LET’S BUILD TOMORROW TODAY
Agenda

• Overview of CCNP Security
• SENSS Exam Information
• SENSS Topics: Technical Introduction
• What You Need to Know?
• Sample Questions
• Conclusion with Q & A
CCNP Security Requirements

• The CCNA Security exam is the pre-requisites for this certification.
  • Candidates will benefit from having some basic routing & switching knowledge and have passed the CCNA Security (Implementing Cisco IOS Network Security - IINS 640-554) exam.

• CCNP Security Certification requires the passing of four exams:
  • 300-206 SENSS – Implementing Cisco Edge Network Security Solutions
  • 300-207 SITCS – Implementing Cisco Threat Control Solutions
  • 300-208 SISAS – Implementing Cisco Secure Access Solutions
  • 300-209 SIMOS – Implementing Cisco Secure Mobile Solutions

• Certification valid for 3 years
300-206 SENSS Exam

- 90-minute exam

- Register with PearsonVUE
  - www.vue.com/.cisco

- Exam cost is $250.00 US
Preparing for the 300-206 SENSS Exam

- Recommended reading
  - CCNP Security Firewall 642-618 Quick Reference
  - CCNP Security FIREWALL 642-618 Official Cert Guide

- Recommended training via CLP
  - Deploying Cisco ASA Firewall Solutions v2.0

- Cisco learning network
  - www.cisco.com/go/learnnetspace

- Practical experience

Available for pre-order
Test Taking Tips

• It’s not possible to cover everything!
• We want you to get a feel for the technical level of the exam, not every topic possible
• Give you suggestions, resources, some examples
• Will focus on key topics

• Expect approx. 50 - 60 hours of reading per exam to achieve a firm understanding on concepts
  – Reading study material and books (reading material suggestions to follow)
  – Watching technical VoDs & Webinars

• Plan for min. 20 - 25 hours of hands on lab practice
  – Initial Setup, Configuration, Troubleshooting specific devices
300-206 SENSS High-Level Topics and Weighting

SENSS (300-206) Exam—Topics and Weighting

• 25% 1.0 Threat Defense
• 25% 2.0 Cisco Security Devices GUIs and Secured CLI Management
• 12% 3.0 Management Services on Cisco Devices
• 10% 4.0 Troubleshooting, Monitoring and Reporting Tools
• 16% 5.0 Threat Defense Architectures
• 12% 6.0 Security Components and Considerations
Threat Defense
Threat Defense—Key Concepts

1.1 Implement Firewall (ASA or IOS depending on which supports the implementation)

- Implement ACLs
- Implement Static/Dynamic NAT/PAT; redesign of Network Address Translation on the Cisco ASA (8.3 or Higher)
- Implement Object Groups
- Describe Threat Detection features
- Implement Botnet Traffic Filtering
- Configure Application Filtering and Protocol Inspection
- Describe ASA security context
Firewall Filtering Technologies

- The following are the mainstream filtering technologies:
  - Stateless packet filtering → Layer 3-only filtering
  - Stateful packet filtering → Layers 3 and 4
  - Stateful packet filtering with AIC (or AVC) → Layers 3—7
  - Reputation-based filtering → Botnet Traffic Filter
  - Application layer gateway → Layer 7
  - Identity Firewall → AD + 5-tuple information

- Cisco ASA version 8.4(2) introduces the concept of Identity Firewall; enables the firewall to allow or deny access to network resources based on the username identity instead of a simple source IP address.

- The Identity Firewall integrates with Microsoft Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping.
Identity Firewall Components

The three main components of the Cisco ASA Identity Firewall solution are:

- Cisco ASA
- Cisco Context Directory Agent
- Microsoft Active Directory Domain Controllers
NAT Post ASA Version 8.3

NAT is redesigned in 8.3 and above to simplify operations:

• A single rule to translate the source and destination IP address.
• You can also manually establish the order in which NAT rules are processed.
• Introduction of NAT to “any” interface

Two Nat modes available in 8.3 and above

• Network Object NAT: translation rule that defines a network object.
  • Well suited for source-only NAT
  • Sometimes referred to as "Auto-NAT"
• Manual NAT:
  • Policy based NAT when the source and destination address or port need to be considered
  • Sometimes referred to as Twice NAT
Deploying Cisco ASA Botnet Traffic Filter

• The Botnet Traffic Filter is a reputation-based mechanism used to prevent traffic from and to known bot-infected hosts.

• The Botnet Traffic Filter compares the source and destination IP address of each connection to the following:
  • Dynamic Cisco SIO database, updated by Cisco
  • Static database, which can be populated manually

• When traffic matches an entry in either database, a syslog message is logged and traffic can be dropped.
Deploying Cisco ASA Botnet Traffic Filter

Dynamic Database

- A dynamic database of known bad hostnames is downloaded from the Cisco SIO to the Cisco ASA and is constantly updated.
- DNS replies for bad hostnames are cached on the appliance in a DNS reverse-lookup cache.
- When a new connection is initiated, its source and destination IP addresses are compared with entries in the DNS reverse-lookup cache.
Deploying Cisco ASA Botnet Traffic Filter

To configure Botnet Traffic Filter, complete these tasks:

1. Enable lookups to the dynamic database
2. Optionally, add entries to the static database
3. Enable DNS inspection (DNS snooping)
4. Enable the Botnet Traffic Filter to detect bot traffic
5. Optionally, enable the Botnet Traffic Filter to drop bot traffic

