

# THALES

## Hard Wired Security and Performance in a Virtual World

Joe Warren, Global Business Development Mgr.  
Network Security Products

Electronic Warfare Europe 2019

5/14/2019

Vitajte!  
**Welcome**

Karşılama! 歡迎 добро пожаловать

ברוך הבא | Bienvenido! Vítejte! Benvenuto!

Fogadtatás! Iarguralcome! ようこそ

Velkommen! Välkommen!

الدهسو الهأ! Willkommen! 환영

Bienvenue  
Tervetuloa! Bem vindo!

# Actual Quotes!

## Pre-WiFi, 802.11b circa 1995

My Desktop PC is wired.  
**Why would I need wireless connectivity at work?**



**A Wireless Network in my home?**  
That's the silliest thing I have ever heard in my life!

# Perspective: The Common Threads are “Change” and “Adapt”

As computing became more mobile, so did networking



As devices and demand for data “changed”,  
networks “adapted” yet security methods remain fairly stagnant

# More Ridiculous Quotes to Ponder

My Network is Wireless and my VPN is Private.  
**No one can see it so why should I worry?**

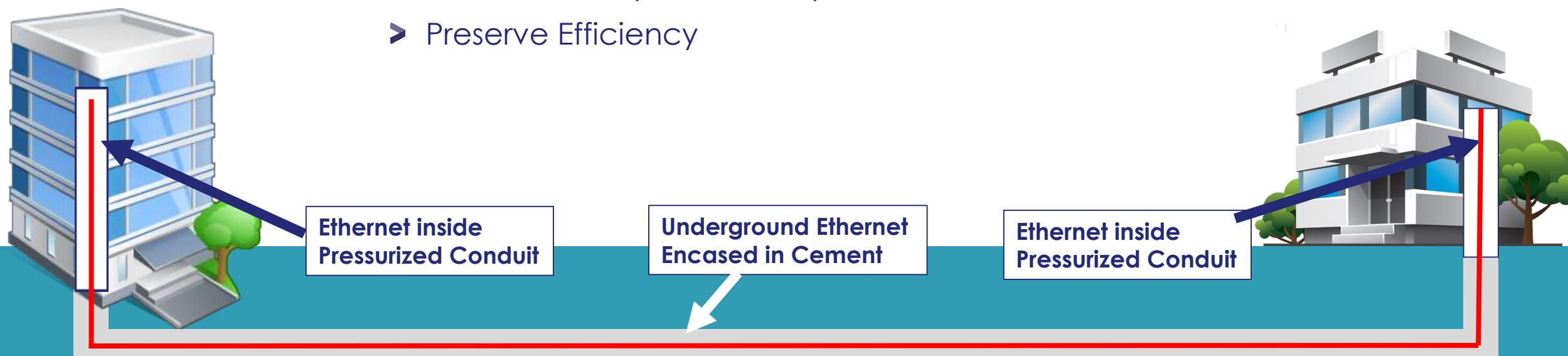


I Spend €70k/yr on a Leased Line.  
65% is used for Overhead, 35% for Data!  
**I'm Wasting €45k/year ... Isn't That Great?**

# Securing Data In Motion – The Old Days....

## Three Fundamental Components

- Encrypt the Data
- Send Encrypted Data Over Physically Secured Links (No Listeners)
- Preserve Efficiency



