Network Working Group Acee Lindem (Redback Networks)
Internet Draft Anand Oswal (Redback Networks)
Expiration Date: Oct 2004
File name: draft-lindem-ospfv3-dest-filter-02.txt May 2004

OSPFv3 Destination Address Filter
draft-lindem-ospfv3-dest-filter-02.txt

Status of this Memo

Abstract

OSPFv2 has been criticized for it vulnerability to Denial of Service (DOS) attacks. With OSPFv3, it is a simple matter to filter on the destination address at an implementation dependent level in order to limit the scope of DOS attacks to directly attached routers. Unlike hop limit checking mechanisms, it is compatible with the existing OSPFv3 behavior. However, this level of protection will preclude the deployment of virtual links in topologies where the filtering is applied.

Table of Contents

1. Overview

OSPFv2 [OSPFv2] and OSPFv3 [OSPFv3] both have been criticised for their vulnerability to Denial of Service attacks [VULNER]. Both support cryptographic authentication to prevent an attacker from being able to spoof an OSPFv2 or OSPFv3 packet ([OSPFv2] and [AUTHv3]). However, in many cases the MD5 or IPSEC protection actually exacerbates the attack due to the computational overhead involved. For OSPFv3, this document proposes limiting accepted OSPFv3 packets to those that are not routable. Doing so allows these packets to be filtered at a low level for a relatively small computational cost.

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. Proposed Solution

In order to limit the vulnerability to DOS attacks to directly attached routers, OSPFv3 packets are only accepted if the destination address in the packet header is a link-local unicast address or link-local scoped multicast address. Both these address types are never forwarded more than one hop. Unlike hop limit checking mechanisms [GTSM], this technique is fully backward compatible with the OSPFv3 which doesn't specify that OSPFv3 packets be sent with a hop limit of 255. The only hop limit specification is that the link-scoped multicast packets are sent with a hop limit of 1. Hence, this mechanism can be deployed on one OSPFv3 router at a time.

In order to make the checking simple and low cost, this document suggests checking the first two octets of the IPv6 destination address for a valid link local unicast or link-local scoped multicast address. Based on the IPv6 Address Architecture [ADDR-ARCH], this would equate to:

```
if (((first-two-octets & 0xffc0) != 0xfe80) &&
    ((first-two-octets & 0xff0f) != 0xff02)) {
    drop the packet;
}
```

Alternately, an implementation may also check the multicast address flags to assure they are 0x0 since the OSPFv3 specification explicitly uses multicast addresses ff02::5 (AllSPFRouters) and ff02::6 (AllDRrouters) [OSPFv3].

```
if (((first-two-octets & 0xffc0) != 0xfe80) &&
    ((first-two-octets & 0xffff) != 0xff02)) {
    drop the packet;
}
```

2.1 Virtual Links

Virtual links make use of a global IPv6 unicast destination address.

Hence, the proposed destination address filter and virtual links are incompatible. Depending on the granularity of the filtering, virtual links may still be used (See Section 3.0).

2.2 Tunnels

In order to support OSPF over tunnels, e.g. GRE [GRE], it is necessary for the destination filter to be applied after OSPF packets are delivered to the tunnel endpoint and decapsulated. Furthermore, the encapsulated OSPFv3 packet's destination address should be AlllSPFRouters (FF02::5).

3.0 Implementation Placement and Granularity of Filter

The placement and granularity of the destination address filter is an engineering decision that must be made for each implementation. Obviously, the sooner it is done after packet reception the less resource that is consumed processing packets that will be dropped. However, since the checking has to be confined to OSPFv3 packets that are delivered locally it may be easier to delay the checking until the packets have been identified as such. A conveinent place in an implementation using the BSD socket model [SOCKET] is the point at which an inbound packet is added to the OSPFv3 socket.

The granularity of the check will limit the usage of virtual links at the granularity which it is applied. For example, if it is applied at the BSD socket level, virtual links may not be used by any OSPF instance utilizing that socket. Alternately, additional configuration and checking could be added at the socket level so that the destination filter is only applied to certain instances, areas, or interfaces. Implementations will need to balance their market requirements for virtual link deployment. In any case, the use of virtual link SHOULD be allowed either by configuration or the filter should be automatically disabled when a virtual link

is configured.

4. RIPng Applicability

The destination filter described herein is also applicable to RIPng [RIPNG]. The filter simply needs to be applied to UDP port 521. In RIPng there is no concept of a virtual link and no requirement to send to IPv6 global addresses.

5. Security Considerations

This document recommends a mechanism that can be used to limit OSPFv3 Denial of Service (DOS) attacks to directly attached networks. Hence, the entire document deals with security.

6. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. Normative References

[RFC-2119] Bradner, S., "Key words for use in RFC's to Indicate Requirement Levels", BCP 14, RFC 2119, March 1977.

[OSPFv2] Moy, J., "OSPF Version 2", RFC 2328, April 1998.

[OSPFv3] Coltun, R., D. Ferguson, and J. Moy, "OSPF for IPv6", RFC 2740, December 1999.

[ADDR-ARCH] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 3513, April 2003.

[SOCKET] Gilligan, B., S. Thomson, J. Bound, J. McCann, and R. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.

[RIPng] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

8. Informative References

[GTSM] Gill, V., J. Heasley, and D. Meyer, The Generalized TTL Security Mechanism (GTSM) drdraft-gill-gtsh-04.txt, Work in progress.

[AUTHv3] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", draft-ietf-ospf-ospfv3-auth-04.txt, Work in progress.

[VULNER] Jones, E. and O. Le Moigne, "OSPF Security Vulnerabilities Analysis", draft-jones-ospf-vuln-01.txt, Work in progress.

[GRE] Farinacci, D., T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

9. Acknowledgments

The authors wish to acknowledge Mukesh Gupta, Venkata Naidu, Enke Chen, and George Apostolopoulos for their review and comments.

10. Authors' Addresses

Acee Lindem
Redback Networks
102 Carric Bend Court
Cary, NC 27519
Email: acee@redback.com

Anand Oswal
Redback Networks
300 Holger
San Jose, CA
Email: aoswal@redback.com