SECURITY

Network Security with NetFlow and IPFIX

Big Data Analytics for Information Security

ciscopress.com

Omar Santos

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Network Security with NetFlow and IPFIX

Big Data Analytics for Information Security

Omar Santos

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Network Security with NetFlow and IPFIX

Omar Santos

Copyright© 2016 Cisco Systems, Inc.

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing September 2015

Library of Congress Control Number: 2015945876

ISBN-13: 978-1-58714-438-7

ISBN-10: 1-58714-438-7

Warning and Disclaimer

This book is designed to provide information about network security using Cisco NetFlow. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, 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 book or from the use of the discs or programs that may accompany it.

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

Trademark Acknowledgments

All terms mentioned in this book 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 book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

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 from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Acquisitions Editor: Denise Lincoln

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Copy Editor: Keith Cline

Technical Editors: Lou Ronnau, John Stuppi

Editorial Assistant: Vanessa Evans

Book Designer: Mark Shirar

Composition: CodeMantra

Senior Indexer: Cheryl Lenser

Proofreader: Sarah Kearns

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.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Author

Omar Santos is a Principal Engineer in the Cisco Product Security Incident Response Team (PSIRT) part of Cisco's Security Research and Operations. He mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities in all Cisco products. Omar has been working with information technology and cyber security since the mid-1990s. Omar has designed, implemented, and supported numerous secure networks for Fortune 100 and 500 companies and for the U.S. government. Prior to his current role, he was a Technical Leader within the World Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations.

Omar is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of several books and numerous whitepapers, articles, and security configuration guidelines and best practices. He has also delivered numerous technical presentations at many conferences and to Cisco customers and partners, in addition to many C-level executive presentations to many organizations. Omar is the author of the following Cisco Press books:

- *CCNA Security 210-260 Official Cert Guide*, ISBN-13: 9781587205668
- *Deploying Next-Generation Firewalls Live Lessons*, ISBN-13: 9781587205705
- *Cisco's Advanced Malware Protection (AMP)*, ISBN-13: 9781587144462
- *Cisco ASA Next-Generation Firewall, IPS, and VPN Services* (3rd Edition), ISBN-10: 1587143070
- *Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance* (2nd Edition), ISBN-10: 1587058197
- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*, ISBN-10: 1587052091
- *Cisco Network Admission Control, Volume: Deployment and Management*, ISBN-10: 1587052253
- *End-to-End Network Security: Defense-in-Depth*, ISBN-10: 1587053322

About the Technical Reviewers

John Stuppi, CCIE No. 11154, is a Technical Leader in the Cisco Security Solutions (CSS) organization at Cisco, where he consults Cisco customers on protecting their network against existing and emerging cyber security threats. In this role, John is responsible for providing effective techniques using Cisco product capabilities to provide identification and mitigation solutions for Cisco customers who are concerned with current or expected security threats to their network environments. Current projects include helping customers leverage DNS and NetFlow data to identify and subsequently mitigate network-based threats. John has presented multiple times on various network security topics at Cisco Live, Black Hat, and other customer-facing cyber security conferences. In addition, John contributes to the Cisco Security Portal through the publication of whitepapers, Security Blog posts, and Cyber Risk Report articles. Prior to joining Cisco, John worked as a network engineer for JPMorgan, and then as a network security engineer at Time, Inc., with both positions based in New York City. John is also a CISSP (#25525) and holds an Information Systems Security (INFOSEC) professional certification. In addition, John has a Bachelor of Science in Electrical Engineering degree from Lehigh University and an MBA from Rutgers University. John lives in Ocean Township, New Jersey (a.k.a the Jersey Shore) with his wife, two kids, and his dog.

Lou Ronnau is a Consulting Engineer in the Cisco Security Solutions group at Cisco Systems, where he has worked for more than 20 years. In this position, he works with customers to identify and mitigate threats to the secure operation of their data networks. Lou has presented at Cisco Live and other industry security conferences and is a Cisco Press author. In his spare time, Lou enjoys flying as a private pilot and scuba diving.

Dedication

I want to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

I also dedicate this book to my father, Jose, and write in memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

Acknowledgments

I want to thank the technical editors, John Stuppi and Lou Ronnau, for their time and technical expertise. They verified my work and corrected me in all the major and minor mistakes that were hard to find.

I also want to thank the Cisco Press team, especially Denise Lincoln, Chris Cleveland, and Mandie Frank for their patience, guidance, and consideration. Their efforts are greatly appreciated.

Kudos to the Cisco product development teams for delivering such a great product portfolio.

Finally, I want to acknowledge the Cisco PSIRT and Security Research and Operations. Some of the best and brightest minds in the network security industry work there, supporting and protecting our Cisco customers, often under very stressful conditions and working miracles daily.

Contents at a Glance

Introduction xvi

Chapter 1 Introduction to NetFlow and IPFIX 1

Chapter 2 Cisco NetFlow Versions and Features 39

Chapter 3 Cisco Flexible NetFlow 59

Chapter 4 NetFlow Commercial and Open Source Monitoring and Analysis Software Packages 75

Chapter 5 Big Data Analytics and NetFlow 111

Chapter 6 Cisco Cyber Threat Defense and NetFlow 129

Chapter 7 Troubleshooting NetFlow 189

Chapter 8 Case Studies 247

Index 273

Contents

Introduction xvi

Chapter 1 Introduction to NetFlow and IPFIX 1

Introduction to NetFlow 1

The Attack Continuum 2

The Network as a Sensor and as an Enforcer 3

What Is a Flow? 4

NetFlow Versus IP Accounting and Billing 6

NetFlow for Network Security 7

Anomaly Detection and DDoS Attacks 8

Data Leak Detection and Prevention 9

Incident Response and Network Security Forensics 9

Traffic Engineering and Network Planning 14

IP Flow Information Export 15

IPFIX Architecture 16

IPFIX Mediators 17

IPFIX Templates 17

Option Templates 19

Introduction to the Stream Control Transmission Protocol (SCTP) 19

Supported Platforms 20

Introduction to Cisco Cyber Threat Defense 21

Cisco Application Visibility and Control and NetFlow 22

Application Recognition 22

Metrics Collection and Exporting 23

Management and Reporting Systems 23

Control 23

Deployment Scenarios 24

Deployment Scenario: User Access Layer 24

Deployment Scenario: Wireless LAN 25

Deployment Scenario: Internet Edge 26

Deployment Scenario: Data Center 28

Public, Private, and Hybrid Cloud Environments 32

Deployment Scenario: NetFlow in Site-to-Site and Remote VPNs 33

NetFlow Remote-Access VPNs 33

NetFlow Site-to-Site VPNs 34

NetFlow Collection Considerations and Best Practices 35

Determining the Flows per Second and Scalability 36

Summary 37

Chapter 2 Cisco NetFlow Versions and Features 39

NetFlow Versions and Respective Features 39

NetFlow v1 Flow Header Format and Flow Record Format 40

NetFlow v5 Flow Header Format and Flow Record Format 41

NetFlow v7 Flow Header Format and Flow Record Format 42

NetFlow Version 9 43

NetFlow and IPFIX Comparison 57

Summary 57

Chapter 3 Cisco Flexible NetFlow 59

Introduction to Cisco's Flexible NetFlow 59

Simultaneous Application Tracking 60

Flexible NetFlow Records 61

Flexible NetFlow Key Fields 61

Flexible NetFlow Non-Key Fields 63

NetFlow Predefined Records 65

User-Defined Records 65

Flow Monitors 65

Flow Exporters 65

Flow Samplers 66

Flexible NetFlow Configuration 66

Configure a Flow Record 67

Configuring a Flow Monitor for IPv4 or IPv6 69

Configuring a Flow Exporter for the Flow Monitor 71

Applying a Flow Monitor to an Interface 73

Flexible NetFlow IPFIX Export Format 74

Summary 74

Chapter 4 NetFlow Commercial and Open Source Monitoring and Analysis Software Packages 75

Commercial NetFlow Monitoring and Analysis Software Packages 75

Lancope's StealthWatch Solution 76

Plixer's Scrutinizer 79

Open Source NetFlow Monitoring and Analysis Software Packages 80

NFdump 81

NfSen 86
SiLK 86
SiLK Configuration Files 87
Filtering, Displaying, and Sorting NetFlow Records with SiLK 87
SiLK's Python Extension 88
Counting, Grouping, and Mating NetFlow Records with Silk 88
SiLK IPset, Bag, and Prefix Map Manipulation Tools 88
IP and Port Labeling Files 89
SiLK Runtime Plug-Ins 89
SiLK Utilities for Packet Capture and IPFIX Processing 90
Utilities to Detect Network Scans 90
SiLK Flow File Utilities 90
Additional SiLK Utilities 91
Elasticsearch, Logstash, and Kibana Stack 92
Elasticsearch 92
Logstash 92
Kibana 93
Elasticsearch Marvel and Shield 94
ELK Deployment Topology 94
Installing ELK 95
Installing Elasticsearch 96
Install Kibana 105
Installing Nginx 106
Install Logstash 107
Summary 109

Chapter 5 Big Data Analytics and NetFlow 111
Introduction to Big Data Analytics for Cyber Security 111
What Is Big Data? 111
Unstructured Versus Structured Data 112
Extracting Value from Big Data 113
NetFlow and Other Telemetry Sources for Big Data Analytics for Cyber Security 114
OpenSOC 115
Hadoop 116
HDFS 117
Flume 119

Kafka 120

Storm 121

Hive 122

Elasticsearch 123

HBase 124

Third-Party Analytic Tools 125

Other Big Data Projects in the Industry 126

Understanding Big Data Scalability: Big Data Analytics in the Internet of Everything 127

Summary 128

Chapter 6 Cisco Cyber Threat Defense and NetFlow 129

Overview of the Cisco Cyber Threat Defense Solution 129

The Attack Continuum 130

Cisco CTD Solution Components 131

NetFlow Platform Support 133

Traditional NetFlow Support in Cisco IOS Software 133

NetFlow Support in Cisco IOS-XR Software 135

Flexible NetFlow Support 135

NetFlow Support in Cisco ASA 140

Deploying the Lancope StealthWatch System 140

Deploying StealthWatch FlowCollectors 142

StealthWatch FlowReplicators 146

StealthWatch Management Console 146

Deploying NetFlow Secure Event Logging in the Cisco ASA 148

Deploying NSEL in Cisco ASA Configured for Clustering 151

Unit Roles and Functions in Clustering 152

Clustering NSEL Operations 152

Configuring NSEL in the Cisco ASA 153

Configuring NSEL in the Cisco ASA Using ASDM 153

Configuring NSEL in the Cisco ASA Using the CLI 155

NSEL and Syslog 156

Defining the NSEL Export Policy 157

Monitoring NSEL 159

Configuring NetFlow in the Cisco Nexus 1000V 160

Defining a Flow Record 161

Defining the Flow Exporter 162

Defining a Flow Monitor 163

Applying the Flow Monitor to an Interface 164

Configuring NetFlow in the Cisco Nexus 7000 Series 164

Configuring the Cisco NetFlow Generation Appliance 166

Initializing the Cisco NGA 166

Configuring NetFlow in the Cisco NGA via the GUI 168

Configuring NetFlow in the Cisco NGA via the CLI 169

Additional Cisco CTD Solution Components 171

Cisco ASA 5500-X Series Next-Generation Firewalls and the Cisco ASA with FirePOWER Services 171

