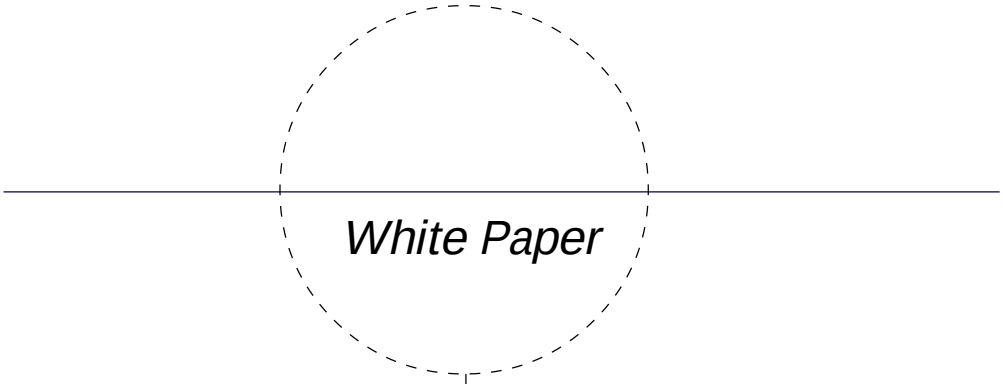
Aventail ExtraNet Center v3.3: A Technical Architecture



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

Table of Contents

Executive Summary

The extranet is where e-business begins. Extranets give companies the ability to manage relationships with business-critical partners and other strategic "outsiders," a capability that transforms collaboration into competitive advantage and allows companies to derive real value from their partnerships. Industry leaders realize the power of Internet-enabled partnership and are capitalizing on it by deploying strategic extranets to conduct business and share resources over IP-based networks.

Today's partnerships are increasingly conducted in "Internet time." Hesitation is opportunity lost. Enterprise IT departments must also move in Internet time, quickly and effectively adapting partner policy for a variety of dynamic user constituencies and extranet implementation types, from intimate supply chain partners using a wide spectrum of applications to mass e-commerce extranets driven by Web-based applications. And while extranet services must be deployed in a fast and flexible way, data owners must also be able to protect and keep total control over valuable internal resources, making sure that only authorized users can access the right resources and services. Enterprises must be able to deploy application services dynamically, while still maintaining the integrity of the perimeter.

What IT managers need in this fast-paced environment is a central place to manage and secure all extranet applications and services as they are deployed to partners. One place where the "rules of engagement" between data owners and outsiders can be centrally defined and enforced, on a technological level, for any TCP/IP application and for every strategic relationship. That "place" is Aventail ExtraNet Center v3.3. Since 1996, Aventail has provided best-of-breed extranet solutions for the management and security of business-to-business commerce and collaboration via the Internet. Aventail's tradition of delivering innovative, sophisticated, high-quality technology continues with Aventail ExtraNet Center v3.3. As discussed in this white paper, Aventail ExtraNet Center meets the extranet's specific technical mandates of privacy, authentication, data integrity, and centralized management, while giving companies the flexibility to quickly respond to immediate business opportunities.

Aventail ExtraNet Center v3.3

Available in early 2000, Aventail ExtraNet Center v3.3 provides both clientless HTTP and agent-enabled TCP/IP extranet functionality in one total solution. This robust functionality allows companies to easily and effectively define and manage business-to-business commerce and collaboration with disparate partners, regardless of network and security infrastructures, platforms, application types, authentication methods, or other variables found in today's heterogeneous enterprise environments. Aventail is the only company that combines browser-only and agent-enabled extranet modules in one solution to support any application deployed as part of an extranet, bridging the investment in the legacy infrastructure with the opportunity of the Web.

