

Plataformas de control de acceso a redes WLAN. Tendencias, aplicaciones y nuevas tecnologías

Access control platform for WLAN networks. Trends, applications and new technologies

Ing. Reinier Consuegra Peniche¹

Recibido: 06/2019 | Aceptado: 10/2019

Palabras clave

WLAN
Infraestructura
Herramientas de
Control de acceso

Resumen

En este artículo se caracteriza un grupo de herramientas de control de acceso a redes WLAN —*Wireless Local Area Network*—. Además, se ratifica lo brutal que es el bloqueo económico impuesto a Cuba, por el gobierno de Estados Unidos y su impacto en las ramas tecnológicas. Este trabajo pretende promover el desarrollo propio dentro del país de este tipo de soluciones e infraestructura tecnológica existentes. Para el desarrollo del mismo fue utilizado el método de investigación descriptivo basando los resultados en la caracterización de las distintas tecnologías, que se expone en el contenido del presente.

Keywords

WLAN
Infrastructure
Control Access Tools

Abstract

This article features a group of access control tools for WLAN —*Wireless Local Area Network*— networks. In addition, the brutality of the economic blockade imposed on Cuba by the United States government and its impact on the technological branches is ratified. This work aims to promote the development of this type of existing technological infrastructure and solutions within the country. For its development, the descriptive research method was used, basing the results on the characterization of the different technologies that is stated in the content of the present.

Introducción

Con el crecimiento de los servicios WLAN en Cuba y en particular el servicio WLAN público de ETECSA, se ha hecho necesario acondicionar la infraestructura que soporta el mismo, con el objetivo de garantizar una mejor calidad y seguridad. Este servicio está siendo víctima de disímiles ataques, suplantación de identidades y virus, entre otros fenómenos; que están afectando la integridad del mismo. El presente trabajo se basa en

el estudio de nuevas tendencias, aplicaciones y nuevas tecnologías para estos fines a nivel mundial.

Por motivos relacionados con el bloqueo económico impuesto brutalmente a Cuba por el Gobierno de los Estados Unidos de América, la adquisición de soluciones de seguridad es compleja para el país. Es por ello que se ha hecho necesario apostar por soluciones de software libre y desarrollo propio con niveles de perso-

nalización acordes a las necesidades y requerimientos dispuestos.

Materiales y métodos

La metodología aplicada para el desarrollo de este trabajo fue fundamentalmente la revisión y análisis de artículos y publicaciones corporativas de distintos proveedores de equipamientos y tecnologías, como Huawei, Cisco, HP entre otros. Estos aplicados con el objetivo de analizar informaciones existentes, así como el análisis de la realidad donde se propone desarrollar la solución.

Resultados y discusión

El presente trabajo expone algunas de las plataformas implementadas en la actualidad para el control de acceso a las redes WLAN. Esto con el objetivo de proponer algunas ideas para posibles despliegues de soluciones de redes inalámbricas. Como parte del desarrollo y crecimiento de las redes de telecomunicaciones a nivel mundial, la exposición e intentos de vulneración a las mismas ha crecido, así como los intentos de clientes de burlar cobros y pagos en los servicios de este tipo brindados por los diferentes proveedores alrededor del mundo. Por esto y otros motivos los distintos proveedores de servicios de internet a través de redes inalámbricas se han dado a la tarea de buscar alternativas para elevar la seguridad y calidad de este tipo de servicios.

Entre los principales proveedores de soluciones de seguridad para redes inalámbricas se encuentra la empresa CISCO, Palo Alto, Juniper entre otras. A continuación, se presenta un resumen de algunas de las soluciones para el control de acceso a redes WLAN.

Impulse SafeConnect

Producto desarrollado por Impulse, empresa emplazada en Estados Unidos. En sus inicios la compañía comenzó en la educación y se ha expandido a los mercados gubernamentales y corporativos. El producto Impulse SafeConnect presenta las siguientes características: soporta la supervisión de 250 a 25 000 terminales con capacidad de conexión en la red. La plataforma está diseñada en una arquitectura escalable lo que posibilita su fácil despliegue operacional. Esta herramienta se centra en lograr control, crear marcos de responsabilidad y mitigar vulnerabilidades en las redes en las que despliega (Impulse, 2019).

