Visibilidad: el requisito previo para la seguridad

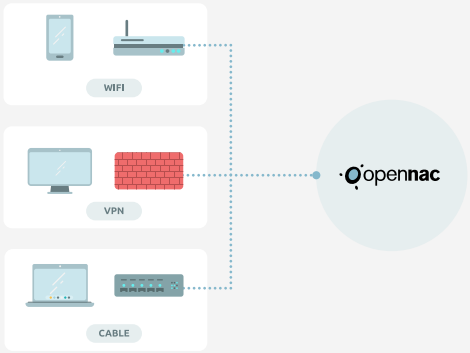
En 2020 habrá más de 30 mil millones * de dispositivos conectados, la inmensa mayoría serán sencillos y no tendrán la capacidad de instalar controles de seguridad estándar. Como estos dispositivos están especialmente diseñados para su fácil manejo por parte del usuario, los cuales generalmente se conectan y juegan, muchas unidades de negocio los comprarán e implementarán sin antes aprovisionarlos con operaciones de red y seguridad.

Si añadimos el Tsunami de IoT al status quo de oficinas dispersas, personal remoto, proveedores de servicios / colaboradores, BYOD, implementando lo nuevo mientras se mantiene lo viejo en electrónica heterogénea, no es de extrañar que los reguladores y auditores estén presionando a la organización para tener una mayor visibilidad de dispositivos que se conectan a la red.

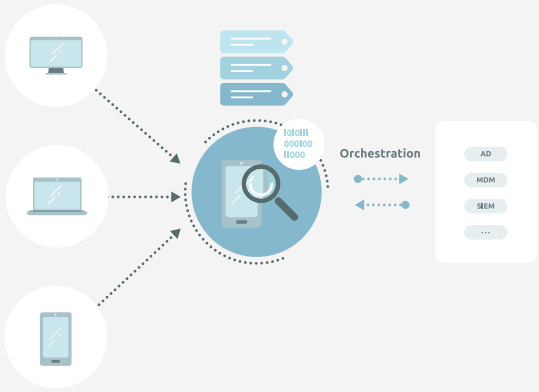
Cada uno de estos puntos débiles es un ataque potencial y / o punto de reconocimiento.

La visibilidad y el control de los activos es CIS ** 's Control de seguridad Nº1

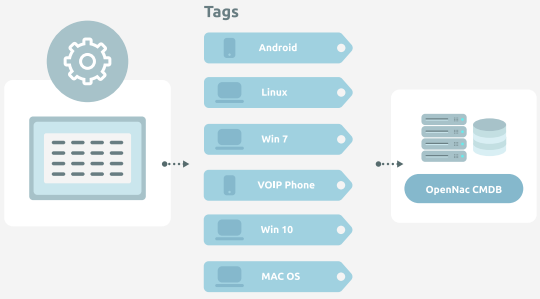
1. Descubrimiento



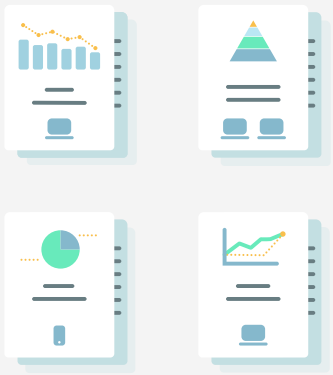
2. Perfilado



3. Registro



4. Valor



* https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

** CIS (Center for Internet Security, Inc.) es una entidad sin fines de lucro que aprovecha el poder de una comunidad global de TI para proteger a las organizaciones privadas y públicas de las amenazas cibernéticas https://www.cisecurity.org

¿Por qué openNAC Enterprise visibility?

OpenNAC Enterprise es una solución “Software first”, permite a las organizaciones conocer y perfilar todos los dispositivos conectados con un impacto mínimo en la red para poder agregar capas de visibilidad y control adicionales que permiten ajustar la seguridad según sea necesario.

La visibilidad se implementa en todos los dispositivos a través de todas las capas de acceso; cable, wi-fi y VPN. La visibilidad es en tiempo real, conectada, y continua. Además de los cambios de estado, que obligarán a una revisión de los activos, también puede establecer procesos de revisión periódicos.

- Como la solución es software first, es adaptable de forma nativa.
- Es vendedor-agnóstico.
- Aplicable a los activos con y sin 802.1x .
- Con y sin agente.
- Utiliza técnicas activas y pasivas para obtener el máximo conocimiento según el contexto.
- Se adapta a múltiples fuentes de identificación.
- Su información de activos se puede ampliar fácilmente para aplicar la lógica de negocios manualmente o a través de terceros.

  Establecer la naturaleza crítica de los dispositivos para facilitar la aplicación de políticas y reportes y así responder a los requisitos de auditoría o a la gestión de incumplimiento.

Toda esta información se procesa mediante restful APIs. Esto significa que la información es fácilmente consumida por terceros, como SIEM, para darles un contexto más amplio y ayudar a las organizaciones a aprovechar su “stack” de seguridad existente. La información se envía al punto de aplicación y decisión de política centralizada para aplicar controles granulares. Estos controles responden directamente a las necesidades de la organización ya que la lógica comercial está integrada en la información de activos.

