Issued:	Enters into force:	Validity:
30.11.2020	30.11.2020	until further notice

Legal basis:
Act on Electronic Communications Services (917/2014), sections 243, 247 and 272

Modification details:
Replaces Finnish Communications Regulation Authority Recommendation 312 A/2018 S

FILTERING TRAFFIC IN TELECOMMUNICATIONS OPERATORS' NETWORKS TO CERTAIN COMMUNICATION PORTS FOR INFORMATION SECURITY REASONS

Recommendation of the Finnish Transport and Communications Agency 312/2020 S

Index

1 Introduction

1.1 Background and purpose of the Recommendation

"Net neutrality" (see chapter 3) is a principle of internet traffic, meaning that in the provision of internet access services, all traffic should be treated equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application of service, or terminal equipment.

At the same time, the legislation also requires that telecommunications operators should ensure the information security of their networks and services and defines certain circumstances and conditions under which it is possible to deviate from the net neutrality principle described above; one such reason for exception is maintaining information security. A telecommunications operator may temporarily block or limit traffic to a certain communications port insofar and as long as it is necessary to maintain information security. When applying such a block, it is essential to:

1. scale the protection measures to match the seriousness of the threat to be tackled
2. ensure that the measures do not limit freedom of speech, confidentiality of messages or the protection of privacy any more than is necessary, and
3. discontinue the measures if the conditions for them specified in legislation no longer exist.

Therefore, when considering filtering in practice, it is always essential to assess whether filtering is necessary at all, and if so, for how long it is necessary. As a rule, filtering measures taken for information security reasons should be temporary, and the filtering should be discontinued once the threat is removed.

As part of its day-to-day information security operations, each telecommunications operator assesses the need and grounds to temporarily filter the traffic of the internet access services it provides. This means that each telecommunications operator determines on the basis of its own information security threat observations whether filtering is necessary, and for how long, in order to maintain the information security of the network, the services provided through the network or the terminals of end users.

The responsibilities of the Finnish Transport and Communications Agency, on the other hand, include the following:

- promote the functionality, freedom from interference and security of telecommunications,
- gather information on violations of and threats to information security in respect of network services, communications services and added value services,
- disseminate information security matters, and
- investigate violations of and threats to information security in respect of network services, communications services and added value services.

The Finnish Transport and Communications Agency also has specific powers to issue regulations on matters related to information security.

When carrying out these responsibilities, the Finnish Transport and Communications Agency is, from time to time, informed of information security threats that make it justified for telecommunications operators to generally filter internet access service traffic in order to provide protection from such threats. In such a situation, the

Finnish Transport and Communications Agency primarily recommends telecommunications operators to launch filtering measures. Binding regulations are issued only when necessary and following separate consideration.

Since the recommendations of the Finnish Transport and Communications Agency are not mandatory, each telecommunications operator decides for itself whether it complies with them. However, it should be noted that the Finnish Transport and Communications Agency issues filtering recommendations only on the basis of careful consideration. Therefore, if a telecommunications operator decides not to comply with such a recommendation, it should carefully assess whether it is able to adequately meet its information security obligations without carrying out the filtering measures recommended by the Finnish Transport and Communications Agency.

To make all filtering recommendations issued by the Finnish Transport and Communications Agency – both valid and expired ones – available in one centralised location, the Finnish Transport and Communications Agency has decided to compile its filtering recommendations into this recommendation for telecommunications operators. The compiled filtering recommendations are those issued since the date of entry into force of the EU net neutrality regulation, 30 April 2016. Previous filtering recommendations issued by the Agency before 30 April 2016 are no longer valid.

In addition, the recommendation describes the procedure by which the Finnish Transport and Communications Agency issues further filtering recommendations or recommends to discontinue filtering.

1.2 The procedure of the Finnish Transport and Communications Agency

1.2.1 Assessment of the necessity of filtering

The Finnish Transport and Communications Agency continuously monitors the national information security situation and assesses the need for information security filtering in internet access services provided by telecommunications operators.

When considering whether information security filtering should be recommended, or evaluating the conditions for lifting a filtering recommendation, the Finnish Transport and Communications Agency pays particular attention to the following questions:

- Why would filtering be necessary, i.e. which information security threat or breach could be prevented or mitigated with filtering?
- Would it be possible to provide protection from the threat with another, less stringent means (such as measures taken by users) that does not involve filtering traffic? Would this means be, under any conditions, sufficiently effective?
- What is likely to happen, or could happen at worst, without filtering? To what extent would the telecommunications operators (the actual communications network or service) bear the consequences of not filtering, and to what extent would end users be concerned?
- How does filtering affect the use of services by end users, i.e. does it prevent, and how, the use of a commonly employed service, or are the potential consequences imposed on a very limited group of users?
- Is there a time-bound necessity for the filtering requirement, i.e. how long would filtering take place?

When a telecommunications operator considers filtering carried out for information security reasons, it is, of course, beneficial for the operator to assess the same questions with respect to its own operations.

1.2.2 Issuing and lifting a recommendation concerning a specific communications port

Whenever the Finnish Transport and Communications Agency issues a new filtering recommendation or lifts a recommendation on the filtering of traffic to a specific communications port, it submits a notification to telecommunications operators as follows:

- Issuing a recommendation: an e-mail is sent to the FI-NSP distribution list with the subject line "*Suositus internetyhteyspalveluliikenteen suodattamisesta*" (Internet access service traffic filtering recommendation)
- Lifting a recommendation: an e-mail is sent to the FI-NSP distribution list with the subject line "*Suositus internetyhteyspalveluliikenteen suodattamisen lopettamisesta*" (Recommendation on discontinuing the filtering of internet access service traffic)

The notification describes the reason for issuing or lifting the recommendation and the technical details of filtering (that is, the information provided in chapter 2).

This recommendation will be updated to correspond to the e-mailed recommendation as soon as possible following the e-mail notification – in practice, within a few working days. The updated recommendation will be published in the Agency's Recommendation series (on the website). The reason for this two-stage recommendation procedure is practical: because effective protection against information security threats and breaches often requires quick action, the Agency wants to notify telecommunications operators as quickly as possible of any filtering requirements it has observed. With the two-stage procedure, the Agency ensures that it is possible to issue filtering recommendations also outside standard office hours.

1.2.3 Setting filtering obligations

As far as filtering out traffic to specific communications ports is concerned, the primary aim of the Finnish Transport and Communications Agency is to issue recommendations. Whether a recommendation is complied with or not is up to each telecommunications operator to decide.

If it is not possible to achieve sufficient protection with a recommendation, or the validity period of a recommended filtering measure is becoming more permanent than temporary, the Finnish Transport and Communications Agency considers, on a case-by-case basis, whether a filtering obligation should be called for.

A filtering obligation may take the form of a decision concerning a certain telecommunications operator or, most probably, by adding a new filtering requirement to Regulation 67 on information security of telecommunications services that is binding to all telecommunications operators. At the time of issuing the first version of this recommendation, there is one valid filtering requirement concerning a specific communications port: as a rule, traffic from consumer access links to communications port 25 must be blocked, unless telecommunications operators' servers dedicated for outgoing SMTP traffic are used.

1.2.4 Consultation of telecommunications operators

Telecommunications operators have been invited to submit their opinions on this recommendation and the recommendation procedure described above in chapter 1.2.2 at the time of issuing the first version of the recommendation (312/2017 S, 2.8.2017). The Agency received six (6) opinions on the draft recommendation. The opinions did not contain suggestions concerning changes to the actual port-specific

recommendations (Table 1). After this consultation round, the following amendments and clarifications were made to the recommendation and the recommendation procedure:

- The details of by which distribution list and with which subject line recommendations will be issued and lifted were added in chapter 1.2.2.
- Links to the regulation, decision or notification issued by the Agency concerning each information security incident were added to Table 2.
- Some spelling errors were corrected.

The Finnish Transport and Communications Agency does not organise separate consultation rounds when it issues or lifts new individual filtering recommendations. If necessary, the entire recommendation may be submitted again for comments, if changes are made elsewhere than in Tables 1 and 2.

Nevertheless, when considering the issuance of a new filtering recommendation concerning traffic to a specific communications port or the lifting of an existing recommendation, the Finnish Transport and Communications Agency will, of course, engage in normal information security co-operation with telecommunications operators, i.e., where necessary, the Agency will gather information and opinions from telecommunications operators on the information security situation on a case-by-case basis to support its decisions.

If the Finnish Transport and Communications Agency is considering setting out filtering obligations (either by a decision or a regulation), it will, pursuant to the Administrative Procedure Act, consult telecommunications operators before setting out such an obligation.

2 Filtering recommendations of the Finnish Transport and Communications Agency

The Finnish Transport and Communications Agency's valid recommendations concerning traffic to a specific communications port are shown in Table 1, where the recommendations are listed in the order of the port numbers.

If a certain filtering recommendation is removed, it will be moved to Table 2, which lists the recommendations that are no longer valid. In Table 2, the expired recommendations are shown with the latest removed recommendation first. In other words, Table 2 is a history log file of previous recommendations.

To provide an outline of the filtering environment on a good-to-know basis, the tables also list mandatory filtering obligations. At the time of issuing the first version of this recommendation, there was one valid mandatory filtering obligation concerning a specific communications port (Regulation 67, section 14).

In each of the tables, the following details are listed:

- Port number
  Describes the number of the communications port concerned by the recommendation.

- Protocol
  Describes the communications protocol concerned by the recommendation, i.e. whether the recommendation concerns only the TCP protocol, only the UDP protocol, or both.

- Direction
  Describes whether the recommendation concerns only one or both communications directions, i.e. uplink (UL) or downlink (DL) or both. UL refers to the traffic from the customer to the network and DL refers to the traffic from the network to the customer.

- Technical specifications
  Describes the technical specifications, if any, related to filtering. As a rule, recommendations apply to all internet access services, i.e. both wired and wireless networks and both consumer and business subscriptions, unless otherwise mentioned in this column. Similarly, recommendations apply to both IPv4 and IPv6 traffic, unless otherwise mentioned in this column. Under Technical specifications, it is also possible to propose recommendations concerning, for example, the exact location of the network where filtering should take place.

- Filtering measure
  Describes how traffic to the communications port should be filtered: whether it should be blocked completely or should it merely be limited in one way or another.

- Reason
  Describes shortly the grounds for the filtering measure, i.e. provides a reason why filtering is necessary. Typically, the Finnish Transport and Communications Agency publishes separate bulletins or issues warnings of information security incidents that cause the adverse effects that filtering measures are intended to mitigate. In such publications, the Finnish Transport and Communications Agency describes the background and impacts of the incident more extensively and precisely than in this recommendation.

Table 1 shows the following additional detail of the filtering recommendation:

- Start date
  Contains the date when the recommendation concerning a specific communications port is issued. In practice, the date is the day when the Finnish Transport and Communications Agency e-mails telecommunications operators a notification of a new recommendation.

Table 2 shows the following additional detail:

- Validity

  Describes the duration of the validity of a lifted recommendation, i.e. the dates when the recommendation was issued and lifted.

Table 1. Valid filtering recommendations.

Port no. (Destination port)	Protocol (TCP, UDP)	Direction (UL, DL)[1]	Technical specifications	Filtering measure (for example, blocking or limiting)	Reason	Start date
25	TCP	UL	Applies to consumer subscriptions' outgoing traffic (see Regulation 67 for limitations of scope and associated requirements)	Blocking TCP traffic from the customer to port 25 through servers other than telecommunications operators' servers dedicated for outgoing SMTP traffic	Obligation of Regulation 67 (section 14; Explanatory notes to Regulation 67, https://www.kyberturvallisuuskeskus.fi/en/saadokset-ohjeistukset-suositukset?query=regulation%2067)	1 January 2015
53	UDP	DL	Applies to traffic to consumer subscriptions	Blocking UDP traffic to the customer's port 53	Prevention of and protection against DoS attacks (DNS reflection attack)	12 January 2018
123	UDP	DL	Applies to traffic to consumer subscriptions	Limiting UDP traffic to the customer's port 123 with techniques which don't restrict customary use of NTP client software or prevent operation of servers in the customer subscriptions (for example filtering of NTP control mode packets or rate limiting)	Prevention of and protection against DoS attacks (NTP reflection attack)	12 January 2018
1900	UDP	DL	n/a	Blocking UDP traffic to the customer's port 1900	Prevention of and protection against DoS attacks (SSDP reflection attack)	13 February 2018

[1] Uplink (UL) refers to traffic from the customer to the network, while downlink (DL) refers to traffic from the network to the customer.

Table 2. Previous filtering recommendations no longer in force.

Port number (Destination port)	Protocol (TCP, UDP)	Direction (UL, DL)	Technical specifications	Filtering measure (for example, blocking or limiting)	Reason	Validity
53	UDP	DL	n/a	Blocking traffic	Prevention of and protection against DoS attacks (DNS reflection attack)	30 April 2016–12 January 2018
1900	UDP	UL and DL	n/a	Blocking traffic	Prevention of and protection against DoS attacks (UPnP protocol vulnerability)	30 April 2016–12 January 2018
7547	TCP	UL and DL	n/a	Blocking traffic	Prevention of and protection against DoS attacks (Mirai bot network)	28 November 2016–30 November 2020

3 Legislation and regulations

3.1 Net neutrality

Net neutrality is subject to the EU Regulation concerning electronic communications in the internal market, i.e. Regulation 2015/2120 of the European Parliament and of the Council[2], which is directly applicable in the member states. Section 110 of the Act on Electronic Communications Services[3] (917/2014, previously the Information Society Code) refers to the above Regulation for information purposes.

Article 3 of the Regulation deals with the safeguarding of open internet access, i.e. the "net neutrality" principle:

> "*1. End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.*
>
> *This paragraph is without prejudice to Union law, or national law that complies with Union law, related to the lawfulness of the content, applications or services.*
>
> *2. Agreements between providers of internet access services and end-users on commercial and technical conditions and the characteristics of internet access services such as price, data volumes or speed, and any commercial practices conducted by providers of internet access services, shall not limit the exercise of the rights of end-users laid down in paragraph 1.*
>
> *3. Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.*
>
> *The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.*
>
> *Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:*

[2] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012: http://data.europa.eu/eli/reg/2015/2120/oj.
[3] https://www.finlex.fi/fi/laki/smur/2014/20140917, in Finnish.

(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;

(b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;

(c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

--.”

3.2 Information security obligations and rights

Section 243 of the Act on Electronic Communications Services lays down provisions on the quality requirements for a communications network and service:

”*Public communications networks and communications services and the communications networks and services connected to them shall be planned, built and maintained in such a manner that:*

1) the technical quality of electronic communications is of a high standard and information security is ensured;

2) the networks and services withstand normal, foreseeable climatic, mechanical, electromagnetic and other external interference as well as information security threats;

--

4) significant information security violations and threats against them and other defects and disruptions that significantly interrupt their functionality can be detected;

--

7) the data protection, information security and other rights of users and other persons are not endangered;

--

9) the networks and services do not cause unreasonable electromagnetic or other interference or information security threats;

--.

The measures referred to in paragraphs 1, 2, 4, 7 and 9 of subsection 1 related to information security mean measures to ensure the security of operations, communications, equipment and programmes, as well as the security of information material. These measures shall be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures.

--.”

Section 247 of the Act on Electronic Communications Services lays down provisions on the obligation of a communications provider (including a telecommunications operator) or a provider of added value services to maintain information security:

"*When transmitting messages, communications providers must maintain the information security of their services, messages, traffic data and location data. However, corporate or association subscribers as communications providers are responsible for maintaining information security of messages, traffic data and location data of their users only.*

--

The information security measures must be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures.

--."

Section 272 of the Act on Electronic Communications Services lays down provisions on the measures to implement information security:

"*A communications provider or an added value service provider, or any party acting on their behalf has the right to undertake necessary measures referred to in subsection 2 for ensuring information security:*

1) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services;

2) in order to safeguard the possibilities of the sender or recipient of the message for communications; or

3) in order to prevent preparations of means of payment fraud referred to in Chapter 37(11) of the Criminal Code planned to be implemented on a wide scale via communications services.

Measures referred to in subsection 1 above may include:

1) automatic analysis of message content;

2) automatic prevention or limitation of message transmission or reception;

3) automatic removal of malicious software that poses a threat to information security from messages;

4) any other comparable technical measures in the meaning of subsections 1–3.

If it is evident due to the message type, form or some other similar reason that the message contains malicious software or commands, and the measure referred to in subsection 2(1) cannot ensure the attainment of the goals referred to in subsection 1, the content of a single message may be processed manually. The sender and recipient of a message whose content has been manually processed shall be informed of the processing, unless the information would apparently endanger the attainment of the goals referred to in subsection 1.

Any measures referred to in this section shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding the goals referred to in subsection 1. Such measures must be discontinued if the conditions for them specified in this section no longer exist."

In the context of the obligations listed above, the Act on Electronic Communications Services authorises the Finnish Transport and Communications Agency to issue specific further regulations.

The predecessor of the Finnish Transport and Communications Agency, the Finnish Communications Regulatory Authority (FICORA), has issued Regulation 67 on information security in telecommunications operations[4]. The regulation contains provisions on the following:

- information security measures in all communications networks and services,
- specific information security requirements for interfaces,
- specific requirements for internet access services,
- specific requirements for e-mail services; and
- informing customers about information security issues.

[4] https://www.kyberturvallisuuskeskus.fi/en/saadokset-ohjeistukset-suositukset?query=regulation%2067