



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Diseño e implementación de solución antiddos usando
Black Hole activado remotamente para Huawei Perú**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de
Telecomunicaciones

AUTOR

Stefano Takeshi SAC MARTINEZ

ASESOR

José VIDAL HUARCAYA

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Sac, S. (2024). *Diseño e implementación de solución antiddos usando Black Hole activado remotamente para Huawei Perú*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Stefano Takeshi Sac Martinez
Tipo de documento de identidad	DNI
Número de documento de identidad	75766523
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	José Vidal Huarcaya
Tipo de documento de identidad	DNI
Número de documento de identidad	09450859
URL de ORCID	https://orcid.org/0000-0002-7702-8162
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Daniel Díaz Ataucuri
Tipo de documento	DNI
Número de documento de identidad	07139361
Miembro del jurado 1	
Nombres y apellidos	Jean Carlos Malca Fernández
Tipo de documento	DNI
Número de documento de identidad	45535181
Miembro del jurado 2	
Nombres y apellidos	Raúl Sixto Hinojosa Sanchez
Tipo de documento	DNI
Número de documento de identidad	08605661
Datos de investigación	
Línea de investigación	C.0.3.10 Redes de datos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: América Móvil Perú S.A.C. País: Perú Departamento: Lima Provincia: Lima Distrito: La Victoria Latitud: -12.086693 Longitud: -77.014545
Año o rango de años en que se realizó la investigación	2021-2022
URL de disciplinas OCDE	Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.00



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN TRABAJO DE SUFICIENCIA PROFESIONAL

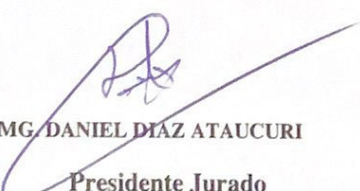
ACTA N°030/FIEE-CTGT/2024

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 4 de abril del 2024, como presidente de Jurado el **MG. DANIEL DIAZ ATAUCURI**, integrado por el Miembro de Jurado el **MG. JEAN CARLOS MALCA FERNANDEZ**, el Miembro de Jurado **MG. RAUL SIXTO HINOJOSA SANCHEZ** y Miembro Asesor el **ING. JOSÉ VIDAL HUARCAYA**.

Después de escuchar la Sustentación presencial del Trabajo de Suficiencia Profesional del Bach. **STEFANO TAKESHI SAC MARTINEZ** con código N° **15190280** que para optar el Título Profesional de Ingeniero de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE SOLUCIÓN ANTIDIDOS USANDO BLACK HOLE ACTIVADO REMOTAMENTE PARA HUAWEI PERÚ**

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió aprobar otorgándole el calificativo de **15 (QUINCE)**

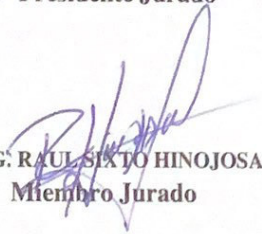
Ciudad Universitaria, 4 de abril del 2024


MG. DANIEL DIAZ ATAUCURI

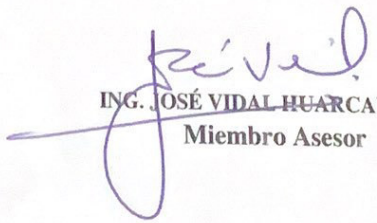
Presidente Jurado


MG. JEAN CARLOS MALCA FERNANDEZ

Miembro Jurado


MG. RAUL SIXTO HINOJOSA SANCHEZ

Miembro Jurado

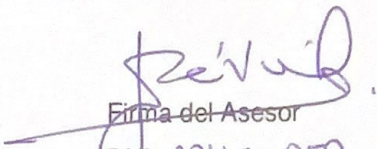

ING. JOSÉ VIDAL HUARCAYA

Miembro Asesor



CERTIFICADO DE SIMILITUD

Yo José Vidal Huarcaya en mi condición de asesor acreditado con el Acta de Sustentación de Trabajo de Suficiencia Profesional: DISEÑO E IMPLEMENTACIÓN DE SOLUCIÓN ANTIDDOS USANDO BLACK HOLE ACTIVADO REMOTAMENTE PARA HUAWEI PERÚ, presentado por el bachiller Stefano Takeshi Sac Martinez, para optar al título profesional de Ingeniero de Telecomunicaciones. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 8% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**. Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado correspondiente.


Firma del Asesor

DNI: 09450859

Nombres y apellidos del asesor:

ING. JOSÉ VIDAL HUARCAYA

DEDICATORIA

Este trabajo está dedicado a mis padres por el gran esfuerzo realizado, la motivación e inspiración para seguir siempre adelante, a mis abuelos y tíos por el cariño y el apoyo constante en todos mis años de vida. A mis amigos que estuvieron siempre para mí y que hicieron la etapa universitaria una gran experiencia de vida.

AGRADECIMIENTOS

Un agradecimiento especial a la Universidad Nacional Mayor de San Marcos que me permitió aprender y vivir una de las mejores etapas de mi vida. A la empresa Claro por brindarme la oportunidad de ser parte de ella y permitirme desarrollarme como profesional, a mis compañeros de trabajo que son excelentes profesionales y personas. A mi asesor José Vidal Huarcaya por su orientación y dedicación para desarrollar el presente trabajo.

RESUMEN

El presente trabajo tiene como objetivo presentar el diseño y la implementación de una solución para evitar ataques de denegación de servicios distribuidos (DDoS – Distributed Denial of service attack por sus siglas en inglés) usando la técnica de filtrado blackhole activado remotamente (RTBH - Remotely Triggered Black Hole en sus siglas en inglés) en los routers de borde (BR – Border Router por sus siglas en inglés) de la red de un operador móvil para brindar un servicio al cliente Huawei.

Se profundizará en qué consiste la técnica de filtrado de black hole activado remotamente, los protocolos usados para su desarrollo y el concepto de términos técnicos como ataque de denegación de servicios distribuidos, protocolo BGP y otros.

El diseño de la solución se realizó de manera conjunta con un proveedor en base a la topología de red actual del operador y a las necesidades del cliente. Finalmente se presentarán las pruebas realizadas, así como los resultados obtenidos de la implementación.

Como conclusión, se comprobó que la solución implementada cumple con el objetivo de mitigar ataques a través del descarte de tráfico malicioso.

Palabras clave: Denegación de ataque de servicio, Black hole activado remotamente, BGP, descarte de tráfico, comunidad BGP.

ABSTRACT

The objective of this present document is to present the design and implementation of a solution to avoid Distributed denial of services (DDoS – Denial of service attack by its acronym in English) using the filtering technique remotely triggered black hole (RTBH - Remotely Triggered Black Hole by its acronym in English) on the border routers (BR – Border Router by its acronym in English) on a carrier's network to provide a service to Huawei as client.

It will deepen about the filtering technique remotely triggered black hole consists, the protocols that were used for its development and the meaning of technical terms like distributed denial of services attack, BGP protocol and others.

The solution's design was executed with support of a vendor based on the current topology of the carrier's network and the client's necessities. Finally, the tests will be showed as well as the results obtained from the implementation.

As a conclusion, the implemented solution fulfills with the objective of mitigate attacks dropping the undesirable traffic.

Keywords: Denial of service attack, Remotely triggered black hole, BGP, traffic dropping, BGP community.

TABLA DE CONTENIDO

RESUMEN	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
LISTA DE FIGURAS	viii
LISTA DE TABLAS	ix
CAPITULO I: INTRODUCCIÓN.....	1
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	2
2.1 Empresa	2
2.2 Periodo de duración de la actividad.....	2
2.3 Finalidad y objetivos de la entidad.....	2
2.4 Razón social	3
2.5 Dirección postal	3
2.6 Correo electrónico del profesional a cargo.	3
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	4
3.1 Organización de la actividad.....	4
3.2 Finalidad y objetivos de la Actividad	4
3.2.1 Finalidad	4
3.2.2 Objetivos	5
3.2.2.1 Objetivo General:	5
3.2.2.2 Objetivos Específicos:.....	5
3.3 Problemática.....	5
3.3.1 Problema General	6
3.3.2 Problemas Específicos	6
3.3.3 Justificación e importancia de la investigación	6
3.4 Metodología	7

3.4.1	Bases teóricas	7
3.5	Marco conceptual	11
3.5.1.1	Ataques DDOS:	11
3.5.1.2	Interfaz null0:	12
3.5.1.3	Protocolo BGP:	13
3.5.1.4	Enrutamiento basado en políticas:	15
3.5.1.5	RTBH:	15
3.6	Procedimiento.....	18
3.6.1	Etapas:	18
3.6.1.1	Análisis de Factibilidad del requerimiento:	18
3.6.1.2	Diseño de la solución:	19
3.6.1.3	Implementación de la solución:	22
3.6.1.4	Pruebas del servicio:	28
3.6.1.5	Entrega del servicio	31
3.7	Resultado de la actividad.....	31
CAPITULO IV: CONCLUSIONES		33
4.1	Justificación	33
4.2	Descripción de la implementación	33
4.3	Conclusiones	34
CAPITULO V: RECOMENDACIONES		36
CAPITULO VI: BIBLIOGRAFIA		38
CAPITULO VII: ANEXOS		40

LISTA DE FIGURAS

<i>Figura 1:</i> Organigrama de la empresa	4
<i>Figura 2:</i> Ejemplo protocolo BGP.....	14
<i>Figura 3:</i> Estructura de una comunidad BGP.....	14
<i>Figura 4:</i> Funcionamiento de la técnica RTBH.....	17
<i>Figura 5:</i> Topología General de la solución RTBH.....	21
<i>Figura 6:</i> Propuesta de ubicación para instalación de gabinete para nuevos equipos en DCs.	24
<i>Figura 7:</i> Gabinetes instalados en DCs.	25
<i>Figura 8:</i> Vista de equipos instalados en DCs.	25
<i>Figura 9:</i> Correo de culminación de integración routers Blackhole.	26
<i>Figura 10:</i> Vista de integración de equipos a los gestores de monitoreo.....	26
<i>Figura 11:</i> Rutas blackhole configuradas en equipos Blackhole.	26
<i>Figura 12:</i> Aprendizaje de ruta blackhole en los equipos de borde.....	27
<i>Figura 13:</i> Confirmación de culminación de configuración de la segunda ventana.	28
<i>Figura 14:</i> Validación de aprendizaje de segmento de red cliente en internet.	29
<i>Figura 15:</i> Tabla de enrutamiento previo a las pruebas de mitigación.....	29
<i>Figura 16:</i> Tabla de enrutamiento recibiendo la ruta estática con la comunidad blackhole.....	30
<i>Figura 17:</i> Correo de validación del servicio por parte del cliente.....	31

LISTA DE TABLAS

<i>Tabla 1:</i> Cronograma de las 3 primeras actividades.	23
<i>Tabla 2:</i> Cronograma de la cuarta y quinta actividad.	23
<i>Tabla 3:</i> Cronograma de la sexta a la octava actividad.	23
<i>Tabla 4:</i> Cronograma de la novena a la undécima actividad.	23

CAPITULO I: INTRODUCCIÓN

El presente documento describe el proceso de diseño e implementación de una solución de mitigación de ataques de denegación de servicios distribuidos como un requerimiento especial para un cliente del sector de la tecnología de la información usando la infraestructura de red de un operador móvil.

A continuación, se describirá la estructura del informe:

En el capítulo I, se brindará el resumen de la estructura del presente documento.

En el capítulo II, se detalla información de la empresa en la que se implementó la solución como el nombre, dirección, razón social, visión, misión, duración de la actividad y personal a cargo.

En el capítulo III, se abordarán los problemas y objetivos tanto específicos como generales, los documentos académicos que se han revisado como referencia para el presente trabajo, conceptos técnicos para mejor entendimiento del informe y la metodología de la implementación.

En el capítulo IV, se brinda la justificación y las conclusiones como resultado de la implementación del siguiente trabajo.

En el capítulo V, se detallan las recomendaciones luego del análisis de las etapas de implementación y del procedimiento utilizado para el desarrollo del presente trabajo.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Empresa

Claro Perú es subsidiaria de América Móvil y opera en el país desde el 10 de agosto de 2005. América Móvil es la empresa líder en servicios integrados de telecomunicaciones en Latinoamérica. Opera bajo la marca Claro en 16 países del continente: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, Paraguay, Perú, Puerto Rico, República Dominicana y Uruguay.

2.2 Periodo de duración de la actividad.

La actividad inició con el análisis de factibilidad del requerimiento en Noviembre de 2019 y culminó con la validación de las pruebas del servicio en fines de Abril de 2022.

2.3 Finalidad y objetivos de la entidad

Proveer servicios de telecomunicaciones con la más alta calidad, más amplia cobertura y constante innovación para anticiparnos a las necesidades de

comunicación de nuestros clientes; generar el mayor bienestar y desarrollo personal y profesional de nuestros trabajadores, proporcionar bienestar y desarrollo a la comunidad y exceder los objetivos financieros y de crecimiento de nuestros accionistas.

2.4 Razón social

La empresa opera con la razón social América Móvil Perú S.A.C. y RUC 20467534026.

2.5 Dirección postal

La sede principal de la empresa queda ubicada en la dirección Av. Nicolás Arriola 480 – La Victoria, Lima, Lima y el código postal es 15034.

2.6 Correo electrónico del profesional a cargo.

Dante Rodriguez Marquez con correo dante.rodriguez@claro.com.pe.

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad



Figura 1: Organigrama de la empresa. Fuente: Success Factors

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

El presente documento tiene como finalidad brindar el procedimiento de diseño e implementación de una solución para mitigar ataques de denegación de servicios distribuidos usando la técnica de filtrado black hole activado remotamente para el cliente Huawei de acuerdo con sus necesidades y con el objetivo de asegurar la continuidad de los servicios que brinda. Este mecanismo de defensa es ampliamente utilizado en los últimos años ante la creciente frecuencia de ataques DDoS y el aumento considerable año tras año

del volumen de tráfico generado por los atacantes ya que es una de las principales virtudes de la técnica blackhole. Esto resulta como consecuencia del desarrollo de la tecnología y la globalización del uso y facilidad de acceso a Internet desde múltiples dispositivos, lo cual hace más vulnerable las redes de los usuarios finales como de empresas y proveedores de servicios de internet como también pone en riesgo los servicios que estos brindan.

3.2.2 Objetivos

3.2.2.1 Objetivo General:

Diseñar e Implementar una solución de blackhole activado remotamente para mitigación de ataques DDoS sobre enlaces de internet para la empresa Huawei.

3.2.2.2 Objetivos Específicos:

- a) Realizar el levantamiento de información de la infraestructura de red, como también de las necesidades del cliente para definir el diseño de la solución.
- b) Determinar los equipos que realizarán el descarte de tráfico malicioso de ataques DDoS.
- c) Realizar simulación de ataque a uno o varios hosts del cliente para validar el funcionamiento correcto de la solución implementada.

3.3 Problemática

Se identificó por parte del cliente Huawei la necesidad de contar con un mecanismo de mitigación de ataques DDoS con el uso de la técnica de blackhole activado remotamente sobre los enlaces de Internet contratados con la empresa Claro sobre los cuales realiza intercambio de segmentos de

red públicos a fin de asegurar la disponibilidad para los distintos servicios que brinda, como también para asegurar la seguridad de su red.

3.3.1 Problema General

¿Cómo podemos diseñar e implementar una solución blackhole activado remotamente para mitigar ataques DDoS para la empresa Huawei?

3.3.2 Problemas Específicos

- a) ¿Qué criterios se pueden establecer para recopilar información adecuada para el diseño de la solución basado en blackhole activado remotamente?
- b) ¿Cómo definir los equipos de red que realizarán el descarte de tráfico malicioso de ataques de denegación de servicios DDoS?
- c) ¿Cómo realizar la validación de la solución implementada y cumplir con la funcionalidad de mitigación de tráfico malicioso?

3.3.3 Justificación e importancia de la investigación

El presente trabajo tiene como importancia brindar a la empresa Huawei un mecanismo de defensa a su red a fin de evitar que sufra ataques de denegación de servicios distribuidos y afectación e indisponibilidad de los servicios que brinda ya que podrían incurrir en incumplimientos contractuales (por ejemplo, incumplimiento de SLA, sanciones económicas, penalidades, etc.), así como podría afectar a los equipos de su infraestructura de red (implicando cambio de equipos servidores, routers, etc.). Asimismo, la solución implementada puede ser habilitada para otros clientes corporativos teniendo en cuenta sus requerimientos y que no todas las redes de clientes son homogéneas.

3.4 Metodología

3.4.1 Bases teóricas

- a) Silvia Bravo realizó un trabajo de tesis doctoral titulado “Contribuciones para la Detección de Ataques Distribuidos de Denegación de Servicio (DDoS) en la Capa de Aplicación” el cual tuvo como objetivo una propuesta de detección ataques DDoS evaluando las características de la interacción del usuario con un sitio web basado en las funciones del mouse y pulsaciones del teclado. Comenta que el enfoque de detección es de bajo costo y que consta de dos pasos. En el primer paso se obtiene las características del usuario en tiempo real mientras navega a través de sitios web y en el segundo cada característica extraída es utilizada en un algoritmo de orden con la finalidad de identificar y diferenciar a un usuario real de un robot o de un ataque DDoS.

La problemática principal de este trabajo estaba centrada en diferenciar las solicitudes de usuarios reales de los ataques DDoS ya que los atacantes envían solicitudes de baja frecuencia emulando la solicitud de un usuario real con lo cual evadían los mecanismos de detección existentes. Por otro lado, también se mencionó el caso de sitios web con alta demanda de solicitudes en un corto intervalo de tiempo ya que pueden ser percibidos como un ataque DDoS ya que generan lentitud en la conexión hasta la interrupción del servicio debido al aumento significativo del tráfico.

En el trabajo especifica los elementos principales que se emplean para ejecutar un ataque DDoS como son el atacante, los programas de control, sistemas de generación de tráfico y las víctimas. También brinda posibles causas por las que se dan los ataques DDoS como son la seguridad global de internet, los recursos limitados de Internet, vacíos

en las comprobaciones de autenticación a nivel de red, difícil identificación de responsables.

Asimismo, clasifica las motivaciones para ejecución de un ataque DDoS en 7 categorías principales los cuales son: Factores financieros, Rendimiento lento de la red, Venganza, Motivos ideológicos, Desafío intelectual, Indisponibilidad del servicio, Guerra cibernética.

Como parte del análisis para el desarrollo de su trabajo propuso 48 diferentes técnicas de detección de ataques DDoS siendo la más utilizada las redes neuronales e identificó 28 variables para la detección de ataques DDoS siendo las más utilizadas los paquetes y direcciones IP. Se indica que la mayoría de las técnicas son implementadas en la red ya que es el medio por donde cursa el tráfico y por lo tanto se puede extraer más información.

Como resultado de las pruebas realizadas se obtuvo que la eficacia de detección era del 100% posicionándose en primer lugar como la mayor tasa de efectividad frente a otras propuestas de detección de ataques DDoS ya que el método de detección consideraba el dinamismo del usuario con los sitios web lo cual permitía diferenciar una solicitud real de un ataque informático. Cuando los ataques DDoS eran detectados, el método propuesto impedía que el usuario siga procesando solicitudes al servidor web. (Bravo Mullo, 2019)

- b) Elsayed M y Azer M realizaron un trabajo titulado “Detección y contramedidas de Ataques DDoS en computación en la nube” que tiene como objetivo la propuesta de una solución para detectar ataques DDoS a través del sistema de detección de fuente abierta SNORT que reaccionaría mitigando el ataque basándose en la técnica de blackhole activado remotamente a fin de asegurar la disponibilidad de los servicios, como antecedentes se menciona que los ataques DDoS son una de las principales amenazas de los servicios Cloud y que el tamaño promedio de estos aumentó a 800Gbps en 2016 y sigue aumentando año tras año. Debido a que los ataques DDoS pueden dañar la infraestructura de los servicios Cloud los autores identificaron la necesidad de un sistema que detecte y mitigue los ataques DDoS antes que estos sean enrutados a

la nube ya que los métodos tradicionales de seguridad como uso de Firewalls y sistemas de detección de intrusos (IDS - Intrusion Detection System por sus siglas en inglés) son incapaces de mitigar y asegurar la continuidad de los servicios Cloud, ya que los Firewalls presentan vulnerabilidades que los hacen fáciles de penetrar y no proveen una detección adecuada ante ataques de alta capacidad. Asimismo, los IDS no pueden reportar que el atacante usa una dirección IP que ha sido suplantada y si lo detectara no podría identificar a los atacantes.

Los autores proponen los equipos de borde como el lugar ideal para el descarte del tráfico ya que el objetivo es descartar el tráfico lo más pronto posible antes que este pueda entrar a la red y evitar dañar a los servidores cloud. Debido a que el principal problema de la técnica RTBH es el descarte de todo el tráfico sin importar que este sea legítimo o malicioso, los autores añadieron a la técnica un centro de limpieza para que el funcionamiento sea de la siguiente forma: Como requerimiento previo el router disparador debe contar con una ruta estática que redirija el tráfico al centro de limpieza en vez de descartarlo, cuando se detecte un ataque DDoS el router disparador propagará la ruta estática preconfigurada hacia los routers de borde usando IBGP. Posterior a ello los routers de borde actualizarán su tabla de enrutamiento con la nueva ruta y redirijan el tráfico al centro de limpieza, este filtraría el tráfico legítimo para que lo reenruten al servidor cloud de destino mientras que el tráfico malicioso sería descartado.

