Umbrella DNS durchsetzen und Umgehung mit Firewall-Regeln verhindern

Inhalt

Einleitung

Voraussetzungen

Erzwingen von Umbrella DNS - gängigste Methode

- Beispiel für Firewall-Regel

Durchsetzung gegen DNS über HTTPS (DoH)

- Empfohlene Konfiguration
  - Details und Hintergrund

Durchsetzung gegen DNS über TLS (DoT)

- Durchsetzungsbeispiel

Haftungsausschluss für Firewall-Support

Einleitung

In diesem Dokument wird beschrieben, wie Sie die DNS-Umgehung verhindern und Umbrella DNS-Schutz mithilfe von Firewall-Regeln und Netzwerkrichtlinien durchsetzen.

Voraussetzungen

- Netzwerk-Firewall
- Firewall-Zugriffsberechtigungen
- Kenntnisse der Firewall-Konfiguration

Erzwingen von Umbrella DNS - gängigste Methode

Bei den meisten Routern und Firewalls können Sie den gesamten DNS-Verkehr über Port 53 durchsetzen, sodass alle Netzwerkgeräte die auf dem Router definierten DNS-Einstellungen verwenden müssen, die auf Umbrella DNS-Server verweisen müssen.

Der bevorzugte Ansatz besteht darin, alle DNS-Anfragen von Nicht-Umbrella-IP-Adressen an die unten aufgeführten Umbrella-DNS-IPs weiterzuleiten. Diese Methode leitet DNS-Anfragen transparent weiter und verhindert, dass die manuelle DNS-Konfiguration einfach fehlschlägt.

Alternativ können Sie eine Firewall-Regel erstellen, um DNS (TCP/UDP) nur für Umbrella DNS-Server zuzulassen und den gesamten anderen DNS-Verkehr zu anderen IP-Adressen zu

blockieren.

Beispiel für Firewall-Regel

1. Fügen Sie diese Regel zur Edge-Firewall hinzu:
    - TCP/UDP ein- und ausgehend an 208.67.222.222 oder 208.67.220.220 auf Port 53 zulassen.
    - Ein- und ausgehende TCP/UDP-Nachrichten an alle IP-Adressen auf Port 53 blockieren.

Die Regel zum Zulassen für Umbrella DNS hat Vorrang vor der Blockregel. DNS-Anfragen an Umbrella sind zulässig, während alle anderen DNS-Anfragen blockiert werden.

Konfigurieren Sie abhängig von der Firewall-Konfigurationsschnittstelle eine separate Regel für jedes Protokoll oder eine einzelne Regel, die TCP und UDP abdeckt. Die Regel auf das Netzwerk-Edge-Gerät anwenden. Sie können eine ähnliche Regel auch auf Software-Firewalls auf Workstations anwenden, z. B. die integrierte Firewall in Windows oder MacOS.

Wenn Sie den Roaming-Client und die Active Directory-Gruppenrichtlinie verwenden, lesen Sie in der Dokumentation nach, wie Sie den Enterprise Roaming-Client mithilfe der Gruppenrichtlinie sperren.

Durchsetzung gegen DNS über HTTPS (DoH)

Empfohlene Konfiguration

1. Aktivieren Sie in Umbrella die Kategorien Proxy/Anonymizer und DoH/DoTcontent.
2. Blockieren Sie die IP-Adressen bekannter DoH-Anbieter auf Ihrer Firewall.

Details und Hintergrund

Umbrella unterstützt die von Mozilla definierteuse-application-dns.netDomäne, um zu verhindern, dass Firefox standardmäßig DoH aktiviert. Weitere Informationen zu Firefox und DoH finden Sie in der zugehörigen Dokumentation.

Auch nach der Blockierung alternativer DNS-Anbieter kann DNS mit DoH umgangen werden. Ein lokaler DNS-Resolver übersetzt DNS-Anfragen in HTTPS und sendet sie mithilfe von JSON oder POST/GET an einen Endpunkt. Dieser Datenverkehr vermeidet in der Regel die DNS-Überprüfung.

