
CCIE 8 Weeks
Learn. Practice. Achieve
ALL-IN-ONE
CCIE SECURITY V5.0
WRITTEN EXAM 400-251 CERT GUIDE
Learn, Practice and Ace the New CCIE Written Exams with Test Prep Resources from CCIEin8Weeks™
CCIEin8Weeks.com
PAUL ADAM, CCIE®
3RD EDITION
SECURITY V5.0
EXAM 400-251 CERT GUIDE
helped thousands of test takers and learners to
, practice and pass the CCIE® written exams
Weeks™ contains supplemental resources such as
dy plans and blog articles to help you further
ms and the real world. Our practice quizzes are
to ensure your exam success.
ide methodically and precisely covers all the
CIE® Security 400-251 V5.0 exam. It follows recently
ial exam blueprint for CCIE® Security written
er contains an Exam Essentials section at the end
y concepts and to help you pass the exam.
nce
rimeter Security and Intrusion Prevention
vanced Threat Protection and Content Security
cure Connectivity and Segmentation
entity Management, Information Exchange, and
ol
frastructure Security, Virtualization, and Automation
olving Technologies V1.1 – Cloud
olving Technologies V1.1 – Network
bility
olving Technologies V1.1 – Internet of Things (IoT)
/CCIEIN8WEEKS | FACEBOOK.COM/CCIEIN8WEEKS
CCIE 8 Weeks
2nd EDITION

All-in-One CCIE Security V5.0
400-251 Written Exam Cert Guide

3rd Edition

Contents at a Glance

Table of Contents

Preface

Congratulations! You have taken your first step towards passing the CCIE Security 400-251 V5.0 written exam.

This study guide is dedicated to *all those souls who will never settle for less than they can be, do, share, and give!*

CCIE Security v5.0 Hardware and Software

Virtual Machines

- Security Appliances
  - Cisco Identity Services Engine (ISE): 2.1.0
  - Cisco Secure Access Control System (ACS): 5.8.0.32
  - Cisco Web Security Appliance (WSA): 9.2.0
  - Cisco Email Security Appliance (ESA): 9.7.1
  - Cisco Wireless Controller (WLC): 8.0.133
  - Cisco Firepower Management Center Virtual Appliance: 6.0.1 and/or 6.1
  - Cisco Firepower NGIPSv: 6.0.1
  - Cisco Firepower Threat Defense: 6.0.1
- **Core Devices**
  - IOSv L2: 15.2
  - IOSv L3: 15.5(2)T
  - Cisco CSR 1000V Series Cloud Services Router: 3.16.02.S
  - Cisco Adaptive Security Virtual Appliance (ASAv): 9.6.1
- Others
  - Test PC: Microsoft Windows 7
  - Active Directory: Microsoft Windows Server 2008 (AD is not required to be configured by the candidate)
  - Cisco Application Policy Infrastructure Controller Enterprise Module : 1.2
  - Cisco Unified Communications Manager: (The CUCM is not required to be configured by the candidate)
  - FireAMP Private Cloud
  - AnyConnect 4.2

Physical Devices

- Cisco Catalyst Switch: C3850-12S 16.2.1
- Cisco Adaptive Security Appliance: 5512-X: 9.6.1
- Cisco 2504 Wireless Controller: 2504: 8.0.133.0
- Cisco Aironet: 1602E: 15.3.3-JC
- Cisco Unified IP Phone: 7965: 9.2(3) (IP Phone is not required to be configured by the candidate)

Topics Added in CCIE Security v5.0 (versus V4.1)

- Advanced Threat Protection
- Virtualization
- Automation
- Information Exchange
- Evolving Technologies

Topics Removed in CCIE Security v5.0 (versus V4.1)

