

FSP 150-XG118Pro (CSH)-G

10Gbit/s Ethernet-Netzzugang mit Hardware-
Verschlüsselung und Server

Ihre Vorteile

- **Zuverlässiger Schutz des Netzes**
Hardware-basierte Ende-zu-Ende Verschlüsselung schützt einzelne Verbindungen oder gesamten Ethernet-Verkehr auf Netzschicht 2
- **Kryptografisches Modul**
Kompaktes, integriertes Sicherheitsmodul schafft Kryptoagilität, schützt den Schlüsselaustausch und verhindert unautorisierten Zugriff auf sensible Daten
- **Freigabe für klassifizierte Daten**
Zulassung für die Übertragung von Verschlusssachen bis „VS-NfD“ und „EU/NATO Restricted“ durch das BSI (BSI-VSA-10433)
- **Präzise Synchronisation**
Hardware-basierte Synchronisation ermöglicht ein genaues Timing mit optionaler Authentifizierung und Integritätsschutz für das PTP-Protokoll^(f)
- **Sicheres Edge-Computing**
Optionaler Server ermöglicht geschütztes Hosting von virtualisierten Netzfunktionen
- **Leistungsfähiges Managementsystem**
Konfiguration und Betrieb von Netz-, Server- und Sicherheitsfunktionen mit leistungsfähiger Ensemble Management Suite

Überblick

Die Nachfrage nach Bandbreite in den Netzen steigt und gleichzeitig verlangen Kunden einen hohen Schutz für ihre sensiblen Daten.

Zugangsnetze sind daher einem kontinuierlichen Wandel unterworfen und müssen flexibel von 1Gbit/s auf 10Gbit/s-Dienste erweitert werden. Mit einer latenzarmen Ende-zu-Ende Verschlüsselung können die hohen Sicherheitsanforderungen von kritischen Infrastrukturen und Behörden auch über bestehende, nicht-vertrauenswürdige Netze erfüllt werden.

Adva Network Security hat mit der neuen FSP 150-XG118Pro (CSH)-G ein leistungsstarkes Netzzugangsgerät entwickelt, das sensible Daten zuverlässig schützt und eine schnelle und flexible Erweiterung von 1Gbit/s auf 10Gbit/s-Dienste ermöglicht. MEF 3.0-konforme Carrier Ethernet- und IP-Verbindungen werden hardwarebasiert und mit geringer Latenz verschlüsselt. Die Kryptoagilität wird durch ein Sicherheitsmodul erreicht, das auch die Erzeugung und Anwendung von Schlüsselmaterial zuverlässig schützt und sensible Daten sicher speichert. Manipulationsversuche an der physischen Hardware und Software werden erkannt und führen zu Schutzmaßnahmen ("Tamper Detection & Response"). Netzwerkverbindungen können im FSP 150-XG118Pro (CSH)-G auf Flow-Basis segmentiert und dynamisch gesteuert werden. Diese Leistungsmerkmale werden durch umfangreiche Synchronisationsfunktionen ergänzt. Ein steckbares Servermodul ermöglicht das sichere Hosting von virtualisierten Netzwerkfunktionen wie beispielsweise einer Firewall oder eines Systemes zur Angriffserkennung. Das sichere Netzzugangsgerät wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Übertragung von Verschlusssachen bis VS-NfD beziehungsweise „EU/NATO Restricted“ zugelassen (BSI-VSA-10433).



FSP 150-XG118PRO (CSH)-G

Technische Spezifikationen auf einen Blick

Sicherheit

- Kryptografisches Modul
- Physischer Manipulationsschutz, Secure Boot, Secure Update
- Echter Zufallszahlengenerator
- AES-Verschlüsselung im FPGA
- BSI-Zulassung bis VS-NfD

Schnittstellen

- 8 x 1/10Gbit/s (SFP/SFP+) Ports mit MACsec-Verschlüsselung
- Zwei interne 10Gbit/s Ports zum Serversteckplatz
- 82 Gbit/s Kapazität

Schutz des Verkehrs

- IEEE 802.1AX Link-Aggregation (LAG) für Lastverteilung und Ausfallschutz (active/stand-by)
- ITU-T G.8032 Ethernet in Ringtopologie
- ITU-T G.8031 Ethernet lineare Schutzschaltung

Ethernet Funktionen

- Hierarchische Dienstklassen
- Traffic Shaping
- Jumbo-Frames und Elephant-Flows
- L2-L4 Zugriffskontrolle
- EoMPLS-Enkapsulierung

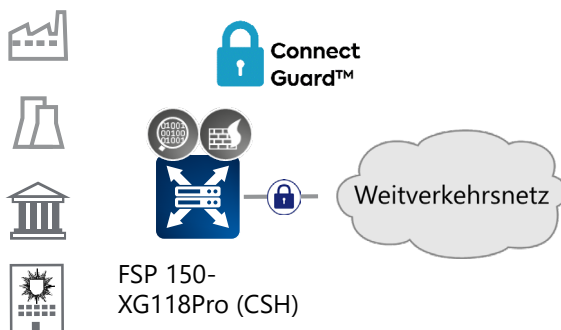
Management

- Betrieb mit leistungsfähigem Ensemble Controller Managementsystem
- MEF-konformes SOAM und OAM
- Zugriffsschutz mit RADIUS/TACACS+

