```
#
| LIESMICH Datei fuer
|
| LANCOM Router
|
|       Firmware Aenderungen und Update-Hinweise
|
| Copyright (c) 2002 LANCOM Systems GmbH, Wuerselen (Germany)
|
| Die LANCOM Systems GmbH uebernimmt keine Gewaehr und Haftung fuer nicht
| von der LANCOM systems GmbH entwickelte, hergestellte oder unter dem
    Namen
| der LANCOM Systems GmbH vertriebene Software, insbesondere nicht fuer
| Shareware und sonstige Fremdsoftware.
|
| LANCOM Systems GmbH                    Internet   : http://www.lancom.de
| Adenauerstrasse 20 / B2
| D-52146 Wuerselen
| Germany
|
| 25.04.2003, FJanssen
```

Inhaltsuebersicht

---

1. Firmware-Aenderungen von 2.92.0004 -> 2.92.0005

Korrekturen/Anpassungen:

- CRC Berechnung korrigiert für LANCOMs mit 10Mbit LAN Interface

Firmware-Aenderungen von 2.90.0009 -> 2.92.0004

Korrekturen/Anpassungen:

- LANCOM verwendet auch fest konfigurierten Backup DNS Server
- IPX Pakete erhalten auf WLAN Verbindungen die korrekte Absender Adresse (Ethernet und IPX Quelle entspricht der MAC Adresse des WLAN Interfaces)
- Bearer Capability und Framing Type werden bei PPTP outgoing Call Request korrekt gesetzt
- Timeout für Software Watchdog Überwachung auf LANCOM 16xx, 821, 7011, 3050 korrigiert, Gerät wird bei einem Softwareproblem hiermit korrekt gebootet.
- Backup Behandlung korrigiert, Backup Verbindungen werden korrekt auf/abgebaut
- Absenderadresse der GRE Pakete einer PPTP Verbindungen werden korrekt gesetzt
- TCP Verbindungen interner Dienste des LANCOM funktionieren auf PPTP Verbindungen
- Fehlermeldung "no remote" bei einer fehlenden Gegenstelle wird wieder korrekt angezeigt
- Public Spot Konfigurationsmenü für freie Netze korrigiert
- IPSec Authentifizierungsmethode "keine" entfernt
- LANCOM bootet nicht mehr mit OS Panic, wenn mehr als 16 Quellen/Ziele in einer Firewall Regel zusammengefasst werden.
- NetBIOS Pakete werden vom NetBIOS Proxy nur noch gespoofed, wenn sie nicht von Firewall Filtern verworfen werden.
- Optimierungen der Verwaltung der WLAN Stationstabelle

Firmware-Aenderungen von 2.90.0005 -> 2.90.0009

Korrekturen/Anpassungen:

- Poll Retries werden im Status Trace korrekt angezeigt
- Layer wird bei Rückruf korrekt gesetzt
- IPSec delete notifications werden vor dem Wechsel der Backup-Verbindung zur Master Verbindung gesendet
- IKE Pakete werden über die Backup-Verbindung gesendet, solange diese aktiv ist
- bei einem IPSec Reconnect wird die Verbindung sofort (nicht erst nach Ablauf eines Timeouts) wieder aufgebaut
- Backup Verbindungen weden wieder zuverlässig aufgebaut
- DNS Client setzt die Intranet IP (nicht die DMZ IP) als Absender
- Automatische Frequenzwahl (802.11a) über Grundkonfigurationswizard möglich
- Anfragen an den internen SNTP Server werden über unmaskierte Verbindungen zugelassen, auf maskierten Verbindungen wird weiterhin ein ICMP unreachable gesendet
- Puffernutzung für stark überlasteten VPN Verbindungen ist nun eingeschräkt, um andere Verbindungen nicht zu belasten
- ICMP Polling Pakete werden mit TOS low delay markiert, damit das Polling auf stark ausgelasteten Verbindungen bevorzugt behandelt wird
- bei deaktiviertem lokalen Routing werden wieder korrekt ICMP Redirects gesendet
- IPSec VPN Pakete werden vom Initiator zurückgehalten, bis der Responder ebenfalls in den connected Status gewechselt ist
- Verwaltung der WLAN Stationstabelle optimiert
- NetBIOS Pakete, die durch eine Firewall Regel verworfen werden, werden vom NetBIOS Proxy nicht mehr gespoofed
- ADSL Linecode aktualisiert
- WEBconfig warnt bei unsicherer WLAN Konfiguration
- Security LED blinkt nun auch bei unsicherer WLAN Konfiguration (z.B. Gerät ohne Passwort)
- RADIUS für PPP Einwahlen auf Business Geräten aktiviert
- IP Adress Zuweisung über RADIUS möglich
- in Trace Ausgaben wird nun die Echtzeit (UTC) anstelle der System Up Time angegeben

