Sicherheitsrelevante Einstellungen von LCOS basierten Routern

Inhaltsverzeichnis

LCOS-Version und -Syntaxbeschreibung

Die beschriebenen Einstellungen beziehen sich auf Geräte mit der minimalen LCOS Version 9.24, 10.12 oder 10.20. Um eine umfassende Absicherung insbesondere im Umfeld der zentralen Administratoren-Verwaltung erreichen zu können, werden die Funktionen der LCOS Version 9.24, 10.12 oder 10.20 vorausgesetzt.

Bereits in früheren Softwareständen verfügbare Einstellungen können für diese sinngemäß übernommen werden.

Zu allen aufgeführten Konfigurationsparametern werden der Kommandozeilenpfad und die notwendigen Befehle zum Setzen der beschriebenen Parameter sowie eine Übersicht der möglichen Werte aufgeführt.

Beispielhaft aufgeführte Skripte werden in der Regel auf die zum Verständnis relevanten Spalten gekürzt.

Management

Passwort Qualität

Die Sicherheit des Passwortschutzes hängt in erster Linie von der Komplexität und Zufälligkeit des verwendeten Passwortes ab. Das LCOS erlaubt Passwörter für lokale Administratoren-Accounts mit max. 15 Zeichen Länge.

Das Input Set umfasst die folgenden Zeichen:

```
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrst
uvwxyz `-
```

Das Passwort sollte zufällig gewählt sein und **mindestens acht Zeichen umfassen**.

Command Line Interface Einstellung für Root-Passwort:

```
passwd                  change password

passwd -n new [old]     change password (no prompt)

passwd -u <username>    change password of local user (TACACS+)
```

Brute Force-Schutz

Verstärkt wird der Passwort Schutz bei lokaler Authentisierung durch den Brute Force Schutz. Die mehrfach wiederholte fehlerhafte Eingabe des Passwortes führt zu einer Sperre von definierbarer Länge.

Pfad:

```
/Setup/Config

/Setup/Voice-Call-Manager/General
```

Kommando:

```
set /Setup/Config/Login-Errors 5

set /Setup/Config/Lock-Minutes 5

set Setup/Voice-Call-Manager/General/Login-Errors 5

set /Setup/Voice-Call-Manager/General/Lock-Minutes 5
```

Mögliche Einträge:

```
Login-Errors            :2 chars from: 1234567890

Lock-Minutes            :2 chars from: 1234567890
```

SSH-Parameter

Pfad:

/Setup/Config/SSH

Kommandos:

```
set cipher-algorithms aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305,aes128-gcm,aes256-gcm

set DH-Groups Group-14,Group-15,Group-16

set Elliptic-Curves nistp256,nistp384,nistp521

set Hostkey-Algorithms ssh-rsa,ssh-dss,ecdsa-sha2,ssh-ed25519

set Key-Exchange-Algorithms diffie-hellman-group-exchange-sha256,ecdh-sha2,curve25519-sha256

set MAC-Algorithms hmac-sha2-256,hmac-sha2-512

set Max-Hostkey-Length 8192

set Min-Hostkey-Length 2048
```

Mögliche Einträge:

```
[ 12] Operating              : Bitmask: No (0), Yes (1)
[ 13] Port                   : 5 chars from 1234567890
[  1] Cipher-Algorithms      : Bitmask: 3des-cbc (1), 3des-ctr (2), arcfour (4), arcfour128 (8), arcfour256 (16), blowfish-cbc (32), blowfish-ctr (64), aes128-cbc (128), aes192-cbc (256), aes256-cbc (512), aes128-ctr (1024), aes192-ctr (2048), aes256-ctr (4096), chacha20-poly1305 (8192), aes128-gcm (16384), aes256-gcm (32768)
[  2] MAC-Algorithms         : Bitmask: hmac-md5-96 (1), hmac-md5 (2), hmac-sha1-96 (4), hmac-sha1 (8), hmac-sha2-256-96 (16), hmac-sha2-256 (32), hmac-sha2-512-96 (64), hmac-sha2-512 (128)
[  3] Key-Exchange-Algorithms : Bitmask: diffie-hellman-group1-sha1 (1), diffie-hellman-group14-sha1 (2), diffie-hellman-group-exchange-sha1 (4), diffie-hellman-group-exchange-sha256 (8), ecdh-sha2 (16), curve25519-sha256 (32)
[  7] DH-Groups              : Bitmask: Group-1 (1), Group-5 (2), Group-14 (4), Group-15 (8), Group-16 (16)
[  9] Elliptic-Curves        : Bitmask: nistp256 (1), nistp384 (2), nistp521 (4)
[  4] Hostkey-Algorithms     : Bitmask: ssh-rsa (1), ssh-dss (2), ecdsa-sha2 (4), ssh-ed25519 (8)
[  5] Min-Hostkey-Length     : 5 chars from 1234567890
[  6] Max-Hostkey-Length     : 5 chars from 1234567890
[  8] Compression            : No (0), Yes (1)
[ 11] Keepalive-Interval     : 5 chars from 1234567890
```

Individuelle SSH-Schlüssel

Sie haben die Möglichkeit, die werksseitig installierten sowie die automatisch generierten SSH-/SSL-Schlüssel durch eigene RSA- und DSA- oder DSS-Schlüssel zu ersetzen, um z.B. eine höhere Verschlüsselungsstärke zu realisieren.

Um herauszufinden, ob Ihr LANCOM Router noch die SSH- & SSL-Standard-Keys verwendet, oder ob er bereits individuelle Keys einsetzt, müssen Sie folgendermaßen vorgehen:

Kommando:

```
ls /status/file-system/content
```

Wenn in der angezeigten Liste die folgenden Dateien vorhanden sind, arbeitet Ihr Gerät bereits mit individuellen SSH- & SSL Keys und es sind keine weiteren Maßnahmen erforderlich:

- ssh_rsakey für den RSA key
- ssh_dsakey für den DSA key
- ssh_ecdsakey für den Eliptic curve DSA key

SSH-Schlüsselerzeugung unter LCOS

Zur Erzeugung eines individuellen Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel müssen Sie folgendermaßen vorgehen

Kommando:

```
sshkeygen [-t (dsa|rsa|ecdsa)] [-b <Bits>] -f <OutputFile> [-q]
```

Mögliche Parameter:

```
-t (dsa|rsa|ecdsa)
```

Dieser Parameter bestimmt den Typ des erzeugten Schlüssels. Insgesamt unterstützt SSH folgende Typen von Schlüsseln:

- RSA-Schlüssel sind am weitesten verbreitet und haben eine Länge von 512 bis zu 16384 Bit. Verwenden Sie nach Möglichkeit Schlüssel mit einer Länge von 1024 bis 2048 Bit.
- DSA-Schlüssel folgen dem Digital Signature Standard (DSS) des National Institute of Standards and Technology (NIST) und werden z. B. in Umgebungen eingesetzt, die eine Compliance mit dem Federal Information Processing Standard (FIPS) erfordern. DSA- oder DSS-Schlüssel haben immer eine Länge von 1024 Bit, sind aber langsamer als die entsprechenden RSA-Schlüssel.
- ECDSA-Schlüssel sind eine Variante von DSA-Schlüsseln, bei der das Gerät für die Schlüsselerzeugung elliptische Kurven verwendet (Elliptic Curve Cryptography, ECC). Die ECC ist eine Alternative zu den klassischen Signatur- und Schlüsselaustauschverfahren wie RSA und Diffie-Hellman. Der Hauptvorteil von elliptischen Kurven liegt darin, dass Sie durch deren mathematische Eigenschaften die gleiche Schlüsselstärke wie bei RSA oder Diffie-Hellman mit einer deutlich kürzeren Schlüssellänge erreichen. Dies erlaubt eine bessere Leistung bei äquivalenter Hardware. ECC und deren Integration in SSL und TLS sind in den RFCs 5656 und 4492 beschrieben.

  Wenn Sie keinen Typ angeben, erzeugt das Kommando immer einen RSA-Schlüssel.

```
-b <Bits>
```

Dieser Parameter bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel. Wenn Sie keine Länge angeben, erzeugt das Kommando immer einen Schlüssel mit einer Länge von 1024 Bit.

```
-f <OutputFile>
```

Über diesen Parameter geben Sie den Mountingpoint der erzeugten Schlüsseldatei im Dateisystem des Gerätes an. Die Wahl des Mountingpoints hängt davon ab, was für einen Schlüssel sie von welchem Typ erzeugen. Zur Auswahl stehen Ihnen in diesem Fall:

- ssh_rsakey für RSA-Schlüssel
- ssh_dsakey für DSA-Schlüssel
- ssh_ecdsakey für ECDSA-Schlüssel
- ssl_privkey für SSL-RSA-Schlüssel

`-q`

Dieser Parameter aktiviert den 'Quiet'-Modus für die Schlüsselerzeugung. Wenn Sie diesen Parameter setzen, überschreibt LCOS bereits existierende RSA- oder DSA-Schlüssel ungefragt; Ausgaben über den Fortschritt der Operation entfallen. Nutzen Sie diesen Parameter z. B. in einem Skript, um die Bestätigung von Sicherheitsabfragen durch den Benutzer zu unterdrücken.

Zentrale Authentisierung

In Installationen mit mehreren zuständigen Administratoren sollte die lokale Verwaltung der Administratoren-Accounts nach Möglichkeit nicht verwendet warden.

Weitere lokale Accounts stehen bei Verwendung der zentralen Authentisierung nicht zur Verfügung!

Um ein desaster recovery zu ermöglichen, kann optional der Fallback auf den lokalen Root-Account ermöglicht werden. Auf eine hohe Qualität des Root-Passwortes ist in diesem Fall besonderer Wert zu legen!

