Novell's Net Security solution helps you find and deploy products that minimize the risk of conducting e-business. (For more information about this solution, see “Minimize Risky e-Business With Novell’s Net Security Solution” on p. 22.) To provide even tighter security for your company’s e-business, Novell has updated or soon will update several of the products the Net Security solution identifies. This article outlines the major updates to three of the key products in Novell’s Net Security solution.

NOVELL MODULAR AUTHENTICATION SERVICE ENTERPRISE EDITION 2.0

Due for release in April 2001, Novell Modular Authentication Service Enterprise Edition 2.0 will include several new features that enable and enhance strong authentication solutions. In addition to the authentication methods Novell Modular Authentication Service Enterprise Edition currently supports, this new version will support the following Novell-developed authentication methods:

- **Advanced X.509 v3 Certificate Method**
  The Advanced X.509 v3 Certificate method enables you to authenticate to NDS eDirectory using any X.509 v3 certificate that complies with the Public Key Cryptographic Standard (PKCS)#12. (PKCS#12 defines a file format for containing digital certificates and their private keys.) All of the leading Public-Key Infrastructure (PKI) vendors, including Entrust, VeriSign, and Baltimore, support and generate certificates that comply with PKCS#12. When you use this certificate method for authentication, Novell Modular Authentication Service can check its Certificate Revocation List (CRL) to validate certificates used for authentication purposes and can also validate the chain of root certificates.

- **Entrust Method**
  Like the Advanced X.509 v3 Certificate method, the Entrust method enables users to authenticate to NDS eDirectory using any X.509 v3 certificate that complies with PKCS#12. It also supports CRL checking and certificate root validation. When you use the Entrust method, you can incorporate the use of Entrust certificates into the graded authentication scheme you set up for your company’s network.

- **Password Policy Management Method**
  The Password Policy Management method enables you to create policies to control and enforce the passwords users generate for NDS eDirectory authentication. For example, you can set up a policy that prevents users from creating a password that is in the dictionary, or you can require users to use alternating uppercase and lowercase letters or at least two numbers. Novell Modular Authentication Service Enterprise Edition 2.0 checks users’ proposed passwords to ensure they comply with this password policy.

- **Universal Smart Card Method**
  The Universal Smart Card method enables users to authenticate to NDS eDirectory using smart cards from a variety of smart-card vendors, such as Gemplus.

- **RADIUS Authentication Method**
  The RADIUS Authentication method enables remote workstations to communicate with a RADIUS server to validate the users’ NDS eDirectory password.

- **Other Authentication Methods**
  Novell Modular Authentication Service Enterprise Edition 2.0 supports more than 20 authentication methods from third-party vendors. For more information about each partner listed below, visit www.novell.com/products/NMAS/partners.

- A ctiVCard Inc.
- Applied Biometrics
- A Root Systems Inc.
- BioID
- Biometric Access Corp.
- Cherry Corp.
- Compaq
- Identix Inc.

- RSA Security Inc.
- SA FLINK Corp.
- SecuGen Corp.
- Secure Computing
- Sonera/iD2
- SPYRUS
- Vasco Data Security
- Veridicom Inc.

NOVELL ICHAIN 1.5

Novell IChain 1.5 includes (but is not limited to) the following three components. (See Figure 3 on p. 32 in the “Minimize Risky e-Business” article.)
The Novell iChain Internet Caching System Server

The Novell iChain Internet Caching System server operates only in reverse proxy mode (also called accelerator mode). A reverse proxy accepts requests for web site data from external users and delivers most of that data from its own cache. The proxy contacts the web server hosting that data only when the data in its own cache is out of date or when additional processing, such as a database lookup, is required.

Most reverse proxies interact with a single web server, but the Novell iChain Internet Caching System server has multihoming capabilities. As a result, you can use the single public IP address from the Novell iChain Internet Caching System server to front-end multiple backend web servers. Because you need to own only one IP address for multiple web servers, you save your company money.

More important, Novell iChain protects your company's web servers by rendering them essentially invisible: All outbound information appears to originate from the Novell iChain Internet Caching System server.

