Servicios de Ingeniería y Capacitación

INFRAESTRUCTURA DE RED

Tecnología FORTINET

Arquitectura & Seguridad NAC

Revisión 2.0

Enero 2024

ARQUITECTURA DE RED

La compañía debe adquirir infraestructura de red fabricada por una empresa de clase mundial, con fuerte orientación a la seguridad de red y líder en gestión unificada de amenazas de ciberseguridad. Los productos y servicios adquiridos deben ofrecer una gran protección integrada y de alto rendimiento contra los vectores de ataque a la seguridad. Contar con el mayor control y que simplifique las funciones de gestión y configuraciones.

Ser un hardware con alta aceleración y el mejor de la categoría en relación precio -rendimiento con una interfaz de administración intuitiva.

Criterios esenciales de adquisición de Infraestructura de Red:

- Mejor relación de retorno sobre la inversión.
- Gestión Centralizada y Ciberseguridad.
- Mayor capacidad de detección de amenazas.
- Alta tolerancia a fallos y redundancia.
- Escalabilidad e integración Security Fabric.
- Mejor soporte de la marca.
- Mayor personal certificado en el mercado.

FIREWALL & SEGURIDAD PERIMETRAL

La Nueva Generación de Firewall que la compañía debe adquirir requiere los siguientes aspectos:

Proteger: Evitar las brechas y las interrupciones del negocio minimizando el riesgo de ransomware y otros ciberataques con la segmentación, la visibilidad total y la seguridad coordinada.

Consolidar y escalar: Reducir los costos y ofrecer seguridad a hiperescala para seguir el ritmo de escalabilidad de la red de la compañía

Accesibilidad: Alta conectividad y eficiencia operativa con una seguridad coherente, coordinada y automatizada desde cualquier lugar.

Figure 1: Magic Quadrant for Network Firewalls

Source: Gartner (November 2021)

GESTIÓN SDWAN

Las soluciones SD-WAN es requerida para lograr una conectividad rápida, escalable y flexible entre diferentes redes de la compañía y busca permitir adaptarse rápidamente a las demandas cambiantes del negocio, entre otras cosas proporciona una arquitectura de WAN virtual que permite a la compañía aprovechar cualquier combinación de servicios de transporte, incluidos MPLS, 4G y servicios de Internet de banda ancha, para conectar de forma segura a los usuarios con las aplicaciones, aumentando la eficiencia de la red y dotando de tolerancia a fallos la compañía con una interesante reducción de costos.

Figure 1: Magic Quadrant for SD-WAN

Source: Gartner (September 2022)

SOLUCIÓN NETWORK ACCESS CONTROL (NAC)

La proliferación de dispositivos convencionales, BYOD e IoT requieren especial atención por parte de los oficiales de seguridad. La solución de control de acceso a la red NAC es una parte integral del modelo Zero Trust Access para la seguridad, en el que la confianza ya no debe ser implícita para los usuarios y las aplicaciones o los dispositivos que intentan acceder a la red.

La solución elegida de control de acceso a la red basado en 802.1X que mejore Security Fabric debe proporcionar visibilidad, control y respuesta automatizada en redes cableadas, inalámbricas y VPN.

ESCANEO DE APLICACIONES EN ENDPOINTS CON O SIN AGENTE.

INCORPORACIÓN SIMPLIFICADA Y AUTOMATIZADA PARA GRAN DENSIDAD DE USUARIOS Y DISPOSITIVOS.

INTEGRACIÓN CON FORTIGATE Y ACTIVE DIRECTORY.

CREA UN INVENTARIO DE TODOS LOS DISPOSITIVOS DE LA RED.

MICROSEGMENTACION PARA USUARIOS Y DISPOSITIVOS ACTIVOS DE LA RED.

AMPLIO SOPORTE CON PROVEEDORES Y DISPOSITIVOS DE RED.

