SNMP-Konfiguration auf dem RV315W VPN-Router

Ziel

Simple Network Management Protocol (SNMP) ist ein TCP/IP-Protokoll für die Netzwerkverwaltung. SNMP ermöglicht es Administratoren, die Netzwerkleistung und Fehlerquoten zu überwachen. SNMP kann auch die Netzwerkverfügbarkeit zuordnen. Das SNMP-Framework besteht aus drei Elementen: einen SNMP-Manager, einen SNMP-Agent und eine MIB. Der SNMP-Manager steuert und überwacht die Aktivitäten der Netzwerk-Hosts, die SNMP verwenden. Der SNMP-Agent ist in der Software des Geräts enthalten und unterstützt die Datenpflege zur Verwaltung des Systems. Die Management Information Base (MIB) ist ein virtueller Speicherbereich für Informationen zum Netzwerkmanagement. Diese drei Komponenten überwachen und verwalten die Geräte in einem Netzwerk.

In diesem Artikel wird erläutert, wie SNMP auf dem RV315W VPN-Router konfiguriert wird.

Anwendbares Gerät

RV315W

Softwareversion

·1.01.03

SNMP konfigurieren

SNMP v1 ist die ursprüngliche Version von SNMP, das nicht über bestimmte Funktionen verfügt und nur in TCP/IP-Netzwerken funktioniert. SNMP v2 ist eine verbesserte Version von v1. SNMP v1&v2 sollte nur für Netzwerke ausgewählt werden, die entweder SNMPv1 oder SNMPv2 verwenden. SNMP v3 ist der neueste Standard für SNMP und behandelt viele Probleme mit SNMP v1 und v2. Insbesondere werden viele der Sicherheitsschwachstellen von v1 und v2 behoben. SNMP v3 ermöglicht es Administratoren außerdem, auf einen gemeinsamen SNMP-Standard zu wechseln.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Systemverwaltung > SNMP aus**. Die Seite *SNMP* wird geöffnet:

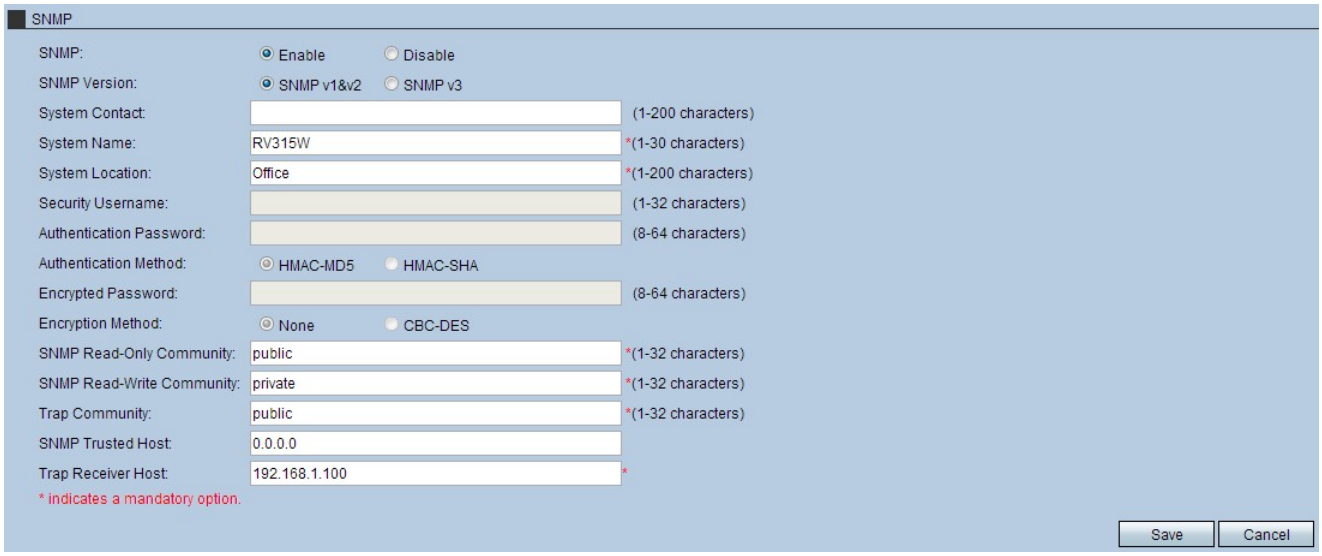
Schritt 2: Klicken Sie auf das Optionsfeld **Aktivieren**, um SNMP zu aktivieren.

