Building a Comprehensive Extranet Infrastructure

Aventail

White Paper

www.aventail.com

Tel 206.215.1111
Fax 206.215.1120

808 Howell Street
Second Floor

Executive Summary

Recent advancements in Internet technologies now have us hurtling toward a global, networked, digital economy in which information rules, as do those who possess, share, and use it to its greatest advantage. Nowhere is the information advantage more clearly illustrated than in business-to-business communication. To remain competitive in today’s information-driven, partner-oriented marketplace, companies must be able to communicate and share mission-critical resources with anyone, anywhere, in real-time—easily and securely. Online business isn’t just about credit card transactions; it’s about using partnership to achieve competitive advantage.

Extending business-to-business access to non-employees is becoming an essential part of every competitive business model. Businesses cannot survive as isolated islands, but instead must merge their business practices and applications. The most visionary companies are now building extranets to move beyond the relatively narrow scope of transactions to include full-scale business processes and negotiations. According to Forrester Research, more than half of the Fortune 1000 currently use extranets, and those companies that delay extranet deployment could permanently lose market share to competitors. The message from leading analysts is clear: corporations that deploy extranets now will gain significant competitive advantage; those that hesitate will be left far behind.

This evolving competitive marketplace brings with it huge implications for IT managers, who must now set their sights on the world outside of their company’s firewall. Historically, IT managers have focused primarily on the internal needs of their company and its employees. But that insular focus is undergoing a radical shift, and over time IT professionals will serve an increasing number of strategic “outsiders”: customers, suppliers, business partners, consultants, contractors, and other third parties who need access to a company’s applications and resources.

As a result of this new competitive mandate, IT managers will hold increasingly strategic positions within a company. They’ll need to figure out how to seamlessly and securely extend their network to thousands or even millions of diverse users, leveraging their company’s already substantial IT investments to do so. That means they’ll need to choose their extranet solutions wisely. When vital, confidential information is involved, IT professionals can’t risk compromising any portion of the network. Likewise, when competitive advantage is at stake, they can’t risk deploying an inferior extranet.

These challenges can be successfully addressed with a comprehensive extranet infrastructure that incorporates best-of-breed extranet solutions and services. This white paper discusses the components of a comprehensive extranet, how they fit together, and how they allow IT managers to leverage existing IT resources to extend a company’s network outward.

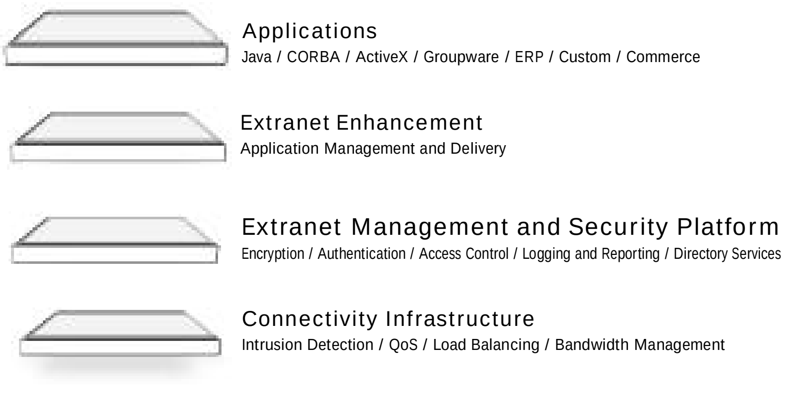
Extranet Overview

An extranet is a business-to-business network, based on Internet technology, that brings business partners together over public IP networks. At its very best, an extranet links not just companies to companies or networks to networks, but rather specific people to specific applications and data. 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 to access corporate networks from anywhere in the world, at any time. Extranets are reshaping internal processes, external relationships, and technical infrastructures—a transformation that's driven by the need to build relationships and satisfy a universal appetite for information and services.

Most companies come to the extranet table with an existing network and the infrastructure needed to operate it. The connectivity infrastructure varies from company to company and incorporates different technologies, protocols, and components that address such issues as intrusion detection, quality of service (QoS), load balancing, and bandwidth management. Companies also have specific applications that they want to extend to their partners, which might include legacy, ERP, and custom applications. An extranet based on open standards accommodates these organizational differences and needs.

