
SEGURINFO 2014
XXXV Congreso y Feria Iberoamericana de Seguridad de la Información
EL NUEVO CIFRADO

SEGURINFO 2014

XXXV Congreso y Feria Iberoamericana de Seguridad de la Información

Presentada por:

BAGGIERI, Ariel

Business Development Manager, NextVision

NV NextVision
IT + SEGURIDAD

Aclaración:

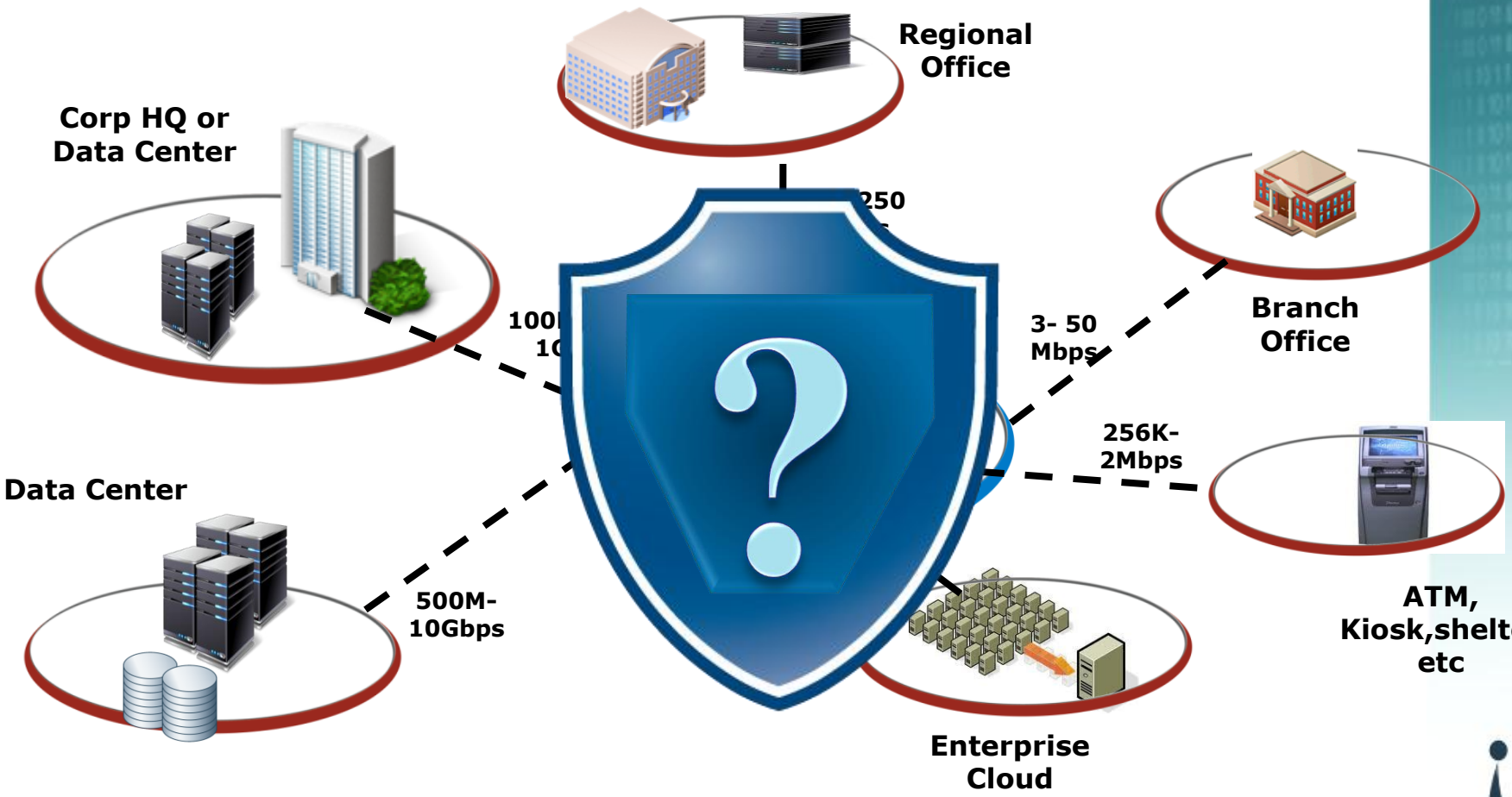
USUARIA

Agenda

- Escenarios
- Problemática de cifrado
- Tecnología
