Implementing and Operating Cisco Security Core Technologies

SCOR 350-701 V1.0 Core Exam

1st Edition

ISBN: 9798614110864

Contents at a Glance

Chapter 1 Security Concepts
Chapter 2 Network Security
Chapter 3 Securing the Cloud
Chapter 4 Content Security
Chapter 5 Endpoint Protection and Detection
Chapter 6 Secure Network Access, Visibility, and Enforcement

Table of Contents

About the Author **10**

Preface **12**

What this Study Guide contains **13**

How to use this Study Guide **13**

What's available on the CCIEin8Weeks website **14**

Chapter 1 Security Concepts **16**

Explain common threats against on-premises and cloud environments 17
Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery 27
Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key and certificate-based authorization 27
Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Crypto map, DMVPN, FLEXVPN including high availability considerations, and AnyConnect 33
Describe security intelligence authoring, sharing, and consumption 33
Explain the role of the endpoint in protecting humans from phishing and social engineering attacks 36
Explain North Bound and South Bound APIs in the SDN architecture 36
Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting 38
Interpret basic Python scripts used to call Cisco Security appliances APIs 54
Chapter Summary 82

Chapter 2 Network Security **84**

Understanding Cisco Security Portfolio Nomenclature 85
Compare network security solutions that provide intrusion prevention and firewall capabilities 86
Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities 87
Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records 90
Configure and verify network infrastructure security methods (router, switch, wireless) 95
Implement segmentation, access control policies, AVC, URL filtering, and malware protection 112
Implement management options for network security solutions such as intrusion prevention and perimeter security (Single vs. multidevice manager, in-band vs. out-of-band, CDP, DNS, SCP, SFTP, and DHCP security and risks) 119
Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL) 121
Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, and encryption, secure logging, and NTP with authentication) 123
Configure and verify site-to-site VPN and remote access VPN 123
Chapter Summary 129

Chapter 3 Securing the Cloud **131**

Identify security solutions for cloud environments 132
Compare the customer vs. provider security responsibility for the different cloud service models 143
Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and security 146
Utilize Docker images in local developer environment 153
Implement application and data security in cloud environments 157
Identify security capabilities, deployment models, and policy management to secure the cloud 159
Configure cloud logging and monitoring methodologies 161
Describe application and workload security concepts 163
Chapter Summary 164

Chapter 4 Content Security 166
Implement traffic redirection and capture methods 167
Describe web proxy identity and authentication including transparent user identification 169
Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA) 170
Configure and verify web and email security deployment methods to protect on-premises and remote users (inbound and outbound controls and policy management) 172
Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption 176
Configure and verify secure internet gateway and web security features such as blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption 179
Describe the components, capabilities, and benefits of Cisco Umbrella 180
Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting) 181
Chapter Summary 183

Chapter 5 Endpoint Protection and Detection 185
Compare Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions. 186
Explain antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry 187
Configure and verify outbreak control and quarantines to limit infection 188
Describe justifications for endpoint-based security 194
Describe the value of endpoint device management and asset inventory such as MDM 194
Describe the uses and importance of a multifactor authentication (MFA) strategy 195
Describe endpoint posture assessment solutions to ensure endpoint security 196
Explain the importance of an endpoint patching strategy 196
Chapter Summary 198

Chapter 6 Secure Network Access, Visibility, and Enforcement 200
Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD 201
Configure and verify network access device functionality such as 802.1X, MAB, WebAuth 209
Describe network access with CoA 215
Describe the benefits of device compliance and application control 216
Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP) 216
Describe the benefits of network telemetry 218
Describe the components, capabilities, and benefits of these security products and solutions 219
Chapter Summary 222

About the Author

Muhammad Afaq Khan started his professional career at Cisco TAC San Jose and passed his first CCIE in 2002 (#9070). He held multiple technical and management positions at Cisco San Jose HQ over his 11 years of tenure at the company before moving into cloud software and data center infrastructure IT industries.

He has worked at startups as well as Fortune 100 companies in senior leadership positions over his career. He is also a published author (Cisco Press, 2009) and holds multiple patents in the areas of networking, security, and virtualization. Currently, he is a founder at Full Stack Networker and a vocal advocate for network automation technologies and NetDevOps. He is a Cisco Certified DevNet Associate[1] and was among the first 500 people #DevNet500 worldwide to pass the exam.

[1] https://bit.ly/2Pt7R9J

Preface

Congratulations! You have taken your first step towards preparing and passing the Cisco Implementing and Operating Cisco Security Core Technologies (SCOR) 350-701 V1.0 Exam.