Next-Generation Intrusion Prevention Systems 172

FireSIGHT Management Center 173

AMP for Endpoints 173

AMP for Networks 176

AMP Threat Grid 176

Email Security 177

Email Security Appliance 177

Cloud Email Security 179

Cisco Hybrid Email Security 179

Web Security 180

Web Security Appliance 180

Cisco Content Security Management Appliance 184

Cisco Cloud Web Security 185

Cisco Identity Services Engine 186

Summary 187

Chapter 7 Troubleshooting NetFlow 189

Troubleshooting Utilities and Debug Commands 189

Troubleshooting NetFlow in Cisco IOS and Cisco IOS XE Devices 194

Cisco IOS Router Flexible NetFlow Configuration 195

Troubleshooting Communication Problems with the NetFlow Collector 201

Additional Useful Troubleshooting Debug and Show Commands 204

Verifying a Flow Monitor Configuration 204

Displaying Flow Exporter Templates and Export IDs 207

Debugging Flow Records 212

Preventing Export Storms with Flexible NetFlow 213

Troubleshooting NetFlow in Cisco NX-OS Software 214

Troubleshooting NetFlow in Cisco IOS-XR Software 217

Flow Exporter Statistics and Diagnostics 219

Flow Monitor Statistics and Diagnostics 222

Displaying NetFlow Producer Statistics in Cisco IOS-XR 226

Additional Useful Cisco IOS-XR Show Commands 228

Troubleshooting NetFlow in the Cisco ASA 228

Troubleshooting NetFlow in the Cisco NetFlow Generation Appliance 235

Gathering Information About Configured NGA Managed Devices 235

Gathering Information About the Flow Collector 236

Gathering Information About the Flow Exporter 237

Gathering Information About Flow Records 237

Gathering Information About the Flow Monitor 238

Show Tech-Support 239

Additional Useful NGA show Commands 245

Summary 246

Chapter 8 Case Studies 247

Using NetFlow for Anomaly Detection and Identifying DoS Attacks 247

Direct DDoS Attacks 248

Reflected DDoS Attacks 248

Amplification Attacks 249

Identifying DDoS Attacks Using NetFlow 250

Using NetFlow in Enterprise Networks to Detect DDoS Attacks 250

Using NetFlow in Service Provider Networks to Detect DDoS Attacks 253

Using NetFlow for Incident Response and Forensics 254

Credit Card Theft 254

Theft of Intellectual Property 259

Using NetFlow for Monitoring Guest Users and Contractors 262

Using NetFlow for Capacity Planning 267

Using NetFlow to Monitor Cloud Usage 269

Summary 271

Index 273

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Cisco NetFlow is now the primary network accounting technology in the industry. Visibility into the network is an indispensable tool for network and security professionals. In response to new requirements and cyber security headaches, network operators and security professionals are finding it critical to understand how the network is behaving. Cisco NetFlow creates an environment where network administrators and security professionals have the tools to understand who, what, when, where, and how network traffic is flowing.

Who Should Read This Book?

This book serves as comprehensive guide for any network and security professional who manages network security, installs and configures network security features to provide additional visibility. It encompasses topics from an introductory level to advanced topics on Cisco NetFlow, Cisco Cyber Threat Defense, and big data analytics tools such as Logstash, Kibana, Elasticsearch, and many others.

How This Book Is Organized

The following is an overview of how this book is organized:

- **Chapter 1, "Introduction to NetFlow and IPFIX":** This chapter provides an overview of Cisco NetFlow and IPFIX. Cisco NetFlow and IPFIX provide a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, denial-of-service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing. Cisco invented NetFlow and is the leader in IP traffic flow technology.
- **Chapter 2, "Cisco NetFlow Versions and Features":** This chapter covers the different Cisco NetFlow versions and features available on each version. It also covers the NetFlow v9 export format and packet details, and includes a detailed comparison between NetFlow and IPFIX.
- **Chapter 3, "Cisco Flexible NetFlow":** Flexible NetFlow provides enhanced optimization of the network infrastructure, reduces costs, and improves capacity planning and security detection beyond other flow-based technologies available today. This chapter provides an introduction to Cisco's Flexible NetFlow, and it covers the Flexible NetFlow components and fields. It also provides step-by-step guidance on how to configure flexible NetFlow in Cisco IOS Software.
- **Chapter 4, "NetFlow Commercial and Open Source Monitoring and Analysis Software Packages":** This chapter provides details about the top commercial NetFlow analyzers. It also provides detailed information about the top open source NetFlow analyzers including SiLK, Flow-tools, FlowScan, NTop, EHNT, BPFT, Cflowd, Logstash, Kibana, Elasticsearch, and others.

- **Chapter 5, "Big Data Analytics and NetFlow":** Big data analytics is a key and growing network security, monitoring, and troubleshooting trend. Cisco NetFlow provides a source of relevant big data that customers should be analyzing to improve the performance, stability, and security of their networks. This chapter describes how NetFlow is used for big data analytics for cyber security, along with other network telemetry capabilities such as firewall logs, syslog, SNMP, and authentication, authorization and accounting logs, in addition to logs from routers and switches, servers, and endpoint stations, among others.

- **Chapter 6, "Cisco Cyber Threat Defense and NetFlow":** Cisco has partnered with Lancope to deliver a solution that provides visibility into security threats by identifying suspicious traffic patterns in the corporate network. These suspicious patterns are then augmented with circumstantial information necessary to determine the level of threat associated with a particular incident. This solution allows a network administrator or security professional to analyze this information in a timely, efficient, and cost-effective manner for advanced cyber threats. This chapter provides detailed coverage of Cisco Cyber Threat Defense Solution. Cisco Cyber Threat Defense Solution utilizes the Lancope StealthWatch System to analyze NetFlow information from Cisco switches, routers, and the Cisco ASA 5500 Next-Generation Firewalls to detect advanced and persistent security threats such as internally spreading malware, data leakage, botnet command-and-control traffic, and network reconnaissance. The Cisco ISE solution supplements StealthWatch NetFlow-based behavioral threat detection data with contextual information such as user identity, user authorization level, device type, and posture. This chapter provides design and configuration guidance when deploying the Cisco Cyber Threat Defense Solution.

- **Chapter 7, "Troubleshooting NetFlow":** This chapter focuses on the different techniques and best practices available when troubleshooting NetFlow deployments and configurations. It assumes that you already have an understanding of the topics covered in previous chapters, such as configuration and deployment of NetFlow in all the supported devices.

- **Chapter 8, "Case Studies":** This chapter covers several case studies and real-life scenarios on how NetFlow is deployed in large enterprises and in small and medium-sized businesses.

This page intentionally left blank

This page intentionally left blank

Chapter 5

Big Data Analytics and NetFlow

This chapter covers the following topics:

- Introduction to big data analytics for cyber security
- NetFlow and other telemetry sources for big data analytics for cyber security
- Open Security Operations Center (OpenSOC)
- Understanding big data scalability: Big data analytics in the Internet of Everything (IoE)

Introduction to Big Data Analytics for Cyber Security

Big data analytics is the practice of studying large amounts of data of a variety of types and a variety of courses to learn interesting patterns, unknown facts, and other useful information. Big data analytics can play a crucial role in cyber security. Many in the industry are changing the tone of their conversation, saying that it is no longer if or when your network will be compromised, but the assumption is that your network has already been hacked or compromised, and suggest focusing on minimizing the damage and increasing visibility to aid in identification of the next hack or compromise.

Advanced analytics can be run against very large diverse data sets to find indicators of compromise (IOCs). These data sets can include different types of structured and unstructured data processed in a "streaming" fashion or in batches. NetFlow plays an important role for big data analytics for cyber security, and you will learn why as you read through in this chapter.

What Is Big Data?

There are a lot of very interesting definitions for the phenomenon called *big data*. It seems that a lot of people have different views of what big data is. Let's cut through the marketing hype and get down to the basics of the subject. A formal definition for big data can be obtained in the Merriam-Webster dictionary: http://www.merriam-webster.com/dictionary/big%20data.

> An accumulation of data that is too large and complex for processing by traditional database management tools.
>
> Big data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process the data within a tolerable elapsed time.

The size of data that can be classified as big data is a moving target. It can range from a few terabytes to yottabytes of data in a single data set. For instance:

- A petabyte is 1000 terabytes.
- An exabyte is 1000 petabytes.
- A zettabyte is 1000 exabytes.
- A yoyabyte is 1000 zettabytes.

Tip Cisco has created the Cisco Visual Networking Index (VNI). Cisco VNI is an ongoing initiative to forecast and analyze the growth and use of the Internet, in addition to the data being transferred. You can find details of the Cisco VNI global IP traffic forecast and the methodology behind it at http://www.cisco.com/go/vni.

Unstructured Versus Structured Data

The term *unstructured data* is used when referring to data that does not have a predefined data model or is not organized in a predetermined way. Typically, unstructured data is defined as data that is not typically tracked in a “structured” or traditional row-column database. The prime examples of unstructured data are as follows:

- Multimedia content such as videos, photos, and audio files
- E-mail messages
- Social media (Facebook, Twitter, LinkedIn) status updates
- Presentations
- Word processing documents
- Blog posts
- Executable files

In the world of cyber security, a lot of the network can be also categorized as unstructured:

- Syslog
- Simple Network Management Protocol (SNMP) logs

- NetFlow
- Server and host logs
- Packet captures
- Executables
- Malware
- Exploits

Industry experts estimate that the majority of the data in any organization is unstructured, and the amount of unstructured data is growing significantly. There are numerous, disparate data sources. NetFlow is one of the largest single sources, and it can grow to tens of terabytes of data per day in large organizations, and it is expected to grow over the years to petabytes. The differentiation in the usefulness of any big data solution is the merging of numerous data sources and sizes that are all in the same infrastructure and providing the ability to query across all of these different data sets using the same language and tools.

There is an industry concept called *Not-Only SQL* (NoSQL), which is the name given to several databases that do not require SQL to process data. However, some of these databases support both SQL and non-SQL forms of data processing.

Big data analytics can be done in combination of advanced analytics disciplines such as predictive analytics and data mining.

Note Cisco acquired Cognitive Security in 2013, a company focused on applying artificial intelligence techniques to detect advanced cyber threats. The new Cisco security solutions integrate a range of sophisticated technologies to identify and analyze key threats through advanced behavioral analysis of real-time data.

Extracting Value from Big Data

Any organization can collect data just for the matter of collecting data; however, the usefulness of such data depends on how actionable such data is to make any decisions (in addition to whether the data is regularly monitored and analyzed).

There are three high-level key items for big data analytics:

- **Information management:** An ongoing management and process control for big data analytics.
- **High-performance analytics:** The ability to gain fast actionable information from big data and being able to solve complex problems using more data.
- **Flexible deployment options:** Options for on-premises or cloud-based, software-as-a-service (SaaS) tactics for big data analytics.

There are a few high-level approaches for accelerating the analysis of giant data sets. The following are the most common:

- **Grid computing:** A centralized grid infrastructure for dynamic analysis with high availability and parallel processing.
- **Intra-database processing:** Performing data management, analytics, and reporting tasks using scalable architectures.
- **In-memory analytics:** Quickly solves complex problems using in-memory, multiuse access to data and rapidly runs new scenarios or complex analytical computations.
- **Support for Hadoop:** Stores and processes large volumes of data on commodity hardware. Hadoop will be covered in a few pages in the section "Hadoop."
- **Visualizations:** Quickly visualize correlations and patterns in big data to identify opportunities for further analysis and to improve decision making.

Examples of technologies used in big data analytics are covered in detail later in this chapter.

NetFlow and Other Telemetry Sources for Big Data Analytics for Cyber Security

As discussed in Chapter 1, "Introduction to NetFlow and IPFIX," NetFlow provides detailed network telemetry that allows the administrator to:

- See what is actually happening across your entire network
- Regain control of your network, in case of denial-of-service (DoS) attack
- Quickly identify compromised endpoints and network infrastructure devices
- Monitor network usage of employees, contractors, or partners
- Obtain network telemetry during security incident response and forensics
- Detect firewall misconfigurations and inappropriate access to corporate resources

As previously mentioned, NetFlow data can grow to tens of terabytes of data per day in large organizations, and it is expected to grow over the years to petabytes. However, many other telemetry sources can be used in conjunction with NetFlow to identify, classify, and mitigate potential threats in your network. Figure 5-1 shows examples of these telemetry sources and how they "feed" into a collection engine.

