VANIX
VANCOUVER INTERNET EXCHANGE

VANCOUVER INTERNET EXCHANGE
(the "Corporation" or "VANIX")

CONNECTION AND PEERING POLICY

Purpose of the Policy

The purpose of this policy is to articulate the rules that apply for connection to, and peering at, the locations operated by VANIX.

The Organisation

VANIX is a not-for-profit corporation incorporated on August 29, 2015, as Vancouver Internet Exchange under the *Canada Not-for-profit Corporations Act*, S.C. 2009, c.23. One of the stated purposes of the Corporation is: "To provide an infrastructure that facilitates the exchange of communications network traffic among Internet service providers, network service providers, content service providers and other entities that need to exchange communications network traffic within Canada".

VANIX Locations

In order to fulfil its mandate, VANIX operates a number of peering locations, which may be amended at the sole discretion of, and timing determined by, VANIX from time-to-time. A list of current locations is available at https://vanix.ca/getting-connected/locations/.

Interconnection with the VANIX Infrastructure at the Locations

Any organisation that operates a communication network and satisfies the following conditions may connect to the VANIX peering infrastructure for the purpose of exchanging traffic with other peers connected to that infrastructure, thereby becoming a participant in the exchange:

1. The organisation has delivered a complete and signed Service Order to VANIX specifying the peering services that it wishes to obtain from VANIX and the location(s) at which it intends to interconnect, based on the options that VANIX makes available to peers from time-to-time;

2. The organisation has specified its applicable Autonomous System number;

3. The organisation has provided a link to its PeeringDB (https://www.peeringdb.com/) peering network database record;

4. The organisation has paid the necessary installation charge(s) so as to be in good financial standing with VANIX;

5. The organisation has provided the technical information that VANIX requires to connect the participant's network to the VANIX exchange (including, without limitation the requested media type(s) and media access control ("MAC") address of the organisation's applicable Layer 3 equipment), and interconnection is being requested to be accomplished in a manner that is compatible with the peering equipment operated by, and technical requirements of, VANIX;

6. The organisation has made the necessary arrangements, including ordering all meet-me-room cross-connect(s) to reach the Ethernet interface at the VANIX port, all at its own expense, at each VANIX location at which it seeks interconnection;

7. The organisation adheres to all required technical interconnection and peering rules of VANIX, as amended from time-to-time.

Technical Requirements for Interconnection and Peering at VANIX

An organisation that peers at VANIX (i.e., is a participant) must also meet the following technical requirements:

1. The participant has a globally unique public autonomous system number issued by a Regional Internet Registry ("RIR").

2. The participant maintains up-to-date contact information in the PeeringDB database.

3. The Ethernet link supporting the connection between the participant and the VANIX port supports an MTU of at least 1500 bytes.

4. The participant holds a valid delegation of its own Internet Protocol ("IP") IPv4 and/or IPv6 address space that the participant intends to advertise.

5. The participant maintains either Resource Public Key Infrastructure ("RPKI") or Internet Routing Registry ("IRR") entries in a corresponding authoritative routing service. In accordance with MANRS for IXP recommendation, the VANIX route-server filtering policy is based on the combination of IRR and PeeringDB entries. Use of the route server must be consistent with the requirements set out at https://vanix.ca/route-server-info/.

6. Broadcast and multicast traffic must not be sent to VANIX except as required for normal operations as determined by VANIX.

7. The participant must disable the following features on the interface facing the VANIX port if/where applicable:
    a. IPv6 Router Solicitation or Advertisement packets
    b. Spanning tree protocol
    c. Layer 2 protocols such as CDP, UDLD, EDP, VTP, DTP, LLDP
    d. Interior routing protocols such as OSPF, ISIS, IGRP, and EIGRP

    e. Protocol-Independent Multicast (“PIM”) traffic
    f. Proxy-ARP

8. Participants must only send traffic to the exchange the following EtherTypes:
    a. 0x0806 – ARP
    b. 0x0800 – IPv4
    c. 0x86dd – IPv6

9. Participants must not point a default route towards another participant without the permission of the other peers.

10. Participants should use a Layer 3 port where possible. If a Layer 2 port is used, only the single MAC address authorized by VANIX must be visible.

11. Participants must use Border Gateway Protocol (“BGP”) 4 to exchange routing information.

12. Where necessary to protect the integrity of the VANIX network infrastructure, as well as peering and other services provided by VANIX, VANIX may direct participants to adhere to additional technical requirements.

Please note that the transceiver on the VANIX switch is provided by VANIX.

Policy breach

Breaches of this policy can lead to suspension and even termination of a peer’s right to interconnect at the VANIX IXP. Additional legal remedies may also apply depending on the consequences and any harm caused by such breaches.

VANIX Peer, Participant and Member Definitions

Organisations that peer at VANIX are known as peers or participants. Organisations that are participants in good standing may also apply for and become members in the VANIX corporate entity in accordance with the terms of the VANIX by-laws. A prescribed membership form is used for that purpose. Members are entitled to vote at annual and other meetings of members. Participants that do not choose to be members do not have such rights.

This Policy was passed by the Board of Directors of the Corporation on the 9th day of September, 2020.