- Enable Botnet Traffic Filter to monitor and drop malicious traffic.
- Add www.example-bad-hostname.com to static blacklist.
- Add www.example-not-so-bad-hostname.com to static whitelist.
Deploying Cisco ASA Botnet Traffic Filter

Task 1: Enable Lookups to the Dynamic Database

- Downloaded database is stored in running memory
- The update server determines how often the ASA polls the server for update
Deploying Cisco ASA Botnet Traffic Filter

Task 2: Optionally, Add Entries to the Static Database

Configuration > Firewall > Botnet Traffic Filter > Black and White Lists

- Add an entry to the blacklist to drop traffic from or to that host
- Add an entry to the whitelist to receive a syslog message when traffic goes to or from that host
Deploying Cisco ASA Botnet Traffic Filter

Task 3: Enable DNS Snooping

Configuration > Firewall > Botnet Traffic Filter > DNS Snooping

- DNS snooping is required to intercept and cache DNS replies in the DNS reverse lookup cache
- This window displays all polices that include DNS inspection
Deploying Cisco ASA Botnet Traffic Filter

Task 4: Enable the Botnet Traffic Filter to Detect Bot Traffic

- Monitoring of traffic triggers a syslog message when traffic goes to or from blacklisted or whitelisted IP address.
- Enable Botnet traffic filter on all interfaces facing the Internet.

Configure an ACL to monitor only a subset of traffic.
Enable Botnet Traffic Filter on an interface.
Enable the ASA to treat ambiguous addresses as blacklisted traffic.
Deploying Cisco ASA Botnet Traffic Filter

Task 5: Optionally, Enable Botnet Traffic Filter to Drop Traffic

Configuration > Firewall > Botnet Traffic Filter > Traffic Settings

- Blacklisted action causes traffic matching a blacklisted host to be dropped.
Threat Defense—Key Concepts

1.2 Describe Layer 2 and Layer 3 Security

- Configure DHCP Snooping
- Describe and configure Dynamic ARP Inspection (DAI)
- Describe and configure Storm Control
- Describe and configure Port Security
- Describe common layer 2 threats and attacks and mitigation
- Describe and configure MACSec
- Describe and configure IP Source Guard
Threat Defense - Layer 2 Security Concepts

- **DHCP Snooping** - Specifically prevents DHCP server spoofing attacks and mitigates DHCP starvation to a degree.

- **ARP Inspection** - Prevents ARP spoofing attacks by intercepting and validating all AF requests and responses.

- **Storm Control** - Monitors incoming traffic levels over a 1-second traffic storm control interval. Prevents traffic from being disrupted by a broadcast, multicast, or unicast flood.

- **Private VLANs** - Provide Layer 2 isolation between ports within the same VLAN.

- **MACsec Encryption** - Provides MAC-layer encryption over wired networks using OOB methods for encryption keying.

---

Diagram explanation:
- **PVLANs, port security, DHCP snooping, ARP inspection, MACsec, storm control, QoS**
- **MAC spoofing**, **DHCP spoofing**, **ARP spoofing**, **Traffic flooding**, **Unauthenticated network access**, **Traffic capture and modification**
- **Provides traffic forwarding functions**
- **Traffic filtering and conditioning, Cryptographic protection**

---

**Cisco Live!**

BRKCRT-2214 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public 23
Threat Defense - Layer 3 Security Concepts

- **uRPF** – Ensures that traffic from known invalid networks should not be accepted on interfaces from which they have never originated.

- **Interface ACL** - Filter traffic on an interface based on match criteria in the packet header-source and destination IP address, source and destination port, protocol, and flags.

- **Flexible Packet Matching** - An ACL pattern-matching tool and provides more thorough and customized packet filters. Enables users to match on arbitrary bits of a packet at an arbitrary depth in the packet header and payload.
Threat Defense—Configure Device Hardening Per Best Practice

• 1.3 Configure Device Hardening Per Best Practices
  • Network Device Planes – Data, Control, Management (Configure device hardening per best practices for Routers, Switches, Firewalls)
## Threat Defense – Network Device Planes

<table>
<thead>
<tr>
<th>Plane</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Plane</td>
<td>Provides traffic forwarding functions: switched and routed data</td>
</tr>
<tr>
<td>Control Plane</td>
<td>Builds control structures required for traffic forwarding</td>
</tr>
<tr>
<td>Management Plane</td>
<td>Provides device management functions</td>
</tr>
</tbody>
</table>
Threat Defense – Control Plane Security Controls

- **Control Plane Policing** – Allows users to configure a quality of service (QoS) filter that can granularly permit, drop, or rate-limit traffic to the CPU using a MQC interface.

- **Control Plane Protection** - Extends the CPP feature by enabling classification of the control plane traffic based on packet destination and information provided by the forwarding plane, allowing appropriate throttling for each category of packet.

- **Router Protocol Authentication & Filtering** - Prevents injection of malicious routing information and adjacency from unknown, unauthenticated peers.
Threat Defense – Control Plane Protection

Configure The ACL

ip access-list extended CPPR-EIGRP
  permit eigrp 10.0.0.0 0.255.255.255 any
!
class-map CPPR-EIGRP-CLASS
match access-group name CPPR-EIGRP
!
policy-map CPPR-POLICY
  class CPPR-EIGRP-CLASS
  police rate 200 pps conform-action transmit exceed-action drop
  class class-default
  police rate 50 pps conform-action transmit exceed-action drop
!
control-plane host
service-policy input CPPR-POLICY
Threat Defense - Additional Reading Topics

- NAT on the ASA (8.3 or Higher) –

- Introduction to the Cisco ASA 1000V –

- Configuring Modules (ASA CX Module, ASA IPS Module, ASA CSC Module) –
Simulation Example
Configure static NAT using network object NAT on the Cisco ASA

You are the network security engineer for the XYZ network. The XYZ network requires network address translation in order to hide internal addressing and to enable connectivity from the network to the Internet. The CSO tasked you with implementing dynamic NAT with PAT on the Cisco ASA for the hosts that require only outbound connectivity. The CSO also tasked you to configure static NAT for servers that require also inbound connectivity. In this activity you will need to do the following:

• Create a new network object with name DMZ-SRV and IP address 192.168.10.10.

