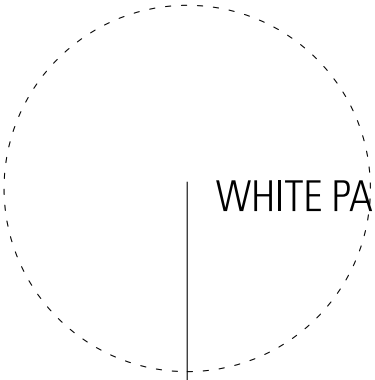
Aventail

A New Security and Management Architecture for Extranets



WHITE PAPER

www.aventail.com
Tel 206.215.1111
Fax 206.215.1120
808 Howell Street
Second Floor
Seattle, WA 98101

Table of Contents

Executive Summary

Business-to-business communication is nothing new, but the latest enabler — the extranet — gives rise to a dramatically different horizon for how companies (and individual people within those companies) share resources. The predictions vary, but the trend is indisputable — separate business enclaves are disappearing, and new associations of interconnected partners are emerging. The increased exposure is alarming to some; but for those who deploy secure and well-managed extranets, the possibilities are tremendous.

"Extranet," as the prefix implies, refers to a private network that is designed to let a company share data securely over the Internet or other public IP networks with outside users, such as partners, suppliers, and customers. By leveraging proven Internet technologies, extranets make it possible for organizations in all industries to optimize processes, collaborate with partners in real time, automate supply chains, and share applications with a distributed group of users, each with unique requirements and permissions. These benefits lead to increased competitiveness, greater customer and partner loyalty, and unforeseen revenue streams — the real drivers of extranets.

Extranets allow organizations to easily manage and secure the flow of enterprise resources and the use of applications. Instead of relying on leased lines or even phones and fax machines to share needed resources, extranet participants can use their existing Internet connections from anywhere in the world to access a corporate network. Extranets conveniently and affordably establish a secure channel through which authorized individuals gain varying levels of access to protected resources within the network.

As we move into the 21st Century, extranets will become an essential part of every competitive business model. Analysts predict that the competitive marketplace will drive IT managers to get business-savvy in order to keep their jobs. They will need to justify purchases and demonstrate ROI, not just cost savings, which is why extranets will be a good investment. Corporations that deploy extranets now will gain a significant advantage, leaving those that hesitate far behind. Already, more than half of the Fortune 1,000 are using extranets today, according to a recent report from Forrester Research. Those that are not rushing to deploy extranets are reportedly holding off because of security concerns. Just as more than locks are needed for any high-security building, more than encryption is needed to securely manage access to corporate resources.

Aventail has designed from the ground up a complete solution for managing and securing shared resources across organizational boundaries. Historically, corporations have put up blockades to protect their networks rather than allow regulated access. Over time, companies have opened their doors to trusted users, such as employees, through the use of LAN-to-LAN encrypted tunnels. Today, companies realize the value of integrating business processes with partners and customers, but they need a better method of securing and managing those interactions over the Internet. Aventail develops a management and security software solution for extranets to help companies overcome security threats and transfer real-world trust models to the virtual world. When a company's user base is diverse — perhaps consisting of consultants and various departments at partner firms, each requiring varying levels of access to different resources — Aventail ExtraNet Center provides the easiest, most secure and complete management architecture for extranets.

Intranet and Extranet Defined

The terms “intranet” and “extranet” are widely used by many people in today’s business world, but they are often used loosely with different connotations. For the sake of clarity, they are defined below.

“Intranet” was a term coined to describe a private network, owned and operated by a corporation and usually protected behind a firewall or series of firewalls, that leverages Internet technologies. Companies have adopted intranets as a cost-effective way to share information with employees. When intranets are extended to remote employees and branch offices, LAN-to-LAN security needs to be applied, usually with a virtual private network (VPN) or encrypting router.

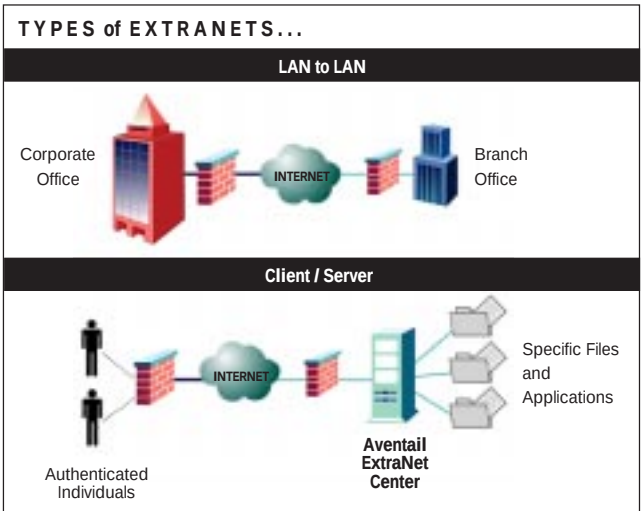
	Internet	Intranet	Extranet
Access	Open	Private	Tightly Controlled
Users	Public	Employees	Business Partners, Customers, etc.
Resources	General	Proprietary	Mixed