Did you just purchase a copy? **Interested in getting access to an SCOR Exam Quiz?** Register here[2] and send us an email at support@cciein8weeks.com to get started.

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

[2] https://bit.ly/2SrWctJ

What this Study Guide contains

This guide will help you comprehensively prepare for the SCOR exam. As you may already have noticed on the "Contents at a Glance" page that this guide has been formatted around the Cisco's official Security Core Technologies 350-701 official exam topics or curriculum[3]. The benefit? Well, as you read through the various topics, you will know exactly where you're within your learning journey.

All contents are carefully covered with core concepts, configurations, and topic summaries to help you master the skills so you can confidently face the pressures of the Cisco exam as well as its real-world application.

How to use this Study Guide

This guide is for anyone who's studying for Cisco Security Core Technologies 350-701 exam. I strongly suggest taking a methodical approach for exam preparation, i.e. start with a target date or 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.

Security Core Technologies SCOR 350-701 V1.0 Exam Topics Bodies of Knowledge	Exam Weight
Security Concepts	25%
Network Security	20%
Securing the Cloud	15%
Content Security	15%
Endpoint Protection and Detection	10%
Secure Network Access, Visibility, and Enforcement	15%

[3] https://bit.ly/2vAEhIk

What's available on the CCIEin8Weeks website

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

- All-in-One Course[4] that covers all bodies of knowledge tested on the SCOR Exam
- 6x Practice Quizzes (one for each section as per the official curriculum)
- 1x Exam Simulation (to help you prepare to face the pressure of a real Cisco exam)
- Hands-on configurations and examples

[4] https://bit.ly/3bBJIaB

Chapter 1 Security Concepts

This chapter covers the following exam topics from Cisco's official Implementing and Operating Cisco Security Core Technologies (SCOR)[5] 350-701 V1.0 exam blueprint.

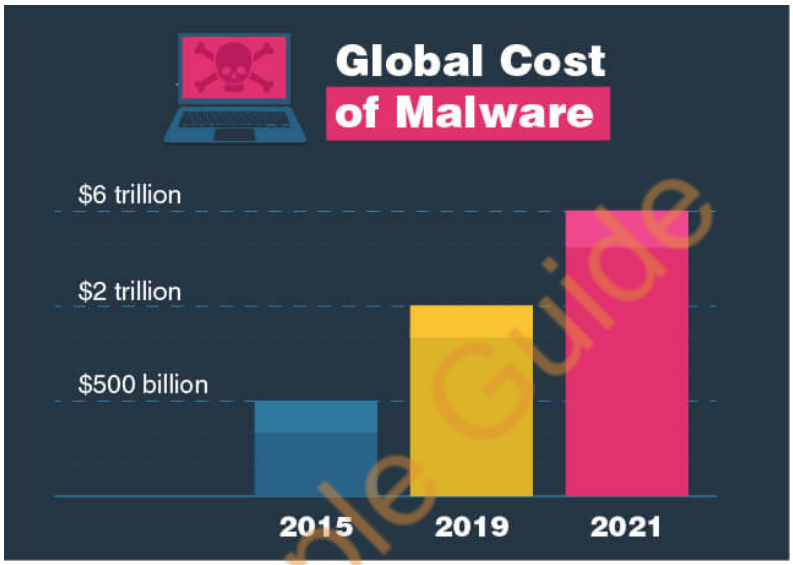
- Explain common threats against on-premises and cloud environments
  - On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware
  - Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials
- Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery
- Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key and certificate-based authorization
- Compare site-to-site VPN and remote access VPN deployment types such as SVTI, IPsec, Crypto map, DMVPN, FLEXVPN including high availability considerations, and AnyConnect
- Describe security intelligence authoring, sharing, and consumption
- Explain the role of the endpoint in protecting humans from phishing and social engineering attacks
- Explain North Bound and South Bound APIs in the SDN architecture
- Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting
- Interpret basic Python scripts used to call Cisco Security appliances APIs

[5] https://bit.ly/2uLalcz

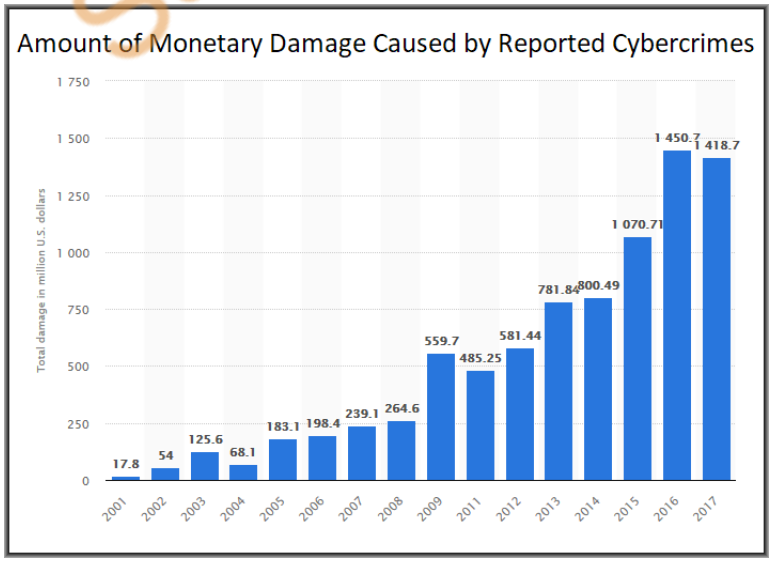
Explain common threats against on-premises and cloud environments

On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware

It is crucial to understand that the global cost of a malware is staggering. With cybercrime on the rise, the cost is expected to reach $6T by 2021.



The amount of monetary damage caused by cybercrimes has exponentially risen over the past two decades, surpassing $1.5T today.



Viruses

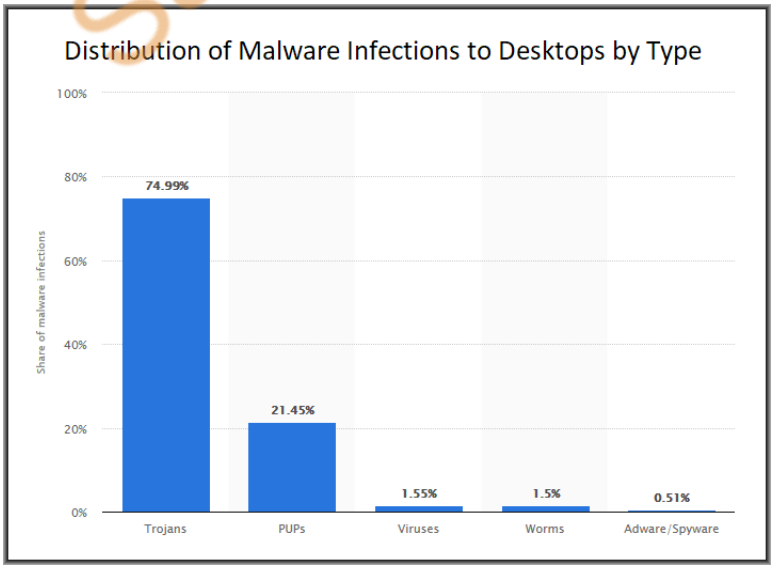
The virus is a type of malware attached to another file and can replicate and spread once a user on the target machine executes it. The terms Virus and malware are often used interchangeably, but they don't mean the same thing. Malware is a broad term that is used to describe all sorts of unwanted and malicious code. All viruses are a form of malware, but not all malware are viruses, i.e., malware can also be spyware, trojan, or worm. Viruses are now a thing of the past. Worms are also rare but can't be completely ruled out.

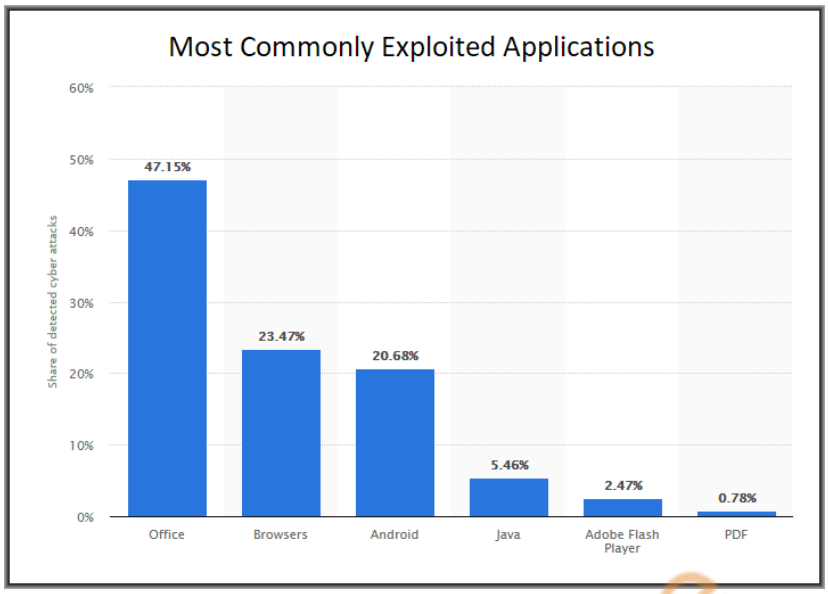
Trojans

A trojan or a trojan horse is neither a virus nor a worm. Unlike a virus, a trojan appears as a bona fide application and requires a user action for execution. Trojans can take various forms, such as free software, or music, even legit apps. If you visit shady websites or download cracked applications or some unknown free programs or any other social engineering method that takes advantage of a recent trend. In late 2017, when Intel announced that most of its x86 processors are vulnerable to Meltdown or Spectre attack, which allowed a rogue process to read all system memory, even when it is not supposed to. Hackers used that panic and released patches (e.g., Smoke loader), which did nothing to fix the problem but helped install a Trojan.

In most recent incidents, trojans have been used to target financial institutions with the aim of opening a permanent backdoor, which can be used to connect to a command-and-control (C2) server primarily for the purposes of data and identity thefts.

Let's review some of the recent statistics on the distribution of malware by type and applications.





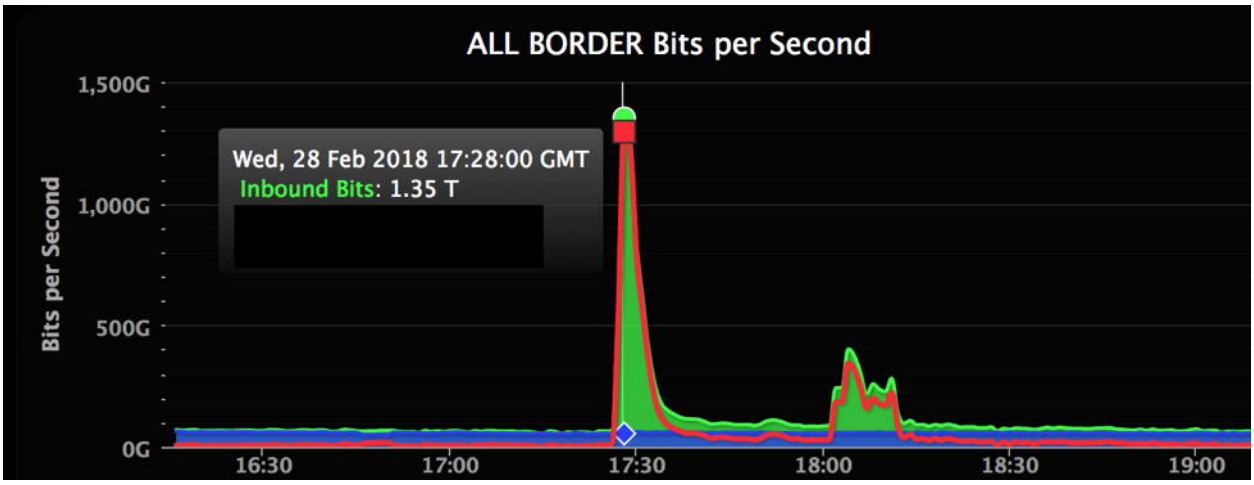
DoS/DDoS Attacks

Denial of Service (or DoS) is a type of cyber-attack in which the attacker tries to disrupt regular traffic directed to a server, service, or even an entire network by overwhelming the target with malicious traffic. The aim is to make the service unavailable to legitimate users. Distributed DoS (or DDoS) is a type of DoS where multiple systems (or botnets) target a single service and bombard it with traffic from various locations.

