Cómo detectar, prevenir y responder a los ataques, intrusiones y otras fallas de los sistemas

La administración unificada de amenazas como tema de estudio - UTM

Presentado por:
Carlos Guerrero
Director de Astaro para Latinoamérica

Contenido de la charla

- Conceptos básicos
- Problemática
- Impacto Financiero
- Impacto en el modelo de seguridad
- Tecnologías en desarrollo
- Propuesta de solución
- Conclusiones, Bibliografía y Cuestionamientos

Mayorista de Valor Agregado

Conceptos Básicos

Ataques más conocidos

- Un ataque de negación de servicios intenta ahogar o exasperar los recursos de un sistema de tal forma que no pueda responder a pedidos de servicio legítimos.
- Si el ataque es realizado por varias máquinas a un servicio se conoce como Ataque de Negación de Servicios Distribuido.

Ataques por el web

- Spyware
  - Se dedican a recolectar datos de los usuarios y enviarlos a servidores de recolección.
  - Pueden recolectar contraseñas, configuraciones o la conducta de los usuarios en Internet (páginas visitadas).
  - Por lo general se distribuye a través de software gratuito.
- Adware
  - Las aplicaciones adware promocionan productos o servicios a través de pop-ups (ventanas emergentes) mientras se navega en Internet.
  - La mayoría de las veces se instala una vez el usuario a aceptado los términos del contrato de software gratuito. El usuario no lee los términos.

Troyanos

- No es considerado un gusano o virus porque no se propaga por si mismo.
- Sin embargo, un gusano o un virus puede ser usado para copiar un troyano en un sistema (*dropping*).
- El objetivo del troyano es trastornar el trabajo normal del usuario. Por ejemplo, el troyano puede crear una puerta trasera en un sistema para robarle la información o alterarle la configuración a éste.

Gusanos

- Si el código malicioso se replica por si mismo, no es un troyano.

- La mayoría de los gusanos se copian a si mismos en un sistema y entonces utiliza los puertos infectados para replicarse por la red:

Virus

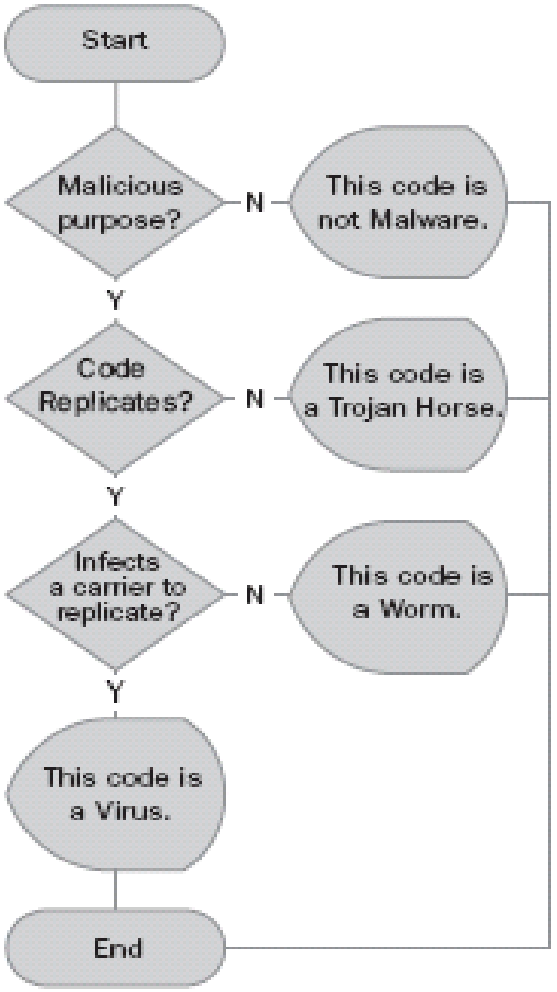
- Si el código malicioso se copia a si mismo en un archivo, un documento o en el sector de arranque de un disco para replicarse, es considerado un virus
- Esta copia puede ser la copia exacta del original o una versión modificada (polimorfismo)
- La mayoría de los virus intentan causar estragos en la máquina infectada, como por ejemplo, eliminar datos.

SPAM

- Spam en correo comercial no solicitado, en el cual se trata de publicitar un producto o servicio.
- Este tipo de amenaza no causa daño a las máquinas, pero sí gasta recursos de los servidores de correos y de los usuarios afectados.
- Muchas veces el *malware* instalan pequeños servidores SMTP con el fin de generar o redireccionar correos Spam a los buzones del mundo (también conocido como volver una máquina en zombie).

Qué no es malware?

- Scams
  - Casi cualquier medio de comunicación ha sido empleado por los criminales para obtener algún beneficio financiero de sus víctimas.
  - Una forma de Scam es conocida como Phishing, brand spoofing o carding.
  - Por ejemplo, un correo que llegue de el Banco X, pidiéndole al usuario que actualice sus datos (incluido el password).

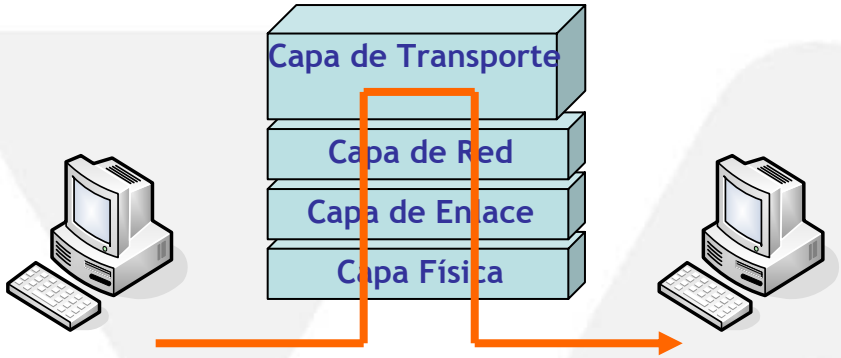
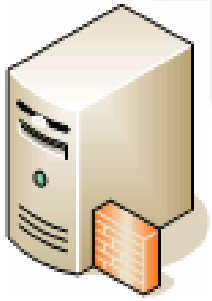
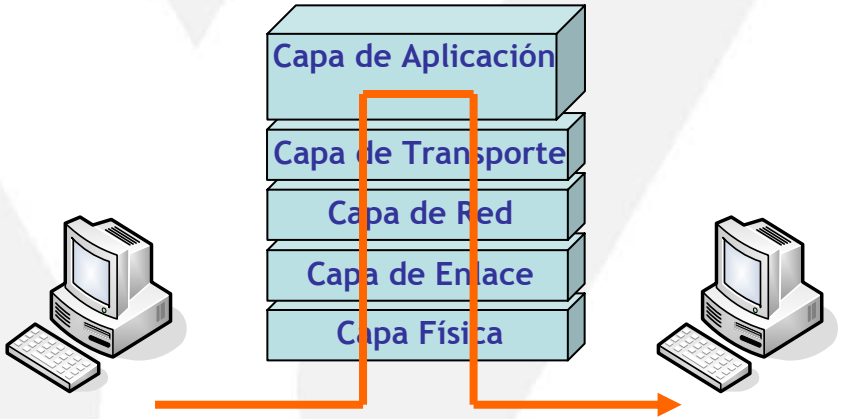


Firewall

- Un firewall es un dispositivo que contiene un conjunto de reglas especificando qué tipo de tráfico puede entrar o salir, hacia o desde nuestra red corporativa

- Los firewalls son típicamente clasificados en tres clases:
  - Firewall de Filtrado de Paquetes (**Packet Filter Firewall**)
  - Firewall de Inspección de los estados de las conexiones (**Stateful Inspection Firewall**)
  - Proxy's de Aplicación (**Proxy Firewall**)

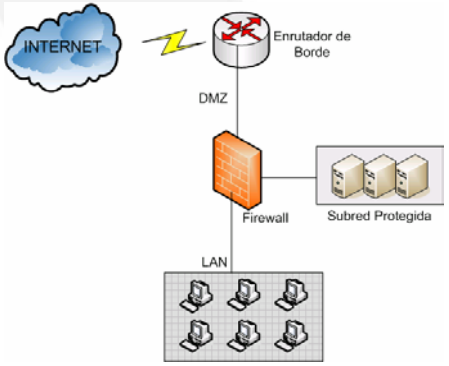
Diferencia Firewall vs proxy

FIREWALL 	
PROXY 	

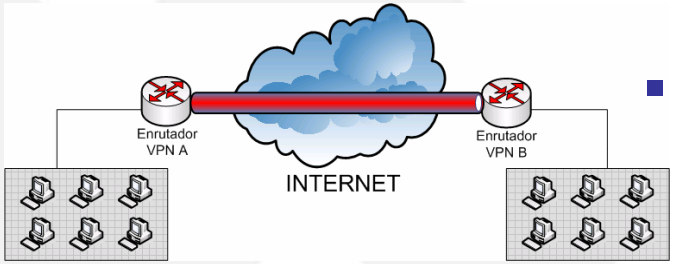
Problemática

Limitaciones

- Por definición un firewall tradicional permite o niega IPs y puertos, permite NAT externo e interno
- No bloquea el tráfico que contenga Virus, Spam, Phising, Spyware, gusanos y el malware
- No hace detección y prevencion de intrusos