- Casos Prácticos

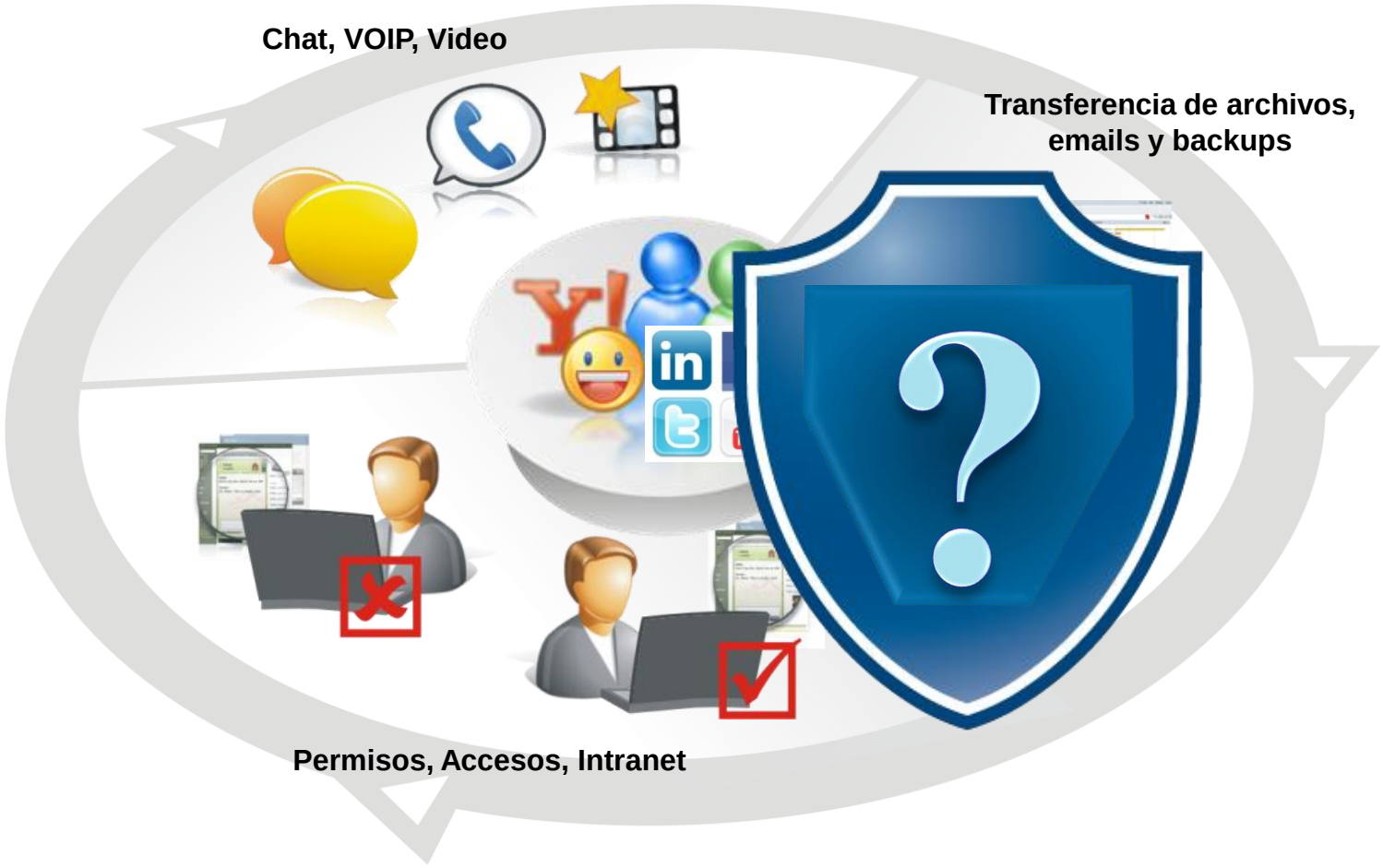
USUARIA

Redes heterogéneas más complejas



USUARIA

Más servicios corporativos

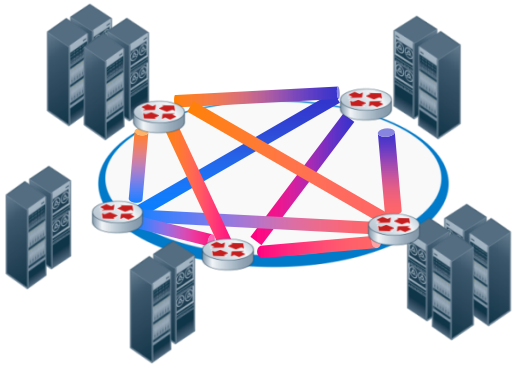


USUARIA

Tecnología: Cifrado de Grupo

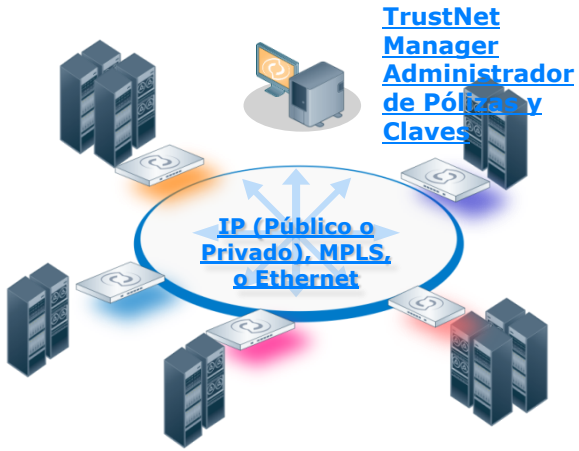
IPSec Tradicional

- **Punto a Punto- Basado en túneles**
- **Difícil de configurar y administrar**
- **Disminuye la velocidad de la red**



