# Operational User Guidance (AGD_OPE)

# for LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN

Version 1.10

**Release**

LANCOM Systems GmbH

Adenauer Str. 20/B2
52146 Würselen
Germany

Document History

| Date | Version | Editor | Change |
|---|---|---|---|
| 19.12.2011 | 0.1 | SKörber | Document creation |
| 10.02.2012 | 1.0 | SKörber | First Release |
| 21.03.2012 | 1.1 | SKörber | Feedback by SRC |
| 04.06.2012 | 1.2 | SKörber | Feedback by SRC and LANCOM |
| 14.06.2012 | 1.3 | SKörber | Feedback by SRC and LANCOM |
| 26.07.2012 | 1.4 | SKörber | Secure usage updated |
| 20.11.2012 | 1.5 | SKörber | Feedback by SRC and LANCOM |
| 08.02.2013 | 1.6 | SKörber | Feedback by LANCOM and SRC |
| 19.03.2013 | 1.7 | SKörber / TJansen | Feedback by SRC |
| 03.04.2013 | 1.8 | SKörber | Feedback by BSI |
| 10.04.2013 | 1.9 | TJansen | Feedback by SRC |
| 17.04.2013 | 1.10 | TJansen | Feedback by SRC |

# Table of Contents

1. General Description ..... 4
1.1. Identification and Characterization of User Roles ..... 4
1.2. Modes of Operations ..... 4
1.3. Setting up a Secure Operational Environment ..... 4
1.4. Further Documentation ..... 4
2. User Role Specific Description ..... 5
2.1. Description of Security Functions ..... 5
2.2. Description of Privileges ..... 5
2.3. Warnings ..... 5
2.4. Description of Interfaces ..... 5
2.5. Method of Invocation ..... 5
2.5.1. Starting a Serial Connection ..... 6
2.5.2. Starting a SSHv2 Connection ..... 6
2.5.3. General Information Concerning the Terminal Commands ..... 6
2.5.4. Structure of the Command-Line Interface ..... 7
2.5.5. Command Description ..... 7
2.6. Specification of Interfaces ..... 10
2.6.1. Firmware Update ..... 10
2.6.2. WAN connection (IP over Ethernet) ..... 10
2.6.3. WAN connection (PPP over Ethernet) ..... 12
2.6.4. WAN connection (PPP over Ethernet over ATM) ..... 14
2.6.5. WAN connection (ADSL) ..... 15
2.6.6. WAN connection (UMTS/LTE) ..... 16
2.6.7. Configuring the Firewall ..... 19
2.6.8. VPN Site-to-Site Connection (Preshared Key) ..... 19
2.6.9. Requirements for the Use of VPN Certificates ..... 24
2.6.10. VPN Site-to-Site Connection (Self-Signed Certificates) ..... 26
2.6.11. VPN Site-to-Host Connection (Self-Signed Certificates) ..... 31
2.6.12. Applying Firewall Rules ..... 37
2.6.13. Using the Port-Forwarding ..... 38
2.7. Events ..... 40
2.8. Recommendation for Secure Usage of the TOE ..... 40
2.8.1. Decommissioning the TOE ..... 41
2.8.2. Secure Key Destruction ..... 41
2.8.3. Required Configuration Settings ..... 42
2.8.4. Regular Maintenance Tasks ..... 59

# 1. General Description

This document describes the requirements to operate the TOE in a secure manner.

## 1.1. Identification and Characterization of User Roles

The LANCOM LCOS has only one valid user: “root”. Therefore, the identification and characterization of user roles is not applicable to the TOE.

## 1.2. Modes of Operations

Not applicable since the TOE has only one mode of operation.

## 1.3. Setting up a Secure Operational Environment

The TOE must be installed on the hardware as described in the preparative procedures.

The administrator must issue a policy that defines if a network connected to the TOE is trusted or untrusted, which packet flows are to be protected and which VPN peer will encrypt / decrypt which packet flow. The administrator must ensure that the VPN peer is also configured according to this policy.

The administrator must initiate remote configuration with SSHv2 while using a trusted network. The administrator must be trained in a secure operation of the TOE as defined in this document. If preshared keys are used to establish a VPN connection, they must be shared between the administrator of the TOE and the administrator of the VPN peer in a secure way avoiding disclosure to third parties. They must also be securely generated (64 characters containing alphabetic, numeric and special characters). Secure ways to exchange keys are either face to face in a secure environment or via encrypted e-mails.

The serial configuration port must only be used to configure the TOE. Every other usage is out of the scope of the evaluated configuration.

## 1.4. Further Documentation

Beside this user guidance, there are two other manuals available, the reference manual and the menu-reference. Both documents can be downloaded from the address below. There may be some linked references to these documents within this guidance.

- Reference Manual 8.00 (LCOS-REFMANUAL-800-EN.pdf)

  ftp://ftp.lancom.de/Documentation/Reference-Manual/
- Menu-Reference (LCOS-MENU-860-EN.pdf)

  ftp://ftp.lancom.de/Documentation/LCOS-Menu/

# 2. User Role Specific Description

## 2.1. Description of Security Functions

Since the LCOS supports only one user role, the following sections will be specific to the administrator (i.e. root). The security functions described in this section are the configuration of the TOE, logging and administration via SSHv2 and serial command-line.

The other security functions provided by the TOE such as IPsec and packet filtering are not assigned to any specific user role.

## 2.2. Description of Privileges

Not applicable since the administrator of the TOE is not restricted.

## 2.3. Warnings

The TOE has the ability to perform traces. Traces monitor internal processes and can be used to display individual steps of several protocols. Experienced users may interpret these outputs to trace errors occurring in the establishment of a connection (e.g. PPP). A particular advantage of this is:

- The errors being tracked may occur from an error in configuration of your own router or that of the remote site.

Note that the trace outputs are slightly delayed after the actual event, but are always in the correct sequence. This will usually not interfere with the interpretation of the trace output but must be taken into consideration if performing a precise analysis. It must also be considered, that some information may be submitted in plain text.

- More information regarding available trace options are defined in LCOS-REFMANUAL-800-EN.pdf (Part 5.1 - Trace information—for advanced users)

## 2.4. Description of Interfaces

The TOE is configured only via a command-line interface.

## 2.5. Method of Invocation

The LCOS configuration has two different ways of invocation in the evaluated configuration: The serial port and the SSHv2 (Secure Socket Shell Version 2) connection. In both cases, a command-line will be opened. The administration of the LCOS and its features is done with the command-line. Certificates are uploaded via SSHv2/SCP (see 2.6 – Firmware update). When logging in via SSHv2, please note that you must login as "root".

### 2.5.1. Starting a Serial Connection

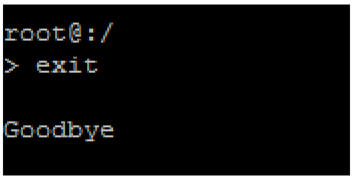
Please connect the serial connector cable to the config-port on the backside. Then start your preferred terminal emulator (e.g. PuTTY / TerraTerm) with the following parameters:

| | |
|---|---|
| Interface: | COMx |
| Speed | 115200 |
| Data bits | 8 |
| Stop bits | 1 |
| Parity bits | none |
| Flow control | RTS/CTS |

### 2.5.2. Starting a SSHv2 Connection

Use your preferred SSHv2 client (e.g. PuTTY or any other management program supporting SSHv2) and type in the IP-address and password given during the initial configuration. To close the SSHv2 session, just enter the command exit:

- “exit”



```
root@:/
> exit

Goodbye
```

When connecting to the LANCOM make sure that it has not the LANCOM default fingerprint: “03:56:e6:52:ee:d2:da:f0:73:b5:df:3d:09:08:54:b7”. Otherwise upload a new and unique SSH-Hostkey as mentioned in “AGD_PRE 1.2.3 Initial configuration”. Make also sure to delete the corresponding entry in your known_hosts file (e.g. ~/.ssh/known_hosts).

The administrator must make sure that no more than 10 MiB of data are transferred within any single SSH session. The administrator must also use a unique SSH session for each file exchange and close SSH sessions when they are no longer used.

### 2.5.3. General Information Concerning the Terminal Commands

- PATH:
  - Path name for a menu or parameter, separated by / or \
  - .. means one level higher
  - . means the current level
- VALUE:
  - Possible input value
  - “” is a blank input value
- NAME:
  - Sequence of characters (made up of _ 0..9 A..Z)
  - First character cannot be a digit
  - Case insensitive

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, command ”sysinfo” can be shortened to ”sys”. Input ”cd /s” is not valid, however, since it corresponds to both ”cd /Setup” and ”cd /Status”.

- Names that contain spaces must be enclosed within quotation marks (““).
- A command-specific help function is available for actions and commands (call the function with a question mark as the parameter). For example, 'ping ?’ shows the options of the integrated ping command.
- Enter ‘help’ or ‘?’ on the command line for a listing of the console commands available.

## 2.5.4. Structure of the Command-Line Interface

The LANCOM command-line interface is always structured on root level in the following way:

- Status Contains the status and statistics of all internal modules in the device
- Setup Contains all adjustable parameters of all internal modules in the device
- Firmware Contains the firmware management
- Other Contains actions for establishing and terminating connections, reset, reboot and upload.

The LANCOM command-line interface can be operated with the following UNIX-style commands. The LCOS menu commands that are available to you can be displayed at any time by entering “help” or “?” at the command line.

## 2.5.5. Command Description

- beginscript Resets the console session to script mode. In this state, entered commands are not transferred directly to the TOEs configuration RAM but initially to the device's script memory.
- cd [PATH] Switches to the specified path. Various abbreviations can be used, such as replacing " cd ../.." with "cd ...", etc.
- del [PATH]* Deletes the table in the branch of the menu tree defined by PATH.
- default [-r] [PATH] Resets individual parameters, tables or entire menu trees back to their default configuration.
- PATH indicates a branch of the menu tree, then the option - r (recursive) must be entered.
- dir [PATH], list [PATH],
  ls [PATH], ll [PATH] Displays the current directory content.

  The suffix parameter "- a" lists the SNMP IDs associated with the content of the query. This starts the output of the SNMP ID from the device, followed by the SNMP ID of the current menu. Before each entry you will see the SNMP IDs of the sub-points.
- do [PATH] [<Parameter>] Executes the action [PATH] in the current directory. Other parameters can be entered in addition.
- echo <ARG>... Display argument on console
- exit/quit/x Ends the command line session

| | |
|---|---|
| feature <code> | Activation of a software feature with the feature code as entered |
| flash Yes/No | Changes to the configuration using commands in the command line are written directly to the boot-resistant Flash memory of the devices as standard (flash yes). If updating the configuration is suppressed in Flash (flash no), changes are only stored in RAM (deleted on booting). |
| history | Displays a list of recently executed commands. Command "!#” can be used to directly call the list commands using their number (#): For example, "!3” runs the third list command. |
| killscript | Deletes the script session contents yet to be processed. The script session is selected by its name. |
| loadconfig | Load configuration into device via TFTP client |
| loadfirmware | Load firmware into device via TFTP client |
| loadscript | Load script into device via TFTP client |
| passwd | Change password (please see AGD_PRE – 1.2.2 part “Initial configuration” for password requirements) |
| passwd -n new [old] | Change password (no prompt) (please see AGD_PRE – 1.2.2 part “Initial configuration” for password requirements) |
| ping [IP address or name] | Sends an ICMP echo request to the IP address specified |
| readconfig | Display of the entire configuration in the device syntax |
| readmib | Display of the SNMP Management Information Base |
| readscript [-n] [-d] [-c] [-m] [PATH] | In a console session, the readscript command generates a text dump of all commands and parame-ters required to configure the LANCOM in its current state. |
| repeat <INTERVAL> <Command> | Repeats the command every INTERVAL seconds until the process is ended with new input |
| sleep [- u] value[suffix] | Delays the processing of configuration commands by a particular time or terminates them at a particular time. Permissible suffixes are s, m and h for seconds, minutes and hours. If no suffix is defined, the command uses milliseconds. With option switch -u, the sleep command accepts times in format MM/DD/YYYY hh:mm:ss (English) or in format TT.MM.JJJJ hh:mm:ss (German). Times will only be accepted if the system time has been set. |
| stop | Ends the PING command |
| set [PATH] <value(s)> | Sets a configuration parameter to a particular value.<br>If the configuration parameter is a table value, a value must be specified for each column. Entering |

| | |
|---|---|
| | the * character leaves any existing table entry unchanged. |
| set [PATH] ? | Listing of the possible input values for a configuration parameter. If no name is specified, the possible input values for all configuration parameters in the current directory are specified. |
| setenv <NAME> <VALUE> | Set environment variable |
| unsetenv <NAME> | Delete environment variable |
| getenv <NAME> | Display environment variable (no line feed) |
| printenv | Display the entire environment |
| show <Options> | Display of special internal data. |
| show ? | Displays all available information, such as most recent boot processes (bootlog), fire-wall filter rules (filter), VPN rules (VPN) and memory usage (mem and heap) |
| sysinfo | Displays system information (e.g. hardware/software version) |
| testmail | Sends an e-mail. See 'testmail ?' for parameters |
| time <invalidate> | Set time (MM/DD/YYYY hh:mm:ss or DD.MM.YYYY hh:mm:ss) or time invalidate (requires a cold boot – do /other/cold-boot/ - to get activated) |
| trace | Configuration of the diagnostics display. |
| who | List active sessions |
| writeconfig | Load a new configuration file in the device syntax. All subsequent lines are interpreted as configuration values until two blank lines occur |
| writeflash | Load a new firmware file (only via TFTP) |
| !! | Repeat last command |
| !<num> | Repeat command <num> times |
| !<prefix> | Repeat last command beginning with <prefix> |
| #<blank> | Comment |

Directories can be addressed with the corresponding SNMP ID. For example, the command “cd /2/8/10/2” has the same effect as “cd /Setup/IP-router/Firewall/Rules".

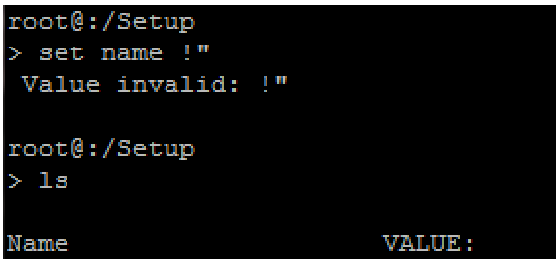
Multiple values in a table row can be changed with one command, for example in the rules table of the firewall:

| | |
|---|---|
| set WINS UDP | sets the protocol of the WINS rule to UDP |
| set WINS UDP ANYHOST | sets the protocol of the WINS rule to UDP and the destination to ANYHOST |
| set WINS * ANYHOST | also sets the destination of the WINS rule to ANYHOST; the asterisk means that the protocol remains unchanged |

The values in a table row can alternatively be addressed via the column name or the position number in curly brackets. The command “set ?” in the table shows the name, the possible input values and the position number for each column. For example, in the rules table of the firewall, the destination has the number 4:

| | |
|---|---|
| set WINS {4} ANYHOST | sets the destination of the WINS rule to ANYHOST |
| set WINS {destination} ANYHOST | also sets the destination of the WINS rule to ANYHOST |
| set WINS {dest} ANYHOST | sets the destination of the WINS rule to ANYHOST, because specifying "dest" here is sufficient to uniquely identify the column name. |

Please note that if you run a set command with invalid values, you will get a syntax error. In this case, no change will be made to the entry or table.



```
root@:/Setup
> set name !"
 Value invalid: !"

root@:/Setup
> ls

Name                        VALUE:
```

For more information regarding the command line interface, check LCOS-MENU-860-EN.pdf (P.1.3 - Command-line commands)

## 2.6. Specification of Interfaces

The following text describes how to run a firmware update and how to set up a WAN IPoE, WAN PPPoE, WAN PPPoEoA, UMTS/LTE, VPN site-to-site and VPN site-to-host connection (Preshared Key & PKI). It also describes how to apply a firewall rule and how to use the port-forwarding.

### 2.6.1. Firmware Update

Before you start with the firmware update you must make sure, that the firmware you are willing to install is genuine. The final certification report will contain a SHA256 hash of the firmware file. The user has to build a SHA256 hash of the downloaded file to compare it to the hash mentioned in the certification report. This way, the user can make sure, that the file is genuine.

If necessary, you can start a firmware update via SCP (SSHv2). To do this, you must use a secure copy client (e.g. Cygwin SCP or any other management program supporting SCP). The command to upload the firmware file would be:

- scp firmware.upx root@10.10.10.1:firmware

If you are about to install a non CC compliant firmware, please note the “Firmware-check” value in /Setup/Config/. You have to set the value from “only certified” to “any” to be able to install non CC compliant firmwares.

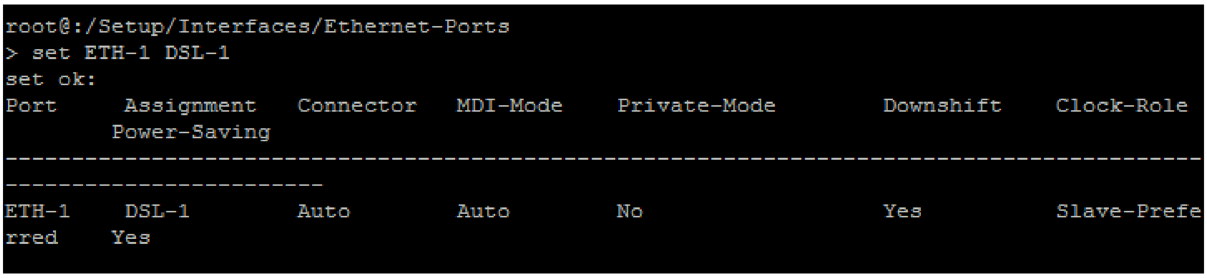
Note that by installing a non CC compliant firmware you will leave the evaluated configuration.

### 2.6.2. WAN connection (IP over Ethernet)

To create an IP over Ethernet WAN connection, you must start with the configuration of the Ethernet-Ports. This must be done in: /Setup/Interfaces/Ethernet-Ports. In this example, the WAN uplink cable was put into Ethernet-Port 1. The first step is to assign the logical interface DSL-1 to the physical interface ETH-1.

The assignment can be set by typing the following command:

- “set ETH-1 DSL-1”

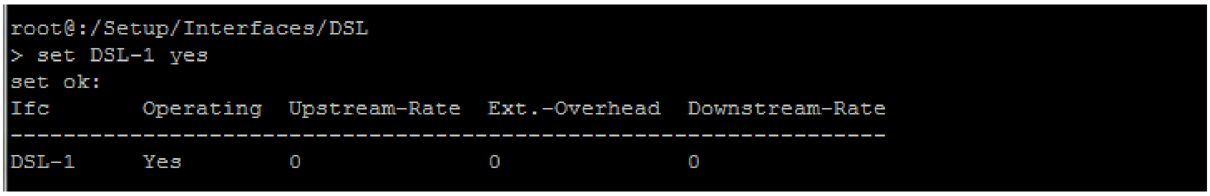


```
root@:/Setup/Interfaces/Ethernet-Ports
> set ETH-1 DSL-1
set ok:
Port     Assignment   Connector   MDI-Mode    Private-Mode        Downshift    Clock-Role
        Power-Saving
-------------------------------------------------------------------------------------------
------------------------
ETH-1    DSL-1        Auto        Auto        No                  Yes          Slave-Prefe
rred    Yes
```

The next step is to activate the logical interface DSL-1. This must be done in: /Setup/Interfaces/DSL

The appropriate command:

- “set DSL-1 yes”

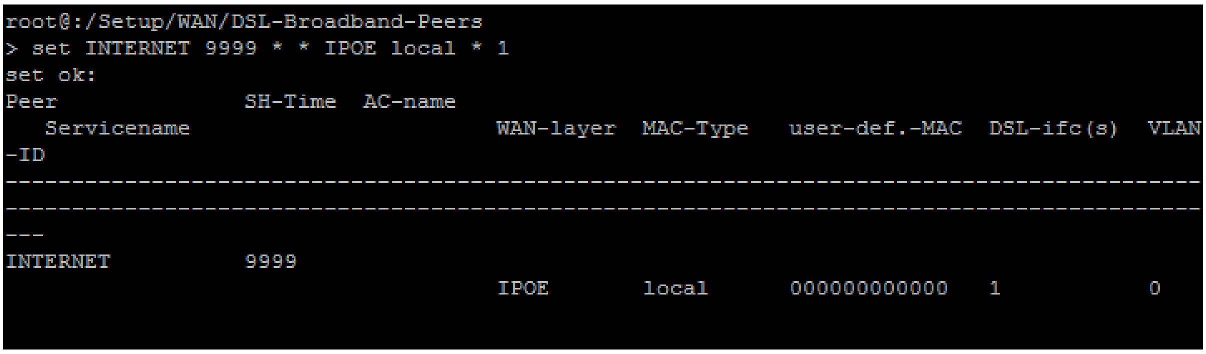


```
root@:/Setup/Interfaces/DSL
> set DSL-1 yes
set ok:
Ifc       Operating  Upstream-Rate  Ext.-Overhead  Downstream-Rate
------------------------------------------------------------------
DSL-1     Yes        0              0              0
```

Now it´s time to configure a DSL-Broadband-Peer. This must be done in: /Setup/WAN/DSL-Broadband-Peers. Here it is necessary to give the peer a name, set a short-hold time, assign an appropriate WAN-Layer and DSL-Interface.

A possible command might be:

- “set INTERNET 9999 * * IPOE local * 1”

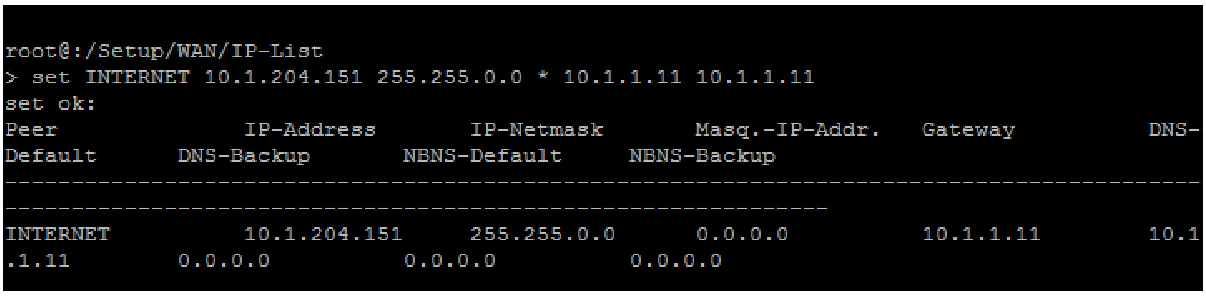


```
root@:/Setup/WAN/DSL-Broadband-Peers
> set INTERNET 9999 * * IPOE local * 1
set ok:
Peer              SH-Time  AC-name
   Servicename                       WAN-layer  MAC-Type   user-def.-MAC  DSL-ifc(s)  VLAN
-ID
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
INTERNET          9999
                                     IPOE       local      000000000000   1           0
```

To set the IP address for this new peer, we switch to: /Setup/WAN/IP-List

A possible command might be:

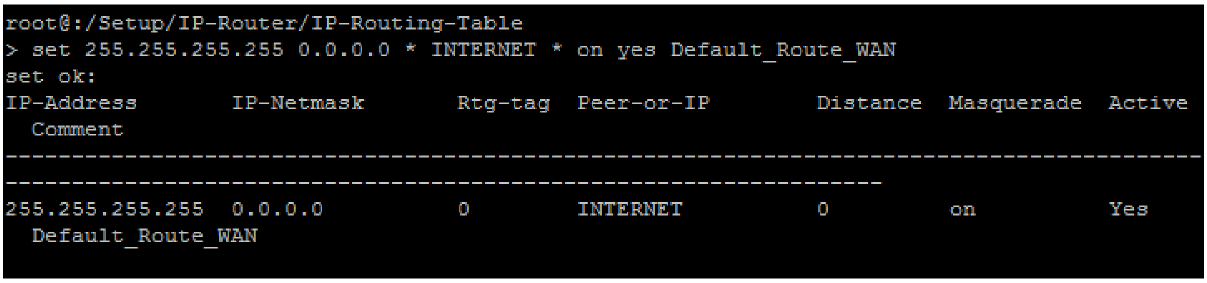
- “set INTERNET 10.1.204.151 255.255.0.0 * 10.1.1.11 10.1.1.11”



```
root@:/Setup/WAN/IP-List
> set INTERNET 10.1.204.151 255.255.0.0 * 10.1.1.11 10.1.1.11
set ok:
Peer              IP-Address       IP-Netmask       Masq.-IP-Addr.   Gateway          DNS-
Default      DNS-Backup       NBNS-Default     NBNS-Backup
------------------------------------------------------------------------------------------
--------------------------------------------------------------
INTERNET          10.1.204.151     255.255.0.0      0.0.0.0          10.1.1.11        10.1
.1.11        0.0.0.0          0.0.0.0          0.0.0.0
```

The last thing to do to get the WAN up and running is creating a default route. This must be done in: /Setup/IP-Router/IP-Routing-Table. To create the default route for the peer INTERNET, type the following:

- “set 255.255.255.255 0.0.0.0 * INTERNET * on yes Default_Route_WAN”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 255.255.255.255 0.0.0.0 * INTERNET * on yes Default_Route_WAN
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active
  Comment
------------------------------------------------------------------------------------------
------------------------------------------------------------------
255.255.255.255  0.0.0.0          0        INTERNET          0         on          Yes
  Default_Route_WAN
```

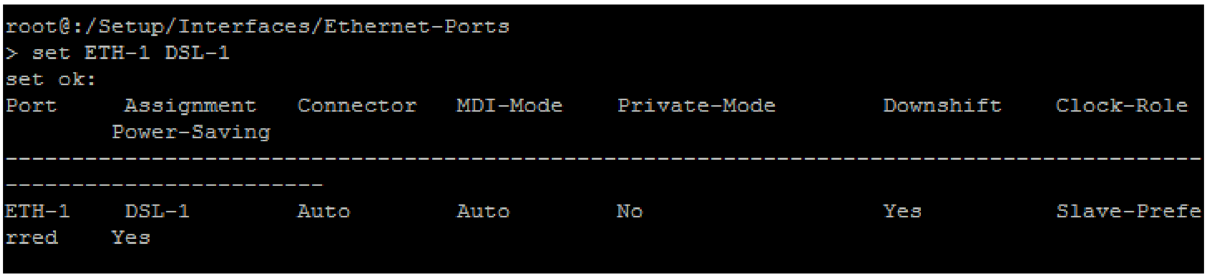
Now the IPoE connection is up and running. You can check /Status/Info-Connection to verify that the connection is established.

### 2.6.3. WAN connection (PPP over Ethernet)

To create a PPP over Ethernet WAN connection, you must start with the configuration of the Ethernet-Ports. This must be done in: /Setup/Interfaces/Ethernet-Ports. In this example, the WAN uplink cable was put into Ethernet-Port 1. The first step is to assign the logical interface DSL-1 to the physical interface ETH-1.

The assignment can be done by typing the following command:

- “set ETH-1 DSL-1”

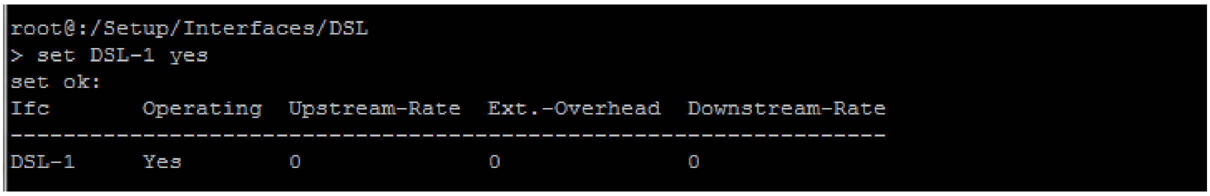


```
root@:/Setup/Interfaces/Ethernet-Ports
> set ETH-1 DSL-1
set ok:
Port     Assignment   Connector   MDI-Mode    Private-Mode        Downshift    Clock-Role
        Power-Saving
------------------------------------------------------------------------------------------
------------------------
ETH-1    DSL-1        Auto        Auto        No                  Yes          Slave-Prefe
rred    Yes
```

The next step is to activate the logical interface DSL-1. This must be done in: /Setup/Interfaces/DSL

The appropriate command:

- “set DSL-1 yes”

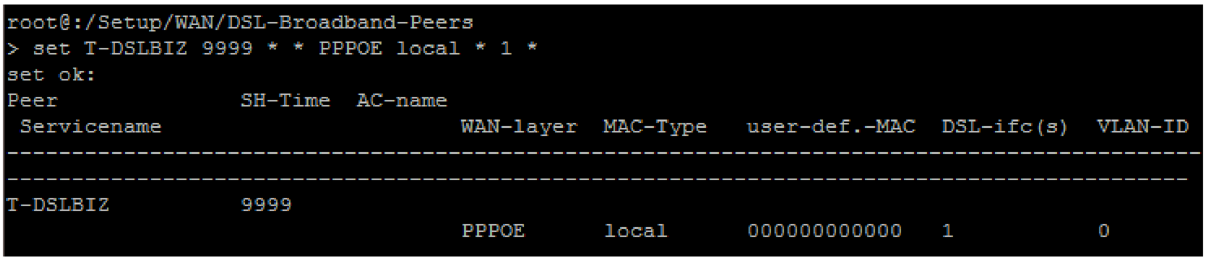


```
root@:/Setup/Interfaces/DSL
> set DSL-1 yes
set ok:
Ifc       Operating  Upstream-Rate  Ext.-Overhead  Downstream-Rate
-------------------------------------------------------------------
DSL-1     Yes        0              0              0
```

Now it’s time to configure a DSL-Broadband-Peer. This must be done in: /Setup/WAN/DSL-Broadband-Peers. Here it is necessary to give the peer a name, set a short-hold time, assign an appropriate WAN-Layer and DSL-Interface.

A possible command might be:

- “set T-DSLBIZ 9999 * * PPPOE local * 1 *”

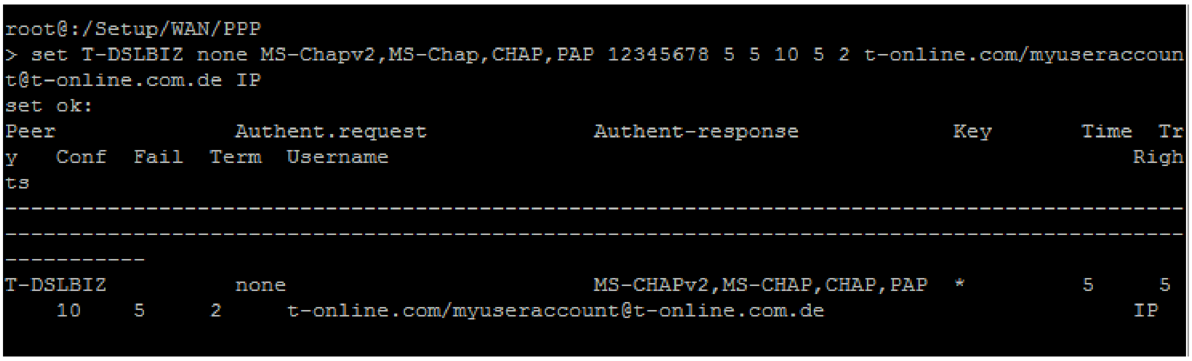


```
root@:/Setup/WAN/DSL-Broadband-Peers
> set T-DSLBIZ 9999 * * PPPOE local * 1 *
set ok:
Peer                SH-Time  AC-name
 Servicename                           WAN-layer  MAC-Type   user-def.-MAC  DSL-ifc(s)  VLAN-ID
----------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------
T-DSLBIZ            9999
                                       PPPOE      local      000000000000   1           0
```

Because this is a PPP connection, the next step is to put in the login information from your internet provider. This must be done in /Setup/WAN/PPP

A possible command might be:

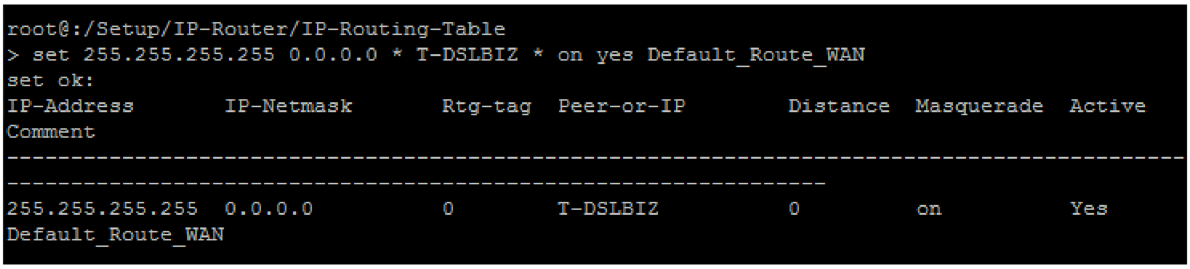
- “set T-DSLBIZ none MS-Chapv2,MS-Chap,CHAP,PAP 12345678 5 5 10 5 2 t-online.com/myuseraccount@t-online.com.de IP”



```
root@:/Setup/WAN/PPP
> set T-DSLBIZ none MS-Chapv2,MS-Chap,CHAP,PAP 12345678 5 5 10 5 2 t-online.com/myuseraccoun
t@t-online.com.de IP
set ok:
Peer               Authent.request             Authent-response            Key       Time  Tr
y   Conf  Fail  Term  Username                                                         Righ
ts
---------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------
-----------
T-DSLBIZ           none                        MS-CHAPv2,MS-CHAP,CHAP,PAP  *         5     5
    10    5     2     t-online.com/myuseraccount@t-online.com.de                       IP
```

The last thing to do to get the WAN up and running is creating a default route. This must be done in: /Setup/IP-Router/IP-Routing-Table. To create the default route for the peer T-DSLBIZ, type the following:

- “set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active
Comment
-------------------------------------------------------------------------------------------
----------------------------------------------------------------
255.255.255.255  0.0.0.0          0        T-DSLBIZ          0         on          Yes
Default_Route_WAN
```

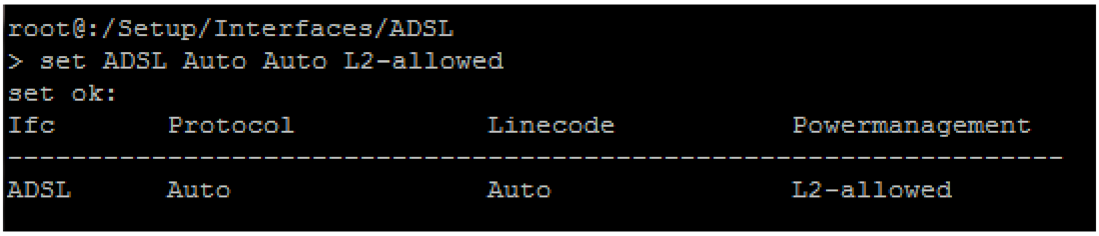
Now the PPPoE connection is up and running. You can check /Status/Info-Connection to verify that the connection is established.

