

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date February 13, 2020

Original Release Date September 23, 2019

Superseding Document

Status 2nd Public Draft (2PD)

Series/Number NIST Special Publication 800-207

Title Zero Trust Architecture

Publication Date February 2020

DOI <https://doi.org/10.6028/NIST.SP.800-207-draft2>

CSRC URL <https://csrc.nist.gov/publications/detail/sp/800-207/draft>

Additional Information

2

3 **Zero Trust Architecture**

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-207-draft>

C O M P U T E R S E C U R I T Y

20 **Draft NIST Special Publication 800-207**

21

22

23 **Zero Trust Architecture**

24

25

26

Scott Rose

27

Oliver Borchert

28

Advanced Network Technologies Division

29

Information Technology Laboratory

30

31

Stu Mitchell

32

Stu2Labs

33

Stafford, VA

34

35

Sean Connelly

36

Department of Homeland Security

37

38

39

This publication is available free of charge from:

40

<https://doi.org/10.6028/NIST.SP.800-207-draft>

41

42

43

September 2019

44



45

46

47

48

U.S. Department of Commerce

49

Wilbur L. Ross, Jr., Secretary

50

51

National Institute of Standards and Technology

52

Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

53

Authority

54 This publication has been developed by NIST in accordance with its statutory responsibilities under the
55 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law
56 (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including
57 minimum requirements for federal information systems, but such standards and guidelines shall not apply
58 to national security systems without the express approval of appropriate federal officials exercising policy
59 authority over such systems. This guideline is consistent with the requirements of the Office of Management
60 and Budget (OMB) Circular A-130.

61 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and
62 binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these
63 guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce,
64 Director of the OMB, or any other federal official. This publication may be used by nongovernmental
65 organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would,
66 however, be appreciated by NIST.

67 National Institute of Standards and Technology Special Publication 800-207
68 Natl. Inst. Stand. Technol. Spec. Publ. 800-207, 49 pages (September 2019)
69 CODEN: NSPUE2

70 This publication is available free of charge from:
71 <https://doi.org/10.6028/NIST.SP.800-207-draft>

72 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
73 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
74 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
75 available for the purpose.

76 There may be references in this publication to other publications currently under development by NIST in accordance
77 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
78 may be used by federal agencies even before the completion of such companion publications. Thus, until each
79 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
80 planning and transition purposes, federal agencies may wish to closely follow the development of these new
81 publications by NIST.

82 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to
83 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
84 <https://csrc.nist.gov/publications>.

85

86 **Public comment period: *September 23, 2019 through November 22, 2019***

87 National Institute of Standards and Technology
88 Attn: Advanced Network Technologies Division, Information Technology Laboratory
89 100 Bureau Drive (Mail Stop 8920) Gaithersburg, MD 20899-8920
90 Email: zerotrust-arch@nist.gov

91 All comments are subject to release under the Freedom of Information Act (FOIA).

92

Reports on Computer Systems Technology

93 The Information Technology Laboratory (ITL) at the National Institute of Standards and
94 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
95 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test
96 methods, reference data, proof of concept implementations, and technical analyses to advance the
97 development and productive use of information technology. ITL's responsibilities include the
98 development of management, administrative, technical, and physical standards and guidelines for
99 the cost-effective security and privacy of other than national security-related information in federal
100 information systems. The Special Publication 800-series reports on ITL's research, guidelines, and
101 outreach efforts in information system security, and its collaborative activities with industry,
102 government, and academic organizations.

103

Abstract

104 Zero Trust is the term for an evolving set of network security paradigms that move network
105 defenses from wide network perimeters to narrowly focusing on individual or small groups of
106 resources. A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust
107 granted to systems based on their physical or network location (i.e., local area networks vs. the
108 Internet). Access to data resources is granted when the resource is required, and authentication
109 (both user and device) is performed before the connection is established. ZTA is a response to
110 enterprise network trends that include remote users and cloud-based assets that are not located
111 within an enterprise-owned network boundary. ZTA focuses on protecting resources, not
112 network segments, as the network location is no longer seen as the prime component to the
113 security posture of the resource. This document contains an abstract definition of ZTA and gives
114 general deployment models and use cases where ZTA could improve an enterprise's overall IT
115 security posture.

116

Keywords

117 architecture; cybersecurity; enterprise; network security; zero trust.

118

119

Acknowledgments

120 This document is the product of a collaboration of multiple federal agencies and overseen by the
121 Federal CIO Council. The Architecture sub-group is responsible for the development of this
122 document, but there are specific individuals who deserve recognition. These include Greg
123 Holden, the project manager of the Federal CIO Council ZTA project, and Alper Kerman, the
124 project manager for the NIST/NCCoE ZTA effort and Douglas Montgomery.

125

Audience

126 This document is intended to be a description of ZTA strategies for enterprise network architects.
127 The document is meant to aid understanding of ZTA for civilian unclassified systems and
128 provide a roadmap to migrate and deploy ZTA concepts to an enterprise network. Agency
129 cybersecurity managers, network administrators, and managers may also gain insight into ZTA
130 from this document. This document is not intended to be a single deployment plan for ZTA, as
131 an enterprise will have unique business use cases and data assets that require protection. Starting
132 with a solid understanding of your organization's business and data will result in a strong
133 approach to zero trust.

134

Note to Reviewers

135 The purpose of this Special Publication is to develop a technology-neutral set of terms,
136 definitions, and logical components of network infrastructure using a ZTA strategy. This
137 document does not give specific guidance or recommendations on how to deploy zero trust
138 components in an enterprise. Reviewers are asked to tailor their comments based on the stated
139 purpose of the document.

140

Trademark Information

141 All registered trademarks or trademarks belong to their respective organizations.
142

143

Call for Patent Claims

144 This public review includes a call for information on essential patent claims (claims whose use
145 would be required for compliance with the guidance or requirements in this Information
146 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
147 directly stated in this ITL Publication or by reference to another publication. This call also
148 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
149 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

150

151 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
152 in written or electronic form, either:

153

154 a) assurance in the form of a general disclaimer to the effect that such party does not hold and
155 does not currently intend holding any essential patent claim(s); or

156

157 b) assurance that a license to such essential patent claim(s) will be made available to applicants
158 desiring to utilize the license for the purpose of complying with the guidance or requirements in
159 this ITL draft publication either:

160

161 i) under reasonable terms and conditions that are demonstrably free of any unfair
162 discrimination; or

163

164 ii) without compensation and under reasonable terms and conditions that are
165 demonstrably free of any unfair discrimination.

166

167 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
168 on its behalf) will include in any documents transferring ownership of patents subject to the
169 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
170 the transferee, and that the transferee will similarly include appropriate provisions in the event of
171 future transfers with the goal of binding each successor-in-interest.

172

173 The assurance shall also indicate that it is intended to be binding on successors-in-interest
174 regardless of whether such provisions are included in the relevant transfer documents.

175

176 Such statements should be addressed to: zerotrust-arch@nist.gov

177

178

179 **Table of Contents**

180 **1 Introduction 1**

181 1.1 Background..... 1

182 1.2 Structure of this Document 2

183 **2 Zero Trust Network Architecture 3**

184 2.1 Tenets of Zero Trust Architecture 4

185 2.2 A Zero Trust View of a Network 5

186 2.2.1 Assumptions for Enterprise-Owned Network Infrastructure..... 5

187 2.2.2 Assumptions for Non-Enterprise-Owned Network Infrastructure 6

188 **3 Zero Trust Architecture Logical Components 7**

189 3.1 Deployed Variations of the Abstract Architecture..... 9

190 3.1.1 Device Agent/Gateway-Based Deployment..... 9

191 3.1.2 Microperimeter-Based Deployment 10

192 3.1.3 Resource Portal-Based Deployment 11

193 3.1.4 System Application Sandboxing 12

194 3.2 Trust Algorithm..... 12

195 3.2.1 Trust Algorithm Variations 14

196 3.3 Network Components 15

197 3.3.1 Network Requirements to Support ZTA..... 15

198 **4 Deployment Scenarios/Use Cases 17**

199 4.1 Enterprise with Satellite Facilities..... 17

200 4.2 Multi-Cloud Enterprise 18

201 4.3 Enterprise with Contracted Services and/or Non-Employee Access..... 18

202 4.4 Collaboration Across Enterprise Boundaries 19

203 **5 Threats Associated with Zero Trust Architecture 21**

204 5.1 Subversion of ZTA Decision Process..... 21

205 5.2 Denial-of-Service or Network Disruption 21

206 5.3 Insider Threat..... 22

207 5.4 Visibility on the Network..... 22

208 5.5 Storage of Network Information 22

209 5.6 Reliance on Proprietary Data Formats..... 23

210 5.7 Use of Non-Person Entities (NPE) in ZTA administration. 23

211 **6 Zero Trust Architecture and Existing Federal Guidance 24**

212 6.1 ZTA and NIST Risk Management Framework 24

213 6.2 ZTA and NIST Privacy Framework 24

214 6.3 ZTA and Federal Identity, Credential, and Access Management Architecture

215 (FICAM) 24

216 6.4 ZTA and Trusted Internet Connection (TIC)..... 25

217 6.5 ZTA and EINSTEIN (NCPS – National Cybersecurity Protection System) ... 25

218 6.6 ZTA and Continuing Diagnostics and Mitigations (CDM) 26

219 6.7 ZTA, Cloud Smart, and the Federal Data Strategy 26

220 **7 Migrating to a Zero Trust Architecture..... 28**

221 7.1 Pure Zero Trust Architecture..... 28

222 7.2 Hybrid ZTA and Legacy Architecture 28

223 7.3 Steps to Introducing ZTA to a Legacy Architected Network..... 28

224 7.3.1 Identify Actors on the Enterprise 29

225 7.3.2 Identify Assets Owned by the Enterprise..... 30

226 7.3.3 Identify Key Processes and Evaluate Risks Associated with Executing

227 Process 30

228 7.3.4 Formulating Policies for the ZTA Candidate 31

229 7.3.5 Identifying Candidate Solutions 31

230 7.3.6 Initial Deployment and Monitoring 31

231 7.3.7 Expanding the ZTA..... 32

232 **References..... 33**

List of Appendices

235 **Appendix A— Acronyms 35**

236 **Appendix B— Identified Gaps in the Current State of the Art in ZTA..... 36**

237 B.1 Technology Survey 36

238 B.2 Gaps that Prevent Immediate Move to ZTA..... 37

239 B.2.1 Lack of Common Terms for ZTA Design, Planning and Procurement 37

240 B.2.2 Perception that ZTA is in Conflict with Existing Federal Cybersecurity

241 Policies..... 37

242 B.3 Systemic Gaps that Impact ZTA 37

243 B.3.3 Standardization of Interfaces Between Components..... 37

244 B.3.4 Emerging Standards that Address Overreliance on Proprietary APIs. 38

245 B.4 Knowledge Gaps in ZTA and Future Areas of Research 38

246 B.4.5 Attacker Response to ZTA 39

247 B.4.6 User Experience in a ZTA Environment 39

248 B.4.7 Resilience of ZTA to Enterprise and Network Disruption..... 39

249 B.5 ZTA Test Environment 40

250 B.6 References 40

251

252

List of Figures

253 Figure 1: Zero Trust Access 3

254 Figure 2: Core Zero Trust Logical Components 7

255 Figure 3: Device Agent/Gateway Model 9

256 Figure 4: Enclave Gateway Model 10

257 Figure 5: Resource Portal Model..... 11

258 Figure 6: Application Sandboxes..... 12

259 Figure 7: Trust Algorithm Input..... 13

260 Figure 8: Enterprise with Remote Employees 17

261 Figure 9: Multi-Cloud Use Case 18

262 Figure 10: Enterprise with Non-Employee Access 19

263 Figure 11: Cross-Enterprise Collaboration 20

264 Figure 12: ZTA Deployment Cycle 29

265

266

List of Tables

267 Table B-1: Summary of Identified Gaps 36

268

269 **1 Introduction**

270 A typical enterprise’s network infrastructure has grown increasingly complex. A single
271 enterprise may operate several internal networks, remote offices with their own local
272 infrastructure, remote and/or mobile individuals, and cloud services. This complexity has
273 outstripped traditional methods of perimeter-based network security as there is no single, easily
274 identified perimeter for the enterprise.

275 This complex enterprise has led to a new way to plan enterprise network security known as Zero
276 Trust Architecture (ZTA). A ZTA approach is primarily focused on data protection but can be
277 expanded to include all enterprise assets. ZTA assumes the network is hostile and that an
278 enterprise-owned network infrastructure is no different—or no more secure—than any non-
279 enterprise owned network. In this new paradigm, an enterprise must continuously analyze and
280 evaluate the risks to their internal assets and business functions and then enact protections to
281 mitigate these risks. In ZTA, these protections usually involve minimizing access to resources to
282 only those who are validated as needing access and continuously authenticating the identity and
283 security posture of each access request.

284 This publication provides a definition of ZTA, its logical components, possible deployment
285 scenarios, and threats. It also presents a general roadmap for organizations wishing to migrate to
286 a ZTA-centered network infrastructure and discusses relevant federal policies that may impact or
287 influence a zero trust architecture.

288 ZTA is not a single network architecture but a set of guiding principles in network infrastructure
289 design and operation that can be used to improve the security posture of any classification or
290 sensitivity level. Transitioning to ZTA is a journey and cannot be accomplished without a
291 wholesale replacement of technology. That said, many organizations already have elements of a
292 ZTA in their enterprise infrastructure today. Organizations should seek to incrementally
293 implement zero trust principles, process changes, and technology solutions that protect its data
294 assets and business functions. Most enterprise infrastructures will operate in a hybrid Zero
295 Trust/Legacy mode during this time while continuing to invest in ongoing IT modernization
296 initiatives and improving organization business processes.

297 Organizations need to implement effective information security and resiliency practices for zero
298 trust to be effective. When complemented with existing cybersecurity policies and guidance,
299 identity and access management, continuous monitoring, and general cybersecurity, ZTA can
300 reinforce an organization’s security posture using a managed risk approach and protect against
301 common threats.

302 **1.1 Background**

303 The concept of zero trust has been present in cybersecurity since before the actual term “zero
304 trust” was coined. The work of the Jericho Forum publicized the idea of limiting implicit trust
305 based on network location and the limitations of relying on static defenses [JERICHO]. The
306 concepts in de-perimeterization evolved and improved into a larger concept that became known

307 as zero trust. Later, Jon Kindervag coined the term “Zero Trust”¹ while at Forrester² (now at
308 Palo Alto Networks). This work included key concepts and a zero trust network architecture
309 model that improved upon the concepts discussed in the Jericho Forum.