Novell iChain Authentication Service

The Novell iChain Internet Caching System server interfaces with the Novell iChain Authentication Service. This service enables users to use one or both of two authentication methods, which are reflected in NDS eDirectory as the Lightweight Directory Access Protocol (LDAP) Authentication profile and the Secure Sockets Layer (SSL) Mutual Authentication profile.

The LDAP Authentication profile enables users to use a loginID and password pair to authenticate to the Novell iChain Internet Caching System server. The SSL Mutual Authentication profile enables users to use an X.509 certificate to authenticate to the Novell iChain Authentication service. You can also use X.509 certificates in conjunction with the loginID and password pair, thus creating a multifactor authentication for added security.

The LDAP Authentication Profile object has several attributes, one of which is the LDAP Login Name Format attribute. By default, the Login Name Format is a user's distinguished NDS name.

The Login Name Format also includes two parameters that you can enable if you want to use different login name formats: You can enable the E-mail Address field to allow users to authenticate using their e-mail address as their login name. Alternatively, you can enable the LDAP Field Name parameter. The LDAP Field Name parameter allows you to specify any LDAP attribute—for example, the User object Employee Number or Social Security Number attributes—which users can then use as their login name.

The Novell iChain Authentication process works as follows:

1. When a user makes a request for web site data, the Novell iChain Internet Caching System server checks its authentication table to determine if this user is already authenticated.
2. Assuming the user is not authenticated, the Novell iChain Internet Caching System server consults NDS eDirectory for the authentication policy, which NDS promptly returns.
3. The Novell iChain Internet Caching System server then switches to an HTTPS port and sends a request for authentication to the user.
4. The user returns his or her authentication credentials, and the Novell iChain Internet Caching System server authenticates him or her (assuming, of course, the user's credentials are valid).
5. The Novell iChain Internet Caching System server also sends a cookie to the user's browser, which the browser stores in memory.

Novell iChain Authorization Service

After a user is authenticated, Novell iChain Authorization Service ensures that users do not access any data except the data they are authorized to access. Novell iChain Authorization Service authorizes access requests based on rules that you create and store as NDS objects. The Novell iChain Internet Caching System server stores these objects in its cache for improved performance.

Within these Access Rule objects, you list various URLs to which you wish to control access. Being able to control access based on the URL enables you to control access right down to specific pages.

However, this doesn't mean you have to list the URL to every page to which you want to control access. The Access Rule objects also include wildcard options so you can grant access to broader areas of a web site without having to specify the URL to each page within an area. For example, a rule that includes an asterisk (*) in the URL, as in web1.novell.com/*, grants users associated with this rule access to all pages under web1.novell.com.

To control access to the URLs you list within the Access Rule objects, you assign these objects to NDS Community, Group, User, and container objects. All users associated with a particular Access Rule object can access the URLs listed within that object. As you would hope, Access Rule objects also have an exception list, so you can grant access to all users within a Group or Community object, for example, barring the users you list as exceptions.

By default, all access is denied through the Novell iChain Internet Caching System server; however, you can create a public access policy to allow access to a restricted set of web site data without requiring authentication. The Novell iChain Authorization service enables you to define a Guest User to provide this public access. The general public can gain access to all resources protected by any Access Control rule associated with the Guest User.

BorderManager Enterprise Edition 3.6

Released last month, BorderManager Enterprise Edition 3.6 features the following enhancements:

• A major code review that has improved the overall performance and stability
• Support for user-based URL blocking for users of Citrix servers
• Support for proxy chaining, previously included only in an enhancement pack
• Faster Remote Authentication Dial-in User Services (RADIUS) authentication, which supports up to 40 authentications per second
• Support for a Virtual Private Network (VPN) over N etwork Address Translation (NAT) to enable cable modem and Digital Subscriber Line (DSL) users to access the corporate network securely from home using the BorderManager VPN
• Simplified installation

CONCLUSION

In today's complex e-business environment, security has become more critical and more difficult than ever before. Through the Net Security solution, Novell helps you find and deploy both Novell and Novell-partner products that help you protect your company's assets.