# FUEL VIRTUAL TEST LAB OVERVIEW

The purpose of the Fuel Virtual Test Lab (vLab) is to provide a lab environment for the Fuel user community to experiment and explore different features and use cases for Palo Alto Networks product. Participation in the vLab should also encourage members of the Fuel user community to share and learn from each other through a common lab environment.

## USING THE FUEL USER GROUP VIRTUAL TEST LAB

In order to access the Virtual Test Lab, you will need to request access from Fuel HQ. Fuel members can request access here. Not a Fuel Member? Join today.

Prior to requesting access, you may want to ensure that your system is optimized to work with the CloudShare environment. Visit http://use.cloudshare.test.mvc to check your connectivity and settings.

Requests for access to the Virtual Test Lab are fulfilled within every Wednesday. Once confirmed, you will receive an email that contains your personal link to the CloudShare hosting environment. You must activate this access within 30 days of receiving your confirmation. Once you access the CloudShare, you will set up a personal login to use for the Lab.

## YOUR VIRTUAL TEST LAB ACCESS

Once you enter the Virtual Test Lab (Figure 1), you will see a button that says “Start Using This Environment”. Clicking on this button or any of the top navigation tabs will activate your session, which lasts **4 hours from the time you start using the lab**, and is continuous; access may not be spread across several sessions and will not stop if you leave the lab. ***If you leave the lab, your remaining time in the lab will not be saved.*** Please make sure you have reserved enough available time in your schedule to fully utilize your session.

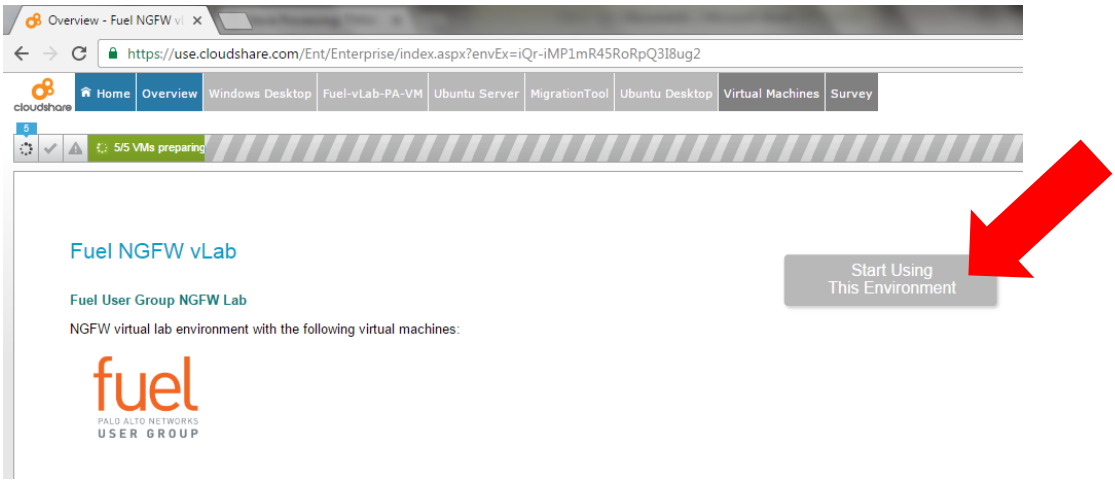


*Figure 1 – Accessing the Virtual Lab*

A few tips and reminders about the vLab:

- Your vLab environment is deleted once your allocated lab time is completed, we do not keep any changes or configuration you make in the vLab.
- You can upload the firewall configuration changes you made in the lab if you want to keep them.
- Please be mindful of what you do in the lab, your activity may be monitored.

## LAB ENVIRONMENT AND VIRTUAL MACHINE DESCRIPTIONS

On the Home page of the vLab, you will find a topology map of the environment (Figure 2), as well as all of the logins for the different VMs and desktops. These logins should be automatically entered for the main VMs, but you may need to enter them for any browser or application.

