



VIGILADA SUPERSERVICIOS - NÚMERO ÚNICO DE REGISTRO NUIR 1 - 25290000-2

PLAN DE CONTINGENCIA DE ADOPCIÓN DE IPV6

Avenida Las Palmas No.4-66PBX 867 98 77 Líneas de atención 24 horas 8672577 - 8675722 - 8673922
emserfusa@emserfusa.com.co pqr@emserfusa.com.co www.emserfusa.com.co

¡Con La Fuerza De La Gente!

CONTENIDO

CONTENIDO	2
INTRODUCCIÓN	3
1. JUSTIFICACIÓN.....	4
2. OBJETIVOS.....	5
2.1. OBJETIVO GENERAL.....	5
2.2. OBJETIVOS ESPECÍFICOS.....	5
3. DEFINICIONES	6
2. ESQUEMA DE CONTINGENCIA	8
2.1. TOPOLOGÍA DE CONTINGENCIA (CON SOPHOS PASIVO)	8
2.2. PRUEBAS DE FUNCIONAMIENTO	9

INTRODUCCIÓN

La Empresa de Servicios Públicos de Fusagasugá adopta el Plan de Contingencia en la Transición del Protocolo IPV4 a IPV6, con base en las directrices dadas por el Ministerio de las Tecnologías de la Información y las comunicaciones a través de la resolución 2710 del 03 de octubre de 2017 y la Resolución 1126 de 8 de mayo 2021, en la cual se establecen los lineamientos para su adopción, igualmente hace uso de los documentos: “GUÍA DE TRANSICIÓN IPV4 A IPV6 PARA COLOMBIA”, “GUÍA PARA EL ASEGURAMIENTO DEL PROTOCOLO IPV6”, con el objetivo de asegurar una hoja de ruta que minimice la ocurrencia de los riesgos asociados.

Debido a que la organización para la cooperación y el desarrollo económico OCDE, ha establecido que la falta de implementación del protocolo IPV6 impactará el desarrollo de la economía sobre internet en términos de reducción de información y de desarrollo de nuevos servicios, es por lo tanto que ante el inminente agotamiento de las direcciones IP existentes, el Plan de transición de Protocolo IPV4 a IPV6, le corresponda un Plan de Contingencias.

El documento CONPES 3650 del 15 de marzo de 2010 ratifica la correspondencia de las Entidades públicas en adoptar las medidas necesarias para garantizar el aprovechamiento de las TIC, e implementar mecanismos que conduzcan al mejoramiento de canales de atención no presencial, la incorporación gradual de medios electrónicos en los procedimientos administrativos, el acceso permanente y gratuito de la información pública, al igual que los mecanismos de seguridad TI para el tratamiento de ésta, como lo indica el Decreto 2693 de 2012.

Dado lo anterior se hace necesario el diagnostico, la planificación, la Adopción, las verificaciones de prueba y error y posterior despliegue del Protocolo IPV6, manteniendo el Protocolo IPV4, asegurando la comunicación Doble Pila.

1. JUSTIFICACIÓN

Para la ejecución de las Plan de Contingencias para IPv6 se hace necesario las contar con las actividades y procedimientos que servicios críticos de la red tales como direccionamiento DHCP, DNS, Pruebas de Nombre IPV6, VPN y servidor del Directorio Activo y los sistemas de información, para que en caso de fallas al momento de implementar IPv6, se tenga el respaldo correspondiente y así mitigar posibles caídas del servicio

2. OBJETIVOS

2.1. OBJETIVO GENERAL

El objeto general es realizar un Plan de Contingencias para IPv6 en EMSERFUSA E.S.P., es para mitigar el impacto y la funcionalidad el esquema Dual Stack del Protocolo IPV6 implementado en la entidad.

2.2. OBJETIVOS ESPECÍFICOS

- Realizar monitoreo de la funcionalidad de IPv6 en los sistemas de comunicaciones y servicios de EMSERFUSA E.S.P., que permita verificar el tráfico de IPv6 de la entidad hacia Internet y viceversa.

3. DEFINICIONES

Para el presente documento se consideran las siguientes definiciones:

- a) Amenaza¹ (Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- b) Análisis de riesgos (Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- c) Auditoría (Inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.
- d) Autenticación (Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una Entidad es correcta.
- e) Confidencialidad (Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.
- f) Disponibilidad (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.
- g) DHCPv6 (Protocolo Dinámico de Configuración de nodos) Protocolo de configuración con estado (“stateful”) que proporciona direcciones IP, direcciones de los servidores DNS y otros parámetros de configuración.
- h) Dirección Identificador único asignado a nivel de la capa de red a una interfaz o conjunto de ellas, que puede ser empleado como campo de origen o destino en datagramas IPv6.
- i) DNS (Sistema de nombres de dominio, Domain Name System) Sistema jerárquico de almacenamiento y el protocolo asociado para almacenar y recuperar información que permite vincular nombres y direcciones IP.
- j) Doble-Pila (dual-stack) Mecanismo de coexistencia IPv4/IPv6, mediante el cual un nodo incorpora tanto la pila IPv4 como la pila IPv6.
- k) Seguridad del Protocolo de Internet, (Internet Protocol security) Conjunto de estándares que proporciona comunicaciones privadas y autenticadas a

nivel de red, por medio de servicios criptográficos. soporta autenticación a nivel de entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección anti-repeticiones.

- l) IPv4 Protocolo de Internet versión 4.
- m) IPv6 Protocolo de Internet versión 6.
- n) ISP – Internet Service Provider Un Proveedor de Servicios de Internet asigna principalmente espacio de direcciones IP a los usuarios finales de los servicios de red que éste provee. Sus clientes pueden ser otros ISPs. Los ISPs no tienen restricciones geográficas como lo tienen los NIRs.
- o) Notación hexadecimal, Notación empleada para expresar direcciones IPv6 en forma literal. La dirección de 128 bits es dividida en 8 bloques de 16 bits cada uno. Cada bloque se expresa como un número hexadecimal y éstos están separados del siguiente por medio del “:”. Los ceros situados a la izquierda de cada bloque pueden ser omitidos. Ejemplo de una dirección IPv6 unicast: 2001:DB8:1234:ABCD:789:EF01:0:1.
- p) Resolución de nombres Obtención de una dirección a partir de un nombre.
- q) RFC (petición de comentarios, request for comments) Paso previo de un documento estándar de Internet (STD), aunque en la actualidad, los fabricantes implementan en sus productos RFCs, sin esperar a que sean STD.
- r) Subred Uno o más enlaces que utilizan el mismo prefijo de 64 bits.
- s) Transición Conjunto de mecanismos que permiten la integración de IPv6 en las redes con IPv4, básicamente doble-pila, túneles y traducción.
- t) RIR - Regional Internet Registry Los Registros de Internet Regionales (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir los recursos de Internet dentro de las respectivas regiones.

4. ESQUEMA DE CONTINGENCIA

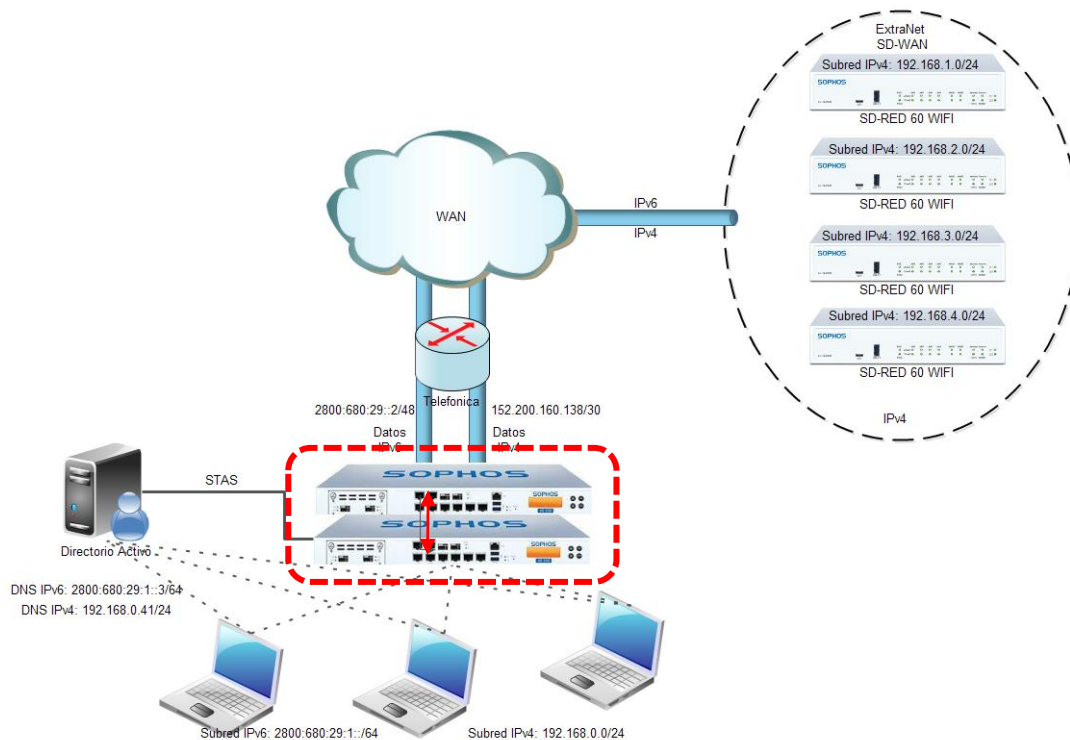
En el Sophos las funciones de IPv4 e IPv6 operan por medio de políticas diferentes comportándose como firewalls independientes para cada uno de estos protocolos, actualmente la infraestructura cuenta con dos (2) firewalls físicos los cuales operan en modelo de activo-pasivo.