As illustrated in Figure 5-1, NetFlow data, syslog, SNMP logs, server and host logs, packet captures, and files (such as executables, malware, exploits) can be parsed, formatted, and combined with threat intelligence information and other "enrichment data" (network metadata) to perform analytics. This process is not an easy one; this is why Cisco has created an open source framework for big data analytics called *Open Security Operations Center* (OpenSOC). The following section provides an in-depth look at the OpenSOC framework.

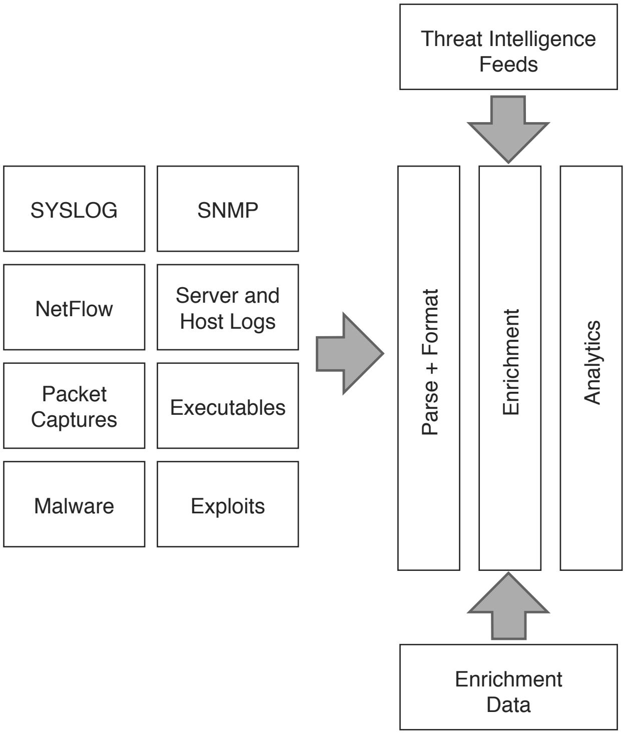

Figure 5-1 *NetFlow and Other Telemetry Sources*

OpenSOC

OpenSOC was created by Cisco to attack the "big data problem" for their Managed Threat Defense offering. Cisco has developed a fully managed service delivered by Cisco Security Solutions to help customers protect against known intrusions, zero-day attacks, and advanced persistent threats. Cisco has a global network of security operations centers (SOCs) ensuring constant awareness and on-demand analysis 24 hours a day, 7 days a week. They needed the ability to capture full packet-level data and extract protocol metadata to create a unique profile of customer's network and monitor them against Cisco threat intelligence. As you can imagine, performing big data analytics for one organization is a challenge, Cisco has to perform big data analytics for numerous customers including very large enterprises. The goal with OpenSOC is to have a robust framework based on proven technologies to combine machine learning algorithms and predictive analytics to detect today's security threats.

The following are some of the benefits of OpenSOC:

- The ability to capture raw network packets, store those packets, and perform traffic reconstruction

- Collect any network telemetry, perform enrichment, and generate real-time rules-based alerts
- Perform real-time search and cross-telemetry matching
- Automated reports
- Anomaly detection and alerting
- Integration with existing analytics tools

Note OpenSOC is open sourced under the Apache license.

The primary components of OpenSOC include the following:

- Hadoop
- Flume
- Kafka
- Storm
- Hive
- Elasticsearch
- HBase
- Third-party analytic tool support (R, Python-based tools, Power Pivot, Tableau, and so on)

The sections that follow cover these components in more detail.

Hadoop

The Apache Hadoop or "Hadoop" is a project supported and maintained by the Apache Software Foundation. Hadoop is a software library designed for distributed processing of large data sets across clusters of computers. One of the advantages of Hadoop is its ability to using simple programming models to perform big data processing. Hadoop can scale from a single server instance to thousands of servers. Each Hadoop server or node performs local computation and storage. Cisco uses Hadoop clusters in OpenSOC to process large amounts of network data for their customers, as part of the Managed Threat Defense solution, and it also uses Hadoop for its internal threat intelligence ecosystem.

Hadoop includes the following modules:

- **Hadoop Common:** The underlying utilities that support the other Hadoop modules.
- **Hadoop Distributed File System (HDFS):** A highly scalable and distributed file system.

- **Hadoop YARN:** A framework design for job scheduling and cluster resource management.
- **Hadoop MapReduce (MapR):** A system designed for parallel processing of large data sets based on YARN.

Figure 5-2 illustrates a Hadoop cluster.

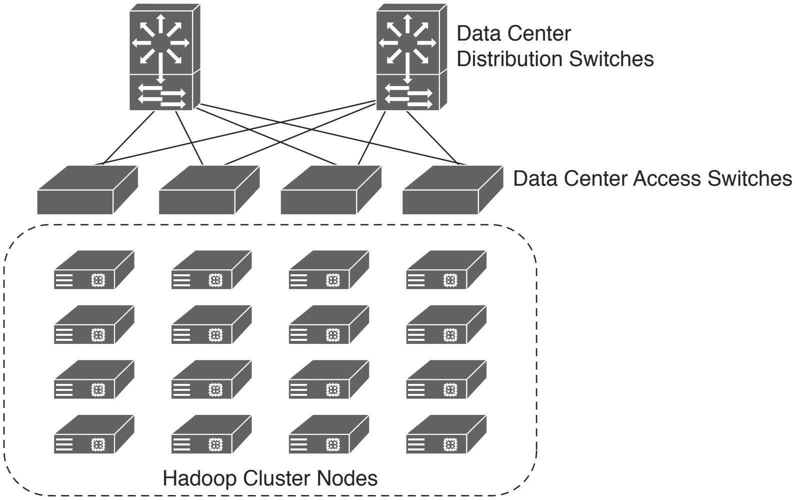

Figure 5-2 *Hadoop Cluster Example*

In Figure 5-2, a total of 16 servers are configured in a Hadoop cluster and connected to the data center access switches for big data processing.

HDFS

HDFS is a highly scalable and distributed file system that can scale to thousands of cluster nodes, millions of files, and petabytes of data. HDFS is optimized for batch processing where data locations are exposed to allow computations to take place where the data resides. HDFS provides a single namespace for the entire cluster to allow for data coherency in a write-once, read-many access model. In other words, clients can only append to existing files in the node. In HDFS, files are separated into blocks, which are typically 64 MB in size and are replicated in multiple data nodes. Clients access data directly from data nodes. Figure 5-3 shows a high-level overview of the HDFS architecture.

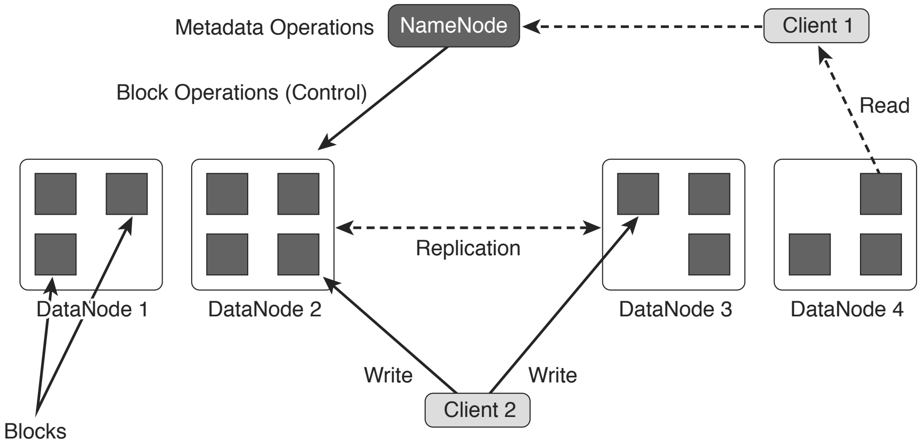

Figure 5-3 *HDFS Architecture*

In Figure 5-3, the NameNode (or Namespace Node) maps a filename to a set of blocks and the blocks to the data nodes where the block resides. There are a total of four data nodes, each with a set of data blocks. The NameNode performs cluster configuration management and controls the replication engine for blocks throughout the cluster. The NameNode metadata includes the following:

- The list of files
- List of blocks for each file
- List of data nodes for each block
- File attributes such as creation time and replication factor

The NameNode also maintains a transaction log that records file creations, deletions, and modifications.

Each DataNode includes a block server that stores data in the local file system, stores metadata of a block, and provisions data and metadata to the clients. DataNodes also periodically send a report of all existing blocks to the NameNode and forward data to other specified DataNodes as needed. DataNodes send a heartbeat message to the NameNode on a periodic basis (every 3 seconds by default), and the NameNode uses these heartbeats to detect any DataNode failures. Clients can read or write data to each data block, as shown in Figure 5-3.

Note You can obtain more detailed information and download Hadoop at http://hadoop.apache.org.

Flume

OpenSOC uses Flume for collecting, aggregating, and moving large amounts of network telemetry data (like NetFlow, syslog, SNMP, and so on) from many different sources to a centralized data store. Flume is also licensed under the Apache license. Figure 5-4 shows how different network telemetry sources are sent to Flume agents for processing.

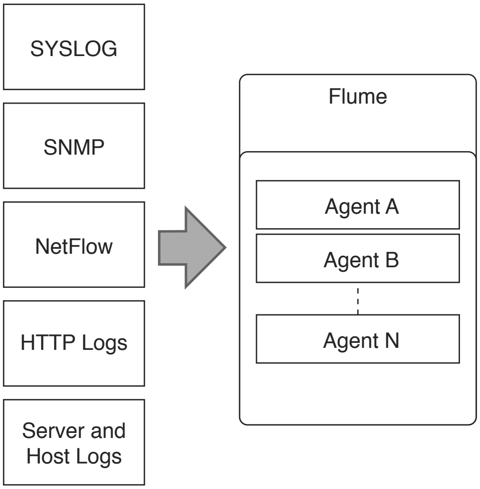

Figure 5-4 *Network Telemetry Sources and Flume*

Flume has the following components and concepts:

- **Event:** A specific unit of data that is transferred by Flume, such as a single NetFlow record.
- **Source:** The source of the data. These sources are either actively queried for new data or they can passively wait for data to be delivered to them. The source of this data can be NetFlow collectors, server logs from Splunk, or similar entities.
- **Sink:** Delivers the data to a specific destination.
- **Channel:** The conduit between the source and the sink.
- **Agent:** A Java virtual machine running Flume that comprises a group of sources, sinks, and channels.
- **Client:** Creates and transmits the event to the source operating within the agent.

Figure 5-5 illustrates Flume's high-level architecture and its components.

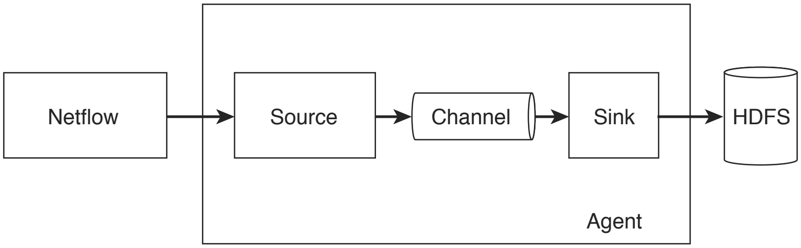

Figure 5-5 *Flume Architecture*

> **Note** You can obtain more detailed information and download Flume at http://flume.apache.org.

Kafka

OpenSOC uses Kafka as its messaging system. Kafka is a distributed messaging system that is partitioned and replicated. Kafka uses the concept of *topics*. Topics are feeds of messages in specific categories. For example, Kafka can take raw packet captures and telemetry information from Flume (after processing NetFlow, syslog, SNMP, or any other telemetry data), as shown in Figure 5-6.