Pfad:

```
/Setup/TACACS+

/Setup/TACACS+/Server

/Setup/Config/Authentication
```

Kommando:

```
set /Setup/Config/Authentication

set /Setup/TACACS+/Shared-Secret "***"

set /Setup/TACACS+/Encryption activated

set /Setup/TACACS+/Connection-Timeout 5

set /Setup/TACACS+/Fallback-to-local-users allowed
```

Mögliche Einträge:

```
Authentication                : Intern (0), Radius (1), Tacacs+ (2)

Authorisation                 : deactivated (0), activated (1)

Shared-Secret                 : 31 chars from:
                                                    #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}
                                                    ~!$%&'()*+-,/:;<=>?[\]^_.0123456789abc
                                                    defghijklmnopqrstuvwxyz `

Encryption                : deactivated (0), activated (1)

Fallback-to-local-users   : allowed (0), prohibited (1)

cd /Setup/Tacacs+/Server

tab  Server-Address    Loopback-Address

set  10.2.3.4          "INTRANET"

cd /
```

Mögliche Einträge für columns in Server:

```
[1][Server-Address]       :31 chars from:
                                      ABCDEFGHIJKLMNOPQRSTUVWXYZ
                                      @{|}~!$%&'()+,/:;<=>?[\]^_.0123456789-
[2][Loopback-Address]  :16 chars from:
                                      ABCDEFGHIJKLMNOPQRSTUVWXYZ
                                      @{|}~!$%&'()+,/:;<=>?[\]^_.0123456789-
```

Zentrale Autorisierung und Logging

Um Änderungen in der Konfiguration zentral zu autorisieren und Änderungen zeitlich und personenbezogen nachhalten zu können unterstützt das LCOS TACACS+ zur zentralen Autorisierung und Aufzeichnung von Konfigurationsänderungen.

Pfad:

```
/Setup/TACACS+
/Setup/TACACS+/Server
```

Kommando:

```
set /Setup/TACACS+/Authorisation activated
set /Setup/TACACS+/Accounting activated

set /Setup/TACACS+/Server/Authorisation activated
set /Setup/TACACS+/Server/Accounting activated
```

Mögliche Einträge:

```
Authorisation            : deactivated (0), activated (1)
Accounting               : deactivated (0), activated (1)
```

Optionale Ausnahmen von TACACS+ Autorisierung und Accounting

LCOS verfügt über einen Schalter, der Befehle, die über die Cron Tabelle `(/Setup/Config/Cron-Table)`, die Aktionstabelle `(/Setup/WAN/Action-Table)` und den Befehl `beginscript` ausgeführt werden, von den TACACS+ Funktionen Autorisierung und Accounting ausnimmt.

Bei Verwendung von TACACS+ ist der Zugriff auf diesen Schalter und bei Schaltzustand `deactivated (0)` der Zugriff auf die Cron Tabelle, die Aktionstabelle und den Befehl beginscript besonders restriktiv zu handhaben, um Administratoren auf diesem Weg keine ungewollten Zugriffsmöglichkeiten auf die Konfiguration zu ermöglichen.

Es wird empfohlen, den Zugriff auf Administratoren und Automaten zu beschränken, die ohnehin mit Root Rechten ausgestattet sind.

Pfad:

`/Setup/TACACS+`

Kommando:

```
set /Setup/TACACS+/ Bypass-Tacacs-for-CRON/scripts/action-table activated
```

Mögliche Einträge:

```
Bypass-Tacacs-for-CRON/scripts/action-table:
deactivated (0),activated (1)
```

SNMP Get Requests von TACACS+ Autorisierung und Accounting ausnehmen

Die TACACS+ Funktionen Autorisierung und Accounting für SNMP GET REQUESTs können zur Entlastung von TACACS+ Servern in SNMP überwachten Netzwerken auf den Setup Pfad eingeschränkt oder auch vollständig deaktiviert werden.

Der Status Pfad beinhaltet keine Informationen über Userdaten. Dennoch ist im Projektumfeld die Unbedenklichkeit der Statusinformationen zu beurteilen. **Die vollständige Deaktivierung der Überwachungsfunktionen von SNMP GET REQUESTs ist nicht anzuraten.**

Um unerwünschte Zugriffe über SNMP auszuschließen, ist der Zugriff auf diesen Schalter besonders restriktiv zu handhaben und sollte nur Administratoren mit Root Rechten zugestanden werden.

Pfad:

```
/Setup/Tacacs+
```

Kommando:

```
set /Setup/Tacacs+/ SNMP-GET-Requests-Authorisation only_for_SETUP_tree

set /Setup/Tacacs+/ SNMP-GET-Requests-Accounting only_for_SETUP_tree
```

Mögliche Einträge:

```
SNMP-GET-Requests-Authorisation:

only_for_SETUP_tree (0), all (1), none (2)

SNMP-GET-Requests-Accounting:

only_for_SETUP_tree (0), all (1), none (2)
```

SNMPv3

Die Protokoll-Struktur von SNMP hat sich in der Version 3 grundlegend geändert. SNMPv3 ist in mehrere Module mit klar definierten Interfaces aufgeteilt, die untereinander kommunizieren.

Die drei wichtigsten Elemente in SNMPv3 sind "Message Processing and Dispatch (MPD)", "User-based Security Model (USM)" und "View-based Access Control Mechanism (VACM)".

Erlaube Admins

In der Standardeinstellung ist die Option aktiv, sodass registrierte Administratoren Zugriff über SNMPv3 erhalten.

Pfad:

```
/Setup/SNMP
```

Kommando:

```
cd /Setup/SNMP
set Allow-Admins YES
```

Zugelassene Protokolle

Aktivieren Sie hier die SNMP-Versionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll. **Es wird empfohlen, ausschließlich SNMPv3 zu verwenden (Standardeinstellung).**

Pfad:

```
/Setup/SNMP
```

Kommando:

```
cd /Setup/SNMP
set Admitted-Protocols SNMPv3
```

SNMPv3-Admin-Authentifizierung

Dieser Wert legt die Autorisierungsmethode für Administratoren fest. Er ist **fest auf HMAC-SHA eingestellt und kann nicht verändert werden**.

SNMPv3-Admin-Verschlüsselung

Dieser Wert die Verschlüsselungseinstellungen für Administratoren fest. Er ist **fest auf AES256 eingestellt und kann nicht verändert werden**.

Benutzer

Wenn abweichend von den Administratoren einzelne Benutzer SNMPv3 Zugriff erhalten sollen, so können diese zusätzlich angelegt werden. Die Authentifizierungs- und Verchlüsselungsmethode kann für jeden Benutzer individuell konfiguriert werden.

Pfad:

```
/Setup/SNMP/Users
```

Kommando:

```
cd /Setup/SNMP/Users
```

```
tab User-Name Authentication-Protocol Authentication-Password Privacy-Protocol
Privacy-Password Status
```

```
set “User1” “HMAC-SHA” “9kuufgz76zzh56hft54gjf7” “AES256” “9kuufgz76zzh56hft54gjf7”
“active”
```

Mögliche Werte:

```
[2] User-Name: 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`
```

```
[5] Authentication-Protocol: None (1), HMAC-MD5 (2), HMAC-SHA (3), HMAC-SHA224 (4),
HMAC-SHA256 (5), HMAC-SHA384 (6), HMAC-SHA512 (7)
```

```
[6] Authentication-Password: 40 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-
,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz `
```

```
[8] Privacy-Protocol: None (1), DES (2), AES128 (4), AES192 (20), AES256 (21)
```

```
[9] Privacy-Password: 40 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-
,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz `
```

```
[13] Status: active (1), inactive (2)
```

Gruppen

In der Gruppenkonfiguration können ReadOnly- bzw. ReadWrite-Communities für SNMPv3 erstellt werden.

Pfad:

```
/Setup/SNMP/Groups
```

Kommando:

```
cd /Setup/SNMP/Groups

tab  Security.Model    Security-Name    Group-Name   Status

set “SNMPv3(USM)” “User1” “SNMPv3-ReadOnly” “active”
```

Mögliche Werte:

```
[1] Security-Model:
SNMPv1 (1), SNMPv2 (2), SNMPv3(USM) (3)

[2] Security-Name:
32 chars from
ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuv
wxyz`

[3] Group-Name:
32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

[5] Status: active (1), inactive (2)
```

Lokale Verwaltung der Konfigurationsprotokolle

Das LCOS unterstützt eine Vielzahl von Protokollen für das Management und Monitoring der enthaltenen Funktionen. Die Verwendung der Konfigurationsprotokolle kann zentral für LAN, WAN und ggf. WLAN Verbindungen konfiguriert werden.

Um die Konfigurationsdaten vor unberechtigten Zugriff zu schützen sollten ausschließlich verschlüsselte Konfigurations-protokolle zum Einsatz kommen. Das LCOS unterstützt SSH, Telnet SSL und HTTPs als verschlüsselte Konfigurations-Protokolle.

Die unverschlüsselten Protokolle Telnet, http und TFTP sollten deaktiviert sein oder ausschließlich auf vertrauenswürdigen Wegen, z.B. IPSec VPN Strecken nutzbar sein.

SNMPv1 und SNMPv2 (zusammengefasst unter der Einstellung „SNMP“) sollte vollständig deaktiviert werden.

IPv4

Pfad:

```
/Setup/Config/Access-Table
```

Kommando:

```
cd /Setup/Config/Access-Table
tab  Ifc.    Telnet  TFTP    HTTP    SNMP    HTTPS   Telnet-SSL  SSH   SNMPv3
set  LAN     No      No      No      No      Yes     Yes         Yes   Yes
set  WAN     No      No      No      No      Yes     Yes         Yes   Yes
set  WLAN    No      No      No      No      Yes     Yes         Yes   Yes
cd /
```

Mögliche Einträge für columns in Access-Table:

```
[1][Ifc.]               : value fixed
[2][Telnet]             : VPN (16), Yes (1), Read (4), No (0)
[3][TFTP]               : VPN (16), Yes (1), Read (4), No (0)
[4][HTTP]               : VPN (16), Yes (1), Read (4), No (0)
[5][SNMP]               : VPN (16), Yes (1), Read (4), No (0)
[6][HTTPS]              : VPN (16), Yes (1), Read (4), No (0)
[7][Telnet-SSL]         : VPN (16), Yes (1), Read (4), No (0)
[8][SSH]                : VPN (16), Yes (1), Read (4), No (0)
[9][SNMPv3]             : VPN (16), Yes (1), Read (4), No (0)
```

IPv6

Pfad:

```
/Setup/IPv6/Firewall/Inbound-Rules
```

Kommando:

```
cd /Setup/IPv6/Firewall/Inbound-Rules

tab Name  Action  Services  Source-Stations  Destination-Services   Active

add "DENYALL" "REJECT" "ANY" "ANYHOST" "ANYHOST" “Yes”

cd/
```

Mögliche Einträge:

```
[1] Name:
36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[5] Action:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[7] Services:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[8] Source-Stations:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[2] Active: Yes (0), No (1)

[3] Prio: 4 chars from 1234567890

[11] Src-Tag: 5 chars from 1234567890

[10] Comment:
64 chars from
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrst
uvwxyz `
```

