Securing an IIS Web Server Using Novell's iChain

Submitted By: Jeff Hermans

February 3, 2005

GIAC Security Essentials Certification - GSEC Practical Assignment v1.4c

Option 1: Research on Topics in Information Security

Table of Contents

Table of Figures

Summary

Web servers are open to many threats just by the nature of their exposure to the Internet. Although the inherent security built into web server products is improving, adding unique layers to the security design proves to be successful in almost any implementation. The addition of multiple "best of breed" solutions can also assist with lowering the risk factor of someone breaking through these barriers. Reverse proxies are one of the ways to accomplish that. This paper will step through the design process, reasons behind the design chosen as well as the recommendations of securely implementing Novell's reverse proxy, iChain, to secure a web server. Providing basic steps to get a web server online and front-ending it with iChain is outside the scope of this document. I will however discuss the in-depth details of properly securing the iChain proxy server itself and the details of getting the proposed design to work securely.

Background

Most web servers are exposed to many threats because they are available to almost anyone on the Internet. The risk of these potential threats can be minimized by lowering the vulnerability of the web server. Typical web server implementations include the web server being placed in a Demilitarized Zone (DMZ) behind a firewall. While this provides a significant amount of protection for the web server, it may still be too visible to someone attempting to circumvent the security of the design. New vulnerabilities and exploits are being exposed rapidly and simply restricting access to a web server over HTTP and HTTPS may not be sufficient. Additional levels of protection may be needed and taking advantage of a reverse proxy device can increase the protection of a web server.

What is a Reverse Proxy?

A reverse proxy is a device that logically sits in front of an organization's web servers. The reverse proxy communicates on behalf of the web client to the web server. All web based communications must pass through the reverse proxy prior to being sent to the actual web server. This prevents the web client from actually having direct access to the web server. Keep in mind that reverse proxies are not meant to replace firewalls since they typically only handle HTTP and HTTPS traffic.

Benefits of a Reverse Proxy

The reverse proxy device can provide additional benefits over simply placing a web server behind a firewall.

- Caching: Most reverse proxy devices can cache static information from a web server. This can reduce the load that the web server has to respond to. If the data that the reverse proxy has cached has not been modified since the time it stored the content, the reverse proxy simply responds to the client instead of the web server having to do it. Depending on the amount of dynamic content that the web server is providing, this can reduce the load on the web server and increase response time dramatically.

- SSL Offloading: Some reverse proxy devices are designed with cryptography in mind. These devices are built to handle the processing power that Secure Socket Layer (SSL) demands. Many times the computational overhead associated with providing SSL from a web server can limit its capacity. Reverse proxies that provide SSL capabilities may allow this service to be handled by the reverse proxy and removed from the web server. It is important to ensure that the communications path between the reverse proxy and the web server is secure.
- Added Protection: Almost all web servers identify the vendor and version information of the web server in the Header of the HTTP response back to the web client. This information can be quite valuable to an attacker by more efficiently determining which exploits to use on the target web server. A reverse proxy can hide or obscure this Header information. Further details on HTTP Headers can be found in the "iChain and the Web Server Header Information" section later in this document.

Novell's iChain includes some additional security benefits over just placing another web server configured as a reverse proxy in front of the back-end web server. iChain does not allow HTTP requests directly to the IP address of the reverse proxy server. Instead, it requires that a valid DNS name be used in the request and iChain validates that DNS name before allowing the request through to the web server. iChain also provides the ability to require user authentication as well as authorization by determining if the user has the appropriate rights to access the content on the web server.

iChain and the Web Server Header Information

Making an HTTP request to a web server presents the client with valuable information about that web server. Attackers can use this information to determine what operating system and web server version is being used. This is known as fingerprinting the web server. Sending an HTTP GET request to the root of the website presents the following information:

```
HTTP/1.1 200 OK
Content-Length: 321
Content-Type: text/html
Content-Location: http://./Default.htm
Last-Modified: Fri, 28 Jan 2005 01:37:02 GMT
Accept-Ranges: bytes
ETag: "40ae3ddd94c51:1f6"
Server: Microsoft-IIS/6.0
Date: Fri, 28 Jan 2005 16:34:45 GMT
Connection: close
```

As shown, it is quite easy to see the type and version of web server being used. In this case you can immediately tell that it is running Microsoft's Internet Information Services (IIS) version 6.0. With this information an attacker can fine tune their attack to just vulnerabilities related to IIS version 6.0 and not waste time with other web server types.

