

Configura azioni regola nei criteri basati su regole per la gestione dei criteri Web

Sommario

Introduzione

In questo documento viene descritto come configurare le azioni delle regole nei criteri basati su regole per la gestione dei criteri Web.

Panoramica

I criteri basati su regole utilizzano set di regole che corrispondono in base all'identità. Ogni set di regole contiene regole e ogni regola corrisponde in base all'identità, alla destinazione e alla pianificazione. Il sistema applica sia i set di regole che le regole in ordine di precedenza decrescente. L'identità viene associata al primo set di regole applicabile, quindi viene applicata la prima regola che corrisponde all'identità, alla destinazione e alla pianificazione.

Una nuova funzionalità dei criteri basati sulle regole consente agli amministratori di assegnare azioni di autorizzazione, avviso, blocco o isolamento alle identità delle regole per destinazioni e applicazioni specifiche.

Per istruzioni su come configurare i set di regole e le regole, consultare la documentazione [relativa alla gestione dei criteri Web](#).

Azioni: Consenti, Consenti (Protetto), Avvisa, Blocca e Isola

È possibile assegnare una di queste azioni a singole regole di un set di regole:

Consenti (protetto)	Consente l'accesso alla destinazione o all'applicazione a meno che non venga rilevato un problema di protezione. Controllo file e categorie di protezione sono ancora applicabili. Questa è l'azione predefinita per "consenti" a meno che non si selezioni una sostituzione di protezione.
Allow (Autorizza)	Consente l'accesso alla destinazione o all'applicazione senza protezione. Impossibile ignorare le impostazioni di protezione per un'intera categoria di contenuto.
Avvisa	Visualizza una pagina di avviso e un'opzione per continuare, in cui è possibile

	visualizzare le identità delle regole anziché bloccare l'accesso.
Block (Blocca)	Nega l'accesso alla destinazione. Le identità delle regole non possono sovrascrivere o continuare oltre la pagina di blocco.
Isolare	Anziché bloccare le identità dagli endpoint di destinazione, un browser basato su cloud ospita la sessione di esplorazione per tale destinazione.

Impostazione di un'azione regola

Selezionare un'azione regola quando si crea o si modifica una regola.

1. Andare a Criterio Web > [Selezionare il set di regole appropriato].
2. Fare clic su Aggiungi regola o su Modifica regola.

The screenshot shows the Cisco Umbrella 'Web Policy' management page. On the left, the 'Web Policy' menu item is highlighted in the sidebar. The main content area shows a table of rules for the 'Block Threats and Social' ruleset. The table has columns for Priority, Rule Name, Rule Action, Identities, Destinations, and Rule Configuration. Two rules are listed: 'Marketing Access to Social Media' (Allow) and 'Block Games/Social' (Block). Annotations with red arrows point to the 'ADD RULE' button, the 'EDIT RULE' button in the rule configuration dropdown, and the three-dot menu icon used to expand rule settings.

3. Nel menu a discesa, selezionare Consenti, Avvisa, Blocca, o Isola per la destinazione.

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. Warn Warns selected ruleset identities before allowing access to destinations. Block Blocks selected ruleset identities from accessing destinations. Isolate Isolates selected ruleset identities' web requests in a virtual cloud-based browser.			Any Day, Any Time No additional configuration applied ...
2	Allowed Sites			ied ...	Any Day, Any Time No additional configuration applied ...
3	Security Block			...	Any Day, Any Time No additional configuration applied ...
4	Security Block - Apps			plied ...	Any Day, Any Time No additional configuration applied ...

- Se viene rilevata una minaccia, per impostazione predefinita viene applicata la protezione e viene bloccata la destinazione.
- Per consentire l'accesso senza protezione, selezionare l'opzione per "ignorare la protezione".

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

Per ulteriori informazioni, [visita l'Umbrella Learning Hub per video sui criteri basati sulle regole](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).