Cisco IT Methods

How Cisco IT Implemented OpenDNS

Introduction

In August 2015, Cisco® completed its acquisition of OpenDNS®, adding threat intelligence and global enforcement capabilities to our cloud-delivered security portfolio. In April 2016, Cisco IT adopted the OpenDNS cloud service for our own use. We had two goals:

- Increase protection against malware, botnets, and breaches. As a global DNS provider network, OpenDNS sees 2 percent of the world's Internet requests. It quickly learns about and blocks emergent threats before they have a chance to do harm.
- Gain insights about risky user behavior. OpenDNS generates a log showing all activity on the Internet, regardless of port and protocol. The logs give our security and IT teams increased visibility and audit capabilities.

Transitioning to OpenDNS was exceptionally simple. "We added powerful new controls without deploying new hardware, reconfiguring the network, conducting extensive interoperability testing, or changing any of our other systems," says Rich West, Information Security (InfoSec) architect. This article describes the process.

Solution

Selecting Team Members and Planning

We formed an 8-member team from IT and InfoSec to plan and implement OpenDNS. Over 2 months, team members spent approximately 5 to 10 percent of their time on the project. "Our goal was making the transition to OpenDNS with no downtime or other impacts," says Steve Smith, member of the technical staff in Cisco IT and lead for Cisco's internal DNS services.

The technical aspects of the transition took very little time. The team members spent most of their time meeting with application owners and network operations teams to explain the benefits of the transition and to answer any questions related to potential application or network performance.

Converting to OpenDNS

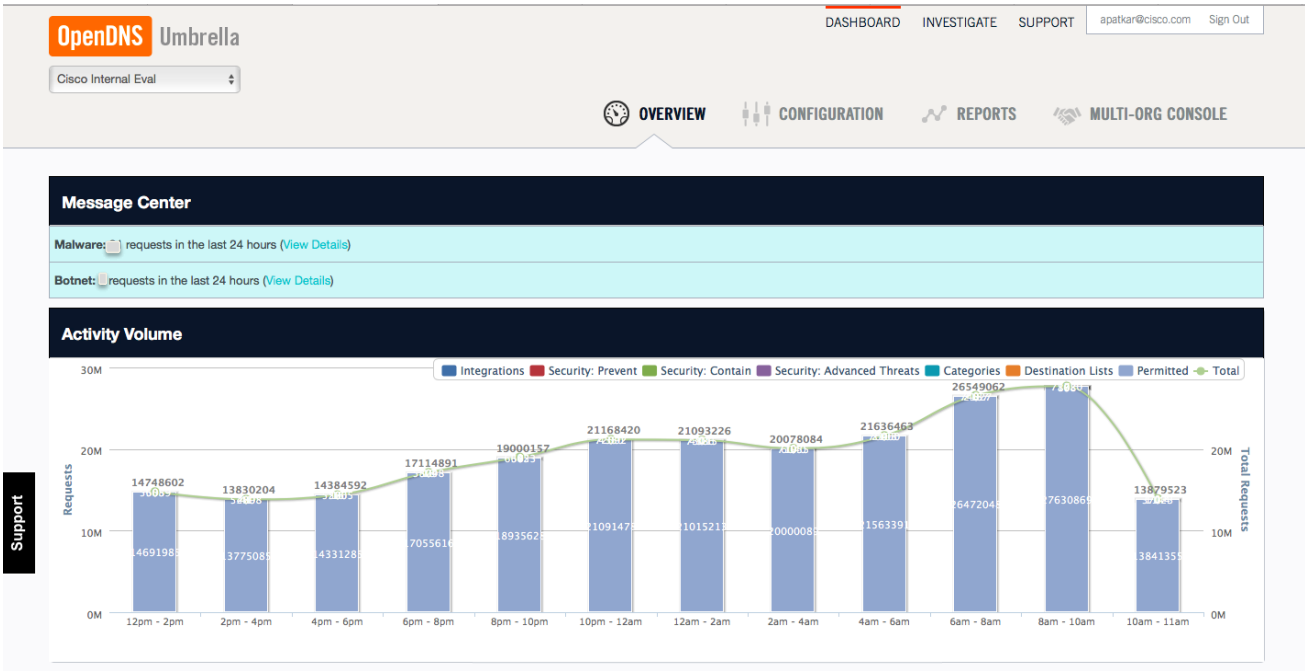
The conversion was as simple as adding four lines of code to the DNS config file on our internal DNS servers to direct queries to OpenDNS. Now Cisco IT's DNS servers ask OpenDNS for recursive DNS queries instead of asking their upstream neighbors. We rolled out OpenDNS so quickly that our internal clients didn't even know a change had taken place.

The beauty of the OpenDNS solution is its simplicity, according to West. "We didn't have to change hundreds of thousands of DHCP scopes, coordinate change management with thousands of labs, or reconfigure thousands of statically defined end nodes," he says. "All it took was pushing out four lines of code to a few dozen DNS servers. It doesn't get much easier to implement an enterprise-wide security control." The change did not interfere with our existing DNS Response Policy Zone (RPZ) service and passive DNS monitoring.

Configuration

We configured OpenDNS using an intuitive dashboard (Figure 1). After we made the change to our internal DNS infrastructure, we used the dashboard to set up user access and network details. The dashboard shows all ports and protocols.

Figure 1. An Intuitive Dashboard Shows All Ports and Protocols



Impact on IT Operations

Transitioning to OpenDNS did not change the support experience for our users. Employees who have questions related to DNS still contact Cisco IT or InfoSec for support. Support engineers can generally answer questions themselves. They can escalate questions about OpenDNS content blocking to OpenDNS support.

Measuring Success

We'll measure success by the number of blocked requests and increased visibility. Blocks prevent incidents such as installation of a malware package or an infected machine calling home to participate in a botnet. Testing revealed that web pages now load slightly faster—an unexpected benefit.

Next Steps

In the next phase, we'll invite employees to download the lightweight OpenDNS client on their laptops and mobile devices. Employees will be protected from malicious websites not only when they connect to the Cisco network, but also at home or on the road. We'll balance data privacy and security to decide which OpenDNS client features to turn on.

Lessons Learned

We learned the following lessons during our OpenDNS transition:

- If you have private internal web servers, configure them to use your own DNS servers, not OpenDNS. OpenDNS only contains DNS entries for public websites, not internal websites. We have approximately 100 internal servers that we configured to not use OpenDNS, including Jabber and our network-monitoring applications.

  "The change was simple enough, but it was essential so that employees could use the services," says Abhijeet Patkar, member of the technical staff for Cisco IT.

- Check whether any of your applications treat requests differently based on whether they originate inside or outside your company network. We have one application like this: our content-delivery application distinguishes between internal and external requests so that partners cannot send private Cisco information outside the network. If you have any of these unusual applications, point them to your own DNS servers instead of OpenDNS.

We discovered the two exceptions above after we went live and a few users received error messages. When we discovered the glitches, we rolled back the implementation.

“Rollback took less than 10 minutes,” Smith says. “We just removed four lines from the config file and told the DNS servers to reread the file.” We went live again a few weeks later.

For More Information

To learn more about OpenDNS, visit http://www.cisco.com/go/opendns.

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT http://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.**