Publicación especial del NIST
NIST SP 800-215

Guía para una empresa segura Panorama de la red

Ramaswamy Chandramouli

Esta publicación está disponible de forma gratuita en: https://doi.org/10.6028/NIST.SP.800-215

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Publicación especial del NIST
NIST SP 800-215

Guía para una empresa segura Panorama de la red

Ramaswamy Chandramouli
División de Seguridad Informática
Laboratorio de Tecnología de la Información

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-215

noviembre 2022

Departamento de Comercio de EE.
UU. Gina M. Raimondo, Secretaria

Instituto Nacional de Estándares y Tecnología Laurie
E. Locascio, directora del NIST y subsecretaria de Comercio de Estándares y Tecnología

Ciertas entidades comerciales, equipos o materiales pueden identificarse en este documento para describir adecuadamente un procedimiento o concepto experimental. Dicha identificación no pretende implicar recomendación o respaldo por parte del Instituto Nacional de Estándares y Tecnología (NIST), ni tampoco implica que el
entidades, materiales o equipos son necesariamente los mejores disponibles para el propósito.

Es posible que en esta publicación haya referencias a otras publicaciones que el NIST está desarrollando actualmente de acuerdo con las responsabilidades legales asignadas. La información de esta publicación, incluidos los conceptos y metodologías, puede ser utilizada por agencias federales incluso antes de completar dichas publicaciones complementarias. Por lo tanto, hasta que se complete cada publicación, los requisitos, pautas y procedimientos actuales, cuando existan, seguirán vigentes. Para fines de planificación y transición, es posible que las agencias federales deseen seguir de cerca el desarrollo de estas nuevas publicaciones por parte del NIST.

Se alienta a las organizaciones a revisar todos los borradores de publicaciones durante los períodos de comentarios públicos y brindar comentarios al NIST. Muchas publicaciones de ciberseguridad del NIST, además de las mencionadas anteriormente, están disponibles en https://csrc.nist.gov/publications.

Autoridad
Esta publicación ha sido desarrollada por el NIST de acuerdo con sus responsabilidades legales según la Ley Federal de Modernización de la Seguridad de la Información (FISMA) de 2014, 44 USC § 3551 et seq., Ley Pública (PL) 113-283.
El NIST es responsable de desarrollar estándares y pautas de seguridad de la información, incluidos los requisitos mínimos para los sistemas de información federales, pero dichos estándares y pautas no se aplicarán a los sistemas de seguridad nacionales sin la aprobación expresa de los funcionarios federales apropiados que ejerzan autoridad política sobre dichos sistemas. Esta directriz es consistente con los requisitos de la Circular A-130 de la Oficina de Gestión y Presupuesto (OMB).

Nada en esta publicación debe considerarse en contradicción con las normas y directrices que el Secretario de Comercio considera obligatorias y vinculantes para las agencias federales en virtud de la autoridad legal. Estas pautas tampoco deben interpretarse como una alteración o sustitución de las autoridades existentes del Secretario de Comercio, el Director de la OMB o cualquier otro funcionario federal. Esta publicación puede ser utilizada por organizaciones no gubernamentales de forma voluntaria y no está sujeta a derechos de autor en los Estados Unidos. Sin embargo, el NIST agradecería la atribución.

Políticas de la serie técnica del NIST
Declaraciones de derechos de autor, uso legítimo y licencia
Sintaxis del identificador de publicaciones de la serie técnica del NIST

Historial de publicaciones
Aprobado por la Junta de Revisión Editorial del NIST el 2022-11-10

Cómo citar esta publicación de la serie técnica del NIST: Guía Chandramouli
R (2022) para un panorama de redes empresariales seguras. (Instituto Nacional de Estándares y Tecnología, Gaithersburg, MD), Publicación especial (SP) NIST NIST SP 800-215. https://doi.org/10.6028/NIST.SP.800-215

Autor ORCID iD
Ramaswamy Chandramouli: 0000-0002-7387-5858

Información del contacto
sp800-215-comments@nist.gov

NIST SP 800-215
noviembre 2022

Instituto Nacional de Estándares y Tecnología
A la atención de: División de Seguridad Informática, Laboratorio de Tecnología de la Información
100 Bureau Drive (parada de correo 8930) Gaithersburg, MD 20899-8930

Abstracto

El acceso a múltiples servicios en la nube, la expansión geográfica de los recursos de tecnología de la información (TI) empresarial (incluidos múltiples centros de datos) y el surgimiento de aplicaciones basadas en microservicios (en contraposición a las monolíticas) han alterado significativamente el panorama de las redes empresariales. Este documento está destinado a proporcionar orientación para este nuevo panorama de redes empresariales desde una perspectiva de operaciones seguras. Por lo tanto, comienza examinando las limitaciones de seguridad de las soluciones actuales de acceso a la red empresarial. Luego considera mejoras en las funciones de seguridad de los dispositivos de red tradicionales en forma de soluciones de seguridad puntuales, configuraciones de red para diversas funciones de seguridad (por ejemplo, seguridad de aplicaciones/servicios, servicios en la nube). seguridad de acceso, seguridad de dispositivos o terminales), marcos de seguridad que integran estas configuraciones de red individuales (por ejemplo, acceso a la red de confianza cero [ZTNA]) y la infraestructura de red de área amplia (WAN) en evolución para proporcionar un conjunto integral de servicios de seguridad para los modernos. panorama de red empresarial (por ejemplo, borde de servicio de acceso seguro [SASE]).

Palabras clave

agente de seguridad de acceso a la nube (CASB); cortafuegos; microsegmentación; borde de servicio de acceso seguro (SASE); puerta de enlace web segura (SWG); orquestación, automatización y respuesta de seguridad (SOAR); perímetro definido por software (SDP); red de área amplia definida por software (SD-WAN); red privada virtual (VPN); Acceso a la red de confianza cero (ZTNA).

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnología de la Información (ITL) del Instituto Nacional de Estándares y Tecnología (NIST) promueve la economía y el bienestar público de los EE. UU. brindando liderazgo técnico para la infraestructura de estándares y mediciones de la nación. ITL desarrolla pruebas, métodos de prueba, datos de referencia, implementaciones de prueba de concepto y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. Las responsabilidades de ITL incluyen el desarrollo de estándares y directrices de gestión, administrativos, técnicos y físicos para la seguridad y privacidad rentables de información distinta de la relacionada con la seguridad nacional en los sistemas de información federales. La publicación especial serie 800 informa sobre las investigaciones, directrices y esfuerzos de divulgación de ITL en materia de seguridad de sistemas de información y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas.

Aviso de divulgación de patentes

AVISO: ITL ha solicitado que los titulares de reivindicaciones de patente cuyo uso pueda ser necesario para cumplir con las directrices o requisitos de esta publicación revelen dichas reivindicaciones de patente a ITL. Sin embargo, los titulares de patentes no están obligados a responder a las convocatorias de patentes de ITL y ITL no ha realizado una búsqueda de patentes para identificar cuáles, si las hubiera, pueden aplicarse a esta publicación.

A la fecha de publicación y tras las convocatorias para la identificación de reivindicaciones de patente cuyo uso puede ser necesario para cumplir con las directrices o requisitos de esta publicación, no se han identificado dichas reivindicaciones de patente para ITL.

ITL no hace ni da a entender que no se requieren licencias para evitar la infracción de patentes en el uso de esta publicación.

Tabla de contenido

Lista de Figuras

Expresiones de gratitud

El autor desea expresar su agradecimiento a Isabel Van Wyk del NIST por su detallada revisión editorial tanto de la versión para comentarios públicos como de la publicación final.

Resumen ejecutivo

El panorama de las redes empresariales ha experimentado enormes cambios en la última década debido a los tres factores siguientes:

- Acceso empresarial a múltiples servicios en la nube,
- La distribución geográfica de los recursos de TI basados en la empresa (locales) (p. ej., múltiples centros de datos, oficinas centrales y sucursales), y
- Cambios en la arquitectura de la aplicación de ser monolítica a un conjunto de elementos débilmente acoplados. microservicios.

Los impactos de estos factores en la seguridad del panorama de la red empresarial incluyen:

- Desaparición del concepto de perímetro de red que se puede proteger y la necesidad de proteger cada endpoint (dispositivo o servicio) que lo trata como un perímetro.
- Aumento de la superficie de ataque debido a la enorme multiplicidad de recursos y componentes de TI (informática, redes, almacenamiento)
- Escalada de ataques a través de varios límites de red aprovechando la conectividad características

Este documento está destinado a proporcionar orientación para este nuevo panorama de redes empresariales desde una perspectiva de operaciones seguras. La metodología adoptada considera primero los desafíos de seguridad que plantea el nuevo panorama de redes y examina las limitaciones de las tecnologías de acceso a redes actuales. Luego muestra cómo las soluciones para enfrentar los desafíos han evolucionado desde una función de seguridad específica hasta un marco de seguridad y una infraestructura de seguridad integral que proporciona un conjunto holístico de servicios de seguridad. Las áreas específicas abordadas incluyen:

- Mejoras en las funciones de los dispositivos de seguridad de red tradicionales
- Configuraciones de redes empresariales seguras para funciones de seguridad específicas
- Marcos de seguridad que integran configuraciones de red individuales
- Infraestructura de red de área amplia (WAN) en evolución que proporciona un conjunto completo de servicios de seguridad

Según los impulsores descritos anteriormente, una red empresarial en el contexto de este documento abarca lo siguiente:

- Las redes virtuales privadas que la empresa (suscriptor de servicios en la nube) configura en la red nativa del proveedor de servicios en la nube dentro de la cual se aprovisionarán sus recursos informáticos (por ejemplo, red virtual [VNet], nube privada virtual [VPC]).
- Varias redes locales en las instalaciones de la empresa (por ejemplo, centros de datos empresariales, oficinas centrales y sucursales)
- La parte de una red de área amplia que utiliza la empresa para conectar sus diversos Ubicaciones geográficamente dispersas y puntos de acceso a servicios en la nube.

1. Introducción

El panorama de las redes empresariales ha experimentado una transformación significativa en la última década. Los impulsores de esta transformación son (a) el acceso empresarial a múltiples servicios en la nube, (b) la distribución geográfica de los recursos de TI de propiedad empresarial (locales) (por ejemplo, en la sede central, en varias sucursales y en los centros de datos) y (c) cambios en la arquitectura de las aplicaciones, que pasan de ser monolíticas a ser un conjunto de microservicios débilmente acoplados, a menudo con una infraestructura dedicada (llamada malla de servicios) que proporciona todos los servicios de las aplicaciones, incluida la seguridad. Los impactos de alto nivel de estos factores en la seguridad del panorama actual de redes empresariales son (a) la desaparición del concepto de perímetro asociado con la red empresarial; (b) un aumento de la superficie de ataque debido a la enorme multiplicidad de componentes de recursos de TI asociados con la informática, el almacenamiento y los dispositivos de red; y (c) la escalada de ataques a través de varios límites de red aprovechando las características de conectividad. Antes de brindar orientación para operaciones seguras en este nuevo panorama de red, este documento considerará las implicaciones estructurales y de seguridad de los impulsores para mejorar la comprensión de sus componentes y flujos de datos.

1.1. Implicaciones estructurales de los impulsores en el panorama de las redes empresariales

Para tener una buena visión estructural del panorama actual de las redes empresariales, es necesario observar el entorno actual de TI empresarial en general. El entorno de TI ahora consta de:

- Suscripción a múltiples servicios en la nube, como Infraestructura como Servicio (IaaS) para informática, Software como servicio (SaaS) para aplicaciones, Plataforma como servicio (PaaS) para una plataforma de desarrollo de aplicaciones y otros servicios en la nube (por ejemplo, identidad como servicio [IDaaS] para autenticación)
- Aplicaciones de TI empresariales (locales) que se encuentran en la sede corporativa y sucursales y centros de datos distribuidos geográficamente
- Aplicaciones de TI que van desde ser monolíticas hasta estar compuestas por microservicios poco acoplados, cada uno alojado en plataformas heterogéneas.
- Presencia de dispositivos informáticos de vanguardia, incluido el Internet de las cosas (IoT), en algunos entornos

Los escenarios anteriores exigen una conectividad generalizada entre los sistemas de TI que ahora define el panorama actual de las redes empresariales. La conectividad, a su vez, implica:

- Conectividad entre recursos de TI (por ejemplo, servidores para computación y almacenamiento) en centros de datos (tejido de red)
- Conectividad entre recursos de TI dentro de una oficina corporativa o sucursal (p. ej., Fidelidad inalámbrica (Wi-Fi), red de área local - LAN y red de área local virtual - VLAN)
- Conectividad para que los usuarios accedan de forma remota a recursos de TI desde sus hogares, lugares de viaje, sucursales y oficinas corporativas utilizando redes de área amplia (WAN), que utilizan múltiples redes como Internet, conmutación de etiquetas multiprotocolo (MPLS) y, en algunos casos, – redes celulares (por ejemplo, 4G/LTE, 5G).

