GUÍA DE IMPLEMENTACIÓN: BLOQUEO DE DOMINIOS CON BIND Y RESPONSE POLICY ZONES (RPZ)

Esta guía detalla los pasos para configurar su servidor DNS recursivo con BIND utilizando Response Policy Zones (RPZ), el método más eficaz para el bloqueo masivo de dominios

. 1. Preparación del Archivo de Zona RPZ

El archivo Coljuegos.db debe ser adaptado al formato RPZ. En lugar de usar registros A apuntando a la IP de desvío, se utiliza un registro CNAME que apunta a un nombre local de "sinkhole".

***Paso 1.1: Crear el Archivo de Zona Cree el archivo RPZ** en el directorio de configuración de BIND (ejemplo: /etc/bind/). Bash sudo nano /etc/bind/rpz.coljuegos.db*

***Paso 1.2: Contenido del Archivo RPZ** El archivo debe contener el siguiente encabezado y estructura: $TTL 300 @ IN SOA localhost. root.localhost. (2025102801 ; Serial (Actualice este número cada vez que modifique la lista) 3H ; Refresh 15M ; Retry 1W ; Expire 1H) ; Negative Cache TTL @ IN NS localhost. ; *** Entrada Sinkhole Local *** rpz-sinkhole.coljuegos.local. IN A 172.17.1.6 ; ---------- ; *** POLÍTICA DE BLOQUEO (CNAME a Sinkhole) *** ; IMPORTANTE: El formato de su archivo Coljuegos.db (DOMINIO A IP) ; debe ser convertido a: DOMINIO IN CNAME rpz-sinkhole.coljuegos.local. r-casinoonline.win IN CNAME rpz-sinkhole.coljuegos.local. w-play.co IN CNAME rpz-sinkhole.coljuegos.local.*

00111.poker IN CNAME rpz-sinkhole.coljuegos.local. ; ... [AGREGUE AQUÍ TODOS LOS DOMINIOS BLOQUEADOS EN ESTE FORMATO]

***2. Configuración de la Zona** en BIND Debe registrar la nueva zona de política en BIND.*

***Paso 2.1: Editar named.conf.local** Abra el archivo de configuración de zonas: Bash sudo nano /etc/bind/named.conf.local*

***Paso 2.2: Agregar la Definición de Zona** Pegue el siguiente bloque de configuración.*

El nombre de la zona es "coljuegos.rpz":

// Zona de Política de Respuesta para Coljuegos (RPZ) zone "coljuegos.rpz" IN { type master; file "/etc/bind/rpz.coljuegos.db"; allow-query { none; }; // Evita consultas directas a la zona };

***3. Activación de la Política de Respuesta** Debe indicar al demonio named que use la zona definida como una política activa.*

***Paso 3.1: Editar named**.conf.options Abra el archivo de opciones principales: Bash sudo nano /etc/bind/named.conf.options*

Paso 3.2: Agregar el Bloque *response-policy Dentro del bloque options { ... };, agregue la siguiente configuración: options { // ... otras opciones ... // *** INICIO DE LA CONFIGURACIÓN RPZ *** response-policy { zone "coljuegos.rpz"; // Si desea bloquear subdominios no listados explícitamente, // use la opción: qname-wait-recurse no; };*

*// *** FIN DE LA CONFIGURACIÓN RPZ *** // ... otras opciones ... };*

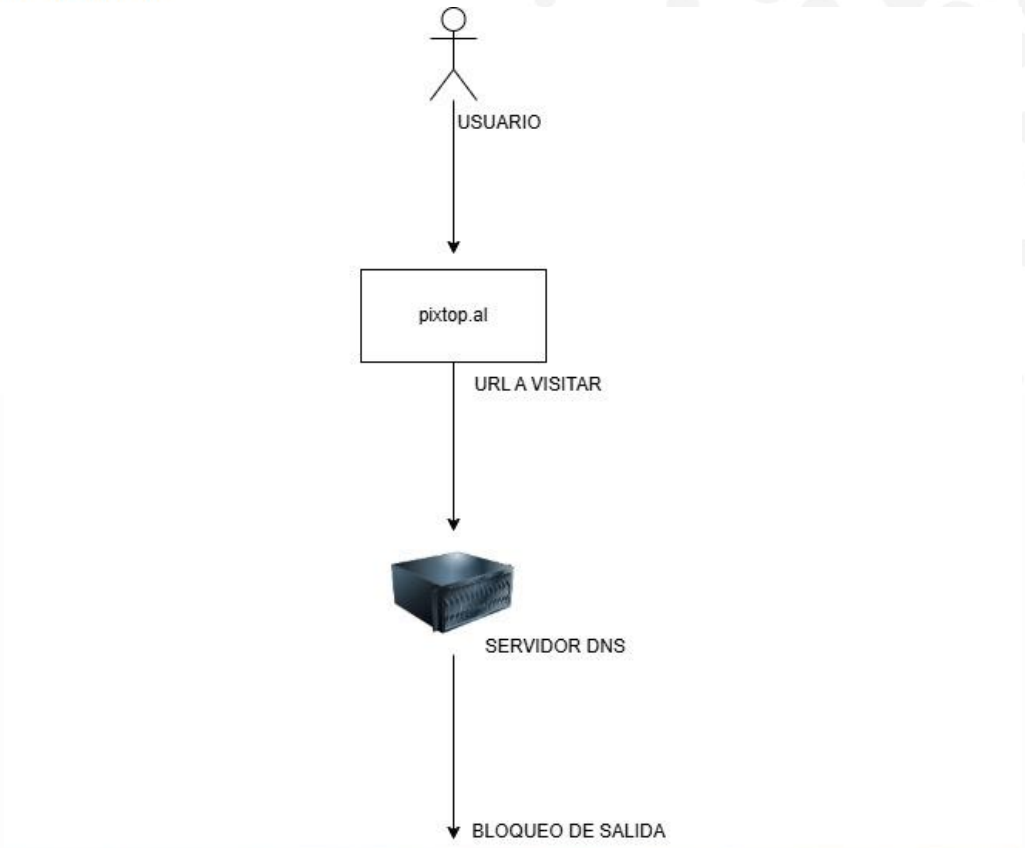
4. Verificación y Aplicación de Cambios Paso

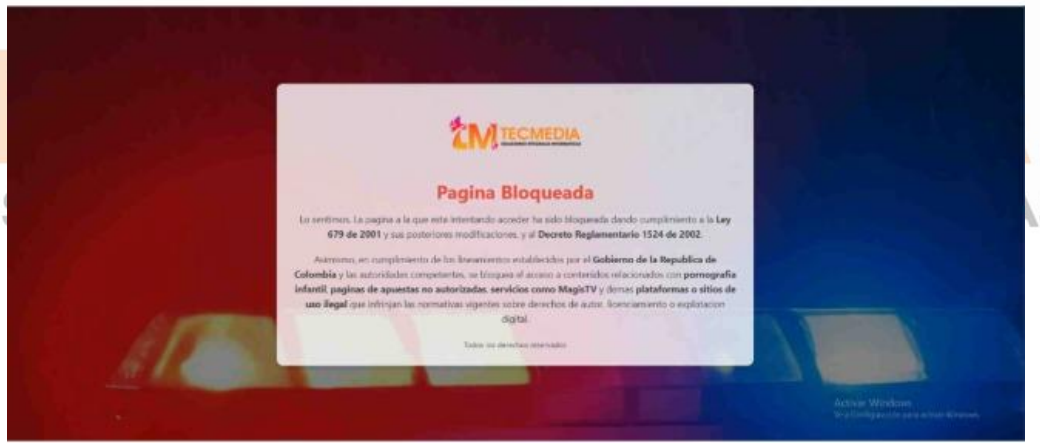
4.1: Verificar la Sintaxis *de BIND Ejecute estos comandos para asegurarse de que no haya errores de sintaxis en los archivos de configuración y la zona: # Verificar archivos principales (named.conf) sudo named-checkconf # Verificar la sintaxis del archivo de zona RPZ sudo named-checkzone coljuegos.rpz /etc/bind/rpz.coljuegos.db (Ambos comandos deberían mostrar un mensaje de "OK").*

Paso 4.2: Recargar el Servicio *BIND Aplique los cambios sin interrumpir completamente el servicio (recarga): sudo systemctl reload named Paso*

4.3: Probar el Bloqueo *Use el comando dig en su servidor DNS (o en un cliente que lo use) para verificar que la resolución se desvíe a la IP 172.17.1.6. Comando de prueba: dig r-casinoonline.win @127.0.0.1*

Resultado esperado: La sección de respuesta (ANSWER SECTION) debe mostrar la redirección al CNAME del sinkhole y luego la IP de desvío: ;; ANSWER SECTION: r-casinoonline.win. 300 IN CNAME rpz-sinkhole.coljuegos.local. rpz-sinkhole.coljuegos.local. 300 IN A 172.17.1.6 Si ve esta respuesta, la zona RPZ está funcionando correctamente.


USUARIO
pixtop.al
URL A VISITAR
SERVIDOR DNS
BLOQUEO DE SALIDA


TECMEDIA
Pagina Bloqueada
Lo sentimos. La pagina a la que esta intentando acceder ha sido bloqueada dando cumplimiento a la Ley 679 de 2001 y sus posteriores modificaciones, y al Decreto Reglamentario 1524 de 2002.
Activar Windows