Implementing Cisco Threat Control Solutions (300-210)

Exam Description: The Implementing Cisco Threat Control Solutions (SITCS) exam (300-210) is part of the CCNP Security certification. It tests a network security engineer on advanced firewall architecture and configuration with the Cisco next-generation firewall, utilizing access and identity policies. This new revision of the SITCS exam replaces 300-207, removes some older technologies, and adds coverage for both Cisco Firepower NGIPS and Cisco AMP (Advanced Malware Protection). This 90-minute exam consists of 65–75 questions and covers integration of Intrusion Prevention System (IPS) and context-aware firewall components, as well as Web (Cloud) and Email Security solutions. Candidates can prepare for this exam by taking the Implementing Cisco Threat Control Solutions (SITCS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

27% 1.0 Content Security

- 1.1 Cisco Cloud Web Security (CWS)
  - 1.1.a Describe the features and functionality
  - 1.1.b Implement the IOS and ASA connectors
  - 1.1.c Implement the Cisco AnyConnect web security module
  - 1.1.d Implement web usage control
  - 1.1.e Implement AVC
  - 1.1.f Implement antimalware
  - 1.1.g Implement decryption policies
- 1.2 Cisco Web Security Appliance (WSA)
  - 1.2.a Describe the features and functionality
  - 1.2.b Implement data security
  - 1.2.c Implement WSA identity and authentication, including transparent user identification
  - 1.2.d Implement web usage control
  - 1.2.e Implement AVC
  - 1.2.f Implement antimalware and AMP
  - 1.2.g Implement decryption policies
  - 1.2.h Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy)
- 1.3 Cisco Email Security Appliance
  - 1.3.a Describe the features and functionality
  - 1.3.b Implement email encryption
  - 1.3.c Implement antispam policies
  - 1.3.d Implement virus outbreak filter

1.3.e Implement DLP policies
1.3.f Implement antimalware and AMP
1.3.g Implement inbound and outbound mail policies and authentication
1.3.h Implement traffic redirection and capture methods
1.3.i Implement ESA GUI for message tracking

22% 2.0 Network Threat Defense

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

2.2 Cisco Advanced Malware Protection (AMP)
2.2.a Describe cloud detection technologies
2.2.b Compare and contrast AMP architectures (public cloud, private cloud)
2.2.c Configure AMP endpoint deployments
2.2.d Describe analysis tools
2.2.e Describe incident response functionality
2.2.f Describe sandbox analysis
2.2.g Describe AMP integration

20% 3.0 Cisco FirePOWER Next-Generation IPS (NGIPS)

3.1 Configurations

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

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

17% 4.0 Security Architectures

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

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

4.3 Design Cisco FirePOWER solutions
- 4.3.a Configure the virtual routed, switched, and hybrid interfaces
- 4.3.b Configure the physical routed interfaces

14% 5.0 Troubleshooting, Monitoring, and Reporting Tools

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

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

5.3 Cisco Email Security Appliance (ESA)
- 5.3.a Implement the ESA Policy Trace tool
- 5.3.b Describe ESA reporting functionality
- 5.3.c Troubleshoot using CLI tools

5.4 Cisco FirePOWER
- 5.4.a Describe the Cisco FirePOWER Management Center dashboards and reports
- 5.4.b Implement health policy
- 5.4.c Configure email, SNMP, and syslog alerts
- 5.4.d Troubleshoot NGIPS using CLI tools