CHILQUINTA servicios	**CHILQUINTA SERVICIOS S.A.** **GERENCIA DE TECNOLOGIA**		
Identificación: CS GT SGTI I 03	**Fecha Creación:** 06/06/2025	**Fecha Revisión/Modificación:** NA	**Versión:** 0

INSTRUCTIVO

FILTRADO WEB

WEB FILTER

Revisado por: JESUS AYALA Fecha: 17.06.2025	Aprobado por: ALFREDO MARTINEZ Fecha: 17.06.2025

1. OBJETIVO

Describir el procedimiento para gestionar el acceso y control de navegación a sitios web desde la red corporativa, con el propósito de proteger los activos de información y sistemas tecnológicos contra contenido malicioso y asegurar que el uso de internet en la compañía se ajuste a las políticas de seguridad y uso aceptable de recursos de la organización.

2. ALCANCE

Instructivo aplicable a las áreas de la Subgerencia de Telecomunicaciones y TI administradoras de los dispositivos de red y de seguridad perimetral, que controlan la navegación web y uso de la red corporativa por parte de los colaboradores del Grupo Empresas Chilquinta.

3. DEFINICIONES Y ABREVIACIONES

Filtrado Web: Proceso técnico mediante el cual se controla el acceso de un usuario a internet, permitiendo o denegando la visualización de sitios web o contenido en línea en función de un conjunto de reglas predefinidas.

Malware: Término genérico para cualquier tipo de software diseñado intencionadamente para infiltrarse en un dispositivo, dañar sistemas o robar información sin el consentimiento del propietario. Incluye, entre otros, virus, troyanos, ransomware, spyware y adware.

Lista Negra: Listado de sitios web, dominios o direcciones IP a los cuales se les niega explícitamente el acceso por ser considerados maliciosos, inapropiados o no productivos.

Lista Blanca: Listado de sitios web, dominios o direcciones IP que están explícitamente aprobados y a los cuales se permite el acceso, denegando todo lo que no esté en la lista.

CSOC: Centro de operaciones de ciberseguridad.

4. RESPONSABILIDAD Y AUTORIDAD

CARGO	DESCRIPCIÓN
Sistemas e Infraestructura	Implementar, configurar y mantener las reglas de filtrado web en los dispositivos de seguridad perimetral, asegurando el correcto funcionamiento de las reglas sin impacto en las operaciones del negocio.
Telecomunicaciones OT	Implementar, configurar y mantener las reglas de filtrado en los dispositivos de seguridad perimetral establecidos para la red OT, asegurando el correcto funcionamiento de las reglas sin impactar en las operaciones del negocio.

Ciberseguridad	Coordinar, con los administradores de firewalls perimetrales de TI y TO, la actualización de las listas de sitios bloqueados, cada vez que se identifique una nueva amenaza. Esta actualización debe basarse en inteligencia de amenazas, reportes de proveedores, publicaciones en fuentes oficiales de ciberseguridad, notificaciones del equipo CSOC sobre vulnerabilidades detectadas o por situaciones de emergencia dada la criticidad de un incidente detectado. Aprobar o rechazar solicitudes de excepción para el acceso a sitios web restringidos asegurando que cuenten con una justificación de negocio válida.

5. CONTENIDO

El control del tráfico web generado desde internet hacia la red corporativa (o viceversa), junto a la respectiva configuración y métodos de filtrado de direcciones URL e IP, se detalla a continuación en los siguientes puntos:

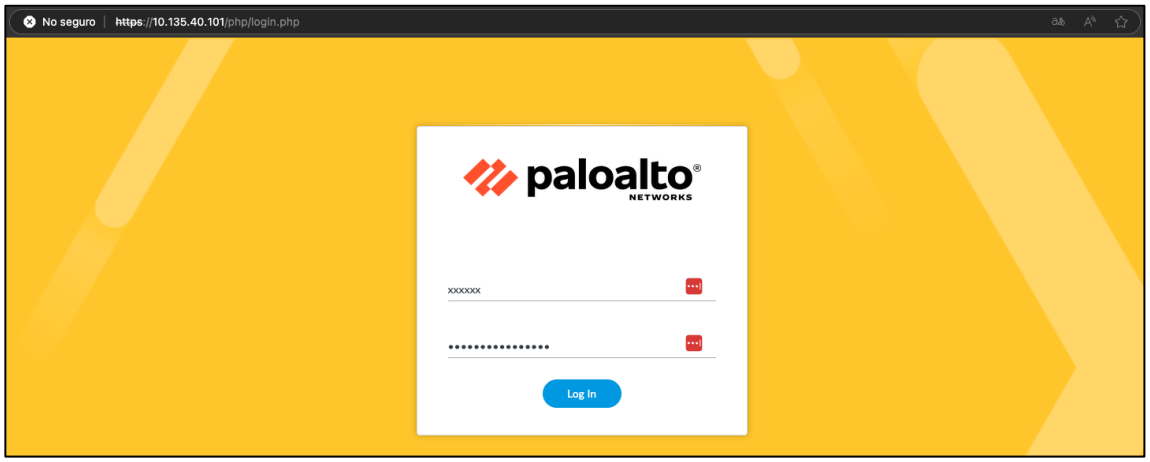
5.1. Administración General

La administración general de los dispositivos de seguridad perimetral es responsabilidad de Sistemas e Infraestructura y Telecomunicaciones TO, para la red TI y TO respectivamente. Ellas velan por la implementación, la configuración y mantención de las reglas de filtrado web en los dispositivos correspondientes, asegurando el correcto funcionamiento de las reglas sin impacto en las operaciones del negocio. Ciberseguridad, por su parte y en conjunto al equipo CSOC, apoyarán la recomendación de bloqueos para prevenir riesgos de ciberseguridad, solicitando, mediante control de cambio, la creación de listas negras para bloquear tanto sitios como direcciones IP consideradas peligrosas y listas blancas, para garantizar el acceso a recursos esenciales y confiables. Lo anterior, a través de los administradores de firewall perimetrales correspondientes. Este enfoque asegura que las medidas de filtrado sean dinámicas, efectivas y adaptadas a las necesidades de seguridad de la organización, minimizando al mismo tiempo cualquier impacto negativo en las operaciones del negocio.

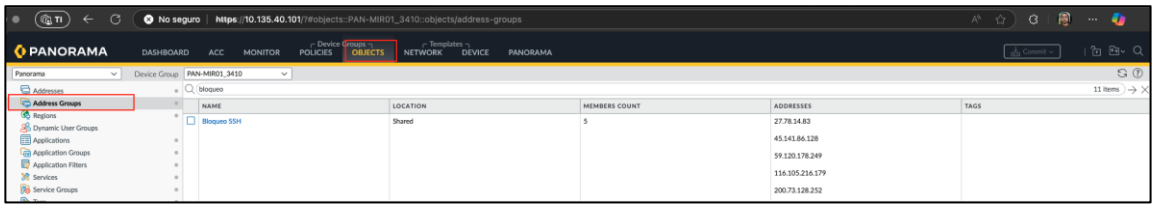
5.2. Proceso de configuración de filtrado web TI

A continuación, se describen los pasos para bloquear direcciones IP y URLs categorizadas como de riesgo utilizando las herramientas de filtrado en dispositivos perimetrales:

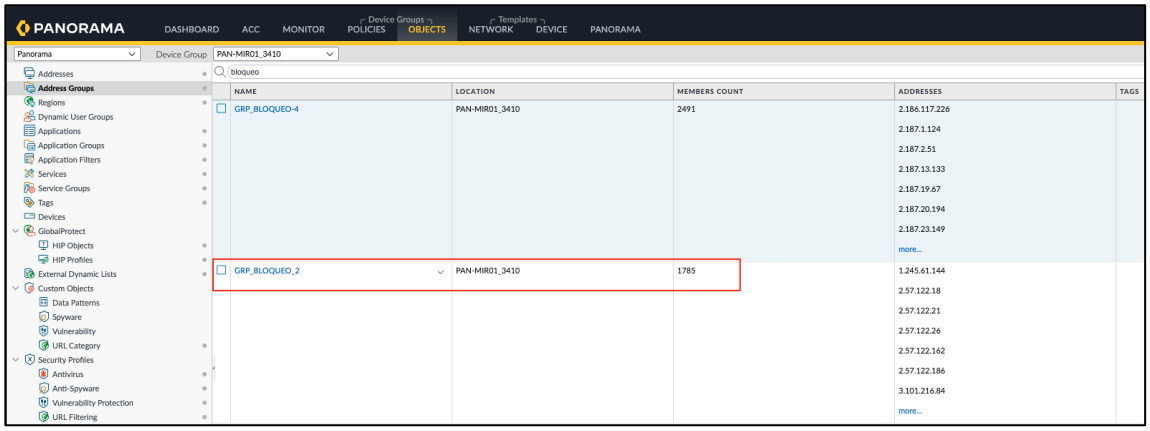
1. Acceder a la plataforma de gestión de seguridad Panorama, utilizando las credenciales autorizadas.



