

1  
2  
3  
4  
5  
6  
7  
8  
9

**NIST Special Publication  
NIST SP 800-215 ipd**

# **Guide to a Secure Enterprise Network Landscape**

Initial Public Draft

Ramaswamy Chandramouli

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-215.ipd>

10  
11  
  
12  
13  
14  
15  
  
16  
17  
18  
19  
  
20  
21  
  
22  
  
23  
24  
25  
26  
27

**NIST Special Publication  
NIST SP 800-215 ipd**

**Guide to a Secure Enterprise  
Network Landscape**

Initial Public Draft

Ramaswamy Chandramouli  
*Computer Security Division  
Information Technology Laboratory*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-215.ipd>

August 2022



U.S. Department of Commerce  
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology  
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

28 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an  
29 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or  
30 endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the  
31 entities, materials, or equipment are necessarily the best available for the purpose.

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

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

#### 41 **Authority**

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

48  
49 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding  
50 on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be  
51 interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or  
52 any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and  
53 is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

#### 54 **NIST Technical Series Policies**

55 [Copyright, Fair Use, and Licensing Statements](#)  
56 [NIST Technical Series Publication Identifier Syntax](#)

#### 57 **Publication History**

58 Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]

#### 59 **How to Cite this NIST Technical Series Publication:**

60 Chandramouli R (2022) Guide to a Secure Enterprise Network Landscape. (National Institute of Standards and  
61 Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-215 ipd.  
62 <https://doi.org/10.6028/NIST.SP.800-215.ipd>

#### 63 **NIST Author ORCID iDs**

64 Ramaswamy Chandramouli: 0000-0002-7387-5858

#### 65 **Public Comment Period**

66 August 5, 2022 – September 19, 2022

67 **Submit Comments**

68 [sp800-215-comments@nist.gov](mailto:sp800-215-comments@nist.gov)

69

70 National Institute of Standards and Technology

71 Attn: Computer Security Division, Information Technology Laboratory

72 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

## 74 **Reports on Computer Systems Technology**

75 The Information Technology Laboratory (ITL) at the National Institute of Standards and  
76 Technology (NIST) promotes the U.S. economy and public welfare by providing technical  
77 leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test  
78 methods, reference data, proof of concept implementations, and technical analyses to advance  
79 the development and productive use of information technology. ITL’s responsibilities include the  
80 development of management, administrative, technical, and physical standards and guidelines for  
81 the cost-effective security and privacy of other than national security-related information in  
82 federal information systems. The Special Publication 800-series reports on ITL’s research,  
83 guidelines, and outreach efforts in information system security, and its collaborative activities  
84 with industry, government, and academic organizations.

## 85 **Abstract**

86 Access to multiple cloud services, the geographic spread of enterprise IT resources (including  
87 multiple data centers), and the emergence of microservices-based applications (as opposed to  
88 monolithic ones) have significantly altered the enterprise network landscape. This document is  
89 meant to provide guidance to this new enterprise network landscape from a secure operations  
90 perspective. Hence, it starts by examining the security limitations of the current network access  
91 solutions to the enterprise network. It then considers security feature enhancements to traditional  
92 network appliances in the form of point security solutions, network configurations for various  
93 security functions (e.g., application security, cloud access security, device or endpoint security,  
94 etc.), security frameworks that integrate these individual network configurations, and the  
95 evolving wide area network (WAN) infrastructure to provide a comprehensive set of security  
96 services for the modern enterprise network landscape.

## 97 **Keywords**

98 cloud access security broker (CASB); firewall; microsegmentation; secure access service edge  
99 (SASE); secure web gateway (SWG); security orchestration, automation, and response (SOAR);  
100 software-defined perimeter (SDP); software-defined wide area network (SD-WAN); virtual  
101 private network (VPN); zero trust network access (ZTNA).

## 102 **Call for Patent Claims**

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

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

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

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

116 i. under reasonable terms and conditions that are demonstrably free of any unfair  
117 discrimination; or

118 ii. without compensation and under reasonable terms and conditions that are  
119 demonstrably free of any unfair discrimination.

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

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

127 Such statements should be addressed to: [sp800-215-comments@nist.gov](mailto:sp800-215-comments@nist.gov).

128	<b>Table of Contents</b>	
129	<b>Executive Summary</b> .....	<b>1</b>
130	<b>1. Introduction</b> .....	<b>2</b>
131	1.1. Structural Implication of Drivers on Enterprise Network Landscape .....	2
132	1.2. Security Implication of Drivers for the Enterprise Network Landscape .....	3
133	1.3. The Need for a Security Guide .....	4
134	1.4. Scope .....	4
135	1.5. Target Audience .....	4
136	1.6. Organization of This Document.....	4
137	<b>2. Traditional Enterprise Network Access Approaches and Their Limitations</b> .....	<b>6</b>
138	2.1. Limitations of Network Perimeter-based Protections .....	6
139	2.2. Limitations of VPN-based Access .....	6
140	2.3. Limitation of MPLS Technology as Enterprise WANs .....	7
141	2.4. Limitation of User Identity-based Controls .....	7
142	<b>3. Network Security Appliances in Enterprise Network Landscape</b> .....	<b>9</b>
143	3.1. Cloud Access Security Broker (CASB).....	9
144	3.2. Enhanced Firewall Capabilities .....	10
145	3.3. Appliance-set with Integrated Functions .....	11
146	3.4. Requirements for Network Automation Tools.....	11
147	3.4.1. Network Monitoring and Observability Tools .....	12
148	3.4.2. Automated Network Provisioning Tools .....	13
149	3.5. Networking Appliances as Services .....	14
150	<b>4. Enterprise Network Configurations for Hybrid Application Environments</b> .....	<b>15</b>
151	4.1. Network Configuration for Device Management.....	15
152	4.2. Network Configuration for User Authentication .....	15
153	4.3. Network Configuration for Device Authentication and Health Monitoring.....	16
154	4.4. Network Configuration for Authorizing Application Access .....	16
155	4.5. Network Configuration for Preventing Attack Escalation (Microsegmentation).....	16
156	4.5.1. Prerequisites for Implementing Microsegmentation.....	16
157	4.5.2. Microsegmentation – Implementation Approaches.....	17
158	4.6. Security Frameworks Governing Network Configurations.....	19
159	4.6.1. Conceptual Underpinnings – Contextual Information .....	19
160	4.6.2. Network Security Framework – Software-defined Perimeter (SDP) .....	20
161	4.6.3. Network Security Framework – Zero Trust Network Access (ZTNA).....	21
162	<b>5. Secure Wide Area Network Infrastructure for an Enterprise Network</b> .....	<b>22</b>
163	5.1. Common Requirements for a Secure SD-WAN .....	22

164	5.2.	Specific Requirements for WANs for Cloud Access.....	23
165	5.3.	Requirements for an Integrated Security Services Architecture for SD-WAN.....	24
166	<b>6.</b>	<b>Summary and Conclusions.....</b>	<b>26</b>
167		<b>References.....</b>	<b>27</b>
168		<b>List of Figures</b>	
169	<b>Fig. 1.</b>	<b>Segment-based Microsegmentation.....</b>	<b>18</b>
170			



171 **Acknowledgments**

172 The author would like to express his thanks to Isabel Van Wyk of NIST for her detailed editorial  
173 review.

## 174 **Executive Summary**

175 The enterprise network landscape has undergone tremendous changes in the last decade due to  
176 the following three drivers:

- 177 1. Enterprise access to multiple cloud services,
- 178 2. The geographical spread of enterprise-based (on-premises) IT resources (e.g., multiple  
179 data centers and branch offices), and
- 180 3. Changes to application architecture from being monolithic to a set of loosely coupled  
181 microservices.

182 The impact of these drivers on the security of the enterprise network landscape include:

- 183 • Disappearance of the concept of a network perimeter that can be protected and the  
184 necessity to protect each endpoint (device or service) that treats it as a perimeter
- 185 • Increase in attack surface due to sheer multiplicity of IT resources (computing,  
186 networking, storage) and components
- 187 • Sophistication of the attackers in their ability to escalate attacks across several network  
188 boundaries and leverage connectivity features

189 This document is meant to provide guidance to this new enterprise network landscape from a  
190 secure operations perspective. The adopted methodology considers the security challenges that  
191 the network poses and then examines the limitations of current network access technologies and  
192 how solutions have evolved from being security function-specific to a security framework to a  
193 comprehensive security infrastructure that provides a holistic set of security services. Specific  
194 areas addressed include:

- 195 • Feature enhancements to traditional network security appliances
- 196 • Secure enterprise networking configurations for various scenarios
- 197 • Security frameworks that integrate individual network configurations
- 198 • Evolving wide area network (WAN) infrastructure that provides a comprehensive set of  
199 security services

200 What is termed as the enterprise network in this document encompasses the various local  
201 networks on enterprise premises and that portion of wide area network that is used to connect its  
202 various geographically dispersed locations and cloud service access points.

## 203 **1. Introduction**

204 The enterprise network landscape has undergone a significant transformation in the last decade.  
205 The drivers for this transformation are (a) enterprise access to multiple cloud services, (b) the  
206 geographic spread of enterprise-owned (on-premises) IT resources (e.g., in a central office,  
207 multiple branch offices, and data centers), and (c) changes to application architecture from being  
208 monolithic to a set of loosely coupled microservices – often with a dedicated infrastructure  
209 (called the service mesh) that provides all application services, including security. The high-level  
210 impact of these drivers on the security of the current enterprise network landscape are (a)  
211 disappearance of the concept of a perimeter associated with the enterprise network; (b) an  
212 increase in attack surface due to the sheer multiplicity of IT resource components associated with  
213 application services, storage, and network appliances; and (c) sophistication of the attackers in  
214 their ability to escalate attacks across several network boundaries and leverage connectivity  
215 features. This document will consider these impacts by identifying the structural components of  
216 the new network landscape as well as specific security threats that they have opened up.

