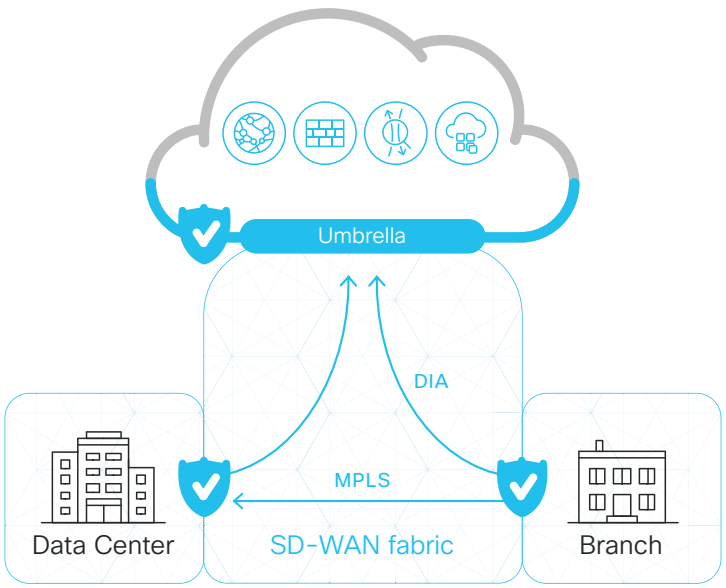
Cisco SD-WAN and Cisco Umbrella

Simplified cloud security for your distributed network

What if you could secure every user across your SD-WAN in minutes with a single configuration, and no additional appliances? That's the power of Cisco SD-WAN and Umbrella together.



Protect users at direct internet access locations in minutes

The Cisco SD-WAN and Umbrella integration enables you to gain simple, effective cloud security for your Cisco SD-WAN fabric. Umbrella combines multiple security services in a single cloud-delivered platform to offer powerful security capabilities that are easy to deploy and manage.

To get started, you can quickly deploy Umbrella's DNS-layer security across your network to hundreds of devices and instantly gain protection against threats such as malware, ransomware, and C2 callbacks – powered by Umbrella's global network and Talos threat intelligence. You can also enable additional security services with Umbrella – such as secure web gateway and firewall capabilities (in Limited Availability) – to gain even greater granularity and control.

Why use the integration?

Simplest way to deploy Umbrella across Cisco SD-WAN fabric

Enable deeper inspection and control with cloud-delivered firewall and secure web gateway capabilities[1]

Easily scale security with future SaaS and web traffic growth

Market trends[2]

1. Four out of five organizations are shifting to direct internet access (DIA) for all or some remote and branch offices
2. 76% of organizations use SD-WAN extensively or selectively
3. 68% of roaming and branch/ remote office employees have been targeted in recent attacks

Take a Test Drive

Sign up for a free 14 day trial. You can get started in less than 30 minutes, with no credit card or phone call required.

1. In Limited Availability | 2. ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019

New to Cisco SD-WAN?

A cloud-delivered WAN architecture that enables digital and cloud transformation at enterprises.

- Manage connectivity across your WAN from a single dashboard
- Connect to SaaS and IaaS platforms with speed, reliability, security and cost-savings
- Visibility and analytics into any connection across your network, whether MPLS or across the cloud edge

New to Umbrella?

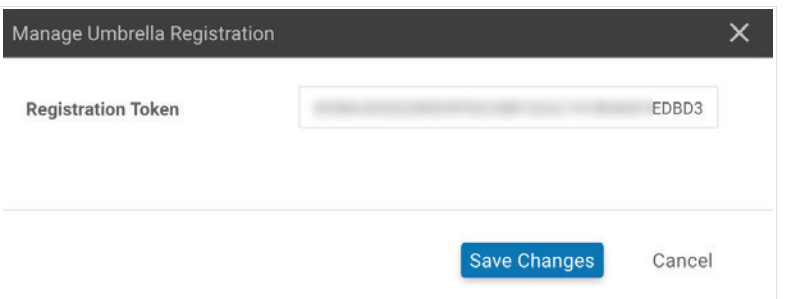
A cloud-delivered secure internet gateway (SIG) that provides the first line of defense and inspection against threats on the internet, anywhere users go.

- Protect against threats such as malware, ransomware, & C2 callbacks with no added latency
- Gain visibility into internet activity across all locations and users
- No hardware to install or software to manually update

How to get started in just minutes with DNS-layer security

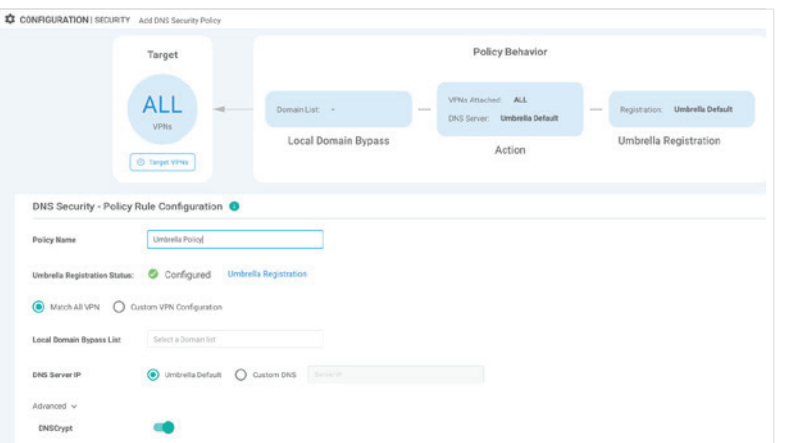
Step 1 - Link accounts

Simply input the API key from Umbrella into the vManage dashboard.



Step 2 - Apply Umbrella policies

In the vManage dashboard, assign Umbrella DNS re-direct policies on a per-VPN basis or to all VPNs.



Step 3 - Create Umbrella security policies

If you're new to Umbrella, we recommend you create policies for your organization. The intuitive Umbrella policy wizard walks you through each step.

To enable additional security services beyond DNS-layer, simply deploy an IPSec tunnel to Umbrella's cloud platform.

Integration features

Feature	Why it matters
Cisco SD-WAN enabled devices will automatically redirect DNS traffic to Umbrella resolvers with a single configuration change	Ensures all devices and users in branch office locations are protected by Umbrella. Provides convenience to deploy Umbrella across many devices without leaving the vManage dashboard.
Appends EDNS (Device ID and Client IP) to the DNS packet	Enables Umbrella to enforce policies per VPN, and provides visibility in the Umbrella dashboard (VPN and client IP).
Supports split DNS to exclude internal DNS requests from being sent to Umbrella resolvers	Allows users to reach your network's local resources (computers, servers, printers, etc.) on internally-hosted domains that rely on local DNS servers
Supports DNSCrypt proxy to encrypt the DNS traffic	Secures DNS traffic from eavesdropping and man-in-the-middle attacks
Traffic can be forwarded to Umbrella using IPSec tunnels for cloud delivered firewall and secure web gateway inspection[3]	Provides additional security controls and granularity to protect users with direct internet access

Get Started Today

Contact a Connection expert to transform your network security with Cisco SD-WAN and Umbrella.

Connection we solve IT

Business Solutions 1.800.800.0014
Enterprise Solutions 1.800.369.1047
Public Sector Solutions 1.800.800.0019
www.connection.com/Cisco

3. In Limited Availability for vEdge devices only, expanded device support planned

C1462798-0921