Contents

Introduction 3
SASE 4
SASE Architecture 5

Connect 6
  Branches 6
  Roaming Users 8
  Home Office 9

Control 10
  SASE Business Flows 10
  Capability Groups 11
    DNS Security 11
    Secure Web Gateway 11
    Cloud Delivered Firewall 12
    Cloud Access Security Broker 12
    Data Loss Prevention 13
    Zero Trust Network Access 13

Business Flow Capability Mapping 14
  Identity 15
  Accessing SaaS applications 16
  Accessing the Internet 17
  Accessing Private Cloud 17
  Accessing Public Cloud from IoT devices 18

Converge 18

Appendix A- Path to SASE 20
Appendix B- SASE Capabilities in Cisco’s Reference Architecture 23
Appendix C- Acronyms Defined 24
Appendix D- References 25
Introduction

Today’s workforce expects seamless access to applications wherever they are, on any device. It is now common practice to provide remote employees direct access to cloud applications such as Office 365 and Salesforce with additional security. The need for cloud-delivered security service expands daily as contractors, partners, IoT devices and more each require network access. IT needs to protect users and devices as if they were located at a corporate office or branch. Each requires secure access to applications and must now be treated as a ‘branch of one.’

Figure 1.
High level SASE Architecture

In this new paradigm, IT requires a simple and reliable approach to protect and connect with agility. This is forcing a convergence of network and security functions closer to users and devices, at the edge—and is best delivered as a cloud-based, as-a-service model called secure access service edge (SASE).
SASE

In 2019, Gartner published a report called The Future of Network Security Is in the Cloud. In this report, Gartner introduced the SASE concept. Back in 2017, several vendors and analysts in the industry defined a new concept – the secure Internet gateway (SIG). This cloud native solution offers multiple functions including domain name system (DNS) security, secure web gateway (SWG), firewall as a service (FWaaS), and cloud access security broker (CASB) to improve security and performance while reducing costs and maintenance tasks. The SASE concept goes beyond the capabilities found within SIG and includes the convergence of networking functionality as well.

![SASE Diagram]

Figure 2.
SASE Capability Overview

Cloud computing services offer convenient, pay-as-you-go models that eliminate costly expenditures and maintenance. Cloud providers host a choice of infrastructure, platform, and software offerings on-site that the “rent”, giving your organization the flexibility to turn cloud computing services up and down according to changing requirements. There are three main cloud computing service options:

- **Infrastructure-as-a-Service (IaaS)** - In this model, a cloud provider hosts infrastructure components that are traditionally located in on-premise data centers. With IaaS, your organization can choose when and how you want to administer workloads, without needing to buy, manage, and support the underlying infrastructure.

- **Platform-as-a-Service (PaaS)** - This model is one layer of abstraction above IaaS. Cloud providers, in addition to providing infrastructure components, also host and manage operating systems and middleware that your developers need to create and run applications.

- **Software-as-a-Service (SaaS)** - With SaaS, cloud providers host and manage an entire infrastructure, as well as end-user applications. When your company chooses a SaaS model, you do not need to install anything; your users will be able to log in and begin immediately using the cloud provider’s application running on their infrastructure.
The goal of SASE is to provide secure access to applications and data from your data center or cloud platforms like Azure, AWS, Google Cloud, and SaaS providers based on:

- **User Identity** – limit application access to specified users
- **Devices** – prevent compromised devices from accessing your network
- **Services** – limit user and device access to only services that have been defined for their usage

Service edge refers to global point of presence (PoP), IaaS, or colocation facilities where local traffic from branches and endpoints is secured and forwarded to the appropriate destination without first traveling to data center focal points.

The Networking-as-a-Service (NaaS) model refers to the ability to offer network management as SaaS. Likewise, for Security-as-a-Service (SECaaS). By delivering security and networking services together from the cloud, organizations will be able to securely connect any user or device to any application without having to install and maintain the network management and security infrastructure.

### SASE Architecture

![SASE Architecture Components](image)

The SASE architecture has three core components:

- **Connect** – Unleash your workforce by delivering a seamless connection to applications in any environment from any location
- **Control** – Simplify security, streamline policy enforcement, and increase threat protection by combining multiple functions into a single, cloud-native service
- **Converge** – Unite security and networking through a flexible, integrated approach that meets multi-cloud demands at scale
Connect
A centralized network model made sense when the enterprise data center was the primary destination for users to access applications and data across the network. The wide-scale use of cloud applications has become fundamental to business operations at all locations. The centralized security approach has become impractical because of the high cost of backhauling traffic and the resulting performance issues at remote locations.

