Zero Trust Architecture

CINDY GREEN-ORTIZ · BRANDON FOWLER
DAVID HOUCK · HANK HENSEL
PATRICK LLOYD · ANDREW MCDONALD
JASON FRAZIER

ciscopress.com

Zero Trust Architecture

Cindy Green-Ortiz, CISSP, CISM, CRISC, CSSLP, PMP, CSM
Brandon Fowler, CCNP Security
David Houck
Hank Hensel, CCIE No. 3577, CISSP
Patrick Lloyd, CCIE Enterprise No. 39750, CISSP
Andrew McDonald
Jason Frazier, CCSI

Cisco Press

Zero Trust Architecture

Table of Contents

Cover
Title Page
Copyright Page
Contents at a Glance
Contents
Preface
Introduction
Chapter 1 Overview of Zero Trust (ZT)
- Chapter Key Points
- Zero Trust Origins
- Planning for Zero Trust
  - Discovery Zero Trust Segmentation Workshop
  - Defining the Zero Trust Discovery Workshop Purpose
  - Defining Participation in the Discovery Workshop
  - Goals and Risks of the Zero Trust Architecture
  - Results of Discovery Processes Already Executed Upon
  - The Definition of Success and Benefits
  - A Practical Approach to Success and Future Needs
  - Artifact Gathering for Successful Workshop Outcomes
  - Exploring the Business to Secure It
- Zero Trust Organizational Dynamics
  - We have a plan
  - Competing Teams

Table of Contents

Problem? What problem?

We are going to the cloud and the cloud is Zero Trust by default

Ciscos Zero Trust Capabilities

Policy & Governance

Identity

Vulnerability Management

Enforcement

Analytics

Summary

References in This Chapter

Chapter 2 Zero Trust Capabilities

Chapter Key Points

Cisco Zero Trust Capabilities

Policy & Governance Pillar

Change Control

Data Governance

Data Retention

Quality of Service (QoS)

Redundancy

Replication

Business Continuity

Disaster Recovery (DR)

Risk Classification

Identity Pillar

Authentication, Authorization, and Accounting (AAA)

AAA Special Conditions

Certificate Authority

Network Access Control (NAC)

Provisioning

Table of Contents

- Device
- User
- People
- Infrastructure
- Services
- Privileged Access
- Multifactor Authentication (MFA)
- Asset Identity
- Configuration Management Database (CMDB)
- Internet Protocol (IP) Schemas
- IPV4
- IPV6
- Dual Stack

Vulnerability Management Pillar

- Endpoint Protection
- Malware Prevention and Inspection
- Vulnerability Management
- Authenticated Vulnerability Scanning
- Database Change

Enforcement

- Cloud Access Security Broker (CASB)
- Distributed Denial of Service (DDOS)
- Data Loss Prevention (DLP)
- Domain Name System Security (DNSSEC)
- Email Security
- Firewall
- Intrusion Prevention System (IPS)
- Proxy
- Virtual Private Network (VPN)

Table of Contents

Security Orchestration, Automation, and Response (SOAR)
File Integrity Monitor (FIM)
Segmentation
Analytics Pillar
Application Performance Monitoring (APM)
Auditing, Logging, and Monitoring
Change Detection
Network Threat Behavior Analytics
Security Information and Event Management (SIEM)
Threat Intelligence
Traffic Visibility
Asset Monitoring & Discovery
Summary
References in This Chapter
Chapter 3 Zero Trust Reference Architecture
Chapter Key Points
Zero Trust Reference Architecture: Concepts Explored
Branch
Campus
Core Network
WAN
Data Center
Cloud
Summary
References in This Chapter
Chapter 4 Zero Trust Enclave Design
Chapter Key Points
User Layer

Table of Contents

Corporate Workstations

Guests

BYOD: Employee Personal Devices

IoT

Collaboration

Lab and Demo

Proximity Networks

Personal Area Network

Cloud

Public Cloud

Private Cloud

Hybrid Cloud

Securing the Cloud

Zero Trust in the Cloud

Enterprise

Business Services

DMZ

Common Services

Payment Card Industry Business Services

Facility Services

Mainframe Services

Legacy Systems and Infrastructure Services

Summary

Chapter 5 Enclave Exploration and Consideration

Chapter Key Points

Addressing the Business

Identifying the Crown Jewels

Identifying and Protecting Shared Enclaves

Table of Contents

- Segmentation Policy Development
- Modeling and Testing of Segmentation Policy

Bringing Blurred Borders Back into Focus

- Monitoring Segment Definitions
- Mitigating Security Holes to Overcome Operational Challenges

Incorporating New Services and Enclaves

- Onboarding: The Challenge of Merger Activity
- Onboarding: The Challenge of Independent Purchasing Decisions
- Planning for Onboarding New Devices

Using Automation in Enclaves

Considerations on the Physicality of an Enclave

Summary

References in This Chapter

Chapter 6 Segmentation

Chapter Key Points

A Brief Summary of the OSI Model

Upper Layer Segmentation Models

Common Network-Centric Segmentation Models

North-South Directional Segmentation

East-West Directional Segmentation

Determining the Best Model for Segmentation

- A Charter for Segmentation
- What is the impact of not segmenting the network?
- Is there a policy that allows us to enforce the need for segmentation of the network?
- To what level do we need to segment the network while still maintaining business as usual?
- An Architectural Model for Success
- Whether the Organization Understands Device Behavior

