

Re: AD Proxy

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-07/msg00543

- *From:* "Hugh" <Hugh@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 7 Jul 2005 13:34:03 -0700
-

Yes, they would be based on AD credentials. Sorry for the confusion.

Specifically, here's what we've got. In the SecureNet, we will have AIX systems which are running Vintela Authentication Services (VAS), which tightly integrates these systems with AD. In fact, the AIX systems are "joined" to AD (via Kerberos) just as any Windows XP PC would be. These AIX systems will be used by individuals in the SecureNet as well as by individuals in the internal network. As an example, when you telnet to the AIX box, the userid and password you enter reside only in AD, not as local accounts on the AIX box. The VAS software then passes the userid and password to AD for authentication. Group membership also provides permissions to the AIX box's filesystems.

Any given user may access the AIX box via the SecureNet today and via the internal network tomorrow. Thus, we would prefer a single identity store.

The AIX systems in the SecureNet must be able to be domain members, but since the SecureNet will also contain non-company computers (VPN clients), we would prefer not to put a production domain controller in the SecureNet.

Since th

--

Hugh

"Al Mulnick" wrote:

- > You lost me.
- > If you need AD/Kerberos authentication services, would that not be based on
- > AD credentials? You're not interested in allowing services across the
- > firewall (somehow you'll need time and DNS services that reflect trusted
- > network information of course), I get that. But you are interested in
- > authentication services. That is what I'm talking about.
- >
- > Maybe there's a bigger picture I'm not seeing? How do you plan to have the
- > clients ask for authentication services? Is this something in the VPN
- > client that allows them to even connect to this network? If so, maybe
- > there's a better way to do this other than what we've talked about so far.

Re: AD Proxy

> RADIUS, AZMAN, or others might be worth investigating.
>
> Al
>
>
>
> "Hugh" <Hugh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
> news:CC52EFEA-A075-4485-8C57-4024B0E5E88D@xxxxxxxxxxxxxxxxxxxx
>> Active Directory integration seems to be useful for controlling access
>> across
>> the firewall based upon AD credentials. If so, this isn't what we're
>> trying
>> to do. We need AD/Kerberos authentication services in the SecureNet, but
>> no
>> other traffic from the SecureNet will be allowed through the firewall.
>> --
>> Hugh
>>
>>
>> "Al Mulnick" wrote:
>>
>>> Hopefully you get a good response from that group. I would imagine it
>>> can
>>> be done fairly easily, but not sure just how easily.
>>>
>>> Active Directory integration
>>> ISA Server can leverage the user database stored in Active Directory
>>> to
>>> authenticate both inbound and outbound access through the firewall.
>>> Active
>>> Directory integration is available even when the ISA Server computer is
>>> not
>>> a member of an Active Directory domain.
>>>
>>>
>>>
>>> You can read more about it here:
>>> <http://www.microsoft.com/isaserver/evaluation/features/default.msp>
>>>
>>> In my mind, you would basically publish the AD servers via ISA to the VPN
>>> network. When you give name resolution information to the vpn client,
>>> they
>>> would use that information to find the AD servers and the ISA server
>>> would
>>> proxy the authentication for you. LDAP might be a little more attached
>>> to
>>> your application if that's what it's for.
>>>
>>> Al
>>>
>>>

Re: AD Proxy

>>> "Hugh" <Hugh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>>> news:E84980BB-AACF-47E9-BF63-BB873AB5A838@xxxxxxxxxxxxxxxxxxxx
>>> > I've put a similar post in the ISA Server area, but we have no
>>> > experience
>>> > with ISA Server at this time.
>>> > --
>>> > Hugh
>>> >
>>> >
>>> > "Al Mulnick" wrote:
>>> >
>>>> Have you already looked at what ISA server can do for you?
>>>>
>>>> Al
>>>>
>>>> "Hugh" <Hugh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>>>> news:79DEDFE7-BFA3-46DA-B03B-877C8F70C330@xxxxxxxxxxxxxxxxxxxx
>>>> > We are creating a secure DMZ area (VPN access only) and would like
>>>> > to
>>>> > have
>>>> > AD
>>>> > services in this network. This "SecureNet" will be firewalled off
>>>> > from
>>>> > the
>>>> > internal network. Rather than putting a domain controller in the
>>>> > SecureNet,
>>>> > we would prefer to put an LDAP proxy server that would accept LDAP
>>>> > requests
>>>> > from systems in the SecureNet and forward those requests through the
>>>> > firewall
>>>> > to the internal domain controllers. Specifically, I said "AD" proxy
>>>> > instead
>>>> > of "LDAP" proxy because I need Kerberos services to be proxied as
>>>> > well.
>>>> > Thus, I need the proxy server to appear and act just like an AD
>>>> > domain
>>>> > controller for the purposes of authentication. Any thoughts on
>>>> > whether
>>>> > this
>>>> > is possible and, if so, how to accomplish it?
>>>> >
>>>> > --
>>>> > Hugh
>>>>
>>>>
>>>>
>>>
>>>
>>>
>>>
>
>

>
.

-
- ***Follow-Ups:***
 - ◆ ***Re: AD Proxy***
 - ◇ *From:* Al Mulnick

 - ***References:***
 - ◆ ***AD Proxy***
 - ◇ *From:* Hugh
 - ◆ ***Re: AD Proxy***
 - ◇ *From:* Al Mulnick
 - ◆ ***Re: AD Proxy***
 - ◇ *From:* Hugh
 - ◆ ***Re: AD Proxy***
 - ◇ *From:* Al Mulnick
 - ◆ ***Re: AD Proxy***
 - ◇ *From:* Hugh
 - ◆ ***Re: AD Proxy***
 - ◇ *From:* Al Mulnick

 - Prev by Date: ***RE: restricted groups?***
 - Next by Date: ***RE: restricted groups?***
 - Previous by thread: ***Re: AD Proxy***
 - Next by thread: ***Re: AD Proxy***
 - Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***