## 2.6.4. WAN connection (PPP over Ethernet over ATM)

To create a PPP over Ethernet ADSL connection, you may start with the configuration of the ADSL-Port. This must be done in: /Setup/Interfaces/ADSL. The first step is to activate the ADSL interface.

This can be done by typing the following command:

- “set ADSL Auto Auto L2-allowed”

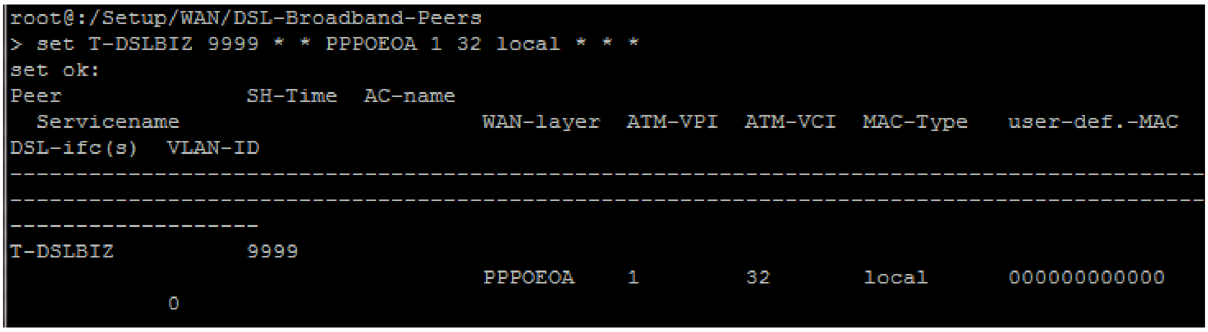


```
root@:/Setup/Interfaces/ADSL
> set ADSL Auto Auto L2-allowed
set ok:
Ifc       Protocol            Linecode            Powermanagement
------------------------------------------------------------------
ADSL      Auto                Auto                L2-allowed
```

Now it’s time to configure a DSL-Broadband-Peer. This must be done in: /Setup/WAN/DSL-Broadband-Peers. Here it is necessary to give the peer a name, set a short-hold time, assign an appropriate WAN-Layer, and set VPI and VCI values and MAC-Type.

A possible command might be:

- “set T-DSLBIZ 9999 * * PPPOEOA 1 32 local * * *”

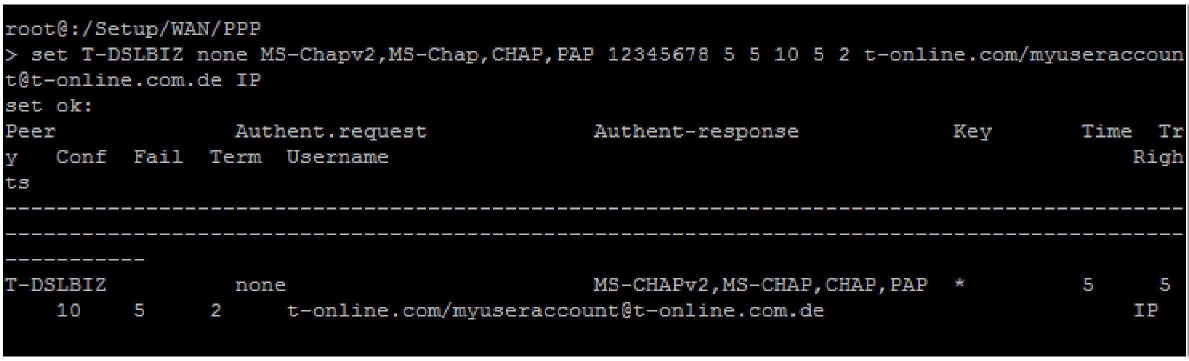


```
root@:/Setup/WAN/DSL-Broadband-Peers
> set T-DSLBIZ 9999 * * PPPOEOA 1 32 local * * *
set ok:
Peer                SH-Time   AC-name
  Servicename                         WAN-layer  ATM-VPI  ATM-VCI  MAC-Type   user-def.-MAC
DSL-ifc(s)  VLAN-ID
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
---------------------
T-DSLBIZ            9999
                                      PPPOEOA    1        32       local      000000000000
            0
```

Because this is a PPP connection, the next step is to put in the login information from your internet provider. This must be done in /Setup/WAN/PPP

A possible command might be:

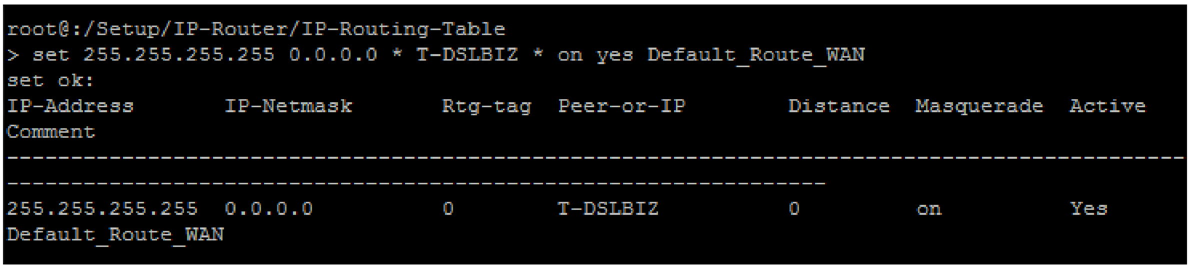
- “set T-DSLBIZ none MS-Chapv2,MS-Chap,CHAP,PAP 12345678 5 5 10 5 2 t-online.com/myuseraccount@t-online.com.de IP”



```
root@:/Setup/WAN/PPP
> set T-DSLBIZ none MS-Chapv2,MS-Chap,CHAP,PAP 12345678 5 5 10 5 2 t-online.com/myuseraccoun
t@t-online.com.de IP
set ok:
Peer              Authent.request            Authent-response            Key       Time   Tr
y   Conf   Fail   Term   Username                                                         Righ
ts
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----------
T-DSLBIZ          none                       MS-CHAPv2,MS-CHAP,CHAP,PAP  *          5      5
    10     5      2      t-online.com/myuseraccount@t-online.com.de                       IP
```

The last thing to do to get the WAN up and running is creating a default route. This must be done in: /Setup/IP-Router/IP-Routing-Table. To create the default route for the peer T-DSLBIZ, type the following:

- “set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN
set ok:
IP-Address        IP-Netmask        Rtg-tag  Peer-or-IP        Distance  Masquerade  Active
Comment
--------------------------------------------------------------------------------------------
----------------------------------------------------------------
255.255.255.255   0.0.0.0           0        T-DSLBIZ          0         on          Yes
Default_Route_WAN
```

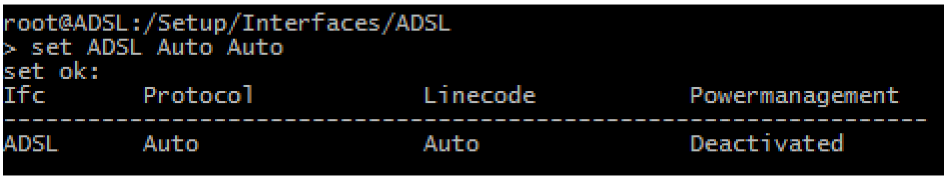
Now the PPPoE ADSL connection is up and running. You can check /Status/Info-Connection to verify that the connection is established.

### 2.6.5. WAN connection (ADSL)

To create a ADSL connection, you may start with the configuration of the ADSL-Port. This must be done in: /Setup/Interfaces/ADSL. The first step is to activate the ADSL interface.

This can be done by typing the following command:

- “set ADSL Auto Auto”

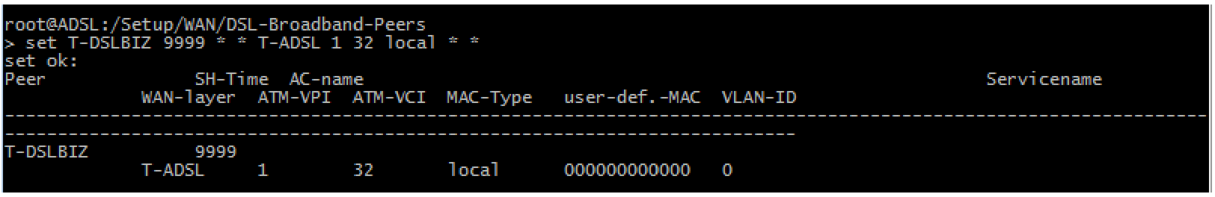


```
root@ADSL:/Setup/Interfaces/ADSL
> set ADSL Auto Auto
set ok:
Ifc       Protocol             Linecode            Powermanagement
-----------------------------------------------------------------
ADSL      Auto                 Auto                Deactivated
```

Now it’s time to configure a DSL-Broadband-Peer. This must be done in: /Setup/WAN/DSL-Broadband-Peers. Here it is necessary to give the peer a name, set a short-hold time, assign an appropriate WAN-Layer, VPI and VCI values and MAC-Type.

A possible command might be:

- “set T-DSLBIZ 9999 * * T-ADSL 1 32 local * *”

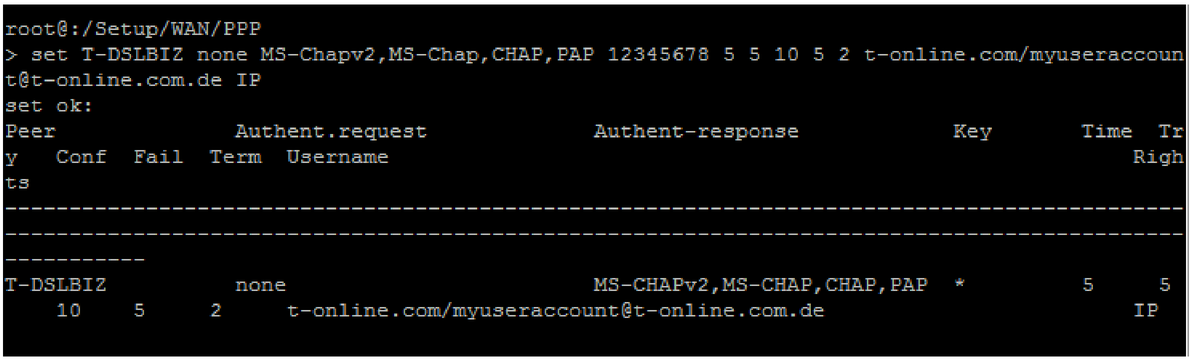


```
root@ADSL:/Setup/WAN/DSL-Broadband-Peers
> set T-DSLBIZ 9999 * * T-ADSL 1 32 local * *
set ok:
Peer              SH-Time  AC-name                                                          Servicename
             WAN-layer  ATM-VPI  ATM-VCI  MAC-Type   user-def.-MAC  VLAN-ID
------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------
T-DSLBIZ          9999
             T-ADSL     1        32       local      000000000000   0
```

The next step is to put in the login information from your internet provider. This must be done in /Setup/WAN/PPP

A possible command might be:

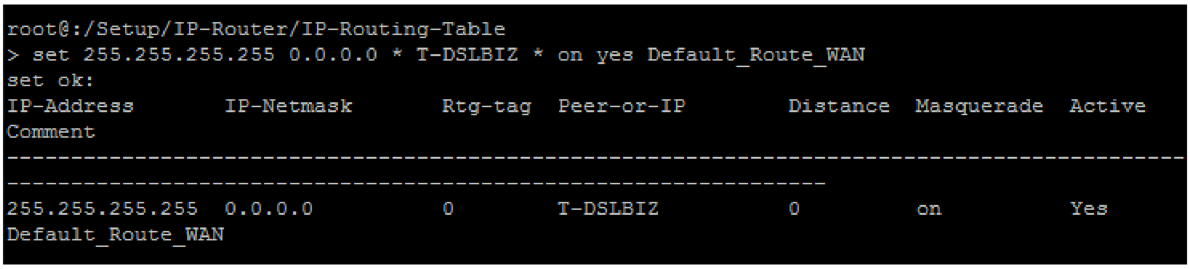
- “set T-DSLBIZ none MS-Chapv2,MS-Chap,CHAP,PAP 12345678 5 5 10 5 2 t-online.com/myuseraccount@t-online.com.de IP”



```
root@:/Setup/WAN/PPP
> set T-DSLBIZ none MS-Chapv2,MS-Chap,CHAP,PAP 12345678 5 5 10 5 2 t-online.com/myuseraccoun
t@t-online.com.de IP
set ok:
Peer              Authent.request             Authent-response            Key       Time  Tr
y   Conf  Fail  Term  Username                                                          Righ
ts
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----------
T-DSLBIZ          none                        MS-CHAPv2,MS-CHAP,CHAP,PAP  *         5     5
    10    5     2     t-online.com/myuseraccount@t-online.com.de                        IP
```

The last thing to do to get the WAN up and running is creating a default route. This must be done in: /Setup/IP-Router/IP-Routing-Table. To create the default route for the peer T-DSLBIZ, type the following:

- “set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active
Comment
--------------------------------------------------------------------------------------------
----------------------------------------------------------------
255.255.255.255  0.0.0.0          0        T-DSLBIZ          0         on          Yes
Default_Route_WAN
```

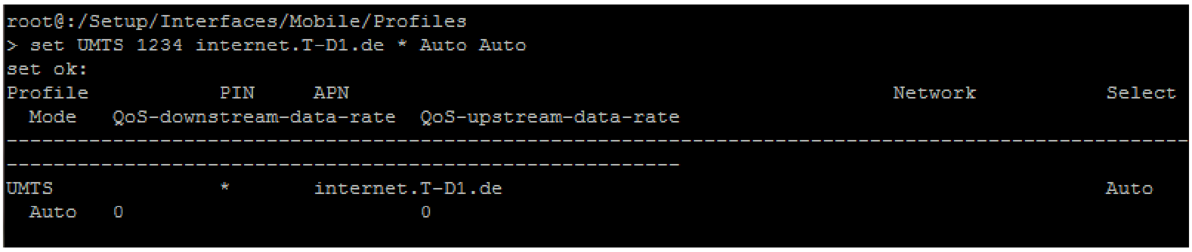
Now the ADSL connection is up and running. You can check /Status/Info-Connection to verify that the connection is established.

### 2.6.6. WAN connection (UMTS/LTE)

To create a 3G/LTE connection, you must start with the configuration of the mobile interface profile. This must be done in: /Setup/Interfaces/Mobile/Profiles. The first step is to create a profile. Here you need your PIN and APN information from your provider.

A possible entry would be:

- “set UMTS 1234 internet.T-D1.de * Auto Auto”

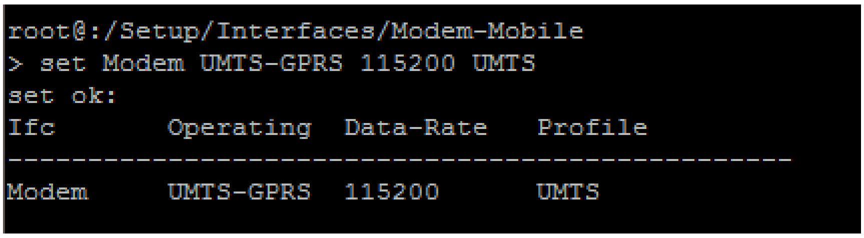


```
root@:/Setup/Interfaces/Mobile/Profiles
> set UMTS 1234 internet.T-D1.de * Auto Auto
set ok:
Profile           PIN     APN                                                Network           Select
  Mode   QoS-downstream-data-rate  QoS-upstream-data-rate
----------------------------------------------------------------------------------------------------
---------------------------------------------------------
UMTS              *       internet.T-D1.de                                                     Auto
  Auto   0                         0
```

To assign the new profile to the mobile interface, please go to /Setup/Interfaces/Modem-Mobile

You must set the new profile with the following command:

- For 3G: “set Modem UMTS-GPRS 115200 UMTS”
- For LTE: “set Modem WWAN 115200 UMTS”

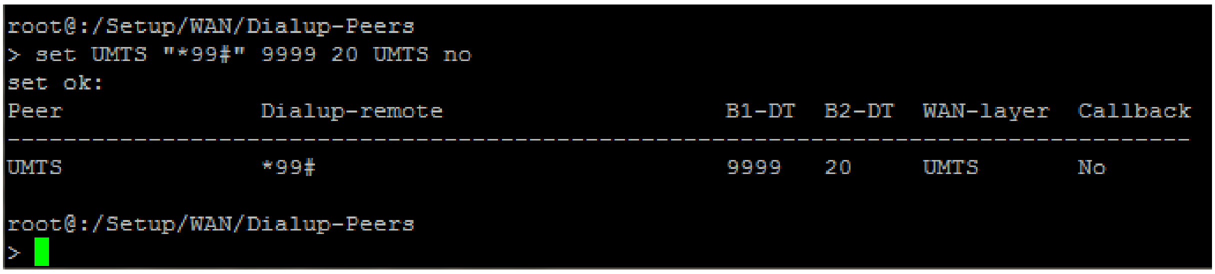


```
root@:/Setup/Interfaces/Modem-Mobile
> set Modem UMTS-GPRS 115200 UMTS
set ok:
Ifc       Operating  Data-Rate   Profile
-------------------------------------------------
Modem     UMTS-GPRS  115200      UMTS
```

Now it’s time to configure a Dialup-Peer. This must be done in: /Setup/WAN/Dialup-Peer. Here it is necessary to give the peer a name, set a Dialup-remote, short-hold times and an appropriate WAN-Layer.

A possible command might be:

- “set UMTS *99# 9999 20 UMTS no”

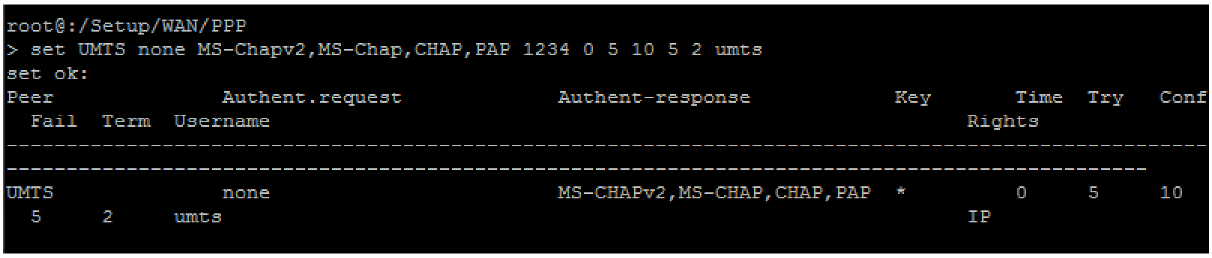


```
root@:/Setup/WAN/Dialup-Peers
> set UMTS "*99#" 9999 20 UMTS no
set ok:
Peer              Dialup-remote                    B1-DT  B2-DT  WAN-layer  Callback
------------------------------------------------------------------------------------
UMTS              *99#                             9999   20     UMTS       No

root@:/Setup/WAN/Dialup-Peers
> 
```

The next step is to create a PPP entry in the PPP table. This must be done in /Setup/WAN/PPP

A possible command might be:

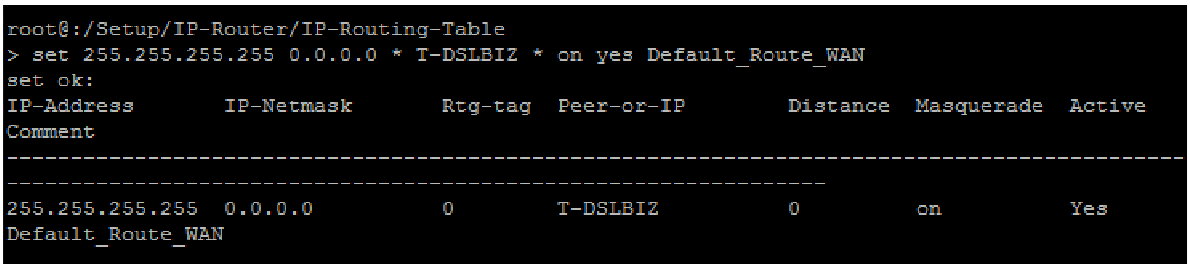
- “set UMTS none MS-Chapv2,MS-Chap,CHAP,PAP 1234 0 5 10 5 2 umts IP”



```
root@:/Setup/WAN/PPP
> set UMTS none MS-Chapv2,MS-Chap,CHAP,PAP 1234 0 5 10 5 2 umts
set ok:
Peer              Authent.request             Authent-response            Key       Time  Try   Conf
  Fail  Term  Username                                                          Rights
----------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
UMTS              none                        MS-CHAPv2,MS-CHAP,CHAP,PAP  *         0     5     10
  5     2     umts                                                              IP
```

The last thing to do to get the WAN up and running is creating a default route. This must be done in: /Setup/IP-Router/IP-Routing-Table. To create the default route for the peer UMTS, type the following:

- “set 255.255.255.255 0.0.0.0 * UMTS * on yes Default_Route_WAN”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 255.255.255.255 0.0.0.0 * T-DSLBIZ * on yes Default_Route_WAN
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active
Comment
---------------------------------------------------------------------------------------------
-----------------------------------------------------------------
255.255.255.255  0.0.0.0          0        T-DSLBIZ          0         on          Yes
Default_Route_WAN
```

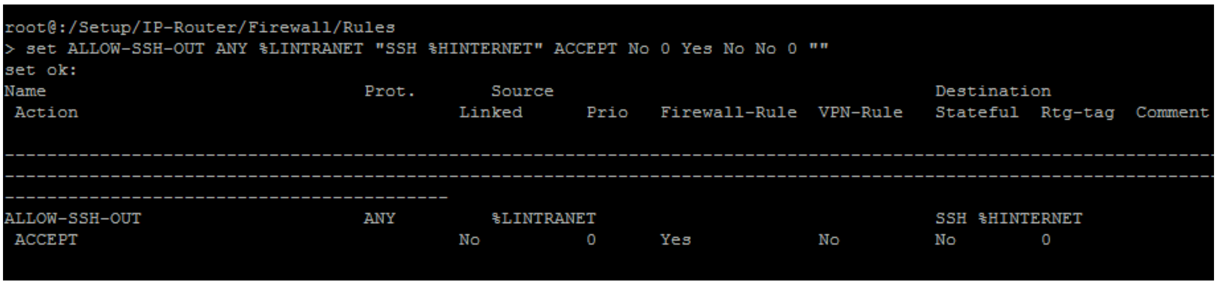
Now the UMTS/LTE connection is up and running. You can check /Status/Info-Connection to verify that the connection is established.

## 2.6.7. Configuring the Firewall

In AGD_PRE (1.2.2 – Installation of the TOE) you already created a deny-all firewall rule. To allow an outgoing connection for example, you must create a firewall rule which allows the required traffic to pass the firewall. To do this, you must go to /Setup/IP-Router/Firewall/Rules

If you want to allow outgoing SSHv2 connections from your Intranet, a possible command might be:

- set ALLOW-SSH-OUT ANY %LINTRANET "SSH %HINTERNET" ACCEPT No 0 Yes No No 0 ""



```
root@:/Setup/IP-Router/Firewall/Rules
> set ALLOW-SSH-OUT ANY %LINTRANET "SSH %HINTERNET" ACCEPT No 0 Yes No No 0 ""
set ok:
Name                              Prot.       Source                                    Destination
 Action                                    Linked      Prio   Firewall-Rule  VPN-Rule   Stateful  Rtg-tag  Comment

------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------
------------------------------------------
ALLOW-SSH-OUT                     ANY         %LINTRANET                                SSH %HINTERNET
 ACCEPT                                    No          0      Yes            No         No        0
```

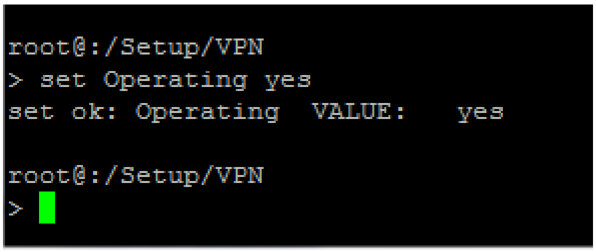
For more information regarding firewall rules, check LCOS-MENU-860-EN.pdf (2.8.10.1-> 2.8.10.2.9).

## 2.6.8. VPN Site-to-Site Connection (Preshared Key)

To get started, you must switch to /Setup/VPN. There you must activate the VPN module.

You must do this by typing the command:

- “set Operating yes”.



