Vicepresidencia Talento Humano y Tecnología > Dirección

Servicios de Infraestructura de TI

epm

PLAN DE IMPLEMENTACIÓN IPV6

EVALUACIÓN INFRAESTRUCTURA Y DIAGNÓSTICO DE LOS COMPONENTES DE TI

DIRECCIÓN DE SERVICIOS DE INFRAESTRUCTURA DE TI

EMPRESAS PÚBLICAS DE MEDELLÍN E.S.P.

Más información:

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

Grupo·epm

EVALUACIÓN INFRAESTRUCTURA Y DIAGNÓSTICO DE LOS COMPONENTES DE TI.

Introducción.

Cumpliendo con los objetivos de innovación tecnológica que exige el país y siguiendo los lineamientos del ministerio de las TIC (Tecnologías de la información y las comunicaciones) respecto a la adopción del protocolo IPV6 (descritos en la circular 002 del 6 de julio de 2011) Empresas Públicas de Medellín, en adelante EPM, aborda el proyecto de transición del protocolo IPV4 hacia el nuevo protocolo IPV6.

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.

Alcance

La adopción del protocolo IPV6 para EPM para esta etapa del proyecto no cubre:

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

1. La infraestructura de las redes operativas de los negocios (sistemas Scada, monitoreo y control Subestaciones y centrales) dado que están restringidas para acceso externo, son independientes de la red Corporativa y manejan sus propios esquemas de direccionamiento privado y controles de seguridad.
2. Las VPNs establecidas para las fronteras comerciales (Proyecto Código de la Medida).
3. Conexiones con operadores de telefonía celular (GPRS y M2M) dado que son de uso interno en la organización.
4. A nivel de seguridad informática no se tendrá en cuenta las VPNs Sitio a Sitio con proveedores o entidades bancarias y las VPNs Cliente a Sitio que permite la comunicación de los empleados y contratistas conectarse remotamente desde redes externas a la de EPM.

1. Diagnostico

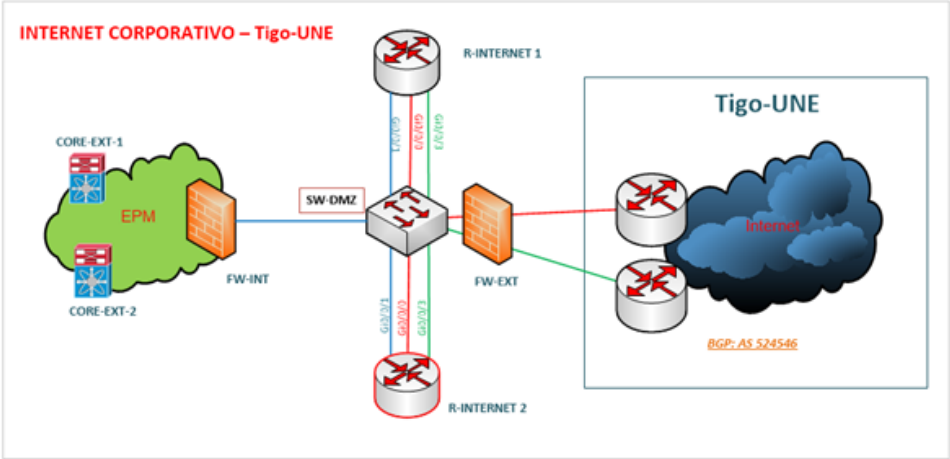
1.1 Topología de red del acceso a Internet Corporativo

Actualmente EPM cuenta con dos proveedores del servicio de Internet Corporativo: TIGO-UNE enlace principal de 1Gbps y Century Link con el enlace de respaldo también de 1 Gbps. Ambas conexiones se encuentran activas simultáneamente, mediante la asignación de la ruta de salida en los Servidores de Proxy se direcciona tráfico por ambos canales. Por la salida con TIGO-UNE se tiene habilitado el tráfico de todas las aplicaciones y servicios que publica y/o consume el Grupo EPM en Internet, para externos, usuarios y clientes en general, mediante la implementación del segmento DMZ, mientras que por el enlace de Century Link solo se habilita la navegación de grupos de usuarios internos y se usa como respaldo de la navegación.

