Handhaaf Umbrella DNS en voorkom bypass met firewallregels

Inhoud

Inleiding

In dit document wordt beschreven hoe u kunt voorkomen dat DNS wordt omzeild en hoe u overkoepelende DNS-beveiligingen kunt afdwingen met behulp van firewallregels en netwerkbeleid.

Voorwaarden

- Netwerkfirewall
- Firewalltoegangsrechten
- Kennis van firewallconfiguratie

Het handhaven van Umbrella DNS—meest voorkomende methode

Met de meeste routers en firewalls kunt u al het DNS-verkeer afdwingen via poort 53, waarbij alle netwerkapparaten de DNS-instellingen moeten gebruiken die op de router zijn gedefinieerd, die moeten verwijzen naar Umbrella DNS-servers.

De voorkeursaanpak is om alle DNS-verzoeken van niet-Umbrella IP-adressen door te sturen naar de Umbrella DNS IP's die hieronder worden vermeld. Deze methode stuurt DNS-verzoeken transparant door en voorkomt dat handmatige DNS-configuratie eenvoudig mislukt.

U kunt ook een firewallregel maken om DNS (TCP/UDP) alleen toe te staan voor Umbrella DNS-servers en al het andere DNS-verkeer naar andere IP-adressen te blokkeren.

Voorbeeld van firewallregel

1. Voeg deze regel toe aan de randfirewall:
    - Inkomende en uitgaande TCP/UDP toestaan naar **208.67.222.222** of **208.67.220.220** op poort 53.
    - BlockTCP/UDP inkomende en uitgaande naar alle IP-adressen op poort 53.

De allow-regel voor Umbrella DNS heeft voorrang op de block-regel. DNS-verzoeken aan Umbrella zijn toegestaan, terwijl alle andere DNS-verzoeken worden geblokkeerd.

Configureer, afhankelijk van uw firewallconfiguratie-interface, een afzonderlijke regel voor elk protocol of een enkele regel voor zowel TCP als UDP. Pas de regel toe op het netwerkrandapparaat. U kunt ook een soortgelijke regel toepassen op softwarefirewalls op werkstations, zoals de ingebouwde firewall in Windows of macOS.

Als u de zwervende client en het groepsbeleid van Active Directory gebruikt, raadpleegt u de documentatie over het vergrendelen van de Enterprise Roaming Client met behulp van groepsbeleid.

Handhaving tegen DNS over HTTPS (DoH)

Aanbevolen configuratie

1. Schakel in Umbrella de categorieën Proxy / Anonimizer en DoH / DoTcontent in.
2. Blokkeer de IP-adressen van bekende DoH-providers op uw firewall.

Details en achtergrond

Umbrella ondersteunt het`use-application-dns.net`domein, zoals gedefinieerd door Mozilla, om te voorkomen dat Firefox DoH standaard inschakelt. Voor informatie over Firefox en DoH, zie de bijbehorende documentatie.

Zelfs na het blokkeren van alternatieve DNS-providers, kan DNS nog steeds worden omzeild met DoH. Een lokale DNS-resolver vertaalt DNS-verzoeken naar HTTPS en verzendt ze naar een eindpunt met behulp van JSON of POST/GET. Dit verkeer vermijdt meestal DNS-inspectie.