This same web server placed behind an iChain reverse proxy server only presents the following information:

```
HTTP/1.0 302 Moved Temporarily
Content-Length: 175
Location: https://www.abc-corp.net/
```

Since the HTTP response from iChain is a redirect to the secure HTTPS page, looking at the HTTPS response presents the following information:

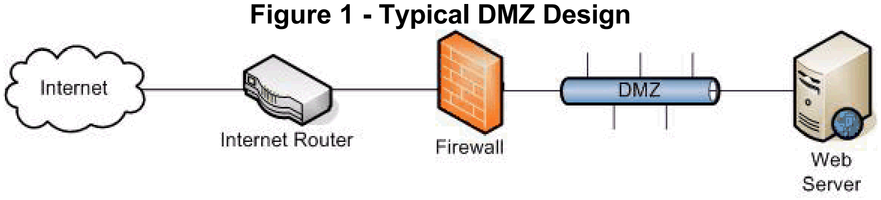
```
HTTP/1.0 302 Found
Content-Type: text/html; charset=utf-8
Content-Length: 1535
Pragma: no-cache
Location: https://www.abc-corp.net/ICSLogin/?"https://www.abc-corp.net/"
```

As shown above, it is much more difficult to determine the type and version of the web server; although the Location line with the ICSLogin URL may give away that it is front-ended by an iChain server. While it is possible to configure each and every web server to mask this header information, placing a properly configured reverse proxy in front of the entire web infrastructure guarantees that the back-end web server Header information remains hidden.

Design

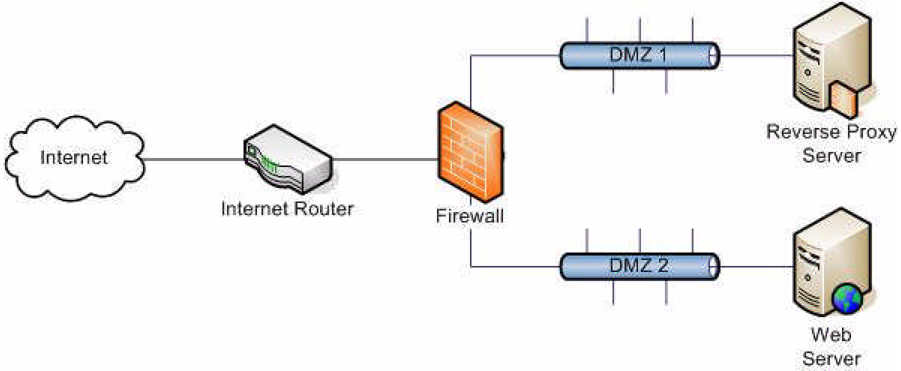
As mentioned earlier, many web infrastructure designs place the web servers behind a firewall (see Figure 1). This allows a certain degree of protection for the web server by typically restricting the communication paths allowed from both the outside world to the web server.

Figure 1 - Typical DMZ Design



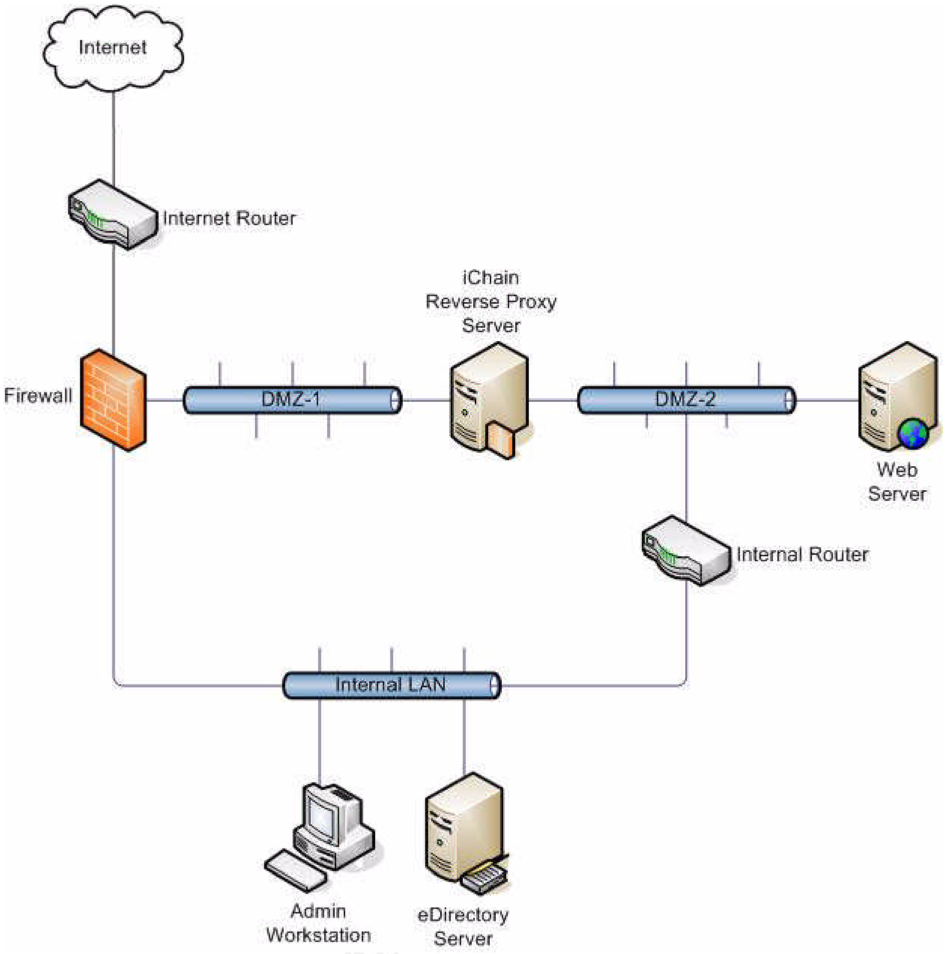
In addition to the firewall, implementing a reverse proxy server logically in front of this same web server can provide additional security; however if another device within the DMZ is compromised, direct access to the web server may be available. This would include all available services running on the web server. This is also the case even if a separate DMZ is created for the reverse proxy and another for the web servers they are protecting as shown in Figure 2.

Figure 2 - Separate DMZ with a Reverse Proxy



The design I have chosen incorporates the recommended defense in-depth method of using multiple layers to protect a resource. As shown in Figure 3, the web servers will be placed physically behind the reverse proxy server. This prevents web clients from going around the reverse proxy and accessing the web server directly.

Figure 3 - Web Server Behind a Reverse Proxy



Although the web traffic will need to traverse through the reverse proxy server to get to the back-end web server, routing will not be allowed through the reverse proxy. Additional details on this can be found in the Routing section of this document. Since the reverse proxy server and the web server will still need to be accessed for administration, a router was added to the design to allow limited access from the internal network to DMZ-2. This communications will be restricted through the use of access lists on the router. Many of the benefits of implementing a reverse proxy can also be accomplished through properly configuring the web server as well as controlling access to the web server with a firewall. However, in addition to the benefits previously mentioned, this design also provides:

- Reduced load on the firewall. This is because many of the required back-end communications can occur without going through the firewall. This includes reverse proxy server to web server communication, administrative management as well as web server to back-end database communications.
- Another layer of security.

Products Used

The products used in this design include Novell's iChain version 2.3 with Support Pack 1 installed as the reverse proxy server. The back-end Lightweight Directory Access Protocol (LDAP) server that iChain authenticates users to is a Windows 2000 server with Service Pack 4 running Novell's eDirectory version 8.7.3. The back-end web server is a Windows 2003 Standard Edition server with Internet Information Services (IIS) 6.0. The router used to control access to DMZ-2 from the Internal LAN is a Cisco router.

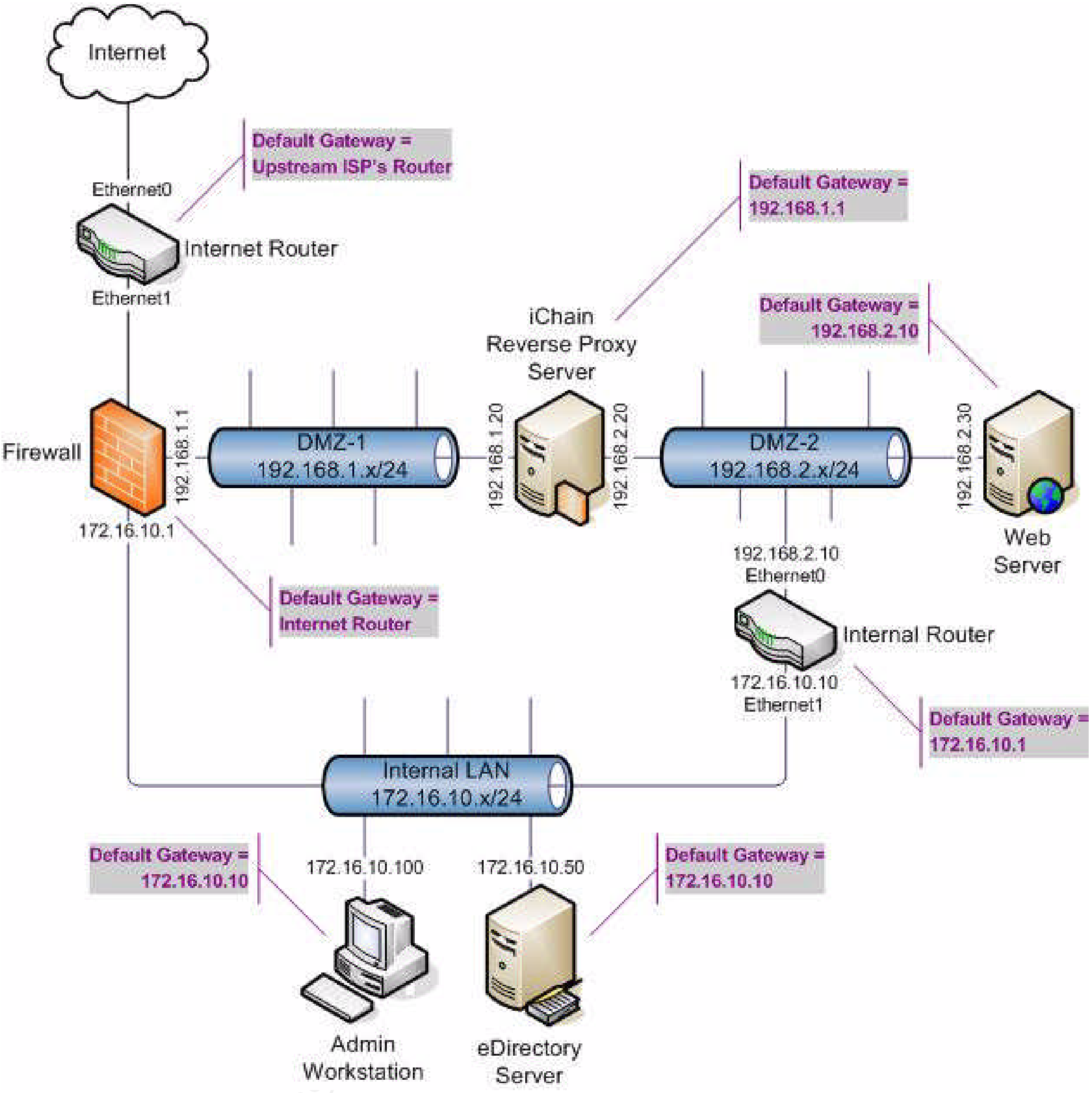
Routing

The iChain server will be used to secure web servers for both Internet clients and internal users. It will also need to communicate with an internal LDAP server for user authentication and authorization. It is critical to the functionality of the design that the iChain proxy server understands the correct routing paths. Details of the iChain routing configuration can be found in the Default Routes section of this document. The iChain proxy server however will not be configured to route between its two interfaces. This is disabled to prevent devices in DMZ-1 from routing through the iChain server to DMZ-2. Make sure routing is disabled on the iChain proxy server by going to the Network | Gateway/Firewall screen and confirming that the "Act as a router" option is not selected.

Default Routes

For routing to work properly on all devices it is important that each device's Default Gateway knows the next hop to take to get to the desired destination. Figure 4 shows the Default Gateway/route for each device as well as the addresses used in the design.

