Documentation & Instructions

SSL Connection Issues using Microsoft ISA Server

Issue

Users behind a Microsoft ISA server had issues with navigating SSL (or HTTPS) based web sites. These issues included slow response time, DNS errors, and timeouts. Normal web browsing (non SSL sites) did not experience any issues.

Cause

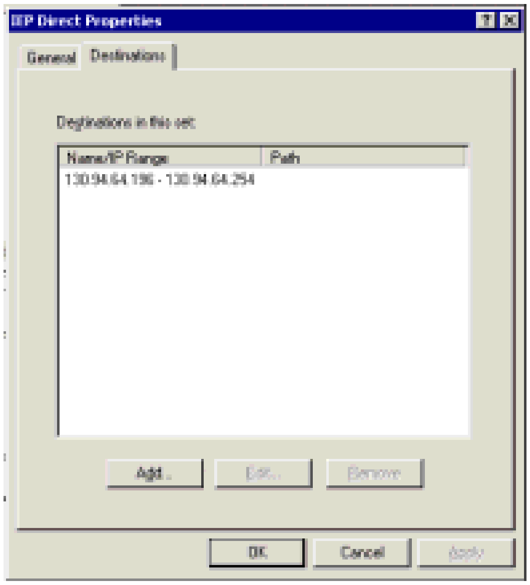
Proxy servers by default cause workstations to interact with the Internet in a different fashion than a device that is not behind a proxy. A proxy server typically “tunnels” all Internet traffic (http, https, ftp, other) over the same port on an internal network (example: port 8080). In order to do this with SSL enabled web sites Microsoft ISA server uses something called SSL tunneling. Most of the time SSL tunneling is effective and does not cause any issues. The likely reason is that most web sites do not use “full time” SSL based connection. Many just encrypt the initial login process. Any site that does employ a “full time” SSL based connection will experience difficulties using SSL tunneling.

Resolution

Since SSL tunneling is an issue it must be disabled. The alternative is to use SSL bridging. It causes a workstation behind a proxy server to operate more like it was not actually behind a proxy server.

To disable SSL tunneling and then enable SSL bridging on Microsoft ISA server do the following:

1. Open up the ISA Management MMC
2. Create a Destination Set with the IP range or domain name of the site that is having issues (Destination Sets are stored in the Policy Elements section). Contact Centris Group (IEPDirect Support) for this information.

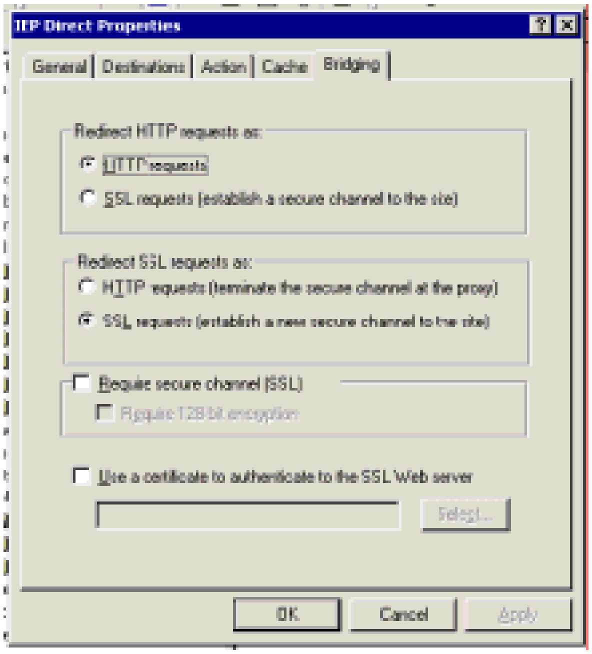


Destinations in this set:

Name/IP Range	Path
130.94.64.196 - 130.94.64.254	

3. Create a Routing Rule for the Destination Set that was just created (Routing Rules are located in the Network Configuration section). This routing rule will disable SSL tunneling and enable SSL bridging just for connections to the specified entry place in the Destination Set. In the Routing Rule be sure the following is set:

   a. Under the “Destinations” tab be sure to select the Destination Set that was created earlier.
   b. Under the “Action” tab leave everything default.
   c. Under the “Cache” tab make sure the the “No content will ever be cached” radio button is highlighted
   d. Under the “Bridging” tab be sure that the “Redirect SSL requests as:” section has the “SSL requests” radio button highlighted.



Redirect HTTP requests as:

● HTTP requests
○ SSL requests (establish a secure channel to the site)

Redirect SSL requests as:

○ HTTP requests (terminate the secure channel at the proxy)
● SSL requests (establish a new secure channel to the site)

□ Require secure channel (SSL)
□ Require 128-bit encryption

□ Use a certificate to authenticate to the SSL Web server

NOTE: These instructions also disable web caching for the specific destinations. Typically SSL based web connections are never cached, however this is the recommended setting. Also, it is possible to make the above changes on the “Default Routing Rule” so that these settings apply to all outbound connections. In some cases it may be best to do this. Sufficient testing is recommended.

More Information

SSL bridging and tunneling explained:
http://www.isaserver.org/tutorials/Understanding_SSL_bridging_and_tunneling_within_ISA.html

More information on SSL bridging:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/isa/proddocs/isadocs/cmt_sslauth.asp

Document prepared by Bill Evans - Systems Engineer, Bethpage UFSD