# The Journey to Zero Trust

## Microsegmentation in Zero Trust Part One: Introduction and Planning

Version: 1.0

Publication: July 29, 2025

Cybersecurity and Infrastructure Security Agency

# REVISION HISTORY

| Version | Summary of revisions | Date |
|---|---|---|
| 1.0 | Initial Release – All Pages | July 29, 2025 |

# PREFACE

*The Journey to Zero Trust* series covers cybersecurity capabilities and architecture supporting organization adoption of modern zero trust (ZT) principles. ZT's core concept of never trust and always verify evolved from prior cybersecurity models. This current ZT series supports an organization's ZT journey and supplements other resources.

> "Implementing a ZTA is a journey rather than a wholesale replacement of infrastructure or processes. An organization should seek to incrementally implement zero trust principles, process changes, and technology solutions that protect its highest value data assets."[1]

Microsegmentation is a networking control that limits connections to a zone or segment. Traditionally, organizations accomplished networking control using Internet Protocol (IP) address ranges, virtual local area networks (VLANs) and devices or services that can accept or reject the connections based on static rules. In this context, microsegments are simply smaller zones or address ranges possessing more granular, manually created and managed access rules. This approach is typically accomplished in static rules and routing applied to network devices, virtualized networking or perimeter defense equipment, such as firewalls, routers and switches.

This document provides background, references and initial planning guidance that apply the principles from traditional network microsegmentation to the challenges associated with zero trust architectures (ZTAs) and dynamic policy enforcement. In the context of dynamic policy enforcement and ZT, microsegmentation is more than a network discussion or capability. It includes not only the current, state of the art network capabilities and controls but also capabilities implemented in hosts or other workflow-aware policy enforcement mechanisms, commonly called policy enforcement points (PEPs).[2] This is an evolving set of capabilities that can be applied at the host, application, database, operating system, virtualization platform or in dedicated devices to accomplish the objectives of microsegmentation for ZT. When applying microsegmentation in ZT at the PEPs, the parameters for the access rules move beyond IP addresses and include contextual information about the connection.[3] This additional contextual information is referred to as attributes[4] and can include a wide range of information to support the dynamic policy decisions for both initial access and continued access.

[1] National Institute of Standards and Technology, U.S. Department of Commerce, "Zero Trust Architecture - NIST Technical Series Publications," Zero Trust Architecture, Section 7, August 2020, https://doi.org/10.6028/NIST.SP.800-207.

[2] National Institute of Standards and Technology, U.S. Department of Commerce, "Zero Trust Architecture - NIST Technical Series Publications," Zero Trust Architecture, Section 7, August 2020, https://doi.org/10.6028/NIST.SP.800-207.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "Guide to a Secure Enterprise Network Landscape," Computer Security Resource Center, November 17, 2022, https://doi.org/10.6028/NIST.SP.800-215.

[4] National Institute of Standards and Technology, U.S. Department of Commerce, "Zero Trust Architecture - NIST Technical Series Publications," Zero Trust Architecture, Section Sections 2.1-4, 3.3, 6.3, August 2020, https://doi.org/10.6028/NIST.SP.800-207.

# CONTENTS

# 1. INTRODUCTION

## 1.1 EXECUTIVE SUMMARY

Traditional perimeter-focused architecture is no longer effective in protecting enterprise resources from cyber intrusions and compromise. Microsegmentation works by protecting a smaller group of resources, thereby reducing the attack surface, limiting lateral movement and increasing visibility for better monitoring of the microsegmented environment. Microsegmentation does not replace defense-in-depth and the proper management of data, assets, configuration and vulnerabilities through various controls and cybersecurity tools. Rather, microsegmentation augments the organization's ability to apply targeted risk- and threat-appropriate protections when it is used in conjunction with existing capabilities.

Adoption of this cultural and technical shift in system security and architecture depends on organizational leadership. The *Journey to Zero Trust* provides leaders with a high-level overview of microsegmentation concepts and a phased implementation approach. While this document has specific federal civilian executive branch (FCEB) references, any organization can apply the information provided to modernize its network and move toward zero trust architecture.

Microsegmentation can be applied to any technology environment, such as information technology (IT), operational technology (OT), industrial control system (ICS), internet of things (IoT), as well as any implementation model, including cloud, on premise and hybrid. Microsegmentation enables applying risk- and threat-appropriate protections and visibility capabilities for the specific system(s) or data within the microsegment. Microsegmentation can significantly enhance the security of systems and data and helps reduce the blast area that a compromised resource can impact.

When implemented as part of ZTAs, microsegmentation solutions utilize additional characteristics at the time of access to protect target resources instead of relying on implicit trust based on network location. PEPs use these characteristics to authorize initial access and validate that continued access remains necessary and authorized while the connection to the resource exists. The Cybersecurity and Infrastructure Security Agency (CISA) addresses microsegmentation in the Zero Trust Maturity Model (ZTMM) within the network pillar.[5]

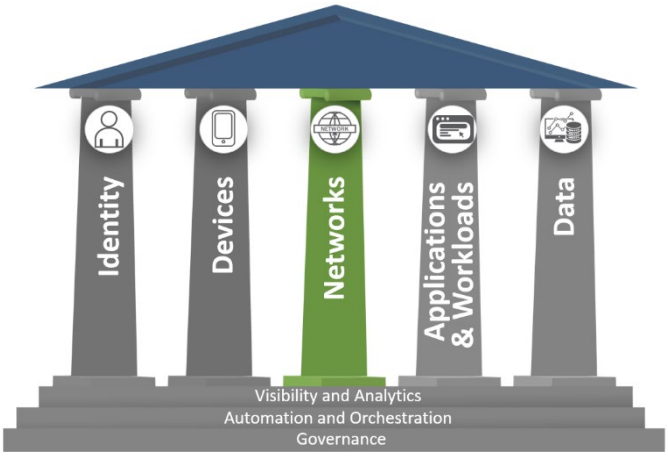


***Figure 1: ZTMM - Network***

[5] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model Version 2.0," Zero Trust Maturity Model Version 2.0, Section 4 and ZTMM pillars, April 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

In the context of this document, microsegmentation is more than network segmentation. The solutions used to implement microsegmentation span multiple technical capabilities and are implemented in multiple layers of the Open Systems Interconnection (OSI) model.[6]

Transitioning an organization from existing traditional segmentation, which relied on large-scale perimeters with limited technical capabilities, to fine-tuned microsegmentation requires a paradigm shift that leaders must champion. Successful adoption of microsegmentation will improve enterprise cybersecurity and availability.

This document focuses on concepts, challenges and benefits of moving to microsegmentation and recommends high-level actions for successful adoption of this architectural initiative in support of advancing ZT. Referenced federal guidelines and acronyms are listed in Appendix A and Appendix B respectively.

A subsequent technical guide will be produced for technical leaders and implementation teams. This technical guide will provide implementation scenarios to illustrate the technical considerations, recommendations, and challenges of this transition.

