Ciberseguridad en la implementación de SD-WAN

Madelaine Nelly Velasquez Blacutt
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
madevelb@gmail.com

***Resumen*—La implementación de redes definidas por software en áreas amplias (SD-WAN) se ha expandido a medida que las empresas necesitan el establecimiento de comunicaciones entre sus sucursales. La tecnología SD-WAN ofrece automatización de procesos y una arquitectura característica para brindar un servicio garantizado a aplicaciones finales de la empresa. Con el desarrollo de SD-WAN, también ha crecido la superficie de ataque que podría vulnerarse, exponiendo información sensible de las empresas, de esta forma, estrategias de ciberseguridad deben ser tomadas en cuenta, relacionando los posibles vectores de ataque a los componentes de la arquitectura SD-WAN. Este artículo pretende recomendar acciones para proteger una arquitectura SD-WAN en sus distintas capas.**

Palabras clave—SDN, SD-WAN, ciberseguridad, red de datos.

I. Introducción

La tecnología de red definida por software o SDN (del inglés *Software Defined Network*) aparece en el mercado como una solución a la necesidad de desplegar redes confiables, flexibles, con control centralizado y monitoreo [1]. Como una aplicación específica para redes de área amplia o WAN (del inglés *Wide Area Network*), SD-WAN o *Software Defined WAN* es ofrecida por distintos fabricantes como solución a los desafíos presentados en redes WAN [2].

Los negocios al tener un crecimiento constante de usuarios y sucursales, que deben ser comunicadas para el consumo de servicios en distintas locaciones, incrementa el número de dispositivos de red que deben ser configurados y administrados. Para esto, la arquitectura de red debe ser flexible a cambios y ofrecer una gestión centralizada, de forma que los equipos adopten cambios rápidamente como crecimiento de ancho de banda y optimización de los canales [3].

El presente trabajo presenta la arquitectura de la tecnología SD-WAN para el análisis de la superficie de ataques en los distintos componentes y capas, de forma que se generen recomendaciones para la implementación tomando en cuenta aspectos de ciberseguridad, para el aseguramiento de datos que usa la red WAN.

II. Software Defined Wan (SD-WAN)

A. Definición y componentes.

Cada componente de la arquitectura de SD-WAN puede contar con su propia infraestructura, dependiendo el fabricante que ofrece la solución, utilizando software libre o software propietario. Entre los componentes principales de la implementación se cuenta con los siguientes:

- Virtualización
- Servicios de red: procesamiento de paquetes, proxy, enrutamiento, plano de datos.
- Administración de servicios: base de datos, intercambio de mensajes, servidores web, servidores de aplicación web, monitoreo de recursos.
- Servicios de seguridad: cifrado, firewall, WAF, IDS, IPS, filtrado y clasificación, antivirus, seguridad DNS
- Software de sistema: sistema operativo.

B. Arquitectura de SD-WAN.

La tecnología SD-WAN busca simplificar las operaciones en redes WAN, optimizando la gestión e incluyendo flexibilidad. Se estudia la arquitectura desde los puntos de vista lógico y físico, describiendo los componentes y capas [4]. SD-WAN separa en plano de control y plano de datos el tráfico que maneja para lograr centralizar la gestión de los dispositivos.

1) Arquitectura lógica

Se consideran tres capas en SD-WAN definidas como capa de datos, capa de control y capa de aplicación, como se muestra en la Figura 1.

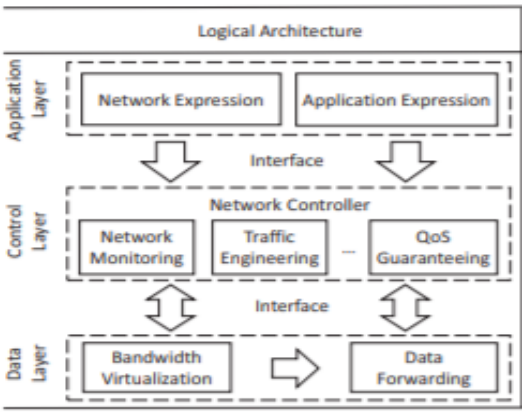

Fig. 1. Arquitectura lógica de SD-WAN [5]

En la capa de datos, se realizan funciones como reenvío de datos y virtualización del ancho de banda. La virtualización del ancho de banda combina diferentes enlaces para un lugar, disponiendo de una reserva de ancho de banda a ser distribuido entre las aplicaciones. El reenvío de datos consiste en la distribución de datos a través de dispositivos de red, usando el ancho de banda proporcionado. El plano de datos funciona solo según las instrucciones de la capa superior de control.

Para referenciar este artículo (IEEE):

[N] M. Velasquez, «Ciberseguridad en la implementación de SD-WAN», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 124-127, 2020.

