An IPSec mediation approach for safe establishment of inter-domain VPNs

Alexandre Matos, Fernando Matos, Paulo Simões, Edmundo Monteiro

CISUC – Informatics Engineering Department, University of Coimbra
Coimbra, Portugal
{aveloso, fmmatos, psimoes, edmundo} @ dei.uc.pt

Abstract. In this paper we propose a new solution to increase the security of BGP/MPLS IP VPNs established across multiple domains. In general, layer 3 VPNs already present a number of security risks when used in single domain scenarios, since they are vulnerable to attacks originated inside the provider backbone. In order to overcome these risks, IPSec tunnels are recommended. In multi-domain scenarios, however, the safe establishment of such IPSec tunnels is much more difficult, due to need to set up proper Security Associations in an open environment. The solution we present in this paper not only solves this problem but also improves the dynamic composition of multi-domain VPNs, thus reducing the effort and time required to provide such VPNs.

Keywords: Inter-domain VPN, IPSec, BGP/MPLS, SOA, Business Layer.

1 Introduction

A Virtual Private Network (VPN) is a solution to restrict communications among a set of endpoints, aiming to provide confidentiality even on public networks [1]. They often provide a cost-effective alternative to private leased lines, and Internet Service Providers (ISPs) currently offer managed VPN services to a wide range of clients, as a means of market expansion and revenue generation.

VPNs are generally classified as Layer 2 VPNs (L2VPNs) and Layer 3 VPNs (L3VPNs). While the former focuses on features of Layer 2 such as the virtual circuits of ATM and Frame Relay networks to provide the architecture for a VPN, the latter is based on IP tunneling to create private channels over shared networks. As L3VPNs are directly associated to the Internet, they have been most widely addressed on research projects and deployments [2].

BGP/MPLS IP VPNs [3] are a particular method through which an ISP may provide a L3VPN to customers through an IP backbone. In a simpler scenario, BGP (Border Gateway Protocol) and MPLS (Multiprotocol Label Switching) are used by an ISP to provide a collection of private channels that connect distinct customer networks. While BGP is used to distribute routing information between devices at the

edge of the provider networks (designated as Provider Edge: PE), MPLS is used to forward VPN traffic.

A customer must have one or more devices that interconnect its network to the ISP network. This is the case of enterprises whose general interconnection to an Internet backbone is supported by an ISP. The reason for this is that with ISP-managed VPNs the customer side does not need to be involved in the establishment of tunnels. Nevertheless, the customer must still supply information about which interface (or sub-interface) should be used as the endpoint of the VPN.

When compared with L2VPNs, L3VPNs provide an important advantage: they can be used in multi-domain scenarios, where each VPN endpoint is connected to a different ISP [4]. In these scenarios several providers (ISPs providing the VPN endpoints and carriers interconnecting those ISPs) cooperatively provide the VPN service. This cooperation is generally based on manual and inefficient exchange of technical and business data between provides, although a few solutions have already been proposed to improve this process [5].

As noted by [6], basic security requirements are addressed both by L2VPNs and BGP/MPLS IP VPNs. However, risks associated with BGP/MPLS IP VPNs are increased by the lack of encryption, which may compromise integrity, confidentiality and authentication. Other drawbacks should be noted, namely the lack of intrinsic protection against misconfiguration and/or attacks inside the core provider network.

Security mechanisms to bypass the aforementioned vulnerabilities have been proposed [6, 8, 9]. All these proposals suggest the incorporation of IP Security Protocol (IPSec) tunneling. However, IPSec requires the establishment of Security Associations (SA), which can become a complex problem with multi-domain scenarios in perspective.

In this paper we present a solution to handle the establishment of SA in multi-domain scenarios.

In a previous work [5] we presented a Business Layer (BL) approach (the Global Business Framework: GBF) for support of dynamic, on-demand multi-domain VPNs. GBF provides a way to dynamically build VPNs, based on automated negotiation of technical and business parameters between providers and collaborative management of the VPN lifecycle. This solution drastically reduces the time and cost of current procedures, based on ad-hoc, manual interactions between providers. GBF is a general business framework, in line with initiatives such as IPsphere [10] and with concepts like Next Generation Networks (NGN) and Future Internet (FI).

Now we propose a solution for the problem of safely providing SA for the dynamic establishment of managed VPNs in multi-domain scenarios, where a key challenge needs to be addressed: how can a reliable communication channel be established between entities unknown to each other?

The rest of this paper is organized as follows: Section 2 discusses security issues encompassing BGP/MPLS IP VPNs. Section 3 presents the current approaches to the dynamic establishment of SA. In Section 4 there is a discussion about security requirements in a Business Layer context. Section 5 discusses implementation topics and in Section 6 we evaluate the proposed framework. Section 7 concludes the paper.

2 Security issues of BGP/MPLS IP VPNs

Figure 1 presents the key architectural elements of a BGP/MPLS IP VPN. Each customer site has an edge router (Customer Edge – CE) which is the frontier device connected to the provider PE. The PE establishes the new VPN through the setup of a VRF (Virtual Routing Forwarding), which is a routing table established for each VPN. Each VRF will be associated to a distinct interface (or sub-interface) and this association allows the correct routing of each packet, according to its source.

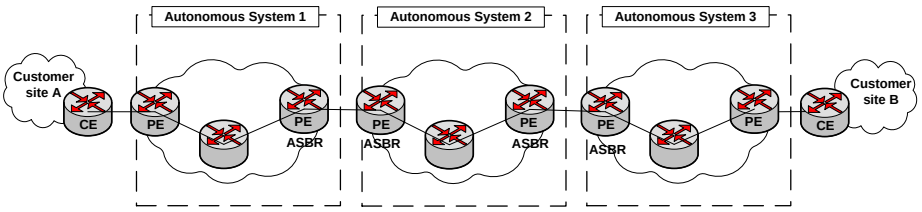

Fig. 1. Inter-domain BGP/MPLS IP VPN (Architectural Elements)

In general, VPN networks should address four typical security requirements [6]: non-intersection of address space, routing and traffic flows between VPNs; hiding of infrastructure details of the core network; resistance to attacks; and protection against label spoofing (particularly concerning MPLS VPNs).

Although BGP/MPLS IP VPN are considered as safe as traditional L2VPNs, the secure connection, which is a feature ultimately expected by a VPN customer, may be not guaranteed. All the traffic flowing through such VPNs is delivered in clear format. This means specific links along the path can be exploited in order to interrupt, corrupt or eavesdrop the VPN traffic.

In this context, CE and PE devices should receive special attention. In order to establish a new VPN, a CE may send route announcements to its PE (actually, announcing a route includes communicating a VPN IPv4 address to the PE). Two prefixes are carried within this address: Route Distinguisher (RD), which is a prefix that makes a VPN unique, and the IPv4 family address of the CE domain. To reduce potential risks, access to PE – on the CE-PE link – should be protected by the use of Access Control Lists (ACL), as suggested by [6], or through an approach to achieve confidentiality, such as IPSec tunneling [8, 11]. These security mechanisms must guarantee protection, including against DoS attacks.

When a VPN packet arrives in a PE, it automatically receives a MPLS label. To determine the correct label it is necessary to discover the target egress PE for that packet. This is a safe mechanism to prevent intermediaries from analyzing the packet content. Only the egress PE router associated to that incoming label should be authorized to access this content.

Despite the mentioned security measures, another type of attack may succeed, such as label spoofing. If an intermediary produces fake labels it can invade an already

established MPLS tunnel. For this reason, if the core network is not trusted, IPSec tunneling must be applied into the whole MPLS cloud.

However, further security measures are demanded when this VPN crosses distinct provider boundaries. Such measures include not only the interconnection between two domains but also those cases where Internet access should be provided within the VPN. In this latter case the obscuration of addresses through NAT operations is recommended [6]. However, this is not appropriate when an inter-domain VPN is involved.

In a multi-domain scenario a VPN crosses distinct Autonomous Systems (AS). As observed in Figure 1, this implies that border routers (ASBRs – Autonomous System Border Routers) exchange critical information such as VPN IPv4 addresses of endpoints. According to [3] this may be accomplished by three different approaches. The first approach requires fixed VRF to VRF connections among ASBRs, which does not scale well. The second approach requires a previous trust relationship between involved ASs so that labeled routes may be exchanged. In the third approach, an ASBR does not distribute labeled routes to other ASBRs. Labeled routes are instead maintained by ASBRs, but only PEs of the same AS can access this information. A three-label stack must be built with the support of all involved routers, so that a packet travels from the ingress PE to the egress PE.

The third approach is a solution for multi-hop distribution of labeled routes. However, this information will travel through distinct domains masked within MPLS packets. Since these packets are not encrypted, there is still the risk of content inspection along the path, indirectly compromising the VPN security.

The above considerations lead to the conclusion that BGP/MPLS IP VPNs are vulnerable even if trust relationships are established. As stated in [8, 9, 11], a possible solution would be to insert cryptography capabilities, more specifically IPSec. With IPSec tunneling even domains that are not MPLS aware may transport packets of a BGP/MPLS VPN. Moreover, related services such as Traffic Engineering would not be compromised.

2.1 IPSec over BGP/MPLS IP VPNs

When using IPsec, VPN data packets traveling from one ASBR to another incorporate an IPSec header. As already mentioned, to perform this operation it is necessary to establish a SA. SAs can be manually negotiated (in fact this is usually the way they are currently established, in multi-domain scenarios). However, this is expensive, slow and not scalable. For this reason, the Internet Security Association and Key Management Protocol (ISAKMP) was proposed as a means to establish, negotiate, modify and delete SAs [12]. Since ISAKMP aims to provide a secure channel, a secret must be exchanged. This secret is a key session which may be delivered in an aggressive mode (e.g. manually) or through the intervention of protocols such as the Internet Key Exchange (IKE).

IPSec modifies IP packets in two different ways. When in transport mode, only the payload of the IP packet is encapsulated. In tunnel mode the whole packet is encapsulated, thus allowing a secure tunnel across non-trusted domains.

After the establishment of SAs a BGP/MPLS VPN may receive an IPSec tunneling through the replacement of the topmost label of a MPLS label stack by two new headers. One guarantees the authentication of the parties and is called Authentication Header (AH). The other is called Encapsulating Security Payload (ESP) and protects the communication, providing confidentiality, authentication and integrity. AH and ESP may be used both in transport and tunnel mode.

As can be concluded, to prevent backbone devices from breaking VPN confidentiality, integrity or authenticity, it is important that every PE is aware of a previously defined SA. Since this scenario involves distinct domains, it is important to provide solutions that dynamically enable the establishment of these SAs.

3 Related Work

Performance evaluation has been the most focused issue on previous work integrating IPSec in BGP/MPLS VPNs. In [7] the authors compare the impact of IPSec usage on networks with and without MPLS support. In the latter case, GRE tunneling increases the overhead and packet loss. Generally, these bad results are consequence of exhaustive handling of large packets in intermediary routers and firewalls.

A contribution for an inter-domain use case is presented at [13]. The authors propose an approach to distribute keys and establish SAs along the path. Security Policies Databases (SPD) and a Security Associations Database (SADB) are used for this intent. SPDs and SADB must be previously established, taking into account keys and certificates distributed by a centralized Certificate Authority (CA). This arrangement enables encryption between two endpoints from the moment a packet leaves a host (CE-CE encryption). To the best of our knowledge, this is the first attempt to implement IPSec features on inter-domain BGP/MPLS VPNs. Despite the contribution of this work, it is an approach that involves intense human intervention to provide relationships among domains. Therefore, this approach does not address the objectives of our GBF framework or the general concepts of NGN and Future Internet.

IPSec encryption is proposed by [14] to address risks associated with BGP route advertisements, such as hijacking of TCP connections, corruption of route updates, replay attacks and intruder masquerading. In this approach, BGP traffic flows through IPSec tunnels before the establishment of the BGP/MPLS VPN. According the authors, the evaluation tests did not present a negative affect at overall performance.

Despite valuable contributions of former works, there is in general a lack of dynamic and scalable solutions to address the management of IPSec security on inter-domain VPNs [15]. The establishment of SA between distinct domains requires the coordination of distinct planes of information, as discussed in Section 3.1.

3.1 Inter-domain IPSec Security Associations

Initiatives to extend the establishment of SAs to inter-domain scenarios are generally associated with trust negotiation [16] or policy deployment within enriched solutions.

Li et. al, for instance, propose a scheme where X.509 certificates are exchanged so that endpoints can achieve a common trust basis [17]. This way, it is possible to establish the identification for each endpoint, and IPSec policies are distributed between endpoints within an extended X.509 certificate. These policies are generated according to the role of the endpoint. After each endpoint completes its certificate specification, this will be sent over to the other endpoint, which will decide whether to adopt the underlying policies or not. Each endpoint must ensure that IPSec policies do not conflict with local policies. Associated interactions are supported by Policy Servers, and the effective establishment of an IPSec tunnel depends on the acceptance of each certificate. It is also worth mentioning that other servers must be present in this framework – the PKI Server and the VPN Server. SSL tunnels are used by each endpoint in order to reach these servers. Although this is an interesting and innovative solution for the establishment of SAs, it has some shortcomings from the scalability point of view, namely the growing number of SSL tunnels required to link endpoints to each server and the complexity of the insertion of a new endpoint (that requires a new extended X.509 certificate and inclusion on the VPN server).

Aurish et al. propose the establishment of IPSec SAs using a group of peers [18]. This is accomplished using the Multicast Internet Key Exchange protocol, which enables the negotiation and establishment of a group key in a secure manner. Their approach demands an IPSec discovery protocol whose intention is to identify capable devices and to configure them to form an IPSec tunnel. This is a strategy to interconnect distinct networks. However, it requires a complete knowledge of all involved elements. If a device leaves a network, this event must be notified. This behavior affects scalability. Nevertheless, this work presents significant contributions regarding the establishment of dynamic tunneling, since the adoption of a strategy to find IPSec capable devices diminishes the complexity of creating tunnels.

One drawback of previously mentioned work is the requirement for a centralized key management entity. In a multi-domain perspective it would hardly be scalable to delegate this task to a single entity. Another negative aspect is deciding how to delegate this high level of trust to an unknown entity. As mentioned by [16], when two parties establish a SA they are sharing a trust relationship. The most remarkable contribution to the trust management of IPSec tunnels comes probably from [19], where the authors propose a compliance checker that evaluates whether a packet conforms to the underlying policies of a SA. This guarantees that only authorized entities are allowed to exchange specific traffic. However, it does not address solutions for fine-grained security policies such as the duration of a SA.

Another drawback with previous work is the fact that many applications are forced to duplicate at the service layer cryptographic functions already provided at the infrastructure layer. To avoid this, our GBF framework can be leveraged to handle security policies and cryptographic operations within its distinct layers. However, a coordinated approach must be provided, to achieve a reliable communication channel.

4 Proposed Approach

The ITU-T model to end-to-end security considers that every system is vulnerable at least on three security planes (Figure 2), and for all these planes it is important to consider the security along three orthogonal layers. This is an appropriate approach to handle the provision of inter-domain VPN services. As pointed by [6], current security solutions for BGP/MPLS VPNs are too focused on infrastructure aspects. Our approach tries to overcome this limitation.

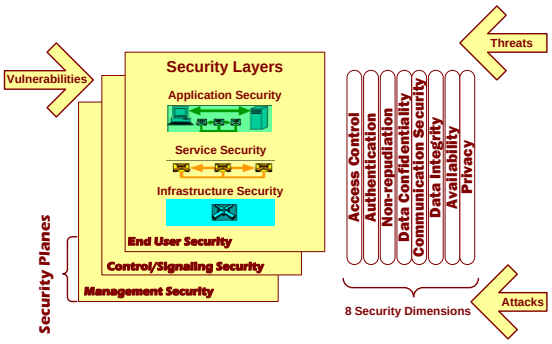

Fig. 2. ITU-T security architecture for E2E systems (adapted from [20]).

4.1 GBF, a Business Oriented Framework

In a previous work [5] we presented the GBF, a BL-oriented approach to handle dynamic creation of services assembled using sub-services (or Elements, according to the GBF terminology) from different providers (ISPs, carriers, content providers, etc.). According to the GBF architecture, service providers may assume two distinct roles: Service Owner (SO) and Element Owner (EO). A SO is the provider that is contacted by the customer to provide the (composed) service. Each EO is another provider that is "subcontracted" by the SO to provide a part of the service (an Element), in order to assemble and provide the whole service for the customer. The discovery of potential Element providers is supported by an UDDI-based (Universal Description, Discovery and Integration) service publishing mechanism, and the description of service components (as well as the negotiation between the SO and the EOs) is based on service templates.

The workflow that leads to service provisioning is based on the exchange of these templates, where two types of templates assume an important role: Service Specification Template (SST) and Element Specification Template (EST). While the SST describes the general parameters of the service, the EST is used to define, with EOs, more complete technical and business details of the participation in the composition of a specific service.

ESTs are crucial to leverage security relationships, since they contain security data related with a specific service instantiation. They can be used, for instance, to negotiate IPSec SAs between distinct domains. Each EST contains security

information identifying the EOs directly involved in the provisioning of that service Element, enabling the establishment of a reliable communication channel.

Authentication and authorization are core features that leverage trust among domains. ITU-T recommendations [21] define authorization and authentication requirements for a number of scenarios. According to the GBF architecture every potential provider must publish, within its service offer, its public key with certificates signed by trusted Certificate Authorities. Although ITU-T defines guidelines for the format of these certificates [22], the GBF platform allows providers to make this information explicit (on ESTs and/or directly gathered from UDDI service discovery services). This simplifies the solution without compromising security.

The WS-Security recommendation [23] establishes guidelines to protect message exchanging, allowing SOAP envelopes to receive XML encryption and, at the same time, indicating that additional credentials may be followed (such as authorization permissions). Public keys are a proper solution for authentication purposes. However, authorization demands a fine-grained evaluation of policies.

4.2 Extending WS-Security on the GBF Business Layer

As shown in Figure 3, two components of the GBF BL are responsible for exchanging templates: Service Instance Manager (SIM) and Element Instance Manager (EIM). While the former belongs to the Service Owner and manages service orchestration, the latter belong to Element Owners and control element services. SIM coordinates service provisioning and, for this reason, it will determine which service parameters – including security credentials – need to me known and enforced by each EIM for the SOAP transactions.

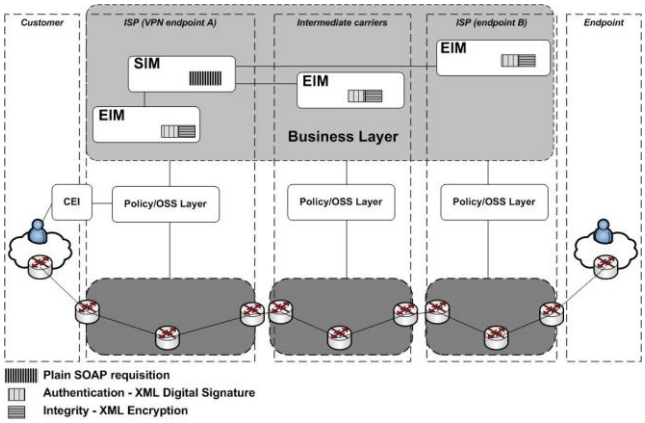

Fig. 3. WS-Security approach applied to the GBF BL.

According to this model, the SO becomes a trusted party, digitally signing the messages. Furthermore, the public keys of each EO should be used to encrypt specific

values generated by the SO to be used during the SA establishment. This is a proper solution to achieve a reliable communication channel among SO and EOs. However, additional information must be accomplished so that both the SO and the EOs (on behalf of the customer) achieve a common set of security decisions. This additional information includes specific policies for firewall traversal (if required) and specific policies for IPSec tunneling between peers, during BGP advertisements.

This specific set of policies requires new information, gathered and exchanged within EST templates. Figure 4 presents a fragment of this additional information. A more extensive discussion of the EST content may be found in [5].

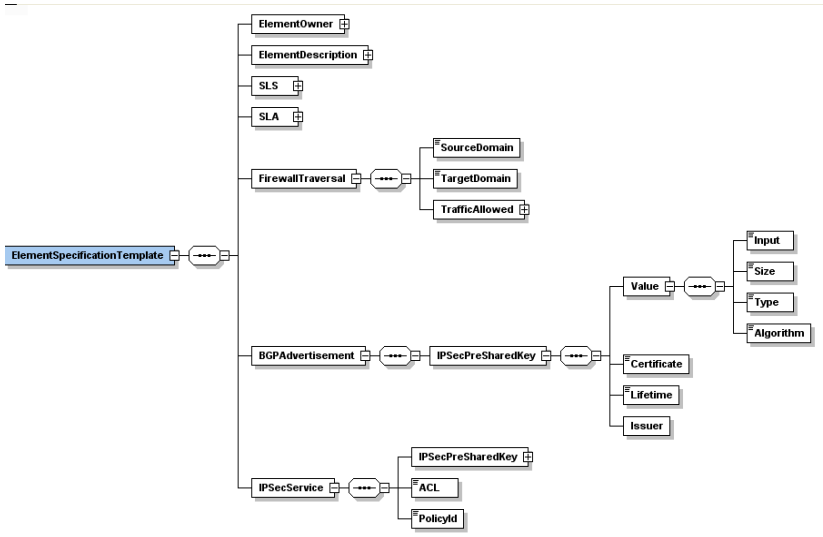

Fig. 4. Extended Element Specification Template (E-EST).

5 Prototype Development

The IPsec-based mediation approach we propose in this paper was incorporated in our prototype implementation of the GBF framework [5].

In order to start provisioning of a new VPN, each EO must supply the Service Owner with minimal information. This corresponds to the *ElementOwner* and *ElementDescription* sections of the EST (Figure 4). This information is then used by the Service Owner to build and propose an agreement (based on Service Level Agreements and Service Level Specifications) to target Element Owners.

Configuration of the service is triggered after each participating EO accepts its proposed agreement. This means that the Service Owner must fill the remaining fields of the EST template (*FirewallTraversal*, *BGPAdvertisement* and *IPSecService*).

However, those fields correspond to sensitive information that requires reliable channels. As mentioned before, this is accomplished using the public keys of each EO and the digital signature of the SO. While EO public keys (and underlying certificate)

are gathered from EOs, the Service Owner fills each EST template with security information. This way each Element Owner only retrieves service templates (including sensitive information) after the Service Owner checks the Element Owner digital certificate associated with its public key. Furthermore, each EO receives sensitive information on a need-to-know basis, since each EST is specifically tailored for a different EO.

As mentioned in [5], each EO plays a distinct role in the composition of the VPN service. One of those roles associates an EO to a transport and connection element, enabling distinct domains to be interconnected trough ASBRs. In this case, the Service Owner must fill *BGPAdverstisement* fields with a distinct *IPSecPreSharedKey* element. This information is then used by the underlying domain to provide an IPSec tunnel to carry safe advertisement of BGP routes and updates.

Apache WSS4J [24] is the implementation of WS-Security recommendations we use in our prototype. Its enables authentication and integrity checking during the EST exchange process.

A secure tunnel was implemented within each Element Owner domain. This "vertical" channel transports decisions from the secure Business Layer to the underlying Network and Infrastructure Layer (NIL). A similar approach was also used in previous work [17].

6 Evaluation

In order to assess the performance penalty resulting from the proposed IPsec mediation approach, we used an experimental testbed where inter-domain VPNs are safely established between three different domains (Figure 5). Previous work [5] already focused on the validation of the general GBF framework for dynamic establishment of multi-domain VPNs.

We now focused on comparing traffic overhead and performance penalties induced by the GBF framework in two distinct situations: with and without the proposed IPsec mediation scheme.

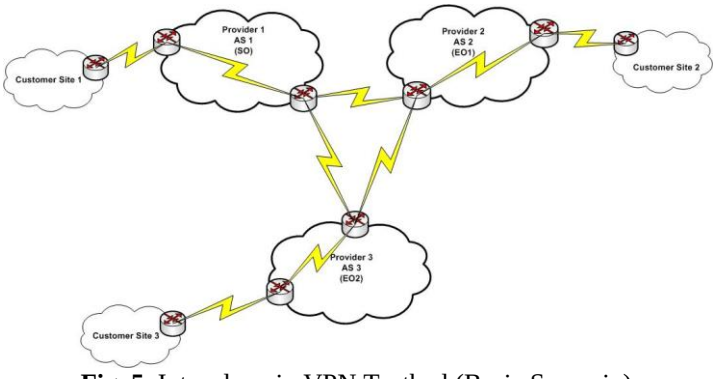

Fig. 5. Inter-domain VPN Testbed (Basic Scenario)

Table 1 presents the traffic exchanged between the Service Owner and each Element Owner. There is an increase in traffic overhead, introduced by the IPsec mediation, but within acceptable limits. Performance is also slightly affected: the average VPN establishment latency raised less than 9%, from 1,200 ms (without IPsec mediation) to 1,300 ms (with IPsec mediation).

Table 1. VPN Establishment With and Without IPSec Mediation
(traffic overhead generated by the GBF framework)

Link	*VPN establishment (without IPSec)*	*VPN establishment (with IPSec)*
SO / EO 1	*47 packets (17721 octects)*	*62 packets (23376 octects)*
SO / EO 2	*47 packets (17721 octects)*	*62 packets (23376 octects)*

These measurements show that IPsec mediation does affect performance and network traffic but well within reasonable values, considering its security benefits.

7 Conclusions

In this we propose a new mechanism to safely create inter domain BGP/MPLS IP VPNs. This mechanism was built on top the Global Business Framework [5], thus allowing the dynamic provisioning of on-demand VPNs.

This proposal, inline with recommendations from IETF and ITU-T, allows the safe application of IPSec tunnels to build BGP/MPLS IP VPNs, bypassing a number of intrinsic vulnerabilities. Since building trust relationships across multiple domains can become a hard task, the Business Layer of GBF was used to establish high-level statements for the service (namely the establishment of the Security Association).

The original EST template used by GBF to describe service instance parameters was extended in order to include additional information, for instance to secure BGP advertisements.

Future work will focus on trust management, more specifically in the improvement of trust mechanisms between EOs and SOs, leading to a more dynamic trust negotiation approach based on SOA.

Acknowledgments. This work was partially funded by FCT (scholarship contracts SFRH/BD/16261/2004 and SFRH/BD/29103/2006) and supported by the IST FP6 OpenNet Project.

8 References

1. Carugi, M., De Clercq J. “Virtual private network services: scenarios, requirements and architectural constructs from a standardization perspective”. In IEEE Communications Magazine, vol. 42, issue 6, pp. 116 – 122 (2004)
2. Minei, I., Marques, P.R., "Scalability Considerations in BGP/MPLS IP VPNs," In IEEE Communications Magazine, vol.45, no.4, pp.26-31 (2007)

3. Rosen, E. and Rekhter, Y. “BGP/MPLS IP Virtual Private Networks (VPNs)”. RFC 4364 (2006)
4. Semeria, C. “RFC 2547bis: BGP/MPLS VPN Hierarchical and Recursive Applications”. Juniper Networks White Paper (2001)
5. Matos, A. V., Matos, F. M., Simões, P., Monteiro, E. “A Framework for the Establishment of Inter-Domain, On-Demand VPNs”. In 11th IEEE/IFIP Network Operations and Management Symposium – NOMS, pp. 232-239 (2008)
6. Behringer, M. “Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)”. RFC 4381 (2006)
7. Alawieh, B. et al., H. T. “Security impacts on establishing MPLS/BGP VPNs”. In Willey Security and Communication Networks Journal, vol. 1, issue 4, pp. 269-275 (2008)
8. Rekhter, Y., Bonica, R., Rosen, E. “Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks”. RFC 4797 (2007)
9. Rosen, E. “Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)”. RFC 4365 (2006)
10. Alateras, J. (Ed.), IPsphere Framework Technical Specification – Release 1. Available at http://www.ipsphereforum.org/Files/IPSF_R1_Spec.pdf. (2007)
11. Woster, T., Rekhter, Y., Rosen, E. “Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)”. RFC 4023 (2005)
12. Kent, S. and Ativkson, S. “Security Architecture for the Internet Protocol”. RFC 4021 (1998)
13. Ren, R., Feng, D. and Ma, K. “A detailed implement and analysis of MPLS VPN based on IPSec”. Proceedings of International Conference on Machine Learning and Cybernetics. Vol. 5, pp. 2779 – 2783 (2004)
14. Pezeshki, J. et al. “Performance Implications of Instantiating IPsec over BGP Enabled RFC 4364 VPNs”. In IEEE Military Communications Conference - MILCOM, pp. 1-7 (2007)
15. Phillips, C., Bigham, J., He, L. and Littlefair, B. “Managing dynamic automated communities with MPLS-based VPNs”. In BT Technology Journal. Vol. 24, number 2, pp. 79-84, Springer Netherlands (2006)
16. Masmoudi, K. and Afifi, H. “Building identity-based security associations for provider-provisioned virtual private networks”. In Journal of Telecommunication Systems, vol. 39, issue 3, pages: 215-222, Springer Netherlands (2008)
17. Li Q., Xu M., Xu, K. “Toward A Practical Scheme for IPSec Management” In International Conference on Information Networking - ICOIN, pp. 1-5 (2008)
18. Aurisch, T., Ginzler, T., Martini, P., Ogden, R., Tran, T. and Seifert, H. “Automatic multicast IPsec by using a proactive IPsec discovery protocol and a group key management”. In Journal of Telecommunications and Information Technology. Number 2, pp. 77-83 (2008).
19. Blaze, M., Ioannidis, J. and Keromytis A. “Trust Management for IPSec”. In ACM Transactions on Information and System Security. Vol. 5, number 2, pp. 95-188 (2002)
20. ITU-T Recommendation X.805: Network security architecture. (2003)
21. ITU-T Recommendation Y.2702: Authentication and authorization requirements for NGN release 1. (2008)

22. ITU-T Recommendation Y.2703: The application of AAA service in NGN. Work in Progress (2008)
23. Nadalin, A., Kaler C., Monzillo R., Hallam-Baker, P. "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)". OASIS Standard Specification (2006)
24. Apache WSS4J, http://ws.apache.org/wss4j/