

Technical Disclosure Commons

Defensive Publications Series

November 08, 2018

LOCATION-AWARE NETWORKING INTENT ENFORCEMENT

AKSHYA KUMAR SINGH

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

SINGH, AKSHYA KUMAR, "LOCATION-AWARE NETWORKING INTENT ENFORCEMENT", Technical Disclosure Commons, (November 08, 2018)
https://www.tdcommons.org/dpubs_series/1634



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

LOCATION-AWARE NETWORKING INTENT ENFORCEMENT

AUTHORS:
AKSHYA KUMAR SINGH

ABSTRACT

Techniques are presented to simplify user workflow by providing a controller that allows the user to define location based intent (profiles) at one central place. Rather than requiring the user to manually dig up the device location and feed in provisioning specific to that location on each device, the controller may simplify these operations by automatically feeding the location aware rules to devices as it learns the device location. Moreover, the user can change the policy rules for a specific location at any time, and the controller can automatically push the change to devices in real time. The user does not need to worry if a device moves from one location to other location as the controller automatically provisions the devices suited for the new location. Furthermore, since the controller has network-wide view, it can simplify user workflow to enforce location based compliance/intent.

DETAILED DESCRIPTION

Automated compliance of environment and system configurations is becoming increasingly critical for large enterprise users. Many products are based on a distributed architecture and deployed by different classes of users across several geographical locations. Beside hardware, there exist virtual form factors of enterprise / service provider products which are deployed in the cloud distributed across geographical locations.

Oftentimes users want to provision policies at the network level to enforce compliance (in terms of security, protocols, access control etc.), environmental policies, and legal policies based on the location of the operating network device. That location might be based on department, state, county, country, etc. Mainly in wireless networking, and to some extent even for wired devices, the user has policies that are very dependent on the location in which the device is placed/operating.

Thus, it would be desirable to have a simple interface which can enable users to manage location based compliance seamlessly. This is not just about device configuration based on time zone or site; rather, this is more related to managing these policies at a central

location and how the device/controller ensures compliance to location based Service Level Agreements (SLAs).

As described herein, a controller may enable location aware profiles. These profiles can be very well modeled and reside on devices themselves. These profiles allows users to provision a set of rules to control the networking intent based the specific location.

There are several set of networking functions which can be optimized/customized specific to a location. Some examples include environmental, SLA, security, and set of features. Environmental settings related to power saving, different thresholds for temperature, failure conditions, etc. Oftentimes SLA depends on the location of the deployed devices, as location would defined criticality, resource reservations (usage), and performance. Security compliance is the key to success for many enterprise users. Set of features may permit automatically enabling/disabling some of the functions based on location (e.g., features relating to radio frequency, operating bands, etc.).

The location aware profiles may be used to define network service compliance through logical models. This might mean different sets of policies on different sets of devices.

These profiles may be provisioned on the controller, and as the controller discovers the devices, policies are automatically enforced. This simplifies the user workflow quite a bit.

These location aware intent based profiles may be pushed to the devices as follows. For static profiles, the provider/user may define these profiles centrally on the controller in advance and push to the devices as the controller discovers them. These profiles may be defined on devices in advance, and the device may automatically select the correct profile to inherit based on operating location.

For live location aware intent enforcement, the user may modify these profiles in real time and the controller may enforce the policies on devices in real time. This is similar to an exec command in a legacy world.

As these are location aware profiles, if a device moves from one location to another location, policies may be inherited/pushed automatically based on the new location. If a virtual services migrates to a new location, location based compliance is enforced automatically.

There is value at the controller level because the controller has a view of the network instead of the device, and it can expose a logical model to enforce location based networking intent. Depending on devices, it can build a concrete device model to enforce the policies.

Figure 1 below illustrates an example overview.

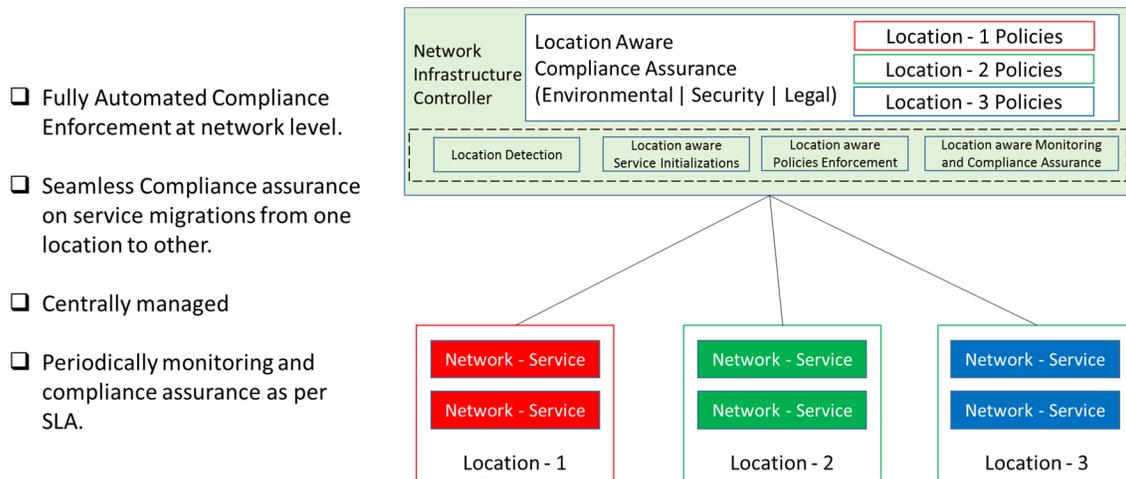


Figure 1

In summary, techniques are presented to simplify user workflow by providing a controller that allows the user to define location based intent (profiles) at one central place. Rather than requiring the user to manually dig up the device location and feed in provisioning specific to that location on each device, the controller may simplify these operations by automatically feeding the location aware rules to devices as it learns the device location. Moreover, the user can change the policy rules for a specific location at any time, and the controller can automatically push the change to devices in real time. The user does not need to worry if a device moves from one location to other location as the controller automatically provisions the devices suited for the new location. Furthermore, since the controller has network-wide view, it can simplify user workflow to enforce location based compliance/intent.