Umbrella DNS mit einem HTTP-Proxy verwenden

Inhalt

Einleitung

In diesem Dokument wird die Verwendung von Umbrella DNS mit einem HTTP-Proxy beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Umbrella Global DNS Service, nicht auf Secure Web Gateway (SWG).

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.

Hintergrundinformationen

Ein HTTP-Proxy fängt den HTTP/S-Verkehr in einem Netzwerk ab. Anschließend stellt er die

HTTP/S-Verbindung zum Remote-Server im Auftrag des ursprünglichen Clients her und leitet die Antworten an diesen Client weiter. Die meisten HTTP-Proxys können Verbindungen zu bestimmten Sites basierend auf Kategorisierung oder Sicherheitsinhalten blockieren oder Antworten von Remote-Servern blockieren, die unerwünschte Inhalte wie Malware enthalten.

Es gibt zwei primäre Methoden für die Umleitung des HTTP-Datenverkehrs an einen Proxy: explizite und transparente Umleitung. Diese unterschiedlichen Verfahren erfordern unterschiedliche Schritte, um in Kombination mit Umbrella ordnungsgemäß zu funktionieren.

In diesem Artikel wird erläutert, wie ein HTTP-Proxy das Verhalten von Umbrella und jedem Teil der Umbrella-Lösung beeinflusst. Anschließend werden zwei Schritte für die explizite Umleitung und die transparente Umleitung beschrieben.

Dieses Diagramm bietet eine Zusammenfassung der beschriebenen Lösungen:

<table>
<tr><th></th><th>No Proxy</th><th>Transparent Proxy (Trusts Client DNS Resolution)</th><th>Transparent Proxy (Does Not Trust Client DNS Resolution)</th><th>Proxy Script</th><th>Explicit Proxy</th></tr>
<tr><td>Internet Connected
208.67.222.222 reachable over UDP 443</td><td colspan="2" rowspan="2">Umbrella protected</td><td colspan="3" rowspan="2">Web traffic via 80/443 resolved/protected by proxy

All other ports, Umbrella protected</td></tr>
<tr><td>Internet Connected
208.67.222.222 reachable over UDP 53</td></tr>
<tr><td>Internet Connected
No Umbrella access</td><td colspan="5" rowspan="2">Local DNS server used</td></tr>
<tr><td>No Internet access</td></tr>
</table>

proxy-umbrella-diagramm.png

Auswirkungen eines HTTP-Proxys auf den globalen Umbrella DNS-Dienst

Beim Abfangen von HTTP/S-Datenverkehr liest ein HTTP-Proxy den Host-Header in der HTTP/S-Anforderung und generiert eine eigene DNS-Abfrage für diesen Host. Daher ist es wichtig, das Verhalten des Proxys bei der Bereitstellung von Umbrella-Lösungen zu berücksichtigen. Auf abstrakter Ebene muss dabei sichergestellt werden, dass HTTP/S-Verbindungen zu Umbrella-IP-Adressen nicht an den Proxy umgeleitet, sondern direkt an ihr beabsichtigtes Ziel gesendet werden.

Netzwerkschutz

Wenn nur Umbrella Network Protection verwendet wird, wird empfohlen, dass der HTTP-Proxy selbst entweder Umbrella direkt für die DNS-Auflösung verwendet oder einen internen DNS-Server verwendet, der wiederum DNS-Abfragen an Umbrella weiterleitet. Die entsprechende externe IP-Adresse kann im Umbrella Dashboard als Netzwerkidentität registriert werden. In diesem Szenario ist keine zusätzliche Aktion erforderlich, um Umbrella zu verwenden.

Wenn dies aus irgendeinem Grund nicht möglich ist und die Clients selbst Umbrella verwenden, können die in diesem Artikel beschriebenen Maßnahmen ergriffen werden, um sicherzustellen, dass die Durchsetzung nicht vom HTTP-Proxy umgangen wird.

Umbrella-Roaming-Client

Wenn Sie den Umbrella-Roaming-Client verwenden, werden DNS-Abfragen vom Client-Computer direkt an Umbrella gesendet. Da ein HTTP-Proxy jedoch seine eigenen DNS-Abfragen durchführt, ist die Durchsetzung durch den Umbrella-Roaming-Client ineffektiv. Daher müssen bei Verwendung des Umbrella-Roaming-Clients in einer Proxyumgebung die in diesem Artikel beschriebenen Aktionen ausgeführt werden.

