UAX FP
Universidad
Alfonso X el Sabio

Integración de sistemas de control de acceso a redes (NAC) con inteligencia artificial para la detección proactiva de amenazas

ASIR / Presencial

Vladimir Edgar Carpio Morales

Tutor del TFG

UAX FP
Universidad
Alfonso X el Sabio

DEDICATORIA (OPCIONAL)

ÍNDICES

De contenido, tablas e ilustraciones. Se recomienda realizarlos de manera automática.

ABSTRACT

Con este proyecto se pretende integrar sistemas de Control de Acceso a la Red (NAC) con inteligencia artificial. La IA analizará los datos de acceso en tiempo real, reaccionará y se adaptará ante amenazas emergentes. A su vez, detectará posibles comportamientos anómalos, modificando las reglas de política de seguridad.

Para la integración, se utilizan las APIs de los sistemas de Control de Acceso a la Red (NAC). La diferenciación respecto a las soluciones tradicionales radica en la capacidad de modificar dinámicamente las políticas de seguridad, permitiendo una respuesta automatizada.

This project aims to integrate Network Access Control (NAC) systems with artificial intelligence. The AI will analyze access data in real time, react, and adapt to emerging threats. Additionally, it will detect anomalous behaviors and modify security policy rules accordingly.

For the integration, the APIs of NAC systems will be used. The key differentiation from traditional solutions lies in the ability to dynamically modify security policies, enabling an automated response.

JUSTIFICACIÓN DEL PROYECTO

Motivación principal del proyecto

A medida que crece la cantidad de dispositivos conectados a la red, la gestión del acceso a y redes corporativas se vuelve más compleja. Actualmente las soluciones de Control de Acceso a la Red (NAC) cuentan con políticas de acceso basadas en reglas estáticas que limitan su capacidad en adaptarse a amenazas emergentes.

Este proyecto solventa la necesidad de implementar una solución que utilice inteligencia artificial que analizara patrones de comportamiento, detección de anomalías en tiempo real y la solución que actúe de forma dinámica modificando las políticas de acceso.

Las principales soluciones de sistemas de Control de Acceso a la Red (NAC) actuales que existen en el mercado son Cisco ISE, Aruba ClearPass y FortiNAC, las cuales permiten la gestión de accesos y segmentación de redes. Sin embargo, estas soluciones no cuentan con un aprendizaje adaptativo basado en IA.

Existen soluciones similares en el mercado que utilizan inteligencia artificial para el análisis de anomalías de los sistemas de control de Acceso a la Red (NAC), pero con enfoques diferentes:

Característica	Aruba AI Insights	Cisco AI Endpoint Analytics	Fortinet FortiAI	Aportación del Proyecto Propuesto
Análisis con IA	Detecta anomalías en redes WiFi.	Identifica y clasifica dispositivos en la red.	Analiza y detecta malware y anomalías.	Aprende patrones de comportamiento en la red y detecta amenazas.
Modificación de políticas NAC	No modifica políticas.	No modifica políticas.	No modifica accesos.	Modifica dinámicamente las reglas de acceso según el análisis de IA. Aplica acciones

				correctivas
Compatibilidad con NACs	Solo Aruba.	Solo Cisco.	Independiente de NACs.	Open-source y compatible con múltiples NACs.

Marcos normativos y legales:

Proyecto debe cumplir con las siguientes normativas de seguridad y protección de datos:

- Reglamento General de Protección de Datos (GDPR) para garantizar el cumplimiento de la privacidad y protección de datos personales.
- Normativas ISO 27001 las cuales implementan normativas sobre las buenas prácticas de seguridad en la gestión de la información.
- Cifrado y copias de seguridad, para los datos manejados por el sistema sean encriptados y se establecerán mecanismos de respaldo para evitar pérdidas o accesos no autorizados.

INTRODUCCIÓN

Que es un NAC y cómo funciona:

Un Sistema de Control de Acceso a la Red (NAC) gestiona y asegura el acceso de dispositivos y usuarios a una red corporativa, tanto cableada como inalámbrica. Su objetivo principal es autenticar usuarios y dispositivos, aplicando políticas de acceso seguro para minimizar riesgos.

Los sistemas NAC funcionan como servidores RADIUS, gestionando las solicitudes de autenticación de dispositivos conectados a switches, puntos de acceso WiFi, routers, entre otros.

Funciones principales de un NAC:

- **Integración con switches y routers** (por ejemplo, Aruba CX).
- **Autenticación de dispositivos** (PCs, laptops, cámaras IP, dispositivos IoT vía autenticación MAC) y usuarios (vía **802.1X**).
- **Aplicación de políticas de acceso** basadas en roles o estados (asignación de VLANs, ACLs).
- **Monitoreo y registro** de accesos a la red.
- **Integración con sistemas de directorio** (Active Directory, usuarios locales).

Tecnologías que utilizadas el NAC:

- **RADIUS**: Gestiona la autenticación entre switches y puntos de acceso.
- **802.1X**: Protocolo de autenticación para redes cableadas e inalámbricas.
- **APIs REST**: Permiten la automatización e integración con sistemas de terceros.

Aplicación de reglas en NAC:

- **Reglas estáticas**: Basadas en listas predefinidas (IP, MAC, usuario).
- **Reglas dinámicas**: Se ajustan en tiempo real según el estado del dispositivo o detección de amenazas.

