Solution Brief

IPv6 + the Zero Trust Exchange

Supporting the transition to IPv6 compliance

Overview

Every device that connects to a network is identified through an internet protocol (IP) address. Today, the internet uses two IP address versions – version 4 (IPv4) and version 6 (IPv6), but the two protocols do not interoperate. IPv6 was created primarily to address the depletion of IPv4 addresses, which leverages a 32-bit addressing scheme that supports 4.3 billion devices. This is no longer enough to fulfill the increase of computers, mobile devices, and IoT. IPv6 uses a 128-bit alphanumeric address that supports 340 undecillion – a trillion times 3 – unique combinations, theoretically ensuring that we should never run out of IPv6 addresses.

IPv4

Deployed 1981

32-bit IP address

4.3 billion addresses
Address must be reused and masked

Numeric dot-decimal notation
192.168.5.18

DHCP or manual configuration

IPv6

Deployed 1998

128-bit IP address

7.9×10^{28} addresses
Every device can have a unique address

Alphanumeric hexadecimal notation
5Ob2:64OO:OOOO:OOOO:6c3a:b17d:OOOO:1Oa9
(Simplified – 5Ob2:64OO::6c3a:b17d:O:1Oa9)

Supports autoconfiguration

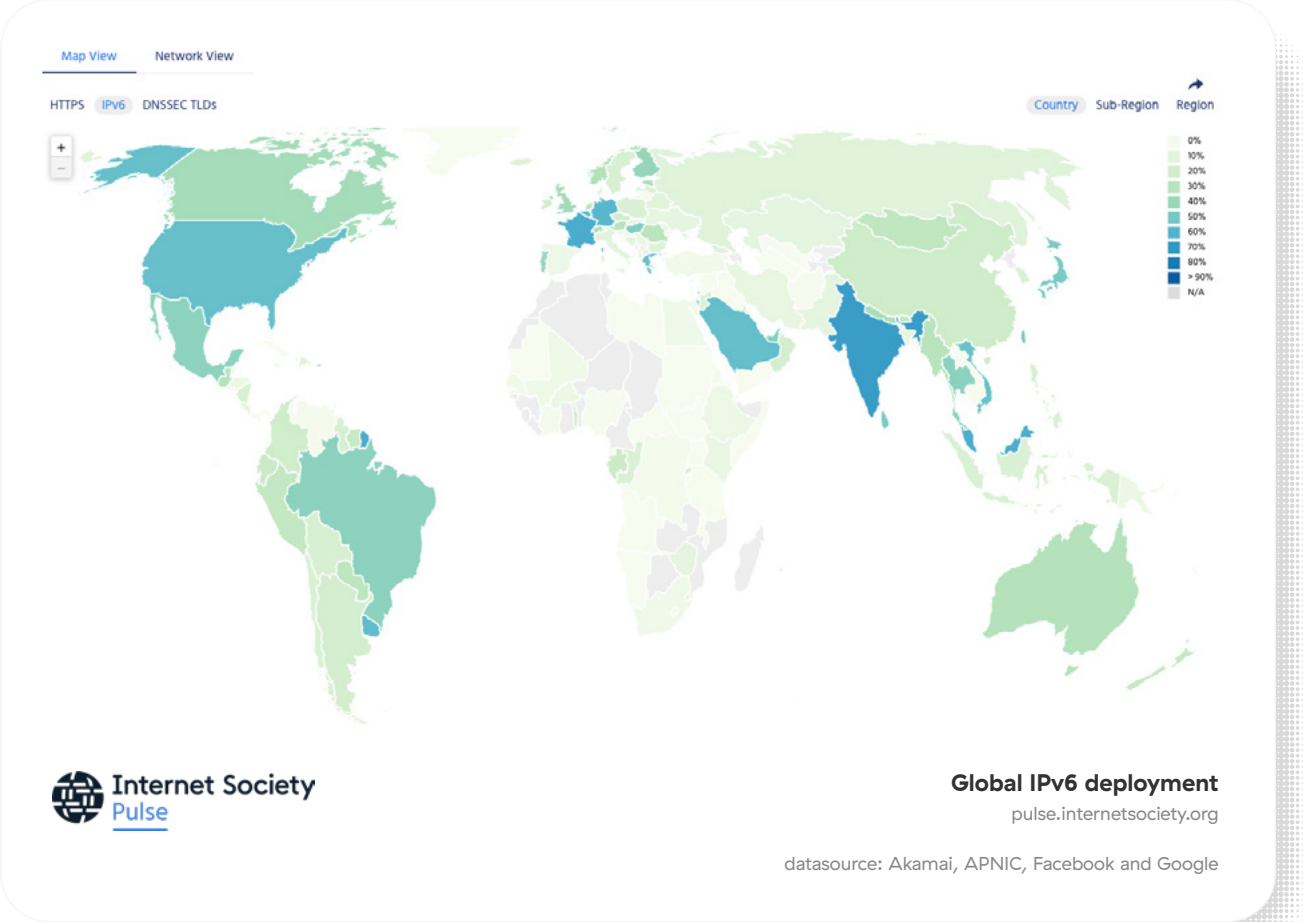
As IPv6 gradually replaces its predecessor, IPv4, enterprises and service providers are migrating their internal networks to IPv6 to overcome IPv4 exhaustion and other shortcomings of IPv4 such as performance, scalability, and security. Mobile internet access has accelerated the depletion of IPv4 address space, leading service providers to deploy IPv6-only addresses to mobile devices.

