COMO DISEÑAR E IMPLEMENTAR UN PLAN DE SEGURIDAD PERIMETRAL

OBJETIVOS

- Situación actual.
- Tipos de Ataques y Métodos de Protección.
- Diseñar un Plan de Seguridad Perimetral.

Computer Security Institute

- El 56% de las empresas sufrieron accesos no autorizados a sus sistemas.
- Las perdidas asociadas a ataques informáticos en el 2003 alcanzaron los 201.797.340 $. (251 organizaciones).
- El robo de información causó perdidas de 70.195.900 $, seguido muy de cerca por los ataques DoS que alcanzaron la cifra de 65.643.300 $.
- El 68% de las grandes firmas españolas apenas protege su seguridad informática.

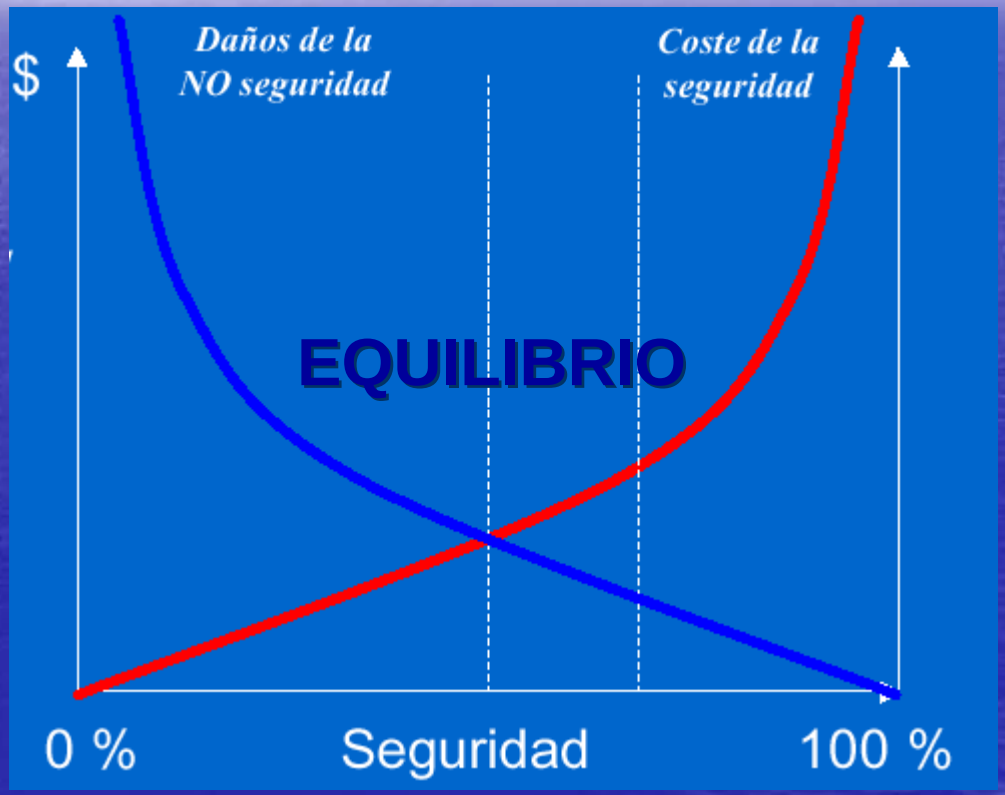
¿Cuáles son las consecuencias?

- Responsabilidad legal (LORTAD).
- Perdida de confianza (Mala Imagen):
  - Accionistas.
  - Clientes en B2C.
  - Empleados (desmotivación, inseguridad).
- Reducción en los beneficios.
- Robo de propiedad intelectual.

COSTES

COSTE DE LA SEGURIDAD

EL 100% DE LA SEGURIDAD NO EXISTE



Tipos De Ataques

Los ataques de red pueden ser tan variados como los sistemas a los que intentan penetrar. Algunos ataques son complejos mientras que otros son realizados por el desconocimiento de los usuarios.

