IPv4 und IPv6 im Parallelbetrieb

In diesem Beitrag:
- Warum IPv6 ein «neues Internet» begründet
- IPv4 und IPv6 nebeneinander betreiben
- Sicherheit als besondere Herausforderung
- «Converged View» auf das Netz

IT-Sicherheit für «zwei Internets»

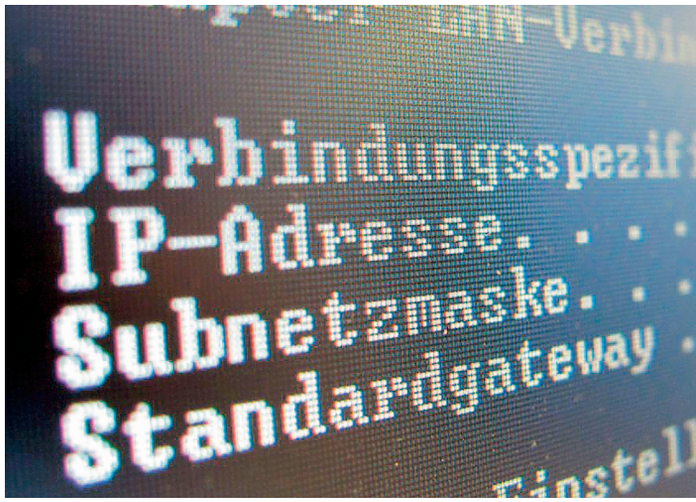
Infos zum Autor

Thomas Boll

Geschäftsführer Boll Engineering, Wettingen

IPv4 und IPv6 sind nicht in der Lage, direkt miteinander zu kommunizieren – ein wesentlicher Grund, weshalb sich die Einführung von IPv6 um Jahre verzögerte. Da eine zeitnahe Migration aller am Internet beteiligten Devices nicht möglich ist, bleibt nur die Variante, beide Netzinfrastrukturen für viele Jahre gleichzeitig zu betreiben.

4,3 Milliarden Adressen – dies sollte für alle Zeiten genügen. Davon dürften die Entwickler des Internet-Protokolls (IP) damals ausgegangen sein. Nicht nur, weil sie das rasante, fast explosionsartige Wachstum des Internets unterschätzt haben dürften, sondern auch, weil sie das zur Verbindung von LANs entwickelte Protokoll nicht primär für ein weltweites IP-Netz konzipiert hatten. Dieser Tatsache zum Trotz: Das mit IPv4 bezeichnete Kommunikationsprotokoll hat sich durchgesetzt und sich als Kommunikationsprotokoll für den weltweiten Internetverkehr etabliert. Mit allen Vor- und Nachteilen. Grösster Engpass ist dabei der begrenzte Adressbereich. So wird es nicht mehr lange dauern, bis die letzten IPv4-Adressen vergeben sind. In einigen, namentlich asiatischen Ländern sind bereits heute keine IPv4-Adressen mehr vorhanden. Dem Data-Highway gehen die «Hausnummern» aus.



Diese Entwicklung kommt nicht überraschend, weshalb bereits vor beinahe 20 Jahren das mit IPv6 bezeichnete Nachfolgeprotokoll entwickelt wurde. Dieses hievt den zur Verfügung stehenden Adressraum in schier unvorstellbare Höhen. Nicht weniger als 340 Sextillionen Adressen – dies entspricht einer Zahl mit 39 Stellen – werden von IPv6 unterstützt. Damit dürfte das Adressproblem definitiv gelöst sein.

Was nach einem simplen Versionsupdate klingt, ist in Wirklichkeit ein neues IP-Protokoll – inkompatibel mit der bestehenden Version und damit im eigentlichen Sinne ein «neues Internet». Dies führt dazu, dass IPv4 und IPv6 nicht in der Lage sind, direkt miteinander zu kommunizieren – ein wesentlicher Grund, weshalb sich die Einführung von IPv6 um Jahre verzögerte. Wer ist denn schon bereit, auf das neue Internet-Protokoll zu migrieren, wenn niemand da ist, mit dem man kommunizieren kann …

Da eine zeitnahe Migration aller am Internet beteiligten Devices nicht möglich ist, bleibt nur die Variante, beide Netzinfrastrukturen für viele Jahre gleichzeitig zu betreiben. Gemäss heutigem Stand der Technik müssen dabei sämtliche ins Netz eingebundenen Devices beide Protokolle gleichzeitig unterstützen (Dualstack Implementation). Naturgemäss ist die Verwaltung zweier IP-Netze komplexer und fehleranfälliger als der Betrieb eines einzigen IP-Netzwerkes. Derzeitige IPv6-Implementationen sehen z. B. vor, Routing-Tabellen oder Security Policies getrennt für beide IP-Versionen anzubieten. Solche Doppelspurigkeiten gehen zulasten der Übersicht und öffnen neue Tore für Fehler und Inkonsistenzen. Da damit gerechnet werden muss, dass IPv4 noch viele Jahre in Betrieb bleiben wird, muss wohl nach eleganteren Lösungen gesucht werden.

Herausforderung Sicherheit

Die Verdoppelung der IP-Infrastruktur beziehungsweise der parallele Betrieb zweier Netze hat nachhaltige Implikationen für System-Hersteller und Anwenderunternehmen – ganz besonders im Bereich der IT-Security. Selbst dann, wenn IPv6 im kleinen Rahmen beziehungsweise punktuell eingeführt wird, müssen zwei Netze konsolidiert konfiguriert und überwacht werden. Dies ist mit «klassischen», portbasierten Firewalls ein höchst komplexes Unterfangen. Deshalb ist ein integrales Management der eingesetzten Security-Lösungen sowie eine konsolidierte Sicht sicherheitsrelevanter Aspekte unabdingbar. Aus heutiger Sicht dürften in diesem Bestreben sogenannte «Next Generation Firewalls» eine bedeutende Rolle spielen. Sie ermöglichen die Abstraktion technischer Grundwerte, was in Bezug auf die zwei IP-Protokolle zu einer «Converged View» führen könnte.

Dazu setzen sie auf abstraktere Begriffe wie die Identifikation und Kontrolle von Anwendungen, Benutzern und Inhalten anstelle von protokollspezifischen Attributen und umgehen so die Begrenzungen herkömmlicher Firewalls. Entsprechende Systeme erkennen User und Applikationen unabhängig von IP-Adressen, von Ports, Protokollen und Verschlüsselungs- oder Verschleierungsmethoden. Dadurch lassen sich Anwendungen und die daraus entstehenden Gefährdungen einfach(er) identifizieren, darstellen und – wenn nötig – blockieren. Was heute bereits möglich ist, dürfte bei Dualstack-Netzwerken unabdingbar sein.

Obwohl die Einführung des neuen Internetprotokolls mit zahlreichen Hürden gespickt ist, ist damit zu rechnen, dass IPv6 schon bald zur Realität wird – namentlich deshalb, weil derzeit keine andere Technologie in Sicht ist, die der Adressnot im Internet begegnen könnte. Es ist folglich keine Frage, ob, sondern wie und wann mit dem Aufbau des zweiten Netzes begonnen wird. Dabei lohnt es sich, den Aspekten der Sicherheit schon jetzt ein besonderes Augenmerk zu schenken. □