



Piercing the Veil: Trade Performance Analytics and Record Keeping in an Encrypted World

Matt Davey, MD Product Management
STAC London December 3rd 2024

The content provided in this presentation or in any other information, data or content (whether written or oral), notice or document supplied or otherwise made available to you or your agents and/or advisors in connection with this presentation contains confidential and proprietary information of Pico.

© Pico 2024. All rights reserved. The Pico symbols and word marks are among the registered and unregistered trademarks of Pico. All other trademarks are the property of their respective owners.

PICO Realtime Monitoring of Encrypted Electronic Trading Flow

Why now? Regulatory landscape driving encryption

The operational challenge

Maintaining visibility in an encrypted world

Case Studies

- Deutsche Boerse
 - NSE India
 - LSEG FXI
-

Summary:

Encryption is now part of the landscape, something to be aware of globally, necessary to plan for, and solutions exist.

PICO Cyber Security Regulatory Drivers for Trading

Electronic Trading designated critical infrastructure by regional and national frameworks, highlighting need for cyber security

- **EU NIS2 directive** (Network and Information Systems Directive) addresses cyber security of critical infrastructure including energy, healthcare, water, and financial markets. Fines of up to \$10M / 2% of revenue. **Adopted 2023, in force since September 2024**
- **German KRITIS Framework** – National NIS2 implementation, with 30,000 affected companies.
- **EU Digital Operational Resilience Act (DORA).** Requirements concerning the security of network and information systems supporting the business processes of financial entities. In force from **January 2025**.
- **Securities and Exchange Board of India (SEBI).** Cybersecurity & Cyber Resilience Framework (CSCRF) issued August 20, 2024.

New rules to boost cybersecurity of EU's critical entities and networks

PAGE CONTENTS

Top

Quote(s)

The Commission has adopted today the first implementing rules on cybersecurity of critical entities and networks under the Directive on measures for high common level of cybersecurity across the Union (NIS2 Directive). This implementing act details cybersecurity

India SEBI's New Cybersecurity and Cyber Resilience Framework: Data Protection Strategies for Regulated Entities

Financial Regulatory News

October 28, 2024

DORA takes effect: Digital resilience and cybersecurity in the EU

By [Renate Prinz](#) on October 29, 2024

Posted In [Dora](#), [EU](#)

on the rise, protecting is imperative. The Securities recently released Cybersecurity lays out a robust approach

HOME

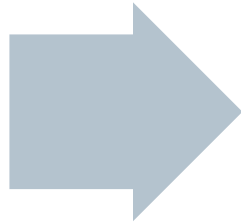
BREAKING NEWS

Bombay Stock Exchange Finally Encrypts All Trader Messages

PICO Operational Challenges of Encrypted Trading

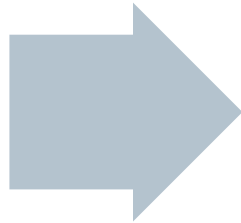
Use of Encryption in low-latency trading brings challenges for overhead, complexity and, crucially, monitoring

Overhead



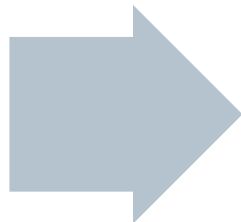
- Encryption necessarily adds latency overhead
- Main impact is on session establishment / handshake
- Hardware acceleration well supported for key ciphers such as AES

Complexity



- Encryption schemes may be standards-based or proprietary
- Proprietary schemes require significant development and test
- Project timelines may depend on vendor implementation

Monitoring and Analytics



- Passive network monitoring provides critical performance optimisation, record keeping, risk analytics. Essential for low-latency environments
- Encryption threatens to eliminate network monitoring, introducing operational blindspots and potential overhead of replacement solutions

PICO Maintaining Visibility - TLS

TLS (Transport Layer Security) Encryption



- Standards Based, widely deployed and supported
- Handshake supports negotiation of cipher suite, and optional mutual authentication of client and server
- Handshake relatively costly, agreeing *symmetric key* for subsequent encryption
- Low overhead after handshake. Modern CPUs and crypto libraries offer good hardware acceleration

