Analysis of the Security of BGP/MPLS IP VPNs

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document analyses the security of the BGP/MPLS IP VPN architecture as described in [RFC2547bis], especially in comparison with other VPN technologies such as ATM and Frame Relay. The target audience is service providers and VPN users. The document consists of two main parts: First the requirements for security in VPN services are defined, second BGP/MPLS IP VPNs are examined with respect to these requirements.

The analysis shows that BGP/MPLS IP VPN networks can be equally secured as traditional layer-2 VPN networks such as ATM and Frame Relay.

Table of Contents

1. Scope and Introduction.............................................2
2. Security Requirements of VPN Networks..........................3
   2.1 Address Space, Routing and Traffic Separation.................3
   2.2 Hiding of the Core Infrastructure.............................4
   2.3 Resistance to Attacks.........................................4
   2.4 Impossibility of Label Spoofing.............................5
1. Scope and Introduction

As MPLS (multi protocol label switching) is becoming a more wide-spread technology for providing IP VPN (virtual private network) services, the security of the BGP/MPLS IP VPN architecture is of increasing concern to service providers and VPN customers. This document gives an overview of the security of the BGP/MPLS IP VPN architecture as described in [RFC2547bis] for both service providers and MPLS users, and compares it with traditional layer-2 services such as ATM or Frame Relay from a security perspective.

The term "MPLS core" is defined for this document as the set of PE and P routers which are used to provide an BGP/MPLS IP VPN service, typically under the control of a single service provider. This document assumes that the MPLS core network is trusted and provided in a secure manner. Thus it does not address basic security concerns such as securing the network elements against unauthorised access, misconfigurations of the core, internal (within the core) attacks and the likes. Should a customer not wish to assume the service provider network as trusted it becomes necessary to use additional security mechanisms such as IPsec over the MPLS infrastructure. One way to implement IPsec over BGP/MPLS is described in [Guichard].

Analysis of the security features of routing protocols is only covered to the extend where it influences BGP/MPLS IP VPNs. IPsec technology is also not covered, except to highlight the combination of MPLS VPNs with IPsec.

The overall security of a system depends on three parts: the architecture, the implementation, and the operation of the system. Security issues can exist in either part. This document analyses the architectural security of BGP/MPLS IP VPNs. It does not cover implementation issues nor operational issues.

This document is targeted at technical staff of service providers and
enterprises. Knowledge of the basic BGP/MPLS IP VPN architecture as described in [RFC2547bis] is required to understand this document.

2. Security Requirements of VPN Networks

Both service providers offering any type of VPN services and customers using them have specific demands for security. Mostly they compare MPLS based solutions with traditional layer 2 based VPN solutions such as Frame Relay and ATM, since these are widely deployed and accepted. This section outlines the security requirements that are typically made in VPN networks. The following section discusses if and how BGP/MPLS IP VPNs address these requirements, for both the MPLS core and the connected VPNs.

2.1 Address Space, Routing and Traffic Separation

Between two non-intersecting layer 3 VPNs of an VPN service it is assumed that the address space between different VPNs is entirely independent. This means that for example two non-intersecting VPNs must be able to both use the 10/8 network without any interference. In addition traffic from one VPN must never enter another VPN. This includes separation of routing protocol information, so that also routing tables are separate per VPN. Specifically:

* Any VPN must be able to use the same address space as any other VPN.
* Any VPN must be able to use the same address space as the MPLS core.
* Traffic from one VPN must never flow to another VPN.
* Routing information, as well as distribution and processing of that information, for one VPN instance must be independent from any other VPN instance.

From a security point of view the basic requirement is to avoid that packets destined to a host a.b.c.d within a given VPN reach a host with the same address in another VPN or the core, or get routed to another VPN even if this address does not exist there.

2.2 Hiding of the Core Infrastructure

The internal structure of the core network (in the case of MPLS PE and P elements) should not be visible to outside networks (Internet or any connected VPN). Whilst a breach of this requirement does not lead to a security problem itself, many service providers feel that it is advantageous if the internal addressing and network structure remains hidden to the outside world. A strong argument is that DoS attacks against a core router for example are much easier to carry out if an attacker knows the address. Where addresses are not known, they can be guessed, but with this attacks become more difficult. Ideally the core should be as invisible to the outside world as a comparable layer 2 (e.g., frame relay, ATM) infrastructure. Core network elements should also not be accessible from a VPN.