Most large companies today have started to identify an extranet community, those third parties with whom they want to share specific applications, data, and services. They're faced with the challenge of developing a secure and manageable "open-door" policy with those diverse users, all of whom have different computing environments, requirements, needs, and permissions. Management and security are at the very heart of that "open-door" policy, and are the very foundation of any robust extranet solution.

To build a full-scale extranet, IT managers usually start by deploying a flexible management and security platform. That underlying platform should provide strong encryption, multi-factor user authentication, granular access control, logging and reporting, and directory services. Depending on a company's needs, policies, and goals, other components and solutions are then added to the management and security framework, such as application management and delivery. Some companies employ a professional services firm to help pull the many pieces of an extranet together. When best-of-breed solutions and services in each of these areas are successfully integrated, the end result is a secure, comprehensive extranet that solves business problems and provides unlimited opportunity.


Applications
Java / CORBA / ActiveX / Groupware / ERP / Custom / Commerce
Extranet Enhancement
Application Management and Delivery
Extranet Management and Security Platform
Encryption / Authentication / Access Control / Logging and Reporting / Directory Services
Connectivity Infrastructure
Intrusion Detection / QoS / Load Balancing / Bandwidth Management

As shown above, an extranet is built upon a company's existing physical network infrastructure. An underlying management and security platform is deployed and then enhanced with other solutions and services that all work together to perform specific functions. The most flexible and comprehensive extranets combine best-of-breed solutions and services in each of the areas shown.

Extranet Issues

Just as companies bring many different technologies and network infrastructures to the extranet table, they also bring a variety of issues and questions, including:

- *Flexibility—Will our extranet work in diverse computing environments, leverage existing investments, and accommodate emerging technologies?*
- *Security and control—How do we maintain control over our resources and make sure that confidential resources stay private?*
- *Performance—What kind of extranet performance and availability can we expect, given the varying reliability of public networks?*
- *Deployment and maintenance—How hard will it be to deploy and maintain an extranet?*
- *Partner politics—How will we negotiate the world of extranet politics?*
- *End-user experience—How will an extranet affect our targeted end users?*
- *Customer service—How do we give and receive the best customer service as it relates to our extranet?*

Each of these issues can be successfully addressed with a best-of-breed extranet.

Flexibility

Most corporate computing environments are heterogeneous. Organizational diversity can best be addressed by choosing a flexible extranet framework that complements, not replaces, existing network architectures and legacy systems, working seamlessly with multiple technologies, applications, operating systems, firewalls, protocols, and security methods and policies. The framework should also support a variety of authentication methods and encryption types. A flexible framework allows companies to build a common "bridge" between disparate partner networks.

Most companies have a huge investment in their IT resources and must be able to leverage those resources. To achieve the highest degree of interoperability and integration, the most effective extranets are based on an open architecture using industry standards. Aventail ExtraNet Center, for example, uses SOCKS v5 and SSL (Secure Sockets Layer) in its extranet management and security platform. SOCKS v5 is the IETF standard for authenticated firewall traversal and allows for the traversal of any type of firewall. SSL is the standard for transmitting private documents on the Internet and uses private keys to encrypt data and enable its secure transmission. By combining SOCKS v5 and SSL, Aventail ExtraNet Center gives corporations and their business partners the flexibility to choose those technologies that best meet their specific business, networking, and security requirements.

Companies use a wide variety of applications. A sophisticated extranet goes beyond HTTP to secure all IP-based applications, supporting:

- *legacy applications such as DB2 and CICS*
- *client/server applications such as ERP and PeopleSoft, as well as SAP and Manguistics (supply chain client/server applications)*
- *collaborative applications such as NetMeeting and Lotus Notes*
- *Internet applications such as RealAudio and SMTP*
- *emerging applications such as those based on Java, CORBA, ActiveX, and DCOM+*

With so many debates about standards now underway, it's hard to know exactly how things are going to shake out and which standards are going to emerge. Again, companies can address this issue by choosing an extranet that's based on open standards. That way, no matter which standards are adopted, the extranet will be able to accommodate them.

Security and control

Concerns about security and resource control—the worry that mission-critical resources will end up in the wrong hands—are among the biggest barriers to extranet implementation. Companies must know, unequivocally, that their connection over public IP networks is secure, that the person coming into their network really is who he or she claims to be, and that authenticated users are accessing only those resources and parts of a network they're supposed to access. A best-of-breed extranet management and security solution takes the worry away by giving companies the complete assurance that what's supposed to be private, stays private. It does so by tightly integrating strong multi-factor user authentication, strong encryption, and granular access control under one flexible management and security umbrella. The best-of-breed extranet management and security solution is discussed later in this white paper.

Performance

Extranet performance and availability are also at issue, given the unpredictable nature of public networks. As the Internet and other public networks mature, they'll become more reliable. In the meantime, an extranet infrastructure that incorporates intelligent load balancing and high availability solutions successfully addresses the issue of performance and availability, creating a reliable infrastructure that allows businesses to deliver the highest level of service to critical third-party users.

Deployment and maintenance

Building an extranet requires vision, planning, and expertise. Although designing an extranet can be a complex process, extranet deployment and maintenance are greatly simplified by choosing an extranet framework that leverages existing IT investments and interoperates with different platforms, protocols, and applications. A well-architected extranet will easily scale as needs grow and technologies emerge, with no hidden maintenance costs or huge new capital outlays.

Partner politics

Partner politics, while not to be underestimated, can be greatly diminished with the right extranet solution. Each extranet partner has its own policies, priorities, infrastructure, and ways of doing business. Because an extranet brings so many diverse entities together, the political challenges surrounding extranet deployment can be immense. Those political challenges can be minimized by choosing an extranet platform that works transparently with partner networks and applications, and doesn't require partners to change their security methods or firewalls. The more flexible an extranet solution, the greater the chance for outside participation because partners aren't being asked to make sacrifices or compromises in order to use the extranet. Providing a flexible extranet solution is one of the best ways to promote the idea that partners and customers are allies, not adversaries.

End-user experience

Companies are also concerned about impacts on the end users of the extranet, most of whom work for their partners and other strategic third parties. Because corporations don't own their partners' desktops, an extranet must be as non-intrusive as possible. Companies can best address this issue by deploying a best-of-breed extranet that has minimal impact on the end user, is easy to use, and runs transparently on the user's desktop without modifying existing drivers, transports, or applications.

HTTP-only extranets have the least impact on the end user and limit functionality to viewing information, performing simple queries against a database, and filling out forms online. An extranet that supports all IP-based applications allows companies to go beyond HTTP to leverage the power of legacy, custom, and ERP systems, while still having minimal impact on the end user. While an extranet that uses a browser as the client might seem like the most desirable way to go, the key is to choose an extranet architecture that supports Web-enabled, legacy, and emerging applications.

Customer service

Customer service is especially vital when mission-critical resources and business partnerships are at stake. Companies will receive the best customer service by choosing an extranet solution from an industry leader that's solely focused on providing superior customer service. Extranet-focused, customer-driven companies know the power of the extranet, and can best help their customers take full advantage of the opportunities an extranet brings.

By deploying a best-of-breed extranet, companies in turn are able to provide stellar customer service to their customers and partners, easily and securely sharing network resources and applications, and providing a quick and effective response to even the most complex customer or partner needs. That premium customer service fosters long-term relationships and engenders new business opportunities.

Aventail's Extranet Management and Security Platform

As mentioned earlier, companies that want to build a full-scale extranet usually start by deploying a flexible extranet management and security (EMS) platform to which other components are added. Aventail ExtraNet Center (AEC) is a best-of-breed EMS solution that provides the management, security, and application and network integration needed to build a sophisticated, easy-to-use extranet.

Technology

Aventail ExtraNet Center is a client/server infrastructure designed specifically for companies that need a fully operational extranet that can back-end seamlessly to existing systems. AEC is composed of Aventail ExtraNet Server, where security and user policies reside, and Aventail Connect, a zero-impact client that runs transparently on the user's desktop. As mentioned earlier, AEC combines SSL with SOCKS v5 to provide the highest level of interoperability and integration. AEC seamlessly integrates with disparate applications, network topologies, firewalls, operating systems, and security policies, allowing companies to leverage existing systems, accommodate future technologies and investments, and facilitate partnership. For more detailed technical information on Aventail ExtraNet Center, its architecture and components, visit http://www.aventail.com/index.phtml/products/whitepaperstech_aec.phtml.

