Use Umbrella DNS with an HTTP Proxy

Contents

Introduction

This document describes how to use Umbrella DNS with an HTTP proxy.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella Global DNS Service, not for Secure Web Gateway (SWG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

An HTTP proxy intercepts HTTP/S traffic on a network. Then, it makes the HTTP/S connection to the remote server on behalf of the original client, relaying the responses back to that client. Most HTTP proxies have the ability to block connections to specific sites based on categorization or security content, or to block responses from remote servers that make contain undesirable content like malware.

There are two primary methods for redirecting HTTP traffic to a proxy: explicit redirection and transparent redirection. These different methods require different steps to be taken in order to function properly in combination with Umbrella.

This article discusses how an HTTP proxy affects the behavior of Umbrella and each portion of the Umbrella solution and then provides two sets of steps for explicit redirection and transparent redirection.

This diagram is a summary of the solutions outlined in more detail:

<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

How an HTTP Proxy Affects the Umbrella Global DNS Service

When intercepting HTTP/S traffic, an HTTP proxy reads the Host header in the HTTP/S request, and generate its own DNS query for that host. Thus, it is important to take the behavior of the proxy into consideration when deploying Umbrella solutions. At an abstract level, this involves ensuring that HTTP/S connections to Umbrella IP addresses are not redirected to the proxy, but are instead sent directly to their intended destination.

Network Protection

When using only Umbrella Network protection, it is recommended that the HTTP proxy itself is configured to either use Umbrella directly for DNS resolution, or it can use an internal DNS server which in turn forwards DNS queries to Umbrella. The appropriate external IP address can be registered as a Network identity in the Umbrella Dashboard. In this scenario, no additional action is required in order to use Umbrella.

If this is not possible for some reason, and clients themselves are using Umbrella, then the actions detailed in this article can be taken in order to ensure that enforcement is not bypassed by the HTTP proxy.

Umbrella Roaming Client

When using the Umbrella roaming client, DNS queries from the client machine are sent directly to Umbrella. However, since an HTTP proxy performs its own DNS queries, this renders enforcement by the Umbrella roaming client ineffective. Thus, when using the Umbrella roaming client in a proxied environment, the actions detailed in this article must be followed.

Virtual Appliances and Active Directory Integration

The Virtual Appliance (VA) is intended to act as the DNS server for client machines on the protected network. As such, the use of an HTTP proxy renders its enforcement ineffective in the same manner as the Roaming Client. As such, the actions detailed in this article can be followed in order to ensure that enforcement is effective and reporting is accurate.

In addition to the actions below, it is recommended that the HTTP proxy be configured to use the VA as its DNS server. This allows you to define a policy specific to the proxy so that queries from the proxy can be

identified. Such a policy also allows you to disable logging for queries originating from the proxy, which avoids have duplicate queries in your reports.

Explicit Proxies

Deploying an explicit proxy entails modifying the browser proxy settings in order to explicitly redirect traffic to a proxy. This is done either by using Group Policy in Windows, or more commonly, by using a Proxy Auto-Configuration (PAC) file. In either case, this causes the browser to send all HTTP traffic directly to the proxy, instead of sending it to the remote site. Because the browser knows that the proxy generates its own DNS request, it does not bother to resolve the hostname of the remote site itself. Additionally, as mentioned earlier, when the HTTP connection reaches the proxy, the proxy generates its own DNS query, which can be given a different result than the client would get.

Thus, in order to function properly with Umbrella, two changes are needed:

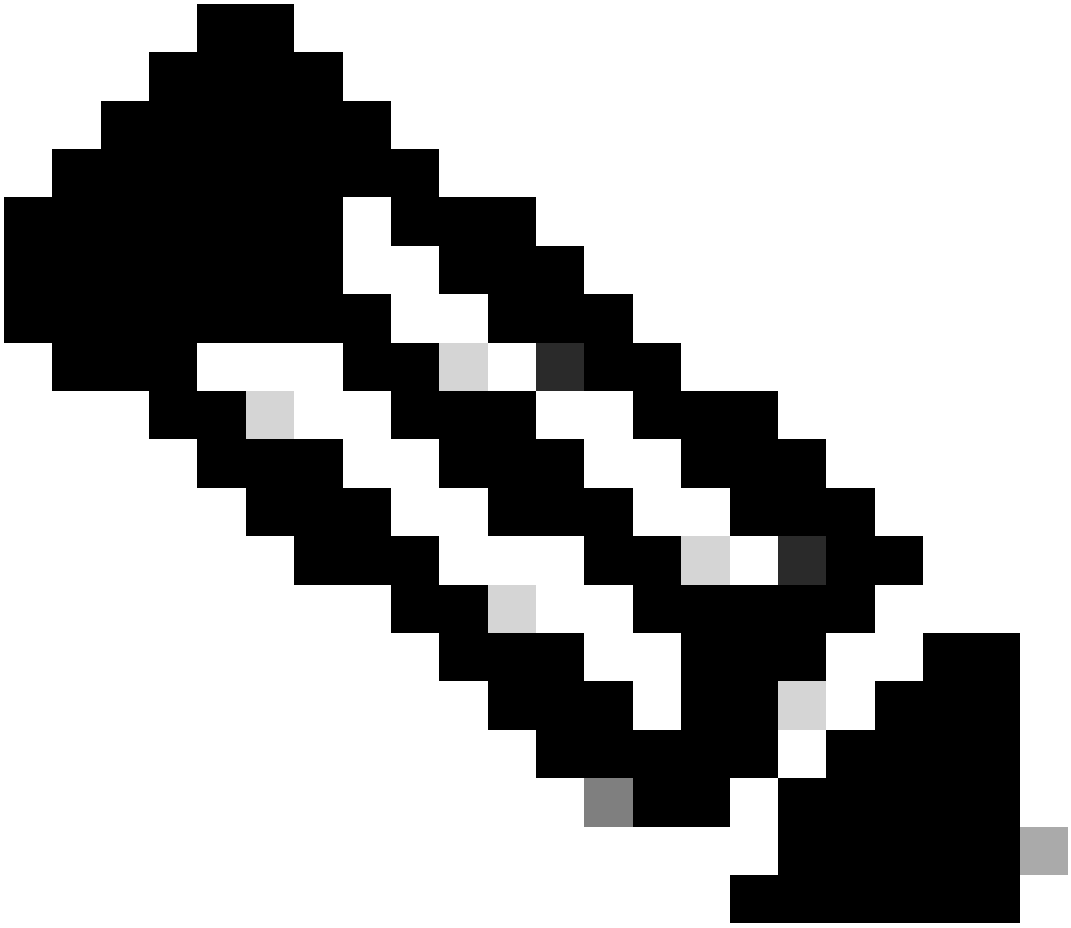
1. The client must be forced to make a DNS query.
2. HTTP connections destined to Umbrella IP addresses must not go to the proxy, but rather go directly to Umbrella.

Both of these changes can be accomplished using a PAC file:

```
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 this sample PAC file, a DNS query is first generated, with the resulting IP being captured in the **hostIP** variable. This resulting IP address is then compared to each Umbrella IP address range. If there is a match, then the query is not sent to the proxy, but instead is sent directly out. If there is not a match, then the request is sent to the appropriate proxies.

Note that, for sites that are not blocked and thus do not get redirected to an Umbrella IP address, the effect of using the previous PAC file is that both the client and the proxy makes a DNS request for the remote host. If the proxy is also using OpenDNS, this means that your reports shows duplicate queries. If you are using the Virtual Appliance, as mentioned earlier, this can be accounted for by creating an Internal Network identity for your proxy. If so desired, you can additionally create a policy for the proxy which disables logging completely in order to hide these duplicate requests.



Note: If you are blocking outbound HTTP/S requests at your firewall from sources other than your proxy, you must ensure that you allow these requests to the IP ranges discussed earlier in order to allow your machines to access the Umbrella block pages.

Transparent Proxies

For a transparent proxy, HTTP traffic is rerouted to the proxy at the network level. Because the client is unaware of the proxy, the browser generates its own DNS request. This means that if the proxy is also using Umbrella, each request is duplicated. Additionally, the policy is not properly applied as the proxy uses the DNS response that it received, not the result the client received.

Unlike the explicit case from earlier in this article, resolving this issue does not require us to force a DNS request on the client, as that is already occurring. However, bypassing the proxy for HTTP connections to Umbrella IP addresses is still required. The method for doing this varies widely depending on what mechanism you are using to redirect traffic to the proxy. In general, however, it involves exempting the Umbrella IP address ranges from being redirected.

For example, suppose WCCP is being used on a Cisco ASA to redirect traffic to the proxy, using this ACL:

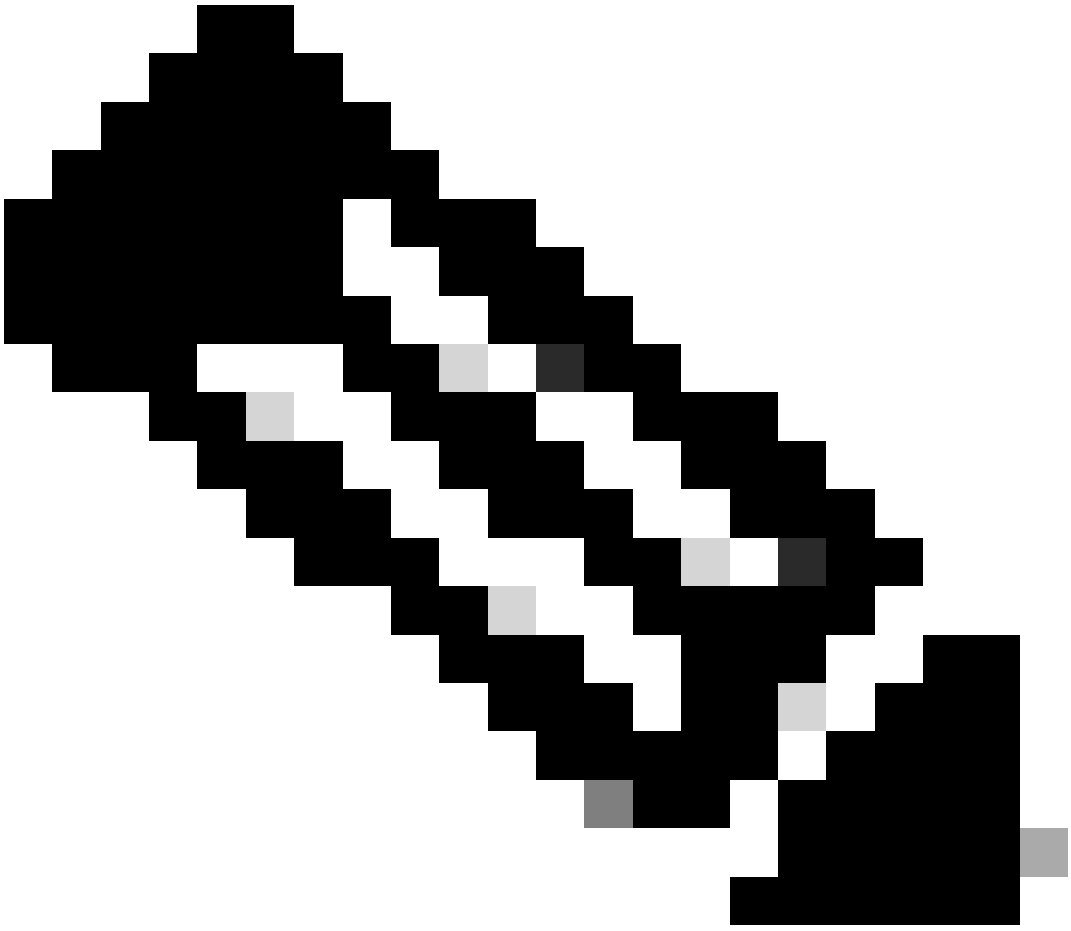
```
access-list wccp-traffic extended permit ip any any
```

The wccp-traffic ACL could be modified to deny redirection to the proxy (thus bypassing the proxy) for Umbrella IP ranges:

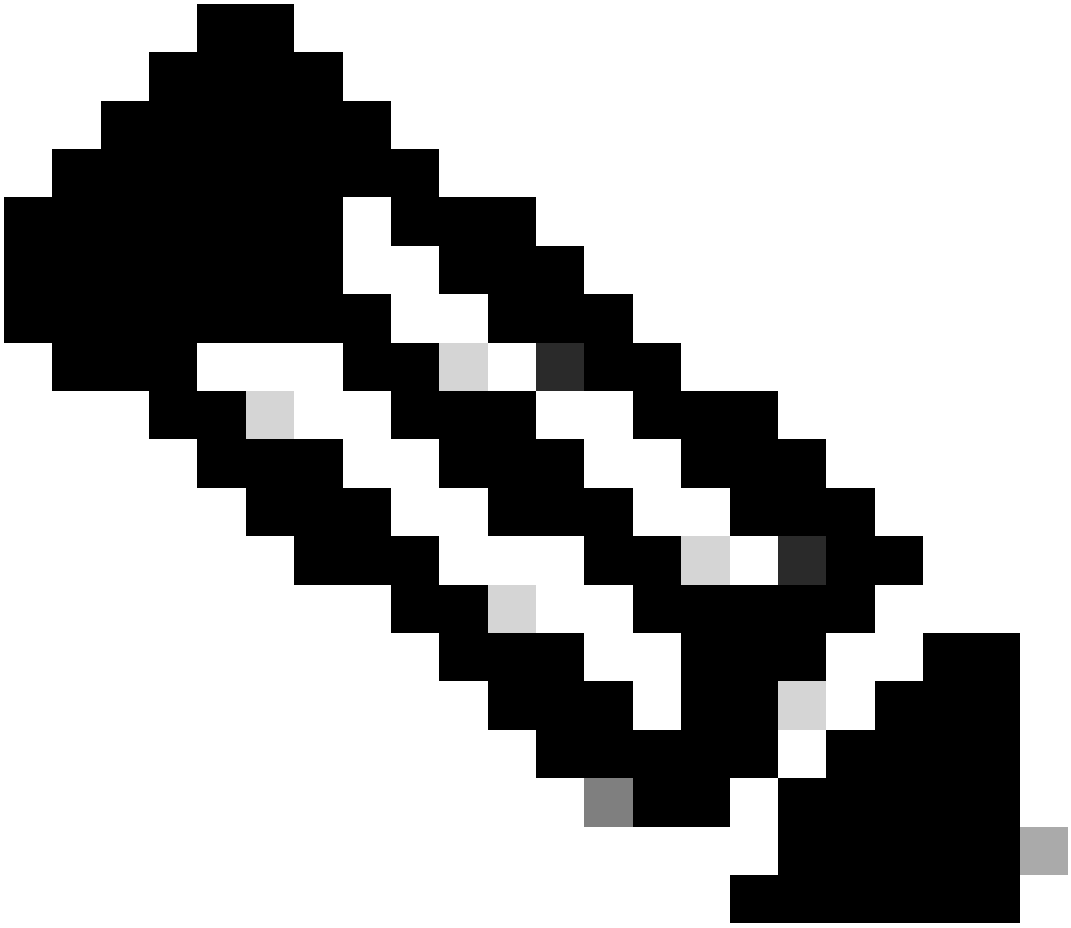
```
access-list wccp-traffic extended deny ip any 67.215.64.0 255.255.224.0access-list wccp-traffic extende
access-list wccp-traffic extended deny ip any 155.190.0.0 255.255.0.0
access-list wccp-traffic extended deny ip any 151.186.0.0 255.255.0.0



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



Note: This ACL has not been tested and vary depending on the ASA version or Cisco IOS® version being used. Please ensure that any ACLs you create are appropriate for your solution, and have been thoroughly tested prior to being deployed in a production environment.



Note: If you are blocking outbound HTTP/S requests at your firewall from sources other than your proxy, you must ensure that you allow these requests to the previously-discussed IP ranges in order to allow your machines to access the Umbrella block pages.