

•



Secure Access Service Edge

/ 'saesi /

A **consolidated** architectural solution that provides effective & homogenous levels of **security** and **experience** for users from anywhere on any device.

Comprehensive Guide to Cisco SASE



Emad M. Abdelhamid

Lead Security Architect & Cybersecurity Advisor CCDE#20230008 | CCIE(sec)#58413 | CISM® | CISA® | CRISC® | CDPSE™ | ISO27001 LA | ITIL®v4 | F5® Big-IP | NSE4 & NSE7 | PCNSE
June 25, 2024

1. Introduction

In this article, we are going to discuss Cisco SASE for both:

1. Cisco Meraki SASE: Secure Access to IaaS and Data Center
2. Secure Direct Internet Access with Cisco Umbrella

Cisco Meraki Secure Access Service Edge (SASE) technology integrates networking and security services into a single cloud-delivered solution. This approach enhances security, simplifies management, and optimizes connectivity for both branch and remote users, ensuring secure access to cloud services (IaaS) and data centers. Additionally, Cisco Umbrella provides secure internet access by filtering DNS requests and blocking malicious sites, ensuring safe browsing and protecting against threats before they reach the network or endpoints. This guide provides an in-depth look into the key components, features, use cases, capacity calculations, and best practices for Cisco SASE solutions.

2. Definitions

- **SASE (Secure Access Service Edge):** A framework that combines networking and security services into a single cloud-delivered service model to enhance security and simplify management.
 - **SD-WAN (Software-Defined Wide Area Network):** A technology that optimizes the management and operation of a WAN by separating the networking hardware from its control mechanism and using software to manage network services.
 - **IaaS (Infrastructure as a Service):** A form of cloud computing that provides virtualized computing resources over the internet.
 - **SaaS (Software as a Service):** A software distribution model in which applications are hosted by a service provider and made available to customers over the internet.
 - **PoP (Point of Presence):** An access point or physical location where two or more networks or communication devices share a connection.
 - **vMX (Virtual MX):** A virtual instance of Meraki's MX security and SD-WAN appliance designed to run in IaaS environments, providing secure connectivity and SD-WAN functionality.
 - **Auto VPN:** A Meraki feature that simplifies the configuration of VPNs, allowing secure site-to-site connections to be established automatically.
 - **CASB (Cloud Access Security Broker):** A security policy enforcement point placed between cloud service consumers and providers to combine and interject enterprise security policies as cloud-based resources are accessed.
 - **ZTNA (Zero Trust Network Access):** A security model that assumes that no part of the network is secure and requires verification for access to all resources, enforcing strict access controls and authentication mechanisms.
-



3. Main Benefits

3.1. Workloads

Workloads include applications and services hosted either on-premises or in the cloud. This encompasses Software as a Service (SaaS) and Infrastructure as a Service (IaaS) environments, ensuring secure and optimized access for users. Cisco Meraki SASE provides seamless connectivity and security for these workloads, enhancing performance and protection.

