LEARNING MADE EASY

Considering Context to Determine Services

for dummies®
A Wiley Brand

VMware Edition

Secure access service edge (SASE) and zero-trust network access (ZTNA) give businesses a more flexible, agile framework for secure network access. In this iPaper, we show you how businesses can use identity and context to securely connect today's dynamic and mobile workforce.

Recognizing the Trouble with Traditional Access

Modern workforces are much more dynamic and distributed than they used to be. Companies are using more cloud-based applications, and user mobility has become the norm rather than the exception. In this new normal, traditional wide-area network (WAN) models, where everything revolves around the central data center, no longer make sense. Now, SASE and ZTNA offer a more comprehensive approach to secure connectivity that's easier for IT to manage, while providing a more consistent application experience for users.

In legacy models, where trust is based on whether users are "inside" or "outside" the network perimeter, security gets complicated. First, IT has to patch together multiple solutions — network and cloud firewalls, virtual private network (VPN) concentrators, secure web gateways (SWGs), and others — to protect against the different types of threats. And patching things together is a bad idea for both Frankenstein's monster and IT. Then, because security policy is dictated by the IP address of the user and network resource, IT has to configure multiple policies for every possible way in which users may connect. This process is typically done manually, so updating these policies can be laborious and require long lead times.

This model isn't great for users either, because they end up with inconsistent, sometimes confusing access methods depending on where or how they connect. Users often wind up being the integration point for the enterprise's disparate security tools — and they may even look for ways to work around them. Security is hard enough without your own users looking to circumvent them to make their lives easier.

Simplifying Access with SASE and ZTNA

With SASE and ZTNA, connectivity is tied to a user's identity and context, not an IP address. The network grants access on a per-application basis. And it can draw on a comprehensive networking and security stack in the cloud to automatically apply the right services for every scenario. Note also that, unlike traditional networks, with SASE and ZTNA, the user can be anywhere — even at home or in a coffee shop. The network applies consistent security regardless of location.

REMEMBER

SASE makes it easy to manage access and security, no matter where or when a user logs in.

Using contextual identity in this way requires a different approach to access. Instead of focusing on abstract or indirect concepts like source and destination IP address, the network makes decisions based on direct measures of security, such as user group membership and device state. Now, security can be enforced based on real-world concepts that are easy to understand and describe:

- Who the user is
- Where and how the user connects
- Which network and security services should be applied to the user's connection

The following sections examine these concepts in detail. Then we explore how a network using SASE and ZTNA can use contextual identity to enable secure, high-performing connectivity for all access scenarios.

REMEMBER

Using smarter, more agile access models has become even more important as the number of remote users explodes. The 2020 ZK Research Work-from-Anywhere Study found that the percentage of users working remotely nearly doubled, growing from 22 percent in 2019 to 42 percent in 2020. This represents a paradigm shift in the way people work, and it demands a comparable shift in how businesses secure those users.

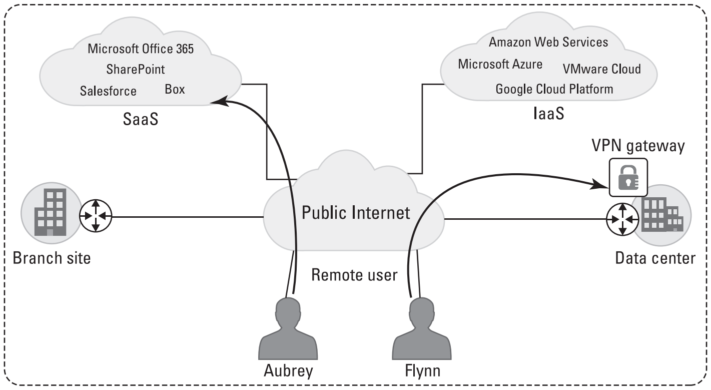
Looking at Identity and Context

To build a framework for secure access that's as dynamic and flexible as today's workforce, we need to define three basic elements:

- Identity types
- Context
- Services

Identity types

Businesses must be able to uniquely identify any user attempting to access business resources, whether hosted within the enterprise data center or in the cloud. Consider two remote users, Aubrey and Flynn (see Figure 4-1). Aubrey is an enterprise employee accessing a software-as-a-service (SaaS) application, such as Office 365, from a coffee shop over a public Internet connection. Flynn is a contractor accessing a controlled enterprise application hosted in the data center. Aubrey and Flynn are both remote users, but their unique identities matter a great deal in determining how and what they can access.