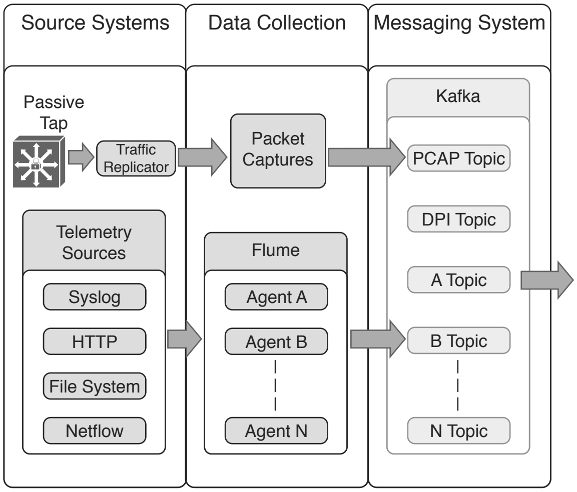

Figure 5-6 *Kafka Example in OpenSOC*

In Figure 5-6, a topic is a category or feed name to which log messages and telemetry information are exchanged (published). Each topic is an ordered, immutable sequence of messages that is continually appended to a commit log.

Kafka provides a single "consumer" abstraction layer, as illustrated in Figure 5-7.

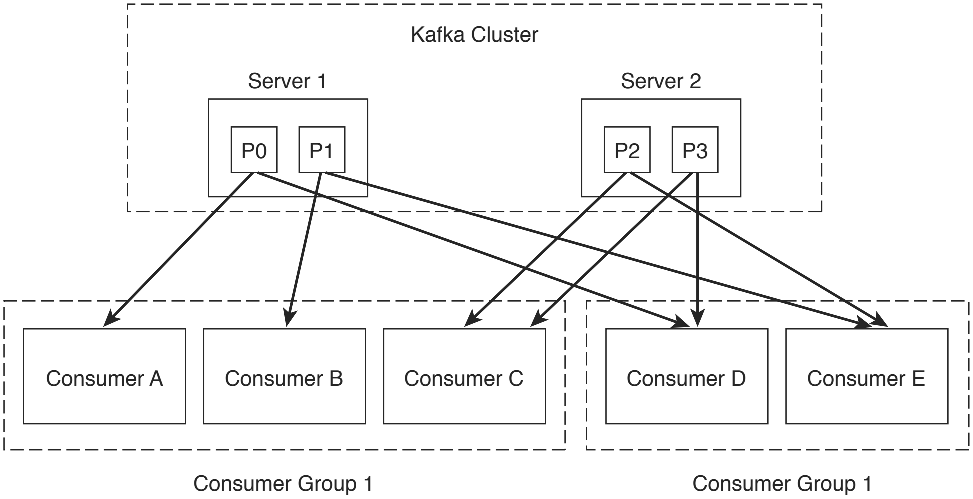

Figure 5-7 *Kafka Cluster and Consumers*

Consumers are organized in consumer groups, and each message published to a topic is sent to one consumer instance within each subscribing consumer group.

Note Consumers can be in separate processes or on separate machines.

All consumer instances that belong to the same consumer group are processed in a traditional queue load balancing. Consumers in different groups process messages in a publish-subscribe mode, where all the messages are broadcast to all consumers.

In Figure 5-7, the Kafka cluster contains two servers (Server 1 and Server 2), each with two different partitions. Server 1 contains partition 0 (P0) and partition 1 (P1). Server 2 contains partition 2 (P2) and partition 3 (P3). Two consumer groups are illustrated. Consumer Group 1 contains consumers A, B, and C. Consumer Group 2 contains consumers: D and E.

Kafka provides parallelism to provide ordering guarantees and load balancing over a pool of consumer processes. However, there cannot be more consumer instances than partitions.

Note You can obtain more detailed information and download Kafka at http://kafka.apache.org.

Storm

Storm is an open source, distributed, real-time computation system under the Apache license. It provides real-time processing and can be used with any programming language.

Hadoop consists of two major components: HDFS and MapReduce. The early implementations of Hadoop and MapReduce were designed on batch analytics, which does not provide any real-time processing. In SOCs, you often cannot process data in batches, and so it can take several hours to complete the analysis.

Note Depending on the amount of data, the number of nodes in the cluster, the technical specifications of each node, and the complexity of the analytics, MapReduce can take anywhere from minutes to hours to perform a job. In security, you need to respond fast!

OpenSOC uses Storm because it provides real-time streaming and because of its amazing ability to process big data, at scale, in real time. Storm can process data at over a million tuples processed per second per node. Figure 5-8 shows how Kafka topics feed information to Storm to provide real-time processing.

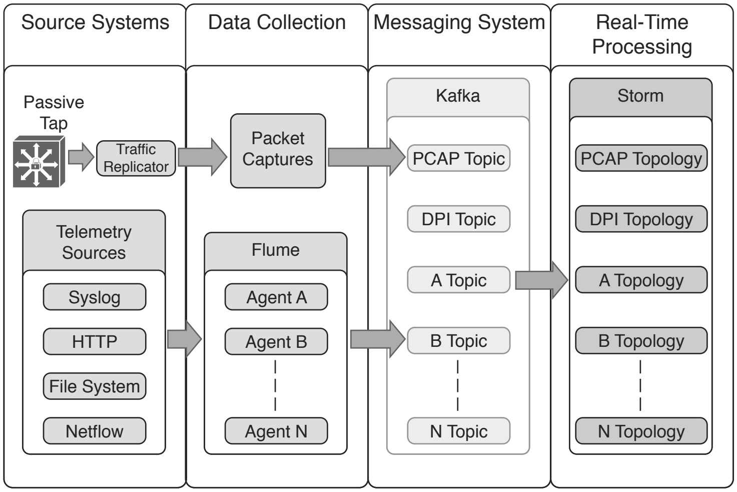

Figure 5-8 *Storm in OpenSOC*

Note You can obtain more detailed information and download Storm at https://storm.incubator.apache.org.

Hive

Hive is a data warehouse infrastructure that provides data summarization and ad hoc querying. Hive is also a project under the Apache license. OpenSOC uses Hive because of its querying capabilities. Hive provides a mechanism to query data using a SQL-like language that is called HiveQL. In the case of batch processing, Hive allows MapR programmers use their own custom mappers.

Figure 5-9 shows how Storm feeds into Hive to provide data summarization and querying.

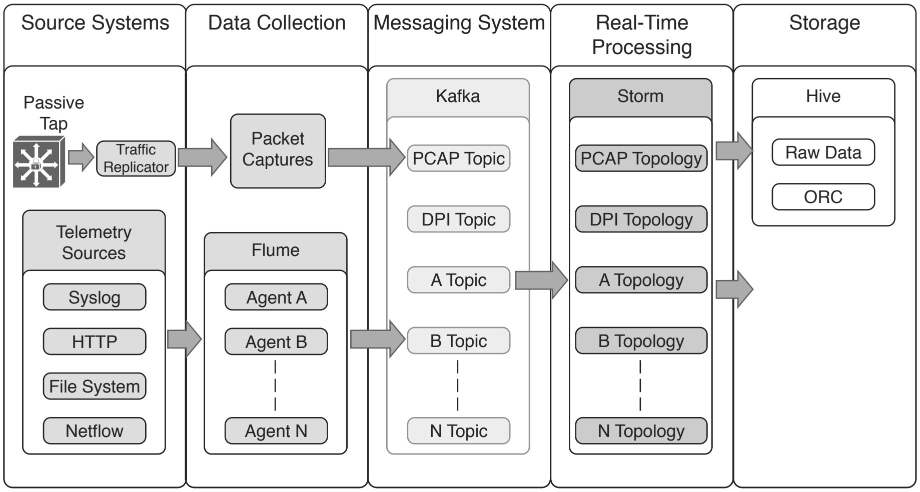

Figure 5-9 *Hive in OpenSOC*

Note You can obtain more detailed information and download Hive at https://hive.apache.org.

Storm can also feed into HBase and Elasticsearch. These are covered in the following sections.

Elasticsearch

Elasticsearch is a scalable and real-time search and analytics engine that is also used by OpenSOC. Elasticsearch has a very strong set of application programming interfaces (APIs) and query domain-specific languages (DSLs). It provides full query DSL based on JSON to define such queries. Figure 5-10 shows how Storm feeds into Elasticsearch to provide real-time indexing and querying.

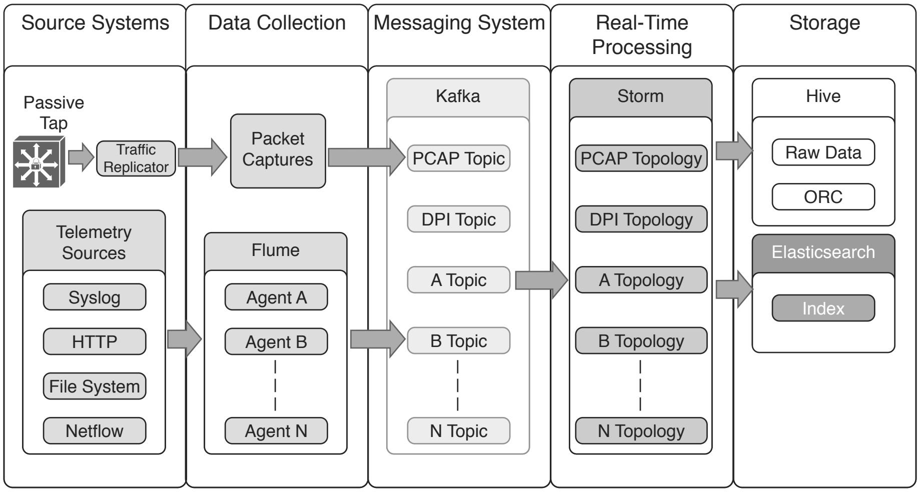

Figure 5-10 *Elasticsearch in OpenSOC*

Note You can obtain more detailed information and download Elasticsearch at http://www.elasticsearch.org.

HBase

HBase is scalable and distributed database that supports structured data storage for large tables. You guessed right: HBase is also under the Apache license! OpenSOC uses HBase because it provides random and real-time read/write access large data sets.

Note HBase is a nonrelational database modeled after Google's Bigtable.

HBase provides linear and modular scalability with consistent database reads and writes.

It also provides automatic and configurable high-availability (failover) support between Region Servers. HBase is a type of "NoSQL" database that can be scaled by adding Region Servers that are hosted on separate servers.

Figure 5-11 shows how Storm feeds into HBase to provide real-time indexing and querying.

Note You can obtain more detailed information and download HBase at https://hbase.apache.org.

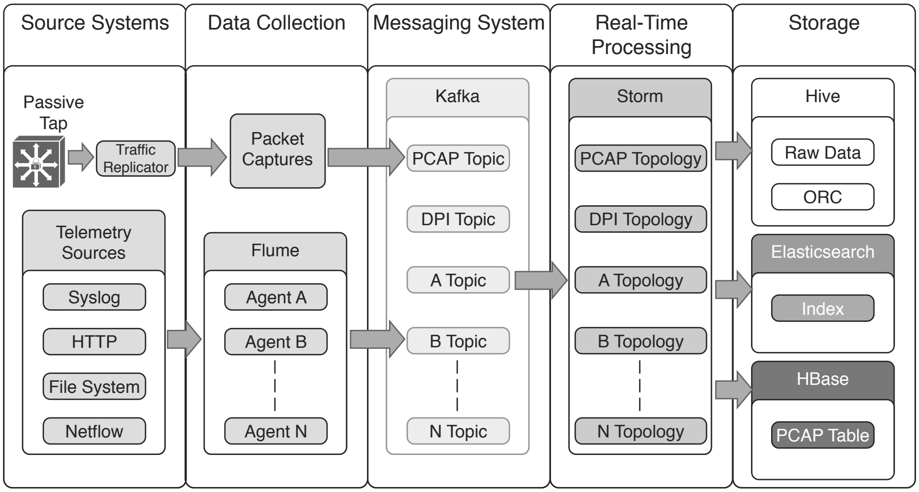

Figure 5-11 *HBase in OpenSOC*

Third-Party Analytic Tools

OpenSOC supports several third-party analytic tools such as:

- R-based and Python-based tools
- Power Pivot
- Tableau

Figure 5-12 shows the complete OpenSOC architecture, including analytics tools and web services for additional search, visualizations, and packet capture (PCAP) reconstruction.

