

Evolución de arquitectura y servicios

GORE-17

Agenda

1. Nueva Red de Servicios
2. Nueva Red de Gestión
3. Securización de servicios
4. Evolución de la Red de Conmutación
5. Nuevos route-servers
6. Blackhole de tráfico
7. Blackhole de DNS
8. En proceso...

Nueva Red de Servicios

- Nueva red de servicios donde se aíslan todos los servidores de Espanix
 - Aislada de la red de switching.
 - Aunciada dentro del AS de Espanix.
 - Filtros de acceso y seguridad.
 - Todo con IPv6.
 - Nuevos servidores:
 - Ticketing
 - Monitorización de red
 - Estadísticas
 - Correo y listas
 - Nueva web (en desarrollo)

Nueva Red de Gestión

- Red de gestión totalmente aislada
 - No “rutable”.
 - Total separación de tráfico de gestión y de servicio en servidores y switches.
 - Totalmente redundante incluyendo PARs.
 - Acceso a consolas y puertos de administración.
 - Gestión.
 - Monitorización.
 - Toma de datos.

Securización de los Servicios

- Actualización de los DNS.
 - Resolución directa e inversa de todas las direcciones de red.
 - DNSSEC en dominios directos e inversos.
- Actualización del correo y listas
 - Validación estricta de los correos entrantes.
 - SPF, DKIM, DMARC, DANE.
- HTTPS en todos los servidores.

Evolución de la Red de Conmutación

- Abandono de los 100Mbps.
- Introducción de los 100Gbps.
- Nuevo PAR en Madrid (Alcobendas).
- Regularización de los controles en los puertos.
 - Desactivado de protocolos innecesarios.
 - Filtrado de tráfico indebido.
 - Protecciones de nivel 2 (tormentas y bucles).
- Monitorización de tráfico no esperado.
 - Excesivos “broadcast”
 - Protocolos de routing interno (OSPF, EIGRP, IS-IS).
 - Protocolos de distribución de multicast (PIM).
 - Protocolos de descubrimiento (CDP, MNDP).
 - Protocolos de gestión remota (MOC).

Nuevos route-servers

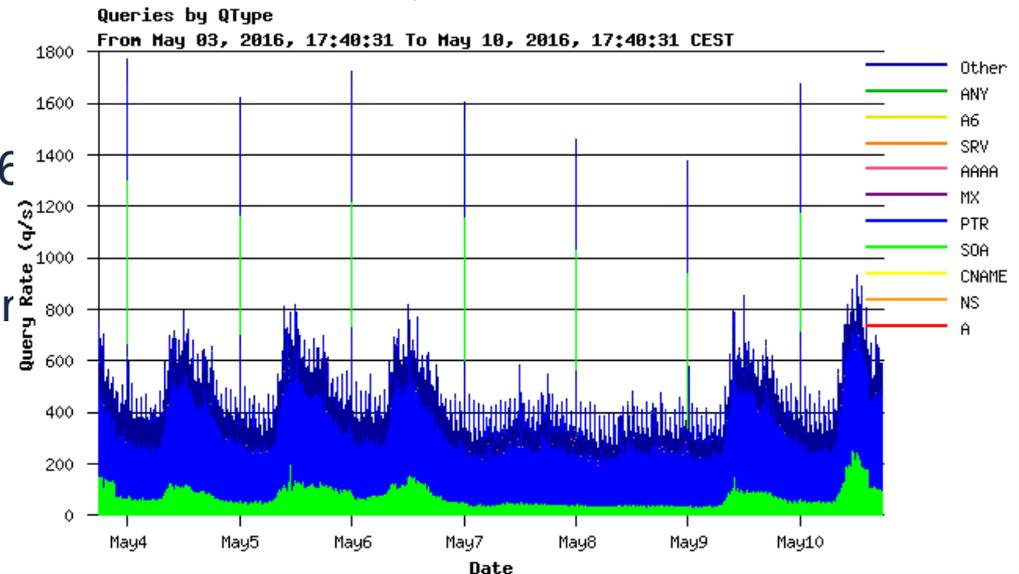
- Mayor capacidad y rendimiento.
- Mayor flexibilidad de configuración.
- Filtrado de redes “bogon”.
- Posibilidad de control de anuncios basándose en communities.
- Interpretado de la community de blackholing.
 - Basta con marcar la ruta con la community de blackholing (65535:666)
 - El route-server enviará los anuncios con el next-hop adecuado.
 - Se puede combinar con el control de anuncios para mitigaciones controladas.

Blackhole de tráfico

- Implementación de blackhole de tráfico tanto para IPv4 como IPv6.
- Los route-servers se encargan de las modificaciones necesarias.
- También disponible para conexiones BGP directas simplemente cambiando el next-hop en el BGP.
- Implementado en la tabla de forwarding de los switches, sin filtros ni ACLs.
- Máximo rendimiento y sin posibilidad de errores de configuración en puertos.
- Espanix anuncia permanentemente 2 prefijos como `blackhole.espanix.net` para pruebas.

Blackhole de DNS (AS112)

- Terminación del tráfico DNS que no debería salir a la Internet pública.
- Dynamic DNS updates
- PTRs de RFC1918
- Destacan las empresas (entrada al trabajo) y los scripts (horarios y diarios).
- Se anuncia tras el AS de
- Disponible en IPv4 e IPv6
- Estadísticas públicas
<http://as112.espanix.r>



En progreso...

- Nueva web, con área de servicio a clientes (solicitudes, cambios, monitorización, informes...)
- Verificaciones en route-servers basadas en registros de routing
 - Verificación de origen
 - Verificación de políticas de encaminamiento
- Control de MACs en puertos de los conmutadores.
- Notificaciones proactivas de tráfico anómalo.
- Panel de control de estado de interfaces y ópticas.
- Obtención de la matriz de tráfico.

Gracias por su atención

<http://www.espanix.net>