Scalability

Aventail ExtraNet Center uses an open architecture and industry standards (including SOCKS v5, the IETF standard for authenticated firewall traversal, and SSL) to provide the highest degree of interoperability and scalability. Because extranets often grow rapidly, scalability is critical—both incremental and exponential. Aventail ExtraNet Center is designed to support and manage thousands of users simultaneously through single or multiple servers, and scale to accommodate future technologies and investments. Aventail ExtraNet Center:

- seamlessly integrates with disparate network topologies, firewalls, and operating systems, giving companies the flexibility to leverage existing infrastructures.

- has a drop-in architecture that makes it ready for immediate implementation. Organizations can deploy an extranet quickly, without having to roll out a new infrastructure or re-architect their applications.
- allows companies to give partners a rich set of TCP/IP resources without requiring modifications to their firewalls and infrastructures, helping to minimize partner politics and speed deployment.
- allows companies to leverage strategic IT investments. Corporate IT departments have huge investments in LDAP directories, PKIs, and Web applications, as well as generations of investment in legacy applications. Aventail ExtraNet Center leverages these investments for maximum business benefit.

Security

IT managers have a "due diligence" responsibility to manage and secure enterprise resources. Aventail is committed to protecting the interests of data owners through standards-based security. Aventail ExtraNet Center's management and security platform provides strong encryption, multi-factor user authentication, and granular access control. Aventail ExtraNet Center:

- uses SSL to provide privacy through encryption for all TCP/IP applications. SSL is internationally recognized as the most mature and market-tested encryption framework available.
- implements standard, mature ciphers such as DES, Triple DES, and RC4.
- supports leading authentication methods and most user databases and directories, including LDAP.
- supports PKI and smart card-enabled environments.
- provides a plain-language policy for deciding how, when, and what resources are accessed by partners. Only authorized users, not entire organizations of outsiders, have access to internal resources.

Management and integration

To capitalize on the enormous opportunity that an extranet provides, more than security is required. Enterprise administrators must have one central place to manage resources that are extended to partners, customers, suppliers, employees, and other key constituents. Because each resource has its own rules and each user has his or her own set of permissions, administrators need an easy way to centrally administer policy and access control decisions. Without that capability, management quickly becomes a nightmare as the user base grows and becomes more externalized. Aventail ExtraNet Center provides the management and integration needed to service a large, heterogeneous, global group of users. It does so by providing:

- dynamic proxy-based security
- outside access to the intranet without a DMZ
- complete application integration
- wide-scale authentication support and integration
- wide-scale directory support
- public key certificate support
- data gathering for data mining

Proxy-based security

Aventail ExtraNet Center relies on a proxy-based model for managing and securing all applications communication. There is never a direct connection between an outside user and an internal resource; all information is brokered by a proxy. With Aventail ExtraNet Center's client/server components, Connect and ExtraNet Server, all traffic is proxied through a SOCKS v5 server with one firewall rule

change to accommodate all application communication. Because Aventail ExtraNet Center uses a session-level proxy architecture, it inherently supports Network Address Translation (NAT), which means that the IP address space of any corporate network is hidden from the outside. SOCKS provides a common authorization layer across any TCP/IP application.

With Aventail ExtraNet Center's browser-only component, ExtraWeb Server, all HTTP traffic is sent to a reverse proxy where authorization rules are then applied. This means that data does not need to be replicated into a DMZ outside of the firewall. Proxied communication can be allowed to one location, ExtraWeb Server, which brokers all communication with downstream servers. The DMZ is managed and no direct internal connections are allowed.

Outside access to the intranet without a DMZ

Some extranet partners need access to HTTP content, but that content is distributed across potentially hundreds of intranet servers. Aventail ExtraNet Center accommodates these environments by providing browser-only access, in which the browser functions as the agent and the only requirement is a browser that supports SSL and forms (Internet Explorer v3.0+ and Netscape v3.0+). All access to servers is managed and authorized through ExtraWeb Server. Unlike other models, Aventail ExtraNet Center easily integrates into the existing infrastructure and does not require plug-ins, cookies, or configuration changes to any application server or browser (see Figure 1).

