IPv6: Not a Solution for Security!!!

Ray Vinson, 2012-02-03

On April 15th, 2011, the last of the IPv4 address blocks was allocated,. Due to IPv4 address depletion, migration to IPv6 is inevitable. This migration to IPv6 will ease IPv4 address depletion but it does not address other significant networking issues such as security. Networks that have already migrated to IPv6 are starting to experience the first Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks can lead to significant amounts of downtime and, especially for Communication Service Providers, loss of revenues and increases in subscriber churn. For CSP's to stay competitive and maintain an acceptable Quality of Experience (QoE), security and mitigation of DoS/DDoS attacks must be included in the migration to IPv6.

Throughout the development of IPv6 technology, security was an integrated part of the standards. In the original version of the RFC, IPsec was integrated into the IPv6 header. IPsec provided basic security in the IP stack. However, in December 2011 IPsec as a requirement was changed to an optional element in the RFC. This means that all IPv6 networks will have to be able to interoperate with traffic that includes both IPsec and non-IPsec. And even though there is the argument that by having non-IPsec integration and IPv6 opens the door for more DoS/DDOS attacks, IPsec is not the ultimate solution to DoS/DDOS attacks.

Migration technologies have been created to make interoperability of IPv4 and IPv6 networks. For CSPs, this technology is crucial when their subscribers are on an IPv6 network and the content that the subscribers demand is on the IPv4 Internet. Carrier grade network address translation (CGNAT) is designed to managed address translations and assignments for IPv4 and IPv6 networks. This technology integrated with Domain Name System 64 (DNS64) ensures that addresses and domains are locatable and accessible from either an IPv4 or IPv6 network. Tunneling technologies, such as Dual Stack Lite and 6RD, transport traffic through encrypted tunnels which allows IPv4 or IPv6 traffic to be delivered across either network. All of these methods provide different tools for the CSP to migrate all or part of their network to IPv6 and still is able to interoperate with the IPv4 Internet. However, none of these methods address the security threats that exist on the Internet.

DoS/DDoS attacks can never be completely prevented. The only strategy that truly works is using security tools, like IPsec, along with distributed architectures to mitigate the impact of these attacks. While CSP's are migrating to new technologies and upgrading to IPv6, new security architecture should be examined. Since almost every part of the network has to be touched, , this is the perfect opportunity for CSP's to update their security architecture along with becoming IPv6 compliant.

No matter which technology scheme for migration to IPv6 is used, all elements of the network can be designed to help mitigate the impacts and costs of Dos/DDoS attacks. Whether it is CGNAT, DNS 64, IPv6 Gateway, or tunneling methodologies, all of the different IPv6 migration technologies can be deployed to maintain service up time during a DoS/DDoS attack. The ultimate goal of mitigating a DoS/DDoS attack is to maintain services for subscribers and minimize degradation of the QoE for subscribers. The challenge of achieving this goal is deploying a network to provide this level of service during an attack without creating a CapEx nightmare. The first step in being successful is creating a network that will maintain service during a DoS/DDoS attack and minimize the expenditures associated is to create an intelligent IPv6 infrastructure that can scale, perform and distribute traffic in an intelligent manner to mitigate the impacts of an attack. Deploying IPv6 is not a solution to attacks from the Internet, however the network architecture can be built to mitigate the impacts of these attacks and this architecture can be deployed as part of the migration to IPv6.

Related Articles

- ZDNet: "First IPv6 Distributed Denial of Service Internet Attacks Seen"
- RFC 6434
- Pete Silva - ipv6

- Ray Vinson - IPv6
- Lori MacVittie - DDoS
- F5 Friday: 'IPv4 and IPv6 Can Coexist' or 'How to eat your cake and ...
- Josh Michaels - DDoS
- Mitigating Slow HTTP Post DDoS Attacks With iRules > DevCentral ...
- IPv6 - DevCentral - DevCentral Groups - Social Forums ...
- IP::addr and IPv6
- Audio White Paper - Controlling Migration to IPv6: A Gateway to ...
- IPv6: Yeah, we got that

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com