• Configure static NAT with the following parameters:
  - Translated IP address: 209.165.201.1
  - Object name for the translated IP address: TRANSLATED-DMZ-SRV
  - Source interface: DMZ
  - Destination interface: outside

• Access the HQ-ASA console. Check the configuration by displaying the NAT table.
Simulation Example (Cont.)
Configure static NAT using network object NAT on the Cisco ASA

Not all ASDM screens are fully functional.
Threat Defense—Type of Exam Questions/Answers

• What is required to configure an application-layer inspection of FTP traffic on port 21 as well as 1056 (a non-standard port)? - create an access list that specifies the ports, and assign it to a new class map

• What network device plane is responsible for device administration, provision configuration and monitoring the device operation? – Control Plane

• What are the two common AAA protocols that are used to configure external AAA for management access on the Cisco ASA? – RADIUS & TACACS+

• Scenario: At an organization, they have salesmen coming in to demo products, and they just pull the Ethernet jack off employee PC and connect it to their laptop, hoping to get Internet access. Which action can the administrator take to prevent this from occurring? - Configure port-security

• Name some hardening techniques for Cisco IOS router? – SSH, ACLs, password encryption

• What command is used to disable Cisco Discovery Protocol (CDP)? And why? - Switch1(config-if)#no cdp enable; for example, on the external interface of the Internet router connected to your ISP because the ISP does not need the details about the internal network configuration.
Cisco Security Devices GUIs and Secured CLI Management
Cisco Security Devices GUls and Secured CLI Management—Key Concepts

- 2.1 Implement SSHv2, HTTPS, SNMPv3 access on the network devices
- 2.2 Implement RBAC on the ASA/IOS CLI and ASDM
- 2.3 Describe Cisco Prime Infrastructure
  - Functions and use cases of Cisco Prime
  - Device Management
- 2.4 Describe Cisco Security Manager (CSM)
  - Functions and use cases of Cisco Prime
  - Device Management
- 2.5 Implement Device Manager
  - Implement ASA firewall features using ASDM

Overview
Licensing Requirements
Prerequisites
Guidelines and Limitations
Configuring the Feature
Monitoring the Logs
2.1 Implement the following access on network devices:

- SSH v2
- HTTPS
- SNMP v3
Implement SSHv2, HTTPS, SNMPv3 Access

- **AAA** – A central repository of authentication credentials, authorization rules, and accounting logs. Permits who can access the device, what they are authorized to do, and what they accomplished by logging.

- **SSH** - A strongly encrypted and strongly authenticated protocol that allows CLI access to the ASA. Requires generating an RSA key of at least 768 bits to enable.

- **HTTPs** - AA strongly encrypted and strongly authenticated protocol that allows GUI and file copy access to the adaptive security appliance.

- **SNMPv3** - v3 uses authentication and encryption for transmission protection, and therefore can be deployed over untrusted network paths.
Implement HTTPS on the ASA

CLI Requirements on the ASA

```
interface Management0/0
  nameif management
  security-level 80
  ip address 10.10.2.1 255.255.255.0
  no shutdown
!
http server enable
http 172.16.200.0 255.255.255.0 management
```
Implement SSH access on an IOS device

1. **Specify hostname and domain name**
   
   ```
   hostname RouterA
   ip domain-name cisco.com !
   ```

2. **Create an RSA key pair**
   * For SSH v2 the modulus size must be at least 768 bits
   
   ```
   crypto key generate rsa modulus 2048 !
   ip ssh version 2
   username admin privilege 15 secret Admin92DXBh !
   ```

3. **Optionally configure an ACL to apply to the vty**
   
   ```
   ip access-list standard 90
   permit 10.10.10.0 0.0.0.255
   deny any log !
   ```

4. **Configure the transport Input to only accept SSH**
   
   ```
   vty 0 15
   transport input ssh
   login local
   access-class 90 in
   ```
Implement RBAC on the ASA/IOS CLI and ASDM

• RBAC is an access control approach that restricts user access based on the role of the user.

• Users are assigned to roles with specific permissions

• RBAC is being depreciated in IOS with the Role Based CLI access “Parser View” command (shown later)

• User accounts have the following attributes: username, password, expiry date, user roles
Implement RBAC on the ASA using ASDM

Setting Privilege Level
Implement RBAC on the IOS device

Configure AAA requirements

Configure usernames and privilege levels

Configure commands and exec levels

---

```bash
aaa-new model
!
aaa authentication login MGMT_ACCESS group tacacs+ local
aaa authorization exec MGMT_ACCESS group tacacs+ local
aaa authorization commands 1 MGMT_ACCESS group tacacs+ local
aaa authorization commands 15 MGMT_ACCESS group tacacs+ local
aaa accounting exec MGMT_ACCESS start-stop group tacacs+
aaa accounting commands 1 MGMT_ACCESS start-stop group tacacs+
aaa accounting commands 15 MGMT_ACCESS start-stop group tacacs+
!
username admin_backup privilege 15 secret admin_backup123
username security_viewer_backup privilege 7 secret
security_viewer_backup123
!
privilege exec level 7 show crypto ipsec sa
privilege exec level 7 show crypto ikev2 sa
!
tacacs server TACACS+
address ipv4 10.10.2.20
key cisco123
```
Implement Role Based CLI access on IOS devices