## 1.2 BACKGROUND

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" (May 12, 2021)[7] instructed agencies to adopt ZT cybersecurity principles and adjust their network architectures accordingly. To support this effort, CISA developed a ZTMM[8] for agency use as they implement ZTAs. This maturity model lists five technology pillars. Over time, organizations can progress through each pillar to secure systems, applications, data and assets toward a ZTA.

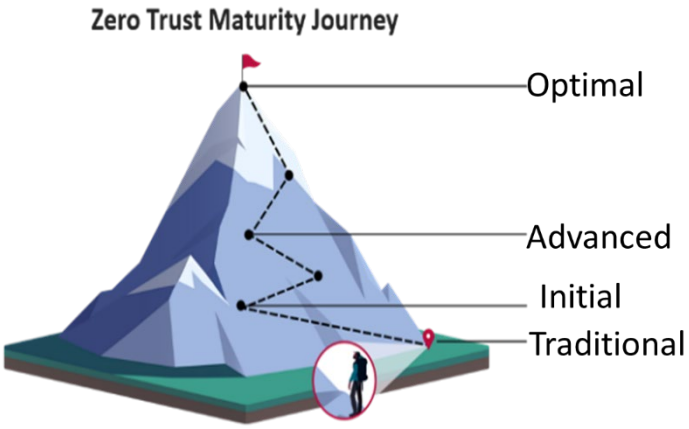


***Figure 2: Zero Trust Maturity Journey***

The ZT journey never ends, evolving with advancing technologies. While an organization's goal may be to reach the ZT maturity journey summit and operate optimally for all components, as shown in Figure 2 (right), the reality is that an organization will need to continuously evaluate its ZT needs to maintain its ZTAs, to address current and anticipated threats and to align to its identified threats and risk tolerances.

[6] International Organization for Standardization/International Electrotechnical Commission, "Information technology–Open Systems Interconnection–Basic Reference Model, 7498-1:1994," June 1, 1996, https://www.iso.org/standard/20269.html.

[7] International Organization for Standardization/International Electrotechnical Commission, "Information technology–Open Systems Interconnection–Basic Reference Model, 7498-1:1994," June 1, 1996, https://www.iso.org/standard/20269.html.

[8] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model Version 2.0," Zero Trust Maturity Model Version 2.0, Section 4 and ZTMM pillars, April 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

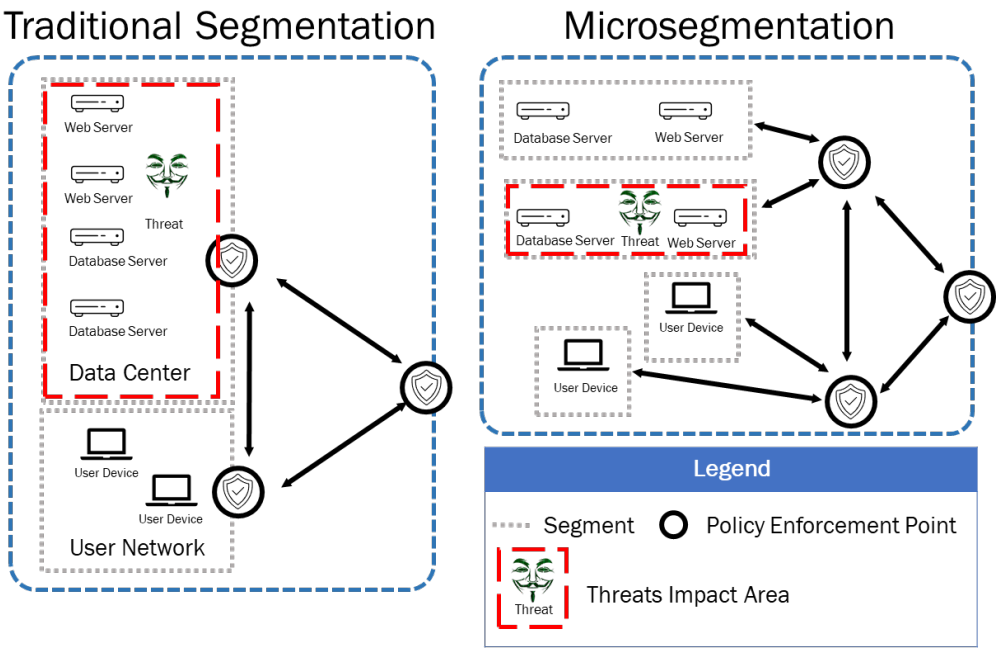


***Figure 3: Threat Impacts and Segmentation***

On Jan. 26, 2022, the Office of Management and Budget (OMB) released Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,"[9] in support of EO 14028, "Improving the Nation's Cybersecurity" to align and base civilian agencies' enterprise security architecture with ZT principles.[10] The memorandum requires agencies to transition to a ZTA structure. In support of this requirement from OMB, CISA updated the ZTMM to version 2. The ZTMM defined key security functions that comprise ZTAs and lays a framework for breaking down functional implementation into manageable increments with increasing levels of rigor.

ZT's design philosophy focused on removing implicit trust (allow by default) and replacing it with explicit verification (deny by default), including access authentication and authorization. Rather than structuring defenses around perimeters and hoping to prevent security breaches; ZT architecture presumes that breaches will occur, networks are already compromised, and the design must minimize the damage of current and future breaches.

M-22-09 requires agencies to "meaningfully isolate environments, so that an adversary that compromises one application or component cannot easily move laterally within an organization and compromise other distinct environments."[11] In line with this, the ZTMM focuses on transitioning networks from a traditional approach for

[9] Office of Management and Budget, "M-22-09 Federal Zero Trust Strategy," Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[10] Executive Office of the President, "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

[11] Office of Management and Budget, "M-22-09 Federal Zero Trust Strategy," Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

network boundaries to one that focuses on segmenting organization networks granularly. As illustrated in Figure 3 (on previous page), microsegmentation limits opportunities for threats to exploit network-adjacent systems and data through vulnerabilities or other weaknesses. As a result, the microsegment limits the impact to an organization if it is exploited.

Historically focused on the organization's boundary with the internet, CISA updated its Trusted Internet Connections (TIC) program to support modern network architectures (refer to *TIC 3.0 Program Guidebook*).[12] Microsegmentation is defined as a TIC security capability in the network security group: "Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data." Microsegmentation is critical as organizations move away from traditional, perimeter-focused architectures (TIC 2.0) and adopt architectures based on microperimeters as part of efforts to modernize security and performance, including those outlined in TIC 3.0 use cases, such as the TIC 3.0 Cloud Use Case.