Schritt 3: Klicken Sie auf das Optionsfeld für die gewünschte SNMP-Version.

·SNMP v1&v2 - SNMP v1 ist die ursprüngliche Iteration von SNMP und bietet keine bestimmten Funktionen. SNMP v2 ist die neuere Version, die die Funktionalität verbessert. Diese Option sollte jedoch nur für Netzwerke ausgewählt werden, die entweder SNMP v1 oder SNMP v2 ausführen.

·SNMP v3 - SNMP 3 ist die neueste Version, mit der Administratoren einen Standard verwenden können. Diese Option sollte ausgewählt werden, da sie viele Sicherheitsfehler in v1 und v2 patcht.

SNMP für SNMP v1&v2 konfigurieren



Schritt 4: (Optional) Geben Sie die Kontaktinformationen im Feld Systemkontakt ein. Dies ist die Kontaktperson, die für Netzwerkunterstützung kontaktiert werden muss.

Schritt 5: Geben Sie im Feld Systemname einen Namen ein. Dies ist der Name, der dem SNMP-Setup zugewiesen wurde.

Schritt 6: Geben Sie im Feld Systemstandort einen Speicherort ein. Hier befindet sich das System.

Schritt 7: Geben Sie im Feld SNMP Read-Only Community (SNMP-schreibgeschützte Community) eine Community ein. Dies ist der Client-Parameter für den schreibgeschützten Zugriff auf das SNMP-Setup.

Schritt 8: Geben Sie im Feld SNMP Read-Write Community (SNMP-Schreib-Community) eine Community ein. Dies ist der Client-Parameter für den Lese- und Schreibzugriff auf das SNMP-Setup.

Schritt 9: Geben Sie im Feld Trap Community (Trap-Community) eine Community ein. In dieser Community können SNMP-Traps verwendet werden. Traps werden an den Administrator weitergeleitet. Mithilfe von Traps kann der Administrator jedes Gerät verwalten, indem er es dem Benutzer ermöglicht, diese über ein Trap zu benachrichtigen.

Schritt 10: Geben Sie einen Host in das Feld "SNMP Trusted Host" ein. Dies ist die IP-Adresse des vertrauenswürdigen Hosts für das SNMP-Setup.

Schritt 11: Geben Sie im Feld Trap Receiver Host einen Host ein. Dies ist die IP-Adresse des Administrators, der die Traps empfängt.