Packet Sniffers

- Un Sniffer es una aplicación que usa el adaptador de red en modo promiscuo para capturar los paquetes que circulan a través de un mismo dominio de colisión. El principal peligro son los datos que circulan sin cifrar (telnet, ftp, smtp, pop3,...).

¿Cómo Protegernos?

- Switched Infraestructure. Mitiga el efecto de los sniffers. Los hackers sólo podrán tener acceso a la información que fluya por el puerto al que están conectados.
- Herramientas anti-sniffers. Detectan cambios en el tiempo de respuesta de las máquinas.
- Cryptografia. Es el método más efectivo. Si un canal es criptograficamente seguro lo único que ve un sniffer es texto cifrado y no el mensaje original. (IPSEC, SSH, SSL).

IP SPOOFING

- Sucede cuando un hacker dentro o fuera de una red se hace pasar por una máquina “de confianza”. Normalmente se utiliza para realizar otros tipos de ataques. El clasico ejemplo es lanzar un DoS usando una ip spoofed para ocultar su identidad.

¿Cómo Protegernos?

- Control de acceso. Denegar el acceso desde la interfaz externa de cualquier ip que resida en al red interna. Esto sólo sirve si las ips de confianza son las internas, si tenemos ips externas a las que se les permite el paso no nos protege contra el uso de esas ips.
- RFC 2827 Filtering. Consiste en denegar el tráfico de salida que no tenga como dirección de origen una ip del rango de nuestra organización.

Denial Of Services

- Es el más conocido de los ataques y a su vez el más difícil de eliminar completamente. Son fáciles de realizar. No intentan acceder a nuestra red sino lograr que uno o más servicios no este disponible. Algunos aprovechan protocolos de Internet como el icmp, otros usan agujeros de seguridad en las aplicaciones o errores en el software.

Tipos de DoS:

1. JAMMING o FlOODYNG. (ping de la muerte).
2. TCP SYN FLOOD.
3. Connection Flood (inundación de la conexión), Net Flood (inundación de la red).
4. Land Attack.
5. Supernuke o Winnuke.
6. MAIL BOMBING-MAIL SPAMMING-JUNK MAIL
7. etc.

¿Cómo Protegernos?

Para prevenirlos se requiere una coordinación con nuestro isp, de nada nos sirve que bloqueemos estos accesos si ya han “llenado” nuestro ancho de banda. Pueden ser reducidos sus efectos de la siguiente forma:

1. Medidas Anti-spoof. Si el hacker no puede enmascarar su identidad no debería atacar
2. Medidas Anti-DoS. Configurar los FW y routers para que limiten el máximo de conexiones que un sistema pueda tener abiertas al mismo tiempo.
3. Limitar la tasa de tráfico con el ISP. Este filtro limita la cantidad de tráfico no esencial que atraviesa ciertos segmentos de red.

Password Attacks

- Los ataques de contraseña usan diferentes métodos: forzado de password, troyanos, ip spoofing, sniffers, ingeniería social. Lo primero que podemos hacer contra estos ataques es evitar que las passwords circulen sin cifrar. También es básico usar passwords difícil de adivinar, al menos 8 caracteres con mayúsculas minúsculas y numéricos.
- Una herramienta muy usada para forzar passwords es la LC3 formerly L0pht Crack). Fuerza passwords de Nt cuando son fáciles de adivinar.

Man in The Middle

- Este ataque requiere que el hacker tenga acceso a los paquetes que provienen de una red, por ejemplo un empleado de un ISP. Usan packet sniffers y protocolos de routing y transporte. Pueden generar DoS, recogida de información, acceso a recursos de red, corrupción de los datos transmitidos e introducción de información en las sesiones. El mejor método para prevenirlos es el uso de criptografía.

