Habrá más tráfico encriptado: Fortinet

El tráfico web y basado en aplicaciones comprende un mayor volumen del tráfico total, y gran parte de éste incluye **datos confidenciales o acceso a información que tradicionalmente estaba oculta en el centro de datos**. Para adaptarse a este cambio, las organizaciones están aumentando su **dependencia a lo encriptado**, principalmente la capa de ***sockets* seguros** (SSL, por sus siglas en inglés) y la **seguridad en la capa de transporte** (TLS, por sus siglas en inglés), para proteger sus datos en movimiento.

"Como resultado, el tráfico encriptado ha alcanzado un nuevo umbral de más de 72 por ciento de todo el tráfico de la red. Eso es un aumento de casi 20 por ciento en tan sólo un año, en comparación con 55 por ciento en el tercer trimestre de 2017", asegura John Maddison, vicepresidente senior de Productos y Soluciones de Fortinet

Esta estrategia, explica, tiene muchos beneficios. "El más importante es que permite que datos, aplicaciones, flujos de trabajo y transacciones iniciadas tanto por empleados como por consumidores se muevan a donde los requerimientos del negocio lo necesitan. A su vez, esto permite la transición global a una **economía digital**".

Retos

Si bien en muchos sentidos el **crecimiento de la encriptación es bueno para la seguridad**, la tasa más alta también presenta desafíos severos a la inspección profunda del tráfico para monitorear y detectar amenazas.

"Debido a que la encriptación es simplemente una herramienta, puede usarse para proteger cualquier **tráfico de detección**, ya sea bueno o malicioso. Los cibercriminales, por ejemplo, son muy conscientes del crecimiento de la encriptación y la utilizan para su ventaja al ocultar su presencia y evadir la detección, ya sea entregando malware o extrayendo datos robados. Y a medida que el volumen y el porcentaje de datos encriptados continúan creciendo, estas tácticas delictivas tienen más probabilidades de ocultarse a simple vista", agrega Maddison.

Una razón por la que esta es una preocupación creciente y está a punto de alcanzar un umbral crítico es que la **inspección del tráfico encriptado impone limitaciones de rendimiento en casi todos los firewalls y dispositivos de sistemas de prevención de intrusión** (IPS, por sus siglas en inglés) disponibles en el mercado hoy en día.

"De acuerdo con los resultados de las pruebas recientes de NSS Labs, muy pocos dispositivos de seguridad pueden inspeccionar datos encriptados sin afectar gravemente el rendimiento de la red.

"En promedio, **el impacto en el rendimiento para la inspección profunda de paquetes es del 60 por ciento**, las tasas de conexión se redujeron en un promedio de 92 por ciento y el tiempo de respuesta aumentó en 672 por ciento. Por supuesto, este tipo de resultados hace que la mayoría de los dispositivos de seguridad tradicionales sean casi inútiles en las redes de hoy en día, donde la encriptación es la norma y el rendimiento es fundamental.

“Como resultado, gran parte del tráfico encriptado de hoy no se está analizando en busca de actividad maliciosa, lo que lo convierte es un mecanismo ideal para que los delincuentes difundan malware o puedan extraer datos”, agregó Maddison.