Location/ID Separation Protocol as Solution for Enterprise Networks

Florin TEODORESCU
IT&C Security Master
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies
ROMANIA
florin.nteodorescu@gmail.com

Abstract: The increased rate of expansion and adoption of the internet has raised a lot of challenges for implementing and designing network infrastructures. Among the most important challenges we find the need to have an efficient routing and address system to cope with the increasing number of devices with internet access, and also to ensure the security of these devices against malicious attacks and prevent access to confidential data. Separating the devices identity from its location by implementing the Loc/ID Split scheme, and implementing Virtual Private Networks (VPN) offer the technical support needed to overcome these challenges and increase efficiency and lower implementation costs. The scope of this article is to analyze the benefits of using Location/ID Separation Protocol together with a VPN implementation for creating a scalable infrastructure for the internet of the feature and for secure enterprise networks. The advantages and limitation of such architecture are presented below.

Key-Words: LISP, GETVPN, GDOI, EID, RLOC, IKE

1. Introduction

The exhaustion of the IPv4 address space and the development and start of the deployment of its successor, IPv6, are a very current and much discussed subject. It's becoming very clear that an IPv6 infrastructure will be the basis of future networks and the internet.
The Internet Service Providers (abbreviated ISPs) and also the enterprise environment are beginning to realize the importance of this change and are starting to allocate budget to make the switch to IPv6, improve their networks scalability and security without lowering their live networks productivity, a vital aspect in today's competitive environment.
A goal of every company is protecting confidential information and stopping unauthorized access to its internal network to avoid financial losses caused by trade secrets theft or disruption of its networks that cause productivity and image loss.
A recent study made by Cisco [2] revealed that the majority of the top companies in IT (78%) have made, or will start to make the transition to IPv6. A large part of this migration effort (94%) has started in the last 2 years. More than half of the respondents (55%) have sought or plan to seek assistance of outside consultants during the IPv6 transition. The main concerns of this transition are security vulnerabilities (60%), maintaining the transition technologies (53%) and implementing the transition technologies (50%).
A solution for securing enterprise networks are Virtual Private Networks (VPN) [1] that use a shared medium, like the Internet, to interconnect regional offices or to provide remote access to telecommuting workers.
VPNs are implemented using encryption and decryption mechanisms to ensure information confidentiality, non-repudiation and integrity for the data that passes through the network. Traditionally there are two types of VPN: site to site VPN and remote VPN. These technologies usually work with IPsec in tunneling mode.

2. Problem Formulation

A basic observation made as far back as the early stages of research and development of the early networks is that using only one identifier for both the device itself and for routing can be problematic, and ineffective.

ISSN 2067 – 4074

To successfully identify a device as a valid endpoint of a connection, the address that identifies the device should not change as the device moves from one place to another (for example, moving from home to work) or if the internet connection of a device is changed from one ISP to another. However, it is not feasible to track the position of billions of devices every second, worldwide, using only the current used addresses that are not that flexible. That is why a device needs an address that is in close correlation with the location it is in so it can benefit from an efficient, scalable routing solution.

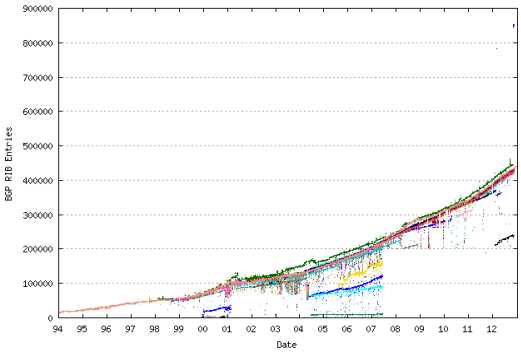

Figure 1. The rise in the number of entries in the BGP routing table

The almost exponential growing rate of the size of the BGP routing tables raises the problem of the sustainability and scalability of such architecture, and makes us rethink the way the internet infrastructure and tomorrows networks should be developed.

But the problems don't stop at the size of the BGP routing tables. In the past 15 years, the IPv4 protocol has suffered some changes, arising from identifying some issues and functional needs, such as the Classless Inter-Domain Routing (abbreviated CIDR [4]), or Private Allocated Addresses [5] and Network Address Translation (abbreviated NAT). These have delayed the development and deployment of IPv6. Until now, these solutions have been seen as low cost alternatives to a full migration to an IPv6 infrastructure, by delaying the IPv4 exhaustion and reusing the existing address space in a more efficient way. This seems a good solution but comes as the cost of an increase in configuration and management complexity.