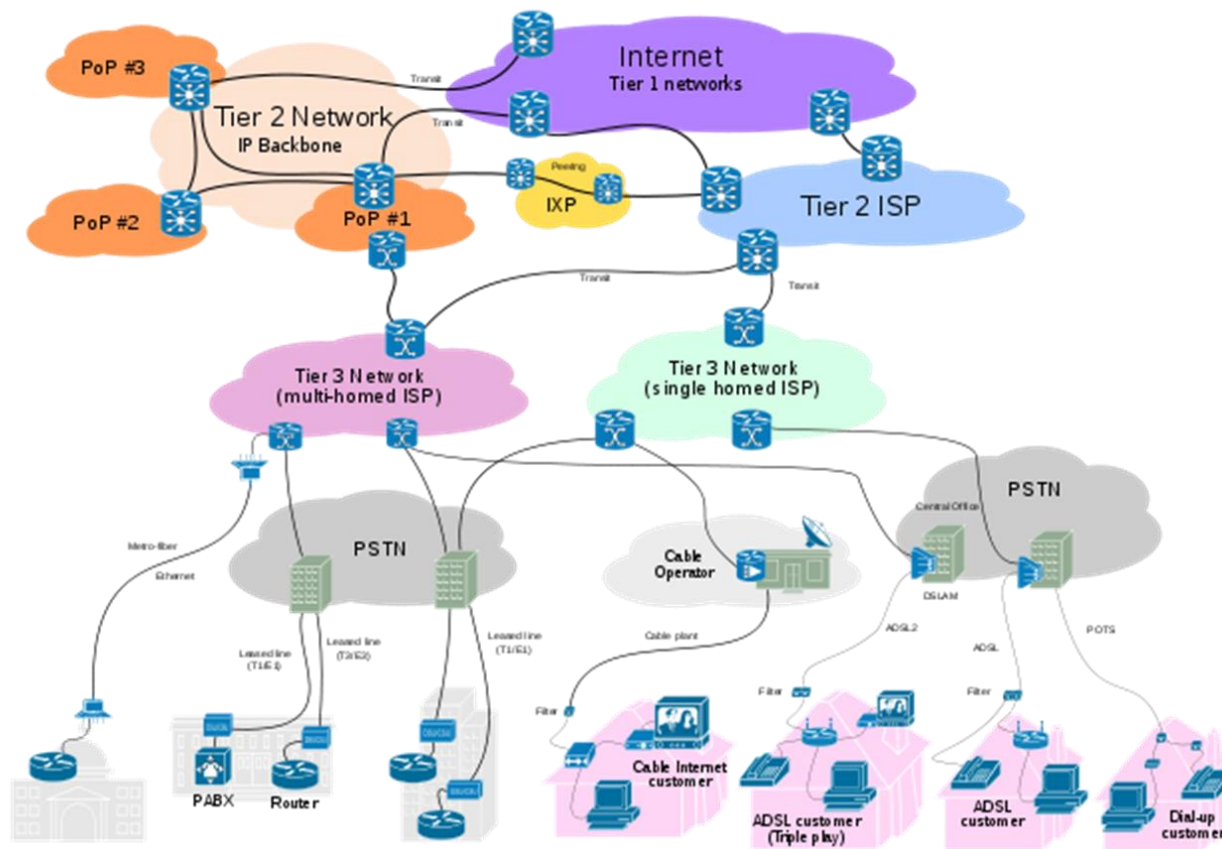
# Securing Data In Motion – Today....

## Networks are more complex

- Wired and Wireless Links
- Layer 2, Layer 3, Layer 4, etc.

## Yet Security Fundamentals Remain

- Encrypt the Data
- Send Encrypted Data Over ~~Physically~~ Secured Links: wired, virtual, and wireless (No Listeners)
- Move data quickly and efficiently



# Ingredients for Successful Data in Motion Security

- ✓ Data encryption



- ✓ Little to No Impact on Network Performance (Efficiency)



- ✓ Complete Connection Obfuscation (No Eyes on Data)



# Data Encryption – to each his own

■ Data Encryption is a matter of regulation and/or personal choice

■ Global Standardization is Neither Desirable Nor Practical

- GOST, AES, RAS, HAIPPE, it doesn't matter
- Protection of Data is best implemented and regulated on its own
- However, hardened hardware encryption ensures best performance and data security

■ If Encryption is the Commodity, then Efficiency and Transport Security are the Key Differentiators

