

# CHILIQUINGA YESHUA SAN MARTIN JOSE TOVAR DENNIS

## ACTIVIDADES DEL PROYECTO

### ACTIVIDADES DEL PROYECTO



CULTURA EMPRESARIAL



TIERRAS  
PROYECTO



## DESARROLLO DE TALENTO

### DESARROLLO DE TALENTO



01 HABILIDADES  
02 PLAN DE CARRERA  
03 CAPACITACIÓN  
04 FORMACIÓN

## ACTIVIDADES DEL PROYECTO



## LÍNEA DEL TIEMPO



ABRIL  
FEBRERO

## PROCESO DE MARKETING



01 CONTENIDO  
02 PUBLICIDAD  
03 ESTRATEGIA  
04 SEGMENTACIÓN

## TIEMPO



ABRIL

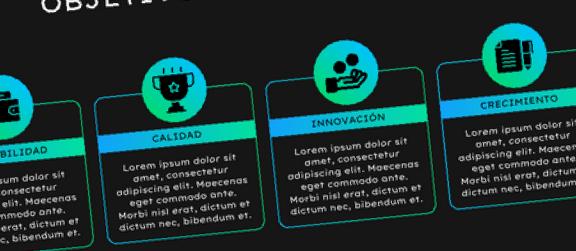


AMENAZA  
OPORTUNIDAD  
DEBILIDAD  
FORTALEZA

TIERRAS  
PROYECTO



## OBJETIVOS DEL PROYECTO



01 RENTABILIDAD  
02 CALIDAD  
03 INNOVACIÓN  
04 CRECIMIENTO

## DESARROLLO DE TALENTO



01 HABILIDADES  
02 PLAN DE CARRERA  
03 CAPACITACIÓN  
04 FORMACIÓN

## OBJETIVOS DEL PROYECTO



01 RENTABILIDAD  
02 CALIDAD  
03 INNOVACIÓN  
04 CRECIMIENTO

# NETWORK

## NG-FIREWALL (NEXT GENERATION FIREWALL)

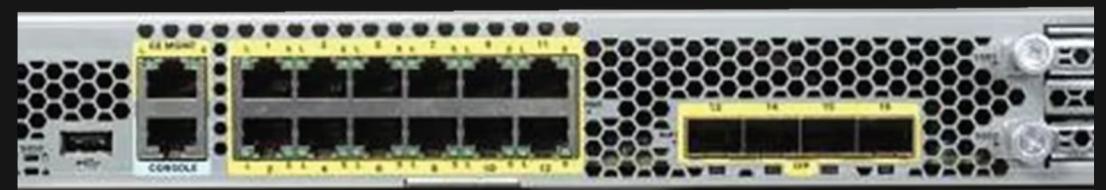
✓ MEJOR PARA: CUALQUIER EMPRESA QUE QUIERA CONTROL GRANULAR DE TRÁFICO.

🔍 MARCAS: PALO ALTO NETWORKS, CISCO FIREPOWER, FORTINET, SONICWALL.

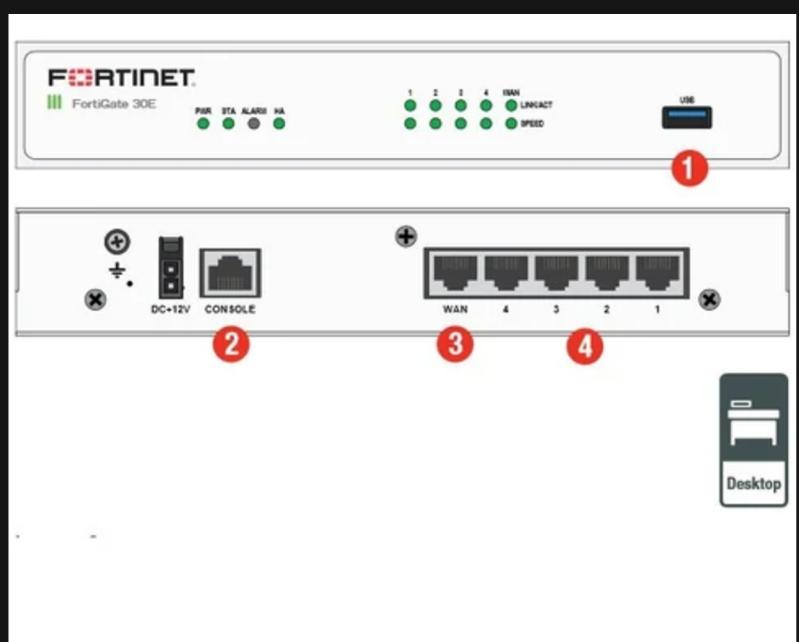
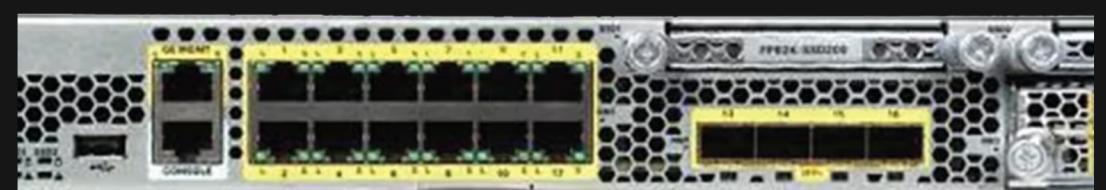
💲 PRECIO: DESDE \$1,000 HASTA \$50,000.

