INFORME DE IMPLEMENTACIÓN DUAL-STACK IPV4-IPV6

DIRECCIÓN DE SERVICIOS DE INFRAESTRUCTURA DE TI

EMPRESAS PÚBLICAS DE MEDELLÍN E.S.P.

2020

Más información:
Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

TABLA DE CONTENIDO

Más información:
Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

Servicios de Infraestructura de TI

Más información:

Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

1. INTRODUCCCIÓN

Continuando con el plan de implementación de IPv6 dentro del marco de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 establecido por EPM siguiendo los lineamientos del ministerio de las TIC (Tecnologías de la información y las comunicaciones) se desarrolla la fase dos que corresponde a la implementación IPv6 en al DMZ de EPM.

De acuerdo al avance obtenido en la primera fase y considerando que todas las aplicaciones y servicios que el Grupo EPM provee o consume en Internet para uso de externos, usuarios y clientes en general se publican a través de la plataforma Netscaler y Servidores Proxy, como estrategia de adopción de IPv6, se utilizará la funcionalidad de doble stack IPv4 e IPv6 siguiendo las recomendaciones de Ministerio de las tecnologías de información y comunicación, en adelante, MInTIC, es decir, se implementará en la zona DMZ y en las conexiones con los proveedores ISP de acceso a Internet TIGO-UNE y Century Link.

Los servicios y aplicaciones internas de la organización se continuarán trabajando con direccionamiento privado en IPv4 y en etapas posteriores se evaluará la conveniencia de implementar IPv6 al interior de la red corporativa.

En este documento se describen las configuraciones en cada uno de los componentes, redes, seguridad, servidores y aplicaciones que se realizaron en el ambiente de producción DMZ del Grupo EPM para la puesta en operación de IPV6 en la modalidad de “dual-stack” con IPV4.

2. COMPONENTE DE RED

2.1 Arquitectura Actual DMZ EPM

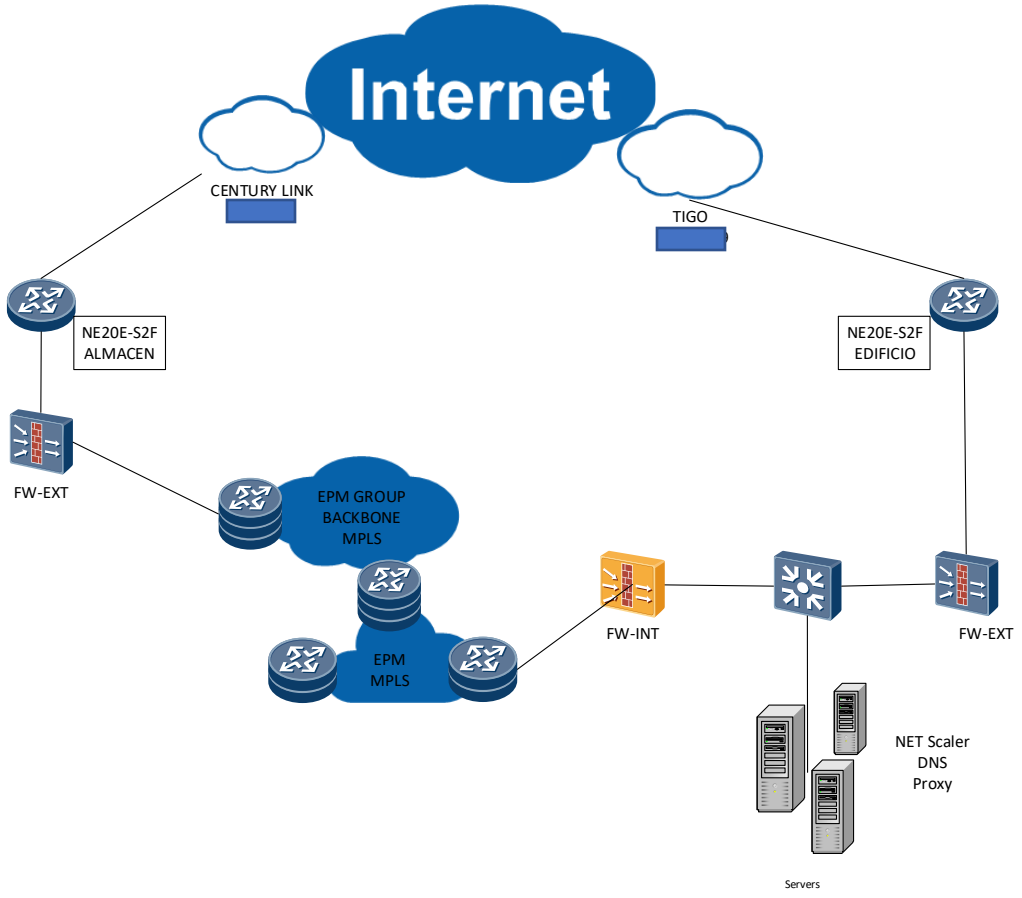
Para todos los servicios del grupo EPM ubicados en la DMZ y que deben ser publicados en internet en IPv6 se dispone de salida internet a través de dos ISP (TIGO y Century Link) ubicados en diferentes localizaciones físicas, una se encuentra en el edificio inteligente y otra en almacén, los servicios de estos son simétricos en cuanto a ancho de banda disponible con un ancho de banda disponible de 1G y estas conexiones actualmente cuentan con servicios IPv4 operativos.

Los diferentes servidores de la DMZ necesarios para la publicación de los servicios del grupo en IPv6 como son NetScaler, DNS, Proxy se encuentran ubicados en el edificio inteligente conectados físicamente a SWs LAN Huawei

que proveen servicios de conexión de capa dos hasta el firewall externo de edificio el cuál provee la protección de estos de los ataques externos, en este edificio se encuentra la salida a internet a través del ISP TIGO.

A nivel interno los SWs también proveen conexión a GW y firewall interno para acceder al core de EPM que está compuesto por Equipos Huawei conectados en Clúster y virtualizados para crear dos Equipos lógicos separados entre sí y estos a su vez acceden a la red Backbone MPLS del grupo que permite la conexión con el nodo de almacén donde se encuentra oro firewall externo y la conexión a internet a través del ISP Century Link.

