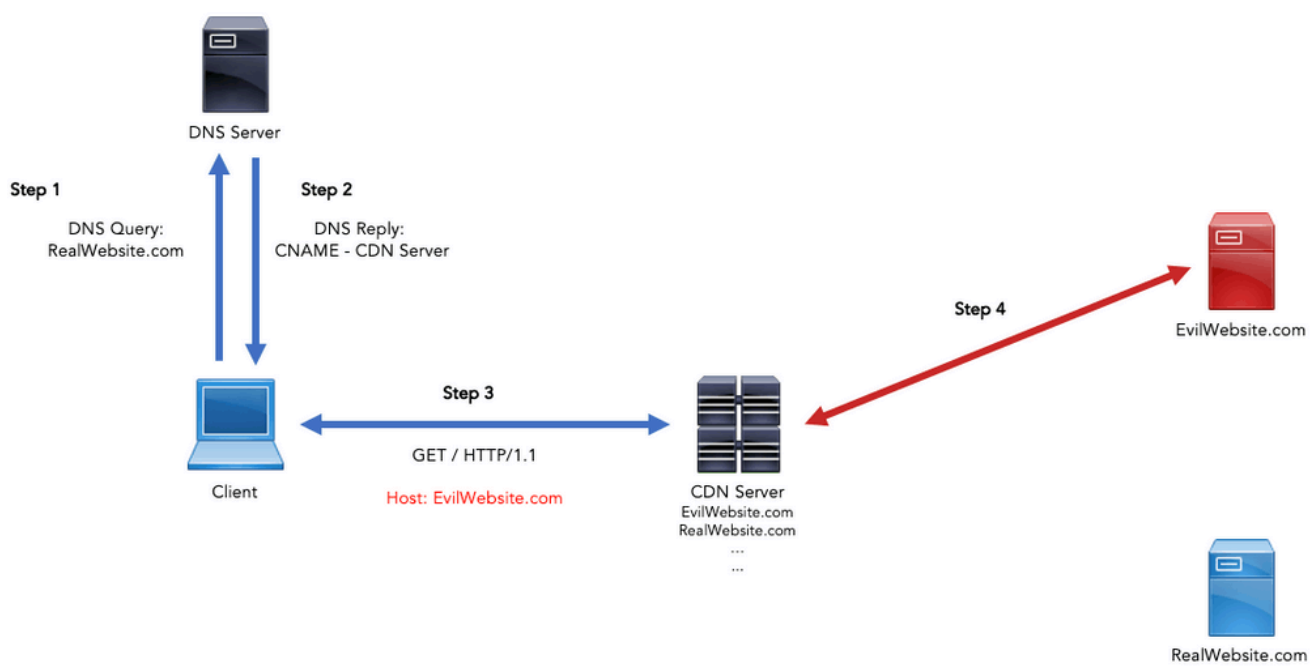
Experts Blog



HIDING BEHIND THE FRONT DOOR

March 18, 2021

Adam Brown

Introduction

Domain fronting is a generic technique based on HTTPS that allows an actor to hide the true destination of a communication from network equipment in the path. While domain fronting has been used in offensive engagements for several years now, the number of frontable cloud services continues to dwindle. Today, Fortalice is publicly adding another service to that list: Azure Front Door.

An Overview of Domain Fronting

Since there are plenty of great write-ups on how domain fronting works, this post will not go in depth on the technique's nuances. However, it is important to understand, at a basic level, the cases in which domain fronting exists.

When a web request is made in most cases, a domain name is used to tell the browser where the requested content lives. The domain name is then resolved to an IP address, and the web request is sent to that IP address. With HTTP/1.0, this simply meant that a request received by a server for a specific filename would always serve the same file. In practice, this means that a web server can only host one set of content for one website.

However, it was inefficient to limit a server to hosting content for just one site. With HTTP/1.1, the Host header was introduced. The Host header is a part of the HTTP request that specifies what website the request is intended for. In practice, this meant that a web server could now host multiple sets of content for multiple websites, a concept known as virtual hosting, and it is the Host header's job to tell the web server which domain is responsible for the requested content. With this knowledge, by changing the host header in an otherwise legitimate request, a user could send a web request to Domain A, supplying a host header for Domain B which is hosted on the same server, and receive content for Domain B.

