Data Sheet

1031

Secure Ruggedized Gateway

Secure Ruggedized Gateway

- ► Secure access and identity management
- ► IP and Serial DPI SCADA firewall (DNP3,ModBus,IEC104/61850)
- ► Network learning – For easy firewall deployment
- ► IPsec VPN over cellular & fiber with X.509 certificates
- ► Ruggedized gateway for Serial and Ethernet devices
- ► Resilient network uplink over Ethernet or Cellular
- ► SCADA protocols gateway
- ► Fit for utilities' harsh environments

radiflow
Secure Your Assets

1031 Secure Ruggedized Gateway

Data Sheet

General

The 1031 Secure Ruggedized Gateway was designed for small remote sites that require a secure connection, over thousands of kilometers, to a limited number of devices. The 1031 assures that utilities maintain control over their networks facing even the most complex threats.

The 1031 offers security solutions for both M2M (Machine to Machine) and H2M (Human to Machine) traffic by incorporating DPI (Deep-Packet Inspection) firewall for deep traffic analysis and monitoring on the SCADA network, as well as a user identity firewall. The 1031 is compliant with NERC CIP V.5 for remote substations.

Networking

INTERFACES

While compact in size, the 1031 Gateway offers a variety of interfaces, including two Ethernet ports (10/100 and 100/1000; RJ- 45 and SFP) and two RS-232 ports, a single RS-485 port, as well as a cellular interface with a dual SIM modem.

Security

DISTRIBUTED FIREWALL

Radiflow's distributed DPI firewall helps the operator to control remote sites by monitoring all network traffic and managing physical and remote access control systems.

The whitelist-based firewall is installed at every port for both Serial and Ethernet traffic, meaning that every access point at the remote site is firewalled.

Radiflow's solution provides maximum protection against cyber threats without having to be a cyber expert

Each SCADA protocol packet (DNP3, IEC 101/104,IEC 61850 ModBus TCP/RTU) is validated by the firewall engine not only for its source and destination, but also for its protocol and packet content.

The firewall has two states: Monitoring and Blocking. In Monitoring state the control center will be alerted for any violation without blocking the traffic.

For sensitive locations, the Blocking state allows blocking suspicious traffic while triggering a violation alarm at the control center. For both states the firewall rules are suggests by the firewall learning mode.

VPN

The 1031 Gateway supports VPN tunnels for secure inter-site connectivity with IPsec, DMVPN, mGRE tunnels (among others) with key management certificates.

The supported VPN modes allow both layer-2 and layer-3 services, to best suit the application's protection needs.

IDENTITY MANAGEMENT

One of the most important requirements in NERC CIP V.5 for protecting remote sites is the capability to identify the user and create specific network privileges per identified user, prior to granting the user access to the network.

The Radiflow 3180 includes a built-in APA (Authentication Proxy Access). Prior to granting a user network access, the user needs to log in to Radiflow's internal authentication process with his unique username and password. After validating the user's profile, specific access is granted to predefined devices and functions, and each operation is logged. In addition, the 3180 is integrated with a physical identity server system allowing other authentication methods such as magnetic card.

EASY DEPLOYMENT

You don't have to be a cyber-expert. At Radiflow, we fully understand the complexity of SCADA networks, so we've made sure that our devices are simple and easy to deploy.

The 3180 secure ruggedized router is fully supported by Radiflow's NMS (network management subsystem) to configure and diagnose network and security features, as well as CLI for command-line configuration.

Configuring the firewall is also very simple. Once the 3180 is connected to the network it begins to gather information from across the network (devices, behaviors, etc.) and list suggested firewall rules. These rules are optional, and can be easily edited using the NMS.

How to Secure Common SCADA Operations

Operation use case	Security risk	Authentication	DPI Monitoring	DPI Enforcement	VPN
SCADA Server ➔ Devices	Medium		✓		
Physical Access	High	✓		✓	
Remote Access	High	✓		✓	✓
Connection Between Remote Sites	High		✓		✓

Specifications

SECURITY

Distributed DPI Firewall
Profile-based firewall
Security rules planning per service group
Firewall Monitoring mode
Firewall Enforcement Mode
Firewall Learning Mode
IEC 104 DPI Firewall
IEC 61850 DPI Firewall
Modbus TCP DPI Firewall
DNP3 TCP DPI Firewall

VPN
IPsec Certificates X.509
IPsec Dynamic Key Exchange
IPSec encryption AES
IPSec encryption 3DES
L3 IPSec VPN policy based L3
IPSec VPN route based
L3 mGRE DM-VPN

Access Control
Access Lists L3
Access Lists L4
NAT
User activity report (local APA - Authentication Proxy Access)
OS image encryption

INTERFACES

1 or 2 x RS-232 RJ45 Serial port
1 x RS-485 RJ-45 Serial port
1 x 10/100TX RJ-45 Ethernet port
1x100/1000 SFP Ethernet port
Cellular Modem with dual SIM for HSPA +/ LTE CDMA 450MHz
Discrete lines: 2 In, 2 Out
Console

PHYSICAL DESIGN

DIN rail mounting, optional wall mount
Rugged enclosure - IP 30
Fanless
Wide range of ambient temperature: min. -40°C, max +70°C (-40°F to +158°F)
Self-cooling
Storage Temperature: min -40°C, max +85°C
Operating humidity up to 90%
Dimensions (HxWxD) 106 x 44.7 x 120mm
Power supply 9-60V
DC IEC 61850-3 conformance
MTBF 25 years

MANAGEMENT

Console serial port
Backup/Restore running config
Conditioned/scheduled system reboot
Remote management and upgrade
TFTP/SFTP Client
Safe Mode
Syslog

NETWORKING

Serial
SCADA gateway for IEC101/104, ModBus RTU/TCP and DNP3
Terminal Server Byte/Frame modes
Serial transparent tunneling byte mode

Routing
Static routing
OSPF v2
IPv4

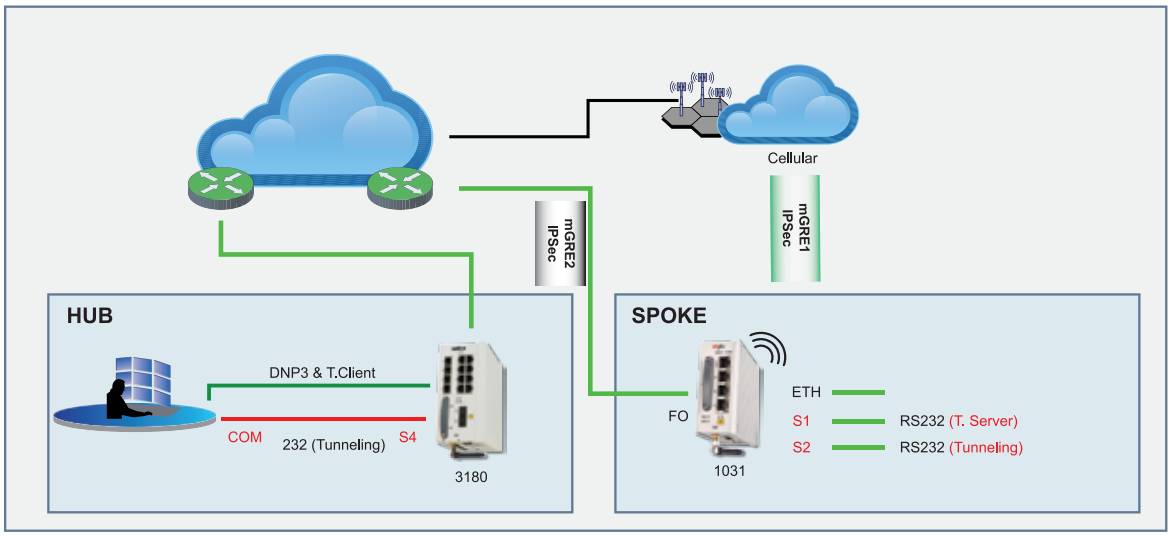
Switching
Auto Crossing
Auto Negotiation IEEE 802.3ab
VLAN Tagging

Time
Local Time settings
SNTP

Diagnostic
Counters & statistics per Port
LED diagnostics
Ping
RMON
DDM

PROTECTION

Protection over wired and cellular connections
Protection between Cellular ISPs (SIM cards backup)
Conditioned/scheduled system reboot



Remote site access over fiber and a backup cellular link

1031 Secure Ruggedized Gateway

Ordering

RF-1031-<P>-<T>/<S>/<E>/<C>

P – Input Power
- 12 -12 VDC (range: 9-18v DC)
- 48 - 48V DC (range: 36-60v DC)

