

Beneficial Life

Opens Its Internet Doors to Clients, Agents, and Employees

Including security in IT solutions from the beginning is far cheaper than adding security after those solutions are in place—according to a recent *Computerworld* article that discusses the difficulty of calculating return on investment (ROI) for security-related expenditures. (See “Security ROI Calculations Pose Challenges for Users,” *Computerworld*, Nov. 5, 2001. You can download this article from www.computerworld.com/storyba/0,4125,NAV47_STO65303,00.html.)

Building security into an IT solution is also more effective than adding security after the fact. After all, your company cannot afford to be vulnerable while you search for and close security holes. The more security holes a solution has, the more vulnerable that solution is.

Assuming these assertions are true, including Novell access and security solutions in the next IT project your company implements could save money and provide most of the security needed to protect that solution. Novell access and security solutions are available individually or as components of Novell Consulting solutions. The goal of these solutions is to enable organizations to securely manage access to applications, databases, and platforms for web, wireless, client, Virtual Private Network (VPN), and dial-up users.

As Novell service line manager Bill Maxey explains, “Access control is at the heart of any good security solution.” As far as Novell is concerned, Maxey adds, Novell eDirectory is the cornerstone of access control. Not surprisingly, eDirectory is the key to Novell access and security solutions, which also include the following directory-enabled products: NDS Authentication Services, Novell iChain, Novell Modular Authentication Service (NMAS), Novell SecureLogin, and Novell BorderManager. You can use eDirectory alone or in combination with other products to build security into your company’s next IT project, as Beneficial Life Insurance Company has been doing for years.

ABOUT BENEFICIAL LIFE

Beneficial Life (www.beneficiallife.com) is a Salt Lake City, Utah-based insurance company that specializes in a wide range of life and disability insurance products. Beneficial Life has been using eDirectory to secure internal access to its network for the past five years. Beneficial Life’s 250–300 employees currently



authenticate to seven NetWare 5.1 servers running on Beneficial Life’s LAN via eDirectory 8.5.

Since 1998, Beneficial Life has also been using another Novell access and security solution—Novell BorderManager Firewall Services 3.5. Beneficial Life is using BorderManager Firewall Services’ forward-proxy caching technology to speed employees’ access to Internet sites. (BorderManager’s forward-proxy caching technology can speed Internet access by 10 to 200 times.)

BorderManager Firewall Services is currently sold both separately and as part of BorderManager Enterprise Edition, which is a suite of BorderManager products. The next version of BorderManager—version 3.7—will combine into a single product all of the separate products included in BorderManager Enterprise Edition. (For more information about BorderManager Firewall Services, visit www.novell.com/products/bordermanager/firewall/details.html. For more information about BorderManager 3.7, see “Run for the BorderManager 3.7” on p. 39.)

TAKING ITS BUSINESS TO THE NEXT LEVEL

Like many companies, Beneficial Life recently decided to expand its business beyond its firewall to the Internet. (Beneficial Life is using a high-end hardware-based firewall that provides packet-level filtering and attack-prevention services.) As Beneficial Life webmaster and network administrator Mark Walter explains, Beneficial Life wanted to extend its business to the Internet for a number of reasons.

For one thing, Beneficial Life wanted to give certain employees the option of working from anywhere that these employees had an Internet connection and a web browser. Beneficial Life also wanted to provide web-based information and services to 800–900 insurance agents, thus making it easier for these agents to do business with Beneficial Life.

Moreover, Beneficial Life wanted to provide additional information and services for a subset of these agents—financial sales professionals. (Financial sales professionals are agents who specialize in Beneficial Life policies and services.) In addition, Beneficial Life wanted to give certain policy holders web-based access to information about their policies.

Naturally, Beneficial Life also wanted to ensure that each of these groups—employees, financial sales professionals, independent agents, and policy holders—could access only the information and services intended specifically for that group. Of course, Beneficial Life wanted to ensure that its confidential information remained secure as it traversed the Internet.

Finally, Beneficial Life wanted to provide single sign-on access to this information and these services. As Walter explains, Beneficial Life did not want to deploy a solution that required users to authenticate separately to each of Beneficial Life's five web servers. Beneficial Life is using a combination of Oracle, Internet Information Server (IIS), and Apache web servers. Before Beneficial Life deployed its e-business solution, these web servers were providing information and applications only for users on Beneficial Life's intranet.

