Firewall-Protokolle auf dem RV315W VPN-Router

Ziel

Ein Protokoll ist ein Satz von Meldungen, die Systemereignisse beschreiben. Protokolle geben einem Administrator eine Warnung, wenn eine Funktion nicht ordnungsgemäß funktioniert, sodass der Administrator Maßnahmen ergreifen kann. Eines der Protokolle, die der RV315W generieren kann, ist ein Firewall-Protokoll. Eine Firewall baut eine Brücke zwischen einem sicheren internen Netzwerk und einem unsicheren externen Netzwerk auf und steuert die eingehende und ausgehende Analyse des Netzwerkverkehrs der Datenpakete.In diesem Artikel wird die Konfiguration von Firewall-Protokollen auf dem RV315W VPN-Router erläutert.

Die folgenden Artikel enthalten weitere Informationen zur Systemprotokollierung auf der RV315W.

·Die Protokolle können lokal auf dem RV315W angezeigt werden. Weitere Informationen finden Sie im Artikel *View Logs (View-Protokolle) auf dem RV315W VPN-Router*.

·Informationen zum Konfigurieren der Protokolle, die auf dem RV315W generiert werden, finden Sie *in* den *Protokollfunktionen auf dem RV315W VPN Router* in folgendem Artikel.

·So konfigurieren Sie die Protokolleinstellungen für lokalen, USB-, E-Mail- und Syslog-Speicher: Weitere Informationen finden Sie im Artikel *Log Settings (Protokolleinstellungen) auf dem RV315W VPN Router*.

Anwendbares Gerät

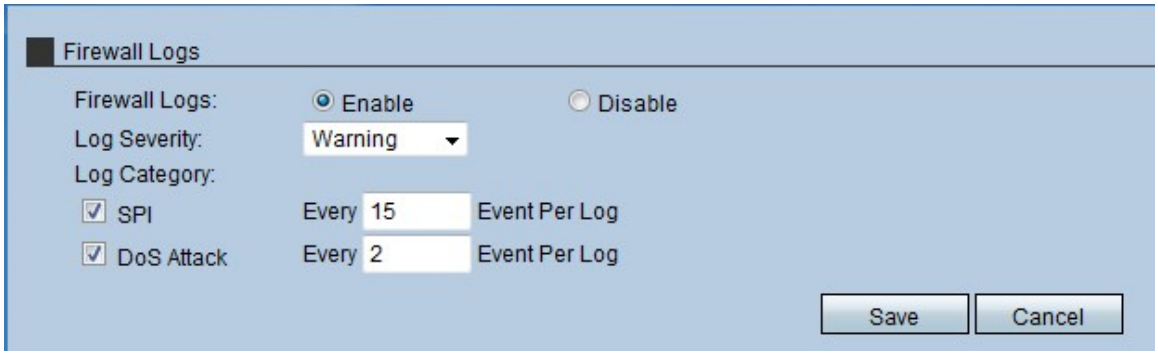
RV315W

Softwareversion

·1.01.03

Firewall-Protokolle

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Systemverwaltung > Protokoll > Firewall Logs aus**. Die Seite *Firewall-Protokolle* wird geöffnet:



Schritt 2: Klicken Sie im Feld Firewall Logs (Firewall-Protokolle) auf das Optionsfeld **Enable (Aktivieren)**, damit der RV315W Firewall-Protokolle generieren kann.

Schritt 3: Wählen Sie aus der Dropdown-Liste "Log Severity" (Protokollschweregrad) die Schweregrad der generierten RV315W-Protokolle aus. Die Liste ist vom höchsten Schweregrad bis zum niedrigsten Schweregrad geordnet:

·Emergency (Notfall): Generiert ein Protokoll, wenn die Firewall im Gerät einen Notfall auslöst, da ein Angriff stattgefunden hat.

·Critical (Kritisch) - Generiert ein Protokoll, wenn sich die Firewall im Gerät in einem kritischen Zustand befindet, da ein Angriff stattgefunden hat.

·Fehler - Generiert ein Protokoll, wenn die Firewall im Gerät einen Fehler aufweist.

·Warnung - Generiert ein Protokoll, wenn die Firewall im Gerät ein mögliches Problem erkannt hat.

·Benachrichtigung - Sendet ein Protokoll, wenn die Firewall im Gerät über eine Statusbenachrichtigung verfügt.

·Informationen - Sendet ein Protokoll über den Status der Firewall im Gerät.

·Debuggen - Generiert ein Protokoll im Gerät, um potenzielle Probleme, die die Firewall haben kann, zu analysieren und zu lösen.

Hinweis: Wenn der Schweregrad aus der Dropdown-Liste ausgewählt wird, erhält der Administrator das Protokoll, das für dieses Ereignis generiert wird, sowie Ereignisse mit höherem Schweregrad in der Liste. Wenn beispielsweise Error ausgewählt wird, erstellt der RV315W Protokolle für Error, Critical und Emergency.

Schritt 4: Aktivieren Sie das Kontrollkästchen der Protokollkategorie, in der die RV315W ein Protokoll aus dem Bereich Protokollkategorie erstellen muss. Es gibt zwei mögliche Kategorien:

·SPI - Geben Sie die Anzahl der Ereignisse ein, die pro Protokoll für jede SPI-Protokollkategorie aufgezeichnet werden müssen. Die System Packet Interface (SPI) wird zum Senden von Paketen über einen bestimmten Kanal verwendet. Diese Verteilung verwendet verschiedene Frames und Schnittstellen.

·DoS Attack (DoS-Angriff): Geben Sie die Anzahl der Ereignisse ein, die pro Protokoll für jede Kategorie des DoS-Angriffsprotokolls aufgezeichnet werden müssen. Denial of Service (DOS) wird verwendet, um ein Netzwerk vor DDoS-Angriffen (Distributed Denial of Service) zu schützen. DDoS-Angriffe sollen ein Netzwerk so weit überfluten, dass die Ressourcen des Netzwerks nicht mehr verfügbar sind.

Schritt 5: Klicken Sie auf **Speichern**.