Figure 4 - Default Routes and Detailed Design

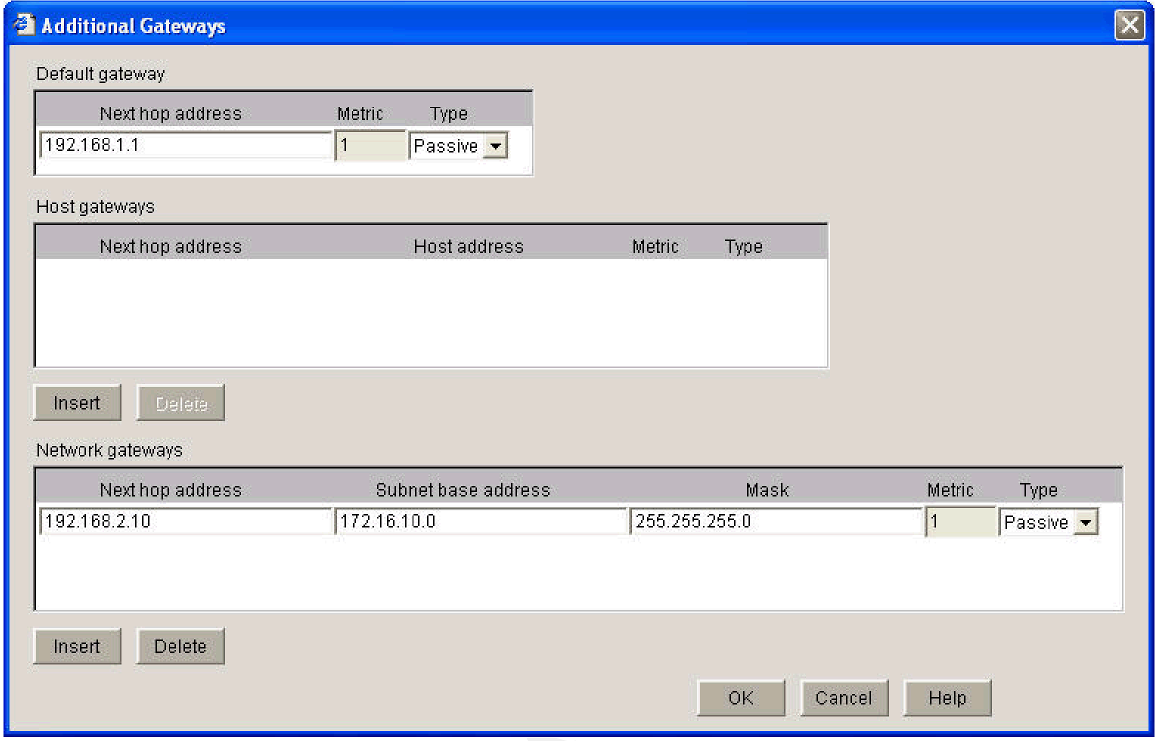


Typical routing within an organization includes the Internet Router having a default gateway of the Internet Service Provider's (ISP) router. The Firewall will then have a default gateway of the Internet Router. The Internal Router will have a default gateway of the Firewall. This chain of default routes will allow all devices using the Internal Router as their default gateway to access the Internet properly.

Since most of the communications for the iChain proxy server will be with clients on the Internet, the default route for it should be the Firewall in DMZ-1 (192.168.1.1). To allow the iChain proxy server to communicate with the back-end LDAP server and the Admin Workstation, a static route (also known as a Network Gateway) is added to the iChain server. This is done through the iChain Administration web GUI on the Network | Gateway/Firewall page. Click on the Additional Gateways button and add the route as shown below in Figure

5.

Figure 5 - iChain Static Route



Default gateway

Next hop address	Metric	Type
192.168.1.1	1	Passive

Host gateways

Next hop address	Host address	Metric	Type

Network gateways

Next hop address	Subnet base address	Mask	Metric	Type
192.168.2.10	172.16.10.0	255.255.255.0	1	Passive

Since the iChain server will now go through DMZ-2 and the Internal Router to communicate with the internal users, I needed to find a way to allow internal users to still access the website through DMZ-1. The new routing configuration on the iChain proxy server will not allow this. Instead I used a NAT address on the firewall to hide the source address of all internal users. This causes the iChain server to think it's communicating with an address on the firewall and not with a workstation on the internal network. The firewall then takes care of routing the packets to the appropriate workstation on the internal network.

Almost all of the communications for the back-end web server will be with the iChain proxy server on the same network so no additional route on the web server is needed. However, for administration of the web server from the internal network and to allow the web server to communicate with any back-end database servers on the internal network, the web server will use the Internal Router as its default gateway.

Implementation

The steps involved with implementing a secure web infrastructure can be summarized within the following topics:

- Hardening the Windows 2003 Standard Server host operating system
- Securing the IIS 6.0 web server

- Hardening the iChain reverse proxy server
- Securing the communication pathways

Hardening the Windows 2003 Host Operating System

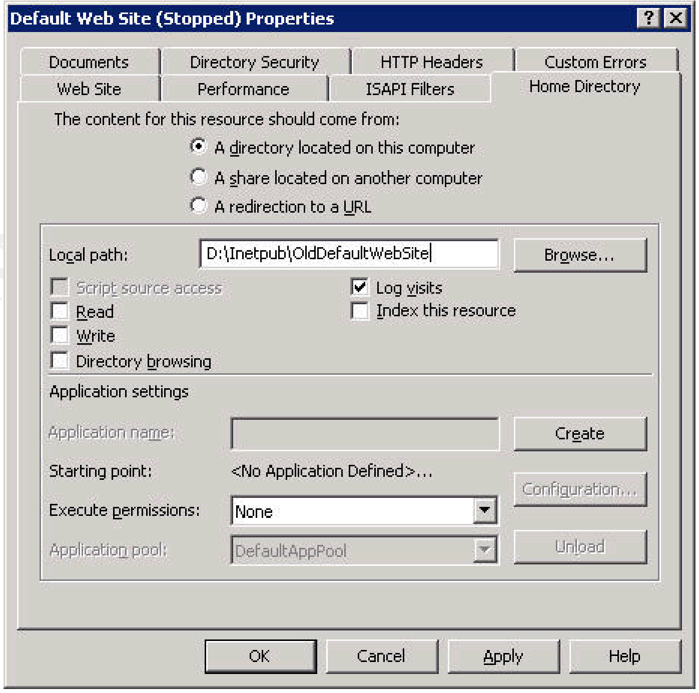
Before installing the IIS web server, you must make sure that the underlying host operating system is secure. This starts with making sure all the latest patches are applied to the operating system, enforcing secure passwords on accounts, disabling unused accounts and stopping unneeded services that are running on the server. Microsoft lists the recommended service startup types for a dedicated web server at http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/iisdg_sec_rmkz.asp

Securing the IIS 6.0 Web Server

IIS 6.0 is more secure out of the box than in previous versions. It is no longer installed by default with the operating system. Instead it requires that you install IIS after the base operating system and it is installed with very limited services enabled. This helps to minimize vulnerabilities immediately.

