Zero Trust in Resilient Cloud and Network Architectures

JOSH HALLEY
DHRUMIL PRAJAPATI
ARIEL LEZA
VINAY SAINI

ciscopress.com

FREE SAMPLE CHAPTER |

Zero Trust in Resilient Cloud and Network Architectures

Josh Halley, CCIEx3 No. 11924

Dhrumil Prajapati, CCIEx2 No. 28071,
CCDE No. 20210002

Ariel Leza

Vinay Saini, CCIE No. 38448,
CWNE No. 69, CCDE No. 20240032

Cisco Press

Zero Trust in Resilient Cloud and Network Architectures

Josh Halley, Dhrumil Prajapati, Ariel Leza, Vinay Saini

Published by:
Cisco Press
Hoboken, New Jersey

$PrintCode

Library of Congress Control Number: 2025934165

ISBN-13: 978-0-13-820460-0
ISBN-10: 0-13-820460-8

Warning and Disclaimer

This book is designed to provide information about segmentation concepts, network access control, and resilient cloud and enterprise network architectures. 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 authors 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.

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.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Head of IT & Professional Learning, Enterprise Learning and Skills: Julie Phifer

Alliances Manager, Cisco Press: Caroline Antonio

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Senior Project Editor: Mandie Frank

Copy Editor: Chuck Hutchinson

Technical Editors: Asier Arlegui Lacunza, Istvan Matyasovszki

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Donna E. Mulder

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.**

About the Authors

Josh Halley is a Principal Architect in the office of the CTO at Cisco Systems, where his current role focuses on domains related to up-and-coming and burgeoning new technology trends and innovation, engaging in large and complex strategic negotiations, and working with C-Levels to set technology strategy and direction within their organizations. Over the years, Josh has worked in many differing roles at organizations ranging from technology companies to banking and finance and management consulting.

Technology has long been a passion and key area of interest throughout his career, leading Josh to pursue three CCIE certifications to advance his expertise across multiple domains. During his years at Cisco, he has been engaged in technology projects and pre-sales activities all around the world, which has given him the opportunity to learn different cultures, perspectives, and customs.

Within Cisco, Josh has worked side by side with many of the company's business units, product managers, and technical marketing engineers and has been directly involved in the creation and deployment of over 180 new software features across multiple technology domains, many of which are associated with zero trust capabilities seen in Cisco's products and portfolio today.

Today Josh maintains his focus on technology, driving innovation with customers in the field and actively participating in the creation of patents and white papers and new product and service offerings for Cisco. Further to his work within Cisco, Josh is also an open-source software advocate who actively participates in working groups from the Cloud Native Computing Foundation, providing him an opportunity to share his knowledge and expertise with the wider open-source community.

Dhrumil Prajapati is a Principal Architect within Cisco CX's GES Architectures team. His focus lies on designing multidomain networks, and he has been offering a complete lifecycle of professional services and architecture advice for the past 15 years. His expertise extends to serving enterprise, government, and service provider entities across the globe. His services are designed to assist clients in planning, designing, deploying, managing, and interoperating all networking technology domains within their private or public infrastructure and application environments.

In his networking career, Dhrumil has designed networks for over 175 organizations, which inspired him to write a book on the subject. He is a coauthor of *Designing Real-World Multi-Domain Networks* (https://www.ciscopress.com/store/designing-real-world-multi-domain-networks-9780138037215) and *Cisco SD-Access for Industry Verticals* (https://cs.co/sda-verticals-book). He also holds patents and has given multiple presentations in Cisco Live on SD-Access, multidomain, and automation.

Dhrumil holds dual CCIEs in Enterprise Infrastructure and Service Provider, as well as a CCDE, in addition to other leading technical certificates. He also assists the Cisco Certifications team by reviewing and providing feedback for Cisco Certification Program. In addition, he leads several initiatives within Cisco CX aimed at driving delivery standardization and enhancing efficiency through automation innovation.

Currently residing in Apex, North Carolina, Dhrumil has a passion for motor racing, woodworking, and innovative electronics that enhance human life. His wife, Devanshi, and son, Ram, bring pure joy to his life, adding a touch of fun every day.

Ariel Leza, an ardent entrepreneur and technology aficionado, currently excels as a Cloud Solutions Architect in the EMEA CX CTO office at Cisco. His expertise is centered on guiding clients toward achieving their unique objectives through intricate cloud and IT architectures. Ariel's journey in the IT realm commenced during his military service as a network engineer in 2011, uncovering his passion for networking and cybersecurity. Today, he stands as a results-driven entrepreneur with a proven track record in technical sales and product positioning, fueled by enthusiasm for creating new businesses.

With over a decade of experience in the field, Ariel specializes in cloud and cross-domain IT architectures, focusing on cloud-native technologies, open-source software, networking, virtualization/compute, and data center software stack components. As a technology leader and technical solution architect in the Israeli market, he has demonstrated an exceptional ability to convey complex technological concepts in simple terms, tailoring his message to diverse audiences and emphasizing Cisco's unique value proposition.

In his role under the Customer Experience CTO Office of EMEA, Ariel has been instrumental in driving strategic programs and building strategic relationships with key accounts, leading to significant achievements such as engagement with top EMEA accounts, patent submissions, and pioneering deployments in blockchain technology and cloud-native services. His skills in cloud-native platforms, DevOps, Linux, and cloud computing are complemented by his deep understanding of decentralized applications, cryptocurrency, microservices, and Web3 blockchain architectures.

Outside of his professional endeavors, Ariel is a passionate participant in open-source and community projects. He also dedicates his time to global business ventures and the management of his demo Innovation Lab initiative. Ariel's commitment to making a meaningful impact as an entrepreneur and businessperson is driven by his belief in taking active responsibility for our civilization's actions and consequences.

With a vibrant spirit and an undying passion for technology and innovation, Ariel Leza continues to make significant strides in the tech world, inspiring others and driving successful customer outcomes with his dynamic approach and creative solutions.

Vinay Saini is a technologist, inventor, author, and mentor with over two decades of experience in the networking industry. As a Principal Architect at Cisco Systems (Customer Experience Group), Vinay guides customers across diverse verticals—including enterprise and IIoT—on their digital transformation journeys.

Vinay holds a bachelor of technology degree in IT and an MBA in international business. He is the first individual in India to achieve dual expert-level certifications: CWNE (#69) and CCIE (#38448). Additionally, Vinay is CCDE certified (#20240032) and holds many other industry credentials. He also actively contributes to Cisco Certification programs.

With a portfolio of over 100 patents filed and numerous defensive innovations, Vinay is at the forefront of technological innovation. As a sought-after speaker at events like Cisco Live, Vinay is also passionate about mentoring professionals worldwide, fostering their growth in technical and behavioral domains to help them reach their full potential.

About the Technical Reviewers

Asier Arlegui Lacunza, CCIE No. 5921, has been with Cisco since 1998 and currently works as a Principal Architect in Cisco's Customer Experience organization. In the past 20+ years of his career at Cisco, he has worked as a technical architect on a wide range of enterprise (data center, campus, and enterprise WAN) and service provider (access and core networking) technology projects, with a focus on network automation. He holds a master's degree in telecommunications engineering from Public University of Navarre, Spain.

Istvan Matyasovszki has been with Cisco since 2007 and is currently a Security Solutions Architect in Cisco's EMEA Customer Experience organization, with a special interest and focus on network access control, remote access, intrusion detection, and microsegmentation. Istvan holds a PhD in computer engineering from the University of Limerick in Ireland and, before that, worked as a UNIX/Linux system administrator for several years.

Dedications

Josh:

I would like to dedicate this book to my two bloodhounds. Thanks for keeping me company and spending many a late night and early morning with me while I was authoring my chapters.

Dhrumil:

Publishing a first book is a core memory, and the third one sets an example for many. I want to dedicate this book to my wife, Devanshi, who has given unconditional love and been a true partner as I achieve my goal. It goes to the silent sacrifices you have made that brought me to where I am today.

