Exam Objectives that do NOT Exist in Security+ SY0-401 but ARE in SY0-501

OBJ/Sub-OBJ	NEW in 501
2.0 Technologies and Tools	
2.1 Install and configure network components, both hardware- and software-based, to support organizational security.	
· Firewall	
o Stateful vs. stateless	NEW
· VPN concentrator	
o IPSec	
§ Tunnel mode	NEW
§ AH	NEW
§ ESP	NEW
o Split tunnel vs. full tunnel	NEW
o Always-on VPN	NEW
· NIPS/NIDS	
o Inline vs. passive	NEW
o Analytics	NEW
· Router	
o Antispoofing	NEW
· Switch	
o Layer 2 vs. Layer 3	NEW
· Proxy	
o Forward and reverse proxy	NEW
o Transparent	NEW
o Application/multipurpose	NEW
· Load balancer	
o Scheduling	NEW
§ Affinity	NEW
§ Round-robin	NEW
o Active-passive	NEW
o Active-active	NEW
o Virtual IPs	NEW
· Access point	
o Band selection/width	NEW
o Fat vs. thin	NEW
o Controller-based vs. standalon	NEW
· SIEM	
o Aggregation	NEW
o Correlation	NEW
o Automated alerting and trigge	NEW
o Time synchronization	NEW
o Event deduplication	NEW

o Logs/WORM	NEW
· DLP	
o USB blocking	NEW
o Cloud-based	NEW
o Email	NEW
· NAC	
o Dissolvable vs. permanent	NEW
o Host health checks	NEW
o Agent vs. agentless	NEW
· Mail gateway	NEW
o Spam filter	NEW
o DLP	NEW
o Encryption	NEW
· Bridge	NEW
· SSL/TLS accelerators	NEW
· SSL decryptors	NEW
· Media gateway	NEW
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.	
· Network scanners	NEW
o Network mapping	NEW
· Wireless scanners/cracker	NEW
· Password cracker	NEW
· Configuration compliance scanner	NEW
· Exploitation frameworks	NEW
· Data sanitization tools	NEW
· Command line tools	
o ping	NEW
o netstat	NEW
o tracert	NEW
o nslookup/dig	NEW
o arp	NEW
o ipconfig/ip/ifconfig	NEW
o tcpdump	NEW
o nmap	NEW
o netcat	NEW
2.3 Given a scenario, troubleshoot common security issues.	
· Unencrypted credentials/clear text	NEW
· Misconfigured devices	
o Content filter	NEW
· Weak security configurations	NEW
· Personnel issues	
o Personal email	NEW
· License compliance violation (availabil	NEW?
2.4 Given a scenario, analyze and interpret output from security technologies.	

· HIDS/HIPS	NEW?
· File integrity check	NEW?
· Advanced malware tools	NEW
2.5 Given a scenario, deploy mobile devices securely.	
· Connection methods	NEW
o Cellular	NEW
o WiFi	NEW
o SATCOM	NEW
o Bluetooth	NEW
o NFC	NEW
o ANT	NEW
o Infrared	NEW
o USB	NEW
· Mobile device management concepts	
o Geofencing	NEW
o Push notification services	NEW
o Passwords and pins	NEW
o Containerization	NEW
· Enforcement and monitoring for:	
o Third-party app stores	NEW
o Rooting/jailbreaking	NEW
o Sideloading	NEW
o Custom firmware	NEW
o Carrier unlocking	NEW
o Firmware OTA updates	NEW
o SMS/MMS	NEW
o USB OTG	NEW
o Recording microphone	NEW
o WiFi direct/ad hoc	NEW
o Tethering	NEW
o Payment methods	NEW
· Deployment models	
o COPE	NEW
o CYOD	NEW
o Corporate-owned	NEW
o VDI	NEW
2.6 Given a scenario, implement secure protocols.	
· Protocols	
o S/MIME	NEW
o SRTP	NEW
o Secure POP/IMAP	NEW
· Use cases	NEW
o Voice and video	NEW
o Time synchronization	NEW
o Email and web	NEW

o File transfer	NEW
o Directory services	NEW
o Remote access	NEW
o Domain name resolution	NEW
o Routing and switching	NEW
o Network address allocation	NEW
o Subscription services	NEW