A continuación, se observa la topología actual de red:



2.2 Antecedentes de Implementación de IPv6 en la Red de EPM

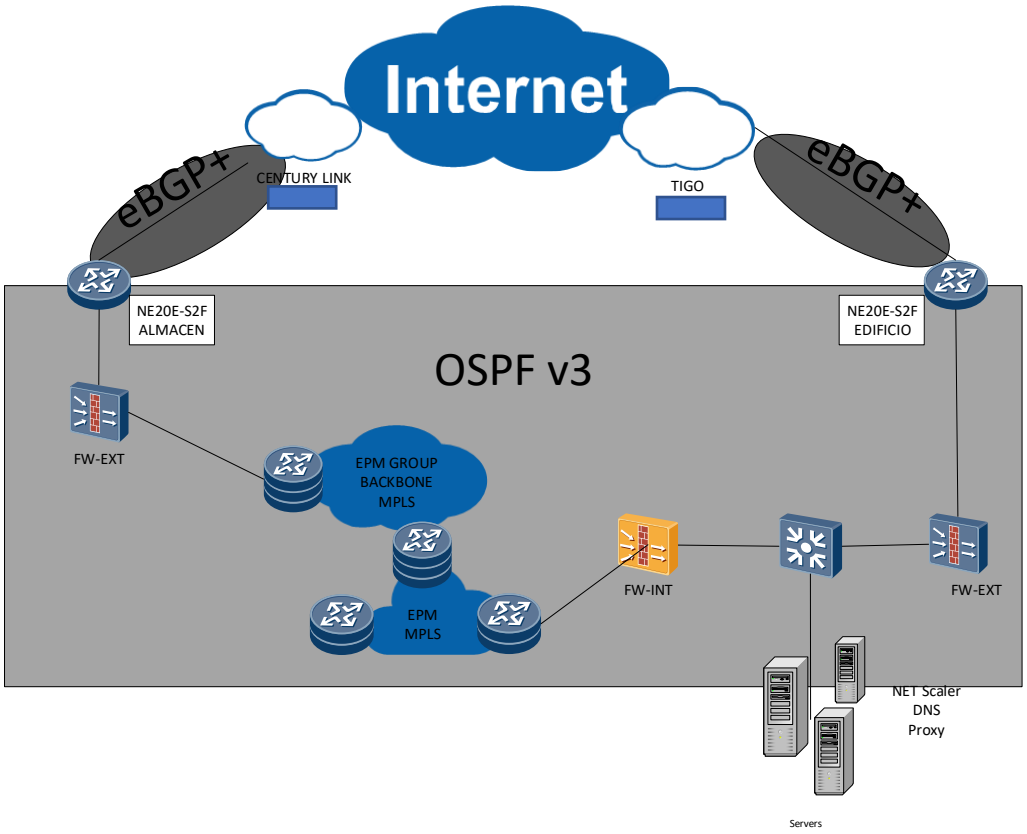
Para que EPM pueda dar el paso a la migración de la red a IPv6 se han llevado a cabo las siguientes fases:

1) Consultoría para definición de marco de trabajo para implementar IPv6 en EPM. De esta se obtiene documentación definición de recomendaciones para implementación de IPv6 de EPM y de las cuáles se recoge información para la entrega del presente servicio.
2) Se llevó a cabo revisión de los equipos de Red, Internet, Seguridad y demás equipos que hagan parte de una red IP para soportar IPv4/IPv6 dual-stack. Para los equipos Huawei se confirmó soporte de dual stack Ipv4/IPv6.
3) De acuerdo con el bloque publico IPv6 asignado por LACNIC a EPM para IPv6 se generó plan de direccionamiento consignado en documento donde se encuentra segmentación y asignación de las redes requeridas de manera similar a como se hace en IPv4. Destacando redes WAN con mascara /126, IPs Loopback /128 y redes LAN con mascara /64 y la red específica para uno en la DMZ.
4) Se llevó cabo restructuración de la DMZ para separar los servidores de servicios internos de los servicios con acceso externo a través de internet.

2.3 Diseño Esquema de Enrutamiento IPv6 para la DMZ de EPM

El diseño del esquema de enrutamiento se aborda evaluando dos aspecto de enrutamiento, el primero el enrutamiento de exterior al sistema autónomo y el segundo el enrutamiento interior al sistema autónomo, para el primero se adopta BGP4+ el cuál con las extensiones adicionadas a BGP4 como protocolo de vector distancia soporta transmisión de paquetes entre sistemas autónomos por medio de protocolos de capa de red y para este caso específico por medio de encapsulamiento por IPv6, con esta implementación se podrá adicionar al protocolo IPv6 información de alcanzabilidad de capa de red NLRI(Network Layer Reachable Information) por sus siglas en inglés, por medio de nuevos atributos(Multiprotocol Reachable NLRI, Multiprotocol Unreachable NLRI) que permiten transmitir información de enrutamiento IPv6 entre sistemas autónomos. Para el segundo se adopta OSPFv3 que es desarrollado para ser independiente de cualquier capa de red específica y es usado para IPv6, OSPFv3 usa el mismo mecanismo básico de implementación de OSPFv2 como protocolo de enrutamiento de estado de enlace interior y que es al actualmente implementado en EPM, sin embargo, este último es usado para IPv4.

A continuación, se observa la implementación global de lo mencionado:



BGP+

Con el fin de tener alta disponibilidad de los servicios publicados a internet a nivel WAN se implementarán dos conexiones BGP4+ para ensenar las rutas de EPM hacia internet y recibir las rutas de internet. A continuación, se detallan los parámetros de las conexiones:

[TABLA 1] Tabla 1. Diseño BGP+ Interconexión EPM TIGO
[TABLA 2] Tabla 2. Diseño BGP+ Interconexión EPM TIGO

Se usará como ruta preferente la de la conexión a UNE teniendo en cuenta que se cuenta con redundancia de peers en esta interconexión, que el path de conexión a los equipos físicos de la DMZ es más corto por estar estos

ubicados en edificio y no requerir tránsito a través de la red Backbone MPLS del grupo EPM, lo anterior se lograra anunciando un AS path más largo en la conexión hacia Century Link y teniendo una preferencia mayor de la ruta default recibida a través de UNE, de la misma manera se ejecuta para las conexiones redundantes hacía UNE pero con valores intermedios en estos atributos.

OSPFv3

A nivel de enrutamiento interno es necesario se requiere proveer conectividad IPv6 entre los routers de internet y la DMZ, de manera que se pueda enrutar el tráfico hacia y desde cualquiera de las dos salidas a internet disponibles en un escenario normal o de falla de salida a internet con alguno de los dos proveedores de internet, esta conectividad además se debe hacer a través de la red MPLS de EPM en la que se implementará una L3VPN tipo VPNv6 que permita obtener la conectividad requerida e intercambio de rutas desde ambos extremos de la VPN.

A continuación, se detallan los parámetros necesarios para implementación de la conectividad mencionada:

[TABLA parámetros OSPFv3]

2.4 Actividades Ejecutadas IPv6 para la DMZ de EPM

BGP+

Se lleva a cabo la implementación de acuerdo con el diseño detallado previamente aplicando durante ventana de mantenimiento la configuración correspondiente y se lleva a cabo verificación de resultado esperado en routers de internet de EPM y de la misma manera se observa la publicación de segmento en proveedores de servicios de internet, tanto directamente conectados como
A continuación, se muestran detalles resultados de la implementación:

- Establecimiento de sesiones BGP:

Router de internet de Edificio

Imagen 1

Router de internet de Almacén

Imagen 2

- Anuncio de segmento IPv6 asignado por LACNIC a EPM

Router de internet de Edificio

Imagen 3

Router de internet de Almacén

Imagen 4

- Rutas IPv6 recibidas en conexiones con TIGO y Century Link

Router de internet de Edificio

Imagen 5

Router de internet de Almacén

Imagen 6

- Verificación de aprendizaje de bloque IPv6 de EPM en sistema autónomo directamente conectados con atributos esperados

Century Link

Más información:
Teléfono: 380 5556 Fax: e-mail: uo9080@epm.com.co

PANAMACITY PANAMA Bgp results for:

Imagen 7

- Verificación de aprendizaje de bloque IPv6 de EPM en sistemas autónomos de internet no conectados directamente con atributos esperados.

NTT

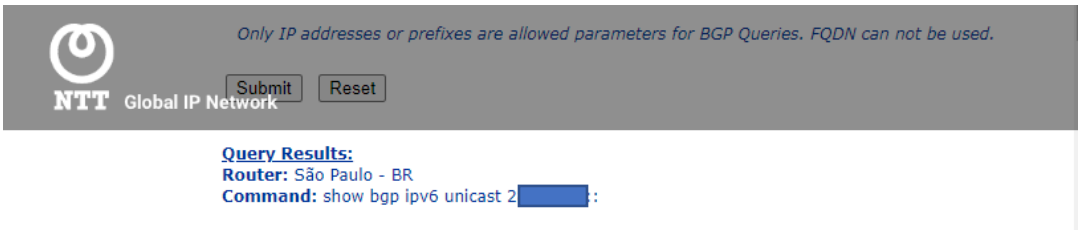


Imagen 8

COGENT

Imagen 9

OSPFv3

Para el desarrollo de esta actividad se tiene como prerrequisito disponer de capacidad de configuración de IPv6 y OSPFv3 en firewalls de acceso externo/interno, lo cual está siendo tramitado por parte de EPM, temporalmente se habilito enrutamiento estático para salida a internet desde firewall externo disponible actualmente.

Se informa direccionamiento IPv6 Global asignado a la DMZ (2801:160:0:2::/64) que será administrado por el grupo de Firewall.

Se informa que para la conexión WAN entre el Router de internet y el clúster de FWs de edificio que se comunican a través del SW DMZ(EPM-EDF_CTTP2B4-LAN-SZ1) en la VLAN 21 se asigna el siguiente direccionamiento IPv6 (2801[redacted]:/124)

2801[redacted]/124	Router de Internet
2801[redacted]/124	Virtual FW
2801[redacted]/124	FW-EXT-1_Internet
2801[redacted]/124	FW-EXT-2_Internet

2.5 Operación y Diagnósticos de Red

Como parte de las actividades de implementación del “dual-stack” IPV4 -IPV6 en la DMZ se documentaron las actividades correspondientes a la operación y diagnósticos sobre IPV6 para el personal de gestión y operación de la red de datos del Grupo EPM. A continuación, se adjunta el documento de Procedimientos de operación y diagnósticos IPv6.

Procedimiento de operacion y diagnos

3. COMPONENTE DE SEGURIDAD

3.1 Direccionamiento IPv6 Asignado al Firewall

En IPv4 se usa el firewall para la salida a internet por el proveedor de Tigo UNE, se implementa dual stack sobre esta interfaz configurando el direccionamiento IPv6 asignado por el área de comunicaciones.

Para el segmento de servidores se crea la VLAN en la red para que sea la nueva DMZ IPv6 en donde se configura el servidor NetScaler y el servidor DNS en este nuevo protocolo.

Para configurar la VLAN en el firewall fue necesario asignarle una IPv4 dado que la sincronización del clúster se realiza por protocolo IPv4.

En el siguiente resumen se detalla las configuraciones por interfaz en el firewall:

Dirección IPv6 sobre la interfaz de salida a Internet
Dirección IPv4 sobre la interfaz de salida a Internet
Dirección IPv6 sobre la interfaz DMZ IPv6
Dirección IPv4 sobre la interfaz DMZ IPv6

3.2 Topología de Red

El protocolo IPv6 se activó sobre los firewalls perimetrales que reciben toda la comunicación desde y hacia el canal de internet TIGO-UNE y adicionalmente tiene configurada la red DMZ donde se encuentran el NetScaler y los servidores que se publican hacia internet.