En qué falla un firewall

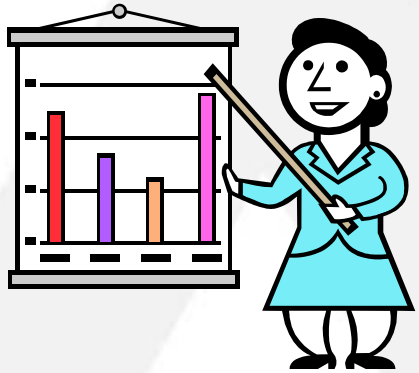


- No cifra los canales con VPN
- Una red privada virtual (VPN – Virtual Private Network) es una sesión establecida entre dos entidades utilizando un canal hostil como medio de comunicación (Internet o la WAN de su proveedor, a menos que los considere seguros)

Impacto Financiero

Impacto Financiero

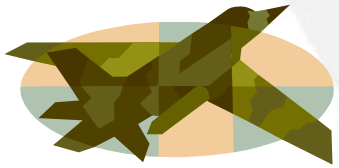
- Una empresa que factura 4000M mensuales factura 1000M semanales, entonces factura diariamente 200M en promedio
- Cuánto le cuesta a la organización no tener sistema durante dos dias?
- Una falla por ejemplo: Un gusano entra por el firewall haciendo un exploit al servidor web, hace un ataque smurf al firewall… y de paso infecta los 600 PCs XP que no tienen suplementos a la fecha



Impacto en el sistema de seguridad

Recordemos:
Propiedades de un sistema de información

- Confidencialidad: Los recursos del sistema sólo pueden ser accedidos por los elementos autorizados
- Integridad: Los recursos del sistema sólo pueden ser modificados o alterados por los elementos autorizados
- Disponibilidad: Los recursos del sistema deben permanecer accesibles a los elementos autorizados



Qué variables afecta

- Confidencialidad: Un exploit deja al atacante con permisos de administrador
- Integridad: el servidor web es modificado o alterado por un usuario no autorizado
- Disponibilidad: Los PCs de la red, el firewall y el servidor web no son accesibles por los elementos autorizados

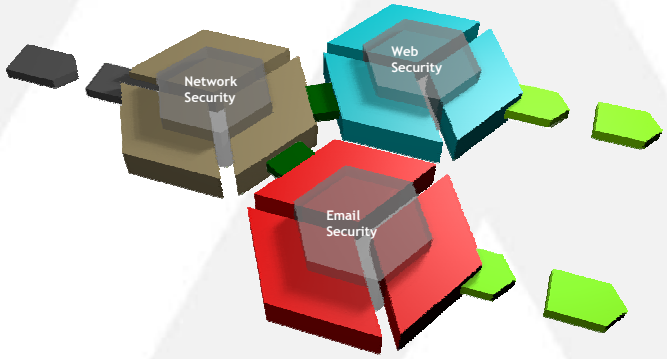
Tecnologías en desarrollo

Detección de intrusos

- Los sistemas de detección de intrusos son usados para detectar y alertar ante la presencia de paquetes maliciosos.
- Los sistemas de prevención ante intrusos son usados para bloquear, luego de ser detectados, paquetes maliciosos presentes en la red o el host.
- NIDS: Sistemas de Detección de Intrusos de Red.
- HIDS: Sistemas de Detección de Intrusos de Host.
- Básicamente, estos sistemas escanean la red (sniffers) en busca de paquetes que sean similares a paquetes reportados, a una base de datos, como paquetes que atenten a una aplicación (MS SQL Server) o a un protocolo estándar (FTP, HTTP).

UTM

- Se está creando la estrategia de integrar en el firewall las tecnologías de IDS, VPN, Filtro WEB, filtro Correo y antivirus
- Otras estrategias son la de configurar un elemento activo de red independiente especializado en la tarea específica
- Obviamente la última estrategia no correlaciona los eventos



Propuesta de solución

UTM: Un primer anillo de seguridad

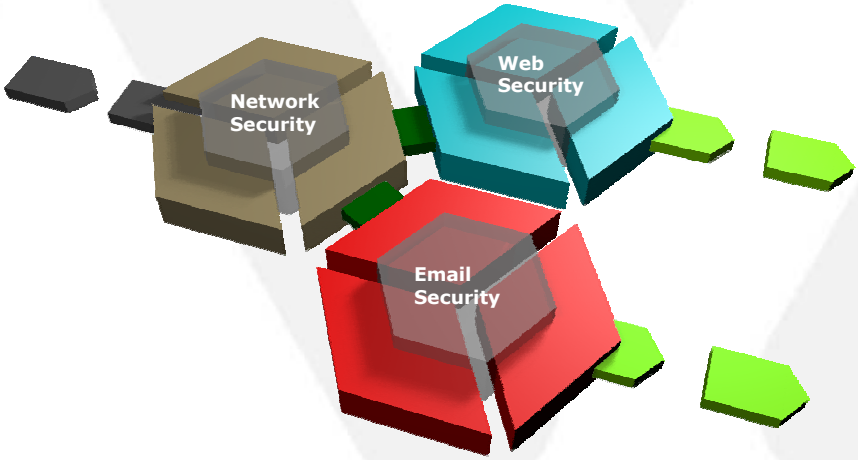
- Un UTM es la mejor solución a bajo costo como primer anillo de seguridad por que integra la gestión y la administración de todas las amenazas
- Correlaciona los eventos que preveen una intrusión
- Escala desde appliance hasta servidor linux
- Administración gráfica intuitiva
- Reportes gráficos para toma de decisiones
- Website: www.astaro.com