The TIC Reference Architecture Section 4.3 describes trust zones and levels of trust associated with them.[13] "A single element or group of elements with shared security capability protections constitute a trust zone." These zones are based on network location and can be defined internal or external to the organization perimeter. As described, this trust zone and trust level concept also permits a more fine-grained approach (e.g., aligning with the concepts of ZT), depending on how an organization might best understand and describe their environment. A trust zone does not necessarily inherit trust and security from an adjacent trust zone, nor do the trust and the subsequent security capabilities depend on the trust of the adjacent zone. Levels of trust may also factor into deployment options for services or data. By deploying security capabilities and ensuring a rigor of implementation commensurate with the level of trust designated to a zone, an agency may use the increased assurance as an opportunity to deploy services or more sensitive data to the zone.

Using microsegmentation to support ZTAs builds upon this approach. Organizations moving to ZT should work from the assumption that all communications are potentially malicious until proven proper and authorized. ZTA's core concept of "Never trust always verify"[14] can work in conjunction with the concept of trust zones and levels of trust though PEPs.

[12] Cybersecurity and Infrastructure Security Agency, "CISA TIC 3.0 Program Guidebook v1.1," Cybersecurity Incident & Vulnerability Response Playbooks, November 2021, https://www.cisa.gov/sites/default/files/publications/CISA%2520TIC%25203.0%2520Program%2520Guidebook%2520v1.1.pdf.

[13] Cybersecurity and Infrastructure Security Agency, "CISA TIC 3.0 Program Guidebook v1.1," Cybersecurity Incident & Vulnerability Response Playbooks, November 2021, https://www.cisa.gov/sites/default/files/publications/CISA%2520TIC%25203.0%2520Program%2520Guidebook%2520v1.1.pdf.

[14] Alper Kerman, "Zero Trust Cybersecurity: 'Never Trust, Always Verify,'" National Institute of Standards and Technology: Taking Measure: Just a standard blog, April 26, 2024, https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.

Beyond the alignment with ZT principles, microsegmentation provides additional benefits, including the following:

- Reducing the surface for lateral movement of adversaries that have breached networks
- Improving containment for malware, malicious code, bugs, misconfigured systems and insider threats
- Improving the visibility into networks and systems
- Improving opportunities for policy enforcement, enabling fine-grained policies to address resource-specific risk-tolerance and protection needs
- Improving support for targeted mitigations, including specific vulnerabilities or exploits and special classes of resource

# 2. WHAT IS SEGMENTATION?

### Introduction

As a physical or virtual architectural approach, network segmentation divides a network into multiple distinct pieces, called segments. These segments typically group related resources, such as infrastructure, applications, data or services. Each segment acts as its own network or subnetwork providing additional security and control. Segmentation is used to limit access to devices, data and applications and restrict communications between networks. In ZTA, PEPs at the segment boundaries govern access to the segment's resources as part of the policy decision function. The PEP can be used to isolate, validate and monitor the traffic entering or exiting these segments. Segmentation can be implemented in the physical infrastructure through logical capabilities, in the operating systems or in applications themselves. A key consideration when choosing how to implement segmentation is understanding how it can be bypassed by an adversary, so that the bypass method can be monitored if not completely blocked.

## 2.1 KEY CONCEPTS

The transition to ZT in general, and the implementation of microsegmentation in particular, represents a significant shift in technology, policy and security culture. As such, success must include extensive cybersecurity and IT technical staff support and effective communication throughout the entire organization. All impacted teams should understand the key concepts behind this transition and the terms utilized to describe the activities and expected outcomes.

**Macrosegmentation:** Traditional network management is based on macrosegmentation of the private (internal) network space. As a network segmentation strategy, macrosegmentation divides a network into multiple discrete chunks that support various business needs. Common use cases for macrosegments include the isolation of development and production environments, demilitarized zones (DMZ), enhanced visibility and control, user segmentation and application segmentation. In summary, macrosegmentation provides high-level control over traffic moving between different areas of an organization's network, ensuring better security, isolation and visibility.

**Microsegmentation:** Microsegmentation builds upon the concept of macrosegmentation of the private (internal) network space. It further divides these business needs-based boundaries or perimeters and extends them from the private internal network space to all networks internal and external that support business needs. These microsegments can be dynamically or statically defined and utilize more than traditional network layer controls and capabilities for enforcement and monitoring.

**Trust Zones:** Traditional networks use "trust zones," which most frequently manifest explicitly in firewall configuration. Some interfaces on a firewall are connected to "trusted" zones while other zones are "untrusted." Some entities may further enhance this concept by introducing various degrees of trust; these degrees of trust may be identified with different terms. Frequently, a management network occupies a particularly trusted position and is ideally subject to stringent controls and monitoring.

As the term "zero trust" might suggest, the concept of associating trust with network location (zones) needs updating. Utilizing the existing trust zones and capabilities is still valid in a solution architecture; however, with microsegmentation in support of ZT, microsegments should be implemented with risk, visibility or control in mind. Although the traditional trust zones will continue to exist in support of general network segmentation, they will not always be closely related to microsegments that enhance traditional network perimeters. In other words, microsegments may subdivide or cross former trust zones. Microsegment zones utilize more than traditional network capabilities in their design and implementation.

**Policy-Controlled Access:** Dynamic access control though policy utilizes a PEP and an associated Policy Decision Point (PDP) to make the access decisions for protected resources and network segments. Decisions can utilize information from a variety of sources, including from traditional network access control solutions. Typically, the Policy Engine (PE) includes identity information, device information, connection metadata and authorization rules that are integrated in the PDP to make the access determination. This access decision is relayed to the PEP though an appropriate control plane. The PEP acts, utilizing this determination to enforce the decision to grant or deny access to the protected resource. This process flow is illustrated below in Figure 4: Policy-Controlled Access (next page). The data sources utilized to make the access decisions are defined in the policy rules. Policy-controlled access is essential to optimal ZT maturity as defined in the ZTMM. The policy rules used in the access decisions align with organizational risk tolerance and threats to the protected resource. PEPs can operate at any layer of the OSI model and may be on endpoints or devices utilized in the network or system. PDPs may support multiple PEPs as determined by architecture design and organizational requirements. Multiple PEPs may be involved in an access enforcement decision.

**Surface Management:** Historically, attack surface has been an important security modeling consideration. The concept is simple: Attack surface is the portion of an organization's resources accessible to an adversary, However, attack surface is difficult to accurately document in a complex enterprise environment using macrosegmentation. Macrosegmentation is simpler to manage than Microsegmentation but lacks the granular control necessary to address modern threats.

Microsegmentation reduces the attack surface into more manageable components. Each segment can be thought of as having its own attack surface; then, since segments exist to protect resources, each segment can be thought of as a "protect surface." These protect surfaces are more manageable as they cover smaller, more well-defined portions of the overall organizational enterprise. In turn, such surfaces support more appropriate and effective protection policies that focus on the risks and threats to resources and activities performed within those protect surfaces.

**Policy-Controlled Access:** Modern network design emphasizes enabling and using policy to dynamically control access to resources. In an example scenario, Figure 4 illustrates the major components of policy-controlled access and how this dynamic decision process occurs.