Note that security should never rely on obscurity, i.e., the hiding of
information. On the contrary services should be equally secure if the implementation is known. However, there is a strong market perception that hiding of details is advantageous. This point addresses that market perception.

2.3 Resistance to Attacks

There are two basic types of attacks: Denial-of-Service (DoS) attacks, where resources become unavailable to authorised users, and intrusions, where resources become available to un-authorised users.

For attacks that give unauthorised access to resources (intrusions) there are two basic ways to protect the network: Firstly, to harden protocols that could be abused (e.g., telnet to a router), secondly to make the network as inaccessible as possible. The latter is achieved by a combination of packet filtering or firewalling and address hiding, as discussed above.

DoS attacks are easier to execute, since in the simplest case a known IP address might be enough to attack a machine. This can be done using normal "allowed" traffic, but higher than normal packet rates, so that other users cannot access the targeted machine. The only way to be certain not be vulnerable to this kind of attack is to make sure that machines are not reachable, again by packet filtering and optionally address hiding.

BGP/MPLS IP VPN networks must provide at least the same level of protection against both forms of attack as current layer 2 networks. Note that this document concentrates on protecting the core network against attacks from the "outside", i.e., the Internet and connected VPNs. Protection against attacks from the "inside", i.e., if an attacker has logical or physical access to the core network is not considered here, since any network can be attacked with access from the inside.

2.4 Impossibility of Label Spoofing

Assuming the address and traffic separation as discussed above, a potential attacker might try to gain access to other VPNs by inserting packets with a label that he does not "own". This could be done from the outside, i.e., another CE router or from the Internet, or from within the MPLS core. The latter case (from within the core) will not be discussed, since the assumption is that the core network is provided in a secure manner. Should protection against an insecure core be required it is necessary to run IPsec across the MPLS infrastructure, at least from CE to CE, since the PEs belong to the core.

Depending on the way several CEs are connected to a PE router, it might be technically possible to intrude into another VPN that is also connected on that PE, based on layer 2 attack mechanisms. Examples are 802.1Q - label spoofing, or ATM VPI/VCI spoofing. Layer 2 security issues will be discussed in section 6.

It is required that VPNs cannot abuse the MPLS label mechanisms or protocols to gain un-authorised access to other VPNs or the core.
3. Analysis of BGP/MPLS IP VPN Security

In this section the BGP/MPLS IP VPN architecture is analysed with respect to the security requirements listed above.

3.1 Address Space, Routing and Traffic Separation

BGP/MPLS allows distinct IP VPNs to use the same address space, which can also be private address space [RFC1918]. This is achieved by adding a 64 bit route distinguisher (RD) to each IPv4 route, making VPN-unique addresses also unique in the MPLS core. This "extended" address is also called a "VPN-IPv4 address". Thus customers of an BGP/MPLS IP VPN service do not need to change current addressing in their networks.

There is only one exception, which is the IP addresses of the PE routers the CE routers are peering with, in the case of using routing protocols between CE and PE routers (for static routing between PE and CE this is not an issue). Routing protocols on the CE routers need to have configured the address of the peer PE router in the core, to be able to "talk" to the PE router. This address must be unique from the CE router’s perspective. In an environment where the service provider manages also the CE routers as CPE, this can be made invisible to the customer. The address space on the CE-PE link (including the peering PE address) must be considered as part of the VPN address space. However, since address space can overlap between VPNs, also the CE-PE link addressing can overlap between VPNs. (Note that for practical management considerations SPs typically choose to address all CE-PE links from a global pool, keeping them unique across the entire core. The considerations of CE-PE addressing are discussed in detail in [Guichard2].)

Routing separation between the VPNs can also be achieved. Every PE router maintains a separate Virtual Routing and Forwarding instance (VRF) for each connected VPN. Each VRF on the PE router is populated with routes from one VPN, through statically configured routes or through routing protocols that run between the PE and the CE router. Since every VPN results in a separate VRF there will be no interferences between the VPNs on the PE router.