When securing an IIS 6.0 web server, some of the recommended tasks to perform include formatting all drives on the system using NTFS, installing IIS on a separate drive from the operating system and securing the Default Web Site as shown in Figure 6. This is accomplished by stopping the Default Web Site, disabling all permissions, unselecting the Read right and changing the Local Path to an unused directory other than the default "wwwroot" directory.

Figure 6 - Disable the IIS Default Web Site



Default Web Site (Stopped) Properties

The content for this resource should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: D:\Inetpub\OldDefaultWebSite

☐ Script source access
☐ Read
☐ Write
☐ Directory browsing
☑ Log visits
☐ Index this resource

Application settings

Application name:

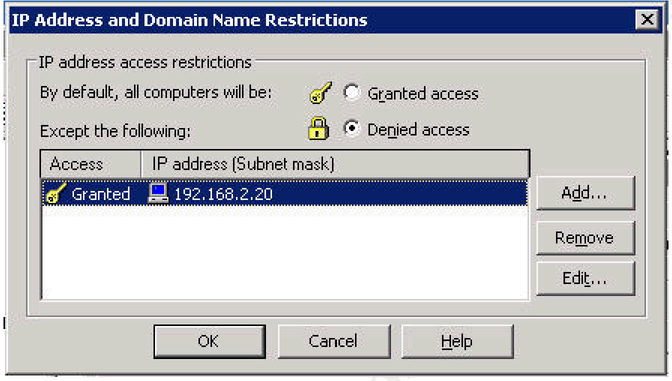
Starting point: <No Application Defined>...

Execute permissions: None

Application pool: DefaultAppPool

One item that should be configured in this design is to restrict access to the website only from users going through the iChain proxy server. This is configured using the Internet Information Services (IIS) Manager. Go to the properties of the website, select the Directory Security tab and click on the Edit button of the "IP address and domain restrictions". Add the IP address of the iChain server's interface that is in DMZ-2 (192.168.2.20) as shown in Figure 7 below.

Figure 7 - IIS IP Address and Domain Restrictions



IP Address and Domain Name Restrictions

IP address access restrictions

By default, all computers will be: ○ Granted access ● Denied access

Except the following:

Access	IP address (Subnet mask)
Granted	192.168.2.20

After this is configured, anyone attempting to access the web server directly using HTTP will get a 403.6 Forbidden error stating that they are not authorized to view the page because the IP address of the client has been rejected.

Microsoft also provides an overall security guide for Windows 2003 and all of the services Windows 2003 server provides. The guide can be downloaded from Microsoft's website found at: http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

Hardening the iChain Server

iChain reverse proxy servers are basically pre-hardened NetWare servers that are fine tuned for caching and cryptography. While most of the services are restricted by default, the following items will tighten the iChain proxy server even more.

- Turn off the ability to administer the iChain proxy server on the interface facing the Internet (192.168.1.20). Administration should only be allowed on the back-end interface (192.168.2.20). This is configured within the iChain Administration GUI on the System | Admin ACL screen.
- Restrict administration of the iChain proxy server to only addresses of administrator workstations. In this design I will only allow administration from the Admin Workstation (172.16.10.100). This is also configured within the iChain Administration GUI on the System | Admin ACL screen. Select the "Allow administration from specified clients" setting and add in the administrator's workstation address.

- Telnet is disabled by default and should not be enabled for administration since the transmission of the data is in clear text. Someone with a packet sniffer may intercept the communications and gain access to the iChain configuration information including passwords.
- A number of services respond by default on an iChain proxy server even though the service may have been disabled on an interface. For example, Telnet is disabled by default, however port 23 (Telnet) still shows up in a port scan of the Internet facing interface along with a few other ports listed below:

Responding Port:	**Service:**
23	Telnet
80	HTTP
443	HTTPS
1958	iChain Administration *Note: iChain 2.3 Support Pack 1 now disables this service/port from advertising if the Admin ACL is not selected for this interface.*
1959	iChain Administration *Note: iChain 2.3 Support Pack 1 now disables this service/port from advertising if the Admin ACL is not selected for this interface.*

Ports 80 (HTTP) and 443 (HTTPS) are required for iChain to proxy the web servers it is protecting; however, even though Telnet and the iChain Administrative ports have been disabled and do not actually function, iChain still has listening services on these ports. To prevent these services from advertising on the interface we need to filter the unwanted ports by using the underlying NetWare utility FILTCFG.NLM.

The following instructions will step through the process of using FILTCFG to restrict the Telnet service from responding on iChain's Internet facing interface (192.168.1.20).

1. From the iChain Proxy Server console, go into the debug mode by typing "DEBUG" followed by the password "PROXYDEBUG".
2. Press Ctrl+Esc to get a listing of current screens.
3. Select option one "System Console".
4. Type "INETCFG" to enter into the Internetworking Configuration screen.
5. Select Protocols.
6. Select TCP/IP from the Protocol Configuration screen.
7. Scroll down and select Filter Support.
8. Change this setting to Enabled.
9. Press Esc and select Yes to Update TCP/IP Configuration.
10. Press Esc until you are back to the main Internetworking Configuration

screen.

11. Select Reinitialize System and select Yes to continue.
12. Reinitializing the system returns you back to the System Console. Type "FILTCFG" to enter into the Filter Configuration screen.
13. Select "Configure TCP/IP Filters".
14. Select "Packet Forwarding Filters" from the TCP/IP menu.
15. Change the Status to Enabled.
16. Select "Filters: (List of Denied Packets)" from the Packet Forwarding Filters menu.
17. Press Ins to insert a new filter.
18. Select the Destination Interface and choose the interface on the iChain proxy server that faces the Internet. This is the interface that the web accelerators run on.
19. Select the Packet Type, scroll down and select "telnet".
20. Press Esc and Yes to save the filter.
21. Continue to press Esc until you exit the Filter Configuration screens and return to the System Console.

After enabling the filter, the only ports that responded to the port scan were ports 80 and 443 as expected.

Securing the Communication Channels

To reduce the risk of an attacker intercepting the web traffic between the iChain proxy server and the web client, iChain's Secure Exchange should be enabled to encrypt the traffic using SSL. This is enabled individually on each web accelerator on the Configure | Web Server Accelerator page by modifying the web accelerator and selecting Enable Secure Exchange.

The web traffic between the iChain proxy server and the back-end web server can also be encrypted using SSL. This is optional and should be enabled if your organization requires a higher level of security. This is also configured on each web accelerator on the Configure | Web Server Accelerator page by modifying the web accelerator, selecting the Secure Exchange Options button and checking the "Enable secure access between the iChain Proxy and the Origin Web Server" box. The web server's SSL certificate will need to be imported into the Trusted Root container specified by the iChain Service Object in eDirectory.

The LDAP authentication and authorization traffic should also be encrypted since usernames and password information would be transmitted in clear text to the eDirectory server if not encrypted using SSL. This is configured on the Configure | Authentication page, modifying the LDAP Authentication profile, select the LDAP Options button and select "Enable secure access to LDAP server". Secure Authorization is enabled by going to the Configure | Access Control page and selecting the "Enable secure access to LDAP server". As with the web server certificate, the eDirectory LDAP certificate will need to be imported into the Trusted Root container in eDirectory specified by the iChain Service Object.

One thing to keep in mind is that the administration of iChain cannot be done over an encrypted communications path. The only two options available are to use Telnet or the web based Administration GUI. Neither method provides a secure pathway to manage iChain. As mentioned in the "Hardening the iChain Server" section, it is recommended to restrict administration to only the Admin Workstation. This is configured on the System | Admin ACL page by selecting "Allow administration from specified clients" and entering in the address of the Admin Workstation. Although it does not guarantee that an internal hacker couldn't spoof the Admin Workstation's address, it does lower the risk.

Firewall Rules and Router Access Control Lists

To restrict access to the iChain reverse proxy server and the web server, rules have to be added to the Firewall as well as access lists on the Internal Router. The following tables summarize the traffic that should be allowed for this design to function.

Firewall Rules:

Source:	Destination:	Service:	Port(s)	Notes:
Any	192.168.1.20	HTTP HTTPS	80 443	Web traffic from the Internet and Internal LAN allowed to the iChain server

Router Access Control Lists:

Source:	Destination:	Service:	Port(s):	Notes:
192.168.2.20	172.16.10.50	LDAPS	636	Secure LDAP authentication to eDirectory
192.168.2.20 192.168.2.30	172.16.10.100	SYSLOG	514	SYSLOG reporting from iChain and the Web Server to the Administration Workstation
172.16.10.100	192.168.2.20	iChain Administration	1959 2222 51100	iChain administration from the Administration Workstation

To restrict the communications to and from DMZ-2, access lists are added to the Internal Router. The Cisco specific commands are listed below. These commands require you to enter into the "enable mode".

```
1.  configure terminal
2.  access-list 101 permit tcp host 172.16.10.100 host 192.168.2.20 eq 1959
3.  access-list 101 permit tcp host 172.16.10.100 host 192.168.2.20 eq 2222
4.  access-list 101 permit tcp host 172.16.10.100 host 192.168.2.20 eq 51100
5.  access-list 101 permit icmp host 172.16.10.100 host 192.168.2.20
6.  access-list 101 permit tcp host 172.16.10.50 host 192.168.2.20 established
7.  access-list 101 deny ip any any
8.  access-list 102 permit tcp host 192.168.2.20 host 172.16.10.50 eq 636
9.  access-list 102 permit udp host 192.168.2.20 host 172.16.10.100 eq 514
10. access-list 102 permit udp host 192.168.2.30 host 172.16.10.100 eq 514
11. access-list 102 permit icmp host 192.168.2.20 host 172.16.10.100
12. access-list 102 permit tcp host 192.168.2.20 host 172.16.10.100 established
13. access-list 102 deny ip any any
14. interface e0
15. ip access-group 102 in
16. interface e1
17. ip access-group 101 in
18. end
```