- Legacy IPS Appliance
- Easy VPN

CCIE Security V5.0 Blueprint Domains	Domain Description	Written Exam %
Perimeter Security and Intrusion Prevention	Cisco FirePOWER, Cisco ASA, Cisco IOS ZBFW, DDoS Mitigation	21%
Advanced Threat Protection and Content Security	AMP Solutions and Security Protocols	17%
Secure Connectivity and Segmentation	IKE/IPSec, TrustSec, GETVPN, DMVPN, FlexVPN, Security protocols and algorithms	17%
Identity Management, Information Exchange, and Access Control	ISE, RADIUS/TACACS+, WLAN Security and Protocols	22%
Infrastructure Security, Virtualization, and Automation	Attacks, Cisco ACI, standard bodies, Cisco DNA/SAFE, NetFlow, ACLs etc.	13%
Evolving Technologies	Cloud, SDN, IoT	10%

It is exciting to see that Cisco has aggressively updated the exam blueprint to keep pace with the changes taking place in the security and networking industries. Following are worth noting:

- As we know, Cisco is an acquisition machine and recently snapped up Lancope (NBA/NetFlow), OpenDNS (cloud-delivered security), and SourceFire (FirePower product line) security companies. Both newly acquired and organically built (ex. ACI) products and solutions are now part of the new CCIE Security blueprint (v5.0)
- Overall exam blueprint now seems more consolidated (8 versus 6 exam sections)

- Identity Management, Information Exchange, and Access Control is the largest content contributor to the exam now (22% and 24% of the written and lab exams respectively)
- Security infrastructure products for perimeter security and intrusion prevention is the second largest content area when it comes written and lab exam content (21% and 23% of the written and lab exams respectively)
- It seems finally all of the VPN content is now consolidated into Secure Connectivity and Segmentation area (17% and 19% of the written and lab exams respectively)
- Infrastructure Security, Virtualization, and Automation now includes Cisco ACI and virtualized security domain
- There is no change to Evolving Technologies section across v4.1 and v5.0 exam blueprint. It continues to include SDN, Cloud and Internet of Things (IoT)
- Last but not least, Cisco also seems to be stepping up on transparency around the CCIE exam content with a lot of details for each section.

What this Exam Cert Guide Covers

As you may already have noticed on the "Contents at a Glance" page that this guide has been formatted around the Cisco's official CCIE 400-251 V5.0 exam topics or curriculum. So as you read through the chapters, you will know exactly where you're within your learning journey.

All contents are carefully compiled and covered in enough details however still trimmed to exactly what's necessary to pass the exam. Each exam topic has "Further Reading" section where we have done the research for you in the form of curated set of links. You can refer to them if you are looking for more in-depth details or want to refer to the source of the original text.

How to Use this Exam Cert Guide

This guide is for anyone who's studying for CCIE Security written 400-251 V5.0 exam, regardless if this is your first time sitting for a CCIE written exam or you're a pro who's recertifying. We strongly suggest to take a methodical approach for exam preparation, i.e. start with a target date when you would like to sit for the actual exam and then work backwards to see what kind of study plan would work for you. We believe you can cover the entire contents within eight weeks including the practice questions (available on our website). We strongly suggest you to also use other study resources in addition to bringing your prior experience to bear in order to successfully pass the exam.

If you're totally in a crunch and consider yourself an advanced learner, you could try your luck by skimming through the "Exam Essentials" sections for each chapter- We guarantee you that you will be better prepared to tackle the exam with them than without!

What's Available on the CCIEin8Weeks Website

CCIEin8Weeks.com carries the extras (sold separately) that go hand in hand with this study guide to further ensure your exam success!

- Six practice exams (one for each section as per official curriculum), One final exam
- Four study plans, to help you track your progress or help you come up with your own plan
- CCIE Exam community forum, to help you interact with others, share knowledge, find study partners etc.
- ExamSkope™ to help you keep up to speed on the buzz around CCIE Security V5 written exam

Chapter 1: Perimeter Security and Intrusion Prevention

This chapter covers the following exam topics from Cisco's official 400-251 V5.0 written exam curriculum.