Ambos canales de acceso corporativo a Internet son utilizados por el Grupo EPM (EPM, filiales de Aguas y filiales de Energía en Colombia)

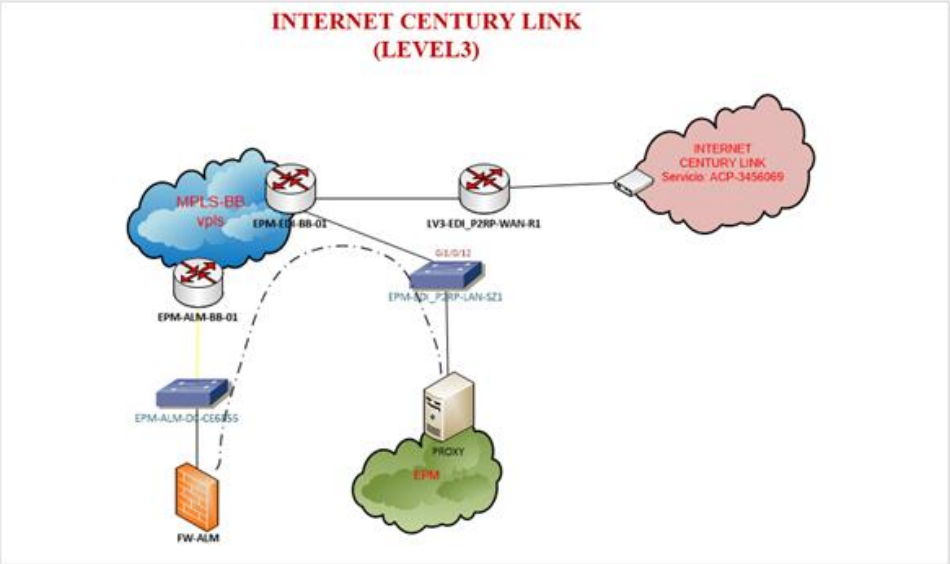
Para el requerimiento de implementar IPV6, la topología objetivo de análisis es la correspondiente a la salida a Internet con TIGO-UNE y obviamente el segmento DMZ. Para la salida con Century Link se contemplará la asignación de un segmento de IPv6 para continuar permitiendo la navegación de usuarios y la contingencia de este servicio.

La siguiente es la tipología de red de la salida a Internet con TIGO-UNE:



Grafica 1. Salida internet Tigo-UNE

A continuación, se muestra la topología de conexión para la salida por el enlace de Century Link.



Grafica 2. Salida internet Century-Lynk

Inventario de equipos de red

El inventario de equipos de red que soportan las salidas a Internet por TIGO_UNE y Century Link se relaciona en el archivo consolidado de inventario, anexo a este documento.

Diagnóstico equipos de red

Según el levantamiento de información y la validación con los fabricantes podemos confirmar que la totalidad de los equipos de la red de datos corporativa de EPM y particularmente, los que manejan el tráfico hacia y desde Internet a través de las conexiones

de TIGO-UNE (salida por el nodo del Edificio EPM) y Century Link (salida por el nodo Almacén), soportan el protocolo IPv6 (y pueden trabajar en modalidad “dual stack”) y no requieren actualización de firmware o sistema operativo, por lo cual es posible habilitarles este protocolo y funcionalidad cuando se requiera. No se tienen excepciones para los componentes de red.

Los equipos Cisco, desde la versión de sistema 12.0S (año 2005) soporta IPv6 (https://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/by-feature-technology.jsp) y los equipos Huawei se puede verificar su compatibilidad IPv6 a través del Link http://support.huawei.com/onlinetoolweb/sqt/index?domain=0&lang=en

Plataforma de gestión de la red

Las plataformas de gestión de la red eSight (versión V300R009C00SPC200) y U2000 (Versión V200R016C50SPC201) desde las cuales de gestiona y opera la red de datos del Grupo EPM, en sus versiones actuales ***NO*** soportan IPv6. Sin embargo, para el alcance de esta implementación de IPv6, no es necesario actualizarlas ya que los equipos de red se continuarán gestionando con IPv4. Adicionalmente, estas plataformas de gestión son para uso interno y exclusivo del equipo de gestión y operación de la red –NOC- y no tienen salida directa a Internet.

