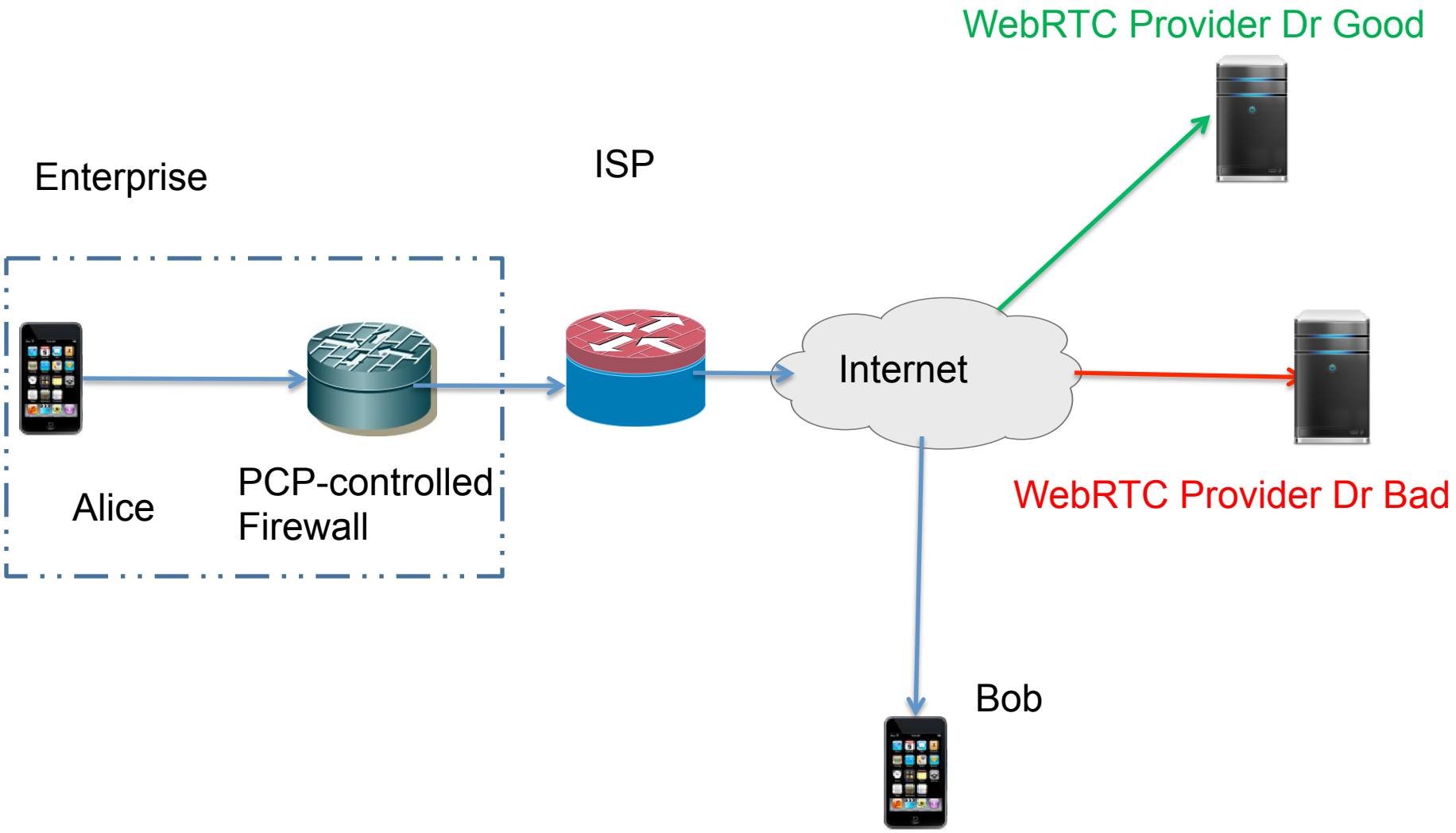
PCP Extension for Third Party Authorization

draft-wing-pcp-third-party-authz-00

Aug 2013 IETF 87 Meeting

Authors : D.Wing, T.Reddy, P.Patil, R.Penno

Firewall/QOS : WebRTC PCP Use Case



Problem Statement with Example

- WebRTC signaling is end-to-end encrypted.

- WebRTC does not enforce a particular session signaling protocol; DPI fails.

- Session signaling and peer-to-peer media traverse different firewalls.

- Firewalls fail to distinguish media session initiated using selected WebRTC servers (Dr. Good) it trusts and block others (Dr. Evil).

