

LCOS FX 10.12

Addendum

04/2023

Inhalt

- 1 Addendum zur LCOS FX-Version 10.12.....4**
- 2 Erweiterung der Desktop-Übersicht um
 Hardware-Monitoring-Daten.....5**
- 3 Hardware-Monitoring.....6**
 - 3.1 System-Informationen.....7
 - 3.2 CPU-Auslastung.....7
 - 3.3 Prozesse.....7
 - 3.4 Netzwerk.....8
- 4 Management-Bericht.....9**
 - 4.1 Aktueller Bericht.....9
 - 4.2 Mail-Bericht.....12
- 5 LLDP.....13**
 - 5.1 Einstellungen für LLDP.....13
 - 5.2 Informationen zu LLDP.....14
- 6 WireGuard.....15**
 - 6.1 WireGuard-Interfaces.....15
 - 6.1.1 Einstellungen zu WireGuard-Interfaces.....15
 - 6.2 WireGuard.....15
 - 6.2.1 WireGuard-Verbindung.....16
 - 6.3 WireGuard-Status.....18
- 7 Export von Protokollen.....19**
- 8 DNS-basierte Regeln.....20**
- 9 BGP-Erweiterung.....22**

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhaltes sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunfts- bezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Bitte senden Sie eine E-Mail an gpl@lancom.de.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (www.openssl.org).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

Bitdefender SDK © Bitdefender 1997-2023

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.12

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.12 gegenüber der vorherigen Version.

2 Erweiterung der Desktop-Übersicht um Hardware-Monitoring-Daten

Im Infobereich des Desktops werden in der Übersicht nun auch einige grundlegende Daten des Hardware-Monitorings angezeigt. So haben Sie jederzeit einen schnellen Überblick über die folgenden Daten:

- > **Betriebszeit:** abgelaufene Zeit seit Start der Firewall
- > **CPU:** durchschnittliche Auslastung aller CPUs in Prozent
- > **RAM:** Belegung des Arbeitsspeichers in Prozent
- > **var-Partition:** Belegung der var-Partition in Prozent. Die Belegung dieser Partion wird hier verwendet, weil auf dieser Partion u. a. Daten für Logs oder Statistiken gespeichert werden.

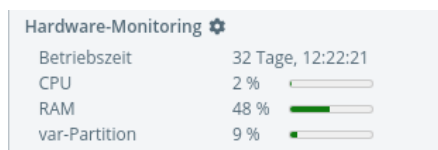



Abbildung 1: Übersicht > Hardware-Monitoring

 Mit einem Klick auf den Titel kommen Sie direkt zum Bereich [Hardware-Monitoring](#) auf Seite 6.

3 Hardware-Monitoring

Im Bearbeitungsfenster **Hardware-Monitoring** können Sie den aktuellen Zustand Ihrer LANCOM R&S® Unified Firewall anzeigen. Es werden Daten zu den folgenden Bereichen angezeigt:

- > System-Informationen
- > CPU-Auslastung
- > Prozess-Liste
- > Netzwerk-Auslastung

i Benutzer müssen über die Berechtigung „Monitoring (Lesen/Öffnen)“ verfügen, um diese Daten anzeigen zu dürfen.

