Zero Trust Architecture

PortSys Total Access Control: Mapping to NIST SP 800-207

The National Institute of Standards and Technology finalized a special publication (SP 800-207) to provide detailed guidance for enterprise organizations on six areas of standards for Zero Trust Architecture (ZTA). This document is intended to be read in conjunction with the NIST SP 800-207 document. It details how Total Access Control (TAC) from PortSys maps to those NIST standards.

AUGUST 27, 2020

1. INTRODUCTION

2. ZERO TRUST BASICS

2.1 **Tenets of Zero Trust –** *Total Access Control supports all the following tenets in Section 2.1.*

- *All data sources and computing services are considered resources.*
- *All communication is secured regardless of network location.*
- *Access to individual enterprise resources is granted on a per-session basis.*
- *Access to resources is determined by dynamic policy – including the observable state of the client identity, application, and the requesting asset – and may include other behavioral and environmental attributes.*
- *The enterprise monitors and measures the integrity and security posture of all owned and associated assets.*
- *All resource authentication and authorization is dynamic and strictly enforced before access is allowed.*
- *The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications, and uses that information to improve its security posture.*

2.2 **A Zero Trust View of a Network –** *Total Access Control supports all the following tenets in Section 2.2.*

- *The entire enterprise private network is not considered an implicit trust zone.*
- *Devices on the network may not be owned or configurable by the enterprise.*
- *No resource is inherently trusted.*
- *Not all enterprise resources are on enterprise-owned infrastructure.*
- *Remote enterprise users cannot fully trust the local network connection.*
- *Assets and workflows moving between enterprise and nonenterprise infrastructure should have a consistent security policy and posture.*

3. LOGICAL COMPONENTS OF ZERO TRUST ARCHITECTURE

3.1 Variations of Zero Trust Architecture Approaches – *TAC supports multiple architecture approaches.*

3.1.1 ZTA Using Enhanced Identity Governance – *TAC supports this approach.*

3.1.2 ZTA Using Micro-Segmentation – *TAC supports this approach.*

3.1.3 ZTA Using Network Infrastructure and Software Defined Perimeters – *TAC partially supports this approach, depending on the interpretation of 3.1.3 definitions. TAC does this logically, but it does not control the network, so this depends on how the supporting network is architected and how access is allowed. TAC provides full segmentation, provided other network routes do not bypass TAC to gain access to resources.*

3.2 Deployed Variations of the Abstract Architecture

3.2.1 Device Agent/Gateway-Based Deployment – *TAC supports this deployment.*

3.2.2 Enclave-Based Deployment – *TAC supports this deployment.*

3.2.3 Resource Portal-Based Deployment – *TAC supports this deployment.*

3.2.4 Device Application Sandboxing – *This deployment is not supported as part of TAC; however, TAC can control access to sandboxes that may already be set up for users.*

3.3 Trust Algorithm

3.3.1 Trust Algorithm Variations

- **Criteria-versus score-based –** *TAC supports criteria-based variations.*
- **Singular versus contextual –** *TAC supports singular variations.*

3.4 Network/Environment Components – *This section is not directly applicable to TAC; however, TAC fully supports the tenets described in Section 3.4.*

4. DEPLOYMENT SCENARIOS/USE CASES

TAC SUPPORTS ALL USE CASES BELOW, AS DESCRIBED IN THIS SECTION.

5. THREATS ASSOCIATED WITH ZERO TRUST ARCHITECTURE

5.1 Subversion of ZTA Decision Process – *This is possible, as with all systems that require an administrator to determine policy. TAC does log changes.*

5.2 Denial-of-Service or Network Disruption – *TAC can be architected to minimize these potential interruptions by implementing a multi-location array. This can be done through local datacenters, cloud hosting locations, and/or a combination of both.*

5.3 Stolen Credentials/Insider Threat – *TAC is particularly resistant to this type of attack, even if valid credentials are stolen. By combining multiple factors of authentication such as MFA, GeoIP location, and device binding. TAC dramatically reduces the opportunity for an attacker to subvert valid credentials to gain access. Should this unlikely event occur, the attacker would still be limited to the resources normally available to the user (under those specific access circumstances, meaning device security state and other factors TAC considers before granting access).*

5.4 Visibility on the Network – *As a reverse proxy solution, TAC breaks the encrypted session and inspects traffic before allowing a user to access resources within the protected enterprise – local and cloud. This helps to mitigate threats through encrypted traffic and tunneled traffic.*

TotalAccessControl™

5.5 Storage of System and Network Information – *TAC protects the storage of network information by controlling access to logs and other traffic information in the same manner as it protects user access to resources on the network. Specifically, organizations can set policies in TAC to require multiple factors of authentication such as device validation, credentials, multifactor authentication, location, device type, device security status, GeoIP location, and more. The combination of these multiple factors of authentication provides a much greater level of secure access to any sensitive information.*