Ataques a nivel de aplicación

- Explotan vulnerabilidades del software de un servidor. Pueden conseguir acceso a la máquina con los permisos que posee la aplicación que tiene la vulnerabilidad. El principal problema es que usan puertos permitidos por los FW.

¿Cómo Protegernos?

Nunca podrán ser completamente eliminados, lo único que podemos hacer es procurar estar al día para corregir las vulnerabilidades.

1. Revisar los logs periódicamente y analizarlos.
2. Estar subscritos a listas de distribución de publican las ultimas vulnerabilidades.
3. Mantener los S.O. y aplicaciones con los últimos parches
4. El uso de IDS.

Reconocimiento de redes

Cuando un hacker intenta penetrar en una organización lo primero que suele hacer es recoger toda la información posible sobre su red.

- DNS queries pueden revelar quien posee cierto dominio y que direcciones le han sido asignadas.
- Ping sweeps de las direcciones reveladas por el dns.
- Escaneo de puertos de los hosts descubiertos por los ping sweeps.

El uso de IDS es muy útil frente a este tipo de ataques.

Trust Explotiation

- Sucede cuando un individuo se aprovecha de las relaciones de confianza dentro de una red. Se pueden mitigar estos ataques instalando niveles de confianza dentro de la Intranet. Los sistemas fuera del FW nunca deberían ser confiado por los de dentro, así como estar limitados a ciertos protocolos y ser autenticados por algo más que su ip.

Redirección de Puertos

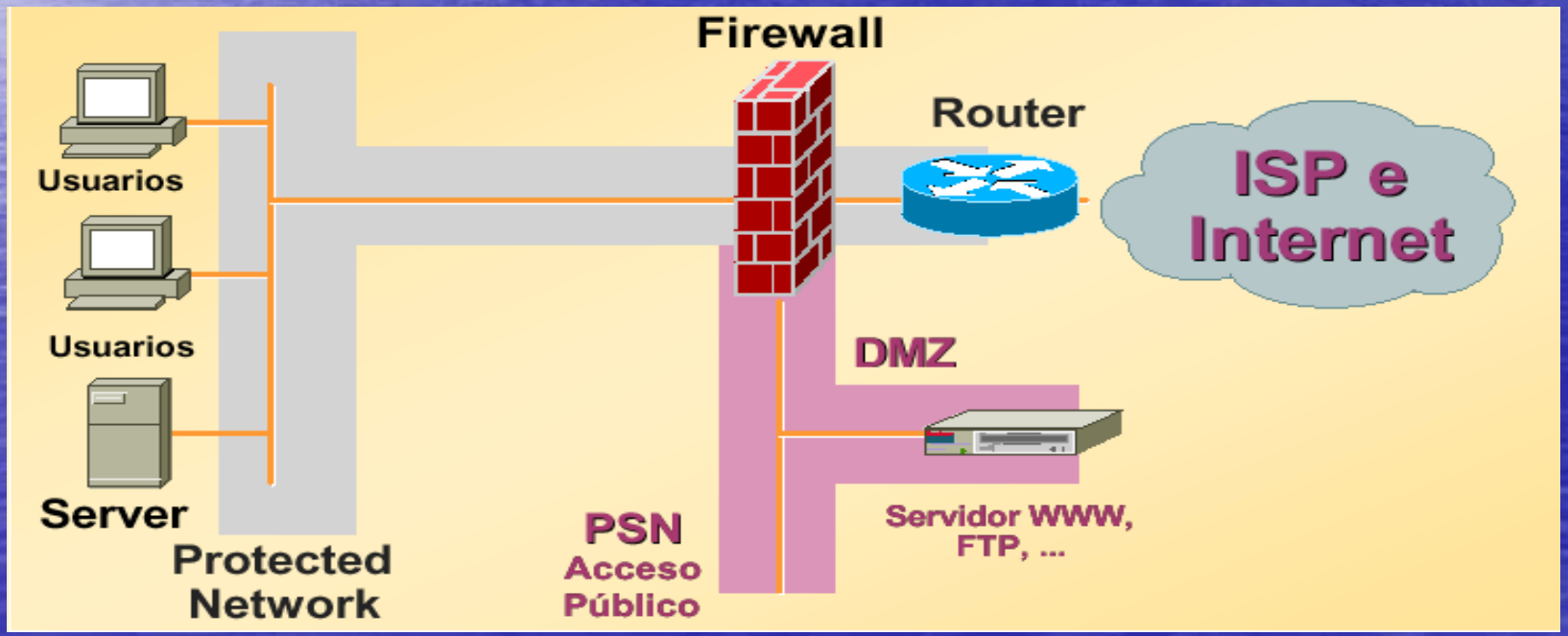
- Son un tipo de Trust Explotiations, usan un host comprometido para pasar tráfico a través del FW. Un ejemplo claro es el caso de tener una red interna y una DMZ. Para este tipo de ataques también se recomienda el uso de IDS.

