



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO
EN ELECTRÓNICA Y TELECOMUNICACIONES**

“Diseño e implementación de una red Hub and Spoke sobre tecnología SD-WAN”

Autor:

Dayana Lizbeth Ruano Chulde

Director del Proyecto: Ing. Aguilar Salazar, Darwin Leonidas, Msc.



AGENDA

1. INTRODUCCIÓN

2. OBJETIVOS

3. DISEÑO DE LA RED

4. IMPLEMENTACIÓN DE LA RED

5. ANÁLISIS DE RESULTADOS

6. CONCLUSIONES Y RECOMENDACIONES

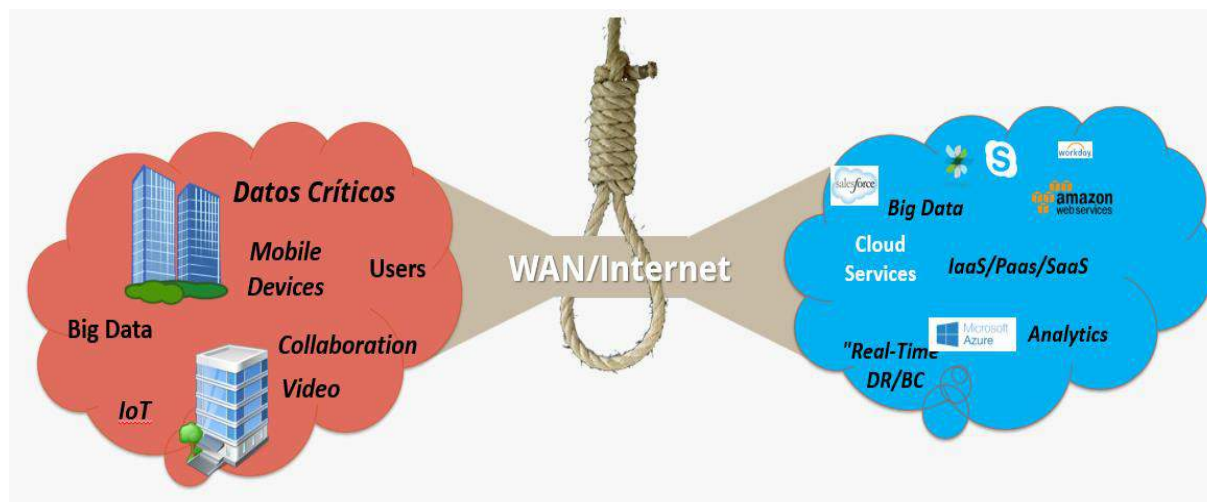
7. TRABAJO FUTUROS



Redes WAN en el área corporativa



La conectividad en redes de área Amplia (WAN) ha evolucionado con el objeto de obtener una funcionalidad más sencilla y segura, pues, ahora el Internet es un medio común para unir sectores empresariales distantes. Pero con todo ello y las nuevas exigencias ha quedado rezagado con el aparecimiento de la nube, pues, ya no resulta eficiente, dado que pernoctan nuevas necesidades de almacenaje, transformación digital y servicios debido a la proliferación de aparatos móviles que buscan acceder a las redes .



Tecnologías de las Redes WAN Tradicional

VPN (Redes Privadas Virtuales)

- Crean redes locales sin necesidad de que los usuarios estén físicamente conectados, es decir únicamente comparten datos e información a través del internet.

MPLS (Multiprotocolo de conmutación de Etiquetas)

- Enruta el tráfico de red mediante el uso de etiquetas en lugar de direcciones IP. Se puede utilizar en cualquier protocolo de red, incluidos Ethernet, ATM y Frame Relay.



SDN y SD-WAN

SDN

- Separación de los **Planos de Control y Datos** para crear redes programables controladas desde un punto central.

SD-WAN

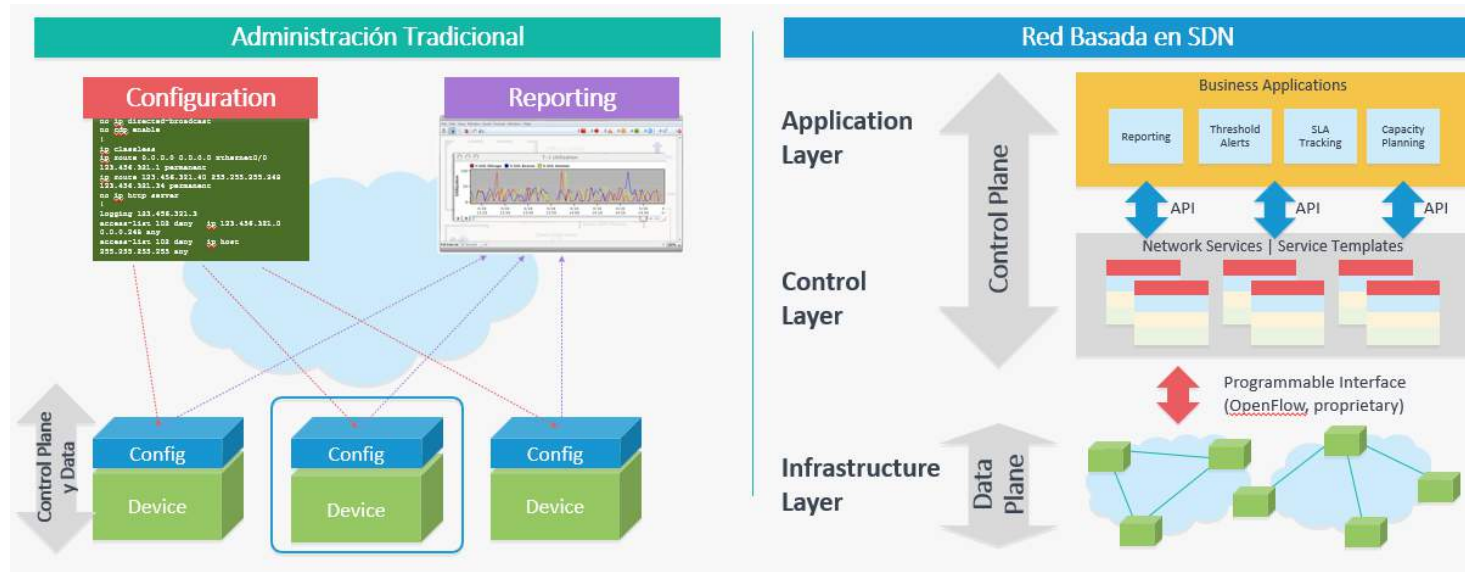
- Es una aplicación de soluciones de SDN que permite el uso eficiente y controlado de las conexiones WAN.
- Capta la base definida por un software similar y extrae el plano de control del plano de datos a la WAN.
- Su finalidad principal es viabilizar a los usuarios la posibilidad de acceso a servicios de conectividad de forma eficaz, al más bajo costo, aprovechando la rápida expansión del internet, así como también en base al aumento del mercado de servicios en la Nube.



Comparación entre SD-WAN, MPLS y VPN

	VPN	MPLS	SD-WAN
Arquitectura	Utiliza diferentes protocolos de tunelización para crear conexiones seguras a través de Internet. Admite diversas implementaciones como Ipvsec, SSL, PPTP, etc.	Maneja conmutación de etiquetas para dirigir el tráfico de manera eficiente. Requiere acuerdos con proveedores de servicios para establecer rutas MPLS.	Maneja software para gestionar la red de forma más dinámica y adaptable. Permite la configuración centralizada y dinámica de la red.
Costo	En general más económica, especialmente al utilizar conexiones a través de Internet.	Suele ser más costoso debido a la infraestructura dedicada, configuración y mantenimiento por parte del proveedor	Ofrece una solución más rentable al permitir la utilización eficiente de conexiones múltiples.
Conectividad y Topología	Puede utilizar Internet para establecer conexiones seguras. Topología más flexible, adapta la red a la infraestructura existente.	Proporciona conectividad segura y fiable entre ubicaciones Topología basada en circuitos y rutas predefinidas	Permite la utilización de múltiples conexiones, como MPLS, Internet y conexiones inalámbricas. Ofrece una topología dinámica y adaptable según las condiciones de la red.
Rendimiento y Latencia	Puede tener un rendimiento variable dependiendo de la conexión a Internet. Latencia puede ser mayor en comparación con MPLS	Ofrece un rendimiento confiable y predecible. Contribuye a la baja latencia.	Optimiza el rendimiento al utilizar múltiples conexiones de manera inteligente. Puede mejorar la latencia al seleccionar la mejor ruta para el tráfico.
Seguridad	Encripta el tráfico para garantizar la confidencialidad de los datos.	Proporciona un nivel básico de seguridad, pero puede requerir medidas adicionales para niveles más altos de privacidad.	Incluye funciones de seguridad integradas como firewalls y encriptación.
Gestión y Configuración	Configuración más flexible y puede ser gestionada internamente.	Configuración más estática, requiere acuerdos con proveedores, para realizar cambios toma más tiempo.	Ofrece configuración centralizada y dinámica, facilitando la gestión de la red a través de software.
Adaptabilidad y Escalabilidad	Más adaptable y escalable, especialmente en entornos cambiantes.	Menos adaptable porque requiere más tiempo para cambios, escalabilidad limitada y puede requerir cambios significativos para expandirse.	Altamente adaptable y escalable, se ajusta a los cambios en los requisitos de la red.





La presente investigación tiene como alcance emplear la tecnología de SD-WAN en un cliente corporativo de un proveedor de servicio de internet con la finalidad de conocer sus beneficios y promover el uso de esta tecnología en Ecuador.

Objetivo General

Diseñar e implementar una red Hub and Spoke sobre SD-WAN para un cliente corporativo de la empresa proveedora de servicios de internet nacional.

Objetivos Específicos



Realizar un estudio previo sobre la red WAN definida por software (SD-WAN), red Multiprotocol label switch (MPLS) y red privada virtual (VPN).



Diseñar la red Hub and Spoke sobre SD-WAN cumpliendo con los requisitos del cliente corporativo de una empresa proveedora de servicios de internet nacional.

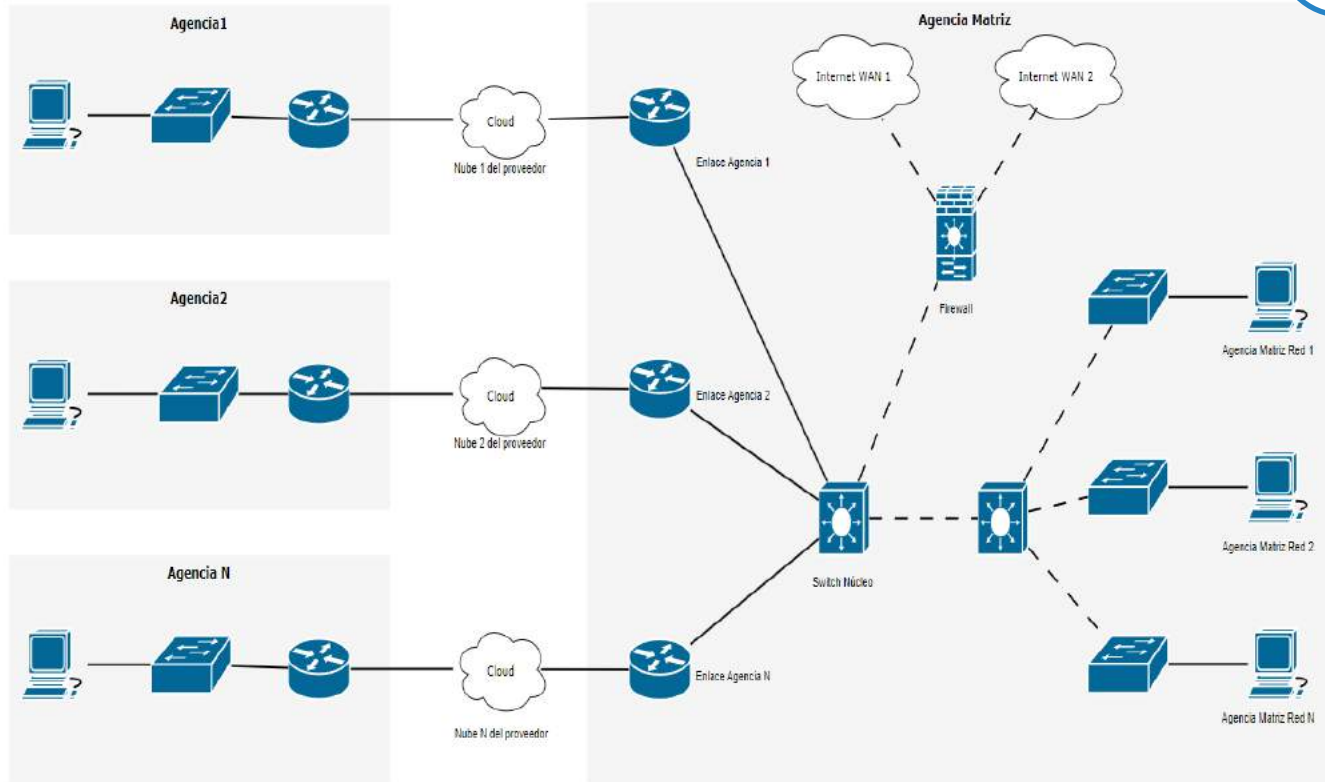


Implementar el diseño de la red Hub and Spoke sobre SD-WAN utilizando como hardware equipos Cisco.



Analizar y verificar métricas de QoS (Calidad de Servicio) y seguridad con el fin de comenzar a implementar la tecnología de SD-WAN en futuras redes.





Cuenta con 9 agencias a nivel Nacional en las ciudades de Cuenca, Quito, Sangolquí, Ambato, Riobamba, Santo Domingo y Latacunga

1400 clientes aproximadamente (150-160 por agencia)

Red híbrida con tecnología MPLS y VPN.

Enlaces con un AB de 5Mbps mediante cable de cobre

Oficina matriz dispone de un núcleo de servicio de red, firewall y el data center.

Topología Estrella

Enlace de backup una IPsec VPN sobre internet desde el switch de core hacia el router de la nube.



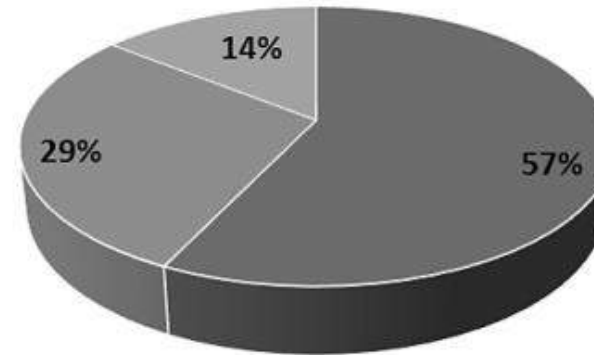
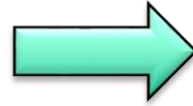
Problemas Red bajo MPLS Y VPN

- Administración no centralizada.
- Dificultad para el control del congestionamiento del tráfico en cada agencia.
- Demora en reporte de alarmas a los administradores de la red.
- Conexiones de un bajo AB
- Soporte presencial ante problemas de configuración.
- Mayor tiempo de gestión y costos.
- Seguridad y control de aplicaciones limitada.

Beneficios Red bajo SD-WAN

- Tener una administración centralizada.
- Aumentar anchos de banda.
- Monitoreo de los servicios a nivel de red, sin gestión presencial.
- Controlar el tráfico, contenido y apps.
- Mejorar la latencia, pérdida de paquetes, gestión de la red WAN.
- Seguridad en el tráfico de las aplicaciones.
- Reducción de costos.






■ CISCO ■ FORTINET ■ VMWARE

Según estudio realizado por (Cusco Perez, Cabrera Mejía, & Lugo García, 2022), en Ecuador el 57% de las empresas tienen implementado SD-WAN con soluciones Cisco, el 29% con soluciones Fortinet y apenas un 14% con VMware.

