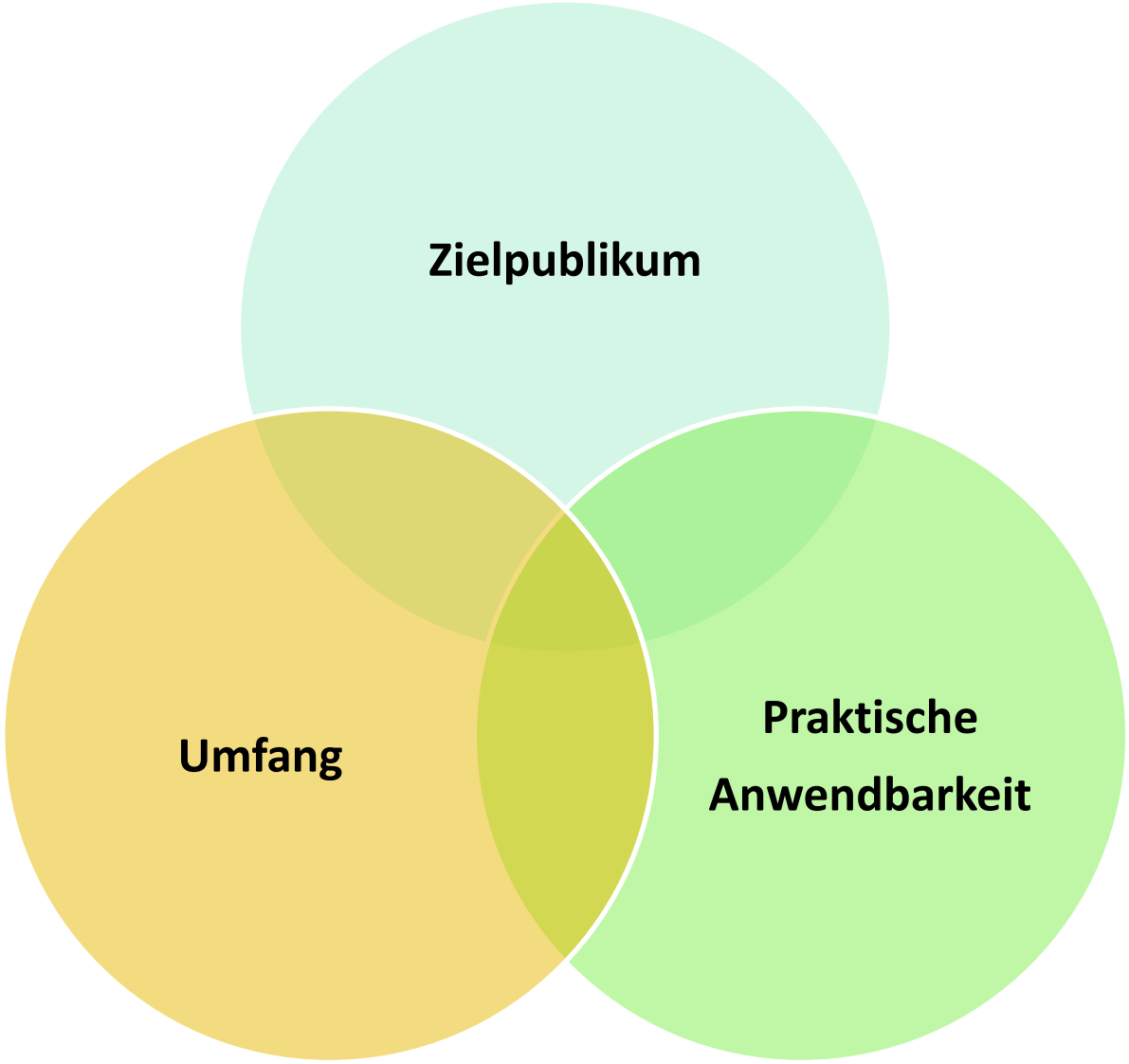
IPv6 Test Suite
Designaspekte und Erfahrungen