Extranets make use of several networking technologies, including virtual private networks. Modern VPNs are proving to be very effective for linking branch offices and subsidiaries. While VPNs provide encryption for data being transferred over the Internet, they lack adequate functionality for controlling where specific users can go and what they can do once they are on a secured network — the primary requirements of extranets. As the VPN market has matured, a need has surfaced for a solid extranet platform on which non-employee access to information and applications can be closely governed.

Contrasted Extranet Models

Not all extranets address the same audience or provide the same level of security and management. Most commonly, they fall under two categories: LAN-to-LAN extranets and client/server extranets. The former includes systems such as electronic data interchange (EDI), and the latter includes both Web-based and fully operational extranets, which encompasses more than just HTTP access.

TYPES of EXTRANETS...



LAN-to-LAN extranets provide basic encryption for information sharing between trusted parties, whereas client/server extranets add granular access control to the basic services for sharing resources with specific users, such as partners.

LAN-to-LAN Extranets

A LAN-to-LAN extranet connects servers between different companies over the Internet. LAN-to-LAN extranets provide only encryption and IP-based authentication, relying on individual applications to provide user-based authentication and access control, which make them unwieldy to manage for companies that want to control individual access. They are much more practical for serving as encrypting gateways that permit or deny connections from entire partner networks.

Take, for example, the Automotive Network eXchange (ANX), which offers an extranet service for major automobile manufacturers and their business partners. The ANX extranet was designed to encrypt document exchange between EDI servers at participating companies. The ANX extranet eliminates the need for expensive leased lines, but it does not allow its participants to control individual access to specific resources at the application level. Client/server extranets may be deployed by several participants to run in conjunction with or on top of the basic functionality provided by the ANX.

The ANX, like most LAN-to-LAN extranets, uses IPSec as the security standard. IPSec was designed to provide security between multiple firewalls and routers. In the client/server configuration, it has a number of disadvantages that may be difficult to get around. IPSec, for all practical intents, requires a public key infrastructure. Today's PKIs are relatively young, and concerns about overall scalability still exist. Any company that wants to use two-factor authentication, such as token cards, should avoid IPSec because maintaining both systems (token cards and key pairs) requires a tremendous amount of administrative overhead. IPSec was designed with the assumption that a large amount of network address space would be available, which is the case with ANX. Most companies, however, use dynamic rather than fixed IP addresses. Because Aventail ExtraNet Center does support Network Address Translation (NAT), it can be a valuable complement to any LAN-to-LAN extranet.

Client/Server Extranets

Client/server extranets connect individual users to a company's internal data and applications, as opposed to connecting entire organizations. With a client/server model, the extranet provides all the security, not just the encryption, as well as sophisticated management of users and policies. Client/server extranets are designed for companies that want to build a model of personal accountability, retaining control over which resources they share and with whom. In contrast, LAN-to-LAN extranets follow more of an all-or-nothing approach to resource access. Client/server extranets strongly authenticate each individual, not just their IP address, and grant them access to specific resources according to detailed user profiles. Encryption is part of the basic infrastructure, so authentication, access control, and management are the distinguishing features among different client/server implementations.

CLIENT/SERVER EXTRANETS COMPARED

	Web Only	Client / Server
Applications Supported	HTTP Only	All IP-Based
Uses	Publishing Information	Dynamically Sharing Resources
Advantages	Universal Access through Browsers	Easy Integration with Existing Systems & Applications
Disadvantages	Limited Functionality and Interactivity	Client Software Required

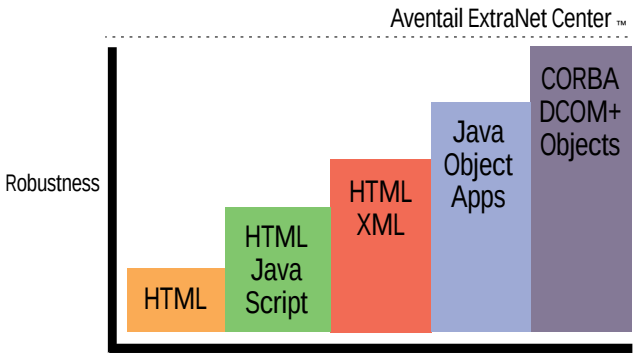
The client/server model can be implemented with either Web-only extranets, which use a browser for the client, or fully operational extranets that use executable client software. One approach is not inherently better than the other, only more suitable for different organizational requirements.

Web-based extranets are wholly appropriate for information sharing, such as with consumer-oriented sites like Federal Express. The notion of having everything go through a browser is gaining momentum, but it still presents a monumental challenge for companies that want to leverage existing systems. Placing a browser front-end on custom or legacy applications is often only a partial solution. Many enterprise applications have native interfaces that offer much greater flexibility and speed than their HTML translations, which limit functionality and interactivity. Also, many organizations are not eager to retrain their employees on new systems.

If a company has no need to leverage existing applications and wants only to deliver information, starting from scratch with a Web-based extranet makes sense. Many companies initiate an extranet by starting with Web-only information delivery and later enabling full client/server applications. Companies should carefully weigh the value of replacing client/server software with "webified" versions. A browser front-end can be handy, but a webified

backend can be very limiting. Though Web-only extranets are useful for publishing information, transitions from client/server to Web-only applications are rarely smooth and are very expensive and time-consuming, not to mention that users often report dissatisfaction with the end result. A better approach is to deploy an extranet that can support more than HTTP.

Aventail ExtraNet Center is designed expressly for those companies that need a fully operational extranet that can back-end seamlessly to existing systems. It is ready for implementation today, and it extends beyond HTTP to include Web-to-host gateways and direct access to ERP, legacy, and other applications that are not easily converted to the Web. It is also designed to work with emerging object-oriented Web technologies, which may someday be the standard.



Application Evolution

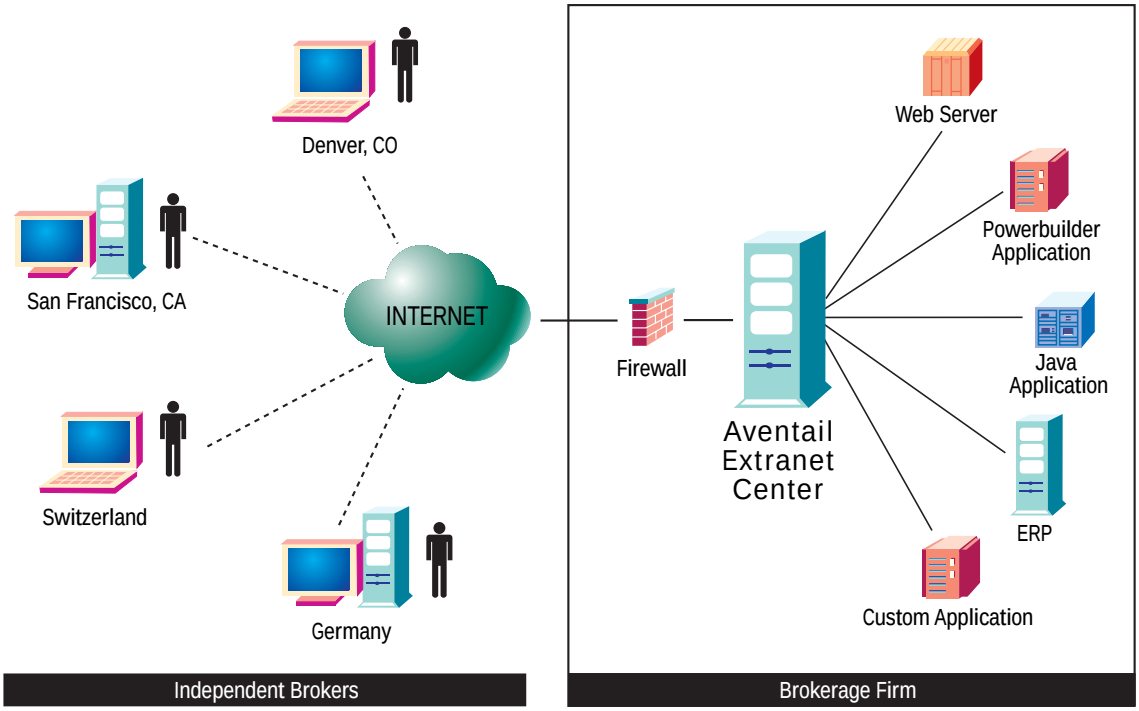
Case Study

To better understand the client/server extranet vision, consider what different industries have already achieved with this technology. The financial services industry is a good example. Brokerage firms, money managers, investment banks, and investors are in the business of clearing trades, which means they care more about the volume of transactions and related transaction fees than the direction the market moves. Firms in this business service independent brokers who do not have their own clearing facilities. These independent brokers are dependent on the clearing firm for rapid, secure, highly available clearing services, which they then use to service their end clients. Independent brokers are demanding and are always on the lookout for a clearing firm that can offer the best, most convenient services. Deploying a client/server extranet can give a clearing firm the means to provide customer care and improve service, whereas a LAN-to-LAN extranet lacks the access control necessary for limiting individual access to confidential resources, which is required when working with multiple (often competing) independent brokers.

