3. CCNP Security

INTRODUCCIÓN:

Este temario se está basado en un diplomado de 120 horas y los temas mencionados en este documento se han basado en las guías de estudio oficiales de Cisco. Para este curso se han tomado en cuenta los temarios de los siguientes exámenes:

- Implementing and Operating Cisco Security Core Technologies (300-701) Examen core
- Implementing Secure Solutions with Virtual Private Networks (300-730) Examen de especialización
- Securing Networks with Cisco Firepower (300-710) Examen de especialización

Cabe señalar que estos temarios se han juntado y se darán los temas intercalados, ya que se tienen muchas similitudes en los temas.

OBJETIVO:

El presente documento tiene como objetivo plantear un temario para el diplomado orientado a la certificación CCNP Security con la especialización de implementación de soluciones seguras con redes privadas virtuales y aseguramiento en redes con cisco firepower.

ALCANCE:

El Curso de Certificación CCNP Security (120 hrs) brinda al estudiante el conocimiento suficiente donde podrá desarrollar: 1) políticas de seguridad coherente para afrontar las amenazas contra la seguridad en la infraestructura, 2) configurar routers en el perímetro de la red, con las funcionalidades aportadas por Cisco IOS Security, 3) configurar un firewall de Cisco IOS para realizar tareas de seguridad básicas en la red, 4) configurar VPNs site-to-site, acceso remoto y SSL usando las características de Cisco IOS, 5) configurar IPS (IntrusionPrevention System) en routers Cisco, 6) configurar dispositivos de LAN para controlar el acceso, resistir ataques, y defender a otros dispositivos de la red y del sistema mediante la interfaz gráfica, 7) además el estudiante aprenderá a configurar el CISCO Adaptive Security Appliance.

TEMARIO:

1.0 Security Concepts

1.1 Explain common threats against on-premises and cloud environments

1.1.a On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware

1.1.b Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials

1.2 Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery

1.3 Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key and certificate-based authorization

1.4 Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN including high availability considerations, and AnyConnect

1.5 Describe security intelligence authoring, sharing, and consumption

1.6 Explain the role of the endpoint in protecting humans from phishing and social engineering attacks

1.7 Explain North Bound and South Bound APIs in the SDN architecture

1.8 Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting

1.9 Interpret basic Python scripts used to call Cisco Security appliances APIs

2.0 Network Security

2.1 Compare network security solutions that provide intrusion prevention and firewall capabilities

2.2 Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities

2.3 Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records

2.4 Configure and verify network infrastructure security methods (router, switch, wireless)

- 2.4.a Layer 2 methods (Network segmentation using VLANs and VRF-lite; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; PVLANs to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
- 2.4.b Device hardening of network infrastructure security devices (control plane, data plane, management plane, and routing protocol security)

2.5 Implement segmentation, access control policies, AVC, URL filtering, and malware protection

2.6 Implement management options for network security solutions such as intrusion prevention and perimeter security (Single vs. multidevice manager, in-band vs. out-ofband, CDP, DNS, SCP, SFTP, and DHCP security and risks)

2.7 Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)

2.8 Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, and encryption, secure logging, and NTP with authentication)

2.9 Configure and verify site-to-site VPN and remote access VPN

- 2.9.a Site-to-site VPN utilizing Cisco routers and IOS
- 2.9.b Remote access VPN using Cisco AnyConnect Secure Mobility client
- 2.9.c Debug commands to view IPsec tunnel establishment and troubleshooting

3.0 Securing the Cloud

3.1 Identify security solutions for cloud environments

3.1.a Public, private, hybrid, and community clouds

3.1.b Cloud service models: SaaS, PaaS, IaaS (NIST 800-145)

3.2 Compare the customer vs. provider security responsibility for the different cloud service models

3.2.a Patch management in the cloud

3.2.b Security assessment in the cloud

3.2.c Cloud-delivered security solutions such as firewall, management, proxy, security intelligence, and CASB

3.3 Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and security

3.4 Implement application and data security in cloud environments

3.5 Identify security capabilities, deployment models, and policy management to secure the cloud

3.6 Configure cloud logging and monitoring methodologies

3.7 Describe application and workload security concepts

4.0 Content Security

4.1 Implement traffic redirection and capture methods

4.2 Describe web proxy identity and authentication including transparent user identification

4.3 Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA)

4.4 Configure and verify web and email security deployment methods to protect on premises and remote users (inbound and outbound controls and policy management)

4.5 Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption

4.6 Configure and verify secure internet gateway and web security features such as blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption

4.7 Describe the components, capabilities, and benefits of Cisco Umbrella

4.8 Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)

