SECURITY

Network Security with NetFlow and IPFIX

Big Data Analytics for Information Security

ciscopress.com

Omar Santos

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: Big Data Analytics for Information Security

Table of Contents

Contents

Introduction

Chapter 1 Introduction to NetFlow and IPFIX

Introduction to NetFlow

The Attack Continuum

The Network as a Sensor and as an Enforcer

What Is a Flow?

NetFlow Versus IP Accounting and Billing

NetFlow for Network Security

Anomaly Detection and DDoS Attacks

Data Leak Detection and Prevention

Incident Response and Network Security Forensics

Traffic Engineering and Network Planning

IP Flow Information Export

IPFIX Architecture

IPFIX Mediators

IPFIX Templates

Option Templates

Introduction to the Stream Control Transmission Protocol (SCTP)

Supported Platforms

Introduction to Cisco Cyber Threat Defense

Pearson

Table of Contents

Cisco Application Visibility and Control and NetFlow

Application Recognition

Metrics Collection and Exporting

Management and Reporting Systems

Control

Deployment Scenarios

Deployment Scenario: User Access Layer

Deployment Scenario: Wireless LAN

Deployment Scenario: Internet Edge

Deployment Scenario: Data Center

Public, Private, and Hybrid Cloud Environments

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

NetFlow Remote-Access VPNs

NetFlow Site-to-Site VPNs

NetFlow Collection Considerations and Best Practices

Determining the Flows per Second and Scalability

Summary

Chapter 2 Cisco NetFlow Versions and Features

NetFlow Versions and Respective Features

NetFlow v1 Flow Header Format and Flow Record Format

NetFlow v5 Flow Header Format and Flow Record Format

NetFlow v7 Flow Header Format and Flow Record Format

NetFlow Version 9

NetFlow and IPFIX Comparison

Summary

Chapter 3 Cisco Flexible NetFlow

Introduction to Ciscos Flexible NetFlow

Simultaneous Application Tracking

Table of Contents

Flexible NetFlow Records

Flexible NetFlow Key Fields

Flexible NetFlow Non-Key Fields

NetFlow Predefined Records

User-Defined Records

Flow Monitors

Flow Exporters

Flow Samplers

Flexible NetFlow Configuration

Configure a Flow Record

Configuring a Flow Monitor for IPv4 or IPv6

Configuring a Flow Exporter for the Flow Monitor

Applying a Flow Monitor to an Interface

Flexible NetFlow IPFIX Export Format

Summary

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

Commercial NetFlow Monitoring and Analysis Software Packages

Lancopes StealthWatch Solution

Plixers Scrutinizer

Open Source NetFlow Monitoring and Analysis Software Packages

NFdump

NfSen

SiLK

SiLK Configuration Files

Filtering, Displaying, and Sorting NetFlow Records with SiLK

SiLKs Python Extension

Counting, Grouping, and Mating NetFlow Records with Silk

SiLK IPset, Bag, and Prefix Map Manipulation Tools

Table of Contents

IP and Port Labeling Files

SiLK Runtime Plug-Ins

SiLK Utilities for Packet Capture and IPFIX Processing

Utilities to Detect Network Scans

SiLK Flow File Utilities

Additional SiLK Utilities

Elasticsearch, Logstash, and Kibana Stack

Elasticsearch

Logstash

Kibana

Elasticsearch Marvel and Shield

ELK Deployment Topology

Installing ELK

Summary

Chapter 5 Big Data Analytics and NetFlow

Introduction to Big Data Analytics for Cyber Security

What Is Big Data?

