

# Konfiguration des Systemprotokolls auf den VPN-Routern der Serien RV320 und RV325

## Ziel

Systemprotokolle sind Datensätze von Netzwerkereignissen. Protokolle sind ein wichtiges Tool, mit dem Sie den Netzwerkbetrieb nachvollziehen können. Sie sind nützlich für das Netzwerkmanagement und die Fehlerbehebung im Netzwerk.

In diesem Artikel wird erläutert, wie Sie die Protokolltypen konfigurieren, die aufgezeichnet werden sollen, wie Sie die Protokolle auf der RV32x VPN Router-Serie anzeigen und wie Sie die Protokolle über SMS, einen Systemprotokollserver oder per E-Mail an einen Empfänger senden.

## Anwendbare Geräte

- RV320 Dual-WAN VPN-Router
- RV325 Gigabit Dual-WAN VPN-Router

## Softwareversion

·v1.1.0.09

## Systemprotokollkonfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Protokoll > Systemprotokoll**. Die Seite *Systemprotokoll* wird geöffnet:

## System Log

---

**Send SMS**

SMS:  Enable  
 USB1  USB2

Dial Number1 :

Dial Number2 :

Link Up  Link Down  Authentication Failed  
 System Startup

---

**Syslog Configuration**

Syslog1:  Enable  
Syslog Server 1:  Name or IPv4 / IPv6 Address

Syslog2:  Enable  
Syslog Server 2:  Name or IPv4 / IPv6 Address

---

**Email**

Email:  Enable  
Mail Server:  Name or IPv4 / IPv6 Address  
Authentication:    
SMTP Port:  Range: 1-65535 Default 25  
Username:

Informationen zur Seite *Systemprotokoll* finden Sie in den folgenden Abschnitten.

- [System Logs by SMS](#) (Systemprotokolle per SMS): Senden der Systemprotokolle über SMS an ein Telefon.
- [Systemprotokolle auf Systemprotokollservern](#) - Senden der Systemprotokolle an einen Systemprotokollserver
- [E-Mail-Systemprotokolle](#) - Senden der Systemprotokolle an eine E-Mail-Adresse
- [Log Settings](#) (Protokolleinstellungen): Konfigurieren der Art der Meldungen, die im Protokoll gespeichert werden.
- [Systemprotokoll anzeigen](#): Anzeigen der Systemprotokolle auf dem Gerät
- [Tabelle ausgehender Protokolle anzeigen](#) - Anzeigen von Systemprotokollen, die sich nur auf ausgehende Pakete beziehen.
- [Tabelle für eingehende Protokolle anzeigen](#) - Anzeigen von Systemprotokollen, die sich nur auf eingehende Pakete beziehen.

## Systemprotokolle per SMS

**Send SMS**

SMS:  Enable

USB1  USB2

Dial Number1 :

Dial Number2 :

Link Up  Link Down  Authentication Failed

System Startup

Schritt 1: Aktivieren Sie im Feld SMS das **Aktivieren**, um Systemprotokolle über SMS-Nachrichten (Short Message Service) an einen Client zu senden.

Schritt 2: Aktivieren Sie die Kontrollkästchen der USB-Ports, an die das 3G-USB-Modem angeschlossen ist.

Schritt 3: Aktivieren Sie das Kontrollkästchen im Feld Dial Number1 (Wählnummer1), und geben Sie die Telefonnummer ein, an die die Nachrichten gesendet werden.

**Hinweis:** Klicken Sie auf **Test**, um die Verbindung mit der Wählnummer 1 zu testen. Wenn die konfigurierte Nummer die Testnachricht nicht empfängt, vergewissern Sie sich, dass die Telefonnummer korrekt im Feld Dial Number1 (Wählnummer1) eingegeben wurde.

Schritt 4: (Optional) Aktivieren Sie das Kontrollkästchen im Feld Dial Number2 (Wählnummer 2), und geben Sie die Telefonnummer ein, an die die Nachrichten gesendet werden.

**Hinweis:** Klicken Sie auf **Test**, um die Verbindung mit der Wählnummer 2 zu testen. Wenn die konfigurierte Nummer die Testnachricht nicht empfängt, stellen Sie sicher, dass die Telefonnummer korrekt in das Feld Dial Number2 (Wählnummer 2) eingegeben wurde.

Schritt 5: Aktivieren Sie die Kontrollkästchen der Ereignisse, die ein zu sendendes Protokoll auslösen.

- Link Up (Verbindung aufheben): Eine Verbindung zum RV320 wurde aktiviert.
- Link Down - Eine Verbindung zum RV320 wurde deaktiviert.
- Authentifizierung fehlgeschlagen - Eine Authentifizierung ist fehlgeschlagen.
- Systemstart - Der Router wird hochgefahren.

Schritt 6: Klicken Sie auf **Speichern**. Die Systemprotokolle über SMS werden konfiguriert.

## Systemprotokolle auf Systemprotokollservern

**Syslog Configuration**

Syslog1:  Enable

Syslog Server 1:  Name or IPv4 / IPv6 Address

Syslog2:  Enable

Syslog Server 2:  Name or IPv4 / IPv6 Address

Schritt 1: Aktivieren Sie **Aktivieren** im Feld Syslog1, um Systemprotokolle an einen Systemprotokollserver zu senden.

Schritt 2: Geben Sie den Hostnamen oder die IP-Adresse des Systemprotokollservers in das Feld Syslog Server 1 (Syslog-Server 1) ein.

Schritt 3: (Optional) Um Protokolle an einen anderen Systemprotokollserver zu senden, aktivieren Sie im Feld Syslog2 die **Option Enable (Aktivieren)**.

Schritt 4: Wenn das Kontrollkästchen im Feld Syslog2 aktiviert ist, geben Sie den Hostnamen oder die IP-Adresse des Systemprotokollservers in das Feld Syslog Server 2 (Syslog-Server 2) ein.

Schritt 5: Klicken Sie auf **Speichern**. Das System protokolliert die Systemprotokollserver und wird konfiguriert.

## E-Mail-Systemprotokolle

**Email**

Email:  Enable

Mail Server:  Name or IPv4 / IPv6 Address

Authentication:  ▾

SMTP Port:  Range: 1-65535 Default 25

Username:

Password:

Send Email to 1:  Email Address

Send Email to 2:  Email Address(Optional)

Log Queue Length:  entries

Log Time Threshold:  min

Real Time Alert:  Email Alert when block/filter contents accessed  
 Email Alert for Hacker Attack

Schritt 1: Aktivieren Sie **Aktivieren** im Feld E-Mail, um Systemprotokolle per E-Mail an einen Empfänger zu senden.

Schritt 2: Geben Sie den Domännennamen oder die IP-Adresse des Mailservers im Feld Mail Server (Mail-Server) ein.

Schritt 3: Wählen Sie im Feld Authentifizierung den Authentifizierungstyp aus, den der Mail-Server verwendet.

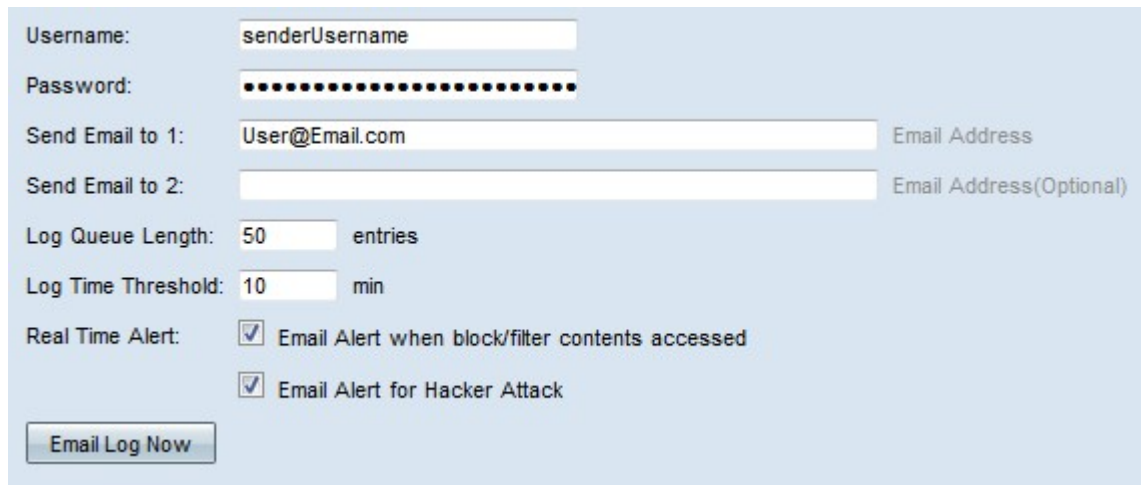
·None (Keine): Der Mailserver verwendet keine Authentifizierung.

·Login Plain (Nur Anmeldung): Der Mailserver verwendet eine Authentifizierung im Textformat.

·TLS - Der Mailserver verwendet Transport Layer Security (TLS), um dem Client und dem Server den sicheren Austausch von Authentifizierungsinformationen zu ermöglichen.

·SSL - Der Mailserver verwendet SSL (Secure Sockets Layer), um dem Client und dem Server den sicheren Austausch von Authentifizierungsinformationen zu ermöglichen.

Schritt 4: Geben Sie den SMTP-Port (Simple Mail Transfer Protocol) ein, den der Mailserver im Feld SMTP Port (SMTP-Port) verwendet. SMTP ist ein Protokoll, das die Übertragung von E-Mails über IP-Netzwerke ermöglicht.



Username:

Password:

Send Email to 1:  Email Address

Send Email to 2:  Email Address(Optional)

Log Queue Length:  entries

Log Time Threshold:  min

Real Time Alert:  Email Alert when block/filter contents accessed

Email Alert for Hacker Attack

Schritt 5: Geben Sie den Benutzernamen des E-Mail-Absenders in das Feld Benutzername ein.

Schritt 6: Geben Sie das Kennwort des E-Mail-Absenders in das Feld Kennwort ein.

Schritt 7: Geben Sie die E-Mail-Adresse des E-Mail-Empfängers im Feld E-Mail an 1 senden ein.

Schritt 8: (Optional) Geben Sie im Feld E-Mail an 2 senden eine zusätzliche E-Mail-Adresse ein, an die Sie Protokollnachrichten senden können.

Schritt 9: Geben Sie die Anzahl der Protokolleinträge ein, die vor dem Senden des Protokolls an den E-Mail-Empfänger im Feld Log Queue Length (Länge der Protokollwarteschlange) gemacht werden müssen.

Schritt 10: Geben Sie das Intervall ein, in dem das Gerät das Protokoll an die E-Mail sendet, im Feld "Log Time Threshold" (Schwellenwert für Protokollzeit).

Schritt 11: Aktivieren Sie das erste Kontrollkästchen im Feld "Real Time Alert" (Echtzeit-Warnung), um sofort eine E-Mail zu senden, wenn jemand, der blockiert oder gefiltert wurde, versucht, auf den Router zuzugreifen.

Schritt 12: Aktivieren Sie das zweite Kontrollkästchen im Feld "Real Time Alert" (Echtzeit-Warnung), um sofort eine E-Mail zu senden, wenn ein Hacker versucht, über einen DOS-Angriff (Denial of Service) auf den Router zuzugreifen.

**Hinweis:** Klicken Sie auf **E-Mail-Protokoll jetzt**, um das Protokoll sofort zu senden.

Schritt 13: Klicken Sie auf **Speichern**. Das System meldet sich per E-Mail an.

## Protokolleinstellungen

**Log**

Alert Log:	<input checked="" type="checkbox"/> Syn Flooding	<input checked="" type="checkbox"/> IP Spoofing	<input checked="" type="checkbox"/> Unauthorized Login Attempt
	<input type="checkbox"/> Ping Of Death	<input type="checkbox"/> Win Nuke	
General Log:	<input type="checkbox"/> Deny Policies	<input type="checkbox"/> Authorized Login	<input checked="" type="checkbox"/> System Error Messages
	<input type="checkbox"/> Allow Policies	<input type="checkbox"/> Kernel	<input checked="" type="checkbox"/> Configuration Changes
	<input type="checkbox"/> IPsec & PPTP VPN	<input type="checkbox"/> SSL VPN	<input checked="" type="checkbox"/> Network

Schritt 1: Aktivieren Sie die Kontrollkästchen der Ereignisse, die einen Protokolleintrag auslösen.

·Warnprotokoll - Diese Protokolle werden erstellt, wenn ein Angriff oder ein versuchter Angriff stattgefunden hat.

- Syn Flooding - Die SYN-Anfrage wird schneller empfangen, als der Router sie verarbeiten kann.

- IP-Spoofing - Der RV320 hat IP-Pakete mit gefälschten Quell-IP-Adressen empfangen.

- Unauthorized Login Attempt (Nicht autorisierter Anmeldeversuch): Ein abgelehnter Anmeldeversuch beim Netzwerk ist fehlgeschlagen.

- Ping of Death - Ein Ping einer ungewöhnlichen Größe wurde an eine Schnittstelle gesendet, um das Zielgerät abzustürzen.

- Win Nuke - Der Remote-DDOS-Angriff (Distributed Denial of Service Attack), bekannt als WinNuke, wurde an eine Schnittstelle gesendet, um das Zielgerät abzustürzen.

·Allgemeines Protokoll - Diese Protokolle werden erstellt, wenn allgemeine Netzwerkaktionen auftreten.

- Richtlinien verweigern - Der Zugriff für einen Benutzer wurde basierend auf den konfigurierten Richtlinien des Routers verweigert.

- Authorized Login (Autorisierte Anmeldung) - Ein Benutzer wurde autorisiert, auf das Netzwerk zuzugreifen.

- Systemfehlermeldungen - Ein Systemfehler ist aufgetreten.

- Richtlinien zulassen - Der Zugriff wurde einem Benutzer basierend auf den konfigurierten Richtlinien des Routers gewährt.

- Kernel - Bringen Sie alle Kernelmeldungen in das Protokoll ein. Der Kernel ist der erste Teil des Betriebssystems, der beim Hochfahren in den Speicher geladen wird. Kernel-Meldungen sind Protokolle, die dem Kernel zugeordnet sind.

- Konfigurationsänderungen - Die Router-Konfiguration wurde geändert.

- IPSEC- und PPTP-VPN - Es ist eine IPSEC- und PPTP-VPN-Aushandlung, -Verbindung oder -Trennung aufgetreten.

- SSL VPN - Es ist eine SSL VPN-Aushandlung, -Verbindung oder -Trennung aufgetreten.

- Netzwerk - Auf den WAN- oder DMZ-Schnittstellen wurde eine physische Verbindung hergestellt oder unterbrochen.

Schritt 2: Klicken Sie auf **Speichern**. Die Protokolleinstellungen werden konfiguriert.

**Hinweis:** Klicken Sie auf **Protokoll löschen**, um das aktuelle Protokoll zu löschen.

## Systemprotokoll anzeigen



The screenshot shows a 'Log' configuration window with several sections of checkboxes. The 'View System Log...' button is circled in red. Below the checkboxes are four buttons: 'View System Log...', 'Outgoing Log Table...', 'Incoming Log Table...', and 'Clear Log'.

Schritt 1: Klicken Sie auf **Systemprotokoll anzeigen**, um die Systemprotokolltabelle anzuzeigen. Das Fenster *Systemprotokolltabelle* wird angezeigt.

Current Time: Sat Apr 6 10:59:40 2013 All Log ▾

System Log Table		
Time ▾	Event-Type	Message
Apr 6 10:59:34 2013	Kernel	kernel: tr_enable=0, smartqos=0, period=0
Apr 6 10:59:34 2013	Kernel	kernel: wrong ip[0],not_list[0]

Refresh Close

Schritt 2: (Optional) Wählen Sie aus der Dropdown-Liste den Protokolltyp aus, den Sie anzeigen möchten.

- All Log (Gesamtes Protokoll): Enthält alle Protokollmeldungen.
- Systemprotokoll: Enthält nur die Systemfehlermeldungen.
- Firewall/DoS-Protokoll - Enthält nur die Warnprotokolle.
- VPN-Protokoll - Enthält nur IPSec- und PPTP VPN- und SSL VPN-Protokolle.
- Netzwerkprotokoll - Enthält nur die Netzwerkprotokolle.
- Kernel Log (Kernelprotokoll) - Enthält nur Kernelmeldungen.
- Benutzerprotokoll: Enthält nur Richtlinien verweigern, Richtlinien zulassen, autorisierte Anmelde- und Konfigurationsprotokolle
- SSL Log (SSL-Protokoll) - Enthält nur SSL VPN-Protokolle.

In der Systemprotokolltabelle werden die folgenden Informationen angezeigt.

·Zeit - Die Uhrzeit, zu der das Protokoll erstellt wurde.

·Ereignistyp: Der Protokolltyp.

·Meldung - Informationen, die dem Protokoll entsprechen. Dazu gehören der Richtlinienentyp, die Quell-IP-Adresse und die Quell-MAC-Adresse.

**Hinweis:** Klicken Sie auf **Aktualisieren**, um die Protokolltabelle zu aktualisieren.

## Tabelle ausgehender Protokolle anzeigen

The screenshot shows a configuration window for logs. It has two sections: 'Alert Log' and 'General Log'. Under 'Alert Log', there are three checked items: 'Syn Flooding', 'IP Spoofing', and 'Unauthorized Login Attempt'. Under 'General Log', there are several unchecked items: 'Deny Policies', 'Allow Policies', 'IPSec & PPTP VPN', 'Authorized Login', 'Kernel', 'SSL VPN', 'System Error Messages', 'Configuration Changes', and 'Network'. At the bottom, there are four buttons: 'View System Log...', 'Outgoing Log Table...' (highlighted with a red circle), 'Incoming Log Table...', and 'Clear Log'.

Schritt 1: Klicken Sie auf **Tabelle ausgehender Protokolle**, um die Protokolltabelle anzuzeigen, die sich nur auf ausgehende Pakete bezieht. Das Fenster *Tabelle ausgehender Protokolle* wird angezeigt.

Current Time: Sat Apr 6 10:57:28 2013

Outgoing Log Table		
Time	Event-Type	Message
Apr 6 10:57:22 2013	Connection Accepted	IN=eth0 OUT=eth1 SRC=192.168.1.150 DST=156.26.180.254 DMAC= SMAC= LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=15306 DF PROTO=TCP SPT=63865 DPT=80 WINDOW=8192 RES=0x00 SYN URGP=0
Apr 6 10:57:24 2013	Connection Accepted	IN=eth0 OUT=eth1 SRC=192.168.1.150 DST=156.26.180.254 DMAC= SMAC= LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=15312 DF PROTO=TCP SPT=63868 DPT=80 WINDOW=8192 RES=0x00 SYN URGP=0

Refresh Close

In der Tabelle für ausgehende Protokolle werden die folgenden Informationen angezeigt.

·Zeit - Die Uhrzeit, zu der das Protokoll erstellt wurde.

·Ereignistyp: Der Protokolltyp.

·Meldung - Informationen, die dem Protokoll entsprechen. Dazu gehören der Richtlinienentyp, die Quell-IP-Adresse und die Quell-MAC-Adresse.

**Hinweis:** Klicken Sie auf **Aktualisieren**, um die Protokolltabelle zu aktualisieren.

## Tabelle für eingehende Protokolle anzeigen



**Log**

Alert Log:  Syn Flooding  IP Spoofing  Unauthorized Login Attempt  
 Ping Of Death  Win Nuke

General Log:  Deny Policies  Authorized Login  System Error Messages  
 Allow Policies  Kernel  Configuration Changes  
 IPSec & PPTP VPN  SSL VPN  Network

Schritt 1: Klicken Sie auf **Tabelle eingehender Protokolle**, um die Protokolltabelle anzuzeigen, die sich nur auf eingehende Pakete bezieht. Das Fenster *Tabelle für eingehende* Protokolle wird angezeigt.

Current Time: Fri Apr 5 11:59:55 2013

Incoming Log Table		
Time	Event-Type	Message
Apr 5 09:04:23 2013	Kernel	kernel: i2c i2c-0: Can't create device at 0x32
Apr 5 09:04:23 2013	Kernel	kernel: gre: can't add protocol

In der Tabelle für eingehende Protokolle werden die folgenden Informationen angezeigt.

- Zeit - Die Uhrzeit, zu der das Protokoll erstellt wurde.
- Ereignistyp: Der Protokolltyp.
- Meldung - Informationen, die dem Protokoll entsprechen. Dazu gehören der Richtlinienotyp, die Quell-IP-Adresse und die Quell-MAC-Adresse.

**Hinweis:** Klicken Sie auf **Aktualisieren**, um die Protokolltabelle zu aktualisieren.