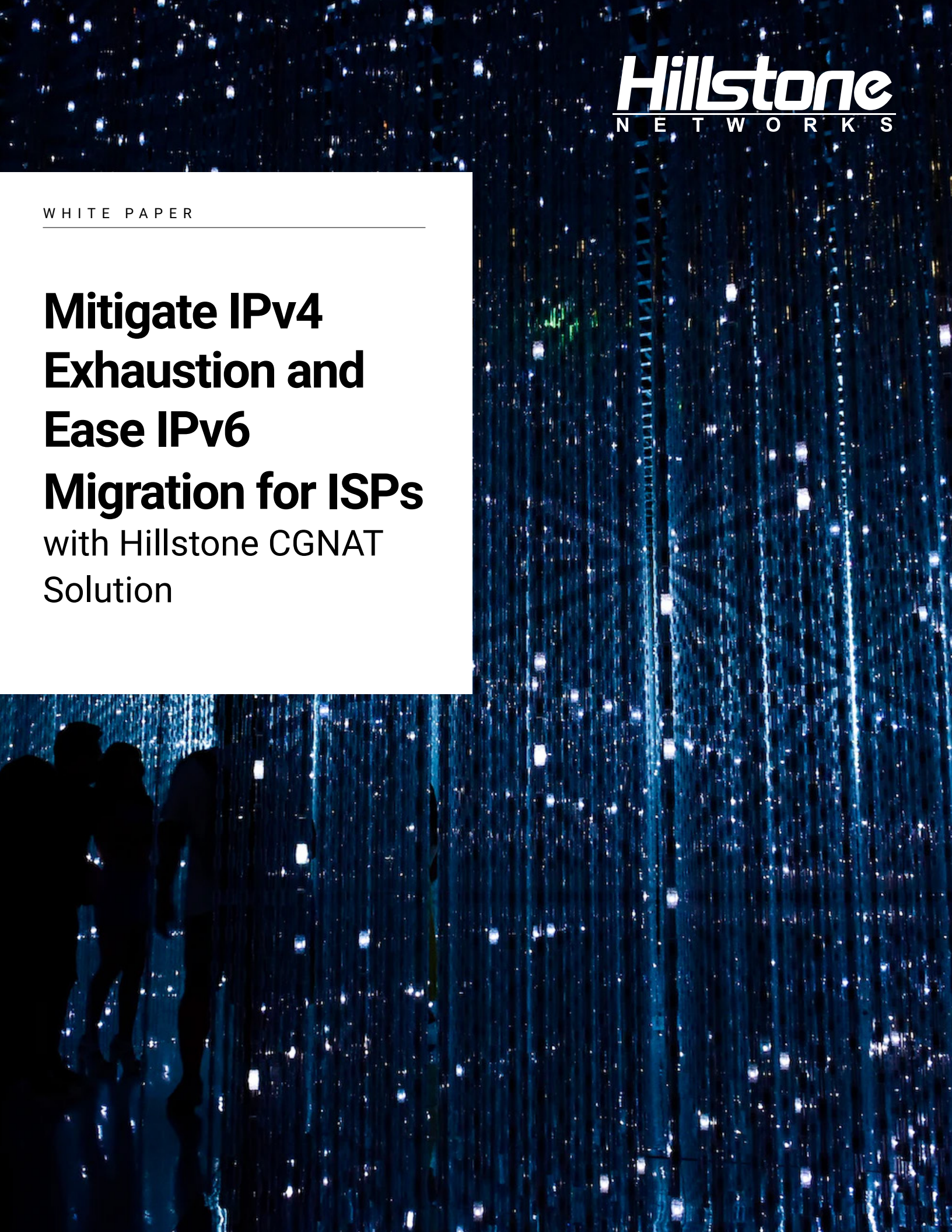


WHITE PAPER

# Mitigate IPv4 Exhaustion and Ease IPv6 Migration for ISPs

with Hillstone CGNAT Solution

## Introduction

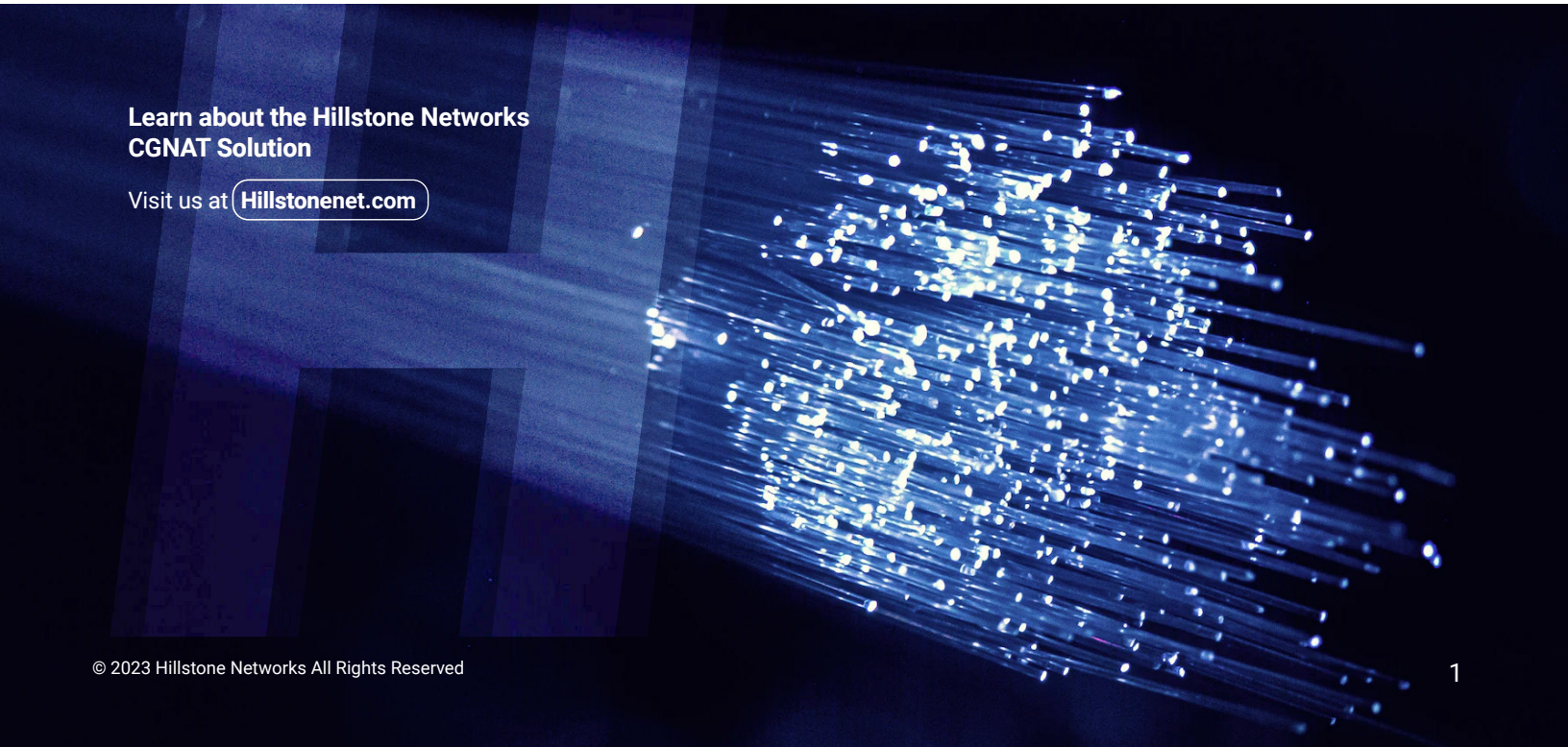
The official start of the Internet was in 1983 with the release of communication protocol called Transmission Control Protocol/ Internet Protocol (TCP/IP) and Internet Protocol version 4 (IPv4), which uses 32-bit address space to provide 4.29 billion unique addresses. With more people having home and work computers connected to the internet, Network Address Translation (NAT) was developed in 1994 as one of the key features in the Private Internet Exchange firewall to conserve IPv4 addresses.

Still facing IPv4 exhaustion despite the emergence of NAT, four years later, we saw the arrival of IPv6, which uses 128-bit addressing and can provide 340 undecillion IP addresses. IPv4 and IPv6 infrastructures will co-exist for years as IPv6 deployment has been ongoing but slow.

Today, with the revolution of the Internet of Things (IoT) and the deployment of 5G networks, internet service providers (ISPs) need to extend the life of IPv4 network infrastructures with scalable and transparent IP address translation.

### Contents






© 2023 Hillstone Networks All Rights Reserved

## What is Network Address Translation (NAT)?

Network Address Translation (NAT) was developed to conserve IPv4 addresses. However, one of the main reasons IPv6 deployment is slow is that NAT was able to preserve IPv4 addresses well by consolidating multiple private IP addresses into one public IP address. NAT also supports security and privacy concerns with a NAT router or firewall that acts as a gateway between the private and public networks. Only the public IP address is visible on the internet.

NAT has some disadvantages; it is small-scale; a single public IPv4 address is shared with multiple devices behind a router or firewall. NAT is commonly used for home or corporate networks, in which multiple devices in the network share a public IP address assigned by an ISP. NAT44 is the primary type of NAT, which translates and maps private IPv4 addresses to public IPv4 addresses.

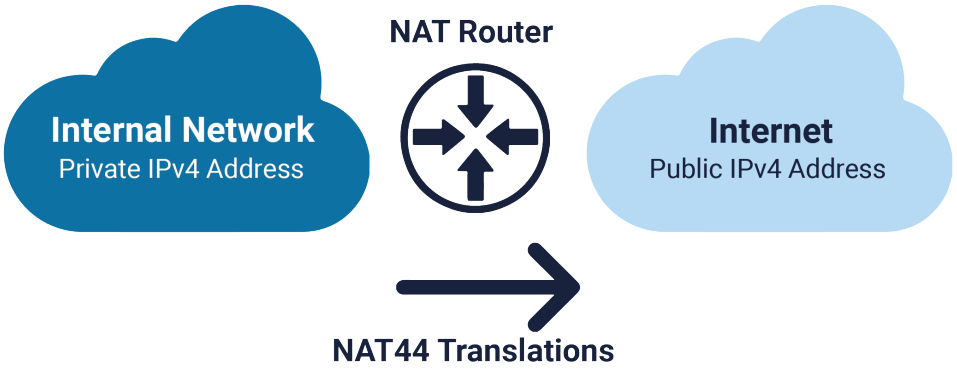



Figure 1: NAT44 Translation

NAT provides basic IPv4 connection, but does not support more advanced features that IPv6 supports such as large address space, built-in security, scalability, and quality of service (QoS) for bandwidth information and delays, which is required for network applications to run smoothly. NAT tampers with IP header fields which causes issues with File Transfer Protocol (FTP), IP Telephony (SIP), and Simple Network Management Protocol (SNMP) and is incompatible with some applications and network devices.

**NAT is a short-term solution to preserve exhausted IPv4 address space but does not support migration to IPv6. This is where Carrier-Grade NAT (CG-NAT) comes in to ease the migration to IPv6.**

© 2023 Hillstone Networks All Rights Reserved

## What is Carrier Grade NAT (CGNAT)?

Carrier grade NAT (CGNAT), also known as large-scale NAT (LSNAT), preserves IPv4 addresses by using private IPv4 address space in ISP networks with NAT444 translation. CGNAT is an extended version of NAT, in which devices' private IPv4 addresses get translated to ISP private IPv4 addresses first, and then to a public IPv4 address.

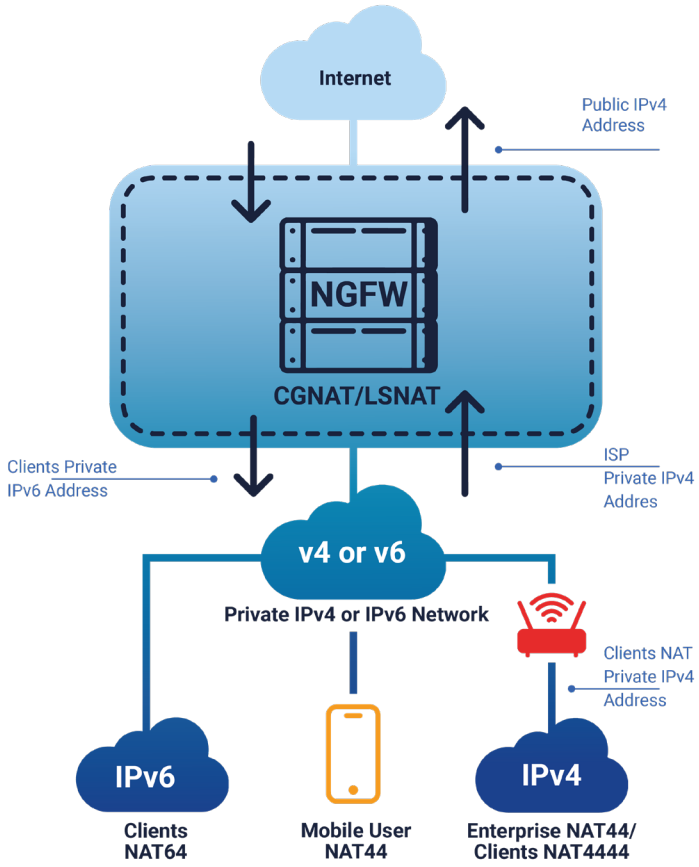



Figure 2: Service Provider NAT444 Translation

With service providers working on IPv6 deployment, CGNAT eases the migration to IPv6 with translation and mapping functions, such as:

- **NAT64** translates IPv6 address to IPv4 address to allow IPv6 devices to access the IPv4 network.
- **DNS64** allows DNS query from an IPv6 service to an IPv4 destination address.
- **NAT46** translates the IPv4 address to IPv6 address to enable IPv4 devices to access deployed IPv6 networks.
- **Full cone NAT** (also known as a one-to-one NAT) allows requests from the same internal IP address and port to map to the same external IP address and port. Any external host can send data and packets to the internal host through the mapped external address and port.

© 2023 Hillstone Networks All Rights Reserved

There is also Dual stack-lite which allows IPv4 users to continue to access IPv4 internet content with minimum disruption to the network while enabling IPv6 users to access IPv6 content.

NAT translates IP addresses on the network layer (layer 3) and port numbers on the transport layer (layer 4). NAT works well with most applications except for applications that include IP addresses or port numbers on the application layer (layer 7). These applications include DNS, VoIP, SIP, H.323, SIP, FTP, TFTP, RPC, RSH, and HTTP. The address information must be translated on the application layer to allow NAT to work with these applications. Application Layer Gateway (ALG) translates the IP address and port information in the payload of the application layer.

For peer-to-peer connections commonly used by gamers to establish direct connections with each other for fast real-time gameplay, gamers need the same constant external public IP address and port as an external source address to establish a stable connection. If the external source address differs from the initial authentication session, the server will reject the peer-to-peer session because the source address is now unauthorized. This is where Endpoint-Independent Mapping (EIM) comes in to ensure that any requests originating from a pair of private IP address and port will always be mapped to the same public NAT IP and port. If the destination address is different for each request, the source IP address/ port will always be mapped to the same NAT public IP and port.

## CGNAT Challenges

Because the same public IP address is shared with other subscribers, it is hard to identify which subscriber is accessing the internet and which subscriber needs support from ISP for internet connection problems. For regulatory compliance, it is required to know the subscriber's identity if they are doing illegal activities on the internet. There are also interferences in which the shared public IP address is blocked with denied access due to malicious activities from an individual user or infected device. Service access interference can also occur based on other subscribers' DNS queries.

Other challenges and misconceptions about CGNAT are complexity and cost.

CGNAT and NAT require CPU and memory resources for reading from and writing to the header and payload of every IP packet for address translation. High-performance and high-availability CGNAT solution is required. As all devices connected to the internet produce session logs, advanced logging techniques such as port batching logs and filtering can quickly help find logs necessary for compliance or provide insights into subscribers' internet usage activities.

Distributed Denial of Service (DDoS) attacks are usually targeted at CGNAT pools of IP addresses as the same public IP address shared among many subscribers is more likely to be used multiple times. ISPs need to set up a user quota to limit the amount of TCP and UDP ports used by a single subscriber to maintain fair resource sharing. All of these would add complexity to CGNAT.

Another concern is the additional costs required to include a Carrier-grade network controller to implement the CGNAT functions for network address translation.

© 2023 Hillstone Networks All Rights Reserved

## Hillstone's CGNAT Solution

Hillstone A-Series enterprise and X-Series data center next-generation firewalls (NGFW) running on the foundational operating system, Hillstone StoneOS, have long provided network security for many ISPs and enterprise networks. Hillstone NGFWs support IPv6 and IPv4 network infrastructures and have NAT and CGNAT capabilities that can be easily configured with StoneOS user interfaces. Hillstone NGFWs are scalable in performance from 20Gbps to 1.2 terabits throughput, 300 thousand to 7 million new sessions per second, and 8 million to 400 million concurrent sessions. With CGNAT, the throughput ranges are from 10Gbps to 600Gbps.

Hillstone Security Audit Platform (HSA) collects NAT, threat, URL, and session logs and has powerful and fast query capabilities for quick search based on source IP, destination IP, URL, public IP, and time of use. The created NAT logs can translate a public IP address into a private IP address, port, and username. This allows quick identification of the subscriber as required for regulatory compliance.

**Hillstone Entrerprise & Data Center NGFWs**

A-Series and X-Series

**Hillstone Security Audit Platform (HSA)**

High-performance NAT, Threat, URL, and Session log storage & query

Figure 3: Hillstone CGNAT Solution based on Hillstone NGFWs and Security Audit Platform (HSA)

© 2023 Hillstone Networks All Rights Reserved

## Advantages of Hillstone's CGNAT Solution

### Advanced CGNAT Configurations to Ease IPv6 Migration

CGNAT and NAT are configurable functions included in Hillstone's high-performance next-generation firewalls (NGFW). NAT functions are created and implemented based on NAT rules. There are two types of NAT rules:

1. **Source NAT (SNAT) rule,**
2. **Destination NAT (DNAT) rule.**

SNAT translates the internal host source IP address from a private to a public IP address. DNAT is used by an external host to initiate the connection to a private network by translating the public IP address of an external host to the private IP address of an internal host. Full-cone NAT, also known as one-to-one NAT, will map all the requests from one IP/ port in the private network to one IP/port in the public network. All the hosts in the public network can communicate with the host that initiated the request by using the mapping relationship. There is also built-in automatic NAT rule redundancy detection which enables more efficient discovery and deletion of redundant NAT rules. This feature enhances the performance and efficiency of NGFWs for NAT and CGNAT functions by eliminating redundant NAT rules that will utilize CPU and memory resources.

Hillstone NGFWs are IPv6-ready and support IPv4 and Pv6 dual stack, making migration to IPv6 easier. Hillstone NGFWs also have translation functions, such as NAT64/ DNS64, Dual-stack lite, and NAT46.

### Application Integrity

Hillstone NGFWs have built-in Intelligent Application Identification and Application Control, in which over 4000 applications can be filtered by name, category, subcategory, technology, and risk. Each application contains a description, risk factors, dependencies, typical user ports, and URLs for additional reference. Hillstone NGFWs provide comprehensive 2-level 8-layer QoS pipes to ensure fast network performance for critical applications with optimized bandwidth and traffic for these critical applications when the network is overloaded or congested.

### Efficient Logging for Regulatory Compliance

One of the challenges with CGNAT is that the same public IP address is shared with other subscribers, making it hard to identify which subscriber is accessing the internet.

Hillstone Network Security Audit Platform (HSA) has high-performance log storage and instantaneous query capability. HSA collects NAT, threat, URL, and session logs. It can receive up to 270,000 events per second from NAT traffic and store these event logs for up to 180 days. HSA also includes powerful queries simplified by port batching that allow easy search across source IP, destination IP, URL, public IP, and time of use. Hillstone's NAT logs can translate a public IP address into a private IP address/ port and user name. These NAT logs can quickly help internet service providers identify which subscribers accessed the internet and meet regulatory compliance.

© 2023 Hillstone Networks All Rights Reserved

## Carrier Grade Security

Since CGNAT and NAT are functions and features available in Hillstone NGFWs, the Hillstone CGNAT solution is more advanced with the built-in full security features of NGFWs such as Intrusion Protection System, Anti-DDoS, Antivirus, URL filtering, Botnet Command and Control Prevention, Application Control, and IP reputation.

To prevent DDoS attacks, session limits can easily be configured for Hillstone NGFWs using StoneOS interfaces. The number of sessions and the session rate can be limited based on source IP address, destination IP address, specified IP address, applications, role, user, and user group. This can prevent DDoS attacks and also control bandwidth for applications.

Traffic quota can also be set to limit and control the allowable traffic flow of users or user groups per day or month. Share access control can block access from unknown devices and allocate user bandwidth. There are a series of ARP defense functions to protect networks against Address Resolution Protocol attacks, such as ARP poisoning. With ARP defense features like ARP learning, MAC learning, ARP binding, and DHCP snooping, ARP packets are dropped if the bindings do not match the IP address, MAC address, port, and MAC address of DHCP.

## Advanced AI/ML-Based Threat Detection and Protection

As cyberattacks are increasingly more sophisticated, threat detection and protection must also be more advanced. AI (Artificial Intelligence) / ML (Machine Learning) based threat detection and protection can detect attacks more accurately based on modeling that predicts attacks and automate responses to these attacks. Hillstone released the industry's first AI-based firewall in 2013 and continuously improved the AI and ML technologies used in Hillstone NGFWs.

The advanced AI and ML technologies in Hillstone NGFWs are:

- **Real-time threat detection** in encrypted traffic without decryption based on ML-based detection model. The ML-based detection model is from sampling encrypted traffic to continuously optimize and improve detection accuracy and efficiency. This can help detect and protect from zero-day attacks, which can be undetected in encrypted traffic.
- **ML-based intelligent DDoS protection** based on baseline establishment of DDoS flood attack protection threshold.
- **Perimeter traffic filtering** (PTF) to perform fast blocking of threats at the edge based on blacklist library.

## Unified Platform Reduce Total Cost

CGNAT and NAT are functions and features available in Hillstone NGFWs; customers using Hillstone NGFWs in their existing network infrastructures can easily configure CGNAT/ NAT functions while still using Hillstone NGFWs for complete Layer 2 to Layer 7 protection. Hillstone CGNAT solution is a unified, easy-to-manage platform based on Hillstone NGFWs and its operating system, StoneOS.

© 2023 Hillstone Networks All Rights Reserved

## Hillstone CGNAT Solution Deployed in ISP's Infrastructure

By looking at how easily NAT and CGNAT functions in Hillstone NGFWs can be configured, it is easy to see why many ISPs use Hillstone NGFWs for CGNAT along with its added carrier-grade security features, such as threat detection and prevention, traffic analysis, policy management, and access control.

Today, Hillstone A-series and X-series NGFWs with CGNAT capabilities are deployed in many large ISP and wireless carriers' infrastructures worldwide. The requirements from all these ISPs and carriers are generally the same:

- **ISPs and carriers support IPv4 and IPv6 network infrastructure and 5G deployment.**
- **ISPs' and carriers' subscriber bases are growing, and the number of internet-connected devices per subscriber is also increasing, which further aggravates the on-going depletion of IPv4 addresses.**
- **ISPs and carriers need high-performance, scalable solutions that can support the increase in subscribers, traffic loads, and bandwidth.**
- **They look for CGNAT solutions that can optimize the use of IPv4 addresses with controlled port mapping, data storage for monitoring and statistics, and modular and scalable design to facilitate large amounts of traffic.**

With Hillstone's CGNAT solutions, ISPs and carriers can scale up based on performance requirements and expand in the future to handle increasing traffic loads. The solution provides complete log visibility and monitoring capabilities with Hillstone Security Audit (HSA) platform to meet regulatory compliance. Based on its next-generation firewalls, the Hillstone CGNAT solutions offer a robust suite of carrier-grade network defenses, including attack defense with flood attack protection, granular application control, advanced intrusion protection, botnet protection, URL filtering, antivirus, and more.

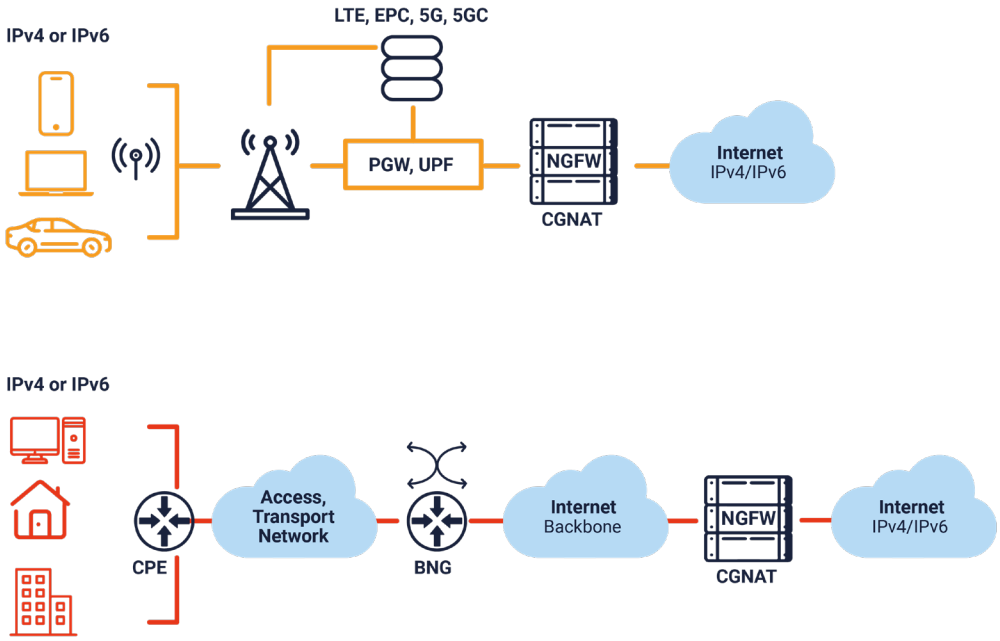



Figure 4: CGNAT deployment with Service Provide

© 2023 Hillstone Networks All Rights Reserved

## Summary

Carrier Grade NAT (CGNAT) allows service providers to leverage existing IPv4 infrastructure by mitigating IPv4 address exhaustion while providing an easy migration path to IPv6 infrastructure that is seamless to subscribers and users. CGNAT support large-scale, carrier deployment by extending IPv4 address translations while supporting translation from IPv4 address to IPv6 address and from IPv6 to IPv4.

As service providers and enterprises already use firewalls as the first line of defense in network security to monitor and block incoming and outgoing network traffic for and from threats, the deployment of Hillstone CGNAT solution is simple as it is just configurations of Hillstone next-generation firewalls (NGFWs) for CGNAT and NAT functions using Hillstone StoneOS, the operating system for Hillstone NGFWs.

## About Hillstone Networks

Hillstone Networks' innovative and accessible cybersecurity solutions reshape enterprise security, enabling cyber resilience. By providing enterprises with the visibility and intelligence to comprehensively see, thoroughly understand, and rapidly act against multilayer, multistage cyber threats, Hillstone's products are favorably rated by leading analysts and trusted by over 23,000 global companies. With a reputation for "security that works," Hillstone's product suite covers enterprise edge to cloud and includes NGFW, SD-WAN, ZTNA, NDR, XDR, and CWPP. Hillstone's cutting-edge solutions leverage AI/ML and integrate seamlessly into SecOps frameworks, providing CISOs the assurance that their enterprises are well-protected while enabling a lower total cost of ownership (TCO).

**Learn about the Hillstone Networks CGNAT Solution**. Visit us at **Hillstonenet.com**

© 2023 Hillstone Networks All Rights Reserved

Hillstone
NETWORKS

Visit **www.hillstonenet.com** to learn more
or contact Hillstone at **inquiry@hillstonenet.com**