A continuación, la topología de red que se utilizó para la implementación del protocolo IPv6:

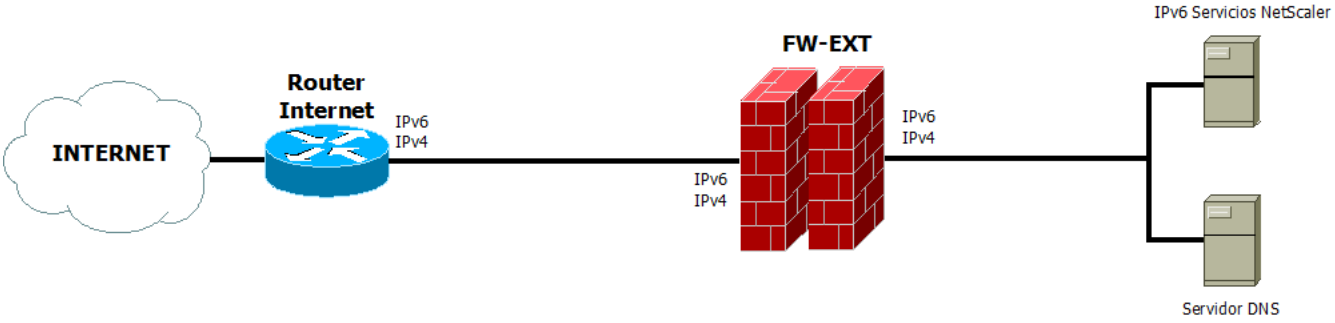
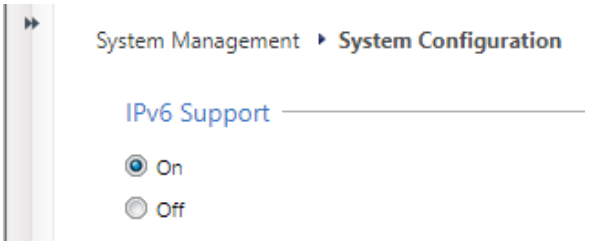


Figura Topología de red

3.3 Instalación Firewalls Perimetrales

Fue necesario realizar la actualización tecnológica de los firewalls perimetrales debido a que sobre los equipos tenían una configuración de balanceo de carga la cual no es compatible con el protocolo IPv6.

Los equipos nuevos se instalan con sistema operativo versión R80.30 y desde su implementación se les activa el protocolo IPv6:



3.4 Configuración de Direccionamiento

Se realiza la configuración de las interfaces, VLANs y direccionamiento IP de los firewalls según la topología de red propuesta.

- Configuración dual stack sobre la conexión del firewall hacia el router de internet
- Configuración de la VLAN para la nueva red DMZ en IPv6

3.5 Pruebas de conectividad hacia equipos de red EPM

Se realizan pruebas de conectividad ipv6 desde el firewall hacia cada interfaz de VLAN creada:

- Prueba de ping desde el firewall hacia el router de internet
- Prueba de ping desde el firewall VLAN hacia una IP del rango asignado para el Netscaler IPv6 y servidores

3.6 Configuración Ruta por Defecto

Se configura ruta por defecto para IPv6 en ambos firewalls.

3.7 Pruebas de conectividad hacia Internet

Se realiza prueba de ping IPv6 hacia una página de internet en este caso www.google.com

```
[                ]# ping6 www.google.com
PING www.google.com(2800:3f0:4005:405::2004) 56 data bytes
64 bytes from 2800:3f0:4005:405::2004: icmp_seq=0 ttl=116 time=13.5 ms
64 bytes from 2800:3f0:4005:405::2004: icmp_seq=1 ttl=116 time=11.7 ms
64 bytes from 2800:3f0:4005:405::2004: icmp_seq=2 ttl=116 time=11.7 ms
64 bytes from 2800:3f0:4005:405::2004: icmp_seq=3 ttl=116 time=31.9 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 11.719/17.242/31.983/8.543 ms, pipe 2
```

3.8 Reglas de Firewall para ICMP6

Se configura una regla que permite realizar pruebas de ping6 desde los segmentos definidos para la DMZ y red entre el firewall y router de internet hacia internet. Permitiendo realizar diagnósticos de conectividad.

3.9 Reglas de Firewall para Publicar Servicio DNS

Se configura las reglas de firewall de entrada y salida para que el servidor DNS IPv6 pueda realizar consultas y ser consultado por el puerto 53

3.10 Reglas de Firewall para Publicar Servicio NetScaler

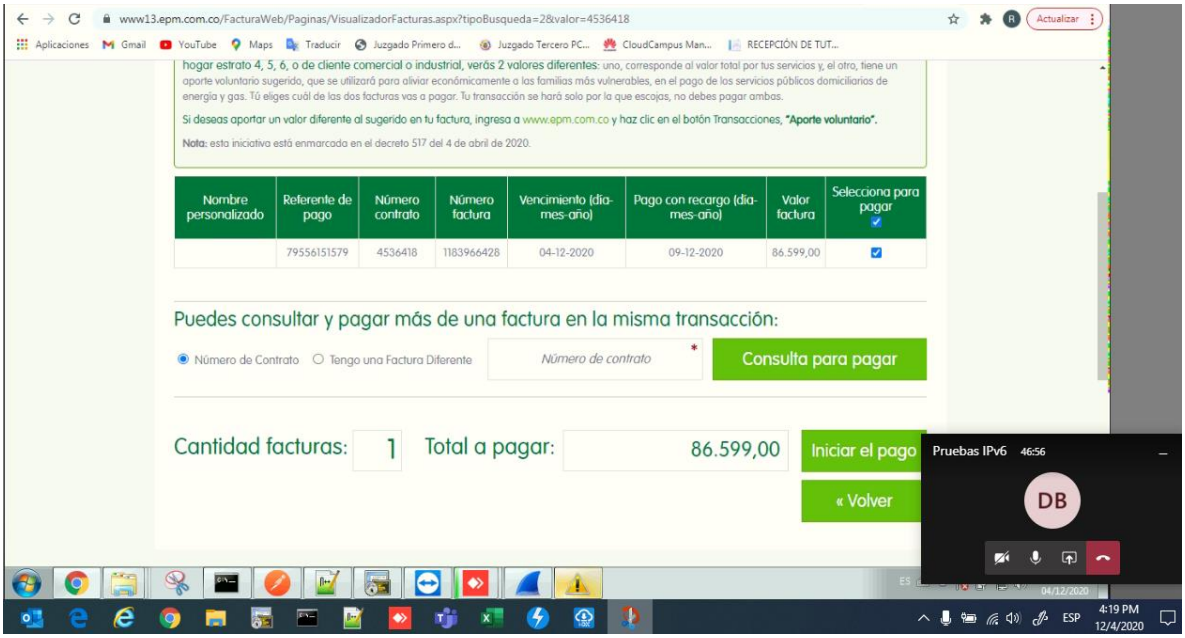
Se configura las reglas de firewall que permite la comunicación desde Internet a las direcciones IPv6 de los servicios publicados a través del NetScaler

3.11 Configuración Inspección HTTPS

Debido a que se tiene habilitada la inspección de HTTPS para servicios IPv4 expuestos por internet desde el NetScaler, se realiza la misma configuración para los servicios en su direccionamiento IPv6.

3.12 Logs de Firewall Durante las Pruebas de las Aplicaciones

Las pruebas de funcionalidad para la aplicación Factura Web en IPv6 se realizaron desde el equipo con dirección IPv6 2800:484:881:c9c2:ccb3:ade4:91a0:6b0b



3.13 Comportamiento del Firewall

Dado que este firewall fue instalado recientemente el activarle el protocolo IPv6 no impacta el consumo de recursos:

4. COMPONENTE DE SERVIDORES

Configuración servicio de DNS público para IPV6

Para el componente de servidores la implementación se realizó sobre el servidor DNS público de epm llamado POSEIDON

Lo primero es ingresar al servidor Poseidon por SSH mediante la herramienta PUTTY con la cuenta que tenga privilegios de administración sobre el servidor y configurar las interfaces, para configurarlos se hace mediante la edición del archivo de la configuración de la interface ubicado en la ruta:

/etc/sysconfig/network-scripts/
Debe quedar de la siguiente manera:
YPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth1
DEVICE=eth1
ONBOOT=yes
IPV4INITR=no
DOMAIN=epm.com.co
IPV6INIT=yes
IPV6_AUTOCONF=no
DHCPV6C=no
IPV6_DEFROUTE=yes
IPV6ADDR=[redacted]
IPV6_DEFAULTGW=[redacted]
IPV6_FAILURE_FATAL=no
IPV6_PEERDNS=no
IPV6_PEERROUTES=yes
DNS1=::1
DNS2=2001:4860:4860::8888
DNS3=2001:4860:4860::8844
# [VMware commented] HWADDR=00:15:5d:1b:36:09

Lo que está resaltado en amarillo son los valores que se deben configurar para IPV6
Luego de configurar las interfaces, el siguiente paso es configurar el servicio de DNS para que pueda publicar los registros con IPV6. Para esto debemos ir a la ruta donde se encuentra ubicado el archivo named.conf [root@poseidon etc]# vi named.conf se verifica que la variable listen-on-v6 { any; }; esté creada de lo contrario se debe crear

```
include "/etc/rndc.key";
options {
        directory       "/var/named";
        //recursion yes;                # enables resursive queries
        //#allow-recursion { trusted; };  # allows recursive queries from "trusted" clients
        //listen-on { [redacted]; };   # ns1 private IP address - listen on private network only
        //allow-transfer { [redacted]; };      # disable zone transfers by default

        dnssec-validation auto;
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        query-source-v6 port 53;

        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
```

Una vez validado esto se debe configurar la zona con la que vamos a trabajar para crear las entradas para IPV6, para nuestro caso es epm.com.co.zone la cual se encuentra en la ruta /var/named
Para modificar la zona se hace con algún editor de texto como el VI

vi epm.com.co.zone
Se agrega la zona
; Zona IPv6
Y se crean los registros AAAA de los sitios que vamos a publicar con su respectiva IPV6

```
ares                IN AAAA  [redacted]
; Zona IPv6

sistemasconsigna        IN AAAA  [redacted]
audisoft                IN AAAA
kairos                  IN AAAA
cef                     IN AAAA
```

www01	IN AAAA	
ws	IN AAAA	
checsiriusserver	IN AAAA	
dialin	IN AAAA	
lyncws	IN AAAA	
lync-dir	IN AAAA	
meet	IN AAAA	
www	IN AAAA	
appmovildllo	IN AAAA	
appmoviluat	IN AAAA	
btsprod	IN AAAA	
passwordreset	IN AAAA	
appmovil	IN AAAA	
jdemovil	IN AAAA	
www13	IN AAAA	
biblio	IN AAAA	
maps	IN AAAA	
cloudportal	IN AAAA	
jdemovilchec	IN AAAA	
jdemovilcens	IN AAAA	
jdemovilessa	IN AAAA	
jdemoviledeq	IN AAAA	
jdemovilevm	IN AAAA	
facturaweb	IN AAAA	
www01	IN AAAA	
ait46	IN AAAA	
www11	IN AAAA	
www8	IN AAAA	
mibitacora	IN AAAA	
bitacora	IN AAAA	
www12	IN AAAA	
mibitacoraessa	IN AAAA	
bp	IN AAAA	
miperfil	IN AAAA	
www5	IN AAAA	
xmcens	IN AAAA	
wscens	IN AAAA	
autconecta	IN AAAA	

