SOLUTECSA
SOLUCIONES DE TECNOLOGÍA S.A.

Protección de su Red

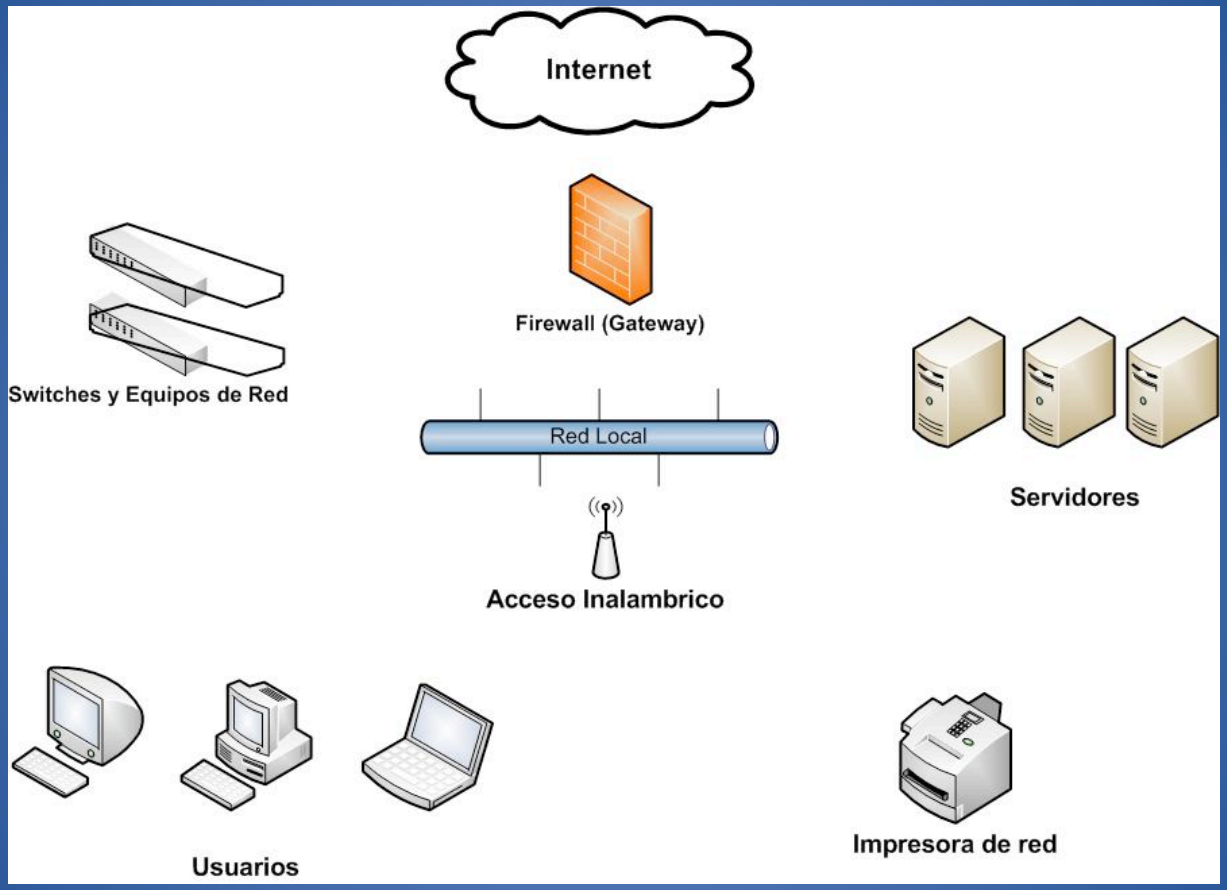
Ing. Teofilo Homsany
Gerente General
SOLUTECSA

Paitilla Mall, Local 45. Telefono: +507.209.4997 E-mail: ventas@solucionesdetecnologia.com

Áreas vulnerables de su red

- Gateway (entrada y salida a internet)
- Routers
- Switches
- Servidores
- Computadoras de empleados

Areas vulnerables de su red



Todas las áreas de su red son vulnerables a ataques por un intruso.

Gateway (Firewall, Routers)

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Ataques a servidor de Web.
- Ataques a servidor de correo.
- Debilidades en el Firewall y Router.

Switches y Routers

- ARP Poisoning
- Man – in – the – middle
- DNS Hijacking
- Wireless hacking

Servidores

- Robo de contraseñas usando sniffing.
- Acceso a servidores web sin certificados.
- SQL injection.
- XSS
- Sistemas sin parches.
- Carpetas compartidas sin permisos configurados.

Ataques a usuarios

- Phishing
- DNS Hijack
- Vulnerabilidades de programas instalados en equipos.
- Carpetas compartidas sin permisos configurados.
- Ingeniería Social

Como protegernos?