SSL Protokoll-Versionen festlegen

SSL Protokoll-Version für HTTPS-Verbindungen

Pfad:

```
/Setup/HTTP/SSL
```

Kommando:

```
cd /Setup/HTTP/SSL
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für Telnet-Verbindungen

Pfad:

```
/Setup/Config/Telnet-SSL
```

Kommando:

```
/Setup/Config/Telnet-SSL
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für das CPE WAN Management Protocol, TR-069

Pfad:

```
/Status/CWMP/SSL
```

Kommando:

```
cd /Status/CWMP/SSL
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für RADSEC

Pfad:

```
/Setup/RADIUS/RADSEC
```

Kommando:

```
cd /Setup/RADIUS/RADSEC
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für die Aktions-Tabelle

Pfad:

```
/Setup/WAN/SSL-fuer-Aktions-Tabelle
```

Kommando:

```
cd /Setup/WAN/SSL-fuer-Aktions-Tabelle
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für Seitentabelle im Public Spot Modul

Pfad:

```
/Setup/Public-Spot-Modul/SSL-fuer-Seitentabelle
```

Kommando:

```
cd /Setup/Public-Spot-Modul/SSL-fuer-Seitentabelle
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für E-Mail2SMS-Authentifizierung

Pfad:

```
/Setup/Public-Spot-Modul/Authentifizierungs-Module/E-Mail2SMS-Authentifizierung/SSL
```

Kommando:

```
cd /Setup/Public-Spot-Modul/Authentifizierungs-Module/E-Mail2SMS-
Authentifizierung/SSL

set Versions TLSv1.2

cd/
```

Mögliche Einträge:

```
[3] Versions                        :

Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für RADIUS-Server Authentifizierung

Pfad:

```
/Setup/Public-Spot-Modul/Authentifizierungs-Module/RADIUS-Server/SSL
```

Kommando:

```
cd /Setup/Public-Spot-Modul/Authentifizierungs-Module/RADIUS-Server/SSL

set Versions TLSv1.2

cd/
```

Mögliche Einträge:

```
[3] Versions                        :

Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für das Laden von Firmware, Konfiguration oder Skripten über das Netzwerk

Pfad:

```
Setup/Automatisches-Laden/Netzwerk
```

Kommando:

```
cd Setup/Automatisches-Laden/Netzwerk
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für das zentrale Firmware Management

Pfad:

```
Setup/WLAN-Management/Zentrales-Firmware-Management
```

Kommando:

```
cd Setup/WLAN-Management/Zentrales-Firmware-Management
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

SSL Protokoll-Version für den Rollout Agent

Pfad:

```
Setup/Config/Rollout-Agent/SSL
```

Kommando:

```
cd Setup/Config/Rollout-Agent/SSL
set Versions TLSv1.2
cd/
```

Mögliche Einträge:

```
[3] Versions                        :
Bitmask: SSLv3 (1), TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8)
```

Rücksetzen der SSL-Einstellungen auf Standard-Werte

Ab der LCOS-Version 10.20 RU1 ist es möglich, mit dem Kommandozeilen-Befehl **ssldefaults** die SSL-Einstellungen im jeweiligen Pfad (z.B. Setup/Public-Spot-Module/SSL-for-Page-Table) oder global (im Root-Pfad) auf Standard-Werte zurück zu setzen.

In der Standard-Einstellung sind dann folgende Protokolle aktiv:

- TLSv1
- TLSv1.1
- TLSv1.2

Die Vorgehensweise ist in diesem Knowledge Base Artikel beschrieben.

Kommando:

```
ssldefaults
```

Lokale Verwaltung der Administratoren- und Funktionsrechte

Bei lokalem Rechtemanagement können neben dem Root User weitere Administratoren angelegt werden, um Administratoren mit unterschiedlichen Berechtigungen zu definieren. Lokale Administratoren stehen für alle Konfigurationsprotokolle zur Verfügung.

Pfad:

```
/Setup/Config/Admins
```

Kommando:

```
cd /Setup/Config/Admins
tab  Administrator Password   Active Access-Rights  Function-Rights
add  "Admin"       "******"   Yes    Admin-RO-Limit 0
cd /
```

Mögliche Einträge für columns in Admins:

```
[1][Administrator]      : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/;<=>?[\]^_.0123456789abcdefghijklmnop
                          qrstuvwxyz`
[2][Password]           : 16 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()
                          *+-,/:;<=>?[\]^_.0123456789abcdefghijklmn
                          opqrstuvwxyz `
[4][Active]             : No (1), Yes (0)

[5][Access-Rights]      : none (0), Admin-RO-Limit (8388608), Admin-
                          RW-Limit (8388864), Admin-RO (16777216),
                          Admin-RW (16777472), Supervisor
                          (4294967295)
```

```
[3][Function-Rights]    : Bitmask: Basic-Wizard (0x1),Security-Wizard (0x2),
                                   Internet-Wizard (0x4),RAS-Wizard (0x10),
                                   Provider-Selection (0x8), LANLAN-Wizard (0x20),
                                   Time-Setting (0x40), Device-Search (0x80),
                                   WTP-Assignment-Wizard (0x400),
                                  Rollout-Wizard (0x2000),
                                  Public-Spot-Wizard (0x800), Dynamic-DNS-Wizard
                                  (0x4000), VoIP-CallManager-Wizard (0x8000),
                                  WLC-Profile-Wizard (0x10000), SSH-Command
                                  (0x20000), CF-Profile-Wizard (0x40000), Public
                                  Spot-Xml-Interface (0x80000), Public-Spot-User
                                  Management-Wizard (0x100000), Public-Spot
                                  Configuration-Wizard (0x200000), Prepare-VoIP
                                  Provider-Access (0x800000),
                                  CA-Web-Interface (0x1000000)
```

Im Beispielscript wird ein Administrator eingerichtet, der lesenden Zugriff hat, durch die Limitierung aber keine Tracefunktionen (Limit) und Wizards (Function Rights) ausführen darf!

Read Only Administratoren ist das Auslesen von Passwort Feldern der Konfiguration nicht gestattet.

Bei zentraler Authentisierung der Administratoren können weitere lokale Administratoren-Accounts nicht genutzt werden!

IPv4 Zugangsliste

Über die TCP Zugangs Liste können die Quelladressen von Administratoren pro Routing Kontext (Rtg-Tag) eingeschränkt werden. Nur vertrauenswürdige Quellnetze in Verwaltungsnetzen dürfen für den Konfigurationszugriff freigegeben werden.

Pfad:

```
/Setup/TCP-IP/Access-List
```

Kommando:

```
cd /Setup/TCP-IP/Access-List
tab  IP-Address       IP-Netmask       Rtg-tag
add  10.0.0.0         255.0.0.0        1
cd /
```

Mögliche Einträge für columns in Access-List:

```
[1][IP-Address]         : 15 chars from: 1234567890.
[2][IP-Netmask]         : 15 chars from: 1234567890.
[3][Rtg-tag]            : 5 chars from: 1234567890
```

Werden keine Adressen in der Zugangs Liste definiert**, ist der Zugriff von jeder Quelladresse erlaubt!**

IPv6 Zugangsliste

Pfad:

/Setup/IPv6/Firewall/Inbound-Rules

Kommando:

cd /Setup/IPv6/Firewall/Inbound-Rules

tab Name Action Services Source-Stations Destination-Services Active

add "DENYALL" "REJECT" "ANY" "ANYHOST" "ANYHOST" “Yes”

cd/

Mögliche Einträge:

[1] Name:
36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[5] Action:
64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[7] Services:
64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[8] Source-Stations:
64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[2] Active: Yes (0), No (1)

[3] Prio: 4 chars from 1234567890

[11] Src-Tag: 5 chars from 1234567890

[10] Comment:
64 chars from
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz `

Remote Dial-In Berechtigung

Per Default ist eine ISDN Remote Konfiguration erlaubt. Für die Einwahl ist eine PPP Authentisierung mit dem Usernamen Admin und dem Root Konfigurationspasswort möglich. Die Remote Konfiguration kann auf eine spezielle MSN eingeschränkt werden.

Sollen die ISDN Interfaces für abgehende Verbindungen genutzt, aber keine ISDN Fernkonfiguration ermöglicht werden, können eingehende Verbindungen für alle ISDN Interfaces unterbunden werden.

Sollen auch eingehende Verbindungen möglich sein, müssen diese auf geprüfte Caller IDs eingeschränkt werden.

Deaktivieren der ISDN Interfaces für eingehende Rufe:

Pfad:

```
/Setup/Interfaces/S0
```

Kommando:

```
cd /Setup/Interfaces/S0

tab  Ifc   Max-in-calls

set  S0-1  Zero

cd /
```

Mögliche Einträge für columns in S0:

```
[1][Ifc]                : value fixed

[13][Max-in-calls]      : Zero (2), One (1), Two (0)
```

Einschränken eingehender Rufe auf geprüfte Caller IDs:

Pfad:

```
/Setup/WAN

/Setup/WAN/Incoming-Calling-Numbers
```

Kommando:

```
set /Setup/WAN/Protect screened
```

Mögliche Einträge:

```
Protect                  :none (0), number (2), screened (4)
```

```
cd /Setup/WAN/Incoming-Calling-Numbers
tab  Dialup-remote                    Peer
add  "2405499360"                     "OFFICE-DIALIN"
cd /
```

Mögliche Einträge für columns in Incoming-Calling-Numbers:

```
[1][Dialup-remote]      : 31 chars from: 0123456789S*#-EF:
[2][Peer]               : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
```

Session Management

Um zu vermeiden, dass Konfigurationsverbindungen ungerechtfertigt übernommen werden, ist die Leerlauf-Dauer einer Konfigurationsverbindung zu beschränken.

Pfad:

```
/Setup/Config
```

Kommando:

`set /Setup/Config/Config-Aging-Minutes 15` (für TCP basierte Verbindungen)

`set /Setup/Config/Outband-Aging-Minutes 5` (für serielle Verbindung)

Layer 2 Management

Das LCOS unterstützt für ein desaster recovery das LANCOM Layer 2 Management Protokoll LL2M, um Geräte ohne direkten physikalischen Zugang über Ethernet authentisiert umzukonfigurieren oder auf die factory default Einstellungen zurückzusetzen.