Más información:
Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

conecta IN AAAA
podascens IN AAAA
www15 IN AAAA
sm IN AAAA
candes IN AAAA
epmcensohi IN AAAA
cmtpruebas IN AAAA
cmt IN AAAA
portalclientes IN AAAA
constructores IN AAAA
media IN AAAA
contactotransparente IN AAA
zonavirtual IN AAAA
clientescorporativos IN AAAA
censsiriusserver IN AAAA
maps3 IN AAAA
sonar IN AAAA
blog IN AAAA
bloguat IN AAAA
passwordregistration IN AAAA
zonaautogestion IN AAAA
vws20 IN AAAA
btsuat2016 IN AAAA
vws20a IN AAAA
vws20b IN AAAA
vws20c IN AAAA
vws20d IN AAAA
vws20e IN AAAA
vws20f IN AAAA
vws20g IN AAAA
vws20j IN AAAA
vws20k IN AAAA
vws20m IN AAAA
vws20n IN AAAA
u IN AAAA
portalesepm IN AAAA
encuestacovid19 IN AAAA
igst IN AAAA

Más información:
Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

servicesepm	IN AAAA	
manillascovid	IN AAAA	
aplicaciones	IN AAAA	
compras	IN AAAA	
www01	IN AAAA	
btsdllo	IN AAAA	
btsuat	IN AAAA	
crl	IN AAAA	
www4	IN AAAA	
mail	IN AAAA	
zonatransaccionesrapidas		
qlikmobile	IN AAAA	
qap	IN AAAA	
enter2	IN AAAA	
wsessa	IN AAAA	
essasanws	IN AAAA	
essatecmovil	IN AAAA	
mapspruebas	IN AAAA	
sacuat	IN AAAA	
www13	IN AAAA	
maps25	IN AAAA	
maps2	IN AAAA	
conectadllo	IN AAAA	

En el servidor se vería de la siguiente manera:

[IMAGEN ZONA IPV6]

Una vez agregados los registros debemos buscar el registro SOA y modificar el serial de la zona el cual está ubicado en la parte superior de la configuración de la zona. El estándar definido para el serial es AAAAMMDD## donde esto corresponde a Año, Mes, Dia y consecutivo del día en el cual se está ejecutando la modificación del registro

```
$TTL    3600
@                       IN SOA  [redacted]. (
                                2020121701 ; serial
                                1200       ; refresh (20 minutes)
                                1800       ; retry (30 minutes)
                                2419200    ; expire (4 weeks)
                                86400      ; minimum (1 day)
                                )
```

Se deben guardar los cambios en el archivo presionando la tecla esc :wq
Luego reiniciar el servicio de named con los comandos: service named restart
Y Validar el estado del servicio con el comado service named status

Para la validación del tráfico en IPV6 desde el exterior hacia la red que tiene IPV6 en EPM se realizó una prueba desde el extremo en la salida a Internet de TIGO siendo exitosa a conectividad, además se validó una transacción en Factura Web:

[IMAGEN PRUEBA CONECTIVIDAD CON DIRECCIONAMINETO IPV6]

Con las validaciones y resultados anteriores, se comprueba que el sitio publicado responde y resuelve con IPV6, tambian se validó la conectividad desde el la red en el edificio que tiene IPV6 y también con IPV4, es decir, se logró implmentar exitosamente el dual stack IPV4/IPV6.

Para el componente de servidores de NETSCALER se tiene lo siguiente:

Implementación IPV6 – NETSCALER

Descripción General

El presente plan de trabajo describe las actividades y el procedimiento para creación y migración de los servicios del cliente EPM de IPv4 a IPv6 esto con el fin de cumplir con los estándares estipulados por el gobierno para la prestación de servicios a entidades públicas y el cual no genera indisponibilidad sobre los servicios ya productivos publicados a través de la plataforma NETSCALER.

Resumen ejecutivo de las actividades

El procedimiento a nivel general incluye las siguientes actividades:

1. Validación política en CS servicios IPv4
2. Validación configuración CS en IPv4
3. Creación de Virtual Server en IPv6
4. Asociar Política de CS a Virtual Server de CS en IPv6
5. Asociar Certificados, políticas (Appflow o Responder), perfiles y parámetros SSL.

Descripción de las actividades

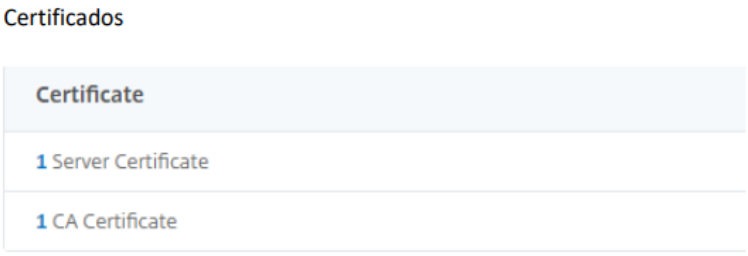
1. Validación política en CS servicios IPv4

Por medio de la Interface de administración de NetScaler (GUI) en la ubicación Traffic Management – Content Switching– Virtual Servers se realiza la validación de todas las políticas asignadas en el Content Switching de los servicios públicos con IPv4, esto con el fin de tener un inventario de las URL que están expuestas, tener un registro de que IPv4 está asignada a cada una de las URL's y enviar un reporte a los administradores de los DNS para poder realizar la nueva IPv6 a estas URL