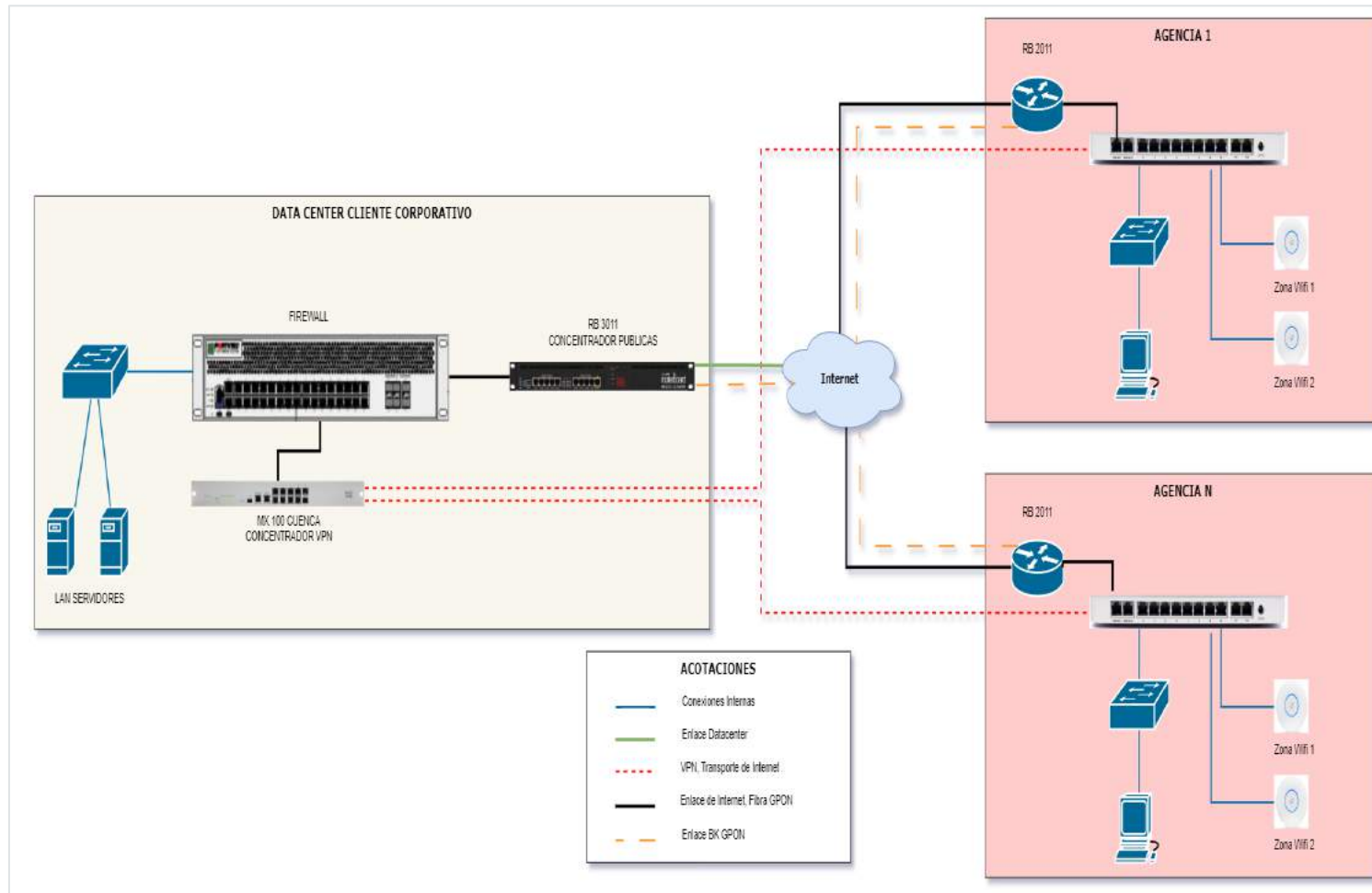


Cloud Managed



Meraki MX64/65	Meraki MX84	Meraki MX100
<ul style="list-style-type: none">High performance and affordable - small branch (small form factor)Integrated threat defense, low operating costs, simplified managementFirewall throughput - 250 MbpsOptional wireless LAN	<ul style="list-style-type: none">Powerful networking and security for the branch (up to 200 clients)Integrated threat defense, low operating costs, simplified managementFirewall throughput - 500 Mbps	<ul style="list-style-type: none">Powerful networking and security for the branch (up to 500 clients)Integrated threat defense, low operating costs, simplified managementFirewall throughput - 750 Mbps





Alcance de crecimiento para 3 años, 10% por año, alrededor de 1820 clientes.

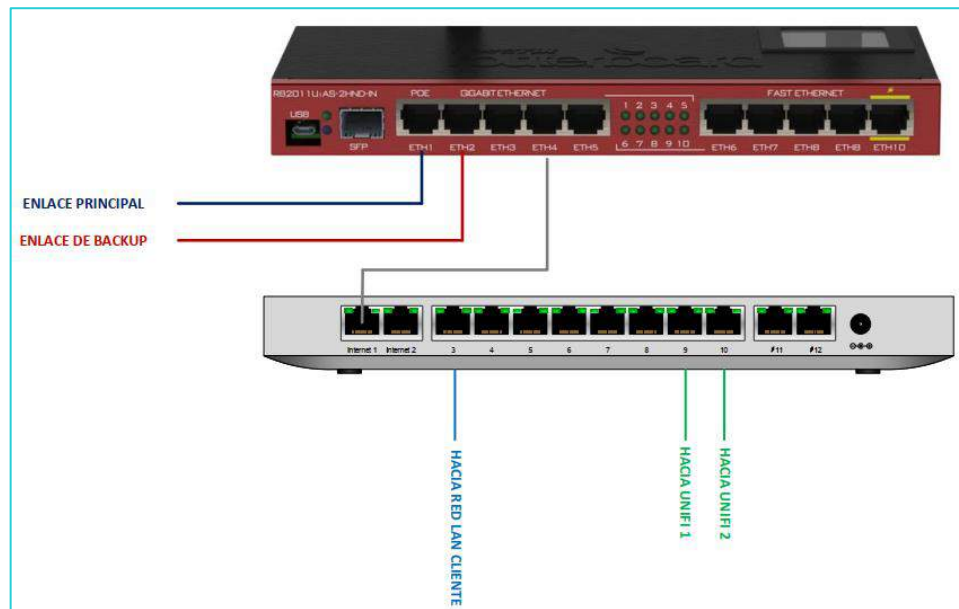
Enlaces de conexión dedicados bajo fibra óptica.

Topología Hub and Spoke

Enlaces con un AB de 5Mbps mediante cable de cobre

Enlace principal una IPsec VPN sobre internet desde el concentrador hacia los equipos merakis.

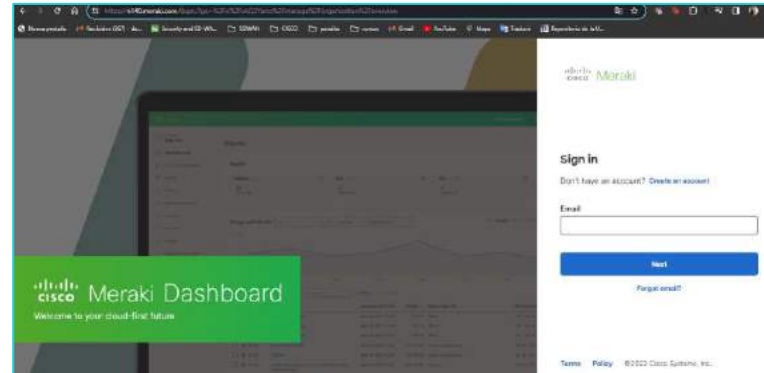
Enlaces backup las conexiones de fibra óptica.



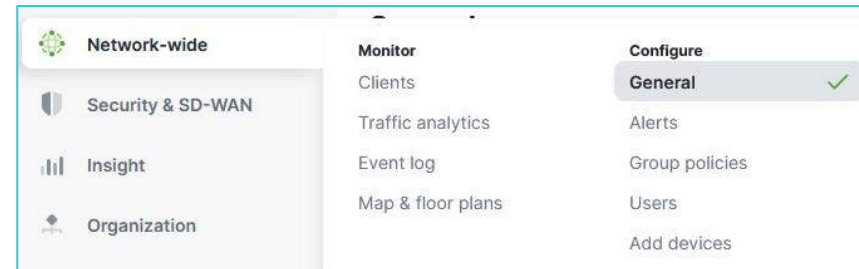
Enlace	IP Pública	Equipo Terminal	Clientes	Ancho de banda	Tecnología
Ambato	190.57.X.X	Meraki MX65	60	15 Mbps	Fibra Óptica
Quito G	190.12.X.X	Meraki MX65	100	35 Mbps	Fibra Óptica
Cuenca DC	190.110.X.X	Meraki MX100	600	50 Mbps	Fibra Óptica
Latacunga	181.188.X.X	Meraki MX65	50	35 Mbps	Fibra Óptica
Riobamba	190.57.X.X	Meraki MX65	400	35 Mbps	Fibra Óptica
Santo Domingo	190.12.X.X	Meraki MX65	80	35 Mbps	Fibra Óptica
Quito L	190.12.X.X	Meraki MX65	80	35 Mbps	Fibra Óptica
Quito M	190.12.X.X	Meraki MX65	300	50 Mbps	Fibra Óptica
San Rafael	179.49.X.X	Meraki MX65	60	35 Mbps	Fibra Óptica

Adquisición y activación de licencias.

