OSPF sobre VPN L2TP/IPSec &WANS Dinámicas

Caso de estudio, sobre implementación en República Dominicana

PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

Exponente

Jose Ml Perez

MTCRE, MTCWE, MTCTCE, MTCUME, MTCIPv6E, MTCINE

Santo Domingo, **Dominican Republic**

OSPF, static routing, WAN load balancing & failover, advanced tunneling, PPP and VPN, bandwidth management and control, advanced QoS for protocols optimization and ISP and WISP bandwidth plans management , HTB, HotSpot with centralized or distributed user control, advanced firewall with added security and network control, distributed indoor wireless implementations for offices and homes, outdoor Wireless interconnections, PtP, PtMP, MESH, wireless security, advanced radius management & integration, local or network bridging, remote offices interconnection, segmentation, security & authentication, network monitoring, flow analysis and advanced troubleshooting, web proxy and advanced cache caching, UTM development, DNS, IPv6 integration, transmission and security. Available for On-Site and Remote Support.

PGA

TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

JMPerez@PGA.com.do
+1-809-878-9879

mum

Mikrotik User Meeting

Objetivo de esta presentación:

- Exponer el caso de implementación donde interconectamos 32 sucursales remotas hacia la sucursal principal de la empresa vía VPN.
- Implementación de OSPF sobre los túneles para la propagación de las redes de las sucursales, permitiendo acceder a los servicios internos actuales y futuros desde cualesquiera de las localidades

PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

Objetivo de esta presentación:

- Centralización de los servicios de telefonía, servidores de aplicaciones y CRM en la sucursal principal.
- Live demo sobre implementación
  - Detalles de router de borde.
  - Detalles routers de borde en sucursales.
  - Comportamiento de implementación y protocolo OSPF con WAN's dinámicas
- Ventajas y desventajas de la implementación

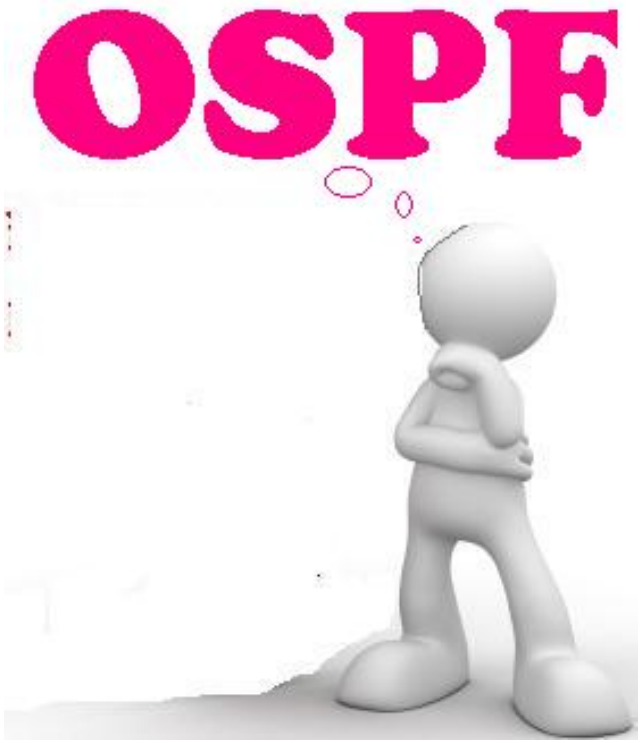
PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

Limitaciones de la presentacion

- Non-disclosure agreement (NDA)
  - Al inicio del proyecto firmamos un acuerdo de confidencialidad. Por lo que los detalles específicos de la instalación del cliente serán omitidos
  - No obstante si trataremos los detalles de cómo realizar estas implementaciones a nivel general.

¿Qué es OSPF?



PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

¿Que es el protocolo OSPF?

