



SECURIZANDO CON CSA / ARUBA



JAVIER PEREZ

9,5min



5 ideas

Aruba Security

Foco en Seguridad

IntroSpect

Behaviour Based Attack Detection, Risk Visibility, IoT Aware

ClearPass

Discovery, Profiling, Identity, Authorization, Context Share, Enforce, Attack Response

Aruba Mobile First Infrastructure with Aruba Secure Core

Secure Boot | Encryption | DPI | VPN | IPS | Firewall

Bases de
datos
AD, MDM...

Firewall

Cloud
Apss

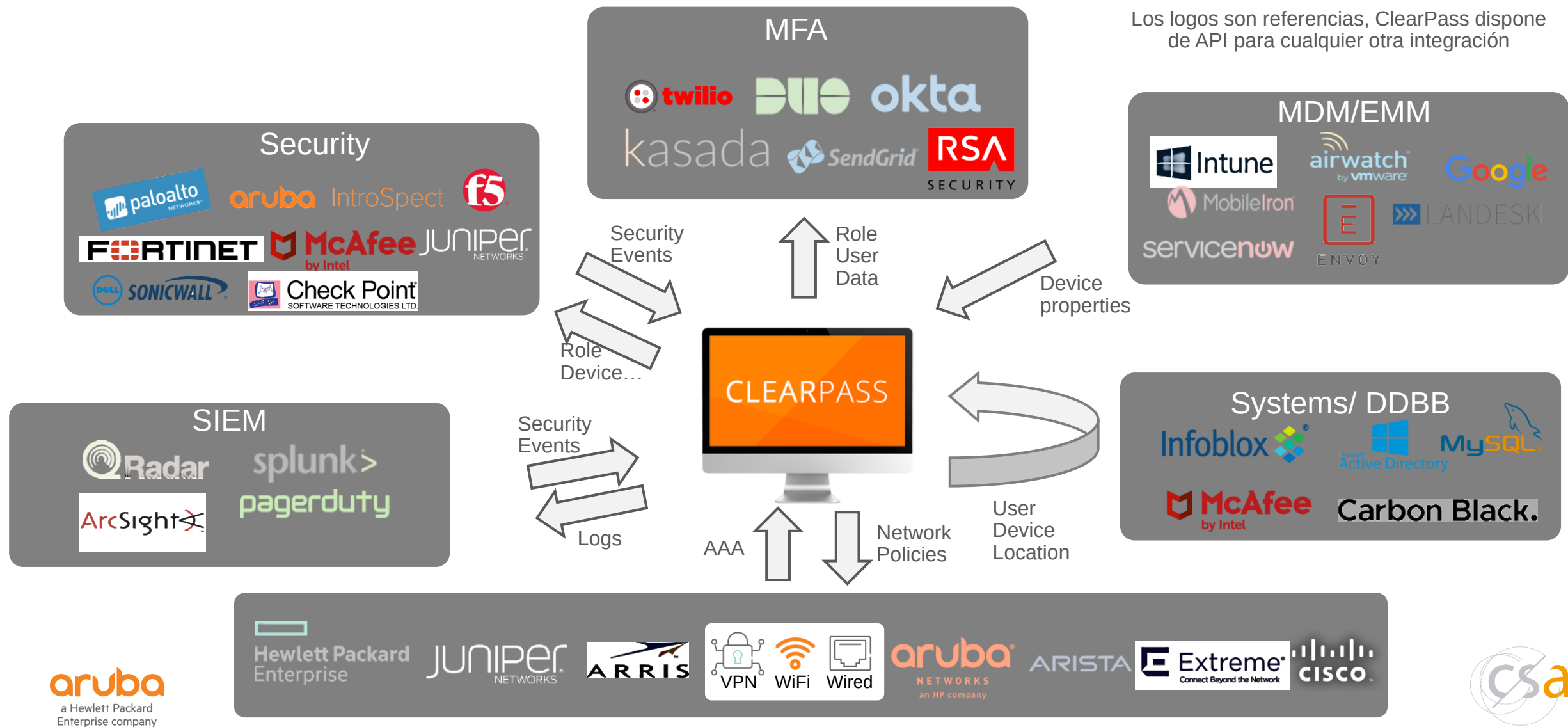
Servers

ClearPass



Respuesta

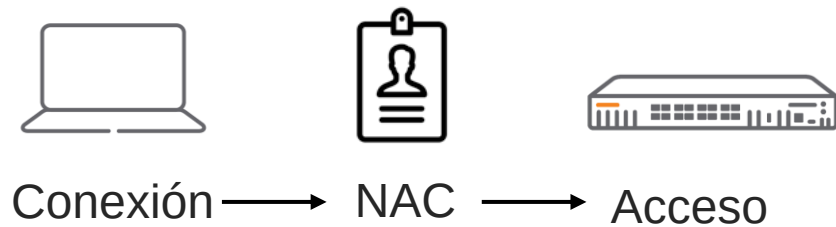
Integraciones con terceros



Adaptación de las autenticaciones según necesidades

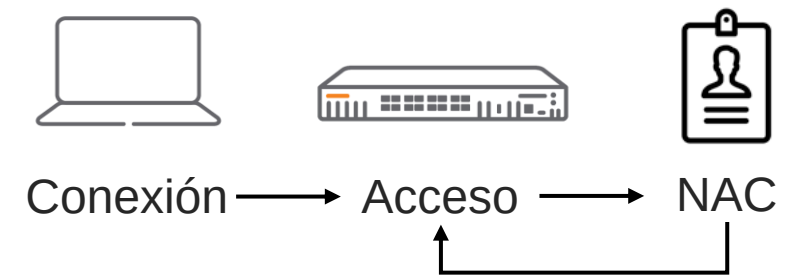
Pre-Auth & Post-Auth

Pre-Authentication



- Control de acceso durante conexión inicial
- Asignación de políticas antes del acceso
- 802.1x, MAC-Auth, EAP-TLS, Guest...
- Validación con fuentes autenticación.