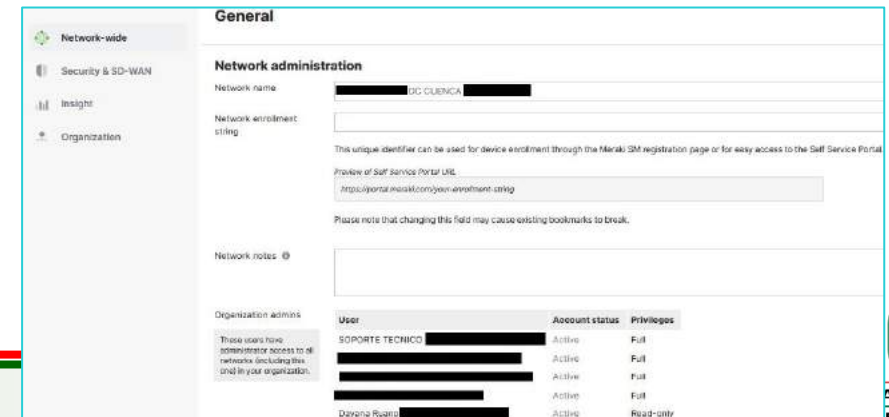
Accedemos al dashboard de Meraki:
<http://dashboard.meraki.com>



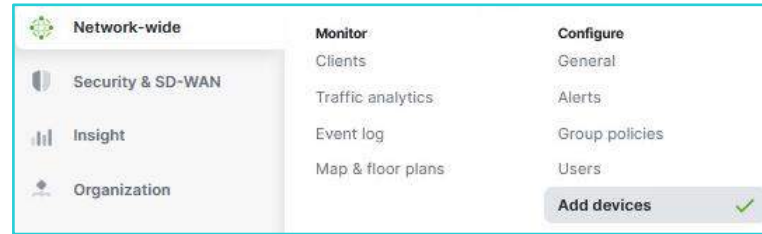
Creación de enlaces o network en la sección de "Network-wide", seleccionar "General".



En la opción de "General" se abre una nueva pantalla, donde definimos el nombre de cada network o enlace.



Agregar el equipo por la serie o mac address a cada network, esto se realiza desde la sección de "Network-wide", seleccionar "Add devices".



En la pantalla se visualizarán las Mac Address y serial numbers de los dispositivos que están disponibles en el sistema para asignarlos a la red de la sucursal que correspondan.

Add security appliances

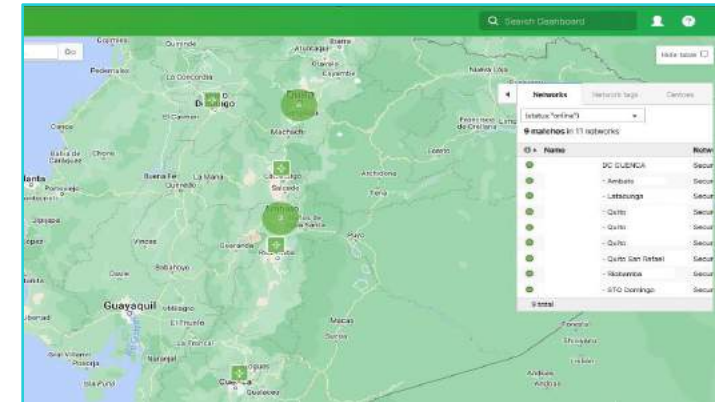
Add security appliances from your organization's inventory. When you claim an order by order number the devices in the order will be added to your inventory. When you claim a device by its serial number that device will be added to your inventory. Once in your inventory, you can add devices to your network(s).

Search inventory

<input type="checkbox"/> MAC address *	Serial number	Model
<input type="checkbox"/> e0:cb:bc:19:fe:33	Q2QN-CG67-HFWN	MX65-HW
<input type="checkbox"/> e0:cb:bc:19:ff:2a	Q2QN-B38N-JYPY	MX65-HW
<input type="checkbox"/> e0:cb:bc:1a:00:bd	Q2QN-9CGU-GVBL	MX65-HW
3 total		

Add security appliances

Se visualizará en el dashboard de la plataforma de Meraki la ubicación de cada agencia en el mapa, para tener un mejor control y administración.



Configurar el direccionamiento y dns de los equipos de forma estática.

The image displays two screenshots of network configuration interfaces for different devices. The left screenshot is for device MX100-CUE-DC, and the right is for MX65-UIO-M. Both show configuration details for WAN 1, including IP addresses, gateway, and DNS settings.

MX100-CUE-DC Configuration:

- General: PUBLIC IP: 190.110. [redacted], corp-190-110: [redacted]
- WAN 1: TYPE: IPv4 (selected), IPv6; CONFIGURED AS: Static; STATUS: Active; IP ADDRESS: 190.110. [redacted]; GATEWAY: 190.110. [redacted]; DNS: 200.105. [redacted], 190.110. [redacted]

MX65-UIO-M Configuration:

- General: PUBLIC IP: 190.12. [redacted], corp-190-12: [redacted]
- WAN 1: TYPE: IPv4 (selected), IPv6; CONFIGURED AS: Static; STATUS: Active; IP ADDRESS: 190.12. [redacted]; GATEWAY: 190.12. [redacted]; DNS: 200.105. [redacted], 190.12. [redacted]



Configurar la red LAN, seleccionamos la sección “Security & SD-WAN”, en las opciones seleccionamos “Addressing & VLANs”, en esta opción, escogemos “Routed” para que el equipo funcione en capa 3 y pueda traducir las direcciones a IP.



En la misma ventana, se realiza la configuración de la LAN y VLANs que requiere el cliente corporativo.



Al finalizar, los puertos del equipo se activan y el tráfico se puede visualizar de manera gráfica sin necesidad de una aplicación adicional.

Addressing & VLANs

Deployment Settings

Mode

Routed

In this mode, the WAN appliance will act as a layer 3 gateway between the subnets configured below. Client traffic to the Internet is translated (NATed) so that its source IP becomes the uplink IP of the WAN appliance. Configures DHCP on the [DHCP settings page](#).

Passthrough or VPN Concentrator

This option can be used for two deployment models: in-line passthrough or one-arm concentrator. In a passthrough deployment, the WAN appliance acts as a Layer 2 bridge, and does not route or translate client traffic.

Routing

LAN setting: **VLANs** | Single LAN

Subnets:

ID	VLAN name	Version	Config	VLAN interface IP	Uplink	Group policy	VPN mode
5	LAN SISTEMAS	Manual	192.168.24	24	Any	None	Enabled
6	VLAN GESTION RED	Disabled	--	--	Any	None	Enabled
7	VLAN 7 INVITADOS	Manual	192.168.24	24	Any	None	Enabled
8	WAN_PALO_ALTO	Manual	10.0.30	30	Any	None	Enabled
10	OFICINAS	Manual	192.168.20	20	Any	None	Enabled

