Astaro Security Linux v5 & NCP Secure Entry Client

A quick configuration guide to setting up NCP’s Secure Entry Client and Astaro Security Linux v5

Document version 2.00
Using NCP Secure Entry Client v8.12 (build 34)
& Astaro Security Linux version 5

Prepared by:
NCP Engineering GmbH
Dombuehler Strasse 2,
90449 Nürnberg, Germany
Phone: +49-911-99.68.0
Fax: +49-911-99.68.299
Disclaimer
Considerable care has been taken in the preparation of this quick guide, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.
NCP makes no representations or warranties with respect to the contents or use of this quick guide, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore, NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.

Copyright
This quick guide is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH, Dombühler Str.2, D-90449 Nürnberg, Germany.

Trademarks
All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© 2004 NCP Engineering GmbH. All rights reserved.
Objective of this document is to show how to setup a VPN connection between a Secure Entry (IPsec) Client and the Astaro Security Linux "ASLv5" as VPN Gateway. For more in depth information please refer to the respective manuals; as this document will only touch on features. Goal is to merely assist in setting up a connection for demonstration purposes.

The configuration (derived from the VPN Consortium’s scenarios) example setup is as follows: A Secure Entry client is installed on a host with a unknown / dynamic IP address, as is often found with remote users requiring access. The ASL firewall is configured with two network interfaces, "External" and "Internal". The external interface has been assigned an IP address of 22.23.24.25, and the internal interface uses 172.23.9.1. The client will establish a connection and gain access to (at least) the internal LAN (172.23.9.1/24) of the ASL firewall.

This document outlines two common setups: the first section connecting with the use of pre-shared keys, and the second section outlines the setup using x509v3 certificates (PKIX).

Section 1: Configuring a VPN connection using pre-shared keys

1.1: Configuring the Astaro Security Linux v5 with pre-shared keys
   1.1.1: IPSec VPN -> Remote Keys
   1.1.2: IPSec VPN -> Policies
   1.1.3: IPSec VPN -> Connections

1.2: Configuring the NCP Secure Entry Client with pre-shared keys.
   1.2.1: Configuration Assistant: Creating a new profile
   1.2.2: Configuration: Checking/Modifying the profile

1.3: Establishing the connection with pre-shared keys

Section 2: Configuring a VPN connection using certificates (PKI)

2.1: Configuring the Astaro Security Linux v5 with certificates (PKI)
   2.1.1: IPSec VPN -> CA Management
   2.1.2: IPSec VPN -> Remote Keys
   2.1.3: IPSec VPN -> Local Keys
   2.1.4: IPSec VPN -> Policies
   2.1.5: IPSec VPN -> Connections

2.2: Configuring the NCP Secure Entry Client with certificates (PKI)
   2.2.1: Configuration Assistant: Creating a new profile
   2.2.2: Configuration: Checking/Modifying the profile
   2.2.3: Configuration: Using certificates

2.3: Establishing the connection with certificates
1. Configuring a VPN connection using pre-shared keys.

1.1 Configuring the Astaro Security Linux v5 with pre-shared keys.

The following section will describe the steps needed to define a VPN link on the ASLv5. Please refer to the documentation for an excellent description and for more details.

1.1.1 IPSec VPN -> Remote Keys

First a pre-shared key must be defined. This Remote IPSec Key can be given a name; as shown below, in this example it’s named VPN-PSK-User01. Additionally, an IP Address that the connection host will be assigned can be defined.

Select PSK (Pre-Shared Key) as Key Type, and enter in a secret that is going to be shared between the connecting host and this machine.

Click Add to activate and make this remote key available.

Confirm the Remote Key is available to use when defining a connection.
1.1.2 IPSec VPN -> Policies

Next step is to define the policies that will be applied to the incoming IPsec connections. This too is given a name: **NCP-demo Policy**. The configuration below is but an example, one is free to choose other combinations as is best suited for the scenario where this is to be applied.

![New IPSec Policy](image)

**NOTE:** IPCOMP (Compression) may also be enabled, as the NCP client supports both ZLIB [DEFLATE], and LZS [STAC].

Remember to click on **Add** to add this to the list of available proposals.
1.1.3 IPSec VPN -> Connections

The screenshot above shows how to configure an incoming IPsec connection. Note that the policy defined in the previous section is selected and applicable to this incoming connection. Furthermore, the VPN-PSK-User01 remote key is the valid key for the incoming requests. For more in depth details please refer to the Astaro help pages.

Finally, remember to enable this connection!
1.2. Configuring the NCP Secure Entry Client with pre-shared keys.

1.2.1 Configuration Assistant: Creating a new profile

The first time you start up the NCP Entry Client you will be prompted to create a profile. You can either use the assistant or modify an existing profile as shown in section 1.2.2.

Select **Link to Corporate Network using IPSec** to create a profile with the parameters needed to establish a connection to the Astaro Security Linux box.

Click **Next >**.

Several profiles can be created and each given different name. In this example, this profile is created and given the name **VPN using PSK**.
Click **Next >**.

**Figure 1.2.3: Configuration Assistant: Link type (Dial up configuration)**

The NCP Secure Entry Client supports different media types; the integrated dialer for example, can be used to establish a connection to the ISP with a modem (if available to the system) prior to building the VPN Tunnel. In this example, select **LAN (over IP)** and then click **Next >**.

**Figure 1.2.4: Configuration Assistant: VPN gateway parameters**

Enter the ASLv5's public IP address or DNS name. The client can first resolve names to IP addresses if these are used.

Click **Next >**.
This example will use **Main Mode** and **Perfect Forward Secrecy** seamless re-keying, employing **DH-Group2 (1024 Bit)**. Enable the **Use IP compression**, and the compression will automatically be negotiated.

Click **Next >**.

In this example, a pre-shared key or shared secret is used, identical passwords on the IPSec communicating peers.

The **Next >** button will not be available until the **Shared Secrets** have been entered in, confirmed and match.
The ASLv5 is configured to assign a **Virtual IP Address** to the incoming connection (see figure 1.1.1). (The NCP Secure Entry client supports three options, manual IP address assignment, IKE-Config Mode, or using the IP address assigned to the physical network interface). Optionally enter in the addresses where the (internal/external) DNS and WINS servers can be found.

Click **Next** to continue.

The NCP Secure Entry Client also comes with a (stateful inspection) personal firewall that can be enabled to provide protection against attacks from the local LAN (for example an environment at a public wlan hotspot). For additional configurable parameters see also **Configuration -> Extended Firewall Settings**.

Click **Finish** to save the setting to this profile.
1.2.2 Configuration: Checking/Modifying the profile

Open the **Profile Settings** to review/modify the connection parameters.

*Figure 1.2.9: Configuration -> Profile Settings*

Either double click on the profile that is going to be modified, or select the profile and then click on **Configure**.

*Figure 1.2.10: Profile Settings*
Figure 1.2.11: Profile Settings: Basic Settings

Review the parameters and ensure they are correct.

Select **Line Management** to continue…

Figure 1.2.12: Profile Settings: Line Management

The **Connection Mode** can be set to connect automatically, meaning that any time a packet is destined for ASLv5’s internal LAN, the VPN Tunnel can automatically be established. In this example however, one manually establishes the connection. The **Inactivity Timeout** is set to 100 seconds.

Select **IPSec General Settings** to continue…
Verify the IP address or DNS name of the ASLv5 is correctly configured.

When **automatic mode** is selected for both the **IKE** (Phase 1) and **IPSec** (Phase 2) **Policies**, the client will submit a range of different commonly used proposals and the ASLv5 can then select the one that matches the policy defined in section 1.1.2 and assigned to the connection in section 1.1.3. The selected settings as shown in section 1.1.2 will work automatically, thereby not necessitating the definition of custom proposals.

Click on **Identities** to move to the next dialog box.

Confirm that the **pre-shared key** has been filled in correctly.

Click on **IP Address Assignment** to continue...
Confirm the settings as entered in figure 1.1.1 (**Virtual IP = Manual IP address**). Then click on **Remote Networks** to move to the next dialog box.

Enter in the **Network address(es)** (depending on the subnet masks defined, these can be individual hosts or network segments) that are to be reached. This is used in the Phase 2 negotiation and often the cause for configuration mistakes.

In this scenario, the ASL is set to **ANY** (see **subnet definition** figure 1.1.4) so no subnets need to be defined here. If you choose however, to set subnets in the configuration as shown in figure 1.1.4, then these need to match the values entered here.

Skip **Certificate Check**, because this example does not call for the use of certificates, select the **Firewall Settings** instead...
Figure 1.2.17: Profile Settings: Firewall Settings

Confirm the settings here as entered in figure 1.2.8. For more details also refer to the manual, and look at the Configuration -> Extended Firewall Settings.

Click on OK to return to the main Profile Settings dialog box.

Figure 1.2.18: Profile Settings

Select OK to return to the monitor (the graphical user interface to configure the VPN Client)
1.3 Establishing the connection with pre-shared keys

Seeing as the connection is set to be established manually, click on **Connect** to create the tunnel.

Then open a dos box/command prompt, and ping the internal network interface of the ASLv5 to confirm the connection has been successfully established. Depending on the VPN Gateway's configuration other hosts on the ASLv5 internal LAN can be reached. (See ASLv5's filtering and routing settings; this is beyond the scope of this quick installation guide).
2. Configuring a VPN connection using certificates (PKI)

2.1 Configuring the Astaro Security Linux v5 with certificates (PKI)

2.1.1 IPSec VPN -> CA Management
First step is to create a Certification Authority and generate the certificates needed.

![Figure 2.1.1: IPSec VPN -> CA Management]

In order to create certificates, a CA or Certification Authority needs to be created that in turn can issue certificates.

This is done by creating a "Signing CA", a self signed certificate: This will be the root CA certificate. Once this certificate is created; all other subsequent certificates can be generated using the key-pair belonging to this certificate.

Click on New… and then Generate and enter in the values for the Certification Authority.

![Figure 2.1.2: IPSec VPN -> CA Management: Creating a Certification Authority]

The self-signed root CA certificate will be referred to as ASLv5-DemoCA.

Next, two "Host CSR"s (Certificate Signing Requests) are to be created, and these then signed to create two host certificates.

![Figure 2.1.3: IPSec VPN -> CA Management: Host CSRs and Certificates]

We will create one certificate for the VPN Gateway itself "VPN-GW01" (the certificate the VPN Gateway will present to the user) and a certificate for a user "VPN-User01" (the certificate the user will present to the VPN Gateway). Click New…

**IMPORTANT NOTE:** please select X509 DN as the VPN ID as shown below!
Figure 2.1.4: IPSec VPN -> CA Management: Defining a Certificate Signing Request (CSR) for gateway

The above screenshot shows the creation of a CSR for a certificate that will be used for the VPN Gateway to present to incoming requests.

Figure 2.1.5: IPSec VPN -> CA Management: CSR for gateway awaiting to be signed

Next create a CSR for a VPN user, click New...
These CSR then can be signed to create certificates.

Select the CSR, and then select **Issue CERT from CSR**, enter the signing CA’s password, and proceed to sign them, and thereby creating usable certificates.
Repeat this process to create a certificate for the **VPN-User01**. Once completed, you will have two certificates:

**Figure 2.1.10: IPSec VPN -> CA Management: Issued certificates overview**

Next step is to transfer the **VPN-User01** and the rootCA **ASLv5-DemoCA** certificates to the host where the client software is installed on. Simply select the certificate and download. (see also section 2.2.3)

**Figure 2.1.11: IPSec VPN -> CA Management: Downloading the rootCA certificate**

In the case of the CA certificate; you will get a zipped file containing two files: **CERT_ASLv5-DemoCA.pem** and **KEY_ASLv5-DemoCA.pem**. We will only require the use of the **CERT_ASLv5-DemoCA.pem**, so **KEY_ASLv5-DemoCA.pem** can (and should!) be deleted immediately. It is not good practice to keep this file on the client machine. Place this certificate in (for example windows 2000 systems) **c:\WINNT\ncple\CaCerts\** directory (see figure 2.2.22)

**Figure 2.1.12: IPSec VPN -> CA Management: Downloading the certificate for the user**

Also select the **CERT+KEY** bearing the name **VPN-User01** and download this as P12 (PKCS#12) which then also contains the private-key used for the signing operations. A password is requested which will be used to open the container (P1CS#12 file) in which the private-key is stored.
2.1.2 IPSec VPN -> Remote Keys

Define authentication parameters of your IPsec peer. In this example we will use the x509(v3) certificate we generated to authenticate the VPN client with to the VPN Gateway.

![New Remote IPSec Key](image)

Click **Add** to activate and make this remote key available.

![CA Management Remote Keys](image)

Confirm the Remote Key is available to use when defining a connection.

2.1.3 IPSec VPN -> Local Keys

Next the VPN Gateway needs to be given a certificate: we'll use the VPN-GW01 we created earlier.

![Local IPSec X.509 Key](image)

Provided the password is correctly entered, the ASLv5 will now load the certificate and reflect this by showing the CN we assigned it.

![Local IPSec X.509 Key](image)

This is then the certificate that the ASLv5 will use to present to incoming VPN connection requests and authenticate itself to the client.

2.1.4 IPSec VPN -> Policies

Although one is free to choose from a whole host of combinations; the screenshot below simply illustrate one combination. (It is however advisable to select AES instead of 3DES because of a dramatic performance increase. AES was designed with performance in mind, and therefore is faster than 3DES.)
**Figure 2.1.17: IPSec VPN -> Policies: New IPSec Policy**
2.1.5 IPSec VPN -> Connections

Now we bring all the components together and define a VPN connection.

![New IPSec Connection](image1.png)

**Figure 2.1.18: IPSec VPN -> Connections: New IPSec Connection**

![IPSec Connections](image2.png)

**Figure 2.1.19: IPSec VPN -> Connections: IPSec Connections**

Be sure to enable the profile, and then proceed with configuring the NCP Secure Entry Client.
2.2. Configuring the NCP Secure Entry Client with certificates (PKI)

In this scenario, the client requires two certificates: one of the CA that issued the certificates, known in this example as the ASLv5-DemoCA filename: CERT_ASLv5-DemoCA.pem, and a client certificate referred to as VPN-User01.p12 (see figure 2.1.6 & 2.1.12). Copy the CERT_ASLv5-DemoCA.pem file into the CaCerts subdirectory within the ncple directory. Any CA certificates placed here can be then set to be trusted; please refer to the manual for more details.

2.2.1 Configuration Assistant: Creating a new profile

![Configuration Assistant: Connection Type](image1)

Select **Link to Corporate Network using IPSec** to create a profile with the parameters needed to establish a connection to the ASLv5 VPN Gateway.

Click **Next >**.

![Configuration Assistant: Connection Name](image2)

Select **ASLv5-VPN-01** as the name of the connection.
Several profiles can be created and each given different name. In this example, this profile is created and given the name **ASLv5VPN-GW01**.

Click **Next >**.

![Figure 2.2.3: Configuration Assistant: Link type (Dial up configuration)](image)

The NCP Secure Entry Client supports different media types; the integrated dialer for example, can be used to establish a connection to the ISP with a modem (if available to the system) prior to building the VPN Tunnel. In this example, select **LAN (over IP)**.

Click **Next >**.

![Figure 2.2.4: Configuration Assistant: VPN gateway parameters](image)

Enter in the gateway’s IP address or DNS name. (XAUTH as defined in draft-beaulieu-ike-xauth-02 is not supported by the ASLv5.)

Click **Next >**.
This example will use **Main Mode** and **Perfect Forward Secrecy** for seamless re-keying, employing **DH-Group2 (1024 Bit)**. Enable the **Use IP compression** to increase the throughput.

Click **Next >**.

In this scenario, a certificate is used. The **ASN1 Distinguished Name** is used from the certificate.
The ASLv5 VPN Gateway is configured to designate a virtual IP address to the incoming VPN connection (see figure 2.1.13). The NCP Secure Entry client supports three options, manual IP address assignment, IKE-Config Mode, or using the IP address assigned to the physical network interface. In this example, the IP address and the appropriate subnet mask is manually assigned to the client as illustrated in the screenshot above.

Click Next > to continue.

The NCP Secure Entry Client also comes with a (stateful inspection) personal firewall that can be enabled to provide protection against attacks from the local LAN (for example an environment at a public wlan hotspot).

Click Finish to save the setting to this profile.
2.2.2 Configuration: Checking/Modifying the profile

Open the Profile Settings to modify/review the parameters.

Either double click on the profile that is going to be modified, or select the profile and then click on Configure.
Review the parameters and ensure they are correct. Select **Line Management** to continue...

![Figure 2.2.12: Profile Settings: Line Management](image)

The **Connection Mode** can be set to connect automatically, meaning that any time a packet is destined for ASLv5's LAN, the VPN Tunnel can automatically be established. In this example however, one manually establishes the connection. The **Inactivity Timeout** is set to 360 seconds.

Select **IPSec General Settings** to continue...

