User-group-based Security Policy for Service Layer

draft-you-i2nsf-user-group-based-policy-01

Presenter: John Strassner

Jianjie You (youjianjie@huawei.com)
Myo Zarny (myo.zarny@gs.com)
John Strassner (john.sc.strassner@huawei.com)
Christian Jacquenet (christian.jacquenet@orange.com)
Mohamed Boucadair (mohamed.boucadair@orange.com)
Yizhou Li (liyizhou@huawei.com)
Sumandra Majee (S.Majee@f5.com)

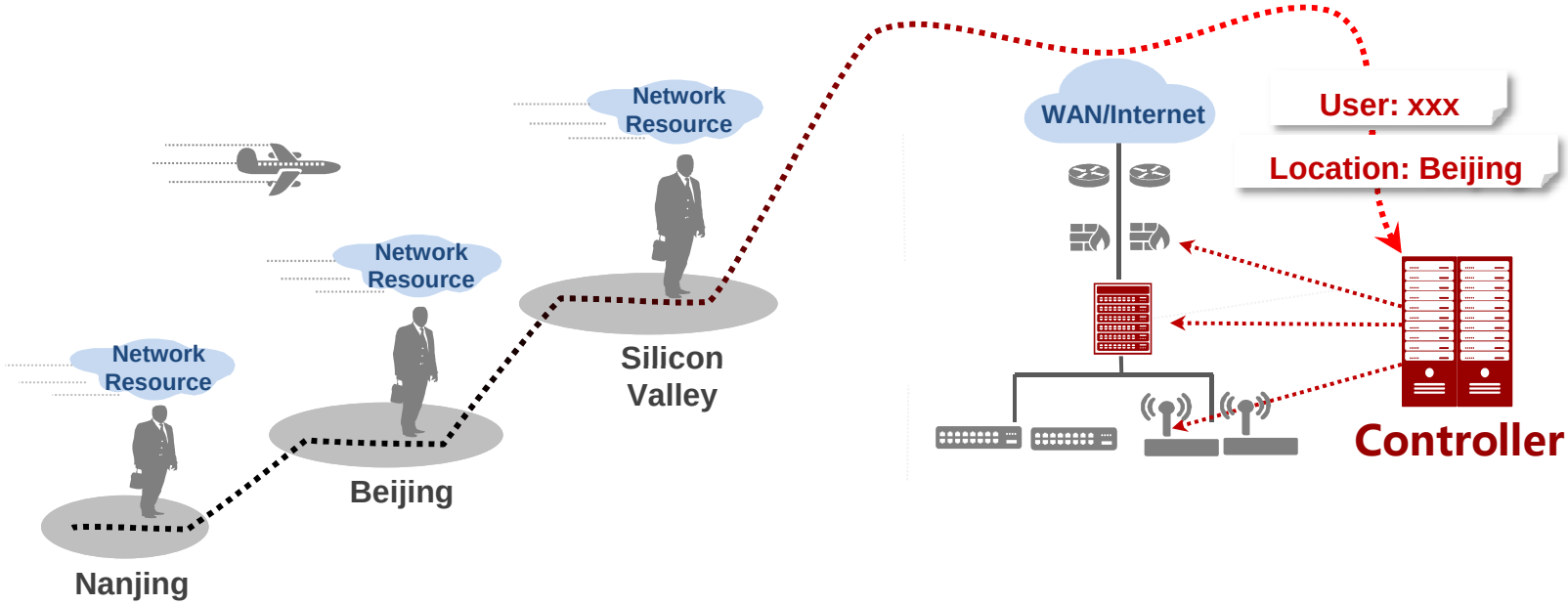
Status of this I-D

- First presented at IETF 94, Yokohama meeting;

The update compared to v-00

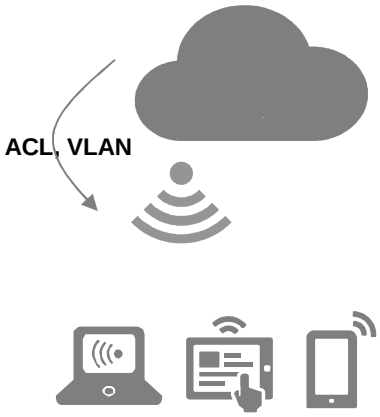
- Add the AAA server as the part of the framework in i2nsf architecture
- Add some clarifications

