

RE: ISA 2006 and SSL

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2006-11/msg00180.html>

- *From:* v-kzhao@xxxxxxxxxxxxxxxxxxxxxx ("Ken Zhao [MSFT]")
 - *Date:* Tue, 21 Nov 2006 08:48:10 GMT
-

Hello,

For the first question, it is no.

For the second question, I agree.

For the third and fourth question, I suggest you refer to the following article:

Authentication in ISA Server 2006

<http://www.microsoft.com/technet/isa/2006/authentication.msp>

Thanks & Regards,

Ken Zhao

Microsoft Online Partner Support

Get Secure! – www.microsoft.com/security

=====
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.
=====

This posting is provided "AS IS" with no warranties, and confers no rights.

| X-Tomcat-ID: 30119956
| References: <9C523D31-2720-460E-950D-953A168AD3F4@xxxxxxxxxxxxxx>
<vFDfLvHCHHA.4372@xxxxxxxxxxxxxxxxxxxxxx>
<A8189375-E97B-4124-9C87-37DDAE74E176@xxxxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain
| Content-Transfer-Encoding: 7bit
| From: v-kzhao@xxxxxxxxxxxxxxxxxxxxxx ("Ken Zhao [MSFT]")
| Organization: Microsoft
| Date: Fri, 17 Nov 2006 01:21:14 GMT

RE: ISA 2006 and SSL

| Subject: RE: ISA 2006 and SSL
| X-Tomcat-NG: microsoft.public.isa
| Message-ID: <h8rx3aeCHHA.1976@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
| Newsgroups: microsoft.public.isa
| Lines: 237
| Path: TK2MSFTNGXA01.phx.gbl
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.isa:69585
| NNTP-Posting-Host: tomcatimport2.phx.gbl 10.201.218.182

| Hello,

| Thanks for your clarification and response. Because the ISA 2006 is a new
| released product, I will perform further research with your issues.

Thanks.

| Thanks & Regards,

| Ken Zhao

| Microsoft Online Partner Support
| Get Secure! – www.microsoft.com/security

=====
| When responding to posts, please "Reply to Group" via your newsreader so
| that others may learn and benefit from your issue.

=====
| This posting is provided "AS IS" with no warranties, and confers no
rights.

|-----
| Thread-Topic: ISA 2006 and SSL
| thread-index: AccIwkHRDo+FL/4IRIOIYY3odFnoEA==
| X-WBNR-Posting-Host: 209.217.222.70
| From: =?Utf-8?B?U211cmZtYW4=?= <smurfman@xxxxxxxxxxxxxxxx>
| References: <9C523D31-2720-460E-950D-953A168AD3F4@xxxxxxxxxxxxxxxx>
| <vFDfLvHCHHA.4372@xxxxxxxxxxxxxxxxxxxxxxxx>
| Subject: RE: ISA 2006 and SSL
| Date: Wed, 15 Nov 2006 06:28:02 -0800
| Lines: 169
| Message-ID: <A8189375-E97B-4124-9C87-37DDAE74E176@xxxxxxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain;
| charset="Utf-8"
| Content-Transfer-Encoding: 7bit
| X-Newsreader: Microsoft CDO for Windows 2000
| Content-Class: urn:content-classes:message
| Importance: normal

RE: ISA 2006 and SSL

|| Priority: normal
|| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830
|| Newsgroups: microsoft.public.isa
|| Path: TK2MSFTNGXA01.phx.gbl
|| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.isa:69529
|| NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250
|| X-Tomcat-NG: microsoft.public.isa

|| Thanks Ken,

|| You lost me on a few items.

|| 1) I have a rule that is HTTP, HTTPS, and HTTPS Server as one object in
| the
|| firewall policy. Are you saying that I should separate each of these
| into
|| three objects / rules?

|| 2) SSL Tunnel was allowed thru the (All Access) rule that I created. I
|| figured out why it was going however, and was not related to the PORT
| 443,
|| but rather the destination. My HTTP / HTTPS / HTTPS Server rule was
| only
|| allowed to the destination of the External network. The requests were
|| attempting to connect on port 8080 of the Local Host, I assume so that
| the
|| SSL encryption that you spelled out could take place. When I added the
| Local
|| host to the rule, the logger then showed the client traffic being
| allowed.
|| This was a test, and my thoughts were that I was going to create a
| separate
|| rule to allow HTTPS to local host, instead of all http and https
| traffic.

|| What do you think?

|| 3) From your port I am reading things about publishing to a web server.

|| This is not what I am attempting to do. Rather I have client software
|| installed written by a third party, that starts up. It appears to be
| Java
|| based application. In my issue, the user goes to an https:\\servername
| from
|| IE, logs in, this all works just fine. Then clicks a link that starts
| up
| a
|| Java based Mainframe application that creates an SSL-Tunnel thru the
|| connection. The user authorizes several certificates, and then
| everything
|| works. What I was seeing was that when the user connected, the

