Verständnis der Einschränkungen des Umbrella DNS Policy Tester

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Technische Details](#)

[Sicheres Web-Gateway](#)

[Sicheres Internet-Gateway](#)

[Umbrella \(DNS Added Layer\)](#)

Einleitung

In diesem Dokument werden die Einschränkungen des Umbrella DNS Policy Tester beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sicheres Web-Gateway
- Sicheres Internet-Gateway
- Umbrella (DNS Added Layer)

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

Mit dem Umbrella Policy Tester kann bestimmt werden, ob ein bestimmtes Ziel von Cisco blockiert

oder zugelassen werden kann, wenn eine bestimmte Identität einen Besuch abstattet. Es gibt jedoch einige Umstände, unter denen der Richtlinientester derzeit keine genauen (oder keine) Informationen für ein bestimmtes Ziel zurückgeben kann. In diesem Artikel werden diese Einschränkungen erläutert.

Technische Details

Die allgemeine Übersicht zu Policy Tester finden Sie in der Umbrella-Dokumentation für [Umbrella Policy Tester](#).

Diese Ergebnisse des Richtlinientesters können falsch sein:

Sicheres Web-Gateway

- Nicht unterstützt

Sicheres Internet-Gateway

- Nicht unterstützt

Umbrella (DNS Added Layer)

- Ziele, die vom intelligenten Proxy blockiert werden, können vom Richtlinientester fälschlicherweise als "Zulässig" gemeldet werden. Dazu gehören auch:
 - Benutzerdefinierte URL-Blocklisten
 - Proxy-Sperrlisten- oder Greylist-Domänen
 - Dateiprüfungsblöcke
- Zieltyp "Anwendung" (wie Dropbox, Box, Facebook, etc. nach Name), die gesperrt sind, kann vom Richtlinientester fälschlicherweise als "Zulässig" gemeldet werden.
- Wenn ein Netzwerk auch auf eine Webrichtlinie angewendet wird, kann die Webrichtlinie falsch angezeigt werden. Der Richtlinientester wird derzeit nicht für Netzwerke unterstützt, die ebenfalls Teil von Webrichtlinien sind.
- Tests, die nicht alle relevanten Identitätsinformationen liefern, können zu falschen Ergebnissen führen. Beispiel: Ein Roaming-Computer mit aktivierter Active Directory (AD)-Integration in einem geschützten Netzwerk: Der Test kann fehlschlagen, wenn nur der AD-Benutzer angegeben wird, aber der Roaming-Computer die Richtlinienentscheidungen gewinnt.
- Ziele, die aufgrund von Inhaltskategorien blockiert wurden, können als zulässig angezeigt werden, wenn sie mit Groß- und Kleinbuchstaben eingegeben oder in Großbuchstaben geschrieben wurden. Wenn Sie beispielsweise die Kategorie "Nacktheit" blockieren, kann die Domäne playboy.com als blockiert angezeigt werden, während Playboy.com als zulässig angezeigt wird.
- "Dynamic DNS"-Ziele können blockiert werden, wenn diese Sicherheitskategorie ausgewählt ist, sie können jedoch vom Richtlinientester fälschlicherweise als "Zulässig" gemeldet werden.
- Von der Anwendungssteuerung zugelassene Ziele können im Richtlinientester fälschlicherweise als blockiert angezeigt werden.

- Ziele, die von der Umbrella Enforcement API für benutzerdefinierte Integrationen blockiert werden, können vom Richtlinientester fälschlicherweise als "zulässig" gemeldet werden.
- Ziele, die durch die Umbrella AMP Threat Grid-Integration blockiert werden, können vom Richtlinientester fälschlicherweise als "erlaubt" gemeldet werden.
- Ziele, die aufgrund eines CNAME blockiert werden, können vom Richtlinientester fälschlicherweise als "Zulässig" gemeldet werden.
- Ziele, die IP-Adressen sind, werden im Richtlinientester derzeit nicht unterstützt.
- Ziele, bei denen es sich um URLs handelt, werden im Richtlinientester derzeit nicht unterstützt.
- Ziele, die für die Auflösung in eine schädliche IP blockiert werden, können vom Richtlinientester fälschlicherweise als "Zulässig" gemeldet werden.
- Potenziell schädliche Ziele können blockiert werden, wenn diese Sicherheitskategorie ausgewählt ist. Sie können jedoch vom Richtlinientester fälschlicherweise als "Zulässig" gemeldet werden.
- Ziele, bei denen automatisierte DDoS-Schutzmechanismen vorübergehend verhindern, dass DNS für die betroffene Domäne antwortet, sind vom Policy Tester nicht sichtbar.
- Ziele, die in der Inhaltskategorie "Deutscher Jugendschutz" gesperrt sind, können vom Policy Tester fälschlicherweise als "erlaubt" gemeldet werden. Diese Kategorie kann in den Ergebnissen des Policy Tester nicht erwähnt werden.
- Ziele, die aufgrund der Sicherheitsklassifizierung "Kryptowährung" blockiert wurden, können fälschlicherweise als "Zulässig" angezeigt werden, selbst wenn sie durch Sicherheitseinstellungen blockiert wurden.
- Blockierungen aufgrund von DNS-Tunneling-VPN-Kategorien können im Richtlinientester keine richtigen Ergebnisse anzeigen. Sie werden fälschlicherweise als zulässig angezeigt.
- Chromebook-Geräte hinter einer virtuellen Appliance können falsche Richtlinien anzeigen. Chromebook (UCC)-Identitätsblöcke können die von virtuellen Appliances angewendeten Richtlinien überschreiben, aber virtuelle Applianceblöcke können UCC-Berechtigungen überschreiben.
- Mitglieder von AD-Gruppen, bei denen die Gruppe nicht mit Umbrella synchronisiert wird (einschließlich Gruppen, die Teil einer übergeordneten oder untergeordneten Domäne sind, und Gruppen, die Mitglieder von Gruppen sind, die nicht selektiv mit Umbrella synchronisiert werden), können als mit der angezeigten Richtlinie im Richtlinientester übereinstimmend angezeigt werden. Die Benutzerrichtlinie kann in der Cloud nicht angewendet werden. Bestätigen Sie dies, indem Sie einen einzelnen Benutzer zu Ihrer Richtlinie hinzufügen und bestätigen Sie, dass diese innerhalb von 5 Minuten korrekt angewendet wird.
- Ziele, die in der Liste Interne Domänen aufgeführt sind. Der Richtlinientester verwendet beim Melden eines Testergebnisses nicht die Liste Interne Domänen.
- Kategorien, die nicht auf der OpenDNS Community-Domain-Tagging-Site angezeigt werden, sind nicht sicher, dass die richtige Kategorie im Richtlinientester angezeigt wird. Es wird nur eine Kategorisierungsquelle dargestellt.
- Der Richtlinientester ist darauf beschränkt, bei der Identitätssuche 20 Ergebnisse anzuzeigen.
- Ein AD-Benutzer ist Mitglied einer geschachtelten AD-Gruppe. Beim Erstellen einer DNS-Richtlinie wird jedoch nur die übergeordnete AD-Gruppe in Identitäten ausgewählt. Die Richtlinientestersuche kann nicht mit der richtigen Richtlinie übereinstimmen.
- Ziele in der Liste der geschützten Zulassen können vom Richtlinientester fälschlicherweise

als "Blockiert" gemeldet werden.

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.