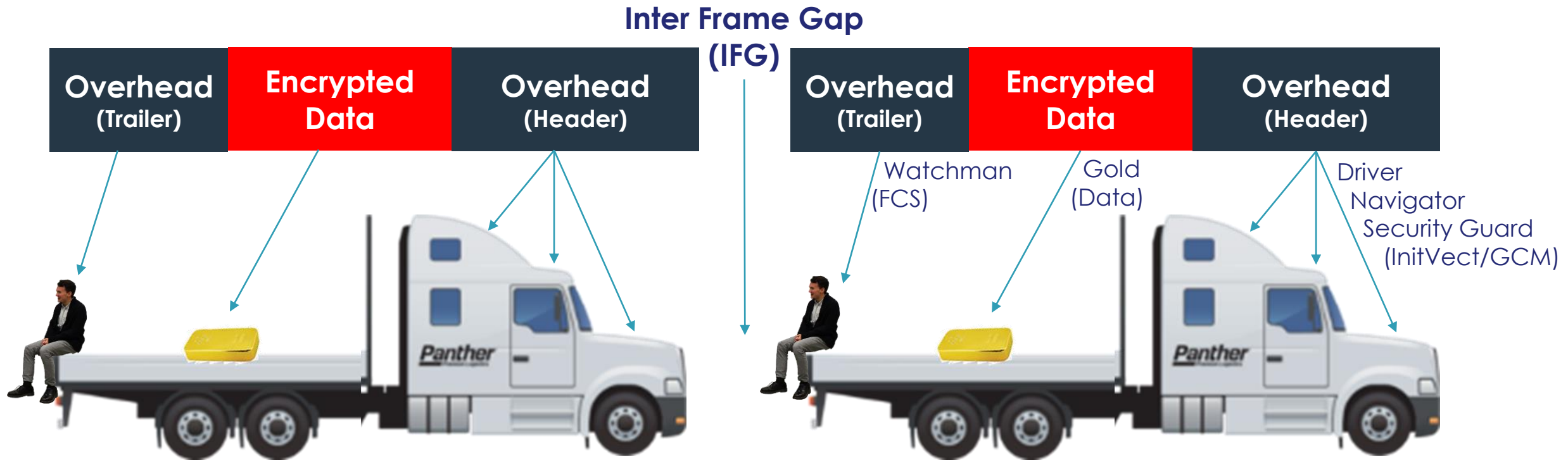




# Efficiency...If Encrypted Data Packets were Bars of Gold....

## How Do We Typically Transport Our Gold?

- Each packet is secured....one at a time
- Overhead required for each and every frame



# Compound Problem – Different Data Types

Depending on the Data Type, The Ratio of Overhead to Data can be exponential

Average Size Data Packets



Smaller Size Data Packets (VoIP)

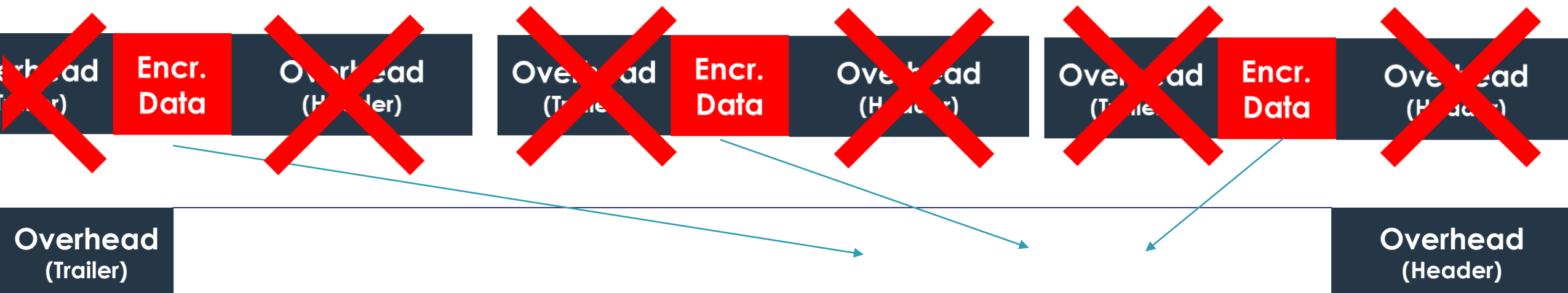


# Efficiency



# Adjusting the MTU Size at the Encryption Point

- Create a Large “Container” and Insert Encrypted Data
- Reduce Overhead from Individual Packets
- Gain Efficiency Through Economies of Scale
  - Same Levels of Security for Data Encryption
  - Same Levels of Security on the Transport of Encrypted Data
  - Larger Packets Reduces Ratio of Overhead to Data



