Experience Today the Network of Tomorrow.

CCIE Security Certification

Yusuf Bhaiji

Welcome to the Human Network.
## Agenda

<table>
<thead>
<tr>
<th>Session</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CCIE® Program Overview</td>
</tr>
<tr>
<td>2</td>
<td>CCIE® Security Overview</td>
</tr>
<tr>
<td>3</td>
<td>Firewall (Cisco PIX/ASA)</td>
</tr>
<tr>
<td>4</td>
<td>VPN</td>
</tr>
<tr>
<td>5</td>
<td>Cisco Intrusion Prevention System (IPS)</td>
</tr>
<tr>
<td>6</td>
<td>Identity Management</td>
</tr>
<tr>
<td>7</td>
<td>Advanced Security</td>
</tr>
<tr>
<td>8</td>
<td>Network Attacks</td>
</tr>
<tr>
<td>9</td>
<td>Preparation Resources and Test-Taking Tips</td>
</tr>
</tbody>
</table>
Disclaimer

- Not all the topics discussed today appear on every exam
- For time reasons, we’re unable to discuss every feature and topic possible on the exam
Session 1

CCIE Program Overview
Overview: CCIE Certification

- Highest regarded IT certification for over 15 years
- Industry standard for validating expert level skills and experience
- Exams continually updated and revised with new technologies
- Theoretical and intensive hands-on lab examination requirements
- Demonstrate strong commitment and investment in networking career, life-long learning, and dedication to remaining an active CCIE
CCIE Roadmap and Exam Basics
Overview: CCIE Tracks

Routing and Switching
• Core networking cert
• 74% of all bookings
• Labs in all regions, all worldwide locations

Security
• Introduced 2002
• Fastest growing cert; 13% of bookings
• Labs in Beijing, Brussels, RTP, San Jose, Sydney, Dubai, Bangalore and Tokyo

Voice over IP
• Introduced 2003
• 10% of bookings
• Labs in Brussels, San Jose, RTP and Sydney

Storage Networking
• Introduced Nov. 2004
• Labs in Brussels, RTP, San Jose

Service Provider Networks
• Introduced 2002
• 3% of bookings
• Labs in Brussels, Beijing, Hong Kong, RTP, Sao Paulo, Sydney

Wireless
• Introduced 2009
• X% of bookings
• Labs in Brussels, San Jose, Sydney

Available in Six Technical Specialties
### CCIE Information Worldwide

<table>
<thead>
<tr>
<th>Total of Worldwide CCIEs:</th>
<th>18,674*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total of Routing and Switching CCIEs:</td>
<td>16,399</td>
</tr>
<tr>
<td>Total of Security CCIEs:</td>
<td>2,007</td>
</tr>
<tr>
<td>Total of Service Provider CCIEs:</td>
<td>1,120</td>
</tr>
<tr>
<td>Total of Storage Networking CCIEs:</td>
<td>140</td>
</tr>
<tr>
<td>Total of Voice CCIEs:</td>
<td>872</td>
</tr>
</tbody>
</table>

*Updated 6-Jan-2009

#### Multiple Certifications

Many CCIEs Have Gone on to Pass the Certification Exams In Additional Tracks, Becoming a “Multiple CCIE.” Below Are Selected Statistics on CCIEs Who Are Certified in More Than One Track

<table>
<thead>
<tr>
<th>Total with Multiple Certifications Worldwide:</th>
<th>1,885</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total of Routing and Switching and Security CCIEs:</td>
<td>706</td>
</tr>
<tr>
<td>Total of Routing and Switching and Service Provider CCIEs:</td>
<td>472</td>
</tr>
<tr>
<td>Total of Routing and Switching and Storage Networking CCIEs:</td>
<td>35</td>
</tr>
<tr>
<td>Total of Routing and Switching and Voice CCIEs:</td>
<td>250</td>
</tr>
<tr>
<td>Total with 3 or More Certifications</td>
<td>302</td>
</tr>
</tbody>
</table>

---

Certification Process

- CCIEs must pass two exams
- The written qualification exam has 100 multiple-choice questions
- The lab exam is what makes CCIE different. The full-day, hands-on lab exam tests the ability to configure and troubleshoot equipment
- Not all lab exams are offered at all lab locations
Process: Steps to CCIE Certification

Routing/Switching: Written → LAB
Security: Written → LAB
Storage: Written → LAB
Service Provider: Written → LAB
Voice: Written → LAB
Wireless: Written → LAB
Session 2

CCIE Security Overview
CCIE Security Overview

- Security is one of the fastest-growing areas in the industry
- Information security is on top agenda to all organizations
- There is an ever-growing demand for Security professionals in the industry
- The CCIE Security certification was introduced in 2001 and has evolved into one of the industry’s most respected high-level security certifications
- Just around 2,000 CCIE Security worldwide
Input Sought From:

- Cisco Business Units/Technology Groups
  Cisco Standard Architectures (AVVID, SAFE)
- Advisory Subject Matter Experts
- Technical Support
  TAC Cases
  Technical Bulletins, Best Practices, Whitepapers
- Enterprise Technical Advisory Board
- Focus Groups/Customer Sessions
- CCIE Field Surveys

Reaching out to Extended Team Ensures Exam Is Realistic and Relevant

Content Manager

Content Advisory Group

CCIE Program Team

Exam Objectives and Blueprints

Welcome to the Human Network.
CCIE Security Written Exam

Welcome to the Human Network.
CCIE Security Written Exam

- Covers networking theory related to:
  - General Networking
  - Security Protocols
  - Application Protocols
  - Security Technologies
  - Cisco Security Appliances and Apps
  - Cisco Security Management
  - Cisco Security General
  - Security Solutions
  - Security General

- Lays foundation for Security lab exam
CCIE Security Written Exam

- The **CCIE Security v2.0 written exam** strengthens coverage of technologies critical to highly-secure enterprise networks.

- **New topics** such as ASA, IPS, NAC/ATD, CS-MARS, IPv6, security policies and standards are added to test candidates on the security technologies and best practices in use today.
CCIE Security Lab Exam
CCIE Security Lab Exam

- Candidates build a network to a series of supplied specifications
- The point values for each question are shown on the exam
- Some questions depend upon completion of previous parts of the network
- Report any suspected equipment issues to the proctor as soon as possible; adjustments cannot be made once the exam is over
Security Lab Exam: Locations

Nine Worldwide CCIE Lab Locations for Security
CCIE Security Lab Exam

- The CCIE Security lab exam content was revised and new exam format delivery started on January 2\textsuperscript{nd} 2007, to include some of the current trends and technologies in the security industry.