### 217 **1.1. Structural Implication of Drivers on Enterprise Network Landscape**

218 In order to have a good structural view of the current enterprise network landscape, it is  
219 necessary to look at the current enterprise IT environment in general. The IT environment now  
220 consists of:

- 221 • Subscription to multiple cloud services, such as IaaS for computing, SaaS for software,  
222 PaaS for an application development platform, and other cloud services (e.g., IDaaS for  
223 authentication)
- 224 • Enterprise IT applications (on-premises) located in corporate headquarters and  
225 geographically distributed branch offices and data centers
- 226 • IT applications range from being monolithic to ones that are made up of loosely coupled  
227 microservices, each of them hosted on heterogeneous platforms
- 228 • Presence of edge computing devices, such as IoTs, in some environments

229 The above scenarios call for widespread connectivity between IT systems that now defines the  
230 current enterprise network landscape. Connectivity, in turn, involves:

- 231 • Connectivity between IT resources (servers for computing and storage) in data centers  
232 (network fabric)
- 233 • Connectivity between IT resources within a corporate office or branch office (Wi-Fi,  
234 LAN, VLAN)
- 235 • Connectivity for users to remotely access to IT resources from home, travel locations,  
236 branch offices, and corporate offices using WANs, which use multiple networks such as  
237 the internet, MPLS, and – in some instances – cellular networks (e.g., 4G/LTE, 5G, etc.)
- 238 • Connectivity to cloud services through a cloud service provider (CSP), virtual private  
239 networks (VPN), or subscription to WAN services (premises based equipment licenses  
240 or cloud-based)

## 241 **1.2. Security Implication of Drivers for the Enterprise Network Landscape**

242 The beginning of this section stated the following as the drivers for the state of the current  
243 enterprise network landscape:

- 244 • Subscription to multiple cloud services
- 245 • Geographically distributed IT resources
- 246 • Changes in application architecture

247 Now consider the immediate security implications of these drivers.

248 Subscription to multiple cloud services: Accessing cloud services from multiple cloud providers  
249 has become the norm for many enterprises. This trend is motivated not only by the need to avoid  
250 a cloud-vendor locked-in situation but also by different CSPs offering different value-added  
251 functions for different services (e.g., IaaS, SaaS). The consequence of this trend is that – from an  
252 enterprise point of view – the following networks have become extensions of the enterprise  
253 network and, thus, come under the scope of enterprise network management with attendant  
254 responsibilities for ensuring security protections becoming a critical function.

- 255 • Network used for accessing the cloud services
- 256 • Inter-cloud network (since communication between one CSP and another may be  
257 inevitable)
- 258 • The network inside the cloud provider that needs to be navigated to access the subscribed  
259 services (e.g., VPC, VNET, etc.)

260 Geographically distributed IT resources: The implication of distributed IT resources is that the  
261 users are also geographically distributed. Applications are now accessed by users not only from  
262 the enterprise premises, such as the corporate office and branch offices (through the enterprise  
263 network), but also from home and public locations (e.g., hotels and cafes) through multiple  
264 devices, such as desktops, laptops, and mobile phones. Ensuring secure access from these  
265 multiple locations and devices becomes the responsibility of the enterprise.

266 Changes in application architecture: Application architectures – especially those of cloud-native  
267 applications – have changed from being monolithic to being microservices-based, with the  
268 distributed nature increasing the communication channels between the components across a  
269 network (instead of just being local procedure/function calls). These applications have enlarged  
270 the threat and attack surface due to:

- 271 • Inherent architectures (multiple independent microservices and APIs),
- 272 • Automation tools used during software development and deployment, and
- 273 • Agile development and deployment methodologies, such as DevSecOps, that contain  
274 CI/CD pipeline code (workflows).

275 Attacks include data breaches, distributed denial of service (DDoS), account takeover (ATO) due  
276 to credential theft, and insider threats.

### 277 **1.3. The Need for a Security Guide**

278 Based on these considerations for security implementation, the arguments for the need for a  
279 security guide to the current enterprise network landscape are:

- 280 • Ubiquitous access locations, ubiquitous hosting locations of the application components,  
281 and multiple WAN transport protocols have caused shifts in security focuses, goals, and  
282 principles.
- 283 • The security focus has enlarged from being network-centric (i.e., internal/corporate  
284 network versus external/public internet) to user- and device/endpoint-centric.
- 285 • The new trust relationship has to be based not just on identity or the location of the access  
286 but enhanced to include validation of each access request (not just at the beginning of an  
287 access session), as well as the applicable set of contextual information associated with the  
288 user, device, or service.

### 289 **1.4. Scope**

290 The scope of this document includes:

- 291 • A structural view of the enterprise network landscape based on the distribution of IT  
292 resources and the consequent security challenges it poses
- 293 • Emerging and state-of-practice solutions in terms of feature sets and requirements to  
294 address the security challenges; solutions discussed will focus on the functional and  
295 operational levels

### 296 **1.5. Target Audience**

297 This guidance is intended for network design architects and network security solution architects  
298 in organizations with a hybrid IT environment (consisting of both on-premises and cloud-based  
299 applications) with a combination of legacy and microservices-based (i.e., cloud-native)  
300 applications.

### 301 **1.6. Organization of This Document**

302 The organization of this document is as follows:

- 303 • Chapter 2 considers traditional network access principles and technologies and their  
304 limitations in the context of the current enterprise network landscape.
- 305 • Chapter 3 provides a brief functional description of network security appliances – some  
306 new, some traditional (e.g., firewall) – that have enhanced capabilities to meet the  
307 security needs of the current network landscape.
- 308 • Chapter 4 outlines various network configurations that have evolved specifically for  
309 meeting the current network landscape (e.g., secure cloud access). It then considers the  
310 frameworks that integrate two or more of these stand-alone configurations in terms of  
311 their conceptual underpinnings and overall architectures.

- 312 • Chapter 5 focuses on the evolution of the WAN portion of the enterprise network
- 313 landscape and enhanced offerings of the WAN services with global spread with a built-in
- 314 security service infrastructure.
- 315 • Chapter 6 provides the summary and conclusions.

## 316 **2. Traditional Enterprise Network Access Approaches and Their Limitations**

317 Section 1 outlined the drivers for the current enterprise network landscape. Both drivers (change  
318 in application architectures and access to cloud-based applications) have impacted the mechanics  
319 of secure access to those applications through the network. Now consider the security limitations  
320 of the traditional enterprise network access approaches in the current enterprise network  
321 landscape context.

- 322 • Limitation of network perimeter-based protections
- 323 • Limitations of VPN-based access
- 324 • Limitations of MPLS technology as enterprise WANs
- 325 • Limitation of user identity-based controls

### 326 **2.1. Limitations of Network Perimeter-based Protections**

327 Early solutions for secure enterprise network access were geared toward environments with well-  
328 defined network perimeters. All enterprise IT resources were endpoints of enterprise LANs  
329 (usually defined as a floor in a large enterprise, building, or small campus), and multiple LANs  
330 connected together inside a defined building or campus constituted the internal corporate  
331 network. Entry points into this corporate network were protected using devices called firewalls,  
332 which were initially implemented as hardware appliances and later used software. In this  
333 environment, all devices and users within firewalls were totally trusted and, hence, considered  
334 safe for accessing application resources. However, the following factors have annulled the  
335 concept of that perimeter:

- 336 • Distributed nature of the application into ones located within a corporate data center,  
337 remote branch offices, and multiple cloud locations
- 338 • Perimeter approach based on the premise that the threat originates outside of the network,  
339 which is why most perimeter security solutions (e.g., IPS, IDS, firewalls) focus only on  
340 north-south traffic. However, over 75 % of network traffic is now east-west or server-to-  
341 server (due to applications being microservices-based), which is largely invisible to  
342 security teams. Any threat that is already inside of a network can move laterally and  
343 remain undetected for days or even months.
- 344 • Edge computing [1], where much of the computing takes place close to the location of  
345 multiple IoT devices
- 346 • Users located both within and outside of the corporate network, such as in homes, remote  
347 branch offices, and public locations (e.g., hotels, pubs, etc.). Some enterprises must also  
348 provide access to ecosystem partners, who may be on their own corporate networks.

349 The above scenarios have greatly expanded the attack surface.

### 350 **2.2. Limitations of VPN-based Access**

351 The increase in teleworking employees due to the pandemic has necessitated a means for secure  
352 access to IT resources inside an enterprise network in the form of virtual private networks  
353 (VPNs). A VPN allows organizations to extend a perimeter-based security across a public

354 network. Security is enabled by setting up a secure tunnel in the public network using protocols  
355 such as IPSEC and TLS.

356 However, there are some limitations and security risks associated with VPNs.

- 357 • An increasing trend involves the movement of corporate resources to the cloud and the  
358 use of mobile devices. The VPN connections that remote users establish terminate at the  
359 VPN concentrators located at the edge of the corporate network. Hence, using a process  
360 called hair pinning, the traffic that lands at the corporate internet edge is routed back to  
361 the internet to access the cloud resources. This extra path increases network latency and  
362 has the potential to cause traffic bottlenecks.
- 363 • The mobile devices used by many employees, such as smartphones and tablets, can  
364 connect directly to software-as-a-service (SaaS) applications and data in the cloud. These  
365 mobile devices are especially prone to phishing attacks that steal credentials or deliver  
366 malware. Thus, the VPN becomes an entry point by which a bad actor could compromise  
367 a device and enter an organization's infrastructure.
- 368 • Two recent vulnerabilities were discovered in some VPNs [2]. One was "session  
369 hijacking," where malicious actors access a valid session ID through brute-force attacks  
370 or reverse engineering. The second vulnerability involved pulling a unique ID for an  
371 account, leveraging web browser development tools to manually set a value to the ID,  
372 and using that to obtain unauthenticated access to the VPN administrator console. That  
373 access was then used to remotely connect to internal systems, harvest passwords, move  
374 laterally in the network, and – in many cases – deploy ransomware.

### 375 **2.3. Limitation of MPLS Technology as Enterprise WANs**

376 Multi-protocol label switching (MPLS) technology is used for enterprise WANs, but the wide  
377 geographic span of an enterprise network due to multiple data centers and cloud services has  
378 imposed some limitations on its use.

- 379 • The geographic span of enterprise IT resources and subsequent networking connections  
380 have made traversal through internet inevitable for many portions of its enterprise's  
381 access network. Since MPLS is a different network, it provides access to the internet only  
382 through designated and limited access points. This increases latency for time-sensitive  
383 corporate applications.
- 384 • Given the different networking technology, the appliances and subsequent configuration  
385 procedures are different, making networking management a complex task.

### 386 **2.4. Limitation of User Identity-based Controls**

387 In traditional monolithic applications, all invocations of applications are either directly from the  
388 user or through scripts written and programmed to run by the user. Hence, the only parameters  
389 for access validation are the user identity or attributes associated with the user.