GETTING FROM THEN TO NOW

In 1999, Novell Consulting and Beneficial Life implemented an e-business solution that met all of these criteria. Not surprisingly, this solution includes another Novell access and security solution: Novell iChain.

iChain is Novell's directory-enabled infrastructure that controls access to—and therefore helps secure—web-based information and services. iChain's proxy-based architecture enforces authentication and access control to these web resources via eDirectory. iChain can also further secure confidential information by using Secure Sockets Layer (SSL) encryption to send that information across the Internet. iChain encrypts information on-the-fly between its reverse-proxy cache and users' browsers, removing the need to implement and manage SSL certificates on web servers to which iChain controls access.

In addition, you can configure iChain's reverse-proxy cache to present a single IP address—the IP address of the iChain proxy server—to all users on the Internet. That is, iChain's reverse-proxy architecture enables you to increase overall security

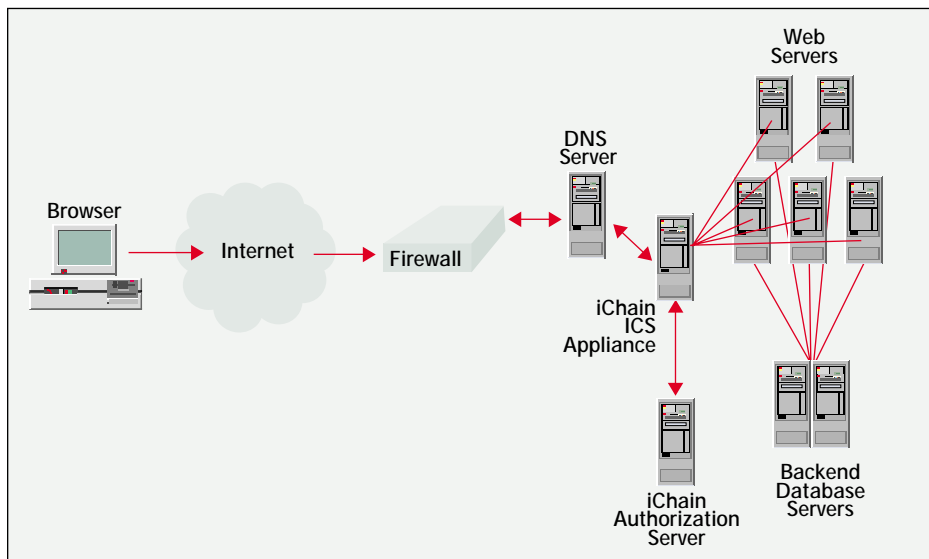


Figure 1. When authorized users access Beneficial Life's e-business site, browser requests first go to Beneficial Life's firewall and then to its DNS server, which resolves these requests to the IP address of a Compaq Proliant iChain ICS appliance. This appliance authenticates users through iChain Authorization Server components running on a NetWare 5.1 server that is also running a read/write replica of Beneficial Life's directory tree. These components access eDirectory for authentication and access control information. iChain then serves requested information and applications from its reverse proxy cache or from one of Beneficial Life's five web servers. These servers access information from two backend Windows 2000 servers running Oracle 8.17.

ty by preventing users from directly accessing to web servers and directory information. You can also configure iChain to provide single sign-on access to web resources. (For more information about iChain, visit www.novell.com/products/ichain/details.html.)

In other words, iChain provided the granular access control, security, and single sign-on capabilities that Beneficial Life wanted its e-business solution to include. In fact, Walter adds, iChain was "really the only product out there" capable of providing these features at the time Beneficial Life implemented its e-business solution. (Beneficial Life used iChain 1.5 to implement its e-business solution. The current version of iChain—version 2.0—includes several new features. For more information about these features, see "What's New in iChain 2.0" in "Novell iChain: How One Company Found Its e-Business Solution," *Novell Connection*, Aug. 2001, p. 16. You can download this article from www.ncmag.com/past.)

THE PARTICULARS

To implement this e-business solution, Novell Consulting and Beneficial Life's web services team—collectively called the *implementation team*—used Beneficial Life's existing eDirectory tree

Visit our advertiser, Wired Red, at www.wiredred.com.

