Exam topic

1. **Security concepts**: no lab
2. **Endpoint Protection and detection**: Configure and verify outbreak control and quarantines to limit infection
3. **Securing the cloud:** Configure cloud logging and monitoring methodologies
4. **Secure Network Access, Visibility, and Enforcement**: Configure and verify network access device functionality such as 802.1X, MAB, WebAuth
5. **Network Security**: configure and verify network infrastructure security methods

* Configure network segmentation using VLANs and VRF-lite
* Configure Layer 2 and port security, DHCP snooping, dynamic ARP inspection, storm control,
* Configure PVLANs to segregate network traffic, defenses against MAC, ARP, vlan hopping, STP, DCHP rogue attacks
* Configure device hardening of network infrastructure security devices (control plane, data plane, management plane, and routing protocol security)
* Implement segmentation, access control policies, AVC, URL filtering, and malware protection
* Implement management options for network security solutions such as intrusion prevention and perimeter security (Single vs. multidevice manager, in-band vs. out-of-band, CDP, DNS, SCP, SFTP, and DHCP security and risks)
* Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)
* 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)
* Configure and verify site-to-site VPN and remote access VPN
* Site-to-site VPN utilizing Cisco routers and IOS
* Remote access VPN using Cisco AnyConnect Secure Mobility client
* Debug commands to view IPsec tunnel establishment and troubleshooting

+++ configuring NTP on ASA, FMC NGFW, **Configure Logging on Cisco ASA Appliance and Cisco Firepower NGFW**

**Configure Logging on Cisco IOS Device**

Configure Netflow on cisco IOS Devices

1. **Content Security**

* Configure and verify web and email security deployment methods to protect on-premises and remote users (inbound and outbound controls and policy management
* Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption
* 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
* Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)

D’aprs le cours pdf

* Configuring TACACS+ Access
* Configuring RADIUS Authentication
* Configuring NetFlow in Cisco IOS and Cisco IOS-XE
* Configuring NetFlow in NX-OS
* Configuring NTP
* Configuring Syslog Support
* Configuring site to site VPNs in the Cisco ASA
* Configuring Remote access VPNs in the Cisco ASA
* Configuring clientless Remote access SSL VPNs in the Cisco ASA
* Configuring client-Based Remote access SSL VPNs in the Cisco ASA
* Configuring Remote access VPNs in the Cisco FTD
* Configuring site to site VPNs in the Cisco FTD

Lab outlines (confer le dossier lab scor)

1. Configure Network Settings and NAT on Cisco ASA
2. Configure Cisco ASA Access Control Policies
3. Configure Cisco Firepower NGFW NAT
4. Configure Cisco Firepower NGFW Access Control Policy
5. Configure Cisco Firepower NGFW Discovery and IPS Policy
6. Configure Cisco NGFW Malware and File Policy
7. Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
8. Configure Mail Policies
9. Configure Proxy Services, Authentication, and HTTPS Decryption
10. Enforce Acceptable Use Control and Malware Protection
11. Examine the Umbrella Dashboard
12. Examine Cisco Umbrella Investigate
13. Explore DNS Ransomware Protection by Cisco Umbrella
14. Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
15. Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
16. Configure Remote Access VPN on the Cisco Firepower NGFW
17. Explore Cisco AMP for Endpoints
18. Perform Endpoint Analysis Using AMP for Endpoints Console
19. Explore File Ransomware Protection by Cisco AMP for Endpoints Console
20. Explore Cisco Stealthwatch Enterprise v6.9.3
21. Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
22. Explore the Cisco Cloudlock Dashboard and User Security
23. Explore Cisco Cloudlock Application and Data Security
24. Explore Cisco Stealthwatch Cloud
25. Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors