SonicWALL Aventail E-Class SSL VPN

Best Practices for Secure Remote Access — A Guide to the Future

The future trend is towards a universal access control model, one which inverts the network so that the protective perimeter is concentrated around application resources.

CONTENTS

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Executive Summary

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 endpoints potentially unsafe. But users will demand access to business resources from any location. The future trend is towards a universal access control model, one which inverts the network so that the protective perimeter is concentrated around application resources. Your focus shifts to securing communications between all users and business-critical applications. SonicWALL® Aventail® E-Class Secure Remote Access (SRA) technology provides you with the solutions you need to establish universal access control today.

The Evolution of Secure Remote Access

Remote access technology has evolved dramatically over the past decade. New mobile devices and business solutions, offered in new combinations—that weren't even on the radar for enterprise IT a few years ago—are announced in the industry nearly every day. Broadband access to the Internet has become an expected standard, at work, at home and everywhere in between. Traditional desktop PCs are being replaced by laptops, PDAs and smartphones, all mobilized with sophisticated wireless and cellular connectivity. The rise in VoIP has turned phone calls into data resources and transformed telephony into yet another network access methodology.

This fundamental technological shift has sparked a remote access revolution across the enterprise, reflected in a sharp increase in teleworker use cases worldwide. Partners, vendors and consultants play an increasingly vital a role in daily operations. Increasingly, traditional network boundaries are disappearing. "The office" no longer has anything to do with any specific physical location:

Executives expect full access to the same application and file resources whether their laptop is at headquarters or in a hotel suite on the other side of the world.

Accountants require secure access to financials on a remote data site mainframe from satellite field offices via the Internet.

Fundamental Changes in Remote Access

- **Increased teleworking**
- **Proliferation of mobile devices**
- **Ubiquity of broadband**
- **Rise in IP telephony**

Sales teams now take their virtual office on the road with them using a host of mobile small form factor devices and also demands access to corporate resources from public kiosks at multiple hotels, airports and convention centers.

Business partners, vendors and consultants, often collaborating in cross-functional teams, require access to "internal" enterprise resources across the extranet from endpoint locations behind their "external" firewalls.

Remote teleworkers in all business capacities connect to business applications and files via WiFi hotspots at their home or neighborhood cafes.

Increased access can mean increased productivity, since work can now be conducted from field offices and home offices, partner sites and manufacturing sites. However, attempts at providing wider access while still protecting network resources have often proven more difficult and expensive.

The Impact on Access Control

Mobile trends in technology and business operations have accelerated the replacement of traditional network nodes from IT-managed hard-cabled desktops to wireless laptops and mobile devices. Even when these devices are issued by IT, It is increasingly hard for IT 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

In many ways, local access is now treated more like remote access and vice versa. 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. Policy can dictate that instead of gaining network-wide access, local users are restricted to only authorized resources. However, policy can also widen access for remote users to a broader set of collaborative business tools.

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. Today, IT must assume that all users are potentially remote and that all endpoints are potentially unsafe. 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 traditional network perimeter must be tightly concentrated into a resource perimeter around the back office systems of the application data center. In effect, enterprise IT data centers will increasingly resemble e-commerce innovators like Amazon and eBay, providing Internet-based, globally-accessible services. Local/remote access evolves into universal access.

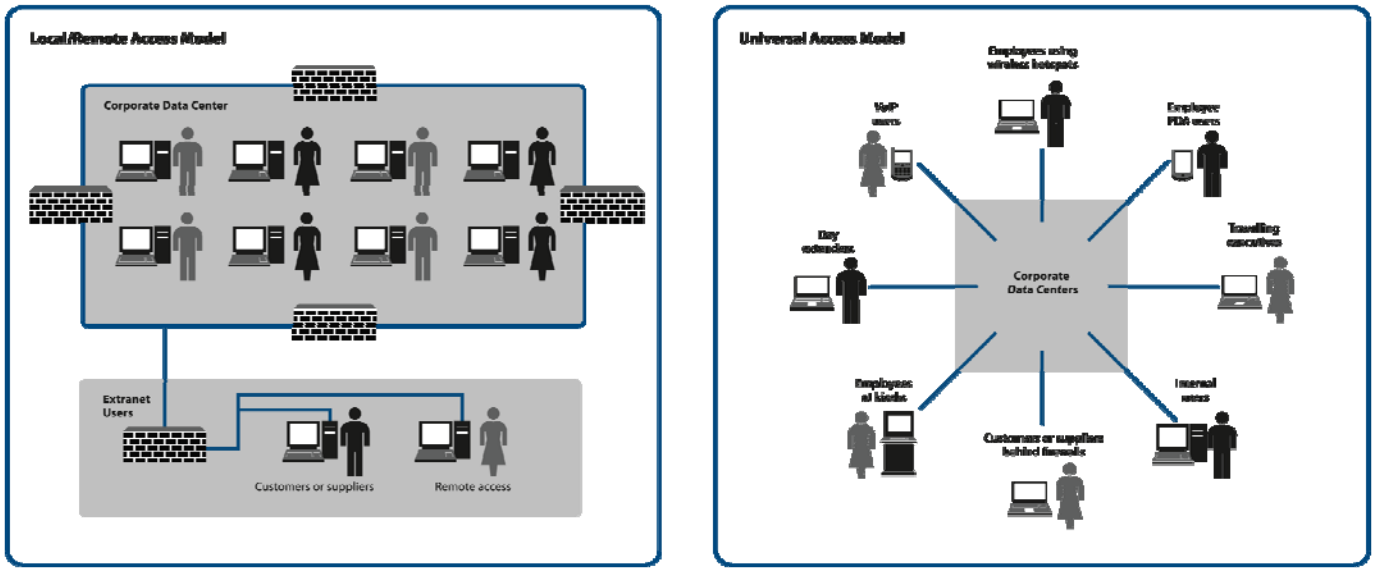
Universal Access

With universal access, the access playing field is leveled. No user, device or location is trusted implicitly and the focal point becomes the information resources: applications, data and services. Additionally, universal access expands the playing field. All users, devices and network technologies are potentially welcome, and all resources must be potentially available with ease from any endpoint device or location. However, while universal access to any resource must be potentially available, it does not mean it should be universally allowed. IT needs a strategy to establish and maintain universal access control.

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. IT managers must now assume that any user and device is a potential risk point, whether the user is gaining access remotely or plugged directly into the LAN. The increasing difficulty of managing end-users and their remote endpoint devices has increased costs for IT. Infrastructure costs have sharply escalated in attempts to harden an increasingly-fluid network perimeter.

The Evolution of Access

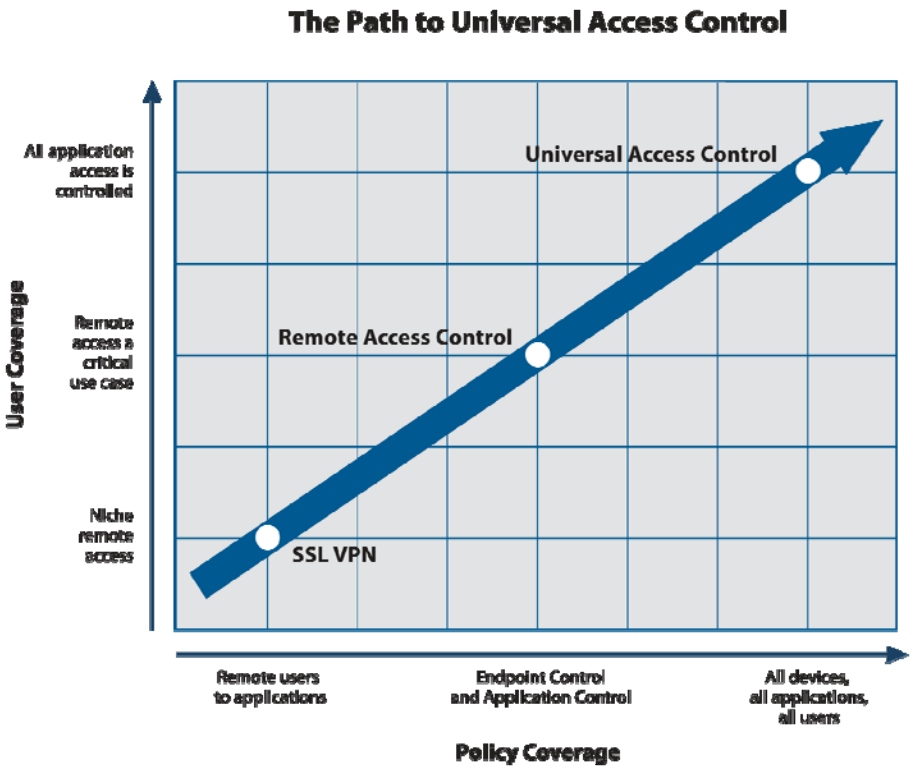


To increase mobile workforce productivity, organizations want to increase access to resources, while not increasing costs or complexity. To meet this goal, organizations need to consider increases in scale of deployments, application diversity and security demands. The scale and complexity of deployments is increasing, driving up costs of managing and maintaining traditional "fat client" remote access solutions. IT needs solutions that scale to existing infrastructure and systems, while maintaining performance. Application resources such as Web and client/server applications are becoming increasingly diverse and complex to use and manage remotely. And in order to mitigate risk, security must be tightened using universal access control.