Limitaciones de los NAC actuales:

Las soluciones actuales como **Cisco ISE, Aruba ClearPass y FortiNAC** dependen de configuraciones manuales y carecen de adaptabilidad automática.

OBJETIVOS

El proyecto tiene como objetivo mejorar la seguridad del acceso en redes corporativas mediante el uso de inteligencia artificial. Las reglas de acceso de los sistemas de Control de Acceso a la Red (NAC) actuales son rígidas y no pueden adaptarse automáticamente a nuevas amenazas y requieren de ajustes manuales. Tiempos de respuesta a incidentes de seguridad lentos, debido a que los cambios en las políticas deben hacerse manualmente. La dificultad en la detección de comportamientos anómalos y amenazas emergentes, en el acceso a la red sin una herramienta que analice patrones en tiempo real.

Los principales problemas que resuelve son:

- Mejorar la seguridad en redes corporativas mediante la integración de sistemas de Control de Acceso a la Red NAC con inteligencia artificial IA.
- Detectar de manera automática la detección de anomalías y amenazas emergentes en tiempo real.
- Realizar la modificación dinámica de políticas de acceso en el NAC basadas en análisis de IA.
- Proporcionar un dashboard para visualizar alertas, rankings de riesgo y métricas.
- Desarrollar una solución compatible con múltiples sistemas NAC.
- Cumplir con normativas de seguridad y protección de datos.

Requisitos generales del cliente

Desde la perspectiva del cliente, la solución debe cumplir con los siguientes requisitos:

- Análisis de datos en tiempo real provenientes de los sistemas NAC.
- Detección de anomalías.
- Modificación dinámica de políticas de acceso basadas en el análisis de la IA.
- Generación de alertas automáticas sobre amenazas detectadas.
- Presenta listados y rankings de riesgo a través de un dashboard que el sistema clasifica y ordena los dispositivos o eventos.

R01 - Autenticar los dispositivos en la red de manera segura

- R01F01 - Integrar el API de ClearPass para autenticación
    - R01F01T01 - Configurar una conexión con la API REST de ClearPass
        - R01F01T01P01 - Ejecutar un script que obtenga un token OAuth2
    - R01F01T02 - Diseñar un endpoint FastAPI para procesar solicitudes
        - R01F01T02P01 - Simular una autenticación desde un dispositivo
- R01F02 - Registrar los dispositivos autenticados
    - R01F02T01 - Crear una tabla "devices" en PostgreSQL
        - R01F02T01P01 - Insertar un registro de prueba
    - R01F02T02 - Implementar una función para actualizar el estado
        - R01F02T02P01 - Simular una desconexión y verificar el estado

R02 – Analizar el tráfico de red en tiempo real

- R02F01 - Recolectar datos del NAC y procesarlos
    - R02F01T01 - Configurar la API de ClearPass para obtener logs
        - R02F01T01P01 - Verificar que los logs se recolecten correctamente
    - R02F01T02 - Implementar un modelo de IA para detectar anomalías
        - R02F01T02P01 - Simular tráfico anómalo y comprobar detección
- R02F02 - Almacenar los resultados del análisis
    - R02F02T01 - Crear una tabla para registrar anomalías
        - R02F02T01P01 - Insertar un registro de anomalía

R03 - Modificar dinámicamente las políticas de acceso

- R03F01 - Usar la API del NAC para aplicar políticas
    - R03F01T01 - Implementar una función para desconectar dispositivos
        - R03F01T01P01 - Simular una anomalía y confirmar desconexión
        - R03F01T02P01 - Enviar un cambio de política y verificar

R04 - Generar alertas y dashboard

- R04F01 - Enviar alertas automáticas
    - R04F01T01 - Desarrollar una función para notificaciones
        - R04F01T01P01 - Simular una amenaza y verificar la alerta

- R04F02 - Mostrar un dashboard
    - R04F02T01 - Diseñar un dashboard para visualizar datos
        - R04F02T01P01 - Confirmar que muestra datos actualizados

DESCRIPCIÓN

ARQUITECTURA DE LA SOLUCIÓN.