310 In many ways, federal agencies have been moving to network security based on zero trust
311 principles for over a decade. Federal agencies have been building capabilities and policies
312 starting with the Federal Information Security Management Act (FISMA) followed by the Risk
313 Management Framework (RMF); Federal Identity, Credential, and Access Management
314 (FICAM); Trusted Internet Connection (TIC); and Continuous Diagnostics and Mitigation
315 (CDM) programs. All of these programs aim to restrict data and resource access to authorized
316 parties. When these programs were started, they were limited by the technical capabilities of
317 information systems. Security policies were largely static and were enforced at large “choke
318 points” that an enterprise could control to get the largest effect for the effort. As technology
319 matures, it is becoming possible to continuously analyze and evaluate access requests in a
320 dynamic and granular fashion.

321 **1.2 Structure of this Document**

322 The rest of the document is broken down as follows:

- 323 • **Section 2:** Defines ZTA and lists some network assumptions when designing ZTA
324 enterprise networks. This section also includes a list of the tenets of ZTA design.
- 325 • **Section 3:** Documents the logical components, or building blocks, of a ZTA. It is
326 possible that unique implementations compose ZTA components differently yet serve the
327 same logical functionality.
- 328 • **Section 4:** Lists some possible use cases where ZTA may make enterprise networks more
329 secure and less prone to successful exploitation. These include enterprises with remote
330 employees, cloud services, guest networks, etc.
- 331 • **Section 5:** Discusses the threats to an enterprise using a ZTA strategy. Many of these
332 threats are similar to more traditionally architected networks but may require different
333 mitigation techniques.
- 334 • **Section 6:** Discusses how ZTA tenets fit into and/or complement existing guidance for
335 federal agencies.
- 336 • **Section 7:** Presents the starting point for transitioning an enterprise (such as a federal
337 agency) to a ZTA. This includes a description of the general steps needed to plan and
338 deploy applications and network infrastructure that are guided by ZTA tenets.

339

¹ <https://www.paloaltonetworks.com/resources/videos/zero-trust>

² Any mention of commercial products or services within NIST documents is for information only; it does not imply recommendation or endorsement by NIST.

2 Zero Trust Network Architecture

Zero Trust Architecture is an end-to-end approach to network/data security that encompasses identity, credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. Zero trust is an architectural approach that is focused on data protection. The initial focus should be on restricting resource access to those with a “need to know.” Traditionally, agencies (and enterprise networks in general) have focused on perimeter defense, and authorized users are given broad access to resources. As a result, unauthorized lateral movement within a network has been one of the biggest challenges for federal agencies. The Trusted Internet Connections (TIC) and agency perimeter firewalls provide strong Internet gateways. This helps block attackers from the Internet, but the TICs and perimeter firewalls are less useful for detecting and blocking attacks from inside the network.

An operative definition of ZTA is as follows:

Zero Trust Architecture (ZTA) provides a collection of concepts, ideas, and component relationships (architectures) designed to eliminate the uncertainty in enforcing accurate access decisions in information systems and services.

This definition focuses on the crux of the issue, which is to *eliminate unauthorized access to data and services*, coupled with making the *access control enforcement as granular as possible*. That is, authorized and approved subjects (user/machine) can access the data to the exclusion of all other subjects (i.e., attackers). To take this one step further, the word “resource” can be substituted for “data” so that ZTA is about resource access (e.g., printers, compute resources, IoT actuators, etc.) and not just data access.

In order to lessen uncertainties (as they cannot be totally eliminated), the focus is on authentication, authorization, and shrinking implied trust zones while minimizing temporal delays in network authentication mechanisms. Access rules are restricted to least privilege and made as granular as possible.

In Figure 1, a user or machine needs access to an enterprise resource. Access is granted through a Policy Decision Point (PDP) and corresponding Policy Enforcement Point (PEP).

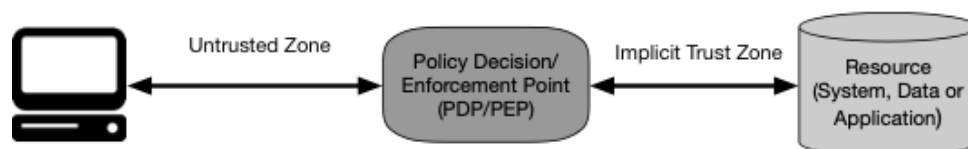


Figure 1: Zero Trust Access

The system must ensure the user is “trustworthy” and the request is valid. The PDP/PEP passes proper judgment to allow the subject to access the resource. This implies that Zero Trust applies for two basic areas: authentication and authorization. Can the system remove sufficient doubt about the user’s true identity? Is the user justified in their access request? Is the device used for

374 the request trustworthy? Overall, enterprises need to develop risk-based policies for resource
375 access and set up a system to ensure that these policies are executed correctly. This means that an
376 enterprise should not rely on implied trustworthiness, wherein if the user has met a base
377 authentication level (i.e., logging into a system), all resource requests are assumed to be equally
378 valid.

379 The “Implied Trust Zone” represents an area where all the entities are trusted to at least the level
380 of the last PDP/PEP gateway. For example, consider the passenger screening model in an airport.
381 All passengers pass through the airport security check point (PDP/PEP) to access the boarding
382 gates. The passengers mill about in the terminal area and all the cleared passengers have a
383 common trust level. In this model, the implied trust zone is the boarding area.

384 The PDP/PEP applies a common set of controls such that all traffic beyond the checkpoint has a
385 common level of trust. The PDP/PEP cannot apply policy beyond its location in the flow of
386 traffic. In order to allow the PDP/PEP to be as specific as possible, the Implied Trust Zone has to
387 be as small as possible.

388 Zero Trust Architecture provides technology and capabilities to allow the PDP/PEPs to move
389 closer to the resource. The idea is to authenticate and authorize every single flow in the network
390 from actor (or application) to data.

391 **2.1 Tenets of Zero Trust Architecture**

392 Many definitions and discussions of ZTN/ZTA stress the concept of removing perimeter
393 defenses (e.g., firewalls, etc.) from the equation. However, most continue to define themselves in
394 relation to perimeters in some way (such as micro-segmentation or micro-perimeters). The
395 following is an attempt to define ZTA in terms of basic tenets that should be involved, not what
396 is excluded.

397 A *Zero Trust Architecture* is designed and deployed adhering to the following basic tenets:

- 398 1. **All data sources and computing services are considered resources.** A network may be
399 composed of several different classes of devices. A network may also have small
400 footprint devices that send data to aggregators/storage, systems sending instructions to
401 actuators, etc. Also, an enterprise may decide to classify personally-owned devices as
402 resources if they are allowed to access enterprise-owned resources.
- 403 2. **All communication is secure regardless of network location.** Network location does
404 not imply trust. Access requests from systems located on enterprise-owned network
405 infrastructure (e.g., inside a legacy network perimeter) must meet the same security
406 requirements as access requests and communication from any other non-enterprise owned
407 network. In other words, there should not be any trust automatically granted based on the
408 device being on enterprise network infrastructure. All communication should be done in a
409 secure manner (i.e., encrypted and authenticated).
- 410 3. **Access to individual enterprise resources is granted on a per-connection basis.** Trust
411 in the requester is evaluated before the access is granted. This could mean only
412 “sometime previously” for this particular transaction and may not occur directly before
413 initiating a connection with a resource. However, authentication to one resource will not
414 automatically grant access to a different resource.

- 415 4. **Access to resources is determined by policy, including the observable state of user**
416 **identity and the requesting system, and may include other behavioral attributes.** An
417 organization protects resources by defining what resources it has, who its members are,
418 and what access to resources those members need. User identity includes the network
419 account used and any associated attributes assigned by the enterprise to that account.
420 Requesting system state includes device characteristics such as software versions
421 installed, network location, previously observed behavior, installed credentials, etc.
422 Behavioral attributes include automated user analytics, device analytics, and measured
423 deviations from observed usage patterns. Policy is the set of attributes an organization
424 assigns to a user, data asset, or application. These attributes are based on the needs of the
425 business process and acceptable level of risk. Resource access policies can vary based
426 upon the sensitivity of the resource/data. Least privilege principles are applied in order to
427 restrict both visibility and accessibility.
- 428 5. **The enterprise ensures all owned and associated systems are in the most secure state**
429 **possible and monitors systems to ensure that they remain in the most secure state**
430 **possible.** An enterprise implementing a ZTA strategy should establish a Continuing
431 Diagnostics and Mitigation (CDM) program to monitor the state of systems and apply
432 patches/fixes as needed. Systems that are discovered to be subverted, vulnerable, and/or
433 non-enterprise-owned may be treated differently (including denial of all connections to
434 enterprise resources) than systems owned by or associated with the enterprise that are
435 deemed to be in their most secure state.
- 436 6. **User authentication is dynamic and strictly enforced before access is allowed.** This is
437 a constant cycle of access, scanning and assessing threats, adapting, and continuously
438 authenticating. An enterprise implementing a ZTA strategy has a user provisioning
439 system in place and uses the system to authorize access to resources. This includes the
440 use of multi-factor authentication (MFA) for access to some (or all) enterprise resources.
441 Continuous monitoring and re-authentication occur throughout user interaction, as
442 defined and enforced by policy (e.g., time-based, new resource requested, resource
443 modification, etc.) that strives to achieve a balance of security, availability, usability, and
444 cost-efficiency.

445
446 The above tenets attempt to be as technology-agnostic as possible. For example, “network ID”
447 could include several factors such as username/password, certificates, one-time password, or
448 some other identification.

449 **2.2 A Zero Trust View of a Network**

450 There are some basic assumptions for network connectivity for any organization that utilizes
451 ZTA in network planning and deployment. Some of these assumptions apply to enterprise-owned
452 network infrastructure, and some apply to enterprise-owned resources used on non-enterprise-
453 owned network infrastructure (e.g., public WiFi). The network in an enterprise implementing a
454 ZTA strategy should be developed with the ZTA tenets outlined above and with the following
455 assumptions.

456 **2.2.1 Assumptions for Enterprise-Owned Network Infrastructure**

- 457 1. **The enterprise private network is not trustworthy.** Systems should always act as if an
458 attacker is present on the enterprise network, and communication should be done in a

- 459 secure manner (see Tenet 2 above). This entails actions such as authenticating all
460 connections and encrypting all traffic.
- 461 2. **Devices on the network may not be owned or configurable by the enterprise.** Visitors
462 and/or contracted services may include non-enterprise-owned systems that need network
463 access in order to perform their role. This also includes bring-your-own-device (BYOD)
464 policies that allow enterprise users to use non-enterprise-owned devices to access
465 enterprise resources.
 - 466 3. **No device is inherently trusted.** Every device must authenticate itself (either to resource
467 or PEP) before connecting to an enterprise-owned resource (see Tenet 6 above).
468 Enterprise-owned devices can have artifacts that enable authentication and provide a
469 higher trust score (see Section 3.2) than the same request coming from non-enterprise-
470 owned devices. User credentials are insufficient for device authentication to an enterprise
471 resource.
472

473 2.2.2 Assumptions for Non-Enterprise-Owned Network Infrastructure

- 474 1. **Not all enterprise resources are on enterprise-owned infrastructure.** This includes
475 remote users as well as cloud services. The enterprise must be able to monitor, configure,
476 and patch any system, but any system may rely on the local (i.e., non-enterprise) network
477 for basic connectivity and network services (e.g., DNS, etc.).
- 478 2. **Remote enterprise users cannot trust the local network connection.** Remote users
479 should assume the local (i.e., non-enterprise-owned) network is hostile. Systems should
480 assume all traffic is being monitored and potentially modified. All connection requests
481 should be authenticated, and all traffic should be encrypted (see the Tenets of ZTA
482 above).

483

484

3 Zero Trust Architecture Logical Components

There are numerous logical components that make up a ZTA network deployment in an enterprise. These components may be operated as an on-premises service or through a cloud-based service. The conceptual framework model in Figure 2 shows the basic relationship of the components and their interactions. Note that this is an ideal model showing logical components and their interactions. From Figure 1, the Policy Decision Point (PDP) is broken down into two logical components: the Policy Engine and Policy Administrator (defined below).

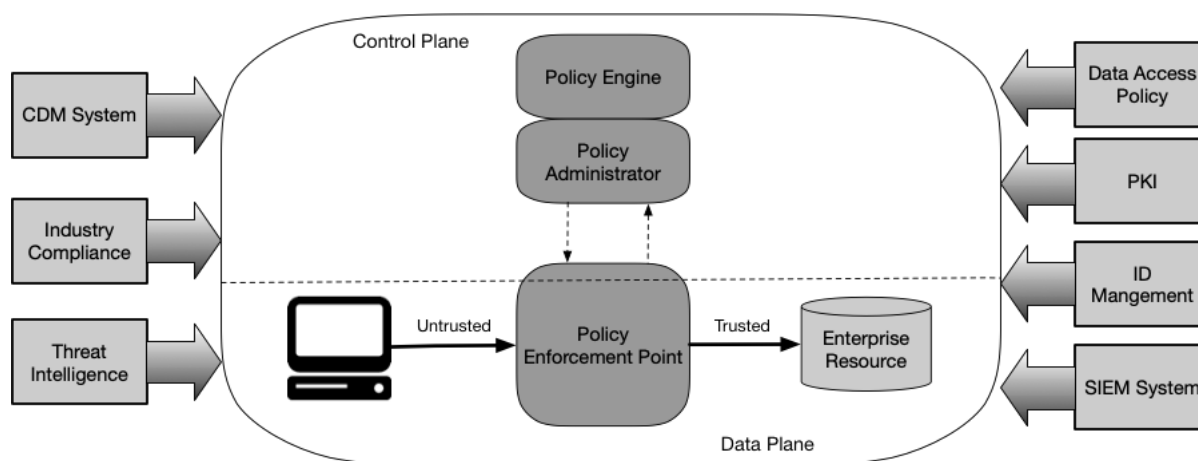


Figure 2: Core Zero Trust Logical Components

The component descriptions:

- Policy Engine (PE):** This component is responsible for the ultimate decision to grant access to a resource for a given client or subject. The Policy Engine uses enterprise policy as well as input from external sources (e.g., IP blacklists, threat intelligence services) as input to a “trust algorithm” to decide to grant or deny access to the resource. The Policy Engine is paired with the Policy Administrator component. The Policy Engine makes (and logs) the decision, and the Policy Administrator executes the decision (approval or denial).
- Policy Administrator (PA):** This component is responsible for establishing the connection between a client and a resource. It would generate any authentication token or credential used by a client to access an enterprise resource. It is closely tied to the Policy Engine and relies on its decision to ultimately allow or deny the connection. Implementations may treat the Policy Engine and Policy Administrator as a single service; here, it is divided into its two logical components. The PA communicates with the Policy Enforcement Point (PEP) when creating the connection. This communication is done via the control plane.
- Policy Enforcement Point (PEP):** This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. This is a single logical component in ZTA but may be broken up into two different components: the client (e.g., agent on user’s laptop) and resource side (e.g., gateway).

