# Withdrawn Draft

**Warning Notice**

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

**Withdrawal Date** December 17, 2019

**Original Release Date** October 17, 2019

**Superseding Document**

| | |
|---|---|
| **Status** | Final |
| **Series/Number** | NIST Special Publication 800-189 |
| **Title** | Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation |
| **Publication Date** | December 2019 |
| **DOI** | https://doi.org/10.6028/NIST.SP.800-189 |
| **CSRC URL** | https://csrc.nist.gov/publications/detail/sp/800-189/final |
| **Additional Information** | |

National Institute of Standards and Technology
U.S. Department of Commerce

**DRAFT (2nd) NIST Special Publication 800-189**

# Resilient Interdomain Traffic Exchange:

## *BGP Security and DDoS Mitigation*

Kotikalapudi Sriram
Doug Montgomery

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-189-draft2

COMPUTER SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

# DRAFT (2nd) NIST Special Publication 800-189

# Resilient Interdomain Traffic Exchange:

## *BGP Security and DDoS Mitigation*

Kotikalapudi Sriram
Doug Montgomery
*Advanced Network Technology Division*
*Information Technology Laboratory*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-189-draft2

October 2019

U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

## Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-189
Natl. Inst. Stand. Technol. Spec. Publ. 800-189, 80 pages (October 2019)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-189-draft2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

**Public comment period: *October 17, 2019* through *November 15, 2019***

National Institute of Standards and Technology
Attn: Advanced Network Technologies Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8920) Gaithersburg, MD 20899-8920
Email: sp800-189@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

## Abstract

In recent years, numerous routing control plane anomalies, such as Border Gateway Protocol (BGP) prefix hijacking and route leaks, have resulted in denial-of-service (DoS), unwanted data traffic detours, and performance degradation. Large-scale distributed denial-of-service (DDoS) attacks on servers using spoofed internet protocol (IP) addresses and reflection-amplification in the data plane have also been frequent, resulting in significant disruption of services and damages. This special publication on Resilient Interdomain Traffic Exchange (RITE) includes initial guidance on securing the interdomain routing control traffic, preventing IP address spoofing, and certain aspects of DoS/DDoS detection and mitigation.

Many of the recommendations in this publication focus on the Border Gateway Protocol (BGP). BGP is the control protocol used to distribute and compute paths between the tens of thousands of autonomous networks that comprise the internet. Technologies recommended in this document for securing the interdomain routing control traffic include Resource Public Key Infrastructure (RPKI), BGP origin validation (BGP-OV), and prefix filtering. Additionally, technologies recommended for mitigating DoS/DDoS attacks focus on prevention of IP address spoofing using source address validation (SAV) with access control lists (ACLs) and unicast Reverse Path Forwarding (uRPF). Other technologies (including some application plane methods) such as remotely triggered black hole (RTBH) filtering, flow specification (Flowspec), and response rate limiting (RRL) are also recommended as part of the overall security mechanisms.

## Keywords

Routing security and robustness; Internet infrastructure security; Border Gateway Protocol (BGP) security; prefix hijacks; IP address spoofing; distributed denial-of-service (DDoS); Resource Public Key Infrastructure (RPKI); BGP origin validation (BGP-OV); prefix filtering; BGP path validation (BGP-PV); BGPsec; route leaks; source address validation (SAV); unicast Reverse Path Forwarding (uRPF); remotely triggered black hole (RTBH) filtering; flow specification (Flowspec).

## Acknowledgements

The authors are grateful to William T. Polk, Scott Rose, Okhee Kim, Oliver Borchert, Susan Symington, William C. Barker, William Haag, Allen Tan, and Jim Foti for their review and comments.

## Audience

This document gives technical guidance and recommendations for resilient interdomain traffic exchange. The primary audience includes information security officers and managers of federal enterprise networks. The guidance applies to the network services of hosting providers (e.g., cloud-based applications and service hosting) and internet service providers (ISPs) when they are used to support federal IT systems. The guidance may also be useful for enterprise and transit network operators and equipment vendors in general.

It is expected that the guidance and applicable recommendations in this publication will be incorporated into the security plans and operational processes of federal enterprise networks. Likewise, it is expected that applicable recommendations will be incorporated into the service agreements for federal contracts for hosted application services and internet transit services.

## Trademark Information

All registered trademarks belong to their respective organizations.

## Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sp800-189@nist.gov

# Executive Summary

There have been numerous incidents in recent years involving routing control plane anomalies such as Border Gateway Protocol (BGP) prefix hijacking, route leaks, and other forms of misrouting resulting in denial-of-service (DoS), unwanted data traffic detours, and performance degradation. Large-scale distributed DoS (DDoS) attacks on servers using spoofed internet protocol (IP) addresses and reflection amplification in the data plane have also been frequent, resulting in significant disruption of services and damages.

This document provides technical guidance and recommendations for technologies that improve the security and robustness of interdomain traffic exchange. The primary focus of these recommendations are the points of interconnection between enterprise networks, or hosted service providers, and the public internet—in other words, between what are commonly known as "stub" networks (i.e., those networks that only provide connectivity to their end systems) and transit networks (i.e., those networks that serve to interconnect and pass traffic between stub networks and other transit networks). These points of interconnection between stub and transit networks are often referred to as the "internet's edge." There is usually a contractual relationship between the transit networks and the stub networks that they service, and the set of technical procedures and policies defined in that relationship is commonly called the "peering policy."

Many of the recommendations in this document also apply to the points of interconnection between two transit networks. There are instances in which the recommendations for interdomain traffic exchange between transit networks will vary from those for exchanges between stub and transit networks.

The provided recommendations reduce the risk of accidental attacks (caused by misconfiguration) and malicious attacks in the routing control plane, and they help detect and prevent IP address spoofing and resulting DoS/DDoS attacks. These recommendations primarily cover technologies (for security and robustness) to be used in border routers that operate the Border Gateway Protocol (commonly called BGP routers). However, they also extend to other systems that support reachability on the internet (e.g., Resource Public Key Infrastructure (RPKI) repositories, Domain Name Servers (DNS), other open internet services).

It is expected that the guidance and applicable recommendations from this publication will be incorporated into the security plans and operational processes of federal enterprise networks. Likewise, it is expected that applicable recommendations will be incorporated into the service agreements for federal contracts for hosted application services and internet transit services. This document may also contribute to the ongoing efforts by NIST and NTIA [DOC-Botnet] [Botnet-Roadmap] to respond to Presidential Executive Order 13800 [PEO-13800].

Technologies recommended in this document for securing interdomain routing control traffic include Resource Public Key Infrastructure (RPKI), BGP origin validation (BGP-OV), and prefix filtering. Additionally, technologies recommended for mitigating DoS/DDoS attacks include prevention of IP address spoofing using source address validation (SAV) with access control lists (ACLs) and unicast Reverse Path Forwarding (uRPF). Other technologies (including some application plane methods) such as remotely triggered black hole (RTBH) filtering, flow

specification (Flowspec), and response rate limiting (RRL) are also recommended as part of the overall security mechanisms.

## Table of Contents

**Executive Summary ..... vi**
**1 Introduction ..... 1**
1.1 What This Guide Covers ..... 1
1.2 What This Guide Does Not Cover ..... 1
1.3 Document Structure ..... 2
1.4 Conventions Used in this Guide ..... 2
**2 Control Plane/BGP Vulnerabilities ..... 3**
2.1 Prefix Hijacking and Announcement of Unallocated Address Space ..... 3
2.2 AS Path Modification ..... 4
2.3 Route Leaks ..... 4
**3 IP Address Spoofing & Reflection Amplification Attacks ..... 7**
3.1 Spoofed Source Addresses ..... 7
3.2 Reflection Amplification Attacks ..... 7
**4 Control Plane/BGP Security – Solutions and Recommendations ..... 9**
4.1 Registration of Route Objects in Internet Routing Registries ..... 9
4.2 Certification of Resources in Resource Public Key Infrastructure ..... 10
4.3 BGP Origin Validation (BGP-OV) ..... 12
4.3.1 Forged-Origin Hijacks – How to Minimize Them ..... 16
4.4 Categories of Prefix Filters ..... 17
4.4.1 Unallocated Prefixes ..... 17
4.4.2 Special Purpose Prefixes ..... 18
4.4.3 Prefixes Owned by an AS ..... 18
4.4.4 Prefixes that Exceed a Specificity Limit ..... 18
4.4.5 Default Route ..... 18
4.4.6 IXP LAN Prefixes ..... 19
4.5 Prefix Filtering for Peers of Different Types ..... 19
4.5.1 Prefix Filtering with Lateral Peer ..... 19
4.5.2 Prefix Filtering with Transit Provider ..... 20
4.5.3 Prefix Filtering with Customer ..... 21
4.5.4 Prefix Filtering Performed in a Leaf Customer Network ..... 21
4.6 Role of RPKI in Prefix Filtering ..... 22
4.7 AS Path Validation (Emerging/Future) ..... 22

4.8 Checking AS Path for Disallowed AS Numbers ........ 24
4.9 Route Leak Solution ........ 24
4.10 Generalized TTL Security Mechanism (GTSM) ........ 25
**5 Securing Against DDoS & Reflection Amplification – Solutions and Recommendations ........ 27**
5.1 Source Address Validation Techniques ........ 27
5.1.1 SAV Using Access Control Lists ........ 27
5.1.2 SAV Using Strict Unicast Reverse Path Forwarding ........ 28
5.1.3 SAV Using Feasible-Path Unicast Reverse Path Forwarding ........ 28
5.1.4 SAV Using Loose Unicast Reverse Path Forwarding ........ 30
5.1.5 SAV Using VRF Table ........ 30
5.1.6 SAV Using Enhanced Feasible-Path uRPF (Emerging/Future) ........ 30
5.1.7 More Effective Mitigation with Combination of Origin Validation and SAV 31
5.2 SAV Recommendations for Various Types of Networks ........ 32
5.2.1 Customer with Directly Connected Allocated Address Space: Broadband and Wireless Service Providers ........ 32
5.2.2 Enterprise Border Routers ........ 33
5.2.3 Internet Service Providers ........ 33
5.3 Role of RPKI in Source Address Validation ........ 34
5.4 Monitoring UDP/TCP Ports with Vulnerable Applications and Employing Traffic Filtering ........ 35
5.5 BGP Flow Specification (Flowspec) ........ 38
**References ........ 41**

## List of Appendices

**Appendix A— Consolidated List of Security Recommendations ........ 55**
**Appendix B— Acronyms ........ 67**

## List of Figures

Figure 1: Illustration of Prefix Hijacking and Announcement of Unallocated Address Space ........ 3
Figure 2: Illustration of the basic notion of a route leak ........ 5
Figure 3: DDoS by IP source address spoofing and reflection and amplification ........ 8

Figure 4: Illustration of resource allocation and certificate chain in RPKI ...................... 11
Figure 5: Creation of Route Origin Authorization (ROA) by prefix owner ...................... 12
Figure 6: RPKI data retrieval, caching, and propagation to routers ............................... 13
Figure 7: Algorithm for origin validation (based on RFC 6811)..................................... 14
Figure 8: Basic principle of signing/validating AS paths in BGP updates ...................... 23
Figure 9: Scenario 1 for illustration of efficacy of uRPF schemes ................................ 28
Figure 10: Scenario 2 for illustration of efficacy of uRPF schemes ............................... 29
Figure 11: Scenario 3 for illustration of efficacy of uRPF schemes ............................... 31
Figure 12: Illustration of how origin validation complements SAV ................................ 32

## List of Tables

Table 1: Common Applications and their TCP/UDP Port Numbers ............................... 36
Table 2: BGP Flowspec types ......................................................................... 39
Table 3: Extended community values defined in Flowspec to specify various types of actions ......................................................................................... 39
Table 4: Consolidated List of the Security Recommendations ..................................... 55

# 1 Introduction

## 1.1 What This Guide Covers

This guide provides technical guidelines and recommendations for deploying protocols and technologies that improve the security of interdomain traffic exchange. These recommendations reduce the risk of accidental attacks (caused by misconfiguration) and malicious attacks in the routing control plane, and they help detect and prevent IP address spoofing and resulting DoS/DDoS attacks. These recommendations primarily cover protocols and techniques to be used in BGP routers. However, they also extend, in part, to other systems that support reachability on the internet (e.g., RPKI repositories, DNS, and other open internet services).

Technologies recommended in this document for securing interdomain routing control traffic include RPKI, BGP origin validation (BGP-OV), and prefix filtering. Additionally, technologies recommended for mitigating DoS/DDoS attacks include prevention of IP address spoofing using source address validation (SAV) with access control lists (ACLs) and unicast Reverse Path Forwarding (uRPF). Other technologies (including some application plane methods) such as remotely triggered black hole (RTBH) filtering, flow specification (Flowspec), and response rate limiting (RRL) are also recommended as part of the overall security mechanisms.

This document addresses many of the same concerns as highlighted in [CSRIC4-WG6] regarding BGP vulnerabilities and DoS/DDoS attacks but goes into greater technical depth in describing standards-based security mechanisms and providing specific security recommendations.

## 1.2 What This Guide Does Not Cover

BGP origin validation relies on a global RPKI system (e.g., certificate authorities, publication repositories, etc.) as the source of trusted information about internet address holders and their route origin authorization statements. Each RIR operates trusted root CA in the RPKI system and publishes a Certificate Practice Statement [RFC7382] describing the security and robustness properties of each implementation. Each RPKI CA has integrity and authentication mechanisms for data creation, storage, and transmission. Nevertheless, compromise of the underlying servers and/or registry services is still a potential, if low probability, threat. Making security recommendations for mitigating against such threats is outside of the scope of this document.

Transport layer security is key to the integrity of messages communicated in BGP sessions. Making security recommendations for the underlying transport layer is also outside of the scope of this document.

DDoS attacks use spoofed IP addresses to exploit connectionless query-response services (e.g., DNS, Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP) servers) to “reflect” and amplify the impact on intended targets. This document addresses some but not all aspects of security hardening of the servers that are exploited for reflection and amplification. Security measures—such as limiting the packet rate of outlier source addresses, IP connections, or syn-proxy—may be effectively employed at servers that are used for reflection and amplification of DoS/DDoS attacks, but this document does not cover them.

## 1.3 Document Structure

The rest of the document is presented in the following manner:

- **Section 2:** Routing control plane attacks (e.g., BGP prefix hijacking, autonomous system (AS) path modification, and route leaks) are described.
- **Section 3:** Data plane attacks involving source IP address spoofing and reflection amplification are described.
- **Section 4:** Solutions are described, and security recommendations are made for routing control plane/BGP security. The solution technologies that are discussed include RPKI, BGP origin validation (BGP-OV), prefix filtering, BGP path validation (BGP-PV), Generalized TTL Security Mechanism (GTSM), and route leak detection and mitigation.
- **Section 5:** Solutions are described, and security recommendations are made for detection and mitigation of source IP address spoofing and reflection amplification attacks. The solution technologies that are discussed include ACLs, various uRPF methods, response rate limiting (RRL), RTBH, and Flowspec.