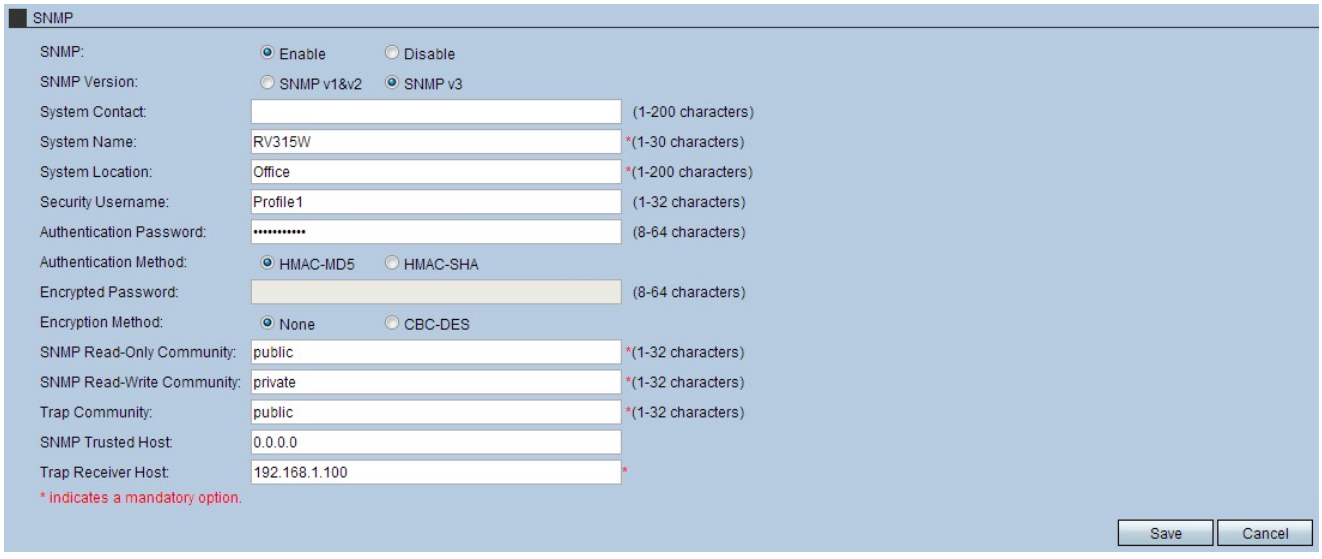
Schritt 12: Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

SNMP für SNMP v3 konfigurieren

Schritt 4: (Optional) Geben Sie die Kontaktinformationen im Feld Systemkontakt ein. Dies ist die Kontaktperson, die für Netzwerkunterstützung kontaktiert werden muss.

Schritt 5: Geben Sie im Feld Systemname einen Namen ein. Dies ist der Name, der dem SNMP-Setup zugewiesen wurde.

Schritt 6: Geben Sie im Feld Systemstandort einen Speicherort ein. Hier befindet sich das System.



Schritt 7: (Optional) Geben Sie im Feld Security Username (Benutzername für Sicherheit) einen Benutzernamen ein. Dies ist der Benutzername, der verwendet wird, um Zugriff auf das SNMP-Setup zu erhalten.

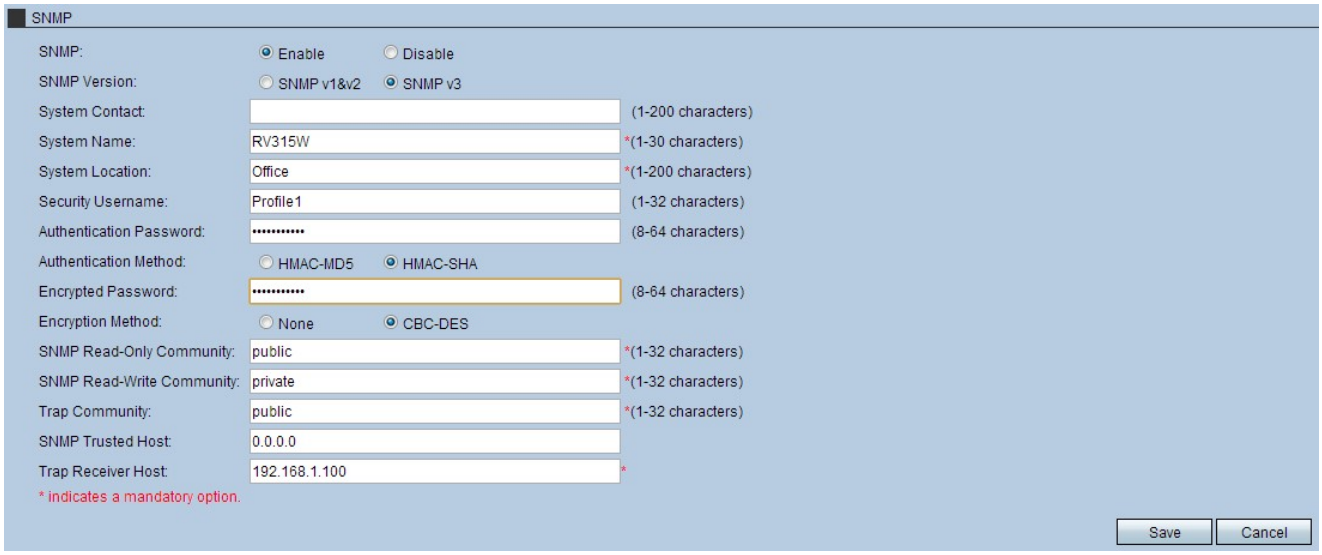
Schritt 8: (Optional) Geben Sie im Feld Authentifizierungskennwort ein Kennwort ein. Dieses Kennwort wird verwendet, um Zugriff auf das SNMP-Setup zu erhalten.