515 component in front of resource that controls access) or a single portal component that acts
516 as a gatekeeper for connections.

517 In addition to the core components in an enterprise implementing a ZTA strategy, there are
518 several data sources that provide input and policy rules used by the policy engine when making
519 access decisions. These include local data sources as well as external (i.e., non-enterprise
520 controlled or created) data sources. These include:

- 521 • **Continuous Diagnostics and Mitigation (CDM) System(s):** This system(s) gathers
522 information about the enterprise system's current state and applies updates to
523 configuration and software components. An enterprise CDM system provides the Policy
524 Engine with the information about the system making an access request, such as whether
525 it is running the appropriate patched OS and applications or whether the system has any
526 known vulnerabilities.
- 527 • **Industry Compliance System:** This system ensures that the enterprise remains
528 compliant with any regulatory regime they may fall under (e.g. FISMA, HIPAA, PCI-
529 DSS, etc.). This includes all the policy rules an enterprise develops to ensure compliance.
- 530 • **Threat Intelligence Feed(s):** This system provides information from outside sources that
531 help the Policy Engine make access decisions. These could be multiple services that take
532 data from multiple external sources and provide information about newly discovered
533 attacks or vulnerabilities. This also includes DNS blacklists, discovered malware, or
534 command and control systems that the Policy Engine will want to deny access to from
535 enterprise systems.
- 536 • **Data Access Policies:** This is the set of attributes, rules, and policies about data access
537 created by the enterprise around enterprise resources. This set of rules could be encoded
538 in the Policy Engine or dynamically generated by the PE. These policies are the starting
539 point for granting access to a resource as they provide the basic access privileges for
540 actors and applications in the enterprise. These roles and access rules should be based on
541 user roles and the mission needs of the organization.
- 542 • **Enterprise Public Key Infrastructure (PKI):** This system is responsible for generating
543 and logging certificates issued by the enterprise to resources, actors, and applications.
544 This also includes the global CA ecosystem and the Federal PKI³, which may or may not
545 be integrated with the enterprise PKI.
- 546 • **ID Management System:** This system is responsible for creating, storing, and managing
547 enterprise user accounts and identity records. This system contains the necessary user
548 information (e.g., name, email address, certificates, etc.) and other enterprise
549 characteristics such as role, access attributes, or assigned systems. This system often
550 utilizes other systems (such as a PKI above) for artifacts associated with user accounts.
- 551 • **Security Incident and Event Management (SIEM) System:** The enterprise system that
552 aggregates system logs, network traffic, resource entitlements, and other events that

³ <https://www.idmanagement.gov/topics/fpki/>

553 provide feedback on the security posture of enterprise information systems. This data is
 554 then used to refine policies and warn of possible active attacks against enterprise systems.

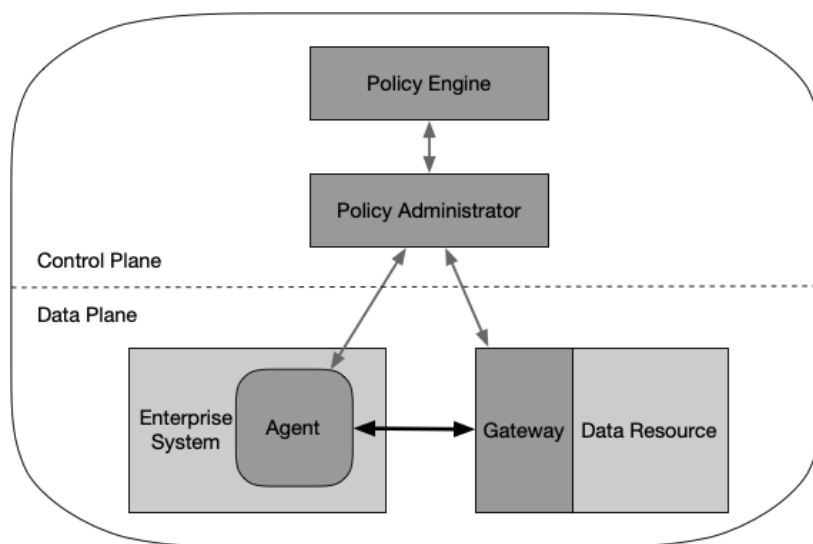
555 3.1 Deployed Variations of the Abstract Architecture

556 All of these components are logical components. They do not necessarily need to be unique
 557 systems. A single system may perform the duties of multiple logical components, and likewise, a
 558 logical component may consist of multiple hardware or software elements to perform the tasks.
 559 For example, an enterprise PKI may consist of one component responsible for issuing certificates
 560 for devices and another used for issuing certificates to end users, but both use intermediate
 561 certificates issued from the same enterprise root certificate authority. In many ZTA network
 562 offerings currently available on the market, the PE and PA components are combined in a single
 563 service.

564 There are several variations on the deployment of selected components of the architecture that
 565 are outlined in the sections below. Depending on how an enterprise network is set up, multiple
 566 ZTA deployment models may be in use for different business processes in one enterprise.

567 3.1.1 Device Agent/Gateway-Based Deployment

568 In this deployment model, the PEP is divided into two components that reside on the resource or
 569 as a component directly in front of a resource. For example, each enterprise-issued system has an
 570 installed device agent that coordinates connections, and each resource has a component (i.e.,
 571 gateway) that is placed directly in front so that the resource only communicates with the
 572 gateway, essentially serving as a reverse proxy for the resource. The gateway is responsible for
 573 connecting to the Policy Administrator and only allows approved connections configured by the
 574 Policy Administrator (see Figure 3).



575

576

Figure 3: Device Agent/Gateway Model

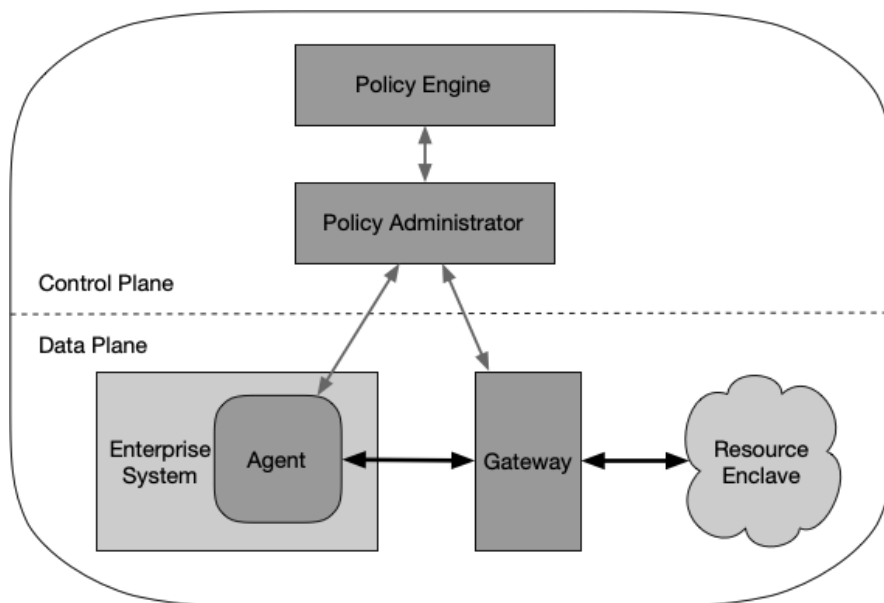
577 In a typical connection scenario, a user with an enterprise-issued laptop wishes to connect to an
 578 enterprise resource (e.g., HR application/database). The connection request is taken by the local
 579 agent, and a connection request is sent to the Policy Administrator. The Policy Administrator
 580 (and Policy Engine) could be an enterprise local system or a cloud-hosted service. The Policy

581 Administrator forwards the request to the Policy Engine for evaluation. If the request is
 582 authorized, the Policy Administrator configures a communication channel between the device
 583 agent and the relevant resource gateway (via the control plane). This may include IP address/port
 584 information, session key, or similar security artifacts. The device agent and gateway then
 585 connect, and encrypted application data flows begin. The connection between the device agent
 586 and resource gateway is terminated when the workflow is completed or when triggered by the
 587 Policy Administrator due to a security event (e.g., session timeout, failure to re-authenticate,
 588 etc.).

589 This model is best utilized for enterprises that have a robust device management program in
 590 place and discrete resources that can communicate with the gateway. For enterprises that heavily
 591 utilize cloud services, this is a client-server implementation of the Cloud Security Alliance
 592 (CSA) Software Defined Perimeter (SDP) [CSA-SDP]. This model is also good for enterprises
 593 that do not want to have a bring-your-own-device (BYOD) policy in place. Access is only
 594 granted via the device agent, which can be placed on enterprise-owned systems.

595 3.1.2 Microperimeter-Based Deployment

596 This deployment model is a variation of the device agent/gateway model above. In this model,
 597 the gateway components may not reside on systems or in front of individual resources but
 598 instead reside at the boundary of a resource enclave (e.g., on-location data center) as shown in
 599 Figure 4. Usually, these resources serve a single business function or may not be able to
 600 communicate directly to a gateway (e.g., legacy database system that does not have an API that
 601 cannot be used to communicate with a gateway). This deployment model may also be useful for
 602 enterprises that use cloud-based microservices for business processes (e.g., user notification,
 603 database lookup, or salary disbursement). In this model, the entire private cloud is located behind
 604 a gateway.



605

606

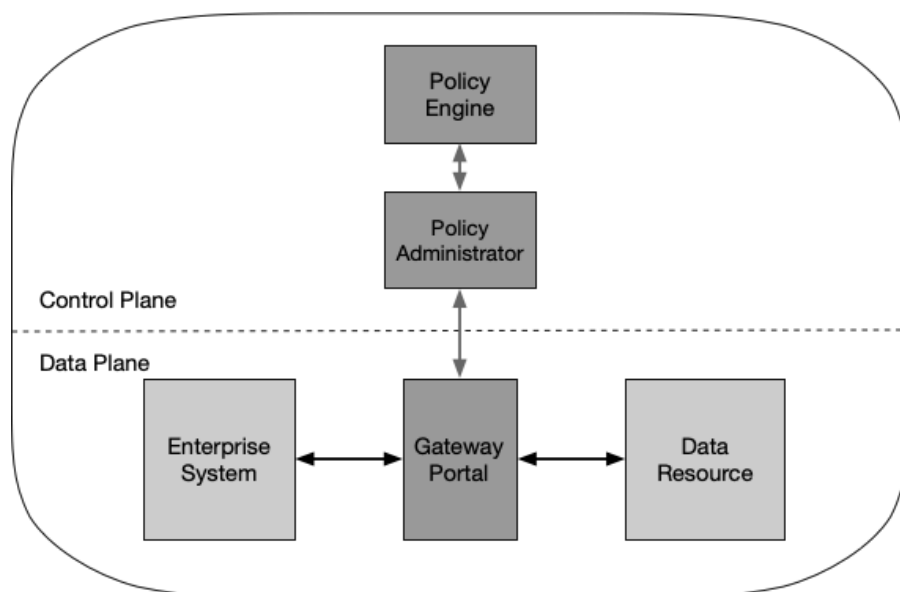
Figure 4: Enclave Gateway Model

607 It is possible for this model to be a hybrid with the device agent/gateway model. In this model,
 608 enterprise systems have a device agent that is used to connect to microperimeter gateways, but
 609 these connections are created using the same process as the basic device agent/gateway model.

610 This model is useful for enterprises that have legacy applications or on-premises data centers that
 611 cannot have individual gateways in place. The enterprise needs to have a robust device
 612 management program in place to install/configure the device agents. The downside is that the
 613 gateway protects a collection of resources and not each resource individually. This is a relaxation
 614 of the ZTA tenet that each resource should have its own PEP protecting it. This may also allow
 615 for clients to see resources for which they do not have privileges to access.

616 3.1.3 Resource Portal-Based Deployment

617 In this deployment model, the PEP is a single component, which acts as a gateway for user
 618 requests. The gateway portal can be for an individual resource or a microperimeter for a
 619 collection of resources used for a single business function. One example would be a gateway
 620 portal into a private cloud or data center containing legacy applications as shown in Figure 5.



621

622

Figure 5: Resource Portal Model

623 The main benefit of this model over the others is that there does not need to be a software
 624 component installed on all enterprise systems. This model is also more flexible for BYOD
 625 policies and inter-organization collaboration projects. Enterprise administrators do not need to
 626 ensure that each device has the appropriate device agent before use. However, limited
 627 information can be inferred from devices requesting access. It can only scan and analyze systems
 628 and devices once they connect to the PEP portal and may not be able to continuously monitor
 629 them for malware and appropriate configuration.

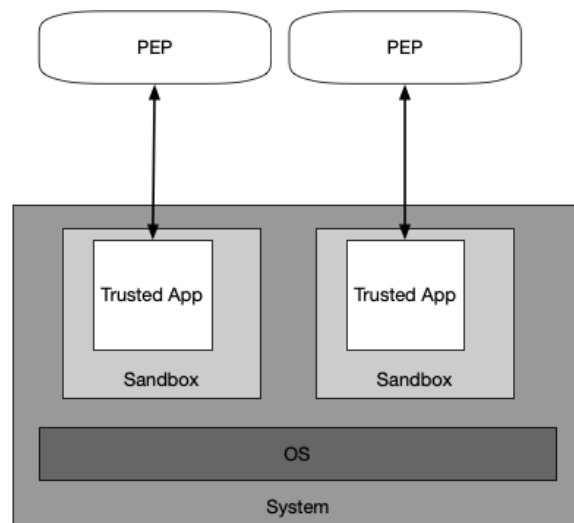
630 The main difference with this model is that there is no local agent that handles requests. This
 631 model allows for more flexibility in client systems and BYOD policies and may make it easier to
 632 grant resource access to non-enterprise collaborators. The disadvantage is that the enterprise may
 633 not have full visibility or control over enterprise-owned systems as they can only see/scan them

634 when they connect to a portal. These systems may be invisible to the enterprise between these
 635 connection sessions. This model also allows for attackers to discover and attempt to access the
 636 portal or attempt a denial-of-service (DoS) attack against the portal.