Post-Authentication

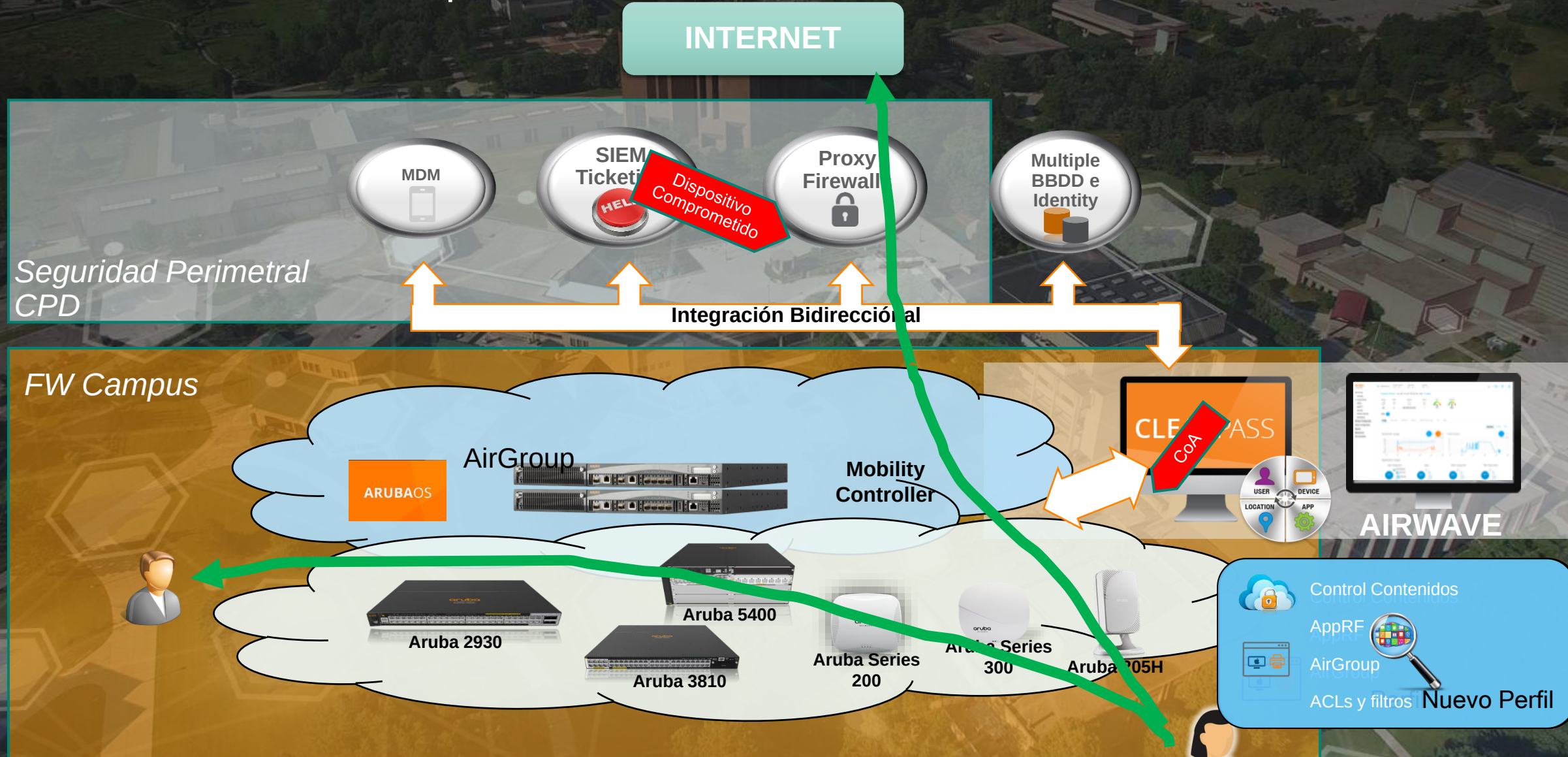


- Permitir el acceso del dispositivo inicialmente
- Validación del acceso con autenticación posterior
- Envío SNMP con autenticadores
- Reasignación de seguridad tras la validación

ClearPass soporta ambos métodos, adaptación según necesidades

Seguridad extendida en el campus

Elementos básicos de la arquitectura



FW interno de campus y extension de la seguridad al dispositivo

WPA3



¿Que novedades trae WPA3?



