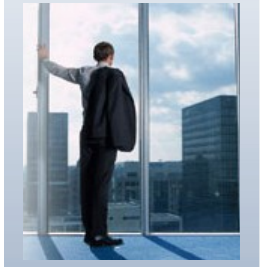


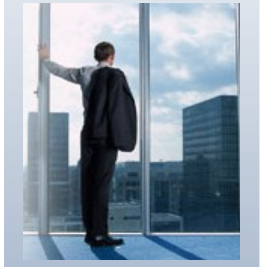
pensamos en TI

Gestión unificada de las amenazas (UTM, Unified Threat Management)

Ámbitos de aplicación y alternativas tecnológicas

Javier Zubieta Moreno
Gerente de Desarrollo de Negocio
Unitronics Comunicaciones

UNITRONICS

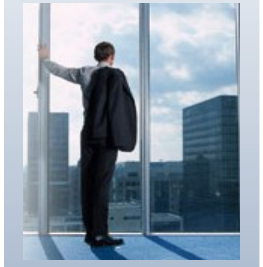


pensamos en TI

Situación actual

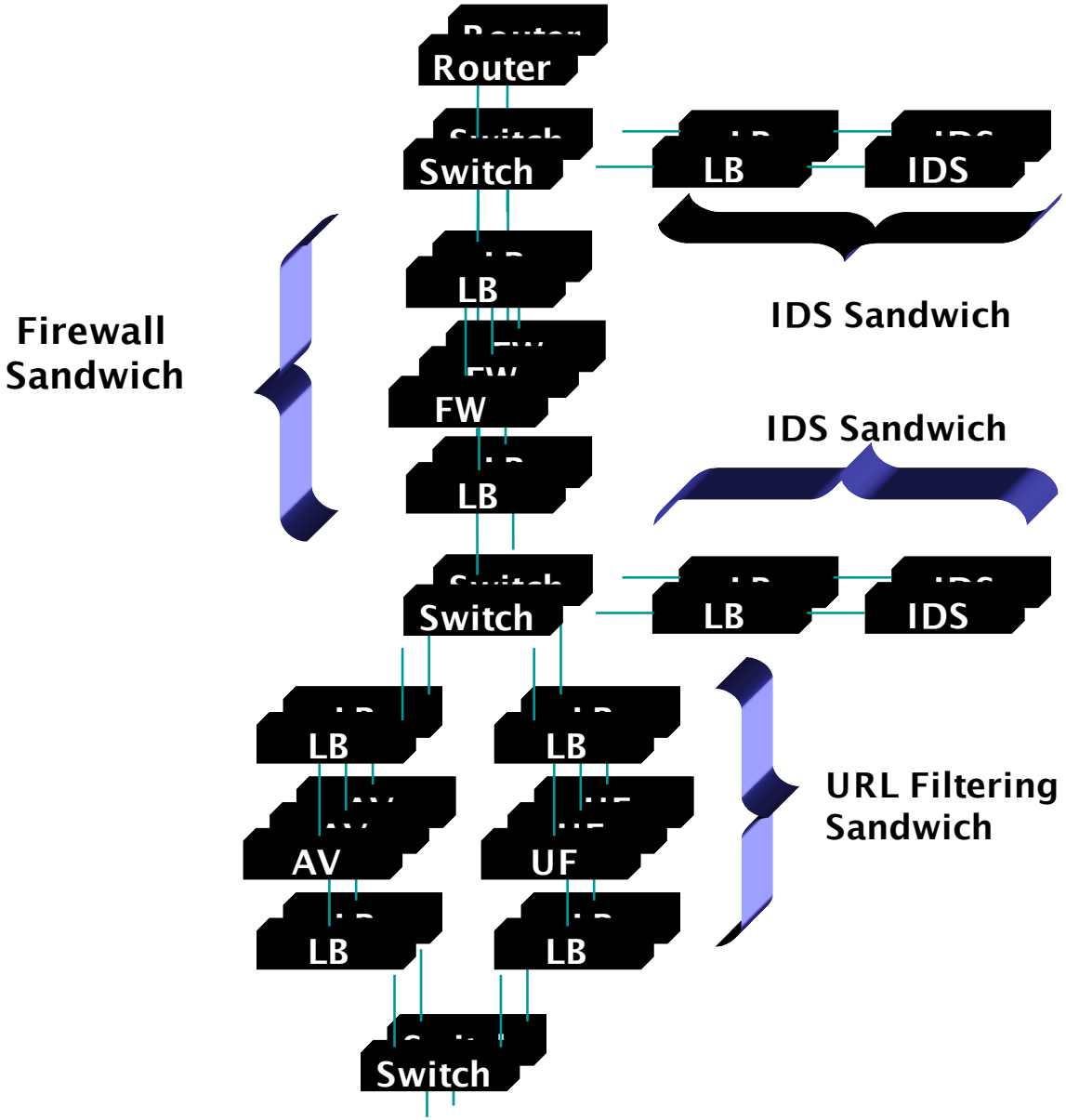
- Realidad en la seguridad: una solución para cada problema (y hay muchos…)
- Realidad en las implementaciones de seguridad: mucho software ha dado paso a mucho hardware (appliances)
- Los appliances han aportado ventajas a los despliegues:
  - Administración claramente identificada
  - Puesta en marcha más rápida
- Pero su proliferación presenta ciertas desventajas:
  - Integración limitada o nula
  - Gestión dispersa

UNITRONICS

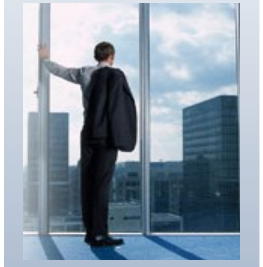


pensamos en TI

Configuraciones habituales

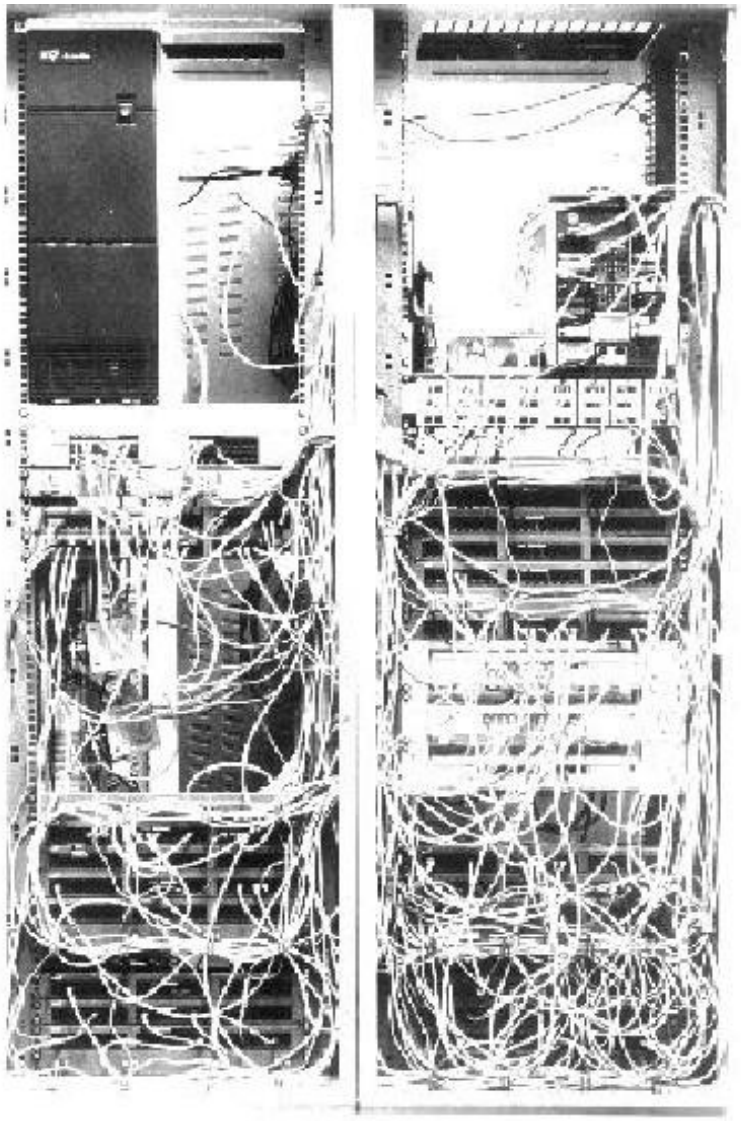


UNITRONICS

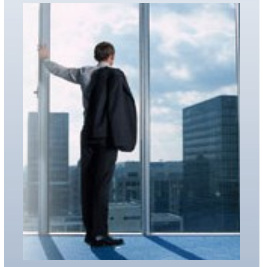


pensamos en TI

Configuraciones habituales



UNITRONICS

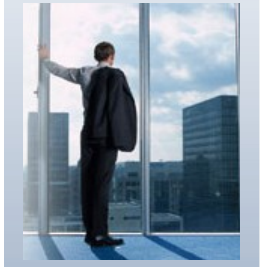


pensamos en TI

Consolidación

- Una manera de abordar estos problemas es mediante la consolidación de tecnologías, ejecutándose en muchos menos dispositivos
- En principio es buena idea:
  - Tendencia de consolidación de cpds
  - Tendencia de consolidación de otras tecnologías (balanceo de carga + terminación ssl + gestión de ancho de banda + …)
- Es decir, que ya hay otras realidades
- Pero se trata de saber si es adecuado para seguridad o no

UNITRONICS

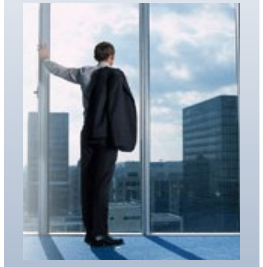


pensamos en TI

UTM

- Definición de IDC: *"UTM security appliance products include multiple security features into one box. To be included in this category, as opposed to other segments, the appliance must contain the ability to perform network firewalling, network intrusion detection and prevention, and gateway antivirus. All of the capabilities in the appliance need not be utilised, but the functions must exist inherently in the appliance. In these products, the individual components cannot be separated"*

