

# 3180

SCADA firewall router

## SCADA firewall router



- Do 16 portów ethernetowych 10/100 oraz 2x100/1000 SFP
- Porty szeregowy RS-232 z obsługą bramy protokołów
- Modem 2G/3G z obsługą 2 kart SIM - redundancja operatorów
- Zaprojektowany do pracy w trudnych i wymagających warunkach przemysłowych
- Per port DPI (Deep Packet Inspection) SCADA firewall (dla protokołów DNP3, ModBus, IEC 104/101/61850)
- Tryb uczenia się ułatwiający tworzenie reguł firewall'a
- APA (authentication proxy access) - kontrola dostępu do aplikacji wrażliwych
- IPSec VPN z obsługą certyfikatów X.509

## OPIS PRODUKTU

Router Radiflow 3180 został zaprojektowany w celu zapewnienia cyberbezpieczeństwa infrastruktury krytycznych i systemów SCADA. Gwarantuje bezpieczny zdalny dostęp i umożliwia wykrycie i zapobieganie skutkom nawet najbardziej złożonych zagrożeń. Oferuje rozwiązania zarówno dla połączeń M2M (Machine to Machine) oraz H2M (Human to Machine), zabezpieczając ruch dzięki DPI firewall (Deep Packet Inspection), który służy do analizy ruchu w systemie SCADA na poziomie przemysłowych protokołów warstwy aplikacyjnej. Urządzenie umożliwia stworzenie modelu prawidłowej pracy systemu. Po wykryciu nieprawidłowości 3180 automatycznie generuje alarmy, może blokować niepoprawne działania oraz izolować wszelkie podsieci, których dotyczą te nieprawidłowości.

## INTERFEJSY

W kompaktowej i wytrzymałej obudowie router 3180 oferuje szereg interfejsów, w tym modem z obsługą 2 kart SIM, porty szeregowy, ethernetowe oraz PoE. Może posiadać do 16 portów ethernetowych, miedzianych lub światłowodowych 10/100 oraz 2 porty SFP 100/1000. Dodatkowo router posiada funkcjonalność bramy dla protokołów szeregowych oraz pozwala na tworzenie tunelowanych połączeń z wykorzystaniem 4 interfejsów szeregowych (RJ45).

## OBSŁUGIWANE PROTOKOŁY

Router Radiflow 3180 obsługuje wszystkie podstawowe protokoły sieciowe między innymi te służące do zarządzania (SSH, Telnet) oraz protekcji sieci (RSTP, ERP i OSPF).

Poza podstawowymi protokołami sieciowymi może również pełnić rolę bramy umożliwiając translację najczęstszych protokołów SCADA m.in. DNP3, IEC-104/101, ModBus.

## BEZPIECZEŃSTWO

Rozproszony firewall DPI zapewnia operatorowi zachowanie kontroli nad siecią nawet w przypadku wyrafinowanych prób ataku. Działający w oparciu o "białą" listę firewall może być zainstalowany dla każdego portu, zarówno szeregowego jak i ethernetowego. Dzięki temu każdy punkt dostępu do źródłowej sieci jest stale kontrolowany. W każdym pakiecie protokołu SCADA (DNP3 RTU/TCP, IEC 101/104, IEC 61850, ModBus RTU/TCP) firewall sprawdza nie tylko adres źródłowy i docelowy, ale również zawartość dla danego protokołu. Rozproszona struktura firewall'a umożliwia realizację odpowiedniego zestawu reguł w każdym punkcie dostępowym do sieci, co jest szczególnie ważne przy zabezpieczeniu przed atakiem "od wewnątrz". Firewall może pracować w dwóch trybach: monitorowania i blokowania. W trybie monitorowania Dyspozytor jest powiadamiany o każdym naruszeniu reguł, ale bez blokowania ruchu. We wrażliwych lokalizacjach, można włączyć tryb blokowania, który pozwala na zablokowanie podejrzanego ruchu oraz wywołanie alarmu w centrum sterowania. W obu przypadkach przy tworzeniu reguł zalecane jest skorzystanie z trybu "uczenia się" firewall'a.

## VPN

W celu zabezpieczenia komunikacji pomiędzy sieciami router 3180 może tworzyć połączenia tunelowane VPN takie jak: IPSec, DMVPN, mGRE z możliwością zarządzania certyfikatami.

Obsługiwane są zarówno tunele VPN L-2 jak i L-3.

Rozwiązanie „Radiflow” zapewnia maksymalną ochronę przed cyberzagroženiami, bez konieczności bycia cyber-ekspertem.

## IDENTYFIKACJA UŻYTKOWNIKA

Jednym z najważniejszych wymagań standardu bezpieczeństwa NERC CIP v.5 przy zdalnym dostępie jest zdolność do identyfikacji użytkownika oraz możliwość utworzenia konkretnych uprawnień sieciowych dla każdego zidentyfikowanego użytkownika przed udzieleniem mu dostępu do sieci.

