

## Re: IPSEC Failing (Secure Server)

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2004-11/0591.html>

---

**From:** Robert L [MS-MVP] ([noreply\\_at\\_hotmail.com](mailto:noreply_at_hotmail.com))

**Date:** 11/17/04

Date: Wed, 17 Nov 2004 15:45:31 -0600

this may help. quoted from <http://www.ChicagoTech.net>  
Troubleshooting IPsec

1. Audit Policy: To troubleshoot IPsec when it does not behave the way that you expect it to, first check the results of the Phase One and Phase Two exchanges by enabling Audit Policy, which causes security events to be logged in the security log of the Event Viewer.
2. Netdiag: netdiag /test:ipsec /debug. If both Phases are Outbound or Inbound, check Tunnel Settings.
3. If the logged events indicate that Phase One Main Mode exchange is failing, do both of the following: 1) Check the IKE settings in your IPsec policy properties: Click the General tab, click the Advanced tab, and then click the Methods tab. 2) Check the configured IKE authentication methods in your IPsec policy properties: Select the IP Security rule that you want to check, click Edit, and then click the Authentication Methods tab.
4. If the logged events indicate that Phase Two Quick Mode is failing, check the IPsec security methods configured on your IPsec rules in your IPsec policy properties: Select the IP Security rule that you want to check, click Edit, select the Filter Action tab, select the filter action that is enabled, and then click Edit.
5. IP Security Monitor: The IP Security Monitor can be used to monitor SAs, IPsec, and IKE statistics. To start IP Security Monitor, click Start, click Run, and then type ipsecmon.
6. Checking Oakley Log: To enable Oakley Log, use Registry Editor to locate the following key in the registry, and if it does not exist, create it:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley  
Add a REG\_DWORD value named EnableLogging with a value of 1 to this key. The Oakley.log file is created in the %SystemRoot%\debug folder. NOTE: A value of 0 for EnableLogging disables logging.
7. Check VPN server log.

--

For more and other information, go to <http://www.ChicagoTech.net>  
Don't send e-mail or reply to me except you need consulting services.  
Posting on MS newsgroup will benefit all readers and you may get more help.  
Bob Lin, MS-MVP, MCSE & CNE  
Networking, Internet, Routing, VPN, Anti-Virus, Tips & Troubleshooting on  
<http://www.ChicagoTech.net>  
Networking Solutions, <http://www.chicagotech.net/networksolutions.htm>  
VPN Solutions, <http://www.chicagotech.net/vpnsolutions.htm>

microsoft.public.windows.server.networking: Re: IPSEC Failing (Secure Server)

VPN Process and Error Analysis, <http://www.chicagotech.net/VPN%20process.htm>  
VPN Troubleshooting, <http://www.chicagotech.net/vpn.htm>  
This posting is provided "AS IS" with no warranties.  
"Aaron" <Aaron@discussions.microsoft.com> wrote in message  
news:4DEDBBBE-DA95-4CBB-9803-AFDDE7452CE2@microsoft.com...  
> Server A has local policy configured as Secure Server(Require Security).  
> Client B has local policy configured as Client(Respond Only). Both A and  
> B  
> are members of the same W2K3 AD domain. Event log error on Server A: IKE  
> security association failed: Key Exchange Mode (Main Mode). Further down  
> it  
> says, Failure Point: Me, Failure Reason: Failed to authenticate using  
> kerberos.  
>  
> Doing some trouble shooting, I found that if I changed the policy on  
> Server  
> A to Server(Request Security) the communication did occur and was  
> encapsulated (verified using NetMon). I also could get this to work if,  
> leaving the policy on Server A on Secure Server, I changed the policy on  
> Client B to Server(Request Security).  
>  
>