Michael Behringer
Jim Guichard
Cisco Systems, Inc.

Pedro Roque Marques
Juniper Networks, Inc.

IETF Internet Draft
Expires: December, 2004
Document: draft-behringer-mpls-vpn-auth-04.txt June, 2004

Layer-3 VPN Import/Export Verification

Status of this Memo

Abstract

Configuration errors on Provider Edge (PE) routers in Layer-3 VPN networks based on [RFC2547] can lead to security breaches of the connected VPNs. For example, the PE router could be mistakenly configured such that a connected Customer Edge (CE) router belongs to an incorrect VPN. Here we propose a scheme that verifies local and remote routing information received by the PE router before it installs new VPN routes into the Virtual Routing & Forwarding Instance (VRF). The proposed changes affect only the PE routers.

Table of Contents

1 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].

2 Problem Statement and Overview

The current Layer-3 VPN architecture as defined in [RFC2547] does not provide any mechanism to determine whether an imported route on a PE router originated from the correct VPN. This opens a potential security hole where the VPN Service Provider could mistakenly assign on a PE router the incorrect "route-target" values, thus inadvertently bringing a connected CE router, with the network/s behind it, into a wrong VPN.

[RFC2547] does not require that PE-CE sessions or PE-PE sessions be authenticated. However, in the cases where this is deployed, route authentication relies on a three-step configuration process; From the CE router to the PE router, from that PE router to other PE routers in the same VPN provider network, and from the other PE routers to the corresponding CE routers.

Correct access control between VPNs relies on the accurate configuration of "route-targets" on the PE routers. Because the 3 authentication steps above are essentially disjoint, the linkage necessary to "glue" them together is the correct configuration of the VPN provider network, and the corresponding "route-target" values. .

If the Service Provider has assigned the wrong "route-target" values then this is hard to detect from within the customer's network, and a real issue in [RFC2547] networks. One possible solution to this problem is to mount IPsec [RFC2401] on all CE routers, but this is

often perceived as too "heavy-weight". Therefore, a mechanism is

required which prevents routes from being passed into a PE router's Virtual Routing & Forwarding Instance (VRF), unless they have been verified to belong to the associated VPN. Also, in the case of such configuration errors, the Service Provider must be alerted so that the mistake can be rectified.

This proposal aims to solve the problem of accidental misconfiguration of VPN parameters on PE routers. The approach is to associate one or more authentication keys to a VPN, and use existing routing protocol authentication mechanisms [RFC2082, 2154, 2385], to provide PE-CE authentication. PE-PE routing exchanges are validated via routing update signatures. Since a PE router can hold several VRF's, the authentication between PEs will use the different MD5 keys, based on which VRF's routes need to be verified.

BGP UPDATE messages between PE routers will include a new BGP attribute, hereby referred to as the "UPDATE-authenticator". This attribute contains a keyed HMAC MD5 signature of a locally generated per-VRF random number, using the MD5 key that is also used on this PE router for the PE-CE routing authentication of that VPN.

The receiving PE router generates a keyed HMAC MD5 signature using information from the "UPDATE-authenticator" attribute contained within the BGP UPDATE message, and the routing key of the CE router that is to receive the routes contained within the update. If the result is different from the signature value transmitted in the UPDATE-authenticator attribute, the routes within the UPDATE are not imported and a warning is logged.

This proposal imposes some operational constraints to be workable; Regardless of whether a routing protocol is used or not within the VRF, at least one authentication key MUST be configured for each VRF that wishes to use the mechanisms described within this document. If a dynamic routing protocol is used, then routing with MD5 authentication [RFC2082, 2154, 2385] SHOULD be configured for all PE-CE links of a particular VPN. All CE routers of the same VPN MAY use the same or different MD5 keys and the PE router MUST indicate which key has been used when advertising routes from the associated VRF. If the Service Provider manages the CE routers on behalf of the customer, then downstream C routers MUST also use the same MD5 key. MD5 keys SHOULD be chosen to be unique to a VPN.

3 CE-CE Authentication

As previously stated, this document proposes to re-use the MD5 key

that is being used for PE-CE routing authentication. This has the advantage that no changes or software upgrades are necessary at the CE routers or within the VPN site. For this proposal to work, each PE router, on export of the routes from within a given VPN, MUST indicate which MD5 key has been used to authenticate the local routes. The MD5 key set SHOULD be unique to each VPN. The VPN customer configures thus all their CE routers with an MD5 key. The

VPN Service Provider also configures the PE routers with this local key on all links to the customers CE routers. This proposal does not affect the CE-PE routing authentication, but the authentication MUST be used for this scheme to work.

This proposal is orthogonal with MD5 authentication between PE routers on the VPN network. Authentication of peering sessions between PEs provides protection of the VPN routing information without any validation of its origin.

While currently, the VPN service provider may choose to configure routing authentication between the PE and CE, this information only affects the local routing session between the two routers. Conceptually, this proposal extends this key verification between the local PE and CE to remote PE to CE connections.

Using the mechanisms described within this document, the BGP UPDATE message, as defined in [RFC1771], is sent between PE routers (or BGP route reflectors), and carries a new UPDATE-authenticator attribute, which is used to verify the source of the routing information.

3.1 PE-CE Authentication Behavior

If a dynamic routing protocol is used between PE and CE routers, then the routing protocol is secured with MD5 authentication. Routes are only put into a VRF that is configured with Layer-3 VPN "Import/Export Verification" if the MD5 authentication is successful.

If a VRF is configured at the PE router for Layer-3 VPN "Import/Export Verification" using MD5 authentication, it is OPTIONAL to confirm local route authentication prior to any route export from the VRF. Route authentication involves checking whether the PE router can confirm route receipt from each CE router that is attached to the VRF.

3.2 Behaviour of PE sending the UPDATE-authenticator

When Layer-3 "Import/Export Verification" is enabled, the PE router SHOULD calculate a random number, referred to as the 'Generator', for each VRF that is configured for authentication. Alternatively a

combination of the local "route-target" values may be used to generate this number. This is implementation specific.

Having generated the VRF specific random number, the PE router on sending a [RFC2858] BGP UPDATE calculates a keyed HMAC-MD5 signature, as defined in [RFC2104], over the 'Generator', using the key of one of the CEs that is connected to the corresponding VRF. The result of this calculation is carried, along with the 'Generator' and an identification of the key used against the 'Generator', in the "HMAC-MD5 Signature" field within the UPDATE-authenticator attribute.

Each key within a VRF will have a corresponding 'key-identifier', which SHOULD be configurable within the VRF, and MUST be unique

across VPNs. Every PE router that holds members of the VPN MUST carry <key, key-identifier> mappings so that they can verify which key to use when authenticating incoming routing updates. The key-identifier MAY be the route-target.

The PE sending an [RFC2858] UPDATE will add a 'key-identifier' to the UPDATE-authenticator attribute to indicate which key should be used by a receiving PE router to verify the update. The UPDATE message is sent to any [RFC2858] BGP peers (other PE routers or BGP route reflectors). The "route-targets" in the [RFC2858] update determine which VRF/s the UPDATE refers to, and these are used as described in [RFC2547] to determine which PE routers will import which routes.

3.3 Behaviour of PE receiving the UPDATE-authenticator

A PE router that receives a [RFC2858] BGP update that contains the UPDATE-authenticator attribute SHOULD verify the contents of the update with the following algorithm. As an OPTIONAL step, the PE router MAY perform this comparison only if it has authenticated local routes from the CE router:

```
IF target VRF is configured for Layer-3 VPN Import/Exp. Verification
THEN
   IF UPDATE-authenticator attribute is present
   THEN
      subroutine determine_MD5-key
      verify UPDATE-authenticator with MD5-key
      IF result = signature of received UPDATE-authenticator
      THEN
         import route into VRF
      ELSE
         mark routes as 'not authenticated'; log error
   ELSE
```

```
      mark routes as 'not authenticated'; log error
   ELSE
      mark routes as 'not authenticated'; log error

   subroutine determine_MD5-key
      IF key-identifier = 0
      THEN
         MD5-key = the MD5 key used for routing authentication
                   with one of the routing peers of the VRF.
      ELSE
         MD5-key = lookup_in_config (key-identifier)
   RETURN MD5-key
```

A router MAY verify whether all MD5 keys for a given VRF are the same. If it does a warning message MUST be logged if it detects differences.

In the case where the Service Provider manages the CE routers, the Service Provider must also configure the key at the CE routers and this should match with any directly connected downstream C routers

within the customer site. If the C routers have a different key than the CE router then the CE will not authenticate any routes from within the site, and will therefore not advertise any routing information to the PE router. The PE router is thus able to use the previously described mechanisms and will not import/export any routes from/to the customers VRF.

4 Extranet VPN Processing

There are typically two types of Extranets that can be defined using the [RFC2547] architecture; Central Services Extranet and Distributed Extranet.

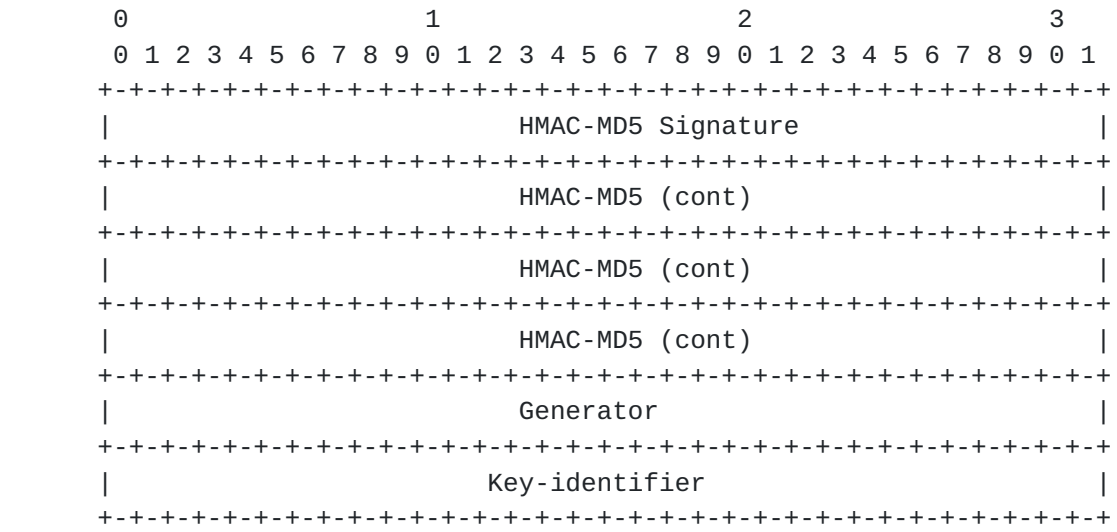
The Central Services Extranet provides connectivity between spoke VPN sites through a central PE router. This PE router carries routes for all members of the extranet whereas spoke PE routers carry only local routes, and a route to the central PE router. To support this type of configuration, the central PE router needs to carry <key, key-identifier> mappings for ALL members of the extranet. On receiving an incoming update, the central PE is able to identify which key to use on the UPDATE-authenticator attribute by looking at the key-identifier carried within the update.

The Distributed Extranet model provides connectivity directly between members of a given VPN. This means that each PE router that holds members of the extranet is configured to import the relevant "route-

target" values used for export by other members of the VPN. Using the key-identifier, a PE router is able to identify which key to use on an incoming update to verify the source. This means that each PE router within the extranet MUST carry <key, key-identifier> mappings for all members of the VPN.

5 The UPDATE-authenticator attribute

The UPDATE-authenticator attribute is an optional, transitive BGP attribute, with an attribute type code value to be assigned. Its length is 24 octets, which is the length of the output of an MD5 function (16 octets), a 'Generator' field, and a 'Key-identifier', as shown in the following figure.



6 IANA Considerations

The UPDATE-authenticator BGP attribute type will need to be registered with IANA, according to the procedures defined in [RFC2042].

7 Security Considerations

This modification to the behavior of the PE router aims at detecting inadvertent configuration mistakes of the Service Provider, and at isolating CE routers that appear not to belong to the VPN they were configured for.

There is no protection against the Service Provider staff maliciously

adding a CE router to a VPN. However, the malicious engineer must know the MD5 key of the VPN to be intruded. This threat can be avoided with CE-CE IPsec authentication, which is configured by the VPN customer, and to which the Service Provider does not have access.

8 Acknowledgements

Many thanks to Dan Tappan, David Allan and Eric Vyncke for their contributions to this work.

9 References

[RFC1771] "A Border Gateway Protocol 4 (BGP-4)". Y. Rekhter, T. Li. March 1995

[RFC2042] "Registering New BGP Attribute Types". B. Manning. January 1997.

[RFC2082] "RIP-2 MD5 Authentication". F. Baker, R. Atkinson. January 1997.

[RFC2104] "HMAC: Keyed-Hashing for Message Authentication". H. Krawczyk, M. Bellare, R. Canetti. February 1997.

[RFC2154] "OSPF with Digital Signatures". S. Murphy, M. Badger, B. Wellington. June 1997.

[RFC2385] "Protection of BGP Sessions via the TCP MD5 Signature Option". A. Heffernan. August 1998.

[RFC2547] "BGP/MPLS VPNs". E. Rosen, Y. Rekhter. March 1999.

[RFC2401] Kent and Atkinson, "Security Architecture for the Internet Protocol, RFC 2401, November 1998.

[RFC2858] Rekhter, Y. et al., Multiprotocol Extensions for BGP-4, RFC 2858, June, 2000.

10 Authors' Addresses

Michael H. Behringer
Cisco Systems, Inc.
Avda de la Vega, 15; 28100 Alcobendas, Madrid; Spain
Email: mbehring@cisco.com

Jim Guichard
Cisco Systems, Inc.
300 Apollo Drive
Chelmsford, MA, 01824
Email: jguichar@cisco.com

Pedro Marques
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
Email: roque@juniper.net

11 Full Copyright Statement