Router Radiflow 3180 zawiera wbudowany moduł APA (Authentication Proxy Access). Użytkownik przed uzyskaniem dostępu do sieci musi zalogować się do wewnętrznego procesu uwierzytelniania Radiflow za pomocą indywidualnego loginu i hasła. Po zweryfikowaniu użytkownika zostaje przydzielony mu odpowiedni profil określający dostęp do zdefiniowanych urządzeń oraz funkcji, a każda operacja jest rejestrowana. Ponadto 3180 może być zintegrowany z systemem serwera fizycznej tożsamości, umożliwiając inne metody uwierzytelniania, np. za pomocą kart magnetycznych.

## ŁATWE WDRAŻANIE

Nie musisz być cyber-ekspertem. W pełni rozumiemy złożoność sieci SCADA, ale mamy pewność, że nasze urządzenia Radiflow są proste i łatwe do wdrożenia. Bezpieczny router 3180 jest w pełni obsługiwany przez Radiflow NMS (podsystem zarządzania siecią), służący do konfiguracji i diagnostyki sieci oraz zabezpieczeń. Konfiguracja może być również prowadzona z linii komend (CLI).

Konfiguracja firewall'a również jest bardzo prosta. Po podłączeniu routera 3180 do sieci, zaczyna on przeszukiwać całą sieć zbierając informacje dotyczące innych urządzeń, zachowań itp. Na ich podstawie tworzy listę proponowanych reguł. Sugerowane reguły są opcjonalne i mogą być edytowane za pomocą aplikacji NMS.

## Jak zabezpieczyć typowe operacje w systemach SCADA

Kierunek operacji	Poziom zagrożenia bezpieczeństwa	Uwierzytelnianie	DPI tryb monitorowania	DPI tryb blokowania	VPN
Serwer SCADA->obiekt	Średni		✓		
Wewnątrz obiektu	Wysoki	✓		✓	
Zdalny dostęp	Wysoki	✓		✓	✓
Połączenie między obiektami	Wysoki		✓		✓



## Specyfikacja

### NETWORKING

#### Advanced Layer 2 feature-set

ITU-T G.8032v2 Ethernet ring  
IEEE 802.1s MSTP  
IEEE 802.1w RSTP, enhanced RSTP  
IEEE 802.3ad LAG with LACP  
IEEE 802.1q VLAN segregation  
IEEE 802.1p per port queues  
DHCP Client, Server and Relay  
QOS Prioritization, shaping, Scheduling  
OAM EFM IEEE 802.3ah  
OAM CFM ITU-T Y.1731/IEEE 802.1ag  
1588v2 PTP Transparent Clock

#### Layer 3 feature-set

Static routing  
OSPF, RIPv2 Routing  
VRRP redundancy scheme

#### SCADA protocol handling

Transparent tunneling of serial streams  
SCADA gateway for IEC101/104,  
ModBus RTU/TCP and DNP3  
Terminal Server Byte/Frame mode  
Terminal Server TCP/UDP

#### Cellular Modem

GPRS/UMTS cellular modem  
2 x SIM cards

#### SYSTEM PERFORMANCE

Line rate L2/L3 switching throughput  
Switching latency <10µSec  
16K MAC addresses  
4K VLANs

#### MULTICAST

L2 MULTICAST  
IGMP snooping for traffic optimization

### SECURITY

#### DISTRBUTED DPI FIREWALL

Profile based firewall  
Security rules planning per service group  
Firewall monitoring mode  
Firewall enforcement mode  
Firewall Learning Mode  
IEC 101 DPI Firewall  
IEC 104 DPI Firewall  
IEC 61850 mms DPI Firewall  
Modbus RTU DPI Firewall  
Modbus TCP DPI Firewall  
DNP3 RTU Firewall  
DNP3 TCP Firewall

#### VPN

IPsec Certificates X.509  
IPsec CRL server  
IPsec CA server  
IPsec Dynamic Key Exchange  
IPsec encryption AES  
IPsec encryption 3DES  
L3 IPsec VPN policy based  
L3 IPsec VPN route based  
L3 mGRE DM-VPN  
L2 VPN GRE

#### Access control

Remote access using SSH tunnel  
SNMPv1/v2/v3  
Enable/Disable port  
Port access filter per MAC / IP addresses  
IEEE 802.1x port-based authentication  
local APA (Authentication Proxy Access)  
User activity report (under local APA)  
Access Lists L2  
Access Lists L3  
Access Lists L4  
NAT - traversal  
VRF

### INTERFACES

2 x 100/1000 SFP ports  
8 x 10/100BaseT ports  
Optionally 8xPoE alternative A or 4x PoE  
alternative A and 4 x alternatives B, max per  
port is 30w and max for switch is 120w.  
8x100FX SFP ports( Optional)  
4x RS-232 ports (Optional)  
2G/3G cellular modem (Optional)  
8x10/100BaseT ports