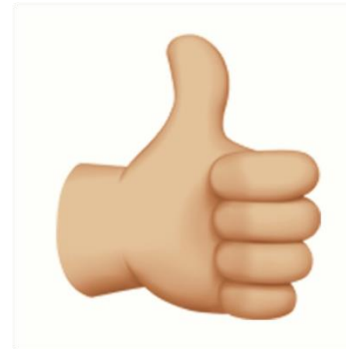
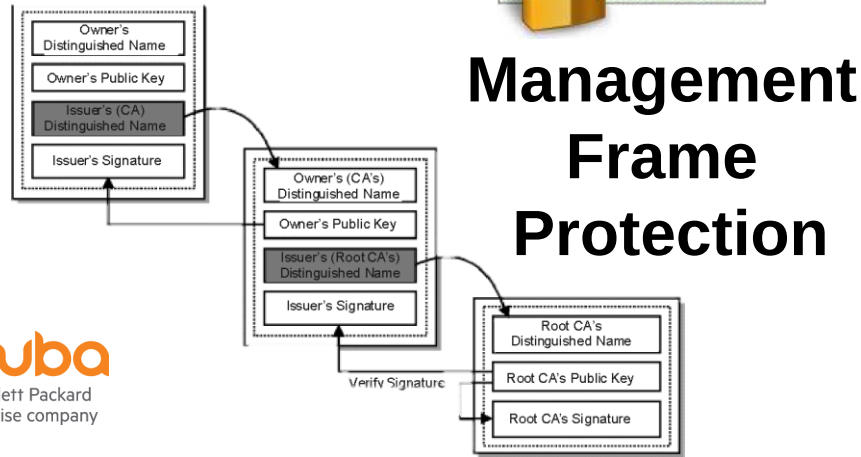
“OWE”: Todo el tráfico WiFi cifrado



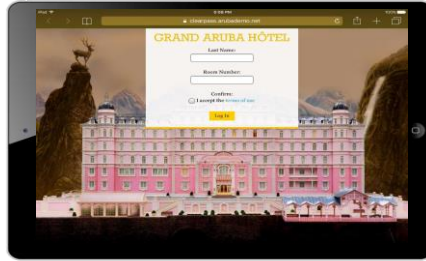
“SAE”: clave compartida “invulnerable” frente a ataques



“SUITE B”: cifrado de grado militar



Implicaciones prácticas de WPA3



“OWE”: Todo el tráfico
WiFi cifrado

Obligatorio

Upgrade SW



“SAE”: clave compartida
“invulnerable” frente a ataques

Obligatorio

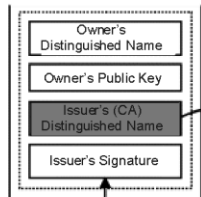
Upgrade SW



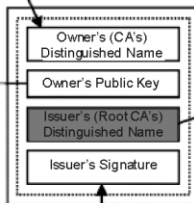
“SUITE B”: cifrado de
grado militar

Opcional

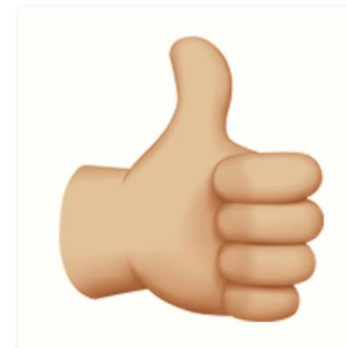
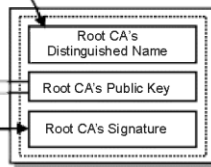
Nuevo HW



Management
Frame
Protection



Verify Signature



Obligatorio

Upgrade SW

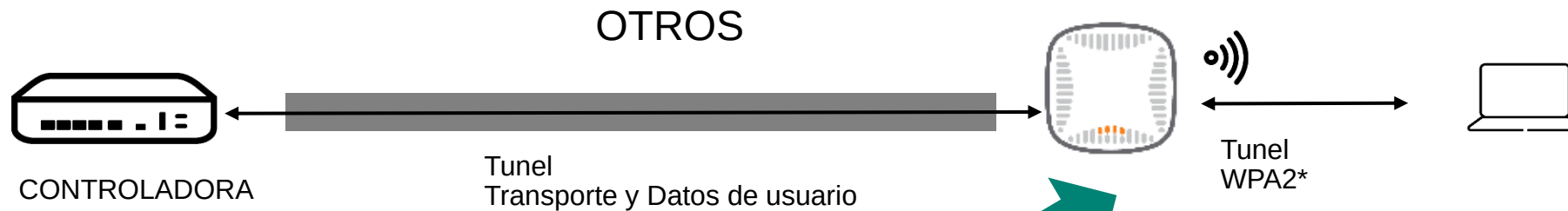
MultiZona



Comparación tratamiento del tráfico WPA2 Aruba vs Otros Fabricantes



Fortaleza: Trafico llega cifrado a la controladora. No es posible manipulación intermedia.