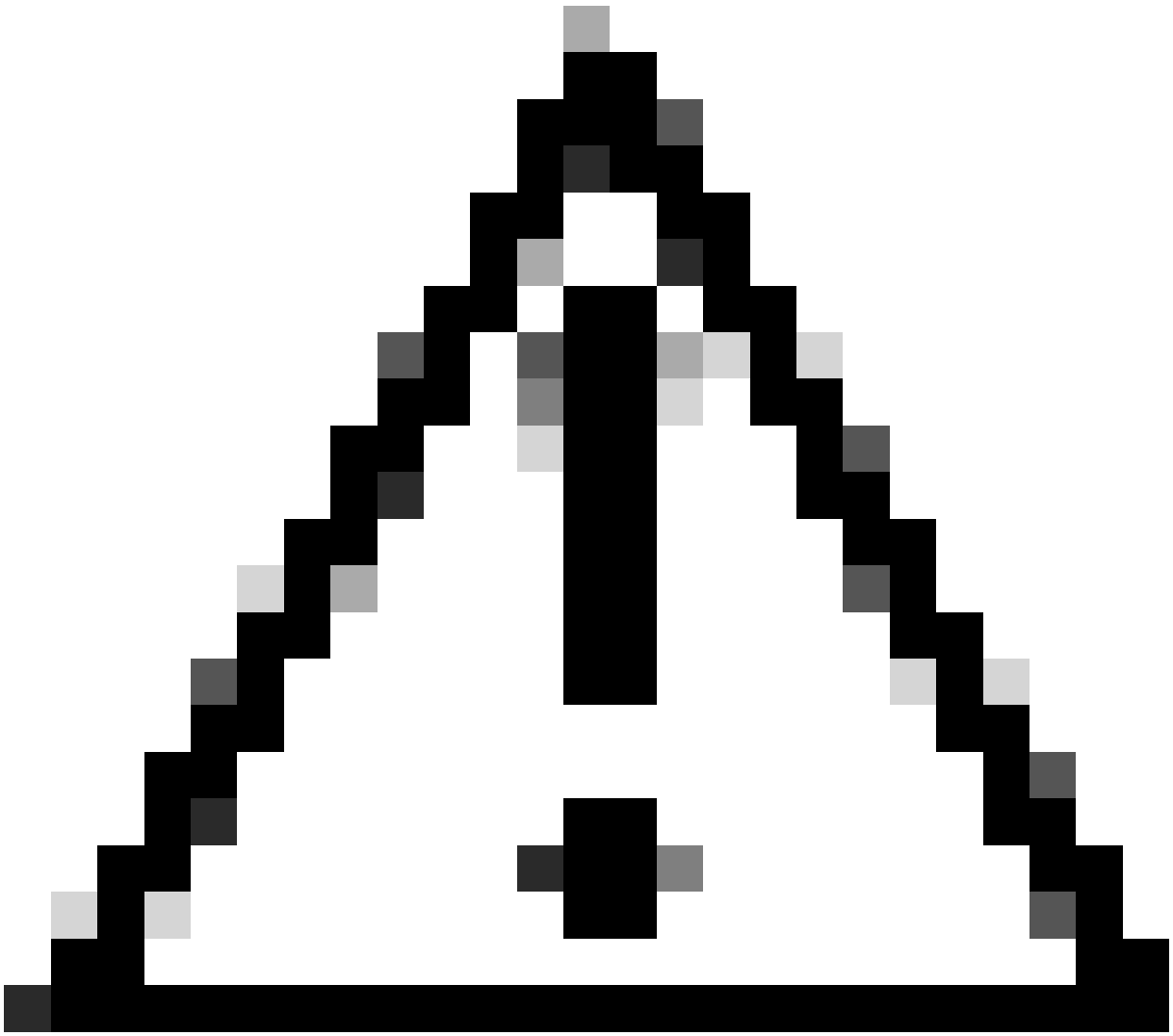
Da DoH verwendet werden kann, um Umbrella zu umgehen, enthält Umbrella bekannte DoH-

Server in der Inhaltskategorie Proxy/Anonymizer. Dieser Mechanismus weist einige Einschränkungen auf:

- Es kann keine brandneuen DoH-Anbieter blockieren, die noch nicht bekannt sind.
- Die DoH-Funktion, die direkt über die IP-Adresse verwendet wird, kann nicht blockiert werden.

Um neue DoH-Anbieter anzusprechen, überwachen Sie auf Updates, und blockieren Sie neu erkannte Domänen, um eine bessere Abdeckung zu gewährleisten.

Für DoH über IP-Adresse sind die Szenarien begrenzt. Firefox mit CloudFlare ist ein prominentes Beispiel.



Vorsicht: Fügen Sie der Sperrliste keine Mozilla Kill Switch-Domänen hinzu. Das

---

Blockieren dieser Domänen führt zu einem A-Eintrag für Blockseiten, und Firefox betrachtet dies als gültig und aktualisiert seine DoH-Nutzung automatisch.

Durchsetzung gegen DNS über TLS (DoT)

Auch nach der Blockierung alternativer DNS-Anbieter und DoH kann DNS über TLS umgangen werden, das RFC7858 über Port 853 verwendet. Beispielsweise ist CloudFlare ein DoT-Anbieter.

Durchsetzungsbeispiel

- Blockieren Sie die IP-Adressen1.1.1.1und1.0.0.1auf Port 853 (CloudFlare).

Haftungsausschluss für Firewall-Support

Dieses Dokument unterstützt Netzwerkadministratoren bei der Durchsetzung von Umbrella DNS. Der Cisco Umbrella Support bietet keine Unterstützung für individuelle Firewall- oder Router-Konfigurationen, da jedes Gerät über eine eigene Konfigurationsschnittstelle verfügt. Lesen Sie in der Router- oder Firewall-Dokumentation nach, oder wenden Sie sich an den Gerätehersteller, um zu überprüfen, ob diese Konfigurationen möglich sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.