ESTUDIO DE LAS SOLUCIONES SD-WAN PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS TECNOLÓGICAS DE LAS ORGANIZACIONES

MÁSTER UNIVERSITARIO DE INGENIERÍA DE TELECOMUNICACIÓN
ÁREA DE TELEMÁTICA

MANUELA CALVO BARRIOS

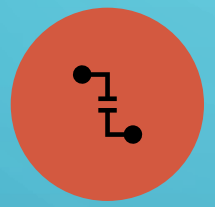
TUTOR: JOSÉ LÓPEZ VICARIO

RESPONSABLE ASIGNATURA: XAVIER VILAJOSANA GUILLÉN

ÍNDICE DE CONTENIDOS

1. OBJETIVOS

Aislamiento de las zonas de la red mediante redes virtuales VLANs para segmentar el tráfico de la red.



Separación de la infraestructura en tres zonas: red interna, zona desmilitarizada y red externa; divididas por elementos de seguridad robustos, como firewalls, y uso de balanceadores de carga.

Control de los recursos disponibles y de los flujos de comunicaciones recibidos del exterior mediante el descarte de paquetes, para prevenir que la congestión en la red ocasione indisponibilidades.

Comparación de los tiempos de respuesta presentes en las comunicaciones realizadas con los diferentes componentes de seguridad de la red.

Mejora superior al 10% de la eficiencia/rendimiento de la red que introduce la configuración de medidas de seguridad en la SD-WAN.

Medición del porcentaje de bloqueo de las comunicaciones no deseadas y del riesgo de ataques exitosos de la red.

2. ESTADO DEL ARTE

Auge de las soluciones SD-WAN

- Los fabricantes del mercado están apostando por este tipo de soluciones.
- La migración a los sistemas cloud ha hecho que las empresas modernicen sus infraestructuras tecnológicas.

Transformación digital de las organizaciones

- Soluciones escalables.
- Variedad de tecnologías distintas interconectadas.
- Necesidad de conexión de gran cantidad de dispositivos.
- Menores costes de mantenimiento.

Importancia de la ciberseguridad

- Durante los últimos años ha adquirido especial relevancia.
- Impulsada por normativas y por la necesidad de proteger los activos críticos de las organizaciones.
- Información es usada actualmente como arma, por lo que debe mantenerse confidencial y sin ser alterada.

Contribución del TFM

- Explora la configuración de medidas de seguridad en una topología SD-WAN virtual.
- Simulación de políticas y configuraciones de filtrado de paquetes para el bloqueo de las comunicaciones.
- Análisis del impacto sobre el rendimiento y el riesgo de ataques de la red con una tecnología novedosa.

3. CONTEXTO TEÓRICO: SDN

- La red definida por software (SDN) permite la separación del plano de control, el plano de datos y el plano de aplicación en la red, permitiendo una mayor agilidad y adaptabilidad en la configuración y gestión de la red y sus políticas.
- De este tipo de redes destaca:
  - El plano de control se separa de los dispositivos de red y se centraliza en un controlador SDN.
  - Este controlador es responsable de tomar decisiones de enrutamiento y políticas de red, y se comunica con los dispositivos de red a través de un protocolo de control, como OpenFlow , por medio de la Southbound API.
  - El controlador se comunica con el plano de aplicación, donde residen las aplicaciones que dan servicios en la red, por medio de la Northbound API.

Ventajas de las SDN frente a las redes tradicionales:

- Permite una mayor flexibilidad y agilidad en la gestión de la red.
- Proporciona un mayor nivel de aislamiento y seguridad en la red.
- Proporciona mejores modelos de escalabilidad.
- Permite la gestión centralizada del tráfico y de los componentes de la red, como los switches.

3. CONTEXTO TEÓRICO: ELEMENTOS DE SEGURIDAD

Zona desmilitarizada

Basada en dos niveles de defensa:

- Firewall expuesto a internet.
- Firewall que protege los activos internos.

Recomendable que los dos niveles cuenten con tecnologías distintas, para reducir el riesgo de presentar las mismas vulnerabilidades.