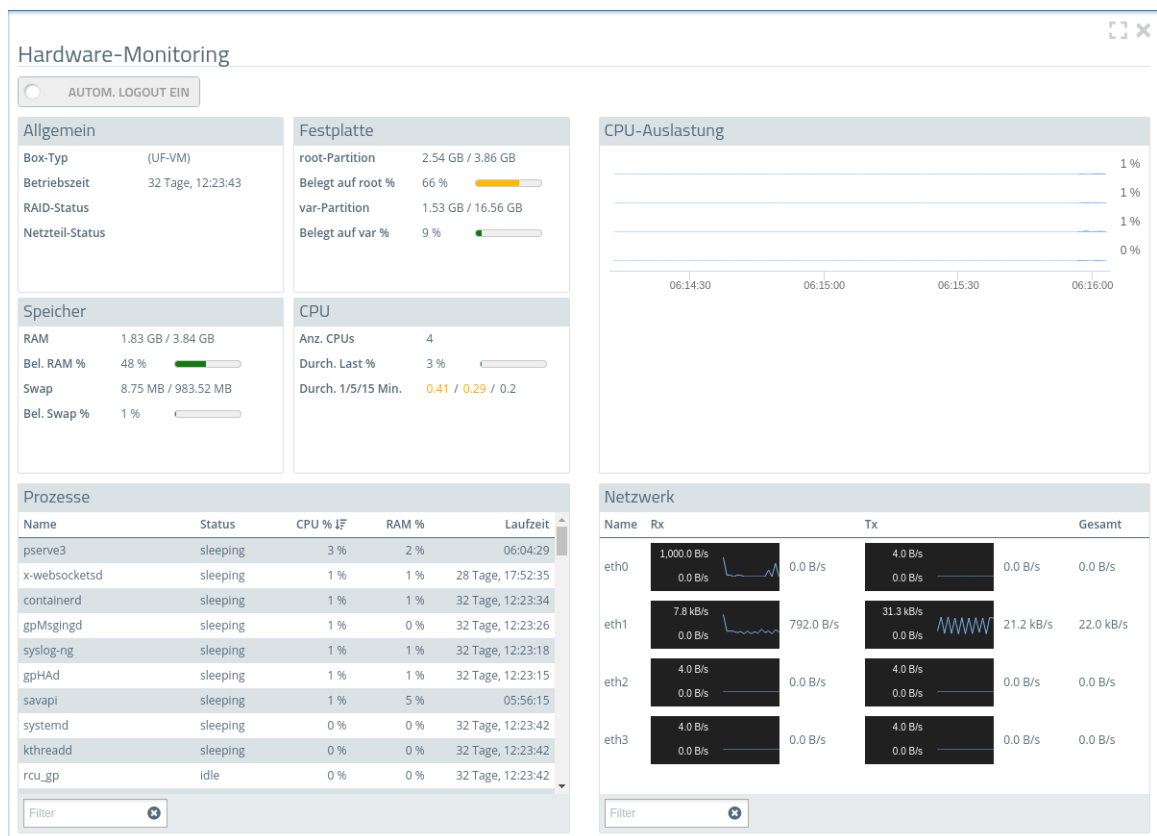


Abbildung 2: Monitoring & Statistiken > Hardware-Monitoring

Eingabefeld	Beschreibung
Automatischer Logout Ein / Aus	Über diesen Schalter können Sie die automatische Abmeldung des Web-Clients ein- bzw. ausschalten. Dadurch lassen sich die Monitor- und Daten über einen längeren Zeitraum verfolgen. ⚡ Dies schaltet eine Sicherheitsfunktion des Web-Clients ab. Nutzen Sie daher in diesem Fall ein von Ihnen anzulegendes Benutzerkonto, welches ausschließlich über die Berechtigung „Monitoring (Lesen/Öffnen)“ verfügt.
	Zeigen Sie den Monitoring-Dialog im Vollbild an.

3.1 System-Informationen

Die System-Informationen werden im oberen linken Bereich angezeigt. Es werden Informationen zu den folgenden Themen angezeigt:

- > **Allgemein:** Informationen über den Firewall-Box-Typ, die Betriebszeit der Firewall, den RAID-Status (wenn vorhanden) und den Netzteil-Status (wenn vorhanden).
- > **Festplatte:** Belegung der root- und var-Partitionen, jeweils in absoluten und prozentualen Werten.
- > **Speicher:** Belegung des Arbeitsspeichers und des Swap, jeweils in absoluten und prozentualen Werten.
- > **CPU:** Anzahl der vorhandenen logischen CPUs, durchschnittliche Auslastung aller CPUs in Prozent und die durchschnittliche CPU-Auslastung der letzten 1, 5 und 15 Minuten. Die angezeigte Auslastung kann auch über 1 liegen. In diesem Fall werden mehr als ein CPU-Kern ausgelastet. Solange der Wert unter der Anzahl der CPUs liegt, ist das System nicht voll ausgelastet. Werte über der Anzahl der verfügbaren CPUs werden in Rot angezeigt.

Die durchschnittliche CPU-Auslastung der letzten 1 bzw. 5 Minuten wird jeweils gelb angezeigt, wenn:

- > 1 Min-Wert: Die durchschnittliche CPU-Auslastung der letzten Minute liegt über dem Auslastungsdurchschnitt der letzten 5 oder 15 Minuten.
- > 5 Min-Wert: Die durchschnittliche CPU-Auslastung der letzten 5 Minuten liegt über dem Auslastungsdurchschnitt der letzten 15 Minuten.

3.2 CPU-Auslastung

Die CPU-Auslastung wird im oberen rechten Bereich angezeigt. Hier wird die Auslastung der einzelnen CPUs über einen Zeitraum von bis zu 5 Minuten angezeigt (bei mehr als 10 CPUs werden zwei Spalten angezeigt, bei mehr als 20 CPUs maximal 3 Spalten).

Wenn der Durchschnitt der letzten 10 Werte der Auslastung einer CPU über 50% liegt, wechselt die Farbe des Diagramms für diese CPU zu orange. Liegt der Durchschnitt der letzten 10 Werte über 75%, wechselt die Farbe des Diagramms zu rot.


3.3 Prozesse

Die Prozesse werden im unteren linken Bereich angezeigt. Zu allen Prozessen werden jeweils die folgenden Informationen angezeigt:

- > **Name**
- > **Status**
- > **CPU-Verwendung in Prozent**
- > **RAM-Verwendung in Prozent**
- > **Laufzeit des Prozesses**

Alle Spalten können auf- oder absteigend sortiert werden.

Zusätzlich kann die Tabelle nach Prozessnamen gefiltert werden. Der Filter unterstützt auch nur den Teil eines Namens.

 Die Liste der verfügbaren Prozesse in dem Filter wird nur einmal beim Öffnen des Hardware-Monitorings geladen, somit werden neu startende Prozesse nicht aufgeführt.

3.4 Netzwerk

Die Netzwerkauslastung wird im unteren rechten Bereich angezeigt. Es wird die aktuelle Auslastung aller verfügbaren Ethernet-Ports mit jeweils den folgenden Informationen angezeigt:

- > **Name**
- > **Rx:** Empfangene Bytes
- > **Tx:** Gesendete Bytes
- > **Gesamt:** Rx + Tx

Über den Filter können einzelne Ethernet-Ports über den Namen gefiltert werden.

4 Management-Bericht

Der Menü-Punkt **Management-Bericht** wurde von **Firewall** zu **Monitoring & Statistiken** verschoben und beinhaltet jetzt zwei Unterpunkte **Aktueller Bericht** und **Mail-Bericht**. Der **aktuelle Bericht** entspricht dabei dem bisherigen **Management-Bericht**.

Navigieren Sie zu **Monitoring & Statistiken > Management-Bericht**, um einen Bericht über die aktuelle Desktopkonfiguration und einige Statistiken zu erstellen und diesen auf Ihren Computer zu übertragen. Alternativ können Sie diesen auch per E-Mail versenden.

4.1 Aktueller Bericht

Navigieren Sie zu **Monitoring & Statistiken > Management-Bericht > Aktueller Bericht**, um einen Bericht über die aktuelle Desktopkonfiguration und einige Statistiken zu erstellen und diesen auf Ihren Computer zu übertragen.

Im Fenster **Management-Bericht** können Sie zwischen den Dateiformaten PDF, HTML und CSV wählen, indem Sie die entsprechende Optionsschaltfläche auswählen. Bei dem Format CSV werden die Tabellen als einzelne CSV-Dateien erstellt und zusammengepackt als ZIP-Datei zum Speichern angeboten. So wird eine eventuelle Weiterverarbeitung der Daten vereinfacht.

Management-Bericht

Bearbeitete Version - Änderungen bleiben erhalten bis zum Zurücksetzen oder Abmelden.

Management-Bericht erstellen als

PDF

HTML

CSV

Kategorien

Desktop-Konfiguration

Sicherheits-Statistiken

Bitte achten Sie darauf, dass in den Statistik-Einstellungen die Datenerfassung aktiviert ist.

Einträge

5

Zeitraum

Letzte Woche

Letzter Monat


Letztes Jahr

Zurücksetzen

Bericht Erstellen & Einstellungen Speichern

Abbildung 3: Management-Bericht – Einstellungen für den Bericht

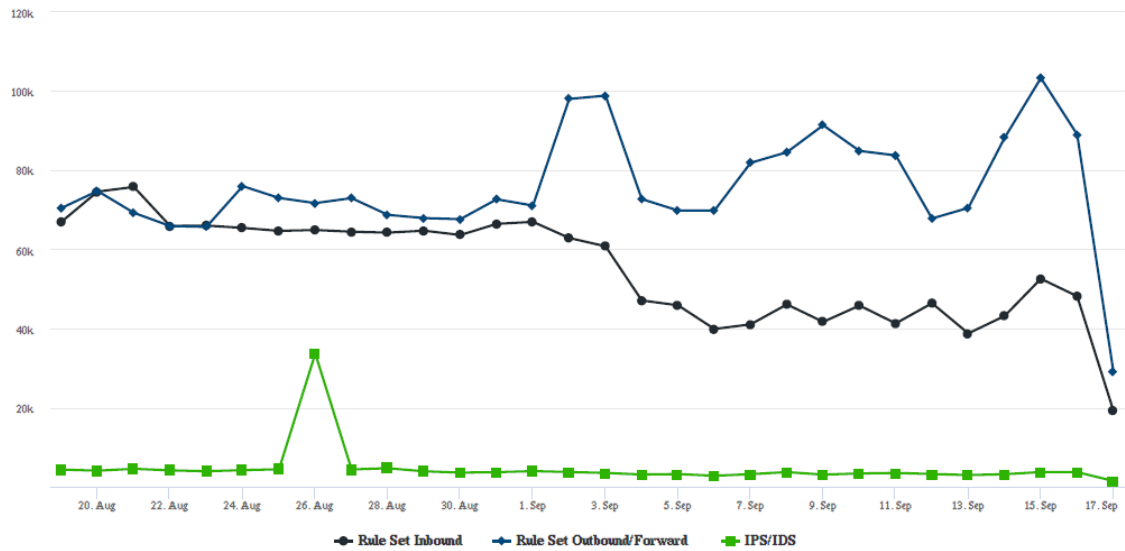
Im Bereich **Kategorien** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Desktop-Konfiguration	<p>Die Exportdatei enthält eine Tabelle mit allen konfigurierten Firewall-Regeln, inklusive zusätzlicher Informationen wie NAT, DMZ, IP-Adressen der Hostobjekte und dem Inhalt der Beschreibungsfelder der konfigurierten Desktop-Objekte und -Verbindungen.</p> <hr/> <p> Desktop-Objekte werden nur mit eingeschlossen, wenn sie mit anderen Desktop-Objekten verknüpft sind.</p>
Sicherheits-Statistiken	<p> Voraussetzung für die Erzeugung von Statistiken ist, dass unter Monitoring & Statistiken > Einstellungen mindestens der Wert „Statistiken führen“ für die Ereignis-Typen eingestellt wurde.</p> <p>Beinhaltet die Statistiken, die auch unter dem Menüpunkt Monitoring & Statistiken > Statistiken > Übersicht verfügbar sind, sowohl als Graph als auch als Tabelle:</p> <ul style="list-style-type: none"> > Blockierte Verbindungen > Blockierter Inhalt > Top aufgerufene Domains > Top blockierte Domains > Top Traffic pro Quelle <p>Wenn Sicherheits-Statistiken aktiviert sind, können weitere Einstellungen vorgenommen werden:</p> <ul style="list-style-type: none"> > Anzahl der Einträge (diese Einstellung gilt nur für die Toplisten) > Zeitraum, Festlegung des zu erfassenden Zeitraums beginnend mit dem aktuellen Zeitpunkt

Klicken Sie auf **Bericht erstellen**, wenn Sie die Exportdatei erstellen und übertragen möchten. Ihre Einstellungen werden gesichert und ein Dateiname mit einem Datumspräfix (YYYY-MM-DD_HH-mm) vorgeschlagen. Klicken Sie ansonsten auf **Zurücksetzen**, um die Einstellungen auf die zuletzt gespeicherten Einstellungen zurück zu setzen.



Blocked Connections



Date	Rule Set Inbound	Rule Set Outbound/Forward	IPS/IDS
17. Sep	19272	29097	1559
16. Sep	48169	88978	3784
15. Sep	52570	103212	3815
14. Sep	43177	88127	3261
13. Sep	38790	70447	3052

Abbildung 4: Beispiel aus einem Management-Bericht

Source	Action	NAT	Destination	Service	Rule Settings	Connection Settings
eth2 LAN Connection 10.10.21.0/24	→	→	WAN eth0 WAN Connection	IMAP4 143 TCP	Proxy: IMAP4	Webfilter: Sex: Content Filter Kriminell: Content Filter Werbung: Content Filter
	→	→		POP3s 995 TCP	Proxy: POP3S	
	→	→		SMTP 25 TCP	Proxy: SMTP	
	→	→		IMAP4s 993 TCP	Proxy: IMAP4S	
	→	→		POP3 110 TCP	Proxy: POP3	
	→	→		SMTPs 465 TCP	Proxy: SMTPS	
	→	→		HTTPS 443 TCP	Proxy: HTTPS	
	→	→		HTTP 80 TCP	Proxy: HTTP	
eth1 LAN Connection 10.10.20.0/24	→	→	WAN eth0 WAN Connection	HTTPS 443 TCP	Proxy: HTTPS	Webfilter: Sex: Content Filter Kriminell: Content Filter Werbung: Content Filter
	→	→		HTTP 80 TCP	Proxy: HTTP	

Abbildung 5: Beispiel aus einem Management-Bericht

4.2 Mail-Bericht

Navigieren Sie zu **Monitoring & Statistiken > Management-Bericht > Mail-Bericht**, um einen regelmäßigen Bericht über die aktuelle Desktopkonfiguration und einige Statistiken zu erstellen und diesen per E-Mail zu versenden. Anders als im **Aktuellen Bericht** beinhaltet der **Mail-Bericht** immer sowohl die Desktop-Konfiguration als auch die Statistiken.


 Der Mail-Bericht nutzt das Firewall-interne Mail-System. Deshalb müssen unter **Firewall > E-Mail-Einstellungen** die Basis-Einstellungen konfiguriert sein, damit E-Mails versendet werden können.

Abbildung 6: Mail-Bericht – Einstellungen für den Bericht

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob das Versenden eines regelmäßig erzeugten Reports derzeit aktiv (I), oder inaktiv (O) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Bericht anhängen als	Wählen Sie aus den möglichen Formaten PDF, HTML oder CSV eines aus.
Intervall	Geben Sie an, ob der Report wöchentlich oder monatlich versendet werden soll.
Start-Zeit	Geben Sie den Zeitpunkt für das erstmalige Versenden des Reports an.
Mail-Betreff	Geben Sie einen eigenen Betreff für die Report-E-Mail an.
Empfänger	Geben Sie in dieser Liste alle E-Mail-Adressen an, die den Report erhalten sollen.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie Änderungen vorgenommen haben. Um die Änderungen zu übernehmen, klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

5 LLDP

Ab LCOS FX 10.12 wird LLDP unterstützt.