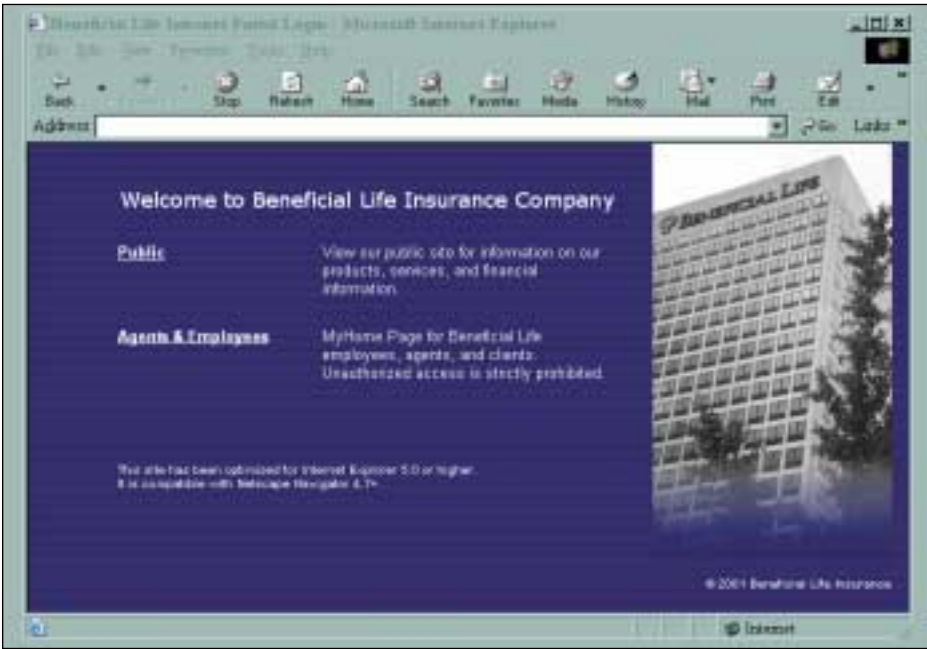


Figure 2. Beneficial Life's e-business site includes a link to Beneficial Life's public web site and a link to its intranet. When you select the Public link, iChain uses the access privileges of Beneficial Life's guest User object to enable you to access this site without logging in to iChain.

and the information and applications running on its five web servers. The implementation team also used the following iChain 1.5 components:

- **iChain Snap-in Module for ConsoleOne.** This component enables you to configure the eDirectory objects that iChain uses to perform its tasks. You also

use this snap-in module to manage these objects. (You install this snap-in module from the iChain 1.5 installation CD. You can install this snap-in module on any Windows workstation that is running ConsoleOne 1.2 or above, or you can install this snap-in module on any NetWare 5.1 or above server running ConsoleOne 1.2 or above.)

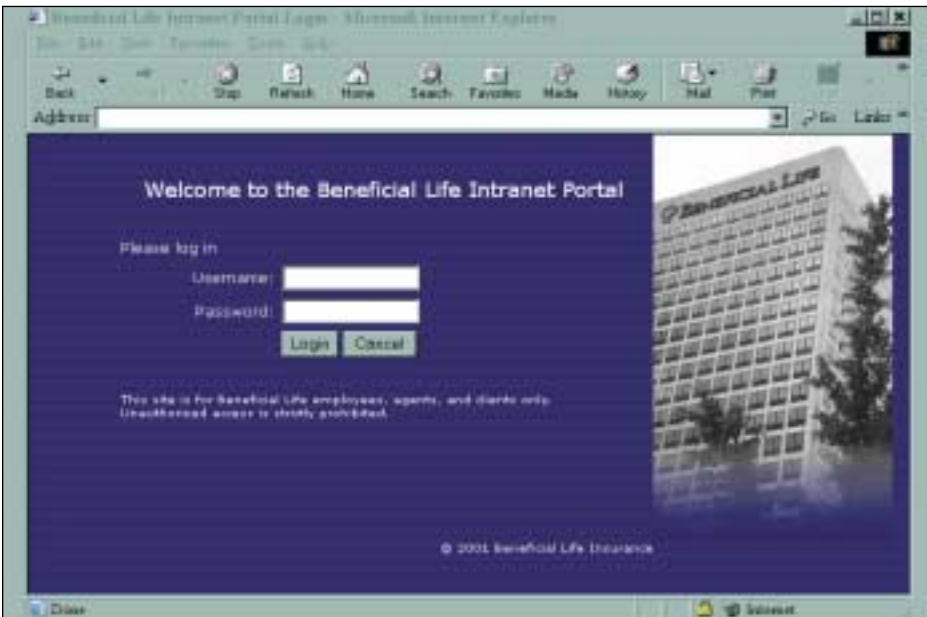


Figure 3. iChain includes a default user interface. However, you can configure iChain to use other user interfaces, such as Novell Portal Services portal. Beneficial Life configured iChain to use an Oracle Application Server Portal as a user interface for web-based users.