Ports

management, internet

1 2 3 4 5 6 7 8 9 10 11

Historical device data

for the last month

Connectivity

Jan 25 Jan 29 Jan 31 Feb 03 Feb 06 Feb 09 Feb 12 Feb 15 Feb 18

Network usage

WAN 1 WAN 2

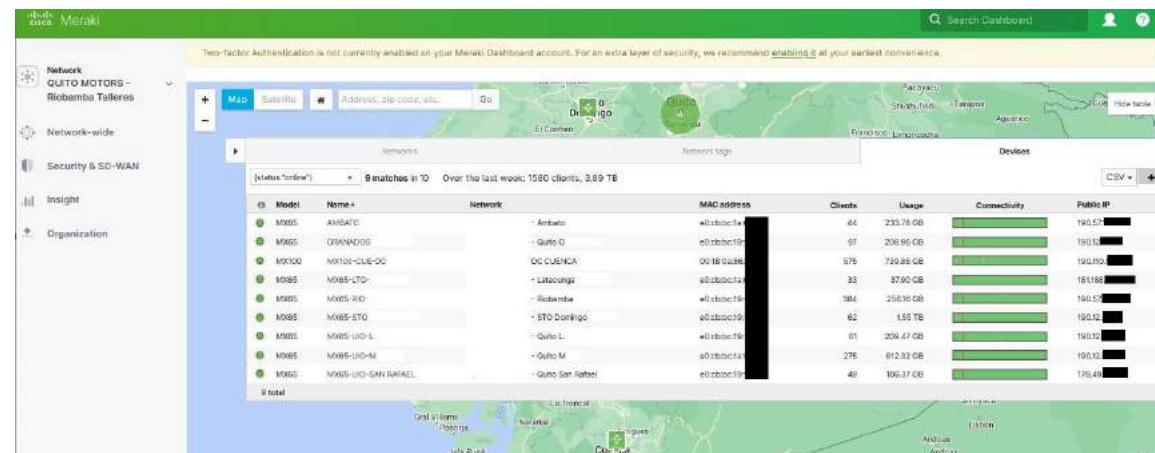
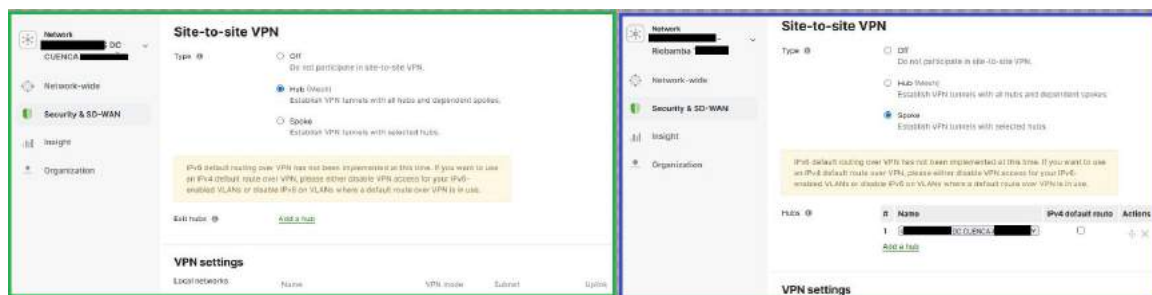
10 Mb/s
8 Mb/s
6 Mb/s
4 Mb/s
2 Mb/s
0 Mb/s

Jan 25 Jan 29 Jan 31 Feb 03 Feb 06 Feb 09 Feb 12 Feb 15 Feb 18



Implementar la VPN site to site con Ipsec.

- Configurar desde el dashboard en la sección “Security & SD-WAN”, opción “Site-to-site VPN”, donde se presentan dos tipos de VPN: Hub y Spoke.
- En el enlace o red de Cuenca DC, se ha seleccionado tipo Hub, ya que en este se encuentra el concentrador de datos y a su vez corresponde al equipo MX100, las demás agencias sucursales, se selecciona tipo Spoke.
- Al finalizar podemos visualizar el dashboard completo para su administración y control.



Configuración de Seguridad

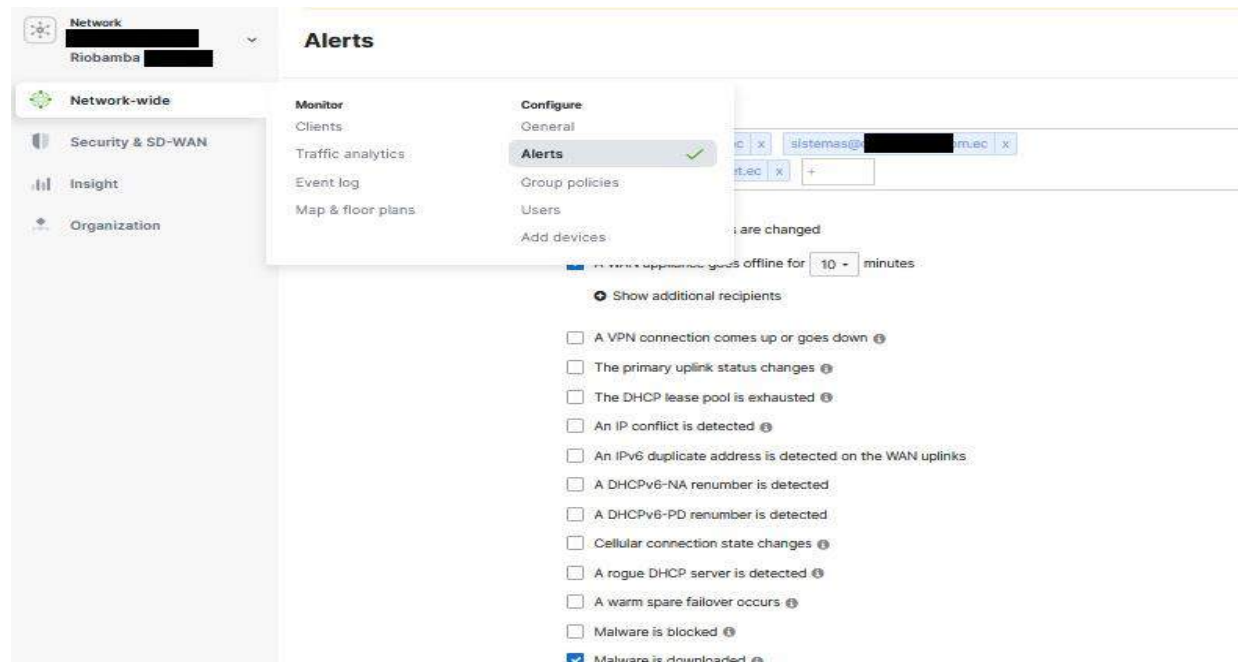
- Crear las reglas de acceso y seguridad de la red, como también bloquear el acceso a ciertas apps o puertos, para mejorar la gestión de la seguridad en la red.
- Configurar desde la sección de “Security & SD-WAN” en la opción “Firewall”

The screenshot displays the 'Layer 3' configuration page for 'Inbound rules' in a network management system. The 'Firewall' option is selected in the 'Configure' menu. The main area shows a table of firewall rules with the following columns: Source, Src port, Destination, Dst port, IPv4 hits, and Enforce.

Source	Src port	Destination	Dst port	IPv4 hits	Enforce
Any	Any	Any	Any	0	<input type="checkbox"/>
Any	Any	Any	25	0	<input type="checkbox"/>
Any	Any	Any	25	0	<input type="checkbox"/>
192.168.255.0/24	Any	192.168.0.0/16	Any	0	<input type="checkbox"/>
Any	Any	Any	Any	69	<input type="checkbox"/>

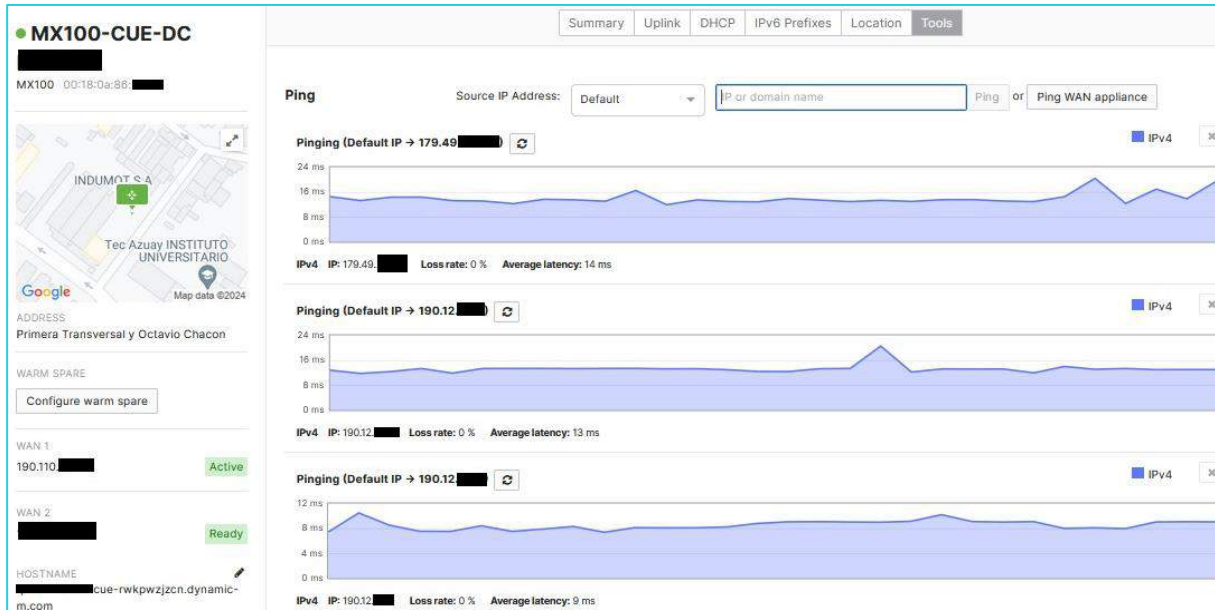
Configuración de Alertas

- Configurar la herramienta denominada “Alerts”, esta herramienta permite seleccionar las cuentas de correo de los usuarios de administración de la red, y a su vez seleccionar los motivos de alerta, los mismo que llegarán como notificación al correo del administrador.
- Esto se configura desde la sección “Network-wide” opción “Alerts”.