My son, Ram, I never imagined I would write a book, but your curiosity in reading books from a young age and gaining as much knowledge as possible has inspired me to write my third book.

Ariel:

I would like to dedicate this book to the open-source community, including the developers and advocates championing the progression of the next generation of decentralized technologies.

Vinay:

To my parents, for instilling in me the values of perseverance and curiosity.

To my wife, Sowbhagya, for her unwavering support and patience throughout this journey.

To my children, Vihaan and Pranav, for inspiring me to think about a better future.

To my colleagues, friends, and mentors, whose insights, encouragement, and collaboration have been invaluable.

This book is dedicated to you.

Acknowledgments

Josh:

There were so many talented individuals who supported me on the journey of writing this publication that I feel it could fill an entire new chapter alone. With that clearly not being possible, I would like to begin by sending my sincere thanks to our reviewers, Asier and Istvan, who patiently provided us with feedback, comments, and creative criticism. Thanks, guys, for taking on this on top of your already hectic and busy day jobs to support me. Thanks also to our publisher, Pearson, and its amazing team who put up with our challenging schedules, updates, changes, and erroneous grammar. I would like to share a very special thank you to Meg Rainbow for her contribution on Chapter 1, Lee Sudduth for his contribution on Chapter 14, and Marcin Hamroz and Jaroslaw Gawron for their contributions on Chapter 22; these contributions added real-world perspectives from other vantage points that certainly enriched the overall manuscript. THANK YOU! Additionally, I would like to thank Kevin Regan, Alex Burger, Gino Corleto, Keith Baldwin, Mahesh Nagireddy, Jerome Dolphin, Sandeep Joseph, Einar Nilsen-Nygaard, Jonothan Eaves, Jeremy Cohoe, Kevin van Hengel, and Darrin Miller for their help and guidance along the way. To my leadership team (past and present), Adele Trombetta, Michael Kaemper, Markus Gierlich, and Haim Pinto, thank you for being supportive of my taking on this endeavor. And, last but certainly not least, I would like to thank my loving wife and children for their all-enduring support and motivation.

Dhrumil:

I would like to thank my leaders—Larry Hohmann, Mike Shomaker, and Jason Penn—for supporting me through this journey.

My peers, colleagues, and esteemed architects who have always shown their technical aptitude and willingness to help.

Lastly, to Amit Singh, without whom Chapter 12 of this book would not have been complete!

Ariel:

I would like to thank the great team at Pearson for their support in reviewing my content and supporting me along the way. I would also like to share a special thank you to my family and fiancé, Lilian, for their patience and support through the process of creating this book.

Vinay:

I would like to express my heartfelt gratitude to my management at Cisco for their unwavering support and encouragement, constantly motivating me to go beyond my defined role and explore new possibilities. Their guidance has been instrumental in shaping my professional growth.

I would also like to extend my appreciation to my colleagues, mentors, and the broader Cisco community for their collaboration, insights, and shared passion for innovation. Their support and camaraderie have made this journey truly enriching.

This book is a reflection of the collective inspiration and knowledge I have gained from working alongside such incredible individuals. Thank you for being a part of my journey.

Contents at a Glance

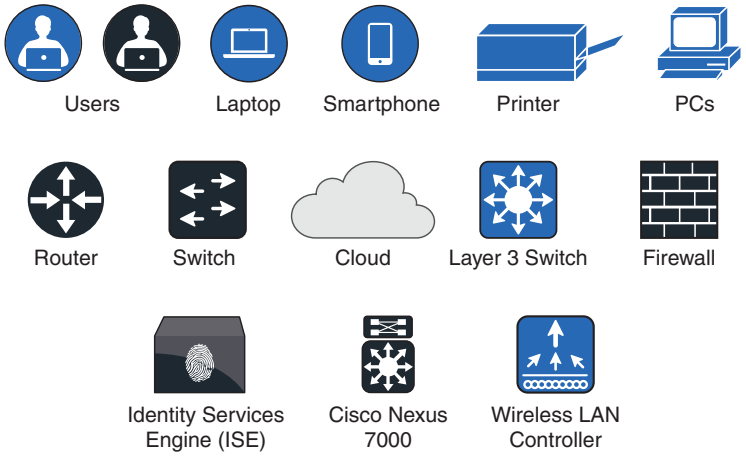
Reader Services

Register your copy at www.ciscopress.com/title/ISBN for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780138204600 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Contents

Icons Used in This Book



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

The idea for this book originally came into existence during a time that the four authors were heavily involved in global deployments of large and complex networks focused on zero trust architectures. Pre-COVID, many of the authors were traveling up to 42 weeks a year, meeting with customers, supporting large deployments onsite, and hearing first-hand about the challenges, pitfalls, and gotchas they were experiencing from deploying advanced and new technology suites that could lead to a more robust and secure network architecture.

Over time, the team observed the technology mature, the escalations and teething issues seen in the early days of deployments of zero trust networks subside, and customers shift gears to realize their visions of a more automated, dynamic, and secure estate, focusing on the principles of providing only the requisite access for a given service. In addition to the maturity of the technology, the expansion of domains to adopt zero trust principles moved beyond the campus, to other domains and verticals, such as edge compute, the data center, cloud, and deployment in containerized form factors in AI agents. These adoptions further cemented the need to ensure a robust and secure estate, regardless of the location of the user, endpoint, workload, or autonomous/semi-autonomous software process.

The key focus areas of this book are not specific to a single technology; this title provides a focus on the domains of resilience, automation, security, and cloud architectures. While separate in their own right, when utilized together, they can result in a scalable, secure, and future-proof deployment.

Who Should Read This Book?

This book is aimed at security engineers, security analysts, site reliability engineers, network engineers, architects, and operations teams who have a key focus on optimizing their network deployments, increasing security, resilience, and automation within their organization. Given the experience of the authors, a heavy focus has been placed on real-life examples from their years of deployment experience globally. While it would have been easy to describe the solutions through rose-colored lenses, this book provides a candid overview of the good, the bad, and the ugly that you can experience on your journey toward building an automated, resilient, and secure enterprise estate.

How This Book Is Organized

Chapter 1, "Zero Trust Demystified": This chapter provides an overview of the importance of zero trust in an organization's network.

Chapter 2, "Secure Automation and Orchestration Overview": This chapter provides an overview of the automation and orchestration strategies available during the writing of this book.

Chapter 3, "Zero Trust Network Deployment": This chapter provides an overview of zero trust deployment on secure service edge and other architectures.

Chapter 4, "Security and Segmentation": This chapter takes you on a deep dive into micro- and macrosegmentation concepts and explains where they can be best applied for a modern enterprise network.

Chapter 5, "DHCP and Dynamic Addressing Concepts": This chapter provides an overview of dynamic addressing and security concepts related to its use.

Chapter 6, "Automating the Campus": This chapter covers concepts of campus automation and how to achieve them securely.

Chapter 7, "Plug-and-Play and Zero-Touch Provisioning": This chapter describes aspects of secure zero-touch and plug-and-play onboarding of network devices in enterprise domains, including resilience automation aspects.

Chapter 8, "Routing and Traffic Engineering": This chapter covers concepts of routing and traffic engineering, showing how proper planning and foresight can lead to building the most resilient networks.

Chapter 9, "Authentication and Authorization": This chapter details concepts associated with authentication and dynamic authorization in enterprise architectures.

Chapter 10, "Quantum Security": This chapter explains the deployment of quantum-based security and explores the concepts associated with how quantum security is relevant to a network estate.

Chapter 11, "Network Convergence and Considerations": This chapter explores concepts of convergence in software-defined architectures for enterprise, data center, and security domains in detail.

Chapter 12, "Software-Defined Network Deployment Best Practices": This chapter covers the best practices of SDN networks and how to deploy them.

Chapter 13, "Wired and Wireless Assurance": This chapter explores enterprise wired and wireless deployment constructs from a resilience perspective, including security options for guest network access in Cisco cloud-based Meraki and on-premises deployments.