The adoption of IPv6 has been relatively slow, with ISPs, CDN, and carrier networks being the first to start deploying it in their networks. In recent years, the adoption of IPv6 slowed for organizations due to the pandemic, where people who worked from home returned to work on their IPv4-based corporate networks, and many organizations felt that there was no compelling business reason to adopt IPv6. However, government mandates across the globe have caused many enterprises and service providers that do business with government agencies to implement IPv6.

The transition to IPv6 is inevitable, and Zscaler supports our customers' transition plans through the Zero Trust Exchange.

The current state of IPv6

Internet Society Pulse curates information about levels of IPv6 adoption in countries and networks around the world. Currently, 45% of the top 1,000 websites globally support IPv6. India leads IPv6 deployment with 72% of connections from Indian end users to popular content sources using IPv6. The US is also worth highlighting as the 50% threshold was passed so that the majority of connections to IPv6–capable content sources will use IPv6.



Google also collects statistics about IPv6 adoption in the Internet on an ongoing basis and shows global IPv6 adoption has been steadily increasing and is currently approaching 40%, with variance day to day.

IPv6 Transition

There are several primary methods for transitioning a network from IPv4 to IPv6 including:

- Dual stack – Running both IPv4 and IPv6 on the same devices
- Tunneling – Transporting IPv6 traffic through an IPv4 network transparently
- Translation – Converting IPv4 traffic to IPv6 traffic for transport and vice versa

Currently, agencies and organizations run dual-stack systems to accommodate the use of both IPv6 alongside the much older IPv4 addresses that have long been exhausted but remain in wide use around the world.

Global adoption of IPv6 is quite uneven. In the US, the Office of Management and Budget (OMB) has set forth a transition schedule for federal agencies to develop a staged plan toward full IPv6 implementation by the end of 2025:

- At least 20% of IP-enabled assets on Federal networks are IPv6-only by the end of FY2023;
- At least 50% of IP-enabled assets on Federal networks are IPv6-only by the end of FY2024;
- At least 80% of IP-enabled assets on Federal networks are IPv6-only by the end of FY2025;
- Identify and justify Federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems

The US Department of Defense (DoD) issued Memorandum DTM-21-004 on June 29, 2021, establishing the policy that new networked DoD information systems will be IPv6-enabled before implementation and use by the end of FY 2023. A number of other US agencies have published IPv6 guidance including the National Security Agency (NSA) and National Institute of Standards and Technology (NIST).

The government of India has taken several policy initiatives so that the service providers, content providers, and the customer premises equipment vendors are encouraged to move to IPv6 address implementation. Based on the National Telecom Policy (NTP)-2012, Indian service providers are ahead of many other worldwide deployments of IPv6 at almost 80% of India's internet traffic transits via IPv6.

IPv6 deployment in the European Union is slowly increasing. The situation varies quite significantly among EU member states, with some better positioned than others including Netherlands, Germany, Greece, Belgium, and Czechia.

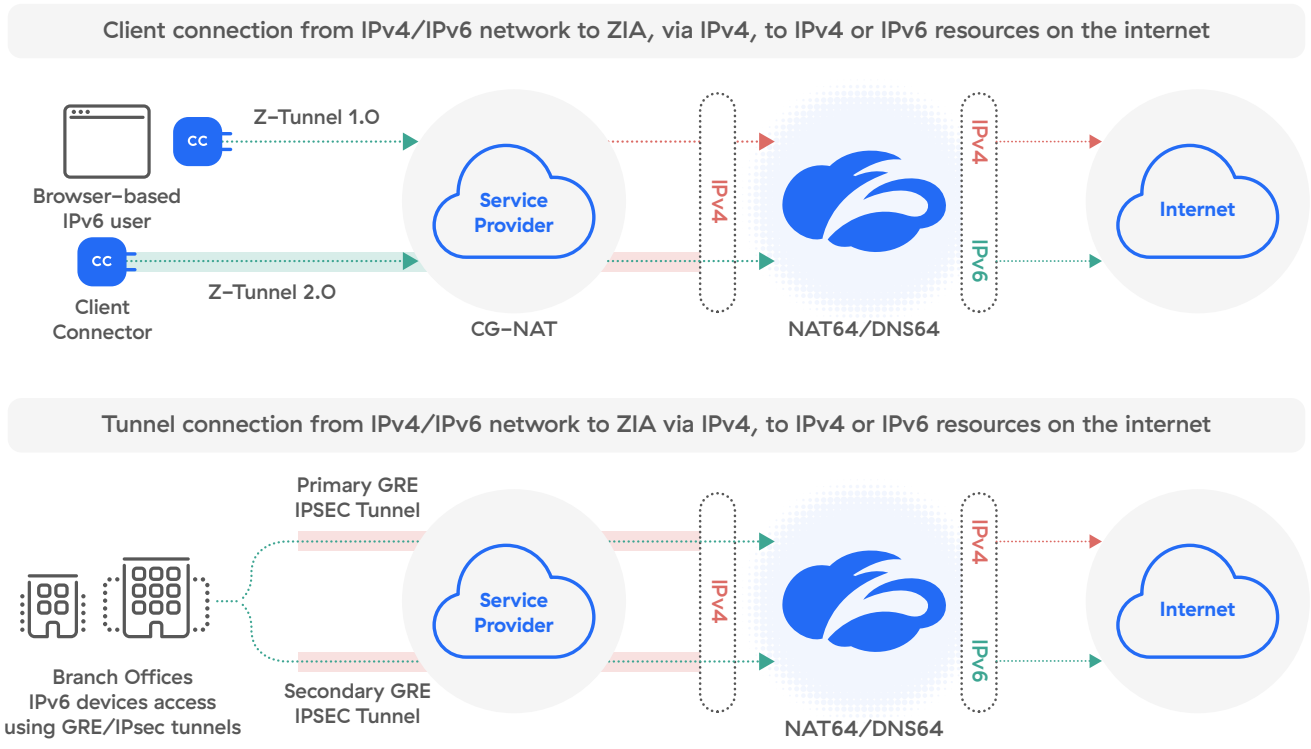
China's Central Cyberspace Affairs Commission and Cyberspace Administration have set out a plan for massive adoption of IPv6, with the goal of running a single-stack IPv6 network by 2030. By the end of 2023, new networks won't be allowed to use IPv4, and by 2025 the IPv6 user population in China will be 800 million, with 400 million IoT devices using the protocol and 70% of mobile traffic running over IPv6.

IPv6 support and the Zero Trust Exchange

At the same time that organizations are transitioning to IPv6, they are also modernizing their IT infrastructure to a Zero Trust Architecture (ZTA). IPv6 is a component of modernization that should be integrated with a zero trust implementation.

Zero trust connections are, by definition, independent of any network for control or trust. Zero trust ensures access is granted by never relying on a shared network between the originator (user/device, IoT/OT device, or workload) and the destination app. By keeping these separate, zero trust can be properly implemented and enforced over any network. The network can be located anywhere and be built on IPv4 or IPv6, since it is simply the means of connecting initiators to destination apps.

The Zero Trust Exchange is a highly available and globally distributed service, so that connections are requested and enforced at the most effective location to ensure the best user experience. The Zero Trust Exchange can also be run wherever is most suitable for the enterprise, meaning that it can be within a customer's premises, cloud, or edge platform. This brings the power of the Zero Trust Exchange as close to the consumer initiator as possible.



To address the network infrastructure's shift toward IPv6, the Zscaler Zero Trust Exchange brings in IPv6 support using tunneling and network address translation (NAT) technologies.

Currently, Zscaler extends IPv6 support for clients that are placed within organization locations. Both web and non-web traffic can be forwarded using these tunneling methods.

IPv6 support is extended by Zscaler based on the traffic forwarding method and also whether the client device is inside a location.

- For clients inside a location: Forward IPv6 traffic inside an IPv4 tunnel to ZIA Service Edges (Public, Private, or Virtual) using a GRE tunnel or IPSec tunnel.
- For clients outside a location: Forward web requests using PAC files or Zscaler Client Connector using Z-Tunnel 1.0 to ZIA Service Edges via a self-hosted or ISP-provided NAT64 gateway. To forward both web and non-web traffic from IPv6 clients, use Zscaler Client Connector over Z-Tunnel 2.0 and a self-hosted or ISP-provided NAT64 gateway.

ZPA

Zscaler Private Access (ZPA) supports IPv4 for TCP-, UDP-, and ICMP-based connections, and supports IPv6 for only TCP-based applications. App Connectors, ZPA Public Service Edges, and ZPA Private Service Edges are dual-stack aware, meaning IPv4 and IPv6 run simultaneously alongside each other. ZPA supports multiple IP use cases including:

- IPv4 Endpoint Accessing an IPv4 Application
- IPv4 or IPv6 Endpoint Accessing an IPv6 Application
- IPv6 Endpoint Accessing an IPv4 Application

ZIA

Zscaler supports full security inspection of IPv6 traffic for a variety of IPv4<->IPv6 or IPv6-only clients and applications. Applications like Tor that switch from IPv4 to IPv6 for evasion can be detected and blocked.

All Zscaler Internet Access (ZIA) services are supported with IPv6. This includes (but is not limited to):

- SSL inspection
- URL filtering
- Ccloud app control
- Firewall
- Bandwidth
- File type
- DNS and IPS control
- Advanced threat prevention
- Malware & sandbox
- Browser isolation
- Data loss prevention
- Logging and analytics

ZIA supports a dual-stack implementation of IPv4 and IPv6. Zscaler's cloud endpoints are still IPv4, though our data centers support IPv6 addressing for egress connectivity to internet or SaaS applications. IPv6 traffic from clients should be encapsulated in an IPv4 connection or tunnel to ZIA. IPv6 addresses in ZIA are used to connect to an IPv6 destination or application. DNS 64/NAT 64 address translation in ZIA is used to prefer IPv4 over IPv6 application addresses.

Client Connector

Zscaler highly recommends using Zscaler Client Connector (ZCC) as your preferred forwarding method for IPv6 traffic whenever feasible. ZCC on Windows and MacOS support dual stack IPv4 and IPv6 forwarding in the current version. Customers using Z-Tunnel 2.0 will be able to tunnel traffic from IPv6-only clients to a Zscaler data center, allowing end-to-end communication between IPv6 clients and IPv6 services. See Zscaler documentation and release notes for the latest support details for IPv6.

Next Steps

As each organization charts its path forward to zero trust and IPv6, Zscaler customers have a clear roadmap for success. IPv6 is an important step in the network and security transformation journey and moving to a zero trust architecture.

Zscaler has been steadily upgrading our Zero Trust Exchange to ensure you are ready to move to an IPv6-only future.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com