3.2. Cloud Security PoPs (Points of Presence)

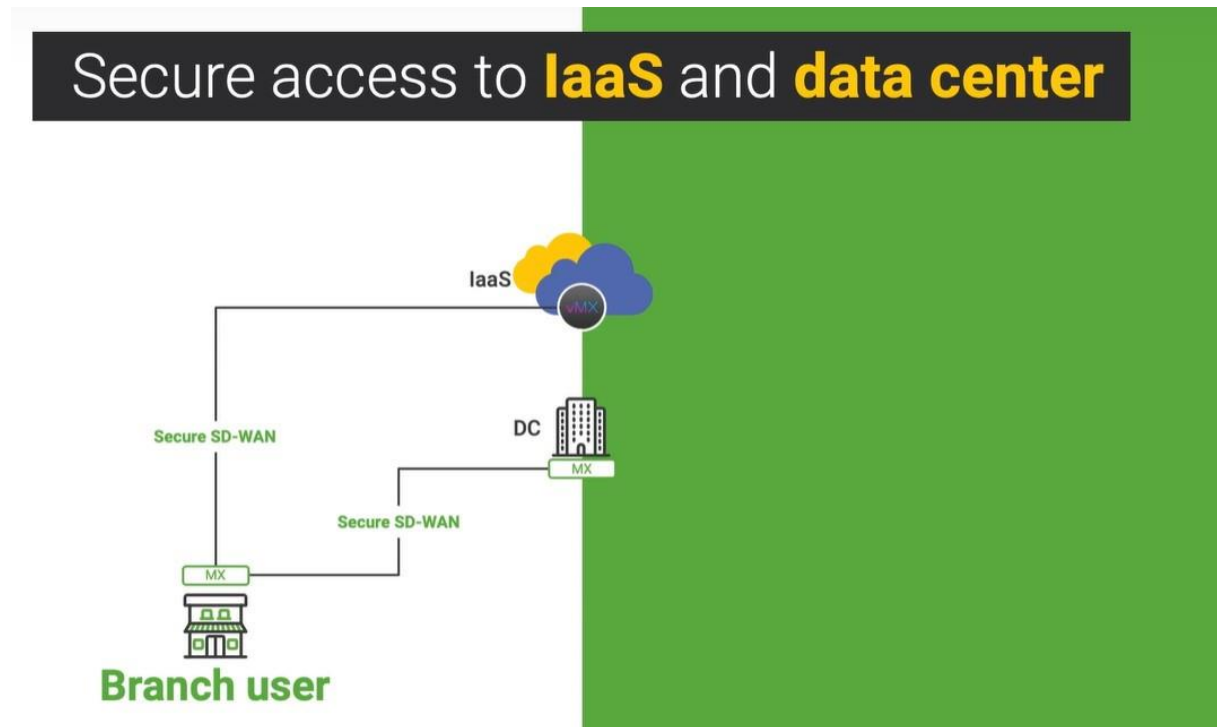
Cloud Security PoPs are strategically located nodes that provide essential security services like threat protection, content filtering, and secure access close to users and workloads. They ensure secure, low-latency connections to cloud applications and data, improving user experience and safeguarding data.

3.3. User Access from Anywhere

The platform supports secure access for any user from any location, ensuring a consistent and reliable experience across devices and networks. This includes solutions like Auto VPN and on-demand software VPNs for remote connectivity, enabling flexible and secure remote work environments.

4. Cisco Meraki SASE: Secure Access to IaaS and Data Center

4.1. Branch User Connectivity



4.1.1. Secure SD-WAN: Meraki MX appliances at branch locations provide secure, high-performance SD-WAN connectivity, optimizing traffic paths, ensuring seamless failover, and applying centralized security policies.

- **Example:** A retail chain uses Meraki MX appliances to connect each store to the corporate data center and cloud services.
- **Use Case:** Retail stores accessing centralized inventory management systems and customer databases.
- **Capacity Calculation:** Determine the number of users/devices. Estimate average bandwidth consumption per user/device. Multiply users/devices by average bandwidth. Add a buffer for peak usage (20-30%).
- **Bandwidth Considerations:** Ensure adequate upstream and downstream bandwidth.
- **Best Practices:**
 - Use traffic shaping and prioritization.
 - Monitor and adjust bandwidth based on usage patterns.

4.1.2. vMX in IaaS: The virtual MX (vMX) appliance runs in the cloud, creating a secure bridge between cloud services and on-premises networks.

- **Example:** A company using AWS for hosting applications integrates vMX in AWS for secure connectivity.
- **Use Case:** Organizations migrating workloads to the cloud need seamless connectivity between on-premises data centers and cloud environments.
- **Capacity Calculation:** Identify data transfer rate between cloud and on-premises. Assess application performance requirements. Allocate sufficient resources in IaaS.
- **Bandwidth Considerations:** Choose appropriate instance types in IaaS.
- **Best Practices:**
 - Use dedicated connections for high-bandwidth requirements.
 - Implement redundancy and failover mechanisms.

4.2. Data Center Connectivity

4.2.1. Secure SD-WAN: MX appliances in the data center ensure secure and optimized connectivity to cloud services and other data centers.