Chapter 14, "Large-Scale Global Software-Defined Network Deployment Best Practices": This chapter focuses on a global Meraki network deployment, whereby Infrastructure as Code concepts and approaches are used to simplify and scale the deployment.

Chapter 15, "Cloud-Native Security Foundation": This chapter covers key security principles for cloud-native environments, focusing on zero trust, workload protection, IAM, encryption, and compliance. It also explores CSPM, infrastructure as code (IaC) security, and AI-driven threat detection.

Chapter 16, "Cloud-Native Application Security": Focusing on securing applications in dynamic environments, this chapter covers DevSecOps, CI/CD security, API protection, and OWASP best practices. It also explores Web3-based identity (DID) and AI-driven security automation.

Chapter 17, "Data Center Segmentation On-Prem to the Cloud": This chapter examines segmentation strategies for hybrid and multi-cloud environments, highlighting zero trust, microsegmentation, and policy enforcement. It also explores cloud-native segmentation models and blockchain-based security.

Chapter 18, "Using Common Policy to Enforce Security": This chapter discusses unified security policies, IAM best practices, and automated enforcement using CASBs and SOAR. It also covers software security frameworks (SDLC to SSDLC) and OWASP SAMM for security maturity.

Chapter 19, "Workload Mobility: On-Prem to Cloud": This chapter explores workload migration strategies, zero trust integration, data security, and compliance. It also covers post-migration optimization, including cost management and observability tools.

Chapter 20, "Resilience and Survivability": The chapter focuses on key concepts around redundancy, survivability, and resilience for network architectures in the context of routed network deployments and security architectures.

Chapter 21, "Zero Trust in Industrial Manufacturing Vertical": This chapter explores OT/IoT-type deployments in the domain of security and zero trust.

Chapter 22, "Third-Party SDN Integrations": This chapter explores the integration of third-party devices and systems into a broader zero trust architecture and domain.

Chapter 23, "Infrastructure as Code": This chapter describes key concepts associated with deploying automation for Infrastructure as Code in secure enterprise networks.

Credits

Front Cover - TechAnimationStock/Shutterstock

Figures 4.12, 4.14, 7.2, 9.13, 11.25 & 13.7 - Wireshark Foundation

Figure 11.21 - Keysight Technologies

Figure 15.2 - Center for Internet Security

Figure 15.6 - Gartner, Inc

Figures 16.1 & 23.3 - GitHub, Inc

Figure 19.1 - Flexera

Figure 19.02- Amazon Web Services, Inc

Figure 19.3 - ChaosSearch, Inc.

Chapter 3

Zero Trust Network Deployment

In this chapter, you will learn about the following:

- Zero trust and functional pillars
- Elements of zero trust policy
- Tools and technologies for zero trust deployment
- Greenfield versus brownfield zero trust network deployment

In today's risky and uncertain times, organizations need to build a solid foundation for reliable and adaptable security operations. This could be achieved by building zero trust in their IT systems. The zero trust framework operates on the principle of "never trust, always verify." Unlike traditional security approaches that rely on a strong perimeter (like firewalls) to protect a trusted internal network, zero trust assumes that threats can originate both inside and outside the organization. Therefore, every request, user, or device must be authenticated and authorized, regardless of its location within or outside the network. It is important to understand the functional pillars of zero trust before any organization starts deploying it. You will need a variety of tools and platforms to deploy zero trust in your organization. Your zero trust approach must be able to perform the following four functions:

- **Establish Trust:** Ensure the system can verify each user and device connecting to the network.
- **Enforce Trust-Based Access:** The system should be able to enforce policies and grant access to the users and devices based on the trust level. The policies should be applied based on the principle of least privilege. The access mechanism should protect all network resources, including applications and data, on-premises and in the cloud.

- **Verify Trust:** The system should be able to continuously verify the trust and dynamically adjust the access to the network. It should not be a time check and then access is allowed for a longer duration or to multiple applications.
- **Enforce Policies and Monitor:** The system should be able to react to changes in trust by analyzing and coordinating responses to potential incidents while gaining better visibility into suspicious activities related to trust levels. A continuous refinement of trust policies is required.

An organization needs to protect all its assets irrespective of their location. Some assets could be mobile-like users and devices, and others like applications, and stationary databases could either be on-premises or hosted in the cloud. The zero trust approach should consider various factors, such as user type, location, device type, data requested, and application accessed, to create robust dynamic policy-based access controls. Some of the common assets you want to protect in your organization include (but are not limited to)

- Users
- Devices
- Network
- Cloud
- Applications
- Data

A common question arises: Where to start, and how can you define the steps toward a zero trust framework adoption?

In the rest of this chapter, you will learn the iterative approach that could be adopted for securing trusted access for users and devices based on the four primary functional requirements of zero trust as covered in this section. We will first look at the key decision points to establish the overall zero trust strategy that includes establishing trust for users and devices, application access, and policy enforcement. Next, we will look at the common tools and technologies to help you deploy zero trust, and finally, we will look at the approach for zero trust adoption in greenfield and brownfield scenarios.

Elements of Zero Trust Strategy Definitions

In this section, we will look at the key considerations that you will need to formulate the zero trust deployment policy. These considerations include

- Establishing user trust
- Establishing device trust
- Defining application access policies
- Enforcing policies

Establishing Trust

A trust level represents the degree of confidence you have that a user or device is who or what they claim to be and that they are authorized to access specific resources. Unlike older models, where access is granted based on location (inside vs. outside the network), trust levels in zero trust are dynamic and can change based on several factors. Trust levels can be assigned to users and devices.

- **User Trust Level:** Based on the identity of the person accessing the network
- **Device Trust Level:** Based on the security status of the device accessing the network

The first functional requirement of zero trust is to establish trust for users and devices. This requirement could be divided into two categories: users and devices. Let's look at both of them in detail.

User Trust Definition

The purpose of defining user trust is to verify the user's trust and enforce the principle of least privilege. You need to start evaluating what mechanisms and processes are there in your organization to authenticate and authorize the users before they can access the resources. But wait, which users? There could be different types of users having different privilege access. To start, do the following:

1. Identify the user types and roles (employees, including contractors, temporary users, and guests).
2. Associate the risk with each user type, based on their function and type of data they need to access.
3. Identify the assets that need to be accessed by these user groups.
4. Identify the location of assets each group needs to access—on-premises, cloud, DMZ, and so on.

Following these steps, you will get a matrix that shows the user group and their need to access, which type of information, and where that information is stored. As a next step, you need to define the trust level for each user type based on the authentication and authorization system in place or planned. You can start evaluating as follows:

- How does an employee need to be authenticated and authorized?
- How does a partner need to be authenticated and authorized?
- Can you deploy multifactor authentication (MFA)? If yes, which applications are critical?
- Is biometric-based passwordless authentication required?
- How often is the MFA required, and what reauthentication triggers need to be deployed?
- Do you have a secure identity database for the full type or contract employees?

Once you have evaluated the responses to the questions, you will then need to devise a policy, plan, and then deploy the solution that allows strong authentication and authorization of the users before they can access any information. User trust can be verified using different methods and actions such as:

- **Multifactor Authentication (MFA):** Ensure users verify their identity through multiple factors (something they know, have, or are)—for instance, a password combined with a mobile authentication app or biometric verification.
- **Role-Based Access Control (RBAC):** Grant users access only based on their roles, ensuring they can access the minimum necessary resources.
- **Contextual Authentication:** Authenticate based on context (time of access, location, device type) to provide a more secure, tailored approach.
- **Just-in-Time Access:** Ensure that users get access only when they need it and that it's revoked immediately after their session ends, minimizing the risk of lingering access.
- **User Behavior Analytics (UBA):** Monitor user activity in real time, including access patterns and application usage. Anomalies (e.g., accessing data from an unusual location or time) trigger additional authentication steps or even block access.
- **Dynamic Risk Scoring:** Assign risk scores to users based on behavior, device posture, and external factors (e.g., suspicious login attempts). Trust levels adjust dynamically based on these scores.