Aubrey is accessing Microsoft Office 365 over the public Internet.
Flynn is a contractor accessing a controlled enterprise application in the data center.

Figure 4-1: Identities make a difference for remote users.

Identity types can be grouped into broad categories, such as the following:

- **Enterprise users:** An enterprise user is typically a traditional employee, connecting to business applications from a branch location or corporate office, over the corporate network.
- **Remote users:** A remote user is someone accessing business resources, hosted in a private or public cloud, from outside an enterprise location or branch.
  - *Internal remote users* are part of the enterprise and need to access critical business applications from outside the office. Think of a sales manager accessing Salesforce while visiting a customer on-site, or an HR employee accessing Workday from home.
  - *External remote users* could be contractors, partners, or customers who need to access a specific business resource for a specific purpose. Examples include a contractor accessing an engineering portal to check in code or a partner accessing technical documents hosted in the private cloud.
- **Internet of Things (IoT) devices:** Human beings aren't the only types of users needing secure

access. IoT devices also connect to the network and require special security considerations. IoT endpoints used to be limited to specific verticals, but they've exploded in recent years. ZK Research predicts the number of IoT endpoints to grow from 25 billion in 2017 to a whopping 80 billion in 2025.

IoT devices can encompass a wide range of technologies. You need to secure everything from basic enterprise devices (printers, phones, videoconferencing equipment) to more innovative connected applications. For example, businesses can build safer workplaces by introducing connected cameras, thermal scanners, voice-activated devices, and other endpoints. In many cases, these devices connect over the public Internet, which means they need a higher level of security. Without adequate security, cybercriminals can easily intercept or alter data transferred between IoT devices and corporate servers hosted on-premises or in the cloud, or even hijack them to host new attacks.

WARNING

There is typically no way to load security tools onto IoT endpoints, so they must be secured via the network. That means everything, right down to the smart refrigerator reminding you to put more orange juice in the breakroom.

Context

After the network has established who the user is (identity), it analyzes the context for the access request. Context is about granting access to the right resources and applying the right services, based on a detailed picture of the user and what the user is trying to do.

The system needs some basic information to help determine context:

- How is the user connecting? What kind of device is she using and what's that device's security posture?
- Which resources is she trying to access and how sensitive are those resources?
- Which location is she accessing the network from and over what kind of connection?

The answers to those questions can dictate policy, allowing the network to apply the right network and security services automatically. In the example from Figure 4-1, we see Aubrey attempting to connect via a laptop running Windows 10, accessing an Internet application from her home Wi-Fi.

Services

The third component of contextual identity entails defining the services that the network will apply to that connection. In SASE, this includes both networking and security services, all of which can be delivered as a service from the cloud.

SASE networking uses software-defined wide-area network (SD-WAN) technology. An intelligent software network overlay selects the best path for each packet, based on real-time network conditions. To assure a consistent application experience no matter where or how users connect, SD-WAN can prioritize applications, monitor links, and automatically remediate issues. Within a SASE framework, this networking intelligence can even extend to "offnet" connections such as users' homes and remote endpoints.

On the security side, the network can apply services from the full security stack, such as the following:

- Access control lists (ACLs)
- Authentication and authorization
- Key management (Secure Sockets Layer [SSL]/Transport Layer Security [TLS])
- VPN

The network can also apply the many intrinsic security functions aggregated within SASE (ZTNA, cloud-based firewall, SWG, and others) to protect users, data, and applications in the cloud from internal and external threats.

