

Re: Problem with certificates/L2TP VPN

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2008-03/msg00324.html>

- *From:* "Bill Grant" <not.available@online>
 - *Date:* Sun, 23 Mar 2008 10:16:20 +1100
-

I certainly agree with your PS. I would never recommend changing to L2TP unless there was an established certificate service (and somebody who understood it). Ditto for SSTP in server 2008.

"Paul Weterings" <Paul-nospam-@syncpuls-dot-com> wrote in message [news:47e58bc8\\$0\\$25712\\$e4fe514c@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:47e58bc8$0$25712$e4fe514c@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I'm assuming you are testing on a LAN without any firewalls in between?

Does the ECU extension (Enhanced Key Usage) on the client contain the 'Client Authentication Purpose' or IPSec purpose? On the VPN server does the ECU extension contain the Server & Client Authentication purpose?

p.s. PPTP isn't that bad you know... It's not -insecure-, just less secure than L2TP, and a lot easier to implement

/) Regards,
// _____
|||_) Paul Weterings
/(O_)
/ (O)
____(O_)

dpetrek wrote:

So we have a Windows 2000 RRAS VPN server which has been serving us with PPTP VPN service for a long time now. We decided to upgrade security and implement L2TP. So I installed standalone CA and installed CA ROOT ccert on both RRAS server and test client. I can see the cert in "Trusted Root Certification Authorities" on both RRAS server and client. Also I issued computer certs to RRAS server (purpose: Server Authentication) and client (purpose: Client Authentication). That should finish the story with certs. However when I try to establish VPN connection from client I get:

Error 786: The L2TP connection attempt failed because there is no valid machine certificate on your computer for security authentication.

Re: Problem with certificates/L2TP VPN

Also I have following in Security log:

IKE security association negotiation failed.

Mode:

Key Exchange Mode (Main Mode)

Filter:

Source IP Address 192.168.0.33

Source IP Address Mask 255.255.255.255

Destination IP Address 192.168.0.15

Destination IP Address Mask 255.255.255.255

Protocol 0

Source Port 0

Destination Port 0

IKE Local Addr 192.168.0.33

IKE Peer Addr 192.168.0.15

IKE Source Port 500

IKE Destination Port 500

Peer Private Addr

Peer Identity:

Certificate based Identity.

Peer Subject

Peer SHA Thumbprint 00

Peer Issuing Certificate Authority

Root Certificate Authority

My Subject CN=HP-SERVER test cert

My SHA Thumbprint 0fd6eb25c8ba67e79b97457014a4b8803b05eb3c

Peer IP Address: 192.168.0.15

Failure Point:

Me

Failure Reason:

IKE failed to find valid machine certificate

Extra Status:

Processed second (KE) payload

Initiator. Delta Time 0

0x80092004 0x100

Please advise, what have I done wrong?