Modos de Visibilidad :

Las organizaciones pueden implementar uno o los tres de los siguientes modos de visibilidad:

Nombre		Modo de dispositivo en la red	Modo Sensor	Modo de Agente
Fuente		Layer1-4	Layer 2-7	Sistema Operativo
Visibilidad de la red de tráfico			Inspección del tráfico de la red de Deep Packet	
Visibilidad de Activos	**Descubri-miento**	802.1x accounting events DHCP requests events MAC table for Switches and routers SNMP traps events Custom reader	El sensor se conecta al dispositivo de red a través del port span. Este dispositivo recopila múltiples protocolos de capa de aplicación que incluyen: DNS,DHCP,FTP,HTTP,IRC,SM-TP,SSH,SIS… para descubrir dispositivos.	La instalación de un agente en endpoints ofrece información detallada sobre los endpoints, incluido el inventario completo de hardware y software. Esta información puede enriquecer tanto el dispositivo de red como el modo de sensor y el agente también puede habilitar políticas de cumplimiento reales y precisas
	Perfilado	Vendedor de MAC Banners / solicitudes HTTP, etc Servicio de información Consultas SNMP Banner Puerto de información Huella dactilar de DHCP Huella digital del sistema operativo + Inventario granular de SW/HW + Servicios, procesos + Procesos de seguridad + Postura de seguridad (parches, estado de la aplicación…)		

Perfilado utilizando Tags/Etiquetas y tipos

Tipos

Por defecto, las tecnologías openNAC incluyen las capacidades para detectar el tipo de dispositivos conectados a la red en función de diferentes herramientas y procesos, esto se denomina perfil de activos. Hay dos métodos para crear perfiles:

1. **Perfiles automáticos:** el sistema incluye reglas de creación de perfiles que se actualizan con frecuencia para cubrir la gran mayoría de los tipos de dispositivos; Cámaras IP, computadoras de escritorio, teléfonos móviles, teléfonos IP, etc.

2. **Perfilado manual:** el administrador puede definir manualmente las reglas de creación de perfiles con unos pocos clics para expandir el conjunto, responder y definir los tipos de dispositivos específicos (activos) conectados a la red utilizando algunos de los siguientes métodos; Huella dactilar DHCP, Puertos.

Tags/ Etiquetas

A medida que la cantidad y el tipo de dispositivos crecen exponencialmente, es fundamental contar con un sistema flexible para adaptarse horizontalmente a ese crecimiento. OpenNAC usa Tags para dispositivos de perfil. Los Tags representan características del dispositivo, como IP, MAC, proveedor, ID de puerto, etc. Estos son ejemplos de datos estructurados por dispositivo, pero también crean, sobre la marcha, Tags no estructuradas para adaptarse a la creciente cantidad de información del dispositivo (tipo de dispositivo, puertos abiertos, Información de seguridad…)

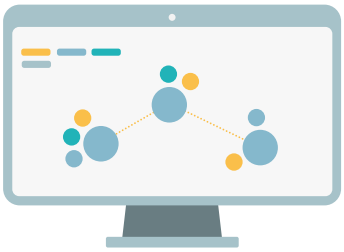
Toda la información de los activos se almacena en una CMDB, que guarda todas las características y atributos en un esquema flexible que se puede expandir fácilmente de forma manual o mediante información de terceros. La organización puede aplicar lógica comercial a través de tags/etiquetas para identificar activos críticos, categorías de IoT, etc.

La creación de perfiles se realiza utilizando múltiples mecanismos según el tipo de implementación que requiera la organización. Los Tags/etiquetas se aprovechan para crear políticas de acceso y establecer controles.

¿Cómo aprovechar los datos?

Perfil de negocios Dashboards

Agrupa diferentes políticas y luego identifica los activos que coinciden con estas reglas de acceso a la red. Muy útil para la gestión del progreso, a un alto nivel, de una situación dada.



Vista CMDB

Aprovecha la CMDB interna aplicando filtros; estructurado (proveedor, MAC, nombre de host, propietario ...) y etiquetas no estructuradas (tipo de dispositivo, puertos abiertos, estado de seguridad ...)

Búsqueda gratuita en el motor de Analytics

El módulo de análisis de openNAC proporciona un poderoso motor de búsqueda que permite encontrar abiertamente cualquier dato, esto se cruza con toda la información (activos, tráfico, etc.)

No intrusivo / todo incluido

- **La implementación en la nube requiere cero infraestructura o mantenimiento.**

  VMs on-premise no requieren HW.

- **Escala horizontalmente para satisfacer las necesidades cambiantes.**
- **Multivendor amistoso / vendedor agnóstico.**
- **Se adapta a su infraestructura de red.**
- **Actualizaciones HW / SW y actualización.**
- **Control a través de todas las capas de acceso (Wi-Fi, Cable, VPN y aplicaciones)**