How Cisco Workforce Connects to Borderless Network from Any Device

AnyConnect client provides secure remote access from laptops, tablets, and handhelds.

> "At Cisco, the question is not if we'll become a true borderless enterprise, but when. One step on the journey is enabling our mobile workforce to use any device to securely connect to the Cisco enterprise network, a goal we've achieved with AnyConnect."
>
> Rami Mazid, Vice President of Client Services, Cisco IT

Cisco IT Case Study / Borderless Networks / AnyConnect Secure Mobility Client: At Cisco, mobile workers remain productive when away from the office by using laptops, tablets, and handhelds for remote VPN access. Secure access from anywhere, anytime, using any device is part of the company's Borderless Networks initiative. Cisco IT wanted to simplify the user experience for mobile workers and simplify the lifecycle management process for VPN client software. This case study describes how Cisco is meeting its goals using the Cisco AnyConnect Secure Mobility Client, a Cisco IOS Software headend for self-provisioning, and the Cisco ASA Adaptive Security Appliance 5500 for VPN tunnel termination. Cisco customers can draw on Cisco IT's real-world experience in this area to plan their own borderless networks initiatives.

Background

Cisco IT is working to create a borderless experience for employees, giving them the flexibility to work from anywhere, using any device. Cisco's enterprise network no longer stops at the building walls and is no longer limited to desktops and laptops. Instead, Cisco employees increasingly connect from customer or partner offices, trains, hotels, or their backyards, using smartphones and tablets as well as laptops. The main benefits are increased productivity, more convenient collaboration, and increased job satisfaction from having a choice of devices for work.

Challenge

Cisco has provided VPN access on laptops since 1999, and on smartphones since 2007. Previously, Cisco IT had to create VPN access accounts for each employee, and then used a third-party tool to install and periodically update client software. But this approach no longer met Cisco's needs, for several reasons.

First, as part of Cisco's Borderless Networks strategy for productivity and collaboration, Cisco IT wanted to improve the experience when employees connect to the Cisco network from outside the office. "The borderless experience means being able to connect from anywhere, on any device, securely and reliably," says Adam Cobbsky, technical lead for Client Services for Cisco IT. "With our previous VPN client, we had to manually reconnect and re-authenticate whenever we moved out of the coverage area and lost the connection."

Second, Cisco IT wanted to reduce helpdesk costs associated with one-time password for VPN software. Support costs approached US$500,000 annually. Using certificate-based rather than password-based authentication would lower this cost and also enable Cisco to implement a robust identity management framework.

Finally, Cisco IT wanted to reduce the overhead of supporting different VPN clients for the growing number of devices used by Cisco employees. These include Symbian OS-based Nokia dual-mode phones, Windows Mobile Operating

System devices, Apple iPhones, Android phones, Apple iPads, Cisco Cius tablets, and Windows, Mac, and Linux desktops and laptops.

“We needed a unified and secure VPN solution for all desktop and mobility platforms used within Cisco,” says Plamen Nedeltchev, Cisco Distinguished Engineer IT. “Our near-term vision is to unify multiple existing and new clients and agents, such as Cisco EnergyWise Orchestrator, Cisco Wide Area Application Services (WAAS) Mobile software, 802.1X clients, VXI client, and so forth. This will give Cisco users a consistent, device-agnostic experience and enable a smooth transition between one device and another without dropping the connection.”