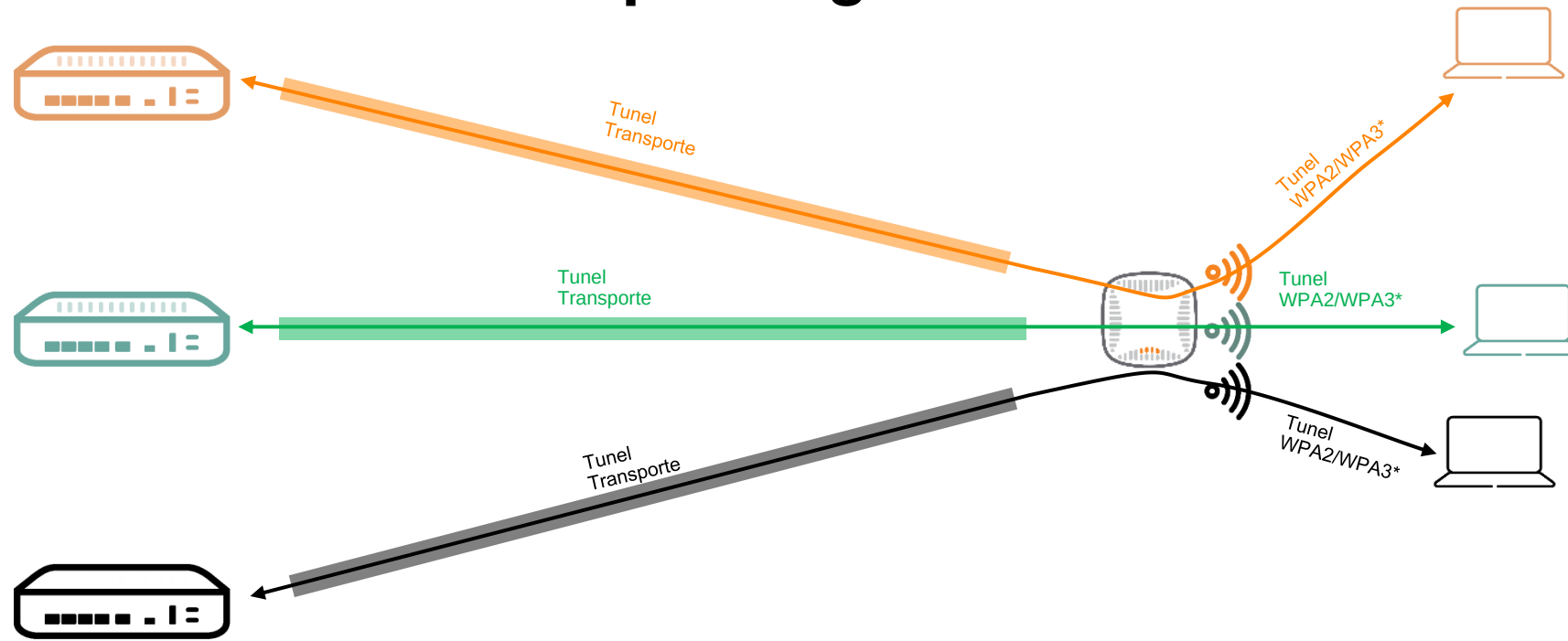


*Punto débil:
Trafico se cambia de túnel*

Aruba Multizona

Punto de Acceso dando servicio a Múltiples Dominios

Seguridad sin alterar el paradigma



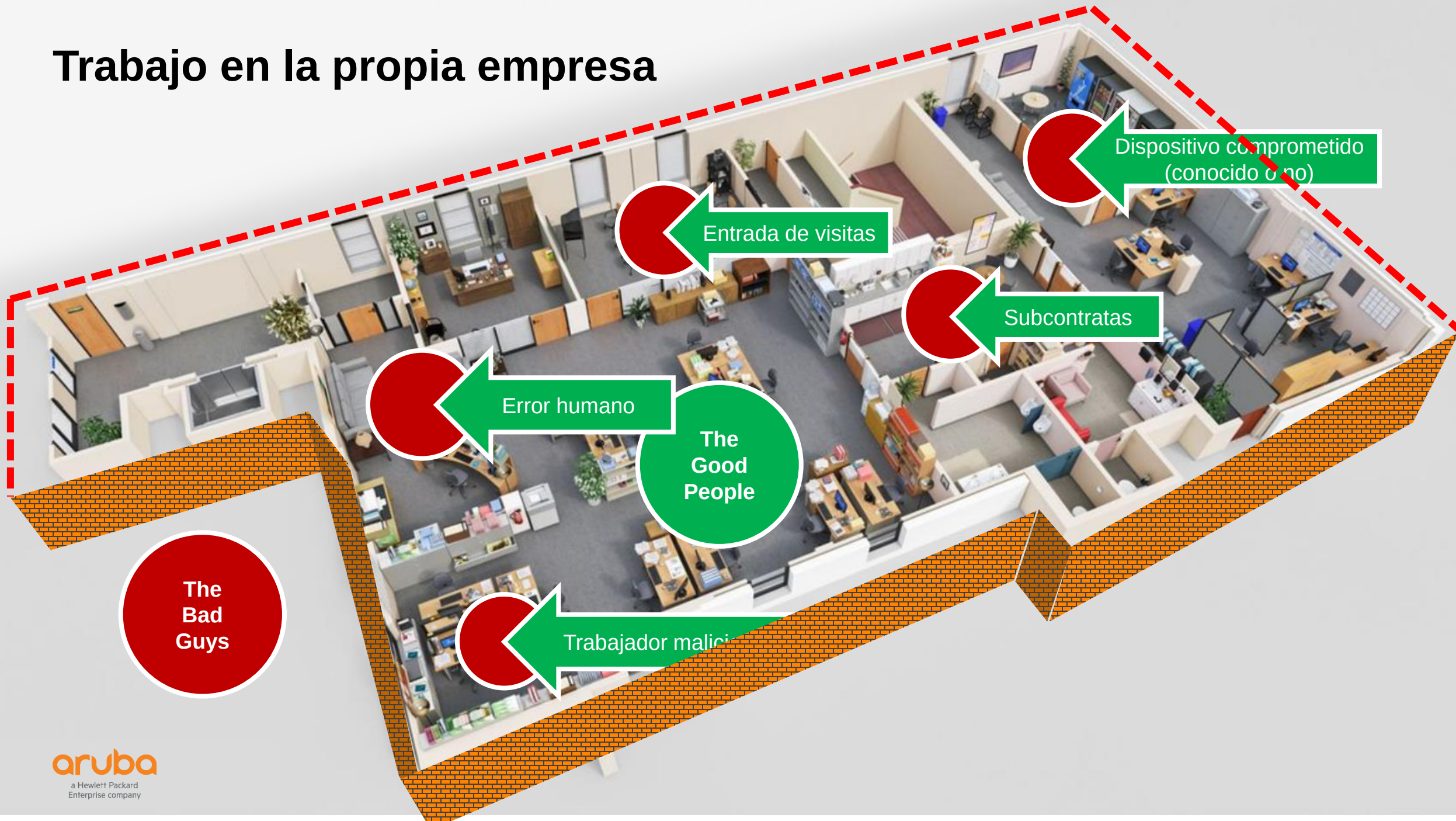
En la solución Multizona un mismo Punto de Acceso sirve a varias controladoras, pero **el aislamiento del tráfico está GARANTIZADO** debido al túnel Extremo a Extremo entre controladora y Cliente WiFi

