Usa criteri basati su regole in Umbrella Secure Internet Gateway

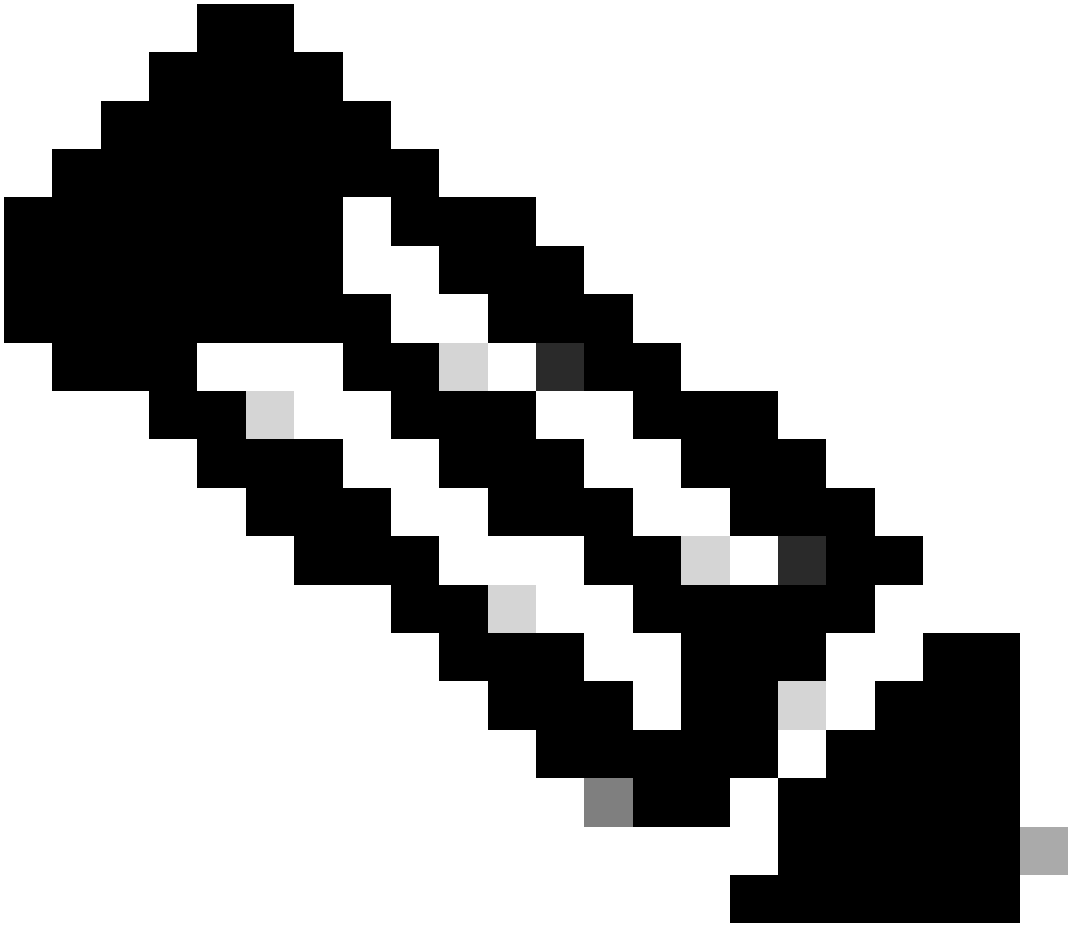
Sommario

Introduzione

Questo documento descrive la funzionalità Criteri basati su regole di Umbrella Secure Internet Gateway (SIG) e risponde alle domande comuni.

Panoramica sulla transizione dei criteri basata su regole

Il 31 marzo 2021, la politica basata su regole è diventata disponibile per i clienti Umbrella SIG. I clienti Umbrella SIG passano gradualmente da criteri Web preesistenti a criteri basati su regole nel corso di diverse settimane. I clienti ricevono notifica della data e della finestra di transizione tramite il dashboard Umbrella. Questa modifica non influisce sui clienti Umbrella DNS o sulle impostazioni dei criteri DNS.



Nota: Questo documento è stato concepito per rispondere a domande rapide sia da utenti nuovi che da utenti esperti di Umbrella in merito al passaggio da policy Web legacy a set di regole. Per una documentazione più dettagliata, vedere la Guida per l'amministratore Umbrella aggiornata.

Domande frequenti

Informazioni sui criteri Web

Un criterio Web è l'insieme di tutti i set di regole di un'organizzazione Umbrella.

Definizione di set di regole

Un set di regole è un contenitore logico per un set di regole e impostazioni che vengono applicate a tali regole all'interno del set di regole.

Perché utilizzare i set di regole

Un set di regole può rappresentare un'area geografica, un gruppo di uffici o utenti specifici che richiedono una gestione distinta dal resto dell'organizzazione.

Impostazioni configurabili in un set di regole

Configurare le impostazioni specificate nei set di regole. Queste impostazioni si applicano solo alle regole all'interno di tale set di regole:

- Nome set di regole
- Identità set di regole
- Blocca pagina
- Controlli tenant
- Analisi file
- Controllo tipo di file
- Controllo HTTPS
- File PAC
- Registrazione set di regole
- SAML
- Impostazioni protezione

Per maggiori informazioni, vedere: Configurare un set di regole.

Cosa sono le regole?

Una regola è un'istruzione che definisce l'azione da eseguire quando un'identità e una destinazione corrispondono.

Perché utilizzare le regole

Le regole consentono un controllo dell'accesso granulare o ampio. Una regola a bassa priorità, ad esempio, può bloccare un'ampia gamma di siti Web per tutti gli utenti, mentre una regola a priorità più alta può consentire l'accesso a siti specifici per un gruppo di destinazione, il tutto all'interno dello stesso set di regole.

Identità supportate

Sia i set di regole che le regole supportano le identità seguenti:

- Utente AD
- Gruppo AD
- Computer in roaming (endpoint AnyConnect)
- Rete interna
- Tunnel
- Rete

Quali destinazioni sono supportate?

Le regole supportano le seguenti destinazioni:

- Categorie di contenuti
- Impostazioni applicazione
- Elenchi di destinazione

Azioni supportate

Le regole supportano le azioni seguenti:

- Allow (Autorizza)
- Block (Blocca)
- Avvisa
- Isolare

Impostazioni configurabili in una regola

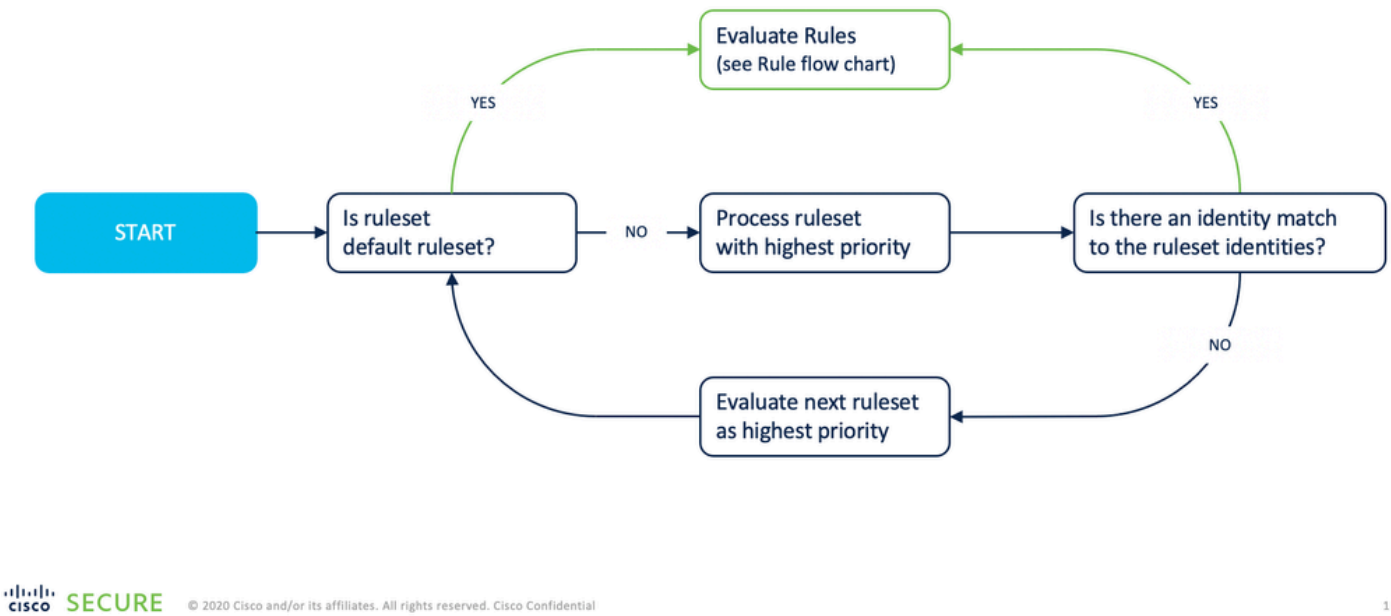
Le regole possono essere configurate con:

- Nome regola
- Azione
- Identità
- Destinazione
- Programmazione ora/giorno

Per ulteriori informazioni, vedere Aggiungere regole a un set di regole.

Valutazione dei set di regole

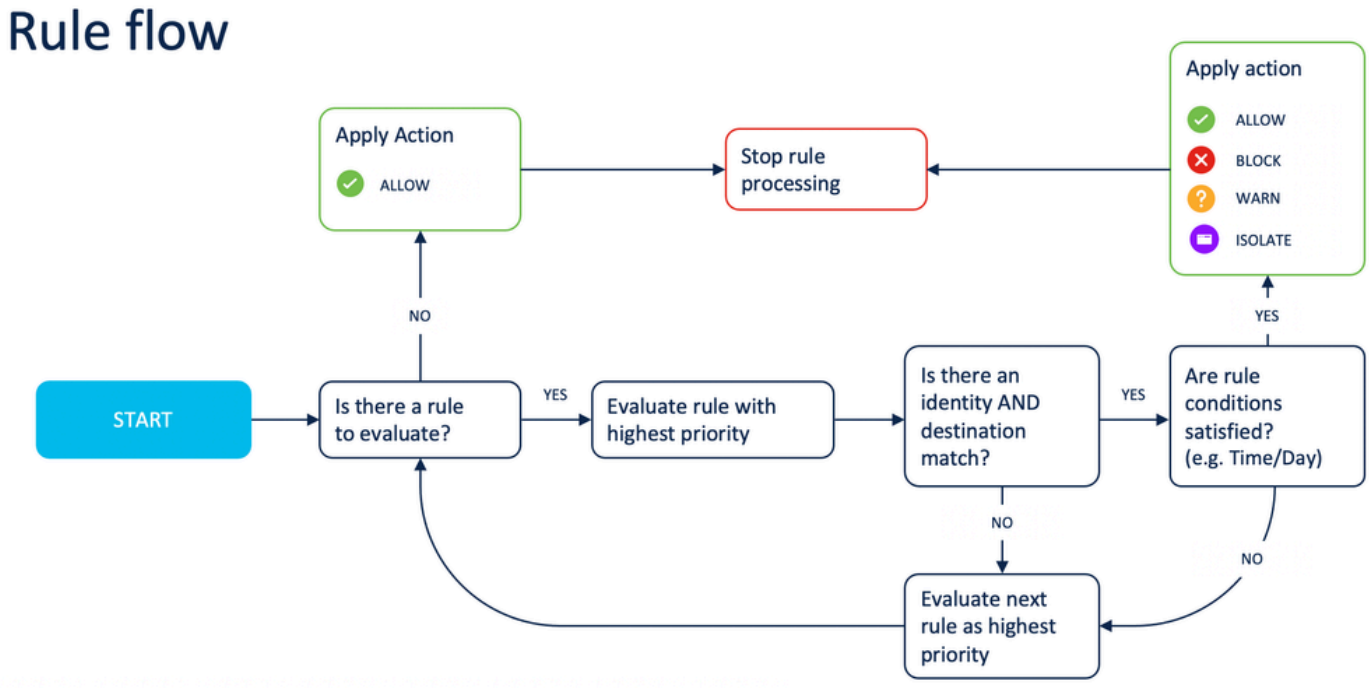
I set di regole vengono valutati in una gerarchia dall'alto verso il basso in base alle identità disponibili. Il set di regole con la priorità più alta viene valutato per primo. Se non si verifica alcuna corrispondenza, viene valutato il set di regole con priorità più alta successivo e così via. Se in un set di regole non si verifica alcuna corrispondenza, viene applicato il set di regole predefinito.



Screen_Shot_2021-04-07_at_2.37.22_PM.png

Modalità di valutazione delle regole

Le regole all'interno di un set di regole selezionato vengono valutate dall'alto verso il basso in base alle identità e alle destinazioni disponibili. Una regola viene applicata solo quando un'identità e una destinazione corrispondono. Viene quindi applicata l'azione configurata per la regola (Consenti, Blocca, Avvisa o Isola).



Screen_Shot_2021-05-10_at_10.3.03_AM.png

Una regola è valida per la stessa identità corrispondente al set di regole?

Una regola può corrispondere alla stessa identità del set di regole, ma ciò non avviene sempre. Quando Umbrella riceve una richiesta Web, raccoglie tutte le identità presenti. Le regole all'interno del set di regole selezionato vengono quindi valutate in base allo stesso pool di identità e devono corrispondere a una destinazione. L'identità effettiva utilizzata da una regola può essere diversa dall'identità corrispondente al set di regole.

Esempio:

- JDoe funziona dalla rete B.
- L'organizzazione dispone dei seguenti set di regole:
  - Set di regole 1: Rete A
  - Set di regole 2: Rete B
  - Set di regole 3: Rete C

Solo il set di regole 2 si applica a JDoe. Nel set di regole 2:

- Regola 1: Identity AsMith, Dominio di destinazione B, Azione consentita
- Regola 2: Identity Marketing, Destinazione SomeSocialApp, Azione Consenti
- Regola 3: Rete di identità B, Categorie di contenuto di destinazione (Dominio B, SomeSocialApp), Blocco azione

Risultati:

- JDoe è bloccato dal dominio B (regola 3).
- JDoe, in qualità di membro di Marketing, è autorizzato ad accedere ad SomeSocialApp (regola 2).

L'ordine di valutazione delle regole determina il risultato. Le identità più specifiche (utente, gruppo) vengono posizionate prima di quelle meno specifiche (rete). Vince il primo incontro.

Come è possibile conoscere la regola utilizzata in una transazione?

Il report Ricerca attività acquisisce sia il set di regole che la regola utilizzata in una transazione. Queste informazioni sono disponibili in Dettagli completi per le richieste URL. Il campo è attualmente etichettato "Policy/Rule" ma viene modificato in "Ruleset/Rule" quando i clienti passano da criteri Web legacy a set di regole.

Dove posso trovare la documentazione online per i set di regole?

Fare riferimento alla Umbrella Admin Guide Manage Web Policies (Guida dell'amministratore Umbrella).

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).