Schritt 9: Klicken Sie im Feld Authentifizierungsmethode auf das Optionsfeld HMAC-MD5

oder HMAC-SHA. Der Hash-basierte Message Authentication Code (HMAC) ist ein verschlüsselter Code, der einen Authentifizierungscode mit einem geheimen kryptografischen Schlüssel kombiniert. Der Hauptzweck von HMAC ist die Nachrichtensicherheit. Ein HMAC authentifiziert die Daten anhand der erstellten geheimen Schlüssel.

·HMAC MD5 — Dieser Hash-Algorithmus weist mehrere Sicherheitsfehler auf, und Daten können kompromittiert werden. Der HMAC MD5 ist ein Mechanismus für die Nachrichtenauthentifizierung mithilfe von kryptografischen Hashfunktionen. MD5 wird in Situationen eingesetzt, in denen eine überragende Leistungsgeschwindigkeit für ein System unerlässlich ist, wenn auch weniger sicher.

·HMAC SHA - Dieser Hash-Algorithmus ist viel sicherer, da die Verschlüsselungsmethode überlegen ist. Dies ist ein sichererer Mechanismus für die Nachrichtenauthentifizierung mithilfe von kryptografischen Hashfunktionen. HMAC SHA sollte verwendet werden, wenn Sicherheit von entscheidender Bedeutung ist.



Schritt 10: Geben Sie im Feld Verschlüsseltes Kennwort ein Kennwort ein.

Schritt 11: Klicken Sie im Feld Verschlüsselungsmethode auf das Optionsfeld CBC-DES. CBC und DES sind Verschlüsselungsstandards, die kombinieren, um übertragene Daten zu sichern.

Schritt 12: Geben Sie im Feld SNMP Read-Only Community (SNMP-schreibgeschützte Community) eine Community ein. Dies ist der Client-Parameter für den schreibgeschützten Zugriff auf das SNMP-Setup.

Schritt 13: Geben Sie im Feld SNMP Read-Write Community (SNMP-Schreib-Community) eine Community ein. Dies ist der Client-Parameter für den Lese- und Schreibzugriff auf das SNMP-Setup.

Schritt 14: Geben Sie im Feld Trap Community (Trap-Community) eine Community ein. In dieser Community können SNMP-Traps verwendet werden. Traps werden an den Administrator weitergeleitet. Mithilfe von Traps kann der Administrator jedes Gerät verwalten, indem er es dem Benutzer ermöglicht, diese über ein Trap zu benachrichtigen.

Schritt 15: Geben Sie einen Host in das Feld "SNMP Trusted Host" ein. Dies ist die IP-Adresse des vertrauenswürdigen Hosts für das SNMP-Setup.

Schritt 16: Geben Sie im Feld Trap Receiver Host einen Host ein. Dies ist die IP-Adresse des Administrators, der die Traps empfängt.

Schritt 17: Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.