### PHYSICAL DESIGN

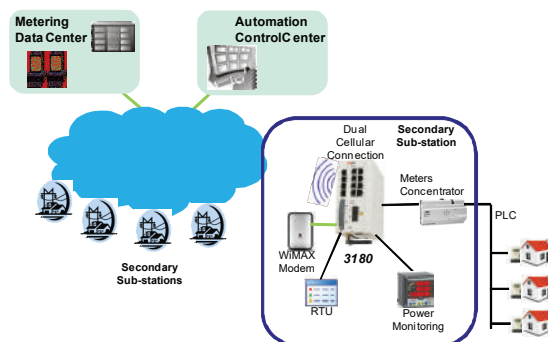
Mmounting: DIN rail (optional wall mount)  
Enclosure: Rugged - IP 30 rated, No fans  
Weight: - 1.4Kg (DC) - 1.8Kg (AC)  
Dimensions - See mechanical drawings  
Operating temperature: -40 to 75°C  
Storage temperature: -40 to 85°C  
Operating Humidity: 5%-95%  
IEC 61850-3 - Electric Utility Substations  
IEEE1613 EMI - Electric Utility Substations  
EN50121-4 Vibration and Shock resistance  
IEC 61000 -4

### MANAGEMENT

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

### LOCAL OPERATION

RS-232 console port  
Local USB port for emergency boot  
Discrete outputs reporting system alarms  
Failsafe output relay reporting critical alarm



Przykład prostego, ale bezpiecznego połączenia podstacji średniego napięcia za pomocą 3180 do sieci Smart-Grid.

## Sposób zamawiania (kody zamówień)

RF-3180<F>-<P>-<T>/<E>/<PE>[/240w]/<R>/<C>

### F- funkcjonalność

- B-podstawowa (obejmuje przełączanie L2, L3- statyczny routing, L-3 vlan routing, PoE)
- S-rozszerzona (obsługuje IPsec VPN i SCADA firewall)

### P- napięcie zasilania

- 12 - 12V DC (9 - 18V DC)
- 24 - 24V DC (18 - 32V DC)
- 48 - 48V DC (36 - 60V DC)
- 11 - 110V DC (85 - 165V DC)
- 22 - 220V DC (170 - 270V DC)
- AC - 230V AC (170 - 270V AC)
- WDC- DC szeroki zakres (18-60V DC)

### T- zakres temp. pracy

- XT- (rozszerzony zakres temp. pracy)

### E- porty ethernetowe

- ET28 -2xGE SFPs + 8x10/100RJ45
- ET216 -2xGE SFPs + 16x10/100RJ45
- ET286 -2xGE SFPs + 8x10/100RJ45 + 8x100 SFPs

PE[/240W] – porty PoE (porty PoE zawierają się w całkowitej liczbie portów określonych powyżej)

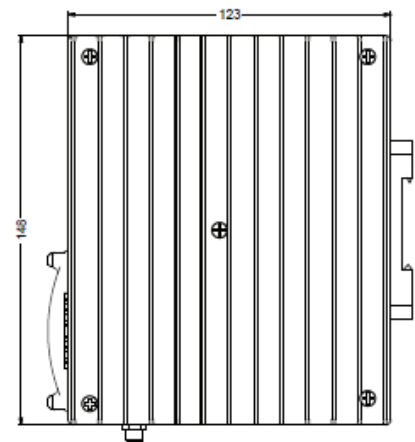
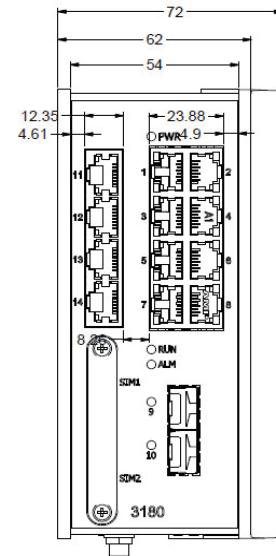
- 8PE30 - 8 portów PoE, max. 30W na port
- 8PE302RW - 8 portów PoE, z tego 2 typu B, max. 30W na port
- 8PE304RW - 8 portów PoE, z tego 4 typu B, max. 30W na port  
- opcja 240W dostępna jest tylko dla zasilania 48V DC i AC

### R\*- porty szeregowo

- 4RS2 - 4 porty RS-232
- 4RS2P - 4 porty RS-232 z izolacją 2KV

### C\*- modem 2G/3G

Uwaga:\* Niedostępne dla wersji podstawowej ,B'



## Tekniska Polska

Przemysłowe Systemy  
Transmisji Danych Sp. z o. o.

ul. Łabędzka 9G  
44-121 Gliwice, Poland

NIP 6312631825  
KRS 0000383694

+48 32 33 111 06 ÷ 09  
tekniska@tekniska.pl



WWW.TEKNISKA.PL