.ca Canadians Connected
Canadiens branchés

CIRA IPv6 Policy

Overview

CIRA’s intention for publishing an IPv6 Security policy is to apply best practices to the implementation and overall management of the IPv6 protocol on CIRA’s network. The IPv6 protocol shares many similarities with IPv4 but there are also significant differences. These differences include 128 bit IP address space, additional features in ICMPv6, new multicast addresses and neighbour discovery just to name a few. These new features also give way to new attack vectors and vulnerabilities which must be mitigated.

Purpose

The purpose of the policy is to outline the best practices for IPv6 security and establish an approval process for any recommended changes to the policy and to CIRA’s network configurations. These rules are in place to protect CIRA and its employees from intentional and unintentional security violations which could lead to loss of network connectivity, interruption in services provided and damage to CIRA’s reputation.

Scope

This policy applies to all employees and covers all equipment including routers, switches, firewalls, VPNs, servers, workstations and any other equipment owned or managed by CIRA.

Policy

- Default deny of IPv6 addresses and services on perimeter devices such as firewalls, VPN appliances and routers.
    - Log all denied traffic
- Block 6to4, ISATAP (rfc5214) and TEREDO (rfc4380) and other IPv6 to IPv4 tunneling protocols on perimeter firewalls, routers and VPN devices as this can bypass security controls.
    - Block TEREDO server UDP port 3544
    - Ingress and egress filtering of IPv4 protocol 41, ISATAP and TEREDO use this IPv4 protocol field
- Filter internal-use IPv6 addresses at border routers and firewalls to prevent the all-nodes multicast address (FF01:0:0:0:0:0:0:1, FF02:0:0:0:0:0:0:1) from being exposed to the Internet.
- Filter unneeded IPv6 services at the firewall just like IPv4.

- Filtering inbound and outbound RH0 & RH2 headers on perimeter firewalls routers and VPN appliances.
- ICMPv6 messages to allow RFC4890.
        - Echo request (Type 128)
        - Echo Reply (Type 129)
    - **Multicast Listener Messages to allow**
        - Listener Query (Type 130)
        - Listener Report (Type 131)
        - Destination Unreachable (Type 1) – All codes
        - Packet Too Big (Type 2 message)
        - Time Exceeded (Type 3) – Code 0 only
        - Parameter Problem (Type 4 message)
        - Listener Done (Type 132)
        - Listener Report v2 (Type 143)
    - **SEND Certificate Path Notification messages:**
        - Certificate Path Solicitation (Type 148)
        - Certificate Path Advertisement (Type 149)
    - **Multicast Router Discovery messages:**
        - Multicast Router Advertisement (Type 151)
        - Multicast Router Solicitation (Type 152)
        - Multicast Router Termination (Type 153)
- Deny IPv6 fragments destined to an internetworking device.
- Drop all fragments with less than 1280 octets (except on the last one).
- Filter ingress packets with IPv6 multicast (FF05::2 all routers, FF05::1:3 all DHCP) as the destination address.
- Filter ingress packets with IPv6 multicast (FF00::/8) as the source.
- Use IPv6 hop limits to protect network devices to drop hop count greater than 255.
- Configure “no ipv6 source-route” and “no ipv6 unreachable” on external facing perimeter devices.
- Drop all Bogon addresses on perimeter firewalls, routers and VPN appliances.
- Infrastructure devices (firewalls, routers, switches, servers, network appliances) must be configured with a static IPv6 address.
- DNS entries must be configured for all network nodes.
- OSPFv3 configured to use filtering, passwords and hashes.
- BGPv4 explicitly configured peers, BGP session shared secret, and IPSEC tunnels whenever possible.

- The following prefixes must be filtered as they should not appear on the Internet, based on rfc5156.

Unspecified address	::
Loopback address	::1
IPv4-compatible addresses	::/96
IPv4-mapped addresses	::ffff:0.0.0.0/96 ::/8
Automatically tunneled packets using compatible addresses	::0.0.0.0/96
Other compatible addresses	2002:e000::/20 2002:7f00::/24 2002:0000::/24 2002:ff00::/24 2002:0a00::/24 2002:ac10::/28 2002:c0a8::/32
Deny false 6to4 packets	2002:e000::/20 2002:7f00::/24 2002:0000::/24 2002:ff00::/24 2002:0a00::/24 2002:ac10:;/28 2002:c0a8::/32
Deny link-local addresses	Fe80::/10
Deny site-local addresses	Fec0::/10
Deny unique-local packets	Fc00::/10
Deny multicast packets (only as a source address)	Ff00::/8
Deny documentation address	2001:db8::/32
Deny 6Bone addresses	3ffe::/16

Monitoring

Quarterly reviews will be performed to evaluate the effectiveness of this policy and to make any modifications required in response to new information, technology or standards.