Release-Notes

CT-Router LAN 5 Port

Release 1.11.12 28-Jun-2022
Sicherheitskorrekturen:
- Update auf openssl-1.1.1n behebt CVE-2022-0778.
- Update auf expat-2.4.7 behebt CVE-2022-23852, CVE-2022-23990, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314 und CVE-2022-25315.
- Update auf openvpn-2.4.12 behebt CVE-2022-0547.
- Update auf zlib-1.2.12 behebt CVE-2018-25032.

Release 1.11.11 15-Dez-2021
Sicherheitskorrekturen:
- IPsec: Korrektur behebt CVE-2021-41990 und CVE-2021-41991.

Neue Funktion:
- Zum E-mail versenden können jeweils bis zu 10 Empfänger angegeben werden. Weitere Empfänger können, getrennt durch ein Komma, in jeder Zeile angegeben werden.

Release 1.11.10 09-Sep-2021
Sicherheitskorrekturen:
- Update auf openssl-1.1.1l behebt CVE-2021-3711 und CVE-2021-3712.

Neue Funktionen:
- IPsec: Im Mode IKEv2 können bis zu 5 Netze (Traffic Selectors) für die lokale und/oder entfernte Adresse, gesetzt werden. Die optionale NAT Funktion wirkt dabei nur auf das erste Paar aus lokalem und entferntem Netz.

Release 1.11.9 29-Jul-2021
Verbesserungen:
- Behebt ein Problem aufgrund mangelnder Entropy im Kernel, welcher zum Stillstand des Gerätes führen kann.

Release 1.11.8 01-Jun-2021
Sicherheitskorrekturen:
- Update auf openssl-1.1.1k behebt CVE-2020-1971, CVE-2021-3449 und CVE-2021-3450.
- Update auf dnsmasq-2.85 behebt CVE-2020-25684 und CVE-2020-25686.
- Update auf openvpn-2.4.11 behebt CVE-2020-15078.

Neue Optionen:
- In OpenVPN Verbindungen kann die ab openvpn-2.4 mögliche option compress benutzt werden. Weiterhin kann die Cipher-Gruppe AES-xxx-GCM ausgewählt werden.

Release 1.11.7 18-Mar-2021
Sicherheitskorrekturen:
- Update auf openssl-1.1.1j behebt CVE-2021-2839, CVE-2021-2840 and CVE-2021-2841.

Fehlerkorrektur:
- IPsec mit XAuth ist wieder Funktionsfähig. Die Web-GUI sorgt dafür das XAuth nur mit IKEv1 arbeiten kann.
  Da XAuth nur für IPv4 geeignet ist, sollte die Adressierung auf IPv4 beschränkt werden wenn als Gegenstelle eine URL verwendet wird.

Verbesserungen:
- In den IPsec Verbindungen kann jetzt eine UDP Verkapselung erzwungen werden.

Release 1.11.6 08-Jan-2021
Sicherheitskorrekturen:

- Update auf openssl-1.1.1i behebt CVE-2020-1971.

Release 1.11.5 19-Okt-2020
Fehlerkorrektur:
- In der Title-Anzeige der Webserver-Schlüssel fehlte die Schlüssellänge.

Release 1.11.4 14-Okt-2020
Verbesserungen:
- die zulässige Startzeit für IPsec verlängert auf 30s um einen vorzeitigen Timeout zu vermeiden. Ansonsten kann es bei grossen Schlüssellängen zu einem vorzeitigen Abbruch des IPsec Prozesses führen.
- Der PKCS#12-Zertifikatsimport unterstützt jetzt Schlüssel mit elliptischen Kurven.

Release 1.11.3 27-Mai-2020
Sicherheitskorrekturen:
- Patch für PPPD, behebt CVE-2020-8597
- Patch behebt CVE-2017-16544 in busybox.
- eine authentifizierte Befehlsinjektion mit Hilfe einer händisch modifizierten POST Anweisung wird jetzt verhindert.
- Update auf openssl-1.1.1g behebt CVE-2020-1967.

Verbesserungen:
- Unterstützung für ext3 formatierte Datenträger (USB-Stick und SD-Karte)
- Der IPsec-Status zeigt den verwendeten Port der Gegenseite an.
- Der OpenNTPd Client wird bei Protokollfehler nicht mehr beendet sondern neu gestarted.
- IPsec arbeitet jetzt auch mit IPv6 Gegenstellen zusammen.

Release 1.11.2 07-Jan-2020
Verbesserungen:
- der SNMP-Daemon wird jetzt im Hintergrund verzögert gestarted um ein 6 minütiges Hängenbleiben bei Hochlaufen des Gerätes zu vermeiden.

Release 1.11.1 8-Nov-2019

Neue Features bzw. Sicherheitsupdates:
- Verwendung von OpenSSL-1.1.1 mit Unterstützung für TLS-1.3.
- Webserver mit TLS-1.3
- OpenVPN mit TLS-1.3
- E-Mail senden mit TLS-1.3

Verbesserungen:
- Verwendung der Native Posix Thread Library (NPTL)
- schnellerer Start-/Stop und Verbindungs-auf/abbau bei IPsec aufgrund der NPTL.

Release 1.10.5 08-Aug-2019
Neue Features:
- Für den openvpn Verbindungsaufbau kann die Adressfamilie eingestellt werden.
- Für den openvpn Server kann die Adressfamilie eingestellt werden.
  "auto" : dual-stack, IPv4 und IPv6
  "IPv4" : nur IPv4
  "IPv6" : nur IPv6
- Ein Firmwareupdate ist jetzt auch über ssh möglich.

Release 1.10.4 10-Jul-2019
Bugfix:
- Die unntige Einschränkung in den "IP and port forwarding" Regeln auf 10 fortlaufende Ports

entfernt wenn Quell- und Zielbereich identisch sind.

Release 1.10.3 19-Jun-2019

Bugfix:

- Statusabfrage der Eingänge via XML-Server wieder funktionsfähig.
- Der Webserver funktioniert jetzt auch mit Zertifikaten welche von einer CA unterschrieben wurden

Release 1.10.2 23-Mai-2019

Bugfix:

- Das Admin Passwort kann nur geändert werden wenn das alte Passwort eingegeben wurde.

Release 1.10.1 09-Mai-2019

Neue Features:

- Auf der WAN Seite kann der IPv6 Dualstack Betrieb aktiviert werden.
- Auf der LAN Seite kann als IPv6 DHCP Service das Routing Advertisement und stateless-/statefull DHCP aktiviert werden.
- OpenVPN ist jetzt voll IPv6 fähig.
- Die TLS-Versionen TLS-1.0 und TLS-1.1 können für den Web-Zugriff deaktiviert werden.

Sicherheitskorrekturen:

- Update auf openSSL-1.0.2r, behebt CVE-2019-1559

Release 1.09.8 19-Mrz-2019

Neue Features:

- Die Ethernet-Ports 2,3,4 sind Abschaltbar.

Release 1.09.7 25-Jan-2019

Neue Features:

- In den Einstellungen zum DHCP-Server kann der autoritative Modus Ein-/Ausgeschaltet werden.
- Webserver mit Zertifikatsimport.
- In Firewall und Portweiterleitungen kann jeder Eintrag Ein-/Ausgeschaltet werden.

Sicherheitskorrekturen:

- Update auf openSSL-1.0.2q, behebt CVE-2018-5407 und CVE-2018-0734.
- Update auf openVPN-2.3.18.

Release 1.09.6 04-Jun-2018

Sicherheitskorrekturen:

- strongswan CVE-2018-10811, CVE-2018-5388
- expat

Verbesserungen:

- strongswan IKEv1 Reauthentisierung verbessert.

Release 1.09.5 25-Mai-2018

Verbesserungen:

- IPsec mit Unterstützung für IKEv2.
- IPsec mit SHA-256/384/512 sowie Diffie-Hellman mit elliptischen Kurven.
- Globale IPsec Firewall um Denial-of-service Angriffe abzuwehren.

Release 1.08.10 04-Dez-2017

Verbesserungen:

- verkürzte Latenzen im Web-GUI.

Bugfix:

- IPsec mit 1:1 NAT und gleichzeitiges Portforwarding beeinflussen sich nicht mehr gegenseitig.

Release 1.08.8 05-Okt-2017

Verbesserungen:

- Anzeige der Lizenz zu jedem Softwarepaket.
- Ablage der Texte aller Open-Source Lizenzen und Versionsinformationen der dazugehörigen Pakete.

Sicherheitskorrekturen:

- dnsmasq CVE-2017-14491, CVE-2017-14492 und CVE-2017-14493.

Bugfix:

- OpenVPN Preshared Key Import im Windows-Format.

