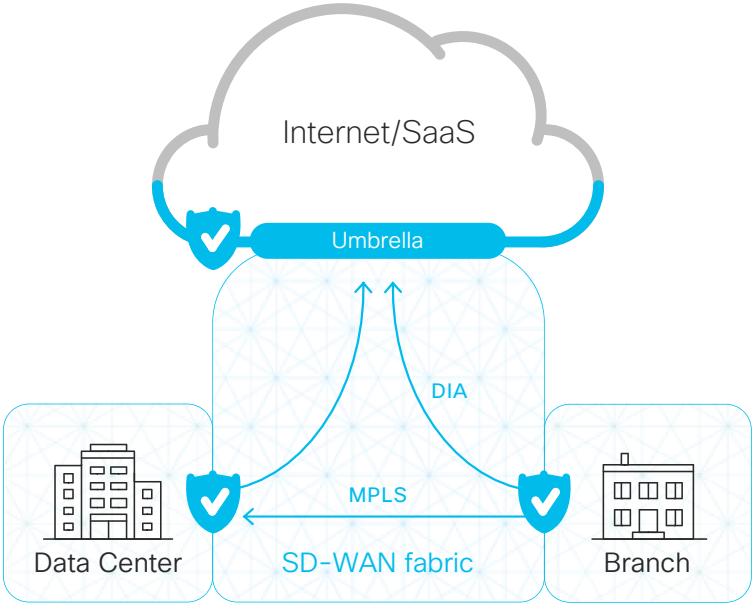
Solution brief
Cisco Umbrella

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? 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 allows you to easily deploy Umbrella across your network to hundreds of devices and instantly gain web and DNS-layer protection against threats such as malware, ransomware, and C2 callbacks.

Why use the integration?

- Simplest way to deploy Umbrella across Cisco SD-WAN fabric
- Gain web and DNS-layer protection against threats
- Create policies and view reports on a per-VPN basis

Market trends

40% to 60% of enterprise data traffic has migrated from private WANs to the internet[1]

For the average enterprise, 80% of users are located at branch offices[2]

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 secure internet gateway that provides the first line of defense against threats on the internet.

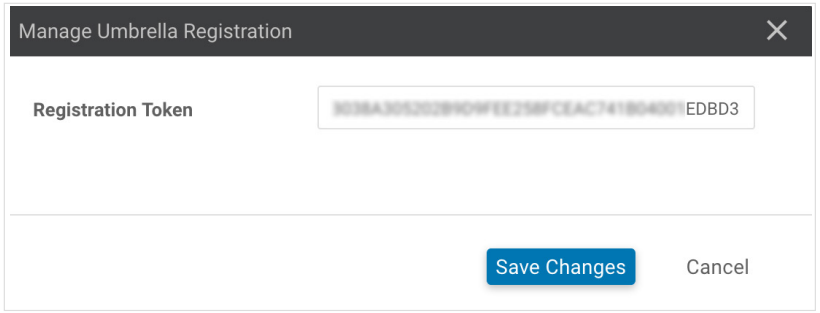
- Protection against threats such as malware, ransomware, & C2 callbacks with no added latency
- Visibility into internet activity across all locations and users
- No hardware to install or software to manually update

1. "Network Evolution and Market Outlook," IDC, 2017 | 2. "It's not your dad's branch office," Nojitter.com, 2016

How it works

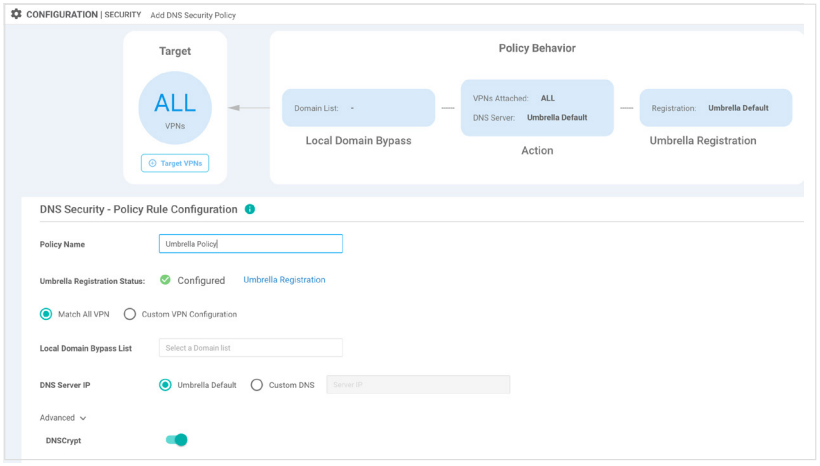
Step 1 - Link accounts

Simply input the API key from Umbrella into the Cisco SD-WAN 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.

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 the right policies for the right devices (Device ID) and provides visibility in the Umbrella dashboard (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

Take a test drive

Start My Free 21-Day Trial

www.VentureNetSolutions.com