Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 3

Exploring Network Technologies and Tools — Tecnologías y Herramientas de Red

---

Este material es un **resumen conceptual elaborado con palabras propias**, pensado como guía de apoyo para estudiar junto al libro original en inglés. No es una traducción ni una reproducción del texto original; cubre los mismos temas, en el mismo orden, para facilitar el repaso en español.

Incluye: resumen por secciones, tablas de puertos y protocolos, glosario EN↔ES y preguntas de práctica originales.

1. Modelo OSI y Protocolos Básicos

El modelo OSI describe, en 7 capas teóricas, todas las actividades que ocurren en una red. Cuanto más bajo el número de capa, más cerca del cableado físico; cuanto más alto, más cerca del usuario y el software.

Capa	Nombre	Qué maneja
1	Física	Cables de cobre, fibra óptica, ondas de radio.
2	Enlace de datos	Switches; usa direcciones MAC para enviar tramas en la red local.
3	Red	Routers; usa direcciones IP para enviar tráfico entre redes distintas.
4	Transporte	TCP y UDP; comunicación de extremo a extremo entre aplicaciones.
5	Sesión	Establece, gestiona y termina sesiones entre aplicaciones.
6	Presentación	Traduce datos a un formato estándar; cifrado y compresión.
7	Aplicación	Servicios de red usados directamente por las aplicaciones.

Es común escuchar 'problema de Capa 3' para referirse a un problema de enrutamiento, o 'Capa 2' para uno de switching. No hace falta memorizar el modelo en profundidad para el examen, solo saber qué hace cada capa.

1.1 Protocolos básicos

- **TCP:** orientado a conexión, con entrega garantizada. Usa el 'saludo de tres vías' (three-way handshake): SYN → SYN/ACK → ACK.
- **UDP:** sin conexión, entrega 'mejor esfuerzo' sin garantías. Muchos ataques de denegación de servicio (DoS) usan UDP.
- **IP:** identifica hosts y entrega tráfico mediante direcciones IP. IPv4 usa direcciones de 32 bits (ej. 192.168.1.100); IPv6 usa 128 bits en hexadecimal.
- **ICMP:** prueba conectividad básica (ping, tracert). Muy usado en ataques DoS, por eso suele bloquearse en firewalls.
- **ARP:** resuelve direcciones IPv4 a direcciones MAC dentro de la subred de destino. Los ataques de 'ARP poisoning' explotan este protocolo.

2. Protocolos por Caso de Uso

2.1 Transferencia de datos (inseguros vs. seguros)

Inseguro	Alternativa segura	Puerto
FTP (texto plano)	SFTP (usa SSH) / FTPS (usa TLS)	22 (SFTP)
Telnet (texto plano)	SSH	22
SSL (comprometido, ataque POODLE)	TLS	—
HTTP	HTTPS (usa TLS)	443

SSH (puerto 22) también sirve para cifrar otros protocolos: **SCP** (copia de archivos) y **SFTP** se apoyan en SSH. **IPsec** cifra tráfico IP en general (se profundiza en el capítulo 4).

2.2 Correo electrónico y web

Protocolo	Función	Puerto sin cifrar / cifrado
SMTP	Envía correo entre clientes y servidores.	25 / 587 (TLS)
POP3	Descarga correo del servidor al cliente.	110 / 995
IMAP	Gestiona correo en carpetas en el servidor.	143 / 993
HTTP/HTTPS	Tráfico web.	80 / 443
LDAP/LDAPS	Consultas a directorios (ej. Active Directory).	389 / 636

2.3 Seguridad de correo — SPF, DKIM y DMARC

- **SPF:** usa registros DNS para definir qué direcciones IP están autorizadas a enviar correo en nombre de un dominio.
- **DKIM:** usa criptografía de clave pública para firmar y verificar el dominio y el contenido de un correo.
- **DMARC:** se apoya en SPF y DKIM, define qué hacer con los correos que fallan la verificación, y genera reportes de cumplimiento.

Juntos, SPF, DKIM y DMARC forman un marco robusto contra el phishing y la suplantación de dominio (email spoofing). Los **gateways de correo** son dispositivos/software que filtran spam y malware entre el correo interno y el externo.

2.4 Voz, video, tiempo y acceso remoto

- **RTP / SRTP:** RTP transporta audio y video (VoIP, streaming); SRTP añade cifrado, autenticación e integridad.