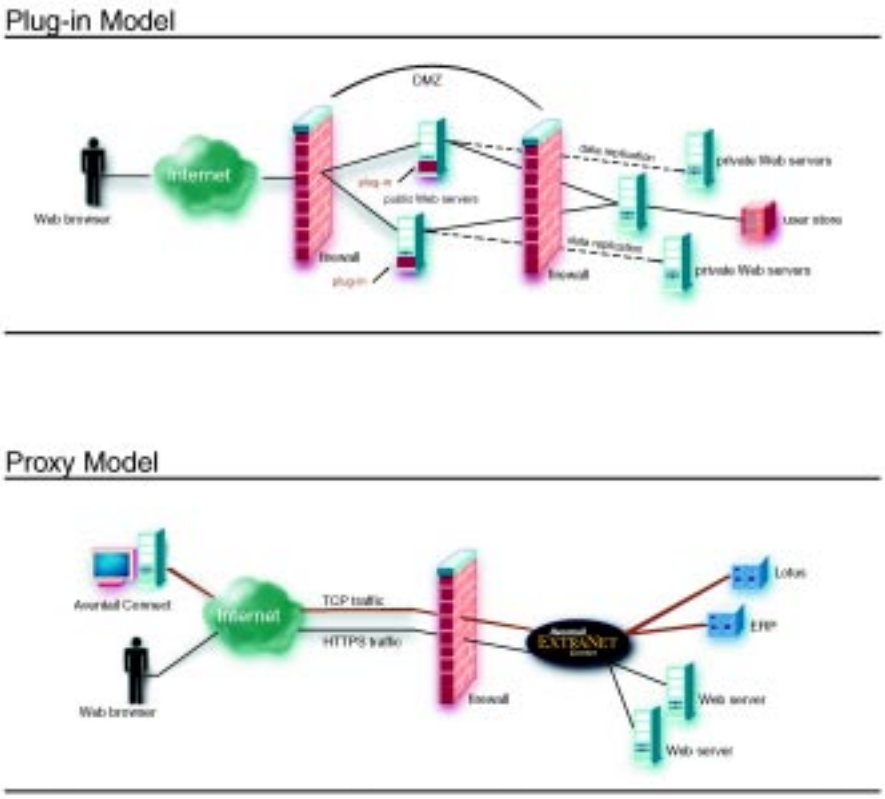


Figure 1. Proxy vs. Plug-in Model. *With Aventail's proxy-based model there is never a direct connection between an outside user and an internal resource. No plug-ins or cookies are required, nor modifications to any application server or browser.*

Application integration

Aventail ExtraNet Center provides management and security for any TCP/IP application. It is designed to meet the core business and technological requirements of the market-driven extranet, creating a bridge between the legacy application environment of the corporate network and the reach of the Internet and its core protocols. Aventail ExtraNet Center immediately brings both legacy and Web-developed applications to the extranet by providing agent-enabled support for TCP/IP, and browser-based access for HTTP.

Authentication support and integration

The diverse populations of the extranet require a wide variety of authentication types, from the most basic to the most secure. Aventail ExtraNet Center supports leading standard authentication types such as Username/Password, CHAP, CRAM, token cards, smart cards, digital certificates, and S/Key. Aventail ExtraNet Center directly integrates with leading back-end authentication systems including LDAP directories, Windows NT Domains, UNIX Password Files, Novell NetWare Directory Services (NDS) and Bindery, and any RADIUS-compliant database. Using the Connect agent, Aventail ExtraNet Center also provides support for Novell Directory Services and Security Dynamics' ACE/Server. Web-based users of Security Dynamics' SecureID token cards can be accommodated via the RADIUS interface.

Directory support

LDAP is quickly becoming the industry-standard authoritative directory for storing user and network element information. Aventail ExtraNet Center supports leading LDAP directories, allowing companies to capitalize on their strategic investments in directories. Administrators can inherit groups defined in LDAP-enabled directories, including those offered by Netscape, IBM, and Novell. Digital certificate or password-based authentication can then be verified against an LDAP repository.