* Tunel WPA3 también será transportado extremo a extremo cuando sea liberada la funcionalidad

Introspect

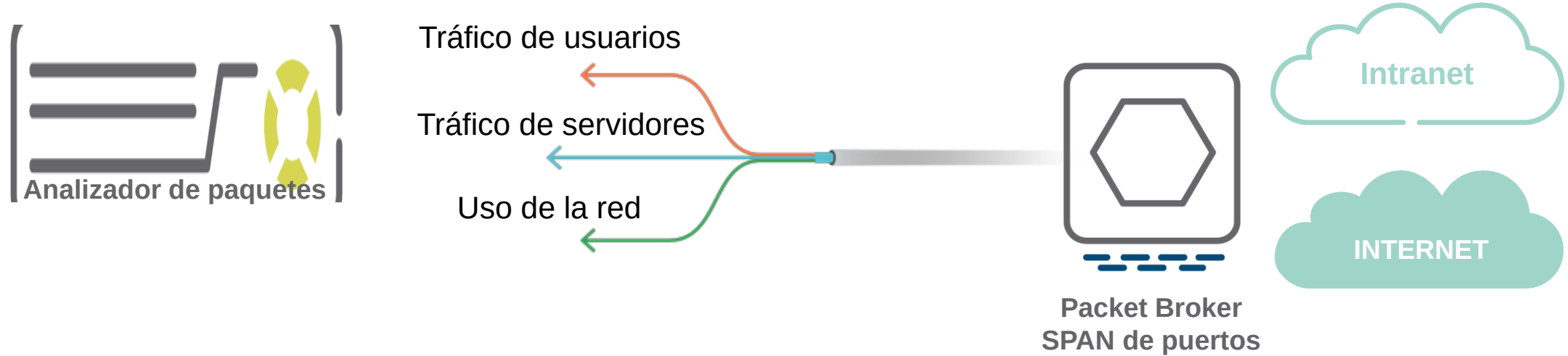


Trabajo en la propia empresa



Análisis por Comportamiento

¿Qué son las soluciones NTA? (Network Traffic Analysis)



Ventajas

- Visión de todo el tráfico de red
- Posibilidad de análisis de paquetes
- Tráfico interno y externo

