Implementing Cisco Threat Control Solutions (SITCS) 300-207

Exam Description:

The Implementing Cisco Threat Control Solutions (SITCS) (300-207) exam tests a network security engineer on advanced firewall architecture and configuration with the Cisco next-generation firewall, utilising access and identity policies. 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

1.0 Content Security

1.1 Cisco ASA 5500-X NGFW Security Services

- 1.1.a Describe features and functionality
- 1.1.b Implement web usage control (URL-filtering, reputation based, file filtering)
- 1.1.c Implement AVC
- 1.1.d Implement decryption policies
- 1.1.e Describe traffic redirection and capture methods

1.2 Cisco Cloud Web Security

- 1.2.a Describe features and functionality
- 1.2.b Implement IOS and ASA connectors
- 1.2.c Implement AnyConnect web security module
- 1.2.d Describe web usage control
- 1.2.e Implement AVC
- 1.2.f Implement anti-malware
- 1.2.g Describe decryption policies

1.3 Cisco WSA (Web Security Appliance)

- 1.3.a Describe features and functionality
- 1.3.b Implement data security
- 1.3.c Implement WSA Identity and Authentication, including Transparent User Identification

1.3.d Describe web usage control

1.3.e Implement AVC

1.3.f Implement anti-malware

1.3.g Describe decryption policies

1.3.h Describe traffic redirection and capture methods (Explicit Proxy vs. Transparent Proxy)

1.4 Cisco ESA

1.4.a Describe features and functionality

1.4.b Implement email encryption

1.4.c Implement anti-spam policies

1.4.d Implement virus outbreak filter

1.4.e Implement DLP policies

1.4.f Implement anti-malware

1.4.g Implement inbound and outbound mail policies and authentication

1.4.h Describe traffic redirection and capture methods

2.0 Threat Defence

2.1 Network IPS

2.1.a Implement traffic redirection and capture methods

2.1.b Implement network IPS deployment modes

2.1.c Describe signatures engines

2.1.d Implement event actions & overrides/filters

2.1.e Implement anomaly detection

2.1.f Implement risk ratings

2.1.g Describe IOS IPS

2.2 Configure device hardening per best practices

2.2.a IPS

2.2.b Content Security appliances

3.0 Devices GUIs and Secured CLI

3.1 Content Security

3.1.a Implement HTTPS and SSH access

3.1.b Describe configuration elements

3.1.c Implement ESA GUI for message tracking

4.0 Troubleshooting, Monitoring and Reporting Tools

4.1 Configure IME and IP logging for IPS

4.2 Content Security

- 4.2.a Describe reporting functionality
- 4.2.b Implement the WSA Policy Trace tool
- 4.2.c Implement the ESA Message Tracking tool
- 4.2.d Implement the ESA Trace tool
- 4.2.e Use web interface to verify traffic is being redirected to CWS
- 4.2.f Use CLI on IOS to verify CWS operations
- 4.2.g Use CLI on ASA to verify CWS operations
- 4.2.h Use the PRSM Event Viewer to verify ASA NGFW operations
- 4.2.i Describe the PRSM Dashboards and Reports

4.3 Monitor Cisco Security IntelliShield

- 4.3.a Describe at a high level the features of the Cisco Security IntelliShield Alert Manager Service

5.0 Threat Defence Architectures

5.1 Design IPS solution

- 5.1.a Deploy Inline or Promiscuous
- 5.1.b Deploy as IPS appliance, IPS software or hardware module or IOS IPS
- 5.1.c Describe methods of IPS appliance load-balancing
- 5.1.d Describe the need for Traffic Symmetry
- 5.1.e Inline modes comparison – inline interface pair, inline VLAN pair, and inline VLAN group
- 5.1.f Management options

6.0 Content Security Architectures

6.1 Design Web Security solution

- 6.1.a Compare ASA NGFW vs. WSA vs. CWS
- 6.1.b Compare Physical WSA vs. Virtual WSA
- 6.1.c List available CWS connectors

6.2 Design Email Security solution

- 6.2.a Compare Physical ESA vs. Virtual ESA 6.2.b Describe Hybrid mode

6.3 Design Application Security solution

- 6.3.a Describe the need for application visibility and control