Procedimiento para el Bloqueo de Acceso No Autorizado de Agentes Externos

1. Objetivo

El presente documento tiene como objetivo establecer y describir el procedimiento implementado por **FIBRATVSAS** para proteger la integridad, confidencialidad y disponibilidad de su infraestructura de red, mediante el bloqueo proactivo de intentos de acceso no autorizado por parte de agentes externos. Esta política es fundamental para mitigar riesgos de ciberseguridad como intrusiones, robos de información y ataques de denegación de servicio.

2. Alcance

Este procedimiento aplica a toda la infraestructura de red perimetral de FIBRATVSAS, incluyendo los enlaces de conectividad, servidores críticos y dispositivos de gestión. El firewall corporativo, que actúa como la primera línea de defensa, es el principal responsable de ejecutar estas medidas.

3. Dispositivo Principal de Seguridad Perimetral

FIBRATVSAS ha seleccionado y configurado dispositivos **MikroTik RouterOS** como la solución firewall principal para la gestión del tráfico de red. La elección de MikroTik se basa en su robustez, flexibilidad, potente filtrado de paquetes y capacidades de estado (stateful inspection), que permiten un control granular del flujo de datos entre la red interna y Internet.

4. Procedimiento Técnico Implementado

El bloqueo de accesos no autorizados se realiza mediante una estrategia de capas en el firewall MikroTik, que incluye las siguientes acciones:

4.1. Política "Denegar por Defecto" (Default Deny):
Se ha configurado una política base donde **todo el tráfico entrante (Input) y de reenvío (Forward) desde la interfaz externa (WAN) está DENEGADO por defecto**. Solo se permiten explícitamente los servicios y puertos necesarios para la operación.

4.2. Filtrado Stateful (Conexiones con Estado):
Se utiliza el filtrado stateful para realizar un seguimiento inteligente de las conexiones. El firewall distingue entre:

- **Tráfico iniciado desde el interior:** Se permite el establecimiento de conexiones desde la red interna hacia el exterior, y el firewall automáticamente permite las respuestas correspondientes.
- **Tráfico no solicitado desde el exterior:** Cualquier paquete que intente ingresar a la red sin haber sido solicitado previamente desde dentro, es bloqueado automáticamente, a menos que una regla explícita lo permita.

4.3. Listas de Control de Acceso (ACLs) Granulares:
Se han creado reglas específicas en la cadena `Filter` para:

- **Permitir servicios esenciales:** Se habilitan únicamente los puertos necesarios para servicios públicos (ej: puerto 80/443 para un servidor web, puerto 25 para un servidor de correo, etc.), aplicando restricciones de IP de origen cuando es posible.
- **Bloquear puertos y protocolos innecesarios:** Se deniega explícitamente el acceso a puertos conocidos por ser vectores de ataque (ej: Telnet, NetBIOS, etc.) y a protocolos no utilizados en la red.
- **Protección contra escaneos y fuerza bruta:** Se implementan reglas que detectan y bloquean IPs que realizan múltiples intentos de conexión en un corto período de tiempo, una técnica común para identificar vulnerabilidades o adivinar credenciales.

4.4. Listas de Bloqueo Dinámicas (Address Lists):
El firewall MikroTik mantiene listas dinámicas de direcciones IP consideradas maliciosas.

- Estas listas se pueden actualizar automáticamente desde fuentes confiables en Internet o manualmente por el equipo de soporte.
- Cualquier intento de conexión desde una IP incluida en estas listas es descartado inmediatamente.

4.5. Hardening del Propio Dispositivo MikroTik:

- El acceso a la interfaz de gestión del MikroTik (Winbox, SSH, API) está restringido únicamente a direcciones IP de la red de administración de FIBRATVSAS.
- Se utilizan contraseñas robustas y se ha deshabilitado el acceso a los servicios de gestión desde la interfaz WAN (Internet).

5. Monitoreo y Respuesta a Incidentes

El equipo de seguridad de FIBRATVSAS monitorea de forma continua los logs del firewall MikroTik para identificar patrones de tráfico sospechoso, intentos de acceso fallidos y posibles amenazas. Ante una alerta, se analiza la IP atacante y se procede a su bloqueo permanente mediante su inclusión en una Address List, reforzando así la seguridad de forma proactiva.

6. Conclusión

Mediante la implementación disciplinada de este procedimiento en nuestro firewall principal MikroTik, FIBRATVSAS garantiza un entorno de red seguro y controlado, minimizando significativamente la superficie de ataque y protegiendo los activos informáticos de la empresa y los datos de sus clientes contra el acceso no autorizado por parte de agentes externos.