Apuntes Tema 04 Acceso remoto

Contenido

Escenarios típicos con conexión a redes públicas

Arquitecturas de Red Habituales

Las empresas adoptan diversas arquitecturas para asegurar la conectividad y proteger sus datos. Aquí exploramos cuatro de las más comunes:

- **Red Corporativa a Internet**

Configuración básica donde la red interna se conecta directamente a Internet, generalmente protegida por un firewall perimetral.

- **Red con DMZ**
    - Se coloca una zona intermedia (la *DMZ*) para los servidores que deben ser accesibles desde Internet, como una web o un servidor de correo.
    - Si son atacados los servidores, **no puede entrar directamente a la red interna**, porque están separados por un firewall.
    - La red interna no puede ser accedida desde internet
- **Red Híbrida (Local + Nube)**

Una empresa usa **sus propios equipos y servidores en el edificio** (local) y además usa **servicios en Internet** (nube), todo funcionando junto.

- **Sedes Remotas con VPN**

Permite conectarse de forma segura a la red corporativa a través de túneles VPN cifrados.

Amenazas Comunes en Sistemas Expuestos

Cuando un sistema está directamente accesible desde Internet, se convierte en un blanco potencial para una variedad de ataques.

Escaneos Masivos

Técnicas de reconocimiento (como Nmap o Shodan) para descubrir puertos abiertos, servicios activos y vulnerabilidades potenciales en los sistemas. Son el primer paso para un ataque.

Ataques de Fuerza Bruta

Intentos automatizados y repetitivos para adivinar credenciales (contraseñas, claves) probando miles de combinaciones. Un método muy común para obtener acceso no autorizado.

Sniffing y MiTM

- El "sniffing" intercepta el tráfico de red,
- "Man-in-the-Middle" permite al atacante interponerse en una comunicación, leerla y modificarla sin ser detectado, comprometiendo la confidencialidad.

Vulnerabilidades en Servicios Públicos

Fallos de seguridad en aplicaciones o servicios expuestos (FTP, RDP, HTTP, SSH) que pueden ser explotados.

Técnicas de Fortificación para Sistemas Expuestos

Para proteger los sistemas accesibles desde internet, es crucial implementar diversas estrategias de seguridad que reduzcan la superficie de ataque y mitiguen los riesgos.

Firewall Perimetral

Una barrera de seguridad esencial que controla el tráfico de red entre la red interna y externa, aplicando reglas predefinidas para permitir o denegar comunicaciones.

NAT / PAT

- NAT: Cambia IP privada por IP pública
- PAT: Cambia IP y también usa puertos para diferenciar a cada equipo

Oculta la topología interna y haciendo que los sistemas internos sean inaccesibles directamente desde internet.

IDS / IPS

Los Sistemas de Detección de Intrusos (IDS) y Prevención de Intrusos (IPS) monitorizan el tráfico de red en busca de actividades maliciosas o violaciones de políticas, alertando o bloqueando las amenazas en tiempo real.

Suricata, Cisco Firepower, ..

Segmentación de Red (VLANs)

- Divide la red en subredes lógicas más pequeñas (VLANs)
- Limita el impacto de una posible brecha
- Aísla diferentes tipos de tráfico y sistemas, como servidores, usuarios o DMZ.

Bastionado de Servidores

Es el proceso de **hacer un servidor más seguro** antes de ponerlo en Internet.

