

**ICAO***International Civil Aviation Organization***Eleventh Meeting of the Common aeRonautical Virtual Private Network Operations Group (CRV OG/11)***Bangkok, Thailand, 01-03 February 2023*

- Agenda Item 4: CRV OG Reference documents
- CRV OG Operations Manual
 - CRV Implementation Plan
 - Outcomes of Ad-hoc expert Strategy, Design, Transition and, Operations Groups

MANDATE FIREWALL

(Presented by Airways New Zealand)

SUMMARY

This paper presents information on the potential to mandate the use of a firewall as part of the CRV implementation.

1. INTRODUCTION

- 1.1 A joint CRV OG Experts and SWIM TF TLs meeting was held on 28 October 2022 and the topic of security was raised by the SWIM TLs.

2. DISCUSSION

- 2.1 The APAC CRV Operations manual states:

Security is the responsibility of States for the implementation of security controls to ensure the integrity of services.

As a minimum the connectivity states is via GE Tunnels.

Other methods of ensuring the security of the connectivity are:

- a. Utilising as small an IP Address range as possible.
- b. Only advertising relevant IP addresses.
- c. Only accepting verified IP Routes when required.
- d. Utilising firewalls.
- e. Utilising NAT.
- f. Utilising Intrusion Protection Software (IPS)

It is recommended that external security advice is sought.

Agenda Item 4

01-03/02/23

2.2 The System Design Document (SDD) states:

ACL will be applied allowing only registered LAN IP ranges to be redistributed. It is highly recommended customer to implement appropriate security measures in the LAN environment as well.

This means that it is possible to only use the router with an ACL to protect systems and services on the LAN.

This does provide very limited security.

2.3 If the APAC CRV OG is to mandate the use of a firewall, several factors should be considered but not limited to:

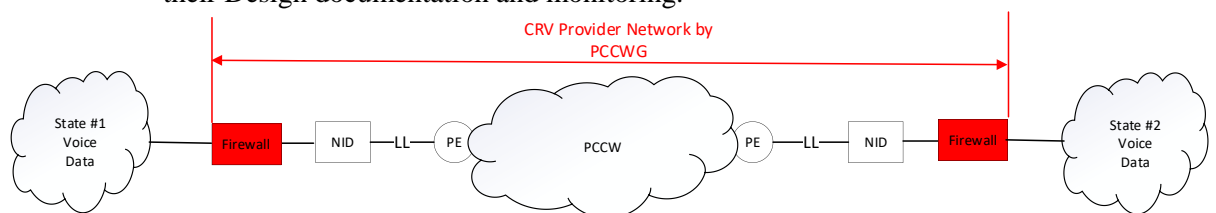
- i. Cost
- ii. Firewall type and capability
- iii. End of life announcements and lifecycle
- iv. Management of the firewall
- v. To what level are we firewalling i.e. L2-L7, blocking traffic etc.

2.4 Any ICAO documentation on Security should also be consulted such as the ICAO Aviation Trust Framework (IATF) and the Trust Framework Study Group (TFSG)

2.5 Options for mandating a firewall could be:

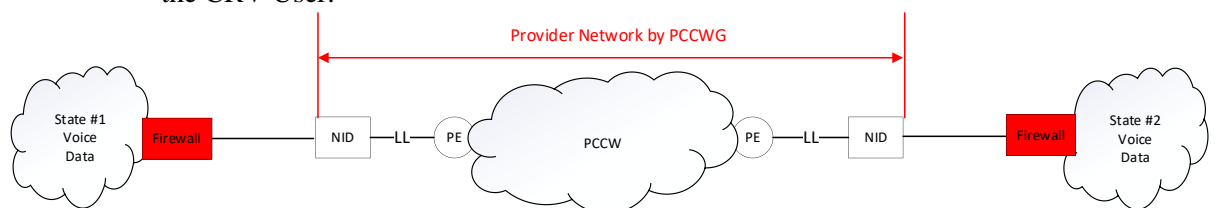
- i. Option 1 – PCCW implemented firewall

In this scenario the CRV User would pay for the implementation of a firewall at each site. This would be managed by PCCW and need to be documented into their Design documentation and monitoring.



- ii. Option 2 – CRV User implemented firewall

In this scenario the CRV user would be required to implement a specified firewall at each of their sites. The firewall would be owned and managed by the CRV User.



- iii. Option 3 – Update INFOSEC Policy

This scenario the INFOSEC Policy, Process and Procedure section would be updated to provide both improved expectations and guidance on the INFOSEC requirements for connecting to the CRV.

It also takes into account the existing security implementations that States may have already implemented.

This could include but not limited to:

- a. Common Criteria EAL or NIAP tested firewall
- b. Intrusion - Detection or Protection
- c. Use of NAT
- d. Recommendations from the IATF and/or TFSG.
- e. Use of IPSEC between states
- f. Use of Public IP addressing between the State and the PCCWG networks.

2.6 It may be prudent to base the decision on firewalling on the outcomes of the Safety Review.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

- a) note the information contained in this paper; and
- b) discuss any relevant matter as appropriate