- Conectividad a servicios en la nube proporcionados por un proveedor de servicios en la nube (CSP) a través de una red privada virtual (VPN) o suscripción a servicios WAN (licencias de equipos locales o basados en la nube)

1.2. Implicaciones de seguridad de los controladores en el panorama de las redes empresariales

Consideremos ahora las implicaciones inmediatas de seguridad de estos factores en el panorama de las redes empresariales.

Suscripción a múltiples servicios en la nube: el acceso a servicios en la nube desde múltiples proveedores de nube se ha convertido en la norma para muchas empresas. Esta tendencia está motivada no sólo por la necesidad de evitar una situación de bloqueo de proveedores de nube, sino también porque diferentes CSP ofrecen diferentes funciones de valor agregado para diferentes servicios (por ejemplo, IaaS, SaaS). La consecuencia de esta tendencia es que, desde un punto de vista empresarial, las siguientes redes se han convertido en extensiones de la red empresarial y, por lo tanto, entran dentro del alcance de la gestión de redes empresariales con las responsabilidades correspondientes de garantizar que las protecciones de seguridad se conviertan en una función crítica.

- Red utilizada para acceder a los servicios en la nube (por ejemplo, VPN o WAN suscritas)
- Red Intercloud (ya que la comunicación entre un CSP y otro puede ser inevitable)
- La red dentro del proveedor de la nube por la que se debe navegar para acceder a los servicios suscritos. servicios (por ejemplo, VPC, VNET).

Distribución geográfica de los recursos y usuarios de TI: los recursos de TI ahora están ampliamente distribuidos no sólo debido a la distribución geográfica de las instalaciones empresariales (por ejemplo, oficinas centrales y sucursales), sino también por consideraciones de confiabilidad y recuperación ante desastres (DR). Además, las aplicaciones alojados en esos recursos ahora pueden acceder los usuarios desde diversas instalaciones empresariales (a través de la red empresarial), así como desde hogares y ubicaciones públicas (por ejemplo, hoteles y cafeterías) a través de múltiples dispositivos, como computadoras de escritorio, portátiles y teléfonos móviles. Garantizar el acceso seguro desde estas diversas ubicaciones y dispositivos se convierte en responsabilidad de la empresa.

Cambios en la arquitectura de aplicaciones: Las arquitecturas de aplicaciones, especialmente aquellas de aplicaciones nativas de la nube, han pasado de ser monolíticas a estar basadas en microservicios para cumplir con los requisitos de agilidad de implementación y escalabilidad modular. Esto, combinado con las primitivas de DevSecOps (un paradigma que cubre desarrollo, seguridad y operaciones), como los canales de integración continua/implementación continua (CI/CD) para el desarrollo y la implementación de software, ha mejorado el perfil de seguridad de las aplicaciones, pero también ha introducido nuevas tecnologías. vectores de amenazas relacionados con los propios flujos de trabajo de CI/CD.

1.3. La necesidad de una guía de seguridad

Según las implicaciones de seguridad analizadas en la subsección anterior, existe un nuevo escenario de seguridad en el panorama actual de redes empresariales que debe abordarse mediante una guía de seguridad. Algunos de los aspectos más destacados de este escenario son:

- Las ubicaciones de acceso ubicuas, las ubicaciones de alojamiento ubicuas de los componentes de la aplicación y los múltiples protocolos de transporte WAN han provocado cambios en los enfoques, objetivos y principios de seguridad.

- El enfoque de seguridad ha pasado de estar centrado en la red (es decir, interno/corporativo) red versus Internet externa/pública) para centrarse en el usuario, dispositivo, punto final y servicio.

- La nueva relación de confianza no sólo debe basarse en la identidad o la ubicación del acceso, pero mejorado para incluir la validación de cada solicitud de acceso (no solo al comienzo de una sesión de acceso), así como el conjunto aplicable de información contextual asociada con el usuario, dispositivo o servicio.

1.4. Alcance

El alcance de este documento incluye:

- Una visión estructural del panorama de la red empresarial basada en la distribución de TI recursos y los consiguientes desafíos de seguridad que plantea
- Soluciones emergentes y de última generación en términos de conjuntos de características y requisitos para abordar los desafíos de seguridad; Las soluciones discutidas se centrarán en los niveles funcional y operativo.

1.5. Público objetivo

Esta guía está dirigida a arquitectos de diseño de redes y arquitectos de soluciones de seguridad de redes en organizaciones con un entorno de TI híbrido (que consta de aplicaciones locales y basadas en la nube) con una combinación de aplicaciones heredadas y basadas en microservicios (es decir, nativas de la nube). .

1.6. Organización de este documento

La organización de este documento es la siguiente:

- La Sección 2 considera los principios, tecnologías y limitaciones del acceso a la red tradicional en el contexto del panorama actual de la red empresarial.
- La Sección 3 proporciona una breve descripción funcional de los dispositivos de seguridad de red (algunos nuevos, otros tradicionales (por ejemplo, firewall)) que tienen capacidades mejoradas para satisfacer las necesidades de seguridad del panorama de red actual.
- La Sección 4 describe varias configuraciones de red que han evolucionado específicamente para realizar funciones de seguridad (por ejemplo, autenticación de dispositivo).
- La Sección 5 considera un marco (es decir, ZTNA) que integra dos o más de estas configuraciones de red independientes para realizar una arquitectura empresarial abstracta (arquitectura de confianza cero [ZTA]) y analiza dos técnicas de seguridad de red empresarial candidatas: microsegmentación y perímetro definido por software (SDP).
- La Sección 6 se centra en la evolución de la parte WAN de la red empresarial. panorama y ofertas mejoradas de servicios WAN con difusión global con una infraestructura de servicios de seguridad incorporada.
- La Sección 7 proporciona el resumen y las conclusiones.

2. Enfoques tradicionales de acceso a la red empresarial y sus limitaciones

La Sección 1 describió las implicaciones estructurales y de seguridad de los impulsores del panorama actual de redes empresariales, que han impactado la mecánica del acceso seguro a las aplicaciones a través de la red. Esta sección analiza las limitaciones de seguridad de los enfoques tradicionales de acceso a la red.

- Limitación de las protecciones basadas en el perímetro de la red.
- Limitaciones del acceso basado en VPN
- Limitaciones de la tecnología MPLS como WAN empresarial
- Limitaciones de la infraestructura de autenticación

2.1. Limitaciones de las protecciones basadas en el perímetro de la red

Las primeras soluciones para el acceso seguro a la red empresarial estaban orientadas a entornos con perímetros de red bien definidos. Todos los recursos de TI de la empresa eran puntos finales de las LAN empresariales (generalmente definidas como un piso en una gran empresa, edificio o campus pequeño), y varias LAN conectadas entre sí dentro de un edificio o campus definido constituían la red corporativa interna. Los puntos de entrada a esta red corporativa estaban protegidos mediante dispositivos llamados firewalls.
En este entorno, todos los dispositivos y usuarios dentro de las LAN con firewall eran totalmente confiables y, por lo tanto, se consideraban seguros para acceder a los recursos de las aplicaciones. Sin embargo, los siguientes factores han anulado el concepto de ese perímetro y ampliado enormemente la superficie de ataque:

- Naturaleza distribuida de la aplicación en aquellas ubicadas dentro de un centro de datos corporativo, sucursales remotas y múltiples ubicaciones en la nube
- Enfoque perimetral basado en la premisa de que la amenaza se origina fuera de la red, razón por la cual la mayoría de las soluciones de seguridad perimetral (por ejemplo, sistema de prevención de intrusiones - IPS, sistemas de detección de intrusiones - IDS, firewalls) se centran únicamente en el tráfico norte-sur (es decir, ingreso, que se refiere al tráfico que se origina desde fuera de la red local y está destinado a puntos finales en la red del clúster local). Sin embargo, más del 75 % del tráfico de red ahora es de este a oeste (es decir, dentro de la red local) o de servidor a servidor (debido a que las aplicaciones se basan en microservicios), lo cual es en gran medida invisible para los equipos de seguridad, aunque ahora hay cierta visibilidad. buscado a través de soluciones de detección y respuesta de endpoints (EDR) que recopilan datos de telemetría de seguridad en los endpoints. Cualquier amenaza que ya esté dentro de una red puede moverse lateralmente y permanecer sin ser detectada durante días o incluso meses.
- Computación perimetral [1], donde gran parte de la computación tiene lugar cerca de la ubicación de múltiples dispositivos de IoT que pueden estar dispersos geográficamente
- Usuarios ubicados tanto dentro como fuera de la red corporativa, como en hogares, sucursales remotas y lugares públicos (por ejemplo, hoteles, pubs); algunas empresas también deben
  Proporcionar acceso a socios del ecosistema, que pueden estar en sus propias redes corporativas.

2.2. Limitaciones del acceso basado en VPN

El aumento de empleados que trabajan a distancia debido a la pandemia ha requerido un medio para el acceso seguro a los recursos de TI dentro de una red empresarial en forma de VPN. Una VPN permite

organizaciones para ampliar la seguridad basada en el perímetro a través de una red pública. La seguridad se habilita mediante la configuración de un túnel seguro en la red pública utilizando protocolos como Internet Protocol Security (IPSEC) y Transport Layer Security (TLS).

Sin embargo, existen algunas limitaciones y riesgos de seguridad asociados con las VPN.

- Una tendencia creciente implica el movimiento de recursos corporativos a la nube y la uso de dispositivos móviles. Las conexiones VPN que establecen los usuarios remotos terminan en los concentradores VPN ubicados en el borde de la red corporativa. Por lo tanto, incluso el tráfico generado durante el acceso al servicio de nube de esos usuarios llega al borde de Internet corporativo y debe validarse y enrutarse de regreso a Internet para acceder a los recursos de la nube. Este fenómeno se denomina “hairpinning”, genera distancia adicional, aumenta la latencia de la red y tiene el potencial de provocar cuellos de botella en el tráfico.
- Divulgación periódica de vulnerabilidades. Dos ejemplos recientes son el "secuestro de sesión" y “extracción de ID de cuenta” [2].
- Cuando las VPN se implementan como dispositivos de hardware, se impone un límite al número de usuarios. quién puede conectarse a través de la puerta de enlace de la red y limita la escalabilidad.
- Las VPN a menudo requieren agentes, lo que dificulta el acceso en escenarios con un gran volumen de usuarios de terceros (contratistas y socios) [53].

2.3 Limitación de la tecnología MPLS como WAN empresarial

La tecnología de conmutación de etiquetas multiprotocolo (MPLS) se utiliza para las WAN empresariales, pero la amplia extensión geográfica de una red empresarial con múltiples centros de datos y servicios en la nube ha impuesto algunas limitaciones a su uso (además del costo).

- La extensión geográfica de los recursos de TI empresariales y las conexiones de red posteriores han hecho que el recorrido a través de Internet sea inevitable para muchas partes de la red de acceso de la empresa. Dado que MPLS es una red diferente, proporciona acceso a Internet sólo a través de puntos de acceso designados y limitados (similar al fenómeno de la fijación del cabello).
  Esto aumenta la latencia para aplicaciones corporativas urgentes.
- Dada la diferente tecnología de red, los dispositivos y los procedimientos de configuración posteriores son diferentes, lo que hace que la gestión de la red sea una tarea compleja.