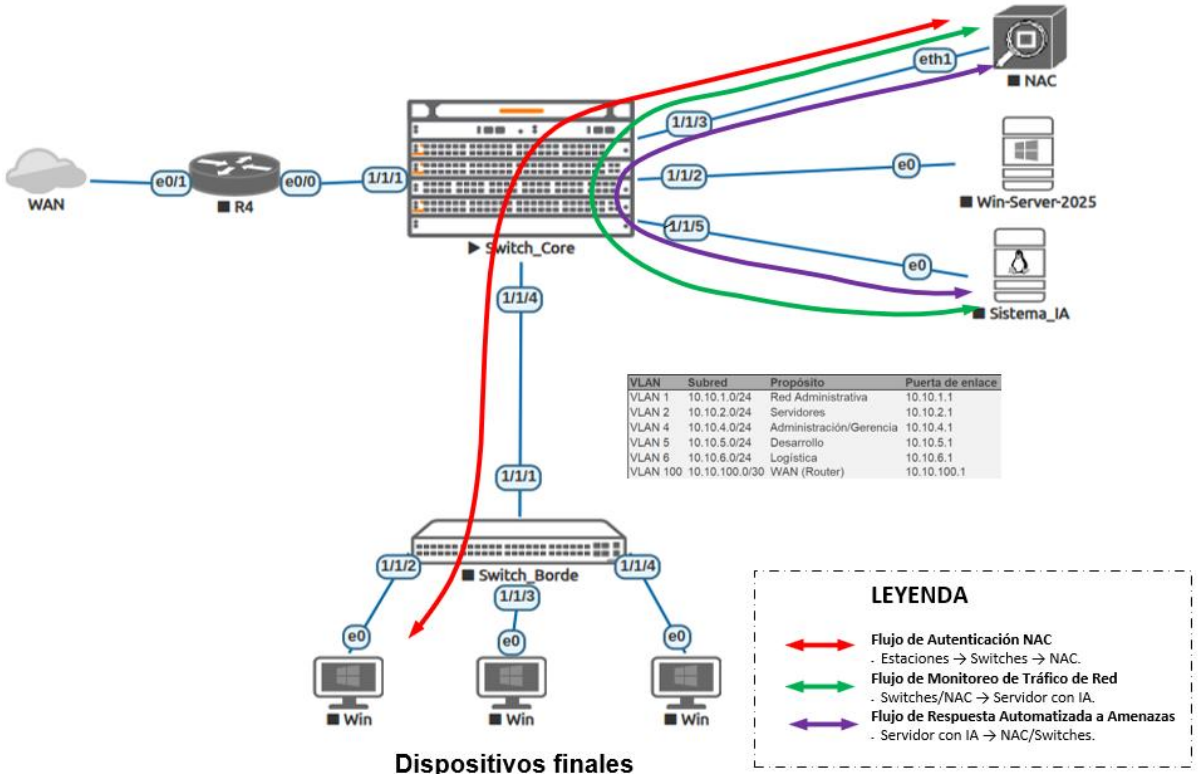


Diagrama de Arquitectura de la Solución:

- **WAN**
  - **Función:** Conectividad a redes externas, como Internet.

- **Router R4 (IP: 10.10.100.2):**
  - **Función:** Enruta el tráfico entre la red local y la WAN, y realiza NAT.

- **Switch Core (IP: 10.10.100.1):**
  - **Función:** Gestiona el tráfico interno de la red, administra las VLANs y enruta el tráfico hacia la WAN.

- **NAC (IP: 10.10.2.100):**
  - **Función:** Gestiona autenticación, políticas NAC, controla el acceso a la red, autentica dispositivos y aplica políticas de seguridad, y envía datos al servidor con IA.

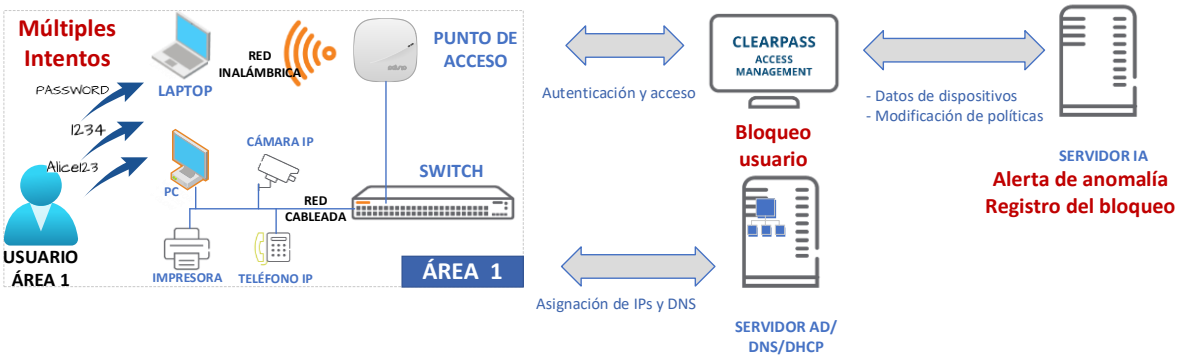
- **Windows Server (IP: 10.10.2.10):**
  - **Función:** Es el servidor DHCP para las VLANs, servidor DNS, servidor AD (Active Directory) y servidor de certificados, políticas de GPO, grupos, usuarios del dominio y se integra con el NAC.

- **Sistema IA** (Ubuntu Server 24.04, IP: 10.10.2.20).
  - **Función:** Aloja la inteligencia artificial (IA), gestiona conexiones con la API de NAC vía API REST, analiza resultados y devuelve respuestas.

- **Switch Borde (IP: 10.10.100.1):**
  - **Función:** Punto de conexión de los dispositivos finales (estaciones de trabajo, dispositivos IoT, cámaras, teléfonos IP, etc.) gestiona el tráfico interno de la red y transporta vlans.

- **Dispositivos finales** (estaciones de trabajo, dispositivos IoT, cámaras, teléfonos IP, etc.)
  - **Función:** Acceder a la red.

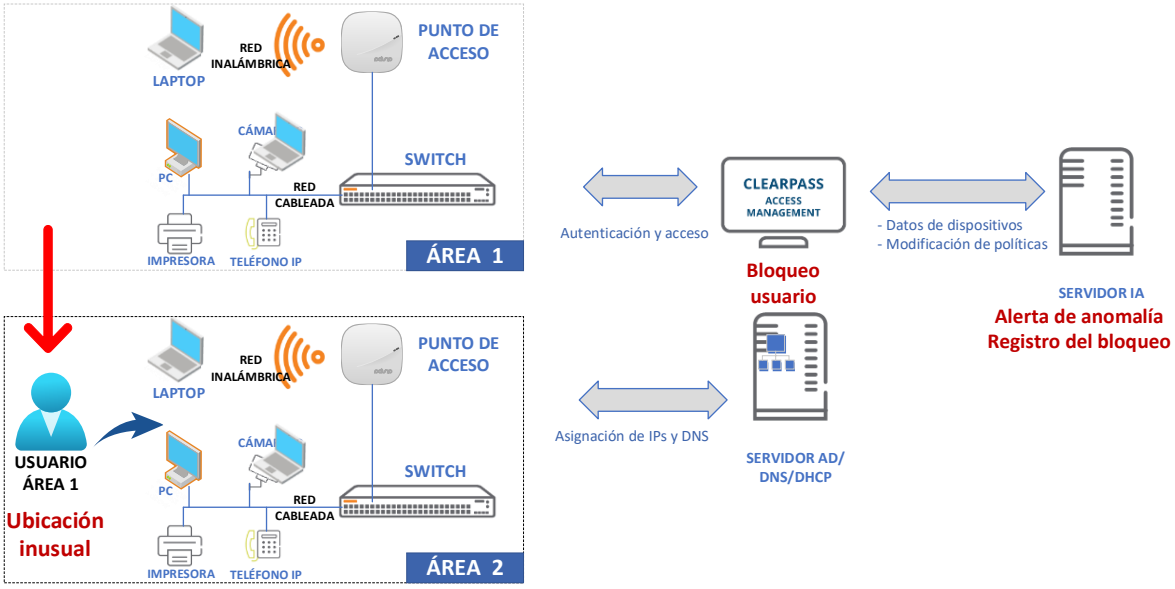
Caso de uso: Intentos de Autenticación repetidos y fallidos



DESCRIPCIÓN: Este caso se muestra múltiples intentos fallidos de autenticación desde un dispositivo o usuario a través de la red cableada o inalámbrica (usando 802.1X o MAC Auth). Esto podría indicar un ataque de fuerza bruta o un intento de intrusión. El servidor con IA analiza los patrones de intentos fallidos y, si se superan umbrales predefinidos, envia una orden al NAC para bloquear el acceso y registra el evento.	
PRECONDICIONES: • El dispositivo/Usuario (PC, Laptop, cámara, teléfono IP, etc.) intenta conectarse a la red. • NAC y Servidor IA están operativos, con el modelo de IA entrenado con datos históricos de autenticaciones. • Los dispositivos de red switch/Access point están configurados para 802.1X y MAC Auth.	**POSTCONDICIONES**: • Si los intentos fallidos se mantienen por debajo del umbral, el sistema permite seguir intentando la autenticación. • Si los intentos fallidos superan el umbral, se bloquea el acceso y registra el evento como anomalía.
DATOS ENTRADA • Credenciales del dispositivo/Usuario	**DATOS SALIDA** • Estado de la autenticación conectado o

<table>
<tr><td>(MAC, usuario de dominio).
• Logs históricos de autenticaciones del dispositivo/Usuario.
• Configuración de política en NAC.
• Configuración de umbrales de cantidad de autenticaciones.</td><td>bloqueado.
• Asignación de VLAN e IP (si es conectado).
• Alerta de anomalía y registro del bloqueo (si es bloqueado).</td></tr>
<tr><td>TABLAS:</td><td>CLASES:</td></tr>
<tr><td colspan="2">INTERFACES:
• Dashboard.html: Muestra estadísticas y alertas de intentos fallidos.</td></tr>
</table>

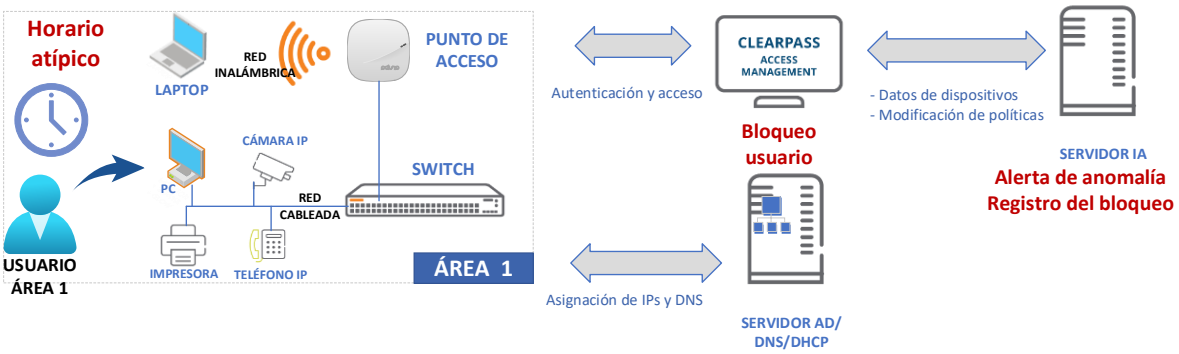
Caso de uso: Ubicación inusual



DESCRIPCIÓN: Este caso se muestra la autenticación de un dispositivo o usuario desde una ubicación diferente a la habitual a través de la red cableada o inalámbrica (usando 802.1X o MAC Auth). Esto podría indicar un acceso no autorizado o un robo de credenciales. El servidor con IA analiza los patrones históricos de ubicación de conexión del dispositivo o usuario y si detecta un acceso en una ubicación no habitual, envía una orden al NAC para bloquear el acceso y registra el evento.	
PRECONDICIONES: • El dispositivo/Usuario (PC, Laptop, cámara, teléfono IP, etc.) intenta autenticarse a la red. • NAC y Servidor IA están operativos, con el modelo de IA entrenado con datos historial de ubicaciones habituales del	**POSTCONDICIONES**: • Si el intento de conexión se realiza desde una ubicación habitual, se permite el acceso. • Si el intento de conexión se realiza desde una ubicación no habitual, se bloquea el acceso y registra el evento

