I2nsf Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2017

J. You
Huawei
M. Zarny
Goldman Sachs
C. Jacquenet
M. Boucadair
France Telecom
Y. Li
J. Strassner
Huawei
S. Majee
F5 Networks

July 8, 2016

User-group-based Security Policy for Service Layer
draft-you-i2nsf-user-group-based-policy-02

Abstract

This draft defines the User-group Aware Policy Control (UAPC) framework, which facilitates consistent enforcement of security policies based on user group identity. Policies are used to control security policy enforcement using a policy server and a security controller. Northbound APIs are also discussed.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In traditional networks, network access is typically controlled through a combination of mechanisms such as maintaining separate static VLAN/IP subnet assignments per organization, applying Access Control Lists (ACLs) on VLANs and/or IP subnets, leveraging Network Access Control (NAC). Common side effects are:

o Network administrators typically assume that users access the network from their own static location--from their assigned switch, VLAN, IP subnet, etc.

- o MAC or IP address of the users’ device is often used as a proxy for the user’s identity. As such, filtering (e.g., via ACLs) of the user is usually based on IP or MAC addresses.

- o Authentication of the user by the network, if it exists at all, typically takes place only at the access switch in conjunction with an AAA (Authentication, Authorization, Accounting) server. Different authentication mechanisms could be used - from machine-based certificates to username/password challenges, to just "authenticating" on MAC addresses, etc.

- o Network security functions such as firewalls often act only on IP addresses and ports - not on the user’s identity.

These are all symptoms of a system not using actual user identification information, but rather, one or more attributes that attempt to represent a user identity.

Traditional network access control mechanisms [I-D.ietf-i2nsf-problem-and-use-cases] do not work well in newer network paradigms.

- o First, both clients and servers can move and change their IP addresses on a regular basis. For example, Wi-Fi and VPN clients, as well as back-end Virtual Machine (VM)-based servers, can move; their IP addresses could change as a result. This means relying on well-known network fields (e.g., the 5-tuple) is increasingly inadequate to ensure consistent security policy enforcement.

- o Secondly, with more people working from non-traditional office setups like "working from home", there is now a need to be able to apply different security policies to the same set of users under different circumstances. Network access needs to be granted based on such criteria as users’ location, time-of-day, type of network device used (e.g., corporate issued device versus personal device), device’s security posture, etc. This means the network needs to recognize the users’ identity and their current context, and map the users to their correct access entitlement to the network.

- o Moreover, implementation of coherent security policy across several network and network security devices is almost impossible. NSFs in operation could be sourced from different vendors, or could be different hardware models/software versions by the same vendor. As a result, the capabilities as well as APIs of the NSFs may not be the same throughout the environment. Finally, few enterprises, if any, have a complete view of all the application flows. It is not uncommon for administrators to update a policy on a firewall, only to later find out that related ACLs, firewall policies, and other related mechanisms were not updated.

Today, addressing the above issues takes considerable time and effort. Most network administrators have to manually plan and implement necessary changes as little automation, if any, exists across diverse sets of network security platforms. In line with the I2NSF effort to standardize APIs so as to facilitate automation, this draft defines User-group Aware Policy Control (UAPC), which facilitates consistent enforcement of policies based on user-group identity, and discusses how it operates in the I2NSF Service Layer [I-D.ietf-i2nsf-framework].

2. Terminology

2.1. Abbreviations and acronyms

AAA: Authentication, Authorization, and Accounting

ACL: Access Control List

ADSL: Asymmetric Digital Subscriber Line

AP: Access Point

LTE: Long Term Evolution

NAC: Network Admission Control

NBI: Northbound Interface

NSF: Network Security Function

UAPC: User-group Aware Policy Control

VLAN: Virtual Local Area Network

2.2. Definitions

User: An individual or a group of individuals that act as a single entity.