- New topics on security appliances such as PIX, IPS and VPN3000 were introduced.

- In addition, the ASA5500 security appliance was added, and CiscoSecure ACS Configuration is now also required, along with other items added to test candidates on the security technologies and best practices in use today.
Security Lab Exam: Equipment and Cisco IOS Versions

Lab May Test Any Feature that Can Be Configured on the Equipment and Cisco IOS Versions Listed Below, or on the CCIE Website; More Recent Versions May Be Installed in the Lab, But You Won’t Be Tested on Them

- Six Routers (26xx/36xx/37xx) running Cisco IOS version 12.2T
- Two Cisco Catalyst 3550 Series switches running 12.2SEE
- Two ASA5500 Series Firewalls running version 7.2.x
- One PIX 500 Series Firewall running version 7.2.x
- One VPN 3000 Series Concentrator running version 4.7.x
- One IPS 4200 Series Sensor Appliance running version 5.1.x
- One Cisco Secure ACS version 4.x
- One Test PC for Testing and Troubleshooting
- One Candidate PC for rack access
Security Lab Exam: Blueprint

- Section 1  Firewall
- Section 2  VPN
- Section 3  IPS
- Section 4  Identity Management
- Section 5  Advanced Security
- Section 6  Network Attacks
Security Lab Exam: Pre-Configuration

The Routers and Switches in Your Topology Are Preconfigured with:

- Basic IP addressing, hostname, passwords
- Switching: Trunking, VTP, VLANs
- Frame Relay: DLCI mapping (static/dynamic)
- Core Routing: OSPF, RIP, EIGRP, BGP
- All pre-configured passwords are ‘cisco’

Security Devices (PIX, VPN3000, IDS) Are Not Initialized. Candidate Is Required to Do So

Do Not Change Any Pre-Configuration on Any Devices Unless Explicitly Stated in a Question
Security Lab Exam: Sample Topology

ASA Multi-Context with Failover

BB1

Context 1

ASA1

ASA2

Context 2

BB2

FR

Welcome to the Human Network.
Security Lab Exam: Grading

- Proctors grade all lab exams
- Automatic tools aid proctors with simple grading tasks
- Automatic tools are never solely responsible for lab exam grading—proctors are
- Proctors complete grading of the exam and submits the final score within 48 hours
- Partial credit is not awarded on questions
- Points are awarded for working solutions only
- Some questions have multiple solutions
Summary
Topics Covered More Heavily in the Exams:
- Firewalls (hardware and software)
- VPNs
- Intrusion protection
- Identity authentication
- Advanced security technologies
- Mitigation techniques to respond to network attacks
CCIE Security Lab Exam Revision
Security Lab Exam: Changes

- The CCIE Security Lab exam content is scheduled to be revised, to include some of the current trends and technologies in the security industry

- New topics and hardware & software upgrades will be introduced

- End-of-Life devices will be removed;
  - PIX500 and VPN3000 will be removed
  - Routers will be replaced with new ISR series
  - 3550 Switches will be replaced with new 3560
Security Lab Exam: Equipment and Software Versions

- Cisco Integrated Services Routers (ISR) series running Cisco IOS version 12.4T
- Cisco Catalyst 3560 series switches running 12.2(x)SE
- Cisco ASA 5500 series Firewalls running version 8.x
- Cisco IPS 4240 Appliance Sensor running version 6.x
- Cisco Secure ACS version 4.1
- Test PC for Testing and Troubleshooting
- Candidate PC for rack access
Security Lab Exam: Blueprint

- Implement secure networks using Cisco ASA Firewalls and Cisco IOS Firewalls
- Implement secure networks using Cisco VPN solutions
- Configure Cisco IPS to mitigate network threats
- Implement Identity Management solutions
- Implement Control Plane and Management Plane Security
- Configure Advanced IOS Security
- Identify and Mitigate Network Attacks
Session 3

Firewall (Cisco PIX/ASA)
Cisco Firewalls

- Cisco PIX Firewall
  - Firewall Appliance
- Cisco IOS Firewall (CBAC)
  - Router integrated Firewall
- Firewall Service Module (FWSM)—(Not in Lab exam)
  - Switch integrated Firewall
- Adaptive Security Appliance (ASA)
  - Multi-function (FW, VPN, IPS) Security Appliance
Cisco PIX 7.0 and ASA 7.0

- Same Binary image file supports both platform
- Same ASDM image file supports both platform
  (ASDM is not allowed in the Lab Exam, only CLI)
- 501/506E are NOT supported under 7.0
- PIX 7.0 does not support following features but offered by ASA 7.0
  - Web VPN
  - VPN LB
  - SSM related (IPS)
  - CF card support
  - AUX port support
Cisco PIX/ASA Firewalls
What Is a Firewall?

- A system that implements a network security policy between segments of a network
  
  Firewalls are security policy enforcement points

- Without a security policy, the availability of your network can be compromised
  
  And it is very difficult to configure your firewall
Stateful Firewall Algorithms

- Recognizes the “stateful” nature of TCP/IP protocols
- Using a state table the firewall can track:
  - Source and destination IP addresses and ports
  - TCP sequence numbers
  - The state of each TCP and UDP session
  - Additional flags and fields
- But isn’t UDP a “stateless” protocol?
  - Builds artificial connection state for UDP and tracks traffic timeouts
- Supports authentication, authorization, syslog
Interface and Security Levels

- Inside Interface always has a security level of 100. Most Secure level
- Outside Interface always has a security level of 0. Least Secure level
- Multiple perimeter networks can exist. Use DMZ Interface. Security levels between 1–99
Initializing Cisco PIX/ASA

- Firewall Mode (Router/Transparent)
- Single/Multiple Context
- Enable/Allocate interfaces
- Assign IP address for each active Interface
- Un-shut Interfaces
- Configure Address Translation (optional)
- Configure Routing
Address Translation
Subject to NAT-Control

- Dynamic translations are built using:
  
  Network Address Translation (NAT)
  (one-to-one mapping)

  or

  Port Address Translation (PAT)
  (many-to-one mapping)

- Static translations are built using:
  
  Static command
  (create permanent mapping between a local IP address and a global IP address)
Policy NAT

- Policy NAT lets you identify local traffic for address translation by specifying the **source and destination addresses** (or ports) in an access list.

