COLTAN OS

NETWORK SYSTEM

Documentación Técnica

Guía de Instalación, Configuración y Módulos

Versión 1.0 — FreeBSD 14.4 — 2025

www.coltanos.com | info@coltanos.com

Índice de Contenidos

1. Introducción y arquitectura del sistema
2. Requisitos de hardware
3. Proceso de instalación desde USB
4. Primer acceso al panel web
5. Módulo: Dashboard
6. Módulo: Networking e Interfaces
7. Módulo: Firewall
8. Módulo: DHCP
9. Módulo: VPN WireGuard
10. Módulo: VPN OpenVPN
11. Módulo: Suricata IDS/IPS
12. Módulo: DNS Blocker (Premium)
13. Módulo: QoS (Premium)
14. Módulo: Site Blocking (Premium)
15. Módulo: Reportes (Premium)
16. Sistema de licenciamiento
17. Upgrade y Downgrade automático
18. Backup y restauración
19. Troubleshooting común

1. Introducción y Arquitectura

Coltan OS es un sistema operativo de seguridad de red basado en **FreeBSD 14.4**, diseñado para convertir hardware x86-64 estándar en un appliance de seguridad profesional. El sistema integra un stack completo de servicios de red administrados desde un **panel web moderno** desarrollado en Node.js/Fastify con frontend Bootstrap 5.

Stack tecnológico:

Componente	Tecnología	Función
Sistema base	FreeBSD 14.4	Kernel, drivers, ZFS
Backend API	Node.js + Fastify	API REST del panel web
Frontend	Bootstrap 5 + JS	Interfaz web del panel
Proceso manager	PM2	Gestión del backend Node.js
Firewall	PF (Packet Filter)	Reglas, NAT, port forwarding
DHCP	Kea DHCP4	Servidor DHCP de red local
DNS	Unbound	Resolución DNS y bloqueos
IDS/IPS	Suricata	Detección/prevención de intrusos
VPN	WireGuard + OpenVPN	Túneles VPN
NTP	OpenNTPd	Sincronización horaria
Almacenamiento	ZFS	Sistema de archivos con snapshots

Archivos de configuración del sistema:

Todos los archivos de configuración de Coltan OS residen en **/usr/local/etc/coltan/**:

Archivo	Contenido
interfaces.json	Roles WAN/LAN/OPT de cada interfaz de red
users.json	Usuarios del panel web (hashes bcrypt)
license.json	Archivo de licencia Premium activa
license-status.json	Estado actual de la licencia (heartbeat)
firewall-rules.json	Reglas de firewall personalizadas
blocked-ips.json	IPs bloqueadas manualmente
vlans.json	Configuración de VLANs
suricata.json	Configuración del IDS/IPS
settings.json	Configuración general del panel

2. Requisitos de Hardware

Componente	Mínimo	Recomendado	Notas
CPU	x86-64 dual core 1 GHz	Quad core 2 GHz+	Sin soporte ARM
RAM	2 GB	4 GB o más	IPS requiere más RAM
Almacenamiento	16 GB HDD/SSD	32 GB SSD	ZFS requiere espacio libre
Interfaces de red	2 NICs	3+ NICs	WAN + LAN + OPT/VLAN
USB (instalación)	8 GB+	16 GB	Solo para el proceso de instalación
Arquitectura	x86-64	x86-64	No compatible con ARM/MIPS

■ NOTA
Coltan OS funciona excelentemente en mini-PCs como Intel NUC, Protectli, o cualquier PC de escritorio/servidor con 2 o más interfaces de red.

3. Proceso de Instalación desde USB

3.1 Preparar el pendrive USB

Descargá la imagen desde **www.coltanos.com** y grabala en un pendrive de 8GB o más usando **Rufus en modo DD** (Windows) o el comando **dd** (Linux/Mac):

```
# Linux/Mac: sudo dd if=coltanos.v1.0.img of=/dev/sdX bs=4M status=progress # Windows: Usar Rufus → seleccionar imagen → Modo de escritura: DD
```

■ **ADVERTENCIA**
Asegurate de seleccionar el disco USB correcto. El proceso borrará todo su contenido.

3.2 Arrancar desde el USB

Conectá el USB al equipo destino y configurá el BIOS/UEFI para bootear desde USB. Coltan OS arranca automáticamente el instalador gráfico con interfaz visual.