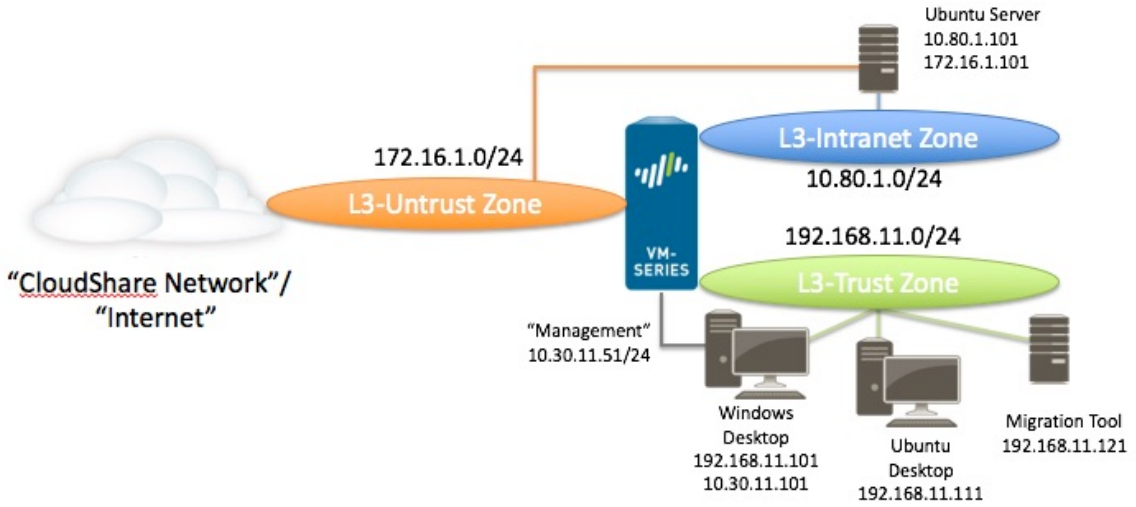


*Figure 2 – vLab Environment*

There are five virtual machines (VMs) in the Next Generation Firewall (NGFW) virtual lab environment. The information about the operating systems, roles, and applications installed on the respective virtual machine are listed below. Note that you have full administrator or super-user access right to add/change applications or services on these VMs. If you install any commercial software in this lab environment, please ensure you have proper license to use the software before installing it on the VMs.

## WINDOW DESKTOP - WINDOW SERVER 2008

**You should start from this VM.** This is the main VM that you will use to manage the firewall and access other VMs. This VM is connected to the Trusted zone on the VM-Series firewall. There is a secondary interface that connects to the management interface on the Virtual firewall. All the traffic, except the management traffic, from this VM goes through the VM-Series firewall so you can configure the firewall and validate any policy changes. This VM is connected to the Internet through the VM-Series firewall and can be used to connect to other VMs in this lab environment. Wireshark and putty are installed for testing and troubleshoot purposes.

- Management Int: 10.30.11.101/24
- L3-Trust Int: 192.168.11.101/24
- Default Gateway: 192.168.11.1
- All traffic is sent on L3-Trust Interface, with the exception of management traffic
- Login: administrator / (dynamic)

## VM-SERIES VIRTUAL FIREWALL

The VM-Series firewall runs PAN-OS 6.1, it is installed in front of VM-01 and VM-02 and have full visibility into any traffic to and from these VMs. This VM-Series firewall has valid licenses for all the PAN-OS subscription services for testing.

- Management Int : 10.30.11.51
- Ethernet1/1 – L3-Untrust – 172.16.1.1/24 (**Down by default**, needs to be enabled before the other VMs can reach the internet.)
- Ethernet1/2 – L3-Trust – 192.16.11.1/24
- Ethernet1/3 – L3-Intranet – 10.80.1.1/24
- Virtual Firewall login: fuel / fuel
- Default gateway on L3-Untrust zone: 172.16.1.254

## UBUNTU DESKTOP - UBUNTU DESKTOP

This is a basic Ubuntu desktop, connected to the Trusted zone on the VM-Series firewall. This VM allows users who want to use software and features commonly available on standard Linux distro. This VM is connected to the Internet through the VM-Series firewall and can be used to connect to other VMs in this lab environment.

- L3-Trust Int: 192.168.11.111/24
- Default Gateway: 192.168.11.1
- Login: fuel / fuel
- Login: sysadmin / (dynamic)

## UBUNTU SERVER - UBUNTU SERVER

This is a basic Ubuntu server connected to the “Intranet” zone on the VM-Series firewall. Service available on this server includes, HTTP, HTTPS, FTP, SSH, MySQL by default. This VM can be used as the server to validate policies on VM-Series firewall while VM-01 or VM-02 act as the clients. This VM is configured to connect to the Internet on the L3-Untrust zone and you can install other services for testing if needed. There is another interface, on the L3-Intranet zone, you can test the services on this zone by creating the appropriate firewall policies.