In the past, strictly from a business point of view and from the point of view of the amount of generated revenue, the deployment of IPv6 was very hard to justify, and was very hard to obtain capital expenditure (abbreviated CapEx) or operating expenditures (abbreviated OpEx) for this transition.

But now, with the recent exhaustion of the IPv4 address space, and with the continuous expansion and growth of e-commerce, the need to transition to IPv6 has a solid ground and is starting to get the necessary support.

3. Problem Solution

3.1. LISP

The Location/ID Separation Protocol can stand at the base of a revolutionary routing architecture and at the same time can enable the enterprise environment and Internet Service Providers to simplify multi homing, facilitate WAN scalability, support virtual machine mobility in data centers, reduce system complexity, and at the same time facilitating the transition to IPv6.

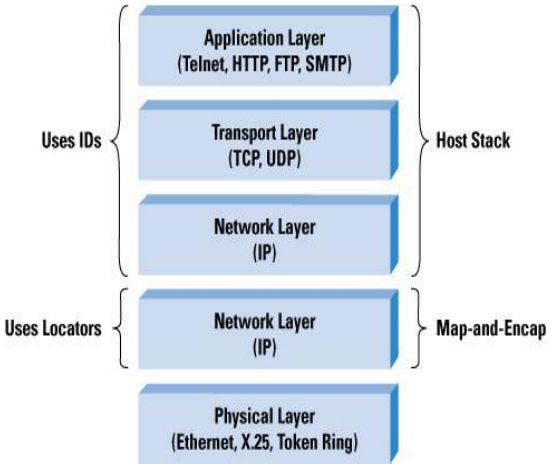

Figure 2. Packet encapsulation in the LISP header

The objective of LISP, as a specific implementation of the Loc/ID split, is to decouple the location of the device from its identity. This split will facilitate improving the RLOC address space aggregation, will implement identity persistence in the EID space and in some cases will improve security and efficiency of the motilities in the network

The following are components of the LISP architecture:

- ITR – Ingress Tunnel Router – is responsible for finding EID-to-RLOC mappings. When a packet destined for an EID is received, it checks that it knows the location of this EID from its cache. If it finds an entry in its cache, it encapsulates the packet with a LISP header, and uses a RLOC as a source IP, and one of the RLOCs in its mapping cache as the destination IP. Then it routes the packet normally.
- ETR – Egress Tunnel Router – sits at the edge of a network that has LISP support, registering EID-to-RLOC mappings for this site, answering Map-Request messaged and removing the LISP header and sending LISP encapsulated data to devices in that site.
- EID – End Point Identifier – is the identifier of a devices identity
- RLOC – Routing Locator – is the identifier of a devices location
- MS – Map Server – is a server of LISP mappings that implements the distribution of mappings databases in the network.
- MR – Map Resolver – accept LISP encapsulated Map-Request messages sent by the ITRs, it removes the LISP header and then it sends the message further over the ALT-LISP infrastructure to the ETR that that has the requested EID.

3.2 LISP Alternative topology

There are a number of protocols that implement the Loc/ID split [3]:

- LISP (or LISP- ALT)
- Identifier-Locator Network Protocol (abbreviated ILNP) – that includes only IPv6 and RRG requirements and advices
- Evolution (architectural design and RRG recommendations)
- Content-centric networking (Ron Spring 2011 - Named Data Networking, Ronald van der Pol (SARA))

Going forward we will focus on an alternative topology for Location/ID Separation Protocol, called LISP Alternative (abbreviated LISP-ALT) and identify its key aspects and differences from the original LISP implementation.

The main idea behind LISP Alternative is to build an alternative logical topology on top of the existing one to facilitate a more efficient management of EID-to-RLOC mappings for LISP. This logical topology uses already existing technologies and tools and has little to no impact on the existing architecture. It uses the Border Gateway Protocol (abbreviated BGP) together with the Generic Routing Encapsulation protocol (abbreviated GRE) to build a new overlaid network layer, which is made out of devices that have a sole purpose, to help EID prefixes provisioning.

