Checklist Post Enforcer Installation

So you've just seen "Script Imported and Executed successfully" printed out to the terminal after running the import command on the file generated by the LucidView Portal. You may be wondering what's next? How do I begin to unpack and understand all the functionality that has been implemented on my MikroTik? We are going to refer to your Mikrotik as an Enforcer from this point, and it is important to note the following information;

Interface: lv_cloud

This is the Interface to the LucidView Cloud, and is arguably the most important technical component of the Enforcer. This VPN facilitates the Cloud informed functionality, including but not limited to: DNS Content Filtering, The Dynamic Kill List, Reports and device vitals submission to our Cloud. Please note that the lv_cloud Host destination is 1.1.1.1. This is both for DNS, as well as netflow collection.
If the lv_cloud VPN is failing to connect, please check the log for errors. A common error is that the Enforcer Profile is disabled on the LucidView Portal

Content Filtering & Kill List

The LucidView Enforcer provides a two stage content filtering solution to ensure your Content and Security Policies are Enforced.

The DNS server of the Enforcer should be set to 1.1.1.1 so the DNS requests are sent along the VPN to the LucidView Cloud so that the Content Filter policy defined on the portal can be adhered to.
If the Enforcer **IS NOT** the DNS server for the network, ensure that the firewall NAT rules for lvcloud_content_filter are active, as these rules will intercept DNS requests and redirect them to the LucidView Cloud.

In the case that DNS is circumvented, and the connection is in contravention of your Content Filter Policy, the LucidView Cloud will issue commands to add these connections to an address list called lvcloud_kill_list_external. This address list is then blocked by the firewall rule, lvcloud_kill_list_external. This process can take up to a maximum of twenty minutes to add new connections, but will remain in the kill list for up to a day.

The Intruder Protection System

The behavior based IPS functions similarly to the Content Filter in the sense that connections are monitored by the LucidView Cloud. When the IPS is enabled on the Portal, your connections are scrutinized by the LucidView Cloud to identify security risks, which in turn issues commands

to the Kill list. Connections will be classified by the IPS as a security risk when performing activities such as(but not limited to): Direct Connections(Non DNS), connectivity using an unusual port configuration and connectivity to known domains which pose a security risk.
False positives are to be expected upon the implementation of the LucidView IPS. LucidView recommends generating a “Security Risk” report from the portal, to identify which connections will be shut down by the IPS.
VoIP servers are commonly flagged by the IPS as a false positive, due to the nature of VoIP configurations. Any false positives can be added to the Exception List of that profile on the portal. Adding these as “Always Allow” entries will ensure that connectivity remains uninterrupted.

LucidView Reports

For the LucidView Reports to correctly reflect all of your data, the LucidView cloud requires both your DNS data, and the Netflow stream which continually runs from your Enforcer.
For DNS information, please see the section above.
To confirm that netflow is correctly being streamed to LucidView Cloud, check the following:
Access your MikroTik via Winbox, From the IP menu item, select “Traffic Flow”. From the status tab, there will be “Active” and “Finished” flow information. Please ensure that values are increasing under finished flows, as active flows show the current number of streams.
If these values are not increasing: from the “General” tab, untick the enabled box to disable, apply to save the change, and then re-enable and click apply and the streams should begin to flow.

LucidView Scripts and The Scheduler

LucidView utilizes the RouterOS scripting system, as well as the scheduler to facilitate the transfer of vitals, as well as the retrieval of updated instruction sets to your Enforcer.

The Scheduler will automatically run these scripts, to ensure that the required ecosystem is maintained for the Enforcer. The Scheduler jobs are:

vpn_dns_failover - every 10 seconds
-This job tests whether this Enforcer is the DNS server of the network, as well as the availability of the LucidView Cloud DNS Servers. If for whatever case that the LucidView DNS becomes unavailable, this script will disable the DNS intercept rules so that DNS requests, and therefore general internet connectivity can resume normally.

lvcloud_profiles - every 4 minutes
-This job executes multiple scripts during its execution. Firstly, lvcloud_download is run, to fetch the latest kill and shaping list instructions from the LucidView Cloud.
These files are typically split into several smaller files, which will be automatically removed.
Next, the current kill and shaping instruction set that is present on the device is submitted to the LucidView Cloud, so that issued, and current commands can be compared, and any

discrepancies repaired. Lastly, a script called lvcloud_info gathers necessary information regarding hardware vitals, device health, and profile information for submission to the LucidView Cloud.

lvcloud_open_dns_protection - every 45 minutes

This script ensures that DNS lookups are not permitted from internet facing interfaces.
This removes the risk of your Enforcer being used in a DNS amplification/DDOS Attack.

enforcer_checkin - Every hour

By performing this check in with the LucidView Cloud, your Enforcer is then able to select which LucidView Point of Presence offers the best response time, and then to switch to that point accordingly.
This script also facilitates and validates any updates to the LucidView Scripts, offered by the LucidView Cloud.
Any changes made to any of the scripts locally, will be overwritten by the check in process to ensure the integrity of the LucidView Scripts.