EANTC Independent Test Report

ADVA ConnectGuard™ Ethernet - MACsec Plus L2 Encryption Security and Performance

October 2018

EANTC

ADVA™ Optical Networking

Introduction

ADVA Optical Networking commissioned EANTC to verify the functionality of its FSP 150 customer premises devices. EANTC conducted a range of tests of the encryption functions, with a particular focus on Carrier Ethernet data protection use cases. The tests were carried out at EANTC's lab in Berlin, Germany, in July 2018. Our tests corroborated the functional aspects of the encryption device along with specific key performance indicators related to the security of transmitted data.

Frequently, service providers are challenged to meet enterprise demands for network service security. Customers want to host data or applications in centralized data centers but are reluctant to transport sensitive data across public or third-party networks, which are considered to be untrustworthy environments. ADVA FSP 150 edge devices implement the highly secure **AES-256 encryption algorithm** applied for Ethernet or IP services, protecting user data as well as control and management traffic.

Test Highlights

- ➔ MACSEC hardware encryption adds only 0.36 µs latency to a P2P link
- ➔ Automatic start/stop of traffic flows and key exchanges triggered by IEEE 802.1ag CFM alarms
- ➔ No frame loss in 1-minute Diffie-Hellman key exchange interval scenario for 7 concurrent sessions
- ➔ Tamper-proof hardware protecting passwords and keys

Encryption is known to affect performance indicators such as latency and throughput. The ADVA FSP 150 implements encryption in hardware to meet customer requests for high performance and low latency.

According to ADVA the FSP 150 devices complement encryption with tamper-resistant design and a trusted compute platform for secure storage of keys and for software attestation. Security control is only as secure as the applied key exchange and key storage mechanisms.

Executive Summary

ADVA FSP 150 ConnectGuard™ Ethernet data protection, based on the Media Access Control (MAC) Security standard defined in IEEE 802.1AE-2006 and IEEE 802.1AEbn-2011, uses a hardware-based design for encryption of Carrier Ethernet services with Gigabit Ethernet and 10 Gigabit Ethernet line speed, allowing the transport of sensitive data across wide area networks and supporting point-to-point topology.

EANTC conducted a vendor-defined limited set of functionality tests of the encryption features. These tests were successful and the results met our expectations. Throughput and latency tests were based on Gigabit Ethernet hardware showing promising results. ADVA claimed that the device's price point can turn data link encryption into a standard product for Service Provider markets.

We found that the ADVA FSP 150 is suitable as an edge device for securing multiple flows between branch, headquarter and data-center premises. This is enabled not only by encryption usage but also by detecting issues in Carrier Ethernet networks and offering hardware tamper resistance.

Hardware: ADVA FSP 150

Hardware Type	Software Version
FSP 150-GE114Pro (C)	9.6.1 (used for automatic start/stop of key exchange test case) 8.5.1 (used for all other tests)

The Crypto "C" variant of the FSP 150 series is an L2/L3 encryption device for the secure connection of main and branch offices via Carrier Ethernet services. Two devices with hardware version 1.01 were used and tests were performed with traffic generators creating flows with Ethernet traffic mix ("EMIX") consisting of a range of frame sizes to ensure a realistic Ethernet traffic load in a Carrier Ethernet service.

Hardware Overview

The FSP 150 version under test comes with special HW engine for encryption related functions. The HW engine ensures the performance and precision of business-critical security tasks.

One of the key functions is a Random Number Generator which generates a physical random bit stream and random numbers at high speeds. The security of cryptographic exchange depends on the quality of the random numbers used. Good random numbers are fundamental to almost all secure computer systems; in case they would lack quality and could be predicted by an attacker, encrypted information would be compromised. In other words, the random number generator is a critical component for the security of the system.

ADVA explained that the additional HW components dual-port, dual-media QSGMII/SGMII GbE PHY enables network-wide layer 2 MACsec encryption and preserves nanosecond-level IEEE 1588v2 network timing accuracy due to its Intellisec™ and VeriTime™ features. In summary, the ASIC enables handling of MACsec encryption in combination with single/dual VLAN tag bypass as well as frequency, phase and time distribution for secure end-to-end services.

Test Results: Functionality

Following FSP 150 features were tested:

- Secure EVPL
- Required VLAN tags in the clear for bypass
- SECTAG format compliance
- Password authenticated Diffie-Hellman Key Exchange
- Tamper resistance
- Crypto user permissions
- Automatic Start/Stop of Key Exchange Messages

Secure EVPL

Media Access Control Security (MACsec) enables the encryption of data between two sites connected via an untrusted network. In this test case, we considered two scenarios, each with two traffic flows transported via a Carrier Ethernet EVPL. Refer Table 1.

	Flow A	Flow B
Scenario 1	Sensitive data	Non-sensitive data
Scenario 2	Sensitive data	Sensitive data

Table 1: Secure EVPL - Test Scenarios

For the first scenario, ADVA mapped flow A to one EVC encrypted as a single Secure Flow; Flow B was mapped to a different EVC and transmitted in clear text. This is shown in Figure 1. In the second scenario, both flows were secured.

The goal of this test was to confirm that the content in the frames, corresponding to a secure EVC, was encrypted. This includes everything except the transport VLAN tag. In the same manner, the content of the frames corresponding to the unsecured EVC was in clear text. We generated traffic consisting of different frame sizes ("Ethernet MIX"). Other parameters are specified in Table 2.

We monitored traffic flows between the two FSP 150 units. EANTC concluded that the FSP 150 was able to separate traffic flows and perform encryption correctly following the configuration, as was expected.

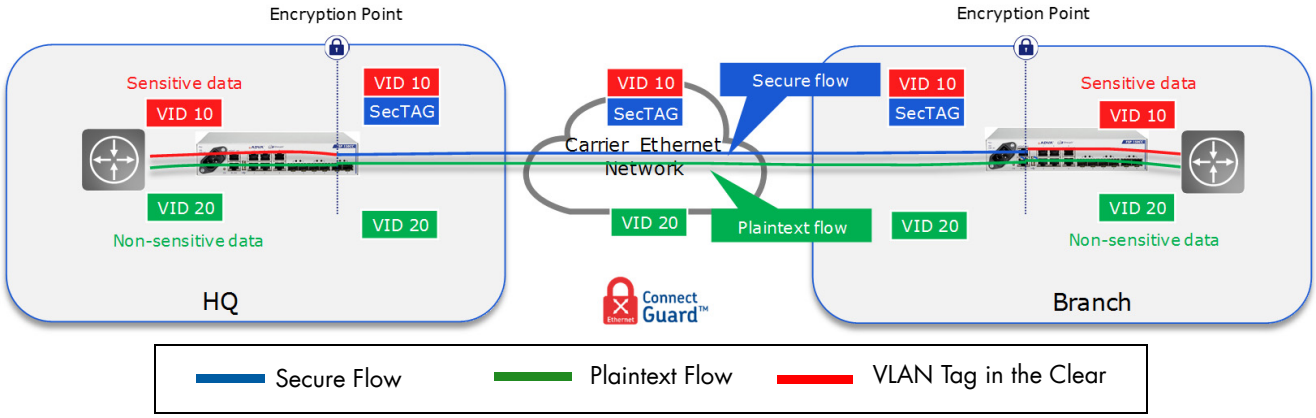


Figure 1: Secure EVPL

Parameter	Value
Bandwidth per direction	100 Mbit/s
Key exchange interval flow A	1 minute
Key exchange interval flow B	3 minutes

Table 2: Parameters for Both Traffic Flows

SECTAG Frame Format Compliance

MACsec is defined in IEEE 802.1AE-2006 and IEEE 802.1AEbn-2011. Complying with this standard is important for interoperability with other vendors. While we did not perform multi-vendor interoperability tests, we did inspect frames to confirm that the format of the SECTAG is compliant. This added header conveys parameters that identify the protocol, key to validate the received frame and provide replay protection. The fields expected to be seen are listed in Table 3.