Enables root view

Configure NOC view

Allows NOC the following:
- dynamic routing protocol
- static routes
- apply interface specific commands
- execute any show commands

Configure SOC view

- Allows SOC configure commands

enable view

parser view NOC
secret 5 $1$TDy.$kquP9EdEYGJ0.oQE3cJaN.
commands configure include all ip access-list
commands configure include all interface
commands configure include ip
commands exec include configure terminal
commands exec include configure
commands exec include show running-config
commands exec include show

parser view secop
secret 5 $1$BLsw$UjHivthLFLACo9ClKXx46/
commands configure include all interface
commands configure include all zone-pair
commands configure include all zone
commands configure include all policy-map
Describe Cisco Prime Infrastructure

Cisco Prime Infrastructure can be used to generate the following:

- Hardware lifecycle (EoX)
- Compliance details
- Security Reports - Product Security Incident Response Team (PSIRT)

**EoX / PSIRT Reports**

- EoX Report
- PSIRT report based on your configuration & not just the IOS version
Describe Cisco Security Manager (CSM)

Cisco Security Manager (CSM) Features:

- AAA and Access Rules
- Zone Based Policy Firewall Rules (IOS)
- Inspection Rules
- Access Control
- IPS Device Management
- DMVPN
- GETVPN
- QoS
- Comprehensive Reporting
Configuring Layer 7 Inspection Using ASDM

Use Case:

1. Create a Layer 7 **class map** to identify traffic by matching criteria specific to applications:

   - IM
   - RTSP
   - SIP
   - DNS
   - FTP
   - H.323
   - HTTP

2. Create a Layer 7 **policy map** to defend against Application Layer attacks by referencing a Layer 7 class-map and applying an action.

3. Create a Layer 3/4 **policy map** to associate traffic defined in a Layer 3/4 class map and reference the Layer 7 **policy map**:

4. Use a **service policy** to activate the Layer 3/4 policy on an interface or globally.
Filtering FTP Commands: Layer 7 Policy Map
Filtering FTP Commands: Layer 7 Policy Map (Cont.)

Inspections
Filtering FTP Commands: Service Policy Rule
Filtering FTP Commands: Service Policy Rule (Cont.)
## Implement Device Manager for Layer 7 Inspection

### Layer 3/4 Class Maps

- Match traffic based on protocols, ports, IP addresses, and other layer 3 or 4 attributes:
  - ACL
  - Any packet
  - Default inspection traffic
  - IP differentiated services code point
  - TCP and UDP ports
  - IP precedence
  - RTP port numbers
  - VPN tunnel group
- Typically contain only one match condition
- Are mandatory MPF components

### Layer 7 Class Maps

- Work with layer 7 policy maps to implement advanced protocol inspection
- Match criteria is specific to one of the following applications:
  - DNS
  - FTP
  - H.323
  - HTTP
  - IM
  - RTSP
  - SIP
- Enable you to specify a not operator for a match condition
- Can contain one or more match conditions
- Can use regular expressions as match criteria
- Are optional MPF components (match criteria can be specified in a layer 7 policy map instead)
Cisco Security Devices GUIs and Secured CLI Management—Prep Resources

25% 2.0 Cisco Security Devices GUIs and Secured CLI Management

- User Guide for Cisco Security Manager 4.3 -

- Cisco Router and Security Device Manager_Technical References -

- Cisco Prime Infrastructure 2.1 Release Notes -

- Administering Cisco ISE -
Cisco Security Devices GUls and Secured CLI Management—Type of Exam Questions/Answer

• List few caveats for ASDM compatibility. - ASDM Launcher requires trusted certificate, requires strong encryption license (3DES/AES) on ASA or workaround etc.

• List some features of the Cisco Prime Security Manager. - Cisco Prime Security Manager provides a range of features for the Cisco ASA 5500-X NGFW platform: preloaded on-box single-device management, central management application for multi-device management, traffic-pattern reports, Object import, behavior-based policy management, event analysis, monitoring, license management etc.

• What is the default service account in Cisco Security Manager 4.4? - casuser
Management Services on Cisco Devices
Management Services on Cisco Devices

• 3.1 Configure NetFlow exporter on Cisco Routers, Switches, and ASA
• 3.2 Implement SNMPv3
• 3.3 Implement logging on Cisco Routers, Switches, and ASA using Cisco best practices
• 3.4 Implement NTP with authentication on Cisco Routers, Switches, and ASA
• 3.5 Describe CDP, DNS, SCP, SFTP, and DHCP
Configure NetFlow exporter on Cisco IOS Device

Configuration Tasks:

2. Configure a Flexible NetFlow monitor.
3. Apply Flexible NetFlow monitors to routed interfaces.
Configure NetFlow exporter on Cisco IOS Device

Configure the Flexible NetFlow exporter.

