

Re: SecureNAT

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2005-10/msg00265.html>

- *From:* "ZVR" <nospamever@xxxxxx>
 - *Date:* Mon, 24 Oct 2005 13:55:49 -0400
-

You are misunderstanding some concepts here.

First of all just to be clear you will not be able to use the caching feature unless you go through the web proxy service/filter (this is by design in ISA).

Second, the web proxy has nothing to do with the NAT / no NAT rule. By definition a proxy service terminates the client connection at the proxy level and initiates a connection to the destination, originating from itself, on behalf of the client. The client is NEVER in direct contact with the server. The proxy connects to the server as it was the "client", but when the response comes back from the server that response gets forwarded to the client. Basically the proxy acts as a client to the final server, and as a server to the original client.

That said, you must understand that when using a proxy service the destination server will ALWAYS see the proxy's own IP, from the interface with the default gateway set (because that is where the packets originate from). Again this is how a proxy functions by design and you cannot change that.

NAT on the other hand is used to transparently route requests between source and destination by replacing on the fly the source IP address with the "external" IP of the NAT device. This happens at the transport level and is different from a proxy service which is protocol-aware and functions at a higher protocol layer. Of course you can NAT or not NAT the http requests too, but in that case, as you just discovered yourself, you lose the http caching feature which is provided by the web proxy service at the "application" level.

What you seem to want is a totally transparent web cache. ISA doesn't do that and I am not aware of other products that do it.

Virgil

"Lakha" <Lakha@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

Re: SecureNAT

news:C4651863-3204-464D-BF1C-F611107F8182@xxxxxxxxxxxxxxxxxxxx

> Hi,
> Many thanks for your help, disabling the web proxy filter stops the
> natting
> which is perfect from a routing point of view as the http traffic is no
> longer natted with the private 172.. external ip.
> However it now means that the ISA server cannot act as a Web Proxy Cache
> Server, all http traffic goes directly to the destination website and does
> not get served from the cache.
> So this fix while it does what I want it to do, compromises the proxy
> feature of ISA Server 2004. I know that when you have a single adapter ISA
> server, the web requests that proxy through this single adapter ISA server
> have their source addresses modified so the request comes from the isa
> server, which then fetches and passes the results to the original client.
> I think with two network cards the ISA by default NAT's http traffic by
> substituting the original ip src addr with the External Interface ip
> address
> (in my case this is a 172 address, so the request never gets to the
> internet). So my next question, Is it possible to force ISA Server 2004 to
> use the internal interface ip address when it does the NAT substistution?
>
> Many Thanks for your help..
> --
> Lakha
>
>
> "Johnnie Mac" wrote:
>
>> Hi,
>> you need to disable the web proxy
>> http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/ts_proxy_traffic.msp#appendix-a
>>
>> this should fix the problems.
>>
>> Regards
>> John
>>
>> Appendix A: Disable the Web Proxy Filter
>> To disable the Web Proxy filter for HTTP, do the following:
>>
>> 1.
>> In ISA Server Management, click the Firewall Policy node.
>>
>> 2.
>> On the Toolbox tab, click Protocols.
>>
>> 3.
>> Expand All Protocols, right-click HTTP, and then click Properties.
>>
>> 4.
>> Click the Parameters tab, and in Application Filters, clear Web Proxy

Re: SecureNAT

Re: SecureNAT

>> Filter. Then click OK.
>>
>> 5.
>> Click Apply to update the firewall policy.
>>
>> Note
>> Requests from Web browsers (with proxy settings pointing to ISA Server)
>> still go through the Web Proxy filter.
>>
>>
>> --
>> JohnnieMac
>>
>>
>> "Lakha" wrote:
>>
>> > Hi All,
>> > I want all the machines in our compnay go through ISA server 2004
>> > firewall.
>> > I have installed ISA server 2004, disabled the default internet access
>> > rule
>> > (nat) and created a new network rule that routes traffic from all
>> > network to
>> > all networks. So as far as I can see no NATting is configured. I have
>> > created
>> > a new access policy rule that allows all traffic out.
>> >
>> > Routing from internal/localhost to external subnets seems to work find,
>> > but
>> > when I use http protocol (try to get on the internet) the ISA server
>> > NAT's
>> > the ip src address of the packet, and this being a private ip address
>> > 172...,
>> > our main corporate firewall drops the packet.
>> >
>> > All machines by microsoft's defintion will be SecureNAT clients,
>> > because
>> > their default gateway is set to point to the internal ip address of the
>> > ISA
>> > server.
>> > Even if i configure the client to be a webproxy client (point its
>> > browser to
>> > the internal ip if the isa server), or even use the Firewall Client
>> > Software
>> > http sessions are still NATted.
>> >
>> > So my question is this, Can you disable NATting on ISA Server 2004, all
>> > i
>> > want is pure routing ?.
>> >
>> > Many Thanks.

Re: SecureNAT

>> >
>> > --
>> > Lakha

• **References:**

- ◆ **RE: SecureNAt**
 - ◇ *From:* Johnnie Mac
 - ◆ **RE: SecureNAt**
 - ◇ *From:* Lakha
-
- Prev by Date: **Re: Windows Update site and ISA 2004**
 - Next by Date: **Proxy Chain Loop error 12206**
 - Previous by thread: **RE: SecureNAt**
 - Next by thread: **Re: Block MSN Messenger in ISA Server 2004**
 - Index(es):
 - ◆ **Date**
 - ◆ **Thread**