En la capa de control, se presentan las funciones implementadas y administradas independientemente, para que los operadores de red puedan modificar, desarrollar y revisar cada una de ellas. Las funciones pueden ser conectadas para trabajar juntas e incrementar la flexibilidad de la red WAN, de esta forma se garantiza la calidad de servicio (QoS, *quality of service*) para aplicaciones que así lo requieren.

En capa de aplicación, se da la posibilidad de definir los requerimientos específicos para la red y aplicaciones. Es posible declarar estos requerimientos en alto nivel, de forma que la solución realice la traducción de estos requerimientos a configuraciones de red. La capa de aplicación permite que los administradores de red y desarrolladores de aplicaciones puedan estar involucrados en el control del funcionamiento de la red.

2) Arquitectura física

Como se observa en la Figura 2, el plano de datos de SD-WAN consiste en los dispositivos que realizan la entrega de datos a los destinos conectados por routers y enlaces físicos.

Fig. 2. Arquitectura física de SD-WAN [5]

Un controlador de red está a cargo de estos dispositivos, el cual es un servidor y un cluster, dependiendo de la necesidad de procesamiento y del tamaño de la red. Por último, la capa de aplicación está expresada por los servicios finales que utiliza el negocio y sus usuarios, mediante políticas para que un controlador de red distribuya los recursos disponibles entre los sitios según la necesidad. De forma que se tenga disponibilidad de información, debe considerarse controladores de respaldo de forma que asuman las tareas de control cuando los controladores principales presenten algún fallo.

C. Arquitectura SD-WAN de Cisco.

En el caso particular de Cisco [6], detalla tres capas esenciales: datos, control, gestión y orquestación, Figura 3.

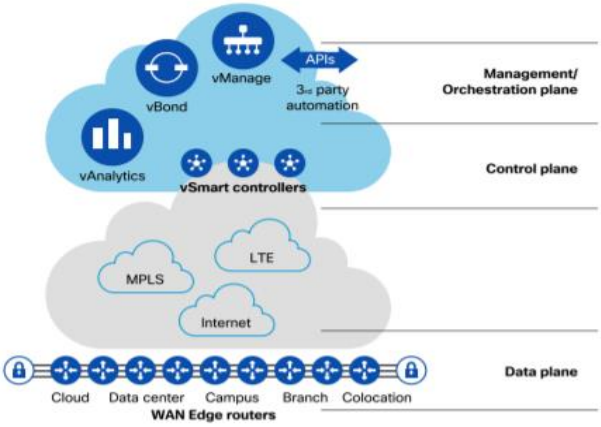

Fig. 3. Arquitectura SD-WAN Cisco [6]

Incluye distintos servidores para lo mencionado: gestión de los administradores de red y despliegue de configuración, resolución de problemas y monitoreo (vManage). La orquestación y aprovisionamiento *zero-touch* después de realizar autenticación (vBond). Plano de control y servidor para la ejecución de las políticas creadas, enrutamiento (vSmart). Por último, los routers Edge, son responsables del flujo del tráfico. Estos componentes y su interconectividad se representan en a Figura 4. Los controladores son máquinas virtuales con sistema operativo Linux.

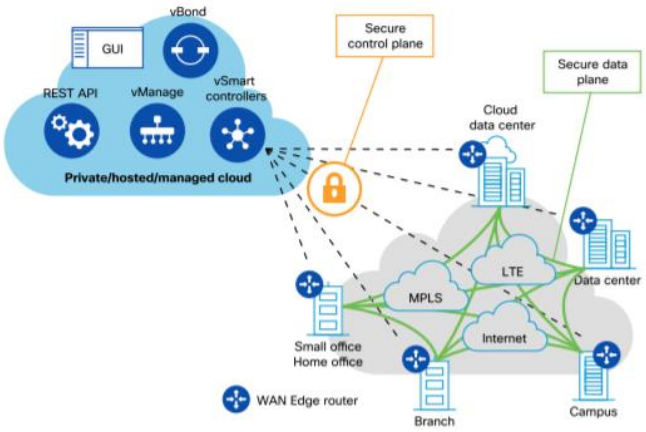

Fig. 4. Interacción componentes Cisco SD-WAN [6]

De esta forma, el objetivo de la presente investigación es realizar el análisis de caso para una implementación segura para la tecnología emergente SD-WAN, la misma que aún no ha sido adaptada en su totalidad en el medio local. Al contar con varios componentes, se debe realizar el análisis para cada uno de ellos de forma que se proteja integralmente la solución.

III. MÉTODOS

El método de investigación para el presente artículo es de tipo deductivo, al emplear razonamiento a partir de principios generales y premisas, para lograr la deducción de conclusiones lógicas. Se realiza la examinación de hechos, para el posterior análisis de lo observado.

