

Aufrechterhaltung von DoH in Firefox und Chrome mit GPO

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Firefox](#)

[Chrom](#)

Einleitung

In diesem Dokument wird beschrieben, wie DNS über HTTPS (DoH) in Firefox und Chrome mithilfe von Gruppenrichtlinienobjekten (Group Policy Objects, GPO) in Cisco Umbrella verwaltet und deaktiviert wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

DNS over HTTPS (DoH) ist eine Funktion, die mehreren Webbrowsern hinzugefügt wurde, mit der DNS den DNS-Stack des Systems über HTTPS umgehen kann. In vielen Fällen können Sie diese Funktion deaktivieren, um sicherzustellen, dass Webbrowser keine Umbrella-Einstellungen überschreiben.

Firefox und Chrome bieten beide DoH-Funktionalität und die Möglichkeit, die DoH-Nutzung in

Ihrem Netzwerk und auf verwalteten Computern zu verhindern. Die DoH-Implementierungen unterscheiden sich jedoch stark von Browser zu Browser.

Firefox

Firefox arbeitet mit einer standardmäßigen DoH-Einstellung, bei der DNS standardmäßig mit 1.1.1.1 an CloudFlare gesendet wird. Diese Einstellung berücksichtigt nicht die DNS-Einstellung des Systems.

Um dies zu bekämpfen, setzt Umbrella standardmäßig die Außerkraftsetzung auf DoH deaktivieren (siehe unseren Artikel hier für weitere Informationen). Diese Überschreibung kann jedoch nur wirksam werden, wenn keine explizit festgelegten DoH-Einstellungen vorhanden sind. Um sicherzustellen, dass DoH niemals aktiviert ist, um Firefox DNS von den Systemeinstellungen abzulenken, sind Gruppenrichtlinienobjekteinstellungen erforderlich.

Um diese Option zu deaktivieren, setzen Sie den Wert für "network.trr.mode" auf 0. Weitere Informationen finden Sie in den TRR-Einstellungen von Firefox.

Weitere Informationen zum Verwalten von Unternehmensrichtlinien in Firefox finden Sie in der Mozilla-Dokumentation.

Chrom

Chrome hat Unterstützung für DoH für mehrere Anbieter einschließlich Umbrella. Im Gegensatz zu Firefox kann Chrome DoH nur aktiviert werden, wenn das System-DNS als teilnehmender DNS-Provider erkannt wird. Daher kann es nicht aktivieren, wenn System DNS ein lokaler DNS-Server oder der Roaming-Client ist, kann aber aktivieren, wenn lokale DNS 208.67.220.220 und 208.67.222.222 ist. Daher lenkt Chrome Ihren DNS nicht vom System-DNS ab, sondern erweitert ihn mit DoH.

Während der Anfangsphase des Chrome DoH-Experiments kann Chrome DoH deaktivieren, wenn das Gerät verwaltet wird, AD beigetreten ist oder eine Enterprise-Richtlinie angewendet wurde.

Weitere Informationen finden Sie auf der Chrome-Website.

Weitere Informationen zur Verwaltung von Unternehmensrichtlinien in Chrome finden Sie in der Chrome-Dokumentation.

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.