<table>
<tr><td colspan="2">dispositivo/usuario.
• Los dispositivos de red switch/Access point están configurados para 802.1X y MAC Auth.</td><td>como anomalía.</td></tr>
<tr><td colspan="2">DATOS ENTRADA
• Credenciales del dispositivo/Usuario (MAC, usuario de dominio).
• Historial de Switch/Access point a los que el dispositivo/Usuario se ha conectado previamente
• Identificador del Switch/Access point actual que se conecta el dispositivo/Usuario</td><td>DATOS SALIDA
• Estado de la autenticación conectado o bloqueado.
• Asignación de VLAN e IP (si es conectado).
• Alerta de anomalía y registro del bloqueo (si es bloqueado).</td></tr>
<tr><td colspan="2">TABLAS:</td><td>CLASES:</td></tr>
<tr><td colspan="3">INTERFACES:
• Dashboard.html: Muestra alertas de ubicaciones inusuales, incluyendo el nombre o identificador del switch involucrado (ejemplo: "Dispositivo X conectado a Switch-B, inusual").</td></tr>
</table>

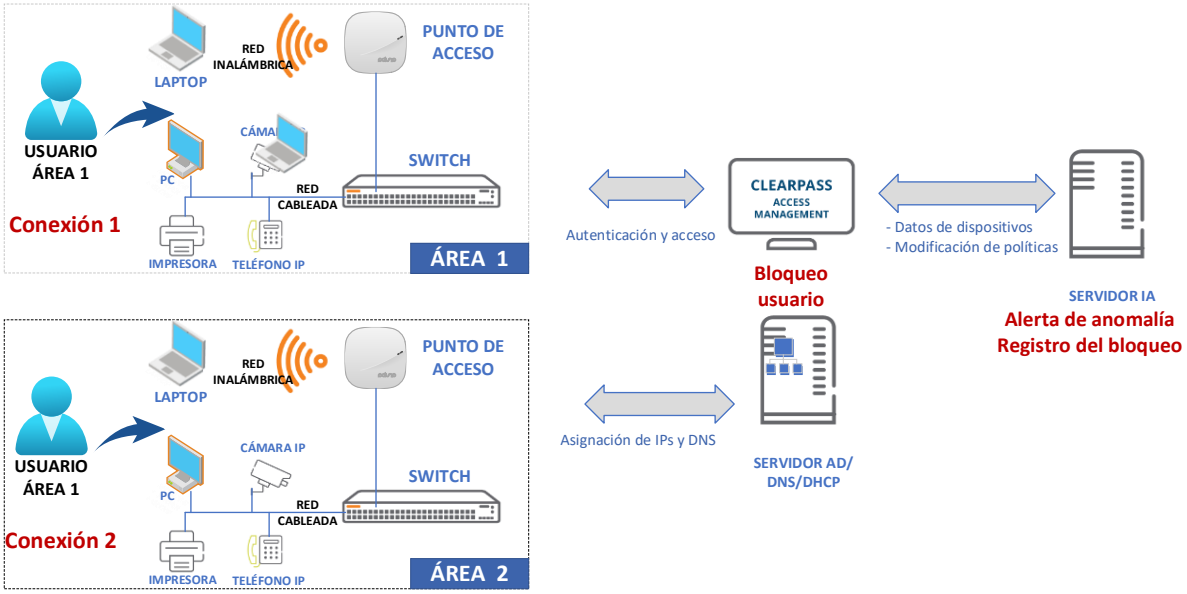
Caso de uso: Horarios atípicos



DESCRIPCIÓN: Este caso se muestra intento de conexión de un dispositivo o usuario realzado fuera de los horarios normales de actividad diferente a la habitual a través de la red cableada o inalámbrica (usando 802.1X o MAC Auth). Esto podría indicar un acceso no autorizado. El servidor con IA analiza los patrones históricos de horarios de conexión del dispositivo o usuario y si detecta un intento de conexión fuera de los horarios habituales, envía una orden al NAC para bloquear el acceso y registra el evento.	
PRECONDICIONES: • El dispositivo/Usuario (PC, Laptop, cámara, teléfono IP, etc.) intenta autenticarse a la red. • NAC y Servidor IA están operativos, con el modelo de IA entrenado con datos historial de horarios habituales de conexión del dispositivo/usuario. • Los dispositivos de red switch/Access point están configurados para 802.1X y	**POSTCONDICIONES**: • Si el intento de conexión se realiza dentro de los horarios habituales, se permite el acceso. • Si el intento de conexión se realiza fuera de los horarios habituales, se bloquea el acceso y registra el evento como anomalía.

