



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957 Fax: 919.217.5769
<http://www.mercurionsystems.com>

USING APACHE TO REVERSE PROXY SHAREPOINT PORTAL SERVER 2001

Products: Apache 2.0.49; SharePoint Portal Server 2001

Overview

Microsoft SharePoint Portal Server 2001 relies upon Internet Information Server 5.0 (IIS 5.0) to provide web-based applications to browser clients. As a result, SharePoint shares all of the weaknesses of IIS, including potential security weaknesses. As with many other applications that rely upon IIS, deploying a reverse proxy in front of the IIS server to block web-based attacks and vulnerabilities is a common practice.

This technical document describes how to deploy Apache 2.0 as a reverse proxy in front of SharePoint Portal Server 2001, and in so doing gain some additional security and functionality.

More Information

The configuration described in this document was built based on a couple of criteria. These criteria are described below.

1. The configuration had to support SSL encryption between the browser and the proxy. Due to the nature of SharePoint Portal Server 2001, it would be impossible to terminate the SSL connection at the reverse proxy and use clear-text HTTP between the proxy and the SharePoint server, so this configuration needed to support SSL bridging (the establishment of a new SSL connection between the reverse proxy and the final destination server).
2. The configuration has to support other web-based applications on other URLs using the same hostname. For example, the hostname "extranet.domain.com" is used in the configuration described in this document. Instead of proxying the entire URL space (/), this configuration needed to proxy only the OWA-specific URLs. This left other URLs open for other web-based applications or content.
3. The configuration had to support multiple name-based virtual hosts, so that other URLs could also be proxied through the same reverse proxy server.

Based on these criteria, Apache 2.0 was installed and configured on a system running Red Hat Linux 9.0. For additional security, iptables was configured to only allow the appropriate traffic to/from the Internet and the server running SharePoint Portal Server 2001 (specifically, HTTP and HTTPS).

SharePoint Portal Server 2001 had already been configured for extranet access and SSL support, as described in the related technical documents listed in the "Related Articles/Resources" section of this document.

A partial listing of the appropriate httpd.conf file for Apache is found below. Most of the configuration has been omitted for brevity; only the pertinent portions, such as the virtual host configuration and the proxy directives, are included. All IP addresses and fully qualified domain names (FQDNs) have been randomized and are not actual or valid entries.

```
NameVirtualHost 1.2.3.4:80
NameVirtualHost 1.2.3.4:443
ProxyRequests Off

<VirtualHost 1.2.3.4:443>
    ServerAdmin webmaster@domain.com
    ServerName extranet.domain.com
    DocumentRoot /var/www/extranet

    ProxyRequests Off
    ProxyPreserveHost On

    SSLEngine On
    SSLProxyEngine On
    SSLCertificateFile conf/extranet-ssl-cert.pem

    <Location /workspace>
        ProxyPass https://extranet.domain.com/workspace
        ProxyPassReverse https://extranet.domain.com/workspace
        SSLRequireSSL
    </Location>

    <Location /msoffice>
        ProxyPass https://extranet.domain.com/msoffice
        ProxyPassReverse https://extranet.domain.com/msoffice
        SSLRequireSSL
    </Location>

</VirtualHost>
```

There are several key components to this configuration.

- **NameVirtualHost:** The NameVirtualHost directive enables Apache to use name-based virtual hosts on the specified IP addresses and ports. The parameter to the NameVirtualHost directive must match one of the VirtualHost definitions, as shown in the sample configuration, or else the content will be served from the default virtual host (the first virtual host listed in the configuration). Note that if the Apache reverse proxy will not be using name-based virtual hosts (using IP address-based virtual hosts instead or running only a single server instance), this directive is not required.
- **ProxyPreserveHost:** This directive configures Apache to pass the original Host header, supplied by the client, to the server to which the request is being proxied. (This is instead of the host name supplied in the ProxyPass directive.) Due to the nature of SharePoint Portal Server 2001, the same hostname has to be used throughout the entire process, from client browser to reverse proxy to final destination server.
- **SSLProxyEngine:** This directive enables the termination of an SSL connection at the reverse proxy (the secured connection between the client browser and the reverse proxy), and then

the establishment of a new SSL tunnel between the reverse proxy and the destination web server (note the use of “https://” in the ProxyPass and ProxyPassReverse directives).

In production, this Apache configuration could be bolstered with additional modules to add security. For example, mod_security offers the ability to block URLs based on pattern matching, regular expressions, and more.

Other Notes

None

Related Articles/Resources

The technical document titled “Converting Certificate Formats using OpenSSL” provides additional information on converting certificates into PEM format for use by Apache.

The technical documents titled “Enabling FQDNs on SharePoint Portal Server” and “Enabling SSL on SharePoint Portal Server” provide additional guidance on the correct configuration of SharePoint Portal Server 2001 for extranet (external) access.

Numerous Internet-based resources (too numerous to list here) are also available to assist in the configuration of Apache and related modules.

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.