

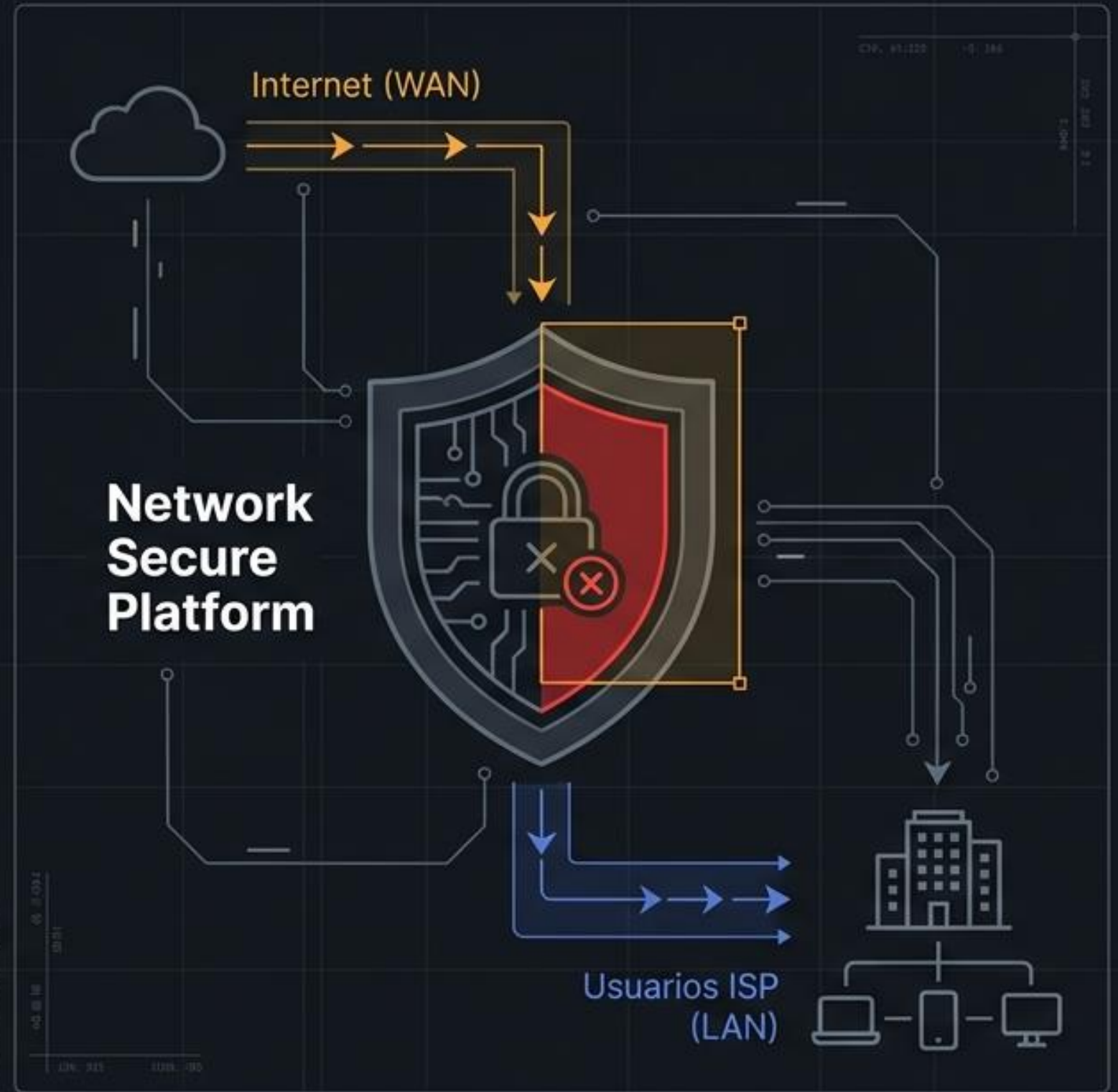
Flujo de Cumplimiento MinTIC: Bloqueo y Auditoría en Network Secure Platform

Guía de configuración técnica para la protección de red
(Categorías 1-6 y Políticas de Denegación).

El Mandato Regulatorio

- Obligación legal ineludible de restringir el acceso a URLs centralizadas y actualizadas por MinTIC.
- Foco en la mitigación de acceso a pornografía infantil y portales de apuestas no autorizados.
- El incumplimiento o la mala configuración impacta directamente la licencia de operación del ISP y conlleva severas sanciones.

Objetivo Técnico: Traducir estas listas dinámicas en reglas perimetrales estáticas con evidencia forense inalterable.



Arquitectura del Flujo de Implementación



Paso 1: Acceso y Descarga de Listados Oficiales

Ingreso periódico al portal transaccional del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Descarga de los archivos oficiales actualizados que contienen los dominios y URLs restringidas.



Preparación de los datos: Asegurar que las listas estén en formato de texto plano, con un dominio/URL por línea, para garantizar la ingesta correcta en la plataforma del firewall.



Servidor Gubernamental MinTIC



HTTPS (Encrypted)



Admin ISP



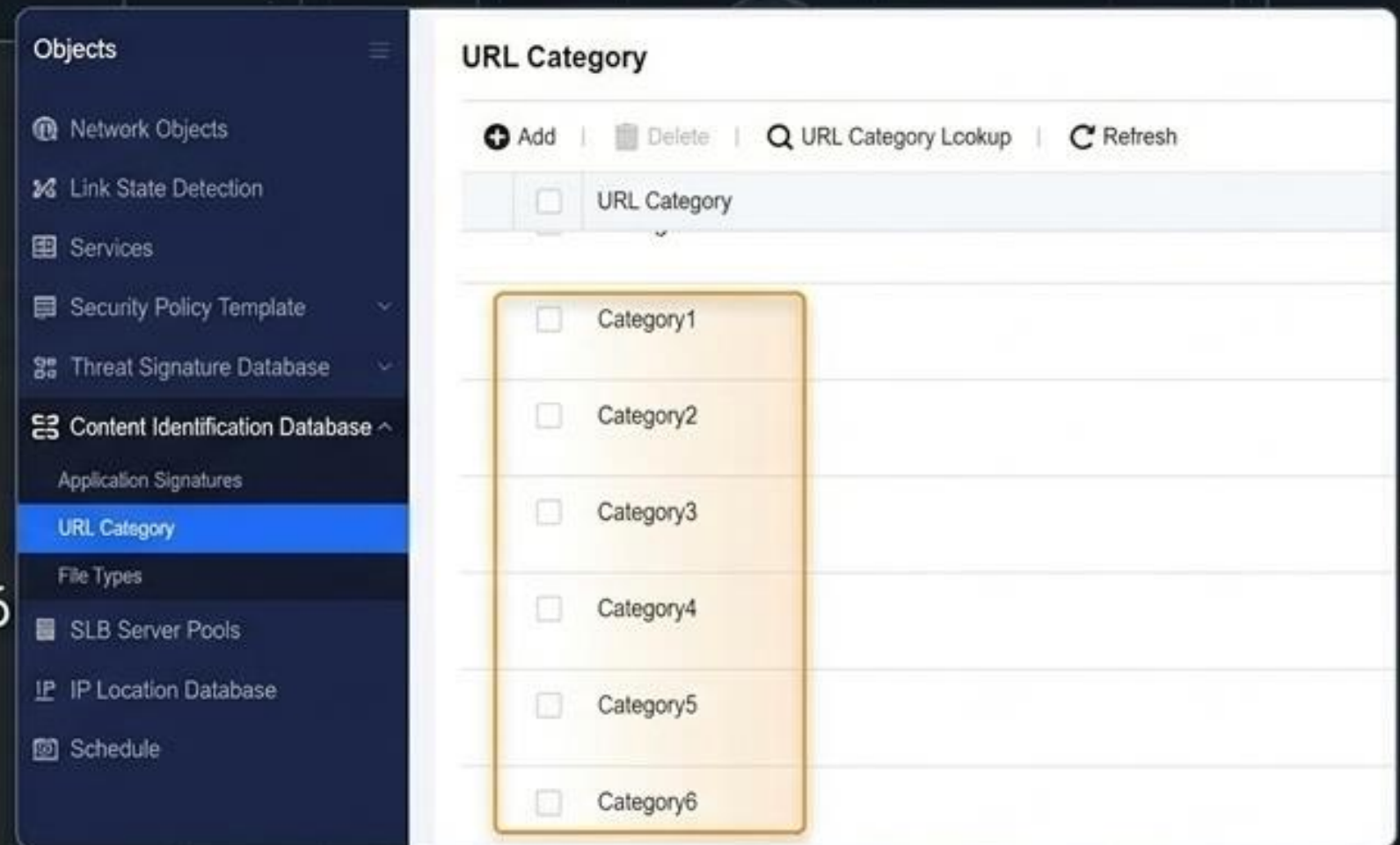
Lista de Dominios/URLs (Texto Plano)

Paso 2: Configuración de Contenedores de Red

Ruta de Navegación: Objects -> Content Identification Database -> URL Category

Descripción del Proceso:

- La plataforma requiere la creación de objetos (contenedores) específicos para estructurar la inmensa base de datos del ministerio.
- Es mandatorio utilizar los objetos denominados Category1 hasta Category6. Estos actuarán como los repositorios lógicos donde residirán las URLs bloqueadas.

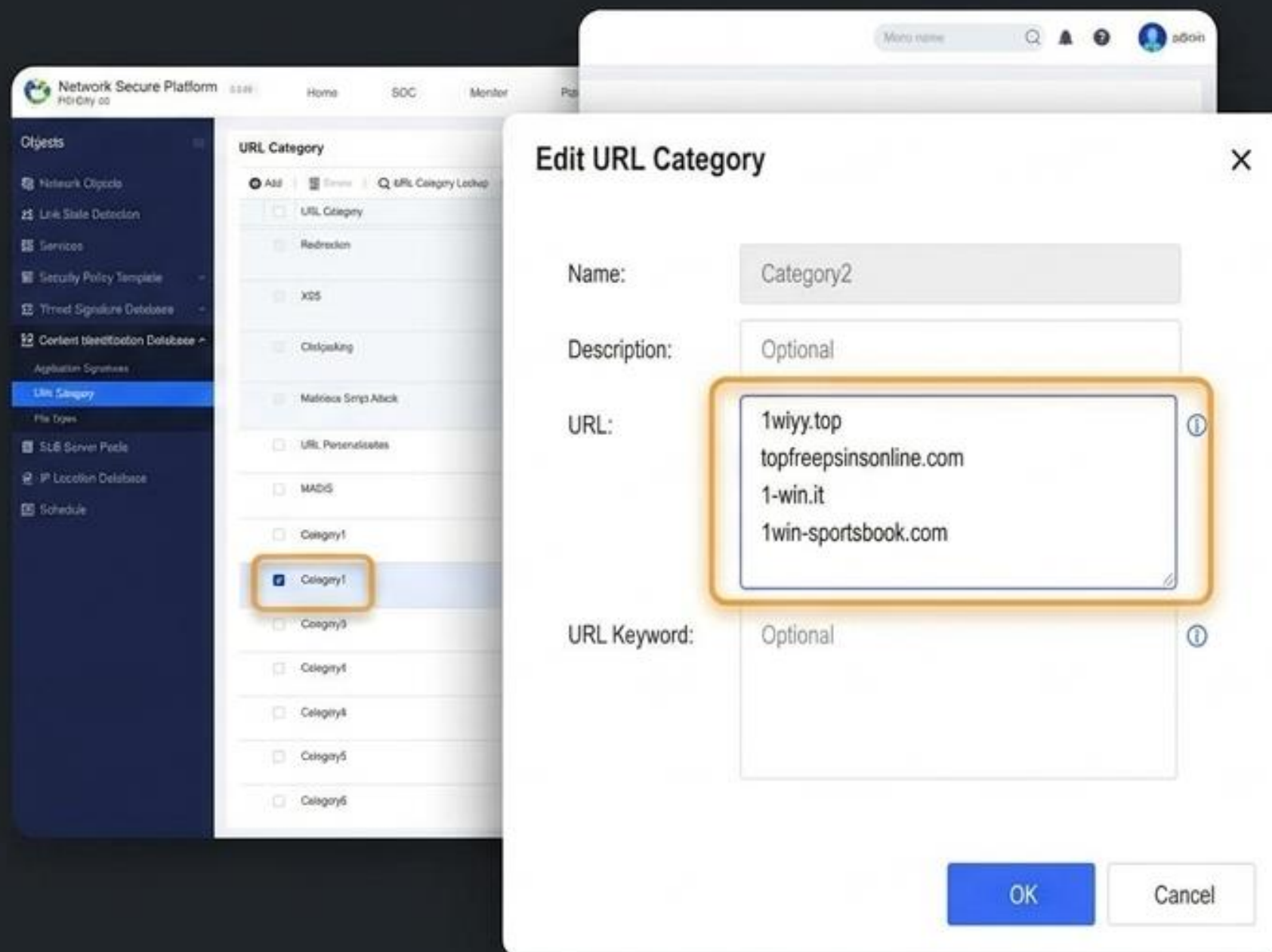


Ingesta de Listados (Categories 1-6)

Acción Técnica:

Seleccionar **Edit** en **Category1** (y subsecuentemente hasta la 6 según el volumen de la lista).

En el cuadro de diálogo, pegar directamente los listados crudos descargados del MinTIC dentro del campo **URL**.



⚠ Nota Crítica: No utilizar el campo URL Keyword para este propósito; la precisión exacta del dominio es requerida por el regulador.



















Paso 3: Creación de la Plantilla "Políticas mintic"

Ruta de Navegación: Objects -> Security Policy Template -> Content Security

Acción Técnica:

- Crear una nueva plantilla nombrada exactamente Políticas mintic. (La estandarización de nombres previene la orfandad de objetos en redes ISP complejas).
- Habilitar obligatoriamente el módulo de inspección URL Filter marcando la casilla correspondiente en la sección de protección.

The screenshot displays the 'Content Security' configuration page. It features a table with columns for 'No.', 'Name', 'Email Protection', 'URL Filter', 'File Protection', 'In Use', and 'Operation'. The first row, 'Políticas mintic', is highlighted. An 'Edit Template' dialog box is open, showing the 'Name' field set to 'Políticas mintic' and the 'Description' field set to 'Optional'. In the 'Protection' section, the 'URL Filter' checkbox is checked, and the 'Sites' field contains 'Illegality & Immorality,URL Personalizadas,MAGIS,Category 1.'. The 'Save' button is highlighted.

No.	Name	Email Protection	URL Filter	File Protection	In Use	Operation
1	Políticas mintic	Enable	Enable	Enable	No	  
2	Políticas mintic	Enable	Enable	Enable	No	  
3	Security research	Enable	Enable	Enable	No	  
4	Poliizcannel	Enable	Enable	Enable	No	  
5	Persait res					  
6	Security m					  

Edit Template

Name:

Description:

Protection

Enable

URL Filter

Sites:

File Protection (filter files and verify files with Engine Zero)

Vinculación de Categorías al Motor de Filtrado

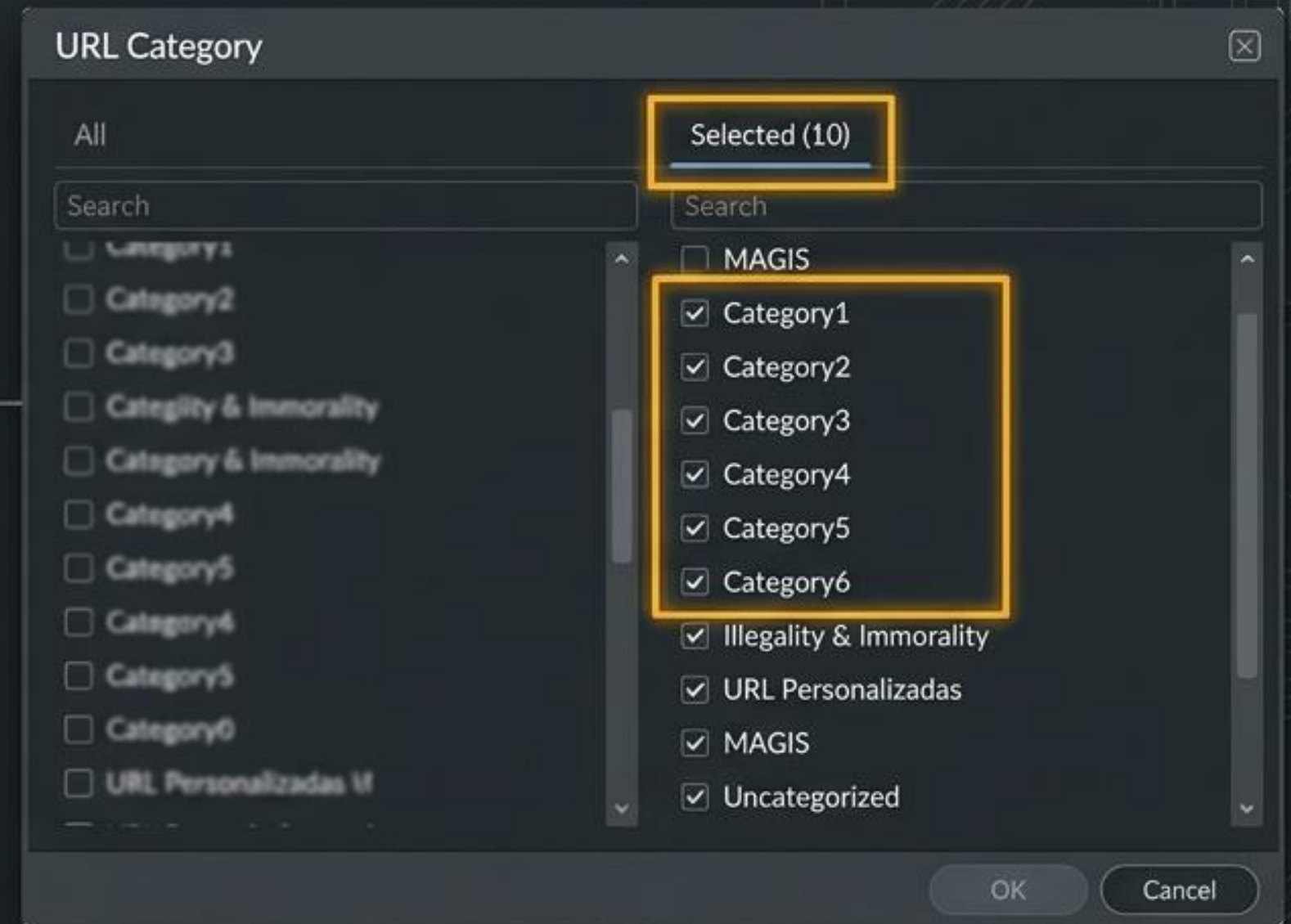
Dentro de la configuración del URL Filter, acceder al menú de selección de sitios.

Navegar a la pestaña Selected.

Verificar y marcar exhaustivamente los contenedores poblados anteriormente (Category1 a Category6).

Impacto Arquitectónico:

Este paso consolida miles de URLs individuales bajo un único perfil de inspección de alto rendimiento, optimizando el uso de CPU del firewall.

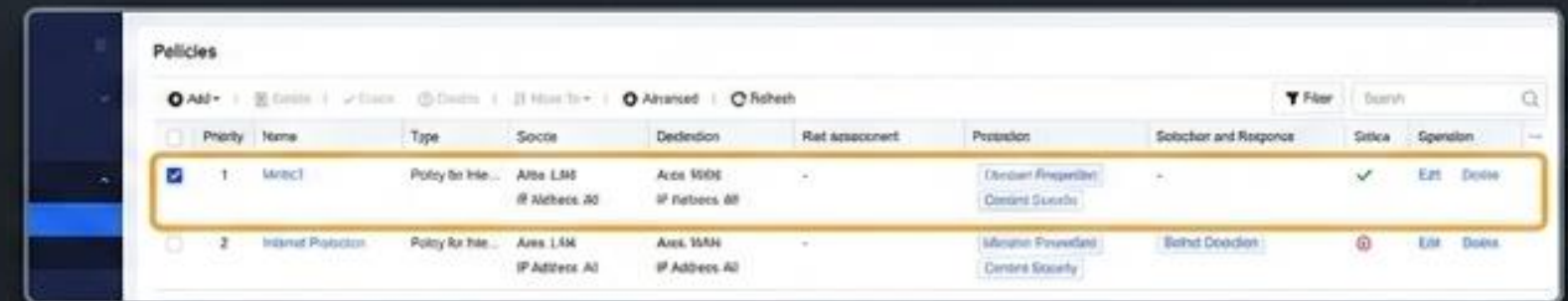


Paso 4: Política de Intercepción ('Mintic1')

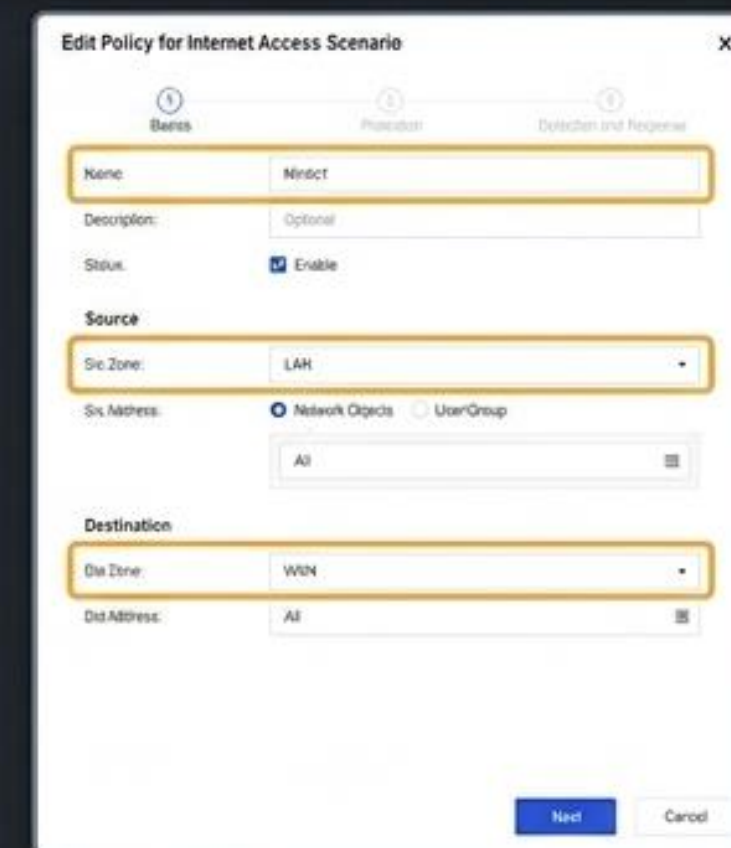
Ruta de Navegación: Políticas -> Network Security

Contexto de Enrutamiento:

- Crear una nueva regla con el nombre Mintic1.
- Source (Origen): Definir la zona LAN (o la zona correspondiente a los suscriptores del ISP). Address: All.
- Destination (Destino): Definir la zona WAN (Internet). Address: All.
- La política debe estar posicionada con la máxima prioridad para inspeccionar el tráfico antes que cualquier regla permisiva general.



Priority	Name	Type	Source	Destination	Rate association	Position	Selector and Response	Criteria	Operation
1	Mintic1	Policy for In...	All LAN IP Address All	All WAN IP Address All	-	Content Inspection Content Security	-	✓	Edit Delete
2	Internet Protection	Policy for In...	All LAN IP Address All	All WAN IP Address All	-	Malware Prevention Content Security	Behavior Detection	⊘	Edit Delete



Edit Policy for Internet Access Scenario

None Mintic1

Description: Optional

Status: Enable

Source

Src Zone: LAN

Src Address: Network Objects UserGroup
All

Destination

Dst Zone: WAN

Dst Address: All

Next Cancel

Ejecución de la Acción "Deny"

Acción Técnica (Pestaña Protection):

- Activar la verificación profunda Content Security.
- Vincular la plantilla previamente creada: Seleccionar Políticas mintic del menú desplegable.

Regla de Oro:

Configurar la acción estrictamente en Deny. Seleccionar 'Allow' en esta fase resultará en un fallo crítico de cumplimiento, permitiendo el tráfico prohibido de manera silenciosa.

Basics Protection Detection and Response

Basic Protection (For All Scenarios)

Intrusion Prevention ⓘ

Block Cloudflare

Action: Allow Deny

Content Security (AI-based Engine Zero file verification) ⓘ

Políticas mintic

Action: Allow Deny

Habilitación de Evidencia Forense (Logging)

Acción Técnica (Pestaña Detection and Response):

Bajo la sección Response (For All Scenarios), es obligatorio marcar la casilla Log events.

Implicación de Negocio:

Sin esta configuración, el equipo de SOC no tendrá visibilidad de las intercepciones.

Es el único mecanismo para exportar los reportes técnicos requeridos durante una auditoría formal del ministerio.

The screenshot shows the 'Edit Policy for Internet Access Scenario' window with three tabs: Basics, Protection, and Detection and Response. The 'Detection and Response' tab is active. Under 'Detection (For All Scenarios)', there is a 'Botnet Detection' checkbox and a dropdown menu. Under 'Response (For All Scenarios)', there is an 'IP Blocking' section with a 'Settings' link and a 'Log events' checkbox which is checked and highlighted with a yellow box. At the bottom, there are 'Back', 'Save', and 'Cancel' buttons.

Paso 5: Monitoreo y Verificación

Ruta de Navegación: Monitor -> Logs -> Security Logs

Parámetros de Búsqueda Base:

- Establecer el **rango temporal** (Start Time y End Time) alineado con el momento de implementación de la política Mintic1 o el periodo de auditoría solicitado.
- Dejar Source y Destination en All para capturar cualquier intento de acceso dentro de la red del ISP.

The screenshot displays the 'Network Secure Platform' interface for device 'FW-OXI_40'. The navigation menu on the left shows 'Monitor' selected, with 'Logs' and 'Security Logs' highlighted. The main panel shows the 'Security Logs' configuration page. The search criteria are as follows:

- Start Time:** 2026-04-17 00:00
- End Time:** 2026-04-18 23:59
- Source:** Src Zone: All; Src Address: All (selected), IP, User, Group
- Destination:** Dst Zone: All; Dst Address: All

Extracción de Evidencia Positiva

Filtros Avanzados:

- **Type:** Seleccionar exclusivamente Website Access Blocking. Esto filtra el ruido de los eventos IPS/DDoS.
- **Action:** Seleccionar Deny.

Resultado Esperado:

Al ejecutar la búsqueda (Search), el panel inferior poblará un registro inmutable de todas las sesiones de usuarios que intentaron acceder a las listas del MinTIC y fueron bloqueados exitosamente por la política perimetral.

Type: All Web App Firewall Website Access Blocking Intrusion Prevention Email Protection Botnet Detection Anti-DoS/DDoS

Advanced

Threat Level: Severe ⓘ High Medium Low Info ⓘ

Action: Allow Deny

Open in Quick Tab

Matriz de Resolución Rápida (Troubleshooting)

Síntoma	Causa Probable	Resolución
Tráfico a URL MinTIC fluye sin restricciones.	Política "Mintic1" no está en "Deny" o fue superada por una regla de mayor prioridad.	Revisar Nodo 4 (Network Security -> Protection).
El tráfico se bloquea correctamente, pero no aparecen registros en "Security Logs".	La generación de eventos está desactivada en la política.	Revisar Nodo 4 (Policy -> Detection and Response -> Log events).
La plantilla de seguridad aparece vacía y no bloquea dominios.	Las Categorías 1-6 no fueron vinculadas en el perfil URL Filter.	Revisar Nodo 3 (Content Security -> Edit Template -> Selected).

Cumplimiento Validado

Checklist de Integración

- ✓ Listas dinámicas estructuradas (Categorías 1-6).
- ✓ Motor de inspección calibrado (Plantilla 'Políticas mintic').
- ✓ Intercepción perimetral activa (Regla 'Mintic1' en modo Deny).
- ✓ Visibilidad forense habilitada (Security Logs).

Cierre Operativo: La infraestructura de red ahora cumple rigurosamente con los lineamientos del Ministerio, protegiendo tanto al usuario final como la integridad legal del ISP.