Das LLDP (Link Layer Discovery Protocol) wird verwendet, um Informationen wie z. B. Interface MAC-Adressen oder System-Beschreibungen mit direkt verbundenen Nachbar-Geräten auszutauschen. Es operiert dabei auf Layer 2. Jedes Interface sendet und empfängt Informationen separat. So sendet das lokale Interface eth1 nur Informationen über sich selbst an Nachbarn, mit denen das lokale Gerät auf diesem Interface verbunden ist. Beim Empfangen verhält es sich genau so. Informationen werden ausschließlich mit unmittelbaren Nachbarn ausgetauscht und können verwendet werden, um beispielsweise beim Verkabeln von Geräten zu unterstützen.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu LLDP.

5.1 Einstellungen für LLDP

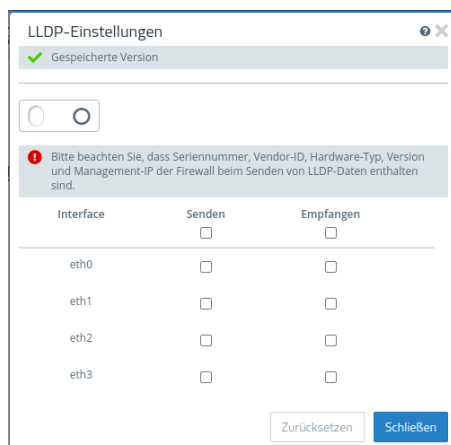



Abbildung 7: Netzwerk > LLDP > LLDP-Einstellungen

Unter **Netzwerk > LLDP > LLDP-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob die LLDP-Einstellungen derzeit aktiv (I), oder inaktiv (0) sind. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Interface	Aktivieren Sie für jedes vorhandene Interface, ob LLDP-Daten separat gesendet oder empfangen werden sollen. Im Tabellenheader können Sie dies auch für alle Interfaces gleichzeitig einstellen.  Beachten Sie, dass beim Senden verschiedene Informationen über die Firewall gesendet werden: Seriennummer, Vendor-ID, Hardware-Typ, Version und Management-IP der Firewall.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie Änderungen vorgenommen haben. Um die Änderungen zu übernehmen, klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

5.2 Informationen zu LLDP

Navigieren Sie zu **Monitoring & Statistiken > LLDP**, um ein Fenster zu öffnen, in dem die Informationen zum Link Layer Discovery Protocol (LLDP) eingesehen werden können, die empfangen wurden.

Spalte	Beschreibung
Port-ID (Lokal)	Lokales Interface der Firewall, auf dem die LLDP-Nachricht empfangen wurde.
Chassis-ID	Die MAC-Adresse des Nachbar-Geräts.
System-Beschreibung	Eine Beschreibung des Geräts, z. B. Betriebssystem, Version, etc.
System-Fähigkeiten	Eine Auflistung von Fähigkeiten, über die das Nachbar-Gerät verfügt.
Port-ID (Remote)	Remote-Interface des Nachbarn, von dem aus die LLDP-Nachricht gesendet wurde.
Port-Beschreibung	Beschreibung des Remote Nachbar-Ports.
Management-Adresse	Adresse, unter der weitere Informationen über den Nachbarn zu finden sind.
TTL	Time To Live, Dauer der Gültigkeit der Nachbar-Informationen in Sekunden.

Alle Spalten können auf Basis einer der Spalten auf- oder absteigend sortiert werden.

6 WireGuard

Das WireGuard-Protokoll wurde für VPN-Verbindungen neu hinzugefügt. Dazu kann man nun ein entsprechendes Interface einrichten. Über dieses dann Verbindungen einrichten und den Status dieser Verbindungen anzeigen.

6.1 WireGuard-Interfaces

Mit den Einstellungen unter **WireGuard-Interfaces** können Sie per WireGuard gesicherte Interfaces einrichten.

In den folgenden Abschnitten finden Sie detailliertere Informationen zu WireGuard-Interfaces.

6.1.1 Einstellungen zu WireGuard-Interfaces

Unter **Netzwerk > Interfaces > WireGuard-Interfaces** können Sie ein neues WireGuard-Interface hinzufügen oder ein vorhandenes bearbeiten.

Im Bearbeitungsfenster **WireGuard-Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob das WireGuard-Interface aktiv (I) oder inaktiv (O) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des WireGuard-Interfaces ändern. Neu angelegte WireGuard-Interfaces sind standardmäßig aktiviert.
Name	Zeigt den Namen des WireGuard-Interfaces an. Der Name wird automatisch nach dem Schema wg-<x> generiert.
Verwendet von	Zeigt die Netzwerkkomponenten (z. B. Verbindungen, andere Interfaces etc.) an, die das WireGuard-Interface verwenden.
Status	Zeigt den aktuellen Status des WireGuard-Interfaces an.
MTU	Legen Sie die maximale Paketgröße in Bytes fest.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues WireGuard-Interface hinzufügen oder ein bestehendes WireGuard-Interface bearbeiten. Klicken Sie für ein neu konfiguriertes WireGuard-Interface auf **Erstellen**, um es zur Liste der verfügbaren WireGuard-Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen WireGuard-Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte WireGuard-Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf **✓ Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

6.2 WireGuard

Richten Sie unter **VPN > WireGuard** per WireGuard gesicherte VPN-Verbindungen ein.