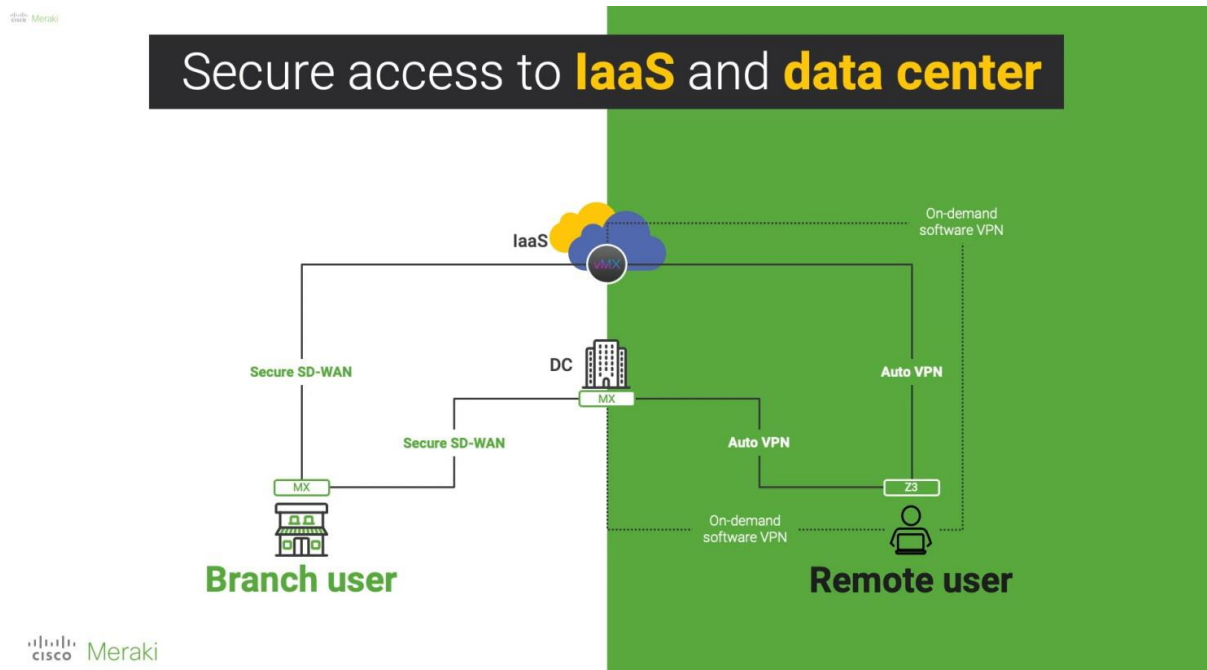
- **Example:** A financial institution uses MX appliances to secure traffic between data centers and cloud services.
- **Use Case:** Enterprises with multiple data centers need secure, reliable inter-data center connectivity.
- **Capacity Calculation:** Measure current and projected data center traffic volumes. Factor in redundancy and failover requirements. Consider future growth and scalability.
- **Bandwidth Considerations:** Ensure sufficient bandwidth for inter-data center replication and backups.
- **Best Practices:**
 - Implement QoS policies to prioritize critical traffic.
 - Regularly review and adjust capacity based on usage.

4.2.2. Integration with vMX: The data center MX appliance connects with vMX in the IaaS environment, providing a secure pathway for data and application access.

- **Example:** An e-commerce company uses vMX in Azure for secure data exchange with its on-premises data center.
- **Use Case:** Businesses requiring hybrid cloud setups benefit from secure, integrated connections.
- **Capacity Calculation:** Evaluate data volume exchanged between on-premises and cloud. Estimate peak and average data transfer rates. Allocate resources to handle the load.
- **Bandwidth Considerations:** Ensure vMX instance type supports required bandwidth.
- **Best Practices:**

- Use encryption to secure data in transit.
- Monitor performance and adjust configurations.

4.3. Remote User Connectivity



4.3.1. Auto VPN: Meraki Z3 teleworker gateway provides automatic VPN connectivity for remote users.

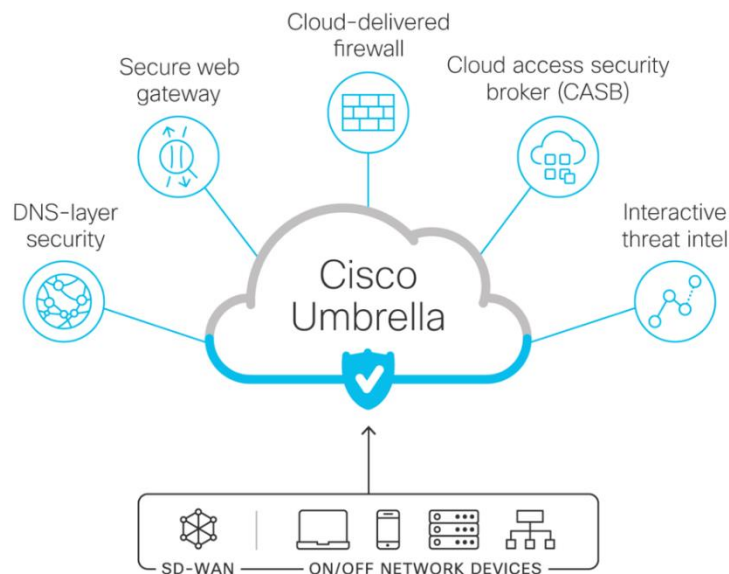
- **Example:** A healthcare organization deploys Z3 gateways for remote clinicians.
- **Use Case:** Remote workers need secure, reliable access to corporate resources.
- **Capacity Calculation:** Determine number of remote users and their bandwidth needs. Calculate aggregate bandwidth for all remote connections. Add a buffer for peak usage.
- **Bandwidth Considerations:** Ensure sufficient bandwidth for remote access traffic.
- **Best Practices:**
 - Use split tunneling to optimize bandwidth.
 - Implement MFA for enhanced security.

4.3.2. On-demand Software VPN: Remote users can use on-demand software VPN to connect securely to the data center.

- **Example:** A consulting firm uses software VPNs for consultants to securely connect to the data center.
- **Use Case:** Employees traveling or working offsite need flexible, secure access.
- **Capacity Calculation:** Estimate concurrent VPN connections. Determine average and peak bandwidth per user. Allocate sufficient resources.

- **Bandwidth Considerations:** Ensure VPN solution supports required bandwidth.
- **Best Practices:**
 - Regularly update VPN client software.
 - Monitor VPN usage and performance.

Multiple security functions in a single cloud security service



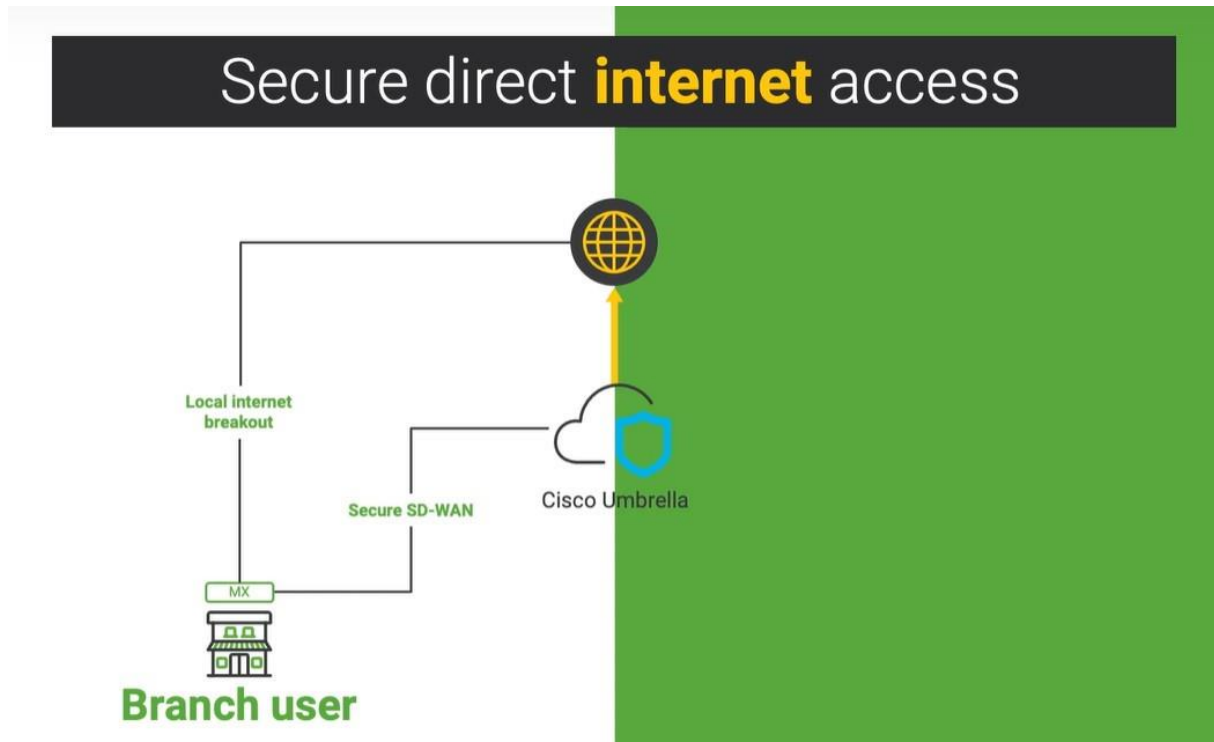
5. Secure Direct Internet Access with Cisco Umbrella

