Simplifying Security, SDN, and Hybrid Cloud Structures with iQuila

Mathew Raio III

Adjunct Professor ~ Network Essentials/Senior Network Administrator

Author of "Getting Started Guide to GNS3 1.0"

Sponsor: David Sweet ~ CEO of iQuila

Author Note:

A student in the Information Security Operations Masters program.

Matt.raio@mymail.champlain.edu

Executive Summary

There are very few products that solve multiple situations as much as iQuila. With the expansion of cloud deployments, the increasing number of security vulnerabilities, and the amount of specialization to architect and administer these new structures, iQuila has positioned itself initially to answer security for remote workers during a time of COVID. The author's experience with other platforms like GNS3 gave iQuila a paradigm shift into becoming a central strategic asset in building not only remote worker access to local resources, but scaling this solution between virtual data centers and intertwining these elevated virtual networks together to form an independent cloud solution using iQuila as a sort of back end 'fabric' interconnecting disparate locations. This simplified technology cannot be overstated. With this white paper, we will bring awareness to this latest technology, a high over view of how it works, and the author's love of experimenting with this technology to assist local, state and government agencies to leverage the structures they have already invested in to create a higher level of networking the author calls the 'mezzanine network'.

The scope of this paper will contain the following sections. Section 1 covers a high level overview of where the iQuila SDN software sits in the famous depreciated OSI model. The second section covers a real world example of an anonymous university in the United States that has been experimenting for several months at the time of this paper. The third section explores concepts this author is going to prototype and experiment with in upcoming papers. The fourth section are the contacts for iQuila should you choose to try these concepts for your own government, state and or

local institution. Of course, the author would prefer you to wait until these concepts are fully vetted out in subsequent white papers, but if you wish to immediately dive in and build your own ‘mezzanine network’ and co-locate virtual networks across multiple data centers; then just mention “MEZZANINE” in the subject of your e-mail and send it to matt.raio@gmail.com.

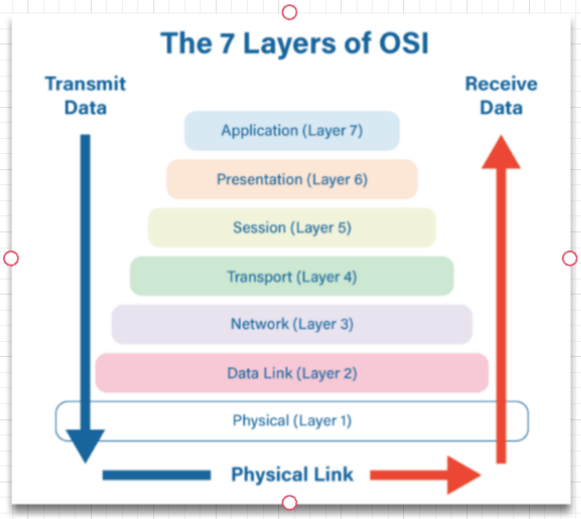
Section 1 ~ High Level Overview of iQuila SDN

Since the author’s time with GNS3 (circa 2016), the author went on to work for a large telecommunications company in Denver for a little over 2 years. The love of experimenting and exploring new concepts in that Fortune 300 was too limiting. Instead, the author took up a position as a senior network administrator at a community college in the United States. This move freed up his ability to integrate virtual networks on top of existing network structures.

There are natural progressive issues with the current infrastructure that gave the author opportunities to improve on it. The overall decision was to build a hybrid cloud structure. How that structure is going to end up looking is very fluid, yet conforms to the overall hybrid design. iQuila came at a time after the author has already designed and started implementing a segmented network based on current ‘level 3’ concepts. With this new piece of technology, the author realizes the network capabilities are far more than what was initially stated. It’s for this reason, the author feels a greater awareness of this product enables existing networks to gain added benefits in contrast to over paying for more virtual networks and services. Initially iQuila shows the product as a means to increase security and improve performance for remote workers.