★ VENTAJA: INSPECCIÓN PROFUNDA DE PAQUETES, CONTROL DE APLICACIONES.

Cisco Firepower 2110/2120 Model

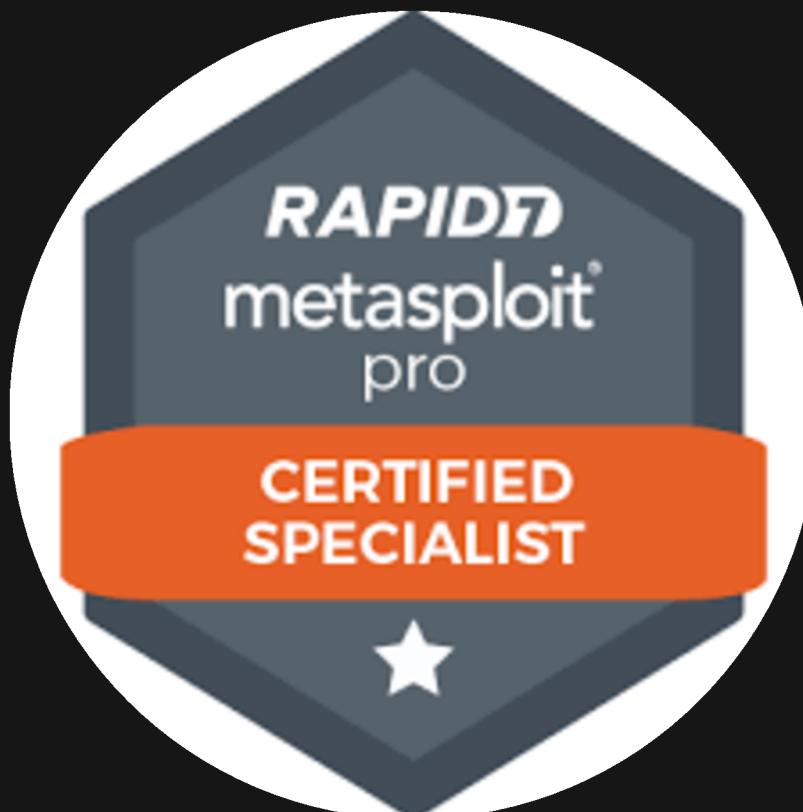


Cisco Firepower 2130/2140 Model



## METASPLOIT

- ✓ **MEJOR PARA: PRUEBAS DE PENETRACIÓN Y ANÁLISIS DE VULNERABILIDADES..**
- 🔍 **MARCAS: RAPID7 METASPLOIT PRO (VERSIÓN DE PAGO).**
- 💲 **PRECIO: VERSIÓN GRATUITA / PRO: DESDE \$5,000/AÑO.**
- ★ **VENTAJA: EXCELENTE PARA AUDITAR Y PROBAR TU RED.**



## OPENVAS

✓ MEJOR PARA: ANÁLISIS DE VULNERABILIDADES COMPLETO.

🔍 MARCAS: GREENBONE (GREENBONE VULNERABILITY MANAGER).

💲 PRECIO: GRATUITO (COMUNIDAD) / ENTERPRISE DESDE \$1,000+.

★ VENTAJA: OPEN SOURCE, POTENTE.



## SIEM BÁSICO (OSSIM)

✓ MEJOR PARA: EMPRESAS MEDIANAS A GRANDES CON INFRAESTRUCTURA COMPLEJA.

🔍 MARCAS: SPLUNK, IBM QRADAR, ARCSIGHT, OSSIM (OPEN SOURCE).