Across the core to the other PE routers this separation is maintained by adding unique VPN identifiers in multi-protocol BGP, such as the route distinguisher. VPN routes are exclusively exchanged by MP-BGP across the core, and this BGP information is not re-distributed to the core network but only to the other PE routers, where the information is kept again in VPN specific VRFs. Thus routing across an BGP/MPLS network is separate per VPN.

On the data plane traffic separation is achieved by the ingress PE prepending a VPN-specific label to the packets. The packets with the VPN labels are sent through the core to the egress PE, where the VPN label is used to determine the correct VPN.

Given the addressing, routing and traffic separation across an BGP/MPLS IP VPN core network, it can be assumed that this architecture offers in this respect the same security as comparable layer-2 VPNs such as ATM.
or Frame Relay. It is not possible to intrude from a VPN or the core into other VPNs through the BGP/MPLS IP VPN network, unless this has been configured specifically.

3.2 Hiding of the BGP/MPLS IP VPN Core Infrastructure

For reasons of security service providers and end-customers do not normally want their network topology revealed to the outside. This is done to make attacks more difficult: If an attacker doesn't know the target he can only guess the IP addresses to attack. Since most DoS attacks don't provide direct feedback to the attacker it would be difficult to attack the network. It has to be mentioned specifically that information hiding as such does not provide security. However, in the market this is a perceived requirement.

With a known IP address a potential attacker can launch a DoS attack more easily against that device. So the ideal is to not reveal any information of the internal network to the outside. This applies equally to the customer networks as to the core. In practice a number of additional security measures have to be taken, most of all extensive packet filtering.

For security reasons it is recommended for any core network – MPLS based or not – to filter packets from the "outside" (Internet or connected VPNs) destined to the core infrastructure, where possible. This makes it very hard to attack the core, although some potentially desired functionality such as pinging core routers will be lost.

Traceroute across the core still works, since it addresses a destination outside the core.

MPLS does not reveal unnecessary information to the outside, not even to customer VPNs. The addressing of the core can be done with private addresses [RFC1918] or public addresses. Since the interface to the VPNs as well as potentially to the Internet is BGP, there is no need to reveal any internal information. The only information required in the case of a routing protocol between PE and CE is the address of the PE router. If this is not desired, and if no dynamic routing protocol is required, static routing on unnumbered interfaces can be configured between the PE and CE. With this measure the BGP/MPLS IP VPN core can be kept completely hidden.

Customer VPNs will have to advertise their routes as a minimum to the BGP/MPLS IP VPN core (dynamically or statically), to ensure reachability across their VPN. Whilst this could be seen as "too open", the following has to be noted: Firstly, the information known to the core is not about specific hosts, but networks (routes); this offers some degree of abstraction. Secondly, in a VPN-only BGP/MPLS IP VPN network (i.e., no shared Internet access) this is equal to existing layer-2 models, where the customer has to trust the service provider to some degree. Also in a FR or ATM network routing information about the VPNs can be seen on the core network.
In a VPN service with shared Internet access the service provider will typically announce the routes of customers that wish to use the Internet to his upstream or peer providers. This can be done via a NAT function to further obscure the addressing information of the customers’ networks. In this case the customer does not reveal more information to the general Internet than with a general Internet service. Core information will still not be revealed at all, except for the peering address(es) of the PE router(s) that hold(s) the peering with the Internet.

In summary, in a pure MPLS-VPN service, where no Internet access is provided, the information hiding is as good as on a comparable FR or ATM network: No addressing information is revealed to third parties or the Internet. If a customer chooses to access the Internet via the BGP/MPLS IP VPN core he will have to reveal the same addressing structure as for a normal Internet service. NAT can be used for further address hiding. Being reachable from the Internet automatically exposes a customer network to additional security threats. Appropriate security mechanisms have to be deployed such as firewalls and intrusion detection systems. But this is true for any Internet access, over MPLS or direct.

If a BGP/MPLS IP VPN network has no interconnections to the Internet, the security is equal to FR or ATM VPN networks. With an Internet access from the MPLS cloud the service provider has to reveal at least one IP address (of the peering PE router) to the next provider, and thus the outside world.