390 Changes in application architectures expand the validation parameters beyond user identity and  
391 attributes. The initial changes to application architectures are found in web-based and API-based  
392 applications where access can take place from any device located in any network (e.g., home,



393 public WiFi, etc.). The latest changes are found in microservices-based applications (often called  
394 cloud-native applications because this architecture is the predominant one among cloud-hosted  
395 applications). This class of application consists of loosely coupled microservices that require the  
396 generation of multiple interservice requests to complete a business process or transaction. The  
397 limitations of identity-based controls can be seen from the following expanded security  
398 requirements for microservices-based applications:

- 399 • Validation is required not only for the identity of the users initiating the transaction but  
400 also for the identity of each service (service identity) making the request and the device  
401 on which the service is hosted (authorized device).
- 402 • The location of the service and device may change due to the virtualized nature of the  
403 application hosting environment (e.g., migration to VMs located in a different subnet,  
404 more powerful hosting devices and storage mechanisms, etc.), necessitating the need for  
405 validating an application request based not only on user identity and attributes but also on  
406 attributes associated with the device, network, geolocations, etc.
- 407 • The validation of identity (authentication) and authorization need to be done continuously  
408 (and not just at the beginning of an application invocation session) as the risk profile of  
409 an access may change due to there being multiple entities involved or changes in  
410 behavioral patterns that need to be included as a validation parameter (and monitored).

### 411 **3. Network Security Appliances in Enterprise Network Landscape**

412 This section will consider some new network security appliances as well as enhanced features in  
413 established appliances for meeting the security needs of the current landscape. These can be  
414 viewed simply as point security solutions, but evaluating their functions and features will provide  
415 an understanding of the effectiveness of network configurations and technologies that form part  
416 of the integrated solutions that are going to be discussed in Sections 4 and 5, respectively.

#### 417 **3.1. Cloud Access Security Broker (CASB)**

418 Given the increasing subscription to multiple clouds in many enterprises, one of the most  
419 important pieces of software is the cloud access security broker (CASB). Just like IAM systems,  
420 a CASB can be run either on-premises or as a cloud-based service. It sits on the network between  
421 the cloud service customers (CSC) and the cloud service providers (CSP). The evolution of  
422 CASB functionality can be traced as follows [3]:

- 423 • The primary function of the first generation of CASBs was the discovery of resources.  
424 They provided visibility into all of the cloud resources that the enterprise users accessed,  
425 thus preventing or minimizing the chances of shadow IT. Shadow IT is the practice of  
426 some users using cloud applications that are not authorized by the enterprise IT  
427 management from home or the office using enterprise desktops. An example of this is the  
428 use of unapproved software-as-a-service (SaaS) applications for file sharing, social  
429 media, collaboration, and web conferencing by some enterprise users [4]. This generation  
430 of CASBs also provides some statistics, such as software-as-a-service (SAAS) utilization.
- 431 • The current generation of CASBs enforces security and governance policies for cloud  
432 applications, thus enabling enterprises to extend their on-premises policies to the cloud.  
433 Specific security services provided by CASBs include:
  - 434 ○ Protection of enterprise data that lives in cloud service providers' servers (due to  
435 SAAS or IAAS subscriptions), as well as data inflow and data outflow from those  
436 servers
  - 437 ○ Tracking of threats, such as account hijacking and other malicious activities.  
438 Some can detect anomalies in users' cloud access behavior (through robust user  
439 and entity behavior analytics, or UEBA, functionality) and stop insider threats and  
440 advanced cyberattacks [5].
  - 441 ○ Detection of misconfigurations in the enterprise's subscribed infrastructure as a  
442 service (IaaS) and cloud servers. These misconfigurations pose serious security  
443 risks such as data breaches. Alerts generated by CASB due to misconfigurations  
444 in the enterprise's IaaS deployments direct the enterprise to follow guidelines,  
445 such as the Center for Internet Security's (CIS) benchmarks for public cloud  
446 services, thus improving the overall security profile of the enterprise for cloud  
447 access [4].

### 448 3.2. Enhanced Firewall Capabilities

449 The security functions in firewalls have enlarged alongside the changing network landscape.  
450 Firewalls started as hardware appliances that prevented network packets from a device with a  
451 particular network location (e.g., combination of IP address and port) in one subnet (e.g.,  
452 external network or internet) from accessing a device on another network location or subnet  
453 (e.g., intranet or DMZ or corporate network). In that setup, it primarily secured a network  
454 perimeter. The evolution of firewall functions can be traced based on the following feature sets  
455 [6]:

- 456 • Packet filters and network address translation: Packet filtering and NAT are used to  
457 monitor and control packets moving across a network interface, apply predetermined  
458 security rules, and obscure the internal network from the public internet.
- 459 • Stateful inspection: Stateful firewalling, also known as dynamic packet filtering, monitors  
460 the state of connections and makes determinations on what types of data packets  
461 belonging to a known active connection are allowed to pass through the firewall.
- 462 • Threat detection and response: Modern firewalls can gather and analyze enough data  
463 across multiple packets and sessions to detect threats and security incidents targeted at a  
464 particular system or a family of systems. The data from multiple firewalls can also be  
465 directed toward security information and event management (SIEM) and correlated with  
466 data from other security tools and IT systems to detect enterprise-wide attacks that span  
467 multiple systems and network layers. In addition, this data can be used to understand  
468 evolving threats and define new access rules, attack patterns, and defensive strategies [6].
- 469 • Logging and auditing capabilities: Logging and auditing capabilities result in the  
470 construction of network events that can be used to identify patterns of performance and  
471 security issues.
- 472 • Access control functions: Access control functions enforce granular sophisticated access  
473 control policies.
- 474 • Multiple locations and functions: Firewalls reside at different locations to perform  
475 different functions. Firewalls at the network edge perform the network perimeter  
476 protection function by filtering disallowed sources and destinations and blocking packets  
477 of potential threats. Firewalls inside a data center can create segmentation of the internal  
478 network to prevent the lateral movement of traffic and isolate sensitive resources (e.g.,  
479 services and data stores). Device-based firewalls prevent malicious traffic in and out of  
480 endpoints.
- 481 • Open APIs integrate with many networking products.
- 482 • Some features centrally define or merge policies so that consistent policies are applied to  
483 different class of users (e.g., those on-premises and on private and public clouds).
- 484 • Web application firewalls (WAF): This class of firewalls has been used ever since web  
485 applications accessed through web protocols, such as HTTP, came into existence. A  
486 feature advancement in this class of firewalls is advanced URL filtering. This is the  
487 ability to detect traffic from malicious URLs and thus prevent web-based threats and

488 attacks by receiving real-time data analyzed by machine learning algorithms [7][8].  
489 Specifically, this class of firewalls can inspect threat vectors for SQL Injection, OS  
490 command injections, and cross-site scripting attacks, as well as prevent inbound attacks.  
491 They are used in content delivery networks (CDN) and to prevent distributed denial-of-  
492 (DDoS) attacks. Some additional features found in this class of firewalls are:

- 493 1. Ability to specify allowable list of services (control at the application level)
- 494 2. Traffic matches the intent of allowed ports
- 495 3. Filtering of some unwanted protocols

### 496 3.3. Appliance-set with Integrated Functions

- 497 • Unified threat management (or UTM)s: UTM devices combine many of the most critical  
498 security functions – firewall, intrusion prevention system (IPS), VPN concentrator,  
499 gateway antivirus, content filtering, and WAN load balancing – into a single device,  
500 usually with a unified management console.
- 501 • Next-generation firewall (NGFW): This all-in-one security appliance is based on the  
502 UTM model but is combined with enterprise-class scalability and performance and a  
503 focus on the granular inspection of Layer 7 application traffic. NGFWs have added  
504 capabilities to facilitate internal segmentation, integration with sandboxing products,  
505 secure sockets layer (SSL) inspection, and SD-WAN. Processing at the edge benefits  
506 from on-premises firewalls, which apply processing on-site. They are more energy-  
507 efficient than virtual machines and reduce latency because they avoid the “round trip” to  
508 the cloud. NGFWs come with high-performance threat protection (e.g., intrusion  
509 prevention, web filtering, anti-malware, application control) for known attacks, SSL/TLS  
510 inspection, and antivirus [9].
- 511 • Web application and API protection (WAAP): This is a comprehensive security approach  
512 and an enhancement over web application firewalls (WAF). WAF is an integral  
513 component for API security, BOT defense, and DDOS protection.
- 514 • These can be offered as a product suite or as a cloud-based service [10][11].
- 515 • Secure web gateway (SWG)s: SWGs are appliances utilized for policy-based access to  
516 and control of cloud-based applications for enterprise users in ubiquitous locations (e.g.,  
517 headquarters, branch offices, home, remote locations). A SWG is fundamentally a web  
518 filter that protects outbound user traffic through HTTP or HTTPS inspection [12]. They  
519 also protect user endpoints from web-based threats that can occur when users click on  
520 links to malicious websites or to websites infected with malware. They centralize control,  
521 visibility, and reporting across many locations and types of users. They are not a  
522 replacement for WAFs, which protect websites housed in enterprise data centers and  
523 large headquarter sites from inbound attacks.

### 524 3.4. Requirements for Network Automation Tools

525 Network automation tools automate the entire life cycle processes involved in deployment,  
526 observability/monitoring, threat intelligence gathering/reporting (e.g., generating alerts of  
527 security violations for security personnel to take timely action), and – in some instances –

528 automatic remediation. These automated tools are an indispensable part of a complex enterprise  
529 network landscape. The requirements for these tools can be broadly classified into generic and  
530 functional requirements. These requirements are described below. Each generic requirement is  
531 tagged with the abbreviation NAUT-GR-x, while each functional requirement is tagged with  
532 NAUT-FR-x, where x in both types of tags stand for the numerical sequence.

- 533 • NAUT-GR-1: Scale to meet the volume, velocity, and variety of today’s application  
534 development deployment and maintenance paradigms [13]. This requirement is critical in  
535 environments where DevSecOps is used to deploy not only applications but also  
536 infrastructures, the latter using infrastructure-as-code (IaC) tools. These tools are made an  
537 integral part of the smart automated workflows called CI/CD pipelines, which invoke  
538 these tools to deploy servers (computing), networking, and storage infrastructure. Hence,  
539 this class of network automation tools can be seamlessly integrated into the  
540 corresponding CI/CD pipelines.
- 541 • NAUT-GR-2: They should have the capability to minimize human intervention for  
542 security remediation, which is slow and prone to error. In other words, the more  
543 automated remediation features built into the tool, the better.

544 The minimum functional requirements of network automation tools should be:

- 545 • NAUT-FR-1 (enhanced threat intelligence and protection): The tools should have  
546 advanced threat intelligence, real-time threat prevention capabilities for known and zero-  
547 day vulnerabilities, and sandboxing features for isolating malicious traffic.
- 548 • NAUT-FR-2 (leveraging knowledge of previous events): The tools should have features  
549 for matching current events to past ones and for leveraging the remediation measures  
550 performed for those instances in the current solution. This brings about reduction to the  
551 average outage time [14].

