Maintain Networks with Dynamic IP Addresses

Contents

Introduction

Prerequisites

- Components Used

Maintain Umbrella on Networks with Dynamic IP Addresses

- Umbrella Dynamic Network Update API

Dynamic IP Addresses: Technical Details and FAQ

- Dynamic DNS
- DNS Request Types
- SmartCache

Other Known DDNS Clients that are Likely to Work with Umbrella

Want to Learn More?

Introduction

This document describes how to maintain Cisco Umbrella network identities that use dynamic public IP addresses with the **Umbrella Dynamic Network Update API**.

Prerequisites

Before you begin, ensure that:

- You have administrative access to the Cisco Umbrella dashboard.
- A network identity has been added to your Umbrella organization.
- The network identity is configured to use a dynamic IP address.
- You have a network device, script, or automation platform capable of sending HTTPS requests when the public IP address changes.

Components Used

The information in this document is based on Cisco Umbrella Dynamic Network Update API.

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.

Maintain Umbrella on Networks with Dynamic IP Addresses

Most home, small school, and small business networks are typically provisioned by Internet Service Providers (ISPs) that issue a dynamic IP address when defining each unique internet network. A dynamic IP address can change when the ISP renews or reassigns the address lease.

Cisco Umbrella uses the registered public IP address to identify DNS requests from a network. If the public IP address changes and the network identity is not updated, DNS requests might no longer match the intended Umbrella network identity and security policy.

The Umbrella Dynamic Network Update API updates the public IP address associated with the network identity when the address changes.

To configure a network identity to use a dynamic IP address:

1. Sign in to the Cisco Umbrella dashboard.
2. Navigate to **Deployments > Core Identities > Networks**.
3. Select the applicable network identity.
4. Click the checkbox to select **Dynamic**.

After the network is configured as dynamic, configure a network device, script, or automation platform to send an update through the Umbrella Dynamic Network Update API when the public IP address changes.

Umbrella Dynamic Network Update API

The Umbrella Dynamic Network Update API allows an authorized HTTPS request to update the public IP address registered for an Umbrella network identity.

The API can be integrated with:

- Routers and firewalls that support custom network updates
- Network-management platforms
- Scheduled scripts
- Automation tools
- Other systems capable of sending authenticated HTTPS requests

For authentication requirements, supported request formats, parameters, endpoints, response codes, and more information, see the Umbrella Dynamic Network Update API documentation.



Note: Store credentials securely. Do not expose credentials in logs, screenshots, shared scripts, or publicly accessible configuration files.

Dynamic IP Addresses: Technical Details and FAQ

Dynamic DNS

Many people get a dynamic Internet Protocol (IP) address assigned to them by their ISP or network operator. The alternative is a static IP address. If you are not sure which one you have, you likely have a dynamic IP address but contact your ISP to be sure.

It is difficult for public Internet resources to know how to find a webserver or mailserver or other Internet-addressable resource located at a dynamic IP address.

DDNS provides a workaround, giving an individual a method of registering their current IP address with a third-party service on the web so they are publicly accessible and addressable, even as their IP address changes over time.

DNS Request Types

This table explains the DNS Request Types that can be collected and listed in an Umbrella report.

DNS Lookup Type	Description	Function
A	IPv4 address record	Returns a 32-bit IP address, which typically maps a domain hostname to an IP address, but also used for DNSBLs and storing subnet masks
AAAA	IPv6 address record	Returns a 128-bit IP address that maps a domain hostname to an IP address
MX	Mail exchange record	Maps a domain name to a list of message transfer agents for that domain
NS	Name server record	Delegates a DNS zone to use the specified authoritative name servers

PTR	Pointer record	Pointer to a canonical name that returns the name only and is used for implementing reverse DNS lookups
SOA	Start of authority record	Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone
SRV	Service locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX
TXT	Text record	Carries extra data, sometimes human-readable, most of the time machine-readable such as opportunistic encryption, DomainKeys, DNS-SD, and so on.

SmartCache

When an authoritative DNS provider suffers an outage, all of the Websites it provides service for are taken offline. They are inaccessible to everyone on the Internet. But no longer for Umbrella users. Our servers now immediately looks for the last known good address for the site in our caches, and use that to load the site. So effectively Umbrella users is able to access websites that appear down for everyone else.

For our millions of users at businesses, schools, and libraries around the world, this saves them from Internet access interruptions.

Authoritative DNS outages happen frequently and can be a big problem. In March of 2009, it was reported that major authoritative DNS provider UltraDNS suffered an outage that took Salesforce.com, Amazon.com and Petco.com offline for several hours. And in October 2016, an attack against DynDNS took down major portions of the internet, including twitter.com and more.

In such cases, SmartCache fixes the inaccessibility problem and allows people to visit those sites despite the authoritative server outage.

This is just the latest in a long series of DNS innovations that Cisco Umbrella developed and passed on to you. Most recently it was blocking the Conficker worm from phoning home. By blocking the domain names the worm used, we were and continue to be able to protect people around the globe.

SmartCache is turned on by default for all users and only applies to queries where the authoritative server hands back a SERVFAIL response code or the query simply goes unanswered.

Other Known DDNS Clients that are Likely to Work with Umbrella

Windows	Marcs Updater	A small updater program that helps keep your Dynamic IP

		information up to date on the Umbrella website. Also supports DNS-O-Matic and DynDNS.
Windows	HomingBeacon Dynamic DNS Update Client	ChangeIP's Dynamic DNS update client supports Umbrella updates with version 3.0.0.6 and later.
Windows	DynSite	DynSite is a shareware, that is you can try it for free for 30 days then you have to register your copy to obtain a license code (also called a serial number) if you want to keep using it. If you decide not to register you have to uninstall the program (from Control Panel > Add or Remove Programs icon.) Add the configuration file, aka the `.dns` file, to the right place.
Windows	Dynamic IP Monitor	There is a 60-minute trial version, and a full version for US$9.95. Umbrella is supported as a built-in option from version 3.2 on.
Linux	ddclient	An open-source dynamic IP updater client written in Perl.

Want to Learn More?

- Visit our tutorial video here: Register & Protect Your Network