Existing Solution: TURN on DMZ

- TURN increases media latency
- No solution to prioritize flows (network is unaware)

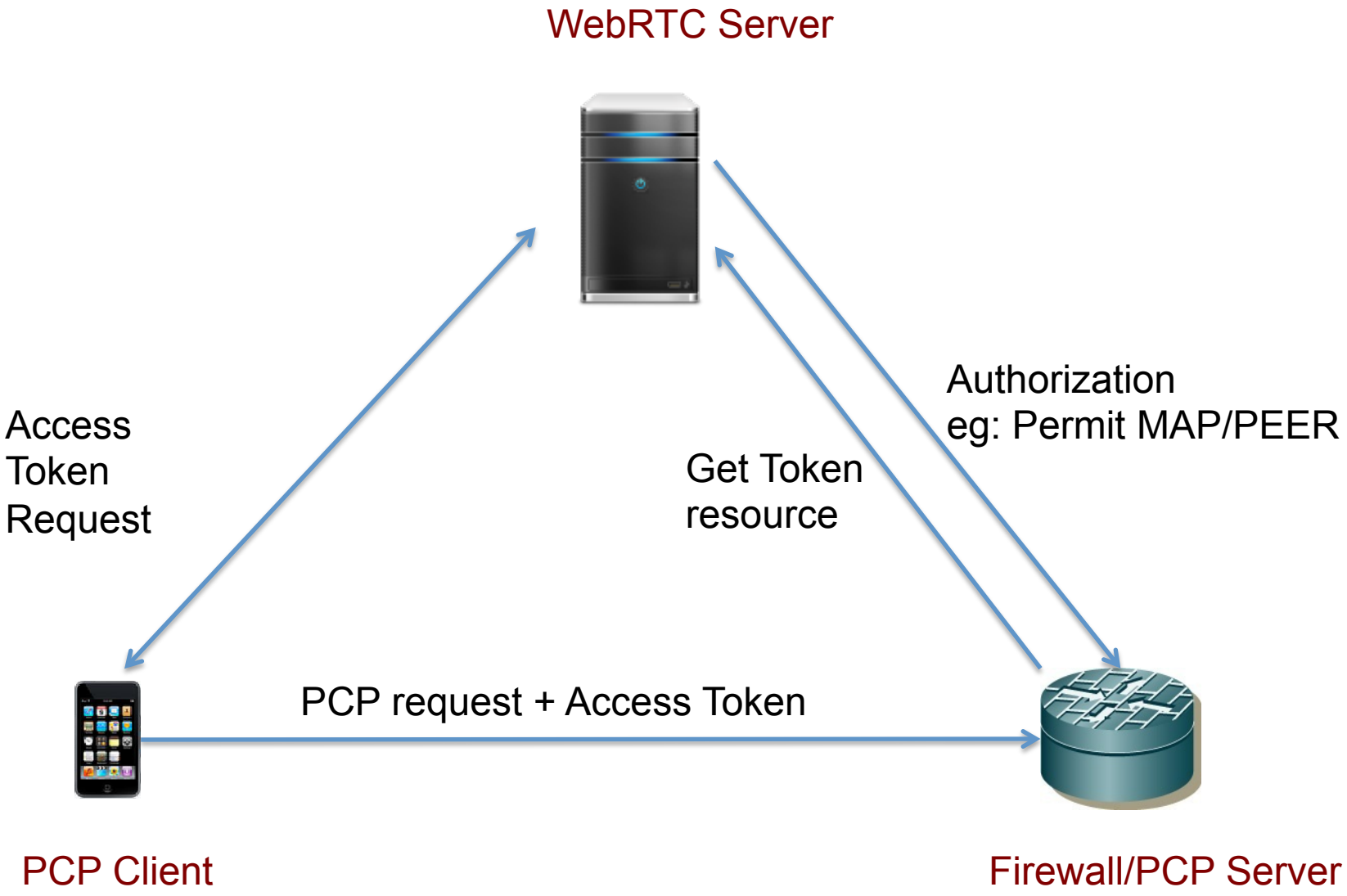
Requirement

REQ-13 (Third Party Authorization) in PCP Authentication Requirements draft discusses this requirement.

Problem Statement

- Need to allow **authorized applications, deny unauthorized applications**
- Need to allow **endpoints to request flow characteristics from the network**

3rd Party authorization for PCP using OAuth



Conclusions

- This is a missing piece of work
- This mechanism is also required by various other drafts (draft-wing-pcp-flowdata)

BACKUP

3rd Party authorization for PCP using OAuth

OAuth	PCP
Client	PCP Client
Resource Owner	Authorization Server (eg: WebRTC server)
Authorization server	Authorization Server
Resource Server	PCP Server

Deployments

•Enterprise Networks.

• IT network which is connected to various client networks.

• 3GPP networks where IMS services of certain other operators are permitted and others are blocked [TR33.830].

• Hot-Spots having tie-up with Social networking sites.