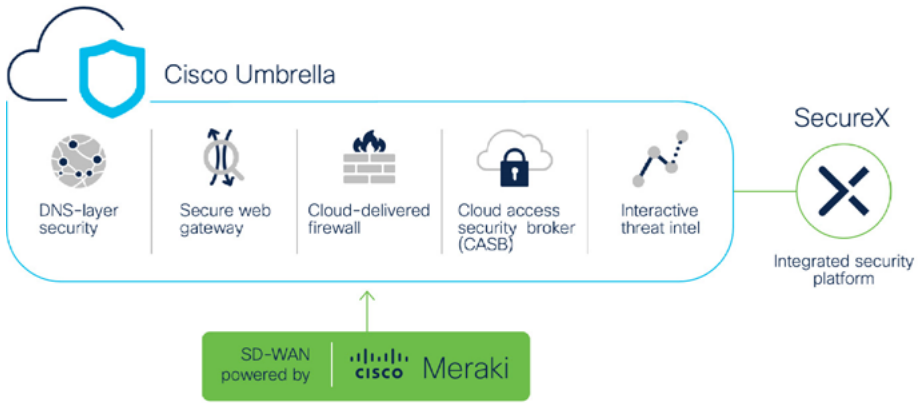
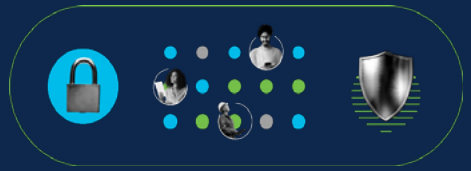
Meraki MX and Cisco Umbrella integration offers simple, fast start to SASE

Secure Access Service Edge (SASE) combines multiple security and networking capabilities to deliver secure access wherever users and applications reside. If you are an existing customer of Cisco Meraki MX or considering Meraki MX for your security and SD-WAN needs, you should explore Cisco Umbrella's cloud-native security. Meraki MX and Umbrella integration provides an easy, fast start to your SASE journey.

The Meraki Umbrella SD-WAN connector integrates Meraki SD-WAN and Cisco Umbrella, making it easy to deploy cloud security across your SD-WAN fabric with only a few clicks. No need to spend hours on manual configuration or building complex routing tables and redundancy anymore! With streamlined network configuration and security enforcement, you can secure cloud access and protect users on- and off- the network more easily and consistently. Meraki's intelligent path selection with automatic load balancing maximize performance and reliability.

Powered by the global cloud architecture, Umbrella enables SSL decryption at a scale not possible with on-premises hardware, protecting every user inside your Meraki SD-WAN network against internet-based threats and also protecting them when they work remotely.





What is SASE?

Gartner coined the term Secure Access Service Edge (SASE) to describe combining comprehensive WAN capabilities with comprehensive network security functions to support the dynamic secure access needs of digital enterprises. Cisco's approach to SASE combines leading security and SD-WAN functionality to help secure access wherever users and applications reside.

Unified security with flexible enforcement

Umbrella is a core component of Cisco's SASE architecture. It unifies multiple security functions, including DNS-layer security, secure web gateway, cloud-delivered firewall, cloud malware protection, application discovery, data loss prevention, and remote browser isolation to simplify management, improve security efficacy, and increase visibility.

With flexible policies, you can choose to deploy only DNS-layer protection or more advanced web and application inspection based on your business needs.

Our global cloud architecture delivers network resiliency and reliability, providing high performance and secure connections. Automatic failover ensures high availability to give your users the secure, reliable experience they expect.

By deploying Umbrella across your Meraki MX devices, you will get simple and scalable security that will help you get a fast start to your SASE journey.

Benefits

Simple

- Fast protection of users across your distributed network with simple, flexible deployment options
- Higher security efficacy with less effort and less resources

Secure

- Multiple layers of security from a single, cloud-native service
- Flexible policy enforcement for any use case
- Off-network protection using Umbrella without a VPN
- Continuous protection with automatic failover

