Offering a Multicast Delivery Service in a Programmable Secure IP VPN Environment

Lina ALCHAAL

Netcelo S.A., Echirolles
INRIA Rhône-Alpes,
Planète project, France
lina.alchaal@inrialpes.fr

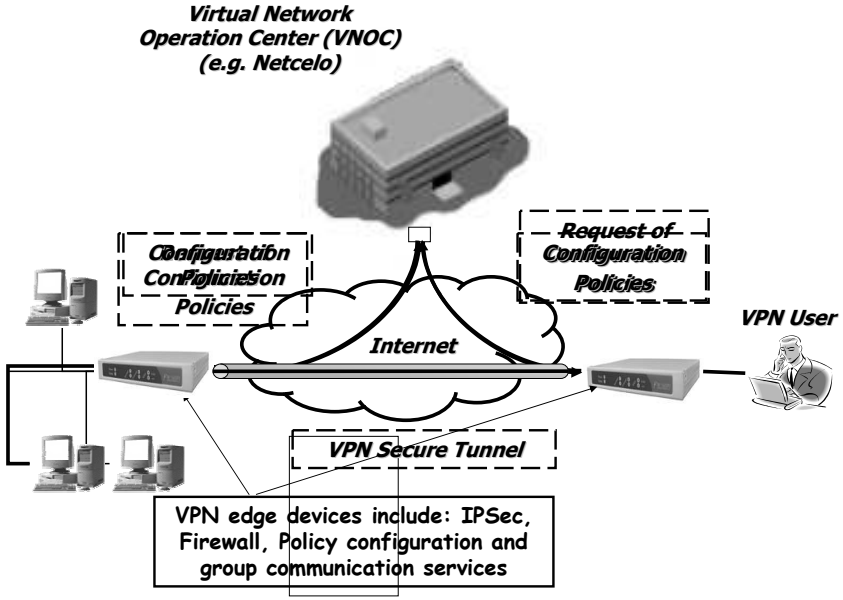
Vincent ROCA

INRIA Rhône-Alpes,
Planète Project, France
vincent.roca@inrialpes.fr

Michel HABERT

Netcelo S.A.,
Echirolles, France
michel.habert@netcelo.com

Introduction: a centralized environment



Introduction

Goal of the work:

offer a group communication service in this fully secure VPN environment

Different from work at IETF MSEC

opposite approach… in our case the environment is already secure!

Different from work at IETF PPVPN (provider provisioned VPN)

in our case we target a VPN service provider who doesn't master the core IP network

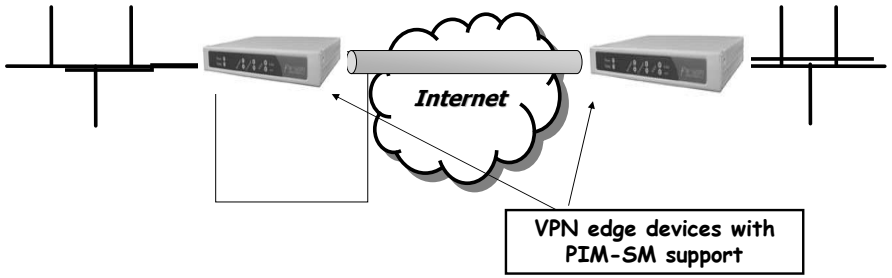
Outline

1. Experiments with Multicast Routing Protocols in a VPN Environment
2. IVGMP in a VPN environment
3. Conclusions

1- PIM-SM in an IP VPN environment

We tried to deploy PIM-SM on VPN edge devices

pimd (University of Southern California/Information Sciences Institute)
Free/SWAN IPSec implementation
Linux / Lanner FW500-ME embedded PC



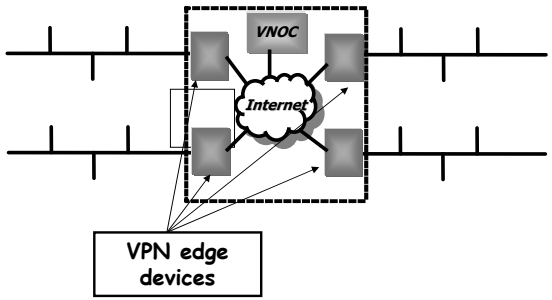
PIM within IP VPN Environment… cont'

Problems:

- PIM-SM and IPSec ignore each other…
  - multicast flag not set for IPSec interfaces
  - two independent routing tables
  - PIM doesn't register itself to IPSec and vice-versa
- Free/SWAN IPSec implementation doesn't support a security association (SA) with a multicast destination address
- PIM is very complex compared to the simplicity of a VPN environment

2. IVGMP in a VPN environment

- **IVGMP benefits from the centralized VPN architecture around the VNOC**
  - close integration of group communication & VPN management
- **Avoids the complexity of Multicast Routing Protocols**
  - a VPN topology is much simpler than the Internet mbone
  - shares some similarities with overlay multicast solutions !