LISP-ALT does not require any changes whatsoever in the BGP and GRE protocols. LISP-ALT is a hybrid of the push/pull architecture. The EID prefixes are pushed through the LISP-ALT routers and/or to ITRs. The specific EID-to-RLOC mappings are then pulled by the ITR by using Map Request messages of Data Probes messages. In both variants, these messages are routed over the alternative topology and result in replies generated by the ETR.

In these conditions, the main idea behind the LISP-ALT protocol is to use BGP over GRE, to build a network that can be used to route the Data Probes, Map Requests and Map Reply messages. The ALT Routing Information Base (abbreviated RIB) is made out of EID prefixes and associated next-hop addresses. LISP-ALT routers use external BGP (eBGP) to communicate with other LISP-ALT routers in order to propagate the updated EID prefixes that are learned using the eBGP connections, from the authoritative ETR or by direct, static configuration.

The access points to the EID prefixes are passed as Network Layer Reachability Information (abbreviated NLRI), without any change, because the EID address space has the same syntax as the IPv4 or IPv6 IPs.

ISSN 2067 – 4074

A single LISP-ALT router at the edge of a network can learn all the EID prefixes that are originated by the authoritative ETRs. In general, LISP-ALT routers aggregate EID prefixes and propagate them using Data Probes messages, or Map Request and Map Reply messages.

3.3 GETVPN

Networks today need to support all forms of media, including data, voice, and video in order to enhance business communications and lower operating costs. Voice and video applications are accelerating the need for instantaneous, branch-to-branch communications, while network security risks are increasing.

In an environment in which network security has become a strategic factor in the success of a business, enterprise network have implemented point to point based security models by using technologies such as VPN (Virtual Private Networks). The LISP configured environments make no exception from this rule, one of the ideal solution to secure this type of network is the CISCO GETPVN solution.

The Cisco Group Encrypted Transport VPN (abbreviated GET VPN) is a IPSec based, tunnel-less solution that has all the benefits of traditional VPN, but brings many advantages over them, and even over other proprietary Cisco solutions like DMVPN (Dynamic Multipoint VPN). These new functionalities improve the ease of configuration and management of these network infrastructures.

This technology introduces the concept of group association (group AS) to eliminate the need for point to point tunneling and the need to create an overlaying routing infrastructure.

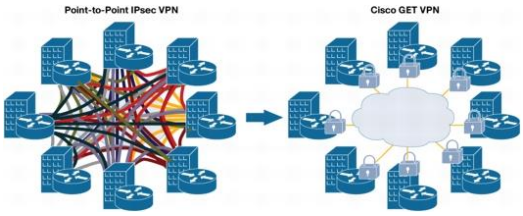

Figure 3. Tunnel-less VPN network using GETVPN

All the group members (abbreviated GM) have the same security group associations (Abbreviated GSA) that allow them to decrypt the traffic generated by other group members, without the need to negotiate a full mesh connation between all the members of the group.

The main benefits of the GETPVN technology are:

- Creating a full-mesh connectivity network between the group members by using the IPSec group security associations.
- GETPVN uses the already existent routing infrastructure
- Easily integrates with the multicasting infrastructure without having multicast replication issues that can be found in traditional tunnel based IPSec solutions.
- Source and destination IP preservation during the encryption and IPSec encapsulation process, using the existing infrastructure and policies for routing
- Simplifies the instantaneous communication between branches - ensuring low latency and jitter and enabling a direct, always-on communication between sites, without the need of a central hub
- Improving security – provides network encryption maintaining at the same time the network intelligence, like full-mesh connectivity, the use of traditional routing protocols for routing the encrypted packets and quality of service (abbreviated QoS)
- Offers an increase in management flexibility by eliminating complex peer-to-peer key management

3.4 GET VPN Solution Comparison

The below table provides a basic comparison of, GETVPN and Standard IPSec VPN technology [6].

