IPsec MIF Requirements

Daniel Migault, Carl Williams

draft-mglt-mif-security-requirements-02.txt - IETF84

Table of Contents

Table of Contents

I. Introduction

IPsec is used to:

- Extend a trusted domain over an untrusted network (like VPN)
- Provide end-to-end security (like TLS)

Untrusted networks are often unreliable:

- L4 protocols (like MPTCP, SCTP) use MIF to overcome unreliability
- L3 IPsec does not provides MIF features
- IPsec protected communications cannot take advantage of MIF features

We define IPsec MIF Requirements so IPsec protected communications can benefit from MIF features

II. Use Cases

This presentation considers the following use cases:

- Offloading Internet Access and Services from RAN to WLAN
- Virtual Private Network (VPN)
- Distributed Firewalls
- Distributed Security Domain (Cloud)

Offloading Services & Internet Access

Motivations and constraints on Offload are:

- ISPs offload RAN communications on WLAN to avoid RAN overload
- Security, QoS MUST be kept unchanged on WLAN

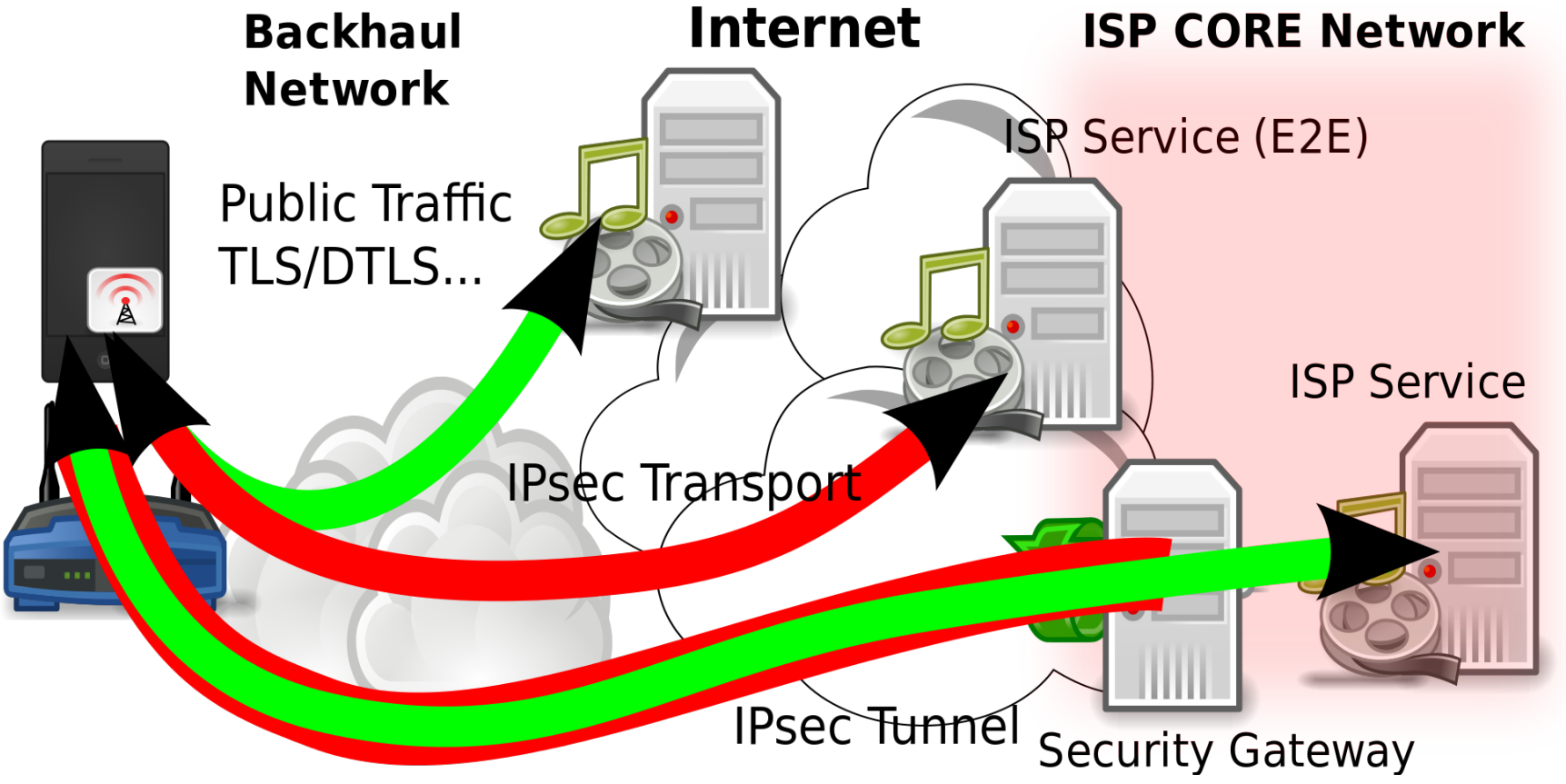
The different Offload Architectures we consider are:

- Offloading Access Architecture (with a Security Gateway)
- Offloading Service Architecture (with end-to-end security)

We expect that IPsec communications can benefit from:

- Bandwidth aggregation
- Multihoming
- Soft / Hard Handover Mobility
- Traffic Management

Access & Service Offload Architectures



Offloading from RAN to WLAN

Major offload challenge is to overcome the differences of WLAN toward RAN

Unlike RAN, on WLAN MN require MIF and Mobility features because:

- WLAN does not handle with Mobility
  - MN handles with Mobility
  - MN decides which Interface(s) to send traffic on
- WLAN are unreliable:
  - Multihoming makes communication reliable
  - Bandwidth Aggregation reduces the impact of Access Point Failover

WLAN may be untrusted networks

- Communications over untrusted networks MUST be secured (IPsec)

Virtual Private Network

VPN architecture is similar to OAA, but with slightly different motivations:

- VPNs are intentionally set up to access the company's resources
- VPNs never rely on RAN's Security or QoS properties
- VPNs have until recently only considered VPNs on PC with restricted Mobility requirements (cf MOBIKE)

In 2009, iPhones and other Smartphones:

- Were as handy as PC to access companies resources
- Had much more Mobility Requirements

We expect that IPsec communications can benefit from:

- Bandwidth aggregation
- Multihoming
- Soft / Hard Handover Mobility
- Traffic Management

Distributed Firewalls

Companies use IPsec to avoid unauthorized traffic:

- Transport mode be is preferred
- Modifications of IP addresses require the IPsec to be set again

We expect that IPsec communications can benefit from:

- Multihoming
- Soft Handover Mobility
- Hard Handover Mobility,
- (Traffic Management, Bandwidth aggregation)

Distributed Security Domain (Cloud)

With Cloud and virtualization:

- A Security Domain may be hosted on various pieces of hardware
- Pieces of hardware use IPsec to interconnect the Security Domain
- A piece of hardware may host multiple Security Domains

This results in:

- Pieces of hardware have established multiple Security Associations
- Mobility, Traffic Management operations of a piece of hardware involve multiple IPsec Security Associations

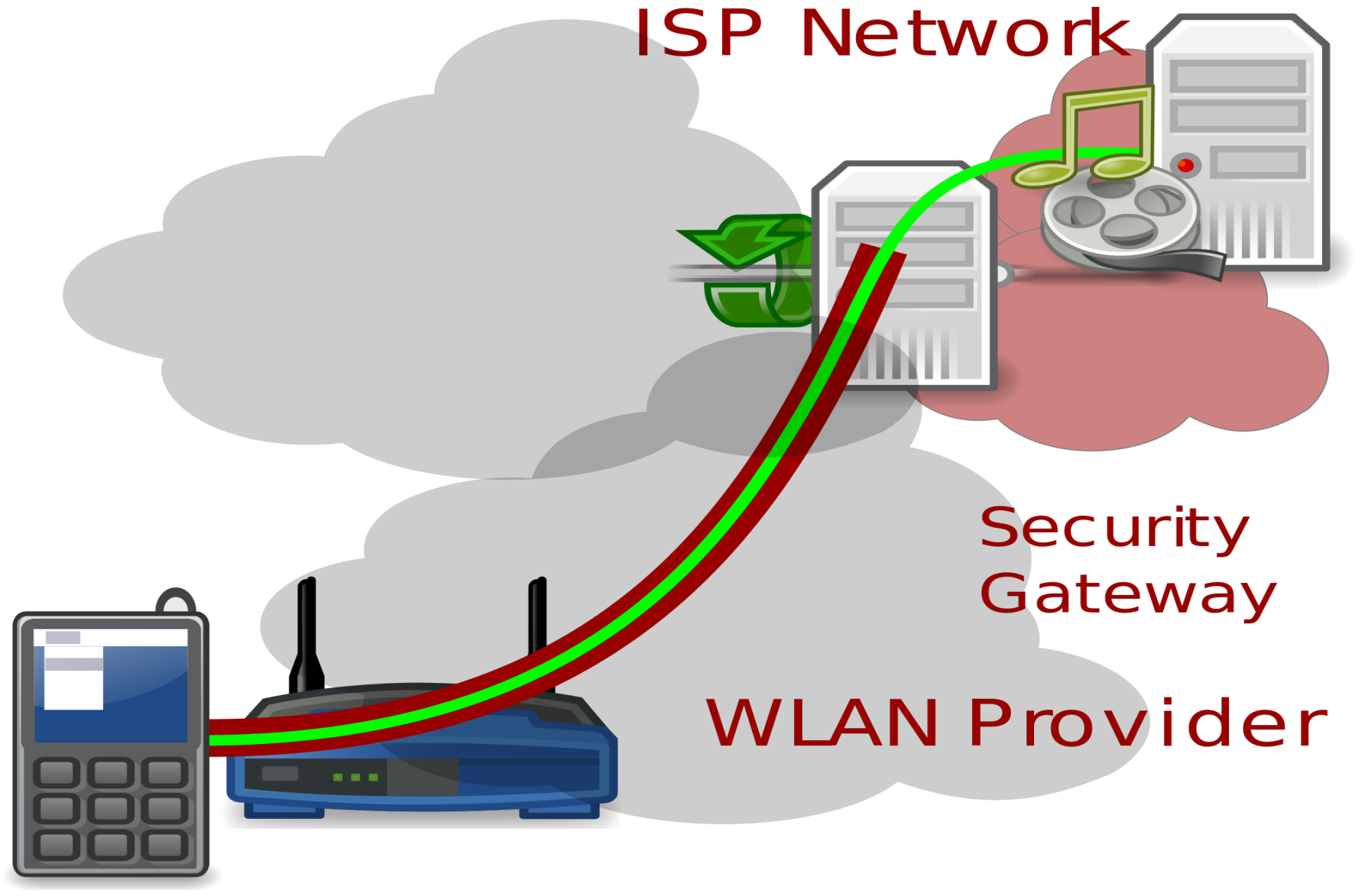
We expect that Multiple IPsec communications can ease:

- Cloud managements
- Traffic Management

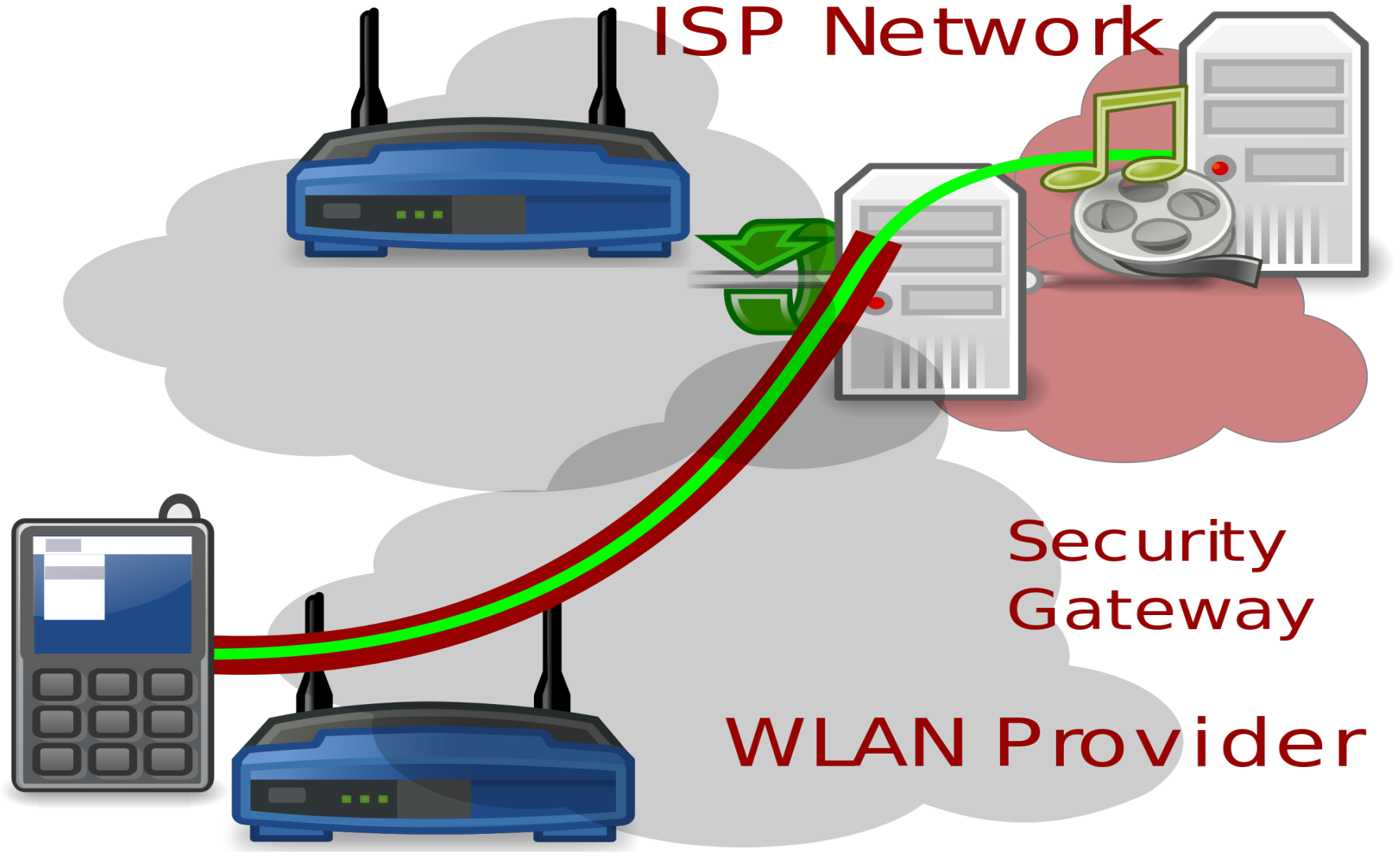
III. IPsec MIF Features

- ADD: When a new Interface appears the IPsec databases must be configured with this new Interface
- REMOVE: When a Interface does is not reachable, the IPsec data must remove this Interface
- SOFT_HAND_OVER: A Mobile Node must be able to move traffic from one Interface to the other without loosing packets, or interrupting the communication
- HARD_HANDOVER: A Mobile must be able to update a existing Security Association when a Mobility is performed (Transport), or to perform a mobility (Tunnel)
- SELECTOR: A Node must be able to select a subtraffic or multiple Security Associations to update the IPsec databases
- MULTIHOMING: IPsec database must be configured to fulfill Multihoming requirements