- **iChain Authorization Server.** This component extends the eDirectory schema to include specialized iChain objects. The Authorization Server component includes three NetWare Loadable Modules (NLMs): AUTHCHK.NLM, ACLCHECK.NLM, and OACINT.NLM. iChain uses AUTHCHK.NLM and ACLCHECK.NLM to perform authentication and access control tasks. OACINT.NLM enables you to provide web single sign-on via Object-level Access Control (OLAC). (OLAC is a protocol that enables iChain to insert Lightweight Directory Access Protocol [LDAP] information into HTTP headers.)
- **iChain Internet Caching System (ICS) Appliance.** In Beneficial Life's implementation, this component is comprised of iChain 1.5 running on Beneficial Life's ICS caching appliance, which is a Compaq ProLiant server running ICS 1.3. (ICS caching appliances are now marketed by Volera as Volera Excelsator. These appliances speed the delivery of Internet content for one or more web servers. For more information about Volera Excelsator, see "Volera Excelsator 2.0: Making Streaming Media Fly," *Novell Connection*, May 2001, pp. 21-31. You can download this article from www.ncmag.com/past.)
- **iChain ICS Browser-Based Administration Utility.** You use this component—which is running on the iChain ICS appliance—to configure the iChain ICS appliance.

The remainder of this article is a step-by-step description of how the implementation team used these components to deploy Beneficial Life's e-business solution.

STEP 1: INSTALL THE ICHAIN 1.5 AUTHORIZATION SERVER

The implementation team installed the iChain 1.5 Authorization Server component on a NetWare 5.1 server that was running Service Pack 2a. (See Figure 1 on p. 37.) This server also runs a read/write replica of the [Root] partition of Beneficial Life's eDirectory tree. As mentioned earlier, the Authorization Server component extends Beneficial Life's eDirectory tree to include specialized attributes and objects.

Specifically, the Authorization Server component extended the eDirectory tree to include the following iChain attributes and objects:

Run for the BorderManager 3.7

As you may already know, Novell BorderManager 3.7 is on the horizon. This new International Computer Security Association (ICSA) firewall-certified version of BorderManager is scheduled for release in April 2002. With this release, you'll notice some significant changes to previous versions of BorderManager. For example, BorderManager 3.7 includes all of the BorderManager products currently available in BorderManager Enterprise Edition 3.6. In fact, BorderManager 3.7 will replace BorderManager Enterprise Edition 3.6, BorderManager Authentication Services 3.6, BorderManager Firewall Services 3.6, and BorderManager VPN Services 3.6.

However, some things won't change with this new version of BorderManager. For example, the BorderManager 3.6 architecture won't change, and BorderManager 3.6 licensing won't change. BorderManager 3.7 will also support the same versions of NetWare and Novell eDirectory that BorderManager 3.6 supports. (BorderManager 3.7 will not be tested with NetWare 4.11 and 5.0, however.)

In other words, Novell product manager Scott Jones explains, upgrading from BorderManager 3.6 to 3.7 will be "completely painless" for most BorderManager customers. This painless upgrade will include the following enhancements:

- **Virtual Private Network (VPN) Client for Windows Millennium Edition (ME).** Because most users access BorderManager VPN services via a home PC, Novell is including support for Windows ME in BorderManager 3.7. (Windows ME is designed exclusively for home use and is the operating system included with most PCs intended for home use that have shipped in the past 9 to 12 months.)
- **The Beginner's Guide to BorderManager by Craig Johnson.** Based on real-world experience and written in plain language, this book is a comprehensive guide to deploying BorderManager. The author, Craig Johnson, is an independent consultant.
- **New Content-Filtering Software by SurfControl.** BorderManager 3.7 will include improved software from SurfControl to help your company filter inappropriate Internet content. This software, which is based on SurfControl's SuperScout Web Filter, includes more than 2 million domains in its library of potentially inappropriate or dangerous Internet sites. (For more information about SuperScout Web Filter from SurfControl, visit www.surfcontrol.com/products/superscout_for_business/super_scout/index.html.)

