Mozilla Implementa Relays De Alta Capacidad En La Red Tor

En noviembre se conoció la iniciativa Polaris, **alianza entre Mozilla y el proyecto TOR**, con el fin de ayudar a reducir el número limitado de conexiones Tor, Mozilla ya esta iniciando los primeros pasos con los **Relays en la red TOR**.

El desarrollador de Firefox ha dado a la red Tor una alta capacidad de Relays con el lanzamiento de 12 Relays, todos ubicados en los Estados Unidos, lo cual ayudará a distribuir el tráfico de usuarios. Mozilla es una de las empresas de mayor confianza en Internet, sobre todo cuando se trata de la privacidad del usuario. La asociación de Mozilla y Tor esta enfocada en proporcionar más ***funciones de privacidad en el navegador Firefox***, y un mayor soporte a la red Tor.

La Iniciativa de Privacidad Polaris, fue un esfuerzo de Mozilla, el Proyecto Tor y el Centro de Democracia y la Tecnología (un grupo de defensa de los derechos digitales), con el fin de ayudar a desarrollar más controles de privacidad en la tecnología.

Los ingenieros que trabajan en el **Proyecto Polaris**, hicieron uso de algunas maquinas de la compañía Mozilla, en la que se incluyó un par de switches Juniper EX4200 y tres ***servidores HP SL170zG6*** (48GB ram, 2*Xeon L5640, 2*1Gbps NIC), junto con una IP dedicada para el proyecto (2 X 10 Gbps).

> *«El diseño actual es completamente redundante. Esto nos permite completar el mantenimiento o fallo de un nodo sin*

impactar el 100% del tráfico. En el peor de los casos es una pérdida del 50% de la capacidad», dijo el ingeniero francés de Mozilla, Arzhel Younsi en un blog.
«El diseño también nos permite añadir fácilmente más servidores en caso necesitamos más capacidad, sin impacto previsto.»

Sin embargo, la plataforma no está cerca de usar su máxima capacidad de ancho de banda y podría recibir nuevas mejoras incluyendo el trasladado a infraestructura gestionada de Mozilla y con soporte de **conectividad IPv6**.

Debido a razones de seguridad, no más de dos **nodos Tor** pueden compartir una **dirección IP dedicada**. Pero si es así, un atacante podría lanzar una variedad de nodos ficticios para eludir el anonimato.

Los ingenieros utilizan la plataforma Ansible de código abierto para la gestión de la configuración. Además, la herramienta no requiere una infraestructura de cliente/servidor pesada que debería hacerlo más accesible a otros operadores.

La plataforma se aseguró con estrictos filtros de cortafuegos, sistemas operativos robustos, gestión de dispositivos de red y filtrado, implementados en un esfuerzo por hacer que los sistemas autorizados puedan conectar con el «plano de gestión de red.»

«Es importante señalar, que muchos de los requisitos de seguridad se alinean muy bien con lo que se considera una buena práctica en el sistema general y administración de la

red», dijo Younsi.

La red Tor ha tenido una serie de cambios útiles para los usuarios, como ya hemos visto anteriormente, los usuarios de facebook ya pueden usar esta red social desde el dominio .onion, con lo cual podrán tener asegurado de cierta manera la privacidad al navegar en este portal.