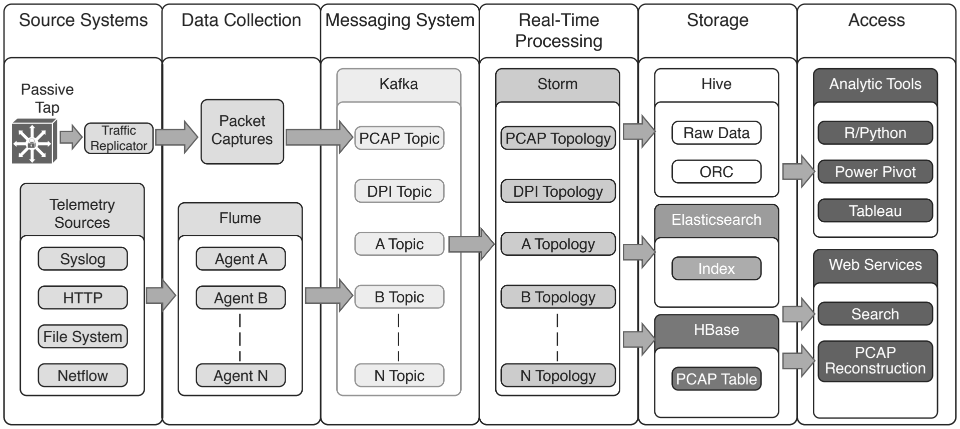

Figure 5-12 *OpenSOC Architecture*

Note You can download OpenSOC from https://github.com/OpenSOC.

Other Big Data Projects in the Industry

There are other Hadoop-related projects used in the industry for processing and visualizing big data. The following are a few examples:

- **Ambari:** A web-based tool and dashboard for provisioning, managing, and monitoring Apache Hadoop clusters.
- **Avro:** A data serialization system.
- **Cassandra:** A scalable multimaster database with no single points of failure.
- **Chukwa:** A data collection system for managing large distributed systems.
- **Mahout:** A scalable machine learning and data mining library.
- **Pig:** A high-level data-flow language and execution framework for parallel computation.
- **Spark:** A fast and general compute engine for Hadoop data.
- **Tez:** A generalized data-flow programming framework, built on Hadoop YARN.
- **ZooKeeper:** A high-performance coordination service for distributed applications.
- **Berkeley Data Analytics Stack (BDAS):** A framework created by Berkeley's AMPLabs. BDAS has a three-dimensional approach: algorithms, machines, and people. The following are the primary components of BDAS:
  - **Akaros:** An operating system for many-core architectures and large-scale SMP systems
  - **GraphX:** A large-scale graph analytics
  - **Mesos:** Dynamic resource sharing for clusters
  - **MLbase:** Distributed machine learning made easy
  - **PIQL:** Scale independent query processing
  - **Shark:** Scalable rich analytics SQL engine for Hadoop
  - **Spark:** Cluster computing framework
  - **Sparrow:** Low-latency scheduling for interactive cluster services
  - **Tachyon:** Reliable file sharing at memory speed across cluster frameworks

You can find detailed information about BDAS and Berkeley's AMPLabs at https://amplab.cs.berkeley.edu

Understanding Big Data Scalability: Big Data Analytics in the Internet of Everything

Evidently, the challenges of big data analytics include the following:

- Data capture capabilities
- Data management (curation)
- Storage
- Adequate and real-time search
- Sharing and transferring of information
- Deep-dive and automated analysis
- Adequate visualizations

Big data has become a hot topic due to the overabundance of data sources inundating today's data stores as applications proliferate. These challenges will become even bigger as the world moves to the *Internet of Everything* (IoE), a term coined by Cisco. IoE is based on the foundation of the Internet of Things (IoT) by adding network intelligence that allows convergence, orchestration, and visibility across previously disparate systems. IoT is the networked connection of physical objects. IoT is one of many technology transitions that enable the IoE.

The goal is to make networked connections more relevant by turning information into actions that create new capabilities. The IoE consists of many technology transitions, including the IoT. The key concepts are as follows:

- **Machine-to-machine connections:** Including things such as IoT sensors, remote monitoring, industrial control systems, and so on
- **People-to-people connections:** Including collaboration technologies such as TelePresence, WebEx, and so on
- **Machine-to-people connections:** Including traditional and new applications

Big data analytics for cyber security in an IoE world will require substantial engineering to address the huge data sets. Scalability will be a huge challenge. In addition, the endless variety of IoT applications presents a security operational challenge. We are starting to experience these challenges nowadays. For instance, in a factory floor, embedded programmable logic controllers (PLCs) that operate manufacturing systems and robots can be a huge target for bad actors. Do we know all the potential true indicators of compromise so that we can perform deep-dive analysis and perform good incident response?

The need to combine threat intelligence and big data analytics will be paramount in this ever-changing world.

Summary

Today, networks are becoming exponentially bigger and more complex. To maintain visibility and control of the network, many organizations are leveraging or planning to combine big data analytics with real-time, predictive analysis to detect attacks and protect against advanced malware across their networks. This combination can help security professionals address the ever-changing nature of threats that threaten their most important asset, which is data. This chapter provided an overview of the technologies and processes to use big data analytics for cyber security. NetFlow and other telemetry sources play a big role in big data analytics for cyber security. This chapter explained how you can use these telemetry sources to look for indicators of compromise in your network.

Cisco has developed and open source OpenSOC to provide a framework for big data analytics for cyber security. In this chapter, you learned the technologies and architectures used in OpenSOC and how they play a crucial role for security operations. The IoE introduces a lot of security challenges. One of the biggest challenges introduced is the ability to scale to large data sets. It is unavoidable that big data will continue to play a big role in cyber security.

This page intentionally left blank

Index

A

ACI (Application Centric Infrastructure) in data center, 30

Adaptive Security Device Manager (ASDM), 153-155

adjusting NetFlow timers in Cisco Nexus 7000 (example 6-18), 166

Ambari, 126

AMP (Advanced Malware Protection), 3

AMP for Endpoints, 175-176

AMP for Networks, 176

AMP ThreatGRID, 176-177

amplification attacks, 249-250

anomaly detection, 8-9

antivirus software, 174-175

Apache Flume, 119-120

Apache Hadoop, 116-118

Apache HBase, 124-125

Apache Hive, 122-123

Apache Kafka, 120-121

Apache Storm, 121-122

appliances

- FlowCollector, 145
- SMC (StealthWatch Management Console), 147

Application Centric Infrastructure (ACI) in data center, 30

application control, 23-24

application recognition, 22

Application Visibility and Control (AVC). *See* Cisco AVC (Application Visibility and Control)

applications, Flexible NetFlow key fields, 63

applying flow monitor to interface

- in Cisco Nexus 1000V, 164
- Flexible NetFlow, 73

applying NetFlow monitor and sampler (example 6-20), 166

apt package database update (example 4-7), 95

ASA 5500-X series, 3

ASA 5585-X Adaptive Security Appliances, 3

ASDM (Adaptive Security Device Manager), 153-155

attack continuum, 2-3, 130-131. *See also* denial-of-service (DoS) attacks; distributed denial-of-service (DDoS) attacks

AVC (Application Visibility and Control). *See* Cisco AVC (Application Visibility and Control)

Avro, 126

B

back doors, 174

bag manipulation tools in SiLK, 88-89

BDAS (Berkeley Data Analytics Stack), 126

best practices, 35-36

big data, 111-112

- unstructured versus structured data, 112-113

big data analytics, 111

- Hadoop-related projects, 126
- IoE (Internet of Everything), 127
- OpenSOC, 115
  - *benefits of, 115-116*
  - *components, 116*
  - *Elasticsearch, 123-124*
  - *Flume, 119-120*
  - *Hadoop, 116-118*
  - *HBase, 124-125*
  - *Hive, 122-123*
  - *Kafka, 120-121*
  - *Storm, 121-122*
  - *third-party tools, 125-126*
- telemetry sources, 114-115
- types of, 113-114

botnets, 8, 172

BYOD (bring your own device), 187

C

cache (NetFlow), 4

- types of, 6

Caligare, 75

capacity planning, 14-15, 267-269

capture command (example 7-45), 230

CAPWAP (Control and Provisioning of Wireless Access Points), 26

case studies

- capacity planning, 267-269
- credit card theft, 254-259
- DDos attack identification, 250-254
- intellectual property theft, 259-262
- monitoring cloud usage, 269-271
- monitoring guest users and contractors, 262-267

Cassandra, 126

cflowd, 80

Chukwa, 126

Cisco AMP for Endpoints, 175-176

Cisco AMP for Networks, 176

Cisco AMP ThreatGRID, 176-177

Cisco ASA

- clear logging command options, 193
- logging buffer-size command, 193
- logging buffered command, 191
- logging timestamp command, 194
- models, list of, 148
- NetFlow support, 140
- NSEL
  - *configuration, 153-160*
  - *deploying in cluster configuration, 151-153*
  - *flow events, 149-151*
- show logging command, 191
- troubleshooting, 228-234

Cisco ASA 5500-X Series Next-Generation Firewalls, 171-172

Cisco ASA with FirePOWER Services, 171-172

Cisco AVC (Application Visibility and Control), 22

application control, 23-24

application recognition, 22

management and reporting systems, 23

metrics collection and exporting, 23

wireless LAN deployment scenario, 25-26

Cisco Cloud Email Security, 179

Cisco CSR (Cloud Services Router) 1000V deployment scenario, 32-33

Cisco CTD (Cyber Threat Defense) Solution, 21-22, 77, 129

AMP for Endpoints, 175-176

AMP for Networks, 176

AMP ThreatGRID, 176-177

Cisco ASA 5500-X Series Next-Generation Firewalls, 171-172

Cisco ASA with FirePOWER Services, 171-172

Cisco Cloud Email Security, 179

Cisco CWS, 185-186

Cisco ESA models, 177-179

Cisco Hybrid Email Security, 179-180

Cisco ISE, 186-187

Cisco SMA, 184-185

Cisco WSA, 180-183

components, 131-133

FireSIGHT Management Center, 173

Lancope StealthWatch System. *See* Lancope StealthWatch System

NetFlow configuration

in Cisco Nexus 1000V, 160-164

in Cisco Nexus 7000 series, 164-166

in Cisco NGA, 166-171

NGIPS, 172-173

NSEL. *See* NSEL (NetFlow Secure Event Logging)