Passive Decryption

- Load static private key on network monitoring tool
- Calculate session-key from TLS Handshake and private key
- ❌ Requires access to private key (rules out clients)
- ❌ Limited to RSA key exchange
- ❌ Does not support TLS v1.3 (RSA disallowed)

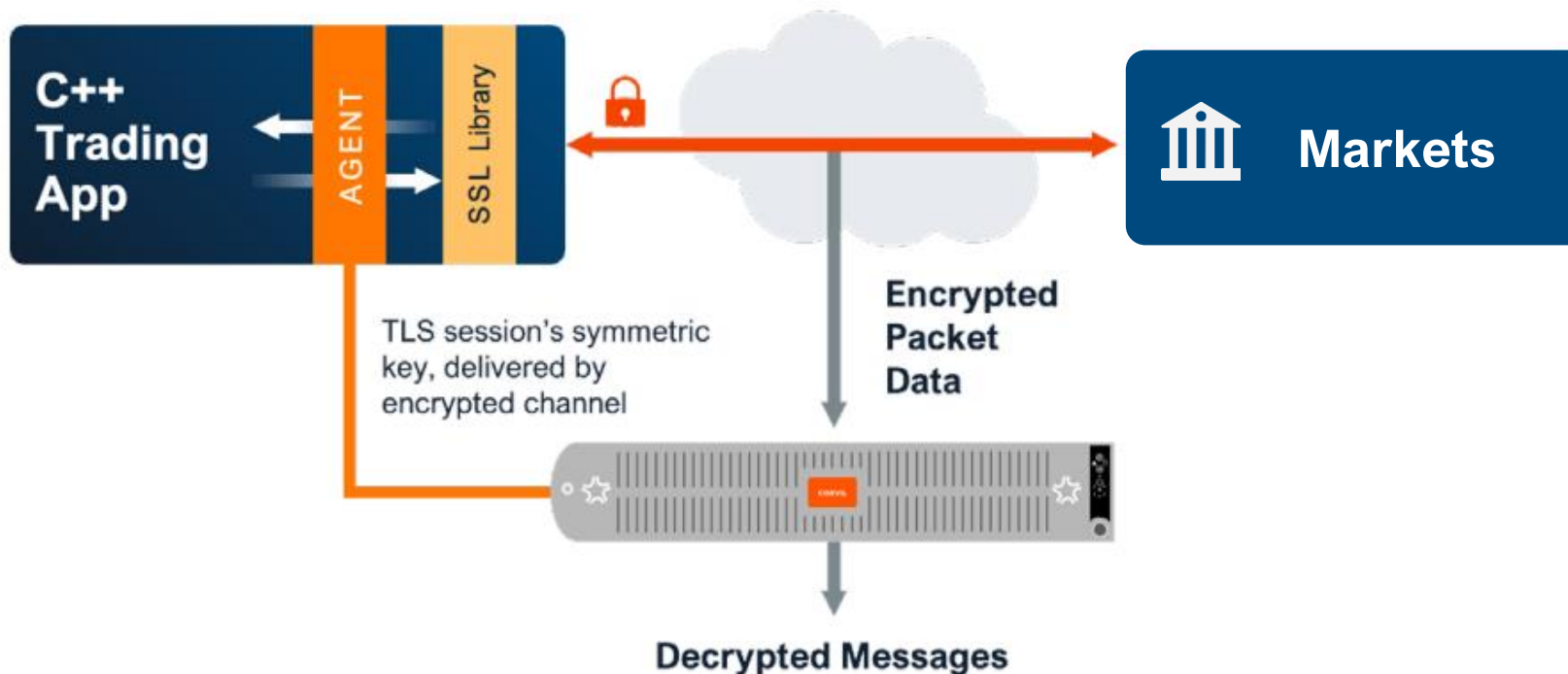
Active Decryption

- TLS Endpoint forwards negotiated session-key to network monitoring tool
- ❌ Requires active agent on TLS endpoint
- ✅ Supports all endpoints, no need for private keys
- ✅ Supports all TLS ciphers and perfect-forward secrecy
- ✅ Supports TLS v1.2 and v1.3