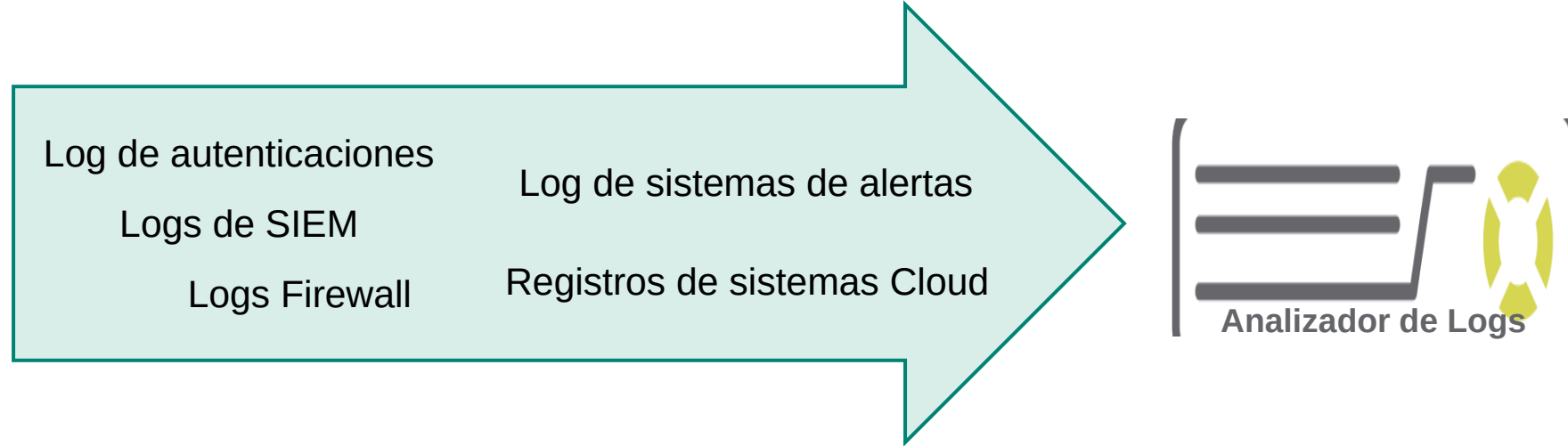


Desventajas

- Difícil correlación con usuarios
- No obtiene info. de otros sistemas
- Necesita visión de todo el tráfico

Análisis por Comportamiento

¿Qué son las soluciones UBA? (User Behavior Analytics)



Ventajas

- Visión del uso de sistemas
- Correlación de uso en toda la red
- Información contextual

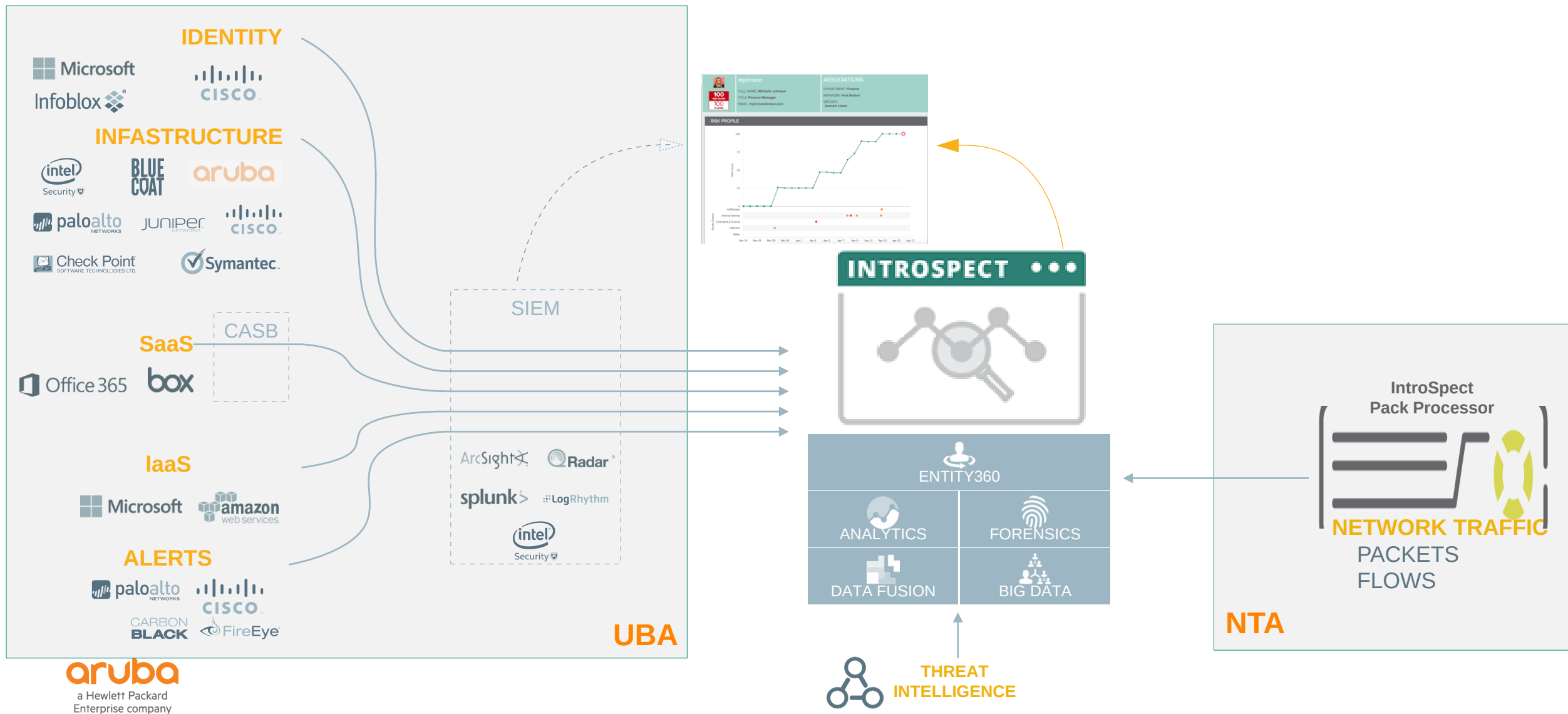


Desventajas

- Falta de visión de tipo de tráfico
- Desconocimiento de destinos
- Información incompleta