552 The network monitoring and observability tools and IaC tools are important classes of network  
553 automation tools, and the requirements and feature set are discussed in the following subsections.

### 554 **3.4.1. Network Monitoring and Observability Tools**

555 This class of tools gathers the data for obtaining visibility into the entire network. The data is  
556 then used to generate a dashboard that presents the topography of the enterprise network by  
557 showing all connections and presenting key operating parameters (e.g., latency, network traffic  
558 level, etc.). Some of the data generated by this class of tool and their uses are:

- 559 • Identification of interfaces: Monitoring tools identify the interfaces for defining the  
560 parameters for network resources provisioning and help the IaC generate the relevant  
561 code for invoking those interfaces.
- 562 • Measurement of drift: Despite using IaC to deploy the network infrastructure,  
563 unauthorized or ad hoc changes in network configuration can alter the performance and  
564 security parameters for application execution (called the drift). Monitoring tools should  
565 have the ability to monitor these parameters (e.g., bandwidth availability, unwanted  
566 traffic, etc.) and alert for corrective action.

- 567 • Secure overlay designs for cloud service access: Monitoring tools can generate data to  
568 enable centralized network management tools to perform security functions, such as  
569 building a virtual network segmentation on top of the native network segmentation  
570 features offered by CSP, provided that suitable APIs are available.
- 571 • Support for incidence response process: Sophisticated network monitoring tools generate  
572 network security alerts and threat intelligence feeds. Handling these alerts and feeds is  
573 part of the incidence response (IR) process in an enterprise and is carried out by members  
574 of a security operations center (SOC). A security strategy that has evolved in recent years  
575 to automate the IR process is called security orchestration, automation, and response  
576 (SOAR). Some of the state of practice applications of SOAR include threat detection and  
577 response, vulnerability prioritization, compliance checks, and security audits with  
578 potential applications in many emerging areas, such as IoT management [15].

### 579 **3.4.2. Automated Network Provisioning Tools**

580 As already stated, automated network resource provisioning is enabled by infrastructure as code  
581 (IaC) tools. The code that describes the networking infrastructure (in addition to the computing  
582 and storage infrastructure) is stored in a code repository. The process of initial deployment of the  
583 networking infrastructure and subsequent upgrade is automated by defining a workflow that  
584 invokes the IaC (e.g., GitOps workflow) as part of a CI/CD pipeline definition [16]. The  
585 advantages of this approach for managing the enterprise networking infrastructure for multi-  
586 cloud deployment are the following:

- 587 • Enables the enterprise to have tight version control (tracking changes) so that  
588 unauthorized networking devices and unauthorized changes in associated configurations  
589 do not open up security vulnerabilities.
- 590 • Enables the enterprise to have a uniform infrastructure across all environments –  
591 development, testing, staging, and production.
- 592 • Monitoring the drift (the unintended changes) between the defined infrastructure (as  
593 found in IaC) and the operational infrastructure (as measured by monitoring tools  
594 described in Section 3.4.1) and taking corrective action to address the drift help to  
595 maintain the necessary security posture for the enterprise networking environment.
- 596 • The DevSecOps paradigm consisting of CI/CD pipelines invokes the network  
597 provisioning tool (IaC code generator) to automate the initial deployment and subsequent  
598 re-configuration of the networking infrastructure. Since the pipelines have a built-in audit  
599 process, the changes in network configuration are automatically captured in the audit,  
600 which in turn enables the enterprise to demonstrate corporate security policy compliance  
601 and regulatory policy compliance for their networks where applicable.
- 602 • Testing the code (IaC code) generated by IaC tools (and invoked by the CI/CD pipeline  
603 code that deploys the infrastructure using IaC) ensures that security policies are  
604 consistently and uniformly applied across the entire enterprise networking infrastructure  
605 (i.e., multiple cloud services).
- 606 • The advantage of having plug-ins for defining network provisioning for different public  
607 cloud provider environments is that they can be used to customize the observability tools

608 used for networking monitoring for each of those cloud services that the enterprise has  
609 subscribed to [17].

### 610 **3.5. Networking Appliances as Services**

611 Another trend in the enterprise network landscape is that a portion of network infrastructure can  
612 be obtained as a leased service called a network as a service (NaaS) from third-party providers.  
613 This service is offered using technologies such as enterprise 5G and edge computing. The  
614 advantages of NaaS are as follows:

- 615 • Just like subscriptions to SaaS and IaaS, it reduces capex costs for the enterprise.
- 616 • Being software-defined and virtualized, it is flexible and scalable.
- 617 • As a consequence of the previous advantage, QoS requirements of diverse applications  
618 can be met by creating customized traffic flow for each application type [18].
- 619 • New applications that require an increased network footprint can be quickly introduced to  
620 the enterprise (agility), thus facilitating business diversification.

## 621 **4. Enterprise Network Configurations for Hybrid Application Environments**

622 Since the enterprise context in this document refers to enterprises that consist of on-premises and  
623 cloud-hosted applications (i.e., hybrid application environments), this document describes the  
624 network configurations or designs (and network communication exchanges based on them) that  
625 have emerged as state of practice in those enterprises.

626 The state of practice network configuration features (NCF) found in enterprises with hybrid  
627 application environments can be classified under the following areas [19]:

- 628 • Network configuration for Device Management
- 629 • Network configuration for User Authentication
- 630 • Network configuration for Device Authentication and Health Monitoring
- 631 • Network configuration for Authorizing Application Access
- 632 • Network configuration for Preventing Attack Escalation (Microsegmentation)

633 Each of the network configuration features are enumerated using the identifier of the form HAE-  
634 NCF-x, where HAE denotes a hybrid application environment, NCF denotes the network  
635 configuration feature, and x stands for the sequence number of the feature.

### 636 **4.1. Network Configuration for Device Management**

637 With the disappearance of the network perimeter (Section 2.1) and the distribution of the  
638 application targets (being a hybrid application environment), enterprises should adopt an  
639 “endpoint is the perimeter” paradigm and have a device management system in place.

640 HAE-NCF-1: All endpoints that will be accessing on-premises and cloud-based applications  
641 should be managed using a dedicated management network. Minimal managed tasks should  
642 include:

- 643 a) Installation and maintenance of device and service authentication certificates
- 644 b) Installation and maintenance of device health applications
- 645 c) Updates of patches on the devices
- 646 d) Creation and maintenance of white pages that contain device-service mappings to prevent  
647 service hijacking (preventing malicious or compromised servers posing as legitimate  
648 hosts for the services)

### 649 **4.2. Network Configuration for User Authentication**

650 HAE-NCF-2: The network should be configured to route the user access request to different  
651 destinations for authenticating the user, depending on the target application accessed.

- 652 a) When the user access request is for a cloud-based application (e.g., SaaS), the user should  
653 be routed to the enterprise IdP. When the user access request is for an on-premises web  
654 application, the user should be directed to a web gateway (reverse proxy). This  
655 redirection can be affected through a process called split DNS. If a digital certificate is  
656 used as the first authentication factor, the IdP should check the validity of the user



657 certificate (right status and not expired) through mechanisms such as CRL, OCSP, or  
658 Active Directory calls.

659 b) A minimum of two authenticator factors must be used to authenticate users. If possession  
660 of a valid certificate is the first factor, then the acknowledgement of a push message  
661 (using technologies such as DuoMobile, TouchID or Yubikey) or OTP to the cell phone  
662 can be used as the second factor.

### 663 **4.3. Network Configuration for Device Authentication and Health Monitoring**

664 HAE-NCF-3: Device authentication can be performed through certificate validation using  
665 appropriate protocols. A device health check can be performed by invoking the resident  
666 application.

667 HAE-NCF-4: Microservices-based applications (on-premises or in cloud) should have service  
668 proxies installed with each service to provide the necessary connectivity for inter-service  
669 communication in addition to performing authentication and authorization services for each  
670 service request.

### 671 **4.4. Network Configuration for Authorizing Application Access**

672 HAE-NCF-4: Standardized protocols, such as OAuth 2.0 [20], should be used to issue access  
673 tokens to the validated user, device, or service to enable access to cloud-based applications.

### 674 **4.5. Network Configuration for Preventing Attack Escalation** 675 **(Microsegmentation)**

676 Microsegmentation is a security design practice where an internal network (e.g., in the data  
677 center, cloud provider region) is divided into isolated segments so that the traffic in and out of  
678 each segment can be monitored and controlled [21].

679 Things enabled by microsegmentation are:

- 680 • Segments being isolated and relatively small enables close monitoring of the traffic  
681 because of better visibility.
- 682 • The consequence of the above capability is that granular access control is possible by  
683 defining associated policies.

684 The enablement of the above capabilities restricts the unauthorized lateral movement of a user or  
685 application that has either (a) breached the perimeter to enter the internal network or (b) been  
686 initiated by users within the internal network itself.

#### 687 **4.5.1. Prerequisites for Implementing Microsegmentation**

688 a) Creation of application identity: The fundamental requirement to enable this is the  
689 assignment of a unique identity to each application or service, just like how each user  
690 carries a unique identity (e.g., userid). Prior to the era of cloud-based applications, the  
691 application requests were validated based on the IP subnet or IP address from which they

692 originated. Ubiquitous access and multi-clouds have eliminated the concept of network  
693 perimeters. Hence, authentication and authorization based on those parameters are neither  
694 feasible nor scalable. Further, the presence of proxies, network address translation, and  
695 load balancers make it impossible for the called application to know the IP address of the  
696 calling application in order to make authentication or authorization decisions. A unique  
697 application identity is inevitable.

698 b) Establishment of trust in application identity: The created application identity should not  
699 be subject to spoofing and should be continuously verifiable. Hence, a cryptographic  
700 identity in the form of a public key carried in a certificate issued by a trusted source is  
701 required to meet these criteria. Verification of the authenticator associated with this  
702 identity is done by the authenticating party by sending a challenge, and insurance against  
703 replay attack for the authentication process is ensured by sending a nonce attached to the  
704 challenge. A secure directory that provides a mapping of the service to the hosting server  
705 should be maintained to ensure that applications or services are hosted only on authorized  
706 servers and that spurious versions of services do not exist.

707 c) Discovery of application resources: There should be a robust means for discovering all  
708 application resources (e.g., services, networks, etc.).

709 d) Segmentation of workloads: Security requirements for all applications and services must  
710 be identified and groupings established based on identical security requirements.

711 e) Mapping of logical application groupings to physical or virtual infrastructures:  
712 Application-centric groupings must be mapped to physical or virtual infrastructures that  
713 constitute the data center topology to facilitate actual applications and services  
714 deployment.

