Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Enfoques Modernos Para la Seguridad de Acceso a Redes

Documento recuperado de:

(CISA) - Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos.
(FBI) - Oficina Federal de Investigación de los Estados Unidos.
(GCSB) - Oficina de Seguridad de Comunicaciones del Gobierno de Nueva Zelanda.
(CERT-NZ) - Equipo de Respuesta a Emergencias Informáticas de Nueva Zelanda.
(CCCS) - Centro Canadiense de Ciberseguridad.

VIEM Vicerrectoría de Innovación y Emprendimiento
ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería
Semillero de Investigación Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veinticuatro
Junio de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Líder
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Ing. Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad – UNAD
Líder Esp. Seguridad Informática - UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Licencia Atribución – Compartir igual

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 24

Junio 2023

Enfoques Modernos Para la Seguridad de Acceso a Redes

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Libardo Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0009-0002-6133-5157

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

[1]El documento **"MODERN APPROACHES TO NETWORK ACCESS SECURITY"** aborda enfoques modernos para la seguridad del acceso a redes, destacando las limitaciones y riesgos asociados con las soluciones tradicionales de VPN, como vulnerabilidades y configuraciones incorrectas que pueden resultar en brechas de seguridad significativas. Este, propone la adopción de marcos de seguridad contemporáneos, como Zero Trust, Secure Access Service Edge (SASE) y Security Service Edge (SSE), que permiten un control de acceso más granular y una monitorización continua. Así mismo presenta mejores prácticas para optimizar la ciberseguridad en las organizaciones, incluyendo la gestión centralizada, la segmentación de redes, la automatización de la seguridad y la formación de usuarios.

Ilustración 1 generada por ChatGPT

La publicación sirve como una guía para que las organizaciones fortalezcan su seguridad en un entorno cada vez más centrado en la nube.

El presente tiene como propósito orientar a las organizaciones respecto a la adopción de soluciones modernas para proteger sus entornos digitales, en línea con las recomendaciones presentadas en el documento **"MODERN APPROACHES TO NETWORK ACCESS SECURITY"**, abordando cómo dichas estrategias pueden ser implementadas para mejorar la seguridad en la infraestructura de red.

[1] https://www.ic3.gov/Media/News/2024/240618.pdf

Desarrollo

El impacto de las vulnerabilidades en sistemas de acceso remoto y VPN puede ser devastador para las organizaciones. Cuando un ciberdelincuente o adversario explota este tipo de vulnerabilidades pueden obtener acceso no autorizado a las redes de datos, lo que les permite realizar movimientos laterales[2] y acceder a datos sensibles.

Esto no solo pone en riesgo la **[I] Integridad** de la información, sino que también puede resultar en pérdidas financieras y reputacionales significativas, Por lo anterior, es crucial que las empresas comprendan estos riesgos y adopten medidas proactivas para fortalecer su seguridad.

En este sentido, el documento aborda enfoques modernos para la seguridad del acceso a redes, especialmente en relación con las vulnerabilidades asociadas a las soluciones tradicionales de VPN. Esté gira en torno a:

Limitaciones del Acceso Remoto y VPN

Las limitaciones del acceso remoto y las VPN tradicionales representan un riesgo significativo para la seguridad de las organizaciones. Aunque las VPN permiten a los usuarios acceder a redes corporativas a través de túneles privados y cifrados, su implementación puede estar sujeta a vulnerabilidades inherentes, configuraciones incorrectas y complejidades que facilitan el acceso no autorizado. Estas debilidades pueden ser explotadas por actores maliciosos, permitiéndoles obtener acceso amplio a la red tras comprometer un acceso VPN. Además, la conexión de terceros a través de VPN puede introducir riesgos adicionales si no se implementan prácticas de ciberseguridad adecuadas como la segmentación de redes y el principio de menor privilegio. Por lo tanto, es crucial que las organizaciones evalúen y fortalezcan su postura de seguridad al considerar alternativas más modernas y seguras para el acceso remoto.