Firmware-Aenderungen von 2.82.0015 -> 2.90.0005

neue Features:

- DFS (dynamic frequency selection) für 802.11a Wireless Geräte
- Radarerkennung für 802.11a Wireless Geräte
- Maximale Anzahl von LANCAPI Kanälen konfigurierbar
- Wireless LAN Durchsatz Anzeige
- CRON Tabelle für zeitgesteuerte Aktionen

Korrekturen/Anpassungen:

- Intranet-only Maskierung: DMZ IP Adressbereich kann eine maskierte Internetverbindung transparent nutzen, auch wenn WAN und DMZ Adresse unterschiedlich sind
- neue VPN Verbindungen funktionieren wieder ohne reboot
- IKE und ESP lassen sich mit NULL Encryption konfigurieren
- Kommando "show vpn" zeigt derzeit gültige IPSec Regeln an
- IPSec Maskierung unterstützt nun mehrere Tunnel zwischen zwei Gegenstellen
- IRC Maskierung
- RFC 2428 Unterstützung für FTP Kommandos EPSV und EPRT
- Portscans auf unmaskierten Verbindungen oder auf invers maskierte Hosts werden für den shorthold timeout nicht mehr ausgewertet
- Traceausgaben für dynamic VPN in vpn-status Trace ergänzt
- EAP Funktion ist wieder ohne Public Spot Option nutzbar
- ADSL Status Anzeige bei Geräten mit ADSL Interface erweitert
- IKE Rekeying Verhalten verbessert
- Namenslisten vergrößert
- GRE Acknowledges werden korrekt ausgewertet, bei Senderaten <2 Pakete/Sekunde

werden keine Pakete mehr verworfen
- dynamic VPN funktioniert auf unmaskierten Verbindungen
- Absender Adresse bei GRE und ESP/AH Paketen auf unmaskierten Verbindungen mit fester IP (IP-Parameter Liste) wird korrekt gesetzt
- IPSec aggressive mode Verbindungen funktionieren auch bei existierendem PPP Listen Eintrag für die Verbindung
- Behandlung von Fragmenten auf maskierten Verbindungen korrigiert (insb. fragmentierte GRE und ESP Pakete werden bei entsprechender Einstellung korrekt reassembliert)
- Pakete mit dont fragment bit werden bei einer anstehenden Fragmentierung wieder mit einer ICMP Fehlermeldung beantwortet
- VPN wird bei Änderungen der Routing Tabelle über Telnet/WEBconfig automatisch neu konfiguriert
- Deny Regeln werden nicht mehr mit anderen Regeln verkettet, wenn bereits das erste Paket verworfen wird
- Statusbehandlung im dynamic VPN korrigiert
- auf transparenten Ethernet WAN Verbindungen wird die WAN-MTU gleich der LAN-MTU gesetzt
- Fragment-ID bzw. IP-ID werden nun zur Vermeidung von Fragment Kollisionen eindeutig gesetzt
- NetBIOS Informationen des LANCOMs werden auf IPSec over PPTP Clientverbindungen korrekt durch den IPSec Tunnel gesendet
- interne Dienste (z.B. DNS Forwarder) werden von Limit Filtern nicht mehr eingeschränkt
- PPP Layer wird nach der Authentifizierung erneut gesetzt (ggf. wurde mit dem Default Layer angenommen und der verbindungsspezifische Layer enthält andere Werte)
- für IPSec IKE Main Mode Verbindungen werden keine VPN Regeln mehr erzeugt, wenn das Remote Gäteway unbekannt ist.
- IPSec Regeln für dynamic VPN / PPTP Verbindungen werden entfernt, wenn die Verbindung abgebaut wird
- statisch konfigurierte DNS-Namen können als Namen in Firewall Regeln verwendet werden