In contrast, SurfControl's Cyber Patrol for Education—the content-filtering software that ships with BorderManager 3.6—has only about 64,000 domains. Furthermore, Cyber Patrol for Education is designed for educational use rather than business use. The content-filtering software that will be included with Novell BorderManager 3.7, on the other hand, is designed to strike a balance between educational and business use.

In addition, the content-filtering software that will be included with BorderManager 3.7 includes a reporting feature that can help you track Internet usage company-wide or on an individual basis. Novell is also working to enable you to place access rules for this software's content-filtering categories any-

where in your company's eDirectory tree. (Using Cyber Patrol for Education, you can place these rules only in Server objects.)

- **Virus Pattern Filtering at Proxy.** Novell developed this virus pattern filtering software as an emergency response to the recent Code Red virus. This software worked so well for the BorderManager 3.6 customers who asked for it that Novell is now including this software in BorderManager 3.7.

Because new virus threats are discovered daily, Novell has permanently assigned an engineer to keep this software updated with new virus patterns. In addition, Novell plans to implement automatic updates for BorderManager 3.7 virus pattern filtering software.

- **Personal Firewall.** Novell also plans to include a personal firewall to protect BorderManager 3.7 VPN clients. As you know, when you extend the boundaries of your company's network with VPN services, users' client machines become entry points to your company's network.

At the time this article was written, Novell had not yet selected a personal firewall to include with BorderManager 3.7. However, Jones affirms that a personal firewall will ship with BorderManager 3.7. This firewall, Jones adds, "will lock down users' client computer so when [these client computers] are connected to BorderManager VPN Services, they won't become a security threat."

- **Novell International Cryptographic Infrastructure (NICI) Support in VPN Client.** Although previous versions of the BorderManager VPN client used encryption software that was unique to BorderManager, BorderManager 3.7 VPN client software uses NICI. (As you probably know, NICI is Novell's standard encryption software. For more information about NICI, see "With NICI, It's All Holes Barred," *Novell Connection*, Dec. 1998, pp. 8–20. You can download this article from www.ncmag.com/past/.)

As Jones explains, using NICI as the encryption engine for BorderManager's VPN client will help Novell "deliver some new functionality for BorderManager VPN Services down the road."

- **Updates.** BorderManager 3.7 includes all of the enhancements included in BorderManager 3.6 Support Pack 1a.
- **Enhancements to Installation Software.** The installation program for BorderManager 3.7 prompts you to enter a default route for connecting servers running BorderManager 3.7 to your company's Internet Service Provider (ISP). (With BorderManager 3.6, you have to configure this default route after you install BorderManager.) The installation program also includes new default filters to provide maximum security at the time of installation.

In addition, Novell plans to support Point-to-Point Protocol over Ethernet (PPPoE). PPPoE support can enable your company to connect its Ethernet LAN to an ISP through a BorderManager 3.7 server. That is, with PPPoE support, your company's ISP can push IP configuration information to a BorderManager server in much the same way that a Dynamic Host Configuration Protocol (DHCP) server can push IP configuration information to computers on a network.

Although PPPoE support will not be included with BorderManager 3.7 when it ships, Novell plans to make PPPoE support available as a download after BorderManager 3.7 is released. ●



Figure 4. Users must log in to Novell iChain before they can access the applications and information on Beneficial Life's intranet. By controlling access to these applications and information, iChain enables Beneficial Life to securely extend its business to e-business.

- Specialized LDAP attributes
- iChain Service object (ISO)
- Access Rule object
- Community Services object

STEP 2: CREATE USER OBJECTS

Using the iChain snap-in module for ConsoleOne, the implementation team created the following User objects: a guest User object and an LDAP User object. The guest User object enables users to access Beneficial Life's public web site from its e-business site without logging in to iChain. (See Figure 2 on p. 38.)

Subcomponents of the iChain Authorization Server component use the LDAP User object to access authentication and authorization information in eDirectory. For example, the AUTHCHK.NLM uses the LDAP User object and LDAP calls to access authentication information that is stored in LDAP authentication profiles.

These authentication profiles are stored in User objects and include specialized LDAP attributes, such as the LDAP name format attribute. (The LDAP name format attribute enables users to use any LDAP attribute—such as an e-mail address or social security number attribute—as a login name.) LDAP authentication profile attributes also include two OLAC attributes, which provide Beneficial Life users with single sign-on access to multiple web servers.

ACLCHK.NLM uses the LDAP User object and LDAP calls to access information from Access Rule objects. Access Rule objects are access control lists

(ACLs) that define which users are able to access which of Beneficial Life's 20 web applications. (For more information about Access Rule objects, see the "Step 4: Create an Access Rule Object" section.)