Soluciones

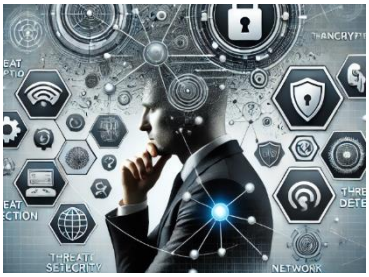

Ilustración 2 generada por ChatGPT

Las soluciones modernas para el acceso a redes, como Zero Trust, Secure Access Service Edge (SASE) y Security Service Edge (SSE), ofrecen un enfoque más seguro en comparación con las VPN tradicionales. Estas soluciones implementan políticas de **control de acceso granular**[3], lo que significa que solo los usuarios que están explícitamente autenticados y autorizados pueden acceder a aplicaciones y servicios específicos. Esto reduce significativamente el riesgo de acceso no autorizado y mejora la seguridad de los datos en tránsito. Además, al adoptar principios de Zero Trust, las organizaciones pueden monitorear continuamente la actividad de los usuarios y limitar el acceso a recursos internos, minimizando así la exposición a amenazas. La transición hacia estas soluciones modernas es esencial para fortalecer la seguridad en un entorno cada vez más centrado en la nube y proteger los activos corporativos de manera efectiva.

[2] https://attack.mitre.org/tactics/TA0008/
[3] **Es un enfoque de seguridad en el que los permisos y el acceso a recursos son definidos y gestionados con un alto nivel de detalle y especificidad**

Confianza Cero (Zero Trust)

El enfoque de Cero Confianza (Zero Trust) se basa en la premisa de que ninguna entidad, ya sea un usuario, dispositivo o aplicación, debe ser confiada por defecto, independiente de su ubicación dentro o fuera de la red. Este modelo requiere que cada acceso a datos y servicios sea autenticado y autorizado de manera continua, aplicando políticas de control de acceso granular que se alinean con el **principio de menor privilegio**[4]. Al implementar estrategias de Cero Confianza, las organizaciones pueden monitorear constantemente la actividad de los usuarios y restringir el acceso a recursos internos, lo que minimiza la exposición a amenazas y mejora la seguridad general de la red.

La adopción de este enfoque es esencial para proteger los activos de información en un entorno cada vez más centrado en la nube.

Ilustración Generada con ChatGPT

Borde de Servicio Seguro (Secure Service Edge)

El Borde de Servicio Seguro (Secure Service Edge, SSE) es un enfoque integral de seguridad en la nube que combina diversas capacidades de seguridad para proteger el acceso a aplicaciones y datos. **SSE** integra funciones como:

- Acceso a la red basado en el principio de Cero Confianza (Zero Trust Network Access)
- Gateway seguro para la web en la nube (Cloud Secure Web Gateway)
- Corredor de seguridad para el acceso a la nube (Cloud Access Security Broker).

Este modelo permite a las organizaciones gestionar la seguridad de manera centralizada, asegurando que solo los usuarios autenticados y autorizados puedan acceder a los recursos, independiente de su ubicación o dispositivo. Al adoptar **SSE**, las empresas pueden mejorar su postura de seguridad, simplificar la administración y garantizando una protección efectiva contra amenazas cibernéticas.

[4] **Es un concepto fundamental en ciberseguridad que establece que cualquier usuario, aplicación o sistema solo debe tener los permisos o privilegios mínimos necesarios para realizar su función**

Acceso a la Red con Confianza Cero (Zero Trust Network Access)

El Acceso a la Red con Confianza Cero (Zero Trust Network Access, ZTNA) es una solución de seguridad diseñada para proporcionar un acceso remoto más seguro a las aplicaciones, datos y servicios de una organización. Este enfoque se basa en políticas de control de acceso estrictamente definidas que siguen los principios de Cero Confianza, lo que significa que ningún usuario o dispositivo es confiable por defecto. Cada solicitud de acceso debe ser autenticada y autorizada continuamente, garantizando que solo los usuarios con los permisos adecuados puedan acceder a los recursos necesarios. Al implementar **ZTNA**[5], las organizaciones pueden limitar las herramientas disponibles para posibles atacantes que logren acceder a la red, reduciendo así el riesgo de movimientos laterales y compromisos de datos.

Pasarela Segura de Navegación en la Nube (Cloud Secure Web Gateway)

La Pasarela Segura de Navegación en la Nube (Cloud Secure Web Gateway, SWG) es una solución de seguridad que protege a los usuarios y dispositivos de amenazas basadas en web, al tiempo que aplica políticas de seguridad dentro de la red. Actúa como un filtro de URL entre los usuarios e internet, detectando contenido malicioso o no autorizado y controlando el acceso a la web. Además, la **SWG**[6] permite la descompresión de tráfico cifrado (SSL/TLS) para su análisis, controla aplicaciones, autentica usuarios y proporciona análisis de informes.