## 1.4 Conventions Used in this Guide

Throughout this guide, the following format conventions are used to denote special use text:

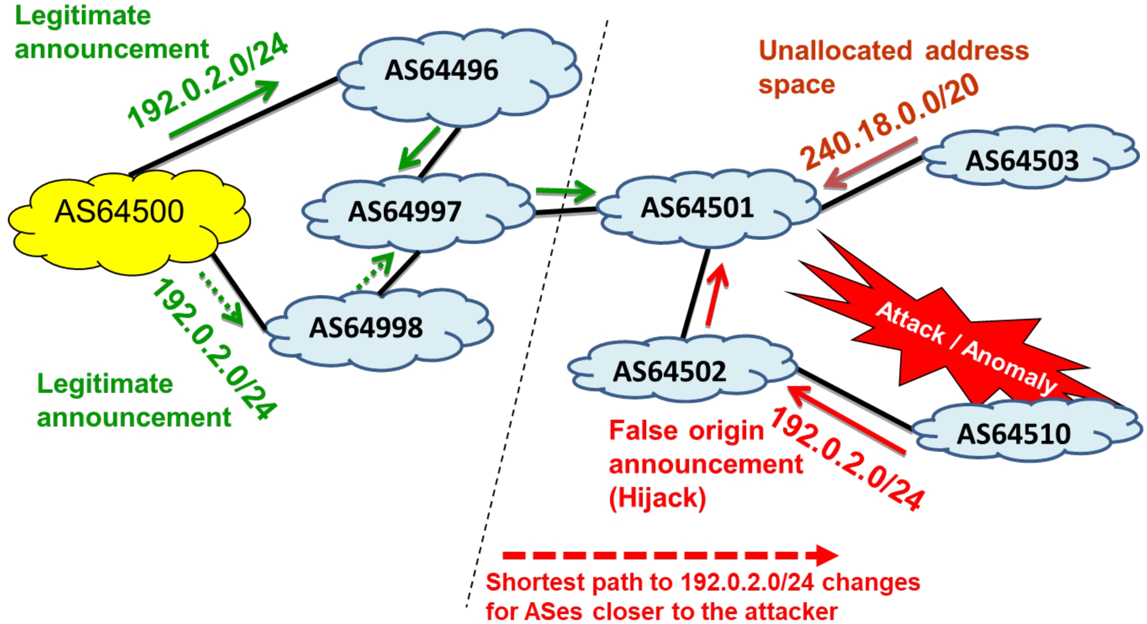
"**Security Recommendation**" denotes a recommendation that should be addressed in security plans, operational practices, and agreements for contracted services.

URLs are included in the text and references to guide readers to a given website or online tool designed to aid administrators. This is not meant to be an endorsement of the website or any product/service offered by the website publisher. All URLs were considered valid at the time of writing.

# 2 Control Plane/BGP Vulnerabilities

## 2.1 Prefix Hijacking and Announcement of Unallocated Address Space

A BGP prefix hijack occurs when an autonomous system (AS) accidentally or maliciously originates a prefix that it is not authorized (by the prefix owner) to originate. This is also known as false origination (or announcement). In contrast, if an AS is authorized to originate/announce a prefix by the prefix owner, then such a route origination/announcement is called legitimate. In the example illustrated in Figure 1, prefix 192.0.2.0/24 is legitimately originated by AS64500, but AS64510 falsely originates it. The path to the prefix via the false origin AS will be shorter for a subset of the ASes on the internet, and this subset of ASes will install the false route in their routing table or forwarding information base (FIB). That is, ASes for which AS64510 is closer (i.e., shorter AS path length) would choose the false announcement, and thus data traffic from clients in those ASes destined for the network 192.0.2/24 will be misrouted to AS64510.




**Adverse effects: denial-of-service, misrouting of traffic, unauthorized routing**

**Figure 1: Illustration of Prefix Hijacking and Announcement of Unallocated Address Space**

The rules for IP route selection on the internet always prefer the most specific (i.e., longest) matching entry in a router's FIB. When an offending AS falsely announces a more-specific prefix (than a prefix announced by an authorized AS), the longer, unauthorized prefix will be widely accepted and used to route data. Figure 1 also illustrates an example of unauthorized origination of unallocated (reserved) address space 240.18.0.0/20. Currently, 240.0.0.0/8 is reserved for future use [IANA-v4-r]. Similarly, an AS may also falsely originate allocated but currently unused address space. This is referred to as prefix squatting, where someone else's unused prefix is temporarily announced and used to send spam or some other malicious purpose.

The various types of unauthorized prefix originations described above are called prefix hijacks or false origin announcements. The unauthorized announcement of a prefix longer than the legitimate announcement is called a sub-prefix hijack. The consequences of such adverse actions can be serious and include denial-of-service, eavesdropping, misdirection to imposter servers (to steal login credentials or inject malware), or defeat of IP reputation systems to launch spam email. There have been numerous incidents involving prefix hijacks in recent years. There are several commercial services and research projects that track and log anomalies in the global BGP routing system [BGPmon] [ThousandEyes] [BGPStream] [ARTEMIS]. Many of these sites provide detailed forensic analyses of observed attack scenarios.

### 2.2 AS Path Modification

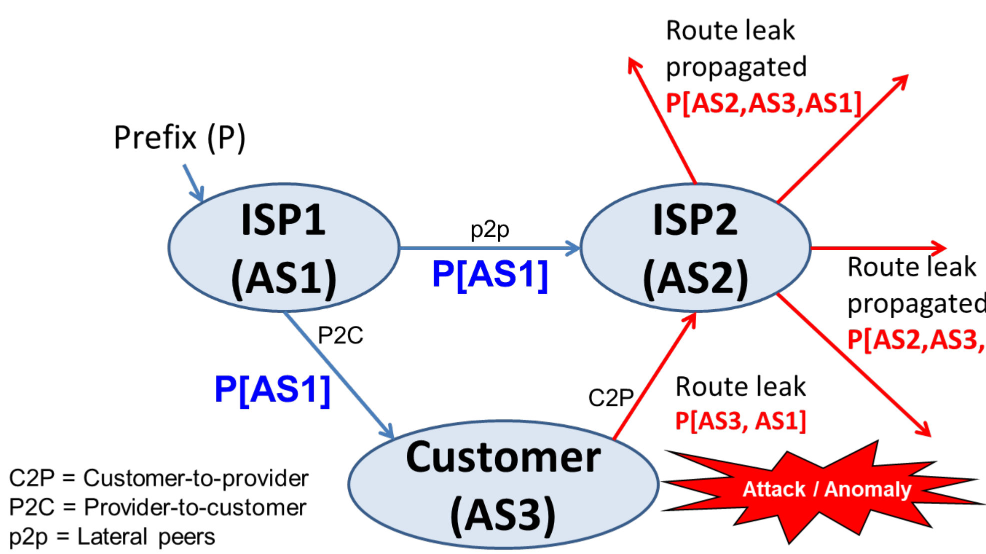
BGP messages carry a sequence of AS numbers that indicates the “path” of interconnected networks over which data will flow. This “AS_PATH” [RFC4271] data is often used to implement routing policies that reflect the business agreements and peering policies that have been negotiated between networks. BGP is also vulnerable to modification of the AS_PATH information that it conveys. As an example, a malicious AS which receives a BGP update may illegitimately remove some of the preceding ASes in the AS_PATH attribute of the update to make the path length seem shorter. When the update modified in this manner is propagated, the ASes upstream can be deceived to believe that the path to the advertised prefix via the adversary AS is shorter. By doing this, the adversary AS may seek to illegitimately increase its revenue from its customers, or may be able to eavesdrop on traffic that would otherwise not transit through their AS.