3.3 Pasos del instalador visual

- ■ **Bienvenida:** Pantalla inicial con logo y advertencia sobre el borrado del disco.
- ■ **Selección de disco:** Lista de discos disponibles con su capacidad. Seleccioná con flechas y Enter.
- ■ **Confirmación:** Confirmación del borrado total del disco seleccionado.
- ■ **Hostname:** Nombre del equipo (ej: coltanos-oficina). Solo letras, números y guiones.
- ■ **Interfaz WAN:** Interfaz conectada a Internet. Generalmente re0, em0 o igb0.
- ■ **Interfaz LAN:** Interfaz conectada a la red local. Debe ser diferente a WAN.
- ■ **IP de LAN:** IP estática del router Coltan OS en la LAN (ej: 192.168.1.1).
- ■ **Máscara:** Máscara de red LAN (default: 255.255.255.0).
- ■ **Instalación:** El sistema instala FreeBSD, software y Coltan OS automáticamente (~10-15 min).
- ■ **Verificación:** Chequeo automático de todos los componentes críticos instalados.
- ■ **Finalización:** Reboot automático al presionar Enter. Retirá el USB antes del reinicio.

✓ **IMPORTANTE**
Credenciales por defecto post-instalación:
• Panel web (puerto 3000): usuario **admin** / clave **coltanos**
Cambiá la clave inmediatamente desde Settings → Security al primer ingreso.

4. Primer Acceso al Panel Web

Una vez reiniciado el sistema, accedé desde cualquier dispositivo en la LAN:

```
http://[IP_LAN]:3000 Ejemplo: http://192.168.1.1:3000 Usuario: admin Clave: coltanos
```

Pasos recomendados al primer ingreso:

- • Ingresar con **admin / coltanos**
- • Ir a **Settings** → **Security** y cambiar la clave del admin
- • Verificar en **Networking** que WAN/LAN estén configuradas correctamente

- Activar el **DHCP** para que los dispositivos de la LAN obtengan IP automáticamente
- Si tenés licencia Premium, ir a **Settings** → **Licencia** y aplicarla

5. Módulo: Dashboard

El dashboard muestra el estado general del sistema en tiempo real. Se actualiza automáticamente.

Sección	Descripción
Estado de servicios	Estado de PF, DHCP, Suricata, VPN, Unbound y NTP
Tráfico de red	Gráfico de tráfico WAN/LAN en tiempo real
Interfaces	IP, estado y velocidad de cada interfaz
Alertas Suricata	Últimas alertas de intrusos detectadas
Resumen del sistema	CPU, RAM, disco y uptime
Badge de licencia	Indica si el sistema está en modo FREE o PREMIUM

6. Módulo: Networking e Interfaces

Permite configurar y gestionar todas las interfaces de red del sistema.

6.1 Roles de interfaz

Rol	Descripción	Configuración típica
WAN	Conexión a Internet o proveedor	DHCP o IP estática del ISP
LAN	Red local principal	IP estática (ej: 192.168.1.1)
OPT	Red adicional (DMZ, guests)	Subred separada
VLAN	Red lógica sobre interfaz física	Tag 802.1Q

> ■ **NOTA**
> Para que los cambios de IP o rol surtan efecto, el sistema reinicia automáticamente los servicios afectados (PF, DHCP, Suricata).

6.2 VLANs

Las VLANs permiten segmentar la red sin hardware adicional. Para crear una VLAN:

- Ir a Networking → VLANs → Nueva VLAN
- Seleccionar la interfaz física padre y el tag VLAN (1-4094)
- Asignar un rol (OPT) y una IP a la interfaz VLAN creada
- El PF aplica automáticamente las reglas de aislamiento entre VLANs

7. Módulo: Firewall

Coltan OS usa **PF (Packet Filter)** de FreeBSD como motor de firewall. El panel genera y aplica la configuración automáticamente.

7.1 Reglas de firewall

Las reglas se aplican en orden. Primera coincidencia gana.

Campo	Opciones	Descripción
Acción	pass / block	Permitir o bloquear el tráfico
Dirección	in / out	Tráfico entrante o saliente
Interfaz	WAN, LAN, OPT...	Interfaz donde aplica la regla
Protocolo	tcp, udp, icmp, any	Protocolo de red
Origen	IP, red o any	IP/red de origen
Destino	IP, red o any	IP/red de destino
Puerto	Número o any	Puerto de destino
Descripción	Texto libre	Comentario descriptivo de la regla

7.2 NAT y Port Forwarding

El NAT permite que los dispositivos de la LAN accedan a Internet con la IP pública de WAN. Se activa automáticamente al configurar WAN y LAN.

Para redirigir puertos externos a dispositivos internos:

- Ir a Firewall → Port Forwarding → Nuevo
- Seleccionar interfaz WAN, protocolo y puerto externo
- Ingresar IP interna y puerto destino
- El sistema agrega automáticamente la regla en PF

7.3 Bloqueo de IPs

Podés bloquear IPs manualmente desde Firewall → IPs Bloqueadas. El sistema muestra información geográfica de cada IP (país, ISP).

8. Módulo: DHCP

Coltan OS usa **Kea DHCP4** para asignar direcciones IP automáticamente.

Parámetro	Descripción	Ejemplo
Interfaz	Interfaz LAN donde escucha el DHCP	re1
Rango de pool	IPs asignables automáticamente	192.168.1.2 - 192.168.1.99
Gateway	IP del router (Coltan OS)	192.168.1.1
DNS	Servidores DNS para los clientes	8.8.8.8, 1.1.1.1
Reservas por MAC	IP fija a un dispositivo específico	aa:bb:cc → 192.168.1.50

9. Módulo: VPN WireGuard

WireGuard es el protocolo VPN moderno: más rápido, más simple y más seguro que OpenVPN. Ideal para acceso remoto de empleados y conexión entre sucursales.

9.1 Configurar el servidor

- Ir a VPN → WireGuard → Configuración
- El sistema genera automáticamente el par de claves del servidor
- Configurar el puerto UDP (default: 51820) y la IP del túnel (ej: 10.0.0.1/24)
- Asegurarse de tener el puerto 51820/UDP habilitado en el firewall WAN

9.2 Agregar peers (clientes)

- Ir a WireGuard → Peers → Nuevo peer
- Ingresar la clave pública del cliente o generar un nuevo par
- Asignar una IP al peer dentro del túnel (ej: 10.0.0.2/32)
- Descargar el archivo de configuración .conf para el cliente

9.3 Configuración típica del cliente

```
[Interface] PrivateKey = [CLAVE_PRIVADA_CLIENTE] Address = 10.0.0.2/32 DNS = 192.168.1.1
[Peer] PublicKey = [CLAVE_PUBLICA_SERVIDOR] Endpoint = [IP_PUBLICA]:51820 AllowedIPs =
0.0.0.0/0 PersistentKeepalive = 25
```

10. Módulo: VPN OpenVPN

OpenVPN es compatible con prácticamente todos los dispositivos y sistemas operativos. Recomendado cuando los clientes no soportan WireGuard.

- Ir a VPN → OpenVPN → Configuración del servidor
- Generar o importar los certificados CA y del servidor
- Configurar protocolo (UDP/TCP), puerto (default: 1194) y subred del túnel
- Activar el servidor y descargar el archivo .ovpn para cada cliente

11. Módulo: Suricata IDS/IPS

Suricata es el motor de detección y prevención de intrusos. En la versión Free opera en modo **IDS** (solo detección y alertas). En Premium activa el modo **IPS** con bloqueo automático de atacantes.

11.1 Diferencia IDS vs IPS

Función	IDS (Free)	IPS (Premium)
Detecta ataques	✓	✓
Genera alertas	✓	✓
Bloquea IPs atacantes	✗	✓
Modifica reglas en caliente	✗	✓
Limpia historial de alertas	✗	✓

11.2 Iniciar Suricata

- Ir a Security → Suricata
- Seleccionar las interfaces a monitorear (WAN y LAN recomendado)
- En Free: modo IDS fijo. En Premium: seleccionar IDS o IPS
- Click en "Iniciar Suricata"
- Las alertas aparecen en tiempo real en la pestaña "Alertas"

12. Módulo: DNS Blocker (Premium)

El DNS Blocker usa **Unbound** para bloquear dominios a nivel DNS, impidiendo que los dispositivos de la LAN accedan a sitios de publicidad, malware, phishing y otras categorías no deseadas.

Categorías disponibles:

- Publicidad y tracking
- Malware y ransomware
- Phishing y fraude
- Contenido adulto
- Redes sociales
- Dominios personalizados

> ■ **NOTA**
> El DNS Blocker actúa como resolver DNS de la LAN. Los dispositivos deben usar la IP de Coltan OS como servidor DNS (se configura automáticamente via DHCP).

13. Módulo: QoS — Calidad de Servicio (Premium)

QoS permite **priorizar el tráfico** según tipo de aplicación o dispositivo, garantizando ancho de banda para servicios críticos.

- Priorizar llamadas VoIP sobre navegación web
- Garantizar ancho de banda para videoconferencias
- Limitar el ancho de banda de descargas P2P
- Asegurar conectividad para sistemas críticos (ERP, cámaras IP)

14. Módulo: Site Blocking (Premium)

Permite bloquear el acceso a sitios web específicos o categorías completas para todos los dispositivos de la LAN.

- Por URL exacta (ej: facebook.com)
- Por categoría predefinida (redes sociales, entretenimiento, etc.)
- Grupos de URLs personalizados

15. Módulo: Reportes (Premium)

Genera reportes detallados del uso de la red exportables en **PDF y CSV**.