Balanceadores de carga

- Técnica que se utiliza para distribuir estática o dinámicamente el tráfico que alcanza una red.
- Configuraciones basadas en algoritmos de asignación de recursos (aleatorio, Round Robin, con pesos).

Ayudan a gestionar la carga de los recursos expuestos y el procesamiento de peticiones que se realiza por parte de los servidores.

Firewalls

- Intercepta y filtra los paquetes, cruzándolos contra una lista de reglas de comportamiento que indican si el tráfico es legítimo en la red.
- Configuración basada en direcciones IP origen y destino, puertos, protocolos, etc.

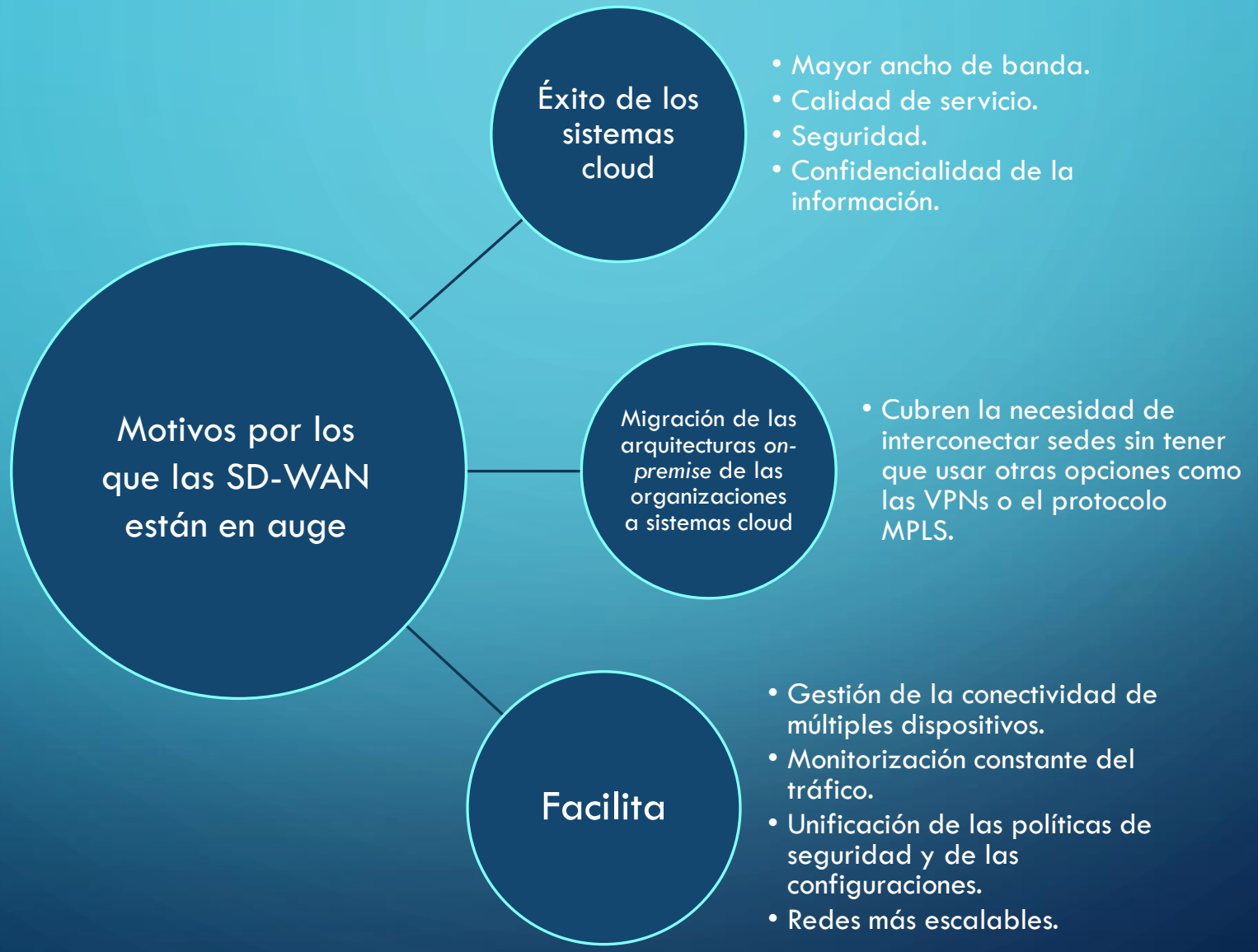
Actualmente en el mercado existen soluciones de firewalls con capacidades de inspección de tráfico avanzadas, y se emplean en muchas ocasiones para separar distintos segmentos de una misma red.

