Gebruik op regels gebaseerd beleid in Umbrella Secure Internet Gateway

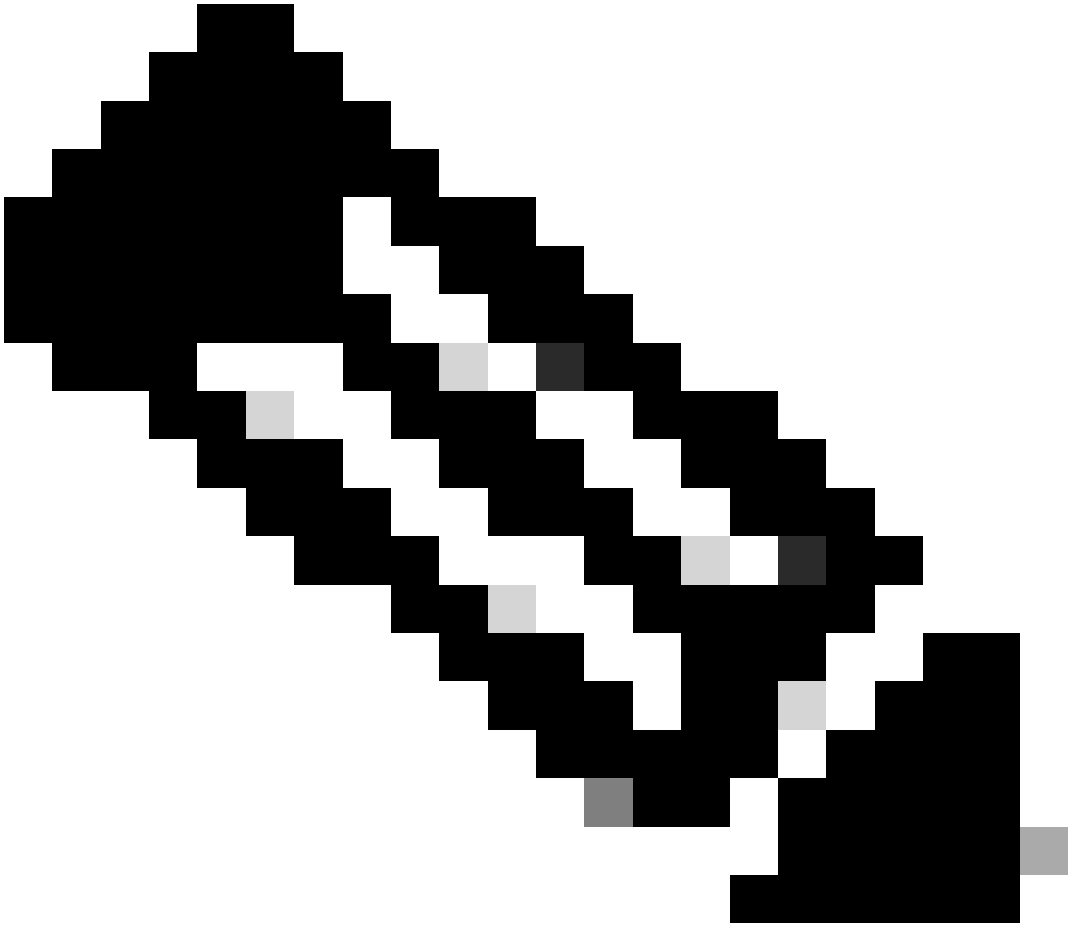
Inhoud

Inleiding

In dit document wordt de beleidsfunctie op basis van regels beschreven in Umbrella Secure Internet Gateway (SIG) en worden veelgestelde vragen beantwoord.

Overzicht van een op regels gebaseerde beleidstransitie

Op 31 maart 2021 werd Rule-Based Policy algemeen beschikbaar voor Umbrella SIG-klanten. Umbrella SIG-klanten worden geleidelijk overgeschakeld naar een op regels gebaseerd beleid van het bestaande webbeleid gedurende enkele weken. Klanten ontvangen een melding van de overgangsdatum en het venster via het Umbrella-dashboard. Deze wijziging heeft geen invloed op Umbrella DNS-klanten of DNS-beleidsinstellingen.



Opmerking: deze veelgestelde vragen zijn bedoeld om snelle vragen van zowel nieuwe als ervaren Umbrella-gebruikers aan te pakken over de verschuiving van verouderd webbeleid naar regelsets. Voor meer gedetailleerde documentatie, zie de bijgewerkte Umbrella Admin Guide.

Veelgestelde vragen

Wat is een webbeleid?

Een webbeleid is het verzamelen van alle regels in een overkoepelende organisatie.

Wat is een regelset?

Een ruleset is een logische container voor een reeks regels en instellingen die van toepassing zijn op die regels binnen de ruleset.

Waarom regelsets gebruiken?

Een regelset kan een specifieke geografie, groep kantoren of gebruikers vertegenwoordigen die een ander management nodig hebben dan de rest van de organisatie.

Welke instellingen kunnen worden geconfigureerd in een regelset?

Configureer de opgegeven instellingen in de regelsets. Deze instellingen zijn alleen van toepassing op de regels binnen die regelset:

- Naam regelset
- Ruleset-identiteiten
- Blokpagina
- Bedieningselementen huurder
- Bestandsanalyse
- Bestandstypecontrole
- HTTPS-inspectie
- PAC-bestand
- Regelset-logboekregistratie
- SAML
- Beveiligingsinstellingen

Zie voor gedetailleerde uitleg: Een regelset configureren.

Wat zijn regels?

Een regel is een instructie die bepaalt welke actie moet worden ondernomen wanneer een identiteit en bestemming beide overeenkomen.

Waarom regels gebruiken?

Regels maken gedetailleerde of brede toegangscontrole mogelijk. Een regel met lage prioriteit kan bijvoorbeeld een breed scala aan websites voor alle gebruikers blokkeren, terwijl een regel met hogere prioriteit toegang kan bieden tot specifieke sites voor een doelgroep, allemaal binnen dezelfde regelset.

Welke identiteiten worden ondersteund?

Zowel de regels als de regels ondersteunen deze identiteiten:

- AD-gebruiker
- AD-groep
- Zwervende computer (AnyConnect-eindpunt)
- Intern netwerk
- Tunnel
- netwerk

Welke bestemmingen worden ondersteund?

Regels ondersteunen deze bestemmingen:

- Inhoudcategorieën
- Toepassingsinstellingen
- Bestemmingslijsten

Welke acties worden ondersteund?

Regels ondersteunen deze acties:

- Allow (toestaan)
- Block (blokkeren)
- waarschuwen
- isoleren

Welke instellingen kunnen in een regel worden geconfigureerd?

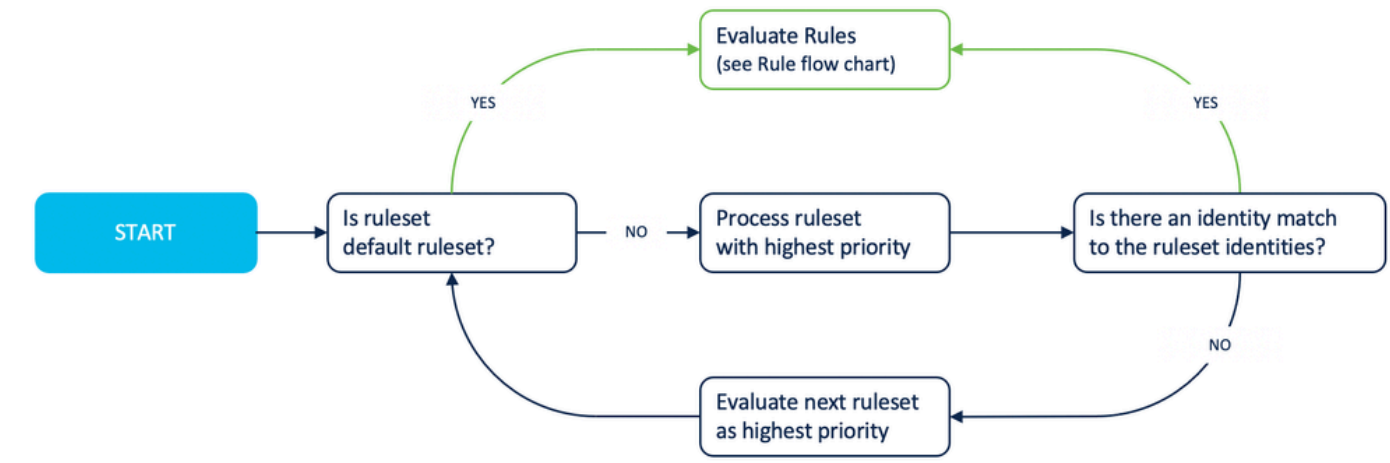
Regels kunnen worden geconfigureerd met:

- Naam regel
- Actie
- identiteit
- Bestemming
- Tijdschema/dag

Zie Regels toevoegen aan een regelset voor meer informatie.

Hoe worden de regels geëvalueerd?

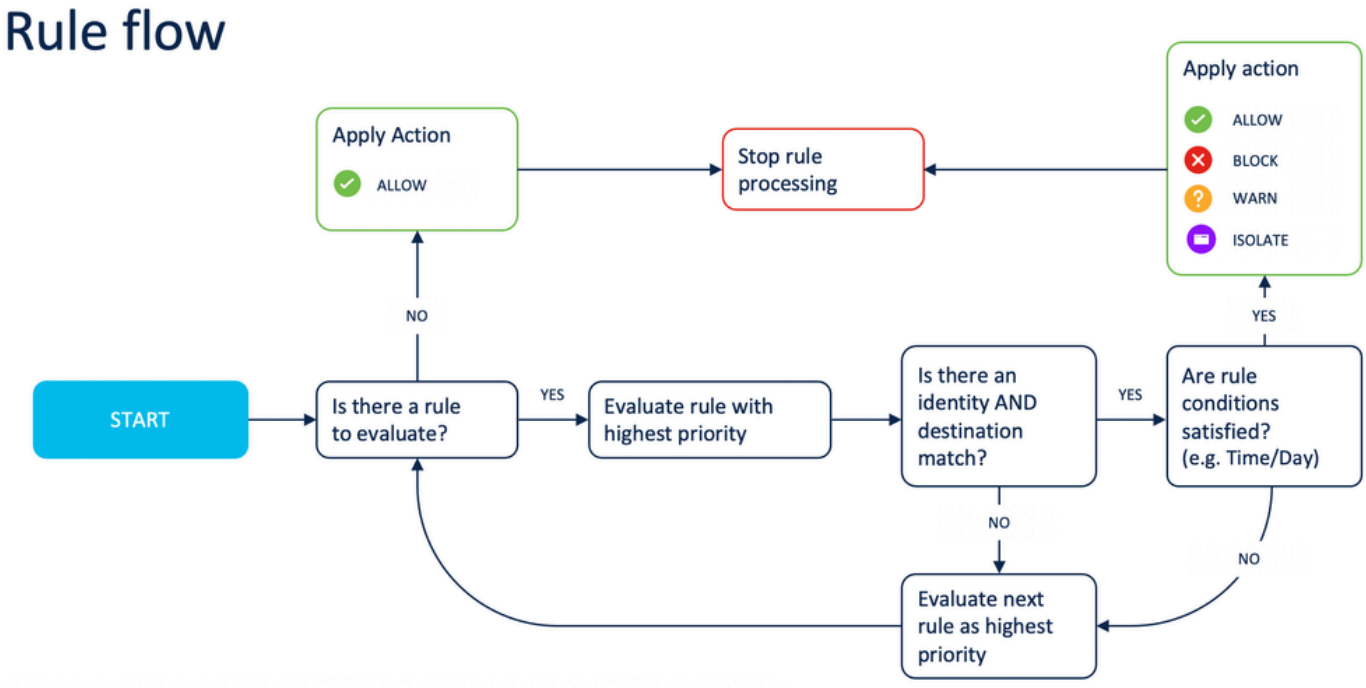
Regelsets worden geëvalueerd in een top-down hiërarchie op basis van beschikbare identiteiten. De regels met de hoogste prioriteit worden eerst geëvalueerd. Als er geen match optreedt, wordt de volgende regel met de hoogste prioriteit geëvalueerd, enzovoort. Als er geen overeenkomst in een regelset optreedt, is de standaardregelset van toepassing.



Screen_Shot_2021-04-07_at_2.37.22_PM.png

Hoe worden de regels geëvalueerd?

Regels binnen een geselecteerde regelset worden top-down geëvalueerd aan de hand van beschikbare identiteiten en bestemmingen. Een regel is alleen van toepassing wanneer zowel een identiteit als een bestemming overeenkomen. De geconfigureerde actie voor de regel (toestaan, blokkeren, waarschuwen of isoleren) wordt vervolgens toegepast.



Screen_Shot_2021-05-10_at_10.33.03_AM.png

Is een regel van toepassing op dezelfde identiteit die overeenkomt met de regelset?

Een regel kan overeenkomen met dezelfde identiteit als de regelset, maar dit is niet altijd het geval. Wanneer Umbrella een webverzoek ontvangt, verzamelt het alle aanwezige identiteiten. Regels binnen de geselecteerde regelset worden vervolgens geëvalueerd aan de hand van dezelfde pool van identiteiten en moeten ook overeenkomen met een bestemming. De werkelijke identiteit die door een regel wordt gebruikt, kan verschillen van de identiteit die overeenkomt met de regelset.

Voorbeeld:

- JDoe werkt vanuit Netwerk B.
- De organisatie heeft de volgende regels:
    - Regel 1: Netwerk A
    - Regelset 2: Netwerk B
    - Regelset 3: Netwerk C

Alleen Ruleset 2 is van toepassing op JDoe. Binnen Ruleset 2:

- Regel 1: Identiteit Amith, Bestemmingsdomein B, Actie toestaan
- Regel 2: Identiteitsmarketing, Bestemming SommigeSocialApp, Actie Toestaan
- Regel 3: Identiteitsnetwerk B, Bestemmingsinhoudscategorieën (domein B, sommige sociale app), Actieblok

Resultaten:

- JDoe is geblokkeerd in domein B (regel 3).
- JDoe, als lid van Marketing, heeft toegang tot SomeSocialApp (Regel 2).

Regel evaluatie volgorde bepaalt de uitkomst. Meer specifieke identiteiten (gebruiker, groep) worden geplaatst voor minder specifieke (netwerk). De eerste wedstrijd wint.

Hoe weet ik welke regel is gebruikt in een transactie?

In het rapport Activiteit zoeken worden zowel de regelset als de regel vastgelegd die in een transactie wordt gebruikt. Deze informatie vindt u onder Volledige details voor URL-aanvragen. Het veld heeft momenteel het label "Beleid/Regel", maar verandert in "Regelset/Regel" als klanten overstappen van het oude webbeleid naar de regels.

Waar vind ik online documentatie voor regelsets?

Raadpleeg de Umbrella Admin Guide Beheer webbeleid.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.