From the inside out:

Cisco IT's adoption of Cisco Secure Access

In the ever-evolving landscape of cybersecurity, organizations have never been more focused on finding simpler, more secure solutions to protect increasingly complex IT environments. Cisco IT, the team responsible for securing users and deploying technology across the entire Cisco organization, is no exception. With a global presence spanning over 300 offices in more than 80 countries, and a workforce of over 86,000 employees and around 50,000 contractors, the challenge of securing the huge number and diversity of users, devices, offices, and connectivity mechanisms is immense.

Like all large enterprises, Cisco IT needed to embrace the trend toward a hyper-distributed workforce and vigorously ensure security in that environment. This was a key driver in the evolution toward Secure Access Service Edge (SASE). Although Cisco IT had been on this journey for years, it needed to accelerate this motion. Cisco IT made the decision to begin deployment of Cisco's own Secure Access to enhance their security strategy, streamline operations, and provide a seamless user experience no matter where teams work.

> "Imagine the complexity of expanding your business into new regions or moving to a different colocation facility for your VPN, branch and internet edge. Cisco Secure Access transforms cloud edge expansion from a logistical marathon into a sprint, slashing setup times from months to mere hours."
>
> Jon Woolwine, Director, Network Engineering and Operations

Problem

Cisco IT’s environment is characterized by massive scale and diversity. The infrastructure includes 27,000 Cisco video devices, roughly 1 million IP connected things, and 62,000 mobile devices across large campuses, small offices, homes, customer sites, roaming users, and more. Plus, Cisco continues to grow, acquiring 9 new businesses and integrating them into the Cisco organization in 2023 alone.

Cisco IT had spent a decade integrating security and networking into regional hubs across the globe, forging some of the capabilities that would later be called “SASE.” This homegrown system successfully delivered a large portion of SASE functionality, yet it required a significant investment of time and resources to integrate and operate the solution.

Despite the strong outcomes, Cisco IT butted up against some limitations and recognized the need to evolve. The goal was to reach their “North Star” vision of steering traffic to a central cloud service, applying consistent security policies, and unifying policy management while deploying Zero Trust principles. However, realizing the full vision with the current solution turned out to be a large undertaking for a single IT organization. Cisco IT decided to shift resources and partner with Cisco product engineering to help build a packaged solution instead that could reduce complexity, enhance security, and improve the user experience without the burden of custom-built architecture.

> “By centralizing telemetry and data, Cisco Secure Access streamlines incident management, eliminating the need for multiple teams to analyze networking and security data and sidestepping complex tasks like IP-user mapping. We’ve seen reductions in mean time to troubleshoot by up to 25%.”
>
> Rich West, Principal Engineer, Security and Trust Organization

Solution

Cisco IT's SASE journey was driven by balancing strong security with a superior user experience in a hyper-distributed world. The team sought a solution that would simplify IT operations, provide a seamless experience for users, streamline threat detection and mitigation, and offer the flexibility to adapt to business demands quickly.

> "We're impressed and amazed at how well the turn up of new Secure Access VPNaaS regions and backhauls has gone! Typically, a single region enablement (on-prem VPN) would take weeks to a month. Today with VPNaaS, it took less than 3 hours to enable 5 regions."
>
> Roel Bernaerts, Principal Engineer, Network Engineering and Operations

Cisco IT carefully weighed the capabilities of Secure Access against the unique needs of connecting and protecting everything across the Cisco ecosystem. A variety of factors drove the decision to move forward with Cisco Secure Access, including:

- **Better, low friction user experience:** Users to just sign on and get to work, regardless of where they are working.
- **Increased consistency:** Uniform security policies applied across a diverse set of users and locations.
- **More effective use of IT resources:** Cisco IT can spend less time building and operating custom capabilities and more time leveraging advanced functionality.
- **Increased velocity of new features and innovation:** New capabilities and fixes can be deployed quickly, unburdened by hardware updates or patch windows.
- **Completeness of vision:** Robust, function-rich roadmap that is unique in the industry.

The functionality of Secure Access aligned with Cisco IT's complex requirements, offering a breadth of connection options, a single agent for connectivity and visibility, and a streamlined user experience.