- **SIP:** inicia, mantiene y termina sesiones de voz/video/mensajería (mensajes en texto plano, útiles para logs forenses).
- **SSH y RDP:** reemplazan a Telnet para administración remota. RDP usa el puerto TCP 3389.
- **NTP:** sincroniza la hora entre sistemas (ej. Kerberos exige que los relojes no difieran más de 5 minutos).

2.5 OpenSSH y autenticación sin contraseña

OpenSSH es un conjunto de herramientas que simplifica el uso de SSH. Permite generar un par de claves (pública/privada) con `ssh-keygen` y copiar la clave pública al servidor remoto con `ssh-copy-id`. Así se puede iniciar sesión sin escribir contraseña cada vez, usando la clave privada (que siempre debe permanecer solo en el equipo del usuario).

3. Resolución de Nombres (DNS)

DNS traduce nombres de host a direcciones IP. Los servidores DNS almacenan zonas (bases de datos) con distintos tipos de registros:

- **A:** nombre de host → dirección IPv4.
- **AAAA:** nombre de host → dirección IPv6.
- **PTR:** dirección IP → nombre (búsqueda inversa; opcional).
- **MX:** identifica el servidor de correo; el de menor número de preferencia es el principal.
- **CNAME:** alias — permite que un mismo sistema tenga varios nombres.
- **SOA:** información de la zona, incluido el TTL (tiempo que un cliente cachea el resultado).

DNSSEC protege contra el envenenamiento de caché DNS (DNS poisoning) agregando una firma digital (RRSIG) a cada registro, garantizando integridad y autenticidad de las respuestas.

4. Dispositivos de Red y Endurecimiento (Hardening)

4.1 Switches

Los switches conectan dispositivos dentro de una red local y dirigen el tráfico unicast solo al puerto correcto (según la dirección MAC aprendida), a diferencia de un hub, que reenvía todo a todos los puertos. Esto reduce el riesgo de que un atacante capture tráfico ajeno con un analizador de protocolos.

- **Seguridad de puertos (port security):** deshabilitar puertos sin uso y limitar cuántas direcciones MAC puede aceptar cada puerto (filtrado MAC).
- **STP / RSTP:** previenen bucles de switching (switching loops) y tormentas de broadcast, por ejemplo si alguien conecta dos puertos del switch entre sí con un cable.
- **BPDU Guard:** detecta mensajes BPDU inesperados en puertos de borde (donde se conectan dispositivos finales, no otros switches) y deshabilita el puerto ante un posible ataque.

4.2 Routers

Los routers conectan múltiples segmentos de red y no reenvían tráfico broadcast, lo que reduce el tráfico en cada segmento. Usan **listas de control de acceso (ACL)** para filtrar tráfico según direcciones IP, puertos y protocolos.

Denegación implícita (implicit deny): todo lo que no está explícitamente permitido en la ACL queda bloqueado por la última regla de la lista. Es el punto de partida seguro tanto en routers como en firewalls.

SNMP: monitorea y gestiona dispositivos de red mediante notificaciones llamadas 'SNMP traps'. SNMPv1/v2 envían las credenciales en texto plano (inseguro); **SNMPv3** las cifra. Usa los puertos UDP 161 y 162.

5. Firewalls

Tipo	Qué hace
Basado en host (host-based)	Protege un único equipo (ej. Microsoft Defender Firewall).
Basado en red (network-based)	Protege toda una red; se ubica en el borde del perímetro.
Sin estado (stateless)	Filtra cada paquete de forma aislada, usando reglas de ACL (como un router).
Con estado (stateful)	Rastrea sesiones y bloquea tráfico que no corresponde a una sesión establecida (ej. TCP sin handshake previo). También llamado firewall de Capa 4.
WAF (Web Application Firewall)	Protege una aplicación web específica contra ataques como XSS; se ubica entre el servidor web y sus clientes, además del firewall de red.
NGFW (próxima generación)	Inspección profunda de paquetes a nivel de aplicación. Se lo considera un firewall de Capa 7, igual que un WAF.

Modos de falla (failure modes): un sistema *fail-open* deja pasar todo el tráfico si falla (no hay interrupción, pero tampoco seguridad); un sistema *fail-closed* bloquea todo si falla (hay interrupción, pero se mantiene la seguridad). Los profesionales de seguridad suelen preferir fail-closed.