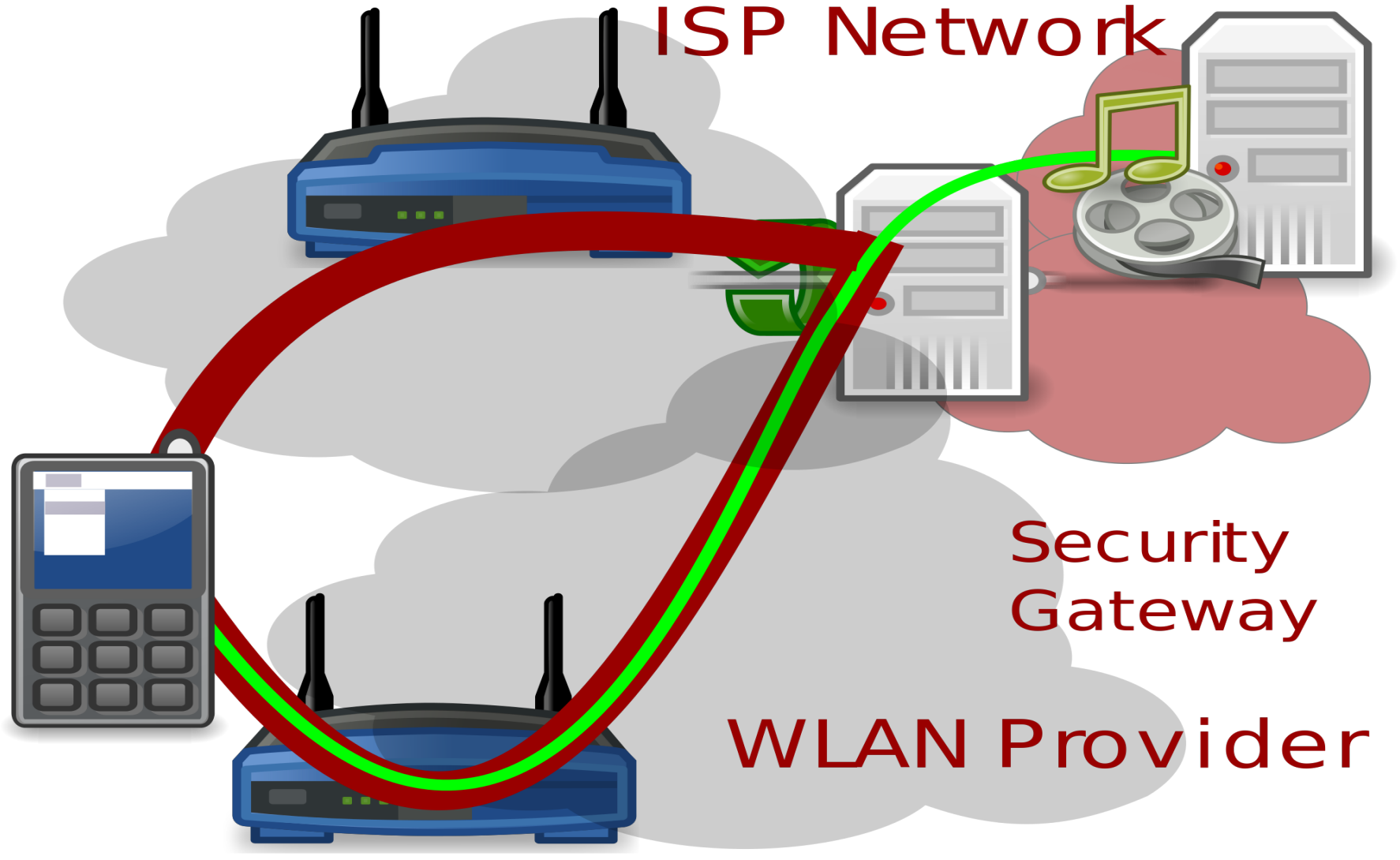
Example: ADD / REMOVE (Tunnel)