2.4 Limitación de la infraestructura de autenticación

En el panorama de red actual, que consiste en acceso a aplicaciones locales y basadas en la nube, existen infraestructuras de autenticación (tanto empresariales como basadas en la nube) para autenticar a los usuarios finales utilizando varios enfoques basados en tokens (por ejemplo, Jason Web Tokens [JWT] o tokens de lenguaje de marcado de afirmación de seguridad (SAML) 2.0). Esta infraestructura por sí sola no es suficiente para satisfacer las necesidades de autenticación del entorno que contiene aplicaciones basadas en microservicios, que se están volviendo omnipresentes tanto en entornos empresariales como en la nube. Esta clase de aplicación consta de microservicios débilmente acoplados que requieren la generación de múltiples solicitudes entre servicios para completar un proceso o transacción comercial. Este escenario, en

a su vez, necesita una infraestructura para autenticar también servicios (además de usuarios) con requisitos especiales como los siguientes:

- Se requiere una identidad criptográfica portátil e interoperable para cargas de trabajo o servicios, así como una forma estandarizada de recuperar, validar e interactuar con esas identidades. Un ejemplo de tal especificación es Secure Production Identity Framework for Everyone (SPIFFE) [47].

- La ubicación del servicio puede cambiar debido a la naturaleza virtualizada de la aplicación. entorno de alojamiento (por ejemplo, migración a diferentes máquinas virtuales (VM), migración a un pod diferente en aplicaciones en contenedores). Por tanto, la identidad debe abstraer el entorno que alberga el servicio.
- La validación de la identidad (autenticación) y la autorización debe realizarse continuamente (y no solo al comienzo de una solicitud de servicio), ya que el perfil de riesgo asociado con la solicitud puede cambiar si hay múltiples entidades involucradas o si hay cambios en el comportamiento. patrones que deben incluirse como parámetro de validación y monitorearse.

3. Dispositivos de seguridad de red en el panorama de redes empresariales

Esta sección considera algunos dispositivos de seguridad de red nuevos y funciones mejoradas en dispositivos establecidos para satisfacer las necesidades de seguridad del panorama de red actual. Estas pueden verse simplemente como soluciones de seguridad puntuales, pero la evaluación de sus funciones y características proporcionará una comprensión de la efectividad de las configuraciones y tecnologías de red que forman parte de las soluciones integradas que se analizarán en las Secciones 4 y 5, respectivamente.

3.1. Agente de seguridad de acceso a la nube (CASB)

Dada la creciente suscripción a múltiples nubes en muchas empresas, una de las piezas de software más importantes es el agente de seguridad de acceso a la nube (CASB). Se encuentra en la red entre los clientes de servicios en la nube (CSC) y los proveedores de servicios en la nube (CSP). La evolución de la funcionalidad CASB se puede rastrear de la siguiente manera [3]:

- La función principal de la primera generación de CASB fue el descubrimiento de recursos. Proporcionaron visibilidad de todos los recursos de la nube a los que accedieron los usuarios empresariales, evitando o minimizando así las posibilidades de TI en la sombra. La TI en la sombra es la práctica de algunos usuarios que utilizan aplicaciones en la nube que no están autorizadas por la administración de TI de la empresa desde el hogar o la oficina utilizando escritorios empresariales. Un ejemplo de esto es el uso de aplicaciones de software como servicio (SaaS) no aprobadas para compartir archivos, redes sociales, colaboración y conferencias web [4]. Esta generación de CASB también proporciona algunas estadísticas, como la utilización del software como servicio (SaaS).

- La generación actual de CASB impone políticas de seguridad y gobernanza para aplicaciones en la nube, lo que permite a las empresas extender sus políticas locales a la nube.
  Los servicios de seguridad específicos proporcionados por CASB incluyen:
  - Protección de los datos empresariales que residen en los servidores de los proveedores de servicios en la nube (debido a suscripciones SaaS o IaaS), así como la entrada y salida de datos (es decir, capacidades de Prevención de pérdida de datos [DLP]) de esos servidores.
  - Seguimiento de amenazas, como secuestro de cuentas y otras actividades maliciosas, algunas de las cuales pueden detectar anomalías en el comportamiento de acceso a la nube de los usuarios (a través de una sólida funcionalidad de análisis de comportamiento de usuarios y entidades (UEBA)) y detener amenazas internas y ataques cibernéticos avanzados [5].
  - Detección de malas configuraciones en los servidores IaaS y cloud contratados de la empresa. Estas configuraciones erróneas plantean graves riesgos de seguridad, como violaciones de datos. Las alertas generadas por CASB debido a configuraciones erróneas en las implementaciones de IaaS de la empresa dirigen a la empresa a seguir pautas, como los puntos de referencia del Centro para la Seguridad de Internet (CIS) para servicios de nube pública, mejorando así el perfil de seguridad general de la empresa para el acceso a la nube [4] .

3.2. Capacidades de firewall mejoradas

Las funciones de seguridad de los cortafuegos se han ampliado junto con el cambiante panorama de las redes. Los firewalls comenzaron como dispositivos de hardware que impedían que los paquetes de red de un dispositivo con una ubicación de red particular (por ejemplo, una combinación de dirección y puerto de Protocolo de Internet (IP)) en un

subred (p. ej., red externa o Internet) acceda a un dispositivo en otra ubicación de red o subred (p. ej., intranet o zona desmilitarizada (DMZ) o red corporativa). En esa configuración, aseguró principalmente un perímetro de red. La evolución de las funciones del firewall se puede rastrear basándose en los siguientes conjuntos de características [6]:

- Filtros de paquetes y traducción de direcciones de red: el filtrado de paquetes y la traducción de direcciones de red (NAT) se utilizan para monitorear y controlar los paquetes que se mueven a través de una interfaz de red, aplicar reglas de seguridad predeterminadas y ocultar la red interna de la Internet pública.

- Inspección de estado: el firewall de estado, también conocido como filtrado dinámico de paquetes, monitorea el estado de las conexiones y determina qué tipos de paquetes de datos pertenecen a una conexión activa conocida y se les puede permitir pasar a través del firewall.

- Inspección profunda de paquetes (DPI): esta característica, también conocida como rastreo de paquetes, examina el contenido de los paquetes (tanto el encabezado como la carga útil, a diferencia de la inspección de estado que inspecciona solo el encabezado del paquete). Además de la capacidad proporcionada por la inspección de estado, tiene capacidades relacionadas con la búsqueda de amenazas ocultas dentro del flujo de datos, como intentos de exfiltración de datos, violaciones de políticas de contenido, malware y más.

- Detección y respuesta a amenazas: los firewalls modernos pueden recopilar y analizar suficientes datos a través de múltiples paquetes y sesiones para detectar amenazas e incidentes de seguridad dirigidos a un sistema en particular o una familia de sistemas. Estos datos de múltiples firewalls también pueden dirigirse a la gestión de eventos e información de seguridad (SIEM) y correlacionarse con datos de otras herramientas de seguridad y sistemas de TI para detectar ataques en toda la empresa que abarcan múltiples sistemas y capas de red. Además, estos datos se pueden utilizar para comprender la evolución de las amenazas y definir nuevas reglas de acceso, patrones de ataque y estrategias defensivas [6].

- Capacidades de registro y auditoría: las capacidades de registro y auditoría dan como resultado la construcción de eventos de red que se pueden utilizar para identificar patrones de rendimiento y problemas de seguridad.

- Funciones de control de acceso: Las funciones de control de acceso imponen un acceso sofisticado granular políticas de control.

- Múltiples ubicaciones y funciones: los firewalls residen en diferentes ubicaciones para realizar diferentes funciones. Los firewalls en el borde de la red realizan la función de protección del perímetro de la red filtrando fuentes y destinos no permitidos y bloqueando los paquetes de amenazas potenciales. Los firewalls dentro de un centro de datos pueden segmentar la red interna para evitar el movimiento lateral del tráfico y aislar recursos sensibles (por ejemplo, servicios y almacenes de datos). Los firewalls basados en dispositivos evitan el tráfico malicioso que entra y sale de los puntos finales.

- Interfaces de programación de aplicaciones (API) abiertas: permiten la integración con muchos productos de red que proporcionan capacidades de seguridad adicionales.

- Capacidades de composición de políticas: algunos firewalls pueden tener la capacidad de fusionar políticas en el momento de la aplicación para garantizar que se apliquen políticas consistentes a diferentes clases de usuarios (por ejemplo, aquellos en las instalaciones y en nubes públicas y privadas).

- Cortafuegos de aplicaciones web (WAF): esta clase de cortafuegos se ha utilizado desde que se accedía a las aplicaciones web a través de protocolos web, como el Protocolo de transferencia de hipertexto.

(HTTP), nació. Una característica avanzada en esta clase de firewalls es el filtrado avanzado del Localizador uniforme de recursos (URL). Esta es la capacidad de detectar tráfico de URL maliciosas y prevenir amenazas y ataques basados en la web al recibir datos en tiempo real analizados por algoritmos de aprendizaje automático [7][8]. Específicamente, esta clase de firewalls puede inspeccionar vectores de amenazas para detectar inyecciones de SQL, inyecciones de comandos del sistema operativo (SO) y ataques de secuencias de comandos entre sitios, así como prevenir ataques entrantes. Se utilizan en redes de entrega de contenidos (CDN) y para evitar la denegación de servicio distribuido (DDoS).
ataques. Algunas características adicionales que se encuentran en esta clase de firewalls son:

a. Capacidad para especificar una lista permitida de servicios (control a nivel de aplicación)

b. El tráfico coincide con la intención de los puertos permitidos

C. Filtrado de algunos protocolos no deseados.

3.3. Juego de electrodomésticos con funciones integradas

- Gestión unificada de amenazas (o UTM): los dispositivos UTM combinan muchas de las funciones de seguridad más críticas (firewall, IPS, concentrador VPN, antivirus de puerta de enlace, filtrado de contenidos y equilibrio de carga WAN) en un solo dispositivo, normalmente con una consola de gestión unificada.

- Firewall de próxima generación (NGFW): la característica distintiva de NGFW es el conocimiento de los datos de las aplicaciones. Puede analizar datos no sólo en las capas 3 y 4 de una pila de interconexión de sistemas abiertos (OSI), sino también en la capa 7, el nivel de aplicación. Sus capacidades se extienden más allá del filtrado de paquetes y la inspección de estado. Hay múltiples opciones de implementación disponibles para NGFW, como un dispositivo en el centro de datos, como software que se ejecuta en una máquina virtual en una nube o como un servicio en la nube (FWaaS). Algunas capacidades de NGFW incluyen [9]:

  a. Inspección profunda de paquetes (DPI)

  b. Descifrado TLS e inspección de la carga útil del paquete

  C. Función del sistema de prevención de intrusiones (IPS)

- Protección de aplicaciones web y API (WAAP): se trata de un enfoque de seguridad integral y una mejora con respecto a WAF. WAF es un componente integral para la seguridad API, BOT
(abreviatura de Robot) defensa y protección DDOS.

  a. Estos pueden ofrecerse como un conjunto de productos o como un servicio basado en la nube [10][11].

  b. Puerta de enlace web segura (SWG): los SWG son dispositivos que se utilizan para
  acceso y control de aplicaciones basadas en la nube, así como gobernanza del acceso a la web abierta para usuarios empresariales en ubicaciones ubicuas (por ejemplo, oficinas centrales, sucursales, hogares, ubicaciones remotas). Un SWG es fundamentalmente un filtro web que protege el tráfico saliente de usuarios a través de la inspección HTTP o del Protocolo seguro de transferencia de hipertexto (HTTPS) [12]. También protege los puntos finales de los usuarios de amenazas basadas en la web que pueden ocurrir cuando los usuarios hacen clic en enlaces a sitios web maliciosos o a sitios web infectados con malware.
  Centralizan el control, la visibilidad y los informes en muchas ubicaciones y tipos de usuarios. No reemplazan a los WAF,

que protegen los sitios web alojados en centros de datos empresariales y grandes sedes centrales de ataques entrantes.

3.4. Herramientas de automatización de seguridad de red

Las herramientas de automatización de la seguridad de la red automatizan los procesos del ciclo de vida involucrados en la implementación, observabilidad/monitoreo, recopilación/información de inteligencia sobre amenazas (por ejemplo, generar alertas de violaciones de seguridad para que el personal de seguridad tome medidas oportunas) y, en algunos casos, remediación automática. Estas herramientas automatizadas son una parte indispensable del panorama actual de redes empresariales, especialmente aquellas que consisten en recursos de TI altamente distribuidos locales y basados en la nube.

Las capacidades de seguridad de las herramientas de red se incluyen en la categoría de capacidades de seguridad de puntos de aplicación de políticas (PEP) que se analizan ampliamente en el Caso de uso de la nube TIC 3.0 de CISA [51]. En ese documento también se incluyen orientaciones para el despliegue de estas capacidades. La intención del material de esta sección es resaltar algunas métricas de nivel superior que esta categoría de herramientas debe satisfacer para realizar sus funciones previstas de manera efectiva; no está destinado a usarse como guía de implementación. Cada métrica de nivel superior está etiquetada con la abreviatura NSAT-HLM-x, donde NSAT significa herramienta de automatización de seguridad de red, HLM significa métrica de alto nivel y x significa secuencia numérica.

- NSAT-HLM-1: Las herramientas deben escalarse para cumplir con el volumen, la velocidad y la variedad de paradigmas actuales de desarrollo, implementación y mantenimiento de aplicaciones [13]. Este requisito es fundamental en entornos donde se utiliza DevSecOps para implementar no solo aplicaciones sino también infraestructuras, estas últimas utilizando herramientas de infraestructura como código (IaC).
  Estas herramientas son una parte integral de los flujos de trabajo automatizados inteligentes llamados canales de CI/CD, que los invocan para implementar servidores (informática), redes e infraestructura de almacenamiento.
  Por lo tanto, esta clase de herramientas de automatización de red debería tener la capacidad de integrarse perfectamente en los canales de CI/CD correspondientes.
- NSAT-HLM-2: Las herramientas deben tener la capacidad de minimizar la intervención humana para la corrección de la seguridad, que es lenta y propensa a errores. En otras palabras, cuantas más funciones de corrección automatizadas estén integradas en la herramienta, mejor.
- NSAT-HLM-3 (inteligencia y protección contra amenazas mejoradas): las herramientas deben tener inteligencia de amenazas avanzada, capacidades de prevención de amenazas en tiempo real para vulnerabilidades conocidas y de día cero, y funciones de espacio aislado para aislar el tráfico malicioso.
- NSAT-HLM-4 (aprovechando el conocimiento de eventos anteriores): Las herramientas deben tener características para hacer coincidir eventos actuales con los pasados y para aprovechar las medidas de remediación realizadas para esas instancias en la solución actual. Esto provoca una reducción del tiempo medio de interrupción [14].

Las herramientas de observación y monitoreo de red y las herramientas de aprovisionamiento de red son clases importantes de herramientas de automatización de seguridad de red. Los requisitos y el conjunto de características solo para estas dos clases se analizan en las siguientes subsecciones.

3.4.1. Herramientas de observación y monitoreo de red

Esta clase de herramientas recopila estos datos para obtener visibilidad de toda la red. Luego, estos datos se utilizan para generar un panel que presenta la topografía de la red empresarial mostrando todas las conexiones y presentando parámetros operativos clave (por ejemplo, latencia, nivel de tráfico de la red). Algunos de estos datos que genera esta clase de herramientas y sus usos son:

- Identificación de interfaces: las herramientas de monitoreo identifican las interfaces (llamadas puntos de seguimiento) para definir los parámetros para el aprovisionamiento de recursos de red y ayudar al IaC a generar el código relevante para invocar esas interfaces.
- Medición de la deriva: a pesar de utilizar IaC para implementar la infraestructura de red, Los cambios no autorizados o ad hoc en la configuración de la red pueden alterar los parámetros de rendimiento y seguridad para la ejecución de la aplicación (lo que se denomina deriva). Las herramientas de monitoreo deben tener la capacidad de monitorear estos parámetros de deriva (por ejemplo, disponibilidad de ancho de banda, tráfico no deseado) y alertar para tomar medidas correctivas.
- Diseños de superposición seguros para el acceso a servicios en la nube: las herramientas de monitoreo pueden generar datos para permitir que las herramientas de administración de red centralizada realicen funciones de seguridad, como la creación de una segmentación de red virtual sobre las funciones de segmentación de red nativas ofrecidas por CSP, siempre que haya API adecuadas disponibles. .
- Soporte a los procesos de respuesta a incidencias: Herramientas sofisticadas de monitorización de red generar alertas de seguridad de red y fuentes de inteligencia sobre amenazas. El manejo de estas alertas y feeds es parte del proceso de respuesta a incidencias (IR) en una empresa y lo llevan a cabo miembros de un centro de operaciones de seguridad (SOC). Una estrategia de seguridad que ha evolucionado en los últimos años para automatizar el proceso de IR se llama orquestación, automatización y respuesta de seguridad (SOAR). Algunas de las aplicaciones actuales de SOAR incluyen detección y respuesta a amenazas, priorización de vulnerabilidades, comprobaciones de cumplimiento y auditorías de seguridad con aplicaciones potenciales en muchas áreas emergentes, como la gestión de IoT [15].

3.4.2. Herramientas de aprovisionamiento de red automatizadas

Como ya se indicó, el aprovisionamiento automatizado de recursos de red está habilitado por herramientas de infraestructura como código (IaC). El código que describe la infraestructura de red (además de la infraestructura informática y de almacenamiento) se almacena en un repositorio de código. La implementación inicial de la infraestructura de red y la actualización posterior se automatizan mediante la definición de un flujo de trabajo que invoca el IaC (por ejemplo, flujo de trabajo GitOps) como parte de una definición de canalización de CI/CD [16]. Las ventajas de este enfoque para gestionar la infraestructura de red empresarial para la implementación de múltiples nubes son:

- Permite a la empresa tener un estricto control de versiones (seguimiento de cambios) para que Los dispositivos de red no autorizados y los cambios en las configuraciones asociadas no abren vulnerabilidades de seguridad.
- Permite a la empresa tener una infraestructura uniforme en todos los entornos. desarrollo, pruebas, puesta en escena y producción.
- Monitorear la deriva (los cambios no deseados) entre la infraestructura definida (como se encuentra en IaC) y la infraestructura operativa (medida por herramientas de monitoreo).

descrito en la Sección 3.4.1) y tomar medidas correctivas para abordar la desviación ayuda a mantener la postura de seguridad necesaria para el entorno de red empresarial.

- El paradigma DevSecOps que consta de canalizaciones de CI/CD invoca la red Herramienta de aprovisionamiento (generador de código IaC) para automatizar el despliegue inicial y la posterior reconfiguración de la infraestructura de red. Dado que las canalizaciones tienen un proceso de auditoría incorporado, los cambios en la configuración de la red se capturan automáticamente en la auditoría, lo que permite a la empresa demostrar el cumplimiento de la política de seguridad corporativa y el cumplimiento de la política regulatoria para sus redes, cuando corresponda.
- Probar el código (código IaC) generado por las herramientas IaC (e invocado por el código de canalización CI/CD que implementa la infraestructura usando IaC en el proceso DevSecOps) garantiza que las políticas de seguridad se apliquen de manera consistente y uniforme en toda la infraestructura de red empresarial (es decir, , múltiples servicios en la nube).
- La ventaja de tener complementos para definir el aprovisionamiento de red para diferentes entornos de proveedores de nube pública es que pueden usarse para personalizar las herramientas de observabilidad utilizadas para el monitoreo de red para cada uno de los servicios de nube a los que la empresa se ha suscrito [17].

3.5. Dispositivos de red como servicios

Otra tendencia en el panorama de las redes empresariales es que una parte de la infraestructura de la red se puede obtener de proveedores externos como un servicio arrendado llamado red como servicio (NaaS). Este servicio se ofrece utilizando tecnologías como 5G empresarial y computación de vanguardia. Las ventajas de NaaS son:

- Al igual que las suscripciones a SaaS e IaaS, reduce los costos de capital para la empresa.
- Es flexible y escalable ya que está definido por software y virtualizado.
- Como consecuencia de la ventaja anterior, los requisitos de calidad de servicio (QoS) de diversas aplicaciones se pueden cumplir creando un flujo de tráfico personalizado para cada tipo de aplicación [18].
- Se pueden introducir rápidamente nuevas aplicaciones que requieren una mayor huella de red. la empresa, facilitando así una ágil diversificación del negocio.

Sin embargo, son soluciones de seguridad puntuales limitadas en lugar de soluciones integrales que aborden todos los aspectos de la seguridad empresarial.

4. Configuraciones de red para funciones de seguridad básicas

Cualquier red segura a nivel empresarial que consta de aplicaciones locales y alojadas en la nube debe basarse en un marco de seguridad establecido. A su vez, los marcos de seguridad constan de muchas funciones de seguridad básicas. El propósito de esta sección es describir las configuraciones o diseños de red (y los intercambios de comunicación de red basados en ellos) que han surgido como el estado de la práctica para implementar estas funciones de seguridad. El estado de la práctica de las funciones de configuración de red (NCF) que se encuentran en empresas con entornos de aplicaciones híbridas se puede clasificar en las siguientes áreas [19]:

- Configuración de red para administración de dispositivos
- Configuración de red para autenticación de usuario
- Configuración de red para autenticación de dispositivos y monitoreo de estado
- Configuración de red para autorizar el acceso a aplicaciones/servicios
- Configuraciones de red para prevenir la escalada de ataques

Cada una de las funciones de configuración de red se enumera utilizando el identificador de la forma HAE-NCF-x, donde HAE indica un entorno de aplicación híbrido, NCF indica la función de configuración de red y x representa el número de secuencia de la función. Primero, considere el fundamento conceptual: información crítica que se utiliza como parte del despliegue de una funcionalidad de seguridad mediante una configuración de red.

4.1 Base conceptual: información contextual

La sección 2.4 analizó la limitación de utilizar únicamente la identidad del usuario para autorizar solicitudes de aplicaciones. Sin embargo, esto no significa que la verificación de identidad pueda quedar relegada a un requisito secundario. Se ha reconocido ampliamente que la validación de identidad es el punto de entrada (puede ser un punto de entrada altamente vulnerable al sistema) a una solicitud de aplicación [26] ya que todas las solicitudes, ya sean de un servicio (o microservicio), usuario o dispositivo: viene con una identidad reclamada. Esta identidad debe verificarse mediante una autenticación multifactor sólida y resistente al phishing.

Sin embargo, otros atributos asociados con el usuario y la información asociada con otras entidades involucradas en una solicitud de acceso a una aplicación, como dispositivos y servicios, son necesarios en los entornos de TI empresariales actuales y se denominan colectivamente información contextual. Este conjunto de información contextual puede variar de una empresa a otra y se basa en el nivel de confianza que la organización requiere para una solicitud de acceso particular. Dado que es posible que no se conozca el papel de la información contextual en posibles ataques, el conjunto que se incluirá en la decisión de acceso es una decisión basada en el riesgo. La información contextual puede pertenecer en términos generales a las siguientes cinco áreas clave [27]:

1. Información sobre el usuario que solicita acceso – Además de la identidad del usuario, atributos asociado con el usuario, como su rol en la organización, asignaciones actuales y estado (verificación cruzada de identidad en el sistema de gestión de identidad empresarial (IDM) vs directorio empresarial)

2. Información sobre el dispositivo desde el que se solicita el acceso: establecer confianza en el dispositivo a través de una combinación de perfiles de salud y riesgo del dispositivo. Por ejemplo, el perfil de riesgo del dispositivo se puede obtener mediante una verificación de postura lista para usar (riesgo del dispositivo [28]) con o sin integración con una herramienta de protección de punto final para el dispositivo. Otra información crucial (proporcionada por datos de telemetría) necesaria para evaluar el estado de seguridad de los dispositivos finales [29] incluye (a) etiqueta de soporte del dispositivo (el dispositivo es administrado o de propiedad corporativa) y (b) información de posición del dispositivo (si tiene sido comprometido). Todos estos factores entran en una evaluación de políticas para determinar el nivel de confianza y deben canalizarse en decisiones de autenticación y monitoreo [30].

3. Información sobre datos contextuales en tiempo real: fecha, hora y geolocalización en la que se realizó el se produce la solicitud de acceso

4. Información sobre los servicios de TI (p. ej., aplicaciones, datos) a los que se accede

5. Información sobre la seguridad del entorno que aloja los servicios de TI a los que se accede

Los requisitos para la información contextual [27]:

- Debe incluir no sólo lo que recopila la plataforma nativa (la plataforma en la que está alojada la aplicación) sino también lo que se puede obtener de plataformas de terceros y puede proporcionar información más detallada.

- Debe estar disponible en tiempo real para que la experiencia del usuario con el acceso no se vea afectada
- Se debe priorizar en función del valor que cada uno proporciona.
- Debe ser consistente con el nivel de riesgo asociado con cada solicitud de acceso.

Ningún acceso a aplicaciones y/o datos en el contexto de la red empresarial moderna puede considerarse seguro ignorando información contextual relevante cuando el escenario de acceso implica permitir a un usuario, dispositivo o servicio desde cualquier canal de red (por ejemplo, red corporativa, red doméstica, red pública). , o sucursal) para acceder a un recurso ubicado en cualquier lugar (local o en la nube).

4.2 Configuración de red para administración de dispositivos

Con la desaparición del perímetro de la red (Sección 2.1) y la distribución de los objetivos de las aplicaciones (al ser un entorno de aplicaciones híbrido), las empresas deberían adoptar un paradigma de "el punto final es el perímetro" y contar con un sistema de gestión de dispositivos.

HAE-NCF-1: Debe existir una solución de administración unificada de terminales (UEM) [48] para administrar y proteger todos los terminales que accederán a aplicaciones locales y basadas en la nube. Las tareas y capacidades mínimas gestionadas de UEM deben incluir:

a. Capacidad para admitir dispositivos terminales con diferentes sistemas operativos

b. Instalación y mantenimiento de certificados de autenticación de dispositivos y servicios.

C. Instalación y mantenimiento de aplicaciones de salud del dispositivo.

d. Actualizaciones de parches en los dispositivos.

mi. Permite a los administradores rastrear, auditar e informar puntos finales para contenido y aplicaciones.

4.3 Configuración de red para autenticación de usuario

HAE-NCF-2: Consistente con el memorando de la OMB M-22-09 [49], que describe la estrategia federal de arquitectura de confianza cero

a. La red debe configurarse para enrutar todas las solicitudes de acceso de los usuarios a todas las aplicaciones (en línea). locales y basados en la nube, como SaaS), a un IdP administrado por la empresa.

b. Se debe utilizar un mínimo de dos factores de autenticación para autenticar a los usuarios. El proceso de autenticación multifactor (MFA) empleado debe utilizar dispositivos resistentes al phishing. autenticadores. También denominados "verificadores resistentes a la suplantación de identidad", estos autenticadores deben cumplir con los requisitos del nivel AAL3 en la guía NIST SP 800-63-3 [50].

4.4 Configuración de red para autenticación de dispositivos y monitoreo de estado

HAE-NCF-3: la autenticación del dispositivo se puede realizar mediante la validación de certificados utilizando los protocolos adecuados. Una verificación del estado del dispositivo puede involucrar tanto su postura de seguridad (por ejemplo, la versión de un sistema operativo que está ejecutando, los parches que se han aplicado, el software de seguridad que está instalado) como información ambiental, como la geolocalización.

4.5 Configuración de red para autorizar el acceso a aplicaciones/servicios

HAE-NCF-4: Se deben utilizar protocolos estandarizados, como OAuth 2.0 [20], para emitir tokens de acceso al usuario, dispositivo o servicio validado para permitir el acceso a aplicaciones basadas en la nube.

HAE-NCF-5: La configuración de red para aplicaciones basadas en microservicios (locales o en la nube) debe incluir capacidades como descubrimiento de servicios, cifrado, autenticación de servicios, equilibrio de carga, observabilidad (visibilidad del tráfico de red en las capas 3-7), y lanzamientos canarios.
Además, se puede habilitar la visibilidad del comportamiento del tiempo de ejecución de los microservicios (y la capacidad de proporcionar controles de seguridad más dinámicos) adjuntando programas eBPF [52] a eventos de puntos de seguimiento (la entrada o salida de cualquier función en el kernel o el espacio de usuario).

4.6 Configuraciones de red para prevenir la escalada de ataques

Las configuraciones de red para la prevención de la escalada de ataques son técnicas utilizadas para implementar ZTNA y se analizan en la siguiente sección. Dos configuraciones establecidas son:

1. Microsegmentación
2. Perímetro definido por software (SDP)

5. Marco de seguridad de red para toda la empresa: acceso a la red de confianza cero (ZTNA)

Cada una de las configuraciones de red descritas en la sección anterior es para seguridad específica. funciones (por ejemplo, autenticación de usuario, autenticación de dispositivo). En muchos entornos empresariales, estas configuraciones de red no son implementaciones aisladas, sino más bien una parte integral de una red empresarial que se rige por un marco o estrategia de seguridad. Una estrategia predominante que ha sido respaldada tanto por el gobierno como por la industria para las empresas híbridas es la confianza cero (ZT). El modelo para lograr los objetivos de ZT es la arquitectura de confianza cero (ZTA), y el paradigma consiguiente para los flujos de comunicación de red es el acceso a la red de confianza cero (ZTNA). Al trabajar con muchas partes interesadas, el NIST ha definido la confianza cero y los principios de confianza cero de la siguiente manera [33]:

- Confianza cero (ZT) es el término para un conjunto en evolución de paradigmas de ciberseguridad que se mueven defensas desde perímetros estáticos basados en red para centrarse en usuarios, activos y recursos. Es un conjunto de primitivas de seguridad más que un conjunto particular de tecnologías. La confianza cero supone que no se otorga ninguna confianza implícita a los activos o cuentas de usuario basándose únicamente en su ubicación física o de red (es decir, redes de área local versus Internet) o en la propiedad de los activos (por ejemplo, de propiedad empresarial o personal). La confianza cero se centra en proteger los recursos (por ejemplo, activos, servicios, flujos de trabajo, cuentas de red) en lugar de segmentos de red, ya que la ubicación de la red ya no se considera el componente principal de la postura de seguridad del recurso.

- Una arquitectura de confianza cero (ZTA) utiliza principios de confianza cero para planificar actividades industriales y empresariales. infraestructura y flujos de trabajo.

La guía del NIST sobre confianza cero también contiene una definición abstracta de arquitectura de confianza cero (ZTA) y brinda modelos de implementación generales y casos de uso donde la confianza cero podría mejorar la postura general de seguridad de la tecnología de la información de una empresa. A partir de la visión del NIST de ZTA y las implementaciones del estado de la práctica [34], los siguientes han surgido como los tres pilares de ZTA:

1. Cliente o navegador: el punto de entrada para que todos los usuarios accedan a cualquier recurso alojado en entornos multinube y locales.
2. El Controlador: El punto de decisión de políticas (PDP), que evalúa las solicitudes de acceso en función de las políticas, condiciones y derechos que otorgan acceso a todos los usuarios, dispositivos y cargas de trabajo desde un único panel o mediante API.
3. La puerta de enlace: el punto de aplicación de políticas (PEP), una puerta de enlace que controla el flujo de acceso a los recursos protegidos y crea dinámicamente reglas de microsegmentación basadas en los derechos otorgados.

Como ya se indicó, las dos técnicas de configuración de red establecidas para habilitar ZTNA son microsegmentación y SDP, que se analizan en las siguientes subsecciones.

5.1 Microsegmentación

La microsegmentación es una práctica de diseño de seguridad en la que una red interna (por ejemplo, en el centro de datos, en la región del proveedor de la nube) se divide en segmentos aislados para que el tráfico que entra y sale de

cada segmento puede ser monitoreado y controlado [21]. El objetivo principal de la microsegmentación es proporcionar un grado de aislamiento para evitar la escalada de ataques.

Las capacidades habilitadas por la microsegmentación incluyen:

- El hecho de que los segmentos estén aislados y sean relativamente pequeños permite una estrecha vigilancia del tráfico. debido a una mejor visibilidad.
- La consecuencia de la capacidad anterior es que el control de acceso granular es posible mediante definir políticas asociadas.

Las capacidades anteriores restringen el movimiento lateral no autorizado de un usuario o aplicación que (a) ha traspasado el perímetro para ingresar a la red interna o (b) ha sido iniciado por usuarios dentro de la propia red interna.

5.1.1 Requisitos previos para implementar la microsegmentación

- Creación de identidad de la aplicación: El requisito fundamental para permitir esto es la asignación de una identidad única a cada aplicación o servicio, de la misma manera que cada usuario lleva una identidad única (por ejemplo, ID de usuario). Antes de la era de las aplicaciones basadas en la nube, las solicitudes de aplicaciones se validaban en función de la subred IP o la dirección IP desde la que se originaban. El acceso ubicuo y las múltiples nubes han eliminado el concepto de perímetros de red. Por lo tanto, la autenticación y autorización basadas en esos parámetros no son factibles ni escalables. Además, la presencia de servidores proxy, traducción de direcciones de red, infraestructura dinámica (por ejemplo, migración de aplicaciones entre máquinas virtuales) y balanceadores de carga hacen imposible que la aplicación llamada conozca la dirección IP de la aplicación que llama para poder tomar decisiones de autenticación o autorización. . Una identidad de aplicación única es inevitable.

- Establecimiento de confianza en la identidad de la aplicación: la aplicación creada (carga de trabajo o servicio) la identidad no debe estar sujeta a suplantación de identidad y debe ser verificable continuamente. Un ejemplo de identidad de carga de trabajo es un ID SPIFFE [47]. Un ID SPIFFE es una cadena que identifica de forma única y específica una carga de trabajo y está codificada como un identificador uniforme de recursos (URI). que toma el siguiente formato: spiffe:// dominio de confianza/identificador de carga de trabajo donde el identificador de carga de trabajo identifica de forma única una carga de trabajo específica dentro de un dominio de confianza. El ID de SPIFFE se lleva en un documento verificable criptográficamente llamado SVID (Documento de identidad verificable de SPIFFE). Los dos formatos admitidos para SVID en la especificación SPIFFE son un certificado X.509 de corta duración o un token Java Web Token (JWT).

- Descubrimiento de recursos de aplicaciones: debe haber un método seguro y sólido para descubrir todos los recursos de la aplicación (por ejemplo, servicios, redes), denominado capacidad de descubrimiento de servicios.
- Segmentación de cargas de trabajo: Se deben identificar los requisitos de seguridad para todas las aplicaciones y servicios y establecer agrupaciones basadas en requisitos de seguridad idénticos.
- Mapeo de agrupaciones lógicas de aplicaciones a infraestructuras físicas o virtuales: Las agrupaciones centradas en aplicaciones deben asignarse a infraestructuras físicas o virtuales que

constituyen la topología del centro de datos para facilitar la implementación real de aplicaciones y servicios.

5.1.2 Microsegmentación – Enfoques de implementación

Antes de discutir la microsegmentación, una discusión sobre una segmentación de red tradicional: denominado enfoque basado en segmentos, es para señalar sus limitaciones y dificultades. En este enfoque, las aplicaciones y recursos de servicio con requisitos de seguridad similares se agrupan en un segmento único y se crean reglas de firewall para bloquear o permitir la comunicación con cada grupo o segmento. Los segmentos se crean utilizando abstracciones de la capa de red, como ID de VLAN u otros enfoques de etiquetado, mientras que las políticas se definen utilizando construcciones de direcciones de red (por ejemplo, direcciones IP y puertos). Las políticas se aplican a subredes (por ejemplo, VLAN) y no a hosts individuales.
Cada segmento está protegido por dispositivos de puerta de enlace, como conmutadores y enrutadores inteligentes o firewalls de próxima generación (NGFW), que deben tener la capacidad de reaccionar y adaptarse en respuesta a las amenazas y cambios en los flujos de trabajo de las aplicaciones. Las puertas de enlace de segmentación monitorean el tráfico, detienen amenazas y aplican el acceso granular en el tráfico de este a oeste (rara vez para el tráfico de norte a sur) dentro de los centros de datos locales o regiones de nube. La principal dificultad con este enfoque es mapear los segmentos basados en requisitos de seguridad de las aplicaciones con los segmentos de red correspondientes [23]. Otra dificultad es la gestión del cambio. El mapeo entre aplicaciones e identidades de red que se mantienen estáticamente debe mantenerse continuamente sincronizado con el escenario operativo donde las ubicaciones de red de la aplicación cambian continuamente debido a razones de rendimiento y seguridad.

En la Figura 1 se muestra un diagrama esquemático de la microsegmentación basada en segmentos. Cada microsegmento numerado en la figura es una VLAN única identificada por una ID de VLAN. El grupo de aplicaciones que se ejecutarán en ese segmento de VLAN en particular se puede definir utilizando diferentes criterios, uno de los cuales es "todas las aplicaciones con requisitos de seguridad similares". Otro criterio es que “todos los niveles (front-end web, servidores lógicos de aplicaciones y servidores de bases de datos) asociados con una aplicación en particular” deben ejecutarse en un único microsegmento, como se muestra en la Figura 1.

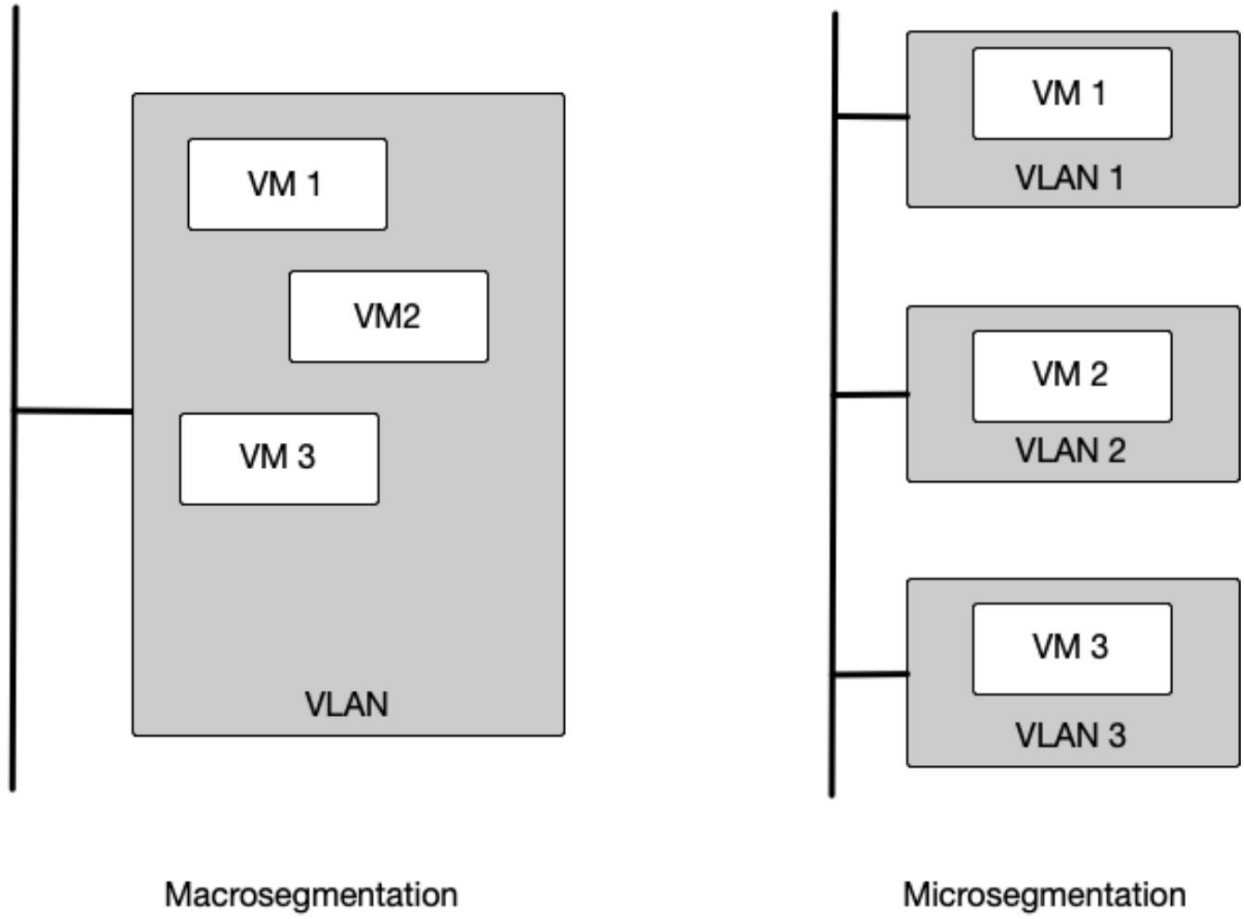

Fig. 1. Microsegmentación basada en segmentos

Los siguientes son algunos enfoques que se emplean para implementar la microsegmentación [22]:

a. Enfoque basado en servidor virtualizado : este enfoque solo es aplicable a redes que contienen servidores virtualizados, ya que está implementado en el hipervisor. Hay dos mecanismos posibles:

1. Usar firewalls virtuales dentro de un hipervisor para aislar el tráfico destinado a diferentes VM dentro del hipervisor
2. Usar técnicas de encapsulación para crear superposiciones (por ejemplo, LAN extensible virtual (VXLAN)) que se ejecutan sobre una red subyacente que consta de designaciones de direcciones IP; Las políticas de control de acceso se aplican en el propio hipervisor fuera de la carga de trabajo (aplicación o microservicio).

b. Microsegmentación basada en host: alternativa (o adicionalmente) basada en host
La microsegmentación se puede implementar utilizando agentes de software en los artefactos del punto final (por ejemplo, servidores). Aprovecha la funcionalidad de firewall nativa integrada en el host. Los agentes de software pueden superponer una red segmentada definida por software en centros de datos, entornos de nube, bare metal y híbridos. El agente proporciona conocimiento del contexto y visibilidad para cada carga de trabajo y permite la definición y aplicación de políticas detalladas.

C. Microsegmentación basada en identidad: uso de políticas de microsegmentación basada en identidad identificadores contextuales basados en aplicaciones (por ejemplo, el servicio front-end de procesamiento de pedidos puede comunicarse con el servicio back-end de inventario) en lugar de parámetros de red (permite llamadas desde la subred 192.168.10.x a 10.0.0.31) [24]. Los identificadores asignados a los servicios son identidades criptográficas (como se analiza en la Sección 5.1.1), que utilizan para la autenticación y autorización mutuas durante cada solicitud y respuesta de servicio.

Las ventajas de este tipo de microsegmentación son:

- Las políticas basadas en identidades de servicios/aplicaciones no utilizan ninguna información relacionada con la infraestructura. variables (por ejemplo, direcciones IP, subredes), por lo que estas políticas son independientes del entorno y brindan la libertad para que los servicios/aplicaciones se migren a diferentes entornos y aún mantengan las mismas políticas.
- El hecho de que las políticas sean independientes de la infraestructura permite probarlas simplemente ejercitar la aplicación y observar los resultados (por ejemplo, seguimiento de la secuencia de llamadas de servicio y solicitudes/respuestas en lugar de configurar la infraestructura correctamente para ejecuciones de prueba).
- Con la disponibilidad de herramientas para la especificación declarativa de políticas a través de herramientas de "política como código" (PaC), las políticas de microsegmentación se pueden definir e implementar incorporando el código en flujos de trabajo automatizados, como canales de CI/CD.
- La microsegmentación permite un control de acceso granular (especificado) al proporcionar visibilidad de las secuencias/interdependencias de llamadas de las aplicaciones y los flujos de datos a través del seguimiento a nivel de host, lo que permite aplicar políticas de seguridad para el tráfico de aplicaciones que es tanto de norte a sur como de este a oeste, independientemente del entorno (por ejemplo, centro de datos corporativo o infraestructura de nube).

La razón por la que la microsegmentación basada en identidad debe incluirse en el panorama de la red empresarial es que solo permite el tráfico de red válido entre los diversos servicios componentes de la aplicación debido a la autenticación y autorización mutuas de las identidades del servicio, permitiendo así los objetivos de ZTNA. cumplirse [25].

5.2 Perímetro definido por software (SDP)

Un fundamento conceptual para el acceso seguro a la red a los recursos de TI es el perímetro definido por software (SDP) [31]. En SDP, la separación entre redes no está definida por el grupo de direcciones de red o las VLAN, lo que la hace independiente de la red. Está definido de forma lógica y dinámica para cada usuario y cada solicitud en particular. En otras palabras, para cada solicitud de usuario, el subconjunto de recursos de TI al que el usuario tiene acceso se asigna dinámicamente independientemente de la ubicación del recurso (por ejemplo, centro de datos corporativo, sucursal, nube pública o privada). Los principios destacados del SDP incluyen:

- El concepto de SDP implica hacer invisibles todos los recursos de TI (por ejemplo, puertos, cargas de trabajo y aplicaciones) y hacerlos conocidos y accesibles sólo después de que el usuario esté autenticado y autorizado. Solo se establece una conexión de red entre el usuario y los recursos de TI permitidos, siguiendo así el principio de privilegio mínimo.

- El nivel de acceso determinado por el proceso anterior se reevalúa continuamente durante la sesión del usuario y se recalibra si es necesario. A medida que el contexto que rodea la identidad cambia en tiempo real, también pueden cambiar los derechos del usuario [31].
- La superficie de ataque se reduce evitando el movimiento lateral [32] mediante técnicas como la microsegmentación, como se describe en la Sección 5.1. Con el creciente despliegue de microservicios, las solicitudes de recursos entre servicios (generador de tráfico este-oeste) dominan las solicitudes de aplicaciones externas (tráfico norte-sur). La aplicación de este principio garantiza así el tráfico de este a oeste.

En todos los marcos de seguridad para los entornos de redes empresariales actuales, los principios comunes que subyacen a los requisitos específicos de las aplicaciones, como baja latencia, altas tasas de transferencia de datos, y alta confiabilidad, que eran aplicables en entornos de red anteriores, siguen siendo los mismos.

6. Infraestructura de red de área amplia segura para una red empresarial

La red de área amplia (WAN) se convirtió en una parte integral de la red empresarial cuando las organizaciones necesitaron conectar sus redes de área local (LAN) en múltiples ubicaciones geográficamente distribuidas (dentro del país y, en algunos casos, globalmente) a partir de la década de 1980. La tecnología WAN inicial implicaba líneas arrendadas punto a punto (P2P) seguidas de retransmisión de tramas. La primera red basada en IP fue la conmutación de etiquetas multiprotocolo (MPLS), que permitía que múltiples tipos de tráfico (como voz, vídeo y datos) viajaran en la misma línea.

Con la llegada de tecnologías como la virtualización y el aumento del acceso empresarial a los servicios en la nube, las empresas han comenzado a adoptar una nueva tecnología WAN llamada red de área amplia definida por software (SD-WAN). La tecnología SD-WAN elimina el estrecho acoplamiento entre las funciones del plano de control y del plano de datos de la red y permite la especificación centralizada de varias políticas, como control de acceso, enrutamiento y priorización del tráfico de aplicaciones.

Otro desarrollo integra todas las soluciones de seguridad puntuales proporcionadas por varios dispositivos de seguridad de red (Sección 3) en una infraestructura de servicios de seguridad de red. La industria y los consorcios industriales utilizan el término borde de servicio de acceso seguro (SASE) [35] para referirse a un marco integral que ofrece redes de área amplia y diversos servicios de seguridad. SASE puede considerarse como la contraparte de red de la malla de servicios de la aplicación, que proporciona un conjunto integral de servicios de aplicaciones, incluida la seguridad para aplicaciones nativas de la nube.

Con base en la discusión anterior, esta sección se centrará en los siguientes temas:

- Requisitos para una SD-WAN segura
- Requisitos específicos para SD-WAN para acceso a la nube
- Requisitos para una arquitectura de servicios de seguridad integrada para SD-WAN

6.1. Requisitos comunes para una SD-WAN segura

Además de las VPN proporcionadas por CSP, una tecnología de red que proporciona conectividad de red para acceder a servicios basados en la nube para empresas es la red de área amplia definida por software (SD-WAN).

Los objetivos de diseño y las características comunes de todas las ofertas de SD-WAN incluyen:

- Amplia conectividad: para conectar de forma segura a los usuarios ubicados en cualquier lugar (p. ej., hogar, ubicación pública, sucursal, oficina corporativa) a aplicaciones y recursos alojados en cualquier lugar (p. ej., centro de datos, servicios de nube únicos o múltiples) utilizando cualquier transporte WAN (p. ej., MPLS). , Internet de banda ancha, 4G/LTE, 5G inalámbrico)
- Conocimiento de la aplicación: para monitorear el tráfico de la red y elegir dinámicamente la mejor ruta disponible en función de (a) el tipo de tráfico de la red, (b) las condiciones de carga de la red y (c) la prioridad comercial de la aplicación. Esta capacidad se habilita mediante técnicas como la utilización del ancho de banda, el equilibrio de carga y la optimización de la velocidad al reducir las fluctuaciones, la latencia y la pérdida de paquetes. Abordar la prioridad empresarial de una aplicación solo es posible si la solución SD-WAN tiene la capacidad de identificar diferentes tipos de aplicaciones (por ejemplo, aplicaciones de mensajería/correo electrónico, aplicaciones de redes sociales, aplicaciones generales relacionadas con el almacenamiento).

aplicaciones, aplicaciones de cadena de suministro) y asignar prioridades de enrutamiento y recursos WAN en consecuencia.

- Integración de funciones de seguridad y redes: uso de dispositivos que contienen un combinación de funciones de red y seguridad (por ejemplo, la presencia de un firewall y funciones de puerta de enlace web segura [SWG] en un enrutador WAN) [36]
- Capacidades centralizadas de visibilidad y administración: incluye la capacidad de reconocer y autenticar dispositivos recién conectados y colocarlos bajo los flujos de trabajo de administración definidos como nodos para configurar un conjunto uniforme de políticas que cubra todos los componentes.
- Integración con ubicaciones LAN remotas: una característica adicional preferida pero no esencial es la integración de funciones WAN y LAN en un solo dispositivo (este último recibe el nombre de SD-Branch), que se puede administrar mediante una única consola de administración, de esta manera proporcionando una mejor visibilidad de ambos componentes. Esta característica permite la conectividad de SD-WAN a la LAN local en las sucursales remotas.

6.2. Requisitos específicos para SD-WAN para acceso a la nube

Las empresas pueden obtener acceso a la nube de dos maneras: 1) a través de los servicios VPN proporcionados por los proveedores de la nube o 2) integrando su propia SD-WAN con las redes privadas de los proveedores de la nube, a menudo denominadas WAN en la nube. En ambos escenarios, es posible que las empresas apliquen sus políticas de seguridad y redes empresariales incluso aunque los recursos de los terminales estén ubicados en la red privada de un proveedor de nube.

- En el primer escenario, el acceso a la nube está habilitado por la disponibilidad de la función proporcionada por muchos CSP para que cada suscriptor establezca sus propias subredes privadas y una conexión de red entre dos de esas subredes privadas (por ejemplo, emparejamiento de VPC). Entonces es posible que los recursos (por ejemplo, instancias de VM) en cualquiera de las subredes privadas se comuniquen entre sí como si estuvieran dentro de la misma red.
- En el segundo escenario (es decir, conectividad a través de SD-WAN), se puede aprovechar la misma función una vez dentro de la red CSP. Además, se puede lograr una mayor orquestación de la red privada del proveedor de la nube diseñando una red superpuesta personalizada sobre la red del proveedor de la nube con esta última como red subyacente. Esta característica depende de que los CSP ofrezcan integraciones de API para diferentes ofertas de SD-WAN [38][39][40].

Las ventajas generales de poder orquestar la red privada de CSP para la empresa suscriptora son:

- Visibilidad completa de extremo a extremo entre el “punto final de acceso” y el recurso de TI punto final (aplicación o datos) aunque este último esté ubicado en la red de un proveedor de nube
- Aplicación de la lógica de segmentación de red implementada para acceder a las instalaciones recursos a los recursos basados en la nube [37]

Ha surgido una arquitectura para gestionar redes empresariales que están conectadas a múltiples CSP. Una parte de la industria llama al conjunto de dispositivos de esta arquitectura una plataforma de red en la nube. Los requisitos para esta plataforma de redes multinube son [41]:

- Debería ofrecer visibilidad operativa común y control a través del acceso a la red nativa proporcionado por múltiples proveedores de nube. El principal desafío es que los proveedores de nube pública tienen diferentes arquitecturas propietarias que utilizan sus propias "construcciones". Para proporcionar una arquitectura de red que pueda “cruzar nubes”, es necesario aprovechar la funcionalidad nativa de la nube (especialmente las construcciones de red nativas de la nube) de cada nube; abstraer esa funcionalidad con API; agregue características avanzadas del plano de datos para alta disponibilidad, seguridad y visibilidad/control operativo; y proporcionar las herramientas para gestionar estas funciones de forma dinámica o automática [42].

- Debería ofrecer una política de seguridad común de entrada y salida para entornos de aplicaciones (por ejemplo, VPC, VNET, VCN) en todas las nubes.

- Debería permitir el cifrado de extremo a extremo dentro de la nube, así como un alto rendimiento. cifrado desde el centro de datos a la nube.

- Debe admitir la automatización para la implementación y configuración.

Con base en los requisitos anteriores, han surgido ofertas de plataformas de redes multinube con los siguientes elementos arquitectónicos:

- Una capa de abstracción se sitúa encima del acceso a la red nativa que ofrecen los CSP individuales. a sus servicios. Esta capa permite a la empresa gestionar toda la red empresarial (que consta de conectividad a múltiples nubes, conexiones dentro de la nube y estructuras de red del centro de datos local) como una sola unidad. Para permitir esto, se necesita una visibilidad completa de todo el panorama de la red empresarial. Por lo tanto, esta capa necesita el aporte de sofisticadas herramientas de observabilidad y monitoreo para llevar a cabo sus funciones.

- Una configuración de red virtual que se ubica en la parte superior de la red proporcionada por cada CSP para alojar aplicaciones CSC. La capacidad de definir esta configuración de red virtual se puede automatizar mediante una clase de herramientas llamadas herramientas IaC, que tienen características con definiciones de configuración de red de los principales CSP integradas como complementos. Estas herramientas facilitan el aprovisionamiento y la configuración inicial de recursos de red y el posterior reaprovisionamiento y reconfiguración a medida que cambian los requisitos de acceso a las aplicaciones.

Hay cuatro tendencias de la industria [43] que pueden tener implicaciones de seguridad con respecto a SD-WAN [44]:

1. El acceso SD-WAN se adquiere como un servicio basado en la nube bajo el paraguas de red como servicio (NaaS), al igual que IaaS y SaaS.
2. Los algoritmos basados en inteligencia artificial (IA) se utilizan para monitorear redes para condiciones relacionadas con la seguridad; para medidas que mejoren la resiliencia, como la limitación de ciertos destinos; y para decisiones de enrutamiento dinámico para mantener los parámetros de QoS, como la latencia y el ancho de banda.
3. Las redes inalámbricas se utilizan para la conectividad de última milla mediante una red de acceso de radio 5G. (CORRIÓ).

4. Las funcionalidades de acceso remoto seguro proporcionadas por tecnologías como VPN se combinan en SD-WAN [45].

6.3. Requisitos para una arquitectura de servicios de seguridad integrada para SD-WAN

Una arquitectura de servicios de seguridad integrada para SD-WAN tiene funciones de seguridad y de red integradas. Las capacidades de la función de seguridad y acceso a la red se ofrecen como un servicio en la nube al que las empresas pueden acceder a través de ubicaciones de red estratégicas distribuidas en una amplia área llamada punto de presencia (PoP). En 2019, Gartner acuñó el término "borde del servicio de acceso seguro" (SASE) para denotar una arquitectura que converge funciones de red y seguridad y las ofrece a escala global como un servicio en la nube [46]. Los servicios de redes y seguridad que ofrece un SASE no son nuevos, sino que simplemente se entregan juntos como un paquete único en lugar de

a través de soluciones puntuales de seguridad (Sección 3). Los diversos puntos de conectividad de la empresa a los PoP de SASE se denominan bordes empresariales. Las ventajas empresariales pueden ser:

- Clientes: usuarios que acceden a través de computadoras de escritorio, portátiles y dispositivos móviles desde sucursales o ubicaciones remotas, como sus hogares o IoT.
- Recursos de TI: aplicaciones internas alojadas en centros de datos, sucursales o la nube (p. ej., SaaS, IaaS)

La infraestructura de red SASE se convierte así en una parte integral de la red empresarial siempre que uno o más de los bordes de la empresa estén conectados a varios PoP de los servicios en la nube de SASE.

Las cuatro funciones principales entregadas por SASE son [46]:

1. Optimización del tráfico de red para diferentes tipos de tráfico: reducir la latencia y mejorar la disponibilidad
2. Control de acceso para diferentes tipos de recursos de TI: aplicaciones o bases de datos en diferentes dominios administrativos (por ejemplo, SaaS suscrito, web abierta)
3. Prevención de amenazas: monitorear, recopilar información sobre amenazas y ataques, y realizar acción correctiva
4. Permite la aplicación de una política de seguridad uniforme para todos los usuarios, independientemente de su ubicación; centraliza la visibilidad de prácticamente todos los usuarios y dispositivos en un único panel; aumenta la seguridad a medida que la organización se expande; y reduce la cantidad de dispositivos de seguridad física que administran [12]

Algunas de las características estructurales de las ofertas de SASE son:

- Punto de presencia (PoP) distribuido globalmente: un servicio SD-WAN global con su propio Red troncal privada que consta de puntos de presencia (PoP) en todo el mundo destinados a minimizar los problemas de latencia. En algunos casos, también se pueden aprovechar los PoP de los principales proveedores de nube.

- Agente de seguridad en los dispositivos: el agente de seguridad en el dispositivo del usuario final se encarga decisiones de red y dirige el tráfico desde diferentes aplicaciones. Capacidades específicas incluyen permitir o denegar dinámicamente conexiones a servicios y aplicaciones según las reglas comerciales definidas por una organización.

Los siguientes son los servicios de seguridad mínimos que se encuentran en la mayoría de las ofertas comerciales de SASE:

- Servicios de cortafuegos
- Servicios de puerta de enlace web segura
- Servicios antimalware
- Servicios IPS
- Servicios CASB
- Servicios de DLP

Algunas de las funciones de seguridad avanzadas que se encuentran en las ofertas de SASE incluyen:

- Tecnología de aislamiento del navegador: a menudo se combina con soluciones de puerta de enlace web segura y proporciona una seguridad mejorada de la actividad web para hacer frente a las amenazas en tiempo real.
- Estrategia de evaluación de confianza y riesgo adaptativo continuo (CARTA): esta estrategia implica monitorear constantemente las sesiones y realizar análisis de comportamiento adaptativo en los parámetros de monitoreo para cambiar dinámicamente los niveles de seguridad y permisos si el perfil de confianza (por ejemplo, déficit de confianza) de un dispositivo cambia.

7. Resumen y conclusiones

El objetivo de este documento es proporcionar información sobre el panorama actual de la red empresarial en términos de topología, flujos de tráfico y amenazas a la seguridad. Plantea que los cambios en la arquitectura y las tecnologías de las aplicaciones (p. ej., monolíticas a microservicios, bare metal a virtualización/contenedores) y el aumento de suscripciones a diversos tipos de servicios en la nube (p. ej., IaaS, SaaS) son impulsores del estado actual de las redes empresariales. .

Este documento describe las limitaciones de las suposiciones y tecnologías de seguridad de acceso a la red existentes debido a los cambios en las topologías de red en las redes empresariales modernas. La aparición de nuevos dispositivos de red (p. ej., CASB), funciones mejoradas en dispositivos existentes (p. ej., firewalls), herramientas de automatización de red para recopilar datos para visibilidad/monitoreo, detección de amenazas y acciones correctivas, y herramientas para el aprovisionamiento automatizado de redes para diferentes CSP públicos. Los entornos (habilitados por herramientas IaC invocadas como parte de los flujos de trabajo inteligentes llamados canalizaciones CI/CD definidos bajo el paradigma DevSecOps) se analizan en soluciones de seguridad puntuales. A esto le sigue una discusión de varias configuraciones de red, cada una de las cuales implementa una función de seguridad específica (por ejemplo, autenticación de usuario, autenticación de dispositivo). Se dedica una sección separada a analizar las características más destacadas de un marco de seguridad en evolución para una red empresarial llamada ZTNA, así como las dos configuraciones de red predominantes (es decir, microsegmentación y SDP) para evitar la escalada de ataques para cumplir uno de los objetivos de ZTNA.

