¿Cómo bloquea el tráfico el monitor de tráfico de capa 4?

Pregunta:

¿Cómo bloquea el tráfico el monitor de tráfico de capa 4 si sólo recibe tráfico reflejado?

Entorno:

Monitor de tráfico de capa 4: L4TM configurado para bloquear el tráfico sospechoso

Solución:

El dispositivo de seguridad Cisco Web Security Appliance (WSA) cuenta con un servicio integrado de monitor de tráfico de capa 4 (L4TM) que puede bloquear sesiones sospechosas en todos los puertos de red (TCP/UDP 0-65535).

Para poder supervisar o bloquear estas sesiones, el tráfico debe redirigirse al WSA, ya sea mediante un dispositivo TAP (puerto de acceso de prueba) o mediante la configuración de un puerto espejo en los dispositivos de red (puertos SPAN en los dispositivos Cisco). El modo en línea L4TM todavía no se soporta.

Aunque el tráfico sólo se duplica (copia) de las sesiones originales al dispositivo, WSA puede bloquear el tráfico sospechoso reiniciando una sesión TCP o enviando mensajes ICMP de "host inalcanzable" para las sesiones UDP.

Para sesiones TCP

Cuando el WSA L4TM recibe un paquete hacia o desde un servidor y el tráfico coincide con una Acción de bloqueo, L4TM enviará un datagrama TCP RST (reinicio) al cliente o al servidor según el escenario. Un datagrama TCP RST es sólo un paquete normal con el indicador TCP RST establecido en 1.

El receptor de un RST lo valida primero y luego cambia el estado. Si el receptor estaba en el estado LISTEN, lo ignora. Si el receptor se encontraba en estado SYN-RECEIVED y había estado anteriormente en el estado LISTEN, entonces el receptor regresa al estado LISTEN, de lo contrario el receptor anula la conexión y pasa al estado CLOSED. Si el receptor se encuentra en cualquier otro estado, anula la conexión y avisa al usuario y pasa al estado CERRADO.

Hay dos casos que se deben tener en cuenta (en ambos casos, los usuarios/clientes se encuentran detrás de un firewall):

- La primera es cuando el paquete sospechoso proviene del exterior del firewall hacia un cliente en la red interna. El RST se enviará al servidor y, en este caso, llegará al firewall que normalmente no reenviará el RST pero terminará la sesión, ya que creerá que el RST en realidad vino del cliente. En este caso, la IP de origen del RST será la IP falsa del cliente. El

cliente terminará la sesión.

Un segundo caso sería cuando el paquete viene del cliente en la red interna y va a un servidor externo (fuera del firewall). El RST se envía entonces al Cliente y la IP de origen RST será la IP falsa del servidor.

Para sesiones UDP

WSA realiza un comportamiento similar cuando el tráfico sospechoso proviene de una sesión UDP, pero en lugar de enviar TCP RST , L4TM enviará mensajes de host ICMP inalcanzables (código ICMP tipo 3 1) al cliente o al servidor. Sin embargo, no hay suplantación de IP en estos casos, ya que el mensaje ICMP indica que el host es inalcanzable para que no pueda enviar paquetes. La IP de origen en este caso será la IP de WSA.

Estos RST y paquetes ICMP se envían desde el WSA usando la tabla de ruteo de datos, a través de M1, P1 o P2, según la implementación.