Release 1.08.7-beta 07-Aug-2017

Sicherheitskorrekturen:

- Update auf OpenVPN-2.3.17 mit Korrektur für Sicherheitslücken CVE-2017-7521, CVE-2017-7479 und CVE-2017-7478.

Bugfix:

- IPsec 1:1 NAT.

Release 1.08.2-beta 23-Mai-2017

Release 1.08.1-beta 15-Feb-2017

Neue Features:

- Unter "Network security/General setup" kann der Zufriff aus dem lokalem Netzwerk auf DNS-Dienste unterbunden werden.
- Unter "System/System configuration" kann die Konfiguration und Verwendung von IPsec komplett ausgeschaltet werden.

Release 1.07.2 23-Nov-2016

Sicherheitskorrekturen:

- SSH in Version dropbear-2016.74 behebt die Sicherheitslücke CVE-2016-3116.
- IPsec strongswan Korrektur für Sicherheitslücke CVE-2013-2054.
- Linux Kernel Korrektur für Sicherheitslücke CVE-2016-5195.
- Der Fingerabdruck für https Zertifikate wird jetzt mit sha256 erstellt.
- Für https werden jetzt 2048 Bit lange Schlüssel verwendet.

Verbesserungen:

- Den stockenden Seitenaufbau über https bei Microsoft Browsern behoben.
- Die Anzahl der möglichen Portweiterleitungen auf 64 erhöht.

Bugfix:

- OpenVPN Preshared Key funktioniert wieder. War in Release 1.04.8 noch ok ab Release 1.05.1 jedoch Fehlerhaft.

Release 1.07.1 28-Okt-2016

Neue Features:

- SSH-Firewall eingeführt.
- Zeige nach dem Login die Seite der Zugangsdaten solange kein Admin Kennwort gesetzt wurde.
- Zeige in der Seite der Zugangsdaten nur dann den Eintrag 'old password' wenn zuvor ein Kennwort gesetzt wurde.

Release 1.06.8 28-Jun-2016

Neue Features:

- IPsec mit XAuth plus Preshared Key
- OpenVPN mit X.509 Zertifikat plus Benutzername und Kennwort.

- In OpenVPN kann bei Verwendung der TLS-Authentifizierung der HMAC Algorithmus ausgewählt werden.

Release 1.06.7 09-Mai-2016

Neue Features:

- Das Laden einer CA Zertifikatskette wird jetzt unterstützt. Eine Zertifikatskette ist im 'Tooltip' an dem Vorhandensein von mehreren 'subjects' zu erkennen.

Release 1.06.6 13-Apr-2016

Neue Features:

- Für jeden auf dem Gerät laufenden Service ist jetzt eine Firewall vorhanden. Der Zugriff auf diesen Service kann getrennt nach lokalem oder externem Netzwerk separat erlaubt der abgewiesen werden.
- IPsec unterstützt jetzt den Hash SHA-256 aus der SHA2 Reihe.
- Die Voreinstellung des Hostnamens auf 'ctrouter' kann geändert werden.

Bugfix:

- Auf USB-Sticks mit SMI-Controller kann jetzt geschrieben werden.

Release 1.06.5 17-Mrz-2016

Neuer DynDNS Client:

- Der neue DynDNS Client berücksichtigt jetzt einen Verfügbarkeitsengpass beim Server. D.h. wenn ein Server wegen momentaner Überlastung nicht Verfügbar ist wird die Verbindung zu einem späteren Zeitpunkt erneut versucht. Fest eingestellt sind hier 10 Minuten. Weiterhin unterstützt der neue Client eine Reihe weiterer DynDNS Provider wie Feste-IP.net, Hurricane Electric sowie FreeDNS.afraid.org.
- Die Reihenfolge in der die Tabellen für 1:1 NAT und "IP and port forwarding" bearbeitet werden, vertauscht. Jetzt sollte ein Problem bei gleichzeitiger Verwendung beider NAT Arten behoben sein.
- Unterstützung für WAN Verbindungen über VLAN.
- IPv6 kann für den LAN- und WAN-Bereich getrennt ein-/ausgeschaltet werden. Im WAN Interface kann IPv6 z.Z. nur auf dem Router selbst genutzt werden. DHCPv6 und Router Advertisement sind noch nicht implementiert.

Security updates:

- OpenSSL aktualisiert auf Version 1.0.0t.

Release 1.05.3 26-Okt-2015

Änderung im ARP-Verhalten:

- Das Gerät antwortet nur noch auf ARP-Requests auf der eingehenden Schnittstelle wenn die Adressanfrage lokal zu der eingehenden Schnittstelle ist.