Management and security features

Granular access control

Granular access control is critical to extranet management and security; it controls exactly what a user can do within a network based on who they are. Ultimately, access control is what distinguishes the level of security among EMS solutions. Aventail ExtraNet Center provides granular access control, allowing administrators to create pre-defined custom access rules based on source, destination, user, group, day, date range, and time. Administrators can limit access to one application, on one device, during a specific hour on a specific day, say between 8 and 9 a.m. every other Wednesday. AEC's access control is flexible enough that administrators can easily create role-based security policies "on the fly" for each individual.

Strong user-based authentication

Aventail ExtraNet Center allows administrators to identify a specific person and not just an IP address, and then confirm that that person really is who he or she claims to be. AEC supports a variety of authentication methods, including:

- *username/password*
- *digital certificates (such as GTE Interworking's CyberTrust solutions)*
- *token cards* (such as Security Dynamics' SecurID hardware tokens)
- *smart cards* (such as those offered by SPYRUS)
- *Challenge-Handshake Authentication Protocol* (CHAP)
- *Challenge-Response Authentication Method* (CRAM)

With Aventail ExtraNet Center, users authenticate just once per session. AEC constantly re-authenticates the user in the background, instead of simply associating a user with a source IP address after authentication (important because IP addresses can be spoofed). AEC also provides credential sharing, which means a user's identity and credentials can be passed to applications and systems sitting behind the extranet server. AEC directly integrates with the most popular back-end authentication systems, so administrators don't have to create a new user account for each person who needs access through the extranet server.

Strong encryption

Encryption is an integral element of user authentication and is the most effective way to ensure data security. Aventail ExtraNet Center uses SSL for data encryption, and allows for the use of other types of encryption as well. AEC provides 128-bit encryption and couples encryption strength with granular access control. It supports a wide variety of ciphers (DES, Triple DES, and RC4), hashes (MD4, MD5, and SHA-1), and key management approaches (RSA and Diffie-Hellman).

Filtering

Filtering is used for Internet policy management and is an important element in any security system. Aventail ExtraNet Center filters active content completely in order to prevent possible network break-ins. It allows the system administrator to block Java or ActiveX in a wholesale fashion, permit use of active content based on users and groups, and permit filtering on the basis of content type. Adminstrators can also prevent users from accessing specific IP addresses. AEC filters both inbound and outbound traffic.

Logging and reporting

For an additional level of security, network administrators must be able to monitor and log several layers of server activity and network traffic. Aventail ExtraNet Center allows this information to be easily imported into spreadsheets, databases, and reporting tools that are used to prepare detailed usage reports for managers and decision-makers.

Directory services

Directory services products are often used to enhance the Aventail ExtraNet Center management and security platform. Due to the explosion of distributed and Internet-based computing, companies are now experiencing a proliferation of application-specific directory services. Having different repositories, access protocols, and management interfaces for each directory is a very expensive maintenance and security proposition.

As extranets become more commonplace, so does the need for global directories that allow any application running on any computer platform to obtain directory objects such as public keys, digital certificates, and other authentication and policy information pertinent to extranet management. An increasingly common and effective strategy is to consolidate all directory offerings into a standards-based LDAP (Lightweight Directory Access Protocol) directory service. Network administrators can then create a single point of overall administration for directories, and quickly and easily change policy attributes and add or drop users without making any changes to the underlying hardware.

LDAP is expected to become the standard multi-vendor directory protocol that enables large-scale distributed extranets. In the extranet environment, where strategic partners and customers rarely are willing to commit to a single vendor for all network services, LDAP provides the freedom and flexibility to use various technologies. AEC (v3.1) simplifies user management by offering support for leading LDAP directories, including IBM's SecureWay Directory.

Management and Security Enhancements

Companies obviously have different needs, goals, and policies. By using Aventail ExtraNet Center as the under-lying EMS solution, companies can easily tailor their extranet to meet specific requirements by integrating enhancements such as intrusion detection and application management and delivery. The integration of other components is seamless because of AEC's flexible framework.