![Figure 2.2.13: Profile Settings: IPSec General Settings](image)

When **automatic mode** is selected for both the **IKE** (Phase 1) and **IPSec** (Phase 2) **Policies**, the client will submit a range of different commonly used proposals and the ASLv5 can then select the one that matches the policy defined in section 2.1.4 and assigned to the connection in section 2.1.18. The selected settings as shown in section 1.1.2 will work automatically, thereby not necessitating the definition of custom proposals.

Click on **Identities** to move to the next dialog box.
In this scenario, the IKE-ID type is taken from the certificate, in the form of the **ASN1 Distinguished Name**. Other IKE-ID types can be used, but are beyond the scope of this document; please refer to the manual for more details.

Click on **IP Address Assignment** to continue

Confirm the settings as entered in figure 2.1.13.

Then click on **Remote Networks** to move to the next dialog box.
Enter in the **Network address(es)** (depending on the subnet masks defined, these can be individual hosts or network segments) that are to be reached. This is used in the Phase 2 negotiation and often the cause for configuration mistakes.

By not specifying any networks/hosts here, all traffic will be pushed through the tunnel. If you do not wish this to be the case, you can specify networks and the appropriate net- or hostmasks.

In this scenario, the ASLv5 gateway is set to **ANY** (see **subnet definition** figure 2.1.18) so no subnets need to be defined here. If you choose however, to set subnets in the configuration, then these need to match the values entered here.

Additional security can be applied by entering the appropriate values here that will then be compared to the values in the certificate presented by the VPN gateway. In other words, additional checks are done on the certificate that the ASLv5 presents when establishing a connection. See the manual for more details.
Figure 2.2.18: Profile Settings: Firewall Settings

Confirm the settings here.

Click on OK to return to the main Profile Settings dialog box and select OK to return to the monitor (the graphical user interface of the VPN Client)
2.2.3 Configuration: Using certificates

Finally, point the client to the certificates that are to be used. These can be downloaded using the browser or simply copied to the appropriate locations. In this example the rootCA ASLv5-DemoCA certificate is placed in c:\WINNT\ncple\CaCerts. (see figure 2.1.11)

![Connection -> Certificates -> Display CA certificates](image)

To verify that this has been done correctly; check to see if the CA certificate is listed in Connection -> Certificates | Display CA Certificates.

![Certificates -> Trusted CA certificates](image)

The green tick denotes that this Certification Authority is to be trusted.

Next define where the client can find the user certificate VPN-User01.p12.

In the same way, place the certificate to be used to authenticate the client in a directory where it can easily be found. For the sake of this example, soft certificates are used. These are encrypted files containing the user's private- and public-keys. These keys could optionally, to obtain a higher security level be generated and stored exclusively on external devices such as smart cards or USB cryptographic devices. These then can be accessed using the PKCS#11 interface that comes with the Secure Client.
Figure 2.2.21: Configuration -> Certificates

To define which and where the certificate that is to be used; one needs to configure the location of the (soft)certificate to be used. **Configuration -> Certificates** brings up the following dialog box:

Figure 2.2.22: Configuration -> Defining user certificate

Select from PKCS#12 File, to set the use of 'soft certificates'. Then the appropriate path and file name are to be filled in where the certificate is located.

Figure 2.2.23: Connection -> Enter PIN (to open user certificate)
To verify that this has been done correctly; check to see if the user certificate is listed in **Connection -> Enter PIN**.

![Enter PIN](image)

*Figure 2.2.24: Connection -> Enter PIN (to open user certificate)*

Enter the **PIN**, and if it is correct; this is indicated by a little green tick in the corner of the Monitor; then then allows you to view the client certificate.

![NCP Secure Entry Client Monitor](image)

*Figure 2.2.25: NCP Secure Entry Client Monitor: Confirm correct PIN*

**Connection -> Certificates | View Client Certificate.**

![Connection -> Certificates -> View Client Certificate](image)

*Figure 2.2.26: Connection -> Certificates -> View Client Certificate*
Figure 2.2.27: Connection -> Certificates -> View Client Certificate

If there is any problem this will be highlighted in red. The example above shows a client certificate generated by the ASLv5_DemoCA used in this example.
2.3. Establishing the connection with certificates

Figure 2.3.1: NCP Secure Entry Client Monitor: Established connection

When this has been completed a connection can be established. Seeing as the connection is set to be established manually, click on Connect to create the tunnel. If the certificate has not been accessed yet, you will be prompted to enter in the PIN to open and use the certificate.

Figure 2.3.2: Command Prompt: Ping response