PICO Realtime Decryption with Corvil TLS Agent

Corvil TLS Agent: small software library that integrates into TLS endpoint application

- Extracts negotiated encryption/decryption key from application during TLS handshake
- Forwards keys in real-time via a secure channel to Corvil CNE
- Corvil decoder decrypts messages to provide full decode and visibility



Ease of Use

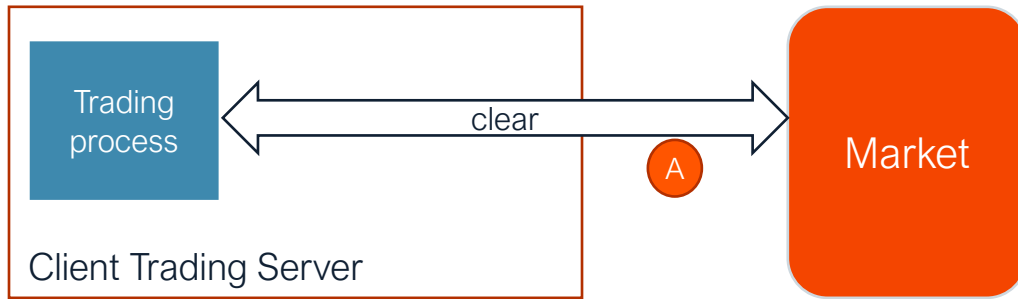
- No code changes or recompilation
- Supports standard Linux apps including stunnel and HAProxy
- Requires dynamic linking of openssl library
- Supports TLS 1.2, 1.3, C++/openssl, and Java

Secure

- **Server Authentication** – agent authenticates the Corvil appliance to avoid interception by malicious impersonator
- **Strong Encryption** – agent uses TLS with PFS to send key
- **In Memory** – decryption key not stored to disk

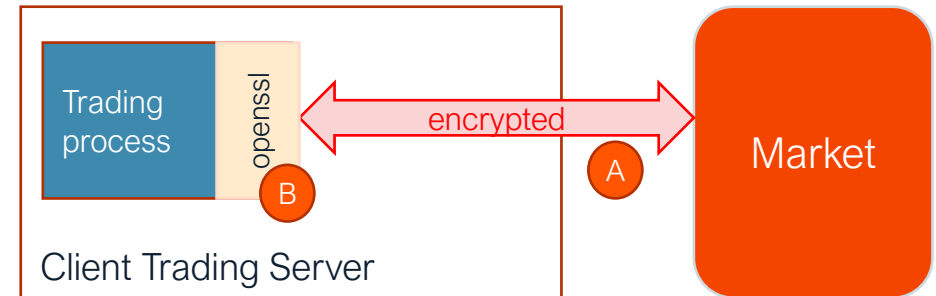
PICO TLS Agent Deployment Models and Decryption Options