Ejemplo: UTM escalable

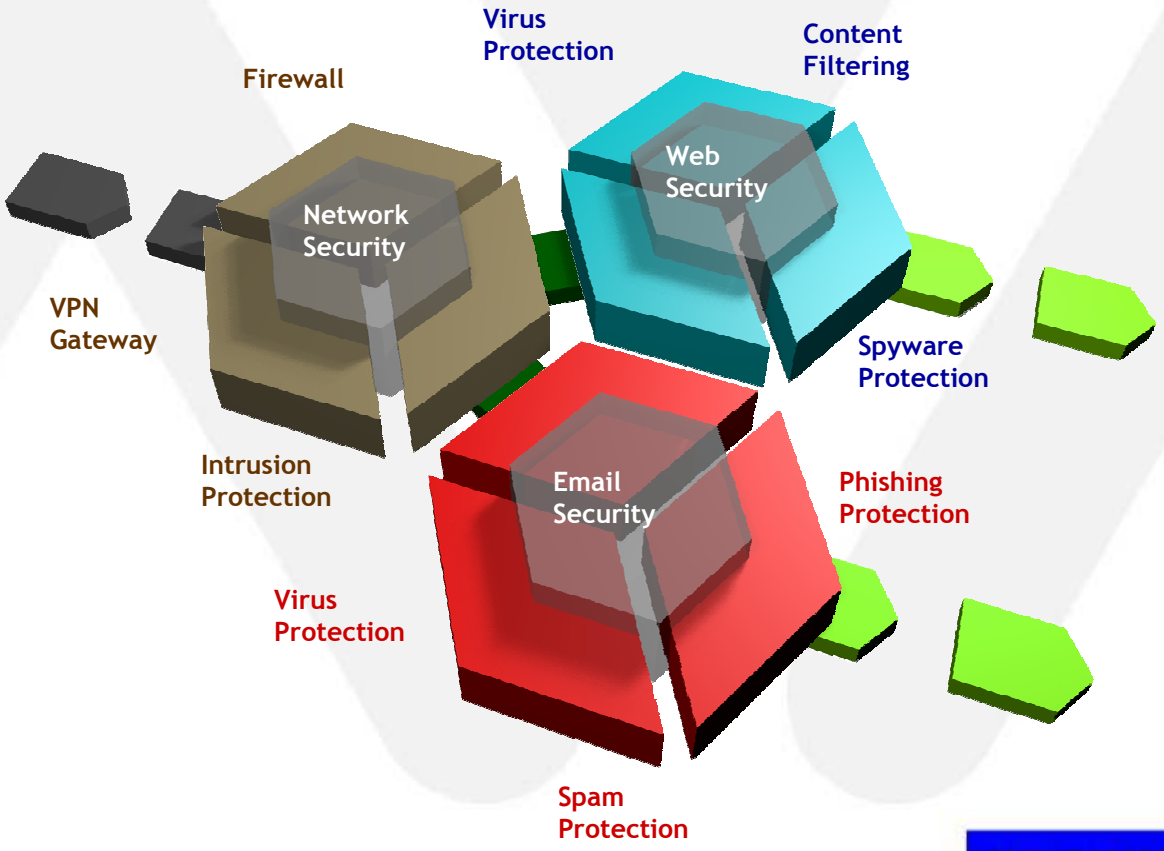
- Control de Contenido: Mejore la productividad de sus empleados y evite problemas legales.
- Firewall: Abra únicamente los puertos necesarios.
- VPN: Reduzca los costos de conectividad.
- Protección contra Intrusos: Bloquee intrusos y asegure la continuidad del negocio.
- Filtrado de Spam: Incremente dramáticamente la eficiencia.
- Anti-Virus: Defienda los datos de su organización y sus estaciones de trabajo

