Routing Control Plane Security Capabilities
draft-zhao-opsec-routing-capabilities-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 not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

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 March 9, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

The document lists the security capabilities needed for routing control plane of IP infrastructure to support the practices defined in [PRACTICES].
Capabilities are defined without reference to specific technologies. This is done to leave room for deployment of new technologies that implement the capability. Each capability cites the practices it supports. Current implementations that support the capability are cited. Special considerations are discussed as appropriate listing operational and resource constraints, limitations of current implementations, tradeoffs, etc.

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]

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>Functional Capabilities</td>
<td>3</td>
</tr>
<tr>
<td>2.1.</td>
<td>Route Authentication Capabilities</td>
<td>3</td>
</tr>
<tr>
<td>2.1.1.</td>
<td>Ability to configure/negotiate an authentication mechanism for an interface</td>
<td>3</td>
</tr>
<tr>
<td>2.1.2.</td>
<td>Ability to generate authentication data for route update</td>
<td>3</td>
</tr>
<tr>
<td>2.1.3.</td>
<td>Ability to verify authentication data of route update</td>
<td>4</td>
</tr>
<tr>
<td>2.1.4.</td>
<td>Ability to rekey manually or automatically</td>
<td>5</td>
</tr>
<tr>
<td>2.1.5.</td>
<td>Ability to be extensible to other authentication mechanisms</td>
<td>6</td>
</tr>
<tr>
<td>2.2.</td>
<td>Route Filtering Capabilities</td>
<td>6</td>
</tr>
<tr>
<td>2.2.1.</td>
<td>Ability to filter inbound or outbound route update</td>
<td>7</td>
</tr>
<tr>
<td>2.2.2.</td>
<td>Ability to filter specially used address</td>
<td>7</td>
</tr>
<tr>
<td>2.2.3.</td>
<td>Ability to filter routing update by address or prefix</td>
<td>8</td>
</tr>
<tr>
<td>2.2.4.</td>
<td>Ability to filter routing updates by protocols or ports</td>
<td>9</td>
</tr>
<tr>
<td>2.2.5.</td>
<td>Ability to filter routing update by TTL</td>
<td>9</td>
</tr>
<tr>
<td>2.2.6.</td>
<td>Ability to filter routing update by neighbour</td>
<td>10</td>
</tr>
<tr>
<td>2.2.7.</td>
<td>Ability to filter routing update by route properties</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.</td>
<td>Ability to limit the number of routes learned from a specific neighbour</td>
<td>11</td>
</tr>
<tr>
<td>2.2.9.</td>
<td>Ability to limit the length of prefixes</td>
<td>12</td>
</tr>
<tr>
<td>2.2.10.</td>
<td>Ability to filter route redistribution</td>
<td>12</td>
</tr>
<tr>
<td>2.3.</td>
<td>log</td>
<td>13</td>
</tr>
<tr>
<td>2.3.1.</td>
<td>Ability to log the failure of authentication</td>
<td>13</td>
</tr>
<tr>
<td>2.3.2.</td>
<td>Ability to counter and log denied packets</td>
<td>13</td>
</tr>
<tr>
<td>2.4.</td>
<td>Route Flap Dampening</td>
<td>14</td>
</tr>
<tr>
<td>2.4.1.</td>
<td>Ability to dampen route flap</td>
<td>14</td>
</tr>
<tr>
<td>2.5.</td>
<td>Architectural Security Capabilities</td>
<td>15</td>
</tr>
</tbody>
</table>
1. Introduction

The control plane is responsible for carrying the control information or signaling of the IP network. Its major elements are various unicast and multicast routing protocols. The control plane is very central to the network. Attacking to the control plane may lead to the collapse of the whole network.

The document tries to sum up the capabilities of control plane for IP networks.

2. Functional Capabilities

In the section, capabilities are listed to ensure the control plane security.

2.1. Route Authentication Capabilities

Routing protocol authentication prevents the introduction of false or unauthorized routing messages from unauthorized sources. With authentication configured, the router authenticates the source of each routing protocol packet that it got from its neighbors. Sometimes authentication keys or passwords are configured between neighbors. The shared keys or passwords are used to verify the authenticity of routing packets.

2.1.1. Ability to configure/negotiate an authentication mechanism for an interface

Capabilities.
The device has one or more methods to allow the protocol to negotiate or be configured an authentication mechanism (null authentication, simple password authentication, MD5 authentication etc) to be used between routing peers. The authentication mechanism implements data origin authentication and integrity verification for any routing update message from peers. Parameters related to the mechanism must be set by administrator or management software, too.