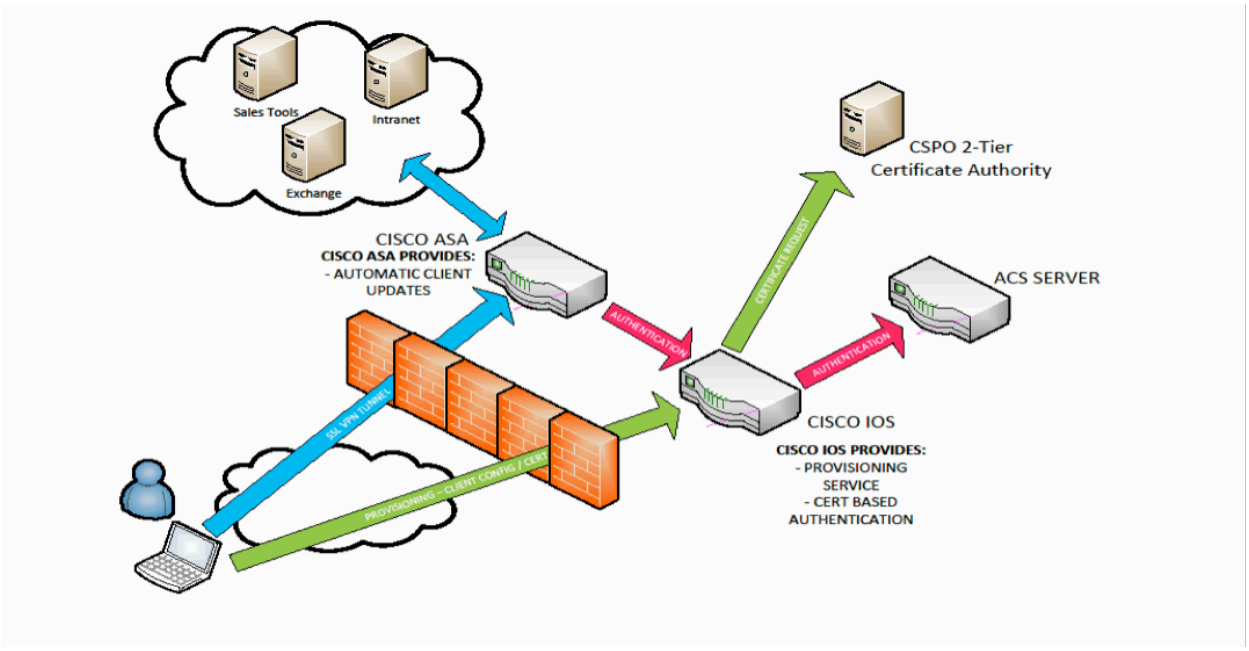
Solution

Cisco IT is meeting its goals using the Cisco AnyConnect Secure Mobility Client. The same software works on all devices that Cisco employees use for work, and Cisco IT is beginning with Windows and Mac devices. “AnyConnect supports the borderless experience by letting employees securely connect to the Cisco network from any location, on any device,” says Nedeltchev. “Cisco IT can manage it centrally. And it is always on.”

The fact that Cisco AnyConnect is always on saves Cisco employees the hassle of repeatedly entering passwords and waiting for a connection. As employees move about, Cisco AnyConnect can automatically select the optimal VPN headend and tunneling protocol. The solution also provides a better user experience for real-time applications. For example, if an employee is using Cisco Unified Personal Communicator at home or a hotel for a Cisco WebEx conference, Cisco AnyConnect uses the Datagram Transport Layer Security (DTLS) protocol, which is optimized for latency-sensitive traffic such as voice and video.

Cisco IT needs very little time to manage the Cisco AnyConnect client. No time at all is needed for provisioning, a significant savings for a company with over 70,000 employees. Instead, employees use their PC or Mac to select AnyConnect from an internal web-based service catalogue. “We coded the service catalogue to retrieve the device’s serial number to confirm it’s a Cisco-managed device,” Cobbsky says. The system automatically generates an account for the employee and sends an email with the URL for the Cisco IOS Software headend used for provisioning (Figure 1). The employee just clicks the link provided in the email and authenticates using the one-time password. The headend provisions the certificate and deploys the AnyConnect client on the device. The headend also installs the associated profiles for the various, globally distributed VPN headends.

Figure 1. Cisco IT AnyConnect Deployment



After self-provisioning the client, Cisco employees can connect to the Cisco network from any location with an Internet connection, just as they would in the office. Behind the scenes, the Cisco AnyConnect Mobility Client establishes a secure tunnel, which is terminated by one of six Cisco ASA 5500 Adaptive Security Appliances. “Later, we plan to use the Cisco ASA SCEP [Simple Certificate Enrollment Protocol] Proxy for provisioning instead of the Cisco IOS headends, making the solution even simpler,” Cobbsky says.

Cisco IT has been gradually inviting employees to download Cisco AnyConnect. The company is beginning with new employees and those who receive new PCs. Cisco IT does not need to remove the old VPN client before installing Cisco AnyConnect because both can coexist on the same client device, even if they terminate on the same Cisco ASA Adaptive Security Appliance. This is possible because the old VPN client and Cisco AnyConnect use different secure protocols, IPSec and SSL, respectively.

Results

Borderless Experience, for High Productivity and Employee Satisfaction

“At Cisco, the question is not if we’ll become a true borderless enterprise, but when,” says Rami Mazid, vice president of IT for global client services at Cisco. “One step on the journey is enabling our mobile workforce to use any device to connect securely to the Cisco enterprise network, a goal we’ve achieved with AnyConnect.”