637 3.1.4 System Application Sandboxing

638 Another variation of the agent/gateway deployment model is having trusted applications run
 639 compartmentalized on systems. These compartments could be VMs, containers, or some other
 640 implementation, but the goal is the same: to protect the application from the host and other
 641 applications running on the system.

642



643

644

Figure 6: Application Sandboxes

645 In Figure 6 above, the user system runs trusted applications in a sandbox. The trusted application
 646 can communicate with the PEP to request access to resources, but the PEP will refuse
 647 connections from other (non-trusted) applications on the system. The PEP could be an enterprise
 648 local service or a cloud service in this model.

649 The main advantage of this model variant is that individual applications are segmented away
 650 from the rest of the system. If the system cannot be scanned for vulnerabilities, these individual
 651 sandboxed applications may be protected from a potential malware infection on the host system.
 652 One of the disadvantages to this model is that enterprises must maintain these sandboxed apps
 653 for all systems and may not have full visibility into client systems.

654 3.2 Trust Algorithm

655 For an enterprise with a ZTA deployment, the Policy Engine can be thought of as the brain and
 656 the PE's trust algorithm its primary thought process. The trust algorithm is the process used by
 657 the Policy Engine to ultimately grant or deny access to a resource. The Policy Engine takes input
 658 from multiple sources: the policy database with information about users, user attributes and
 659 roles, historic user behavior patterns, threat intelligence sources, and other metadata sources. The
 660 process can be visualized in Figure 7.

661

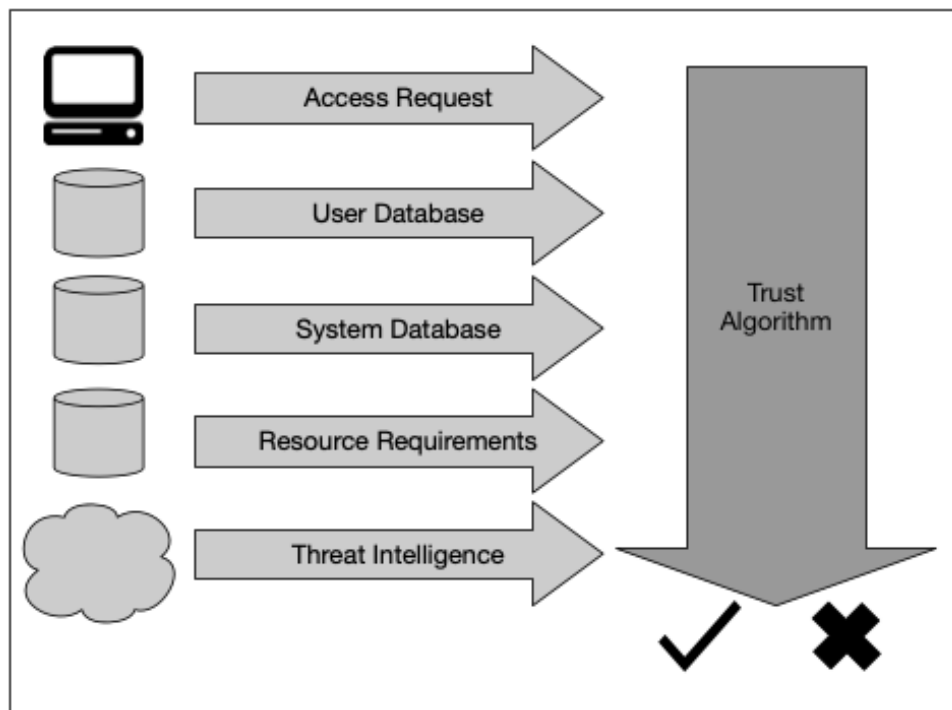
662
663

Figure 7: Trust Algorithm Input

664 In the figure, the inputs can be broken down into categories based on what they provide to the
665 trust algorithm.

- 666
- 667 • **Access request:** The actual request from the application. The resource requested is the
668 primary information used, but information about the requester is also used. This can
669 include OS version, application used, and patch level. Depending on the system state,
670 access to assets might be restricted or denied.
 - 671 • **User identification, attributes, and privileges:** This is the “who” that is requesting
672 access to a resource. This is the set of users (human and processes) of the enterprise and a
673 collection of user attributes developed by the enterprise. These users and attributes form
674 the basis for policies for resource access [SP800-162][NISTIR 7987]. User identities can
675 include a mix of logical identity (e.g., account ID/password), biometric data (e.g.,
676 fingerprints, facial recognition, iris recognition, retina, and odor/scent), and behavior
677 characteristics (e.g., typing rhythm, gait, and voice). Attributes of identity that should be
678 factored into deriving trust scores include time and geolocation. A collection of privileges
679 given to multiple users could be thought of as a role, but privileges should be assigned to
680 a user on an individual basis and not simply because they may fit into a particular role.
681 This should be encoded and stored in an ID management system and policy database.
 - 682 • **System database and observable status:** This is the database containing the known
683 status of each enterprise-owned system (physical and virtual, to some extent). This is
684 compared to the observable status of the system making the request. This can include OS
685 version, application used, location (network location and geolocation), Trusted Platform

685 Module (TPM), and patch level. Depending on the system state, access to assets might be
686 restricted or denied.

- 687 • **Resource access requirements:** This is the complementary set of policies to the user ID
688 and attributes database. This defines the minimal requirements for access to the resource.
689 Requirements may include authenticator assurance levels, such as multifactor
690 authentication (MFA) and network location (e.g., deny access from overseas IP
691 addresses) or requests for system configuration. These requirements should be developed
692 by both the data custodian (i.e., those responsible for the data) and those responsible for
693 the business processes that utilize the data (i.e., those responsible for the mission).
- 694 • **Threat intelligence:** This is an information feed (or feeds) about general threats and
695 active malware operating on the Internet. This can include attack signatures and
696 mitigations. This is the only component that will rarely be under control of the enterprise
697 but most likely a service.

698 The weight of importance for each data source may be a proprietary algorithm or may be
699 configured by the enterprise. These weight values can be used to reflect the importance of the
700 data source to an enterprise.

701 The final determination is then passed to the PA for enforcement. The PA's job is to configure
702 the necessary PEPs to enable the connection. Depending on how the ZTA is deployed, this may
703 involve sending authentication results and connection configuration information to gateways and
704 agents or resource portals. The PA is also responsible for terminating the connection based on
705 policy (e.g., after a timeout, when the workflow has been completed, or due to a security alert).

706 3.2.1 Trust Algorithm Variations

707 There are different ways to implement a ZTA Trust Algorithm (TA). Different implementors
708 may wish to weigh the above factors differently, according to their perceived importance. There
709 are two other major characteristics that can be used to differentiate TAs. The first is how the
710 factors are evaluated, either as binary decisions or weighted parts of a whole "score." The second
711 is how they evaluate requests in relation to other requests by the same user (or application) ID.

- 712 • **Criteria vs. Score-based:** A criteria-based TA assumes a set of qualified attributes that
713 must be met before access is granted to a resource. These criteria are configured by the
714 enterprise and should be independently configured for every resource. Access is granted
715 to a resource only if all the criteria are met. A score-based TA computes a "score" based
716 on values for every data source and enterprise-configured weights. If the score is greater
717 than the configured threshold value for the resource, access is granted. Otherwise, the
718 access is denied.

- 719 • **Singular vs. Contextual:** A singular TA treats each request individually and does not
720 take the user/application history into consideration when making its evaluation. This can
721 allow for faster evaluations, but there is a risk that an attack can go undetected if it stays
722 within a user's allowed role. A contextual TA takes a user's (or network agent's) recent
723 history into consideration when evaluating access requests. This means the PE must
724 maintain some state information of all users and applications but may be more likely to
725 detect an attacker using subverted credentials to access information in a pattern that is
726 atypical of what the PE sees for the given user/agent.

727 The two factors are not dependent on each other. It is possible to have a TA that assigns trust
728 scores to every user and/or device and still considers every access request independently (i.e.,
729 singular). Likewise, a different TA may be score-based but be contextual in that every successful
730 and failed access request could be used to change the ultimate trust score value.

731 Ideally, a ZTA Trust Algorithm should be contextual, but this may not always be possible. This
732 can mitigate threats where an attacker stays close to a “normal” set of access requests for a
733 compromised user account (or insider attack). It is important to balance security, usability, and
734 cost effectiveness when defining and implementing Trust Algorithms. Continually prompting a
735 user for re-authentication against behavior that is consistent with historical trends and norms for
736 their mission function and role within the organization can lead to usability issues. For example,
737 if an employee in the HR department of an agency normally accesses 20-30 employee records in
738 a typical workday, a contextual TA may send an alert if the access requests suddenly exceed 100
739 records in a day as this could be an attacker exfiltrating records using a compromised HR
740 account. This is an example where a contextual TA can detect an attack whereas a singular TA
741 may fail to detect the new behavior. Another example is an accountant who typically accesses
742 the financial system during normal business hours and is now trying to access the system in the
743 middle of the night from an unrecognizable location. A contextual TA may trigger an alert and
744 require the user to satisfy a more stringent score or other criteria as outlined in NIST SP 800-63a
745 [SP800-63A].

746 Developing a set of criteria or weights/threshold values for each resource requires planning and
747 testing. Enterprise administrators may encounter issues during the initial deployment of ZTA
748 where access requests that should be approved are denied due to misconfiguration. This will
749 result in an initial “tuning” phase of deployment. Criteria or scoring weights may need to be
750 adjusted to ensure that the policies are enforced while still allowing the enterprise’s business
751 processes to function.

752 **3.3 Network Components**

753 In a ZTA network, there should be a separation (logical or possibly physical) between
754 communication flows used to control and configure the network and application communication
755 flows used to perform the actual work of the organization. This is often broken down to a *control*
756 *plane* for network control communication and a *data plane* for application communication flows
757 [Gilman].

758 The control plane is used by the various infrastructure components for maintaining systems;
759 judging, granting, or denying access to resources; and performing any necessary operations to set
760 up connections between resources. The data plane is used for the actual communication between
761 applications. This communication channel may not be possible prior to the connection being
762 established via the control plane. For example, the control plane could be used by the PA and
763 PEP to set up the connection between the user and the enterprise resource. The application
764 workload would then use the data plane connection that was established.

765 **3.3.1 Network Requirements to Support ZTA**

766 1. **Enterprise systems have basic network connectivity.** The local network provides basic
767 routing and infrastructure (e.g., DNS, etc.). The remote enterprise system may not
768 necessarily use all infrastructure services.

- 769 2. **The enterprise must be able to determine which systems are owned or managed by**
770 **the enterprise and which devices are not owned or managed.** This is determined by
771 enterprise-issued credentials and not unauthenticated information (e.g., MAC addresses,
772 etc.).
- 773 3. **The enterprise can capture all network traffic.** The enterprise can record packets seen
774 on the data plane but may not be able to perform Deep Packet Inspection (DPI) on all
775 packets. The enterprise can filter out metadata about the connection (e.g., destination,
776 time, device identity, etc.).
- 777 4. **Enterprise resources should not be discoverable without accessing a PEP.** Enterprise
778 resources do not accept arbitrary incoming connections from the Internet. Resources only
779 accept custom configured connections after a client has been authenticated. These
780 connections are set up by the PEP. This prevents attackers from scanning the network to
781 identify targets and launching DoS attacks against resources.
- 782 5. **The Data Plane and Control Plane are logically separate.** The Policy Engine, Policy
783 Administrator, and PEPs communicate on a network that is logically separate and
784 inaccessible by enterprise systems and resources. Enterprise systems use the data plane
785 when performing network tasks. The Policy Engine, Policy Administrator, and PEPs use
786 the control plane to communicate and manage connections between systems. The PEPs
787 must be able to send and receive messages from both the data and control planes.
- 788 6. **Enterprise systems can reach the PEP component.** Enterprise users must be able to
789 access the PEP component on their enterprise ZTA network in order to gain access to
790 resources. This could take the form of a web portal or software agent on the enterprise
791 system that enables the connection.
- 792 7. **The PEP is the only component that can access the Policy Administrator and Policy**
793 **Engine.** Each PEP operating on the enterprise network has a connection to the Policy
794 Administrator in order to establish connections from clients. The PA may be
795 discoverable, but only PEPs are allowed to connect.
- 796 8. **Remote enterprise systems should be able to access enterprise resources without**
797 **needing to traverse through enterprise infrastructure.** For example, a remote user
798 should not be required to use a secure link back to the enterprise network (i.e., VPN) in
799 order to access services utilized by the enterprise and hosted by a public cloud provider
800 (e.g., email).
- 801 9. **Enterprise systems may not be able to reach certain PEPs due to observable factors.**
802 For example, mobile systems may not be able to reach certain resources unless they are
803 using enterprise network infrastructure. These factors could be based on location
804 (geolocation or network location), device type, etc.

805

806 4 Deployment Scenarios/Use Cases

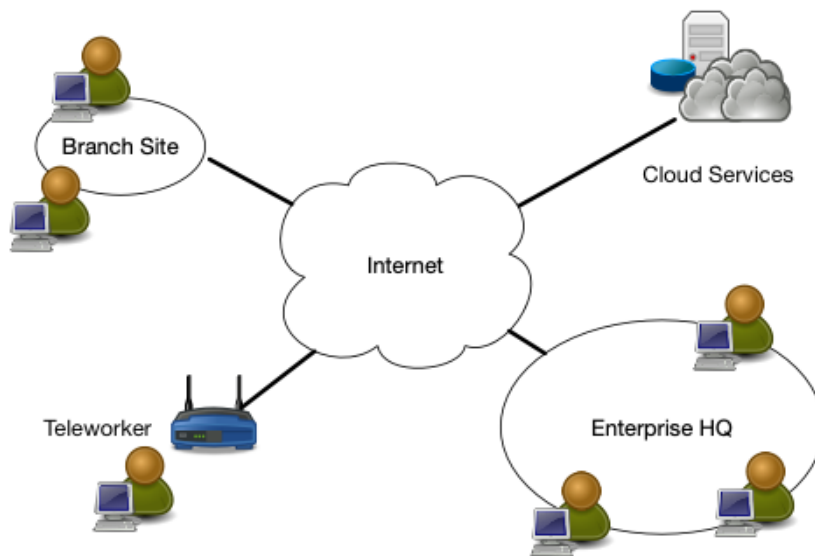
807 Any enterprise network can be designed with zero trust tenets in mind. Most organizations
 808 already have some elements of zero trust in their enterprise infrastructure today or are on their
 809 way through implementation of information security and resiliency policies and best practices.
 810 There are several deployment scenarios and use cases that lend themselves more readily to a zero
 811 trust architecture. For instance, ZTA has its roots in organizations that are geographically
 812 distributed and/or have a highly mobile workforce. That said, any organization that has a sizable
 813 network with multiple resources can benefit from a zero trust architecture.

814 In the use cases below, ZTA is not explicitly indicated, as the enterprise likely has both legacy
 815 and (possibly) ZTA infrastructures. As discussed in Section 7.2, there will likely be a period of
 816 time when ZTA components and legacy network infrastructure are concurrently in operation in
 817 an enterprise.

818 4.1 Enterprise with Satellite Facilities

819 The most common scenario is an enterprise with a single headquarters and one or more
 820 geographically dispersed locations that are not joined by an enterprise-owned physical network
 821 connection (see Figure 8). Employees at the remote location may not have a full enterprise-
 822 owned local network but still need to access enterprise resources in order to perform their tasks.
 823 Likewise, employees may be teleworking or in a remote location using enterprise-owned or
 824 personally-owned devices. In such cases, an enterprise may wish to grant access to some
 825 resources (e.g., employee calendar, email) but deny access to more sensitive resources (e.g., HR
 826 database).

827 In this use case, the PE/PA is best hosted as a cloud service with end systems having a
 828 connection agent (see Section 3.1.1) or accessing a resource portal (see Section 3.1.3). It may not
 829 be most responsive to have the PE/PA hosted on the enterprise local network as remote offices
 830 and workers must send all traffic back to the enterprise network in order to reach cloud services.



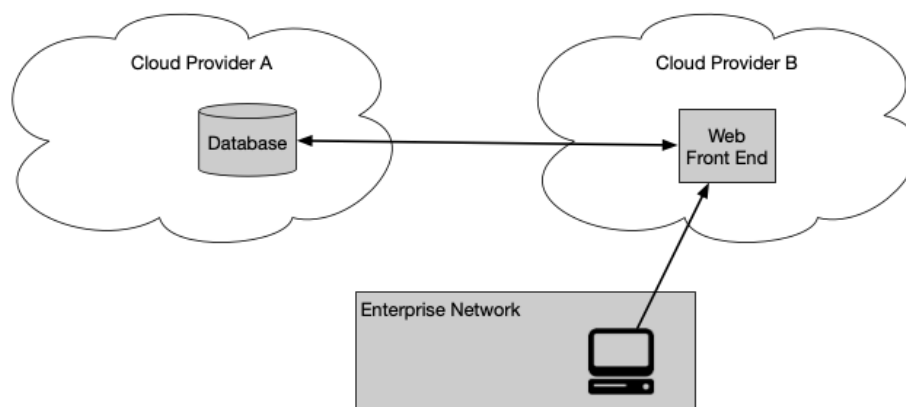
831

832

Figure 8: Enterprise with Remote Employees

833 4.2 Multi-Cloud Enterprise

834 One increasingly common use case for deploying a ZTA strategy is an enterprise utilizing
 835 multiple cloud providers (see Figure 9). In this use case, the enterprise has a local network but
 836 uses two (or more) cloud service providers to host applications and data. Sometimes, the
 837 application is hosted on a separate cloud service than the data source. For performance and ease
 838 of management, the application hosted in Cloud Provider A should be able to connect directly to
 839 the data source hosted in Cloud Provider B rather than force the application to tunnel back
 840 through the enterprise network.



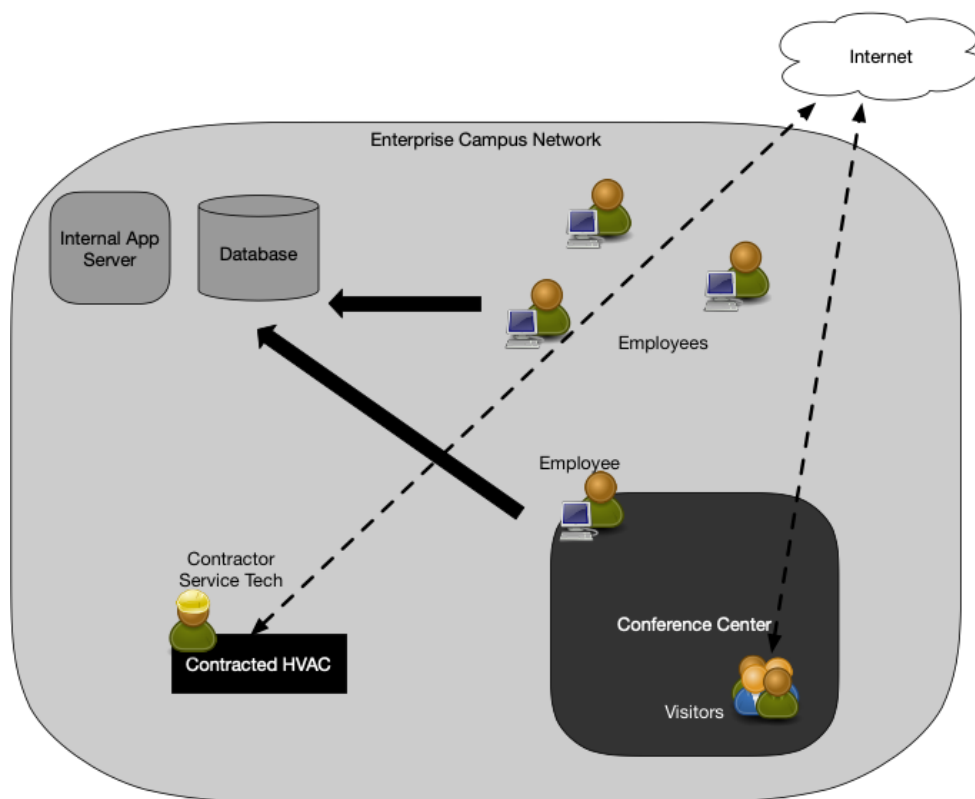
841
842

Figure 9: Multi-Cloud Use Case

843 This multi-cloud use case is one of the main drivers of ZTA adoption. It is the server-server
 844 implementation of the CSA's SDP specification [CSA-SDP]. As enterprises move to more
 845 cloud-hosted applications and services, it becomes apparent that relying on the enterprise
 846 perimeter for security becomes a liability. As discussed in Section 2.2, ZTA takes the view that
 847 there should be no difference between enterprise-owned and operated network infrastructure and
 848 infrastructure owned by any other service provider. The zero trust approach to multi-cloud use is
 849 to place PEPs at the access points of each application and data sources. The PE and PA may be a
 850 service located in either cloud or even on a third cloud provider. The client (via a portal or local
 851 installed agent) then accesses the PEPs directly. That way, the enterprise can still manage access
 852 to resources even when hosted outside of the enterprise.

853 4.3 Enterprise with Contracted Services and/or Non-Employee Access

854 Another common scenario is an enterprise that includes on-site visitors and/or contracted service
 855 providers that require limited access to enterprise resources to do their work (see Figure 10). For
 856 example, an enterprise has its own internal applications, databases, and employee work systems.
 857 These include services contracted out to providers who may occasionally be on-site to provide
 858 maintenance tasks (e.g., a smart HVAC system and lighting system that is owned and managed
 859 by external providers). These visitors and service providers will need network connectivity to
 860 perform their tasks. A ZTA network could facilitate this by allowing these devices (and any
 861 visiting service technician) access to the Internet while obscuring enterprise resources.



862

863

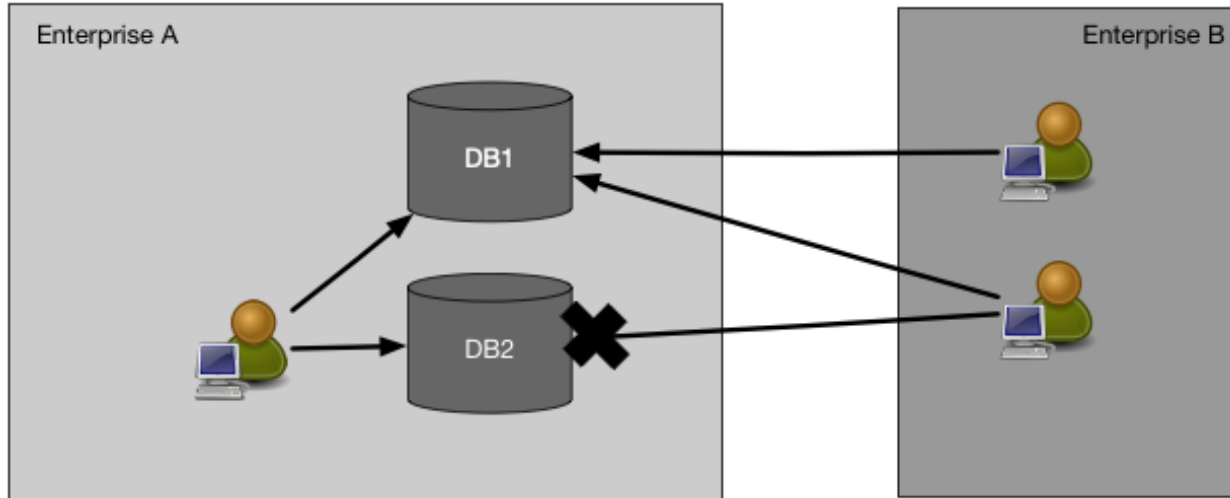
Figure 10: Enterprise with Non-Employee Access

864 In this example the organization also has a conference center where visitors interact with
 865 employees. Again, with a ZTA strategy of SDPs, employee devices and users are differentiated
 866 and may be able to access appropriate enterprise resources. Visitors to the campus can have
 867 Internet access but cannot access enterprise resources. They cannot even conduct network scans
 868 to look for enterprise services that may be visible (i.e., prevent active network reconnaissance).

869 In this use case, the PE and PA could be hosted as a cloud service or on the LAN (assuming little
 870 or no use of cloud-hosted services). The enterprise systems could have an installed agent or
 871 access resources via a portal. The PA ensures all non-enterprise systems (those that do not have
 872 installed agents or cannot connect to a portal) cannot access local resources but may access the
 873 Internet.

874 **4.4 Collaboration Across Enterprise Boundaries**

875 A fourth use case is cross-enterprise collaboration. For example, there is a project involving
 876 employees from Enterprise A and Enterprise B (see Figure 11). The two enterprises may be
 877 separate federal agencies (G2G) or even a federal agency and a private enterprise (G2B).
 878 Enterprise A operates the database used for the project but must allow access to the data for
 879 certain members of Enterprise B. Enterprise A can set up specialized accounts for the employees
 880 of Enterprise B to access the required data and deny access to all other resources.



881

882

Figure 11: Cross-Enterprise Collaboration

883 This scenario can be similar to use case 1 above as employees of both enterprises may not be
 884 located on their organization's network infrastructure, and the resource they need to access may
 885 be within one enterprise network or hosted in the cloud. This means that there do not need to be
 886 complex firewall rules or enterprise-wide ACLs allowing certain IP addresses belonging to
 887 Enterprise B to access resources in Enterprise A. How this access is accomplished depends on
 888 the technology in use. Similar to use case 1, the PE and PA would ideally be hosted as a cloud
 889 service. The employees of Enterprise B may be asked to install a software agent on their system
 890 or access the necessary data resources through a web proxy gateway (see Section 3.1.3).

891

892 **5 Threats Associated with Zero Trust Architecture**

893 No enterprise can completely eliminate cybersecurity risk. When complemented with existing
894 cybersecurity policies and guidance, identity and access management, continuous monitoring,
895 and general cyber hygiene, ZTA can reduce overall risk exposure and protect against common
896 threats. However, there are some threat risks unique to ZTA.

897 **5.1 Subversion of ZTA Decision Process**

898 In ZTA, the Policy Engine and Policy Administrator components are the key components of the
899 entire enterprise. No connection between enterprise resources occurs unless it is approved, and
900 possibly configured, by the PE and PA. This means that these components must be properly
901 configured and maintained. Any enterprise administrator with configuration access to the PE's
902 rules may be able to perform unapproved changes (or make mistakes) that can disrupt enterprise
903 operations. Likewise, a compromised PA could allow access to resources that would otherwise
904 not be approved (e.g., to a subverted personally-owned device). Mitigating associated risks
905 means that the PE and PA components must be properly configured and monitored, and any
906 configuration changes must be logged and subject to audit.

907 **5.2 Denial-of-Service or Network Disruption**

908 In ZTA, the Policy Administrator (PA) is the key component for resource access. Enterprise
909 resources cannot connect to each other without the PA's permission and, possibly, configuration
910 action. If an attacker disrupts or denies access to the PEP or PA (i.e., denial-of-service (DoS)
911 attack), it can adversely impact enterprise operations. It is assumed that most enterprises will
912 mitigate this threat by having the policy enforcement reside in a cloud or be replicated in several
913 locations following guidance on cyber resiliency [SP800-160].

914 This mitigates the risk but does not completely eliminate it. Botnets such as Mirai produce
915 massive DoS attacks against key Internet service providers and disrupt service to millions of
916 Internet users. It is also possible that an attacker could intercept and block traffic to a PEP or PA
917 from a portion (or all) of the user accounts within an enterprise (e.g., a branch office or even a
918 single remote employee). In such cases, only a portion of enterprise users are affected. This is
919 also possible in traditional VPN-based access, as well, and is not unique to ZTA.

920 There is also the possibility of the hosting provider accidentally taking the Policy Administrator
921 offline. Similar to the Amazon S3 outage in February 2017⁴ that prevented access to customers,
922 an operational error could prevent an entire enterprise from functioning if the policy enforcement
923 component becomes inaccessible from the network.

924 There is also the risk that enterprise resources may not be reachable from the PA, so even if
925 access is granted to a user, the PA cannot configure the access connection from the network. This
926 is similar to any other network disruption in that some or all enterprise users cannot access a
927 particular resource due to that resource not being available for some reason.

⁴ <https://aws.amazon.com/message/41926/>

928 **5.3 Insider Threat**

929 Properly implemented ZTA strategies, information security and resiliency policies, and best
930 practices reduce the risk of an insider attack. ZTA does prevent a compromised account or
931 system from accessing resources outside of its normal purview or normal access patterns.
932 Implementation of MFA for network access may also reduce the risk of access from a
933 compromised account. However, just like traditional enterprises, an attacker with valid
934 credentials (or a malicious insider) may still be able to access resources for which the account
935 has been granted access. For example, an attacker (or compromised employee) who has the
936 credentials and enterprise-owned system of a valid human resources employee may still be able
937 to access an employee database.

938 ZTA increases resistance to this attack and prevents any compromised accounts or systems from
939 moving laterally throughout the network. In addition, a contextual Trust Algorithm (see Section
940 3.2.1) is more likely to detect and respond quickly to this attack than in a legacy network. The
941 contextual TA can detect access patterns that are out of normal behavior and deny the
942 compromised account (or insider threat) access to sensitive resources.

