



Solución de seguridad Clavister OT

Descripción de la solución

Descripción de la solución – Seguridad OT

Los entornos de tecnología operativa (OT) abarcan varios sistemas responsables de monitorear y controlar los dispositivos físicos, los procesos y la infraestructura. Estos entornos están cada vez más integrados con los sistemas informáticos, lo que los hace vulnerables a las amenazas cibernéticas. Un firewall de seguridad de OT robusto es esencial para proteger estos sistemas críticos. Las soluciones de seguridad OT de Clavister son una solución integral para la seguridad OT, destacando las características necesarias.

Un Clavister NetWall con la suscripción OT es un dispositivo de seguridad especializado diseñado para proteger las redes OT de las amenazas cibernéticas. A diferencia de los firewalls de TI tradicionales, los firewalls de OT deben abordar los requisitos únicos de los sistemas de control industrial (ICS), los sistemas SCADA y otros entornos de OT.

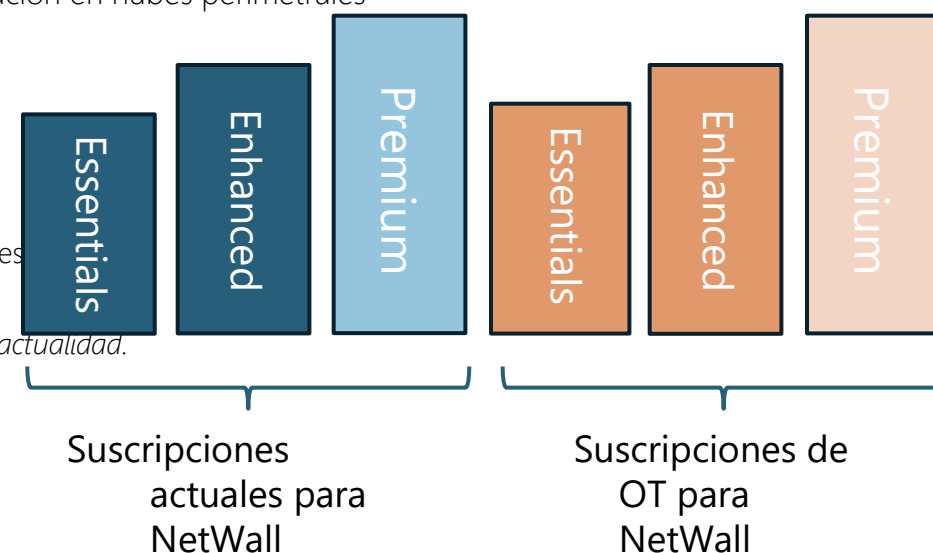
Solución de seguridad Clavister OT

Dispositivos disponibles:

- Dispositivos no reforzados: cuando se implementan en centros de datos o ubicaciones climatizadas
- Dispositivos resistentes: cuando se implementan en entornos hostiles con amplios requisitos de temperatura.
- Dispositivos virtuales: se entregan como imágenes de HyperV, KVM o VMware para su ejecución en nubes perimetrales

Suscripción

- Suscripciones a Clavister OT
 - Suscripción a plazo que contiene lo mismo que la suscripción NGFW correspondiente
 - Agregar el derecho de uso de políticas de IA (PASAD), protocolos OT, O&M basados en soluciones
 - Vinculante/Inicial durante un máximo de 10 años (máx. 5 años para NGFW)
 - *Premium reservado para uso futuro, ya que Premium no está disponible para todos NetWall en la actualidad.*



Clavister NetWall – Línea de dispositivos OT



Disponible

Clavister NetWall 200R

El Clavister NetWall 200R es un firewall robusto montado en DIN diseñado para entornos industriales, que ofrece una seguridad robusta con una amplia tolerancia a la temperatura esencial para condiciones adversas.



Disponible

Clavister NetWall 500 Series

Los NetWall 510 y 550 son firewalls de OT diseñados para entornos controlados, con fuentes de alimentación redundantes, compatibilidad opcional con PoE y capacidad de montaje en rack para mejorar la confiabilidad y versatilidad.



Disponible

Clavister NetWall 6000 Series

El NetWall 6000 es un firewall OT para centros de datos equipado con fuentes de alimentación redundantes y soporte de módulos flexibles para adaptarse a una amplia gama de estándares de red, lo que garantiza un rendimiento y una adaptabilidad sólidos.