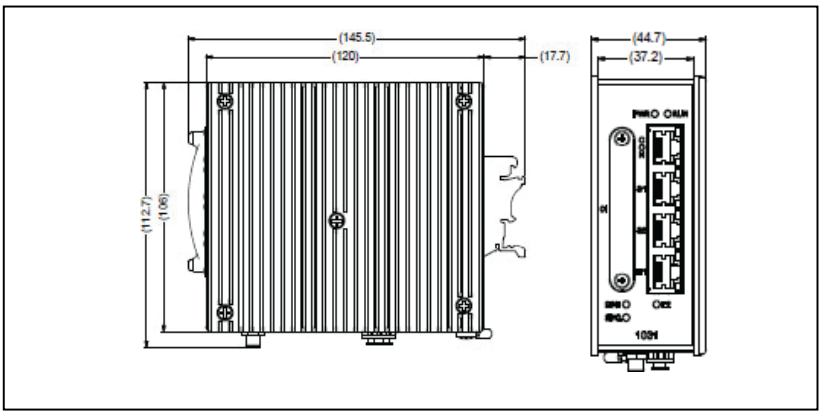
T - Temperature Range
- XT: -40º+75ºC

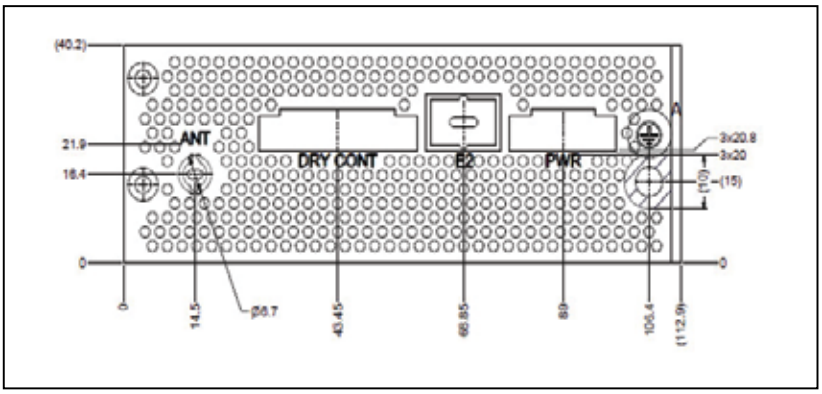
S – Serial interfaces
- RS22 – 2 x RS-232
- RS11 – 1 x RS-232 and 1 x RS-485

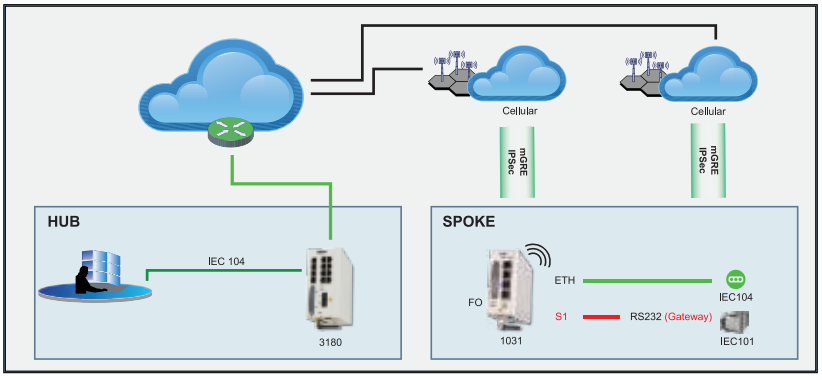
E – Ethernet interfaces
- ETS - 10/100BaseT+SFP 1000

C – Cellular interface
- CELHP - HSAP + dual SIM modem
- CELEU - LTE dual SIM modem for European bands
- CELANA - LTE dual SIM modem for North American bands

Supported Protocols:
- ***ModBus***
- ***DNP 3.0***
- ***IEC 104***
- ***IEC 101***
- ***IEC 61850***







Remote site access over redundant cellular networks

Headquarters:
31 HaBarzel St.
Tel Aviv 6971045, Israel

North America:
900 Corporate Dr
Mahway, NJ 07430

info@radiflow.com
www.radiflow.com

radiflow
Secure Your Assets