A Quick, Temporary Solution to Secure Wireless Extranet Access

Cisco IT Insights

What

Wireless access to the Cisco extranet had become an urgent requirement in our offshore development centers (ODCs). Engineers in the ODCs need wireless access so that they can test new Cisco wireless solutions. Now engineers in three ODCs in India can securely access the Cisco extranet from wireless laptops.

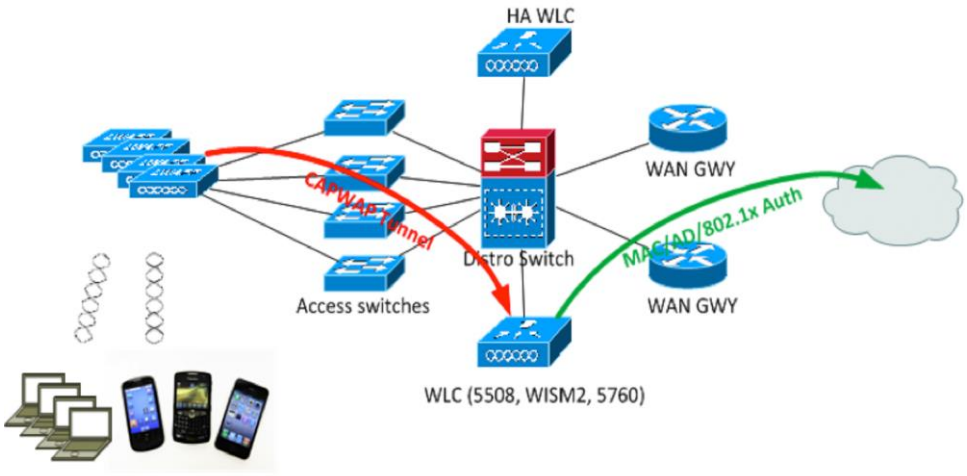
“The initial solution is quite simple,” says Simon Finn, information security architect, Cisco IT. ODC engineers can connect if three conditions are met. They must be using a company-owned and managed laptop. The laptop needs to meet our minimum standards. And the engineer must be part of a particular Active Directory group.

Here’s how it works: When an engineer logs in, the Cisco® Identity Services Engine (ISE) confirms that the device is Cisco-managed and meets our standards. Then Cisco ISE checks whether the engineer belongs to the Active Directory group with extranet privileges. If both the device and the user identity check out, the device is allowed onto the extranet for voice and data services.

“Requests are authenticated again at the firewall,” says Ivana Mihajlovik, security architect, Cisco IT. “Wireless access is just as secure as wired access.”

Engineers in the three ODCs are pleased with the wireless extranet solution, and other ODC partners have requested it. Figure 1 shows the deployment. We’re using Cisco Aironet™ 3702 Wireless Access Points, which support 802.11ac. The access points and a Cisco 5508 Wireless LAN Controller reside on the partner’s premises. Cisco ISE resides in a Cisco data center. Currently, we broadcast one SSID for the Cisco extranet. Built-in Cisco CleanAir® technology automatically detects and works around wireless interference such as microwave ovens.

Figure 1. Wireless Access to Cisco Extranet Logical Network Diagram



WAN GWY = WAN gateway router
Distro switch = Layer 2 distribution switch
HA WLC = High-availability wireless LAN controller

The decision to allow wireless extranet access is a simple yes or no. Later we'll grant different levels of extranet access depending on the user, device, location, and time and date. After authenticating the user, Cisco ISE will assign a security group tag (SGT), which is a 16-bit value, to all traffic from that laptop. The Cisco Wireless LAN Controller (WLC) will insert the tag in every packet that the laptop sends. Switches and firewalls that control access to different resources look at the tag to decide whether to allow that traffic.

"We'd already be using SGTs if we had onboarding processes for ODC partners that created different Active Directory groups depending on the employee's role," Finn says.

Initial benefits of secure wireless access in our ODCs include:

- Supports test of mobile applications
- Enables developers to work side by side in collaborative areas of the ODC, one of the principles of Scrum development
- Makes meetings more efficient by enabling everyone in a conference room to connect. Most conference rooms have only one or two wired ports.
- Eliminates the cost of patch cords for our partners.

Why

Cisco rigorously protects its intellectual property, and part of that effort is secure extranet access. Partners are required to build a physically separate network for employees who work on the Cisco extranet. These employees work in a secured area and connect over a VPN. Wireless access used to be prohibited. But now wireless access is mandatory for product and application testing, as well as mobility.

We had two options for secure wireless extranet access: maintain static access control lists (ACLs) based on IP addresses, or use Cisco ISE and identity-based access controls.

"Cisco ISE takes much less work," says Mihajlovik. "To use ACLs based on static IP addresses, we'd have to build a different subnet for each employee role." That's not a scalable solution, either for IP addressing or management.

With Cisco ISE, in contrast, Cisco IT doesn't need to reconfigure access switches when engineers join or leave an ODC team. When engineers leave the team, their Active Directory classification changes and Cisco ISE automatically starts denying extranet access.

Finn concludes, "With Cisco ISE, we can enforce very granular access control. Eventually, we'd like to eliminate the distinction between the intranet and extranet. Access control will be based on the user's identity rather than the connection method."

For More Information

Cisco IT Article: Cisco IT and the Identity Services Engine Deployment

To read additional Cisco IT articles and case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events.

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.**