THALES

Protecting Application Delivery without Network Security Blind Spots

Juan Asenjo, Thales e-Security
Don Laursen, F5 Networks

Objectives

- Describe how network security blind spots occur
- Outline threat that they represent to organization
- Define the best practices to protect against them
- Explain how to configure a trusted secure system

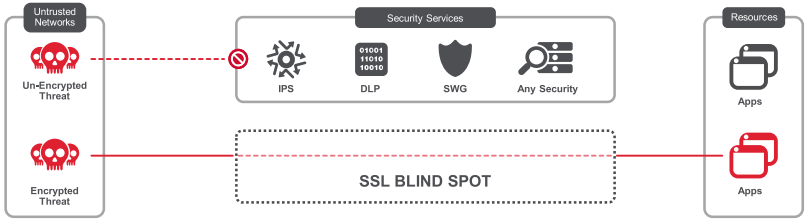
THALES

Introduction

SSL is growing and that presents a challenge for our customers

Most network architectures are obsolete. They are not built for SSL encryption. Enabling SSL on NG security products impacts performance **(80% degradation).**

Cyber criminals are growing **more sophisticated** and **evasive** in their **attacks**



Traditional network architectures are built for little or no encryption. Attackers are planting SSL-encrypted malware on compromised servers to evade network monitoring. Without security tools to inspect SSL traffic, attacker actions can go undetected.

THALES

Network Security Blind Spots

Hinders work of network security tools

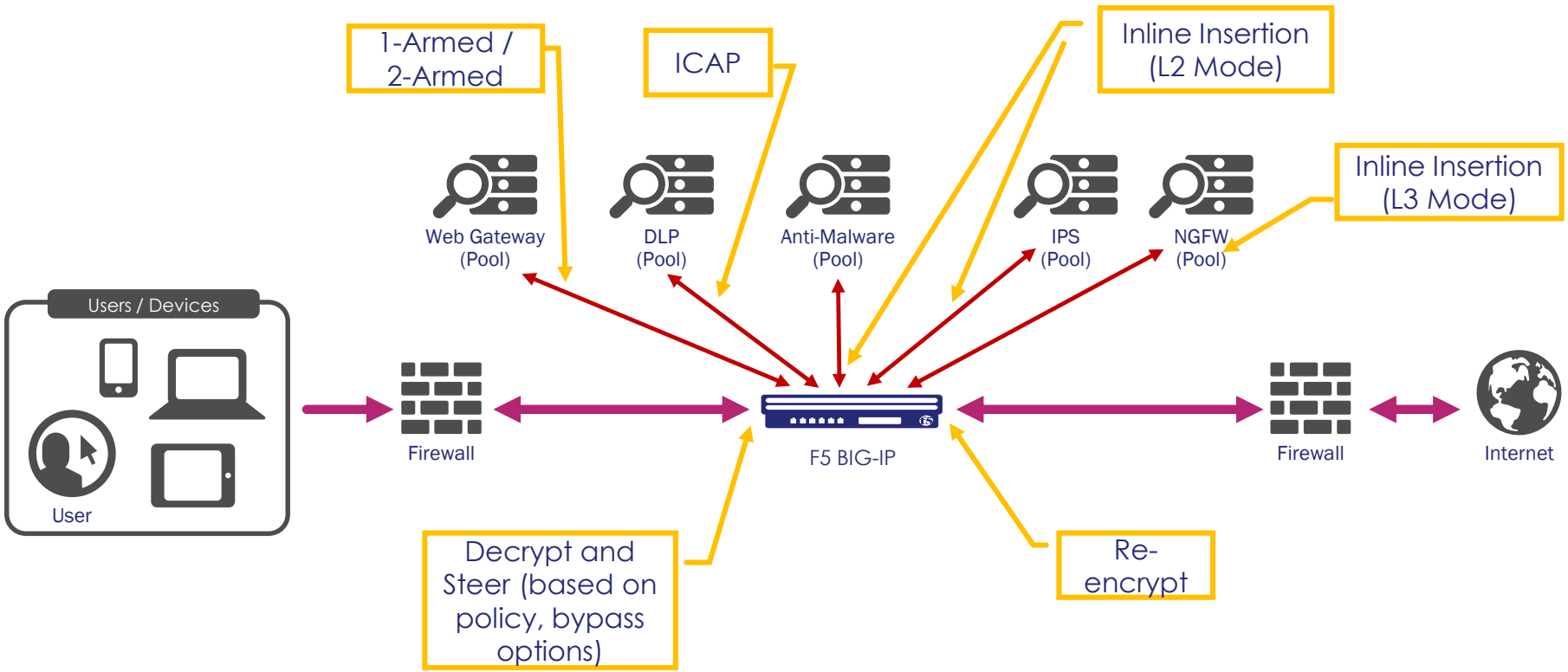
- Network health monitoring
- DLP, IDS, IPS
- Malware detection