User-group: A group of users that share one or more characteristics and/or behaviors in common, which allows each user in the user-group to be assigned the same access control permissions. For example, sales employees are treated with equivalent service policy rules when accessing the network.

Profile: A set of capabilities, in terms of functions and behaviors, for a given entity or set of entities.

Role: A role defines a set of responsibilities of an object that it is attached to. This enables the functions and behavior of a complex object to be abstracted into just those that are required by a client in a particular context.

User-group Identifier (User-group ID): An identifier that represents the collective identity of a group of users, and is determined by a set of one or more matching criteria (e.g., roles, 4-, 5-, and 6-tuples, VLAN ID, etc.) that disambiguates this user-group entity from other entities.

3. Use Cases for User-group Aware Policy Control

With the increased popularity of enterprise wireless networks and remote access technologies such as Virtual Private Networks (VPN), enterprise networks have become borderless, and employees' locations can be anywhere. Enabling large-scale employee mobility across many access locations improves enterprise production efficiency but also introduces challenges related to enterprise network management and security. The IP address of the user can change frequently when the user is in motion. Consequently, IP address-based policies (such as forwarding, routing, QoS and security policies) may not be flexible enough to accommodate users in motion.

The User-group Aware Policy Control (UAPC) approach is intended to facilitate the consistent enforcement of policies. As shown in Figure 1, a multi-technology network (e.g., Wi-Fi, 3G/LTE, ADSL and fiber infrastructures) can connect different types of terminal devices (e.g., Smartphone, tablet, and laptop) which should be able to access networks in a secure manner. Security policies should be consistently enforced based on their user-group identities, regardless of whether these terminal devices connect to a wired or a wireless infrastructure.

```
                                   +--------------------+
                                   |       PDP          |
                                   | (policy, security, |
                                   |  management)       |
                                   +---+--------------+-+
                                       |              |
                                       |              |
                                       |     UAPC     |
                                       |              |
                                       |              |
     +--------------+       +----------+---+      +---+----------+
     |+------------+|       |              |      |              |
     ||smartphone  ||       |              |      |              |
     |+------------+|       |  3G/LTE      |      |              |
     |+------------+|       |              |      |   Data       |
     ||  tablet    ||       |  Pulic WiFi  |      |              |
     |+------------+|       |              |      |   Center     |
     |+------------++-------+  ADSL        +------+              |
     ||  laptop    ||       |              |      |              |
     |+------------+|       |  AP          |      |              |
     |+------------+|       |              |      |              |
     ||    PC      ||       |  ...         |      |              |
     |+------------+|       |              |      |              |
     |              |       | Access       |      | Enterprise   |
     | Devices      |       | Networks     |      | HQ           |
     +--------------+       +--------------+      +--------------+
```

Figure 1: UAPC Framework Example

4. User-group Aware Policy Control

4.1. Overview

The UAPC framework is as follows enables users to be authenticated and classified into different user-groups at the network ingress by the Security Controller; this may require obtaining information from the Policy Server and an AAA server. The user-group is an identifier that represents the collective identity of a group of users, and is determined by a set of pre-defined policy criteria (e.g., source IP address, geo-location data, time of day, or device certificate). Users may be moved to different user-groups if their composite security context and/or environment change.

The Security Controller, if necessary, pushes the required user-group policies to all Network Security Functions (NSFs) that need them. The policies are expressed as user-group (not IP or MAC address) IDs so as to decouple the user identity from the network addresses of the user’s device.

(Note that User-group IDs may be implemented in at least two ways: (1) the ingress switch inserts the user-group ID into the packets, and downstream NSFs match and act on the user-group ID, or (2) the Security Controller updates each NSF with the mapping between the user-group IDs and the packet tuples; NSFs map incoming packets to their rightful user-group IDs, and act on the user-group IDs. These and other implementation methodologies are out of scope of this document.)

