Begrijp de beperkingen van de Umbrella DNS Policy Tester

Inhoud

Inleiding

Dit document beschrijft de beperkingen en beperkingen van de Umbrella DNS Policy Tester.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- beveiligde webgateway
- beveiligde internetgateway
- Paraplu (DNS-laag toegevoegd)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

De Umbrella Policy Tester kan worden gebruikt om te bepalen of een bepaalde bestemming kan worden geblokkeerd of toegestaan door Cisco bij een bezoek van een bepaalde identiteit. Er zijn

echter een paar omstandigheden waaronder de Policy Tester momenteel geen nauwkeurige (of enige) informatie voor een bepaalde bestemming kan retourneren. In dit artikel worden deze beperkingen beschreven.

Technische details

Het algemene overzicht van de Policy Tester is te vinden in de overkoepelende documentatie voor de Umbrella Policy Tester.

Deze resultaten van de beleidstester kunnen onjuist zijn:

beveiligde webgateway

- niet ondersteund

beveiligde internetgateway

- niet ondersteund

Paraplu (DNS-laag toegevoegd)

- Bestemmingen die worden geblokkeerd door de Intelligente proxy kunnen door de Beleidstester ten onrechte als "Toegestaan" worden gerapporteerd. Dit omvat ook:
  - Aangepaste URL-blokkeringslijsten
  - Proxy-blocklist of greylist domeinen
  - Blokken voor bestandsinspectie
- Bestemmingstype "Toepassing" (zoals Dropbox, Box, Facebook, enz. op naam) die zijn geblokkeerd, kunnen door de Policy Tester onjuist worden gerapporteerd als "Toegestaan".
- Wanneer een netwerk ook wordt toegepast op een webbeleid, kan het webbeleid onjuist worden weergegeven. De beleidstester wordt momenteel niet ondersteund voor netwerken die ook deel uitmaken van het webbeleid.
- Tests die niet alle relevante identiteitsgegevens leveren, kunnen onjuiste resultaten opleveren. Een zwervende computer waarop de Active Directory (AD)-integratie is ingeschakeld terwijl deze zich op een beveiligd netwerk bevindt: de test kan mislukken als alleen de AD-gebruiker wordt geleverd, maar de zwervende computer beleidsbeslissingen wint.
- Bestemmingen die zijn geblokkeerd vanwege inhoudscategorieën kunnen worden weergegeven als toegestaan als ze zijn ingevoerd met hoofdletters of hoofdletters. Als u bijvoorbeeld de categorie "naakt" blokkeert, kan het domein playboy.com worden weergegeven als geblokkeerd terwijl Playboy.com wordt weergegeven als toegestaan.
- "Dynamische DNS"-bestemmingen kunnen worden geblokkeerd als die beveiligingscategorie is geselecteerd, maar kunnen door de beleidstester onjuist worden gerapporteerd als "Toegestaan".
- Bestemmingen die zijn toegestaan door toepassingsbesturing kunnen onjuist worden weergegeven als geblokkeerd in de Beleidstester.
- Bestemmingen die zijn geblokkeerd door de Umbrella Enforcement API voor aangepaste integraties kunnen door de Policy Tester onjuist worden gerapporteerd als "Toegestaan".

- Bestemmingen die worden geblokkeerd door de overkoepelende AMP Threat Grid Integration kunnen door de Policy Tester ten onrechte worden gerapporteerd als "Toegestaan".
- Bestemmingen die zijn geblokkeerd vanwege een CNAME kunnen door de Policy Tester onjuist worden gerapporteerd als "Toegestaan".
- Bestemmingen die IP-adressen zijn, worden momenteel niet ondersteund in de Beleidstester.
- Bestemmingen die URL's zijn, worden momenteel niet ondersteund in de Beleidstester.
- Bestemmingen die zijn geblokkeerd voor het oplossen van een kwaadaardig IP-adres, kunnen door de Policy Tester ten onrechte worden gemeld als "Toegestaan".
- "Potentieel schadelijke" bestemmingen kunnen worden geblokkeerd als die beveiligingscategorie is geselecteerd, maar kunnen door de beleidstester ten onrechte als "toegestaan" worden gerapporteerd.
- Bestemmingen waarbij geautomatiseerde DDOS-beveiligingen DNS tijdelijk beletten om te reageren voor het betreffende domein, zijn niet zichtbaar door de Policy Tester.
- Bestemmingen die zijn geblokkeerd onder de inhoudscategorie "Duitse Jeugdbescherming" kunnen door de Beleidstester ten onrechte als "Toegestaan" worden gerapporteerd. Deze categorie kan niet worden vermeld in de resultaten van de beleidstester.
- Bestemmingen die zijn geblokkeerd vanwege de beveiligingsclassificatie "Cryptocurrency" kunnen onjuist worden weergegeven als "Toegestaan", zelfs als ze zijn geblokkeerd door beveiligingsinstellingen.
- Blokkeringen als gevolg van DNS Tunneling VPN-categorieën kunnen de resultaten niet correct weergeven in de Beleidstester. Ze tonen ten onrechte zoals toegestaan.
- Chromebook-apparaten achter een virtueel toestel kunnen een onjuist beleid weergeven. Identiteitsblokken van Chromebooks (UCC) kunnen het toegepaste beleid van Virtual Appliance overschrijven, maar blokken van Virtual Appliance kunnen het UCC overschrijven.
- Leden van AD-groepen waarin de groep niet is gesynchroniseerd met Umbrella (inclusief groepen die deel uitmaken van een bovenliggend of onderliggend domein en groepen die lid zijn van groepen die niet selectief zijn gesynchroniseerd met Umbrella) kunnen worden weergegeven als overeenkomend met het beleid dat wordt weergegeven in de Beleidstester. Het gebruikersbeleid is niet van toepassing in de cloud. Bevestig door de enkele gebruiker toe te voegen aan uw beleid en bevestig dat het correct van toepassing is binnen 5 minuten.
- Bestemmingen die op de lijst Interne domeinen staan. De Beleidstester neemt de lijst Interne domeinen niet mee bij het rapporteren van een testresultaat.
- Categorieën die niet worden weergegeven op de OpenDNS Community-domeincoderingssite, worden niet gegarandeerd om de juiste categorie op de Policy Tester weer te geven. Slechts één bron van categorisaties wordt weergegeven.
- De Policy Tester is beperkt tot het tonen van 20 resultaten bij het zoeken naar een identiteit.
- Een AD-gebruiker is lid van een groep Geneste AD, maar alleen de bovenliggende AD-groep wordt geselecteerd in identiteiten bij het maken van DNS-beleid. Policy Tester-zoekopdrachten kunnen niet overeenkomen met het juiste beleid.
- Bestemmingen in de lijst met beschermde machtigingen kunnen door de Policy Tester onjuist worden gerapporteerd als "Geblokkeerd".

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.