3.3 Resistance to Attacks

Section 3.1 shows that it is not possible to directly intrude into other VPNs. Another possibility is to attack the MPLS core, and try to attack other VPNs from there. As shown above it is not possible to address a P router directly. The only reachable address from a VPN or the Internet are the peering addresses of the PE routers. Thus there are two basic ways the BGP/MPLS IP VPN core can be attacked:

1. By attacking the PE routers directly.
2. By attacking the signaling mechanisms of MPLS (mostly routing)

To attack an element of an BGP/MPLS IP VPN network it is first necessary to know this element, that is, its address. As discussed in section 3.2 the addressing structure of the BGP/MPLS IP VPN core is hidden to the outside world. Thus an attacker does not know the IP address of any router in the core that he wants to attack. The attacker could now guess addresses and send packets to these addresses. However, due to the address separation of MPLS each incoming packet will be treated as belonging to the address space of the customer. Thus it is impossible to reach an internal router, even through IP address guessing. There is only one exception to this rule, which is the peer
interface of the PE router. This address of the PE is the only attack point from the outside (a VPN or Internet).

The routing between a VPN and the BGP/MPLS IP VPN core can be configured two ways:

1. Static; in this case the PE routers are configured with static routes to the networks behind each CE, and the CEs are configured to statically point to the PE router for any network in other parts of the VPN (mostly a default route). There are now two sub-cases: The static route can point to the IP address of the PE router, or to an interface of the CE router (e.g., serial0).

2. Dynamic; here a routing protocol (e.g., RIP, OSPF, BGP) is used to exchange the routing information between the CE and the PE at each peering point.

In the case of a static route from the CE router to the PE router, which points to an interface, the CE router doesn’t need to know any IP address of the core network, not even of the PE router. This has the disadvantage of a more extensive (static) configuration, but from a security point of view is preferable to the other cases. It is now possible to configure packet filters on the PE interface to deny any packet to the PE interface. This way the router and the whole core cannot be attacked.

In all other cases, each CE router needs to know at least the router ID (RID; peer IP address) of the PE router in the core, and thus has a potential destination for an attack. One could imagine various attacks on various services running on a router. In practice access to the PE router over the CE-PE interface can be limited to the required routing protocol by using ACLs (access control lists). This limits the point of attack to one routing protocol, for example BGP. A potential attack could be to send an extensive number of routes, or to flood the PE router with routing updates. Both could lead to a denial-of-service, however, not to unauthorised access.

To restrict this risk it is necessary to configure the routing protocol on the PE router as securely as possible. This can be done in various ways:

* By ACL, allow the routing protocol only from the CE router, not from anywhere else. Furthermore, no access other than that should be allowed to the PE router in the inbound ACL on each CE interface.

* Where available, configure MD-5 authentication for routing protocols. This is available for BGP [RFC2385], OSPF [RFC2154] and RIP2 [RFC2082] for example. It avoids that packets could be spoofed from other parts of the customer network than the CE router. Note that this requires service provider and customer to agree on a shared secret between all CE and PE routers. Note that it is necessary to do this for all VPN customers, it is not sufficient to do this for the customer with the highest security requirements.
* To configure where available parameters of the routing protocol, to further secure this communication. For example the rate of routing updates should be restricted where possible (in BGP this can be done through dampening). Also, a maximum number of routes accepted per VRF should be configured where possible.

In summary, it is not possible to intrude from one VPN into other VPNs, or the core. However, it is theoretically possible to exploit the routing protocol to execute a DoS attack against the PE router. This in turn might have negative impact on other VPNs on this PE router. For this reason PE routers must be extremely well secured, especially on their interfaces to the CE routers. ACLs must be configured to limit access only to the port(s) of the routing protocol, and only from the CE router. MD5 authentication in routing protocols should be used on all PE-CE peerings. With all these security measures the only possible attack is a DoS attack against the routing protocol itself. However, BGP for example has a number of counter-measures such as prefix filtering and dampening built into the protocol, to assure stability. It is also easily possible to track the source of such a potential DoS attack. Without dynamic routing between CEs and PEs the security is equivalent to the security of ATM or Frame Relay networks.

