ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

IP Expiration and Host Name Mismatch: A Common Client Server Connectivity Issue

Prashanth Kodurupati

Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, USA

ABSTRACT

Most whitelists refer to IP addresses, not host names, so when an IP address expires, a client-server may be unable to establish a secure connection with the host server because the new IP address is not on the whitelist. The problem is different for dynamic and static IP addresses because of the inherent change frequency, thus warranting different solutions. For dynamic IP, more flexible whitelists or automated whitelist modifications may be more feasible. For static IPs, manually modifying the script that allows whitelisted servers to pass through the firewall may make more sense, especially if security is a major concern.

***Corresponding author**

Prashanth Kodurupati, Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, USA.

Received: September 01, 2022; **Accepted:** September 07, 2022; **Published:** September 15, 2022

Keyword: IP Expiration

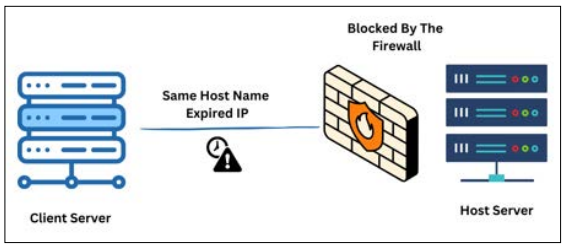
Introduction

Over the years, the internet has become as critical for life as basic utilities, and it's just as important for businesses as it is for individuals. However, with everything connected to the internet and businesses relying on these connections for their various operations, their "attack surface" stretches out, resulting in a range of cybersecurity vulnerabilities. Therefore, almost all businesses have certain cybersecurity layers in place, though they may vary based on the business, their security needs, and how they may interfere with operations and convenience. While some businesses may allow a comprehensive range of client servers to connect and exchange data, others employ more stringent security measures like whitelisting, allowing only a select few client servers to connect. However, it may lead to certain problems connected to common networking elements like dynamic IPs and IP expiration.

Literature Review

IP whitelisting is a time-tested security mechanism to prevent unauthorized client servers from making connections with the host servers, and over the years, it has evolved into a more comprehensive solution, often working in combination with other similar solutions like a blacklist, which may lead to a better distribution or defensive tasks [1]. A wide range of challenges associated with IP whitelisting that may diminish its utility as a security measure or cause it to hinder normal operations have been identified and rectified over the years, and there is ample literature covering those solutions, including dynamically adding or subtracting IP whitelisting [2]. Management, allotment, and expiration on IP addresses have been a focus for even longer than IP whitelisting, as it's one of the key components of internet infrastructure and global connectivity. There is literature on IP expiration being used as a defensive mechanism in a wide array of conditions, including the safety of vehicles connected to the internet [3]. IP address expiration and updation of the whitelist or at least exclusion from blacklists or suspicious IP, as a pattern that modern firewalls can be made to understand and leverage with the right rules, is another avenue that has already been explored in the industry as well as in the literature, establishing it as a mature practice [4].

Problem Statement: IP Expiration and Whitelisting



Maintaining an IP whitelist manually or through a script capable of handling certain changes, especially if automated requests can be generated and sent to client servers for updated IPs that can be used to modify the IP whitelist, is a crucial part of most networking professionals. The tasks get a bit more complicated when the firewalls have to be managed just from the perspective of establishing a connection but for file transfer protocols as well. Still, the primary goal when you have a whitelist is to ensure that it's updated with the latest IPs of the servers/host names of the client servers permitted to establish a connection with the host server. Otherwise, their requests would be rejected like any other unknown IP or hostname trying to establish a connection.

There are multiple reasons why you may need to refresh your whitelist with the latest IP addresses associated with your clients and their host names, and a common reason is IP expiration.

IP Expiration in Dynamic IPs

Most IP addresses nowadays are dynamic, and they are assigned to a device or server by an Internet Service Provider (ISP) through a Dynamic Host Configuration Protocol (DHCP). This protocol automatically assigns IPs to each device connected to the internet through the ISP, and the IPs change over time, following a "lease system" [5]. An IP address is assigned to a device or a server for a predefined time, which may range from a few hours to a few days, and once the lease is up, the protocol assigns a new IP to it. If the new address isn't updated on the whitelist of the host server it wishes to connect with (even though the hostname is unchanged), the connection may fail.

IP Expiration in Static IPs

The concept of lease is rare for static IP addresses and may be found in very specific use cases, like behavior-aware IP configurations [6]. These IP addresses are assigned manually and individually by ISPs to businesses like financial institutions and VPN companies that require their servers to have a consistent, static address. While these IPs may be permanent in most cases, there are some instances when they may have a "life" or a lease period, though it's typically in years, not hours or days. Once they expire and if all the host servers the client-server with an expired static IP wishes to connect to is not intimated, it can prevent the servers from establishing a secure connection.

Another scenario where static IPs may expire is when the servers are provided by clouds and hosted on Virtual Machines (VMs). Other than that, major changes in a network or if a business is switching to another ISP, may also result in a new static IP being assigned to a business's server.

Suggested and Implemented Solutions

The basic solution to both dynamic and static IP expirations is updating the whitelist with the new IP addresses. However, they are implemented differently.

Dynamic IP Whitelist Update

Since dynamic IP addresses expire quite frequently, updating the whitelist with new addresses manually is not feasible, especially when the individual responsible for maintaining the whitelist has to deal with several client servers.

One solution is that client servers use a dynamic Domain Name System or dynamic DNS, which always points to the latest IP [7]. However, that would require the whitelist rules to allow for Host Name pass-throughs instead of (or in addition to) IP addresses.

Another solution that is more relevant to use cases where safety and security are paramount and good communication exists between client and host business is to write a script for automating the whitelist update process. Once new IP addresses are received from the client servers, the script can update the whitelist on the host servers, allowing the client servers to pass through the firewall and establish a connection.

Static IP Whitelist Update

Since static IPs change rarely, and usually, there is a significant gap between two consecutive changes in the static IP of the same client-server, it's feasible to do it manually or via a script that handles the content and rules of the whitelist. However, reaching out to the client is required to obtain the latest static IP address.

Summary of Problems and Proposed Solutions

IP Expiration Problem	Solution
Dynamic IP expiration: Client-server receives new IP, but host server whitelist isn't updated.	1. DDNS (Dynamic DNS): Client-server uses a service to register a hostname that always points to its latest IP. Host server whitelists the hostname instead of specific IP.
	2. Changing Script (Limited Use): Script automates updating whitelist based on information provided by the client. Requires client cooperation and can be cumbersome for frequent changes.
Static IP expiration (rare): Lease expires, or network changes cause a new static IP.	Manual update or script-based update of the host server whitelist with the new static IP obtained from the client.

Best Practices to Avoid Client Server Issues

The two best practices that may help you avoid this issue arising are:

- Ensuring clear communication channels and encouraging clients to share the updated IPs as soon as possible. Ideally, the process should be automated from the client side so as soon as the server receives a new IP after the expiration of the old one, you have access to it and can use it to update your whitelist.
- Establishing clear protocols for updating both dynamic and static IPs. This will prevent any unintended consequences if the whitelist/firewall rules are more comprehensive and not automatically updated along with the whitelist. Clear protocols and instructions can prevent expired IPs from hindering any business activity.

Potential Use Cases

The use cases for different solutions that can be implemented to avoid IP expiration issues are different from business to business. For most local connections where cybersecurity concerns are limited, easy-to-implement solutions like flexible, host-name-oriented whitelists on the host side and Dynamic DNS on the server side may be considered viable solutions. In contrast, high-risk environments like financial institutions may warrant a more hands-on approach, i.e., modifications to the script that contains the rules for the whitelist.

Conclusion

While the IP expiration and update (both static and dynamic) is an arrangement between client servers and their ISPs and influenced heavily by the ISP's DHCP, client businesses should find a way to keep host servers in the loop. If the new IP addresses are communicated promptly, the whitelist can be updated, preventing any disconnectivity issues. An IP expiration (if it prevents client servers from establishing a secure connection with the host server) can be a critical operational challenge for businesses that rely upon information and data from certain host servers to continue their activities (like banks and credit bureaus). Host servers should have protocols for generating the request for a new IP address, ideally as soon as the old one expires, so they can update their script to govern this connection.

References

1. Spathoulas G, Collen A, Pandey P, Nijdam NA, Katsikas S, et al. (2018) Towards Reliable Integrity in Blacklisting: Facing Malicious IPs in GHOST Smart Contracts. 2018 Innovations in Intelligent Systems and Applications (INISTA) https://ieeexplore.ieee.org/document/8466327.
2. Burton R, Rocha L (2019) Whitelists that Work: Creating Defensible Dynamic Whitelists with Statistical Learning. 2019 APWG Symposium on Electronic Crime Research (eCrime) https://docs.apwg.org/ecrimeresearch/2019/Nov14_ReneeBurton.pdf.
3. Ayrault M, Borde E, Kühne U (2019) Run or Hide? Both! A Method Based on IPv6 Address Switching to Escape While Being Hidden. MTD'19: Proceedings of the 6th ACM Workshop on Moving Target Defense https://dl.acm.org/doi/10.1145/3338468.3356827.
4. Ahmad W, Singh DD (2018) VoIP Security: A Model Proposed to Mitigate DDoS Attacks on SIP Based VoIP Network. Research for Resurgence A Multi-Disciplinary Research Book https://www.researchgate.net/publication/331149311_VoIP_Security_A_Model_Proposed_to_Mitigate_DDoS_Attacks_on_SIP_Based_VoIP_Network.
5. Wang H, Wang JH, Wang J, Dang W, Xue J, et al. (2020) Squeezing the Gap: An Empirical Study on DHCP Performance in a Large-Scale Wireless Network. IEEE/ACM Transactions on Networking 28.
6. Miao C, Wang J, Ji T, Wang H, Xu C, et al. (2019) BDAC: A Behavior-aware Dynamic Adaptive Configuration on DHCP in Wireless LANs. 2019 IEEE 27th International Conference on Network Protocols (ICNP) https://ieeexplore.ieee.org/document/8888048.
7. Liu J, Huo S, Wang Y (2018) A Hierarchical Mapping System for Flat Identifier to Locator Resolution Based on Active Degree. Future Internet 10.