Como conclusión se validó que el sistema de detección SNORT al detectar un ataque enviaba la ruta estática al router disparador el cual enviaba las actualizaciones a los router de borde vía BGP interno redirigiendo el tráfico al centro de limpieza como se había mencionado previamente. (Elsayed & Azer, 2018)

- c) El fabricante Cisco en el White paper llamado "Remotely Triggered Black Hole – Destination based and Source based" en el cual describe el filtrado RTBH como una técnica que provee la habilidad de descartar tráfico no deseado antes de que este entre a la red de un ISP. El documento tiene como propósito describir la técnica RTBH y su

funcionamiento como sus beneficios, aplicaciones, consideraciones para el despliegue y finalmente brinda ejemplos de configuración de routers. Como beneficios de la técnica RTBH resalta la efectividad para mitigación de ataques DDoS, pone en cuarentena todo el tráfico dirigido al objetivo bajo ataque, aplica los filtrados de lista negra(blacklist).

Se indica que los black hole son situados en los equipos de borde de la red y que se puede descartar todo el tráfico de ataque cuando es detectado basado en direcciones de origen o destino reenviándolo a la interfaz null0.

Nos refiere que el filtrado RTBH basado en dirección de destino permite un blackhole simplemente propagando una ruta estática desde el equipo disparador, el cual envía actualizaciones iBGP hacia los equipos de borde que setean una IP de siguiente salto hacia otra ruta estática preconfigurada que apunta a la interfaz null0. Cuando el ataque cesa la ruta estática del disparador es removida e instala una nueva ruta hacia el host o segmento de red atacado basado en la base de información de enrutamiento (RIB – Routing Information Base por su acrónimo en inglés). Mediante este método se evitan daños colaterales como consumo de ancho de banda, consumo de utilización del procesador y pérdida de servicios en algunos puntos de la red.

Por otro lado, el filtrado RTBH basado en dirección de origen provee la habilidad de descartar tráfico en el borde de la red basado en una dirección de origen en específico o en un rango de direcciones. Si la dirección de origen o rango del ataque puede ser identificado (sin importar si se trata de una suplantación o no) se descartará el tráfico permitiendo a otras direcciones de origen poder alcanzar el destino. Este método comúnmente usa Unicast Reverse Path Forwarding (URPF) el cual descarta el tráfico si el router no tiene una entrada en la base de información de reenvío para la dirección IP de origen o si la entrada apunta a la interfaz null0.

Dentro de las aplicaciones de la técnica de filtrado RTBH se destacan la mitigación de ataques DDoS a través del descarte de tráfico no deseado previniendo de esta manera el daño a la infraestructura de red del ISP y

brindando al cliente y al proveedor tiempo para responder al ataque y reestablecer el servicio, la cuarentena o redirección de tráfico de ataque que permite reenviar el tráfico de ataque a un sistema de seguridad para un mayor análisis del mismo, filtros de lista negra la cual es un conjunto de segmentos de red destinos que una organización no permite el acceso y que son enviadas al agujero negro previniendo el acceso de los usuarios dentro de la organización a estos.

También se brindan consideraciones para la implementación basado en 2 casos comunes como son el uso de un siguiente salto para redireccionar el tráfico y no exportarlo hacia la red y el enfoque basado en comunidades con el cual se tiene alternativas más flexibles para proceder con la redirección del tráfico o descartarlo ante un ataque. La parte final del documento provee ejemplos de configuración para los equipos routers PE como para los equipos disparadores como referencia para la implementación de esta solución.

3.5 Marco conceptual

3.5.1.1 Ataques DDOS:

Un ataque de denegación de servicios distribuidos ocurre cuando una o múltiples computadoras y/o dispositivos operan juntos para atacar un objetivo con la única finalidad de interrumpir el tráfico o servicio de un servidor, router, red de un usuario final o de una empresa como también proveedores de servicios de internet. Los ataques de denegación de servicio buscan agotar los recursos de sus objetivos, como puede ser la infraestructura de red o el desempeño del servicio. Por ejemplo: dar de baja servidores, saturación del ancho de banda del enlace, saturación del buffer de las conexiones TCP o buffer de aplicaciones, aumentar el procesamiento del CPU, etc.

Debido a que los ataques DDoS son realizados en una larga escala son muchos más complejos y difíciles de prevenir, el volumen de tráfico generado

por los atacantes suele ser mucho mayor a la cantidad de los recursos disponibles de las víctimas (el volumen ha incrementado exponencialmente llegando a superar los Gigabit o Terabit por segundo (Gbps/Tbps) durante los últimos años), lo cual genera una degradación del servicio hasta la interrupción completa del mismo. Los ataques DDoS han incrementado en frecuencia, sofisticación y severidad debido a que la vulnerabilidad de las computadoras ha incrementado rápidamente en conjunto con la facilidad de acceso a internet, permitiendo a los atacantes acceder a los dispositivos de red de los usuarios y a su información como también brindado la posibilidad de instalar múltiples herramientas de ataques en muchas computadoras para generar estos ataques.

¿Cómo detectar un ataque DDoS?

Algunos de los ejemplos más recurrentes para identificar un posible ataque DDoS son los siguientes:

- Desempeño lento atípico de la red.
- Indisponibilidad de un segmento de red particular o de un dominio/sitio web.
- Incapacidad para acceder a internet o cualquier sitio web.
- Una dirección IP realiza una gran cantidad de solicitudes inusuales en un determinado intervalo de tiempo.
- Servidores responden con error 503 debido a un corte de servicio.
- Gráficas de tráfico de interfaces registran un pico muy alto e inusual.
- Extraños patrones en las gráficas de tráfico en horas inusuales.(Radware, 2023)

3.5.1.2 Interfaz null0:

Es una pseudointerfaz que siempre se encuentra activa ya que es una interfaz lógica y como característica principal no cuenta con la capacidad de enviar o recibir tráfico por lo que cualquier paquete enviado a la interfaz null0 es descartado. Es decir, si una ruta estática configurada hacia un segmento de red cuenta como siguiente salto una interfaz null0, todos los paquetes de datos

que tengan como destino este segmento de red serán descartados sin excepción.(Cisco Systems, 2005)

3.5.1.3 Protocolo BGP:

Es un protocolo de enrutamiento interdominio diseñado para proveer enrutamiento sin bucles. El objetivo principal de sistemas que hablan BGP es intercambiar información de accesibilidad de red con otros sistemas BGP, estos incluyen información de los sistemas autónomos por los que el tráfico debe pasar para alcanzar a estos segmentos de red. Es un protocolo de vector de ruta comúnmente usado para intercambiar rutas entre distintos sistemas autónomos. BGP es diseñado para correr sobre un protocolo de transporte confiable por lo que usa TCP (puerto 179) porque es un protocolo orientado a la conexión. (K. Lougheed & Y. Rekhter, 1989)

Es principalmente usado para conectar una red local a una red externa para brindar acceso a internet o para conectarla a otras sedes a través de sesiones BGP. Aunque BGP sea relacionado a un protocolo de puerta de enlace externa (EGP- External Gateway Protocol por sus siglas en inglés), muchas redes dentro de una organización se vuelven tan complejas que usan BGP para simplificar la operación usándolo como un protocolo de puerta de enlace interna (IGP – Internal Gateway Protocol por sus siglas en inglés).

BGP usa un algoritmo para intercambiar información de accesibilidad a la red con otros equipos con los que tenga sesiones BGP establecidas a través de actualizaciones de tabla de enrutamiento. La información de accesibilidad a la red contiene número de redes, atributos de ruta específica y la lista de números de sistemas autónomos por los que una dirección IP origen debe transitar para alcanzar una red de destino. BGP previene bucles de enrutamiento rechazando cualquier ruta que contiene el sistema autónomo local porque esto indica que la ruta ya ha viajado a través de ese sistema autónomo.(Cisco Systems Inc., 2013)

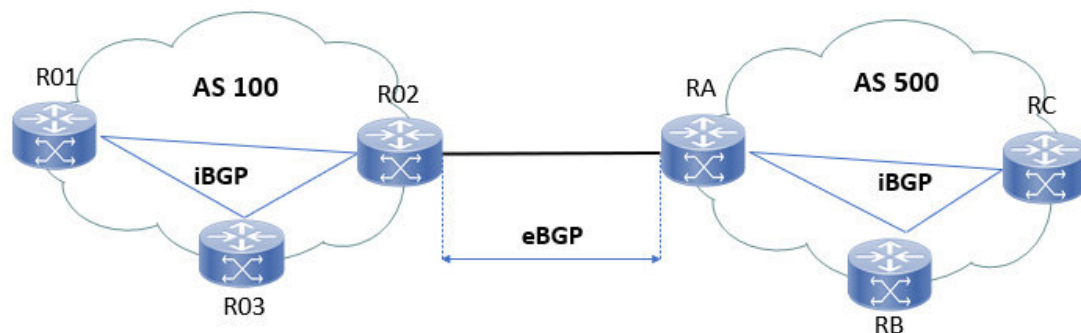


Figura 2: Ejemplo protocolo BGP. Fuente: Elaboración propia.

Comunidad BGP:

Es un atributo de BGP que es usado por proveedores de servicios con múltiples propósitos como etiquetar clientes, pares, rutas originadas geográficamente. El etiquetado es comúnmente usado para controlar la redistribución de rutas dentro de la red de un proveedor como para sus clientes y pares. Las comunidades también son usadas permitiendo a los clientes configurar el atributo de Preferencia Local enviando las prioridades correctas a sus proveedores de servicios a través de redes privadas virtuales, servicios de internet, etc. Están conformadas por un conjunto de 4 octetos (32 bits) del rango 0x00000000 hasta 0x0000FFFF, siendo el rango reservado 0xFFFF0000 al 0xFFFFFFFF. Las mejores prácticas consideran el uso de los 2 primeros octetos para el sistema autónomo del proveedor de servicios y los otros 2 últimos octetos para representar la clasificación de la ruta. (D. Meyer, 2006)

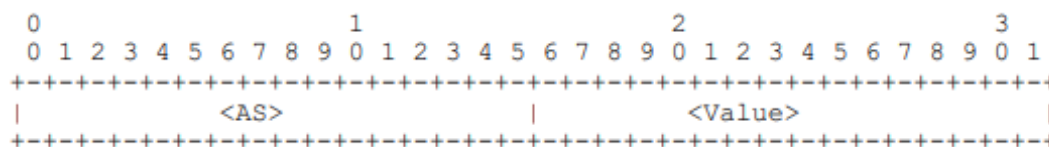


Figura 3: Estructura de una comunidad BGP. Fuente: RFC 4384.

Comunidad Blackhole:

La comunidad blackhole permite a una red interpretar la presencia de esta como un aviso para descartar cualquier tráfico que haya sido enviado hacia

un prefijo etiquetado con esta comunidad y que es usado en el método de blackhole activado remotamente basado en dirección de destino. La Autoridad de Números Asignados en Internet (IANA) registró los últimos 2 octetos 0xFFFF029A (666 en decimal) como “Blackhole” en el registro de comunidades conocidas ya que este valor es comúnmente usado con el BGP blackholing entre operadores de red.(King et al., 2016)

3.5.1.4 Enrutamiento basado en políticas:

El enrutamiento basado en políticas es un proceso por el cual un equipo pasa los paquetes de datos a través de un mapeo de rutas antes de enrutarlos. El mapeo de rutas determina cuales son los paquetes enrutados hacia el siguiente dispositivo de acuerdo con ciertos criterios de cumplimiento. Se utiliza una política de enrutamiento para hacer coincidir rutas o atributos de rutas y para cambiar los atributos como acción resultante cuando se cumplen las reglas de coincidencia. Las reglas de coincidencia de una política de enrutamiento pueden usar otros filtros como listas de control de acceso, listas de prefijos de IP, filtros AS Path, filtros de comunidad, filtros de comunidad ampliados, entre otros. (Cisco Systems, 2013)

3.5.1.5 RTBH:

Es una técnica de filtrado muy conocida y efectiva que es usada para mitigar rápidamente ataques DDoS a gran escala. Un ataque DoS dirigido contra un cliente de un ISP involucra generar un volumen de tráfico significativo hacia el objetivo que opacará al tráfico legítimo y que comúnmente resulta en un daño colateral o efectos negativos para otros clientes como también para la infraestructura de red. Los clientes pueden consultar con sus proveedores de servicios de Internet la posibilidad de filtrar el tráfico dirigido hacia una o varias direcciones IP para prevenir que todos los equipos de su red no sean afectados por un ataque DDoS o el proveedor de servicios puede determinar

si es necesario para ellos mismos la habilitación de estos filtros a fin de asegurar la disponibilidad de los servicios que brinda.

Un método que los proveedores de servicios pueden usar para implementar esta técnica es desplegar listas de control de acceso (ACL – Access List Control por sus siglas en inglés) en los equipos de borde de sus redes. Esta alternativa provee bastante flexibilidad en el filtrado, sin embargo, no es escalable debido al número de entradas en el filtro y a la cantidad de puertos TCP/UDP que se deben ingresar manualmente. RTBH aprovecha la característica de los routers modernos para filtrar más entradas y a un mayor tamaño que los ACL. Esta técnica puede basarse en el filtrado de las direcciones IP de destino o en el origen:

Basado en dirección IP de origen:

En muchos casos los ataques DoS pueden ser generados desde redes de robots que son programados para atacar un dominio web, esto hace necesario emplear una técnica de blackholing basado en dirección origen. Combinando la técnica RTBH con uRPF un operador puede filtrar el tráfico malicioso desde la dirección IP de origen. uRPF realiza una búsqueda de la ruta de la dirección IP de origen y revisa si la interfaz de ingreso del paquete es la misma interfaz por la cual el tráfico es recibido (modo estricto) o si alguna ruta de la dirección IP de origen del paquete existe. Si la validación falla, el paquete es descartado.

Habilitando la funcionalidad de uRPF en las interfaces de equipos específicos (idealmente en los equipos de borde) de la red y anunciando la dirección IP de origen del tráfico de ataque, una red de operador puede descartar el tráfico identificado en los equipos específicos basado en la dirección IP de origen.

Es recomendado que cuando se emplea la técnica RTBH basado en dirección IP de origen entre dominios, se defina una política explícita que habilite a los pares solo anunciar rutas que ellos originen.

Basado en dirección IP de destino:

Una ruta de descarte es instalada en cada equipo de borde de la red con el segmento de red destino asociado como interfaz de salida a la interfaz null0. Una vez el ataque es detectado, el router disparador usa actualizaciones de los protocolos de enrutamiento para manipular las tablas de ruteo, redirigiendo

el tráfico a la interfaz null0 para descartar todo el tráfico no deseado evitando malgastar recursos a lo largo del camino hacia la víctima.

Esto hace que la dirección IP o el segmento de red de destino sea inalcanzable minimizando el daño colateral. Asimismo, hace posible cambiar la dirección IP del host o servidor destino a una nueva dirección IP para mantener el servicio activo. (W. Kumari & D. McPherson, 2009)

Un escenario típico para la implementación de esta técnica requiere el uso del protocolo BGP en los equipos de acceso y/o agregación y configurando un equipo que actúa como un “disparador”. El equipo disparador envía actualizaciones de la tabla de enrutamiento BGP al equipo de borde lo cual hace que el tráfico no deseado sea reenviado a la interfaz null0 y a su vez descartado.

Las principales ventajas de esta técnica de mitigación frente a otras alternativas son: el bajo costo de implementación, de rápida reacción, facilidad de uso y efectividad especialmente frente a ataques de volumen significativo. Por otro lado, la principal desventaja es que todo el tráfico enviado a la interfaz null0 es descartado sin discriminar si este es legítimo. Por lo que mientras el ataque esté en progreso no se podrá tener acceso a Internet desde la dirección IP del host o desde el segmento de red que se encuentre bajo ataque. (Cisco Systems, 2005)

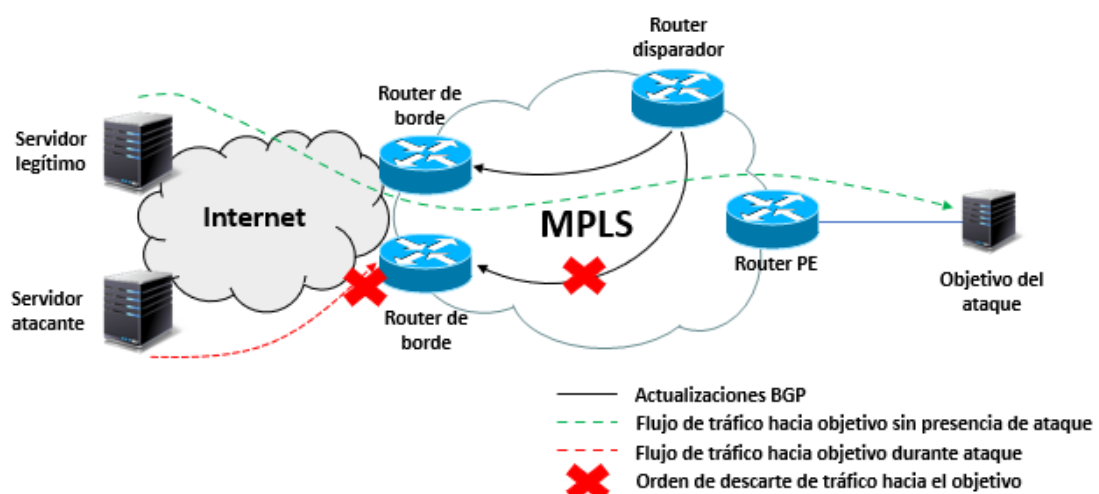


Figura 4: Funcionamiento de la técnica RTBH. Fuente: Elaboración propia.

3.6 Procedimiento

El presente trabajo de diseño e implementación de una solución de mitigación de ataques DDoS utilizando la técnica de blackhole activado remotamente fue desplegada en 5 fases. Las cuales se detallan a continuación, teniendo como base los flujos y procedimientos internos establecidos por la empresa para las actividades de habilitación de servicios y configuraciones en la red.

3.6.1 Etapas:

3.6.1.1 Análisis de Factibilidad del requerimiento:

Como parte inicial del flujo de la empresa, el área de Consultoría y Diseño derivó el proyecto al área de Planificación de Red a través del portal GMyD (sitio web interno donde se derivan las consultas técnicas y evaluación de factibilidad de servicios corporativos e información de la red como KPIs, ocupación de tráfico, entre otros) para determinar la viabilidad técnica del pedido de habilitación de una solución de Blackhole activado remotamente como una “solución a la medida” para el cliente Huawei al tratarse de un servicio que no brinda la empresa. Durante esta fase se revisó a detalle los requerimientos del cliente, se revisó la documentación de la solución RTBH así como también se realizaron consultas con las marcas respecto a las especificaciones técnicas de los equipos de red a fin de validar la necesidad de adquirir hardware y/o software adicional. Posterior al análisis realizado se determinó que era factible la habilitación del servicio solicitado, se atendió el proyecto a través del portal y se brindaron los lineamientos considerando cargar al proyecto el costo de diseño e implementación de la solución con un fabricante. Con lo indicado, se quedó a la espera de confirmación de generación de la Solicitud de Orden de Trabajo (SOT). La SOT es la orden de trabajo con la cual se generan las tareas para las áreas que participan en el

proyecto como parte del proceso interno para habilitar un servicio y que se genera una vez que el cliente acepta la habilitación del servicio, a su vez cuenta con datos relacionados al servicio del cliente tales como Ancho de banda contratado, tipo de servicio, dirección del cliente, nombre del cliente, contactos técnicos y documentación del proyecto.

3.6.1.2 Diseño de la solución:

Con la información del punto anterior y la SOT generada, se diseñó la solución basada en los requerimientos del cliente tales como redundancia de enlaces, enrutamiento dinámico, tabla de enrutamiento completa, mitigación automática, etc. y la arquitectura de red de la empresa según los siguientes criterios:

Se determinó que para mantener el criterio de redundancia se debería contar con 2 equipos distintos y ubicados geográficamente en distintos lugares para brindar el servicio y los cuales a su vez serían los equipos que contarían con la capa 3 del servicio. Los equipos routers Capa 3 se determinaron teniendo en cuenta el pedido de contar con la tabla de enrutamiento completa, los cuales lo manejan los equipos de borde de la red del operador.

Los equipos de acceso que abarcarían la capa 2 del servicio se determinaron por cercanía a la ubicación del Data Center donde se encontraban los equipos del cliente y de acuerdo con la disponibilidad de hilos de fibra óptica.

No se consideró en el diseño un equipo “disparador” ya que el cliente indicó que contaba con una solución AntiDDoS propia con la cual al detectar un ataque enviarían una ruta estática con la IP del dispositivo bajo ataque marcado con una comunidad BGP blackhole que fue asignada por Claro.

A fin de evitar que el tráfico malicioso ingrese a la red y pueda causar daños a la infraestructura como a demás servicios que se brindan y siguiendo las recomendaciones técnicas de fabricantes respecto a descartar el tráfico en el punto más próximo al intercambio de ruta hacia los proveedores de servicios de internet, se planteó que los routers de borde puedan inyectar la ruta estática con siguiente salto la interfaz null0 a fin de descartar el tráfico.

Una vez definida la topología del diseño propuesto se planteó la solución a las áreas de operación y mantenimiento(O&M) para su conformidad al ser un nuevo escenario, se coordinó una reunión donde se explicó el detalle y funcionamiento esperado de la solución y de lo expuesto se identificó la necesidad de instalar un equipo adicional por cada router de borde con los que tendría una sesión eBGP para recibir las rutas o segmentos de red bajo ataque para el descarte del tráfico malicioso y para inyectar la ruta estática de descarte a los demás equipos router de la red, como también la necesidad de contar con participación de la marca fabricante de los equipos de red al tratarse de un escenario no estándar y con el fin de asegurar la operatividad de la red y contar con soporte especializado en caso de presentarse algún inconveniente durante la implementación.

Con las consideraciones brindadas, se elaboró el documento de diseño a bajo nivel (LLD – Low Level Design por sus siglas en inglés) y se presentó a las áreas de O&M con lo cual se brindó la viabilidad por su parte y se quedó a la espera de la implementación de la solución. Posterior a ello se procedió con la asignación de recursos lógicos como segmentos de red públicos para la WAN y LAN del servicio, VLANs de servicio, direcciones IPs para los router Blackhole, la dirección IP privada máscara 32 para la ruta estática de descarte y la comunidad BGP blackhole siguiendo las recomendaciones de fabricantes y estándares. Estos recursos fueron a su vez compartidos al área de Datacom del cliente para configuración en sus equipos de red y plataforma AntiDDoS.

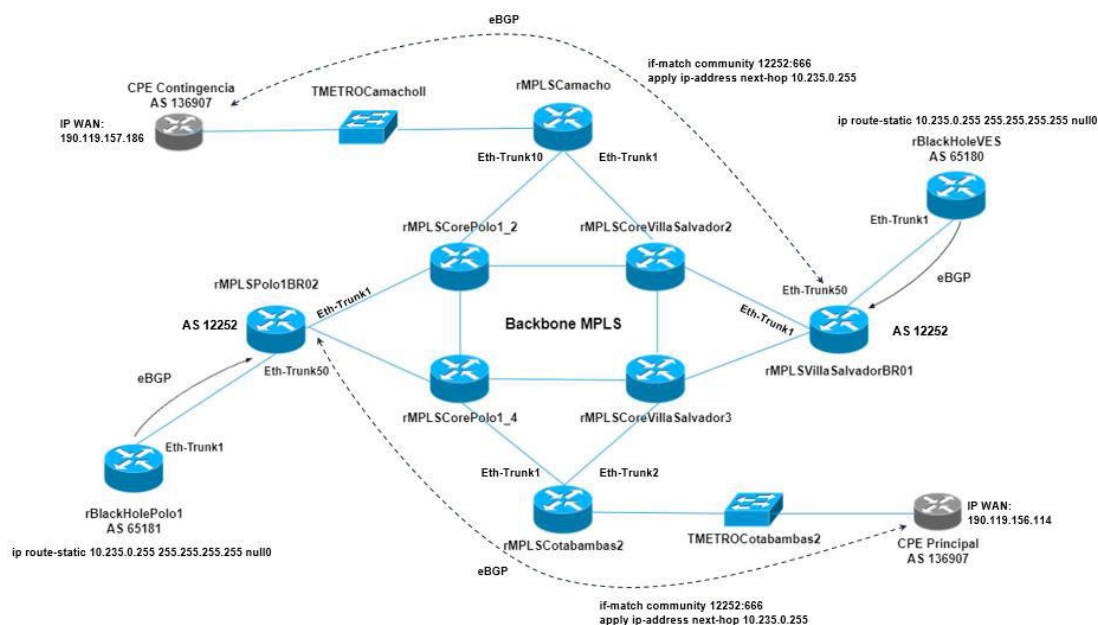


Figura 5: Topología General de la solución RTBH. Fuente: Elaboración propia.

Funcionamiento esperado de la solución:

El flujo del funcionamiento esperado de la solución teniendo en cuenta las consideraciones del diseño del punto previo es el siguiente:

- Una vez el ataque DDoS sea detectado por la plataforma AntiDDoS del cliente, esta añadiría de manera automática una ruta estática en el router cliente con la dirección IP del host o segmento de red bajo ataque marcada con la comunidad blackhole a través del protocolo BGP FlowSpec.
- El equipo router cliente enviará la ruta estática con la dirección del host o segmento de red bajo ataque a través de la sesión eBGP hacia los equipos PE de la red de Claro.
- Los equipos routers Blackhole contarían con una ruta estática de descarte que contiene una dirección IP privada de destino con máscara 32 y como siguiente salto la interfaz null0. Esta ruta estática de descarte se anuncia a los routers de borde a través de sesiones eBGP y estos a su vez recibirían los segmentos de red públicos bajo ataque marcados con la comunidad blackhole.
- Los router PE del servicio cuentan con una política de enrutamiento que filtrarían los segmentos de red enviados por el router cliente marcados con la comunidad BGP Blackhole 12252:666 y se modificaría el siguiente salto

con la dirección IP de descarte que redirige el tráfico hacia el host bajo ataque hacia los router Blackhole.

- Esta redirección de tráfico impediría que el tráfico no deseado llegue hacia el objetivo del ataque y que la dirección IP o el segmento de red LAN cliente no se anuncie hacia los peers internacionales y que no sea alcanzable desde internet.
- Los segmentos de red LAN públicos del cliente restantes recibidos a través de la sesión eBGP que no se encuentren bajo ataque y sin la comunidad blackhole marcada seguirían su flujo de publicación hacia Internet.
- Una vez culmine el tráfico de ataque DDoS se eliminaría automáticamente la ruta estática en el router cliente con lo cual el segmento de red LAN seguiría su flujo de tráfico de publicación hacia Internet al llegar a la red de Claro.

3.6.1.3 Implementación de la solución:

Habilitaciones físicas y relacionados en sede cliente:

Se inicia con las coordinaciones con las áreas de implementación de Mercado corporativo para realizar las habilitaciones físicas como tendido de Fibra óptica hacia la sede de cliente, mediciones de los hilos de fibra óptica habilitados con OTDR y trabajos Planta Interna como conexión de jumpers de fibra óptica hacia equipos cliente y etiquetados correspondientes.

Instalación de equipos router Blackhole:

Como parte del procedimiento interno, se generó un Requerimiento al área de Implementación de Red para instalación de los 02 router Blackhole en Data Centers distintos. Se envió al área de Implementación de red los alcances del Requerimiento como son visita técnica del sitio (TSS – Technical Site Survey por sus siglas en inglés), adecuaciones de espacios y energía, instalación de equipos en Salas técnicas asignadas, gestión e integración a la red, protocolos de pruebas de aceptación, documentaciones tales como entrega de reporte de instalación, mediciones de Fibra óptica, entre otros para revisión de presupuesto y asignación de personal técnico.

Una vez definida la contrata a cargo del proyecto, se revisó con el área de implementación de Red las actividades a realizar y se solicitó la elaboración del cronograma de actividades, el cual tomó aproximadamente 02 meses desde la elaboración del TSS hasta la liberación de los equipos por parte de las áreas Operativas. A continuación, se detalla el cronograma de ejecución del proyecto:

		Noviembre 2021																		
		L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V
Ítem	Actividad	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
1	Aprobación de requerimiento																			
2	Asignación Contrata																			
3	Elaboración de TSS																			

Tabla 1: Cronograma de las 3 primeras actividades. Fuente: Elaboración propia

		Noviembre 2021										Diciembre 2021							
		L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	
Ítem	Actividad	22	23	24	25	26	27	28	29	30	01	02	03	04	05	06	07	08	
4	Generación y Liberación OC																		
5	Retiro de equipos																		

Tabla 2: Cronograma de la cuarta y quinta actividad. Fuente: Elaboración propia

		Diciembre 2021													
		J	V	S	D	L	M	M	J	V	S	D	L	M	M
Ítem	Actividad	09	10	11	12	13	14	15	16	17	18	19	20	21	22
6	Validación de espacios y energía														
7	Instalación de equipos														
8	Energizado de equipos														

Tabla 3: Cronograma de la sexta a la octava actividad. Fuente: Elaboración propia

		Enero 2022																
		M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V
Ítem	Actividad	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21
9	Integración de equipos																	
10	Pruebas ATP																	
11	Liberación de los equipos																	

Tabla 4: Cronograma de la novena a la undécima actividad. Fuente: elaboración propia.

Como actividad inicial de la instalación del equipo se realizó el TSS en el cual se realizó la visita de inspección a las salas técnicas propuestas para validar la posible ubicación del equipo con lo que se identificó la necesidad de instalación de gabinetes, el consumo de energía como la temperatura del Data Center (DC) como la capacidad de los equipos en DC y de los equipos de aire acondicionado (AA).

Posterior al TSS realizado la contrata elaboró un reporte con las vistas fotográficas obtenidas y el análisis de la nueva carga a añadir a nivel de energía y de clima para realizar las validaciones con las áreas de O&M Field y O&M Energía y Clima.

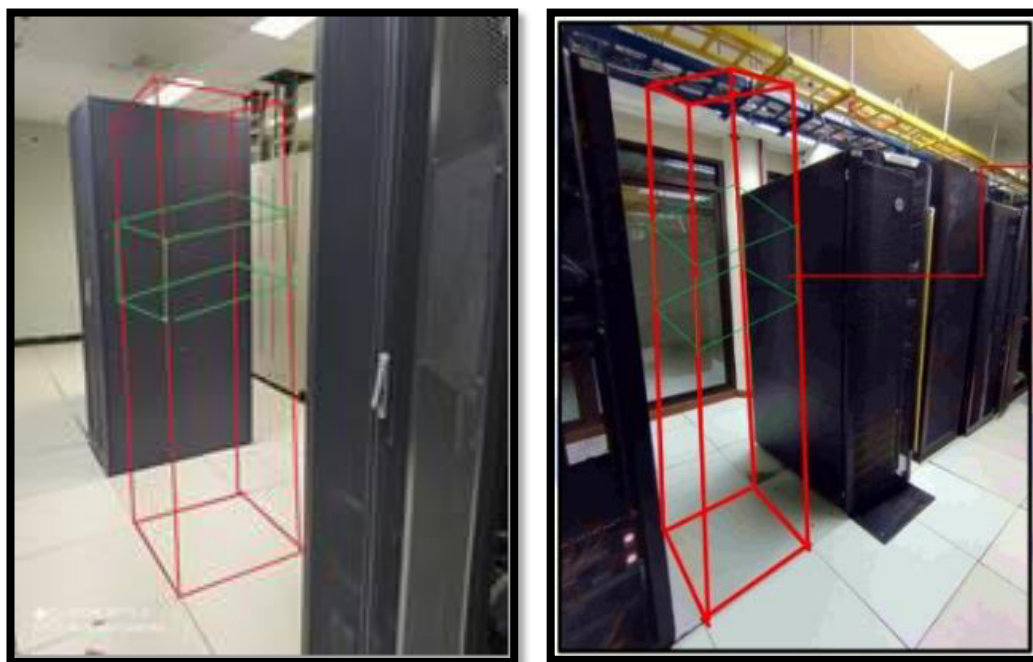


Figura 6: Propuesta de ubicación para instalación de gabinete para nuevos equipos en DCs. Fuente: Elaboración propia

Una vez se contó con la aprobación de la propuesta de ubicación para instalación de gabinetes para los nuevos equipos como de la adición de las nuevas cargas a nivel de energía y clima se procedió con la asignación del equipamiento necesario para la instalación como son routers, tarjetas, módulos de energía, módulos ópticos, entre otros y en paralelo se siguió las

coordinaciones para retiro de almacén e instalación de los equipos, así como también del energizado de los equipos en Ventana de mantenimiento (VM).



Figura 7: Gabinetes instalados en DCs. Fuente: Elaboración propia



Figura 8: Vista de equipos instalados en DCs. Fuente: Elaboración propia

Como siguiente paso luego del energizado de los equipos se procedió a enviar la configuración de las direcciones IP para gestión de los nuevos router, así como también los protocolos básicos (TACACS, Syslog, NTP, SNMP, BGP, entre otros) a fin de poder integrar los equipos a las plataformas de Gestión y Monitoreo de las áreas de OyM. A su vez, se realizó la configuración de las rutas blackhole de descarte apuntando hacia la interfaz null como interfaz de salida.