6. Diseño de Red: Zonas y Segmentación

- **Intranet:** red interna de la organización. **Extranet:** parte de la red accesible por terceros autorizados (socios, clientes, proveedores).
- **Subred filtrada / DMZ (screened subnet):** zona intermedia entre Internet y la red interna, protegida por dos firewalls. Aloja servidores accesibles desde Internet (web, correo, VPN) sin exponer directamente la red interna.
- **NAT (Network Address Translation):** traduce direcciones IP privadas a públicas y viceversa, ocultando los equipos internos de Internet. *NAT estática* = mapeo 1 a 1; *NAT dinámica* = mapeo de muchas IP privadas a un pool de IP públicas.
- **Air gap / aislamiento físico:** un sistema literalmente no está conectado a ninguna otra red (ej. sistemas SCADA críticos).
- **VLAN:** segmentación lógica dentro de un switch, agrupando equipos por función o departamento sin importar su ubicación física. También separa tipos de tráfico (ej. voz en una VLAN, datos en otra).
- **Tráfico este-oeste vs. norte-sur:** este-oeste es el tráfico entre servidores; norte-sur es el tráfico entre clientes y servidores.

7. Aplicaciones y Dispositivos de Red (Appliances)

- **Proxy directo (forward proxy):** reenvía solicitudes de clientes internos hacia Internet. Mejora el rendimiento cacheando contenido y permite filtrado de contenido/URL según categorías (malware, contenido inapropiado, etc.). Puede ser centralizado o basado en agente (instalado en cada equipo).
- **Proxy inverso (reverse proxy):** recibe solicitudes desde Internet y las reenvía a uno o varios servidores web internos; también sirve como balanceador de carga para una granja de servidores.
- **UTM (Unified Threat Management):** un solo dispositivo que combina varias funciones de seguridad — filtrado de URL, inspección de malware, inspección de contenido y mitigación de DDoS — simplificando la administración.
- **Jump server:** servidor endurecido (hardened) usado como puente para administrar equipos en otra zona de seguridad (ej. acceder a la DMZ desde la red interna) sin exponer esa zona directamente.

8. Confianza Cero (Zero Trust)

El modelo tradicional confiaba en todo lo que estaba 'dentro' del perímetro protegido por firewalls. Con el trabajo remoto y la nube, esa frontera dejó de ser clara. El enfoque de **Zero Trust Network Access (ZTNA)** no confía automáticamente en nadie por su ubicación de red; en cambio, exige autenticación fuerte y controles de acceso basados en políticas y en la identidad del usuario, con el objetivo de reducir el alcance de las amenazas (threat scope reduction).

- **Autenticación de identidad adaptativa:** el nivel de exigencia de autenticación cambia según el contexto (ej. red corporativa vs. cafetería con dispositivo personal).
- **Plano de control (control plane):** red usada para configurar y controlar la infraestructura. Incluye el *Policy Engine (PE)*, que decide si otorgar acceso, y el *Policy Administrator (PA)*, que comunica esa decisión. Juntos forman el *Policy Decision Point (PDP)*.
- **Plano de datos (data plane):** red donde circula el tráfico real de usuarios y aplicaciones. Incluye al sujeto, el sistema que usa, el recurso al que quiere acceder, y el *Policy Enforcement Point (PEP)* — el único componente que cruza entre ambos planos, ya que recibe instrucciones del plano de control y las aplica en el plano de datos.

SASE (Secure Access Service Edge): filosofía de diseño relacionada con Zero Trust que combina funciones de red y seguridad como servicio en la nube: firewall, gateway web seguro, anti-malware, prevención de intrusiones, CASB y prevención de pérdida de datos (DLP), todo integrado.

9. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
OSI Model	Modelo OSI	Modelo de 7 capas que describe las comunicaciones de red.
TCP / UDP	TCP / UDP	Protocolo orientado a conexión / sin conexión.
Implicit deny	Denegación implícita	Todo lo no permitido explícitamente queda bloqueado.
ACL	Lista de control de acceso	Reglas que permiten o bloquean tráfico.
Screened subnet / DMZ	Subred filtrada / DMZ	Zona intermedia entre Internet y la red interna.
NAT	Traducción de direcciones de red	Traduce IP privadas a públicas y viceversa.
Air gap	Aislamiento físico (air gap)	Ausencia total de conexión entre redes.
VLAN	Red virtual local	Segmentación lógica de tráfico dentro de un switch.
Stateful / stateless firewall	Firewall con/sin estado	Con estado rastrea sesiones; sin estado filtra paquete por paquete.
WAF	Firewall de aplicación web	Protege aplicaciones web específicas.
NGFW	Firewall de próxima generación	Inspección profunda a nivel de aplicación (Capa 7).
Fail-open / fail-closed	Falla abierta / falla cerrada	Comportamiento del sistema de seguridad ante un fallo.
Forward / reverse proxy	Proxy directo / inverso	Reenvía solicitudes salientes / entrantes.
UTM	Gestión unificada de amenazas	Combina varias funciones de seguridad en un dispositivo.
Jump server	Servidor de salto	Puente endurecido entre zonas de seguridad distintas.
Zero trust	Confianza cero	No confiar por ubicación de red; verificar siempre identidad y contexto.