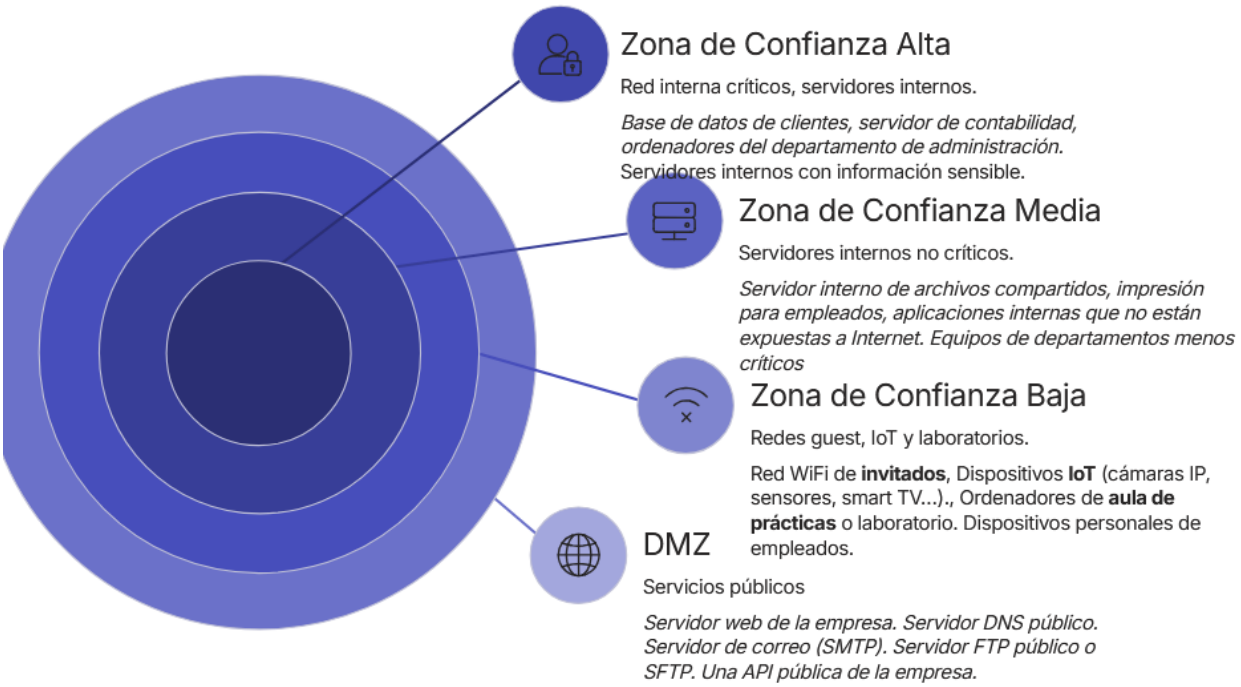
Consiste en cosas como:

- **Quitar lo que no se usa** (servicios, programas...).
- **Configurar bien** lo que sí se usa (por ejemplo, SSH, Apache, ...).
- **Actualizar** el servidor para cerrar fallos.
- **Controlar quién puede entrar** y cómo (contraseñas fuertes, claves, firewall...).

Clasificación de zonas de riesgo según seguridad perimetral

Capas de Seguridad Perimetral

La seguridad perimetral divide una red en distintas zonas, cada una con un nivel de confianza y protección diferente, creando una defensa en profundidad.



Esta segmentación es fundamental para contener posibles brechas y limitar el acceso de amenazas a los recursos más valiosos de la organización.

Principios de seguridad perimetral

Este enfoque clasifica la red en áreas con diferentes niveles de confianza y acceso.

Segmentación de Red

Divide la infraestructura en zonas aisladas, desde las más débiles y expuestas hasta las más fuertes y protegidas. El acceso entre ellas está estrictamente controlado.

Principio de Mínimo Privilegio

En cada zona, se otorga a usuarios y sistemas solo el acceso necesario para realizar sus funciones, reduciendo la superficie de ataque y el impacto de una posible brecha.

Control Estricto de Tráfico

Se definen políticas claras sobre qué tipo de tráfico se permite entre zonas, utilizando firewalls y otros dispositivos de seguridad para aplicar estas reglas.

Riesgos por Zona

Exposición Directa a Internet

Los sistemas y servicios directamente accesibles desde la red pública son blancos constantes de ataques, explotaciones de vulnerabilidades y escaneos maliciosos.

Riesgos de Dispositivos Móviles

La salida de dispositivos (portátiles, smartphones) fuera del perímetro controlado introduce riesgos de pérdida, robo, conexiones inseguras a redes públicas y propagación de malware.

Accesos Remotos y Teletrabajo

La conexión a la red corporativa desde ubicaciones externas (VPN, RDP) abre vectores de ataque como credenciales débiles, dispositivos personales no seguros y redes domésticas comprometidas.

