

Häufig gestellte Fragen: PCI-Konformität für Cisco Router der RV-Serie

Ziel

In diesem Artikel werden einige häufig gestellte Fragen zur PCI-Konformität für Router der Cisco RV-Serie erläutert.

Unterstützte Geräte

- RV160 | ([Neueste herunterladen](#))
- RV260 | ([Neueste herunterladen](#))
- RV34x | ([Neueste herunterladen](#))

Häufig gestellte Fragen zur PCI-Compliance

Sind die RV-Router PCI-konform?

Die RV-Router wurden nicht als PCI-konform zertifiziert und werden nicht als PCI-konform angekündigt.

Kann ich die PCI-Konformität meines Routers sicherstellen?

Obwohl die RV-Router nicht als PCI-konform zertifiziert sind, konnten viele Kunden eine Sicherheitsprüfung bestehen.

Wie kann ich sicherstellen, dass mein Router die Sicherheitsprüfung besteht?

Jeder Sicherheitsscan ist anders. In vielen Fällen können Schritte unternommen werden, um Warnmeldungen in Sicherheitsscans zu behandeln. Die Deaktivierung der Remote-Verwaltung, des VPN und die Einschränkung der Port-Weiterleitung kann hilfreich sein. Deaktivieren Sie außerdem nicht benötigte Funktionen wie SNMP, UPnP, Ping Request usw.

Warum werden bei der Durchführung einer Sicherheitsprüfung Warnmeldungen für TLS 1.0, TLS 1.1, SSLv3, 3DES angezeigt?

Einige Sicherheitsscans berichteten von einigen der älteren kryptografischen Protokolle, die unterstützt wurden, selbst wenn sie nicht verwendet wurden. Die neueste Firmware hat die Unterstützung für TLS 1.0, TLS 1.1 und SSLv3 entfernt. 3DES wird derzeit noch von IPsec unterstützt.

Warum wird eine Warnmeldung für UDP 500 angezeigt?

IPsec verwendet UDP 500 für die Tunnelverhandlung. Wenn IPsec aktiviert ist, wird UDP 500 für Scans angezeigt. Mit der neuesten Firmware können Sie die Option "Global IPsec" deaktivieren, um den UDP-Port 500 zu deaktivieren.

Schlussfolgerung

Dies sind einige der häufigsten Fragen, die bezüglich der Router der Cisco RV-Serie hinsichtlich der PCI-Konformität gestellt wurden. Ich hoffe, dass dies auch bei der Beantwortung Ihrer Fragen hilfreich ist!