Newer Network Paradigms



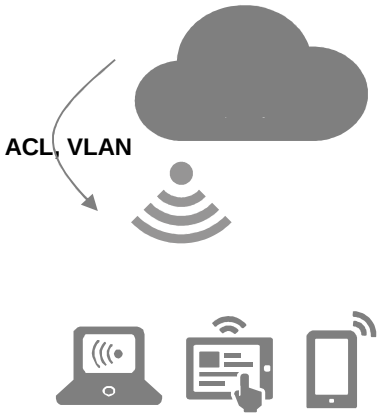
Increasing demands of business mobility, anytime, anywhere collaboration, etc. introducing challenges to network security management and enforcement

Traditional Network Access Control



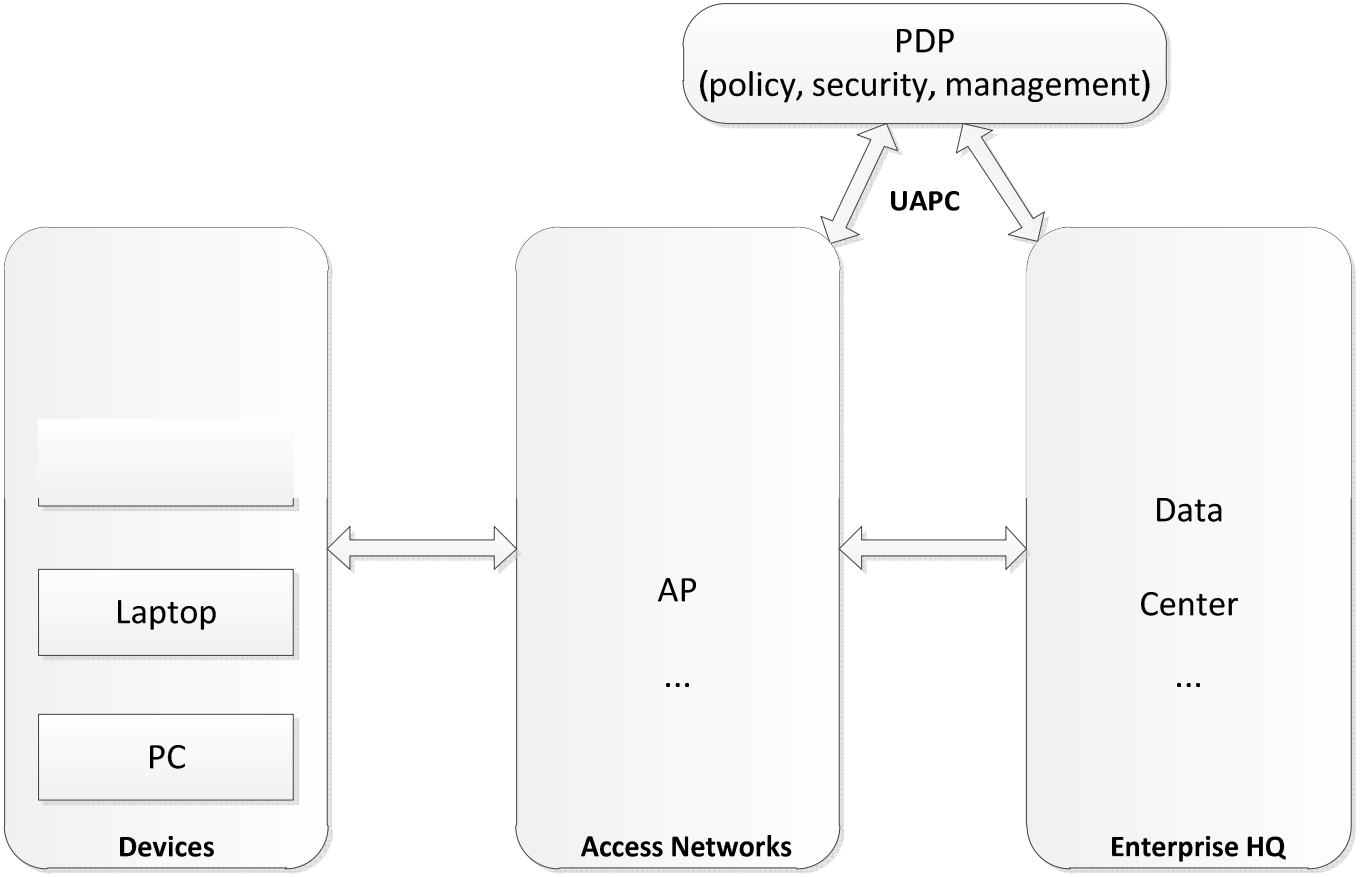
- Access the network typically from their own static location – from their assigned switch, VLAN, IP subnet, etc.
- MAC or IP address of the users' device is often used as a proxy for the user's identity. As such, filtering (e.g., via ACLs) of the user is usually based on IP or MAC addresses.
- Authentication of the user by the network, typically takes place only at the ingress switch
- Network security functions such as firewalls often act only on IP addresses and ports - not on user identity.