To overcome these cost and performance issues, many organizations are adopting a more decentralized networking approach to optimize performance, otherwise known as direct Internet access (DIA). DIA is an architecture component in which certain Internet-bound traffic or public cloud traffic from the branch can be routed directly to the Internet, thereby bypassing the latency of tunneling Internet-bound traffic to a central site. The goal of SASE is to connect users and devices, regardless of location, to any application across any cloud. A secure automated WAN is used to optimize performance by ensuring the fastest, most reliable and secure path to the cloud.

Branches
Configuring multiple routers connected to different circuits (for example, an MPLS link and a broadband Internet link) to route network traffic efficiently and optimally can be challenging. Beyond simple load balancing, available bandwidth capacity may go unused during periods of congestion. For example, your broadband Internet connection may be running slowly during a given period of time, while your costly MPLS link is relatively uncongested and may actually be able to provide faster Internet connectivity. The inability to aggregate disparate links means wasted bandwidth capacity and lower employee satisfaction.

Software defined wide area network (SD-WAN) combines and optimizes traditional WAN technologies, such as MPLS and broadband Internet connections. This allows organizations to efficiently route network traffic to multiple remote branch locations while providing enhanced monitoring and management capabilities. SD-WAN monitors network traffic across all available links in real-time and dynamically selects the best route for each data packet traversing the network.
A SASE architecture should have the following characteristics for connecting branch locations:

- Flexible, as a service WAN management for on-premises, cloud, and multitenant environments
- Route traffic across different links (MPLS, Internet, 5G, etc.) based on destination
- Route traffic across different links based on cost
- Aggregate multiple links to provide greater total bandwidth
- Rerouting traffic across an alternate link when a link is congested, unstable, or down
- Prioritizing certain application traffic to ensure quality of service
Roaming Users
Modern organizations increasingly recognize that work is an activity, not a place. The remote workforce can be broadly classified into two groups

- **Users with managed devices** - corporate devices controlled by IT policies. Managed devices include endpoint security, device health checks and VPN clients to ensure a device has not been compromised before connecting to the VPN network

- **Users with unmanaged devices** - includes the personal or mobile devices or other non-corporate devices that are not strictly controlled by the IT policies. Without the ability to install software on the device itself, exposure to sensitive applications may be minimized. However, business critical applications, data, as well as credentials may still be exposed when presented with proof of identity

The differentiation between public and private applications will be discussed in the ‘Control’ section below.

![Diagram of Roaming User to SASE Cloud]

Figure 5.
Roaming User to SASE Cloud

A SASE architecture should have the following characteristics for connecting roaming users:

- VPN as a service to provide network connectivity to private cloud resources
- VPN-less access, leveraging a Zero Trust Access approach
- DIA for off network roaming
Home Office

Home office solutions, otherwise known as a ‘branch of one’, provide teleworkers with office like experiences that combine voice, video, wireless, and real-time data applications in a secure environment.

A SASE architecture should have the following characteristics for connecting the home office:

- VPN as a service to provide network connectivity to private cloud resources
- As a service management
- Prioritizing certain application traffic to ensure quality of service
- DIA for improved application performance
Control
Network security is no longer confined to the campus, branches, and data center - it is shifting to the cloud. As work moves outside the office and security moves to the cloud, the tried-and-true static perimeter-based security model just cannot keep up. Applying such static based methods to such a dynamic environment commonly ends up establishing exceptions as the rule. Effectively weakening standards and introducing new security risks, threats, as well as policy and auditing nightmares. SASE security should:

- Provide secure seamless access for users
- Provide security with consistent policy
- Update threat protection and policies without hardware and software upgrades
- Restrict access based on user, device, context and application identity
- Increase network and security staff effectiveness with centralized policy management

SASE Business Flows
SAFE uses the concept of business flows to simplify the analysis and identification of threats, risks, and policy requirements for effective security. This enables the selection of very specific capabilities necessary to secure them.

Once limited to personal apps that employees downloaded to their smartphones, SaaS apps have now become core business apps supporting critical business functions in the modern digital workplace. This solution addresses the following business flows for the modern network:

- An unmanaged device accessing business critical SaaS applications
- A managed device browsing the public Internet, such as researching product information
- An unmanaged device accessing corporate applications that are publicly accessible
- A managed device accessing corporate applications that are not publicly accessible
- A building controls application that periodically sends telemetry data to a public cloud
Figure 7.
SASE Business Flows

Capability Groups
Take a look at the key security components that comprise a SASE solution.