```
root@:/Setup/VPN
> set Operating yes
set ok: Operating  VALUE:   yes

root@:/Setup/VPN
> 
```

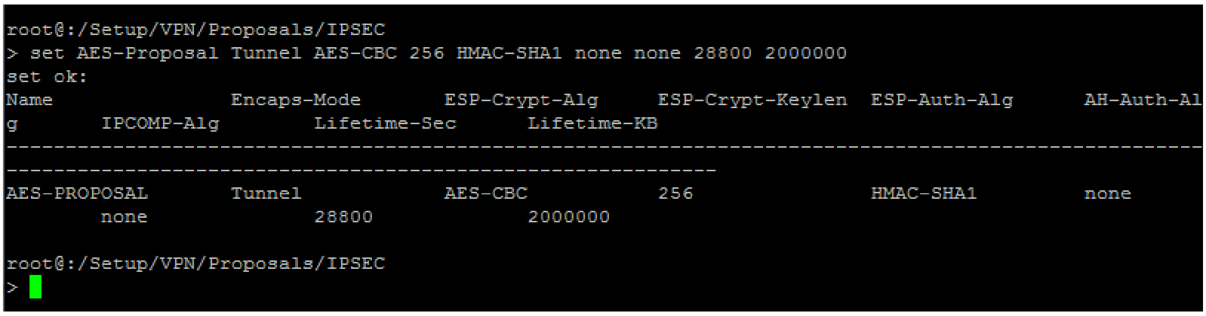
Then you must switch to /Setup/VPN/Proposals/IPSEC. Here you must define your IPsec proposal settings. There are several settings you must set, such as Name, Encaps-Mode, ESP-Crypt-Alg, ESP-Crypt-Keylen, ESP-Auth-Alg, AH-Auth-Alg, IPCOMP-Alg, Lifetime-Sec and Lifetime-KB. For secure operation only use AES Encryption and HMAC-SHA Authentication.

Available options are:

| ESP-Crypt-Algorithm | ESP-Crypt-Keylength | ESP-Authentication-Algorithm |
|---|---|---|
| **AES-CBC** | 128 | HMAC-SHA-1 |
| **AES-CBC** | 128 | HMAC-SHA-256 |
| **AES-CBC** | 192 | HMAC-SHA-1 |
| **AES-CBC** | 192 | HMAC-SHA-256 |
| **AES-CBC** | 256 | HMAC-SHA-1 |
| **AES-CBC** | 256 | HMAC-SHA-256 |

Here is an example of how a command might look like:

- “set AES-PROPOSAL Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000”



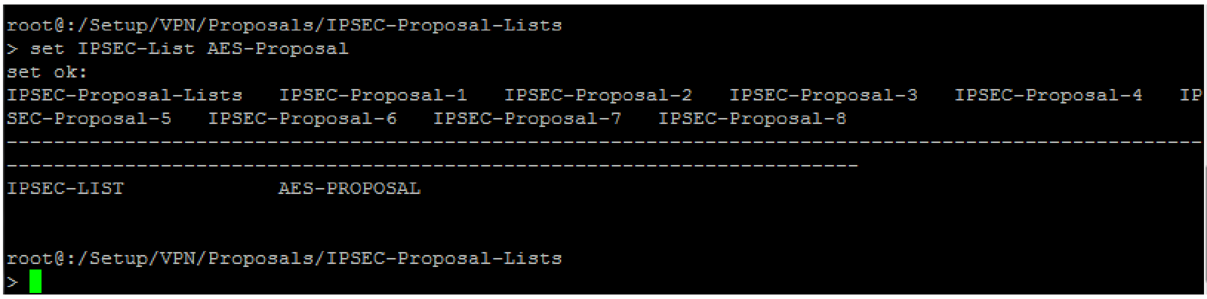
```
root@:/Setup/VPN/Proposals/IPSEC
> set AES-Proposal Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000
set ok:
Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-Auth-Alg      AH-Auth-Al
g       IPCOMP-Alg        Lifetime-Sec      Lifetime-KB
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------
AES-PROPOSAL       Tunnel            AES-CBC           256               HMAC-SHA1         none
        none              28800             2000000

root@:/Setup/VPN/Proposals/IPSEC
> █
```

Note: The Encaps-Mode mode must be set to “Tunnel”, the AH-Auth-Alg. must be set to “none” and the lifetimes must be set to 28800 sec / 2000000 KB.

Now an IPsec proposal has been created. To use it later on, you must put the proposal into a proposal list and give the list a name. This must be done in /Setup/VPN/Proposals/IPSEC-Proposal-Lists.

To add the created IPsec proposal to a new proposal list, you can type the following command:

“set IPSEC-LIST AES-PROPOSAL”



```
root@:/Setup/VPN/Proposals/IPSEC-Proposal-Lists
> set IPSEC-List AES-Proposal
set ok:
IPSEC-Proposal-Lists   IPSEC-Proposal-1   IPSEC-Proposal-2   IPSEC-Proposal-3   IPSEC-Proposal-4   IP
SEC-Proposal-5   IPSEC-Proposal-6   IPSEC-Proposal-7   IPSEC-Proposal-8
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------------------
IPSEC-LIST             AES-PROPOSAL


root@:/Setup/VPN/Proposals/IPSEC-Proposal-Lists
> █
```

As you can see, there is now a new proposal list with the name “IPSEC-LIST” and the referenced IPsec proposal “AES-Proposal” we created above.

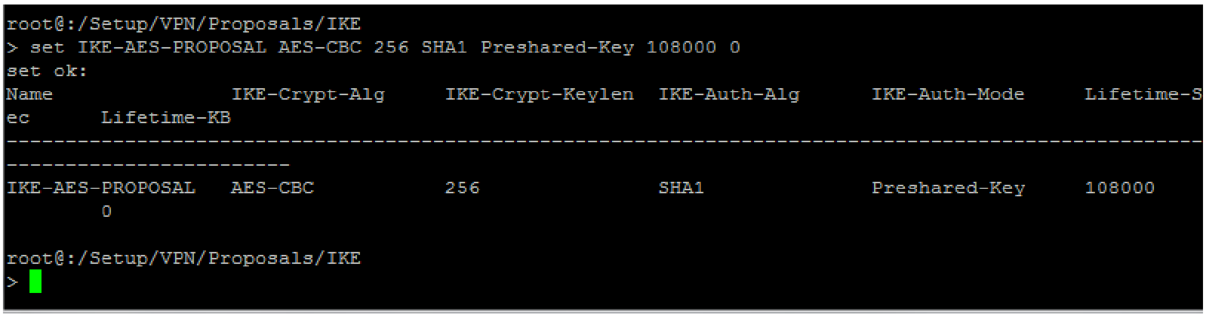
The next step is to create an IKE proposal, which must be done in /Setup/VPN/Proposals/IKE. It works very similar to the IPsec proposal configuration. Again you must give the proposal a name, set an IKE-Crypt-Algorithm etc. For secure operation make sure only use AES Encryption and SHA Authentication.

Available options are:

| IKE-Crypt-Algorithm | IKE-Crypt-Keylength | IKE-Auth-Algorithm |
|---|---|---|
| **AES-CBC** | 128 | SHA-1 |
| **AES-CBC** | 128 | SHA-256 |
| **AES-CBC** | 192 | SHA-1 |
| **AES-CBC** | 192 | SHA-256 |
| **AES-CBC** | 256 | SHA-1 |
| **AES-CBC** | 256 | SHA-256 |

A possible command might be:

- “set IKE-AES-PROPOSAL AES-CBC 256 SHA1 Preshared-Key 108000 0”

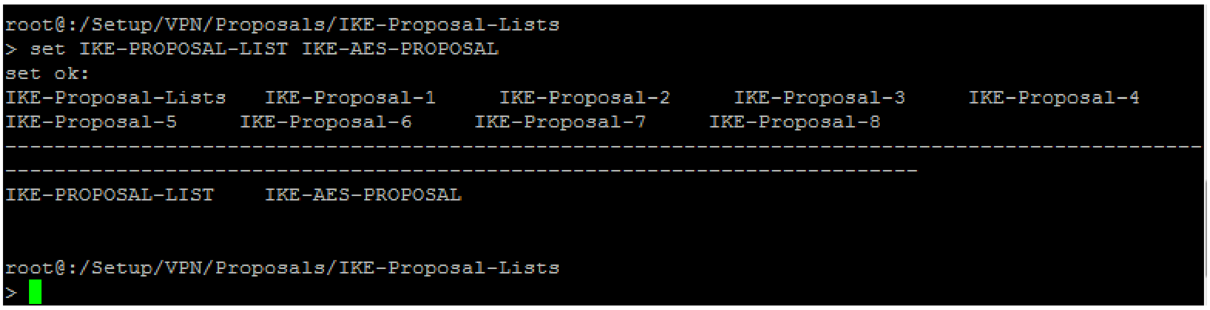


```
root@:/Setup/VPN/Proposals/IKE
> set IKE-AES-PROPOSAL AES-CBC 256 SHA1 Preshared-Key 108000 0
set ok:
Name               IKE-Crypt-Alg     IKE-Crypt-Keylen  IKE-Auth-Alg      IKE-Auth-Mode     Lifetime-S
ec       Lifetime-KB
---------------------------------------------------------------------------------------------------------
------------------------
IKE-AES-PROPOSAL   AES-CBC           256               SHA1              Preshared-Key     108000
        0

root@:/Setup/VPN/Proposals/IKE
>
```

The now created IKE proposal must be added to an IKE-proposal-list, like we did with the IPsec proposal. This must be done in /Setup/VPN/Proposals/IKE-Proposal-Lists.

A possible command might be:

- “set IKE-PROPOSAL-LIST IKE-AES-PROPOSAL”



```
root@:/Setup/VPN/Proposals/IKE-Proposal-Lists
> set IKE-PROPOSAL-LIST IKE-AES-PROPOSAL
set ok:
IKE-Proposal-Lists   IKE-Proposal-1     IKE-Proposal-2     IKE-Proposal-3     IKE-Proposal-4
IKE-Proposal-5     IKE-Proposal-6     IKE-Proposal-7     IKE-Proposal-8
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
IKE-PROPOSAL-LIST    IKE-AES-PROPOSAL


root@:/Setup/VPN/Proposals/IKE-Proposal-Lists
>
```

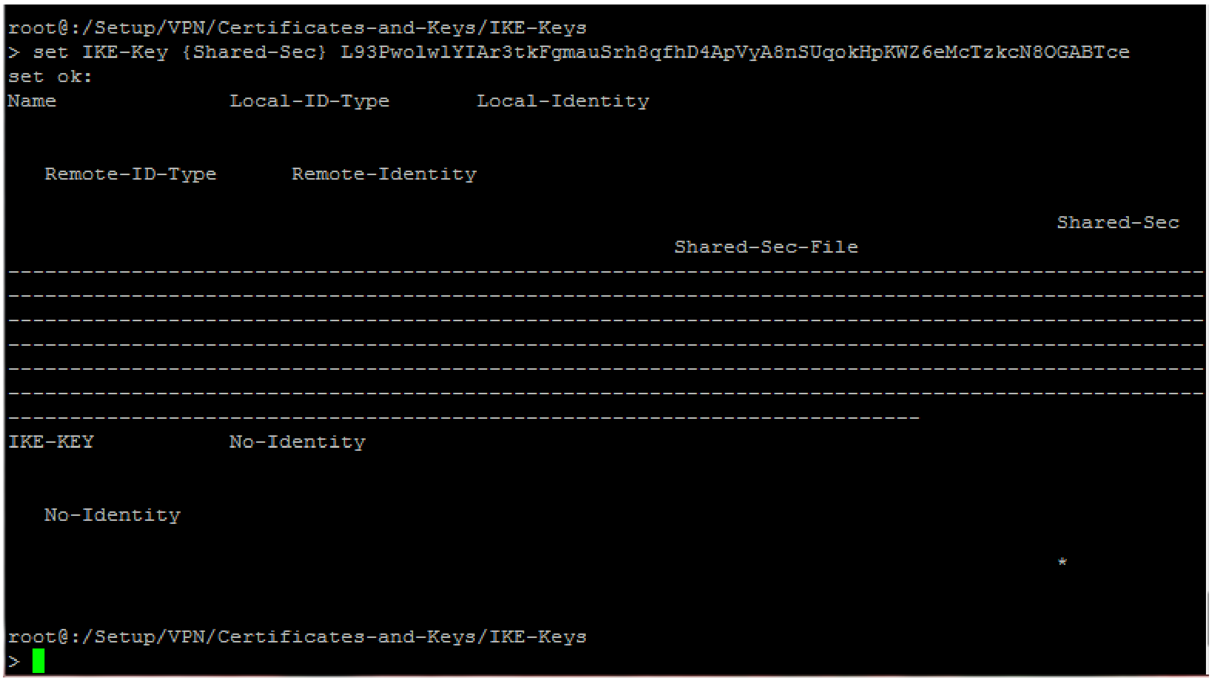
Since we have our proposals for IKE and IPsec ready, the next thing to do is create an IKE-Key.

This must be done in /Setup/VPN/Certificates-and-Keys/IKE-Keys.

Here we only need a name for the entry and the shared secret (preshared key containing 64 alphabetic, numeric and special characters), everything else can be skipped. The preshared key must be securely generated as a password would be generated. A strong preshared key must be of maximal length (64 characters) and be resistant against dictionary attacks.

A possible command might be:

- “set IKE-Key {Shared-Sec} L93PwolwlYIAr3tkFgmauSrh8qfhD4ApVyA8nSUqokHpKWZ6eMcTzkcN8OGABTce”



```
root@:/Setup/VPN/Certificates-and-Keys/IKE-Keys
> set IKE-Key {Shared-Sec} L93PwolwlYIAr3tkFgmauSrh8qfhD4ApVyA8nSUqokHpKWZ6eMcTzkcN8OGABTce
set ok:
Name              Local-ID-Type       Local-Identity


   Remote-ID-Type      Remote-Identity

                                                                                     Shared-Sec
                                                      Shared-Sec-File
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------
IKE-KEY           No-Identity


   No-Identity


                                                                                     *


root@:/Setup/VPN/Certificates-and-Keys/IKE-Keys
>
```

The next step is to put this information into a VPN layer. This must be done in /Setup/VPN/Layer.

Here you must define the created proposals for IKE and IPsec, the just created IKE-Key and the IKE- and PFS-Groups (both Diffie-Hellman).

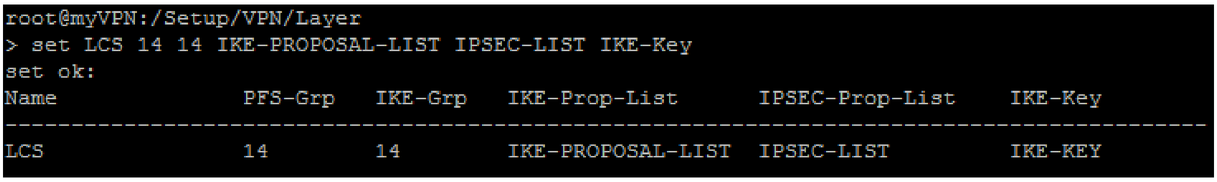
For secure operation make sure you only use Diffie-Hellman group 14 (2048 Bit). Available options are:

| PFS-Group (Diffie-Hellmann) | IKE-Group (Diffie-Hellmann) |
|---|---|
| 14 (2048 Bit) | 14 (2048 Bit) |

will be checked by cctest

A possible command would be:

- “set LCS 14 14 IKE-PROPOSAL-LIST IPSEC-LIST IKE-Key”

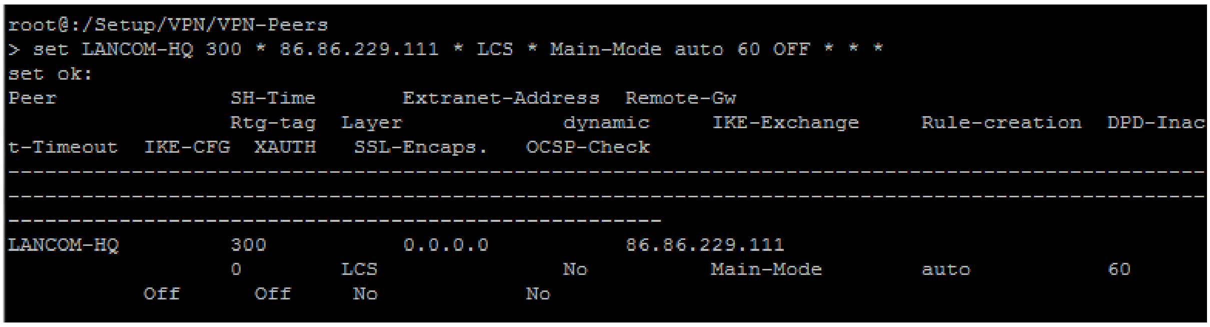


```
root@myVPN:/Setup/VPN/Layer
> set LCS 14 14 IKE-PROPOSAL-LIST IPSEC-LIST IKE-Key
set ok:
Name              PFS-Grp   IKE-Grp   IKE-Prop-List      IPSEC-Prop-List    IKE-Key
-------------------------------------------------------------------------------------------
LCS               14        14        IKE-PROPOSAL-LIST  IPSEC-LIST         IKE-KEY
```

With this newly created VPN-Layer, we are able to add a VPN-Peer. This must be done in /Setup/VPN/VPN-Peers. Available options are: Peer-Name, Short-hold-time, Extranet-Address, Remote-Gateway-Address, Routing-tag, Layer, IKE-Exchange, Rule-Creation, DPD-Timeout and IKE-cfg-mode

A possible command might be:

- “set LANCOM-HQ 300 * 86.86.229.111 * LCS * Main-Mode auto 60 OFF * * *”

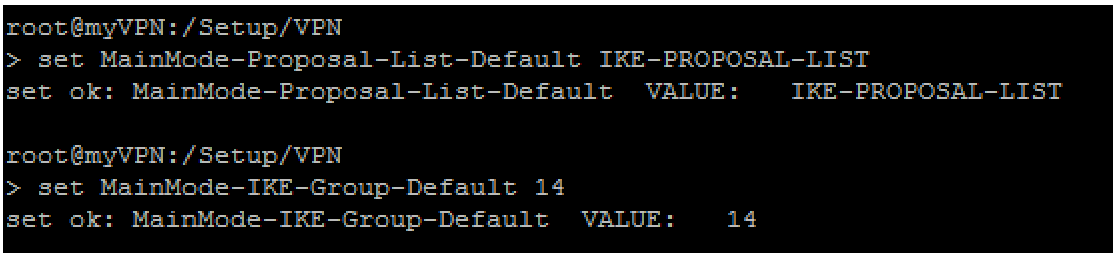


```
root@:/Setup/VPN/VPN-Peers
> set LANCOM-HQ 300 * 86.86.229.111 * LCS * Main-Mode auto 60 OFF * * *
set ok:
Peer              SH-Time       Extranet-Address  Remote-Gw
                  Rtg-tag  Layer              dynamic     IKE-Exchange     Rule-creation  DPD-Inac
t-Timeout  IKE-CFG  XAUTH   SSL-Encaps.   OCSP-Check
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
LANCOM-HQ         300           0.0.0.0           86.86.229.111
                  0        LCS                No          Main-Mode        auto           60
           Off      Off     No            No
```

To allow incoming Main Mode connections, we must set default values. This must be done in /Setup/VPN. The IKE-Group-Default (Diffie-Hellman) value must be the same as chosen above.

Possible commands might be:

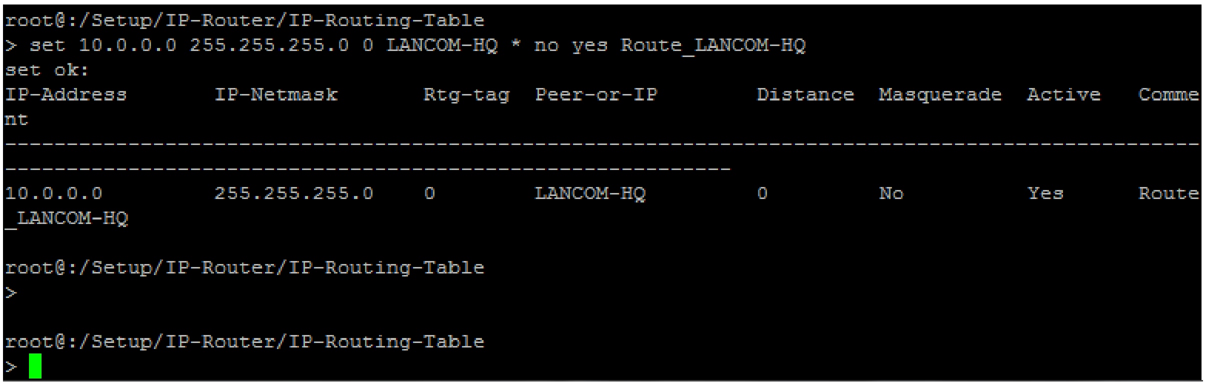
- “set MainMode-Proposal-List-Default IKE-PROPOSAL-LIST”
- “set MainMode-IKE-Group-Default 14”



```
root@myVPN:/Setup/VPN
> set MainMode-Proposal-List-Default IKE-PROPOSAL-LIST
set ok: MainMode-Proposal-List-Default  VALUE:   IKE-PROPOSAL-LIST

root@myVPN:/Setup/VPN
> set MainMode-IKE-Group-Default 14
set ok: MainMode-IKE-Group-Default  VALUE:   14
```

The last remaining step is to set the destination network in the IP-routing-table. This must be done in: /Setup/IP-Router/IP-Routing-Table. Here you must set the network details of your remote network. A possible command might be:

- “set 10.0.0.0 255.255.255.0 0 LANCOM-HQ * no yes Route_LANCOM-HQ”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 10.0.0.0 255.255.255.0 0 LANCOM-HQ * no yes Route_LANCOM-HQ
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active   Comme
nt
-------------------------------------------------------------------------------------------------
-----------------------------------------------------------
10.0.0.0         255.255.255.0    0        LANCOM-HQ         0         No          Yes      Route
_LANCOM-HQ

root@:/Setup/IP-Router/IP-Routing-Table
>

root@:/Setup/IP-Router/IP-Routing-Table
>
```

Now we are all set and able to establish a secure VPN site-to-site connection via Preshared-Key.

## 2.6.9. Requirements for the Use of VPN Certificates

It is mandatory for the evaluated configuration to use self-signed certificates when using certificates for VPN connections. The use of a CA (Certificate Authority) is not allowed. All certificates must be based on a RSA key with 2048 bit length. When creating a self-signed certificate it is mandatory to include the X509v3 extension “Basic Constraints” and set the value to “CA:FALSE”[1]:

To import VPN certificates it is necessary to create a PKCS12 (*.p12) file containing the device certificate and the corresponding private key. It is only allowed to use this PKCS12 file for one device. All other devices must have their own PKCS12 file with individual certificates and private keys. To import the VPN certificate you must use the following command:

- LCS_PASSWORD="EnterCertificatePasswordHere" scp -o SendEnv=LCS_PASSWORD vpn.p12 root@10.10.10.1:vpn_pkcs12_2

You must make sure to import the VPN certificate to one of the VPN slots between 2 to 9, since the first slot does not support self-signed certificates.

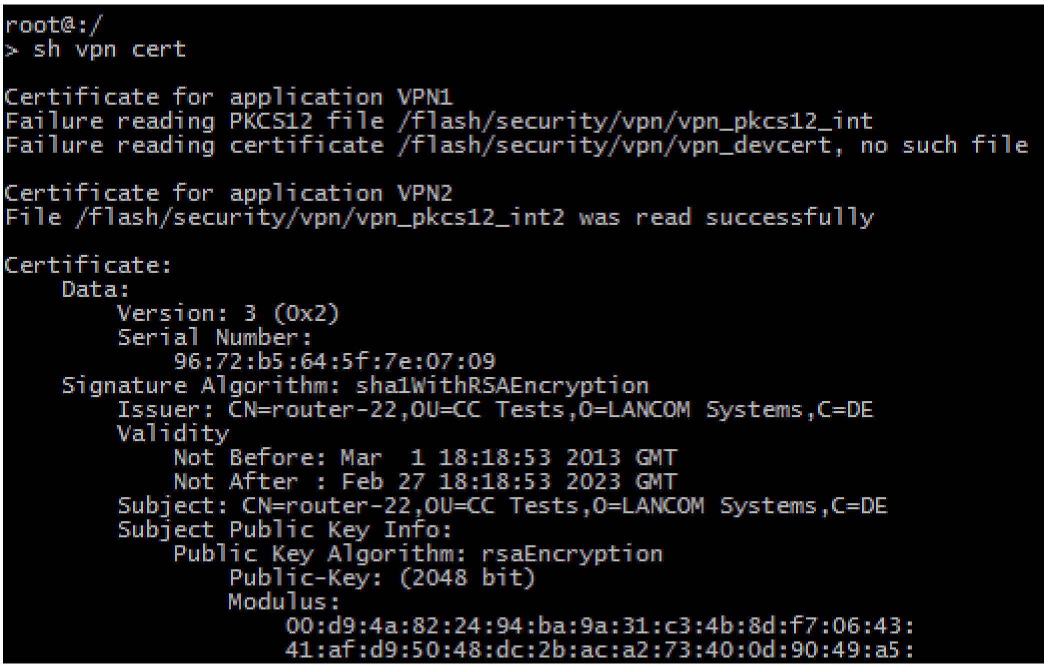
| VPN slot | Usage |
|---|---|
| **vpn_pkcs12** | Not allowed |
| **vpn_pkcs12_2** | Allowed |
| **vpn_pkcs12_3** | Allowed |
| **vpn_pkcs12_4** | Allowed |
| **vpn_pkcs12_5** | Allowed |
| **vpn_pkcs12_6** | Allowed |
| **vpn_pkcs12_7** | Allowed |
| **vpn_pkcs12_8** | Allowed |
| **vpn_pkcs12_9** | Allowed |

Every VPN slot can only be used with one self-signed certificate. Importing a new self-signed certificate into an already used slot will overwrite the existing certificate. To make sure the existing certificate is securely erased you must use the “secure erase” command as mentioned in - 2.8.2 Secure Key Destruction.

Once this is done, you are able to verify that the upload was successful. This can be done with the show command:

- show vpn cert

[1] For more information regarding the creation of self-signed certificates please check https://www.lancom-systems.de/certificate-generation.



```
root@:/
> sh vpn cert

Certificate for application VPN1
Failure reading PKCS12 file /flash/security/vpn/vpn_pkcs12_int
Failure reading certificate /flash/security/vpn/vpn_devcert, no such file

Certificate for application VPN2
File /flash/security/vpn/vpn_pkcs12_int2 was read successfully

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            96:72:b5:64:5f:7e:07:09
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=router-22,OU=CC Tests,O=LANCOM Systems,C=DE
        Validity
            Not Before: Mar  1 18:18:53 2013 GMT
            Not After : Feb 27 18:18:53 2023 GMT
        Subject: CN=router-22,OU=CC Tests,O=LANCOM Systems,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:4a:82:24:94:ba:9a:31:c3:4b:8d:f7:06:43:
                    41:af:d9:50:48:dc:2b:ac:a2:73:40:0d:90:49:a5:
```

Additionally you must import the public key of each VPN peer. The public key is the certificate of the peer without the matching private key and must be used in the PKCS12 (*.p12) file format. When creating a public key for the distribution to other peers you must ensure the file does not include the private key. To import public keys from remote peers you must use the following command:

- LCS_PASSWORD="EnterCertificatePasswordHere" scp -o SendEnv=LCS_PASSWORD public_key_remote.p12 root@10.10.10.1:vpn_add_cas

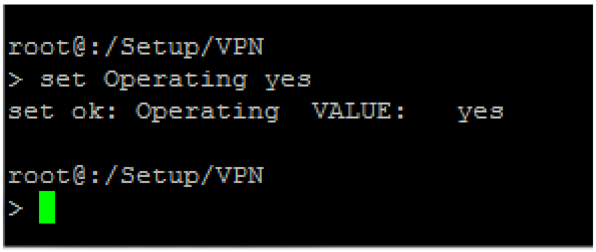
The command mentioned above can be used for each remote public key and will add new public keys to the set of accepted public keys. The previously imported public key will neither be deleted nor overwritten during that process. The set of accepted public keys can only be deleted collectively. It is not possible to delete individual public keys. To make sure existing public keys are securely erased you must use the "secure erase" command as mentioned in - 2.8.2 Secure Key Destruction.

## 2.6.10. VPN Site-to-Site Connection (Self-Signed Certificates)

To get started, you must upload your X.509 VPN certificate and public key of the remote peer as described in the previous chapter. To set up a VPN connection, switch to /Setup/VPN where you must activate the VPN module.

You must do this by typing the command:

- “set Operating yes”.



```
root@:/Setup/VPN
> set Operating yes
set ok: Operating  VALUE:   yes

root@:/Setup/VPN
> 
```

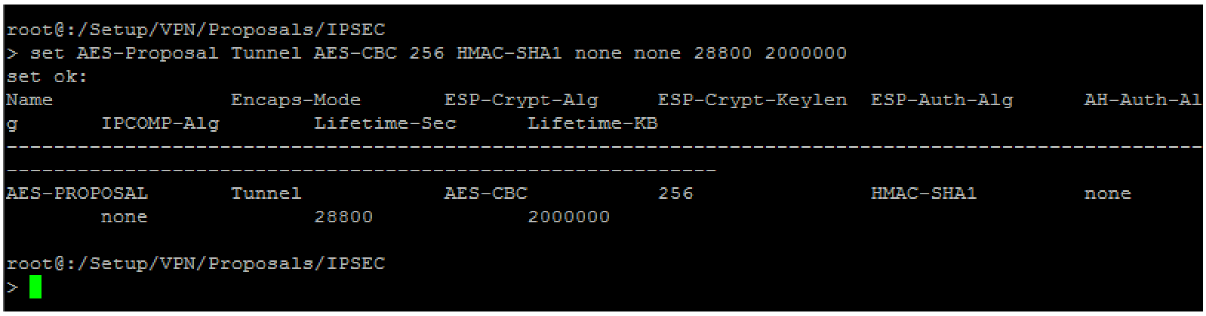
Then you must switch to /Setup/VPN/Proposals/IPSEC. Here you must define your IPsec proposal settings. There are several settings you must configure, such as Name, Encaps-Mode, ESP-Crypt-Alg, ESP-Crypt-Keylen, ESP-Auth-Alg, AH-Auth-Alg, IPCOMP-Alg, Lifetime-Sec and Lifetime-KB. Please only use AES Encryption and HMAC-SHA Authentication.

Available options are:

| ESP-Crypt-Algorithm | ESP-Crypt-Keylength | ESP-Authentication-Algorithm |
|---|---|---|
| **AES-CBC** | 128 | HMAC-SHA-1 |
| **AES-CBC** | 128 | HMAC-SHA-256 |
| **AES-CBC** | 192 | HMAC-SHA-1 |
| **AES-CBC** | 192 | HMAC-SHA-256 |
| **AES-CBC** | 256 | HMAC-SHA-1 |
| **AES-CBC** | 256 | HMAC-SHA-256 |

Here is an example of how a command might look like:

- “set AES-PROPOSAL Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000”



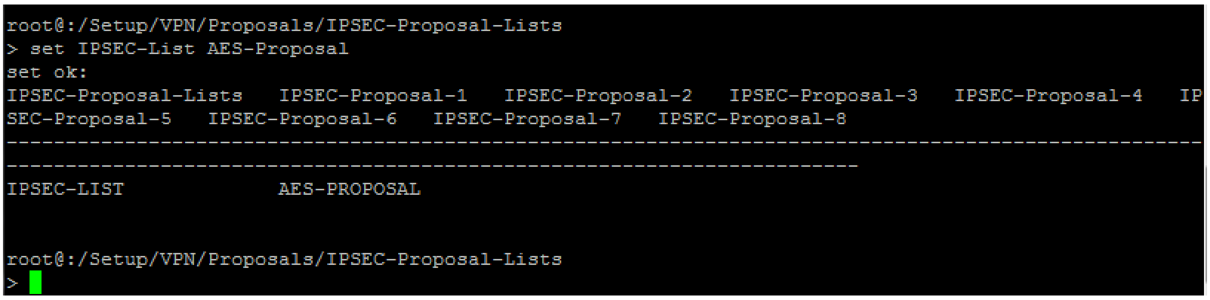
```
root@:/Setup/VPN/Proposals/IPSEC
> set AES-Proposal Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000
set ok:
Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-Auth-Alg      AH-Auth-Al
g       IPCOMP-Alg        Lifetime-Sec      Lifetime-KB
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------
AES-PROPOSAL       Tunnel            AES-CBC           256               HMAC-SHA1         none
        none              28800             2000000

root@:/Setup/VPN/Proposals/IPSEC
> 
```

Note: The Encaps-Mode mode must be set to “Tunnel”, the AH-Auth-Alg. must be set to “none” and the lifetimes must be set to 28800 sec / 2000000 KB.

Now an IPsec proposal has been created. To use it later on, we must put the proposal into a proposal list and give the list a name. This must be done in /Setup/VPN/Proposals/IPSEC-Proposal-Lists.