All required fields were present, except the SCI since it is not encoded in SECTAG for point-to-point traffic. Compliance was confirmed as shown in Figure 2.

Field	Size
Ethertype (0x88E5)	2 bytes
Tag Control Information (TCI)	4 bits
Association Number (AN)	4 bits
Short Length (SL)	1 byte
Packet Number (PN)	4 bytes
Secure Channel Identifier (SCI) - Optional	8 bytes

Table 3: SECTag Fields

```
802.1AE Security tag
> 0000 11.. = TCI: 0x03, VER: 0x0, E, C
  .... ..01 = AN: 0x1
  Short length: 0
  Packet number: 1693023
  ICV: 95f84cc3017fc6e50883a24d18074497
```

Figure 2: SECTAG Section of Captured Frame

VLAN Tags in the Clear

The FSP 150 provides support of end-to-end services while keeping the IEEE 802.1AE protocol format across the wide-area network. The number of VLAN tags in the clear is configurable on each Secure Flow independently. Possible values are 0, 1 or 2. We validated each possible value. Table 4 describes the VLANS used in each scenario, in all of them the VLAN Tag added by the Traffic Generator (TFGEN) was encrypted.

We witnessed three successful test case executions, each with a 200 Mbps traffic flow. The corresponding number of required VLANS in the clear was observed, allowing the encrypted data to be transported across a single or double VLAN-tagged network as regular non-MACSec frames.

VLAN Tags in the Clear	S-TAG	C-TAG	TFGEN TAG
0	NO TAG	NO TAG	32
1	NO TAG	3	32
2	1003	3	32

Table 4: VLAN Tag Specification

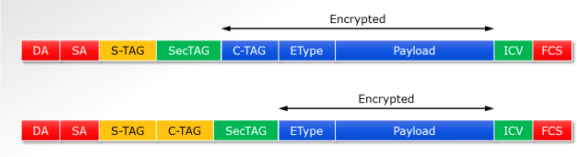


Figure 3: VLAN Tags in the Clear

Diffie-Hellman Key Exchange

To maintain the security of sensitive data, the keys used to encrypt must be changed frequently. The FSP 150 uses the Diffie-Hellman algorithm to perform the key exchange via an unsecured channel between two encryption devices. Key sizes vary according to groups specified in RFC3526. The ADVA FSP 150 supports key sizes of 2048 and 4096 bits.

Frame Type	Ethertype Value
Regular MACSec	0x88E5
Key exchange	0x88B7

Table 5: Ethertype Values

Key exchange frames are distinguished from regular MACsec frames by their Ethertype values, displayed in Table 5. In this test, we observed two different Secure Flows to determine whether the key exchange would occur at the configured frequency (the configurable range is 1–60 minutes). Key exchange frames are identified as belonging to a Secure Flow by their VLAN tags as seen in Figure 5.

The devices were also configured to use a unicast address belonging to the peer for the key exchange messages. We noticed that the initial frame was directed to a multicast MAC address and subsequent ones used the unicast MAC address as expected. Other parameters are specified in Table 6.