Release 1.05.2 19-Okt-2015

Erweiterung:

- Das 1:1 NAT zwischen WAN und LAN kann nun bis zu 64 Hosts von der LAN Seite auf die WAN Seite spiegeln.

Bugfix:

- Korrektur der Zustandsanzeige in den Knöpfen für die Ausgänge.

Release 1.05.1 04-Sep-2015

Neue Features:

- Separate Login Seite.
- Neues Design der Seite "Network security setup".
- Ein 1:1 NAT zwischen WAN und LAN ist für statische und DHCP Addressvergabe möglich. Es können bis zu 16 Hosts von der LAN Seite auf die WAN Seite gespiegelt werden. Einstellung "Hostmapping via 1:1 NAT".
- In der Seite "IP and port forwarding", ehemals "NAT table", kann jetzt bestimmt werden von welcher IP-Adresse der Zugriff erlaubt ist.
- Es kann jetzt das Masquerading für ausgehende Daten per Tabelle eingestellt werden. Als Vorgabe wird von allen internen IP-Adressen ein Masquerading durchgeführt.

- In der Tabelle zur Firewall ist ein Kommentar Feld eingefügt.
- Neues Design der Tabellen: die Bedienelemente zum Anlegen, Löschen verschieben von Zeilen, etc., sind jetzt auf der linken Seite angeordnet.
- Für OpenVPN Tunnel Verbindungen kann ein Proxy aktiviert werden.
- In der Tabelle "Port forwarding" für OpenVPN kann als Filter die eintreffende IP-Adresse festgelegt werden. Als Vorgabe ist 0.0.0.0 (also von jeder Adresse) eingestellt.
- Bugfix:
- Korrektur der Policy in der Firewall.
- Die gesamte Firewall Funktionalität kann aus technischen Gründen nicht mehr deaktiviert werden. Um jegliche eingehende Daten zu erlauben ist eine entsprechende Regel (Protocol=All, From-IP=0.0.0.0/0, To-IP=0.0.0.0/0, Action=Accept) unter "Incoming traffic" anzulegen.
- Security updates:
- OpenSSL aktualisiert auf Version 1.0.0s.

Release 1.04.8 13-Mai-2015

Bugfix:
- Passwort Eingabe bei SMTP korrigiert.

Neue Features:
- Neuer Eintrag in Network Security: Drop invalid packets.

Release 1.04.3 16-Okt-2014

Neue Features:
- Der Fernzugriff auf das Gerät per SSH kann über "Network security/General Setup/External access via SSH" aktiviert werden.
- Der SNMP Fernzugriff auf das Gerät kann über "Network security/General Setup/External SNMP access" aktiviert werden.
- Die Konfiguration kann von USB-Stick oder SD-Karte direkt importiert werden.
- Es werden auch USB-Sticks welche im "Superfloppy"-Format, d.h. ohne Partitionierungtabelle formatiert wurden, erkannt.
- In OpenVPN Tunnel Verbindungen ist "Remote Masquerading" möglich.

Release 1.04.2 02-Okt-2014

Neue Features:
- Web-based Management auch über https möglich.
- OpenVPN Tunnel Verbindungen können jetzt über die Eingänge gesteuert werden.
- IPsec und OpenVPN Tunnel Verbindungen können jetzt über den XML-Server gesteuert werden.
- Die Funktion des Reset-Buttons ist Konfigurierbar.
  a) Nur Web-Zugang auf Werkseinstellung, temporär.
  b) Alle Benutzereinstellungen löschen und mit der Werkseinstellung neu starten.

Release 1.03.5 18-Sep-2014

Bugfix:
- OpenVPN baut nach einer Unterbrechung die Verbindung wieder vollständig auf.

Neue Features:
- OpenVPN Multiclient-Server mit vollständiger Netzwerk-Kopplung wenn "Client to Client Traffic" aktiviert wurde.

Release 1.03.4 22-Aug-2014

Bugfix:
- Eine PPPoE Paketdatenverbindung wird jetzt bei einer Konfigurationsänderung korrekt auf- und abgebaut.
- Anzeige der "Tooltips" zu den Zertifikaten auch dann wenn im Namen runde Klammern verwendet werden.
- COM-Server

Neue Features:
- Für OpenVPN Verbindungen kann TLS-Auth aktiviert werden.

- Der SSH-Server ist in der Werkseinstellung ausgeschaltet. Er kann unter "Network security/Device access via SSH" bei Bedarf wieder aktiviert werden.

