Release Note

SecFlow-1

Version 4.0.02

November 4, 2015

Status: General Availability

Ruggedized SCADA-Aware Router Gateway

SecFlow-1 is an Ethernet router gateway, a member of RAD's SecFlow suite of ruggedized Ethernet family.

With a unique built-in packet-processing SCADA-aware engine, SecFlow-1 fits mission-critical industrial applications. It is most suitable for infrastructure, used by utility companies with remote sites, connected to a SCADA control center. SecFlow-1 is installed at remote locations, forwarding Ethernet or serial traffic over fiber optic or cellular links.

Main Features

Ethernet

Features	Description	Customer Benefits
Ethernet interface	- 10/100/1000T SFP based port - 10/100BaseT RJ-45 port - Auto crossing - Autonegotiation per IEEE 802.3ab	• Resilient redundant networking over various WAN infrastructures
Routing	- Up to 60 routing paths - IPv4 - Static routing - OSPF v2 - NAT	• Layer-2 and Layer-3 routing in a single-box
Networking	- DHCP client	• Additional MAC based pool allocation

Serial

Features	Description	Customer Benefits
Serial interfaces	- Two RS-232 RJ-45 ports - One RS-232 and One RS-485 Serial RJ-45 ports	• Multiservice support in a compact single device

SecFlow-1

Version 4.0.02

Features	Description	Customer Benefits
Serial gateway	- Serial tunneling for byte-oriented streams - Serial tunneling for frame streams - Terminal server supporting: ▪ Byte and frame modes ▪ TCP ▪ Configurable NULL_CR - IEC 101/104 gateway - Modbus RTU/TCP gateway	• Seamless communication between IP SCADA equipment and both legacy and new RTUs, featuring a single box for multiservice application and smooth migration to all IP networks

Cellular

Features	Description	Customer Benefits
Cellular modem	- GPRS /UMTS, or LTE (US and European bands) - HSPA+ - Two SIM cards - Cellular band manual/auto selection - CLI reading of IMEI identifier - Power control - SIM redundancy based on RSSI - Optional preference of preferred SIM - VPN support - IPSec support - Operation as main network link - Operation as backup link of fixed line	• Utilizing cellular network for main link • Improved link resiliency and service continuity using cellular backup links

SecFlow-1

Version 4.0.02

Resiliency

Features	Description	Customer Benefits
Cellular link protection	- Protection switching between the cellular ISPs (SIM cards backup based on ICMP)	• Improved link redundancy. Switch-over between two cellular links according to predefined cellular signal strength threshold.
System reload	- System automatically reloads when the cellular ISP is inaccessible	• Increased system reliability and availability
Dynamic routing	- Dynamic routing protection using OSPF	• Increased reliability of network connections

Timing and Synchronization

Features	Description	Customer Benefits
Timing	- Local time setting	• Flexible clock distribution and network synchronization

Monitoring and Diagnostics

Features	Description	Customer Benefits
Port statistics	- Counters and statistics per port	• Extensive diagnostic tools for fault monitoring • Monitoring SFP parameters, such as optical output power, optical input power, temperature etc. • Guaranteed SLA (Service Level Agreement) of contracted Ethernet service • Network fault monitoring, performance measurement, and gathering of statistic data • Monitoring and troubleshooting failures quickly, using the Ethernet sniffer and debug serial link tools
LED indicators	- Power, system, and main interfaces status indication	
RMON v1	- Remote network monitoring	
IMEI reading	- CLI enables reading the International Mobile Station Equipment Identity	
DDM reading	- SFP operation Digital Diagnostics Monitoring	
Trace route	- Displaying the route (path) and measuring transit delays of packets across an IP network	
Tcpdump	- Common packet analyzer	
Serial applications monitoring	- Set of tools for serial applications debugging and monitoring	

SecFlow-1

Version 4.0.02

Management and Security

Features	Description	Customer Benefits
Serial console port	- Direct ASCII terminal connection	• Key management system can negotiate a new secure access before the connection lifetime expires and avoid management disconnection • Secured remote sites interconnected over public networks, using Layer-2 or Layer-3 VPN with encryption • Support for large-scale networks • Filtering user traffic according to variety of criteria • Better security and control of authorized traffic • Variety of management tools
Inband management	- Embedded terminal server	
CLI via Telnet or SSH	- Remote CLI control via Telnet and SSH connection	
TACACS	- Remote authentication for networked access control through a centralized server	
Syslog, Severity levels	- Syslog for informational, analysis, and debugging messages	
Configuration database backup/restore	- Configuration file can be kept on external server	
Remote software download	- Software file download from the external server	
Safe mode	- System problems recovery tool	
Scheduled system reload	- Preventive system reload according to a written schedule	
EMS	- Element management system	
Port shutdown	- Disabling unoccupied ports	
Local authentication	- User identification based on username and password	
SSH server	- Secure Shell cryptographic network protocol support	
SFTP client	- SSH File Transfer Protocol support	
IPSec	- IP Sec encryption using 3DEC or AES algorithm and IKEv1 Dynamic Kew Exchange	
L3 mGRE DM-VPN	- Dynamic Multipoint VPN based on Generic Routing Encapsulation	
VLAN stacking	- VLAN IEEE 802.1q double-tagging	
Application-aware firewall	- Distributed application-aware firewall per port for ModBus TCP, IEC104, DNP3	

SecFlow-1

Version 4.0.02

Compatibility

SW Compatibility

The SecFlow-1 version is released as a single compressed file: SecFlow-1_4.0.02.67.tar.

Do not uncompress before installing and activating on the unit.

OS files available on the switch can be seen using the following command:

```
OS-image show list
```

The boot version is shown by the following command:

```
show system information
```

Management Compatibility

SecFlow-1 is managed by RADview version 4.2 and up.

Interoperability

SecFlow-1 can operate with SecFlow-2 and SecFlow-4.

Limitations

Ethernet

Description	Status
Total **eth1** and **eth2** ports throughput should be limited to: • 1200 pps duplex with VPN • 5000 pps duplex without VPN. Exceeding this limit may interrupt the management connection.	
X.509 certificate authentication method is not supported.	Workaround: Use pre-shared keys.
When IP interfaces are not configured, L2 traffic may be switched between **eth1** and **eth2** ports.	Workaround: Set at least one IP interface to avoid this behavior.
LED link indication may not be accurate when used in no-autoneg mode.	

Discrete Channels

Description	Status
Discrete input and output channels are not supported.	

Serial

Description	Status
Serial tunneling frame mode is not supported.	Workaround: Use Byte mode.
Serial tunneling TCP mode is not supported.	Workaround: Use UDP mode.
9600 or 19200 Bd rate should be used for serial channel normal operation.	
The serial channel control signals are not supported.	
The serial channel bitstream mode is not supported.	
101/104 gateway operates in balanced mode only.	
Modbus and TG809 gateways are not supported.	
Terminal server operates in point-to-point topology, and in TCP mode only.	
QOS is not supported for serial services.	

Timing and Synchronization

Description	Status
System reload erases local the time settings.	

Ports

Description	Status
To complete SFP port configuration, the user must: • extract an SFP module and reinsert it • disable and enable the port using the CLI.	
Fiber SFPs	
RAD SFP types SFP-9F (copper 100) and 'Miric' are not supported.	
SFP 6 (Fiber 1000) – when autoneg OFF, Led stays off when link is up.	