Supported Practices.

1. Route Authentication([PRACTICES] section 2.5.7)

2. Authentication is configurable

Current Implementations.

Authentication is defined in most routing protocols. Basically most routing protocols support 3 basic mechanisms: null authentication, simple password authentication and MD5 authentication. Null authentication doesn’t provide any data origin authentication or integrity verification service, and simple password authentication provides very weak authentication capability and is subject to many kinds of attacks. Relatively MD5 provides the security service in a more secure manner than other two mechanisms by applying cryptographic computation.

Considerations.

Null authentication and simple password authentication should be avoided in IP infrastructure network unless a high trustable environment is available.

The progress of cryptography makes MD5 collision feasible with current computation technologies. Whenever possible more strong authentication algorithm should be considered for candidate, such as SHA-256.

2.1.2. Ability to generate authentication data for route update

Capabilities.

When sending a route update to a peer a device is provided capability to invoke authentication algorithm to generate authentication data for the route update. The authentication data is sent to routing peer along with route update message.

Supported Practices.
1. Route Authentication([PRACTICES] section 2.5.7)

Current Implementations.

Once configured with authentication mechanism, routing protocol will invoke the algorithm to generate message authentication code (MAC), which is carried in a specific field of the message, 64 bit authentication field in OSPF for example. Typically MAC is generated by applying a key hash algorithm (MD5 for example) to the total message or part of the message.

Considerations.

None.

2.1.3. Ability to verify authentication data of route update

Capabilities.

When got a route update message with authentication data from routing peer, the device must be able to invoke a proper procedure to verify the rightness of the data. If the data is not correct, the message must be silently dropped.

Supported Practices.

1. Route Authentication([PRACTICES] section 2.5.7)

Current Implementations.

The receiver of the message applies keyed hash algorithm to the message or part of the message and gets a MAC. If the MAC is same to the one in the message, authentication passes.

Considerations.

None.

2.1.4. Ability to rekey manually or automatically

Capabilities.

The device provides the capability to allow rekey the shared secret by manually configuration or dynamic negotiation.

Supported Practices.
TBD

Current Implementations.

Most device implementation allows administrator to configure authentication parameters, including shared secret.

Considerations.

Dynamically parameter negotiation may be preferable feature for operator to reduce the effort of configuration.

2.1.5. Ability to be extensible to other authentication mechanisms

Capabilities.

The routing protocol can be extensible to support other authentication algorithm, such as SHA-1 or SHA-256.

Supported Practices.

This allows device to improve the security of control plane by extending stronger authentication mechanism to routing protocols.

Current Implementations.

OSPF has an AuType field to identify the authentication mechanism, new mechanism can be added to the protocol by defining new AuType and relevant processing procedure.

Considerations.

Most current routing protocols use MD5 for authentication. MD5 is proven a weak authentication algorithm and subject to some cryptographic attacks. It is important for routing protocols to support other authentication algorithm, such as SHA-1 or SHA-256, in the future.

2.2. Route Filtering Capabilities

In [FILTER] there are different filtering capabilities defined, some filtering capabilities in [FILTER] are applied to route update.

Route filtering is a generic method which is important and used widely in the field of the route security. We can prevent route looping and black hole through deploying it properly. Route filtering is also used to keep route information from leaking into illegal site
and often be used to counter against some attacks, such as by injecting false routes.

2.2.1. Ability to filter inbound or outbound route update Capabilities.

The device has the capability to filter the incoming or outgoing route updates according to configured filters. The receiver will spend less CPU cycles and memory to process route updates once inbound or outbound filtering is applied.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7)
2. Ability to filter inbound and outbound ([FILTER] section 2.1.10)
3. Filtering the inbound route updates is an effective countermeasure against spurious packets attack.

Current Implementations.

Most of the route protocols support methods to configure route filters which permit or deny learning or advertising of specific routes.

Consideration.

None

2.2.2. Ability to filter prefix for specific purpose Capabilities.

Some address spaces should not be used globally. For example, for an edge router the address blocks listed below should not be accepted:

loopback address, 127.0.0.0/8

RFC1918 address for private use, such as 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

prefix for link local address 169.254.0.0/16

prefix for multicast address 224.0.0.0/4
reserved address for IPv6/v4 interoperation 240.0.0.0/4

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7)

Current Implementations.

It is an essential function to filter prefix mentioned above to a edge router.

Consideration.

None

2.2.3. Ability to filter routing update by prefix

Capabilities.

