	Informe de Prácticas Profesionales como Opción de Grado	

TÍTULO DE INFORME:

Guía de entrenamiento para la solución de problemas básicos en el tráfico a través por medio de los Firewalls ASA y Firepower

PRESENTADO POR:

David Humberto Bueno Prada

Código:

2012119312

PRESENTADO A:

Tutor de prácticas profesionales

Dora Elena Ayala Pérez
Jefe inmediato empresa

UNIVERSIDAD DEL MAGDALENA
FACULTAD DE INGENIERÍA
Ingeniería Electrónica

Fecha de entrega: 15/11/2022

Contenido

1. PRESENTACIÓN 3
2. OBJETIVOS Y/O FUNCIONES 4
   2.1. Objetivo General: 4
   2.2. Objetivos Específicos: 4
   2.3. Funciones del practicante en la organización: 5
3. JUSTIFICACIÓN: 6
4. GENERALIDADES DE LA EMPRESA: 7
5. SITUACIÓN ACTUAL 8
6. BASES TEÓRICAS RELACIONADAS 9
7. DESARROLLO DE ACTIVIDADES: 10
8. CRONOGRAMA: 12
9. CONCLUSIONES Y LÍNEAS FUTURAS 12
10. BIBLIOGRAFÍA 13

1. PRESENTACIÓN

A partir de la necesidad de proveer un entrenamiento unificado para los nuevos ingenieros del equipo de Firewall para la campaña de Cisco en Sykes Enterprises, Inc., nace este proyecto basado en los conocimientos necesarios para la solución de problemas básicos para el tráfico a través de los Firewalls de la empresa Cisco y los procesos derivados para la resolución de los casos.

SYKES es una compañía multinacional, líder en la prestación de soluciones de marketing digital y experiencias inteligentes para clientes de las más grandes compañías a nivel global. En Colombia, Sykes tiene campañas como la de Cisco, donde se proporcionan ingenieros de redes y afines, para la resolución de problemas en el área de telemática en el equipo de Technical Assistance Center (TAC).

Sykes es una compañía que posee políticas de privacidad, y es muy importante la confidencialidad que brinda a sus clientes en función a los proyectos que se desarrollen para ellos, por lo cual, este proyecto se centra solo en la construcción de la guía y los conocimientos aplicados.

Los conocimientos proporcionados por Cisco para este fin son un conjunto de guías separadas en su página web, que solo incluyen la configuración básica de los dispositivos, por esto, este proyecto es de beneficio para Sykes, dado que facilita la instrucción de nuevos ingenieros y explica de manera unificada los procesos para la resolución de casos con la información provista por Cisco.

Con lo anterior mencionado en mente, este proyecto busca, de manera apropiada, desarrollar una guía para el entrenamiento de los ingenieros de Sykes en la solución de problemas básicos con el flujo de tráfico a través de los dispositivos de firewall, aplicando los conocimientos previos en el área de telemática y los aprendidos durante las practica profesionales en Sykes.

Al concluir el proyecto, se espera tener la guía para la resolución de problemas de tráfico que atraviesa los Firewall de Cisco, cumpliendo las recomendaciones de Cisco y los temas necesarios para la resolución de estos casos, para que así se estudie la posibilidad de su implementación en el entrenamiento regular de nuevos ingenieros.

2. OBJETIVOS Y/O FUNCIONES

Describa cual es el objetivo general y los específicos del proyecto) (Recuerde que los objetivos deben iniciar con un verbo en infinitivo, que implique una acción, relacionado con el problema central. Aquí se debe definir el fin concreto que persigue el trabajo, para que se pueda considerar resuelto el problema planteado, características de los objetivos medibles, alcanzables, ejecutables etc.)

2.1. Objetivo General:

Desarrollar una guía de entrenamiento para la solución de problemas básicos en el tráfico por medio de los Firewalls ASA y Firepower

2.2. Objetivos Específicos:

1. Con los entrenadores y lideres de equipo, establecer cuáles son los casos que se presentan con mayor regularidad relacionados con el tráfico que pasa por medio de los Firewalls y establecer uno a uno los procesos básicos que sigue el Firewall en cada problema que se presente.
2. Determinar las configuraciones del dispositivo que se van a tener en cuenta para la resolución de problemas en cada uno de los procesos.
3. Revisar los comandos "show" en el ASA y los ficheros Linux en el Firepower, para determinar las configuraciones y el estado actual de los dispositivos.
4. De acuerdo con el resultado encontrado en el diagnóstico del dispositivo, determinar las guías correspondientes basándonos en diagrama de flujo del tráfico en el dispositivo.
5. Confirmar con los entrenadores y líderes de equipo los parámetros requeridos por la empresa para las guías de entrenamiento.
6. Verificar con los entrenadores y lideres de equipo que las guía y los procedimientos son los apropiados para cada uno de los panoramas planteados y que cumplen los parámetros requeridos por la empresa para una guía de entrenamiento.
7. Conformar la guía general que permita la resolución de cada uno de los problemas presentados.

2.3. Funciones del practicante en la organización:

Diseñar soluciones de red enfocadas en seguridad para los diferentes clientes de Cisco. De igual forma verificar que los dispositivos y configuraciones cumplan con los estándares de seguridad requeridos para garantizar el correcto funcionamiento de las redes.

- Asistir en las diferentes configuraciones que los clientes desean implementar como:
  - NAT (Estática y Dinámica) y PAT.
  - OSPF, EIGRP, Rutas Estáticas y demás protocolos de enrutamiento.
  - DHCP.
  - Control de acceso (SSH, HTTP, Telnet, etc.).
  - Subneting.
  - Listas de acceso a la red (estándar y extendidas) y programación basada en objetos.
  - Servidores Syslog y SNMP.
  - Conexiones basadas en protocolos y puertos de red.
  - MPF (Modular Policy Framework) y PBR (Policy Based Routing).
- Verificar que los dispositivos de los clientes cuenten con el apropiado cableado según la
- configuración que desean y cumplan con los estándares (IEEE 802.3),
- Verificación de los enlaces de red, tasa de transferencia de datos, estado físico de los puertos, temperatura de los disipadores y procesadores, integridad de la base de datos y apropiado funcionamiento de esta en los dispositivos que están a su cargo, con el objetivo de prever y/o corregir fallas en la estructura de red del cliente.

3. JUSTIFICACIÓN:

Dada la alta demanda por parte de Cisco, la empresa Sykes se encuentra en procesos para la contratación de nuevos ingenieros cada semestre para los distintos equipos de la compañía de Cisco.

En pos de proveer un entrenamiento apropiado, cada entrenador de la campaña de Cisco prepara un conjunto de temáticas correspondientes a los temas que aseguren todos los procesos que se soportan en cada equipo, y proceden a la adaptación de las guías de Cisco para añadir procesos y procedimientos no incluidos en las guías que ayudan al diagnóstico y resolución de problemas.

Al momento de publicado este documento, el equipo de Firewall, no posee una guía para la solución de problemas con el tráfico que pasa a través de los Firewalls. Este hecho hace que estos casos, sean un fuerte punto de escalación dado que muchos ingenieros no tienen una guía apropiada que les permita consultar esta temática en profundidad y deben proceder a realizar investigaciones mas exhaustivas con sus Lideres de Escalación e Ingenieros Superiores.

Para que Sykes proporcione a Cisco y a sus clientes una experiencia apropiada, se le requiere a los ingenieros manejar unos tiempos para la resolución de casos de menos de 10 días, y las escalaciones son el principal factor que retrasa la resolución de los casos.

Con esto en mente nace este proyecto para el desarrollo de una guía para la solución de problemas con el tráfico que pasa a través de los Firewalls que incluya el análisis de los problemas más comunes, y las investigaciones pertinentes en cada uno de los casos.

4. GENERALIDADES DE LA EMPRESA:

Sykes fue fundada en 1977 por John H. Sykes en Charlotte, Carolina del Norte, para brindar servicios de ingeniería y diseño a grandes corporaciones.

Desde hace más de 5 años, Sykes provee equipos de ingenieros para el soporte técnico en muchas tecnologías de Cisco.

Cisco Systems fue fundada en 1984 por un grupo pequeño de científicos de la Universidad de Stanford y actualmente es el líder del mercado en diversas áreas, tales como routing y switching, comunicaciones unificadas, soluciones inalámbricas y seguridad.