6.2.1 WireGuard-Verbindung

Unter **VPN > WireGuard** können Sie WireGuard VPN-Verbindungen verwalten.

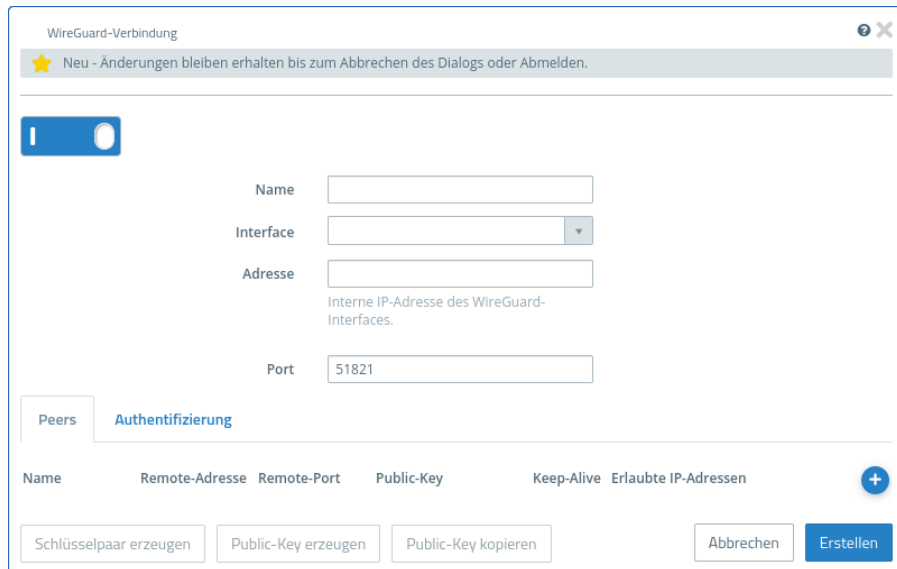



Abbildung 8: VPN > WireGuard > WireGuard-Verbindung

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob diese WireGuard-Verbindung aktiv (I) oder inaktiv (O) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Name	Geben Sie dieser WireGuard-Verbindung einen Namen.
Interface	Auswahlliste, in der WireGuard-Interfaces ausgewählt werden können. Siehe WireGuard-Interfaces auf Seite 15.
Adresse	Geben Sie hier die IP-Adresse des WireGuard-Interfaces an. Dies kann sowohl eine implizite IP-Adresse (/32 Präfix-Länge) als auch eine IP-Adresse mit Präfix-Länge kleiner als 32 sein.
Port	Port auf der Firewall, über den die WireGuard-Verbindung von der Gegenstelle aufgebaut werden kann. Für die erste Verbindung wird der Standard-Port 51820 vorgeschlagen, danach wird für jede weitere Verbindung hochgezählt bzw. der nächste nicht verwendete Port vorgeschlagen.

Unter dem Reiter **Peers** können Gegenstellen konfiguriert werden. Klicken Sie auf , um den Peer-Dialog zu öffnen.