Requires visibility into network traffic

- Security Dashboard (SIEMS)
- Policy and Privacy Enforcement
- Troubleshooting

THALES

Typical Security Stack



THALES

Significant Performance Impact on Existing Security Stack

Malware
uses encrypted channels to evade detection

Visibility
is reduced due to the growth of SSL usage

Performance
for decryption is a significant undertaking

79% Next-Gen Firewall
Performance Impact

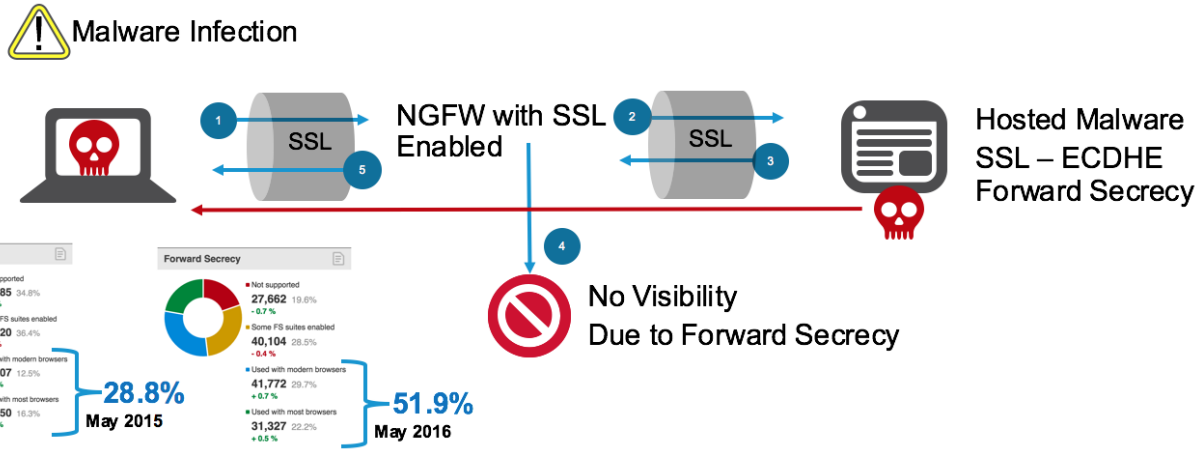
75% Next-Gen IPS
Performance Impact

100% Threat Defense
No SSL Support

Enabling SSL on a firewall, SWG or an IPS will reduce the overall performance of the appliance, often by more than 80%