Inglés	Español	Definición breve
Policy Enforcement Point (PEP)	Punto de aplicación de políticas	Aplica las decisiones de acceso entre plano de control y de datos.
SASE	SASE	Red y seguridad entregadas como servicio integrado en la nube.
SPF / DKIM / DMARC	SPF / DKIM / DMARC	Estándares de autenticación de correo contra phishing y spoofing.
DNSSEC	DNSSEC	Extensiones de seguridad DNS que firman digitalmente los registros.
LDAP / LDAPS	LDAP / LDAPS	Protocolo de consulta de directorios / su versión cifrada con TLS.

10. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 3. Las respuestas están al final.

1. Un consultor detecta que los administradores usan Telnet para configurar switches vía interfaz web. ¿Qué protocolo debería reemplazarlo para cifrar la sesión completa?

2. Una empresa necesita monitorear y configurar remotamente sus routers, protegiendo la confidencialidad de las credenciales. ¿Qué versión de SNMP deberían usar?

3. Un firewall tiene solo dos reglas: permitir tráfico TCP en el puerto 80 y permitir tráfico TCP en el puerto 443. No hay ninguna otra regla explícita. ¿Qué pasa con el resto del tráfico?

4. Una organización quiere alojar un servidor web accesible al público sin exponer directamente la red interna. ¿Dónde debería ubicarse ese servidor?

5. Una planta de energía tiene computadoras de monitoreo que nunca deben conectarse a ninguna red, ni siquiera a la red interna. ¿Qué técnica de aislamiento es la más adecuada?

6. Un administrador detecta tráfico TCP en la red que no corresponde a ninguna sesión con three-way handshake previo. ¿Qué tipo de firewall detectaría y bloquearía mejor este tráfico?

7. Una empresa quiere separar el tráfico de voz (VoIP) del tráfico de datos normales dentro del mismo switch físico, sin necesidad de cambiar el cableado. ¿Qué tecnología deberían usar?

8. Un sitio web recibe un ataque de cross-site scripting (XSS). ¿Qué dispositivo de seguridad está específicamente diseñado para prevenir este tipo de ataque?

9. Un administrador quiere acceder a servidores en la DMZ desde la red interna sin exponer esos servidores directamente. ¿Qué tipo de servidor debería usar como intermediario?

10. Una organización adopta un modelo donde no confía en ningún dispositivo solo por estar dentro de la red corporativa, y en cambio verifica identidad y contexto en cada solicitud de acceso. ¿Cómo se llama este enfoque?

Respuestas

1. TLS (Transport Layer Security) — SSL está deprecado por vulnerabilidades como POODLE, por lo que TLS es la opción correcta para mantener la misma interfaz de navegador de forma cifrada.

2. SNMPv3 — es la única versión que cifra las credenciales antes de enviarlas por la red.

3. Se bloquea por la regla de denegación implícita (implicit deny), que es la última regla por defecto en toda ACL o firewall.

4. En una subred filtrada / DMZ (screened subnet) — permite acceso público controlado sin exponer la red interna.

5. Aislamiento físico o 'air gap' — no debe existir ninguna conexión, ni siquiera a la red interna.

6. Un firewall con estado (stateful firewall) — analiza el estado de la sesión y bloquea tráfico TCP que no corresponde a una conexión establecida.

7. VLAN (red virtual local) — permite separar lógicamente el tráfico de voz y de datos usando el mismo switch físico.

8. Un WAF (Web Application Firewall) — está diseñado específicamente para proteger aplicaciones web de ataques como XSS.

9. Un jump server (servidor de salto) — sirve de puente endurecido entre la red interna y la DMZ.

10. Confianza cero (Zero Trust / ZTNA) — verifica identidad y contexto en cada acceso, sin confiar por ubicación de red.