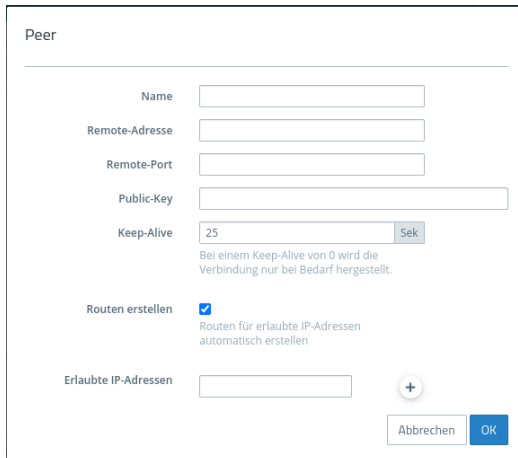


Abbildung 9: VPN > WireGuard > WireGuard-Verbindung > Peers

Tabelle 1: Peers

Eingabefeld	Beschreibung
Name	Geben Sie dieser Gegenstelle einen Namen.
Remote-Adresse	Optionale externe und somit über das Internet erreichbare Adresse der Gegenstelle. Kann auch ein Domainname sein. Wenn angegeben, dann wird die Firewall versuchen, die Verbindung zu initiieren. Die Angabe wird benötigt, wenn ein Remote-Port angegeben ist.
Remote-Port	Optionaler Port, über den die Verbindung aufgebaut werden soll. Wird benötigt, wenn eine Remote-Adresse angegeben ist.
Public-Key	Der Base64-kodierte Public-Key der Gegenstelle.
Keep-Alive	Intervall in Sekunden zum Senden von Paketen zur Aufrechterhaltung der Verbindung, Default 25, bei einem Wert von 0 wird die Verbindung nur bei Bedarf hergestellt.
Routen erstellen	Wenn aktiviert, dann werden alle IP-Adressen unter Erlaubte IP-Adressen automatisch in die Routing-Tabelle 201 eingetragen. Sonst müssen Sie die Routen manuell erstellen.
Erlaubte IP-Adressen	IP-Adressen oder Netze mit Subnetzmaske, die über die WireGuard-Verbindung erreichbar sein sollen.

Unter dem Reiter **Authentifizierung** kann ein Private- / Public-Key-Paar erzeugt werden. Diese werden bei WireGuard anstelle von Zertifikaten verwendet.



Abbildung 10: VPN > WireGuard > WireGuard-Verbindung > Authentifizierung

Tabelle 2: Authentifizierung

Eingabefeld	Beschreibung
Private-Key ändern	Diese Option soll verhindern, dass ein bereits eingegebener Key überschrieben wird. Das Aktivieren dieses Hakens aktiviert auch die Schaltfläche Schlüsselpaar erzeugen .
Private-Key	Geben Sie entweder einen Base64-String als Private-Key ein oder lassen Sie das Feld leer.
Public-Key	Der Public Key zum Private Key. Generieren Sie ihn ggfs. mittels Schlüsselpaar erzeugen .
Schlüsselpaar erzeugen	Mit einem Klick auf diese Schaltfläche erzeugen Sie ein Private- / Public-Key-Paar. Falls bereits ein Private-Key existiert, dann erhalten Sie eine Sicherheitsabfrage.
Public-Key erzeugen	Mit einem Klick auf diese Schaltfläche erzeugen Sie einen Public-Key zu einem bereits eingetragenen Private-Key.
Public-Key kopieren	Kopieren Sie den Public Key in die Zwischenablage. Der kopierte Schlüssel kann dann auf der Gegenstelle eingetragen werden, oder an den Admin der Gegenstelle versendet werden.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Verbindung hinzufügen oder eine bestehende bearbeiten. Klicken Sie für eine neu konfigurierte Verbindung auf **Erstellen**, um sie zur Liste der verfügbaren Verbindungen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Verbindung klicken Sie auf **Speichern**, um die neu konfigurierte Verbindung zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen.

6.3 WireGuard-Status

Unter **Monitoring & Statistiken > WireGuard-Status** kann der Status der WireGuard-Verbindungen überwacht werden. Ob eine Verbindung tatsächlich aufgebaut wurde wird bei WireGuard nicht angezeigt.

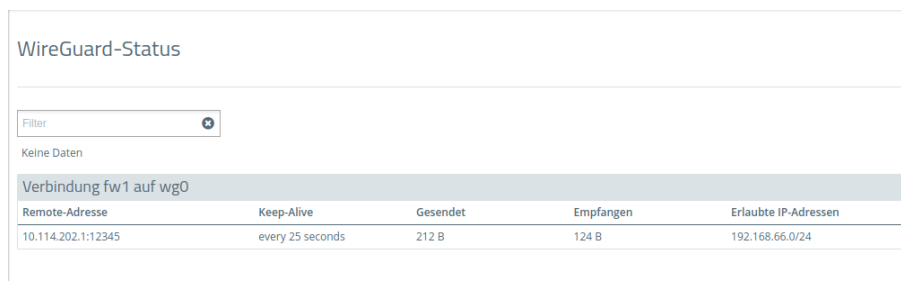


Abbildung 11: Monitoring & Statistiken > WireGuard-Status

Spalte	Beschreibung
Remote-Adresse	Die Remote-Adresse dieser WireGuard-Verbindung. Nach dieser Spalte kann gefiltert werden.
Keep-Alive	Der eingestellte Keep-Alive-Wert dieser WireGuard-Verbindung.
Gesendet	Über diese Verbindung gesendete Bytes.
Empfangen	Über diese Verbindung empfangene Bytes.
Erlaubte IP-Adressen	Die konfigurierten erlaubten IP-Adressen dieser WireGuard-Verbindung. Nach dieser Spalte kann gefiltert werden.

7 Export von Protokollen

Audit-, Alarm- und Systemprotokolle können nun in den Formaten PDF, HTML und CSV exportiert werden. Dafür wurde jeweils ein neues Dropdown **Export** hinzugefügt bzw. das vorhandene erweitert. Der Export der Protokolle berücksichtigt hierbei alle eingestellten Filter.

