access

1. **Configure VPN**:

   ```
   crypto isakmp policy 10
   encryption aes
   hash sha
   group 2
   lifetime 86400
   ```

2. **Set Transform Set**:

   ```
   crypto ipsec transform-set MY_SET esp-aes esp-sha-hmac
   ```

3. **Apply Crypto Map**:

```
crypto map MY_MAP 10 ipsec-isakmp
set peer 192.168.1.1
set transform-set MY_SET
match address 101
```

Example: AAA with RADIUS

1. **Enable AAA**:

```
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local
```

2. **Configure RADIUS Server**:

```
radius-server host 192.168.1.2 key SECRET
```

Conclusion

This cheat sheet provides a comprehensive overview of essential concepts, configurations, and commands for CCNP Security. Use these tips and tricks to secure your network effectively.

By Ahmed Baheeg Khorshid

ver 1.0