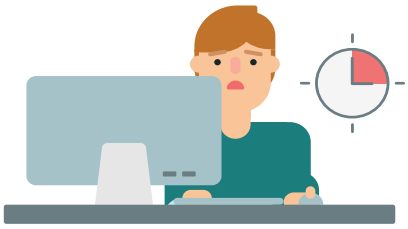
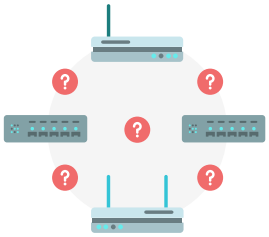
El *hardening* de la capa de acceso es un **punto clave** en la adecuación de estándares de buenas prácticas de seguridad, ya que supone un punto que podría multiplicar el riesgo asociado a cada activo conectado a la red.
A pesar de lo **estratégica** que puede ser la capa de acceso en cuanto a la seguridad de la organización y sus sistemas, en ocasiones resulta un punto de vulnerabilidad conocida que requiere aseguramiento y mejora continua.





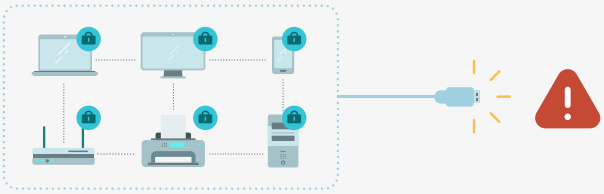
El problema

El hardening de la capa de acceso es un punto clave en la adecuación de estándares ya que supone un punto que multiplica el riesgo asociado a cada activo conectado a la red.

- La gestión manual y descentralizada de la infraestructura hace que la tarea de actualización, mantenimiento etc. y su correspondiente proceso de auditoria esté sujeto a personas.
- Las empresas gestionan muchos tipos de electrónica, (multi-fabricante y multi-versión). Cada uno requiere sus configuraciones concretas en puntos muy dispersos.
- La mayoría de las empresas no tienen una visibilidad centralizada del 100% de todos los dispositivos de red, lo que hace imposible su auditoría / hardening.

¿Por qué la capa de acceso es tan estratégica para la seguridad?

La capa clave e insegura



La estrategia de Zero Trust (donde no se confía en ninguna conexión sin validación) se aplica sobre la capa de acceso con lo cual, si la capa de acceso no está bastionada, la estrategia de Zero Trust se ve comprometida

Inseguras por defecto

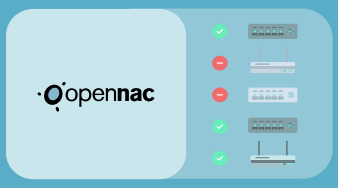
- Para facilitar la instalación, operación y mantenimiento fabricantes crean y distribuyen dispositivos de red con servicios explotables habilitados de forma predeterminada.

Desactualizadas

- A menudo no se modifican las configuraciones predeterminadas de los dispositivos, tampoco se realizan actualizaciones de versiones o de configuraciones de seguridad.

"El 31% de las organizaciones ha experimentado ciberataques a la infraestructura de tecnología operativa". **CISCO**

La Solución: Network Device Compliance **(NDC)**



Network Device Compliance es un módulo dentro de la solución OpenNAC Enterprise que **centraliza y automatiza parte** del proceso de auditoría de las configuraciones de la electrónica con configuraciones de referencia, líneas base y best practices.

Facilita la adecuación de estándares y frameworks como ISO2700x, NIST, ENS etc. y garantiza la implementación segura de la tecnología NAC (Pure & Sure NAC). Centraliza el almacenamiento de back-ups y establece un punto de gestión de configuraciones de dispositivos de red.

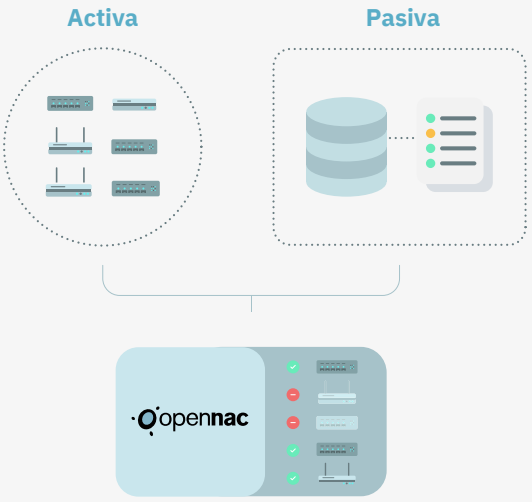
Network Device Compliance (NDC) de forma activa o pasiva

De forma activa

- NDC puede lanzar reglas de comprobación **activas** de manera **dinámica** (directamente) contra dispositivos de red y de manera **estática** (primero generando un backlog de la configuración para posteriormente realizar la comprobación)

De forma pasiva

- También puede realizar el mismo proceso de **manera pasiva** contra un repositorio de configuraciones sin tener que consultar la electrónica en ningún momento



Puesta en marcha en 3 pasos

1. Dar de Alta

1. Un dispositivo de red (por SSH)
2. Un repositorio de configuraciones en el caso de una comprobación pasiva (por SCP)

2. Definir reglas y lanzar

1. Definir las reglas, grupo de reglas correspondientes para el dispositivo y/o grupo de dispositivos
2. Posibilidad de lanzar las comprobaciones en el momento o programarlas.

3. Revisar resultados

1. Desde los cuadros de mando centralizados se muestran los resultados (comprobaciones con éxito, fallos / hallazgos etc.)

“Debido a la visibilidad centralizada del dispositivo y capacidad de remediación centralizada sobre la electrónica, pudimos reducir nuestros tiempos de respuesta a incidentes de usuarios finales (en incidentes típicos) entre 60-70%; fue un valor añadido inesperado de un proyecto NAC”

Testimonio del responsable de infrastructura y comunicaciones de uno de nuestros clientes. (Empresa multinacional de seguros)

Principales beneficios de Network Device Compliance (NDC)

Centraliza

- Las comprobaciones de toda la electrónica se realizan desde una solución única y una interfaz única, simplificando y acelerando el trabajo de auditoría.

Automatiza

- Las comprobaciones se puedan lanzar bajo demanda o de manera programada para alinearse con las tareas de auditoría.

Facilita la adecuación con estándares y frameworks

- Se pueden implementar las reglas de comprobación de configuraciones necesarias para la adecuación de estándares y frameworks.

Garantiza la implementación segura de NAC

- Se puede asegurar que la electrónica está correctamente configurada para que NAC funciona de manera óptima.

Arquitectura

La instalación de **Network Device Compliance (NDC)** requiere dos máquinas virtuales (Core y Analytics)

Core

- Motor de políticas
- CMDB
- Portal de administración
- Motor de Reglas

Analytics

- Motor de búsqueda
- Dashboards
- Informes

Reconocimientos

Gartner

Único fabricante europeo de tecnología NAC incluido en Gartner Market Guide.

Common Criteria

Plataforma certificada en Common Criteria 3.1 release 5 por parte del Organismo de Certificación del Centro Criptológico Nacional OC-CCN de España.

CCN-CERT centro criptológico nacional

Incluido en el catálogo de productos de Seguridad de las Tecnologías de la información y la comunicación del Centro Criptológico Nacional, Ministerio de Defensa - Gobierno de España.

Contacta con nosotros

opencloud factory

+34 91 614 53 22

www.opencloudfactory.com/contacto