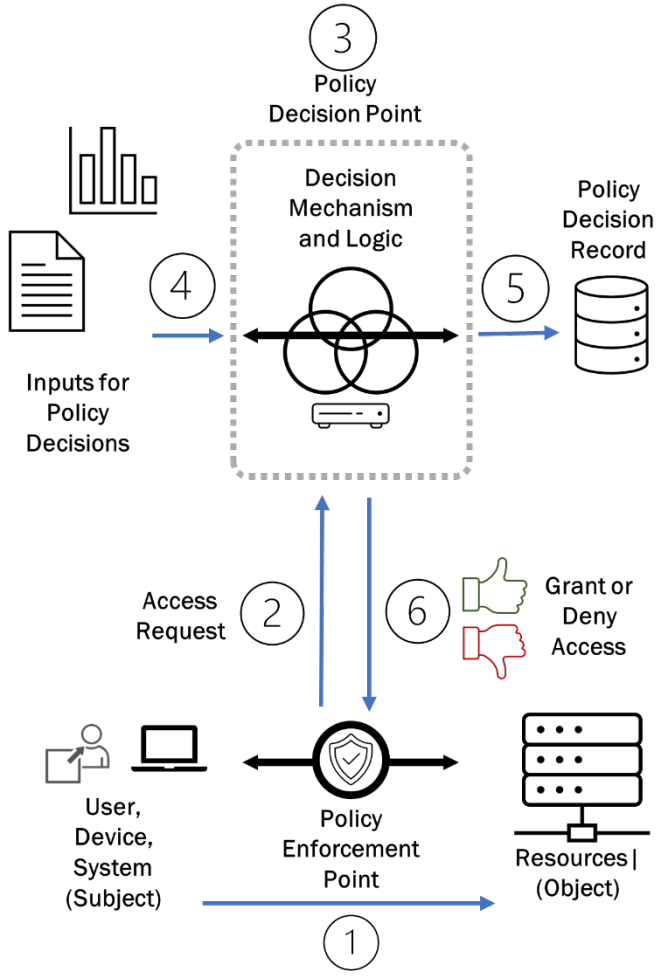


*Figure 4: Policy-Controlled Access*

1. The user (Subject) requests access to a protected resource (Object) through PEP.
2. The PEP communicates with the PDP, requesting an access decision. This request includes information about the user and can include many other attributes, such as device information and connection characteristics.
3. The PDP utilizes established policy rules to make the access decision. This may include querying other data sources.
4. Based on policy rules utilized by the decision logic, multiple input data sources can be utilized by the PDP, including device health, user training status, threat intelligence and logs.
5. An access decision based on the policy is recorded and passed along to the PEP(s) for action.
6. The PEP grants or denies access and directs the subject connection accordingly to the object.

While these concepts are not exclusive to microsegmentation or ZT, they enable the automated, dynamic and conditional access decisions needed to fully realize the benefits of microsegmentation and ZTAs. These conditional access decisions can include a variety of user and connecting device attributes and connection characteristics. A user connecting to a resource from a known organizational device during normal business hours may have different access capabilities than if the same user connects after hours from an unknown device located in a foreign country. This ability to conditionally determine initial access rights and privileges automatically coupled with periodically validating the continued access need during a session significantly improves the security of resources and reduces risk to the organization and its assets.

**TIC and Microsegmentation:** The TIC program within the federal government describes required capabilities and architectures to improve the security and visibility of connections to and from agencies.[15] Non-federal organizations may apply the principles and design concepts from the documents and artifacts by looking at intended outcomes of the capabilities and architectures and mapping them to organization-specific requirements and risk management. Note that TIC 3.0 evolved the perimeter architecture of TIC 2.0, improving the protection and visibility capabilities and documenting how to meet the intent of the program.

Figure 5 (below) illustrates the evolution of TIC from the organization perimeter (macrosegmentation) toward smaller trust zones (microsegmentation) and PEPs. The changes enhanced the TIC program support for cloud

[15] Cybersecurity and Infrastructure Security Agency, "Trusted Internet Connections (TIC): CISA," Cybersecurity and Infrastructure Security Agency CISA, accessed January 13, 2025, https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic.

computing, mobile and remote users through the addition of specific use cases in the documentation. As this move occurred, trust zones also evolved from being network location specific to attribute based, enabling the migration of organizations to ZTA.

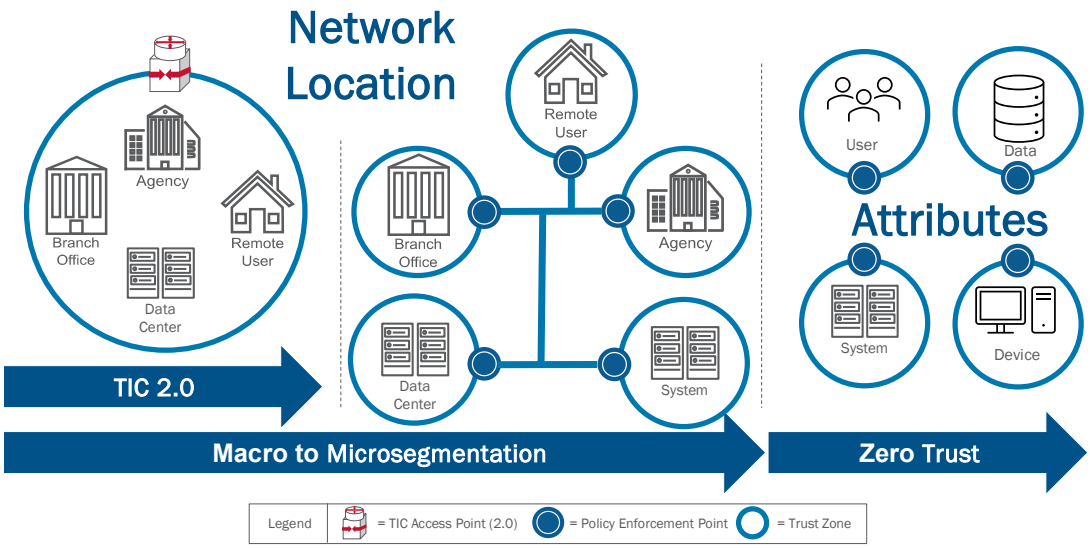


***Figure 5: Evolution of TIC***

**Traditional Network Segmentation**

Traditional networks often build around coarse-grained network segments that closely reflect the physical network layout and support specific business needs or functions. The security protections in these architectures often focus on perimeter protection between the organization's internal network and other networks such as the internet. In these scenarios, a compromised endpoint becomes an attacker's jumping-off point for discovery and lateral movement throughout the environment. Figure 6 (right) shows an example of such a network. The segments depicted are examples, and there may be others such as development, scientific, research, backup and administration under macrosegmentation.