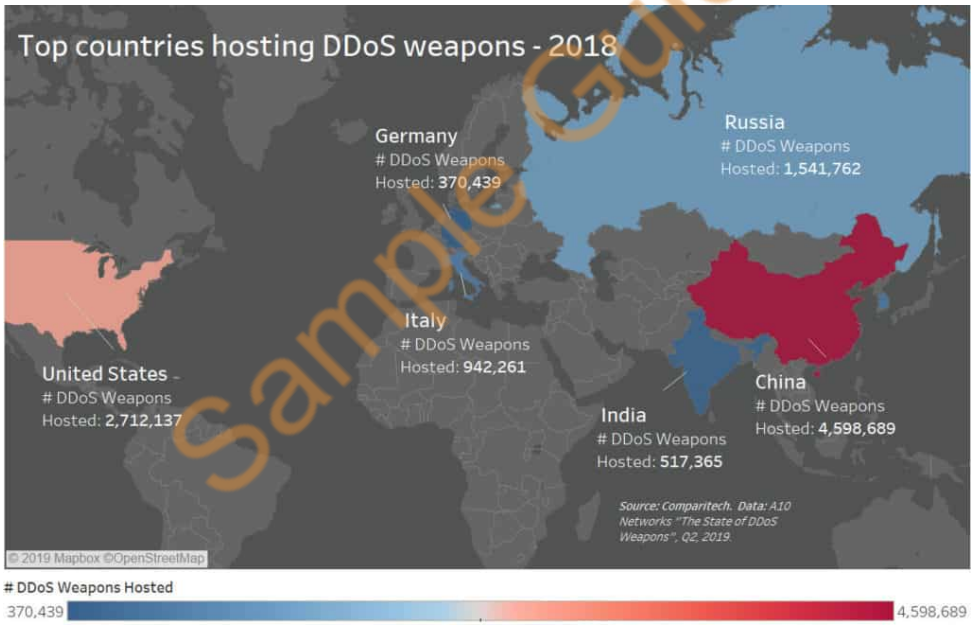
There are several types of DDoS attacks. The most prevalent form is a volume-based attack, where the target service is flooded with massive amounts of UDP or ICMP traffic. DDoS attacks can also target a protocol such as TCP by swamping the target service with SYN floods, fragmented packets, etc. The DDoS attack can also be orchestrated by exploiting a certain vulnerability within the application software stack.

The most recent examples of DDoS include GitHub, where the service was flooded with about 1.3 Tbps of traffic. The attackers didn't use botnets but instead exploited vulnerable web servers on the internet with spoofed traffic, which in turn flooded GitHub servers. Despite the enormity of the traffic volume and the clever exploit of the mem cached databases, GitHub services were impacted for only about 20 minutes.

The traffic graph below shows real-time traffic while the biggest DDoS in the history of the internet, was underway.



Here is the list of hosting countries with the largest DDoS weapons, China, USA and then Russia make the top three.



The statistics below shows that large and very large DDoS attacks are on the rise.

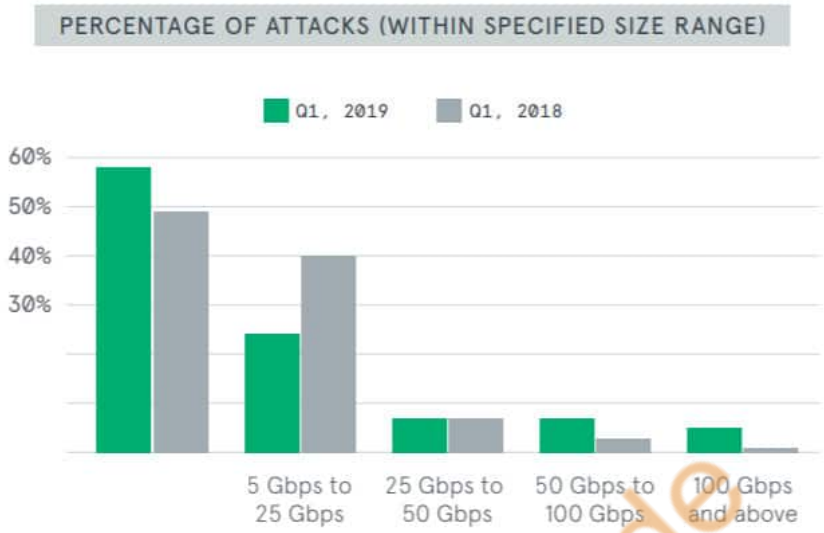
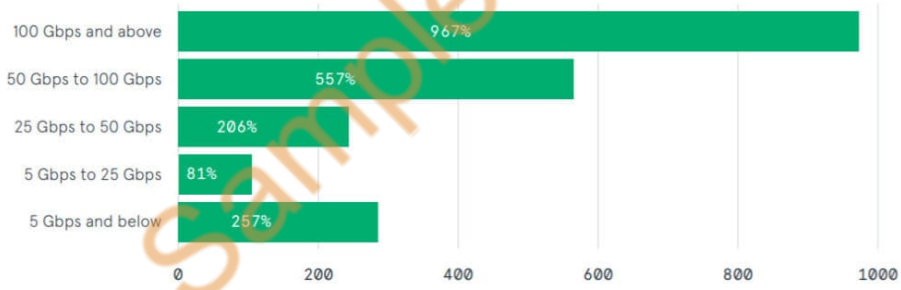


Figure 6 - Comparison of attacks by size Q1, 2019 vs. Q1, 2018



As per A10 Networks, the top 5 BGP ASNs with infected IP addresses include China, Brazil, Russia and S. Korea.

- China Unicom
- China Telecom
- TIM Cellular S.A. (Brazil)
- Rostelecom (Russia)
- Korea Telecom (South Korea)