Securing the mobile workforce with SonicWALL appliances

By Patrick Sweeney and Matthew Dieckman

The mobile workforce presents significant security challenges to IT departments. SonicWALL® Aventail® E-Class Secure Remote Access (SRA) appliances are designed to support a comprehensive, policy-based approach to remote access that helps streamline management while enhancing security and flexibility.

Mobile technology is changing the face of business, enabling employees to be productive from virtually anywhere, cutting time and costs out of operations, and helping companies reach their customers effectively. But this technology is also presenting a significant challenge to IT departments—especially when it comes to security. With a growing range of devices and points of entry on the network, the “workplace” is no longer restricted to a protected area behind a hardened perimeter.

In response, IT departments often find themselves having to adopt a one-size-fits-all approach to authenticating end users and providing remote access, which often is not enough in a multifaceted mobile world. Alternatively, they may create a thicket of individual rules to try to meet the different enterprise and security needs presented by the wide range of users and devices, which can be complex, time-consuming, and expensive.

The growing emphasis on mobility requires a sophisticated, nuanced view of security. SonicWALL Aventail E-Class Secure Remote Access (SRA) appliances are designed to support a comprehensive, policy-based approach to security in Dell™ hardware-based IT environments—enabling access to mission-critical resources from virtually any endpoint device, streamlining policy management, and helping IT groups effectively provide the security and flexibility to support the increasingly mobile workforce.

Blurring the network perimeter

The expansion of mobile technology means that IT departments must contend with a wide range of data and voice devices, a growing number of which are personal devices used by employees. Mark Bouchard, founder of the AimPoint Group research and analysis firm, calls this the “consumerization” of IT. IT groups, he writes, are “being given no option other than to support the ongoing cross-over and melding of equipment, services, and activities of a personal nature with those historically identified as being ‘business-oriented.’” As a result, “the IT department, along with its network security infrastructure, must be able to account for a mixed bag. Not all devices will have a robust security model, not all devices will be corporate-owned and managed, and neither will there be clear relationships between a
device’s location (e.g., inside the network) and its type, security state, or category of user. 1

Beyond the use of mobile technology, other enterprise practices are also blurring the traditional network perimeter. Increased collaboration and the rise of extended enterprises mean that a rising number of external partners may need to access internal applications. And the use of teleworking is growing—a trend that is likely to continue, as rising transportation costs and environmental concerns encourage flexibility regarding working from home.

Many organizations are also looking at the role that a remote workforce can play in business continuity. This interest increased sharply with the recent focus on the H1N1 virus, which had the potential to keep large numbers of people away from offices. But disruptions such as snowstorms, earthquakes, and terrorist acts could also require an increased reliance on remote employees, and on the variety of managed and unmanaged devices they need to use.

Perhaps most significantly, as the importance of remote workers grows, many companies find that the complexity of providing security in this type of environment can actually stifle growth and productivity. According to a report from Nemertes Research, “new applications and services can, increasingly, transform operations or customer interactions, but 67% of enterprises in Nemertes Security and Information Protection benchmark have rejected attractive and useful applications.”

Designing an effective mobile security policy

SonicWALL Aventail E-Class SRA appliances are designed to support an increasingly mobile workforce securely and cost-effectively. By using Secure Sockets Layer (SSL) virtual private network (VPN) technology, these appliances enable security at the application level rather than the network level and can allow secure access even from unmanaged devices. They also provide a layered approach that enables increased granularity of policy and access control, which is key when dealing with a variety of locations and remote devices (see Figure 1).

The SonicWALL Aventail E-Class SRA policy-based approach encompasses three fundamental elements of mobile security: user authentication, endpoint device identification, and application access. The first element, user authentication, is based on authentication realms, which administrators set up to establish how end users are identified. Organizations can create multiple authentication realms to accommodate different requirements for different users. For example, some users may be required to provide only a username and password, whereas others may be required to use token authentication or stacked authentication. E-Class SRA appliances support a variety of authentication methods, including server-side digital certificates, usernames and passwords, client-side digital certificates, RSA SecurID and other onetime password tokens, and dual or stacked authentication.

For endpoint device identification, E-Class SRA appliances let organizations enforce granular access control rules for Microsoft® Windows®, Microsoft Windows Mobile®, Linux®, and Apple Mac OS X endpoints. Administrators can create device profiles that include attributes such as the presence of specific files, directories, registry settings, and antivirus programs; Windows hard drive serial number and Windows domain membership, and device type. These profiles are then used to scan and verify device attributes before access is granted. Based on the results of the scan, the device is placed into a security category, or “policy zone”, depending on the zone the device falls into, access may be granted or denied, or the device may be quarantined until some action is taken, such as installing a required antivirus update. Policy zones make it possible to provide differentiated access based on the type of device being used and the overall security state of the device—a significant enhancement over a typical approach that grants access to many potential resources regardless of the safety of the endpoint device.

