Cisco IT Methods

Cisco IT Hits Milestone with Cisco Umbrella

Introduction

Cisco Umbrella, formerly known as OpenDNS, is a secure Internet gateway in the cloud. It provides increased protection from phishing, malware, botnets, and breaches and gives our security and IT teams increased visibility and audit capabilities. Cisco acquired OpenDNS in 2015 and began adopting the cloud service for our own use in April 2016, eventually renaming the product.

Implementation of Cisco Umbrella has been easier and faster than the teams from Cisco IT and Information Security (InfoSec) had expected. “This product really scales,” says Abhijeet Patkar, Cisco IT technical lead and software architect on the project. “We were able to deploy and scale it with minimal changes to our internal network. We did it quickly, too, and without disrupting users, even though we had a legacy deployment of our DNS that was about 18 years old.” He adds, “The results have been very encouraging, and the ability to deploy through cloud configuration has proven to be less invasive. End users are hardly noticing the changes deployed during their day-to-day activities until they are blocked from accessing malicious sites.”

By mid-April 2017, Cisco IT had successfully upgraded more than 123,000 Cisco AnyConnect Secure Mobility Client desktop users to the Cisco Umbrella service. The mandatory upgrade for all AnyConnect desktop users marked a critical milestone in the second phase of deployment for Cisco Umbrella, which is planned for completion in July 2017. Before the AnyConnect desktop deployment, threat-blocking capabilities were only available to internal DNS users on the Cisco network. But with the lightweight Cisco Umbrella client, AnyConnect users now get the same protection when they are outside the Cisco network.

Cisco Umbrella also helps to protect employee privacy; while it provides Cisco information about what threats it blocks when a device is not attached to the Cisco network, it offers no details about users’ private browsing activities.

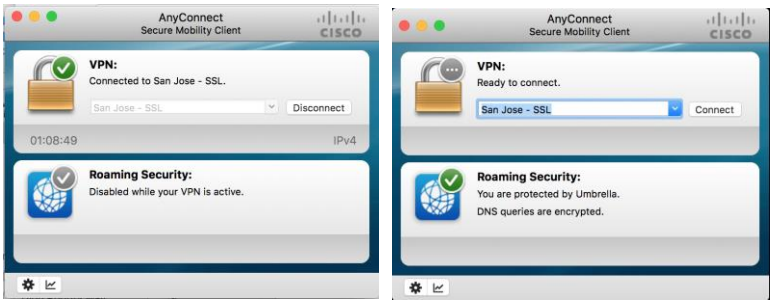
Solution and Deployment

The Roaming Security Module

The pilot program for the second phase of the Cisco Umbrella deployment began in late 2016 and included about 400 users in the Cisco AnyConnect Early Adopters Program, a voluntary sign-up test environment. About 300 additional volunteers from Cisco IT and InfoSec also took part in the pilot. Damien Stenning, a senior network engineer with Cisco’s Home and Remote Access Team, led the effort to implement the roaming security module for the Cisco AnyConnect solution. “We pushed out Cisco Umbrella as an update to our existing AnyConnect clients,” he explains.

Once implemented, users can see the roaming security module displayed below their VPN module in AnyConnect (Figure 1).

Figure 1. The New Cisco AnyConnect Client Includes Cisco Umbrella; a Green Checkmark Toggles between VPN and Roaming Security.



Stenning adds, “The configuration for the module was very simple. We uploaded a new version of the AnyConnect package to the Cisco Adaptive Security Appliance (ASA) and added a profile for roaming security that connected back to our instance of Cisco Umbrella. We tied the package to the group policy for desktop clients, and then enabled the new module within the entire group configuration.”

Blocking of Malware and Botnet Activity

Cisco Umbrella’s threat-blocking policies were deployed on the network during the second phase of the rollout. Cisco Umbrella is dormant when a user is on a trusted network. As soon as the AnyConnect client understands that the user is outside of the network, the service becomes active and starts monitoring the user’s requests and providing protection from malware, botnets, and other threats, according to Patkar.

“That’s where the real value started coming in for Cisco IT,” he says, “and it’s what the InfoSec team has been most excited about.”

Figure 2 shows the impact of Cisco Umbrella’s threat-blocking policies on preventing malware and botware from being downloaded to the desktops of Cisco AnyConnect users.

Figure 2. Malware and Botnet Activity Volume Before and After Deployment of Cisco Umbrella with Threat-Blocking Capabilities

“Cisco Umbrella shows value add immediately,” says Patkar. “It is delivering value to Cisco by providing good protection when users are off the network—and by being easy to deploy.”

A Testament to Remote Working at Cisco

Cisco Umbrella was rolled out to Cisco’s smaller VPN sites during a four-day period in February 2017, and then to all sites, including San Jose, Calif., later that same week. By the following Monday, 76,818 user desktops had been upgraded to the new AnyConnect client. And by late April, more than 123,000 Windows and Mac desktops had been upgraded.

Stenning says, “The fact that we were able to hit 100,000 unique endpoints so quickly with the deployment shows that remote working is thriving at Cisco. It’s a testament to how valuable our remote access services are to Cisco and its employees.”

Next Steps

By mid-April 2017, about 20,000 AnyConnect desktop users had not yet upgraded to Cisco Umbrella. Patkar and Stenning say these users were Cisco employees who don’t work remotely, or use the Cisco Virtual Office (CVO) for remote access. (CVO is a solution that allows remote users to have a router in their home connected back to Cisco; it eliminates the need for software VPN and enables remote users to have an office-like experience with collaboration endpoints in addition to their desktops.)

The remaining users were upgraded to Umbrella by the end of April. The task was completed in about two weeks with help from Cisco IT’s desktop team.

Another next step, longer term, is to provide protection for mobile users whether or not they are on a trusted network. “Cisco’s OpenDNS business unit is working to develop a solution that will protect mobile devices,” says Patkar.

Lessons Learned

We learned the following lessons during the second phase of our Cisco Umbrella deployment:

- The mandatory upgrade was effective at transitioning thousands of AnyConnect clients in about a week’s time. However, this was a departure from our usual approach of giving users about a month to upgrade. “We will strive to improve our communication to users and the people selling our products about any planned mandatory upgrades,” says Stenning.
- We will likely need less time to deploy new modules in the future. “This was our first new module deployment in the AnyConnect environment, so we were cautious,” says Stenning. “Moving forward, it’s likely that we can reduce the time needed for testing and shrink our timelines for deployment. We can probably test and deploy a new module in a two-month time window.”

For More Information

To learn more about Cisco Umbrella, visit https://umbrella.cisco.com/.

For more details on how Cisco IT implemented OpenDNS (now Cisco Umbrella), go to http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/m-sec-06292016-openDNS.html.

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.