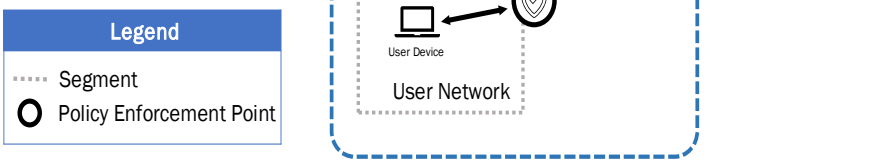





***Figure 6: Traditional Network Segmentation***

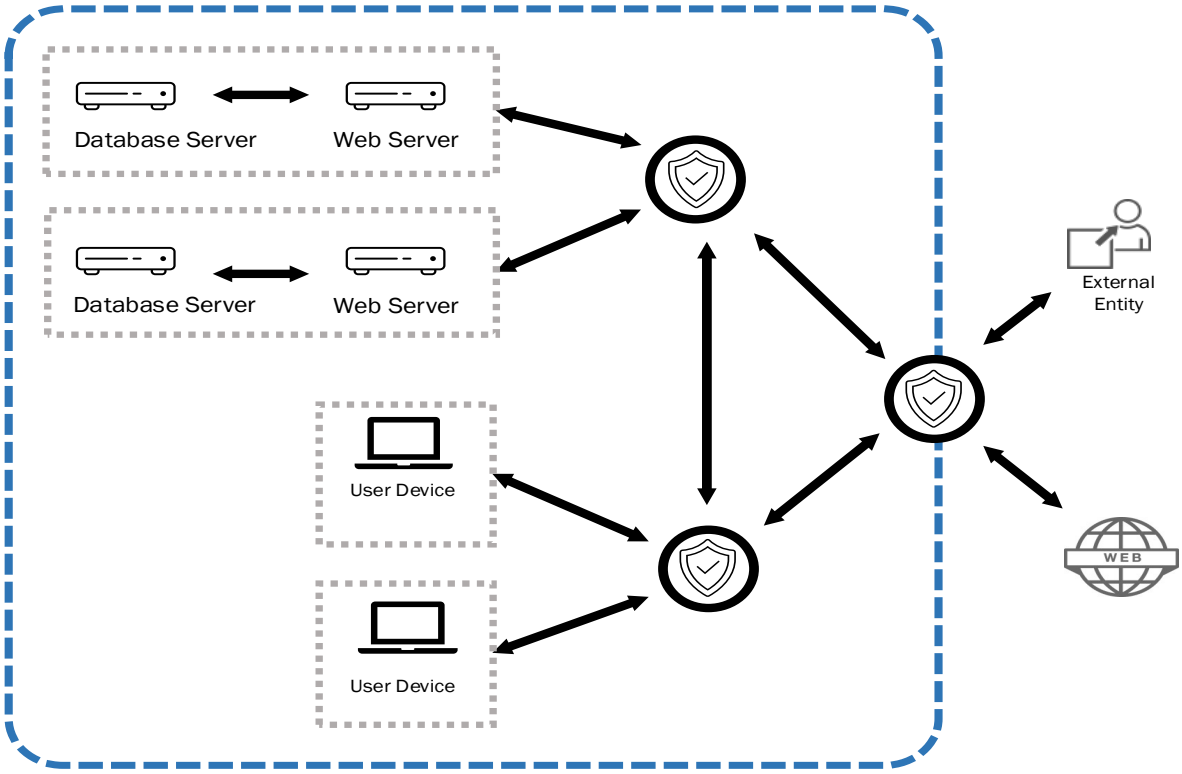


*Figure 7: Microsegmentation*

### Microsegmentation

Microsegmentation is a design philosophy focused on minimizing the size of network segments to increase the opportunities for discovery and limit lateral movement from a compromised endpoint, as illustrated in Figure 3.[16] For example, a traditional network might place all servers in its datacenter into a single network segment, making them potentially accessible by any compromised organization endpoint. Using a microsegmentation approach, as depicted in Figure 7 (above), the organization might create segments so servers can only communicate with other servers needed to perform their business function, thereby limiting the opportunities for lateral movement.

More advanced microsegmentation implementations might enhance network segmentation through greater integration with application workflows, creating logical network segments based on those application workflows instead of the physical network layout. See an example of this more advanced approach in Figure 8 (next page). In the context of ZTA, microsegmentation works in tandem with other policy control mechanisms to enable more in-depth authorization policies. Under such a model, the exact boundary of a microsegment may change from moment to moment as the microsegment may include dynamic system components and access needs in real time. These dynamic components and variable access needs should be governed by policies enforced by PEPs.

[16] Nanosegmentation is sometimes used in lieu of microsegmentation to place greater emphasis on minimizing the size of the network segments.

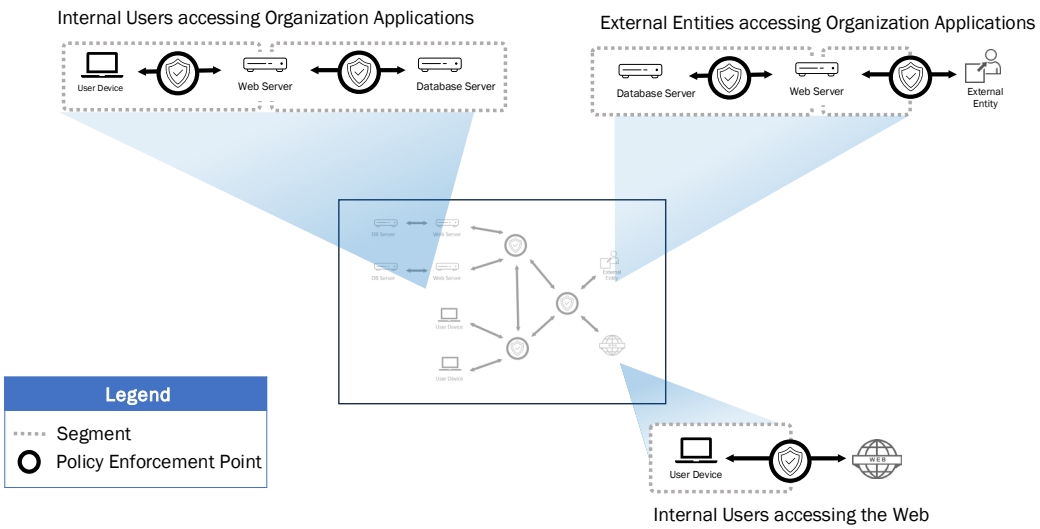


***Figure 8: Workflow-Based Microsegmentation***

## 2.2 SEGMENTATION TYPES

Given the variety of environments that may comprise an organization's enterprise architecture, it may not be feasible or advisable to use a single solution to implement microsegmentation throughout the enterprise. For most enterprise architectures, organizations will need to combine multiple microsegmentation capabilities, potentially through a combination of preexisting capabilities and one or more vendor products, applying each where appropriate to align with the identified use cases, needs and objectives. Organizations will need to understand the available options and how best to apply them in their environment.

