Best Practices for Secure Remote Access

Aventail

Table of contents

Overview

SSL VPNs from companies like Aventail provide anywhere access that increases employee productivity. However, that key advantage brings with it increased risk. That's because today's organizations support remote access that is harder to manage, more public, and more mobile than ever before. You have more users accessing from untrusted environments such as kiosks and wireless hot spots. To reduce risk due to the increasing number of vulnerabilities these scenarios can cause, customers are tightening their remote access information security policies.

As the maker of the most widely deployed SSL VPN, Aventail provides more than half a million users and over 500 global organizations with complete secure remote access solutions. We have the opportunity to see common trends—both the pitfalls to avoid and the consistently successful practices—in how customers safeguard remote access to their networks.

Here is the list of some of the best practices for secure remote access implemented by our customers:

1. Strong, secure access policy for the corporate network
2. Personal firewall, anti-virus, and intrusion-prevention for all desktops
3. One-time passwords, especially from public machines
4. Policy by end-user environment and not just user identity
5. Disabled split tunneling, when connected to the corporate network
6. Extra protection for kiosks and other public PCs

Additionally, instead of prohibiting "unsafe" behavior on paper with no enforcement mechanisms in place, information security professionals are using technology to automatically enforce these essential policies.

The Aventail SSL VPN solutions provide an easy way for you to implement and enforce these best practices, thus enhancing security while simplifying your end user experience as well as your information security technology infrastructure. Give your employees and business partners secure remote access to the data they need—but maintain control of your policy.

1. Strong, secure access policy for the corporate network

Access control policies have become increasingly complex. Just a few years ago, only a few select employees had broad access to everything on the corporate network from remote locations using dial-up, and each application was secured and managed individually in a "demilitarized zone." Then IPSec VPNs, which promised the convenience of centralized security policy, administration, and management, became an appealing option for remote access.

Unfortunately, IPSec VPNs were designed to facilitate site-to-site communications between branch offices rather than to accommodate remote access users. They required client software that was difficult to deploy and expensive to support. Additionally, some IPSec VPNs revealed private IP addresses inside the corporate network, making the internal network vulnerable to denial-of-service and other network attacks. Finally, IPSec VPNs did not offer the granular access control essential for controlling access to internal applications for different types of users.

As more employees gained remote access privileges, the management burden and risks for unauthorized access increased. Consolidating all of the remote access users—employees, customers, and business partners—using one centralized secure remote access platform that offered strong encryption and authentication, and granular access control appealed to security professionals.

SSL VPNs provide a simple, clientless way to deliver access to business partners, customers, and employees from an Internet browser without exposing your network environment or having to manage client software. Aventail SSL VPNs provide proxy technology as well as granular access control to eliminate direct network connections to your corporate network, while providing transparent access to authorized users. With Aventail's SSL VPN, you can reduce the complexity and support costs associated with IPSec client software on end-users' desktops.

Aventail's granular access control enables you to limit access based on parameters like source (IP Address or Host Name) and port; destination; user identity and/or group affiliation; time, day, and/or date; application and/or service; authentication method and/or encryption algorithm; and path-level access for Web access and Windows file shares—even down to the specific file. That means you can limit each user—partners and employees—to relevant applications, Web sites, and other corporate resources, down to the specific URL.

For example, instead of simply identifying a user as an employee with access to the whole corporate network, the

individual can be identified as a member of the sales organization. A sales group is then provided with access to the CRM applications, the corporate portal and sales file shares, but not to the ERP or the company's financial systems.

Aventail enables you to shelter your internal network domain name system (DNS) and network topology, and reduces the risk of unauthorized access or attacks on your network resources. For additional security, Aventail integrates with popular access control or authorization systems for more complex authorization scenarios. No direct connections to the internal network are allowed.

2. Personal firewall, anti-virus, and intrusion-prevention for all desktops

If a PC is infected with worms or viruses, these malicious applications will try to spread to your corporate network using the encrypted tunnel of the VPN. Active personal firewall and anti-virus applications eliminate worms and viruses from PCs, thus protecting the corporate network.

So, as a part of their security policy, many organizations require active and up-to-date personal firewall, anti-virus, and other desktop security applications on all PCs. It is especially important to enforce this on remote PCs before the remote access connection is established.

However, enforcement of this policy is challenging. If the required desktop security applications stop running for any reason, the user must either remediate the problem or the system has to shut down the connection. If the user is at a public kiosk, he or she may be denied access if appropriate security applications are not installed.

Today, Aventail® Connect™, our Web-deployed Windows SSL VPN agent for full secure access to network resources, automatically detects all running desktop security applications. If the required application is not running or is not up-to-date, Aventail Connect warns the user and provides him or her with an option to remediate this problem. Unless the problem is resolved, the Aventail SSL VPN shuts down the connection.

What is Aventail Connect?

Aventail Connect is a Windows agent that provides authorized users with secure access to the entire corporate enterprise. Remote or traveling employees with a corporate laptop would take advantage of this full-access VPN. This option is also appropriate in situations where IT wants tight integration with the user's operating system for additional security and ease of use. Connect provides:

- Transparency for the end user. Deep Microsoft Windows integration enables an effortless user experience, including Microsoft single sign-on and mapped drives.
- Effortless administration. AutoUpdating makes ongoing administration simple.
- Advanced security options. Aventail Connect supports advanced security options, like split tunneling control, personal firewall integration, and anti-virus detection.

In addition to Aventail Connect, we seamlessly integrate clientless access options, including browser-based access for web applications and file shares, and Aventail® OnDemand™, a Java agent for secure client/server application access. For more information, please go to http://www.aventail.com/products_services/access_options.asp.