- Describe, implement, and troubleshoot HA features on Cisco ASA and Cisco FirePOWER Threat Defense (FTD)
- Describe, implement, and troubleshoot clustering on Cisco ASA and Cisco FTD
- Describe, implement, troubleshoot, and secure routing protocols on Cisco ASA and Cisco FTD
- Describe, implement, and troubleshoot different deployment modes such as routed, transparent, single, and multi-context on Cisco ASA and Cisco FTD
- Describe, implement, and troubleshoot firewall features such as NAT (v4,v6), PAT, application inspection, traffic zones, policy-based routing, traffic redirection to service modules, and identity firewall on Cisco ASA and Cisco FTD
- Describe, implement, and troubleshoot IOS security features such as Zone-Based Firewall (ZBF), application layer inspection, NAT (v4,v6), PAT and TCP intercept on Cisco IOS/IOS-XE
- Describe, implement, optimize, and troubleshoot policies and rules for traffic control on Cisco ASA, Cisco FirePOWER and Cisco FTD
- Describe, implement, and troubleshoot Cisco Firepower Management Center (FMC) features such as alerting, logging, and reporting
- Describe, implement, and troubleshoot correlation and remediation rules on Cisco FMC
- Describe, implement, and troubleshoot Cisco FirePOWER and Cisco FTD deployment such as in-line, passive, and TAP modes
- Describe, implement, and troubleshoot Next Generation Firewall (NGFW) features such as SSL inspection, user identity, geolocation, and AVC (Firepower appliance)
- Describe, detect, and mitigate common types of attacks such as DoS/DDoS, evasion techniques, spoofing, man-in-the-middle, and botnet

Chapter 1: Perimeter Security and Intrusion Prevention

Cisco continues to be in the process of integrating the acquired FirePower product lines (from SourceFire) to existing ASA legacy firewall product line. Over the last two years, Cisco has been adding Firepower features to the ASA product line. In September 2014, Cisco added Firepower services from Sourcefire to Cisco ASA firewalls. With the new Firepower NGFW, an existing ASA 5500 can be upgraded via software to the new image. Additionally, some of the older Firepower appliances can now also be upgraded to the new image.

The core of the Firepower NGFW is a new Linux operating system distribution dubbed as FXOS (Firepower eXtensible Operating System). The new FXOS introduces service-chaining capabilities that can help to enable a security inspection and remediation workflow. Chaining and understanding context is further enhanced through the integration of the Cisco Identity Service Engine (ISE). Firepower can now consume Cisco ISE information about users and policy. Additionally, the integration of ISE and Firepower enables rapid threat containment where an alert from Firepower can be extended through ISE to keep a threat or malicious end point off the network.

The Firepower Threat Defense appliance provides a unified next-generation firewall and next-generation IPS device. In addition to the IPS features available on Firepower Software models, firewall and platform features include Site-to-Site VPN, robust routing, NAT, clustering (for the Firepower 9300), and other optimizations in application inspection and access control.

The Firepower Threat Defense software is supported on the following platforms:

- Firepower 9300
- Firepower 4100 series
- ASA 5512-X through 5555-X
- ASA 5508-X and 5516-X
- ASA 5506-X series

As you go through the sections below, please note that a lot of the features and system behaviors apply across legacy ASA and new integrated platform running FXOS. However, not all ASA features are available in FXOS at the time of writing this text.

Further Reading

You can read up on current state of integration and ASA versus FXOS compatibility below.

https://goo.gl/ZRRO75

Describe, implement, and troubleshoot HA features on Cisco ASA

Configuring high availability requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a Stateful Failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The ASA supports two failover configurations, Active/Active failover and Active/Standby failover. Each failover configuration has its own method for determining and performing failover. With Active/Active failover, both units can pass network traffic. This also lets you configure traffic sharing on your network. Active/Active failover is available only on units running in multiple context mode. With Active/Standby failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby failover is available on units running in either single or multiple context mode. Both failover configurations support stateful or stateless (regular) failover. When the security appliance is configured for Active/Active stateful failover, you cannot enable IPsec or SSL VPN. Therefore, these features are unavailable. VPN failover is available for Active/Standby failover configurations only.

Failover System Requirements

This section describes the hardware, software, and license requirements for ASAs in a failover configuration.

Hardware Requirements

The two units in a failover configuration must be the same model, have the same number and types of interfaces, and the same SSMs installed (if any). Both units must have the same amount of RAM memory installed. If you are using units with different Flash memory sizes in your failover configuration, make sure the unit with the smaller Flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger Flash memory to the unit with the smaller Flash memory will fail.