For a greenfield scenario (described more fully later in this chapter), it is easy to plan, design, and implement first. Users are then onboarded to a well-defined and secure environment. But in a brownfield environment, you might face challenges such as users being hesitant to adopt new methods of authentication. Some workflows might need to be interrupted to adopt a new user identity verification system. To overcome some of these challenges, you must do the following:

- Prepare clear communication and messaging for the need for change.
- To avoid any hiccups due to technical glitches, ensure that all systems are tested. You can start the pilot with a small group and data set as identified in the matrix.

Device Trust Definition

Defining device trust means ensuring that a device is safe and authorized to access the network. You must never assume that any device is safe because it is inside the network or is company-owned. Especially with BYOD policies, employees are now allowed to bring their own devices to work. Such devices need to be secured and segmented properly. Ensuring devices accessing your network are in a healthy state is a critical step for zero trust deployment. You can start by doing the following:

- Evaluate the type of the company's own assets, such as model, make, and operating systems.
- Rank devices based on the risk and data sensitivity.

- Create a list of technologies that can be used for device trust such as virtual private network (VPN), mobile device management (MDM), and certificates.
- Create a strategy based on supported devices and their capabilities such that each device can be continuously authenticated.

It is important to understand the difference between a company-owned asset and company-managed asset. A company-owned asset is owned, managed, and fully controlled by the organization, whereas a company-managed-only device typically includes BYOD devices that an employee can purchase but are managed by the company. This is typically done by enrolling devices in an MDM system that defines the security policy and configuration for the device such as certificate requirements or password lengths. You can even wipe an entire device remotely if an employee reports it as stolen. Access to further applications and resources could be constrained for such devices. Because managed devices are tracked, enrolled in configuration and patch management programs, and continuously monitored for security incidents, the trust level for such devices is always higher than for unmanaged personal devices. As such, your zero trust policy usually allows Internet-only access for unmanaged personal devices. We have discussed managed and unmanaged devices, but how do you bring a device under management? You can use a combination of solutions such as

- **Certificate-Based Trust:** In zero trust, every device must prove itself before accessing any resource. Using certificate-based trust, a device proves its identity by showing its digital certificate. Even if the device is already inside the network, it must keep proving its trustworthiness every time it tries to access new resources or data.
- **Device Health:** It is important to ensure that a device is healthy before it can be allowed on the company's network. Even a company-managed device with a certificate installed can get infected. It is important to use device posture as one of the device trust points. Validating if the endpoint security agent is installed to protect against the threats helps in establishing trust.

Device trust further strengthens the security because now an attacker needs not only a valid user credential but also a trusted device to launch any attack. A combination of trusted users with trusted devices is commonly used as part of the zero trust policy definition to provide different levels of access. Typical components you will require for device trust include

- **PKI Infrastructure:** PKI (Public Key Infrastructure) is a framework that manages digital certificates and encryption keys to enable secure communication and authentication over networks. In zero trust PKI is used to issue device certificates. These issued certificates will be used for identifying all company-managed assets, including company-owned or BYOD assets.
- **Security Agents:** A variety of tools can be installed on company-owned assets, such as endpoint agents, VPN, VPNless remote access, and device posture agents. For BYOD, an MDM solution could be used.
- **Central Inventory:** It is important to have a central inventory of all devices in your network with proper asset tags, owners, type of access required, and so on.

One common challenge with device trust is the hesitation of users to install any agent or certificate on their devices due to privacy concerns. This requires careful validation based on the local laws, so the organization must use a solution to verify the trust without violating privacy. As an example, monitoring the website that a user visits on a BYOD could be considered a privacy issue, while suggesting a stronger login password with a specific key length could be considered a genuine safety measure.

With user and device trust policies established, you now know who can access the network using which types of devices. We have covered a high-level approach, but you need to go multiple levels down to establish detailed policies, tools, procedures, and ways to track the user and device trust. Once you have done this, the next step is to enable access to the application by framing policies that a combination of users and devices can access.

Trust Score Calculation

Trust levels can be represented as scores or risk levels based on multiple factors. Here's a simple breakdown of how they might be calculated.

Each factor gets a score, and the total score determines the user/device trust level:

- Base Trust for User Credentials (e.g., MFA or SSO): 50 points
- Device Security (e.g., fully patched, antivirus running): 30 points
- Geolocation (known/unknown location): 10 points
- Time of Access (normal/abnormal): 10 points

If all conditions are met, the trust score would be 100. A lower score (below a set threshold, e.g., 70) might trigger additional security actions, like reauthentication or restricted access.

Instead of adding points, you can subtract trust based on risk indicators. For instance:

- Base Trust: Start at 70.
- Subtract 40 if the user uses only a password (no MFA).
- Subtract 20 if the device is missing recent patches.
- Subtract 10 for unrecognized geolocation.

Once a trust score or risk level is assigned, the system decides how much access to grant and whether any additional actions are needed:

- **High Trust Score (90–100):** Full access to the system, no extra verification needed.
- **Medium Trust Score (70–89):** Limited access, or additional verification required like MFA.
- **Low Trust Score (Below 70):** Deny access or allow access only to less-sensitive resources.

Defining Application Access Policies

The entire idea of establishing trust for users and devices is to allow them access to business applications in a secure way. This ensures that even after the user and device are verified, they get access only to specific applications they need. One of the important considerations you need to make is where the application and data are hosted, such as public or private cloud, on-premises, or SaaS applications. You will need to devise the policies for different data sets and applications based on how often they are accessed, keeping in mind the user experience you want to provide. Following are some of the decision points for creating policy around application access:

- A comprehensive list of applications used in the organization, both internal and external, should include cloud-based, on-premises, and hybrid applications.
- It is also important to identify the application dependencies like interactions with databases, other services, and APIs. This information will come in handy while building the microsegmentation.
- What user types need to access the application? We covered this step from a user authentication perspective earlier in the user trust definition, but now you need to map the application in detail, along with the frequency at which different user groups typically access any applications, and rank the risk of the applications.
- Policies also need to consider device type and location of user groups concerning the application accessed. Do you want to reauthorize or have stricter controls when users try to access the service from a location that is different from their regular location? If your entire workforce is mobile, then your strategy needs to include the fact that random location is normal behavior. In such a case, frequent location-based reauthorization may result in poor user experience. You may want to club the common application sets and allow access based on single sign-on (SSO).
- The SSO-based approach is essential because users often forget passwords for multiple applications. When many applications are involved, users may resort to using the same password for all. Here, SSO provides a centralized enforcement point, allowing the establishment of policies on password length and change frequency. It is advisable to implement multifactor authentication with biometrics alongside SSO.

Access policies should align with user and device trust levels. Trust depends on contextual factors like location, time, and behavior, necessitating continuous monitoring even for authorized access. For example, if a terminated employee quickly downloads multiple files, this could indicate potential malicious intent. Such behavior should trigger alerts or adjust access per established protocols. This strict approach reflects a zero trust framework, which emphasizes that no one is inherently trusted. Ongoing supervision and adaptive policies are vital to enforce zero trust principles.

Macro- and microsegmentation form the basis of the zero trust network access, as you will learn later in this book. From an application perspective, it is also critical that segmentation considers the following constructs:

- **Application-Level Segmentation:** Isolate applications from one another so that a compromise in one doesn't lead to a breach in others. This involves defining granular policies for inter-application communication and blocking unnecessary pathways.
- **Data and API Segmentation:** Segregate databases, APIs, and other backend services from applications and users that don't require direct access.
- **Environment Segmentation:** Separate development, testing, and production environments to ensure that an issue or breach in one environment doesn't spread to others.

It is also important to think about securing the data in motion. When the authorized user groups access specific applications, it must be secure. Following are some of the approaches you may consider:

- **Transport Layer Security (TLS):** Ensure that all traffic between users and applications is encrypted using TLS, preventing interception by attackers.
- **End-to-End Encryption:** For sensitive applications, ensure that data is encrypted at rest and in transit, especially when communicating with external services or across untrusted networks.
- **API Security:** Use API gateways and API security tools to secure communications between applications, especially in cloud environments where APIs are frequently exposed.

