

RE: Microsoft IPsec via group policy

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-02/msg00170.html>

- *From:* "Jesse Rink" <jesse-rink@xxxxxxxxxx>
 - *Date:* Thu, 7 Feb 2008 22:15:48 -0600
-

Perhaps I need to re-think this a bit.

My original intention for enabling IPsec was to prevent users from sniffing Kerberos hashes. I was under the assumption based on the communication I had with several security "experts" from a couple consulting companies that IPsec could accomplish this.

What I'm here from Rodrigo and Scott, is that IPsec cannot encrypt the packets containing Kerberos hashes that are sent over the network between the XP client and domain controller. Is this correct?

I am not so concerned with encrypting traffic between the clients and members servers or emails servers as I am with encrypting traffic that contains the Kerberos hashes which users can sniff and then hack offline.

Comments welcome. ... Paul? Rodrigo? Scott?

Thanks.
J

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxxxx] On Behalf Of Ramsdell, Scott
Sent: Thursday, February 07, 2008 8:36 AM
To: Jesse Rink; Paul J. Brickett
Cc: security-basics@xxxxxxxxxxxxxxxxxxxx;
security-basics-return-47647@xxxxxxxxxxxxxxxxxxxx
Subject: RE: Microsoft IPsec via group policy

JR,

Requiring ipsec between a client and a DC via GPO is problematic.

You'll have much more success allowing the initial auth to the domain via Kerberos, then using ipsec to secure communication from the client machine to the file/email servers.

RE: Microsoft IPSec via group policy

From Microsoft: Currently, we do not support the use of IPSec to encrypt

network traffic from a domain client or member server to a domain controller when you apply the IPSec policies by using Group Policy or when you use the Kerberos version 5 protocol authentication method.

<http://support.microsoft.com/kb/q254949/>

You're putting the cart before the horse, so to speak, by requiring ipsec communication before your client machines can auth and read the GPO that requires the ipsec.

Kind Regards,

Scott Ramsdell
CISSP CCNA MSCE

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]
On Behalf Of Jesse Rink
Sent: Wednesday, February 06, 2008 8:04 AM
To: 'Paul J. Brickett'
Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx;
security-basics-return-47647@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: Microsoft IPSec via group policy

Hello.

Sorry for the delayed response. For some reason when I post on this list, my posts sometimes don't show up for 16-30 hours. Not quite sure why.

What I'm attempting is to encrypt network traffic between my clients and my domain controllers and clients and my member servers.

I have tried setting IPSec up in group policy however I'm running into some strange issues. What I've done to set this up for testing is this...

1. In the Domain Controllers OU and GPO, I set the IP Sec policy for Server (request security) – Assigned.
2. In the test PC OU and GPO, I set the IP Sec policy for Client (respond only) – Assigned.

At this time, I think I should be good to go. I go to the XP client and do

RE: Microsoft IPSec via group policy

RE: Microsoft IPsec via group policy

a gpupdate /force and reboot the computer. Now, here's what's odd. According to documentation I've read, I should be able to tell the IP Sec policy applied to the client in the following ways:

1. I should be able to do an RSOP.msc from Start|Run on the XP client and see the IP Sec policy. I try that, but nothing shows up.
2. I should be able to look at the Local Security Policy on the XP client and it should show that IP Sec policy has been applied from a GPO. I try that, but nothing shows up.

I am starting to wonder if the documentation I've read is WRONG about these things. I have noticed this... If I look on the XP Client's registry, under HKLM\SOFTWARE\Policies\Microsoft\Windows\IPsec\GPTIPSECPolicy and under HKLM\SOFTWARE\Policies\Microsoft\Windows\IPsec\Policy\Cache, I "DO" find that these keys are created/updated after doing the gpupdate /force and rebooting, so it SEEMS like IPsec is getting applied? But again, RSOP.msc and the Local Security Policy show NOTHING. Why is this?

Also, I am testing what happens if the IPsec policy on the client is unapplied. This is very strange as well. If after having applied the IP Sec policy via GPO to the XP Client, I remove it a short time later by going into the GPO for the PC OU, and changing Client (respond only) to Unassign, when I then go to the XP client and do a gpupdate /force and then reboot, the XP client can no longer contact the domain controller. I can't even ping it, nor can the domain controller ping the client. This doesn't make sense. I am removing the IP Sec policy from the client "by the book" as far as I can tell by unassigning it first, and then making sure the new GPO is applied to the PC. Any idea on this particular issue?

I'm about ready to open up a case with Microsoft to figure this stuff out. Thanks for any help.

JR

RE: Microsoft IPsec via group policy

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]

On

Behalf Of Paul J. Brickett

Sent: Tuesday, February 05, 2008 11:02 AM

To: jesse-rink@xxxxxxxxxx

Cc: security-basics@xxxxxxxxxxxxxxxxxxxx;
security-basics-return-47647@xxxxxxxxxxxxxxxxxxxx

Subject: Re: Microsoft IPsec via group policy

What exactly are you trying to do? Providing detail to the group may elicit more responses.

I've deployed several IPsec GPOs- I generally have used IPsec GPOs to more granularly block/allow access to specific ports/protocols. I find that it's a more precise tool than Windows Firewall. I often find myself comparing it to IPTables.

-PJB

On Mon, 4 Feb 2008, jesse-rink@xxxxxxxxxx wrote:

Just curious if anyone on the list has implemented IPsec for Windows 2003/XP via Group Policy? I am testing this out and finding some

strange

results that I'd like to bounce off someone who's done this before. Anyone?

JR

mail2web.com - Enhanced email for the mobile individual based on

MicrosoftR

Exchange - <http://link.mail2web.com/Personal/EnhancedEmail>