

## Re: IPSec policie is not working like it should

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2004-04/0550.html>

---

**From:** Arjen Steur (*arjensteur\_at\_hotmail.com*)

**Date:** 04/14/04

Date: Wed, 14 Apr 2004 09:09:36 +0200

Eventually I posted my problem a little to complicated; I'll simplifie my problem a little bit.

I'm running a webserver on which port 80 (http) inbound, and port 25 (smtp) outbound have to be enabled.

the rest has to be blocked. My question is: Is it possible to achieve this by using IP Security Policies which I prefer because it helps to keep my server clean. If it isn't possible, which firewall would you suggest?

Greetings,

Arjen  
Dijkoraad-Hawar BV

"David Beder [MSFT]" <dbeder@online.microsoft.com> schreef in bericht news:uruseoTHEHA.2612@TK2MSFTNGP09.phx.gbl...

> *I'm not sure how you can force all your traffic to go out a single port.*

> *Almost all of your applications are going to be given dynamic outbound ports*

> *(ie they'll get a different one each time). Do you have some sort of port translation software? Even if you did get this to happen or instead use the*

> *dynamic outbound port, that will let you push traffic out, but when it returns, your inbound filters are going to block it.*

>

> *It sounds like you're looking for a firewall, not data protection.*

>

> --

> *David*

> *Microsoft Windows Networking*

> *This posting is provided "AS IS" with no warranties, and confers no rights.*

>

>

> *"Arjen" <arjensteur@hotmail.com> wrote in message*

> *news:f2dfcd96.0404070402.46b34b02@posting.google.com...*

> *Hello,*

microsoft.public.windows.server.networking: Re: IPSec policie is not working like it should

> >  
> > *I've got a Windows Server 2003 Web-Edition installed on my webserver*  
> > *which is placed somewhere else. I designed IP Security policies to*  
> > *this machine which work fine.*  
> > *- All inbound ports are blocked at first (no mirroring)*  
> > *- Inbound Port 80, 443 (http/https) enabled (no mirroring)*  
> > *- Inbound Port 3389, 6699 (Terminal Services and RDC) enabled from a*  
> > *specific IP adress (no mirroring)*  
> >  
> > *\* Inbound means that the source IP is 'Any IP adress' and the*  
> > *destination IP is 'My IP adress'.*  
> >  
> > *This works fine! But I can't get the following rules to work. They are*  
> > *a little redundant, but nevertheless they should work I think. My*  
> > *question is how to get these rules to work correctly.*  
> >  
> > *- All Outbound ports are opened (not mirrored)*  
> > *- Outbound 25 is opened. (not mirrored) (I know this one is also*  
> > *implied by the upper one but just to make shure.*  
> >  
> > *The problem is I cant vissit any website or send any mail through port*  
> > *25 to an outside computer. When i unassign the policie everything*  
> > *works fine! Please help!!!*  
> >  
> > *Greetings*  
> >  
> > *Arjen*  
>  
>

---  
Outgoing mail is certified Virus Free.  
Checked by AVG anti-virus system (<http://www.grisoft.com>).  
Version: 6.0.633 / Virus Database: 405 - Release Date: 18-3-2004