Public key certificate support

Aventail ExtraNet Center supports but does not require PKI for authentication and security. It is full PKI-enabled, supporting X.509 certificates and RSA PKCS standards encompassing a wide range of digital certificate support—from basic algorithms, to support for certificate-enabled smart cards from DataKey and SPYRUS and Universal Serial Bus tokens from Rainbow.

Aventail ExtraNet Center supports the following RSA PKCS standards:

- **PKCS #1—RSA Encryption Standard.** Encrypts data using the Rivest-Shamir-Adelman (RSA) algorithm construction.
- **PKCS #3—Diffie-Hellman Key Agreement Standard.** Describes a mutually shared secret key between parties (the Diffie-Hellman Standard).
- **PKCS #5—Password-Based Cryptography Standard.** Describes methods for performing password-based cryptography.
- **PKCS #7—Cryptographic Message Syntax Standard.** Specifies message encryption constructions for mail (S/MIME) and bank and credit card payments.
- **PKCS #8—Private-Key Information Syntax Standard.** Demonstrates the attributes of private keys in establishing trust between CAs and users of public key/private key communications.
- **PKCS #10—Certification Request Syntax Standard.** Provides the parameters for certification requests and how those requests can be transmitted to certifying authorities. PKCS #10 also addresses certificate revocation.
- **PKCS #11—Cryptographic Token Interface Standard.** Specifies an API to smart cards and other devices.

- **PKCS #12—Personal Information Exchange Syntax Standard.** Describes the format that popular Web browsers use to export certificates.

Aventail is committed to supporting leading PKI standards ahead of the market. Each new version of Aventail ExtraNet Center will continue to raise the bar for PKI support.

Data gathering for data mining

Aventail ExtraNet Center provides common data gathering for data mining across diverse applications. In a complex application environment it is often hard to evaluate which resources are most valuable to extranet partners for designing systems and analyzing commercial efforts, or for billing and charge-back. With Aventail ExtraNet Center, all application access and activity is centrally logged and can be output to a flat file or to WebTrends for analysis. More formats will be added in the future.

Specific Components

Aventail ExtraNet Center v3.3 provides management and security for Web-based applications accessed through a standard browser, and for client/server applications accessed through an agent. Aventail ExtraNet Center is one solution with several components. Its modular design gives companies the flexibility to choose the components that best fit their technical requirements and the business opportunity at hand. The components are:

- **Connect and ExtraNet Server—** client/server components that provide support for all IP-based applications, including Java-or ActiveX-based applications.
- **ExtraWeb Server—**HTTP reverse proxy server that uses a standard Web browser for a client and provides support for HTTP content only.
- **Aventail Policy Console—**graphical management tool used to manage extranet servers, users, and resources.
- **Aventail Management Server—**optional service for remote management.
- **Customizer—**wizard-based tool for agent software deployment and customization.
- **Secure Extranet Explorer—**application for extranet file browsing.

As shown in Figure 2, Aventail's technology can be described along three different service layers: Management Services, Core Services, and Agents. Each layer is responsible for a different aspect of the extranet.

Management Services

Aventail Policy Console

Aventail Policy Console is the graphical administrative tool used for creating, viewing, managing, and changing