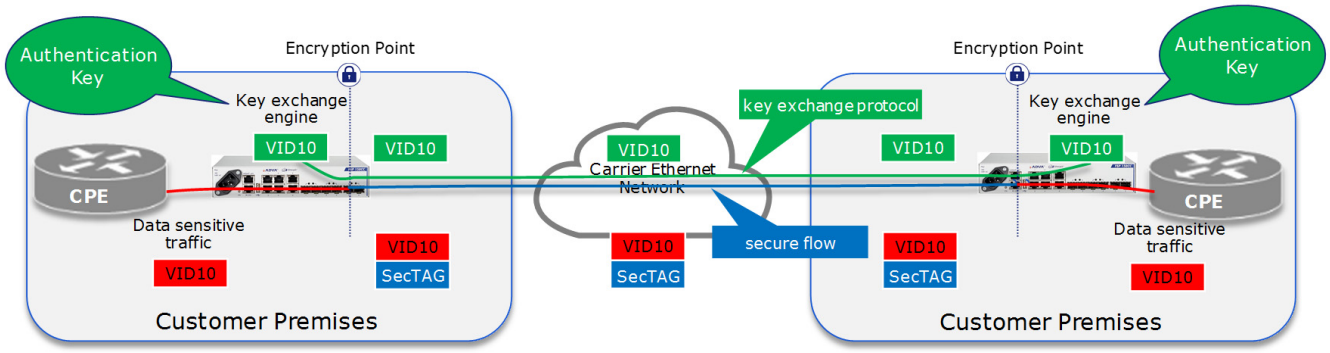


Figure 4: Diffie-Hellman Key Exchange Traffic Separation

Both flows showed key exchanges at the desired interval; the process did not interrupt normal traffic (no frame loss). This feature was tested again performance-wise in a subsequent section.

Parameter	Value
Number of secure flows	2
Flow bandwidth	1 Mbps/flow
Key exchange interval	1 minute
Key size	4096 bits
Authentication password	32 characters
Number of tags pushed	2

Table 6: Configuration Parameters

Tampering Resistance

The physical security of firewalls or encryption devices is normally assumed to be covered by locking them in a data center. However, protection is desirable In case an attacker gets their hands on the equipment. We validated the FSP 150's tampering resistance feature which promises to prevent physical access to authentication passwords and private keys.

Figure 5: Crypto Password Initial Login

If the cover of ADVA FSP 150 is opened during operation, a tamper event will be reported, the passwords will immediately be erased and the equipment will perform a cold reboot clearing all keys in memory. We tested this function with traffic. The encryption device was configured to run a Secure Flow with no traffic loss.

The cover was opened and the device performed a cold reboot, a new login is seen in Figure 4. A login to the device confirmed that it had effectively erased authentication passwords/keys and showed logs stating "ConnectGuard RAM cleared/Key Exchange Authentication Password Missing".

Crypto User Permissions

The Crypto user is a special privilege level that is required for the configuration & management of encrypted services. Users with any other privilege than the Crypto user (e.g. Super User or Provisioning) neither have access to key management settings nor can they provision Secure Flows or create Secure Flow associations.

Provision	Super-User	Crypto-User
Crypto user	Not allowed	Allowed
Key exchange	Not allowed	Allowed
Secure flow	Not allowed	Allowed

Table 7: User Privilege Results

We created a Crypto User and a Super-User to test the permissions of both. The results are shown in Table 7. Security in the internal device management and configuration prevents not only intruder access but also a human error by less experienced administrators. Test results were positive as only the Crypto-user was allowed to perform all the tasks mentioned.

Automatic Start/Stop of Key Exchanges

Ethernet Operations, Administration and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to increase management capability within the context of the overall Ethernet infrastructure. The ADVA FSP 150 uses Ethernet OAM to support encrypted Carrier Ethernet services.

➔ Demonstrated an automatic start/stop of traffic and key exchange, in a Secure Flow, triggered by IEEE 802.1ag CFM alarms

In this test, we used two FSP 150 running a Secure Flow with activated Continuity Check Messages (CCM), which are part of standard IEEE 802.1ag Connectivity Fault Management (CFM). CCM acts as a "keep alive" mechanism to ensure the Carrier Ethernet service is available.

Software Release Used in this Test Case
9.6.1

Table 8: Software Release

The Secure Flow with CCM was running smoothly. Then we proceeded to block CCM messages to simulate a network failure. The FSP 150 placed the Secure Flow in a Secured Block state, which basically stopped all traffic in the flow including the key exchange as expected until CCM certified correct connectivity of the Carrier Ethernet service again. By detecting a high frame loss ratio and preventing key exchange failures the FSP 150 eliminates any manual intervention of the Crypto user to restart the key exchange process. For this test only, it was required to upgrade the device software version to release 9.6.1.