Firmware-Aenderungen von 2.82.0009 -> 2.82.0015

Korrekturen/Anpassungen:

-Adressauflösung für Accounting korrigiert
-Setzen Button im WEBconfig in speziellen Menüs ergänzt
-Quelladressprüfung für IP Pakete im Bridge Betrieb deaktiviert
-Rückfall auf Multimode wird bei fest eingestelltem ADSL Linecode verhindert
-Verhalten bei VPN only Filtern korrigiert
-Verhalten bei verketteten Filterregeln korrigiert
-NetBIOS scan des NetBIOS Proxy bei deaktiviertem NetBIOS Modul ausgeschaltet
-Mehrere IKE SAs für aggressive mode Verbindungen zulässig
-Geräte mit Modemfunktion nehme keine Rufe mit Fax Dienstekennung mehr an

Firmware-Aenderungen von 2.82.0002 -> 2.82.0009

Korrekturen/Anpassungen:

-VPN Flag für die Firewall Filter wird jetzt bei Geräten ohne VPN korrekt ausgeblendet
-Auswahl "more" bei Telnet Ausgaben kann jetzt mit jeder Taste abgebrochen werden
-Windows XP NTP Client kann nun die Zeit vom LANCOM SNTP Server beziehen
-Timestamps in den Logging Tabellen werden beim Ändern der Systemzeit jetzt korrekt umgesetzt
-Deassoziierung von Wireless Stationen über WEBconfig oder Telnet funktioniert

wieder
-Ausgabe der VPN Verbindungs Statusinformationen korrigiert
-WAN seitige IP auf unmaskierten Verbindungen ist jetzt erreichbar
-Verhalten bei limitierten Filtern mit Einschränkung auf die Default Route oder "nur bei bestehender Verbindung" korrigiert
-Automatische Ratenfestlegung für 54Mbit Wireless Verbindungen korrigiert
-Behandlung kurzer FTP Pakete in der Firewall korrigiert
-gebündelte Backupverbindungen einer Festverbindung funktionieren wieder
-Anpassungen für die Verwendung von AirLancer MC-2 Karten in LANCOM Accesspoints
-Verhalten der IDS beim Umschalten zwischen Haupt- und Backupverbindung korrigiert
-Freigabe der ISDN Kanäle bei dynamic VPN Aufbauten und Überschreiten der max. zulässigen VPN Verbindungen korrigiert
-Mailtext für Login Sperre (IDS) korrigiert
-Auswertung von IP-Router connection table und IP Masquerading table korrigiert
-Timeout für TFTP Verbindungen erhöht
-WLAN Stationstabelle neu strukturiert
-Setzen der VPN seitigen IP Adresse korrigiert, wenn sowohl Intranet- als auch Internet IP konfiguriert sind -> ICMP Polling funktioniert auch bei gleichzeitigem IPSec over WLAN und WAN seitigen VPN.

