Umbrella DNS gebruiken met een HTTP-proxy

Inhoud

Inleiding

In dit document wordt beschreven hoe u Umbrella DNS gebruikt met een HTTP-proxy.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Umbrella Global DNS Service, niet voor Secure Web Gateway (SWG).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een HTTP-proxy onderschept HTTP/S-verkeer op een netwerk. Vervolgens maakt het de HTTP / S-verbinding met de externe server namens de oorspronkelijke client en stuurt de antwoorden terug naar die client. De meeste HTTP-proxies hebben de mogelijkheid om verbindingen met specifieke sites te blokkeren op basis van categorisatie of beveiligingsinhoud, of om reacties van

externe servers te blokkeren die ongewenste inhoud zoals malware bevatten.

Er zijn twee primaire methoden voor het omleiden van HTTP-verkeer naar een proxy: expliciete omleiding en transparante omleiding. Deze verschillende methoden vereisen verschillende stappen om goed te kunnen functioneren in combinatie met Umbrella.

Dit artikel bespreekt hoe een HTTP-proxy het gedrag van Umbrella en elk deel van de Umbrella-oplossing beïnvloedt en biedt vervolgens twee sets stappen voor expliciete omleiding en transparante omleiding.

Dit diagram is een samenvatting van de oplossingen die in meer detail worden beschreven:

<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-diagram.png

Hoe een HTTP-proxy de wereldwijde DNS-service beïnvloedt

Bij het onderscheppen van HTTP/S-verkeer leest een HTTP-proxy de hostheader in het HTTP/S-verzoek en genereert hij zijn eigen DNS-query voor die host. Het is dus belangrijk om rekening te houden met het gedrag van de proxy bij het inzetten van Umbrella-oplossingen. Op abstract niveau houdt dit in dat ervoor wordt gezorgd dat HTTP/S-verbindingen met Umbrella IP-adressen niet worden doorgestuurd naar de proxy, maar rechtstreeks naar hun beoogde bestemming worden verzonden.

netwerkbeveiliging

Wanneer alleen Umbrella Network-beveiliging wordt gebruikt, wordt aanbevolen dat de HTTP-proxy zelf is geconfigureerd om Umbrella rechtstreeks te gebruiken voor DNS-resolutie, of dat deze een interne DNS-server kan gebruiken die op zijn beurt DNS-query's doorstuurt naar Umbrella. Het juiste externe IP-adres kan als netwerkidentiteit worden geregistreerd in het Umbrella Dashboard. In dit scenario is geen extra actie vereist om Umbrella te gebruiken.

Als dit om een of andere reden niet mogelijk is en klanten zelf Umbrella gebruiken, kunnen de in dit artikel beschreven acties worden ondernomen om ervoor te zorgen dat de handhaving niet wordt omzeild door de HTTP-proxy.

Umbrella Roaming-client

Bij gebruik van de Umbrella roaming-client worden DNS-query's van het clientsysteem rechtstreeks naar Umbrella verzonden. Aangezien een HTTP-proxy echter zijn eigen DNS-query's

uitvoert, maakt dit de handhaving door de Umbrella-roamingclient ondoeltreffend. Wanneer u de Umbrella-roamingclient in een geproxed-omgeving gebruikt, moeten de in dit artikel beschreven acties worden gevolgd.

Virtuele apparaten en Active Directory-integratie

De Virtual Appliance (VA) is bedoeld als de DNS-server voor clientmachines op het beveiligde netwerk. Als zodanig maakt het gebruik van een HTTP-proxy de handhaving ervan op dezelfde manier ondoeltreffend als de roamende klant. Als zodanig kunnen de in dit artikel beschreven acties worden gevolgd om ervoor te zorgen dat de handhaving doeltreffend is en de rapportage nauwkeurig is.

Naast de onderstaande acties wordt aanbevolen om de HTTP-proxy zodanig te configureren dat de VA als DNS-server wordt gebruikt. Hiermee kunt u een beleid definiëren dat specifiek is voor de proxy, zodat vragen van de proxy kunnen worden geïdentificeerd. Met een dergelijk beleid kunt u ook de logboekregistratie uitschakelen voor query's die afkomstig zijn van de proxy, waardoor dubbele query's in uw rapporten worden vermeden.

expliciete volmachten

Het implementeren van een expliciete proxy houdt in dat de proxy-instellingen van de browser worden gewijzigd om het verkeer expliciet naar een proxy om te leiden. Dit wordt gedaan door Groepsbeleid in Windows te gebruiken of, vaker, door een PAC-bestand (Proxy Auto-Configuration) te gebruiken. In beide gevallen zorgt dit ervoor dat de browser al het HTTP-verkeer rechtstreeks naar de proxy stuurt, in plaats van naar de externe site. Omdat de browser weet dat de proxy zijn eigen DNS-verzoek genereert, neemt het niet de moeite om de hostnaam van de externe site zelf op te lossen. Bovendien, zoals eerder vermeld, wanneer de HTTP-verbinding de proxy bereikt, genereert de proxy zijn eigen DNS-query, die een ander resultaat kan krijgen dan de client zou krijgen.

Om goed te kunnen functioneren met de paraplu zijn twee veranderingen nodig:

1. De client moet worden gedwongen om een DNS-query te maken.
2. HTTP-verbindingen die bestemd zijn voor Umbrella IP-adressen moeten niet naar de proxy gaan, maar rechtstreeks naar Umbrella.

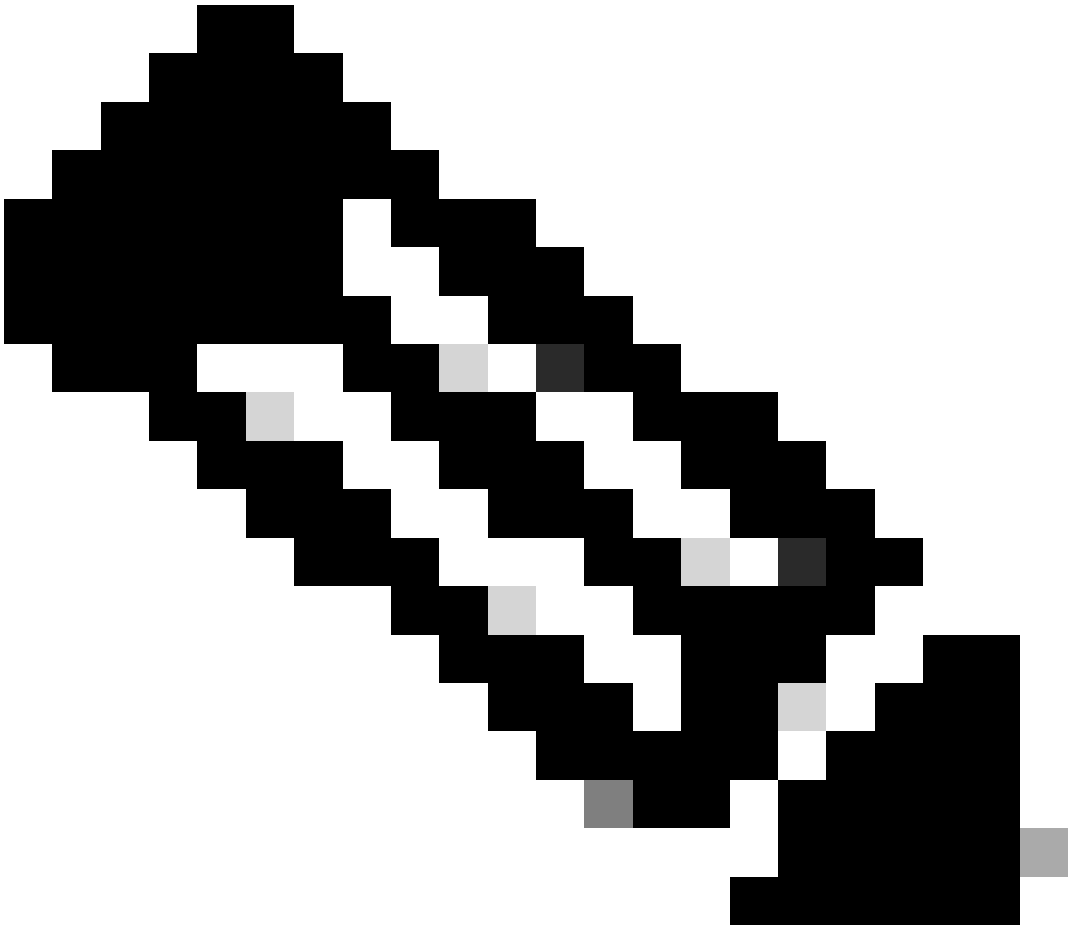
Beide wijzigingen kunnen worden uitgevoerd met behulp van een PAC-bestand:

```
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 dit PAC-voorbeeldbestand wordt eerst een DNS-query gegenereerd, waarbij het resulterende IP wordt vastgelegd in de variabele hostIP. Dit resulterende IP-adres wordt vervolgens vergeleken

met elk Umbrella IP-adresbereik. Als er een overeenkomst is, wordt de query niet naar de proxy verzonden, maar in plaats daarvan rechtstreeks verzonden. Als er geen match is, wordt het verzoek naar de juiste proxies gestuurd.

Merk op dat voor sites die niet zijn geblokkeerd en dus niet worden omgeleid naar een overkoepelend IP-adres, het effect van het gebruik van het vorige PAC-bestand is dat zowel de client als de proxy een DNS-verzoek voor de externe host doet. Als de proxy ook OpenDNS gebruikt, betekent dit dat uw rapporten dubbele query's tonen. Als u de Virtual Appliance gebruikt, zoals eerder vermeld, kan dit worden verklaard door een interne netwerkidentiteit voor uw proxy te maken. Indien gewenst kunt u ook een beleid voor de proxy maken dat de registratie volledig uitschakelt om deze dubbele verzoeken te verbergen.



Opmerking: Als u uitgaande HTTP/S-verzoeken bij uw firewall blokkeert van andere bronnen dan uw proxy, moet u ervoor zorgen dat u deze verzoeken toestaat om de eerder besproken IP-bereiken te bereiken om uw machines toegang te geven tot de pagina's van de Umbrella-blokkering.

Transparante proxies

Voor een transparante proxy wordt HTTP-verkeer omgeleid naar de proxy op netwerkniveau. Omdat de client niet op de hoogte is van de proxy, genereert de browser zijn eigen DNS-verzoek. Dit betekent dat als de proxy ook Umbrella gebruikt, elk verzoek wordt gedupliceerd. Bovendien wordt het beleid niet correct toegepast omdat de proxy het DNS-antwoord gebruikt dat hij heeft ontvangen, niet het resultaat dat de client heeft ontvangen.

In tegenstelling tot het expliciete geval van eerder in dit artikel, vereist het oplossen van dit probleem niet dat we een DNS-verzoek aan de klant forceren, omdat dat al gebeurt. Het omzeilen van de proxy voor HTTP-verbindingen naar Umbrella IP-adressen is echter nog steeds vereist. De methode om dit te doen varieert sterk, afhankelijk van welk mechanisme u gebruikt om verkeer naar de proxy te leiden. In het algemeen gaat het echter om het vrijstellen van de Umbrella IP-adresbereiken van omleiding.

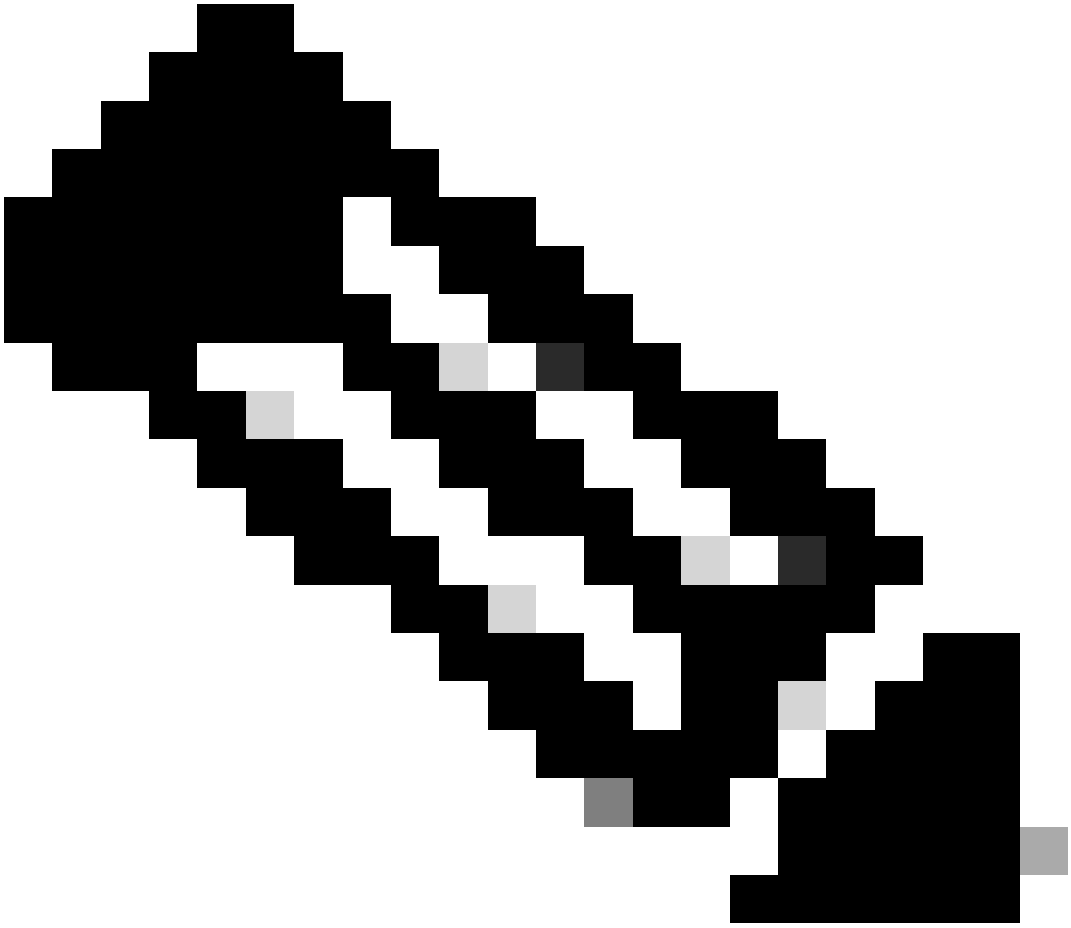
Stel bijvoorbeeld dat WCCP wordt gebruikt op een Cisco ASA om verkeer naar de proxy om te leiden, met behulp van deze ACL:

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

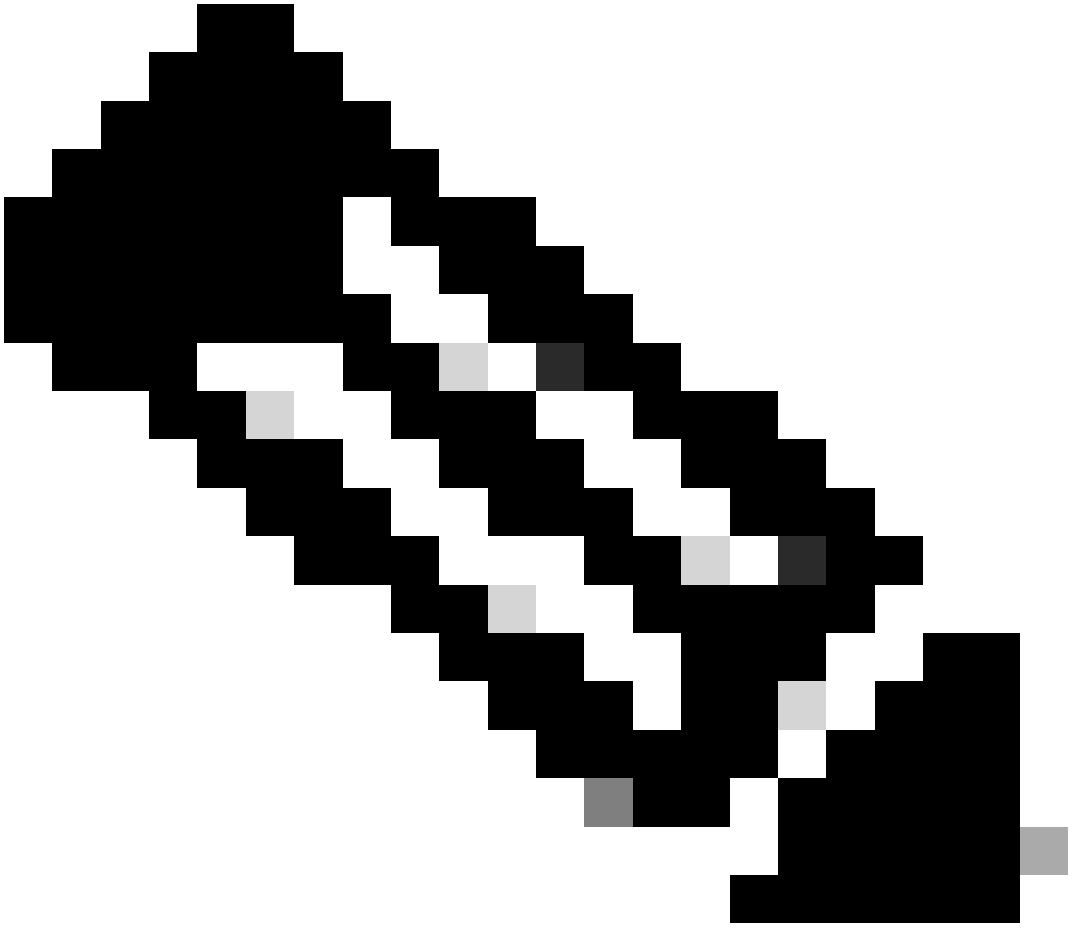
Het WCCP-verkeer ACL kan worden gewijzigd om omleiding naar de proxy (dus omzeilen van de proxy) voor Umbrella IP bereiken weigeren:

```
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
```



Opmerking: deze ACL is niet getest en varieert afhankelijk van de ASA-versie of de Cisco IOS®-versie die wordt gebruikt. Zorg ervoor dat alle ACL's die u maakt, geschikt zijn voor uw oplossing en grondig zijn getest voordat ze in een productieomgeving worden geïmplementeerd.



Opmerking: Als u uitgaande HTTP/S-verzoeken bij uw firewall blokkeert van andere bronnen dan uw proxy, moet u ervoor zorgen dat u deze verzoeken toestaat tot de eerder besproken IP-bereiken om uw machines toegang te geven tot de pagina's van de Umbrella-blokkering.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.