A. Diseño de la investigación

Exploratorio, se realiza el estudio de la bibliografía de interés, para la identificación de problemas y propuesta de futuras investigaciones relacionadas.

Descriptivo, caracteriza y observa los escenarios y sus componentes, así como su interacción para establecer una descripción, lo más detallada posible.

Propositivo, por proponer soluciones en base a la información analizada, para la adopción del modelo más seguro ante riesgos identificados.

B. Fuentes de información

Las fuentes de información principales son los artículos donde se estudian casos de implementación de clientes para distintas marcas que adquieren soluciones del tipo SD-WAN. Esta información se adquiere a través de observación directa de implementación de soluciones por administradores de red, quienes tienen contacto con el objeto de investigación.

IV. RESULTADOS

Entre los escenarios posibles para las implementaciones de SD-WAN, se toma en cuenta los componentes identificados y arquitectura para el análisis de vulnerabilidades y amenazas y planteo de contramedidas para los riesgos identificados.

Toda empresa debe considerar en su implementación medidas de ciberseguridad en su infraestructura, de forma que se reduzca el riesgo de ataques que puedan afectar al negocio. De esta forma, al haber desaparecido el perímetro de red por las tecnologías emergentes, se debe considerar para el aseguramiento de la red: autenticidad de los dispositivos involucrados en la comunicación, aseguramiento de los enlaces mediante cifrado de canales y la escalabilidad, flexibilidad y alta disponibilidad en la solución.

Según Cisco [7], su solución SD-WAN ha sido diseñada, tomando en cuenta la seguridad de la solución basado en los siguientes puntos:

- *Autenticación*. Solo manejan tráfico los dispositivos autenticados y permitidos.
- *Cifrado*. Los canales de comunicación entre los dispositivos incluyen cifrado AES-GCM-256, incluyendo una verificación de integridad.
- *Integridad*. Garantiza que los datos transmitidos no sufrirán cambios no autorizados, mediante una versión modificada del protocolo ESP.

A. *Análisis de vulnerabilidades y amenazas en la arquitectura SD-WAN.*

Según la bibliografía consultada, se considera las amenazas y vulnerabilidades de seguridad relacionados a los componentes y capas de SD-WAN, en la arquitectura genérica de este tipo de solución.

1) *Software no actualizado*. Al ser una tecnología nueva, SD-WAN está en constante desarrollo; los componentes en su mayoría (routers de borde, controladores, orquestadores) tienen un núcleo Linux, en distintas distribuciones, lo cual es propenso a ataques de día cero, y vulnerabilidades conocidas del núcleo.

2) *Funciones básicas de red*. Un componente de red puede ser un dispositivo físico, software, virtual o en la nube, puede estar expuesto según [5]:

   - Enrutamiento basado en protocolos de enrutamiento tradicionales.
   - VPN implementada con cifrado no seguro, los cuales se exponen a las vulnerabilidades conocidas de estos algoritmos. Así también debe implementarse protocolos seguros combinados como AH+ESP.
     - Mecanismos de cifrado no implementados correctamente
     - Uso de algoritmos de cifrado inseguros
     - Suplantación de *peer*
     - Selección de parámetros IKE débiles
     - Selección de contraseñas y llaves débiles para autenticación

3) *Configuración automática para autenticación de dispositivos con el orquestador*, mediante túneles cifrados. De esta forma se exponen a ataques de suplantación de identidad o MITM en plano de datos.

4) *En la virtualización de funciones de red* (VNF, *virtual network function*), una expresión regular incorrecta de un IDS o WAF basado en software, puede exponer una vulnerabilidad a un ataque de denegación de servicios de expresión regular [5]. También si se ve comprometido algún mecanismo de configuración de una VNF y se obtiene control en un sistema operativo, es posible comprometer a otras VNF en el mismo segmento:

   - Denegación de servicio por función de seguridad.
   - Acceso no autorizado a los recursos de una VNF
   - Escalamiento de privilegio.

5) *En interfaces de gestión por SSH, HTTP, HTTPS*, expuestas a Internet, separación lógica de redes de gestión. Las interfaces de gestión son utilizadas no solo para que un administrador pueda acceder, sino también para comunicación con otros componentes como un controlador. Entre algunas debilidades se tiene:

   - Credenciales predeterminadas débiles y no cambiadas.
   - Uso de una cuenta privilegiada con todos los accesos.
   - Configuración permisiva de sudo
   - Configuración de control de accesos ausente o incorrectamente configurada
   - Fuerza bruta para contraseña
   - XSS (reflejado, almacenado)
   - Acceso no autorizado a información del proveedor y tenants configurados

6) En los servicios de orquestación, para la comunicación de los controladores y routers se usa Openflow, REST API o protocolos sobre TLS para programar la conectividad de los componentes y establecimiento de túneles [7]. Provisionamiento zero touch (ZTP, zero touch provisioning) [5], es un mecanismo que permite a los nodos ser configurados automáticamente.