- Regular NAT uses source addresses/ports only, whereas policy NAT uses both source and destination addresses/ports.

- With policy NAT, you can create multiple static statements that identify the same local address as long as the source/port and destination/port combination is unique for each statement.

- Use an **access list** with the static command to enable policy NAT.
Object Grouping

- Used for simplifying complex access control policies. Object grouping provides a way to reduce the number of access rule entries required to describe complex security policies.

- Following types of objects:
  - **Protocol**—group of IP protocols. It can be one of the following keywords: icmp, ip, tcp, or udp, or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword ip.
  - **Service**—group of TCP or UDP port numbers assigned to different services
  - **icmp-type**—group of ICMP message types to which you permit or deny access
  - **Network**—group of hosts or subnets
Routing

- PIX/ASA supports RIP and OSPF routing protocols
- Both protocols support clear text and MD5 authentication
- Practice route filtering and summarization for both protocols
- Running both OSPF and RIP concurrently on the same Firewall is now supported
VLAN

- Virtual LANs (VLANs) are used to create separate broadcast domains within a single switched network.
- You can configure multiple logical interfaces on a single physical interface and assign each logical interface to a specific VLAN.
- PIX/ASA supports 802.1q, allowing it to send and receive traffic for multiple VLANs on a single interface.
Basic Feature Summary: Practice Them All

- Address Translation
- AAA
- VPN IPsec
- PPTP
- TCP Intercept
- RIP
- OSPF
- Syslog
- Failover
- Java Filtering
- ActiveX Filtering
- Packet Capture
- VLAN
- Object Grouping
- DHCP
- PPPoE
- URL Filtering
- IDS
- SSH
- SNMP
- NTP
- Policy NAT
New Firewall Features in v7.0

- Virtual Firewall (Security Contexts)
- Transparent Firewall
- Modular Policy Framework (MPF)
- Application Firewall
- High Availability FO
- No NAT-Control
- Access-Group Keyword: OUT
- Access-List Keyword: TIME-RANGE
- VPN Hub-and-Spoke/Spoke-to-Spoke Enhancement
Troubleshooting Firewall
Firewall Troubleshooting Tools

- Understanding the packet flow
- Syslog
- Debug commands
- Show commands
- Packet capture
Understanding the Packet Flow

- To effectively troubleshoot a problem, one must first understand the packet path through the network.
- Attempt to isolate the problem down to a single device.
- Then perform a systematic walk of the packet path through the device to determine where the problem could be.
- For problems relating to the PIX, always:
  - Determine the flow: SRC IP, DST IP, SRC port, DST port, and protocol.
  - Determine the interfaces through which the flow passes.

Note: All Firewall Issues Can Be Simplified to Two Interfaces (Ingress and Egress) and the Rules Tied to Both.
Example Flow

- **Flow**
  - SRC IP: 10.1.1.9
  - DST IP: 172.16.1.5
  - SRC Port: 11030
  - DST Port: 8080
  - Protocol: TCP

- **Interfaces**
  - SRC Interface: Inside
  - DST Interface: DMZ

With the Flow Defined, Examination of Config Issues Boils Down to Just the Two Interfaces: Inside and DMZ.
Once the Device and Flow Have Been Identified, Walk the Path of the Packet Through the Device

Welcome to the Human Network.
Translation and NAT Order of Operations

1. nat 0 access-list (nat-exempt)
2. Match existing xlates
3. Match static commands (first match)
   a. Static NAT with and without access-list
   b. Static PAT with and without access-list
4. Match nat commands
   a. nat <id> access-list (first match)
   b. nat <id> <address> <mask> (best match)
      i. If the ID is 0, create an identity xlate
      ii. Use global pool for dynamic NAT
      iii. Use global pool for dynamic PAT
Debug ICMP Trace

- Valuable tool used to troubleshoot connectivity issues
- Provides interface and translation information to quickly determine flow
- Echo-replies must be explicitly permitted through ACL

Example `debug icmp trace output`

```
ICMP echo-request from inside:10.1.1.2 to 198.133.219.25 ID=3239 seq=4369 length=80
ICMP echo-request: translating inside:10.1.1.2 to outside:209.165.201.22

ICMP echo-reply from outside:198.133.219.25 to 209.165.201.22 ID=3239 seq=4369 length=80
ICMP echo-reply: untranslating outside:209.165.201.22 to inside:10.1.1.2
```
Show Traffic
The Show Traffic Command Displays the Traffic Received and Transmitted out Each Interface of the PIX

pixfirewall# show traffic
outside:
    received (in 124.650 secs):
        295468 packets  167218253 bytes
        2370 pkts/sec  1341502 bytes/sec
    transmitted (in 124.650 secs):
        260901 packets  120467981 bytes
        2093 pkts/sec  966449 bytes/sec
<..>
inside:
    received (in 124.650 secs):
        261478 packets  120145678 bytes
        2097 pkts/sec  963864 bytes/sec
    transmitted (in 124.650 secs):
        294649 packets  167380042 bytes
        2363 pkts/sec  1342800 bytes/sec
Show Local-Host

- A local-host entry is created for any source IP on a higher security level interface
- It groups the xlates, connections, and AAA information together
- Very useful for seeing the connections terminating on servers

PIX# show local-host
Interface inside: 1131 active, 2042 maximum active, 0 denied
local host: <10.1.1.9>,
   TCP connection count/limit = 1/unlimited
   TCP embryonic count = 0
   TCP intercept watermark = 50
   UDP connection count/limit = 0/unlimited
AAA:
   user 'cisco' at 10.1.1.9, authenticated (idle for 00:00:10)
      absolute timeout: 0:05:00
      inactivity timeout: 0:00:00
Xlate(s):
   Global 172.18.124.69 Local 10.1.1.9
Conn(s):
   TCP out 198.133.219.25:80 in 10.1.1.9:11055 idle 0:00:10 Bytes 127 flags UIO
Show Xlate and Show Xlate Debug

```
show xlate [global|local <ip1[-ip2]> [netmask <mask>]]
[gport |lport <port1[-port2]>] [debug]
```

PIX# show xlate
2 in use, 2381 most used
Global 172.18.124.68 Local 10.1.1.9
PAT Global 172.18.124.65(1024) Local 10.9.9.3(11066)

PIX# show xlate debug
2 in use, 2381 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
o - outside, r - portmap, s - static

NAT from inside 10.1.1.9 to outside 172.18.124.68
  flags - idle 0:02:03 timeout 3:00:00

TCP PAT from inside:10.9.9.3/11066 to outside:172.18.124.65/1024
  flags r idle 0:00:08 timeout 0:00:30
### Show Conn and Show Conn Detail

**PIX# show conn**

2 in use, 64511 most used

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Flags</th>
<th>Idle Time</th>
<th>Bytes Transferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>198.133.219.25:23</td>
<td>10.9.9.3:11068</td>
<td>idle 0:00:06</td>
<td>Bytes 127</td>
<td>flags UIO</td>
</tr>
<tr>
<td>UDP</td>
<td>172.18.124.1:123</td>
<td>10.1.1.9:123</td>
<td>idle 0:00:13</td>
<td>flags -</td>
<td></td>
</tr>
</tbody>
</table>

**PIX# show conn detail**

2 in use, 64511 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN, B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN, G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data, i - incomplete, J - GTP, j - GTP data, K - GTP t3-response, k - Skinny media, M - SMTP data, m - SIP media, O - outbound data, P - inside back connection, q - SQL*Net data, R - outside acknowledged FIN, R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN, s - awaiting outside SYN, T - SIP, t - SIP transient, U - up

TCP outside:198.133.219.25/23 inside:10.9.9.3/11068 flags UO
UDP outside:172.18.124.1/123 inside:10.1.1.9/123 flags -
Packet Capture

- Capture command first introduced in PIX 6.2; it deprecates the “debug packet” command

- Capture sniffs packets on an interface that match an ACL

- Key steps:
  - Create an ACL that will match interesting traffic
  - Define the capture and bind it to an access-list and interface
  - View the capture on the PIX, or copy it off in pcap format
Session 4

VPN
Virtual Private Network (VPN) Defined

“A Virtual Private Network carries private traffic over public network.”
Network Security

Data Security Assurance Model (CIA)

Confidentiality
- Benefit: Ensures data privacy
- Shuns: Sniffing, Replay

Integrity
- Benefit: Ensures data is unaltered during transit
- Shuns: Alteration, Replay

Authentication
- Benefit: Ensures identity of originator or recipient of data
- Shuns: Impersonation, Replay
What Is IPsec?
Internet Protocol Security

- A set of security protocols and algorithms used to secure IP data at the network layer

- IPsec provides data confidentiality (encryption), integrity (hash), authentication (signature/certificates) of IP packets while maintaining the ability to route them through existing IP networks
Encryption Layers

Application-Layer (SSL, PGP, S-HTTP, SSH)

Network-Layer (IPsec)

Link-Layer Encryption (KG, KIV)

Application Layers (5–7)

Transport/Network Layers (3–4)

Link/Physical Layers (1–2)
Understanding IPsec
IPsec

- IPsec can ensure the confidentiality and/or the authenticity of IP packets

- The key points are
  - Two modes of propagation (transport and tunnel)
  - Security associations (SAs)
  - Two types of header (ESP and AH)

- IPsec does not provide a key exchange mechanism
IKE (Phase 1)

IPsec (Phase 2)

Data

IPsec: Building a Connection

- Two-phase protocol:
  - Phase 1 exchange: two peers establish a secure, authenticated channel with which to communicate; Main mode or Aggressive mode accomplishes a Phase 1 exchange.
  - There is also a Transaction Mode in between which is used for EzVPN client scenario performing XAUTH and/or Client attributes (Mode Config).
  - Phase 2 exchange: security associations are negotiated on behalf of IPsec services; Quick mode accomplishes a Phase 2 exchange.

- Each phase has its SAs: ISAKMP SA (Phase 1) and IPsec SA (Phase 2)
Implementing IPsec
IPsec Scenarios

Site-to-Site Hub-and-Spoke

Site-to-Site Partial Mesh

Site-to-Site Full Mesh

Remote Access

Welcome to the Human Network.
IPsec Scenarios

- Router to Router
- PC to Firewall
- One Router (or Firewall) to Many
- PC to Router
IPsec/GRE: Scalable Site-to-Site VPNs

- Routing Protocol (OSPF, EIGRP…) necessary
- Routing (or multicast) not specified by IPsec
- Supported in Cisco IOS using GRE/IPSec
IPsec Remote Access (EzVPN)

- Client-server architecture
- Client always initiates IPsec connection
- Client may have dynamic IP address
- Very easy to configure
- Very scalable, no routing expertise required
IPsec Remote Access (EzVPN) (Cont.)

- **Client extension mode:**
  
Packets from all devices behind EzVPN Client are PATed to one ip address (then tunneled in IPsec)

- **Network extension mode:**
  
Packets from all devices behind EzVPN client are tunneled in IPsec (no PAT before IPsec)
Dynamic Multipoint VPN (DMVPN)

What Is DMVPN?

- It is GRE, NHRP and IPsec mix
- NHRP allows the peers to have dynamic addresses (Dial, DSL, ...) with GRE/IPSec tunnels
- The backbone is a hub and spoke topology
- It allows direct spoke to spoke tunneling by auto leveling to a partial mesh
Dynamic Multipoint VPN (DMVPN)

- Yellow = Dynamic and Permanent Spoke-to-Hub IPsec Tunnels
- Green = Dynamic and Temporary Spoke-to-Spoke IPsec Tunnels

10.1.0.0 255.255.255.0
10.1.1.0 255.255.255.0
10.1.1.1
10.1.0.1
130.25.13.1
10.1.2.0 255.255.255.0
10.1.2.1
10.1.3.0 255.255.255.0
10.1.3.1
10.1.0.0 255.255.255.0
10.1.1.0 255.255.255.0
10.1.1.1
10.1.0.1
130.25.13.1
10.1.2.0 255.255.255.0
10.1.2.1
10.1.3.0 255.255.255.0
10.1.3.1

Dynamic (or Static) Public IP Addresses

Welcome to the Human Network.
High-Availability Designs: Stateless Options

IPsec and HSRP + with Reverse Route Inj. (RRI)

IPSec/GRE: Routing Protocols

IPsec and Dead Peer Detection (DPD)

Cisco Expo 2009

Welcome to the Human Network.
Practice IPsec
Practice Every Possible Scenario and Combination

- IPsec LAN-to-LAN using pre-shared and certificates
  - Cisco IOS
  - PIX/ASA
  - VPN 3000