943 **5.4 Visibility on the Network**

944 As mentioned in Section 3.3.1, all traffic is inspected and logged on the network and analyzed to
945 identify and react to potential attacks against the enterprise. However, as also mentioned, some
946 (likely the majority) of the traffic on the enterprise network may be opaque to network analysis
947 tools. This traffic may be from non-enterprise-owned systems (e.g., contracted services that use
948 the enterprise infrastructure to access the Internet) or applications that are resistant to passive
949 monitoring. The enterprise cannot perform DPI or examine the encrypted traffic and must use
950 other methods to assess for a possible attacker on the network.

951 That does not mean that the enterprise is unable to analyze encrypted traffic that it sees on the
952 network. The enterprise can collect metadata about the encrypted traffic and use that to detect
953 possible malware communicating on the network or an active attacker. Machine learning
954 techniques [Anderson] can be used to analyze traffic that cannot be decrypted and examined.
955 Employing this type of machine learning would allow the enterprise to categorize traffic as valid
956 or possibly malicious and subject to remediation. In a ZTA deployment, only the traffic from
957 non-enterprise-owned systems would need to be examined as all enterprise traffic is subject to
958 analysis by the Policy Administrator (via the PEPs).

959 **5.5 Storage of Network Information**

960 A related threat to enterprise analysis of network traffic is the analysis component itself. If
961 network traffic and metadata are being stored for further analysis, that data becomes a target for
962 attackers. Just like network diagrams, configuration files, and other assorted network architecture
963 documents, these resources should be protected. If an attacker can successfully gain access to
964 stored traffic information, they may be able to gain insight into the network architecture and
965 identify assets for further reconnaissance and attack.

966 Another source of reconnaissance information for an attacker on a ZT network is the
967 management tool used to encode access policies. Like stored traffic, this component contains
968 access policies to resources and can give an attacker information on which accounts are most
969 valuable to compromise (e.g., the ones that have access to the desired data resources).

970 Like all valuable enterprise data, adequate protections should be in place to prevent unauthorized
971 access and access attempts. As these resources are vital to security, they should have the most
972 restrictive access policies and only be accessible from designated (or dedicated) administrator
973 accounts.

974 **5.6 Reliance on Proprietary Data Formats**

975 ZTA relies on several different data sources in order to make access decisions, including
976 information about the requesting user, system used, enterprise and external intelligence, threat
977 analysis, etc. Often, the systems used to store and process this information do not have a
978 common, open standard on how to interact and exchange information. This can lead to instances
979 where an enterprise is locked into a subset of providers due to interoperability issues. If one
980 provider has a security issue or disruption, an enterprise may not be able to migrate to a new
981 provider without extreme cost (e.g., replacing several systems) or going through a long transition
982 program (e.g., translating policy rules from one proprietary format to another). Like DoS attacks,
983 this risk is not unique to ZTA, but since ZTA is heavily dependent on the dynamic access of
984 information (both enterprise and service providers), disruption can affect the core business
985 functions of an enterprise. To mitigate associated risks, enterprises should evaluate service
986 providers on a holistic basis by taking into consideration factors such as vendor security controls,
987 enterprise switching costs, and supply chain risk management.

988 **5.7 Use of Non-Person Entities (NPE) in ZTA administration.**

989 Artificial Intelligence (AI) and other software-based agents are being deployed to manage
990 security issues on enterprise networks. These components need to interact with the management
991 components of ZTA (e.g., Policy Engine, Policy Administrator, etc.), sometimes in lieu of a
992 human administrator. How these components authenticate themselves in an enterprise
993 implementing a ZTA strategy is an open issue. It is assumed most automated technology systems
994 will use some means to authenticate when using an API to resource components.

995 The associated risk is that an attacker will be able to induce or coerce an NPE agent to perform
996 some task that the attacker does not have privilege to perform. The software agent may have a
997 lower bar for authentication (e.g., API key vs. MFA) to perform administration or security-
998 related tasks compared to a human user. If an attacker can interact with the agent, they could
999 theoretically trick the agent into allowing the attacker greater access or to perform some task on
1000 behalf of the attacker. There is also a potential risk that an attacker can gain access to a software
1001 agent's credentials and impersonate the agent when performing tasks.

1002

1003 **6 Zero Trust Architecture and Existing Federal Guidance**

1004 There are several existing federal policies and guidance that intersect with the planning,
1005 deployment, and operation of a ZTA strategy. These policies do not prohibit an enterprise from
1006 moving to a more zero trust-oriented network strategy but can influence the development of a
1007 zero trust architecture for an agency. When complemented with existing cybersecurity policies
1008 and guidance; identity, credential, and access management (ICAM); continuous monitoring; and
1009 general cyber hygiene, ZTA may reinforce an organization's security posture and protect against
1010 common threats.

1011 **6.1 ZTA and NIST Risk Management Framework**

1012 A ZTA deployment involves developing access policies around acceptable risk to the designated
1013 mission or business process (see Section 7.3.3). It is possible to deny all network access to a
1014 resource and only allow access via a connected terminal, but this is disproportionately restrictive
1015 in most cases. In order for a federal agency to perform its mission, there is an acceptable level of
1016 risk. The risks associated with performing the given mission must be identified, evaluated, and
1017 mitigated. To assist in this, the NIST Risk Management Framework (RMF) was developed.

1018 ZTA planning and implementation may change the authorization boundaries defined by the
1019 enterprise. This is due to the addition of new components (e.g., Policy Engine, Policy
1020 Administrator, and PEPs) and a reduction of the reliance on network perimeter defenses. The
1021 process described in the RMF will not change in a ZTA cybersecurity strategy.

1022 **6.2 ZTA and NIST Privacy Framework**

1023 Protecting the privacy of users and private information (e.g., personally identifiable information
1024 (PII)) is often a prime concern for organizations. Privacy and data protections are included in
1025 compliance programs such as FISMA and HIPAA. Recently, NIST issued a draft Privacy
1026 Framework⁵ for public comment. This document provides a framework to describe privacy risks
1027 and mitigation strategies, as well as a process for an enterprise to identify, measure, and mitigate
1028 risks to user privacy and private information stored and processed by an organization.

1029 Part of the core requirements for ZTA is that an enterprise should inspect and log all traffic on its
1030 network. This includes decrypting traffic as much as possible to enable inspection. Some of this
1031 traffic may contain private information or have associated privacy risks. Organizations will need
1032 to identify any possible risks associated with the interception, scanning, and logging of network
1033 traffic. This may include such things as informing users and obtaining consent (via a login page,
1034 banner, or similar) and educating enterprise users. The NIST Privacy Framework could help in
1035 developing a formal process to identify and mitigate any privacy-related risks to a ZTA network.

1036 **6.3 ZTA and Federal Identity, Credential, and Access Management Architecture** 1037 **(FICAM)**

1038 User provisioning is a key component of ZTA. The Policy Engine cannot determine if attempted
1039 connections are authorized to connect to a resource if the PE has insufficient information to
1040 identify associated users and resources. Strong user provision and authentication policies need to

⁵ NIST Privacy Framework (DRAFT) <https://www.nist.gov/privacy-framework/working-drafts>

1041 be in place before moving to a more zero trust-aligned deployment. Enterprises need to have a
1042 clear set of user attributes and policies that can be used by a PE to evaluate access requests.

1043 Recently, the Office of Management and Budget (OMB) issued M-19-17 on improving identity
1044 management for the Federal Government. The goal of the policy is to develop "...a common
1045 vision for identity as an enabler of mission delivery, trust, and safety of the Nation" [M-19-17].
1046 The memo calls on all federal agencies to form an ICAM office to govern efforts related to
1047 identity issuance and management. Many of these management policies should use the
1048 recommendations in NIST SP 800-63-3, *Digital Identity Guidelines* [SP800-63]. As ZTA is
1049 heavily dependent on precise identity management, any ZTA effort will need to integrate with an
1050 agency's ICAM policy.

1051 **6.4 ZTA and Trusted Internet Connection (TIC)**

1052 TIC is a federal cybersecurity initiative jointly managed by OMB, DHS, and the General
1053 Services Administration (GSA), and is intended to establish a network security baseline across
1054 the Federal Government. Historically, TIC was a perimeter-based cybersecurity strategy which
1055 required agencies to consolidate and monitor their external network connections. Inherent in TIC
1056 1.0 and TIC 2.0 is the assumption that the inside of the perimeter is "trusted," whereas ZTA
1057 assumes that network location does not infer "trust" (i.e., there is no "trust" on an agency's
1058 internal network). TIC 2.0 provides a list of network-based security capabilities (e.g. content
1059 filtering, monitoring, authentication, and others) to be deployed at the TIC Access Point at the
1060 agency's perimeter; many of these capabilities are aligned with ZTA.

1061 TIC 3.0 will be updated to accommodate cloud services and mobile devices [M-19-26]. In TIC
1062 3.0, agencies can define trust zones as low-trust, moderate-trust, and high-trust based on the level
1063 of control, transparency, and verification an agency has over a particular computing
1064 environment, as well as the sensitivity of data associated with that environment. In addition, TIC
1065 3.0 has updated the network-based security capabilities to be applied to multiple policy
1066 enforcement points (PEPs), which are located at the boundary of a trust zone and not at a single
1067 PEP at the agency perimeter. Many of these TIC 3.0 security capabilities directly support ZTA
1068 (e.g., encrypted traffic, default/deny, virtualization security, network and system inventory, and
1069 others). TIC 3.0 defines specific use cases that describe the implementation of trust zones and
1070 security capabilities across specific applications, services, and environments.

1071 TIC 3.0 is focused on network-based security protections, whereas ZTA is a more inclusive
1072 architecture addressing application, user, and data protections. As TIC 3.0 evolves its use cases,
1073 it is likely that a ZTA TIC use case will be developed to define the network protections to be
1074 deployed at ZTA enforcement points.

1075 **6.5 ZTA and EINSTEIN (NCPS – National Cybersecurity Protection System)**

1076 NCPS (aka EINSTEIN) is an integrated system-of-systems that delivers intrusion detection,
1077 advanced analytics, information sharing, and intrusion prevention capabilities to defend the
1078 Federal Government from cyber threats. The goals of NCPS, which align with the overarching
1079 goals of Zero Trust, are to manage cyber risk, improve cyber protection, and empower partners
1080 to secure cyber space. EINSTEIN sensors enable CISA's National Cybersecurity and
1081 Communications Integration Center (NCCIC) to defend federal networks and respond to
1082 significant incidents at federal agencies.

1083 The placement of NCPS sensors is based on a perimeter network defense in the Federal
1084 Government, while Zero Trust Architectures move protections closer to the data and resources. If
1085 ZTA is adopted across the Federal Government, the NCPS implementation would need to
1086 evolve, or new capabilities would need to be deployed to fulfill NCPS objectives. Incident
1087 responders could potentially leverage information from the authentication, traffic inspection, and
1088 logging of agency traffic available to federal agencies that have implemented a Zero Trust
1089 Architecture. Information generated in a ZTA may better inform event impact quantification;
1090 machine learning tools could use ZTA data to improve detection; and additional logs from ZTA
1091 may be saved for after-the-fact analyses by incident responders.

1092 **6.6 ZTA and Continuing Diagnostics and Mitigations (CDM)**

1093 The DHS CDM program is an effort to improve federal agency IT security posture. Key to that
1094 posture is for agencies to have insight into the systems, configuration, and users within an
1095 agency. In order to protect a system, agencies need to set up processes to discover and
1096 understand the basic components and actors on their infrastructure:

- 1097 • **What is connected?** What devices, applications, and services are used by the
1098 organization? This includes observing and improving the security posture of these
1099 artifacts as vulnerabilities and threats are discovered.
- 1100 • **Who is using the network?** Which users are part of the organization or are external and
1101 allowed to access enterprise resources? This includes non-person entities (NPEs) that
1102 may be performing autonomous actions.
- 1103 • **What is happening on the network?** Enterprises need insight into traffic patterns and
1104 messages between systems.
- 1105 • **How is data protected?** The enterprise needs a set policy on how information is
1106 protected at rest and in transit.

1107 Having a strong CDM program is key to the success of ZTA. For example, in order to move to
1108 ZTA, an enterprise must have a complete inventory of both physical and virtual assets. The DHS
1109 CDM program has initiated several efforts to build up the capabilities needed within federal
1110 agencies to move to a ZTA strategy. For example, the DHS Hardware Asset Management
1111 (HWAW) [HWAW] program is an effort to help agencies identify devices on their network
1112 infrastructure in order to deploy a secure configuration. This is similar to the first steps in
1113 developing a roadmap to ZTA. Agencies must have visibility into the systems active on the
1114 network in order to categorize, configure, and monitor its activity.

1115 **6.7 ZTA, Cloud Smart, and the Federal Data Strategy**

1116 The Cloud Smart⁶ strategy, updated Data Center Optimization Initiative [M-19-19] policy, and
1117 the Federal Data Strategy⁷ influence some requirements for agencies when planning a ZTA
1118 strategy for its enterprise. These policies require agencies to inventory and assess how they
1119 collect, store, and access data, both on-premises and in the cloud.

1120 This inventory is critical in determining which business processes and resources would benefit

⁶ Federal Cloud Computing Strategy <https://cloud.cio.gov/strategy/>

⁷ Federal Data Strategy <https://strategy.data.gov/>

1121 from implementing ZTA. Data resources and applications that are primarily cloud-based or
1122 primarily used by remote workers are good candidates for a ZTA approach (see Section 7.3.3)
1123 since the users and resources are located outside of the enterprise network perimeter.

1124 One additional consideration with the Federal Data Strategy is how to make agency data assets
1125 accessible to other agencies or the public. This corresponds with the cross-enterprise
1126 collaboration ZTA use case (see Section 4.4). Agencies using a ZTA for these assets may need to
1127 take collaboration (or publication) requirements into account when developing the strategy.

1128

1129 **7 Migrating to a Zero Trust Architecture**

1130 Implementing a ZTA strategy is a journey rather than a wholesale replacement of infrastructure
1131 or processes. Organizations should seek to incrementally implement zero trust principles, process
1132 changes, and technology solutions that protect its highest value data assets. Most enterprises will
1133 continue to operate in a hybrid zero trust-legacy mode for an indefinite period of time while
1134 continuing to invest in ongoing IT modernization initiatives.