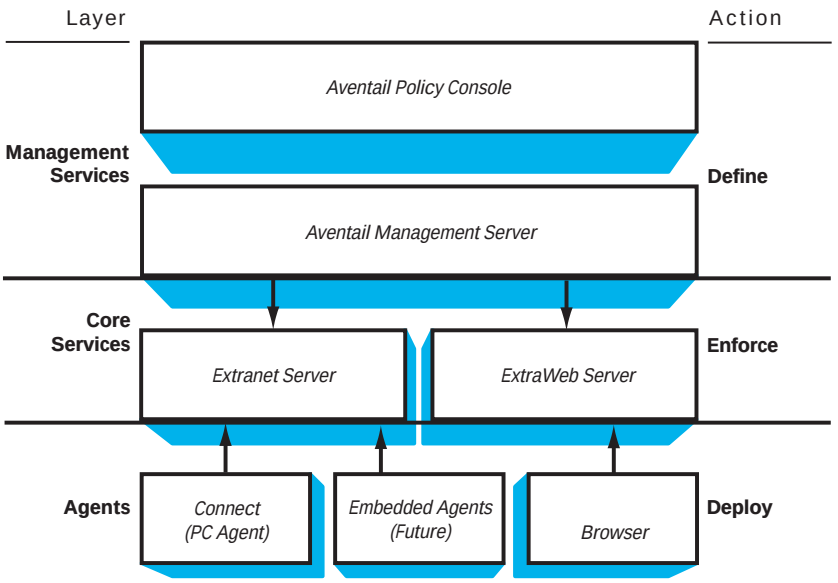


Figure 2. The Aventail ExtraNet Center Solution Architecture: Layers of Service

extranet policies. It can also be used for starting and stopping extranet servers and viewing log and license files. This intuitive tool gives administrators a plain-language policy that defines all application access privileges for partners. In Aventail ExtraNet Center v3.3, ExtraWeb and ExtraNet Servers are both managed through the same Aventail Policy Console interface; administrators simply switch modes to manage each server (including the optional Aventail Management Server). This capability simplifies and strengthens user and resource management by giving administrators an easy way to centrally administer policy and access control decisions.

Aventail Policy Console allows multiple extranet servers to be monitored and administered from a central interface, locally or remotely, via an encrypted connection. When being run remotely, Aventail Policy Console establishes a secure LAN, WAN, or Internet connection to Aventail Management Server via an SSL connection over port 2080 (by default). Aventail Policy Console runs on both Windows NT and UNIX platforms and supports cross-platform management.

Aventail Management Server

Aventail Management Server is an optional service that allows administrators to remotely manage ExtraNet and ExtraWeb Servers through Aventail Policy Console. Again, Aventail Management Server allows remote management of ExtraWeb and ExtraNet Servers through a secure connection to an outbound/inbound port. This guarantees the same even administrative experience on any supported platform, anywhere in the world.

Core Services

ExtraNet Server

ExtraNet Server is a core service of Aventail ExtraNet Center and provides the proxy-based management of TCP/IP applications. ExtraNet Server is a SOCKS v5 proxy that manages the authentication of users and processes all connection requests, managing both incoming and outgoing network traffic. It contains an SSL module for the authentication and encryption of all TCP/IP traffic. ExtraNet Server is managed using Aventail Policy Console and runs on all platforms, including:

- Windows NT
- Solaris
- Linux (libc6 for RedHat Linux 5.x and libc5 for other distributions)
- AIX
- HP/UX

ExtraWeb Server

ExtraWeb Server is also a core service of Aventail ExtraNet Center v3.3 and provides browser-only access to internal Web resources. ExtraWeb Server is an enhanced reverse proxy for Web traffic that manages all user authentication and encryption based upon SSL. Users can access a diverse range of Web resources with just a browser; client software is not used and the only client requirement is a browser that supports SSL v3.0 and forms. ExtraWeb Server is standards-based and requires no proprietary applets or Web server plug-ins. Technical advantages specific to ExtraWeb Server include:

Automatic Web resource discovery

ExtraWeb Server “crawls” an enterprise’s Web servers, automatically discovering Web resources and creating a directory tree. The Web servers and their corresponding URL pages and directories can then be easily selected to develop policy, making it extremely easy for administrators to create policies.

Authorization down to the Web element

ExtraWeb Server allows Web resources to be controlled down to the Web object (such as GIF, JPEG, and any URL-definable object). The extranet user is given a defined, authorized view of the extranet as defined by the administrator. All intranet sites accessed by extranet

partners can be clearly and centrally managed down to the directory or URL using the following parameters:

- source—host, domain, range, subnet
- destination URL—from a Web server down to a specific page
- user/group—NT , NDS, UNIX, LDAP, SSL, RADIUS
- time/date—ranges or shifts
- key length—40-bit or higher, 56-bit or higher, or 128-bit

This granular access control lets data owners protect and maintain total control over valuable internal Web resources, ensuring that only authorized users have access to the right resources.