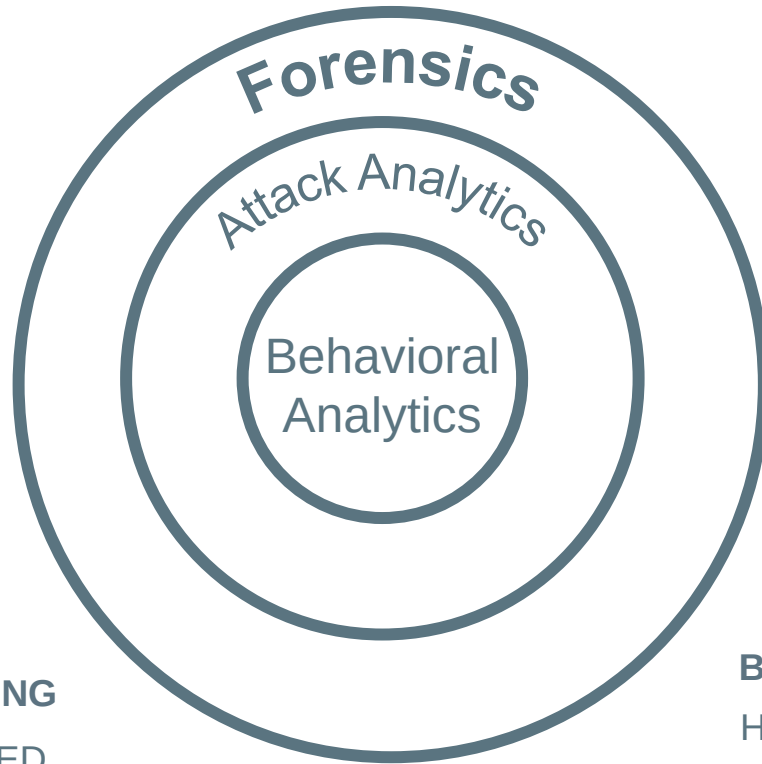
IntroSpect, solución UEBA

UEBA (User and Entity Behavior Analytics)