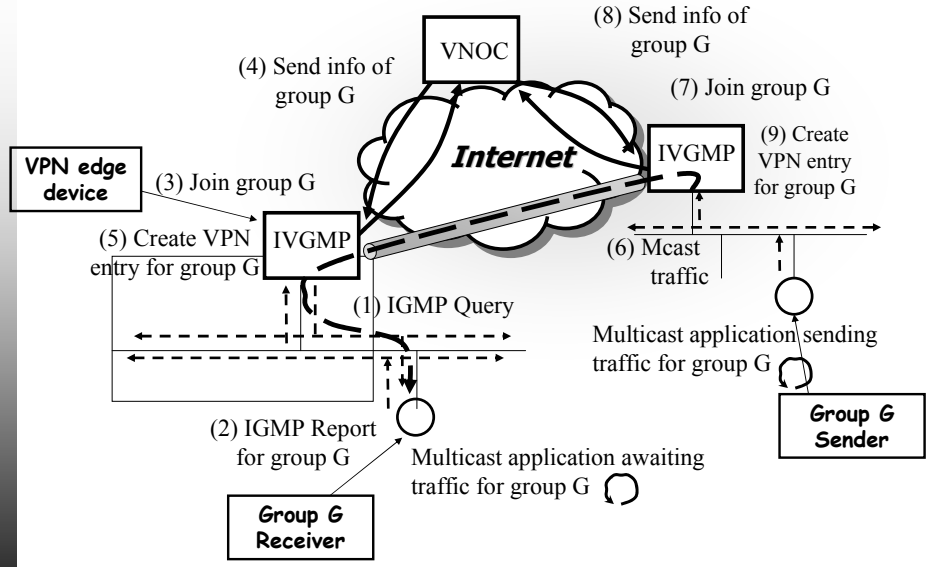


IVGMP features

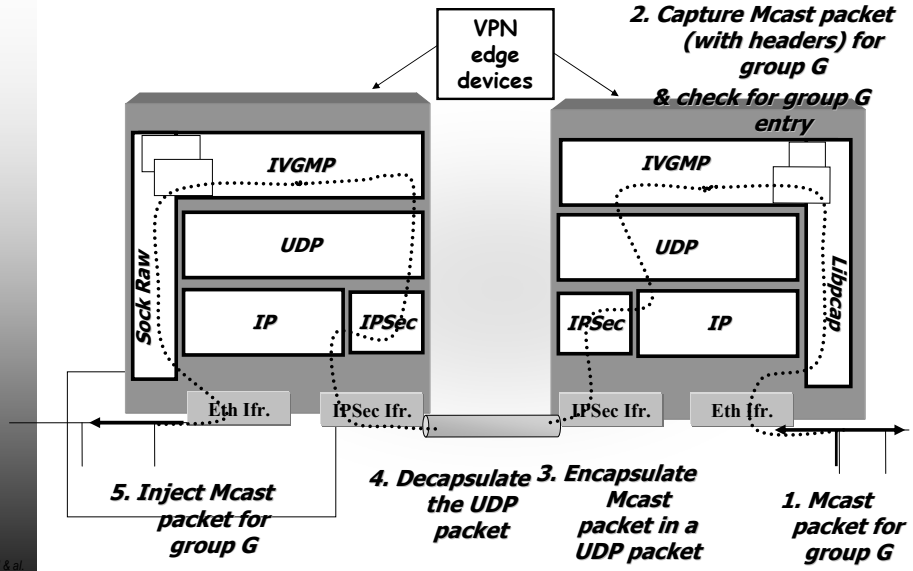
IVGMP functions:

- **dynamic discovery of group members/sources located in local subnets**
  - use IGMP queries / traffic listening
  - more or less easy, depending on the site configuration (single LAN vs.
- **add/remove a site dynamically to a group VPN**
  - … with the help of the VNOC
  - depends on the presence or not of receivers/sources
- **send multicast packets to other sites belonging to the same group via IPSec tunnels**

