ZIVARO

···· BRILLIANT IT ····

Securing Your Network for the Permanent Remote Workforce

Amanda Ludwig-Chambers
Resident Network Engineer

It is no secret that 2020 has been a trial by fire for many industries working to maintain business continuity during an unprecedented uptick in full-time employees now finding themselves remote. Research from Gallup[i] concluded that over 50% of full-time employees saw themselves completely remote during the height of the remote worker influx, revealing numerous opportunities for improvement in network design and visibility to help support this trend.

One such glaring need for supporting business continuity across this expanding network is in *how* users connect, *securing* those connections end-to-end, and providing *visibility* for ongoing management and operations. Nearly overnight, organizations went from protected and mostly in-house, private-network users to literally everyone leaving the castle. Suddenly there was an enormous strain to supply remote access to private and public applications from any device and likely on unsecured home and Wi-Fi networks, including access to public cloud services the organization may not control. The pandemic-induced worker shift was yet another step accelerating the end of contained, private networks to the free-range workstyle model using the internet and cloud SaaS providers. Given the circumstances, the network access methods and controls became instantly paramount. So how does an organization respond quickly, rethink network access and authentication, ensure it can scale under the new demands, and be manageable for administrators?

Managing the security of networks has always been an integral component of Cisco network architecture from tools like Cisco ISE and recently with the launch of SecureX. According to the Cisco Annual Cybersecurity Report, the total volume of events has increased almost fourfold between January 2016 and October 2017 alone, with threats growing exponentially each year.[ii] Understanding this data is from a pandemic free world, what does an organization do when over half of their workers suddenly find themselves remote?

Despite organizations securing the office, at the height of the pandemic in 2020, Gallup reports that in a few months the remote work force jumped from 33% to a staggering 61%.[iii] What was once a nice to have, non-necessity became a must have for network operations almost overnight. CPO magazine reports 96% of organizations said that the COVID-19 pandemic has caused the need for change in organizations' cybersecurity policies centering on the need for securing the remote worker and the systems they need: "59% (of change) pertains to increased VPN capacity, 55% incorporated new web controls and changes to acceptable use policies, and 53% have new multi-factor authentication requirements in place."[iv] What is more, 95% of these organizations surmise that they expect some of these changes to be permanent.

In addition to the sheer numbers game of more employees utilizing these remote resources, users also find themselves working to stay connected on an increased usage of BYOD to access the networks' resources. According to CSO Online, 83% of phishing attacks over the past year took place outside the inbox.[v] So what is available to immediately protect the business? For organizations already utilizing the Cisco ASA VPN, solutions for necessary insight already exist within their infrastructure.

With little room for error when it comes to sensitive data, VPN technologies can put an organization's entire network at risk. Zero trust cyber security solutions exist to strategically manage and secure the user experience – on whatever device they find themselves using.

Cisco has been a thought-leader since the pandemic began. Anticipating the increase in VPN remote-access capacity and the associated changes in network performance, vulnerability, and management requirements, Cisco quickly launched a Secure Remote Worker[vi] solution to help organizations finding themselves in the line of fire. The solution is a collection of assessment and analysis recommendations as well as the solution themselves, assembled to relieve the time pressure of responding in crisis mode. The key building blocks of Cisco's remote workforce solution include:

- Authorized User Verification
- VPN Access
- Defending the Endpoint

For this paper, we will focus the discussion on a couple of key component solutions; Duo multi-factor authentication for secure access, and Cisco AnyConnect Mobility VPN client. Hidden behind the latter is a neat product I will touch on called Cisco Endpoint Security Analytics, or CESA. There are several more pieces to the Secure Remote Worker solution not covered in this paper or only touched on including AMP for Endpoints (endpoint security), Cloud Mailbox Defense (email protection), Umbrella (internet security), and Cisco SecureX for unified visibility. These each have tons of features and functionality, and I highly recommend the reader explore these as together Cisco has built a terrific vision for unified security for modern network requirements.

Cisco acquired multi-factor authentication leader Duo in 2018 to provide zero-trust solutions for joint customers and bring strong user and device security by integrating with the Cisco ASA VPN, Firepower VPN, or Cisco Identity Services Engine (ISE) to provide two-factor authentication to AnyConnect logins. This now allows network and security administrators to gain insight about the devices connecting to the VPN and provide the ability to apply policies to support device health requirements or apply policies for varying networks. Duo's access security shields any and every application from compromised credentials and devices, and in a world where seemingly any user from anywhere is trying to access an organization's data, securing access and complete device visibility allows peace of mind.