   - Acceso no autorizado a recursos del sistema operativo por funciones vulnerables.
   - Suplantación de nodo SD-WAN
   - Suplantación de servidor o cliente ZTP.
   - Acceso no autorizado al servicio y datos del orquestador.

7) Amenazas de cifrado, los mecanismos de cifrado deben implementarse en todas las capas de la arquitectura.

   - Utilización de llaves públicas por defecto y certificados que son usados para todos los clientes.
   - Utilización de certificados autofirmados para generación de llave pública, emitidas por el fabricante.
   - Instalación manual de certificados autofirmados en los nodos SD-WAN.

B. Recomendaciones de implementación y contramedidas.

Como medida de seguridad para cada uno de los vectores de ataque planteados en el punto anterior, se describen las siguientes medidas:

a) Actualización constante de la solución

- Cada componente de la arquitectura debe recibir actualizaciones contantes, al ser SD-WAN una tecnología aún en desarrollo.
- Recibir firmas actualizadas para análisis de datos.

b) Funciones de cifrado y elección de protocolos

- Utilizar protocolos de red y criptográficos estándar
- Actualizar un sistema operativo y componentes de terceros.
- Emplear mecanismos de confinamiento como SElinux y AppArmor.
- Utilizar parámetros criptográficos seguros
- Emplear primitivas criptográficas seguras

c) Contra suplantación de identidad

- Aplicar métodos de mitigación basados en hardening.
- Desarrollar mecanismos internos que detecten ataques a la red.
- Implementar mecanismos de red para la detección de ataques MitM.

d) Hardenizar cada componente de las VNF

- Las VNF al tener en su mayoría un núcleo Linux, deben cambiarse los parámetros por defecto para evitar ataques a vulnerabilidades conocidas de la distribución.

e) En la gestión:

- Cambio de contraseñas por defecto.
- Confinamiento y segmentación de redes.
- Configurar correcta del protocolo TLS.
- Proteger la interfaz web mediante WAF.
- Deshabilitar de cuenta privilegiada o acceso por contraseña compartida en caso de emergencia.
- Control de accesos según mínimo privilegio.
- Bloqueo de acceso ante falla repetida de ingreso de credenciales.

f) Mecanismos de autenticación seguros para autenticación de los componentes del sistema, mediante certificados emitidos por una entidad de confianza [8].

g) Utilización de algoritmos de cifrado no vulnerados y uso de certificados emitidos por una entidad autorizada, evitar el uso de certificado auto firmados.

V. Discusión

La tecnología SD-WAN al ser relativamente nueva, ofrece ventajas significativas para una red corporativa al ser flexible, con gestión centralizada y con uso inteligente del ancho de banda según especificación de aplicaciones y servicios. Sin embargo, esta tecnología no cuenta con un diseño de seguridad implementado desde el inicio, lo cual deja abierta una superficie de ataques considerable. Al separar en varias capas su arquitectura y utilizar componentes del tipo virtualizado para funciones de red, cifrado de enlaces y autenticación en un orquestador, se debe considerar las vulnerabilidades de cada componente que puede causar el acceso a datos que maneja la solución. Entre las recomendaciones que deben implementarse desde un inicio es la hardenización y actualización constante de software de los componentes individuales, los cuales pueden ser vulnerables a un atacante y obtener acceso a los controladores para la modificación de políticas e información crítica. Así también el cifrado, presente en todas las capas, debe ser utilizado con algoritmos no vulnerados y establecer mecanismos de autenticación de los componentes de SD-WAN con su orquestador de forma segura, con certificados emitidos por entidades de confianza. De esta forma se podrá mitigar riesgos de ataques a la solución SD-WAN desde la implementación y en posterior operación productiva de la misma.

Referencias

[1] X. Zuo, Y. Cui, M. Wang, T. Wang, and X. Wang, “Low-latency networking: Architecture, techniques, and opportunities,” IEEE Internet Computing, 2018.

[2] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities," 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, España, 2019.

[3] F. Bannour, S. Souihi, and A. Mellouk, “Distributed sdn control: Survey, taxonomy, and challenges,” IEEE Communications Surveys & Tutorials 2018.

[4] Rangan, R.K.m "Trends in SD-WAN and SDN", CSI Publicactions. Abril 2020.

[5] Sergey G., Kolegov, D. "SD-WAN Threat Landscape". Noviembre 2018.

[6] Cisco. (2019). Cisco SD-WAN Cloudscale architecture. https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

[7] Security Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12 - Security Overview [Cisco SD-WAN]. (2020, 26 agosto). Cisco. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/security-overview.html#id_118806

[8] FCC TAC Cybersecurity Working Group, "Security BCP Recommendations for SDN/NFV". Diciembre 2016.