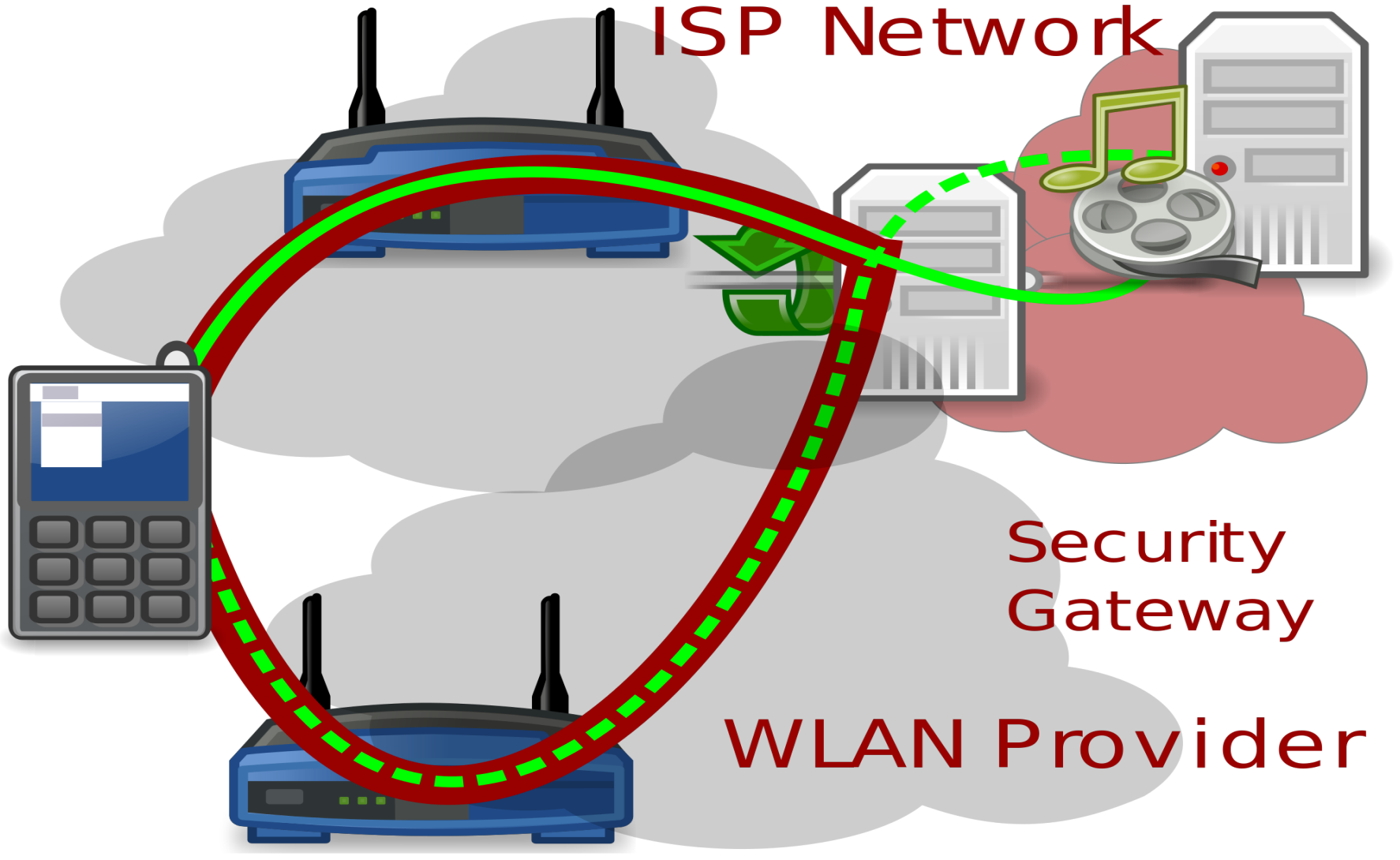
New Interface Detected



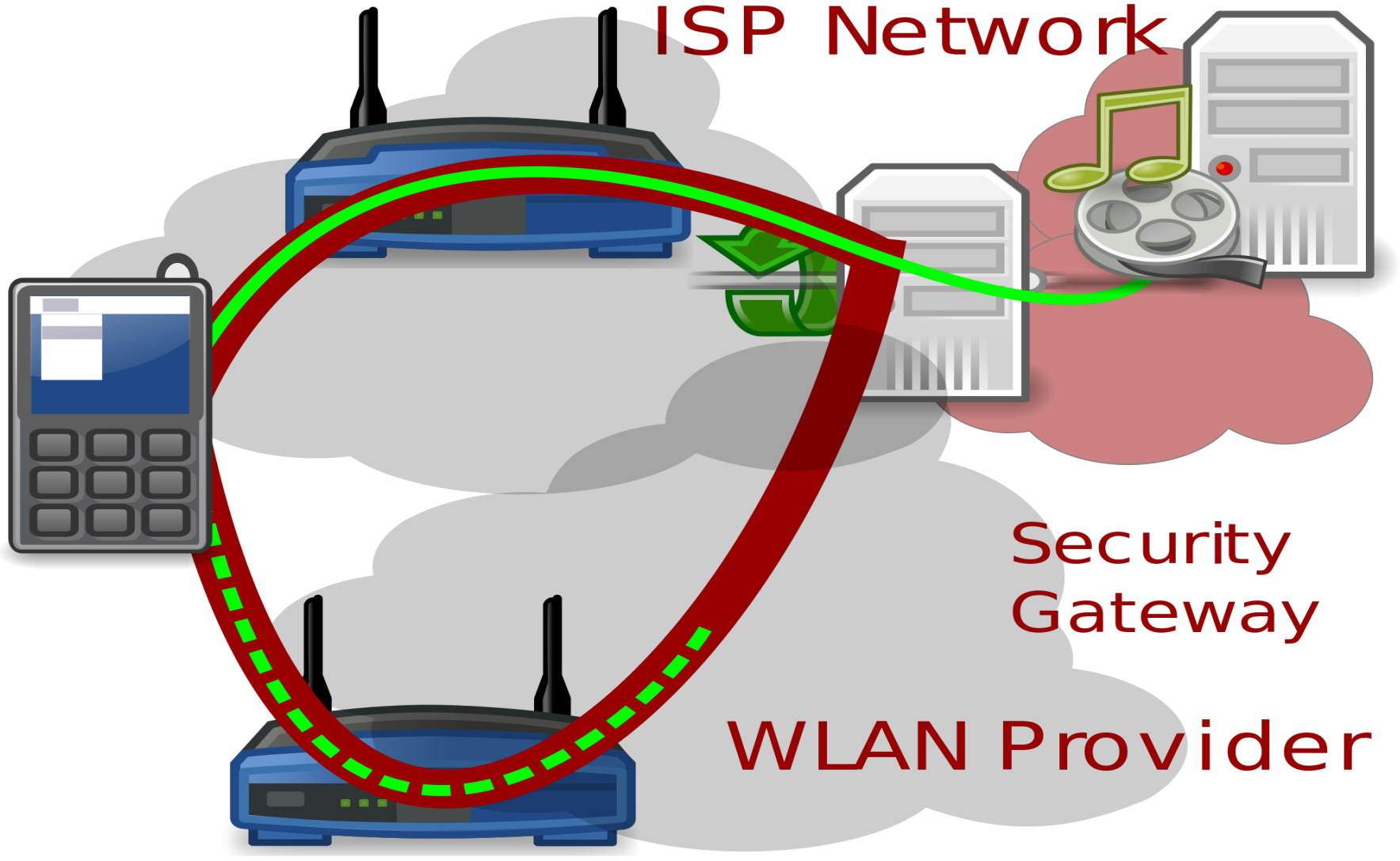
ADDing new Interface to IPsec databases



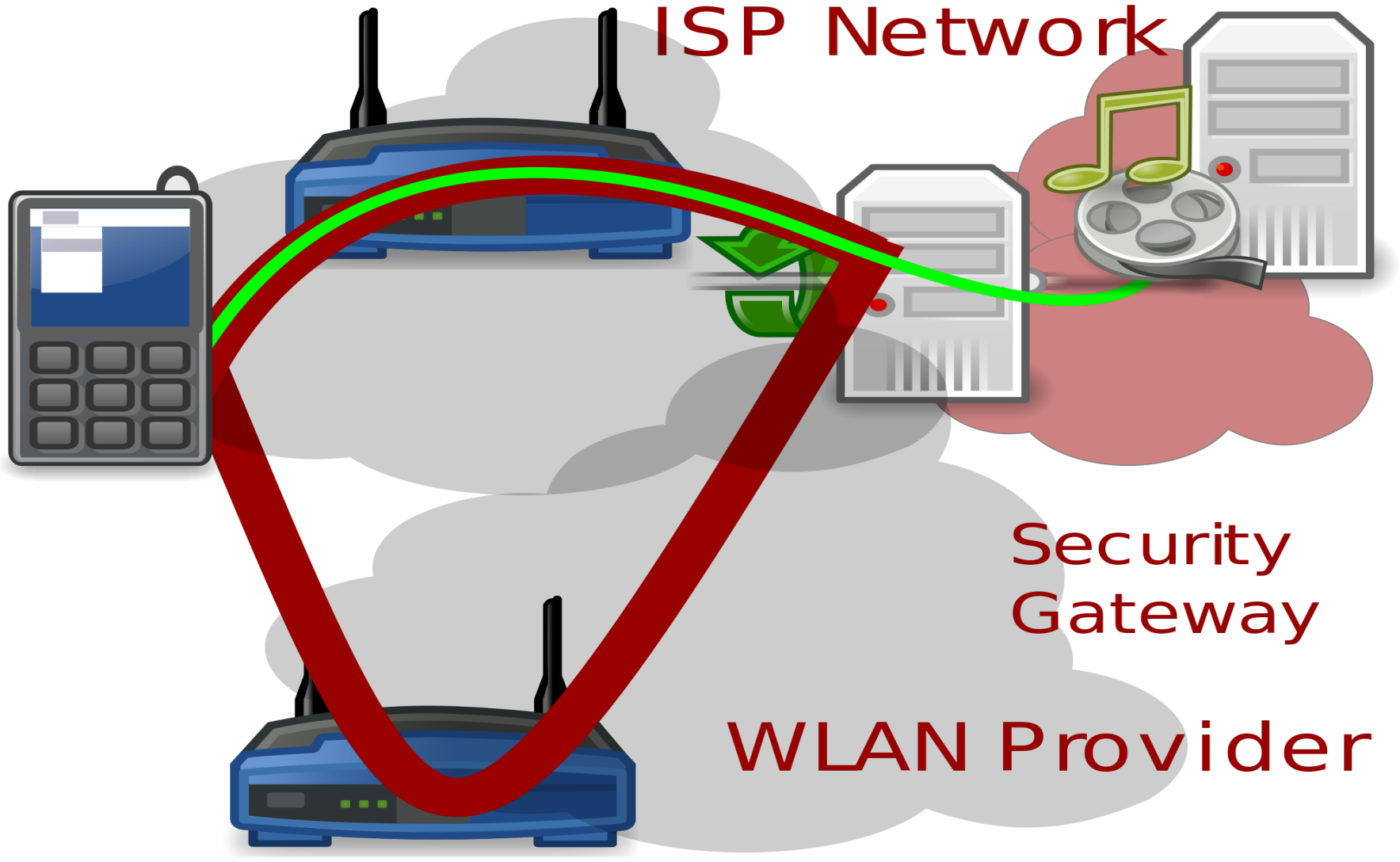
Moving Traffic (IPsec Mobility)