Cisco CWS (Cloud Web Security), 185-186

Cisco ESA (email security appliances) models, 177-179

Cisco Feature Navigator, 21

Cisco FirePOWER 7000 series appliances, 172

Cisco FirePOWER 8000 series appliances, 172

Cisco FirePOWER 9300 series appliances, 172

Cisco FireSIGHT Management Center, 173

Cisco Flexible NetFlow. *See* Flexible NetFlow

Cisco Hybrid Email Security, 179-180

Cisco IOS devices

clear log command, 193

logging buffered command in, 190

service timestamps command, 193

show logging command, 192

troubleshooting

communication problems with NetFlow collector, 201-204

debugging flow records, 212-213

displaying flow exporter templates and export IDs, 207-212

preventing export storms, 213-214

sample configuration, 194-201

verifying flow monitor configuration, 204-206

Cisco IOS software

Flexible NetFlow support, 134

NetFlow support, 133

Cisco IOS-XE software, Flexible NetFlow support, 136

Cisco IOS-XR software

NetFlow support, 134

troubleshooting

architecture configuration, 217-219

flow exporter statistics and diagnostics, 219-222

flow monitor statistics and diagnostics, 222-226

flow producer statistics and diagnostics, 226-228

show commands, 228

Cisco ISE (Identity Services Engine), 77, 186-187

Cisco Nexus 1000V NetFlow configuration, 160-164

flow exporter definition, 162-163

flow monitor application to interface, 164

flow monitor definition, 163-164

flow record definition, 161-162

Cisco Nexus 7000 series NetFlow configuration, 164-166

flow exporter definition, 165

flow monitor application to interface, 164

flow monitor definition, 165

flow record definition, 165

timer adjustments, 166

Cisco NGA (NetFlow Generation Appliance)

configuration

initialization, 167-168

via CLI, 169-171

via GUI, 168-169

in data center, 30-31, 166-167

troubleshooting

flow collector information, 236-237

flow exporter information, 237

flow monitor information, 238-239

flow record information, 237-238

managed devices, 235

show commands, 245

show tech-support command, 239-245

Cisco NX-OS software

Flexible NetFlow support, 138

troubleshooting, 214-217

Cisco Platform Exchange Grid (pxGrid), 187

Cisco SenderBase, 178

Cisco SMA (Security Management Appliance), 184-185

Cisco VNI (Visual Networking Index), 112

Cisco WSA (Web Security Appliance), 180-183

ClamAV, 175

clear log command in Cisco IOS devices, 193

clear logging command options in Cisco ASA, 193

CLI (command-line interface)

Cisco NGA configuration, 169-171

NSEL configuration, 155-156

Cloud Email Security, 179

cloud environment deployment scenario, 32-33

cloud usage, monitoring, 269-271

Cloud Web Security (CWS), 185-186

clustering, NSEL deployment in, 151-153

Cognitive Security, 113

collecting process (CP), 16

commercial monitoring and analysis software packages

- Lancope StealthWatch System, 76-79
- list of, 75
- Plixer International Scrutinizer, 79-80

communication problems with NetFlow collector, troubleshooting, 201-204

configuration

- Cisco IOS-XR software, 217-219
- Cisco NGA (NetFlow Generation Appliance)
  - *initialization, 167-168*
  - *via CLI, 169-171*
  - *via GUI, 168-169*
- Flexible NetFlow, 66-67
  - *distribution switches, 268*
  - *flow exporter configuration, 71-73*
  - *flow monitor application to interface, 73-74*
  - *flow monitor configuration for IPv4 or IPv6, 69-70*
  - *flow record configuration, 67-69*
  - *Internet-edge router, 251*
- flow monitors, verifying, 204-206
- NetFlow
  - *in Cisco Nexus 1000V, 160-164*
  - *in Cisco Nexus 7000 series, 164-166*
- NSEL, 153-160
  - *with ASDM, 153-155*
  - *with CLI, 155-156*
  - *defining export policy, 157-159*
  - *disabling redundant syslog messages, 155-156*
  - *monitoring NSEL, 159-160*

configuration files, SiLK, 87

contractors, monitoring, 262-267

Control and Provisioning of Wireless Access Points (CAPWAP), 26

counters, Flexible NetFlow non-key fields, 63

counting flow records with SiLK, 88

CP (collecting process), 16

CPU utilization, 190

credit card theft case study, 254-259

D

daemons, SiLK, 87

data center deployment scenario, 28-32

data FlowSets

- definitions, 54
- format, 54

data leak detection, 9

DDoS (distributed denial-of-service) attacks, 247

- amplification attacks, 249-250
- anomaly detection, 8-9
- direct attacks, 248
- identifying
  - *in enterprise networks, 250-253*
  - *in service provider networks, 253-254*
- reflected attacks, 248-249

debug commands, 189-192
clear log command in Cisco IOS devices, 193
clear logging command options in Cisco ASA, 193
CPU utilization, 190
logging buffered command
in Cisco ASA, 191
in Cisco IOS devices, 190
logging buffer-size command in Cisco ASA, 193
logging timestamp command in Cisco ASA, 194
service timestamps command in Cisco IOS devices, 193
show logging command
in Cisco ASA, 191
in Cisco IOS devices, 192
debug flow exporter command, 202
options, 202
output, 209
debug flow monitor command output (example 7-28), 209
debug flow record command output (example 7-30), 212
debugging flow records, 212-213
defining flow collector (example 6-22), 170
defining flow exporter
in Cisco Nexus 1000V, 162
in Cisco Nexus 7000 series, 165
in Cisco NGA, 170
defining flow monitor
in Cisco Nexus 1000V, 163
in Cisco Nexus 7000 series
custom records, 165
original records, 165
in Cisco NGA, 170
defining flow record
in Cisco Nexus 1000V, 161
in Cisco Nexus 7000 series, 165
defining NSEL export policy (example 6-3), 159
denial-of-service (DoS) attacks, 247
deploying
FlowCollectors, 142-146
FlowReplicators, 146-147
NSEL in cluster configuration, 151-153
deployment scenarios, 24
cloud environment, 32-33
data center, 28-32
Internet edge, 26-28
user access layer, 24-25
VPNs, 33-35
wireless LAN, 25-26
direct DDoS attacks, 248
disabling redundant syslog messages (example 6-2), 157
displaying
export IDs, 207-212
flow exporter templates, 207-212
flow records
predefined Cisco Nexus 1000V records, 160
with SiLK, 87
distributed denial-of-service (DDoS) attacks. *See* DDoS (distributed denial-of-service) attacks
distribution switch Flexible NetFlow configuration (example 8-2), 268
DoS (denial-of-service) attacks, 247
downloaders, 174

E

east-to-west communication, 28

Elasticsearch, 92

- installing, 96-105
- in OpenSOC, 123-124

elasticsearch.yml configuration file (example 4-8), 96-105

ELK (Elasticsearch, Logstash and Kibana), 80, 92-109

- deployment topology, 94
- Elasticsearch, 92
  - *installing, 96-105*
- installing, 95-96
- Kibana, 93
  - *installing, 105-106*
- Logstash, 92-93
  - *installing, 107-109*
- Marvel and Shield, 94
- Nginx, installing, 106-107

email security appliances (ESA) models, 177-179

email-based threats

- Cisco Cloud Email Security, 179
- Cisco ESA models, 177-179
- Cisco Hybrid Email Security, 179-180
- list of, 177

enforcer, network as, 4

enterprise networks, identifying DDoS attacks, 250-253

EP (exporting process), 16

ESA (email security appliances) models, 177-179

Evident Software Evident Analyze, 75

exabytes, 112

examples

- adjusting NetFlow timers in Cisco Nexus 7000, 166
- applying flow monitor to interface, 73, 164
- applying NetFlow monitor and sampler, 166
- apt package database update, 95
- capture command, 230
- clear logging command options in Cisco ASA, 193
- configuring NSEL using the CLI, 155
- configuring sampled NetFlow in Cisco Nexus 7000, 166
- creating IPv4 flow record with key and non-key fields, 169
- debug flow exporter and debug flow monitor command output, 209
- debug flow exporter command, 202
- debug flow exporter command options, 202
- debug flow record command output, 212
- debugging specific flow exporter, 203
- defining flow collector, 170
- defining flow exporter
  - *in Cisco Nexus 1000V, 162*
  - *in Cisco Nexus 7000 series, 165*
  - *in Cisco NGA, 170*
- defining flow monitor
  - *in Cisco Nexus 1000V, 163*
  - *in Cisco NGA, 170*
  - *with custom record in Cisco Nexus 7000, 165*
  - *with original record in Cisco Nexus 7000, 165*
- defining flow record
  - *in Cisco Nexus 1000V, 161*
  - *in Cisco Nexus 7000 series, 165*

defining NSEL export policy, 159

disabling redundant syslog messages, 157

displaying predefined flow records, 160

distribution switch Flexible NetFlow configuration, 268

elasticsearch.yml configuration file, 96-105

Flexible NetFlow configuration, 73

incorrectly configured logstash-netflow.conf file, 234

installing NFdump in Ubuntu, 81-82

Internet-edge router Flexible NetFlow configuration, 251

IPFIX export format enabled, 74

logging buffer-size command in Cisco ASA, 193

logging buffered command

- *in Cisco ASA, 191*
- *in Cisco IOS devices, 190*

nfcapd command usage, 83

nfcapd daemon command options, 84

nfdump man pages excerpt, 86

Oracle Java PPA installation, 95

ping command output, 203

preventing export storms, 214

processing and displaying nfcapd files with nfdump, 84

RTP-R1 Flexible NetFlow configuration, 195

service timestamps command, 193

show capture command output, 230

show capture netflow-cap detail command output, 231

show capture netflow-cap dump command output, 232

show flow collector command output, 236

show flow command options, 236

show flow exporter command output

- *in Cisco IOS and IOS XE devices, 201*
- *in Cisco IOS-XR software, 220*
- *in Cisco Nexus 1000V, 163*
- *in Cisco NGA, 237*
- *Flexible NetFlow, 72*

show flow exporter export-ids netflow-v9 command output, 208

show flow exporter NX-OS command output, 215

show flow exporter option application table command output, 209

show flow exporter statistics command output, 202

show flow exporter templates command options, 207

show flow exporter templates command output, 207

show flow exporter-map command output in Cisco IOS-XR, 221

show flow interface command output

- *in Cisco Nexus 1000V, 164*
- *in Cisco NX-OS software, 216*

show flow interface GigabitEthernet 0/0 command output, 204

show flow monitor command options, 205

show flow monitor command output

- *in Cisco IOS and IOS XE devices, 204*
- *in Cisco IOS-XR software, 222*
- *in Cisco Nexus 1000V, 164*
- *in Cisco NGA, 239*
- *Flexible NetFlow, 70*

show flow monitor monitor-name cache summary command options in Cisco IOS-XR, 225

show flow monitor name NY-ASR-FLOW-MON-1 cache format record command output, 72

show flow monitor RTP-DC-MONITOR-1 cache command output in Cisco NX-OS, 216

show flow monitor RTP-FLOW-MONITOR-1 cache command output, 205

show flow monitor RTP-FLOW-MONITOR-1 statistics command output, 206

show flow monitor type performance-monitor command output, 214

show flow monitor-map command output, 226

show flow platform producer statistics command output, 227

show flow record command output

in Cisco IOS and IOS XE devices, 198

in Cisco Nexus 1000V, 162

in Cisco NGA, 238

Flexible NetFlow, 69

show flow record RTP-FLOW-RECORD-1 command output, 197

show flow sw-monitor RTP-DC-MONITOR-1 statistics command output in Cisco NX-OS, 216

