QUICK GUIDE

SSL VPN Technical Primer

Today's increasingly mobile workforce can now take advantage of ubiquitous broadband service, expanding wireless access, and a proliferation of Internet-enabled devices. These users expect access from everywhere—whether they're at home, in a hotel room, working from behind another company's firewall, at an airport kiosk, or at the neighborhood coffee shop.

SSL VPN technology is designed specifically to enable increased productivity for remote users by providing easy-to-use, secure access to applications and resources on your network, while minimizing many associated risks and significantly lowering administration and support costs.

HOW TO USE THIS PRIMER

This primer explains the basics of SSL VPN technology and includes distinguishing factors between IPSec and SSL VPN technologies. You'll learn why these two technologies, based on fundamentally different designs and methodologies, each serve specific use cases best.

The format of this primer is designed to help you quickly find the necessary answers to many common questions about SSL VPNs and to understand the many advantages of SSL VPNs for everywhere remote access. Armed with facts about the capabilities of existing offerings, you'll be well-prepared to make decisions regarding the remote access technology that best meets your company's specific needs.

Aventail
More secure. More access. It's that simple.

WHAT'S DRIVING THE NEED FOR SECURE REMOTE ACCESS?

To maintain the level of productivity that today's workforce demands, more users are accessing more applications remotely than ever before. They are doing so from a broad range of devices and environments, including many that IT departments cannot control. With limited resources, IT must accomplish all of the following:

- Provide remote access to multiple complex applications
- Reduce risks from increasing numbers of unmanaged access points
- Lower administration and support costs

A growing number of companies are turning to SSL VPNs for their flexibility, ease of administration, and proven security.

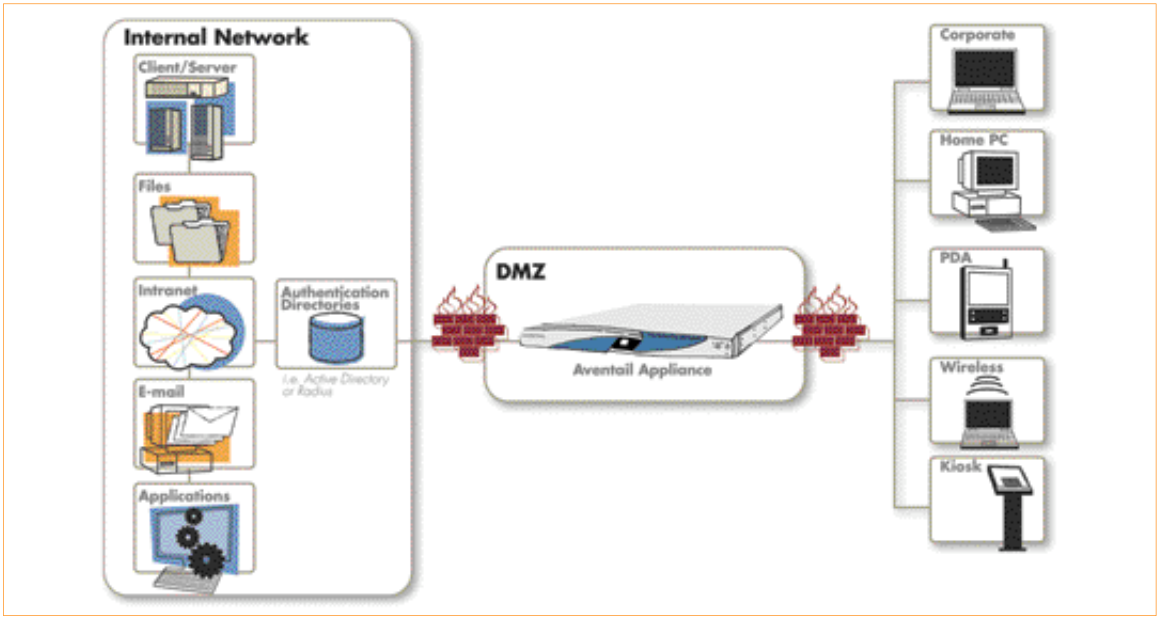
Compared to an IPSec VPN, an SSL VPN offers:

- Increased productivity, because it works in more wired and wireless environments—including home PCs, kiosks, PDAs, and other unmanaged devices
- Lower costs, because it is "clientless"—reducing management and support calls
- Increased security suited to remote access—by providing granular access controls and endpoint control

WHAT IS AN SSL VPN?