Virtuelle Appliances und Active Directory-Integration

Die virtuelle Appliance (VA) soll als DNS-Server für Client-Computer im geschützten Netzwerk fungieren. Die Verwendung eines HTTP-Proxys macht seine Durchsetzung daher ebenso unwirksam wie der Roaming-Client. Daher können die in diesem Artikel beschriebenen Maßnahmen verfolgt werden, um eine wirksame Durchsetzung und eine korrekte Berichterstattung zu gewährleisten.

Zusätzlich zu den unten aufgeführten Aktionen wird empfohlen, den HTTP-Proxy so zu konfigurieren, dass er die VA als DNS-Server verwendet. Auf diese Weise können Sie eine proxyspezifische Richtlinie definieren, sodass Abfragen vom Proxy identifiziert werden können. Mit einer solchen Richtlinie können Sie auch die Protokollierung für Abfragen deaktivieren, die vom Proxy stammen. Dadurch werden doppelte Abfragen in Ihren Berichten vermieden.

Explizite Proxys

Bei der Bereitstellung eines expliziten Proxys müssen die Proxyeinstellungen des Browsers geändert werden, um den Datenverkehr explizit an einen Proxy umzuleiten. Dies geschieht entweder mithilfe der Gruppenrichtlinie in Windows oder in der Regel mithilfe einer Proxy-Autokonfigurationsdatei (PAC). In beiden Fällen wird der Browser dazu veranlasst, den gesamten HTTP-Datenverkehr direkt an den Proxy zu senden, anstatt ihn an die Remotesite zu senden. Da der Browser weiß, dass der Proxy seine eigene DNS-Anforderung generiert, muss er den Hostnamen des Remote-Standorts selbst nicht auflösen. Wenn die HTTP-Verbindung den Proxy erreicht, generiert der Proxy zudem, wie bereits erwähnt, eine eigene DNS-Abfrage, die ein anderes Ergebnis erhalten kann, als der Client erhalten würde.

Um mit Umbrella ordnungsgemäß zu funktionieren, sind daher zwei Änderungen erforderlich:

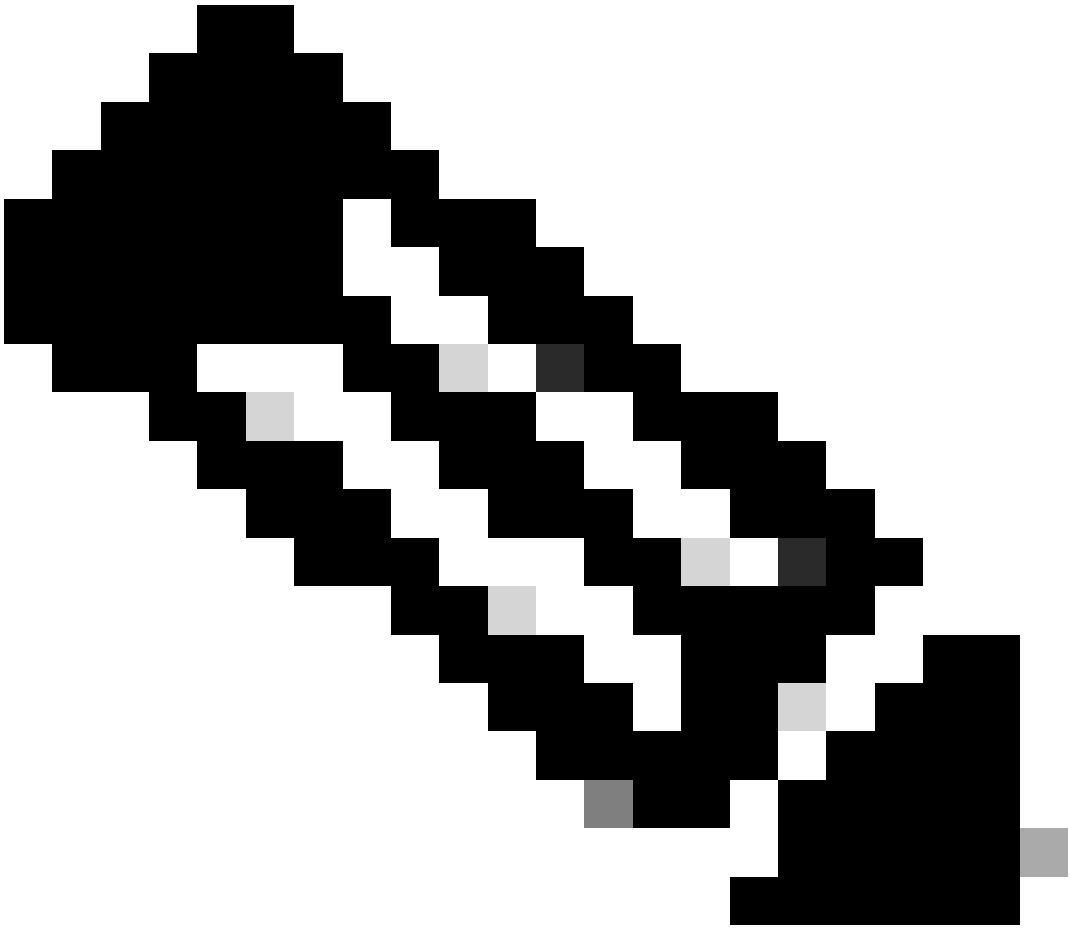
1. Der Client muss gezwungen werden, eine DNS-Abfrage durchzuführen.
2. HTTP-Verbindungen, die an Umbrella-IP-Adressen gerichtet sind, dürfen nicht an den Proxy geleitet werden, sondern direkt an Umbrella.