- IPsec remote access using pre-shared and certificates
  - Cisco IOS
  - PIX/ASA
  - VPN 3000
Practice IPsec Features

- Reverse Route Injection (RRI)
- Split Tunnel
- Xauth/Mode config
- RADIUS
- NAT-T (IPsec over TCP/UDP)
- IPsec and NAT
- SSL VPN
- Fragmentation and PMTU Discovery
- QoS
- DMVPN/mGRE/NHRP
- High Availability scenarios
Troubleshooting IPsec
Troubleshooting IPsec
Determine the Problem Characteristics

- Is the problem in connection establishment?
  - Phase 1 failure
  - Transaction Mode/XAUTH
  - Phase 2 failure

- Is the problem in passing traffic?
  - All traffic
  - Specific traffic
Always Use Show Command Before Debug

show crypto isakmp sa
show crypto ipsec sa
show crypto engine connection active

Important Show

Show Functionality Flowchart

Interesting Traffic Received
Main Mode IKE Negotiation
Quick Mode Negotiation
Establishment of Tunnel

Welcome to the Human Network.

IKE
IPsec
Data
Debug Commands

Important Debugs
- debug crypto isakmp
- debug crypto ipsec
- debug crypto engine

Debug Functionality Flowchart
- Interesting Traffic Received
- Main Mode IKE Negotiation
- Quick Mode Negotiation
- Establishment of Tunnel
  - IKE
  - IPsec
  - Data

Welcome to the Human Network.
Common Mistakes
Common Mistakes

- Incompatible ISAKMP Policy
- Incompatible Preshared Secrets
- Incompatible Transform Sets
- Incompatible or Incorrect Access Lists
- Crypto Map on the Wrong Interface
- Incorrect SA Selection by the Router
- Routing Issues
- NAT with IPsec
- Firewall and ACLs
Session 5

Intrusion Prevention Systems (IPS)
IPS Terminology: The Marketing of IPS/IDS

- **IDS** Intrusion Detection System—Typically limited to promiscuous sensors (out of packet stream)
- **IPS** Intrusion Prevention/Protection System—The term most commonly applied to a sensor that sits inline (in the packet stream) and can drop malicious packets, flows or attackers
- **IDP** Intrusion Detection and Prevention—Marketing term coined by a vendor for product differentiation
IPS Terminology: What Is IPS?

Different Understandings of “What Is IPS?”

- **IPS feature vs. IDS feature**—The IPS feature is specifically inline monitoring with “deny packet” capability (but not necessarily used) while IDS feature is promiscuous-only monitoring with post attack response actions (TCP reset or block on external device).

- **Cisco IPS software vs. Cisco IDS software**—IPS software is usually capable of both inline (IPS feature) and promiscuous (IDS feature) monitoring while IDS software is only capable of promiscuous (IDS feature) monitoring; Cisco v5.0 vs v4.x software versions.

- **Cisco IPS hardware vs. Cisco IDS hardware**—IDS hardware is generally designed with only one port for promiscuous monitoring; to get inline monitoring typically requires addition of an interface card; IPS hardware is designed for inline operations; typically two or more sensing ports by default.
IPS Terminology: What Is IPS? (Cont.)

IPS Closely Resembles a Layer 2 Bridge or Repeater

- “Identical to a wire” is the closest analogy
- Inline interfaces have no MAC or IP and cannot be detected directly
- Network IPS passes all packets without directly participating in any communications including spanning tree (but spanning tree packets are passed)
- Default behavior is to pass all packets even if unknown, (i.e. IPX, Appletalk, etc.) unless specifically denied by policy or detection
IPS Terminology: Signatures and Anomalies

- **Signatures** explicitly define what activity should be considered malicious
  - Simple pattern matching
  - Stateful pattern matching
  - Protocol decode-based analysis (including protocol anomalies)
  - Heuristic-based analysis

- **Anomaly** detection involves defining or learning “normal” activity and looking for deviations from this baseline
IPS Terminology: Signature Implementations and Structures

- **Signature implementation**
  - Context—trigger data contained in packet header
  - Content—trigger data contained in packet payload

- **Signature structure**
  - Atomic—trigger contained in a single packet
  - Composite—trigger contained in a series of multiple packets
Network-Based IDS: The Sensor

Network Link to the Management Console

IP Address

Promiscuous Interface: No IP Address

Data Capture

Monitoring the Network

Data Flow

Welcome to the Human Network.
Network-Based IPS: The Sensor

Network Link to the Management Console

Management Interface: IP Address

Data Flow

Transparent Interfaces: No Mac or IP Address
Initializing the Sensor

- Default username/password will be changed in the lab exam. Follow the instructions/guidelines in your workbook. In most cases, username and password will be set to `cisco/123cisco123`. Do not change this user credentials, else; you will lose all points.

- Configure **basic parameters** such as the host name, IP address, netmask, gateway and communications options.

- Use IDS Device Manager (IDM) to browse the sensor management IP address to complete remaining exam.
Scaling Analysis: Signature Engines

- Cisco IPS analysis implemented with a series of engines that each inspect for a specific type of activity

- Signature engine types:
  - Atomic
  - Meta
  - State
  - Sweep
  - Flood
  - Service
  - String
  - Trojan
  - Traffic
  - Normalizer
  - AIC
  - Other
Signature Tuning

- Sensors are shipped with default signature configuration
- Signature specific:
  - Ports, protocols, services, analysis length, etc.
- Filtering: what networks to alarm on
- Event count: number of events to see before alarm
- Severity: what level of alarm to send
- Alarm aggregation: how many alarms to send
  - Summary mode: fire all, summarize, global summarize
  - Summary interval: summarization window
  - Summary threshold: high water mark to change summarization
- Event action: what to do following when the sig is triggered (includes producing an alert)
Custom Signatures

- Customize vendor-provided signatures
  For example, if a web signature is set to watch TCP 80, and you’re running a web server on TCP8080, you can change the signature to also watch that port

- New environment specific signatures can be created

- Custom signature configuration tasks:
  1. Select the signature micro-engine that best meets your requirements
  2. Enter values for the signature parameters that are required and meet your requirements
  3. Save and apply the custom signature to the sensor
Active Response: IPS

- A sensor deployed in IPS mode operates on the actual network packets instead of copies
  
  Multiple different deny actions are possible in addition to all actions supported in IDS mode
  
  Deny attacker
  Deny connection
  Deny packet

- Actions configurable per signature
TCP Resets

- For TCP applications, connection is prematurely terminated by a RST sent from “sensing” interface

- Must guess correct TCP sequence number and successfully insert RST into session
  
  Makes TCP resets somewhat unreliable especially when source and destination are “close”

- Certain applications will automatically reconnect and resend (e.g., SMTP), making this less effective

- Note that initial trigger packet will make it to its destination, so can’t necessarily stop event
  
  Code red 1 was a single packet attack and couldn’t be reset

- **Conclusion:** TCP resets are a temporary solution while you readjust your security posture
Blocking (Shunning)

- When signature fires, sensor inserts ACL on router/issues shun command on firewall
  
  Deny subsequent traffic from that source IP address or associated with that specific connection

  Note that initial trigger packets will make it to the destination because of the time required to establish the block

- Sensor connects to firewall and/or router from management interface

  Need to configure authentication credentials for firewall/router

- Conclusion: Blocking can be effective at stopping an infected host but can’t stop first attack
IPS Appliance Deployment Examples

IPS Appliance Sensor Deployment Examples:

- Two L2 devices (non trunk)
- Two L3 devices
- Bridging 2 VLANs on same switch
- Two L2 devices (trunked; 802.1q)
Inline-on-a-Stick or VLAN Pairing

- VLAN pairing allows a sensor to bridge VLANs together on the same physical interface by creating, in effect, sub-interfaces that allow the sensor to bring packets in on VLAN X and out on VLAN Y.

- Multiple VLAN pairs per physical interface reduces the need to have many physical interfaces per chassis.

Diagram:

Inline on a Stick or VLAN Pairing
Int GigEth1:Vlan X<->Y

VLAN X
VLAN Y
Trunk port allowing VLAN’s X and Y
Useful Show Commands on IDS Console

- show statistics eventStore
- show events alert {high|medium|low}
- show events status
- show interface
- show configuration
- show version
- show statistics
Session 6

Identity Management (AAA)
AAA Overview

- Authentication, Authorization, and Accounting (AAA) network security services provide the primary framework through which you set up access control.

- The CiscoSecure ACS uses authentication, authorization, and accounting (AAA) to provide network security. Each facet of AAA significantly contributes to the overall security of your network:
  
  Authentication determines the identity of users and whether they should be allowed access to the network.
  
  Authorization determines the level of network services available to authenticated users after they are connected.
  
  Accounting keeps track of each user’s network activity.
RADIUS vs. TACACS+

RADIUS

- RADIUS uses UDP port 1645/1646 and as per RFC 2138; 1812/1813
- RADIUS encrypts only the password in the packet
- Single challenge response
- Combines authentication and authorization
- Industry standard (created by Livingston)
- Does not support command authorization

TACACS+

- TACACS+ uses TCP port 49
- TACACS+ encrypts entire packet
- Multiple challenge response
- Uses the AAA architecture and separates each process
- Cisco proprietary
- Supports command authorization
CiscoSecure ACS

- CiscoSecure ACS Server supports both RADIUS and TACACS+ protocols
- ACS is not pre-configured in the lab exam; candidates are required to configure all aspects of ACS system.
- Full access will be provided for configuration, verification and troubleshooting purpose
- How to bring up ACS GUI remotely?
  http://ip_address:2002
CiscoSecure ACS: Connection Method

http://ACS_ip_address:2002

Candidate PC

CiscoSecure ACS

CCIE Backbone

Candidate Switch

Your Network

Test PC

Welcome to the Human Network.
Device Management

- **Practice** device management using AAA on router and Cisco Catalyst switches equally
- Device management via Telnet, SSH, HTTP/HTTPS are the most *commonly* authenticated protocols
- Console/Aux port should not be affected by any AAA commands unless otherwise specified
- Device management can be performed on all devices such as routers, Cisco Catalyst switches, PIX and VPN3000 (IDS does not support AAA)
- **TACACS**+ gives you the best control for managing a device by allowing you to restrict commands used while on the device using various privilege levels
Command Authorization

- A device can be configured to authorize commands through a AAA server at all or specific levels.
- The following router configuration allows all users to have per-command authorization set up on the server.
- Here we authorize all commands through CiscoSecure ACS using TACACS+; but if the AAA server is down, fallback authorization is set to local database.
- Example:

  ```
  aaa authorization commands 1 default group tacacs+ local
  aaa authorization commands 15 default group tacacs+ local
  ```
VPN3000 Management

- Configure AAA servers to authenticate administrators. VPN3000 can be configured to govern the level of access for administrators authenticated by a TACACS+ server (be sure that any servers you reference are properly configured).

- Authentication is performed when a user browses via **HTTP/HTTPS**

- This method does not provide security for console access of the VPN3000 concentrator. Console port is **not** affected and is your backdoor if the AAA does not respond.

- Default username and password is **admin/admin**
PIX/ASA Management

- AAA support is available to authenticate Telnet, SSH and Console access on PIX/ASA using TACACS+ and RADIUS

- Make sure you can Telnet from the inside network to the inside interface of the PIX/ASA without any AAA authentication

- PIX/ASA command authorization and expansion of local authentication was introduced in version 6.2

- Commands performed may be controlled locally on the firewall or remotely through TACACS+
Cisco PIX/ASA Service Authentication

- RADIUS and TACACS+ **authentication** can be done for HTTP, HTTPS, FTP, Telnet, SSH, and ICMP connections through the Firewall using AAA.

- Authentication for other less common protocols, non-standard services and/or other TCP/UDP ports can also be made to work using tcp/<port> and udp/<port>.

- Note that TACACS+ **authorization** is supported, however, RADIUS authorization is not.
AAA Test Command

- AAA test command provides protocol connectivity test from the NAS to the RADIUS/TACACS+ server. It validates if the NAS can establish connectivity with the server using RADIUS/TACACS+ ports.

- At times, the ‘test aaa’ may yield a failed result even if the ping (ip connectivity) is successful. Why?

- Example:

  Router# test aaa group tacacs+ testuser mypassword legacy
  Attempting authentication test to server-group tacacs+ using tacacs+
  User was successfully authenticated

  or

  Router# test aaa group radius testuser mypassword legacy
  Attempting authentication test to server-group radius using radius
  User was successfully authenticated
Troubleshooting AAA

- `debug aaa authentication`
- `debug aaa authorization`
- `debug aaa accounting`
- `debug radius`
- `debug tacacs`
- `test aaa group radius|tacacs+ username pwd legacy`
Session 7

Advanced Security
Disable Ports Not Used on the Router?