Virtual Private Networks (VPN)

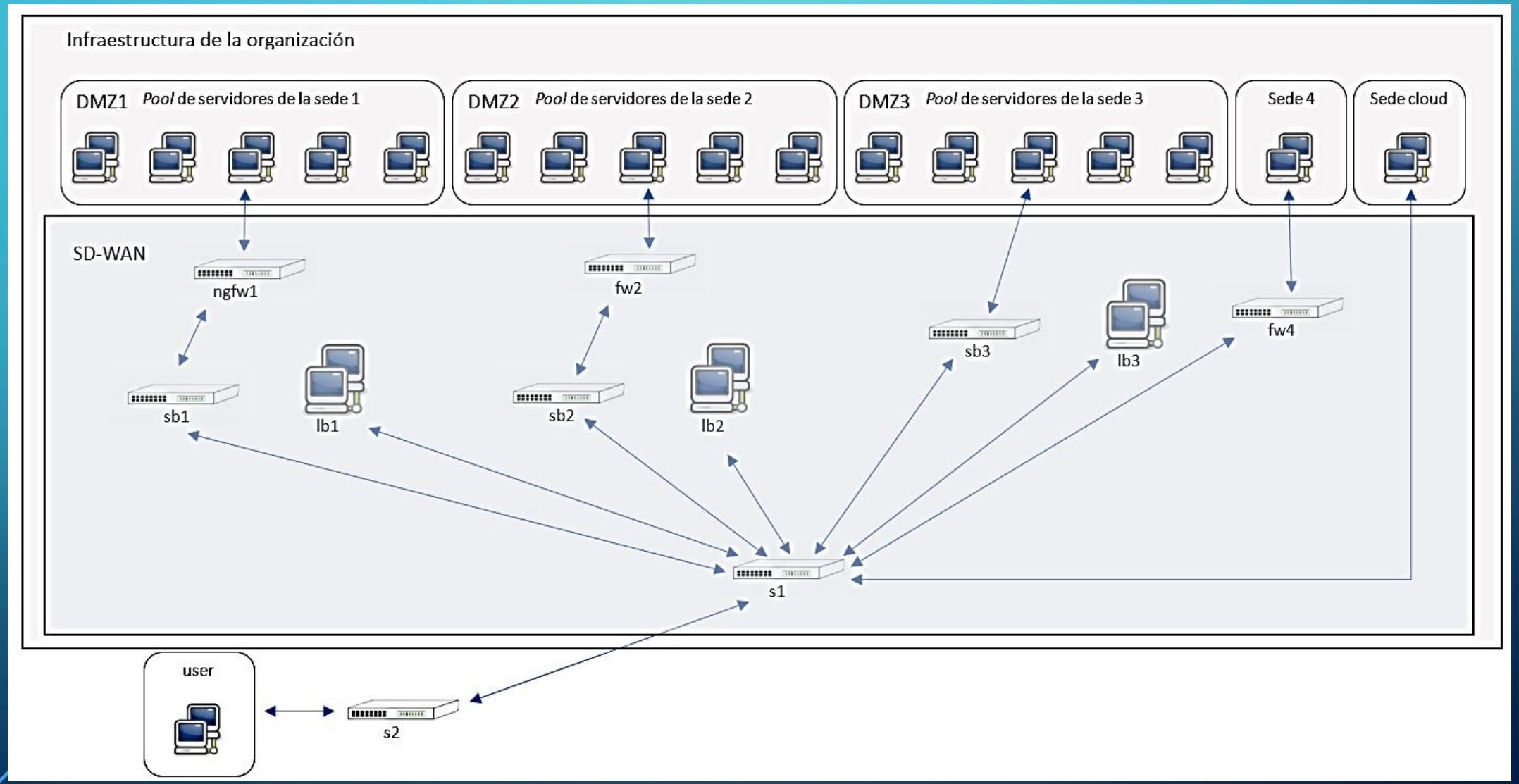
- Se emplea para garantizar la confidencialidad e integridad de las comunicaciones transmitidas entre sedes o de un usuario a una sede.
- Además, también proporcionan autenticación y protección anti-repetición.