- Open Shortest Path First (OSPF) es un protocolo de la familia de los protocolos de estado de enlace (link state protocolos) desarrollado en la década del 1980 por el equipo de trabajo de la IETF.
- Al configurarlo, el protocolo escuchara a sus routers vecinos y obtendrá toda la información de los estados de sus enlaces; para así, armar un mapa de topología de todos los enlaces de la red.
- Grabara toda esta información en su base de datos de topología, llamada Link-State Database (LSDB)

¿Como funciona OSPF?

- Con la información de la base de datos de la topología, el protocolo calculara la mejor y mas corta ruta (Shorted Path First – SPF) para cada red aprendida.
- Para lograr esto utiliza el algoritmo de Dijkstra, creado por Edsger W. Dijkstra en1956. Luego de efectuado el cálculo, OSFP construirá 3 tablas:

¿Como funciona OSPF?

- **Neighbor Table:** contiene a todos los routers con OSFP vecinos con los que intercambiara información de enrutamiento.
- **Topology Table:** posee todo el mapa de la red, con la información de los routers OSPF y el calculo de las mejores rutas directas y alternas.
- **Routing Table:** contiene las mejores rutas encontradas para el reenvío de trafico entre los routers vecinos.

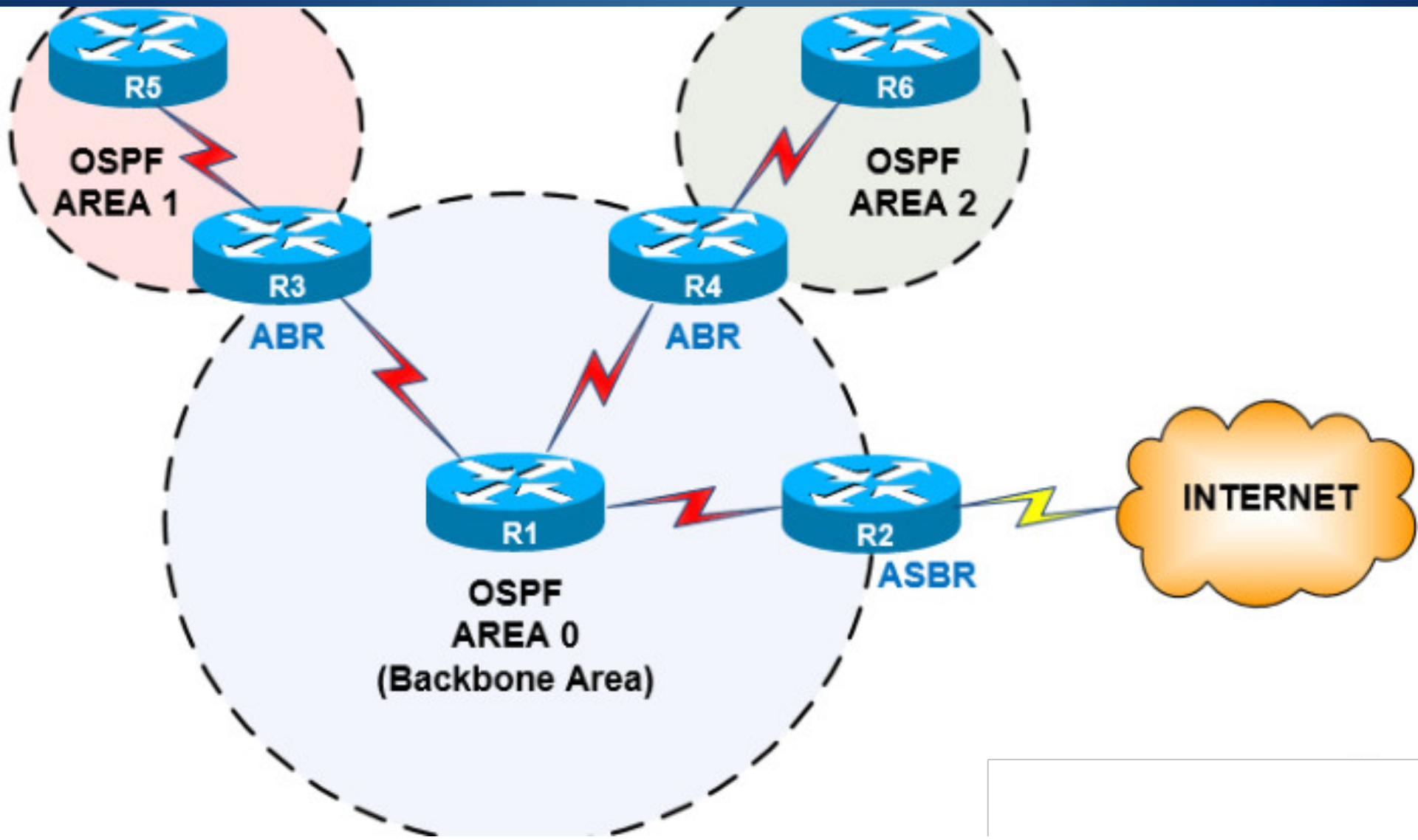
Areas de OSPF

- Una de las principales funciones de OSPF es que nos permite dividir los routers en **Áreas de enrutamiento.** Cada una de estas áreas consiste en un grupo de routers interconectados entre si.

- Al segmentar en áreas simplificamos la administración y optimizamos los recursos, sobretodo cuando tenemos redes grandes y evitamos que las actualizaciones de estado de los enlaces saturen la red.

Areas de OSPF

- Las áreas corresponden a colecciones lógicas de routers que comparten el mismo **“Area ID”** dentro de la red OSPF.
- La primera area y al mismo tiempo la principal es llamada **“Area 0”** o **“Backbone”** las demás áreas deben estar conectadas al área 0



PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

Areas de OSPF

- El objetivo de tener un área es organizar la red de la siguiente manera:
- **Sumarización de redes: y**a que no es posible resumir los prefijos de red porque se asume que todos los routes tienen la misma topología de mapa de red para coincidir con sus vecinos.