Automatic URL aliasing and translation

With ExtraWeb Server, all URLs accessed by a partner are defined via an alias that is determined by the server administrator. Unless the policy dictates otherwise, the partner is never shown the actual internal URL. This functionality provides greater convenience to the partner—who sees a simplified URL—and greater security to the organization. All links in pages served by ExtraWeb Server are automatically translated to the aliased URLs, which means that no absolute- vs.-relative link requirements are needed, and cross-server links are supported.

Effective DMZ management

As mentioned earlier, ExtraWeb Server does not allow a direct connection to any Web server. All HTTP traffic is sent to a reverse proxy where authorization rules are then applied, so data does not need to be replicated into a DMZ outside of the firewall. And because ExtraWeb Server provides proxied, protected access to Web servers without costly replication, the size of the DMZ is greatly limited and its management is greatly simplified. More importantly, this capability means that because the Web server is not modified or adapted, it does not need to be "owned" or deployed centrally to allow centralized extranet access.

Basic authentication forwarding

If a Web server generates non-personalized content for which no internal authentication is required, users only need to log on to ExtraWeb Server once to gain access to protected Web servers that they're allowed to access. For Web servers that dynamically build personalized pages based on the user's credentials, ExtraWeb Server provides an Authentication Forwarding feature. With this feature administrators can forward user credentials in the HTTP header to selected Web servers, allowing servers that use basic authentication (Username/Password) to provide customized content for users without having to prompt them for additional authentication.

Agents

Connect

Connect is a secure agent that works in conjunction with ExtraNet Server to secure both outbound and inbound traffic from 16- and 32-bit Windows applications. It runs transparently on the end user's desktop and supports all IP-based applications, requiring no contact with the end user beyond authentication.

Connect redirects only TCP/IP application calls bound for the extranet, allowing the user to continue to use local network or VPN resources. It supports both Winsock 1.1 and WinSock 2.0, where it is deployed as a Microsoft Layered Service Provider. The Connect agent deploys as a self-extracting executable and allows a company's non-technical users to access all authorized extranet content—from Web applications to legacy client/server applications—by clicking on the business application itself. Connect runs on:

- Windows 95
- Windows 98

- Windows for Workgroups 3.11
- Windows 3.1
- Windows NT 3.51 and 4.0

Customizer

Aventail ExtraNet Center includes Customizer, a wizard-based tool that simplifies the deployment and installation of Connect for large numbers of users. Administrators can use Customizer to preconfigure custom self-installing executables that require minimal action on the part of the end user.

Secure Extranet Explorer

Aventail ExtraNet Center includes an extranet file-browsing application called Secure Extranet Explorer (SEE), which is displayed as Extranet Neighborhood on Windows desktops. Styled after Windows' drag-and-drop Network Neighborhood, SEE allows Connect to share files with other members of a networked extranet. It enhances security by presenting a resource view that is determined by the extranet policy, so users see only those resources that they have permission to access. Extranet Neighborhood allows users to browse, open, copy, move, and delete files from remote computers via the Connect extranet connection. Users simply double-click on the Extranet Neighborhood icon to navigate through domains, hosts, and folders. SEE is a client-side implementation of SMB (Server Message Block protocol).

How It Works

Aventail ExtraNet Center gives technology managers one central place to securely deploy services to partners via extranets. ExtraNet and ExtraWeb Servers can be managed remotely via Aventail Management Server; administrators can switch modes on Aventail Policy Console to manage all three servers locally or remotely.

Administrators use Aventail ExtraNet Center's components in concert to solve their needs (see Figure 3). They might first grant users access to specific internal Web content by modifying a rule on ExtraWeb Server. Later, when some or all of those users also need access to legacy applications, the administrator can deploy the Connect agent and modify a rule on ExtraNet Server. The result is flexible, secure extranet management for large enterprises.