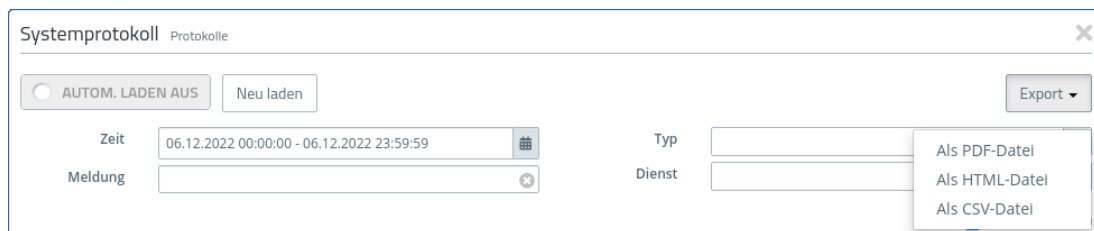


Abbildung 12: Monitoring & Statistiken > Protokolle > Systemprotokoll

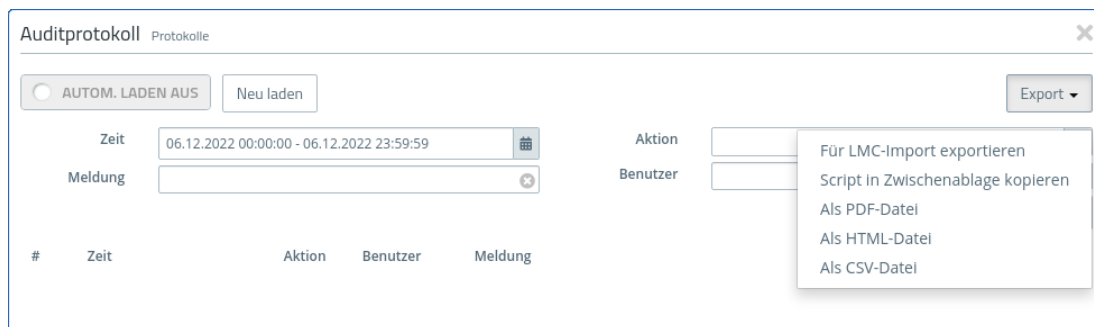


Abbildung 13: Monitoring & Statistiken > Protokolle > Auditprotokoll

8 DNS-basierte Regeln

Es ist nun möglich, Host-Objekte und Objekte in Hostgruppen neben IP-Adressen auch mit Domainnamen zu konfigurieren, so dass Regeln dynamisch für diese Objekte erzeugt werden können.

Dafür wurden im Frontend zwei Dialoge angepasst.

- Im Host-Dialog wurde das Feld **IP-Adresse** in **Host** umbenannt
- Im Hostgruppen-Dialog wurde die Spaltenüberschrift von **Host-/Netzwerk-IP** in **Host/Netzwerk** umbenannt

Hosts

Neu - Änderungen bleiben erhalten bis zum Abbrechen des Dialogs oder Abmelden.

Name

Beschreibung

Tags

Farbe

Anmeldung erlauben

Icon Computer Notebook
 Server VoIP
 Drucker

Interface

Host

Von IDS/IPS-Überprüfung ausnehmen

Von Anti-Virus-Überprüfung ausnehmen

Abbrechen Erstellen

Abbildung 14: Desktop > Desktop-Objekte > Hosts

The screenshot shows a configuration window titled 'Host-/Netzwerk-Gruppe' with a 'Neu' (New) button. The form contains the following fields and options:

- Name:** A text input field.
- Beschreibung:** A larger text input field.
- Tags:** A text input field.
- Farbe:** A color selection dropdown menu.
- Von IDS/IPS-Überprüfung ausnehmen:** A checkbox.
- Von Anti-Virus-Überprüfung ausnehmen:** A checkbox.
- Hosts/Netzwerke:** A table with columns: Name, Login erlaubt, Interface, and Host/Netzwerk.

Hosts/Netzwerke	Name	Login erlaubt	Interface	Host/Netzwerk
	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

At the bottom right, there are two buttons: 'Abbrechen' (Cancel) and 'Erstellen' (Create). A blue '+' button is also visible next to the 'Host/Netzwerk' column header.

Abbildung 15: Desktop > Desktop-Objekte > Host-/Netzwerk-Gruppen

9 BGP-Erweiterung

Zwei neue Einstellungen wurden der BGP-Konfiguration hinzugefügt.

Abbildung 16: Netzwerk > Routing > BGP

Eingabefeld	Beschreibung
Multihop-Peers	Stellen Sie die max. Anzahl an Hops ein, über die ein Peer erreicht werden kann. Mögliche Werte: 0 bis 255 (bei 0 werden nur direkt verbundene Peers berücksichtigt).
Ziel-Routing-Tabelle	Routing-Tabelle, in die die gelernten Routing-Einträge geschrieben werden sollen. Mögliche Werte: 254 (Haupttabelle) oder 512 bis 65535 (benutzerdefinierte Tabellen)