A breakdown of each line is as follows:

- Line 1 enters into the configuration mode.
- LDAPS Authentication:
    - Line 8 allows the iChain proxy server to communicate to the eDirectory server over secure LDAP.
    - Line 6 allows the return LDAPS traffic from the eDirectory server back to the iChain proxy server.
- SYSLOG Monitoring:
    - Lines 9 and 10 allow both the iChain proxy server and the Web Server to send SYSLOG alerts to the Admin Workstation.
    - The iChain proxy server requires that it can ping the SYSLOG server prior to sending the alert. Lines 5 and 11 allow the ping to work.
- iChain Administration:
    - Lines 2 through 4 allow the Admin Workstation to configure the iChain proxy server using the Administration Web GUI.
    - Line 12 allows the return administration traffic from the iChain proxy server back to the Admin Workstation.
- Deny all other traffic:
    - Line 7 denies all other traffic from the internal network to DMZ-2.
    - Line 13 denies all other traffic from DMZ-2 to the internal network.
- Apply access lists:
    - Lines 14 and 15 apply the appropriate access list to the router interface in DMZ-2.

  - Lines 16 and 17 apply the appropriate access list to the router interface on the internal network.
  - Line 18 completes the configuration.

Other Considerations

One of the downsides of tightening the security of a design is that some functionality that was available before may now be inaccessible. Since most of the paths for administrating and updating the iChain and web servers have been blocked or restricted, how do we go about managing those devices? Every environment is unique and the organization will have to weigh the pros and cons of the security risks involved with each option.

Options for Managing the Secured iChain and Web Servers

Web administrators may use FTP to update the content on the web server. If that is deemed too much of a security risk, another option might be burning a CD with the updated site and copying it to the web server if the developers have physical access to the web server's console. Updates to the login, logout and error pages of the iChain proxy server could be handled in the same manner. Use the TOOLBOX.NLM included with iChain and the COPY command.

Other Services

Other services that may be needed and therefore have to be allowed through the Internal Router's access lists may include:

- Network Time Protocol (NTP) to ensure that the system clocks on the iChain proxy server and the web servers are in sync. This is critical for logging to ensure proper time stamps. The NTP server would most likely be on the internal network; however the Internal Router could also be used as an NTP server for the devices in DMZ-2.
- Structured Query Language (SQL) may be required by a web application running on the web server. The SQL server might be either in DMZ-2 or on the internal network.
- Windows Update Service (WUS) to ensure that the Windows based web servers have the latest patches applied to them. The WUS server would be on the internal network.

Conclusion

A reverse proxy server can provide many benefits to an organization's web infrastructure in addition to enhanced security. The defense in-depth design provides a higher level of security than just relying on an individual device to protect everything behind it. With this design in place, an attacker would have to break through multiple, unique check points of security to gain access to the web server.

1. Internet Router's access lists
2. Firewall rules
3. iChain reverse proxy server authentication and authorization
4. Host security on the web server

Since security is only as good as the weakest entry point, the key thing to remember is to make sure that each device within the design is configured as securely as possible.

References

"Novell iChain 2.3 (SP2) Documentation." Novell, Inc. January 28, 2005
<http://www.novell.com/documentation/ichain23/index.html>

"Port Numbers." Internet Assigned Numbers Authority – IANA. January 27, 2005
<http://www.iana.org/assignments/port-numbers>

"Checklist: Securing Your Web Server." Microsoft Corporation. January, 2004
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod104.asp>

Lima, Joe "Mask Your Web Server for Enhanced Security." port80 Software. March, 2004
<http://www.port80software.com/support/articles/maskyourwebserver>

Kurt Dillard, Jose Maldonado and Brad Warrender "Windows Server 2003 Security Guide." Microsoft Solutions for Security. April 23, 2003
<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx>

Tulloch, Mitch "Inside IIS 6." O'Reilly – WindowsDevCenter. March 2, 2004
<http://www.windowsdevcenter.com/pub/a/windows/2004/03/02/inside_iis.html>

Stricek, Art "A Reverse Proxy Is A Proxy By Any Other Name." SANS InfoSec Reading Room. January 10, 2002
<http://www.sans.org/rr/whitepapers/webservers/302.php>

"Access Control Lists: Overview and Guidelines." Cisco. April 2, 2004
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfacls.htm>

"NetWare 6 Documentation: How to Run FILTCFG." Novell, Inc. October, 2001
<http://www.novell.com/documentation/nw6p/filtrenu/data/hq768iej.html>