💲 PRECIO: DESDE \$1,500/MES HASTA LICENCIAS ENTERPRISE DE \$100,000+.

★ VENTAJA: CORRELACIÓN DE EVENTOS, ALERTAS AVANZADAS.



# ROUTER

## FILTRADO DE PAQUETES

- Control de tráfico por reglas: Evalúa encabezados de los paquetes y decide si permitirlos o bloquearlos según reglas definidas.
- Operación en capa 3 y 4 del modelo OSI
- No inspecciona contenido
- Rapidez y bajo consumo:
- Puede implementarse como ACLs (Access Control Lists):
- Estático o dinámico:



## TIPO DE HERRAMIENTA

### PREVENCIÓN



# ROUTER

## ACL

- Definen reglas de filtrado en dispositivos de red
- Implementación en Router o Switches
- Dos tipos principales
  - ACL Estándar
  - ACL Extendido
- Secuenciales
- Sin Estado
- Fácil de configurar

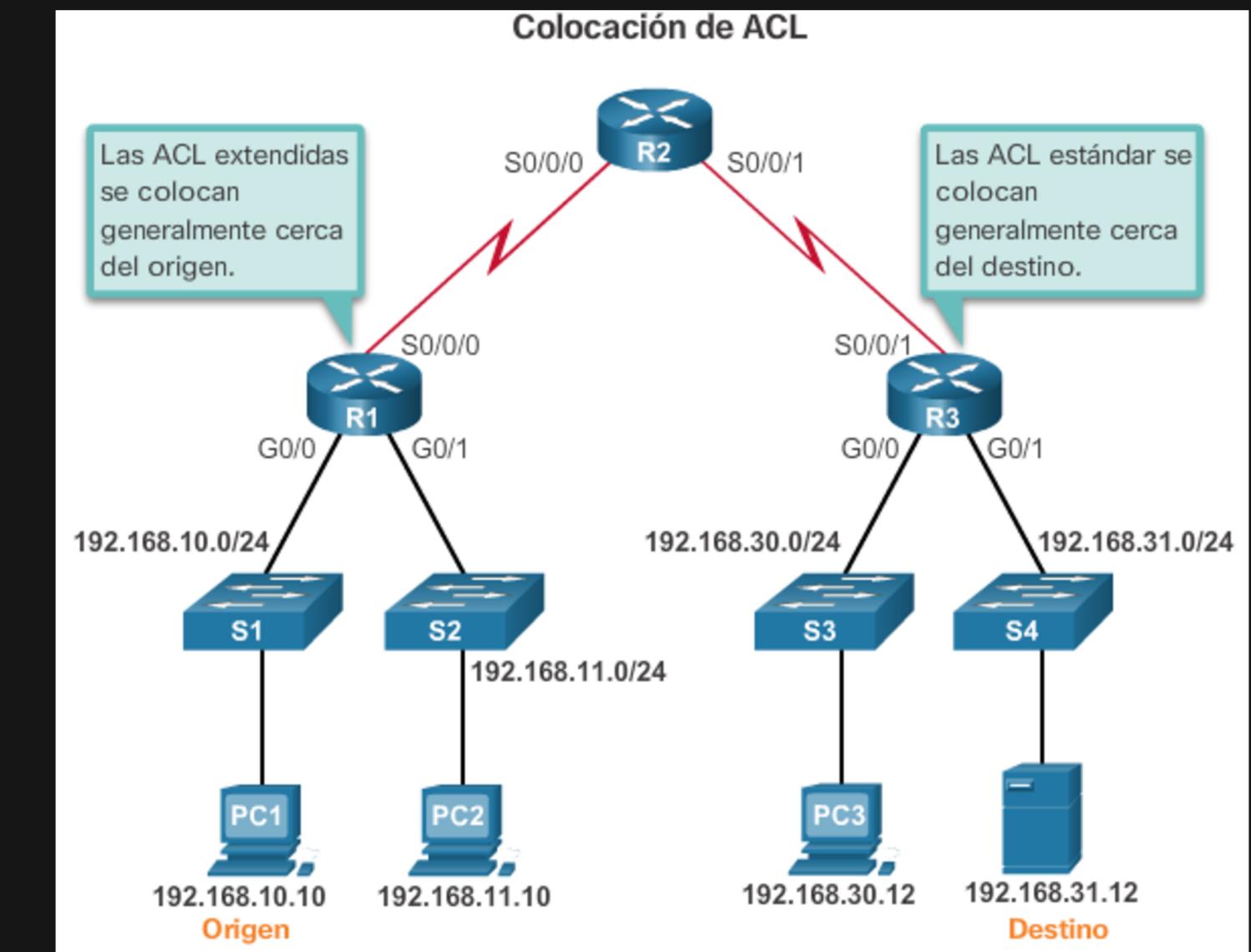


## TIPO DE HERRAMIENTA

### PREVENCIÓN



#### Colocación de ACL



# VPN

## CARACTERISTICAS

- Crear un tunel para redes seguras
- Cifrados de datos
- Oculta IP
- Permite Acceso Remoto Seguro
- Permite Intervenciones



## TIPO DE HERRAMIENTA

CIFRADO



# FIREWALLS

## CLEAROS

### Descripción general

- Base: derivado de CentOS/RHEL, convierte un PC o VM en un UTM completo.
- Interfaz: WebConfig, panel web modular donde se instalan “apps” para distintas funciones.

### Características principales

- Firewall stateful con inspección de paquetes y UTM (antivirus, IPS/IDS).
- Más de 120 apps: QoS, DHCP, DNS, proxy web, filtrado de contenido, VPN, servidor de impresión, etc.
- Gestión centralizada: ClearVM para administrar múltiples instancias.
- Ediciones: Community (gratuita), Home y Business (con suscripción opcional).

### Casos de uso

- PyMEs que necesitan UTM todo-en-uno sobre hardware genérico.
- Entornos virtualizados donde se despliegan múltiples instancias con ClearVM.



# FIREWALLS

## PFSENSE

### Descripción general

- Base: distribución FreeBSD con el firewall PF de OpenBSD.
- Licencia: código abierto, mantenido por Netgate.

### Características principales

- Stateful Packet Inspection (SPI), NAT, GeoIP blocking, anti-spoofing.
- VPN: IPsec, OpenVPN, WireGuard.
- IDS/IPS: integración con Snort y Suricata.
- Multi-WAN y balanceo de carga, CARP para alta disponibilidad.
- Plugins: Squid, SquidGuard, FRR (BGP, OSPF), captive portal, RRD graphs.

### Casos de uso

- Protección perimetral de oficinas remotas y sedes principales.
- Segmentación de redes, VPN site-to-site y acceso remoto seguro.



# FIREWALLS

## CISCO RCS5516FW

### Descripción general

- Firewall COTS basado en Cisco ASA 5516, encapsulado en un chasis militarizado de aluminio para entornos extremos (MIL-STD).

### Características principales

- Throughput: hasta 1.8 Gbps de firewall; ASA IPS: 450 Mbps sin hardware adicional
- Sesiones concurrentes: 250 000; conexiones nuevas: 20 000 c/s
- Puertos: 8x 10/100/1000 Mbps RJ-45 integrados
- Dimensiones: chasis 1U < 13" profundidad; peso ≈ 14 lbs (6.4 kg)
- Servicios: soporte Cisco FirePOWER (NGIPS, AMP, URL filtering)

### Casos de uso

- Despliegue en campo: unidades móviles, vehículos y emplazamientos remotos donde la vibración, polvo y temperatura son críticos.
- Redes tácticas militares: protección perimetral con capacidades NGFW y VPN site-to-site.
- Infraestructura crítica: SCADA/ICS en entornos industriales hostiles.



# FIREWALLS

## UFW E IPTABLES (FIREWALLS “DESMILITARIZADOS”)

### UFW (Uncomplicated Firewall)

- Frontend para iptables diseñado por Canonical para Ubuntu/Debian, orientado a host, simplifica la configuración de reglas netfilter
- Funciones: reglas por servicio, puerto, IP origen/destino, logging, IPv6, rate-limit, perfiles de aplicaciones, GUI opcional (Gufw)
- Limitaciones: no hay robustez física ni certificaciones MIL-STD; se instala sobre hardware/VM genérico, adecuado para proteger servidores o estaciones individuales.

40

### iptables

- Herramienta nativa de Netfilter en Linux para filtrado de paquetes, NAT y mangling; funciona en todas las distros
- Tablas: filter, nat, mangle, raw, security; chains: INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING
- Estado: completamente stateful con connection tracking (ESTABLISHED, RELATED)
- Módulos y extensiones: ipset, limit, geoip, string match, recent, u32, etc.
- Flexibilidad: scripting completo, integración con nftables, políticas avanzadas de QoS y redirección de puertos.



UFW – IPtables Firewall configuration made easier