Understand Allowed IPs in Firewalls for Secure Web Gateway

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background

IP Addresses

Domains

Introduction

This document describes which IPs and domains are allowed in the firewalls for Secure Web Gateway (SWG).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on SWG deployments with a PAC file or an AnyConnect client with SWG module.

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

If you are deploying Umbrella's Secure Web Gateway (SWG), Umbrella recommends allowing SWGs IP space to ensure traffic is allowed through their perimeter firewalls. This also applies to any web filtering appliances you have.

For additional details, refer to the Cisco Umbrella SIG User Guide.

IP Addresses

Cisco Umbrella is an elastic cloud service, and its IP space is dynamic and constantly changing. If you are deploying Umbrella SWG, Umbrella recommends allowing these CIDRs on their perimeter firewalls to ensure they can connect to the Umbrella SWG service:

```
67.215.64.0/19
146.112.0.0/16
151.186.0.0/16
155.190.0.0/16
185.60.84.0/22
204.194.232.0/21
208.67.216.0/21
208.69.32.0/21
```

Traffic Profile:

- Protocol = TCP
- Ports = Outbound 80 and 443

Domains

Umbrella also recommends these domains are bypassed at the source to ensure all traffic is allowed:

```
isrg.trustid.ocsp.identrust.com
*.cisco.com
*.opendns.com
*.umbrella.com
*.okta.com
*.oktacdn.com
*.pingidentity.com
secure.aadcdn.microsoftonline-p.com
```

Additional details on Secure Access can be found:

- Cisco Secure Access Help - DNS Requirements
- Cisco Secure Access Help - Secure Web Gateway Service Requirements