Además de desarrollar el hardware de sus equipos, Cisco Systems también se ocupa de desarrollar su propio software de gestión y configuración de los mismos.

En 2005, Cisco introdujo un dispositivo Firewall físico basado en Linux conocido con el nombre de Cisco Adaptive Security Appliance o Cisco ASA.

Sourcefire creo otros dispositivos de Firewall físicos creando una versión comercial de Snort, y años más tarde, Cisco compraría Sourcefire en Julio de 2013 y aplicaría estas tecnologías a sus propios dispositivos, dando origen a los Firepower modernos.

Cuando Sykes comenzó a trabajar para Cisco, nació el programa SYKES Tech Academy como un proyecto para crear una "fábrica de ingenieros" para proporcionar un flujo constante de talento para Cisco que pudiera suplir la demanda.

En SYKES Tech Academy se encargan de que los ingenieros tengan conocimientos clave en CCNA, LINUX, y programación.

Para trabajar en una tecnología del equipo de TAC, Sykes requiere que se completen los cursos de CCNA de SYKES Tech Academy, 1-3 meses de training de la tecnología especifica a desempeñar, validación de los conocimientos de inglés, y un periodo de tiempo de prueba con casos básicos.

Cada vez que el los clientes abren un requerimiento con Cisco se crea un tiquete con los ingenieros llamados casos. La calificación de los casos es determinada por métricas prefijadas por nuestros jefes directos para asegurar la resolución de casos de manera rápida y eficaz.

5. SITUACIÓN ACTUAL

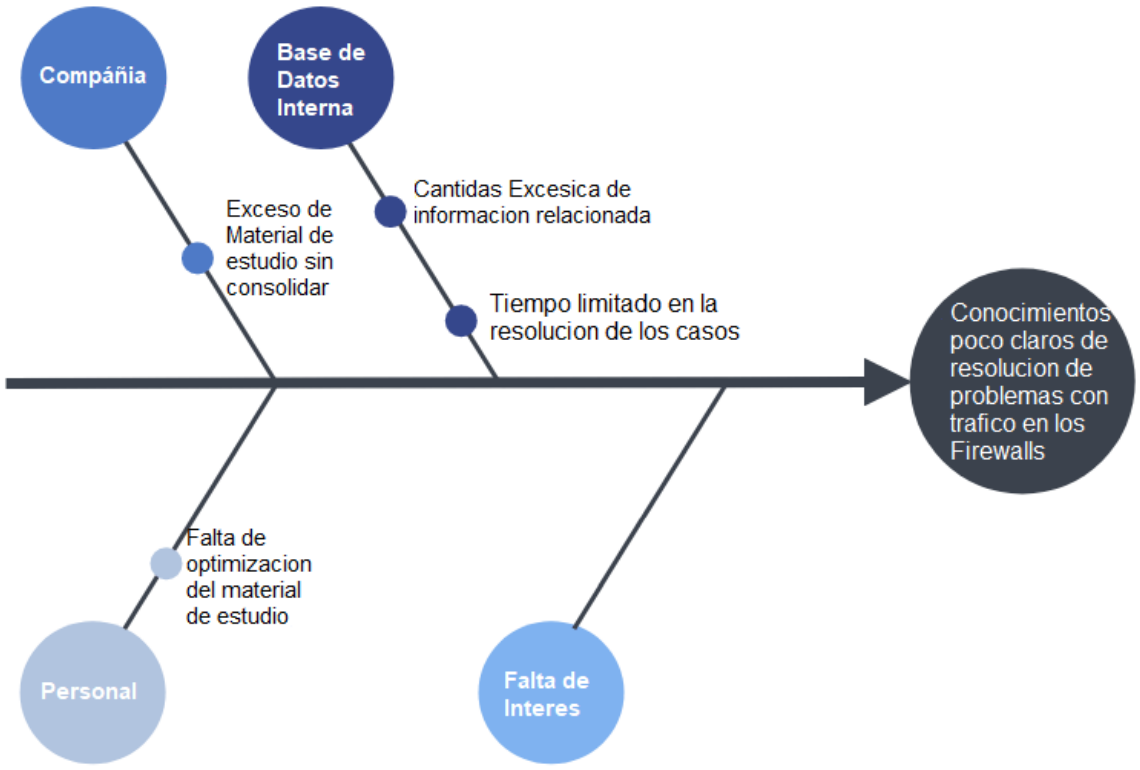

Figura 1. Diagrama de causa y efecto

6. BASES TEÓRICAS RELACIONADAS

Telemática y Telecomunicaciones: La base principal de conocimientos requeridos por la empresa, una gran herramienta que me brindó la universidad ya que todos los conocimientos requeridos para estar en Cisco son en base a la Telemática.

Metodología de investigación y Seminario: Fundamental para la creación de esta guía y fueron conocimientos importantes para el desarrollo de mis conocimientos en la empresa y como ingeniero.

Ética Profesional: Imprescindible para la empresa y para mí como ingeniero, fueron conocimientos de suma importancia, ya que bien aplicada hacen destacar a mi como ingeniero y deja en buen nombre a la universidad

7. DESARROLLO DE ACTIVIDADES:

Investigar las herramientas, comandos y procedimientos para la revisión de problemas con tráfico que pasa atreves de un Firewall.

En la primera semana se procedió a consultar las guías públicas de Cisco, los libros de conocimientos simples y complejos de Networking de Cisco, las bases de datos internas, los registros de casos previos, los lideres de escalación y los ingenieros superiores.

De esta interacción se determinó que hay 8 fases principales en el tráfico de datos en los Firepowers, determinamos los pasos pertinentes para la resolución de algunos problemas en los ASA y Firepower relacionados con la guía, tomamos los diagramas de flujo de los Firepower de Cisco, y reunimos información del funcionamiento de los motores que componen el Firewall.

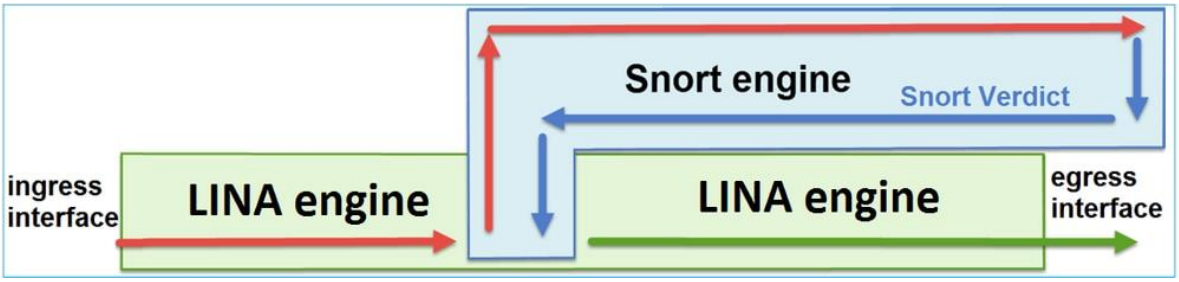

Figura 2. Ilustración de la interacción entre el motor LINA y Snort

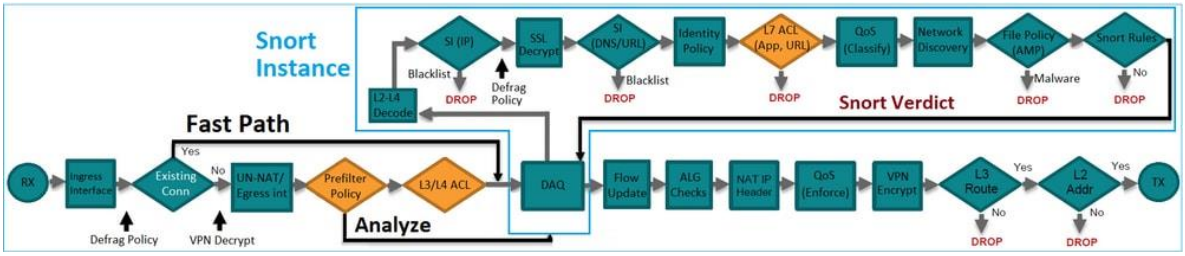

Figura 3. Diagrama de flujo de los Firewalls de Cisco

Organizar estos conocimientos por orden de prioridad.