| SSL-Tunnel
|| traffic was dropping because the only rule that allow https to the
local
| host
|| was my (all access) rule, and this user was not allowed to use the rule.
||
|| 4) Here is my issue as it stands. I have two clients that perform the
| steps
|| as outlined above in #3. One machine connects and works just fine.
|| Originally I thought the issue was SSL-Tunnel related, but I am
starting
| to
|| think not. Here is what I see, the same user logs into 2 machines, one
|| connects to the Java based client, the other does not, instead they are
|| prompted with a message box "Password Needed – Networking" the dialog
box
|| continues with "Firewall: Unknown Site" "Realm: ntlm" "Scheme" then
there
| are
|| two boxes for User Name and Password. If the user enters his/her logon
|| credentials, then nothing happens. If an Administrator enters his,
then
| the
|| (Java Program) loads. The box appears to be Java based. I suspect
that
|| this is machine based, and some setting. I have combed thru the IE
| settings
|| and can't see any differences, all the settings are the same. The only
| thing
|| I saw, was the version of Java, but this doesn't explain why it works
for
| an
|| admin.
||
|| Other notes, each user takes the exact same GPO and the GPO Results
|| printouts are exact for each respective machine.
||
|| Sorry for all the notes, just trying to give you a good picture of what
I
| am
|| seeing.
||
|| Thanks again.
|| J
||
||
|| ""Ken Zhao [MSFT]"" wrote:
||
|| > Hello,
|| >
|| > Thank you for using newsgroup!

||>
||> In ISA Server 2006, SSL bridging is automatically configured when the
||> specified Web listener is configured to listen for HTTPS traffic.
||> Specifically, SSL bridging works in the following scenarios:
||>
||> 1. A client requests an SSL object. ISA Server decrypts the request,
| and
||> then encrypts it again and forwards it to the Web server. The Web
| server
||> returns the encrypted object to ISA Server. ISA Server decrypts the
| object
||> and then encrypts it again and sends it to the client. SSL requests
are
||> forwarded as SSL requests.
||>
||> 1. A client requests an SSL object. ISA Server decrypts the request
and
||> forwards it to the Web server. The Web server returns the HTTP object
| to
||> ISA Server. ISA Server encrypts the object and sends it to the
client.
| SSL
||> requests are forwarded as HTTP requests.
||>
||> For incoming Web requests, an external client uses HTTPS to request
an
||> object from a Web server located on your Internal network. The client
||> connects to ISA Server on a port—by default, port 443.
||>
||> After receiving the client's request, ISA Server decrypts it,
| terminating
||> the SSL connection. The Web publishing rules determine how ISA Server
||> communicates the request for the object to the publishing Web server
| (FTP,
||> HTTP, or SSL).
||>
||> If the secure Web publishing rule is configured to forward the
request
||> using HTTPS, ISA Server initiates a new SSL connection with the
| publishing
||> server, sending a request to port 443. Because the ISA Server
computer
| is
||> now an SSL client, it requires that the publishing Web server
responds
| with
||> a server-side certificate.
||>
||> Secure Application Publishing
||> http://www.microsoft.com/technet/isa/2006/secure_web_publishing.mspx
||>

> Thanks & Regards,
>
> Ken Zhao
>
> Microsoft Online Partner Support
> Get Secure! – www.microsoft.com/security
>
> =====
> When responding to posts, please "Reply to Group" via your newsreader
> so
> that others may learn and benefit from your issue.
> =====
> This posting is provided "AS IS" with no warranties, and confers no
> rights.
>
>
>
>
>
> -----
> | Thread-Topic: ISA 2006 and SSL
> | thread-index: AccILIAo7lgFESD7TqqriFyuatgNrQ==
> | X-WBNR-Posting-Host: 209.217.222.70
> | From: =?Utf-8?B?U211cmZtYW4=? <smurfman@xxxxxxxxxxxxxx>
> | Subject: ISA 2006 and SSL
> | Date: Tue, 14 Nov 2006 12:36:02 -0800
> | Lines: 26
> | Message-ID: <9C523D31-2720-460E-950D-953A168AD3F4@xxxxxxxxxxxxxx>
> | MIME-Version: 1.0
> | Content-Type: text/plain;
> | charset="Utf-8"
> | Content-Transfer-Encoding: 7bit
> | X-Newsreader: Microsoft CDO for Windows 2000
> | Content-Class: urn:content-classes:message
> | Importance: normal
> | Priority: normal
> | X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830
> | Newsgroups: microsoft.public.isa
> | Path: TK2MSFTNGXA01.phx.gbl
> | Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.isa:69508
> | NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250
> | X-Tomcat-NG: microsoft.public.isa
> |
> | Afternoon,
> | In my firewall rules, I have an (All Access) rule for "All Outbound
> | Protocols" for my administrators. For my users there are various
> | special
> | rules for obscure ports, but the main rule is an "HTTP / HTTPS /
> | HTTPS"
> | Server rule.
> |

RE: ISA 2006 and SSL

||>| When my administrator connects to a site using a client installed
||> program,
||>| say xxx.xxx.xxx.xxx:443 the traffic passes out my (All Access) rule
| just
||> fine.
||>|
||>| When my client connects to the same site, using the same client
| installed
||>| program, xxx.xxx.xxx.xxx:443 the log shows that the traffic was
| denied,
||> using
||>| the (HTTP/HTTPS/HTTPS Server) rule. It reports SSL-Tunnel on port
| 443.
||>|
||>| I can't figure out how to allow this type of traffic
| xxx.xxx.xxx.xxx:443
||> so
||>| that non-browser programs can get out to these SSL enabled sites.
||>|
||>| I don't want to allow all of my users (All Access)
||>|
||>| My one option that I thought of, was an All access rule to the
| specific
||> IP
||>| address of the software that the client is trying to go to.
||>|
||>| Please advise, how do I add a protocol for SSL-Tunnel so that it
can
| be
||>| added to my HTTP rule?
||>|
||>| Thanks
||>| J
||>|
||>
||>
||
|
|