To add the created IPsec proposal to a new proposal list, you can type the following command:

- “set IPSEC-LIST AES-PROPOSAL”



```
root@:/Setup/VPN/Proposals/IPSEC-Proposal-Lists
> set IPSEC-List AES-Proposal
set ok:
IPSEC-Proposal-Lists   IPSEC-Proposal-1   IPSEC-Proposal-2   IPSEC-Proposal-3   IPSEC-Proposal-4   IP
SEC-Proposal-5   IPSEC-Proposal-6   IPSEC-Proposal-7   IPSEC-Proposal-8
----------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------
IPSEC-LIST             AES-PROPOSAL


root@:/Setup/VPN/Proposals/IPSEC-Proposal-Lists
> 
```

As you can see, there is now a new proposal list with the name “IPSEC-LIST” and the referenced IPsec proposal “AES-Proposal” we created above.

The next step is to create an IKE proposal, which must be done in /Setup/VPN/Proposals/IKE. It works very similar to the IPsec proposal configuration. You must give the proposal a name, set an IKE-Crypt-Algorithm etc. For secure operation make sure you only use AES Encryption and SHA Authentication.

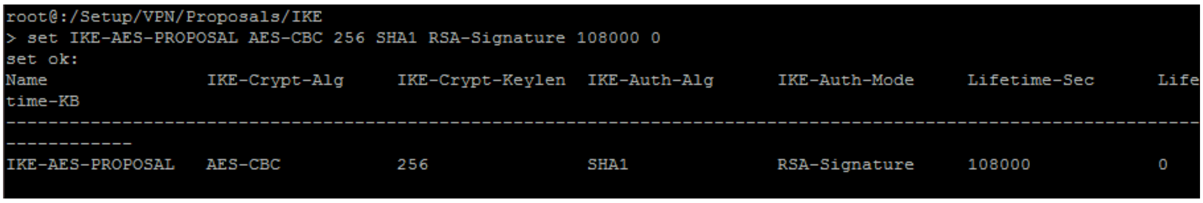
Available options are:

| IKE-Crypt-Algorithm | IKE-Crypt-Keylength | IKE-Auth-Algorithm |
|---|---|---|
| **AES-CBC** | 128 | SHA-1 |
| **AES-CBC** | 128 | SHA-256 |
| **AES-CBC** | 192 | SHA-1 |
| **AES-CBC** | 192 | SHA-256 |
| **AES-CBC** | 256 | SHA-1 |
| **AES-CBC** | 256 | SHA-256 |

will be checked by cctest

A possible command might be:

- “set IKE-AES-PROPOSAL AES-CBC 256 SHA1 RSA-Signature 108000 0”

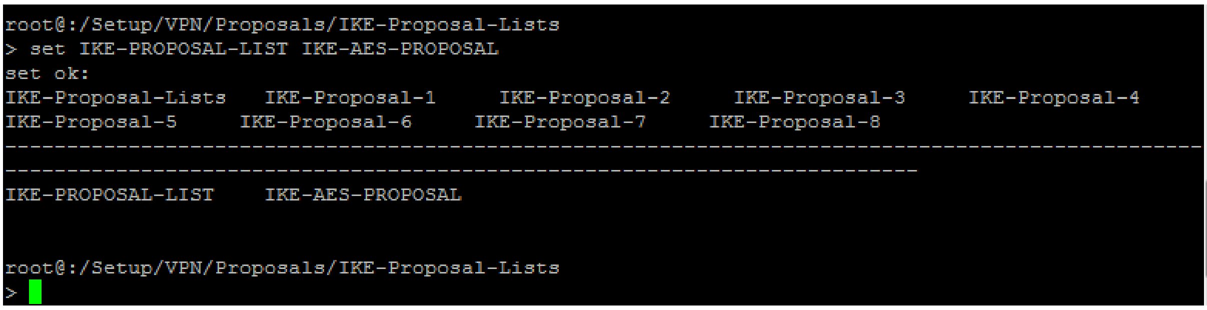


```
root@:/Setup/VPN/Proposals/IKE
> set IKE-AES-PROPOSAL AES-CBC 256 SHA1 RSA-Signature 108000 0
set ok:
Name              IKE-Crypt-Alg     IKE-Crypt-Keylen  IKE-Auth-Alg      IKE-Auth-Mode     Lifetime-Sec      Life
time-KB
------------------------------------------------------------------------------------------------------------------
------------
IKE-AES-PROPOSAL  AES-CBC           256               SHA1              RSA-Signature     108000            0
```

The now created IKE proposal must be added to an IKE-proposal-list, like we did with the IPsec proposal before. This must be done in /Setup/VPN/Proposals/IKE-Proposal-Lists.

A possible command might be:

- “set IKE-PROPOSAL-LIST IKE-AES-PROPOSAL”



```
root@:/Setup/VPN/Proposals/IKE-Proposal-Lists
> set IKE-PROPOSAL-LIST IKE-AES-PROPOSAL
set ok:
IKE-Proposal-Lists    IKE-Proposal-1     IKE-Proposal-2     IKE-Proposal-3     IKE-Proposal-4
IKE-Proposal-5     IKE-Proposal-6     IKE-Proposal-7     IKE-Proposal-8
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
IKE-PROPOSAL-LIST    IKE-AES-PROPOSAL


root@:/Setup/VPN/Proposals/IKE-Proposal-Lists
> 
```

Since we have our proposals for IKE and IPsec ready, the next thing to do is create a local and remote identity (distinguished name).

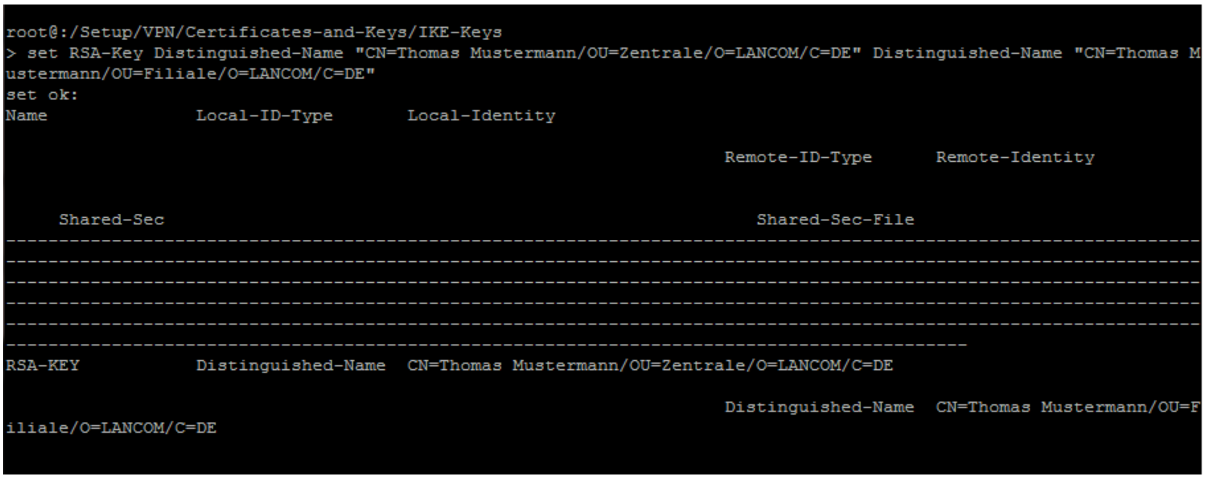
This must be done in /Setup/VPN/Certificates-and-Keys/IKE-Keys.

Here we need a name for the entry and local and remote identities like mentioned in your X.509 certificate.

A possible command might be:

- “set RSA-Key Distinguished-Name "CN=Thomas Mustermann/OU=Zentrale/O=LANCOM/C=DE" Distinguished-Name "CN=Thomas Mustermann/OU=Filiale/O=LANCOM/C=DE"

Please note that the Distinguished-Names are highlighted by “”. This is necessary when using spaces like in the common-name.



```
root@:/Setup/VPN/Certificates-and-Keys/IKE-Keys
> set RSA-Key Distinguished-Name "CN=Thomas Mustermann/OU=Zentrale/O=LANCOM/C=DE" Distinguished-Name "CN=Thomas M
ustermann/OU=Filiale/O=LANCOM/C=DE"
set ok:
Name                 Local-ID-Type       Local-Identity

                                                                    Remote-ID-Type      Remote-Identity


     Shared-Sec                                                        Shared-Sec-File
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
RSA-KEY              Distinguished-Name  CN=Thomas Mustermann/OU=Zentrale/O=LANCOM/C=DE

                                                                    Distinguished-Name  CN=Thomas Mustermann/OU=F
iliale/O=LANCOM/C=DE
```

The next step is to put this information into a VPN layer. This must be done in /Setup/VPN/Layer.

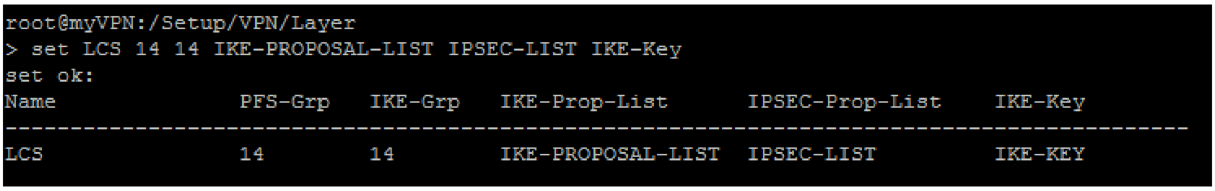
Here you must define the created proposals for IKE and IPsec, the just created RSA information and the IKE- and PFS-Groups (both Diffie-Hellman).

For secure operation make sure you only use Diffie-Hellman group 14 (2048 Bit). Available options are:

| PFS-Group (Diffie-Hellmann) | IKE-Group (Diffie-Hellmann) |
|---|---|
| 14 (2048 Bit) | 14 (2048 Bit) |

A possible command would be:

- “set LCS 14 14 IKE-PROPOSAL-LIST IPSEC-LIST IKE-Key”

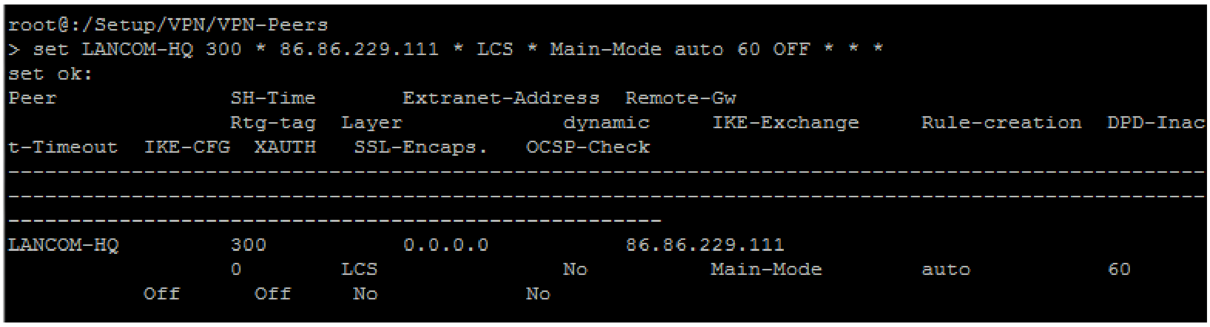


```
root@myVPN:/Setup/VPN/Layer
> set LCS 14 14 IKE-PROPOSAL-LIST IPSEC-LIST IKE-Key
set ok:
Name              PFS-Grp   IKE-Grp   IKE-Prop-List      IPSEC-Prop-List    IKE-Key
-------------------------------------------------------------------------------------------
LCS               14        14        IKE-PROPOSAL-LIST  IPSEC-LIST         IKE-KEY
```

With this newly created VPN-Layer, we are able to add a VPN-Peer. This must be done in /Setup/VPN/VPN-Peers. Available options are: Peer-Name, Short-hold-time, Extranet-Address, Remote-Gateway-Address, Routing-tag, Layer, IKE-Exchange, Rule-Creation, DPD-Timeout and IKE-cfg-mode

A possible command might be:

- “set LANCOM-HQ 300 * 86.86.229.111 * LCS * Main-Mode auto 60 OFF * * *”

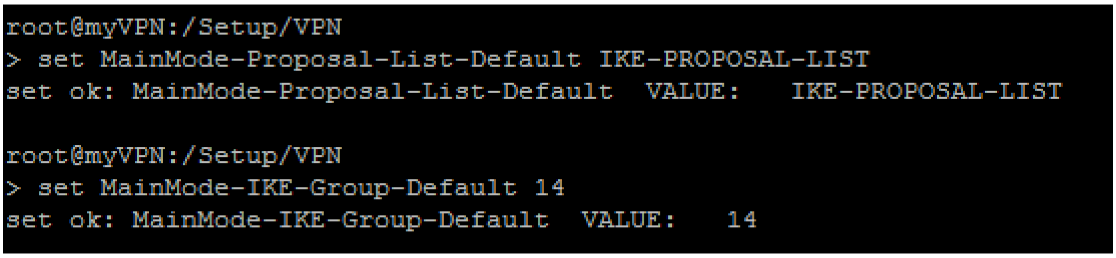


```
root@:/Setup/VPN/VPN-Peers
> set LANCOM-HQ 300 * 86.86.229.111 * LCS * Main-Mode auto 60 OFF * * *
set ok:
Peer              SH-Time       Extranet-Address  Remote-Gw
                  Rtg-tag  Layer             dynamic     IKE-Exchange     Rule-creation  DPD-Inac
t-Timeout  IKE-CFG  XAUTH   SSL-Encaps.   OCSP-Check
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
LANCOM-HQ         300           0.0.0.0           86.86.229.111
                  0        LCS               No          Main-Mode        auto           60
           Off      Off     No            No
```

To allow incoming Main Mode connections, we must set default values. This must be done in /Setup/VPN. The IKE-Group-Default (Diffie-Hellman) value must be the same as chosen above.

Possible commands might be:

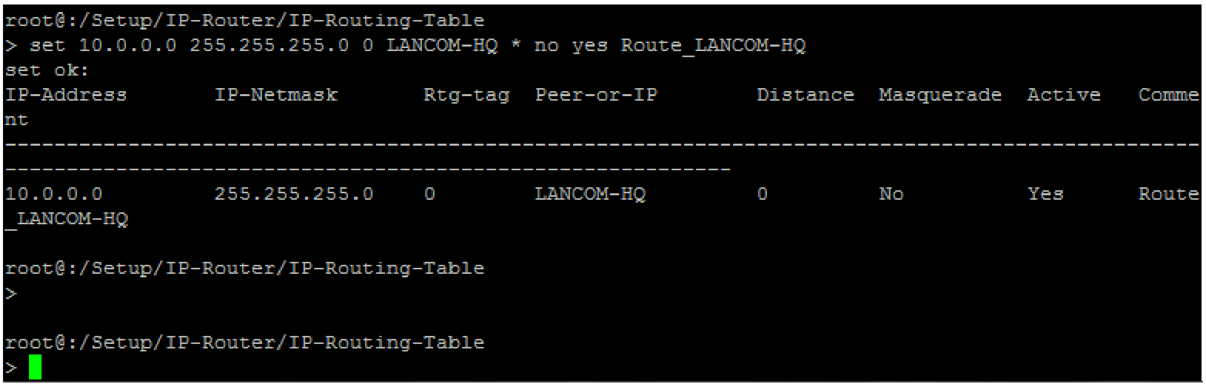
- “set MainMode-Proposal-List-Default IKE-PROPOSAL-LIST”
- “set MainMode-IKE-Group-Default 14”



```
root@myVPN:/Setup/VPN
> set MainMode-Proposal-List-Default IKE-PROPOSAL-LIST
set ok: MainMode-Proposal-List-Default  VALUE:   IKE-PROPOSAL-LIST

root@myVPN:/Setup/VPN
> set MainMode-IKE-Group-Default 14
set ok: MainMode-IKE-Group-Default  VALUE:   14
```

The last remaining step is to set the destination network in the IP-routing-table. This must be done in: /Setup/IP-Router/IP-Routing-Table. Here you must set the network details of your remote network. A possible command might be:

- “set 10.0.0.0 255.255.255.0 0 LANCOM-HQ * no yes Route_LANCOM-HQ”



```
root@:/Setup/IP-Router/IP-Routing-Table
> set 10.0.0.0 255.255.255.0 0 LANCOM-HQ * no yes Route_LANCOM-HQ
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active   Comme
nt
-------------------------------------------------------------------------------------------------
-----------------------------------------------------------
10.0.0.0         255.255.255.0    0        LANCOM-HQ         0         No          Yes      Route
_LANCOM-HQ

root@:/Setup/IP-Router/IP-Routing-Table
>

root@:/Setup/IP-Router/IP-Routing-Table
> 
```

Now we are all set and able to establish a secure VPN site-to-site connection via self-signed certificates.

## 2.6.11. VPN Site-to-Host Connection (Self-Signed Certificates)

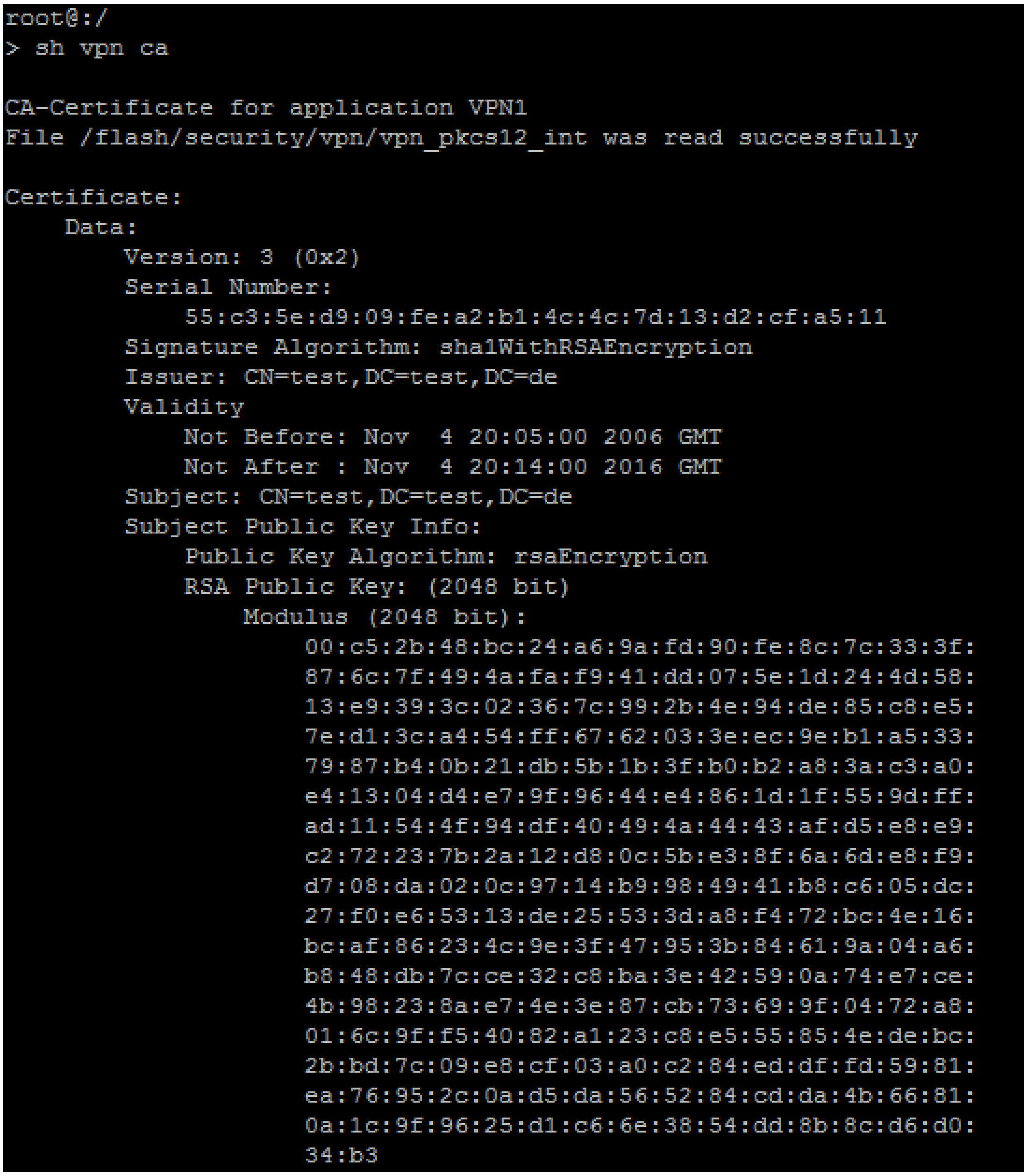
To get started, you first must upload your X.509 VPN certificate. Please make sure you have your VPN certificate in a PKCS12 file format (*.p12) with all necessary information ready.

To upload your certificate, you must use a secure copy client (e.g. Cygwin SCP). The command to upload the file would be:

- LCS_PASSWORD="EnterCertificatePasswordHere" scp -o SendEnv=LCS_PASSWORD vpn.p12 root@10.10.10.1:vpn_pkcs12

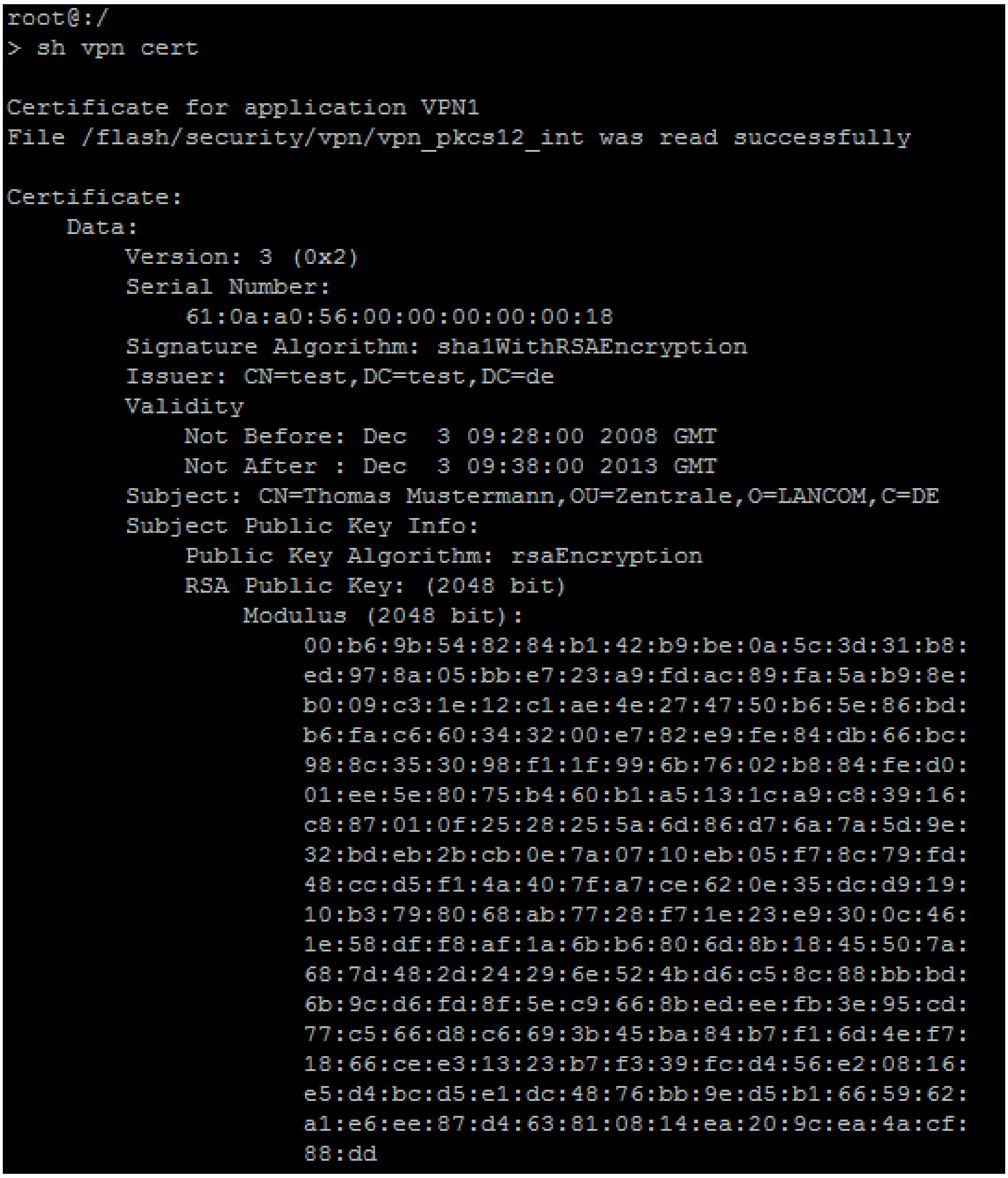
Once this is done, you are able to verify that the upload was successful. This can be done with two show commands.

- show vpn ca (shows the VPN Root Certificate)



```
root@:/
> sh vpn ca

CA-Certificate for application VPN1
File /flash/security/vpn/vpn_pkcs12_int was read successfully

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:c3:5e:d9:09:fe:a2:b1:4c:4c:7d:13:d2:cf:a5:11
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=test,DC=test,DC=de
        Validity
            Not Before: Nov  4 20:05:00 2006 GMT
            Not After : Nov  4 20:14:00 2016 GMT
        Subject: CN=test,DC=test,DC=de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:c5:2b:48:bc:24:a6:9a:fd:90:fe:8c:7c:33:3f:
                    87:6c:7f:49:4a:fa:f9:41:dd:07:5e:1d:24:4d:58:
                    13:e9:39:3c:02:36:7c:99:2b:4e:94:de:85:c8:e5:
                    7e:d1:3c:a4:54:ff:67:62:03:3e:ec:9e:b1:a5:33:
                    79:87:b4:0b:21:db:5b:1b:3f:b0:b2:a8:3a:c3:a0:
                    e4:13:04:d4:e7:9f:96:44:e4:86:1d:1f:55:9d:ff:
                    ad:11:54:4f:94:df:40:49:4a:44:43:af:d5:e8:e9:
                    c2:72:23:7b:2a:12:d8:0c:5b:e3:8f:6a:6d:e8:f9:
                    d7:08:da:02:0c:97:14:b9:98:49:41:b8:c6:05:dc:
                    27:f0:e6:53:13:de:25:53:3d:a8:f4:72:bc:4e:16:
                    bc:af:86:23:4c:9e:3f:47:95:3b:84:61:9a:04:a6:
                    b8:48:db:7c:ce:32:c8:ba:3e:42:59:0a:74:e7:ce:
                    4b:98:23:8a:e7:4e:3e:87:cb:73:69:9f:04:72:a8:
                    01:6c:9f:f5:40:82:a1:23:c8:e5:55:85:4e:de:bc:
                    2b:bd:7c:09:e8:cf:03:a0:c2:84:ed:df:fd:59:81:
                    ea:76:95:2c:0a:d5:da:56:52:84:cd:da:4b:66:81:
                    0a:1c:9f:96:25:d1:c6:6e:38:54:dd:8b:8c:d6:d0:
                    34:b3
```

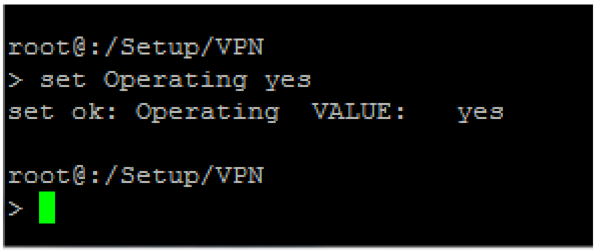
- show vpn cert (shows the VPN Device Certificate)



```
root@:/
> sh vpn cert

Certificate for application VPN1
File /flash/security/vpn/vpn_pkcs12_int was read successfully

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:0a:a0:56:00:00:00:00:00:18
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=test,DC=test,DC=de
        Validity
            Not Before: Dec  3 09:28:00 2008 GMT
            Not After : Dec  3 09:38:00 2013 GMT
        Subject: CN=Thomas Mustermann,OU=Zentrale,O=LANCOM,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b6:9b:54:82:84:b1:42:b9:be:0a:5c:3d:31:b8:
                    ed:97:8a:05:bb:e7:23:a9:fd:ac:89:fa:5a:b9:8e:
                    b0:09:c3:1e:12:c1:ae:4e:27:47:50:b6:5e:86:bd:
                    b6:fa:c6:60:34:32:00:e7:82:e9:fe:84:db:66:bc:
                    98:8c:35:30:98:f1:1f:99:6b:76:02:b8:84:fe:d0:
                    01:ee:5e:80:75:b4:60:b1:a5:13:1c:a9:c8:39:16:
                    c8:87:01:0f:25:28:25:5a:6d:86:d7:6a:7a:5d:9e:
                    32:bd:eb:2b:cb:0e:7a:07:10:eb:05:f7:8c:79:fd:
                    48:cc:d5:f1:4a:40:7f:a7:ce:62:0e:35:dc:d9:19:
                    10:b3:79:80:68:ab:77:28:f7:1e:23:e9:30:0c:46:
                    1e:58:df:f8:af:1a:6b:b6:80:6d:8b:18:45:50:7a:
                    68:7d:48:2d:24:29:6e:52:4b:d6:c5:8c:88:bb:bd:
                    6b:9c:d6:fd:8f:5e:c9:66:8b:ed:ee:fb:3e:95:cd:
                    77:c5:66:d8:c6:69:3b:45:ba:84:b7:f1:6d:4e:f7:
                    18:66:ce:e3:13:23:b7:f3:39:fc:d4:56:e2:08:16:
                    e5:d4:bc:d5:e1:dc:48:76:bb:9e:d5:b1:66:59:62:
                    a1:e6:ee:87:d4:63:81:08:14:ea:20:9c:ea:4a:cf:
                    88:dd
```

To get started, you must switch to /Setup/VPN. There you must activate the VPN module. You must do this by typing the command:

- “set Operating yes”.



```
root@:/Setup/VPN
> set Operating yes
set ok: Operating  VALUE:   yes

root@:/Setup/VPN
> 
```

Then you must switch to /Setup/VPN/Proposals/IPSEC. Here you must define your IPsec proposal settings. There are several settings you must configure, such as Name, Encaps-Mode, ESP-Crypt-Alg, ESP-Crypt-Keylen, ESP-Auth-Alg, AH-Auth-Alg, IPCOMP-Alg, Lifetime-Sec and Lifetime-KB. Please only use AES Encryption and HMAC-SHA Authentication.