<table>
<tr><td>MAC Auth.</td><td></td></tr>
<tr><td>DATOS ENTRADA
Credenciales del dispositivo/Usuario (MAC, usuario de dominio).
Historial de Switch/Access point a los que el dispositivo/Usuario se ha conectado previamente
Identificador del Switch/Access point actual que se conecta el dispositivo/Usuario</td><td>DATOS SALIDA
Estado de la autenticación conectado o bloqueado.
Asignación de VLAN e IP (si es conectado).
Alerta de anomalía y registro del bloqueo (si es bloqueado).</td></tr>
<tr><td>TABLAS:</td><td>CLASES:</td></tr>
<tr><td colspan="2">INTERFACES:
Dashboard.html: Muestra alertas de conexiones en horarios atípicos</td></tr>
</table>

Caso de uso: Conexiones Simultáneas desde múltiples ubicaciones

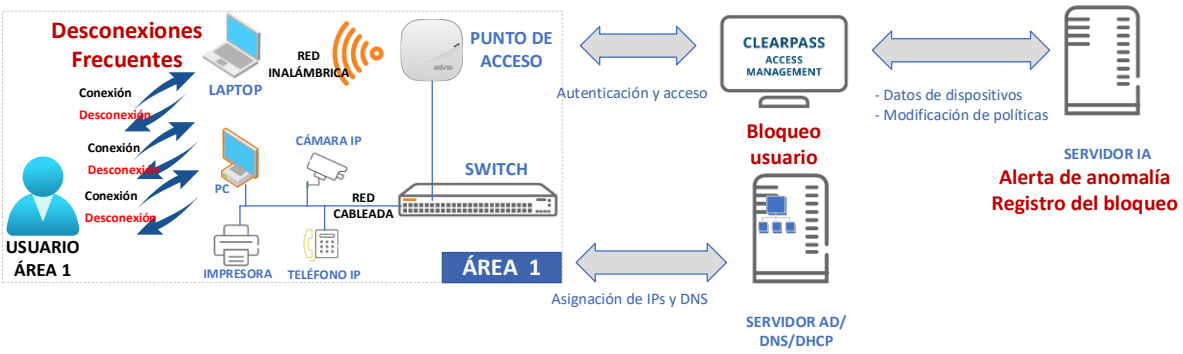


DESCRIPCIÓN: Este caso se muestra intentos de conexión de un dispositivo o usuario realizadas de manera simultánea desde diferentes ubicaciones a través de la red cableada o inalámbrica (usando 802.1X o MAC Auth). Esto podría indicar un acceso no autorizado o un robo de credenciales. El servidor con IA analiza los patrones históricos de ubicación de conexión del dispositivo o usuario y si detecta múltiples accesos desde diferentes ubicacione al mismo tiempo, envía una orden al NAC para bloquear el acceso y registra el evento.

PRECONDICIONES:	**POSTCONDICIONES**:
• El dispositivo/Usuario (PC, Laptop, cámara, teléfono IP, etc.) intenta autenticarse a la red desde 2 o más ubicaciones en un corto intervalo. • NAC y Servidor IA están operativos, con	• Si el intento de conexión se realiza desde solo una ubicación, se permite el acceso. • Si el intento de conexión se realiza desde múltiples ubicaciones, se

<table>
<tr><td>el modelo de IA entrenado con datos historial de Switch/Access point a los que el dispositivo/Usuario se encuentra conectado previamente.
• Identificador del Switch/Access point actual que se conecta el dispositivo/Usuario.</td><td>bloquea el acceso y registra el evento como anomalía.</td></tr>
<tr><td>DATOS ENTRADA
• Credenciales del dispositivo/Usuario (MAC, usuario de dominio).
• Historial de Switch/Access point a los que el dispositivo/Usuario se ha conectado previamente
• Identificador del Switch/Access point actual que se conecta el dispositivo/Usuario</td><td>DATOS SALIDA
• Estado de la autenticación conectado o bloqueado.
• Asignación de VLAN e IP (si es conectado).
• Alerta de anomalía y registro del bloqueo (si es bloqueado).</td></tr>
<tr><td>TABLAS:</td><td>CLASES:</td></tr>
<tr><td colspan="2">INTERFACES:
• Dashboard.html: Visualiza alertas de conexiones simultáneas sospechosas.
• LoginPage.html: Interfaz para la autenticación de usuarios.</td></tr>
</table>

Caso de uso: Desconexiones frecuentes



DESCRIPCIÓN: Este caso se muestra múltiples patrones de conexiones y desconexiones frecuentes de un dispositivo o usuario a través de la red cableada o inalámbrica (usando 802.1X o MAC Auth) en un corto periodo. Esto podría indicar problemas de conectividad o intentos de ataque de malware. El servidor con IA analiza los patrones históricos de frecuencia de conexión del dispositivo o usuario y si detecta una anomalía, envía una orden al NAC para bloquear el acceso y registra el evento.

PRECONDICIONES:	**POSTCONDICIONES**:
• El dispositivo/Usuario (PC, Laptop, cámara, teléfono IP, etc.) está conectado y conectado varias veces en un corto intervalo. • NAC y Servidor IA están operativos, con el modelo de IA entrenado con datos historial de número de conexiones/desconexiones del dispositivo/Usuario.	• Si la frecuencia de intentos de conexión se mantiene por debajo del umbral, el sistema permite seguir intentando la autenticación. • Si la frecuencia de los intentos de conexión supera el umbral, se bloquea el acceso y registra el evento como anomalía.

<table>
<tr><td colspan="2">

- Los dispositivos de red switch/Access point están configurados para 802.1X y MAC Auth.

</td></tr>
<tr><td>

DATOS ENTRADA

- Credenciales del dispositivo/Usuario (MAC, usuario de dominio).
- Historial de comportamiento de conexión del dispositivo/Usuario.
- Logs de conexión/desconexión.

</td><td>

DATOS SALIDA

- Estado de la autenticación conectado o bloqueado.
- Asignación de VLAN e IP (si es conectado).
- Alerta de anomalía y registro del bloqueo (si es bloqueado).