- **Reducción de actualizaciones:** al producirse una actualización dentro de un área esta no es replicada a toda la red OSPF, optimizando el uso de recursos dentro la red completa

OSPF Link Packet States

- Los routers OSPF generan paquetes de información que con compartidos con sus routers vecinos. Por medio de estos paquetes formamos las relaciones entre routers adyacentes, calculamos el mejor costo y la mejor ruta para acceder entre las redes
- Sobre estos tipos de paquetes tenemos:

OSPF Link Packet States

- **Link State Advertisement (LSA):** es el principal medio de comunicación entre los routers OSPF, es el paquete que contiene toda la información fundamental sobre la topología y está inundado entre áreas para realizar diferentes funciones

- **Link State DataBase (LSDB):** contiene la información actualizada del estado de los enlaces intercambiados de la red, y todos los enrutadores dentro de la misma área tienen LSDB idéntico. Además cuando dos routers forman una nueva adyacencia, sincronizan su LSDB para ser completamente adyacentes

- **Link State Request (LSR):** una vez realizada la adyacencia entre los routers e intercambiados los LSDB. Los routers vecinos pueden localizar la información de su base de datos de topología faltante (LSDB), para luego enviar un paquete de actualización a sus vecinos. Estos lo reciben y le responden con la actualización (LSU)

OSPF Link Packet States

- **Link State Update (LSU):** es un paquete de respuesta que envía una pieza específica de información LSDB solicitada por un router vecino a través del paquete LSR .
- **Link State Acknowledgment (LSAcK):** el routerque envía el paquete LSR confirma que recibe la LSU del vecino enviando un paquete de confirmación que reconoce que recibió las LSU solicitadas.

Tipos de Routers OSPF

- **Area Boarder Routers (ABR):** se encuentran en los perímetros de área dentro de la topología de OSPF. Se encargan de sumarizar o resumir las direcciones IP de cada área; así como también suprimir las actualizaciones entre áreas evitando la contención de fallas.

- **Autonomous System Boundary Router (ASBR) y Backbone Router:** es el router que conectadas a una o más áreas OSPF, parecido al **ABR**, pero se conecta a otros sistemas como BGP, EIGRP, Internet y otros. Generalmente el ASBR, anuncia rutas desde otros sistemas al área OSPF a la que pertenece.