Challenges for Traditional NAC



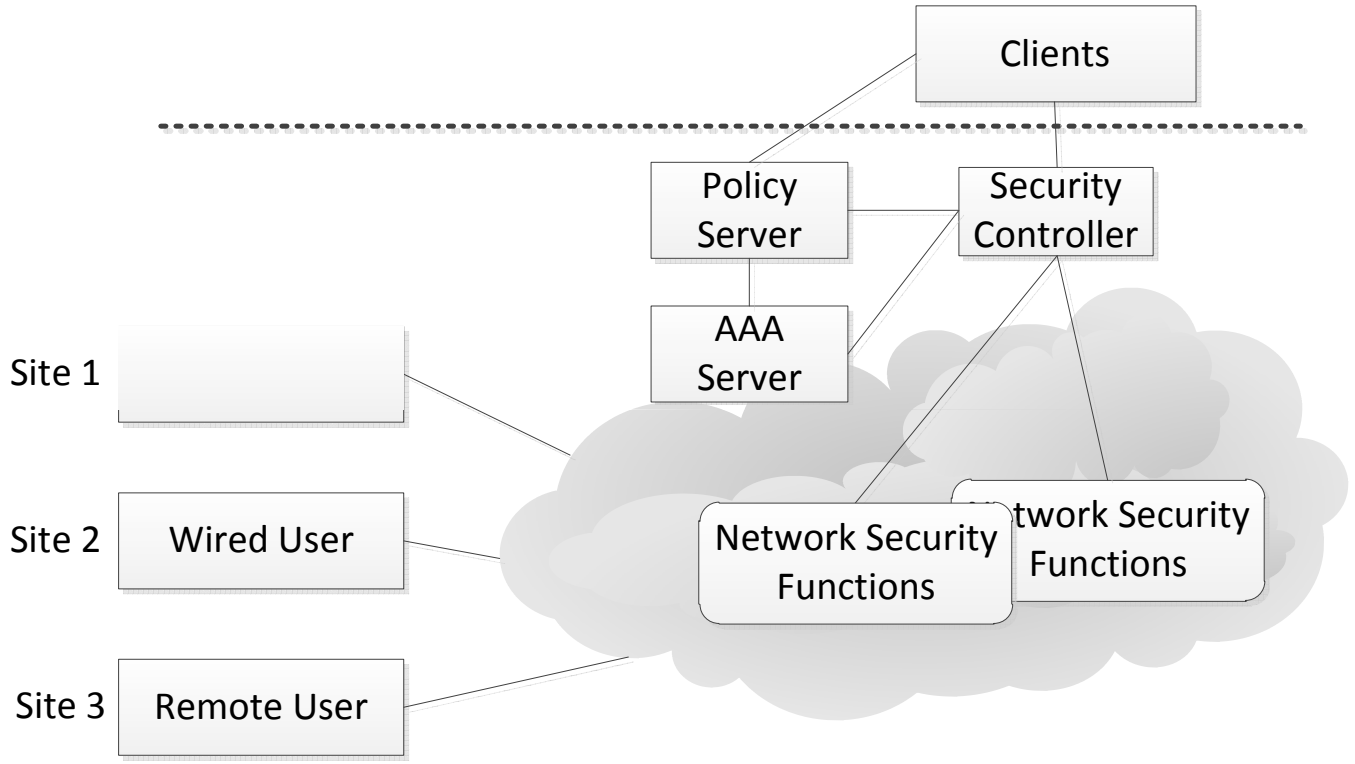
- Both clients and servers can move and change their IP addresses on a regular basis
- Need to apply different security policies to the same set of users under different circumstances
- Implementation of coherent security policy across several network and network security devices is almost impossible.