Astaro Security Gateway

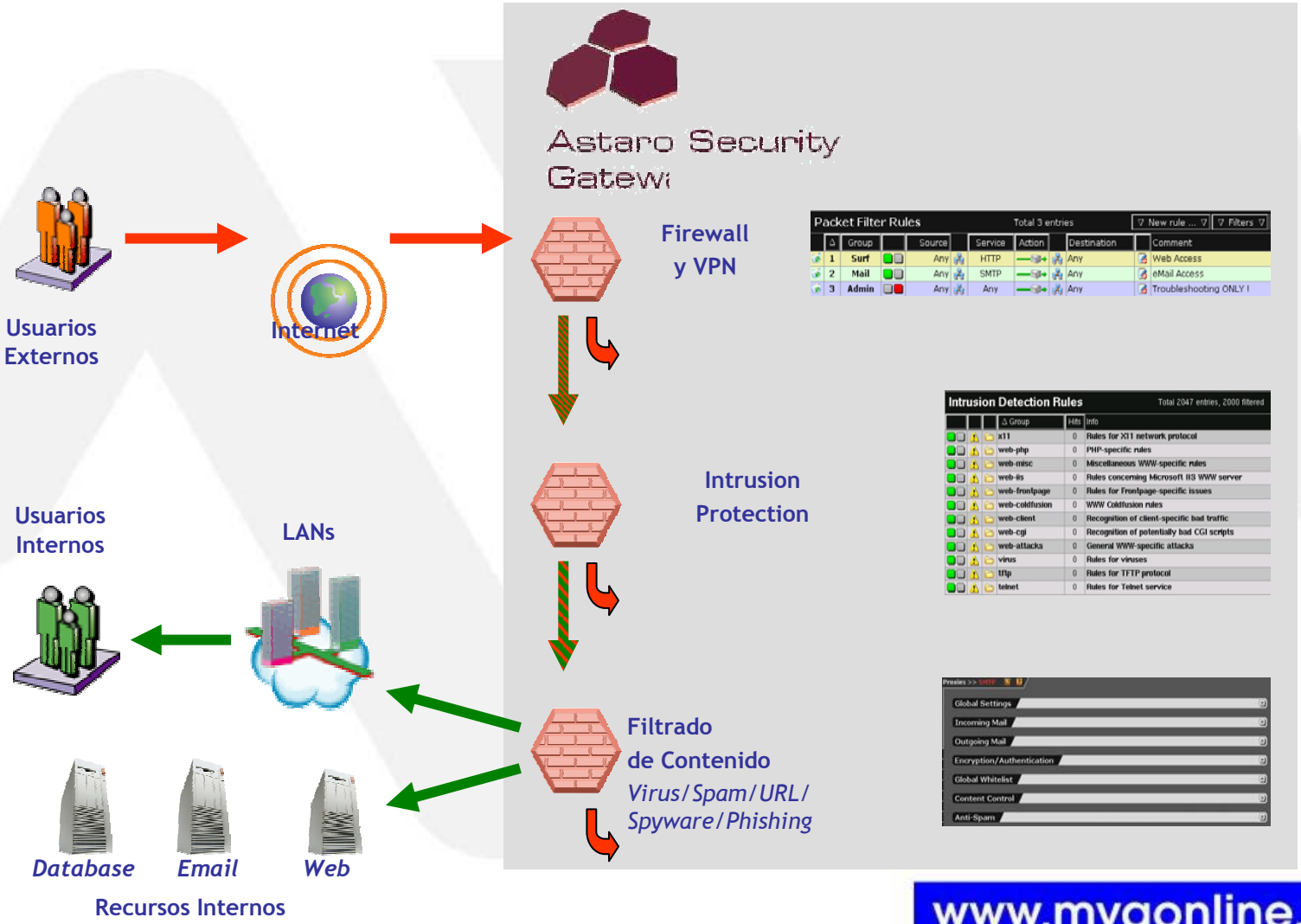
- Seguridad Perimetral Completa



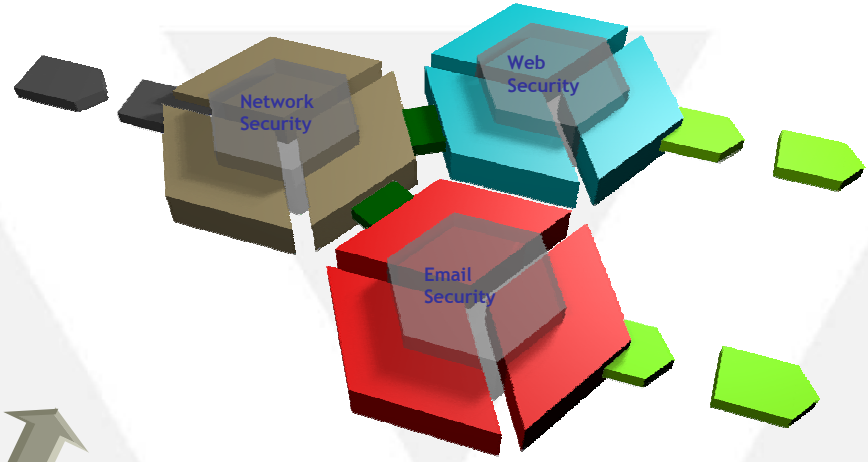
Nueve Aplicaciones de Seguridad Integradas

