

## Re: IPSEC Router-to-Router Tunnel established – now what?

---

*Source:* <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2005-08/msg00167.html>

---

- *From:* "Mark C. Walton" <[mcw@xxxxxxxxxxxxxxxxxxxxxx](mailto:mcw@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 8 Aug 2005 16:51:32 -0400
- 

Hi Phillip –

Thanks very much for the helpful & complete (and quick!) explanation. I believe I understand everything you have written – I admit I am still learning.

I guess I assumed, perhaps incorrectly, that if I could establish the tunnel at all, then everything was communicating properly. What I was trying to avoid is adding a Linksys at this end with a public IP address on the WAN interface, and then plugging one of the LAN interfaces on the Linksys directly into one of my internal switches – effectively bypassing ISA. How much, if anything, do you think I would be losing in the way of security if I did this? I do try to keep a very close eye on everything, and as of yet I have never had a serious security issue I am aware of (famous last words, no doubt).

Regarding the static routes in RRAS, now that I think about it, I think I found had to do that because some of the remote sites needed to see some of the other remote sites – does that make sense?

Thanks again, Phillip.

– Mark

"Phillip Windell" <@.> wrote in message

[news:uMERJeFnFHA.3988@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uMERJeFnFHA.3988@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

- > VPN Solutions tend to be proprietary to the brand of device being used.
- > Functionality may be limited, or worse, non-functional when brands are mixed.
- > Match the VPN Devices at both ends.
- >
- > If you use Linksys, then use it at both ends.
- > If you use Seimens, then use it at both ends.
- > If you use ISA, then use ISA or RRAS at both ends.
- >
- > Window's RRAS based Router-to-Router VPN (includes ISA) uses a \*double\*

Re: IPSEC Router-to-Router Tunnel established – now what?

> connection. Each RRAS Device calls the other and each Device answers the  
> other. One logical connection is used for one direction of travel and the  
> other is used for the other direction of travel. Each connection is  
> "one-way" so it takes two,...kinda like a freeway with a median in  
> between.  
>  
> IPsec doesn't play a functional role,...it is just another level of  
> complexity on top of what is already there. But it can certainly get in  
> the  
> way if something is wrong with it.  
>  
> No matter what brand you use, the VPN Devices all must have two interfaces  
> (they are a type of router after all). The outer public interface only  
> provides the means for the two devices to connect and establish the  
> Tunnel,...they have \*no\* role in the routing. \*Everything\* else  
> concerning  
> routing and networkability is based on the internal side interfaces and  
> the  
> private internal IP# ranges they represent.  
>  
> I see no reason to have any Static Routes anywhere. All routers (VPN or  
> otherwise) are perfectly aware of networks that they are directly  
> connected  
> to, so they already know how to get there. If you have multiple subnets  
> on  
> each end then you probably need Static Routes, but what is actually needed  
> varies with the situation..  
>  
>  
> ---  
> Phillip Windell [MCP, MVP, CCNA]  
> www.wandtv.com  
> -----  
> Understanding the ISA 2004 Access Rule Processing  
> [http://www.isaserver.org/articles/ISA2004\\_AccessRules.html](http://www.isaserver.org/articles/ISA2004_AccessRules.html)  
>  
> Microsoft Internet Security & Acceleration Server: Guidance  
> <http://www.microsoft.com/isaserver/techinfo/Guidance/2004.asp>  
> <http://www.microsoft.com/isaserver/techinfo/Guidance/2000.asp>  
>  
> Microsoft Internet Security & Acceleration Server: Partners  
> <http://www.microsoft.com/isaserver/partners/default.asp>  
> -----  
>  
>  
>  
> "Mark C. Walton" <mcw@xxxxxxxxxxxxxxxxxxxx> wrote in message  
> <news:Og%23OQBFnFHA.2156@xxxxxxxxxxxxxxxxxxxxxxxx>  
>> I thought I was starting to get a pretty good handle on routing, I'm not  
> too  
>> sure now. But I'm not sure if this is really an ISA issue or a routing

Re: IPSEC Router-to-Router Tunnel established – now what?

Re: IPSEC Router-to-Router Tunnel established – now what?

>> issue.  
>>  
>> I have a number of remote sites which need access here to the corporate  
>> network (and us to them). I have ISA installed on Win2K along with RRAS.  
>> The way I have done this in the past is by installing a Win2K box at the  
>> remote site and using RRAS to establish a PPTP tunnel back to the ISA box  
>> (the remote site Win2K Server also has 2 NICs, internal private IP and  
>> external public IP into the router). Then I use static routes in RRAS on  
>> both ends to establish two-way communication. The static routes are  
>> bound  
>> to the respective remote site interfaces in RRAS.  
>>  
>> Now I want to try and eliminate the Win2K box at the other side and just  
> use  
>> a VPN router – most of the sites have only a few users and a Win2K setup  
>> seems overkill. From what I have been able to discern, ISA won't pass  
> IPSEC  
>> to the internal interface without a lot of trouble (and maybe not even  
>> then). So what I am trying to do is setup router-to-router VPNs – the  
>> remote router being a simple Linksys and my local router right now being  
>> a  
>> Seimens 5940 (connected to a T1). I can establish the tunnel just fine,  
> but  
>> I cannot get the two internal networks to see each other no matter how I  
> try  
>> to set up the routing. The Seimens has public IP address of, say,  
>> 100.100.100.1 and is connected to the external interface of the ISA box  
>> at  
>> 100.100.100.2 with GW 100.100.100.1. The internal ISA interface has  
> private  
>> IP of 10.10.10.1 with no gateway. The remote site has public IP  
>> 200.200.200.200 GW 200.200.200.1 and internal 10.20.20.20. On the  
>> Seimens  
>> router IPSEC configuration I am setting the Remote Destination Subnet of  
>> 10.20.20.20 and Remote Gateway of 200.200.200.200. The remote router is  
> set  
>> for Remote IP Address of 100.100.100.1 (since there is no local private  
>> IP  
>> subnet on the Seimens) and the Remote Gateway is the same (100.100.100.1)  
>>  
>> As I said, I can establish the tunnel just fine and can ping the external  
>> ISA interface from the remote router. I think maybe I just keep getting  
> the  
>> routing wrong, but it seems like I've tried everything that makes any  
> sense.  
>>  
>> I would greatly appreciate any help here.  
>>  
>> Thanks,  
>>  
>> – Mark

Re: IPSEC Router-to-Router Tunnel established – now what?

Re: IPSEC Router-to-Router Tunnel established – now what?

>>  
>>  
>  
>

.

---

• **References:**

- ◆ **[IPSEC Router-to-Router Tunnel established – now what?](#)**

◇ *From:* Mark C. Walton

- Prev by Date: **[Re: VPN Problems after subnet change](#)**
- Next by Date: **[Re: Extensions tab in HTTP filtering options – allow default doc somehow?](#)**
- Previous by thread: **[IPSEC Router-to-Router Tunnel established – now what?](#)**
- Next by thread: **[Re: IPSEC Router-to-Router Tunnel established – now what?](#)**
- Index(es):
  - ◆ **[Date](#)**
  - ◆ **[Thread](#)**