An example…



The implementation

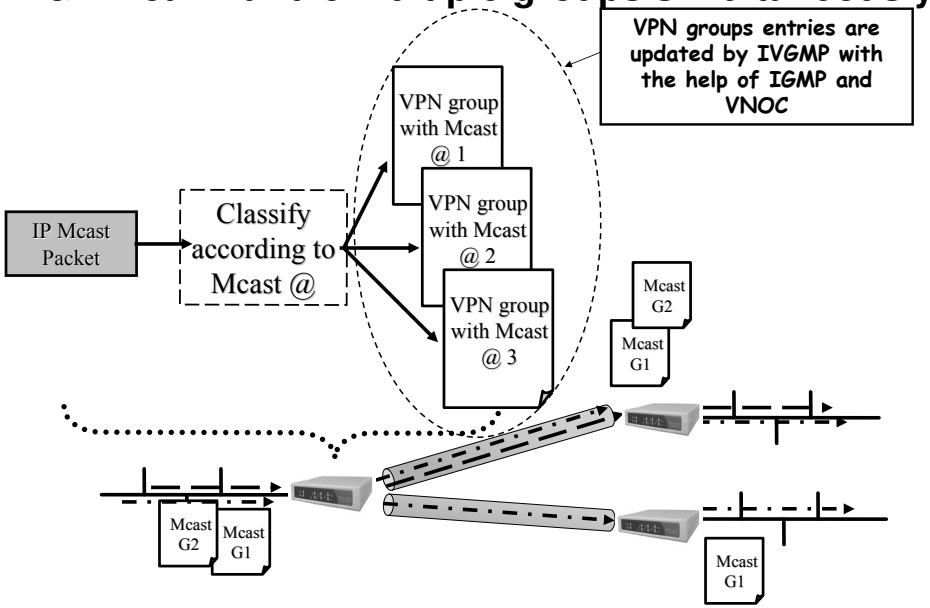


IVGMP advanced features

IVGMP goes beyond these simple examples…

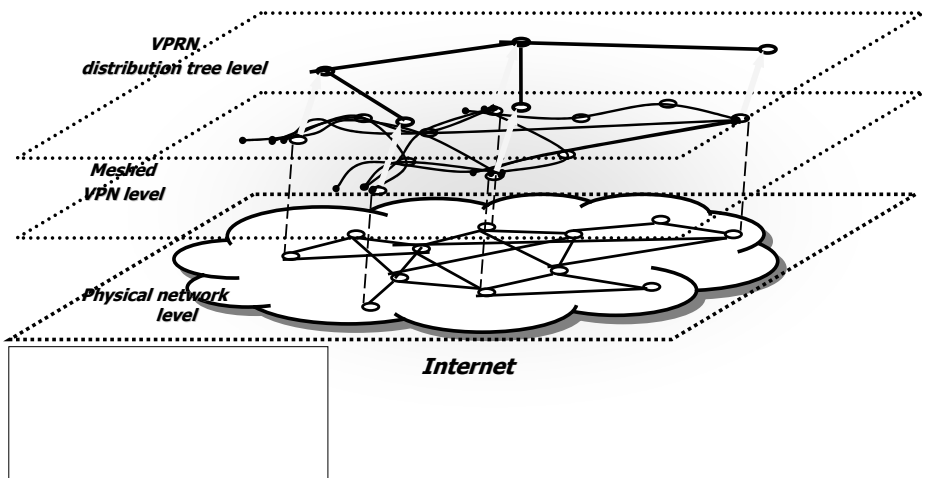
Handling multiple groups

IVGMP can handle multiple groups simultaneously



Scalability Improvement

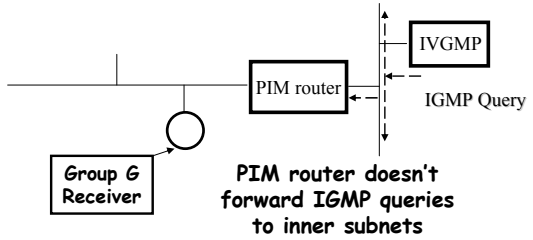
Scalability problem can be addressed by provisioning some sites (or dedicated servers) as VPRN nodes that perform traffic forwarding



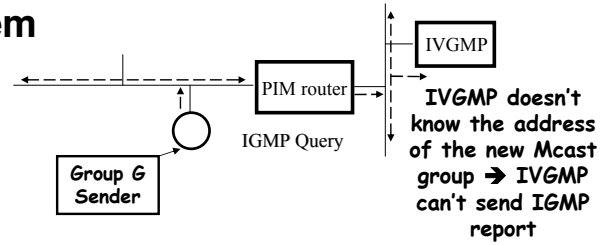
IVGMP and Mcast routing Protocols Interoperability

When a site is composed of several subnets supporting a multicast routing protocol…

- **Receiver problem**



- **Sender problem**



IVGMP and Mcast routing Protocols Interoperability… cont'

Possible solutions…

- **Use IGMP-proxying on inner subnets routers:**
  - Solves only the « receiver problem »
  - Requires some administration work on clients sites ☹
- **Predefine a small number of multicast groups**
  - Solves only the « source problem »
  - Might be used with the first solution , but increases IGMP signaling
- **Use a dedicated application to inform the local IVGMP of new multicast groups**
  - Doesn't require any modification to the internal site
  - It's the responsibility of users to announce new groups

3. Conclusions

This approach :

- **gets out with a simple way to manage a communicating group sparsed over the Internet**
- **offers a secure multicast delivery service over the Internet**
- **is fully dynamic**
- **is fully transparent to the end users/applications**
  - ➔ No configuration burdens on group members

Many thanks for your attention!

VPRN Definition

A VPRN consists of a mesh of IP tunnels between ISP routers, together with the routing capabilities needed to forward traffic received at each VPRN node to the appropriate destination site