Configure a Flexible NetFlow monitor

Optionally set the source address of the Netflow export device

Apply the configured Flexible NetFlow monitor to a network interface

```plaintext
flow exporter MYEXPORTER
  destination 172.16.200.12
  transport udp 9996
  export-protocol netflow-v9

! flow monitor MYMONITOR
  record netflow ipv4 original-input
  exporter MYEXPORTER

! ip flow-export source Loopback0

! interface GigabitEthernet 0/1
  ip flow monitor MYMONITOR input
```

Optionally you can configure Sampled Netflow:

Implement SNMPv3 on the ASA

Create a SNMPv3 group and user for use.
Implement SNMPv3 on the ASA (Cont.)

Allow the SNMP clients to poll or to receive traps from the ASA.
Select the events to notify on through SNMP traps using ASDM. Example link up/down state.
Implement logging on Cisco Routers, Switches, and ASA

Logging of device and network events can be used for:

- Device failure notifications
- Network telemetry and forensics
- Security audit

Support for the following logging destinations:

- Console
- Telnet or SSH administrative sessions (Terminal)
- The internal in-memory buffer
- Remote syslog servers
Implement logging on Cisco Routers, Switches, and ASA

Logging on Cisco IOS Software
loggin on
! logging buffered informational
! logging trap debugging logging host 192.168.20.51

Router# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)
<output omitted>
  Console logging: level debugging, 3306 messages logged, xml disabled, filtering disabled
  Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
  Buffer logging: level informational, 3306 messages logged, xml disabled, filtering disabled
<output omitted>
  Trap logging: level debugging, 61 message lines logged
    Logging to 192.168.21.51 (udp port 514, audit disabled, link up),
<output omitted>

Logging buffered enabled
Logging trap enabled
Logging to host 192.168.21.51
Implement logging on the ASA using the ASDM

Globally enable logging on the ASA

Possible message severity levels are:

0. Emergencies
1. Alert
2. Critical
3. Error
4. Warning
5. Notification
6. Informational
7. Debugging:

Configuration > Device Management > Logging > Logging Setup

Suppress message logging example:

MY_ASA(config)# no logging message 111009 level 7
NTP with authentication on Cisco Routers, Switches, and ASA

Overview of NTP

- NTP is used for clock synchronization between network devices
- Uses UDP on port 123
- NTP authentication and logging are disabled by default
- NTP authentication can be enabled to eliminate spoofing attacks (Best Practice)
- Accurate clock settings are required for:
  - Logging with accurate timestamps
  - Digital certificate validation
  - SSO authentication mechanisms
Implement NTP on Cisco IOS Devices

NTP on Cisco IOS Example

clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
!
ntp server 192.16.20.123
!
ntp authenticate
ntp authentication-key 1 md5 cisco
ntp server 192.168.20.123 key 1
ntp trusted-key 1

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ntp associations [Detail]</td>
<td>Displays the status of NTP associations</td>
</tr>
<tr>
<td>show ntp status</td>
<td>Displays the status of NTP</td>
</tr>
</tbody>
</table>
Management Services on Cisco Devices—Type of Exam Questions/Answers

• Which command Enables random mode and specifies a sampling rate for the NetFlow sampler? - `mode random one-out-of sampling-rate`
  
  Example: `Router(config-sampler)# mode random one-out-of 100`

• Name three security features provided in SNMPv3? - Message integrity, Authentication, and Encryption

• Which commands can disable logging to the console sessions and terminal lines? - `no logging console`, `no logging monitor`

• What is the severity level of the following partial event message? `Jan 5 2011 09:27:16 FIREWALL : %ASA-6-725002: Device completed ... - Informational`
Troubleshooting, Monitoring and Reporting Tools
Troubleshooting, Monitoring and Reporting Tools

• 4.1 Monitor firewall using analysis of packet tracer, packet capture, and syslog
  • Analyze packet tracer on the firewall using CLI/ASDM
  • Configure and analyze packet capture using CLI/ASDM
  • Analyze syslog events generated from ASA
Use ASDM Packet Tracer to analyze packets.

