ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

DISEÑO DE UNA iWAN

OPTIMIZACIÓN DE APLICACIONES PARA REDES INTELIGENTES WAN (iWAN) EMPRESARIALES

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

CARLOS ANDRÉS MONTALVO CHICAIZA

carlos.montalvo@epn.edu.ec

DIRECTOR: CARLOS ALFONSO HERRERA MUÑOZ

carlos.herrera@epn.edu.ec

Quito, marzo del 2022

CERTIFICACIONES

Yo, CARLOS ANDRÉS MONTALVO CHICAIZA declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

CARLOS ANDRÉS MONTALVO CHICAIZA

Certifico que el presente trabajo de integración curricular fue desarrollado por CARLOS ANDRÉS MONTALVO CHICAIZA, bajo mi supervisión.

CARLOS ALFONSO HERRERA MUÑOZ

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el producto resultante del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

NOMBRE_ESTUDIANTE CARLOS ANDRÉS MONTALVO CHICAIZA

NOMBRE_DIRECTOR CARLOS ALFONSO HERRERA MUÑOZ

NOMBRE_COLABORADOR(ES)

DEDICATORIA

Este logro profesional va dedicado principalmente para mi mamá, por ser un apoyo incondicional y brindarme toda la confianza para poder desarrollarme como profesional, a mi abuelita, por todas sus enseñanzas y valores que desde muy niño me los inculco, también para mis tías, tíos y abuelito que siempre supieron darme una palabra de aliento para culminar con mis estudios.

AGRADECIMIENTO

Doy gracias a Dios por permitirme la oportunidad de estudiar, a mi madre por darme las facilidades que se necesitan para estudiar en otra ciudad, a todos mis compañeros de la Universidad que a la final se hicieron mis grandes amigos después de tantos días largos de estudio y tantas vivencias juntos, a mis amigos de toda la vida que son como mis hermanos que se hicieron presentes siempre con palabras de apoyo y ánimo para que siga adelante, finalmente agradezco a mi novia que estos últimos semestres siempre me dio fortaleza para culminar con mis estudios e igual me acompaño en mis desvelos por estudiar y realizar trabajos.

También agradezco al Ing. Carlos Alfonso Herrera Muñoz por guiarme en este semestre paso a paso ya que gracias a su paciencia y conocimientos se pudo lograr de mejor manera el Trabajo de Integración Curricular.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE COMANDOS

RESUMEN

Las redes iWAN surgen por la necesidad y la falta de recursos, los cuales eran deficientes con las redes WAN, gracias a los avances tecnológicos cada vez se requiere de mayor ancho de banda, movilidad, conectividad, disponibilidad, entre otros.

El presente trabajo consta de cuatro capítulos, busca optimizar las aplicaciones de la red inteligente WAN (iWAN) a través de nuevas tecnologías propuestas por CISCO.

En el capítulo I se presenta las generalidades de la red iWAN, como son fundamentos de la red iWAN, en donde encontraremos las deficiencias y problemáticas de la red WAN, también encontraremos los componentes principales de la red iWAN y un detalle de los más importantes, por ultimo veremos una introducción de las tecnologías que nos ayudan con la optimización de aplicaciones.

En el capítulo II se estudia las tecnologías Cisco WAAS presentando soluciones a los problemas recurrentes y falencias que tiene la red WAN, también se describirá Cisco AVC, detallando las ventajas de usarlos para las redes inteligentes WAN (iWAN) y por último se recopilará información de optimización de flujo TCP.

En el capítulo III se detalla las configuraciones y características para la implementación de optimización de aplicaciones para redes inteligentes WAN (iWAN). Se explicará cómo se deben configurar los diferentes componentes de WAAS y AVC para iWAN.

Por último, en el capítulo IV se exponen los resultados que son las principales diferencias entre una red WAN de una iWAN y sus beneficios. También se detallan conclusiones y recomendaciones del trabajo realizado.

PALABRAS CLAVE: iWAN, optimización, WAAS, AVC, TCP.

ABSTRACT

iWAN networks arise from necessity and lack of resources, which were deficient in WAN networks. As a consequence of technological advances, greater bandwidth, mobility, connectivity, availability, among others, are increasingly required.

The presented work consists of four chapters that pursue optimizing the applications of the intelligent WAN network (iWAN) by new technologies proposed by CISCO.

In Chapter I presents the generalities of the iWAN network, such as the fundamentals of the iWAN network, where we will find the deficiencies and problems of the WAN network. In addition, we will also find the main components of the iWAN network and a detail of the most important ones. At the end of the chapter, we will see an introduction to the technologies that help us with the optimization of applications.

In chapter II, Cisco WAAS technologies are studied, presenting solutions to recurring problems and shortcomings that the WAN network has. Similarly, Cisco AVC will be described by detailing the advantages of using them for intelligent WAN networks (iWAN). As a result, TCP stream optimization information will be recorded.

Chapter III details the configurations and characteristics for the implementation of optimization applications for intelligent WAN networks (iWAN). It will be explained how the different components of WAAS and AVC for iWAN should be configured.

Finally, chapter IV presents the results that are the main differences between a WAN network and an iWAN and its benefits. Additionally, the conclusions and recommendations the work accomplished are detailed.

KEYWORDS iWAN, optimization, WAAS, AVC, TCP.

1 INTRODUCCIÓN

En la actualidad debido al requerimiento de altos recursos para la implementación de las Redes WAN, la empresa CISCO ha propuesto las Redes inteligentes WAN (iWAN).

Esta tecnología de Cisco iWAN es una red, la misma que reduce el costo de la implementación para redes WAN, sin dejar a un lado la mejoría que brinda al rendimiento de aplicaciones que van hacia la nube de Internet. La tecnología Cisco iWAN formula la utilización de una red completamente independiente WAN con el control de trayecto inteligente, la optimización de la aplicación y la conectividad con buen rendimiento y con seguridad. [1]

La tecnología iWAN aprovecha los recursos para la implementación WAN en base a la capacidad de ancho de banda y su uso óptimo.

Como punto principal de la tecnología iWAN a diferencia de WAN es la reducción de costos que brinda, lo que se da debido a la infraestructura de la red y también que libera recursos, para futuras innovaciones tecnológicas.

La tecnología antigua se ha visto exigida por lo que los requerimientos de red que son diferentes por lo que ha tenido que avanzar continuamente, ya que, con la llegada de los smartphones, tabletas, aplicaciones a la nube, video, etc., ha sido cada vez más altos los requerimientos a alcanzar. La cifra de dispositivos por persona alcanza hasta a 2.4 dispositivos por persona, anteriormente el promedio solo era de 1.7.

Por la demanda que va en aumento el encontrar un mayor ancho de banda ha sido uno de las principales labores de los departamentos de TI (Infraestructura Tecnológica), debido a que con una video llamada se puede llegar a saturar una de las sucursales, generando un ancho de banda WAN bastante congestionado lo cual puede desatar riesgos a la seguridad, respuesta lenta a las necesidades del negocio, entre otros.

La tecnología Cisco iWAN, brinda una conversión rápida entre conexiones WAN con un transporte de Internet menos costoso y sin afectar al rendimiento, confiabilidad y seguridad de aplicaciones. Se asegura una confiabilidad del 99.9%, ya sea por MPLS, Internet o de WAN híbrida. [1]

Las diferencias en su estructura de iWAN y WAN, se indican en la Figura 1.1.

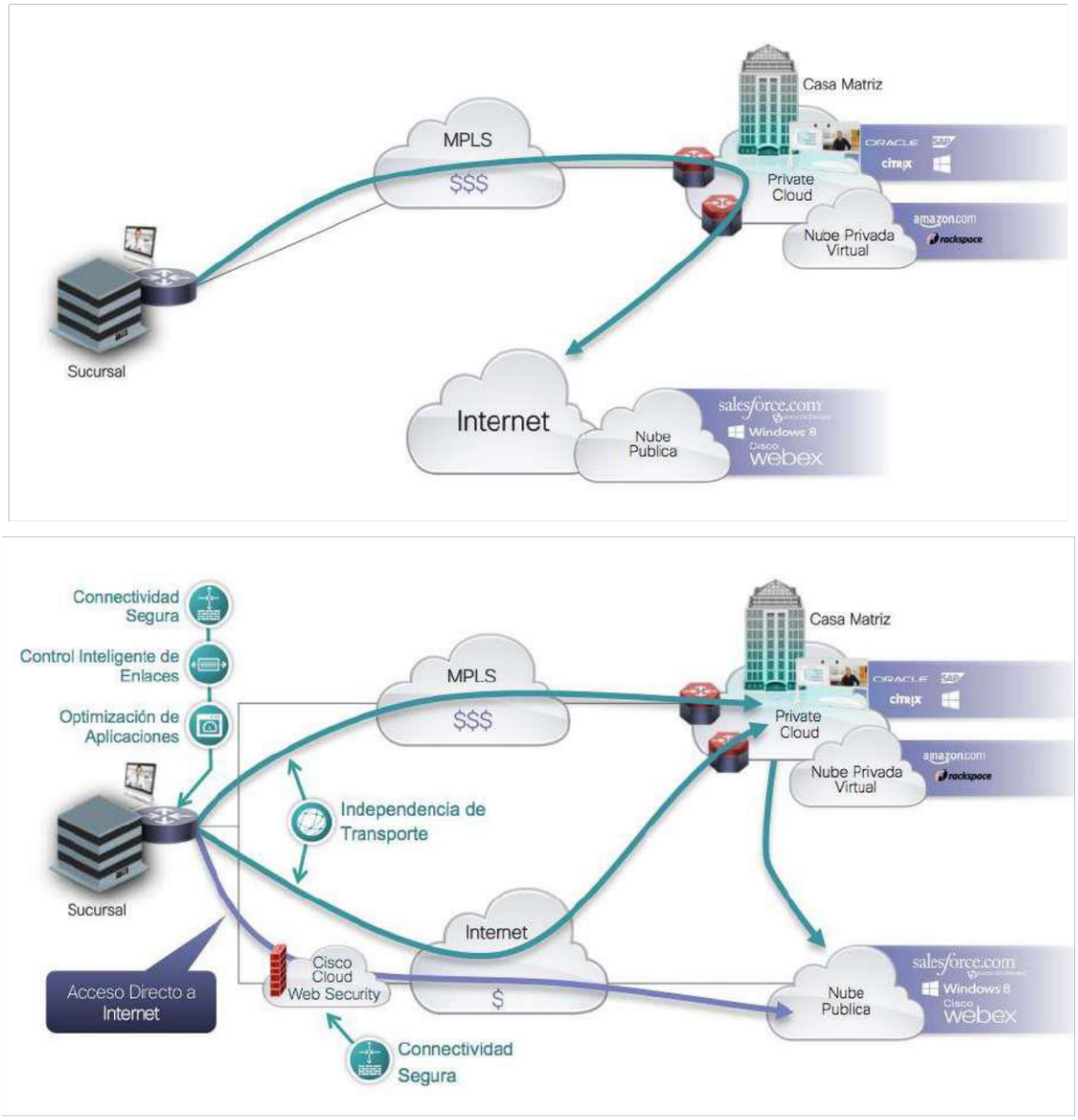

Figura 1.1. Diferencias de estructura de WAN vs iWAN [1]

Con la tecnología de CISCO iWAN, aprovechamos DMVPN (Dynamic Multipoint VPN) y PfRv3 (Performance Routing), para proveer una red WAN híbrida, es decir tanto de MPLS más Internet o WAN basada solo en Internet.

La misión de la tecnología de Cisco iWAN es reducir los precios, a niveles incluso más económicos que los costos de MPLS. Lo que se puede lograr gracias a la tecnología PfR3,

gracias a que así el tráfico pasa directo a Internet sin pasar por el núcleo de la red reduciendo costos de tráfico.

El presente trabajo tiene como objetivo optimizar aplicaciones mediante las tecnologías WAAS, AVC y flujo de tráfico TCP. El estudio principal va hacia estas tecnologías, sobre todo su configuración, estructura, arquitectura y sus componentes importantes a la hora de aplicar dichas tecnologías. [1]

1.1 Objetivo general

El objetivo general de este Trabajo de Integración Curricular es:

- Optimizar aplicaciones para redes iWAN empresariales.

1.2 Objetivos específicos

Los objetivos específicos de este Trabajo de Integración Curricular son:

- Estudiar los conceptos básicos de optimización de las redes inteligentes WAN (iWAN) y sus componentes principales.
- Describir la tecnología Cisco WAAS, configuraciones y sus diferentes beneficios que presenta para las redes inteligentes WAN (iWAN).
- Describir la tecnología Cisco AVC.
- Recopilar información sobre optimización de flujo TCP y compresión avanzada.

1.3 Alcance

Las redes WAN han ido evolucionando por el constante crecimiento de usuarios, la cantidad de información que se maneja hoy en día, el aumento de capacidad que se requiere y otras características más, por lo que se requiere que las Redes iWAN tengan

mejor acceso a nuestros datos y a las diferentes aplicaciones para lograr mejor desempeño de las Redes iWAN.

- En el presente trabajo se va a describir los fundamentos de iWAN, el estudio de las tecnologías que permitan optimizar aplicaciones de usuario en base a las tecnologías WAAS, AVC y estudiar la optimización de flujo TCP. [4]
- En la tecnología WAAS se describirá su arquitectura y los componentes básicos para realizar la optimización de aplicaciones en las redes iWAN.
- En la tecnología AVC se especificará su uso, los dispositivos compatibles y las configuraciones necesarias para una red iWAN básica.
- En la optimización de flujo TCP se realizará un estudio sobre conceptos básicos y su forma de usarlo con la tecnología WAAS debido a que estas dos tecnologías van de la mano.

En base a una topología de red empresarial, se describirá la configuración básica de los equipos para el correcto uso de estas tecnologías como son CISCO WAAS, AVC y optimización de flujo TCP.

1.4 Marco teórico

A continuación, se indica un resumen teórico que permita entender los conceptos básicos y saber de mejor manera como están funcionando las Redes iWAN.

1.4.1 Componentes de la tecnología iWAN

Las redes iWAN están conformadas con los siguientes componentes:

1.4.1.1 DMVPN (Dynamic Multipoint VPN)

DMVPN es una tecnología de enrutamiento que se utiliza para construir redes VPN con múltiples sitios sin una configuración estática de todos los dispositivos. Esta es una red de "hub y spoke" donde los radios pueden comunicarse directamente entre sí sin pasar por un

centro. El cifrado compatible se realiza mediante IPsec, lo que hace que DMVPN se considere una de las mejores opciones para conectar diferentes sitios mediante una conexión a Internet normal. Es una muy buena copia de seguridad/alternativa a las redes privadas como MPLS VPN, y una alternativa muy conocida a DMVPN es FlexVPN.

La tecnología DMVPN es una solución de software de Cisco que sirve para crear VPN IPsec escalables. La arquitectura planteada por CISCO DMVPN se basa en la ejecución y administración sencillas para redes que requieren control de acceso para diferentes grupos de usuarios, incluidos clientes/trabajadores móviles y usuarios domésticos.

CISCO DMVPN brinda a todas las sucursales acceso para comunicarse entre sí directamente a través de una WAN pública o Internet, similar al uso de Voz sobre IP entre dos sucursales, pero no requiere una conexión VPN permanente entre sitios. Nos permite implementar IPsec VPN, lo que mejora el rendimiento de la red al reducir la latencia y la inestabilidad, al tiempo que optimiza el uso del ancho de banda de la oficina central. [2]

En la Figura 1.2. se presenta un diagrama de la Red iWAN propuesta.

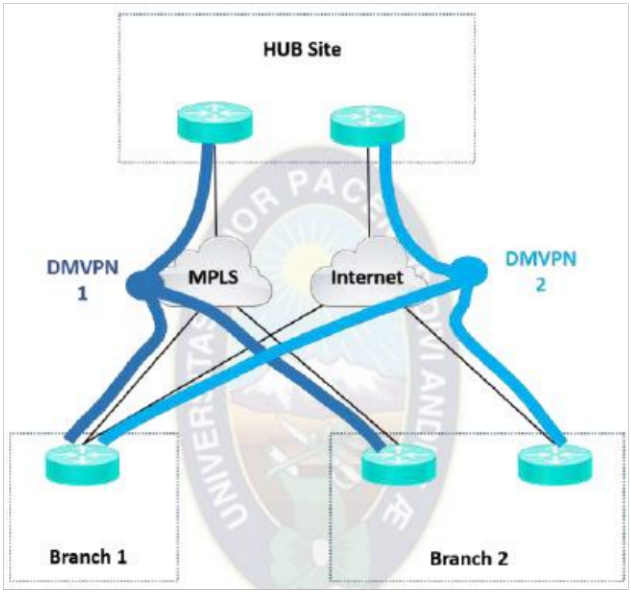

Figura 1.2. Diagrama de la Red iWAN propuesta [1]

Se pueden observan líneas gruesas las cuales son túneles DMVPN encriptados y tenemos uno para MPLS y el otro de Internet. Los mismos que proveen una conectividad cifrada y segura entre las sucursales y el hub. [1]

Componentes DMVPN: [3]

- Varias interfaces de túnel GRE: única interfaz GRE, reduciendo el alcance general de la configuración DMVPN protegiendo túneles IPsec.

- Descubrimiento de puntos finales de túnel IPsec: Significa que no es necesario configurar asignaciones criptográficas estáticas entre puntos finales de túnel IPsec individuales.
- Protocolos de enrutamiento: permiten que DMVPN localice rutas diferentes de manera mucho más acertada.
- NHRP: implementan radios con direcciones IP asignadas las cuales después se conectan desde el concentrador DMVPN central.

Fases de DMVPN [4]

Existen tres distintas fases de diseño de DMVPN, y se resumen a continuación:

- La Fase 1 de DMVPN se implementa mediante túneles HUB-and-Spoke. Los túneles que establecen las conexiones de sucursal a sucursal se construyen solo a través del concentrador DMVPN central y los radios individuales, y funcionan muy parecido al sistema VPN tradicional.
- La Fase 2 de DMPVN se implementa mediante túneles de radio a radio, lo que significa que los datos no tienen que transmitirse primero a un concentrador central, siempre que la red de radio tenga una ruta específica.
- La Fase 3 de DMPVN permite la implementación de túneles de radio a radio sin rutas pre construidas específicas, en lugar de asegurar estas rutas sobre la marcha utilizando mensajes de indicación de tráfico NHRP de los concentradores.

1.4.1.2 Control de trayecto inteligente PfR3 (performance routing)

Cisco *Performance Routing (PfR),* es un componente de control de ruta inteligente de iWAN, la misma que ayuda a los administradores en lo siguiente:

- Menor costo de Internet gracias al aumento de la WAN con un ancho de banda mayor.
- Puede elegir las tecnologías de transporte como: MPLS L3VPN, VPLS o Internet.
- Tiene beneficios de costos por la flexibilidad del proveedor.

- Puede descargar la WAN corporativa con acceso a Internet altamente seguro.
- Mejora notablemente el rendimiento y disponibilidad de aplicaciones, según sea el requerimiento de rendimiento de la aplicación.

CISCO Performance Routing (PfR) ayuda a la eficiencia de la WAN y entrega de aplicaciones. PfR observa parámetros como el tipo de aplicación, las políticas, el rendimiento y el estado de ruta para controlar dinámicamente el reenvío de paquetes; también protege aplicaciones tipo empresariales del rendimiento de la WAN y se equilibra la carga del tráfico inteligentemente sobre la mejor ruta en base a su rendimiento. [5].

Para una WAN empresarial.

El control de la ruta inteligente de iWAN es clave para proporcionar una WAN de clase empresarial sobre el transporte por Internet. Como se observa en la Figura 1.3 una topología básica de PfR en iWAN. [1]

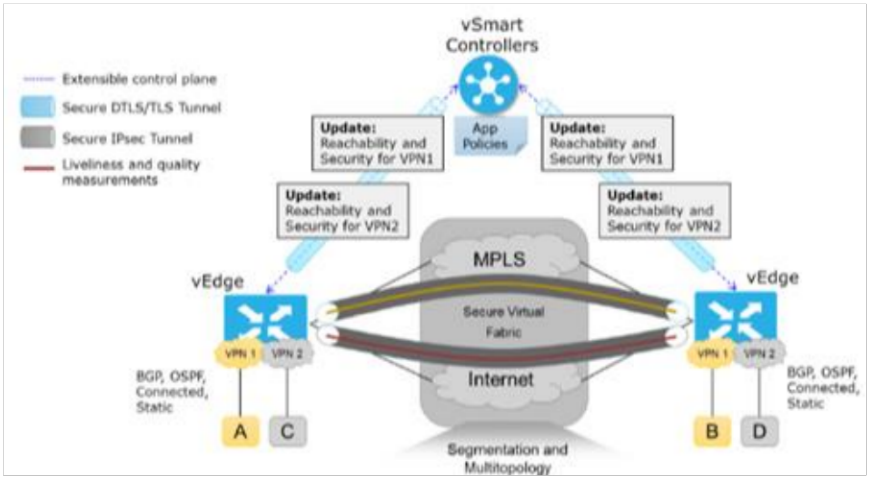

Figura 1.3. Topología Básica PfR en IWAN [1]

Los ruteadores de borde (BR): están en la ruta de reenvío de datos. Los ruteadores vecinos seleccionan datos y los coleccionan de su caché de Monitor de rendimiento y de los resultados de la sonda inteligente, influyen en la ruta de reenvío de paquetes como fue indicado por el Controlador Maestro (MC) para la administración del tráfico de usuarios.

Controlador Maestro (MC): Este es el que toma decisiones. Tenemos diferentes MC, para un sitio grande, el MC es un chasis independiente; para sucursales más pequeñas el MC en ocasiones se encuentra en la plataforma del ruteador de borde. Se usa siempre en sitios grandes un chasis para el MC por lo que administran más prefijos y aplicaciones de red que una sucursal más pequeña. [1]

1.4.1.3 Optimización de aplicaciones

Entre las tecnologías que optimizan las aplicaciones, tenemos: Cisco Application Visibility and Control (AVC) y *Wide Area Application Services* de Cisco (WAAS), las mismas que nos ofrecen optimización del rendimiento sobre la aplicación WAN. Para aumentar el espacio de las aplicaciones es importante aumentar la reutilización de puertos conocidos, ya que así se observa un mejor rendimiento de la red.

Gracias a Cisco WAAS, se puede acelerar las aplicaciones y también optimizar el tráfico en las redes tanto cableadas como inalámbricas. Se obtiene beneficios de optimización WAAS en los departamentos de tecnología e información, ya no necesitan actualizar cada determinado tiempo, sino que aumenta el periodo, lo cual es bueno ya que estas actualizaciones consumen un gran ancho de banda de la WAN. [1]

Lo que llama la atención de Cisco WAAS, también es su facilidad de uso, sin dejar atrás la aceleración de aplicaciones y que a su vez minimiza el consumo de ancho de banda de la WAN. Resolviendo constantemente problemas sobre tiempos de respuesta en aplicaciones, consolidación de servidores y también, por último, corrigiendo la *performance* de los servicios centralizados, elevando los niveles de performance de servicios. [6]

1.4.1.4 Conectividad segura (IPsec)

La Red iWAN protege la Red WAN y al mismo tiempo descarga el tráfico de clientes directamente hacia Internet. Se utiliza algunas tecnologías para proteger la red WAN sobre la Internet pública como puede ser la IPSec fuerte, los Firewall basados en zona, y listas de acceso estrictas. La manera de mejorar el rendimiento de la aplicación pública de la nube y a su vez reducir el tráfico sobre la red WAN es rutear a los usuarios de la infraestructura de red directamente hacia Internet. [1]

1.4.2 Ventajas de la tecnología iWAN

A continuación, se muestran ventajas más sobresalientes sobre la red e infraestructura que se tiene gracias a la tecnología Cisco iWAN.

- El retorno de inversión de la red iWAN es mucho más rápido en comparación de con la red WAN, debido a que gracias a iWAN se aprovecha de mejor manera los recursos de la red WAN y evita que se invierta en compra de líneas de proveedores.
- Se disminuye en la infraestructura debido a la flexibilidad y plazos de prestación de servicios con iWAN, gracias a que los administradores de red pueden usar una variedad de proveedores ISP (Proveedor de Servicios de Internet) se tiene una disminución en el costo del transporte sin afectar al rendimiento, confiabilidad y seguridad de la red.
- Tenemos la opción de descargar el tráfico eficientemente con Cisco Cloud Web Security (CWS) para brindar una conexión segura a todas las sucursales, a la vez que se afirma la conectividad en todas las sucursales.
- Al tener el reconocimiento de aplicaciones se tiene una optimización del rendimiento de la red WAN, debido a que se tiene visibilidad y control general de a qué nivel puede ser configurada la red, asegurándonos así de resolver problemas de red rápidamente, administrando servicios importantes para la empresa.
- La compresión avanzada minimiza en gran medida el consumo de ancho de banda en la red WAN.
- Usando una transferencia de datos redundante como resultado se tendrá aplicaciones con mejor rendimiento.[1] [7]

2 OPTMIZACIÓN DE APLICACIONES INTELIGENTES iWAN

Las ventajas que se tiene sobre la optimización WAN son: la reducción de costos en infraestructura y ancho de banda, se mejora en gran medida la productividad, la aceleración de aplicaciones y mejor seguridad en los datos. [8]

En este capítulo se habla de las tecnologías más importantes que plantea como solución Cisco. Ya que tenemos 3 tecnologías importantes que son WAAS, AVC y optimización de flujo TCP.

2.1 WAAS

Cisco WAAS (*Wide-Area Aplication Services*) se considera una solución práctica para acelerar las aplicaciones y reducir el consumo de ancho de banda de la WAN a través del enrutamiento consciente de las aplicaciones y la optimización del tráfico. Por las razones anteriores, WAAS ayuda a resolver problemas de tiempo de respuesta en las aplicaciones, ayuda a consolidar servidores y optimiza el rendimiento de los servicios centralizados.

Beneficios de Cisco WAAS: [6]

- Una mejor experiencia de usuario con aplicaciones y servicios críticos para el negocio aumenta la productividad de los empleados.
- Reducir ancho de banda de la WAN y costos operativos de todas las sucursales.
- Reduce el tiempo y los recursos que TI necesita para dar servicio a las sucursales.
- Promover la protección de datos y la continuidad del negocio.

Solución WAAS de Cisco.

Combinando técnicas de optimización de TCP y funciones de aceleración de aplicaciones, Cisco WAAS puede mejorar aspectos importantes, incluso dejar atrás problemas comunes que eran asociados con el tráfico de una WAN. [9]

2.1.1 Aceleración específica de la aplicación

Cisco WAAS incluye estas funciones de aceleración de aplicaciones: [10]

- Predicción de operación y procesamiento por lotes: reduce los viajes de ida y vuelta de la WAN al transformar la secuencia de comando a una más corta.
- Supresión inteligente de mensajes: cada dispositivo WAAS tiene proxies de aplicaciones, que sirven para responder a los mensajes localmente, lo cual hace que el cliente no espere una respuesta del servidor remoto. *"Los proxies de aplicaciones utilizan una variedad de técnicas que incluyen el almacenamiento en caché, el procesamiento por lotes de comandos, la predicción y la captación previa de recursos para aumentar el tiempo de respuesta de las aplicaciones remotas".*
- Almacenamiento en caché WAFS: Es más rápido porque cada dispositivo WAAS responde solicitudes de los clientes usando datos almacenados en caché local, en vez de buscar datos de servidores de aplicaciones y archivos remotos.
- Preposición: el dispositivo WAAS obtiene datos de recursos e introduce datos antes de que el cliente haga una solicitud futura.

Cisco WAAS usa módulos de software de aplicaciones inteligentes, para aplicar estas funciones de aceleración.

2.1.2 Arquitectura WAAS de Cisco

La Arquitectura WAAS de Cisco se basa en el sistema operativo Linux. El sistema operativo Cisco Linux está reforzado para garantizar que los servicios no autorizados no estén instalados y protegido para evitar el establecimiento de software de terceros y otros cambios. El sistema operativo Cisco Linux proporciona un shell CLI similar a los dispositivos Cisco IOS. Este shell CLI especial, junto con WAAS Central Manager, constituye el medio principal para configurar, administrar y solucionar problemas de un dispositivo o sistema WAAS. [11]

La plataforma Cisco Linux aloja una variedad de servicios para la operación en tiempo de ejecución WAAS, como cifrado de disco, subsistema de administración central (CMS), administrador de interfaz, funciones de informes, interceptación y derivación de la red, y motor de política de tráfico de aplicaciones (ATP), como se observa en la Figura 2.1.

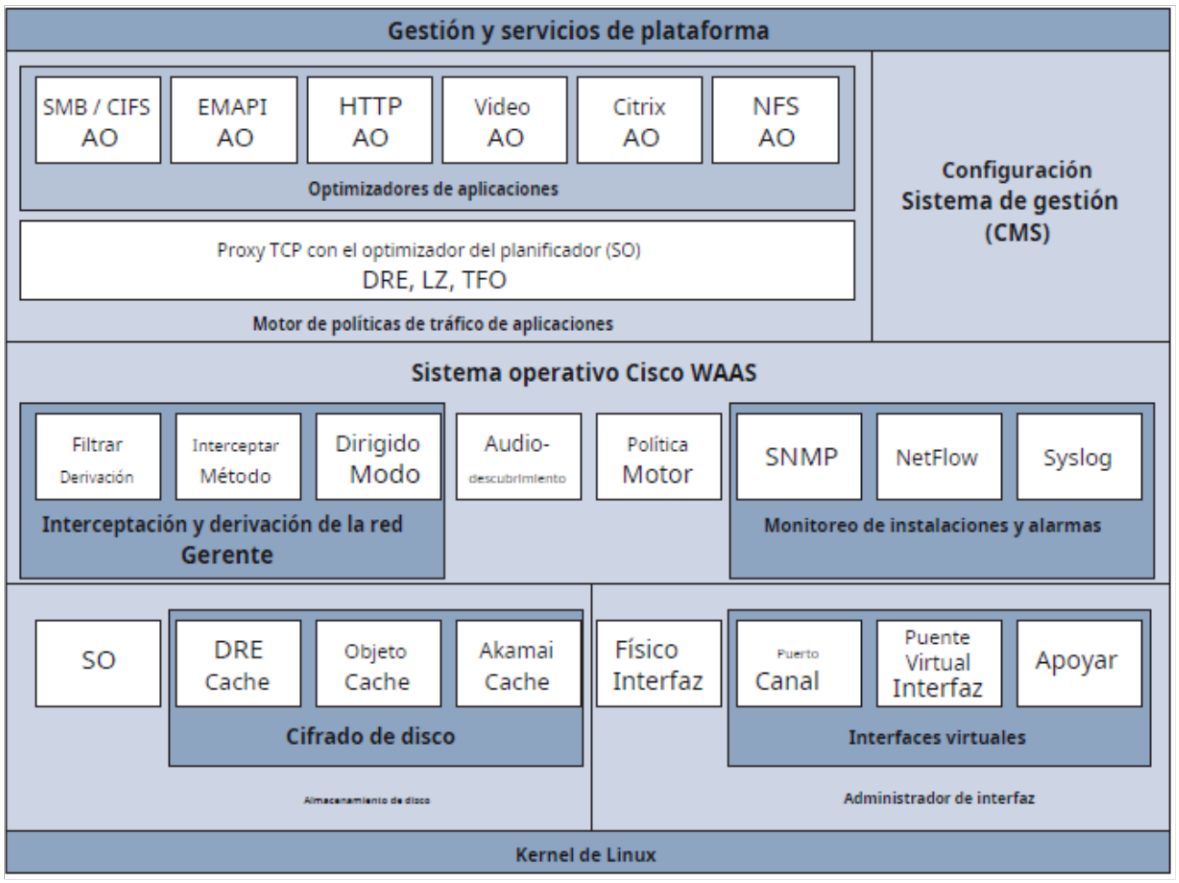

Figura 2.1. Arquitectura de Hardware y Software de Cisco WAAS [11]

2.1.3 Interfaces WAAS

Cisco WAAS facilita las siguientes interfaces con la finalidad de ayudar a administrar, configurar y monitorear los diversos elementos de su red WAAS: [12]

- GUI de WAAS Central Manager
- GUI de WAE Device Manager
- GUI de administración de servicios de impresión WAAS
- WAAS CLI

2.1.3.1 GUI de WAAS Central Manager

Todas las redes con WAAS constan con un dispositivo WAAS Central Manager principal, el cual administra todos los dispositivos en su red con tecnología WAAS. Estos dispositivos cuentan con GUI WAAS *Central Manager* que es la interfaz que permite configurar, administrar y monitorear los dispositivos WAAS en su red.

La GUI de WAAS Central Manager permite que los administradores realicen diferentes tareas como: [12]

- Configurar ajustes de sistema y de la red para uno o varios dispositivos WAAS.
- Crear y editar políticas de aplicaciones, para cuando intercepta tipos específicos de tráfico.
- Configurar servicios de archivo, políticas de bloqueo.
- Crea grupos de dispositivos para la ayuda de administración y configuración de múltiples WAE al mismo tiempo.
- Nos permite observar informes detallados acerca del tráfico optimizado en su red WAAS.

Los componentes de la GUI de WAAS Central Manager están detallados en la Figura 2.2:

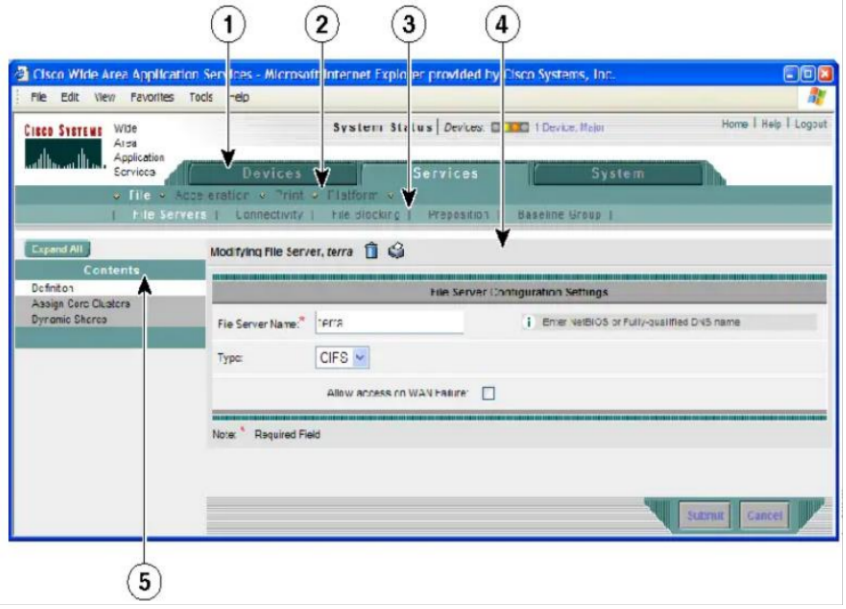

Figura 2.2 GUI de WAAS Central Manager [12]

1. Fichas (dispositivos, servicios y sistema)
2. Páginas específicas de pestañas
3. Subpáginas
4. Barra de tareas
5. Panel de control

Pestañas GUI de WAAS Central Manager.

- Dispositivos.

Permite la configuración de servicios WAAS y configuración en general para uno o varios dispositivos en específico. Se puede ver también información y mensajes detallados del dispositivo.

- Servicios.

Permite la configuración de los principales servicios WAAS como puede ser archivo, impresión y aceleración de aplicaciones.

- Sistema.

Permite realizar tareas simples del sistema como configurar cuentas, roles de usuario y ver registros del sistema.

2.1.3.2 GUI de WAE Device Manager

Esta interfaz es establecida en web y permite configurar, administrar y monitorear un dispositivo WAE en su red. En algunos casos existen las mismas configuraciones tanto en WAE Device Manager como en WAAS Central Manager GUI, por lo que siempre se recomienda configurar en GUI de WAAS Central Manager en caso de ser posible.

Se usa esta interfaz para realizar tareas que no se puedan realizar desde GUI de WAAS Central Manager, también la habilitación de servicios de impresión en WAE y cerrar los servicios del dispositivo.

A continuación, en la Figura 2.3. se observa la interfaz de GUI.

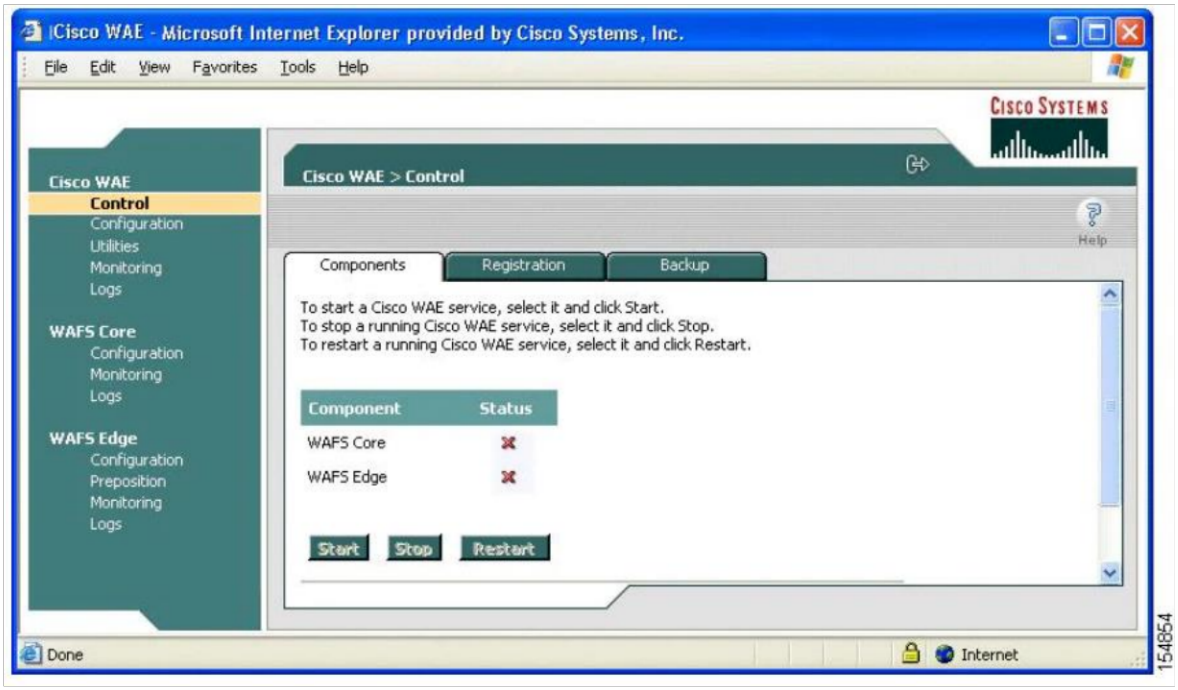

Figura 2.3. Interfaz GUI de WAE Device Manager [12]

2.1.3.3 GUI de administración de servicios de impresión WAAS

Es una interfaz basada en web que permite la configuración de un servidor de impresión WAAS y ver una lista de trabajos de impresión activos y completados. [12]

Puede ejecutar las siguientes tareas desde la GUI de administración de servicios de impresión:

- Agregar una impresora al servidor de impresión WAAS.
- Modificar la configuración de una impresora existente.
- Configurar grupos de impresión.
- Ver trabajos de impresión.

2.1.3.4 WAAS Command-line interface (CLI)

La CLI de WAAS también le permite configurar ciertas características que son compatibles solo a través de la CLI. Es recomendable usar la GUI de WAAS Central Manager en vez de CLI de WAAS, siempre que sea posible.

La CLI de WAAS está organizada en cuatro modos de comando. Cada modo de comando tiene su propio conjunto de comandos para usar en la configuración, mantenimiento y monitoreo de un WAE. Los cuatro modos de comando WAAS son los siguientes: [12]

- Modo EXEC: para configurar, ver y probar las operaciones del sistema. Este modo se divide en dos niveles de acceso: usuario y privilegiado. Para usar el nivel de acceso privilegiado, ingrese el comando enable en el indicador del nivel de acceso del usuario, luego ingrese la contraseña EXEC privilegiada cuando vea el indicador de contraseña.
- Modo de configuración global: para configurar, ver y probar la configuración de las funciones del software WAAS para todo el dispositivo. Para usar este modo, ingrese el comando configure desde el modo EXEC privilegiado.
- Modo de configuración de interfaz: para configurar, ver y probar la configuración de una interfaz específica. Para usar este modo, ingrese el comando de interfaz desde el modo de configuración global.
- Modo de configuración de función específica: varios modos de configuración están disponibles en el modo de configuración global para administrar funciones específicas.

2.1.4 Plataformas Cisco WAAS

La plataforma Cisco WAAS actual consta de módulos de red integrados en ruteadores, modelos de dispositivos, ruteadores de la serie ISR 4000 integrados con WAAS (ISR-WAAS) y modelos de dispositivos virtuales. Cisco WAAS se puede implementar en cada ubicación con la cantidad adecuada de capacidad de optimización para las necesidades de los usuarios o servidores en esa ubicación en particular. [11]

2.1.4.1 Módulos de red integrados en el ruteador

Están diseñados para dar servicios de optimización a la sucursal remota, los mismos que ocupan una ranura de módulo de red disponible en un ruteador de servicios integrados de Cisco (ISR). El ISR es una plataforma que se usa para la sucursal, debido a que brinda una plataforma de servicio convergente para la oficina remota, en la cual también se incluye

enrutamiento, conmutación, conectividad inalámbrica, voz, seguridad y optimización de WAN. Este es un componente de hardware fundamental para soluciones de CISCO iWAN. [11]

2.1.4.2 Accesorios

Las plataformas de dispositivos Cisco WAAS se adaptan a escenarios de implementación desde tamaños pequeños hasta grandes. La plataforma del dispositivo Cisco WAVE incluye los modelos 294, 594, 694, 7541, 7571 y 8541. Los modelos 294 y 694 del dispositivo WAVE, junto con el modelo 594 del dispositivo WAVE, están designados a implementaciones de sucursales, en tanto que los modelos del dispositivo WAVE 7541, 7571, y 8541 están designados a grandes desarrollos de centros de datos y oficinas a nivel regional. El WAVE-694 es un dispositivo híbrido que se usa comúnmente para sucursales más grandes o pequeños centros de datos. [11]

2.1.4.3 WAAS virtual

WAAS Virtual está diseñada para usarse o ser implementada en lugares donde no se pueda instalar dispositivito WAVE físicos. El software vWAAS se puede instalar en VMware ESXi 5.0 y posterior y se le asigna como Dispositivo virtual abierto (OVA) que está empaquetado previamente con disco, memoria, CPU, NIC y otra configuración relacionada con VMware en un Formato de virtualización abierto OVF (Formato de Virtualización abierto). WAN

En la Figura 2.4 se indica los diferentes modelos de OVA:

Nombre OVA	Conexión Capacidad	Aparato Similar	UPC	RAM (GB)	Disco (GB)	Optimizado Conexiones	WAN Banda ancha	LAN Rendimiento (Mbps)	Máximo Número de compañeros (Fan-out)
vWAAS-200	200	294-4G	1	2	160	200	10	20	100
vWAAS-750	750	594-8G	2	4	250	750	50	100	100
vWAAS-1300	1300	594-12G	2	6	300	1300	80	150	200
vWAAS-2500	2500	694-16G	4	8	400	2500	200	400	300
vWAAS-6000	6000	694-24G	4	8	500	6000	200	500	300
vWAAS-12000	12 000	N / A	4	12	750	12 000	310	1000	1.400
vWAAS-50000	50.000	N / A	8	48	1500	50.000	1000	2000	2.800

Figura 2.4. Modelos de OVA [11]

También Cisco ofrece un Virtual Central Manager (vCM) con modelos de capacidad propicias que se pueden ver en la Figura 2.5.

Nombre OVA	Capacidad	Aparato Similar	UPC	RAM (GB)	Disco (GB)
vCM-100N	Gestiona 100 nodos		2	2	250
vCM-500N	Gestiona 500 nodos		2	2	300
vCM-1000N	Gestiona 1000 nodos	594-8G	2	4	400
vCM-2000N	Gestiona 2000 nodos	694-16G	4	8	600

Figura 2.5 Virtual Central Manager [11]

2.1.4.4 ISR-WAAS

Es una WAAS virtualizada ejecutándose con un router ISR 4000 usando un contenedor integrado de Cisco IOS XE. El término “contenedor” tiene como referencia el hipervisor KVM el cual ejecuta aplicaciones virtualizadas. [11]

2.1.5 Métricas de diseño y rendimiento de WAAS

En esta sección se describen las consideraciones de diseño e implementación al implementar WAAS en arquitecturas de sucursales y centros de datos. [11]

2.1.5.1 Dispositivo de memoria

El dispositivo de memoria es importante ya que nos dicta el nivel de rendimiento y escalabilidad que llega a tener el dispositivo; cuando aumenta la capacidad de memoria, aumenta la capacidad de un dispositivo WAAS y puede manejar mayor cantidad de conexiones, también permite que el dispositivo ejecute otros servicios adicionales como aceleración de aplicaciones o cifrado de disco. Existen dispositivos que tienen una configuración de memoria flexible y con estos se puede lograr un mayor ancho de banda WAN y mayor número de conexiones TCP optimizadas simultáneamente. [11]

2.1.5.2 Capacidad de disco

Cisco WAAS también aprovecha el disco para los servicios de optimización. En este caso tenemos algo parecido a la memoria, y podemos decir que cuanto más grande sea la capacidad del disco disponible, mayor será la optimización que pueda aprovechar el dispositivo WAAS durante el tiempo en ejecución. Por ejemplo en un equipo con 4GB de DRAM, tiene 200 GB de capacidad de disco físico, de los mismos que 40 GB van a estar disponibles para que los use DRE para el historial de compresión, se puede estimar la duración del historial de compresión dadas las condiciones de la WAN, la utilización esperada de la red y los niveles de redundancia supuestos.

La capacidad de disco disponible para un dispositivo Cisco WAAS se divide en los siguientes componentes principales: [11]

- Historial de compresión DRE: almacena firmas y datos fragmentados de DRE.
- Caché CIFS: Esta capacidad está reasignada.
- Servicios de plataforma: sirve para almacenamiento de imágenes del sistema operativo, archivos y espacio de intercambio.
- Servicios de impresión: nos indica la cola de impresión.
- Caché de objetos de Akamai Connect: es para la capacidad de cache de objetos HTTP de AKC.

2.1.5.3 Número de conexiones TCP optimizadas

Cada dispositivo WAAS tiene un número estático de conexiones TCP que se pueden optimizar al mismo tiempo. A cada conexión TCP se le asigna memoria y otros recursos dentro del sistema, y si se alcanza el límite estático de la conexión TCP optimizada al mismo tiempo, las conexiones adicionales se manejan en forma de paso. El almacenamiento en búfer adaptativo (asignación de memoria) se utiliza para garantizar que a las conexiones más activas se les asigne memoria adicional y que a las conexiones menos activas se les asigne solo la memoria que necesitan.

El límite de conexión TCP de cada dispositivo WAAS puede correlacionarse aproximadamente con la cantidad de usuarios admitidos por un modelo de dispositivo WAAS dado, pero se debe tener en cuenta que la cantidad de conexiones TCP abiertas en

un nodo en particular puede variar según la productividad del usuario, el comportamiento de la aplicación y otros factores. Se asume comúnmente que un usuario tiene de 10 a 15 conexiones abiertas en un momento dado. Si es necesario, las políticas se pueden ajustar en WAAS Central Manager para pasar a través de ciertas aplicaciones que pueden obtener solo un pequeño beneficio de WAAS. Este tipo de cambio podría potencialmente ayudar a aumentar la cantidad de usuarios que pueden ser compatibles con un dispositivo WAAS en particular.

2.1.5.4 Licencia

Las licencias no se aplican en WAAS, pero la licencia Enterprise va incluida con las compras de dispositivos WAAS, al igual que la licencia empresarial que permite que un dispositivo WAAS aplique todas las técnicas de aceleración de aplicaciones y WAN. También dispositivos que actúan como administradores centrales requieren de licencia empresarial y por ultimo para implementar componentes como ISR-WAAS y AppNav-XE, se necesita licencia Apllication Experience.

2.1.6 Modos operativos de Cisco WAAS

Cisco WAAS trabaja en dos modos operativos que son:

- Modo transparente.
- Modo dirigido.

2.1.6.1 Modo transparente

WAAS maneja el tráfico de manera transparente preservando las direcciones IP de origen, destino y los puertos TCP originales del paquete. Este modo nos permite la visibilidad del tráfico de un extremo al otro, facilitando la interoperabilidad con la QoS, control de acceso, generando informes de rendimiento.

2.1.6.2 Modo dirigido

En la versión 4.1 de WAAS viene un modo de operación alternativo, que es el modo dirigido.

A diferencia del otro modo, este transporta conexiones optimizadas por medio de un mecanismo no transparente en medio de dos dispositivos WAAS. El modo dirigido se basa en el proceso de descubrimiento automático para establecer la relación entre pares entre dos WAE. Esto significa que el modo dirigido no elude ninguna medida de seguridad. Los flujos de tráfico TCP iniciales entre el cliente y el servidor deben atravesar cualquier firewall antes de que WAAS pueda optimizar el tráfico en modo dirigido.

2.2 Application Visibility and Control (AVC)

En esta sección se hablará sobre conceptos básicos de AVC, dispositivos compatibles con la tecnología y solución de problemas que se presentan con dicha tecnología.

2.2.1 Que es AVC

Cisco Application Visibility and Control (AVC) nos brinda una gran solución de gestión de servicios integrada y generalizada que se basa en la inspección profunda de paquetes (DPI), Cisco AVC no procesa paquetes como eventos individuales. Esta tecnología permite monitorear el tráfico con interfaces específicas y al mismo tiempo genera informes de estadísticas basadas en el rendimiento de ancho de banda, al momento que genera los informes los envía, y cada informe da información al Datasheet. Para la configuración de la visibilidad de aplicación se recomienda CLI o WSMA, las cuales son más fáciles de configurar y en una manera más eficiente y a su vez confiable. [13]

Las ventajas de Cisco AVC incluyen:

- Mejora la visión del tráfico y mejora el control de aplicaciones en la capa 7.
- Aumenta el rendimiento de aplicaciones críticas para negocio.
- La resolución de problemas es mucho más rápida lo que ayuda a tener menos interrupciones de la red.
- La experiencia del usuario final es mucho mejor.

- Los costos operativos de la red son claramente disminuidos.

2.2.2 Dispositivos compatibles con AVC

La tecnología AVC es compatible con las siguientes plataformas:

- Plataforma de la serie ASR 1000 de Cisco IOS-XE versión 15.3 (1) S1 o posterior.
- Plataforma ISR G2 de Cisco IOS versión 15.2 (4) M2 o posterior como se indica a continuación:
- Routers de servicios integrados de la serie Cisco 1900.
- Ruteadores inalámbricos móviles Cisco MWR 1900.
- Ruteadores de servicios integrados de la serie Cisco 2900.
- Ruteadores de servicios integrados de la serie Cisco 3900.
- Ruteadores de servicios integrados Cisco 812 CiFi.
- Ruteador de servicios integrados no reforzado Cisco 819.
- Ruteador de servicios integrados reforzado Cisco 819.
- Cisco 819 Hardened 3G - ISR WiFi 802.11n de radio dual.
- Ruteador de servicios integrados Cisco 861,861W G2.
- Ruteador de servicios integrados Cisco 867,867W G2.
- Ruteador de servicios integrados Cisco 881,881W G2.
- Cisco 881SRST, 881SRSTW Ruteador de servicios integrados G2.
- Ruteador de servicios integrados Cisco 881W, 881WD.
- Ruteador de servicios integrados Cisco 886,886W G2.
- Cisco 886SRST, 886SRSTW Ruteador de servicios integrados G2.
- Cisco 886VA, 886VAG Ruteador de servicios integrados G2.
- Ruteador de servicios integrados Cisco 886VA-W G2.
- Ruteadores de servicios integrados Cisco 887,887W G2.

- Ruteador de servicios integrados Cisco 887V G2.
- Ruteador de servicios integrados Cisco 886VA G2 Mejore.

2.2.3 Solución de problemas de flujos de tráfico mediante AVC

Puede recopilar datos de visibilidad de la aplicación para cada flujo a través de la interfaz supervisada. Pero debido a que esto puede tener un impacto significativo en el rendimiento del dispositivo, los datos de visibilidad de la aplicación se recopilan de forma agregada.

Para seguir solucionando problemas de un proceso específico, puede habilitar una sesión de resolución de problemas de visibilidad de la aplicación en el dispositivo. Las sesiones se activan en interfaces específicas y tráfico específico. Le permiten recopilar información no agregada a nivel de flujo para proporcionar informes de NetFlow sin procesar en el formato. Esta información se puede utilizar para analizar un flujo específico más adelante.

La función de solución de problemas de AVC le permite:

- Crea y activa una sesión para la resolución de problemas en una determinada interfaz.
- Desactiva y elimina una sesión para la resolución de problemas en una determinada interfaz

2.3 OPTIMIZACIÓN DE FLUJO TCP

Cisco WAAS utiliza funciones TCP Flow Optimización (TFO), para la optimización del tráfico TCP interceptado por los dispositivos WAAS. Esta tecnología protege ya sea a clientes como a servidores que poseen malas condiciones de la WAN, como bajo ancho de banda, pérdida de paquetes, congestión y retransmisión. [11]

TFO incluye las siguientes funciones de optimización:

- Compresión
- Escalado de Windows
- Maximización del tamaño de la ventana inicial de TCP

- Mayor almacenamiento en búfer
- Reconocimiento selectivo (SACK)
- BIC TCP

2.3.1 Compresión

Para reducir el tamaño de datos transmitidos por medio de una WAN, Cisco WAAS usa las siguientes técnicas de compresión:

- Eliminación de redundancia de datos (DRE).
- Compresión LZ.

Dichas técnicas de compresión eliminan información redundante de la WAN por lo que se reduce el tamaño de datos transmitidos. WAE usa la compresión de tráfico TCP intercambiando datos duplicados con referencias cortas y envía después el flujo de datos reducido por medio de la WAN.

La compresión LZ funciona en flujos de datos más pequeños y recuerda un historial de compresión limitado, por lo que DRE es mejor porque puede operar en flujos más grandes (por ejemplo, cientos de bytes o más) y tiene un historial de compresión más largo.

2.3.2 Escalado de Windows TCP

El escalado de ventana ayuda al receptor de un paquete TCP a anunciar que su ventana de recepción de TCP superará los 64KB. El tamaño de la ventana de recepción establece la cantidad de espacio que el receptor tiene disponible para datos desconocidos. Los encabezados TCP también limitan a 64KB el tamaño de la ventana de recepción, pero el escalado de ventana permite que el encabezado TCP detalle ventanas de recepción de hasta 1 GB.

El escalado de ventana da acceso a los puntos finales TCP que se beneficien de todo el ancho de banda disponible en su red, sin estar limitados al tamaño de ventana preestablecido en el encabezado TCP.

2.3.3 Maximización del tamaño de la ventana inicial de TCP

El aumento del tamaño de la ventana inicial de TCP proporciona las siguientes ventajas:

- Si tenemos un solo segmento en la ventana TCP inicial, el receptor que usa ACK retrasados toma la decisión de esperar un tiempo antes de generar otra respuesta ACK. Por otro lado, cuando hay al menos dos segmentos, el receptor genera una respuesta ACK justo después de que llegue el segundo segmento de datos y así eliminando el tiempo de espera.
- Una ventana más grande, reduce el tiempo de transmisión cuando hay conexiones que transmiten una cantidad pequeña de datos.
- Para conexiones que usan grandes ventanas de congestión, la ventana inicial más grande excluye hasta 3 RTT, y un tiempo de espera ACK retrasando la fase inicial.

2.3.4 Capacidad del almacenamiento en búfer

Cisco WAAS optimizó el algoritmo de almacenamiento en búfer utilizando kernel de TCP, lo hizo para que los WAE extraigan los datos de clientes de servidores remotos y también de las sucursales. Gracias a este almacenamiento aumentado del búfer los WAE se pueden enlazar entre ellos, lo que hace que se aumente la utilización del enlace.

2.3.5 Reconocimiento selectivo (SACK)

Este reconocimiento selectivo facilita a los clientes la recuperación de pérdida de paquetes de una manera más rápida, ya que este reconocimiento selectivo es la función de retrasmisión y recuperación de pérdida de paquetes. Y es más eficaz en comparación al mecanismo usado por TCP.

En TCP tenemos que, de manera predeterminada, se usa un esquema de acuse de recibo, el cual obliga al receptor a esperar un viaje de ida y de vuelta para saber si dicho destinatario recibió o no los paquetes, o por otro lado lo que hacen es retransmitir innecesariamente segmentos que pueden haberse recibido correctamente.

Por otro lado, SACK, solo requiere retransmitir segmentos que se han perdido ya que el receptor informa sobre todos los paquetes que llegaron exitosamente, por lo que se descartan los mismos.

2.3.6 Binary increase in congestion (BIC) TCP

Es un protocolo de administración que permite que la red se recupere más rápido de pérdidas de paquetes.

Al momento en que ocurre pérdida de paquetes, BIC TCP hace más pequeño el tamaño de la ventana del receptor y da un nuevo valor reducido al de ventana mínima, luego establece el valor de tamaño máximo de ventana al tamaño de ventana justo antes de que ocurriera la pérdida de paquetes. Debido a que la pérdida de paquetes se produjo en el tamaño máximo de ventana, la red puede transferir tráfico sin descartar paquetes cuyo tamaño se encuentre dentro de los valores de tamaño de ventana mínimo y máximo.

3 CONFIGURACIONES PARA OPTIMIZACIÓN iWAN

En este capítulo se indica las configuraciones que se requieren para optimizar las aplicaciones de las redes iWAN, tanto para WAAS como también para AVC.

3.1 WAAS

A continuación, se presenta una guía básica sobre la implementación de dispositivos a redes WAAS. [14]

3.1.1 Configuración del administrador central de Cisco WAAS

A continuación, en la Tabla 3.1. se especifican parámetros y datos universales de diseño necesarios para la instalación y configuración de un administrador central de Cisco WAAS.

Tabla 3.1. Parámetros de red de Cisco WAAS

PARÁMETRO	VALORES
Cambiar el número de interfaz	1/0/10
Número de VLAN	148
Zona horaria	PST8PDT – 8 0
Dirección IP	10.4.48.100/24
Puerta de enlace predeterminada	10.4.48.1
Nombre de host	waas-wcm-1
Red de gestión (opcional)	10.4.48.0/24
Clave compartida TACACS (opcional)	Llave secreta

Para continuar tenemos los siguientes procedimientos:

3.1.1.1 Configuración del switch para Central Manager

Esta guía asume que los switches ya fueron configurados. Aquí se obtiene información necesaria para completar conexión entre el swithc y los dispositivos Cisco WAVE.

Existe dos opciones de configuraciones:

OPCIÓN 1: Configurar el swithc del área de servidores.

Paso 1: Conectar el puerto Ethernet externo del dispositivo Cisco WAVE a un puerto Ethernet en el switch, luego restablezca la configuración del puerto del switch a su valor predeterminado como se observa en el Comando 3.1.

```
default interface GigabitEthernet1/0/10
```

Comando 3.1. Default Interface

Paso 2: Defina el switchport como un puerto de acceso y luego aplique la configuración de calidad de servicio (QoS) que, a continuación, se muestra en el Comando 3.2.

```
interface GigabitEthernet1/0/10
 description Link to WAAS-CM
 switchport access vlan 148
 switchport host
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

Comando 3.2. Definir Switchport

OPCIÓN 2: Configurar el switch del centro de datos.

Paso 1: Conecte el dispositivo a un Cisco Fabric Extender (FEX), defina el puerto del switch como un puerto de acceso y luego aplique la configuración de calidad de servicio (QoS), como se observa en el Comando 3.3.

```
interface Ethernet102/1/1
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Comando 3.3. Conecte Cisco Fabric Extender

3.1.1.2 Instalación de máquina virtual vWAAS

Este procedimiento es necesario solo si se usa una máquina virtual Cisco Virtual WAAS (Cisco vWAAS).

Cisco vWAAS se abastece como si fuera un dispositivo virtual abierto (OVA). El cual cuenta con muchos parámetros de configuración relacionados con la máquina virtual como memoria, CPU, tarjetas de interfaz de red (NIC). Cisco proporciona un archivo OVA distinto para cada modelo de vWAAS.

Paso 1: Implemente la plantilla OVF con el cliente VMware vSphere.

Paso 2: Instalar vWAAS OVA en el servidor VMware ESX/ESXi, antes de que configure Cisco vWAAS.

Paso 3: Configure Cisco WAAS en la consola de VMware.

3.1.1.3 Configuración del administrador central de WAAS

Para la función de administrador central de Cisco WAAS use un dispositivo Cisco WAVE apropiado, que debe estar en la ubicación principal para la administración gráfica, configuración e informes de la red Cisco WAAS. Para poder configurar el administrador central de WAAS, este debe tener acceso de terminal al puerto de la consola y así asignar direcciones IP y configuraciones básicas. Todos los dispositivos Cisco WAVE tienen como nombre de usuario predeterminado “administración” y contraseña de fábrica por defecto.

Paso 1: Ingrese en *setup.* Se observa en el Comando 3.4.

```
    Parameter                 Default Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 1/0
 5.     Autosense                Enabled
 6.     DHCP                     Enabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change
specific default [y]: n
```

Comando 3.4. Setup

Paso 2: Digite la opción 2 para configuración de *Central Manager.*

Paso 3: Configuración de Zona Horaria.

Paso 4: Configuración de la interfaz de administración, dirección IP y Gateway predeterminada. Como se muestra en el Comando 3.5.

```
No.      Interface Name      IP Address    Network Mask
  1. GigabitEthernet 1/0           dhcp
  2. GigabitEthernet 2/0           dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]: 10.4.48.100/24
Enter Default Gateway IP Address [Not configured]: 10.4.48.1
```

Comando 3.5. Configuración de la interfaz de administración

Paso 5: Configuración DNS, host y NTP, se muestra en el Comando 3.6.

```
Enter Domain Name Server IP Address [Not configured]: 10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAAS-WCM-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

Comando 3.6. Configuración DNS, host, NTP

Paso 6: Seleccionar la licencia apropiada.

Paso 7: Comprobar los ajustes de configuración e inicie la recarga, observe en el Comando 3.7.

```
   Parameter                 Configured Value
 1. Device Mode               Central Manager
 2. Time Zone                 PST8PDT -8 0
 3. Management Interface      GigabitEthernet 1/0
 4.     Autosense                Enabled
 5.     DHCP                     Disabled
 6.     IP Address               10.4.48.100
 7. IP Network Mask           255.255.255.0
 8. IP Default Gateway        10.4.48.1
 9. DNS IP Address            10.4.48.10
10. Domain Name(s)            cisco.local
11. Host Name                 WAAS-WCM-1
12. NTP Server Address        10.4.48.17
13. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration ————————————
Press 'y' to select configuration, 'd' to toggle defaults display, <1-13> to
change specific parameter [y]: y
Apply WAAS Configuration: Device Mode changed in SETUP; New configuration takes
effect after a reload. If applicable, registration with CM, CM IP address, WAAS
WCCP configuration etc, are applied after the reboot. Initiate system reload?
<y/n> [n] y
Are you sure? <y/n> [n]: y
```

Comando 3.7. Ajustes de configuración

Paso 8: Reinicie y después inicie sesión en Cisco WAAS Central Manager.

Paso 9: Genere la clave RSA y luego habilite el servicio sshd.

Paso 10: Habilite el protocolo SNMP y configure SNMPv2c para cadena de solo lectura y de lectura y escritura.

Paso 11: Configure las listas de control de acceso ACL, solo si desea limitar el acceso al dispositivo.

Paso 12: Guarde la configuración.

Paso 13: Reiniciar el dispositivo Cisco WAAS Central Manager.

3.1.2 Configuración del dispositivo Cisco WAVE como un nodo WAAS (Cliente)

A continuación, en la Tabla 3.2. se especifican los parámetros y datos universales de diseño que se necesita para la instalación y configuración de la red Cisco WAAS, puede consultar los valores cuando configure la red WAAS.

Tabla 3.2. Parámetros de red de Cisco WAVE

PARÁMETRO	**VALORES WAVE PRIMARIA**	**VALORES WAVE SECUNDARIA**
Cambiar el número de interfaz	1/0/2 2/0/2	1/0/2 2/0/2
Número de VLAN	350	350
Nombre de VLAN (opcional)	WAN_ServIce_Net	WAN_ServIce_Net
Zona horaria	PST8PDT – 8 0	PST8PDT – 8 0
Dirección IP	10.4.32.161/26	10.4.32.161/26
Puerta de enlace predeterminada	10.4.32.129/26	10.4.32.129/26
Gerente central de WAAS	10.4.48.100	10.4.48.100
Nombre de host	WAVE-1	WAVE-1
Direcciones IP de ruteadores que interceptan tráfico con WCCP	10.4.32.241 10.4.32.242 10.4.32.243	10.4.32.241 10.4.32.242 10.4.32.243
Contraseña de WCCP	cisco123	cisco123
Red de gestión (opcional)	10.4.48.0/24	10.4.48.0/24
Clave compartida TACACS (opcional)	Llave secreta	Llave secreta

3.1.2.1 Configure el switch para dispositivos WAVE

Se tiene cuatro opciones en las que se puede conectar dispositivos Cisco WAVE. El switch de distribución es la ubicación adecuada para conectar físicamente dispositivos WAVE en el sitio de WAN y sitios remotos de dos niveles. El switch de acceso es la ubicación correcta para conectar los dispositivos WAVE físicamente en sitios remotos de un solo nivel.

- Switch de capa de distribución.
- Switch de capa de distribución para Cisco vWAAS.
- Pila de switches de capa de acceso de sitio remoto o switch modular.
- Switch de capa de acceso de sitio remoto.

Esta guía asume que los switches ya se han configurado, por lo tanto, explica procedimientos para completar conexión del switch a los dispositivos WAVE.

OPCIÓN 1: Conectar un switch de capa de distribución.

Paso 1: Configure la VLAN en el switch de la capa de distribución (en caso de que aún no exista).

Paso 2: Configure la capa 3, asegurándonos de configurar una interfaz VLAN (SVI).

Paso 3: Conecte los enlaces ascendentes EtherChannel del dispositivo Cisco WAVE, luego configure dos o más interfaces físicas para miembros del EtherChannel, como se observa en el Comando 3.8.

```
interface GigabitEthernet 1/0/2
 description Link to WAVE port 1
interface GigabitEthernet 2/0/2
 description Link to WAVE port 2
!
interface range GigabitEthernet 1/0/2, GigabitEthernet 2/0/2
 switchport
 macro apply EgressQoS
 channel-group 7 mode on
 logging event link-status
 logging event bundle-status
```

Comando 3.8. Enlaces EtherChannel

Paso 4: Asigne la VLAN creada al comienzo del procedimiento a la interfaz, debe coincidir el número del canal del puerto con el grupo de canales configurados en el paso 3.

OPCIÓN 2: Conectar un switch de capa de distribución para vWAAS.

Paso 1: Configurar VLAN en el switch de la capa de distribución en caso de no existir.

Paso 2: Configure la capa 3 y asegurarse de configurar una interfaz VLAN (SVI).

Paso 3: Conecte los puertos del servidor ESXI a switches separados y configure 2 o más interfaces físicas para que sean de la misma VLAN, como se observa en el Comando 3.9.

```
interface GigabitEthernet 1/0/12
 description Link to ESXi vmnic1
interface GigabitEthernet 2/0/12
 description Link to ESXi vmnic2
!
interface range GigabitEthernet 1/0/12, GigabitEthernet 2/0/12
 switchport
 switchport host
 switchport mode access
 switchport access vlan 350
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

Comando 3.9. Conexión de puertos ESXI

OPCION 3: Conectar una pila de switches de capa de acceso de sitio remoto o un switch modular.

Paso 1: Conecte enlaces ascendentes de EtherChannel del dispositivo Cisco WAVE para separar los switches en la pila, luego configure dos o más interfaces físicas para que sean miembros del EtherChannel. Es recomendable agregar en múltiplos de dos. Esto asegura que se priorice el tráfico, como se va observa en el Comando 3.10.

```
default interface GigabitEthernet 1/0/2
default interface GigabitEthernet 2/0/2
!
interface GigabitEthernet 1/0/2
 description Link to WAVE port 1
interface GigabitEthernet 2/0/2
 description Link to WAVE port 2
!
interface range GigabitEthernet 1/0/2, GigabitEthernet 2/0/2
 switchport
 macro apply EgressQoS
 channel-group 7 mode on
 logging event link-status
 logging event bundle-status
```

Comando 3.10. EtherChannel con Cisco WAVE

Paso 2: A la interfaz se le asigna la VLAN de datos, al usar EtherChannel debe coincidir el número de canal del puerto con el grupo de canales configurados en el paso anterior.

OPCIÓN 4: Conectar un switch de capa de acceso de sitio remoto.

Paso 1: Conectar el puerto Ethernet externo del dispositivo Cisco WAVE a un puerto Ethernet en el switch de acceso de sitio remoto y restablezca la configuración predeterminada del puerto del switch.

Paso 2: Defina el puerto del switch en el switch de acceso al sitio remoto como un puerto de acceso para la VLAN de datos y aplique seguridad al puerto y configuración QoS, tal como se observa en el Comando 3.11.

```
interface GigabitEthernet1/0/3
 description Link to WAVE
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

Comando 3.11. Configuración del puerto de switch

3.1.2.2 Configuración del dispositivo Cisco WAVE

La configuración de Cisco WAVE es similar a la configuración de Cisco WAAS Central Manager, pero al momento de elegir el acelerador de aplicaciones como modo de dispositivo los pasos comienzan a cambiar, ya que el script de configuración cambia para que pueda registrar el dispositivo WAVE con el Administrador central de WAAS actual.

Paso 1: Desde la línea comandos, ingrese *setup* y se inicia la configuración inicial como indica el Comando 3.12.

```
    Parameter                 Default Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 1/0
 5. Autosense                 Enabled
 6.     DHCP                     Enabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————————
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change
specific default [y]: n
```

Comando 3.12. Setup

Paso 2: Configure el dispositivo como acelerador de aplicaciones.

Paso 3: Configure el método de interceptación.

Paso 4: Configure la zona horaria.

Paso 5: Configure interfaz de administración, dirección IP y Gateway predeterminada, como observamos en el Comando 3.13.

```
No.      Interface Name      IP Address    Network Mask
  1. GigabitEthernet 1/0           dhcp
  2. GigabitEthernet 2/0           dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]: 10.4.32.161/26
Enter Default Gateway IP Address [Not configured]: 10.4.32.129
Enter Central Manager IP Address (WARNING: An invalid entry will cause SETUP to
take a long time when applying WAAS configuration) [None]: 10.4.48.100
```

Comando 3.13. Configuración interfaz de administración, IP, Gateway

Paso 6: Configure DNS, hots y NTP.

Paso 7: Configurar la lista de ruteadores WCCP.

Paso 8: Seleccionar la licencia adecuada.

Paso 9: Verifique los ajustes de configuración, como observamos en el Comando 3.14.

```
   Parameter                 Configured Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 PST8PDT -8 0
 4. Management Interface      GigabitEthernet 1/0
 5.     Autosense                Enabled
 6.     DHCP                     Disabled
 7.     IP Address               10.4.32.161
 8.     IP Network Mask          255.255.255.192
 9. IP Default Gateway        10.4.32.129
10. CM IP Address             10.4.48.100
11. DNS IP Address            10.4.48.10
12. Domain Name(s)            cisco.local
13. Host Name                 WAVE-1
14. NTP Server Address        10.4.48.17
15. WCCP Router List          10.4.32.241 10.4.32.242 10.4.32.243
16. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration ————————
Press 'y' to select configuration, <F2> to see all configuration, 'd' to toggle
defaults display, <1-16> to change specific parameter [y]: y
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
```

Comando 3.14. Verificar ajustes

Paso 10: En el modo EXEC, habilite la propagación de cambios de configuración local a Cisco WAAS Central Manager.

Paso 11: Configure la conexión de canal de puerto y regístrela en Cisco WAAS Central Manager como observamos en el Comando 3.15.

```
interface GigabitEthernet 1/0
 no ip address 10.4.32.161 255.255.255.192
 exit
!
primary-interface PortChannel 1
!
interface PortChannel 1
 ip address 10.4.32.161 255.255.255.192
 exit
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 no shutdown
 exit
```

Comando 3.15. Cisco WAAS Central Manager

Paso 12: Configure devolución negociada por GRE con sus respectivos ruteadores WCCP.

Paso 13: Configure la lista de ruteadores WCCP.

Paso 14: Inicie sesión en el dispositivo Cisco WAVE.

Paso 15: Generar clave RSA y habilitar el servicio sshd.

Paso 16: Habilitar el protocolo SMNP y configure SNMPv2c para cadena de comunidad de solo lectura y lectura y escritura.

Paso 17: Configure ACL de administración para limitar el acceso al dispositivo, como se observa en el Comando 3.16.

```
ip access-list extended 155
 permit tcp 10.4.48.0 0.0.0.255 any eq ssh
 deny tcp any any eq ssh
 permit ip any any
 exit
interface [interface]
 ip access-group 155 in
 exit
!
ip access-list standard  55
 permit 10.4.48.0 0.0.0.255
 exit
snmp-server access-list 55
```

Comando 3.16. Configuración de ACL

Paso 18: Habilitar la autenticación AAA si se tiene un servidor TACACS+ centralizado.

Paso 19: En el modo EXEC, guarde la configuración.

3.1.3 Configuración del dispositivo Cisco WAVE como controlador de AppNav

A continuación, en la Tabla 3.3. se especifican los parámetros y datos universales de diseño que se necesita para la instalación y configuración de la red Cisco WAAS, puede consultar los valores cuando configure la red WAAS.

Tabla 3.3. Parámetros de red de Cisco WAVE

PARÁMETRO	**VALORES WAVE PRIMARIA**	**VALORES WAVESECUNDARIA**
Cambiar el número de interfaz	1/0/19 2/0/19	1/0/20 2/0/20
Cambiar el número de canal de puerto.	9	10
Número de VLAN	350	350
Nombre de VLAN (opcional)	WAN_Service_Net	WAN_Service_Net
Controlador de AppNav números de interfaz	1/0 1/1	1/0 1/1
Controlador de AppNav numero de canal de puerto	1	1
Zona horaria	PST8PDT – 8 0	PST8PDT – 8 0
Dirección IP	10.4.32.163/26	10.4.32.164/26
Puerta de enlace predeterminada	10.4.32.129/26	10.4.32.129/26
Gerente central de WAAS	10.4.48.100	10.4.48.100
Nombre de host	WAVE-APPNAV-1	WAVE-APPNAV-1
Red de gestión (opcional)	10.4.48.0/24	10.4.48.0/24
Clave compartida TACACS (opcional)	Llave secreta	Llave secreta

Se sigue con los procesos para configurar y son 4.

3.1.3.1 Configuración del switch para dispositivos WAVE

La guía está asumiendo que los switches ya están configurados, es decir que la guía nos brinda procedimientos para completar la conexión del switch a los dispositivos WAVE.

Paso 1: Configure las VLAN en el switch de capa de distribución como indica el Comando 3.17.

```
vlan 350
 name WAN_Service_Net
vlan 349
 name AppNav_Intercept_Net
```

Comando 3.17. Configuración VLAN

Paso 2: Configure la capa 3. Asegúrese de configurar una interfaz VLAN (SVI) para que todos las VLAN nuevos se conecten al resto de la red, se observa en el Comando 3.18.

```
interface Vlan350
 ip address 10.4.32.129 255.255.255.192
 no shutdown
interface Vlan349
 ip address 10.4.32.65 255.255.255.192
 no shutdown
```

Comando 3.18. Configuración VLAN (SVI)

Paso 3: Se configurará enlaces ascendentes EtherChannel, es recomendable que cada interfaz física sea agregada en múltiplos de dos, como podemos ver en el Comando 3.19.

```
interface GigabitEthernet 1/0/19
 description Link to AppNav-WAVE port 1/0
interface GigabitEthernet 2/0/19
 description Link to AppNav-WAVE port 1/1
!
interface GigabitEthernet 1/0/21
 description Link to AppNav-WAVE port 1/2 (Intercept Network)
interface GigabitEthernet 2/0/21
 description Link to AppNav-WAVE port 1/3 (Intercept Network)
!
interface range GigabitEthernet 1/0/19, GigabitEthernet 2/0/19
 switchport
 macro apply EgressQoS
 channel-group 9 mode on
 logging event link-status
 logging event bundle-status
!
interface range GigabitEthernet 1/0/21, GigabitEthernet 2/0/21
```

Comando 3.19. Configuración EtherChannel

Paso 4: Las VLAN creadas al inicio de este procedimiento, deben ser asignadas. Si se usa EtherChannel, deben coincidir los números de canal de puerto con los canales configurados en el paso 3. Como se observa en el Comando 3.20.

```
interface Port-channel 9
 description EtherChannel link to AppNav-WAVE
 switchport access vlan 350
 logging event link-status
 no shutdown
!
interface Port-channel 11
 description EtherChannel link to AppNav-WAVE (Intercept Network)
 switchport access vlan 349
 logging event link-status
 no shutdown
```

Comando 3.20. EtherChannel con mismo número de canal de puerto

3.1.3.2 Configuración del controlador Cisco AppNav

Se puede implementar un clúster de Cisco AppNav (ANC), en un sitio llamado agregación de la WAN y así se proporciona la terminación de cabecera dado el tráfico Cisco WAAS para los sitios remotos WAN. Después se conecta estos dispositivos al switch de capa de distribución. A continuación, en la Figura 3.1. se presenta una topología.

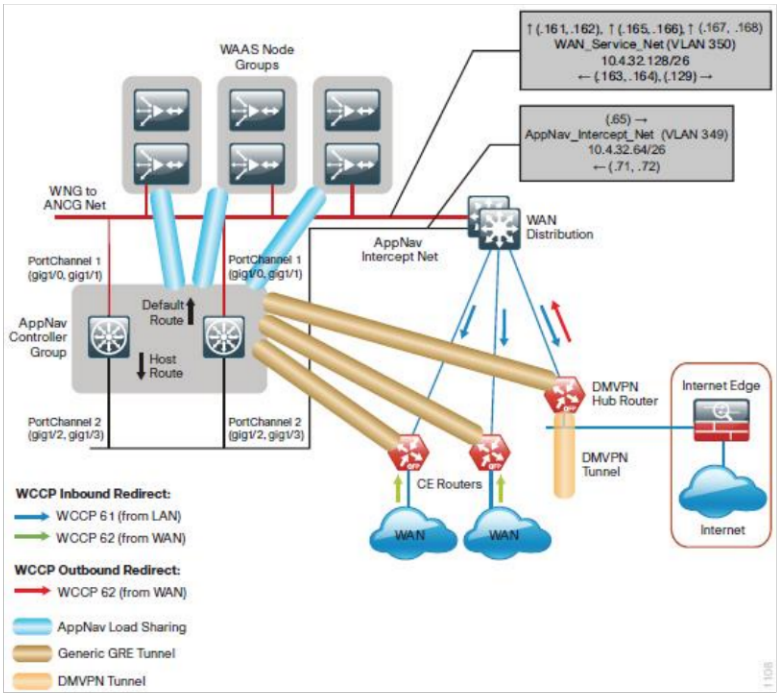

Figura 3.1. Topología Cisco AppNav

Estos dispositivos Cisco AppNav necesitan de una configuración básica por medio de su puerto de consola y con esta asignar la configuración inicial. Para configurar dispositivos Cisco AppNav se hace la configuración parecida a la configuración de Cisco WAAS Central Manager, pero al momento de escoger el modo del dispositivo ya cambia debido a que el script de configuración es distinto.

Para configurar hay los siguientes pasos:

Paso 1: Ingrese *setup,* desde la línea de comando, como se observa en el Comando 3.21.

```
    Parameter                 Default Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 0/0
 5.      Autosense               Enabled
 6.      DHCP                    Enabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————————
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change
specific default [y]: n
```

Comando 3.21. Setup

Paso 2: Configurar el dispositivo como un Cisco AppNav, como muestra el Comando 3.22.

```
1. Application Accelerator
2. AppNav Controller
3. Central Manager
Select device mode [1]: 2
Device Mode AppNav Controller selected in SETUP; New configuration takes effect
after a reload. If applicable, AppNav Controller I/O Module is recognized after
the reboot. Re-run Setup CLI to perform AppNav Controller related configuration
post reboot. Initiate system reload? <y/n> [n] y
Are you sure? <y/n> [n]:y
```

Comando 3.22. Cisco AppNav

Paso 3: Inicie sesión de nuevo en el dispositivo y en la línea de comando escriba *setup,* se observa que la configuración cambia a Cisco AppNav controller en el Comando 3.23.

```
    Parameter                 Default Value
 1. Device Mode               AppNav Controller
 2. Interception Method       Inline
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 0/0
 5.     Autosense                Enabled
 6.     DHCP                     Enabled
ESC Quit ? Help ———————— WAAS Default Configuration ————————
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change
specific default [y]: n
```

Comando 3.23. AppNav Controller

Paso 4: Seleccione la configuración Cisco AppNav Controller.

Paso 5: Configurar en el modo de WCCP.

Paso 6: Configurar zona horaria.

Paso 7: Configurar interfaz de administración, dirección IP y Gateway predeterminada, como se observa en el Comando 3.24.

```
No.      Interface Name      IP Address    Network Mask
  1. GigabitEthernet 0/0           dhcp
  2. GigabitEthernet 0/1           unassigned
  3. GigabitEthernet 1/0           unassigned
  4. GigabitEthernet 1/1           unassigned
  5. GigabitEthernet 1/2           unassigned
  6. GigabitEthernet 1/3           unassigned
  7. GigabitEthernet 1/4           unassigned
  8. GigabitEthernet 1/5           unassigned
  9. GigabitEthernet 1/6           unassigned
 10. GigabitEthernet 1/7           unassigned
 11. GigabitEthernet 1/8           unassigned
 12. GigabitEthernet 1/9           unassigned
 13.GigabitEthernet 1/10           unassigned
 14.GigabitEthernet 1/11           unassigned
Press <any key> to close

Select Management Interface [14]: 3
Enable Autosense for Management Interface? (y/n)[y]: y
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]: 10.4.32.163/26
Enter Default Gateway IP Address [Not configured]: 10.4.32.129
Enter Central Manager IP Address (WARNING: An invalid entry will cause SETUP to
take a long time when applying WAAS configuration) [None]: 10.4.48.100
```

Comando 3.24. Configuración interfaz de administración, IP y Gateway

Paso 8: Configuración de DNS, Host, NTP.

Paso 9: Seleccionar licencia adecuada, en este caso de empresa.

Paso 10: Comprobar que los ajustes de configuración estén bien como se observa en el Comando 3.25.

```
   Parameter                 Configured Value
 1. Device Mode               AppNav Controller
 2. Interception Method       WCCP
 3. Time Zone                 PST8PDT -8 0
 4. Management Interface      GigabitEthernet 1/0
 5.     Autosense                Enabled
 6.     DHCP                     Disabled
 7.     IP Address               10.4.32.163
 8.     IP Network Mask          255.255.255.192
 9. IP Default Gateway        10.4.32.129
10. CM IP Address             10.4.48.100
11. DNS IP Address            10.4.48.10
12. Domain Name(s)            cisco.local
13. Host Name                 AppNav-WAVE-1
14. NTP Server Address        10.4.48.17
15. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration ————————
Press 'y' to select configuration, <F2> to see all configuration, 'd' to toggle
defaults display, <1-16> to change specific parameter [y]: y
Service Context configuration, including interception settings, must be performed
using  central manager .......
Please press ENTER to continue ...
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
WAAS configuration applied successfully!!
Saved configuration to memory.
Press ENTER to continue ...
```

Comando 3.25. Ajustes de configuración

Paso 11: Configurar la conexión del canal del puerto, para la red AppNav, como se observa en el Comando 3.26.

```
interface PortChannel 2
 ip address 10.4.32.71 255.255.255.192
 exit
!
interface GigabitEthernet 1/2
 channel-group 2
 no shutdown
 exit
interface GigabitEthernet 1/3
 channel-group 2
 no shutdown
 exit
```

Comando 3.26. Red AppNav

Paso 12: Para ruteadores de agregación WAN se configura rutas estáticas, como se observa en el Comando 3.27.