Obviously, the trick to the previous scenario is knowing which sites are hosted on the same web server. With services like CloudFront, Azure CDN, and now Azure Front Door, their web servers handle content delivery for thousands of websites. This means that web requests for many public websites are routed to the service's web servers, and the web servers use the host header to determine which customer's content to serve. Identifying sites that use these services is as simple as performing a DNS request and looking for certain domain names in a CNAME response. For example,

Categories

Application Security
Press Release
Client Advisory
Defensive Perspectives
Offensive Perspectives
Executive Perspectives

Recent Posts

Predicting the Future of Cybersecurity
UnitedHealth Breach
Navigating SEC Cybersecurity Disclosures and Materiality

Let's Talk

Name

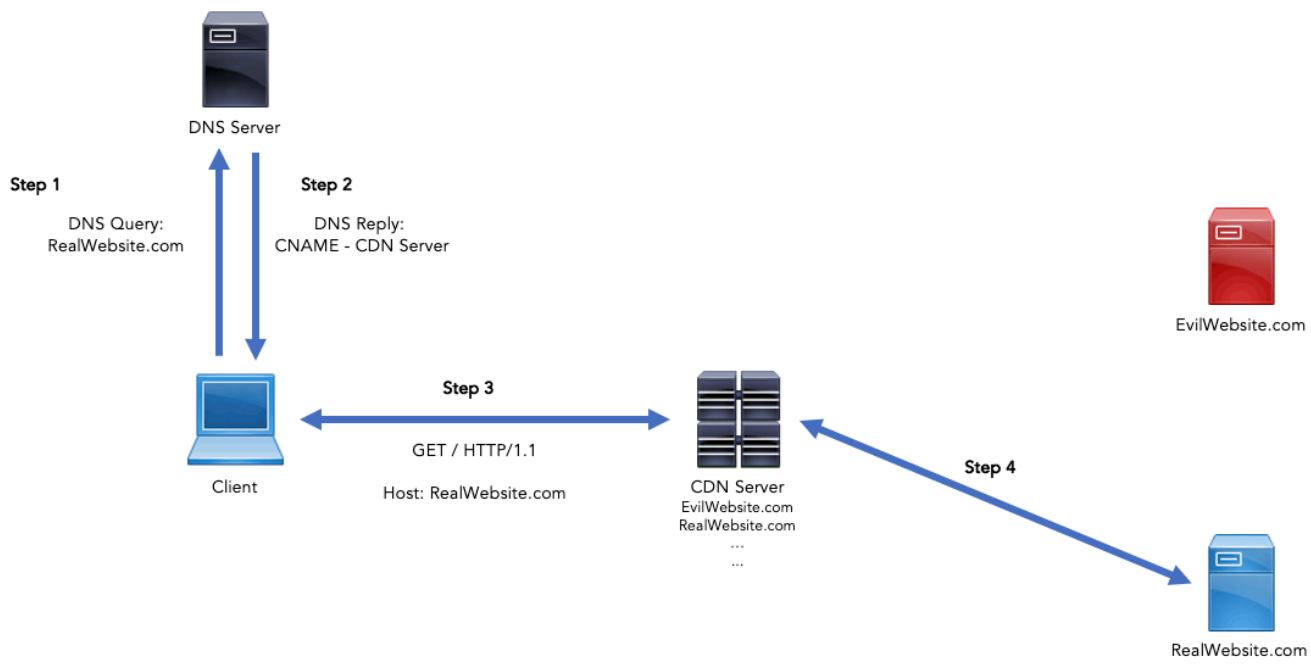
Email Address

Message

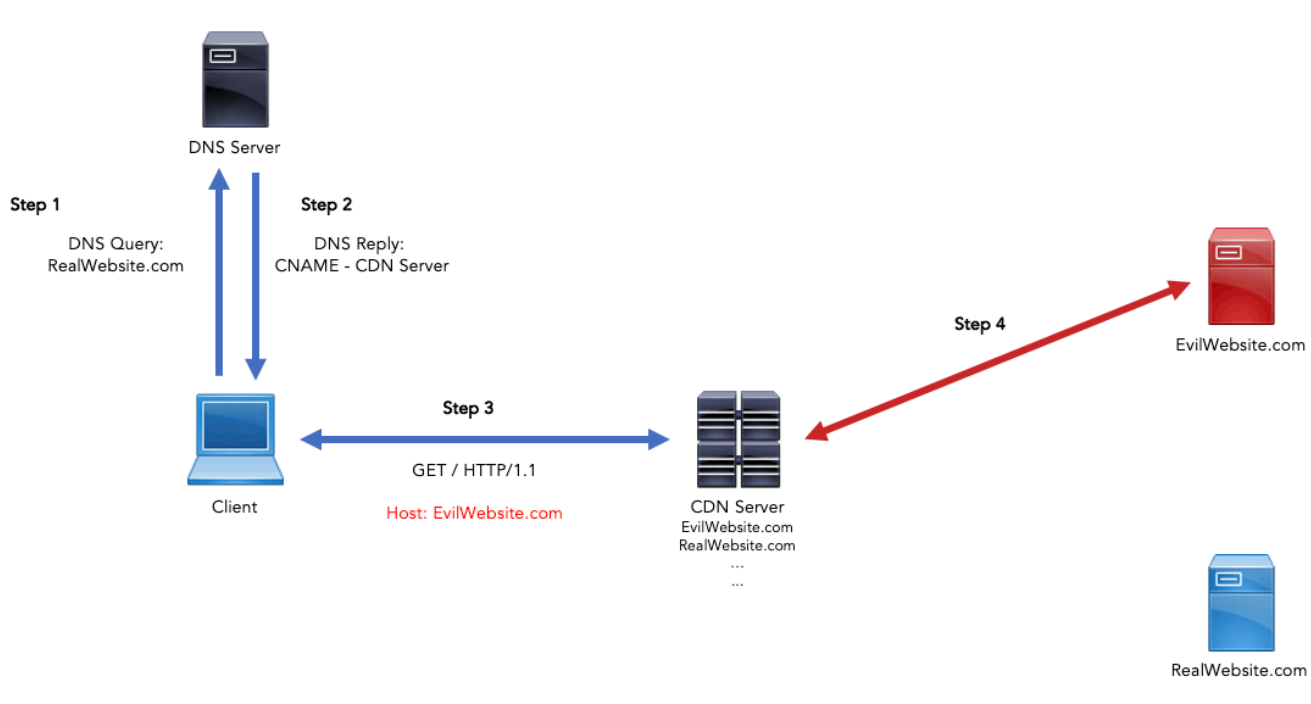
Submit

if a DNS request fora domain returns a CNAME of *.azureedge.net, then it is known that the site uses Azure CDN to serve its content.

The over-simplified graphic below demonstrates how domain fronting works, visually. A client makes a DNS query for a website, RealWebsite.com. A DNS server replies to that query with a CNAME record that points to a Content Delivery Network (CDN) server hosting the content for RealWebsite.com. When the client sends an HTTP request to that server with the correct host header, the CDN server responds with content for RealWebsite.com.



As described earlier, the CDN server's response is based solely on the Host header given in step 3. If the host header were to be changed by a malicious user to EvilWebsite.com, then the CDN server would serve content for EvilWebsite.com, even though everything leading up to the original request appeared to be intended for RealWebsite.com.