show flow trace command options, 228

show flow-export counters command output

in Cisco ASA, 229

NSEL monitoring, 159

show ip router 172.18.104.179 command output, 203

show logging command

in Cisco ASA, 191

in Cisco IOS devices, 192

show managed-device command output, 235

show running-config flow exporter command output

in Cisco IOS and IOS XE devices, 196

Flexible NetFlow, 72

show running-config flow monitor command output, 70

show running-config flow record command output

in Cisco IOS and IOS XE devices, 196

Flexible NetFlow, 69

show tech command output, 239-244

exploits, 174

export IDs, displaying, 207-212

export packets (NetFlow v9), 44

field descriptions, 45

header format, 44

export policies (NSEL), defining, 157-159

export storms, preventing, 213-214

exporting metrics, 23

exporting process (EP), 16

F

filtering flow records with SiLK, 87

FireSIGHT Management Center, 173

firewalls

Cisco ASA 5500-X Series Next-Generation Firewalls, 171-172

personal firewalls, 175

five-tuple, 4-5

Flexible NetFlow

with Cisco CTD, 132

configuration, 66-67

distribution switches, 268

flow exporter configuration, 71-73

flow monitor application to interface, 73-74

flow monitor configuration for IPv4 or IPv6, 69-70

flow record configuration, 67-69

Internet-edge router, 251

flow exporters, 65-66

flow information gathered, 5

flow monitors, 65

flow samplers, 66

IPFIX export format, 74

records, 61-65

key fields, 61-63

non-key fields, 63-64

predefined records, 65

user-defined records, 65

simultaneous application tracking, 60

supported platforms

Cisco IOS software, 134

Cisco IOS-XE software, 136

Cisco NX-OS software, 138

supported protocols, 59

troubleshooting

communication problems with NetFlow collector, 201-204

debugging flow records, 212-213

displaying flow exporter templates and export IDs, 207-212

preventing export storms, 213-214

sample configuration, 194-201

verifying flow monitor configuration, 204-206

Flexible NetFlow configuration (example 3-9), 73

flow collectors

defining, 170

gathering information about, 236-237

troubleshooting communication problems, 201-204

flow directors in clustering, 152

flow events, NSEL, 149-151

flow exporters

defining

in Cisco Nexus 1000V, 162-163

in Cisco Nexus 7000 series, 165

in Cisco NGA, 170

displaying templates and export IDs, 207-212

Flexible NetFlow, 65-66

configuration, 71-73

IPFIX export format, 74

statistics and diagnostics

in Cisco IOS-XR software, 219-222

in Cisco NGA, 237

troubleshooting communication problems, 201-204

flow file utilities, SiLK, 90-91

flow forwarders in clustering, 152

flow header format

NetFlow v1, 40

NetFlow v5, 41

NetFlow v7, 42

NetFlow v9, 44-45

flow licenses, 22, 142

flow monitors

application to interface

in Cisco Nexus 1000V, 164

in Cisco Nexus 7000 series, 164

defining

in Cisco Nexus 1000V, 163-164

in Cisco Nexus 7000 series, 165

in Cisco NGA, 170

Flexible NetFlow, 65

application to interface, 73-74

configuration, 69-70

statistics and diagnostics

in Cisco IOS-XR software, 222-226

in Cisco NGA, 238-239

verifying configuration, 204-206

flow owners in clustering, 152

flow producers in Cisco IOS-XR software, 226-228

flow records, 6

counting with SiLK, 88

creating with key and non-key fields, 169

debugging, 212-213

defining

in Cisco Nexus 1000V, 161-162

in Cisco Nexus 7000 series, 165

displaying

predefined Cisco Nexus 1000V records, 160

with SiLK, 87

filtering with SiLK, 87

Flexible NetFlow, 61-65

configuration, 67-69

key fields, 61-63

non-key fields, 63-64

predefined records, 65

user-defined records, 65

format

NetFlow v1, 40

NetFlow v5, 41

NetFlow v7, 42

gathering information about, 237-238

grouping with SiLK, 88

mating with SiLK, 88

sorting with SiLK, 87

Flow Replicator (Plixer), 79-80

flow samplers, Flexible NetFlow, 66

FlowCollector, 22, 79, 142

appliances, 145

deployment topology, 142-146

FlowCollector VE (virtual edition), 146

flowd, 80

FlowPro, 79-80

FlowReplicator, 22, 79, 142

deployment topology, 146-147

flows

explained, 4-6

Flexible NetFlow key fields, 61

IPFIX. *See* IPFIX

sessions versus, 6

flows per second (fps), 36-37

FlowSensor, 22, 79, 142

FlowSets

template FlowSets

field descriptions, 46

field type definitions, 47

format, 45-46

flowtools, 80

flowviewer, 80

Fluke Networks, 75

Flume, 119-120

forensics, 9-14

credit card theft case study, 254-259

intellectual property theft case study, 259-262

fps (flows per second), 36-37

G

grouping flow records with SiLK, 88

guest users, monitoring, 262-267

GUI (graphical user interface), Cisco NGA configuration, 168-169

H

hackers, 2-3, 130-131

Hadoop, 116-118

HBase, 124-125

HDFS, 117-118

Hewlett Packard NetFlow Insight, 75

HIPS (host intrusion prevention systems), 175

Hive, 122-123

hybrid cloud environments, 32-33

Hybrid Email Security, 179-180

I - J

IBM NetFlow Aurora, 75

IdeaData NetFlow Auditor, 75

immediate cache, 6

Immunet, 175

incident response, 9-14

credit card theft case study, 254-259

intellectual property theft case study, 259-262

indicators of compromise (IOCs)

big data analytics, 111

discovering, 9-14

InfoVista 5View NetFlow, 75

initialization, Cisco NGA, 167-168

installing

Elasticsearch, 96-105

ELK, 95-96

Kibana, 105-106

Logstash, 107-109

NFdump in Ubuntu, 81-82

Nginx, 106-107

intellectual property theft case study, 259-262

interface

Flexible NetFlow key fields, 61

flow monitor application to, 73-74

in Cisco Nexus 1000V, 164

in Cisco Nexus 7000 series, 164

internal buffer, logging messages to, 190-194

Internet edge

deployment scenario, 26-28

Flexible NetFlow configuration, 251

Internet Protocol Flow Information Export. ***See*** **IPFIX**

IOCs (indicators of compromise)

big data analytics, 111

discovering, 9-14

IoE (Internet of Everything), 127

IoT (Internet of Things), 127

IP Accounting, NetFlow versus, 6-7

IP labeling files in SiLK, 89

IPFIX (Internet Protocol Flow Information Export)

architecture, 16

explained, 15-16

Flexible NetFlow IPFIX export format, 74

mediators, 17

NetFlow comparison, 57

SCTP, 20

SiLK utilities, 90

templates, 17-20

IPFIX export format enabled (example 3-10), 74

IPFlow, 80

IPset manipulation tools in SiLK, 88-89

IPv4

Flexible NetFlow key fields, 61

Flexible NetFlow non-key fields, 64

flow monitor configuration, 69-70

flow record creation, 169

IPv6

Flexible NetFlow key fields, 61

Flexible NetFlow non-key fields, 64

flow monitor configuration, 69-70

iSiLK, 80

K

Kafka, 120-121

key fields in Flexible NetFlow records, 61-63

key loggers, 174

Kibana, 93

installing, 105-106

L

Lancope NetFlow Bandwidth Calculator, 37

Lancope StealthWatch System, 75-79

components, 21-22, 79, 142

FlowCollector, deployment topology, 142-146

FlowReplicator, deployment topology, 146-147

SMC. *See* SMC (StealthWatch Management Console)

LAN-to-LAN VPN (virtual private network) deployment scenario, 34-35

Layer 2 services, Flexible NetFlow key fields, 61

Layer 3 routing protocols, Flexible NetFlow key fields, 62

listeners, 179

logging buffered command

in Cisco ASA, 191

in Cisco IOS devices, 190

logging buffer-size command in Cisco ASA, 193

logging messages

to internal buffer, 190-194

network forensics, 12-14

logging timestamp command in Cisco ASA, 194

logic bombs, 174

Logstash, 92-93

installing, 107-109

logstash-netflow.conf file (example 7-49), 234

M

Mahout, 126

mailers, 173

malware

AMP for Endpoints, 175-176

AMP for Networks, 176

AMP ThreatGRID, 176-177

antivirus software, 174-175

email attachments, 177
HIPS, 175
personal firewalls, 175
types of, 173-174

managed devices, troubleshooting, 235

ManageEngine NetFlow Analyzer, 75

management and reporting systems, 23

Marvel, 94

master units in clustering, 152

mating flow records with SiLK, 88

mediators, IPFIX, 17

metering process (MP), 16

metrics, collection and exporting, 23

mitigation accelerator, network as, 4

monitoring
cloud usage, 269-271
guest users and contractors, 262-267
NSEL, 159-160

monitoring and analysis software packages
commercial packages
Lancope StealthWatch System, 76-79
list of, 75
Plixer International Scrutinizer, 79-80
open source packages
ELK (Elasticsearch, Logstash and Kibana), 92-109
list of, 80
NFdump, 81-86
NfSen, 86
SiLK, 86-91

MP (metering process), 16

multicasts
Flexible NetFlow key fields, 63
Flexible NetFlow non-key fields, 64

N

NAT stitching, 79

NBAR2 (Network Based Application Recognition Version 2), 22

NetFlow
best practices, 35-36
cache, 4-6
commercial monitoring and analysis software packages
Lancope StealthWatch System, 76-79
list of, 75
Plixer International Scrutinizer, 79-80
configuration
in Cisco Nexus 1000V, 160-164
in Cisco Nexus 7000 series, 164-166
deployment scenarios, 24
cloud environment, 32-33
data center, 28-32
Internet edge, 26-28
user access layer, 24-25
VPNs, 33-35
wireless LAN, 25-26
Flexible NetFlow. *See* Flexible NetFlow
flows per second (fps), 36-37
IP Accounting versus, 6-7
IPFIX comparison, 57
open source monitoring and analysis software packages
ELK (Elasticsearch, Logstash and Kibana), 92-109

list of, 80

NFdump, 81-86

NfSen, 86

SiLK, 86-91

security usage

anomaly detection, 8-9

data leak detection, 9

incident response and forensics, 9-14, 254-262

network visibility, 7-8

supported platforms, 20-21

Cisco ASA, 140

Cisco IOS software, 133

Cisco IOS-XR software, 134

traffic engineering and capacity planning, 14-15

troubleshooting. *See* troubleshooting

UDP ports, 16

usage, 1-2

versions

list of, 39

NetFlow v1, 40

NetFlow v5, 41

NetFlow v7, 42

NetFlow v9, 43-55

NetFlow v1

flow header format, 40

flow record format, 40

NetFlow v5

flow header format, 41

flow record format, 41

NetFlow v7

flow header format, 42

flow record format, 42

NetFlow v9, 43-55

export packets, 44

flow header format, 44-45

templates

benefits of, 44

data FlowSet definitions, 54

data FlowSet format, 54

field type definitions, 47

FlowSet field descriptions, 46

FlowSet format, 45-46

options template definitions, 55

options template format, 55

NetUsage, 75

network, security role of, 3-4

Network Based Application Recognition Version 2 (NBAR2), 22

network forensics, 9-14

network scan detection utilities, SiLK, 90

Network Time Protocol (NTP), 14

network traffic. *See* traffic

network visibility, 7-8

Next-Generation Intrusion Prevention Systems (NGIPS), 172-173

nfcapd command usage (example 4-2), 83

nfcapd daemon command options (example 4-3), 84

nfcapd files processing and displaying with nfdump (example 4-4), 84

NFdump, 80, 81-86

components, 82

installing in Ubuntu, 81-82

nfdump man pages excerpt (example 4-5), 86

NfSen, 80, 86

Nginx, installing, 106-107

NGIPS (Next-Generation Intrusion Prevention Systems), 172-173

non-key fields in Flexible NetFlow records, 63-64

normal cache, 6

north-to-south communication, 28

NoSQL, 113

NSEL (NetFlow Secure Event Logging)

configuration, 153-160

with ASDM, 153-155

with CLI, 155-156

defining export policy, 157-159

disabling redundant syslog messages, 156-157

monitoring NSEL, 159-160

deploying in cluster configuration, 151-153

flow events, 149-151

NTP (Network Time Protocol), 14

NX-OS. *See* Cisco NX-OS software

O

Open Resolver Project, 249

open source monitoring and analysis software packages

ELK (Elasticsearch, Logstash and Kibana), 92-109

list of, 80

NFdump, 81-86

NfSen, 86

SiLK, 86-91

OpenSOC, 115

benefits of, 115-116

components, 116

Elasticsearch, 123-124

Flume, 119-120

Hadoop, 116-118

HBase, 124-125

Hive, 122-123

Kafka, 120-121

Storm, 121-122

third-party tools, 125-126

options templates

definitions, 55

format, 55

IPFIX, 19-20

Oracle Java PPA installation (example 4-6), 95

P

packet captures

network forensics, 12

SiLK utilities, 90

packet header format. *See* flow header format

packets. *See* export packets

Paessler PRTG, 75

Panoptis, 80

PDUs (protocol data units), 6

permanent cache, 6

personal firewalls, 175

petabytes, 112

phishing, 177

Pig, 126

ping command output (example 7-18), 203

Platform Exchange Grid (pxGrid), 187

Plixer International Scrutinizer, 75, 79-80

Plixer Scrutinizer NetFlow Analyzer, 80

port labeling files in SiLK, 89

ports, UDP ports for NetFlow, 16

predefined records in Flexible NetFlow records, 65

prefix map manipulation tools in SiLK, 88-89

preventing export storms, 213-214

private cloud environments, 32-33

protocol data units (PDUs), 6

public cloud environments, 32-33

pxGrid (Platform Exchange Grid), 187

PySiLK (Python Extension), 88

Q

QoS (quality of service)