Análisis de Resultados

Prueba de latencia (ping) con la herramienta del dashboard desde MX100 hacia los equipos MX65 de las sucursales del cliente corporativo

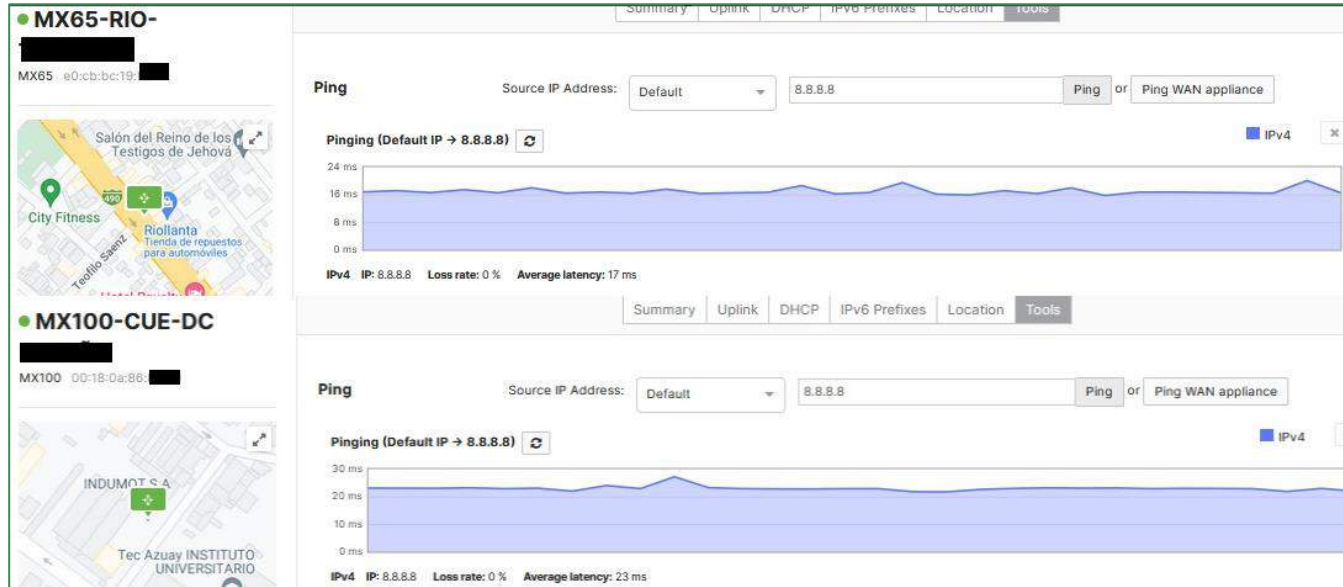


Agencias	Latencia	Tasa de pérdida
Ambato	14 ms	0
Latacunga	12 ms	0
Riobamba	14 ms	0
Santo Domingo	15 ms	0
Quito L	12 ms	0
Quito G	9 ms	0
Quito M	13 ms	0
San Rafael	14 ms	0

El valor de latencia promedio es de 13 ms de los enlaces desde la sucursal de Cuenca que es el punto Hub hacia las demás sucursales como spokes, que representa un valor menor con lo establecido para conexiones VPN donde oscila entre 20 ms y 100 ms



Prueba de latencia (ping) desde las sucursales del cliente corporativo hacia internet.

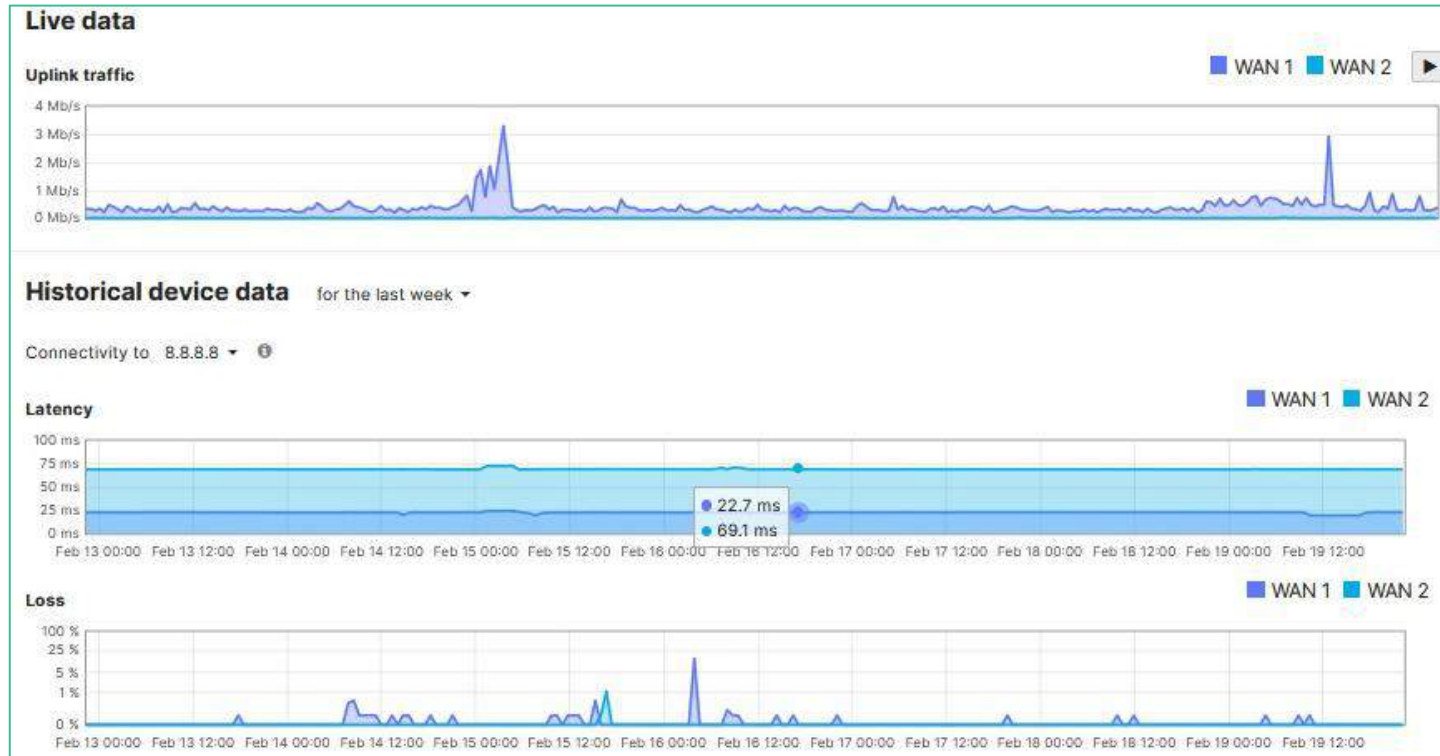


Agencias	Latencia	Tasa de pérdida
Cuenca DC	23 ms	0
Ambato	16 ms	0
Latacunga	15 ms	0
Riobamba	17 ms	0
Santo Domingo	15 ms	0
Quito L	13 ms	0
Quito G	13 ms	0
Quito M	13 ms	0
San Rafael	16 ms	0

El valor de latencia promedio es de 16 ms de los enlaces desde cada una de las sucursales del cliente corporativo hacia el Internet, como se observó en la prueba anterior es un valor menor a 20 ms.



Monitoreo de los enlaces en tiempo real o en períodos de tiempo.

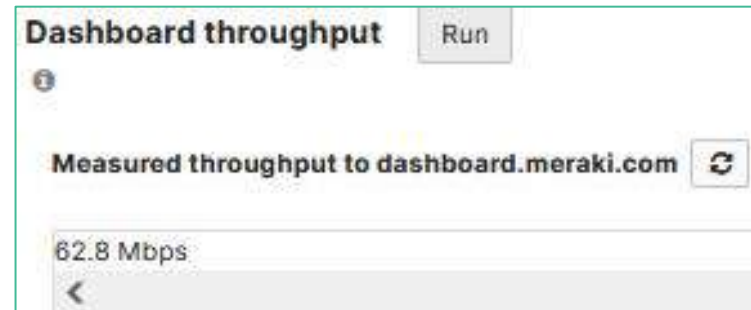


La plataforma de cisco Meraki también nos permite obtener un reporte de latencia y pérdida de paquetes en un período de tiempo, para poder determinar el estado de la red en tiempo real y agilizar la toma de decisiones.