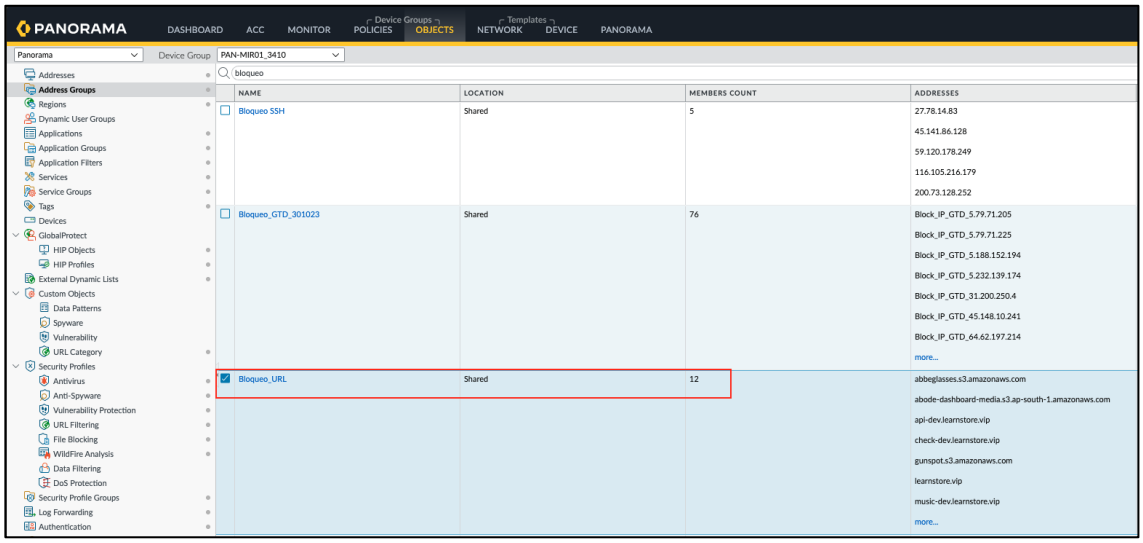
2. En la interfaz, dirigirse a la sección OBJECTS → Address Group para gestionar grupos de bloqueo.



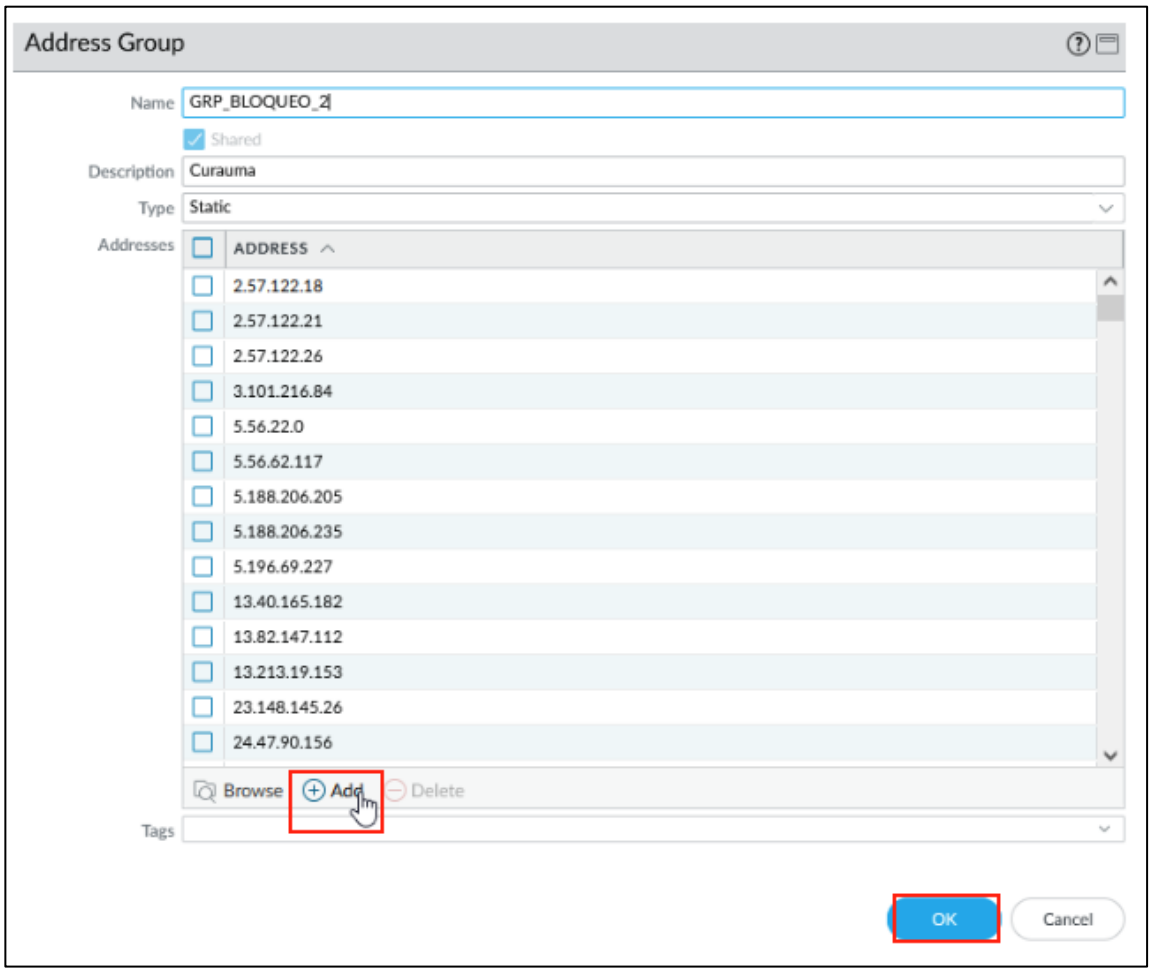
3. Seleccionar el grupo de bloqueo adecuado según la capacidad y el uso actual. Por ejemplo: GRP_Bloqueo_2 para el bloqueo de direcciones IP.



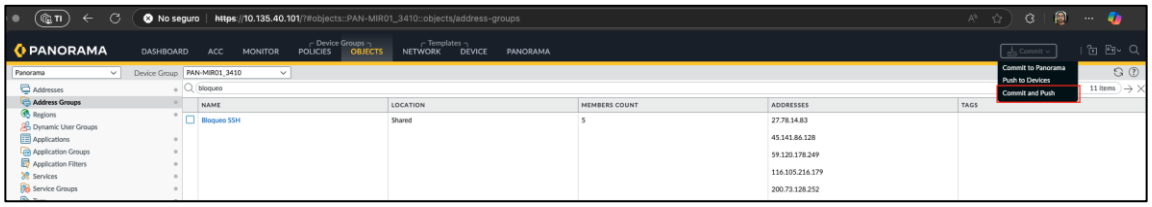
4. BLOQUEO_URL para el bloqueo de URLs.



5. Para ambos casos haga clic en el objetivo posteriormente en Add y proceda agregar la dirección IP o URL que se desea bloquear según la política correspondiente. Para finalizar presione “OK”.



5.6. Una vez realizadas las adiciones, proceder a aplicar las políticas en el firewall mediante las opciones Commit and Push para asegurarse de que los cambios entren en vigor.



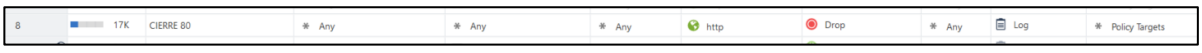
5.3. Categorías de filtrado web TI

Con el objetivo de reforzar las medidas preventivas ante el acceso a sitios web clasificados como de riesgo, se implementa un sistema de filtrado basado en categorías predefinidas que permiten el bloqueo de contenidos no deseados detallados a continuación:

- abortion
- abused-drugs
- adult
- command-and-control
- copyright-infringement
- dating
- dynamic-dns
- extremism
- games
- hacking
- malware
- nudity
- parked
- phishing
- proxy-avoidance-and-anonymizers
- questionable
- shareware-and-freeware
- social-networking
- weapons
- web-advertisements
- web-hosting

5.4. Proceso de configuración de filtrado web TO

De acuerdo con las políticas de filtrado web y gestión de acceso, las reglas configuradas en los firewalls de las zonas DMZ y SCADA están destinadas a controlar estrictamente el tráfico de origen, destino y servicio. No se permite la salida a internet desde los equipos ubicados en la zona de confianza (Trust), y se establece una regla específica que bloquea cualquier intento de tráfico orientado a la navegación por internet. Los firewalls operan exclusivamente bajo políticas de acceso aprobadas, garantizando un entorno seguro y alineado con las directrices establecidas para la seguridad de la información.



6. NORMATIVA VIGENTE

- ISO/IEC 27001: Gestión de Seguridad de la información.
- ISO/IEC 27002: Controles de Seguridad de la información.

7. REFERENCIAS

- CS GT SGTI PO 32 Control de Cambios al Ambiente Operativo

8. ASUNTOS ÉTICOS

Consultas o inquietudes relacionadas con temas éticos pueden ser realizadas al Oficial de cumplimiento (Gerente Legal) al fono: 322452429.

9. HISTORIAL DE REVISIONES Y MODIFICACIONES

Nº Versión	Fecha Vigencia	Comentario	Elaborado por	Revisado por	Aprobado por
0	17.06.2025	Creación del documento	OHS	JAD	AMB

CHILQUINTA servicios	**CHILQUINTA SERVICIOS S.A.** **TECHNOLOGY MANAGEMENT**		
Identification: CS GT SGTI I 03	**Creation Date:** 6/6/2025	**Date Reviewed/Modified:** NA	**Version:** 0
INSTRUCTIVE **WEB FILTER** **FILTRADO WEB**			

Reviewed by: JESUS AYALA Date: 17.06.2025	Approved by: ALFREDO MARTINEZ Date: 17.06.2025

1. OBJECTIVE

Describe the procedure to manage access and navigation control to websites from the corporate network, with the purpose of protecting information assets and technological systems against malicious content and ensure that the use of the Internet in the company complies with the security policies and acceptable use of resources of the organization.

2. SCOPE

Instructive applicable to the areas of the Subgerencia de Telecomunicaciones y TI administradoras de los dispositivos de red y de seguridad perimetral, which control the web browsing and use of the corporate network by the collaborators of the Grupo Empresas Chilquinta.

3. DEFINITIONS AND ABBREVIATIONS

Web filtering: Technical process by which a user's access to the Internet is controlled, allowing or denying the display of websites or online content based on a set of predefined rules.

Malware: Generic term for any type of software intentionally designed to infiltrate a device, damage systems or steal information without the owner's consent. It includes, but is not limited to, viruses, Trojans, ransomware, spyware and adware.

Blacklist: List of websites, domains or IP addresses that are explicitly denied access because they are considered malicious, inappropriate or unproductive.

White List: List of websites, domains, or IP addresses that are explicitly approved and allowed access, denying anything not on the list.

CSOC: Cybersecurity Operations Center.

4. RESPONSIBILITY AND AUTHORITY

POSITION	DESCRIPTION
Systems and Infrastructure	Implement, configure and maintain web filtering rules on edge security devices, ensuring the proper functioning of the rules without impact on business operations.
OT Telecommunications	Implement, configure and maintain filtering rules on the perimeter security devices established for the OT network, ensuring the proper functioning of the rules without impacting business operations.

Cybersecurity	Coordinate, with IT and TO edge firewall administrators, the updating of blocked site lists, whenever a new threat is identified. This update should be based on threat intelligence, vendor reports, publications in official cybersecurity sources, CSOC team notifications about detected vulnerabilities or emergency situations given the criticality of a detected incident. Approve or reject exception requests for access to restricted websites by ensuring that they have a valid business justification.

5. CONTENT

The control of web traffic generated from the Internet to the corporate network (or vice versa), together with the respective configuration and methods of filtering URLs and IP addresses, is detailed below in the following points:

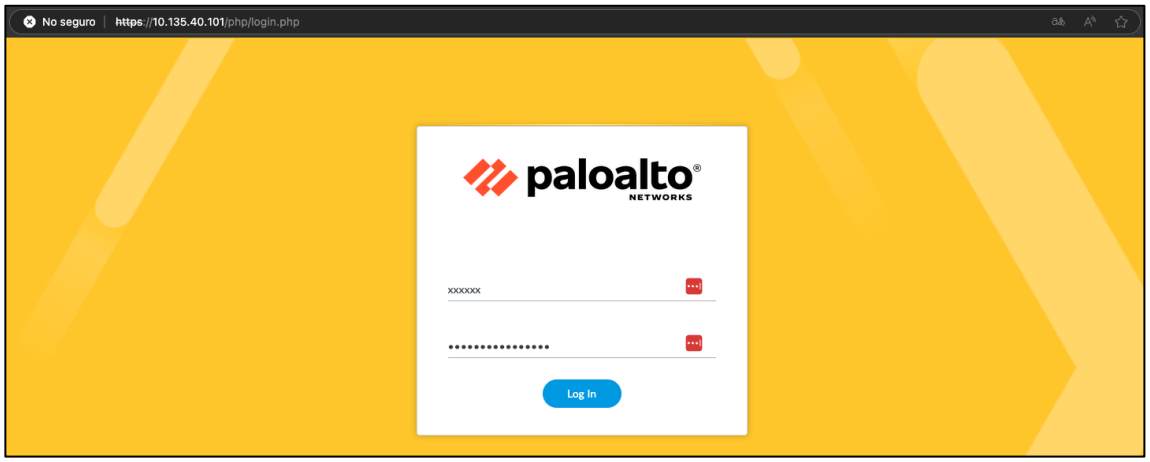
5.1. General Management

The overall management of the perimeter security devices is the responsibility of Systems and Infrastructure and Telecommunications TO, for the IT network and TO respectively. They ensure the implementation, configuration and maintenance of web filtering rules on the corresponding devices, ensuring the correct functioning of the rules without impact on business operations. Cybersecurity, for their part and together with the CSOC team, will support the recommendation of blocks to prevent cybersecurity risks, requesting the creation of blacklists to block both sites and IP addresses considered dangerous and whitelists, to guarantee access to essential and reliable resources. The above, through the corresponding perimeter firewall administrators. This approach ensures that filtering measures are dynamic, effective and tailored to the security needs of the organization, while minimizing any negative impact on business operations.

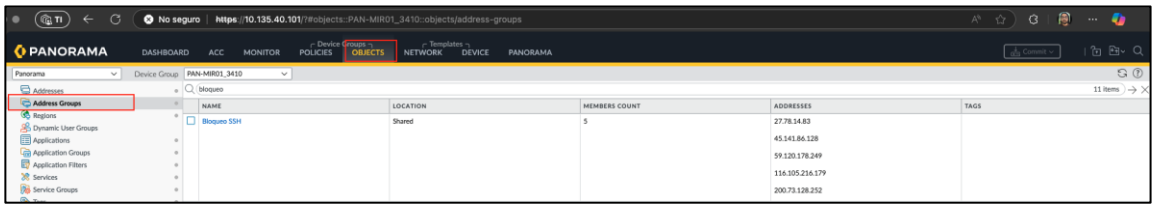
5.2. IT Web Filtering Configuration Process

The steps to block IP addresses and URLs categorized as risky using the filtering tools on edge devices are described below:

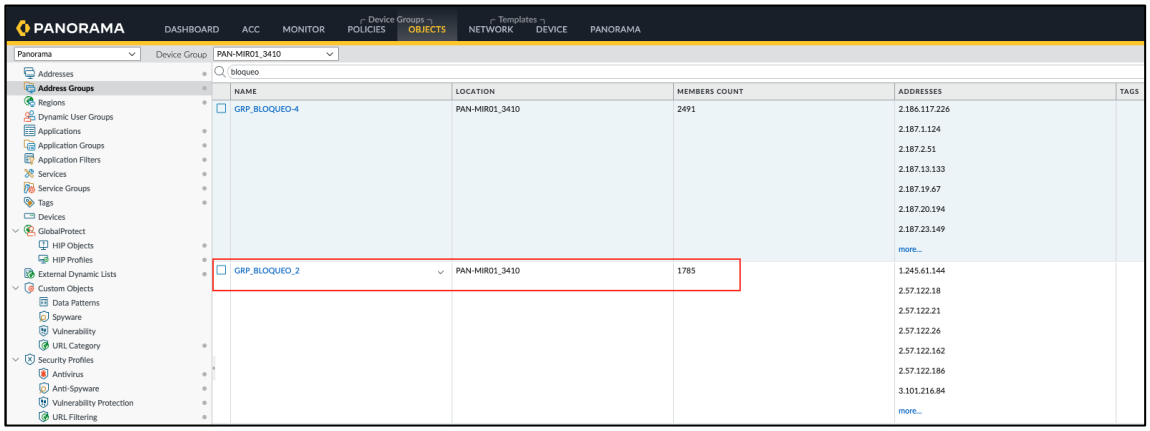
1. Access the Panorama security management platform, using the authorized credentials.



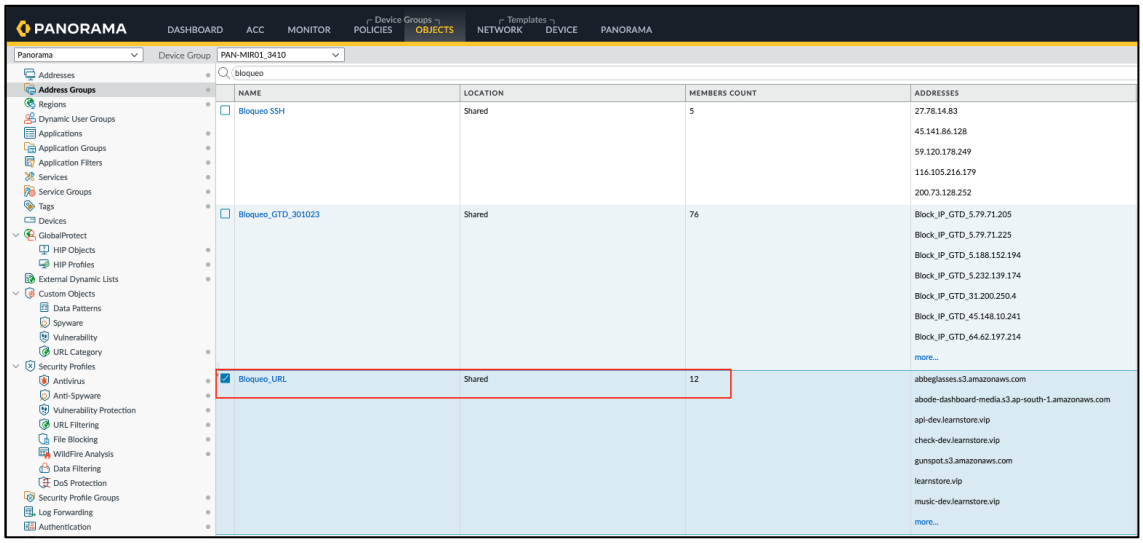
2. On the interface, go to the OBJECTS → Address Group section to manage lock groups.



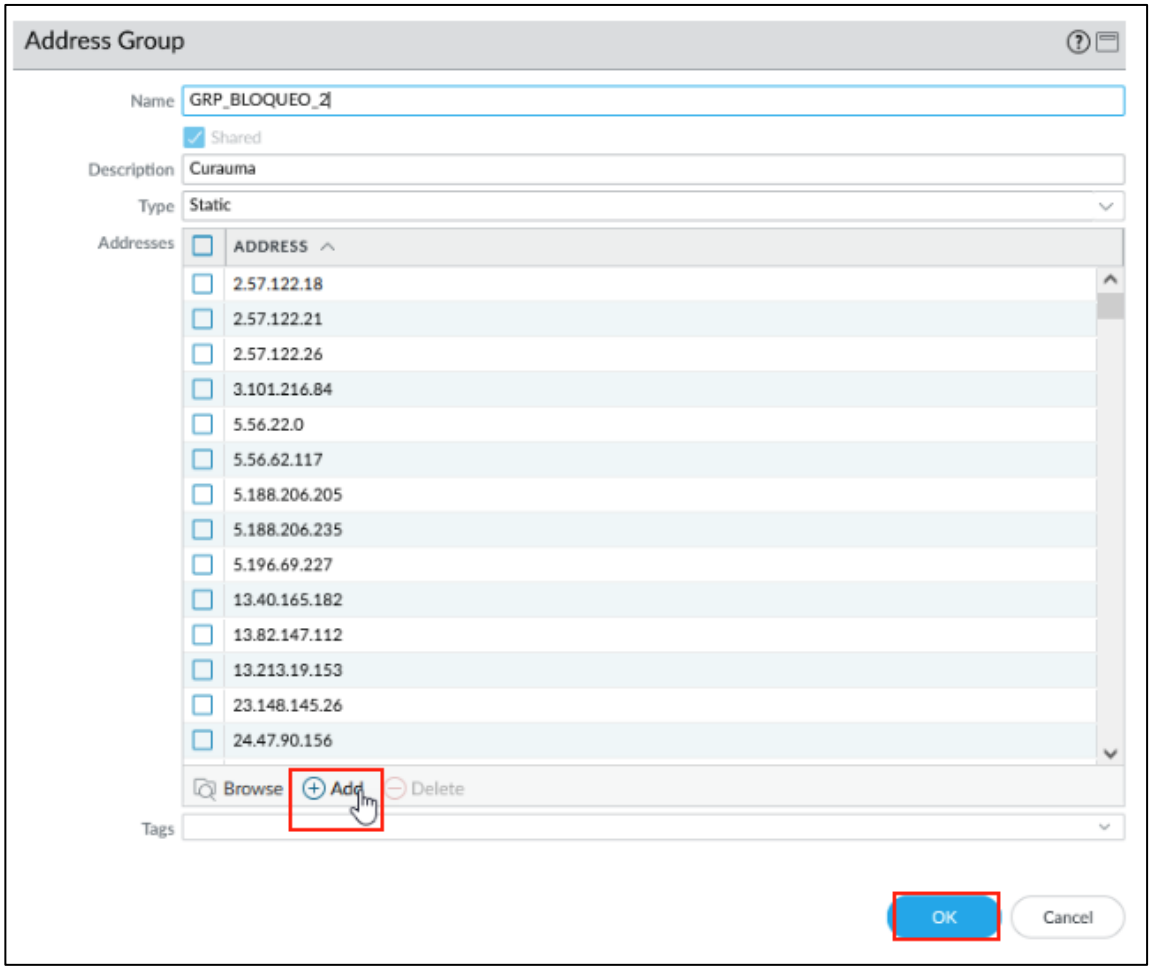
3. Select the appropriate lock group based on current capacity and usage. For example: GRP_Block_2 for IP address blocking.



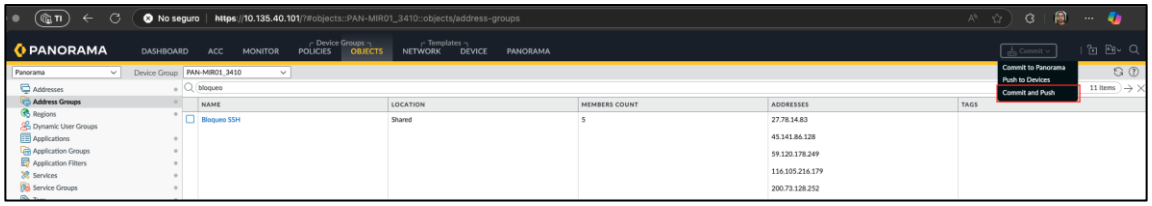
4. URL_BLOCK for URL blocking.



5. For both cases click on the target later in Add and proceed to add the IP address or URL that you want to block according to the corresponding policy. To finish press “OK”.



5.6. Once the additions are made, proceed to apply the policies in the firewall using the Commit and Push options to ensure that the changes take effect.



5.3. IT Web Filtering Categories

In order to strengthen preventive measures against access to websites classified as risky, a filtering system based on predefined categories is implemented that allow the blocking of unwanted content detailed below:

- abortion
- abused-drugs
- adult
- command and control
- copyright-infringement
- dating
- dynamic-dns
- extremism
- games
- hacking
- malware
- nudity
- parked
- phishing
- proxy-avoidance-and-anonymizers
- questionable
- shareware-and-freeware
- social-networking
- weapons
- web-advertisements
- web hosting

5.4. TO Web Filtering Configuration Process

In accordance with web filtering and access management policies, the rules configured in the firewalls of the DMZ and SCADA zones are intended to strictly control source, destination, and service traffic. Internet access is not allowed from computers located in the Trust zone, and a specific rule is established that blocks any attempt at traffic oriented to Internet browsing. Firewalls operate exclusively under approved access policies, ensuring a secure environment and aligned with established guidelines for information security.

6. CURRENT LEGISLATION

- ISO/IEC 27001: Information Security Management.
- ISO/IEC 27002: Information Security Controls.

7. REFERENCES

- CS GT SGTI PO 32 Control of Changes to the Operating Environment

8. ETHICAL ISSUES

Inquiries or concerns related to ethical issues can be made to the Compliance Officer (Legal Manager) at the phone number: 322452429.

9. REVISION AND MODIFICATION HISTORY

Version No	Effective Date	Comment	Prepared by	Reviewed by	Approved by
0	17.06.2025	Creating the document	OHS	JAD	AMB