The security policy provisioning information can be derived from the user’s profile and credentials, as well as the group to which the user belongs; such information can also be derived from the outcomes of the dynamic security service parameter negotiation that could possibly take place between the user and the service provider or the network administrator (e.g., parameters like whether the user is entitled to access the enterprise network while in motion or not, the lease time associated to an IP address, whether the user can access the Internet or not, and whether traffic needs to be encrypted or not). This information is transferred to the Network Security Functions (NSF) from the controller. Once an incoming packet matches a certain user group on the NSF, the corresponding security policy will be enforced on that packet.

4.2. Functional Entities

The UAPC framework consists of four main components: (1) Policy Server, (2) Authentication Server, (3) Security Controller, (4) Network Security Functions:

o Policy Server

The Policy Server houses two policy databases: (1) the user-group criteria, which assigns users to their user-group, and (2) the rule base of what each user group has access to.

- Contains (G)UI and/or APIs to enable policies to be created, modified, and deleted using command line, graphical tools, and/or programming logic

- Contains logic to create, read, update, and delete policies and policy components, and apply policies to user-groups from one or more policy repositories

- Contains logic to detect conflicts between policies

- Contains logic to resolve conflicts between policies

- Contains logic to broker and/or federate policies between domains

The above subjects are beyond the scope of this document.

o AAA Server

The AAA Server authenticates users, and then performs associated authorization and accounting functions. The AAA server classifies users into different user-groups at the network ingress. AAA server implementation details are out of scope for this document.

o Security Controller

The Security Controller coordinates various network security-related tasks on a set of NSFs under its administration. In general, there may be multiple security domains, where each domain has its own security controller. The detailed architecture is beyond the scope of this document.

- Authenticates the user at the ingress using an authentication service. While the authentication functionality is an integral part of the framework, the topics of defining and managing authentication rules are out of scope of this document.

- Asks policy server for decisions to security-related requests; takes these decisions and invokes the set of NSFs that are required to implement security for that particular packet. The security controller may cache policies.

- May perform additional actions as specified by the metadata associated with a policy rule (e.g., the "function(s)" to be executed after the actions in a policy rule are executed)

- Has an authoritative database of NSFs under its administration

- Determines on which NSFs a given policy needs to be enforced

- Presents a set of NBIs for applications, orchestration engines, etc.

- Interfaces with NSFs via (to-be-developed) I2NSF Capability Layer APIs.

o Network Security Functions

- Packet classification: Depending on the implementation model, the NSF may match on User-group IDs in the packets; or it may match on common packet header fields such as the 5-tuple, and map the n-tuple to the appropriate User-group ID supplied out-of-band by the Security Controller.

- Policy enforcement: Enforce the corresponding policy (or set of policies) if the packet matches a specified User-group ID or set of User-group IDs

- Presents I2NSF Capability Layer APIs

4.3. User Group

The user-group is an identifier that represents the collective identity of a group of users, whose definition is controlled by one or more policy rules (e.g., source IP, geo-location, time of day, and device certificate).

A given user is authenticated, and classified at the network ingress, and assigned to a user-group. (The term "user" refers to any user of the network. As such, servers, terminals and other devices are also classified and assigned to their respective user-groups.) A user’s group membership may change as aspects of the user change. For example, if the user-group membership is determined solely by the source IP address, then a given user’s user-group ID will change when the user moves to a new IP address that falls outside of the range of addresses of the previous user-group.

Table 1 shows an example of how user-group definitions may be constructed. User-groups may share several common criteria. That is, user-group criteria are not mutually exclusive. For example, the policy criteria of user-groups R&D Regular and R&D-BYOD may share the same set of users that belong to the R&D organization, and differ only in the type of client (firm-issued clients versus users’ personal clients); likewise, the same user may be assigned to different user-groups depending on the time of day or the type of day (e.g., weekdays versus weekends); and so on.