European Advanced Networking Test Center

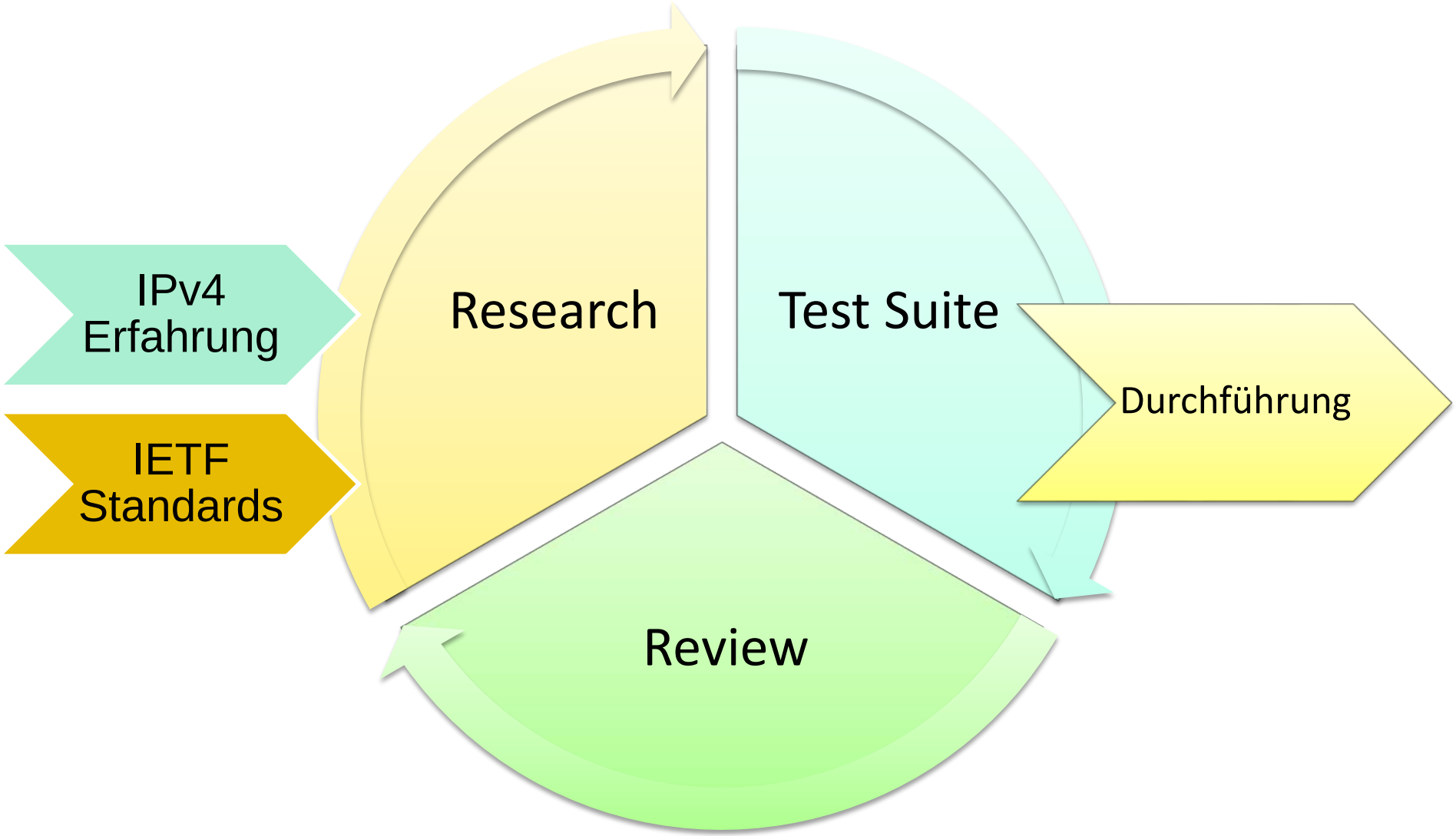
Eldad Zack,12. Juni 2013

EANTC
EUROPEAN ADVANCED NETWORKING TEST CENTER

Designerwägungen



Designverfahren



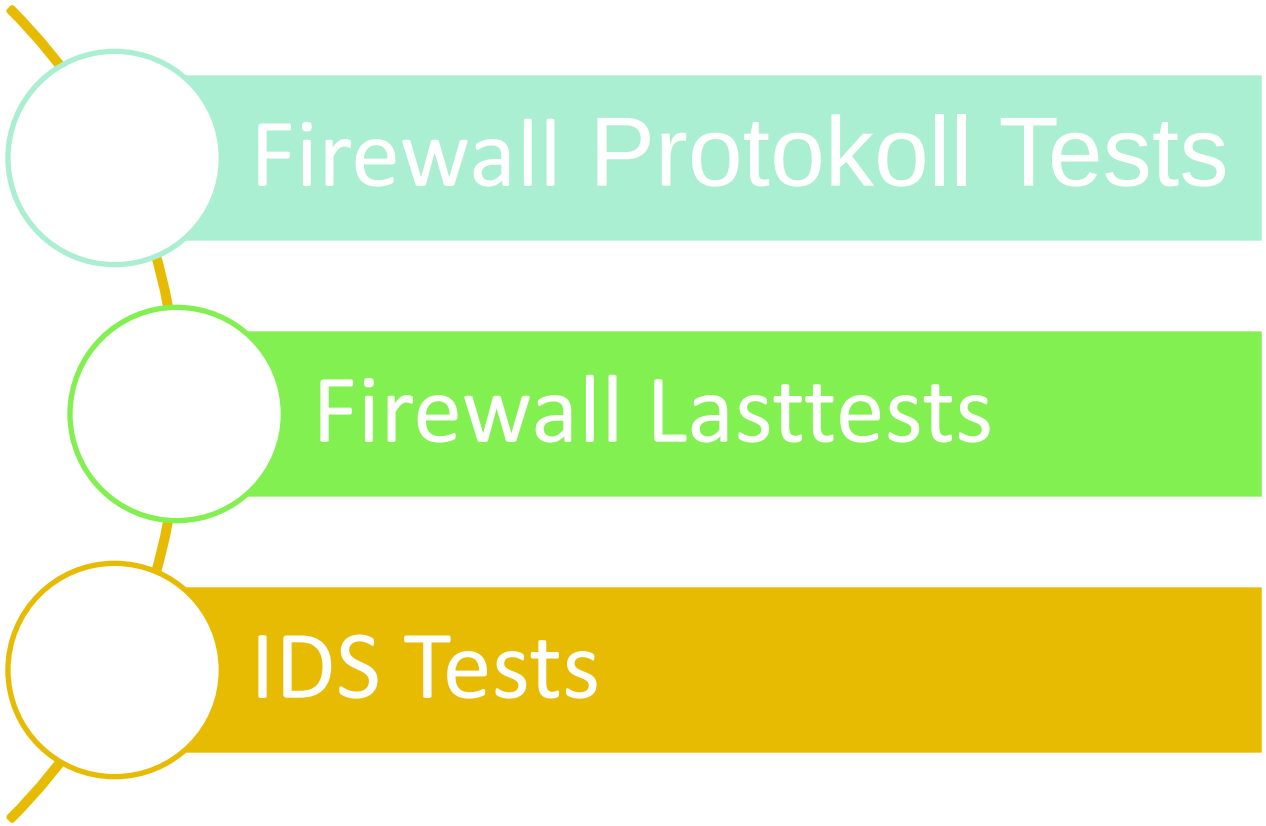
Struktur eines Testcases

- Erläuterung
- Attribute
- Durchführung
- Referenzen

1.8 Excessive Hop-by-Hop Options

PURPOSE	Verify that the firewall detects IPv6 packets with excessive number of hop-by-hop options and applies the security policy.
DESCRIPTION	With the possible exception of the padding options (Pad1, PadN), options should not appear more than once in any given IPv6 packet, as discussed in RFC 4942 section 2.1.9.4. This test verifies that the firewall detects and can filter such packets. It must be noted if additional policy configuration is required for the firewall to do so.
TEST PARAMETERS	• The minimal list of Hop-by-Hop/Destination Options types shall contain: – Jumbo Payload – Tunnel Encapsulation Limit – Router Alert – Home Address – Unassigned option with the "act" field set to 00. • The minimal list of Hop-by-Hop/Destination Options profiles shall contain: – For each member of the types list above, a profile containing only the option repeated twice (and additional padding if needed). – At least 4 of the possible option types permutations. Each option type shall appear twice in at least one profile. Only one option shall appear twice in a single profile.
TEST PROCEDURE & EXPECTED RESULTS	• Verify the currently applied policy contain no rules applying to Hop-by-Hop/Destination Options. • Generate traffic according to each of the defined profile in a Hop-by-Hop options header. 100% traffic loss is expected. • Generate traffic according to each of the defined profile in a Destination Options header. 100% traffic loss is expected.
REFERENCES	"IPv6 Transition/Coexistence Security Considerations", RFC 4942, September 2007

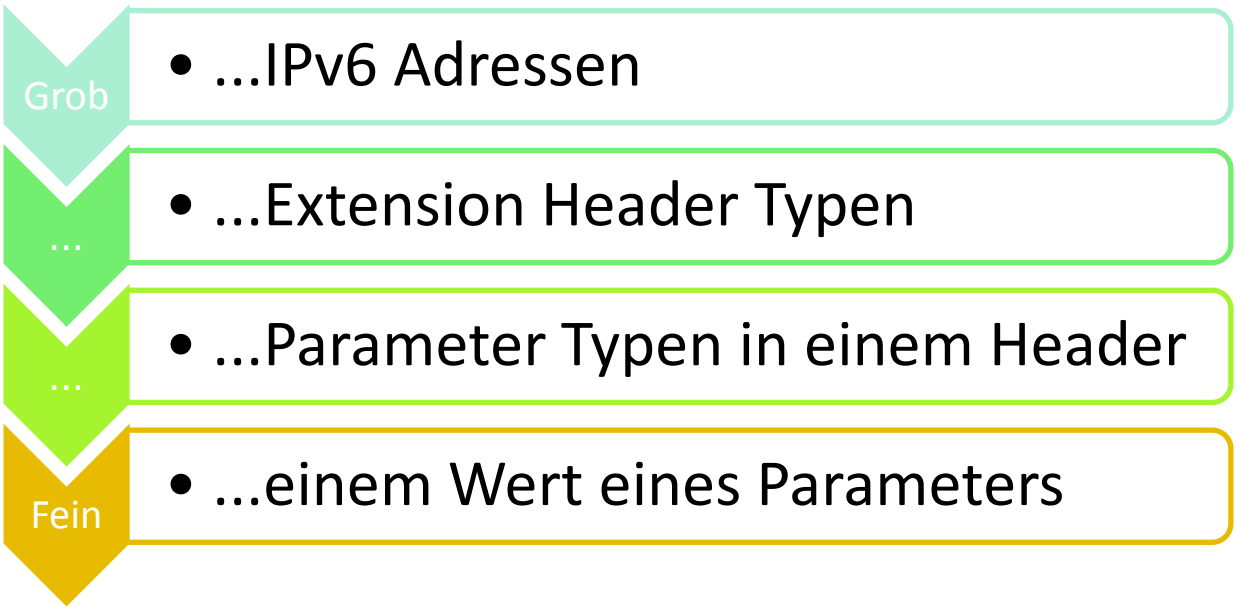
Test Suite Teile

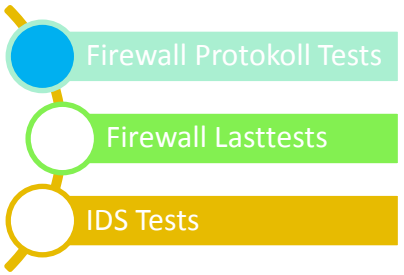


Firewall Funktionalitätstests
Schwerpunkt: Policy (1/2)

- Was soll eine Firewall einem Administrator an Möglichkeiten anbieten?
  - Flexibilität, Granularität

Filter nach...





Firewall Funktionalitätstests
Schwerpunkt: Policy (2/2)

- Beispiel:

  “Security Implications of IPv6 Options of Type 10xxxxxx”

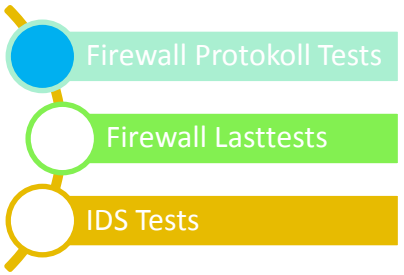
  draft-gont-6man-ipv6-smurf-amplifier

IPv6 maintenance Working Group (6man) — F. Gont
Internet-Draft — SI6 Networks / UTN-FRH
Updates: 2460, 4443 (if approved) — W. Liu
Intended status: Standards Track — Huawei Technologies
Expires: September 22, 2013 — March 21, 2013

Security Implications of IPv6 Options of Type 10xxxxxx
draft-gont-6man-ipv6-smurf-amplifier-03

Abstract

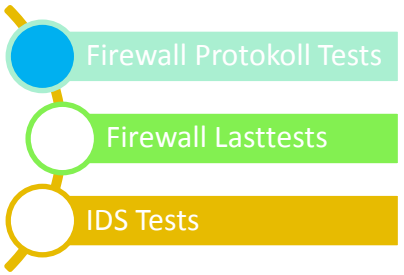
When an IPv6 node processing an IPv6 packet does not support an IPv6 option whose two-highest-order bits of the Option Type are '10', it is required to respond with an ICMPv6 Parameter Problem error message, even if the Destination Address of the packet was a multicast address. This feature provides an amplification vector, opening the door to an IPv6 version of the 'Smurf' Denial-of-Service (DoS) attack found in IPv4 networks. This document discusses the security implications of the aforementioned options, and formally updates RFC 2460 and RFC 4443 such that this attack vector is eliminated. Additionally, it describes a number of operational mitigations that could be deployed against this attack vector.



Robustheitsgrundsatz

“In general, an implementation should be conservative in its sending behavior, and liberal in its receiving behavior.”

IETF RFC 760, “Internet Protocol”



Firewall Funktionalitätstests
Schwerpunkt: Konformität

- Was ist von einer Firewall in Bezug auf IPv6 erwartet?
  - Konformität
  - Strenge Interpretation

1.9 PadN Covert Channel

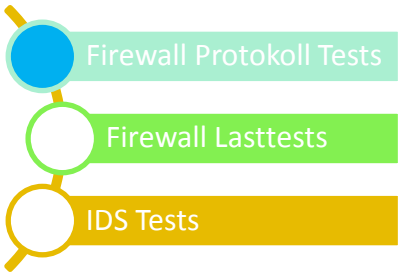
PURPOSE

Verify that the firewall detects and can block packets with non-zero padding in the IPv6 header.

DESCRIPTION

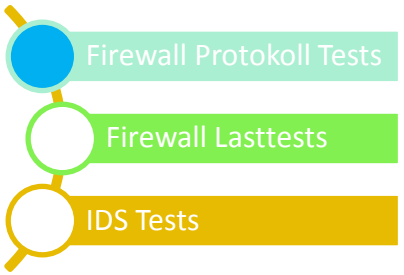
The PadN option is used to insert two or more octets of padding into the Option area of a header, in order to align the headers to multiples of 8 bytes. This is required since the length of the Hop-by-Hop header and the Destination Options header is specified is multiples of 8 bytes. The PadN header can also be used as a covert channel using a the option data field. RFC 4942 discusses this issue in section 2.1.9.5 and recommends that the firewall should verify that the PadN option payload contains only zeroes.

This test will be performed with the Hop-by-Hop header, which should be examined by any IPv6 node forwarding the packet, as well as the Destination Options header.



Firewall Funktionalitätstests
Überblick

Test Case	Anwendbarkeit
ICMPv6 Filtering	Policy
IPv6 Routing Headers	Konformität
IPv6 Header Chain Inspection	Konformität
Filtering Packets According To IPv6 Headers	Policy
Overlapping IPv6 Fragments	Konformität
Tiny IPv6 Fragments	Konformität
Hop-by-Hop/Destination Options Policy	Policy
Excessive Hop-by-Hop Options	Konformität
PadN Covert Channel	Konformität*
Address Scopes	Konformität
Filtering IPv6 Tunneling	Policy

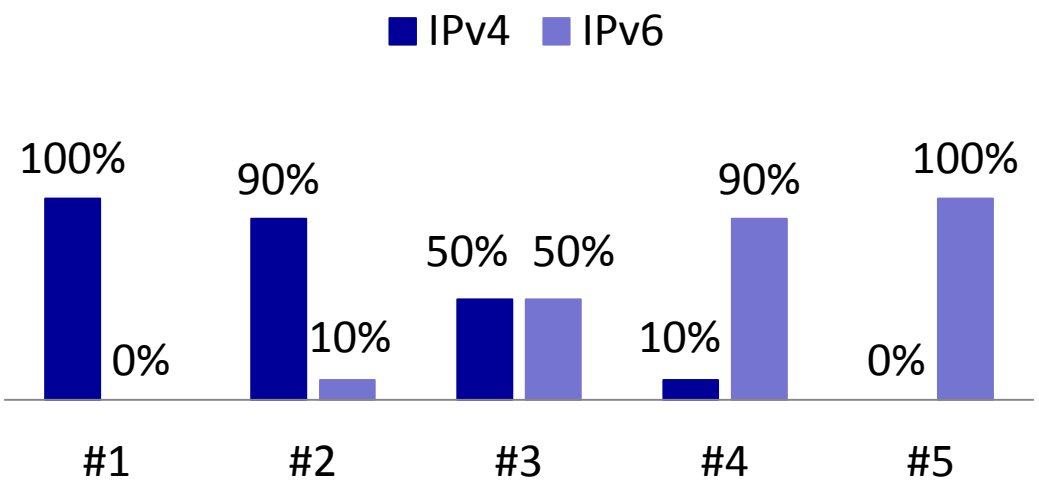


Firewall Lasttests
Schwerpunkt: “Coexistence Traffic”

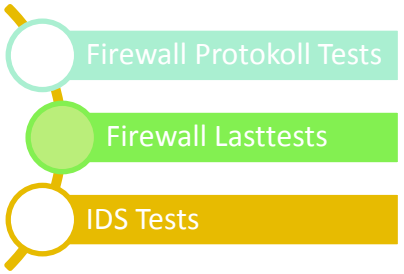
- Auswirkung verschiedener IPv4+IPv6 Mischungen
- Test Methodologie basiert auf IETF RFC 3511

  “Benchmarking Methodology for Firewall Performance”

Coexistence Traffic Mixtures
Based on IETF RFC 5180

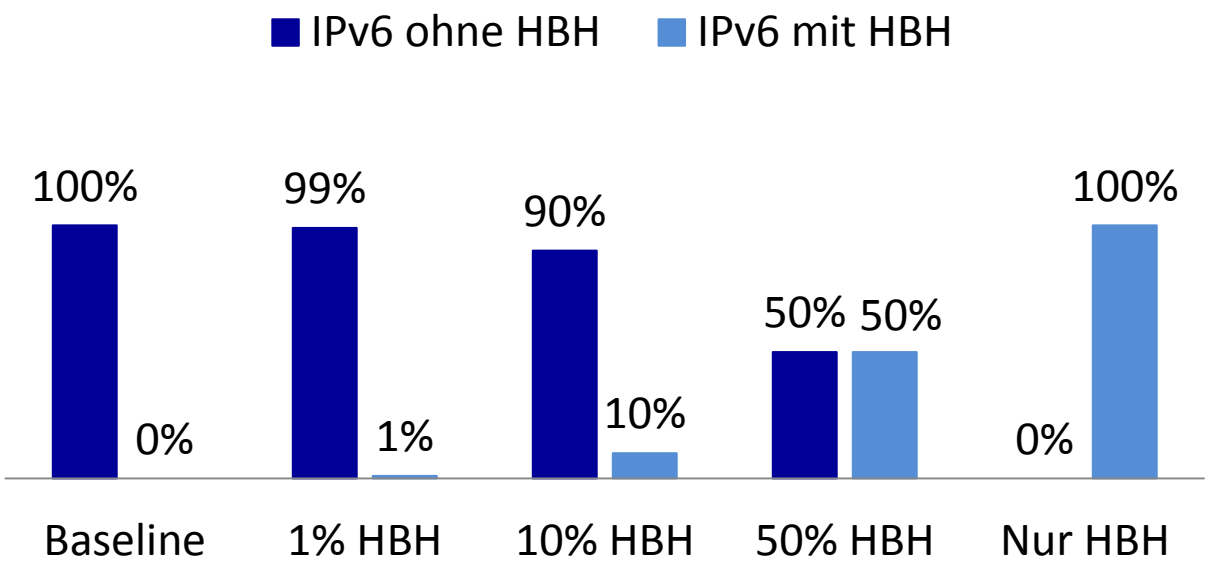


Layer 3 Throughput
TCP Concurrent Connections
TCP Connection Setup Rate
Application Layer Throughput
Latency
Reset Recovery
System Overload Recovery



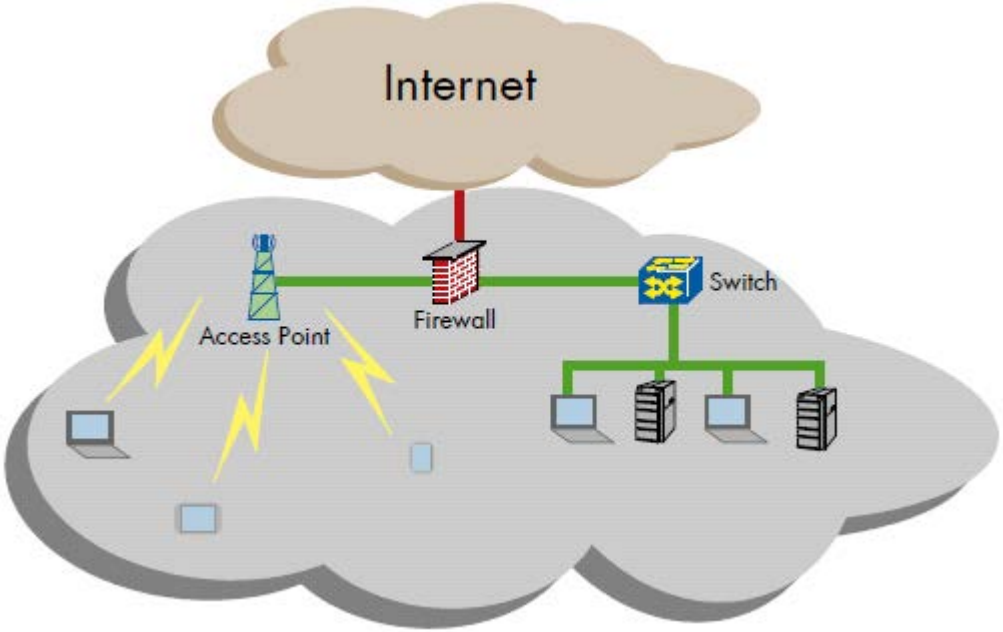
Firewall Lasttests
Schwerpunkt: IPv6-Spezifische Erwägungen

- IPv6 Spezifische Strukturen
  - Hop-by-Hop Options Header
  - Fragmentation Headers
  - Andere Extension Headers, Extension-Headers-Ketten



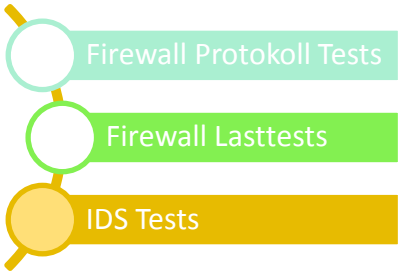
IDS Tests
Schwerpunkt: IPv6 On-Link Angriffe

- Relevanz zu IPv4-Netwerken
- Neighbor Discovery Schwachstellen



IDS Tests
Überblick

- Spoofed Neighbor Discovery Messages
- Duplicate Address Detection DoS
- Spoofed Redirect Message
- Spoofed Zero-Lifetime Router Advertisement Messages
- Router Advertisements Flooding
- Neighbor Advertisements Flooding



Die Test Suite
Zusammenfassung

- 28 Test Cases
  - 11 Firewall Protokoll Tests
  - 11 Firewall Lasttests
  - 6 IDS Tests

- Veröffentlichung nach dem Projektabschluss unter einer Creative Commons Lizenz

Danke für Ihre Aufmerksamkeit!

Ihre Ansprechpartner:

EANTC AG
Salzufer 14
10587 Berlin

Telefon: 030 318 05 95-0
Fax: 030 318 05 95-10
E-mail: info@eantc.de
www.eantc.de