- `show ip sockets`—show some of the UDP ports opened
- Two steps required for TCP ports:
  
  - `show tcp brief all`
  
  - `show tcp tcb`
Global Services That Should Be Disabled

Some Services, Turned On by Default, Should Be Turned Off to Save Memory and Prevent Security Breaches/Attacks

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
Interface Services You Turn Off
All Interfaces on a Backbone Router Should Have the Following as a Default:

- no ip redirects
- no ip directed-broadcast
- no ip proxy-arp
- no ip source-routing
VTY Security

- Control is done via access lists
- Authentication: local password, TACACS+, RADIUS
- Transport mechanism should be SSH

Need to run crypto image for SSH
SNMP

- Change your community strings; do not use public, private, secret
- Use different community strings for the RO and RW communities
- Use mixed alphanumeric characters in the community strings: SNMP community strings can be cracked, too
- Turn off SNMP if it isn’t needed:
  - Cisco IOS: no snmp-server
- Block SNMP access to outsiders
ICMP Message Types
Control the Direction of a Ping

access-list 111 permit icmp any 10.1.1.0 0.0.0.255 echo-reply

interface Serial 0
access-group 111 in

Summary of ICMP Message Types

0  Echo Reply
3  Destination Unreachable
4  Source Quench
5  Redirect
8  Echo
11  Time Exceeded
12  Parameter Problem
13  Timestamp
14  Timestamp Reply
15  Information Request
16  Information Reply
IP Spoofing

- Hacker claims he is one of the inside hosts
- Inside host may have a trust relationship with spoofed host
IP Spoofing: How to Avoid It

- Deny incoming packets if source address is one of yours
- Deny outbound packets if source address is not one of yours
Unicast Reverse Path Forwarding (uRPF)

- Mitigates source address spoofing by checking that a packet’s return path uses the same interface it arrived on.
- Source IP packets are checked to ensure that the route back to the source uses the same interface.
- Requires CEF.
- Not always appropriate where asymmetric paths exist.

```
ip cef
!
interface Serial 0
  ip verify unicast (reverse-path | source reachable-via rx | source reachable-via any) <ACL_Number>
```
Packet-Marking and Classification

Packets Are Marked at the Edge, for Purposes of Classification in the Core

The IPv4 Header and the Type of Service (ToS) Byte
Class-Based Weighted Fair Queuing (Modular QoS CLI—MQC)

- Traffic is queued by user defined classes
- A queue is reserved for each class
- Queue uses tail drop or WRED
- Unclassified traffic is flow-based
NBAR: Network-Based Application Recognition

- NBAR is used for classifying traffic
  - Classification of applications that dynamically assign TCP/UDP port numbers
  - Classification of HTTP traffic by URL, HOST, or Multipurpose Internet Mail Extension (MIME) type
  - Classification of application traffic using sub-port information

- Use the classification in conjunction with CAR or traffic policing
NetFlow

- Provides network administrators with “packet flow” information
- Allows for:
  - Traffic flow analysis
  - Security monitoring
  - Anomaly detection
Enabling NetFlow

- Receive NetFlow information only on the specific interface(s) of interest
- Typical use case for NetFlow: Accounting, Security and Capacity Planning

Router(config-if)# ip flow ingress

- Starting Cisco IOS v12.2(15)T a simple “ip flow ingress” interface command starts collecting NetFlow data on that interface

This New Command Was Added in Cisco IOS v12.2(15)T
Older Command “ip route-cache flow” Also Enables Ingress NetFlow on the Interface but Should No Longer Be Used
Cisco Catalyst Security and Advance Features

Practice Cisco Catalyst Security Features; Some Examples Are:

- Port Security
- BPDU/Root Guard
- 802.1x
- Router ACLs, Port ACLs, VLAN ACLs
- AAA on Switch
- Traffic Control
- EtherChannels
- 802.1Q and Layer 2 Protocol Tunneling
- SPAN, RSPAN
Session 8

Network Attacks
Proactive vs. Reactive

The Questions in this Section of the Exam Are Mainly Focused on Reactive Measures

- Focus on techniques used to mitigate network attacks
- Same tools and techniques are used as discussed in previous section “Advanced Security”
- Questions will also test knowledge of protocols, e.g. TCP, HTTP, ICMP
- Questions will also test knowledge of Headers and standard packet format, e.g. TCP Header
- Questions will also test knowledge of reading packet captures and various show and debug outputs
Common Attacks

- Network reconnaissance
- Denial of Service (DoS)
- IP spoofing
- DHCP snooping
- DNS spoofing
- MAC spoofing
- ARP snooping
- Fragment attack
- Smurf attack
- TCP SYN attack
Knowledge of Protocols

- Traffic Characterization
- Packet Classification
- Marking Techniques
- Identifying Attack Patterns
- Understanding Attack Vectors
  
  Example: SYN, TCP/UDP options, ICMP Type/Code

- Common Protocol and Port Numbers
Understanding Protocol Headers

- Understanding & Interpreting ARP Header Structure
- Understanding & Interpreting IP Header Structure
- Understanding & Interpreting TCP Header Structure
- Understanding & Interpreting UDP Header Structure
- Understanding & Interpreting ICMP Header Structure
- Understanding & Interpreting ICMP Type/Code
- Understanding & Interpreting SYSLOG Messages
- Understanding & Interpreting Sniffer Capture Outputs
Mitigation Using Various Techniques

- Preventing SYN Attack using ACL
- Preventing SYN Attack using NBAR
- Preventing SYN Attack using Policing
- Preventing SYN Attack using CBAC
- Preventing SYN Attack using CAR
- Preventing SYN Attack using TCP Intercept
- Preventing SYN Attack using MPF
Mitigation Using Various Techniques

- Preventing IP Spoofing Attack using anti-spoofing ACLs
- Preventing IP Spoofing Attack using uRPF
- Preventing IP Spoofing Attack using IP Source Guard
Mitigation Using Various Techniques

- Preventing MAC Spoofing Attack using Port Security
- Preventing ARP Spoofing Attack using DAI
- Preventing STP Attack using Root/BPDU Guard
- Preventing DHCP Spoofing Attack using Port Security
- Preventing DHCP Spoofing Attack using DAI
- Preventing Fragment Attack using ACL
Session 9

Preparation Resources and Test-Taking Tips
Preparation Resources
Planning Resources

- There is an abundance of material available to prepare for the CCIE certification. However, you have to be very selective of the material you choose to use.

