Cheat Sheet for comprehensive Cisco Certified Internetwork Expert (CCIE) - Security

Network Security Fundamentals

- **Security Principles**
  - **CIA Triad**: Confidentiality, Integrity, Availability
  - **AAA**: Authentication, Authorization, Accounting
  - **Defense in Depth**: Multiple layers of security controls
- **Common Threats**
  - **Malware**: Viruses, Worms, Trojans, Ransomware
  - **Phishing**: Deceptive emails or websites
  - **DDoS**: Distributed Denial of Service attacks
  - **Man-in-the-Middle (MitM)**: Intercepting communication

Cisco Security Devices

- **ASA (Adaptive Security Appliance)**
  - **Modes**: Router, Transparent, Multi-context
  - **Interfaces**: Inside, Outside, DMZ
  - **Basic Commands**

- `show running-config`
- `show version`
- `show interface`
- `show access-list`

- **Firepower (Next-Generation Firewall)**
  - **Components**: FMC (Firepower Management Center), FTD (Firepower Threat Defense)
  - **Basic Commands**

- `show running-config`
- `show inventory`
- `show interface`

- `show policy`

- **ISE (Identity Services Engine)**

  - **Roles**: Policy Service Node, Monitoring & Troubleshooting Node

  - **Basic Commands**

- `show identity-policies`
- `show endpoint`
- `show user-session`

Access Control Lists (ACLs)

- **Types**

  - **Standard ACL**: Filters based on source IP

  - **Extended ACL**: Filters based on source/destination IP, protocol, port

- **Configuration**

  - **Standard ACL**

```
    access-list 1 permit 192.168.1.0 0.0.0.255
```

  - **Extended ACL**

```
    access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 10.0.0.1 eq
80
```

- **Application**

  - **Interface**

```
    interface GigabitEthernet0/1
    ip access-group 101 in
```

VPN Technologies

- **Site-to-Site VPN**

  - **Protocols**: IPSec, IKEv1/IKEv2

  - **Configuration**

```
crypto isakmp policy 10
encryption aes
hash sha
authentication pre-share
group 2
lifetime 86400
```

- **Remote Access VPN**
  - **Protocols**: SSL/TLS, AnyConnect
  - **Configuration**

```
vpn-sessiondb logon
username admin password cisco123
```

Intrusion Prevention System (IPS)

- **Deployment Modes**
  - **Inline**: Traffic passes through the IPS device
  - **Passive**: IPS monitors traffic without affecting it
- **Configuration**
  - **Policy Creation**

```
policy-map type inspect ips_policy
class type inspect ips_class
```

- **Monitoring**
  - **Commands**

```
show policy-map type inspect
show running-config | include ips
```

Secure Routing Protocols

- **OSPF with Authentication**
  - **MD5 Authentication**

```
    router ospf 1
    area 0 authentication message-digest
    interface GigabitEthernet0/1
    ip ospf message-digest-key 1 md5 cisco
```

- **EIGRP with Authentication**
  - **MD5 Authentication**

```
    router eigrp 1
    key chain eigrp_auth
    key 1
    key-string cisco
    interface GigabitEthernet0/1
    ip authentication mode eigrp 1 md5
    ip authentication key-chain eigrp 1 eigrp_auth
```

Secure Management

- **SSH Configuration**
  - **Basic Setup**

```
    hostname R1
    ip domain-name cisco.com
    crypto key generate rsa
    username admin privilege 15 secret cisco123
    line vty 0 4
    login local
    transport input ssh
```

- **SNMPv3 Configuration**
  - **Basic Setup**

```
    snmp-server view myview iso included
    snmp-server group mygroup v3 priv read myview
    snmp-server user admin mygroup v3 auth sha cisco123 priv aes 128
cisco123
```

Logging and Monitoring

- **Syslog Configuration**

- **Basic Setup**

```
logging 10.0.0.1
logging trap informational
logging source-interface GigabitEthernet0/1
```

- **NetFlow Configuration**
  - **Basic Setup**

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

Security Best Practices

- **Regular Updates**
  - **Software Patches**: Regularly update firmware and software
  - **Security Advisories**: Monitor Cisco security advisories
- **Strong Passwords**
  - **Complexity**: Use a mix of characters, numbers, and symbols
  - **Rotation**: Change passwords periodically
- **Network Segmentation**
  - **VLANs**: Use VLANs to segment network traffic
  - **Firewall Rules**: Apply strict firewall rules between segments

Troubleshooting Tools

- **Packet Capture**
  - **Commands**

```
packet-capture input interface GigabitEthernet0/1
```

- **Debugging**
  - **Commands**

```
debug ip packet
debug crypto isakmp
```

Example Scenarios

- **Scenario 1: Configuring a Site-to-Site VPN**

  - **Steps**

1. Configure ISAKMP policy

2. Configure IPSec transform set

3. Configure crypto map

4. Apply crypto map to interface

- **Scenario 2: Setting Up SSH on a Router**

  - **Steps**

1. Generate RSA key

2. Configure local user

3. Enable SSH on VTY lines

Useful Resources

- **Cisco Documentation**

- [Cisco Security Documentation](https://www.cisco.com/c/en/us/support/security/index.html)

- **Community Forums**

- [Cisco Community](https://community.cisco.com/)

- **Training Platforms**

- [Cisco Learning Network](https://learningnetwork.cisco.com/)

Tips and Tricks

- **Backup Configuration**

  - **Commands**

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

- **Restore Configuration**

  - **Commands**

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

- **Quick Access to Help**

  - **Commands**

```
?
```

- **Save Time with Abbreviations**

  - **Examples**

- `sh run` instead of `show running-config`
- `int gi0/1` instead of `interface GigabitEthernet0/1`

Conclusion

- **Continuous Learning**

- Stay updated with the latest security trends and technologies
- Practice regularly to maintain proficiency

- **Hands-On Experience**

- Use labs and simulations to reinforce theoretical knowledge
- Participate in CCIE Security lab exams to validate skills

By Ahmed Baheeg Khorshid

ver 1.0