Adjusted MTU Size – Filling the Large Container

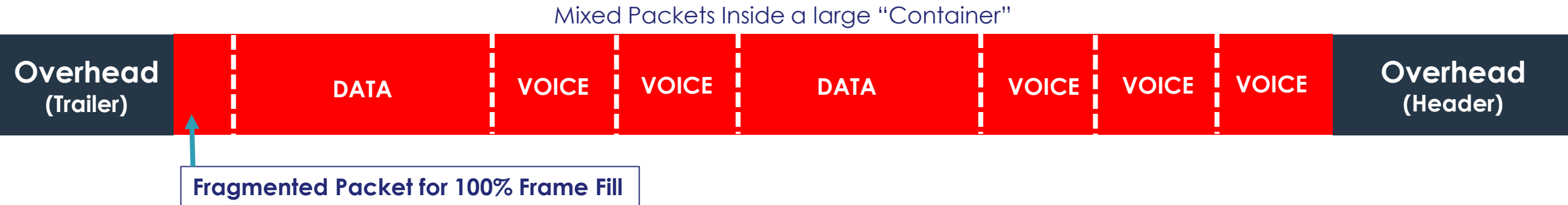
# Efficiency Through Economies of Scale

## Up to 98% Network Efficiency Can Be Obtained

➤ Reduction in Overhead

## No Reductions in Data Security or Transport Security

➤ Same Great Security, Just Fewer Packets to Secure



# The Must Haves



Data encryption



Little to No Impact on Network Performance (Efficiency)



Complete Connection Obfuscation (No Listeners)



# Leveraging Efficiency Mode for Obfuscation

## COMPLETELY FILLED WITH REAL DATA

Appears as one large encrypted data packet



## PARTIALLY FILLED WITH REAL DATA, REAL DATA vs. RANDOM DATA vs. PADDING

Appears as one large encrypted data packet



## NO REAL DATA – ALL RANDOM DATA

Appears as one large encrypted data packet



**ALL THREE APPEAR AS ONE LARGE, ENCRYPTED PACKET!**  
– FOR THE LISTENER –

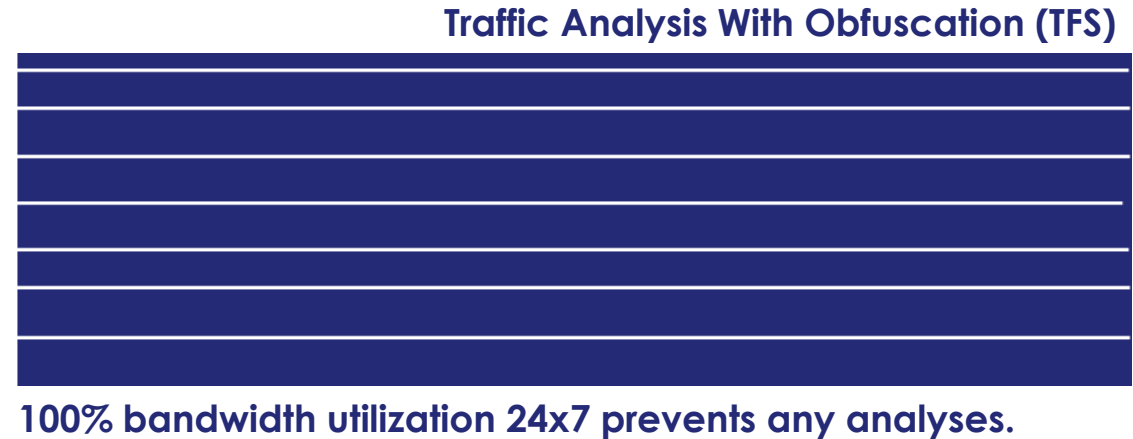
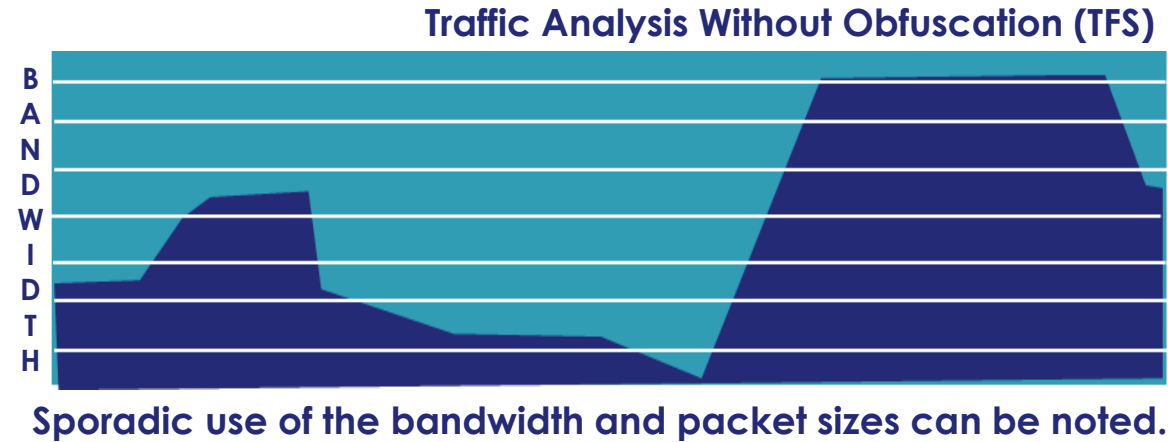
# What Does The Listener See?