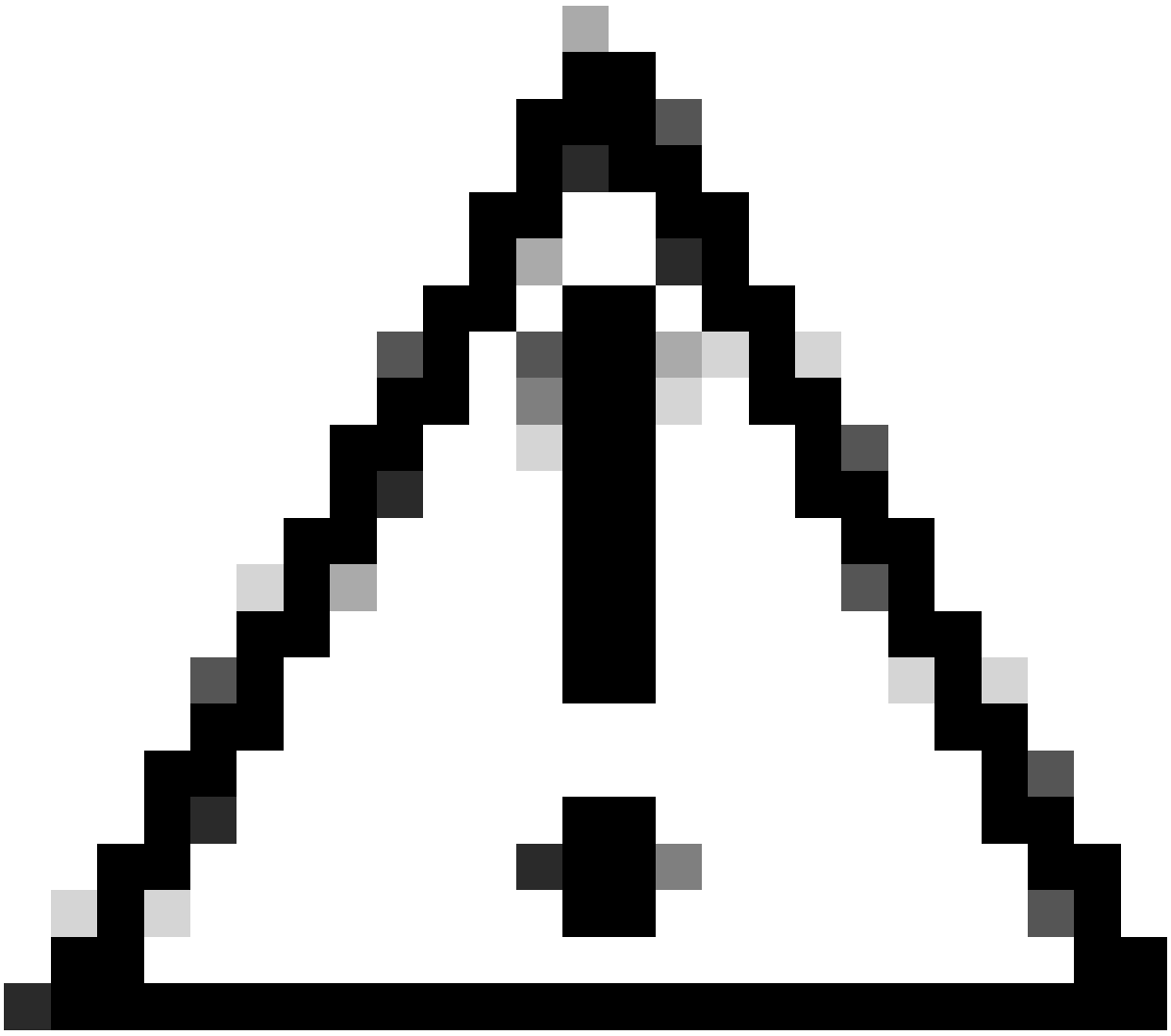
Omdat DoH kan worden gebruikt om Umbrella te omzeilen, bevat Umbrella bekende DoH-servers

in de inhoudscategorie Proxy / Anonymizer. Dit mechanisme heeft een aantal beperkingen:

- Het kan geen gloednieuwe DoH-providers blokkeren die nog niet bekend zijn.
- Het kan DoH niet blokkeren die rechtstreeks via het IP-adres wordt gebruikt.

Om nieuwe DoH-providers aan te spreken, controleert u op updates en blokkeert u Newly Seen Domains voor een betere dekking.

Voor DoH via IP-adres zijn de scenario's beperkt. Firefox met CloudFlare is een goed voorbeeld.



Let op: voeg geen Mozilla Kill Switch-domeinen toe aan de blokkeerlijst. Het blokkeren van deze domeinen resulteert in een A-record voor blokpagina's, en Firefox behandelt dit als geldig en upgradet automatisch het DoH-gebruik.

Handhaving tegen DNS over TLS (DoT)

Zelfs na het blokkeren van alternatieve DNS-providers en DoH, kan DNS worden omzeild over TLS, die RFC7858 gebruikt over poort 853. CloudFlare is bijvoorbeeld een DoT-provider.

Voorbeeld van handhaving

- Blokkeer de IP-adressen1.1.1.1en klik1.0.0.1op poort 853 (CloudFlare).

Disclaimer voor firewallondersteuning

Dit document helpt netwerkbeheerders bij het afdwingen van Umbrella DNS. Cisco Umbrella Support biedt geen hulp bij individuele firewall- of routerconfiguraties, omdat elk apparaat een unieke configuratie-interface heeft. Raadpleeg de documentatie van uw router of firewall of neem contact op met de fabrikant van het apparaat om te bevestigen of deze configuraties mogelijk zijn.

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.