### 3.4 Label Spoofing

Within the MPLS network packets are not forwarded based on the IP destination address, but based on labels that are pre-pended to the IP packets by the inbound PE routers. Similar to IP spoofing attacks, where an attacker replaces the source or destination IP address of a packet, it is also theoretically possible to spoof the label of an MPLS packet. In the first section the assumption was made that the core network is trusted. If this assumption cannot be made IPsec must be run over the MPLS cloud. Thus in this section the emphasis is on whether it is possible to insert packets with (spoofed) labels into the MPLS network from the outside, i.e., from a VPN (CE router) or from the Internet.

Principally the interface between any CE router and its peering PE router is an IP interface, i.e., without labels. The CE router is unaware of the MPLS core, and thinks it is sending IP packets to a simple router. The "intelligence" is done in the PE device, where based on the configuration, the label is chosen and pre-pended to the packet. This is the case for all PE routers, towards CE routers as well as the upstream service provider. All interfaces into the MPLS cloud only require IP packets, without labels.

For security reasons a PE router should never accept a packet with a label from a CE router. [RFC3031] specifies: "Therefore, when a labeled packet is received with an invalid incoming label, it MUST be discarded, UNLESS it is determined by some means (not within the scope of the current document) that forwarding it unlabeled cannot cause any harm." Since accepting labels on the CE interface would allow passing packets to other VPNs it is not permitted by the RFC.
Thus it is impossible for an outside attacker to send labelled packets into the BGP/MPLS IP VPN core.

There remains the possibility to spoof the IP address of a packet that is being sent to the MPLS core. However, since there is strict addressing separation within the PE router, and each VPN has its own VRF, this can only do harm to the VPN the spoofed packet originated from, in other words, a VPN customer can attack himself. MPLS doesn’t add any security risk here.

The Inter-AS and CsC cases are special cases, since on the interfaces between providers typically packets with labels are exchanged. See section 4 for an analysis of these architectures.

3.5 Comparison with ATM/FR VPNs

ATM and FR VPN services often enjoy a very high reputation in terms of security. Although ATM and FR VPNs can also be provided in a secure manner, it has been reported that also these technologies can have severe security vulnerabilities [DataComm]. Also in ATM/FR the security depends on the configuration of the network being secure, and errors can also lead to security problems.


The BGP/MPLS IP VPN architecture as described in [RFC2547] defines the PE-CE interface as the only external interface, as seen from the service provider network. In this case, the PE treats the CE as untrusted, and only accepts pure IP packets from the CE. The IP range however is treated as belonging to the VPN of the CE, thus the PE maintains full control over VPN separation.

Subsequently, [RFC2547bis] has defined more complex architectures, with more open interfaces. These interfaces allow the exchange of label information and labelled packets to and from devices outside the control of the service provider. This section discusses the security implications of these architectures.

4.1 Carriers’ Carrier (CsC)

In the CsC architecture the CE is linked to a VRF on the PE. The CE may send labeled packets to the PE. The label has been previously assigned by the PE to the CE, and represents the LSP from this CE to the remote CE via the carrier’s network.

RFC2547bis specifies for this case: "When the PE receives a labeled packet from a CE, it must verify that the top label is one that was distributed to that CE." This ensures that the CE can only use labels that the PE correctly associates with the corresponding VPN. Packets with incorrect labels will be discarded, and thus label spoofing is not possible.

The use of label-maps on the PE equally leaves the control of the label information entirely with the PE, so that this has no impact on the security of the solution.
The packet underneath the top label will - as in standard RFC2547 networks - remain local to the carrier’s VPN and not be looked at in the carrier’s carrier core. Consequently potential spoofing of subsequent labels or IP addresses remains also local to the carrier’s VPN, and has no implication on the carriers’ carrier core, nor on other VPNs on that core. This is specifically stated in RFC2547bis in section 6.

Note that if the PE and CE are interconnected using a shared layer 2 infrastructure such as a switch, attacks are possible on layer 2, which might enable a third party on the shared layer 2 network to intrude into a VPN on that PE router. RFC2547bis specifies therefore that either all devices on a shared layer 2 network have to be part of the same VPN, or the layer 2 network must be split logically to avoid this issue. This will be discussed in more detail in section 6.

In the CsC architecture the carrier needs to trust the carriers’ carrier for correct configuration and operation. The customer of the carrier thus implicitly needs to trust both his carrier and the carriers’ carrier.

In summary, a correctly configured carriers’ carrier network provides the same level of security as comparable layer 2 networks, or traditional RFC2547 networks.

4.2 Inter-provider backbones

RFC2547bis specifies three sub-cases for the inter-provider backbone (Inter-AS) case.

a) VRF-to-VRF connections at the AS border routers

In this case each PE sees and treats the other PE as a CE; each will not accept labelled packets, and there is no signalling between the PEs other than inside the VRFs on both sides. Thus the separation of the VPNs on both sides and the security of those are the same as on a single AS RFC2547 network. This has already been shown above to have the same security properties as traditional layer 2 VPNs.

This solution has potential scalability issues in that the ASBRs need to maintain a VRF per VPN, and all of the VRFs need to hold all routes of the specific VPNs. Thus an ASBR can run into memory problems affecting all VPNs if one single VRF contains too many routes. Thus the service providers needs to assure that the ASBRs are properly dimensioned, and apply appropriate security measures such as limiting the number of routes per VRF.

The two service providers connecting their VPNs in this way must trust each other. Since the VPNs are physically separated on different (sub-)interfaces all signalling between ASBRs remains within a given VPN. This means that no dynamic cross-VPN security breaches are possible. However, it is conceivable that a service provider connects a specific connection from a given VPN to a wrong interface, thus interconnecting
two VPNs that should not be connected. This has to be controlled operationally.

b) EBGP redistribution of labeled VPN-IPv4 routes from AS to neighboring AS

In this case the ASBRs on both sides hold the full routing information for all VPNs on both sides, but not in separate VRFs, but in the BGP database. (Note this is typically limited to the Inter-AS VPNs through filtering.) The separation inside the PE is maintained through the use of VPN-IPv4 addresses. The control plane between the ASBRs is using MP-eBGP, exchanging the VPN routes as VPN-IPv4 addresses, and their own addresses as BGP next hop IPv4 addresses, plus labels to be used on the data plane.

The data plane is separated through the use of a single label, representing a VRF or a subset thereof. RFC2547bis states that an ASBR should only accept packets with a label that it has assigned to this router. This prevents the insertion of packets with unknown labels, but it is possible for a service provider to use any label that the ASBR of the other provider has passed on to the other ASBR. This allows one provider to insert packets into any VPN of the other provider to which it has a label.

Also this solution needs to consider the security on layer 2 at the interconnection. The RFC states that this type of interconnection should only be implemented on private interconnection points. See section 6 for more details.

RFC2547bis states for this case that a trust relationship between the two connecting ASes must exist for this model to work securely. Effectively all ASes interconnected in this way form together one single zone of trust. The VPN customer needs to trust all the service providers involved in this architecture.

c) PEs exchange labeled VPN-IPv4 routes, ASBRs only exchange loopbacks of PEs with labels.

In this solution there are effectively two control connections between ASes. The route reflectors (RRs) exchange via multihop eBGP the VPN-IPv4 routes. The ASBRs only exchange the labeled addresses of those PE routers that hold VPN routes which are shared between those ASes. This maintains scalability for the ASBR routers, since they do not need to know the VPN-IPv4 routes.

In this solution the top label specifies an LSP to an egress PE router, the second label specifies a VPN connected to this egress PE. The security of the ASBR connection has the same constraints as in solution b): An ASBR should only accept packets with top labels that it has assigned to the other router, thus verifying that the packet is addressed to a valid PE router. But any label which was assigned to the other ASBR router will be accepted, thus it is not possible for an ASBR to distinguish between different egress PEs, nor between different VPNs.
on those PEs. A malicious service provider of one AS could therefore introduce packets into any VPN of the other AS to which it holds valid information on its ASBR and PEs.

This means that such an ASBR-ASBR connection can only be made with a trusted party, over a private interface, as described in b).

In addition this solution exchanges labeled VPN-IPv4 addresses between route reflectors (RR) via MP-eBGP. The control plane itself can be protected via routing authentication [RFC2385], which ensures that the routing information has been originated by the expected RR and has not been modified in transit. But the received VPN information cannot be verified, as in the previous case. The ASes need to trust each other to configure their respective networks correctly. Again all ASes involved in this design form together one trusted zone. The customer therefore needs to trust all the service providers involved.

The difference between case b) and case c) is that in b) the ASBRs act as iBGP next-hops for their AS, thus each SP needs to know of the other SP’s core only the addresses of the ASBRs. In case c) the SPs exchange the loopback addresses of their PE routers, thus each SP reveals information to the other of his PE routers, and these routers must be accessible from the other AS. As stated above, accessibility does not necessarily mean insecurity, and networks should never rely on "security through obscurity". So if the PE routers are appropriately secured this should not be an issue. However, there is an increasing perception that network devices should generally not be accessible.

In addition for case c) scalability considerations, for example for the number of BGP peerings, have now to be made for the overall network including all ASes linked this way. So SPs on both sides need to work together in defining a scalable architecture, probably with route reflectors.

In summary all of these Inter-AS solutions logically merge several provider networks together. For all cases of Inter-AS configuration all ASes together form a single zone of trust, and service providers need to trust each other. For the VPN customer the security of the overall solution is equal to the security of traditional RFC2547 networks, but he needs to trust all service providers involved.

5. What BGP/MPLS IP VPNs Do Not Provide

5.1 Protection against Misconfigurations of the Core and Attacks "within" the Core

The security mechanisms discussed here assume correct configuration of the involved network elements on the core network (PE and P routers).
Deliberate or inadvertent misconfigurations from SP staff may result in undesired behaviour including severe security leaks.

Note that this paragraph specifically refers to the core network, i.e., the PE and P elements. Misconfiguration of any of the customer side elements such as the CE router are covered by the security mechanisms above. This means that a potential attacker must have access to either PE or P routers to gain advantage from misconfigurations. If an attacker has access to core elements, or is able to insert into the core additional equipment, he will be able to attack both the core network as well as the connected VPNs. Thus the following is important:

* To avoid the risk of misconfigurations it is important that the equipment is easy to configure, and that SP staff have the appropriate training and experience when configuring the network. Also, proper tools are required for configuring the core network.

* To avoid the risk of "internal" attacks the core network must be properly secured. This includes network element security, management security, physical security of the service provider infrastructure, access control to service provider installations and other standard SP security mechanisms.

BGP/MPLS IP VPNs can only provide a secure service if the core network is provided in a secure fashion. This document assumes this to be the case.

There are various approaches to control the security of a core if the VPN customer cannot or does not want to trust the service provider. IPsec from customer controlled devices is one of them. [Bonica] proposes a CE based authentication scheme based on cookies, aimed at detecting misconfigurations in the MPLS core. [Behringer] proposes a similar scheme based on using the MD5 routing authentication. Both schemes aim to detect and prevent misconfigurations in the core.

5.2 Data Encryption, Integrity and Origin Authentication

BGP/MPLS IP VPNs themselves does not provide encryption, integrity or authentication services. If these are required IPsec should be used over the MPLS infrastructure. The same applies to ATM and Frame Relay: Also here IPsec can provide these missing services.

5.3 Customer Network Security

BGP/MPLS IP VPNs can be secured so that they are comparable with other VPN services. However, the security of the core network is only one factor for the overall security of a customer’s network. Threats in today’s networks do not only come from the "outside" connection, but also from the "inside" and from other entry points (modems for example). To reach a good security level for a customer network in an BGP/MPLS infrastructure, MPLS security is necessary but not sufficient. The same applies to other VPN technologies like ATM or frame relay. See also [RFC2196] for more information on how to secure a network.
6. Layer 2 security considerations

In most cases of Inter-AS or Carrier’s Carrier solutions a network will be interconnected to other networks via a point-to-point private connection, that is, a connection which cannot be interfered by third parties. It is important to understand that the use of any shared medium layer 2 technology for such interconnections, such as ethernet switches, may carry additional security risks.