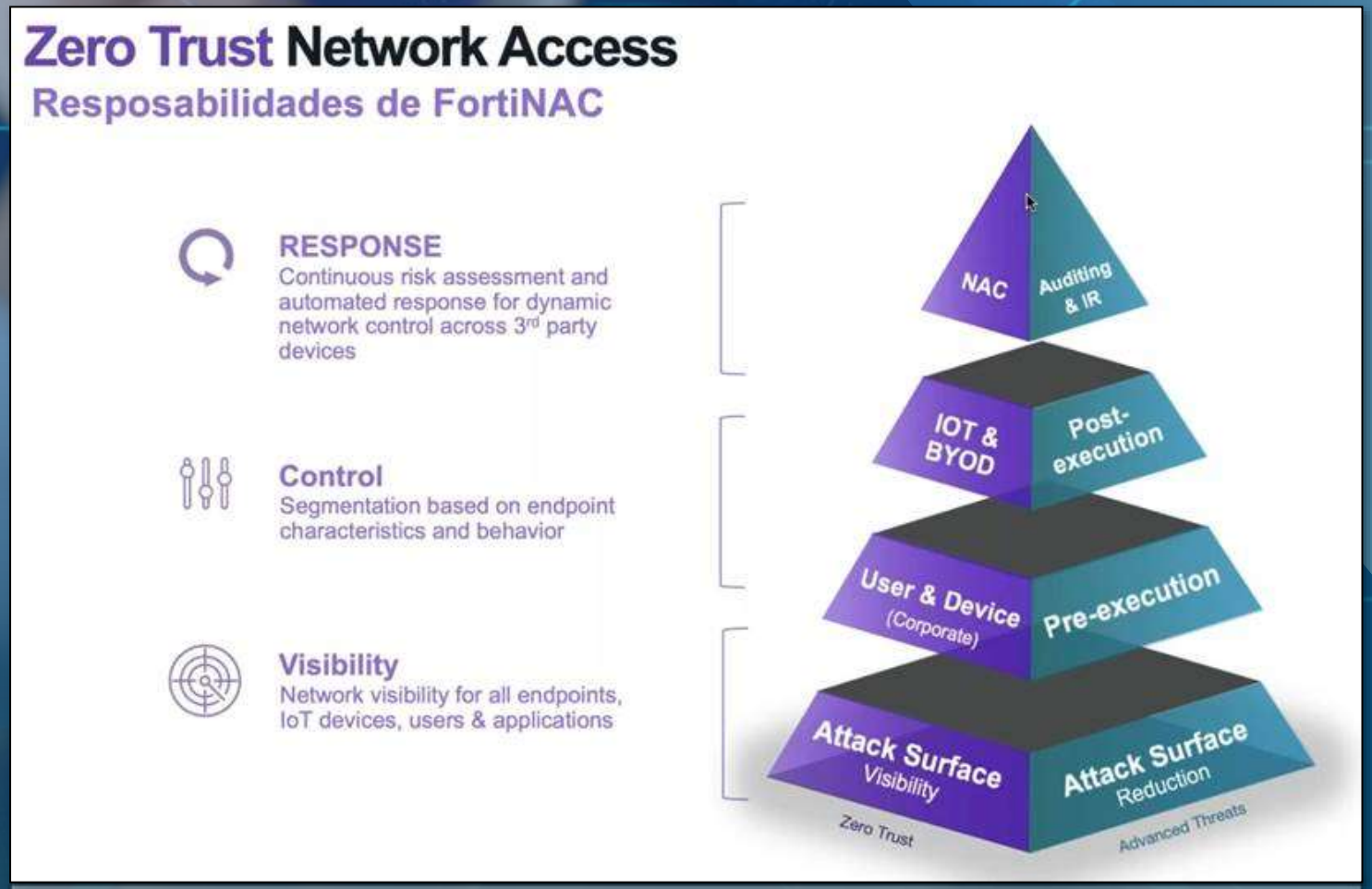
PORTAL CAUTIVO PARA INVITADOS Y CONTRATISTAS.

EVALUA LOS RIESGOS DE CADA DISPOSITIVO DE RED.

ZERO TRUST NETWORK

La seguridad tradicional de las redes informáticas se basa en el concepto perimetral. En donde si se rompe la seguridad perimetral, el atacante puede moverle libremente por el interior de la red.

