

## Re: Audited an ISA 2000 – part I

**Source:** <http://www.tech-archive.net/Archive/ISA/microsoft.public.isaserver/2004-11/0097.html>

---

**From:** Tristan Kington [MSFT] ([tristank\\_at\\_online.microsoft.com](mailto:tristank_at_online.microsoft.com))

**Date:** 11/05/04

Date: Fri, 5 Nov 2004 17:39:09 +1100

If ISA is removed and reinstalled, you lose all the rules, settings, etc.

This might be a positive thing if you're in the situation you're in as the result of the rule configuration, but it also means setting up all the access rules, publishing rules, and packet filters again.

If you have a pretty clear idea of what to do, this is probably the simplest method of getting everything where it needs to be (and there are several guides on the web and at <http://isaserver.org>) on general ISA Server configuration.

If you experience a specific problem with what you're trying to achieve, I'd strongly suggest contacting PSS, explaining the situation, and working with them on it.

If you're able to run ISAINFO on the server and email me the text file output (<http://isatools.org>), I'll take a quick look at the settings and let you know if there are any simple things you could do. You need to remove "online." from my posting address to email me.

If you suspect you've been hacked (from other post), it'd be a good opportunity to rebuild the box, changing all the passwords used on it; IMO, it's the best way to be sure.

--

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

--

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

"Doug Fox" <[dfox168@hotmail.com](mailto:dfox168@hotmail.com)> wrote in message

news:OP8A5ftwEHA.3492@TK2MSFTNGP11.phx.gbl...

> Tristan;

>

> I want the ISA server to be "air-tighted"! What steps should I take to  
> remedy this "chaos"?

>

> Many thanks!

>

> "Tristan Kington [MSFT]" <[tristank@online.microsoft.com](mailto:tristank@online.microsoft.com)> wrote in message

> news:eMU8khsWEHA.1292@TK2MSFTNGP10.phx.gbl...

>> If you have very permissive packet filtering set up, or packet filtering

>> disabled, that might explain this port range.

>>

## microsoft.public.isaserver: Re: Audited an ISA 2000 – part I

```
>> With the default settings, a multi-NIC ISA 2000 installation is invisible
>> from the Internet (but is accessible internally) - it drops all packets.
>>
>> Creating packet filters that are too permissive - or disabling them
>> altogether - might lead to the situation you've described.
>>
>> --
>> http://blogs.msdn.com/tristank/
>> --
>> This post is provided "AS-IS", and confers no warranty.
>>
>>
>> "Doug Fox" <dfox168@hotmail.com> wrote in message
>> news:ek9wTFswEHA.3416@TK2MSFTNGP09.phx.gbl...
>> > Did an internal and an external port scan on a production ISA 2000
>> > server
>> > and found the following ports opened, but seems quite unusual. Any
>> > comments/suggestions are appreciated.
>> >
>> > The external scan, i.e., scanning the server from the internet, which
>> > reported the following ports are open:
>> >
>> > TCP Ports
>> > 110 (POP3)
>> > 135 (DCE endpoint resolution)
>> > 139 (NETBIOS Session Service)
>> > 515 (Spooler)
>> > 1027 (unknown or ICQ?)
>> > 3372 (Microsoft Distributed Transaction Coordinator (MSDTC) / TIP 2)
>> > 10000 Webmin / Network Data Management Protocol
>> >
>> > UDP Port:
>> > 137 (NETBIOS Name Service)
>> >
>> > The internal scan, i.e., scanning the server's internal interface, the
>> > result is:
>> >
>> > TCP Ports
>> > 135 (DCE endpoint resolution) (also appears on the external interface.)
>> > 139 (NETBIOS Session Service) (also appears on the external interface.)
>> > 445 (Microsoft-DS)
>> > 515 (Spooler) (also appears on the external interface.)
>> > 1027 (unknown) (also appears on the external interface.)
>> > 1080 (socks)
>> > 1745 (ISA Server proxy autoconfig / remote winsock)
>> > 3372 (Microsoft Distributed Transaction Coordinator (MSDTC) / TIP 2)
>> > (also
>> > appears on the external interface.)
>> > 8080 (HTTP/HTTP Proxy)
>> > 10000 Webmin / Network Data Management Protocol (also appears on the
>> > external interface.)
>> >
>> > UDP Ports
>> > 137 (NETBIOS Name Service)(also appears on the external interface.)
>> > 2967 (SSC-AGENT / Norton Anti-virus)
>> >
>> > I
>> >
>> >
>> >
>> >
>> >
>> >
```

microsoft.public.isaserver: Re: Audited an ISA 2000 – part I

>