DETECCIÓN Y CONTROL DE CLIENTES CON EXCESO DE CONEXIONES SIMULTÁNEAS
Fecha: 10 de Noviembre de 2025

1. INTRODUCCIÓN

Con el fin de de detectar posibles casos de reventa de servicio o uso indebido de la red, se plantea un análisis en los equipos Mikrotik de Gestión, cubriendo clientes residenciales y corporativos, para identificar y controlar clientes que generan un número inusual de conexiones simultáneas. El sistema se implementa de manera no intrusiva en fase de observación, con posterior escalamiento a acciones de mitigación y bloqueo según los resultados del análisis.

2. OBJETIVO

Implementar un mecanismo de detección y control de clientes que superen un umbral establecido de conexiones TCP simultáneas, permitiendo evidenciar posibles casos de reventa, abuso de red o configuraciones inadecuadas que afecten el desempeño general del servicio.

3. DESCRIPCIÓN TÉCNICA DE LA IMPLEMENTACIÓN

Se implementó una regla de firewall con el parámetro *connection-limit* para contar las conexiones simultáneas por IP cliente.

```
/ip firewall filter
add chain=forward protocol=tcp connection-state=new tcp-flags=syn \
   connection-limit=1500,32 \
   action=add-src-to-address-list \
   address-list=Conexiones_excesivas address-list-timeout=1h \
   comment="Detecta clientes con >1500 conexiones TCP"
```

Esta configuración permite que cuando una IP supere las 1500 conexiones simultáneas activas, se añada automáticamente a la lista *Conexiones_excesivas* durante una hora y se genere un registro en el log del router.

4. METODOLOGÍA DE ANÁLISIS

- ***Fase de observación***
  1. Se mantiene la regla en modo log durante 24 horas.
  2. Se recolectan los datos de las IPs añadidas a la lista de Conexiones_excesivas.
  3. Se identifican las IPs con mayor frecuencia de aparición y número de conexiones.
- ***Fase de identificación***
  Cada IP detectada se cruza con la base de datos de asignaciones para determinar:
  - Nombre del cliente
  - Tipo de servicio (Residencial/Corporativo)
  - Plan contratado
  - Número de conexiones de las IPs
  - Puertos y destinos de las IPs
  - VLAN/PON/Segmento de red
- ***Fase de análisis***
  Durante la observación se analizaron los puertos y destinos más utilizados en las IP detectadas para determinar las causas más probables del alto número de conexiones:

CAUSA PROBABLE	INDICADORES OBSERVADOS	ACCIÓN
NAT interno masivo	Múltiples conexiones a distintos destinos, mismo origen	Revisar router del cliente e identificar servicio al cual se está conectando para corroborar si es normal la cantidad de solicitudes requeridas
Proxy o reventa	Picos de cientos/miles de conexiones concurrentes	Verificar uso comercial no autorizado, plantear visita técnica
Servidor interno (Hosting/Juegos)	Conexiones constantes a puertos fijos	No es crítico
Tráfico P2P/torrents	Multiplicidad de conexiones a IPs globales	Aplicar política de limitación o bloqueo

- ***Fase de acción y verificación***
  Conforme al análisis obtenido, se determina si se realiza el bloqueo de la IP, la limitación de las conexiones u otras medidas de control. En casos de sospecha de reventa, se programa visita técnica para comprobar en sitio el uso del servicio.

5. CONCLUSIONES

Este sistema es efectivo y automatizable para la identificación de clientes con comportamientos anómalos de tráfico. Actualmente se encuentra funcionando en los Mikrotik de Gestión de Sogamoso y Duitama en fase de observación para que, posterior a un periodo de pruebas, se implemente un script que recolecte los datos y envíe reportes a un servidor log para su análisis y gestión.