5.1. Branch User

5.1.1. Via Local Internet Breakout: Cisco Umbrella provides secure internet access by filtering DNS requests and blocking malicious sites for branch users utilizing local internet breakout.

- **Explanation:** Branch users connect directly to the internet from their local site while Cisco Umbrella enforces security policies and filters traffic.
- **Example:** A branch office uses local internet breakout for faster internet access while relying on Cisco Umbrella for security.
- **Use Case:** Branch offices needing direct, secure internet access for improved performance.
- **Capacity Calculation:** Determine the number of users and their internet usage patterns. Estimate average and peak internet bandwidth requirements. Allocate sufficient bandwidth for user traffic.
- **Bandwidth Considerations:** Ensure enough bandwidth to support direct internet access.

- **Best Practices:**
- Use Cisco Umbrella to enforce web filtering and security policies.
- Regularly monitor internet usage and adjust bandwidth as needed.

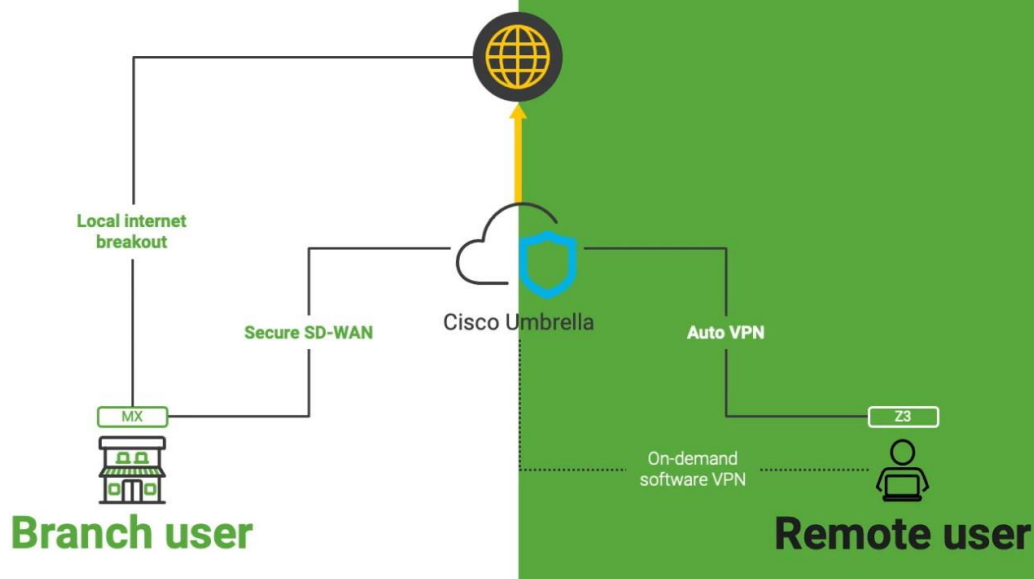


5.1.2. Branch User Using Secure SD-WAN: Branch users leverage secure SD-WAN with Cisco Umbrella for direct internet access and enhanced security.