09-Jul-2014
Release 1.03.3
Modifikation XML-Server:
- der Server schliesst die Verbindung nachdem die Daten übertragen wurden.

30-Jun-2014
Release 1.03.2
Neue Features:
- Konfiguration von USB-Stick oder SD-Karte laden sowie derMöglichkeit dies über einen Eingang zu erlauben.
- "Port forwarding via NAT table" ist über einen globalen Schaltersperrbar (Voreinstellung: gesperrt).
- OpenVPN-Server: erweiterte Statusansicht incl. Sub-Netze.

Release 1.03.1 26-Feb-2014
Neue Features:
- COM-Server
- SNMP

Release 1.02.2 27-Jan-2014
Bugfix: OpenVPN Firewall Input Rule wurde nicht immer korrekt gesetzt.

Release 1.02.1 07-Jan-2014
Neue Features:
- OpenVPN Server mit und ohne Client Subnet. Die Zertifikate sind z.B. mit dem Tool easy-rsa zu erstellen.
- IPsec mit Zertifikaten und erweiterter Authentifizierung.
  Diese Art wird auch gelegentlich als "Cisco IPsec" bzw IPsec+Xauth bezeichnet. Es ist jetzt möglich von einem iOS-Gerät (iPhone, iPad) eine direkte Verbindung zu dem Router und seinen dahinter liegenden Netzen aufzubauen. Auf dem iOS-Gerät ist dazu die Auswahl IPsec und "Zertifikat verwenden" auszuwählen. Die dafür notwendigen Zertifikate sind nach den Regeln wie in http://wiki.strongswan.org/projects/strongswan/wiki/IOS_%28Apple%29 beschrieben, zu erstellen.
- Informationen zu installierten Zertifikaten sind jetzt über einen"Tooltip" über dem i-Symbol oder dem grünen Haken abrufbar.

Release 1.01.6 12-Dez-2013
Wenn in OpenVPN als Connection-NAT "Port Forwarding" ausgewählt ist
dann kann ein (lokales) Masquerading separat hinzugeschaltet werden.

Release 1.01.5 04-Nov-2013
Bugfix: Upload von OpenVPN CA-Zertifikaten und Einstellungen bei der Authentifizierung zu Username/Password korrigiert.

Release 1.01.4 31-Okt-2013
Bugfix: Fehlerhafter Verbindungsabbau bei der Einstellung PPPoE behoben.

Release 1.01.3 22-Okt-2013

Release 1.01.2 15-Okt-2013
neue Features bzw. Verbesserungen:
- OpenVPN mit Benutzername/Passwort Authentifizierung.
- Einlesen von CA-Zertifikaten unter OpenVPN/Certificates ermöglicht.

- Erweiterte OpenVPN Einstellungen unter dem Knopf "Advanced".
- zum OpenVPN Verbindungs-NAT sind neben der bisherigen Einstellung a) jetzt weitere Einstellungen hinzugekommen:
  a) 1:1 NAT
  b) Local Masquerading
  c) Port Forwarding
  d) Host Forwarding
- Für das OpenVPN Port Forwarding ist eine eigene Tabelle vorhanden.
- Kommentieren von Einträgen in der NAT-Tabelle.
- Die NAT-Tabelle kann unter "Network Security/General Setup" ein-/ausgeschaltet werden.
- In der Konfiguration für DynDNS kann als Provider "custom DynDNS" ausgewählt werden. Dann kann die Server-URL frei gewählt werden (z.B. für andere DynDNS kompatible Provider).
- Verbesserungem im Benutzerdialog: Nicht benötigte Felder werden jetzt
- überwiegend per JavaScript ein-/ausgeblendet. Benutzername und Passwort Eingabefelder sind von der Autovervollständigen Funktion aktueller Browser ausgenommen. D.h. die lästige Nachfrage einiger Browser, ob der Benutzername und das Passwort gespeichert werden soll, entfällt.
- Anzeige eines Reboot Knopfes in der Einstellseite "Local Network/IP Configuration" wenn zur Übernahme der gewählten Einstellung ein Reboot nötig ist.

Fehlerkorrekturen:

- In der IPsec Konfiguration für Preshared Key werden jetzt die Local- und Remote-ID korrekt an das Secret gebunden.
- ICMP's type 3 code 4 (fragmentation needed) werden jetzt auch bei blockiertem externen Ping durchgelassen um die MTU path discovery zu ermöglichen.