FAQ: PCI Compliance for Cisco RV Series Routers

Objective

This article will explain some frequently asked questions regarding PCI Compliance for the Cisco RV series routers.

Applicable Devices

- RV160 | **(Download Latest)**
- RV260 | **(Download Latest)**
- RV34x | **(Download Latest)**

Frequently Asked Questions on PCI Compliance

Are the RV Routers PCI Compliant?

The RV routers have not been certified as PCI Compliant and are not advertised as PCI Compliant.

Can I make my router PCI Compliant?

While the RV routers are not certified as PCI Compliant, many customers have been able to pass a Security Scan.

What can I do to make my router pass the Security Scan?

Each Security Scan is different. Steps can be taken in many cases to help address alerts in Security Scans. Disabling Remote Administration, VPN, and restricting any Port Forwarding can help. In addition, turn off unnecessary features like SNMP, UPnP, ping request, etc.

When running a Security Scan, why do I see alerts for TLS 1.0, TLS 1.1, SSLv3, 3DES?

Some Security Scans reported some of the older cryptographic protocols as they were supported, even if not being used. The latest firmware has removed support for TLS 1.0, TLS 1.1, and SSLv3. 3DES is currently still supported with IPsec.

Why do I see an alert for UDP 500?

IPsec uses UDP 500 for negotiating tunnels. If IPsec is enabled, scans will see UDP

500. With the latest firmware, you can turn off the “Global IPsec” option to disable UDP port 500.

Conclusion

These were some of the most common questions that have been asked about the Cisco RV series routers for PCI Compliance. Hope this helped answer your questions too!