Umweltbedingungen

- IHE-Gehäuse, ETSI-kompatibel
- Betriebstemperatur: -40 bis +65°C (erweiterter Temperaturbereich)
- Redundantes, modulares Netzteil (AC und DC)

Anwendungen im Netz



- Ende-zu-Ende Verschlüsselung von Ethernet-Verbindungen auf Netzschicht 2
- Hosting virtualisierter Netzfunktionen
- Überwachung des Verkehrs (Demarkation) und VLAN Segmentierung
- Redundante Wegeführung
- Synchronisation mit SyncE und PTP

- Hochsicherer Netzzugang für Dienste mit 10Gbit/s Bandbreitenbedarf im Ethernet- und IP-Verbindungsnetz
- Ende-zu-Ende-Verschlüsselung von Ethernet VLAN-Verbindungen oder gesamten Ethernet Schnittstellen (Netzschicht 2)
- Krypto-Agilität ermöglicht den Wechsel zu neuen, quantensicheren Algorithmen für den Schlüsselaustausch
- Hosting von virtualisierten Netzfunktionen (VNF) wie Firewall und Intrusion Detection auf optionaler Server-Einschubkarte
- Hardware-basierte Synchronisation für ein präzises und zuverlässiges Timing mit optionaler Authentifizierung und Integritätsschutz des PTP-Protokolls^(f)
- Schnelle Bereitstellung von Verbindungen durch zentrale SDN-Steuerung im Zusammenspiel mit der bewährten und äußerst zuverlässigen Netzmanagementlösung Ensemble Controller

Product specifications

FSP 150-XG118Pro (CSH)-G overview

Traffic ports	Traffic plane	Operating temperature	Power supply	Size	Power consumption
8 x 1/10GbE, 2 x 10GbE to server	82Gbit/s	-40°C to +65°C	Modular Dual AC or DC	1RU (H) 445mm (W)	85W typical (without server)

XG118Pro (SH) Server Card	Processor	Cores	DDR4	SSD	Temperature Range
F150/VME/SRV/X8/32	Intel D-1539	8	32GB	256 – 512GB	I-Temp
F150/VME/SRV/X12/32	Intel D-1559	12	32GB	256 – 512GB	I-Temp
F150/VME/SRV/X16/64	Intel D-1577	16	64GB	256GB – 1TB	C-Temp

Traffic ports

- Eight 1/10GbE (SFP/SFP+) ports with MACsec capability
- Two internal 10GbE ports to server slot
- Flexible allocation of bandwidth to traffic and server ports
- 82 Gbit/s traffic capacity

Hardware-based encryption engine

- AES encryption implemented in FPGA
- 80 Gbps line rate encryption
- MACsec transformation with VLAN bypass
- GCM-AES-128/256 cipher suites
- Extended packet numbering
- Integrity and confidentiality protection
- Configurable replay protection
- Up to 128 secure flows
- IPsec ready

Crypto module and physical security

- Built-in hardware cryptographic module
- Hardware trust anchor and secure boot
- True random number generator and deterministic random bit generator
- Authenticated key exchange
- Secure storage of critical security parameters with power backup for up to 60 hours
- Hardware-ready for IPsec and post-quantum cryptography such as McEliece

Traffic protection

- IEEE 802.1AX link aggregation – active/standby or load balancing
- ITU-T G.8032 Ethernet ring protection
- ITU-T G.8031 Ethernet linear protection switching^(f)

VLAN support

- 4096 VLANs (IEEE 802.1Q customer-tagged) and stacked VLANs (Q-in-Q service provider tagged)
- 2-tag management (push/pop/swap) for c-tag and s-tag
- IEEE 802.1ad provider bridging (c-tag, s-tag)
- Ethertype translation
- Point-to-point, multipoint and rooted-multipoint Ethernet virtual circuits (EVC)
- 9612 byte-per-frame MTU transparency
- EoMPLS encapsulation

Server capability

- Fully open architecture supporting Ensemble Connector or other VNFs
- Hot pluggable server option
- High-performance Xeon-D® CPU with up to 16 cores
- Up to 64 GBytes DDR4 SDRAM, up to 1TB of SSD
- Independent supervision processor installs and monitors server software and status
- Expandable via eSATA and USB interfaces

Synchronization

- ITU-T G.8261 / G.8262 / G.8264 Synchronous Ethernet on all traffic interfaces
- Sync status message support
- IEEE 1588v2 Precision Time Protocol with hardware time-stamping
- ITU-T G.8265.1^(f) and G.8275.1 PTP telecom profiles
- G.8265.1 telecom slave^(f)
- G.8273.2 telecom boundary clock
- BITS-in and BITS-out with sync status messaging
- Combined 1PPS and TOD clock output
- Internal Stratum-3E clock with holdover