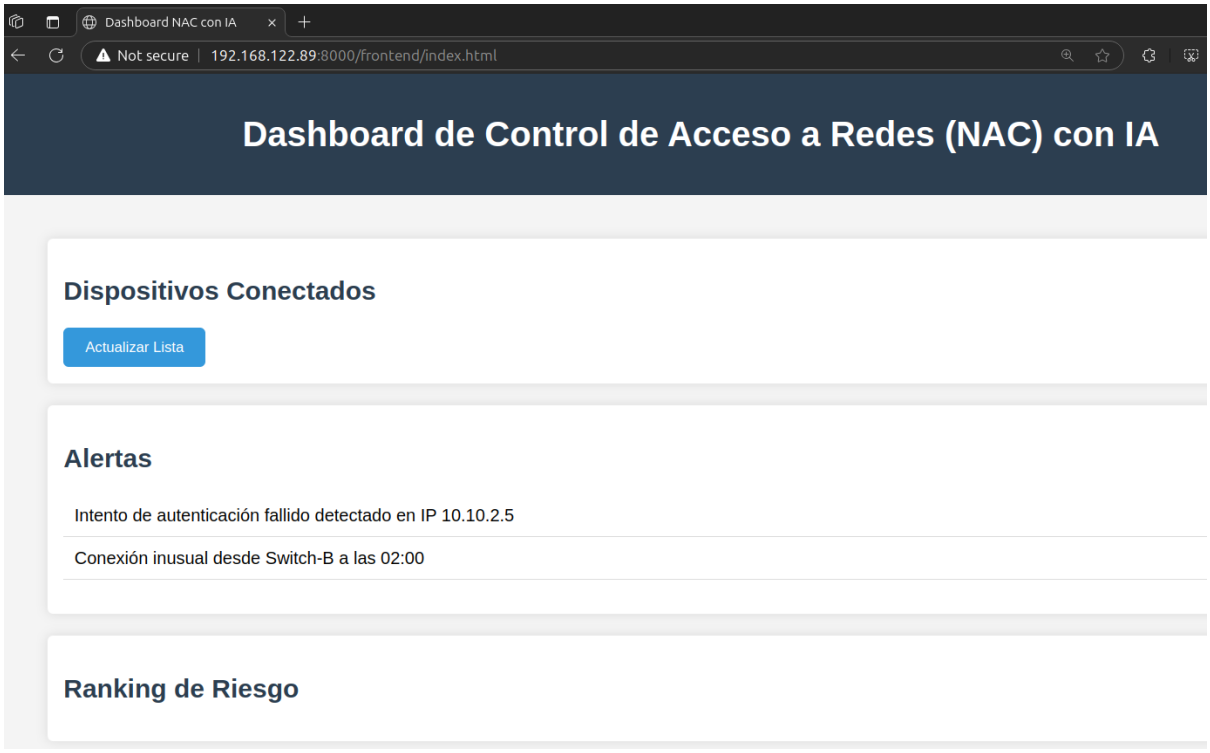
</td></tr>
<tr><td>**TABLAS:**</td><td>**CLASES:**</td></tr>
<tr><td colspan="2">

INTERFACES:

- **Dashboard.html:** Visualiza alertas de desconexiones frecuentes sospechosas.
- **LoginPage.html:** Interfaz para la autenticación de usuarios.

</td></tr>
</table>

DISEÑOS


Dashboard NAC con IA
Not secure | 192.168.122.89:8000/frontend/index.html
Dashboard de Control de Acceso a Redes (NAC) con IA
Dispositivos Conectados
Actualizar Lista
Alertas
Intento de autenticación fallido detectado en IP 10.10.2.5
Conexión inusual desde Switch-B a las 02:00
Ranking de Riesgo

TECNOLOGÍA

Las tecnologías y herramientas utilizadas para este proyecto son las siguientes:

Ubuntu Server 24.04.

Descripción de la herramienta: Sistema operativo basado en Linux, de código abierto, que sirve como plataforma para alojar el backend, base de datos, modelo de IA y frontend.

Aruba ClearPass: Sistema NAC.

Descripción de la herramienta: Sistema de control de acceso a la red (NAC) desarrollado por Aruba Networks, que gestiona la autenticación y las políticas de seguridad para dispositivos y usuarios. Proporciona API REST para la autenticación de dispositivos (mediante 802.1X y MAC Auth), la aplicación de políticas de acceso y la obtención de datos en tiempo real sobre sesiones y endpoints.

PostgreSQL.

Descripción de la herramienta: Sistema de gestión de bases de datos relacional de código abierto, encargado de almacenar los datos de dispositivos y logs.

HTML/CSS/JAVA.

Descripción de la herramienta: Tecnologías para el desarrollo web, utilizamos HTML para la estructura, CSS para los estilos y JavaScript para la funcionalidad. Utilizadas para construir el frontend del sistema, como un dashboard interactivo que muestra listas de dispositivos y alertas.

Visio Profesional 2021.

Descripción de la herramienta: Software de Microsoft para la creación de diagramas profesionales, como arquitecturas, modelos entidad-relación (E/R) y casos de uso.

Creación de diagramas (arquitectura, E/R, casos de uso).

EVE-NG.

Descripción de la herramienta: Plataforma de emulación de redes utilizada para simular entornos de red en laboratorio, utilizada para simular la red (switches, routers, ClearPass) y generar datos de prueba, como tráfico anómalo.

