CGNAT is a critical network function which allows you to preserve IPv4 investments and manage the migration to IPv6. Reduce OpEx and CapEx by deploying as a virtual network function on Commercial-off-the-shelf (COTS) hardware or consolidate with other network services on a carrier-grade appliance.

Protect your investment in IPv4 infrastructure with carrier-grade network address translation (CGNAT). NetScaler delivers a high-performance, application-transparent CGNAT service, enabling telecommunications service-providers to extend the life of their IPv4 networks, manage the migration to IPv6 and scale S/Gi-LANs to support rapidly growing subscriber traffic.

Even in environments where change is constant, some things remain the same. Such is the case with IPv4, which is not going away any time soon despite full allocation of its global address space. Network address translation is a proven technology for remapping one IP address space into another. While NAT technology itself is nothing new, carriers continue to face two challenges when implementing CGNAT: cost and capabilities. Some CGNAT solutions require a dedicated system, which increases both CapEx and OpEx owing to the need to deploy and maintain separate hardware. A better approach is to implement CGNAT in software which can be integrated with other network services in a high powered application delivery controller (ADC) or can be deployed as dedicated standalone virtual network function on COTS hardware.

The capabilities challenge involves the need to implement the different forms and related functions of NAT that might be needed to support different protocols and applications with total transparency. For example. UDP, TCP and ICMP each require a specific form of NAT to operate transparently end-to-end. Certain tunneling and signaling protocols, especially those that include IP addresses and/or TCP/UDP ports in packet payloads, require an application-level gateway (ALG) capability. An ALG functions like a proxy that makes the translations necessary for applications to operate seamlessly across public and private address realms, but unlike a proxy, does not require any changes to clients or servers.

Citrix meets both of these challenges with a software-based high-performance CGNAT solution which can be deployed as standalone software or integrated as a network service in the industry-leading, high-performance NetScaler appliance. This enables carriers to consolidate equipment and eliminate the need for yet another single-purpose system while securing a path to a fully virtualized network. The cost-effectiveness of consolidation and the cost benefits of using COTS hardware are both critically important as S/Gi-LAN traffic grows at a rate of 50 percent to 100 percent annually.

While performance can be an issue with some ADCs that support CGNAT, rigorous testing has demonstrated the ability of NetScaler to support up to 256 million sessions in a 2 RU platform. Test results also demonstrate its ability to handle over a million connections/second with a Layer 7 throughput of up to 160 Gbps. Alternately, one single virtual instance of the product can now achieve up to 100Gps of throughput.

The NetScaler CGNAT solution also includes broad support for the ALGs carriers need today, and its extensible design enables other ALGs to
be added to satisfy changing market conditions. The breadth and depth of these ALGs enable carriers to satisfy the connectivity requirements of businesses and individual subscribers with a high-quality experience, and without restrictions.

Key features

**NAT44**
NetScaler CGNAT offers standards-based private IPv4 to public IPv4 network address translation (NAT44) based on the latest RFCs, making it interoperable and transparent in both client-server and peer-to-peer (P2P) applications. CGNAT uses a pool of public IPv4 addresses to assign a global IPv4 address to each subscriber, and then maps each subscriber’s private IPv4 addresses to and from its global address automatically and transparently as needed to traverse the Internet or other public IP network.

**NAT64**
NAT64 allows IPv6 hosts to communicate with IPv4 servers. The NAT64 solution in NetScaler is a full implementation of this capability. It includes a translator which performs protocol translation, while maintaining session information on NetScaler. When NetScaler receives an IPv4 response packet belonging to a particular NAT64 session, it uses the information stored in the NAT64 session to translate the IPv4 packet into an IPv6 packet, and then sends the IPv6 response to the client.

**464XLAT**
Not every application or service works as an IPv6 host and there are still many IPv4-only applications/services. 464XLAT support in NetScaler enables IPv4-only clients to communicate with IPv4 nodes in the internet via an IPv6 infrastructure.

**Controlled openness to inbound connections**
NetScaler can permit any external host to connect to any internal host (“behind” the CGNAT service) with an open or mapped internal address, a behavior known as endpoint independent filtering (EIF). The Internet Engineering Task Force recommends EIF as the default filtering behavior for CGNAT.

**Mapped address persistence**
NetScaler can use the same external, public IP address for all sessions from the same internal hosts, a behavior known as endpoint independent mapping (EIM). EIM offers transparency for P2P and VoIP applications by providing a persistent external IP address and port for all connections originating from the same internal host/port, thereby minimizing the potential for connectivity problems.

**Support for full cone NAT**
NetScaler provides support for full cone NAT when both EIF and EIM are enabled. Also known as static, one-to-one and port forwarding NAT, full cone is the least restrictive form of NAT, making it a good choice for applications that do not require stringent security provisions.

**ALGs**
NetScaler offers broad support for ALGs to ensure transparency for a full range of enterprise and consumer applications. ALG support is provided for ICMP, FTP, TFTP, SIP, PPTP and RTSP.

**Hairpinning**
NetScaler supports hairpinning, which enables endpoints with private IP addresses to communicate with one another without the need to translate these addresses to and from public IP addresses when both endpoints are behind the same CGNAT service. This makes it possible, for example, for subscriber clients to reach a carrier’s servers, or for one subscriber VoIP device to call another subscriber VoIP device directly without address translation.

**Connection limiting**
To ensure consistent performance across all subscribers and to help protect against DDoS attacks, NetScaler can restrict the number of sessions available for each commercial and consumer subscriber.

**High-speed logging**
NetScaler can continuously log all NAT transactions to SYSLOG servers, which is required to comply with certain government regulations, which for example, mandate metadata retention periods. The CGNAT syslog messages can be sent via high-speed links using TCP to ensure that NetScaler performs accurate logging at the full rate of incoming connections. Furthermore, NetScaler can load-balance SYSLOG servers for high availability and performance.

**Compact logging**
Regulations can mean that very large quantities of data must be collected and stored. Compact format is a NetScaler feature which reduces the size and amount of logs by employing short operational codes for events and protocol names. This also reduces the logging infrastructure required.

**Deterministic NAT**
Deterministic NAT enables carriers to allocate a fixed block of ports and IP addresses that may be used dynamically to subscribers, which eliminates the need for extensive logging. In typical NAT environments, the requirement for logging is critical, and for carriers with CGNAT, the log files can become quite large, making log management a continuous and costly challenge.

**Dual Stack Lite**
Dual Stack Lite (DS Lite) is an IPv6 transition solution for ISPs and telco’s with IPv6 infrastructure to connect their IPv4 subscribers to the Internet. DS Lite uses IPv6 tunneling to send a subscriber’s IPv4 packet over a tunnel on the ISP’s or telco’s IPv6 network. The IPv6 packet is de-capsulated to recover the subscriber’s IPv4 packet and is then sent to the Internet after NAT address and port translation and other CGNAT-related processing. The response packets traverse through the same path to the subscriber.

**Port Control Protocol (PCP)**
In today’s networks, the NAT service plays an important role in providing IPv4 preservation, IPv6 migration and security. There is a high likelihood that NAT will be performed during any end to end communication. Port Control Protocol (PCP) was developed (RFC 6887) to allow explicit control of the NAT function. PCP enables applications and equipment to read/write explicit mappings between an external IP address, protocol and port, and an internal IP address, protocol and port. These explicit mappings allow inbound communication to reach the hosts behind a NAT or firewall. The NetScaler PCP solution works in conjunction with NAT44, NAT64 and Dual Stack Lite.

**Integration with NFV and SDN**
The CGNAT service can run as a virtual network function in the NFV framework and integrate with any NFV Management & Orchestration (MANO) stack. Full integration is carried out via the NetScaler Management and Analytics System, NetScaler MAS.
<table>
<thead>
<tr>
<th>Capabilities Summary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance (NetScaler T1300)</td>
<td>• Up to 256 million concurrent sessions</td>
</tr>
<tr>
<td></td>
<td>• Up to 1.2 million connections/second</td>
</tr>
<tr>
<td></td>
<td>• Up to 1 million static CGNAT mapping entries</td>
</tr>
<tr>
<td>NAT functionality</td>
<td>• N:M NAPT</td>
</tr>
<tr>
<td></td>
<td>• Address restricted</td>
</tr>
<tr>
<td></td>
<td>• Port restricted</td>
</tr>
<tr>
<td></td>
<td>• Symmetric</td>
</tr>
<tr>
<td></td>
<td>• Static mapping</td>
</tr>
<tr>
<td></td>
<td>• Sticky NAT</td>
</tr>
<tr>
<td></td>
<td>• Deterministic NAT</td>
</tr>
<tr>
<td></td>
<td>• Session timeout</td>
</tr>
<tr>
<td>Transparency</td>
<td>• Full cone / Paired IP pooling</td>
</tr>
<tr>
<td></td>
<td>• Hairpinning</td>
</tr>
<tr>
<td></td>
<td>• Mapping and filtering:</td>
</tr>
<tr>
<td></td>
<td>• End-point Independent</td>
</tr>
<tr>
<td></td>
<td>• Address dependent</td>
</tr>
<tr>
<td></td>
<td>• Address and port dependent</td>
</tr>
<tr>
<td>ALGs</td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• TFTP</td>
</tr>
<tr>
<td></td>
<td>• ICMP</td>
</tr>
<tr>
<td></td>
<td>• SIP</td>
</tr>
<tr>
<td></td>
<td>• RTSP</td>
</tr>
<tr>
<td></td>
<td>• PPT</td>
</tr>
<tr>
<td>RFC compliance</td>
<td>• 4787 (UDP)</td>
</tr>
<tr>
<td></td>
<td>• 5382 (TCP)</td>
</tr>
<tr>
<td></td>
<td>• 5508 (ICMP)</td>
</tr>
<tr>
<td></td>
<td>• 6888 (CGNAT)</td>
</tr>
<tr>
<td></td>
<td>• 6146 (NAT64)</td>
</tr>
<tr>
<td></td>
<td>• 6147(DNS64)</td>
</tr>
<tr>
<td></td>
<td>• 6887(PCP)</td>
</tr>
<tr>
<td>High-speed logging</td>
<td>• SYSLOG over TCP</td>
</tr>
<tr>
<td></td>
<td>• Load balancing of SYSLOG servers</td>
</tr>
<tr>
<td></td>
<td>• Compact logging</td>
</tr>
<tr>
<td>IPv6 transitioning</td>
<td>• NAT64</td>
</tr>
<tr>
<td></td>
<td>• Dual Stack Lite</td>
</tr>
<tr>
<td>Port Control Protocol (PCP)</td>
<td>• NAT44</td>
</tr>
<tr>
<td></td>
<td>• NAT64</td>
</tr>
<tr>
<td></td>
<td>• Dual Stack Lite</td>
</tr>
</tbody>
</table>