Revisión

- Se buscan los equipos conectados a la red.
- Se identifican servidores, estaciones de trabajo.
- Se identifican switches, routers, equipos vitales para la comunicación.

Detección

- Se detectan las debilidades con herramientas y métodos.
- Se identifican y dividen los problemas por área en la red.
- Se trata de explotar aquellas debilidades encontradas (dependiendo del caso).

Reporte

- Se documenta todo lo encontrado en un reporte.
- Este reporte debe contener información específica de cada sistema con debilidades y vulnerabilidades.
- En el reporte tambien se debe incluir las soluciones a los diversos problemas encontrados.

Validación

- Se revisan los puntos del reporte contra los sistemas afectados.
- Se levanta un plan de trabajo para dicho equipo en plan de asegurarlo.

Implementación

- Se le aplican los arreglos al equipo.
- Esto puede incluir:
  - Parches
  - Configuraciones especiales
  - Reinstalaciones

Protocolos de Autenticación

- Los dividimos en diferentes áreas:
  - Nivel de Red y Transporte (OSI)
  - Nivel de Aplicación
  - Nivel de Inalámbricos

Red y Transporte

- VPN
- IPSec
- Internet Key Exchange (IKE)

Aplicación

- SSL / TLS / HTTPS / SSH / SMIME
- SSL en detalle
- Kerberos
- PGP
- Ejemplos: PGP, Apache y SSL

Seguridad Inalámbrica

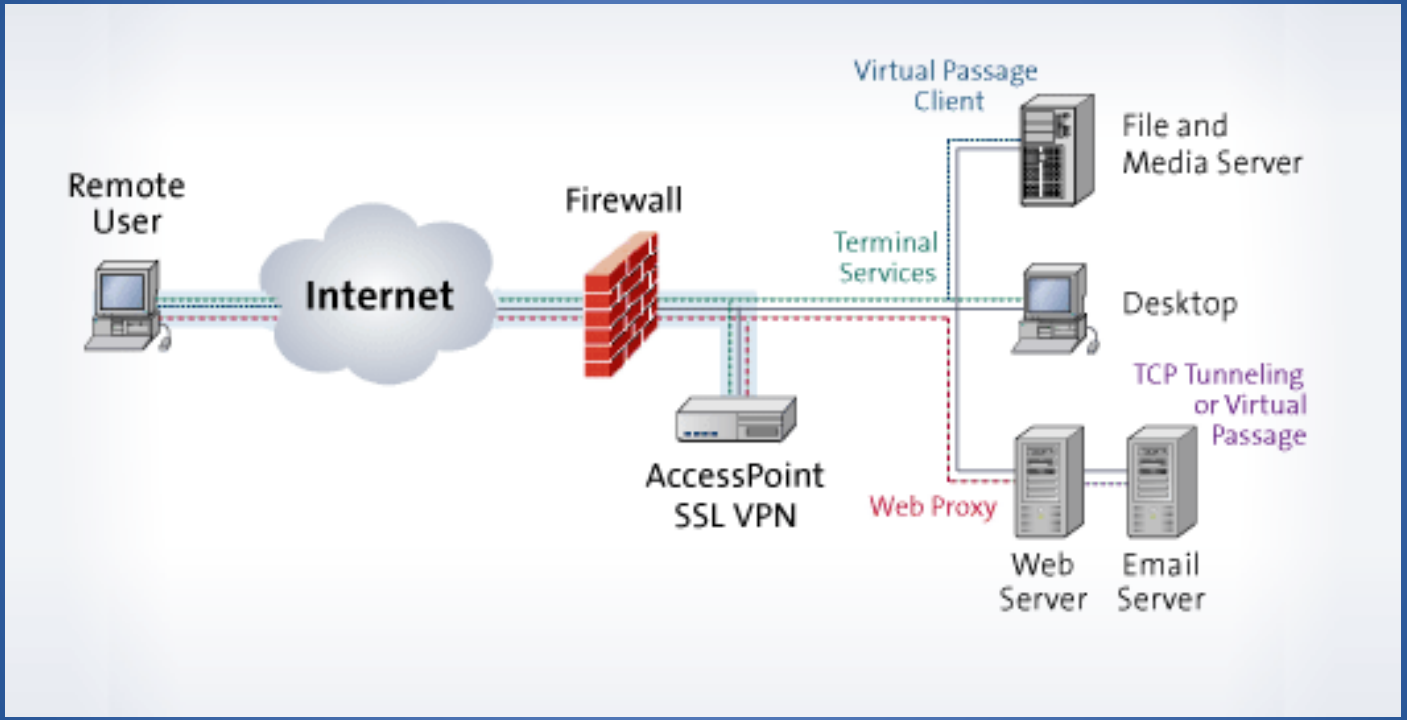
- Protocolos de seguridad inalámbrica.
  - WEP, WPA, WPA2
- Seguridad para dispositivos Bluetooth.
- UMTS (Seguridad de redes moviles GPRS)

Protocolos de Comunicación

Virtual Private Networks (VPN)

- El propósito básico del VPN es ofrecer autenticación, control de acceso, confidencialidad e integridad de la información.
- Un proceso llamado “Tunneling” activa la parte virtual del VPN.
- Hay dos tipos de protocolos de Tunneling:
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
- El servicio IPSec mantienen los paquetes privados, íntegros y autenticados.
  - IPSec AH Cabecera de autenticación.
  - IPSec ESP Encapsulating Security Payload.