Ilustración 3 generada por ChatGPT

Agente de Seguridad para Acceso a la Nube (Cloud Access Security Broker)

El Agente de Seguridad para Acceso a la Nube (Cloud Access Security Broker, CASB)[7] es una solución de seguridad que ayuda a las organizaciones a gestionar y proteger sus datos en entornos de múltiples aplicaciones de software como servicio (**SaaS**)[8]. El CASB actúa como un intermediario entre los usuarios y los servicios en la nube, permitiendo la aplicación de políticas de seguridad, gobernanza y cumplimiento normativo. Además, es capaz de detectar y mitigar amenazas en la nube, asegurando que los datos estén protegidos tanto en tránsito como en reposo.

Cortafuegos como Servicio (Firewall-as-a-Service)

El Cortafuegos como Servicio (Firewall-as-a-Service, FWaaS) es una solución de seguridad basada en la nube que permite a las organizaciones monitorear y gestionar el tráfico de red de manera centralizada. Funciona de de forma similar a un cortafuegos tradicional, inspeccionando y filtrando el tráfico para aplicar políticas de seguridad y proteger contra amenazas cibernéticas. Con FWaaS, las empresas pueden beneficiarse de una administración simplificada y escalable, ya que se gestiona a través de un panel de control en la nube. Esta solución no solo mejora la seguridad de la red, sino que también facilita la integración de funciones de seguridad adicionales, promoviendo una postura de seguridad más robusta y flexible.

[5] ¿Qué es ZTNA? Acceso a la red Zero Trust | Control de acceso en red | Cloudflare
[6] ¿Qué es una puerta de enlace web segura (SWG)? | Cloudflare
[7] ¿Qué es un agente de seguridad de acceso a la nube (CASB)? | Microsoft
[8] ¿Qué es el SaaS? - Explicación del software como servicio - AWS (amazon.com)

Borde de Servicio de Acceso Seguro (Secure Access Service Edge)

El Borde de Servicio de Acceso Seguro (Secure Access Service Edge, SASE) es un modelo de arquitectura en la nube que combina capacidades de red y seguridad en un único servicio. Integra diversas funciones, como:

- Acceso a la red basado en el principio de Cero Confianza (Zero Trust Network Access)
- Pasarela Segura de Navegación en la Nube (Cloud Secure Web Gateway)
- Agente de Seguridad para Acceso a la Nube (Cloud Access Security Broker)
- Cortafuegos como Servicio (Firewall-as-a-Service).

Este enfoque permite a las organizaciones gestionar de manera centralizada la seguridad y el acceso a aplicaciones y datos, independiente de la ubicación o el dispositivo del usuario.

Red de Área Amplia Definida por Software (Software-Defined Wide Area Networking)

La Red de Área Amplia Definida por Software (Software-Defined Wide Area Networking, SD-WAN) es una tecnología que simplifica la gestión y operación de redes de área amplia al abstraer la infraestructura de red y permitir un control centralizado a través de software. SD-WAN optimiza el rendimiento de las aplicaciones y mejora la seguridad al integrar funciones de seguridad en la red. Sus características clave incluyen la selección dinámica de rutas, la administración centralizada y la visibilidad analítica, lo que permite a las organizaciones gestionar el tráfico de manera más eficiente y adaptarse a las necesidades cambiantes del negocio.

Cortafuegos de Nueva Generación (Next Generation Firewall)

El Cortafuegos de Nueva Generación (Next Generation Firewall, NGFW) es un dispositivo de seguridad de red que combina las funciones tradicionales de un cortafuegos con capacidades avanzadas de protección contra amenazas y vulnerabilidades. Aparte de realizar filtrado de paquetes y análisis de estado, los NGFW ofrecen características como la inspección profunda de paquetes, la detección de intrusiones y la prevención de intrusiones, así como la capacidad de gestionar el tráfico de aplicaciones específicas. Esta integración de funciones permite a las organizaciones mejorar su seguridad de red al proporcionar una defensa más robusta y adaptativa frente a ataques cibernéticos.

Segmentación de Red Reforzada por Hardware

La Segmentación de Red Reforzada por Hardware es una práctica de seguridad que añade una capa adicional de protección a las redes, especialmente en entornos donde las operaciones cibernéticas representan amenazas significativas para la seguridad pública y nacional. Esta técnica utiliza tecnologías unidireccionales, como puertas de enlace unidireccionales o diodos de datos, para asegurar que las conexiones a redes críticas sean controladas y limitadas. Al implementar esta segmentación, las organizaciones pueden mitigar los riesgos asociados con vulnerabilidades conocidas y desconocidas en soluciones de seguridad basadas en software, mejorando así su postura de defensa en profundidad.

