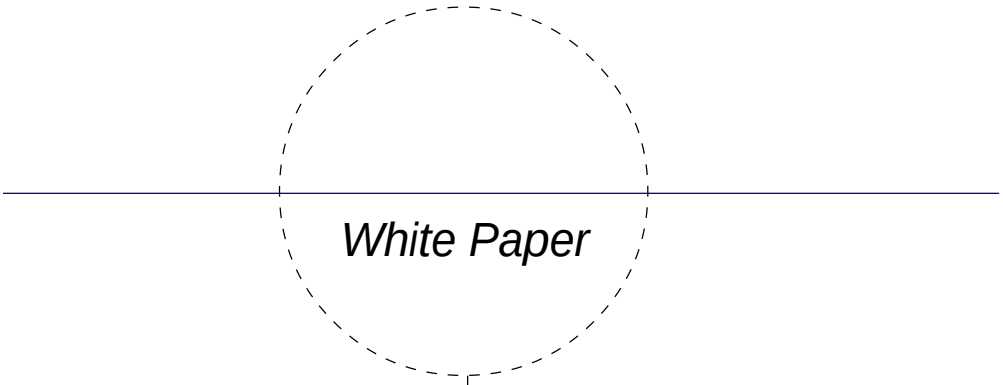
# Developing an Enterprise Extranet Service


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

## *Executive Summary*

A variety of market research firms, including International Data Corporation, Forrester Research, and Gartner Group, predict that extranets—third-party connectivity from outside the enterprise—will increase dramatically in the years ahead. The reason behind this growth is simple: lines of business in the enterprise increasingly want to collaborate with elements of the supply and demand chains, and they want to use the Internet as a means of transport. This demand for partner connectivity has companies focused on building effective extranets. In some cases, companies will react to demand from lines of business by "Web-enabling" a core application and calling it an extranet. While this approach may fulfill immediate needs, it fails to address the strategic issue of managing the flood of extranet demand. To address the issue at a strategic level, the IT organization must establish an extranet service.

The typical IT organization offers a suite of services to its business unit customers, which deliver relatively common technologies such as e-mail, directory services, LAN/WAN connectivity, and PC support. These services have a degree of maturity fitting their widespread use in the enterprise. There are policies, procedures, systems, and architectures that allow the IT organization to deliver these services to the business, accommodate new requests, and share costs. Going forward, extranet connectivity will be in such great demand that IT departments must bring these service aspects together to create the enterprise extranet service. Such a service would incorporate:

- user and security policies
- cost sharing
- robust architecture
- service level agreements
- support for a wide continuum of applications
- a focus on enhancing business relationships

This white paper outlines a process for developing an enterprise extranet service.

### Business Needs, Relationships, and Applications

To begin the creation of the extranet service, first consider the business the company is in today and the new businesses that may be started in the future. Now consider the business relationships that drive and enhance the company's efforts. Also consider the new relationships that will help the company, such as new markets, sales and distribution channels, and suppliers. By creating a list of these relationships, a constituent inventory is drawn.

Based on the constituent inventory, you can form an application inventory. The application inventory should include all current and future applications that are used by both internal users and business partners. An application that adds value internally can add value to a partner relationship. Therefore, the extranet service needs to support the entire spectrum of possible applications, regardless of whether the applications are Web-enabled. More than likely the application inventory will include legacy applications, Internet applications, and potentially Java or even ActiveX applications.

### Policies and Processes

Having identified the applications that the lines of business might want to share, the next step is to consider policies, processes, and service levels for the extranet service. Extranet policies can be divided into three categories:

- security policies
- user policies
- general use policies

### *Security policies*

The security policies should be developed by personnel with strong security knowledge and knowledge of the corporate business objectives. Central to the policies should be the concept of expanding and strengthening existing business relationships and creating new ones through the use of the extranet. The goal should be a set of policies that is established and enforced based on discrete business relationships, not a set of wholesale rules that apply to all traffic from the Internet. This means that third-party agents use appropriate authentication, their data is encrypted, and they only access systems and information that are relevant to their relationship as an agent. The trust model should be user-based, not wholesale and not network-based. In the extranet context, security technologies such as authentication and encryption are offensive weapons that allow the business to do something new. This notion is a break from tradition for many companies. Security policies must reflect the business objectives and relationships and be oriented around enabling the business.

### *User policies*

User policies should also be centered around enhancing or expanding business relationships, and should clearly delineate the sharing of responsibility between IT and the lines of business. The concept of sponsorship should be central to the user policies. For example, the distribution and logistics department might sponsor a group of users from third-party distributors who are accessing systems over the extranet. Sales or marketing might sponsor customers, agents, and brokers. The sponsorship role is important because it establishes responsibility within the business for the partners using the extranet. It also gives the IT department a resource to turn to as a liaison to the external user community.

### *General use policies*

General use policies will likely be a permutation of the enterprise Internet usage policy and should set the basic ground rules for the extranet. Crisp verbiage will bring clarity to the policy: "The corporate extranet is solely for the use of established business partners and customers. All users must be sponsored by a business unit of the company." The policies should also establish clear divisions between IT and line of business (LOB) responsibilities. For example, the IT department may be responsible for maintaining privacy of data as it traverses the Internet, and authenticating users on the extranet and restricting them to specific applications; the LOB may be responsible for the activities of the users once they reach the actual applications on the extranet. The general use policies should also establish the cost-sharing policy. If the extranet service works on a charge-back basis, that should be clearly stated.