DNS Security

Primary Security Capability

Figure 8.
DNS Filtering capability group

DNS resolution is the first step when a user attempts to access a website or other service on the Internet. DNS Security logs and categorizes DNS activity by type of security threat or web content and the action taken, whether it was blocked or allowed.

It is critical that the DNS filter is underpinned by excellent threat intelligence sources. Threat intelligence itself is not a solution but is a crucial security architecture component. A threat intelligence platform centralizes the collection of threat data from numerous sources and formats and—most importantly—presents the data in a usable format.

Secure Web Gateway

A cloud-based web proxy or SWG provides security functions such as web category filtering, web reputation-based filtering and Web Application Firewall functions along with real-time inspection of inbound files for
malware and other threats. Content filtering by category or specific uniform resource locators (URLs) is used to block destinations that violate policies or compliance rules.

A Web Application Firewall is used to block specific user activities in select applications, such as uploading files or sharing social media content. TLS/SSL Decryption is necessary to inspect encrypted web traffic.

Network anti-malware inspects files as they traverse the network, using dynamic threat intelligence to check the disposition of files before they reach the device. File sandboxing is used to open and inspect untrusted files which could compromise an endpoint.

Figure 9.
SWG capability group

Cloud Delivered Firewall

Figure 10.
CDFW capability group

FWaaS is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. This typically includes enabling intrusion prevention rules for application-level visibility and control.

Cloud Access Security Broker
Primary Security Capability

- Application Visibility & Control
- Data Loss Prevention
- Identity Authorization

Figure 11.
CASB capability group

CASBs help control and secure the use of SaaS applications. The value of CASBs stems from their capability to give insight into cloud application usage across cloud platforms and to identify unsanctioned use. CASBs use auto discovery to expose shadow IT, detecting and reporting on the cloud applications that are in use across the network.

A vital ability of CASB is data loss prevention – the capability to detect and provide alerts when abnormal user activity occurs to help stop both internal and external threats.

Data Loss Prevention

Figure 12.
In line Data Loss Prevention

Although included as part of CASB, DLP warrants its own group. A common CASB deployment is to install out of band and to provide API based DLP functionality. For increased security, DLP should be implemented as a standalone inline feature of the SASE security stack to catch sensitive information as it passes through the network. This can then be supplemented with DLP capabilities built into a CASB.

Zero Trust Network Access
Zero Trust security takes a “never trust, always verify” approach to security. ZTNA verifies user identities and establishes device trust before granting access to authorized applications, helping organizations prevent unauthorized access, contain breaches, and limit an attacker’s lateral movement on your network. ZTNA requires a strong, cloud-based, multi-factor authentication (MFA) solution that ensures users are verified before granted access to specified resources.

**Business Flow Capability Mapping**

Not all business flows have the same requirements. Some use cases are subject to a smaller attack vector and therefore require less security to be applied. Some have larger and multiple vectors and require more. Evaluating the business flow by analyzing the attack surfaces provides the information needed to determine and apply the correct capabilities for flow specific and effective security. This process also allows for the application of capabilities to address risk and administrative policy requirements.
Figure 14.
SASE Business Flows with required Capabilities

Identity
Common across all use cases, identity is the fundamental component of ZTNA. To allow a user to communicate across the network, one must ensure the user is who they say they are through mechanisms such as MFA. Clients can include both managed and unmanaged devices. With managed devices, there is option to install endpoint security software to ensure that devices connecting to trusted networks have not been compromised. Endpoint security verifies that security patches have been installed and no harmful applications are running on the endpoint before granting access to the network.

Figure 15.
Security controls on a managed device

Unmanaged devices do not provide that luxury. When using an unmanaged device, such as a personal smartphone or PC, the user can verify their identity using MFA, however, there is no insight into what services are running on the device. Network controls must be put in place to limit network access and to detect suspicious traffic patterns.
Figure 16. Security controls on an unmanaged device

Users are not the only endpoints connected to the network. Building management systems, an example of how the Internet of Things (IoT) has brought change to the network, monitor building services such as lighting, heating and air conditioning. These devices are not only absent a user, but many do not have the capability to leverage an 802.1X supplicant or a Certificate. In this case, posture assessment can be used to control devices as they connect to the network. Typically, the device MAC address is used to uniquely identify the device, and a profile is built using information such as:

- Is the device secured using a strong method of authentication?
- What are the services it is trying to connect to?
- What ports is the device communicating on?

