NIST SPECIAL PUBLICATION 1800-35A

Implementing a Zero Trust Architecture

Volume A:
Executive Summary

Alper Kerman
Murugiah Souppaya
National Institute of Standards and Technology
Rockville, Maryland

Dr. Parisa Grayeli
Susan Symington
The MITRE Corporation
McLean, Virginia

June 2022

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

Executive Summary

As an enterprise's data and resources have become distributed across the on-premises environment and multiple clouds, protecting them has become increasingly challenging. Many users need access from anywhere, at any time, from any device to support the organization's mission. Data is programmatically stored, transmitted, and processed across different organizations' environments, which are distributed across on-premises and the cloud to meet ever-evolving business use cases. It is no longer feasible to simply protect data and resources at the perimeter of the enterprise environment and assume that all users, devices, applications, and services within it can be trusted.

A zero-trust architecture (ZTA) enables secure authorized access to each individual resource, whether located on-premises or in the cloud, for a hybrid workforce and partners based on an organization's defined access policy. For each access request, ZTA explicitly verifies the context available at access time—this includes the requester's identity and role, the requesting device's health and credentials, and the sensitivity of the resource. If the defined policy is met, a secure session is created to protect all information transferred to and from the resource. A real-time and continuous policy-driven, risk-based assessment is performed to establish and maintain the access.

This guide summarizes how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are using commercially available technology to build interoperable, open standards-based ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. As the project progresses, this preliminary draft will be updated, and additional volumes will also be released for comment.

CHALLENGE

Organizations would like to adopt a ZTA, but they have been facing some challenges which may include:

- Leveraging existing investments and balancing priorities while making progress toward a ZTA
- ZTA deployment requiring leveraging integration of many deployed existing technologies of varying maturities and identifying technology gaps to build a complete ZTA
- Concern that ZTA might negatively impact the operation of the environment or end-user experience
- Lack of common understanding of ZTA across the organization, gauging the organization's ZTA maturity, determining which ZTA approach is most suitable for the business, and developing an implementation plan

This preliminary practice guide can help your organization:

- **Identify milestones for gradually integrating ZTA into your environment,** based on the demonstrated examples and using a risk-based approach, to:
  - **Support teleworkers** with access to resources regardless of user location or user device (managed or unmanaged)
  - **Protect resources regardless of their location** (on-premises or cloud-based)
  - **Limit the insider threat** (insiders are not automatically trusted)

This preliminary practice guide can help your organization:
▪ **Limit breaches** (reduce attackers' ability to move laterally in the environment) ▪ **Protect sensitive corporate information** with data security solutions ▪ **Improve visibility** into the inventory of resources, what configurations and controls are implemented, and how resources are accessed and protected ▪ **Real-time and continuous policy-driven, risk-based assessment** of resource access

SOLUTION

NCCoE is collaborating with ZTA technology providers to build several example ZTA solutions and demonstrate their ability to meet the tenets of ZTA. The solutions will enforce corporate security policy dynamically and in near-real-time to restrict access to authenticated, authorized users and devices while flexibly supporting a complex set of diverse business use cases involving a remote workforce, use of the cloud, partner collaboration, and support for contractors. The example solutions are designed to demonstrate the ability to protect against and detect attacks and malicious insiders. They showcase the ability of ZTA products to interoperate with existing enterprise and cloud technologies with only minimal impact on end-user experience.

The project can help organizations plan how to evolve their existing enterprise environments to ZTA, starting with an assessment of their current resources and setting milestones along a path of continuous improvement, gradually bringing them closer to achieving the ZTA goals they have prioritized based on risk, cost, and resources. We are using a phased approach to develop example ZTA solutions that is designed to represent how we believe most enterprises will evolve their enterprise architecture toward ZTA, i.e., by starting with their already-existing enterprise environment and gradually adding or adapting capabilities. Our first implementations are crawl versions of the enhanced identity governance (EIG) deployment because EIG is seen as the foundational component of the other deployment approaches utilized in today's hybrid environments. Our initial EIG implementations use the identity of subjects and device health as the main determinants of access policy decisions.

Depending on the current state of identity management in the enterprise, deploying EIG solutions is an initial key step that will be leveraged to support micro-segmentation and software-defined perimeter (SDP) deployment approaches, which will be covered in the later phases of the project. Our strategy is to follow an agile implementation methodology to build everything iteratively and incrementally while adapting or adding more capabilities to evolve to a complete ZTA. We are starting with the minimum viable EIG solution that allows us to achieve some level of ZTA, and then we will gradually deploy additional functional components and features to address an increasing number of ZTA requirements, progressing the project toward demonstration of more robust micro-segmentation and SDP deployment options.

Collaborators		
Appgate	IBM	Ping Identity
AWS	Ivanti	Radiant Logic

Collaborators		
Broadcom Software	Lookout	SailPoint
Cisco	Mandiant	Tenable
DigiCert	Microsoft	Trellix
f5	Okta	VMware
Forescout	Palo Alto Networks	Zimperium
Google Cloud	PC Matic	Zscaler

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and information technology (IT) system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-35A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-35B: Approach, Architecture, and Security Characteristics* once it is available. It will describe what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-35C: How-To Guides* once it is available. It will provide specific product installation, configuration, and integration instructions for building this project's example implementations, allowing them to be replicated in whole or in part.

SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at the NCCoE ZTA project page. NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solution and developing other parts of the content. As a preliminary draft, this volume will have at least one additional draft released for public comment before it is finalized.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and recommended practices for transforming the processes associated with implementing this guide.

To provide comments, join the community of interest, or learn more by arranging a demonstration of this example implementation, contact the NCCoE at nccoe-zta-project@list.nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.