

View/Add Trusted IPSec-Zertifikat auf RV320- und RV325 VPN-Routern

Ziel

Zertifikate werden verwendet, um die Benutzeridentität auf einem Computer oder im Internet zu überprüfen und um ein privates oder sicheres Gespräch zu verbessern. In RV320 können Sie maximal 50 Zertifikate durch Selbstsignierung oder Autorisierung von Drittanbietern hinzufügen. Sie können ein Zertifikat für einen Client oder für einen Administrator exportieren, dieses auf einem PC oder USB speichern und anschließend importieren. IPsec wird für den Austausch von Schlüsselgenerierungs- und Authentifizierungsdaten, des Key-Establishment-Protokolls, des Verschlüsselungsalgorithmus oder des Authentifizierungsmechanismus für die sichere Authentifizierung und Validierung von Online-Transaktionen mit SSL-Zertifikaten verwendet.

In diesem Artikel wird erläutert, wie Sie das Trusted IPSec-Zertifikat auf der RV32x VPN Router-Serie anzeigen und hinzufügen.

Anwendbare Geräte

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

Softwareversion

- v1.1.0.09

Trusted IPSec-Zertifikat

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Certificate Management > Trusted IPSec Certificate** aus. Die Seite *Trusted IPSec Certificate* wird geöffnet:

Type	Subject	Duration	Details	Export
<input type="radio"/> Self-Sign Authorized	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		

Die Seite *Trusted IPSec Certificate* enthält die folgenden Felder:

- Typ - Es stehen zwei Arten von Zertifikaten zur Verfügung
 - Self-Signed (Eigene Signatur) - Es ist ein SSL-Zertifikat (Secure Socket Layer), das vom eigenen Ersteller signiert wird. Sie ist weniger vertrauenswürdig, da sie nicht abgebrochen werden kann, wenn der private Schlüssel vom Angreifer irgendwie kompromittiert wird.
 - Certified Signing Request - Hierbei handelt es sich um eine Public Key Infrastructure (PKI), die an die Zertifizierungsstelle gesendet wird, um ein digitales Identitätszertifikat zu beantragen. Sie ist sicherer als selbstsignierte Schlüssel, da der private Schlüssel geheim

gehalten wird.

·Betreff: Es zeigt, wem das Zertifikat ausgestellt wird.

·Dauer: Es wird das Datum angezeigt, an dem das Zertifikat abläuft. Die Sicherheit der Website kann bei Überschreitung dieses Datums nicht gewährleistet werden.

·Details - Hier werden alle Details zum Zertifikataussteller, zur Zertifikatsseriennummer und zum Ablaufdatum vom Zertifizierungsstellendienst generiert. Die Informationen werden verwendet, wenn eine Signaturanfrage für das Zertifikat generieren erstellt und zur Validierung an den Zertifizierungsstellen-Dienst gesendet wird.

·Exportieren: Um ein Zertifikat zu exportieren oder anzuzeigen, klicken Sie auf das Symbol Zertifikat exportieren. Es wird ein Popup-Fenster angezeigt, in dem Sie das Zertifikat zur Überprüfung öffnen oder das Zertifikat auf einem PC speichern können.

Schritt 2: Klicken Sie auf das Kontrollkästchen **Aktivieren**, um ein bestimmtes IPsec-Zertifikat zu aktivieren.

Schritt 3: Klicken Sie auf **Hinzufügen**, um ein neues Zertifikat vom PC oder USB zu erhalten.

·Aus dem PC importieren: Auf dem PC können Sie das Zertifikat suchen und in das Gerät importieren.

·Import From USB (Aus USB importieren): Über den USB, der an das Gerät angeschlossen ist, können Sie auch das Zertifikat importieren.

Trusted IPsec Certificate

3rd-Party Authorized

Import Remote Certificate

My Certificate : 01. Issuer : 6c:20:56:c6:16:52

Import from PC

Certificate: (PEM format)

Import from USB Device

USB Device Status: No Device Attached

Schritt 3: Klicken Sie auf **Durchsuchen**, um das Zertifizierungsstellen-Zertifikat vom PC zu suchen.

Trusted IPsec Certificate

3rd-Party Authorized

Import Remote Certificate

My Certificate : 01. Issuer : 6c:20:56:c6:16:52 ▼

Import from PC

Certificate: C:\CSR\MyCertWithKey.pem (PEM format)

Import from USB Device

USB Device Status: No Device Attached

Schritt 4: Klicken Sie auf **Speichern**, um das Zertifikat der Tabelle mit vertrauenswürdigen IPsec-Zertifikaten hinzuzufügen.