Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

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

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

Reinier Consuegra Peniche

ETECSA, Dirección de Operaciones de Seguridad. 10200. reinier.consuegra@etecsa.cu

Resumen: Con el crecimiento de los servicios WLAN en nuestro país 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. También este servicio está siendo víctima de disimiles ataques, suplantación de identidades y virus, entre otros fenómenos; que están afectando la integridad del mismo. En este documento se caracterizan un grupo de herramientas de control de acceso a redes WLAN. Además, se ratifica lo brutal que es el bloqueo económico que tiene nuestro país impuesto por el gobierno de Estados Unidos y su impacto en las ramas tecnológicas. Este trabajo pretende además buscar incentivar que sigamos promoviendo el desarrollo propio dentro del país de este tipo de soluciones.

Palabras clave: WLAN, Infraestructura, Estrategia, Plataformas TI

Abstract: *With the growth of WLAN services in our country and in particular the public WLAN service of ETECSA, it has become necessary to prepare the infrastructure that supports it, with the aim of guaranteeing better quality and safety. This service is also being the victim of dissimilar attacks, identity theft and viruses, among other phenomena; that are affecting its integrity. This document characterizes a group of access control tools for WLAN networks. In addition, the brutality of the economic blockade that our country has imposed by the United States government and its impact on the technological branches is ratified. This work also seeks to encourage us to continue promoting our own development within the country of this type of solutions.*

Keywords: *WLAN, Infrastructure, Strategy, IT Platforms*

Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

Introducción

Con el crecimiento de los servicios WLAN en nuestro país 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 disimiles 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 complejo para el país. Es por ello que se ha hecho necesario apostar por soluciones de software libre y desarrollo propio con niveles de personalización acordes a las necesidades y requerimientos dispuestos.

Materiales y métodos

La metodología aplicada para el desarrollo del trabajo fue fundamentalmente la realización de estudios basados en métodos de investigación teóricos y empíricos. 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 una algunas ideas de solución 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

Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

través de redes inalámbricas se han dado a la tarea de buscar alternativas para elevar las 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, les presentamos un resumen de alguna de las soluciones para el control de acceso a redes WLAN.

Impulse SafeConnect

Producto desarrollado por la empresa 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 tiene como 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.

Sitio web: https://impulse.com/

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, acceso de invitados e IoT 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 conecte 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 frece una arquitectura basada en reglas para automatizar el acceso según los casos de uso.

Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

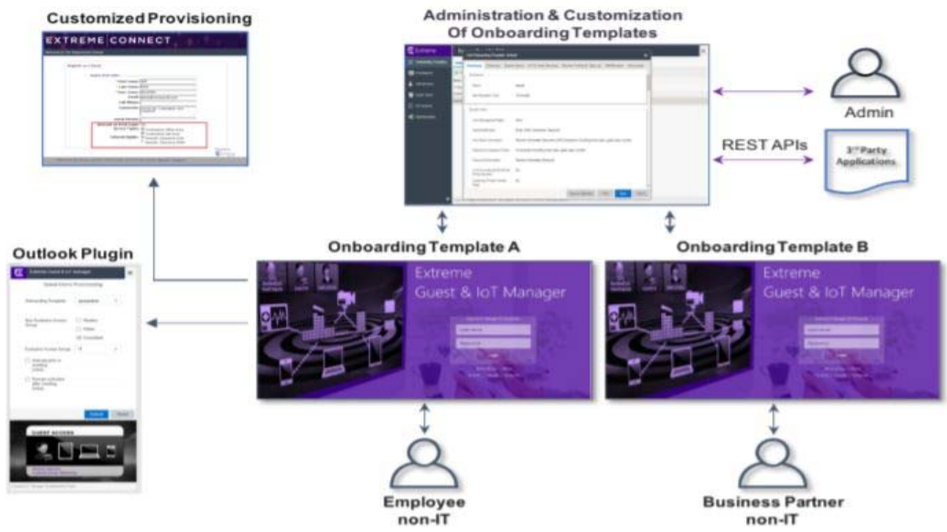

Fig. 1 Esquema funcional de ExtremeControl

Sitio web: https://www.extremenetworks.com

Auconet BICS

El producto Auconet BICS está desarrollado por la empresa Auconet fundada en 1998 por un ingeniero alemán, esta radicada en San Francisco, Estados Unidos. La plataforma propone un sistema NAC 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.

Sitio web: https://auconet.com/solutions/bics-for-security/

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,

Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

tiene la capacidad de monitoreo sobre más de un 1 000 000 de distintos tipos 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.

Fig. 2 Alcance operacional plataforma ForeScout CounterACT

Sitio web: https://www.forescout.com/platform/counteract/

HPE Aruba ClearPass

El producto HPE Aruba ClearPass es un producto desarrollado por empresa holandesa Wentzo Wireless. Es una plataforma que esta 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. Esta basada en una arquitectura escalable y de rápido despliegue. También responde a los estándares de las tecnologías BYOD.

Fig. 3 Aruba ClearPass

Sitio web: https://www.clearpass.net/

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

Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

esta entre los líderes de este tipo de herramientas a nivel mundial. Entre las características que más se destacan esta que admite hasta 500 000 sesiones concurrentes y soporta hasta 1 500 000 de dispositivos por cada implementación. Ofrece motores de inteligencia adaptativa, detección y respuesta automatizadas y aprendizaje automático. Además, posee una arquitectura de despliegue y escalabilidad tanto horizontal como vertical.

Sitio web: https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

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 autodesarrollo. Está basado en estándares de la industria como FreeRadius, 802.1x, AD, ldap, ... Es muy extensible, se pueden incorporar nuevas características porque 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.

Sitio web: http://www.opennac.org/opennac/en.html

Conclusiones

El presente trabajo realiza 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 nuestro país 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 nuestro país en el entorno tecnológico.

Vol. 1, No. 2, Año 2019.
ISSN-e: 1813-5056
|RNPS-e: 0514

Bibliografía

Páginas Web:

https://www.auconet.com/solutions/bics-for-security/

https://www.cisco.com/

https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

https://www.clearpass.net/

https://www.extremenetworks.com

https://www.forescout.com/platform/counteract/

https://www.ieee.org/

https://www.impulse.com/

https://www.itu.int/