## Without Data Obfuscation a Listener CAN

- Determine packet sizes
- Determine data types (backups vs. voice)
- Tell when utilization occurs (peak vs. downtime)
- Possibly determine classified vs. unclassified data
- Potentially determine location of assets

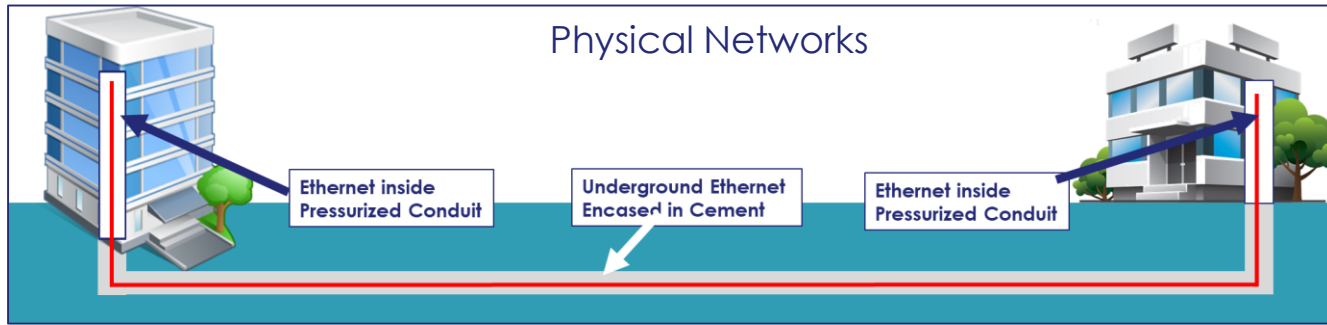
## With Data Obfuscation a Listener

- Cannot determine packet sizes or data types
- Cannot distinguish between real and random data
- Cannot determine utilization times
- Cannot determine classified vs. unclassified data





# Just Like The Good Old Days....



Then

and

Now



Familiar Data Encryption



Complete Obfuscation



Superior Performance

# More Quotes!

**Now I Can Fully Secure Wired, Wireless, and Virtual Networks Without Sacrificing Performance!  
Who Knew?**



**I Reduced Overhead by 75% and I Don't Need To Purchase More Capacity.....I Saved €70,000!  
Who Knew?**

# Summary

- Data Security and Transport Security are separate yet complementary
- As networks and transport techniques evolve, transport security methods must evolve as well
- NEVER sacrifice security for performance or performance for security
- The techniques abbreviated in this presentation preserve the fundamental requirements of Data Security, Transport Security, and Efficiency over hard-wired and virtual infrastructures

# THALES

**Joe Warren**

**Business Development, Network Security**

**HIGH SPEED ENCRYPTION (HSE) Products**

**[Joe.Warren@Thalesecurity.com](mailto:Joe.Warren@Thalesecurity.com)**

**@JoeWarren99**

**+1-321-704-6494**

# Thank you

Gracias مكمل اركش

धन्यवाद Merci

Danke 謝謝

ありがとうございました