Test Results: Performance

Although functionality was the main focus of this testing, some performance testing was required to demonstrate that the ADVA FSP 150's encryption functions work without decreasing customer's KPIs. Among the cases are:

- Throughput in Secure EPL
- Latency added by MACsec Hardware Encryption
- Concurrent Secure Flows

Throughput in Secure EPL

This test was performed using a Gigabit Ethernet link between two FSP 150s with a Secure EPL configured. Traffic generators produced an "EMIX" traffic flow, consisting of a range of frame sizes (128, 256, 512, 1024, 1518 Bytes) to ensure a realistic traffic load in the network. The goal was to determine the maximum throughput with no frame loss through a Secure Flow. The result was a net throughput of 934 Mbit/s. In other words, this is the actual bandwidth of the payload in a Secure flow, with one VLAN tag, through a 1Gbps WAN link, with no frame loss.

The reason for the stream not having a higher throughput is in part caused by the overhead. The overhead consisted of 8 bytes SecTag, providing protocol and key identification plus replay protection, 16 bytes Integrity Check Value designed to protect a frame against tampering by allowing a receiver to detect alterations to the frame. Added to this was also the inner (encrypted) Ethernet Header with one VLAN tag, and the outer Ethernet Header, inter-frame gap, and preamble as well.

Latency Added by Hardware Encryption

Encryption and integrity Checking are powerful but costly operations. Real-time sensitive applications, such as voice and video, require low latency. This test compared the latency between a Secure and a non-Secure Flow. The goal was to ensure that the encryption function would not introduce a significant amount of additional latency.

The test was performed by running the traffic stream via the non-Secure Flow, i.e. no MACsec activated. We measured 157.86 µs of latency. The other stream of traffic was forwarded through a Secure Flow, i.e. MACsec activated. We measured 158.22 µs of latency. We calculated the difference between both results as 0.36 µs (0.00036 ms). The streams of traffic consisted of a mix of different frame sizes as shown in Table 9.

The 0.36 µs added to the latency are negligible. We understand that this minimal value is due to the hardware-based design. The vendor expected to measure an added latency of less than 1 microsecond; the actual results met and exceeded the expectations.

Concurrent Secure Flows

The idea behind any edge device running a Carrier Ethernet EVPL service is to have at least one VLAN based point-to-point connection for each remote location configured in the core network. The customer can use several point-to-point connections to the same remote location, for instance, to separate different VPNs.

The FSP 150 is able to support several Secure Flows per port, each using different VLAN IDs. The goal of the test was to show the encryption device handling seven concurrent Secure Flows (quantity established by ADVA), all configured with the minimum key exchange interval and maximum key size allowed by

the device, with no frame loss. The parameters for the test are shown in Table 9.

Parameter	Value
Number of secure flows	7
Flow bandwidth	132 Mbit/s per flow
Key size	4096 bits
Key exchange interval	1 minute
Number of tags pushed	1 per flow

Table 9: Configuration Parameters for Concurrent Secure Flows Test

The FSP 150 was able to handle the seven concurrent Secure Flows. Each refreshed their Diffie-Hellman 4096 bits keys every minute. The total throughput of all seven flows was measured at 924 Mbit/s. There was no traffic loss as expected.

Test Results: Penetration Test

Penetration Testing, also known as "Pen-Testing", is the action of performing a simulated, previously authorized, attack on a network in order to evaluate its capacity to avoid an outsider to gain access and provide security recommendations. Normally an initial target and a goal are defined, in this case, the Edge device FSP 150 and finding vulnerabilities that could be exploited through its Management (MGMT) port, to make sure that an internal aggressor would not be able to gain access to it. These tests were performed by *dacoso* in a lab environment.

This section consisted of three test cases. First, a vulnerability scan was conducted on the FSP 150's MGMT port. Second, a vulnerability scan specific for web applications was performed on the device's MGMT port as well. Finally, a brute force attack for the administrator login password was attempted. The different software tools used for each test are shown in Table 10.