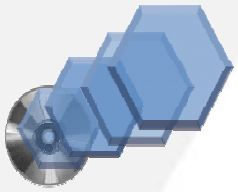


Seguridad por Capas



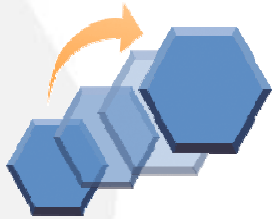
Administración Integrada





Instalación

Interface de Administración

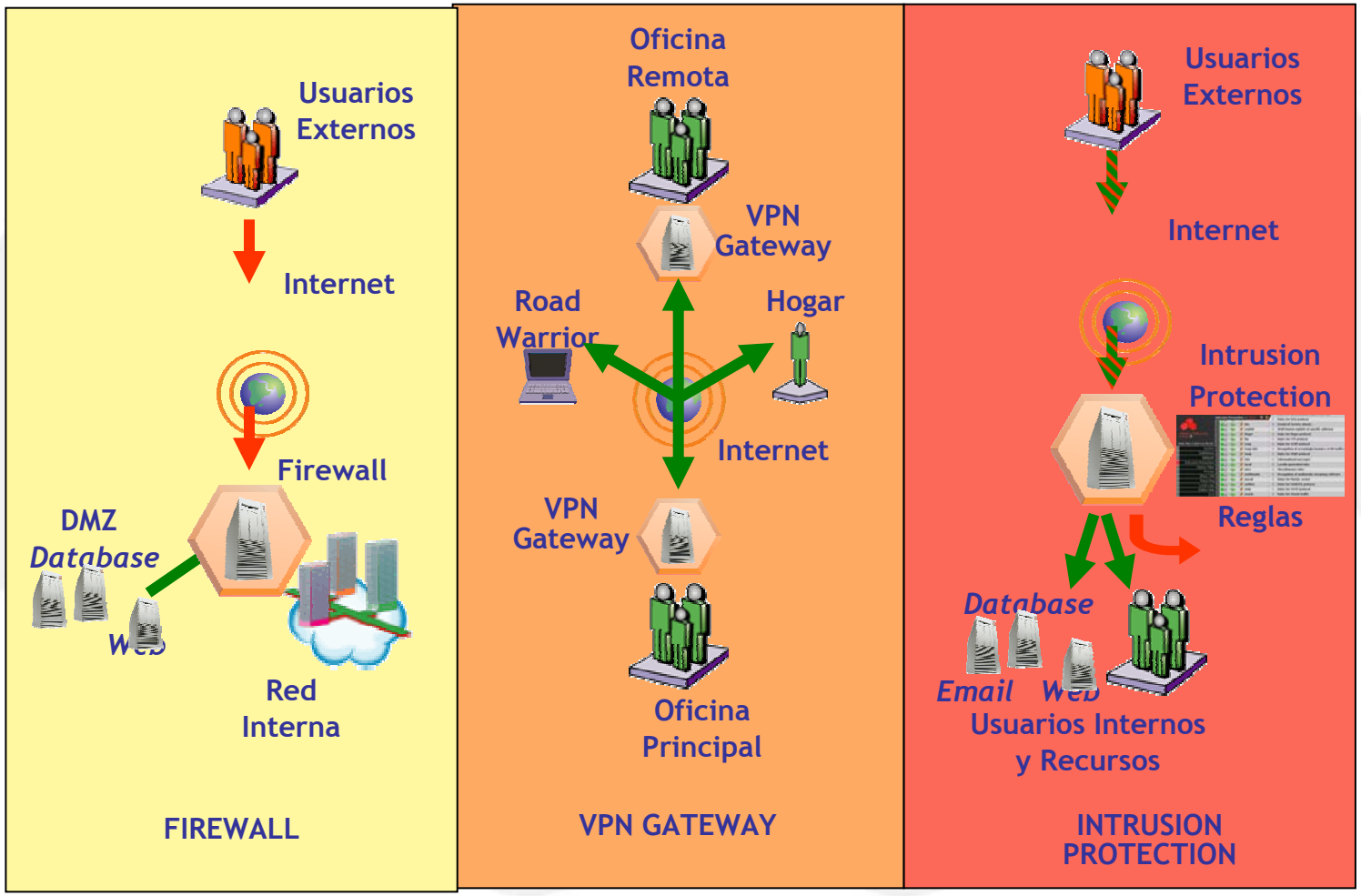


Actualizaciones

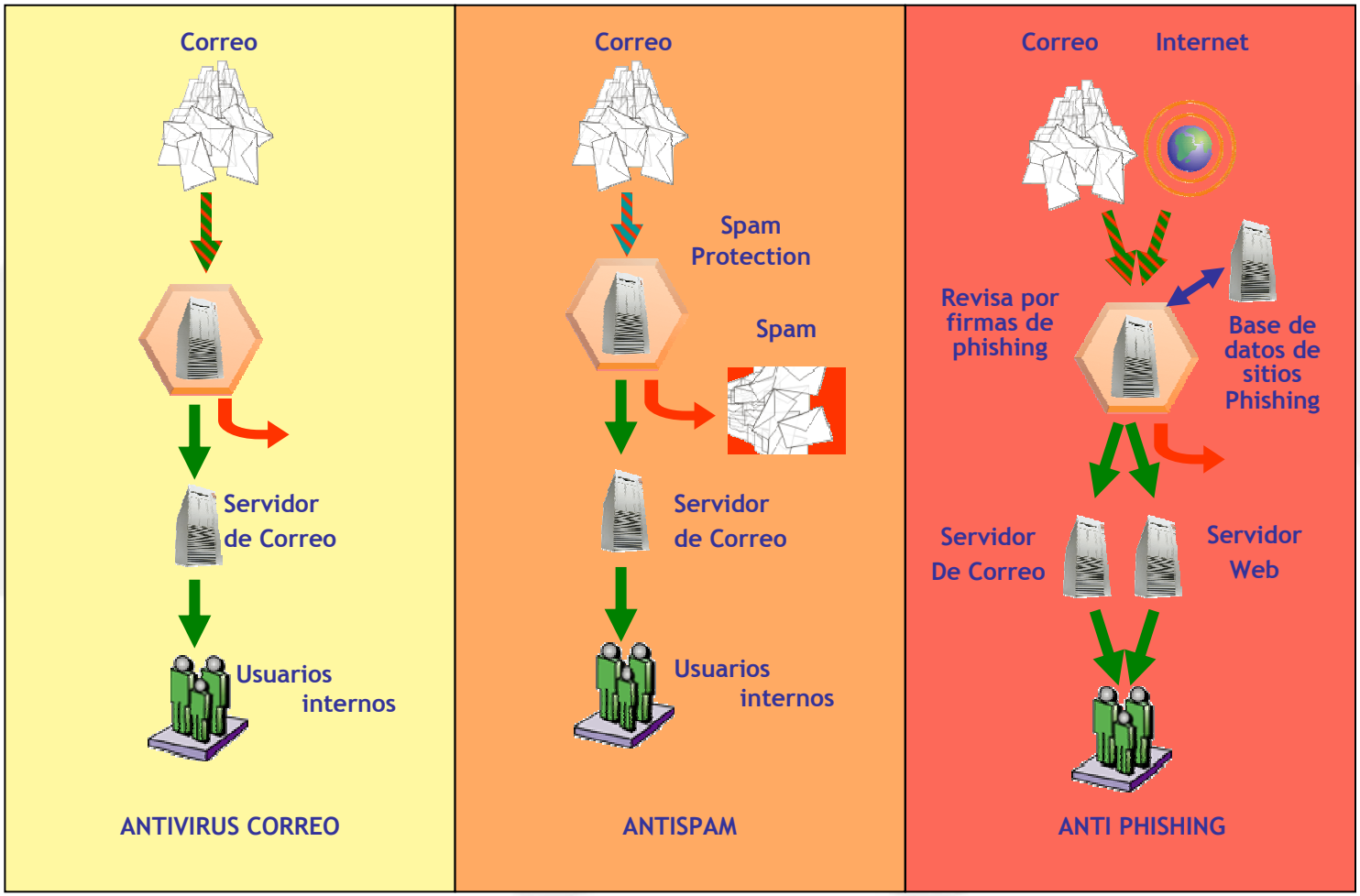
Reportes y Logs

Seguridad de Red

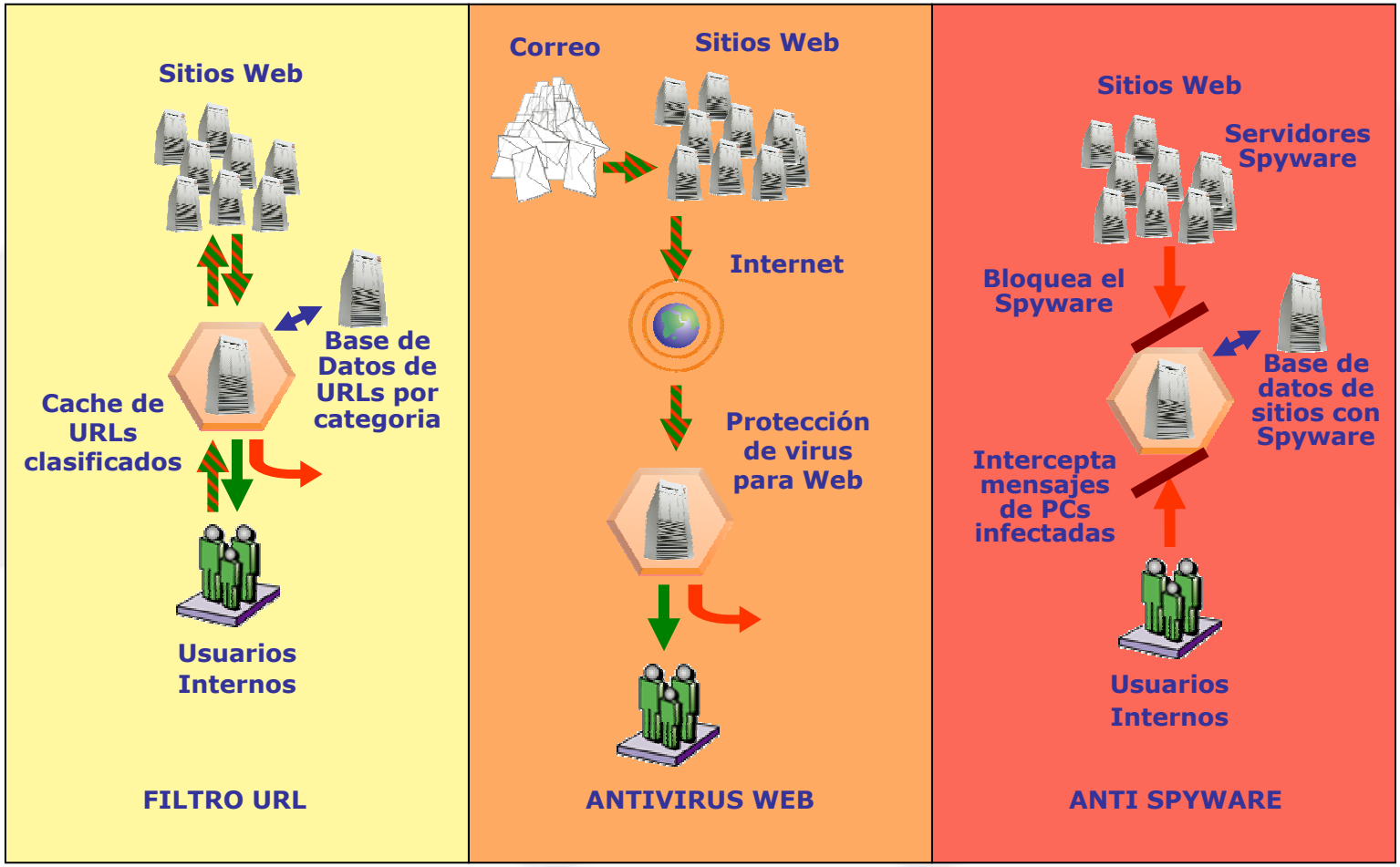
Network Security



Email Security



Web Security



Valor del negocio

- Mejora la Seguridad
  - Bloquea amenazas con total seguridad de perímetro
  - La administración integrada reduce el error humano e incrementa la velocidad de respuesta
- Aumenta la Productividad
  - Priorize el uso de los recursos según los requerimientos del negocio