All of which allows us to build control policies and assign identifying tags to the devices traffic as it communicates across the network.

Figure 17. Security controls on a device that is not associated with a user persona

Accessing SaaS applications

The traffic destination also has influence on the security controls that is applied to the traffic. When accessing SaaS applications, not all security capabilities are needed. Although DNS filtering is not necessarily a requirement, it is still important that the DNS lookup for the SaaS service is secured, so the capability requirement still applies. The biggest exclusion from the list of SASE capabilities is Web security. Many business-critical applications will actually recommend, and some have the requirement for not breaking the application, to not proxy the traffic. Since the application is typically trusted, the traffic can bypass proxy rules and rely on identity (user and/or device) validation and identity-based authorization policies to control activity on the application. CASB capabilities in the SASE cloud safeguard access to SaaS applications and provide DLP services to protect data. Anti-malware must be enabled to inspect all files that go to and from the application.
Figure 18.
Security capabilities for accessing SaaS from an unmanaged device

Accessing the Internet

The Internet is the most untrusted part of any network and therefore requires the most rigorous inspection. DNS filtering blocks malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established. Web security is used to proxy all of the web traffic for a greater level of visibility and control. An increasing percentage of web traffic is encrypted, and attackers are exploiting this to hide malware, hoping to avoid detection. Web security can decrypt either all or selective TLS/SSL encrypted traffic to allow for proper filtering, inspection, blocking, and auditing.

Figure 19.
Security capabilities for accessing the Internet

Accessing Private Cloud

Although cloud is becoming widely adopted, SASE must still support the existing corporate applications that reside in private data centers or public cloud instances. Applications can be designated into two buckets; those that are accessible from the internet and those who are not. External corporate applications may have the ability to be accessed via a reverse proxy, where client’s credentials are checked before navigating through the security stack for application access. It is expected that the applications support SSO (SAML 2.0) to communicate identities across the web.

Figure 20.
Security capabilities for accessing corporate applications that can be reached from public Internet

Existing legacy apps, or the ones difficult to re-architect to be made compatible to an SSO or Zero Trust model, can be made available using VPN. In SASE, VPN as a Service (VPNaaS) should be implemented to connect roaming users and home offices to on premise applications. VPNaaS removes the need of on-premise infrastructure and becomes an easily accessible connection that is integrated within the SASE cloud platform.

Managed devices (or unmanaged devices with an installed VPN client) may access the network over an encrypted tunnel as if they were sitting on the corporate network. While some applications suit a reverse proxy implementation, more sensitive applications may require the extra layer of protection an IPsec tunnel would provide. Access could, through policy, be limited to managed devices, where endpoint software can be installed to protect sensitive information from compromised devices.
Accessing Public Cloud from IoT devices

Industrial control systems (ICS) are ever more connected to corporate IT networks. The fundamental concept of Zero Trust, who is connected to the network, works a little differently when the device has no user presence. Technology like MFA or SAML cannot be used as there are no credentials or persona assigned to the device. The “thing” is strictly just a device. In this building control use case, we identify the necessary tag to add to the traffic using the device posture as discussed in Figure 16. Once that tag, or device identity has been added to the traffic then policy can be applied as if it was a user sending data to the cloud. All data must pass through a firewall (is the device speaking to only those intended), be checked for malware (are reports, really just reports) and have some form of application visibility (is the device doing its intended function). Users who require access to the building controls application from outside of the network would follow the recommendations as outlined in the other business flows, depending on how the application has been installed.

In addition, DNS security has been purposely left out for this specific business flow, as an assumption has been made the device is communicating with a known public cloud application. DNS security is still a fundamental security capability for IoT devices to ensure the device only speaks to its intended destination. A typical next step for a compromised device is to make a command-and-control (C2) callback for control by a remote attacker. This type of attack is stopped using DNS security.

Converge

Security teams are frequently inundated by mountains of data from standalone, point security products that do not integrate with other products and require different knowledge levels and skill sets to operate and maintain. The Enterprise Strategy Group reports that 31 percent of organizations use over 50 disparate tools, and Cisco research indicates that the majority of them find it challenging to orchestrate alerts from these different tools. This lack of integration and interoperability makes it difficult, if not impossible, for security analysts to monitor and correlate security and threat information in real-time.