1.2 Diagnóstico componente de servidores

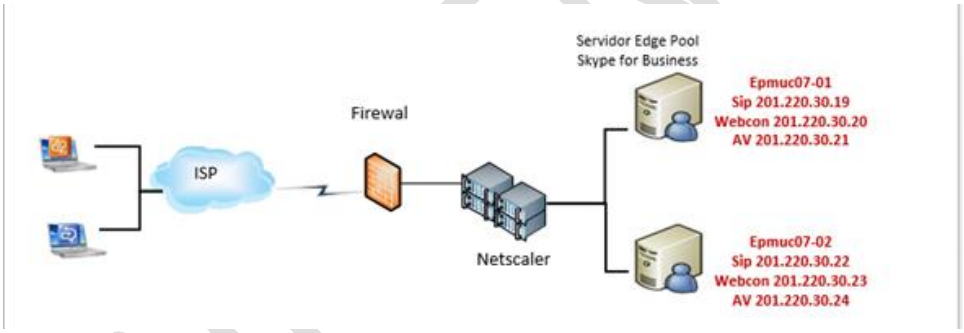
1.2.1 Topología Solución Comunicaciones Unificadas y servicios de colaboración Corporativos

La plataforma de comunicaciones unificadas que utiliza el Grupo EPM tiene únicamente dos (2) servidores expuestos a Internet (Epmuc07-01 y Epmuc07-02) resaltados en la

gráfica anexa que gestionan todas las comunicaciones y servicios que requiere la solución desde y hacia Internet.

La versión del sistema operativo de estos 2 servidores es Windows Server 2012 y la aplicación de Skype Empresarial para Office 365 (versión actual 16.0.11328.20362) soporta IPv6 dual Stack.

La siguiente es la topología de la solución proxy para comunicaciones unificadas



Grafica 3. Solución de comunicaciones Unificadas.

Se anexa el diagrama general detallado de la solución,

Poster CU EPM 2019.jpg

1.2.2 Solución para la resolución de nombres de dominio -DNS

Esta solución se compone de los siguientes elementos:

POSEIDON: Poseidón es un servidor Linux Red Hat Enterprise 7.5, el rol que cumple en EPM es ser el servidor DNS público, la función del DNS público es un servidor de computadora que contiene una base de datos de direcciones IP públicas y sus nombres de host asociados, y en la mayoría de los casos sirve para resolver o traducir esos nombres a direcciones IP según lo solicitado. Este servidor se encuentra preparado para la adopción de IPV6

PERSEO: Perseo es un servidor Linux Red Hat Enterprise 7.5, el rol que cumple en EPM es ser el servidor DNS publico secundario, En la mayoría de los casos, un servidor DNS primario y uno secundario están configurados en su enrutador y / o computadora cuando está conectado a su proveedor de servicios de Internet (ISP). Hay dos servidores DNS en caso de que uno de ellos falle, en cuyo caso el segundo se usa para resolver los nombres de host que ingrese. Este servidor se encuentra preparado para la adopción de IPV6.

WAP Servers: En general, WAP en EPM proporciona la funcionalidad de proxy inverso para aplicaciones web en la red corporativa que permite a los usuarios en la mayoría de los dispositivos acceder a aplicaciones web internas desde redes externas. En EPM se tiene este servicio en alta disponibilidad en 2 nodos, los nombres de los servidores son epmws02-01 y epmws02-02, ambos servidores tienen sistema operativo Windows server 2016 estándar y estos servidores están alojados en la DMZ.

La siguiente topología corresponde al acceso de aplicaciones y servicios publicados en Internet

Grafica 4. Servidores DNS - Servidores de nombres de dominio.

La siguiente grafica representa la solución servicios de federación de Directorio Activo - ADFS- Proxy web de aplicaciones – WAP

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

Grafica 5. Solución ADFS-WAP

1.3 Diagnóstico componente de Seguridad

1.3.1 Topología esquemas y controles de seguridad para el acceso a Internet y Nube.

Los equipos de seguridad que intervienen para la configuración de Dual Stack (IPv4/IPv6) son los siguientes:

- Firewall Externo

Es un clúster de firewall marca Check Point modelos 12400, están configurados en alta disponibilidad en modo Activo-Activo, se encuentran en la versión de software R77.30. En el levantamiento de información se evidenció que es necesario ejecutar una actualización a la versión R80.20 para cumplir con los requerimientos de configuración de IPv6 en dual stack.