Cuando un paquete va a ser enviado, los dispositivos añaden en las cabeceras los campos necesarios para que el tráfico se envíe de manera segura y cifran el paquete IP original para enviarlo a través de internet.

3. CONTEXTO TEÓRICO: SD-WAN



4. DISEÑO DE LA RED: DIAGRAMA DE RED (1/2)



4. DISEÑO DE LA RED: DIAGRAMA DE RED (2/2)

MATRIZ DE COMUNICACIONES

Destino / Origen	Sede 1	Sede 2	Sede 3	Sede 4	Cloud	User
Sede 1	-	OK	KO	OK	OK	OK
Sede 2	OK	-	KO	OK	KO	OK
Sede 3	KO	KO	-	OK	OK	OK
Sede 4	OK	OK	OK	-	OK	OK
Cloud	OK	KO	OK	OK	-	OK
User	OK	OK	OK	OK	OK	-

DESCRIPCIÓN GENERAL DE LA RED

- Red compuesta por:
  - 3 pools de servidores de procesamiento de peticiones para las sedes 1, 2, 3.
  - Tres servidores de balanceo de carga.
  - 3 componentes firewalls que realizan el filtrado de tráfico en diferentes niveles.
  - 5 sedes de la misma organización conectadas por medio de la SD-WAN.
- Para interpretar las comunicaciones que pueden llevarse a cabo dentro de la red, a través de la SD-WAN, hay que consultar la matriz de comunicaciones.

4. DISEÑO DE LA RED: MÉTRICAS DE RENDIMIENTO, SEGURIDAD Y RIESGO

REQUISITOS TÉCNICOS Y MÉTRICAS PROPUESTAS

- Balanceo de carga de tráfico: métricas de ancho de banda y tiempo de respuesta.
- Filtrado de paquetes: porcentaje de bloqueo de las comunicaciones.
- Seguridad de las comunicaciones: uso de protocolos cifrados.
- Caminos vulnerables: medición del riesgo asociado a los caminos de la red.

UMBRAL ASOCIADO A LAS MÉTRICAS

Métrica	Medición	Umbral
Ancho de banda máximo	En cada uno de los caminos desde *user* hacia las sedes	Mayor a 50 Mbps
Tiempo de respuesta	En cada uno de los caminos desde user hacia las sedes	Menor a 0,15 segundos
Porcentaje de bloqueo	En todas las comunicaciones de la red	40% de bloqueo
	Comunicaciones por VLANs	89% de bloqueo
	Comunicaciones UDP	100% de bloqueo
	Comunicaciones HTTP	100% de bloqueo
	Comunicaciones no cifradas	100% de bloqueo
Métrica de riesgos de ataque	Basado en el riesgo de seguridad presente en cada camino de la red.	Comparativa de los diferentes caminos

4. DISEÑO DE LA RED: COMPONENTES DE SEGURIDAD IMPLEMENTADOS

- Firewalls: para el filtrado de paquetes en la zona SD-WAN.
  - Capa 2: filtran por dirección Ethernet origen y destino, así como por protocolo ARP.
  - Capa 3: filtran por dirección IP origen y destino, VLANs, y protocolo ICMP.
  - Capa 4: bloquean el tráfico UDP.
- Uso de certificados: para el cifrado de la información transmitida dentro de la SD-WAN.
  - Desplegados en los servidores para garantizar que las comunicaciones son seguras, confidenciales e íntegras.
- Balanceadores de carga de la SD-WAN: algoritmos de asignación de recursos implementados.
  - Aleatoria: selecciona aleatoriamente qué servidor procesa las peticiones.
  - Round Robin: asigna cíclicamente las peticiones a los servidores.
  - Round Robin con pesos dinámicos: asignación cíclica combinada con la modificación dinámica de pesos.

