GeForce NOW SDK: NGN Endpoints

API Reference

Document History

SDK-GFN-001_v1.0

Version	Date	Description of Change
0.1	*05/09/2019*	*Initial version*
1.0	*07/17/2019*	*First release version*
1.1	11/23/2021	Updated to reflect use of CIDR, as well as some rewording/formating

Introduction

The NGN Endpoint API is part of the GeForce NOW (GFN) SDK and allows clients to perform a web query and receive a complete list of IPs associated with GFN.

Audience

This document is directed towards Publishers, those that are game launcher/store application developers leveraging GeForce NOW in their application to stream content via seamless UI, and Game Developers, those that are developing games to be streamed via GeForce NOW.

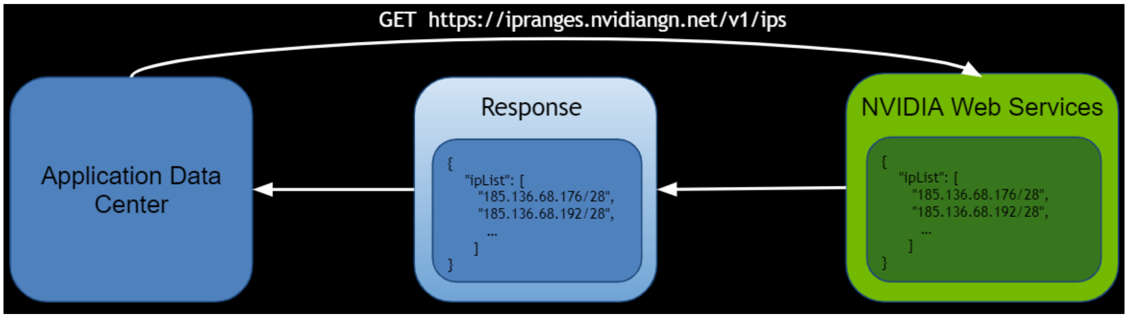
The API defined in this document allows this audience to query the full list of IPs associated with GeForce NOW traffic to set traffic rules such as QoS rules for prioritizing the traffic, or whitelisting to prevent false positives for threat detections.

Overview

This document contains a high-level overview of the API, as well as the format of the API query and the definition schema of the response.

Key Concepts

The API is a simple single HTTP GET query, which provides a response in the form of a JSON string list of all the GFN-specific IPs.



```
{
  "ipList": [
    "185.136.68.176/28",
    "185.136.68.192/28",
    ...
  ]
}
```

```
{
  "ipList": [
    "185.136.68.176/28",
    "185.136.68.192/28",
    ...
  ]
}
```

This API should be called on initialization of any applications or systems that rely on the IPs for proper traffic handling, or routines that attempt to detect and block any traffic that might look suspicious. For example:

- A group of gamers playing a specific game that phones home with data in GFN on the same server could be interpreted as a DDoS attack, triggering traffic blocking rules.
- A single gamer playing a specific game frequently in GFN could be playing on different server instances each time, resulting in the game's source IP changing frequently, and triggering certain account protection rules.

Instead of treating these scenarios as potential threats and degrading the gamer's experience in playing the game, these source IPs and the traffic from them can be assumed to be valid and thus ignored by any threat detection algorithms and software.

As GFN servers are routinely added to improve users' experiences with the service, new IPs are constantly added to the returned data. As such, it is suggested that the IP data be cached for no more than 24 hours at a time.

API Reference

This section details the HTTP GET endpoint as well as the JSON schema of the response.

The table below lists all methods of the NGN Endpoint interface.

Method	Description
GET IPs	Get a list of all GeForce NOW NGN IPs

Get IPs

Queries the GeForce NOW data center for all GFN-related IPs via a JSON-based response.

Common Use Cases

The table below lists the common use cases for this method.

Use Case	Description
QoS Rules	Prioritizing traffic from GFN IPs
Multiple IPs from account	Allowing a game account to be used from multiple GFN IPs in a short span of time
Multiple accounts from IP	Allowing multiple game accounts from a single GFN service IP to be used at once

Request

HTTP Request

```
GET https://ipranges.nvidiangn.net/v1/ips
```

Authentication

None

Parameters

None

Request Body

None

Success Response

HTTP 200 with JSON data utilizing Classless Inter-Domain Routing (CIDR) format. Schema:

```
{
    “ipList: {
        “type”:”array”,
        “items”: {
            “type”:”string”
        }
    }
}
```

Error Responses

Standard HTTP error responses

Expected Response Time

Response to the query will be within 1 second.

Examples

```
{
   {
     "ipList": [
         "185.136.68.176/28",
         "209.66.87.160/27",
         "8.7.235.176/28",
     ...
   }
}
```

CIDR is used to greatly reduce the amount of data transmitted by covering a range of sequential IPs in a single entry.. This means it is up to the caller to process an entry for its entire range. For example, the single entry:

```
     "185.136.68.176/28"
```

Covers all IPs in the range of 185.136.68.176 to 185.136.68.191 inclusively.