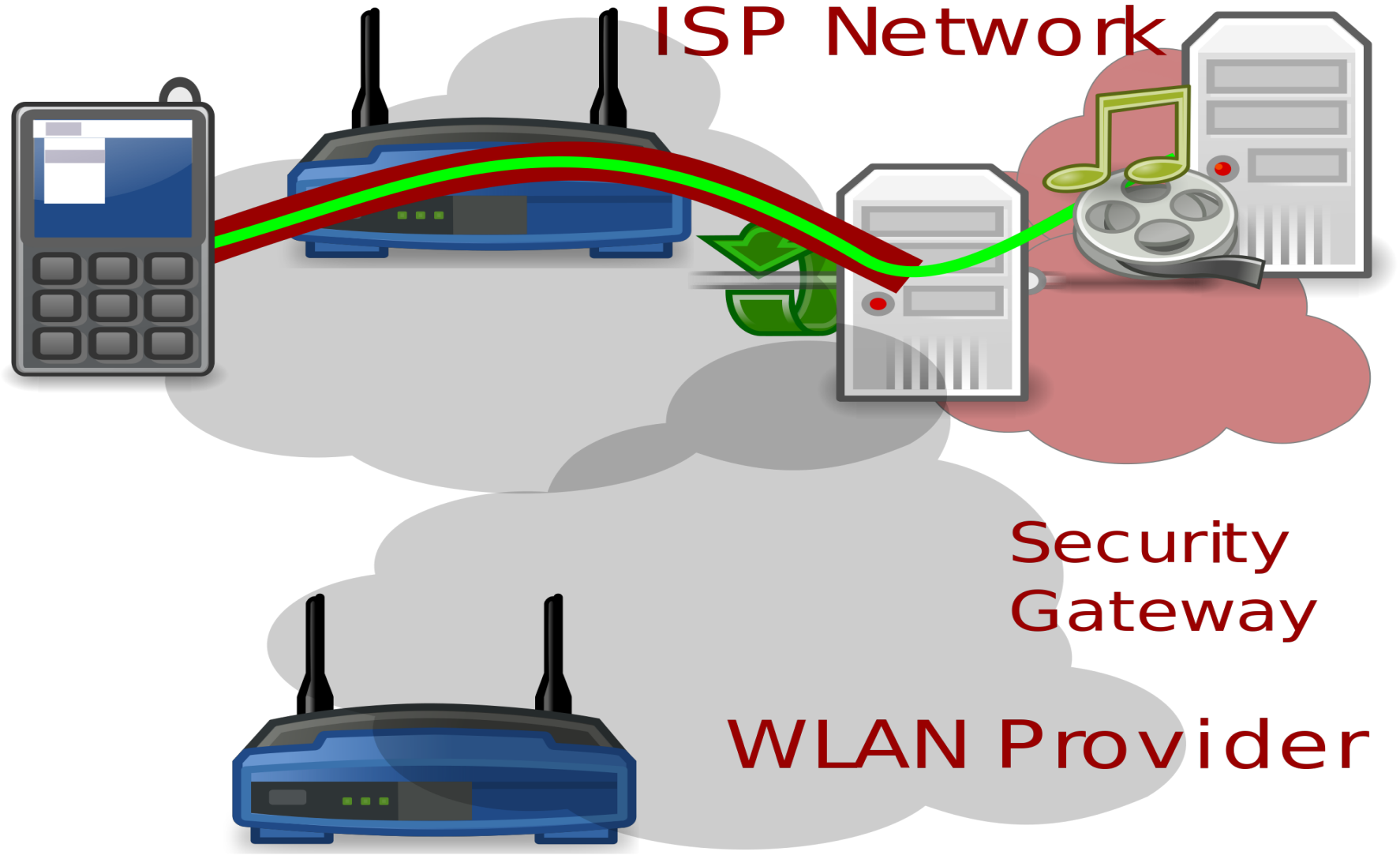
Waiting for the last packets



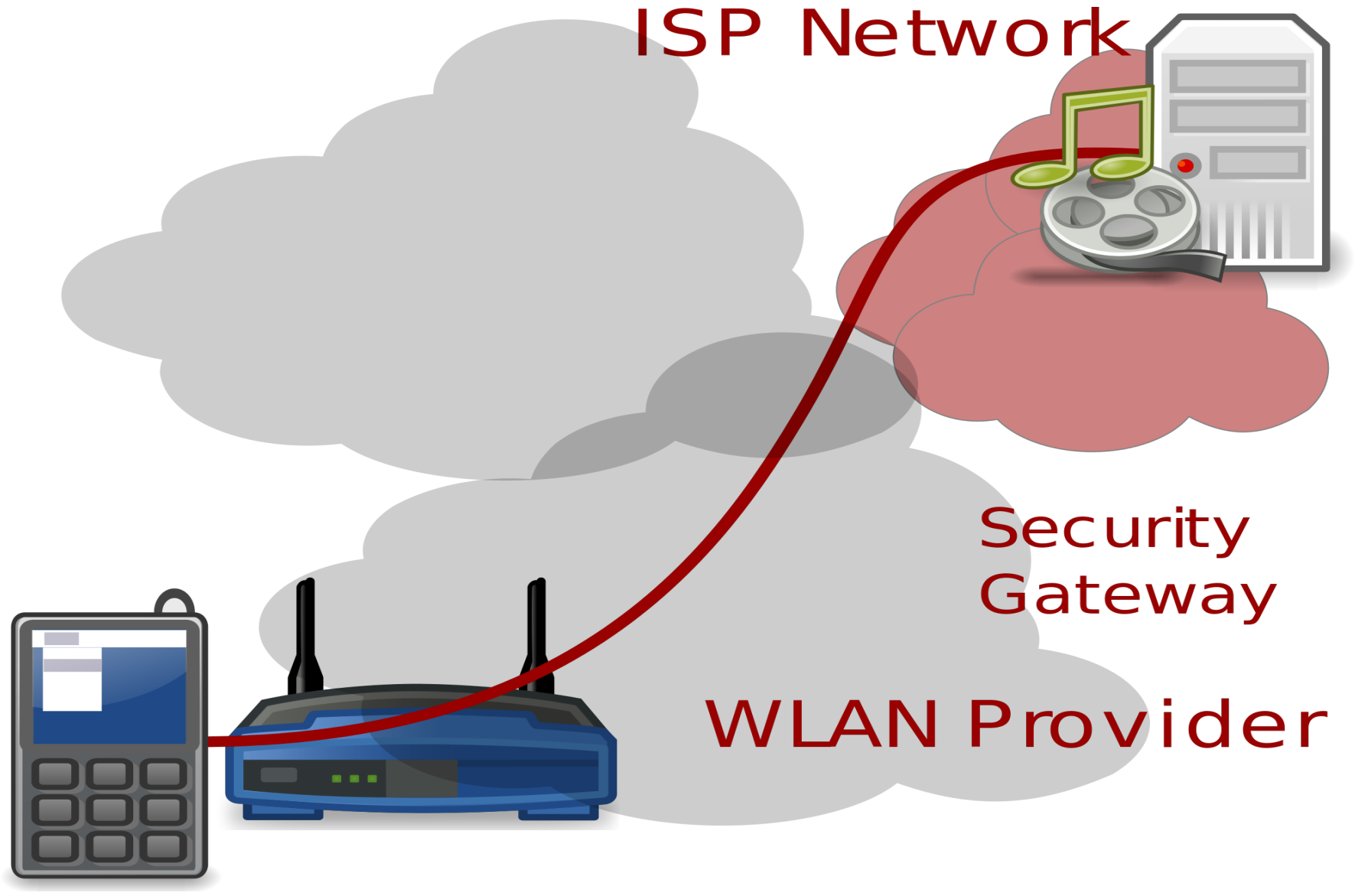
Last packets received



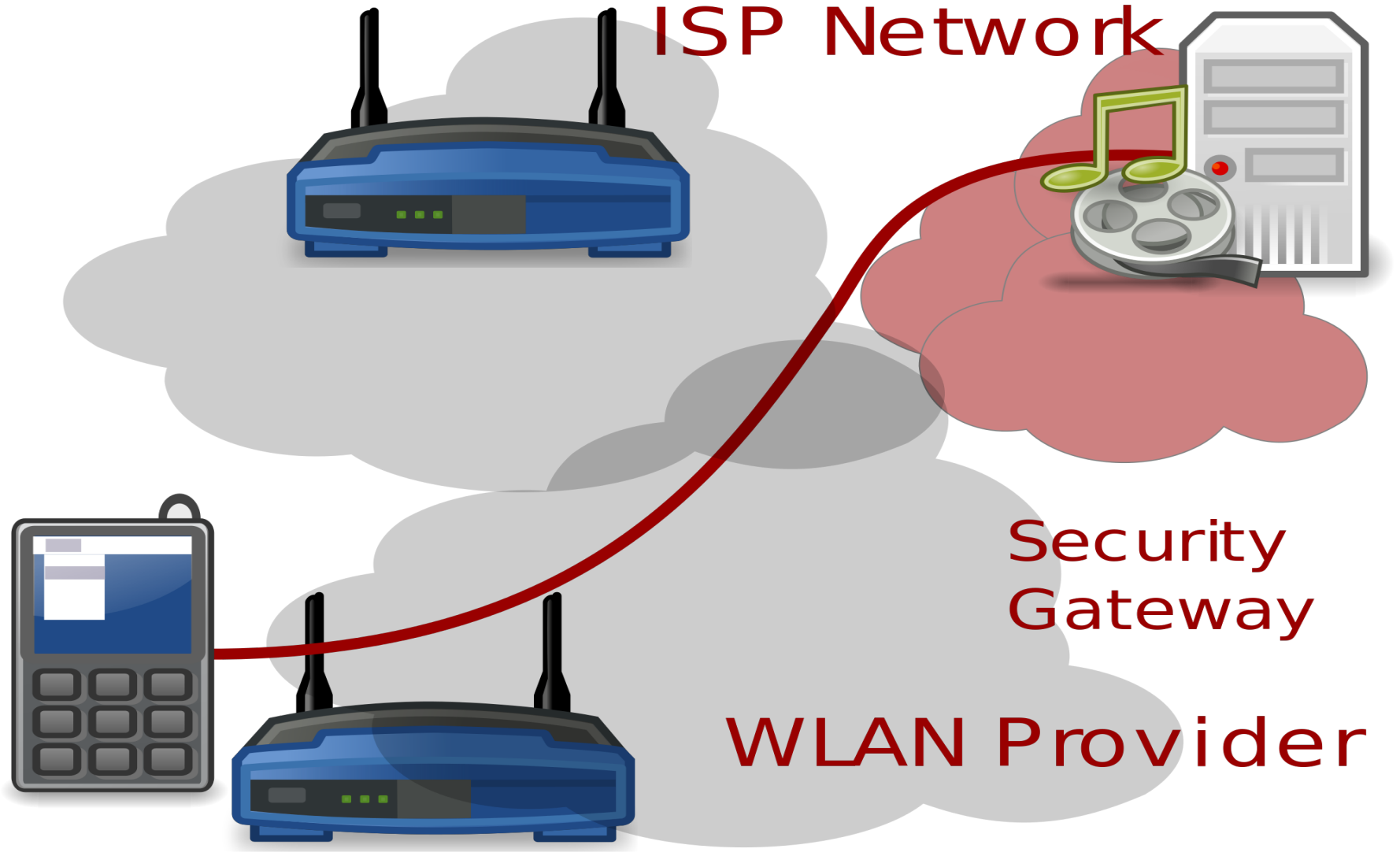
Removing the old Interface



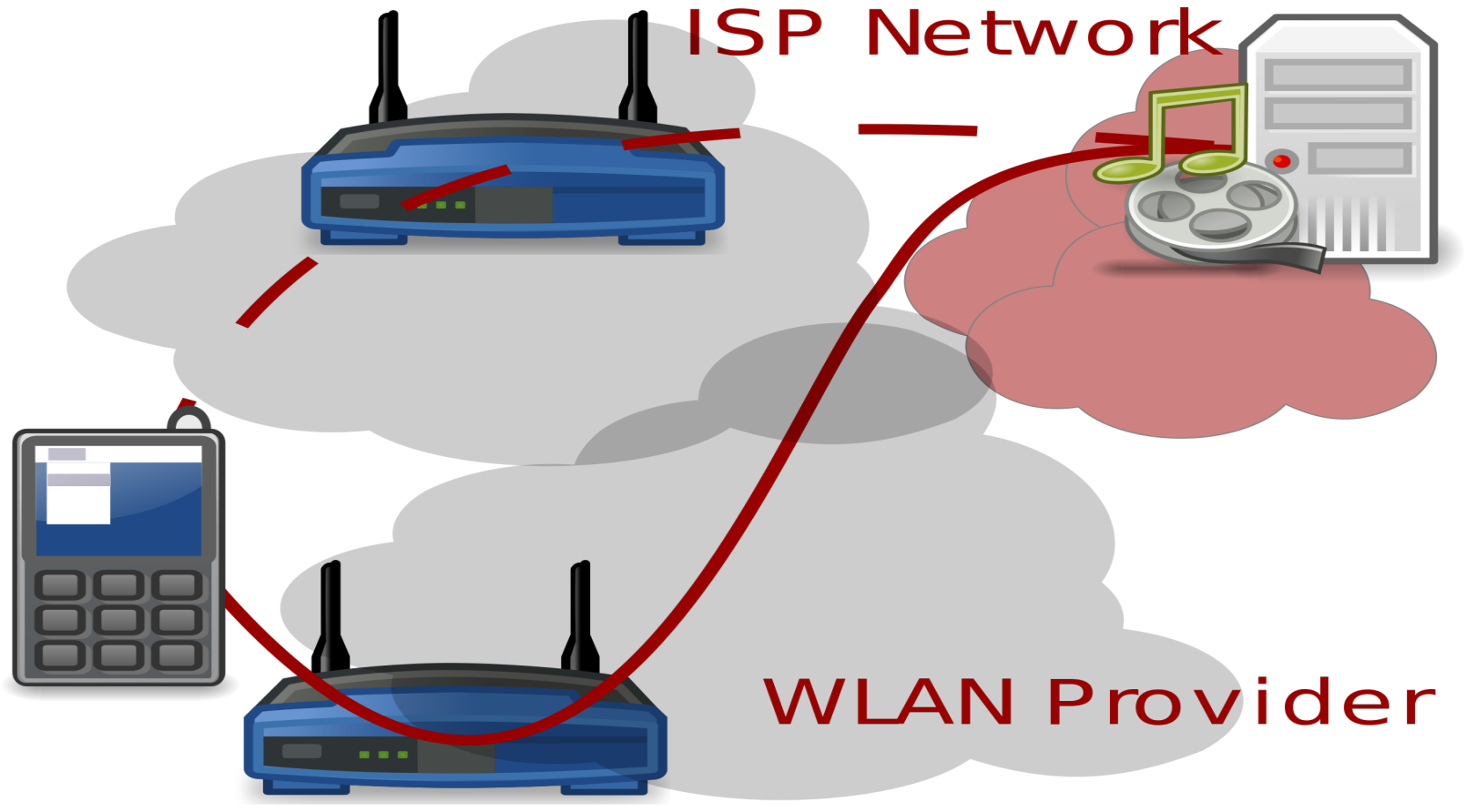
Example: ADD / REMOVE (Transport)