ExtremeControl

Producto desarrollado por la empresa Extreme TM, fundada en 1996 y radicada en Estados Unidos. El producto permite aplicar controles granulares sobre quién, qué, cuándo, dónde y cómo se comportan los dispositivos en la red. Puede habilitar BYOD —*Bring Your Own Device*—, acceso de invitados e IoT —*Internet of Things*—, seguros mediante la implementación de políticas en tiempo real, basadas en la postura de seguridad de los dispositivos. ExtremeControl hace coincidir los dispositivos en la red con atributos, como usuario, tiempo, ubicación, vulnerabilidad o tipo de acceso, para crear una identidad contextual que lo abarque todo. Las identidades basadas en roles siguen a un usuario, sin importar desde dónde o cómo se conecta a la red. Se pueden utilizar para aplicar políticas de acceso altamente seguras. Además, permite la supervisión de hasta 200 000 dispositivos conectados a la red y ofrece una arquitectura basada en reglas para automatizar el acceso según los casos de uso (Extreme TM, 2019). (Figura 1)

Auconet BICS

El producto Auconet BICS —*Business Infrastructure Control Solution*— está desarrollado por la empresa Auconet fundada en 1998 por un ingeniero alemán. Esta radica en San Francisco, Estados Unidos. La plataforma propone un sistema NAC —*Network Access Control*— robusto. A diferencia de la mayoría de los proveedores de NAC, BICS puede combinar la autenticación basada en MAC y 802.1X, para una protección más segura orientada para cada tipo de dispositivo. BICS proporciona capacidades para autorizar a los usuarios, dispositivos y puertos, por separado o en cualquier combinación, o bloquea cualquiera de ellos, de acuerdo con las políticas que se predefinan en el sistema, proporcionando así un mayor grado de seguridad. Propone una implementación a gran escala de hasta 1 000 000 de dispositivos identificados en la red, soportada en entornos virtualizados (Auconet, s.f.).

ForeScout CounterACT

El producto ForeScout CounterACT está desarrollado por la empresa ForeScout radicada en San José, California, Estados Unidos. Es una plataforma orientada a entornos regulados como defensa, finanzas, atención médica y ventas. Además, tiene la capacidad de monitoreo sobre más de un 1 000 000 de distintos tipos

¹ Empresa de Telecomunicaciones de Cuba S.A. Dirección de Operaciones de Seguridad, La Habana, Cuba. reinier.consuegra@etecsa.cu

