August 21, 2019

Achieving network safety by continuously limiting authorization rates

N/A

Achieving network safety by continuously limiting authorization rates

ABSTRACT

Changes in network parameters can generally be made only with authorization. However, an authorized person or workflow can quickly make large changes to the network and destabilize it. This disclosure describes techniques that account for the rate and magnitude of recent changes made by an authorized person or workflow. If preset limits to rates or magnitudes of changes are met or exceeded, authorization is declined for a certain period of time, thus ensuring continued network stability.

KEYWORDS

- Network parameters
- Rate limit
- Network safety
- Network stability
- Authorization rate
- Authorization scope
- Authorization context
- Control plane

BACKGROUND

Changes in network parameters can be made by humans or workflows with proper authorization. However, any person or entity with the necessary authorization can make unbounded amounts of change, do so very quickly, do so without regard to how much change has been made in the recent past, and do so without regard to what the authorizing person or workflow is doing. Making changes without accounting for rate, amount, breadth (scope), and context of change can destabilize and damage the network very quickly.

DESCRIPTION

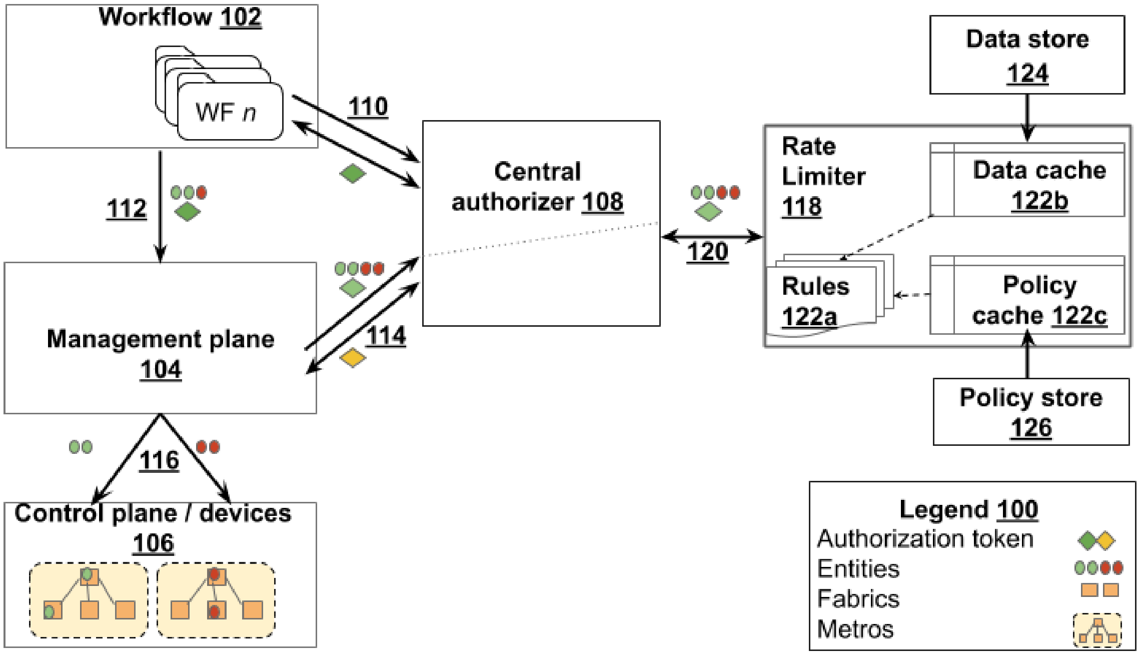

Fig. 1: Achieving network safety by continuously limiting authorization rates

Fig. 1 illustrates achieving network safety by continuous application of rate-limits to authorization requests, per techniques of this disclosure. A workflow (102) is a set of activities that achieves the tuning of network parameters. For example, workflows can be defined for turning on network devices, turning off network devices, ramping up speeds within network links, upgrading software of a device, changing device configurations, etc. Management plane (104) includes a set of tools, commands, scripts, interfaces, etc. that enables the modification of network parameters. Control plane (106) comprises ethernet metros, network fabrics, network entities, e.g., routers, modems, switches, hubs, repeaters, etc. that accept modifications to their parameters. In the legend (100) to the figure, the different colors of the entities allude to different types of entities.

Authorization tokens are used to authorize humans, workflows, or other entities or processes to make changes to the network. Authorization tokens can be chained, e.g., a first workflow (or human) can issue a first authorization token, referred to as a root token, to a second workflow (or process) which in turn can issue a second token to a third workflow. The second token can inherit a subset of properties or scope from the first token. The chaining of tokens enables a third workflow to work on behalf of the second workflow, which in turn works on behalf of the first workflow. In the figure, chained tokens are indicated by different colors, e.g., green and yellow.

A central authorizer (108) authorizes requests for network changes. For example, a workflow can make a request for authorization to the central authorizer a root token and receive it (110). The workflow in turn authorizes via token (112) a process within the management plane, specifying the entities within the control plane whose parameters are to be modified. The management plane confirms with the central authorizer the validity of the token received from the workflow (114). On the basis of the confirmatory token received from the central authorizer, the management plane modifies (116) appropriate components within the control plane. The central authorizer maintains a record of all current and past authorizations granted or rejected, and if granted, to which entity and for what purpose.

Per techniques of this disclosure, a rate limiter (118) caches policies (122b) and data (122c) relating to network changes. The central authorizer communicates (120) with the rate limiter to verify if a given request complies with policies relating to rates, magnitudes, scope, agents, and contexts of network changes. Based on network-changing policy and data, the rate limiter may apply rules (122a) to limit network changes. If certain rate limits are met or exceeded, the rate limiter can decline change authorizations for a period of time.

To perform its tasks, the rate limiter maintains a running tally of authorizations requested and granted or rejected, along with timestamps and other data relating to the authorization request. The data cache and the policy cache respectively draw data and policies from the data store (124) and the policy store (126), which are longer-term memories. Thus, the central authorizer, which has an overall measure of the health of the network, allows or disallows changes based on policy guidance issued by the rate limiter. Per the techniques, an authorization token is disabled if it is renewed (superseded) by another token.

In summary, the techniques have the following features:

- Centralized accounting of all network changes on some unit of compute/entity.
- Policy-based accounting for allowed changes, e.g., changes that are deemed operationally safe, coupled with real-time health checks from the network.
- Interface with a central authorizer to validate a request from workflows or human users.
- Policies that evolve based on current perception of network safety.

In this manner, the techniques of this disclosure enable safe operation of a network, enable fast debugging of network problems, reduce the blast radius of an outage, and prevent small issues from becoming bigger problems.

Alternatively, a workflow or human can consult a global trusted system and self-regulate network changes based on data and feedback provided by the trusted system. Such an alternative does not scale, and can suffer from races if changes are made locally.

CONCLUSION

This disclosure describes techniques that account for the rate and magnitude of recent changes made by an authorized person or workflow. If preset limits to rates or magnitudes of changes are met or exceeded, authorization is declined for a certain period of time, thus ensuring continued network stability.