Another example of maliciously modifying a BGP update is when an adversary AS replaces a prefix in a received update with a more-specific prefix (subsumed by the prefix) and then forwards the update to neighbors. This attack is known as a Kapela-Pilosov attack [Kapela-Pilosov]. Only the prefix is replaced by a more-specific prefix, but the AS path is not altered. In BGP path selection, a more-specific prefix advertisement wins over a less-specific prefix advertisement. This means that ASes on the internet would widely accept and use the adversary AS’s advertisement for the more-specific prefix. The exceptions are the ASes that are in the AS path from the adversary to the prefix. These exception ASes reject any advertisements that they may receive for the more-specific prefix because they detect their own AS number in the AS path. This is called avoidance of loop detection and is a standard practice in BGP. Thus, the data path from the adversary AS to the prefix (i.e., the network in consideration) remains intact (i.e., unaffected by the malicious more-specific advertisement). The net result of this attack is very serious. The adversary would be able to force almost all traffic for the more-specific prefix to be routed via their AS. Thus, they can eavesdrop on the data (destined for the more-specific prefix) while channeling it back to the legitimate destination to avoid detection.

### 2.3 Route Leaks

Previously, it was noted that the interconnections of networks on the internet are dictated by contracted business relationships that express the policies and procedures for the exchange of control and data traffic at each point of interconnection. Such peering policies often specify limits on what routing announcements will be accepted by each party. Often these policies reflect a customer, transit provider, and/or lateral peer business relationship between networks.

***Definitions of Peering Relations, Customer Cone:*** These definitions are useful for route leaks (here and in Section 4.9) and also for BGP-OV (Section 4.3), prefix filtering (Sections 4.4 and 4.5), and SAV/uRPF (Sections 5.1 and 5.2). A transit provider typically provides service to connect its customer(s) to the global internet. A customer AS or network may be single-homed to one transit provider or multi-homed to more than one transit providers. A stub customer AS has no customer ASes or lateral peer ASes of its own. A leaf customer is a stub customer that is single-homed to one transit provider and not connected to any other AS. Peering relationships considered in this document are provider-to-customer (P2C), customer-to-provider (C2P), and peer-to-peer (p2p). Here, "provider" refers to transit provider. The first two are transit relationships. A peer connected via a p2p link is known as a lateral peer (non-transit). A customer cone of AS A is defined as AS A plus all the ASes that can be reached from A following only P2C links [Luckie]. The term "customer cone prefixes" of an AS refers to the union of the prefixes received from all directly connected customers and the prefixes originated by the AS itself. Naturally, this set recursively includes customers' prefix advertisements (down the hierarchy). ASes that have a lateral peering (i.e., p2p) relationship typically announce their customer cone prefixes to each other and subsequently announce the lateral peer's customer cone prefixes to their respective customers but not to other lateral peers or transit providers.




In general, ISPs prefer customer route announcements over those from others.

**Figure 2: Illustration of the basic notion of a route leak**

These relationships are significant because much of the operation of the global internet is designed such that a stub or customer AS should never be used to route between two transit ASes. This policy is implemented by insuring that stub or customer ASes do not pass BGP routing information received from one transit provider to another. Figure 2 illustrates a common form of route leak that occurs when a multi-homed customer AS (such as AS3 in Figure 2) learns a prefix update from one transit provider (ISP1) and "leaks" the update to another transit provider (ISP2) in violation of intended routing policies, and the second transit provider does not detect the leak and propagates the leaked update to its customers, lateral peers, and transit ISPs

[RFC7908]. Some examples of recent route leak incidents include: 1) the MainOne (a Nigerian ISP) leaks of Google prefixes, which caused an outage of Google services for over an hour in November 2018 [Naik]; (2) the Dodo-Telstra incident in March 2012, which caused an outage of internet services nationwide in Australia [Huston2012]; and (3) the massive Telekom Malaysia route leaks, which Level3, in turn, accepted and propagated [Toonk-B].

More generally, as defined in [RFC7908], a route leak is the propagation of routing announcements beyond their intended scope. That is, an AS's announcement of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender, and/or one of the ASes along the preceding AS path.

In [RFC7908], several types of route leaks are enumerated and described together with examples of recent incidents. The result of a route leak can include redirection of traffic through an unintended path, which may enable eavesdropping or malicious traffic analysis. When a large number of routes is leaked simultaneously, the offending AS is often overwhelmed by the resulting unexpected data traffic and drops much of the traffic that it receives [Huston2012] [Toonk-A] [Naik]. This causes blackholing and denial-of-service for the affected prefixes. Route leaks can be accidental or malicious but most often arise from accidental misconfigurations.

# 3 IP Address Spoofing & Reflection Amplification Attacks

## 3.1 Spoofed Source Addresses

Distributed denial-of-service (DDoS) is a form attack where the attack traffic is generated from many distributed sources to achieve a high-volume attack and directed towards an intended victim (i.e., system or server) [ISOC] [Huston2016] [Mirai1]. To conduct a direct DDoS attack, the attacker typically makes use of a few powerful computers or a vast number of unsuspecting, compromised third-party devices (e.g., laptops, tablets, cell phones, Internet of Things (IoT) devices, etc.). The latter scenario is often implemented through botnets [Arbor] [Huston2016] [DOC-Botnet]. In many DDoS attacks, the IP source addresses in the attack messages are "spoofed" to avoid traceability [Arbor]. Some DDoS attacks are launched without using spoofed source addresses. For example, in the Mirai attacks [Mirai1] [Mirai2] [Winward] [TA16-288A], a very large number of compromised bots (IoT devices) sending the attack traffic used the normal source IP addresses of the IoT devices. Further, the source addresses could also belong to a hijacked prefix with the intention of deceiving source address validation (SAV) [BCP38] [BCP84] (also see Section 5.1.7). If a hijacked prefix is being used, then the source addresses appearing in the DDoS attack packets are sometimes randomly selected from that prefix.

## 3.2 Reflection Amplification Attacks

Source address spoofing is often combined with reflection and amplification from poorly administered open internet servers (e.g., DNS, NTP) to multiply the attack traffic volume by a factor of 50 or more [ISOC]. The way this works can be explained with the illustration shown in Figure 3. The attacker typically makes use of a botnet consisting of many compromised devices to send query requests to high-performance internet servers. The attacking systems insert the IP address of the target (203.0.113.1) as the source address in the requests. For internet services that use the User Datagram Protocol (UDP) (e.g., DNS, NTP), the query and response are each contained in a single packet, and the exchange does not require the establishment of a connection between the source and the server (unlike Transmission Control Protocol (TCP)). The responses from such open internet servers are directed to the attack target since the target's IP address was forged as the source address field of the request messages. Often, the response from the server to the target address is much larger than the query itself, amplifying the effect of the DoS attack (see Table 1 in Section 5.4). Such reflection and amplification attacks can result in massive DDoS with attack volumes in the range of hundreds of Gbps [Symantec] [ISTR-2015] [ISTR-2016] [ISTR-2017] [ISOC] [Verisign1] [Verisign2] [Bjarnason]. In Q1 2018, there was an increase of 100% quarter-over-quarter and 700% year-over-year in DNS amplification attacks [HelpNet]. The attack volumes may still rise significantly if the Mirai-scale attacks are combined with reflection amplification attacks.