Virus y Troyanos

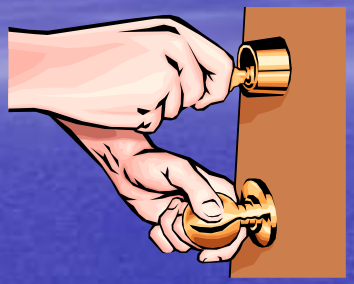
- Son la principal vulnerabilidad para los pc’s de los usuarios. Como ya sabemos lo mejor que se puede hacer es el uso de antivirus actualizados y permanecer informado. (Nimda, Blaster,....)

Seguridad Perimetral

Consiste en separar nuestra red, mediante el uso de un FW, en zonas a las que asignamos distintos niveles de seguridad.



Cuando la seguridad logica imita a la seguridad fisica



- Estamos todos familiarizados con pautas, productos y tecnologias de seguridad fisica
  - Cerramos puertas y ventanas
  - Usamos sistemas con tarjetas
  - Sistemas de alarmas
  - Camaras de vigilancia

- Las contrapartidas en seguridad logica
  - Firewalls = cierre de puertas y ventanas
  - IDS = sistemas de alarma y camaras de vigilancia

EBIOSPHERE

¿Qué es VPN-1/FW-1 NG?

Garantiza las conexiones de red basándonos en los tres componentes de seguridad esenciales: encriptación, autenticación y control de acceso. (Stateful Inspection)

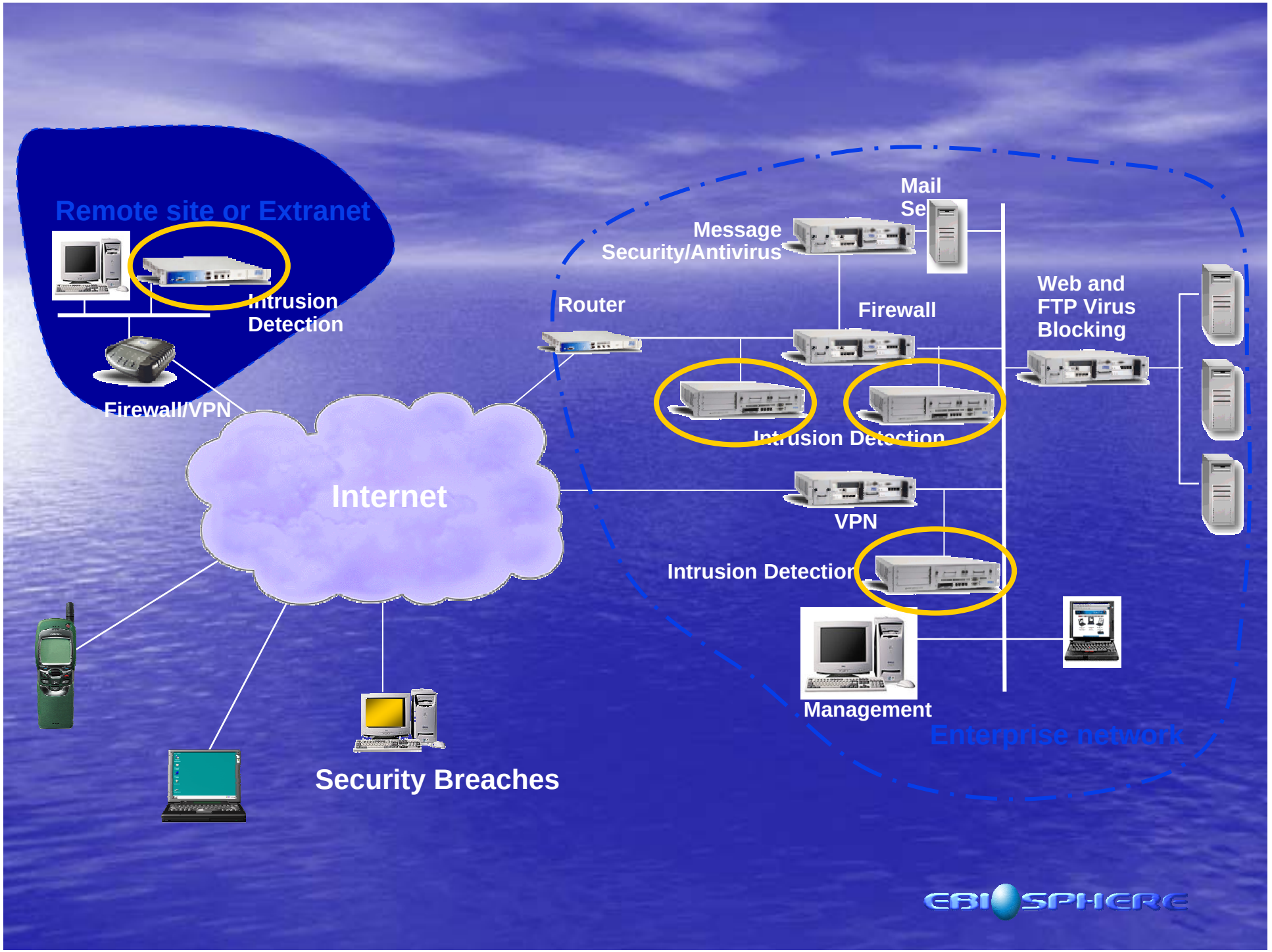
1. Provee de seguridad de contenidos para HTTP, FTP, UFP y SMTP. Content Vectoring Protocol
2. Creación de VPN site to site y client to site. Secure Remote y Secure Client. Policy Server.
3. Open Platform for Security (OPSEC).
4. Suspicious Activities Monitoring (SAM).
5. Check Point Malicious Activity Detection (CPMAD)

Porque combinar IDS´s y Firewalls?

