

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-07/msg00253

- *From:* "Chris Swinney" <swin@xxxxxxxxxxxxxx>
 - *Date:* Sun, 6 Jul 2008 20:12:33 +0100
-

I will look into WebEx. The "Password" is just an example of the administration I would expect to have. I can just see it being tough to manage lots of individual computers, unless they are somehow tied to a central directory.

Chris

"Anthony [MVP]" <anthony@xxxxxxxxxxxxxx> wrote in message news:OR%23DFTa3IHA.5112@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I don't know if they have a "change password" button, but you can script it if not,
Anthony,
<http://www.airdesk.co.uk>

"Chris Swinney" <swin@xxxxxxxxxxxxxx> wrote in message news:OjPwcYX3IHA.2524@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Anthony,

Many thanks for these informative replies. I had been breaking out into a cold sweat just thinking about creating an unwieldy IPSEC VPN network. A lot of the machines connect to Cisco gatekeepers, but this is not my area and I am unsure if they contain any VPN functionality within their IOS software revision.

We obviously want to be able to make global changes to what effectively will be stand alone systems. Can Webex, for example, allow us to make a change to a user's password across all user accounts with the same name? We are trying to implement a password policy and change 200 machines individually is a little time consuming. I have only ever managed such tasks in a domain environment.

Chris

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

"Anthony [MVP]" <anthony@xxxxxxxxxxxx> wrote in message
news:%23X09xaP3IHA.4284@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Chris,
Just to give a slightly fuller answer.
You can't run AD in that sort of dispersed environment by opening ports.
The firewalls would never allow it. Even if they did, they would have to put you in a DMZ so as not to open up their whole network. You would on practice have your machines open on the internet. You could run IPSec between all the machines, in effect creating machine to machine VPN's. This would be a large job to administer. You would also need all the firewalls to allow your IPSec connections into their networks. This is the best link I can find to give you an overview of this: <http://support.microsoft.com/kb/816514>. If you were going down this route, it would almost be simpler to provide your own small VPN router in front of the remote computer and use that to create a VPN network.
All this assumes that you have sufficient control over the firewalls, but in my experience it is very hard to manage or co-ordinate these sort of changes to firewalls. Most people are fairly reluctant to allow stuff in, and it can be difficult and time consuming to troubleshoot problems. You can't see the firewall rules, so you have to rely on them to help you make it work.
I mentioned Webex for two reasons. One is that it is hard to manage any remote machine if you don't have access. As you say, there are several alternatives for this. The second is that they also provide agents that give you the control you were asking for. These are an OEM version of Everdream, which was recently bought by Dell. There are other ways of doing this as well. As I said, we manage servers fully behind firewalls

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

that we don't control, and without AD.
Hope that helps,
Anthony
<http://www.airdesk.co.uk>

"Anthony [MVP]" <anthony@xxxxxxxxxxxx> wrote in message
<news:OjsjRfJ3IHA.2348@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Chris,
If you have enough control over the firewalls
you could use IPSEC, yes,
Anthony,
<http://www.airesk.co.uk>

"Chris Swinney" <swin@xxxxxxxxxxxx>
wrote in message
<news:OV4%23LuG3IHA.2336@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Just to let you know,
something similar can be
done with different VNC
flavours, such as UltraVNC,
using a repeater. Anyhow,
this still does
not satisfy all requirements
as previously illustrated

Even though we are going
through foreign firewalls,
we do have a
certain degree of sway with
the Network managers' to
allow certain
traffic. Any management
traffic would need to be sent
encrypted so I
am wondering if this could
be sent using IPSEC or SSL
so utilising
just one or two open
ports/protocols.

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Any further thoughts?

"Anthony [MVP]"

<anthony@xxxxxxxxxxxx>

wrote in message

news:%23Gj3pSE3IHA.3544@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Chris,
VNC will
not work
through
standard
firewalls,
but Webex
Remote
Access
will,
because it is
an outbound
connection
to an
intermediary.
We manage
remote
servers fully
without
using AD.
Anthony,
<http://www.airdesk.co.uk>

"Chris

Swinney"

<swin@xxxxxxxxxxxx>

wrote in

message

news:OoH8RID3IHA.4800@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Many
thanks
for
this.
At
a
simple
level,
we
already
use
remote

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

management
tools
such
as
VNC
to
manage
some
of
these
workstations,
however
not
all
(because
of
firewall
restraints)
can
be
managed
in
this
way.
Still,
remotely
managing
the
desktop
is
only
part
of
the
problem.
A
central
management
point
is
required
that
is
able
to
be
use
to
push
out
key

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other instiutions firewalls?

changes
to
all
desktops,
maybe
such
as
would
be
available
using
Group
Policy.
In
addition,
some
management
applications
(such
as
software
firewall
policies)
require
AD
integration.

Chris

"Anthony
[MVP]"
<anthony@xxxxxxxxxxxx>
wrote
in
message
news:OldbPLA3IHA.2424@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Chris,
AD
is
only
one
way
of
creating
a
shared
security
context

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other instiutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

between
machines.
It
would
not
work
in
your
case,
as
the
firewalls
will
not
allow
AD
traffic.
Something
like
Webex
Remote
Access
would
allow
you
to
control
all
the
machines.
Anthony,
<http://www.airdesk.co.uk>

"Chris
Swinney"
<swin@xxxxxxxxxxxxxx>
wrote
in
message
news:eZg1rG92IHA.5060@xxxxxxxxxxxxxxxxxxxxxxxx

Or
is
this
even
a
practical
deployment
scenario

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

for
AD?

"Chris
Swinney"

<swin@xxxxxxxxxxxxxx>

wrote

in

message

news:%23c5Cz182IHA.4476@xxxxxxxxxxxxxx

Hi,

We
maintain
a
wide
network
of
PCs
(Win
2000
and
XP,
approx
200–300
machines).
Most
of
these
are
single
use
machines
designed
for
use
in
a
Video
Conference
environment.
The
machines
are
effectively
standalone
with
public
IP's,

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

and
they
are
deployed
in
various
institutions,
some
behind
firewalls
that
we
don't
manage.
Although
we
have
a
certain
amount
of
sway
with
the
other
network
managers
to
allow
traffic
to
and
from
these
machines,
we
obviously
do
not
have
full
control
over
ALL
the
traffic
that
can
be
passed
to

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

them.

I
feel
that
if
we
can
create
a
secure
AD
environment
to
centrally
manage
these
machines
it
would
be
beneficial.
I'm
not
entirely
sure
what
ports/protocols
need
to
be
configured
to
allow
AD
traffic,
and
then
if
this
traffic
can
be
secured
across
foreign
firewalls.

Is
there
a

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

Re: Is it possible to create a secure AD environment for widely dispersed PC's behind other institutions firewalls?

way
to
create
such
an
environment?

Many
thanks
for
any
insight
or
articles
you
may
have.

Chris