- application control, 23-24
- NBAR2 and, 22

R

ransomware, 174

records. ***See*** **flow records**

reflected DDoS attacks, 248-249

remote-access VPN (virtual private network) deployment scenario, 33-34

rootkits, 174

routing protocols, Flexible NetFlow key fields, 62

RTP-R1 Flexible NetFlow configuration (example 7-8), 195

runtime plug-ins, SiLK, 89-90

S

scalability, NetFlow, 36-37

Scrutinizer, 75, 79-80

- free version, 80

SCTP (Stream Control Transmission Protocol), 20

security

- anomaly detection, 8-9
- attack continuum, 2-3, 130-131
- Cisco CTD Solution. *See* Cisco CTD (Cyber Threat Defense) Solution
- data leak detection, 9
- DDos attacks, 247
  - *amplification attacks, 249-250*
  - *direct attacks, 248*
  - *in enterprise networks, 250-253*
  - *reflected attacks, 248-249*
  - *in service provider networks, 253-254*
- DoS attacks, 247
- email-based threats
  - *Cisco Cloud Email Security, 179*
  - *Cisco ESA models, 177-179*
  - *Cisco Hybrid Email Security, 179-180*
  - *list of, 177*
- incident response and forensics, 9-14
  - *credit card theft case study, 254-259*
  - *intellectual property theft case study, 259-262*
- IoE (Internet of Everything), 127
- malware
  - *AMP for Endpoints, 175-176*
  - *AMP for Networks, 176*
  - *AMP ThreatGRID, 176-177*
  - *antivirus software, 174-175*
  - *HIPS, 175*
  - *personal firewalls, 175*
  - *types of, 173-174*
- network visibility, 7-8
- OpenSOC. *See* OpenSOC
- role of network in, 3-4

web security, 180

Cisco CWS, 185-186

Cisco SMA, 184-185

Cisco WSA, 180-183

security operations centers (SOCs), 115

sensor, network as, 4

service provider networks, identifying DDoS attacks, 253-254

service timestamps command in Cisco IOS devices, 193

sessions, flows versus, 6

Shield, 94

show audit-trail command, 245

show cache statistics cumulative monitor_name command, 245

show cache statistics rates monitor_name command, 245

show capture command output (example 7-46), 230

show capture netflow-cap detail command output (example 7-47), 231

show capture netflow-cap dump command output (example 7-48), 232

show cdp settings command, 245

show collector statistics collector_name command, 245

show cpu command, 190

show dataport statistics cumulative command, 245

show dataport statistics rates command, 245

show dataport statistics rates queues command, 245

show exporter statistics exporter_name command, 245

show flow collector command output (example 7-52), 236

show flow command options (example 7-51), 236

show flow exporter command output

in Cisco IOS and IOS XE devices, 201

in Cisco IOS-XR software, 220

in Cisco Nexus 1000V, 163

in Cisco NGA, 237

Flexible NetFlow, 72

show flow exporter export-ids netflow-v9 command output (example 7-27), 208

show flow exporter NX-OS command output (example 7-33), 215

show flow exporter option application table command output (example 7-29), 209

show flow exporter statistics command output (example 7-14), 202

show flow exporter templates command options (example 7-26), 207

show flow exporter templates command output (example 7-25), 207

show flow exporter-map command output in Cisco IOS-XR (example 7-38), 221

show flow filter filter_name command, 245

show flow interface command output

in Cisco Nexus 1000V, 164

in Cisco NX-OS software, 216

show flow interface GigabitEthernet 0/0 command output (example 7-20), 204

show flow monitor command options (example 7-22), 205

show flow monitor command output

in Cisco IOS and IOS XE devices, 204

in Cisco IOS-XR software, 222

in Cisco Nexus 1000V, 164

in Cisco NGA, 239

Flexible NetFlow, 70

show flow monitor monitor-name cache summary command options in Cisco IOS-XR (example 7-40), 225

show flow monitor name NY-ASR-FLOW-MON-1 cache format record command output (example 3-7), 72

show flow monitor RTP-DC-MONITOR-1 cache command output in Cisco NX-OS (example 7-35), 216

show flow monitor RTP-FLOW-MONITOR-1 cache command output (example 7-23), 205

show flow monitor RTP-FLOW-MONITOR-1 statistics command output (example 7-24), 206

show flow monitor type performance-monitor command output (example 7-32), 214

show flow monitor-map command output (example 7-41), 226

show flow platform nfea interface command, 228

show flow platform nfea policer np command, 228

show flow platform nfea sample command, 228

show flow platform nfea sp location command, 228

show flow platform producer statistics command output (example 7-42), 227

show flow record command output

in Cisco IOS and IOS XE devices, 198

in Cisco Nexus 1000V, 162

in Cisco NGA, 238

Flexible NetFlow, 69

show flow record netflow layer2-switched input command, 217

show flow record RTP-FLOW-RECORD-1 command output (example 7-11), 197

show flow sw-monitor RTP-DC-MONITOR-1 statistics command output in Cisco NX-OS (example 7-36), 216

show flow timeout command, 217

show flow trace command, 228

show flow trace command options (example 7-43), 228

show flow-export counters command output

in Cisco ASA, 229

NSEL monitoring, 159

show hardware flow aging command, 217

show hardware flow entry address table-address type command, 217

show hardware flow ip command, 217

show hardware flow sampler command, 217

show hardware flow utilization command, 217

show inventory command, 245

show ip command, 245

show ip router 172.18.104.179 command output (example 7-19), 203

show log config command, 245

show log patch command, 245

show log upgrade command, 245

show logging command

in Cisco ASA, 191

in Cisco IOS devices, 192

show managed-device command output (example 7-50), 235

show patches command, 245

show processes cpu command, 190

show running-config flow exporter command output

in Cisco IOS and IOS XE devices, 196

Flexible NetFlow, 72

show running-config flow monitor command output (example 3-4), 70

show running-config flow record command output

in Cisco IOS and IOS XE devices, 196

Flexible NetFlow, 69

show sampler name command, 217

show snmp command, 245

show tech-support command, 239-245

SiLK, 80, 86-91

additional utilities, 91

configuration files, 87

counting, grouping, mating NetFlow records, 88

daemons, 87

filtering, displaying, sorting NetFlow records, 87

flow file utilities, 90-91

IP and port labeling files, 89

IPset, bag, prefix map manipulation, 88-89

network scan detection utilities, 90

packet capture and IPFIX processing utilities, 90

Python Extension (PySiLK), 88

runtime plug-ins, 89-90

simultaneous application tracking, Flexible NetFlow, 60

site-to-site VPN (virtual private network) deployment scenario, 34-35

slave units in clustering, 152

SLIC (StealthWatch Labs Intelligence Center), 78

SMC (StealthWatch Management Console), 22, 77-79, 142

appliances, 147

form factors, 147-148

visualization examples, 140-142

SMC (StealthWatch Management Console) VE (virtual edition), 148

SMTP daemons, 179

sniffers, network forensics, 12

SOCs (security operations centers), 115

SolarWinds NetFlow Traffic Analyzer, 75

sorting flow records with SiLK, 87

SourceFire, 172

spam, 177

spammers, 174

Spark, 126

spear phishing, 177

Stager, 80

StealthWatch IDentity, 79

StealthWatch Labs Intelligence Center (SLIC), 78

StealthWatch Management Console (SMC) VE (virtual edition), 148

StealthWatch System. *See* Lancope StealthWatch System

Storm, 121-122

Stream Control Transmission Protocol (SCTP), 20

structured data, unstructured data versus, 112-113

syslog

disabling redundant messages, 155-156

network forensics, 12-14

T

telemetry sources, big data analytics, 114-115

templates

benefits of, 44

data FlowSet definitions, 54

data FlowSet format, 54

displaying, 207-212

field type definitions, 47

FlowSet field descriptions, 46

FlowSet format, 45-46

IPFIX, 17-20

options templates

definitions, 55

format, 55

Tez, 126

ThreatGRID, 176-177

time stamps, 14

Flexible NetFlow non-key fields, 64

logging timestamp command, 194

service timestamps command, 193

timer adjustments in Cisco Nexus 7000 series, 166

traffic

anomaly detection, 8-9

application recognition, 22

Cisco CTD Solution, 21-22

engineering and capacity planning, 14-15, 267-269

network forensics, 10-12

transports, Flexible NetFlow key fields, 62

trojan horses, 174

troubleshooting

in Cisco ASA, 228-234

in Cisco IOS devices

communication problems with NetFlow collector, 201-204

debugging flow records, 212-213

displaying flow exporter templates and export IDs, 207-212

preventing export storms, 213-214

sample configuration, 194-201

verifying flow monitor configuration, 204-206

Cisco IOS-XR software

architecture configuration, 217-219

flow exporter statistics and diagnostics, 219-222

flow monitor statistics and diagnostics, 222-226

flow producer statistics and diagnostics, 226-228

show commands, 228

Cisco NGA (NetFlow Generation Appliance)

flow collector information, 236-237

flow exporter information, 237

flow monitor information, 238-239

flow record information, 237-238

managed devices, 235

show commands, 245

show tech-support command, 239-245

in Cisco NX-OS software, 214-217

debug commands, 189-192

clear log command, 193

clear logging command options, 193

CPU utilization, 190

logging buffered command in Cisco ASA, 191

logging buffered command in Cisco IOS devices, 190

logging buffer-size command in Cisco ASA, 193

logging timestamp command, 194

service timestamps command, 193

show logging command in Cisco ASA, 191

show logging command in Cisco IOS devices, 192

network traffic, 15

U

Ubuntu

Elasticsearch installation, 96-105

Kibana installation, 105-106

Logstash installation, 107-109

NFdump installation, 81-82

Nginx installation, 106-107

UDP ports for NetFlow, 16

unstructured data, structured data versus, 112-113

user access layer deployment scenario, 24-25

user-defined records in Flexible NetFlow records, 65

V

versions of NetFlow

list of, 39

NetFlow v1, 40

NetFlow v5, 41

NetFlow v7, 42

NetFlow v9, 43-55

Virtual NGIPSv for VMware, 173

virtual private network (VPN) deployment scenarios, 33-35

viruses, 173

visibility of network, 7-8

VPN (virtual private network) deployment scenarios, 33-35

W

WCCP (Web Cache Communication Protocol), 180

Web Cache Communication Protocol (WCCP), 180

web security, 180

Cisco CWS, 185-186

Cisco SMA, 184-185

Cisco WSA, 180-183

whaling, 177

WLAN (wireless LAN) deployment scenario, 25-26

worms, 173

X - Z

yottabytes, 112

zettabytes, 112

zombies, 8

ZooKeeper, 126