UNITRONICS

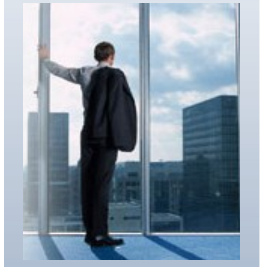


pensamos en TI

UTM

- Ventajas
  - Unificación y simplificación de la gestión (o al menos parte de la gestión)
  - Facilidad de los despliegues
  - Rápida reacción a la hora de abordar un nuevo proyecto
- Desventajas o incertidumbres
  - Simplificar la seguridad… ¿eso es buena idea?
  - Unificar la gestión a veces significa desechar un fabricante concreto
  - Unificar la gestión a veces puede desencadenar un problema de competencias
  - Rendimiento anunciado vs. real

UNITRONICS

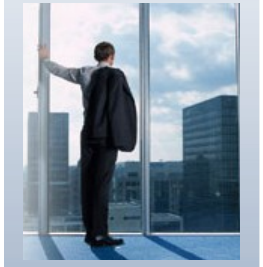


pensamos en TI

Tecnologías en UTM

- Según la definición, obligatoriamente debe incluir:
  - FW
  - IDS o IPS
  - AV de pasarela
- También se suele incluir
  - VPN y SSLVPN
  - AntiX
  - Filtrado de URLs
- Algunas otras
  - FW de aplicación

UNITRONICS

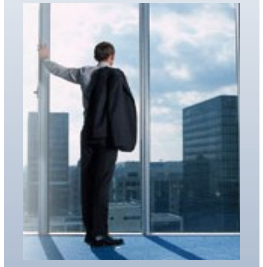


pensamos en TI

Alternativas de UTM

- Desde el prisma de la gestión
  - Unificar la gestión
    - Más preocupación por llegar a la “consola única”
    - Implica hw y sw del mismo fabricante o, al menos, fuertemente integrado
  - Reutilizar lo existente
- Desde el prisma de la localización
  - Altísimo rendimiento
  - Oficinas remotas o sedes pequeñas
  - Resto de localizaciones