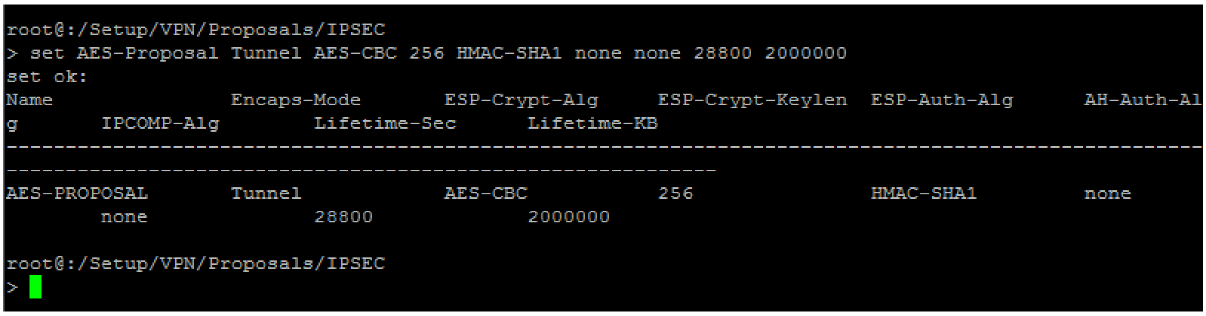
Available options are:

| ESP-Crypt-Algorithm | ESP-Crypt-Keylength | ESP-Authentication-Algorithm |
|---|---|---|
| **AES-CBC** | 128 | HMAC-SHA-1 |
| **AES-CBC** | 128 | HMAC-SHA-256 |
| **AES-CBC** | 192 | HMAC-SHA-1 |
| **AES-CBC** | 192 | HMAC-SHA-256 |
| **AES-CBC** | 256 | HMAC-SHA-1 |
| **AES-CBC** | 256 | HMAC-SHA-256 |

will be checked by cctest

Here is an example of how a command might look like:

- “set AES-PROPOSAL Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000”



```
root@:/Setup/VPN/Proposals/IPSEC
> set AES-Proposal Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000
set ok:
Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-Auth-Alg      AH-Auth-Al
g       IPCOMP-Alg        Lifetime-Sec      Lifetime-KB
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------
AES-PROPOSAL       Tunnel            AES-CBC           256               HMAC-SHA1         none
        none              28800             2000000

root@:/Setup/VPN/Proposals/IPSEC
>
```

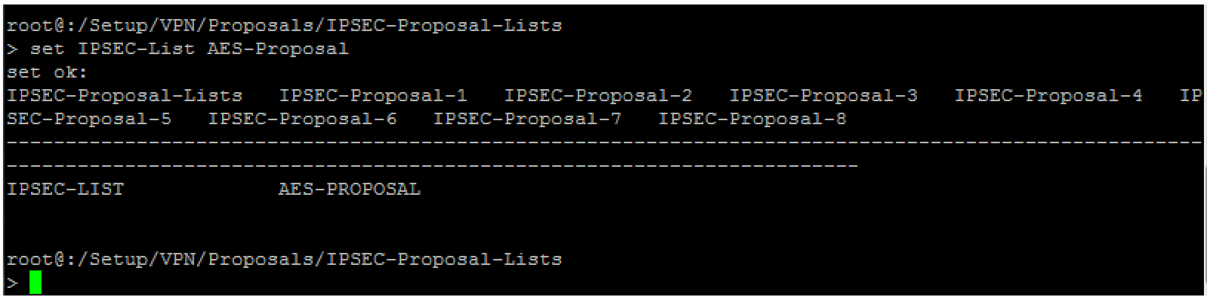
Note: The Encaps-Mode mode must be set to “Tunnel”, the AH-Auth-Alg. must be set to “none” and the lifetimes must be set to 28800 sec / 2000000 KB.

Now an IPsec proposal has been created. To use it later on, we must put the proposal into a proposal list and give the list a name. This must be done in /Setup/VPN/Proposals/IPSEC-Proposal-Lists.

To add the created IPsec proposal to a new proposal list, you can type the following command:

- “set IPSEC-LIST AES-PROPOSAL”

will be checked by cctest



```
root@:/Setup/VPN/Proposals/IPSEC-Proposal-Lists
> set IPSEC-List AES-Proposal
set ok:
IPSEC-Proposal-Lists   IPSEC-Proposal-1   IPSEC-Proposal-2   IPSEC-Proposal-3   IPSEC-Proposal-4   IP
SEC-Proposal-5   IPSEC-Proposal-6   IPSEC-Proposal-7   IPSEC-Proposal-8
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------------------
IPSEC-LIST             AES-PROPOSAL


root@:/Setup/VPN/Proposals/IPSEC-Proposal-Lists
>
```

As you can see, there is now a new proposal list with the name “IPSEC-LIST” and the referenced IPsec proposal “AES-Proposal” we created above.

The next step is to create an IKE proposal, which must be done in /Setup/VPN/Proposals/IKE. It works very similar to the IPsec proposal configuration. Again you must give the proposal a name, set an IKE-Crypt-Algorithm etc. For secure operation only use AES Encryption and SHA Authentication.

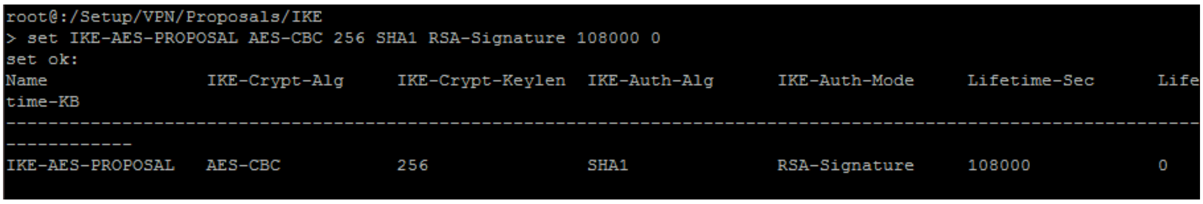
Available options are:

will be checked by cctest

| IKE-Crypt-Algorithm | IKE-Crypt-Keylength | IKE-Auth-Algorithm |
|---|---|---|
| **AES-CBC** | 128 | SHA-1 |
| **AES-CBC** | 128 | SHA-256 |
| **AES-CBC** | 192 | SHA-1 |
| **AES-CBC** | 192 | SHA-256 |
| **AES-CBC** | 256 | SHA-1 |
| **AES-CBC** | 256 | SHA-256 |

A possible command might be:

- “set IKE-AES-PROPOSAL AES-CBC 256 SHA1 RSA-Signature 108000 0”

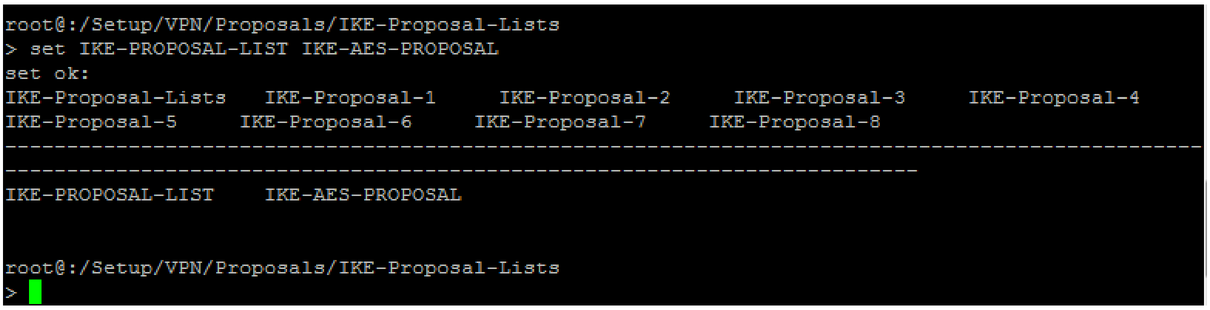


```
root@:/Setup/VPN/Proposals/IKE
> set IKE-AES-PROPOSAL AES-CBC 256 SHA1 RSA-Signature 108000 0
set ok:
Name                IKE-Crypt-Alg     IKE-Crypt-Keylen  IKE-Auth-Alg      IKE-Auth-Mode     Lifetime-Sec      Life
time-KB
--------------------------------------------------------------------------------------------------------------------
------------
IKE-AES-PROPOSAL    AES-CBC           256               SHA1              RSA-Signature     108000            0
```

The now created IKE proposal must be added to an IKE-proposal-list, like we did with the IPsec proposal. This must be done in /Setup/VPN/Proposals/IKE-Proposal-Lists.

A possible command might be:

- “set IKE-PROPOSAL-LIST IKE-AES-PROPOSAL”



```
root@:/Setup/VPN/Proposals/IKE-Proposal-Lists
> set IKE-PROPOSAL-LIST IKE-AES-PROPOSAL
set ok:
IKE-Proposal-Lists    IKE-Proposal-1      IKE-Proposal-2      IKE-Proposal-3      IKE-Proposal-4
IKE-Proposal-5      IKE-Proposal-6      IKE-Proposal-7      IKE-Proposal-8
------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
IKE-PROPOSAL-LIST     IKE-AES-PROPOSAL


root@:/Setup/VPN/Proposals/IKE-Proposal-Lists
>
```

Since we have our proposals for IKE and IPsec ready, the next thing to do is create a local and remote identity (distinguished name).

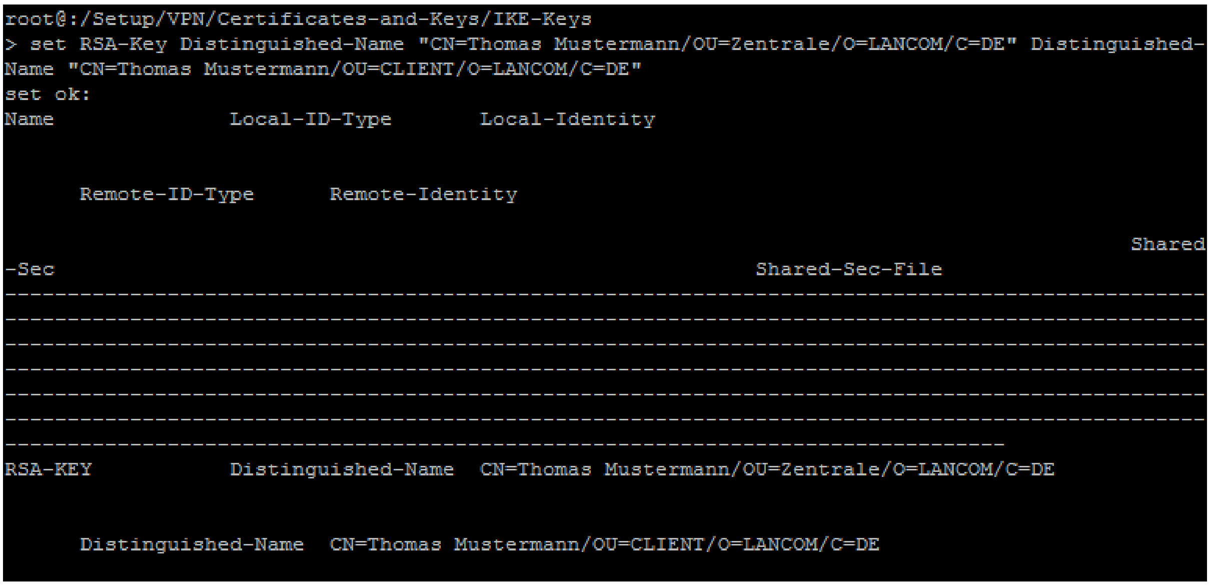
This must be done in /Setup/VPN/Certificates-and-Keys/IKE-Keys.

Here we need a name for the entry and local and remote identities like mentioned in your X.509 certificate.

A possible command might be:

- “set RSA-Key Distinguished-Name "CN=Thomas Mustermann/OU=Zentrale/O=LANCOM/C=DE" Distinguished-Name "CN=Thomas Mustermann/OU=CLIENT/O=LANCOM/C=DE"

Please note that the Distinguished-Names are highlighted by “”. This is necessary when using spaces like in the common-name.



```
root@:/Setup/VPN/Certificates-and-Keys/IKE-Keys
> set RSA-Key Distinguished-Name "CN=Thomas Mustermann/OU=Zentrale/O=LANCOM/C=DE" Distinguished-
Name "CN=Thomas Mustermann/OU=CLIENT/O=LANCOM/C=DE"
set ok:
Name              Local-ID-Type       Local-Identity


      Remote-ID-Type      Remote-Identity

                                                                                          Shared
-Sec                                                        Shared-Sec-File
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
RSA-KEY           Distinguished-Name  CN=Thomas Mustermann/OU=Zentrale/O=LANCOM/C=DE


      Distinguished-Name  CN=Thomas Mustermann/OU=CLIENT/O=LANCOM/C=DE
```

The next step is to put this information into a VPN layer. This must be done in /Setup/VPN/Layer.

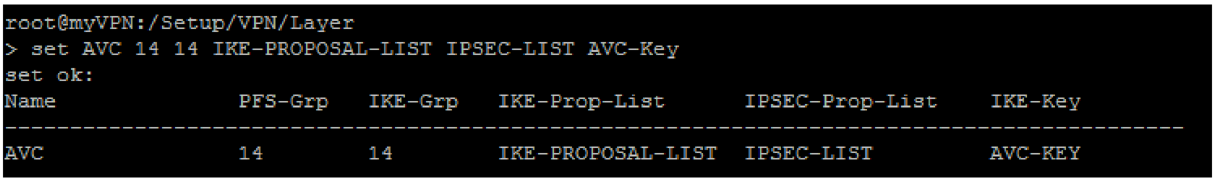
Here you must define the created proposals for IKE and IPsec, the just created IKE-Key and the IKE- and PFS-Groups (both Diffie-Hellman).

For secure operation make sure you only use Diffie-Hellman group 14 (2048 Bit). Available options are:

| PFS-Group (Diffie-Hellmann) | IKE-Group (Diffie-Hellmann) |
|---|---|
| 14 (2048 Bit) | 14 (2048 Bit) |

A possible command would be:

- “set AVC 14 14 IKE-PROPOSAL-LIST IPSEC-LIST AVC-Key”

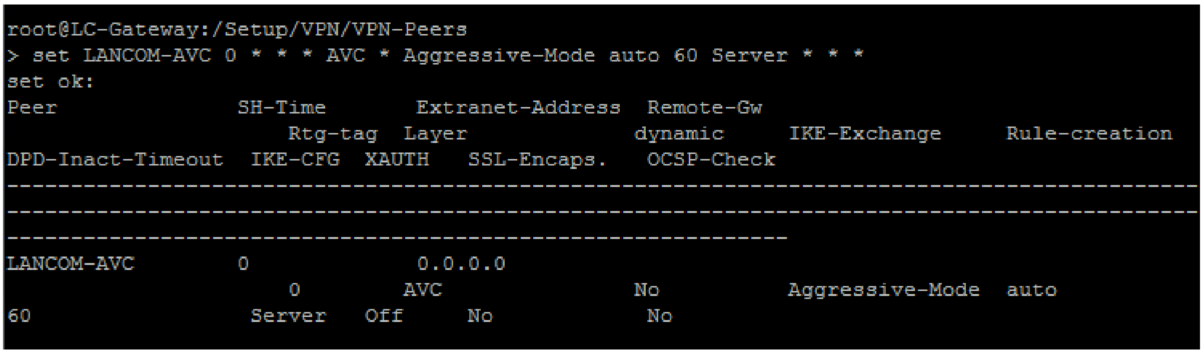


```
root@myVPN:/Setup/VPN/Layer
> set AVC 14 14 IKE-PROPOSAL-LIST IPSEC-LIST AVC-Key
set ok:
Name              PFS-Grp   IKE-Grp   IKE-Prop-List      IPSEC-Prop-List    IKE-Key
-------------------------------------------------------------------------------------------
AVC               14        14        IKE-PROPOSAL-LIST  IPSEC-LIST         AVC-KEY
```

With this newly created VPN-Layer, we are able to add a VPN-Peer. This must be done in /Setup/VPN/VPN-Peers. Available options are: Peer-Name, Short-hold-time, Extranet-Address, Remote-Gateway-Address, Routing-tag, Layer, IKE-Exchange, Rule-Creation, DPD-Timeout and IKE-cfg-mode

A possible command might be:

- “set LANCOM-AVC 0 * * * AVC * Main-Mode auto 60 Server * * *”

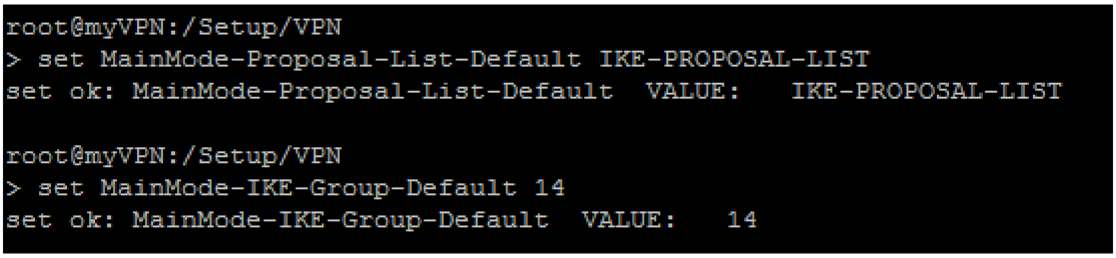


```
root@LC-Gateway:/Setup/VPN/VPN-Peers
> set LANCOM-AVC 0 * * * AVC * Aggressive-Mode auto 60 Server * * *
set ok:
Peer                 SH-Time        Extranet-Address  Remote-Gw
                     Rtg-tag  Layer             dynamic      IKE-Exchange     Rule-creation
DPD-Inact-Timeout  IKE-CFG  XAUTH   SSL-Encaps.   OCSP-Check
---------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------
-------------------------------------------------------------
LANCOM-AVC           0              0.0.0.0
                     0        AVC               No           Aggressive-Mode  auto
60                   Server   Off      No              No
```

To allow incoming Main Mode connections, we must set default values. This must be done in /Setup/VPN. The IKE-Group-Default (Diffie-Hellman) value must be the same as chosen above.

Possible commands might be:

- “set MainMode-Proposal-List-Default IKE-PROPOSAL-LIST”
- “set MainMode-IKE-Group-Default 14”

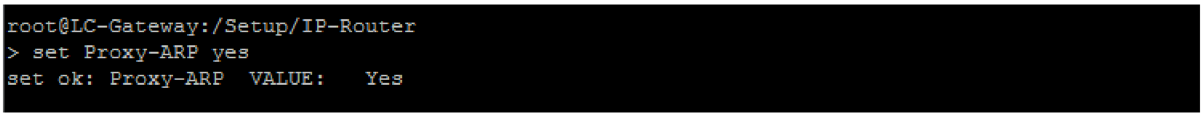


```
root@myVPN:/Setup/VPN
> set MainMode-Proposal-List-Default IKE-PROPOSAL-LIST
set ok: MainMode-Proposal-List-Default  VALUE:   IKE-PROPOSAL-LIST

root@myVPN:/Setup/VPN
> set MainMode-IKE-Group-Default 14
set ok: MainMode-IKE-Group-Default  VALUE:   14
```

When using site-to-host connections, it is necessary to activate ProxyARP. This must be done in /Setup/IP-Router.

You must activate ProxyARP with the following command:

- “set Proxy-ARP yes”

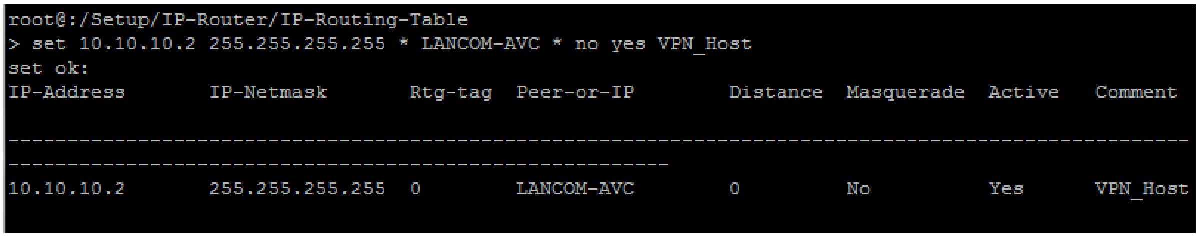


```
root@LC-Gateway:/Setup/IP-Router
> set Proxy-ARP yes
set ok: Proxy-ARP  VALUE:   Yes
```

The last remaining step is to set an IP address for this host. This must be done in: /Setup/IP-Router/IP-Routing-Table. ***If you like to use the automatic address assignment, you can skip this step and use an address range like mentioned in the next step.***

A possible command might be:

- “set 10.10.10.2 255.255.255.255 * LANCOM-AVC * no yes VPN_Host”

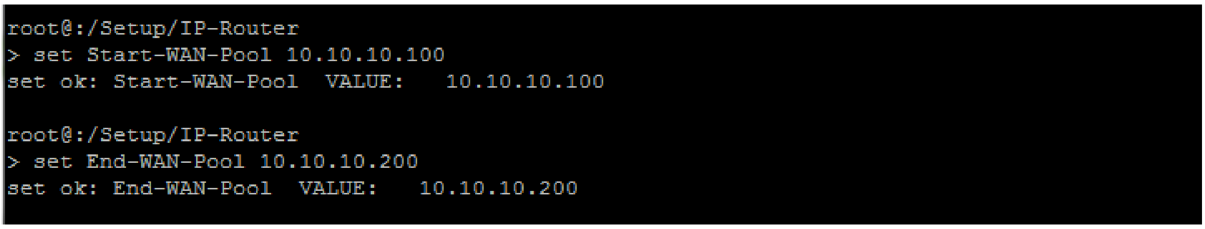


```
root@:/Setup/IP-Router/IP-Routing-Table
> set 10.10.10.2 255.255.255.255 * LANCOM-AVC * no yes VPN_Host
set ok:
IP-Address       IP-Netmask       Rtg-tag  Peer-or-IP        Distance  Masquerade  Active   Comment

----------------------------------------------------------------------------------------------------
--------------------------------------------------------
10.10.10.2       255.255.255.255  0        LANCOM-AVC        0         No          Yes      VPN_Host
```

*If you like to use the automatic address assignment*, you must set an address range in: /Setup/IP-Router

Possible commands might be:

- “set Start-WAN-Pool 10.10.10.100”
- “set End-WAN-Pool 10.10.10.200”



```
root@:/Setup/IP-Router
> set Start-WAN-Pool 10.10.10.100
set ok: Start-WAN-Pool  VALUE:   10.10.10.100

root@:/Setup/IP-Router
> set End-WAN-Pool 10.10.10.200
set ok: End-WAN-Pool  VALUE:   10.10.10.200
```

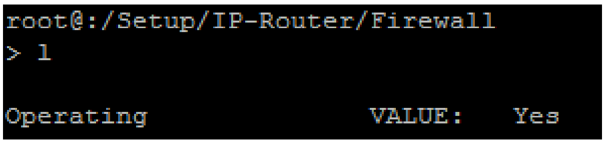
Now we are all set and able to allow incoming VPN host connections via Public-Key-Infrastructure.

## 2.6.12. Applying Firewall Rules

At first, please make sure the firewall is activated. This must be checked in /Setup/IP-Router/Firewall

If necessary, the command to activate the firewall would be:

- “set Operating yes”

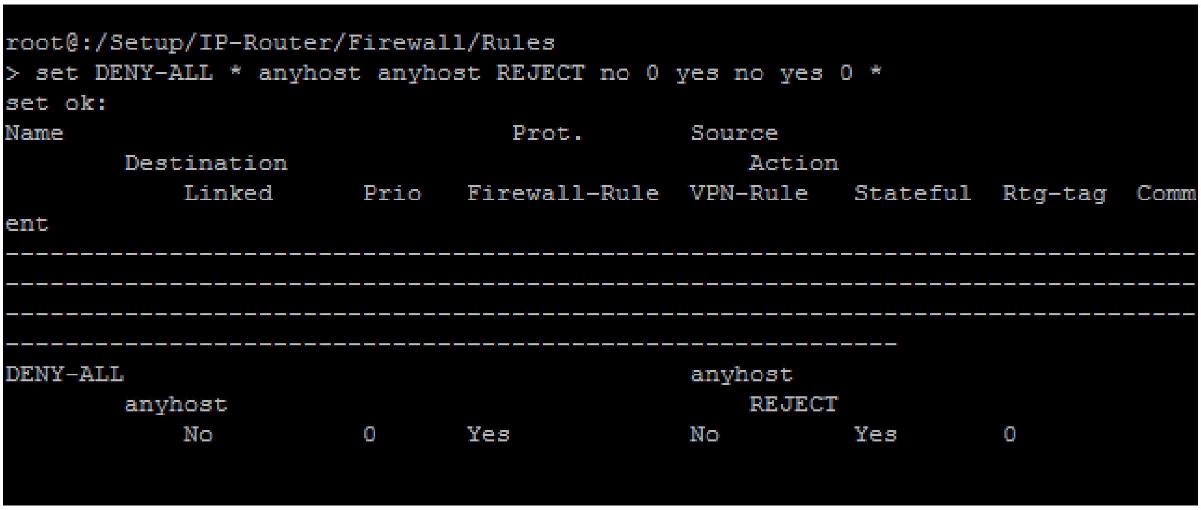


```
root@:/Setup/IP-Router/Firewall
> l

Operating                VALUE:    Yes
```

To create a firewall rule go to /Setup/IP-Router/Firewall/Rules. Here you can create firewall rules if needed. It is recommended to start with creating a DENY-ALL rule at first and then only allow traffic, which must be allowed.

A DENY-ALL Rule must be created with the command:

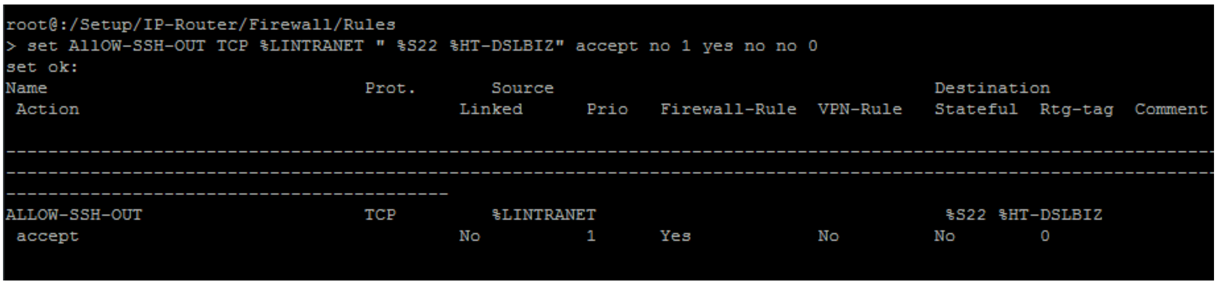
- “set DENY-ALL * anyhost anyhost REJECT no 0 yes no yes 0 *”



```
root@:/Setup/IP-Router/Firewall/Rules
> set DENY-ALL * anyhost anyhost REJECT no 0 yes no yes 0 *
set ok:
Name                              Prot.       Source
        Destination                               Action
            Linked      Prio   Firewall-Rule  VPN-Rule   Stateful  Rtg-tag  Comm
ent
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------------------------
DENY-ALL                                      anyhost
        anyhost                                   REJECT
            No          0      Yes            No         Yes       0
```

To create a firewall rule that only allows outgoing SSH connections (via T-DSLBIZ) from the source INTRANET use this command:

- “set ALLOW-SSH-OUT TCP %LINTRANET " %S22 %HT-DSLBIZ" accept no 1 yes no no 0”



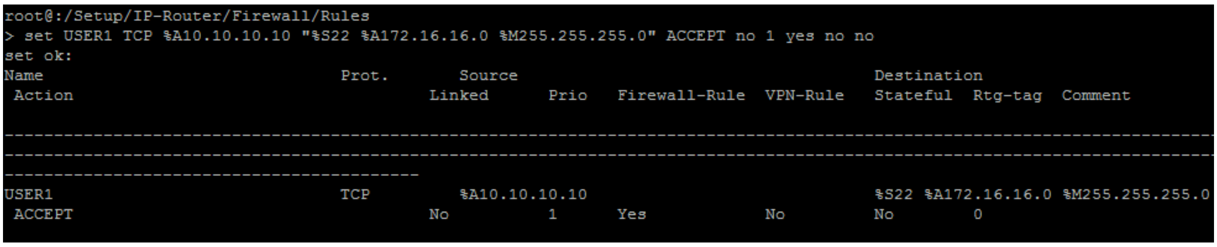
```
root@:/Setup/IP-Router/Firewall/Rules
> set AllOW-SSH-OUT TCP %LINTRANET " %S22 %HT-DSLBIZ" accept no 1 yes no no 0
set ok:
Name                              Prot.       Source                                  Destination
 Action                                   Linked      Prio   Firewall-Rule  VPN-Rule   Stateful  Rtg-tag  Comment

------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------
------------------------------------------
ALLOW-SSH-OUT                     TCP         %LINTRANET                                 %S22 %HT-DSLBIZ
 accept                                   No          1      Yes            No         No        0
```

If you need a firewall rule for one host (10.10.10.10) to connect to a remote network (172.16.16.0/24) with the use of SSHv2, the command would be:

- “set USER1 TCP %A10.10.10.10 "SSH %A172.16.16.0 %M255.255.255.0" ACCEPT no 1 yes no no”

  or

- “set USER1 TCP %A10.10.10.10 "%S22 %A172.16.16.0 %M255.255.255.0" ACCEPT no 1 yes no no”



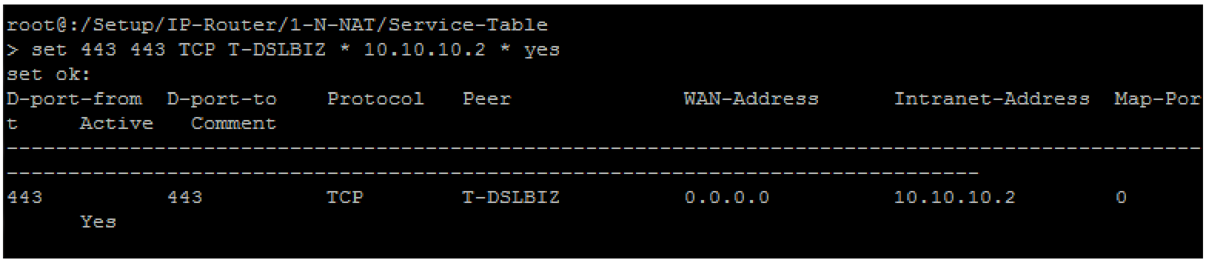
```
root@:/Setup/IP-Router/Firewall/Rules
> set USER1 TCP %A10.10.10.10 "%S22 %A172.16.16.0 %M255.255.255.0" ACCEPT no 1 yes no no
set ok:
Name                              Prot.       Source                                  Destination
 Action                                   Linked      Prio   Firewall-Rule  VPN-Rule   Stateful  Rtg-tag  Comment

------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------
------------------------------------------
USER1                             TCP         %A10.10.10.10                           %S22 %A172.16.16.0 %M255.255.255.0
 ACCEPT                                   No          1      Yes            No         No        0
```

## 2.6.13. Using the Port-Forwarding

The port-forwarding can be configured in /Setup/IP-Router/1-N-Nat/Service-Table. Here you can configure the forwarding of source ports to internal clients. For example, if you want to reach the HTTPS interface of an internal host from WAN, you must forward TCP port 443 to the internal client.