This remote access technology describes a secure type of virtual private network (VPN); the Secure Sockets Layer (SSL) protocol protects all traffic using encryption and authentication to keep communications private between two devices, which are typically a Web server and a user's computer.

- SSL was originally designed to secure the HTTP protocol for better protected Web-based communications at the application layer.
- In the most simplified form, an SSL VPN is a reverse proxy that uses SSL for encryption and a sophisticated access control engine.



SSL VPN delivers secure remote access for business communications.

HOW DOES AN SSL VPN WORK?

From any Internet browser, a user connects to the SSL VPN appliance and, after valid authentication, gains access to the applications and resources for which he or she has access privileges. Access is proxied, so there is never a direct connection to the network. In addition, this access occurs at the application layer, not the network layer, which enables finely grained access control. The entire data stream is encrypted using SSL.

WHAT IS AN IPSEC VPN?

This suite of protocols provides security for IP traffic at the network layer. Internet Protocol Security (IPSec) VPN technology is predicated on the existence of a trusted relationship between networks or between users and a network, and defines how to provide data integrity, authenticity, and confidentiality across a public network such as the Internet. It accomplishes these goals through tunneling, encryption, and authentication but allows enterprises to select the specific security policy appropriate for their business.

- IPSec VPN technology originally was developed to protect data communication between private, trusted networks over the Internet.
- IPSec was later extended to protect data communication between mobile workers gaining remote access to a company's internal network in a more efficient manner than legacy dial-in methods.

HOW DO IPSEC AND SSL VPNS COMPARE?

When applied appropriately, both IPSec and SSL VPNs use authentication and encryption standards that secure enterprise communications over the Internet.

- IPSec VPNs use tunneling and encryption to secure the data transfer over the Internet between a private network and a trusted computer.
- SSL VPNs provide data encryption using the RC4 or DES/Triple-DES algorithms. SSL VPNs also provide key management through the standard SSL key exchange method using the RSA algorithm with bit lengths up to 1,024.

SECURITY AND ACCESS CONTROL

IPSec and SSL VPNs provide flexibility in allowing enterprises to define the level of security that best meets their needs. But based on its architecture, Secure Sockets Layer is better suited for securing application-based remote access. Aventail SSL VPN technology provides employees, business partners, and customers with secure anywhere access—including clientless access to Web applications, client/server applications, and file sharing.

IPSec VPN: By its very nature, this technology assumes that the end point is secure and authorizes users unless otherwise restricted. This assumption addresses unauthorized network access but does not prevent a user entering with a virus or keystroke logger. In addition, IPSec has difficulty with NAT (network address translation) and personal firewall traversal and has not proven effective in connecting home networks, consultants, or business partners because the different networks demand changes in configuration each time. Furthermore, IPSec's network-based connection model is not capable of determining application-layer access. IPSec solutions can't provide granular access control due to their lack of application-layer support.

SSL VPN: This VPN technology can easily address the vulnerabilities of IPSec VPNs. With SSL VPNs, end-user access to any given resource is restricted unless authorized, a vastly different approach from that of IPSec VPNs. As a result, SSL VPN technology provides the granular access control that requires all users, regardless of location, to be granted explicit permission to access specific network resources. With SSL VPN technology, access control to applications and networks can be as general or specific as required.