There are two types of risks involved in a layer 2 infrastructure:

a) Attacks against layer 2 protocols or mechanisms

Risks in a layer 2 environment include many different forms of ARP attacks, VLAN trunking attacks, or CAM overflow attacks. For example ARP spoofing allows an attacker to re-direct traffic between two routers through his device, thus being able to see all packets between those two routers.

All of those can be prevented by appropriate security measures, but often these security concerns are overlooked. It is of utmost importance that if a shared medium such as a switch is used in the above scenarios, that all available layer 2 security mechanisms are used to prevent layer 2 based attacks.

b) Traffic insertion attacks

Where many routers share a common layer 2 network, for example on an Internet exchange point, it is possible for a third party to introduce packets into a network. This has been abused in the past on traditional exchange points by some service providers to default to another provider on this exchange point. In effect they are sending all their traffic into the other SPs network, even though the control plane (routing) might not allow that.

For this reason routers on exchange points or other shared layer 2 connections should only accept non-labelled IP packets into the global routing table. Any labelled packet must be discarded. This maintains VPN security of connected networks.

7. Summary and Conclusions

BGP/MPLS IP VPNs provide full address and traffic separation as in
traditional layer-2 VPN services. It hides addressing structures of the core and other VPNs, and it is in today’s understanding not possible from the outside to intrude into the core or other VPNs abusing the BGP/MPLS mechanisms. It is also not possible to intrude into the MPLS core if this is properly secured. However, there is a significant difference between BGP/MPLS based IP VPNs and for example FR or ATM based VPNs: The control structure of the core is on layer 3 in the case of MPLS. This caused significant skepticism in the industry towards MPLS, since this might open the architecture to DoS attacks from other VPNs or the Internet (if connected).

As shown in this document, it is possible to secure an BGP/MPLS IP VPN infrastructure to the same level of security than a comparable ATM or FR service. It is also possible to offer Internet connectivity to MPLS VPNs in a secure manner, and to interconnect different VPNs via firewalls. Although ATM and FR services have a strong reputation with regard to security, it has been shown that also in these networks security problems can exist [DataComm].

As far as attacks from within the MPLS core are concerned, all VPN classes (BGP/MPLS, FR, ATM) have the same problem: If an attacker can install a sniffer, he can read information in all VPNs, and if he has access to the core devices, he can execute a large number of attacks, from packet spoofing to introducing a new peer routers. There are a number of precautions measures outlined above that a service provider can use to tighten security of the core, but the security of the BGP/MPLS IP VPN architecture depends on the security of the service provider. If the service provider is not trusted, the only way to fully secure a VPN against attacks from the "inside" of the VPN service is to run IPsec on top, from the CE devices or beyond.

This document discussed many aspects of BGP/MPLS IP VPN security. It has to be noted explicitly that the overall security of this architecture depends on all components, and is determined by the security of the weakest part of the solution. For example a perfectly secured static BGP/MPLS IP VPN network with secured Internet access and secure management is still open to many attacks if there is a weak remote access solution in place.

Acknowledgements

The author would like to thank everybody who has provided input to this document. Specific thanks go to Yakov Rekhter for his continued strong support, and Loa Andersson, Alexander Manhenke and Jim Guichard for their extended feedback and support.

Author’s Address

Michael H. Behringer
Avda de la Vega, 15
28100 Alcobendas, Madrid
Spain
E-mail: mbehring@cisco.com
References

[Bonica] "CE-to-CE Authentication for Layer 3 VPNs". R. Bonica et al; draft-ietf-ppvpn-l3vpn-auth-00.txt; work in progress

[Behringer] "MPLS VPN Authentication". M. Behringer, J. Guichard; draft-behringer-mpls-vpn-auth-00.txt; work in progress


[Guichard] "CE-CE IPSec within an RFC-2547 Network". J. Guichard et al. draft-guichard-ce-ce-ipsec-00.txt; work in progress

[Guichard2] "Address Allocation for PE-CE links within an RFC2547bis Network". J. Guichard et al. draft-guichard-pe-ce-addr-00.txt; work in progress [xxx: ref correct?]


draft-behringer-mpls-security-04.txt page 19

Internet Draft Security of the MPLS Architecture May 2003


Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."