Firmware-Aenderungen von 2.82.0001 -> 2.82.0002

Korrekturen/Anpassungen:

-Verhalten beim Versand von SNMP Traps korrigiert
-Setzen der Zeit über NTP wird bei der Angabe der Verbindungszeit korrekt behandelt
-TCP-Pakete mit gesetzten ECN-Flags werden akzeptiert
-Sortierung portbezogener Filter korrigiert
-Regeln für aggessive Mode IPSec Verbindungen werden beim Aufbau der zugrunde liegenden Verbindung korrekt angepasst

Firmware-Aenderungen von 2.80.0014 -> 2.82.0001

Korrekturen/Anpassungen:

-Gleichzeitig zu einer IP aufgebaute Verbindungen über denselben Port (z.B. Aufruf einer Webseite mit mehr Elementen als die IDS Schwelle) führt nicht mehr zur Erkennung eines Portscans)
-Firewall Regeln können wieder über Telnet und WEBconfig gesetzt werden
-Timeouts nach TCP-RST und -FIN erhöht. Verhindert Zuschlagen eines Deny all Filters nach einem TCP Verbindungsabbruch.

Firmware-Aenderungen von 2.72.0009 -> 2.80.0014

neue Features:

- Stateful-Inspection: Nur selbstinitiierter Datentransfer ist zulässig. Alle "unverlangten" Datenpakete, die nicht zu einer bekannten Session werden verworfen. Alle Ports, die eine Verbindung benötigt werden dynamisch geöffnet (z.B. für FTP, Netmeeting oder H.323)
- Abwehr von Denial-of-Service-Angriffen (z.B. Fragmentierungs-"Fehler", SYN-Floodings)
- Intrusion Detection zur Erkennung von Portscans; "Verstecken" des Gerätes durch PING-Blocker und Stealth-Mode
- IP QoS: "Vorziehen" von von Datenpaketen, die anhand einer Firewall-Regel identifiziert wurden (z.B. garantierte Mindestbandbreite für VoIP-Traffic oder anderen Dienste/Applikationen)
- IP-Traffic Limiting: Begrenzung von Bandbreiten (z.B. FTP-Speed pro User

begrenzt, alle FTP-User zusammen nicht mehr als 1 Mbit/s)
- EMail-Benachrichtigung frei einstellbar z.B. bei Angriffen, Einbruchsversuchen oder Überschreitung von Transfervolumina.
- VPN IKE Aggressive Mode Unterstützung. In VPN-Installationen sind die LANCOM VPN Gateways durch die Unterstützung des IKE Aggressive Modes nun auch interoperabel an bzw. gegen 3rd Party VPN Gateways mit dynamischen IP-Adressen.
- Neues WEBconfig: WEBconfig kann neben der "Expertenkonfiguration" und den "Installations-Assistenten" nun auch die aus LANconfig für Windows bekannten komfortablen Konfigurationsdialoge anzeigen.
- H.323 Masquerading: Unterstützung von VoIP TK-Anlagen oder Netmeeting
- NTP-Server können jetzt komfortabel per URL angesprochen werden, incl. Drop-Down-Liste mit frei benutzbaren Time-Servern
- Sichere Funk-LANs durch Unterstützung von 802.1x zum dynamischen Austausch der WEP-Schlüssel

Korrekturen/Anpassungen:

- beim Abbau von VPN werden Queues geleert
- MSS Anpassung korrigiert
- NetBIOS Berechtigung korrigiert
- DSL Backup Verhalten korrigiert
- SNTP Trace ergänzt
- Überwachung des Verbindungsabbaus optimiert
- Next Hop Gateway bei IPSec over WLAN (WLAN auf LAN Interface) wird jetzt korrekt bestimmt
- Änderungen des NTP Request Intervalls über LANconfig werden auch ohne Neustart des Gerätes aktiviert
- NTP Pakete des LANCOM NTP Clients werden nicht mehr maskiert
- Erkennung eines Abbruches des Konfigurationsuploads korrigiert (unvollständige Konfiguration wird nicht mehr aktiviert)
- Behandlung von ? in DNS forwarding list korrigiert
- Umbenennung WAN Ethernet Interfaces DSL10 -> DSL
- default Zeitzone auf +01 geändert
- Firewall default Objekte um PPTP und IPSec ergänzt
- Behandlung des IPSec Verbindungszustandes korrigiert
- WEBconfig (neue Konfigurationsansicht) aktualisiert
- in ICMP Rückmeldugen des LANCOMs wird der IP Header des eingebetteten Paketes nicht mehr verändert
- wiederholte Suche nach NetBIOS Stationen im lokalen Netz
- Spoofing von NetBIOS Watchdog Paketen korrigiert
- ADSL Multi Mode Erkennung erweitert. Timeout erhöht, um Gegenstellen mit lä ngerer Synchronisationsphase korrekt erkennen zu können.
- IPSec Maskierung akzeptiert jetzt Verbindungen ohne Angabe von Lifetimes
- IPSec Maskierung akzeptiert jetzt auch Lifetimes ohne Längenangaben
- MAC Adress Filterauswertung für Pakete aus dem WAN korrigiert
- Accountingausgaben bei VPN Verbindungen über das LAN Interface korrigiert
- Absender IP Adresse von GRE Paketen auf unmaskierten Verbindungen korrigiert
- Tabellen in IP Router Statistik werden mit dem Befehl delete-values wieder korrekt gelöscht
- Änderungen der Y-Verbindungseinstellung werden wieder ohne Booten übernommen
- Groß/Kleinschreibung wird bei Einträgen der DNS Filterliste nicht mehr ausgewertet

Firmware-Aenderungen von 2.70.0025 -> 2.72.0009

- VPN Optimierungen bei komplexen Netzstrukturen
- NetBIOS Namensinformationen werden jetzt gesichert uebertragen
- NetBIOS Namen von maskierten Gegenstellen werden nicht propagiert
- LANCOM Business 6011/6021 Timeslot 16 bei G.703 Verbindungen funktioniert wieder

Firmware-Aenderungen von 2.62.0002 -> 2.70.0025

neue Features:
- Erste LANCOM Systems Firmware. Voll abwärtskompatibel zu ELSA-Altgeräten
- HTTPS-Unterstützung für gesicherte WEBconfig-Konfiguration
- BusinessOnline-Unterstützung im Internet-Wizard
- IP Quality-Of-Service: Unterstützung von TOS "Low Delay" und DiffServ " Expedited Forwarding". Entsprechende Pakete werden bevorzugt weitergeleitet, und ggfs. auch entsprechend in VPNs gekennzeichnet.
- NTP-Client/-Server: Bezug der aktuellen Uhrzeit von einem Timeserver moeglich
- Backup Verbindungen ueber separate Backup Liste (z.B. Internetprovider mit unterschiedlichen Zugangsdaten fuer DSL und ISDN)
- Erweiterte Verbindungsueberwachung, Polling Liste zur Angabe von erreichbaren IP Adressen
- Berechtigungen von Telnet, TFTP, http, https und snmp koennen individuell eingestellt werden
- VPN Client (IPSec over PPTP) vorbereitetet, Unterstuetzung von IP Pooling
- IPSec-Pass-Through / IPSec-Masquerading
- ueber die IP Parameterliste koennen nun auch Adressen fuer PPP Verbindungen festgelegt werden

Korrekturen/Anpassungen:
- Anpassungen Umstellung auf LANCOM Systems
- Anpassungen der Wizards von WEBconfig
- Verhalten bei VPN Verbindungen über das LAN Interface korrigiert
- MAC Adress Filter funktionieren auf virtuellen Interfaces (VPN Verbindungen)
- Einstellungsmöglichkeit zum Ignorieren von Filterregeln bzgl. VPN Policies
- unterschiedliche Einstellungen der Amtsholungsnummer der ISDN Interfaces (Business 4100) werden bei Buendlungen korrekt ausgewertet
- Optimierungen im VPN Umfeld

