L3VPN Working Group
Internet-Draft
Expires: June 1, 2005

R. Bonica
Y. Rekhter
Juniper Networks
E. Rosen
R. Raszuk
D. Tappan
Cisco Systems

December 2004

CE-to-CE Member Verification for Layer 3 VPNs
draft-ietf-l3vpn-l3vpn-auth-01

Status of this Memo

Copyright Notice

Abstract

This document describes a CE-based verification mechanism that VPN customers can use to detect security breaches caused by misconfiguration of the provider network.

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 RFC2119 [3].

2. Overview

When properly configured, a Layer 3 Virtual Private Network (L3VPN) permits communications within a VPN, but prevents communication across VPN boundaries. In order to maintain this posture, the Service Provider must configure its network correctly. If the SP assigns a customer interface to the wrong VPN, or commits some other configuration error, unauthorized parties might join a VPN, while legitimate VPN members are unaware of the security breach.

Therefore, some VPN customers may require a CE-based mechanism for VPN membership verification. VPN customers could use the mechanism to detect security breaches caused by misconfiguration of the provider network.

This document describes a token-based approach to VPN membership verification. In order to join a VPN, each VPN site sends a token to the Provider Edge (PE) router to which it is attached. In many cases, the Customer Edge (CE) router originates the token. In configurations where the SP manages the CE, the customer can designate another device contained by the VPN site as the token originator.

Having received a token, the PE joins the VPN site to the VPN. The PE accepts and activates routes to the VPN site and distributes those routes throughout the provider network. The PE router also distributes the token throughout the provider network. All PE routers that support the VPN receive the token and relay it to each directly connected customer device that participates in the VPN. Customer devices use the token to verify membership of the newly joined VPN site.

If a customer device receives a token that it does not recognize, it issues an alarm requesting operator intervention. The customer device may also withdraw from the VPN, neither sending traffic to the VPN nor accepting traffic from it until an operator clears the security condition.

Note that the PE will not reveal any tokens to a customer device until it has received a token from the site that the customer device supports.

The token-based approach described by this document contains three components. These are:

Customer-to-PE signaling
PE-to-PE signaling
PE-to-Customer signaling

This document dedicates a section to each component.

3. Motivation

Currently, L3VPN customers cannot detect security breaches that are caused by accidental misconfiguration of the SP network. For example, assume that an SP maintains two VPN's. The first VPN supports Customer A while the second VPN supports Customer B. Assume also that Customer B requests a new VPN service connection. The SP processes Customer B's request, but accidentally configures Customer B's new connection into Customer A's VPN.

Typically, Customer B is first to detect the problem. Customer B tells the SP that an error has occurred and the SP corrects the error. The SP may or may not tell Customer A that his/her VPN has been breached.

The CE-to-CE verification mechanism, described herein, informs both customers of the VPN breach, providing immediate and automatic notification. It does not prevent the breach or the misconfiguration that caused it.

The CE-to-CE verification mechanism does not protect VPN customers from intentional misbehavior on the SP's part. The VPN customer must trust the SP to implement this mechanism faithfully.

4. Customer-to-PE Signaling

In order to join a VPN, each VPN site sends a token to the PE router to which it is attached. In many cases, the CE will originate the token. In configurations where the SP manages the CE, the customer may designate another device contained by the VPN site as the token originator.

If the device that originates the token also maintains a BGP [1] peering session with the PE, the originating device can append the token to each BGP update. To support this purpose, this document defines a new transitive extended community [EXTBGP] called CE-to-CE Verification Token. This community uses the format of the opaque extended community.

The high-order octet of the Type field of the CE-to-CE Authentication Token is 0x03. The low-order octet of the Type field is 0x02. The 6 octets of the Value field carries the token itself.

If the device that originates the token does not maintain a BGP peering session with the PE, the VPN site can use new protocol described in Section 7 of this document to send tokens to the PE. This protocol can be used in any VPN configuration, regardless of whether the originating device maintains a BGP peering session with the PE.

5. PE-to-PE Signaling

In order to support CE-based verification, the PE router MUST not activate routes to a directly connected VPN site until it has received a token from that site. When the PE has received a token, it activates those routes and advertise them to its iBGP peers. (That is, the PE advertises those routes to remote PE routers that support the VPN.)

If the provider network uses BGP to distribute VPN routes among PE routers, it appends the token to each BGP update. Section 4 of this document describes a BGP extended community attribute that supports this purpose.

If the provider network does not use BGP to distribute VPN routes among PE routers, it can use the new protocol described in Section 7 of this document to distribute tokens among PE routers.

6. PE-to-Customer Signaling

In order to support CE-based verification, the PE router MUST relay tokens that it receives from other PE routers to directly connected customer devices. The customer device can be a CE router or a directly connected host. If the PE and customer device maintain a BGP peering session with one another, the PE can use this BGP peering session to send tokens to the customer device. Section 4 of this document describes a BGP extended community attribute that supports this purpose.

Section 7 of this document describes a new protocol that also can be used to propagate tokens from PE to customer device. This protocol can be used in any VPN configuration, regardless of whether the customer device maintains a BGP peering session with the PE.

The PE MUST relay every token that it has acquired regarding a VPN to each directly connected customer device that participates in the VPN. When the PE router receives a new token, it MUST relay it to the appropriate customer devices immediately. Furthermore, the PE router MUST not reveal any tokens to customer devices that are contained by sites from which a token has not yet been received.

7. VPN Token Propagation Protocol

The VPN Token Propagation Protocol is used to distribute tokens. Figure 1 depicts the format of all messages.

Figure 1

Figure 1: message

The Version field is equal to 1.

The AuType field indicates how this message should be authenticated. It may contain the following values:

No Authentication 0
Simple Password 1
Message Digest-5 2

The Token field contains the verification token.

The Authentication field contains 64 bits of authentication data used to authenticate the message. The AuType field specifies how these 64 bits are to be used.

The VPN Token Propagation Protocol establishes soft state between PE and customer device. Announcements expire automatically upon expiration of a configurable timer. Therefore announcements must be repeated periodically. By default, announcements expire in 30 minutes, and should be refreshed 10 minutes.

The VPN Token Propagation Protocol obtains transport services from UDP. All VPN Token Propagation Protocol messages are directed to UDP port 3694.

8. Configurability

SPs can deploy the verification mechanisms described above globally or on a per-VPN basis. In either case, a particular VPN site within the verification domain may not be capable of announcing a token to the PE that supports it. In this case, the SP can configure the PE router so that it will permit that particular VPN site to join the VPN. The PE router will associate a null token (i.e., 0x000000000000) with the VPN site. The PE router will distribute this null token into the VPN as if it had been announced by the VPN site.

Although the null token may be useful during migration periods, customer should avoid its long term use.

9. Security Considerations

If VPN customer receives a token that it does not recognize, the VPN customer should contact his/her SP immediately. The VPN customer should also consider changing its token value, as the SP may have revealed that value to an unauthorized party.

10. IANA Considerations

IANA will assign a new extended BGP community sub-type, with the high-order octet of the Type field equal to 0x03 and low-order octet equal to 0x02. This BGP extended community type will represent the CE-to-CE Authentication Token.

IANA will has assigned UDP port number 3694 to the VPN Token Propagation Protocol, described in Section 7.

11. Acknowledgements

Thanks to Beth Alwin, Eduard Metz, Richard Morgan, Benson Schliesser and Paul Hoffman for their comments on this draft.

12 Normative References

[1] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[2] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Sangli, S., Tappan, D. and Y. Rekhter, "BGP Extended Communities Attribute", draft-ietf-idr-bgp-ext-communities-07 (work in progress), March 2004.

Authors' Addresses

Ronald P. Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, VA 20171
US

Phone: +1 571 203 1704
EMail: rbonica@juniper.net

Yakov Rekhter
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
US

EMail: yakov@juniper.net

Eric C. Rosen
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
US

EMail: erosen@cisco.com

Robert Raszuk
Cisco Systems
170 West Tasman Dr
San Jose, CA 95134
US

EMail: raszuk@cisco.com

Dan Tappan
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
US

EMail: tappan@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.