Solution Brief

Cybersecurity Capabilities of SecFlow-1p for Utilities

This document provides a list of essential cybersecurity features supported by SecFlow-1p, tailored to the needs of utilities to protect critical infrastructure from emerging threats.

Secure Connectivity

SecFlow-1p is a gateway designed with the security needs of utilities in mind. This isn't just another piece of hardware; it's a fortress equipped with an array of features to thwart cyber threats. At its core, SecFlow-1p ensures secure connectivity through VPN support, creating encrypted communication channels that protect data as it travels between the gateway and central systems. This secure connectivity is crucial for substations where sensitive operational data must be protected from interception and tampering. It employs TLS/SSL encryption to shield this data from unauthorized access, while IPsec provides end-to-end encryption and authentication, ensuring that all network traffic, whether from substations, microgrids, or field area networks, remains secure.

RAD

Your Network's Edge®

Access Control

But secure communication is just the beginning. The real strength of SecFlow-1p lies in its multi-layered approach to cybersecurity. Role-Based Access Control (RBAC) assigns permissions based on user roles, ensuring that only authorized personnel can access sensitive functions and data. This is especially important in microgrids, where different user roles might require varying levels of access to the network and its resources. Multi-Factor Authentication (MFA) adds an extra layer of security, requiring additional verification methods beyond passwords to fend off unauthorized access attempts. SecFlow-1p also features port-based access control, utilizing 802.1X on Ethernet and Wi-Fi for authentication, ensuring devices in field area networks are authenticated before accessing the network. SecFlow-1p supports various authentication methods, including local authentication, RADIUS, and TACACS+. Login lockout mechanisms protect against brute-force attacks by locking accounts after a set number of failed login attempts, further enhancing security.

Intrusion Detection and Prevention

In the realm of intrusion detection and prevention, SecFlow-1p stands out with its integration capabilities. It includes a Docker engine allowing for the quick integration of third-party Docker cybersecurity applications. For utilities, this means seamless incorporation, maximum flexibility, and futureproofing to stay up to date with critical cybersecurity applications. For example, SecFlow-1p integrates anomaly detection systems tailored for Operational Technology (OT), Industrial IoT (IIoT), and Advanced Metering Infrastructure (AMI). These applications detect threats at an early stage, even those that manage to bypass traditional firewall defenses, making it highly effective for protecting substations and field area networks. The solution's strength lies in its ability to identify unusual patterns in network traffic through machine learning algorithms, leveraging external threat intelligence feeds to stay ahead of the latest vulnerabilities and attack vectors. Real-time monitoring and response mechanisms provided by IDS/IPS ensure unauthorized access attempts and attacks are detected and prevented promptly.

Data Integrity and Protection

Data integrity and protection are paramount in SecFlow-1p's design. Symmetric encryption protects data both in transit and at rest, while secure boot processes verify the authenticity and integrity of the gateway firmware during startup, preventing malicious alterations. The inclusion of a Trusted Platform Module (TPM 2.0) adds a hardware-based security layer, ensuring platform integrity.

Network Segmentation

Network segmentation is another critical feature, offering micro-segmentation to provide fine-grained security controls within the network. Virtual LAN (VLAN) support segments the network into isolated sections, limiting the spread of potential breaches. Advanced firewall capabilities and access lists further control traffic flow, protecting critical resources and data across all utility applications, from substations to microgrids.

System Management and Updates

Managing and updating the system is streamlined through management, ensuring updates to address vulnerabilities. Secure firmware updates transmitted over encrypted channels and verified with digital signatures maintain the system's security posture. Remote management capabilities allow for centralized control and monitoring of firmware updates across multiple gateways, including those in field area networks.

Compliance and Reporting

Compliance and reporting are essential for utilities to meet regulatory standards. SecFlow-1p adheres to industry standards like IEC62443, and NERC CIP. Detailed audit logs and Public Key Infrastructure (PKI) for zero-touch provisioning ensure comprehensive compliance.

Resilience and Redundancy

SecFlow-1p also emphasizes resilience and redundancy, with failover capabilities to ensure continuous operation through redundant systems. Comprehensive disaster recovery plans minimize downtime in the event of a cyber incident, while high availability design guarantees reliable operation with minimal interruptions.

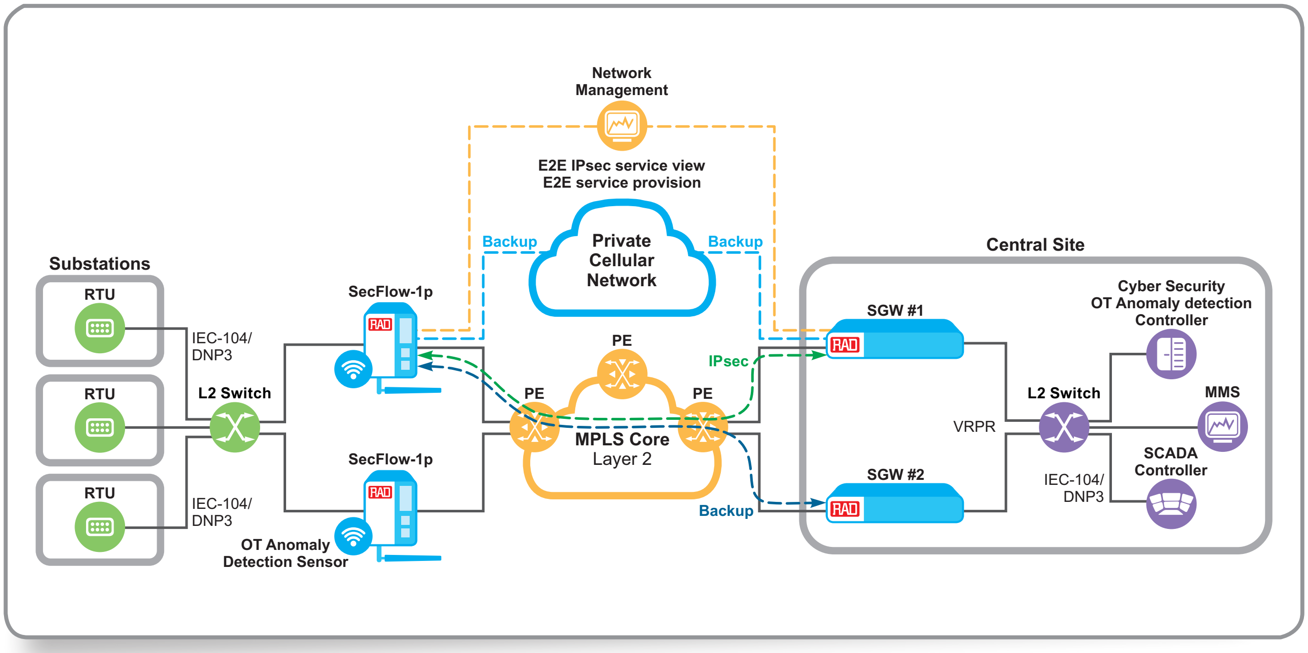
Advanced Security Features

Advanced security capabilities like AppArmor enhance security with mandatory access control. The secure-by-design architecture, with separation and isolation using containers and minimal privilege execution, further fortifies the system.

Logging Capabilities

Logging capabilities capture every detail, from user logins and configuration changes to network traffic and system events, providing a comprehensive view for forensic analysis and compliance.

In essence, SecFlow-1p weaves a narrative of security, resilience, and foresight. It transforms the landscape of utility cybersecurity, offering a robust shield against the myriad threats that loom over critical infrastructure. For utilities, whether managing substations, microgrids, or expansive field area networks, SecFlow-1p isn't just a gateway; it's a guardian ensuring the seamless and secure operation of their vital services.