Firmware-Aenderungen von 2.50.0005 -> 2.62.0002

- Problem im Outband gelöst
- os_panic bei udp portscan gefixt
- alle udp ports sind geschlossen bei portscans
- Haltezeit 9999 wird für VPN-Verbindungen ignoriert
- layer 2 und layer 3 können nun die richtige Anzahl der Verbindungen handhaben
- SNMP MIB: Kommandos werden als Strings gehandhabt
- os_panic in der Kanal-Statistik behoben
- DHCP requests für feste Addressen gefixt
- TCP-Optionen bei Masquerading berücksichtigen (betrifft FTP und PPTP)
- Löschen von Fehlern in der Kanalstatistik aus dem LANmonitor
- os_panic bei PPTP/VPN-Client Verbindung beseitigt
- os_panics beim Abbau von "PPTP über VPN" Verbdinungen beseitigt
- Backupverzögerung wird nach dem Rückfall aus dem Backup wieder berücksichtigt
- Möglicher Queue Block Verlust bei passivem disconnect behoben (ADSL)
- Fehlermeldungen können im Lanmonitor wieder gelöscht werden
- Physikalische Verbindungen werden nun nach dem virtuellen Kanal (PPTP/VPN) getrennt
- Geschwindigkeit des PPTP Verbindungs-Abbaus verbessert

- DNS Domänen-Weiterleitung funktioniert mit (getrennten) VPN und PPTP Verbindungen
- einige Webconfig Texte geändert
- CHAP Reauthentifizierung benutzt die Userdaten der angesprochenen Gegenstelle und nicht die des Default-Users
- CHAP Reauthentifizierung wird nur verwendet wenn die erste Authentifizierung mit CHAP erfolgt ist
- PPTP funktioniert im LAN
- bei einem Reboot werden alle PPTP und VPN Verbindungen auf dem LAN geschlossen
- CRC10 Berechnung und Überprüfung auf OAM Zellen
- VPN verwendet jetzt beide (Internet und Intranet) Addressen korreckt
- Kein Datenverlust mehr beim debugging via Telnet
- DNS Forwarder funktioniert nun korreckt auf nicht maskierten Verbindungen
- Texte für den RAS Wizard im WEBconfig korrigiert
- /Setup/ab-module kann jetzt auch im WEBconfig konfiguriert werden
- ADMIN User kann den Router nicht mehr (miss)brauchen
- ADMIN User wird abgewiesen, wenn die WAN Konfiguration auf "nicht erlaubt" steht
- WAN-IP Adresse kann jetzt auch aus dem LAN erreicht werden
- PPTP-Server funktioniert jetzt auch mit entfernten NAT Verbindungen
- Blink Codes "Unsichere Konfiguration" und "Gebühren Limit" überlappen nicht mehr
- Interface Auswahl im WEBconfig für spanisch, französisch, portugisisch und italienisch korrigiert
- Probleme mit PPP-Verbindungen im Webconfig Wizard gelöst
- LC6000-Internetwizard: Wird der S0-Bus als Interface gewählt, so erscheint nun auch die Proviedrauswahl anstelle des generischen "INTERNET" Providers
- Im VPN-Stichleitungsbetrieb ist das LANCOM durch den Tunnel auf seiner "internen" Adresse erreichbar

---

2. Bemerkungen

Installieren Sie als erstes die aktuellen LANTools.
Anschliessend starten Sie LANconfig und laden ueber den Button "Firmware-Upload" die Firmware in das Geraet.

Fuer die Geraete:
==========

LANCOM 821 ADSL/ISDN Annex A
LANCOM 821 ADSL/ISDN Annex B
LANCOM 1621 ADSL/ISDN Annex A
LANCOM 1621 ADSL/ISDN Annex B

Achten Sie bitte unbedingt darauf, dass Sie die passende Firmware für Ihr Gerät heruntergeladen haben (Annex A / Annex B).
