

microsoft.public.win2000.security: Re: Why doesn't IPSEC respect revoked certificates.

Re: Why doesn't IPSEC respect revoked certificates.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-06/2765.html>

From: PB (<_@no_where.nospam>)

Date: 06/29/02

From: "PB" <_@no_where.nospam>
Date: Sat, 29 Jun 2002 04:48:25 +0100

Hello David,

Thanks for your response – but it still doesn't work.

I have set up a new certificate authority (and removed all the old certificates used for this test)– issued and installed only two IPSEC Certificates – one for the SMTP server one for the SMTP "Client".

Made the registry changes to the SMTP Server for
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent\StrongCRLCheck=0x1 etc

Set the publication schedule of the CRL to 1 hour.

Created IPSEC Policies to secure port 25 traffic using the new certificate authority's certificates/

I can test the traffic with IPSECMON – and yes I have IPSEC working for port 25.

I have then revoked at the CA the IPSEC Certificate used by the client.

Now from this point I've done just about everything I can think of to get the Server to reject a connection using IPSEC from the client.

The published CRL contains the revoked certificate.
The Certificate MMC snap in on the server shows that the Revoked Client IPsec Certificate is in the CRL under Local Computer::Intermediate Certification Authority::Certification List.

I've rebooted the server.
I've rebooted the client.

I've waited 5 hours and more!

Re: Why doesn't IPSEC respect revoked certificates.

microsoft.public.win2000.security: Re: Why doesn't IPSEC respect revoked certificates.

And still the Server will negotiate IPSEC where the client is using the revoked Certificate.

(I do not have the Client doing StrongCRLCheck – since I figure that if a Client is in the hands of a miscreant then I cannot be sure that they haven't just changed the Registry and also removed any CRL that might have the certificate revoked.)

Any more help of guidance would be appreciated? (We can take this offline from the newsgroup if you would like me to contact you direct – I have your internal MS email)

Peter

"D. Cross" <vaq130@alias.hotmail.com> wrote in message news:OHFZNzqHCHA.2464@tkmsftngp10...

> *You are probably seeing a cached CRL which is normal and expected behavior.*

> *when the old CRL expires, the new one should be downloaded and then the revocation will work.*

>

>

> <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechn>

> *ol/WinXPPro/support/tshtcrl.asp*

>

> --

>

> *David B. Cross [MS]*

>

> --

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

>

> *"PB" <_@no_where.nospam> wrote in message*

> *news:_zLS8.1487\$xn1.132419@news8-gui.server.ntli.net...*

>> *For the purposes of this test I setup*

>>

>> *1) Enterprise Certificate Authority,*

>> *2) issued Offline IPSEC Certificates to two machines – both in different*

>> *domains.*

>> *3) Created IPSEC Policies that require IPSEC for port 25 traffic– using*

>> *a*

>> *Certificate from the Enterprise CA.*

>> *4) On the Email 'Server' (on which the Enterprise CA is hosted) I created*

>> *the registry entries in*

>>

>>

>>

Re: Why doesn't IPSEC respect revoked certificates.

microsoft.public.win2000.security: Re: Why doesn't IPSEC respect revoked certificates.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent\StrongCRLCh

> > *eck=0x1 etc*

> > *5) I also configured the EnableLogging registry entry.*

> >

> > *6) Restarted IPSEC Policy Agent on both machines.*

> > *7) Ran up the IPSECMON tool.*

> >

> > *Now Port 25 traffic does indeed negotiate IPSEC – and the certificates do*

> > *need to be on the Server and the Client – or else it doesn't work.*

> >

> > *So far so good I have what I want.*

> >

> > *BUT assume then that the Client machine is stolen or in a miscriant's hands*

> > *or whatever and I want to revoke the certificate – I can revoke the*

> > *certificate for the AWOL Client at the Enterprise CA, and can publish a new*

> > *CRL. – but this CRL is not respected by the server and the client can*

> > *continue to connect port 25 traffic even though it's IPSEC certificate is*

> > *supposedly revoked – and that StrongCRLCheck in the registry is set.*

> >

> > *I've tried just about every combination of rebooting and the like and*

> > *restarting IPSEC Policy Agents – but to no avail.*

> >

> > *So what is it that I'm missing? Is this really something that just doesn't*

> > *work? I'm supposed to be writing an article on this but at the moment it*

> > *is*

> > *looking like I'd be publishing that it doesn't work as it indicates that*

> > *it*

> > *should.*

> >

> > *Any help would be appreciated.*

> >

> >

>

>