Preguntas más frecuentes sobre OpenNAC Enterprise

? ¿Es una solución Cloud?

- ✓ OpenNAC Enterprise se despliega sobre la infraestructura del cliente, ya sea on-premise o en su propia nube privada. No es una solución SaaS. Cipherbit proporciona imágenes OVA listas para desplegar sobre entornos virtualizados del cliente.

? ¿Cómo se despliega OpenNAC Enterprise?

- ✓ El despliegue se realiza mediante imágenes virtuales (OVA) que incluyen los distintos componentes de la plataforma: core, analytics, sensor, VPN gateway, portal cautivo, etc. Se requiere configurar adecuadamente la infraestructura del cliente y cumplir ciertos requisitos técnicos para cada módulo. No se requiere adquirir appliances o servidores concretos, sino capacidad en la plataforma de virtualización del cliente.

? ¿Tenéis un listado de fabricantes-modelos de equipos (switches firewall) que se integran perfectamente con OpenNAC Enterprise?

- ✓ Sí, consulta con nosotros para conseguir el catálogo de la electrónica de red que tenemos homologada.

? Ante un ataque de Ransomware ¿cómo me puede ayudar OpenNAC Enterprise?

- ✓ OpenNAC Enterprise puede ayudar conteniendo la amenaza aislando los equipos infectados de forma dinámica y automática en un segmento de red de cuarentena para evitar la propagación del malware al resto de la red.

Preguntas más frecuentes sobre OpenNAC Enterprise

- ?** ¿OpenNAC Enterprise puede complementar otra(s) solución(es) que ya tengo desplegadas en la red?

✓ Sí, además dispone de una APIs para integración con soluciones de monitorización, SIEM, antivirus, EDR o sistemas de terceros. Pudiendo actuar como capa de enforcement para decisiones de seguridad generadas por otras soluciones ya desplegadas.
- ?** ¿Quién se encarga de realizar la implantación y proporcionar soporte?

✓ Las jornadas de implantación y los servicios de soporte de OpenNAC Enterprise son proporcionadas por los integradores/partners certificados.
- ?** ¿Ayuda OpenNAC Enterprise a conocer si tengo aplicado algún parche o vulnerabilidad crítica en mi electrónica de red?

✓ Sí, OpenNAC Enterprise, a parte, de ayudar a bastionar (desplegar) las políticas de configuración de la electrónica de red, aunque no gestiona parches, identifica desviaciones respecto a configuraciones seguras y documentadas.

Preguntas más frecuentes sobre OpenNAC Enterprise

- ❓ **OpenNAC Enterprise segmenta la red si detecta un ataque o cualquier actividad maliciosa, ¿quiere decir esto que el endpoint o los endpoints infectados se traslada a una VLAN aislada? ¿Cómo sería el funcionamiento de esta funcionalidad?**
- ✅ Hay que aclarar que OpenNAC Enterprise no es una herramienta de detección de amenazas al uso como IDS o SIEM. La información del procesamiento de datos obtenido a través del sensor puede enviarse a herramientas externas a través de syslog o mediante integraciones APIRest, como, por ejemplo: AntiVirus, AntiMalware, SIEMs, etc. Cuando OpenNAC recibe un evento que genere la necesidad de reubicar lógicamente un dispositivo dentro de la red, se comunica activamente con la electrónica de red para esta acción (RADIUS CoA o SNMP). Siempre que exista una VLAN de cuarentena conocida se podrá indicar a los switches por ejemplo que una sesión de un dispositivo a ella para limitar su conectividad y facilitar su remediación.
- ❓ **¿Qué es el agente soluble de OpenNAC Enterprise? ¿Cómo funciona? ¿Es compatible con dispositivos minimalistas a nivel de sistema como pueden ser los de IoT?**
- ✅ El agente soluble permite conocer la postura de seguridad de los dispositivos en el momento en el que se ejecuta, no requiere permisos de administrador ya que no se instala en los dispositivos. Nació sobre la necesidad de escenarios donde se quiere controlar el acceso a la red de dispositivos no corporativos de flujos de portal cautivo como Invitados o BYOD. Agente multiplataforma soportado en sistemas operativos Windows, macOS y varias distribuciones Linux, por lo que sería necesario acotar que OS utilizan estos dispositivos para poder evaluarlo mejor.

Preguntas más frecuentes sobre OpenNAC Enterprise

- ❓ **¿Cuántas conexiones simultáneas se podrían soportar en la red gestionada por OpenNAC Enterprise? ¿Y en el acceso remoto?**
- ✅ No existe una limitación exacta de conexiones simultáneas para infraestructuras de OpenNAC Enterprise ya que todas las arquitecturas están planteadas para poder crecer horizontalmente y adaptarse a entornos de mayor volumen de dispositivos. Existen actualmente arquitecturas desplegadas desde para unos cientos de dispositivos hasta para organismos con más de 150.000 dispositivos.