The Cisco AnyConnect Mobility Client supports Cisco’s borderless network strategy by giving users a choice of devices and locations to work. “AnyConnect is part of a trend at Cisco toward unified platforms, to simplify the user experience,” Cobbsky says. “Just as Cisco Quad provides everything we need for collaboration, Cisco AnyConnect provides everything we need for secure access, including VPN connectivity, security, and authentication.”

Employees appreciate not having to re-enter a one-time password every time they lose a connection—for example, while driving through a tunnel or roaming between Wi-Fi and cellular coverage areas. Now they enter a one-time password only once, at the start of their working day. “Employees who commute by train to our London office frequently lose their connections,” Cobbsky says. “Now they don’t have to keep reentering a password because the AnyConnect VPN session automatically re-connects. This makes it easier to be productive while commuting.”

Simplified Provisioning and Deployment, Reducing Operational Costs

Centralized management saves time for Cisco IT throughout the client software lifecycle. One reason is that employees self-provision from the service catalogue web page. The headend automatically installs the latest software, eliminating the time previously needed for provisioning and upgrades. Furthermore, Cisco IT no longer needs to spend time troubleshooting when employees experience problems with the VPN access software. "Previously, a Cisco engineer working on a customer site who had a problem with the VPN client would have to return to a Cisco office to reinstall it," Nedeltchev says. "Now, if you're using a Cisco managed device, you can visit the provisioning URL from any location, even a public Internet café, download the software, and be fully operational within five minutes."

"On a typical business day, over 15,000 clients may be concurrently connected to the Cisco intranet with a software VPN client," says David Iacobacci, member of the technical staff at Cisco and project leader for remote access solutions. "By expanding the device pool with the AnyConnect certificate-based implementation, Cisco IT can support more clients in a secure manner, without increasing deployment and support costs."

End-to-End Security

End-to-end secure management is an important part of Cisco's Borderless Networks strategy. "Smartphone operating systems have security features, but they are ineffective if users don't set them up properly," Nedeltchev says. "AnyConnect provides both authentication and PKI-based device authorization, in a fully automated way with zero effort from IT. In a 70,000-person organization, that's a significant cost savings for an integrated security solution."

Cisco AnyConnect also addresses the security challenges associated with giving Cisco employees the flexibility to use unmanaged assets. Cisco IT currently supports registered devices only. To make sure a device attempting to establish an SSL VPN session is registered, the solution checks the device's certificate against its serial number. "Requiring device registration also associates the device with a person, aiding security investigations and helping to ensure end-user accountability," says Nedeltchev.

"As part of the Cisco AnyConnect launch, Cisco IT uses the Cisco ASA 5500 Adaptive Security Appliance capability to check devices for compliance with corporate security standards. A device that fails to meet the standards is not allowed to connect to the network," says Rich West, Information Security Architect in the Cisco Security Programs Office group. For example, a user who has not entered a screen-lock password cannot establish a VPN connection with Cisco until doing so.

Cisco AnyConnect also helps prevent non-employees from connecting to the Cisco network using lost devices. When an employee informs Cisco IT of a lost device, Cisco IT can immediately terminate any active VPN sessions for the asset on the headend and prevent any further VPN connections. Cisco IT can also easily terminate accounts of employees who leave the company.

Next Steps

Cisco IT's plans for Cisco AnyConnect include:

- Using Cisco AnyConnect Secure Mobility Solution to enforce security policies.
- Integrating Cisco AnyConnect with Cisco's premises-based Cisco IronPort S-Series Web Security Appliance. "Later Cisco IT will augment the on-premise solution with Cisco ScanSafe SaaS Web Security Cloud Services," says Jawahar Sivasankaran, senior manager in the Cisco IT Customer Strategy and Success group.
- Integrating with 802.1X to provide network-based identity management. Cisco IT is also considering implementing smart cards for user authentication, so that mobile employees can log into shared kiosks in Cisco offices and receive the appropriate access privileges.

- Coordinating with Cisco's IPv6 adoption strategy.

Nedeltchev concludes, "Cisco AnyConnect is not a very complicated implementation, but it has a terrific magnitude of benefits. The borderless experience lets us be productive wherever we are and gives us the freedom to use our choice of device."

For More Information

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.

To read more about Cisco AnyConnect Mobility Client, visit www.cisco.com/go/anyconnect.

To read more about how the borderless experience, visit www.cisco.com/go/borderless.

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.**