STEP 3: CREATE AN ISO

The implementation team also used ConsoleOne to create and configure an ISO for Beneficial Life's iChain implementation. This object is the tie that binds other iChain objects and iChain components into a unified solution. iChain components and other iChain objects access this object for information.

For example, Beneficial Life's ISO contains the names and URL prefixes of each of the five web servers to which iChain controls access. This information is linked to Beneficial Life's Access Rule objects, which the Authorization Server component accesses for information about who can—and who can't—access information and applications on these servers.

This ISO also includes Beneficial Life's password policy, which applies to all users who access information and applications on these web servers. In addition, the ISO identifies the User Interface (UI) (an Oracle9i Application Server Portal) that Beneficial Life's users see when they access these web servers via iChain. (See Figure 3 on p. 38.)

The Beneficial Life ISO also includes links to the LDAP User object and the guest User object. As you know, the Authorization Server uses these objects to access information in eDirectory and to provide access to Beneficial Life's

publicly available web content. (iChain 2.0 includes the iChain Web Server Accelerator Wizard to help you configure the iChain ISO. For more information about installing and configuring iChain 2.0, visit www.novell.com/documentation/lg/ichain20.)

STEP 4: CREATE AN ACCESS RULE OBJECT

Finally, the implementation team created and configured five Access Rule objects for Beneficial Life's iChain implementation. Each Access Rule object contains a URL list, which includes the URLs to which the object controls access. Access Rule objects also include an Apply To list, which is an ACL. This Apply To list includes the User, Group, and Organizational Unit (OU) objects that define who is authorized to access the URLs on the URL list.

If a user is not represented in the Apply To list, iChain denies that user access to the URLs in the URL list. In addition, Access Rule objects include an Exception list, which enables you to deny access to users, groups, and OUs.

For example, the implementation team created an Access Rule object called *CommissionStatementRULE*. This object's URL list includes the URL for a web-based application that enables insurance agents to view their commission statements. (Like other web-based applications running on Beneficial Life's web servers, this application accesses an Oracle 8.17 database running on a Windows 2000 server.)

The *CommissionStatementRULE* object's Apply To list includes Group objects that represent independent agents and financial sales professionals. Of course, the *CommissionStatementRULE* object also includes an Exception list, which Beneficial Life can use to explicitly deny access to a particular User, Group, or OU object.

For example, suppose Beneficial Life needed to audit a particular agent's commissions and wanted to deny that agent access to his or her online commission statement until that audit was completed. Using the iChain ConsoleOne snap-in module, Beneficial Life could add this agent's User object to the *CommissionStatementRULE* object's Exception list.

Another Beneficial Life Access Rule object—the *HomeOfficeRULE* object—includes the URL for a tele-underwriting application. When you apply for a policy with Beneficial Life, a Beneficial Life cus-

In Case You Were Wondering

When users access Beneficial Life Insurance Company's intranet via iChain, the first thing they see is a login box. (See Figure 4.) The second thing these users see is an Oracle Application Server Portal, which enables these users to see only the information and applications that they are authorized to see. (See Figure 3 on p. 38.) What users don't see is the data flow within iChain.

Of course, data flow doesn't interest most users. Users are generally interested only in a convenient, fast way to access the information they need.

As a network administrator, however, you probably want to know how iChain works. Although a description of every step that iChain takes to perform its tasks is beyond the scope of this article, the following description should give you a basic understanding of how data flows through iChain from user to web server and vice-versa:

1. A user points his or her web browser to Beneficial Life's intranet site (www.benlife.com). Beneficial Life's Domain Naming System (DNS) server then resolves this URL to iChain's IP address.
2. PROXY.NLM, which is running on Beneficial Life's iChain Internet Caching System (ICS) appliance, accepts this browser's request and returns the Beneficial Life Insurance Company welcome page from iChain's proxy cache.
3. The user selects the Employees & Agents link on this page, and his or her browser requests that link.
4. PROXY.NLM accepts this browser's request and, in turn, requests the Beneficial Life site's iChain authentication cookie. (PROXY.NLM stores authentication cookies in RAM on users' computers when users authenticate to iChain.) Since this user has not yet authenticated to iChain, the user's browser does not find and return this cookie.
5. PROXY.NLM establishes a Secure Sockets Layer (SSL) connection with the browser and returns a login box. (See Figure 3 on p. 38.)
6. The user provides his or her login credentials—a Lightweight Directory Access Protocol (LDAP) username and password—which the browser returns to PROXY.NLM.
7. PROXY.NLM uses AUTHCHK.NLM, which is running on Beneficial Life's iChain Authorization Server, to verify the login credentials. To perform this task, AUTHCHK.NLM accesses eDirectory using LDAP calls. PROXY.NLM also uses another iChain Authorization Server component—OACINT.NLM—to retrieve Object-level Access Control (OLAC) parameters from Novell eDirectory. (OLAC is a protocol that enables iChain to provide single sign-on access to web-based information and applications.)
8. PROXY.NLM updates the user's authentication information in the AUTHCHK list, which is a dynamically generated table stored in RAM cache on the iChain ICS appliance. This information includes a new iChain authentication cookie and an HTTP authorization header containing OLAC parameters, which iChain uses to enable single sign-on access to web-based information and services for this user.
9. PROXY.NLM retrieves the authentication cookie from the AUTHCHK list in the iChain ICS appliance's RAM cache and sends that cookie to the user's browser.
10. PROXY.NLM again requests the authentication cookie from the user's browser. This browser then returns the authentication cookie.
11. PROXY.NLM uses this cookie and the AUTHCHK list to verify that this user is now authenticated.
12. PROXY.NLM then uses ACLCHECK.NLM, which is running on the iChain Authorization Server component, to identify the specific URLs that this user is authorized to access. Like AUTHCHK.NLM, ACLCHECK.NLM performs its task by making LDAP calls to eDirectory, wherein this information is stored.
13. PROXY.NLM records information about this user's access rights in the iChain ICS appliance's RAM cache.
14. PROXY.NLM then sends to the user's browser an Oracle Application Server Portal page containing links to the applications and information to which this user has authorized access.

Each time the user selects a link from this page, PROXY.NLM uses the information in the users' cookie and the iChain ICS appliance's RAM cache to verify that the user is authenticated and that the user is authorized to access the linked URL. If the user is authorized, PROXY.NLM either returns the requested web page from its proxy cache or requests this information from the origin web server, depending on whether or not that information exists in cache.

If access to this URL requires further authentication, PROXY.NLM accesses the AUTHCHK table in the iChain ICS appliance's RAM cache and retrieves this user's HTTP authentication header. PROXY.NLM then submits this header to the web server that is requiring authentication. ●

tomer service representative telephones you and asks you to answer medical questions. As you answer these questions, these representatives use this application to complete an online medical questionnaire.

Naturally, only Beneficial Life employees need access to this personal information. Therefore, the HomeOfficeRULE object's Apply To list includes only User, Group, and OU objects that represent Beneficial Life employees.

Beneficial Life uses another Access Rule object—the GroupPolicyholder-RULE object—to enable group insurance

policy holders to access an online e-bill application. This application enables policy holders to view and manipulate their monthly billing. Only these group policy holders have access to this application.

To give users access to Beneficial Life's public web site via its e-business site, the implementation team created an Access Rule object that lists Beneficial Life's public URL (www.beneficiallife.com). Not surprisingly, this Access Rule object's Apply To list includes only one User object: the Guest User object, which enables unauthenticated users to access this site.

FINAL STEP: INSTALL AND CONFIGURE THE ICHAIN ICS APPLIANCE

After creating Access Control objects for Beneficial Life's web-based applications and information, the implementation team installed iChain 1.5 on a Compaq ProLiant server running ICS 1.3. (This server is Beneficial Life's ICS appliance. Because iChain 2.0 includes a specialized release of ICS, you do not have to install iChain 2.0 on an ICS appliance.) The iChain installation program installed the following components on this appliance:

- iChain web-based management utility
- PROXY.NLM
- Interfaces to the Authorization Server component
- SSLizer

The installation program also configured ICS in the reverse-proxy caching mode, enabling the iChain ICS appliance to accelerate the delivery of Beneficial Life's web content. After the installation program completed its tasks, the implementation team configured an IP address, subnet mask, and gateway address on the iChain ICS appliance.

