

Re: Secure File Transfers

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-09/0206.html>

From: Jono (jono_at_discussions.microsoft.com)

Date: 09/22/05

Date: Thu, 22 Sep 2005 00:46:01 -0700

Both server are physically next to each other, but connected to different networks.

One network faces the Internet, the other is an internal network that cannot be exposed to the Internet for security reasons.

We need to transfer data from the Internet server to the internal server securely, ideally without the user being able to affect the data and without introducing any viruses.

In an ideal world there would be no user intervention, if we could find some device that would allow only the CSV file that needs to be moved to come across.

"Steven L Umbach" wrote:

> *I would need more information about the device though I wonder if it just is
> a USB network adapter. I was under the impression that one server was at a
> remote location connected via the internet and the challenge would be secure
> file transfer over the internet. Maybe I misunderstood?? --- Steve*

>

>

> *"Jono" <jono@discussions.microsoft.com> wrote in message
> news:F1E68BAA-D63F-4BAA-9BBD-AAC2B1BAA8AC@microsoft.com...*

> *Thanks for the info.*

>>

>> *Just out of interest, what do you think of this device.*

>>

>> *I've seen a USB device that basically plugs into both servers to allow
>> files*

>> *transfers as and when necessary.*

>>

>> *"Steven L Umbach" wrote:*

>>

>>> *A VPN solution [virtual private network] would work but add complexity of
>>> configuration if you do not already have one in place though ipsec*

>>> *endpoint*

>>> *devices are affordable these days and can create a encrypted ipsec tunnel*

> >> *between the networks. This sounds like something you do occasionally and*
> >> *you*
> >> *could use Remote Desktop or Terminal Services in remote administration*
> >> *mode*
> >> *to access the computer and transfer the files. RDP by default will use*
> >> *encryption [you should configure the server to only accept high*
> >> *encryption]*
> >> *and configure the encrypted tunnel before user authentication is*
> >> *attempted.*
> >> *The downside to that is leaving your computer port 3389 TCP exposed to*
> >> *the*
> >> *internet. If you can configure your firewall or even an ipsec filter on*
> >> *the*
> >> *server to only accept port 3389 TCP connections from a specific public IP*
> >> *address that can greatly increase the security of using RDP over the*
> >> *internet. Otherwise you still can use it but be sure to use complex*
> >> *passwords for the users that are allowed access via RDP. The link below*
> >> *may help. --- Steve*
> >>
> >> http://www.windowsecurity.com/articles/Windows_Terminal_Services.html
> >>
> >> *"Jono" <jono@discussions.microsoft.com> wrote in message*
> >> *news:2DED0A55-6574-4869-A34D-CD5D1EF5DF4B@microsoft.com...*
> >> > *We have two servers that are on different networks, one on a closed*
> >> > *internal*
> >> > *network and one an external network, connected to the Internet.*
> >> >
> >> > *We need to transfer data from the external server onto the server on*
> >> > *the*
> >> > *internal network.*
> >> >
> >> > *At the moment we copy the data onto a floppy disk and then transfer it*
> >> > *to*
> >> > *the internal server, after virus checking.*
> >> >
> >> > *Does anyone know any other ways to securely transfer the data?*
> >>
> >>
> >>
>
>
>