



GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Seguridad en Redes

Mecanismos de mitigación



GSI - Facultad de Ingeniería



GRUPO DE SEGURIDAD INFORMÁTICA

Redes Privadas Virtuales (VPN)



¿Qué es una VPN?

- Una estructura de red que permite el tráfico de información privada sobre una infraestructura de red pública
- Las redes privadas virtuales (VPN) tienen muchos años de existencia
- Se han utilizado muchas tecnologías para ello
- Uno de los modelos de VPN, muy popular (especialmente por su bajo costo), son las VPN sobre Internet



VPNs sobre Internet

- Aquí directamente estamos utilizando una red insegura para interconectar redes seguras
- Es imprescindible agregar seguridad
- La forma standard es mediante túneles y encriptación
- Grandes familias
 - IPSec
 - SSL
 - PPTP, L2TP



VPNs utilizando IPSec

- La forma estándar es utilizar IPSec en modo túnel entre equipos de ambas redes seguras
- Por ejemplo, entre los firewalls
- También entre un equipo conectado a Internet y el firewall de la empresa (Road Warriors), por ejemplo para acceso remoto desde el hogar o durante un viaje
- En la política de IPSec se configura qué tráfico debe ir por el túnel y cual no



Protección

- En las VPNs mediante IPSec, se conecta la red remota (o host remoto) directamente al equipo que termina el túnel
- El filtrado que se puede hacer es el mismo que se realiza en el firewall para cualquier red



VPNs usando SSL/TLS

- Diversos tipos de solución de VPN que utilizan como base SSL
- Algunos de ellos no son más que un proxy a través de una página web segura
 - En algunos casos esto puede ser una ventaja
 - Permite acceso a través de un navegador standard
- Otros permiten diversos tipos de acceso, llegando a una conexión remota completa
- Otras soluciones son más bien un híbrido. Ej: OpenVPN



Seguridad

- Un problema, si se utilizan para el acceso remoto, es la seguridad del equipo que se conecta
- En particular, las VPNs con SSL se suelen promocionar con “conéctese desde cualquier máquina con un navegador”.
- Hay que evaluar qué derechos de acceso se les da a los ingresos por estos caminos
- La granularidad de acceso suele ser mayor



VLAN Virtual LAN



VLAN (802.1Q)

- Mecanismo para definir distintos dominios de broadcast a nivel ethernet
- Normalmente se define a nivel de los switches de una LAN
- Usados para definir distintas zonas o segmentos de red (capa 2 - IP)
- Se pueden asociar a “grupos de puertos de uno o mas switches de comunicación” o “subredes IP”



Bibliografía y referencias

- **R. Anderson**, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2001.
- **D. Gollman**, *Computer Security*, Wiley, 2006.
- **W. Stallings**, *Cryptography and Network Security. 4ta. ed.* Prentice Hall, 2005