

Re: Cannot browse SSL pages

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2006-02/msg00123.html>

- *From:* Mourad <Mourad@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 9 Feb 2006 07:20:28 -0800
-

OK I think you misunderstood me :)

This is my scenario, it is really simple:

LAN (internal network) <----> ISA 2004 Server <-----> Internet

All i need to do is to be able to browse the internet from the LAN. It works for http websites but not https.

I hope this helps.

Thanks,
Mourad.

"ZVR" wrote:

"Mourad" <Mourad@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:53BB965E-C94E-40C8-AEF8-F20AD7EE07D6@xxxxxxxxxxxxxxxxxxxx>

All I need to do is allow access of https:// websites from the internal network to the internet. Right now, people can browse http websites but any website that uses SSL (https) get blocked even though I have the protocol enabled in my ISA 2004 firewall.

Well this is different from your original description of the problem.

Anyway, you can publish the SSL-secured websites behind ISA by creating web publishing rules for each of them. But your problem must be that you did not configure a SSL listener on ISA, which would have allowed you to web-publish SSL sites.

Now before going on I must warn you this will be a long one and I suggest you go through all of it, so you might as well grab a mug of coffee before moving on... No? OK, here it goes:

The way web-publishing with SSL works in ISA is that you install the web server certificate on ISA, then you create a web listener that uses that certificate. Then you create a web publishing rule which takes advantage of that web listener. In effect ISA will behave to the Internet user as the SSL webserver. Then you need to forward the incoming traffic from the Internet

Re: Cannot browse SSL pages

client to the appropriate webserver on your LAN/DMZ etc. You configure this through the "SSL bridging" tab of the web publishing rule. Essentially you have two options – either break the SSL channel at ISA and use a regular HTTP session from ISA to the webserver, or create another SSL stream from ISA to destination webserver. Obviously the 2nd method is more secure but can also take a tool on ISA system resources if you have many incoming sessions.

Here'some links to articles that deal with various web publishing scenarios:

Publishing web servers using ISA2004 (check the "SSL bridging" section)
<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/publishingwebservers.mspix>

Troubleshooting SSL Certificates in ISA Server 2004 Publishing (very good article that explains some of the gotchas we usually see with SSL publishing)
<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/tscerts.mspix>

I also gather from your post that you have multiple internal sites protected with SSL and want to publish them all. Depending on what server they are located and what kind of host headers are being used (are all sites part of the same Internet domain? like *.mycompany.com or whatever), you can find yourself in one of the following situations:

a) All sites are within a single Internet (sub)domain, for example you have www.mycompany.com, www.billing.mycompany.com, www.reports.mycompany.com etc. Then you can use a wildcard SSL certificate which will allow you to publish all SSL sites using a single web listener – i.e. a single external IP address. See the following articles for more info:

Publishing Multiple Web Sites using a Wildcard Certificate in ISA Server 2004 (by Tom Shinder)
<http://www.isaserver.org/tutorials/2004wildcardcert.html>

Same article by MS:
<http://www.microsoft.com/technet/prodtechnol/isa/2004/maintain/wildcard.mspix>

b) If you're not so lucky and your sites are not part of the same domain, you will need multiple external IP addresses and multiple SSL listeners (one per IP) to publish all your sites, UNLESS you don't care about warning messages when the users access the published servers – in which case you can use a wildcard certificate and a single IP address. (The warnings will appear because some of the sites will not match the name on the wildcard SSL certificate). Or you could create multiple SSL listeners with a single IP but on different ports – one will run on port 443, another on port 444 etc. Of course this has the disadvantage that the users will have to enter the port part as well in their URL's – something like <https://www.company.com:444/> which may be acceptable to you or not – you decide.

Re: Cannot browse SSL pages

FINALLY, if you don't want to install the web server certificates or a wildcard certificate on the ISA machine, you can also use SSL tunneling which will basically forward all requests made to port 443 on the ISA external interface to an internal IP. This is documented in the following article:

<http://support.microsoft.com/default.aspx?kbid=837834&product=isas2004>

However this is not as secure as the SSL bridging method because ISA will no longer decrypt the incoming SSL stream and won't be able to inspect the incoming traffic. And it can only be used once, i.e. if you have multiple internal web servers, running on different IP addresses, only one of them can be published on port 443 using this method; the rest can be published on different ports, or on different external IP's (if you have more than one, that is).

Virgil