AEC Features Summary

- *Works in almost any IP environment and secures all TCP/IP traffic.*
- *Traverses any firewall and functions with multiple platforms and protocols (such as IPSec).*
- *Leverages legacy systems and supports emerging technologies.*
- *Supports the strongest authentication and encryption methods.*
- *Provides granular access control and allows administrators to easily create, modify, and enforce sophisticated security policies.*
- *Runs transparently on the user's desktop without modifying existing drivers, transports, or applications.*
- *Is highly scalable on both NT and UNIX platforms.*
- *Is designed to support and manage thousands of users simultaneously through single or multiple servers.*
- *Provides plug-and-play capabilities that include protocol filtering, content filtering, traffic monitoring, logging and reporting, and administration applications.*

Intrusion detection

Intrusion detection is a form of security technology designed to monitor, detect, diagnose, and respond to attacks on a network. Intrusion detection technologies are often used in conjunction with the EMS solution and its authentication, encryption, and access control mechanisms, providing regular feedback on network effectiveness and a real-time check of network status. Best-of-breed intrusion detection solutions enhance protection for any IP-based network. Internet Security Systems (ISS), for instance, provides an intrusion detection solution that integrates with Aventail ExtraNet Center and adds yet another layer of security by raising alarms or automatically shutting down suspicious network access.

Note: As mentioned earlier, security-conscious companies often use an intrusion detection solution as a standard component of their connectivity infrastructure.

Application management and delivery

Another EMS enhancement is application management and delivery, which refers to the ability to deliver applications and upgrades quickly and securely to customers, partners, and suppliers. Application management and delivery are among the biggest benefits of an extranet, easing a huge burden for network administrators who often must make applications available to thousands or even millions of users.

A best-of-breed application management and delivery solution performs personalized distribution; publishes any application; provides for multi-level management; and allows administrators to set up rules based on the specific needs of users, groups, or machines. Several companies provide solutions that help automate and secure application management and delivery in the extranet arena, including Marimba with its Castanet product suite.

Extranet Consulting and Services

So how does a corporation bring the many extranet pieces together into a whole that works? How does an organization know which solutions are right for its network and its extranet objectives? Some companies tackle those questions in-house, while others outsource.

Professional services firms

To shape and deploy their extranet strategies some companies turn to professional services firms, which help define business objectives, set an extranet deployment schedule, choose technologies, define a security policy, and estimate cost. Professional services firms evaluate a company's existing infrastructure, determining which systems need to be upgraded or replaced and how the networking, security, and application components of the extranet will mesh with the existing architecture. PricewaterhouseCoopers is one of a number of professional services firms that help clients achieve the greatest return on their extranet investment.

Application service providers (ASPs)

Web hosting and other types of outsourcing are nothing new. The next big variation on the outsourcing theme is application hosting. A number of firms (including ISPs), are now positioning themselves to be application service providers (ASPs), hoping to take advantage of a potentially lucrative opportunity to extend client/server, Web, and object-oriented applications to clients over the Internet.

ASPs give their clients the value of an application without the burdens and costs associated with ownership. They provide consulting services and essentially lease applications to their clients. The service is especially attractive to companies looking to deploy large ERP systems, which typically require significant infrastructure changes, a lengthy and complex evaluation cycle, and a specialized staff. ASPs are a relatively new phenomenon. In the future, some companies may choose to have an ASP host their extranet and extranet applications.

Case Study: Financial Services

One of the best ways to understand how the many components of an extranet come together is to look at a real-world scenario. The following case study represents an example of how a comprehensive extranet infrastructure can be built and used. Consider a leading financial services firm that needs to securely extend applications and services to independent brokers. By using an extranet as a secure conduit for information exchange, the firm is able to gain competitive advantage.

Profile

Based in New York, the large brokerage firm provides trade-clearing services for thousands of independent brokers who don't have their own clearing services. With transaction-based trade clearing, profits don't ride on the specific movement of a volatile securities market but rather on revenue from trading fees. Trading volume is critical to success.

Independent brokers depend on the brokerage firm for rapid, secure, immediate clearing services, which they then use to service their end clients. The brokers are always on the lookout for a clearing firm that can offer better, faster, more convenient services. Because it can take months or even years for clearing firms to become profitable, client retention is of utmost importance.

Extranet need

The brokerage firm needs an easy, secure, manageable way to extend resources to brokers, while still enforcing its stringent security policies. The independent brokers need access to the firm's trading applications, portfolio management applications, proprietary market research, and other services via a secure, transparent, cost-effective connection. They also need to stay connected to the firm over a strongly authenticated and encrypted session, without disconnecting from their critical real-time market research feeds. The brokers must be able to connect to the firm's extranet over the Internet through any ISP, or across a leased line or Frame Relay connection.

