Fidelis Cybersecurity

DATASHEET

Fidelis Decryption™

A High Performance TLS Visibility Appliance

Overview

Use of encryption is widespread with over 80% of internet traffic secured over https using TLS[1]. While encryption enables much-needed data privacy and integrity it also creates blind spots allowing malware and trojans to bypass security controls and provides an encrypted tunnel to bypass advanced counter threat measures put in place.

The Fidelis TLS Decryption appliance provides Man-in-the-Middle (MITM) decryption of TLS traffic to expose application protocol traffic and content to the enterprise security team for threat detection and response. Decrypting traffic increases ROI on existing security investments.

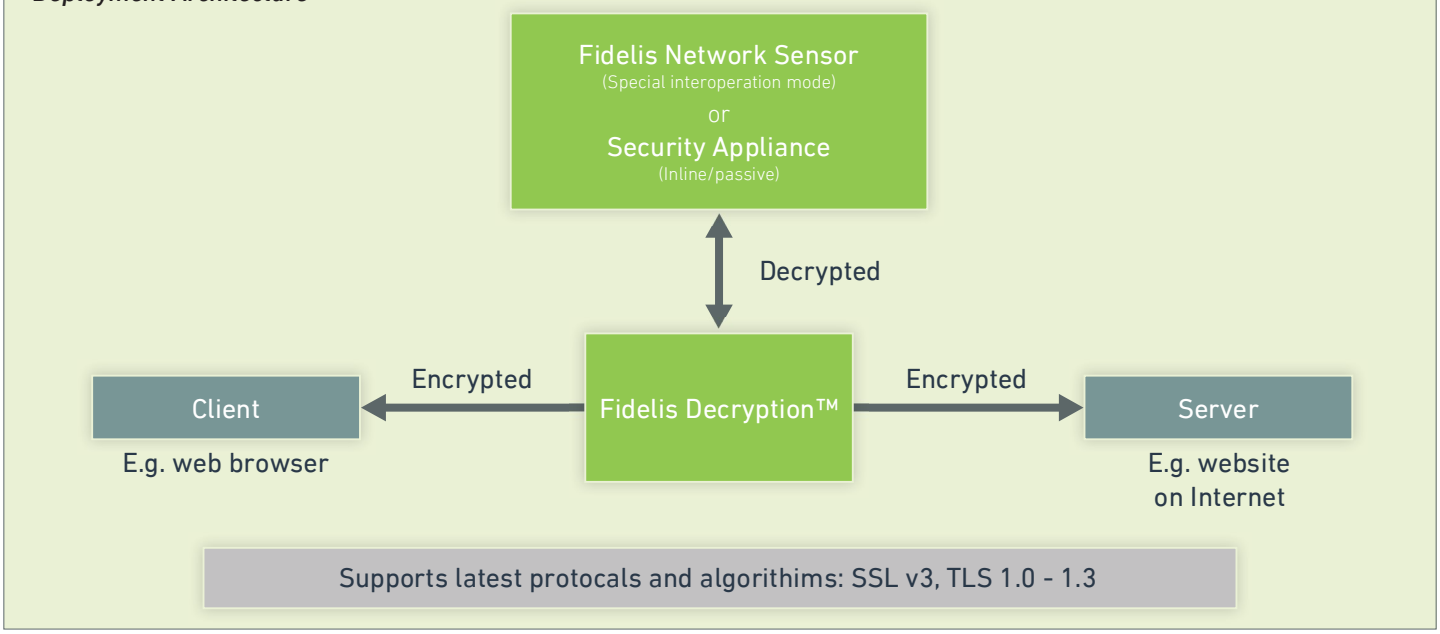
Fidelis Decryption is the only solution that, when deployed with the award-winning Fidelis Network®, can extract the TLS session metadata as well as the decrypted application protocol and content. This additional visibility extends to the Fidelis Elevate platform to detect and respond to even encrypted threats.

