# Remote Work: Keeping It Secure

## How Cisco scales our secure remote workforce

Every Cisco employee teleworks at least some of the time. So when the pandemic sent everyone home to work, we already had the technology, culture, and processes in place. The big changes were scaling our existing VPN and implementing split tunneling. This article explains our solution–a collaboration between Cisco IT and our Security and Trust Organization.

# Goal: enable employees so they can get the job done

Our top priority is enabling employees to access the services and data they need to be productive when working from home. If they can't, business stops. To confidently allow remote access we need to secure the network, mobile devices, servers, applications, and information–and enforce good behavior.

At the same time, we need to take care that sure security solutions and policies don't make it harder to get work done–so that employees won't be tempted to work around them. For employees to follow Cisco policies, security needs to be an enabler rather than a burden.

Our secure remote worker solution at Cisco has two parts. One is deciding whether a user's device can be trusted to consume or produce content. The other is securely delivering services housed in our data centers and the cloud to the employee's home office.

# Can the device be trusted? Treating the device as a container

All employees, contractors, and partners who use Cisco IT applications housed in our data centers or branch offices have VPN access. They install Cisco AnyConnect Secure Mobility Client on their laptops and mobile devices. Full-time teleworkers have a Cisco Virtual Office setup, which includes a hardware-based VPN service.

Our users can connect to the VPN from their company-managed laptops or personal tablets or smartphones registered with Cisco IT.  (Read our BYOD story here.)

## Multi-factor authentication

To connect to the VPN, employees open AnyConnect, which calls Cisco Duo for multi-factor authentication (MFA). Duo allows users multiple options for verifying their identity, from using built-in biometrics such as TouchID to using a secure password generated by a physical token. Most commonly, the employee enters a username and password plus a one-time code sent to a mobile device. Once the user authenticates, the AnyConnect Network Visibility Module (NVM) starts collecting flow data we use for capacity and service planning, auditing, compliance, and security analytics.

## Checking device posture

Before an employee authenticates, the AnyConnect client connects to the closest available VPN headend. AnyConnect and the headend perform lightweight posture checks on the device. Minimum requirements include recent operating system version, encryption, password-protected screen lock after 10 minutes, and the Cisco Secure Remote Worker software suite (AnyConnect, Duo Umbrella, and AMP for Endpoints). Mobile devices also need certificates for VPN access, issued by Meraki Systems Manager.

Think of the security-posture check as getting measured against the sign seen at amusement parks around the world: "You must be this tall to ride." If the device passes, it connects to the network.

We manage Windows devices with Microsoft SCCM, Macs with JAMF, and smartphones and tablets with Meraki Systems Manager.

### DNS-level security

As employees visit websites, the Umbrella cloud service blocks malicious domains, IP addresses, and cloud applications–before the connection is established. DNS-level protection helps prevent malware, phishing, and ransomware.

Umbrella is especially useful for remote work because it operates whether or not the device is connected to our VPN. As an example of how we balance security and privacy, we've configured Umbrella to notify us whenever the device hits a site we're blocking but to not report other sites visited.

### Advanced Malware Protection (AMP) for Endpoints

For years we used an endpoint protection solution that blocked malware before it entered our network, what's called *point-in-time detection*. But some malware will always manage to sneak through, and detecting it requires *retrospective detection*.

We use Cisco Advanced Malware Protection (AMP) for Endpoints, a cloud service combining point-in-time and retrospective detection. We're currently using AMP for Endpoints on Windows, Mac, Linux, and Android devices. Read more here.

Compared to our old endpoint protection solution, AMP for Endpoints doubles the malware detection rate. It identifies critical, vulnerable third-party software on laptops, even when that software isn't running. That's useful when remote workers take extended personal time off, for instance. We've successfully tested quarantining home devices when AMP reports an infection. We can put the device in a "penalty box" even if it's not connected to the VPN.

In early 2020 we simplified security investigations and threat hunting by activating a feature of AMP called Orbital Advanced Search. It lets us look across all employee devices at a given point in time to hunt for threats. Our incident response team also uses Orbital to quickly find the root cause of incidents. That faster we find the root cause, the faster we can remediate and the shorter the risk exposure.