Test Tool	Software Used
Vulnerability scanner	Nessus 7.1.2 (#118) LINUX from TenableTM
Web vulnerability scanner	Acunetix version 12 (Build 12.0.180709159)
Brute force	THC hydra v8.6 (2017)

Table 10: Software Used for Penetration Tests

Vulnerability Scan on WAN Port

A vulnerability scan detects and classifies known weaknesses in a system to be used to gain access to it or break it. In this test, *dacoso* used the Nessus vulnerability scanner.

The software sweeps all ports and recognizes applications running in them, then it matches that information against its database to display all vulnerabilities found. These vulnerabilities are classified as one of four priorities: High, Medium, Low or informational. The expectation was that no high, medium or low vulnerabilities would be detected by the scan, meaning no open opportunities for an attacker.

After running the scan, the report showed only one high priority vulnerability for the SNMP protocol, indicating that the default "public" community string was used. This was caused due to the default configuration of the encryption device. The recommendation is to change the community string, which is normally the case in production devices configuration, and to use SNMPv3.

The result of this test was positive, as the only vulnerability found was due to the default configuration. No other high, medium or low severity vulnerabilities were detected meeting our expectations.

Web GUI Vulnerability Scan

ADVA's FSP 150 implements a web-based GUI for configuration and management. It is accessed via HTTPS through the device's management IP. In this case, a specialized tool for web vulnerability scanning, Acunetix, was used for an emulated attack. The goal, expectations and process of this test case were identical to the previous test case. The difference is that this vulnerability scan tool used is specialized in web vulnerabilities. As expected, no high, medium or low severity vulnerabilities were detected by the software.

Brute Force Attack

A brute force attack is a trial-and-error method used to obtain information such as, in this case, a user password. In this type of attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. The specific characters and the number of guesses are also specified to construct simpler or more complicated attempts. The goal was to try to login with the administrator password, and the expected result was to fail the attempt proving that the administrator password was not able to be obtained via a brute-force attack.

dacoso used the THC hydra tool in this case. It was set to use the full keyboard character set, this means the combinations for the password guesses utilized all the characters present on a keyboard, and to use a range from 0 to 8 characters.

The device detected failed login attempts and locked the device for an increasing period of time for each failed attempt. It did not block the attacker's IP automatically. Finally, it was not possible to obtain the administrator password via the brute force attack, as expected.

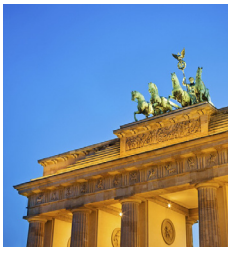
Conclusion

During the three days of the test campaign, EANTC verified the functionality of a range of security features. Additionally, a few performance aspects of ADVA's FSP 150 encryption edge device were evaluated.

Initially, we verified the principal operation of the encryption in different types of Carrier Ethernet services, frame format compliance with standards, Diffie-Hellman Key exchange, and VLAN tags in the clear for bypass. Then we proceeded to confirm that the bandwidth consumed by overhead and the latency added were acceptable. Finally, special features like OAM and Tamper Resistance were tested.

We confirm that the ConnectGuard™ end-to-end encryption effectively and efficiently protects all Ethernet traffic streams at line-rate at the interface level with negligible added latency. It secures traffic transparently over existing Ethernet networks, which makes it ideal for offering security as an additional feature to increase the value of established connectivity services.

About EANTC



EANTC (European Advanced Networking Test Center) is internationally recognized as one of the world's leading independent test centers for telecommunication technologies.

Based in Berlin, the company offers vendor-neutral consultancy and realistic, reproducible high-quality testing services since 1991. Customers include leading network equipment manufacturers, tier 1 service providers, large enterprises and governments worldwide. EANTC's Proof of Concept, acceptance tests and network audits cover established and next-generation fixed and mobile network technologies.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/
[v1.2 20181009]