The following section gives a high level understanding of how this is possible in comparison to a standard OSI model:

Figure 1
Traditional OSI Model



Note: By Bouchard(2020) illustration showing the basic levels of the OSI

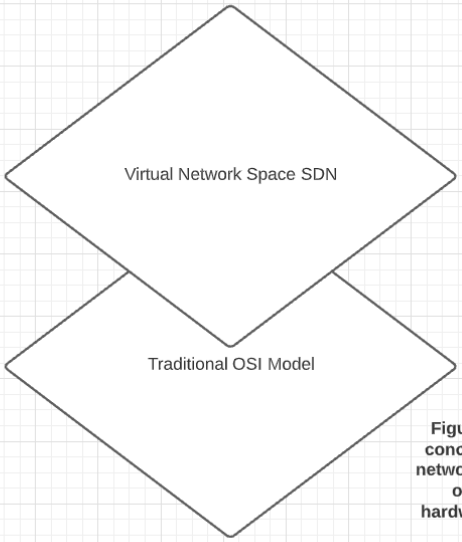


Figure 2: Abstract concept of a virtual network space on top of traditional hardware support of the OS.

With the depreciated seven layer OSI model as a reference, we can see that SDN covers quite a few levels. Starting from the application and presentation layer, the iQuila software now carves out the Session layer, the Transport layer, the Network layer and the Data Link layer.

Without going too technical into the layers that iQuila handles; suffice it to say right now that ‘under the hood’, iQuila utilizes a special A.I. module to handle transport segmentation as well as a proprietary VEN protocol between end points. The entire layer 2 segment is encrypted with their own security protocols which makes iQuila very attractive from a security and support perspective.

With respects to security, this proprietary algorithm allows for a very confined and isolated deployment of secret cryptography that is not known ‘in the wild’. Whereas other very large Cloud Service Providers break from current IEEE standards such as Google’s QUIC or Amazon’s Sidewalk devices as an example; this technology is not open source. Consequently, in addition to buying functionality, you also pay for specialized security for all your layer 2 traffic.

Some of the immediate concerns with using proprietary security is the basic question of how effective is it? Since iQuila is better known in the U.K., the author chose to ‘vet’ out the security aspects of this connection and run a series of tests. Later in the white paper, the author will ‘road map’ out the layers of testing for those who wish to experiment with us here in the U.S.

Section 1:2 ~ The ‘mezzanine’ concept.

Realistically, the OSI is meant to only frame our discussion of how impactful SDN can be. When meditating on the ramifications of this solution, the author considered the concept akin to a mezzanine in architecture.

Figure 2

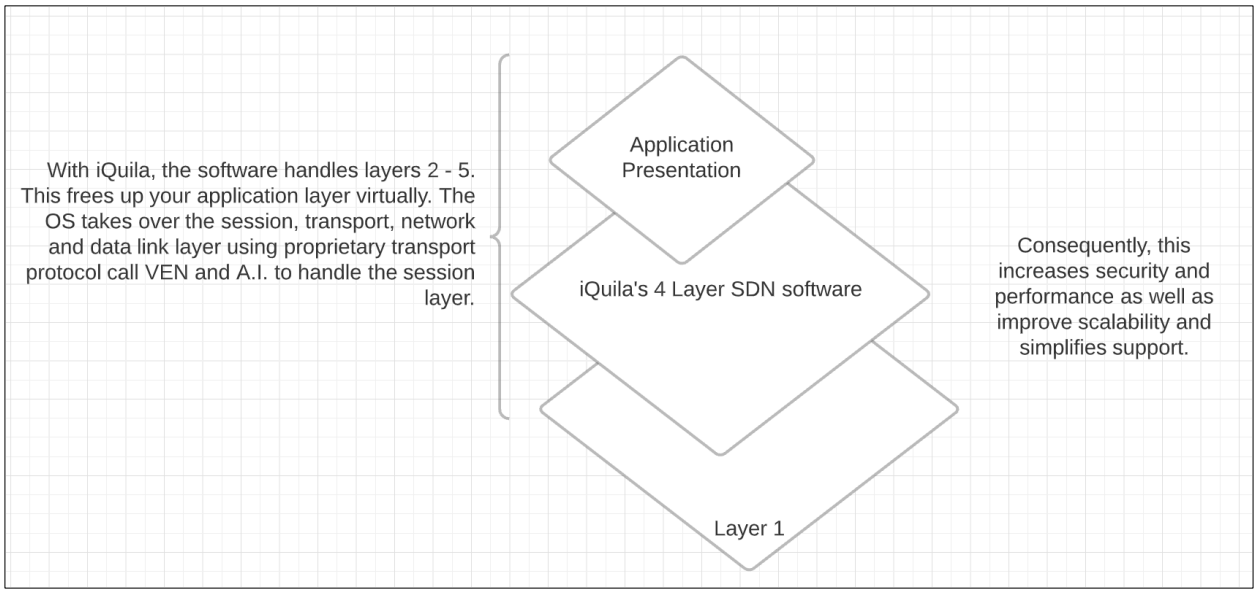
Mezzanine example

The mezzanine concept is to allow a ‘stacking’ of a virtualized network on top of an existing physical one. This concept of using SDN with iQuila, allows a state agency or institution to offer ‘virtualized data-centers’ to each other; offsetting costs for co-location purposes.

Note: Photograph by Panel-Built(*Mezzanine Gallery*, n.d.)

The mezzanine network is born with an understanding that now iQuila will handle those layers in a secure, efficient manner; leveraging their proprietary A.I. as shown below:

Figure 3: iQuila takes over 4 levels of the OSI model.



Now with the modified iQuila OSI model, we can discuss current uses in section 2 and plans for expansion in section 3.

Section 2 ~ Current uses for iQuila

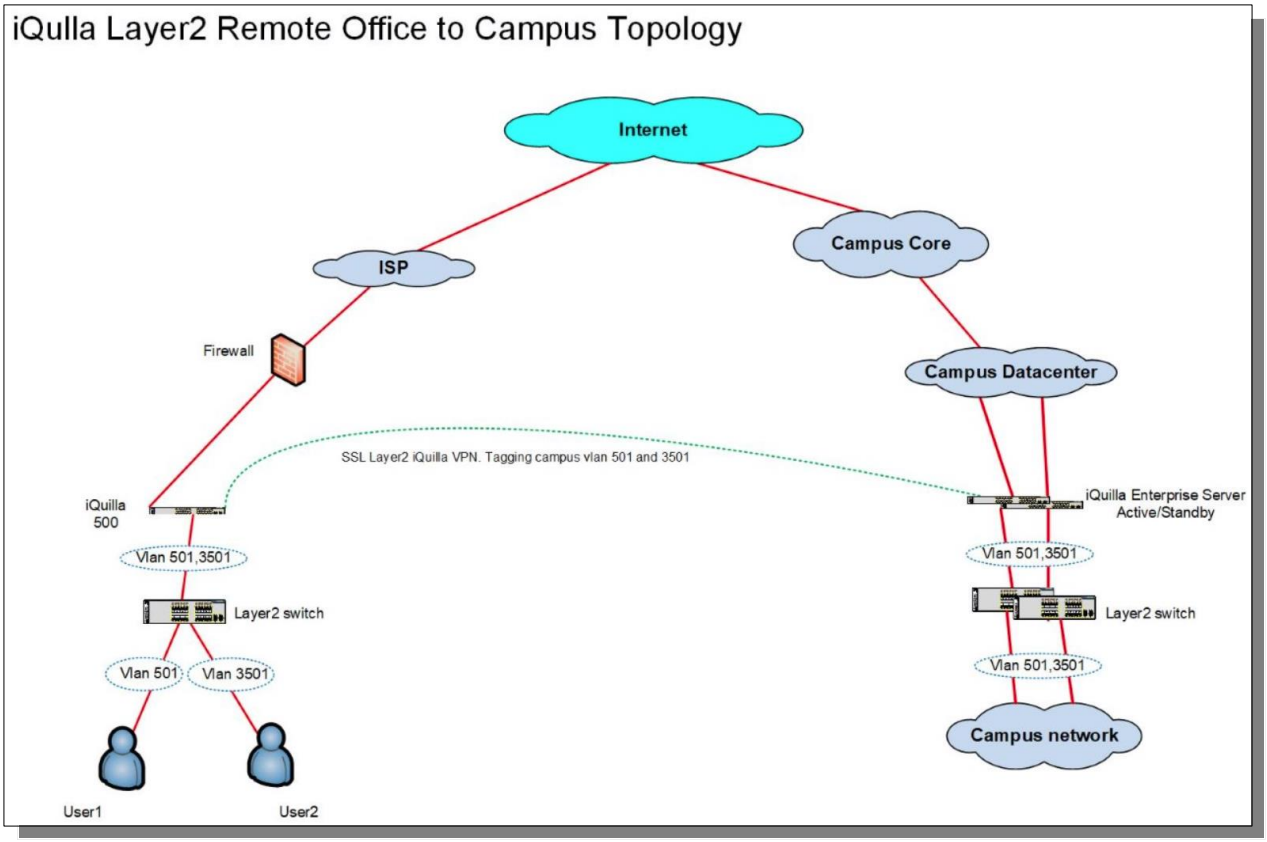
Due to legal reasons, the author was unable to obtain the permission of the university in question over it's tests of the iQuila application. If you are part of a local, state, or government entity, and you wish to be featured in future white papers, please send me your contact information to matt.raio@gmail.com

The university in this white paper will only be mentioned as "University A". The engineer at that university will be referred to as "Jim". Jim had a need to expand his current network due to COVID concerns and was interested in iQuila for its claims of efficiency and security. After interviewing him for a few minutes, we agreed that his analysis showed that

iQuila was able to perform a complete fail over from his location to the virtual test server at the university.

He stated that he was able to perform the active/standby configurations of two servers and was able to see full connectivity after the loss of two pings. Please see illustration below:

Fig.



Note: Jim's logical design showing iQuila's ability to create layer 2 connections as if they are on the same campus.("Working Failover Concept IQuila," n.d.)

Unfortunately, we cannot discuss the locations of these two servers. What we can state is that both servers were not on the same physical network in two different locations. iQuila was able to establish a layer 2 connection to allow the fail over to happen at a much lower level than conventional knowledge of layer 3 networks.

I explained the implications of a layer 2 network is just as valuable from a network fundamental standpoint as the security itself. Iquila is in the figurative ‘cross-hairs’ of a number of areas to disrupt. This author was admittedly too glad to ‘pull this trigger’ and be the touchstone of changing the SDN and cloud conversations. Obtaining a verbal agreement from Jim allowed me to trust the seven months of testing prior to my involvement and gave me confidence I can now expand the role of iQuila to be at the forefront of a decentralized Government/Military Cloud Fraternity (G/MCF) using the mezzanine networking concept.

Section 3 ~ Concepts Worthy of Exploration

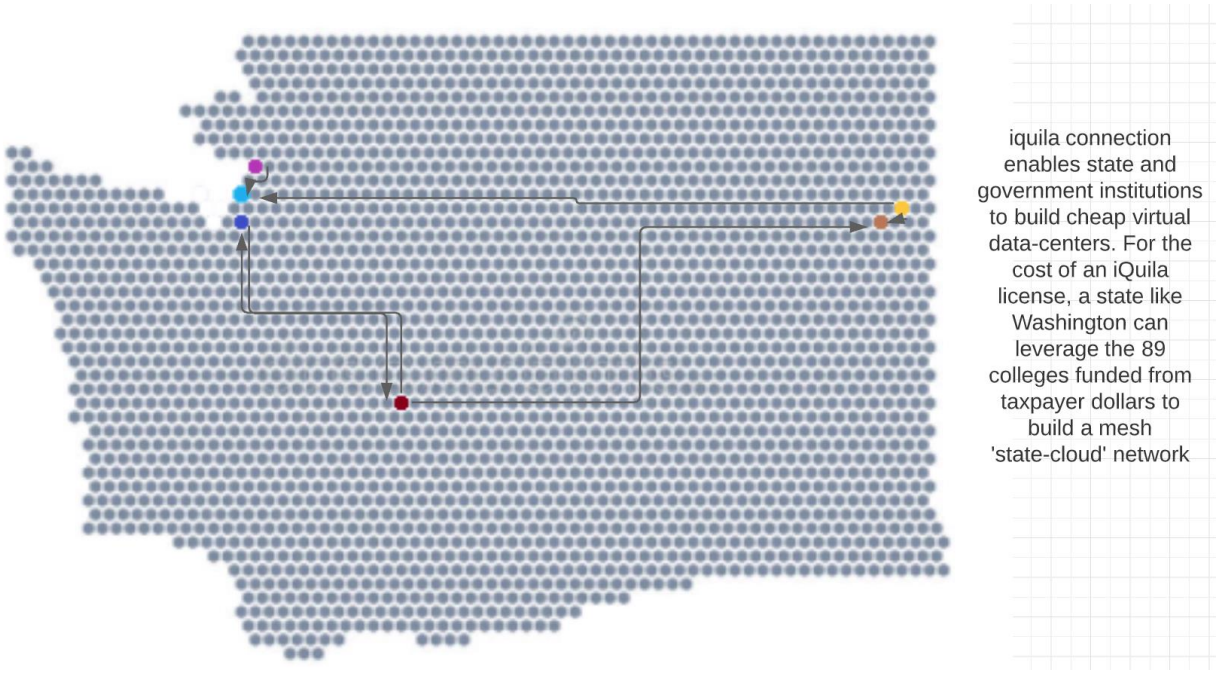
From an academic standpoint, freedoms should be allowed to students willing to break conventional wisdom and glean new understandings of our modern world. This explains that truly this is a white paper, but as a student and teacher of network essentials; since the days of GNS3, the author loves collaborating with all sorts of people across the globe. Becoming ‘the World Teacher’ is a tremendous gift and responsibility that is taken with all seriousness.

The white paper in itself allows a large collection of collaborators to be included in this new scalable experimentation. This section is an overview of concepts we build upon from the previous two sections.

Section 3.1 ~ A ‘federation’ of mezzanine networks.

Now that we have spent time on a new novel concept, let’s look at how that would shape data centers for various state and federal agencies. In this example, the author works as a senior network administrator for a college in Washington State. A simple Google search would reveal that there are 89 colleges in the State of Washington. By using a simple hexagonal map, the

following illustration shows a very small sampling of existing colleges and their relative locations to each other:



Assuming iQuila is secure and efficient as propounded by Jim, we can now build a mezzanine network in College B (the college I work at), with ‘neighbor’ colleges in Washington. If each one of them connected to the mezzanine network the author built, then file sharing and authentication can happen in a virtualized cloud solution that is manned by each IT team, but together controlled in what I only liken to as a ‘fraternity of colleges’ herein referred to as the first fraternity of mezzanine networks.

The simple premise is this: For the money spent on individual cloud solutions with AWS, Azure and GCP, why not create virtual data centers in each location since they already exist?

What most technical people forget is the accounting aspect of purchasing new assets. If College B built a virtualized data-center and offered an invitation to the other 88 colleges in Washington to have some of their domain servers 'hosted', then college "B" could do the same and both structures offset the cost to build with the savings of purchasing a new co-location.

A convergence in cost would 'shrink' to the point that a hybrid cloud between the on-prem, the individual cloud accounts and now the fraternity would exist; thereby offsetting co-location costs for both colleges. The savings would increase across all 89 colleges in Washington State.

The 'mezzanine' concepts using iQuila facilitates that ability while at the same time, not crossing into existing networks; which is what SDN promises. The other thing to note about SDN, is the term and the technology is still very vendor-centric. To achieve this level of SDN, considerable expense is given to building the virtual structure in other frameworks such as VMWare and Cisco. This too would disrupt their business model. To say nothing that the State of Washington would have their own cloud solution independent of the big three CSP!

Section 3.2 ~ Current road map to get to 'fraternities of mezzanine networks'.

The logical structure for completely vetting out these concepts have a logical format. Future white papers will discus the following levels:

Level 1 ~ Test the validity of iQuila's product between two server endpoints within College B's new virtual networks.

Level 2 ~ Integrate this connection with another College (herein referred to as College C).

Level 3 ~ Test iQuila's cloud product.

Level 4 ~ Integrate 5 more colleges / universities into the first “fraternita primaria”

Level 5 ~ Move existing images off of AWS / GCP / Azure into Fraternita Primaria

Level 6 ~ Advanced virtualized network mezzanines inside emulated networks (GNS3, EVE-ng).

Section 4 ~ Contacting iQuila

Currently, THERE IS NO ONE THAT SELLS iQuila in the U.S. I happen to understand and bridge the solution and will gladly forward your interest to them. If you wish to work with them directly, please mention this white paper. Since you have read this white paper in it’s entirety, feel free to mention “fraternita primaria” in the subject of your e-mail and send it to David.Sweet@iquila.com

Special Thanks!

I wish to thank David Sweet, the iQuila Team, Jim, the colleges, my employers (past and present) for this wonderful opportunity to help iQuila and all entities in the U.S. I look forward to writing more white papers and building upon this new SDN network. Thank you for reading!

References

Bouchard, G. (2020, April 30). The 7 Layers of OSI [Illustration]. OSI 7 Layers Explained the Easy Way. https://insights.profitap.com/osi-7-layers-explained-the-easy-way

Mezzanine Gallery. (n.d.). [Photograph]. Mezzanine Gallery Images. https://www.panelbuilt.com/mezzanine-gallery-images/nggallery/page/1

Working Failover Concept iQuila. (n.d.). [Illustration]. In *Working Failover Concept iQuila*.