Organizations should research available solution types and plan for an implementation that meets their mission needs.

The following table provides a high-level overview of commonly available segmentation types. While these are distinct high-level types, vendor solutions may comprise multiple types:

*Table 1: Segmentation Types and Features*

| Type | Description |
|---|---|
| Network | Network-based devices and appliances enforce segmentation policy on network traffic routed through the device.<br>**Overview**<br>• Can potentially allow for easier transition through familiarity and reuse existing network infrastructure<br>• Can support situations where legacy infrastructure does not support microsegmentation<br>• Can be difficult to fully transition and maintain the environment to microsegmentation<br>• May have more limited visibility into endpoints, identities and application workflows<br>**Applicability**<br>• On-premises environments<br>• Infrastructure as a Service (IaaS)/Platform as a Service (PaaS) cloud deployments<br>**Examples**<br>• Routers<br>• Software-defined Wide Area Network (SD-WAN)<br>• Next Generation Firewall<br>• Web Application Firewall (WAF) |
| Endpoint | Capabilities deployed on hosts or other devices enforce segmentation policy for the endpoint.<br>**Overview**<br>• Can potentially support better integration with application workflows, identities and endpoints.<br>• Can typically work independent of endpoint location, supporting itinerant and remote endpoints<br>• Requires deployment of agent to every endpoint, which can require additional maintenance and may not work with appliances, IoT, OT or legacy infrastructure<br>**Applicability**<br>• On-premises and remote user devices<br>• Servers<br>• IaaS cloud deployments<br>**Examples**<br>• Secure Access Service Edge (SASE) agent<br>• Host-based firewall |
| Container | A method for packaging and securely running an application within an application virtualization environment. These capabilities enforce segmentation policies for container deployments.[17]<br>**Overview**<br>• Can potentially be easily integrated with continuous integration/continuous delivery (CI/CD) deployment models<br>• Can potentially work with existing container deployments<br>• Solutions can be specific to a given container orchestration framework, limiting portability<br>**Applicability**<br>• Container deployments |

[17] National Institute of Standards and Technology, "Application Container Security Guide NIST SP 800-190," Computer Security Resource Center, September 2017, https://doi.org/10.6028/NIST.SP.800-190.

| Type | Description |
|---|---|
| Container (Cont.) | **Examples**<br>• Container orchestration framework segmentation<br>• Service mesh |
| Hypervisor | Capabilities deployed to endpoints that host virtual machines to enforce segmentation policies for deployed virtual machines<br>**Overview**<br>• Can potentially work in existing virtual machine (VM) deployments<br>• Similar to well-understood network-based segmentation<br>• Solutions can be specific to a given hypervisor, limiting portability<br>**Applicability**<br>• VM deployments where the organization manages the hardware on which the VMs are deployed |
| Cloud | Cloud-native capabilities enforce segmentation policies for cloud-deployed infrastructure.<br>**Overview**<br>• Potential for strong integration with application workflows, identities and cloud-deployed resources<br>• Solutions can be specific to a given cloud-vendor, limiting portability.<br>**Applicability**<br>• Cloud service deployments<br>**Examples**<br>• Cloud native<br>• Cloud Workload Protection Platform (CWPP)<br>• Cloud Security Posture Management (CSPM)<br>• Cloud-Native Application Protection Platform (CNAPP) |

# 3. PHASED APPROACH

### Introduction

In alignment with National Institute of Standards and Technology (NIST) Planning for a Zero Trust Architecture,[18] organizations should assess their current enterprise systems, resources, infrastructure, personnel and processes before investing in ZT capabilities. Given the complexity involved in transitioning an existing organizational enterprise from traditional network segmentation to a microsegmentation approach, organizations should use a phased approach, transitioning portions of their enterprise over time. This document provides a high-level approach that can help inform an organization's approach; however, each organization needs to determine the approach that best meets its needs.

Organizations should plan for a phased approach, transitioning portions of overall enterprise to microsegmentation over time, to ensure a smoother and easier transition.

[18] National Institute of Standards and Technology, "Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators," Computer Security Resource Center, May 6, 2022, https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final.

As an example, an organization might segment a single application, workflow, asset or environment at a time, prioritizing based on various organization-specific criteria (e.g., criticality, ease of transition), and iteratively segmenting their enterprise over time. The phases outlined below are not one-time tasks and would need to be repeated by the organization during the transition. These can be repeated while legacy segmentation approaches remain in use, as well as where more advanced segmentation has been adopted. Through iteration, the organization gains experience and insight into where changes to organization applications or environments, the technology landscape, threats or attacker techniques necessitate updates. This knowledge can improve already-deployed microsegments.

This document uses the term candidate resource to refer to any group of systems, services, components and data considered for microsegmentation. By grouping these resources, an organization can identify the potential and appropriate microsegmentation options to meet the security objectives.

## 3.1 PHASE 1: IDENTIFY CANDIDATE RESOURCES FOR SEGMENTATION

The organization goes through its applications, workflows, data, assets and environments to identify potential candidate resources for transition to microsegmentation. The organization uses organization-specific criteria (e.g., criticality, security, ease of transition) to prioritize among the candidates. For example, during initial microsegmentation implementation, the organization might prioritize ease of transition; later, when the organization is more experienced with microsegmentation, the organization might prioritize critical assets (e.g., high-value assets as candidates).

## 3.2 PHASE 2: IDENTIFY DEPENDENCIES FOR SELECTED CANDIDATE RESOURCES

For candidate resources, the organization identifies any other applications, workflows, data, assets and environments needed to perform the business function. Stakeholders should be included in this identification process.

## 3.3 PHASE 3: DETERMINE APPROPRIATE SEGMENTATION POLICIES

The organization investigates different segmentation options that enable the candidate resource to perform its business function. Then, the organization selects the appropriate policy using organization-specific criteria (e.g., security, ease of implementation, ease of long-term maintenance). The organization should include users in this process to adequately assess the impact to various workflows and understand the relevant risks.

## 3.4 PHASE 4: DEPLOY UPDATED SEGMENTATION POLICIES

The organization tests the segmentation policy to validate its correctness. For example, the organization might implement the policy in a permissive mode that flags policy violations to detect potentially missed dependencies. The organization then deploys the policy, ensuring that appropriate visibility is in place to validate policy deployment. The organization should provide public documentation of the changes and the current enforcement level, as well as a clearly defined channel for users to provide feedback and receive assistance.

# 4. PLANNING CONSIDERATIONS

Transitioning and existing enterprise from traditional network segmentation to microsegmentation is a complex task that will benefit from the phased approach outlined in this document. Even organizations that can leverage the opportunity to use a greenfield approach (e.g., a project free from previous project constraints, a blank slate) can benefit from using a phased approach. By executing a phased transition, the organization can identify unknown challenges and conflicts and develop strategies to resolve them, enabling the organizations' attainment of ZT objectives while minimizing the risk to operational missions. This document provides a high-level approach that can help inform an organization's plans; however, each organization needs to determine the approach that best meets its needs.