3. One-time passwords, especially from public machines

Although they are convenient, static passwords present a number of known security issues. First, users have a tendency to choose dictionary words or other relatively easy-to-guess static password and then re-use them across multiple systems. Second, a number of password-guessing tools are readily available on the Internet. Easy passwords combined with sophisticated password-guessing tools make remote access systems reliant on static password fairly insecure. Also, in public places, hackers can use a number of methods to intercept static passwords—from shoulder-surfing by standing right behind the legitimate user, to key stroke logging with hidden software, to network eavesdropping using legitimate network monitoring tools. Organizations reduce the risk of password guessing or interception by investing in one-time password mechanisms or other authentication

methods that generate authentication credentials that are not reused.

Aventail integrates with all of the commonly used authentication systems, including RSA SecurID, Secure Computing Safeword, Swivel technologies and others. The user is required to authenticate to the Aventail SSL VPN using his one-time password or other authentication credential before the network connection is established.

4. Policy by end-user environment, not just user identity

Employees, customers and business partners are pushing the envelope for convenience. They demand access to corporate resources from public places, potentially exposing the corporate network to worms and viruses that hide and spread on public computers and networks. As a result, information security professionals now must take into consideration the level of risk in the user's environment, not just the user's identity.

With End Point Control, Aventail helps you enforce policy based upon the level of trust that you have for the user's environment, not just the level of trust that you have for the user. Using Aventail to manage access by environment and Aventail partners to make those environments safer, you can truly deliver secure access from virtually anywhere. Aventail's partners enforce policies for firewalls, intrusion detection, virus protection and other client-side security issues, while Aventail encrypts and authorizes access to all corporate resources with access control policies based on both the user's identity and the security of the user's environment. Today Aventail delivers End Point Control through source-based access policy rules, control over split tunneling, strong authentication support, automatic detection of desktop security applications, cache protection, AutoCompletion blocking, user authorization, and crypto level access control. This allows Aventail to first detect the individual and their environment, then to secure that environment, and finally to deliver the right level of access to that user.

5. Disabled split tunneling when connected to the corporate network

Many VPN products allow connections to multiple networks simultaneously. A user can browse the Web using a public Internet connection while concurrently accessing his or her corporate network through a VPN. This is called "split tunneling." Unless properly configured, split tunneling can make your corporate network accessible to a hacker connected to the public Internet.

Public Internet, cable networks and wireless LANs are all shared among multiple users, and therefore introduce additional risks. These networks are frequently accessed using a home PC that may not be securely configured for sharing or networking. If this is the case, a hacker can use the shared or public network to gain access to the home PC.

A legitimate user can initiate a VPN connection to the corporate network, while a hacker is accessing the employee's home PC. If this happens, the intruder can gain access to the corporate network through the compromised home PC, unbeknownst to the end user or the corporate security manager. Even worse, with broadband, many of these home PCs are always on, providing intruders with uninterrupted opportunity to cause harm. To prevent hackers from gaining access to the corporate network by utilizing a shared network and improperly configured home PC, organizations explicitly turn off split tunneling capabilities on their VPNs.

The Aventail SSL VPN supports split tunneling, but perhaps more importantly, it provides organizations an ability to turn it off. Organizations can implement split tunneling control settings enterprise-wide, for specific groups, or for specific users.

6. Extra protection for kiosks and other public PCs

Public machines, including PCs at Internet cafes or airport kiosks, can be dangerous. Public machines can be infected with viruses or Trojan horses that capture user key strokes or execute malicious code. Additionally, the next person in line to use the PC can hit the Browser "Back" button and see potentially sensitive information from the previous user's login session.

Given the risky nature of this environment, additional training about kiosk security is common for employees who tend to use public machines for remote access. In fact, many organizations go a step further and ban users from accessing their corporate network from public machines altogether. Unfortunately, some users may forgo compliance to such a draconian policy for convenience, when running to catch that last-minute flight and needing to download their itinerary from e-mail.

If the corporate policy indeed prohibits access from kiosks, the VPN technology should be able to identify kiosks and prohibit or limit access from these machines. Alternatively, through the use of one-time passwords, organizations can allow limited access from

public machines, while eliminating cached and saved data stored on the public machines.

Aventail End Point Control provides the best possible protection for public PCs with cache cleaning. Additionally, if the corporate policy mandates no access from public machines, the Aventail SSL VPN can be configured to allow access with the Aventail Connect agent only, which is not available on public machines.

Summary

Every time a remote user accesses your internal network, your organization faces a number of different risks. With the best practices described above, you can mitigate the most serious risks, while enabling users convenient and flexible access. As the leading SSL VPN vendor, providing thousands of customers with complete secure remote access solutions, Aventail has a proven track record of enabling secure access for the real world. We can help you refine your secure remote access policy and enforce this policy with our award-winning SSL VPN.

About Aventail

Aventail, the recognized SSL VPN leader, provides clientless VPN appliances and services that give employees and business partners transparent, secure, anywhere access to any application. Aventail makes the world's most widely deployed and proven SSL VPN, with more than half a million users and more than 500 global organizations using it. With the most award-winning SSL VPN on the market, Aventail has been recognized as the fastest growing SSL VPN vendor and has been named a Gartner Magic Quadrant leader three times since 2002.

WP-4066-1103/1

Corporate Headquarters
808 Howell Street
Seattle, WA 98101
Tel 206.215.1111
Fax 206.215.1120
americas@aventail.com
www.aventail.com

Aventail Europe Ltd
Tel +44 (0) 870.240.4499
emea@aventail.com

Aventail Asia-Pacific
Tel +65 6832.5947
asaipac@aventail.com