Best Practices for Secure Remote Access to Your Firm's Network

Significant changes in mobile technology and global business practices have spurred an evolution of both local and remote access. With more people working from more locations using more devices than ever before, attempts at providing access while still protecting network resources have become more difficult and expensive. Now, local user access must be as tightly secured as if they were remote and remote user access must be as simple and comprehensive as if they were local. Today, all users are potentially remote and all end points potentially unsafe. But users will demand access to business resources from any location. The future trend is towards a model where the network perimeter is concentrated around application resources. Your focus shifts to securing communications between all users and business critical applications. There are several security appliance manufacturers (WatchGuard, Dell/Sonicwall, etc.) that are equipped with features to control access to applications, data and network resources for both on-site and remote users.

The Impact on Access Control

Mobile trends in technology and business operations have accelerated the replacement of traditional network nodes from hard cabled desktops to wireless laptops and mobile devices. Even when these devices are issued by your firm, It is increasingly hard for the firm to control what users do with access devices and to limit ways in which users expose these devices to threats that can impact the security of enterprise resources. For example, an end user might use the same mobile computing device at home as in the office, use a personally owned device for business purposes, or use a corporate owned device for personal purposes.

The Convergence of Local and Remote Access

As more types of users work from multiple locations, demand for remote access is on the rise, while demand for local-only access has fallen off. Hard-wired LAN access is being outmoded by ubiquitous high-speed connectivity over wireless networks and the Internet. Data centers are becoming virtualized, providing fluid access to resources from anywhere. But IT must also assume that your users will demand full access to all their business resources from any location using whatever device they have at hand. With the convergence of local/remote access, rather than striving for a secure network, IT should focus on establishing secure communications to network resources. The most important piece of this puzzle is ensuring that your firewall and other network perimeter security devices are current generation, and are up to date on the latest security software features.

Universal Access Control

As laptops and other mobile devices move in and out of an increasingly fluid perimeter, the traditional network cannot be fully protected by IT. The most dangerous attacks on your network may actually come from local rather than remote users. The increasing difficulty of managing end users and their remote end point devices has increased costs for IT

In order to manage and secure communications across the enterprise, three fundamental questions must be answered:

1. **Who is the user?**
2. **What is on the end point device?**
3. **What resources are being accessed?**

To establish universal access control, every user should be authenticated; every end point system should be interrogated to determine its identity and state of integrity; and only then should users be provided appropriate, policy-based access to resources. Your firm's IT vendor needs to make a comprehensive evaluation of the state of the end point device in order to implement a policy decision and classify the device accordingly. IT also needs to be able to correlate authenticated users with the resources which they are authorized to access.

A staged approach can bring immediate and ongoing results without making a significant impact on budget and resources. For instance, a first step might invert the internal wired office network by replacing it with a wireless network secured via an SSL VPN appliance. This would unchain end users from their desks and provide them with flexible access to application tools from other offices and conference rooms located within the corporate wireless campus, thereby promoting collaboration and increased productivity.

A second step could extend secure remote access via the Internet to employees at home or on the road. A third step might apply standardized remote access as the foundation for a remedial disaster recovery strategy in case workers are forced to work away from the office during an emergency. Step four might standardize remote access policy for all mobile devices. Step five might incorporate SSL VPN access policy and end point controls into broader enterprise network access control (NAC) initiatives. With each step, the organization moves closer to it's goal of providing universal access with universal control.

As local and remote users and their associated devices continue to converge, the demand for a secure, controlled, policy based remote access policy becomes more and more imperative. Your exact approach to network perimeter security should closely follow your firms' business demands and need to protect sensitive firm and client data. Please review next month's article on the specifics of remote application and data access.

Ernesto T. Negron – partner, technical delivery, Eric D. Jordan – partner, emerging technologies and delivery, David N. Boughter Jr. – partner, sales and marketing, R. Matthew Wadsworth – partner, sales/client relations.

FirmTech Inc.

Firm Tech, Inc. is an information technology consulting firm servicing the Southeastern United States of America. Our vertical markets include legal and professional services firms, not for profit and hospitality companies.
Firm Tech, Inc. builds, manages and optimizes customized, client-centric networks that are strategically tailored to meet an organization's specific business goals and requirements.
http://www.firmtechnology.net