

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/2002-06/2727.html>

From: D. Cross (vaq130@alias.hotmail.com)

Date: 06/28/02

From: "D. Cross" <vaq130@alias.hotmail.com>

Date: Fri, 28 Jun 2002 07:05:52 -0700

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/prodtechnol/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

>

>

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

Re: Why doesn't IPSEC respect revoked certificates.

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

> 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.
>
>