```
ip route 10.4.32.2 255.255.255.255 10.4.32.65
ip route 10.4.32.6 255.255.255.255 10.4.32.65
ip route 10.4.32.18 255.255.255.255 10.4.32.65
```

Comando 3.27. Rutas estáticas

Paso 13: Guardar la información en el modo EXEC.

3.1.3.3 Configuración del clúster de AppNav

Con este procedimiento se crea el clúster y asignamos nodos de Cisco WAAS. Y para configurar hay que seguir los siguientes pasos:

Paso 1: Iniciar sesión en Cisco WAAS Central Manager por medio de la interfaz.

Paso 2: *AppNav Clusters > All AppNAv Clusters.*

Paso 3: Inicie el asistente de AppNav Clúster. Como se puede observar en la Figura 3.2.

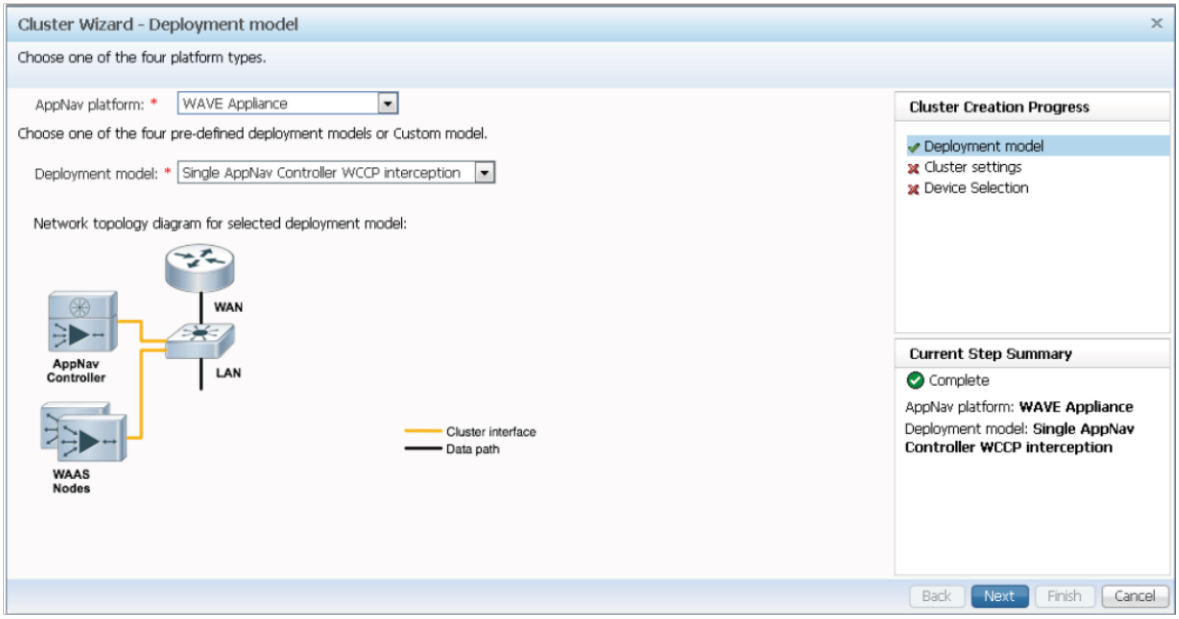

Figura 3.2. Asistente AppNav Clúster

Paso 4: En la siguiente ventana configure de la siguiente manera: Plataforma AppNav para Dispositivo WAVE, modelo de implementación se selecciona personalizado y método de interceptación elegimos WCCP. Ejemplo en la Figura 3.3.

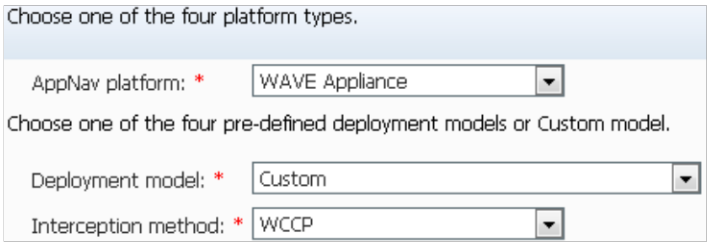

Figura 3.3. Configuraciones

Paso 5: Se le asigna un nombre al clúster y se agrega una descripción como se observa en la Figura 3.4.

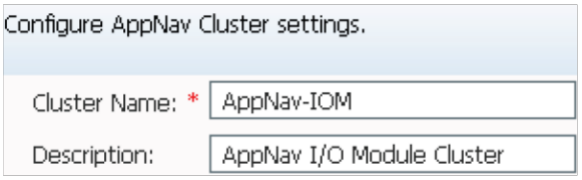

Figura 3.4. Clúster settings

Paso 6: Habilitar WCCP y configurar el método de redirección como la dirección IP.

Paso 7: Habilitar configuración avanzada de WCCP como se observa en la Figura 3.5.

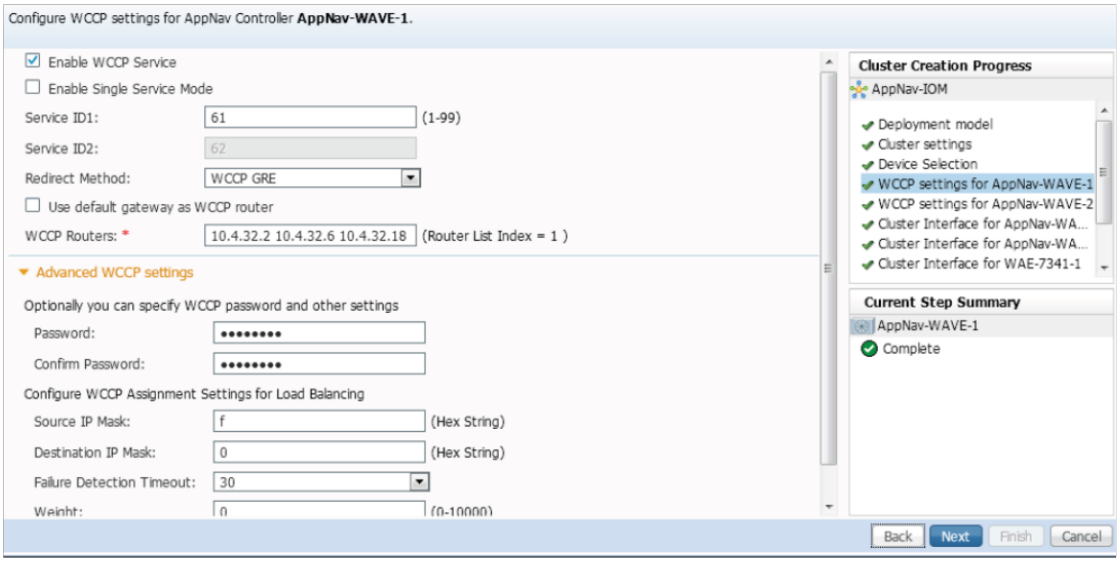

Figura 3.5. Configuración Avanzada WCCP

Paso 8: Repetir los pasos 6 y 7 si necesita controladores AppNav adicionales.

Paso 9: Seleccionar el Interfaz clúster, como vemos a continuación en la Figura 3.6.

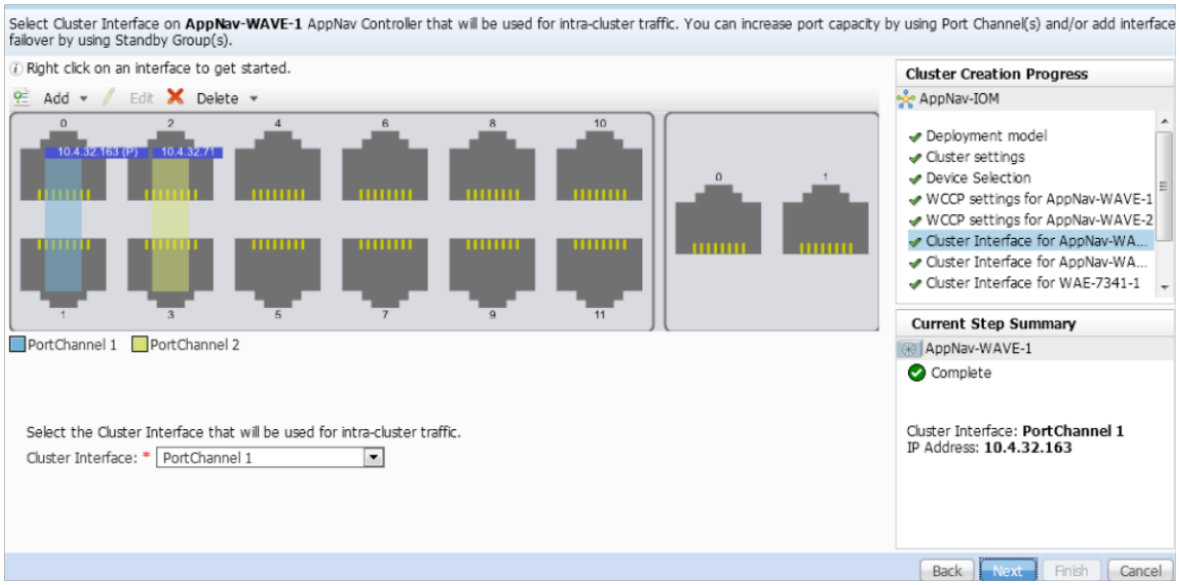

Figura 3.6. Interfaz Clúster

Paso 10: Repetir el paso anterior para cada uno de los miembros clúster (controladores Cisco AppNav y nodos Cisco WAAS).

Paso 11: Haga clic en terminar.

Paso 12: Autenticación del clúster, como indica la Figura 3.7.

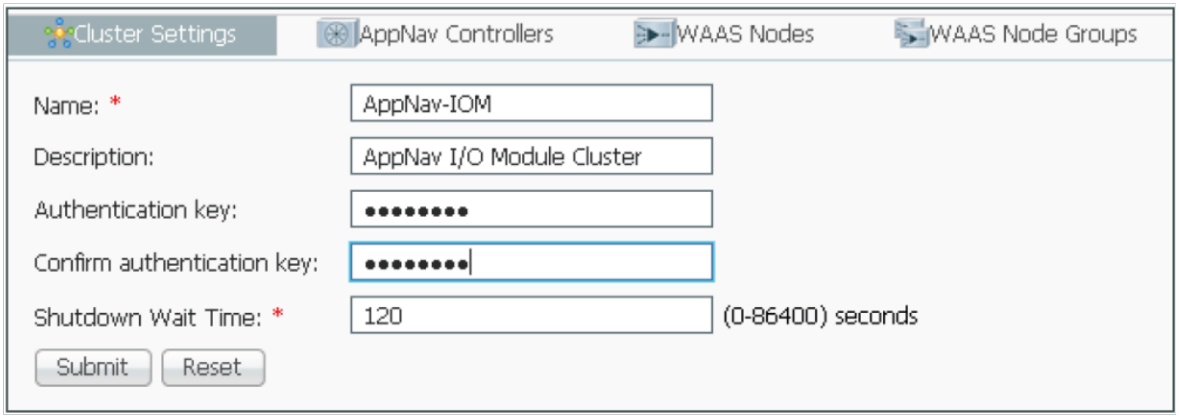

Figura 3.7. Autenticación de Clúster

3.2 Application Visibility and Control (AVC)

A continuación, se indica configuraciones básicas para instalación de AVC, pero primero se detallarán requisitos y restricciones sobre la tecnología AVC. [15]

3.2.1 Requisitos y restricciones sobre AVC

Con las reglas de AVC, puede limitar el ancho de banda para aplicaciones específicas para todos los clientes conectados a la WLAN. Estos contratos de ancho de banda existen con límites de velocidad de descarga por cliente y tiene preferencia sobre los límites de velocidad por aplicación.

La funcionalidad FNF es compatible con la tecnología inalámbrica y se basa en habilitar NetFlow en el controlador inalámbrico incorporado para el modo flexible.

El comportamiento de la solución AVC varía según la implementación inalámbrica. Las siguientes secciones describen los puntos en común y las diferencias entre todos los escenarios:

Modo flexible.

- NBAR está habilitado en un AP
- AVC empuja la configuración de FNF a los AP.
- Admite transferencia de contexto para roaming en AVC-FNF.
- Soporta exportador NetFlow.

Requisitos para AVC.

- Los puntos de acceso necesariamente deben ser compatibles con AVC.
- Configurar la función visibilidad con FNF para que funcione sin problemas la parte de control AVC

Restricciones para AVC.

- Itinerancia en la capa 2 es incompatible con los controladores inalámbricos integrados.
- Tráfico multidifusión.
- El tráfico de multidifusión no es compatible.
- AVC es compatible con limitados puntos de acceso y son:
    - Puntos de acceso de la serie Cisco Aironet 1800.
    - Punto de acceso de la serie Cisco Aironet 2700.
    - Punto de acceso de la serie Cisco Aironet 2800.
    - Puntos de acceso de la serie Cisco Aironet 3700.
    - Puntos de acceso de la serie Cisco Aironet 3800.
    - Puntos de acceso de la serie Cisco Aironet 4800.
- No compatibles con los siguientes puntos de acceso: Cisco Aironet 702W, 702I
- QoS pueden reconocer solo aquellas aplicaciones con la visibilidad de aplicación.
- NetFlow no es compatible en los enlaces de datos.
- No asignar el perfil WLAN al perfil de política no habilitado para AVC.
- La configuración de la política de QoS que se basa en NBAR es compatible a nivel de cliente y nivel de BSSID.
- AVC admite un límite máximo de 23 reglas.

3.2.2 Descripción general de la configuración de AVC

Para configurar AVC, siga estos pasos:

- Utilice el comando básico *record Wireless AVC,* para crear el monitor.
- Iniciar un perfil de política inalámbrica.
- A esta política aplicar el monitor de flujo.

- Crear una etiqueta de política inalámbrica.
- Al perfil de política se le asigna la WLAN.
- A los AP se le adjunta la etiqueta de política.

3.2.3 Configuración de una WLAN para AVC

Para configurar tenemos que seguir los siguientes pasos:

Paso 1: Se configura WLAN, con el Comando 3.28. que se presenta a continuación.

```
Device(config)# wlan wlan1 1 ssid1
```

Comando 3.28. Configurar WLAN

Paso 2: Apagar WLAN para guardar configuraciones como se muestra en el Comando 3.29.

```
Device(config-wlan)# shutdown
```

Comando 3.29. Apagar WLAN

Paso 3: Desactivar la configuración AKM para dot1x con el Comando 3.30. que se muestra a continuación.

```
Device(config-wlan)# no security wpa akm dot1x
```

Comando 3.30. Desactivar AKM

Paso 4: Deshabilitar cifrados WPA2 para AES como se muestra en el comando 3.31.

```
Device(config-wlan)# no security wpa wpa2 ciphers aes
```

Comando 3.31. Deshabilita WPA2

3.2.4 Configuración de una etiqueta de política

Para configurar realizamos el siguiente procedimiento:

Paso 1: Entrar en el modo de configuración global, como se indica en el Comando 3.32.

```
Device# configure terminal
```

Comando 3.32. Configuración Global

Paso 2: Configurar la etiqueta de política entrando al modo de configuración de etiqueta de política como se observa a continuación en el Comando 3.33.

```
Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag
```

Comando 3.33. Política de etiquetas

Paso 3: Guardar configuración y salir del modo de configuración para regresar al modo EXEC privilegiado como se observa a continuación en el Comando 3.34.

```
Device(config-policy-tag)# end
```

Comando 3.34. Fin

3.2.5 Verifique la configuración de AVC

Para la verificación nos basamos en los siguientes pasos que se observan a continuación:

Paso 1: Mostrar información acerca de las principales aplicaciones y usuarios que usan estas aplicaciones, detallado en el Comando 3.35.

```
Device# show avc wlan wlan_avc top 2 applications aggregate
```

Comando 3.35. Muestre AVC WLAN

Paso 2: Mostrar información acerca del número de aplicaciones, como se observa en el Comando 3.36.

```
Device# show avc client 9.3.4 top 3 applications aggregate
```

Comando 3.36. Mostrar AVC Client

Paso 3: Mostrar información acerca de las principales aplicaciones y usuarios que utilizan dichas aplicaciones como se observa en el Comando 3.37.

```
Device# show avc wlan wlan_avc application app top 4 aggregate
```

Comando 3.37. Muestre AVC WLAN

Paso 4: Mostrar el resumen de todos los puntos de acceso conectados al controlador inalámbrico incorporado, como se observa en el Comando 3.38.

```
Device# show ap summary
```

Comando 3.38. Mostrar resumen ap

Paso 5: Mostrar el resumen de todos los puntos de acceso con etiquetas de política, observado en el Comando 3.39.

```
Device# show ap tag summary
```

Comando 3.39. Mostrar el resumen de etiqueta ap

Nota: Asegurarse que los clientes inalámbricos estén asociados a la WLAN y generen tráfico, después esperar 90 segundos para ejecutar el comando.

4 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En este capítulo se va a comentar todos los aspectos importantes y sobresalientes del trabajo, para exponer los resultados se realiza una comparación para poder describir las mejorías y avances que se tiene gracias a la tecnología iWAN.

4.1 Resultados

En términos generales al finalizar este trabajo se pudo observar el gran paso y progreso brindado para redes WAN empresariales, al implementar la solución de Cisco que es la Red Inteligente WAN (iWAN). Esta tecnología ha marcado un antes y un después y a continuación se detallarán más a profundidad los aspectos más importantes de esta tecnología.

Analizando, uno de los aspectos generales que ayudó a iWAN es la migración de WAN a Internet, por la amplia demanda de ancho de banda, Internet tiene una plataforma más estable y a su vez el precio en comparación al rendimiento es mejor ya que tiene bajo costo, pero por lo general se implementa en sitios pequeños, aunque sin inconvenientes se puede implementar en todas las sucursales iWAN de Cisco.

Los resultados que se obtiene al tener una empresa con Cisco iWAN:

- **Retorno de inversión:** Se maximiza el uso de la WAN.
- **Disminución de costos:** Transporte menos costoso, sin dejar a un lado el rendimiento, confiabilidad y seguridad.
- **Interconexión rápida entre sucursales:** Asegurar todos los terminales de sucursales.
- **Rendimiento óptimo:** Red que tiene reconocimiento de aplicaciones, resolviendo problemas de red más rápido.
- **Compresión Avanzada:** Minimiza la carga de WAN, reduce el ancho de banda.

- **Simplificación de operaciones para sucursales:** Se podrá administrar de manera remota.

Debido a los cambios ya existentes, Cisco desarrolló una nueva tecnología llamada WAAS (Wide-Area Apllication Services), fue implementada con el objetivo de optimizar las aplicaciones de iWAN.

WAAS presenta soluciones bastante importantes para la red iWAN y como resultados sobresalientes se detallam los siguientes:

- Cuando la latencia de la red es alta, WAAS reduce en gran cantidad las respuestas de ida y vuelta gracias a los adaptadores de protocolo.
- Si se tiene un ancho de banda muy pequeño, lo que hace WAAS es reducir el monto de la cantidad datos enviados a la WAN por medio de la funcionalidad de archivos y compresión de datos, esto mejora notoriamente el tiempo de respuesta de aplicaciones con enlaces con bastante tráfico.
- Cuando se presenta deficiente utilización del enlace, WAAS usa las funciones de optimización de TCP, las mismos que bajan el número de errores de TCP receptados por la WAN y a su vez le hace más grande a la ventana TCP; esto se hace para que un usuario/cliente pueda recibir en el mismo tiempo una mayor cantidad de datos.
- En el momento en que se pierde un paquete, la pila TCP optimizada en WAAS pone fin a estas dificultades que son asociadas con la gran pérdida de paquetes y a su vez protege la comunicación de la WAN.
- Acelera paquetes, Cisco WAAS tiene varias funciones de aceleración de aplicaciones, como predicción de operación y procesamiento de lotes, supresión de mensajes inteligentes, almacenamiento en caché entre otros.

La tecnología AVC también presenta grandes cambios en las redes iWAN, y presenta los siguientes beneficios:

- Tiene acceso a una mayor visibilidad de uso de aplicación, lo cual mejora la seguridad y el conocimiento del cliente.
- Gestiona y también planifica la capacidad de red por medio de informes anteriormente predefinidos y personalizados.

- Usa técnicas llamadas prioridad y modelado de QoS para la priorización de aplicaciones para la empresa.
- Reduce los costos operativos por medio de optimización de la red.
- Gracias a que se implementó las políticas de uso justo se obtiene una mejor calidad de experiencia (QoE) impartida para todos los usuarios/clientes.

4.2 Conclusiones

- Con la optimización de las aplicaciones iWAN se ha notado un cambio notable en cuanto a que ahora se ajusta mucho mejor a las necesidades del cliente/usuario, ofreciéndole un mayor ancho de banda, con menor latencia y a su vez bajando costos, se concluye que era necesario este avance tecnológico ya que en la actualidad se procesa una cantidad de datos mayor por lo que se requiere un ancho de banda mayor para poder hacerlo sin ningún inconveniente.
- Las tecnologías de optimización que tenemos en iWAN las presenta Cisco WAAS que es una alternativa que presenta soluciones para optimizar las diferentes aplicaciones aprovechando al máximo los recursos y mejorando los problemas frecuentes que tenían las redes WAN, como son la alta latencia de red, restringido ancho de banda, deficiente utilización del enlace entre otros. A su vez Cisco WAAS presenta mejoras en la experiencia del usuario ya que cuenta con aplicaciones y servicios que brindan mayor efectividad y productividad.
- Con la tecnología Cisco AVC ya no hay necesidad de instalar actualizaciones que son costosas, también Cisco AVC brinda un servicio totalmente innovador basado en optimizar las operaciones y también maximizar inversiones en la red, sin dejar a un lado la reducción de costos.
- La tecnología Cisco AVC marca una diferencia en resolución de problemas, debido a que esta tecnología hace posible la resolución de problemas de forma mucho más rápidas que las anteriores y esto hace que se tenga menos interrupciones de red, lo cual lo hace destacarse y más confiable.

- Con las características de TFO (TCP Flow Optimization) que es una función que es usada por WAAS, se logra la compresión que consiste en reducir el tamaño de los datos que pueden ser transmitidos a una WAN, esto se da gracias a que se elimina información redundante de la WAN, optimizando el espacio.

- Se realizó una recopilación de información para analizar y aprender acerca de la optimización de aplicaciones para redes iWAN empresariales, por lo que logramos comprender que gracias a estas tecnologías tanto WAAS como AVC, la red iWAN tiene un alto impacto en el mundo empresarial por sus beneficios en relación con el cliente que nos brindan y da un gran salto tecnológico ya que las ventajas y resultados que se obtienen son considerables.

- La tecnología Cisco iWAN tiene un retorno de inversión más rápido que la red WAN, ya que la tecnología Cisco iWAN sabe aprovechar en su totalidad los recursos de WAN, por lo que no se necesita mayor inversión que la que ya se hizo inicialmente y se economiza en costos. La tecnología Cisco iWAN tiene una infraestructura en la que se aprovecha de DMVPN y PfR, lo cual hace que el tráfico pase directo sin pasar por el núcleo de la red, reduciendo costos de tráfico. La meta es que Cisco iWAN sea más económico incluso que los costos con MPLS.

4.3 Recomendaciones

- Se recomienda utilizar la implementación de WAAS virtual, por medio del software vWAAS que tiene un interfaz sencillo de utilizar y tienen la mayoría de funciones que se presentan en el dispositivo físico. El software vWAAS es más usado en general cuando no se puede implementar dispositivos WAVE en físico.

- Se recomienda usar las interfaces de Cisco WAAS adecuadamente, ya que fueron hechas para que el usuario pueda administrar, configurar y monitorear los diferentes componentes de la red. La interfaz más importante es la GUI de WAAS *Central Manager*, es el dispositivo principal con el que se ayuda a la administración, por lo que es recomendable siempre utilizar GUI de WAAD *Central Manager*, siempre que sea posible ya que hay funciones que se hacen directamente desde la propia interfaz como es el caso de WAAS *Command-line Interface* (CLI), el cual tiene funciones específicas.

- Antes de instalar o configurar la tecnología AVC, se recomienda revisar y verificar las plataformas que son compatibles, también tomar en cuenta los requisitos y restricciones que presentan para no tener problemas futuros, ya que AVC al ser una tecnología nueva se tiende a tener problemas.

- Cuando se use la función TCP de WAAS se debe tener en cuenta qué técnica de compresión usar, se debe tomar en cuenta el flujo de datos, debido a que el flujo de datos no supera los cientos de bytes, es recomendable usar Compresión LZ y por otro lado si supera esa cantidad es recomendable usar la técnica de Eliminación de redundancia de datos (DRE).

- Debido a que ahora se consume un mayor ancho de banda, es recomendable para todas las empresas migrar de la WAN a Internet, gracias a la migración se puede economizar debido a que Internet es una alternativa de bajo costo, sin afectar al rendimiento, confiabilidad y seguridad; también en base a Internet mejora la disponibilidad de la red. Debido a que conlleva riesgos, la mayoría de las empresas está optando por implementar Internet como WAN solamente en sitios más pequeños o simplemente a la ruta de soporte.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] C. R. W. ECHEVERRIA, «DISEÑO E IMPLEMENTACIÓN DE LA TECNOLOGÍA IWAN Y SEGURIDAD NGFW EN LA ADUANA NACIONAL,» vol. 1, nº 1, p. 98, 2018.

[2] «Introduction to DMVPN,» 30 Octubre 2015. [En línea]. Available: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn. [Último acceso: 05 Enero 2022].

[3] CISCO, «Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs) - Cisco,» [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html. [Último acceso: 05 Enero 2022].

[4] «Dynamic Multipoint VPN (DMVPN),» [En línea]. Available: https://www.fieldengineer.com/blogs/dynamic-multipoint-vpn. [Último acceso: 4 Enero 2022].

[5] CISCO, «Introducción al enrutamiento de rendimiento (PfR) > Enrutamiento de rendimiento (PfR) | Prensa de Cisco,» *Cisco Press,* vol. I, pp. 50-60, 2018.

[6] C. Spera, «CÓMO OPTIMIZAR EL TRÁFICO WAN,» *INFORMACIÓN TÉCNICA,* vol. l, nº 1, p. 2, 2019.

[7] CISCO, «WAN inteligente de Cisco (IWAN),» *CISCO,* vol. l, nº 2, p. 2, 2013.

[8] S. e. I. T. S.A.C, «Optimización WAN :: Servitic,» 2014. [En línea]. Available: https://servitic0.webnode.es/servicios/servicios-ti-/optimizacion-wan-wan-opt-/. [Último acceso: 05 Enero 2022].

[9] CISCO, «Cisco Wide Area Application Services Configuration Guide (Software Version 4.0.7) - Introduction to Cisco WAAS [Cisco Wide Area Application Services (WAAS) Software],» CISCO, 2019. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/app_ntwk_services/waas/waas/v407/configuration/guide/cfgd/intro.html. [Último acceso: 05 Enero 2022].

[10] CISCO, «Introduction to Cisco WAAS [Cisco Wide Area Application Services (WAAS) Software],» 2019. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/app_ntwk_services/waas/waas/v407/configuration/guide/cfgd/intro.html. [Último acceso: 05 Enero 2022].

[11] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, Cisco Intelligent WAN (IWAN), Indianápolis, IN 46240 EE. UU.: Cisco Systems, Inc., 2017.

[12] CISCO Systems, Inc., Cisco Wide Area Application Services Configuration Guide, 170 West Tasman Drive San Jose, CA 95134-1706 USA: Americas Headquarters, 2007.

[13] CISCO, Improve Application Performance With Application Visibility and Control (AVC), 2012.

[14] CISCO, Application Optimization Using Cisco WAAS, 2014.

[15] CISCO, «Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE Cupertino 17.7.x - Application Visibility and Control [Cisco Embedded Wireless Controller on Catalyst 9115AX Access Points],» Cisco, Febreo 2021. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-7/config-guide/ewc_cg_17_7/application_visibility_and_control.html. [Último acceso: 18 Enero 2022].

6 ANEXOS