2. Validación configuración CS en IPv4

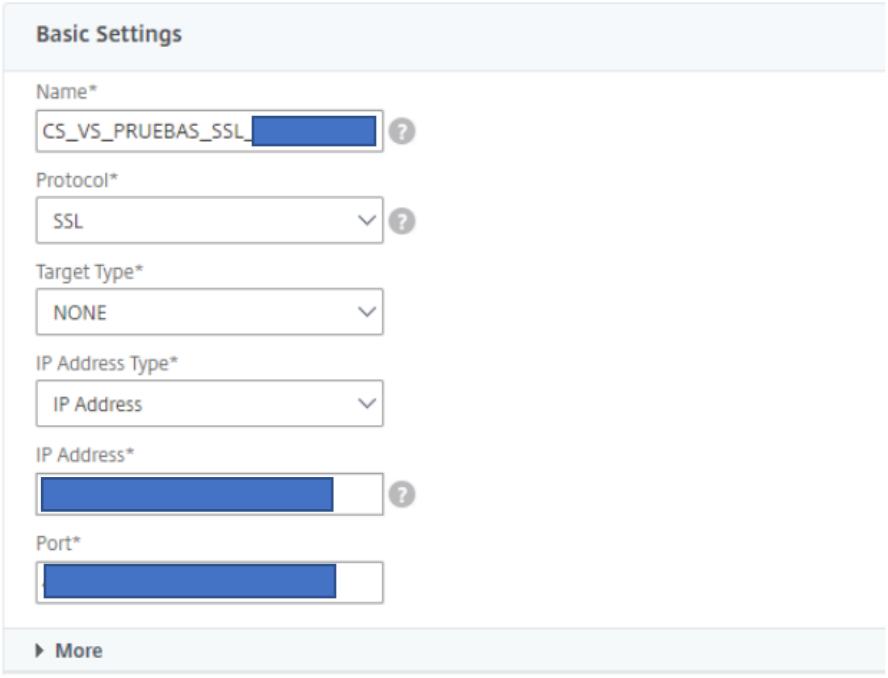
Por medio de la Interface de administración de NetScaler (GUI) se valida la configuración de: certificados, parámetros SSL, perfiles y políticas (responder o appflow) por cada uno de los Content Switching en la Ubicación Traffic Management – Load Balancing –Content Switching. Es necesario validar los parámetros de cada uno de los Content Switching para poder replicar la configuración al nuevo Content Switching con IPv6, para esto se valida parámetros como los siguientes:

[IMAGEN PARÁMETROS SSL Y PERFILES]



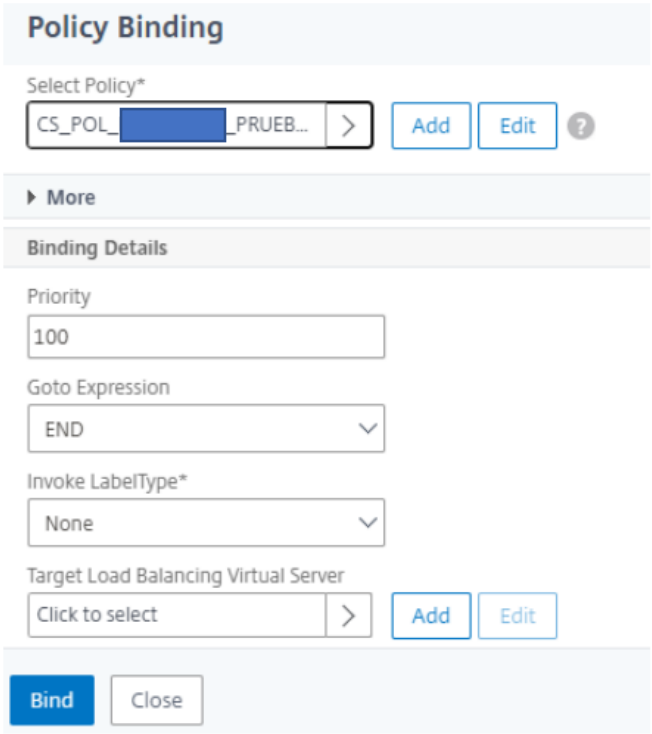
3. Creación de Virtual Server en IPv6

Por medio de la Interface de administración de NetScaler (GUI) se creará el virtual server en la Ubicación Traffic Management – Content Switching – Virtual Servers, seleccionar Add y especificar la información de Nombre, Protocolo y en la opción de IP Address Type se agrega la IPv6 deseada al Content Switching y se selecciona el puerto de acuerdo a la configuración necesitada (HTTP o SSL).



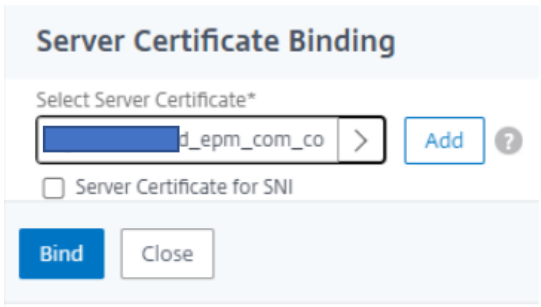
4. **Asociar Política de CS a Virtual Server de CS en IPv6**

Por medio de la interface de administración de Netscaler (GUI) se asociará la política de Content Switching IPv4 al virtual server de Content Switching IPv6 en la Ubicación Traffic Management – Content Switching – Virtual Server, Seleccionar el virtual server correspondiente y seleccionar Edit, Es necesario asociar la política que se encuentra creada en el Content Switching IPv4 respetando la prioridad que se encuentra configurada.

