

Re: Routing and Remote Access – Authentication Failure

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2009-05/msg00065.html>

- *From:* "George Valkov" <a@xxxxx>
 - *Date:* Thu, 7 May 2009 20:01:09 +0300
-

"Matrixx333" wrote in message

news:ffd8287f-27ed-4638-8923-fbddada9407b@xx

> <http://i43.tinypic.com/rvd2l1.png>

|

| Looks fine

|

> <http://i41.tinypic.com/2ez0n7k.png>

|

| Looks fine

|

> <http://i44.tinypic.com/s49rsy.png>

|

| Looks fine

|

> <http://i39.tinypic.com/2wew9yf.png>

|

| This might be a problem. I understand you said the VPNSERVER and the
| CLIENT were on the same network segment, but if your using your
| VPNSERVER as a secure way to access a remote network, then "Routing"
| needs to be checked to access any other remote network beyond the
| VPNSERVER.

I think that the answer to that remark would be: Router is not needed, because the real client computer can tunel through it's local NAT router, travel the Intrenet, join the VPN and access the server, when this feature is disabled.

Initially the Router feature was enabled and I tried either sub-options... either way, if I use CHAP I'll get unknown user name or password error. I disabled the Router, because I didn't want to have features enabled that I can do without.

When I wrote my first message, I decided to omit a few details – some that I thought were less important, so that we can focus on: why I get the "unknown user name or password" error. Here are the details:

My aim is to put the server and the client on the same LAN (VPN) so that

Re: Routing and Remote Access – Authentication Failure

they can use File and Printer Sharing. The client already has internet connectivity so the VPN server does not need to offer that to the client. Infact initially the server did offer that functionality, but that caused a problem with my ISP:

in short, the client decided to access the internet from the VPN interface, the server rerouted that to the gateway of the ISP, which received a packet from the MAC of the server, but with IP that my ISP has assigned to the client PC. Their security system decided that the server was trying to steal the IP address of the client and they blocked access to server's MAC. After 4 phone calls to unblock the server internet connection we finally figured out what exactly happens so I took measures to prevent the VPN side from accessing anything outside it's scope. – I disabled Router and assigned proper IP filtering.

I said that the VPNSERVER and client are on the same LAN. Sure they already have File and Printer sharing, but that's only a laptop I had in hand for the test. The real client computer is in another town and is behind a NAT router, so it has to join the VPN.

Or...? Hm, would it be possible to use IPSec and create tunnel for all ports used by File and Printer Sharing between the server and a client that is behind a NAT router? If yes than I don't need to set a VPN.

| > <http://i42.tinypic.com/2h32cqx.png>

|

| At the bottom you have "Allow custom IPSec Policy for L2TP connection" and it looks like you have a pre-shared key typed in. If the client doesn't also have this key configured, the connection will fail.

I am aware of that, but notice that it says "Allow" and not "Force". According to my tests, if the client does not enable ISpec it will still connect without security. And if the client enables IPSec and enters a correct preshared key, it will establish a secure tunnel for the VPN connection, despite it's still using PAP or SPAP and unsecured VPN.

|

| > <http://i43.tinypic.com/5b8arm.png>

|

| Looks fine

|

| > <http://i39.tinypic.com/2ljt7js.png>

|

| Generally, if you have a DHCP server on the network, you wouldn't want to configure a static address pool, as Ace had mentioned. Also, is the scope of the static address pool in the same subnet as the network you are trying to access from the VPNSERVER? If not, you wont be able to access anything beyond the VPNSERVER.

Re: Routing and Remote Access – Authentication Failure

And then the VPN server will relay the DHCP to that DHCP server, instead of the static pool that I configured. But I don't need additional DHCP server. There will be only two hosts in the VPN, the VPNSERVER and the client. I was also planning to assign a static IP on the user account's Dial-in configuration page.

| > <http://i40.tinypic.com/a32mbc.png>

|
| Not really applicable unless you were using ISDN or multiple modems to
| establish the vpn connection

Thanks for the remark!

| I know for MS-CHAP v1 the password cannot exceed 14 characters, but as
| Ace had mentioned, any non-windows machine is going to use CHAP
| anyways. I would also agree with Ace's advise about using the password
| requirements for your domain, if you are on one.

I think that this answers one of my questions!
Probably PAP and SPAP are limited to 14 characters too.
I'm not planning to have non windows clients for now.
The password "1" was temporary set for testing only. By default my server
has the complex password requirements and minimum password length set to 10.

This reminds me that the password policy on the server is even more secure.
I just thought about what setting could be the cause:

Local Security Policy/ Local Policies/ Security Options/
Network security: Do not store LAN Manager hash value on next password
change
=ENABLED

Since the LM hash is not stored, it can't be attacked, and the NTLM hash is
supposed to be much harder to crack (not to mention that account lockout is
enabled). If some one tries to logon using a LM hash, since there's no LM
hash stored, the logical result would be "unknown user name and password".

And if that is the case, would it be possible to force the use of NTLM hash
for authentication, I don't want to relay on the LM hash?

EDIT:

I created a password that has both NTLM and with LM hashes, but still get
"unknown user name or bad password".

I have also altered a few other settings to make my server even more secure
(but they are probably not related to my problem):

Re: Routing and Remote Access – Authentication Failure

Network security: LAN Manager authentication level
=Send NTLMv2 response only\refuse LM & NTLM

Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

=Require message integrity;

Require message confidentiality;

Require NTLMv2 session security;

Require 128-bit encryption.

| Speaking of Domain or Workgroup, the account you are using to
| establish the connection must either be in AD or configured in the
| local SAM of the VPNSERVER if it is a workgroup.

Yes, it is allowed to dial-in in the SAM on the VPNSERVER.

| If you are on a
| domain and have an account in AD, I would suggest looking at the
| Remote Access Policies in Routing and Remote Access. Is the username a
| member of a group that hasn't been configured with a Remote Access
| Policy? Does the AD account have dial-in permissions? Also the client,
| server, and policy all have to be configured with at least one common
| authentication protocol and encryption strength.
| Hope this helps.

Thank You, Matrixx333! :-)

George Valkov

.