Organization plans for transitioning to microsegmentation should account for the variety of deployed applications, workflows, assets and environments along with how best to provide support for the transition across the organization.

## 4.1 USER AND ORGANIZATIONAL SUPPORT

Before and during the transition to microsegmentation, organizations need to understand user requirements to gain user buy-in and to avoid negative user and mission impacts. Organizations should spend time and other resources during transition planning to understand the needs of their users and system owners.

Communicating the purpose and benefits of this transition to their users and system owners provides them with the knowledge necessary to gain buy-in, and such communication is essential to success.

## 4.2 IDENTIFYING CANDIDATE RESOURCES FOR SEGMENTATION

To effectively identify candidates for transition, organizations must understand their applications, workflows, environments and assets. Next, organizations need to prioritize these candidates. Doing so may entail criticality concerns (e.g., security, importance to business function) and transition concerns (e.g., ease of transition).

Organizations' adoption of new applications, assets or transition to new environments (e.g., cloud migrations) provides opportunities to apply microsegmentation principles. For example, instead of using the lifting and shifting model of taking an existing application or environment and transitioning it as is to the cloud, organizations should consider a cloud-native approach that fully integrates microsegmentation.

## 4.3 IDENTIFYING DEPENDENT RESOURCES

Organizations will need to understand the resources that a transition candidate uses in performing its business function, including those that the candidate depends on as well as those that depend on the candidate. Where the transition candidate is an existing deployed resource, the initial list of dependent resources may be developed through tracking the communications of the transition candidate. Organizations should validate the comprehensiveness of their dependent resource list.

## 4.4 DETERMINING APPROPRIATE SEGMENTATION POLICIES

Organizations need to establish segmentation policies that enable necessary business functions while limiting potential for lateral adversarial movement within the network. Organizations should understand the trade-offs between different segmentation policies to determine whether the policy can meet their objectives. For example, fine-grained segments can limit opportunities for lateral movement; however, the development, deployment and maintenance of those fine-grained segments can be a challenge. Coarse-grained segments are easier to manage, though may require additional security protections and visibility to account for the potential for increased lateral movement. Alternatively, an organization's existing microsegmentation infrastructure might make it easier to develop and maintain a segmentation approach based around the network architecture, whereas a segmentation approach based around that organization's application workflows might better align the security with the applications.

## 4.5 DEPLOYING UPDATED SEGMENTATION POLICIES

Organizations should account for potential issues when deploying updated microsegmentation policies and consider including opportunities to revert these updated policies. Before updating policies, organizations should implement proper monitoring, testing and assessment procedures throughout the deployment process, so business functions continue while security requirements are being met.

## 4.6 HANDLING USER DEVICES

User devices form a core part of most organization workflows. With increased remote work, many user devices operate in both on-premises and off-premises locations (i.e., roaming devices), regularly transitioning between the two. The roaming nature of these devices can complicate microsegmentation considerations. At the same time, these devices create additional security concerns, due to their access to untrusted resources (e.g., the internet, email) and operation in potentially untrusted locations. For on-premises endpoints, traditional network-based microsegmentation approaches can be taken for user endpoints. However, for user endpoints that operate remotely, organizations may need to consider agent-based or even application-based approaches to provide appropriate segmentation for user endpoints. Organizations should also consider additional security protections and visibility as part of a defense-in-depth strategy for user devices.

## 4.7 HANDLING OT, IOT AND LEGACY ENVIRONMENTS AND DEVICES

OT, IoT and legacy environments, devices and applications may not be as amenable to microsegmentation solution deployment. For example, agent-based segmentation solutions may not be available for these devices, necessitating the deployment of network-based segmentation solutions. At the same time, these resources may have limited security protections, increasing the need for segmentation for both protecting these resources and limiting the potential for their misuse if compromised. While organizations should consider replacement solutions, if available, they will need to account for these resources when defining segmentation policies. This might entail limiting access, as much as feasible, both to and from these resources.

For example, an organization might segment their OT environment from their IT environment and define policies that only permit the traffic necessary for performing business functions with the OT environment. Where possible, organizations might supplement this segmentation with additional security protections and visibility as part of a defense-in-depth strategy.

### 4.8 CENTRALIZING CONTROL AND VISIBILITY

Organizational enterprises comprise a variety of environments, applications, endpoints, users and other resources. For example, an organization might have on-premises locations, cloud-based Infrastructure as a Service (IaaS) and Software as a Service (SaaS) deployments and users operating in both on-premises and remote locations. Maintaining and validating microsegmentation policies across the enterprise can be difficult. Organizations should investigate ways to centralize the management of these policies, independent of where the policies are implemented, and ensure the visibility necessary to understand and validate the proper application of the policies.

### 4.9 ONGOING MAINTENANCE AND EVOLUTION

The changeover to a microsegmentation architecture is not a singular transition. Changes to organization applications or environments, the technology landscape, threats or attacker techniques may necessitate validating the existing segmentation approach and may require updates to account for these changes. Changes as part of an organization's overall ZTA implementation may necessitate additional changes in the organization's microsegmentation architecture. Defining, validating and testing these network segmentation policies as part of the process for deploying organization applications and infrastructure can help ensure that microsegmentation policies evolve along with changes to applications and infrastructure. Additionally, organizations should periodically evaluate their segmentation approach and validate its effectiveness against the current threat landscape.

## 5. EXAMPLE MICROSEGMENTATION SCENARIOS

CISA worked with various agencies transitioning to ZTAs. The following example scenarios show how different agencies handled their initial approach toward implementing microsegmentation. In each of these scenarios, the transition to microsegmentation was handled as part of the organization's overall ZT strategy. While these examples highlight some specific high-level initial approaches, each organization may have used additional methods for specific applications, environments, or mission needs as they evolve their overall implementation of ZTA.

### 5.1 SCENARIO #1: REARCHITECTING AN EXISTING ON-PREMISES ENTERPRISE

This organization primarily consisted of infrastructure, services and applications deployed in on-premises environments. Given large existing deployment, the organization decided to focus initial efforts on increasing segmentation for existing infrastructure. These efforts primarily took the form of implementing a network-based microsegmentation model, using existing network infrastructure and updating components only where necessary.

The organization developed a detailed inventory of applications, workflows, data, hardware assets and environments to provide sufficient data to identify candidate resources for segmentation and the associated dependencies. For the initial transition candidate, the organization focused on properly segmenting high-level environments, such as data center, servers, and users by creating policies to define their architectural objectives. These policies are then implemented with technical solutions that meet the requirements of the objectives. Once those high-level segmentation capabilities were in place, the organization began to look for candidates for more finely tuned microsegmentation. The organization selected the initial candidate for

transition, focusing on ease of transition to help the organization learn to apply microsegmentation principles in practice.