1 – Unencrypted



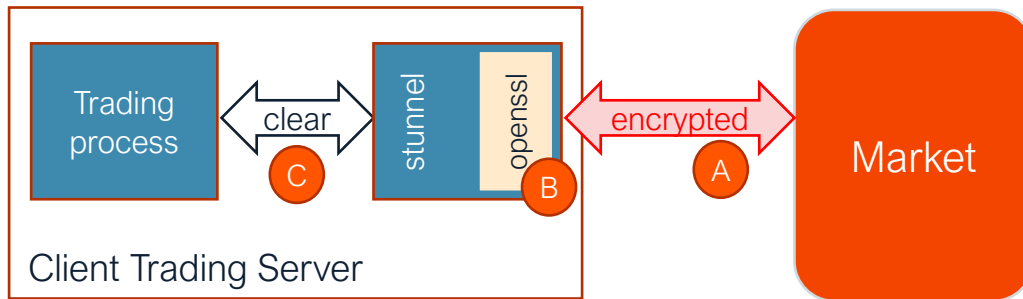
Tap network traffic at A

2 – Encryption handled by openssl library integrated into trading server



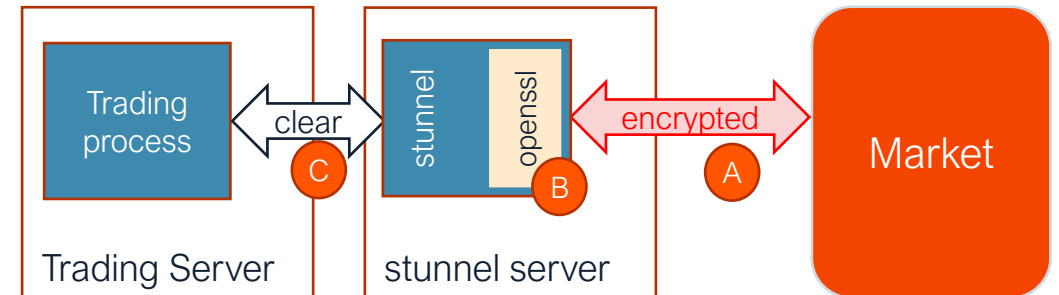
Tap network traffic at A, and integrate TLS Agent with trading server B

3.a – Encryption handled by stunnel process running on same server



“Sensor at C” and/or “TLS agent at B with tap at A”

3.b – Encryption handled by stunnel process running on different server



“Tap at C” and/or “TLS agent at B with tap at A”

PICO Alternatives to TLS Agent

TLS Agent not suitable for all situations:

- TLS Endpoint may not use openssl or Java
- Local policies may prohibit use of agents
- Proprietary non-TLS encryption protocol

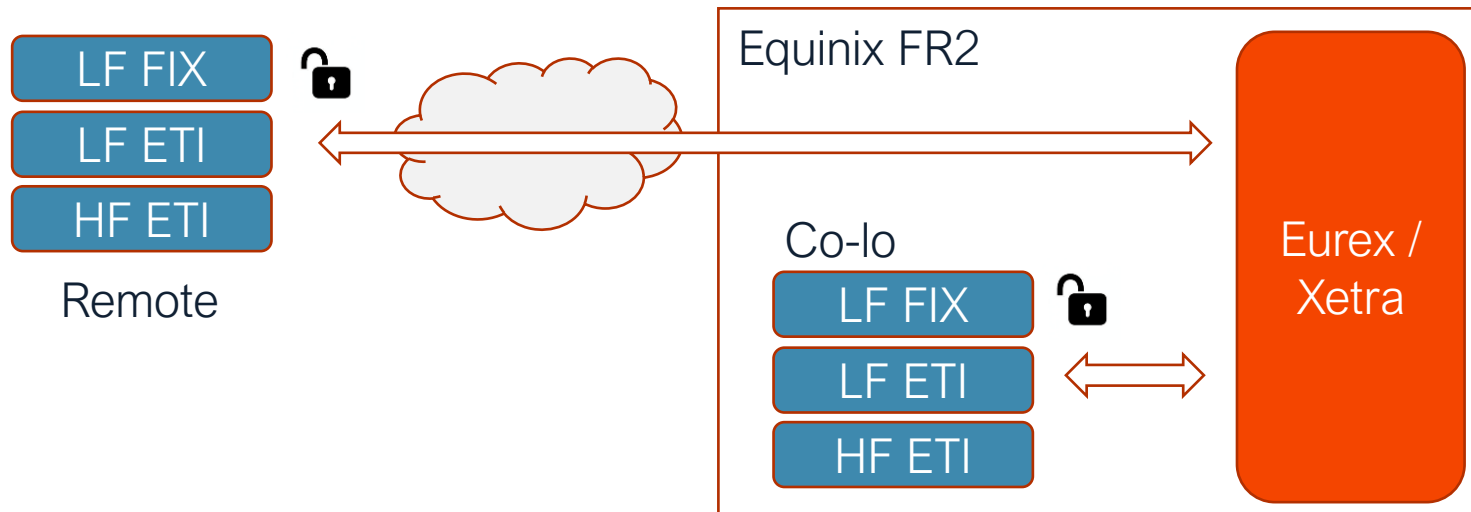
Solution: Network Monitoring with open Key-Forwarding API:

	STEP	TRADING SESSION ENDPOINT	NETWORK MONITORING SOLUTION
	Session Handshake	Establish connection, negotiate session encryption key	Passive monitoring of all communication. Detect new connection, create connection state, buffer all packets.
	Key Server Session	Open secure connection to network monitoring tool, optional authentication.	Authenticate client
	Key Forwarding	Forward negotiated session key, including session identifiers (IP src/dst, TCP ports). Shut down key server session.	Associate session key with connection state
	Trading Session	Encrypted trading session continues as normal, with no monitoring overhead	Passive Network monitoring, using session key for realtime decryption

PICO Case Study: Deutsche Boerse Eurex and Xetra

Prior to October 2023:

- Sessions can be co-lo in Equinix FR2 or remote
- Sessions are FIX or binary (ETI)
- ETI sessions either low-frequency or high-frequency
- 6 combinations – all available without need to encrypt

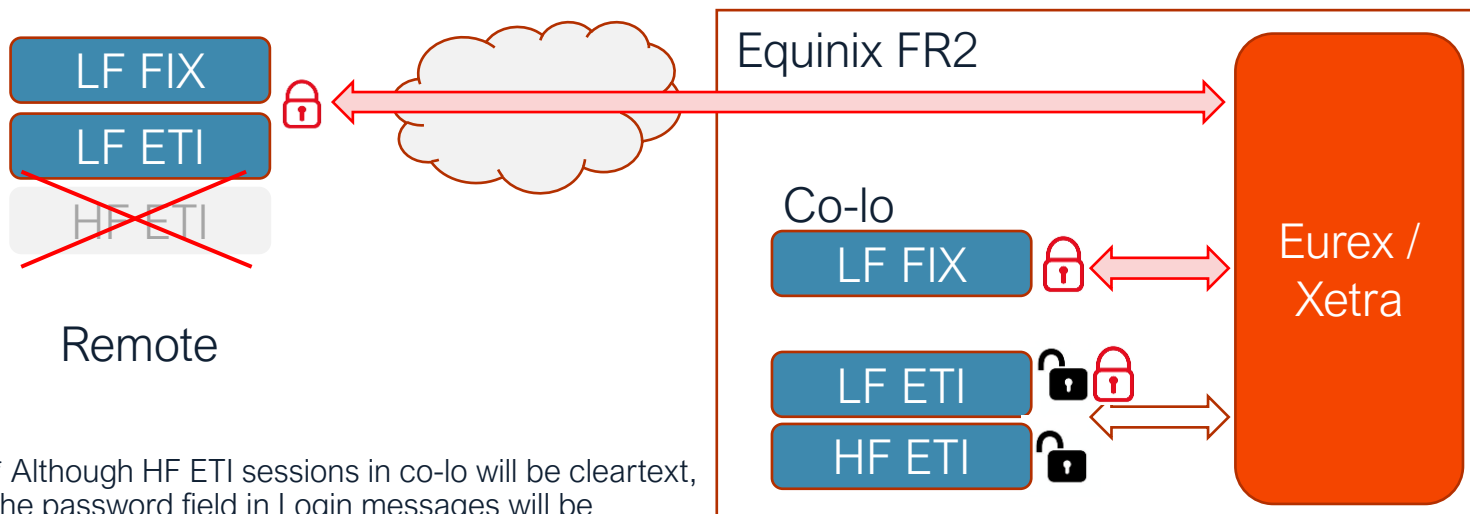


LF	versus	HF
Multi-partition gateway		Partition-specific (PS) gateways
Orders for any symbol		Orders only for GW's symbol range
Extra hop from gateway to matching Engine		Integrated PS GW and ME - <i>45us faster</i>
Lower message rate throttles		
		Less features (trade broadcast etc)

PICO Eurex and Xetra – Mandatory Encryption Over Public Links

Post October 2023:

- Remote HF ETI sessions are no longer allowed
- Remote sessions LF, FIX or ETI, must use TLS payload encryption
- Equinix FR2 – HF ETI sessions must use password encryption only, not TLS payload encryption
- Equinix FR2 – LF ETI sessions must use password encryption, **or** TLS payload encryption
- Equinix FR2 – LF FIX sessions must use TLS payload encryption



* Although HF ETI sessions in co-lo will be cleartext, the password field in Login messages will be encrypted

Corvil Analytics, with TLS Agent, can deliver full realtime performance analytics, tick-to-order and record keeping

PICO Case Study – NSE India Proprietary Encryption protocol

Client connects to Exchange Gateway Router (GR) using TLS 1.3 to request a login session

GR responds specifying which gateway to use, session ID, encryption key, and initialization vector

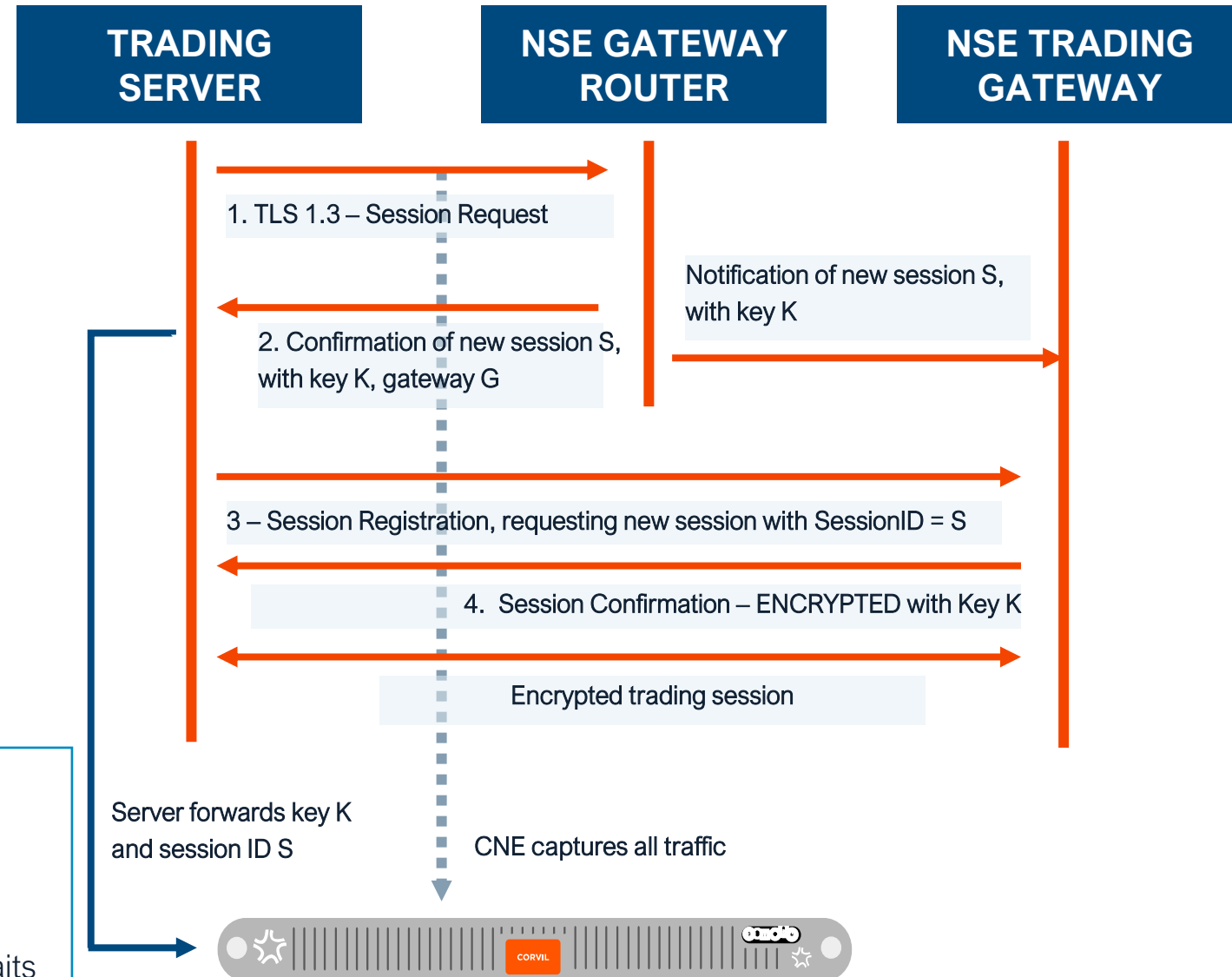
Client makes a new connection to the specified gateway and sends an unencrypted registration message containing the provided session ID

Gateway sends a response encrypted with the symmetric key and Initialization Vector

All subsequent messages from client and gateway are encrypted

Corvil solution:

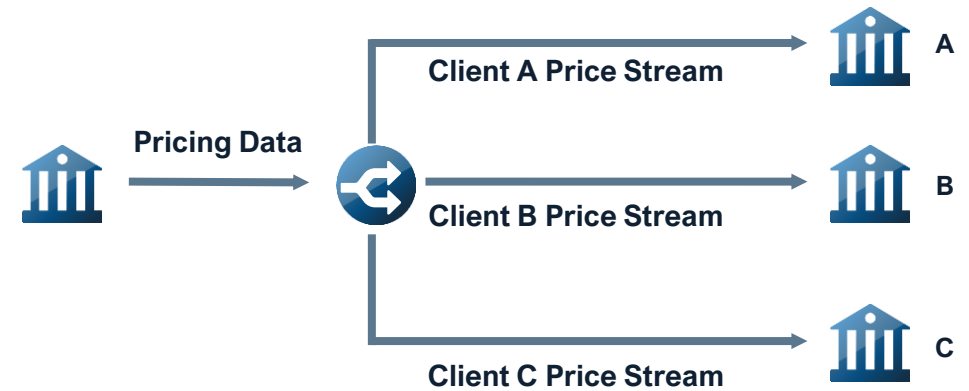
- CNE monitors all traffic, detecting new encrypted TLS connections
- Client uses key-forwarding API to deliver session ID and encryption key when provided by gateway router
- CNE stores the decryption info keyed by the session ID and waits for the client connection to the Gateway



PICO Case Study – LSEG FXI Market Data dissemination

FX Price Dissemination

- FXI streams prices to clients
- Prices are client-specific (counterparty risk, volume,...)
- Prices are calculated per currency pair, per client, per conflation interval
- **CHALLENGE:** how to ensure all clients receive prices simultaneously?



FXI Solution

- Prices are **encrypted** before sending
- Encryption is client-specific, and conflation period specific
- Decryption keys are sent simultaneously to all clients by Multicast
- **Prices visible simultaneously to all clients (within multicast delay variation)**

Corvil Support

- Buffer the encrypted data, remembering the received time
- When the key arrives, decrypt, and tag decoded prices with timestamps of the data packet and the key packet
- Use-Cases: tick-to-order / tick-to-quote / pricing engine latency performance; visibility of prices for analytics, record-keeping, and streaming.

PICO In Conclusion...

- Encryption for Electronic Trading is increasing, driven by regs.
- Passive Network Monitoring remains an essential Ops tool.
- Don't give up! Techniques are available to maintain visibility.
- Ensure your analytics vendor supports encrypted flow.

Any questions? We'd love to hear from you...

Thank You