La seguridad Zero Trust es un modelo/Filosofía de seguridad que establece como principio en que no se debe confiar en nadie tanto fuera como dentro de la red. Esto significa que para un dispositivo o usuario pueda acceder a la red debe realizar una estricta verificación de identidad.

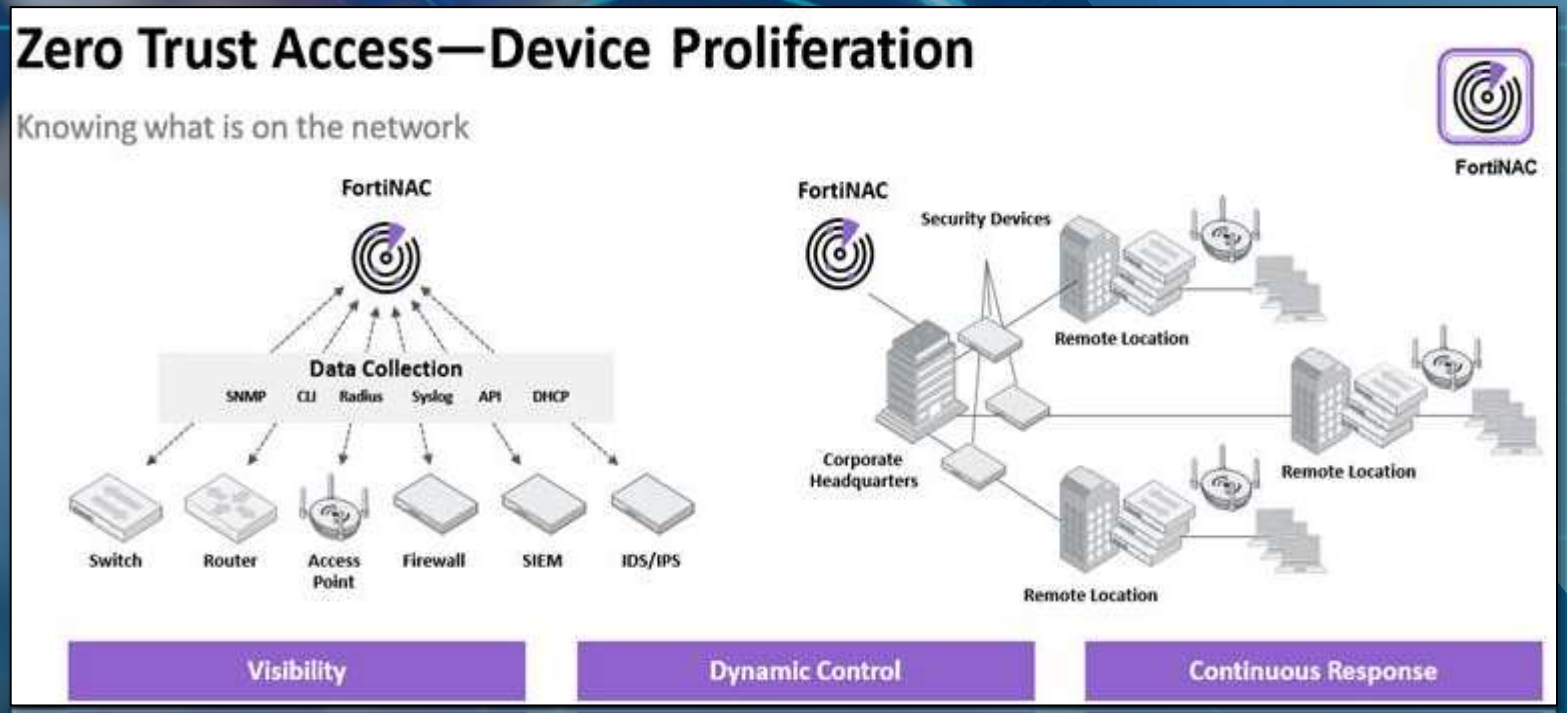


MICROSEGMENTACIÓN

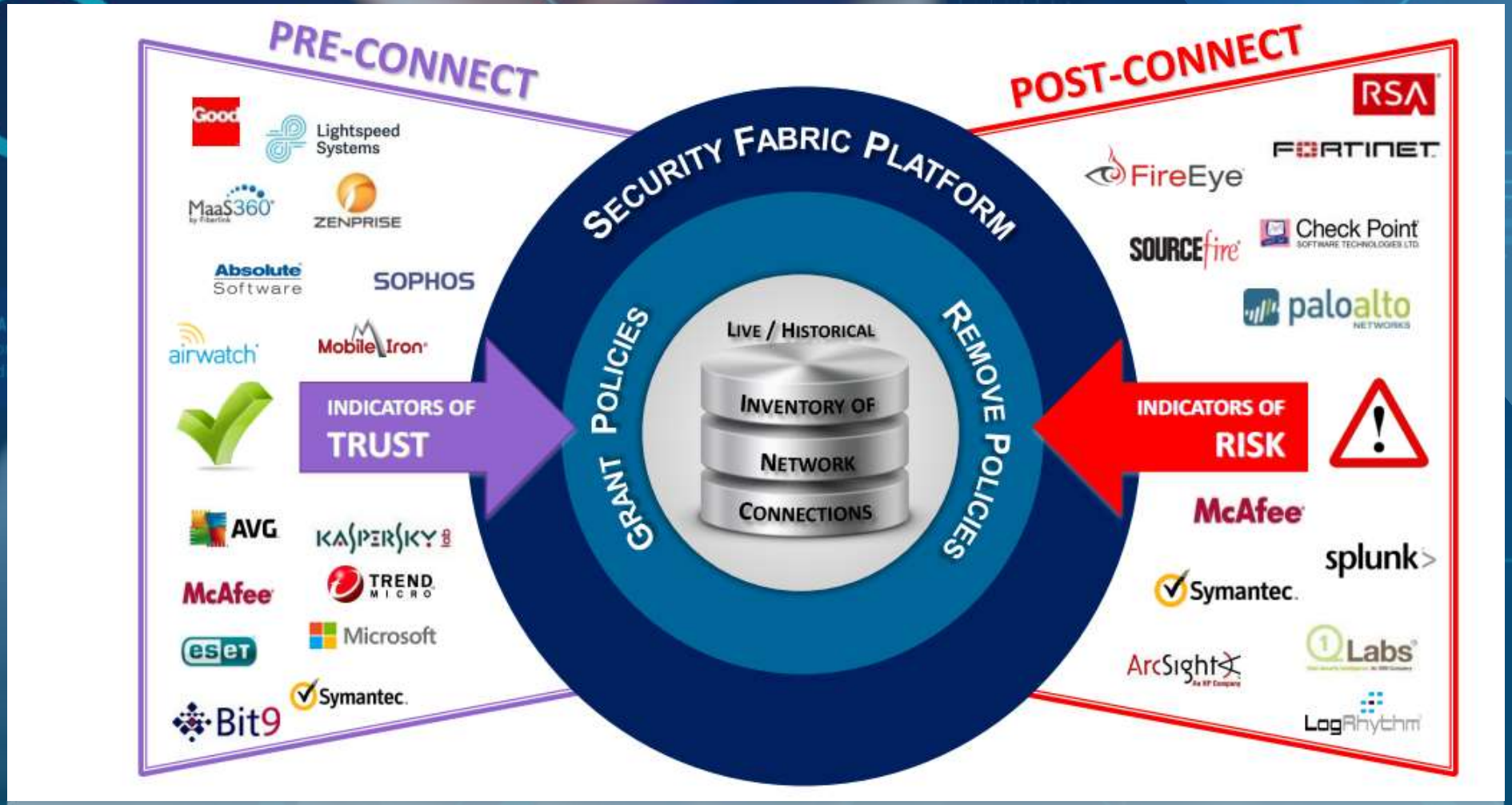
FortiNAC es capaz de limitar a dónde pueden ir o no los dispositivos y usuarios sobre la red. Para ello implementa microsegmentación y realiza cambios en las configuraciones en los dispositivos de red basado en políticas de seguridad.

La recolección de información hacia la base de datos de FortiNAC utiliza diferentes protocolos estándar y de uso común en todos los fabricantes.

Esto permite la integración con miles de tipos de dispositivos de red.