Extranet solution

To keep clients satisfied, increase trading volume, and improve trading quality, the brokerage firm replaced its manual trading process with an extranet. It used a best-of-breed extranet management and security (EMS) platform, and then integrated other best-of-breed components (given the open architecture of the EMS platform, each of the components was easily integrated.)

The EMS platform

The firm chose the only EMS platform that met its stringent requirements, including its need to:

- *enforce a truly comprehensive security policy.*
- *deliver security in a completely transparent way.*
- *connect securely across any firewall to any user.*
- *deliver services to diverse customers who use a variety of platforms.*
- *share any TCP/IP application with customers.*
- *support a variety of authentication methods and devices, including digital certificates, hardware tokens, and smart cards.*

Directory services

Because the firm has a number of trading and portfolio management applications, it decided to incorporate a directory services solution into the EMS platform. The firm chose to consolidate all directory offerings into a standards-based LDAP directory service, which means administrators can create a single point of overall administration for directories, and easily change policy attributes and add or drop users.

Intrusion detection

To add another layer of network security, the firm incorporated intrusion detection into its connectivity infrastructure. The intrusion detection component gives the firm enhanced networking protection by monitoring the network, identifying and responding to attacks, and providing a real-time check of network status.

Application management and delivery

The firm also needs to deliver applications and upgrades quickly and securely to brokers. It added an application management and delivery software solution to the EMS platform, greatly simplifying the delivery process for the firm's administrators and enhancing customer service.

Professional services

The brokerage firm hired a large professional services company to help chart an extranet strategy and pull the many extranet pieces together, streamlining planning and deployment and accomplishing the firm's extranet objectives.

Extranet success

By deploying a comprehensive extranet based on the best-of-breed EMS framework, the brokerage firm clearly gained competitive advantage. The firm has more than 30 servers set up, pushing secured, up-to-the-second trading information to thousands of brokers. It can extend more than 20 PowerBuilder and Java applications to brokers over the extranet, while enforcing its rigid security policies in a seamless and transparent fashion. As a result of this robust extranet functionality, the firm continues to reap huge benefits, including:

- *Increased client retention.* Brokers can easily and quickly get the information they need—there's no reason to jump to competitors or even consider such a move.
- *Increased transactions.* Brokers have secure, continuous access to the trading network—it's easier for them to trade securities through the brokerage firm, and the number of transactions continues to increase.
- *Increased quality of trades.* Brokers now enter orders at their office—the number of keystrokes per trade is dramatically reduced, and there's less chance for data entry error.
- *Increased revenue opportunities.* The brokerage firm can easily deploy new applications and services to its client base—the firm now has new revenue opportunities.

Companies in virtually every industry are using extranets similar to the one just described to conduct mission-critical business over public networks and achieve competitive advantage. For more examples, visit http://www.aventail.com/index.phtml/products/case_studies/index.phtml.

Summary

To achieve competitive advantage in today's networked world corporations must be able to extend their network and its resources to strategic partners, customers, suppliers, and a myriad of third parties. This business necessity brings with it a complex business challenge: how to best enable and manage secure information exchange over public IP networks while leveraging existing IT investments.

Companies must be able to overcome security threats and easily transfer real-world trust models to the virtual world, granting third parties access to internal resources with the click of a button without changing their infrastructure or compromising their security. To do that, companies need a complete extranet solution that is simple to deploy, integrates seamlessly into disparate computing environments and infrastructures, leverages existing network investments, and accommodates emerging technologies. By starting with a best-of-breed extranet management and security framework and adding other best-of-breed products and services to it, IT managers can build a comprehensive extranet infrastructure—optimized for growth—that works in even the most demanding network environments.

More information

For more information on the specific solutions mentioned in this white paper:

Aventail www.aventail.com

GTE www.gte.com

IBM www.ibm.com

Internet Security Systems www.iss.net

Marimba www.marimba.com

Security Dynamics www.securitydynamics.com

SPYRUS www.spyrus.com

For more information on technologies mentioned in this white paper, including SOCKS, SSL, IPSec, and LDAP, visit Aventail's Web site at http://www.aventail.com.