Cifrado de Grupo

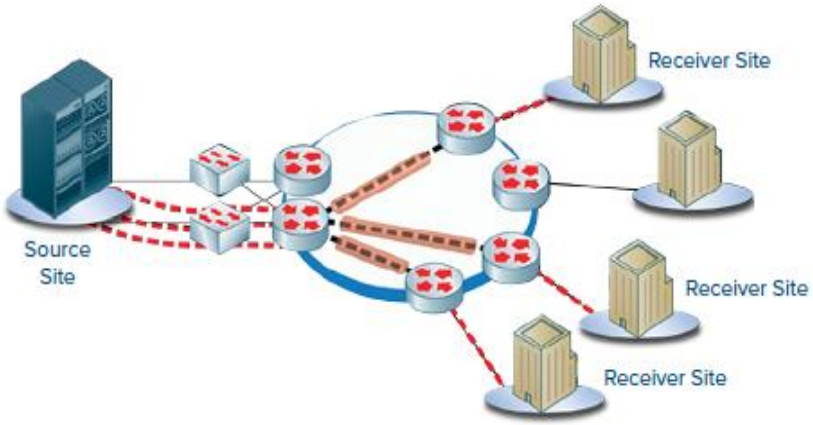
- **No utiliza túneles !**
- **Fácil de configurar y administrar**
- **Trabaja a la velocidad de la línea**

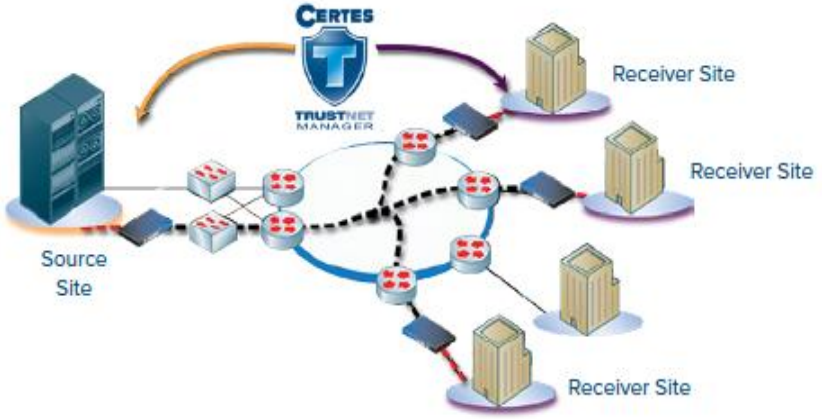


USUARIA

Tecnología: Cifrado de Grupo

IPSec Tradicional	Cifrado de Grupo
• No proveen servicios a la Capa 4	Preserva los servicios de la Capa 4 Compatible con VoiP y Video
• No tiene soporte para ambientes con doble proveedor	Soporta ambientes con doble proveedor
• Las aplicaciones multicast pierden la conexión o bajan su velocidad	Compatible con aplicaciones multicast





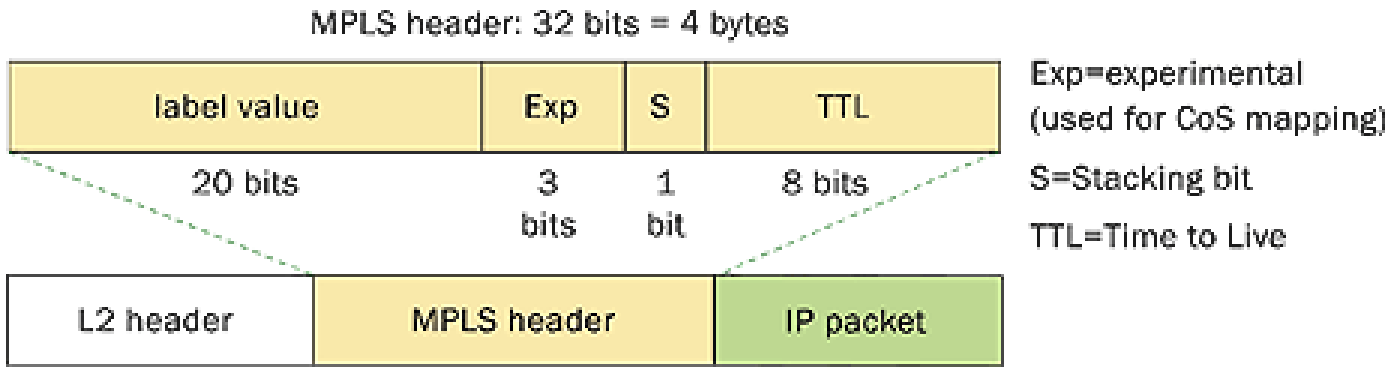
Tecnología: MPLS

Es una tecnología de envío de paquetes

- **El envío del paquete se basa en etiquetas**
- **Un paquete puede tener múltiples etiquetas**

