

Comdasy FAQ: VPN

Comdasy AG
Rüdesheimer Str. 7
D-80686 München
Tel.: +49.89.5484333-0
Fax: +49.89.5484333-29
support@comdasy.com
<http://www.comdasy.com>

Disclaimer

We have taken all possible care to ensure that this manual contains correct, accurate information. However, the manufacturer cannot assume liability for any possible errors. In addition, the manufacturer cannot guarantee that the hardware will meet the purpose you require.

Comdasys reserves the right to make changes according to technical progress at any time. Brand names may be registered trademarks and must be treated as such.

© Copyright 2005-2008
Comdasys AG
80686 München, Germany

All rights reserved. No part of this manual may be reproduced, processed or distributed in any form (print, photocopy, microfilm or any other process) or processed by an electronic system without prior written permission from the manufacturer.

Inhaltsverzeichnis

| | |
|--|---|
| 1. Hints on configuring IPSEC L2TP Road Warrior Access Tunnels with Windows..... | 4 |
| 1.1. Introduction..... | 4 |
| 1.2. L2TP vs. PPTP..... | 4 |
| 1.3. Advantages of L2TP..... | 4 |
| 1.4. Problems with Windows and L2TP behind NAT..... | 5 |
| 1.5. Other Clients..... | 5 |
| 2. Writing a VPN "watchdog"..... | 5 |
| 2.1. Introduction..... | 5 |
| 2.2. Prerequisite..... | 5 |
| 2.3. Watchdog script..... | 5 |
| 2.4. Cron..... | 6 |

1. Hints on configuring IPSEC L2TP Road Warrior Access Tunnels with Windows

1.1. Introduction

The Convergences are able to support L2TP Tunneling over IPSEC. This type of VPN is often used for realizing a road warrior access. The typical client for this type of configuration are the built in Windows Dial-Up-Networking Facilities. There are two types of VPN Tunnels Windows is able to support, PPTP/IPSEC or L2TP/IPSEC. The following will give an overview over these two types. Comdasys has deliberately chosen to support L2TP only for security reasons.

1.2. L2TP vs. PPTP

One of the choices to make when deploying Windows 2000-based VPNs is whether to use L2TP/IPSec or PPTP. Windows XP VPN client computers and Windows 2000 VPN client and server computers support both L2TP/IPSec and PPTP by default. However, you still must decide whether one or both are supported on your network.

L2TP/IPSec and PPTP are similar in the following ways:

- They provide a logical transport mechanism to send PPP payloads.
- They provide tunneling or encapsulation so that PPP payloads based on any protocol can be sent across an IP network.
- They rely on the PPP connection process to perform user authentication and protocol configuration.
- L2TP/IPSec and PPTP are different in the following ways:
- With PPTP, data encryption begins after the PPP connection process (and, therefore, PPP authentication) is completed. With L2TP/IPSec, data encryption begins before the PPP connection process.
- PPTP connections use MPPE, a stream cipher that is based on the Rivest-Shamir-Aldeman RC-4 encryption algorithm and provides 40, 56, or 128-bit encryption keys. Stream ciphers encrypt data as a bit stream. L2TP/IPSec connections use the Data Encryption Standard (DES), which is a block cipher that uses either a 56-bit key for DES or three 56-bit keys for 3-DES. Block ciphers encrypt data in discrete blocks (64-bit blocks, in the case of DES).
- PPTP connections require only user-level authentication through a PPP-based authentication protocol. L2TP/IPSec connections require the same user-level authentication and, in addition, computer-level authentication through a computer certificate.

1.3. Advantages of L2TP

- IPsec provides per-packet data origin authentication (proof that the data was sent by the authorized user), data integrity (proof that the data was not modified in transit), replay protection (prevention from resending a stream of captured packets), and data confidentiality (prevention from interpreting captured packets without the encryption key). By contrast, PPTP provides only per-packet data confidentiality.
- L2TP/IPSec connections provide stronger authentication by requiring both computer-level authentication through certificates and user-level authentication through a PPP authentication protocol.
- PPP packets exchanged during user-level authentication are never sent in an unencrypted form because the PPP connection process for L2TP/IPSec occurs after the IPsec security associations (SAs) are established. If intercepted, the PPP authentication

exchange for some types of PPP authentication protocols can be used to perform offline dictionary attacks and determine user passwords. By encrypting the PPP authentication exchange, offline dictionary attacks are only possible after the encrypted packets have been successfully decrypted.

1.4. Problems with Windows and L2TP behind NAT

Windows 2000 and Windows XP VPN clients cannot be placed behind a network address translator (NAT) unless the Windows NAT-T Patch is installed on the client. You have to install this patch or Service Pack 2 for Windows XP in order to gain access to your Comdasys Convergence via L2TP VPN.

1.5. Other Clients

Comdasys supports and tests multiple clients with its products. Among these are:

- Windows XP Professional / Home
- Windows 2000 Professional / Server (used as a client)
- Windows Server 2003 (used as a client)
- Microsoft ISA Server is also reported to work.
- The "Microsoft L2TP/IPSec VPN Client" (alias MSL2TP)
- SafeNet SoftRemote and OEM versions such as Netscreen-Remote and CoSine (Sprint Business)
- SSH Sentinel (Note: SSH has sold Sentinel to its competitor SafeNet. Development has ceased. Windows XP with SP2 does not support it.)
- Windows Mobile for Pocket PC 2003

As already mentioned above, there might be problems with these client depending on their versions. If you experience such difficulties with any of the above listed clients please do not hesitate to contact us support@comdasys.com. For further installation instructions concerning your client please consult the documentation of your client software.

2. Writing a VPN "watchdog"

2.1. Introduction

In some environments VPN tunnels (especially IPsec) are not as reliable as they should be. To work around those problems we can use a "watchdog" which periodically pings a host on the other side of the tunnel to test whether the connection is still up and restart the connection if it is down.

2.2. Prerequisite

Before you use the script below, please make sure that you are able to ping the host you'd like to use for testing the VPN connection from your Convergence. If you can't ping the host from your Convergence, the VPN connection will be restarted constantly for no reason.

2.3. Watchdog script

The following script can be used for restarting a VPN connection when the host can't be ping'ed. Please replace 10.42.0.1 with the host you'd like to use for testing the VPN connectivity. Save the script as /etc/vpnwatchdog.sh (it would be erased if you install an update in all other locations).

```
#!/bin/bash
HOST=10.42.0.1
if ! ping -c 1 -w 3 $HOST >/dev/null ; then
    /sbin/rc/rcipsec stop
    /sbin/rc/rcipsec start
    /sbin/rc/rcopenvpn stop
    /sbin/rc/rcopenvpn start
fi
```

2.4. Cron

Now we need to call the watchdog periodically. We do this by creating a file `/etc/cron.d/vpnwatchdog` with the following content:

```
*/15 * * * * root /bin/bash /etc/vpnwatchdog.sh
```

This will start the watchdog every 15 minutes (`*/15`), if you'd like to test every 5 minutes you can use `*/5`. Testing every minute is done by omitting the slash and number.