UNITRONICS

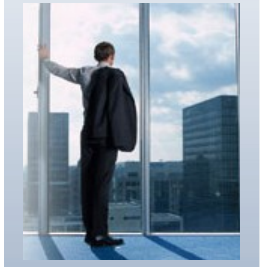


pensamos en TI

Ámbitos de aplicación: CPD

- Escenario:
  - CPD sin medidas (o medidas mínimas) de protección o segmentación
- Necesario:
  - Estabilidad “a prueba de bombas”
  - No necesariamente la mejor de las tecnologías del mercado
  - Embebido en circuitería
  - Activar FW e IDS (ampliaciones improbables de otras tecnologías, aunque debe estar preparado)
  - Altísimo rendimiento

UNITRONICS

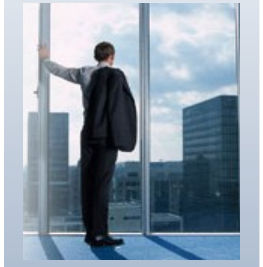


pensamos en TI

Ámbitos de aplicación: Reutilización

- Escenario
  - Seguridad perimetral ya desplegada, normalmente con tecnología tipo “best of breed”
- Necesario:
  - Convivencia UTM con lo existente
  - HW abierto a SW de marca diferente
  - Posibilidades de ampliación de tecnologías y capacidad
  - No pretender consolidar la administración, tarea prácticamente imposible

UNITRONICS

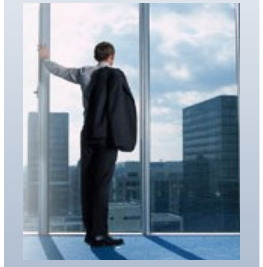


pensamos en TI

Ámbitos de aplicación: Reutilización + Consolidación

- Escenario
  - Muchos firewalls desplegados con administración dispersa y no precisamente optimizados en reglas
- Necesario:
  - UTM sustituye casi completamente lo existente, pero debe ser compatible con la marca de firewalls en cuestión
  - Se pretende consolidar la administración, pero de sólo una tecnología
  - Posibilidades de ampliación de tecnologías y capacidad

UNITRONICS

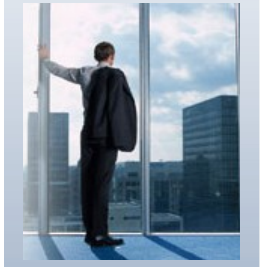


pensamos en TI

Ámbitos de aplicación: Sedes remotas y oficina pequeña

- Escenario
  - Infraestructura de TI dimensionada para un pequeño colectivo de usuarios sin apenas seguridad
- Objetivos
  - Todas las medidas de seguridad que se puedan con presupuestos ajustados
    - Empezando por las obligatorias
  - Facilidad extrema en instalación y administración
    - Posibilidades de administración multidispositivo para despliegues masivos
  - Capacidad de crecimiento en prestaciones si se incrementa el ancho de banda o el número de usuarios

UNITRONICS



pensamos en TI

Algunos fabricantes

CISCO

FORTINET

CROSSBEAM SYSTEMS

Check Point SOFTWARE TECHNOLOGIES LTD.

Juniper NETWORKS

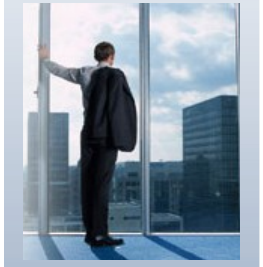
IBM

SONICWALL

Panda Software

IRONGATE Are you safe?

UNITRONICS

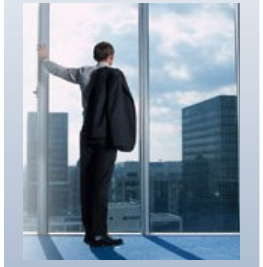


pensamos en TI

Conclusiones

- La aparición de UTM es natural y ha venido para quedarse
  - Es ligeramente diferente de: “sustituirá a la actual seguridad perimetral”
- Supone un paso adelante en la simplificación de la operación de seguridad
  - Pero no es la panacea
- La oferta de la industria está girando hacia UTM
  - Recuerda a lo que pasó con la tecnología sólo VPN
  - Vamos a tener UTM “hasta en la sopa”
- Hay una explosión de posibilidades, que habrá que cualificar correctamente
  - Las ventajas de las unas son las desventajas de las otras y viceversa

UNITRONICS



pensamos en TI

Muchas gracias

jzubieta@unitronics.es

UNITRONICS