Renovar Internet

1. Antecedentes: a pesar de la rápida adopción y el amplio despliegue de Internet para convertirse en la infraestructura de comunicación mundial de facto, siempre ha existido una preocupación persistente sobre su vulnerabilidad a la violación de la seguridad. Es decir, en comparación con la PSTN tradicional capaz de localizar a la persona que llama incluso antes de que se responda una llamada, ¿por qué Internet tarda tanto tiempo, días, meses o incluso más, para comenzar a especular sobre el perpetrador de un gran ataque cibernético?

La causa de este problema radica en el hecho de que el diseño original de Internet basado en IPv4 no tenía un conjunto de direcciones lo suficientemente grande como para identificar de forma explícita y única todos los IoT que se utilizan. Se desarrollaron varios planes provisionales para hacer frente dinámicamente a esta desventaja. Desafortunadamente, también proporcionaron el camuflaje perfecto para los perpetradores, mientras que los usuarios comunes eran patos sentados al aire libre. Aunque la nueva versión, IPv6 tiene direcciones más que suficientes para identificar todos los IoT, de alguna manera persistió el uso de los esquemas provisionales. Además, IPv6 es más complicado y costoso que IPv4, lo que dificulta que las regiones menos afortunadas adopten IPv6. Un reemplazo completo para cualquier sistema grande de uso continuo como Internet está fuera de discusión. Para sortear este punto muerto, un esquema que pueda coexistir con las prácticas actuales mientras las mejora hacia un sistema a largo plazo es el único camino realista.

2. Solución: Afortunadamente, se descubre que una parte significativa (un dieciseisavo, para ser exactos) del grupo de direcciones IPv4, llamado 240/4 netblock ha sido "RESERVADO" para "Uso futuro" desde los primeros días. En consecuencia, ninguno de los equipos de Internet actuales es capaz de utilizarlo. Esto ofrece una oportunidad única para que una nueva clase de enrutadores lo utilicen para identificar hasta 256 millones de IoT de cada dirección IPv4 existente. Administrado adecuadamente, un sistema de comunicación mundial totalmente direccionable de extremo a extremo no solo brinda todos los servicios deseados de manera uniforme a cada suscriptor, sino que también mitiga la causa raíz de la vulnerabilidad de seguridad cibernética, todo dentro del alcance de la tecnología IPv4 existente.

3. Implementación por fases: para integrarse con el modo actual de operación de servidor-cliente de Internet, el enfoque anterior puede implementarse inmediatamente con un formato degenerado, en el que el bloque de red 240/4 se usa como si fuera el cuarto grupo de direcciones de red privada, en además de 192.168/16, 172.16/12 y 10/8. Esta fase introductoria solo requiere habilitar el bloque de red 240/4, sin modificar nada más en los diseños IPv4 existentes.

4. Implementación: este enfoque apenas requiere ningún esfuerzo de ingeniería. El costo de implementación es el mismo que el del equipo IPv4 actual comparable. Y, los gastos de operación se reducirán debido a las prácticas simplificadas que mitigan las interrupciones, como los ataques cibernéticos:

A. Desarrollo de productos (ProDev): simplemente deshabilite los códigos de software existentes que han estado deshabilitando el uso del netblock 240/4.

B. Gastos de Capital (CapEx): Los mismos que los actuales equipos IPv4 para la misma capacidad de servicio, usando el mismo hardware.

C. Gastos de Operación (OpEx): Reducidos por prácticas optimizadas que no dependen de esquemas dinámicos.

D. Seguridad cibernética: Mejorada por la administración determinista de identificación (dirección) de IoT.

5. Acciones propuestas:

A. Con las características inherentes de iniciar servicios de Internet desde una red privada sin esfuerzos de desarrollo, este sistema propuesto puede ser implementado por cualquier parte interesada (agencias gubernamentales, empresas, empresarios, etc.) desde una dirección IPv4 válida disponible utilizando el equipo IPv4 existente.

B. Dado que este enfoque es de naturaleza genérica, se recomienda que el UIT-D lo revise para determinar su idoneidad en el despliegue universal para modernizar Internet.

Referencias:

I. Estado de vulnerabilidad de la seguridad cibernética

https://blog.apnic.net/2021/02/03/el-internet-de-la-basura/

II. Una demostración de factibilidad fácilmente replicable de esta propuesta.

https://www.avinta.com/phoenix-1/home/RegionalAreaNetworkArchitecture.pdf

III. tercero Comentario a un blog de IAB: Proponer este esquema para facilitar la participación del usuario final en el desarrollo de protocolos/productos.

https://blog.apnic.net/2020/08/31/rfc-8890-internet-es-para-usuarios-finales/

IV. Borrador del IETF: detalles técnicos de esta propuesta

https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space

V. Propiedad Intelectual: Patente de EE. UU. No.: 11,159,425

Terminología, abreviatura y acrónimo:

. CG-NAT: traducción de direcciones de red de nivel de operador

. DHCP: protocolo de configuración de host dinámico

. DNS: Sistema de nombres de dominio

. IAB: Junta de Arquitectura de Internet

. IETF: Grupo de Trabajo de Ingeniería de Internet

. IoT: Internet de las cosas

. IPv4: Protocolo de Internet versión 4

. IPv6: Protocolo de Internet versión 6

. UIT-D: Unión Internacional de Telecomunicaciones – Sector de Desarrollo

. PSTN: Red Telefónica Pública Conmutada

. 240/4 Netblock: grupo de direcciones IPv4 que va desde 240.0.0.0 a 255.255.255.255, que asciende a aproximadamente 256 millones (256 M) o un cuarto de billón (0,25 B) de direcciones

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml