

Cambio de las políticas web a las políticas basadas en reglas en general

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Comparación de reglas con un modelo de políticas antiguo](#)

[Acciones de transición](#)

[Temporización de transición](#)

[Cambios posteriores al 31 de marzo de 2021](#)

[SOPORTE TÉCNICO](#)

Introducción

Este documento describe el cambio de las políticas web a las políticas basadas en reglas en Cisco Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella Secure Internet Gateway (SIG).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

A partir del 31 de marzo de 2021, se puso a disposición de los clientes de Umbrella Secure Internet Gateway (SIG) una nueva función denominada "Política basada en reglas". Las políticas web pasaron de su modelo de políticas actual a un modelo de reglas. Las directivas web antiguas utilizaban un orden estático de operaciones para los componentes de políticas que representaban

uno o más destinos como, por ejemplo, las listas de destino de permitidos/bloqueados, la configuración de la aplicación y las categorías de contenido. El orden de las operaciones estáticas fue el siguiente:

1. Permitir listas de destino
2. Permitir configuración de aplicación
3. Bloques de categoría de seguridad
4. Bloquear listas de destino
5. Bloquear la configuración de la aplicación
6. Bloques de categorías de contenido

Otra restricción del modelo de política era que todas las identidades asociadas a la política recibirían la política. Por lo tanto, si un usuario o grupo de identidades necesita un cambio en su política web, se debe crear una nueva política web para ellas.

Sin embargo, el nuevo modelo de reglas deja el control total en manos del administrador. Se crearon algunas reglas que afectan a un grupo grande de identidades, mientras que otras reglas se aplican a una única identidad o a grupos más pequeños de identidades sin necesidad de mover estas identidades a una directiva independiente. Además, el administrador puede controlar fácilmente el orden de las operaciones simplemente reordenando las reglas.

Comparación de reglas con un modelo de políticas antiguo

Las nuevas reglas permiten a los usuarios finales realizar estas acciones mientras que el modelo anterior no puede:

- Invalidar la seguridad después de realizar una acción "Permitir"
- Programaciones de hora del día y día de la semana para la aplicación de reglas
- Realizar una acción de "advertencia" para las categorías de contenido
- Cree un navegador virtual que "aisle" las solicitudes de hosts a los destinos mediante las identidades definidas de la regla

The screenshot displays the Umbrella configuration interface. At the top, there is a header area with a menu icon, a text input field containing "Rule 1", and a dropdown menu currently set to "Block". To the right of the dropdown are two "No Selections" labels with "Add Identity" and "Add Destination" links. Further right, there is a "Change Schedule" link, a "SAVE" button with a trash icon, and the text "Any Day, Any Time" and "No additional configuration applied".

Below the header, there is a "Ruleset Settings" section with a sub-header "Ruleset settings affect the rules within their respective components before be". To the right of this section, there is a table with columns for "Ruleset Name", "Ruleset Identities", "Block Page", "Tenant Controls", and "File Analysis". Each row in the table has an "Edit" link on the right.

A dropdown menu is open, showing four action options:

- Allow - Security Enforced** (green checkmark icon): Allows selected ruleset identities access to destinations unless Umbrella detects a security issue. (checked)
- Warn** (yellow warning icon): Warns selected ruleset identities before allowing access to destinations.
- Block** (red minus icon): Blocks selected ruleset identities from accessing destinations.
- Isolate** (purple minus icon): Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

Screen_Shot_2021-05-05_at_3.51.38_PM.png

Para obtener más información, lea la documentación de configuración de Umbrella: [Gestionar la política web](#)

Acciones de transición

Había que crear un nuevo lenguaje de reglas en Umbrella para facilitar el procesamiento de las reglas, y con eso se creó una nueva base de datos para almacenar estas reglas. La transición tuvo dos pasos:

1. Los componentes de políticas existentes se copiaron de la antigua base de datos utilizada por las políticas web a la nueva base de datos utilizada por las reglas. Estos componentes se han eliminado de cualquier acción (como permitir o bloquear), ya que las reglas pueden llevar a cabo la acción. Por lo tanto, los componentes de políticas pasaron a ser agnósticos en cuanto a acciones. Sin embargo, los componentes copiados heredaron una etiqueta "permitir" o "bloquear" a su nombre para designar cuál era su intención en el sistema antiguo para el contexto. La configuración de la aplicación era un caso especial porque era única en el sentido de que incluía acciones de permitir y bloquear. Cualquier componente de la configuración de la aplicación que llevara a cabo ambas acciones se dividiría en dos: una para las aplicaciones permitidas y otra para las bloqueadas. Se crearon hasta 5 reglas para cada política web en transición. Si una política web no tenía todos los tipos de componentes de política configurados para ella, solo los componentes que se configuraron para esa política web que se transitaron, lo que dio como resultado menos reglas generadas automáticamente. Esta captura de pantalla es un ejemplo de una política web que se cambió con las 5 reglas generadas automáticamente:

Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration	
1	migrated allow destinatio...	Allow	Policy Identities	1 Destination List ...	Any Day, Any Time	...
2	migrated allowed applicat...	Allow	Policy Identities	Application List Applied ...	Any Day, Any Time	...
3	migrated block destinatio...	Block	Policy Identities	2 Destination Lists ...	Any Day, Any Time	...
4	migrated blocked applicat...	Block	Policy Identities	Application List Applied ...	Any Day, Any Time	...
5	migrated content categori...	Block	Policy Identities	Category List Applied ...	Any Day, Any Time	...

2. Una vez que el back end fue totalmente transicionado la nueva interfaz de usuario fue habilitada. Tenga en cuenta que, hasta que se habilite la nueva interfaz de usuario, cualquier usuario que inicie sesión en el panel podrá interactuar con la interfaz de usuario anterior.

- Los cambios realizados en las políticas web en esta etapa incompleta se guardaron cuando se habilitó la nueva interfaz de usuario.

Temporización de transición

Se le ha proporcionado una fecha y una hora en las que se ha producido la transición y ha sido retransmitido por su representante de éxito del cliente o por el sistema de mensajería de Umbrella en su panel. Una regla generada automáticamente sustituyó y priorizó cada componente de política configurado para todas las políticas web anteriores. Una vez que se habilitó la nueva interfaz de usuario, la transición se realizó sin problemas y, dado que las reglas generadas automáticamente reflejaban la misma acción y prioridad de las políticas web heredadas, no se produjo ningún cambio en el comportamiento al pasar de las políticas web a los conjuntos de reglas. No hubo tiempo de inactividad para la aplicación de políticas web durante esta transición.

Cambios posteriores al 31 de marzo de 2021

Durante la transición, los cambios realizados en las políticas web se capturaron en los nuevos conjuntos de reglas. Esto se debe a la copia de componentes de política existentes de la base de datos antigua a la nueva base de datos. Una vez completada la copia, se produjo un retraso en la activación de la nueva interfaz de usuario. Hasta que se habilitó la nueva interfaz de usuario, las políticas web estaban activas y cualquier cambio en dichas políticas web se escribía en la base de datos antigua y no se convertía en reglas.

SOPORTE TÉCNICO

Si trabaja con un gerente de éxito de clientes, un gerente de cuentas técnico o un gerente de prestación de servicios, estos podrán responder a preguntas. Informe sobre problemas técnicos a [Cisco Umbrella Support](#).

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).