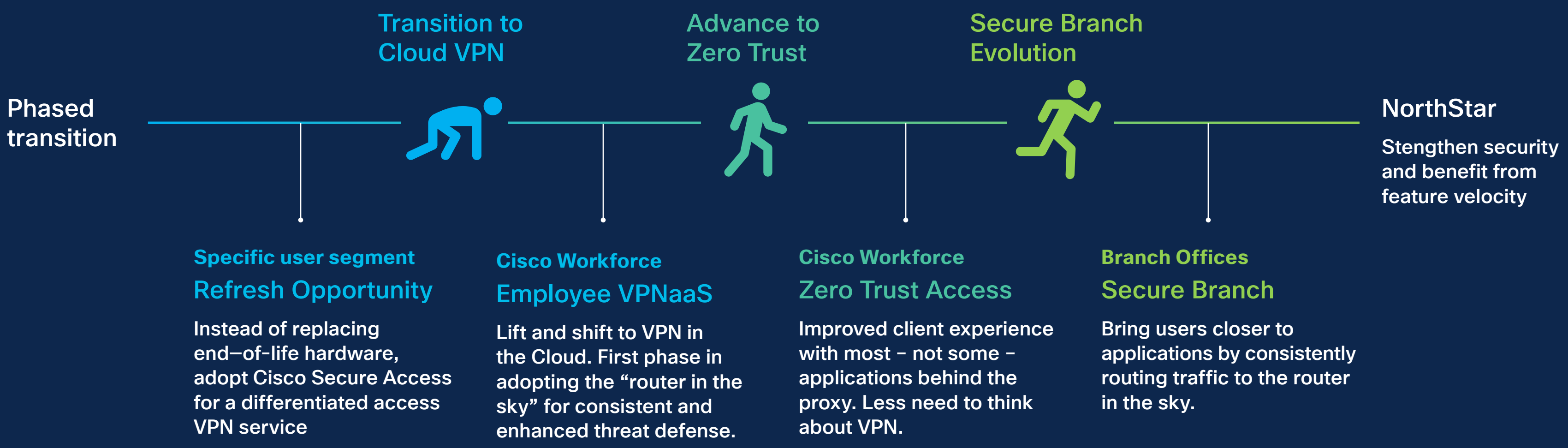
Deployment

The first step in the partnership between Cisco IT and the Secure Access product team was to identify must-have features required to adopt Cisco Secure Access at scale. Cisco IT pushed the product team hard on this, but everyone understood that because Cisco IT was a typical enterprise customer, other enterprise customers have similar needs. All Secure Access customers would benefit from Cisco IT's insistence on specific features in the commercial solution.

Cisco IT is rolling out Secure Access in strategic phases, incrementally securing additional groups of users and iteratively implementing more functionality.

- Migrate remote users from on-premises VPN to VPN-as-a-Service (VPNaaS), segment by segment. The initial 8,000 user move is well underway, and the majority of the Cisco workforce will move to VPNaaS by the end of 2024.
- Evolve remote users from the current ZTNA capability to the Zero Trust Access (ZTA) capability of Secure Access, which will provide more robust, granular, and high performance least privilege controls via a simpler approach.
- Deploy in Cisco offices/branches by using Secure Access to protect internet, SaaS app, and selected private traffic from SD-WAN connected office workers.

Figure 1. Cisco IT and Secure Access deployment approach



Phased transition

Transition to Cloud VPN

Advance to Zero Trust

Secure Branch Evolution

NorthStar

Stengthen security and benefit from feature velocity

Specific user segment

Refresh Opportunity

Instead of replacing end–of-life hardware, adopt Cisco Secure Access for a differentiated access VPN service

Cisco Workforce

Employee VPNaaS

Lift and shift to VPN in the Cloud. First phase in adopting the “router in the sky” for consistent and enhanced threat defense.

Cisco Workforce

Zero Trust Access

Improved client experience with most – not some – applications behind the proxy. Less need to think about VPN.

Branch Offices

Secure Branch

Bring users closer to applications by consistently routing traffic to the router in the sky.

Spotlight on Zero Trust: Cisco has been on the Zero Trust journey for years with good success, yet limitations with the current approach have emerged. Today’s ZTNA capability is securing many applications, but Cisco IT believes that Secure Access ZTA will enable them to press forward with protecting many more applications with deep and granular security, a more efficient and secure access model, simplified user experience, and reduced reliance on traditional VPNs.

Cisco IT’s perspective on Zero Trust has been integral to this transition. By focusing on functional principles rather than getting entangled in varying definitions, Cisco IT is focused on the end goal: Delivering appropriate access levels based on device and user entitlements as well as leveraging data such as device compliance and user behavior to make more intelligent access control decisions.

Security for AI: Artificial Intelligence (AI) has the potential to empower innovation in ways previously unimaginable, but it is not without risk. Cisco IT plans to leverage the power of Cisco Secure Access to foster the benefits of AI while mitigating the risk. For example, Cisco IT can warn users about risks, monitor to prevent data leakage to generative AI tools, and monitor to decide when to block data from AI tools.

Challenges and lessons learned

Although Cisco IT is in the process of deploying Secure Access, with many more phases of the journey yet to come, there are already "lessons learned." And of course, learnings don't emerge from things going perfectly. Rather, they form by bumping into challenges and finding ways to solve them. Some of the top lessons learned are below.

Firm executive commitment, above peer teams: This is a transformation project, with broad implications (and benefits) across the entire company. It demands firm executive commitment above all the groups involved.

Fundamental changes in IT, networking, and security teams. These teams, which previously ran as distinct entities, had to embrace shared responsibilities – genuinely and fully – to achieve optimal security and efficiency. Even within any one team, there are typically many silos that must work together.

Mindset shift. While Cisco IT was already on a Zero Trust journey, this project pushed them toward further alignment with Zero Trust principles, unencumbered by definitional differences or semantics.

Not all desired capabilities can be instantly available. The scale, complexity, and diversity of an organization like Cisco meant that sometimes, a desired function wasn't yet there. However, Secure Access's cloud-native, continuous delivery model meant Cisco IT received fixes and new features without long waits – far faster than was possible from the former bespoke approach.

Visibility for troubleshooting. Troubleshooting was faster, simpler, and more effective with Secure Access providing visibility in one place.

Balance progress with user choice. Early on, users were concerned about access changes interfering with their work. That proved to be a non-issue because Cisco IT started small, moved iteratively, and gave users choice (opt-in vs. forced changes for a period of time).

Outcome

Cisco IT's adoption of Secure Access is progressing swiftly, and the team is seeing excellent results. It's clear already that Secure Access will be a driving force for achieving Cisco IT's North Star vision of steering traffic to a central service, applying consistent security policies, unifying policy management, and deploying Zero Trust protection. By "drinking our own champagne" (using Cisco's own products), Cisco IT is marching toward improving the company's security posture and is demonstrating the scalability and effectiveness of Secure Access in a large and demanding IT environment. The success of Secure Access in the Cisco enterprise, being rolled out segment by segment, serves as a testament to its ability to meet the complex challenges of modern cybersecurity.

> "By moving our first cohort of employees from on-prem VPN to VPNaaS in 2024, we will avoid replacing end-of-life VPN appliances and save the time/effort our IT staff would typically spend managing those appliances."
>
> Jennifer Huber, Program Manager, Network Engineering and Operations