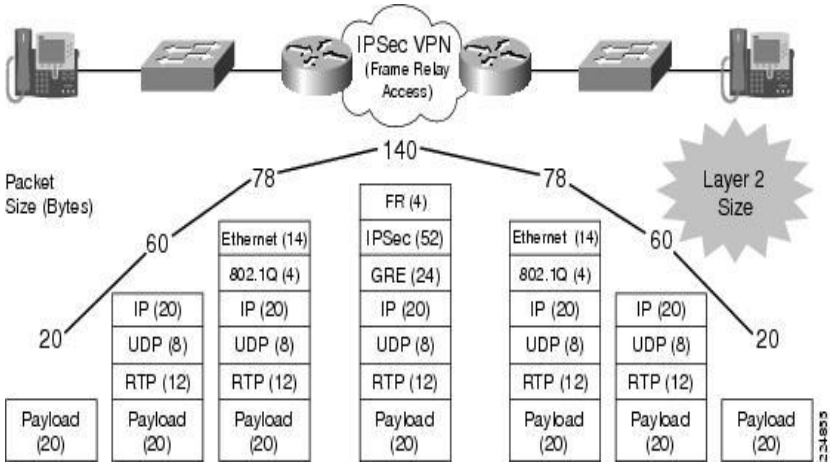
MPLS no provee

- **Protección contra errores en configuración**
- **Protección contra ataques a la red.**
- **Confidencialidad, Autenticación o integridad de la data.**
- **Seguridad al cliente (cifrado)**



