

Re: IPsec: Network sooo sloooooow

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2005-03/0636.html>

From: D Hartry (DHartry_at_discussions.microsoft.com)

Date: 03/17/05

Date: Thu, 17 Mar 2005 14:51:04 -0800

Steve,

Thank you, exactly the information I was after.

"Steven L Umbach" wrote:

- > *The Windows free 2003 Security Guide covers this in detail by describing how*
- > *to use ipsec filtering to secure domain controllers. Ipsec filtering uses an*
- > *ipsec policy that uses only permit and deny filter actions to act as a*
- > *packet filtering firewall instead of negotiation policy. The link below is*
- > *to the Windows 2003 Security Guide. There is also a challenge in dynamic RPC*
- > *port assignment that can be remedied with a registry entry to restrict ports*
- > *that will be used. The second link will give a basic idea of what*
- > *ports/protocols are used. --- Steve*

>
>

> [http://www.microsoft.com/downloads/details.aspx?FamilyID=8a2643c1-0685-4d89-b655-521ea6c7b4db&display=](http://www.microsoft.com/downloads/details.aspx?FamilyID=8a2643c1-0685-4d89-b655-521ea6c7b4db&display=details)

> <http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B179442>

>

> *Windows NT*

> *Client Port(s) Server Port Service*

> *1024-65535/TCP 135/TCP RPC **

> *137/UDP 137/UDP NetBIOS Name*

> *138/UDP 138/UDP NetBIOS Netlogon and Browsing*

> *1024-65535/TCP 139/TCP NetBIOS Session*

> *1024-65535/TCP 42/TCP WINS Replication*

>

> *Windows 2000*

> *For a mixed-mode domain with either Windows NT domain controllers or legacy*

> *clients or trust relationship between two windows 2000 domain controllers*

> *that are not in the same forest, all of the preceding ports for Windows NT*

> *may need to be opened in addition to the following ports: Client Port(s)*

> *Server Port Service*

> *1024-65535/TCP 135/TCP RPC **

> *1024-65535/TCP/UDP 389/TCP/UDP LDAP*

> *1024-65535/TCP 636/TCP LDAP SSL*

> *1024-65535/TCP 3268/TCP LDAP GC*

microsoft.public.windows.server.networking: Re: IPsec: Network sooo sloooooow

> 1024-65535/TCP 3269/TCP LDAP GC SSL
> 53,1024-65535/TCP/UDP 53/TCP/UDP DNS
> 1024-65535/TCP/UDP 88/TCP/UDP Kerberos
> 1024-65535/TCP 445/TCP SMB
>
>
> "D Hartry" <DHartry@discussions.microsoft.com> wrote in message
> news:95B2E066-C844-4200-95F0-91C59753EBD3@microsoft.com...
> > Thanks Steve,
> >
> > I had almost come to this conclusion myself after searching on the web,
> > but
> > you have confirmed my suspicions. If possible, I would like to secure all
> > traffic to DCs except for the logon etc traffic that needs to be
> > unsecured. I
> > think I need to set specific filters to allow unsecured domain membership
> > traffic to/from DCs, but to secure all other traffic. I'm unsure exactly
> > what
> > traffic needs to be excluded. Can anyone tell me the protocols and ports
> > used in 'domain membership' communications between DCs and domain
> > computers?
> >
> > Thanks again,
> > Dave
> >
> >
> > "Steven L Umbach" wrote:
> >
> >> My guess is that since you enabled this at the domain level you are
> >> causing
> >> problems with domain computers accessing domain controllers since domain
> >> controllers are also the kerberos key distribution centers. When you
> >> configure an ipsec policy in the domain you must exempt domain
> >> controllers
> >> from ipsec negotiation. The is best done by adding a filter list to the
> >> ipsec policy with a rule for permit action for all traffic to and from
> >> domain controllers by their static IP addresses. It is best to not
> >> configure
> >> an ipsec policy at the domain level but instead do it at the OU level.
> >> The
> >> link below explains more. --- Steve
> >>
> >> <http://support.microsoft.com/default.aspx?scid=kb;en-us:254949>
> >>
> >> "D Hartry" <DHartry@discussions.microsoft.com> wrote in message
> >> news:9AB91D6A-8FC9-42E2-BB1A-2915EC6CED15@microsoft.com...
> >> > I have been fiddling with IPsec on a test network running in VMWare.
> >> > I've
> >> > not set up IPsec policies before so am unsure if I have done something
> >> > stupid, perhaps made a mistake many have before me.....??
> >> >

Re: IPsec: Network sooo sloooooow

> > > *I have a simple network of two servers (2003 Ent) and a client (XP Pro
> > > SP2).
> > > One server is an offline root standalone CA, the other a DC and
> > > enterprise
> > > sub-CA. This autoenrolls certificates to users and computers.
> > >
> > > I have enabled the Server (respond) policy for the entire domain, and
> > > with
> > > the policy active, I can log onto the DC from the XP client, but very
> > > slowly.
> > > From the DC I can monitor the SAs, they are being set up between the DC
> > > and
> > > the XP client.
> > >
> > > I get the same result whether I set the authentication for the policy
> > > to
> > > certificates or kerberos, I have tried with both.
> > >
> > > It might also be relevant that the DC is running the highsecdc.inf and
> > > the
> > > client the highsecws.inf security templates. I am going to try the
> > > scenairo
> > > without any security policy in place next.
> > >
> > > Any ideas why the IPSec policy would 'work' but slow the network down
> > > so
> > > much? eg The XP client has been logging on, at the 'applying computer
> > > settings/'applying your personal settings' stage for about 5-10
> > > minutes
> > > now.
> > >
> > > I understand that there is an overhead associated with IPSec, but
> > > surely
> > > not
> > > this much? Even given the fact that the machines are VMs? BTW the
> > > physical
> > > machine this is all running on is an Athlon 2.2GHz with 512MB RAM, Big
> > > disks.
> > >
> > > --
> > > David Hartry
> >>
> >>
> >>
>
>
>*