EdgeFirewall S2104 Datasheet

Aiming to create better and safer working environments and life experiences through the products we deliver.

Product Overview

The AVCOMM industrial ethernet firewall S2104 is a dedicated firewall device for industrial network perimeter protection with proprietary intellectual property rights, which is independently developed by AVCOMM. The device can effectively protect the information security of industrial control systems and equipment such as SCADA, DCS, PCS, PLC, and RTU. In addition to the security function of traditional firewalls, it also provides the built-in function of industrial communication protocol analysis and filtering and can adopt deep packet inspection technology and application layer communication tracking technology for industrial protocols to prevent illegal commands and block non-industrial control protocols in order to protect the controller.

Product Features

System
- B/S management structure, HTTPS encrypted communication to protect management actions from eavesdropping.
- Account + password, certificate or Ukey dual-factor authentication.

Operating Mode
- Support intelligent learning mode. The system can intelligently learn the traffic in the communication and automatically generate the corresponding protection rules.
- Support warning mode. In warning mode, communication that does not comply with the security policy is alerted.
- Support strict protection mode, and business is protected according to the system's set policy. It blocks data that does not comply with the security policy and logs it.
- Support bypass mirror mode, no need to change network configuration, realize mirror traffic self-learning, and automatically generate corresponding protection rules.

Monitoring Center
- Support shortcut buttons, which can quickly realize view menu and message, refreshing, full screen, display of administrator's personal information, administrator's password modification, administrator's logout, and other functions.
- Support button style switching; support hiding and displaying of footer.
- Monitoring Center, Log Audit, Network Configuration, Routing Management, Industrial Control Protection, Protection Settings, Object Management, Virtual Private Network, Report Statistics, Diagnostic Tools, System Management.
- Display device alias, device type, device serial number, system version, system memory, disk capacity, running time, and authorization status.
- Evaluate and score the current network status using intelligent algorithms.
- Classify and display the current protection logs, supporting pie chart display .
- Display the current CPU, memory, and disk usage.
- Display the top 10 attack sources in the past 1/3/7 days, supporting bar chart display.
- Classify and display the log levels in the past 1/3/7 days, supporting pie chart display .
- Display the policy type and number of policy entries.

Product Features

- Real-time monitoring of system network card traffic, temporarily displaying the network card name, receive speed, send speed, receive packet count, send packet count, receive byte count, and send byte count.

Log Auditing
- Whitelist protection logs, protocol alarm logs, vulnerability protection logs, intrusion defense logs, IP/MAC protection logs, ACL protection logs, system logs, and management logs.
- Support querying logs based on different dimensions.
- Support batch deletion of logs.
- Support displaying basic information of logs and current protection network overview.
- Support local export of logs.
- Support clearing current logs.
- Support paging and locating in the log list and selecting the number of log entries per page as 10/20/50/100/200/500 entries/ page.

Network configuration
- Support querying interface names, IP addresses, and statuses.
- Support adding, modifying, and deleting of network interfaces.
- Support querying bridge names and IP addresses.
- Support adding, modifying, and deleting of bridges.
- Support querying tags and IP addresses.
- Support adding, modifying, and deleting of VLANs.
- Support querying names, IPs, and statuses.
- Support adding, modifying, and deleting of aggregate interfaces.
- Support various algorithms such as load balancing, active-standby, balancing, broadcasting, and dynamic link aggregation.
- Support multiple mapping methods for SNAT/DNAT.
- Support querying the IP address after translation.
- Support adding, modifying, and deleting of NATs.
- Support DHCP domain configuration and DHCP static IP configuration.

Routing Management
- Support static routing.

Industrial Control Protection
- Support OPC.DA communication, synchronous and asynchronous monitoring data collection, only need to bind a fixed starting port to meet the dynamic data port data transmission.
- Dynamic port ensures normal communication after abnormal recovery.
- Support filtering OPC methods in OPC protocol, such as allowing only OPC reading, not allowing data writing or parameter setting.
- Support filtering read and write functions in Profinet protocol, control connection, release, read, write, control.
- Support command-level control.
- Support cross-platform OPC UA protocol.
- Support MODBUS protocol module, can control specific function codes, address ranges, value ranges, etc. according to user requirements.
- Support JOB, USERDATA, and ACK processing for Siemens S7-related PDU, support read and write control.