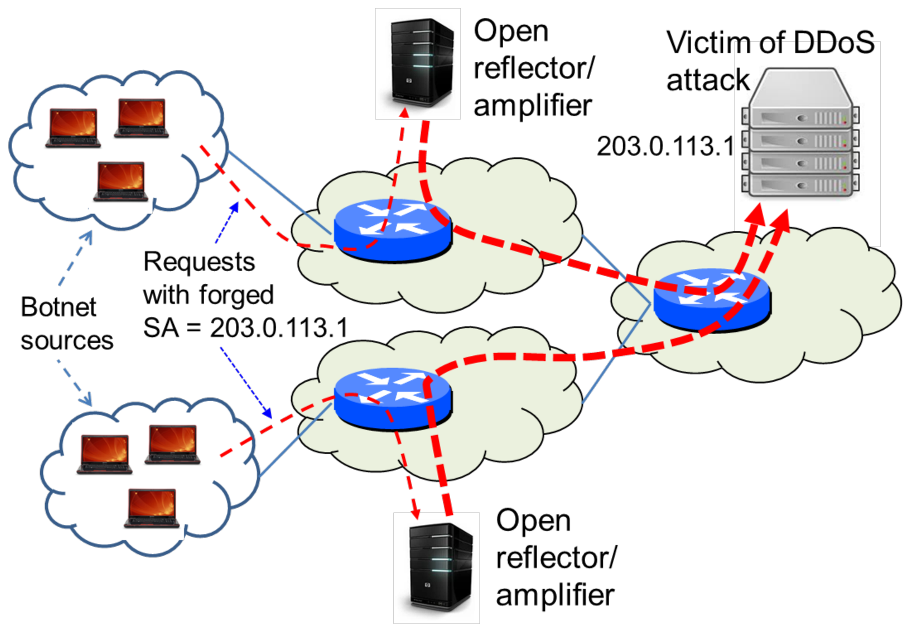



**Figure 3: DDoS by IP source address spoofing and reflection and amplification**

# 4 Control Plane/BGP Security – Solutions and Recommendations

BGP security vulnerabilities and mitigation techniques have been of interest within the networking community for several years (e.g., [IETF-SIDR] [RFC7454] [NIST800-54] [NANOG] [Murphy] [MANRS] [MANRS2] [ENISA] [Quilt] [Levy1] [CSRIC4-WG6] [CSRIC6-WG3] [RFC6811] [RFC8205] [NSA-BGP] [CSDE]). This section highlights key BGP security technologies that have emerged from such efforts and makes related security recommendations. Many of the solution technologies discussed here have been developed and standardized in the IETF [IETF-SIDR] [IETF-SIDROPS] [IETF-IDR] [IETF-OPSEC] [IETF-GROW]. The [MANRS] document can be thought of as complementary to this document since it provides implementation guidance for some of the solution technologies described in this section and Section 5. This document addresses many of the same concerns regarding BGP vulnerabilities and DoS/DDoS attacks as highlighted in [CSRIC4-WG6] but goes into greater technical depth in describing standards-based and commercially available security mechanisms and providing specific security recommendations.

## 4.1 Registration of Route Objects in Internet Routing Registries

Declarative data about internet resource allocations and routing policies have traditionally been available from regional internet registries (RIRs) and internet routing registries (IRRs). The RIR data are maintained regionally by ARIN in North America, RIPE in Europe, LACNIC in Latin America, APNIC in Asia-Pacific, and AfriNIC in Africa. The IRRs are maintained by the RIRs (RIPE NCC, APNIC, AfriNIC, and ARIN) as well as some major internet service providers (ISPs). Additionally, Merit's Routing Assets Database (RADb) [Merit-RADb] and other similar entities provide a collective routing information base consisting of registered (at their site) as well as mirrored (from the IRRs) data. The route objects available in the IRRs provide routing information declared by network operators. Specifically, the route objects contain information regarding the origination of prefixes (i.e., the association between prefixes and the ASes which may originate them). Routing Policy Specification Language (RPSL) [RFC4012] [RFC7909] and the Shared Whois Project (SWIP) [SWIP] are two formats in which the data in RIRs/IRRs are presented. ARIN predominantly uses SWIP, but some use RPSL as well. LACNIC also uses SWIP. The rest of the RIRs and the ISPs' IRRs use only RPSL.

The completeness, correctness, freshness, and consistency of the data derived from these sources vary widely, and the data is not always reliable. However, there are efforts underway to make the data complete and reliable [RFC7909]. Network operators often obtain route object information from the IRRs and/or RADb, and they can make use of the data in the creation of prefix filters (see Sections 4.4 and 4.5) in their BGP routers.

It is worth noting that RIPE NCC, APNIC, and AfriNIC each run internet routing registries (IRRs) that are integrated with regional internet registry (RIR) allocation data that facilitate stronger authentication schemes. These are documented in [RFC2725]. In the case of address block (NetRange) registration in ARIN, the originating autonomous system (origin AS) is permitted to be included.[1]

While efforts are encouraged to create complete and accurate IRR data in line with the current operational reality, greater efforts should be devoted to creating route origin authorizations (ROAs) (see Section 4.3) because RPKI provides a stronger authentication and validation framework for network operators than IRR.

> **Security Recommendation 1:** All internet number resources (e.g., address blocks and AS numbers) should be covered by an appropriate registration services agreement with an RIR, and all point-of-contact (POC) information should be up to date. The granularity of such registrations should reflect all sub-allocations to entities (e.g., enterprises within the parent organization, branch offices) that operate their own network services (e.g., internet access, DNS).

> **Security Recommendation 2:** In the case of address block (NetRange) registration in ARIN, the originating autonomous system (origin AS) should be included.[2]

> **Security Recommendation 3:** Route objects corresponding to the BGP routes originating from an AS should be registered and actively maintained in an appropriate RIR's IRR. Enterprises should ensure that appropriate IRR information exists for all IP address space used directly and by their outsourced IT systems and services.

## 4.2 Certification of Resources in Resource Public Key Infrastructure

Resource Public Key Infrastructure (RPKI) is a standards-based approach for providing cryptographically secured registries of internet resources and routing authorizations [RFC6480] [RFC6482] [NANOG] [Murphy]. The IPv4/IPv6 address and AS number resource allocations follow a hierarchy. The Internet Assigned Numbers Authority (IANA) allocates resources to the reginal internet registries (RIRs) (e.g., ARIN, RIPE, etc.), and the RIRs suballocate resources to ISPs and enterprises. The ISPs may further suballocate to other ISPs and enterprises. In some regions, RIRs suballocate to local internet registries (LIRs), which in turn suballocate to ISPs and enterprises. RPKI is a global certificate authority (CA) and registry service offered by all reginal internet registries (RIRs). The RPKI certification chain follows the same allocation hierarchy (see Figure 4). Although RPKI certifications are illustrated only under ARIN in Figure 4, a similar pattern is found in all other RIRs. Ideally, there should be a single root or trust anchor (TA) at the top of the hierarchy, but currently, each of the five RIRs (AFRINIC, APNIC, ARIN, LACNIC, and RIPE) maintains an independent TA for RPKI certification services in its respective region. Thus, the global RPKI is currently operating with five TAs (see [ARIN1] [ARIN2] [RIPE1] [RIPE2]).

---

[1] See https://whois.arin.net/rest/net/NET-128-3-0-0-1/pft?s=128.3.0.

[2] See https://whois.arin.net/rest/net/NET-128-3-0-0-1/pft?s=128.3.0.

