PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS
II CONVENCIÓN CIENTÍFICA INTERNACIONAL
"II CCI UCLV 2019"

DEL 23 AL 30 DE JUNIO DEL 2019.
CAYOS DE VILLA CLARA. CUBA.

XVIII Simposio Internacional de Ingeniería Eléctrica. "SIE 2019"

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 Peniche

1-Reinier Consuegra Peniche. ETECSA, Cuba. E-mail: 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. Actualmente las condiciones que soportan este servicio desde el punto de vista de la seguridad no son las más óptimas. También 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 proponer una nueva estrategia tecnológica para mejorar la calidad y seguridad del servicio WLAN público de ETECSA, basado fundamentalmente en las nuevas tendencias, aplicaciones y nuevas tecnologías para estos fines a nivel mundial. En este documento se realiza una descripción de las problemáticas existente en el servicio WLAN público de ETECSA, desde el punto de vista de la seguridad. Además, se caracteriza una propuesta de solución para mejorar la seguridad del mismo basado en un conjunto de plataformas TI. Como conclusiones del trabajo se realiza una representación del estado actual y una solución hacia donde se deberían apostar los esfuerzos para garantizar una mejor seguridad del servicio WLAN público de ETECSA.

Información de contacto
convencionuclv@uclv.cu
www.uclv.edu.cu

Asbtract:

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, in order to guarantee a better quality and security. Currently the conditions that support this service from the point of view of security are not the most optimal. This service is also the victim of dissimilar attacks, identity theft and viruses, among other phenomena; that are affecting the integrity of it. The present work is based on proposing a new technological strategy to improve the quality and security of ETECSA's public WLAN service, based fundamentally on new trends, applications and new technologies for these purposes worldwide. In this document a description of the existing problems in the public WLAN service of ETECSA is made, from the point of view of security. In addition, a solution proposal is characterized to improve its security based on a set of IT platforms. As conclusions of the work is made a representation of the current state and a solution where you should bet the efforts to ensure a better security of the public WLAN service of ETECSA.

Palabras Claves: WLAN, Infraestructura, Estrategia, Plataformas TI

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

1. 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. Actualmente las condiciones que soportan este servicio desde el punto de vista de la seguridad no son las más óptimas. También 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 proponer una nueva estrategia tecnológica para mejorar la calidad y seguridad del servicio WLAN público de ETECSA,

basado fundamentalmente en las 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 ETECSA y en general para el país. Es por ello que se ha hecho necesario apostar por soluciones de software libre con niveles de personalización acordes a las necesidades y requerimientos dispuestos, para los servicios provistos por ETECSA.

En tal sentido ETECSA cuenta en estos momentos varios elementos que proveen una solución tecnológica para mitigar y minimizar los impactos, desde el punto de vista de la seguridad, en el servicio WLAN público. Estas plataformas tecnológicas se están viendo limitadas actualmente por el crecimiento constante del servicio antes mencionadas debido a que se están reflejando algunos comportamientos anómalos, virus informáticos y tendencias al comprometimiento de los elementos de acceso, poniendo en peligro la infraestructura de acceso, la calidad del servicio y experiencia de usuario.

El presente trabajo se basa en proponer una nueva estrategia tecnológica para mejorar la calidad y seguridad del servicio WLAN público de ETECSA, basado fundamentalmente en las nuevas tendencias, aplicaciones y nuevas tecnologías para estos fines a nivel mundial.

2. Metodología

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.

3. 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 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.

3.1. 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/

3.2. 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.

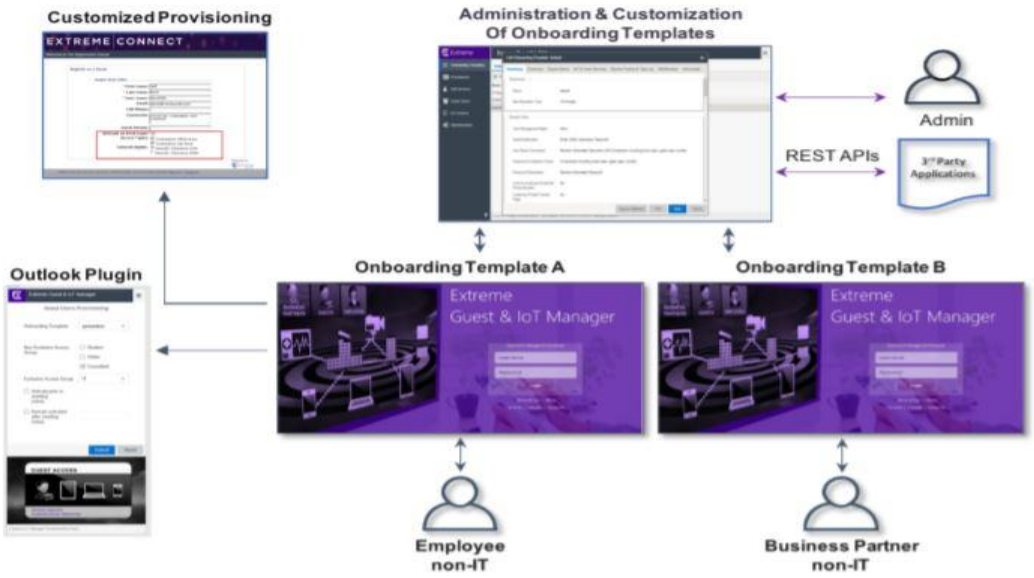

Fig. 1 *Esquema funcional de ExtremeControl*

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

3.3. 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/

3.4. ForeScout CounterACT

El producto ForeScout CounterACT esta 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 mas 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/

3.5. 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/

3.6. 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 esta entre los líderes de este tipo de herramientas a nivel mundial. Entre las características que mas 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

Vendor	Use Cases	Metrics	Intelligence	Delivery	Pricing
Impulse	Education, government, enterprise	500 to 50,000 users, no network performance hit	Automatic detecion, fingerprints new devices	Virtual or physical appliances support 25,000 endpoints and can scale	Starts at $7,000 for 250 concurrent devices
Extreme Networks	Education, entertainment, hospitality, healthcare	Can scale up to 200,000 endpoints	Rules-based architecture and automation	Physical or virtual appliance	Per-user pricing model
Auconet	Large companies and complex implementations	100% device discovery; largest implementation 500,000+ ports	Also offers network monitoring and asset management	Physical or virtual appliance or cloud	Varies by architecture and range of functions
ForeScout	Government/defense, financial services, healthcare, retail	1 million+ port implementations; can protect medical devices	Automated segmentation and enforcement	Physical or virtual appliances with failover option	Starts at $3,701 for virtual and $4,995 for physical appliance
HPE Aruba	Education, finance, healthcare, retail, distributed environments	10 million+ authentications per day	Shares information with third-party and UEBA products	Physical or virtual appliance	Costs vary with size
Cisco Systems	Government and regulated industries	500,000 concurrent sessions and 1.5 million endpoints per deployment	Adaptive intelligence, machine learning, automated response	Physical or virtual appliance	Based on subscription term and number of points protected

Fig. 4 *Características de las plataformas NAC*

3.7. Solución NAC ETECSA

La empresa ETECSA posee una infraestructura de red de distintos proveedores o fabricantes de tecnología. En la red WLAN pública de esta empresa el proveedor predominante es Huawei por lo que la solución NAC que tiene implementada, en su mayoría, es del fabricante antes mencionado. Esta solución está parcialmente cubierta según las buenas prácticas y estándares internacionales. Además, combina soluciones de software libre con un dimensionamiento bastante limitado para el constante crecimiento y demanda de este servicio. También no hay implementada soluciones como BYOD, lo que hace que la red se vea expuesta constantemente a distintos eventos que ponen en riesgo la calidad e integridad del servicio.

3.8 Propuesta de solución NAC para ETECSA

Por los estudios realizados y los elementos desarrollados en el presente trabajo, la propuesta de solución NAC para el servicio WLAN publico brindado por ETECSA es seguir potenciando el desarrollo de la existen. Incorporando a la misma a través de productos y plataformas compatibles soluciones de la filosofía BYOD. También incorporar a la solución NAC un sistema de detección y supresión de malwares.

4. Conclusiones

El presente trabajo realiza un resumen de alguno de los productos y plataformas NAC que hoy existen en el mercado. Además, se hace un breve resumen de la solución NAC implementada en ETECSA. También se realiza la propuesta como solución NAC de ETECSA potenciar la solución existente, incorporando elementos de objeto específicos en los campos de detección de malwares, implementación de soluciones BYOD y otros elementos que fortalezcan la seguridad del servicio WLAN público de ETECSA.

5. Referencias bibliográficas

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/