Protocolos seguros de comunicación

Protocolos seguros y su propósito

La implementación de protocolos de comunicación seguros es fundamental para proteger la **confidencialidad, integridad y disponibilidad** de la información en sistemas expuestos a redes públicas.

HTTPS

Asegura la comunicación en la web, cifrando los datos entre el navegador y el servidor.

SSH

Permite la administración remota segura de servidores y equipos, con autenticación robusta y cifrado.

SFTP / SCP

Para la transferencia segura de archivos sobre SSH, garantizando la privacidad y la integridad de los datos.

IPsec

Crea túneles de VPN seguros entre redes (site-to-site) o entre un host y una red (host-to-network).

OpenVPN / WireGuard

Soluciones VPN modernas y flexibles para crear conexiones seguras punto a punto o acceso remoto.

SMTP(S), IMAP(S), POP3(S)

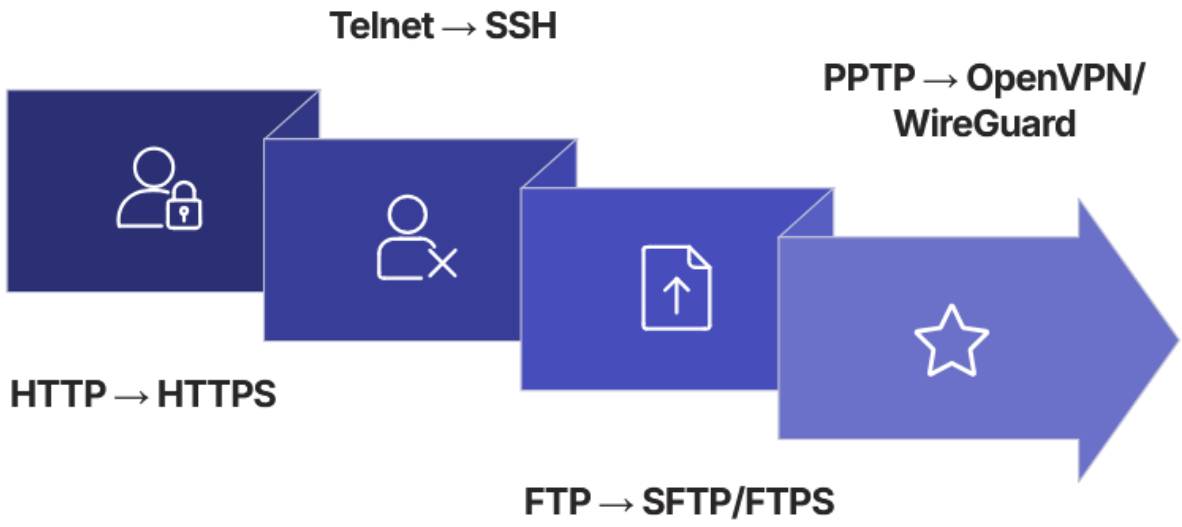
Extensiones seguras de los protocolos de correo electrónico para cifrar las comunicaciones y proteger los mensajes.

Escritorio remoto de Windows

Asegura el acceso remoto al escritorio, requiriendo autenticación antes de establecer una sesión completa.

Migración a Protocolos Seguros

La evolución de las amenazas cibernéticas exige el abandono de protocolos heredados e inseguros en favor de alternativas que garanticen la confidencialidad e integridad de la información.



Certificados Digitales: Pilares de la Confianza Online

Los certificados digitales son credenciales electrónicas que vinculan la identidad de una entidad (persona, servidor, organización) con un par de claves criptográficas, garantizando la autenticidad y seguridad en las comunicaciones.

Autoridad de Certificación (CA)

- Entidad de confianza que emite y valida los certificados, confirmando la identidad del titular.
- Garantiza que la clave pública pertenece a quien dice ser.

Autenticación y Confidencialidad

- Permiten verificar la identidad de servidores y clientes, y cifrar la información para que solo los destinatarios autorizados puedan leerla, protegiendo la privacidad.

Handshake TLS

- Proceso inicial donde cliente y servidor negocian parámetros de seguridad, intercambian certificados y establecen una clave de sesión simétrica para la comunicación cifrada.