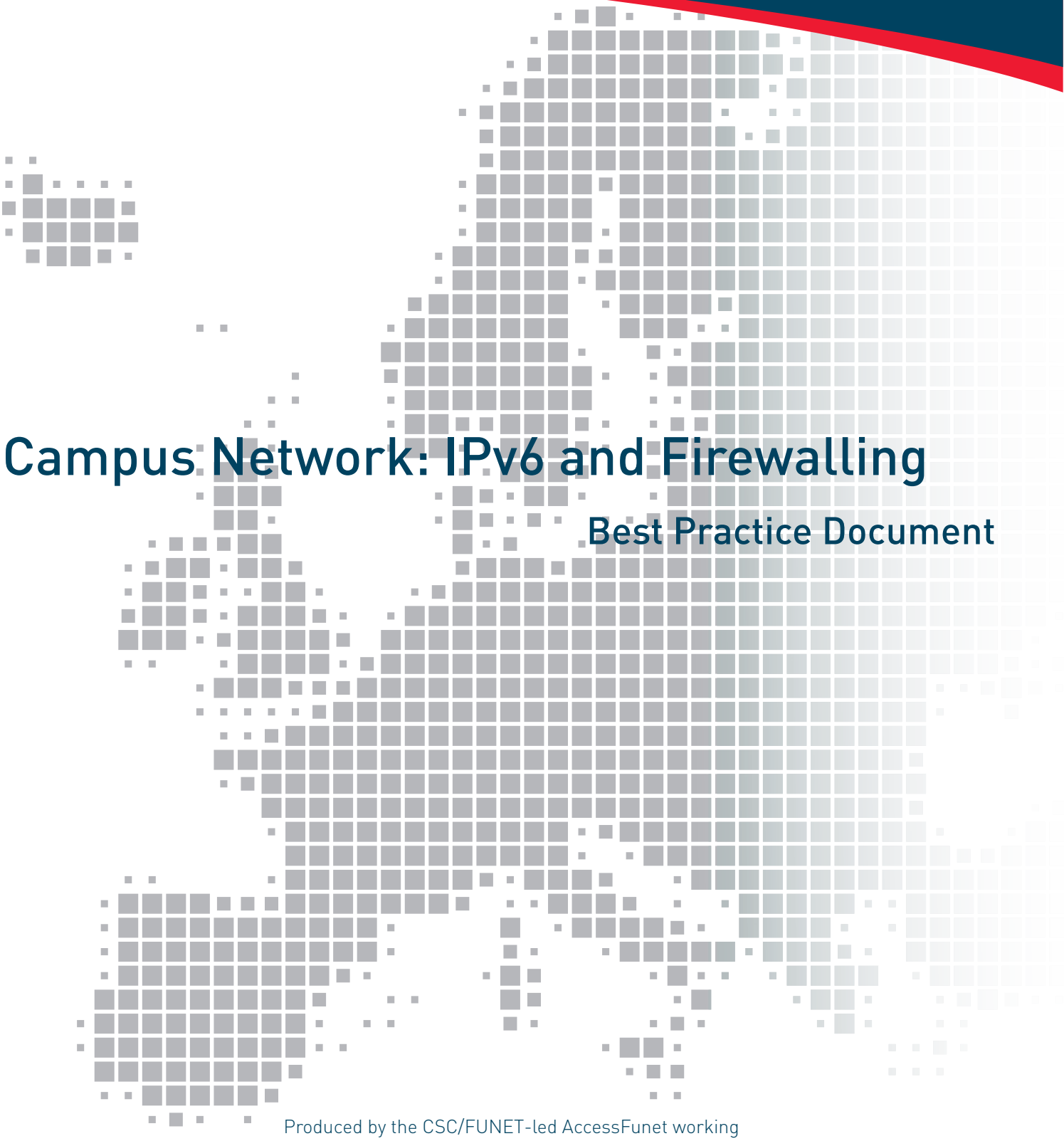
GÉANT
Networks • Services • People



Campus Network: IPv6 and Firewalling

Best Practice Document

Produced by the CSC/FUNET-led AccessFunet working group

Authors: Kaisa Haapala (CSC/FUNET), Ville Mattila (CSC/FUNET), Jani Myyry (CSC/FUNET), Tuukka Vainio (Univ of Turku), Jari Miettinen (CSC/FUNET), Janne Oksanen (CSC/FUNET)
March 2016

Document No: GN4-NA3-T2-FN3.2
Version / date: v1.0/March 2015
Original language : Finnish
Original title: Kampusverkko: IPv6 ja palomuuraus
Original version / date: v1.0/March 2015
Contact: accessfunet@postit.csc.fi

The work has been carried out by a CSC/Funet led working group AccessFunet as part of a joint-venture project within the HE sector in Finland.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Best Practice Document
Campus network: IPv6 and firewalling

Table of Contents

1 Introduction

Firewalls are commonly used to separate different networks with the purpose of filtering out harmful or unintended traffic before it reaches its target. Campus networks often have a firewall at the outer edge of the network, and sometimes also other firewalls in different parts of the network. When planning the IPv6 migration of campus networks, one of the early tasks is to determine the IPv6 readiness of the existing network infrastructure. With firewalls in particular, the IPv6 support may be deficient if IPv6 support was not a requirement at the time of acquisition. Sometimes, for instance, the implementation schedule of features promised by the device manufacturer has been delayed, or enabling the features significantly reduces the performance of the device.

A good starting point is usually to have the same filtering policy for IPv6 as for IPv4. Sufficient attention should be paid to planning the filtering ruleset. The most straightforward method is to create identical filtering rules for both IPv4 and IPv6 using DNS, if the device supports this. There are manufacturer-specific differences in the creation of automated rules, and not all devices work quite as expected. The increase in the number of firewall rules cannot be avoided, and strict filtering policy combined with a needlessly detailed filtering policy leads to the filtering ruleset growing to a very large size. As a consequence, the management of the filtering ruleset suffers and the firewall functionality may turn against itself.

This document is a collection of issues to be taken into consideration when planning and implementing filtering for IPv6 traffic, and practical instructions. Furthermore, the document describes some functions that work differently in IPv6 than in IPv4. You should also keep in mind that a firewall is not the only or even the best solution for all information security risks.

2 Differences in IPv4 and IPv6 traffic

2.1 Migration techniques

IPv6 has been on its way for over ten years. In order to facilitate the migration process, many different tunnelling mechanisms have been developed, and some terminal devices use them automatically to a degree. Tunnelling may open information security holes that have not been taken into consideration in the network firewall, as tunnelling may offer a route bypassing the firewall rules. Examples of tunnelling techniques include 6to4 and Teredo [RIPE 68]. There are also proxy servers in use, allowing traffic to move between IPv4 and IPv6 networks. Proxy servers typically mask the original source address at least in one direction.

2.2 On IPv6 addresses

The large size of the IPv6 address space enables the planned use of addresses, allowing the networks to be grouped by purpose of use, for example. Grouping may be useful in the creation of the filtering ruleset, allowing larger network domains to be handled as a single group. It is justifiable to configure servers to use static IPv6 addresses in place of an automatically generated address so as to prevent the address from changing when, for instance, the network interface card is replaced. The default size of IPv6 subnets is /64; the number of addresses in actual use is only a small part of this.

Link-local addresses beginning with the fe80::/10 prefix form their own challenge for users. Server maintainers might not differentiate between global and link-local addresses and may inadvertently request firewall openings for non-routing addresses. One device usually has at least two IPv6 addresses that look different. Unique local addresses (ULA) with an FD00::/8 prefix that correspond to IPv4 private addresses can be used in local area networks that have no connection to the Internet or that feature network prefix translation (NPT) at the edge of the network.

There are several different presentation formats for IPv6 addresses. The address segments are separated with colons, with the last four bytes possibly separated by dots. There may also be differences in whether zeros are marked or not, and whether lower or uppercase letters are used. This must be taken into consideration if performing address searches or comparisons. It is recommended to follow the RFC 5952 guidelines in the presentation format of IPv6 addresses [RFC 5952].

3 Observations on the special characteristics of IPv6

Address translation, NPT and NA(P)T

If network address translation (NAT) is used for IPv4, no fully equivalent exists for IPv6, nor is it usually required: stateful filtering is sufficient. NPTv6 (Network Prefix Translation, RFC 6296) is a stateless address translation function developed for multihoming purposes. Address translation functions such as NAT64 [RFC 6146] and DNS64 [RFC 6147] are used as migration techniques, allowing IPv4 servers to be visible to IPv6-only clients. NPT also enables switching ISPs without having to renumber the intranet.

IPv6 extension headers

The header of an IPv6 packet is 40 bytes long; furthermore, the header can have a varying number of additional fields. This would enable the flexible introduction of new network functionality. The downside is that the location of a specific header field cannot be known without going through the entire datagram. Compared to IPv4, this makes stateless filtering more laborious or even insufficient. Extension headers can be used for attack purposes by making them large, adding a lot of them, adding malformed header fields or by hiding, for example, a SYN packet opening a TCP connection at the end of a fragment header datagram [RIPE 68].

RFC 5095 finds the Routing header Type 0 (Source Routing) extra field, that should no longer be in use, particularly problematic. It is advisable to check the status of one's own devices, but no action usually needs to be taken [RFC 5095].

Link-local Multicast

In many situations, IPv6 uses multicast for opening connections in the local area network, while multicast is not necessarily needed in IPv4 at all. Necessary multicast traffic must not be prevented (MLD).

ICMPv6

All ICMPv6 traffic cannot be filtered in order for the connections to work. In order to work end-to-end, Path MTU Discovery (PMTUD) requires the ICMPv6 "packet too big" (type 2) messages to be relayed, as the intermediate equipment will not fragment the packets: they will drop packets that are too large. ICMPv6 type 2 packets must be allowed from everywhere. Furthermore, traceroute must be allowed (some firewalls hide themselves from traceroute).

IPv6 Neighbor Discovery

Do not filter the following packets: ICMPv6 type 133, 134, 135 and 136.

IPv4's ARP functionality has been implemented in IPv6 using the Neighbor Discovery address resolution functionality. When a device wishes to discover the MAC address of a neighbour, it sends a Neighbor Solicitation packet (ICMPv6 type 135) to a multicast address formed from the neighbour's IPv6 address. The neighbour will respond to this using unicast with a Neighbor Advertisement packet (ICMPv6 type 136). The devices maintain address information in a Neighbor Cache table. Routers are correspondingly discovered with router discovery. The device sends a Router Solicitation packet (ICMPv6 type 133) to a special all routers multicast address (FF02::2), and the routers respond by sending a Router Advertisement packet (ICMPv6 type 134) to the all nodes multicast address (FF02::1). IPv6 Neighbor Discovery packets have only local significance with the link in question, and

they are not intended to be relayed over routers. The TTL value of the packets must always be 255, which means that packets coming from further away are automatically rejected. For more information, see RFC 4890, "Recommendations for Filtering ICMPv6 Messages in Firewalls" [RFC 4890].

Ping

RFC 4890 recommends allowing Echo Request (Type 128) and Echo Response (Type 129). Ping packets can be used to investigate reachability [RFC 4890].

Filtering unreserved ICMP types

If a firewall blocks ICMPv6 packets of an unknown type, you should check regularly whether IANA has reserved new packet types for use.

Filter these

RFC 4890 recommends filtering the following ICMPv6 packets coming from the outside, none of which should be outgoing from your own network, either. Filtering these will not usually disrupt the connections.

- Node Information Query (Type 139)
- Node Information Response (Type 140)
- Experimental and extension (Types 100, 101, 200, 201, 127, and 255)

4 Device support

4.1 IPv6 support of firewall devices

At the time of writing (03/2015), many widely-used stateful firewalls do not support IPv6 at all, or the implementations are lacking. Some later implementations have not yet been tested in the network environments of Funet member organisations. Due to the problems during the deployment stage of stateful filtering, some Funet organisations have ended up implementing stateless filtering for IPv6 traffic. However, there are situations where stateful filtering is an absolute necessity for information security.

Depending on the device manufacturer, deploying IPv6 may create default rules in the firewall that allow certain packets necessary for the functioning of IPv6. These default rules may be different, depending on whether the firewall is routing or bridged. However, the rules may not necessarily be viewable in the firewall's configuration or user interface. Furthermore, there are still deficiencies in the IPv6 implementations of many device manufacturers. Some of the IPv6 features are relatively new,

and there is only limited operating experience of them. The situation is gradually improving, however, as the defects are identified and corrected.

Firewall performance may become a problem, particularly with IPv6, as the implementation may be a lot poorer than with IPv4. Overloading can be prevented by packet filtering performed before the firewall or by using traffic limitations. With regard to your own device, we recommend contacting the device manufacturer in order to find out its IPv6 filtering functionality and the effects that high amounts of IPv6 traffic have on the firewall's performance. You should ascertain from the device manufacturer how the firewall handles higher-level headers hidden behind extension headers, and attacks using fragments, and how their handling will affect the firewall's performance.

RIPE NCC's IPv6 working group has prepared a document that lists requirements on IPv6 functionality for different network devices. You should utilise this document, for instance during hardware procurement [RIPE 554].

5 On maintenance practices

In order to maintain the uniformity of the firewall ruleset with regard to both IPv4 and IPv6 rules, the maintenance practices must ensure that both are taken care of [RIPE 68]. If the device allows, the rules should be created for both at once. We recommend planning the firewall ruleset management practices taking the long view. We also recommend preparing for changes in network topology, such as the growth of the networks.

A well-made addressing plan makes network maintenance easier. A documented network topology enables flexible changes to the networks.

Abbreviations

ARP	Address Resolution Protocol
DNS	Domain Naming System
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IPv4	Internet Protocol, version 4
IPv6	Internet Protocol, version 6
ISP	Internet Service Provider
MAC	Medium Access Control
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
NAT	Network Address Translation
NPT	Network Prefix Translation
PC	Personal Computer
PMTUD	Path MTU Discovery
RFC	Request For Comment
SYN	Synchronize
TCP	Transmission Control Protocol
TTL	Time To Live
ULA	Unique Local Address

References

[RFC 4861] https://tools.ietf.org/html/rfc4861
[RFC 4890] https://tools.ietf.org/html/rfc4890
[RFC 5095] http://tools.ietf.org/html/rfc5095
[RFC 5952] http://tools.ietf.org/html/rfc5952
[RFC 6146] http://tools.ietf.org/html/rfc6146
[RFC 6147] http://tools.ietf.org/html/rfc6147
[RFC 6296] http://tools.ietf.org/html/rfc6296
[RIPE 68] https://ripe68.ripe.net/presentations/190-IPv6SecurityMyths_RIPE68_May2014.pdf
[RIPE 554] https://www.ripe.net/ripe/docs/ripe-554#requirements5