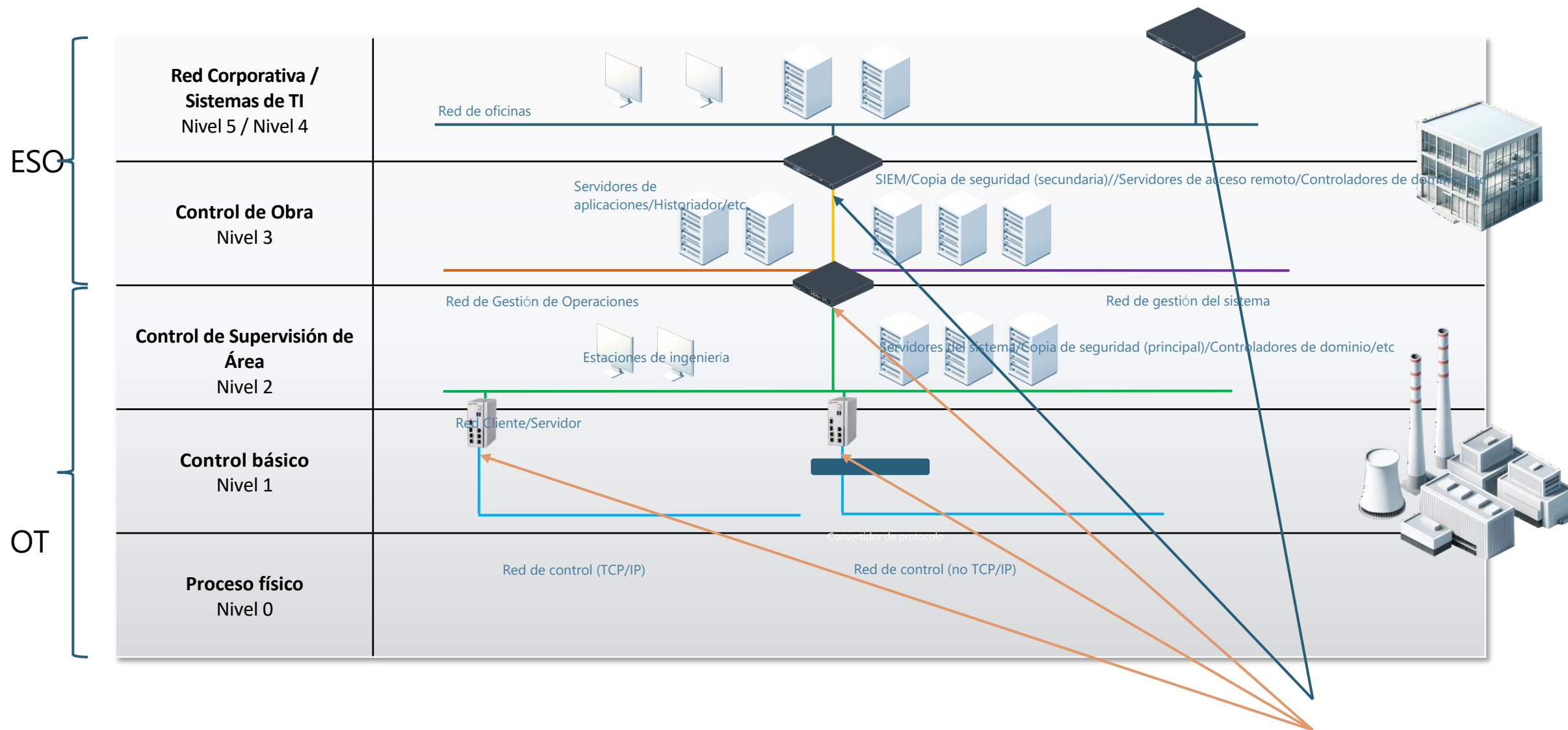
La arquitectura de referencia empresarial de Purdue.

La arquitectura actual de Purdue modela OT y IT en seis niveles funcionales que van desde el Nivel 0 hasta el Nivel 5 y abarcan tres zonas.

