It has been estimated that by the year 2000, 50% of computer access will be from external associations. This rise in external access comes from telecommuters, business associates, customers, or potential customers, each with a unique set of computing and data requirements. The solution will not be the same for all; more aptly stated, should not be the same for all.

Before traveling too far down the path of presenting secure extranet architectures, it is helpful to get a solid foundation of what an extranet actually is. In and of itself, this discussion could provide sufficient material for a dissertation; however, to keep it brief, any omission of an opinion is clearly intentional.

WHAT IS AN EXTRANET?
Extranets are the evolution of business requirements to create a separate and distinct category of network participants; for lack of a more descriptive phrase, that is neither intranet nor Internet. An intranet, in people terms (vs. network terms), is the business association of computer users who are known and managed within a controllable computing environment. The controllable environment has rules, order, and known boundaries. The Internet, on the other hand, is aclassification of data and systems. To state the overstatement, there has been a paradigm shift; business data cannot be sacrificed in order to permit external business associates to have access to it. Security solutions must utilize the technologies provided with today's networking tools to allow their companies to compete on the Internet.
er hand, is, in people terms, anarchy. Although more attempts are being made to provide etiquette for the Internet and to establish a sense of societal normalcy, the goal is lofty and will take time because the Internet is global and imposing common ethics across the world is a gargantuan task.

As a result of the various extranet architectures, several definitions have evolved. Some support a tight, well-managed membership view, whereas others, like Richard Baker, author of Extrane... the Complete Sourcebook, take a broader view that equates extranets to “a state of mind, not a technology.” Because there are many ways to implement an extranet, the author of this article favors the broader view: His definition is: “Extranets are comprised of an association of individuals, outside your direct control, with a valid need to have access to your data.” Just as a mailman has a valid reason to go to an individual’s home to deliver mail, there is no expectation that he will open the door and put mail on the kitchen table; however, people do expect the furniture delivery man to enter their home and to place a chair in the family room instead of leaving it at the doorstep. Extranet partnerships may be established for many reasons, each with different expectations of service from both the company and the extranet partner.

BUSINESS BASICS: WHAT THE ARCHITECT NEEDS TO KNOW
When developing an extranet architecture, the architect must understand the business requirement and manage expectations to properly manage security. Questions generated by the business request should include, but not be limited to, the following:

- What is the expected frequency and duration of access?
- How much modification to the extranet client is allowed?
- What applications are required?
- Must the data be protected when transmitted?
- Is data coming in or going out?
- What is the expected level of performance?

Architects must ask enough questions to thoroughly understand the request before beginning to create an extranet. They must ask these questions again and make sure they understand the answers. They must restate the problem. Most important, separate, different requests do not force two problems into one solution. If it is a delivery issue, are we including the mailmen with furniture delivery: I need my mail delivered every day to the doorstep; I need furniture delivered inside the house once every three years.

SECURITY COMPONENTS
Maintaining security for an extranet varies depending on the solution. However, understanding what the security requirements are is necessary
before designing the architecture. Security is so much easier when considered early. First, the architect must understand the security policy of their corporation: Some will not allow external users access to internal systems whereas others would rather not risk the data and accept controls that permit a small population to penetrate the firewall. The security factors in an extranet are universal: Architects must provide only those services required to get the job done (least privilege rule), prevent or audit, and protect valuable data.

The "least privilege rule" minimizes the risk to a network by reducing the number of security vulnerabilities that can be exploited. Even though the mail can come in the mail slot, it is wise to keep the mailman at the door. Just as users should not be given administrator access, extranet partners should be limited in their access as well as in their level of services that can be used.

"Prevent or audit" is a variation on the concept; if it cannot be protected, it must be watched. User accountability and auditability are important when users are allowed access within an intranet; however, some techniques allow "guest" users into controlled space in an intranet with little increased risk to the rest of the network. This topic is discussed later.

The "protect valuable data" factor identifies the need to ensure that the data acquired by a company's extranet partner is protected if it contains sensitive business data, either the company's or the partner's. This may be protecting authentication tokens (i.e., user ID and password) or the entire session.

Security considerations must include options based on business requirements, security policy, risk assessment, and life-cycle costs. The risk assessment can be put simply: What are the security measures protecting against? The life-cycle costs must include maintenance costs along with the start-up costs. These can become tough to estimate when the design requires licensing of client software, key management, user registration, and auditing. Just as in the delivery scenario, only the furniture delivery should need auditing. However, a poor implementation could require daily auditing of the postman.

When developing extranet architectures, the architect should consider processes separately and combine them only with other needs if the types of data, applications, access controls, and data protection mechanisms are the same.

**TYPES OF EXTRANETS**
Choosing the best extranet solution for a company's needs is important. To choose the correct solution, it is important to understand clearly the available alternatives.

There are six basic extranet technologies as well as some specialized and hybrid solutions: (1) external resources, (2) Internet protocol (IP) address filtering, (3) authentication servers, (4) application layer manage-
ment, (5) proxy servers, and (6) encryption services. Each is sufficient to initiate business communications, but each carries different performance, cost, and security. Following is a detailed review of each technology.

External Resources
Providing information via external resources is the first category of an extranet. It is pure Internet. Data is made available to the entire intranet community, and anything the company wants to protect is not made available and is kept separate from the public data, also described as the air-gap approach. The early Internet thrived on bulletin boards and file transfer protocol (FTP) sites to support this sharing of information. It meets the basic definition of an extranet in that the company is sharing its information with a community it has selected. Unfortunately, from the security standpoint, this data is totally at risk. In this environment, the business decision to include everyone in the extranet forces the company to decide that protection of the content of the data is important. This means that the company wants to ensure that it is its data that is available and not some modified version that someone has put in its place. Protection can be as simple as reposting information each time the company finds it has been changed.

**TIP:** The basic key to managing extranets is understanding the components that make up the extranet. Choosing the best security solution is somewhat of a menu approach.

IP Address Filtering
Address management was the solution-du-jour in the early days of firewalls. Truly, this is the heritage solution. It allows a company to select its constituents by their IP address. Essentially, a group is selected to be allowed access based on the physical devices that are used, not by the users themselves. Most network routers provide this simple security mechanism via access control lists (ACLs). Using routers for this service has some drawbacks. Routers were not designed as security devices. They were designed to efficiently manage network traffic. Adding ACLs to a router creates a processing overhead that must be considered, as well as the management effort to create and maintain these lengthy lists.

Authentication Servers
Looking deeper into ACLs, another layer of granularity can be implemented beyond basic address management: port/service management. The ACL is a three-part statement that identifies source (external address), destination (internal address), and port or service desired. The ports/service identifier are part of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack and can be used as an extra feature to limit
access to one or a few services such as HTTP (port 80), FTP (port 20/21), and Mail (port 25).

This approach is susceptible to spoofing of IP addresses and configuration errors. IP spoofing is the process in which crackers masquerade as authorized IP addresses to be permitted access into the company’s network. Configuration errors occur when the network technician demonstrates human frailties, a more common event as the ACLs grow large and cumbersome. Even without these problems, the security profile is based on managing access by hardware, not by users. The bottom line is that routers operate on a simple security principle that make it unsuitable as a single security mechanism.

Application Layer Management

Another component to consider when establishing an extranet is authentication management. The security controls are now moved from managing a piece of hardware (IP address) to managing the user, which adds complexity to the situation by requiring that an authentication mechanism be managed locally and then distributed to the company’s extranet partners. The benefits are allowing control over who has access to the company’s information. It allows for controlled access into specific applications as well as establishing identity to manage accountability of the user. Various authentication approaches are available; user ID and password combinations are the most prevalent. Token-based authentication is a more secure method, but it is more expensive.

Communications sent via the Internet are subject to packet sniffing that will compromise any cleartext transmission of a user ID and password. Therefore, the success of the user ID and password authentication mechanism depends on the encryption technology being used to transmit the information. However, once this technology is compromised, anyone masquerading as that person can use it to access data.

The use of token-based authentication requires that the user have a special token in their possession that must be used as part of the authentication process. The more prevalent systems available today are challenge-response or time-synchronous tokens.