Software Requirements

The two units in a failover configuration must be in the same operating modes (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version. However, you can use different versions of the software during an upgrade process; for example, you can upgrade one unit from Version 7.0(1) to Version 7.0(2) and have failover remain active. We recommend upgrading both units to the same version to ensure long-term compatibility.

Licensing Requirements

The licensed features (such as SSL VPN peers or security contexts, for example) on both units participating in failover must be identical.

Failover and Stateful Failover Links

This section describes the failover and the Stateful Failover links, which are dedicated connections between the two units in a failover configuration.

Failover Link

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

You can use any unused Ethernet interface on the device as the failover link; however, you cannot specify an interface that is currently configured with a name. The LAN failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface should only be used for the LAN failover link (and optionally for the Stateful Failover link).
Connect the LAN failover link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the LAN failover interfaces of the ASA.
- Using a crossover Ethernet cable to connect the appliances directly, without the need for an external switch.

When you use a crossover cable for the LAN failover link, if the LAN interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which interface failed and caused the link to come down.

Stateful Failover Link

To use Stateful Failover, you must configure a Stateful Failover link to pass all state information. You have three options for configuring a Stateful Failover link:

- You can use a dedicated Ethernet interface for the Stateful Failover link.
- If you are using LAN-based failover, you can share the failover link.
- You can share a regular data interface, such as the inside interface. However, this option is not recommended.

If you are using a dedicated Ethernet interface for the Stateful Failover link, you can use either a switch or a crossover cable to directly connect the units. If you use a switch, no other hosts or routers should be on this link. Be sure to enable the PortFast option on Cisco switch ports that connect directly to the ASA. If you use a data interface as the Stateful Failover link, you receive the following warning when you specify that interface as the Stateful Failover link:

******* WARNING ***** WARNING ******* WARNING ****** WARNING ********
Sharing Stateful failover interface with regular data interface is not a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING ********

Sharing a data interface with the Stateful Failover interface can leave you vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems on that network segment. Using a data interface as the Stateful Failover interface is supported in single context, routed mode only.
In multiple context mode, the Stateful Failover link resides in the system context. This interface and the failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.
The IP address and MAC address for the Stateful Failover link does not change at failover unless the Stateful Failover link is configured on a regular data interface.
All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords, and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

Failover Interface Speed for Stateful Links

If you use the failover link as the Stateful Failover link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the Stateful Failover interface.
Use the following failover interface speed guidelines for the adaptive security appliances:

- Cisco ASA 5510
  – Stateful link speed can be 100 Mbps, even though the data interface can operate at 1 Gigabit due to the CPU speed limitation.
- Cisco ASA 5520/5540/5550
  – Stateful link speed should match the fastest data link.
- Cisco ASA 5580/5585

– Use only non-management 1 Gigabit ports for the stateful link because management ports have lower performance and cannot meet the performance requirement for stateful failover.
For optimum performance when using long distance LAN failover, the latency for the failover link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than10 milliseconds, some performance degradation occurs due to retransmission of failover messages.
All platforms support sharing of failover heartbeat and stateful link, but we recommend using a separate heartbeat link on systems with high Stateful Failover traffic.

Avoiding Interrupted Failover Links

Because adaptive security appliances uses failover LAN interfaces to transport messages between primary and secondary units, if a failover LAN interface is down (that is, the physical link is down or the switch used to connect the LAN interface is down), then the adaptive security appliance failover operation is affected until the health of the failover LAN interface is restored. If all communication is cut off between the units in a failover pair, both units go into the active state, which is expected behavior. When communication is restored and the two active units resume communication through the failover link or through any monitored interface, the primary unit remains active, and the secondary unit immediately returns to the standby state. This relationship is established regardless of the health of the primary unit.

Because of this behavior, stateful flows that were passed properly by the secondary active unit during the network split are now interrupted. To avoid this interruption, failover links and data interfaces should travel through different paths to decrease the chance that all links fail at the same time. If only one failover link is down, the adaptive security appliance takes a sample of the interface health, exchanges this information with its peer through the data interface, and performs a switchover if the active unit has a greater number of down interfaces. Subsequently, the failover operation is suspended until the health of the failover link is restored.