Al activar IPv6 en los equipos Check Point aumenta un 30% la carga en recursos de máquina. Actualmente este dispositivo tiene un consumo alto de CPU y memoria, por ende, con apoyo del fabricante y del proveedor se está realizando un análisis de rendimiento al equipo con el fin de ejecutar la actualización que mejor se ajuste al procesamiento del firewall.

Para dar cumplimiento al cronograma de actividades plateadas en el proyecto, se cuenta con un Firewall de contingencia con las mismas especificaciones técnicas del Firewall Externo productivo, para realizar las pruebas que concluyen el entregable.

A continuación, se muestran que en los firewalls externos con referencias 12400 del fabricante Check Point cuentan con la configuración para IPV6

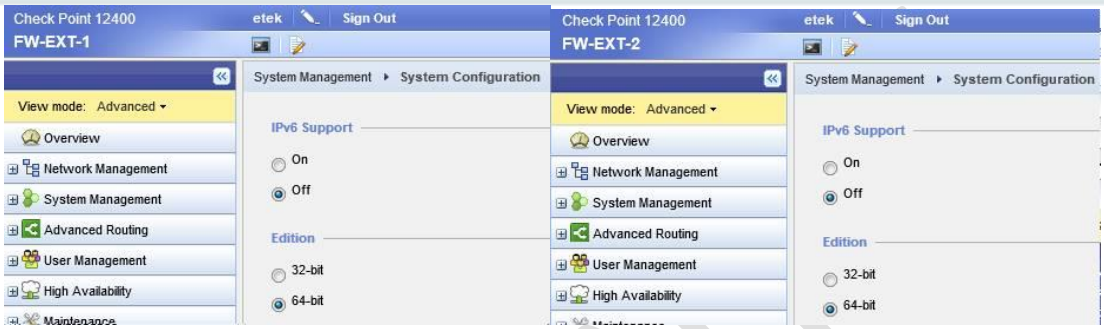


Imagen 1. Verificación del protocolo IPV6 en los Firewall.

- Firewall Almacén

Es un clúster de firewall VSX marca Check Point modelos 15400, están configurados en alta disponibilidad en modo Activo-Pasivo, se encuentran en la versión de software R80.10. En el levantamiento de información se evidenció que es necesario ejecutar una actualización a la versión R80.20 para cumplir con los requerimientos de configuración de IPv6 en dual stack.

- Nube Azure

Actualmente Microsoft en el enunciado publicado el 14 de Julio, informa que para Azure Virtual Network se encuentra actualmente en versión preliminar pública. Esta vista previa se proporciona sin un acuerdo de nivel de servicio y no se recomienda para cargas de trabajo en producción. Ciertas características pueden no ser compatibles o tener capacidades limitadas.

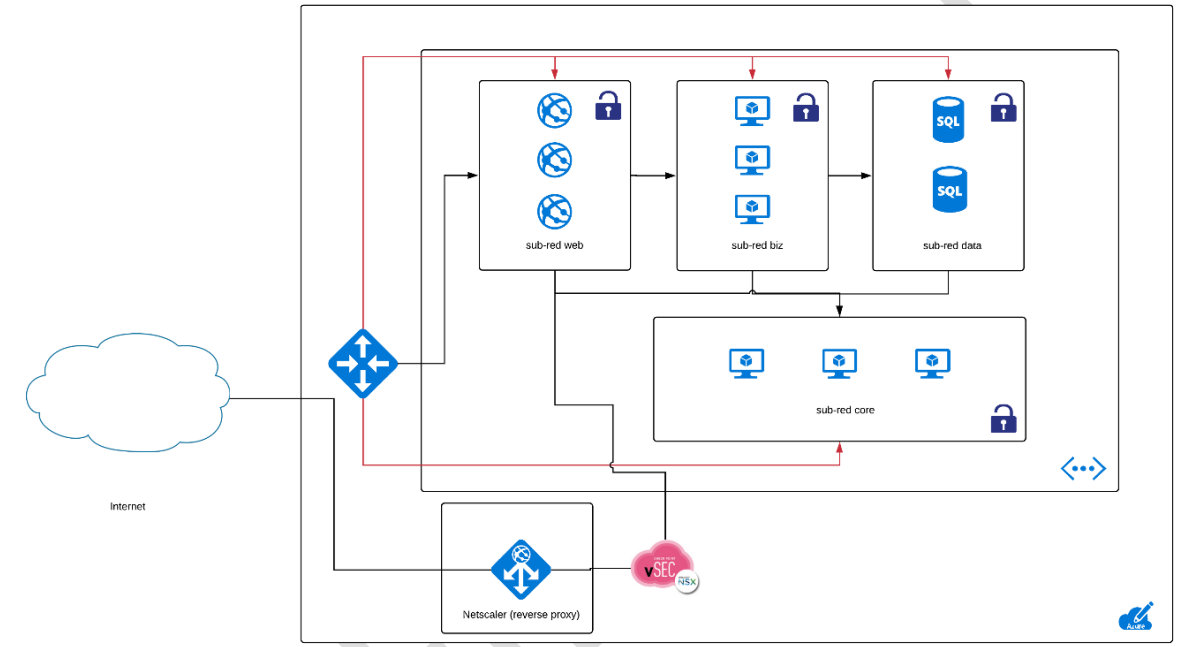
La versión preliminar de IPv6 para la red virtual de Azure tiene las siguientes limitaciones:

- IPv6 para la red virtual de Azure (Vista previa) está disponible en todas las regiones globales de Azure, pero solo en Global Azure, no en las nubes gubernamentales.
- El soporte del portal para componentes de Standard Load Balancer es de solo lectura. Sin embargo, el soporte completo y la documentación (con ejemplos) están disponibles para implementaciones de Standard Load Balancer con Azure Powershell e interfaz de línea de comandos (CLI).
- El soporte de Network Watcher para la vista previa está limitado a registros de flujo NSG y capturas de paquetes de red.
- El emparejamiento de red virtual (regional o global) no se admite en la vista previa.
- Cuando se usa el equilibrador de carga externo estándar IPv6, se aplican los siguientes límites:

  - Las reglas de salida pueden hacer referencia a múltiples IP públicas front-end, pero no pueden hacer referencia a un prefijo público IPv6. El prefijo público IP solo admite prefijos IPv4.
  - Las reglas de equilibrio de carga de IPv6 no pueden usar la función de IP flotante. La reutilización de puertos en instancias de back-end solo es compatible con IPv4.
  - La función de prefijo de dirección IP pública de Azure no admite la reserva de un bloque de direcciones IPv6 con conexión a Internet.

A continuación, la gráfica del esquema de red en Microsoft Azure

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



Grafica 6. Solución Microsoft Azure.

La siguiente grafica muestra la topología general de la DMZ y sus diferentes componentes:

Grafica 6. Solución Microsoft Azure.

1.4 Diagnóstico componente aplicaciones

1.4.1 Componente Aplicaciones en Internet

El grupo EPM tiene un número significativo de sitios web publicados en internet. En el levantamiento de información se realizó el análisis previo para la revisión de cada uno de los sitios y servicios que se tienen publicados y se identificó que no presentan inconvenientes con las IP's configuradas a nivel de código. De esta manera cumple para la implementación de IPV6 en el dispositivo en el que se publican, para el caso del balanceador Netscaler.

Cabe recomendar que se presentan algunos sitios expuestos con servicios internos en los cuales hay que revisar, al igual que las aplicaciones internas.

Se recomienda realizar las pruebas con el UAT de factura web, este esquema o panorama depende de los equipos para conformar un ambiente de pruebas.

Los equipos que intervienen: Servidor DNS, Netscaler, Firewall y el segmento en IPV6 asignado según diseño entregado por Huawei.

Se adjunta el documento en la carpeta de documentos." *Análisis de sitios publicados en Netscaler"*

Analisis de Sitios publicados NetScale

Inventarios Aplicaciones V 2.xls›

Inventario general de hardware, software y aplicaciones

En el siguiente documento de Excel se detalla el inventario de equipos por componente, que están involucrados en la implantación del dual stack de IPv6

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

Vicepresidencia Talento Humano y Tecnología > Dirección

Servicios de Infraestructura de TI

Inventarios Aplicaciones V 2.xls›

Más información:

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

Grupo·epm