THALES

Threat to your organization



In One Year: You've lost half of your visibility

THALES

Best Practices

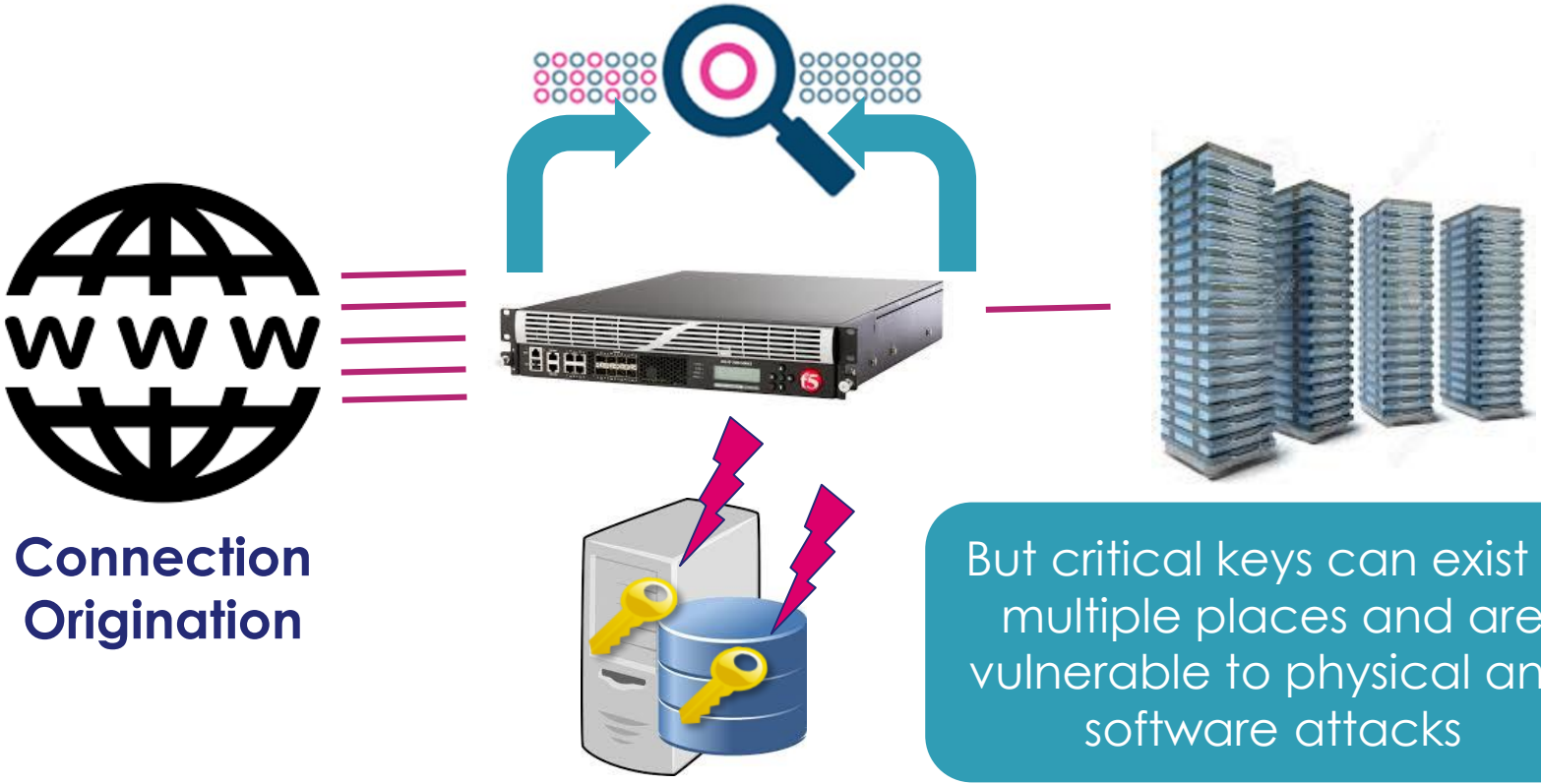
Protecting against encryption blind spots with BIG-IP

- Optimizes security stack through SSL offload
- Centralized decrypt/encrypt capability
- Support for latest ciphers and suites providing network traffic visibility
- Flexible deployment to support diverse environments