- Nivel 5 - Red corporativa: Un conjunto más amplio de sistemas de TI empresariales, incluidas las conexiones a la Internet pública.
- Nivel 4 - Sistemas de TI: Los sistemas de logística empresarial pueden incluir servidores de bases de datos, servidores de aplicaciones y servidores de archivos.
- Nivel 3 — Control del sitio: Este nivel incluye sistemas que soportan las funciones de control y monitoreo en toda la planta. Los sistemas de nivel 3 también agregue datos de nivel inferior que deben enviarse a sistemas empresariales de nivel superior.
- Nivel 2 — Control de supervisión de área: Lógica de control para analizar y actuar sobre los datos de nivel 1. Los sistemas incluyen interfaz hombre-máquina (HMI); software de supervisión y adquisición de datos (SCADA).
- Nivel 1 — Control Básico: Estos son los dispositivos de control, como los controladores lógicos programables que monitorean y controlan los equipos de Nivel 0 y los sistemas instrumentados de seguridad.
- Nivel 0 — Proceso físico: Este es el equipo físico que realiza el trabajo y se conoce como el equipo bajo control. Se trata de válvulas, bombas, sensores, actuadores, compresores, etc.

Normalmente, estos niveles se describen como la creación de tres zonas lógicas, con los niveles 4 y 5 que comprenden la zona empresarial, que está separada de la zona de fabricación (que comprende los niveles 0 a 3) por una zona desmilitarizada (DMZ). Este enfoque jerárquico ha funcionado muy bien durante las últimas dos décadas para ayudar a diseñar la infraestructura de OT.

La arquitectura de referencia empresarial de Purdue



Características clave de un firewall de seguridad de OT

Filtrado de protocolos

- Soporte para protocolos industriales: El firewall debe admitir y comprender varios protocolos de comunicación industrial como Modbus, DNP3, OPC UA, BACnet y más. Esto permite que el firewall inspeccione y filtre el tráfico en la capa de la aplicación, lo que garantiza que solo se permita la comunicación legítima.
- Inspección profunda de paquetes (DPI): Esta función permite que el firewall inspeccione el contenido de cada paquete en busca de cargas útiles maliciosas o anomalías, lo que garantiza un filtrado de protocolo sólido.

Segmentación de la red

- Segmentación basada en zonas: El firewall debe permitir la creación de zonas de seguridad para segmentar diferentes partes de la red OT, como separar los sistemas de control de las redes empresariales.
- Microsegmentación: Mayor segmentación dentro de las zonas de seguridad para limitar el movimiento lateral de las amenazas dentro de la red.

Sistema de Detección y Prevención de Intrusiones (IDS/IPS)

- Detección basada en firmas: utiliza firmas de amenazas conocidas para detectar y bloquear ataques.
- Detección basada en anomalías: identifica comportamientos inusuales o desviaciones de la actividad de referencia, lo que puede indicar una amenaza nueva o desconocida.
- Capacidades de prevención: Toma medidas automáticamente para bloquear o mitigar las amenazas identificadas.

Acceso remoto seguro

- Compatibilidad con VPN: proporciona acceso remoto seguro para el mantenimiento y la gestión, al tiempo que garantiza que las conexiones estén cifradas y autenticadas.

Características clave de un firewall de seguridad de OT

Control de acceso

- Control de acceso basado en roles (RBAC): garantiza que solo el personal autorizado tenga acceso a segmentos o dispositivos de red específicos.
- Autenticación multifactor (MFA): agrega una capa adicional de seguridad al requerir múltiples formas de verificación antes de otorgar acceso.

Identificación y monitoreo de dispositivos

- Detección y gestión de activos: identifica y cataloga automáticamente los dispositivos dentro de la red de OT, proporcionando visibilidad de lo que necesita protección.
- Análisis de comportamiento: Supervisa continuamente el comportamiento del dispositivo para detectar desviaciones que podrían significar un compromiso.

Registro e informes

- Registro completo: registros detallados de toda la actividad de la red, que son esenciales para la auditoría y el análisis forense.
- Alertas en tiempo real: Notificación inmediata de actividad sospechosa o incidentes de seguridad.
- Informes de cumplimiento: genera informes para demostrar el cumplimiento de las regulaciones y estándares de la industria.

Alta disponibilidad y fiabilidad

- Redundancia: Garantiza el funcionamiento continuo a través de hardware redundante y capacidades de conmutación por error.
- Hardware de grado industrial: diseñado para funcionar en entornos hostiles teniendo en cuenta la temperatura, el polvo y otros factores físicos.