Tipos de Routers OSPF

- **Designated Router (DR):** el router DR al ser elegido, es el responsable de mantener la tabla de topología para el segmento o area que pertenece. El DR tiene 2 principales funciones:
  - Llegar a ser adyacente en todos los demás routers del segmento de red.
  - Actuar como portavoz de la red (generando los SLA)

Tipos de Routers OSPF

- **Backup Designated Router (BDR):** este router se convierte en DR si falla la DR existente. El BDR tiene la segunda prioridad más alta (el DR primario es quien tiene la prioridad más alta) en la red OSPF. Cuando el BDR se convierte en DR , se realizan nuevas elecciones para encontrar un nuevo BDR .

VPN

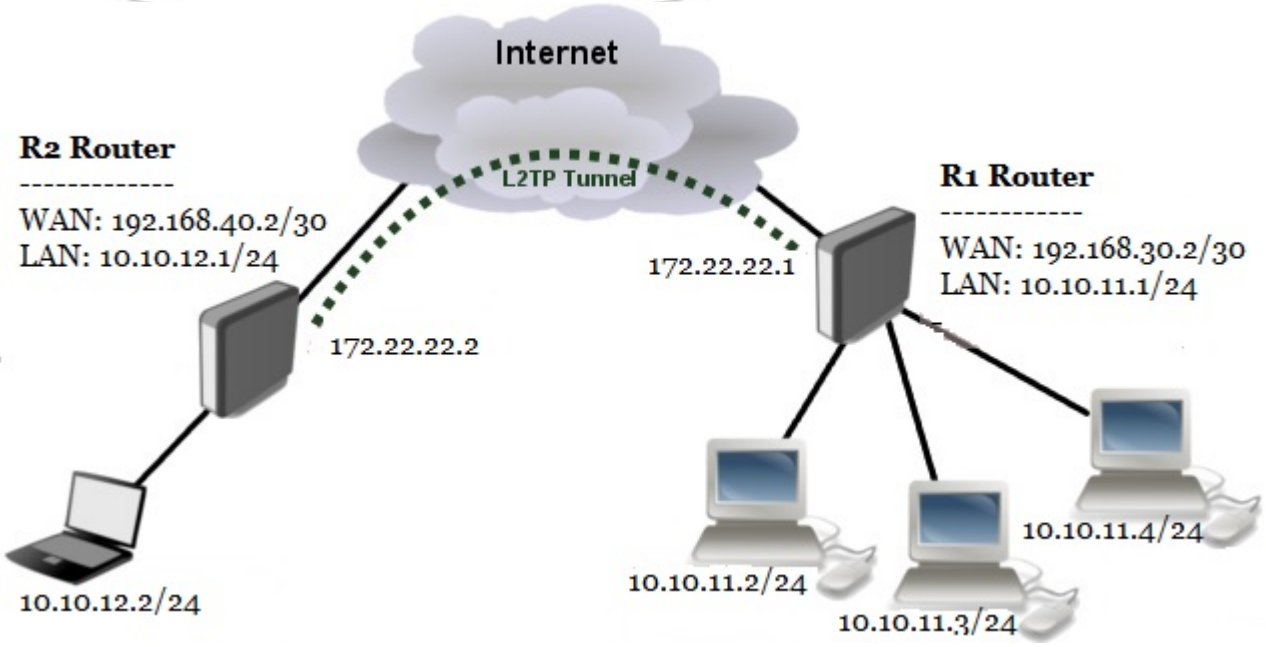
PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

¿Qué es un VPN?

- VPN son las siglas de “Virtual Private Network” o red privada virtual. Esta proporciona la misma conectividad de red para usuarios remotos a través de una infraestructura pública.
- Una red VPN ofrece lo siguiente:
  - Confidencialidad
  - Integridad de los datos
  - Autenticación

¿Qué es un VPN?



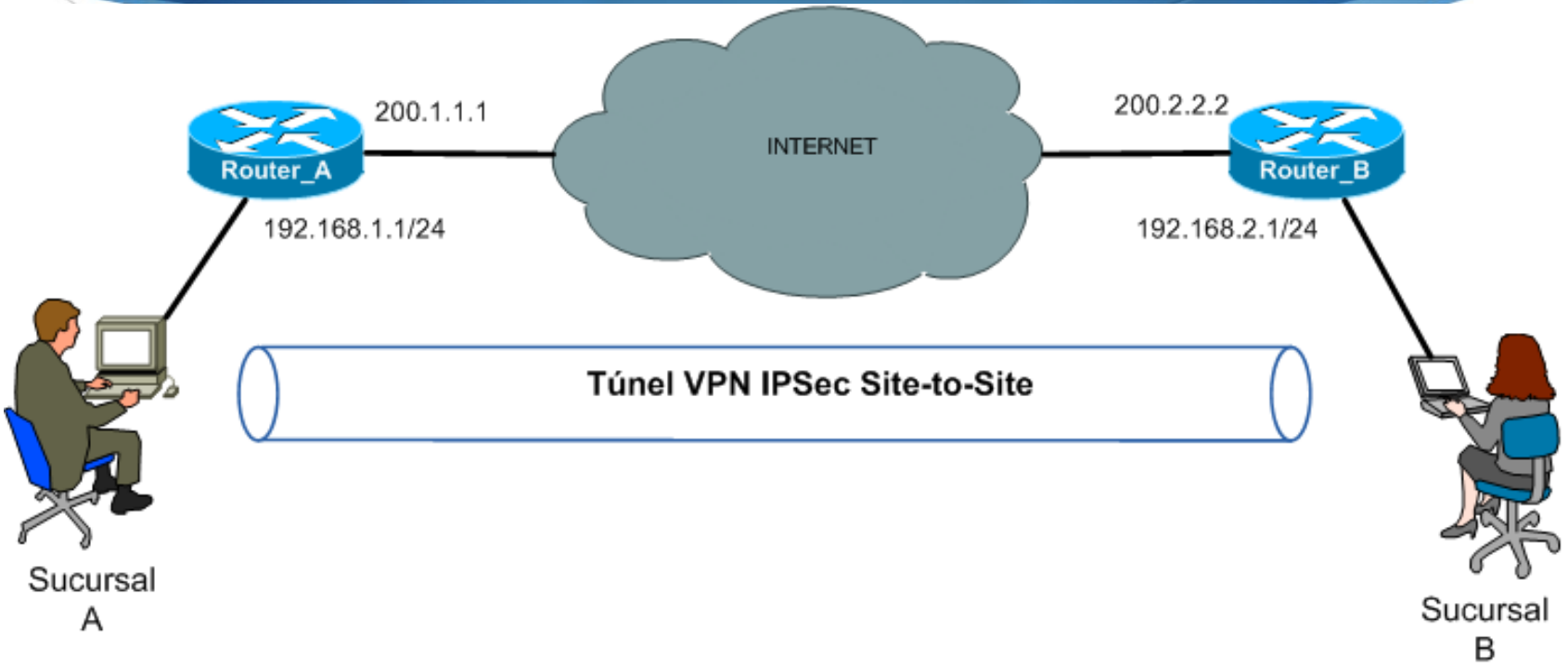
PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

MUM
Mikrotik User Meeting

Tipos de VPN

- **VPN Site to Site:** se utilizan principalmente para enlazar 2 o mas sucursales remotas a través de un medio compartido (internet). Los usuarios de ambas sucursales podrán establecer conectividad end to end a través del túnel

VPN Site to Site



PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum
Mikrotik User Meeting

Tipos de VPN

- **VPN Client to Site (Road Warrior):** es comúnmente utilizada por los usuarios que necesitan trabajar de manera remota y utilizar los servicios y sistemas dentro de la empresa.

VPN Client to Site

L2TP VPN/IPSec

- **Layer 2 Tunneling Protocol (L2TP):** es un tipo de túnel resultado de una asociación entre Cisco y Microsoft.
- Fue creado para proporcionar un protocolo VPN más rapido y seguro que PPTP.
- L2TP es un protocolo de túnel que permite a los usuarios acceder a una red de forma remota. Posee todas las características de PPTP, pero se ejecuta sobre un protocolo de transporte más rápido (UDP).Pero no posee encriptación de manera nativa.

IPSec

- **Internet Protocol security:** es un conjunto de es un cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

- IPsec trabaja en la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa 7 . Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP.

L2TP & IPSec

- Al implementar un túnel VPN utilizando L2TP & IPSec, buscamos, lograr un túnel rápido, al mismo tiempo que ciframos los datos al momento de ser transmitidos por el túnel.

Caso de Estudio

- Obtuvimos un lead de un cliente, cual necesitaba interconectar sus 32 oficinas remotas hacia su sucursal principal.
- Poder compartir recursos como su software CRM.
- Recortar los gastos de telecomunicaciones en cuanto a telefonía y conectividad cuales rondaban los **RD$380,000 ~ US$7, 775**

PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

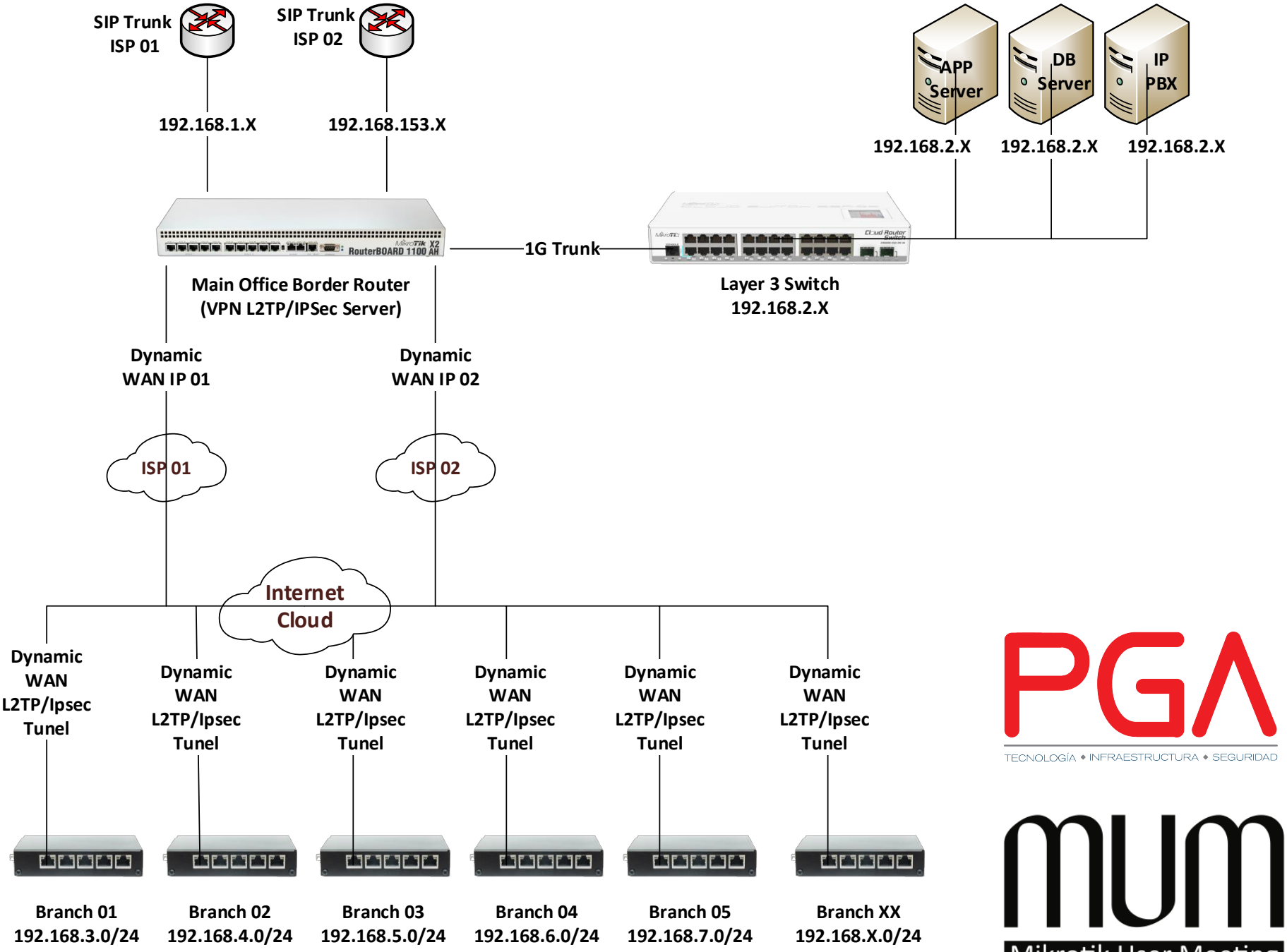
mum
Mikrotik User Meeting

Caso de Estudio

- Realizamos los levantamientos en sus localidades y trabajamos con los ISP's para confirmar cual podía ser el mejor escenario aplicable a la infraestructura y necesidades del cliente.
- Sobre los detalles tenemos:

PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