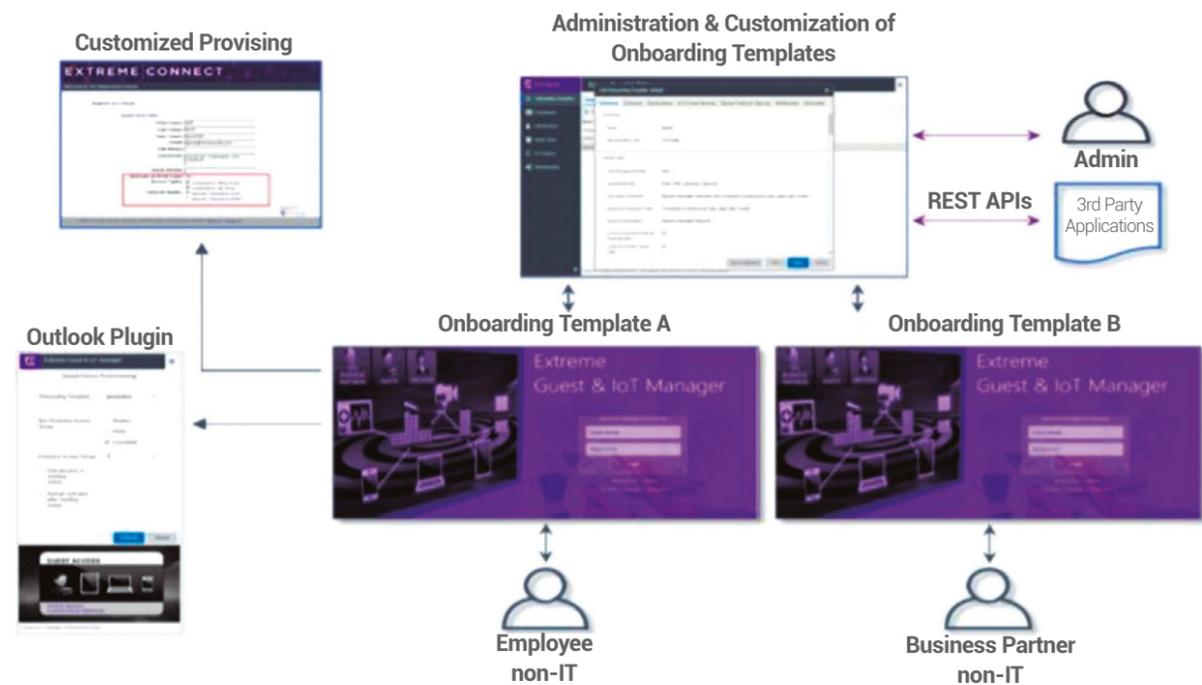


Figura 1. Esquema funcional de ExtremeControl

de dispositivos de red. Es una plataforma que propone una arquitectura escalable vertical y horizontalmente. También propone solución en la nube de internet y está consagrada como una de las principales soluciones de este tipo a nivel mundial (Forescout, s.f.). (Figura 2)

HPE Aruba ClearPass

El producto HPE Aruba ClearPass es un producto desarrollado por empresa holandesa Wentzo Wireless. Es una plataforma que está adecuada fundamentalmente a entornos alto volumen de autenticación, ya que soporta más de 10 millones de autenticaciones por día. Además, se ajusta especialmente a entornos

distribuidos geográficamente distantes. Está basada en una arquitectura escalable y de rápido despliegue. También responde a los estándares de las tecnologías BYOD (Wentzo Wireless, s.f.). (Figura 3)

Cisco Identity Services Engine

La plataforma Cisco Identity Services Engine es un producto desarrollado por la empresa Cisco radicada en Estados Unidos. Cisco ISE como también se le conoce está entre los líderes de este tipo de herramientas a nivel mundial. Entre las características que más se destacan se tiene que admite hasta 500 000 sesiones concurrentes y soporta hasta 1 500 000 de dispositivos por cada im-

EMPLOYEES, GUESTS, CONTRACTORS

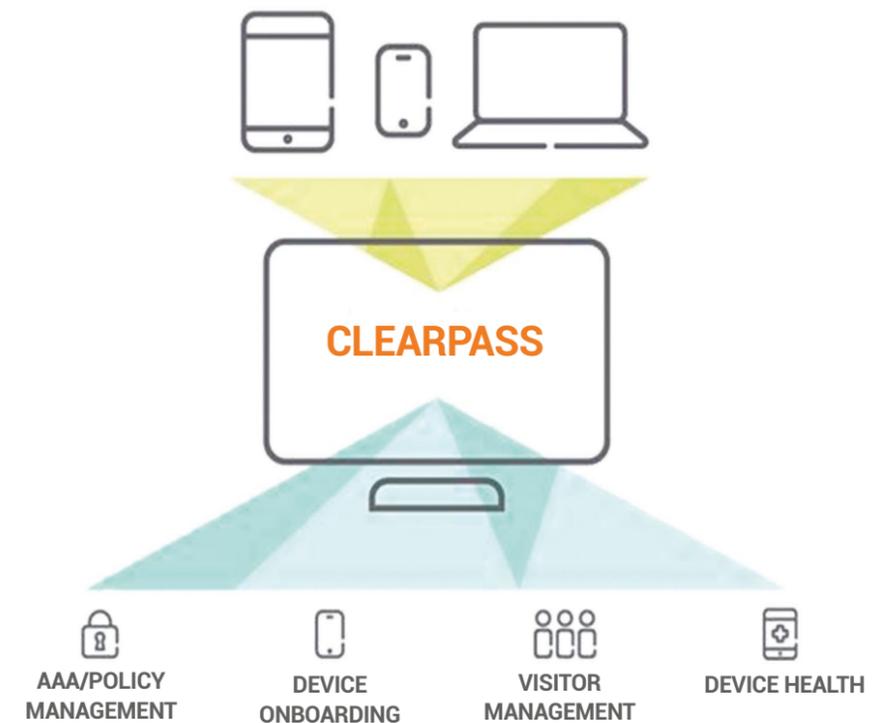


Figura 3. Aruba ClearPass

plementación. Ofrece motores de inteligencia adaptativa, detección y respuesta automatizada y aprendizaje automático. Además, posee una arquitectura de despliegue y escalabilidad tanto horizontal como vertical (Cisco, s.f.).