- Choose materials that offer configuration examples and take a “hands-on” approach.

- Look for materials approved or provided by Cisco and its Learning Partners.

- Customize your study plan to reflect your own personal strengths and weaknesses.

A Good Study Plan Is Key to Your Success
Assessing Strengths

- Evaluate your experience and knowledge in the major topic areas listed on blueprint
- Using the content **blueprint**, determine your experience and knowledge level in the major topic areas
- For areas of **strength**: practice for speed
- For **weaker** areas: boost knowledge with training or book study first, then practice
Trainings

Although No Formal Training Is Required for the CCIE Security Certification, **Cisco Recommends** the Following Training Courses, Which Are Described Further on the Cisco Website at:

Books

- Many Cisco Press® and other vendor books are available to assist in preparing for CCIE exams
- No single resource is uniformly great; you will likely need to add multiple books to your collection
Trainings

- Securing Networks with Cisco Routers and Switches (SNRS)
- Securing Networks with PIX and ASA (SNPA)
- Cisco Secure Virtual Networks (CSVPN)
- Implementing Cisco Intrusion Prevention System (IPS)
- Securing Cisco Network Devices (SND)

Free Online Cisco Quick Learning Web-Based Modules:

- Securing Cisco Routers (SECR)
- Configuring ASA and PIX Security Appliances
- Configuring IPS 4200 Series Sensors
- Security and VPN Quick Learning Modules
- Cisco IOS and IP Routing Quick Learning Modules
Bootcamp

- Many candidates ask if I can recommend a Security boot camp?

- In my opinion, bootcamps are intended to give an overview of the lab, offer tips-and-tricks for exam taking, and provide mock scenarios which help you gauge your readiness.

- Therefore, to gain the most benefit, I recommend you study the technologies involved before attending any boot camp.
Many candidates overlook one of the best resources for useful material and technical information—the Cisco website.

There are many sample scenarios available on the Tech Support pages for each Cisco product and technology. For instance, the Tech Support page for IPsec has more than 150 samples and tips available.

These articles are written to reflect current trends and demands and include sample diagrams, configurations, and invaluable show and debug command outputs.
Forums

Forums Can Play an Essential Role for a Candidate During Preparation; You Can Generally Find Qualified CCIEs and Other Security Engineers Available 24x7 to Answer Your Queries and Work Through Your Technical Problems

- Cisco’s Networking Professional Connection
  
  http://www.cisco.com/go/netpro

  Networking Professionals can post questions for technical assistance, seek suggestions or share experiences at NetPro

- Cisco Learning Network (CLN)
  
  http://www.cisco.com/go/learnnetspace

  Offers online learning network to enhance and advance your IT career. Browse technical content and connect and share insights, opinions, and knowledge with the community.

- Cisco’s Certification Online Support
  
  http://www.cisco.com/go/certsupport

  Q and A on certification related topics such as exam info, books, trainings, requirements, resources, tools and utilities and much more
Documentation CD (Your Lifeline)

- You need to be able to navigate the Cisco documentation CD with confidence
- This is the only resource you are allowed during the exam and you will need to be able to look up anything you need with speed and confidence
- Make it part of your regular practice; if you are familiar with it, it can save you time during the exam
Practice Labs

- Practice lab exercises with a high level of complexity will assist you in making improvements in your exam strategy and identifying areas requiring extra study. Practice labs can be used to gauge your readiness and help identify your strengths and weaknesses. This will help you refocus and revise your study plan and adjust it according to your findings.

- Technical skill is not the only thing you need to work on; time management and your exam-taking strategy is also important to succeed in the CCIE exam. Practice labs also assist you in improving your time management and test-taking approach.
Equipment (Home Lab vs. Rental Racks)

- Although acquiring a personal home lab is an ideal scenario, it can be costly to gather all the equipment to build a security rack. You can start with just a few devices—three to four routers, a switch and a PIX firewall. The goal is to obtain a thorough understanding of the technologies and the architecture and also know how they integrate with each other.

- For the hardware devices which are more costly to obtain, such as the IDS Sensor or VPN3000 concentrator, I would advise looking at renting the equipment online. There are many vendors who provide such services. This is far less expensive than purchasing a home security rack.
Test-Taking Tips
Lab Preparation: Hands-On Practice

- **Essential** for passing lab
- Borrow or rent equipment you can practice on
- Two or three routers will support most scenarios
- Build and practice scenarios for each topic
- Go beyond the basics—practice additional features
- If a technology has multiple configurations—practice all of them
- Learn show and debug commands for each topic
Lab Exam Tips

- Reduce stress—arrive early
- Leave yourself time—exam can run over
- Read entire exam
- Redraw topology to clarify scenario
- Manage your time
- Make no assumptions
- Keep a list
- Work questions as a unit
- Test your work
- Save configurations often
- Minimize last-minute changes
Troubleshooting

- Know how to troubleshoot using tools available
- Verify each question before moving on. Work the simple or basic questions first and then the complex ones
- Check for typos when configuring maps, network statements, IP addresses, etc.
- Keep in mind the point value; don’t lose too much time working on a two or three point question
- Save your configurations. If necessary, you can reload a device and work on something else while it comes back up in a known state
Lab Exam Proctors

Ask the Proctor Questions

- Proctor’s role is to keep exam fair
- Talk to proctor if you don’t understand question
- Ask the proctor clarifying questions
- Report any equipment or technical problems to proctor as soon as it occurs
For More Information

- Beware of rumors
- Visit the CCIE web page
  
  http://www.cisco.com/go/ccie
- Online Support
  
  www.cisco.com/go/certsupport
- E-mail
  
  ccie-lab@cisco.com
- Cheating
  
  ccie-nda-enforcement@cisco.com
Recommended Reading

Network Security Technologies and Solutions (CCIE Professional Development Series)

ISBN: 1587052466

By Yusuf Bhaiji
Recommended Reading (Cont.)

CCIE Security Practice Labs (CCIE Self-Study)
ISBN: 1587051346
By Yusuf Bhaiji
Recommended Reading (Cont.)

CCIE Security Exam Quick Reference Sheets
ISBN: 1587053349
By Lancy Lobo, Umesh Lakshman