RE: CRQ000002394579_Integracion de equipos BlackHole Polo1 - VES



Robert Sanchez

Para: Balthym Salatiel Morales Huerta; Luz Zegarra; Luis Enrique Aljabin Cumpa <luis.aljabin.wx@huawei.com>; daniel.ticonab.outs@huawei.com; Carlos Isaac Navarro Rosenberg (A) <isaac.navarro.outs@huawei.com>; Trabajos Programados, Control de RED; Personal Gestión y Supervisión CC: Armando Quiroga; Stefano Takeshi Sac Martinez; kenneth.rangel; Administración Transporte IP; Anthony Frank Ipanaque Casquina (A) <anthony.ipanaque.outs@huawei.com>; Back Office Transporte Nacional

Vie 21/01/2022 1:30

Estimados, se culmina con la integración.

Saludos
Robert Sanchez
BOTN

Figura 9: Correo de culminación de integración routers Blackhole. Fuente: Elaboración propia.

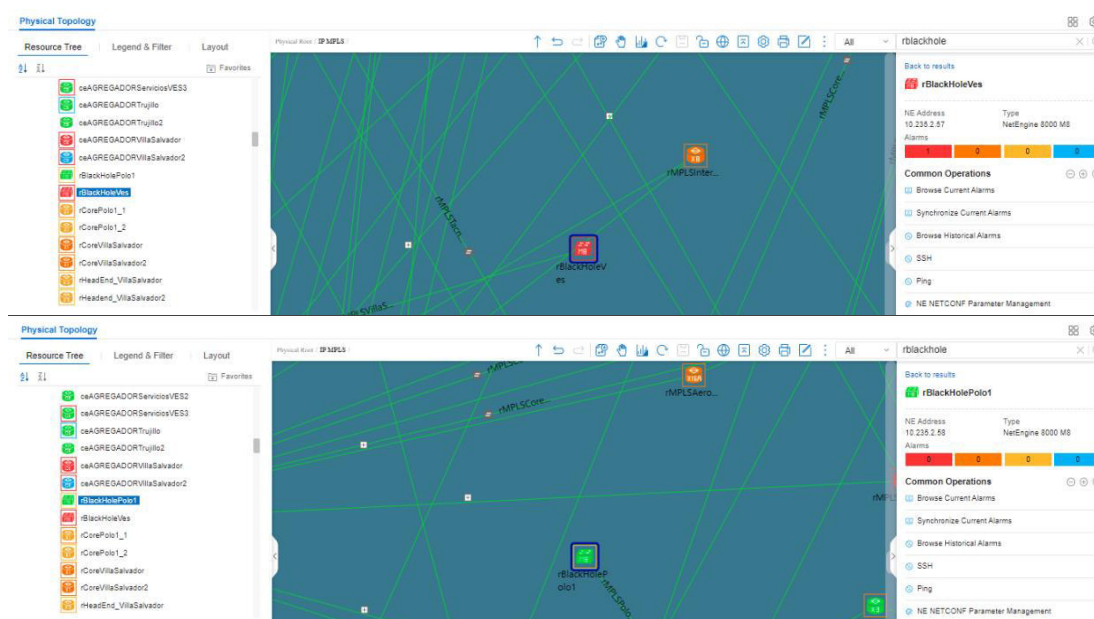


Figura 10: Vista de integración de equipos a los gestores de monitoreo. Fuente: Gestor Huawei.

```
<rBlackHoleVes>disp current-configuration configuration route-static
#
ip route-static 10.235.0.255 255.255.255.255 NULL0
<rBlackHolePolo1>disp current-configuration configuration route-static
#
ip route-static 10.235.0.255 255.255.255.255 NULL0
```

Figura 11: Rutas blackhole configuradas en equipos Blackhole. Fuente: Secure CRT

```

<rMPLSVillaSalvadorBR01>disp ip routing-table 10.235.0.255
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
-----
Routing Table : _public_
Summary Count : 1

Destination/Mask    Proto   Pre  Cost           Flags NextHop         Interface
-----
10.235.0.255/32    EBGP    20   0              RD  10.95.155.206      Eth-Trunk50

<rMPLSPolo1BR02>disp ip routing-table 10.235.0.255
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
-----
Routing Table : _public_
Summary Count : 1

Destination/Mask    Proto   Pre  Cost           Flags NextHop         Interface
-----
10.235.0.255/32    IBGP    200  0              RD  190.81.128.124     Eth-Trunk1

```

Figura 12: Aprendizaje de ruta blackhole en los equipos de borde. Fuente: Secure CRT

Continuando con el procedimiento, los equipos pasaron por un protocolo de pruebas de aceptación (ATP - Acceptance Test Protocol por su acrónimo en inglés) con personal de O&M a fin de asegurar la operatividad ante eventos como pérdida de fluido eléctrico en los DC o en zona, falla de tarjetas de línea, tarjetas controladoras, módulos FAN, entre otros. También se validó la correcta instalación física del equipo, documentación de reportes de instalación, mediciones de hilos de FO en la SOT, correcto etiquetado de conexiones como requisito previo para la liberación del equipo por las áreas de OyM. Con la información previa, se liberaron los 2 routers Blackhole para continuar con las configuraciones del servicio.

Configuración del servicio sobre equipos operativos:

Se realizaron las coordinaciones con las áreas de O&M para realizar las configuraciones necesarias para habilitación del servicio en los routers Blackhole ya operativos como también con el fabricante a fin de asegurar las coordinaciones internas con su personal de soporte remoto. En paralelo se realizó la revisión de plantillas de configuración a ejecutar en ventana de mantenimiento como parte de las buenas prácticas para evitar afectación de servicios y se encuentre según lo establecido en el documento LLD.

En la primera ventana se realizó la configuración lógica de las VLAN del servicio y la limitación del ancho de banda contratado en los puertos asignados al cliente de los 2 equipos de acceso.

En la segunda ventana se realizó la configuración lógica de túneles capa 2 entre los equipos PE (siglas en inglés de Provider Edge) locales y los equipos router de borde (BR – Border Router por sus siglas en inglés) como también la capa 3 del servicio, el cual involucraba la configuración de direcciones IP Gateway del servicio, las políticas de enrutamiento y las sesiones eBGP hacia las direcciones IPs WAN asignadas al cliente.



Figura 13: Confirmación de culminación de configuración de la segunda ventana. Fuente: Correo empresarial

3.6.1.4 Pruebas del servicio:

Al culminar las implementaciones a nivel físico y las configuraciones lógicas necesarias se notificó al cliente para confirmar la culminación de configuración en sus equipos y a su vez se solicitaron ventanas para realizar pruebas iniciales como son validaciones de potencias entre los equipos de acceso de Claro como del equipo cliente, pruebas de conectividad punto a punto y establecimiento de sesiones eBGP en los 2 enlaces del servicio, validaciones de prefijos importados desde equipo cliente y exportados desde la red de Claro, validaciones desde aplicativos looking glass del anuncio del segmento de red LAN público hacia Internet como puntos necesarios previo a la prueba del descarte de tráfico.

show bgp 119.8.192.0/20

Router: gin-ddv-tcore1
Site: US, Denver, DDV
Command: show route protocol bgp 119.8.192.0/20 terse exact

```
Restart Complete
* = Active Route, - = Last Active, * = Both

A V Destination      Next hop      AS path
* ? 119.8.192.0/20    0             1299 12252 136907 I
  unverified          >64.86.79.4
  ?                   0             1299 12252 136907 I
  unverified          >209.58.57.17
  ?                   0             1299 12252 136907 I
  unverified          >209.58.57.17
  ?                   0             1299 12252 136907 I
  unverified          >209.58.57.17
[master]
```

Figura 14: Validación de aprendizaje de segmento de red cliente en internet. Fuente: Looking glass Tata Communications.

Posterior a ello se coordinó una ventana de pruebas con el cliente para realizar la simulación de un ataque hacia la dirección IP de un host a fin de validar el correcto funcionamiento de la solución implementada. Previo a la ventana se validó en la tabla de enrutamiento BGP del router de borde que la dirección IP del host se aprendía con el segmento de red LAN público del cliente y se mostraba como siguiente salto la dirección IP WAN de lado del CPE cliente. A su vez, se advertía a 4 peers siendo uno de ellos el peer internacional hacia Internet.

```
crMPLSVillaSalvadorBR01>display bgp routing-table 119.8.192.100

BGP local router ID : 190.81.128.124
Local AS number : 12252
Paths: 6 available, 1 best, 1 select, 0 best-external, 0 add-path
BGP routing table entry information of 119.8.192.0/20:
From: 190.116.157.186 (172.16.6.168)
Route Duration: 32d02h33m28s
Relay IP Nexthop: 190.116.157.186
Relay IP Out-Interface: Virtual-Ethernet6/0/1.1
Original nexthop: 190.116.157.186
Qos information : 0x0
Community: <65301:61051>
AS-path 136907, origin incomplete, pref-val 0, valid, external, best, select, pre 20
Advertised to such 4 peers:
  190.81.128.123
  190.116.138.214
  62.115.182.196
  10.95.155.206
```

Figura 15: Tabla de enrutamiento previo a las pruebas de mitigación. Fuente: Secure CRT

En la ventana un operador del equipo router cliente configuró manualmente una ruta estática con destino la IP del host atacado marcado con la comunidad BGP blackhole 12252:666 a través de la sesión EBGP del enlace principal, con lo cual se validó en un router de borde que en la tabla de enrutamiento la dirección IP del host atacado se aprendía explícitamente con la máscara 32 y como nuevo siguiente salto la dirección IP 10.235.0.255 que es la dirección IP destino de la ruta estática de descarte con interfaz de salida la interfaz null0 preconfigurada en los routers Blackhole y que a su vez no se anunciaba esta dirección IP hacia los peers internacionales.

```

rMPLSVillaSalvadorBR01>display bgp routing-table 119.8.192.100

BGP local router ID : 190.81.128.124
Local AS number : 12252
Paths: 1 available, 1 best, 1 select, 0 best-external, 0 add-path
BGP routing table entry information of 119.8.192.100/32:
From: 190.116.157.186 (172.16.6.168)
Route Duration: 0d00h12m30s
Relay IP Nexthop: 10.95.155.206
Relay IP Out-Interface: Eth-Trunk50
Relay Tunnel Out-Interface:
Original nexthop: 10.235.0.255
Qos information : 0x0
Community: <12252:666>
AS-path 136907, origin incomplete, pref-val 0, valid, external, best, select, pre 20
Advertised to such 3 peers:
  190.81.128.123
  190.116.138.214
  10.95.155.206
rMPLSVillaSalvadorBR01>
rMPLSVillaSalvadorBR01>

```

Figura 16: Tabla de enrutamiento recibiendo la ruta estática con la comunidad blackhole. Fuente: Secure CRT

A su vez se hicieron pruebas adicionales de trazabilidad y conectividad desde la herramienta looking glass para validar que el segmento de red no se aprenda a través de la red de Claro. Con lo indicado, de la simulación realizada se validó que la solución implementada mitigaba el ataque DDoS redirigiéndolo hacia el router Blackhole y descartándolo para evitar que este llegue a la dirección IP objetivo del ataque.

Para concluir con las pruebas, se eliminó manualmente la ruta estática del host atacado con la comunidad blackhole en el equipo router cliente con lo

cual se validó que la dirección IP 119.8.192.100 del cliente se recibía de la misma manera que en la figura 15 previo a las pruebas de mitigación de ataque. Asimismo, se elaboró la Guía Operativa del servicio Blackhole que contaba con todas las líneas de configuración aplicadas en los equipos involucrados, las consideraciones y restricciones del servicio, topología de la solución, entre otros.

3.6.1.5 Entrega del servicio

Debido a que las pruebas de homologación del servicio se realizaron en ventanas coordinadas y con participación de las áreas de Datacom y Data Center del cliente Huawei, por su lado pudieron validar que la solución implementada funcionaba correctamente y con ello se brindó la aceptación del servicio. A su vez, se entregó la Guía Operativa del servicio Blackhole al área de Atención Tecnológica Corporativa a fin de brindar soporte ante algún inconveniente en la postventa del servicio.

RE: PROYECTO **BLACKHOLE** AUTOMÁTICO HUAWEI - CLARO (Internet Link)-SOT 38711271

...
Dom 01/05/2022 8:37

Z Zhumingliang <zhumingliang3@huawei-partners.com>
Para: Jessica Villegas
CC: Oscar Raul Tipula; guixiaowei <guixiaowei@huawei.com>; Carlos Isaac Navarro Rosenberg (A) <isaac.navarro.outs@h-partners.com>; Stefano Takeshi Sac Martinez y 4 más

Hi Jessica,
Good day.The test of black hole was succeed on 28th April.

朱明良 ZhuMingliang

Figura 17: Correo de validación del servicio por parte del cliente. Fuente: Correo empresarial

3.7 Resultado de la actividad

Como se evidencia en la figura 16, al buscar la dirección IP del host bajo ataque en la tabla global de enrutamiento del router de borde una vez que se envía la ruta estática con la comunidad blackhole desde el equipo cliente se observa que a diferencia de la figura 15 se recibe la ruta con una máscara 32 y como nuevo siguiente salto la dirección IP 10.235.0.255, la cual es la dirección IP destino de la ruta estática de descarte preconfigurada en los

routers blackhole que apuntan hacia la interfaz null0 de la Figura 11. Asimismo, se aprecia que la ruta se anuncia solo a 3 peers en comparación con la figura 15 ya que no se está anunciando el segmento de red máscara 32 a través del peer internacional hacia Internet. Con lo indicado se valida que el funcionamiento esperado es el adecuado de acuerdo con lo establecido como funcionamiento esperado de la solución implementada ya que al recibir un ataque DDoS y la ruta estática con la IP del host bajo ataque con la comunidad blackhole, todo el tráfico es redirigido hacia la dirección IP 10.235.0.255 ubicada en los routers Blackhole y que a su vez será descartado ya que cuenta con siguiente salto la interfaz null0.

CAPITULO IV: CONCLUSIONES

4.1 Justificación

La solución descrita en el presente trabajo se realizó debido a la necesidad del cliente Huawei de contar con una alternativa de mitigación adicional a su plataforma AntiDDoS y con la finalidad de asegurar la disponibilidad de los servicios que brinda, como también evitar perjuicios a nivel económico por incumplimientos de SLA, contratos, entre otros y a nivel de infraestructura por baja o daño de algún equipo o servidor por alto procesamiento de los CPU, rendimiento, etc. Como es sabido, la principal amenaza de las empresas que brindan servicios en Internet son los ataques DDoS y estos a su vez han aumentado considerablemente a nivel de frecuencia como también a nivel de volumen de tráfico y sofisticación. Por lo cual nace la necesidad del empleo de mecanismos de mitigación de ataques DDoS como es la técnica del blackhole activado remotamente que tiene múltiples ventajas como ser una alternativa de bajo costo, fácil de implementar en comparación con otras técnicas y que es efectiva en la mitigación de ataques de larga escala.

4.2 Descripción de la implementación

Se analizó la factibilidad de habilitación del mecanismo de mitigación usando la técnica de blackhole activado remotamente acorde al requerimiento del cliente y se realizó un diseño inicial del servicio, se brindó como factible y se quedó a la espera de aceptación por parte del cliente para iniciar con la

habilitación del servicio. Con la conformidad del cliente, se realizó la revisión del diseño propuesto con las áreas operativas de Red y con el fabricante como soporte para asegurar la operatividad de la red durante la implementación como también asegurar el funcionamiento de la solución. Como parte de la solución, se consideró la instalación de 2 equipos que se encargarían del descarte del tráfico del ataque DDoS y finalizada la implementación se procedió con la configuración de los equipos en VM. En una ventana coordinada con el cliente se hicieron las pruebas en conjunto con lo que se determinó que la solución funcionaba correctamente. Finalmente se brindaron los documentos para la postventa del servicio, así como la aceptación del servicio por parte del cliente.

4.3 Conclusiones

- Se realizó el levantamiento de la información de la infraestructura de la red de Claro como también de las necesidades del cliente con lo cual se diseñó la solución.
- La solución diseñada e implementada contempló los requerimientos del cliente como también la arquitectura de la red actual de Claro, de acuerdo con las consultas realizadas con el equipo de Preventa y con el fabricante de los equipos.
- Se determinó y se validó con las áreas de Operación y Mantenimiento de Claro, los equipos de la red que cumplirían la función del descarte de tráfico de ataques DDoS provenientes de Internet, de lo cual se realizó la instalación de los router Blackhole para cumplir con dicha funcionalidad.
- De las pruebas realizadas a través de la simulación de ataque DDoS a un host del cliente, se observó que la solución implementada funciona correctamente redirigiendo el tráfico hacia los router Blackhole para ser descartado una vez el ataque DDoS es detectado. Asimismo, cuando el ataque DDoS es detenido el flujo de tráfico del cliente desde Internet vuelve a la normalidad.

- La solución diseñada e implementada cumplió con la necesidad del cliente Huawei para el descarte de tráfico de ataques DDoS provenientes de internet, dicha solución puede ser aplicada para otros clientes que lo requieran teniendo en cuenta las características propias de cada red, considerando que no todas las redes son homogéneas.

CAPITULO V: RECOMENDACIONES

- Durante el levantamiento de información, los requerimientos del cliente deben estar bien definidos y claros a fin de evitar modificaciones en el diseño durante la implementación.
- Todo escenario nuevo o solución no estándar debe contemplar el soporte del fabricante como también la entrega de la documentación relacionada (LLD, Guías Operativas, entre otros) a fin de asegurar la operatividad y la seguridad de la red.
- Cada escenario nuevo o solución no estándar debe ser validado por las áreas operativas de Red con la documentación del proyecto, previo a la etapa de implementación.
- Toda implementación física de hardware en salas técnicas o en Data Centers debe ser realizada solo por personal técnico capacitado y autorizado a fin de velar por la seguridad de la infraestructura de red y operatividad de los servicios, así como por la salud del personal.
- Durante la implementación física de equipos en salas técnicas o en Data Centers, se deben realizar las coordinaciones necesarias y mantener comunicaciones constantes con las áreas involucradas según el proceso interno correspondiente de cada empresa a fin de evitar demoras en el procedimiento, tales como accesos al sitio, validación de espacios y energía, adecuaciones físicas, validación de instalación, entre otros.
- Todo segmento de red público de cliente que se anuncia hacia internet debe contar con una salida principal definida, a fin de tener mayor claridad del flujo de tráfico tanto en entrada como en salida ante algún incidente o troubleshooting que se deba realizar.
- Para futuras implementaciones y de acuerdo con el diseño de la solución, se podría considerar la habilitación de una plataforma que pueda discriminar el

tráfico legítimo del tráfico malicioso a fin de asegurar la disponibilidad del servicio, en caso se reciba un ataque DDoS. Para la presente solución este caso no fue contemplado ya que no se encontraba dentro de los requerimientos del cliente.

CAPITULO VI: BIBLIOGRAFIA

- Bravo Mullo, S. J. (2019). Contribuciones para la Detección de Ataques Distribuidos de Denegación de Servicio (DDoS) en la Capa de Aplicación. In *Universidad Nacional Mayor de San Marcos*.
<https://cybertesis.unmsm.edu.pe/handle/20.500.12672/18699>
- Cisco Systems. (2013). *Policy-Based Routing*.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-mt/iri-15-mt-book/iri-pbr.pdf
- Cisco Systems. (2005). Remotely Triggered Black Hole filtering-destination based and source based. *White Paper*.
https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf
- Cisco Systems Inc. (2013). *IP Routing: BGP Configuration Guide*.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-15-mt-book.pdf
- D. Meyer. (2006). *RFC 4384 - BGP Communities for Data Collection*. RFC.
<https://datatracker.ietf.org/doc/html/rfc4384>
- Elsayed, M. S., & Azer, M. A. (2018). Detection and Countermeasures of DDoS Attacks in Cloud Computing. *International Conference on Ubiquitous and Future Networks, ICUFN, 2018-July*, 708–713.
<https://doi.org/10.1109/ICUFN.2018.8436989>
- K. Lougheed, & Y. Rekhter. (1989). *RFC 1105 - Border Gateway Protocol (BGP)*. RFC. <https://datatracker.ietf.org/doc/html/rfc1105>
- King, T., Dietzel, C., Snijders, J., Doering, G., & Hankins, G. (2016). Blackhole Community. *RFC*. <https://doi.org/10.17487/RFC7999>

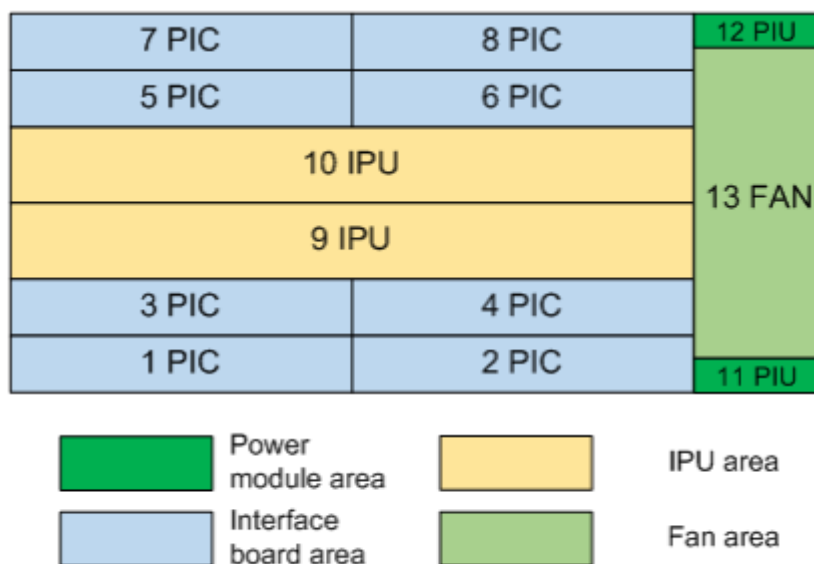
Radware. (2023). *What is a DDoS Attack? - Distributed Denial of Service | Radware*. <https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/>

W. Kumari, & D. McPherson. (2009). *RFC 5635 - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)*. RFC. <https://datatracker.ietf.org/doc/html/rfc5635>

CAPITULO VII: ANEXOS

Anexo A: Datasheet del equipo instalado.