5. RESULTADOS: LISTADO DE PRODUCTOS OBTENIDOS

- Script *topo.py*: configuración de la red y de la SD-WAN
- Script *lb.py*: configuración del balanceador de carga lb1 con algoritmo aleatorio
- Script *lb_round_robin.py*: configuración del balanceador de carga lb2 con algoritmo Round Robin
- Script *lb_weighted_round_robin.py*: configuración del balanceador de carga lb3 con algoritmo Round Robin con pesos
- Script *https_server.py*: configuración de los servidores para que usen el protocolo HTTPS en el puerto 443 con la instalación de certificados

5. RESULTADOS: BLOQUEO DE LAS COMUNICACIONES

Bloqueo del tráfico UDP

- 100% de bloqueo en las sedes 1, 2, 4
- 0% de bloqueo en las sedes 3 y cloud, debido a que no cuentan con protección de filtrado de paquetes por firewall.

Bloqueo del tráfico HTTP

- 100% de bloqueo por parte de todos los servidores de los *pools* de las sedes 1, 2 y 3, de los servidores de la sede 4 y de la sede cloud, y de los balanceadores de carga.
- La configuración de los servidores hace que solo acepten comunicaciones en su puerto 443 con uso de certificados.

Cifrado de las comunicaciones

- 100% de cifrado de las comunicaciones de la capa de aplicación, con uso de protocolo TLS 1.3.
- Debido al despliegue de certificados en los servidores de la red.

5. RESULTADOS: BLOQUEO DE LAS COMUNICACIONES

Comunicaciones no permitidas

41% de bloqueo del tráfico de la red.

Matriz de comunicaciones indica que, de los 30 caminos existentes en la red, la SD-WAN no permite comunicación exitosa en 6 de ellos. A nivel de máquinas, existe un 60% de hosts interconectados.

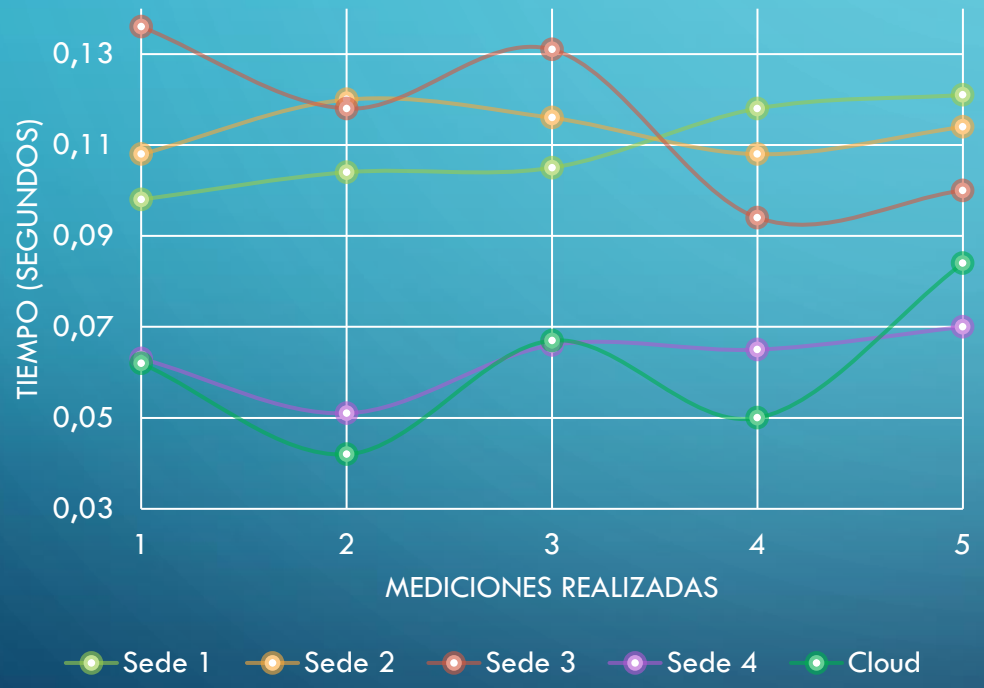
Comunicaciones por VLANs

89% del tráfico bloqueado por no usar etiquetado de VLANS.