- Packet Tracer is a tool that can verify how rules will affect traffic passing through the firewall.
- Optionally this can also be done CLI.

```bash
ciscoasa# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed```
Use ASDM Packet Capture Wizard to analyze packets.

- A wizard can be used to capture traffic to the ASDM GUI.
- Optionally this can also be done CLI.
Troubleshooting, Monitoring and Reporting Tools—Prep Resources


Which of the following represent ASA functions that can be tested with Packet Tracer? - Routing table lookup, Network Address Translation entries, Host connection limits, Access list results.....

What are optional parameters of the `packet-tracer` command? - `packet-tracer input [src_int] protocol src_addr src_port dest_addr dest_port [detailed] [xml]`

Which command shows the current logging rate-limit setting? - `show running-config logging rate-limit`
Threat Defense Architectures
Threat Defense Architectures

5.1 Design a Firewall Solution
- High-availability
- Basic concepts of security zoning
- Transparent & Routed Modes
- Security Contexts

5.2 Layer 2 Security Solutions
- Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
- Describe best practices for implementation
- Describe how PVLANs can be used to segregate network traffic at Layer 2
Know the Cisco ASA Product Portfolio

ASA 5506-X
ASA 5506W-X
ASA 5506H-X

ASA 5505
(150 Mbps, 4K cps)

ASA 5512-X
(1 Gbps, 10K cps)

ASA 5515-X
(1.2 Gbps, 15K cps)

ASA 5525-X
(2 Gbps, 20K cps)

ASA 5545-X
(3 Gbps, 30K cps)

ASA 5555-X
(4 Gbps, 50K cps)

ASA 5585-X SSP-10
(4 Gbps, 50K cps)

ASA 5585-X SSP-20
(10 Gbps, 125K cps)

ASA 5585-X SSP-40
(20 Gbps, 200K cps)

ASA 5585-X SSP-60
(40 Gbps, 350K cps)

ASA 5505-
X

ASA 5508-X

ASA 5506W-X

ASA 5506H-X

ASA 5505
(150 Mbps, 4K cps)

ASA 5512-X
(1 Gbps, 10K cps)

ASA 5515-X
(1.2 Gbps, 15K cps)

ASA 5525-X
(2 Gbps, 20K cps)

ASA 5545-X
(3 Gbps, 30K cps)

ASA 5555-X
(4 Gbps, 50K cps)

ASA 5585-X SSP-10
(4 Gbps, 50K cps)

ASA 5585-X SSP-20
(10 Gbps, 125K cps)

ASA 5585-X SSP-40
(20 Gbps, 200K cps)

ASA 5585-X SSP-60
(40 Gbps, 350K cps)

ASA 5505

ASA 5508-X

ASA 5506W-X

ASA 5506H-X

ASA 5505
(150 Mbps, 4K cps)

ASA 5512-X
(1 Gbps, 10K cps)

ASA 5515-X
(1.2 Gbps, 15K cps)

ASA 5525-X
(2 Gbps, 20K cps)

ASA 5545-X
(3 Gbps, 30K cps)

ASA 5555-X
(4 Gbps, 50K cps)

ASA 5585-X SSP-10
(4 Gbps, 50K cps)

ASA 5585-X SSP-20
(10 Gbps, 125K cps)

ASA 5585-X SSP-40
(20 Gbps, 200K cps)

ASA 5585-X SSP-60
(40 Gbps, 350K cps)

ASA 5505

ASA 5508-X

ASA 5506W-X

ASA 5506H-X

ASA 5505
(150 Mbps, 4K cps)

ASA 5512-X
(1 Gbps, 10K cps)

ASA 5515-X
(1.2 Gbps, 15K cps)

ASA 5525-X
(2 Gbps, 20K cps)

ASA 5545-X
(3 Gbps, 30K cps)

ASA 5555-X
(4 Gbps, 50K cps)

ASA 5585-X SSP-10
(4 Gbps, 50K cps)

ASA 5585-X SSP-20
(10 Gbps, 125K cps)

ASA 5585-X SSP-40
(20 Gbps, 200K cps)

ASA 5585-X SSP-60
(40 Gbps, 350K cps)

ASA 5505

ASA 5508-X

ASA 5506W-X

ASA 5506H-X

ASA 5505
(150 Mbps, 4K cps)

ASA 5512-X
(1 Gbps, 10K cps)

ASA 5515-X
(1.2 Gbps, 15K cps)

ASA 5525-X
(2 Gbps, 20K cps)

ASA 5545-X
(3 Gbps, 30K cps)

ASA 5555-X
(4 Gbps, 50K cps)

ASA 5585-X SSP-10
(4 Gbps, 50K cps)

ASA 5585-X SSP-20
(10 Gbps, 125K cps)

ASA 5585-X SSP-40
(20 Gbps, 200K cps)

ASA 5585-X SSP-60
(40 Gbps, 350K cps)
Layer 2 Security Solutions Private VLANs (PVLAN)

PVLANs allow you to provide coarse access control within a VLAN to limit connectivity:

- A VLAN can be divided into multiple logical segments (secondary VLANs) that have specific connectivity needs.
- Secondary VLANs can create host groups or isolate individual hosts and still provide Layer 3 routing out of the VLAN.
- Private VLANS run over VLAN Trunking Protocol in transparent mode.
Layer 2 Security Solutions Private VLANs (Cont.)

A port in a PVLAN can be one of three types:

- **Isolated**: Communicate only with promiscuous ports
- **Promiscuous**: Communicate with all other ports
- **Community**: Communicate with other members of the community and all promiscuous ports

Note: For PVLANs, the VTP mode must be transparent, not client or server.
Layer 2 Security Solutions Private VLANs (Cont.)

- vtp mode transparent
- !
- vlan 600
  - private-vlan community
- vlan 400
  - private-vlan isolated
- vlan 200
  - private-vlan primary
  - private-vlan association 400,600
- !
- interface FastEthernet 5/1
  - switchport mode private-vlan host
  - switchport private-vlan host-association 200,400

- interface range FastEthernet 5/2 - 3
  - switchport mode private-vlan host
  - switchport private-vlan host-association 200,600

- interface FastEthernet 5/4
  - switchport mode private-vlan promiscuous
  - switchport private-vlan mapping 200,400,600

- interface GigabitEthernet0/1
  - switchport mode trunk
  - switchport trunk encapsulation dot1q
Threat Defense Architectures—Prep Resources

• Firewall and IPS_Technology Design Guide:

• Design Zone for Security
Threat Defense Architectures—Type of Exam Questions/Answers

• What is a Zone-Based Policy Firewall zone? - collection of networks reachable over one or a specific set of router interfaces

• Which two options are the default behavior when interfaces are tagged into Cisco IOS Zone-Based Policy Firewall zones? - Interfaces in the same zone can freely communicate and All traffic is denied between zones.
Security Components and Considerations