Unstructured Versus Structured Data

Extracting Value from Big Data

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

OpenSOC

Hadoop

HDFS

Flume

Kafka

Storm

Hive

Elasticsearch

Table of Contents

HBase

Third-Party Analytic Tools

Other Big Data Projects in the Industry

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

Summary

Chapter 6 Cisco Cyber Threat Defense and NetFlow

Overview of the Cisco Cyber Threat Defense Solution

The Attack Continuum

Cisco CTD Solution Components

NetFlow Platform Support

Traditional NetFlow Support in Cisco IOS Software

NetFlow Support in Cisco IOS-XR Software

Flexible NetFlow Support

NetFlow Support in Cisco ASA

Deploying the Lancope StealthWatch System

Deploying StealthWatch FlowCollectors

StealthWatch FlowReplicators

StealthWatch Management Console

Deploying NetFlow Secure Event Logging in the Cisco ASA

Deploying NSEL in Cisco ASA Configured for Clustering

Unit Roles and Functions in Clustering

Clustering NSEL Operations

Configuring NSEL in the Cisco ASA

Configuring NSEL in the Cisco ASA Using ASDM

Configuring NSEL in the Cisco ASA Using the CLI

NSEL and Syslog

Defining the NSEL Export Policy

Monitoring NSEL

Table of Contents

Configuring NetFlow in the Cisco Nexus 1000V

Defining a Flow Record

Defining the Flow Exporter

Defining a Flow Monitor

Applying the Flow Monitor to an Interface

Configuring NetFlow in the Cisco Nexus 7000 Series

Configuring the Cisco NetFlow Generation Appliance

Initializing the Cisco NGA

Configuring NetFlow in the Cisco NGA via the GUI

Configuring NetFlow in the Cisco NGA via the CLI

Additional Cisco CTD Solution Components

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

Next-Generation Intrusion Prevention Systems

FireSIGHT Management Center

AMP for Endpoints

AMP for Networks

AMP Threat Grid

Email Security

Email Security Appliance

Cloud Email Security

Cisco Hybrid Email Security

Web Security

Web Security Appliance

Cisco Content Security Management Appliance

Cisco Cloud Web Security

Cisco Identity Services Engine

Summary

Chapter 7 Troubleshooting NetFlow

Table of Contents

Troubleshooting Utilities and Debug Commands

Troubleshooting NetFlow in Cisco IOS and Cisco IOS XE Devices

- Cisco IOS Router Flexible NetFlow Configuration
- Troubleshooting Communication Problems with the NetFlow Collector
- Additional Useful Troubleshooting Debug and Show Commands
- Verifying a Flow Monitor Configuration
- Displaying Flow Exporter Templates and Export IDs
- Debugging Flow Records
- Preventing Export Storms with Flexible NetFlow

Troubleshooting NetFlow in Cisco NX-OS Software

Troubleshooting NetFlow in Cisco IOS-XR Software

- Flow Exporter Statistics and Diagnostics
- Flow Monitor Statistics and Diagnostics
- Displaying NetFlow Producer Statistics in Cisco IOS-XR
- Additional Useful Cisco IOS-XR Show Commands

Troubleshooting NetFlow in the Cisco ASA

Troubleshooting NetFlow in the Cisco NetFlow Generation Appliance

- Gathering Information About Configured NGA Managed Devices
- Gathering Information About the Flow Collector
- Gathering Information About the Flow Exporter
- Gathering Information About Flow Records
- Gathering Information About the Flow Monitor
- Show Tech-Support
- Additional Useful NGA show Commands

Summary

Chapter 8 Case Studies

Using NetFlow for Anomaly Detection and Identifying DoS Attacks

- Direct DDoS Attacks
- Reflected DDoS Attacks

Table of Contents

Amplification Attacks

Identifying DDoS Attacks Using NetFlow

Using NetFlow in Enterprise Networks to Detect DDoS Attacks

Using NetFlow in Service Provider Networks to Detect DDoS Attacks

Using NetFlow for Incident Response and Forensics

Credit Card Theft

Theft of Intellectual Property

Using NetFlow for Monitoring Guest Users and Contractors

Using NetFlow for Capacity Planning

Using NetFlow to Monitor Cloud Usage

Summary

Index