For each candidate, the organization developed new policies and applied those policies in a permissive mode that alerted when violations of the policies occurred. This allowed them to hone the policies over time before eventually transitioning them to production. The organization worked with a pilot group of users to test each resource being transitioned to verify the resource continued to meet mission needs.

## 5.2 SCENARIO #2: MICROSEGMENTATION AS PART OF AN ENVIRONMENT TRANSITION

This organization sought to transition from a model where organization environments and applications were primarily deployed in on-premises environments to a model where most infrastructure was deployed in cloud environments. The greenfield nature of these new deployments provided an opportunity to embed microsegmentation principles from the beginning. As they transitioned the legacy environments and services to the cloud, the organization implemented microsegmentation using cloud-native segmentation capabilities.

The organization developed a detailed inventory of their applications, workflows, data, endpoints, users and environments to determine how best to transition each of these to the cloud environment. The organization opted to implement the transitioned candidates using cloud-native technologies instead of doing a "lift and shift" into the cloud. This approach allowed them to integrate microsegmentation using the capabilities available within the cloud environment.

For each candidate resource, the organization worked with a pilot group of users to reimplement it in the cloud environment. This might take the form of adopting an equivalent SaaS solution or reimplementing the functionality using Platform as a Service (PaaS) or IaaS. The organization used capabilities native to the deployment method to implement appropriate segmentation. For example, for container-based PaaS deployments, the organization might use a service mesh architecture, whereas for SaaS deployments, the organization used a native Cloud Access Security Broker (CASB) deployment. After the pilot user group tested and validated the pilot deployment, the organization transitioned the pilot into production and moved the full user base over to the new deployment. This approach allowed the organization to spin down their on-premises infrastructure over time, including the legacy segmentation.

## 5.3 SCENARIO #3: MICROSEGMENTATION OF A DISTRIBUTED ENTERPRISE

This organization has a distributed workforce, including a variety of branch offices and numerous remote workers. All traffic from the branch offices was routed through the main location, enabling access to on-premises applications and allowing centralized security policies to be applied to organization traffic. Using a virtual private network, remote users would connect with on-premises locations to access on-premises applications. The organization initially focused on using a SASE solution for implementing microsegmentation, including a combination of network- and agent-based deployments, which enabled them to centralize the policy and visibility into organization endpoint and branch office connections with both organization and remote resources. The goal was to use the centralized control provided by the SASE solution to implement microsegmentation.

The organization worked with a pilot set of branch offices as well as a pilot group of on-premises and remote users. The organization used a network-based deployment method to send branch office traffic to the SASE provider and an agent-based deployment method to enable user endpoint access to the SASE provider. Initially, the SASE deployment was used to mediate access to the internet, replacing the need for the branch offices and remote users to access the internet through the main location. After that, the organization was able to use capabilities from the SASE provider to allow the pilot group to access organization internal applications through the SASE provider instead of directly accessing them. After validating approach success, the

organization transitioned remaining branch offices and deploy SASE agents more broadly to organization user endpoints.

This model allowed the organization to make the SASE solution the central policy enforcement point mediating all connections between organization endpoints and the deployed services. For each organization internal application, the organization would first make it available to a pilot group through the SASE solution. Then after testing, the organization would make it available across the enterprise. After all access to the service transitioned to the SASE solution, the organization disabled direct access to the service, except potentially for legacy resources that needed to access the service.

# 6. CONCLUSION

Supporting ZTA through microsegmentation implementation requires a significant shift in the technology, policy and security culture of an organization. Organizations should leverage technology updates and the transition to the cloud to move from macrosegmentation to microsegmentation.

This document provides high-level guidance and recommendations as organizations begin planning and scoping their transition to microsegmentation as part of a ZTA. CISA plans to release a subsequent technical guide to support implementation teams during this transition.

# APPENDIX A: FEDERAL GUIDELINES

The following list of documents includes the most recent version of the guidance documents available at time of publication, including drafts:

- Cybersecurity and Infrastructure Security Agency, *CISA's Zero Trust Maturity Model, Version 2.0*, April 2023.
- Cybersecurity and Infrastructure Security Agency, *Trusted Internet Connections 3.0 Cloud Use Case, Version 1.1*, December 2023.
- Cybersecurity and Infrastructure Security Agency, *Trusted Internet Connections 3.0 Program Guidebook, Version 1.1*, July 2021.
- Cybersecurity and Infrastructure Security Agency, *Trusted Internet Connections 3.0 Reference Architecture, Version 1.1*, July 2021.
- Cybersecurity and Infrastructure Security Agency, *Trusted Internet Connections 3.0 Security Capabilities Catalog, Version 3.2,* November 2024.
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), *7498-1:1994, Information technology – Open Systems Interconnection – Basic Reference Model* Section 3.1 *(updated 1996).*
- National Institute of Standards and Technology, *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators*, May 2022.
- National Institute of Standards and Technology, *NIST Special Publication, 800-190: Application Container Security Guide*, September 2017.
- National Institute of Standards and Technology, *NIST Special Publication, 800-207: Zero Trust Architecture*, August 2020.
- National Institute of Standards and Technology, *NIST Special Publication, 800-215: Guide to Secure Enterprise Network Landscape*, November 2022.
- Office of Management and Budget, *Executive Order 14028 on Improving the Nation's Cybersecurity*, May 2021.
- Office of Management and Budget, *Memorandum 22-09: Federal Zero Trust Strategy*, January 2022.

# APPENDIX B: ACRONYMS

| Acronym | Meaning |
|---|---|
| CASB | Cloud Access Security Broker |
| CI/CD | Continuous Integration/Continuous Delivery |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CNAPP | Cloud-Native Application Protection Platform |
| CSPM | Cloud Security Posture Management |
| CWPP | Cloud Workload Protection Platform |
| DMZ | Demilitarized Zones |
| EO | Executive Order |
| FCEB | Federal Civilian Executive Branch |
| IaaS | Infrastructure as a Service |
| ICS | Industrial Control System |
| IOT | Internet of Things |
| IP | Internet Protocol |
| ISO/IEC | International Organization for Standardization/International Electrotechnical Commission |
| IT | Information Technology |
| M | Memorandum |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| OSI | Open Systems Interconnection |
| OT | Operational Technology |
| PaaS | Platform as a Service |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| SASE | Secure Access Service Edge |
| SaaS | Software as a Service |
| SD-WAN | Software-Defined Wide Area Network |
| TIC | Trusted Internet Connections |
| VM | Virtual Machine |
| VLAN | Virtual Local Area Network |
| WAF | Web Application Firewall |
| ZT | Zero Trust |
| ZTA | Zero Trust Architecture |
| ZTMM | Zero Trust Maturity Model |