Because it can take months, sometimes years, to make clearing firms profitable, client retention is paramount. To improve service and speed manual processes, a number of financial services firms have deployed Aventail ExtraNet Center. One firm in particular uses Aventail's security and management software to extend more than 20 Powerbuilder and Java applications to independent brokers over an extranet. The Aventail solution enforces the firm's rigid security policies in a seamless and transparent fashion. The architecture of the solution allows the brokers to stay connected to the firm over a strongly authenticated and encrypted session without requiring that they disconnect from their critical real-time market research feeds. The brokers can connect to the firm's extranet over the public Internet through any ISP, or they can access the extranet across a leased line or frame-relay connection.

The brokers now have access to trading applications, portfolio management applications, proprietary market research, and other services over a highly secure, transparent, cost-effective connection. Other benefits include:

- **Increased Client Retention**
  Independent brokers are less likely to consider working with competitors because it is easier for them to work with the brokerage that provides information via an extranet.



- **Increased Transactions**
  Allowing brokers to access the trading network securely and continuously makes it easier for them to trade securities through the brokerage firm, which increases the rate of transactions.
- **Increased Quality of Trades**
  Because orders are entered at the independent broker's office, the number of key strokes per trade is dramatically reduced, and the chance for errors in data entry is reduced.
- **New Services Opportunity**
  By using Aventail's extranet solution as a secure conduit for information exchange, the firm can easily deploy new applications and services to its client base. This means new revenue opportunities for the firm.

Technology Used

The technology used to implement such client/server extranets is SSL, a standard for transmitting private documents over the Internet. It uses private keys to encrypt data and has two implementations — Web SSL, used to secure HTTP, and Enterprise SSL, which secures all IP-based traffic. Aventail combines enterprise SSL with SOCKS v5, the IETF standard for authenticated firewall traversal, which gives Aventail ExtraNet Center the ability to traverse any firewall. This is particularly useful in extranet environments where participants use different firewalls.

Because SOCKS v5 and SSL are both open standards, Aventail ExtraNet Center supports most authentication, encryption, and key management methods, providing IS managers the freedom to adopt the best technologies for their needs. Plug-and-play capabilities include access control tools, protocol filtering, content filtering, traffic monitoring, reporting, and administration applications. Aventail ExtraNet Center also peacefully co-exists with lower-layer protocols, which is important if a company is already using protocols such as PPTP and IPSec.

To expedite true interoperability of IPSec and SOCKS v5/SSL, Aventail is currently working with a variety of vendors such as Microsoft, Intel, NEC, Novell, and RedCreek on multiple industry initiatives to define a common security association that can be used for network-layer tunneling and session-layer security. Aventail provides the most comprehensive management framework for client/server extranets available today, and it is a solid foundation for future extranet possibilities.

Planning an Extranet Strategy

Most large corporations are faced with an incredibly complex business challenge — determining the best solution to enable secure information exchange over the Internet with business partners without requiring infrastructure changes or security

compromises for any partner. Aventail ExtraNet Center is ideally suited to address this paradigm. It is a standards-based proxy solution that provides unparalleled flexibility and a balanced approach to security and management.

Without a solution like Aventail ExtraNet Center, the options for securing and managing extranets are grim. Firewall administration is too bulky for the transitive nature of extranets. Due to the expanding and changing series of business partners associated with an extranet, network administrators should be able to regularly and easily add, remove, or modify users from the system. Reconfiguring firewalls on a regular basis is risky. For the most part, they are designed to be configured once and then left alone.

Some companies set up a firewall (or firewalls) to keep intruders out and a demilitarized zone (DMZ) to share corporate data. The DMZ sits outside of the private network and is accessible through the public Internet. Though some security precautions can be taken, such as stronger packet filtering rules on the router, hardening of the Web servers, and SSL to encrypt and authenticate user sessions, sensitive corporate data is basically exposed on the public Internet. In addition to the lack of security, another drawback to the DMZ is administration. If a company wants to share its intranet resources with a partner, it has to replicate the data for the DMZ. Access control has to be managed by each Web server.

The best practice for security-conscious companies is to use their firewall as a gateway to the organization and deploy an extranet-specific solution behind their firewall that proxies content between users and the host network. Aventail ExtraNet Center functions as an intelligent proxy that controls who can access what resources, and with what restrictions. It is helping the virtual business-to-business marketplace evolve away from static information postings toward the dynamic and secure delivery of individually tailored information over the Internet.