Mejores Prácticas

Las mejores prácticas en seguridad de redes incluyen la implementación de entrenamientos en planes de capacitación periódicos obligatorios sobre conceptos básicos de seguridad, como phishing y gestión de contraseñas, para fomentar una cultura de ciberseguridad dentro de la organización. Además, es crucial establecer una solución robusta de gestión de identidad y acceso que utilice autenticación multifactor resistente al phishing.

Para sistemas críticos, se recomienda el uso de tecnologías unidireccionales que permitan la transferencia segura de datos de auditoría y forenses desde redes sensibles hacia sistemas de monitoreo de seguridad, mitigando así el riesgo de ciberataques que puedan pivotar[9] a través de la nube o internet hacia redes protegidas. La siguiente tabla plantea que tecnologías podrían aplicarse según su enfoque.

Tabla 1Aplicación de tecnologías para el aseguramiento de una red

Enfoque	Recomendación	Tecnología que puede implementarse
Seguridad de Acceso Remoto y VPN	Evaluar las vulnerabilidades inherentes en las soluciones tradicionales de VPN y adoptar enfoques modernos para un acceso más seguro.	• Zero Trust, Secure Access Service Edge (SASE) • Security Service Edge (SSE) • Next Generation Firewall (NGFW)
Autenticación y Control de Acceso	Implementar autenticación continua y control de acceso granular basado en el principio de menor privilegio para mitigar riesgos de accesos no autorizados.	• Zero Trust Network Access (ZTNA) • Cloud Secure Web Gateway (SWG) • Cloud Access Security Broker (CASB)
Segmentación de Redes	Adoptar una segmentación de redes reforzada por hardware para proteger los entornos críticos, utilizando tecnologías que limiten la conexión a redes sensibles.	• Segmentación de Red Reforzada por Hardware • Firewalls como Servicio (FWaaS) • SD-WAN
Gestión Centralizada de Seguridad	Implementar una gestión centralizada a través de soluciones que integren diversas funciones de seguridad para controlar de forma eficiente el acceso a aplicaciones y datos.	• Secure Service Edge (SSE), Secure Access Service Edge (SASE) • Cloud Secure Web Gateway (SWG) • CASB
Capacitación y Cultura de Ciberseguridad	Establecer capacitaciones periódicas sobre conceptos de seguridad como phishing y gestión de contraseñas para fortalecer la cultura organizacional.	• No aplica (pero se recomienda incluir autenticación multifactor y entrenamiento en Zero Trust).
Tecnologías de Defensa en Profundidad	Utilizar tecnologías unidireccionales para transferir datos sensibles de auditoría desde redes críticas hacia sistemas de monitoreo, mitigando el riesgo de ciberataques.	• Diodos de datos • Firewalls como Servicio (FWaaS) • Segmentación de Red Reforzada por Hardware

[9] Hace referencia a la técnica utilizada por atacantes para realizar movimientos laterales dentro de una red una vez que han comprometido un sistema.

Conclusiones

En un entorno donde las amenazas cibernéticas son cada vez más sofisticadas y persistentes, los enfoques tradicionales de seguridad, como las VPN, ya no son suficientes para proteger los entornos digitales. La adopción de tecnologías modernas como Zero Trust, Secure Access Service Edge (SASE) y Security Service Edge (SSE) son esenciales para mitigar riesgos y garantizar un control de acceso más seguro y granular.

Estas soluciones permiten una gestión centralizada de la seguridad, combinando funciones avanzadas como pasarelas seguras de navegación en la nube (SWG), agentes de seguridad para acceso a la nube (CASB) y cortafuegos como servicio (FWaaS), lo que refuerza la postura de defensa en profundidad.

Además, la segmentación de redes reforzada por hardware y la adopción de tecnologías unidireccionales añaden una capa adicional de protección, especialmente en entornos críticos.

De forma paralela, la capacitación periódica del personal en buenas prácticas de ciberseguridad sigue siendo un componente clave para crear una cultura organizacional resiliente ante ataques.

En conjunto, estas estrategias no solo contribuyen en mejorar la seguridad de la infraestructura de red, sino que también aseguran que los activos y datos estén protegidos frente a las amenazas modernas.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Página web: https://csirt.unad.edu.co

Referentes Bibliográficos

[1] https://www.ic3.gov/Media/News/2024/240618.pdf

[2] https://attack.mitre.org/tactics/TA0008/

[5] https://www.cloudflare.com/es-la/products/zero-trust/zero-trust-network-access/

[6] https://www.cloudflare.com/es-es/learning/access-management/what-is-a-secure-web-gateway/

[7] https://www.microsoft.com/es-co/security/business/security-101/what-is-a-cloud-access-security-broker-casb

[8] https://aws.amazon.com/es/what-is/saas/