An appropriate command would be:

- “set 443 443 TCP T-DSLBIZ * 10.10.10.2 * yes”



```
root@:/Setup/IP-Router/1-N-NAT/Service-Table
> set 443 443 TCP T-DSLBIZ * 10.10.10.2 * yes
set ok:
D-port-from  D-port-to    Protocol   Peer              WAN-Address      Intranet-Address  Map-Por
t      Active   Comment
--------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
443          443          TCP        T-DSLBIZ          0.0.0.0          10.10.10.2        0
      Yes
```

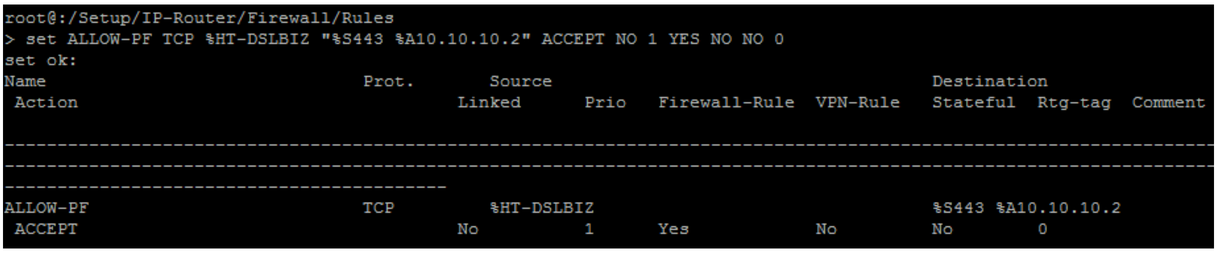
Now the client 10.10.10.2 will be reachable from WAN (T-DSLBIZ) on Port 443. Please notice that if you use a Deny-All firewall strategy like recommended above, you must create a firewall rule which allows this incoming connection. Otherwise the firewall will block any connection.

An appropriate command would be:

- “set ALLOW-PF TCP %HT-DSLBIZ "%S443 %A10.10.10.2" ACCEPT NO 1 YES NO NO 0”

or

- “set ALLOW-PF ANY %HT-DSLBIZ "HTTPS %A10.10.10.2" ACCEPT NO 1 YES NO NO 0”



```
root@:/Setup/IP-Router/Firewall/Rules
> set ALLOW-PF TCP %HT-DSLBIZ "%S443 %A10.10.10.2" ACCEPT NO 1 YES NO NO 0
set ok:
Name                              Prot.       Source                                  Destination
 Action                                    Linked      Prio   Firewall-Rule  VPN-Rule   Stateful  Rtg-tag  Comment

-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
------------------------------------------
ALLOW-PF                          TCP         %HT-DSLBIZ                              %S443 %A10.10.10.2
 ACCEPT                                    No          1      Yes            No         No        0
```

For further information regarding the firewall settings and port-forwarding table, please check (2.8.10 - Firewall) and (2.8.9.4 - Service table) of the LCOS-MENU-860-EN.pdf.

## 2.7. Events

If the device crashes, the administrator can get more information using to the command-line to run the command “show bootlog”. With this information, he must contact LANCOM Systems Support (http://www.lancom.eu/).

The administrator must check SYSLOG messages (/Status/TCP-IP/Syslog/Last-Messages) daily. If the administrator recognizes warning or error messages, he must use the trace functionality as described in 2.3 to obtain further information and has to manually save the logs as mentioned in the next section (2.8 - Recommendation for secure usage of the TOE).

## 2.8. Recommendation for Secure Usage of the TOE

To make sure, the device is configured for secure usage with the TOE check the following setup settings of your device.

The activation of the following features is not allowed:

- Public Spot
- Content-Filter
- Fax-Gateway
- WLC-6 option

If necessary, you must reset your configuration by running the command “default –r”, when you are in the top level directory “/”. This will reset the router configuration and set LCOS default values which are outside of the evaluated configuration. To change the configuration so that it conforms to the restrictions for the evaluated configuration, you must run the command “ccset”.

With every system boot, the LANCOM operating system checks the configuration for compliance to the recommended configuration. It will trigger a syslog message with the information that “The current configuration is CC compliant” or “The following configuration items are not CC compliant”. If your configuration is not CC compliant, you will get information about the command-line path and the value which is not compliant (syslog).

When connected to the command line, you are able to run the command “cctest” which will do the same. If your configuration is not CC compliant, you will get information about the command-line path and the value which is not compliant directly in your command-line. The administrator must check if the current configuration is CC compliant with every configuration change (by running cctest). Configuration items which are checked by “cctest” are also highlighted with this icon:

will be checked by cctest

Some commands mentioned in (2.5 Method of invocation) must not be used:

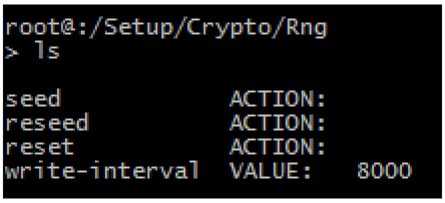
| | |
|---|---|
| Loadconfig | Not available since the use of TFTP / HTTPS protocols is not allowed and excluded from the TOE. |
| Loadfirmware | Not available since using of TFTP / HTTPS protocols is not allowed and excluded from the TOE. |
| Loadscript | Not available since using of TFTP / HTTPS protocols is not allowed and excluded from the TOE. |
| Testmail | As mentioned in this section (2.8 – Recommendation for secure usage of the TOE) E-Mail / SMTP must be deactivated. Therefore, this command must not be used. |
| Writeflash | Not available since the use of the TFTP protocol is not allowed and excluded from the TOE. |

- Ll2mdetect — As mentioned in this section (2.8 – Recommendation for secure usage of the TOE), LL2M must be deactivated. Therefore, this command must not be used.
- Ll2mexec — As mentioned in this section (2.8 – Recommendation for secure usage of the TOE), LL2M must be deactivated. Therefore, this command must not be used.
- sshkeygen — The use of the rsa / dsa key generator is not allowed and excluded from the TOE.
- ssh — The use of the internal SSH client is not allowed and excluded from the TOE.

### 2.8.1. Decommissioning the TOE

Destroying the state of the random number generator is only allowed when placing the TOE out of order (note that this will fully destroy the internal state of the random number generator). This must be done in:

- /Setup/Crypto/Rng/
  - "do reset"



```
root@:/Setup/Crypto/Rng
> ls

seed              ACTION:
reseed            ACTION:
reset             ACTION:
write-interval    VALUE:    8000
```

You must also delete the cryptographic keys as described in 2.8.2 Secure Key Destruction. It is mandatory to destroy the random number generator state (first) and delete the cryptographic keys (second) in this exact order.

### 2.8.2. Secure Key Destruction

This section describes how cryptographic keys and certificates must be securely deleted when they are no longer used, for example if the TOE is retired at the end of its use period. When cryptographic keys and certificates are replaced by overwriting them with new cryptographic keys or certificates, the last step must be performed to ensure that the old keys are securely deleted.

- /Status/File-System/Contents

To manually delete the locally saved SSH-key or VPN certificate, the administrator must run the following delete commands.

Delete the SSH key:

- "del ssh_rsakey"

Delete VPN certificate in slot "2" (certificates in other slots are deleted in an analogous manner):

- "del vpn_pkcs12_int2"

Delete public keys of all VPN peers simultaneously:

- "del vpn_add_cas"

*To securely delete these files, the next step must also be completed.*

- /Status/File-System/

The administrator of the TOE must run:

- "do Secure-Erase flash"

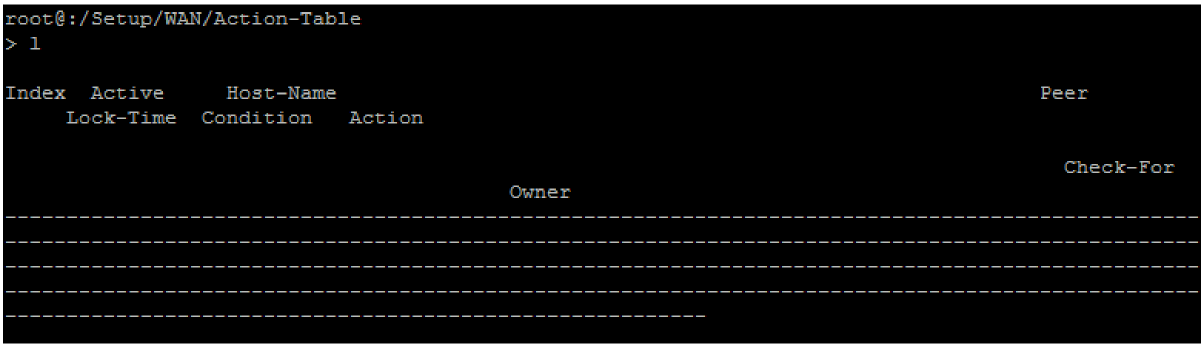
### 2.8.3. Required Configuration Settings

The limitations mentioned below are mandatory to operate the TOE in a evaluated configuration. They result from the limited scope of the evaluation where non-essential modules were disabled. Other restrictions are required to only allow secure algorithms, e.g. by limiting the evaluated configuration to AES rather than allowing alternatives which are considered to be cryptographically weak.

The action-table must only be used with “exec:” commands as described in LCOS-MENU-860-EN.pdf (2.2.25 - Action table). Any other usage is not allowed.

will be checked by cctest

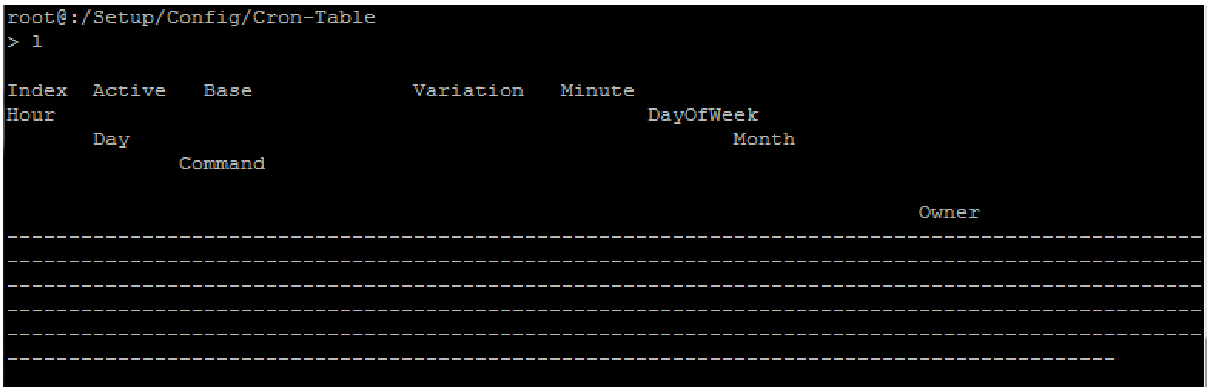
- /Setup/WAN/Action-Table



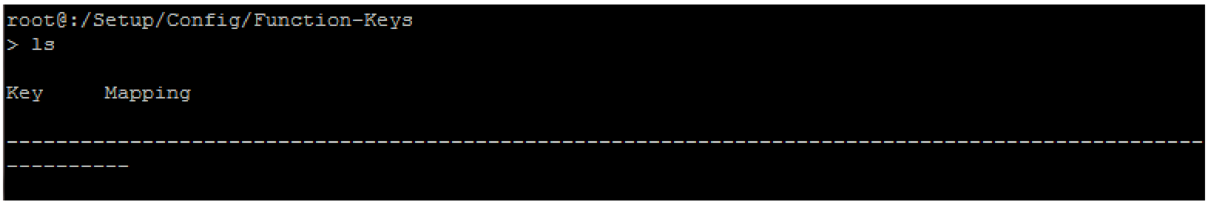
```
root@:/Setup/WAN/Action-Table
> l

Index   Active     Host-Name                                                        Peer
     Lock-Time  Condition   Action

                                                                                      Check-For
                                         Owner
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
---------------------------------------------------------
```

The following tables must only be used with commands which are allowed to the administrator to operate the TOE in a secure manner as described in this section (2.8 - Recommendation for secure usage of the TOE):

- /Setup/Config/Cron-Table
- /Setup/Config/Function-Keys



```
root@:/Setup/Config/Cron-Table
> l

Index  Active   Base             Variation   Minute
Hour                                                DayOfWeek
       Day                                                 Month
              Command

                                                                          Owner
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

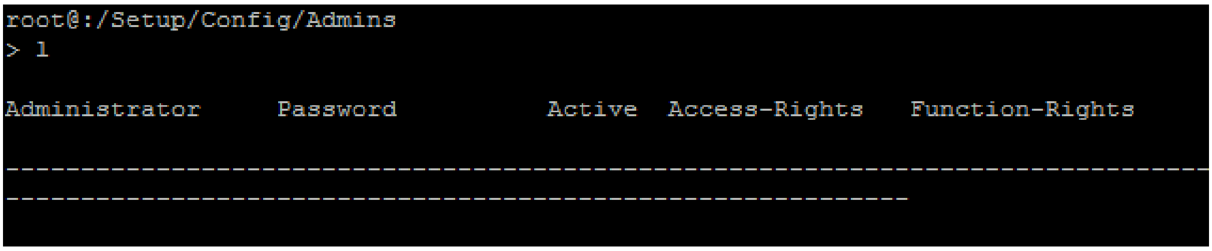


```
root@:/Setup/Config/Function-Keys
> ls

Key     Mapping

-------------------------------------------------------------------------------------------------
----------
```

- /Setup/Config/Admins

Since there is only one user role defined (i.e. ”root”) the admin table must be left empty.

will be checked by cctest

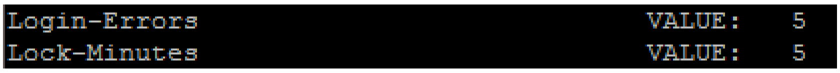


```
root@:/Setup/Config/Admins
> l

Administrator      Password          Active   Access-Rights    Function-Rights

------------------------------------------------------------------------------
------------------------------------------------------------
```

- /Setup/Config

Please make sure that the lock minutes and login-errors are not deactivated (i.e. have the values “0”). The value for login-errors must be between 5-10 and the lock-minutes must be at least 5. The default value for both settings is “5”.

will be checked by cctest

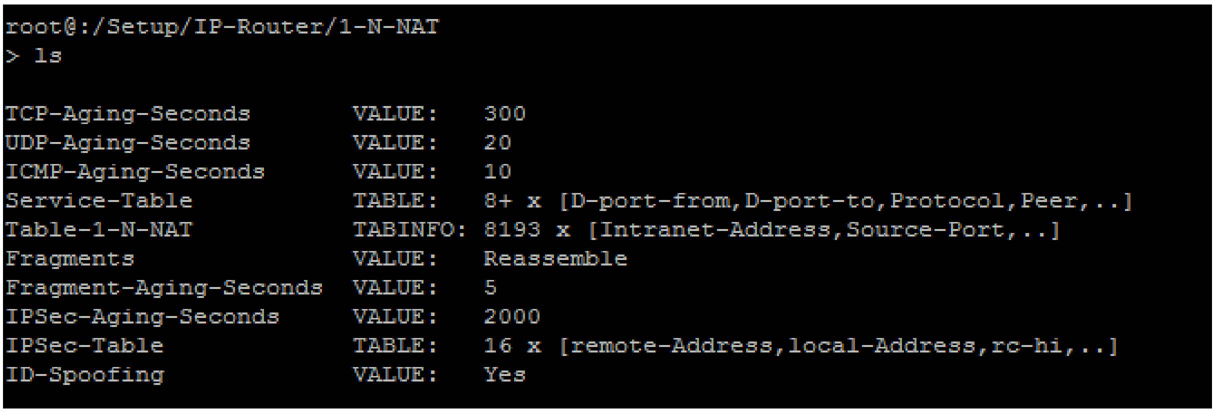


```
Login-Errors                                  VALUE:    5
Lock-Minutes                                  VALUE:    5
```

- /Setup/IP-Router/1-N-NAT

Some attacks from the Internet try to outsmart the firewall by fragmented packets (packets split into several small units). One of the main features of the firewall is the ability to reassemble fragmented packets in order to check afterwards the entire IP packet. Please make sure that the “Fragments” setting is set to “Reassemble”. No other setting must be used here.

will be checked by cctest



```
root@:/Setup/IP-Router/1-N-NAT
> ls

TCP-Aging-Seconds        VALUE:    300
UDP-Aging-Seconds        VALUE:    20
ICMP-Aging-Seconds       VALUE:    10
Service-Table            TABLE:    8+ x [D-port-from,D-port-to,Protocol,Peer,..]
Table-1-N-NAT            TABINFO:  8193 x [Intranet-Address,Source-Port,..]
Fragments                VALUE:    Reassemble
Fragment-Aging-Seconds   VALUE:    5
IPSec-Aging-Seconds      VALUE:    2000
IPSec-Table              TABLE:    16 x [remote-Address,local-Address,rc-hi,..]
ID-Spoofing              VALUE:    Yes
```

- /Setup/IP-Router/Firewall/Rules

When creating firewall rules, make sure the stateful setting is set to “no”.

will be checked by cctest

- /Setup/IP-Router/Firewall/Actions

When creating firewall rules or actions, make sure QoS, bandwidth reservation, fragmentation and PMTU are neither activated nor used.

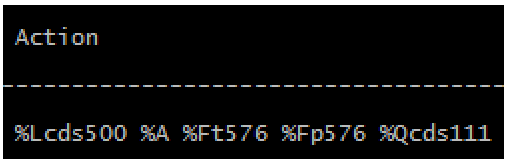
will be checked by cctest

%L (for bandwidth reservation)

%Q (for Quality of Service)

%Ft (for fragmentation)

%Fp (for PMTU)



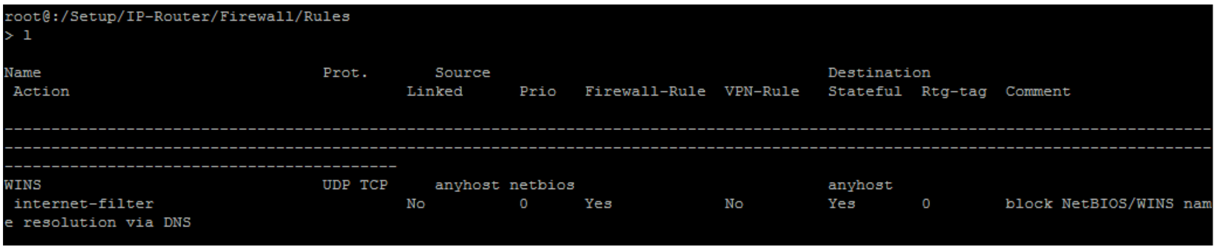
```
Action
------------------------------------
%Lcds500 %A %Ft576 %Fp576 %Qcds111
```

Note: If you run the “ccset” command, every firewall rule which is not compliant to these secure usage requirements will be deleted.

- /Setup/IP-Router/Firewall/Rules

The default rule “WINS” must be deleted.

will be checked by cctest



```
root@:/Setup/IP-Router/Firewall/Rules
> l

Name                              Prot.       Source                                     Destination
 Action                                     Linked      Prio   Firewall-Rule  VPN-Rule    Stateful  Rtg-tag  Comment

----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
------------------------------------------
WINS                              UDP TCP     anyhost netbios                            anyhost
 internet-filter                           No          0      Yes            No          Yes       0        block NetBIOS/WINS nam
e resolution via DNS
```

- /Setup/IP-Router/Firewall/Rules

No “Action” column of any firewall rule must contain actions beginning with %XcCF.

will be checked by cctest

- /Setup/IP-Router/Firewall/Actions

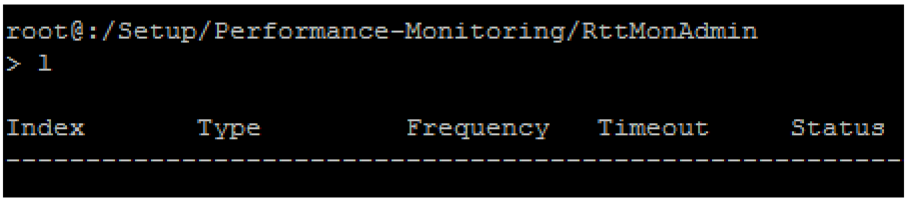
No “Description” column of any firewall action must contain actions beginning with %XcCF.

will be checked by cctest

- /Setup/Performance-Monitoring/Admin

The Performance-Monitoring table has to be empty.

will be checked by cctest

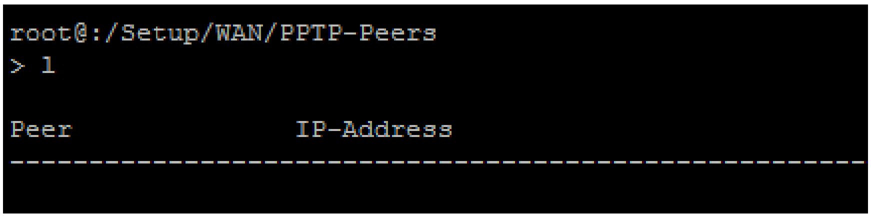


```
root@:/Setup/Performance-Monitoring/RttMonAdmin
> l

Index       Type         Frequency   Timeout     Status
--------------------------------------------------------
```

- /Setup/WAN/PPTP-Peers

To make sure, no PPTP connection is possible, this table must be empty.

will be checked by cctest

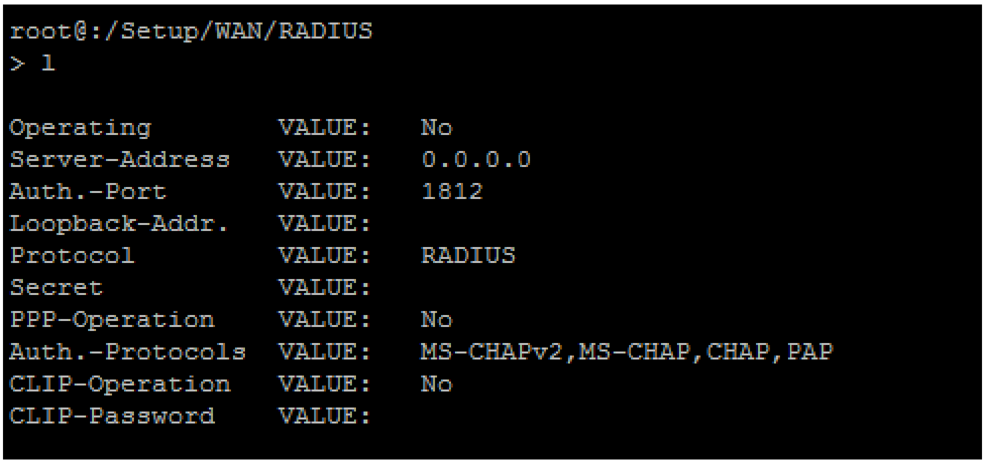


```
root@:/Setup/WAN/PPTP-Peers
> l

Peer              IP-Address
-------------------------------------------------------
```

- /Setup/WAN/Radius

For secure operation deactivate the radius service by setting the Operating value to “no”.

will be checked by cctest

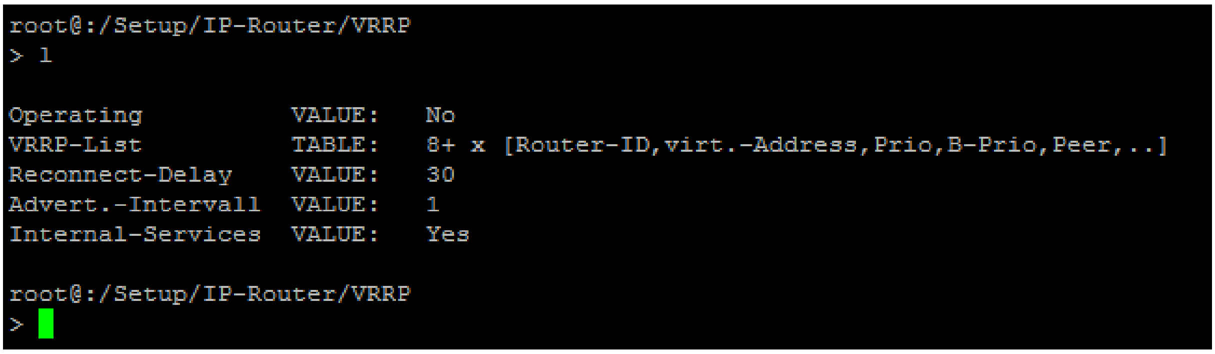


```
root@:/Setup/WAN/RADIUS
> l

Operating         VALUE:   No
Server-Address    VALUE:   0.0.0.0
Auth.-Port        VALUE:   1812
Loopback-Addr.    VALUE:
Protocol          VALUE:   RADIUS
Secret            VALUE:
PPP-Operation     VALUE:   No
Auth.-Protocols   VALUE:   MS-CHAPv2,MS-CHAP,CHAP,PAP
CLIP-Operation    VALUE:   No
CLIP-Password     VALUE:
```

- /Setup/IP-Router/VRRP

To make sure, that the VRRP service is not running, the value of Operating must be set to “No”:

will be checked by cctest

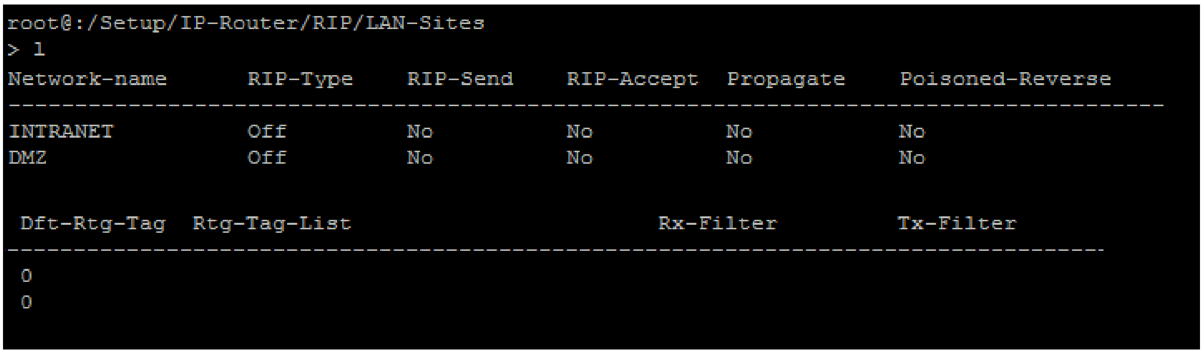


```
root@:/Setup/IP-Router/VRRP
> l

Operating          VALUE:   No
VRRP-List          TABLE:   8+ x [Router-ID,virt.-Address,Prio,B-Prio,Peer,..]
Reconnect-Delay    VALUE:   30
Advert.-Intervall  VALUE:   1
Internal-Services  VALUE:   Yes

root@:/Setup/IP-Router/VRRP
> 
```

- /Setup/IP-Router/RIP/LAN-Sites

To make sure, you are using LAN-RIP in a secure manner, either turn RIP off (RIP-Type “Off”) or use RIP-2 with RIP-Send enabled and RIP-Accept disabled. This way, the route propagation is enabled and the route learning is disabled.

will be checked by cctest

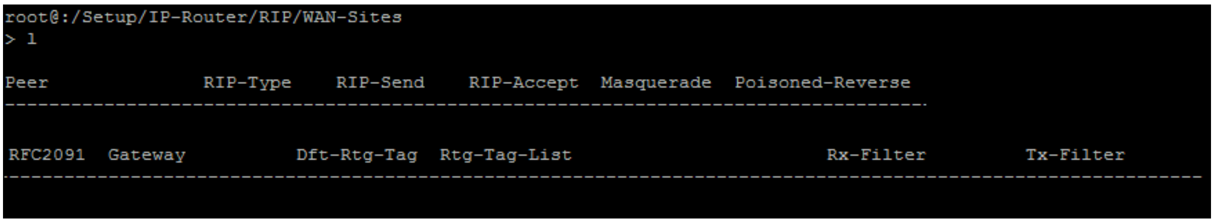


```
root@:/Setup/IP-Router/RIP/LAN-Sites
> l
Network-name      RIP-Type    RIP-Send    RIP-Accept  Propagate    Poisoned-Reverse
---------------------------------------------------------------------------------------
INTRANET          Off         No          No          No           No
DMZ               Off         No          No          No           No


 Dft-Rtg-Tag  Rtg-Tag-List                      Rx-Filter         Tx-Filter
-----------------------------------------------------------------------------------
 0
 0
```

- /Setup/IP-Router/RIP/WAN-Sites

Make sure WAN-RIP is turned off (no table entry).

will be checked by cctest

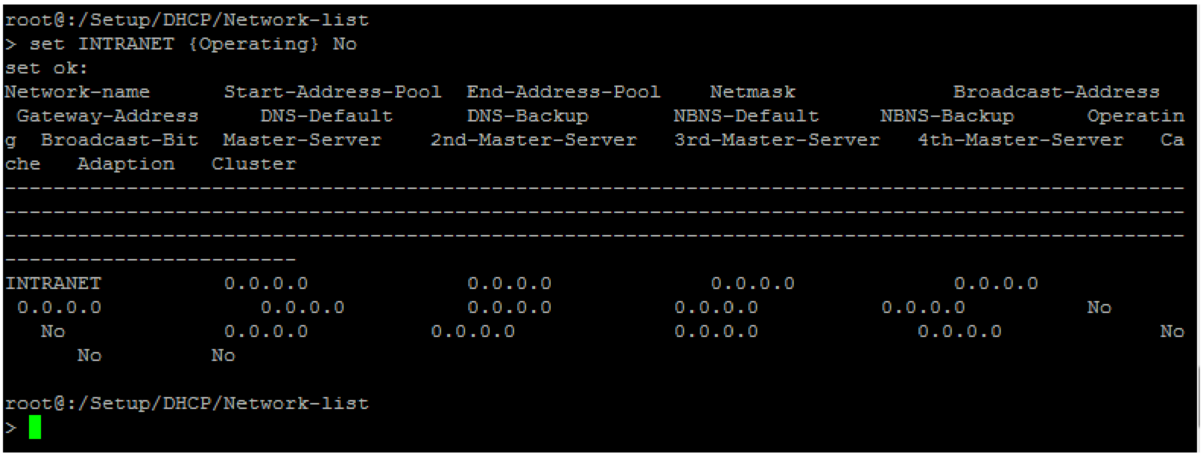


```
root@:/Setup/IP-Router/RIP/WAN-Sites
> l

Peer              RIP-Type    RIP-Send    RIP-Accept  Masquerade  Poisoned-Reverse
-----------------------------------------------------------------------------------

RFC2091  Gateway          Dft-Rtg-Tag  Rtg-Tag-List                       Rx-Filter         Tx-Filter
------------------------------------------------------------------------------------------------------------
```

- /Setup/DHCP/Network-List

DHCP must be deactivated for all networks.

will be checked by cctest

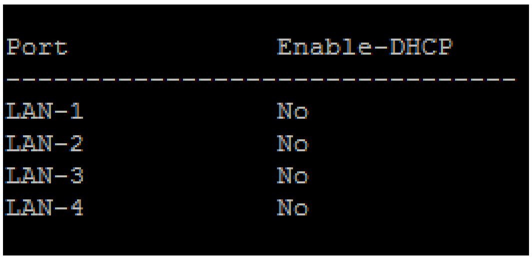