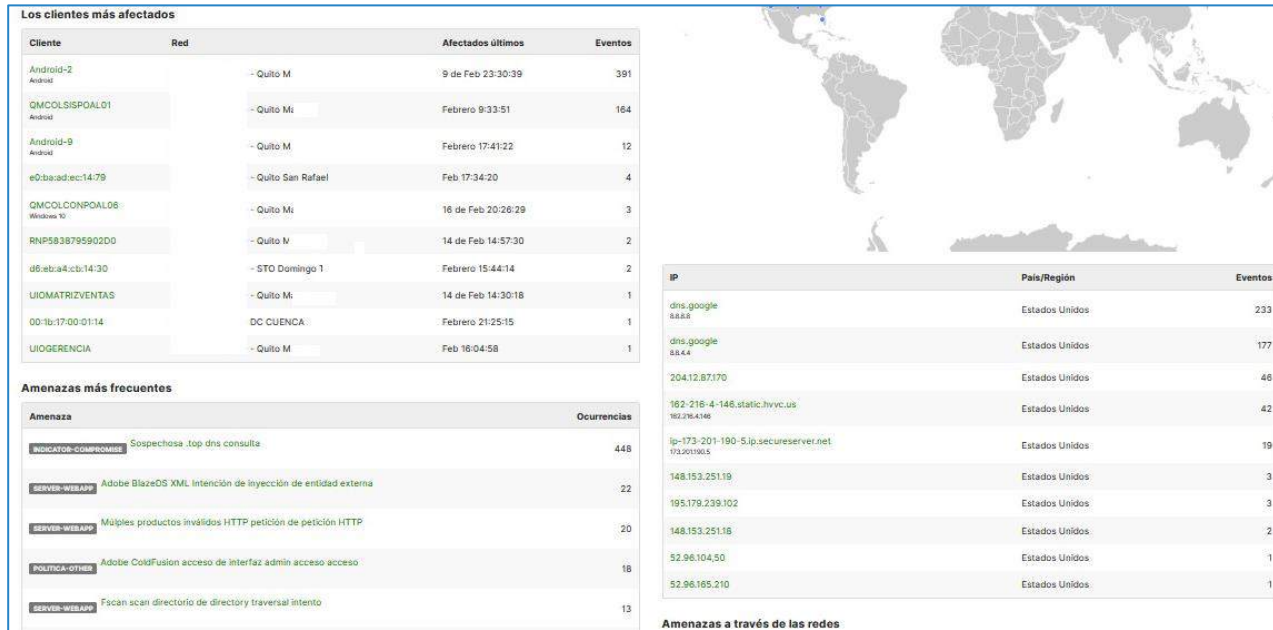
Cálculo de la tasa real de transferencia (throughput)

Agencias	Throughput
Cuenca DC	62.8 Mbps
Ambato	16.7 Mbps
Latacunga	9.1 Mbps
Riobamba	16.9 Mbps
Santo Domingo	8.4 Mbps
Quito L	12.6 Mbps
Quito G	8.2 Mbps
Quito M	60.3 Mbps
San Rafael	12.4 Mbps



Análisis de Resultados

Reporte de Seguridad



Permite tomar acciones efectivas para mejorar la seguridad de la red.

Creación de nuevas reglas en la configuración de firewalls que permitan mejorar la seguridad y control de la red

Identificar los clientes o redes más vulnerables.

Permite limitar el acceso ya sea por vlans o sucursales a diferentes aplicaciones, como redes sociales, juegos, y ciertas plataformas de streaming.



Análisis de Tráfico

Permite visualizar el consumo de ancho de banda que hay en la red.

Visualizar las aplicaciones que se utilizan dentro de la red y la cantidad de clientes que acceden.

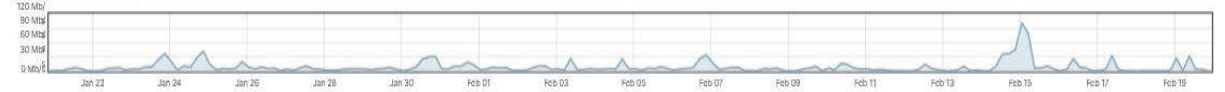
Analizar el balanceo del tráfico como a su vez generar reglas para limitar el tráfico según la importancia de algunas aplicaciones como VoIP.

Traffic analytics for the last 30 days -

Client counts approximately 1560 Unique clients



Usage 2.67 TB (-1.24 TB, ↑ 1.44 TB)



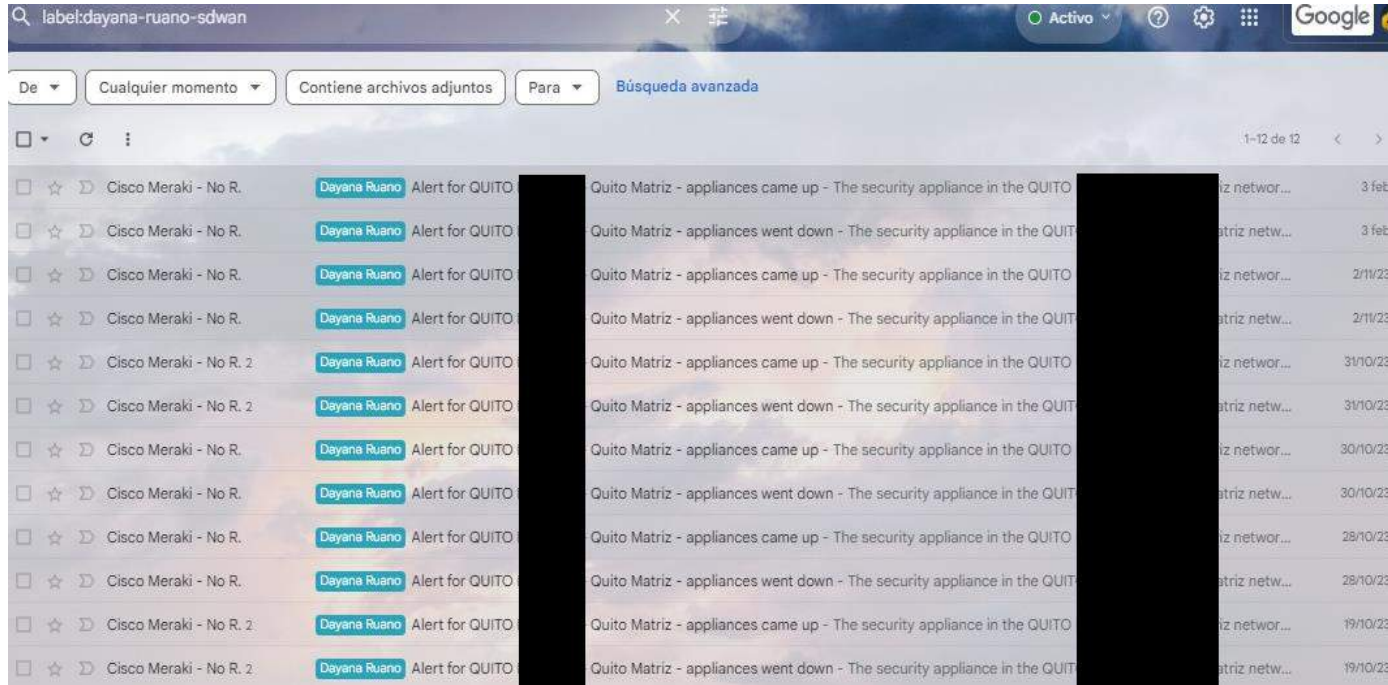
Application	Destination	Country/Region	Protocol	Port	% Usage	Usage Y	Sent	Received	Flows	Active time	# clients
Unknown	-	-	-	-	39.3%	1.05 TB	575.13 GB	498.94 GB	1151076	3.5 months	154
Unknown	-	-	-	-	36.5%	988.55 GB	973.22 GB	25.33 GB	2432	45 days	34
Facebook	-	-	-	-	3.9%	108.02 GB	2.24 GB	105.78 GB	160889	46 days	439
Microsoft Windows Update Service	-	-	-	-	2.3%	63.87 GB	1.46 GB	62.42 GB	96970	16 days	83
Sharepoint	-	-	-	-	2.2%	61.24 GB	57.92 GB	3.32 GB	12405	25 days	20
Remote Desktop Protocol	-	-	-	-	1.8%	44.45 GB	29.60 GB	14.85 GB	13286	11.5 weeks	17
Google Services	-	-	-	-	1.5%	41.40 GB	9.10 GB	32.29 GB	381473	11.2 weeks	807
WhatsApp	-	-	-	-	1.2%	33.06 GB	4.04 GB	29.02 GB	110675	3.2 months	642
Skype	-	-	-	-	1.1%	30.25 GB	1.33 GB	28.92 GB	25347	27 days	530
Akamai	-	-	-	-	1.1%	29.81 GB	478.2 MB	29.34 GB	29501	4.6 days	143
Windows Live Hotmail and Outlook	-	-	-	-	0.9%	23.33 GB	4.18 GB	19.15 GB	70677	3.7 months	98
Encrypted TCP (SSL)	live-ftc-sa-west-1.media.starott.com	US	TCP	443	0.8%	23.19 GB	208.4 MB	22.99 GB	18	6.8 hours	2
Encrypted TCP (SSL)	proditdownloads.galaxionetworks.com	EC	TCP	443	0.8%	20.81 GB	161.5 MB	20.65 GB	1350	26 hours	2
Azure	-	-	-	-	0.8%	20.78 GB	20.17 GB	623.4 MB	9016	5.3 days	32
Real-time Transport Protocol Audio	-	-	-	-	0.7%	19.30 GB	10.51 GB	8.79 GB	9721	10 days	33