1135 How an enterprise migrates to a ZTA strategy depends on their current cybersecurity posture and
1136 operations. There is a baseline of competence that an enterprise should reach before it becomes
1137 possible to deploy a significant ZTA-focused network [7]. This baseline includes having the
1138 assets, users, and business processes identified and cataloged for the enterprise. The enterprise
1139 needs this information before it can develop a list of ZTA candidate business processes and the
1140 users/systems that are involved for this process.

1141 **7.1 Pure Zero Trust Architecture**

1142 In a green field approach, it would be possible to build a zero trust architecture network from the
1143 ground up. Assuming the enterprise knows the applications and work flows it wants to use for its
1144 operations, it can produce an architecture based on zero trust strategy tenets for those workflows.
1145 Once the workflows are identified, the enterprise can narrow down the components needed and
1146 begin to map how the individual components interact. From that point, it is an engineering
1147 exercise in building the network infrastructure and configuring the components.

1148 In practice, this is rarely a viable option for federal agencies or any organization with an existing
1149 network. However, there may be times when an organization is asked to fulfill a new
1150 responsibility that would require building its own infrastructure. In these cases, it might be
1151 possible to introduce ZT concepts to some degree. For example, an agency may be given a new
1152 responsibility that entails building a new application and database. The agency could design the
1153 newly needed infrastructure around ZT principles, such as having users' trust evaluated before
1154 access is granted, having micro perimeters around new resources, etc. The degree of success
1155 depends on how dependent this new infrastructure is on existing resources (e.g., ID management
1156 systems).

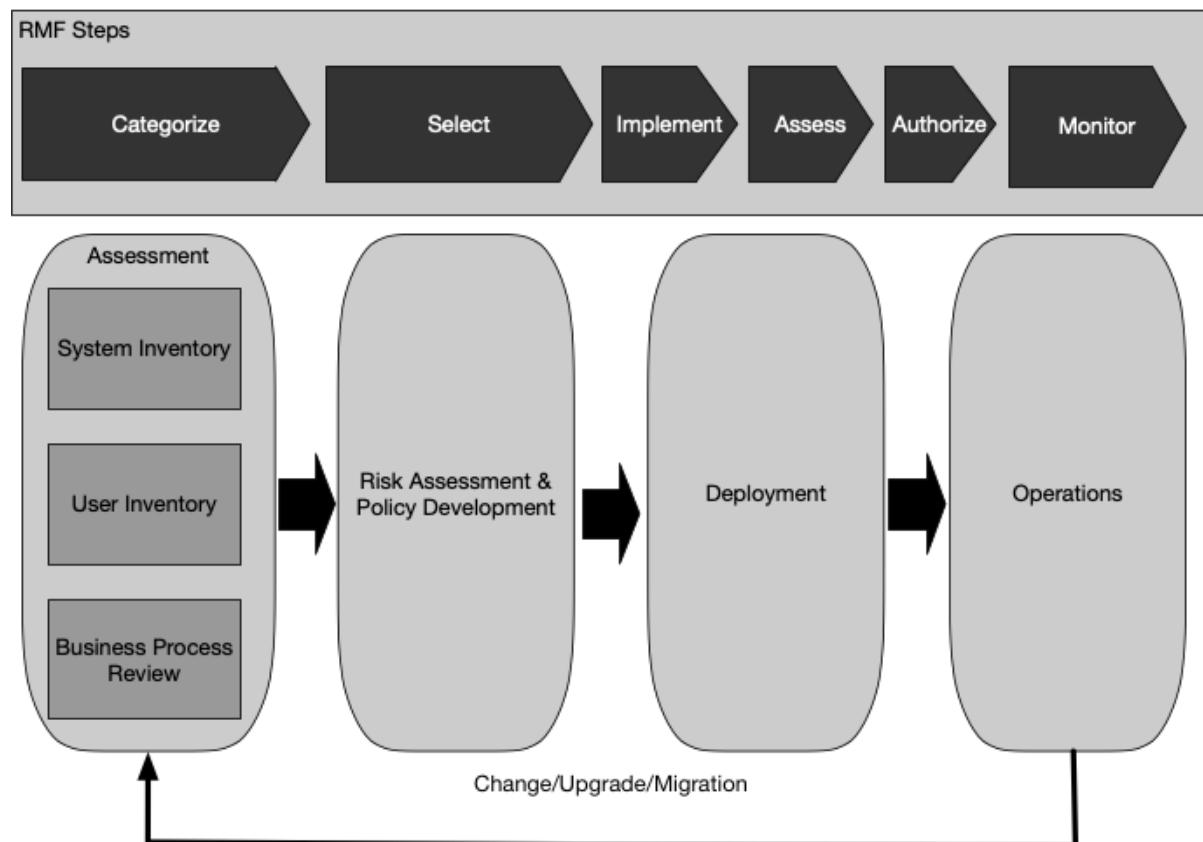
1157 **7.2 Hybrid ZTA and Legacy Architecture**

1158 It is unlikely that any significant enterprise can migrate to a ZTA network in a single technology
1159 refresh cycle. There will be a (perhaps indefinite) period of time when ZTA workflows coexist in
1160 a traditional enterprise. The migration to a ZTA approach to the enterprise may take place one
1161 business process at a time. The enterprise needs to make sure that the common elements (e.g., ID
1162 management, device management, event logging, etc.) are flexible enough to operate in a ZTA
1163 and legacy hybrid security architecture. Enterprise architects may also want to restrict ZTA
1164 candidate solutions to those that can interface with existing components.

1165 **7.3 Steps to Introducing ZTA to a Legacy Architected Network**

1166 Migrating to ZTA requires an organization to have detailed knowledge of its assets (physical and
1167 virtual), users, and business processes. This knowledge is accessed by the PE when evaluating
1168 resource requests. Incomplete knowledge will most often lead to a business process failure where
1169 the PE denies requests due to insufficient information.

1170 Before undertaking an effort to bring ZTA to an enterprise, there should be a survey of assets and
 1171 users. This is the foundation state that must be reached before a ZTA deployment is possible.
 1172 These surveys can be conducted in parallel, but both are tied to an examination of the business
 1173 processes of the organization. These steps can be mapped to the steps in the Risk Management
 1174 Framework (RMF) [SP800-37] as any move to ZTA can be seen as a process to reduce risk to an
 1175 agency's business functions. The pathway to ZTA can be visualized in Figure 12.



1176

1177

Figure 12: ZTA Deployment Cycle

1178 After the initial inventory is created, there is a regular cycle of maintenance and updating. This
 1179 updating may change business processes or not have any impact, but the evaluation of business
 1180 processes should be conducted. For example, a change in digital certificate providers may not
 1181 appear to have a significant impact but may involve certificate root store management,
 1182 Certificate Transparency log monitoring, and other factors that are not apparent at first.

1183 7.3.1 Identify Actors on the Enterprise

1184 In order for a ZTA network to operate, the PE must have knowledge of enterprise subjects.
 1185 “Subjects” encompasses both human and possible non-person entities (NPEs), such as service
 1186 accounts that interact with resources.

1187 Users with special privileges, such as developers or system administrators, need additional
 1188 consideration when being assigned attributes or roles. In a traditional security architecture, these
 1189 accounts may have blanket permission to access all enterprise resources. ZTA should allow for
 1190 developers and administrators to have sufficient flexibility to satisfy their business requirements

1191 while logging and auditing behavior. ZTA deployments may require administrators to satisfy a
1192 more stringent score or criteria as outlined in NIST SP 800-63A, Section 5 [SP800-63A].

1193 **7.3.2 Identify Assets Owned by the Enterprise**

1194 As mentioned in Section 2.1, one of the key requirements of ZTA is the ability to identify and
1195 manage enterprise-owned devices. ZTA also requires the ability to identify and monitor non-
1196 enterprise owned devices that may be on enterprise-owned network infrastructure or that access
1197 enterprise resources. The ability to manage enterprise assets is key to the successful deployment
1198 of ZTA. This includes hardware components (e.g. laptops, phones, IoT devices, etc.) and digital
1199 artifacts (e.g., user accounts, applications, digital certificates, etc.).

1200 This goes beyond simply cataloging and maintaining a database of enterprise assets. This also
1201 includes configuration management and monitoring. The ability to observe the current state of a
1202 system is part of the process of evaluating access requests (see Section 2.1). This means that the
1203 enterprise must have the ability to configure, survey, and update enterprise systems, including
1204 virtual systems, containers, etc. This also includes both its physical (as best estimated) and
1205 network location. This information should inform the PE when making resource access
1206 decisions.

1207 Non-enterprise-owned assets should also be cataloged to the best extent possible. This may
1208 include whatever is visible by the enterprise (e.g., MAC address, network location) and
1209 augmented by administrator data entry. This information is not just used for access decisions (as
1210 collaborator and BOYD systems may need to contact PEPs) but for monitoring by the enterprise.

1211 Many federal agencies have already begun the task of identifying enterprise assets. Agencies that
1212 have established CDM capabilities such as Hardware Asset Management (HWAM) [HWAM]
1213 and Software Asset Management (SWAM) [SWAM] have a rich set of data to draw from when
1214 enacting a ZTA strategy. Agencies may also have a list of ZTA candidate processes that involve
1215 High Value Assets (HVA) [M-19-03] that have been identified as key to the agency mission.
1216 This work would need to exist enterprise or agency-wide before any business process could be
1217 (re-)designed with a ZTA strategy. These programs must be designed to be expandable and
1218 adaptable to changes in the enterprise, not just when migrating to ZTA but to account for new
1219 systems, services, and business processes that become part of the enterprise.

1220 **7.3.3 Identify Key Processes and Evaluate Risks Associated with Executing Process**

1221 The third inventory that an agency should undertake is to identify and rank the business
1222 processes (i.e., missions) of the agency. Business processes should inform the circumstances
1223 under which resource access requests are granted and denied. An enterprise may wish to start
1224 with a low risk business process for the first transition to ZTA as disruptions will likely not
1225 negatively impact the entire organization. Once enough experience is gained, more critical
1226 business processes can become candidates.

1227 Business processes that utilize cloud-based resources or are used by remote workers are often
1228 good candidates for ZTA. This is because the clients and resources are outside of the enterprise
1229 perimeter, one of the main advantages of ZTA over legacy enterprise network architecture.
1230 Rather than project the enterprise perimeter into the cloud or bring clients into the enterprise
1231 network via a Virtual Private Network (VPN), enterprise clients can request cloud services

1232 directly. The enterprise’s PEPs ensure that enterprise policies are followed before resource
1233 access is granted to a client.

1234 **7.3.4 Formulating Policies for the ZTA Candidate**

1235 The process of identifying a candidate application or business workflow depends on several
1236 factors: the importance of the process to the organization, the group of users affected, and the
1237 current state of resources used for the workflow. The value of the asset or workflow based on
1238 risk to the asset or workflow can be evaluated using the NIST Risk Management Framework
1239 [SP800-37].

1240 After the asset or workflow is identified, the next step is to identify the user set that would be
1241 affected. This may influence the candidate choice as a first migration to ZTA. An application
1242 used by an identified subset of enterprise users (e.g., a purchasing system) may be preferred over
1243 one vital to the entire user base of the enterprise (e.g., email).

1244 The enterprise administrators then need to determine the set of criteria (if using a criteria-based
1245 TA) or trusted score weights (if using a score-based TA) for the resources used in the candidate
1246 business process (see Section 3.2.1). Administrators may need to make adjustments to these
1247 criteria or values during the tuning phase. These adjustments are necessary to make sure policies
1248 are effective but do not hinder necessary access to resources.

1249 **7.3.5 Identifying Candidate Solutions**

1250 Once a list of candidate business processes has been developed, enterprise architects can
1251 compose a list of candidate solutions. Some deployment models (see Section 3.1) are better
1252 suited to particular workflows and current enterprise ecosystems. Likewise, some vendor
1253 solutions are better suited to particular use cases than others. Some factors to take into
1254 consideration are:

- 1255 • **Does the solution require that components be installed on the client system?** This
1256 may limit business processes where non-enterprise-owned systems are used or desired,
1257 such as BYOD or cross-agency collaborations.
- 1258 • **Does the solution work where the business process resources exist entirely on
1259 enterprise premises?** Some solutions assume requested resources will reside in the cloud
1260 (so-called “north-south” traffic) and not within an enterprise perimeter (“east-west”
1261 traffic). The location of candidate business process resources will influence candidate
1262 solutions as well as the ZTA for the process.

1263 One solution is to model an existing business process as a pilot program and not just as a
1264 replacement. This pilot program could be made general to apply to several business processes or
1265 specific to one use case. The pilot can be used as a “proving ground” for ZTA before
1266 transitioning users to the ZTA deployment and away from the traditional process infrastructure.

1267 **7.3.6 Initial Deployment and Monitoring**

1268 Once the candidate workflow and ZTA components are chosen, the initial deployment can start.
1269 Enterprise administrators must implement the developed policies using the selected components
1270 but may wish to make them more lenient at first. Few enterprise policy sets are complete in their
1271 first iterations: important user accounts (e.g., administrator accounts) may be denied access to

1272 resources they need or may not need all the access privileges they have assigned.

1273 The new ZT business workflow could be operated in “reporting only mode” for some time to
1274 make sure the policies are effective and workable. “Reporting only” means that access should be
1275 granted for most requests, and logs and traces of connections should be compared to the initial
1276 developed policy. Basic policies such as denying requests that fail MFA or appear from known,
1277 blacklisted IP addresses should be enforced and logged, but after initial deployment, access
1278 polices should be more lenient to collect data on actual interactions of the ZT workflow. If it is
1279 not possible to operate in a more lenient nature, enterprise network operators should monitor logs
1280 closely and be prepared to modify access policies based on operational experience.

1281 **7.3.7 Expanding the ZTA**

1282 After enough confidence is gained in the workflow policy set, the enterprise enters the steady
1283 operational phase. The network and systems are still monitored, and traffic is logged (see Section
1284 2.2.1), but responses and policy modifications are done at a lower tempo as they should not be
1285 severe. At this stage, the enterprise administrators can begin planning the next phase of ZT
1286 deployment. Like the previous rollout, a candidate workflow and solution set need to be
1287 identified and initial policies developed.

1288 However, if a change occurs to the workflow, the operating ZT architecture needs to be
1289 reevaluated. Significant changes to the system—such as new devices, major updates to software
1290 (especially ZT logical components), or shifts in organizational structure—may result in changes
1291 to the workflow or policies. In effect, the entire process should be reconsidered with the
1292 assumption that some of the work has already been done. For example, new devices have been
1293 purchased, but no new user accounts have been created, so only the device inventory needs to be
1294 updated.