One topic that hasn't been covered yet is encryption. In both of the above scenarios, the certificate presented belongs to RealWebsite.com making the traffic appear even more legitimate. If you would like to read further on domain fronting, please reference the following resources:

https://www.bamsoftware.com/papers/fronting/

https://malcomvetter.medium.com/simplifying-domain-fronting-8d23dcb694a0

https://digi.ninja/blog/domain_fronting.php

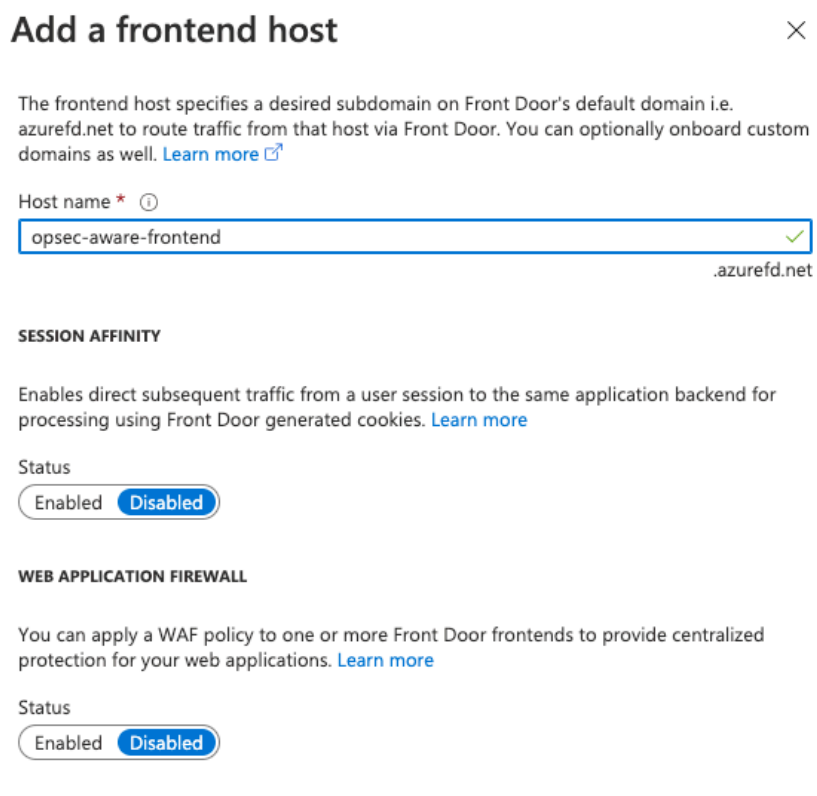
Azure Front Door

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. The goal of this product is to route client requests to the fastest and most available application backend that exists for the application in the given scenario. Since this is a system that serves web content from many different backend locations, it was assumed to be susceptible to domain fronting. While users of Front Door will gain functionality over a service such as Azure CDN, it comes with a price. Data transfer rates are similar between the service offerings but be aware that the standard Azure Front Door service has a base fee for hourly uptime.

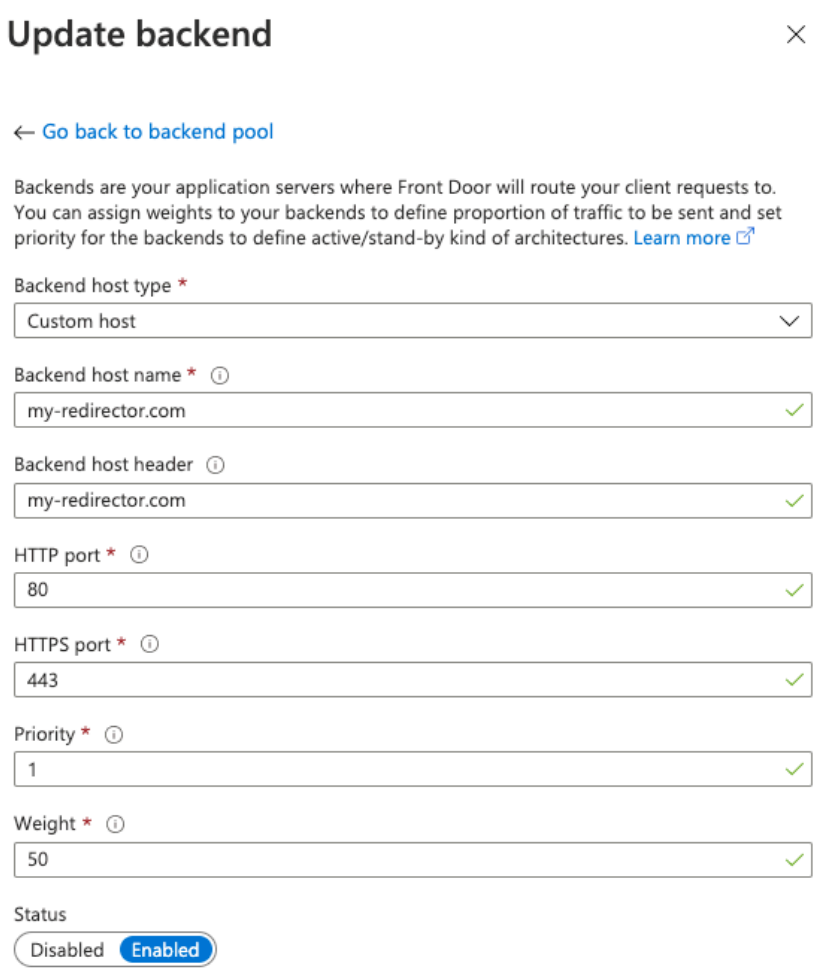
It is very easy to start domain fronting using the Azure Front Door service. Navigate to the Front Doors section of the Azure Portal and click the "Add" button to create a new Front Door instance.