Enforcing Policies

With the details gathered so far, now you have a clear understanding of the users, devices, and applications in your environment. It is time to think about how to enforce these policies, monitor the users, and continuously refine them. Because there is a complex matrix of users, devices, and applications, it is important to set a baseline and expand from there. This means a base trust with the users and devices is based on certain factors like

- If the user is seen for the first time
- Which factors are used to authenticate and authorize the users
- If there are signs of malicious activities
- If the device is managed; if yes, company-owned or BYOD?
- Device posture details

If these basic checks pass, you can assign the base trust-level policies that allow access to the common and less risky applications. You can then add further levels of trust

confirmation for the highly sensitive user and application combination. This means that with base trust users can access common applications such as email and Microsoft Office. For example, if the user login happens at the usual time, using the known devices with an attempt to access the regular applications, the decision engine could assign a high trust level with no additional authorization steps required. This will also help you define trust tolerance, as explained later in this chapter.

Granular policies and secondary trust verification are required to access critical assets, including code or financial information. At this point, you also need to decide what actions or changes will result in a loss of trust—for example, a change in hardware. A real-time decision engine is typically used for adaptive access.

Contextual information from the users needs to be collected, stored, and then analyzed to continuously evolve the policies. Advanced AI/ML-based analysis engines could be deployed for this behavior analysis. The information base must have information from events, as described in the following subsections.

Contextual Data

User roles and devices change over time. Employees might change their role for various reasons, such as changing teams or getting a promotion. As a result, the location to access the information also changes. Device type, operating system, and applications used might also change. It is important to collect all this information.

Connection Metadata

It is important to collect user role information and device details at the time of login. User roles could easily be collected from the active directory group memberships, and device details can be collected during posture assessment. Operating system version, installation of mandatory endpoint solutions, device status (e.g., if jailbroken)—all must be collected and stored for further analysis. This also allows you to have a central inventory of all the devices in one place with their security state. This information, when combined with the user information, provides insights into the compliance status of teams and individuals. Necessary actions can be taken if noncompliance is related to a specific group or team.

Logging Suspicious Actions

As you established the baseline trust earlier, it is also important to create the baseline behavior of the users within that trust level. Any deviation from the baseline needs to be recorded and analyzed, and immediate action should be taken. Continuous failed attempts at authorization, use of unsupported platforms to access resources (like jailbroken devices), and attempts to access resources with different user credentials from the same device must all trigger alerts, and immediate action needs to be taken based on company security policies. Additional authorization using MFA, device quarantines, and reduced trust level with each event like this are some of the many actions you can take in these cases. Detailed analysis will help you identify the repeat offenders (intentional or

unintentional). AI-based predictive analysis could be used once sufficient data points are available, to help prevent the attacks, reduce the attack surface, and create a self-healing network. Details on self-healing and maturity levels are covered in the later chapters.

Trust Tolerance

Trust tolerance is the degree of flexibility in the zero trust model. While the fundamental principle is "never trust, always verify," trust tolerance allows for different levels of stringency depending on various factors like the sensitivity of the resource, user context, or current security posture of the device. It answers the question: "How much risk are we willing to accept for this specific access?"

- **High Sensitivity (Low Trust Tolerance):** When a user is accessing critical systems (e.g., financial records, confidential data), there is minimal tolerance for risk. Trust levels must be high, and any small deviation (like accessing from a new location or using a noncompliant device) should trigger additional security measures or block access.
- **Low Sensitivity (Higher Trust Tolerance):** When a user is accessing less critical resources (e.g., internal HR portals or general information), the system can tolerate more variations in trust. For instance, accessing from an unfamiliar device might still be allowed, but with more monitoring.

In zero trust, you will create a dynamic trust tolerance, which adjusts based on the current risk environment. A user trust value could be very high at the time of initial login and authentication. However, as the user tries to access different applications, the trust level can erode based on that user's behavior. Every organization needs to devise policies that reflect its trust tolerance. Threshold-based dynamic access policies need to be defined. If the trust level of a user is maintained, the sessions and access levels could be extended by a predefined time. In that case of trust falling below a certain threshold, the user needs to be reauthorized before access to the existing or new applications can be granted.

Several tools can help organizations manage trust tolerance within a zero trust architecture:

- Identity and access management (IAM) tools like Okta or Microsoft Azure Active Directory allow for context-based access policies that adjust trust levels dynamically.
- Security information and event management (SIEM) solutions like Cisco Splunk or Elastic Stack help monitor security events and adjust trust tolerance based on real-time risk factors.
- Endpoint detection and response (EDR) solutions like Cisco Secure Endpoint or CrowdStrike provide continuous monitoring of device security, adjusting trust tolerance based on device posture.

By this point, you must have a clear understanding of the overall approach and key decision points to develop a zero trust policy by defining clear objectives around user and device trust, application access, and policy definition requirements. In the next section, we will explore various tools and technologies that help you achieve these outcomes.

Tools and Technologies

When an organization implements a robust zero trust architecture, a variety of tools and technologies are essential for continuously validating users, devices, and applications at every access point. These solutions work together to ensure that only authenticated and authorized entities are allowed to access specific resources. By leveraging these technologies, organizations can enforce strict security policies, limit potential attack surfaces, and create an environment where trust is never implicitly granted but is verified with each interaction.

Central Inventory

A central user and device inventory is like a list that keeps track of who the users are and what corporate and personal devices they are using. Each user or device has a role or job. These roles tell the system what the user or device is allowed to do. This inventory helps the security system decide if a user or device can access certain information or parts of the network. One of the primary ways to implement zero trust is to assign users and devices to specific domains based on their communication needs. Typically, every organization will maintain the active directory for its users, grouped under different business groups. These active directories are then mapped with authentication servers like the Cisco Identity Services Engine, and different policies can then be created for different sets of users. Additional parameters—device type, posture state, time of day, and so on—can be used in authorization policies.

Having a central repository is one of the prime requirements of zero trust implementation. At the time of writing this chapter, Cisco Identity Services Engine can join up to 50 active directory domains. This allows segmented domains to be brought under a single zero trust policy domain.

Identity and Access Management

Validating the user identity using strong methods is fundamental to the zero trust implementation. Passwords can be easily stolen and reused; as such, strong authentication methods such as MFA need to be part of the user validation. Following are some of the approaches you can take:

- **Multifactor Authentication (MFA):** Ensure users provide two or more ways to prove their identity (for example, a password plus a one-time code sent to their phone).
- **cMFA:** Use tools that support continuous validation of the user identity at fixed intervals or based on triggers.

- **Single Sign-On (SSO):** Allow users to log in once and access multiple applications securely.
- **Role-Based Access Control (RBAC):** Set up permissions based on user roles, ensuring people access only what they need. For example, a marketing team member should not access financial systems.

Tools like Okta, Microsoft Azure Active Directory, or Duo Security can help you manage identities and enforce MFA and SSO.

Network Segmentation

To apply the zero trust polices, a network must be segmented using macro- and microsegmentation approaches. Remember that zero trust is not only about providing secure access; it is also about reducing or limiting the impact of any attack. Network segmentation reduces the attack surface by limiting access to a specific domain.

Macrosegmentation is a way to divide a network into smaller virtual networks (segments), usually based on the types of users, devices, or applications. Each virtual network will have its own security rules. For example, you might create one network segment for employees, another for guests, and a third for sensitive data. In zero trust deployment, macrosegmentation helps by limiting who can access certain parts of the network. Even if someone gets access to one segment, that person can't move freely to other segments without passing additional security checks. This makes it harder for attackers to spread across the network, improving security and reducing the risk of unauthorized access. You will create macrosegmentation using firewall boundaries and virtual segmentation using concepts of virtual routing and forwarding (VRF).

