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

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)