FORTINET NSE 4 — FORTIOS ADMINISTRATOR

CATÁLOGO DE TEMAS OFICIALES PARA EL EXAMEN DE CERTIFICACIÓN FCP

Este catálogo detalla el desglose completo del contenido oficial requerido para superar el examen de certificación **Fortinet Certified Professional (FCP) - Network Security / NSE 4 (FortiOS Administrator)**. Es una guía de referencia fundamental para administradores de red dedicados a la implementación, gestión y soporte de firewalls de la familia FortiGate.

1. Configuración de Sistema y Despliegue (System & Deployment)

Peso: 15% - 20%

- **Instalación y Configuración Inicial:**
  - Modos de operación (Modo NAT/Ruta vs. Modo Transparente).
  - Gestión de licencias, interfaces de red locales y actualización segura de firmware de FortiOS.
- **Sistemas de Diagnóstico y Monitoreo:**
  - Configuración de registros locales (logging) e integración con FortiAnalyzer y FortiCloud.
  - Diagnóstico y troubleshooting de recursos de sistema (CPU, memoria, logs de fallos).
- **Alta Disponibilidad (HA) y Virtualización:**
  - Configuración y operación de clústeres FGCP en modos Activo-Pasivo y Activo-Activo.
  - Entendimiento de Virtual Domains (VDOMs) para segmentar el firewall físicamente en múltiples instancias lógicas.
  - Introducción de escenarios de nube (FortiGate VM / FortiGate CNF) y onboarding en FortiSASE.

2. Políticas de Firewall y Autenticación (Firewall Policies & NAT)

Peso: 25% - 30%

- **Políticas de Firewall:**
  - Lógica de procesamiento y coincidencia de reglas de firewall de arriba hacia abajo (Top-Down matching).
  - Creación de políticas de IPv4 e IPv6, reglas implícitas de denegación y su respectiva configuración de logs.
- **Traducción de Direcciones de Red (NAT):**
  - Configuración de Source NAT (SNAT) y Destination NAT (DNAT).
  - Uso e implementación de Virtual IPs (VIPs) para mapear IPs públicas a servidores internos.
  - Diferencias operativas entre NAT Central (Central NAT) y NAT basado en políticas tradicionales.
- **Autenticación de Usuarios y FSSO:**
  - Métodos de autenticación local y remota (Active Directory, LDAP, RADIUS) dentro de las políticas de firewall.
  - Implementación, flujo y resolución de problemas con Fortinet Single Sign-On (FSSO).

3. Inspección de Contenido (Content Inspection / Security Profiles)

Peso: 20% - 25%

- **Inspección SSL/TLS (Descifrado de Tráfico):**
  - Configuración de inspección de certificados (Certificate Inspection) frente a inspección profunda (Deep Inspection).
  - Gestión de certificados CA para evitar advertencias de seguridad en los navegadores clientes.
- **Modos de Inspección de FortiOS:**
  - Diferencias arquitectónicas entre la inspección basada en proxy (Proxy-based) y la inspección basada en flujo (Flow-based).
- **Perfiles de Seguridad:**
  - **Web Filtering:** Bloqueo por categorías de FortiGuard, URLs estáticas y cuotas de navegación.
  - **Application Control:** Monitoreo y bloqueo de aplicaciones específicas o comportamientos en la red.
  - **Antivirus:** Configuración de escaneos para mitigar malware en tránsito.
  - **Intrusion Prevention System (IPS):** Protección contra vulnerabilidades conocidas, exploits de red y control de firmas de ataque.

4. Enrutamiento y SD-WAN (Routing & SD-WAN)

Peso: 10% - 15%

- **Enrutamiento IP:**
  - Configuración de rutas estáticas IPv4 e IPv6, rutas de host, por defecto y flotantes.
  - Principios de enrutamiento dinámico (BGP básico y OSPF) en FortiOS.
  - Prioridades de rutas estáticas frente a distancias administrativas en la tabla de enrutamiento local.
- **Redes Definidas por Software (SD-WAN):**
  - Configuración de interfaces miembros de SD-WAN y zonas.
  - Configuración de Performance SLAs (pruebas de salud a través de ping, http, dns) para evaluar latencia, pérdida de paquetes y jitter.
  - Reglas de SD-WAN (estrategias de selección de enlaces: Best Quality, Lowest Cost, Manual, SLA).

5. Redes Privadas Virtuales (VPN - IPsec & SSL)

Peso: 15% - 20%

- **IPsec VPN (Túneles de Sitio a Sitio):**
  - Entendimiento de la negociación IKE Fase 1 (propuestas, encriptación, DH) y Fase 2 (Quick Mode).
  - Configuración de VPNs de sitio a sitio malladas (Meshed) y parcialmente redundantes.
  - Instalación y configuración de VPN Dial-up para usuarios remotos.
- **SSL VPN:**
  - Diferencias fundamentales entre el Modo Web (sin agente) y el Modo Túnel (utilizando FortiClient).
  - Configuración de portales de usuarios, asignación de rangos IP dinámicos y mapeo de políticas.
  - Diagnóstico y troubleshooting de fallas de conexión VPN comunes en consola CLI.

💡 Recomendaciones Clave para Rendir el Examen:

El examen de FortiOS Administrator evalúa tanto conceptos de diseño de políticas de seguridad como la habilidad práctica de interpretar salidas de depuración en consola (CLI Debugs) y el orden de procesamiento de paquetes del kernel. Se recomienda encarecidamente simular topologías con máquinas virtuales en entornos EVE-NG, GNS3 o mediante laboratorios oficiales del Fortinet Training Institute.