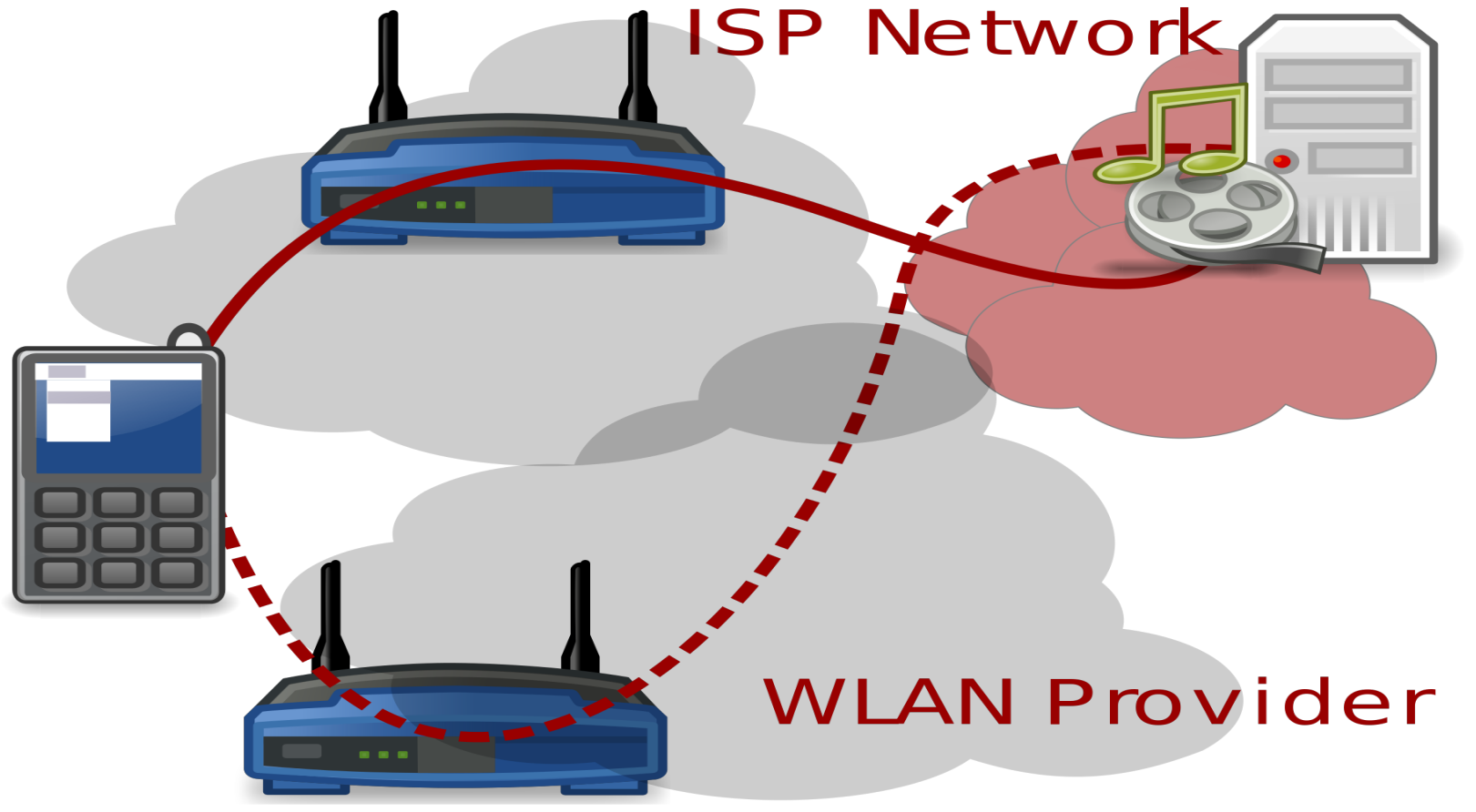
New Interface Detected



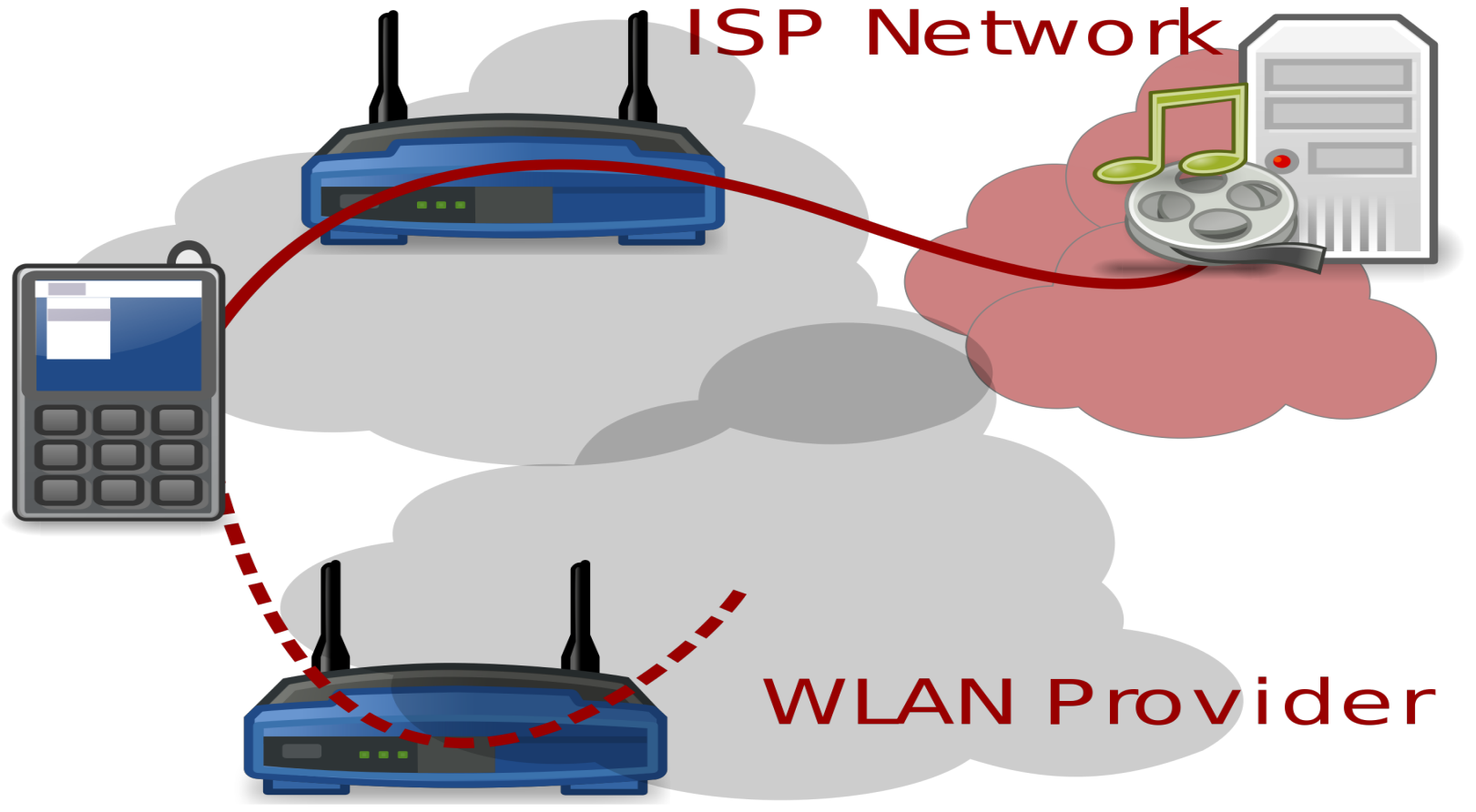
ADDing new Interface to IPsec databases



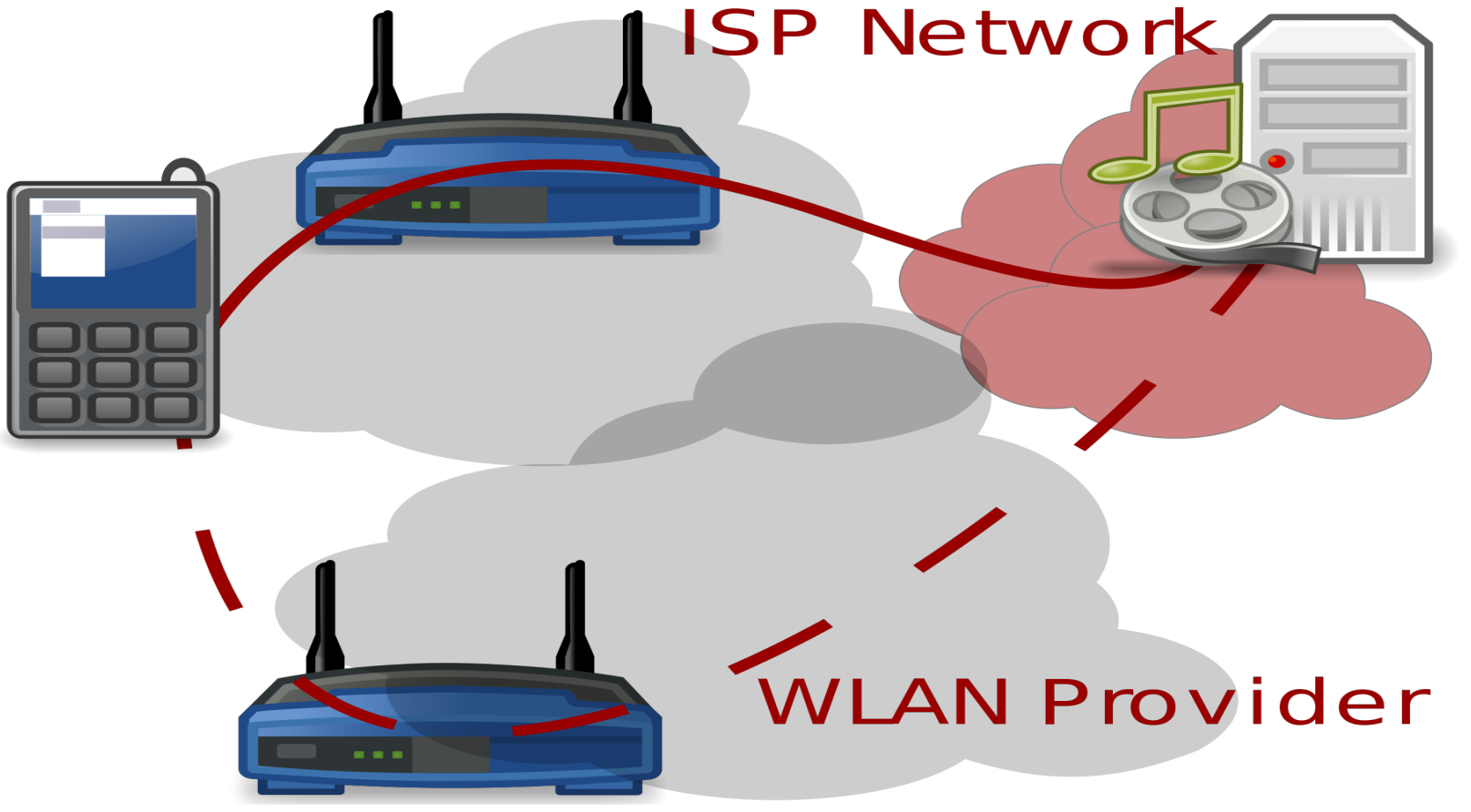
Moving Traffic (Not IPsec)



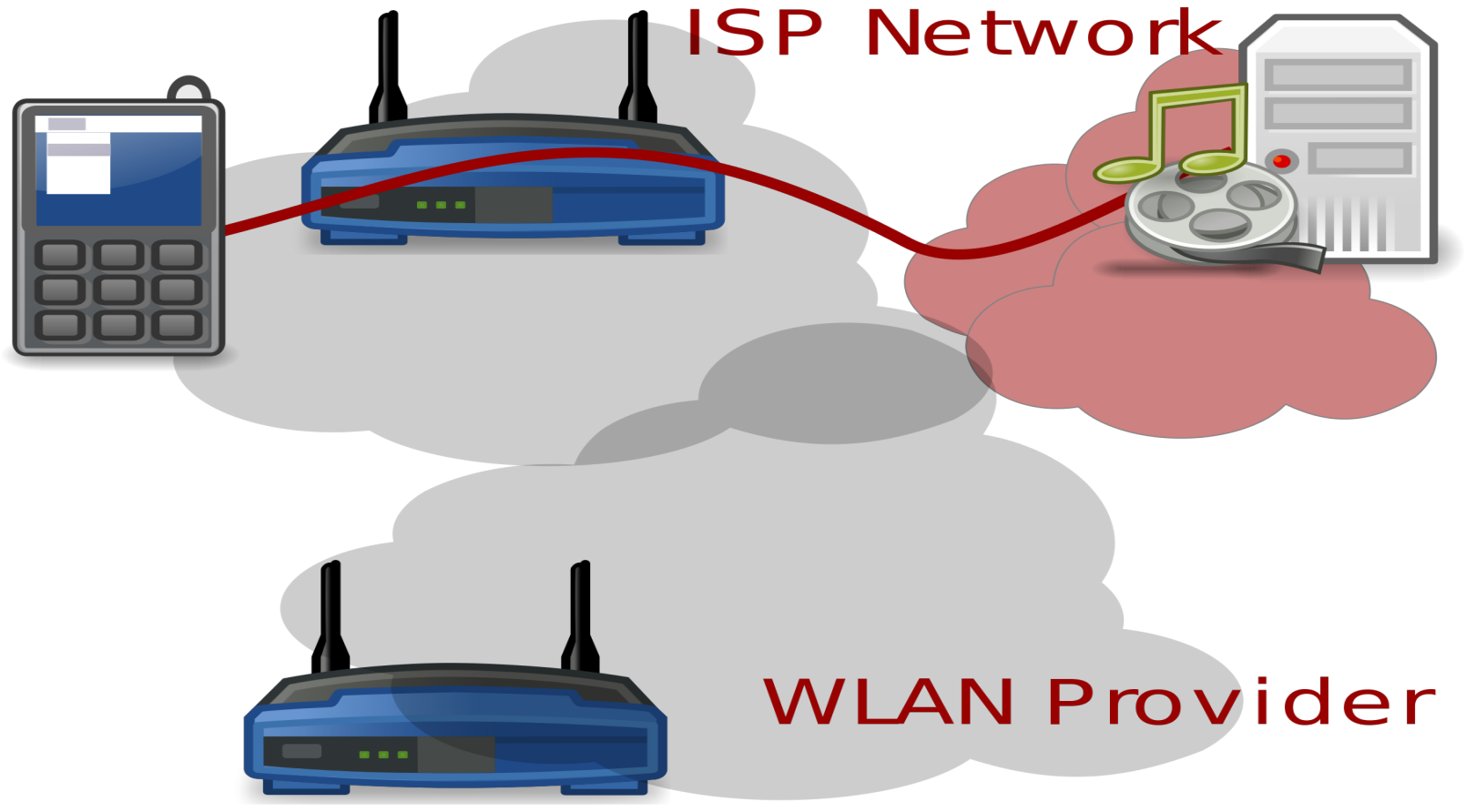
Waiting for the last packets



Last packets received



Removing the old Interface



IV. Problem Statement

The only extension for IPsec Mobility and Multihoming is MOBIKE:

- MOBIKE has been designed in 2008 for the VPN use case
- MOBIKE considers a single Interface
- MOBIKE considers only the IPsec Tunnel Mode

IKEv2 can ADD a Security Association with CREATE_CHILD:

- CREATE_CHILD is not mandatory for IKEv2
- CREATE_CHILD support is not advertised to the peers
- CREATE_CHILD is a per SA negotiation
- CREATE_CHILD is complex

IKEv2 can REMOVE a Security Association with DELETE Exchange

- CREATE_CHILD is a per SA negotiation (not Interface)

V. IPsec MIF Requirements

- Mobility, Multihoming and MIF features MUST be provided for IPsec tunnel and transport modes
- IPsec nodes can dynamically ADD a new Interface for IPsec protected communications
- IPsec nodes dynamically REMOVE an old Interface for IPsec protected communications
- IPsec nodes can perform soft and hard handover
- IPsec nodes can select the IPsec Security Association an action occurs

Next Steps

- Get feedbacks: version 2 considered the multiple feedbacks we had in the Paris IETF
- Starting designing an IKEv2 Extension for these requirements
- Is there any interest in working on this document?