OpenNAC

OpenNAC es una plataforma de control de acceso a la red de código abierto para entornos LAN / WAN corporativos. Permite la autenticación, la autorización y la auditoría basada en todos los accesos a la red. Es compatible con diferentes proveedores de redes como Cisco, Alcatel, 3Com o Extreme Networks, y diferentes clientes como PC con Windows o Linux, Mac, dispositivos como teléfonos inteligentes y tabletas. Basado en componentes de código abierto y auto-desarrollo. Está basado en estándares de la industria como FreeRadius, 802.1x, AD, ldap. Es muy extensible, pueden incorporarse nuevas características por-

que está diseñado en los complementos. Se integra fácilmente con los sistemas existentes. Por último, pero no menos importante, proporciona servicios de valor agregado tales como administración de configuración, red, configuraciones de respaldo, descubrimiento de red y monitoreo de red (Opennac, s.f.).

Conclusiones

El presente trabajo realizó una caracterización de un grupo de herramientas y plataformas que existen en el mercado de los sistemas de control de acceso para las redes WLAN. También reafirma la complejidad para Cuba de adquirir este tipo de plataformas por los temas relacionados con el brutal bloqueo económico impuesto a Cuba por el gobierno de Estados Unidos de América. Además, reafirma el llamado de estos tiempos a seguir abogando por la soberanía tecnológica que debe tener Cuba en el entorno tecnológico.

Device Visibility Across the Extended Enterprise



Figura 2. Alcance operacional plataforma ForeScout CounterACT

Referencias

- Auconet. (s.f.). *Solutions bics for security*. Obtenido de Auconet.com: <https://auconet.com/solutions/bics-for-security>
- Cisco. (s.f.). *Cisco Identity Services Engine*. Obtenido de Cisco: <https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html>
- Extreme TM. (2019). *ExtremeControl*. Obtenido de Extreme Networks: <https://extremenetworks.com>
- Forescout. (s.f.). *Plataform Counteract*. Obtenido de Forescout : <https://www.forescout.com/platform/counteract/>
- Impulse. (2019). *Safe Connect*. Obtenido de Impulse: <https://impulse.com/>
- Opennac. (s.f.). *Open Source Nac Solution*. Obtenido de Opennac: <http://www.opennac.org/opennac/en.html>
- Wentzo Wireless. (s.f.). *Aruba ClaerPass*. Obtenido de Clearpass: <https://www.clearpass.net/>

INVESTIGACIÓN

Proyecto de Telemedicina para el Cardiocentro de Villa Clara

Telemedicine project for the Cardiocenter of Villa Clara

MSc. Arelys Emiliana Ramos Fleites^{1*}, Ing. Lidisvey Herrero González², Dr.Sc. Félix Álvarez Paliza³

Recibido: 06/2019 | Aceptado: 10/2019

Palabras clave

Telemedicina
PACs
DICOM
Modelación
Simulación de redes

Resumen

La telemedicina abarca varias líneas de investigación siendo el telediagnóstico y la teleimagenología de los temas que se les ha prestado especial importancia en la actualidad. En Cuba, esta es un área que se le ha dedicado mucha atención y es el Cardiocentro de Villa Clara uno de los centros médicos más beneficiados con estos avances. Actualmente, el centro quirúrgico cuenta con una red de alcance nacional, con modernos medios de diagnóstico y terapéuticos y con un personal médico de alta calificación profesional. La presente investigación se centra en evaluar si la actual red del Cardiocentro puede soportar los nuevos servicios de transmisión, recepción y procesamiento de las imágenes que se generan en el tomógrafo computarizado, el angiógrafo y el ecocardiógrafo entre otros equipos usando herramientas de simulación de redes que permiten evaluar el desempeño de la red.

Keywords

Telemedicine
PACs
DICOM
Modeling
Network simulation

Abstract

Telemedicine encompasses several lines of research, with telediagnosis and the imaging of topics that have been particularly important today. In Cuba this is an area in which special attention has been dedicated and it is the Cardiocentro of Villa Clara from the medical centers that benefit most from these advances. Currently, the surgical center has a network of national scope, with modern diagnostic and therapeutic means and with highly qualified medical personnel. This research focuses on evaluating whether the current Cardiocentro network can support the new transmission, reception and processing services of the images generated in the computerized tomograph, the angiograph and the echocardiograph among others using network simulation tools that allow evaluate network performance.

^{1*}Universidad Central "Marta Abreu" de las Villas. Villa Clara, Cuba. arelys@uclv.edu.cu

²Hospital Cardiocentro Villa Clara. Villa Clara, Cuba. lidisvey@infomed.sld.cu

³Universidad Central "Marta Abreu" de las Villas. Villa Clara, Cuba. fapaliza@uclv.edu.cu.