Proxy Servers

Proxy servers are another tool that can be used to support extranet clients. A proxy device prevents a direct transmission between internal and external computers. It intercedes by receiving the request, then, using IP address translation, forwards the packet to the proper destination while logging the process if it is desired. These proxy servers can be application specific. For example, all E-mail can be routed to a specific server, which is a handy way to offload traffic to other servers and still maintain
a level of security. From a security standpoint, it masks the IP addresses to help prevent spoofing attacks that can foil basic router ACLs.

**Encryption Services**

Encryption is the last technology to be addressed before delving into the available solutions for creating an extranet. Encryption has received a lot of press lately with the U.S. government's restrictions on the export of extended-length keys as a threat to national security. However, paramount to establishing a secure extranet is the dependency on encryption for some, if not all, of the communication process. The use of encryption is based on the time value of the data. Shorter (a.k.a. less secure) key lengths can be used to transmit critical data with short life spans or low-value data. Rather than discussing which algorithm is best, suffice it to say that use of encryption methodology is a key resource.

A network firewall is a technology that conjures up visions of security. It is a tool that manages the boundary between the intranet and the Internet. It is a collection of the four technologies mentioned previously, depending on how it is designed and configured, although some do not proxy and some do not use encryption. Today, most firewall products have been augmented with instructions on how to react based on the type of attack. However, it is only one component of an extranet architecture.

**A QUICK REVIEW**

Thus, extranet architects are faced with the following questions: What is an extranet architecture? How can the architect create one? How does the material just presented help the architect know what is the right solution for the job at hand? To review: There is a business requirement, a security policy, a risk assessment, and four basic technologies: firewalls (to include router ACLs), authentication mechanisms, proxy services, and encryption.

**Costs**

When reviewing costs, the architect must look at the cost of implementation, the cost of maintenance, both administrative and hardware, and the cost of data. Cost of implementation is simply what additional hardware, software, and personnel must be used to implement the architecture. Maintenance costs are a little harder to estimate. Hardware maintenance is generally packaged by the vendor, but there are also possibly client licenses, audit reviews, change management, and scalability of solution. Finally, what is meant by data costs? This is the value of the data — its realistic value. If it is compromised, will the company lose hundreds, thousands, or millions of dollars? This, too, is a key factor in choosing how to architect the extranet. Another consideration is the ex-
tranet partner’s desire to get to the data. Will the company lose business if the architecture is too cumbersome?

Reminder: Each extranet architecture should be separately evaluated to avoid the trap of putting voluntary extranet clients into a too restrictive environment and losing their business. Instead, provide a little information with ease and then require more security for the true business partnerships.

DMZ, ISLANDS, PROXIES, VPNS, WEB-BASED EXTRANETS, AND HYBRIDS

Exhibit 1 diagrams a zone of networked devices (DMZs) that are placed between the intranet firewall and the intranet. The DMZ hosts relative low-value business information for a large contingent of users. It is usually protected from the Internet with a router and limited ACLs established by limiting the ports/services and blocking any undesired IP addresses. This type of extranet is fairly simple to install and has low overhead. It has no authentication, encryption, or proxies. A DMZ is a simple approach for any business systems placed on the Internet.

An Internet island, shown in Exhibit 2, is a variation on the DMZ theme. It is an isolated subnet within the intranet with no outbound intranet service connections. It allows an extranet client to access the island for information but without being given access to any other information in the intranet. This configuration requires an ACL to open access to the isolated subnet. This design is best for accessing a specific application server that requires authentication. If authentication fails, the session goes no further.

An application gateway, shown in Exhibit 3, may also be used to support extranet clients. This goes beyond the Internet island concept by ac-
cessing resources within the intranet while the application server itself remains in the DMZ or on the island. This approach is to “dual home” the application server, in essence creating a proxy device. A user logs onto the application server and the application brokers all transactions for information within the intranet. Dual homing is the use of multiple network interface cards to allow the application server to have multiple addresses. One is usually an exposed address where an extranet client accesses the server; the other is the trusted side from which access to the intranet is allowed. These application gateways, in addition to proxying transactions, are software programmable with both application and router-type rules, have enhanced audit capabilities, support various authentication mechanisms, and might even include session encryption technology. This is a more constrained set of users, access control mechanisms are stricter, and accountability of users is strictly controlled.