Security Components and Considerations

6.1 Describe security operations management architectures
   • Single device manager vs. multi-device manager

6.2 Describe Data Center security components and considerations
   • Virtualization and Cloud security

6.3 Describe Collaboration security components and considerations
   • Basic ASA UC Inspection features
   • Protocols that can be inspected: SIP, MGCP, H323 (225, 245), SCCP, protocol inspection/anomaly check

6.4 Describe common IPv6 security considerations
   • Unified IPv6/IPv4 ACL on the ASA
   • IPv6 First-Hop Security Concerns
   • IPv6 and IPv4 Threat Comparison and Best Practices
Security Components and Considerations— Prep Resources

Cisco TrustSec 2.0: Design and Implementation Guide

Security and Virtualization in the Data Center

Cisco Collaboration Security

IPv6 First-Hop Security Concerns
http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html

IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)

Security Intelligence Operations - Technical White Papers
http://tools.cisco.com/security/center/whitePapers.x?i=43
Security Components and Considerations—Type of Exam Questions/Answers

• Match each Cisco SecureX component with its definition – Cisco TrustSec, Identity Services Engine (ISE), Security Intelligence Organization (SIO), Cisco AnyConnect Secure Mobility

• Threats that are unique to IPv6?
  – Reconnaissance attacks, although more difficult but possible using IPv6 tools such as Parasit6, Fakeroute6, or Scapy6
  – IPv6 protocol stack attacks
  – Attacks against ICMPv6

• What is IPv6 stateless address autoconfiguration (SLAAC)? - IPv6 stateless address autoconfiguration (SLAAC) is a mechanism that enables an IPv6 endpoint to get an IPv6 address from the link it is coming up on without requiring DHCPv6 address allocation.
Additional Reference Material: Lab Equipment, Software Requirements and Recommended Labs
CCNP Security ILT—Lab Topology
## Laboratory Equipment

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA 5515-X with IPS SW 6GE Data 1 GE Mgmt AC 3DES/AES</td>
</tr>
<tr>
<td>ASA 5512-X through 5555-X 120GB MLC SED SSD</td>
</tr>
<tr>
<td>Cisco 2901 w/2 GE, 4 EWIC, 2DSP, 256 CF 512 DRAM IP Base</td>
</tr>
<tr>
<td>Cisco 2901-2921 IOS Universal</td>
</tr>
<tr>
<td>512MB to 1.5GB DRAM Upgrade for Cisco 2901-2921</td>
</tr>
<tr>
<td>256MB Compact Flash for 1900, 2900, 3900 ISR</td>
</tr>
<tr>
<td>Cisco 2610XM with 1 FE interface</td>
</tr>
<tr>
<td>Cisco 3560 Catalyst 24 port</td>
</tr>
<tr>
<td>UCS C22 MD SFF w/ rail kit w/o PSF, CPU, mem, HDD PCIe</td>
</tr>
<tr>
<td>2.30 GHz , E5-2470/95W 8C/20MB Cache/DDR3 1600MHz</td>
</tr>
<tr>
<td>16GB DDR-1600-MHz RDIMM/PC3-12800/dual rank/1.35v</td>
</tr>
<tr>
<td>900GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive slide mounted</td>
</tr>
<tr>
<td>MegaRAID 9240-8i, RAID 0/1/10/5/50 for C22/C24</td>
</tr>
<tr>
<td>650W Power Supply for C-series rack servers</td>
</tr>
<tr>
<td>Software</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>ASA 9.1</td>
</tr>
<tr>
<td>ASA 5515-X</td>
</tr>
<tr>
<td>ASA 5500</td>
</tr>
<tr>
<td>AnyConnect</td>
</tr>
<tr>
<td>ISE 1.2</td>
</tr>
<tr>
<td>ESA Premium SW Bundle</td>
</tr>
<tr>
<td>Cisco Context Directory Agent</td>
</tr>
<tr>
<td>C2900 Software</td>
</tr>
<tr>
<td>C3560 Software</td>
</tr>
<tr>
<td>Security License for 2901-2951</td>
</tr>
<tr>
<td>IP Base License 2901-2951</td>
</tr>
<tr>
<td>Microsoft Windows 7 Enterprise</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 Enterprise</td>
</tr>
<tr>
<td>Wireshark</td>
</tr>
<tr>
<td>Kiwi Syslog Server, Free Edition</td>
</tr>
<tr>
<td>Scrutinizer (NetFlow) Trial Edition</td>
</tr>
<tr>
<td>Solar Winds REaltime Netflow Analyzer</td>
</tr>
</tbody>
</table>
Lab Equipment

- There are “free” products & demo software available (Example IPS, ASA, ISE)
  - Cisco ASDM 713

- Home/Work lab environment is highly recommended

- Cisco Routers, Switches, and ASA
  - Two Cisco routers configured or at least one to emulate the Internet traffic.

- Your exam preparation should be around ASA, Routers, and Switches

- Similar to the old SECURE exam but includes basic ASA Firewall concepts now
Minimal Lab Solution

Stripped down Lab

- 1 ASA
- 1 Router
- 1 Switch
- 2 Servers and 2 PCs
SENSS 1.0 ILT—Lab Activities

- Lab 2-1: Configure Control and Management Plane Security Controls
- Lab 2-2: Configure Traffic Telemetry Methods
- Lab 2-3: Configure Layer 2 Data Plane Security Controls
- Lab 2-4: Configure Layer 3 Data Plane Security Controls
- Lab 3-1: Configure Cisco ASA NAT
- Lab 3-2: Configure Cisco IOS Software NAT
- Lab 4-1: Configure Basic Cisco ASA Access Policies
- Lab 4-2: Configure Advanced Cisco ASA Access Policies
- Lab 4-3: Configure Cisco ASA Botnet Traffic Filter
- Lab 4-4: Configure Cisco ASA Identity Firewall
- Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies
- Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies
Lab 2-1: Configure Control and Management Plane Security Controls

- Implement secure management using cryptographically protected protocols (SSH, SNMPv3)
- Configure Control Plane Protection (CPPr)
Lab 2-2: Configure Traffic Telemetry Methods

- Verify clock synchronization on devices
- Configure NTP, Logging, Netflow ( Flexible and Random Sampled) using ASDM