The Aventail Approach

Extranets are not about faster, cheaper encryption boxes or transaction-based e-commerce; they are about collaborative partnerships. Communicating over the Internet in real-time to negotiate business deals, procure inventory, collaborate on architectural CAD designs, quickly update production schedules, view patient health records, synchronize distribution channels, combine co-marketing efforts — this is the charge of the extranet. Aventail believes that extranet design should be shaped according to business requirements, not the reverse. In line with that idea, Aventail ExtraNet Center is the direct result of customer requests for a product that could secure and manage extranet communication while satisfying criteria such as user transparency, granular access control, diverse platform and application support, scalability, and remote server management. Aventail ExtraNet Center tackles the intricate technological requirements so that organizations can concentrate on their business strategies.

Aventail ExtraNet Center consists of the following server and client software.

Aventail ExtraNet Server™

The server is the brain of Aventail ExtraNet Center. It houses the business rules that determine what to do with connection requests based on parameters such as who the user is, what their role is to the organization, how they are trying to access information, and what they want to do with it. It is essentially an optimized SOCKS v5 proxy server that secures and controls all incoming and outgoing TCP/IP traffic.

The Aventail Policy Console is the graphical management tool that makes it easy for network managers to create, view, and edit extranet policies. It can also be used to start and stop the server, as well as view log, audit, and license files. It can be run locally on the same machine as the server or remotely, which enables remote management of the extranet through a secure LAN, WAN, or Internet connection. The Policy Console is platform independent. It can be used to configure extranets on both Windows and UNIX platforms, regardless of whether the Console is running on a Windows NT or UNIX machine.

Screen shots of Aventail ExtraNet Center's Policy Console

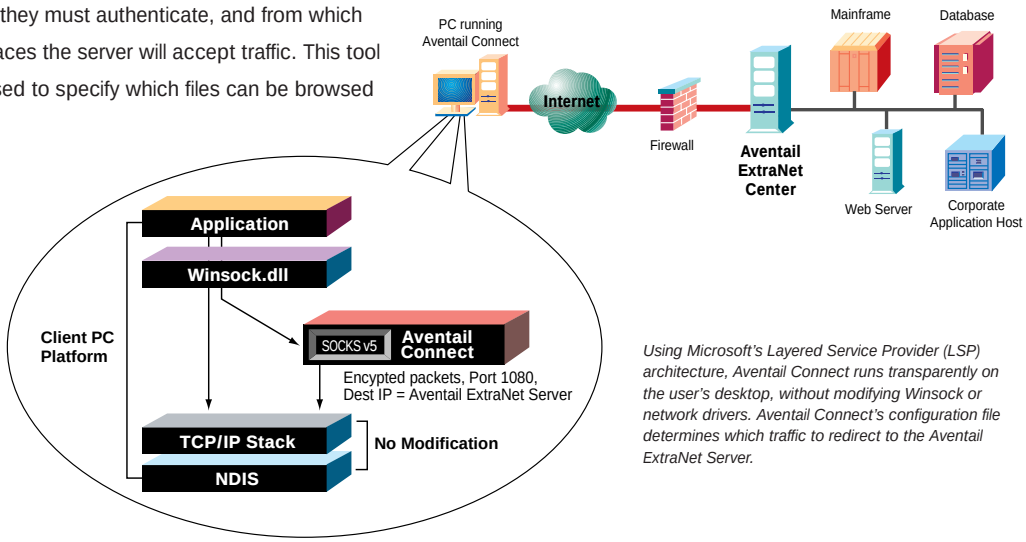
If a network administrator wants to manage an ExtraNet Server remotely, there is a component called the Aventail Management Server that is used to communicate with the Policy Console via a highly secure, encrypted connection.

It can be configured with the graphical Management Server Config Tool. This tool enforces who can manage the extranet, how they must authenticate, and from which network interfaces the server will accept traffic. This tool also can be used to specify which files can be browsed remotely.

Aventail Connect™

Aventail Connect is the client component of Aventail ExtraNet Center that redirects all TCP/IP application calls to the ExtraNet Server. It is extremely lightweight and easy to deploy, modify, and update, and it is transparent to the end user. In most cases, the user will not know it is running until prompted for credentials, which happens once per session when connecting to a secure server.

Unlike tunneling technologies like IPSec that typically insert a low-level shim (which can wreak havoc with desktop applications), Aventail Connect does not replace or modify networking transport components. It sits between the application layer and the Winsock level using Microsoft's Layered Service Provider architecture, redirecting traffic as needed. In extranet scenarios where non-employees are connecting to a corporation that does not manage their desktop environments, it is essential that the client be non-intrusive. In other words, users should not have to make a conscious decision or effort to launch an extranet. Everything should happen automatically and transparently.



Using Microsoft's Layered Service Provider (LSP) architecture, Aventail Connect runs transparently on the user's desktop, without modifying Winsock or network drivers. Aventail Connect's configuration file determines which traffic to redirect to the Aventail ExtraNet Server.

Typically, network administrators distribute Aventail Connect as a self-extracting *.exe* file on an FTP or Web server. It is sometimes distributed on CD-ROM. In most cases, it is the network administrator, not the end user, who creates and distributes the configuration file. The configuration file (about two to three KB) specifies the redirection rules. It is usually distributed via e-mail. In the optimum scenario, it is the server-based access control, not the client configuration file, that determines the user's privileges.

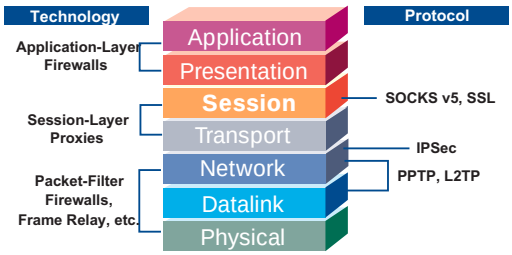
Aventail has created the Customizer™, a step-through wizard, to guide administrators through sophisticated customizations of Aventail Connect. It makes it very easy to create thousands of configuration files instantaneously. It supports multiple client configurations for users who access multiple extranets, and it allows administrators to mix and match authentication and configuration options.

Technology Used

Much of Aventail's success stems from the fact that its solutions easily integrate with existing infrastructures. Aventail chose to build Aventail ExtraNet Center using open standards SSL and SOCKS v5, which have been tested rigorously in the marketplace and proven to be very stable, flexible, and secure. Aventail ExtraNet Center essentially protects resources by intelligently proxying traffic between source and destination computers. When used in conjunction with a firewall, data packets are passed through a single port in the firewall (port 1080 by default) to the ExtraNet Server, which then filters what is retrieved according to sophisticated rules. This prevents administrators from having to open multiple holes in their firewall for different applications.

Because SOCKS is the IETF standard for authenticated firewall traversal, it allows use of any type of firewall, which is critical in extranet deployments. If a business partner has an Axent firewall and the host company has a Check Point firewall, SOCKS makes a seamless connection, whereas IPSec generally requires client compatibility with firewalls.

Both SOCKS v5 and SSL operate at the session layer of the OSI networking model, providing far more detailed access control than protocols operating at lower layers like IPSec, which permit or reject packets based solely on source and destination IP addresses. Aventail ExtraNet Center establishes a virtual circuit between a client and a host on a session-by-session basis and provides monitoring and strong access control based on user authentication. The host can never initiate a session with the client, which prevents the possibility of anyone creating a "hacker's bridge" from one point of access to another, which is possible with LAN-to-LAN extranets.



Aventail ExtraNet Center operates at the Session layer

Another issue Aventail addresses with its SOCKS/SSL approach is network address translation. Aventail's products use dynamic network address translation and proxied connections. This is beneficial for companies that may have illegitimate addresses on their private network or who do not want to show their private addresses. IPSec, by comparison, is always going to be limited to legitimate, routable addresses to the target peer device. Some vendors get around this by replicating all routable addresses outside of the firewall. However, if a company has a lot of resources they want to provide access to that change frequently, the IPSec approach is not very realistic from an administrative perspective.

Core Competencies	Features	Benefits
Superior Security	Granular Access Control	Enables definition of user access based on a wide range of parameters, such as source, destination, authenticated UserID, type of application and/or service request, type of encryption and/or authentication, and day and/or time. Aventail ExtraNet Center is the only product on the market that can drill down to this level of granularity.
	Support for Multiple Levels of Encryption	Allows tailoring of encryption by application and security needs. Aventail ExtraNet Center supports 40-bit, 56-bit, and 128-bit levels of DES, Triple DES, MD4, MD5, SHA-1, RC4, and Diffie-Hellman.
	Support for Multiple Authentication Methods	Facilitates and makes the best use of a variety of methods, including passwords, tokens, digital certificates, and biometrics. Aventail ExtraNet Center supports CHAP, RADIUS, NT Domain Passwords, Digital Certificates, Token Cards, S/Key, and Username/Password.
	Directed Proxy Architecture	Provides tighter security than standard encrypted tunnels by eliminating direct connections to business-critical resources and preventing the exposure of private addresses to public networks.
Built-In Flexibility	Infrastructure Independence	Extranets should complement, not replace, existing network architec tures. Aventail ExtraNet Center can be seamlessly integrated with partner networks. No other extranet solution offers comparable firewall, protocol, and infrastructure compatibility. AEC also works with most encryption and authentication methods.
	Application Independence	All TCP/IP applications. Applications that are difficult to webify, such as mainframe, custom, and other non-HTTP applications, can be secured. Aventail ExtraNet Center also supports Java and Active X applications, as well as those based on CORBA and DCOM+.
	Cross-Platform Support	Aventail ExtraNet Center is one of the only extranet products to support Windows NT and all major platforms of UNIX for the server. The client runs on all Windows desktops.
	Database/Directory Integration	Aventail ExtraNet Center backends to multiple user directories to prevent administrators from having to replicate user policies. User rules are stored in a policy database on the server, where user passwords, etc., can be manually entered or imported from directories such as Windows NT Domain, NetWare Directory Services (NDS), Remote Authentication Dial-In User (RADIUS), and Security Dynamics ACE/Server.
Powerful Management	Easy Installation/Deployment	Aventail ExtraNet Center eliminates the complexities of extranet deployment by allowing administrators to easily create and distribute customized configurations for the clients (even thousands at a time) through a wizard-based tool called the Customizer.
	Transparent Client	The client piece of Aventail ExtraNet Center is designed to run transparently on the user's desktop without making any modifications to existing drivers, transports, or applications.
	Simple Remote and Local Management	Aventail ExtraNet Center comes with an intuitive graphical interface called the Aventail Policy Console that makes it easy to create user profiles and enforce security policies. It can be administered on the server itself, from the administrator's desktop, or from any remote location.
	Intelligent Datastream Filtering	Aventail ExtraNet Center includes a sophisticated engine that allows administrators to create pre-defined or custom access rules based on multiple parameters, such as source, destination, user, group, day, date range, and time.
	Traffic Monitoring and Logging	Aventail ExtraNet Center allows administrators to monitor and log several layers of server activity and network traffic, and the information can be easily imported into spreadsheets, databases, and other reporting tools.
	Scalability	There are no inherent scalability issues with Aventail ExtraNet Center, only with the hardware it runs on. AEC is designed to manage thousands of users simultaneously through single or multiple servers.

Features and Benefits

Companies need tools that can simplify extranet security and management. They want to be able to give third-party users access to internal resources with a click of a button. Aventail's client/server software paradigm makes it easy for organizations to give users around the world access to the resources they need. According to Forrester Research, what separates extranets from the Internet is their security architecture. Aventail ExtraNet Center tightly integrates encryption, authentication, and access control under one robust, open-standards management umbrella. Because of its architecture and design strengths, analysts expect that Aventail ExtraNet Center will be used primarily for extending mission-critical data to diverse user groups across multiple organizational perimeters.

In order to allow third-party individuals to access a corporate network, access control is imperative and should be flexible enough that corporations can create security policies "on the fly" for each individual. Aventail ExtraNet Center simplifies management of user-based security policies so that IS managers can define access parameters according to an individual's role, function, or group. In addition, it offers cross-vendor interoperability and can accommodate heterogeneous systems. Unlike intranets, extranets must be able to complement a wide variety of systems because corporations can rarely assume ownership of their partners' security infrastructures and/or desktops. Most importantly, the solution requires no training or change in network configuration for end users.

Essentially, the features of Aventail ExtraNet Center are designed to eliminate the headaches typically associated with setting up a secure system for internetworking among partners and other business associates. Unlike firewalls, routers, and tunneling protocols, Aventail ExtraNet Center allows IT managers and line-of-business managers to build a truly agile extranet.

By clicking on a desktop icon called "Extranet Neighborhood" (á la Network Neighborhood), users see only those resources that have been made available to them.

Competitive Advantage Over Cost Savings

Companies that deploy an extranet only to save money are missing the point. With business-to-business commerce over the Internet projected to eclipse business-to-consumer spending by a large margin over the next few years, according to International Data Corp., the business case for extranets is compelling. Extranets allow companies to turn business ideas and strategies into realities, generating new revenue opportunities. Processes that typically require human intervention are being automated, streamlining operations. Rather than relying on phone, fax, and overnight express, companies can use their extranet to exchange mission-critical data in real time with their business partners, from anywhere, at any time of day. The net effect enables companies to break into new markets, globalize communication, and deliver products and services faster and cheaper.

Extranets are the most effective system for giving authorized individuals customized, immediate access to information 24 hours a day, seven days a week. As enterprises plan their strategies for prospering in today's and tomorrow's marketplace, they should clearly define each segment of the user population and determine which processes could be better carried out through beneficial relationships that increase the potential for huge economic opportunity by allowing companies to automate well-codified business rules.

Improved Customer Care

With a greater emphasis on relationship building and increased customer demand for information and services, companies are turning to extranets to care for existing customers, who are the most cost-effective customers to support and the most expensive to lose.

Healthcare is an industry that makes a convincing argument for the justification of extranet technology. Take a federal health agency, for example, that wants to immunize all children by the age of two. Maintaining a record of who has been immunized and making that information available to health agencies around the country is exactly the kind of task driving the extranet market. Extranets coordinate rather than duplicate information. Health records need to be kept private and made available only to authorized individuals, which is exactly the need that Aventail addresses. Extranets provide broad, immediate access to information, and Aventail secures that data and provides tools to manage it.

If a federal health agency wanted to create a network of shared databases, it could use Aventail ExtraNet Center to secure and manage the extranet so that all data transferred would be secure and access could be strictly controlled. Aventail ExtraNet Center can be seamlessly integrated into a variety of infrastructures, and all IP-based applications are supported, including databases, distributed Web sites, and custom applications and interfaces.

Supply Chain Automation

Without an extranet, tracking inventory, accounting, and shipping costs involves a lot of guesswork and hidden costs, which means project bids are often off-target. By giving the appropriate people direct access to the information they need, companies can eliminate wasteful steps and speed up the entire distribution system. Businesses that delay deploying extranets risk losing essential market share.

To adapt to the new Internet economy, companies must adopt the notion of dynamic trading, which refers to the evolution from static Web marketing to interactive online procurement of information, production and distribution logistics, customer support, scheduling, and order processing. “By the end of 1999, more than 25 percent of major distributors and financial-service providers will use the ‘extranet’ banner to attempt to ‘extend’ their business models to include the sale of extranet management services to their trading partners (.8 probability),” reported a Gartner Advisory in April 1997. Extranets are reshaping internal processes, improving external relationships, and seamlessly tying together technical infrastructures.

Supply chain management is a popular topic, because improving these processes pays off. Enterprise resource planning (ERP) applications help control the financial aspects of supply chain coordination, but they alone do not change business practices. They need to be combined with systems that facilitate communication and planning among internal departments, distributors, other manufacturers, and consumers. Extranets optimize the use of resources, planning, communication, and response time. In the process they reduce costs, improve customization, and enable companies to gain market share.

Summary

The success of any company depends greatly on its ability to manage its partners. Irrefutably, Aventail ExtraNet Center provides the power to create business opportunity. It does so by allowing organizations to share key resources with the right people over public networks seamlessly, securely, and effectively. Aventail ExtraNet Center is designed to work in almost any IP environment. It can be customized to fit very specific needs; it can traverse any firewall; it functions with multiple protocols and platforms; it secures all TCP/IP traffic (not just HTTP); and it is transparent to end-users. Aventail ExtraNet Center leverages legacy systems and is designed to support emerging technologies, such as CORBA/IIOP traffic. It also offers an extensible API for adding custom, protocol-specific filtering modules for unique networking environments.

Aventail has approached extranet management and security as a business problem, building on the notion that companies cannot survive as isolated islands. They need partnerships and easy access to information — the resource that is single-handedly controlling our economy. Aventail has replaced Internet hype and enabled real success stories of businesses connecting online. Through the use of industry standards, Aventail has developed a comprehensive extranet solution that offers unparalleled flexibility and ease of use for connecting key players in every industry, including financial services, healthcare, manufacturing, insurance, telecommunications, and automotive companies. With Aventail ExtraNet Center, the technology and capabilities are advanced, while the execution and management are simple. By enabling companies to build a highly secure, interactive extranet today that can grow with tomorrow's technologies, Aventail ExtraNet Center provides continuous, visible return.

Glossary

Access Control: the ability to determine who has access to what network resources, with the ability to deny service.

API: Application Programming Interface.

Authentication: verification of who is trying to gain access to a system.

CORBA: Common Object Request Broker Architecture; allows applications to communicate with one another no matter where they are located or who has designed them.

E-Business: business conducted online, which could consist of procurement, order processing, e-commerce, fulfillment, relationship management, etc.

E-Commerce: online financial transactions.

EDI: Electronic Data Interchange; supports procurement efficiencies and automates tasks, requires significant overhead, and the infrastructure is limiting.

Encryption: the manipulation of a packet's data in order to prevent anyone but the intended recipient from reading that data. There are many types, including DES, Triple DES, and RSA.

Extranet: the extension of resources from a corporation to its partners and other third-party users. When mission-critical resources are shared, security and management are essential.

Extranet Management and Security (EMS): the platform for providing encryption, authentication, access control, and policy management for extranets.

Firewall: a system that enforces a boundary between two or more networks.

IPSec: IP layer security protocol intended to secure LAN-to-LAN connections over the Internet with a public-key system.

Proxy Server: a software agent that acts on behalf of something or someone else; decides whether or not the user has permission to access a resource, then connects to a remote destination on behalf of the user.

Session Layer: The OSI layer of the networking hierarchy that provides means for dialogue control between end systems.

SOCKS: networking middleware that creates a secure, proxy data channel between two computers; SOCKS v5 adds strong authentication and encryption.

SSL: Secure Socket Layer; a standard for transmitting information securely over public networks. It is most often used to secure HTTP traffic but can also be extended to secure all IP-based traffic.

VPN: Virtual Private Network; generally an encrypted tunnel between LANs or remote employees and their corporate network.