Tipo de reporte	Contenido
Tráfico de red	Ancho de banda por interfaz, hora y dispositivo
Ataques detectados	Alertas Suricata con IP, tipo de ataque y timestamp
Consultas DNS	Dominios más consultados y bloqueados
Accesos al panel	Log de logins al panel web con IP y hora

16. Sistema de Licenciamiento

El sistema de licencias usa **firma criptográfica** para validar las licencias. Cada licencia es un archivo JSON vinculado al equipo específico.

16.1 Activar una licencia Premium

- Adquirir la licencia en www.coltanos.com o contactando info@coltanos.com
- Recibir el archivo de licencia (.json) por email
- Ir al panel → Settings → Licencia
- Cargar el archivo .json y hacer click en "Aplicar Licencia"
- El sistema valida contra los servidores de Coltan OS y activa Premium automáticamente

16.2 Validación continua

El sistema valida periódicamente que la licencia siga activa. Si la licencia es revocada o expira, el sistema inicia el downgrade automáticamente.

16.3 Forzar verificación

Desde Settings → Licencia podés hacer click en **"Forzar verificación"** para validar el estado de la licencia en tiempo real.

> ■ **ADVERTENCIA**
> La licencia es por equipo. No se puede usar la misma licencia en dos equipos simultáneamente.

17. Upgrade y Downgrade Automático

17.1 Upgrade Free → Premium

Al activar una licencia válida, el sistema descarga e instala automáticamente los módulos Premium. El proceso es completamente transparente:

- Valida la licencia contra los servidores de Coltan OS
- Descarga el código premium del repositorio oficial
- Instala los módulos sobre la instalación existente
- Reinicia el backend para activar los módulos
- Toda la configuración del usuario se conserva intacta

17.2 Downgrade Premium → Free

Si la licencia es revocada o expira, el sistema ejecuta automáticamente el downgrade en el siguiente ciclo de validación (pocos minutos):

- Detecta que la licencia está inactiva
- Descarga la versión Free desde el repositorio público
- Reemplaza los módulos Premium con las versiones Free
- La configuración de red, firewall y VPN se mantiene intacta

18. Backup y Restauración

El módulo de Backup permite guardar y restaurar toda la configuración de Coltan OS en un archivo comprimido.

¿Qué incluye el backup?

- Interfaces y roles de red
- Reglas de firewall y port forwarding
- IPs bloqueadas y configuración DHCP
- Usuarios del panel web
- Configuración de VLANs, WireGuard y OpenVPN
- Configuración de Suricata, DNS Blocker, QoS y Site Blocking

> ■ **ADVERTENCIA**
> El backup NO incluye las claves privadas de VPN ni el archivo de licencia. Guardá esos archivos por separado en un lugar seguro.

Proceso de restauración:

- Ir a Backup → Restaurar
- Cargar el archivo de backup (.tar.gz)
- Confirmar la restauración
- El sistema aplica la configuración y reinicia los servicios afectados

19. Troubleshooting Común

El panel web no carga en el puerto 3000

- Verificar que el servicio del panel esté corriendo desde la consola del equipo
- Reiniciar el servicio si es necesario
- Verificar que el puerto 3000 no esté bloqueado por el firewall LAN

Los clientes de LAN no obtienen IP por DHCP

- Verificar que el DHCP esté activo en el panel → DHCP
- Verificar que la interfaz LAN esté correctamente configurada en Networking
- Reiniciar el servicio DHCP desde el panel

Sin acceso a Internet desde la LAN

- Verificar que la interfaz WAN tenga IP asignada (Dashboard → Interfaces)
- Verificar que el NAT esté activo (el firewall debe tener regla NAT en WAN)
- Comprobar que el cable WAN esté conectado y el ISP entregue IP por DHCP

Suricata no inicia

- Verificar que la interfaz seleccionada exista y esté activa
- Reiniciar Suricata desde Security → Suricata → Iniciar
- Contactar soporte en info@coltanos.com si el problema persiste

Error al aplicar licencia

- Verificar conectividad a internet desde el equipo
- Verificar que el archivo .json de licencia no esté corrupto
- Usar el botón "Forzar verificación" desde Settings → Licencia
- Contactar info@coltanos.com con el mensaje de error exacto

Coltan OS Updates muestra error

- Ir a Settings → System → Coltan OS Updates
- Hacer click en "Verificar actualizaciones"
- Si el error persiste, contactar soporte técnico

Logs del sistema útiles para diagnóstico

Log	Ubicación	Descripción
Panel web	/root/.pm2/logs/coltanos-backend-*.log	Logs del servidor Node.js
Arranque	/var/log/rc.local.log	Log del arranque y servicios
Instalación	/var/log/coltan-install.log	Log del proceso de instalación
Suricata	/var/log/suricata/eve.json	Eventos y alertas de intrusos
DHCP	/var/log/kea/	Logs del servidor DHCP

Para soporte técnico, consultas o reportar inconvenientes:
info@coltanos.com | www.coltanos.com