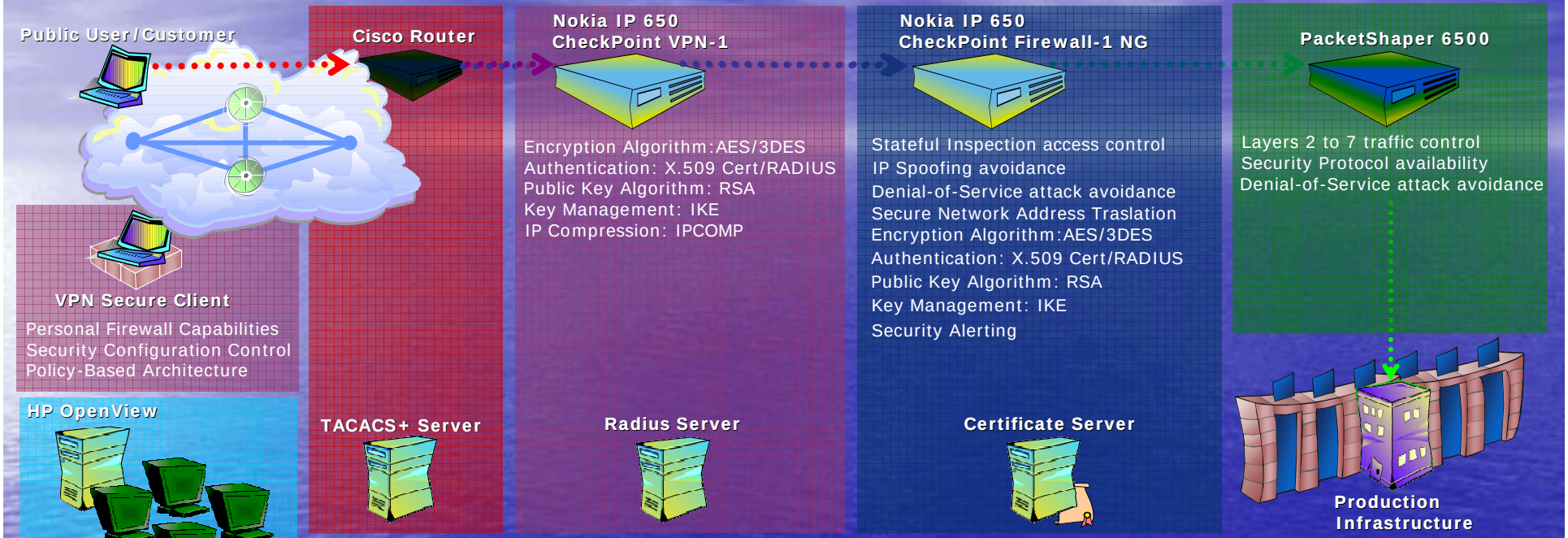
- Firewalls bloquearan "visitantes" no autorizados
  - Bloqueando sesiones y direcciones no deseadas
  - Bloqueando algunos ataques – de insercion o fragmentados
  - Deben de ser **SIEMPRE** la primera linea de defensa
- Pero al mismo tiempo el cortafuegos es debil
  - Simplemente permiten accesos autorizados - si el puerto esta abierto, no detendran ataques como Code Red, Nimda,...
- Los IDS`s toman el relevo cuando los cortafuegos son superados
  - Inspeccionan las cabeceras en busqueda de anomalias, protocolos inusuales...
  - Inspeccionan y busquan ataques, backdoor, troyanos, gusanos, etc.....

Ambos dispositivos son absolutamente complementarios

EBI SPHERE


Remote site or Extranet
Intrusion Detection
Firewall/VPN
Internet
Router
Mail Se
Message Security/Antivirus
Firewall
Web and FTP Virus Blocking
Intrusion Detection
VPN
Intrusion Detection
Management
Enterprise network
Security Breaches

Network perimetral security



Conectividad Un router gestiona la conexión, asegurado mediante TACACS+, lo que impide los accesos no autorizados al dispositivo.

Inspección Un firewall, mediante una política de seguridad basada en múltiples parámetros, revisa los accesos, y deniega cualquier intento no autorizado. Se autentifica al usuario y se encripta la conexión.

Gestión de ancho de banda Un gestor asigna los recursos necesarios a cada conexión, impidiendo problemas de seguridad derivados de abuso de recursos u originados por su escasez.

Virtual Private Networking Asegurando la conexión extremo a extremo, e impidiendo que el punto de acceso sea un riesgo, utilizamos cliente y servidor VPN seguros, con encriptación fuerte y autentificación.

Monitorización y gestión de alertas Todos los dispositivos anteriores generan y envían alertas, gestionadas por nuestro Network Control Center, así como logs y estadísticas.

Total Security Management Toda la información y los procesos anteriores están gestionados y dirigidos desde una autoridad de seguridad central, proactiva y con las máximas certificaciones profesionales.

CSI SPHERE