Cisco 300-210

Exam Name Implementing Cisco Threat Control Solutions
Exam Number 300-210 SITCS
Cisco Certified Network Professional Security

Content Security

1 Cisco Cloud Web Security (CWS)
a) Describe the features and functionality
b) Implement the IOS and ASA connectors
c) Implement the Cisco AnyConnect web security module
d) Implement web usage control
e) Implement AVC
f) Implement antimalware
g) Implement decryption policies

2 Cisco Web Security Appliance (WSA)
a) Describe the features and functionality
b) Implement data security
c) Implement WSA identity and authentication, including transparent user identification
d) Implement web usage control
e) Implement AVC
f) Implement antimalware and AMP
g) Implement decryption policies
h) Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy)

3 Cisco Email Security Appliance
a) Describe the features and functionality
b) Implement email encryption
c) Implement antispam policies
d) Implement virus outbreak filter
e) Implement DLP policies
f) Implement antimalware and AMP
g) Implement inbound and outbound mail policies and authentication
h) Implement traffic redirection and capture methods
i) Implement ESA GUI for message tracking

Network Threat Defense

1 Cisco Next-Generation Firewall (NGFW) Security Services
a) Implement application awareness
b) Implement access control policies (URL-filtering, reputation based, file filtering)
c) Configure and verify traffic redirection
d) Implement Cisco AMP for Networks

2 Cisco Advanced Malware Protection (AMP)
a) Describe cloud detection technologies
b) Compare and contrast AMP architectures (public cloud, private cloud)
c) Configure AMP endpoint deployments

d) Describe analysis tools
e) Describe incident response functionality
f) Describe sandbox analysis
g) Describe AMP integration

Cisco FirePOWER Next-Generation IPS (NGIPS)

1 Configurations

2 Describe traffic redirection and capture methods
a Describe preprocessors and detection engines
b Implement event actions and suppression thresholds
c Implement correlation policies
d Describe SNORT rules
e Implement SSL decryption policies

3 Deployments
a Deploy inline or passive modes
b Deploy NGIPS as appliance, virtual appliance, or module within an ASA
c Describe the need for traffic symmetry
d Compare inline modes: inline interface pair and inline tap mode

Security Architectures

1 Design a web security solution
a) Compare and contrast Cisco FirePOWER NGFW, WSA, and CWS
b) Compare and contrast physical WSA and virtual WSA
c) Describe the available CWS connectors

2 Design an email security solution
a) Compare and contrast physical ESA and virtual ESA
b) Describe hybrid mode

3 Design Cisco FirePOWER solutions
a) Configure the virtual routed, switched, and hybrid interfaces
b) Configure the physical routed interfaces

Troubleshooting, Monitoring, and Reporting Tools

1 Design a web security solution
a) Compare and contrast FirePOWER NGFW, WSA, and CWS
b) Compare and contrast physical WSA and virtual WSA
c) Describe the available CWS connectors

2 Cisco Web Security Appliance (WSA)
a) Implement the WSA Policy Trace tool
b) Describe WSA reporting functionality
c) Troubleshoot using CLI tools

3 Cisco Email Security Appliance (ESA)
a) Implement the ESA Policy Trace tool
b) Describe ESA reporting functionality
c) Troubleshoot using CLI tools
4 Cisco FirePOWER
a) Describe the Cisco FirePOWER Management Center dashboards and reports

b) Implement health policy
c) Configure email, SNMP, and syslog alerts
d) Troubleshoot NGIPS using CLI tools