Red River

cisco Partner

SECURITY SERVICES

WHITEPAPER

Security Solutions for the Distributed Workforce

In the wake of a national pandemic, organizations are realizing the saving of enabling a remote work force. Former 9-to-5 employees have taken to their new home offices to conduct their business. Face to face meetings have been replaced by faces on the computer monitor. And this mentality has spread from executives of the offices to teachers of the classroom.

With such a vast remote work or student force, security has had to reevaluate the traditional way of thinking. Protecting the border of the enterprise no longer involves the hand off between the Internet and on-premise resources. A stack of firewalls does not protect clients who operate solely on the outside. In short, security must realize that protecting the border means addressing the remote work staff.

CISCO UMBRELLA

The first layer of defense is to protect users from suspicious domains and Internet sites. Cisco Umbrella provides a unique ability to protect both on and off premise users by accepting and inspecting DNS requests. DNS acts as the "Internet Phonebook" by replying with the IP address for domain names. Umbrella acts as an intermediary to the internet DNS, inspecting domains for any indicators of compromise or content not allowed by organizational policies. Integration into the organization identity provider, such as Active Directory, allows for role-based access to internet resource, regardless of location.

AMP FOR ENDPOINTS

Continuously running on endpoints, Cisco AMP is able to detect for signs of compromise to the end host. This information is able to beacon to a an Internet resource for organizational visibility. One aspect of this visibility is into the Identity Services Engine (ISE) or other products to restrict the access of the endpoint into the organization. Cisco ISE can in turn use the PX-Grid to distribute this information to other security platforms throughout the environment to provide a hardened infrastructure to possible threats.

ANYCONNECT

While AnyConnect is most popularly known for its ability to provide a cient Virtual Private Network (VPN) to the organization on prem or cloud resources, it is able to provide much more functionality. While information technology shops are able to leverage device managers for the mobile cients but are unable to ensure BYOD (Bring Your Own Device) endpoints are in compliance. Using the compliance module of AnyConnect ensures that devices meet the minimum organization requirements for security such as OS level, antivirus installed, or other organizational criteria.

In addition, when the device attempts to connect whether on prem or via the client VPN, the authenticating server, such as Cisco ISE is able to query the reported health of the client from sources such as AMP or via Adaptive Network Controls provided through Cisco Firepower.

FIREWALLING

When connecting through a client VPN, next generation firewalls with Firepower Threat Defense ensure that traffic entering or leaving the environment to remote clients adheres to organizational standards as well as inspects file transfers for any possible malware or prohibited application types.

Within the remote worker office, Meraki firewalls provide a cost effective solution while still providing robust security functionality. With onboard functionality for NetFlow, security and visibility is able to maintains all the way to the home office to detect possible attacks to the organizational resources. With firewalling all the way to layer 7, basic security may be upheld even at the home office. With the Meraki security suite, the technology professionals are able to manage via the Meraki cloud portal providing a single UI to monitor, troubleshot, configure, and maintain all the Meraki assets from a single user interface.

WIFI REMOTE ACCESS

For home offices only in need of a few connections over wireless, the Cisco FlexConnect capability allows a simple point of entry to the corporate WAN. Allowing for local switching when the WAN connection is lost, business continuity is maintained. When Flex Connect operates in a connected mode, the client is able to be authenticated against the corporate servers and traffic is tunneled back through an encrypted tunnel based on the Cisco CAPWAP technology. This sleek solution is able to provide WiFi access for non-corporate home devices, locally switching them to prevent unauthorized access into the corporate environment. This small solution allows users to securely extend the corporate office to home. When coupled with the Cisco TrustSec environment, end user devices can be protected at ingress to the corporate environment thought identity-based access lists and next generation firewalls.

CISCO CLOUD MAILBOX DEFENSE

Cloud mailbox defense is designed for office 3658 to provide disability inbound, outbound, and internal messages. Do with simplicity there are no required changes to male flow or any added administrative overhead or altering MX records. Because of the simple integration of cloud mailbox defense and open APIs this allows super flexible integration of organizations existing email, security, and incident response operations. By addressing some of these gaps we are able to detect and black advanced email threads using Cisco's superior threat intellligence.

CISCO DUO

One of the key components of moving the on prem workforce to virtual and geographically dispersed locations is verifying that the employee or the contractor is accessing the services is actually who they say they are and that their session or connection is not interrupted and stolen. Through the use of tools such as above and a combination of multi factor authentication we can tie user session together with their geographic location and continue to verify that we have legitimate user combined with legitimate access. Further we can combine users, devices, and applications which allow the business to stay focused on delivering other needs. This becomes a core of the zero-trust security philosophy.

SCALABLE SOLUTIONS TO MEET YOUR ORGANIZATION NEEDS

Based on over 25 years of industry knowledge, Red River solutions provide scalable solutions to support your remote work force. Scaling from one device to a small site, the Red River solutions provide environments of scale while maintaining the secure posture of a large enterprise campus.

CISCO MOBILE REMOTE ACCESS

Throughout the pandemic over the past year, Red River has also seen the very clear need for end users to be able to work from anywhere, from any device, at any time. With Cisco Expressway, Red River is able to provide our customers the ability to deliver voice and video calling services to their users no matter where they're located. Home office, kitchen table, a bench in a park, or even many times their bed, we've seen it all. With Mobile and Remote Access (MRA) our customers are able to provide connectivity on-the-go as though they are sitting on the corporate network. With Cisco Expressway, devices can register to the Expressway Edge in the customer's DMZ. Expressway then provides firewall traversal to the Expressway Core server adjacent to the Unified Communications Manager. Red River has been able to assist customers with connecting Jabber or Webex Teams clients on Android, IOS, MacOS, or Windows devices. This gives the users the ability to use their mobile devices

to place and receive calls from their business phone number without having to jump through all sorts of hoops and ensure they are on VPN when each and every call is coming into their business number. Along with the ability to use soft phone clients on many devices, customers can connect their new generation of desk phones (Cisco 7800 and 8800 series) as well as Cisco Desk Pro and DX80 devices from home.

SUMMARY

At Red River we standby to assist our clients with securing the remote workforce. As you can see from the above there are several areas that we can assist our clients across various different threat vectors. One of the key elements that differentiates Cisco from all of the other vendors is the integrated threat intelligence included in all of their products, these products work together in order to give our customers Faster response, more integration, and fewer tasks for their engineers to respond to incidents. In support of our customers Red River has repeatedly leveraged our 20-year business relationship solidified by our 12-year standing as a Cisco Gold certified partner. Red River has a broad range of experience and expertise in advanced Cisco technologies with Technical/Sales certifications. We have both Master Collaboration and Master Security Specializations in the Federal space, hold the highest level Customer Satisfaction Rating of Excellent, and have a proven record of helping customers utilize Cisco technology to empower collaboration, meet existing and future data center demands, and establish a reliable and secure network infrastructure.

For assistance with Securing your remote workforce reach out to security@redriver.com.