Cisco Umbrella Branch

Benefits

- Easily manage content filtering for guests and corporate users
- Use threat prevention to reduce your branch-office attack surface
- Deploy in minutes; no need for special security skills
- Benefit from a cloud service that integrates with your existing Cisco 4000 Series Integrated Services Router security

"Monitor your DNS connection, among the single best sources of data within your organization. Compare these to your threat intelligence, and mine this data often."

– Verizon
2014 Data Breach Investigations Report

Shrink the Attack Surface in Your Branches

Organizations with lots of distributed branch offices – like those in retail, finance, hospitality, and education – deliver guest Wi-Fi service as part of transacting business. Organizations must prevent guests and employees from accessing inappropriate and productivity-impacting content. They also need to keep them off risky Internet sites that might host phishing campaigns or malware that could be downloaded to the user's computer.

You need a simple way to defend against these type of threats. With about 80 percent of enterprise workers and customers served in branch sites today, that's a lot of users and devices to protect. And Cisco® Umbrella Branch does just that.

The solution is a cloud security service integrated with your Cisco 4000 Series Integrated Services Router (Cisco IOS® Software Release 16.3). Up and running in no time, it is your first layer of defense against threats at the branch office.

Simple Yet Powerful

Cisco Umbrella Branch brings a simple-to-use content filtering solution to your branch offices. It stops Wi-Fi guests from accessing inappropriate content and keeps employees focused on productivity when on the Internet, so you can keep customers happy with Internet access while protecting your business with the ability to block millions of malicious sites without performance impact.

Cisco Umbrella Branch also delivers much more. You get a layer of protection for all branch users from malware, botnets, phishing, and targeted online attacks. Extensive real-time threat intelligence works in conjunction with DNS to keep users from connecting to malicious sites. Because DNS precedes all Internet activity, it's a powerful way to enforce security and gain insight at branch offices. Protection is built in and enabled by default.

Protection in Minutes

You'll have Cisco Umbrella Branch up in no time. Cisco 4000 Series ISR configuration is simple, and so is configuring the Umbrella service, with no need for special security skills. Default policies and security are enabled from the start.

The solution runs alongside the Cisco VPN, Zone-Based Firewall, Snort® IPS, Cisco Firepower™ threat defense, and Cloud Web Security on the 4000 branch ISR. Interoperability testing helps to ensure that all the components work together smoothly.

Start protecting your branch computers and your own network today.
Visit www.cisco.com/go/umbrella-branch.

C45-737403-00 07/16