## Scaling VPN

Many companies design their VPN for use by a fraction of the workforce–when they occasionally work from home, travel, administer back-end systems, etc. At Cisco, so many employees telework at least one day a week that we've built out a more robust VPN than most organizations. In major sites, for example, if power goes down in one building, the services in other buildings can support all users. And if an entire site goes down, we have failover sites – for example, a US Central site is a backup site for our US Headquarters.

But during global events like the pandemic, when all employees use the VPN every day, sites that ordinarily provide failover are already running at full capacity. To keep the business running smoothly during the pandemic, we needed to scale up our VPN infrastructure. We did it by adding IP addresses, VPN hubs, and firewalls where needed:

- **IP addresses.** We monitor IP address usage with an automated script. During the first weeks of the pandemic we added addresses to the locations that were nearing device capacity.
- **VPN hubs.** The pandemic expedited plans to build new regional VPN hubs. Connecting to nearby sites reduces latency, improving the user experience.
- **Peering connections.** To further reduce latency, we've deployed switches in some of the same facilities as cloud providers like Microsoft. We ran fiber between our switches and the service provider's to create a direct, 20Gbps connection. Read the blog here.

- **Service provider capacity.** We typically contract for a committed information rate (CIR) a bit higher than typical usage, with an option to burst when needed. In larger sites, for example, we have a 10-Gbps pipe, pay for 2-Gbps CIR, and can burst to the full 10 Gbps. Although bursting is costly, in some cases it costs less per month than paying for a larger CIR. To see what's most economical, we consider the number of circuits that are bursting and for how long. Tip: Check with your service provider to be sure your pipes are burstable. When we scaled up the VPN during the pandemic we discovered that one of our Chinese service providers limits our rate. Knowing this changed our plans for the other circuits.

For more, see "Q&A: How we scaled VPN when the global workforce moved home."

## Split tunneling for certain cloud services

Global work from home during the pandemic fast-tracked our existing plans for split tunneling. Over three days in early March 2020 we configured the VPN client to direct traffic destined for Cisco data centers over the VPN while directing certain cloud-bound traffic directly to the Internet. Bypassing the VPN for certain cloud-bound traffic improves the user experience and reduces the load on the enterprise network and its links to the internet.

Split tunneling *all* Internet traffic would expose us to too much risk. For example, clicking links on Facebook or Twitter during a quick visit to break up the workday might expose the laptop to malware that could spread across the company. We want to bring most general traffic back through Cisco, where we have a layered security stack. Therefore, to minimize risk, we use split tunneling only for about a dozen cloud services that pass stringent security criteria, including good data hygiene and compatibility with Duo MFA. These include corporate services like Cisco TV, Office 365 and Box, as well as Apple and Microsoft updates. These dozen cloud services produce about one-third of our Internet traffic.

A real-world test of split tunneling came in early March 2020, when Cisco's CEO held his first COVID19 Q&A on Cisco TV, a cloud service. More than 100,000 people watched a live video stream simultaneously. Without VPN split tunneling, some of our ISP links would have been saturated, leading to a poor experience.

# Change management

Before Cisco offices closed in March 2020, we asked business leaders to send their teams an email we'd written urging them to reset passwords, update business apps, and try logging on to the VPN before the last day in the office. (Users can't log in unless they have the latest security patches.) For employees with a Cisco Virtual Office setup, we sent out a reminder to keep it powered on all the time instead of powering down at night so it could receive security patches.

Cisco business leaders and regional IT teams also shared tips for working from home with their teams, including:

- Check PC health using our internal tool.
- Make sure to use the latest version of AnyConnect.
- Confirm Cisco Duo Security is working correctly by visiting the site we set up for that purpose.
- Schedule application upgrades and backups outside of normal work hours to avoid VPN congestion.

## What’s next

We continue to make the secure remote worker solution stronger. Plans include:

- Simplify the VPN user experience on Windows and Mac devices using certificates—as we already do for mobile devices.
- Fine-tune new-hire onboarding and laptop procurement. We need processes for when the new hire or the person onboarding the new hire (or both) can’t come into the office.
- Introduce desktop-as-a-service (DaaS) in public clouds. During the pandemic lockdown we’re providing virtual desktops to contractors outside the U.S., avoiding the risk and logistical problems of providing physical laptops.