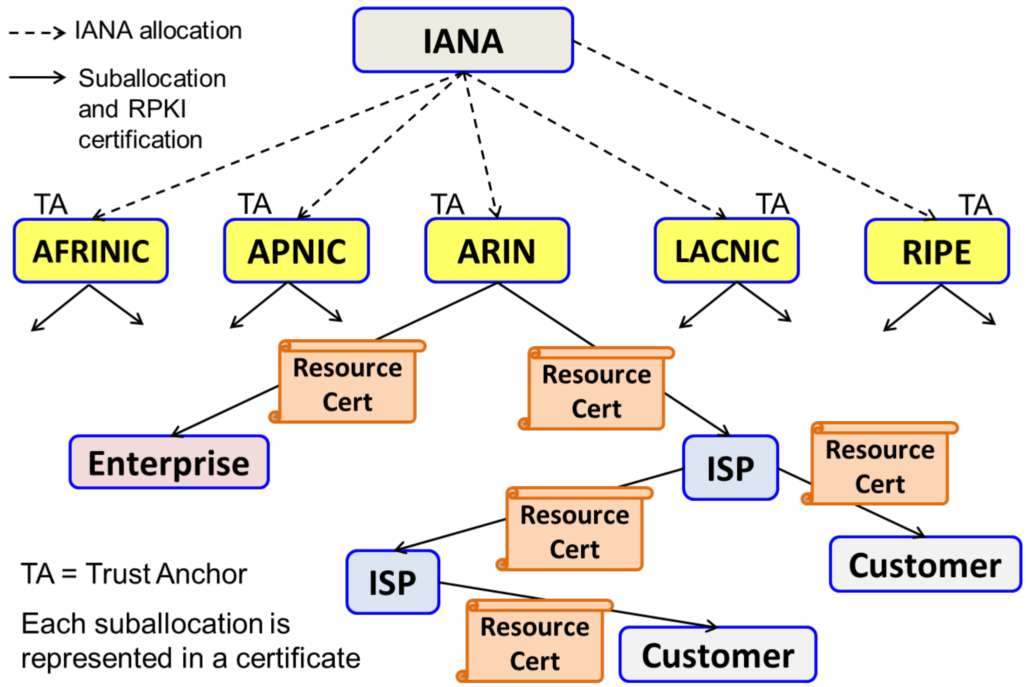



**Figure 4: Illustration of resource allocation and certificate chain in RPKI**

RPKI is based on the X.509 standard with RFC 3779 extensions that describe special certificate profiles for internet number resources (prefixes and AS numbers) [RFC5280] [RFC6487] [RFC3779]. As shown in Figure 4, the RIRs issue resource certificates (i.e., certificate authority (CA) certificates) to ISPs and enterprises with registered number resource allocations and assignments. There are two models of resource certification: hosted and delegated [ARIN1] [RIPE1]. In the hosted model, the RIR keeps and manages keys and performs RPKI operations on their servers. In the delegated model, a resource holder (an ISP or enterprise) receives a CA certificate from their RIR, hosts their own certificate authority, and performs RPKI operations (e.g., signs route origin authorizations (see Section 4.3), issues subordinate resource certificates to their customers).

> **Security Recommendation 4:** Internet number resource holders with IPv4/IPv6 prefixes and/or AS numbers (ASNs) should obtain RPKI certificate(s) for their resources.

> **Security Recommendation 5:** Transit providers should provide a service where they create, publish, and manage subordinate resource certificates for address space and/or ASNs suballocated to their customers.[3]

[3] Currently, RPKI services based on the hosted model and offered by RIRs are common. Security Recommendation 5 can be implemented in the hosted or delegated model based on service agreements with customers.

### 4.3 BGP Origin Validation (BGP-OV)

Once an address prefix owner obtains a CA certificate, they can generate an end-entity (EE) certificate and use the private key associated with the EE certificate to digitally sign a route origin authorization (ROA) [RFC6482] [RFC6811]. An ROA declares a specific AS as an authorized originator of BGP announcements for the prefix (see Figure 5). It specifies one or more prefixes (optionally a maxlength per prefix) and a single AS number. If a maxlength is specified for a prefix in the ROA, then any more-specific (i.e., longer) prefixes (subsumed under the prefix) with a length not exceeding the maxlength are permitted to be originated from the specified AS. In the absence of an explicit maxlength for a prefix, the maxlength is equal to the length of the prefix itself. If the resource owner has a resource certificate listing multiple prefixes, they can create one ROA in which some or all those prefixes are listed. Alternatively, they can create one ROA per prefix.

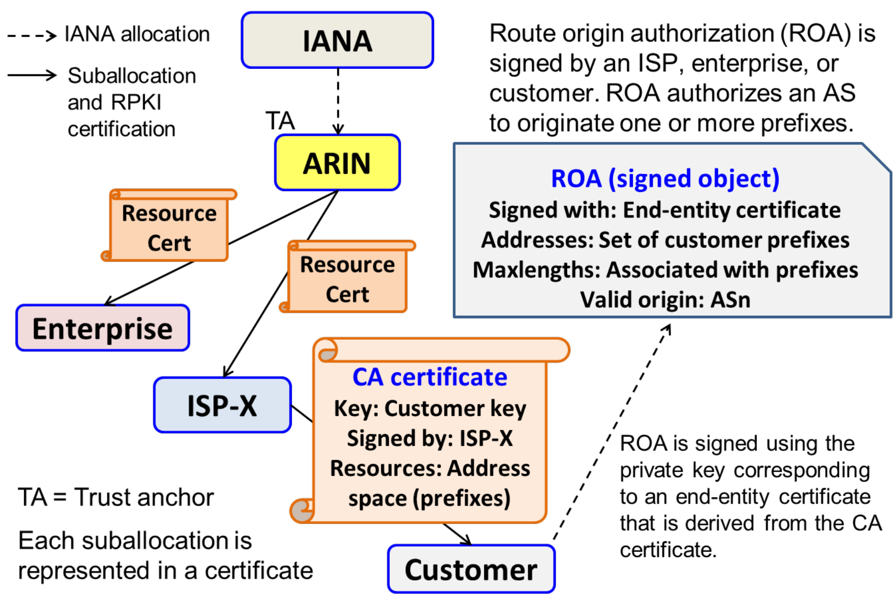



**Figure 5: Creation of Route Origin Authorization (ROA) by prefix owner**

ROAs can also be created (signed) by an ISP (transit provider) on behalf of its customer based on a service agreement provided that the ISP suballocated the address space to the customer. The ISP can offer a service to its customers where the ISP creates and maintains CA certificates for the customers' resources and ROAs for the customers' prefixes.

Once created, RPKI data is used throughout the internet by relying parties (RPs). RPs, such as RPKI-validating servers, can access RPKI data from the repositories (see Figure 6) using either the rsync protocol [Rsync] [Rsync-RPKI] or the RPKI Repository Delta Protocol (RRDP) [RFC8182]. The RRDP protocol is often called "delta protocol" as shorthand. A BGP router typically accesses the required ROA data from one or more RPKI cache servers that are maintained by its AS. As shown in Figure 6, the RPKI-to-router protocol is used for communication between the RPKI cache server and the router [RFC6810] [RFC8210]. More details regarding secure routing architecture based on RPKI can be found in [RFC6480].

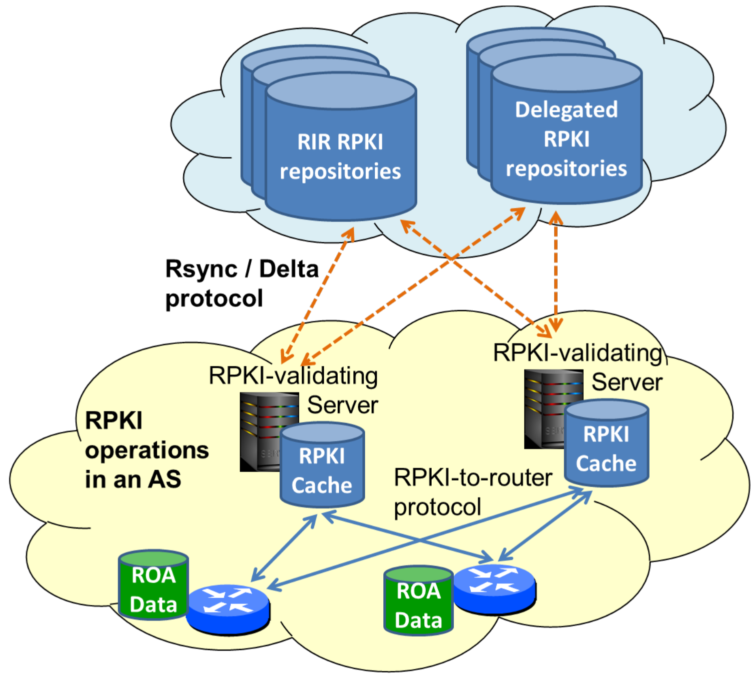



**Figure 6: RPKI data retrieval, caching, and propagation to routers**

A BGP router can use the ROA information retrieved from an RPKI cache server to mitigate the risk of prefix hijacks and some forms of route leaks in advertised routes. A BGP router would typically receive a validated list of {prefix, maxlength, origin AS} tuples (derived from valid ROAs) from one or more RPKI cache servers. This list may be called a white list. The router makes use of this list with the BGP origin validation (BGP-OV) process depicted in Figure 7 to determine the validation state of an advertised route [RFC6811]. A BGP route is deemed to have a "Valid" origin if the {prefix, origin AS} pair in the advertised route can be corroborated with the list (i.e., the pair is permissible in accordance with at least one ROA; see Figure 7 for the details). A route is considered "Invalid" if there is a mismatch with the list (i.e., AS number does not match, or the prefix length exceeds maxlength; see Figure 7 for additional details). Further, a route is deemed "NotFound" if the prefix announced is not covered by any prefix in the white list (i.e., there is no ROA that contains a prefix that equals or subsumes the announced prefix). When an AS_SET [RFC4271] is present in a BGP update, it is not possible to clearly determine the origin AS from the AS_PATH [RFC6811]. Thus, an update containing an AS_SET in its AS_PATH can never receive an assessment of "Valid" in the origin validation process (see Figure 7). The use of AS_SET in BGP updates is discouraged in BCP 172 [RFC6472]. The RPKI-based origin validation may be supplemented by validation based on IRR data (see Section 4.1).

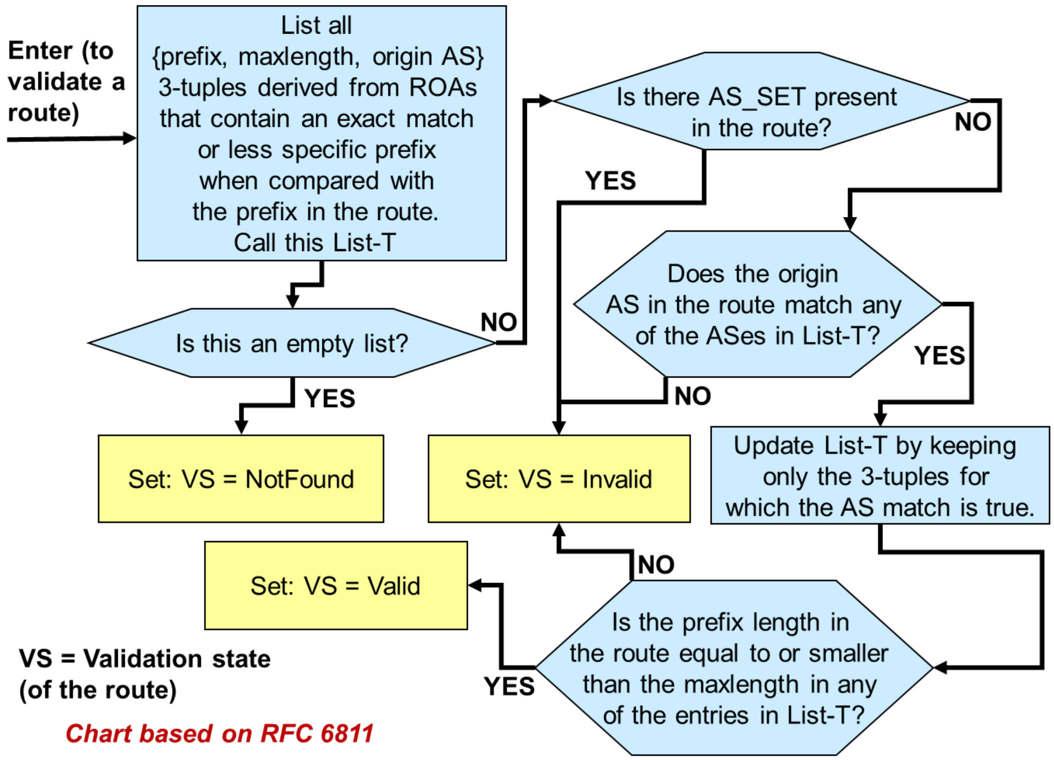



**Figure 7: Algorithm for origin validation (based on RFC 6811)**

There are several implementations of RPKI-based BGP OV in both hardware and software-based router platforms [Juniper1] [Cisco1] [Patel] [Scudder] [NIST-SRx] [Parsons2] [goBGP] [RTRlib]. Deployment guidance and configuration guidance for many of these implementations are available from several sources, including [NCCoE-sidr] [RIPE1] [MANRS]. Although BGP-OV is already implemented in commercial BGP routers, the activation and ubiquitous use of RPKI and BGP-OV in BGP routers require motivation and commitment on the part of network operators.

> **Security Recommendation 6:** Resource holders should register ROA(s) in the global RPKI for all prefixes that are announced or intended to be announced on the public internet.

> **Security Recommendation 7:** Each transit provider should provide a service where they create, publish, and maintain ROAs for prefixes suballocated to their customers. Alternatively, as part of the service, customers can be allowed to create, publish, and maintain their ROAs in a repository maintained by the transit provider.[4]

> **Security Recommendation 8:** If a prefix that is announced (or intended to be announced) is multi-homed and originated from multiple ASes, then one ROA per originating AS should be registered for the prefix (possibly in combination with other

[4] Security Recommendation 7 can be implemented in the hosted or the delegated model based on service agreements with customers.

prefixes which are also originated from the same AS).

**Security Recommendation 9:** When an ISP or enterprise owns multiple prefixes that include less-specific and more-specific prefixes, they should ensure that the more-specific prefixes have ROAs before creating ROAs for the subsuming less-specific prefixes.

**Security Recommendation 10:** An ISP should wait until more specific prefixes announced from within their customer cone have ROAs prior to the creation of its own ROAs for subsuming less-specific prefix(es).

AS0 is a special AS number that is not allocated to any autonomous system. AS0 is also not permitted in routes announced in BGP. An AS0 ROA is one which has an AS0 in it for the originating AS [RFC6483] [APNIC1]. An address resource owner can create an AS0 ROA for their prefix to declare the intention that the prefix or any more-specific prefix subsumed under it must not be announced until and unless a normal ROA simultaneously exists for the prefix or the more-specific prefix.

**Security Recommendation 11:** An ISP or enterprise should create an AS0 ROA for any prefix that is currently not announced to the public internet. However, this should be done only after ensuring that ROAs exist for any more-specific prefixes subsumed by the prefix that are announced or are intended to be announced.