* destinations with less than 0.1% of total network traffic are excluded

[Download report as CSV](#)



Reporte de Alarmas



Al usuario dayana.ruano llegan las notificaciones por correo en el caso de haber algún problema de seguridad o caída del enlace en la red de la sucursal Quito M.

Las alarmas en el correo indican el problema existente como también cuando este se soluciona.



Resultados del despliegue de la Red Hub and Spoke sobre SD-WAN

Checks:	
Verificación de SDWAN puede ser configurado en Cisco Meraki MX.	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Facilidad de implementación	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Gestión Centralizada	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Monitoreo de interfaces y tráfico en Tiempo Real	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Herramientas de troubleshooting	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Creación de Redes LAN	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Configuración de Alertas	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Configuración de Usuarios	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Visualización de trafico de usuarios	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Aplicación de políticas de priorización de tráfico	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Aplicación de Políticas de Seguridad	Pass: <input checked="" type="checkbox"/> Fail: <input type="checkbox"/>
Resultados Esperados:	Cisco Meraki SDWAN en MX trabaja según los resultados esperados.

La red del cliente corporativo paso de 40 Mbps con tecnología de cobre a 350 Mbps en fibra óptica.

Servicio Wi-fi en diferentes zonas para clientes y áreas corporativas. Es decir, separados por VLANS.

Administración de las aplicaciones priorizando VoIP.

Control de la red WAN y LAN.

Control del tráfico y anchos de banda.

Gestión de la seguridad.

Gestión centralizada y automatización.



CONCLUSIONES

- En el estudio de la tecnología SD-WAN para aplicación en diseños de redes corporativas, se logró concluir que es más conveniente a diferencia de tecnologías como MPLS y VPN, como se evidencio en la comparativa, donde se pudo comparar las tres tecnologías, siendo SD-WAN una tecnología más completa que permite a las redes corporativas adaptabilidad y escalabilidad junto al desarrollo de las telecomunicaciones a la era digital.
- Se consideró los diferentes proveedores de tecnología SD-WAN existentes, concluyendo como mejor opción los equipos Cisco Meraki ya que en Ecuador son los más utilizados por otras empresas, adicional es la opción prioritaria del proveedor de servicios de internet corporativo.
- Se desarrollo el diseño de la red, tomando los antecedentes y requisitos de la red antigua del cliente corporativo, permitiendo con el nuevo diseño bajo la tecnología SD-WAN, reducir el número de dispositivos que eran usados por la tecnología MPLS que antes tenía el cliente, como a su vez reducción de costos al no usar enlaces dedicados sino VPN sitio a sitio bajo IPsec como enlaces de fibra que son menos costosos y su ancho de banda es mayor desde 15 Mbps hasta 1Gbps.
- Se implemento una topología Hub and Spoke dado que los equipos cisco Meraki tienen esta limitación en el desarrollo de su software, seleccionando como Hub a la sucursal donde se encuentra la central de datos y las demás sucursales se configuraron como spoke, permitiendo una gestión centralizada.



CONCLUSIONES

- Se realizó pruebas de latencia entre los enlaces de las sucursales hacia la salida de internet como también entre la sucursal designada como Hub y las sucursales spoke, donde el valor promedio en los dos casos fue menor a 20 ms como se muestran en las tablas 4 y 5 de resultados, esto nos indica que la latencia obtenida es menor al promedio que se obtiene en enlaces de VPN y fibra óptica que varía entre 20ms a 100ms.
- Se reviso la herramienta de seguridad que tiene el dashboard de Meraki, donde se puede observar las amenazas registradas en cada red de las sucursales como general, lo que permite disminuir las vulnerabilidades que puede presentar la red corporativa. Crear nuevas reglas para aplicar en el firewall que viene integrado dentro del dashboard.
- Se verifico el funcionamiento de la herramienta de análisis de tráfico que permite tomar decisiones precisas para el balanceo de carga en el tráfico de la red, como también establecer políticas que limiten el ancho de banda para ciertas aplicaciones y a su vez generar prioridad para otras, limitar el acceso a ciertas aplicaciones como redes sociales, juegos, etc en cada vlan de la red.
- En la implementación se concluyó que es más sencillo la configuración de la red, ya que solo es necesario conectar el equipo Meraki con una licencia activa a una fuente de internet, ingresar al dashboard de Meraki con la cuenta asignada al usuario, configurar y realizar soporte remotamente.



CONCLUSIONES

- Se conoció varias herramientas y funciones que presenta el dashboard de Meraki, las mismas que facilitan la administración y automatización de la red, como por ejemplo las notificaciones de alarmas que llegan a los correos de los administradores de la red cuando hay algún inconveniente o caída de los enlaces.
- El diseño e implementación de la red del cliente corporativo bajo la tecnología SD-WAN evidenció los varios beneficios que se obtiene al migrar a esta tecnología permitiendo que otros clientes del proveedor de servicios de internet se interesen por este tipo de tecnología que adicional va de la mano con el crecimiento de las telecomunicaciones en la era digital, IoT y cloud.



RECOMENDACIONES

- Conocer los objetivos comerciales y tecnológicos que requiere el cliente corporativo, como los antecedentes de la red actual, incluyendo la topología, tecnología y calidad del servicio, para realizar un preciso diseño de red.
- Identificar y priorizar las aplicaciones críticas para la red del cliente corporativo. Configurar la SD-WAN para optimizar el tráfico de estas aplicaciones y garantizar su rendimiento.
- Después de la implementación del nuevo diseño de red, dar un monitoreo continuo para evaluar el rendimiento de la red. Ajustar la configuración según sea necesario del cliente corporativo.
- Realiza auditorías de seguridad periódicas para garantizar que la SD-WAN cumpla con las políticas de seguridad de la organización y para identificar y abordar posibles vulnerabilidades.
- Seleccionar proveedores de SD-WAN confiables que se ajusten a las necesidades de la red, considerando que este sea compatible con los equipos que se posee para generar un costo menor, como también que sean escalables y con una fácil gestión de soporte.
- Para la implementación es muy importante verificar que las licencias de los equipos Meraki estén activas, ya que sin una licencia no hay como configurar las características que son necesarias para que este acceda a la red de SD-WAN en la nube.



TRABAJOS FUTUROS

- Como trabajos futuros se propone realizar un estudio de cada una de las funciones que dispone el dashboard de Cisco Meraki, para poder sacar más beneficios de las herramientas.
- Comparar la tecnología Cisco Meraki con otro proveedor de servicio de SD-WAN como Fortinet o VMware, al ser los proveedores más utilizados en Ecuador.
- Realizar un estudio sobre el avance de la tecnología SD-WAN en el Ecuador para permitir que más empresas opten por esta tecnología y mejorar la brecha digital en el país.





GRACIAS POR SU
ATENCIÓN



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA