Singapore Internet Exchange

Singapore Internet Exchange Limited
10 Collyer Quay #10-01
Ocean Financial Centre Singapore 049315

Company Registration No: 200916410W

SINGAPORE INTERNET EXCHANGE (SGIX)

Acceptable Use &
Technical Requirements Policies

Acceptable Use Policy

General

1. All Peers are responsible for ensuring that the Peering Fabric is available on a fair basis to all other Peers, meaning that all Peers shall have access to their maximum contracted port bandwidth for useful traffic unhindered by any inadvertent or deliberate act.
2. Where it is in their power to do so, Peers shall take all reasonable measures, including measures that SGIX may propose, to ensure the correct functioning of the exchange, including proactively managing traffic on their own networks, regardless of how or by whom that traffic is generated.

Prevention of network flooding and denial-of-service attacks

1. Peers are responsible for monitor their networks appropriately on a 24/7 basis and to ensure that their usage of SGIX Services is not likely to and does not cause network flooding or denial-of-service attacks.
2. To reduce the probability of unintentional network flooding, or deliberate denial-of-service attacks, Peers shall comply with all requirements of the Technical Requirements policy which specifies which kind of traffic and packet types may be forwarded to the Peering Fabric.
3. To prevent unknown unicast flooding to all ports in Peering Fabric, Peers are responsible for drain their traffic during their planned maintenance.

Unauthorised access or malicious attempts to compromise the SGIX network

1. Peers shall take reasonable measures to prevent unauthorised access or malicious attempts to compromise the SGIX network.
2. Peers shall not release information to any unauthorised party, that could assist with any attempt to compromise the SGIX network. This includes privileged confidential information provided to Peers, as well as general information, not already in the public domain, about SGIX that might be useful to this unauthorised party.
3. Violations of system or network security are prohibited. SGIX reserves the right to release the contact information of Peers involved in violations of system security to other Peers, in order to assist them in resolving security incidents. SGIX will also fully cooperate with law enforcement authorities in investigating suspected lawbreakers.

4. Examples of system or network security violations include, but are not limited to, the following:
    a. Using SGIX services to compromise the security or tamper with system resources or accounts on the SGIX infrastructure or at any other site;
    b. Use or distribution of tools designed for compromising security. Examples of these tools include but are not limited to password guessing programs, cracking tools or network probing tools;
    c. Unauthorized access to, or use of data, systems or networks. This includes any attempt to probe, scan or test the vulnerability of a system or network or to breach security;
    d. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network;
    e. Forging of any TCP/IP packet or packet header or any part of the header information in an email or newsgroup posting;
5. SGIX reserves the right to disconnect all ports involved in malicious activities, and/or port scanning.

Technical Requirements Policy

General

1. Peers must ensure that all traffic sent over the Peering Fabric conforms to the requirements of this policy.
2. Peers shall ensure that their usage of SGIX is never detrimental to the Peering Fabric. The term "detrimental" refers to usage which, in the reasonable opinion of SGIX Management:
    a. does not conform to this technical connection policy;
    b. causes undesirable load and/or traffic patterns;
    c. adversely affects other Peers and/or the entire exchange.

Physical interfaces

1. Ethernet interfaces attached to SGIX ports shall be explicitly configured with duplex, speed and other configuration settings and shall not be auto-sensing.

MAC layer

1. Frames forwarded to SGIX ports shall have one of the following ethertypes:
    a. 0x0800 - IPv4;
    b. 0x0806 – ARP;
    c. 0x86dd - IPv6;
2. All frames forwarded to a single SGIX port must have the same source MAC address.
3. Use of proxy ARP on the router's interface to the Exchange is not allowed.
4. Frames forwarded to SGIX ports shall not be addressed to a multicast or broadcast MAC destination address except as follows:
    a. Broadcast ARP packets
    b. LACP Multicast group MAC address
    c. Multicast IPv6 Neighbour Discovery packets. This does not include Router solicitation, Advertisement and Renumbering packets.

5. Traffic for link-local protocols shall not be forwarded to SGIX ports except for the following:
    a. ARP
    b. IPv6 ND
6. Link-local protocols which shall not be forwarded to SGIX ports includes but is not limited to:
    a. IRDP
    b. ICMP redirects
    c. IEEE802 Spanning Tree
    d. Vendor proprietary discovery protocols (e.g. CDP, EDP)
    e. VLAN trunking protocols (e.g VTP, DTP)
    f. Interior routing protocol broadcasts (e.g. OSPF, ISIS, IGRP, EIGRP)
    g. BOOTP/DHCP
    h. PIM-SM
    i. PIM-DM
    j. DVMRP
    k. ICMPv6 ND-RA
    l. LLDP
    m. UDLD
    n. L2 Keepalives

IP layer

1. Interfaces connected to SGIX ports shall only use IP addresses and net masks assigned to them by SGIX. In particular: IPv6 addresses (link & global scope) shall be explicitly configured and not auto-configured. IPv6 site-local addresses shall not be used.

Routing

1. All exchange of routes across the SGIX network shall be via BGP4+.
2. AS numbers used in BGP4+ sessions across the SGIX network may not be from ranges reserved for private use.
3. Peers using multi-lateral peering via SGIX Route Servers MUST ensure that their devices support the disabling of BGP enforce-first-AS checking.
4. Advertising of private IP address ranges (RFC1918) and default routes is not allowed on SGIX Route-Servers.

5. SGIX supports good engineering practice and SGIX Peers are encouraged to aggregate their routes in accordance with RFC2519 "A Framework for Inter-Domain Route Aggregation".
6. IP address space assigned to SGIX peering LAN shall not be advertised to other networks without explicit permission of SGIX.
7. All routes advertised across the SGIX network shall point to the router advertising it unless an agreement has been made in advance in writing by the two Peers involved, and SGIX remains informed of this by the Peers involved.
8. All routes to be advertised in peering sessions across the SGIX public peering network shall be registered in the RIR Routing Information Service database or other public routing registry.

Forwarding

1. Traffic shall only be forwarded to a Peer when permission has been given by the receiving Peer either:
    a. By advertising a route across the SGIX network;
    b. or explicitly in writing.
2. Traffic must not be routinely exchanged between two SGIX ports owned by the same Peer.