CISCO ASA SECURITY

Duración: 5 días, 35 horas

Objetivos

- Presentación de la familia Cisco ASA
- Nuevas funcionalidades del la línea 5500-X Next-Generation Firewalls
- Conectividad básica y administración
- Integración con la red
- Configuración de las funcionalidades principales
- Control de políticas
- Componentes de las VPNs de Cisco ASA
- Soluciones de VPNs de acceso remoto clientless
- VPNs de acceso remoto full tunnel con AnyConnect
- Soluciones de alta disponibilidad y virtualización de Cisco ASA

Guión del curso

- Módulo 1: Presentación de la familia de equipos Cisco ASA
  - Tecnologías de cortafuegos
  - Características de Cisco ASA
  - Descripción Hardware de la línea Cisco ASA
  - Licenciamiento

- Módulo 2: Conectividad básica y administración
  - Proceso de arranque
  - Uso de la línea de comandos (CLI)
  - Empleo del soporte gráfico Cisco ASDM
  - Navegación básica Cisco ASDM
  - Actualización del sistema operativo
  - Empleo de los niveles de seguridad de los interface
  - Configuración de VLANs y etiquetado de VLANs
  - Configuración de ruta por defecto
  - Configuración del servicio DHCP y Relay DHCP
  - Resolución de problemas de conectividad

- Módulo 3: Integración con la red
  - Funcionalidades de NAT
  - Configuración de Objetos en Auto-NAT
  - Configuración de NAT manual
  - Ajuste de y resolución de problemas relativos a NAT
  - Tablas de conexiones y traducciones de nat
  - Configuración y verificación de los ACLs de interfaces
  - Configuración y verificación de ACLs globales
  - Configuración y verificación de grupos de objetos
  - Configuración y verificación de traducciones de servidores públicos
  - Configuración y verificación de otros controles de acceso
  - Resolución de problemas relativos a ACLs
  - Routing estático
  - Routing dinámico
  - Configuración y verificación de EIGRP
  - Soporte de IP Multicast

- Módulo 4: Control de políticas en Cisco ASA
  - Presentación de Cisco MPF (Modular Policy Framework)
  - Configuración y verificación de políticas de capas 2 y 3 de OSI
  - Configuración y verificación de la política para tráfico de administración
  - Presentación de las política de control de capas superiores (5 a 7) de OSI
  - Configuración y verificación de la inspección HTTP
  - Configuración y verificación de la inspección FTP
  - Soporte de otras aplicaciones
  - Resolución de problemas relativos a inspección de aplicaciones

- Módulo 5: Componentes de las VPNs de Cisco ASA (Adaptive Security Appliance)
  - Definición de VPN
  - Amenazas a las comunicaciones WAN y remotas
  - Tipos de VPNs y sus componentes
  - Implementación de Perfiles, Grupos de políticas y políticas de usuario
  - Perfiles de Conexión
  - Grupos de políticas referidas a administración de AAA y almacenamiento de políticas externa
  - Atributos de métodos de Acceso de Control de usuario
  - Contabilidad de accesos por VPN SSL mediante servidores externos DAP
  - Implementación de servicios PKI (Public Key Infrastructure)
  - Registro de certificados de CA externos para ASA

Configuración de autenticación de clientes mediante certificados digitales
Operaciones de proxy SCEP
Habilitar en el perfil de conexión la autenticación mediante certificados digitales
Mapeo de Perfiles de Conexiones contra certificados digitales

- Módulo 6: VPN remotas en modo Clientless
  - Presentación de la solución
  - Configuración y administración de claves
  - Autentificación del servidor y cliente
  - Administración de la página (URLs, bookmarks, ...) de la VPN SSL clientless
  - Monitorización de las VPNs Clientless SSL
  - Resolución de problemas
  - Plug-Ins de applicaciones
  - Resolución de problemas Clientless relativos a Plug-Ins
  - Smart Tunnels
  - Configuración y verificación de Smart Tunnels
  - Opciones de autenticación de clientes
  - Autenticación de doble factor mediante servidores AAA
  - Resolución de problemas

- Módulo 7: Cisco AnyConnect Full Tunnel VPN Solution
  - Presentación de VPNs SSL con AnyConnect
  - Autenticación de clientes de VPNs
  - Asignación de direcciones
  - Split Tunneling en VPNs de acceso remoto
  - Monitorización de conexiones AnyConnect en cliente y servidor
  - Componentes de la solución de Cisco AnyConnect
    - DTLS
    - Descarga de SW de Cisco AnyConnect
    - Integración con el sistema operativo: Arranque con VPN AnyConnect activado
  - Empleo de certificados digitales
  - Autenticación de doble factor
  - Integración con directorios de usuarios LDAP/AD
  - Protocolos IKEv1 y v2
  - Resolución de problemas relativos a Cisco AnyConnect

- Módulo 8: Soluciones de alta disponibilidad y de virtualización de Cisco ASA
  - Configuración y verificación de agregados de líneas (EtherChannel)
  - Configuración y verificación de enlaces redundantes
  - Configuración de failover en modo Active/Standby
  - Cisco ASA en Modo Contexto
  - Configuración de failover en modo Active/Active
  - Ajustes de failover
  - Ejecución de comandos en contextos
  - Configuración de contextos de seguridad
  - Configuración y verificación de gestión de recursos de contextos

Laboratorios

Lab 1-1: Acceso al entorno del laboratorio remoto

Lab 2-1: Configuración del Cisco ASA Adaptive Security Appliance

Lab 3-1: Configuración de NAT
Lab 3-2: Configuración de control de acceso y funcionalidades asociadas

Lab 4-1: Configuración mediante MPF, Inspección básica de la tabal de estado y QoS
Lab 4-2: Configuración mediante MPF de Inspecciones Avanzadas de Aplicaciones

Lab 6-1: Implementación básica de VPN SSL Clientless
Lab 6-2: Configuración de acceso a aplicaciones de la intranet mediante VPN SSL
Lab 6-3: Implementación de servidores externos AAA para VPNs SSL

Lab 7-1: Implementación básica de VPNs SLL AnyConnect
Lab 7-2: Configuración avanzada de autenticación para VPNs SSL Cisco AnyConnect
Lab 7-3: Configuración de IKEv1 y v2 para VPNs de acceso remoto IPSec

Lab 8-1: Configuración de failover Active/Standby
Lab 8-2: Configuración de failover Active/Active