Beide Änderungen können mit einer PAC-Datei vorgenommen werden:

```
function FindProxyForURL(url, host) {    // Generate DNS request on the client    hostIP = dnsResolve(h
        isInNet(hostIP, "155.190.0.0", "255.255.0.0") ||
        isInNet(hostIP, "146.112.0.0", "255.255.0.0")) ||
        isInNet(hostIP, "151.186.0.0", "255.255.0.0"))
    {         return "DIRECT";     }     // DEFAULT RULE: All other traffic, use below proxies, in fai
```

In dieser Beispiel-PAC-Datei wird zunächst eine DNS-Abfrage generiert, wobei die resultierende IP in der hostIP-Variablen erfasst wird. Diese resultierende IP-Adresse wird dann mit jedem Umbrella IP-Adressbereich verglichen. Wenn eine Übereinstimmung vorliegt, wird die Abfrage nicht an den Proxy gesendet, sondern direkt gesendet. Wenn keine Übereinstimmung gefunden wird, wird die Anforderung an die entsprechenden Proxys gesendet.

Beachten Sie, dass bei Sites, die nicht blockiert sind und daher nicht an eine Umbrella IP-Adresse umgeleitet werden, die Verwendung der vorherigen PAC-Datei dazu führt, dass sowohl der Client als auch der Proxy eine DNS-Anfrage für den Remote-Host stellen. Wenn der Proxy auch OpenDNS verwendet, bedeutet dies, dass Ihre Berichte doppelte Abfragen anzeigen. Wenn Sie die virtuelle Appliance verwenden, wie bereits erwähnt, kann dies durch die Erstellung einer internen Netzwerkidentität für Ihren Proxy berücksichtigt werden. Falls gewünscht, können Sie zusätzlich eine Richtlinie für den Proxy erstellen, die die Protokollierung vollständig deaktiviert, um diese doppelten Anfragen zu verbergen.



Anmerkung: Wenn Sie ausgehende HTTP/S-Anforderungen an Ihrer Firewall von anderen Quellen als Ihrem Proxy blockieren, müssen Sie sicherstellen, dass Sie diese

---

Anforderungen auf die oben genannten IP-Bereiche zulassen, damit Ihre Computer auf die Umbrella-Blockseiten zugreifen können.

Transparente Proxys

Bei einem transparenten Proxy wird der HTTP-Datenverkehr auf Netzwerkebene an den Proxy umgeleitet. Da der Client den Proxy nicht erkennt, generiert der Browser eine eigene DNS-Anforderung. Das bedeutet, dass, wenn der Proxy auch Umbrella verwendet, jede Anforderung dupliziert wird. Außerdem wird die Richtlinie nicht ordnungsgemäß angewendet, da der Proxy die empfangene DNS-Antwort verwendet und nicht das vom Client empfangene Ergebnis.