Key Benefits:

- Removes blind spots by decrypting traffic
- Increases ROI on existing security investments
- Improves performance of existing appliance by offloading decryption
- Comprehensive protocol and cipher support

[1] https://letsencrypt.org/stats/#percent-pageloads

Deployment Architecture



Features

Gain Visibility into Encrypted Traffic

The TLS decryption appliance enables application protocol and content analysis for encrypted traffic thereby removing any blind spots.

- Leverages high performance hardware accelerated TLS decryption and re-encryption
- Decrypts inbound and outbound encrypted traffic
- Server keys and certificates stored in disk encrypted using keys stored in FIPs certified TPM

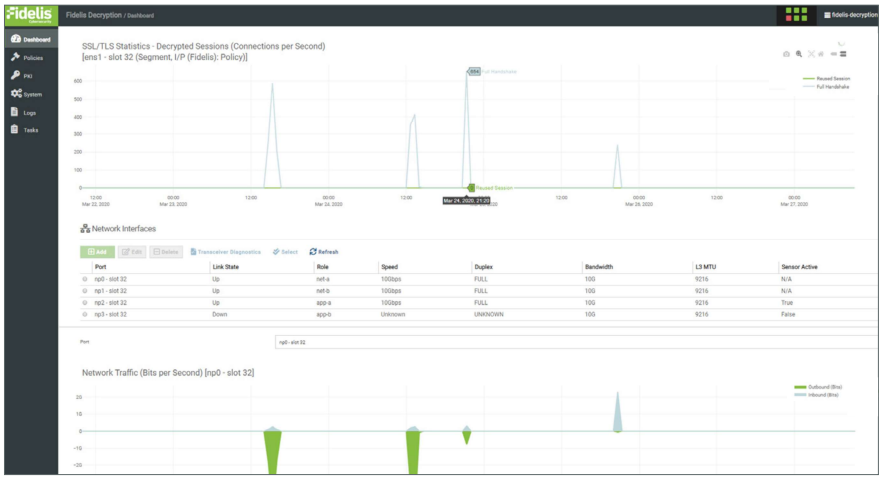
Comprehensive Protocol and Cipher Support

The Fidelis appliance has a comprehensive protocol and cipher support to ensure full coverage of encrypted traffic. These include:

- TLS 1.0, 1.1, 1.2 and 1.3
- SSLv3
- AES-GCM, AES-SHA (128/256-bit keys), ChaCha20-Poly1035 cipher suites
- RSA and ECDH public key mechanisms
- Line rate performance

The decryption/re-encryption is performed at line rate, which when forwarded to a security appliance facilitates malware and anomaly detection at near real time. The appliance comes in 5 Gbps and 25 Gbps line speeds to match different enterprise network needs.

Decryption Appliance Management Console



Flexible Deployment Modes

The decryption appliance can be deployed in active inline mode. Send decrypted traffic to one or more security appliances in passive mode for investigation. Traffic is automatically load balanced when sent to more than one appliance

- Bypass with external packet broker should a need arise (e.g. in the event of power failure)
- Certified to work with Niagara bypass switch (inline deployment mode)

Granular Policy and Security Compliance

A policy-based traffic steering technology provides flexible and granular control over decryption to meet data privacy and compliance requirements.

- URL database for category-based decryption (optional additional Subscription required)
- Block traffic by specifying drop (silently discard packets) and reject (actively close connection) rules.
- Bypass decryption based on SNI, IP range or other conditions including expired certificates

Easy to Use Management, Administration and Maintenance

The simplified management console is the one stop shop to configure, manage, monitor and maintain the decryption appliance

- Configure System and Policies: Setup the appliance, chose the mode right (inline/passive) for your enterprise. Select policies to determine traffic to be decrypted (e.g. healthcare or financial data are typically not decrypted) or certificates and keys to be employed in the process.
- Manage Certificates and Keys: Configure certificate authorities (internal/external), CRLs and SSH intercept keys. Generate self-signed CAs or import external CAs.
- Monitor: Dashboard to monitor system, appliance and traffic health.
- Maintain: Backup/Restore configurations. Restart services reboot appliance. Administer users.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

