CRV & SWIM WS– **WP/06**
Agenda Item 3
17-19/09/24

International Civil Aviation Organization

Workshop and One Day PSIDS meeting for preparation of new-CRV requirements and specifications for future SWIM/other aviation services
Guam, USA, 17-20 September 2024

Agenda Item 3: New CRV Technical Specifications including SWIM requirements.

POSSIBLE CRV ARCHITECTURE

(Presented by New Zealand)

SUMMARY

This paper presents potential architecture options for the CRV network.

1. INTRODUCTION

1.1 When the Common aeRonautical Virtual Private Network (CRV) was established, it was done to replace the legacy point to point telecommunication circuits and support AFTN/AMHS and Voice across Asia Pacific (APAC).

The discussion for the network started in 2013 and there have technology and application changes since then that the network had not considered.

2. DISCUSSION

2.1 Future Architecture

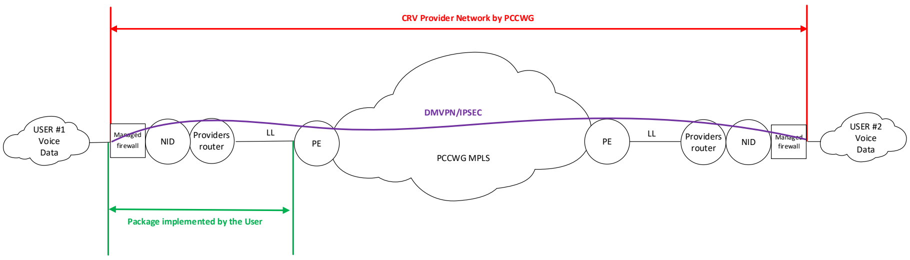
The following discussion describes potential architecture for the CRV taking into account some of the requirements for current and new applications, as well as details provided by other network groups such as PENs and REDDIG.

These are not exhaustive and the current CONOPS and Requirements will need to be reviewed to ensure any changes or risks are managed or mitigated.

Implementation of a managed firewall, no GRE tunnels.

In this option a managed firewall is provided by the service provide. All NIDs and traffic would be visible to each NID. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection as well options for threat detection, antivirus and IPSEC VPNs.

PCCWG has indicated that the managed firewall option they currently offer does not extend into the Private Network architecture that CRV is built on and is only available on internet based connections. There would be a development cost to provide a Private Network based managed firewall.

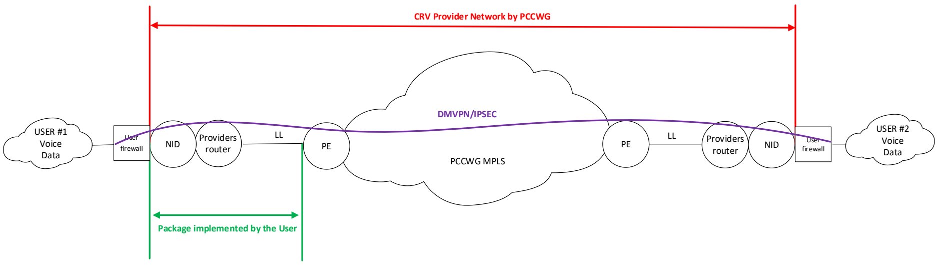


User provided firewall, Service Provider WAN.

Two options exist under this scenario.

Option 1 – non specified firewall.
In this option a is firewall mandated to connect to the CRV and is provided by each user. The type of firewall is not specified. All NIDs and traffic would be visible to each NID across the Service Providers WAN. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection and could provide options for threat detection, antivirus and IPSEC VPNs.
Management of the firewall would be retained by each user.

Option 2 – OG specified firewall.
In this option a is firewall mandated to connect to the CRV and is provided by each user. The type of firewall is specified. All NIDs and traffic would be visible to each NID across the Service Providers WAN. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection and could provide options for threat detection, antivirus and IPSEC VPNs.
Management of the firewall could be retained by each user or could be centralized.

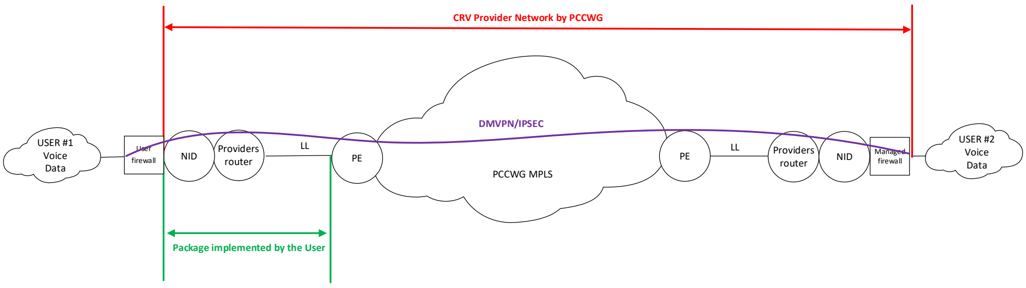


User firewall, Managed firewall, Service Provider WAN.

Option 1 – non specified firewall.
In this option a firewall is mandated to connect to the CRV and is provided by the user if they have the capability to provide and manage a firewall, otherwise the firewall is provided and managed by the Service Provider. The type of firewall is not specified. All NIDs and traffic would be visible to each NID across the Service Providers WAN. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection and could provide options for threat detection, antivirus and IPSEC VPNs.

Management of the firewall would be retained by each user, where that user has provided the firewall, otherwise the firewall is managed by the Service Provider.

Option 2 – OG specified firewall.
In this option a firewall is mandated to connect to the CRV and is provided by the user if they have the capability to provide and manage a firewall, otherwise the firewall is provided and managed by the Service Provider. The type of firewall is specified. All NIDs and traffic would be visible to each NID across the Service Providers WAN. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection and could provide options for threat detection, antivirus and IPSEC VPNs.
Management of the firewall would be retained by each user, where that user has provided the firewall, otherwise the firewall is managed by the Service Provider.



User firewall, Internet based WAN

This solution would provide the most flexibility for the least cost but would require being supported and managed solely within the CRV OG users. There would be no single Service Provider involved.
More consideration is required to the support model for this.

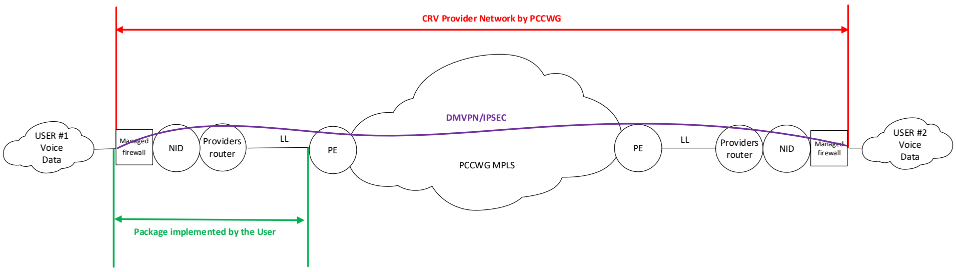
Two options for the firewall and two options for the WAN exist under this scenario.

WAN Option 1
In this option the WAN is provided by each user, using business grade internet connections where possible. The router used to connect to the internet would not be specified.

WAN Option 2
In this option the WAN is provided by each user, using business grade internet connections where possible. The router used to connect to the internet is specified.

Firewall Option 1 – non specified firewall.
In this option a is firewall mandated to connect to the CRV and is provided by each user. The type of firewall is not specified. All NIDs/Routers and traffic would need to be constrained in VPNs so as not to be visible to the wider internet. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection and could provide options for threat detection, antivirus and IPSEC VPNs.
Management of the firewall could be retained by each user or could be centralized.

Firewall Option 2 – OG specified firewall.
In this option a is firewall mandated to connect to the CRV and is provided by each user. The type of firewall is specified. All NIDs/Routers and traffic would need to be constrained in VPNs so as not to be visible to the wider internet. ACLs on the router would provide a first layer of control or protection. The firewall will provide an additional layer of protection and could provide options for threat detection, antivirus and IPSEC VPNs.
Management of the firewall could be retained by each user or could be centralized.



<u>Tunnel or VPN.</u>

The current architecture provides for multiple GRE tunnels across the network to facilitate connectivity. Multiple QoS queues are required to keep traffic separated.

Multiple GRE tunnels could be created to manage specific applications or connections.

An alternative to running multiple tunnels is to implement multiple VPNs. This could account for the test and development requirements, but routers and firewalls have limits on the number of VPNs supported.

QoS will still be required as it is applied to the WAN and not the VPN.

2.2 Conclusion
Whilst there are options available the CRV architecture, the following will need to be considered:

1. Cost
The implementation of either managed or unmanaged, specified or not specified firewalls has a cost implication. Where the cost of purchasing a firewall by a user is borne by that user, it can be capitalized.
Using the internet as the WAN would significantly reduce the cost of the network.

Item	**Service Provider Managed Cost**	**User cost**
Managed NID (Monthly)	USD918	USD100
Package C (Monthly)	USD3181	USD0
Package D (Monthly)	USD1819	USD0
Supplied Internet (Monthly)	USD75 - USD1000	USD75 - USD1000
Firewall (Annual)	USD0	USD1200

2. Availability
   Whilst the internet is a cheaper option for the provision of the network, the availability metrics would/could change.

3. Supportability.
   Several options rely on the user to implement specific router and/or firewalls. Without a Service Provider, how would we manage the network?

4. Requirements.
   The requirements issued as part of the tender will need to be review to ensure they are still valid or require changing.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) discuss proposed options and way forward; and

c) discuss any relevant matter as appropriate

– – – – – – – – – – – – –