#### 715 **4.5.2. Microsegmentation – Implementation Approaches**

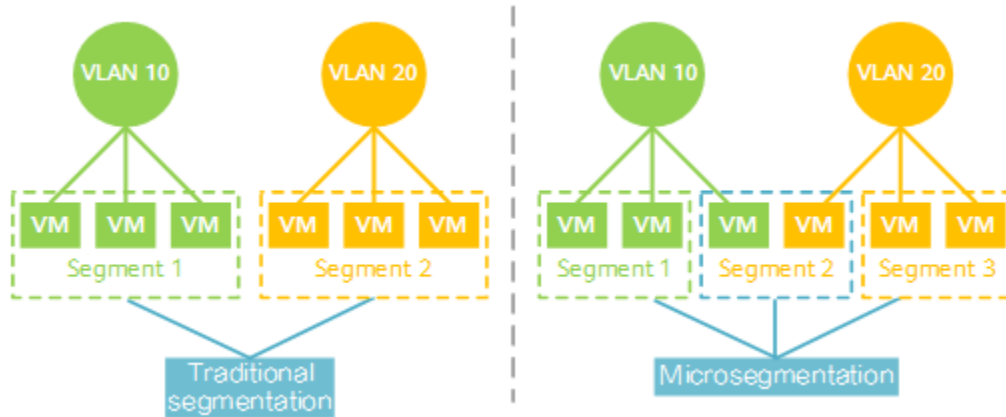
716 The following approaches are employed to implement microsegmentation [22]:

717 a) Segment-based approach: In this approach, the applications and services resources with  
718 similar security requirements are grouped into a unique segment, and firewall rules are  
719 created to block or allow communication with each group or segment. The segments are  
720 created using network layer abstractions, such as VLAN IDs or some other tagging  
721 approaches, while policies are defined using network address constructs (e.g., IP addresses  
722 and ports). Policies apply to subnets (e.g., VLANs) and not to individual hosts. Each  
723 segment is protected by gateway devices, such as intelligent switches and routers or next-  
724 generation firewalls (NGFWs), which should have the capacity to react and adapt in  
725 response to the threats and changes in the application workflows. Segmentation gateways  
726 monitor traffic, stop threats, and enforce granular access across east-west traffic (rarely for  
727 north-south traffic) within on-premises data centers or cloud regions. The main difficulty  
728 with this approach is the difficulty in mapping the applications security requirements-  
729 based segments created to corresponding network segments [23].

730 A schematic diagram of the segment-based microsegmentation is shown in Figure 1.  
731 Each numbered microsegment in the figure is a unique VLAN identified by a VLAN ID.  
732 The group of applications that will run in that particular VLAN segment can be defined  
733 using different criteria. One of the criteria is “all applications with similar security

734 requirements.” Another is that “all tiers (web frontend, application logic servers, and  
735 database servers) associated with a particular application” should run in a single  
736 microsegment, as shown in the figure.

737



738

739

**Fig. 1. Segment-based Microsegmentation**

740 b) Virtualized server-based approach: This approach is only applicable to networks that  
741 contain virtualized servers since it is implemented in the hypervisor. There are two  
742 possible mechanisms:

- 743 1. Using virtual firewalls inside a hypervisor to isolate traffic destined for different  
744 VMs inside the hypervisor  
745 2. Using encapsulation techniques to create overlays (e.g., VXLAN) that run on top  
746 of an underlay network consisting of IP addresses designations; access control  
747 policies are enforced on the hypervisor itself outside of the workload (application  
748 or microservice)

749 c) Host-based microsegmentation: Alternatively (or additionally), host-based  
750 microsegmentation can be implemented using software agents on the endpoint artifacts  
751 (e.g., servers). It leverages native firewall functionality built into the host. Software agents  
752 can overlay a software-defined segmented network across data centers, cloud, bare metal,  
753 and hybrid environments. The agent provides context awareness and visibility for each  
754 workload and, hence, enables the definition and enforcement of fine-grained policies.

755 d) Identity-based microsegmentation: Identity-based microsegmentation policies use  
756 contextual, application-driven identifiers (e.g., order processing front-end service can  
757 communicate with inventory back-end service) instead of network parameters (permit  
758 calls from 192.168.10.x subnet to 10.0.0.31) [24]. The identifiers assigned to services are  
759 cryptographic identities, which they use for mutual authentication and authorization  
760 during each service request and response.

761 The advantages of this type of microsegmentation are:

- 762 • Policies based on service/application identities do not use any infrastructure-related  
763 variables (e.g., IP addresses, subnets, etc.), so these policies are environment-agnostic  
764 and provide the freedom for the services/applications to be migrated to different  
765 environments and still maintain the same policies.

- 766 • Policies being independent of infrastructure enables them to be tested by merely  
767 exercising the application and observing the outcomes (e.g., trace of the sequence of  
768 service calls and requests/responses instead of configuring the infrastructure correctly for  
769 test runs).
- 770 • With the availability of tools for the declarative specification of policies through “policy  
771 as code” tools, microsegmentation policies can be defined/implemented by incorporating  
772 the code into automated workflows, such as CI/CD pipelines.
- 773 • Microsegmentation enables granular (fine-grained) access control by providing visibility  
774 to application call sequences/interdependencies and data flows through host-level tracking,  
775 thus enabling the enforcement of security policies for application traffic that is both north-  
776 south and east-west, irrespective of the environment (e.g., corporate data center or cloud  
777 infrastructure).

778 The reason that identity-based microsegmentation is studied under the enterprise network  
779 landscape is that it enables only valid network traffic between the various component services of  
780 the application due to the mutual authentication and authorization using service identities, thus  
781 enabling the goals of zero trust network access (ZTNA) to be met [25].

## 782 **4.6. Security Frameworks Governing Network Configurations**

783 The network configurations described in Sections 4.1 through 4.5 are each for specific functions  
784 (e.g., user authentication, preventing attack escalation, etc.). In many enterprise environments,  
785 these network configurations are not ad hoc but are driven by some conceptual underpinning  
786 (e.g., contextual information) and/or some evolving enterprise network security framework that  
787 the enterprise has chosen to implement. Examples of such frameworks are software-defined  
788 perimeter (SDPs) and zero trust network access (ZTNA).

### 789 **4.6.1. Conceptual Underpinnings – Contextual Information**

790 Section 2.4 discussed the limitation of using user identity alone to authorize application access.  
791 This, however, does not mean that identity verification can be relegated to a secondary  
792 requirement. It has been widely recognized that identity validation is the entry point (may be a  
793 highly vulnerable point of entry into the system) to an application request [26] since all requests  
794 – whether coming from a service (or microservice), user, or device – come with a claimed  
795 identity. This identity must be verified using robust, phishing-resistant multi-factor  
796 authentication.

797 However, other attributes associated with the user and the information associated with other  
798 entities involved in an application access request, such as devices and services, are required in  
799 current enterprise IT environments and are collectively called contextual information. This  
800 contextual information set may vary from one enterprise to another and is also based on the level  
801 of trust that the organization requires for a particular access request. Since the role of contextual  
802 information in potential attacks may not be known, the set to be included in the access decision is  
803 a risk-based decision. Contextual information may broadly belong to the following five key areas  
804 [27]:

- 805 1. Information about the user requesting access – Apart from user identity, attributes  
806 associated with the user, such as their role in the organization, current assignments, and  
807 status (cross verification of identity in the enterprise IDM vs enterprise directory)
- 808 2. Information about the device from which access is being requested – Establishing trust in  
809 the device through a combination of health and risk profiles of the device. For example,  
810 the risk profile of the device can be obtained through an out-of-the-box posture check  
811 (risk of the device [28]) with or without integrating with an endpoint protection tool for  
812 the device. Other crucial information (provided by telemetry data) needed to assess the  
813 security status of the endpoint devices [29] include (a) device support label (the device is  
814 managed or corporate-owned) and (b) device posture information (whether it has been  
815 compromised). All of these factors go into a policy evaluation for determining the level  
816 of trust and must be channeled into authentication and monitoring decisions [30].
- 817 3. Information about real-time contextual data – Date, time, and geolocation at which the  
818 access request occurs
- 819 4. Information about IT services (e.g., app, data, etc.) being accessed
- 820 5. Information about the security of the environment hosting the IT services being accessed

821 The requirements for contextual information [27]:

- 822 • Should include not only that which is collected by the native platform (the platform on  
823 which the application is hosted) but also that which can be obtained from third-party  
824 platforms and can provide more detailed information
- 825 • Should be available in real time so that user experience with access is not affected
- 826 • Should be prioritized based on the value each provides
- 827 • Should be consistent with the level of risk associated with each access request

828 No application and/or data access in the modern enterprise network context can be deemed  
829 secure by ignoring relevant contextual information when the access scenario involves allowing a  
830 user, device, or service from any network channel (e.g., corporate network, home network,  
831 public network, or branch office) to access a resource located anywhere (on-premises or cloud).

#### 832 **4.6.2. Network Security Framework – Software-defined Perimeter (SDP)**

833 One conceptual underpinning for secure network access to IT resources is the software-defined  
834 perimeter (SDP) [31]. In SDP, the separation between networks is not defined by network  
835 address group or VLANs, making it network-agnostic. It is logically and dynamically defined for  
836 each user and each particular request. In other words, for each user request, the subset of IT  
837 resources to which the user has access is dynamically allocated irrespective of the location of the  
838 resource (e.g., corporate data center, branch office, private or public cloud, etc.). The salient  
839 principles of SDP include:

- 840 • The SDP concept involves making all IT resources invisible (e.g., ports, workloads, and  
841 applications) and making them known and accessible only after the user is authenticated  
842 and authorized. Only a network connection between the user and the allowed IT  
843 resources is established, thus following the least privilege principle.

- 844 • The access level determined by the previous process is continuously reevaluated during  
845 the user session and recalibrated if required. In other words, as the context surrounding  
846 the identity changes in real time, so can the user’s entitlements [31].
- 847 • Reduce the attack surface by preventing lateral movement [32] through techniques like  
848 microsegmentation, as described in Section 4.4. With the increasing deployment of  
849 microservices, the inter-services resource requests (generator of east-west traffic)  
850 dominate external application requests (north-south traffic). Application of this principle  
851 thus secures east-west traffic.

