

RE: Outbound VPN to remote Netscreen fails

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-10/msg00772.html>

- *From:* v-edtian@xxxxxxxxxxxxxxxxxxxxxx (Edward Tian)
 - *Date:* Mon, 10 Oct 2005 03:22:50 GMT
-

Dear Gregg:

Thank you for posting here.

>From the description, I understand that your internal workstation cannot establish the VPN connection to a remote VPN router. The Netscreen VPN client is installed on the workstation. The ISA monitoring shows that the IKE client protocol is blocked by the ISA Server. If I have misunderstood your concern, please do let me know.

First I would like to confirm with you if the firewall client is installed on the internal workstation? The VPN tunnel would not work in firewall client method. If firewall client is installed, please temporarily disable it. Moreover, we need to configure the workstation as a SecureNAT client.

To be a SecureNAT client, the workstation should point its default gateway to the internal IP address of the ISA Server.

Then, we need to modify the existing access rule to allow the VPN connection for the workstations. To do so, please try the following steps:

1. Open the ISA 2004 management console, navigate to Firewall Policy.

2. On the right pane, locate the "SBS Internet Access Rule", and then double click this rule.

By default, this rule is applied to "SBS Internet Users", please change it to "All users".

3. Then move this rule to the top. After that, click "Apply" to apply the settings.

The reason why IKE client protocol was denied by the ISA Server:

As mentioned, by default the rule "SBS Internet Access Rule" is applied to "SBS Internet Users", which means only authenticated users can be allowed to access the internet by using this rule. Technically, the firewall client is responsible for sending the authentication credential to the ISA Server. In your case, considering that firewall client cannot be installed on the workstation, the VPN connection will surely be denied by the ISA Server. Therefore, we should change the rule to apply to "All Users", in this way, the workstations that haven't firewall client installed will also be

RE: Outbound VPN to remote Netscreen fails

allowed to pass through the ISA Server.

After modifying the access rule, please establish the VPN connection again, does it work now?

If you are using Windows XP workstations, please ensure that the Windows XP SP2 has been applied:

818043 L2TP/IPSec NAT-T Update for Windows XP and Windows 2000

<http://support.microsoft.com/?id=818043>

Note:

The L2TP/IPSec VPN could only work in the NAT-T supported scenario. It cannot pass through ISA if IPSec implementation doesn't support NAT Traversal. So we should make sure NAT-T is supported.

The reason for this is that the IPSec protocols are not NAPT (Network Address & Port Translation) compatible. The IPSec protocols are designed to authenticate and/or encrypt information in the packet. When a NAPT device (i.e. an ISA server) tries to change the information in the packet, it will either cause the packet to be considered invalid by an IPSec protocol, or it will be unable to perform the translation because information the NAPT device needs to access is encrypted.

More information:

http://isaserver.org/articles/IPSec_Passthrough.htm

IPSec NAT-T is not recommended for Windows Server 2003 computers that are behind network address translators.

<http://support.microsoft.com/Default.aspx?id=885348>

In addition, the issue could also be related to the Netscreen application. Considering the current status, please also contact Netscreen support since it may need additional configuration for compatibility with the current ISA 2004 configuration.

Hope the above information helps. Please feel free to let me know if there is anything I can do for you.

Have a nice day! :)

Best Regards

Edward Tian(MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner. You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

RE: Outbound VPN to remote Netscreen fails

RE: Outbound VPN to remote Netscreen fails

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

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

| Reply-To: "Gregg Hill" <bogus@xxxxxxxxxxxx>
| From: "Gregg Hill" <bogus@xxxxxxxxxxxx>
| Subject: Outbound VPN to remote Netscreen fails
| Date: Sun, 9 Oct 2005 11:07:06 -0700
| Lines: 30
| X-Priority: 3
| X-MSMail-Priority: Normal
| X-Newsreader: Microsoft Outlook Express 6.00.2900.2670
| X-RFC2646: Format=Flowed; Original
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2670
| Message-ID: <uXDNDxPzFHA.2652@xxxxxxxxxxxxxxxxxxxxxx>
| Newsgroups: microsoft.public.windows.server.sbs
| NNTP-Posting-Host: rrcs-67-52-120-246.west.biz.rr.com 67.52.120.246
| Path:
TK2MSFTNGXA02.phx.gbl!TK2MSFTNGXA03.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP1
4.phx.gbl
| Xref: TK2MSFTNGXA02.phx.gbl microsoft.public.windows.server.sbs:211463
| X-Tomcat-NG: microsoft.public.windows.server.sbs
|
| Hello!
|
| I am running SBS 2003 SP1 and ISA 2004 on my home network. I need to use
the
| Netscreen VPN client to access a remote Netscreen VPN router at a new
| client's office. Another company actually installed their Netscreen
router.
|
| My setup is Internet > cable modem > router > SBS WAN NIC > ISA 2004 >
SBS
| LAN NIC > Switch for SBS LAN NIC and workstations.
|

RE: Outbound VPN to remote Netscreen fails

| I can access it just fine if I use my laptop on its own router (I have
| five
| IPs). It does NOT have the ISA client on it, and it goes out its own
| router,
| so I know the remote end works, and my end works without ISA in the
| picture.
|
| If I try to connect with my workstation, it fails to connect. My
| workstation
| goes through the SBS and ISA 2004, and it has the ISA client. I set up a
| query in the ISA 2004 monitoring to watch what happens when I try to hit
| the
| remote Netscreen's IP address. It logs the destination IP of the
| Netscreen
| router, destination port 500, protocol is IKE Client, action is Denied
| Connection, rule is SBS Internet Access Rule, client IP is
| 192.168.16.101,
| source network is Internal, destination network is External.
|
| I looked at the SBS Internet Access Rule, and it is set to allow all
| outbound traffic. If that is true, then why is the IKE Client outbound
| traffic denied?
|
| Thank you for your time!
|
| Gregg Hill

• **Follow-Ups:**

- ◆ **Re: Outbound VPN to remote Netscreen fails**
◇ From: Gregg Hill

• **References:**

- ◆ **Outbound VPN to remote Netscreen fails**
◇ From: Gregg Hill
- Prev by Date: **RE: Changing external IP address**
- Next by Date: **Re: Help With Intranet Re-Install**
- Previous by thread: **Outbound VPN to remote Netscreen fails**
- Next by thread: **Re: Outbound VPN to remote Netscreen fails**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**