EXHIBIT 2 — Internet Islands

EXHIBIT 3 — Application Gateway
Like the application gateway, an inbound proxy server, shown in Exhibit 4, allows access to data on the intranet. Although the use of a proxy isolates an inbound user at the proxied server, it also provides protection of the information by maintaining it internally to prevent tampering. Firewall access control rules manage the proxied address and services.

Virtual private networks, shown in Exhibit 5, primarily utilize encryption technologies to protect the data sent. Using encryption can protect log-in across the Internet as well as be used as a front-end filter, which allows only clients with the encryption software to pass. Routers, firewalls, and even some operating systems are incorporating encryption technologies. Performance must be considered when implementing any
encryption solution. Methodologies support server-to-server or client-to-server encryption.

Because of the focus on Web-based communications, the security options when creating the extranet’s Web-enabled applications are more abundant. Web browsers can incorporate current encryption technologies (secure socket layer, or SSL, http-s or shttp) to act as the front end to protect the data, as well as broker data through a firewall (see Exhibit 6). Benefits result from using a tool that is installed on most Web browsers. The browsers themselves and possibly each client must have a certificate registered with a third party to support the mutual authentication of each party. This third-party certificate service is commercially available or may be managed by the company. Some of the issues concerning certificates today are generation, management, and, most difficult, revocation.

The hybrid category is a collection of tools, discussed earlier, that create a unique business solution to control security and provide information to a unique extranet business group.

CASE STUDY
An example from the real world demonstrates how creative solutions can be developed. A company desires to provide a client with production information that is maintained on an Oracle database. The client does not have knowledge in using Oracle; in fact, the company has a large user population that varies in computer skills. Most users can send E-mail and
Web browse. The Internet is the required network architecture because of cost limitations and global distribution of the clients. Authentication is required because protection of the customer's data is important.

Following is a restatement of the business requirements:

- Access to an internal Oracle database is required.
- Users have varied skills but all are running Web browser products.
- Internet access is required.
- User authentication is required
- Data privacy is required.

In addition, the following information is important:

- Company policy does not allow unauthenticated access to intranet.
- Company business decision does not allow external access to database.
- Cost to replicate data is prohibitive.

The design description ends up as follows:

- A Web-based client architecture that provides access to an internal Oracle database to which extranet clients must authenticate, but not directly have access to, and receive data that is provided privacy during transmission across the Internet.

The architecture, shown in Exhibit 7, consisted of four components:

1. Web server with certificate to create an http-s (SSL) encrypted session
2. Address/service filtering on firewall to allow SQL call to database
3. Oracle Web listener installed on Web server to translate html document into a database query (application proxy)
4. Oracle’s authentication mechanism to validate the extranet users

There are four steps to operating the security mechanism.

Step 1: Establish Secure Communications
The user sends a request to connect with the Web server. The Web server replies with its certificate to the client, who accepts the certificate for the encrypted session. (Note: A user certificate is not required as the authentication of the user occurs later.)

Step 2: Authenticate via Oracle Database
This step has several components:

1. The client sends the query to the Web server.
2. The Oracle Web listener translates the Web query into an Oracle SQL request.
3. The Oracle database receives the query and prompts for user ID and password, which are transmitted to the client by the Web listener.
4. The client sends user ID and password to the Web listener via the encrypted pipe created in Step 1, which is then forwarded on to the Oracle database.

**Step 3: Transmit Data to Client Using Encrypted Mechanism**
The database allows access, resulting from a proper user ID and password, and fulfills the query via the Web listener.

**Step 4: Close Transaction**
Once the data is sent, the encrypted session is closed. The benefits are that the user only logs on once, only one certificate is required, user ID/password can be quickly managed because the resource is local, and only one more port was opened on the firewall (port 447-SQL) specific to that database server.

This case study presented an implementation of an application gateway with proxying and using the Oracle database as an authentication server with encryption provided by the Web server.
CONCLUSION
As more robust security solutions are developed and move into mainstream computing, more options will become available for customizing the security of an extranet. One newer technology that may be considered is internally managing security certificates of extranet partners. Another factor that will strengthen extranet security is up in the air and depends on how the U.S. government resolves the encryption export issue.

The ultimate evolution of the extranet will occur when the delineation of intranet and extranet disappears and business users operate under the same security controls no matter where their computing resources reside.

Steve Trolan is information security manager at Altera Corporation in San Jose, CA.