These challenges have grown exponentially as connected branch and remote offices have proliferated. Each location typically requires a router and firewall at minimum. In remote and branch locations, these are often purchased as commodity components that provide limited functionality and remote management capabilities. When switching to DIA at remote locations, there is a need to deliver the right level of security to users – web security, firewalls, data loss prevention, and so on. However, it is impractical to buy a separate stack of security appliances for each location. Even if some of these components in branch locations do include security tools, there are usually no IT personnel in these locations to maintain them. Over time, the hardware cannot cope with
the ever-increasing traffic loads, so the security tools will need to be migrated from these appliances to the cloud where they can be applied, managed, and audited centrally.

Figure 23. Convergence of Networking and Security capabilities into a single as a service cloud offering

The convergence and orchestration of networking and security into a single pane of glass enables enterprise networking and security teams to confidently build out their networks with the agility that modern businesses require. By consolidating secure access services from a single provider, the overall number of vendors will be reduced, the number of physical and/or virtual appliances will be reduced, and the number of agents required on an end-user device will be reduced.
Appendix A- Path to SASE

As of today, there is no known solution that covers all of the needs for SASE in a single platform. However, that does not mean that the transition and the realization of the benefits of SASE cannot begin. Cisco has many of the SASE components already in place, with additional integration among current solution sets well underway.

Figure 24.
Current Cisco SASE Architecture

Moving to a SASE model will be a gradual process as enterprise IT rethinks how to connect to the distributed information resources they need. Flexibility will be fundamental as IT chooses among multiple security and networking capabilities that best fit their operations, regulatory requirements, and types of applications. Security services can be predominately delivered from the cloud to provide consistent access policies across all types of endpoints. However, globally distributed organizations may need to apply security and routing services differently according to regional requirements.

Starting with the endpoints, your chosen method of protection will depend on where your applications are currently hosted.
Figure 25.
Which platforms protect which resources?

When protecting applications hosted in the public cloud, or protecting users as they traverse the web, Cisco Umbrella unifies SWG, DNS, firewall, and CASB functionality in one single integrated cloud-native platform. Built as a micro-services-based architecture with dozens of points of presence around the world, Umbrella provides the scale and reliability needed to secure today’s remote workforce and branch networks.

Figure 26.
Cisco Umbrella security capabilities
For applications that still remain in corporate owned data centers, many organizations will have an existing VPN infrastructure to provide enterprise connectivity to the roaming workforce. The VPN headend for most of these organizations are hardware or software appliances terminating IPsec tunnels at the corporate headquarters. For large organizations, with thousands of corporate applications and backhauled internet access, there are multiple approaches to take. Rather than making the immediate jump to VPNAaaS solutions or a clientless Zero Trust solution, organizations can make use of a combination of options to provide access to their remote workforce and gradually transition to a true SASE based architecture. The Cisco Duo Network Gateway (DNG) is a reverse proxy solution that can used to provide Zero Trust access to supported applications. For the rest of the network, continue to use the split tunnel VPN model to route users and traffic through a combination of Umbrella and the DC, depending on the application.

Finally, Cisco SD-WAN provides an overlay WAN architecture with application optimization to deliver predictable application performance in multi-cloud environments. Whether it is one site or ten thousand, the Cisco SD-WAN solution leverages an intuitive, web-based dashboard to give you instant insights about your WAN’s health, access to built-in live tools and packet capture, and centralized visibility and control over application usage both inside and between your networked sites. Cisco has two available SD-WAN solutions.

**Cisco SD-WAN powered by Meraki**

Cisco Meraki’s SD-WAN solution has a globally proven platform that gives enterprises the control to build a SASE solution that suits their needs today and easily adapts to their needs in the future. Best-in-class networking, network security and endpoint management are converged on to one platform, in the simplest way imaginable. The platform takes complexity out of every step of the enterprise SASE journey with open APIs for seamless integration across Cisco technologies and third-party systems. The Meraki Secure SD-WAN then leverages our industry leading technology and curated subset of the services enable customer flexibility, and to performantly be protected by edge or cloud security services in a seamless and automatic fashion. In doing so we connect users to applications and optimize the first mile access from whatever distributed or remote location the customer is working from. For more information see [Cisco SD-WAN powered by Meraki](https://www.cisco.com/c/en/us/products/sd-wan/meraki-smart-cloud.html).

**Cisco SD-WAN powered by Viptela**

Cisco SD-WAN is a secure, cloud-scale architecture that is open, programmable, and scalable. Through the Cisco vManage console, you can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and colocation facilities to improve network speed, security, and efficiency. Comprehensive on-premises and cloud-based security helps accelerate the transition to a SASE architecture where and when it’s needed while increasing user productivity by optimizing cloud and on-premises application performance with real-time analytics, visibility, and control. For more information see [Cisco SD-WAN powered by Viptela](https://www.cisco.com/c/en/us/products/sd-wan/viptela.html).

The advantage of staying with a single vendor is often these separate products have tight integrations between them as they move towards a SASE offering. Until a full SASE platform is available, organizations can manage their SD-WAN overlay using dedicated management software and build auto tunnels to Cisco’s Umbrella SIG platform. The SD-WAN overlay can manage which traffic is sent to the SIG and the SIG platform will manage the security policies of that traffic. As Cisco expands capabilities and provides even more integration of the platforms, adopters of these platforms will gain the benefits and move closer to a complete SASE solution.
Appendix B- SASE Capabilities in Cisco’s Reference Architecture

Considering the design discussed in previous sections of this document, all the capabilities and Cisco solutions corresponding to each capability can be mapped as below.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Security Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-malware</td>
<td>Cisco Advanced Malware Protection (integrated with Umbrella, Firewall &amp; SD-WAN)</td>
</tr>
<tr>
<td></td>
<td>Cisco Threat Grid</td>
</tr>
<tr>
<td>Application Visibility &amp; Control</td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td></td>
<td>Cisco Cloudlock</td>
</tr>
<tr>
<td></td>
<td>Cisco Secure Firewall</td>
</tr>
<tr>
<td></td>
<td>Cisco WSA</td>
</tr>
<tr>
<td>Client-based security</td>
<td>Cisco Secure Endpoint</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>Cisco Cloudlock</td>
</tr>
<tr>
<td></td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td>DDOS Protection</td>
<td>Radware</td>
</tr>
<tr>
<td>DNS Filtering</td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td>Firewall</td>
<td>Cisco Secure Firewall</td>
</tr>
<tr>
<td></td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td>Identity</td>
<td>Cisco Secure Access by Duo</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Cisco SD-WAN powered by Viptela</td>
</tr>
<tr>
<td></td>
<td>Cisco SD-WAN powered by Meraki</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Cisco Talos</td>
</tr>
</tbody>
</table>
### Appendix C - Acronyms Defined

<table>
<thead>
<tr>
<th>Capability</th>
<th>Security Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Cisco Secure Firewall</td>
</tr>
<tr>
<td>Web Security</td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td></td>
<td>Cisco WSA</td>
</tr>
</tbody>
</table>

**AWS** - Amazon Web Services  
**C2** - Command and Control  
**CASB** - Cloud Access Security Broker  
**DIA** - Direct Internet Access  
**DLP** - Data Loss Prevention  
**DNG** - Duo Network Gateway  
**DNS** - Domain Name System  
**FWaaS** - Firewall as a Service  
**IaaS** - Infrastructure as a Service  
**ICS** - Industrial Control Systems  
**IoT** - Internet of Things  
**LAN** - Local Area Network  
**MFA** - Multi-Factor Authentication  
**MPLS** - Multiprotocol Label Switching  
**NaaS** - Network as a Service  
**PaaS** - Platform as a Service  
**SaaS** - Software as a Service  
**SASE** - Secure Access Service Edge  
**SAML** - Security Assertion Markup Language  
**SD-WAN** - Software Defined Wide Area Network  
**SECaaS** - Security as a Service  
**SIG** - Secure Internet Gateway  
**SSL** - Secure Sockets Layer  
**SWG** - Secure Web Gateway
TLS – Transport Layer Security
URL – Uniform Resource Identifier
VPN – Virtual Private Network
VPNaaS – VPN as a Service
WLAN – Wireless Local Area Network
WSA – Web Security Appliance
ZTNA – Zero Trust Network Access

Appendix D - References

- Cisco SD-WAN powered by Meraki: https://meraki.cisco.com/sdwhat/en
- Cisco Umbrella: https://umbrella.cisco.com/
- SASE for Dummies: https://umbrella.cisco.com/info/secure-access-service-edge-sase-for-dummies-ebook