

Re: Connection denied

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isaserver/2004-11/0044.html>

From: Tristan Kington [MSFT] (tristank_at_online.microsoft.com)

Date: 11/03/04

Date: Wed, 3 Nov 2004 19:05:25 +1100

For anyone interested, private IP addresses (also known as "non-routable" IP addresses) are defined in RFC 1918:

<http://www.ietf.org/rfc/rfc1918.txt?number=1918>

Quote:

Because private addresses have no global meaning, routing information about private networks shall not be propagated on inter-enterprise links, and packets with private source or destination addresses should not be forwarded across such links. Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured to reject (filter out) routing information about private networks. If such a router receives such information the rejection shall not be treated as a routing protocol error.

--

<http://blogs.msdn.com/tristank/>

--

This post is provided "AS-IS", and confers no warranty.

"Tristan Kington [MSFT]" <tristank@online.microsoft.com> wrote in message news:%23wSm2pXwEHA.1400@TK2MSFTNGP11.phx.gbl...

> Hi,

>

> This is not actually an ISA Server issue, it's an IP routing issue.

>

> If you remove ISA Server and just configure routing between two network adapters, you'll get the same behaviour.

>

> Between a private IP address and an Internet IP address, a Route relationship can't exist; you must NAT.

>

> The ISP will not route packets back to your external IP that have a source address of a private IP address range.

>

> --

> <http://blogs.msdn.com/tristank/>

> --

> This post is provided "AS-IS", and confers no warranty.

>

>

> "Mykhaylo Khodorev" <ralfeus@chicagocentre.com.ua> wrote in message

microsoft.public.isaserver: Re: Connection denied

```
> news:cma24n$2qab$1@news.dg.net.ua...
>> I've found a strange behavior of ISA 2004 (Windows 2003 Server
>> Standard). At the beginning the network rule was:
>> Source networks: Internal
>> Dest networks: All networks (and Local Host)
>> Relation: NAT
>>
>> and firewall rule was:
>> From: Internal
>> To: All networks (and Local Host)
>> Condition: All users
>> Protocols: pings
>> Action: Allow
>>
>> I could ping any external destination.
>> But when I've changed Relation of network rule from NAT to Route, I've
>> got such records in the log:
>> Client IP: 192.168.0.200
>> Destination IP: 216.109.112.135
>> Destination Port: 0
>> Protocol: Ping
>> Action: Initiated Connection
>> Rule: Allow Pings
>> Source network: Internal
>> Dest network: External
>>
>> Client IP: 192.168.0.200
>> Destination IP: 216.109.112.135
>> Destination Port: 0
>> Protocol: Ping
>> Action: Denied Connection
>> Rule:
>> Source network: Internal
>> Dest network: External
>>
>> Client IP: 192.168.0.200
>> Destination IP: 216.109.112.135
>> Destination Port: 0
>> Protocol: Ping
>> Action: Denied Connection
>> Rule:
>> Source network: Internal
>> Dest network: External
>>
>> Client IP: 192.168.0.200
>> Destination IP: 216.109.112.135
>> Destination Port: 0
>> Protocol: Ping
>> Action: Closed Connection
>> Rule: Allow pings
>> Source network: Internal
>> Dest network: External
>>
>> I read on microsoft.com that when packet is dropped before getting rules
>> engine the rule name won't appear. But why packet can be dropped before
>> getting rules engine? Why NAT is working fine, but route doesn't?
>> Thanks.
>> Mykhaylo Khodorev
>>
>
>
```