UAPC Framework Example



The User-group Aware Policy Control (UAPC) approach is intended to facilitate the consistent enforcement of policies, e.g., 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.

UAPC Framework Example



Goal: Apply appropriate user-group identity-based network security policies on NSFs throughout the network

UAPC Functional Entities

- **Policy Server**
  - Holds the user-group criteria, which assigns users to their user-group
  - Holds the rule base, of what each user-group has access to
- **AAA Server**
  - Authenticates users, and then performs associated authorization and accounting functions.
- **Security Controller**
  - Coordinates various network security-related tasks on a set of NSFs under its administration
- **Network Security Functions**
  - Packet classification
  - Policy enforcement
  - Presents I2NSF Capability Layer APIs

User Group

- Identifier that represents the collective identity of a group of users
- Controlled by one or more policy rules (e.g., source IP, geo-location, time of day, device certificate, etc.)

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

Inter-Group Policy Enforcement

Key components

1. User-group-to-user-group access policies – think “firewall rule-base but with user-groups instead of IPs and ports”
2. Sets of NSFs on which individual policies need to be applied

Destination Group / Source Group	Workflow Group	R&D Resource Group	Sales Resource Group
R&D group	Permit	Permit	Deny
R&D BYOD group	Permit	Deny	Deny
Sales group	Permit	Deny	Permit
VIP user group	Permit	Permit	Permit

Inter-Group Policy

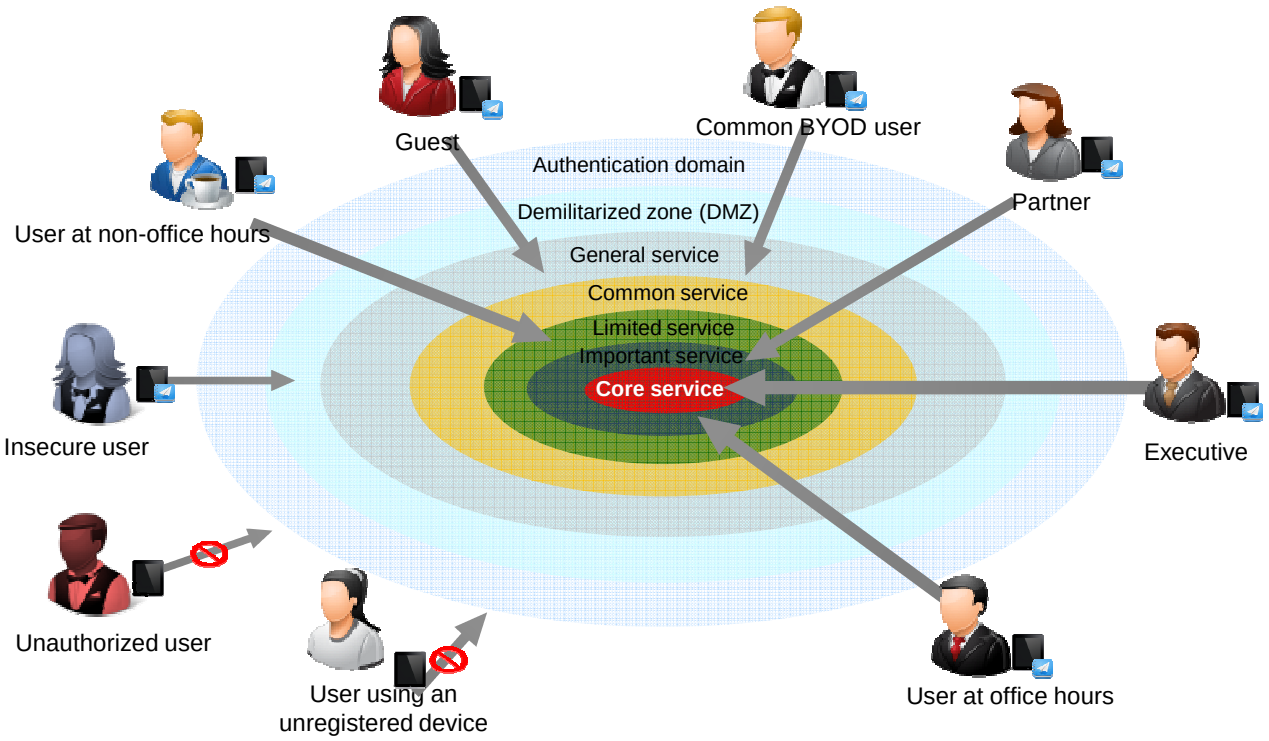
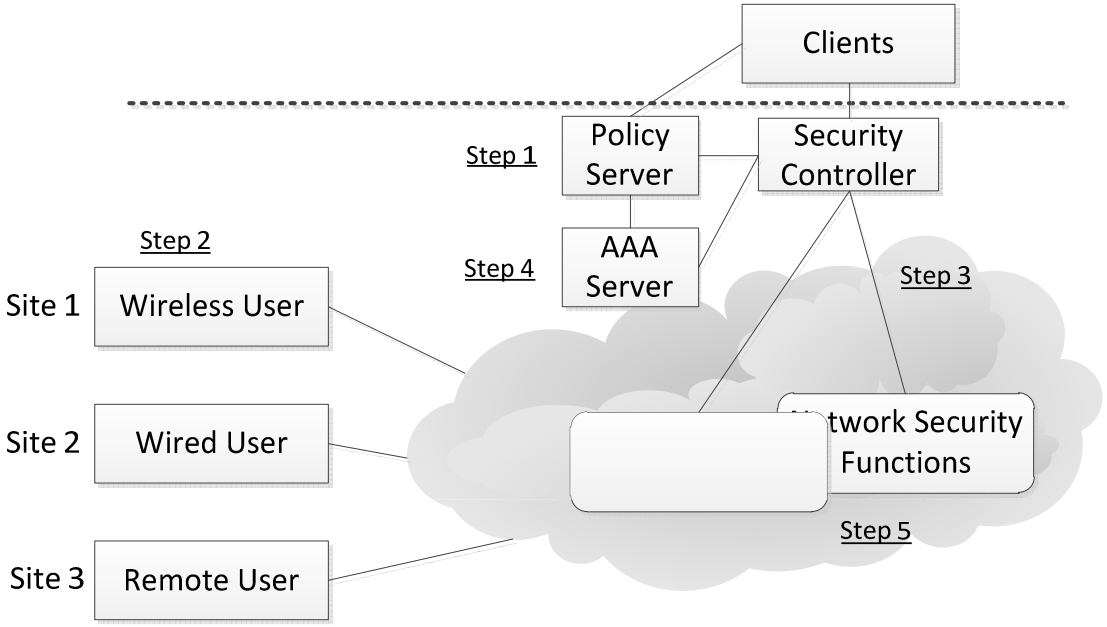


Figure 2: Sample Authorization Rules for User-group Aware Policy Control

UAPC Implementation



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

Requirements for I2NSF

Key aspects of the UAPC framework falls 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.

Next Steps

- Solicit comments and suggestions on the mailing list
- Encourage implementation specific drafts

Thank you!