Microsegmentation approaches like VLAN, security group tags (SGTs), or endpoint groups (EPGs) in data centers allow microsegmentation within a macrosegment. The idea is to further restrict and control the communication. With the zero trust principle, only allow communication to what is required. To implement this, smaller network segments are desired. However, the manual assignment of users and devices becomes a management overhead. That is why automated assignment of microsegments is done using AAA servers like ISE.

Figure 3-1 shows high-level macrosegmentation using VRFs and firewalls. You will notice that firewalls are used to isolate the different sections of the network such as the data center, Internet, and BMS/OT areas. The microsegmentation approaches of SGT/VLAN can be used to create microsegmentation within each group. In this example, the enterprise LAN is microsegmented into various segments for corporate laptops, IoT endpoints, and collaboration endpoints. The OT network is using VLAN as a microsegmentation approach with the firewall creating a separate OT zone and macrosegment.

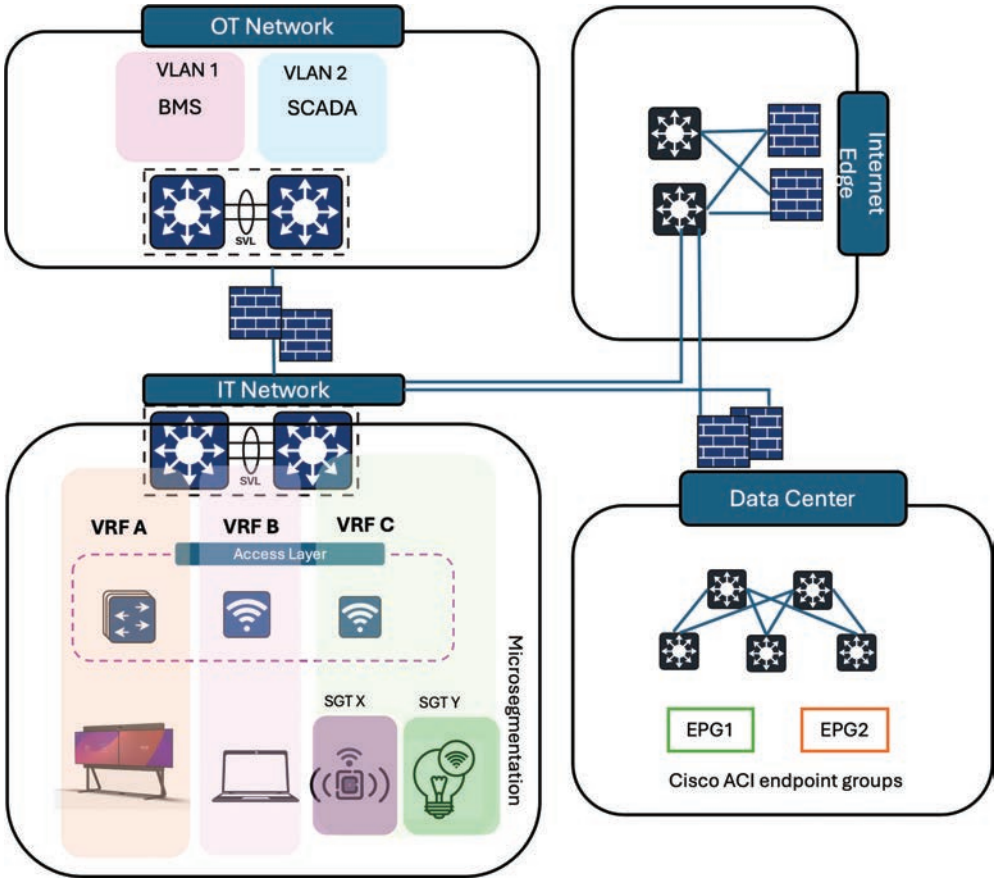


Figure 3-1 *Network Segmentation for a Typical Enterprise with IT, OT, and Data Center Blocks*

Device Posture with Endpoint Security

Because different types of endpoints will connect to different parts of the network, it is important to ensure these endpoints are healthy. Even though the devices will connect in their own microsegments, still they can pose risks to the network and other devices. Accessing the device health and providing that information to AAA servers allow them to be put in the correct microsegments. If a device is detected as unhealthy, usually it is kept in a quarantine zone with access to only remediation tools.

- **Check Device Health:** Ensure all devices that access your network have security updates and antivirus software installed.
- **Device Authentication:** Verify that devices are authorized to access the network. If a device is not secure (e.g., using outdated software), block or limit its access.
- **Endpoint Detection and Response (EDR):** Monitor devices in real time to detect and respond to potential threats.

Tools like mobile device management (MDM), Jamf, or Microsoft Intune can help control device security and access their posture. Cisco Secure Client provides a modular approach with VPN, Posture, and zero trust network access (ZTNA) modules for zero trust deployment.

Virtual Private Network (VPN)

A virtual private network is a technology that creates a secure connection over the Internet. Please note that not all VPN types offer encryption and authentication. In the context of this section, our focus is on SSL/IPsec remote access VPN technologies. VPN allows users to send and receive data as if their devices were directly connected to a private network, even when they're using public networks like Wi-Fi in a coffee shop or hotel. This secure connection is made possible by encrypting the data being transferred and masking the user's IP address, ensuring privacy and security. In a zero trust environment, users and devices must be verified before accessing sensitive resources. VPNs help enforce this by requiring users to authenticate themselves before they can establish a connection. This authentication process adds an extra layer of protection, ensuring that only trusted users can connect. However, you will not be able to apply granular controls with the VPN as demanded by the zero trust. You will note that many companies are moving away from VPN-based access and adopting VPNless secure access using SASE/SSE. VPN is used only for the legacy use cases and that can also be toward the SSE module in the cloud rather than the data center. What it means is that users will connect via VPN into the SSE module with a VPN concentrator sitting in the cloud. Once the user is connected via VPN, it has to go through the regular security service chain before it can access any kind of data either from cloud service providers like SaaS applications or anything in the company data center. This is explained in detail in the section "Applying Zero Trust Using SSE."

In summary, traditional VPN connections to the organization's data center allow you to tunnel traffic into the organization, but there is no easy way to apply detailed zero trust checks and policies. Doing so is not impossible, but it does make the design complex. At the time of writing this chapter, the industry is moving toward centralized cloud-based ZTN deployments.

Identifying Business Workflows

At the start of this chapter, we presented an approach to identify and define the trust for users and devices to allow access to different applications using zero trust principles. Now at the time of the deployment, you need to convert them into business workflows. Following are some of the common workflows:

- On-premises employee with a trusted device accessing a private application in the local data center
- On-premises employee with a trusted device accessing a private application in the cloud/SaaS
- On-premises contractor with an untrusted device accessing private applications

- On-premises guests with untrusted access accessing the Internet only
- Remote employees with trusted devices accessing private applications in the data center
- Remote employees with trusted devices accessing applications on SaaS

Applying Zero Trust Using SSE

Secure Access Service Edge (SASE) is a cloud-based security model that merges networking and security services into one platform, integrating features like software-defined wide area network (SD-WAN), firewalls, and identity-based access control. Security Service Edge (SSE), a subset of SASE, focuses on security technologies such as Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB). In a zero trust environment, cloud security is crucial as applications move to the cloud. SASE and SSE offer cloud-native tools like CASB to monitor data use and ensure compliance, verifying security continuously even when accessing services remotely. SASE facilitates secure remote connections without traditional VPNs, providing scalable security. SSE safeguards access to cloud apps regardless of user location and, while initially for cloud use, SSE has become the primary method for implementing zero trust due to its simplicity and flexibility. This topic requires detailed discussion for zero trust deployment by any organization in the current era.