Por lo que en operación solo se encuentra uno y el otro sube en el momento que el principal falle este tiempo fue probado y la transición es de 1-2 minutos en los que las sesiones se reinician.

Los servicios de conmutación por error entre el protocolo IPv4 e IPv6 dependerá de los servicios que se consuman si los servicios que fallen son alojados en IPv4 solo los servicios externos e internos que soporte el protocolo IPv6 funcionaran, de igual manera pasara en caso contrario donde falle el protocolo IPv6.

4.1. TOPOLOGÍA DE CONTINGENCIA (CON SOPHOS PASIVO)

Tabla 1 Diseño de Red en Contingencia.

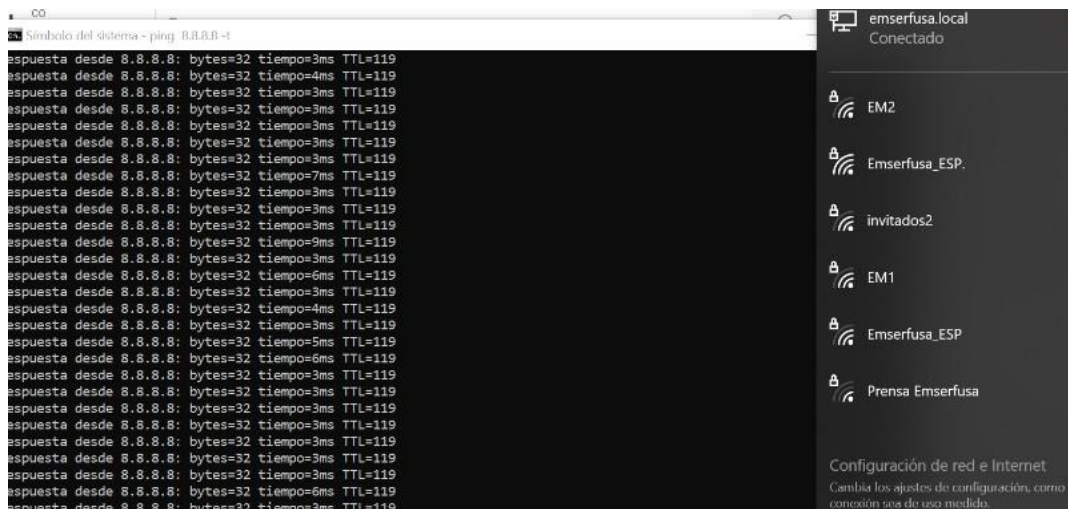


4.2. PRUEBAS DE FUNCIONAMIENTO

Se realiza la desconexión del firewall principal para evidenciar el protocolo de respaldo del firewall auxiliar.

Se evidencia que el firewall auxiliar tarda en promedio 90 segundos para tomar asumir el rol del firewall principal gestionando la red y los servicios configurados.

Tabla 2 Pruebas de Funcionamiento de la Red.



VIGILADA SUPERSERVICIOS - NÚMERO ÚNICO DE REGISTRO NUIR 1 – 25290000-2

Tabla 3 Evidencia de la Configuración de Red en Contingencia.



Las pruebas de funcionamiento se realizan en compañía del personal encargado de área de sistemas de **EMSERFUSA E.S.P.** en el cuarto de comunicaciones, los equipos conectados de manera individual y simultanea evidenciando el proceso de gestión de los equipos en la red local y la salida a servicios web.

VIGILADA SUPERSERVICIOS - NÚMERO ÚNICO DE REGISTRO NUIR 1 – 25290000-2