To successfully establish universal access control, enterprises should re-examine how they view network security. Today, all users are potentially remote, all endpoints potentially unsafe and the underlying network is inherently insecure. Therefore, in order to manage and secure communications across the enterprise, three fundamental questions must be answered:

- Who is the user?
- What is on the endpoint device?
- What resources are being accessed?

To establish universal access control, every user should be authenticated; every endpoint 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. IT needs to make a comprehensive evaluation of the state of the endpoint device in order to implement a policy decision (e.g., based upon whether the user is authorized to use the particular device, or whether the device contains a valid device certificate or current anti-virus signature file) and classify the device accordingly. IT also needs to be able to correlate authenticated users with the resources which they are authorized to access according to security policy. And IT needs to unequivocally discern proof of the user's identity, using a strong authentication method.



A Step-by-Step Path to Universal Access Control

Instead of merely reacting to external trends, IT needs to provide leadership in directing the course of universal access control. IT managers should consider a strategic, phased approach to easing their organization's transition to universal access control. There are many areas in which IT can take incremental steps focused on immediate solutions for specific business and technology pain points, such as:

- **Remote Access:** Increase productivity by providing all employees with anywhere access that is easy to use and deploy.
- **Extranet Access:** Open access to partner to increase collaboration, yet do it in such away that access control and security is not compromised.
- **Mobility:** Mobile devices are increasingly functional for voice and data, requiring policy-based access control for IT-managed and non-managed mobile devices.
- **Securing Wireless Networks:** Secure users on the wireless network as tightly as remote users because of the concerns over who has access to the wireless network.
- **Enforcing Policy:** Collaboration and compliance is encouraging granular access controls, yet IT struggles to enforce policy across disparate points of entry.

- **Disaster Recovery:** During a business disruption, demand for access from remote locations could instantly spike to include the majority of your workforce.
- **Network Access Control (NAC):** NAC is positioned around host integrity checking and network access, yet many organizations want to extend that to cover application access control as well.

This 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, or to authorized business partners. 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 endpoint 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.

SonicWALL Aventail E-Class Secure Remote Access Appliances Deliver Universal Access Control

At the heart of managing this new reference architecture is the secure remote access control provided by SSL VPN technology. SonicWALL Aventail E-Class Secure Remote Access Appliances (SRAs) deliver best-of-breed SSL VPN to the most resources from the most endpoint locations. Consistently recognized by leading independent research analyst firms as a leader in the SSL VPN industry, SonicWALL Aventail E-Class SRA solutions are the easiest-to-use and easiest-to-manage solution for universal access control.

SonicWALL Aventail E-Class Secure Remote Access

Detect what is on the endpoint device. SonicWALL Aventail Endpoint Control™ lets IT enforce granular access control rules based upon the trust of the user and the user's endpoint environment, as well as certificate-based watermarking of mobile devices.

Protect resources being accessed. SonicWALL Aventail Unified Policy™ provides granular access control based upon user identity and device integrity. Aventail Unified Policy centralizes control of all users, groups, resources and devices, allowing administrators to quickly set a single policy across all objects

Connect users securely and easily to applications on any device. SonicWALL Aventail Smart Access™ delivers a seamless common user experience across a wide range of applications and platforms—including Windows®, Windows Mobile, Apple Macintosh®, iPhone®, iPad™ and Linux®—from managed or unmanaged devices, over a single gateway. Appropriate security is automatically selected based upon centralized resource policy, user authorization and the integrity of the endpoint.

About SonicWALL

Guided by its vision of Dynamic Security for the Global Network, SonicWALL develops advanced intelligent network security and data protection solutions that adapt as organizations evolve and as threats evolve. Trusted by small and large enterprises worldwide, SonicWALL solutions are designed to detect and control applications and protect networks from intrusions and malware attacks through award-winning hardware, software and virtual appliance-based solutions. Visit http://www.sonicwall.com/

SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 www.sonicwall.com