The device is configured to explicitly permit or deny prefix received in route updates from neighbors by applying IP address filters. Implementation should support a rule set in which each element of the set is a rule with a specific action (deny/permit) to a prefix. If no rule is matched, the default action is applied to reject the route update.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7)

2. Avoid injection of false routes.

3. Limit propagation of invalid routes

Current Implementations.

Most route protocols support the feature.

By this feature administrator can prevent false routes from injecting and constrain the propagation of invalid routing information.

Consideration.

None
2.2.4. Ability to filter routing updates by protocols or ports

Capabilities.

The device provide a means to filter route packets based on the value of the protocol field in the IP header or the port field in the TCP or UDP header.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7

Current Implementations.

It is very common that more than one route protocols, such as OSPF and BGP, run in the same router. IGP update messages from outside of the route domain should be dropped.

It may be implemented by deploying ACLs.

Consideration.

None

2.2.5. Ability to filter routing update by TTL

Capabilities.

The device should provide a means to filter route packets based on the value of the TTL field in the IPv4 header or the Hop-Limit field in the IPv6 header.

Take adjacent routers for example, it is a good policy to drop the protocols packets whose TTL is not equal to 255.

TTL filters should not be enabled by default.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7

Current Implementations.

When a router got a packet, it will decrement TTL (Hop-Limit for IPv6) value of the packet by one. Thus, TTL spoofing is considered nearly impossible. Furthermore, vast majority of routing peers are adjacent.
TTL filter is a simple mechanism to authenticate origins and avoid attack by spoofing a routing packet.

[GTMS] introduced a generalized TTL security mechanism which can be used in several protocols.

Consideration.

It may be inadequate to use the technology where the situation is multi-hop and the number of hops changes frequently.

If a router is in an environment where neighbor can be spoofed or is not trustable the mechanism is not applicable.

2.2.6. Ability to filter routing update by neighbor.

Capabilities.

By default the device can learn routes from all available neighbors. Neighbor filtering can be configured to explicitly permit or deny learning route from specific neighbor.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7

Current Implementations.

By the method administrator can implement simple origin controlling without cryptographic authentication.

Consideration.

None

2.2.7. Ability to filter routing update by route attributes

Capabilities.

Some route protocols, such as BGP, attach attributes after route information. So route can be classified and filtered by the attributes values. Processing of receiving route is flexibly controlled.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7
Current Implementations.

Take BGP for example: router can filter routes received from BGP4 neighbors based on community names by either of the following methods. A community is an optional attribute that identifies the route as a member of a user defined class of routes. Community names are arbitrary values made of two five-digit integers joined by a colon. Administrator determines what the name means when community name is generated as one of a route’s attributes. Each string in the community name can be a number from 0 - 65535. This format allows administrator to easily classify community names. For example, a common convention used in community naming is to configure the first string as the local AS and the second string as the unique community within that AS. Using this convention, communities 1:10, 1:20, and 1:30 can be easily identified as member communities of AS 1.

Router can filter updates received from BGP4 neighbors based on the contents of the AS-path list accompanying the updates. For example, if administrator want to deny routes that have the AS 4.3.2.1 in the AS-path from entering the BGP4 route table, he can define a filter to deny such routes.

Consideration.

The device may support this type of filter, only if it is applicable.

2.2.8. Ability to limit the number of routes learned from a specific neighbor

Capabilities.

The device should provide a method to allow user to configure the amount of routes that can be learned for a specific neighbor.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7

Current Implementations.

A potential malicious neighbor may attack the routing table through injecting large amounts of routes which may result in the decline of efficiency. So it is reasonable to limit the amount of routes that can be learned from a specific neighbor.

Some BGP implementations has a ‘’Max Prefix-Limit’’ feature. A BGP neighbor would be shut down when the number reaches some threshold.
Consideration.

None

2.2.9. Ability to limit the length of prefixes

Capabilities.

The device may have the capability to allow filtering route updates by prefix length.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7)

Current Implementations.

With this method attacks can be mitigated, such as attacks mentioned in 2.2.8. In order to forge enough routes, the prefix length in false updates will always be long. For the routers used for large ISPs, prefix length in the routing table should be relatively short, so it is adequate to limit long prefix.

Consideration.

Some ISPs declare that they will not accept the announcements whose prefix length is greater than a specific threshold.

''long'' and ''short'' are relative. Administrator may choose a proper value according to the actual environment.

2.2.10. Ability to filter route redistribution

Capabilities.

The device should provide method to limit the scope of route redistribution between different route protocols.