Lab 2-3: Configure Layer 2 Data Plane Security Controls

- Perform DHCP Snooping attack to show vulnerability
- Configure ARP inspections; ip-to-mac bindings are verified against DHCP snooping database, or, static ARP access list
- Configure DHCP snooping
Lab 2-4: Configure Layer 3 Data Plane Security Controls

- Attack internal host with spoofed IP address
- Configure u RPF to protect subnets
- Configure Source Guard to protect VLANs
Lab 3-1: Configure Cisco ASA NAT

- Configure fixed/static translations
- Configure dynamic NAT/PAT
- Monitoring in ASD and CLI
Lab 3-2: Configure Cisco IOS Software NAT

- Enabling Inbound and Outbound connectivity from certain sources to certain destinations/services
- CLI Commands:
  ✓ show ip nat translations
  ✓ show ip nat statistics
  ✓ debug ip nat
Lab 4-1: Configure Basic Cisco ASA Access Policies

- Configuring Network Object Groups
- Configure Service Object Groups
- Monitoring ACLs in ASDM and CLI
Lab 4-2: Configure Advanced Cisco ASA Access Policies

• Configure deep packet inspection for services that open channels on dynamically assigned ports (default vs secondary TCP/UDP ports)
• Commands:
  ✓ Show conn address x.x.x.x detail
  ✓ Show service policy
Lab 4-3: Configure Cisco ASA Botnet Traffic Filter

- Configure Botnet Traffic filter (using Dynamic or Static database)
- If Static Database, configure “Whitelist” destinations
- Enable DNS Inspection
Lab 4-4: Configure Cisco ASA Identity Firewall

- Configure CDA: mapping IP-addresses-to-Usernames
- Configure ASA for AD integration; LDAP on MS AD
- Configure Identity Based ACLS
Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies

- Configure Zones, Zone Pairs, and Policies
- Configure Class Maps, Policy Maps and ACLs
Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

- Configure parameter map of type “regex” - regular expression for argument matching
- ‘regex’ matches exe file extension
Reading Material & Resources
Firewall Guides

Cisco ASA 5500-X Series Next-Generation Firewalls

Content Security Services for Cisco ASA Series
Interfaces and Modules
Data Sheets and Literature
Models

End-to-End Network Intelligence
Your people need access to legitimate business applications while using their device of choice. But with that choice comes the need for greater visibility and control. Your business, regardless of size, can get an end-to-end network security solution with the Cisco ASA 5500-X Series Next-Generation Firewalls.

Start Here
Cisco dot com Resources

- No CCO login required to download the command references and configuration guides.

- No need to read these documents cover to cover, but they are essential as reference material during exam preparation.

- ‘Overview’ or ‘Information About’ section very helpful for each of the many topics and features covered on the exams.
Firewall Configuration Guides (46)


<table>
<thead>
<tr>
<th>Configuration Guides</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASA 9.1/ASDM 7.1</strong></td>
</tr>
<tr>
<td>Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1 Updated</td>
</tr>
<tr>
<td>Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1 Updated</td>
</tr>
<tr>
<td>Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.1 Updated</td>
</tr>
<tr>
<td>Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, 7.1 Updated</td>
</tr>
<tr>
<td>Book 2: Cisco ASA Series Firewall ASDM Configuration Guide, 7.1 Updated</td>
</tr>
<tr>
<td>Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.1 Updated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ASA 9.0 and Earlier</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA Series CLI Configuration Guide, 8.6</td>
</tr>
<tr>
<td>Cisco ASA 1000V Command Line Configuration Guide, 8.7</td>
</tr>
<tr>
<td>Cisco ASA Services Module CLI Configuration Guide, 8.5</td>
</tr>
<tr>
<td>Cisco ASA 5500 Series Configuration Guide using the CLI 8.4 and 8.6</td>
</tr>
<tr>
<td>Cisco ASA 5500 Series Configuration Guide using the CLI 8.3</td>
</tr>
<tr>
<td>Cisco ASA 5500 Series Configuration Guide using the CLI 8.2</td>
</tr>
<tr>
<td>Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x</td>
</tr>
</tbody>
</table>

Read these guides
Find the ones with the topics in the exam blueprint
Configuration Examples & Technotes (261)


- Initial Configuration
- AAA
- Allow and Block the Traffic Through the Security Appliance
- NAT and Access Lists
- ASDM
Search, Search, and Search Again!

• Many YouTube VODs out on the Internet contain good insight into Cisco ISE technologies. Search beyond CCNP material, for example: “ASA Firewall”…“ASA NAT 9.1”

• Not every document out on the Internet is 100% correct, so verify your findings, then share!!!

• Cisco Configuration documents are a good resource.
  • These documents provide valuable information into the theory behind different ASA configuration challenges and the solutions.
  • Key resource: for day-to-day work related problems and exam writers
Cisco Learning Network – Study Portal
Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

- Complete your session surveys through the Cisco Live mobile app or your computer on Cisco Live Connect.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at [CiscoLive.com/Online](http://CiscoLive.com/Online)
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions
Thank you