Under the basic options, select the desired subscription and resource group for the new Front Door instance and proceed to the next section. The configuration section is where the frontend, backend, and routing rules will be set up. The frontend will be a *.azurefd.net domain that is chosen by the

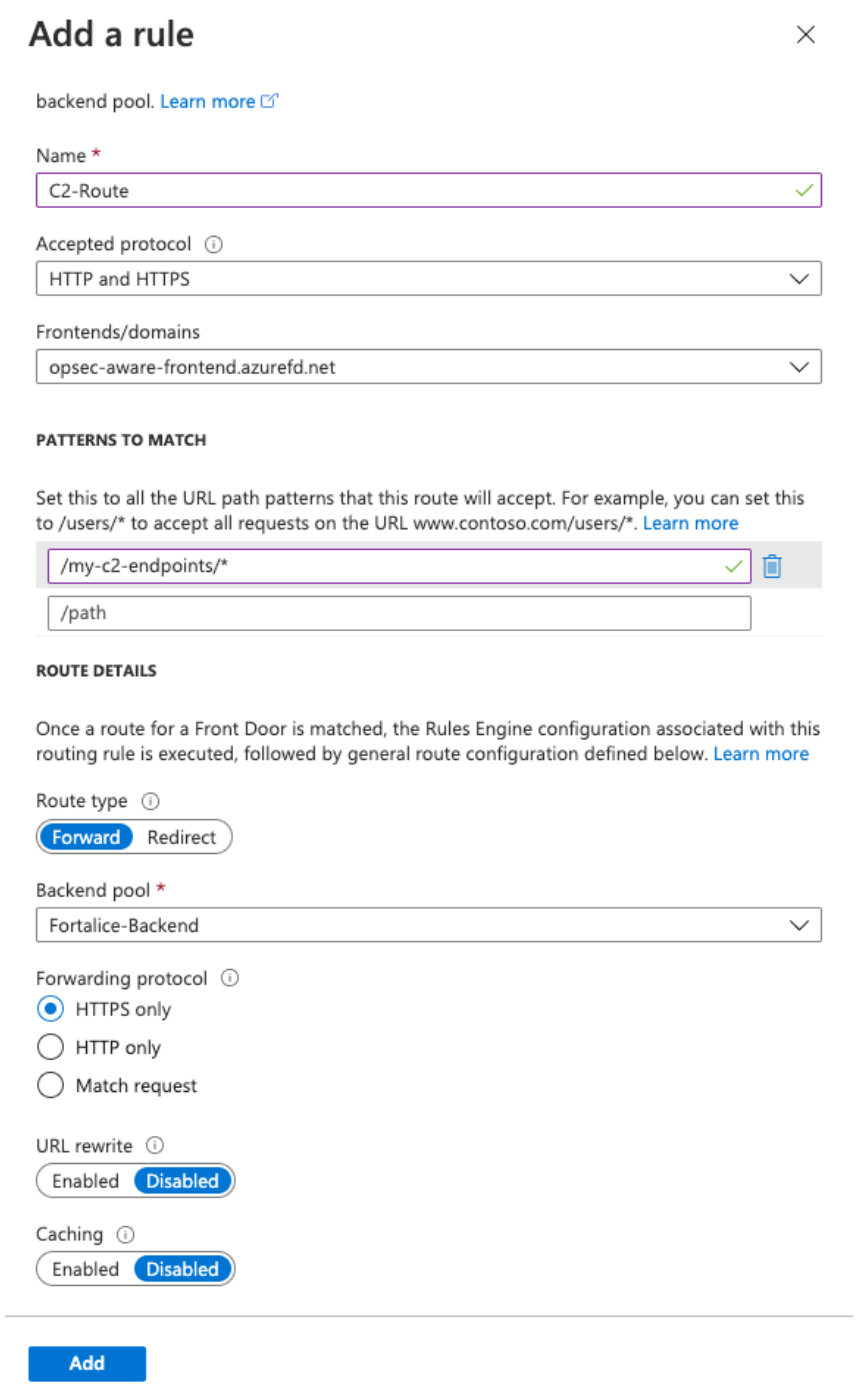
creator. This can be anything but should be something that categorically fits the domain that will be fronted. Feel free to leave the session affinity and web application firewall disabled, or tweak to your heart's content.



When adding a backend pool, the creator will specify where the web content (in this case, command and control (C2) servers, redirectors, or decoys) exist. Give the backend an identifiable name and click "Add a backend". The backend host type should be "Custom host", and the rest of the information should be relatively straight-forward. Feel free to disable Health Probes and configure the rest of the backend pool as it fits your needs.



Finally, the routing rules can be added. These rules are used to connect frontends to backends, and multiple rules can be used in conjunction with C2 profiles to control which traffic is forwarded back to a C2server, and which traffic is forwarded to a decoy site. The default options should work but can be customized for your own opsec considerations.



Finding Domains That Use Front Door

With the routes set, the Front Door is ready to be utilized directly or through the use of a fronted domain. Finding frontable domains is a separate problem that has already been solved by a variety of public toolsets. With this post, the Fortalice team will be issuing a pull request to a popular tool called FindFrontableDomains. This tool uses Sublist3r to enumerate subdomains for a chosen target. Sublist3r discovers subdomains through many different sources including search engines, Netcraft, DNSdumpster, VirusTotal, SSL certificates, and Passive DNS to find subdomains. FindFrontableDomains then takes the assets discovered by Sublist3r and attempts DNS requests foreach subdomain. Any response that includes a CNAME reference to a cloud provider known to be frontable is marked and given to the user as a potentially frontable domain. The pull request Fortalice issues will add Azure Front Door to the list of services that FindFrontableDomains is looking for.

Detection Points

With any offensive tooling improvement, disclosing how to defend against it is always important. However, there are no new detection techniques to be disclosed here because domain fronting is not a new technique. Using SSL inspection, the Host field of the HTTP header can be checked if it matches the HTTPS SNI, or against a blocklist or allow list of domain names. More information about domain fronting can be found on the MITRE ATT&CK website. For additional information on Fortalice Solutions service offerings, contact the team via email at watchmen@fortalicesolutions.com

Offensive Cybersecurity Operations

Related Posts

UnitedHealth Breach

Red Team

Comprehensive Application Security Assessments: Identifying and Addressing Application Vulnerabilities

Fortalice Solutions

Discover the significance of comprehensive application security assessments in identifying and addressing software vulnerabilities. Learn about the different types, including manual code reviews, automated vulnerability scanning, penetration testing, and security architecture reviews. Fortalice blog offers valuable insights to help you choose the right assessment for your organization.

Let's Talk

Stay Connected

Fortalice

Fortified Security

US: 877.487.8160
watchmen@fortalicesolutions.com

Headquartered in Charlotte, NC

First Name*

Last Name*

Email*

Phone

Company Name

Title

Message

SEND MESSAGE

Privacy Policy