Scalable

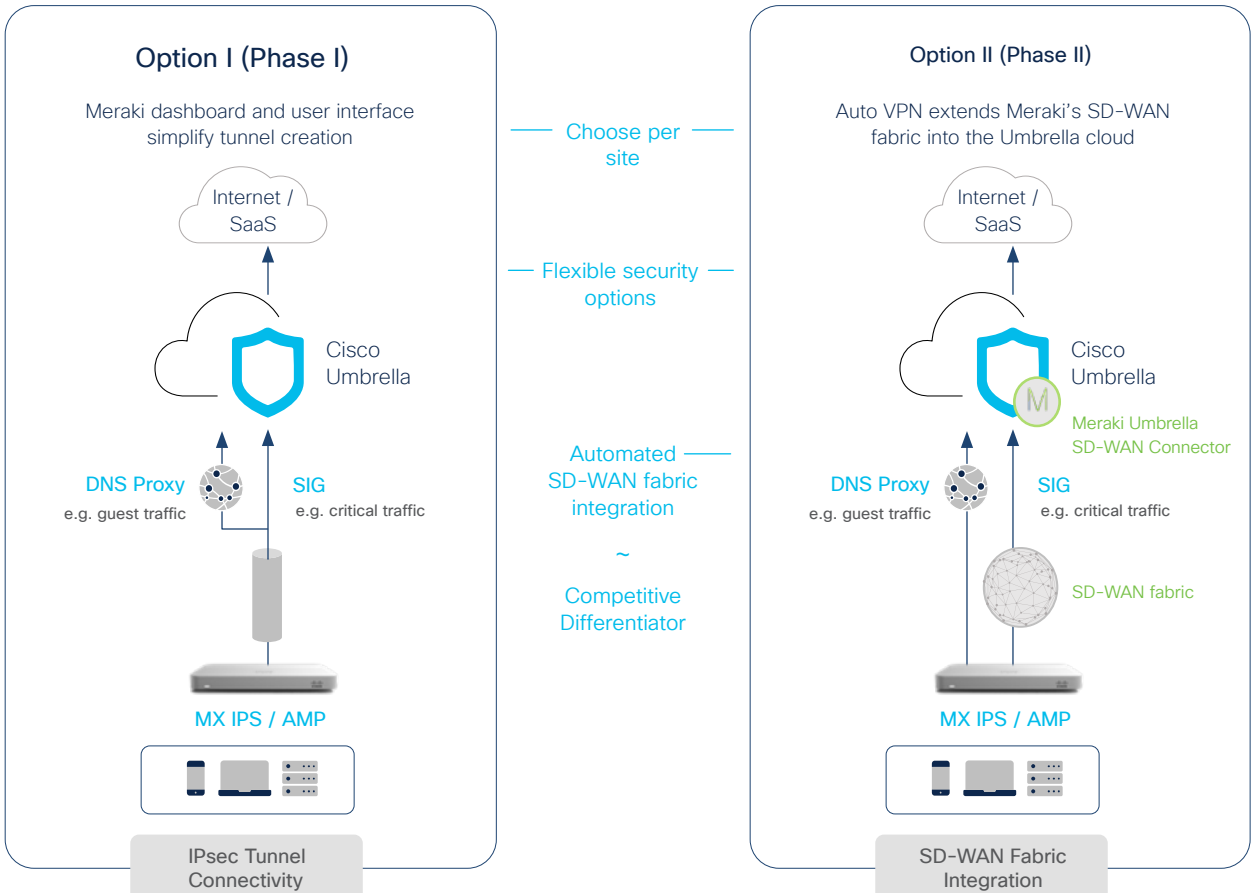
- Consistent high-performance security for multi-cloud demands
- SSL decryption at scale not possible with on-premises hardware

Integration options

Option I enables customers to easily create IPSEC tunnels from Meraki MX devices to Umbrella through the Meraki dashboard and user interface. It uses the non-Meraki VPN peer options and can leverage API scripts for scale.

Option II leverages the Meraki Auto VPN to extend Meraki's SD-WAN fabric into the Umbrella cloud with just a few clicks. As new tunnels are added, Umbrella policies are automatically applied for easy setup and consistent enforcement. Meraki's dynamic policies and intelligent path selection with automatic load balancing maximize performance and reliability.

Customers can mix and match Options I & II as it makes sense in their environments.



cisco SECURE

Features

Capability description	Why it matters
Can utilize Meraki application-based routing to selectively inspect traffic	Trusted applications can be excluded from Umbrella's deep inspection engines when you want to leverage a regional co-location facility, a direct connection to a cloud provider, or simply remove the security inspection overhead
Allows traffic forwarding to Umbrella using IPSec tunnels for cloud-delivered firewall and secure web gateway inspection	Provides additional security controls and granularity to protect users with direct internet access
Offers traffic exclusion (VLANs/subnets)	Enables basic traffic controls by IP address or interface

797321389 12/21