Table 1: User-Group Example

Group Name	Group ID	Group Definition
R&D	10	R&D employees
R&D BYOD	11	Personal devices of R&D employees
Sales	20	Sales employees
VIP	30	VIP employees
Workflow	40	IP addresses of Workflow resource servers
R&D Resource	50	IP addresses of R&D resource servers
Sales Resource	54	IP addresses of Sales resource servers

4.4. Inter-group Policy Enforcement

Within the UAPC framework, inter-group policy enforcement requires two key components: (1) user-group-to-user-group access policies, and (2) sets of NSFs that are managed by sets of policies.

First, the framework calls for an authoritative rule-base that lists all the destination user-groups to which all the source user-groups are entitled to access. The rule-base, hosted on the Policy Server, enables administrators to construct authorized inter-group access relationships. The simple example in Table 2 shows a policy matrix in which the row represents source user-groups and the column represents destination ones. The inter-group rule-base is similar to firewall rule-bases, which are mostly made up of 5-tuples. (Firewall rule-bases could and do include criteria other than the standard 5-tuple. Also, the user-group rule-base could consist of other criteria. Actual implementation details are out of scope of this document.)

The responsibility of implementing and managing the inter-group policies falls to the Security Controller. The controller first needs to determine, (or is told) the specific NSFs on which a given policy is to be implemented. The controller then communicates with each NSF via the I2NSF APIs to execute the required tasks.

Table 2: Inter-group Policy Example

	Destination Group		
Source Group	Workflow Group	R&D Resource Group	Sales Resource Group
R&D group	Permit	Permit	Deny
R&D BYOD group	Traffic-rate	Deny	Deny
Sales group	Permit	Deny	Permit
VIP user group	Traffic-mark	Traffic-mark	Traffic-mark

Inter-user-group rules are configurable. Figure 2 illustrates how various user-groups and their entitlements may be structured. The example shows a "north-south" model that shows how users may access internal network resources. Similar models can be developed for "east-west" intra-data center traffic flows.

```
             +---------------------------------+
             |  Authentication Domain          |
             |+------------------------------+ |
             || DemilitarizedZone            | |
             ||+---------------------------+ | |
             ||| General Service           | | |
Common BYOD  |||+------------------------+ | | |
User --------++++ Common Service         | | | |
             ||||+---------------------+ | | | |
Guest--------++|||Limited Service      | | | | |
             |||||+------------------+ | | | | |
Insecure     ||||||Important Service +-+-+-+-+-+-- Partner
User    -----+|||||   +------------+ | | | | | |
             ||||||   |Core Service+-+-+-+-+-+-+-- Executive
User at   ---+++++|   +------------+ +-+-+-+-+-+-- User at office
non-office   |||||+------------------+ | | | | |   hours
hours        ||||+---------------------+ | | | |
             |||+------------------------+ | | |
             ||+---------------------------+ | |
             |+------------------------------+ |
             +---------------------------------+

             Unauthorized user (X)
             User using an unregistered device (X)
```

Figure 2: Sample Authorization Rules for User-group Aware Policy Control

4.5. UAPC Implementation

The security policies are instantiated and maintained by the policy server. The associated computation logic (to instantiate such policies) may be dynamically fed with instructions coming from the application. The policy decisions could also be from the outcomes of dynamic security service parameter negotiations that typically take place at the management plane between the user and the service provider [RFC7297].