A lo largo de la segunda semana se procedió a dividir las guías y procedimientos anteriormente descritos basándonos en el diagrama de flujo del Firewall.

En el análisis de paquetes para esta guía, se analizan los procesos en el siguiente orden:

1. Interface de ingreso y salida

2. Un-Nat
3. Politica de Prefiltrado y Preprocesado
4. Listas de control de acceso de capa 3 y capa 4
5. Politica de inteligencia de seguridad (SI policy)
6. Política de control de acceso
7. Política de intrusión
8. NAT
9. Enrutamiento en capa 3
10. Enrutamiento en capa 2

A su vez cada análisis se revisará la configuración por parte del cliente primero y el análisis de errores en el hardware y versión del dispositivo después.

Desarrollar como estas guías deben usarse para para la solución de los problemas más comunes y que componentes tiene que tenerse en cuenta.

Durante la segunda y tercera semana, se procedió la construcción de la guía incorporando los procedimientos para la revisión de cada uno de los procesos anteriormente descritos, y se incorporo un sistema de pasos a seguir para los casos más comunes.

Apoyo y aprobación de superiores en estructurar la guía.

Durante la segunda y tercera se consulto con mis superiores para asegurar que los conocimientos recolectados eran los requeridos para la resolución de los problemas anterior mente planteados y se presento un boceto de la guía a presentar en el proyecto.

Desarrollo y estructuración de la Guía.

De la tercera semana en adelante, se procedió con la construcción de la guía de manera que los conocimientos fueran relacionados entre sí. Esto crearía la guía unificada que se requeriría para la implementación en el programa de entrenamiento de los nuevos ingenieros en el equipo de Firewall en la campaña de Cisco dentro de Sykes.

Consolidación de Guías y corrección de errores.

Paralelamente a la construcción de la guía, se trabajó en la corrección de errores y la verificación de los principios descritos en esta para la resolución de casos para su posterior revisión y corrección de errores por parte de los ingenieros superiores y líderes de equipo para confirmar que la guía.

8. CRONOGRAMA:

De acuerdo a las funciones y las actividades realizadas ubíquelas a través de un diagrama de Gantt (ver ejemplo)

FASES	ACTIVIDAD	SEMANAS															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
FASE I	Investigar la documentación de Cisco y las Bases de datos internas con respecto a la resolución de problemas con tráfico que pasa a través de los Firepower que soportamos.																
FASE II	Organizar la información por orden de prioridad basándome en los diagramas de flujo recolectados																
FASE III	Desarrollar como estas guías deben usarse de forma conjunta para la solución de los problemas más comunes.																
	Apoyo y aprobación de superiores en estructurar la guía.																
	Desarrollo y estructuración de la guía																
FASE IV	Consolidación de guías y corrección de errores.																

9. CONCLUSIONES Y LÍNEAS FUTURAS

Al concluir la guía de entrenamiento para la solución de problemas básicos con el tráfico a través de los Firewalls, se espera que tenga acogida por parte del jefe inmediato y por las demás personas al interior de la empresa, para que se evalúe la posibilidad de una implementación en el programa de entrenamiento de los nuevos ingenieros en un futuro cercano.

10.BIBLIOGRAFÍA

1. Rajib Nazmul (2022). CCNP Security Cisco Secure Firewall and Intrusion Prevention System Official Cert Guide 1st Edition. Cisco Press.
2. Odom, Wendell (2019). CCNA 200-301 Official Cert Guide, Volume 1 1st Edición. Cisco Press.
3. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting: Overview. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214572-firepower-data-path-troubleshooting-ove.html*
4. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting Phase 1: Packet Ingress. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html*
5. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting Phase 2: DAQ Layer. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html*
6. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting Phase 3: Security Intelligence. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html*
7. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting Phase 4: Access Control Policy. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html*
8. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting Phase 7: Intrusion Policy. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html*
9. Cisco System Inc, (s.f.). Firepower Data Path Troubleshooting Phase 8: Network Analysis Policy. Recuperado el Julio 8 de 2019 de *https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html*