Python 3.12

Descripción de la herramienta: Lenguaje de programación de alto nivel usado para desarrollar el backend con FastAPI, integrar la API de ClearPass.

METODOLOGÍA

Metodología usada y justificación de la misma.

Se presentarán dos planificaciones, una valoración inicial y previa a la implementación del proyecto y otra final con el tiempo real dedicado a cada parte del RFTP. Se analizarán las desviaciones.
El tiempo se expresará en horas. Debe existir una totalización final.

Diagrama de Gantt (Microsoft Project o similar). Real, contrastable con GIT, RFTP y Casos de uso.

ID	Task	Start	Finish	Duration	Progress	Priority	Resources
1	**Analysis**	**2018-10-01 08:00**	**2018-10-10 16:00**	**8 d**	**98.9%**	1	**Rita; William; Tyler; Wenger; Steve**
2	Requirement Meetings	2018-10-01 08:00	2018-10-04 16:00	4 d	100%	1	Rita; William
3	Communication with Stakeholders	2018-10-05 08:00	2018-10-08 16:00	2 d	95.5%	3	Rita; William; Tyler; Wenger; Steve
4	Document Current System	2018-10-09 08:00	2018-10-10 16:00	2 d	100%	3	William
5	Analysis Finished	2018-10-10 08:00	2018-10-10 16:00	1 d	0%	1	
6	**Design**	**2018-10-11 08:00**	**2018-11-05 16:00**	**18 d**	**14.9%**	2	**Steve; Yvette; Zoe**
7	Design Database	2018-10-11 08:00	2018-10-17 16:00	5 d	62.4%	1	Steve
8	Software Design	2018-10-18 08:00	2018-10-25 16:00	6 d	0%	2	Yvette
9	Interface Design	2018-10-26 08:00	2018-10-30 16:00	3 d	0%	4	Zoe
10	Create Design Specifications	2018-10-26 08:00	2018-11-05 16:00	7 d	0%	2	Steve
11	Design Finished	2018-11-05 08:00	2018-11-05 16:00	1 d	0%	2	
12	**Development**	**2018-10-11 08:00**	**2018-11-09 16:00**	**22 d**	**22.5%**	3	**Tyler; Wenger**
13	Develop System Module	2018-10-11 08:00	2018-10-26 16:00	12 d	41.2%	1	Tyler; Wenger
14	Integrate System Module	2018-10-29 08:00	2018-11-06 16:00	7 d	0%	1	Tyler
15	Perform Initial Testing	2018-11-07 08:00	2018-11-09 16:00	3 d	0%	2	Wenger
16	Development Finished	2018-11-09 08:00	2018-11-09 16:00	1 d	0%	3	
17	**Testing**	**2018-10-29 08:00**	**2018-11-20 16:00**	**17 d**	**29.4%**	4	**Vicky; Mike**
18	Perform System Testing	2018-10-29 08:00	2018-11-07 16:00	8 d	62.5%	3	Vicky
19	Document Issues Found	2018-11-08 08:00	2018-11-15 16:00	6 d	0%	4	Mike
20	Correct Issues Found	2018-11-16 08:00	2018-11-20 16:00	3 d	0%	1	Mike
21	Testing Finished	2018-11-20 08:00	2018-11-20 16:00	1 d	0%	3	
22	**Implementation**	**2018-11-20 08:00**	**2018-12-10 16:00**	**15 d**	**0%**	1	**Tyler; Mike**
23	On-Site Installation	2018-11-20 08:00	2018-11-20 16:00	1 d	0%	5	Tyler
24	Support Plan for the System	2018-11-20 08:00	2018-12-10 16:00	15 d	0%	4	Mike
25	**Completion**	**2018-11-21 08:00**	**2018-12-03 16:00**	**9 d**	**0%**	2	**Rita; William**
26	System Maintenance	2018-11-21 08:00	2018-12-03 16:00	9 d	0%	3	Rita
27	Evaluation	2018-11-21 08:00	2018-12-03 16:00	9 d	0%	1	William

Presupuesto. Con detalle de horas, indispensable si se realiza en grupo, y coste total del desarrollo por cada requisito.

README y GIT.

https://github.com/vladimircarpiomorales/TFG-UAX/blob/main/README.md

https://github.com/vladimircarpiomorales/TFG-UAX.git

TRABAJOS FUTUROS

El sistema desarrollado tuvo como marca base a Aruba/HPE mediante su API REST para ampliaciones futuras el sistema se integrará con otras marcas lideres como Cisco y Fortinet y sus soluciones de NAC FortiNAC y Cisco ISE.

CONCLUSIONES

Conclusión profesional del proyecto.

REFERENCIAS

Aplicado para realizar las instalación y configuración de EVE-NG

https://www.eve-ng.net/index.php/documentation/

Aplicado para la instalación del NAC (Clearpass)

https://arubanetworking.hpe.com/techdocs/ClearPass/6.12/Installation-Guide/Default.htm

Aplicado para la configuración de las políticas del NAC (Clearpass)

https://arubanetworking.hpe.com/techdocs/ClearPass/6.12/PolicyManager/Content/home.htm

Aplicado para la configuración de API de NAC (Clearpass)

https://developer.arubanetworks.com/aruba-cppm/docs/introduction-and-overview

Documentación de descarga e instalación oficial de Python Official

https://docs.python.org/3.14/download.html