FENIX Project Connection Rules

1. INTRODUCTORY PROVISIONS

1.1. These Rules regulate the conditions of connection to the FENIX Project established by the above-mentioned founders within NIX.CZ Association (hereinafter referred to as „**FENIX**“)

1.2. FENIX is established in accordance with the valid Operating Rules and Services Pricelist and the Articles of Association of NIX.CZ Association (hereinafter referred to as „**NIX.CZ**“).

1.3. These Rules also fully apply to the Founders, including any exclusion from the FENIX Project.

1.4. FENIX was founded as a project in the field of cybersecurity and serves mainly as an emergency means of communication between the members and customers of NIX.CZ Association, with a high level of trust and security in the event of a massive attack on the Internet infrastructure.

1.5. The purpose of creating the FENIX Project is to enable a last-resort connection in the event of an attack on a FENIX Project’s member’s infrastructure.

1.6. Connection to the FENIX Project is free of charge.

1.7. NIX.CZ Association is not the Founder, but it is a part of the FENIX Project; it can be connected to it at any time and is entitled to its use in the same way as the Project’s members.

2. CONDITIONS OF INCLUSION OF NEW MEMBERS OR CUSTOMERS OF NIX.CZ ASSOCIATION INTO THE FENIX PROJECT

2.1. Only those members or customers who have been connected to any of the NIX.CZ peering nodes for more than six months can become members of the FENIX Project.

2.2. The applicant must apply for membership in the FENIX Project in writing, while providing:

2.2.1. recommendations for admission from at least two existing members of the FENIX Project who hold positions of responsibility listed in the NIX.CZ Association contact database, while these existing members cannot be part of the same business group as the applicant (i.e., they are economically independent of each other);

2.2.2. a solemn declaration proving the fulfilment of the conditions pursuant to Article 2 (except paragraph 2.5.9);

2.2.3. a description of how the conditions specified in paragraph 2.5.9 are implemented;

2.2.4. a commitment to comply with the Rules;

2.2.5. copies of model customer contracts or Terms and Conditions.

2.3. Any existing member of the FENIX Project can comment on the application for membership in the FENIX Project. Unless at least one sixth of the existing members raise an objection within 14 days from the date of informing the current members of the FENIX Project about the application for membership, the applicant may join the FENIX Project and become a member. Admission to the FENIX project is not a legal right, even if all the conditions under Article 2.5 have been met.

2.4. Membership is closed to NIX.CZ customers who are connected to a NIX.CZ node as part of a partnership programme via another member or customer of NIX.CZ as a partner.

2.5. A valid application for connection to the FENIX Project can be submitted by a member or customer of NIX.CZ which

2.5.1. actively participates in working groups and, if a member, also votes in NIX.CZ bodies at least once a year;

2.5.2. has no overdue liabilities to NIX.CZ and in the last six months has had no overdue liabilities to NIX.CZ for more than 14 days;

2.5.3. does not commit and has not previously committed a repeated or material violation of the NIX.CZ Operating Rules or Articles of Association;

2.5.4. operates fully redundant and independent connections to at least two NIX.CZ nodes, so that in case of failure of all connections to one NIX.CZ node, other nodes can automatically take over and transfer without overload all data traffic exchanged with partners in NIX.CZ. Congestion means exceeding the 95th percentile of the total traffic on other connections; ([1])

2.5.5. contractually prohibits its customers from abusing the network (spamming, attacks, etc.);

2.5.6. operates both IPv4 and IPv6 protocols on its network and assigns them to its customers, while both protocols are actively used to connect to NIX.CZ nodes. It uses IPv4 and IPv6 to make its services available to customers (e.g., web presentations and DNS servers);

2.5.7. has its domains, under which it communicates with its customers or business partners (including company and product websites), signed using DNSSEC technology, so that the algorithms used meet current security standards, except in situations where the deployment of signing is prevented due to serious technical reasons, and has DNSSEC validation enabled on the resolvers operated;

2.5.8. has a monitoring centre (NOC) operating smoothly in 24x7 mode with at least one telephone contact that can be easily accessed even in the event of a massive DDoS attack on the Internet infrastructure of a member published on the NIX.CZ intranet, while the telephone connection goes directly to technicians capable of solving the problem and must not be implemented through IVR;

2.5.9. it uses source address filtering (IP spoofing prevention) in terms of BCP-38 or SAC004 on its network or the part it reports to the FENIX VLAN. For IP addresses within their own AS, granularity must be at least /24 for IPv4 and /48 for IPv6, except for prefixes announced for special purposes (such as RTBH, DDoS Protector,

[1] In the floating time period of the last 720 hours, the other connections must be able to absorb all data traffic exchanged with partners in NIX.CZ, with a tolerance / exception of any 432 five-minute intervals (representing 5 percent of 720 hours) within this time period, in which the traffic reached its highest volume (i.e., 432 operationally significant five-minute intervals, which are ignored during the evaluation).

FlowSpec rules, etc.). Network prefixes obtained within a FENIX VLAN may only be reported to those ASs whose prefixes are available within the FENIX VLAN;

2.5.10. has an amplification-type system for detection and liquidation of attack sources (for example DNS, SNMP, NTP, ban on unmanaged open resolvers, implementation of response rate limiting);

2.5.11. monitors backbone lines and customer connections at least in terms of flows and transmitted packets (e.g., MRTG or similar), where monitoring must be able to actively warn against the deviations of the monitored values from the normal interval;

2.5.12. does not promote, using the BGP protocol, ranges other than those to which it is authorized;

2.5.13. does not send traffic from its network to FENIX VLAN from ranges that it is not authorized to promote from its network;

2.5.14. protects its routers in accordance with RFC 6192 (control plane policy) or in another equally effective way;

2.5.15. runs a CERT / CSIRT team, at least "listed" with the Trusted Introducer (http://www.trusted-introducer.org);

2.5.16. has internal incident management processes in place;

2.5.17. takes measures to eliminate or reduce a security incident as quickly as possible, but no later than 30 minutes after its announcement;

2.5.18. monitors the security notifications of suppliers of its network components and responds to them accordingly;

2.5.19. has all its websites, through which it communicates with its customers or business partners, permanently redirected to the HTTPS protocol provided with a TLS certificate trusted by the most common web browsers, without so-called "mixed content" and with disabled ciphers that are not considered secure.

3. OPERATING CONDITIONS OF CONNECTING TO THE FENIX PROJECT

3.1. A Member of the FENIX Project

3.1.1. actively participates in working groups and voting within the FENIX Project;

3.1.2. monitors the communication of special mailing lists intended for FENIX Project members;

3.1.3. is involved in a Remotely-Triggered Black Hole Filtering (RTBF) system, which is a technique for mitigating the impact of DDoS attacks, through which the target network can determine, using a label designated by the BGP community, which part of the traffic will be blocked on NIX.CZ; the principle of signing valid RPKI prefixes according to point 3.1.7 may only be violated due to the activation of the RTBH system and DDoS filtering;

3.1.4. uses the Route Servers of the FENIX Project, in particular to connect to the RTBH and DDoS filtering system described in Article 3.1.3 and to connect with other members of the FENIX Project;

3.1.5. does not use the connection to the FENIX Project as its main interconnection platform for connecting to the NIX.CZ node, unless there is a technical reason for this, which the member of the FENIX project must announce via the mailing list;

3.1.6. uses RPKI technology to securely route network traffic. The use of RPKI technology refers to the creation and maintenance of ROA records of the owned prefixes. Its input filters are set to reject invalid RPKI prefixes from 31 January 2022 at the latest.

3.2. Connection to the FENIX Project is through a physical port or an 802.1Q.

3.3. BGP sessions within the Project are protected against session hijacking.

3.4. A member must guarantee that the rules according to Article 2.5 and Article 3 are applied appropriately, at least in the part of the network whose address ranges are promoted within the FENIX VLAN.

4. SUPERVISION OF COMPLIANCE

4.1. Compliance with the Rules is supervised by NIX.CZ employees who are authorized to continuously test compliance with these Rules (NIX.CZ is entitled to violate the Rules during such testing). They will report any violations detected to the members of the FENIX Project. The member concerned shall be entitled to comment on the findings made; other members may request explanations or additions to such findings.

4.2. In the event of a breach of the Rules identified by NIX.CZ employees pursuant to Article 4.1 or a Project member, including cases where a FENIX Project member ceases to meet the conditions set out in Article 3, the Director of NIX.CZ shall call for the identified deficiencies to be corrected and sets a reasonable deadline. A member of the Association informs the Director of NIX.CZ immediately about the correction of deficiencies. If the member does not arrange for a correction, the Director of NIX.CZ will suggest to the members of the Project to exclude the said member from the Project. Re-entry to the Project is then only possible in accordance with Article 2.

4.3. If a Project member harms individual members or the FENIX project through their actions or communication, the members shall decide on the exclusion of the member in question, based on the proposal of two or more members of the Project.

4.4. The exclusion decision according to Articles 4.2 and 4.3 is taken if it is voted for by an absolute majority of all Project members.

5. CHANGES TO THE RULES AND OTHER DECISIONS; COMMUNICATION

5.1. Any member of the FENIX Project can propose a change to the Rules. Having discussed the proposal, the Director of NIX.CZ invites the members of the FENIX Project to vote. The proposed change is accepted if it is voted on by the absolute majority of all members of the FENIX Project.

5.2. All members' communication takes place via a special FENIX Project mailing list.

5.3. Each member of the FENIX Project is obliged to inform other members of significant security incidents, which the FENIX Project is intended to prevent or resolve.

5.4. Members voting takes place via the electronic voting system introduced in NIX.CZ.

5.5. Members of the FENIX project must maintain confidentiality regarding the facts they have learnt during their membership in the Project, especially all information exchanged between members in mutual communication, the detected security incidents in other members' networks, matters of compliance or non-compliance with these Rules, as well as the rejection of an applicant for membership in the FENIX project. This information can only be publicized if the member concerned has given their explicit consent; in cases where the source of the information is unknown, all members of the FENIX project must give their consent.

5.6. In the event of a dispute over the interpretation of any of the provisions of these Rules, especially in the case of assessing whether any of the provisions of these Rules have been violated, the decision rests with the Director of NIX.CZ.

6. PUBLICITY

6.1. Each member of the FENIX Project has the right to use a special FENIX logo in the design approved by the Project's members.

6.2. FENIX Project members figure on a special Member's list posted on the NIX.CZ website and explaining the importance of the FENIX project.