5.0 Endpoint Protection and Detection

5.1 Compare Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions

5.2 Explain antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry

5.3 Configure and verify outbreak control and quarantines to limit infection

5.4 Describe justifications for endpoint-based security

5.5 Describe the value of endpoint device management and asset inventory such as MDM

5.6 Describe the uses and importance of a multifactor authentication (MFA) strategy

5.7 Describe endpoint posture assessment solutions to ensure endpoint security

5.8 Explain the importance of an endpoint patching strategy

6.0 Secure Network Access, Visibility, and Enforcement

6.1 Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD

6.2 Configure and verify network access device functionality such as 802.1X, MAB, WebAuth

6.3 Describe network access with CoA

6.4 Describe the benefits of device compliance and application control

6.5 Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP)

6.6 Describe the benefits of network telemetry

6.7 Describe the components, capabilities, and benefits of these security products and solutions

6.7.a Cisco Stealthwatch

6.7.b Cisco Stealthwatch Cloud

6.7.c Cisco pxGrid

6.7.d Cisco Umbrella Investigate

6.7.e Cisco Cognitive Threat Analytics

6.7.f Cisco Encrypted Traffic Analytics

6.7.g Cisco AnyConnect Network Visibility Module (NVM)

7.0 Site-to-site Virtual Private Networks on Routers and Firewalls

7.1 Describe GETVPN

7.2 Implement DMVPN (hub-and-spoke and spoke-to-spoke on both IPv4 & IPv6)

7.3 Implement FlexVPN (hub-and-spoke on both IPv4 & IPv6) using local AAA

8.0 Remote access VPNs

8.1 Implement AnyConnect IKEv2 VPNs on ASA and routers

8.2 Implement AnyConnect SSLVPN on ASA and routers

8.3 Implement Clientless SSLVPN on ASA and routers

8.4 Implement Flex VPN on routers

9.0 Troubleshooting using ASDM and CLI

9.1 Troubleshoot IPsec

9.2 Troubleshoot DMVPN

9.3 Troubleshoot FlexVPN

9.4 Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers

9.5 Troubleshoot Clientless SSLVPN on ASA and routers

10.0 Secure Communications Architectures

10.1 Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions

10.2 Identify functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions

10.3 Identify VPN technology based on configuration output for site-to-site VPN solutions

10.4 Identify VPN technology based on configuration output for remote access VPN solutions

10.5 Identify split tunneling requirements for remote access VPN solutions

10.6 Design site-to-site VPN solutions

10.6.a VPN technology considerations based on functional requirements

10.6.b High availability considerations.

10.7 Design remote access VPN solutions

10.7.a VPN technology considerations based on functional requirements

10.7.b High availability considerations

10.7.c Clientless SSL browser and client considerations and requirements

10.8 Identify Elliptic Curve Cryptography (ECC) algorithms

11.0 Deployment

11.1 Implement NGFW modes

11.1.a Routed mode

11.1.b Transparent mode

11.2 Implement NGIPS modes

11.2.a Passive

11.2.b Inline

11.3 Implement high availability options

11.3.a Link redundancy

11.3.b Active/standby failover

11.3.c Multi-instance

11.4 Describe IRB configurations

12.0 Configuration

12.1 Configure system settings in Cisco Firepower Management Center

12.2 Configure these policies in Cisco Firepower Management Center

- 12.2.a Access control
- 12.2.b Intrusion
- 12.2.c Malware and file
- 12.2.d DNS
- 12.2.e Identity
- 12.2.f SSL
- 12.2.g Prefilter

12.3 Configure these features using Cisco Firepower Management Center

- 12.3.a Network discovery
- 12.3.b Application detectors (Open AppID)
- 12.3.c Correlation
- 12.3.d Actions

12.4 Configure objects using Firepower Management Center

- 12.4.a Object Management
- 12.4.b Intrusion Rules

12.5 Configure devices using Firepower Management Center

- 12.5.a Device Management
- 12.5.b NAT
- 12.5.c VPN
- 12.5.d QoS
- 12.5.e Platform Settings
- 12.5.f Certificates

13.0 Management and Troubleshooting

13.1 Troubleshoot with FMC CLI and GUI

13.2 Configure dashboards and reporting in FMC

13.3 Troubleshoot using packet capture procedures

14.0 Integration

14.1 Configure Cisco AMP for Networks in Firepower Management Center

14.2 Configure Cisco AMP for Endpoints in Firepower Management Center

14.3 Implement Threat Intelligence Director for third-party security intelligence feeds

14.4 Describe using Cisco Threat Response for security investigations

14.5 Describe Cisco FMC PxGrid Integration with Cisco Identify Services Engine (ISE)

14.6 Describe Rapid Threat Containment (RTC) functionality within Firepower Management Center