OSPFv3 Automated Group Keying Requirements
draft-liu-ospfv3-automated-keying-req-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

This document MAY only be posted in an Internet-Draft.

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

This Internet-Draft will expire on August 26, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).
RFC 4552 describes how to provide authentication/confidentiality to OSPFv3 using IPsec. It specifies that same IPsec SA parameters be configured for both inbound and outbound SAs to provide the "one to many" security for multicast OSPFv3 communications over broadcast links (e.g., Ethernet). Manual keying is specified as the mandatory and default group key management solution. However, issues of scalability and security exist with manual keying. It is better to replace manual keying with automated group key management. This document discusses the requirements on OSPFv3 automated group key management, assuming that the centralized group key management architecture introduced in [RFC4046] is used.
1. Introduction

OSPFv3 [RFC2740] relies on IPSec to provide integrity, authentication, and/or confidentiality. RFC4552 describes how to provide authentication/confidentiality to OSPFv3 using AH/ESP. In Section 7 of RFC4552, it is proved that best scalability and feasibility can be achieved if the same parameters are used for both inbound and outbound AH/ESP SAs to provide the "one to many" communication security while running OSPFv3 over broadcast interfaces. It means that group security model be used to protect OSPFv3 multicast communications over broadcast network.

However, RFC4552 specifies Manual Keying [RFC4301] as the default group key management method, which is neither scalable nor secure. This document discusses replacing manual keying with automated keying. It is based on the fact that several GKM protocols have been, or being, standardized by MSEC working group [RFC3547] [RFC3830] [RFC4535] [GKDP], which makes it feasible to provide automated group key management for OSPFv3 using GKM protocols.
Meanwhile, [I-D: draft-ietf-msec-ipsec-extensions] describes multicast extensions to IPsec, which makes it feasible to provide group security to OSPFv3 using standard multicast IPsec.

This document describes the requirements on OSPFv3 automated group key management. It is assumed that the centralized group security architecture [RFC3740] and group key management architecture [RFC4046] would be used, where group SAs are centrally managed on separate key server(s). Use of group key agreement techniques, for example, Cliques [CLQUIES], is out of consideration.

2. Terminology

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.

Group Key Management (GKM) Protocol

A group key management protocol used by a GCKS to distribute IPsec Security Association policy and keying material. A GKM protocol is used when a group of IPsec devices require the same SAs. For example, when an IPsec SA describes an IP multicast destination, the sender and all receivers MUST have the group SA.

Group Member

An IPsec device that belongs to a group. A Group Member is authorized to be a Group Speaker and/or a Group Receiver.

Group Security Association (Group SA)

A collection of IPsec Security Associations (SAs) and GKM SAs necessary for a Group Member to receive key updates. A GSA describes the working policy for a group. Refer to RFC 4046 [RFC4046] for additional information.

State Synchronization (SS)

A generalization of OSPFv3 communications that occur after two routers discover each other. It includes neighbor discovering, exchanging DDs and LSAs, etc.

3. Requirements

The scenario shown in Fig.1 is used as the sample OSPFv3 deployment case to discuss the following requirements.
N1 is a broadcast network, where group SA is used to protect the OSPFv3 multicast communications among RT1-RT5. A separate machine serves as key server, which is not depicted in Fig. 1. Group members attached to N1, including RT1-RT5, get the group SA from key server. Every group member should know through which of its interfaces it reaches the key server. For convenience, broadcast interfaces attached to N1 are numbered as #1, which makes sense inside each router.

Types of networks N2-N6 are not fixed. They MAY be either broadcast, P2MP, or NBMA. It is likely that one, or more, of N2-N6 is a broadcast network either, and shares same group SA and key server with N1.

3.1. REQ-1: Protecting neighboring routers’ start process

When neighboring routers initially start, e.g., routers attached to N1, they have no routes to the key server and so, can not get the group SA. Measures MUST be provisioned to protect the initial communications among OSPFv3 routers before their adjacencies are established and routes are calculated out.
3.2. REQ-2: Protecting a single router’s join process

When a new router joins, it first performs SS process with its neighbors, and then calculates its routes. The new comer cannot access the key server, and thus cannot get the current group SA until the SS process is finished. Measures MUST be provided to protect the new comer’s OSPFv3 communications with existing routers before it gets group SA.

Another case is single router’s restart and re-join. During that process, key server MAY update the group SA and redistribute it to remaining routers. Therefore, after a router restarts and resumes the GSA from its storage (e.g., flash), it MAY find that its local GSA is out of synchronization with its neighbors’ GSA. Measures MUST be defined to deal with such de-synchronization.

3.3. REQ-3: Protecting neighboring routers’ restart process

Neighboring routers MAY simultaneously restart because of accidents (e.g., power-off). They need to re-perform SS and re-calculate their routes. Similar to REQ-1, routers can not get the group SA from the key server before routes converge. Measures MUST be provided to protect the redoing SS process.

3.4. REQ-4: Dealing with single point of key server failure

This requirement is obvious. And it is common to all Client/Server applications. The key servers MAY be out of service because of attacks, accidents, etc. Measures MUST be prepared to provide continuous keying service in case of single point of key server failure.

3.5. REQ-5: Secure distribution of group SA

Eavesdroppers can not access the group keys by intercepting the group SA distribution packets. All existing GKM protocols can meet this requirement.

3.6. REQ-6: Dealing with route flap

Routers might be shortly out of contact with the key server by reasons of route flaps,. During that process, the key server MAY update the group keys and distribute them to group members. Measures MUST be prepared for the group members to deal with such problems.

For example, only by #1 interface does RT1 reach the key server. If a route flap (e.g. Interface down/up) occurs on #1 interface, RT1 will
be out of contact with the key server, thus cannot receive the server-pushed rekeying messages any more. After the route resumes, RT1 will redo SS with its neighbors. Measures MUST be provided for RT1 to synchronize its group SA with others before re-handshaking in case that the server updates the group SA during the route flap.

3.7. REQ-7: Improving key server scalability

Some GKM protocols (e.g., GDOI and GKDP) support key server initiated rekeying. It is better to push rekeying messages using IP multicast to achieve better scalability for the key server when it serves a number of OSPFv3 routers.

On the other hand, it MAY be unpractical to set up one key server for each broadcast network. Therefore, it is likely to share same key server, even same GSA, among broadcast links. Both N1 and N2, for example, are broadcast networks and share same key server. Since inter-network IP multicast is seldom deployed, scalability issue MUST be carefully considered when key server initiated-rekeying mechanisms are used in above scenarios. Measures MUST be defined to improve the key server scalability in case that IP multicast is unavailable.

4. Security Considerations

This document lists requirements for automated group keying of OSPFv3. No new protocol is specified. Hence there is no security consideration.

5. IANA Considerations

This document has no IANA considerations.

6. Acknowledgments

Thank Zengjie Kou, Jinliang Feng and Zhenhai Li for technical discussions.

7. References

7.1. Normative References


7.2. Informative References


Author’s Addresses

Ya Liu  
Huawei Technologies  
Kuike Bld., No.9 Xinxi Rd., Shang-Di Information Industry Base  
Hai-Dian District, Beijing, P.R. China  
Phone: 8610-82836072  
Email: liuya@huawei.com

Russ White  
Cisco Systems  
Email: riw@cisco.com

Brian Weis  
Cisco Systems  
Email: bew@cisco.com

Michael Barnes  
Cisco Systems  
Email: mjbarnes@cisco.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that MAY cover technology that MAY be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Acknowledgment

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