  - Optimize la eficiencia del personal bloqueando actividades no productivas
  - Simplifique el mantenimiento de sus seguridades
- Administración Simplificada
  - Una solución completa de seguridad perimetral que es fácil de instalar, configurar, administrar y actualizar; y que es completamente escalable de oficinas pequeñas a oficinas regionales

Conclusiones

- Se necesitan proveedores de UTM con soporte local y global
- La correlacion de eventos por LOGS es clave en un UTM
- El futuro es de gestión centralizada de amenazas por que las amenazas se aunan y evolucionan
- Existen dos alternativas: “Lo construyo yo por servicios” o “Lo compro a un costo razonable”

Bibliografía

- Ziegler, Robert. Linux Firewalls. 2nd ed. 2002. New Riders Publishing.
- Harrison, Richard. The Antivirus Defense-in-Depth Guide. 2004. Microsoft Corporation.
- Tabacman, Eduardo. Elementos de Seguridad Informática. 2005. VIRUSPROT.COM.
- http://www.jrwhipple.com/virus_iloveyou.html
- http://www.astaro.com
- IATF. Defense in Depth. Release 3.1. 2002.
- McGuiness, Todd. Defense In Depth. Version 1.2E. 2001. SANS Institute.
- Cole, Krutz, Conley James. Network Security Bible. 1st ed. 2005. Wiley Publishing.

Gracias por su atención

Más información en www.mvaonline.com
Email: info@mvaonline.com

Lo esperamos en el área de Exhibición a las 6:00 PM