Table of Contents

Applying Segmentation Throughout Network Functions

VLAN Segmentation

Access Control List Segmentation

TrustSec Segmentation

Layering Segmentation Functions

Outside the Branch or Campus

How To: Methods and Considerations for Segmentation in an Ideal World

The Bottom Line: Ideal World

Understanding the Contextual Identity

Understanding External Resource Consumption of the Device

Validating Vulnerabilities to External Sites

Understanding Communication Within the Organization

Validating Vulnerabilities Within the Organization

Understanding Communication Within the Broadcast Domain or VLAN

Restricting Peer-to-Peer or Jump-Off Points

Summary

References in This Chapter

Chapter 7 Zero Trust Common Challenges

Chapter Key Points

Challenge: Gaining Visibility into the Unknown (Endpoints)

Overcoming the Challenge: The Use of Contextual Identity

NMAP

Operating System (OS) Detection

Vulnerability Management Integration Systems

Sneakernet

Profiling

System Integrations

Table of Contents

Challenge: Understanding the Expected Behavior of Endpoints

Overcoming the Challenge: Focusing on the Endpoint

Challenge: Understanding External Access Requirements

Overcoming the Challenge: Mapping External Communication Requirements

- Taps
- NetFlow
- Encapsulated Remote Switch Port Analyzer (ERSPAN)
- Proxied Data
- Source of Truth
- CMDBs
- APMs

Challenge: Macrosegmentation vs. Microsegmentation for the Network

Overcoming the Challenge: Deciding Which Segmentation Methodology Is Right for an Organization

Challenge: New Endpoint Onboarding

Overcoming the Challenge: Consistent Onboarding Processes

Challenge: Policies Applied to Edge Networks

Overcoming the Challenge: Ubiquitous Policy Application

Challenge: Organizational Belief That a Firewall Is Enough

Overcoming the Challenge: Defense in Depth and Access-Focused Security

- Vulnerability Scanners
- Device Management Systems
- Malware Prevention and Inspection
- Endpoint-Based Analysis Policies

Overcoming the Challenge: The Case for Securing the Application, Not the Network

Table of Contents

- Summary
- References in This Chapter

Chapter 8 Developing a Successful Segmentation Plan

- Chapter Key Points
- Planning: Defining Goals and Objectives
  - Risk Assessments and Compliance
  - Threat Mapping
  - Data Protection
  - Reducing Attack Surfaces
- Plan: Segmentation Design
  - Top-Down Design Process
  - Bottom-Up Design Process
- Implement: Deploying the Segmentation Design
  - Creating a Segmentation Plan by Site Type
  - Business Services
  - Building IoT
  - Infrastructure Management
  - Guest
  - Services
  - Creating a Segmentation Plan by Endpoint Category
  - Common or Shared Devices
  - Labs
  - Pharma
  - Imaging
  - Point of Care
  - Clinical VDI
  - Creating a Segmentation Plan by Service Type
  - Partner/Vendor Remote Access VPN
  - Employee Remote Access VPN

Table of Contents

Partner Leased Lines

DMZ Services

Corporate WAN

Employee Outbound Internet

Guest Outbound Internet

Unknown

Implement: The Segmentation Model

Summary

References in This Chapter

Chapter 9 Zero Trust Enforcement

Chapter Key Points

A Practical Plan for Implementing Segmentation

Endpoint Monitor Mode

Initial Application of Monitoring Mode

Endpoint Traffic Monitoring

Monitoring of Additional Sites

Enforcement

Network Access Control

Environmental Considerations

Greenfield

Brownfield

Practical Considerations Within Contextual Identity

Authentication (AuthC)

Authorization (AuthZ)

Segmentation

Greenfield

Brownfield

Unified Communications

Table of Contents

Data Exchange

Summary

Chapter 10 Zero Trust Operations

Chapter Key Points

Zero Trust Organization: Post-Implementation Operations

Adoption Barriers

Innovators and Early Adopters

The Early Majority

The Late Majority

Laggards

Applications Owners and Service Teams

Operations and Help Desk

Network and Security Teams

The Life Cycle of Zero Trust Policies

Zero Policy Management

Practical Considerations: Cisco Network Architecture

Moves, Adds, and Changes in a Zero Trust Organization

Summary

References in This Chapter

Chapter 11 Conclusion

Chapter Key Points

Zero Trust Operations: Continuous Improvements

Policy & Governance

Identity

Vulnerability Management

Enforcement

Analytics

Summary

Table of Contents

Appendix A: Applied Use Case for Zero Trust Principles

- Business Problem
- Goals and Drivers
- Application of the Principles of Zero Trust
  - Policy and Governance
  - Understanding the Business
  - Identifying and Vulnerability Management
  - Application of Enforcement
  - Firewalls
  - Identity Services Engine (ISE)
  - TrustSec Tags
  - DNS
  - Analytics
- Conclusion

Index

Pearson