FSP 150-XG118PRO (CSH)-G

Layer 2 traffic management

- Acceptable client frame policy: tagged or untagged
- Service classification based on IEEE 802.1p, 802.1Q and IP-TOS/DSCP
- VLAN tag priority mapping (IEEE 802.1ad PCP encoding)
- MEF-compliant policing (CIR/CBS/EIR/EBS) with three-color marking and eight classes of service
- Port shaping on transmit
- MEF 10.3 hierarchical policing with token-share envelopes
- DiffServ supporting WFQ/SP mix
- Elephant flows management

Layer 3 traffic management^(F)

- L2-L4 access control lists (ACL) for classification
- VRF-lite virtual routing and forwarding
- BGP and OSPF dynamic routing
- DHCP relay agent and DSCP remarking

Operation, administration and maintenance (OAM)

- IEEE 802.3ah EFM-OAM link management
- IEEE 802.1ag connectivity fault management (CFM) with hardware assistance
- ITU-T Y.1731 performance monitoring
- ITU-T Y.1564 service activation testing
- Terminal and facility loopbacks on port- and EVC-level for all interfaces
- MEF-compliant Layer 2 control protocol disposition and extensive filter options for Layer 2 packet types
- Link loss forwarding to signal local link and network path failures
- Dying gasp message for power failure alarm (EFM-OAM and SNMP trap option)
- Port mirroring (local and remote)^(F)

Performance monitoring

- RFC 2819 RMON Etherstats on a per-port and per-service basis
- 15-minute and 1-day performance data bins
- IEEE 802.3ah/ITU-T G.8021 PHY level monitoring
- ITU-T Y.1731 single- and dual-ended frame loss measurement
- Synthetic frame loss and delay measurement for multi-point service monitoring
- TWAMP sender/reflectors for L3- based service assurance^(F)
- Multi-CoS monitoring on EVCs
- IPFIX^(F)
- Threshold-setting and threshold-crossing alerts
- Physical parameter monitoring for SFP optics with TCAs
- Temperature monitoring and thermal alarms

Low-touch provisioning^(F)

- DHCP/BOOTP auto-configuration
- IEEE 802.1x port authentication (supplicant and authenticator)
- Text-based configuration files
- TFTP/SCP for software image upgrade and configuration file copy

Management and security

Local management

- Local LAN port (RJ45) using CLI, NETCONF, and web GUI interfaces
- RS-232 using CLI
- 3G/LTE/Wi-Fi USB interface^(F)

Remote management

- Maintains in-band VLAN-based management tunnels
- Fully interoperable with other FSP 150 products

Management protocols

- IPv4 and IPv6 DCN protocol stacks, including dual-stack operation and 6-over-4 tunnels
- Telnet, SSHv2, HTTPS, SNMPv3, NETCONF/YANG

Secure administration

- Configuration database backup and restore
- System software download via HTTPS, SFTP or SCP (dual flash banks)
- Remote authentication via RADIUS/TACACS
- SNMPv3 with authentication and encryption
- IPsec on management traffic^(F)
- Access control list (ACL)

IP routing

- DHCP, OSPF, and static routes, ARP cache access control

System logging

- Alarm log, audit log and security log

Regulatory and standards compliance

- FIPS 140-3 Level 2 compliant (certification pending)
- MEF CE 3.0 compliant
- IEEE 802.1Q (VLAN), 802.1p (Priority), 802.1ag (CFM), 802.3ah (EFM)
- ITU-T Y.1731, G.8010/Y.1306, G.8011.1+2, G.8032
- MEF-6.1, -9, -10.2, -11, -14, -20, -21, -22.1, -23.1, -25, -26.1, -30, -33, -35, -36
- RFC 2863 (IF-MIB), RFC 2865 (RADIUS), RFC 2819 (RMON), RFC 5357 (TWAMP)
- MEF-48 and MEF-49 compliant ITU-T Y.1564 service activation testing
- ANSI C84.1-1989
- ETSI 300 132-2, BTNR2511, ETS 300-019, ETS 300-019-2-[1,2,3], ETS 300-753
- NEBS Level 3 compliant
- Telcordia GR-499, GR-63-CORE, SR-332
- Safety IEC/UL/EN 60950, 21CFR1040.10, EN 60825, EN 50371, EN 300-386, EN 50160, IEC 60320/C14
- EMI EN 300-386, GR-1089-CORE, ETS 300-132, FCC Part 15, Class A, Industry Canada

Environmental

- Dimensions (W x H x D):
 - AC: 445.5 mm x 43.6 mm x 366.6 mm
 - DC: 445.5 mm x 43.6 mm (1.7 in.) x 255.4 mm
- Operating temperature:
-40°C to +65°C / -40°F to 149°F
(hardened environment)
- Storage temperature:
-40°C to +70°C / -40°F to 158°F (GR-63-CORE)
- Humidity:
5 to 95%, B1 (non-condensing)
- Redundant modular hot-swappable power supply:
 - AC: 110/240VAC, with over-voltage and over-current protection or
 - DC: -48 to -72VDC with over-voltage and over-current protection

(F) = future

