SIEMENS
Ingenuity for life

SICAM A8000 CP-8050

Hardware based application layer Firewall

www.siemens.com/sicam-a8000

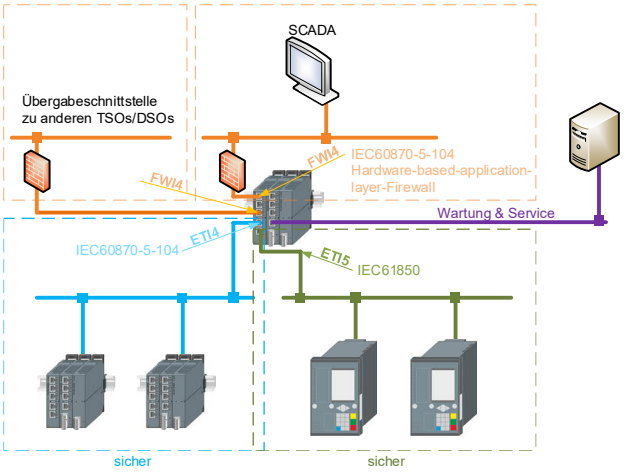
Was zeichnet eine "Hardware based application layer firewall" aus?

Mindestens zwei unterschiedliche Ethernet LANs werden verwendet (z.B: Stations-LAN A und Stations-LAN B), Information von/zu diesen LANs soll allerdings ausschließlich über eine Verbindung über Layer 7 (Application Layer) ausgetauscht werden. Das bedeutet, dass keine TCP/IP Verbindung zwischen diesen LANs existieren darf. Die TCP/IP Stacks müssen unabhängig voneinander laufen.

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

Anmerkung: CI-8520 ist lediglich eine Vervielfältigung von Ethernet Schnittstellen ohne eigene CPU. Das bedeutet die Ports sind logischer Teil der CP-8050. Jeder dieser Ports ist Teil des konfigurierbaren Switches, kann daher von allen anderen Ports getrennt werden (keine physikalische Verbindung) und kann dadurch auch seine eigene MAC Adresse haben.

In dieser Lösung hat das IEC60870-5-104 Protokoll seinen eignen TCP/IP Stack. Das bedeutet, dass zusätzlich zu der Hardwaretrennung (jeder Port hat eine eigene MAC Adresse) ein anderer, eigenständiger TCP/IP Stack verwendet wird. Das ermöglicht die mehrmalige Verwendung von gleichen IP-Adressen innerhalb eines CP-8050 Systems. Weder das Betriebssystem noch die Services haben auf diese Ports noch Zugriff. Das wird durch die Implementierung eines eigenen Kanals erreicht, der die einzige Verbindung zwischen eigenständigem Stack und eigenständigem Treiber darstellt. Das Betriebssystem kann dadurch die speziell parametrierten „Hardware based application layer firewall"-Ports nicht mehr sehen/verwenden. Auch die IP-Adressen, die dafür parametriert wurden, sind dem Betriebssystem nicht bekannt.



Konfigurationshinweise

- Protokoll FWI4 und CI-8520 muss für diese Funktion verwendet werden
- FWI4 kann mehrmals pro CP-8050 System verwendet werden
- Virtuelle-LAN Konfiguration ist möglich (Verbindung mehrerer Ports zu einem LAN)
- Auf dieses Interface haben keine anderen Services mehr Zugriff

Vorteile der "Hardware based application layer firewall"

- Netzwerk-Security auch innerhalb des Umspannwerks
- Keine transparente IP-Verbindung zwischen Geräten "hinter" der "Hardware based application layer Firewall"
- Keine zusätzliche SICAM A8000 Hardware notwendig

Vergleich zu SICAM RTUs

BDEW White Paper konform

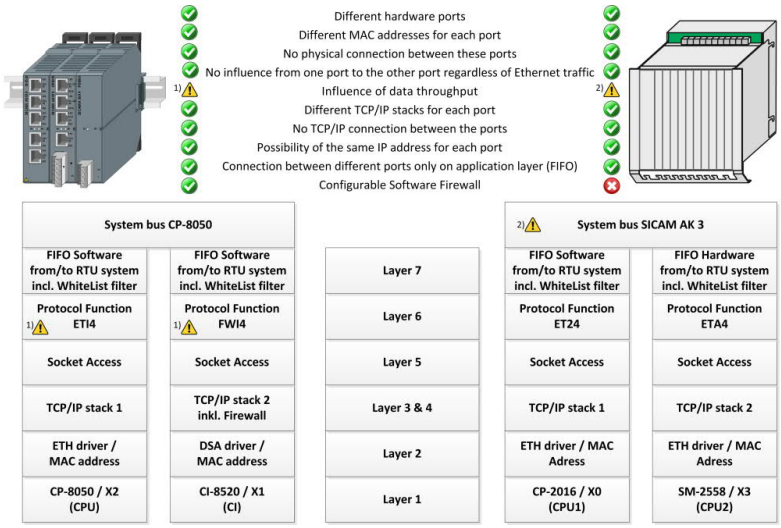
Wenn die Anforderung “For the network separation the use of Gateways that perform a protocol conversion and do not allow any direct IP traffic should be examined.” (nach BDEW White Paper) erfüllt werden soll, können keine konventionellen Firewalls (Layer 3+4) verwendet werden.

In diesem Fall kann SICAM A8000 CP-8050/CI-8520 als Firewall verwendet werden. Die Daten von einer Netzwerkschnittstelle bleiben verpackt bis zu Layer 7, bevor sie über einen anderen TCP/IP Stack als neue IP Pakete zu einer anderen Netzwerkschnittstelle weitergeleitet werden.

Vergleich zu SICAM RTUs Lösung (SICAM AK3/ TM)

Die Lösung in SICAM AK3 oder SICAM TM kann daher im neuen SICAM A8000 System mit CP-8050 und CI-8520 abgedeckt werden.

SICAM RTUs haben zwei unabhängige CPUs mit ihrem jeweils eigenen TCP/IP Stack. SICAM A8000 CP-8050 ist ein Single-CPU system, bietet aber durch die Konfigurierbarkeit der Ports trotzdem die Möglichkeit eine Hardware-Trennung herzustellen (eigene MAC Adressen). Aufgrund der zwei unterschiedlichen TCP/IP Stacks, kann jeder der Ports seine eigene IP-Adresse und sogar gleiche IP Addresse haben.



1) Durch Single-CPU Architektur kann das nicht erreicht werden, die Beeinflussung wird allerdings durch die Firmwarefunktion limitiert (Interrupt während Broadcast-Storm reduziert Datenlast am CI-8520 in Richtung CPU)

2) Datendurchsatz ist durch den Knotenbus an der Backplane limitiert.

Siemens AG 2019

Smart Infrastructure
Digital Grid
Humboldtstrasse 59
91459 Nürnberg, Deutschland

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