HUAWEI NetEngine 8000 M8



Slot type	Slot ID	Description
PIC	1-8	Physical Interface Card
IPU	9,10	Integrated Network Processing Unit
PIU	11,12	Power Interface Board
FAN	13	-

Product Features:

Feature	Description
---------	-------------

Interface type	100GE/50GE/40GE/25GE/10GE/GE/FE/E1/cPOS/POS
Typical port density	100GE:12; 50GE:16; 25GE:32; 10GE:80; GE:160
Routing	RIP, RIPng, OSPF, OSPFV3, IS-IS, IS-ISV6, BGP, BGPv6, Static routing, IPv4 Multicast, IPv6 Multicast, Multicast static, etc
IPv4	TCP/IP, for example, ICMP, IP, TCP, UDP, Socket (TCP/UDP/RAW IP), ARP Static DNS DNS Client FTP Server FTP Client TFTP Client DHCP Relay and DHCP Server Ping Tracert NQA IP policy-based routing Forwarding next hop based on traffic IP Policy - based route load balancing The QinQ interface (QinQ termination and dot1q termination) supports IPv4 load balancing. Enabling and disabling the rapid ping reply function based on interface boards Forcible fragmentation for packets with length greater than MTU and DF enabled MPLS-in-UDP tunnel egress
MPLS	LDP, MPLS TE, Segment Routing MPLS、MPLS-TP
L2VPN	PWE3/VLL, VPLS, EVPN, EVPN L3VPN, VxLAN
L3VPN	CE routers can access the L3VPN through L3 interfaces. Support static routes between CE and PE, BGP, RIP, OSPF and ISIS Inter-AS VPN NG-MVPN IPv6 VPN HoVPN Seamless MPLS BGP LSP entropy label Redirect to VPN L3VPN PIPE / Uniform mode L3VPN Statistics
OAM	iFIT IPFPM NQA TWAMP BFD MPLS OAM MPLS-TP OAM VRRP Ethernet OAM 802.3ah Y1731 Ethernet LPT Bit-error-triggered protection switching
QoS	QPPB, Differ-Serv, HQoS, Redirection, ACL, PBR

Others	AAA, Radius, TACACS, Telnet, SSH, SNMP v1 / v2 / v3, Syslog
--------	---

Product Specifications:

Item	NetEngine 8000 M8
Dimensions (H x W x D)	132.6 mm (3 U) x 442 mm x 220 mm (5.22 in. x 17.4 in. x 8.66 in.)
Weight (full configuration)	16.5 kg (36.38 lb)
Typical power consumption	428.11 W
Typical heat dissipation	1350.19 BTU/hour
Slot quantity	8
Availability	0.999999439
Redundant fans	1+1
Redundant power supply	1+1
Operating temperatura	-40°C to +65°C
Routes	IPv4: 4,096,000 IPv6: 2,048,000
BGP Neighbor Capacity	512
NetStream	1M original flows and 512K aggregated flows

Anexo B: Puntos resaltantes de los estándares:

Comunidad Blackhole (RFC 7999):

5. IANA Considerations

The IANA has registered BLACKHOLE in the "BGP Well-known Communities" registry.

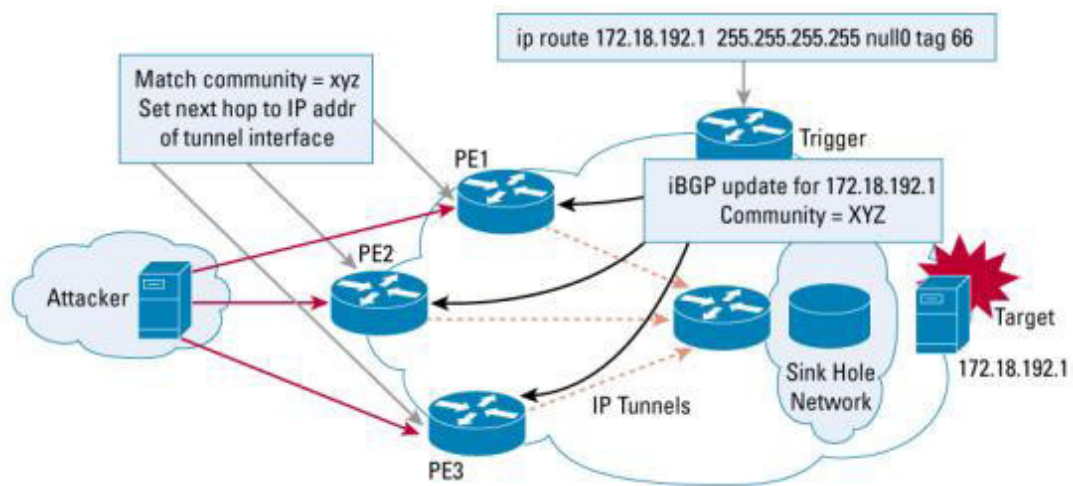
BLACKHOLE (= 0xFFFF029A)

The low-order two octets in decimal are 666, a value commonly associated with BGP blackholing among network operators.

Método del siguiente salto (White Paper Cisco Systems):

“In the next hop method the trigger device sets the next hop route for the destination IP address that is to be black holed and the uses iBGP route update to propagate this route to all the edge routers (iBGP peers). The iBGP peers then set their next hop to the destination based on this update from the trigger. On every edge router, there is a static route for this next hop set to null0. Upon receiving a route update for the destination IP address, all edge routers set their next hops accordingly. The static route for the next hop effectively forwards all traffic for the black holed destination IP address to null0.”

Example:



The sequence of events for next hop RTBH filtering is as follows:

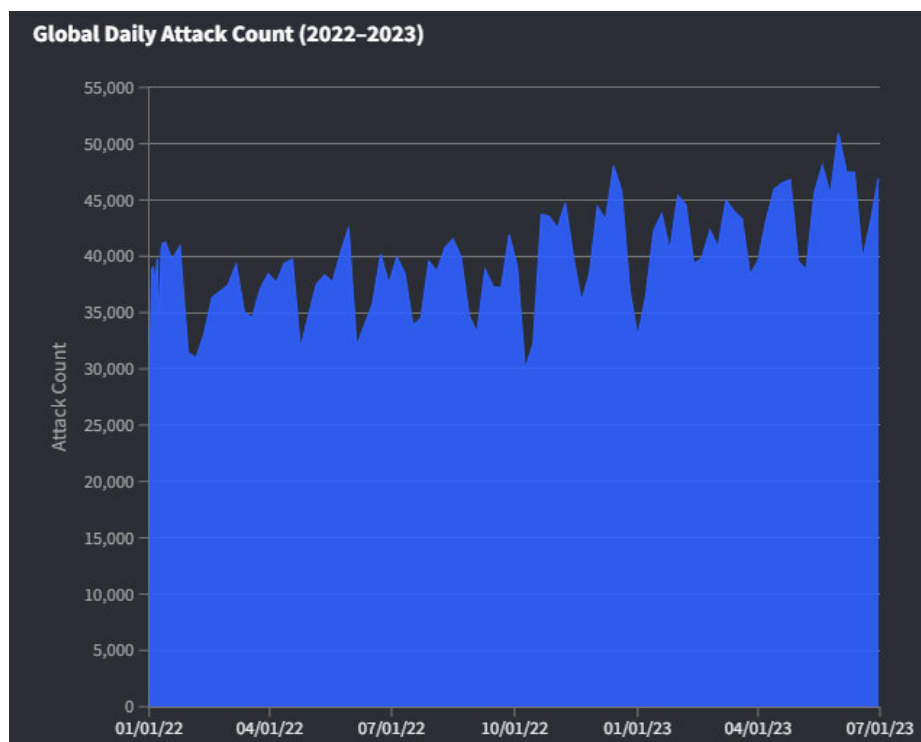
1. An attack is targeted at 172.18.192.1.
2. A static route to the target IP address, 172.18.192.1, is added to the triggering device with the tag 66.
3. A route map in the trigger matches the tag 66 and sets the next hop to 192.0.2.1, origin to IGP, and community to no-export.
4. The trigger sends the route as an iBGP route update to its peers.
5. The edge routers that are peers receive the update and accordingly set the next hop to the target, 172.18.192.1, as 192.0.2.1.
6. Because the edge routers have static routes of 192.0.2.1 set to null0, the final FIB entry for the target IP address (172.18.192.1) is set to null0.

7. All future traffic to 172.18.192.1 will be forwarded to null0 and dropped.

Enfoque basado en comunidades (White Paper Cisco Systems):

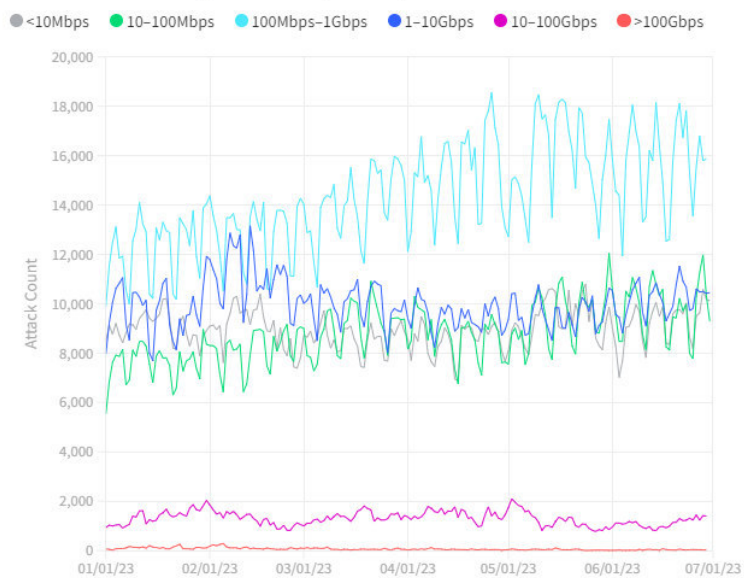
“Community-based triggering allows for better control over the drop process. In this technique, the trigger router is used to set different BGP community values and then send these values to its iBGP peers (BGP send-community) in its route update. The edge routers have the flexibility to act or not act on updates based on the community values. So, the decision to act or change route attributes such as next hop is based on community values, and the decision-making process is pushed out to the edge of the network, making it a highly flexible solution that can be used to selectively drop traffic.”

Conteo de Ataques DDoS registrados diariamente a nivel mundial:



Rango de ancho de banda de ataque a nivel global:

Global Bandwidth Range Breakdown (1H 2023)



BANDWIDTH BY PERCENTAGE

<10Mbps	21%
10-100Mbps	20%
100Mbps-1Gbps	33%
1-10Gbps	23%
10-100Gbps	3%
100Gbps-1Tbps	<1%

Top 5 Países más atacados a nivel LATAM:

