Enforce Umbrella DNS and Prevent Bypass with Firewall(우산 DNS 시행 및 방화벽 규칙으로 우회 방지)

목차

소개

사전 요구 사항

Umbrella DNS 시행—가장 일반적인 방법

  방화벽 규칙의 예

HTTPS를 통한 DNS 시행(DoH)

  권장 컨피그레이션

    세부 정보 및 배경

DNS over TLS(DoT)에 대한 시행

  적용 예

방화벽 지원 면책조항

소개

이 문서에서는 방화벽 규칙 및 네트워크 정책을 사용하여 DNS 우회를 방지하고 Umbrella DNS 보호를 적용하는 방법에 대해 설명합니다.

사전 요구 사항

- 네트워크 방화벽
- 방화벽 액세스 권한
- 방화벽 구성에 대한 지식

Umbrella DNS 시행—가장 일반적인 방법

대부분의 라우터와 방화벽에서는 포트 53을 통해 모든 DNS 트래픽을 적용할 수 있으므로, 모든 네트워크 디바이스에서 라우터에 정의된 DNS 설정을 사용해야 하며, 이는 Umbrella DNS 서버를 가리켜야 합니다.

기본 접근 방식은 비Umbrella IP 주소에서 모든 DNS 요청을 아래에 나열된 Umbrella DNS IP로 전달하는 것입니다. 이 방법은 DNS 요청을 투명하게 전달하고 수동 DNS 컨피그레이션이 단순히 실패하는 것을 방지합니다.

또는 Umbrella DNS 서버에만 DNS(TCP/UDP)를 허용하고 다른 IP 주소에 대한 다른 모든 DNS 트래픽을 차단하도록 방화벽 규칙을 생성합니다.

방화벽 규칙의 예

1. 에지 방화벽에 이 규칙 추가:
    - AllowTCP/UDP 인바운드 및 아웃바운드208.67.222.222를 포트 53208.67.220.220에 또는 포트.
    - BlockTCP/UDP 인바운드 및 포트 53의 모든 IP 주소로 아웃바운드.

Umbrella DNS에 대한 허용 규칙은 차단 규칙보다 우선합니다. Umbrella에 대한 DNS 요청은 허용되지만 다른 모든 DNS 요청은 차단됩니다.

방화벽 컨피그레이션 인터페이스에 따라 각 프로토콜에 대해 별도의 규칙을 구성하거나 TCP와 UDP를 모두 포괄하는 단일 규칙을 구성합니다. 네트워크 에지 디바이스에 규칙을 적용합니다. Windows 또는 macOS의 내장형 방화벽과 같이 워크스테이션의 소프트웨어 방화벽에 유사한 규칙을 적용할 수도 있습니다.

로밍 클라이언트 및 Active Directory 그룹 정책을 사용하는 경우 그룹 정책을 사용하여 엔터프라이즈 로밍 클라이언트를 잠그는 방법에 대한 설명서를 참조하십시오.

HTTPS를 통한 DNS 시행(DoH)

권장 컨피그레이션

1. Umbrella에서 Proxy/AnonymizerandDoH/DoContent 범주를 활성화합니다.
2. 방화벽에 있는 알려진 DoH 공급자의 IP 주소를 차단합니다.

세부 정보 및 배경

Umbrella는use-application-dns.netMozilla에서 정의한 대로 도메인을 지원하여 Firefox가 기본적으로 DoH를 활성화하지 않도록 합니다. Firefox 및 DoH에 대한 자세한 내용은 관련 설명서를 참조하십시오.

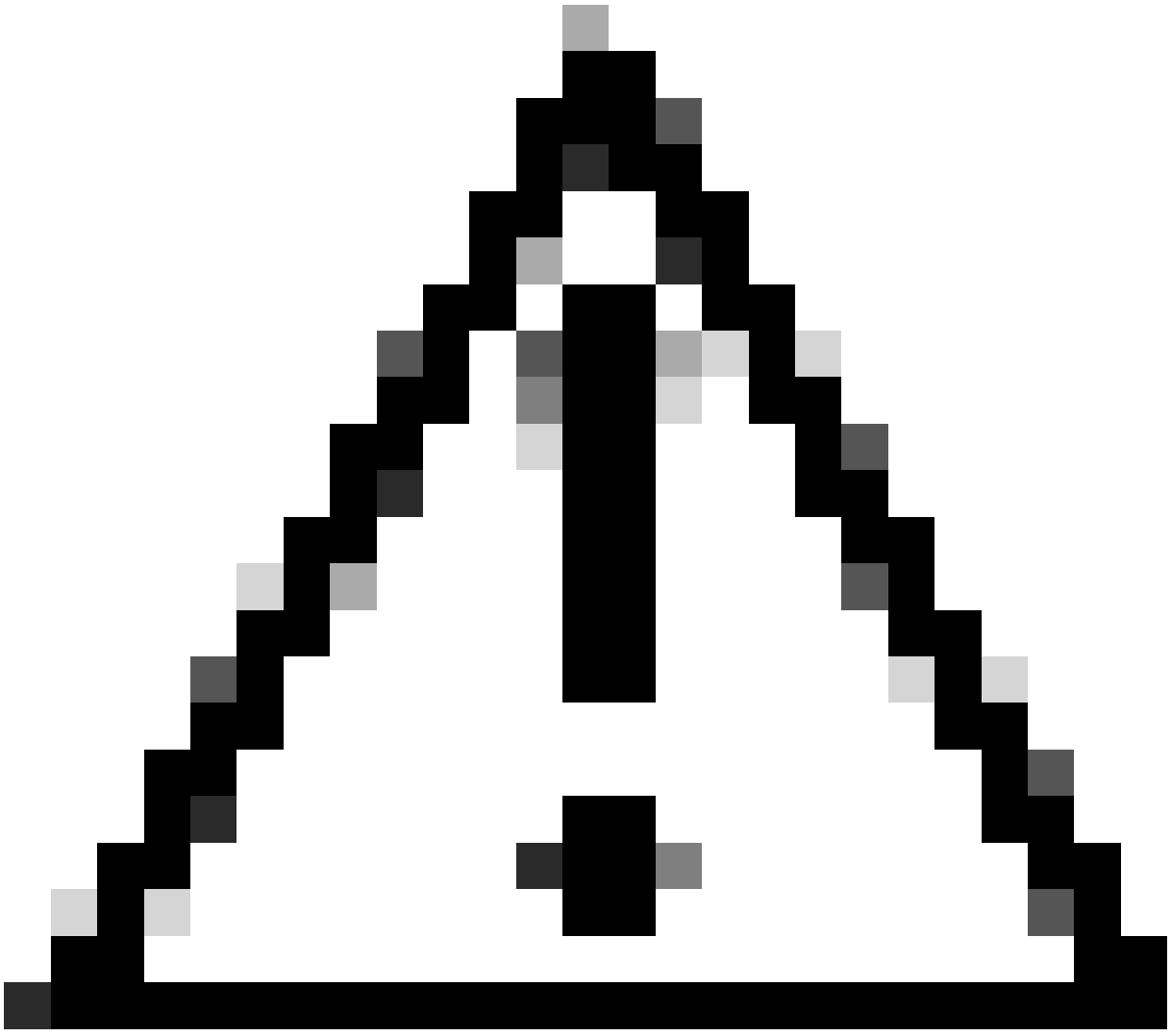
대체 DNS 제공자를 차단한 후에도 DNS는 DoH로 우회할 수 있습니다. 로컬 DNS 확인자는 DNS 요청을 HTTPS로 변환하고 JSON 또는 POST/GET을 사용하여 엔드포인트로 전송합니다. 이 트래픽은 일반적으로 DNS 검사를 피합니다.

Umbrella를 우회하는 데 DoH를 사용할 수 있으므로 Umbrella에는 프록시/익명 장치 콘텐츠 범주에 알려진 DoH 서버가 포함됩니다. 이 메커니즘에는 몇 가지 제한이 있습니다.

- 아직 알려지지 않은 새로운 DoH 제공자를 차단할 수 없습니다.
- IP 주소를 통해 직접 사용되는 DoH를 차단할 수 없습니다.

새로운 DoH 제공자를 해결하려면 업데이트를 모니터링하고 향상된 커버리지를 위해 Newly Seen Domains(새로 확인된 도메인)를 차단합니다.

IP 주소를 통한 DoH의 경우 시나리오가 제한됩니다. CloudFlare가 포함된 Firefox가 대표적인 예입니다.



주의: 차단 목록에 Mozilla Kill Switch 도메인을 추가하지 마십시오. 이러한 도메인을 차단하면 차단 페이지에 대한 A 레코드가 생성되고, Firefox는 이를 유효한 것으로 간주하여 DoH 사용량을 자동으로 업그레이드합니다.

DNS over TLS(DoT)에 대한 시행

대체 DNS 제공자와 DoH를 차단한 후에도 DNS를 TLS를 통해 우회할 수 있습니다. TLS는 포트 853을 통해 RFC7858을 사용합니다. 예를 들어 CloudFlare는 DoT 제공자입니다.

적용 예

- IP 주소1.1.1.1 및 포트 853(1.0.0.1CloudFlare)을 차단합니다.

방화벽 지원 면책조항

이 문서는 네트워크 관리자가 Umbrella DNS를 적용하는 데 도움이 됩니다. Cisco Umbrella Support는 각 디바이스에 고유한 컨피그레이션 인터페이스가 있으므로 개별 방화벽 또는 라우터 컨피그레이션에 대한 지원을 제공하지 않습니다. 라우터 또는 방화벽 설명서를 참조하거나 디바이스 제조업체에 문의하여 이러한 컨피그레이션이 가능한지 확인하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.