FORTINET®

Identifying Security Requirements for Supporting a Remote Workforce at Scale

Designing a Secure Telework Program

Table of Contents

Executive Overview

Organizations should support telework as a component of their business continuity plan, which requires the ability to rapidly transition to a partly or wholly remote workforce. Doing so creates new networking and security challenges for an organization since the company network is being used in a very different way from on-site employees.

Securing a remote workforce requires identifying and deploying security solutions that meet the needs of the employees and the headquarters network. The majority of employees only need secure access to the corporate network and cloud-based applications, which requires VPN access and multi-factor authentication (MFA). Network administrators and executives may have additional network requirements, such as persistent connectivity and a secure telephony solution. The organization’s headquarters network must also be capable of supporting and securing the network connections coming from the vast majority of an organization’s workforce, requiring robust user authentication and advanced perimeter security.

Introduction

The ability to support remote workers can help improve an organization’s business continuity plan. It allows the organization to adapt when unforeseen circumstances, such as natural disasters or a pandemic, make it impossible for employees to work on-site.

Under these circumstances, an organization may be forced to rapidly transition to a mostly or wholly remote workforce. When designing or implementing a telework solution, it is important to consider not only networking requirements but also the additional security concerns created by remote work.

Meeting Basic Telework Requirements

Employees may have different requirements of their remote work environment. However, all teleworkers have a set of basic requirements to ensure that they have a secure, authenticated connection to the enterprise network. These include access to a virtual private network (VPN) and a strong authentication solution to protect accounts from compromise.

Virtual Private Networking

When teleworking, an employee will be processing sensitive company data on their home network. Protecting this data against compromise requires the ability to ensure that a teleworker's connection to the company network is secure.

Teleworkers must have access to a VPN that provides direct and encrypted connectivity between their machine and the corporate network. This not only protects the confidentiality and integrity of sensitive company data in transit but also ensures that all traffic between the employee and the public internet is monitored and protected by the organization's existing cybersecurity infrastructure.

Multi-factor Authentication

With employees working from home, there is an increased probability that stolen login credentials, combined with access to an unattended machine, could enable unauthorized access to a user's account. In these situations, many of the features used to detect anomalous access patterns, such as the location and time of the authentication attempt, may not be applicable as employees' work patterns shift due to working from a home office.

Securing access to the corporate network, resources, and data requires a more robust authentication solution than traditional usernames and passwords. All teleworkers should be issued a secure authentication token. Options for MFA tokens include physical devices such as a key fob or software-based solutions such as a mobile application, which can be used to verify a user's identify before they are able to initiate a VPN connection to the corporate network or access other sensitive company resources.

PCI DSS guidance for remote work requires that employees accessing cardholder data authenticate via a VPN and use multi-factor authentication.[1]

Supporting Remote Power Users

While many teleworkers can get by with a VPN connection and an MFA token, others have additional requirements. Power users, including network administrators and executives, require a more advanced remote office to perform their core job duties. These users may need persistent connectivity to the enterprise network and a secure telephony solution.

Persistent Connectivity

Some users, such as network administrators and security personnel, require more flexible and persistent access to the corporate network. These employees may have multiple devices that must be connected to the company network or require long-lived connectivity not limited by automatic session timeouts.

The requirements of power users working from a home office can be satisfied by the deployment of a wireless access point, which can provide a reliable VPN tunnel to the corporate network. In order to ensure a secure connection, this wireless access point should be combined with a desktop-based next-generation firewall (NGFW) to provide traffic inspection, access management, and advanced threat protection.

Secure Telephony

When working remotely, it is essential that staff members—especially executives—have access to a secure telephony solution in order to protect sensitive communications and company data. Otherwise, a company risks exposure of sensitive data due to eavesdropping on cellular networks or using malicious mobile applications.

An effective way to provide secure telephony to off-site workers is to leverage Voice-over-IP (VoIP) communications. If a user already has access to a secure, persistent, and reliable internet connection, then routing their voice traffic over this connection requires minimal additional overhead. This also enables the organization to monitor voice traffic and scan it at the network perimeter for potentially malicious content intended to exploit vulnerable VoIP software.

Telephony solutions for teleworkers should provide them with all of the features of their on-site business phones. This minimizes the probability that workers will use personal devices for business communications. Important options include the ability to make and receive calls, access voicemail, check call history, and access the organization’s telephone directory.

72% of a CEO’s workday is spent in meetings, making secure telecommunications essential for their remote offices.[2]

Headend Security and Stability

Security solutions for a remote workforce are not limited to the client side. An increased number of teleworkers introduce new security threats and network requirements at the organization's headquarters as well.

When designing a telework program to ensure business continuity, it is essential to ensure that the headquarters network is capable of authenticating users and devices attempting to access it remotely and managing and securing a much larger number of inbound VPN connections.

Authenticating Users and Devices

A zero-trust security model is very important when an organization is supporting a mostly or wholly remote workforce. Employees may attempt to connect to the company network using unknown or personal devices, and systems connected to untrusted networks have a greater probability of being compromised by cyber-threat actors.

Securing the organization's network and the sensitive data and resources that it contains requires the ability to authenticate users and devices attempting to connect to it. This can be accomplished by using a centralized authentication server with connectivity to the organization's active directory, Lightweight Directory Access Protocol (LDAP), and Remote Authentication Dial-In User Service (RADIUS).

This server should be capable of scaling to meet the needs of a larger remote workforce without hampering user productivity. Support for single sign-on (SSO), certificate management, and guest management also ensures user authentication without creating a significant burden for remote employees.

Securing the Network Perimeter

One difference between an on-site and remote workforce is the number of VPN connections that an organization must be capable of managing. On-site employees are connected directly to the corporate LAN, but teleworkers must send all of their traffic over a VPN connection. An organization's NGFW must be capable of terminating all VPN connections and performing inspection of a large number of encrypted network connections. Since encrypted traffic inspection is computationally expensive, it is vital that an organization's NGFW can scale to meet demand. Doing so requires NGFWs with dedicated advanced security processors. These minimize latency and maximize throughput, preventing network bottlenecks that can significantly degrade employee productivity.

NGFWs at the headend must also perform Layer 7 inspection of all traffic. This is important in any enterprise context, but with a remote workforce, an organization can expect a higher concentration of malicious content on inbound connections from remote workers. This is because employee machines connected to personal networks have a higher probability of being infected with malware, which may attempt to move laterally through them to the corporate network. A Layer 7 NGFW can identify the application that an inbound packet is trying to reach and block packets from applications with known vulnerabilities. Headend NGFWs should also be integrated with sandboxing capabilities to safely analyze suspicious content that cannot be associated with any known threat.

Inspection of transport layer security (TLS)/secure sockets layer (SSL) decreases firewall throughput by 60% on average.[3]

Conclusion

When transitioning quickly and massively to teleworking, it is essential that an organization not only be able to sustain operations but also to ensure the security of teleworkers and the sensitive data that they process.

Doing so requires an organization to deploy security solutions both at teleworkers' remote work locations and on the main corporate network. When doing so, it is essential to select solutions capable of addressing the unique infrastructure requirements and security concerns associated with a remote workforce. During a disaster situation, when an immediate response is required, selecting a solution that can be deployed quickly and easily ensures minimal impact to business operations.

[1] Emma Sutcliffe, "How the PCI DSS Can Help Remote Workers," PCI Security Standards Council, March 26, 2020.

[2] Michael E. Porter and Nitin Nohria, "How CEOs Manage Time," Harvard Business Review, July 2018.

[3] "NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports," NSS Labs, July 24, 2018.

www.fortinet.com