Ejemplo de VPN



Seguridad de Aplicación

- SSL: Secure Socket Layer. Seguridad aplicada a nivel de la entrada a protocolos como FTP, Telnet y HTTP.
- TLS: Transport Layer Security = SSL 3.0 (TLS 1.0)
- HTTPS: HTTP sobre SSL/TLS
- SSH: Secure Shell soporta accesos remotos y los autentica. Es un programa y protocolo.
- SMIME: Protocolo de seguridad MIME. Formato para el seguro intercambio de correos.

Resistencia de SSL ante ataques

- Replay Attack: Numeros aleatorios dentro del SSL handshake previene ataques de replay.
- Man-in-the-middle: Cambio de llaves dinámicas a traves de reto y respuesta.
- Paquetes de un IP falso no pueden ser prevenidos porque SSL no ofrece protección para la capa de red y de transporte.

Seguridad de Redes Inalámbricas

- No usar los SSIDs por defecto que vienen con los equipos (nombre de la red).
- Esconder el SSID en el equipo para prevenir usuarios que buscan penetrar su red.
- Limitar acceso al equipo por direcciones MAC. (direcciones MAC pueden ser engañadas)
- Activar WPA o WPA2 para protección de la red.

Seguridad de Bluetooth

- Usar una llave de combinación entre los equipos.
- Reto y respuesta en la llave de enlace.
- Llave de encriptación para llave de enlace usando un numero aleatorio.

Preocupaciones de Seguridad Bluetooth

- Uso de una sola llave fija para autenticación causa problemas.
- La calidad del numero aleatorio puede ser muy debil dependiendo de las diferentes implementaciones.
- Seguridad depende de un numero PIN porque el reto de seguridad y la dirección son conocidos.

Seguridad Blackberry

- Ofrece seguridad mediante dos tipos de encriptación para transporte:
  - AES (Advanced Encryption Standard)
  - 3DES (Triple Data Encryption Standard)
- Llaves de encriptación son generadas para cada equipo para una autenticación bidireccional con el servidor.
- La comunicación viaja totalmente encriptada entre los servidores.

Aplica a usuarios con un Blackberry Enterprise Server.

Tecnología SwitchPort

- Tecnología usada en equipos para limitar el robo de direcciones MAC dentro de la red.
- Tipos de operación del Switchport:
  - Shutdown: El puerto se apaga y no permite mas conexiones. Esta función se deshabilita manualmente para reactivarlo.
  - Protect: Permite traficos de direcciones MAC conocidas y tumba cualquier paquete de MAC desconocidas.
  - Restrict: Funciona de la misma forma que el Protect pero envía notificación de que hubo una violación.

Que causa una alerta al Switchport?

- Cuando el máximo numero de direcciones MAC han sido agregadas a la tabla de direcciones y el mismo recibe una nueva solicitud.
- Cuando una dirección ya se ha visto previamente en otro switchport (MAC clonado).

Kerberos

- Protocolo de autenticación por red creado para autenticar usuarios, clientes y servidores entre ellos.
- El sistema usa criptografía con una llave secreta a traves de una red insegura.
- La comunicación entre cliente y servidor puede ser segura una vez se haya usado Kerberos para comprobar su identidad.

SSL

- Provee una conexión encriptada de equipo a equipo sin importar la plataforma ni el sistema operativo.
- Seguridad y servicios de autenticación son brindados por la encritación de data, autenticación de servidor, integridad del mensaje, y la autenticación del cliente por una conexión TCP como HTTPS, LDAP y POP3.

Protección contra ARP Spoofing

- No hay muchos metodos para prevenir este tipo de envenenamiento.
- El mas comun es usar entradas ARP estáticas.

Protección a nivel de una PC

- Antivirus
- Antispam
- Antispyware
- Controlador de dispositivos periféricos.
- Politicas centrales de dominio.

Como aseguro mi red?

- Para asegurar su red debe usar varias de las tecnologías a la vez.
- No hay una sola tecnología que protege todo.
- Ningun sistema es 100% seguro.
- Ninguna tecnología es 100% segura.
- Con revisiones periodicas su empresa puede minimizar los riesgos de robo de información.

Preguntas