SSL/TLS and encrypt/decrypt feature use crypto keys

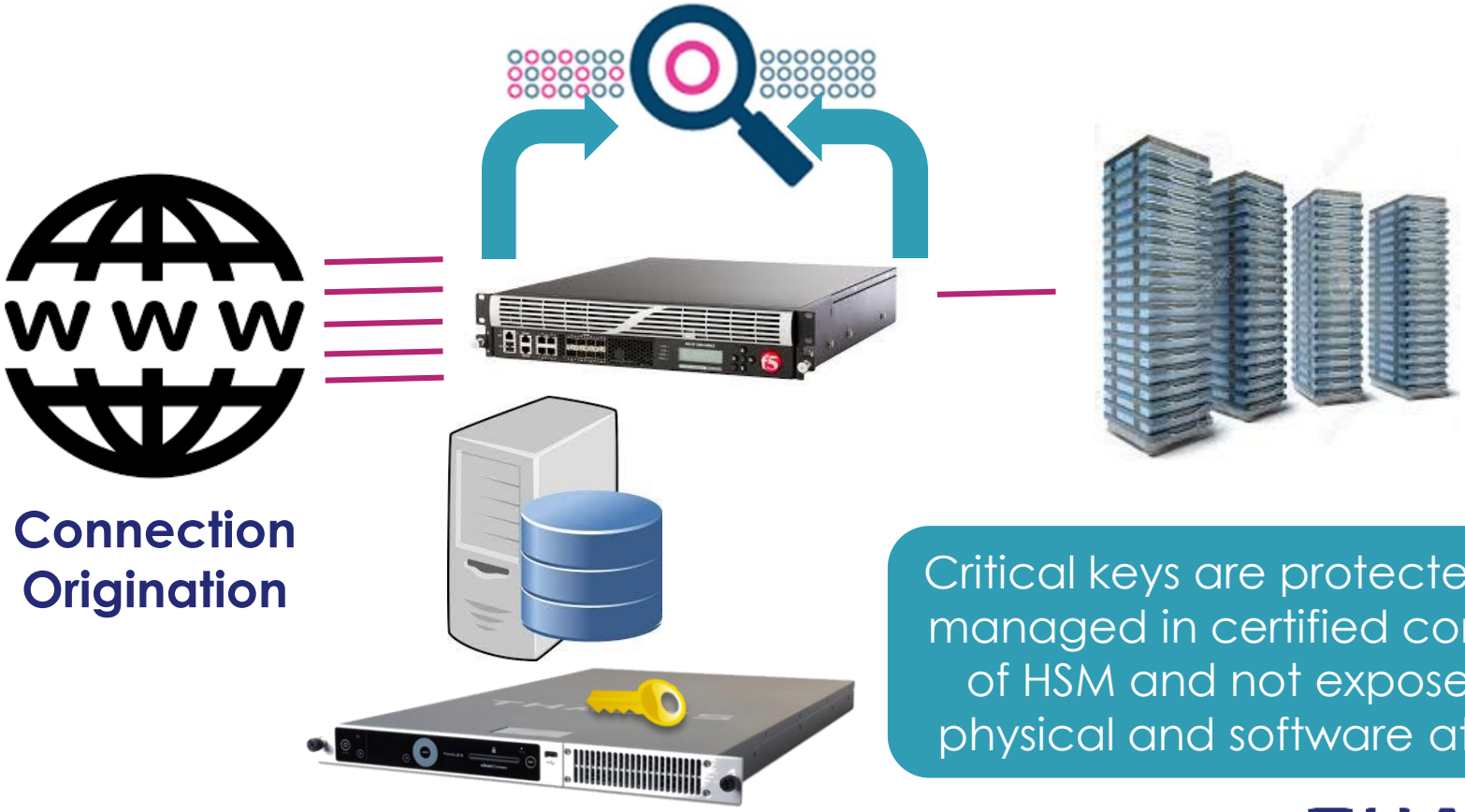
- Keys maintained in software can be exposed to threats
- Increasing number of crypto keys are harder to manage
- Customers require certified key protection for compliance

F5 BIG-IP Solution



THALES

F5 BIG-IP Solution with Thales nShield HSM



Critical keys are protected and managed in certified confined of HSM and not exposed to physical and software attacks

THALES

Protecting and Managing the Keys

External nShield HSM enables enhanced security

- Protects and manages critical SSL keys used by BIG-IP and encrypt/decrypt feature
- Isolate cryptography and keys in secure FIPS 140-2 Level 3 and Common Criteria EAL 4+ boundary
- Deliver lifecycle hardware key management, mitigates risks, and facilitates regulatory compliance

Value of HSM Integration

F5 BIG-IP

- Optimizes SSL traffic, response times, and customer experience
- Provide traffic visibility and prevent security blind spots

THALES

Enhances security protecting crypto keys in dedicated hardware
Provide dual controls facilitating auditing/regulatory compliance

