



GeForce NOW SDK: NGN Endpoints

API Reference

Document History

SDK-GFN-101_v1.0

Version	Date	Description of Change
1.0	05/09/2019	Initial version

NVIDIA CONFIDENTIAL

GeForce NOW SDK: NGN Endpoint API

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

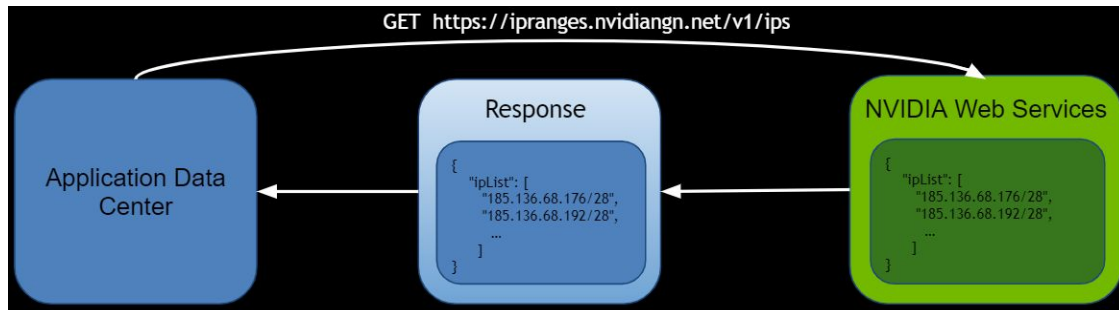
This document is directed towards Publishers and Affiliates that will receive network traffic from the GeForce NOW ecosystem, allowing them to query the full list of IPs associated with the traffic. The returned list of IPs allows for setting traffic rules such as QoS rules for prioritizing the traffic, 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.



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 in GeForce NOW that phones home with various data could be interpreted as a DDoS attack, triggering traffic blocking rules that degrade the gamer's experience in the game. Instead of triggering such traffic blocking rules, these IPs and the traffic from them can be assumed to be secure from such attacks and thus whitelisted in threat detection software.

API Reference

This 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	Traffic from GeForce NOW IPs to be given a specific priority
Threat Whitelisting	Traffic from GeForce NOW IPs to be whitelisted in threat detection

Request

HTTP Request

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

Authentication

None

Parameters

None

Request Body

None

Success Response

HTTP 200 with JSON data. Schema:

NVIDIA CONFIDENTIAL

GeForce NOW SDK: NGN Endpoint API

```
{
  "ipList": {
    "type": "array",
    "items": {
      "type": "string"
    }
  }
}
```

Error Responses

Standard HTTP error responses

Expected Response Time

Response to query will be within 1 second.

Examples

```
{
  {
    "ipList": [
      "185.136.68.176/28",
      "185.136.68.192/28",
      "209.66.87.160/27",
      "8.38.38.128/28",
      "8.44.52.192/27",
      "8.42.102.240/28",
      "185.136.69.160/28",
      "8.44.45.192/26",
      "8.44.53.248/29",
      "8.7.235.176/28",
      ...
    ]
  }
}
```