Soll diese Funktion nicht genutzt werden, ist sie zu deaktivieren. Bei aktiviertem Layer 2 Management empfiehlt sich die Einschränkung auf einen konfigurierbaren Zeitraum in Sekunden, der nach dem Reboot des entsprechenden Gerätes für Layer 2 Managementzugriffe zur Verfügung steht.

Pfad:

```
/Setup/Config/LL2M
```

Kommando:

```
set /Setup/Config/LL2M/Operating No

set /Setup/Config/LL2M/Time-Limit 0
```

Mögliche Einträge:

```
Operating                : No (0), Yes (1)

Time-Limit               : 10 chars from: 1234567890
```

Diebstahlschutz

Der Betrieb des IP Routers kann an eine Standortüberprüfung gekoppelt werden. Diese Diebstahlschutz Funktion schränkt den Betrieb des LANCOM Routers auf vorgegebene Standorte ein.

Der Betrieb eines gestohlenen LANCOM Routers wird bedeutend erschwert bis unmöglich gemacht. Zur Standortüberprüfung stehen in absteigender Sicherheitabstufung je nach Gerätetyp die Funktionen GPS, Rufweiterleitungsüberprüfung und Selbstanruf zur Verfügung.

Die bestmögliche zur Verfügung stehende Diebstahlschutz Funktion sollte zum Einsatz kommen.

Pfad:

```
/Setup/Config/Anti-Theft-Protection
```

Kommando:

```
set /Setup/Config/Anti-Theft-Protection/Enabled No
set /Setup/Config/Anti-Theft-Protection/Method Basic-Call
set /Setup/Config/Anti-Theft-Protection/ISDN-Ifc S0-1
set /Setup/Config/Anti-Theft-Protection/Called-Number ""
set /Setup/Config/Anti-Theft-Protection/Outgoing-Calling-Number ""
set /Setup/Config/Anti-Theft-Protection/Checked-Calling-Number ""
```

Mögliche Einträge:

```
Enabled                  : No (0), Yes (1)
Method                   : Basic-Call (0), Facility (1), GPS
ISDN-Ifc                 : S0-1 (1), S0-2 (2)
Called-Number            : 14 chars from: 0123456789S*#-EF:
Outgoing-Calling-Number  : 14 chars from: 0123456789S*#-EF:
Checked-Calling-Number   : 14 chars from: 0123456789S*#-EF:
```

Offline Konfigurationen

Die Konfiguration von LCOS basierten Geräten kann für eine Offline Bearbeitung und zur Archivierung ausgelesen werden. Die Konfiguration kann in zwei unterschiedlichen Formaten ausgelesen werden, LANconfig Konfiguration „.lcf“ bzw. LANCOM Script Konfiguration „.lcs“.

Die LANconfig Konfiguration stellt ein vollständiges Abbild der LANCOM Konfiguration dar. Insbesondere enthält diese Konfigurationsdatei das Root Konfigurationspasswort in auslesbarer Form!

Die LANCOM Script Konfigurationen enthalten nach dem Auslesen alle Passwörter mit Ausnahme des Root Konfigurationspasswortes in Klartext Form.

Kommando:

`Readconfig`	(LANconfig File Format)
`Reascript`	(LANCOM Script Format)

Die Kommandos sind jeweils über tftp, serielle Konsole, http, https, Telnet, Telnet SSL und SSH ausführbar.

Das Auslesen vollständiger Konfigurationen über die genannten Befehle ist ausschließlich Administratoren mit Supervisor Rechten gestattet!

Sämtliche LANCOM Konfigurationsdateien sind als sicherheitsrelevant zu bewerten und entsprechend gesichert zu archivieren!

Interne Dienste und Logging

Dienstaktivierung

Das LCOS stellt zahlreiche interne Dienste zur Verfügung. Nicht benötigte Dienste sind zu deaktivieren, um unerwünschte Nutzung zu unterbinden.

DHCP

Soll die dynamische IP Adresszuteilung duch den DHCP Dienst des LCOS nicht verwendet werden, kann diese Funktion pro ARF Kontext separat geschaltet werden.

Pfad:

```
/Setup/DHCP/Network-list
```

Kommando:

```
cd /Setup/DHCP/Network-list
tab  Network-name      Operating
add  "INTRANET"        No
cd /
```

Mögliche Einträge für columns in Network-list:

```
[1][Network-name]       : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*
                          +-,/:;<=>?[\]^_.0123456789
[11][Operating]         : No (0), Yes (1), Auto (2), Relay (16),
                          Client (4)
```

DNS

Der DNS Server des LCOS ist in der Lage statisch konfigurierte Namen sowie über DHCP und NetBIOS gelernte Namen aufzulösen. Soll diese Funktion nicht genutzt werden ist der Dienst zu deaktivieren.

Das DNS Forwarding zu einem definierten DNS Server ist hiervon nicht betroffen! **DNS und der NetBIOS Proxy arbeiten ausschließlich als lokale Dienste und haben keine Verbindung zum WAN.**

Pfad:

```
/Setup/DNS
```

Kommando:

```
set /Setup/DNS/Operating No
```

Mögliche Einträge:

```
Operating                : No (0), Yes (1)
```

NetBIOS Proxy

Der NetBIOS Proxy des LANCOMs lernt automatisch Namensstrukturen aus Windows Netzwerken und beantwortet NetBIOS Namensanfragen. Soll diese Funktion nicht genutzt werden, ist sie global oder pro ARF Kontext zu deaktivieren.

Pfad:

```
/Setup/NetBIOS
```

Kommando:

```
set /Setup/NetBIOS/Operating No                (global)
```

Mögliche Einträge:

```
Operating                : No (0), Yes (1)
```

```
cd /Setup/NetBIOS/Networks                     (pro ARF Kontext)
tab  Network-name      Operating  NT-Domain
add  "INTRANET"        No              ""
cd /
```

Mögliche Einträge für columns in Networks:

```
[1][Network-name]       : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[2][Operating]          : No (0), Yes (1)
[3][NT-Domain]          : 15 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
```

LANCAPI

Der LANCAPI Dienst des LCOS stellt die abhängig vom Gerätetyp vorhandenen ISDN Interfaces für die Nutzung über eine Remote CAPI bereit. Die Kontrolle der ISDN Interfaces wird in diesem Fall von der LANCAPI übernommen. Die Verfügbarkeit des LANCAPI Dienstes kann auf bestimmte Quelladressen eingeschränkt werden.

Seit der LCOS Version 10.00 RU1 können LANCAPI-Verbindungen von der WAN-Seite grundsätzlich nur noch über VPN-Verbindungen aufgebaut werden. Der Zugriff über unmaskierte WAN-Verbindungen ist nicht mehr möglich. Diese Einstellung kann in der Firmware nicht verändert werden!

Pfad:

```
/Setup/LANCAPI/Access-List
```

Kommando:

```
cd /Setup/LANCAPI/Access-List
tab  IP-Address       IP-Netmask       Rtg-tag
add  10.0.0.0         255.0.0.0        1
cd /
```

Soll die LANCAPI nicht genutzt werden, ist der Dienst im LCOS pro ISDN Interface zu deaktivieren.

Pfad:

```
/Setup/LANCAPI/Interface-List
```

Kommando:

```
cd /Setup/LANCAPI/Interface-List
tab  Ifc   Operating
set  S0-1  No
set  S0-2  No
cd /
```

Quell-Routen Überprüfung

Die Dienste im LCOS sind in der Lage eine Quell-Routen Überprüfung durchzuführen. In den Default Einstellungen akzeptiert das LCOS Zugriffe auf die internen Dienste unabhängig von der Quell Adresse.

Dies ermöglicht die Remote Administration eines LANCOMs, das keine konfigurierte Rückroute enthält. Soll die Administration nur aus explizit im Routing konfigurierten Quell Netzen möglich sein, ist die Überprüfung der Quell-Routen für interne Dienste zu aktivieren (Src-check: strict).

Pfad:

```
/Setup/TCP-IP/Network-list
```

Kommando:

```
cd /Setup/TCP-IP/Network-list
tab  Network-name      Src-check
add  "INTRANET"        strict
cd /
```

Mögliche Einträge für columns in Network-list:

```
[1][Network-name]       : 17 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[6][Src-check]          : strict (1), loose (0)
```

Zeiteinstellungen

Um Status Informationen im zeitlichen Zusammenhang auswerten zu können, sollte auf dem Gerät eine Zeitsynchronisation per NTP Dienst eingerichtet sein. Werden Authentisierungen über digitale Zertifikate durchgeführt, ist eine synchronisierte Zeit im LCOS zwingend notwendig.

Pfad:

```
/Setup/Time

/Setup/NTP

/Setup/NTP/RQ-Address
```

Kommando:

```
set /Setup/Time/Fetch-Method NTP


set /Setup/NTP/RQ-Interval 86400

set /Setup/NTP/RQ-Tries 4


cd /Setup/NTP/RQ-Address

tab  RQ-Address                        Loopback-Addr.

add  "NTPS1-0.CS.TU-BERLIN.DE"         "INTRANET"

add  "NTPS1-1.CS.TU-BERLIN.DE"         "INTRANET"

cd /
```

Der LANCOM Router kann die Zeit als Zeitserver intern bereitstellen. Soll dieser Dienst nicht genutzt werden, ist der Zeitserver zu deaktivieren.

Pfad:

```
/Setup/NTP/Server-Operating
```

Kommando:

```
set /Setup/NTP/Server-Operating No
```

MD5-Authentifizierung für NTP-Server

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Server.

Pfad:

```
/Setup/NTP
```

Kommando:

```
set /Setup/NTP/Server-Authentication Yes
```

MD5-Schlüssel

Der Eintrag enthält den Wert des/der Schlüssel.

Pfad:

```
/Setup/NTP/Authentication Keys
```

Kommando:

```
cd /Setup/NTP/Authentication Keys

tab Key-ID                      Key

add "1"         "dsajfndyjkvhfhgh"
```

Mögliche Werte:

```
[1] Key-ID: 10 chars from 1234567890

[2] Key: 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-
,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz `
```

Vertrauenswürdige-Schlüssel

Enthält die Liste der vertrauenswürdigen Schlüssel (kommaseparierte Liste aus Schlüsselnummern).

Pfad:

```
/Setup/NTP/Server-Trusted_Keys
```

Kommando:

```
set /Setup/NTP/Server-Trusted_Keys [0-9,..]
```

MD5-Authentifizierung für NTP-Client

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Client.