MUM
Mikrotik User Meeting



PGA

TECNOLOGÍA • INFRAESTRUCTURA • SEGURIDAD

mum

Mikrotik User Meeting

Live Demo Implementación

PGA

TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

mum

Mikrotik User Meeting

Ventajas

- Interconexión de todas las sucursales del cliente, para acceso a servicios de VoIP, aplicaciones comunes y CRM. Donde solo tenemos el "trafico interesante" pasando por el túnel. Todas las comunicaciones que no correspondan al túnel salen por el gateway local de cada sucursal.
- Segmentación de las redes entre sucursales
- Implementación de políticas de filtrado de contenido en todas las localidades, por medio del servicio de **FlashStart** attachado directamente a los routers Mikrotik
- Reducción de costos en un **+80%** (Facturación mensual en servicios de telecomunicaciones descendió a: **RD$74,500 ~ USD1,520**)

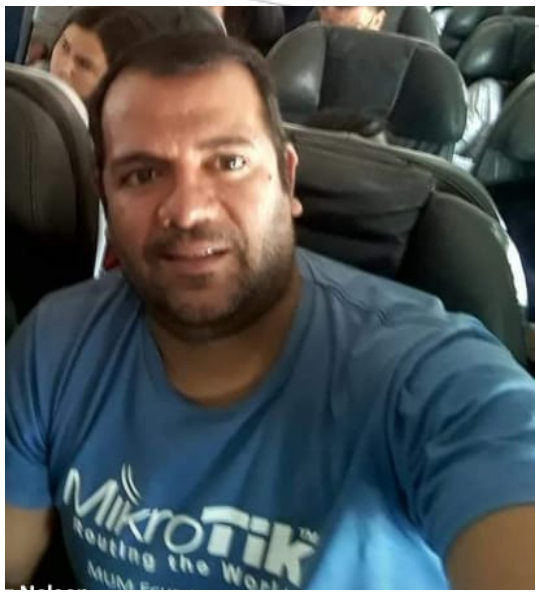
PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

MUM
Mikrotik User Meeting

Desventajas

- Como las interfaces WAN son todas dinámicas, estamos expuestos a muchos SLA. Esto cuando cambian las WANS de los clientes y se restablecen los túneles. **
- Implementación de políticas de NAT en la IP PBX, para permitir el trafico de los túneles directo a la central.**
- Perdida de comunicaciones en las sucursales ante una avería del ISP que la supla

Agradecimiento Especial



Nelson López
Trainer Mikrotik
Certinet Venezuela

PGA
TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

MUM
Mikrotik User Meeting

!Gracias!

PGA

TECNOLOGÍA ◆ INFRAESTRUCTURA ◆ SEGURIDAD

pgacomdo | pga.com.do | info@pga.com.do

MUM
Mikrotik User Meeting