For Cisco VPN environments, the Network Visibility Module (NVM) is available to support deeper visibility into the rising number of endpoints users are introducing into their environments, be it desktop and mobile. The NVM collects endpoint telemetry for visibility into the device, user, application, location, and destination by exporting flow records to a collector such as Cisco's Secure Network Analytics (formerly Stealthwatch) or a third-party tool like Splunk, providing a narrative to the data flow and an opportunity to protect not just the user, but the very business itself. The Cisco NVM provides a rich data set; auditing users' network history, confirming system or admin rights and how they impact what network connected processes are running on users' machines, OS information to support patching and vulnerability monitoring, bandwidth monitoring at the application level, to name a few. This rich endpoint data analyzed by a powerful tool like Splunk Enterprise can provide context for the user experience and reveal opportunities where security can be massaged. Coupled with Cisco's Advanced Malware Protection (AMP) and Cisco Cloud Security, organizations can improve response and remediation, bettering business continuity posture and the user endpoint experience.

By example the Cisco AnyConnect Network Visibility Module (NVM) App for Splunk allows IT admins to analyze and correlate user and endpoint behavior in their Splunk Enterprise instance. This app allows for visualization of data and pre-built reports for AnyConnect NVM as part of the Cisco Endpoint Security Analytics for Splunk solution (CESA).

CESA built on a powerful third-party app like Splunk, provides that in-depth analysis and visibility, shortens the investigation time from days to hours while overall increasing the security of the network by providing quick and easy data analysis. One key is the out-of-the-box dashboards, allowing the information to be immediately used for answering questions and decision support. If Splunk Enterprise is already deployed, then CESA Built on Splunk provides a license for use of the NVM App and Add-on for Splunk, as well as to count your NVM endpoints separately from all other Splunk data, which provides a more cost-effective approach to analyzing NVM data in Splunk.[vii]

The team at Zivaro has extensive experience utilizing these tools and helping create well-rounded security postures in light of the heightened remote worker requirements. Clients leverage Zivaro for a broad range of consulting, deployment, and operational support across hybrid cloud infrastructure, application development, security operations, and workforce collaboration tools. With deep roots in network infrastructure, Zivaro helps plan, build, and operate complex, multi-cloud architectures with an emphasis on security policy and control for public sector and regulated environments.

Zivaro delivers an array of cyber protection services including risk management and cybersecurity framework planning, assessments, and accreditation services, planning and prevention, and managed security services for continuous monitoring.

Zivaro's security performance management enables security and risk leaders to measure the performance of an organization's cybersecurity program and align investments and actions with the highest measurable impact over time. Zivaro's use of NIST best practices and cutting-edge industry tools can immediately identify cyber risk within an organization's supply chain, helping focus resources and time to work alongside critical vendors to achieve significant and measurable cyber risk reduction.

Further, Zivaro’s security assessments provide insight into information technology (IT) vulnerabilities and compliancy status to include:

- Strategic roadmaps providing predictive budget planning for several years out
- Insider threat tools, policies, and procedures
- Security dashboards and visualization to continuously monitor your IT assets

With the uncertainty of what future readiness looks like, organizations can make quick improvements by leveraging the broad portfolio of Cisco remote-worker solutions available. In a recent report, Cisco’s posits that “35% of small businesses, 38% of medium businesses and 37% of large enterprises believed that more than half of their employees will be remote workers post-COVID-19”.[viii] Given this new normal, the time for network security, and preparing for a permanent expansion of remote workers is now. Utilizing tools like Duo, NVM and CESA can help administrators see and manage this user population with greater accuracy, protection, and response capabilities. Together with the broader portfolio of Cisco’s network and security tools, organizations can prepare infrastructure for the next wave of growth and can help create a new standard remote connectivity, protecting businesses for whatever comes next.

Sources:

i. https://www.gallup.com/workplace/307622/leaders-responding-covid-workplace-disruption.aspx

ii. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

iii. https://www.gallup.com/workplace/307622/leaders-responding-covid-workplace-disruption.aspx

iv. https://www.cpomagazine.com/cyber-security/cisco-report-on-future-of-secure-remote-working-sees-work-from-home-and-attendant-security-risks-continuing-beyond-covid-19/

v. https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html?page=2

vi. https://www.cisco.com/c/en/us/products/security/secure-remote-worker-solution.html

vii. https://www.cisco.com/c/en/us/products/collateral/security/endpoint-security-analytics-built-on-splunk/at-a-glance-c45-742564.html

viii. https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-remote-worker-solution/future-of-secure-remote-work-report.pdf