Pfad:

```
/Setup/NTP/RQ-Address
```

Kommando:

```
cd /Setup/NTP/RQ-Address

cd <Listeneintrag>

set Authentication-Enabled yes
```

Schlüsselnummer

Kennzeichnet den zur MD5-Authentifizierung verwendeten Schlüssel für den Client.

Pfad:

```
/Setup/NTP/RQ-Address
```

Kommando:

```
cd /Setup/NTP/RQ-Address

cd <Listeneintrag>

set Key-ID [1 … 65535]
```

Mögliche Werte:

```
[1] RQ-Address:
64 chars from
ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789abcdefghijklmn
opqrstuvwxyz`

[2] Loopback-Addr.:
39 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789

[3] Authentication-Enabled: No (0), Yes (1)

[4] Key-ID: 10 chars from 1234567890
```

Internes und externes Event-Logging

Um interne Abläufe im LCOS möglichst lückenlos dokumentieren zu können, sollten Syslog Events lokal sowie auf einem externen Server aufgezeichnet werden. Um die Anzahl der Informationen überschaubar zu halten, sollten die Quellen und Prioritäten dem Verwendungszweck angepasst werden.

Der **Parameter Log-CLI-Changes** aktiviert das Protokollieren der Kommandozeilenbefehle. Aktivieren Sie diesen Parameter, um bei der Ausführung eines Befehls an der Kommandozeile des Gerätes einen Eintrag im internen SYSLOG-Speicher vorzunehmen.

Pfad:

```
/Setup/SYSLOG

/Setup/SYSLOG/Server
```

Kommando:

```
set /Setup/SYSLOG/Operating Yes

set /Setup/SYSLOG/ Log-CLI-Changes Yes


cd /Setup/SYSLOG/Server

tab  Idx.    IP-Address       Source  Level   Loopback-Addr.

add  "0001"  127.0.0.1        ff      07      "INTRANET"    (intern)

add  "0002"  10.1.1.11        ff      07      "INTRANET"    (extern)

cd /
```

Das Beispielscript aktiviert Syslog Nachrichten aus allen Quellen mit Level ab Warnung.

IP und Routing

Loopback Adressen

Sollen die LANCOM Router zusätzlich zu den Interface gebundenen IP Adressen über einzelne Management IP Adressen erreichbar sein, können benamte Loopbackadressen konfiguriert und für aktive und passive Kommunikation des LANCOMs genutzt werden.

Die Loopback Adressen müssen im Routing des Netzes berücksichtig werden und können den internen Diensten des LANCOMs als Absenderadressen zugeordnet werden. Über das Routing Tag werden die Loopback Adressen ARF Kontexten zugeordnet.

Pfad:

```
/Setup/TCP-IP/Loopback-List
```

Kommando:

```
cd /Setup/TCP-IP/Loopback-List
tab  Name              Loopback-Addr.    Rtg-tag
add  "MANAGEMENT"      10.1.2.3          1
cd /
```

Den internen Diensten, die aktiv kommunizieren, können Loopback Adressen als Absenderadressen zugeordnet werden:

Syslog:

```
/Setup/SYSLOG/Server
```

E-Mail:

```
/Setup/Mail
```

NTP:

```
/Setup/NTP/RQ-Address
```

SCEP:

```
/Setup/Certificates/SCEP-Client/CAs
```

Definition virtueller Router

Abhängig vom Gerätetyp stellt das LCOS zwei bis 64 virtuelle Router zur Verfügung, die über Routing Tags voneinander getrennt werden können.

Diese virtuellen Router oder ARF Kontexte können an physikalische Interfaces und/oder VLANs gebunden werden. Gleiche Routing Tags erlauben ein Routing zwischen den entsprechenden Netzen, unterschiedliche Routing Tags separieren Netze voneinander.

Das Routing Tag wird als Filter über die Routing Tabelle gelegt und bestimmt somit die zur Verfügung stehenden Routen je ARF Kontext.

Pfad:

```
/Setup/TCP-IP/Network-list
```

Kommando:

```
cd /Setup/TCP-IP/Network-list
tab  Network-name IP-Address IP-Netmask   VLAN-ID  Interface Rtg-tag
add  "INTRANET-1" 10.1.1.11  255.255.0.0  1        LAN-1     1
add  "INTRANET-2" 10.2.1.11  255.255.0.0  2        LAN-1     1
add  "OFFICE"     10.5.1.11  255.255.0.0  5        LAN-1     5
cd /
```

Die Zuordnung der ARF Netze zu VLANs und Interfaces kann über das Kommando `show bindings` überprüft werden:

```
Ifc.: LAN-1
INTRANET          10.1.1.11       255.255.0.0    1
OFFICE            10.5.1.11       255.255.0.0    5
```

Das Beispielscript richtet drei Netze ein, von denen INTRANET-1 und INTRANET-2 aufgrund des gleichen Routing Tags durch den Router verbunden werden und das Netz OFFICE von den anderen separiert wird.

Es ist sicher zu stellen, dass voneinander zu separierende Netze mit unterschiedlichen Routing Tags ausgestattet sind!

Das Schnittstellen Tag 0 bewirkt eine gesonderte Behandlung eines Netzes als Supervisor Netz, das auf alle anderen Netze Zugriff hat und ist somit mit besonderer Vorsicht zu verwenden!

Verwendung virtueller Router im Routing

Die Routing Tags bestimmen die Auswahl der sichtbaren Routen aus der globalen Routingtabelle. ARF Kontexte können Routen nutzen, die dasselbe Routing Tag tragen, das dem ARF Kontext zugewiesen wurde.

Des Weiteren sind Routen mit dem Routing Tag 0 aus allen Kontexten heraus gemeinsam nutzbar.

Pfad:

```
/Setup/IP-Router/IP-Routing-Table
```

Kommando:

```
cd /Setup/IP-Router/IP-Routing-Table
tab  IP-Address IP-Netmask    Rtg-tag  Peer-or-IP
add  10.11.0.0  255.255.0.0   1        "VPN-INTRANET”
add  10.15.0.0  255.255.0.0   5        "VPN-OFFICE”
cd /
```

Es ist sicher zu stellen, dass Routing Tag des jeweiligen ARF Kontextes mit den zugeordneten Routen übereinstimmt und keine fehlerhaften Beziehungen zu ungewolltem Forwarding führen.

WAN seitig empfangenen IP Paketen wird standardmäßig das Routing Tag 0 zugewiesen. In dieser Konfiguration sind alle lokalen Netze prinzipiell erreichbar.

Soll die ARF Routingzuordnung automatisch bidirektional auch für empfangene Daten gelten, muß das Routing Tag automatisch aus der Quellroute bestimmt werden.

Pfad:

```
/Setup/IP-Router
```

Kommando:

```
set /Setup/IP-Router/WAN-Tag-Creation Auto
```

Mögliche Einträge:

```
WAN-Tag-Creation          : Manual (0), Auto (1)
```

Soll mit dynamischem Routing gearbeitet werden, kann das Routing Tag für dynamisch zu lernende Routen der Gegenstelle zugeordnet werden. Dynamisch gelernte Routen erhalten dann das Routing Tag der jeweiligen Gegenstelle.

Pfad:

```
/Setup/IP-Router/Tag-Table
```

Kommando:

```
cd /Setup/IP-Router/Tag-Table
tab  Peer              Rtg-tag  Start-WAN-Pool   End-WAN-Pool
add  "OFFICE-*"        5        0.0.0.0          0.0.0.0
cd /
```

Mögliche Einträge für columns in Tag-Table:

```
[1][Peer]               : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*
                          +-,/:;<=>?[\]^_.0123456789
[2][Rtg-tag]            : 5 chars from: 1234567890
[3][Start-WAN-Pool]     : 15 chars from: 1234567890.
[4][End-WAN-Pool]       : 15 chars from: 1234567890.
```

Um Gegenstellen zu Gruppen zusammenfassen zu können, ist das Zeichen * als Wildcard nutzbar. Gegenstellen mit demselben definierten Namensbeginn erhalten das zugewiesene Routing Tag und können im Falle von Einwahl Clients, wie VPN Clients Adressen aus einem individuellen Pool zugewiesen bekommen.

Das ARF mit seinen Interface, VLAN und Routing Tag Zuordnungen stellt den zentralen Punkt der Verbindung oder Trennung von Netzen dar. **Es ist sicherzustellen, dass ARF Kontexte ausschließlich mit den beabsichtigten Routen und Gegenstellen über das Routing Tag verknüpft werden!**

Routing Tags können über die Firewall für Zwecke des Policy based Routing umgesetzt werden. **Firewall Regeln sind auf korrekte Behandlung des Routing Tags zu überprüfen, um die korrekte Trennung der ARF Kontexte sicherzustellen!**

Dynamisches Routing

Das LCOS unterstützt RIPv2, OSPFv2 (ab LCOS 10.12) und BGPv4 als dynamische Routing Protokolle.

RIPv2

Da RIPv2 ohne Authentisierung arbeitet, darf dynamisches Routing nur von vertrauenswürdigen lokalen Netzen und Gegenstellen aktiviert werden.

LAN

Pfad:

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

Kommando:

```
cd /Setup/IP-Router/RIP/LAN-Sites
tab  Network-name      RIP-Type    RIP-Accept
add  "OFFICE"          RIP-2       Yes
cd /
```

Mögliche Einträge:

```
[1][Network-name]       : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[2][RIP-Type]           : Off (0), RIP-1 (1), R1-comp (2), RIP-2 (3)
[3][RIP-Accept]         : No (0), Yes (1)
```

WAN

Pfad:

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

Kommando:

```
cd /Setup/IP-Router/RIP/WAN-Sites
tab  Peer              RIP-Type    RIP-Accept
add  "OFFICE-PPTP"     RIP-2       Yes
cd /
```

Mögliche Einträge:

```
[1][Peer]               : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*
                          +-,/:;<=>?[\]^_.0123456789
[2][RIP-Type]           : Off (0), RIP-1 (1), R1-comp (2), RIP-2 (3)
[3][RIP-Accept]         : No (0), Yes (1)
```

Um missbräuchliche Manipulation der Routing Information zu verhindern, ist es auszuschließen, dass RIP die Routinginformationen von unberechtigten Teilnehmern in das Netz propagiert.

Im LAN arbeitet RIPv2 auf Multicast-Basis. Es ist sicherzustellen, dass der Zugriff auf das physikalische Ethernet nur vertrauenswürdigen Netzwerk Teilnehmern gewährt wird.