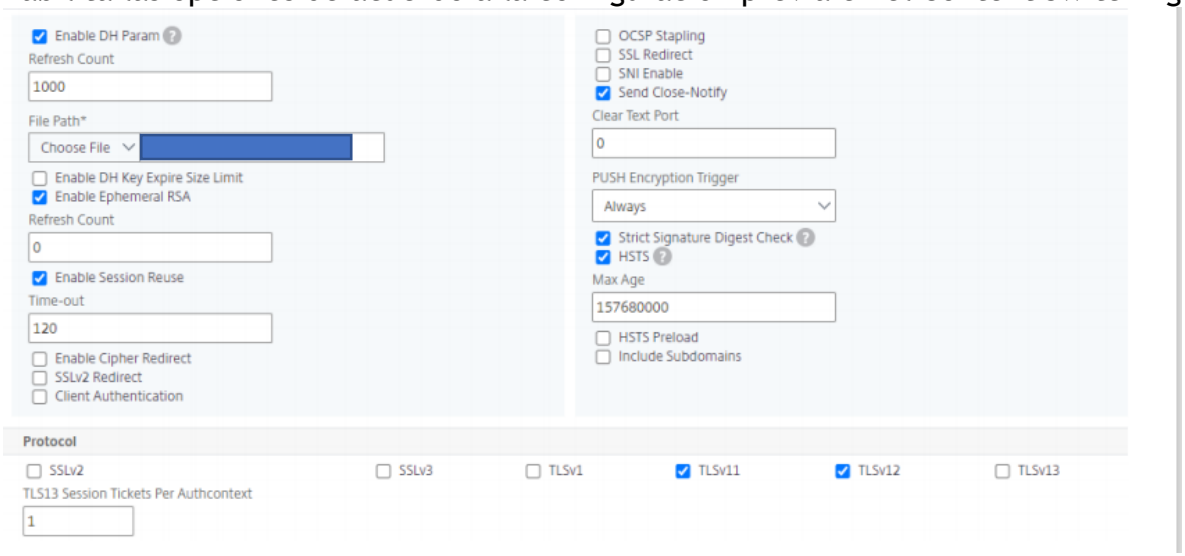


5. Asociar Certificados, políticas (Appflow o Responder), perfiles y parámetros SSL

Por medio de la Interface de administración de Netscaler (GUI) se realiza la asignación de certificado, políticas, perfiles y parámetros SSL en la Ubicación Traffic Management – Content Switching. Nota: Los parámetros antes dichos son para los protocolos SSL En la opción de Certifícate, se asigna los certificados ya sea el Server Certificate o el CA Certificate, asignando los mismos certificados que están configurados en el Content Switching de IPv4. Tanto en el Server como en el CA Certificate se da click en edit y se selecciona el certificado deseado, por último, se da click en bind para asociar el certificado al Content Switching en IPv6.

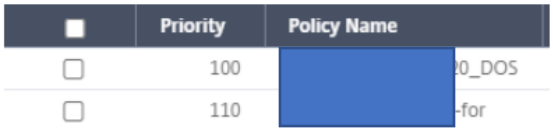


En la opción SSL Parameters, se realiza configuración de TLS, parámetros DH, etc. Se habilita las opciones de acuerdo a la configuración previa en el Content Switching en IPv4.



De igual manera en la opción de profiles y Policies, se da click en editar y se selecciona los perfiles y las políticas de acuerdo a la configuración que se encuentra en el Content Switching en IPv4.

Para el caso de las políticas, se asignará de acuerdo con la configuración en el Content Switching en IPv4, esta política corresponde a acciones de Responder o Appflow. De igual manera se asigna prioridad a estas políticas y se asignara al Content Switching



Se adjunta evidencia de todos los content switching creados con su respectiva IPV6

Servicios de Infraestructura de TI

Name	State	IP Address	Port	Protocol
CS_VS_PUB_EPM_SLL_IPV6	UP	[redacted]	[redacted]	SSL
CS_VS_PUB_HTTP_EPM_IPV6	UP			HTTP
CS_VS_PUB_HTTP_FIL_IPV6	UP			HTTP
CS_VS_EXT_FIL_SSL_IPV6	UP			SSL
CS_VS_SIRIUS_SSL_EPM_IPV6	UP			SSL
CS_VS_PUB_HTTPS_LYNC_IPV6	UP			SSL
CS_VS_PUB_HTTPS_FIL_IPV6	UP			SSL
CS_VS_EVM_HTTPS_IPV6	UP			SSL
CS_VS_EVM_HTTP_IPV6	UP			HTTP
CS_VS_EVM_SSL_IPV6	UP			SSL
CS_VS_PUB_SSL_UAT_DLLO_IPV6	UP			SSL
CS_VS_PUB_CAS_IPV6	UP			SSL
CS_VS_PUB_AFINIA_HTTPS_IPV6	UP			SSL
CS_VS_PUB_AFINIA_HTTP_IPV6	UP			HTTP
CS_VS_PUB_SSL_EPM_TLS_1.2_IPV6	UP			SSL
CS_VS_PUB_PROD_ESSA_HTTPS_IPV6	UP			SSL
CS_VS_PUB_PROD_ESSA_HTTP_IPV6	UP			HTTP
CS_VS_PUB_GRUPOEPM_HTTPS_IPV6	UP			SSL
CS_VS_PUB_GRUPOEPM_HTTP_IPV6	UP			HTTP
CS_VS_PUB_CENS_HTTPS_IPV6	UP			SSL
CS_VS_PUB_CENS_HTTP_IPV6	UP			HTTP
CS_VS_PUB_ESSA_HTTPS_IPV6	UP			SSL
CS_VS_PUB_CHEC_HTTPS_IPV6	UP			SSL
CS_VS_PUB_CHEC_HTTP_IPV6	UP			HTTP
CS_VS_PUB_EDEQ_HTTPS_IPV6	UP			SSL
CS_VS_PUB_EDEQ_HTTP_IPV6	UP			HTTP
CS_VS_PRUEBAS_SSL_EPM_IPV6	UP			SSL

Más información:

Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

5. COMPONENTE DE APLICACIÓN

A nivel de aplicaciones no se requirió realizar ninguna modificación o configuración especial sobre estas. La evidencia de su funcionamiento con IPV6 se muestra en el reporte de pruebas de aplicativos.

Más información:
Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co

6. CONCLUSIONES

- Se logró activar exitosamente y con mínimo impacto en la operación el doble stack IPV4-IPV6 en la DMZ y en ambas conexiones corporativas a Internet: TIGO y Century Link
- Se pudo implementar con éxito el protocolo IPv6 sobre los firewalls perimetrales.
- La publicación de las páginas y aplicaciones en IPv6 continuara realizándose a través del NetScaler al igual que los servicios que tenemos en protocolo IPv4.
- A nivel de firewall se crearon las políticas de manera específica en direcciones IPs y puertos para permitir la publicación de servicios en IPv6 de manera controlada.
- Los servicios de IPv4 continuaron funcionando correctamente cuando se activó el dual stack en los dispositivos de seguridad.
- No fue necesario realizar cambios en las aplicaciones para permitir su funcionamiento con IPV6
- Se requiere evaluar la habilitación de IPV4-IPV6 en los equipos terminadores de VPN para permitir el acceso a empleados y contratistas de EPM en aquellas situaciones en las que tengan conexiones IPV6 en sus casas o sitios de trabajo.
- Se continuará evaluando la posibilidad de permitir el acceso IPV6 a otros segmentos internos de la red de EPM para situaciones específicas que lo exijan.

Más información:
Teléfono: 380 5556 Fax: @ e-mail: uo9080@epm.com.co