Description	Status
SFP 6 (Fiber 1000) – when a link is not connected to the SFP, Led status is Green instead of OFF.	
SecFlow-1 <--> Cisco 3550, SFP-30 (10/100/1000) Autoneg OFF. Changing SecFlow-1 speed result: Link up SecFlow-1, Link down Cisco. Changing Cisco speed result: Link down SecFlow-1, Link down Cisco.	
Copper SFPs	
Auto-negotiation may not be supported if a non-RAD copper SFP is used.	It is recommended to use RAD copper SFP or RAD SFP-30. In this case, use fixed speed.
SFP 9G (1000 Copper)- when autoneg is OFF, LED stays off although link is up, traffic is available and CLI state is up.	
Support SGMII types of 10/100/1000	
Support type 1000mbps (SERDES based) with auto negotiation	
RJ45	
The **eth1** port is recommended to be used with 'auto negotiation' mode (default mode) versus fix speed.	
In a case where a SecFlow-1 router is connected to a second SecFlow-1 via their respective **eth1** interfaces, when changing mode **autoneg** from off to on, the speed is not changed.	Workaround: Disable/Enable the interfaces.
In a case where a SecFlow-1 **eth1** is connected to PC with Intel NIC and **autoneg** is OFF, after reload the link is down.	Workaround: Disable/Enable the interfaces.
When using SFP 9G (1000 Copper), the CLI **show port output** command indicates SFP type of 1000 Fiber.	

Monitoring and Diagnostics

Description	Status
Syslog: • Cannot be enabled | disabled • Cannot be saved to local file • Cannot be reset • Local and remote modes cannot function simultaneously.	

Description	Status
SFP port statistics counters cannot be reset.	
RMON is not supported.	
The cellular modem echo quality tests are not supported.	

Management and Security

Description	Status
The Host Name parameter is not configurable.	
The Welcome banner is not configurable.	
Only the default **su** user is available.	
SFTP client can be used with fixed line only.	Workaround: Use TFTP for cellular connection.
Telnet server cannot be enabled by user.	
Proxy authentication is not supported.	
ACL is not supported.	
DPI Firewall operates with TCP protocols (IEC104 or Modbus) only.	
Modbus firewall is not supported when the both link sides are connected through the different SecFlow-1 routers.	
Firewall and VPN cannot be used simultaneously.	

Software Upgrade

Description	Status
While using the tftp action to download a new software OS file, and the tftp CLI command is not accurately placed, the operation may fail resulting in the router losing its running image.	Workaround: Use the correct command as detailed in the user manual or use the EMS.
Device allows activation of corupped version.	Workaround: Verify the OS image was downloaded successfully. If not or the tftp action was interrupted, do not reboot the unit. In this case, download the file again.

SecFlow-1

Version 4.0.02

Solved Limitations

Networking

Description	Status
DM-VPN co-existence with dpi firewall over fixed network connection is supported.	
RS485 4w support is available with relevant ordering option of hardware.	
IEC 101/104 gateway supports SQ bit.	

Cellular

Description	Status
Fixed loop bug at the modem code resulting in the modem not transmitting traffic, although it seems to be up and connected. Bad initialization of the socket to the modem.	
Fix bug related Sierra (LTE, 3.5G) modem not allowing roaming.	

Ports

Description	Status
Fiber SFPs	
SFP port configuration doesn't take effect automatically. Types of 1000mbps **only** are supported.	Workaround: 1. Take the SFP out and replace it in the port. 2. Disable and enable the port via the CLI.
RAD SFP types SFP-9G and SFP-9F are not supported.	
Copper SFPs	
For non-RAD SFP, auto negotiation may not be supported. Use fixed speed.	
Copper SFP state shows as **down** after system power loss.	
Fixed issue with Copper 10/100/1000 when Fixed Speed& Duplex are selected.	
Eth2 is down after 'reload'	

SecFlow-1

Version 4.0.02

Description	Status
RJ45	
When connecting a device which supports 10/100/1000 at the eth1 port, it must be set to a fixed speed of 100 or 10 with no auto-negotiate. Attempting to work in auto negotiation with such devices may cause CLI management to be interrupted.	
Fix issue with Copper 10/100/1000 no Link after plug/unplug, when ETH2 port is set to fixed speed 10 or 100 with Autoneg OFF.	

Release Note

SecFlow-1

Version 4.0.02

Marketing Contact

Moshe Lavi

Product Line Manager

eSupport

Technical Information Center