### *Processes*

With the policies in place, processes can be established for the extranet. The processes should cover the establishment of new users, the introduction of new applications (including risk assessment and application audit), the distribution of credentials to identify users, and the revocation of those credentials. These processes should ultimately streamline the expansion of the extranet service and set clear expectations among LOB sponsors and end users. The processes should set reasonable expectations for response to requests, and outline the steps for adding and removing new users and applications. The processes should be documented and distributed proactively to the business.

## Architecture

With applications identified and policies and processes in place, an architecture can be established. The architecture should be designed to facilitate any reasonable user request that might be made. Put another way, it should allow the secure sharing of any and all applications that have been identified in the application inventory—including fat client and legacy applications. The architec-

ture should incorporate the various technologies required by the security policy as well, especially directory services and authentication technologies.

Since the extranet service will be in high demand, the architecture should have a high degree of redundancy and fault tolerance built into it. In most cases this will mean not only dedicated Internet connections, but redundant connections from multiple ISPs to avoid the service going down due to an ISP failure. Load balancing technologies should be factored in for high-use application servers and security servers. Security enforcement should be incorporated at the perimeter and layered to include application-level security as well. Some organizations isolate extranet applications to their own subnet. Others enforce granular access control that allows extranet users to access the same systems that internal users do. Regardless of how the application servers are layered or segregated, enforcement should be done by an Extranet Management and Security (EMS) system that can secure any of the applications on the application inventory and can enforce a security policy based on business relationships. The EMS system should also be able to provide audit information as necessary and have reporting capabilities that service the charge-back and usage policies.

Substantial consideration should be given to the authentication methods used on the extranet in both the policies and architecture phases. Generally speaking, extranet security is as strong as the combination of authentication and access control used, relative to the information shared. Some EMS systems, including Aventail ExtraNet Center, allow modulation of the authentication method used based on the systems that are being targeted and other factors. This kind of flexibility lets you use different authentication methods depending on the user and the systems being accessed. There may be distinct advantages to this, such as allowing access to less valuable information via password authentication while protecting more sensitive data and applications with certificates or tokens. This kind of flexibility lets the extranet service strike a balance between security, user friendliness, and cost when bringing a new application or partner online.

The architecture should allow the company to divorce itself from a number of thorny extranet challenges. Foremost among these is firewall traversal. Your business partners will have a variety of firewalls. If your EMS solution or applications do not respect the fact that there are disparate firewall brands in use by your partners, and that your partners do not particularly like to have to reconfigure them, your service may have additional deployment obstacles that hamper its success. IP address issues also need to be avoided. For example, your partners should never have to have routable IP addresses relative to your own, should be able to use Network Address Translation (NAT), and ought to be able to use whatever addressing scheme they choose. To avoid problems associated with IP addresses, avoid using VPN technologies that run at the Network or Transport layers of the OSI model. If you must deploy a client of some kind to your business partners, make sure it is as unobtrusive as possible. If these notions are built into the architecture, the deployment and ultimate success of the extranet service will be greatly enhanced.

Software distribution and maintenance tools should be part of the architecture. Most companies have a means of distributing software that services internal users. For a variety of reasons, this most likely will not work in the extranet setting, so the extranet service should utilize modern, extranet-ready software distribution tools. There are a variety of such tools on the market, some focused on fat client distribution and updating, others focused on Java, and others that cover a number of application types.

## Integration, Marketing, and Deployment

Once the architecture is in place, the components need to be integrated and tested both in proof-of-concept and pilot mode. Having a business unit sponsoring the pilot in

conjunction with an actual group of business partners is helpful. Testing the extranet service with internal users may not provide all of the input you need to make the small changes to policy, process, and architecture that are almost inevitable.

With the extranet service assembled and tested, the IT department should actively begin marketing the extranet service. This should be done by the CIO to LOB executives because of the need to focus on business more than technology when introducing the service. You may also wish to invite senior managers to a demonstration event, focusing on business impact as well as technology.

Next comes extranet deployment. Once again, deployment should be conducted as a process. Specific roles and procedures should be in place for the distribution of software, the contacting of business partners, and the issuing and distribution of credentials. Extranet users should be contacted by phone or e-mail to alert them of the deployment and to outline the chain of events for getting them running. Additionally, contacting the security administrator at the business partner site may be helpful. That person may want to understand how the extranet works and be satisfied that it represents no security threat to the partner firm.

The issuing of credentials needs to be thoroughly considered, and strong processes and systems built to support it. Here again, the systems and processes that are used to issue authentication credentials inside the enterprise may not work as well in an extranet setting. Security expertise is paramount in establishing the credential distribution process.

### Extranet Management

Companies must also tackle the question of extranet management: should they manage the extranet service in-house, or outsource? An extranet requires a new level of integration between network security and applications, not only in design and deployment but also in ongoing operations. Extranets also require new services and capabilities that can be inefficient and costly for individual companies to support. What's needed is extranet expertise that goes beyond the core competencies of most corporate IT departments. Because of the complex and highly specific nature of the extranet, many companies choose to outsource its management.

## *Summary*

Extranets deliver significant competitive advantage to the enterprise. Because their potential to positively impact the business is so great and their value so strategic, IT managers must focus on delivering extranet connectivity as a service, rather than as a single application or a simple Web site. By incorporating thoughtful policies, robust architecture, and thorough processes for delivery and management of the extranet service, the IT organization will create a service that is critical to fulfilling the company's e-business strategy.

## *Glossary*

**Application inventory**—A list of applications that could be useful for collaboration with business partners. These applications need not be Web-enabled. The list should include all present and future applications that are used within the enterprise.

**Constituent inventory**—A thorough list of all current and potential users of the extranet, organized by their relationship to the enterprise.

**Extranet service—**A service offered by the IT organization to accommodate collaboration with and connectivity by business partners.