# Contents

VPN with L2TP and certificates and the Mac OSX VPN-client ................................................................. 3

1 Configuration of the appliance .............................................................................................................. 4
  1.1 Setting up network-objects in the Securepoint Security Manager .................................................. 4
  1.2 Creating firewall-rules ...................................................................................................................... 5
  1.3 Setting up certificates ....................................................................................................................... 6
  1.4 L2TP basic settings .......................................................................................................................... 10
  1.5 L2TP-configuration ......................................................................................................................... 11
  1.6 Setting up users ............................................................................................................................... 15

2 Configuration of the Mac OSX-L2TP-VPN-Roadwarrior under Mac OSX ..................................... 16
  2.1 Importing the client certificate over the Mac OSX keychain ....................................................... 16
  2.2 Setting up the VPN-connection ...................................................................................................... 19
VPN with L2TP and certificates and the Mac OS X VPN-client

A VPN connects one or several computers or networks by using a different network, e.g. the internet, as a means of transport. For instance, this could be the computer of a member of staff at their home or in a subsidiary which is linked to the network at the headquarter through the internet.

For the user, the VPN looks like a normal network connection to the destination computer. The actual way of transmission is not perceived. The VPN provides the user with a virtual IP-connection which is tunneled by an actual one. The data packages transmitted via this connection are encoded at the client and decoded by the Securepoint servers - and the other way around.

Target: Establishing a VPN-L2TP with certificates between the Securepoint appliance and a Mac OS X L2TP-client.
Prerequisite: The L2TP connection was tested under Mac OS X 10.4.9 (Intel). The minimum requirement is Mac OS X 10.4.X. Only with this you will be able to import the PKCS#12 certificates with L2TP.
1 Configuration of the appliance
1.1 Setting up network-objects in the Securepoint Security Manager

Proceed as follows:

- Over Firewall select the folder Network objects.
- Set up network-objects as shown in the following image.

![Network-objects Image](Image: Network-objects)
1.2 Creating firewall-rules

Proceed as follows:

- **Over Firewall select the folder Rules.**
- **Set up the firewall-rules as shown in the following image.**

*Image: Firewall Rules*
1.3 Setting up certificates

Proceed as follows:

- **Over VPN** select the folder *Certificates.*

![Image: Certificates]

First the Certification Authority (CA) with which the server-certificate and the client-certificates are signed, has to be established. Therefore, a root certificate is created first.

- Click on the icon *New* and select *Root certificate.*
- Insert the data as shown in the following image.
After a CA has been created, server- and client-certificates can be generated. A server is required and a client-certificate for each Roadwarrior. The Mac OSX L2TP client requires as IPsec ID the host name of the firewall server with which it is connected. In our example, this is the DynDNS name of the firewall. It is inserted in the area X.509 V3 Name.

- Click on the icon *New* and then select *User / server certificate*.
- Insert the data as shown in the following image.

![Image: Creating a server certificate]

In the following step, client-certificates are needed.

- Click the icon *New* and select *User / server certificate*.
- Insert the data as shown in the following image.

![Image: Creating a client-certificate]
After creating the client-certificate, now export the certificates for usage on a Roadwarrior.

- Click on the icon Export and select the suitable data type.

Depending on the destination system you have to choose whether the certificates are to be saved in the standard format (.pem) or in the Personal Information Exchange Syntax (.p12). PKCS#12-Dateien are given a password. For the Mac OSX client export the certificate in the PKCS#12 format.

- After that the certificate can be stored locally.
1.4 L2TP basic settings

Proceed as follows:

- In the main menu select VPN through the selection list VPN L2TP.
- The local L2TP-interface should be a free IP-address from the internal net. The L2TP-IP-addresses (L2TP address-pool) are assigned following the connection to the L2TP-interface.
- With this configuration the L2TP-client can communicate over the proxy-arp function with the internal net, because it is assigned an IP-address from this net upon dial-in.
1.5 L2TP-configuration

Proceed as follows:

- Over VPN select the folder VPN connections.
- Move the existing firewall-object in the left window with the mouse onto the VPN viewport.

Now create a new Roadwarrior-object in the left window.

- Click on the Notebook-Symbol in the image bar of the upper window. In the dialogue window Roadwarrior – hinzufügen (adding Roadwarrior) the Roadwarrior is created without IP (0.0.0.0), because this may vary all the time!
- Click L2TP in the Roadwarrior-dialogue in order to activate L2TP.
Now move the freshly created Roadwarrior-object from the left window onto the VPN viewport.

Now click on the icon Connecting and on the Roadwarrior-object. A flag with the information Please click destination object appears on the Roadwarrior-object.

Now click the firewall-object.
Now, a new dialogue window *IPSec connection accept* appears automatically.

- Select a new the authentication method CERT and the ID-type HOSTNAME in the new window.
- In a default case, all other settings can simply be adopted.

- Under *Lokal Certificate* select the server certificate. For the “Local gateway ID” insert the ID of the server certificate with the sign “@” in front of it.

- If the client-pc works behind a router (natted), the client-subnet has to be inserted as well.
- If the entry is to be valid for all kinds of subnets, one has to insert 0.0.0.0/0.
After clicking the icon Update, the configuration on the appliance has been concluded.

In the following step check the status of the services. SERVICE_IPSEC und SERVICE_L2TP are required for a L2TP-connection. Now upload the certificates created in the section "certificates" into the target systems.
1.6 Setting up users

Proceed as follows:

- Click under User administration on the icon New.
- Set up an L2TP-user with name, login, password etc.

- Optionally, the L2TP-user may be assigned directly an IP-address outside the L2TP-pool.
2 Configuration of the Mac OSX-L2TP-VPN-Roadwarrior under Mac OSX
2.1 Importing the client certificate over the Mac OSX keychain

Proceed as follows:

- Open a terminal window under Mac OSX.
- If you are working with limited user privileges, change to a privileged user by using the command `su <nameoftheadministrator>`.
- Then open the Mac OSX keychain in the way shown in the screenshot. Do not open the keychain under the area Programme!

```
sudo "/Applications/Utilities/Keychain Access.app/Contents/MacOS/Keychain Access"
```

Through the import function, the certificate can be fed into the directory “system” of the key chain. In order to do that, the password of the certificate has to be inserted.

- Once the certificate has been inserted, copy the CA into the directory "X509Anchors".
- You have to re-start the system in order for the certificate to be displayed as valid.
After the re-start, the certificate should be displayed as valid.
2.2 Setting up the VPN-connection

Proceed as follows:

- Set up a new VPN-connection with the program "Internet-Connection". As a server address, insert the name of the host which is also provided in the certificate of the firewall server.

- Open the extended Konfiguration and select “Certificate” as computer-identification and then the relating imported certificate.

- Confirm the entries and test the connection.
How-to: VPN with L2TP and certificates and the Mac OSX VPN-client

Securepoint Version 2007nx

Image: Standard-VPN-connection under Mac OSX, extended settings

Select Certificate

Select your machine authentication certificate:

roadwarrior01

Cancel OK