Supported Practices.

1. Route Filter ([PRACTICES] section 2.5.7)

Current Implementations.

When more than two route protocols are available in a device in the same time, it is neccessary to share route information among them. Although route redistribution bridges between different route domains
and improves the flexibility of routing system, it may lead to looping or black hole as well. Furthermore, if false routes injected by the attacker are redistributed into other route domains (such as BGP), the scope of the attack may be extended. Thus filtering redistribution routes is necessary.

Some ISPs demand that an adjacent ISP should not configure unfiltered redistribution from his interior routing protocol into BGP.

Consideration.

None

2.3. log

2.3.1. Ability to log the failure of authentication

Capabilities.

The device has a capability to allow the failing authentication to be logged. The log must be stored in non-volatile media of the device or other log server.

Supported Practices.

Logging consideration ([PRACTICES] section 2.7)

Current Implementations.

Most devices provide logging function. A failing authentication indicates a security violation of the routing peer or an attack by malicious nodes.

Considerations.

None

2.3.2. Ability to counter and log denied packets

Capabilities.

The device should provide ability to counter and log denied packets. The log data is important for the audit. It is unnecessary to log everything, but the follow points should be captured:

Source and destination address
Source and destination port

Protocol

Packet type

Time

Supported Practices.

1. Logging consideration ([PRACTICES] section 2.5.7

Current Implementations.

Logging is an essential function used for auditing.

Consideration.

None

2.4. Route Flap Dampening

''route flap'' means that a route’s state changes from up to down or down to up. When ''route flap'' occurs, the route process has to insert or delete an item and the advertise update. That large amounts of routes continue to flap will exhausting CPU and finally result in DoS. The attacker can delete and insert routes to make route flap.

2.4.1. Ability to dampen route flap

Capabilities.

The device should provide ability to dampen route flap.

Different dampening algorithms may be involved in different parameters.

Supported Practices.

Route flapping dampening is the primary mechanism to mitigate the influence caused by flapping.

Current Implementations.

The function to dampen route flap may enhance the stability of routing system and minimize the influence of flapping. It is useful to counter against some DoS attacks.
BGP has implemented a dampening algorithm based on a penalty value.

Consideration.

None

2.5. Architectural Security Capabilities

Protective measures can be taken to prevent data from the data plane and management plane into the control plane. In fact majority of attacks aimed at the control plane are launched by the user in the data plane.

2.5.1. Ability to isolate control plane from data plane logically

Capabilities.

The device should provide the ability to isolate the control plane from the data plane.

Supported Practices.

1. Route Authentication([PRACTICES] section 2.5.7

Current Implementations.

Using routes authentication and origin filtering, it is ensured in some certain that malicious users in the data plane can not establish a session with the control plane.

Consideration.

None

2.6. Ability to provide route confidentiality

Capabilities.

The device should provides a means to prevent routing information from unauthorized disclosure. It is generally realized through using encryption.

Supported Practices.

1. Route Authentication([PRACTICES] section 2.5.7

Current Implementations.
It is not enough that only authentication is applied to route updates. Through intercepting route information, the attacker may perform analysis to the data and obtains the network topology.

Typically, a route protocol does not provide any encryption feature by itself. The most common measure is to combine an external encryption mechanism, such IPSec, SSL/TLS.

BGP can be deployed together with IPSec to ensure route data confidentiality.

Consideration.

None

2.7. Anti-replay

2.7.1. Ability to anti-replay

Capabilities.

The device should provide anti-replay mechanism to make it impossible for an attacker to insert packet in the route traffic.

Supported Practices.

1. Route Authentication ([PRACTICES] section 2.5.7

Current Implementations.

It is natural for protocol based on TCP that provides the slide window mechanism and detects sequence numbers repetition.

Other protocols which are not based on TCP can combine with special security protocols, such as IPSec, to provide the anti-replay feature.

Consideration.

None

3. Security Considerations

TBD

4. Acknowledgments

TBD
5. References

5.1. Normative References


5.2. Informative References


Author’s Addresses

Zhao Ye
Huawei Technologies
No.3, Xinxi Road, Shangdi Information Industry Base
Haidian District, Beijing City
P.R. China 100085
Phone: 86-10-8288 2793
Email: z48186@huawei.com

Miao Fuyou
Huawei Technologies
No.3, Xinxi Road, Shangdi Information Industry Base
Haidian District, Beijing City
P.R. China 100085
Phone: 86-10-8288 2502
Email: miaofy@huawei.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
Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2005).

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.

Acknowledgment

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