

Configurar acciones de regla en una política basada en reglas para la administración de políticas web

Contenido

Introducción

Este documento describe cómo configurar acciones de regla en la política basada en reglas para la administración de políticas web.

Overview

La política basada en reglas utiliza conjuntos de reglas que coinciden en función de la identidad. Cada conjunto de reglas contiene reglas y cada regla coincide en función de la identidad, el destino y la programación. El sistema aplica conjuntos de reglas y reglas en orden descendente de prioridad. La identidad coincide con el primer conjunto de reglas aplicable y, a continuación, se aplica la primera regla que coincide con la identidad, el destino y la programación.

Una nueva función de la directiva basada en reglas permite a los administradores asignar, permitir, advertir, bloquear o aislar acciones a identidades de regla para destinos y aplicaciones específicos.

Para obtener instrucciones sobre cómo configurar conjuntos de reglas y reglas, refiérase a la documentación [Administración de la Política Web](#).

Acciones: Permitir, Permitir (seguro), Avisar, Bloquear y Aislar

Puede asignar una de estas acciones a reglas individuales de un conjunto de reglas:

Permitir (seguro)	Permite el acceso al destino o la aplicación a menos que se detecte un problema de seguridad. Aún se aplican las categorías de seguridad e inspección de archivos. Esta es la acción predeterminada para "permitir" a menos que seleccione una anulación de seguridad.
Permiso	Permite el acceso al destino o a la aplicación sin protección de seguridad. La configuración de seguridad no se puede reemplazar para una categoría de contenido completa.

Avisar	Presenta las identidades de regla con una página de advertencia y una opción para continuar, en lugar de bloquear el acceso.
Bloqueo	Deniega el acceso al destino. Las identidades de regla no pueden anular ni continuar más allá de la página de bloqueo.
Aislar	En lugar de bloquear las identidades de los terminales de destino, un navegador basado en la nube aloja la sesión de navegación de ese destino.

Establecer una acción de regla

Seleccione una acción de regla al crear o editar una regla.

1. Vaya a Web Policy > [Seleccione el conjunto de reglas apropiado].
2. Haga clic en Agregar regla o en Editar regla.

3. En el menú desplegable, seleccione Permitir, Avisar, Bloquear o Aislar para el destino.

Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
	Rule 1	Block	No Selections Add Identity	No Selections Add Destination	Any Day, Any Time Change Schedule No additional configuration applied CANCEL
1	Content Warn Sites	Allow - Security Enforced Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.			Any Day, Any Time No additional configuration applied ...
2	Allowed Sites	Warn Warns selected ruleset identities before allowing access to destinations.		ied ...	Any Day, Any Time No additional configuration applied ...
3	Security Block	Block Blocks selected ruleset identities from accessing destinations.		...	Any Day, Any Time No additional configuration applied ...
4	Security Block - Apps	Isolate Isolates selected ruleset identities' web requests in a virtual cloud-based browser.		plied ...	Any Day, Any Time No additional configuration applied ...

- El valor predeterminado para "permitir" aplica seguridad y bloquea el destino si se detecta una amenaza.
- Para permitir el acceso sin protección de seguridad, seleccione la opción para "anular la seguridad".

1	Marketing Access to So...	Allow Override Security	1 AD Group... Edit Identity	2 Applications ... Edit Destination	Any Day, Any Time Change Schedule	CANCEL SAVE
2	Block Games/Social	Block	All AD Groups All Networks	2 Categories ...	Mon-Fri 09:00-17:00	...

▲ Ruleset Settings

Para obtener más información, [visite el centro de aprendizaje de Umbrella para ver vídeos sobre las políticas basadas en reglas.](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).