Product Features

- Support control of DNP3 signals and parameters, such as source/destination address, range, and variant values.
- Support remote control, remote signaling, remote adjustment, and remote measurement command control, with controllable public address and information address range, read and write control.
- Support MMS message control, device and node control, data read and write control.
- Support the addition, modification, and deletion of self-learning tasks.
- Generate whitelist protection strategies through self-learning.
- Support 1000+ predefined blacklist feature libraries.
- Support importing blacklist feature libraries.
- Support actions such as adding, deleting, modifying, searching, importing, exporting, starting, stopping, and batch modification of protection policy.
- Support new policy creation: rule name, action, service, source address, source zone, destination zone, destination address, and time.
- Support IP-MAC binding protection policy.
- Support IP-MAC table query.
- Support 10,000+ pre-defined intrusion attack feature libraries.
- Support importing intrusion attack feature libraries.

Protection Settings
- Set the threshold for scanning ports.
- Support protection against attacks such as PING OF DEATH, SMURF, teardrop, land, and winnuke.
- Support protection against attacks such as SYN FLOOD, UDP FLOOD, and ICMP FLOOD.

Object Management
- Support the addition, deletion, modification, and retrieval of address and address group objects.
- Support the addition, deletion, modification, and retrieval of zone objects.
- Support the addition, deletion, modification, and retrieval of time objects.
- Support defining time cycles based on fixed time, daily, weekly, and monthly.
- Support predefined services such as http, ftp, pop3, smtp, telnet, and rtsp.
- Support custom services.

Industrial Control Audit
- Support statistical analysis and graphical display based on device, traffic, and other types.
- Display the current system session entries.

IPSEC VPN
- Support pre-shared key and certificate authentication.
- Support CA certificate import.

Report Statistics
- Support report download in .html and .xlsx formats.
- Statistical analysis can be performed based on source address, destination address, start time, log action, protocol type, and log type.

Diagnostic Tools
- Support functions such as Ping, Talent, and Traceroute for users to diagnose network conditions.
- Support multi-dimensional network packet capture tools based on device, port, IP address, protocol, and packet capture count.

Product Features

System management

- Support configuration of management port IP, port, and gateway.
- Uses out-of-band management and in-band management, without occupying any communication resources of customer business links.
- Support SNMP management.
- Support start/stop of SSH management and selection of port number.
- Support active detection of network qualifications.
- One-click binding and unbinding of IPMAC.
- Support uniqueness check of accounts, maximum login retry times, password rule settings, and login time restrictions.
- There are security administrators, system administrators, and audit administrators.
- Set the IP or subnet of trusted hosts.
- Support manual upgrade mode.
- Support importing product licenses.
- Support importing and exporting device configurations.
- Support enabling hardware port bypass when power outage, reboot, or system crash occurs, ensuring uninterrupted network.
- Device reboot.
- Device shutdown.
- Device factory reset.
- Support one-stop wizard configuration for security protection
- Synchronize time between devices (maintain consistency via NTP)
- Support creating new session restriction entries.
- Entry display: address, maximum connection count, new creation limit per second.

Specification

S2104	
Throughput	600Mbps
Maximum Concurrent Connections	500,000
Network Interface	4GE
BYPASS	2 Pair
Expandability	No
Serial Port	1 RJ45
USB Interfaces	2 x USB2.0
Memory	2G
Hard Disk	64G
Power	
Power Supply	Dual power supply
Power Consumption	25W
Power Input Range	12~36V DC
Machanical	
Dimension	52*165*109.6mm, Fanless
Weight	1.25 Kg
Installation	DIN Rail
Environment	
Operating temperature	-20℃ ~ +70℃
Storage temperature	-40℃ ~ +85℃
Humidity	10% ~ 90% Non- Condensing
MTBF	30 Years
EMC	
EMC	GB9254 Class A or above, with at least 10DB redundancy