- L3-Untrust : eth0 – 172.16.1.101
- L3-Intranet: eth1 – 10.80.1.101
- Login: fuel / fuel
- Login: sysadmin / (dynamic – see Connection)
- Services:
  - SSH, LAMP
  - MySQL: root / utd135

## MIGRATION TOOL

This is the Migration Tool developed by Palo Alto Networks. It makes the best effort to convert selected 3rd party firewall configuration files to a PAN-OS 8.0 configuration file. This migration tool is developed in a virtual appliance where it is supported on most VM-Ware hypervisors. The Web UI of this tool is accessible from the VM01 Windows Desktop, bookmarked in the Chrome browser.

- Trust Int: 192.168.11.121/24
- Login: admin / paloalto

## LAB ACTIVITIES

There are no pre-set workshops or test drives within the vLab; this is an open learning environment. You may choose to use this as a dev environment and import your own policies, or to test out new configurations.

Some of the things that you can try to do in this virtual lab environment include:

1) Test application visibility on the VM-Series
    - Create application policy to allow specific applications and turn on logging
    - Initiate traffic between VMs to generate some traffic and review the logs and see what applications are used
2) Test the various security profile
    - Create different security profiles, try different actions and options
    - Explore the various options in the security profiles
3) Enable WildFire and review the WildFire report
    - Enable WildFire in the policy
    - Use the Wildfire test file or other file to test WildFire analysis results
    - Review the “WildFire Submissions” logs for WildFire analysis
4) Decrypt SSL traffic
    - Create decryption policy to decrypt traffic from specific websites
    - Create decryption policy based on various decryption profile options
5) Use API interface
    - Use API interface to review specific firewall configuration
    - Use API interface to change the configuration
6) Create custom application signature
    - Create a custom application signature
    - Validate that custom signature using various policies
7) Enable captive portal to try User-ID policy
    - Create captive portal to enforce user login
    - Create policy to enable application base on user-id
8) Setup DoS protection policy
    - Create aggregate or classified DoS protection policy
    - Apply DoS protection policy to specific interface for validation
9) Migration tools
    - Use the migration tool to convert 3rd party firewall configuration file to PAN-OS configuration
    - Extract selected configuration and apply it to the VM-Series firewall
    - Try to implement application base policy
10) Enable GlobalProtect
    - Setup and enable GlobalProtect portal and gateway function
    - Try to connect to GlobalProtect gateway from outside of the virtual lab.

If you do not have specific issues or scenarios you need to address in this environment, and would like ideas on potential lab activities, please reference the Palo Alto Networks administrator guides, which contain workflows for sample migrations, implementing App-ID and User-ID, and optimization projects.

- Palo Alto Networks Administrator Guide (7.0) - https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os
- Migration Tool Guide - https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/MigrationTool-3-3-Info-and-Guide/ta-p/72559?attachment-id=3854

## EXAMPLE SCREENSHOTS FROM INSIDE THE VLAB

Here are just a few example screenshots to give you a sense of the options inside the vLab.

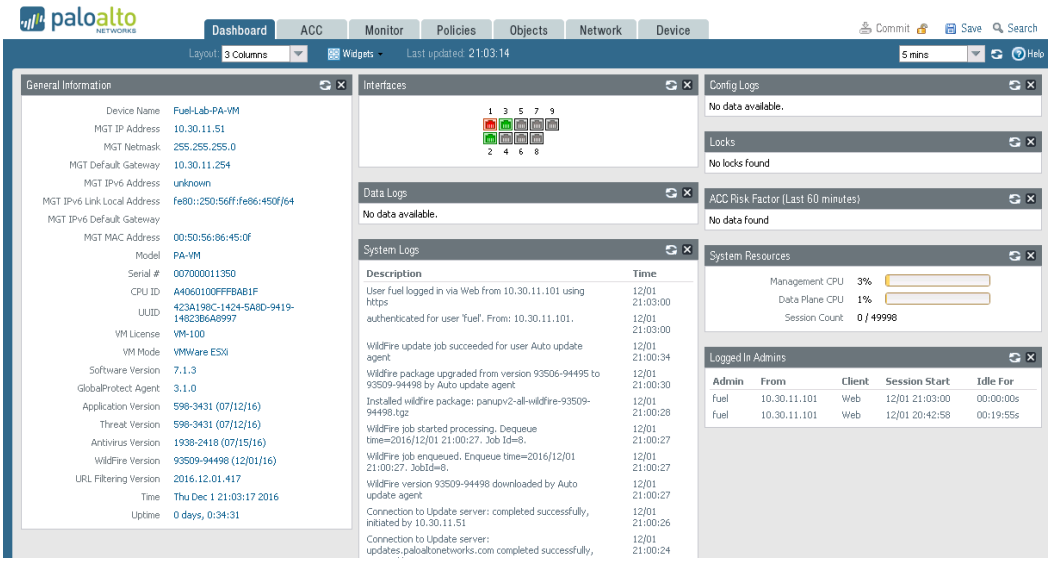


*Figure 3 – VM-Series Firewall Dashboard*

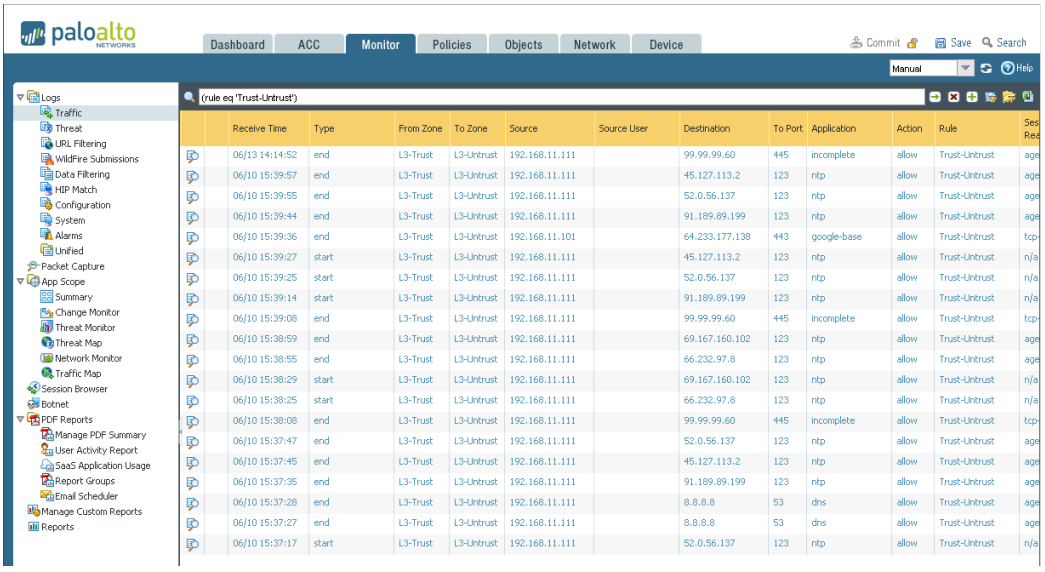


*Figure 4- Monitoring, Reporting and Logs*

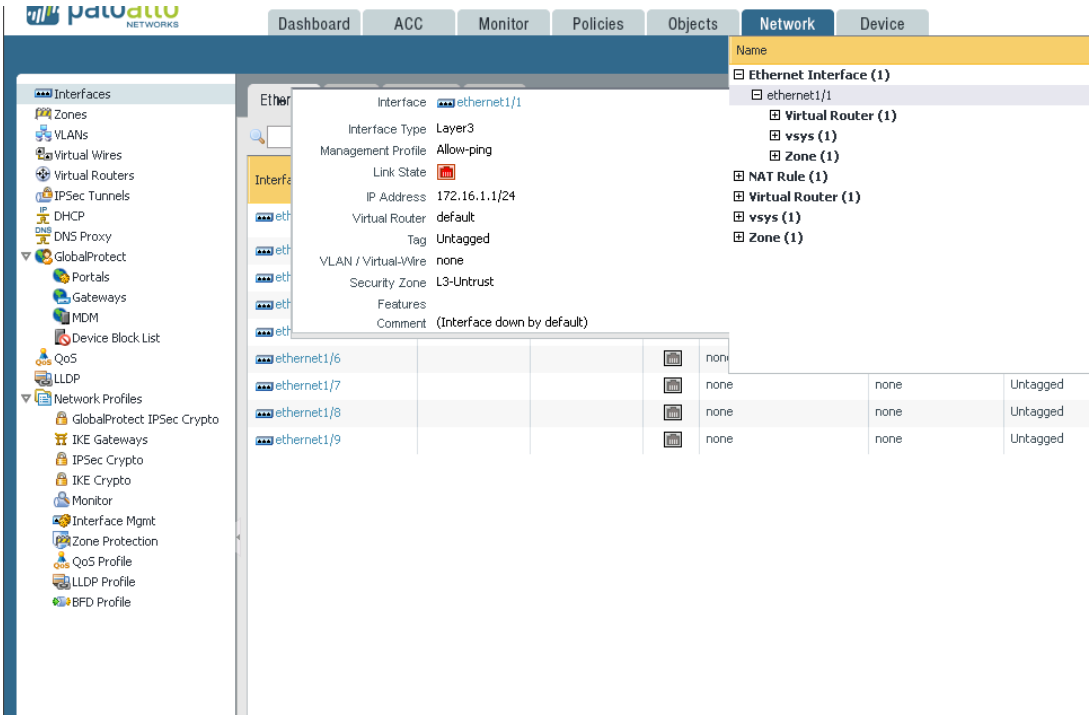


*Figure 5 – Network > Interfaces View*

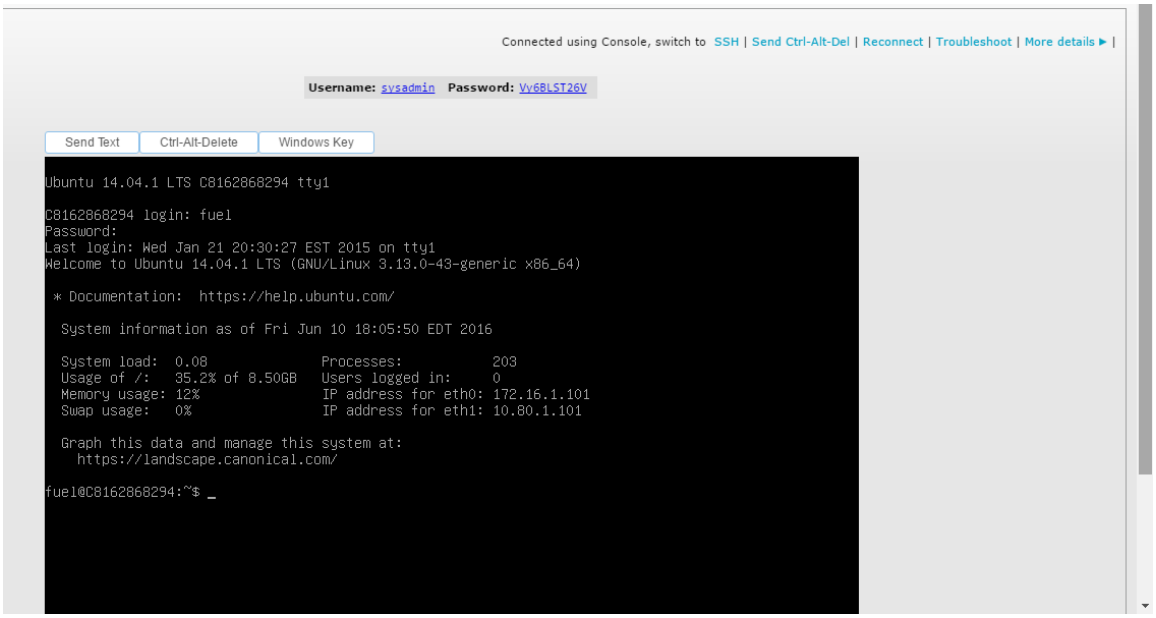


*Figure 6– Ubuntu Server View Console*

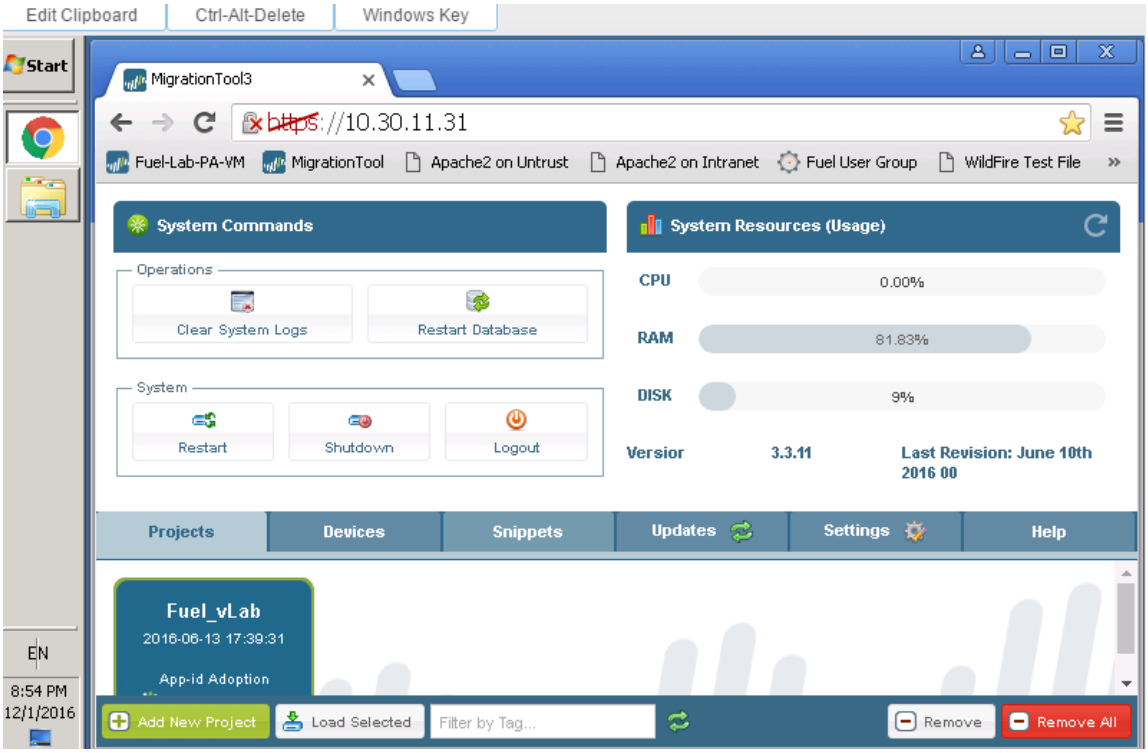


*Figure 7– Migration Tool*

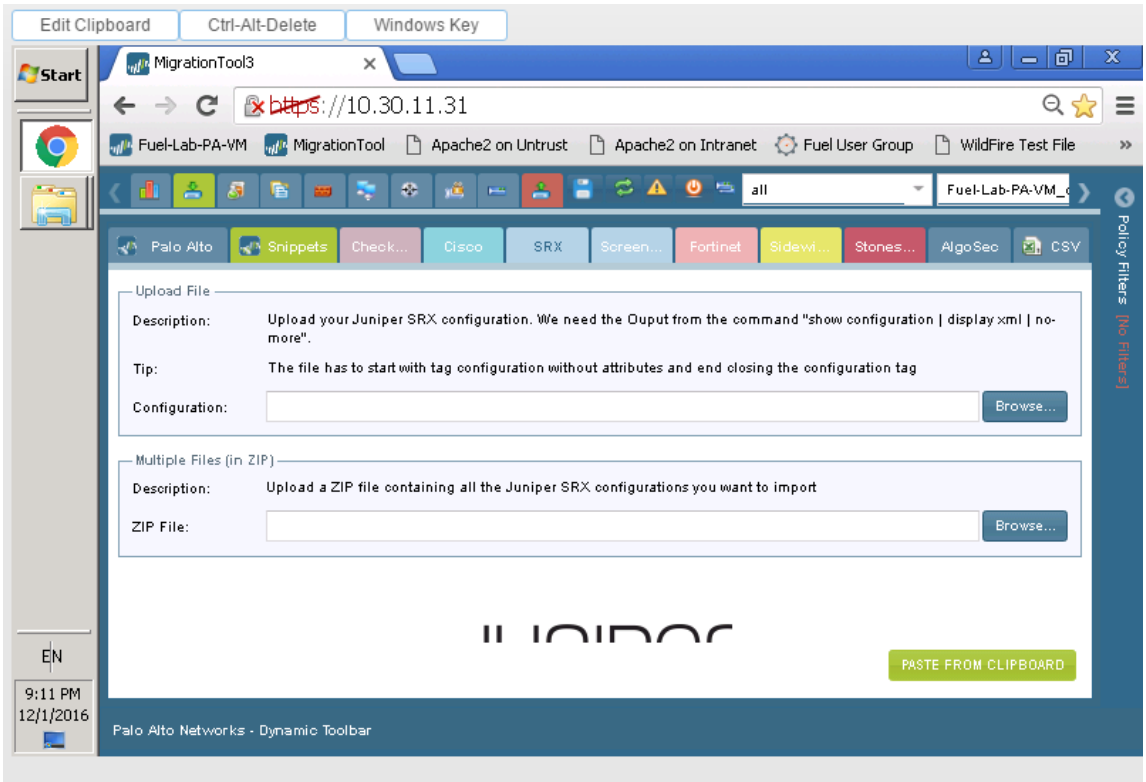


*Figure 8 – Policy Import in the Migration Tool*