```
root@:/Setup/DHCP/Network-list
> set INTRANET {Operating} No
set ok:
Network-name      Start-Address-Pool  End-Address-Pool    Netmask             Broadcast-Address
 Gateway-Address     DNS-Default      DNS-Backup       NBNS-Default     NBNS-Backup      Operatin
g  Broadcast-Bit  Master-Server    2nd-Master-Server   3rd-Master-Server   4th-Master-Server   Ca
che   Adaption   Cluster
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
------------------------
INTRANET          0.0.0.0             0.0.0.0             0.0.0.0             0.0.0.0
 0.0.0.0             0.0.0.0          0.0.0.0          0.0.0.0          0.0.0.0          No
   No             0.0.0.0          0.0.0.0             0.0.0.0             0.0.0.0             No
      No         No

root@:/Setup/DHCP/Network-list
> 
```

- /Setup/DHCP/Ports

DHCP must be deactivated on all ports.

will be checked by cctest

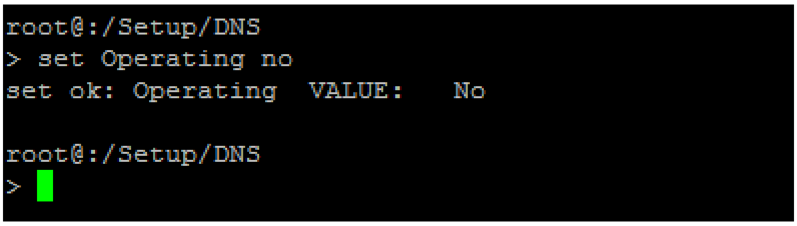


```
Port             Enable-DHCP
---------------------------------
LAN-1            No
LAN-2            No
LAN-3            No
LAN-4            No
```

- /Setup/DNS

DNS must be deactivated.

will be checked by cctest

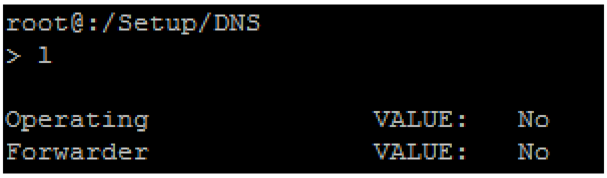


```
root@:/Setup/DNS
> set Operating no
set ok: Operating  VALUE:   No

root@:/Setup/DNS
> 
```

- /Setup/DNS

The DNS forwarder must also be deactivated.

will be checked by cctest

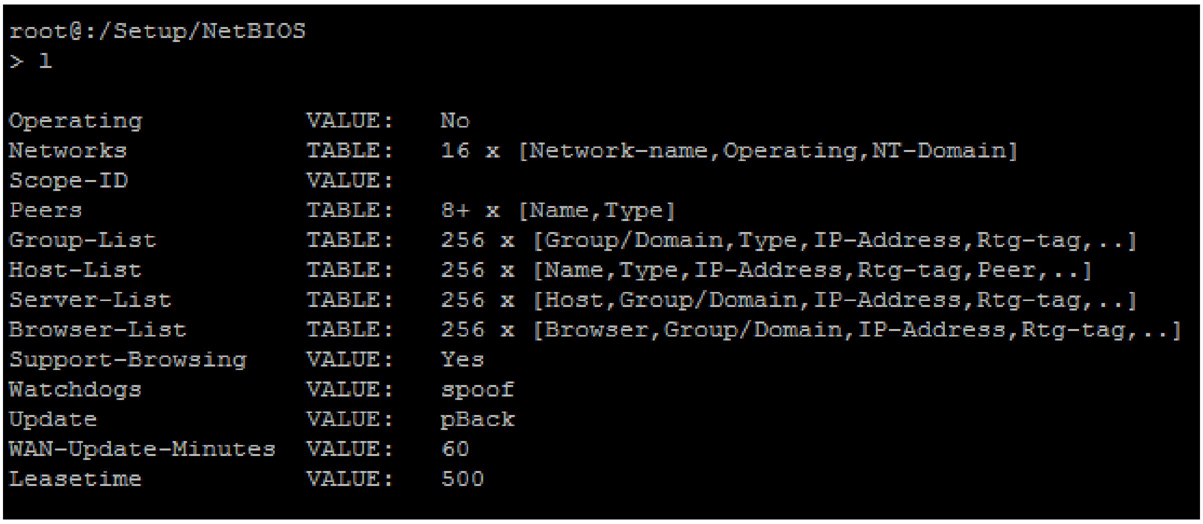


```
root@:/Setup/DNS
> l

Operating                VALUE:    No
Forwarder                VALUE:    No
```

- /Setup/NetBIOS

NetBIOS must also be deactivated. You must do this by setting the value of Operating to “no”.

will be checked by cctest

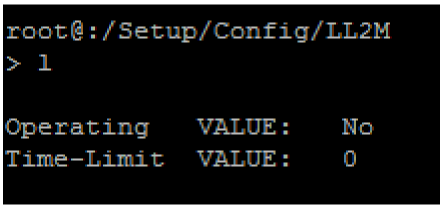


```
root@:/Setup/NetBIOS
> l

Operating            VALUE:    No
Networks             TABLE:    16 x [Network-name,Operating,NT-Domain]
Scope-ID             VALUE:
Peers                TABLE:    8+ x [Name,Type]
Group-List           TABLE:    256 x [Group/Domain,Type,IP-Address,Rtg-tag,..]
Host-List            TABLE:    256 x [Name,Type,IP-Address,Rtg-tag,Peer,..]
Server-List          TABLE:    256 x [Host,Group/Domain,IP-Address,Rtg-tag,..]
Browser-List         TABLE:    256 x [Browser,Group/Domain,IP-Address,Rtg-tag,..]
Support-Browsing     VALUE:    Yes
Watchdogs            VALUE:    spoof
Update               VALUE:    pBack
WAN-Update-Minutes   VALUE:    60
Leasetime            VALUE:    500
```

- /Setup/Config/LL2M

LL2M must be deactivated.

will be checked by cctest

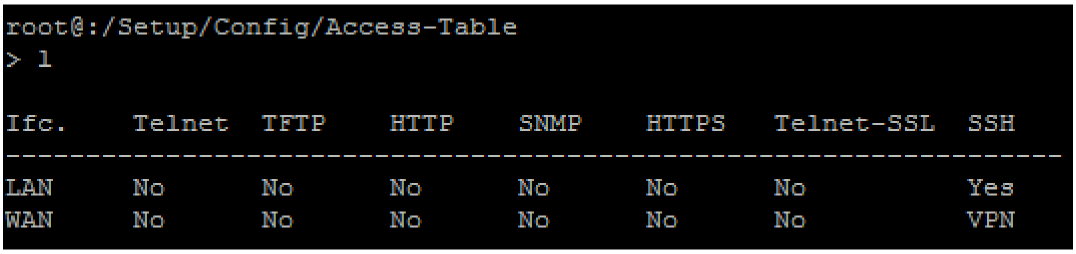


```
root@:/Setup/Config/LL2M
> l

Operating    VALUE:    No
Time-Limit   VALUE:    0
```

- /Setup/Config/Access-Table

Only SSH should be enabled and everything else must be deactivated. If necessary you can enable SSHv2 for connections from remote VPN networks. In this case you have set the SSH entry for WAN to “VPN”. Otherwise, this field must be set to “No”.

will be checked by cctest

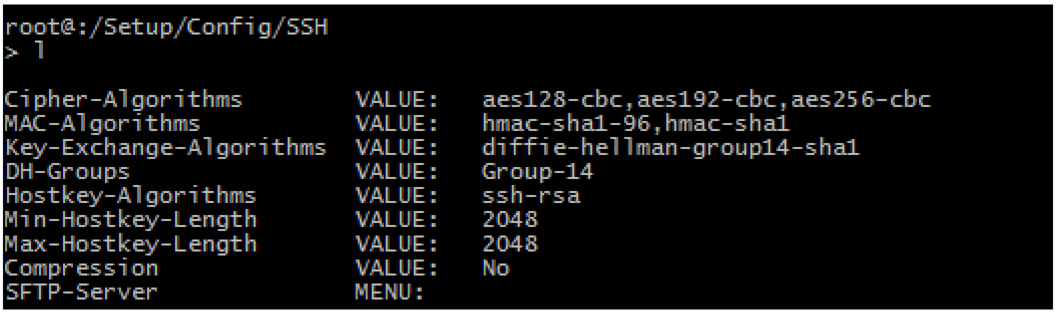


```
root@:/Setup/Config/Access-Table
> l

Ifc.     Telnet   TFTP     HTTP     SNMP     HTTPS    Telnet-SSL   SSH
-------------------------------------------------------------------
LAN      No       No       No       No       No       No           Yes
WAN      No       No       No       No       No       No           VPN
```

- /Setup/Config/SSH

To operate the SSH module in a secure way, only the following parameters are allowed:

will be checked by cctest



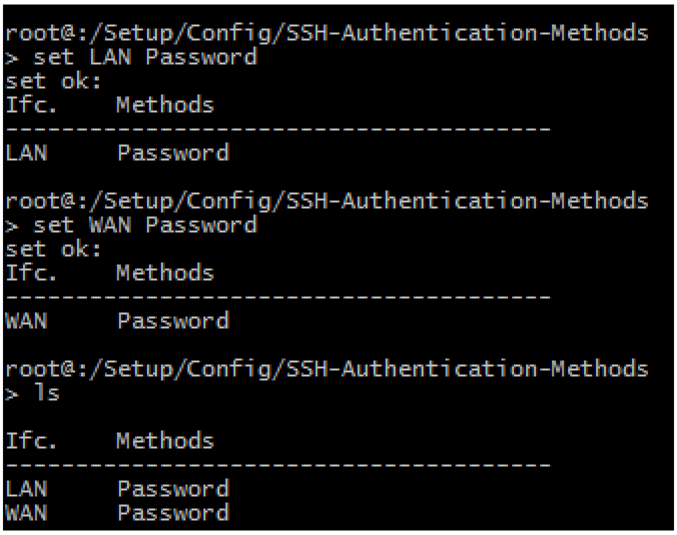
```
root@:/Setup/Config/SSH
> l

Cipher-Algorithms         VALUE:   aes128-cbc,aes192-cbc,aes256-cbc
MAC-Algorithms            VALUE:   hmac-sha1-96,hmac-sha1
Key-Exchange-Algorithms   VALUE:   diffie-hellman-group14-sha1
DH-Groups                 VALUE:   Group-14
Hostkey-Algorithms        VALUE:   ssh-rsa
Min-Hostkey-Length        VALUE:   2048
Max-Hostkey-Length        VALUE:   2048
Compression               VALUE:   No
SFTP-Server               MENU:
```

| | |
|---|---|
| Cipher-Algorithms: | aes128-cbc, aes192-cbc, aes256-cbc |
| MAC-Algorithms: | hmac-sha1-96, hmac-sha1 |
| Key-Exchange-Algorithms: | diffie-hellman-group14-sha1 |
| DH-Groups | Group-14 |
| Hostkey-Algorithms: | ssh-rsa |
| Min-Hostkey-Length: | 2048 |
| Max-Hostkey-Length: | 2048 |
| Compression | no |

The SSH authentication methods for LAN and WAN must be set to “password” only:

will be checked by cctest

- “set /Setup/Config/SSH-Authentication-Methods/LAN Password”
- “set /Setup/Config/SSH-Authentication-Methods/WAN Password”

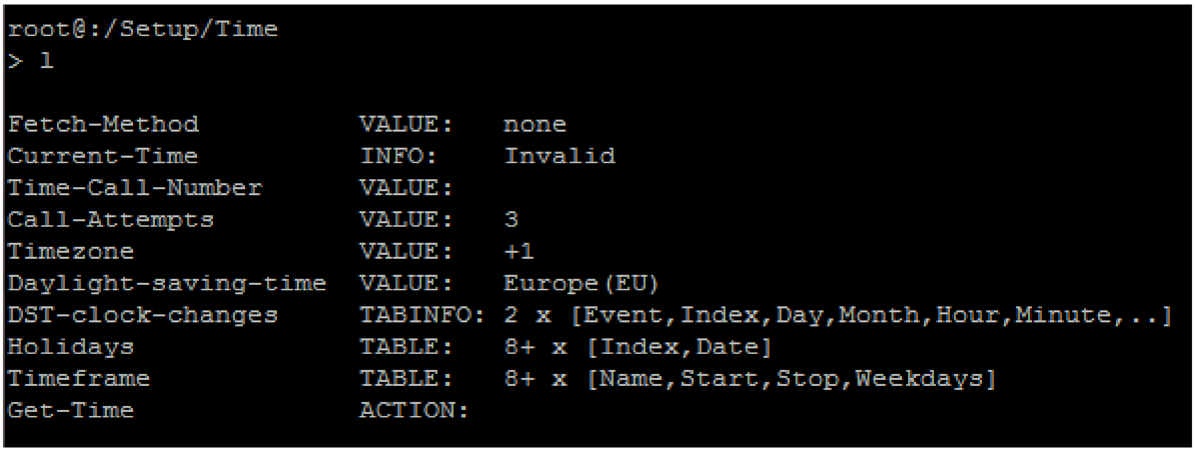


```
root@:/Setup/Config/SSH-Authentication-Methods
> set LAN Password
set ok:
Ifc.    Methods
---------------------------------------
LAN     Password

root@:/Setup/Config/SSH-Authentication-Methods
> set WAN Password
set ok:
Ifc.    Methods
---------------------------------------
WAN     Password

root@:/Setup/Config/SSH-Authentication-Methods
> ls

Ifc.    Methods
---------------------------------------
LAN     Password
WAN     Password
```

- /Setup/Time

The time must be set by the administrator; therefore the fetching method must be set to “none”. The administrator of the TOE must regularly check and set the system time (see AGD_PRE 1.2.3 - Initial configuration).

will be checked by cctest

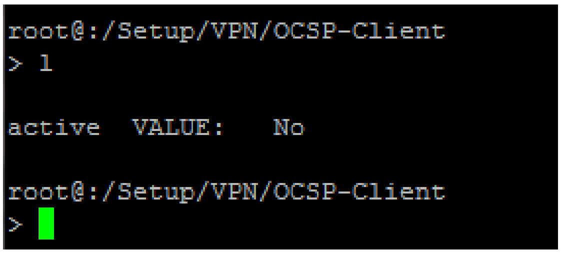


```
root@:/Setup/Time
> l

Fetch-Method            VALUE:    none
Current-Time            INFO:     Invalid
Time-Call-Number        VALUE:
Call-Attempts           VALUE:    3
Timezone                VALUE:    +1
Daylight-saving-time    VALUE:    Europe(EU)
DST-clock-changes       TABINFO: 2 x [Event,Index,Day,Month,Hour,Minute,..]
Holidays                TABLE:    8+ x [Index,Date]
Timeframe               TABLE:    8+ x [Name,Start,Stop,Weekdays]
Get-Time                ACTION:
```

- /Setup/VPN/OCSP-Client

The OCSP-Client has to be deactivated.

will be checked by cctest

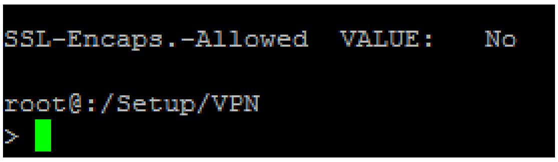


```
root@:/Setup/VPN/OCSP-Client
> l

active   VALUE:    No

root@:/Setup/VPN/OCSP-Client
> 
```

- /Setup/VPN/

The SSL Encapsulation for VPN connections has to be disabled.

will be checked by cctest

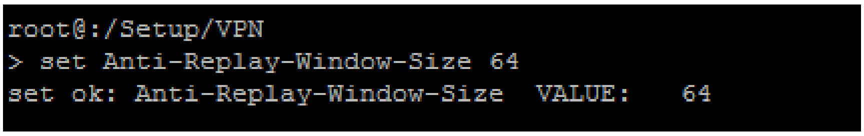


```
SSL-Encaps.-Allowed  VALUE:    No

root@:/Setup/VPN
> 
```

- /Setup/VPN/

The anti-replay protection has to be enabled and set to the value of: 64

will be checked by cctest

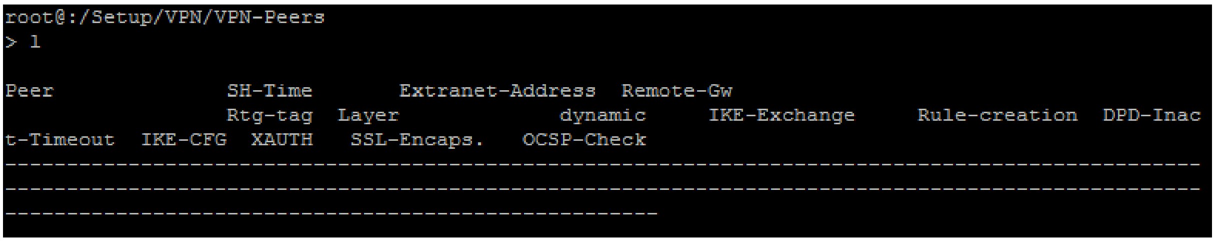


```
root@:/Setup/VPN
> set Anti-Replay-Window-Size 64
set ok: Anti-Replay-Window-Size  VALUE:    64
```

- /Setup/VPN/VPN-Peers/

When creating a VPN peer, the options SSL-Encaps, OCSP-Check, XAUTH and dynamic VPN must be deactivated.

will be checked by cctest

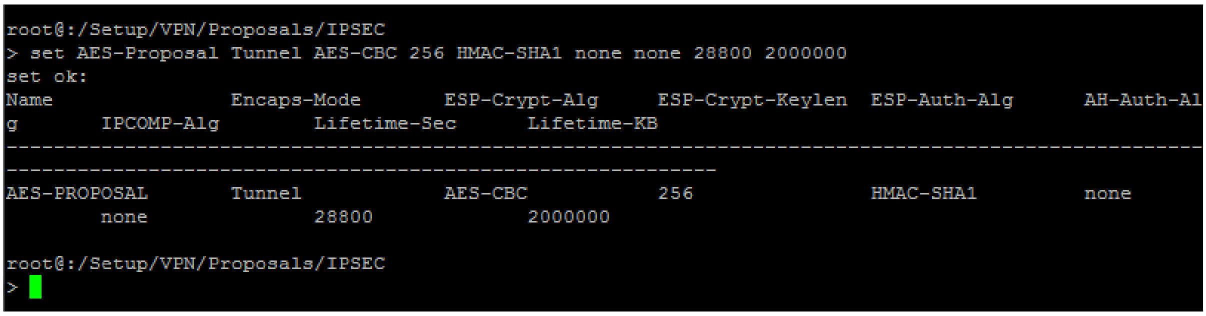


```
root@:/Setup/VPN/VPN-Peers
> l

Peer              SH-Time       Extranet-Address  Remote-Gw
                  Rtg-tag  Layer             dynamic     IKE-Exchange     Rule-creation  DPD-Inac
t-Timeout  IKE-CFG  XAUTH   SSL-Encaps.   OCSP-Check
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
```

- /Setup/VPN/Proposals/IPSEC

When creating an IPSEC proposal the use of “tunnel mode” is mandatory. Any other setting is not allowed.

will be checked by cctest

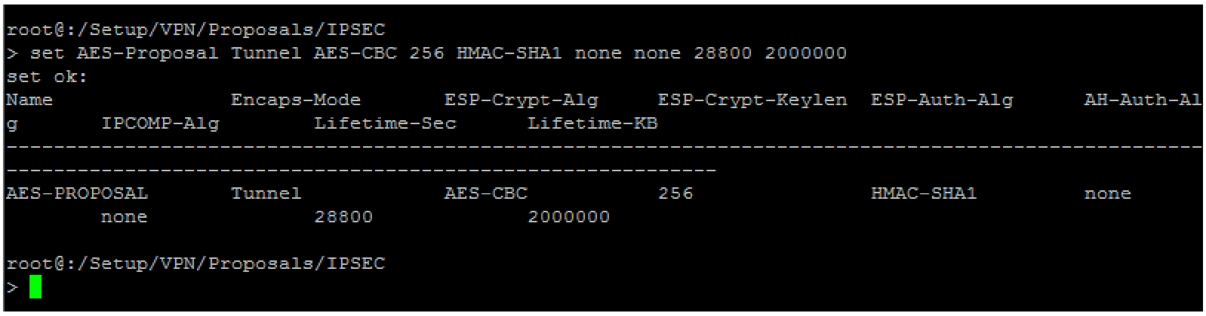


```
root@:/Setup/VPN/Proposals/IPSEC
> set AES-Proposal Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000
set ok:
Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-Auth-Alg      AH-Auth-Al
g       IPCOMP-Alg        Lifetime-Sec      Lifetime-KB
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------
AES-PROPOSAL       Tunnel            AES-CBC           256               HMAC-SHA1         none
        none              28800             2000000

root@:/Setup/VPN/Proposals/IPSEC
>
```

- /Setup/VPN/Proposals/IPSEC

When creating an IPSEC proposal the “AH-Auth-Alg” must be set to “none”. Any other setting is not allowed.

will be checked by cctest

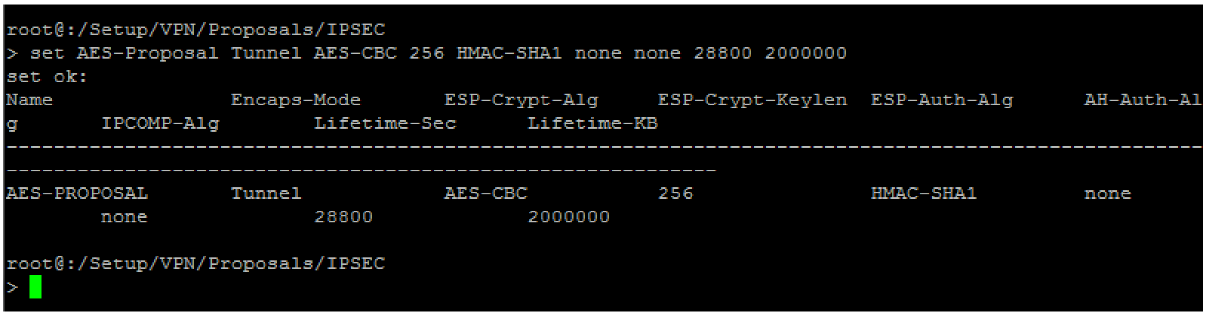


```
root@:/Setup/VPN/Proposals/IPSEC
> set AES-Proposal Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000
set ok:
Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-Auth-Alg      AH-Auth-Al
g       IPCOMP-Alg        Lifetime-Sec      Lifetime-KB
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------
AES-PROPOSAL       Tunnel            AES-CBC           256               HMAC-SHA1         none
        none              28800             2000000

root@:/Setup/VPN/Proposals/IPSEC
>
```

- /Setup/VPN/Proposals/IPSEC

When creating an IPSEC proposal the “lifetime” must be set to 28800 sec / 2000000 KB. Any other setting is not allowed.

will be checked by cctest

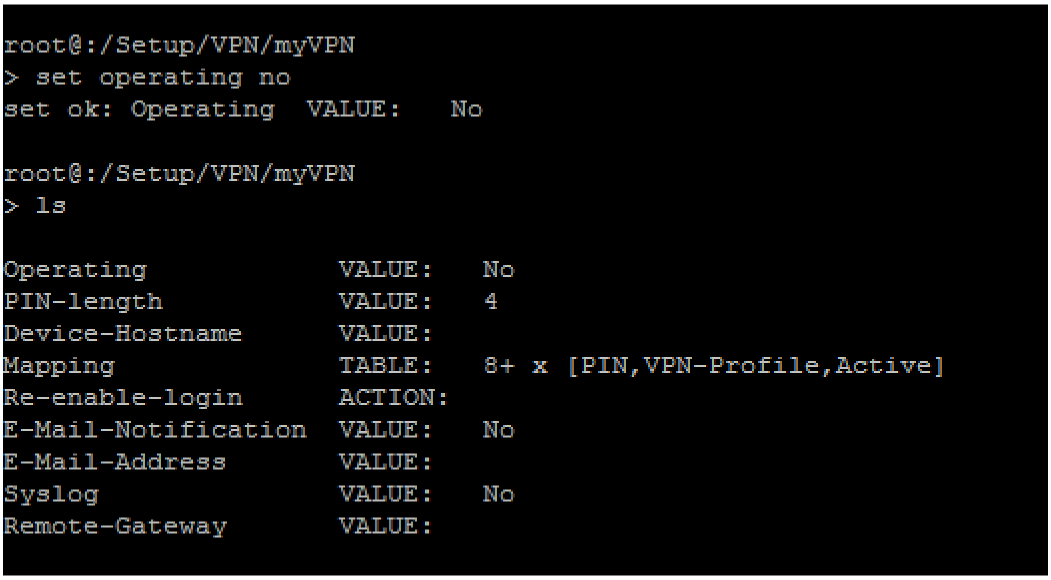


```
root@:/Setup/VPN/Proposals/IPSEC
> set AES-Proposal Tunnel AES-CBC 256 HMAC-SHA1 none none 28800 2000000
set ok:
Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-Auth-Alg      AH-Auth-Al
g       IPCOMP-Alg        Lifetime-Sec      Lifetime-KB
-----------------------------------------------------------------------------------------------------
------------------------------------------------------------
AES-PROPOSAL       Tunnel            AES-CBC           256               HMAC-SHA1         none
        none              28800             2000000

root@:/Setup/VPN/Proposals/IPSEC
>
```

- /Setup/VPN/myVPN

The myVPN option must be disabled by setting operating to “no”.

will be checked by cctest

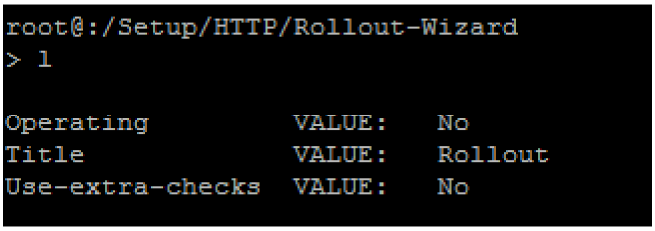


```
root@:/Setup/VPN/myVPN
> set operating no
set ok: Operating  VALUE:   No

root@:/Setup/VPN/myVPN
> ls

Operating             VALUE:   No
PIN-length            VALUE:   4
Device-Hostname       VALUE:
Mapping               TABLE:   8+ x [PIN,VPN-Profile,Active]
Re-enable-login       ACTION:
E-Mail-Notification   VALUE:   No
E-Mail-Address        VALUE:
Syslog                VALUE:   No
Remote-Gateway        VALUE:
```

- /Setup/HTTP/Rollout-Wizard

The rollout-wizard has to be deactivated.

will be checked by cctest

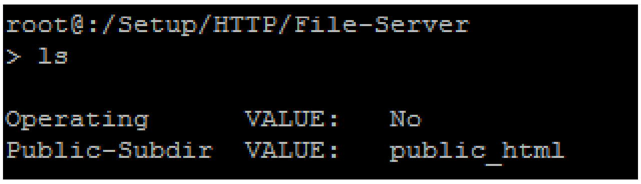


```
root@:/Setup/HTTP/Rollout-Wizard
> l

Operating         VALUE:   No
Title             VALUE:   Rollout
Use-extra-checks  VALUE:   No
```

- /Setup/HTTP/File-Server

The file-server also has to be deactivated.

will be checked by cctest

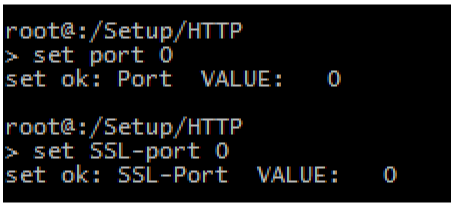


```
root@:/Setup/HTTP/File-Server
> ls

Operating       VALUE:    No
Public-Subdir   VALUE:    public_html
```

- /Setup/HTTP/

The HTTP and HTTPS Port must be set to “0”.

will be checked by cctest

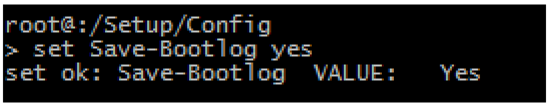


```
root@:/Setup/HTTP
> set port 0
set ok: Port  VALUE:   0

root@:/Setup/HTTP
> set SSL-port 0
set ok: SSL-Port  VALUE:   0
```

- /Setup/Config/

The bootlog must be saved persistently.

will be checked by cctest

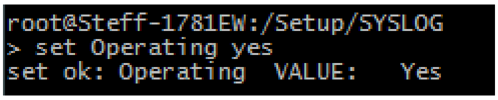


```
root@:/Setup/Config
> set Save-Bootlog yes
set ok: Save-Bootlog  VALUE:   Yes
```

- /Setup/SYSLOG/

The internal SYSLOG must be activated.

will be checked by cctest

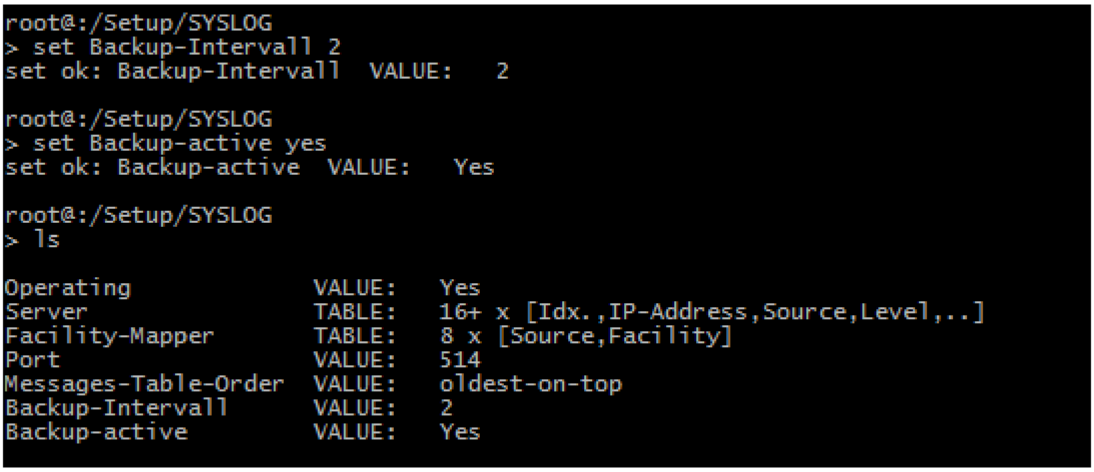


