

Re: Front-End server question

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.design/2005-03/0038.html>

From: Clayton Sutton (*none_at_none.com*)

Date: 03/04/05

Date: Fri, 4 Mar 2005 15:09:10 -0600

Thanks Al for the input, that helped a lot!

Clayton

"Al Mulnick" <amulnick_No_SPAM@ncDOTrr.com> wrote in message
news:uJtP7gAIFHA.1528@TK2MSFTNGP09.phx.gbl...

- > *It's not a substitute. It's a different concept altogether aimed at*
- > *solving a different problem.*
- >
- > *IPSec solves the problem of n'er-do-wells lurking in your DMZ sniffing the*
- > *line for information because it allows you to protect the transmission*
- > *with encryption.*
- >
- > *In this scenario, IPSec is used to secure the transmission of the data*
- > *between the servers (from the DMZ server to the domain servers.)*
- >
- > *IPSec does nothing for the application layer of the solution. So you're*
- > *left with the risk of placing a domain member (if Exchange, it also has*
- > *elevated rights by virtue of the computer group membership) in a*
- > *semi-trusted network area. Does that comply with your security policies?*
- > *It's not a Microsoft best practice but it might fit with your security*
- > *policies.*
- >
- > *By contrast ISA is an application-layer firewall (layer-7 firewall device*
- > *in other words) that is used to firewall intent (application useage) vs.*
- > *packet destination (like a router, right?). It happens to understand*
- > *Microsoft products better than most other layer-7 firewall devices. That*
- > *makes sense as well right?*
- >
- > *Typically, you'd want to deploy ISA <insert your solution here if not ISA>*
- > *in the DMZ to project the application. That machine would be a hardened,*
- > *stand-alone solution. It would also terminate your external SSL*
- > *connections (note that SSL is also used to protect transmission of data*
- > *between machines ONLY). Ideally, you'd want a device that could bridge*
- > *SSL because you'd want to inspect the packet before it reaches its*
- > *destination and make a permit/deny decision based on the intent prior to*
- > *it hitting the intended application. From the DMZ, you'd want a way to*

> protect the conversation of the <ISA> server to the target application
> server. This is often done with SSL (bridging) where the ISA server
> creates a new SSL session with the target from its internally facing
> interface, or with IPSec encryption to the target. In this case, IPSec
> and SSL would be interchangeable for their intended function and it would
> be a matter of choice/policy which you chose.
>
> Does that help you to understand where IPSec can fit in all of this?
>
> Note that *some* would argue that if you had an application layer
> firewall, you wouldn't really need a DMZ. A DMZ would be an archaic
> throwback since it's job is to allow you to cutoff conversation from the
> untrusted to the trusted (soft squishy core). I still see some value in a
> DMZ myself, but just throwing that out there.
>
> Al
>
>
> "Clayton Sutton" <none@none.com> wrote in message
> news:uaIXeGAI FHA.576@TK2MSFTNGP15.phx.gbl...
>> How is this a substitute for ISA? Does it work better then ISA? Like I
>> said, I don't really want to use ISA.
>>
>>
>> Clayton
>>
>>
>>
>> "Rodney R. Fournier [MVP]" <rod@die.spam.die.nw-america.com> wrote in
>> message news:e00pvr3HFHA.2476@TK2MSFTNGP12.phx.gbl...
>>> You mean like this one
>>> <http://support.microsoft.com/default.aspx?scid=kb;en-us;821839>? You
>>> will need Exchange 2003, 2000 did not support IPsec in this matter. I
>>> can tell you from personal experience that it works nicely :)
>>>
>>> Cheers,
>>>
>>> Rod
>>>
>>> MVP – Windows Server – Clustering
>>> <http://www.nw-america.com> – Clustering
>>> <http://msmvps.com/clustering> – Blog
>>>
>>> "Clayton Sutton" <none@none.com> wrote in message
>>> news:uYoVLi3HFHA.2656@TK2MSFTNGP09.phx.gbl...
>>>> Do tell more Rod. I like that idea. Got any white papers or links
>>>> that talk about it? I really don't like to have to use ISA.
>>>>
>>>>
>>>> Clayton
>>>>

>>>>
>>>>
>>>>
>>>> *"Rodney R. Fournier [MVP]" <rod@die.spam.die.nw-america.com> wrote in*
>>>> *message news:O12bxb1HFHA.2700@TK2MSFTNGP09.phx.gbl...*
>>>>> *If you are not a fan of ISA. Put the FE's in the DMZ and use IPSec to*
>>>>> *the backend. That works nicely too.*
>>>>>
>>>>> *Cheers,*
>>>>>
>>>>> *Rod*
>>>>>
>>>>> *MVP – Windows Server – Clustering*
>>>>> *<http://www.nw-america.com> – Clustering*
>>>>> *<http://msmvps.com/clustering> – Blog*
>>>>>
>>>>> *"Russ Kaufmann" <russ@exchangemct.com> wrote in message*
>>>>> *news:e6W%23cU1HFHA.3928@TK2MSFTNGP09.phx.gbl...*
>>>>>> *"Ed Woodrick" <ewoodrick@ed-nospam-com.com> wrote in message*
>>>>>> *news:OLcs6Y0HFHA.2936@TK2MSFTNGP15.phx.gbl...*
>>>>>>> *There is no specific need for different FE servers for the different*
>>>>>>> *domains. One FE server can handle the requirements of both.*
>>>>>>>
>>>>>>>> *Don't put your FE servers in the DMZ. Put them on the internal*
>>>>>>>> *network. If you need enhanced security, user a ISA server to reverse*
>>>>>>>> *proxy the connection from the Internet.*
>>>>>>>
>>>>>>>> *I agree with Ed here. Putting FEs in the DMZ can be really difficult*
>>>>>>>> *to configure properly, and it just doesn't make sense to me when you*
>>>>>>>> *can publish them back into the LAN.*
>>>>>>>
>>>>>>
>>>>>>
>>>>
>>>>
>>>
>>>
>>
>>
>>
>
>