Auf WAN Verbindungen ist darauf zu achten, dass RIP nur von vertrauenswürdigen Gegenstellen akzeptiert wird und gerichtete RIP Unicasts auf WAN Verbindungen nicht weitergeleitet werden.

OSPFv2

OSPF unterstützt ab LCOS 10.12 die Authentisierung einer Schnittstelle. Es wird empfohlen, den Authentisierungstyp „Cryptographic-MD5“ zu nutzen. Das Passwort sollte zufällig gewählt sein und mindestens acht Zeichen umfassen.

Pfad:

```
/Setup/Routing-Protocols/OSPF/Interfaces
```

Kommando:

```
cd /Setup/Routing-Protocols/OSPF/Interfaces

tab Interface     OSPF-Instance     Area-ID     Authentication-Type  Authentication-
Key

add INTRANET            DEFAULT           0.0.0.0     Cryptographic-MD5       ********

cd /
```

Mögliche Einträge für Interfaces:

```
[1] Interface:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789

[2] OSPF-Instance:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789

[3] Area-ID:
15 chars from 1234567890.

[11] Authentication-Type:
Null (0), Simple-Password (1), Cryptographic-MD5 (2)

[12] Authentication-Key:
16 chars from
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrst
uvwxyz `
```

Bei der Nutzung von virtuellen Links (Transit-Area) um Areas mit der Backbone Area zu verbinden, sollten Sie ebenfalls den Authentisierungstyp „Cryptographic-MD5“ für den virtuellen Link konfigurieren.

Pfad:

```
/Setup/Routing-Protocols/OSPF/Virtual-Links
```

Kommando:

```
cd /Setup/Routing-Protocols/OSPF/Virtual-Links

tab OSPF-Instance Transit-Area-ID   Router-ID   Authentication-Type
      Authentication-Key

add DEFAULT             1.2.3.4           1.1.1.1     Cryptographic-MD5
      ********

cd /
```

Mögliche Einträge für Virtual-Links:

```
[1] OSPF-Instance:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789

[2] Transit-Area-ID:
15 chars from 1234567890.

[3] Router-ID:
15 chars from 1234567890.

[4] Authentication-Type:
Null (0), Simple-Password (1), Cryptographic-MD5 (2)

[5] Authentication-Key:
16 chars from
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrst
uvwxyz `
```

BGPv4

Sie haben die Möglichkeit Ihren BGP-Nachbarn mit einem Passwort zu authentifizieren. Das Passwort sollte zufällig gewählt sein und muss mindestens acht Zeichen umfassen.

Pfad:

```
/Setup/Routing-Protocols/BGP/Neighbors
```

Kommando:

```
cd /Setup/Routing-Protocols/BGP/Neighbors
tab IP-Address    Port  Remote-AS   Name        Operating   Password
add 10.10.10.10   179   65000       NEIGHBOR1   yes         ********
cd /
```

Mögliche Einträge für Neighbors:

```
[1] IP-Address:
56 chars from 0123456789ABCDEFabcdef:./
[2] Port:
5 chars from 1234567890
[5] Remote-AS:
10 chars from 1234567890
[6] Name:
16 chars from 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[7] Operating:
No (0), Yes (1)
[8] Password:
16 chars from
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrst
uvwxyz `
```

Proxy ARP

Um remote Netze und IP Adressen, die innerhalb eines lokal definierten IP Netzes liegen, über WAN Verbindungen einzubinden, wird der Mechanismus Proxy ARP verwendet.

Wird dieser Mechanismus nicht explizit gewünscht und sollen lokale IP Adressen ausschließlich in der lokalen Ethernet-Umgebung genutzt werden, ist Proxy ARP zu deaktivieren.

Pfad:

```
/Setup/IP-Router
```

Kommando:

```
set /Setup/IP-Router/Proxy-ARP No
```

Mögliche Einträge:

```
Proxy-ARP                : No (0), Yes (1)
```

Stealth-Modus

Eine umstrittene Methode, die Sicherheit zu erhöhen, ist das Verstecken des Routers. indem TCP- und UDP-Anfragen nicht mehr normgerecht abgelehnt, sondern ignoriert werden (Stealth-Modus). Dies ist insofern umstritten, als auch ein Nichtantworten auf die Existenz eines Gerätes schließen lässt.

Ist nämlich wirklich kein Gerät vorhanden, so beantwortet der jeweils vorherige Router die entsprechenden Pakete mit "nicht zustellbar", da er sie wirklich nicht zustellen kann. Antwortet hingegen der jeweils vorherige Router nicht mit einer entsprechenden Ablehnung, so war das Paket für ihn zustellbar und unabhängig vom darauf folgenden Verhalten des Empfängers ist dieser auf jeden Fall vorhanden.

Das Verhalten des jeweils vorherigen Routers kann nicht simuliert werden, ohne Ihr Gerät wirklich offline (und damit auch für selbst angeforderte Dienste unerreichbar) zu halten oder abzuschalten.

Pfad:

```
/Setup/IP-Router/Firewall
```

Kommando:

```
set /Setup/IP-Router/Firewall WAN
```

Mögliche Einträge:

```
Ping-Block    :off (0), always (1), WAN (2), default-route (3)
```

VPN und Firewall

IKEv1 Authentisierung

IKEv1 unterstützt verschiedene Authentisierungsmethoden (Main Mode und Aggressive Mode jeweils mit Pre Shared Key und Zertifikatsauthentifizierung).

Der Aggressive Mode ist als offline angreifbar zu betrachten und sollte außer in begründeten Ausnahmefällen in sicherheitsrelevanten Umgebungen nicht zum Einsatz kommen.

Das LCOS unterstützt zur Vermeidung des Aggressive Mode zwei Verfahren, die auch die Anbindung von IPSec Gegenstellen mit dynamischen IP Adressen zulassen, Main Mode mit Zertifikatsauthentifizierung und LANCOM dynamic VPN mit Main Mode und Pre Shared Key Authentisierung.

LANCOM empfiehlt die Nutzung des Main Mode mit Zertifikatsauthentifizierung.

Pfad

```
/Setup/VPN/VPN-Peers
```

Kommando:

```
cd /Setup/VPN/VPN-Peers
tab  Peer          Layer        dynamic     IKE-Exchange
add  "OFFICE-VPN"  PAR-OFFICE   Yes         Main-Mode
cd /
```

Mögliche Einträge:

```
[1][Peer]               : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[4][Layer]              : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[5][dynamic]            : No (0), ICMP (4), UDP (8)
[7][IKE-Exchange]       : Main-Mode (0), Aggressive-Mode (1)
```

Der Layer definiert den Proposalsatz pro VPN Gegenstelle. Über die IKE (Phase 1) Proposals wird festgelegt, ob mit PSK oder Zertifikaten authentisiert wird.

Pfad:

```
/set/vpn/layer
/Setup/VPN/Proposals/IKE-Proposal-Lists
```

Kommando:

```
cd /Setup/VPN/Layer
tab  Name              IKE-Prop-List
add  "PAR-OFFICE"      " IKE_RSA_SIG "
cd /
```

Mögliche Einträge für Layer:

```
[1][Name]               : 16 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[5][IKE-Prop-List]      : 17 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
```

```
cd /Setup/VPN/Proposals/IKE-Proposal-Lists
tab  IKE-Proposal-List  IKE-Proposal-1
add  "IKE_RSA_SIG"      "RSA-AES-MD5"
cd /
```

Mögliche Einträge für IKE-Proposal-Lists:

```
[1][IKE-Proposal-Lists] : 17 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[2][IKE-Proposal-1]     : 17 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
```

```
cd /Setup/VPN/Proposals/IKE
tab  Name              IKE-Auth-Mode
add  "RSA-AES-MD5"     RSA-Signature
cd /
```

Mögliche Einträge für IKE:

```
[1][Name]               : 17 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[5][IKE-Auth-Mode]      : Preshared-Key (1), RSA-Signature (3)
```

Bei der Verwendung von Zertifikaten ist auf eine sinnvolle Zertifikatslebensdauer zu achten und möglichst ein automatisiertes Zertifikats Rollout Verfahren mit dem Protokoll SCEP zu nutzen!

Bei der Verwendung von Pre Shared Key (PSK) ist auf einen manuellen Schlüsselwechsel in geeigneten Zeiträumen zu achten!

IKEv1 Verschlüsselung

Das LCOS unterstützt verschiedene Verschlüsselungsalgorithmen mit unterschiedlichen Schlüsseltiefen und Hash Algorithmen.

Der Schlüsselaustausch über Diffie Hellman kann mit den Gruppen 1, 2, 5, 14, 15, 16 durchgeführt werden.

LANCOM empfiehlt für die IKE Phase 1 die Nutzung des Verschlüsselungsalgorithmus AES-CBC mit einer Schlüsseltiefe von 256 Bit, den Hash-Algorithmus SHA256 und die Diffie-Hellman Gruppe 16.

Pfad:

```
/Setup/VPN/Proposals/IKE
```

Kommando:

```
cd /Setup/VPN/Proposals/IKE

tab   Name                    IKE-Crypt-Alg          IKE-Crypt-Keylen       IKE-
Auth-Alg

add   RSA-AES256-SHA256 AES-CBC          256               SHA256

cd/
```

Mögliche Einträge für IKE:

```
[1] Name: 17 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789

[2] IKE-Crypt-Alg: AES-CBC (7), BLOWFISH-CBC (3), CAST128-CBC (6), 3DES-CBC (5), DES-
CBC (1), NULL (42)

[3] IKE-Crypt-Keylen: 5 chars from 1234567890

[4] IKE-Auth-Alg: MD5 (1), SHA1 (2), SHA-256 (4), SHA-384 (5), SHA-512 (6)
```

Das konfigurierte IKE Proposal muss einer Proposal Liste hinzugefügt werden.

Pfad:

```
/setup/VPN/Proposals/IKE-Proposal-Lists
```

Kommando:

```
cd /setup/VPN/Proposals/IKE-Proposal-Lists

tab   IKE-Proposal-Lists      IKE-Proposal-1

Add   IKE-List                RSA-AES256-SHA256

cd/
```

Mögliche Einträge für IKE-Proposal-Lists:

```
[1] IKE-Proposal-Lists: 17 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789

[2] IKE-Proposal-1: 17 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789
```

Für die IPsec Phase (IKE Phase 2) empfehlen wir die Nutzung von ESP im Tunnel Modus, den Verschlüsselungsalgorithmus AES-CBC mit einer Schlüsseltiefe von 256 Bit und den Hash-Algorithmus SHA256. Die Konfiguration von AH (Authentication Header) ist ebenfalls möglich.

Da AH jedoch keine Verschlüsselung bietet, raten wir von der Nutzung ab.

Pfad:

```
/Setup/VPN/Proposals/IPSEC
```

Kommando:

```
cd /Setup/VPN/Proposals/IPSEC

TAB   Name               Encaps-Mode       ESP-Crypt-Alg     ESP-Crypt-Keylen  ESP-
Auth-Alg          AH-Auth-Alg

add   TN-AES256-MD5      Tunnel            AES-CBC           256               HMAC-
SHA-256           none
```

Mögliche Einträge für IPSEC:

```
[1] Name: 17 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789

[2] Encaps-Mode: Tunnel (1), Transport (2), Mixed(LCOS4) (65001)

[3] ESP-Crypt-Alg: none (0), AES-CBC (12), BLOWFISH-CBC (7), CAST128-CBC (6), 3DES-
CBC (3), DES-CBC (2), NULL (11)

[4] ESP-Crypt-Keylen: 5 chars from 1234567890

[5] ESP-Auth-Alg: none (0), HMAC-MD5 (1), HMAC-SHA1 (2), HMAC-SHA-256 (5), HMAC-SHA-
384 (6), HMAC-SHA-512 (7)

[6] AH-Auth-Alg: none (0), HMAC-MD5 (1), HMAC-SHA1 (2), HMAC-SHA-256 (5), HMAC-SHA-
384 (6), HMAC-SHA-512 (7)
```

Auch das IPsec Proposal muss einer Proposal Liste hinzugefügt werden.

Pfad:

```
/setup/VPN/Proposals/IPSEC-Proposal-Lists
```

Kommando:

```
cd /setup/VPN/Proposals/IPSEC-Proposal-Lists

Tab   IPSEC-Proposal-Lists   IPSEC-Proposal-1

Add   ESP_TN                 TN-AES256-SHA256

cd/
```

Mögliche Einträge für IPSEC-Proposal-Lists:

```
[1] IPSEC-Proposal-Lists : 17 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789

[2] IPSEC-Proposal-1     : 17 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-
,/:;<=>?[\]^_.0123456789
```

IKEv2 Authentisierung

Unter IKEv2 haben Sie die Wahl aus drei unterschiedlichen Authentisierungsmethoden:

PSK = Authentifizierung mittels PreShared Key

RSA = Zertifikatsbasierte Authentifizierung

RSASSA-PSS = Zertifikatsbasierte Authentifizierung + probabilistisches Signaturverfahren

LANCOM Router unterstützen ebenfalls das ältere probabilistisches Signaturverfahren gemäß rsassa-pkcs1-v1_5. LANCOM empfiehlt an dieser Stelle jedoch die Nutzung von RSASSA-PSS.

Pfad:

```
Setup/VPN/IKEv2/Auth/Parameter/
```

Kommando:

```
cd Setup/VPN/IKEv2/Auth/Parameter/

tab   Name        Local-Auth        Local-Dig-Sig-Profile   Remote-Auth
      Remote-Dig-Sig-Profile

add   VPN-AUTH    digital-signature      default-rsa-pss         digital-signature
      default-rsa-pss

cd /
```

Mögliche Einträge für Parameter:

```
[1] Name:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[2] Local-Auth:
RSA-Signature (1), PSK (2), Digital-Signature (14)

[13] Local-Dig-Sig-Profile:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[6] Remote-Auth:
RSA-Signature (1), PSK (2), Digital-Signature (14)

[14] Remote-Dig-Sig-Profile:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
```

Das ausgewählte Digital-Signature-Profil bestimmt das genutzt Verfahren und die für die Aushandlung zur Auswahl stehenden Hash-Algorithmen.

Pfad:

```
/Setup/VPN/IKEv2/Auth/Digital-Signature-Profiles
```

Kommando:

```
cd /Setup/VPN/IKEv2/Auth/Digital-Signature-Profiles

tab   Name              Auth-Method               Hash-Algorithms

add   DEFAULT-RSA-PSS   RSASSA-PSS                SHA-512,SHA-384,SHA-256

cd/
```

Mögliche Einträge für Digital-Signature-Profiles:

```
[1] Name:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[2] Auth-Method:
RSASSA-PSS (1), RSASSA-PKCS1-v1_5 (2)

[3] Hash-Algorithms:
Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8)
```

IKEv2 Verschlüsselung

LANCOM empfiehlt die Nutzung aktueller DH-Gruppen für den Schlüsselaustausch. Für die Verschlüsselung und Integritätsprüfung der IKE_SA, sowie der Child_SA wird die Verwendung der höchstmöglichen Algorithmen empfohlen.

Pfad:

```
/Setup/VPN/IKEv2/Encryption
```

Kommando:

```
cd /Setup/VPN/IKEv2/Encryption

tab   Name  DH-Groups   PFS   IKE-SA-Cipher-List      IKE-SA-Integ-Alg-List   Child-
SA-Cipher-List    Child-SA-Integ-Alg-List

add   ENCR  DH30        yes    aes-gcm-256           sha-512
      aes-gcm-256                   sha-512

cd/
```

Mögliche Einträge für Encryption:

```
[1] Name:
16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[2] DH-Groups:
Bitmask: DH30 (32), DH29 (64), DH28 (128), DH21 (256), DH20 (512), DH19 (1024), DH16
(1), DH15 (2), DH14 (4), DH5 (8), DH2 (16)

[3] PFS:
No (0), Yes (1)

[4] IKE-SA-Cipher-List:
Bitmask: AES-CBC-256 (1), AES-CBC-192 (2), AES-CBC-128 (4), 3DES (8), AES-GCM-256
(16), AES-GCM-192 (32), AES-GCM-128 (64)

[5] IKE-SA-Integ-Alg-List:
Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8), MD5 (16)

[6] Child-SA-Cipher-List:
Bitmask: AES-CBC-256 (1), AES-CBC-192 (2), AES-CBC-128 (4), 3DES (8), AES-GCM-256
(16), AES-GCM-192 (32), AES-GCM-128 (64)

[7] Child-SA-Integ-Alg-List:
Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8), MD5 (16)
```

Bei der Verwendung von Zertifikaten ist auf eine sinnvolle Zertifikatslebensdauer zu achten und möglichst ein automatisiertes Zertifikats Rollout Verfahren mit dem Protokoll SCEP zu nutzen!

Zertifikatsverwaltung

Das LCOS bietet die Möglichkeit, Zertifikate manuell oder per automatischen Zertifikatsrollout zu verwalten. Der automatische Zertifikatsrollout verwendet das Protokoll SCEP (Simple Certificate Enrollment Protokoll).

Zertifikate können initial und in einem definierten Zeitraum vor deren Ablauf automatisch vom Gerät bezogen werden. Neben der automatischen Beantragung bietet die Verwendung von SCEP insbesondere den Sicherheitsgewinn, dass der private Schlüssel direkt im Gerät erzeugt wird und den Speicher des Gerätes nie verlässt.

Der private Schlüssel wird in einem nicht auslesbaren Speicherbereich abgelegt. **In sicherheitsrelevanten Umgebungen sollte nach Möglichkeit das SCEP Protokoll verwendet werden.**

Pfad:

```
/Setup/Certificates/SCEP-Client
```

Kommando:

```
set /Setup/Certificates/SCEP-Client/SCEP-Operating Yes
```

Mögliche Einträge:

```
SCEP-Operating           : No (0), Yes (1)
```

```
cd /Setup/Certificates/SCEP-Client/CAs

tab Name URL DN Enc-Alg RA-Autoapprove CA-Signature-Algorithm Application Loopback-Addr.

add "VPN-CA" "http://10.1.2.3/cgi-bin/pkiclient.exe" "/CN=VPN-CA" 3des Yes md5 VPN "INTRANET"

cd /
```

Mögliche Einträge:

```
[1][Name]                       : 16 chars from:
                                  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!
                                  $%&'()+,/:;<=>?[\]^_.0123456789
[2][URL]                        : 251 chars from:
                                  abcdefghijklmnopqrstuvwxyzABCDEFGH
                                  IJKLMNOPQRSTUVWXYZ0123456789/?.-
                                  ;:@&=$_+!*'(),%
[3][DN]                         : 251 chars from:
                                  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"
                                  $%&'()*+-,/:;<=>?[\]^_.0123456789
                                  abcdefghijklmnopqrstuvwxyz `
[4][Enc-Alg]                    : des (0), 3des (1), blowfish (2),
                                  aes128 (3)
[7][RA-Autoapprove]             : No (0), Yes (1)
[6][CA-Signature-Algorithm]     : md5 (0), sha1 (1)
[10][Application]               : General (2), VPN (0),
                                  WLAN-Controller (1), EAP/TLS (3)
[11][Loopback-Addr.]            : 16 chars from:
                                  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$
                                  %&'()+-,/:;<=>?[\]^_.0123456789
```

```
cd /Setup/Certificates/SCEP-Client/Certificates
tab Name CADN Subject Device-Certificate-Keylength Application
add "VPN-CERT" "/CN=VPN-CA " "/CN=VPN-GW1" 2048 VPN
cd /
```

Mögliche Einträge für Certificates:

```
[1][Name]                 : 16 chars from:
                            ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                            -,/:;<=>?[\]^_.0123456789
[2][CADN]                 : 251 chars from:
                            #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'
                            ()*+-,/:;<=>?[\]^_.0123456789abc
                            defghijklmnopqrstuvwxyz `
[3][Subject]              : 251 chars from:
                            #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'
                            ()*+-,/:;<=>?[\]^_.0123456789abc
                            defghijklmnopqrstuvwxyz `
[7][Device-Certificate-Keylength]          : 10 chars from: 1234567890
[8][Application]          : VPN (0), WLan-Controller (1), EAP/TLS (3)
```

IPSec Policy Verwaltung

Das LCOS erzeugt die Gegenstellen-spezifischen IPSec Policies je nach Konfiguration automatisch aus den lokalen ARF Netzen und statisch konfigurierten Routing Informationen (automatische Regelerzeugung), manuell aus den lokalen ARF Netzen, statisch konfigurierten Routing Informationen und VPN Regeln der Firewall (manuelle Regelerzeugung) oder optional für Zertifikat-basiert authentisierte Gegenstellen automatisch ohne statische Routen (Proadaptives VPN).

Regelerzeugung ohne Proadaptives VPN

Pfad

```
/Setup/VPN
```

```
/Setup/VPN/VPN-Peers
```

Kommando:

```
set /Setup/VPN/Simple-Cert-RAS-Operating no
```

Mögliche Einträge:

```
Simple-Cert-RAS-Operating:no (0), yes (1)
```

```
set /Setup/VPN/Allow-Remote-Network-Selection no
```

Mögliche Einträge:

```
Allow-Remote-Network-Sele:no (0), yes (1)
```

```
cd /Setup/VPN/VPN-Peers
tab  Peer              Rule-creation
add  "OFFICE-VPN"      auto
cd /
```

Mögliche Einträge:

```
[1][Peer]               : 16 chars from: ABCDEFGHIJKLMNOPQR
                          STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]
                          ^_.0123456789
[9][Rule-creation]      : auto (0), manually (1), off (2)
```

```
cd /Setup/IP-Router/Firewall/Rules
tab  Name        Source    Destination Action  Firewall- VPN-Rule
add  "VPN-RULES" "***"     "***"       "%A"    No        Yes
cd /
```

Mögliche Einträge:

```
[1][Name]               : 32 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[3][Source]             : 40 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[4][Destination]        : 40 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[7][Action]             : 40 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[10][Firewall-Rule]     : No (1), Yes (0)
[11][VPN-Rule]          : No (0), Yes (1)
[12][Stateful]          : No (1), Yes (0)
```

Manuell und automatisch erzeugte VPN Regeln sind über den Befehl „`show vpn`“ auf ihre Korrektheit zu prüfen!

```
> show vpn


VPN SPD and IKE configuration:


  # of connections = 1


  Connection #1            10.1.2.0/255.255.255.0:0 <->
                           10.5.1.0/255.255.255.0:0 any


    Name:                  OFFICE-VPN
    Unique Id:             ipsec-0-OFFICE-VPN-pr0-l0-r0
    Flags:                 main-mode
    Local  Network:        IPV4_ADDR_SUBNET(any:
                           0, 10.1.2.0/255.255.255.0)
    Local  Gateway:        IPV4_ADDR(any:0, 1.2.3.4)
    Remote Gateway:        IPV4_ADDR(any:0, 0.0.0.0)
    Remote Network:        IPV4_ADDR_SUBNET(any:
                           0, 10.5.1.0/255.255.255.0)
```

Proadaptives VPN

Pfad:

`/Setup/VPN`

Kommando:

```
set /Setup/VPN/Simple-Cert-RAS-Operating yes
```

Mögliche Einträge:

`Simple-Cert-RAS-Operating:no (0), yes (1)`

```
set /Setup/VPN/Allow-Remote-Network-Selection yes
```

Mögliche Einträge:

`Allow-Remote-Network-Sele:no (0), yes (1)`

Das Proadaptive VPN erlaubt einer Zertifikat-basiert authentisierten Gegenstelle die Auswahl eines beliebigen IP Netzes. Dieses Netz wird automatisch in das Routing des LCOS übernommen.

Aus diesem Grund ist proadaptives VPN ausschließlich auf vertrauenswürdigen Gegenstellen zu verwenden!

IPv4 Firewall Strategie

Die LCOS IPv4-Firewall verfolgt im factory default Zustand eine „allow all“ Strategie. Um maximale Datensicherheit im Datentransfer zu erzielen ist zunächst die Firewall Strategie auf ein „deny all“ Verfahren umzustellen.

Nur gewünschte Datenkommunikation ist an den Übergängen von trusted zu untrusted Netzen zu erlauben.

Pfad:

```
/Setup/IP-Router/Firewall/Rules
```

Kommando:

```
cd /Setup/IP-Router/Firewall/Rules
tab Name      Prot. Source    Destination Action            Firewall
add "DENYALL" "ANY" "ANYHOST" "ANYHOST"   "%Lcds0 %R %Lcd0" Yes
cd /
```

Mögliche Einträge:

```
[1][Name]               : 32 chars from:
                          ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                          -,/:;<=>?[\]^_.0123456789
[2][Prot.]              : 10 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[3][Source]             : 40 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[4][Destination]        : 40 chars from:
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[7][Action]              : 40 chars from:
```

```
                          #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                          )+-,/:;<=>?[\]^_.0123456789abc
                          defghijklmnopqrstuvwxyz`
[10][Firewall-Rule]     : No (1), Yes (0)
[12][Stateful]          : No (1), Yes (0)
```

IPv6 Firewall Strategie

Die LCOS IPv6-Firewall verfolgt im factory default Zustand eine „deny all“ Strategie,um maximale Datensicherheit im Datentransfer zu erzielen.

Nur gewünschte Datenkommunikation ist an den Übergängen von trusted zu untrusted Netzen zu erlauben.

Pfad:

```
/Setup/IPv6/Firewall/Forwarding-Rules
```

Kommando:

```
cd /Setup/IPv6/Firewall/Forwarding-Rules

tab Name  Action  Services  Source-Stations  Dsetination-Services

add "DENYALL" "REJECT" "ANY" "ANYHOST"   "ANYHOST"

cd /
```

Mögliche Einträge:

```
[1] Name:
36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[5] Action:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[7] Services:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[8] Source-Stations:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[9] Destination-Stations:
64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

[2] Flags:
Bitmask: none (0), deactivated (1), linked (4), stateless (8)

[3] Prio:
4 chars from 1234567890

[11] Src-Tag:
5 chars from 1234567890

[4] Rtg-tag
: 5 chars from 1234567890

[10] Comment:
64 chars from
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz
```

Firewall Session Management, IDS und DOS

Die LCOS Firewall arbeitet als Stateful Inspection Firewall. Um potentielle Angriffe über erlaubte Protokolle zu vermeiden, sollten Firewall Regeln stateful definiert sein.

Des Weiteren analysiert das LCOS die aktuellen Zustände von IP Verbindungen, um Portscans und Denial of Service Angriffe zu unterbinden. Um den Schutz dieser Funktionen zu nutzen müssen die IDS und DOS Aktionen entweder auf zurückweisen oder verwerfen gesetzt sein.

Die Schwellwerte sind den Netzwerkumgebungen anzupassen.

Pfad:

```
/Setup/IP-Router/Firewall
```

```
/Setup/IP-Router/Firewall/Rules
```

Kommando:

```
set /Setup/IP-Router/Firewall/Max.-Half-Open-Conns. 100
```

Mögliche Einträge:

```
Max.-Half-Open-Conns.    :4 chars from: 1234567890
```

```
set /Setup/IP-Router/Firewall/DoS-Action "%d%n"
```

Mögliche Einträge:

```
DoS-Action                :29 chars from:
                             #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&
                             '()+-,/:;<=>?[\]^_.0123456789abc
                             defghijklmnopqrstuvwxyz`
```

```
set /Setup/IP-Router/Firewall/Port-Scan-Threshold 50
```

Mögliche Einträge:

```
Port-Scan-Threshold       :4 chars from: 1234567890
```

```
set /Setup/IP-Router/Firewall/IDS-Action "%d%n"
```

Mögliche Einträge:

```
IDS-Action                :29 chars from:
                             #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&
                             '()+-,/:;<=>?[\]^_.0123456789abc
                             defghijklmnopqrstuvwxyz`
```

```
cd /Setup/IP-Router/Firewall/Rules
tab  Name            Action    Firewall-    Stateful
add  "ALLOW-XYZ"     "%A"      Yes          Yes
cd/
```

Mögliche Einträge:

```
[1][Name]                : 32 chars from:
                           ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+
                           -,/:;<=>?[\]^_.0123456789
[7][Action]              : 40 chars from:
                           #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'(
                           )+-,/:;<=>?[\]^_.0123456789abc
                           defghijklmnopqrstuvwxyz`
[10][Firewall-Rule]      : No (1), Yes (0)
[12][Stateful]           : No (1), Yes (0)
```

Als Aktionen stehen die folgenden grundlegenden Parameter zur Verfügung:

```
ACCEPT   %A
DROP     %D
REJECT   %R
```

Die effektiv vom LANCOM ausgewerteten Firewall Regeln sind mit den folgenden Hilfsmitteln zu kontrollieren:

Kommando:

```
show filter


Filter 0001 from Rule DENYALL:
  Protocol: 0
  Src: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
  Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
  use routing tag 0000
  Limit per conn.:  after transmitting or receiving of 0 kilobits
  per second
  actions after exceeding the limit:
      reject

  Limit per conn.:  after transmitting or receiving of 0 kilobits
  actions after exceeding the limit:
      accept
```

In den Statusinformationen der Firewall kann die korrekte Arbeitsweise der Filter überprüft werden. Hierzu sind die gewünschten IP Verbindungen aufzubauen. Die Übersicht der offenen IP Verbindungen der Firewall stellt die Information bereit, welche Firewall Regel für die Verbindung angewendet wurde.

Pfad:

```
/Status/IP-Router/Connection-List
```

Damit etablierte IP Verbindungen nicht missbräuchlich weiterverwendet werden können, werden die Einträge der etablierten Verbindungen nach Schließen der Verbindung bzw. nach einem Idle Timeout aus der Verbindungs Liste entfernt. Eine IP Verbindung muss danach standardkonform neu aufgebaut werden.

Die Timeouts können über die folgenden Einstellungen passend zu den verwendeten Applikationen gesetzt werden.

Um Angriffe durch nicht standardkonform fragmentierte Pakete zu vermeiden, sind Fragmente vom LCOS zu reassemblieren.

Pfad:

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

Kommando:

```
set /Setup/IP-Router/1-N-NAT/TCP-Aging-Seconds 300
set /Setup/IP-Router/1-N-NAT/UDP-Aging-Seconds 20
set /Setup/IP-Router/1-N-NAT/ICMP-Aging-Seconds 10
set /Setup/IP-Router/1-N-NAT/Fragments Reassemble
set /Setup/IP-Router/1-N-NAT/Fragment-Aging-Seconds 5
set /Setup/IP-Router/1-N-NAT/IPSec-Aging-Seconds 2000
```

Mögliche Einträge:

```
TCP-Aging-Seconds         :5 chars from: 1234567890
UDP-Aging-Seconds         :5 chars from: 1234567890
ICMP-Aging-Seconds        :5 chars from: 1234567890
Fragments                 :Filter (0), Route (1), Reassemble (2)
Fragment-Aging-Seconds    :3 chars from: 1234567890
IPSec-Aging-Seconds       :5 chars from: 1234567890
IPSec-Table               :try 'set IPSec-Table ?'
```