INTEGRATION

- Delivers a proven solution with a strong and certified root of trust

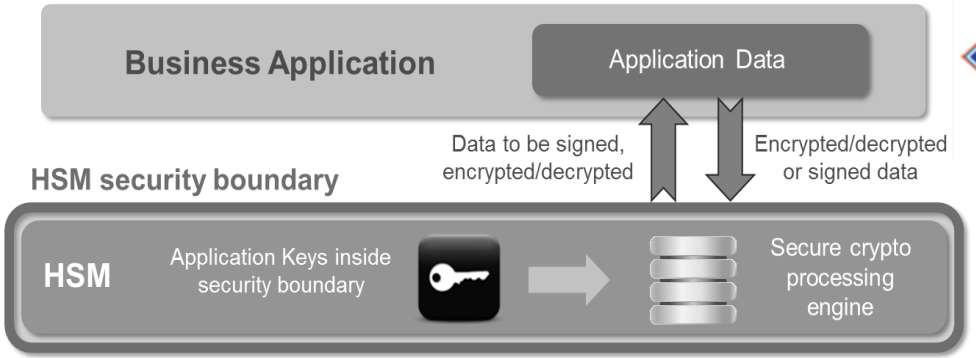
HSMs and Problems they Address

What are HSMs?

- Hardware Security Module
- Hardened, tamper-resistant devices isolated from host environment
- Alternative to software crypto libraries

What do HSMs do?

- Secure cryptographic operations
- Protect critical cryptographic keys
- Segregate administration and security domains and enforce policy over the use of keys

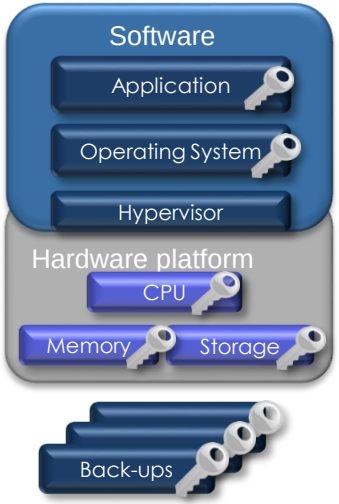


nShield HSMs are FIPS 140-2 Level 3 and Common Criteria EAL4+ certified

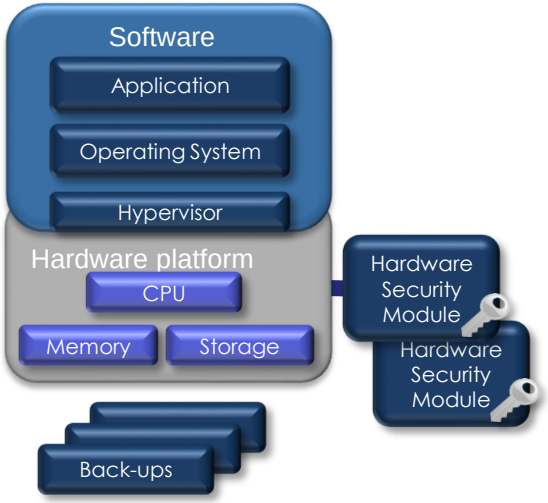
THALES

Enhanced Security for Application Delivery Controllers

- Software-only system
- Numerous copies of keys across system and backups



- Hardened security system
- Keys are segregated within isolated security environment



THALES

Root of Trust

- Provides FIPS 140-2 and Common Criteria certified security
- Isolates crypto keys and processes from host environment
- Enforces dual controls and protects from rogue super users
- Enhances security and ensures availability of critical keys
- Facilitates security compliance, auditing, and reporting

Why Thales e-Security?

- **Experience** – Leading global provider of data protection solutions for 40+ years
- **Leadership** – HSMs help secure more than 80% of the world's payment transactions and most valuable corporate and government information
- **Market focus** – Provides the best data protection solutions possible
- **Independently certified** – Products certified to FIPS standards
- **Expert advice** – Provides training and deployment assistance


Banking


Government


Utilities


High Tech


Mobile

THALES

Why F5?

- **Experience** – 7+ Years providing SSL offload and transformation
- **Leadership** – Gartner ADC Magic Quadrant Leader
- **Market focus** – Application Availability, Security and Performance
- **Certified** – Products certified for US Government and Global Markets
- **Partnerships** – Marketing leading partnerships and ecosystem

In Summary…

- Preventing network security blind spots should be priority
- ADCs increasingly taking on task/enabling traffic visibility
- Solution delivers better performance and robust root of trust

THALES

Time for Questions…

Thank you !

THALES