Substation SCADA backhauling solution

- Network segmentation
  - Management: SecFlow-1p managed by NMS
  - User data: RTU controlled by SCADA HMI (supports multiple separated user data services)
- Data and management separation tools
  - Separation between RTU data by VLANs
  - Separation by IPsec and BGP policy in SecFlow-1p
  - Separate IPsec tunnel per management and user data service
  - Separate VRF in security GW (SGW)
- Management security elements
  - Hardened security EMS server (RADview)
  - EMS Role-Based Access Control (RBAC)
  - Management protocols are SNMPv3, SSH, HTTPS
  - Management traffic runs over IPsec tunnel
  - Management access control – block access from unauthorized ports
- Certificates managed by X.509 SCEP server
- Intrusion detection and prevention – OT anomaly detection
  - OT security sensor is installed on each SecFlow-1p as Docker container
  - The sensor mirrors all SCADA communications passing through SecFlow-1p, transfers info back to the central controller that inspects it for anomality's
- Private / public network connection (e.g. cellular) protected by SGW and SecFlow-1p stateful zone-based firewall.
- Resiliency:
  - **Substations** – Two SF-1p gateways are located in each substation connected via VRRP for redundant backhauling of SCADA information.
  - **Connectivity** – Multiple redundant IPsec tunnels, primary and secondary via fiber, and third via private cellular network
  - **Central site** – Two security gateways connected via VRRP
  - Redundancy mechanism based on BGP

EMS – E2E management

- SecFlow-1p and SGW management, IPsec tunnels, ZTP, MAP, EMS, IPsec tunnel configuration, IPsec tunnel view and status fault manager, software management.

SecFlow-1p Cybersecurity Features

Feature	Description
Access Lists	Standard and extended access lists to control access to network resources
AppArmor	Enhanced security by restricting programs' capabilities with mandatory access control, ensuring applications run with minimal privileges
Authentication	Local authentication, RADIUS, and TACACS+ for authorization and accounting, ensuring robust access control mechanisms
Docker Container Engine	Installation of any cybersecurity application, futureproofing the system through containerization
Firewall	Stateful firewall and zone-based policy to control traffic flow and prevent unauthorized access to critical segments
Segmentation	Isolate the IoT network from other networks to limit the impact of potential breaches with support off VLAN and multi VRFs
IKEv1 and IKEv2	Secure key exchange and authentication via pre-shared key (PSK) or certificates, supporting AES CBC 128/256 and SHA-1, SHA-2 256/512 algorithms
IPsec DH Group (Including PFS)	DH-1, DH-2, DH-5, DH-14, DH-19, DH-20 for Diffie-Hellman key exchange protocols
IPsec Integrity Protection and Authenticity	AES GMAC 128/256, SHA-1, SHA-2 256/512 for data encryption
IPsec Symmetric Encryption	AES CBC 128/256, AES GCM 128/256
IPSec Tunnels	Up to 30 IPsec tunnels for end-to-end encryption and authentication of network traffic
Login Lockout	Protection against brute-force attacks by blocking the attacker's IP address after a defined number of failed login attempts
Multi-Factor Authentication	Additional verification methods beyond passwords to enhance security against unauthorized access

Solution Brief

Cybersecurity Capabilities of SecFlow-1p for Utilities

Port-Based Access Control	802.1X on Ethernet and Wi-Fi for port-based authentication, ensuring devices are authenticated before accessing the network
Product Integrity Protection	No JTAG or similar interface that can be used to circumvent the integrity of a product or steal device secrets
Public Key Infrastructure (PKI)	X.509 certification for zero-touch provisioning and SCEP CA server for certificate management
Regulatory Compliance	Adherence to industry standards such as IEC62443 SL1, and NERC CIP, ensuring compliance with regulatory requirements
Secure Boot	Verification of the authenticity and integrity of the gateway firmware during startup to prevent malicious alterations
Secure by Design Architecture	Developed by RADs, employs separation and isolation using containers and Linux users, microservice architecture, minimal privilege execution, and secure code practices
Security Measures	Blocks malicious code, ensuring cryptographic keys are never stored in clear text, passwords and secrets are different between devices, and specific operations run in a single context
Session Monitoring and Limiting	Monitoring of active sessions and limiting the number of concurrent sessions to prevent abuse and ensure optimal performance
Signed Software Upgrade	Digital signatures for verifying the authenticity of firmware updates, ensuring only authorized updates are applied
Single Sign-On	Users are authenticated once and gain access to multiple systems without re-entering credentials
Trusted Platform Module (TPM 2.0)	Hardware-based security functions ensure platform integrity, protecting against unauthorized firmware and software changes

To learn how SecFlow-1p can help secure your network, contact us at: market@rad.com.

RAD
Your Network's Edge®