Let's look at the components of SSE before we delve into the details of the deployment strategies. SSE has multiple components such as (but not limited to)

- **Firewall as a Service (FWaaS):** FWaaS delivers firewall functionality via a cloud service, enabling organizations to apply security policies throughout their network, even for remote users. It evaluates and controls traffic flowing between users and applications to thwart threat attacks.
- **Secure Web Gateway (SWG):** SWG safeguards users from web-based threats by filtering out unwanted content, blocking malicious websites, and enforcing acceptable use policies. It also inspects encrypted traffic to ensure that threats aren't concealed within SSL/TLS.
- **Cloud Access Security Broker (CASB):** CASB serves as a security gatekeeper between users and cloud services, implementing security policies, tracking usage, and safeguarding sensitive information in cloud applications.
- **Data Loss Prevention (DLP):** DLP is designed to detect and prevent unauthorized access or sharing of sensitive data. It monitors and controls the movement of sensitive information across the network to ensure it is not leaked or accessed by unauthorized users.
- **Secure DNS:** It helps endpoints from rogue websites. User DNS requests are forwarded to the secure DNS module within the SASE platform, where the URLs are validated against the central database for any vulnerability. Only safe websites are resolved for the users, while URLs hosting malicious content are blocked and the user is notified.

Using SSE, you can deploy zero trust for all common use cases including

- Private application access by the users either on-premises or in the cloud/private cloud
- Secure Internet access
- Legacy VPN-based connectivity to resources both on-premises and in the cloud

As identified in the business workflows, different types of users and device combinations will be used in any organization. Based on the user types, devices can be managed or unmanaged. The SSE architecture typically supports client-based access for managed endpoints and clientless access for unmanaged devices. Cisco Secure Access is an example of SSE that provides secure access to the applications on-premises or in the cloud with zero trust components built in.

Next, let's look at the different use-case types and deployment approaches.

Client-Based ZTNA Deployment for Managed Corporate Devices

For this first scenario, a zero trust access module needs to be installed on an endpoint for client-based secure access. Cisco Secure clients have a specific module for zero trust. Other vendors have similar functionality, either as a standalone zero trust architecture (ZTA) module or integrated into other endpoint software solutions. The primary function of the ZTA module is to intercept and send traffic to the SSE in the cloud based on policies defined by network administrators. This works as follows:

- The user tries to open any application on their device. The ZTA client sitting on the laptop controls the traffic routing and usually also handles functions like device posture. Typically, you define which applications need to be routed via SSE and which traffic needs to be sent directly to the Internet. These policies are defined in the SSE module and pushed to the ZTA client on the device.
- This traffic is intercepted and sent to the SSE in the cloud. The method to send this traffic to the SSE client is based on the vendor implementation. Cisco uses the QUIC protocol to send traffic to SSE per application. SSE providers usually have multiple points of presence (PoPs) across the planet. Traffic is usually sent to the nearest POP using anycast IP address.
- Traffic first hits the authentication module that decides whether the user/device combination is allowed to access that specific application. Based on the policies defined by the network admin, further authorization flows such as MFA and device posture checks are triggered.
- SSE also has policies that define how traffic needs to be routed toward its destination. The application may reside in the company's local data center, served from the public cloud, or it can be an SaaS application like Office 365.

- Once the user is authorized, traffic is then routed to the specific destination because SSE usually has direct connections to the specific data (such as IPsec tunnel to the organization's data center, direct high-speed secure connections to cloud service providers).
- The authentication module may trigger periodic reauthorization based on the trust of the device and application access required based on the policies defined in the SSE module.

In this scenario, users can access the required application from anywhere in the world (or from space, as long they have a connection to the SSE portal) without the need for any VPN client. Their application access experience is consistent and without the need to reconnect the company VPN. This method is also known as *VPNless secure access*. Figure 3-2 shows the client-based zero trust access architecture for a corporate device.

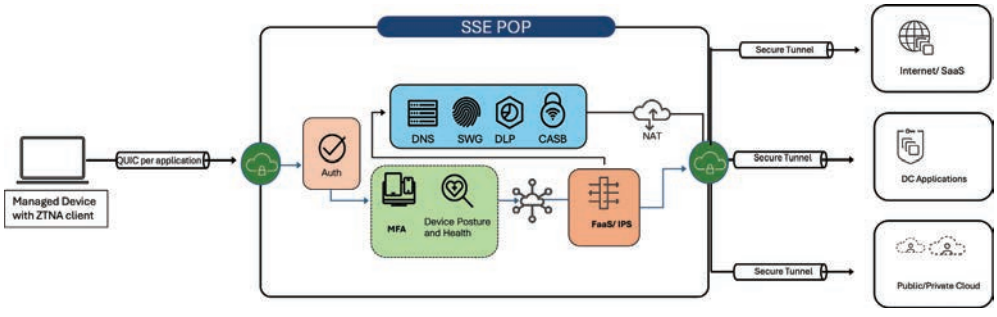


Figure 3-2 *ZTNA Client-Based Access Using SSE*

Clientless ZTNA Deployment for Unmanaged Devices

In the previous example, because the device was managed, it was easy to install the zero trust access module on the client. However, if the user is a partner or guest and the device is not managed, you cannot use the client-based ZTA access methods. In such cases, you need to rely on the browser-based ZTA access. This is also known as *clientless zero trust access*. It works as follows:

1. The user tries to access the application via the browser.
2. Traffic is sent to the SSE via HTTPS tunnels.
3. Based on the authentication and authorization policies, the user is allowed to access a specific set of applications.
4. Traffic is then sent to its destination either in the public cloud, partner data center, or a company data center.

One important difference in this method is that, because there is no ZTA client present on the device posture, information available to the SSE module is limited and based on the browser data only. In such cases, it is recommended to have more restrictive policies.

Even in this case, there is no need for VPN clients. Figure 3-3 shows the browser-based access architecture to specific applications in the data center/private cloud. Notice that service chains specific to Internet/SaaS applications have been removed from this flow.

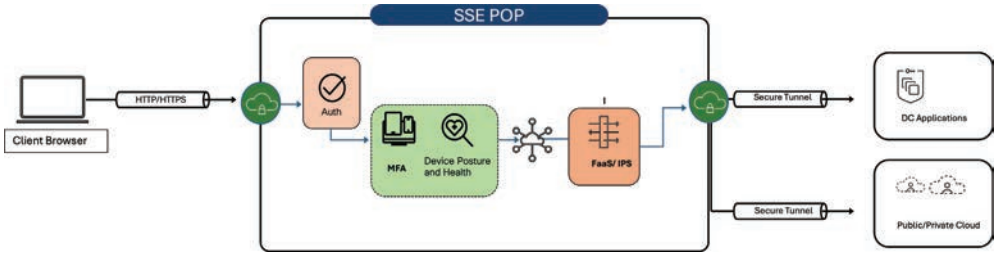


Figure 3-3 *Browser-Based ZTNA*

VPN-Based ZTNA Using SSE

Let's assume that some users require mandatory VPN access. In such cases, you can move your VPN concentrator from the company data center to the SSE cloud. Users will still connect to the SSE via VPN, and from there, security service chains and data policies can remain similar to clientless user access. Figure 3-4 shows the architecture for VPN-based access to private applications only. It is assumed that the Internet/SaaS application could be accessed via split tunneling from the VPN client directly.

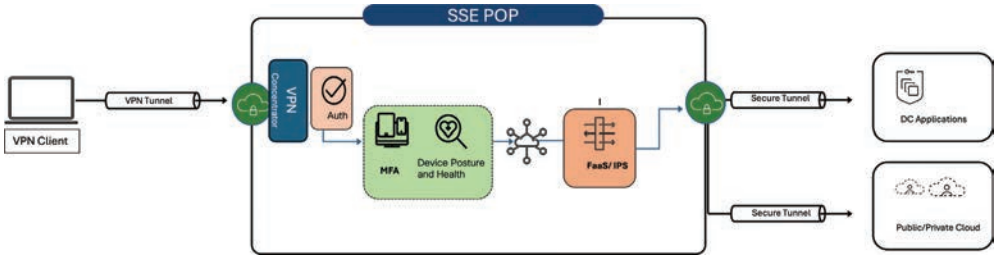


Figure 3-4 *VPN-Based SSE Integration*

SSE Integration for IoT Devices Using SD-WAN

It is not only the users but many devices and IoT devices that need to access their servers via the Internet. You can direct traffic to the SSE in that case also. In such cases, endpoints cannot initiate the tunnels or connections to the SSE POP. Here, technologies like SD-WAN become handy. Assuming that zero trust–based macro- and microsegmentation are already implemented using firewalls, VRFs, and VLANs, traffic from a specific macro- and microsegmentation can then be routed to the SSE using SD-WAN. Most SD-WAN solutions like Cisco SD-WAN can route traffic to a specific destination using a tunneling mechanism based on application type. Cisco SD-WAN calls it *application-aware routing*. You can route traffic toward SaaS applications to SSE and create service

chains specific to SaaS or Internet only. Cisco SD-WAN also supports the auto tunneling capability to Cisco SSE.