The implementation team then used the iChain web-based administration utility to perform the following configuration tasks for this appliance:

- Configured a time zone
- Configured the IP addresses of each of Beneficial Life's five web servers
- Configured the IP address of Beneficial Life's Domain Naming System (DNS) server
- Configured a private name for the iChain ICS appliance

In addition, the implementation team used the iChain web-based administration utility to provide the iChain ICS appliance with the following information:

- Fully distinguished names of Beneficial Life's ISO object, guest User object, and LDAP User object
- The LDAP User object's password
- The LDAP server's IP address

The implementation team also configured the iChain ICS appliance to use SSL when prompting users for a username and password. In addition, the implementation team provided the iChain ICS appliance with the contexts in which web-based users reside. This information enables those users to log in without having to provide their full LDAP context. (LDAP contexts are eDirectory contexts that are delimited with commas rather than periods.)

The implementation team then configured the iChain ICS appliance to accelerate web content for each of Beneficial Life's web servers and to encrypt confidential content using SSLizer. (With iChain 2.0, you use the iChain Web Server Accelerator Wizard to configure acceleration and encryption for protected resources.)

As its name implies SSLizer—which is called *Secure Exchange* in iChain 2.0—uses SSL to encrypt this web content, thus offloading compute-intensive data encryption from Beneficial Life's web servers. (SSLizer is an ICS technology that is available as Secure Excelerator through Volera. For more information about Secure Excelerator, visit www.volera.com/products/acceleration/secure.html.) That is, SSLizer enables Beneficial Life to send confidential web content—such as billing information—across the wire encrypted without having to burden its web servers. Beneficial Life's implementation of SSLizer uses a signed certificate from VeriSign to encrypt web content.

Because single sign-on access to web applications is important to Beneficial Life, the implementation team also configured the iChain ICS appliance to use OLAC to forward authentication information to its web servers.

A DONE DEAL

After the implementation team configured the iChain ICS appliance, Beneficial Life was ready to roll out its e-business site to Beneficial Life policy holders, insurance agents, and employees. To access the applications and information running on Beneficial Life's intranet through the e-business site, these users simply launch their web browsers, go to www.benlife.com, and select the Agents & Employees link. iChain then prompts these users to log in. (See Figure 4 on p. 40. For detailed information about what happens when users access iChain, see "In Case You Were Wondering," on p. 41.)

Before deploying this solution, Beneficial Life agents and group policy holders had to call a representative at Beneficial Life's corporate office to access the information that these agents and policy holders can now access through a standard web browser. Similarly, group policy holders had to call Beneficial Life's corporate office to obtain billing information. (Incidentally, Beneficial Life's e-business site is optimized for Internet Explorer 5.0 and above and is compatible with Netscape Navigator 4.7 and above.)

Because these agents and policy holders can now access this information for themselves, Beneficial Life is saving on the number of employees required to answer requests for information. According to Beneficial Life web services team lead Russ Newman, Beneficial Life is also

benefiting from increased employee, agent, and policy holder satisfaction.

Over the past few years, Beneficial Life has been conducting surveys among employees and agents to gauge employee and agent satisfaction in regards to their ability to get needed information. "Satisfaction among these groups has gone up drastically" since Beneficial Life deployed its e-business site, Newman reports.

Although Beneficial Life could more easily calculate the ROI for its e-business solution in terms of the time this solution saves employees, user satisfaction is demonstrably valuable to Beneficial Life. After all, Beneficial Life regularly monitors user satisfaction.

CONCLUSION

Of course, Beneficial Life also values iChain's security features, although attaching an ROI to those features would be difficult (if not impossible). (See "Security ROI Calculations Pose Challenges for Users," *Computerworld*.) In fact, Beneficial Life would probably not have even considered implementing its e-business solution if that solution had not included tight security. Because security is built in to Beneficial Life's iChain-based e-business solution, Beneficial Life probably spent less on that security than it would have if it had added security after the solution was in place.

In addition, Beneficial Life's e-business solution is more secure than it might have been if Beneficial Life had implemented an after-the-fact security solution (such as a firewall) alone. Since Novell access and security solutions are interoperable, Beneficial Life can also add layers of security to this solution by deploying additional access and security solutions.

For example, Beneficial Life could add NMAS to its e-business solution. NMAS would enable the company to require graded authentication to confidential information. (For information about how the Taipei County Government is using NMAS to enable graded authentication on its network, see "Taipei County Government Secures Access to Its Assets" on p. 24.) In other words, Novell access and security solutions go a long way toward mitigating the inherent security risks of attaching confidential and valuable information to a network without threatening Beneficial Life's bottom line.

Cheryl Walton works for Niche Associates, a technical writing and editing agency. ●