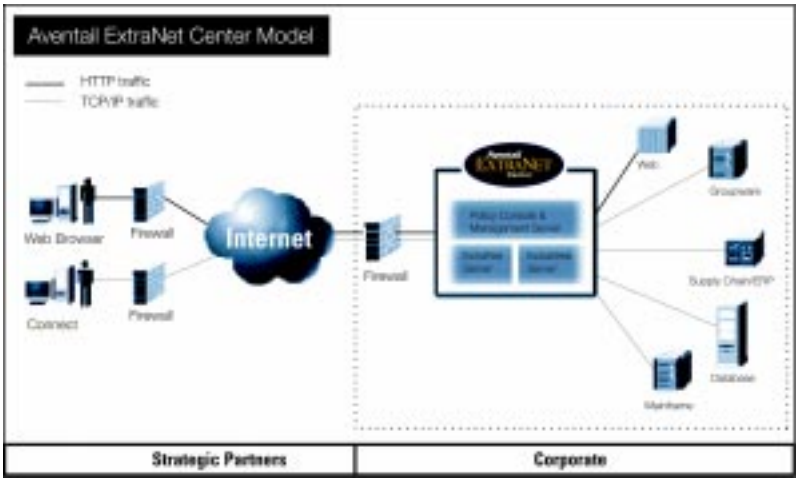


Figure 3. Aventail ExtraNet Center Components. *Corporations can use Connect and ExtraNet Server to leverage the power of legacy, custom, ERP, and emerging applications, and an SSL-enabled browser and ExtraWeb Server to provide access to HTTP content.*

Connect and ExtraNet Server

Connect resides transparently on end users' desktops or laptops. ExtraNet Server typically sits behind any firewall, router, or proxy server near the perimeter of the corporate network. Connect and ExtraNet Server work as follows:

1. As the user's workstation boots, Connect launches automatically in the background. It is usually added to the Start-Up directory.
2. The user selects a network application that initiates a connection to the corporation's network.
3. Connect intercepts this request and redirects it to ExtraNet Server. If the request is for a "non-secure" application or resource, it is ignored and passed on to the TCP/IP stack, allowing it to proceed normally.
4. Based on the source of the request, ExtraNet Server specifies the required authentication method, establishes a secure connection, and prompts the user for his or her credentials. An encrypted tunnel between Connect (on the user's computer) and ExtraNet Center is set up.
5. The user sends his or her authentication credentials (such as Username/Password, token passcode, digital certificate) via an encrypted channel, and ExtraNet Server verifies the validity of the user's credentials.
6. Based on a set of access parameters defined by an administrator, Aventail ExtraNet Center either allows or denies access to the desired resource. The corporation's administrator has the option to apply application-specific filters to a given user or connection, which provides additional application-specific policy enforcement.
7. Once properly identified, the user proceeds, with Aventail ExtraNet Center proxying all connections to secured resources.

Network applications that do not require secure connections are not affected by the Connect agent.

ExtraWeb Server

ExtraWeb Server typically sits behind a firewall at the network perimeter and provides security and central management for internal Web resources. ExtraWeb Server works as follows:

1. The user requests a resource by entering a URL or following a link.
2. The browser establishes an SSL session with ExtraWeb Server and requests a page.
3. ExtraWeb Server receives the request, and then determines which method the client should use to authenticate for that particular resource.
4. ExtraWeb Server then prompts the user for credentials (unless the user has already successfully authenticated), and verifies those credentials against the appropriate user store (they're sent as a form).
5. Once the user successfully authenticates, ExtraWeb Server then reviews the access control rules to determine if the user is allowed to access the resource.
6. If access permission is granted, ExtraWeb Server converts the request from public to private URL form, and then retrieves the Web page for the user.
7. ExtraWeb Server parses the page and translates all internal links to their proper alias.
8. The page is cached in its public state and all transactions are logged in detail.