- **Explanation:** Secure SD-WAN optimizes traffic routing while Cisco Umbrella provides threat protection and content filtering.
- **Example:** A branch office uses secure SD-WAN to route traffic efficiently and Cisco Umbrella for secure internet access.
- **Use Case:** Branch offices needing optimized, secure internet access through SD-WAN.
- **Capacity Calculation:** Assess the number of users and their internet usage. Determine bandwidth needs for SD-WAN and Cisco Umbrella services. Allocate sufficient resources for traffic routing and security.
- **Bandwidth Considerations:** Ensure adequate bandwidth for SD-WAN traffic and secure internet access.
- **Best Practices:**
 - Implement traffic shaping to prioritize critical applications.
 - Use Cisco Umbrella for comprehensive threat protection.

5.2. Remote User

Secure direct **internet** access



5.2.1. Via Auto VPN: Remote users connect to the corporate network using Auto VPN while Cisco Umbrella secures internet traffic.

- **Explanation:** Auto VPN provides seamless connectivity to corporate resources, and Cisco Umbrella secures direct internet access.
- **Example:** Remote employees use Auto VPN for corporate access and Cisco Umbrella for secure internet browsing.
- **Use Case:** Remote workers needing secure access to both corporate resources and the internet.
- **Capacity Calculation:** Determine the number of remote users and their bandwidth needs. Estimate bandwidth for Auto VPN and Cisco Umbrella services. Allocate sufficient resources for remote user traffic.
- **Bandwidth Considerations:** Ensure adequate bandwidth for VPN and secure internet access.
- **Best Practices:**
 - Use split tunneling to optimize VPN bandwidth.
 - Implement Cisco Umbrella for secure internet browsing.

5.2.2. On-Demand Software VPN: Remote users can use on-demand software VPN for secure internet access, protected by Cisco Umbrella.

- **Explanation:** On-demand software VPN provides secure connectivity for remote users, and Cisco Umbrella ensures internet traffic is secure.
- **Example:** Consultants use on-demand VPN for secure internet access while Cisco Umbrella filters and protects their browsing.

- **Use Case:** Remote employees needing flexible, secure internet access.
 - **Capacity Calculation:** Estimate concurrent VPN connections and internet usage. Determine bandwidth requirements for VPN and Cisco Umbrella. Allocate sufficient bandwidth for secure connections.
 - **Bandwidth Considerations:** Ensure VPN solutions support required bandwidth.
 - **Best Practices:**
 - Regularly update VPN client software.
 - Monitor VPN and internet usage to ensure performance.
-

6. Additional Features

A platform designed to **easily embrace SASE**



6.1. Best-in-Class Security:

Cisco Meraki SASE provides comprehensive security features like VPN, firewall, SWG, CASB, and ZTNA to protect data, applications, and users.

- **Example:** A manufacturing company uses Meraki SASE to enforce security policies across facilities.
 - **Use Case:** Industries with stringent security requirements, such as finance and healthcare.
 - **Best Practices:** Implement comprehensive security policies. Conduct periodic security audits and vulnerability assessments.
-

6.2. Quality of Experience:

The platform ensures high-quality user experience by optimizing network performance and minimizing latency.

- **Example:** A global enterprise ensures Traffic prioritization and QoS (Quality of Service) for smooth video conferencing and VoIP calls for employees worldwide.
 - **Use Case:** Organizations with remote and mobile workforces.
 - **Best Practices:** Monitor network performance and user experience metrics. Implement QoS policies to prioritize critical applications.
-

7. Conclusion

Cisco Meraki SASE offers a comprehensive, scalable, and secure solution for modern network access and security needs. By integrating SD-WAN and advanced security features into a single, cloud-managed platform, Meraki simplifies network management while ensuring robust protection and optimal performance for both branch and remote users. The visual representations illustrate how Meraki SASE facilitates secure access to IaaS and data center resources, addressing diverse use cases across various industries.

8. List of Resources

- Cisco Meraki SASE Overview: [Cisco Meraki SASE](#)
- Cisco Meraki SD-WAN: [Cisco Meraki SD-WAN](#)
- Cisco Meraki vMX in IaaS: [Cisco Meraki vMX](#)
- Cisco Meraki Auto VPN: [Cisco Meraki Auto VPN](#)
- Cisco Meraki Security Features: [Cisco Meraki Security](#)
- Cisco Umbrella for Cloud Security: [Cisco Umbrella](#)
- Best Practices for Implementing SD-WAN: [Cisco SD-WAN Best Practices](#)
- Zero Trust Network Access: [Cisco Zero Trust](#)