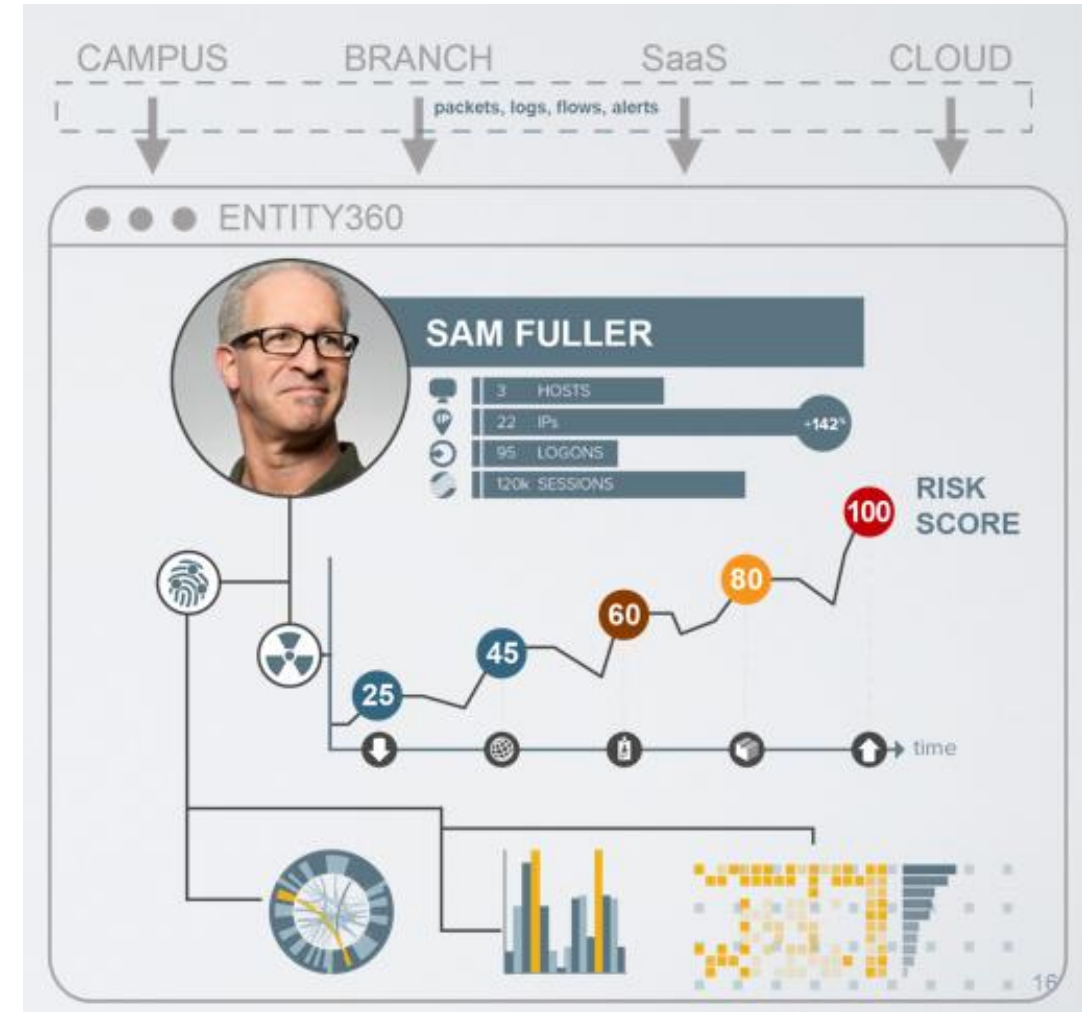
IntroSpect

Aplicación de ML y análisis de todo tipo de datos



MACHINE LEARNING
SEMI- SUPERVISED
&&
UNSUPERVISED

BASELINES
HISTORICAL
+
PEER GROUP



Entorno Normativo



Centro Criptológico Nacional

Guía CCN-STIC-647B



Nueva guía CCN-STIC-647B, Configuración segura de equipos de red Aruba para entornos WiFi

Detalles

Publicado: 07 Febrero 2018

- Realizada gracias a la colaboración de la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid.
- Las redes WiFi están cada vez más extendidas y pese a los riesgos añadidos que las acompañan su uso en ciertas circunstancias se hacen necesarias.
- Contar con una guía que detalle cómo realizar adecuadamente un despliegue de una red WiFi ayudará a las Organizaciones a desplegar infraestructuras WiFi con unas medidas de seguridad apropiadas.
- La guía indica los pasos necesarios para realizar una instalación en equipos Aruba, pero puede servir como referencia para la instalación de arquitecturas basadas en otros fabricantes.

Las tecnologías inalámbricas son cada vez más habituales en nuestras organizaciones. Cada vez son más los dispositivos que las soportan y las organizaciones que las requieren para sus usuarios. Una de las más extendidas es la tecnología WiFi. Siendo evidentes las ventajas que ofrece no se deben pasar por alto los riesgos añadidos que suponen. Estos riesgos deben tratarse de forma que se pueda garantizar la confidencialidad, integridad y disponibilidad de estas infraestructuras así como de los datos que se transmiten haciendo uso de ellas.

En esta guía CCN-STIC se describen las medidas de seguridad mínimas recomendables para la instalación de una solución WiFi dentro de una Organización que quiere ofrecer este servicio a sus usuarios. Se excluye de la guía los servicios públicos ofrecidos mediante WiFi o servicios a invitados. Para ello se ha tomado como ejemplo los equipos del fabricante Aruba Networks, una compañía de Hewlett Packard Enterprise, concretamente el sistema ClearPass 6.6.8 y aquellos de la familia ArubaOS 6.5.4.

Dentro de la solución presentada se describen 3 niveles de seguridad que se recomienda aplicar antes de dar conectividad a cualquier usuario: un primer nivel en el que se autentica al usuarios mediante mecanismos robustos; un segundo en el que se analiza el estado de la máquina del usuario; y un tercero en el que se levanta un túnel VPN/IPsec.

La solución se explica quedando abierta a cualquier modificación que pueda hacer cada Organismo en función de su Análisis de Riesgos, de modo que pueda no implementar todos los niveles de seguridad o modificarlos (por ejemplo no levantar túneles VPN/IPsec, no comprobar el estado de la máquina o modificar las variables de comprobación). No se recomienda en ningún caso eliminar o modificar el primer nivel de seguridad.

Por otro lado, la arquitectura presentada puede servir como base a soluciones que requieran un nivel mayor de seguridad mediante el uso de dispositivos de hardware de cifra y que requieran protocolos específicos para su acreditación.

La guía comienza explicando el modelo de seguridad empleado para pasar a explicar el escenario que se ha tomado como ejemplo. Posteriormente da todos los pasos necesarios para la instalación de la arquitectura propuesta así como las tareas necesarias para mantener la seguridad del sistema, continúa con la implementación de los niveles de seguridad y termina con unas recomendaciones generales de seguridad. Se adjuntan varios anexos con comandos básicos, ejemplos de configuración de servidores y creación de certificados necesarios así como una lista de comprobación.

Está previsto seguir trabajando en otras guías del fabricante Aruba. En concreto se van a desarrollar guías CCN-STIC para switches ArubaOs-Switch (acceso y agregación) y switches ArubaOs-CX (Core Campus) así como para la solución Clearpass.

CCN-CERT (07/02/2018)

[CCN-STIC-647B Configuración segura de equipos de red Aruba para entornos WiFi](#)

Escenario completo Arquitectura ARUBA

Elementos básicos de la arquitectura



- CPP_ND_V1.0
- PP_NDCPP_APP_AUTHSVR_EP_V1.0



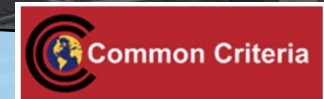
AIRWAVE



NetInsight



IntroSpect



- PP WLAN AS V1.0
- PP VPN IPSEC CLIENT V1.4



Mobility Controller



Mobility Master



Aruba 2930



Aruba 8400/8300



Aruba 3810



Aruba 5400



- CPP_ND_V2.0E
- INICIANDO CERTIFICACION



- CPP_ND_V2.0E
- INICIANDO CERTIFICACION



Aruba Series 200



Aruba Series 300



RESUMEN

CLEARPASS

WPA3

Multizona

Instrospect

**Catalogo
STIC**





aruba

a Hewlett Packard
Enterprise company

Muchas Gracias