5.6 Reliance on Proprietary Data Formats or Solutions – *Typically, security products from different vendors are not interchangeable, as they are reliant on their own development methodologies. This is the case with TAC as well.*

5.7 Use of Non-person Entities (NPE) in ZTA Administration – *TAC does not use NPEs, so this is not a risk factor.*

6. ZERO TRUST ARCHITECTURE AND POSSIBLE INTERACTIONS WITH EXISTING FEDERAL GUIDANCE

6.1 ZTA and NIST Risk Management Framework – *TAC supports organizations by allowing them to determine risk levels associated with each resource individually and make determinations on acceptable usage under a variety of circumstances in accordance with the risk tolerance for each resource.*

6.2 ZT and NIST Privacy Framework – *This question is mostly policy beyond the scope of ZTA. However, TAC fully supports the encryption and privacy of information as it travels both internally and externally to the organization. Also, any use of personal information as part of security policies (biometrics, device information, GeoIP, etc.) is under the control of the organization and an appropriate user message can be displayed to users when they log into TAC as required.*

6.3 ZTA and Federal Identity, Credential and Access Management Architecture – *Contrary to the NIST statement in Section 6.3, PortSys does not believe user provisioning is a key component of a ZTA solution. Identity solutions already exist, are quite robust, and are in place in most organizations – with far deeper controls and policies than a new solution may offer. Identity management should be a system unto itself, while maintaining a separation between the identity system and access control through a ZTA solution. TAC works hand in hand with identity providers, consuming identity and combining it with other factors of authentication, rather than relying on a single factor for authentication and authorization. TAC combines identity with information about the device, security state, GeoIP location, and other factors. TAC also combines those factors with policies for*

each individual resource to enable vast flexibility in how access is provided to resources, while keeping those resources fully protected. TAC's comprehensive approach to a user's full context of access ensures a stronger validation of the end user and is much less likely to be compromised.

6.4 ZTA and Trusted Internet Connections 3.0 – *As TIC 3.0 is still under development, it is not possible to speculate in specifics on how it will be implemented. However, as TIC 3.0 is aware of ZTA, PortSys fully anticipates that TAC will integrate into NIST's final approved framework.*

6.5 ZTA and EINSTEIN (NCPS-National Cybersecurity Protection System) – *Organizations will be able to integrate or share logs and information from TAC with the NCPS to further strengthen security, should this be deemed desirable.*

6.6 ZTA and DHS Continuous Diagnostics and Mitigations (CDM) Program – *TAC offers an integral component in providing rich, detailed information about users, devices, applications, security postures, and a great many other details about all access. This highly detailed information is invaluable for understanding who is gaining access to what and under what circumstances – both at the moment of access as well as after the fact. Additionally, TAC may not require the same level of discovery of network devices prior to implementing ZTA. TAC allows organizations to create their own security policies to analyze any endpoints attempting access, and then TAC provides dynamic enforcement of those policies at the time access is attempted. It may not be required to fully manage or understand everything about a user's device prior to attempting access – only that at the time of requesting access, the device and user meet the requirements for the specific resource being protected. This dynamic enforcement extends far beyond just the device itself, but also to user credentials, GeoIP location, security status, and many more attributes – all of which can be combined to provide dramatically increased control over access, without placing an undue burden for security on end users.*

6.7 ZTA, Cloud Smart, and the Federal Data Strategy *– TAC fully supports a wide variety of cloud-based solutions and provides significant control over access to those resources. TAC also grants the same controls over access to cloud-based resources that are available to an organization's locally based resources – providing greater consistency and a central control point over all resources, local and cloud. In addition, TAC increases the levels of security applied to access to local and cloud-based resources, beyond the more limited levels cloud providers offer today.*

7. MIGRATING TO A ZERO TRUST ARCHITECTURE

TAC ENABLES FLEXIBLE DEPLOYMENTS WHILE AN ORGANIZATION'S EXISTING ACCESS INFRASTRUCTURES ARE IN PLACE, LEAVING THEM UNDISTURBED DURING THE MIGRATION. ADDITIONALLY, TAC IS VERY SIMPLE FOR END USERS TO UNDERSTAND, SO IT TYPICALLY REQUIRES VERY LITTLE TRAINING. TAC FULLY SUPPORTS A PHASED MIGRATION APPROACH OVER TIME TO HELP AN ORGANIZATION MORE EFFECTIVELY MANAGE CHANGE ACROSS ITS CULTURE AS IT IMPLEMENTS A NEW PROCESS.