Once the traffic hits the SSE, POP traffic can then be passed to Internet/SaaS service providers via security service chains or a NAT module as required. Figure 3-5 shows the users and things traffic via SSE for SaaS application access for users and Internet-only access for things like IoT devices.

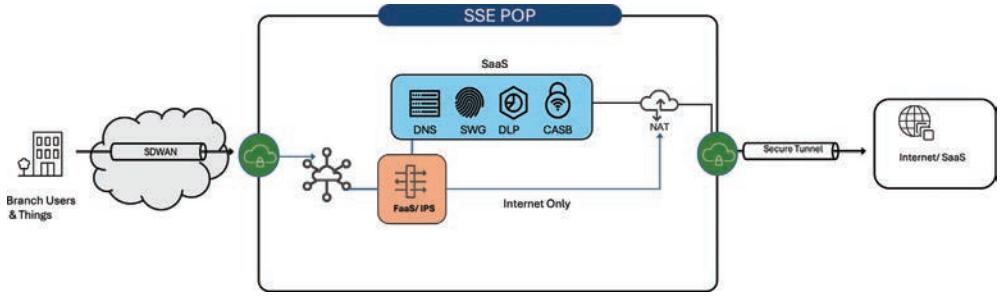


Figure 3-5 *SD-WAN-Based SSE Integration*

ZTNA Deployment Scenarios

Organizations looking to implement zero trust network access (ZTNA) face different challenges depending on whether they have a greenfield or brownfield environment. Greenfield deployments refer to starting from scratch with no existing infrastructure, allowing for a clean, streamlined implementation of ZTNA principles. In contrast, brownfield deployments involve integrating ZTNA into existing, often complex, infrastructures, which requires careful planning to avoid disrupting current operations. Both approaches come with unique considerations, from resource allocation to compatibility with legacy systems, shaping how zero trust principles are applied. In this section, we will look at the high-level strategy for both greenfield and brownfield scenarios.

Greenfield ZTNA Deployment

In a greenfield ZTN, you can build all infrastructure with a zero trust mindset from the start. This allows for a cleaner and simpler implementation, eliminating the need to manage outdated systems.

In the context of deploying zero trust in a greenfield environment, you can take the following steps based on the strategic steps included earlier:

1. Define the zero trust objective:
   - Formulate a distinct vision for the objectives of zero trust within the organization, such as strengthening security, ensuring better compliance, or gaining improved control over the network access.

- Make sure the zero trust deployment is in sync with overall business goals and strategies. This ensures a strong case for investments and secures executive support.
- Secure support from senior leadership to guarantee that the initiative receives essential resources and strategic backing import.

2. Define a roadmap:
   - Develop a comprehensive roadmap for implementing zero trust. It must outline milestones, timelines, and essential deliverables. Divide the deployment into manageable phases for organized execution implementation.
   - Establish the budget needed for deployment, factoring in expenses for technology, personnel, and training. Distribute resources appropriately to facilitate each phase of the project deployment.
3. Develop the architecture and design:
   - Develop a high-level architecture that outlines the application of zero trust principles across the organization. This framework should encompass network segmentation, identity management, and access controls.
   - Design the network layout while considering zero trust principles. Ensure segmentation by establishing zones for various types of assets and data.
   - Plan for microsegmentation to limit lateral movement within the network. Define security boundaries for different workloads and services.
4. Deploy:
   - Establish strong IAM systems for overseeing user identities, devices, and applications. Implement multifactor authentication to enhance access security controls.
   - Create granular access policies based on user roles, device types, and the sensitivity of the resources they are accessing.
   - Implement next-generation firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), and secure access gateways.
   - Deploy endpoint protection solutions that include antimalware, encryption, and device management.
   - Ensure that applications are securely developed and deployed. Use application firewalls and secure coding practices.
   - Configure access controls to enforce the principle of least privilege. Use tools to continuously evaluate and enforce access policies.
   - Ensure all data in transit and at rest is encrypted. Use strong encryption protocols and key management practices.
   - Set up comprehensive logging and monitoring to track access, detect anomalies, and respond to security incidents.

5. Validate and train:
   - Test access policies to ensure they correctly enforce zero trust principles and do not inadvertently allow unauthorized access.
   - Develop clear documentation and guidelines for users and administrators on zero trust practices and policies.
6. Adapt and update:
   - Regularly update security controls and policies to address emerging threats and changes in the organizational environment.

By following these steps, organizations can effectively deploy zero trust in a greenfield environment, ensuring a secure and adaptive access control framework from the outset.

Brownfield ZTNA Deployment

In a brownfield environment, you deal with established systems, networks, and infrastructure that have been in place for a while. These systems may be outdated and were probably designed without zero trust principles. As a result, there may be existing security vulnerabilities, implicit trust models, or legacy technologies that present challenges for securing them. When you're implementing zero trust in a brownfield, it's essential to thoroughly assess and adjust the current setup while minimizing disruptions to ongoing operations. The aim is to gradually transition to zero trust, identify weaknesses, and bolster security while ensuring smooth operation. Brownfield settings typically require more phased and adaptable strategies to prevent business interruptions, whereas greenfield environments enable quicker and more seamless zero trust integration since they don't require working around existing infrastructure setups.

You can start with the following steps to define your approach to adopt zero trust in brownfield environment.

1. Define objectives and business needs:
   - Assess the organization's security goals and what assets are most critical.
   - Conduct a comprehensive assessment of the current security landscape, including existing access controls, user privileges, and device management.
   - Identify where zero trust is most needed; start with high-risk areas such as critical data or sensitive applications.
   - Define the scope of the zero trust implementation, identifying critical applications, sensitive data, and high-risk areas that require immediate attention.
2. Outline the current infrastructure:
   - Conduct a thorough audit of the current network, devices, and user access points.
   - Identify gaps where security is lacking or where implicit trust exists that needs to be eliminated.
   - Inventory all applications, devices, and users to understand the current access state and any potential issues vulnerabilities.

3. Establish user and device trust:
   - Start by establishing a baseline level of trust for all users and devices, regardless of their current access privileges.
   - Deploy multifactor authentication to strengthen user identity verification.
   - Implement device posture checks to ensure that all devices are secured and compliant before access is granted.
4. Segment the network:
   - Assess whether legacy applications can be segmented or modernized to reduce security risks and enhance overall security posture within the brownfield environment.
   - Apply microsegmentation to limit access to sensitive resources. Each user or device gets access only to the resources they specifically need.
5. Implement adaptive policies:
   - Develop dynamic policies that can adapt based on real-time user behavior, device status, or location.
   - Implement measures to enhance device visibility within the brownfield environment to improve security and reduce risks associated with legacy technologies.
6. Begin with small steps, then scale:
   - Start by applying zero trust principles to a single department or system.
   - Test the framework, gather feedback, and expand gradually across the organization.
7. Continuously monitor and improve:
   - Use security monitoring tools like SIEM to detect anomalies.
   - Regularly review and adjust access controls, policies, and system configurations.
   - Continuously iterate on the zero trust implementation, incorporating feedback, insights, and lessons learned to improve security posture over time.

Summary

In this chapter, you learned about the approach for zero trust deployment by first defining the strategy for user and device trust, and application access policies, and then you learned methods for deploying those policies. You also learned about common tools and technologies, including the SSE approach to adopting zero trust. Lastly, you looked at greenfield and brownfield approaches to zero trust deployment.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z