Active/Active and Active/Standby Failover

Two types of failover configurations are supported by the ASA: Active/Standby and Active/Active. In Active/Standby failover, one unit is the active unit. It passes traffic. The standby unit does not actively pass traffic. When a failover occurs, the active unit fails over to the standby unit, which then becomes active. You can use Active/Standby failover for ASAs in single or multiple context mode, although it is most commonly used for ASAs in single context mode.

Active/Active failover is only available to ASAs in multiple context mode. In an Active/Active failover configuration, both ASAs can pass network traffic. In Active/Active failover, you divide the security contexts on the ASA into failover groups. A failover group is simply a logical group of one or more security contexts. Each group is assigned to be active on a specific ASA in the failover pair. When a failover occurs, it occurs at the failover group level.

Determining Which Type of Failover to Use

The type of failover you choose depends upon your ASA configuration and how you plan to use the ASAs.
If you are running the ASA in single mode, then you can use only Active/Standby failover. Active/Active failover is only available to ASAs running in multiple context mode.
If you are running the ASA in multiple context mode, then you can configure either Active/Active failover or Active/Standby failover.

- To allow both members of the failover pair to share the traffic, use Active/Active failover. Do not exceed 50% load on each device.
- If you do not want to share the traffic in this way, use Active/Standby or Active/Active failover.

Feature	Active/Active	Active/Standby
Single Context Mode	No	Yes
Multiple Context Mode	Yes	Yes
Traffic Sharing Network Configurations	Yes	No
Unit Failover	Yes	Yes
Failover of Groups of Contexts	Yes	No
Failover of Individual Contexts	No	No

Stateless (Regular) and Stateful Failover

The ASA supports two types of failover, regular and stateful. This section includes the following topics:

Stateless Failover

When a failover occurs, all active connections are dropped. Clients need to reestablish connections when the new active unit takes over.

Stateful Failover

When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

tate Information Passed to Standby Unit	State Information Not Passed to Standby Unit
NAT translation table	The HTTP connection table (unless HTTP replication is enabled).
TCP connection states	The user authentication (uauth) table.

	Inspected protocols are subject to advanced TCP-state tracking, and the TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.
UDP connection states	The routing tables. After a failover occurs, some packets may be lost or routed out of the wrong interface (the default route) while the dynamic routing protocols rediscover routes.
The ARP table	State information for Security Service Modules.
The Layer 2 bridge table (when running in transparent firewall mode)	DHCP server address leases.
The HTTP connection states (if HTTP replication is enabled)	Stateful failover for phone proxy. When the active unit goes down, the call fails, media stops flowing, and the phone should unregister from the failed unit and re register with the active unit. The call must be re-established.
The ISAKMP and IPSec SA table	—
GTP PDP connection database	—
SIP signalling sessions	—

For VPN failover, VPN end-users should not have to reauthenticate or reconnect the VPN session in the event of a failover. However, applications operating over the VPN connection could lose packets during the failover process and not recover from the packet loss.

Transparent Firewall Mode Requirements

When the active unit fails over to the standby unit, the connected switch port running Spanning Tree Protocol (STP) can go into a blocking state for 30 to 50 seconds when it senses the topology change. To avoid traffic loss while the port is in a blocking state, you can configure one of the following workarounds depending on the switch port mode:

- Access mode—Enable the STP PortFast feature on the switch:

```
interface interface_id
spanning-tree portfast
```

The PortFast feature immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

- Trunk mode—Block BPDUs on the ASA on both the inside and outside interfaces:

```
access-list id ethertype deny bpdu
access-group id in interface inside_name
access-group id in interface outside_name
```

Blocking BPDUs disables STP on the switch. Be sure not to have any loops involving the ASA in your network layout.
If neither of the above options are possible, then you can use one of the following less desirable workarounds that impacts failover functionality or STP stability:

- Disable failover interface monitoring.
- Increase failover interface holdtime to a high value that will allow STP to converge before the ASAs fail over.
- Decrease STP timers to allow STP to converge faster than the failover interface holdtime.