#### 852 **4.6.3. Network Security Framework – Zero Trust Network Access (ZTNA)**

853 ZTNA is the consequence of a zero trust architecture, which in turn is a realization of zero trust  
854 principles. NIST defines zero trust and zero trust principles as [33]:

- 855 • Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move  
856 defenses from static, network-based perimeters to focus on users, assets, and resources. It  
857 is a set of security primitives rather than a particular set of technologies. Zero trust  
858 assumes that there is no implicit trust granted to assets or user accounts based solely on  
859 their physical or network location (i.e., local area networks versus the internet) or based  
860 on asset ownership (enterprise or personally owned). Zero trust focuses on protecting  
861 resources (e.g., assets, services, workflows, network accounts, etc.) rather than network  
862 segments, as the network location is no longer seen as the prime component to the  
863 security posture of the resource.
- 864 • A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise  
865 infrastructure and workflows.

866 NIST’s guidance on ZTA [33] contains an abstract definition of zero trust architecture (ZTA)  
867 and gives general deployment models and use cases where zero trust could improve an  
868 enterprise’s overall information technology security posture. From the NIST vision of ZTA and  
869 state of practice implementations [34], the following have emerged as the three building blocks  
870 of ZTA:

- 871 1. **Client or Browser:** The point of entry for all users to access any resources hosted in  
872 multi-cloud and on-premises environments
- 873 2. **The Controller:** The policy decision engine, which manages the policies, conditions, and  
874 entitlements that grant access for all users, devices, and workloads from a single  
875 dashboard or via API
- 876 3. **The Gateway:** The policy enforcement point. Gateways control the flow of access to  
877 protected resources. It dynamically builds micro-segmentation rules based on granted  
878 entitlements.

879 In all security frameworks for current enterprise network environments, the common principles  
880 that underly application-specific requirements – such as low latency, high data transfer rates, and  
881 high reliability – that were applicable in previous network landscapes remain the same.

## 882 **5. Secure Wide Area Network Infrastructure for an Enterprise Network**

883 The wide area network (WAN) became an integral part of the enterprise network when  
884 organizations needed to connect their local area networks (LANs) across multiple geographically  
885 distributed locations (within the country and, in some cases, globally) starting in the 1980s. The  
886 initial WAN technology involved point-to-point (P2P) leased lines followed by Frame Relay.  
887 The first IP-based network was multiprotocol label switching (MPLS), which enabled multiple  
888 types of traffic – such as voice, video, and data – to travel on the same line.

889 With the advent of technologies such as virtualization and increasing enterprise access to cloud  
890 services, enterprises have begun to adopt a new WAN technology called the software-defined  
891 wide area network (SD-WAN). SD-WAN technology removes the tight coupling between the  
892 control plane and data plane functions of the network and enables the centralized specification of  
893 various policies, such as access control, routing, and application traffic prioritization.

894 Another development involved integrating all of the point security solutions provided by various  
895 network security appliances (Section 3) into a network security services infrastructure. Industry  
896 and industry consortiums use the term secure access service edge (SASE) [35] to refer to a  
897 comprehensive framework that offers wide area networking and various security services. SASE  
898 can be looked upon as the networking counterpart of the application’s service mesh, which  
899 provides a comprehensive set of application services, including security for cloud-native  
900 applications.

901 Based on the above discussion, this section will focus on the following topics:

- 902 • Requirements for a secure SD-WAN
- 903 • Requirements for an integrated security services architecture for SD-WAN

### 904 **5.1. Common Requirements for a Secure SD-WAN**

905 In addition to CSP-provided VPNs, a networking technology that provides network connectivity  
906 for accessing cloud-based services for enterprises is the software-defined wide area networking  
907 (SD-WAN).

908 The design goals and common features in all SD-WAN offerings include:

- 909 • Extensive connectivity: To securely connect users located anywhere (e.g., home, public  
910 location, branch office, corporate office, etc.) to applications and resources hosted  
911 anywhere (e.g., data center, single or multiple cloud services) using any WAN transport  
912 (e.g., MPLS, Broadband Internet, 4G, LTE, 5G wireless)
- 913 • Application awareness: To monitor the network traffic and dynamically choose the best  
914 path available based on (a) the type of network traffic, (b) network load conditions, and  
915 (c) the application’s business priority. This capability is enabled using techniques such as  
916 bandwidth utilization, load balancing, and the optimization of speed by reducing jitters,  
917 latency, and packet loss. Addressing application’s business priority is only possible if the  
918 SD-WAN solution has the ability to identify different types of applications (e.g.,  
919 messaging/email application, social media application, general storage-related  
920 applications, supply chain applications) and allocate routing priorities and WAN  
921 resources accordingly.

- 922 • Integration of security and networking functions: Use of appliances that contain a  
923 combination of networking and security functions (e.g., the presence of a firewall and  
924 secure web gateway [SWG] functions in a WAN router) [36]
- 925 • Centralized visibility and management capabilities: Includes the ability to recognize and  
926 authenticate newly connected appliances and bring them under the defined management  
927 workflows as nodes so as to configure a uniform set of policies that cover all components
- 928 • Integration with remote LAN locations: An additional preferred but non-essential feature  
929 is the integration of WAN and LAN functions in a single appliance (the latter going by  
930 the name SD-Branch), which can be managed using a single management console, thus  
931 providing better visibility into both components. This feature enables the connectivity of  
932 SD-WAN into the local LAN at the remote branch offices.

## 933 **5.2. Specific Requirements for WANs for Cloud Access**

934 Enterprises can gain cloud access in two ways: (1) through the VPN services provided by the  
935 cloud providers or by (2) integrating their own SD-WAN with cloud providers' private networks,  
936 often called the cloud WAN. The advantage of the second approach is that enterprises can extend  
937 their existing WANs into and across a cloud provider's private network, enabling consistent  
938 enterprise networking and security policy enforcement. Two of the advantages of this extension  
939 are:

- 940 1. Complete end-to-end visibility between "access endpoint" and IT resource (application or  
941 data) endpoint even though the latter is located in a cloud provider's network
- 942 2. Application of the network segmentation logic deployed for accessing on-premises  
943 resources to the cloud-based resources [37]

944 This orchestration of the cloud provider's private network can be achieved by designing a  
945 customized overlay network on top of the cloud provider's network as the underlay network.  
946 This feature is contingent upon CSPs offering API integrations for different SD-WAN offerings  
947 [38][39][40].

948 An architecture has emerged for managing enterprise networks that are connected to multiple  
949 CSPs. A portion of the industry calls the collection of appliances in this architecture a cloud  
950 network platform. The requirements for this multi-cloud networking platform are [41]:

- 951 • It should deliver common operational visibility and control across native network access  
952 provided by multiple cloud providers. The big challenge is that public cloud providers  
953 have different proprietary architectures using their own "constructs." In order to provide  
954 a networking architecture that can "cross clouds," one needs to leverage the cloud-native  
955 functionality (especially native cloud networking constructs) of each cloud; abstract that  
956 functionality with APIs; add advanced data plane features for high-availability, security,  
957 and operational visibility/control; and provide the tools to manage these features  
958 dynamically or automatically [42].
- 959 • It should deliver a common ingress and egress security policy for application  
960 environments (e.g., VPCs, VNETs, VCNs, etc.) across clouds.



- 961 • It should enable end-to-end encryption inside of the cloud as well as high-performance  
962 encryption from the data center to the cloud.
- 963 • It should support automation for deployment and configuration.

964 Based on the above requirements, multi-cloud networking platform offerings have emerged with  
965 the following architectural elements:

- 966 • An abstraction layer that sits on top of the native network access offered by individual  
967 CSPs to their services. This layer enables the enterprise to manage the entire enterprise  
968 network – consisting of connectivity to multiple clouds, intra-cloud connections, and the  
969 on-premises data center network fabrics – as one unit. To enable this, complete visibility  
970 into the entire enterprise network landscape is needed. Hence, this layer needs input from  
971 sophisticated observability and monitoring tools to carry out its functions.
- 972 • Choosing an infrastructure configuration (e.g., virtual private cloud configuration with  
973 isolated network segments) for hosting applications in the network infrastructure  
974 provided by the CSP is facilitated by a class of tools called IaC tools, which have features  
975 with network configuration definitions of major CSPs built in as plug-ins. This facilitates  
976 initial networking resource provisioning and subsequent modification of networking  
977 configuration and resources for hosting enterprise applications in clouds.

978 There are four industry trends [43] that may have security implications with regard to SD-WAN  
979 [44]:

- 980 1. SD-WAN access is acquired as a cloud-based service under the umbrella of network as a  
981 service (NaaS), just like IaaS and SaaS.
- 982 2. AI-based algorithms are used for monitoring networks for security-related conditions; for  
983 resiliency-improving measures, such as throttling for certain destinations; and for  
984 dynamic routing decisions to maintain QoS parameters, such as latency and bandwidth.
- 985 3. Wireless networks are used for last mile connectivity using a 5G Radio Access Network  
986 (RAN).
- 987 4. Secure remote access functionalities provided by technologies such as VPN are combined  
988 into SD-WAN [45].

### 989 **5.3. Requirements for an Integrated Security Services Architecture for SD-WAN**

990 An integrated security services architecture for SD-WAN has integrated within it both  
991 networking and security functions. The network access and security functions capabilities are  
992 offered as a cloud service that are accessible for enterprises through strategic network locations  
993 spread over a wide area called Point of Presence (PoP). The term coined by Gartner in 2019 to  
994 denote an architecture that converges networking and security functions and delivered at a global  
995 scale as a cloud service is called Secure Access Service Edge (SASE) [46]. The networking and  
996 security services delivered by a service called SASE are not new but just delivered together as a  
997 single package instead of through point security solutions (chapter 3). The various points of  
998 connectivity from the enterprise to SASE PoPs are called enterprise edges. The enterprise edges  
999 can be either:

- 1000 • Clients (Users accessing through desktops, laptops and mobile devices either from branch  
1001 offices or remote locations such as Home, or IoTs)

- 1002       • IT Resources (Internal Apps hosted in data centers or branch offices, Cloud-based Apps  
1003       (SaaS, IaaS))

1004       The SASE network infrastructure thus becomes an integral part of the enterprise network  
1005       whenever one or more of the enterprise edges get connected to various PoPs of SASE cloud  
1006       service.

1007       The three primary functions delivered by SASE are [46]:

- 1008       • Optimization of Network Traffic for different types of Traffic – Reduce Latency and  
1009       Improve Availability
- 1010       • Access Control for accessing different types of IT resources -Applications, Databases etc.
- 1011       • Threat Prevention – Monitoring, Gathering threat and attack information, remedial action

1012       Some of the structural features in SASE offerings are:

- 1013       • Globally distributed point of presence (PoP): A global SD-WAN service with its own  
1014       private backbone network consisting of worldwide points of presence (PoPs) intended to  
1015       minimize latency problems. In some instances, major cloud vendors' PoPs may also be  
1016       leveraged.
- 1017       • Security agent on devices: The security agent on the end user's device undertakes  
1018       networking decisions and directs traffic from different applications. Specific capabilities  
1019       include dynamically allowing or denying connections to services and applications based  
1020       on an organization's defined business rules.