Existen en la red 6 enlaces configurados por VLANs para interconectar servidores de 3 sedes distintas. Quedan sin configurar 49 enlaces, en los que no se aceptan las comunicaciones.

5. RESULTADOS: RENDIMIENTO DE LA RED

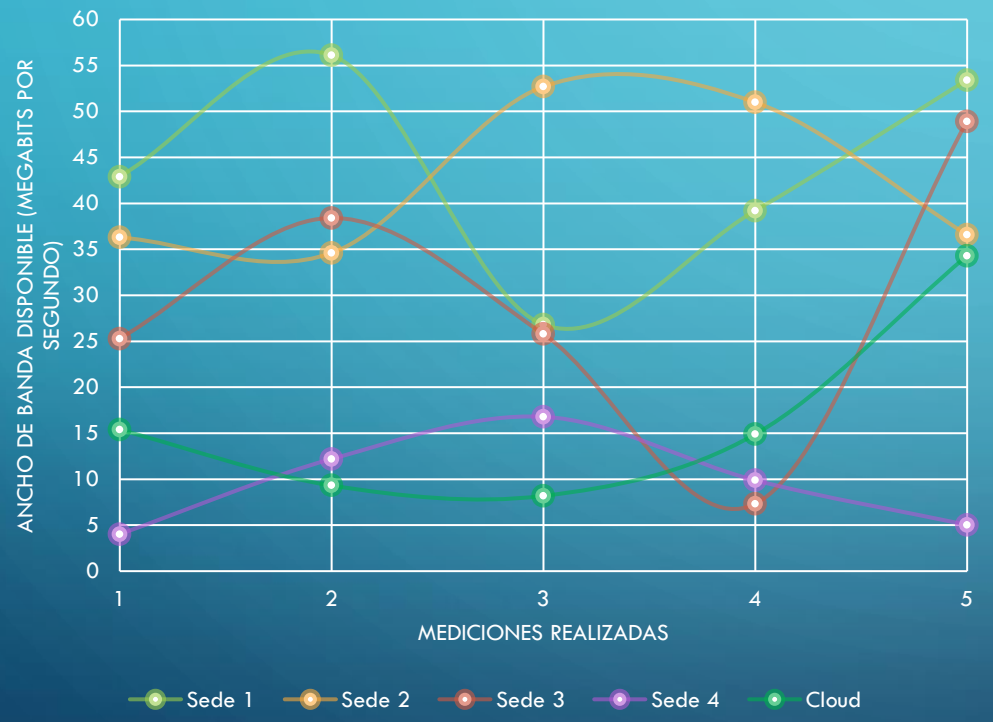
TIEMPO DE RESPUESTA



- Mejores resultados obtenidos para los caminos:
  - user → sede 4
  - user → sede cloud
- Peores caminos cuando hay balanceo de carga.
  - Aplicación de los algoritmos de balanceo introduce retardo en las redes.
  - Se comprueba que, entre los dos mejores caminos, el que presenta un menor tiempo de respuesta es el que tampoco cuenta con firewalls, por lo que se demuestra que estos elementos también consumen tiempo de procesamiento de paquetes.

5. RESULTADOS: RENDIMIENTO DE LA RED

ANCHO DE BANDA



- Mejores resultados obtenidos para los caminos:
  - user → sede 1
  - user → sede 2
  - user → sede 3
- Peores resultados de ancho de banda cuando no hay balanceo de carga.
  - Demuestra la efectividad de la gestión de los recursos dentro de la red.
  - El balanceo de carga combinado con firewall de próxima generación (user → sede 1), cuenta con mejor ancho de banda, pudiendo ser el motivo que se limpia el tráfico no deseado de los enlaces de la SD-WAN.

5. RESULTADOS: RIESGO DE LA RED EN FUNCIÓN DE LA COMPLEJIDAD DE ATAQUE

MÉTRICAS DE RIESGOS DE LA RED

- Métricas:
  - Número de caminos de ataque (NAP): son 5 caminos.
  - Esfuerzo medio de los caminos de ataque (ALAP): 6,1 puntos de complejidad por camino.
  - Camino más corto de ataque (SAP): user → sede cloud.
- Los caminos con menores componentes de seguridad reciben menos puntuación y son más propensos a que un atacante con conocimientos pueda explotar sus vulnerabilidades y acceder exitosamente a los recursos internos albergados en la sede.

TABLA DE PONDERACIONES DE LOS COMPONENTES DE SEGURIDAD

Componente de seguridad de la SD-WAN	Puntuación de seguridad
Firewall de capa 2	2 puntos
Firewall de capa 3	2 puntos
Firewall de capa 4	2 puntos
Bloqueo de UDP	1 punto
Bloqueo de HTTP	1 punto
Uso de comunicaciones cifradas	1 punto
Balanceo de carga	0,5 puntos

PONDERACIONES DE LOS CAMINOS

Origen – destino	Protección	Puntuación
User – Sede 1	Balanceo de carga, firewall de capas 2, 3, 4, cifrado de comunicaciones y bloqueo UDP, HTTP	10,5
User – Sede 2	Balanceo de carga, firewall de capas 3, 4, cifrado de comunicaciones y bloqueo UDP, HTTP	8,5
User – Sede 3	Balanceo de carga, cifrado de comunicaciones y bloqueo HTTP	2,5
User – Sede 4	Firewall de capas 2, 4, cifrado de comunicaciones y bloqueo UDP, HTTP	7
User – Sede cloud	Cifrado de comunicaciones y bloqueo HTTP	2

6. CONCLUSIONES (1/2)

Uso de elementos de seguridad

- Permiten el bloqueo de las comunicaciones no deseadas dentro de la red, para proteger los activos albergados en las distintas sedes.
- Posibilidad de establecer comunicaciones por medio de VLANs para segmentar el tráfico entre sedes (red interna), sin que todas las máquinas estén conectadas entre sí.

Tiempo de respuesta

- Las soluciones de seguridad introducen retardos en las comunicaciones debido al tiempo que se emplea en el procesamiento de los datos.
- Es necesario seguir estudiando las tecnologías de transmisión de datos y las soluciones de seguridad para garantizar que se transmite información de forma confidencial e íntegra, sin que haya penalización en el tiempo de respuesta.

Ancho de banda

- Se obtienen mejores resultados experimentales cuando existe protección completa de las comunicaciones.
- La protección de la red por medio de la configuración de políticas de restricción de tráfico evita la presencia de tráfico no deseado en los enlaces de la SD-WAN, por lo que hay más recursos de ancho de banda disponibles para su uso por parte de las comunicaciones legítimas.

6. CONCLUSIONES (2/2)

Riesgo de la red

- Según cálculos teóricos, la presencia de elementos de protección de los activos y recursos proporcionados por la SD-WAN otorga una mejor ponderación de capacidad de resiliencia frente ataques externos.
- Los caminos de la red desprotegidos cuentan con un mayor riesgo de sufrir ataques externos que sean exitosos y que comprometan los activos de la red.

Objetivos

- Se han cubierto todos los objetivos marcados para el TFM. Respecto a los objetivos específicos:
  - Se han comparado los tiempos de respuesta y se ha logrado ordenar siguiendo este criterio los diferentes caminos presentes en la red diseñada.
  - Se ha comprobado que la mejora de ancho de banda disponible en los caminos que cuentan con protección frente a aquellos que no cuentan con medidas de seguridad es superior al 10%.
  - Se han podido calcular los riesgos de la red y realizar las mediciones de bloqueo de las comunicaciones.

¡GRACIAS POR SU ATENCIÓN!