```
root@Steff-1781EW:/Setup/SYSLOG
> set Operating yes
set ok: Operating  VALUE:   Yes
```

- /Setup/SYSLOG/

The SYSLOG messages must be saved persistently.

will be checked by cctest

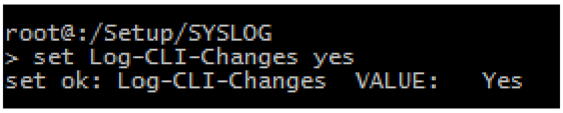


```
root@:/Setup/SYSLOG
> set Backup-Intervall 2
set ok: Backup-Intervall  VALUE:   2

root@:/Setup/SYSLOG
> set Backup-active yes
set ok: Backup-active  VALUE:   Yes

root@:/Setup/SYSLOG
> ls

Operating             VALUE:   Yes
Server                TABLE:   16+ x [Idx.,IP-Address,Source,Level,..]
Facility-Mapper       TABLE:   8 x [Source,Facility]
Port                  VALUE:   514
Messages-Table-Order  VALUE:   oldest-on-top
Backup-Intervall      VALUE:   2
Backup-active         VALUE:   Yes
```

- /Setup/SYSLOG/

CLI changes must be logged.

will be checked by cctest



```
root@:/Setup/SYSLOG
> set Log-CLI-Changes yes
set ok: Log-CLI-Changes  VALUE:   Yes
```

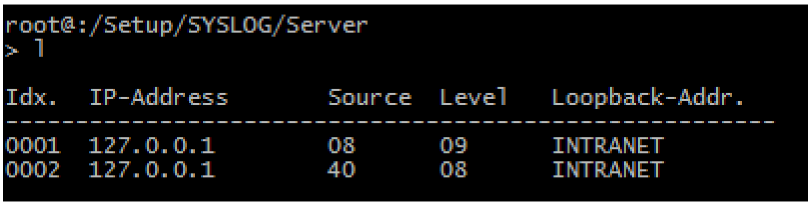
- /Setup/SYSLOG/Server

The syslog server must only be used to save information internally (IP-Address 127.0.0.1). All external IP addresses are not allowed for a secure usage. Please note that the administrator of the TOE has to manually save (copy & paste) the SYSLOG log messages at least every 48 hours to backup the log. Additionally the administrator must analyze the log file every 48 hours. The syslog messages can be found in /Status/TCP-IP/Syslog/Last-Messages.

will be checked by cctest

More information regarding SYSLOG can be found in LCOS-MENU-860-EN.pdf (2.22 - SYSLOG).

The following entries must be set:

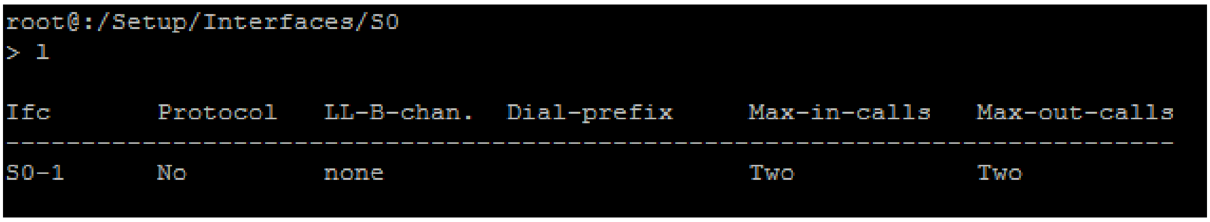


```
root@:/Setup/SYSLOG/Server
> l

Idx.  IP-Address       Source  Level   Loopback-Addr.
-------------------------------------------------------
0001  127.0.0.1        08      09      INTRANET
0002  127.0.0.1        40      08      INTRANET
```

- /Setup/Interfaces/S0

To make sure ISDN is not being used, the protocol has to be deactivated (set to “no”).

will be checked by cctest

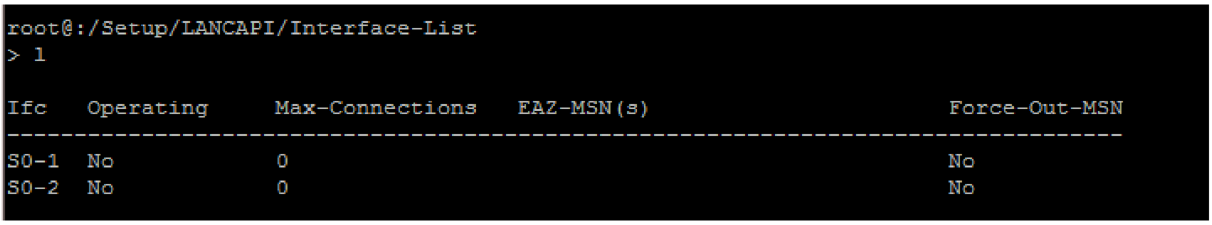


```
root@:/Setup/Interfaces/S0
> l

Ifc       Protocol   LL-B-chan.  Dial-prefix     Max-in-calls   Max-out-calls
------------------------------------------------------------------------------
S0-1      No         none                        Two            Two
```

- /Setup/LANCAPI/Interface-List

You must also deactivate the LANCAPI interfaces.

will be checked by cctest

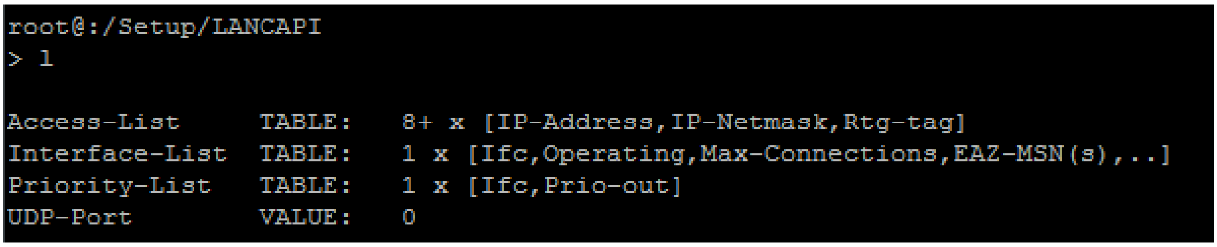


```
root@:/Setup/LANCAPI/Interface-List
> l

Ifc    Operating      Max-Connections   EAZ-MSN(s)                       Force-Out-MSN
--------------------------------------------------------------------------------------
S0-1   No             0                                                  No
S0-2   No             0                                                  No
```

- /Setup/LANCAPI/UDP-Port

The UDP-Port for LANCAPI must be set to “0”.

will be checked by cctest

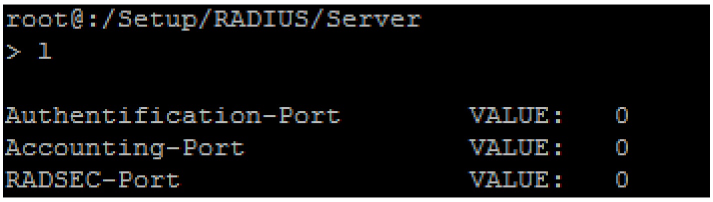


```
root@:/Setup/LANCAPI
> l

Access-List      TABLE:   8+ x [IP-Address,IP-Netmask,Rtg-tag]
Interface-List   TABLE:   1 x [Ifc,Operating,Max-Connections,EAZ-MSN(s),..]
Priority-List    TABLE:   1 x [Ifc,Prio-out]
UDP-Port         VALUE:   0
```

- /Setup/RADIUS/Server

To make sure, RADIUS is disabled, the Authentification-Port, Accounting-Port and RADSEC-Port must be set to “0”.

will be checked by cctest

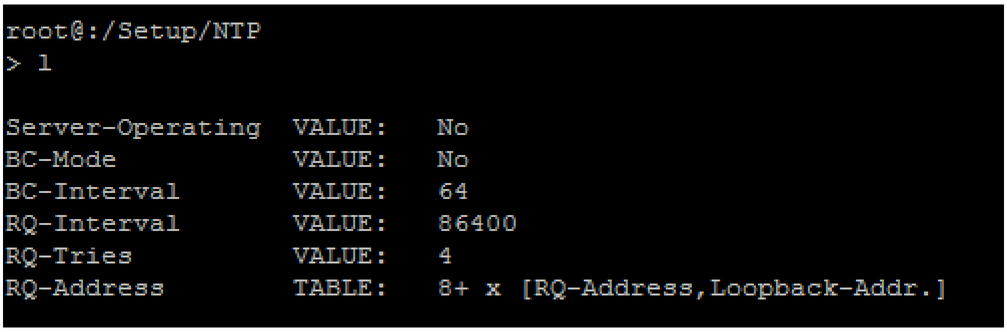


```
root@:/Setup/RADIUS/Server
> l

Authentification-Port        VALUE:    0
Accounting-Port              VALUE:    0
RADSEC-Port                  VALUE:    0
```

- /Setup/NTP/

The server-operating mode must be disabled.

will be checked by cctest

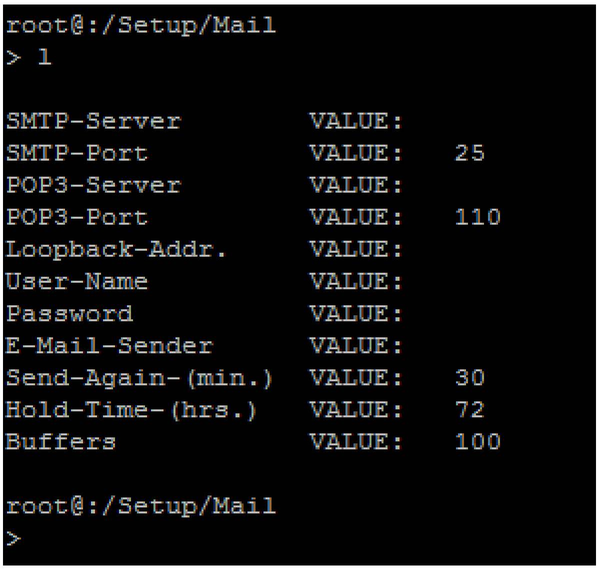


```
root@:/Setup/NTP
> l

Server-Operating  VALUE:    No
BC-Mode           VALUE:    No
BC-Interval       VALUE:    64
RQ-Interval       VALUE:    86400
RQ-Tries          VALUE:    4
RQ-Address        TABLE:    8+ x [RQ-Address,Loopback-Addr.]
```

- /Setup/Mail

For not allowing outgoing E-Mails, leave the SMTP Server, POP3 Server, Loopback-Addr., User-Name, Password and E-Mail-Sender blank. This will affect all E-Mail related configurations.

will be checked by cctest

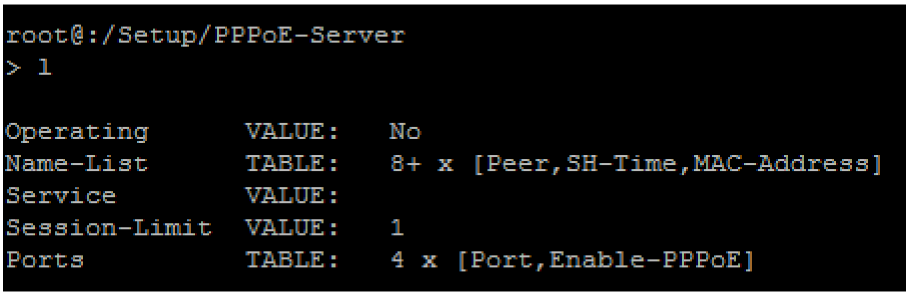


```
root@:/Setup/Mail
> l

SMTP-Server         VALUE:
SMTP-Port           VALUE:    25
POP3-Server         VALUE:
POP3-Port           VALUE:    110
Loopback-Addr.      VALUE:
User-Name           VALUE:
Password            VALUE:
E-Mail-Sender       VALUE:
Send-Again-(min.)   VALUE:    30
Hold-Time-(hrs.)    VALUE:    72
Buffers             VALUE:    100

root@:/Setup/Mail
>
```

- /Setup/PPPoE-Server

For secure operation also disable the PPPoE-Server:

will be checked by cctest

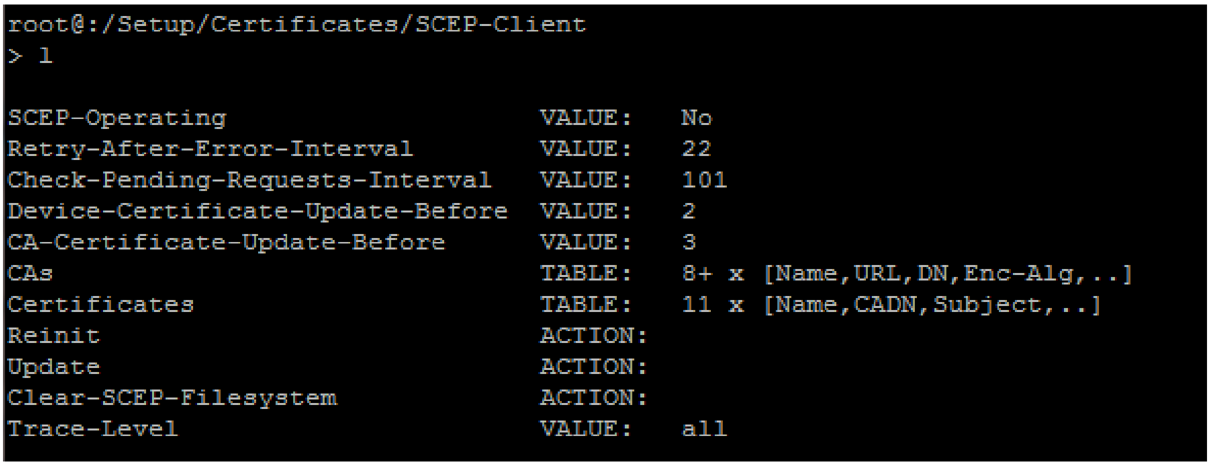


```
root@:/Setup/PPPoE-Server
> l

Operating       VALUE:    No
Name-List       TABLE:    8+ x [Peer,SH-Time,MAC-Address]
Service         VALUE:
Session-Limit   VALUE:    1
Ports           TABLE:    4 x [Port,Enable-PPPoE]
```

- /Setup/Certificates/SCEP-Client

The SCEP-Operating mode has to be disabled.

will be checked by cctest

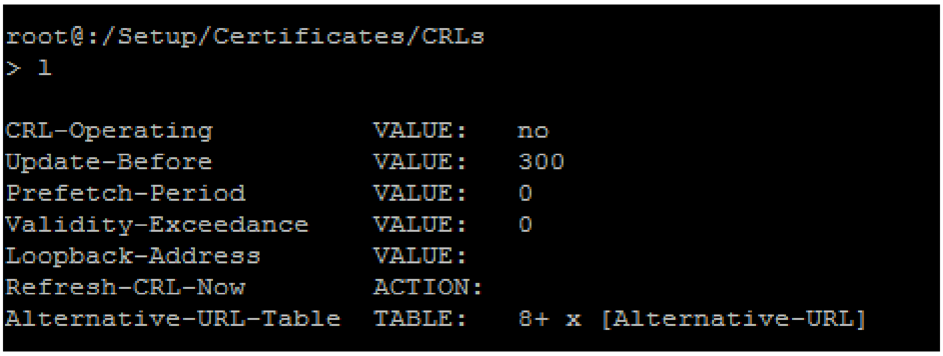


```
root@:/Setup/Certificates/SCEP-Client
> l

SCEP-Operating                     VALUE:    No
Retry-After-Error-Interval         VALUE:    22
Check-Pending-Requests-Interval    VALUE:    101
Device-Certificate-Update-Before   VALUE:    2
CA-Certificate-Update-Before       VALUE:    3
CAs                                TABLE:    8+ x [Name,URL,DN,Enc-Alg,..]
Certificates                       TABLE:    11 x [Name,CADN,Subject,..]
Reinit                             ACTION:
Update                             ACTION:
Clear-SCEP-Filesystem              ACTION:
Trace-Level                        VALUE:    all
```

- /Setup/Certificates/CRLs

CRL-Operating must also be deactivated.

will be checked by cctest

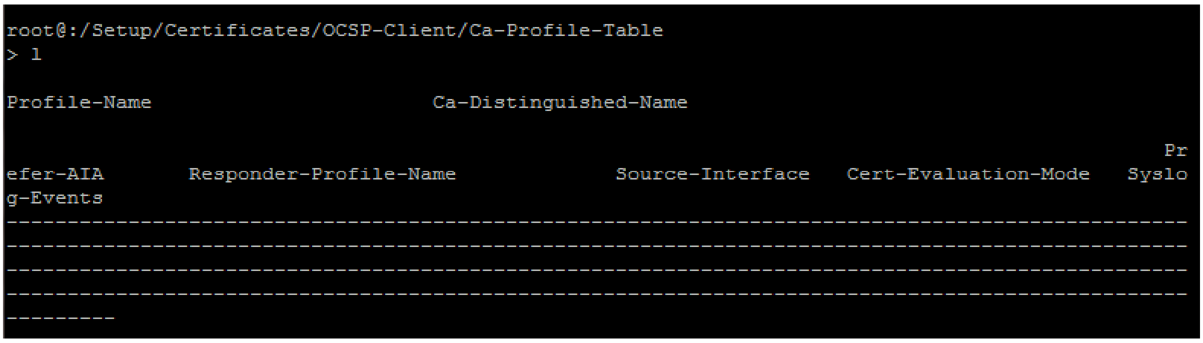


```
root@:/Setup/Certificates/CRLs
> l

CRL-Operating           VALUE:    no
Update-Before           VALUE:    300
Prefetch-Period         VALUE:    0
Validity-Exceedance     VALUE:    0
Loopback-Address        VALUE:
Refresh-CRL-Now         ACTION:
Alternative-URL-Table   TABLE:    8+ x [Alternative-URL]
```

- /Setup/Certificates/OCSP-Client/CA-Profile-Table

This table must be blank.

will be checked by cctest

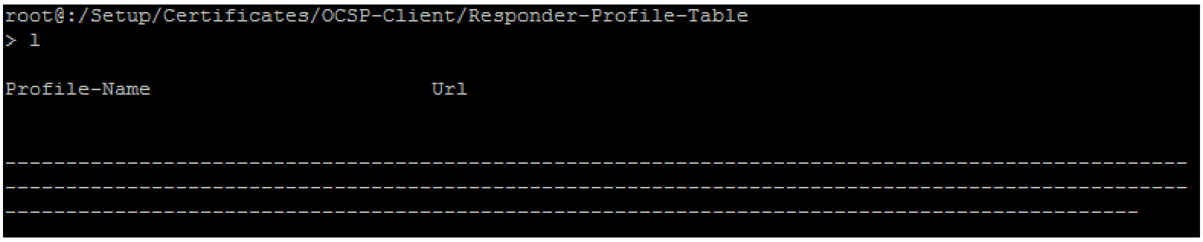


```
root@:/Setup/Certificates/OCSP-Client/Ca-Profile-Table
> l

Profile-Name                      Ca-Distinguished-Name

                                                                                              Pr
efer-AIA       Responder-Profile-Name             Source-Interface   Cert-Evaluation-Mode   Syslo
g-Events
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
---------
```

- /Setup/Certificates/OCSP-Client/Responder-Profile-Table

This table must be blank.

will be checked by cctest

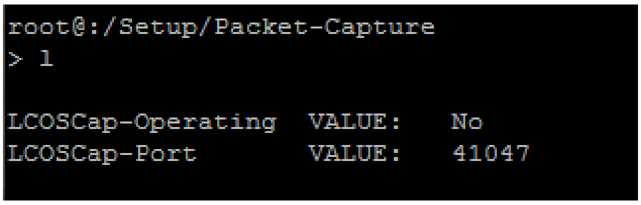


```
root@:/Setup/Certificates/OCSP-Client/Responder-Profile-Table
> l

Profile-Name                      Url


-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
```

- /Setup/Packet-Capture

Packet capturing must be deactivated.

will be checked by cctest

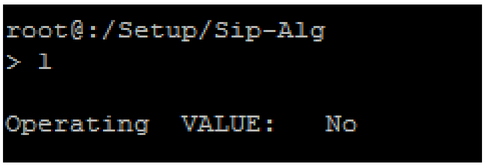


```
root@:/Setup/Packet-Capture
> l

LCOSCap-Operating   VALUE:    No
LCOSCap-Port        VALUE:    41047
```

- /Setup/Sip-Alg

The SIP-ALG must also be deactivated.

will be checked by cctest

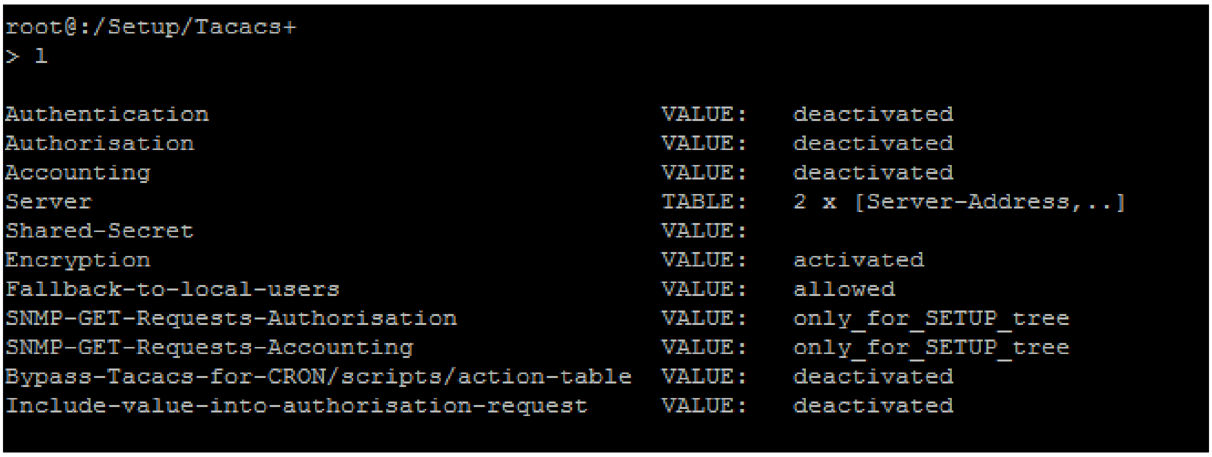


```
root@:/Setup/Sip-Alg
> l

Operating   VALUE:    No
```

- /Setup/Tacacs+

Authentication, Authorization and Accounting must be deactivated.

will be checked by cctest

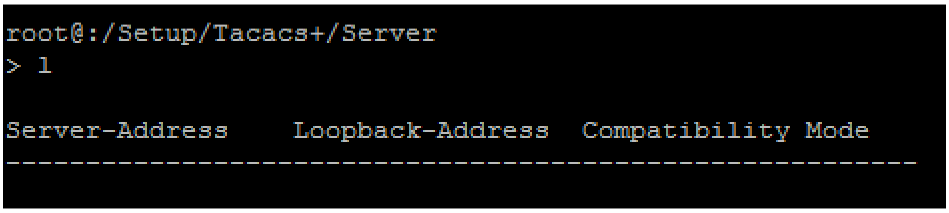


```
root@:/Setup/Tacacs+
> l

Authentication                              VALUE:   deactivated
Authorisation                               VALUE:   deactivated
Accounting                                  VALUE:   deactivated
Server                                      TABLE:   2 x [Server-Address,..]
Shared-Secret                               VALUE:
Encryption                                  VALUE:   activated
Fallback-to-local-users                     VALUE:   allowed
SNMP-GET-Requests-Authorisation             VALUE:   only_for_SETUP_tree
SNMP-GET-Requests-Accounting                VALUE:   only_for_SETUP_tree
Bypass-Tacacs-for-CRON/scripts/action-table VALUE:   deactivated
Include-value-into-authorisation-request    VALUE:   deactivated
```

- /Setup/Tacacs+/Server

This table must be blank.

will be checked by cctest

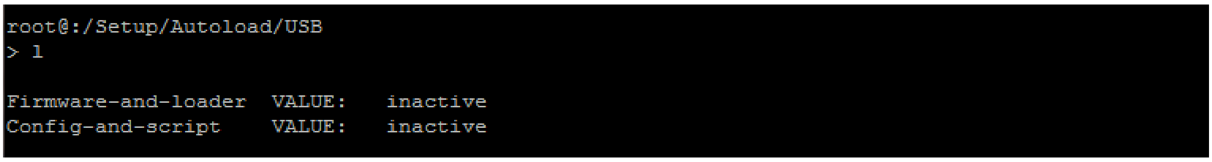


```
root@:/Setup/Tacacs+/Server
> l

Server-Address    Loopback-Address  Compatibility Mode
--------------------------------------------------------
```

- /Setup/Autoload/USB

Firmware-and-loader and Config-and-script must be set to “inactive”.

will be checked by cctest

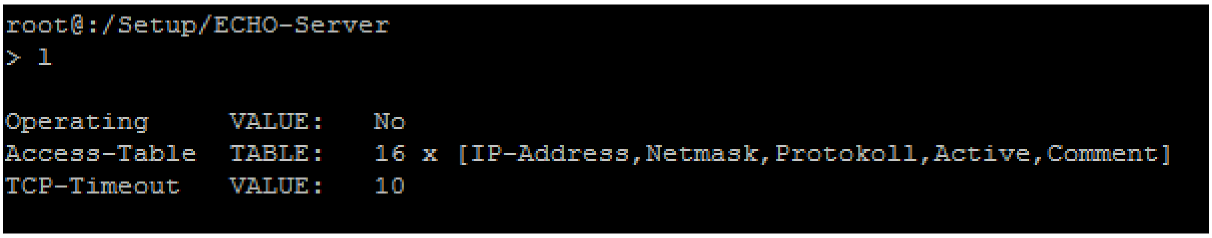


```
root@:/Setup/Autoload/USB
> l

Firmware-and-loader  VALUE:   inactive
Config-and-script    VALUE:   inactive
```

- /Setup/ECHO-Server

The ECHO-Server must be disabled.

will be checked by cctest

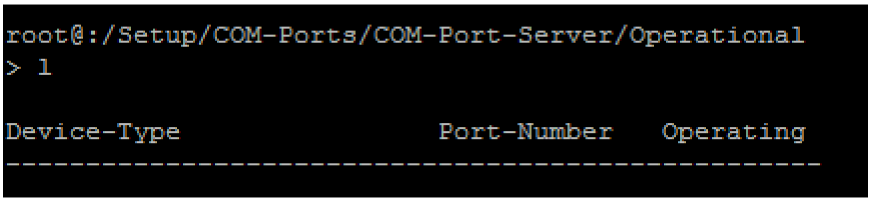


```
root@:/Setup/ECHO-Server
> l

Operating      VALUE:   No
Access-Table   TABLE:   16 x [IP-Address,Netmask,Protokoll,Active,Comment]
TCP-Timeout    VALUE:   10
```

- /Setup/COM-Ports/COM-Port-Server/Operational

This table must be empty.

will be checked by cctest

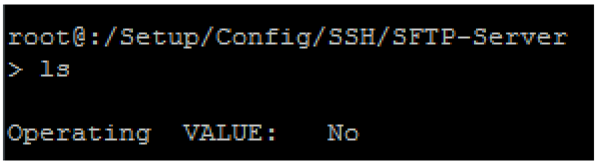


```
root@:/Setup/COM-Ports/COM-Port-Server/Operational
> l

Device-Type                Port-Number   Operating
-----------------------------------------------------
```

- /Setup/Config/SSH/SFTP-Server

The SFTP Server has to be deactivated.

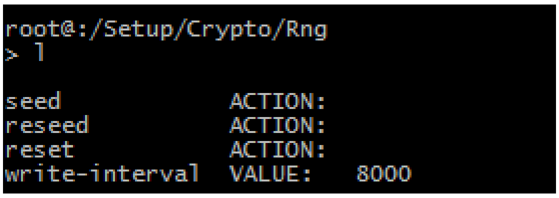
will be checked by cctest



```
root@:/Setup/Config/SSH/SFTP-Server
> ls

Operating  VALUE:   No
```

- /Setup/Crypto/Rng

It is not allowed to run “do reset”.

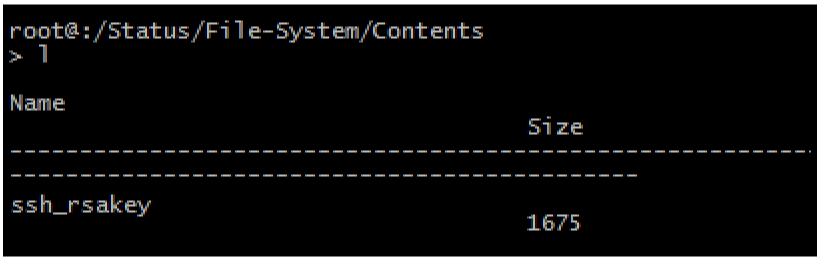


```
root@:/Setup/Crypto/Rng
> l

seed            ACTION:
reseed          ACTION:
reset           ACTION:
write-interval  VALUE:    8000
```

- /Status/File-System/Contents

It is not allowed to delete the ssh_rsakey. With running “cctest” you must check the existence of the file.

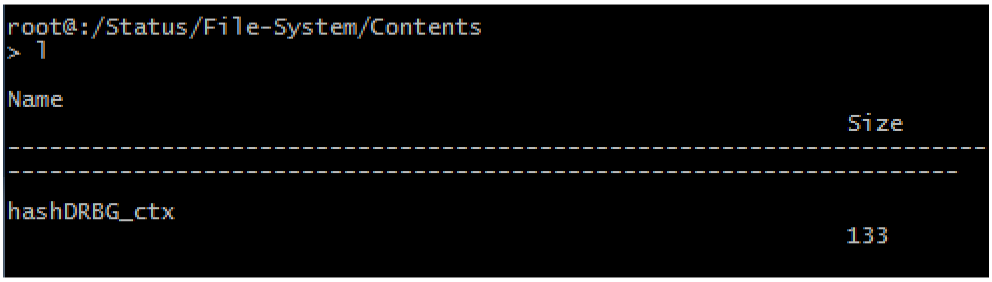
will be checked by cctest



```
root@:/Status/File-System/Contents
> l

Name
                                     Size
------------------------------------------------------------
---------------------------------------------
ssh_rsakey
                                     1675
```

- /Status/File-System/Contents

It is not allowed to delete the “hashDRBG_ctx“:



```
root@:/Status/File-System/Contents
> l

Name
                                                            Size
----------------------------------------------------------------------
--------------------------------------------------------------------
hashDRBG_ctx
                                                            133
```

- USB Devices

Make sure no USB device is connected to the device at any time.

- Serial modems

Make sure no serial modems are connected at any time.

### 2.8.4. Regular Maintenance Tasks

This section describes which tasks the administrator has to perform on a regular basis.

- /Status/Crypto/RNG

The administrator has to check the percentage of the used random numbers on a weekly basis. If the value reaches 99 % the administrator must perform a reseed (see AGP_PRE 1.2.3 - Initial configuration)

- /Status/TCP-IP/Syslog/Last-messages/

The administrator has to backup, check, and analyze the internal SYSLOG every 48 hours.

- /Status/Current-time

The administrator has to check that the TOE has a valid time every 48 hours (see AGD_PRE 1.2.3 – Initial configuration).