1021       The following are the minimal security services found in an integrated architecture:

- 1022       • Firewall services
- 1023       • Secure web gateway services
- 1024       • Anti-malware services
- 1025       • IPS services
- 1026       • CASB services
- 1027       • DLP services

1028       Some of the advanced security features found in SASE offerings include:

- 1029       • Browser isolation technology: This is often combined with secure web gateway solutions  
1030       and provides improved web activity security to tackle threats in real time.
- 1031       • Continuous adaptive risk and trust assessment (CARTA) strategy: This strategy involves  
1032       constantly monitoring sessions and performs adaptive behavior analysis on monitoring  
1033       parameters to dynamically change security levels and permissions if the trust profile (e.g.,  
1034       trust deficit) of a device changes.

## 1035 **6. Summary and Conclusions**

1036 The purpose of this document is to provide insights into the current enterprise network landscape  
1037 in terms of topology, traffic flows, and security threats. It takes the view that changes in  
1038 application architecture and technologies (monolithic to microservices-based, bare metal to  
1039 virtualization/containers) and increased subscriptions to various types of cloud services (e.g.,  
1040 IaaS, SaaS) are drivers of the current state of enterprise networks.

1041 It outlines the limitations of existing network access security assumptions and technologies due  
1042 to changes in network topologies in modern enterprise networks. The emergence of new network  
1043 appliances (e.g., CASB), enhanced features in existing appliances (firewalls), network  
1044 automation tools for gathering data for visibility/monitoring, threat detection and remedial  
1045 actions, and tools for automated network provisioning for different public CSP environments  
1046 (enabled by IaC tools invoked as part of the smart workflows called CI/CD pipelines defined  
1047 under the DevSecOps paradigm) are all discussed under point security solutions. Various  
1048 networking configurations for user, device, and service authentication and authorization as well  
1049 as microsegmentation to prevent the escalation of attacks are also discussed.

1050 Finally, this document discusses the latest WAN technologies that form part of the current  
1051 enterprise network landscape, as well as the features of WAN offerings with global PoP and  
1052 integrated security services called SASE.

1053 **References**

- 1054 [1] Craven C (2019) *What is the Difference between Edge Computing and MEC*. Available at  
1055 [https://www.sdxcentral.com/edge/definitions/whats-the-difference-between-edge-](https://www.sdxcentral.com/edge/definitions/whats-the-difference-between-edge-computing-and-mec/)  
1056 [computing-and-mec/](https://www.sdxcentral.com/edge/definitions/whats-the-difference-between-edge-computing-and-mec/)
- 1057 [2] The Monitor Issue 13 (2020) *VPN Vulnerabilities Tied to Raising Data Exposure,*  
1058 *Ransomware*. Available at  
1059 [https://www.kroll.com/en/insights/publications/cyber/monitor/vpn-vulnerabilities-rising-](https://www.kroll.com/en/insights/publications/cyber/monitor/vpn-vulnerabilities-rising-data-exposure-ransomware)  
1060 [data-exposure-ransomware](https://www.kroll.com/en/insights/publications/cyber/monitor/vpn-vulnerabilities-rising-data-exposure-ransomware)
- 1061 [3] Hardcastle JL (2018) *Why CASB Is the Fastest Growing Security Category*. Available at  
1062 [https://www.sdxcentral.com/articles/news/casb-fastest-growing-security-category-](https://www.sdxcentral.com/articles/news/casb-fastest-growing-security-category-ever/2018/02/)  
1063 [ever/2018/02/](https://www.sdxcentral.com/articles/news/casb-fastest-growing-security-category-ever/2018/02/)
- 1064 [4] Proofpoint (2021) *Getting Started with CASB*. Available at  
1065 <https://www.proofpoint.com/us/resources/white-papers/getting-started-with-casb>
- 1066 [5] Lookout (2021) *Embracing Zero Trust: A Guide for Agencies to Address the Cybersecurity*  
1067 *Executive Order*. Available at [https://www.govexec.com/media/embracing-zero-trust-guide-](https://www.govexec.com/media/embracing-zero-trust-guide-agencies-address-cybersecurity-executive-order.pdf)  
1068 [agencies-address-cybersecurity-executive-order.pdf](https://www.govexec.com/media/embracing-zero-trust-guide-agencies-address-cybersecurity-executive-order.pdf)
- 1069 [6] CATO Networks (2022) *Network Firewall: Components, Solution Types, and Future*  
1070 *Trends*. Available at <https://www.catonetworks.com/network-firewall/>
- 1071 [7] Palo Alto Networks (2022) *Advanced URL Filtering*. Available at  
1072 <https://www.paloaltonetworks.com/network-security/advanced-url-filtering>
- 1073 [8] Oswal (2022) *Cloud NGFW: Managed Next-Generation Firewall Service for AWS*.  
1074 Available at [https://www.paloaltonetworks.com/blog/2022/03/next-generation-firewall-](https://www.paloaltonetworks.com/blog/2022/03/next-generation-firewall-service-for-aws/)  
1075 [service-for-aws/](https://www.paloaltonetworks.com/blog/2022/03/next-generation-firewall-service-for-aws/)
- 1076 [9] Fortinet (2021) *Fortigate Next Generation Firewall*. Available at  
1077 [https://www.fortinet.com/content/dam/maindam/PUBLIC/02\\_MARKETING/02\\_Collateral/](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/SolutionBrief/sb-fortigate-network-firewall.pdf)  
1078 [SolutionBrief/sb-fortigate-network-firewall.pdf](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/SolutionBrief/sb-fortigate-network-firewall.pdf)
- 1079 [10] F5 Networks (2022) *WAAP Buying Guide*. Available at  
1080 [https://media.bitpipe.com/io\\_15x/io\\_158522/item\\_2439191/EBOOK-SEC-798086545-](https://media.bitpipe.com/io_15x/io_158522/item_2439191/EBOOK-SEC-798086545-waap-buying-guide_FNL%20%281%29.pdf)  
1081 [waap-buying-guide\\_FNL%20%281%29.pdf](https://media.bitpipe.com/io_15x/io_158522/item_2439191/EBOOK-SEC-798086545-waap-buying-guide_FNL%20%281%29.pdf)
- 1082 [11] F5 Networks (2022) *Choose the WAF That's Right for You*. Available at  
1083 [https://media.bitpipe.com/io\\_15x/io\\_158522/item\\_2439191/EBOOK-SEC-798087620-](https://media.bitpipe.com/io_15x/io_158522/item_2439191/EBOOK-SEC-798087620-which-waf-is-right-for-you-refresh-FNL%20%281%29.pdf)  
1084 [which-waf-is-right-for-you-refresh-FNL%20%281%29.pdf](https://media.bitpipe.com/io_15x/io_158522/item_2439191/EBOOK-SEC-798087620-which-waf-is-right-for-you-refresh-FNL%20%281%29.pdf)
- 1085 [12] AT&T (2020) *The essential guide to secure web gateway*. Available at  
1086 [https://cybersecurity.att.com/resource-center/white-papers/essential-guide-to-secure-web-](https://cybersecurity.att.com/resource-center/white-papers/essential-guide-to-secure-web-gateway)  
1087 [gateway](https://cybersecurity.att.com/resource-center/white-papers/essential-guide-to-secure-web-gateway)
- 1088 [13] Itential (2020) *Redefining Network Configuration Management*. Available at  
1089 [https://www.itential.com/resource/ebook/redefining-network-configuration-compliance-](https://www.itential.com/resource/ebook/redefining-network-configuration-compliance-across-hybrid-infrastructure/)  
1090 [across-hybrid-infrastructure/](https://www.itential.com/resource/ebook/redefining-network-configuration-compliance-across-hybrid-infrastructure/)