The NSFs receive group-based policy provisioning information from the security controller. The security policies will be enforced so that participating NSFs can process traffic accordingly. There are five steps for implementing the UAPC framework, which are shown in Figure 3.

```
                                +-----------------+
                                |   Orchestrator  |
                                +-+-------------+-+
                                  |             |
            ======================|=============|==============
                             +----+---+        ++---------+
                             | Policy +--------+Security  |
                     (Step 1)| Server |   +----+Controller|
                             +----+---+   |    +-+---+----+
                                  |       |      |   |
                             +----+-------+-+    |   |
                             |     AAA      |    |   |
                             |    Server    |    |   |
                             +--------------+    |   |
                                                 |   | (Step 2)
                                                 |   |
                             (Step 4)   +------+-+   |
                                      ----------------
          (Step 3)                /////  |      |     | \\\\\
         +-------------+       ///      |      |     |      \\\
    Site1|Wireless User+--------        |      |     |         \\
         +-------------+   ||        +--+-+ +--+-+ +-+--+        ||
         +-------------+   |         |    | |    | |    |         |
    Site2|Wired User   +--+          |NSFs| |NSFs| |NSFs|          |
         +-------------+   |         |    | |    | |    |         |
         +-------------+   ||        +----+ +----+ +----+        ||
    Site3|Remoter User +-------         (Step 5)               //
         +-------------+       \\\                          ///
                                  \\\\\                /////
                                       ----------------
```

Figure 3: Unified Policy Procedures

1. User-group identification policies and inter-user-group access polices on the Policy Server are managed by authorized user(s) and/or team(s).

2. The user-group-based policies are implemented on the NSFs under the Security Controller’s management.

3. When a given user first comes logs onto the network, the user is authenticated at the ingress switch.

4. If the authentication is successful, the user is placed in a user-group, as determined by the Policy Server. If the authentication is not successful, then the user is not assigned a user-group, which means that the user has no access permissions for the network.

5. The user’s subsequent traffic is allowed or permitted based on the user-group ID by the NSFs per the inter-user-group access policies. (It is beyond the scope of this document as to how user-group IDs may be delivered to non-ingress NSFs. See Section 4.1 for a brief overview of possible implementation methods.)

5. Requirements for I2NSF

Key aspects of the UAPC framework fall within the Service Layer of the I2NSF charter. If the community adopts the approach as one possible framework for the Service Layer, the I2NSF Service Layer MUST support at least the following northbound APIs (NBIs):

- The user-group classification policy database on the Policy Server

- The inter-user-group access policy rule-base on the Policy Server

- The inventory of NSFs under management by the Security Controller

- The list of NSFs on which a given inter-user-group policy is to be implemented by the Security Controller.

The framework also assumes that the I2NSF Capability Layer APIs will be there for the NSFs.

6. Security Considerations

This document provides the UAPC framework, and discusses how it operates in the I2NSF Service Layer. It is not intended to represent any particular system design or implementation, nor does it define a protocol, and as such it does not have any specific security requirements.

7. IANA Considerations

This document has no actions for IANA.

8. Acknowledgements

The editors would like to thank Linda Dunbar for a thorough review and useful comments.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, DOI 10.17487/RFC7297, July 2014, <http://www.rfc-editor.org/info/rfc7297>.

9.2. Informative References

[I-D.ietf-i2nsf-framework] elopez@fortinet.com, e., Lopez, D., Dunbar, L., Strassner, J., Zhuang, X., Parrott, J., Krishnan, R., and S. Durbha, "Framework for Interface to Network Security Functions", draft-ietf-i2nsf-framework-02 (work in progress), July 2016.

[I-D.ietf-i2nsf-problem-and-use-cases] Hares, S., Dunbar, L., Lopez, D., Zarny, M., and C. Jacquenet, "I2NSF Problem Statement and Use cases", draft-ietf-i2nsf-problem-and-use-cases-00 (work in progress), February 2016.

Authors' Addresses

Jianjie You
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, 210012
China

Email: youjianjie@huawei.com

Myo Zarny
Goldman Sachs
30 Hudson Street
Jersey City, NJ 07302
USA

Email: myo.zarny@gs.com

Christian Jacquenet
France Telecom
Rennes 35000
France

Email: christian.jacquenet@orange.com

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Yizhou Li
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, 210012
China

Email: liyizhou@huawei.com

John Strassner
Huawei
2330 Central Expressway
San Jose, CA
USA

Email: john.sc.strassner@huawei.com

Sumandra Majee
F5 Networks
3545 N 1st St
San Jose, CA 95134

Email: S.Majee@f5.com