7.1 Pure Zero Trust Architecture – *TAC supports both a "greenfield" system as well as a step-by-step migration from existing access methods to TAC, at the pace that works best for an organization to achieve a successful transition.*

7.2 Hybrid ZTA and Perimeter-Based Architecture – *TAC is designed to be flexible. It works alongside or in concert with existing security infrastructures. It is designed for real-world environments, whereas a rip-and-replace strategy is extremely cost-prohibitive and not possible to achieve in a timely manner. TAC easily works within an existing perimeter-based architecture to bring more control over access to make the pace of change customized to an organization's unique requirements.*

7.3 Steps to Introducing ZTA to a Perimeter-Based Architected Network – *TAC offers an organization with a perimeter-based architected network the ability to take an accelerated approach to introducing a Zero Trust Architecture. Instead of analyzing and cloning all its legacy assets, users, privileges, and business processes, TAC enables an organization to more comprehensively define the modern controls it needs for all access – to every resource across the enterprise, local and cloud. Once an organization is comfortable with the more comprehensive secure access TAC provides across the enterprise, legacy solutions an organization has been using for access can be discontinued. Until an organization reaches that level of confidence, TAC continues to support all methods of access.*

7.3.1 Identify Actors on the Enterprise – *With its approach to ZTA, TAC excels at being able to provide variable levels of access for different types of accounts. TAC provides access only to the resources each individual or account qualifies for under specific circumstances. This provides much more granularity than traditional security methods, especially for admin accounts. For example, access can be granted or limited based on numerous factors – including GeoIP location, device type, certificates, hidden files, registry key entries, device security status, credentials, multifactor authentication, and more. TAC uses any or all of these factors to determine whether access should be allowed or denied for each specific resource.*

7.3.2 Identify Assets Owned by the Enterprise – *TAC fully supports an organization's legacy owned identity assets. TAC provides strong capabilities for identifying and evaluating devices, and then uses this information in the process to determine whether access should be granted or denied to resources. All this information is kept and logged in one central location for further inspection as required.*

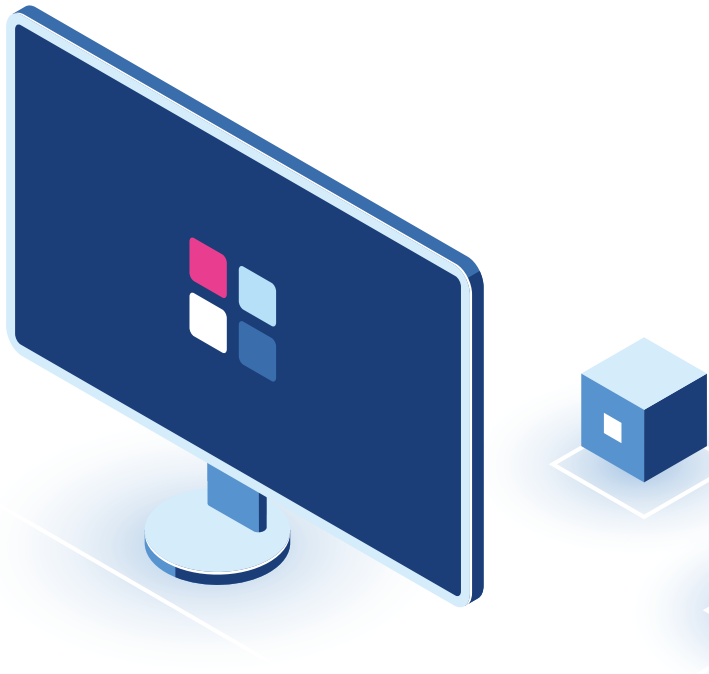
7.3.3 Identify Key Processes and Evaluate Risks Associated with Executing Process – *TAC fully supports the choices an organization makes for which business processes to prioritize and implement first.*

7.3.4 Formulating Policies for the ZTA Candidate – *Selecting which business processes to move to ZTA is beyond the scope of TAC. However, TAC fully supports whichever direction an organization wishes to take.*

7.3.5 Identifying Candidate Solutions – *TAC supports many deployment strategies and situations, including having clients installed on endpoints or offering full clientless deployments. The support and engineering teams at PortSys provide expert insights to enable an organization to fully understand the critical variations in different strategies that need to be considered to determine which method works best for its unique environment.*

7.3.6 Initial Deployment and Monitoring – *TAC supports a variety of methods for managing trial periods and gradually tightening security policies over applications. TAC provides real-time monitoring of access and policy violations in one central location, which is critical to troubleshooting policies when necessary.*

7.3.7 Expanding the ZTA – *TAC easily scales to add new resources and user groups, along with the required accompanying security policies. When new or significant shifts occur – such as the introduction of device upgrades or regulatory requirements – TAC's access policies are quickly and easily modified to adapt to those changes.*



To learn more about how Total Access Control maps to the Zero Trust Architecture standards in NIST SP 800-207, or to set up a demo to learn how PortSys can help your organization to create a more comprehensive, integrated and fortified architecture:

Call: +1 781-996-4900 in North America
+44 208 196 2420 in Europe, the Middle East, or Africa
Email: Sales@PortSys.com
Web: Contact Us

PORTSYS®