Finalmente, este documento analiza las últimas tecnologías WAN que forman parte del panorama actual de redes empresariales, así como las características de las ofertas de WAN con PoP global y servicios de seguridad integrados llamados SASE.

Referencias

[1] Craven C (2019) ¿Cuál es la diferencia entre Edge Computing y MEC? Disponible en https://www.sdxcentral.com/edge/definitions/whats-the-difference-between-edge-computer-and-mec/

[2] The Monitor Número 13 (2020) Vulnerabilidades de VPN vinculadas al aumento de la exposición de datos, Secuestro de datos. Disponible en https://www.kroll.com/en/insights/publications/cyber/monitor/vpn-vulnerabilities-rising-data-exposure-ransomware

[3] Hardcastle JL (2018) Por qué CASB es la categoría de seguridad de más rápido crecimiento. Disponible en https://www.sdxcentral.com/articles/news/casb-fastest-growing-security-category-ever/2018/02/

[4] Proofpoint (2021) Introducción a CASB. Disponible en https://www.proofpoint.com/us/resources/white-papers/getting-started-with-casb

[5] Lookout (2021) Adoptando la confianza cero: una guía para que las agencias aborden la orden ejecutiva de ciberseguridad. Disponible en https://www.govexec.com/media/embracing-zero-trust-guide-agencies-address-cybersecurity-executive-order.pdf

[6] Cato Networks (2022) Firewall de red: componentes, tipos de soluciones y tendencias futuras. Disponible en https://www.catonetworks.com/network-firewall/

[7] Palo Alto Networks (2022) Filtrado de URL avanzado. Disponible en https://www.paloaltonetworks.com/network-security/advanced-url-filtering

[8] Oswal A (2022) Cloud NGFW: servicio de firewall administrado de próxima generación para AWS. Disponible en https://www.paloaltonetworks.com/blog/2022/03/next-generation-firewall-service-for-aws/

[9] Cato Networks (2022) Seguridad del firewall: comprensión de sus opciones. Disponible en https://www.catonetworks.com/network-firewall/firewall-security/

[10] F5 Networks (2022) Guía de compra de WAAP. Disponible en https://media.bitpipe.com/io_15x/io_158522/item_2439191/EBOOK-SEC-798086545-waap-guia-de-compra_FNL%20%281%29.pdf

[11] F5 Networks (2022) Elija el WAF adecuado para usted. Disponible en https://media.bitpipe.com/io_15x/io_158522/item_2439191/EBOOK-SEC-798087620-cual-waf-es-adecuado-para-usted-refresh-FNL%20%281%29.pdf

[12] AT&T (2020) La guía esencial para proteger la puerta de enlace web. Disponible en https://cybersecurity.att.com/resource-center/white-papers/essential-guide-to-secure-web-gateway

[13] Itential (2020) Redefiniendo la gestión de la configuración de la red. Disponible en https://www.itential.com/resource/ebook/redefining-network-configuration-compliance-cross-hybrid-infrastructure/

[14] McGillicuddy S (2022) Adoptar un enfoque estratégico para las operaciones de red. Disponible en https://media.bitpipe.com/io_16x/io_161947/item_2553630/NBT002b_NetBrain-WP_Final%20%281%29.pdf

[15] Palo Alto Networks (2020) Informe sobre el estado de SOAR, 2020. Disponible en https://media.bitpipe.com/io_15x/io_154375/item_2268964/the-state-of-soar-report-2020.pdf

[16] Aviatrix (2021) Guía de DevOps para redes multinube. Disponible en https://media.bitpipe.com/io_15x/io_158772/item_2444655/devops-guide-to-multi-cloud-networking%20%281%29.pdf.

[17] Itential (2021) Automatización de redes multinube. Disponible en https://www.itential.com/solutions/automation-use-cases/multi-cloud-network-automation/#:~:text=Automating%20Multi%2DCloud%20Networking&text=By%20leveraging%20the%20right%20automation,automatiza%20the%20Network%20of%20Clouds

[18] Verizon (2021) El futuro de las redes está aquí. Disponible en https://media.erepublic.com/document/Network-as-a-Service_Solution_Brief.pdf

[19] Miller LC (2021) Seguridad en centros de datos y nube híbrida – Libro electrónico. https://www.paloaltonetworks.com/resources/ebooks/data-center-and-hybrid-cloud-security-for-dummies

[20] Vertocci B (2021) Perfil de token web JSON (JWT) para tokens de acceso OAuth 2.0. (Grupo de trabajo de red del Grupo de trabajo de ingeniería de Internet (IETF), Solicitud de comentarios (RFC) 9068 del IETF. https://datatracker.ietf.org/doc/html/rfc9068

[21] ColorTokens (2022) ¿ Qué es la microsegmentación? Disponible en https://colortokens.com/micro-segmentation/

[22] Mandal A (2020) Microsegmentación: la arquitectura por excelencia para Zero Trust. Disponible en https://medium.com/@anandadip/microsegmentation-the-quintessential-architecture-for-zero-trust-344715990c8e

[23] Kollimarla S (2021) Cómo funciona la microsegmentación para centros de datos. Disponible en https://colortokens.com/blog/data-center-micro-segmentation/

[24] Palo Alto Networks (2021) Microsegmentación basada en identidades de Prisma Cloud. Disponible en https://media.bitpipe.com/io_15x/io_157597/item_2439737/prisma-cloud-identity-based-microsegmentation.pdf

[25] Slattery T (2022) Cómo implementar la segmentación de red para una mejor seguridad. Disponible en https://www.techtarget.com/searchnetworking/tip/How-to-implement-network-segmentation-for-better-security

[26] Frazier S (2021) Por qué el EO cibernético hizo que la confianza cero ya no sea una sugerencia. Disponible en https://federalnewsnetwork.com/federal-insights/2021/09/why-the-cyber-eo-made-zero-trust-no-longer-a-suggestion/

[27] Brasen S (2020) Conciencia contextual: avance de la gestión de identidades y acceso al siguiente nivel de eficacia de la seguridad. Disponible en https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/advancing-identity-access-management-to-next-level-security- Effectiveness-pdf-7-w-7727.pdf

[28] Appgate (2020) SDP y dispositivos riesgosos. Disponible en https://www.appgate.com/blog/sdp-and-risky-devices-dynamic-controls-for-secure-access

[29] Srinivas S (2020) democratizando la confianza cero con una alianza BeyondCorp ampliada. Disponible en https://cloud.google.com/blog/products/identity-security/google-cloud-announces-new-partners-in-its-beyondcorp-alliance

[30] Tanium (2021) Tanium Insights: Es hora de deshacerse de la VPN por Zero Trust. Disponible en https://site.tanium.com/rs/790-QFJ-925/images/EB-ZeroTrust.pdf

[31] Scheels C (2021) VPN VS. ZTNA VS. SDP VS. NAC: ¿Cuál es la diferencia? Disponible en https://www.appgate.com/blog/vpn-vs-ztna-vs-sdp-vs-nac

[32] QTS (2020) Impulsando la innovación del centro de datos con microservicios. Disponible en https://media.bitpipe.com/io_15x/io_155464/item_2314862/QTS_Whitepaper_SDP.pdf

[33] Rose S, Borchert O, Mitchell S, Connelly S (2020) Arquitectura de confianza cero. (Instituto Nacional de Estándares y Tecnología, Gaithersburg, MD), Publicación especial (SP) NIST NIST SP 800-207. https://doi.org/10.6028/NIST.SP.800-207

[34] Appgate (2021) 5 pasos para una migración exitosa de VPN a ZTNA. Disponible en https://d3aafpiipsak2t.cloudfront.net/docs/VPN_to_ZTNA_migration_ebook-6.pdf

[35] Shread P (2020) ¿ Qué es SASE y cómo funciona? Disponible en https://www.esecurityplanet.com/networks/sase/

[36] Fortinet (2022) Capacidades necesarias para una SD-WAN eficaz y segura: la red Guía del líder. Disponible en https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/eBooks/eb-network-leaders-guide-to-secure-SD-WAN.pdf.

[37] Mann T (2021) AWS Cloud WAN evita a Google y Microsoft. Disponible en https://www.sdxcentral.com/articles/news/aws-cloud-wan-parries-google-microsoft/2021/12/

[38] Mann T (2021) ¿Es el destino final de la SD-WAN multinube? Disponible en https://www.sdxcentral.com/articles/news/is-multi-cloud-sd-wans-final-destination/2021/12/

[39] Mann T (2021) Google Cloud impulsa SD-Underlays en Cisco SD-Wan. Disponible en https://www.sdxcentral.com/articles/news/google-cloud-drives-sd-underlays-into-cisco-sd-wan/2021/03/

[40] Mann T (2021) Fortinet fortalece Microsoft Azure vWAN con firewalls SD-WAN. Disponible en https://www.sdxcentral.com/articles/news/fortinet-fortifies-microsoft-azure-vwan-with-sd-wan-firewalls/2021/11/

[41] Aviatrix (2021) La guía del arquitecto de seguridad para redes multinube. Disponible en https://media.bitpipe.com/io_15x/io_158772/item_2444655/security-architects-guide-multi-cloud-networking-v2%20%281%29.pdf

[42] Aviatrix (2020) Redes multinube. Disponible en https://aviatrix.com/wp-content/uploads/2020/07/Multi-Cloud-Networking-by-Futuriom-July2020.pdf

[43] Robb D (2022) Principales tendencias SD-WAN definidas por software. Disponible en https://www.enterprisestorageforum.com/networking/sd-wan-trends/

[44] TechTarget (2022) 4 tendencias clave de SD-WAN a seguir en 2022. Disponible en https://media.bitpipe.com/io_14x/io_148038/item_2494980/4%20key%20SD-WAN%20trends%20to%20watch%20in%202022.pdf

[45] Doyle L (2020) Los pros y los contras de SD-WAN y el acceso remoto. Disponible en https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-SD-WAN-and-acceso remoto

[46] Cato Networks (2021) Cinco preguntas para hacerle a su proveedor SASE. Disponible en https://go.catonetworks.com/rs/245-RJK-441/images/5_Questions_to_Ask_Your_SASE_Provider.pdf

[47] Spiffe.io (2021) Conceptos SPIFFE. Disponible en https://spiffe.io/docs/latest/spiffe-about/spiffe-concepts/#trust-bundle

[48] Vmware (2022) ¿Qué es la gestión unificada de terminales (UEM)? Disponible en https://www.vmware.com/topics/glossary/content/unified-endpoint-management.html

[49] Oficina de Gestión y Presupuesto (2022) Moviendo al gobierno de EE. UU. hacia principios de ciberseguridad de confianza cero. (La Casa Blanca, Washington, DC), Memorando de la OMB M-22-09, 26 de enero de 2022. Disponible en https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09 .pdf

[50] Grassi PA, García ME, Fenton JL (2020) Directrices de identidad digital. (Instituto Nacional de Estándares y Tecnología, Gaithersburg, MD), Publicación especial (SP) NIST NIST SP 800-63-3. https://doi.org/10.6028/NIST.SP.800-63-3

[51] Agencia de Seguridad de Infraestructura y Ciberseguridad (2022) Conexiones de Internet confiables 3.0 – Caso de uso de la nube. Disponible en https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Cloud%20Utilice%20Case%20Draft_0.pdf

[52] eBPF (2022) ¿Qué es eBPF? El panorama del proyecto. Disponible en https://ebpf.io/

[53] sdxcentral (2022) ¿Sobrevivirán las VPN a la revolución ZTNA y SASE? Disponible en https://www.sdxcentral.com/articles/analysis/will-vpns-survive-the-ztna-sase-revolution/2022/09/