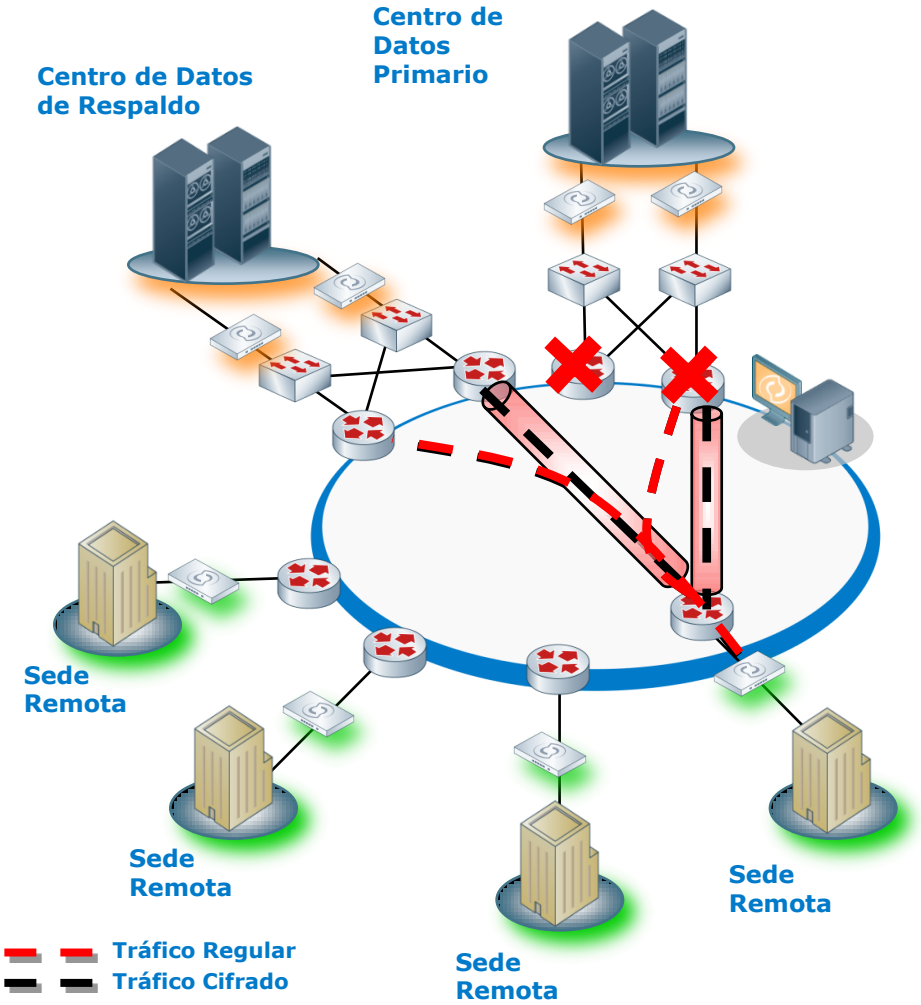
USUARIA

Performance y Eficiencia



USUARIA

Cifrado transparente para la red



- **Encabezados en texto claro**

⇨ **Balanceo de carga transparente**

- **Falla**

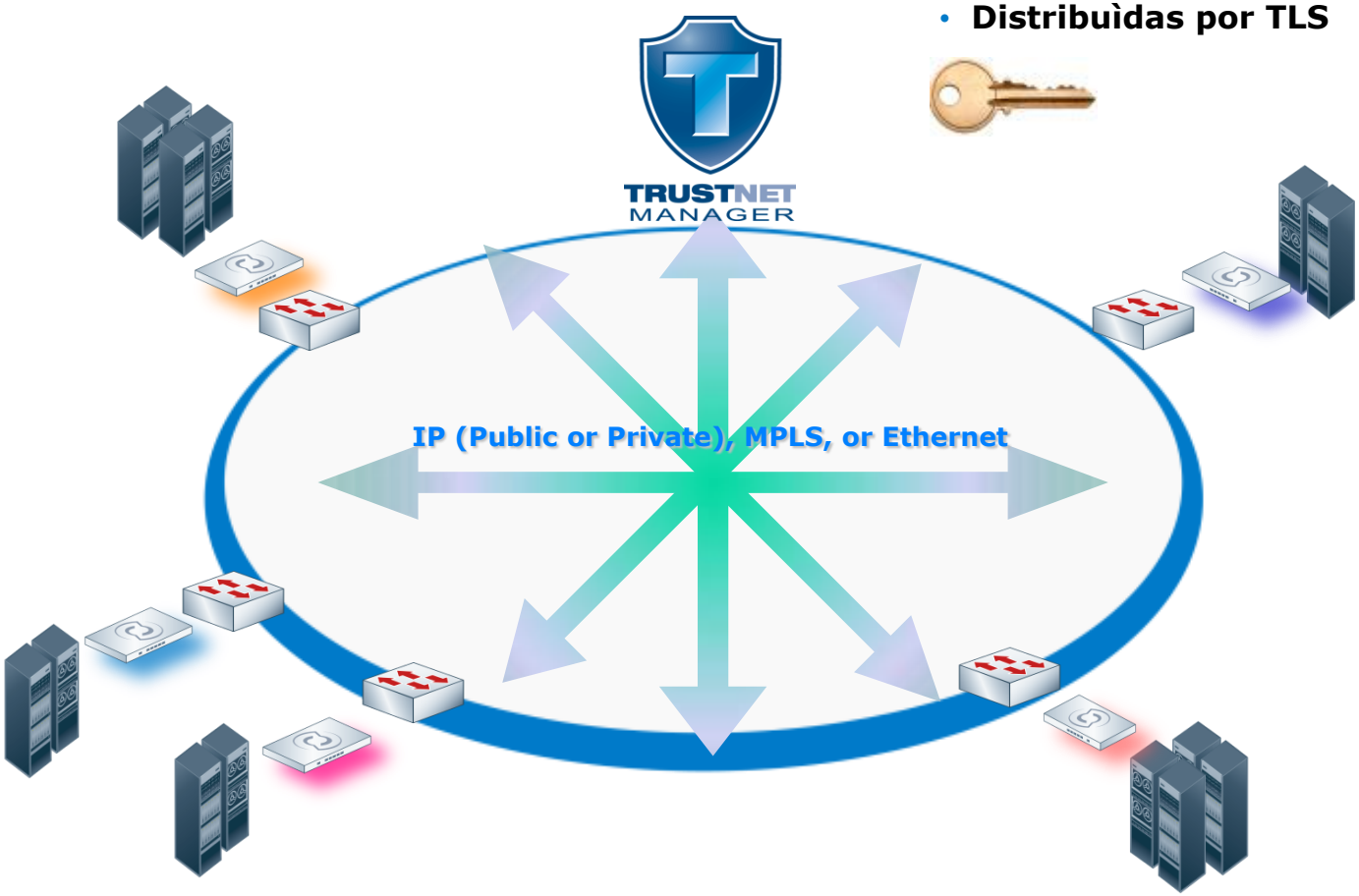
⇨ **Tráfico es re dirigido**

- **Clave actualizada y correcta**

USUARIA

Llaves simétricas con gestión centralizada

- Definición de las políticas de grupo
- Generación de llaves centralizada
- Distribuìdas por TLS



USUARIA

Cifrado de nueva generación

Define políticas basadas en la red o en las aplicaciones

Topologías
- **Mesh**
- **Hub and Spoke**
- **Multicast**
- **Híbridos**

Aplicaciones
- **Voz**
- **Video**
- **Control de Data**
- **FTP u otros protocolos**

Crea las claves necesarias para cifrar

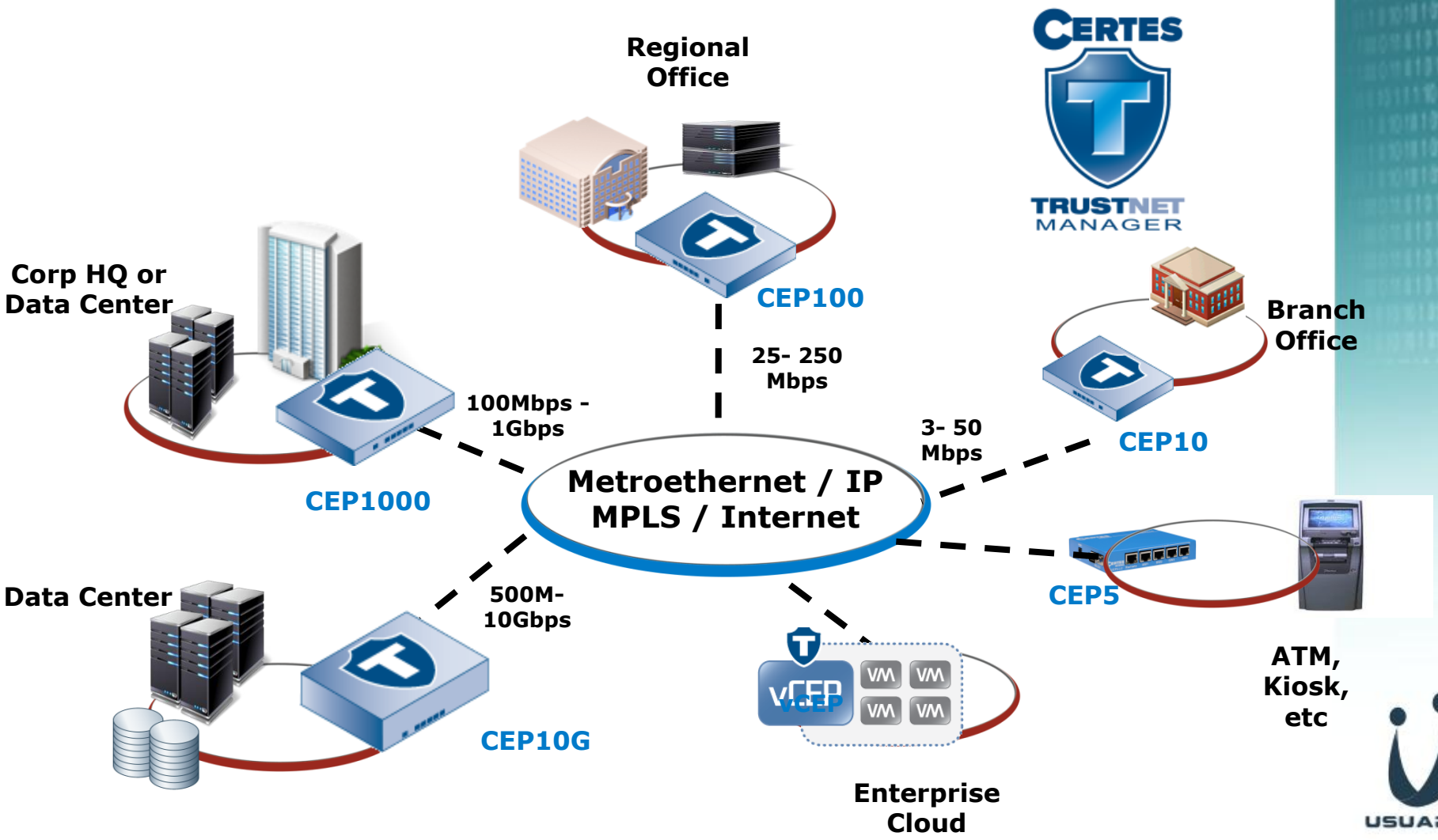
Utiliza los protocolos de seguridad estándar
- **AES 256**
- **Autenticación de paquetes ***
- **SHA-256**

No tiene que crear túneles

Preserva el enrutamiento original y los protocolos
- **Capa 2 – Cifrado por VLAN**
- **Capa 3 – Preserva las rutas de IP y las subredes**
- **Capa 4 – Mantiene el manejo de tráfico y Netflow/Jflow al cifrar**

USUARIA

Solución de cifrado



Solución de cifrado

- **Gestión de encripción (L2, L3, L4) y autenticación.**
- **Roles para distintos perfiles**
- **Generación segura de claves, distribución y actualización periódica.**

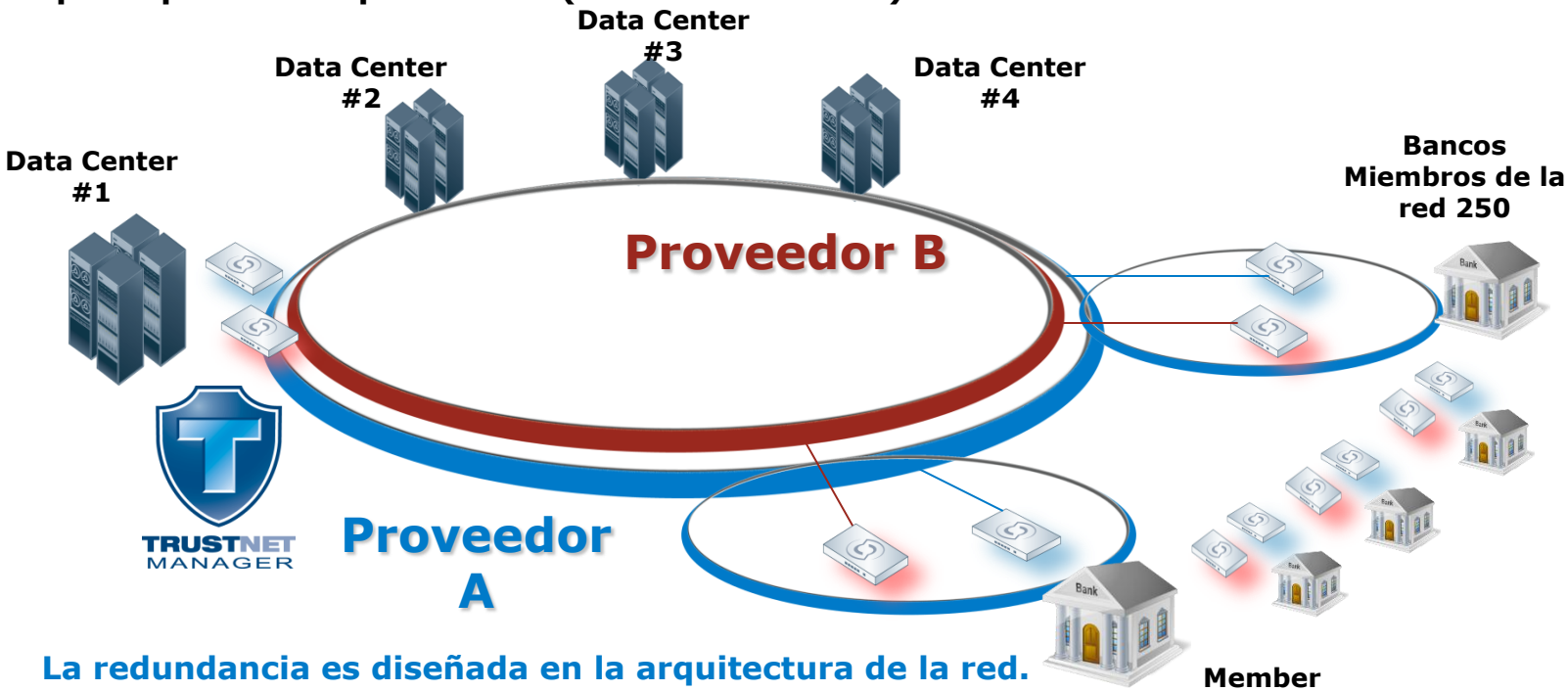
CERTES TRUSTNET MANAGER

- **Arquitectura redundante appliance o virtual**
- **Simple configurador de políticas con validación.**
- **Capacidades de log y auditoría**

USUARIA

Caso Mercado Financiero

- Leyes y reglamentos que requieren que los datos sean transmitidos en forma cifrada
- Múltiples data center o sedes centrales conectadas a 250 bancos a nivel mundial.
- Requieren alto rendimiento con baja latencia y cifrado AES 256
- Soporte para doble proveedor (sin túneles IPsec)



- La redundancia es diseñada en la arquitectura de la red.
- La carga del tráfico cifrado es balanceado entre los proveedores utilizando una sola política
- No afecta los niveles de servicios establecidos