Finally, for application access, E-Class SRA appliances look at the information gathered about users and devices—that is, the degree of trust established for those factors—and then matches it to a customized authorization policy that determines which applications and resources the user and device can access. For example, the policy may specify that employees working from home on unmanaged devices would be given just enough application access to carry out the basics of their work, while those same employees would have greater access to more sensitive content when using a highly secured, IT-managed device. A business partner using an external corporate system, an IT technician working from a home PC, and a traveling executive with a company laptop can all be given different yet appropriate access with relative ease—providing far more flexibility than a typical one-size-fits-all approach.

The policy-based approach is not only effective; it also helps reduce the complexity of managing access. This simplicity is further enhanced with the advanced, object-based SonicWALL Aventail Unified Policy™ model, which enables administrators to view and manage the entire organization’s remote access policy structure using a single integrated view in an intuitive management console. The centralized administration is designed to consolidate control of Web resources, file shares, and client/server applications in a single location.

Unified Policy also enables administrators to quickly and easily create a single rule set covering a comprehensive range of resources and access methods—avoiding the need to create separate access-control policies.2


"SonicWALL Aventail E-Class SRA appliances are designed to support an increasingly mobile workforce securely and cost-effectively."
rules for each user based on the type of resource he or she wants to access and the access method being used, all spread across separate pages in the management interface. A single rule can define access for an entire group of users across multiple resources using multiple access methods. For example, from one console page, administrators can define a single rule granting every user in a sales group access to sales-specific Web resources, file shares, and client/server applications from their workstations or their managed smartphones.

Taking advantage of the layered approach
The comprehensive, layered approach to mobile access provided by SonicWALL Aventail E-Class SRA appliances can provide a wide range of benefits, including the following:

• Effective remote access security: Effective remote access security includes comprehensive access management policies based not only on users, but also on the level of risk presented by the users’ environments. Granular access enables organizations to customize secure access for diverse endpoints rather than relying on a single approach that may or may not be appropriate for a given device.

• Streamlined IT management: Unified Policy helps to simplify use and administration, ease the burden on IT resources, and reduce systems management costs. The object-based model is also highly scalable—for example, E-Class SRA appliances have been successfully deployed in global organizations with more than 85,000 users. This scalability helps to reduce repetition for administrators and simplify network changes.

• Low total cost of ownership: In addition to helping reduce management costs, E-Class SRA appliances help lower IT costs by enabling network managers to easily deploy and manage a single secure access gateway to network resources for both internal and external users—including Web browser-based, host-based, and client/server applications. The appliances can be clientless or use lightweight Web-delivered clients, which helps reduce management overhead and support calls. They can also deliver high availability, with integrated load balancing and active/active failover on some models, helping eliminate the need for a third-party load balancer.

• Business continuity: In the event of a business disruption, organizations can quickly establish secure, appropriate access to an expanded remote workforce. E-Class SRA appliances can provide a secure application access gateway at primary data centers and serve as a gateway to hot, warm, or cold disaster recovery facilities. An optional SonicWALL Aventail Spike License Pack lets organizations temporarily and cost-effectively increase their remote user count to the maximum capacity of their E-Class SRA appliance, whether this capacity is a few dozen or a few thousand additional users.

• Increased productivity: Employees and partners can have appropriate yet controlled access to enterprise applications from a wide variety of devices and locations, helping to deliver the right information to users when and where they need it. E-Class SRA appliances also provide session persistence, which lets mobile users retain a current session when they switch between networks—for example, as they move between offices, cars, homes, and hotels—without needing to re-authenticate.

Supporting the mobile workforce
A mobile workforce brings with it specific security challenges that call for comprehensive, policy-based control of remote access. Using this type of approach in conjunction with SonicWALL Aventail E-Class SRA appliances and Dell hardware, IT departments can simplify the management of remote access without sacrificing sophistication or driving up costs. And they can meet the dual demands of providing high levels of security while supporting the flexible delivery of vital information—and help the enterprise thrive in the era of the mobile workforce.

Patrick Sweeney is vice president of the product management team at SonicWALL, where he oversees its network security, content security, business continuity, and policy and management product lines.

Matthew Dieckman is the product manager for SRA solutions at SonicWALL, where he drives the development road map for SonicWALL SSL VPN products and services.

Learn more
SonicWALL Aventail E-Class SRA appliances: www.sonicwall.com