INDICADORES DE RIESGO Y CONFIANZA.

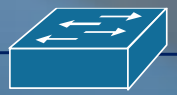


PROCESOS DE AUTENTICACIÓN

Agente persistente
MAC : AB:CC:12:15:BC:12
Usuario: Userlab_04

Interfaces	MAC	VLAN
Fast 0/19	**AB:CC:12:15:BC:12**	**1**

F 0/19



El switch con su interface Fast 0/19 en la VLAN de aislación notifica mediante un SNMP TRAP a FortiNAC

FortiNAC Validara el usuario en el AD mediante el agente.

Active Directory

Luego de Validar el usuario verificara las Políticas de seguridad y asignara a una VLAN correspondiente. Etiquetara al usuario con agente persistente.

FortiNAC modifica la interface del SW para la Vlan Corporativa.

Interfaces	MAC	VLAN
Fast 0/19	**AB:CC:12:15:BC:12**	**100**

El agente persistente reside en la máquina host perteneciente al dominio de AD y funciona junto con el FortiNAC para completar tareas como registro, autenticación y escaneo (adaptadores, aplicaciones, etc.).

PROCESOS DE AUTENTICACIÓN

Interfaces	MAC	VLAN
Fast 0/19	AB:CC:12:15:BC:12	1

El switch con su interface Fast 0/19 en la VLAN de aislación notifica mediante un SNMP TRAP a FortiNAC

FortiNAC Presentara Portal Cautivo para usuario sin Agente.

F 0/19

Active Directory

Sin Agente persistente
MAC : AB:CC:12:15:BC:12
Usuario: Juan Perez

Interfaces	MAC	VLAN
Fast 0/19	AB:CC:12:15:BC:12	122

FortiNAC
Lo etiqueta como Rogue y solicitara registro mediante Portal Cautivo.

El portal cautivo se inicia automáticamente en los dispositivos no pertenecientes al dominio del AD y se notifica al usuario que se encuentra en una red cautiva. Una vez que el portal cautivo se inicia, el usuario ingresa información para registrarse.
Este proceso es habitualmente usado para contratistas o asesores externos.

FortiNAC Realiza Validacion con Active Directory.

El usuario ingresa los datos Solicitados Por el Portal Cautivo.

F 0/19

Active Directory

Sin Agente persistente
MAC : AB:CC:12:15:BC:12
Usuario: Juan Perez

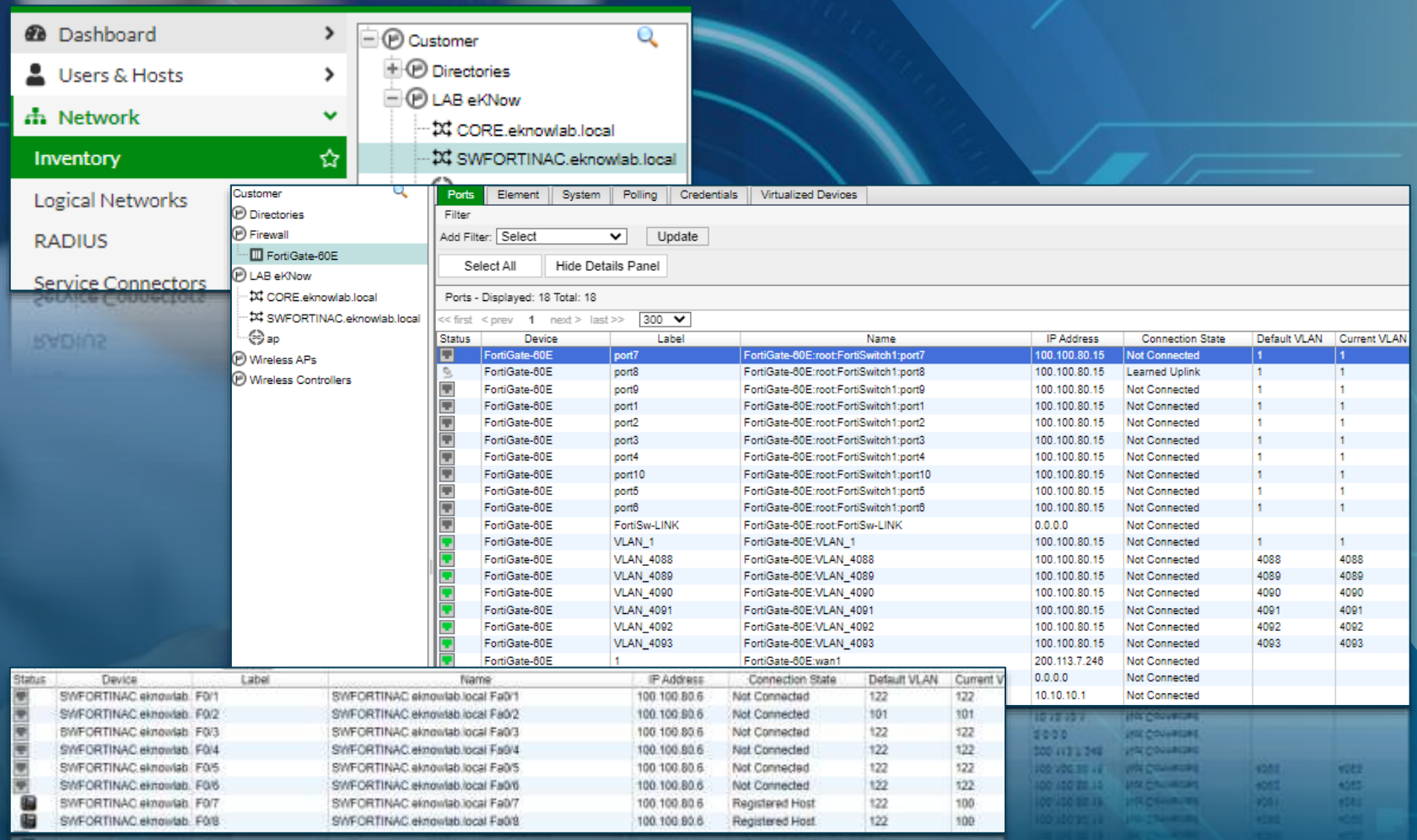
Interfaces	MAC	VLAN
Fast 0/19	AB:CC:12:15:BC:12	101

Luego de Validar el usuario verificara las Políticas de seguridad y asignara a una VLAN correspondiente. Etiquetara al usuario como BYOD.

eKNOW

ACTIVOS DE INFORMACIÓN

FortiNAC crea un árbol de inventario con los dispositivos de red. Permite obtener información en tiempo real de la interface y dispositivos conectados. Gestiona la interface y obtiene la configuración de Startup-Config y Running-Config



SOLUCIÓN FÍSICA O VIRTUAL APPLIANCE

FortiNAC-CA-500C

Integrated Control Server and Application Server

Small Environments

Manages up to 2000 ports in the network

VM SERVER Small Environment

Vcpu : 4
Memory : 16 GB
Disk : 100 GB
Up to 2000 ports in the network*

FortiNAC-CA-600C

Integrated Control Server and Application Server

Medium Environments

Manages up to 15 000 ports in the network*

VM SERVER Medium Environment

Vcpu : 20
Memory : 32 GB
Disk : 100 GB
Up to 15 000 ports in the network*

FortiNAC-CA-700C

Ultra High Performance Control and Application Server

Large Environments with few Persistent Agents

Manages up to 25 000 ports in the network*

VM SERVER Large Environment

Vcpu : 36
Memory : 96 GB
Disk : 100 GB
Up to 25 000 ports in the network*

Expertos en Seguridad

- ☑ **Empresa con 17 años** de trayectoria e ingenieros certificados y expertos en ciberseguridad, acreditados en ISO/IEC 27001.
- ☑ **Líderes en auditoría** e implantación de modelos avanzados de gestión de ciberseguridad y cumplimiento normativo.
- ☑ **Seguridad 360º** para la protección de la seguridad y enfocados en la mitigación del riesgo de nuestros clientes.

Av. Pedro de Valdivia 555, Oficina 801, Providencia • Correo: info@eknow.cl • http://www.eknow.cl