USUARIA

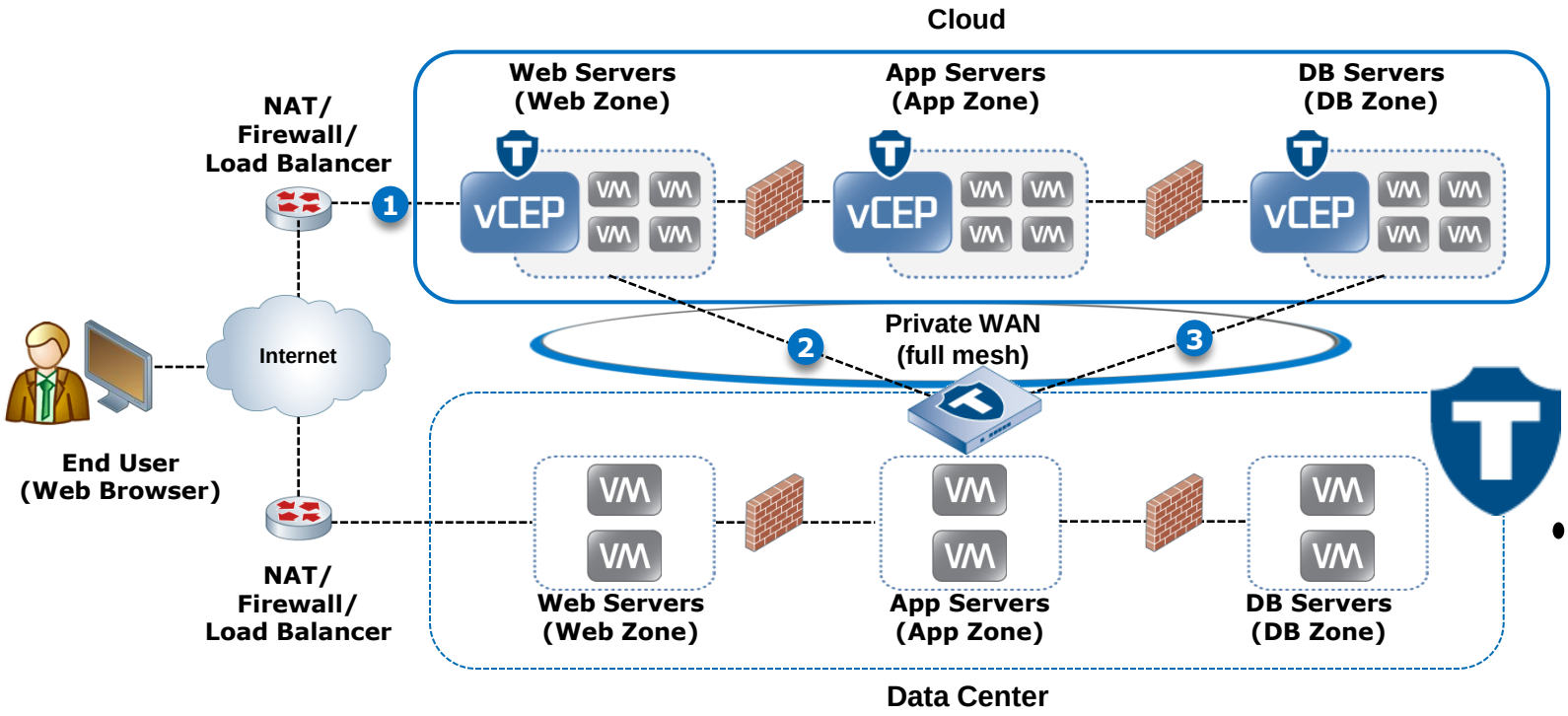
Caso Manufactura (Protección PI)

- **Empresa preocupada por la seguridad de datos en la última milla.**
- **Las políticas y llaves de cifrado son generadas desde la sede principal de la empresa en USA.**
- **Múltiples aplicaciones en tiempo real corriendo en redes con aceleradores.**

- **30 sedes en malla creciendo a 300**
- **El cifrado de capa 4 ofrece una solución totalmente invisible y no puede ser detectada por los proveedores de la línea.**

USUARIA

Caso Segmentación Criptográfica



USUARIA

Resumen Final

- **Ventajas significativas sobre las soluciones tradicionales**
  - **Performance de línea. Se puede encriptar aplicaciones sensitivas al retardo, como voz y video.**
  - **Gestión y Gerenciamiento Simple. Rotación de llaves de encripción automática.**

- **Funciona donde otras no**
  - **Nivel 2, 3 y 4 (incluídas redes mixtas)**
  - **Redes con diferentes tecnologías.**
  - **Clientes con multiples proveedores de redes.**
  - **Seguridad dentro o entre nubes.**

- **Transparentes a las infraestructuras de redes.**
  - **Permite separar las funciones de seguridad de las de red.**
  - **No impacta en la HA ni DR y es compatible con QoS u otros servicios.**
  - **No impacta en la calidad de servicio (SLA) de protocolos o aplicaciones de negocios.**

Gracias por asistir a esta sesión…

Preguntas y Respuestas…

USUARIA

Para mayor información:

Ariel BAGGIERI

(abaggieri@nextvision.com)

NextVision
IT + SEGURIDAD

Para descargar esta presentación visite www.segurinfo.org

Los invitamos a sumarse al grupo "Segurinfo" en LinkedIn

USUARIA