- 1091 [14] McGillicuddy S (2022) *Taking a Strategic Approach to Network Operations*. Available at  
1092 [https://media.bitpipe.com/io\\_16x/io\\_161947/item\\_2553630/NBT002b\\_NetBrain-](https://media.bitpipe.com/io_16x/io_161947/item_2553630/NBT002b_NetBrain-)  
1093 [WP\\_Final%20%281%29.pdf](https://media.bitpipe.com/io_16x/io_161947/item_2553630/NBT002b_NetBrain-WP_Final%20%281%29.pdf)
- 1094 [15] Palo Alto Networks (2020) *The State of SOAR Report, 2020*. Available at  
1095 [https://media.bitpipe.com/io\\_15x/io\\_154375/item\\_2268964/the-state-of-soar-report-](https://media.bitpipe.com/io_15x/io_154375/item_2268964/the-state-of-soar-report-)  
1096 [2020.pdf](https://media.bitpipe.com/io_15x/io_154375/item_2268964/the-state-of-soar-report-2020.pdf)
- 1097 [16] Aviatrix (2021) *DevOps Guide to Multi-cloud Networking*. Available at  
1098 [https://media.bitpipe.com/io\\_15x/io\\_158772/item\\_2444655/devops-guide-to-multi-cloud-](https://media.bitpipe.com/io_15x/io_158772/item_2444655/devops-guide-to-multi-cloud-)  
1099 [networking%20%281%29.pdf](https://media.bitpipe.com/io_15x/io_158772/item_2444655/devops-guide-to-multi-cloud-networking%20%281%29.pdf).
- 1100 [17] Itential (2021) *Automating Multi-Cloud Networking*. Available at  
1101 <https://www.itential.com/solutions/automation-use-cases/multi-cloud-network->  
1102 [automation/#:~:text=Automating%20Multi%2DCloud%20Networking&text=By%20levera](https://www.itential.com/solutions/automation-use-cases/multi-cloud-network-automation/#:~:text=Automating%20Multi%2DCloud%20Networking&text=By%20levera)  
1103 [ging%20the%20right%20automation,automate%20the%20Network%20of%20Clouds](https://www.itential.com/solutions/automation-use-cases/multi-cloud-network-automation/#:~:text=Automating%20Multi%2DCloud%20Networking&text=By%20levera)
- 1104 [18] Verizon (2021) *The future of networking is here*. Available at  
1105 [https://media.erepublic.com/document/Network-as-a-Service\\_Solution\\_Brief.pdf](https://media.erepublic.com/document/Network-as-a-Service_Solution_Brief.pdf)
- 1106 [19] Miller LC (2021) *Data Center and Hybrid Cloud Security – E-Book*.  
1107 <https://www.paloaltonetworks.com/resources/ebooks/data-center-and-hybrid-cloud-security->  
1108 [for-dummies](https://www.paloaltonetworks.com/resources/ebooks/data-center-and-hybrid-cloud-security-for-dummies)
- 1109 [20] Vertocci B (2021) *JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens*. (Internet  
1110 Engineering Task Force (IETF) Network Working Group), IETF Request for Comments  
1111 (RFC) 9068. <https://datatracker.ietf.org/doc/html/rfc9068>
- 1112 [21] ColorTokens (2022) *What is Micro-segmentation?* Available at  
1113 <https://colortokens.com/micro-segmentation/>
- 1114 [22] Mandal A (2020) *Microsegmentation – the quintessential architecture for Zero Trust*.  
1115 Available at <https://medium.com/@anandadip/microsegmentation-the-quintessential->  
1116 [architecture-for-zero-trust-344715990c8e](https://medium.com/@anandadip/microsegmentation-the-quintessential-architecture-for-zero-trust-344715990c8e)
- 1117 [23] Kollimarla S (2021) *How Micro-Segmentation for Data Centers Works*. Available at  
1118 <https://colortokens.com/blog/data-center-micro-segmentation/>
- 1119 [24] Palo Alto Networks (2021) *Prisma Cloud Identity-based Microsegmentation*. Available at  
1120 [https://media.bitpipe.com/io\\_15x/io\\_157597/item\\_2439737/prisma-cloud-identity-based-](https://media.bitpipe.com/io_15x/io_157597/item_2439737/prisma-cloud-identity-based-)  
1121 [microsegmentation.pdf](https://media.bitpipe.com/io_15x/io_157597/item_2439737/prisma-cloud-identity-based-microsegmentation.pdf)
- 1122 [25] Slattery T (2022) *How to implement network segmentation for better security*. Available at  
1123 <https://www.techtarget.com/searchnetworking/tip/How-to-implement-network-segmentation->  
1124 [for-better-security](https://www.techtarget.com/searchnetworking/tip/How-to-implement-network-segmentation-for-better-security)
- 1125 [26] Frazier S (2021) *Why the cyber EO made zero trust no longer a suggestion*. Available at  
1126 <https://federalnewsnetwork.com/federal-insights/2021/09/why-the-cyber-co-made-zero->  
1127 [trust-no-longer-a-suggestion/](https://federalnewsnetwork.com/federal-insights/2021/09/why-the-cyber-co-made-zero-trust-no-longer-a-suggestion/)
- 1128 [27] Brasen S (2020) *Contextual Awareness: Advancing Identity and Access Management to the*  
1129 *Next Level of Security Effectiveness*. Available at <https://dbac8a2e962120c65098->  
1130 [4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/advancing-identity-access-](https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/advancing-identity-access-)  
1131 [management-to-next-level-security-effectiveness-pdf-7-w-7727.pdf](https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/advancing-identity-access-management-to-next-level-security-effectiveness-pdf-7-w-7727.pdf)

- 1132 [28] Appgate (2020) *SDP and Risky Devices*. Available at [https://www.appgate.com/blog/sdp-](https://www.appgate.com/blog/sdp-and-risky-devices-dynamic-controls-for-secure-access)  
1133 [and-risky-devices-dynamic-controls-for-secure-access](https://www.appgate.com/blog/sdp-and-risky-devices-dynamic-controls-for-secure-access)
- 1134 [29] Srinivas S (2020) *Democratizing Zero Trust with an expanded BeyondCorp Alliance*.  
1135 Available at [https://cloud.google.com/blog/products/identity-security/google-cloud-](https://cloud.google.com/blog/products/identity-security/google-cloud-announces-new-partners-in-its-beyondcorp-alliance)  
1136 [announces-new-partners-in-its-beyondcorp-alliance](https://cloud.google.com/blog/products/identity-security/google-cloud-announces-new-partners-in-its-beyondcorp-alliance)
- 1137 [30] Tanium (2021) *Tanium Insights: It's Time to Ditch the VPN for Zero Trust*. Available at  
1138 <https://site.tanium.com/rs/790-QFJ-925/images/EB-ZeroTrust.pdf>
- 1139 [31] Scheels C (2021) *VPN VS. ZTNA VS. SDP VS. NAC: What's the Difference?* Available at  
1140 <https://www.appgate.com/blog/vpn-vs-ztna-vs-sdp-vs-nac>
- 1141 [32] QTS (2020) *Driving Data Center Innovation with Microservices*. Available at  
1142 [https://media.bitpipe.com/io\\_15x/io\\_155464/item\\_2314862/QTS\\_Whitepaper\\_SDP.pdf](https://media.bitpipe.com/io_15x/io_155464/item_2314862/QTS_Whitepaper_SDP.pdf)
- 1143 [33] Rose S, Borchert O, Mitchell S, Connelly S (2020) *Zero Trust Architecture*. (National  
1144 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)  
1145 NIST SP 800-207. <https://doi.org/10.6028/NIST.SP.800-207>
- 1146 [34] Appgate (2021) *5 Steps for Successful VPN to ZTNA Migration*. Available at  
1147 [https://d3aafpijpsak2t.cloudfront.net/docs/VPN\\_to\\_ZTNA\\_migration\\_ebook-6.pdf](https://d3aafpijpsak2t.cloudfront.net/docs/VPN_to_ZTNA_migration_ebook-6.pdf)
- 1148 [35] Shread P (2020) *What is SASE and How does it Work?* Available at  
1149 <https://www.esecurityplanet.com/networks/sase/>
- 1150 [36] Fortinet (2022) *Required Capabilities for Effective and Secure SD-WAN: The Network  
1151 Leader's Guide*. Available at  
1152 [https://www.fortinet.com/content/dam/maindam/PUBLIC/02\\_MARKETING/02\\_Collateral/](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/eBooks/eb-network-leaders-guide-to-secure-SD-WAN.pdf)  
1153 [eBooks/eb-network-leaders-guide-to-secure-SD-WAN.pdf](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/eBooks/eb-network-leaders-guide-to-secure-SD-WAN.pdf).
- 1154 [37] Mann T (2021) *AWS Cloud WAN Parries Google, Microsoft*. Available at  
1155 [https://www.sdxcentral.com/articles/news/aws-cloud-wan-parries-google-](https://www.sdxcentral.com/articles/news/aws-cloud-wan-parries-google-microsoft/2021/12/)  
1156 [microsoft/2021/12/](https://www.sdxcentral.com/articles/news/aws-cloud-wan-parries-google-microsoft/2021/12/)
- 1157 [38] Mann T (2021) *Is Multi-Cloud SD-WAN's Final Destination?* Available at  
1158 <https://www.sdxcentral.com/articles/news/is-multi-cloud-sd-wans-final-destination/2021/12/>
- 1159 [39] Mann T (2021) *Google Cloud Drives SD-Underlays into Cisco SD-Wan*. Available at  
1160 [https://www.sdxcentral.com/articles/news/google-cloud-drives-sd-underlays-into-cisco-sd-](https://www.sdxcentral.com/articles/news/google-cloud-drives-sd-underlays-into-cisco-sd-wan/2021/03/)  
1161 [wan/2021/03/](https://www.sdxcentral.com/articles/news/google-cloud-drives-sd-underlays-into-cisco-sd-wan/2021/03/)
- 1162 [40] Mann T (2021) *Fortinet Fortifies Microsoft Azure vWAN With SD-WAN Firewalls*.  
1163 Available at [https://www.sdxcentral.com/articles/news/fortinet-fortifies-microsoft-azure-](https://www.sdxcentral.com/articles/news/fortinet-fortifies-microsoft-azure-vwan-with-sd-wan-firewalls/2021/11/)  
1164 [vwan-with-sd-wan-firewalls/2021/11/](https://www.sdxcentral.com/articles/news/fortinet-fortifies-microsoft-azure-vwan-with-sd-wan-firewalls/2021/11/)
- 1165 [41] Aviatrix (2021) *The Security Architect's Guide to Multi-Cloud Networking*. Available at  
1166 [https://media.bitpipe.com/io\\_15x/io\\_158772/item\\_2444655/security-architects-guide-multi-](https://media.bitpipe.com/io_15x/io_158772/item_2444655/security-architects-guide-multi-cloud-networking-v2%20%281%29.pdf)  
1167 [cloud-networking-v2%20%281%29.pdf](https://media.bitpipe.com/io_15x/io_158772/item_2444655/security-architects-guide-multi-cloud-networking-v2%20%281%29.pdf)
- 1168 [42] Aviatrix (2020) *Multi-Cloud Networking*. Available at [https://aviatrix.com/wp-](https://aviatrix.com/wp-content/uploads/2020/07/Multi-Cloud-Networking-by-Futuriom-July2020.pdf)  
1169 [content/uploads/2020/07/Multi-Cloud-Networking-by-Futuriom-July2020.pdf](https://aviatrix.com/wp-content/uploads/2020/07/Multi-Cloud-Networking-by-Futuriom-July2020.pdf)
- 1170 [43] Robb D (2022) *Top Software-Defined SD-WAN Trends*. Available at  
1171 <https://www.enterprisestorageforum.com/networking/sd-wan-trends/>

- 1172 [44] TechTarget (2022) *4 Key SD-WAN Trends to Watch in 2022*. Available at  
1173 [https://media.bitpipe.com/io\\_14x/io\\_148038/item\\_2494980/4%20key%20SD-](https://media.bitpipe.com/io_14x/io_148038/item_2494980/4%20key%20SD-)  
1174 [WAN%20trends%20to%20watch%20in%202022.pdf](https://media.bitpipe.com/io_14x/io_148038/item_2494980/4%20key%20SD-WAN%20trends%20to%20watch%20in%202022.pdf)
- 1175 [45] Doyle L (2020) *The pros and cons of SD-WAN and remote access*. Available at  
1176 [https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-SD-WAN-and-](https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-SD-WAN-and-remote-access)  
1177 [remote-access](https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-SD-WAN-and-remote-access)
- 1178 [46] CATO (2021) *5 Questions to Ask Your SASE Provider*. Available at  
1179 [https://go.catonetworks.com/rs/245-RJK-](https://go.catonetworks.com/rs/245-RJK-441/images/5_Questions_to_Ask_Your_SASE_Provider.pdf)  
1180 [441/images/5\\_Questions\\_to\\_Ask\\_Your\\_SASE\\_Provider.pdf](https://go.catonetworks.com/rs/245-RJK-441/images/5_Questions_to_Ask_Your_SASE_Provider.pdf)