How It's Used

Aventail ExtraNet Center v3.3 gives companies in all industries the technical agility they need to manage,

secure, and track the flow of applications and data to outside partners. Consider the following real-world scenarios.

Aerospace

A leading global aerospace firm has a wide set of supply chain and service partners. It also has a long-standing set of legacy applications, some of which are Web-enabled. The company wants to create a browser-based extranet to share project-tracking information with supply chain partners. It also wants to bring key legacy applications directly to a select set of outsourcing partners. Ideally, the company would also like to manage each of these diverse extranets under the same policy umbrella. Aventail ExtraNet Center meets the company's objectives, providing the only comprehensive management and security solution available that supports Web-based and legacy extranets simultaneously under one policy console.

Pharmaceutical

In the pharmaceutical industry, partners are often competitors. It's common for a large firm to release a patent on a drug and for a competitor to find a new use for the drug or develop a valuable byproduct. The competitor then patents that new use or byproduct, forcing the drug's original developer into a partnership. Aventail ExtraNet Center protects the interests of data owners and the integrity of data in scenarios in which extranet partners are also fierce competitors. Plain-language policy can be generated from Aventail Policy Console to give board members definitive information regarding which partners can access which resources. No changes to firewall policies are required, which means competitors have limited contact with one another. No routing is possible through Aventail ExtraNet Center between the two partners. Aventail ExtraNet Center allows for fast deployment, as well as quick rules changes when the partnership ends, giving pharmaceutical companies the flexibility they need to take control of their partnerships and resources.

Manufacturing

A large manufacturer wants to outsource all component manufacturing and needs an interactive, intimate extranet relationship for product co-development—one that provides rich application access for CAD sharing and whiteboarding, and allows for dynamic interaction with robust enterprise applications. Aventail ExtraNet Center meets the company's needs, allowing suppliers to securely connect to supply-chain management, ERP, Messaging, NetMeeting, and CAD applications over the Internet. Engineers can discuss design changes with component manufacturers during a secure Internet meeting, and then securely access and download new designs to immediately implement changes. If some users also require access to specific internal Web content, administrators can grant that access simply by modifying a rule on ExtraWeb Server. With Aventail ExtraNet Center's centralized logging and reporting capabilities, the host company can easily track and measure extranet use and success, and develop reliable metrics for management. The company can ultimately reduce cash-to-cash cycle time, have faster time-to-market, and improve component quality.

These are just a few examples of how Aventail ExtraNet Center can be used to help companies achieve their extranet management, security, and business objectives. For more case studies, see http://www.aventail.com/products/case_studies/index.phtml.

Summary

The extranet presents a unique business opportunity and a well-differentiated set of technology needs. Companies can use extranets to build more effective partner networks, deepen their relationships with customers, and increase revenue. But to realize those benefits they must be able to quickly provide extranet services to a vast number of diverse user constituencies, over a wide variety of extranet

implementation types, while maintaining complete control over their resources. Not an easy proposition, given the fact that user constituencies are constantly changing as mergers and acquisitions increase and organizations become more reliant on outside consultants and outsourcers.

What technology managers need is one central place from which to easily and effectively deploy, secure, and manage all extranet applications and services to partners. Aventail ExtraNet Center v3.3 is that place. Aventail ExtraNet Center provides both HTTP and TCP/IP extranet functionality in one solution, allowing enterprises to manage and secure every strategic relationship, no matter how diverse the user constituencies, computing environments, and applications. Aventail balances the intense "dot com" pressure of e-business with the never-ending need to protect data ownership. Finding this balance is where e-business begins.

More Information

For more information about Aventail and the technologies mentioned throughout this white paper, visit Aventail's Web site at www.aventail.com.

© 1996–1999 Aventail Corporation. All rights reserved. Printed in the USA. Aventail is a registered trademark of Aventail Corporation. Aventail ExtraNet Center, Aventail.Net, and Aventail Connect are trademarks of Aventail Corporation. Other product names mentioned may be trademarks or registered trademarks of their respective companies.