The GETVPN solution comprises of the following elements:

- GDOI [7]
- KS – Key servers
- Cooperative (COOP)KSs
- GM – Group Members
- IP header preservation
- Group Security Association (Group SA)
- Rekey mechanisms
- Time-based anti-replay (TBAR)

Table 1: Comparison between IPSec solutions

	Cisco GET-VPN	Standard IPsec VPN
	Tunnel-less VPN	**Tunnel-based VPN**
Customer Benefits	• Simplifies encryption integration on IP and Multiprotocol Label Switching (MPLS) WANs • Simplifies encryption management through use of "group keying" instead of point-to-point key pairs • Enables scalable and manageable any-to-any connectivity between sites • Supports quality of service (QoS), multicast, and routing	• Provides encryption between sites • Supports QoS
When to use	• Adds encryption to MPLS or IP WANs while preserving any-to-any connectivity and • networking features • Offers scalable, full-time meshing for IPsec VPNs • Enables participation of smaller routers in meshed networks • Simplifies encryption key management while supporting routing, QoS, and multicast	• Use when multivendor interoperability is required
Product interoperability	Cisco routers only	Multivendor
Topology	Hub and spoke; any-to-any	Hub and spoke; small-scale meshing as manageability allows
Routing	Supported; Cisco GET-VPN any-to-any connectivity capability can also be used to provide secure routing across an entire router backbone	Not supported
QoS	Supported	Supported

3.4 GDOI

The Group Domain of Interpretation (Abbreviated GDOI), IETF RFC-6407 is an integrated part of the GETVPN solution and it is used to distribute the IPSec keys to a group of VPN gateways that need to communicate in a secure way. These keys are updated constantly and distributed to all the VPN gateways buy using a process called rekey.

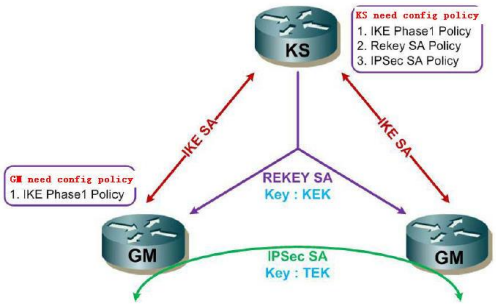

Figure 5. GETVPN topology and GDOI

The GDOI protocol uses the Internet Key Exchange Phase 1 algorithm (abbreviated IKE Phase 1). All the participant gateways need to authenticate themselves to the devices distributing the keys using IKE. After the VPN gateways are authenticated and receive appropriate security keys via IKE SA, the IKE SA expires and GDOI is used to update the GMs in a more efficient and scalable way.

GDOI uses two different encryption keys: one key for securing GET VPN control plane (this is the Key Encryption Key - KEK) and the other key to secure the data traffic (this one is called Traffic Encryption Key - TEK).

4. Conclusions

LISP is an evolving technology that has many variants and alternatives of implementation, and can undergo changes and improvements until getting to a certain maturity that can make it suitable for implementing in live/production networks.

Besides providing increased scalability, LISP offers other interesting features that enable easy transition to IPv6, an increase in security or enable device mobility.

Perhaps the most interesting functionality of this protocol is that it does not interfere with the existing network architecture and does not need any hardware changes but only minimal software updates.

Furthermore, this protocol allows the use of other new protocols that can further enhance its functionality, as it is in the case of GETVPN. But nothing can stop us to think of many other combinations or to think that LISP cannot be used with future technologies.

The ease with which this protocol is configured and administered with the minimal changes that it brings, make it a viable solution for the future of the

ISSN 2067 – 4074

internet, and enterprise networks, whatever it may be.

Acknowledgment

Parts of this research have been published in the Proceedings of the 6th International Conference on Security for Information Technology and Communications, SECITC 2013.

References

[1] IETF, RFC 2341- IP Based Virtual Private Networks, online, http://www.ietf.org/rfc/rfc2341.txt
[2] Industrial Ethernet Book Issue 65 / 99, Cisco
[3] B. Overeinder (NLnet Labs) Jac Kloots(SURFnet) – “Future Internet”
[4] IETF, RFC 4632, Classless Inter-domain Routing (CIDR), online, http://tools.ietf.org/search/rfc4632
[5] IETF, *RFC 1918 - Address Allocation for Private Internets*, online, https://tools.ietf.org/html/rfc1918
[6]11/06 - Cisco at a glance - Cisco Site-to-Site VPN Technologies Comparison
[7] IETF, RFC 6407 - The Group Domain of Interpretation, online, http://tools.ietf.org/search/rfc6407