

Syllabus del Curso de Sophos Firewall y Zentyal, Seguridad Defensiva con GNS3, AD, VLANs, Proxy, DPI, VPN, WAF, IPS, DOS, HotSpot

Introducción

- Introducción a los firewalls.
- Firewalls de red, UTM y NG
- Sophos Firewall, historia
- Ciclo de Vida de las versiones de Sophos Firewall
- Funcionalidades de Sophos Firewall
- Escenarios de Despliegue

Instalación de Xubuntu 20.04 y GNS3

- Configuración del sistema operativo.
- Configuración de IP Pública
- Configuración de red virtual en netplan
- Acceso Remoto por SSH
- Reglas IPtables para configurar a Linux como router
- Configuración de Acceso remoto rdp en Xubuntu
- Instalación de GNS3
- Instalación de Máquina Virtual Windows
- Creación del router virtual

Instalación de Sophos Firewall 18.5

- Configuración en GNS3 de la red LAN y WAN
- Agregación de switches en GNS3
- Creación de la máquina virtual Sophos Firewall XG con Qemu KVM
- Instalación de Sophos Firewall Home
- Registro de Sophos ID y Key de Sophos XG
- Configuración inicial de Firewall Sophos
- Configuración de la IP pública
- Configuración de la licencia y sincronización
- Actualización del Firmware de Sophos
- Prueba de Navegación a internet desde Windows.

Configuración Básica de Reglas de Firewall y NAT Vinculado

- Reglas de Firewall de LAN a WAN
- Reglas de NAT Vinculados
- Configuración de NAT Fuente
- Gestión de Objetos de Red

Servidor de Directorio Activo con Windows Server 2016

- Introducción al directorio activo
- Descarga de trial e Instalación de máquina virtual Windows Server 2016
- Definición del Dominio Windows
- Configuración Inicial del Bosque
- Creación de Unidades Organizativas, Usuarios y Grupos
- Prueba de estaciones windows enlazados al dominio AD
- Políticas de grupo (GPO)

Servidor de Directorio Activo con Zentyal Server 7

- Descarga de Zentyal Developer Edition 7
- Instalación de Zentyal Developer Edition 7
- Definición del Dominio Windows
- Despliegue de AD
- Configuración de DNS Server
- Creación de Unidades Organizativas, Usuarios y Grupos
- Prueba de estaciones windows enlazados al dominio AD Zentyal
- Políticas de grupo (GPO)
- Servidor de Archivos en Zentyal
- Migración de Windows Server a Zentyal

Filtrado Web y Filtrado de Aplicaciones, Inspección SSL, Intercepción SSL.

- Capa de Identidad Layer 8
- Integración de Sophos XG a Active Directory Windows Server
- Integración de Sophos Firewall con Zentyal.
- Configuración de STAS en Windows Server
- Filtrado Web e Inspección SSL
- Despliegue de certificado SSL por medio de GPO
- Políticas de Filtrado Web para usuarios y grupos de ADS
- Intercepción SSL.
- Filtrado de Aplicaciones
- Reportes y monitores en tiempo real.

Configuración de Switch Cisco con VLANs, trunking con SophosXG

Calle Marginal de la Selva 587, Urb. Tambo de Monterrico, Santiago de Surco, Lima, Perú.

WhatsApp: +51 922 394 498 +51 922 414 392

informes@aulautil.com - <https://aulautil.com>

- Instalación en GNS3 de Switch Core Cisco con soporte de VLANs
- Reconfiguración de las redes LAN,
- Creación de VLANs para servidores y PCs
- Configuración de Trunk y VLANs con SophosXg y Switch core
- Reconfiguración de STAS en Windows Server
- Pruebas de capa de identidad, filtrado Web y de Aplicaciones con las VLANs
- Configuración en Sophos restricción de acceso entre las VLANs.

Configuración de DMZ, Instalación del Sistema Operativo de Servidor Rocky Linux 8

- Habilitación de Red DMZ en Sophos Firewall
- Instalación de Rocky Linux 8
- Instalación de Servidor Apache en Rocky Linux
- Configuración de Reglas de Firewall para DMZ
- Regla de Salida para Servidor DMZ
- Regla de NAT de servicios para DMZ
- Reglas de VLANs a DMZ

Configuración de VPN Site2Site y VPN Móvil (SSL e IPsec)

- Instalación de Sophos XG en una sucursal con Ip dinámica
- Configuración de VPN SSL Site2Site
- Configuración de VPN IPsec Site2Site
- Reglas y restricciones de la VPN a LAN
- Reglas y restricciones de la VPN a DMZ
- Configuración de VPN Móvil en Linux y Windows
- Sophos Connect y Sophos VPN SSI
- Pruebas de Conexión

Configuración de DNS Público y Certificados Letsencrypt

- Resolución de nombres local y en red
- Registro de Dominio Público
- Configuración de DNS Público, registros de DNS en Freenom
- Zonas de Dominio y Registros MX, PTR y SPF
- Certificados Letsencrypt
- Generación de certificado para dominio único y múltiples dominios
- Configuración de certificados Letsencrypt para Sophos Firewall

Políticas de Prevención de Intrusos (IPS), Anti DOS y QoS, Reportes

- Políticas de IPS
- Protección DOS y DDOS

- Configuración de QoS por grupos, aplicaciones y reglas de firewall
- Reportes históricos en Sophos
- Visor de Registros

Protección con WAF en http y https, Configuración del Servidor Web Apache y Wordpress

- Servidor Web con Apache en Rocky Linux
- Configuración básica
- Configuración de dominios virtuales en Apache
- Instalación de WordPress CMS
- Protección WAF para http
- Configuración de HTTPS
- Configuración de MySQL, permisos, creación y respaldo de base de datos
- Instalación de Certificado Letsencrypt en el VPS
- Carga de certificados digitales de dominios https
- Protección WAF para https
- Formulario de autenticación para sitios inseguros

Configuración del Servidor de Correo Zextras Carbonio CE (fork de Zimbra)

- Requisitos previos
- Configuración de registros públicos DNS y hostname para Carbonio CE
- Instalación de Zextras Carbonio CE
- Publicación de Zextras Carbonio CE con Ip pública
- Instalación de Certificado digital para Carbonio CE.

Configuración de Gateway AntiSpam con Sophos Firewall

- Habilitación de Gateway AntiSpam
- Antispam en modo bridge
- Listas Blancas y Negras
- Políticas de filtrado
- Antispam en modo Gateway
- Cuarentena
- Revisión de Logs

Configuración de WAN Failover

- Configuración de Interfaz de Red Adicional
- Configuración de Ip pública
- Configuración de WAN Failover
- Pruebas Funcionales

Seguridad Inalámbrica y HotSpot

- Configuración de WIFI público
- Configuración de portal cautivo
- Filtrado Web, App y Traffic Shaping del WIFI público
- Creación de cupones de hotspot