CCNA Security 640-554 Quick Reference

Anthony Sequeira

Cisco Press

CCNA Security 640-554 Quick Reference

Anthony Sequeira
CCIE, CCSI, VCP, Data Center Specialist

ciscopress.com

Table of Contents

About the Author

Anthony Sequeira, CCIE No. 15626, is a Cisco Certified Systems Instructor and author regarding all levels and tracks of Cisco Certification. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about Microsoft and Cisco technologies. Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company KnowledgeNet, and Anthony trained there for many years. Anthony is currently pursuing his second CCIE in the area of Security and is a full-time instructor for the next generation of KnowledgeNet, StormWind Live.

About the Technical Editor

Sean Wilkins is an accomplished networking consultant for SR-W Consulting (http://www.sr-wconsulting.com) and has been in the field of IT since the mid 1990s working with companies such as Cisco, Lucent, Verizon and AT&T. Sean currently holds certifications with Cisco (CCNP/CCDP), Microsoft (MCSE), and CompTIA (A+ and Network+). He also has a master's of science degree in Information Technology with a focus in Network Architecture and Design, a master's of science degree in Organizational Management, a master's certificate in Network Security, a bachelor's of science degree in Computer Networking, and an associate's degree in Applied Science in Computer Information Systems. In addition to working as a consultant, Sean spends a lot of his time as a technical writer and editor for various companies.

Chapter 3
Cisco IOS Firewalls

Firewall Technologies

Firewalls are a key security technology in the modern network infrastructure. This section details their evolution and the technologies that have resulted.

Firewall Fundamentals

The firewall should

- Be resistant to attacks.
- Be the only transit point.
- Enforce the access control policy of the organization.

Static Packet-Filtering Firewalls

These work at Layers 3 and 4, examining packets one at a time and are implemented on a Cisco router using access control lists (ACL).

Advantages of these firewalls include the following:

- Based on simple `permit` and `deny` sets
- Low impact on network performance

- Easy to implement
- Supported on most routers
- Initial security at a low network layer
- Perform most of what high-end firewalls do at a lower cost

Disadvantages of these firewalls include the following:

- Susceptible to IP spoofing.
- Packet filters do not filter fragmented packets well.
- Complex ACLs are difficult to implement and maintain correctly.
- Packet filters cannot dynamically filter certain services.
- Packet filters are stateless; they do not maintain any state information for added protection.

Application Layer Gateways

Application layer firewalls (also called *proxy firewalls* or *application gateways*) operate at Layers 3, 4, 5, and 7 of the OSI model. Proxy services are specific to the protocol that they are designed to forward and can provide increased access control, provide careful detailed checks for valid data, and generate audit records about the traffic they transfer. Sometimes, application layer firewalls support only a limited number of applications.

Application layer firewalls offer advantages:

- Authenticate individuals, not devices
- Make it harder for hackers to spoof and implement denial-of-service (DoS) attacks
- Can monitor and filter application data
- Can provide detailed logging

The disadvantages are as follows:

- Process packets in software
- Support a small number of applications
- Sometimes require special client software
- Are memory- and disk-intensive

Dynamic or Stateful Packet-Filtering Firewalls

Stateful inspection is a firewall architecture classified at the network layer; although, for some applications it can analyze traffic at Layers 4 and 5, too.

Unlike static packet filtering, stateful inspection tracks each connection traversing all interfaces of the firewall and confirms that they are valid. Stateful packet filtering maintains a state table and allows modification to the security rules dynamically. The state table is part of the internal structure of the firewall. It tracks all sessions and inspects all packets passing through the firewall.

Although this is the primary Cisco Firewall technology, it has some limitations:

- Cannot prevent application layer attacks.
- Not all protocols are stateful.
- Some applications open multiple connections.
- Does not support user authentication.

Other Types

Application inspection firewalls ensure the security of applications and services. Advantages include the following:

- Are aware of the state of Layer 4 and Layer 5 connections
- Check the conformity of application commands at Layer 5
- Can and affect Layer 7
- Can prevent more kinds of attacks than stateful firewalls can

Transparent firewalls (Cisco PIX and Cisco Adaptive Security Appliance Software Version 7.0) can deploy a security appliance in a secure bridging mode as a Layer 2 device to provide security services at Layer 2 through Layer 7.

Cisco Firewall Family

Cisco IOS Firewall features follow:

- Zone-based policy framework for intuitive policy management
- Application firewalling for web, e-mail, and other traffic
- Instant messenger and peer-to-peer application filtering
- VoIP protocol firewalling
- Virtual routing and forwarding (VRF) firewalling
- Wireless integration
- Stateful failover
- Local URL whitelist and blacklist support; remote server support, through Websense or SmartFilter

Cisco PIX 500 Series Security Appliance features follow:

- Advanced application-aware firewall services
- Market-leading VoIP and multimedia security
- Robust site-to-site and remote-access IP security (IPsec) VPN connectivity
- Award-winning resiliency
- Intelligent networking services
- Flexible management solutions

Cisco ASA 5500 Series Adaptive Security Appliance features follow:

- World-class firewall
- Voice and video security
- SSL and IPsec VPN
- IPS
- Content security
- Modular devices
- High scalability

Best Practices

Firewall best practices include the following:

- Position firewalls at key security boundaries.
- Firewalls are the primary security device, but it is unwise to rely exclusively on a firewall for security.

CCNA Security 640-554 Quick Reference

Anthony Sequeira

Published by Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

First Release May 2012

ISBN-13: 978-1-58714-317-5

Warning and Disclaimer

This digital Quick Reference is designed to provide information about the CCNA Security Certification. Every effort has been made to make this digital Quick Reference as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this digital Quick Reference.

The opinions expressed in this digital Quick Reference belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this digital Quick Reference that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this digital Quick Reference should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this digital Quick Reference, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the digital Quick Reference title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this digital Quick Reference when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com.

For sales outside the United States please contact:
International Sales
international@pearsoned.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**