SIEMENS

Ingenuity for life

SICAM A8000 CP-8050

Hardware based application layer Firewall

www.siemens.com/sicam-a8000

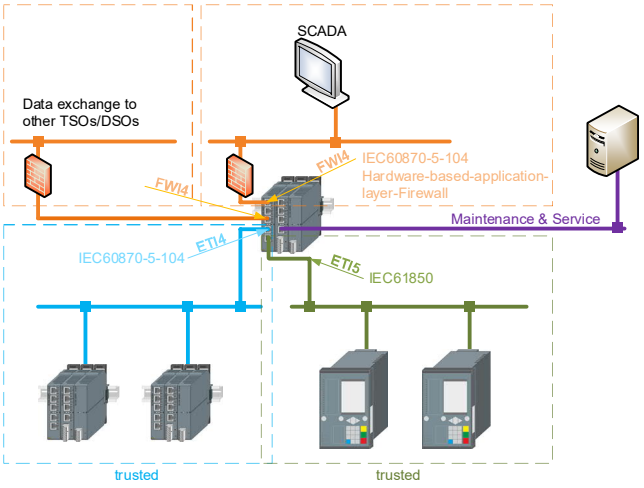
What describes a "Hardware based application layer firewall"?

At least two different Ethernet LANs are used (e.g. control center LAN A and station LAN B), information should be transferred from/to these LANs but without any physical connection and without any layer < 7 connection. That means no TCP/IP connection between these LANs. The TCP/IP stacks run independently from each other.

"Hardware based application layer firewall" with SICAM A8000 CP-8050/CI-8520

Note: CI-8520 is only a "multiplier of Ethernet ports" without any CPU that means the ports are logical part of the CP-8050. Each of the ports are part of a switch but can be configured that every single port is separated from each other (no physical connection) and each of the ports can have its own MAC address.

In this solution, IEC60870-5-104 has its own TCP/IP stack. That means additional to the already possible hardware split of the Ethernet ports (each Ethernet port can have its own MAC address), a different TCP/IP stack is used to allow even the same IP address multiple times in the same CP-8050 system. The operating system and other communication services and protocols cannot see these ports anymore. This is reached by implementation of a different path to the drivers to handle the communication between the Ethernet driver and the TCP/IP stacks. The operating system can only see the Ethernet interfaces that are not special parametrized for hardware based application layer firewall, which means all TCP/IP functions in the operation system can only see their own ports. (SNMP or statistic cannot see these ports). Also the IP addresses parametrized for this protocol are unknown to the operating system.



Configuration information

- Protocol FWI4 has to be used for this feature
- FWI4 can be used more than one time on a CP-8050 system
- Virtual-LAN configuration is possible (connect multiple ports to one LAN)
- No other services can be used on this dedicated interface

Benefits of a hardware based application layer firewall

- Network security also within the Substation zone
- No transparent IP-connection to devices "behind" the "Hardware based application layer Firewall"
- No additional hardware needed to SICAM A8000

Compared to SICAM RTUs

BDEW White Paper conformity

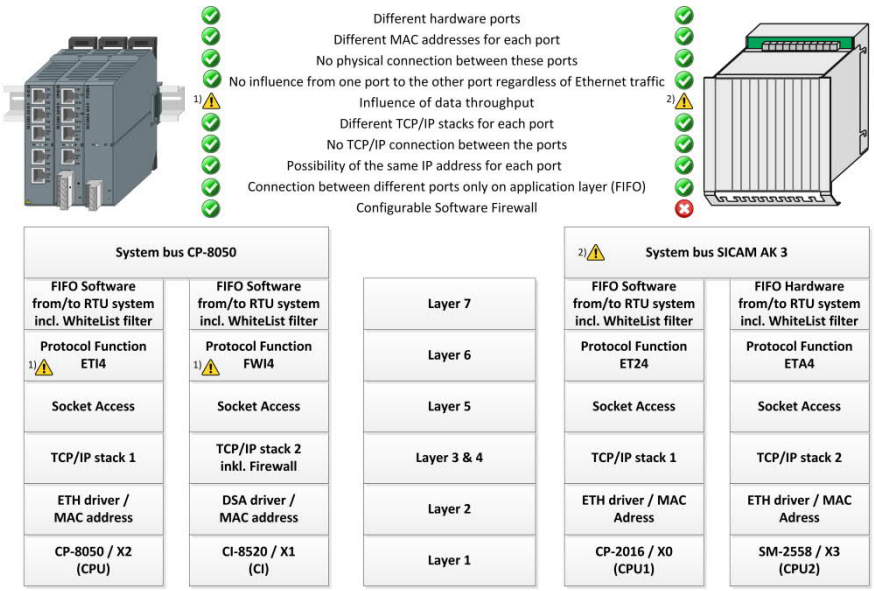
If the specification "For the network separation the use of Gateways that perform a protocol conversion and do not allow any direct IP traffic should be examined." (BDEW White Paper) is to be implemented; no conventional network firewalls (Layer 3+4) can be used.

In this case SICAM A8000 CP-8050/CI-8520 can be used as a firewall. The data of one network interface are unpacked up to Layer 7 before they are packed again into IP packets at another network interface and forwarded.

Comparison to the solution in SICAM RTUs

The solution with SICAM AK3 or SICAM TM can be covered within in the new SICAM A8000 system with CP-8050 and CI-8520.

SICAM RTUs had two independent CPUs each with its own TCP/IP stack. SICAM A8000 is a single CPU system. But still each of the ports can be configured to be separated from each other (no physical connection) and each of the ports has its own MAC address. Because of the two different TCP/IP stacks each can have its own IP address, subnet mask, default gateway, even the same IP address.



1) Regarding the single CPU architecture this cannot be achieved, influence is reduced with software capabilities (disable interrupt during broadcast storm, switch reduced traffic on CI-8520 module)

2) Data throughput is limited regarding system internal bus between CPUs.

Siemens 2019

Smart Infrastructure
Digital Grid
Humboldtstrasse 59
91459 Nuremberg,
Germany

For the U.S. published by Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Customer Support: http://www.siemens.com/csc