1295 **References**

- [ACT-IAC] American Council for Technology and Industry Advisory Council (2019) *Zero Trust Cybersecurity Current Trends*. Available at <https://www.actiac.org/zero-trust-cybersecurity-current-trends>
- [Anderson] Anderson B, McGrew D (2017) Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM, Halifax, Nova Scotia, Canada), pp 1723-1732. <https://doi.org/10.1145/3097983.3098163>
- [CSA-SDP] Cloud Security Alliance (2015) SDP Specification 1.0. April 2015. <https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/>
- [Gilman] Gilman E, Barth D (2017) *Zero Trust Networks: Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., Sebastopol, CA), 1st Ed.
- [HWAM] Department of Homeland Security (2015) *Hardware Asset Management (HWAM) Capability Description*. Available at https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf
- [JERICHO] The Jericho Forum (2007) *Jericho Forum Commandments*, version 1.2. Available at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf
- [M-19-03] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. Available at <https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf>
- [M-19-17] Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf>
- [M-19-19] Office of Management and Budget (2019) Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019. Available at https://datacenters.cio.gov/assets/files/m_19_19.pdf
- [M-19-26] Office of Management and Budget (2019) Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB

Memorandum M-19-26, September 12, 2019. Available at <https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf>

- [NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W (2015) Policy Machine: Features, Architecture, and Specification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. <https://doi.org/10.6028/NIST.IR.7987r1>
- [SP800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- [SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of December 1, 2017. <https://doi.org/10.6028/NIST.SP.800-63-3>
- [SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of December 1, 2017. <https://doi.org/10.6028/NIST.SP.800-63A>
- [SP800-160] Ross R, Pillitteri V, Graubart R, Bodeau D, and McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), Final Public Draft NIST Special Publication (SP) 800-160, Vol. 2. Available at <https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft>
- [SP800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of February 25, 2019. <https://doi.org/10.6028/NIST.SP.800-162>
- [SWAM] Department of Homeland Security (2015) *Software Asset Management (SWAM) Capability Description*. Available at https://www.us-cert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

1298

Appendix A—Acronyms

CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
NIST	National Institute of Standards and Technology
PA	Policy Administrator
PE	Policy Engine
PEP	Policy Enforcement Point
RMF	NIST Risk Management Framework
SIEM	Security Incident and Event Monitoring
ZTA	Zero Trust Architecture
ZTE	Zero Trust Ecosystem

1299

1300 **Appendix B—Identified Gaps in the Current State-of-the-Art in ZTA**

1301 The current maturity of zero trust components and solutions was surveyed during the background
 1302 research in producing this document. This survey concluded that the current state of the ZTA
 1303 ecosystem is not mature enough for widespread adoption. While it is possible to use ZTA
 1304 strategies to plan and deploy an enterprise network, there is no single solution that provides all
 1305 the necessary components. Also, few ZTA components available today can be used for all of the
 1306 various workflows present in an enterprise.

1307 The following is a summary of identified gaps in the ZTA ecosystem and areas that need further
 1308 investigation. Some of these areas have some foundation of work, but how ZTA tenets change
 1309 these areas is not well-known as there is not enough experience with diverse ZTA-focused
 1310 enterprise networks.

1311 **B.1 Technology Survey**

1312 Multiple vendors were invited to present their products and views on zero trust. The goal of this
 1313 survey was to identify missing pieces that prevent agencies from moving to a ZTA infrastructure
 1314 now or maintaining an existing ZTA deployment. These gaps can be categorized into immediate
 1315 deployment (immediate or short term), systemic gaps that affect maintenance or operations
 1316 (short or mid-term), and missing knowledge (areas for future research). They are summarized in
 1317 Table B-1:

1318 **Table B-1: Summary of Identified Gaps**

Category	Example Questions	Identified Gaps
Immediate	<ul style="list-style-type: none"> • How to write procurement requirements • How a ZTA strategy works with TIC, FISMA, etc. 	<ul style="list-style-type: none"> • Lack of a common framework and vocabulary for ZTA • Perception that ZTA is in conflict with existing policy
Systemic	<ul style="list-style-type: none"> • How to prevent vendor lock-in • How different ZTA environments interact 	<ul style="list-style-type: none"> • Too much reliance on vendor APIs
Research Areas	<ul style="list-style-type: none"> • How threats will evolve in the face of ZTA • How business processes change in the face of ZTA 	<ul style="list-style-type: none"> • What a successful compromise looks like in an enterprise with a ZTA • End user experience in an enterprise with a ZTA

1319

1320 **B.2 Gaps that Prevent Immediate Move to ZTA**

1321 These are the issues that are slowing down the adoption of a ZTA strategy at present. These were
1322 classified as “immediate” issues, and no thought of future maintenance or migration were
1323 considered for this category. Forward-thinking enterprise may also consider the maintenance
1324 category to be of immediate concern in preventing the initial deployment of ZTA components,
1325 but they are considered a separate category for this analysis.

1326 **B.2.1 Lack of Common Terms for ZTA Design, Planning, and Procurement**

1327 Zero trust as a strategy for the design and deployment of enterprise infrastructure is still a
1328 forming concept. Industry has not yet coalesced around a single set of terms or concepts to
1329 describe ZTA components and operations. This makes it very difficult for organizations (e.g.,
1330 federal agencies) to develop coherent requirements and policies for designing ZTA infrastructure
1331 and procuring components.

1332 The driver for Section 2.1 and Section 3.1 is an initial attempt to form a neutral base of terms and
1333 concepts to describe ZTA. The abstract ZTA components and deployment models were
1334 developed to serve as basic terms and ways to think about ZTA. The goal is to provide a
1335 common way to view, model, and discuss ZTA solutions when developing enterprise
1336 requirements and performing market surveys. The above sections may prove to be incomplete as
1337 more experience is gained with ZTA strategies in federal agencies, but they currently serve as a
1338 base for a common conceptual framework.

1339 **B.2.2 Perception that ZTA is in Conflict with Existing Federal Cybersecurity Policies**

1340 There is a misconception that ZTA is a single framework with a set of solutions that are
1341 incompatible with the existing view of cybersecurity. Zero trust should actually be viewed as an
1342 evolution of current cybersecurity strategies as many of the concepts and ideas have been
1343 circulating for a long time. Federal agencies have been encouraged to take a more zero trust
1344 approach to cybersecurity through existing guidance (see Section 6). If an agency has a mature
1345 ID management system and robust CDM capabilities in place, it is on the road to a ZTA strategy
1346 (see Section 7.3). This gap is based on a misconception of ZTA and how it has evolved from
1347 previous cybersecurity paradigms.

1348 **B.3 Systemic Gaps that Impact ZTA**

1349 These are the gaps that affect initial implementation and deployment of ZTA strategies and
1350 continued operation/maturity. These gaps could slow the adoption of ZTA strategies in agencies
1351 or result in a fragmentation of the ZTA component industry. Systemic gaps are areas where open
1352 standards (produced either by a Standards Development Organization (SDO) or industry
1353 consortium) can help.

1354 **B.3.3 Standardization of Interfaces Between Components**

1355 During the technology survey, it became apparent that no one vendor provides a single solution
1356 that will provide zero trust. Furthermore, it might not be desirable to use a single vendor solution

1357 to achieve zero trust and risk “vendor lock-in.” This leads to the issue of interoperability within
1358 components, not only at the time of purchase but over time.

1359 The spectrum of components within the wider Zero Trust Ecosystem (ZTE) is vast, with many
1360 products focusing on a single niche within ZTE and relying on other products to provide either
1361 data or some service to another component (e.g., integration of multi-factor authentication
1362 (MFA) for resource access). Vendors too often rely on proprietary APIs provided by partner
1363 companies rather than standardized, vendor-independent APIs to achieve this integration. The
1364 problem with this approach is that these APIs are proprietary and single-vendor-controlled. The
1365 controlling vendor can change the API behavior, and integrators are required to update their
1366 products in response. This requires close partnerships between communities of vendors to assure
1367 early notification of modifications within APIs which may affect compatibility between
1368 products. This adds further burden on vendors and consumers: vendors need to expend resources
1369 to make changes to their products, and consumers need to apply updates to multiple products
1370 when one vendor makes a change to their proprietary API. Additionally, vendors are required to
1371 implement and maintain wrappers for each partner component to allow for maximum
1372 compatibility and interoperability. For example, many MFA product vendors are required to
1373 create a different wrapper for each cloud provider or identity management system in order to be
1374 usable in different kinds of client combinations.

1375 On the customer side, this generates additional problems when developing requirements for
1376 purchasing products. There are no standards that purchasers can rely on to identify compatibility
1377 between products. Hence, it is very difficult to create a multi-year roadmap for moving into ZTA
1378 since it is impossible to identify a minimum set of compatibility requirements for components.

1379 **B.3.4 Emerging Standards that Address Overreliance on Proprietary APIs**

1380 As there is not a single solution to deploying a ZTA strategy, there is no single set of tools or
1381 services for a zero trust architecture. Thus, it is impossible to have a single protocol or
1382 framework that enables an enterprise to move to a ZTA strategy. Currently, there are a wide
1383 variety of models and solutions seeking to become the leading authority of ZTA.

1384 This indicates that there is an opportunity for a set of open, standardized protocols (or
1385 frameworks) to be developed to aid organizations in migrating to a ZTA strategy. Standards
1386 Development Organizations (SDOs) like the Internet Engineering Task Force (IETF) have
1387 specified protocols that may be useful in exchanging threat information (called XMPP-Grid [1]).
1388 The Cloud Security Alliance (CSA) has produced a framework for Software Defined Perimeter
1389 (SDP) [2] that may also be useful in ZTA. Efforts should be directed toward surveying the
1390 current state of ZTA-related frameworks or the protocols necessary for a useful ZTA strategy
1391 and toward identifying places where work is needed to produce or improve these specifications.

1392 **B.4 Knowledge Gaps in ZTA and Future Areas of Research**

1393 The gaps listed here do not hinder an organization from adopting a ZTA strategy for their
1394 enterprise. These are gray areas in knowledge about operational ZTA environments. Most are
1395 due to a lack of time and experience with mature, zero trust deployments. These are areas of
1396 future work for researchers.

1397 **B.4.5 Attacker Response to ZTA**

1398 A properly implemented ZTA strategy for an enterprise will improve its cybersecurity posture
1399 over legacy network perimeter-based security. The tenets of ZTA aim to reduce the exposure of
1400 resources to attackers and minimize (or prevent) lateral movement within an enterprise should a
1401 host system be compromised.

1402 However, determined attackers will not sit idle but will, instead, change behavior in the face of
1403 ZTA. The open issue is how the attacks will change. One possibility is that attacks aimed at
1404 stealing credentials (e.g., phishing, social engineering) could become more prevalent as one of
1405 the main tenets of ZTA is frequent authentication before accessing resources. Another possibility
1406 is that in a hybrid ZTA/legacy enterprise, attackers will focus on the business processes that have
1407 not had ZTA tenets applied (i.e., follow traditional network perimeter-based security)—in effect,
1408 targeting the low-hanging fruit in an attempt to gain some foothold in the ZTA business process.

1409 As ZTA matures, more deployments are seen, and experience gained, the effectiveness of ZTA
1410 over older methods of network perimeter-based security may become apparent. The metrics of
1411 “success” of ZTA over older cybersecurity strategies will also need to be developed.

1412 **B.4.6 User Experience in a ZTA Environment**

1413 There has not been a rigorous examination of how end users act in an enterprise using a ZTA
1414 strategy. This is mainly due to the lack of large ZTA use cases available for studies. There have
1415 been studies on how users react to MFA and other security operations that are seen as part of a
1416 ZTA enterprise strategy. This work could form the basis of predicting end user experience and
1417 behavior when using ZTA workflows in an enterprise.

1418 One set of studies that can predict how ZTA affects end user experience is the work done on the
1419 use of MFA in enterprises and “security fatigue.” Security fatigue [3] is the phenomenon
1420 wherein end users are confronted with so many security policies and challenges that it begins to
1421 impact their productivity in a negative way. Other studies show that MFA may alter user
1422 behavior, but the overall change is mixed [4] [5]. Some users readily accept MFA if the process
1423 is streamlined and involves devices they are used to using or having with them (e.g., apps on a
1424 smartphone). However, some users resent having to use personally-owned devices for business
1425 processes or feel that they are being constantly monitored for possible violations of IT policies.

1426 **B.4.7 Resilience of ZTA to Enterprise and Network Disruption**

1427 The survey of the ZTA vendor ecosystem displayed the wide range of infrastructure that an
1428 enterprise deploying a ZTA strategy would need to consider. As previously noted, there was no
1429 one single provider of a full zero trust solution. As a result, enterprises will purchase several
1430 different services and products. This can lead to a web of dependencies for components. If one
1431 vital component is disrupted or unreachable, there could be a cascade of failures that impact one
1432 or multiple business processes.

1433 Most products and services surveyed relied on a cloud presence to provide robustness, but even
1434 cloud services have been known to become unreachable either through an attack or simple error.
1435 When this happens, key components used to make access decisions may be unreachable or may

1436 not be able to communicate with other components. For example, PE and PA components
1437 located in a cloud may be reachable during a distributed denial-of-service (DDoS) attack but may
1438 not be able to reach all PEPs located with resources. There will need to be research on
1439 discovering possible “choke points” of ZTA deployment models and the impact on network
1440 operations when a ZTA component is unreachable or has limited reachability.

1441 The Continuity of Operations (COOP) plans for an enterprise will likely need revision when
1442 adopting a ZTA strategy. A ZTA strategy makes many COOP factors easier as remote workers
1443 may have the same access to resources as they had on premises. However, policies like MFA
1444 may also have a negative impact if users are not properly trained and lack experience. Users may
1445 forget (or not have access to) tokens and enterprise devices during an emergency, and that will
1446 impact the speed and effectiveness of enterprise business processes.

1447 **B.5 ZTA Test Environment**

1448 TBD – describe NCCoE test lab and tests to be performed

1449 **B.6 References**

- [1] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. <https://doi.org/10.17487/RFC8600>
- [2] Software Defined Perimeter Working Group “SDP Specification 1.0” Cloud Security Alliance. April 2014. <https://cloudsecurityalliance.org/artifacts/software-defined-perimeter/>
- [3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. *IT Professional* 18(5):26-32. <https://doi.org/10.1109/MITP.2016.84>
- [4] Strouble D, Shechtman GM, Alsop AS (2009) Productivity and Usability Effects of Using a Two-Factor Security System. *S AIS 2009 Proceedings* (AIS, Charleston, SC), p 37. Available at <http://aisel.aisnet.org/sais2009/37>
- [5] Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)* (ACM, Orlando, FL), pp 212-224. <https://doi.org/10.1145/3134600.3134629>

1450