CONFIGURATIONS OPTIONS

IPSec configuration choices include:

- Tunneling—Authentication Header (AH) or Encapsulating Security Payload (ESP)
- Encryption—56-bit DES; 112- or 168-bit 3DES; 128-, 192- or 256-bit AES; or none
- Authentication—Username/Password (such as Active Directory or RADIUS); user name and token pin (such as RSA SecurID); Internet key exchange (IKE); or X.509 digital certificates (such as Entrust or VeriSign)

SSL VPN configuration choices include:

- Encryption—40-bit or 128-bit RC4; 56-bit DES; 112- or 168-bit 3DES encryption
- Authentication—Username/Password (such as Active Directory or RADIUS); user name and token pin (such as RSA SecurID); or X.509 digital certificates (such as Entrust or VeriSign)

COST DIFFERENCES

Today, the initial price to purchase an IPSec VPN is less than that of an SSL VPN. However, when companies tally all related costs, the return on investment (ROI) for an SSL VPN is much greater. Because SSL VPNs have no client to deploy and manage, and are much easier to use, the ongoing costs to IT for administration and support are far lower. In addition, since users have anywhere access, overall productivity increases.

HOW DO IPSEC AND SSL VPNS APPROACH MOBILITY?

Inherent design differences exist between IPSec and SSL VPN protocols. IPSec VPN technology was designed to establish a connection and protect private data streams between trusted networks. It does not qualify that access. SSL VPN technology, on the other hand, was developed to address the weaknesses of IPSec for remote access. SSL VPNs—which were designed to protect data streams between associated sources, all of which are untrusted, regardless of whether they are users or a network—supplement security by qualifying access to applications. Understanding this key concept is fundamental to selecting and implementing the appropriate VPN solution for your business needs.

NETWORK LAYER VS. APPLICATION LAYER

IPSec is network-layer centric, while SSL is application-layer centric. That means an SSL VPN can easily provide secure, granular access controls, ensuring that users gain access only to the designated resources or applications specific to their needs, and according to security policy. Using an IPSec VPN, it is very difficult to create such precise control rules, so most organizations end up providing open access to their whole network.

HOW DO IPSEC AND SSL VPNS APPROACH MOBILITY? (CONTINUED)

FIXED VS. MOBILE ACCESS

IPSec was designed to tie together separate trusted networks in different locations. Because SSL VPN was designed for mobility, it delivers clientless anywhere access to the network from multiple locations and from the widest variety of devices possible through any Internet browser.

CLIENT SOFTWARE VS. CLIENTLESS

IPSec cannot be used without pre-installed client software running on the user's machine. SSL VPNs use any Web browser as the client, providing clientless access that increases the number of points from which employees, partners, and customers can access network data. Clientless access also simplifies the connection process for the user as well as the configuration and management for the IT administrator.

INCREASED ADMIN VS. SEAMLESS NAT/FIREWALL TRAVERSAL

Not all IPSec VPN solutions can provide secure access through NAT and firewalls, and those that do often require additional administrative support. Because SSL VPNs were designed specifically for remote access, they seamlessly traverse NAT, firewalls, and proxy servers.

WHAT USE CASES MUST A SUCCESSFUL REMOTE ACCESS SOLUTION ADDRESS?

Providing remote access improves user productivity, yet carries security risks. Access is no longer limited to corporate-owned and –maintained devices, so external resources such as personal digital assistants (PDAs) must be incorporated into a growing list of supported devices and environments. Although you probably don't place equal trust in all points of access, such as partner networks or airport kiosks, you'll need to grant access to them, as well as to corporate wireless users, consultants, and day extenders working from other untrusted networks. A successful remote access solution handles a broad range of internal and external users securely from any end point.

IPSEC VPN BEST-USE SCENARIOS

IPSec is best suited for point-to-point access. Open tunneling protects data between two private networks or between IT-managed machines and a private network. IPSec VPNs are optimal for transmissions between headquarters and:

- Branch offices
- Corporate-issued laptop PCs

SSL VPN BEST-USE SCENARIOS

SSL VPN is best suited for remote access. It is network-independent, so there is no need to reconfigure administration rights as the user changes end points. Additionally, application-level access ensures that all users gain access only to the information and applications they require. SSL VPN is optimal for accessing applications and data on the corporate network from anywhere with Internet access, including:

- Kiosks at airports, tradeshows, and libraries
- Hotel rooms
- Home offices
- Behind a customer's firewall

WHY CHOOSE AN AVENTAIL SSL VPN?

Aventail's leading SSL VPN technology is the most secure in the industry, offers the most transparent, flexible combination of anywhere access options, and is extremely easy to administer and use. Whether the customer is using an appliance or managed service, Aventail's award-winning technology offers superior End Point Control, efficient centralized policy management, and greater scalability, resulting in a lower total cost of ownership (TCO). Aventail is exclusively focused on SSL VPNs, investing more in the development of the technology than any other company.

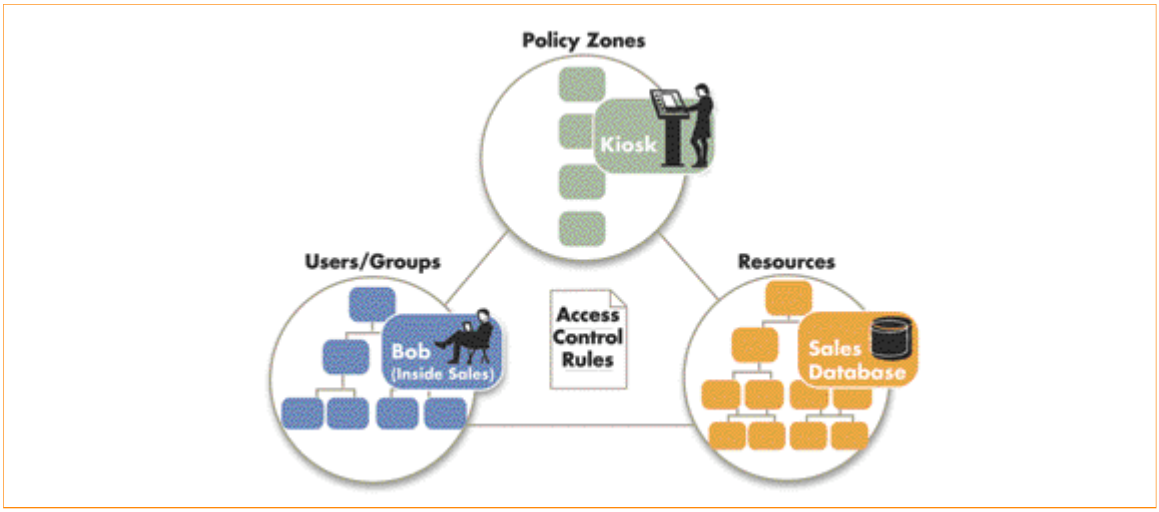
Supported applications and protocols:

- Web-based applications, including most Java script and Visual Basic (VB) script content
- Any TCP-based application
- Most UDP-based applications
- HTTP and HTTPS protocol
- SSL protocol

HOW DOES AVENTAIL ENHANCE SECURITY?

Aventail's SSL VPN technology sets the standard for delivering full secure access to a broad range of applications on your corporate network from anywhere—including many locations and devices that the IT department cannot control. Time-tested and standards-based, Aventail's SSL VPN technology helps reduce risk through its combination of SSL and proxy technologies, granular access control, and a single point of management.

At the core of Aventail security is Aventail's object-oriented policy model. This scalable model is both flexible and efficient. You gain a single view of all access control rules, which is far simpler and ultimately more secure than the typical flat policy management approach used by other SSL VPN vendors' products. Unlike those models, which become increasingly complex as you add groups and resources, Aventail's access control rules match users/groups to defined resources, which can then be made dependent upon the specified Policy Zones. In a single step, you can make object changes.



Aventail's object-oriented policy model offers a single view of all access control rules.

Aventail's hierarchical, object-oriented policy model lays a strong foundation for Aventail® End Point Control™ (EPC). With EPC, your business can deliver secure anywhere access to network resources from even the most dangerous places—airport kiosks, employee-owned PCs, wireless hotspots, and unmanaged PDAs—without sacrificing the integrity of the corporate network.

WHAT IS END POINT CONTROL?

Aventail End Point Control is the ability to enforce policy based upon the level of trust that IT has not just for the user but also his or her environment. With EPC, IT organizations can establish and define Policy Zones, including untrusted machines such as kiosks, semi-trusted machines such as home PCs, and trusted corporate assets like laptops, and then manage those zones with a simple set of parameters. Aventail's leading policy-based EPC solution provides the high degree of granularity required so IT can reduce risk, provide access from more places at a lower cost to the organization, and control access by user location.

Aventail End Point Control ensures security using three essential components:

- **Device Interrogation:** Aventail End Point Control automatically interrogates the end point when the user accesses the company's SSL VPN in order to determine what is and what is not on the machine. To ensure that the access point is free of malicious software ("malware") like keystroke loggers and Trojan horses before allowing access, Aventail automatically launches an agent from one of its best-of-breed partners. This happens prior to authentication so login can be stopped if any malware is discovered. It's easy for administrators to enable this critical first step simply by checking a box on the Aventail® ASAP™ Management Console (AMC).

- **Policy Zones:** Device Interrogation looks for certain applications or "watermarks" on the end point. For example, if a specified antivirus product or a personal firewall is present, Device Interrogation may instantly classify the end point into one of the predetermined Policy Zones—such as trusted, semi-trusted, and non-trusted. Each zone enables a different level of access, appropriate to its level of risk.

- **Enhanced data protection and remediation:** Aventail combines its market-leading data protection features, Aventail® Cache Control™ and Aventail® Secure Desktop™, with Policy Zones to provide the most flexible remote access options available. Remediation efforts launch the appropriate tools to allow access with complete security.

WHY ARE POLICY ZONES NECESSARY FOR SECURE REMOTE ACCESS?

Many organizations want to support a broad range of access environments but would like to differentiate that access for less trusted end points. To do so requires multiple zones of access control. Aventail Policy Zones extend Aventail's market leadership in End Point Control by allowing administrators to create multiple zones of trust based on the security of an end device. Unlike competing models that allow only "on" or "off" options of access control, Aventail Policy Zones allow three or more zones to be created, such as trusted, semi-trusted, and non-trusted. Three or more zones are needed to ensure maximum security while meeting the range of trust on an end device and range of access requirements by end users.

Creating Aventail Policy Zones, with different levels of access tuned to a user's identity and the risks of his environment, is fast and easy with the Aventail Zone Wizard, a step-by-step process for administrators to match users, resources, and zones. As an example, you could create three zones:

- **Non-trusted zone:** access from airport kiosks and other unprotected machines, with many restrictions.
- **Semi-trusted zone:** access for users working from home PCs or machines behind a supplier's firewall, with fewer restrictions.
- **Trusted zone:** access for employees using corporate assets like a laptop PC, with the highest level of access.

HOW DOES AVENTAIL PROTECT AGAINST SECURITY THREATS?

Individuals who gain unauthorized access to a private corporate network can cause extensive damage by hacking through critical files. Likewise, viruses and other malicious agents can delete important files and programs or simply divert valuable resources to rectify ensuing problems. Corporate IT departments configure PCs under their control with antivirus software, firewalls, and other safeguards designed to protect them from malicious software. In contrast, unmanaged PCs can easily contain keystroke recorders, viruses, Trojan horses, and other hazards that can compromise a company's network.

- Aventail SSL VPNs detect personal firewalls and applications and perform other client-integrity checks.
- Aventail ensures that only authenticated users can gain access by checking privileges against an LDAP-enabled database, a RADIUS server, an NT domain, a UNIX user name/password database, RSA SecurID ACE servers, and others.
- To verify that a user's environment is secure, Aventail SSL VPNs integrate with third-party client-integrity controls that automatically check for malware on the client system before allowing access.

PROTECTING NETWORK AND USER DATA

Removing user data from a PC after a user has accessed network data in a Web-browsing session is an important security mechanism. For example, a user who logged in from a public kiosk can inadvertently leave sensitive data in the PC's cache, including passwords, browser cookies, and bookmarked URLs. Users may also accidentally leave files or e-mail attachments on the hard disk.

Aventail offers advanced data protection features—Aventail® Cache Control™ and Aventail® Secure Desktop™—to help reduce these risks.

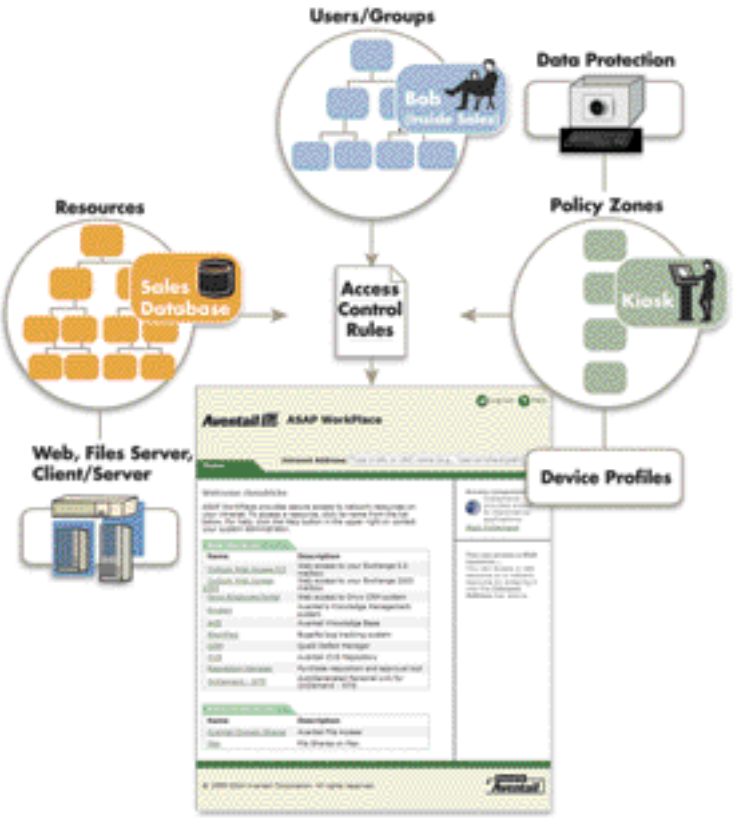
- **Aventail Cache Control (ACC)** significantly improves data protection by removing cached data (not simply moving it to the Recycling Bin) not only from the browser, but also from the browser history and downloaded files.
- **Aventail Secure Desktop (ASD)** is an optional component that provides enhanced data protection for Windows users. ASD creates a virtual desktop environment, which looks and feels like the regular desktop, but is actually an "encrypted vault." That means that all the user's local data—attachments, cookies, cached content, and the like—are encrypted in real time, and at the end of the session, all data is destroyed to U.S. Department of Defense standards. In addition to deleting downloaded or new files stored anywhere, ASD ensures that the entire session is encrypted.

With an Aventail SSL VPN, you can meet the needs of the business—anywhere access at a lower cost—without sacrificing the integrity of the corporate network or intellectual property.

HOW DOES AVENTAIL HELP SIMPLIFY THE POLICY MANAGEMENT EXPERIENCE?

Aventail has the only SSL VPN platform that was architected from the ground up for ease of administration. Aventail® Unified Policy™ enables IT to quickly manage complex access control rules for their SSL VPNs. Unified Policy provides a flexible, consolidated access control rule set for creating and managing rules for Web resources, file shares, and client/server resources, regardless of the access method used.

- With Unified Policy, you can easily define rules for remote access in fewer, simpler steps than you would encounter with competing products. On average, policy setup with the Aventail product takes just 15 minutes compared to hours for other SSL VPNs.
- All policy management information is centralized and streamlined for ease of administration and ongoing management, so you gain tight control of all methods of accessing the corporate network.
- Because Policy Zones are treated as an additional object in Aventail's policy model, configuration is simple.
- Aventail's object-based policy management model provides extremely granular access control.
- Unified Policy also enables you to achieve greater security yet spend less time on setup, training, and maintenance, which leads to lower cost of management and administration.



Aventail Unified Policy reduces the time that IT administrators spend on setup and ongoing management.

HOW DOES AVENTAIL PROVIDE A BETTER USER EXPERIENCE?

Aventail® Smart Access™ makes access easier, faster, and more transparent for end users, because it automatically determines and launches the most appropriate access method. In Aventail® ASAP™ WorkPlace, a Web portal that provides intuitive access to Web and client/server applications and file shares, users simply select the link to the desired application and Aventail Smart Access dynamically utilizes the appropriate access method. Users don't need to think about the required access method, what software is loaded on their PC, or the operating system that they are using; access to the required application just works in real time. Plus, users never have to worry about pop-ups or downloads.

THE BENEFITS OF AVENTAIL CONNECT

Aventail® Connect™ is a Web-deployed Microsoft Windows SSL VPN client that provides authorized users with secure, anywhere access to the entire corporate LAN for a complete "in-office" experience. While Connect does require an initial download, it's not the traditional VPN client. It provides an extremely high level of transparency and simplicity for the end user, including features such as network auto-discovery and integration with third-party dialers. It is ideal for situations where users have a corporate laptop and need full application and file access, and IT wants to support secure access with strong desktop security, including split tunneling control and personal firewall detection.

AVENTAIL'S VISION

At Aventail, we envision a world where end users have the freedom of secure access from everywhere and IT departments have the power to easily and securely manage that access to all network resources. That means providing maximum control and flexibility for IT, as well as ease of use and mobility for the end user.

Aventail delivers the technology leadership and research innovation to support this vision, investing more in the development of SSL VPN technology than any other comp a n y, large or small. Aventail's award-winning technology is designed to give users a seamless, transparent experience and IT a streamlined remote access management solution. With its best-of-breed partnerships, Aventail offers the industry's most comprehensive SSL VPN platform.

Aventail is happy to assist you in learning more about existing SSL VPN solutions and future developments, so you can make the most informed decision about your company's unique remote access needs.

ABOUT AVENTAIL

Aventail is the leading SSL VPN product company and the authority on clientless anywhere secure access. Aventail's appliances and managed services deliver secure, seamless access from anywhere, to any application, on any device. Positioned in the Leader quadrant in Gartner's 2004 SSL VPN Magic Quadrant and ranked as a Leader in the 2004 METAspectrum report on SSL VPNs, Aventail also was recently awarded "Best VPN" by *SC Magazine.* Major service providers such as AT&T, MCI, Sprint, and Bell Canada have built their SSL VPN managed service businesses on Aventail's SSL VPN technology. To find out what Aventail customers like Aetna, DuPont, Office Depot, TNT, and Sanyo already know about Aventail's SSL VPN, go to www.aventail.com.

FOR MORE INFORMATION

Visit www.aventail.com for additional information. Download educational papers on our document download page, including:

- "Comparing Secure Remote Access Options: IPSec VPNs vs. SSL VPNs"
- "Buyer's Guide: Criteria for Choosing the Right SSL VPN"
- "SSL VPN Checklist"

Aventail
More secure. More access. It's that simple.

Aventail Corporate Headquarters:
808 Howell Street
Seattle, Washington 98101

Phone: (877) AVENTAIL (283.6824)
or 206.215.1111
Fax: 206.215.1120
E-mail:
aventailcustomerservice@aventail.com
www.aventail.com

Asia-Pacific
Phone: +65 6832 5947
E-mail: asiapac@aventail.com

Northern EMEA
Phone: +44 (0) 870 240 4499
E-mail: emea@aventail.com

Central EMEA
Phone: +49 (0) 69 7593 8122
E-mail: emea@aventail.com

Southern EMEA
Phone: +33 1 47 48 22 11
E-mail: france@aventail.com

International (rest of the world)
E-mail: info@aventail.com

WP-4092-0904/1