Im Gegensatz zum expliziten Fall aus dem vorherigen Artikel müssen wir für die Lösung dieses Problems keine DNS-Anforderung auf dem Client erzwingen, da dies bereits geschieht. Die Umgehung des Proxys für HTTP-Verbindungen zu Umbrella-IP-Adressen ist jedoch weiterhin erforderlich. Die Methode hierfür ist sehr unterschiedlich, je nachdem, welchen Mechanismus Sie zum Umleiten von Datenverkehr an den Proxy verwenden. Im Allgemeinen beinhaltet dies jedoch eine Ausnahme von der Umleitung der Umbrella-IP-Adressbereiche.

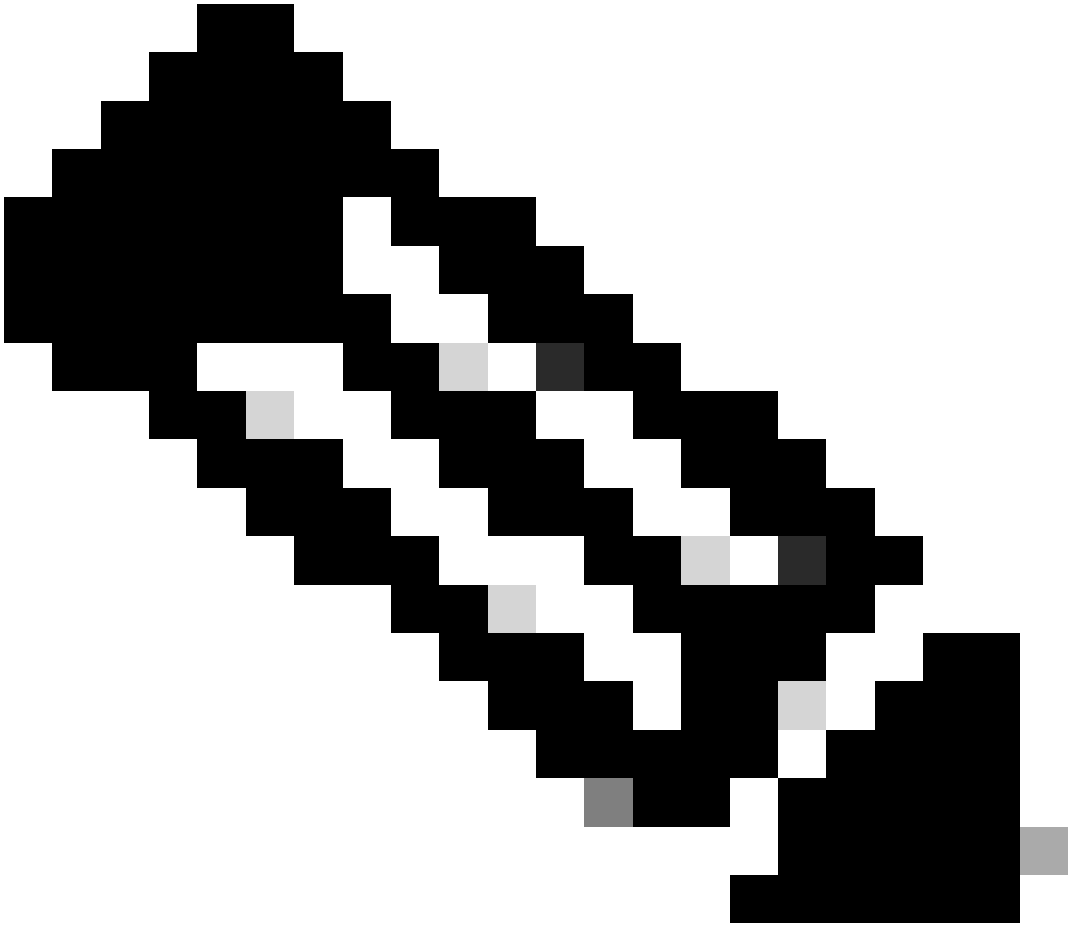
Angenommen, WCCP wird auf einer Cisco ASA verwendet, um Datenverkehr mithilfe dieser ACL an den Proxy umzuleiten:

```
access-list wccp-traffic extended permit ip any any
```

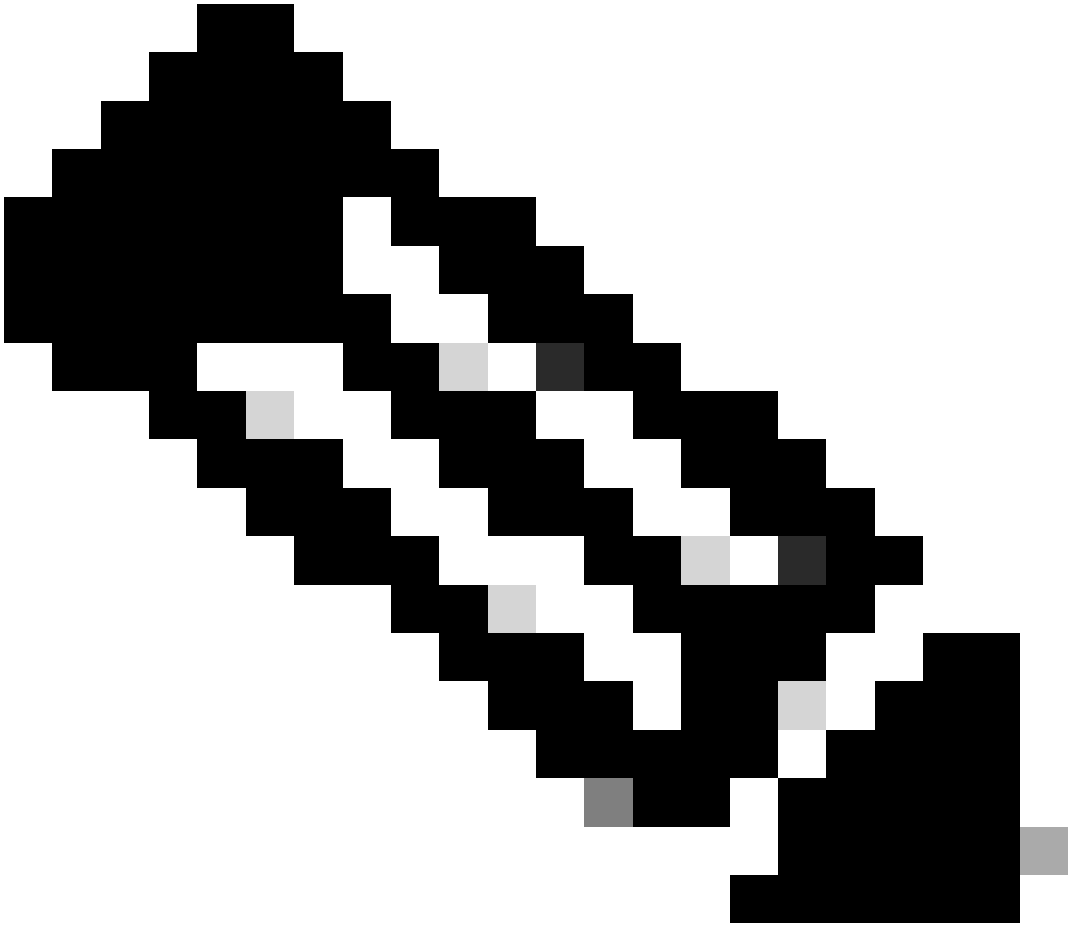
Die ACL für den wccp-Datenverkehr könnte so geändert werden, dass die Umleitung zum Proxy (und somit die Umgehung des Proxys) für Umbrella IP-Bereiche verweigert wird:

```
access-list wccp-traffic extended deny ip any 67.215.64.0 255.255.224.0access-list wccp-traffic extende
access-list wccp-traffic extended deny ip any 155.190.0.0 255.255.0.0
access-list wccp-traffic extended deny ip any 151.186.0.0 255.255.0.0
```

```
access-list wccp-traffic extended permit ip any any
```



Anmerkung: Diese ACL wurde nicht getestet und unterscheidet sich je nach verwendeter ASA-Version oder Cisco IOS®-Version. Stellen Sie sicher, dass alle von Ihnen erstellten ACLs für Ihre Lösung geeignet sind und vor der Bereitstellung in einer Produktionsumgebung umfassend getestet wurden.



Anmerkung: Wenn Sie ausgehende HTTP/S-Anforderungen an Ihrer Firewall von anderen Quellen als Ihrem Proxy blockieren, müssen Sie sicherstellen, dass Sie diese Anforderungen für die zuvor diskutierten IP-Bereiche zulassen, damit Ihre Computer auf die Umbrella-Blockseiten zugreifen können.

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.