Ausarbeiten und Implementieren von IPv6 im Dual-Stack-Betrieb

Studiengang: MAS Information Technology
Betreuer: Piotr Kusak
Experte: Prof. Hansjürg Wenger
Industriepartner: V-Zug AG, Zug

Die Master-Thesis soll in Form eines Proof-of-Concepts Aufschluss geben, wie Systeme bei der V-Zug AG mit IPv4 und IPv6 im Dual-Stack-Betrieb ans Netzwerk angebunden werden können. Nebst einem Adresskonzept wird das IPv6-Protokoll analysiert und vertieft, auf Schwachstellen geprüft und mögliche Gegenmassnahmen dazu empfohlen.

Umfeld / Problemstellung

Die V-Zug AG betreibt aktuell ein reines IPv4-Netzwerk. Wichtige Basis-Dienste wie DNS, DHCP, NTP, Proxy, FTP etc. sind daher ausschliesslich für die Übertragung über IPv4 konfiguriert. IPv6 ist auf den meisten Systemen (PC's, Servers, Firewalls, Routers, etc.) schon seit längerer Zeit verfügbar, jedoch noch nicht implementiert und eingerichtet.

Das IPv4-Problem

Durch die enorme Zunahme an Netzwerkteilnehmern (TV's, Smartphones, Autos, PC's, Servers, Cloud-Dienste…) schwinden die verfügbaren IPv4-Adressen rasant. IPv4 bietet einen gesamten Adressraum von rund 4.2 Milliarden Adressen (2^{32}), wovon rund 3.7 Milliarden verwendet werden können. Die für Nordamerika zuständige Regional Internet Registry ARIN (American Registry for Internet Numbers) hat mit Stand 07. September 2015 im letzten verfügbaren /8-Adressblock nur noch rund 21'810 IPv4-Adressen frei (s. https://www.arin.net/resources/request/ipv4_countdown_plan.html). Nebenbei: Eine IPv6-Adresse wird über 128 Bits definiert. Insgesamt sind damit rund 2^{128} (ca. 340 Sextillionen) eindeutige Adressen möglich.

Ziel

Ein Proof-of-Concept (PoC) soll mit ausgewählten Diensten in einer Testumgebung bestätigen, dass IPv6 im Dual-Stack-Betrieb funktioniert und bei der V-Zug AG Schritt für Schritt eingeführt werden kann. In Form des sogenannten «Dual-Stacks» können beide Protokolle parallel zueinander, jedoch unabhängig voneinander, funktionieren und interagieren. Ebenso soll das IPv6-Protokoll analysiert (ICMPv6, NDP, MLD, Happy Eyeballs, DAD etc.) und auf Schwachstellen geprüft werden. Das Adresskonzept wird aufzeigen, wie die bestehenden Netzwerkzonen mit IPv4 und IPv6 betrieben werden können und welche Adressen (GUA, ULA) verwendet werden sollen. Zudem wird erläutert, wie die IPv6-Adressen verteilt werden (static vs. DHCPv6 vs. SLAAC) können. Basierend auf den Erkenntnissen, die während der ganzen Arbeit gewonnen wurden, werden Empfehlungen abgegeben, wie IPv6 im Dual-Stack bei der V-Zug AG eingeführt werden kann.

Lösung / Erkenntnisse

Die Protokollanalyse hat gezeigt, dass IPv6 ähnliche Schwachstellen wie IPv4 aufweist. Ich habe festgestellt, dass vielerlei Systeme (Firewalls, Switches, Routers) noch nicht für die immense Menge an verfügbaren IPv6-Adressen ausgelegt sind, was wiederum Möglichkeiten für Attacken bietet. So kann bspw. ein IPv6-Neighbor-Cache eines Routers nur ein paar hundert bis tausend Einträge aufnehmen. Mit geeigneten Tools kann dieser Cache ausgeschöpft werden, was wiederum neue Einträge verhindert und somit zu einem Denial-of-Service (DoS) führt.
Es hat sich gezeigt, dass nicht überall, wo IPv6 drauf steht, auch IPv6 drin ist. Der zum Zeitpunkt der Master-Thesis aktuelle Checkpoint-Release (R77.20) loggt bspw. ICMPv6-Errors (Packet too big) nicht. Die Funktionalität als DHCPv6-Relay ist auch nicht gegeben. NDP-Mechanismen wie bspw. Neighbor-Solicitation und Neighbor-Advertisements sind hingegegen fest im Code verankert und können nur durch sehr umständliches Editieren von Konfigurationsfiles angepasst werden. Ebenso kann die Link-Local-Adresse nicht über ClusterXL hochverfügbar gehalten werden.
Ich empfehle zudem, mindestens auf den Etagen-Switches das DHCPv6-Snooping- und das RA-Guard-Feature zu aktivieren. Ebenso sollte der spezifizierte Subnet-Präfix von /64 beibehalten und nicht angepasst werden.
Der PoC war erfolgreich, so dass einer schrittweisen Einführung – beginnend in der DMZ – durch das «Edge-to-Core»-Modell nichts im Weg.

Weiteres Vorgehen

In einem ersten Schritt wird vom Provider ein unabhängiger IPv6-Adressrange (PI-Range) bezogen. Erste Services werden zu Erfahrungszwecken zusätzlich mit IPv6 im Dual-Stack konfiguriert (bspw. öffentlicher FTP-Server). Parallel zu diesem Aufbau muss verifiziert werden, ob die aktuelle auf Windows basierte DNS- und DHCP-Infrastruktur den steigenden Anforderungen von IPv6 genügt, oder ob ebenfalls noch ein IPAM-System evaluiert und eingeführt werden muss.

Thomas Amgarten