Putting It All Together

Now, let's look at how identity, context, and services come together within a SASE and ZTNA framework. First, let's review how secure access works today.

As shown in Figure 4-2, a remote user seeking to access a business application must connect to the centralized data center via a VPN tunnel or some form of proxy device. Even if he's accessing a cloud application — even if there's a nearby cloud point of presence (PoP) for that application close to his remote location — all his traffic still gets routed through the data center, because that's where the security services live.

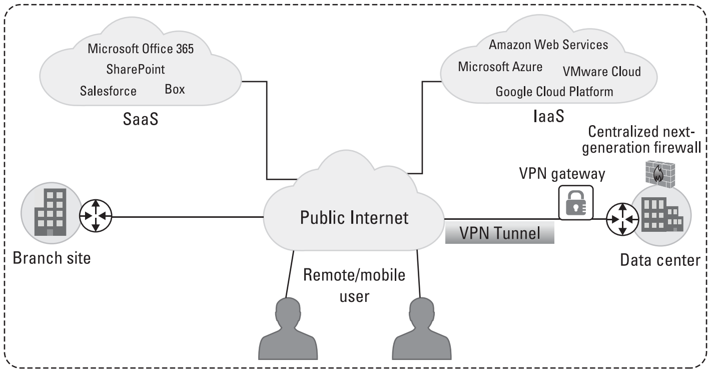


Figure 4-2: No matter where you are, the data has to make the same long journey.

Backhauling traffic in this way is inherently inefficient, adding latency that can deteriorate application performance. When large numbers of people are working remotely via public Internet connections, such as during the COVID-19 crisis, the problem gets even worse. Imagine a Los Angeles freeway at rush hour, but everybody is driving Big Wheels. This system also adds unnecessary bandwidth (and costs) as traffic "trombones" back and forth, effectively doubling the traffic volume. Finally, cloud applications often have issues with proxy security gateways, causing applications to time out and users to be frustrated.

To address these issues, enterprises want a more flexible secure connectivity model, one that's application-centric rather than network-centric and that lets users access cloud applications directly over the Internet, without performance penalties. Enter SASE and ZTNA.

WARNING

Traditional remote connectivity models based on VPNs aren't as secure as they could be, because they rely on an antiquated "inside-versus-outside" approach to trust. After a remote user is granted access to the network, she can access any resource there, including cloud applications. VPNs are also expensive and hardware-dependent, leading to high total cost of ownership. Ultimately, VPNs were designed for an earlier time, when just a small percentage of employees worked remotely. VPNs were never meant to handle today's large remote workforces.

Identity + context + services = ZTNA

ZTNA changes the game for secure remote connectivity. It implements a zero-trust model, where users can't even see corporate resources, much less access them, without explicit permission. Users access each individual application — not the full enterprise network — via a secure, encrypted connection. The network automatically applies the right security (services), allowing only trusted devices (context) and users (identity) to access the application. The network does this for both on-premises and cloud-hosted applications.

ZTNA maps each user to the policy defined for that specific application, regardless of whether the user is inside or outside the office. This allows IT personnel to maintain a single set of policies per user, reducing operational complexity and costs. It also ensures a consistent application experience, no matter where users connect from (remote or branch) or where the application resides (branch, data center, cloud, or Internet).

In the following sections, we explore what this means for different kinds of users and access scenarios.

Remote users

Bob is a remote user working on his corporate laptop from home, accessing applications hosted in the corporate data center as well as SaaS applications over the public Internet. This common scenario actually encompasses three different access models:

- **Bob accesses the Internet.** Bob types www.yahoo.com in his browser. The traffic from his home network gets redirected to a nearby SASE cloud PoP. SASE uses ZTNA to identify the user (Bob) and traffic type (Internet). As per corporate policy for Internet access, it enables URL filtering, blocking access to web content that's inappropriate or potentially dangerous.
- **Bob accesses an enterprise application.** Bob, who works in sales, logs onto an internal sales application hosted in the corporate data center. The ZTNA framework verifies that Bob is authorized to access the application, and an application-layer firewall continues to inspect all traffic over that connection. Through his zero-trust connection, Bob can't even see, much less access, any application he's not specifically authorized to use. For example, if Bob were to click a link in an email for an HR SharePoint folder, ZTNA would block that connection, because Bob's identity as a sales employee doesn't allow him access.
- **Bob accesses a SaaS application.** Bob wants to use the company's cloud-based Salesforce application to access a bill of materials for a customer. Here, the cloud-based SASE solution provides seamless, secure connectivity to a nearby Salesforce cloud PoP, without ever routing Bob's application traffic through the corporate network or exposing it to the public Internet. The SASE solution also applies the right security based on Bob's identity and the application he's accessing. Finally, the SASE solution automatically adds cloud-based anti-malware protection, guarding against viruses, spyware, and other harmful or malicious programs.

Enterprise users at a branch

Vanessa is working from an enterprise branch office, accessing corporate applications hosted in the central data center, as well as SaaS applications and infrastructure-as-a-service (IaaS) resources in the cloud, over the enterprise network.

All traffic leaving Vanessa's workstation is inspected by the lightweight firewall at the branch to apply stateful application-aware policy.

REMEMBER

This policy can be applied per user, just as in the remote access case.

Traffic destined for cloud and SaaS applications gets redirected to a nearby SASE cloud PoP for more granular inspection and analysis. As Figure 4-3 shows, this analysis can include a variety of cloud-based security services:

- Intrusion detection service/ intrusion prevention service (IDS/IPS)
- URL filtering
- Anti-malware protection
- Cloud access security broker (CASB)
- Data loss prevention (DLP)

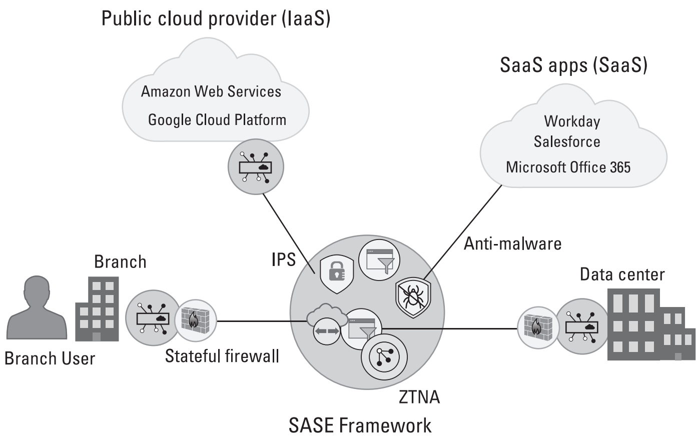


Figure 4-3: A typical SASE framework

Now, the enterprise can automatically apply additional layers of cloud security to Vanessa's SaaS and IaaS traffic, even when she's working in the branch. It uses cloud-based security like CASB and DLP to protect against data leakage and ensure that corporate security policy is always enforced — even when Vanessa is using cloud applications that don't get routed through the data center.

Internet of Things devices

A large regional grocery store chain wants to connect sensors in refrigerators at its retail stores and send temperature data to an application running in the corporate data center. The company also wants to communicate with local temperature control devices at the stores, which connect over each store's Wi-Fi network. The devices upload historical data, logs, and statistics to a cloud-based management station over the public Internet.

For both of these IoT scenarios, the framework invokes SASE components such as cloud-based firewall, IDS/IPS, and anti-malware. It automatically applies the right protection for privacy, security, and data loss. The stores stay safe, and the milk stays cold.

Where to go from here:

SASE & ZTNA for Dummies eBook

SASE & ZTNA for Dummies iPaper

Identifying the Key Components of SASE iPaper

Looking at SASE & ZTNA Use Cases iPaper

Ten (Or So) Benefits of SASE & ZTNA iPaper

ISBN: 978-1-119-81178-7