NIX.CZ Peering Security Policy

Introduction

The purpose of this document is drafted to serve as a guideline for IXP peering security and its implementation in NIX.CZ.

Scope

This policy defines the procedures to be followed by NIX.CZ and NIX.CZ members/customers to ensure all exchanged routing information is correct and the peering platform is secure and reliable.

Peering partnership – A high security level peering platform is offered to NIX.CZ members and customers. Private peering sessions are also allowed.

FENIX peering partnership – NIX.CZ offers a peering platform to its members and customers with top level security. Members of the FENIX project are required to meet strict rules and policies.

Definitions

"Peering" – connection of two (or more) partners (Internet service providers) exchanging their data

"Peering platform" – set of all technical resources to provide technology for data interconnect

"FENIX" – is a project founded to provide even stricter peering policy

"Route server" – Route server, (RS) is a device re-distributing routing information based on security rules

"Client" – NIX.CZ customer or member

Peering platform physical security

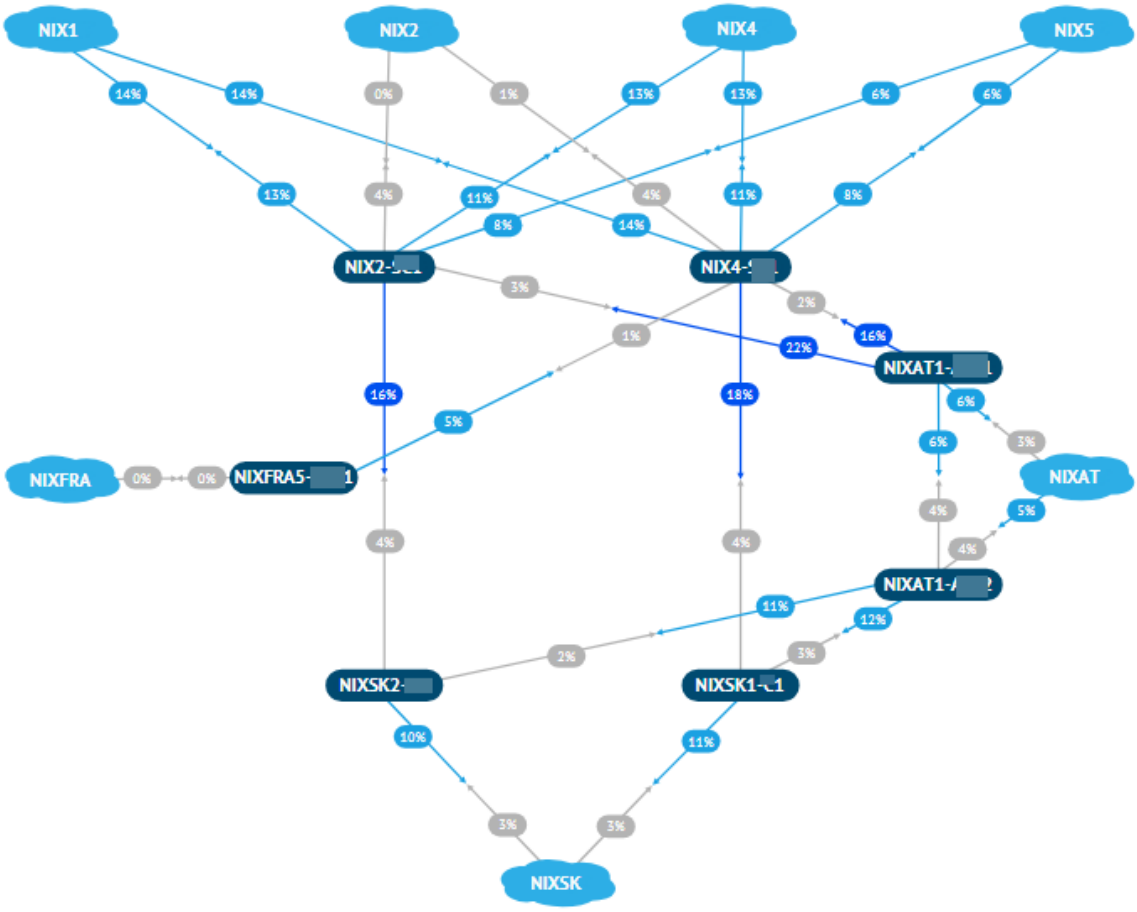
NIX.CZ offers connection to its peering platform with the highest possible security settings. The network topology is fully redundant with its dual star configuration. All nodes are powered with multi-homed power sources including AC and DC diversity. Active nodes are hosted in Tier 3 level datacenters or Tier 3 equivalent (all systems are redundant in N+1 level).

Active technology is placed in dedicated security cages or rooms within datacenters with limited access permission. All access is actively monitored using an access electronic alarm (door switch) escalated to an on call technician. All caged premises are monitored with CCTV surveillance cameras and are logged.

All operation parameters are monitored 24x7 with instant notification to technician on call.

Peering platform network security

Network topology



Each peering client has the following port configuration settings:

Client's port security settings contain

- MAC address per port and VLAN limitation
- BPDU filter – don't send BPDU packets
- BPDU guard – don't receive BPDU packets
- Storm control for broadcast and multicast (where multicast is not provided as a service)
- MAC address limitation – 2 MAC per VLAN with strict shutdown on violation
- RTBH filtering on ingress
- On trunk ports – only allowed VLANs are permitted
- Filtering all unnecessary L2 protocols as CDP, VTP etc.

Route servers

NIX.CZ provides the option to peer on BGP route servers. We do encourage all peering partners to use route server, however private peering policy is also available. By the end of September, new route servers will be running with the following configuration.

Filtering steps

1. Drop small prefixes – longer than /24 for ipv4 and longer than /48 for ipv6.
2. Drop all well-known martians and bogons.
3. Ensure that there is at least 1 ASN and less than 64 ASNs in the AS path.
4. Ensure that the peer AS is the same as the first AS in the AS path.
5. Drop any prefix where the next-hop IP address is not the same as the peer IP address
6. Drop any prefix with a transit network ASN in the AS path.
7. Ensure that origin AS is in set of ASNs from the client's IRRDB AS-SET.
8. If the prefix is evaluated as RPKI valid, accept
9. If the prefix is evaluated as RPKI invalid, drop
10. If the prefix is evaluated as RPKI unknown, revert to standard IRRDB prefix filtering.

RTBH filtering (Remotely Triggered Black Hole) settings is available to each customer/client. When an IP prefix with BGP community settings is advertised, the client has a possibility to influence their own prefix to be blackholed by a peering partner.

DDoS protection

NIX.CZ offers DDoS protector to its members and customers. Clients can configure Route Server in order to re-direct traffic to their own network via DDoS protector. This is done using BGP communities. Redirected traffic is sent back from DDoS protector to destination network, filtered, without unwanted traffic.

DDoS filtering is only available when using Route Servers, it does not have any effect on direct peering.

FENIX project

Since 2013 clients can apply for FENIX project membership. All networks connected in this project have to implement even stricter network and administrative policies within their own network and be able to mitigate all kind of network related issues such as DDoS or other malicious behavior. Members have a virtually separated peering platform. This is to be used in case of emergency or other critical event as a closed, dedicated or even completely isolated connection environment.

Organizational conditions

- Active participation in the Association's workshops and voting procedures regarding the FENIX project
- 24/7 Network Operation Center
- Operational CERT/CSIRT team with an appropriate status at least listed with Trusted Introducer

- Implemented internal incident resolution procedures

Technical conditions

- Fully redundant connection into at least two of NIX.CZ nodes
- Network uses both IPv4 and IPv6 protocols
- Domain names signed by DNSSEC technology
- Part of the RTBH filtering system
- Use of FENIX-operated Route Servers

Reference

- A candidate must provide reference from at least two existing FENIX members and submit a written declaration of having fulfilled all technical and organizational requirements

Detailed conditions and rules can be found here https://www.nix.cz/cs/file/NIX_RULES_FENIX