**Security Recommendation 12:** A BGP router should not send updates with AS_SET or AS_CONFED_SET in them (in compliance with BCP 172 [RFC6472]).

**Security Recommendation 13:** ISPs and enterprises that operate BGP routers should also operate one or more RPKI-validating caches.

**Security Recommendation 14:** A BGP router should maintain an up-to-date white list consisting of {prefix, maxlength, origin ASN} that is derived from valid ROAs in the global RPKI. The router should perform BGP-OV.

Concerning Security Recommendation 14, BGP-OV is implemented by the majority of major router vendors. The white list of {prefix, maxlength, origin ASN} 3-tuples is typically obtained and periodically refreshed by a router from a local RPKI cache server. As mentioned before, the RPKI-to-router protocol [RFC6810] [RFC8210] is used for this communication.

**Security Recommendation 15:** In partial/incremental deployment state of the RPKI, the permissible {prefix, origin ASN} pairs for performing BGP-OV should be generated by taking the union of such data obtained from ROAs, IRR data, and customer contracts.

**Security Recommendation 16:** BGP-OV results should be incorporated into local policy decisions to select BGP best paths.

Concerning Security Recommendation 16, exactly how BGP-OV results are used in path selection is strictly a local policy decision for each network operator. Typical policy choices include:

- Tag-Only – BGP-OV results are only used to tag/log data about BGP routes for diagnostic purposes.
- Prefer-Valid – Use local preference settings to give priority to valid routes. Note that this is only a tie-breaking preference among routes with the exact same prefix.
- Drop-Invalid – Use local policy to ignore invalid routes in the BGP decision process.

Careful planning and thought should be given to the application of such policies. In general, it is important that BGP-OV local policies be consistent throughout an individual AS, both in terms of which peering sessions BGP-OV is enabled on and how the results are used to influence the BGP decision process. It is recommended that network operators proceed through an incremental deployment process of adopting more stringent policies over time after gaining experience and confidence in the system. The three example polices above can be viewed as recommended stages of an incremental adoption plan.

Enterprises should require their hosted service providers (e.g., cloud, CDN, DNS, email) to follow the security recommendations stated in this section concerning the certification of resources and creation of ROAs for the prefixes that are used in providing the hosted services and that belong to the providers. An enterprise can do this themselves if the hosted service provider is using the enterprise's own address space for the hosted services.

### 4.3.1 Forged-Origin Hijacks – How to Minimize Them

With ROA-based origin validation alone, it is possible to prevent accidental misoriginations. However, a purposeful malicious hijacker can forge the origin AS of any update by prepending the number of an AS found in an ROA for the target prefix onto their own unauthorized BGP announcement. For greater impact, in conjunction with forging the origin, the attacker may replace the prefix in the route with a more-specific prefix (subsumed under the announced prefix) that has a length not exceeding the maxlength in the ROA. The security recommendations that follow are useful to minimize forged-origin attacks.[5]

The following recommendation provides some degree of robustness against forged-origin attacks:

> **Security Recommendation 17:** The maxlength in the ROA should not exceed the length of the most specific prefix (subsumed under the prefix in consideration) that is originated or intended to be originated from the AS listed in the ROA.

The following recommendation provides an even greater degree of robustness against forged-origin attacks:

> **Security Recommendation 18:** If a prefix and select more-specific prefixes subsumed under it are announced or intended to be announced, then instead of specifying a maxlength, the prefix and the more-specific prefixes should be listed explicitly in

[5] BGP path validation (i.e., BGPsec [RFC8205]) described in Section 4.7 is required for full protection against prefix and/or path modifications.

multiple ROAs (i.e., one ROA per prefix or more-specific prefix).[6]

## 4.4 Categories of Prefix Filters

BGP prefix filtering (also known as route filtering) is the most basic mechanism for protecting BGP routers from accidental or malicious disruption [RFC7454] [NIST800-54]. Prefix filtering differs from BGP-OV in that only the prefixes expected in a peering (e.g., customer) relationship are accepted, and prefixes not expected—including bogons and unallocated—are rejected. Further, origin validation is not a part of traditional prefix filtering, but it is complementary. Filtering capabilities on both incoming prefixes (inbound prefix filtering) and outgoing prefixes (outbound prefix filtering) should be implemented. Route filters are typically specified using a syntax similar to that used for access control lists. One option is to list ranges of IP prefixes that are to be denied and then permit all others. Alternatively, ranges of permitted prefixes can be specified, and the rest denied. The choice of which approach to use depends on practical considerations determined by system administrators. Typically, BGP peers should have matching prefix filters (i.e., the outbound prefix filters of an AS should be matched by the inbound prefix filters of peers that it communicates with). For example, if AS 64496 filters its outgoing prefixes towards peer AS 64500 to permit only those in set *P*, then AS 64500 establishes incoming prefix filters to ensure that the prefixes it accepts from AS 64496 are only those in set *P*.

Different types of prefix filters are described in the rest of Section 4.4, and their applicability is described in the context of different peering relations in Section 4.5.

### 4.4.1 Unallocated Prefixes

The Internet Assigned Numbers Authority (IANA) allocates address space to RIRs. All the IPv4 address space (or prefixes), except for some reserved for future use, have been allocated by IANA [IANA-v4-r]. The RIRs have also nearly fully allocated their IPv4 address space [IANA-v4-r].[7] The IPv6 address space is much larger than that of IPv4, and, understandably, the bulk of it is unallocated. Therefore, it is a good practice to accept only those IPv6 prefix advertisements that have been allocated by the IANA [IANA-v6-r]. Network operators should ensure that the IPv6 prefix filters are updated regularly (normally, within a few weeks after any change in allocation of IPv6 prefixes). In the absence of such regular updating processes, it is better not to configure filters based on allocated prefixes. Team Cymru provides a service for updating bogon prefix lists for IPv4 and IPv6 [Cymru-bogon].

> **Security Recommendation 19:** IPv6 routes should be filtered to permit only allocated IPv6 prefixes. Network operators should update IPv6 prefix filters regularly to include any newly allocated prefixes.

If prefix resource owners regularly register AS0 ROAs (see Section 4.3) for allocated (but possibly currently unused) prefixes, then those ROAs could be a complementary source for the update of prefix filters.

---

[6] In general, the use of maxlength should be avoided unless all or nearly all more-specific prefixes up to a maxlength are announced or intended to be announced [maxlength].

[7] Some of the prefixes are designated for special use as discussed in Section 4.4.2.

### 4.4.2 Special Purpose Prefixes

IANA maintains registries for special-purpose IPv4 and IPv6 addresses [IANA-v4-sp] [IANA-v6-sp]. These registries also include specification of the routing scope of the special-purpose prefixes.

> **Security Recommendation 20:** Prefixes that are marked "False" in column "Global" [IANA-v4-sp] [IANA-v6-sp] are forbidden from routing in the global internet and should be rejected if received from an external BGP (eBGP) peer.

### 4.4.3 Prefixes Owned by an AS

An AS may originate one or multiple prefixes. In the inbound direction, the AS should (in most cases) reject routes for the prefixes it originates if received from any of its eBGP peers (transit provider, customer, or lateral peer). In general, the data traffic destined for these prefixes should stay local and should not be leaked over external peering. However, if the AS operator is uncertain whether a prefix they originate is single-homed or multi-homed, then the AS should accept the prefix advertisement from an eBGP peer (and assign a lower local preference value) so that the desired redundancy is maintained.

> **Security Recommendation 21:** For single-homed prefixes (subnets) that are owned and originated by an AS, any routes for those prefixes received at that AS from eBGP peers should be rejected.

### 4.4.4 Prefixes that Exceed a Specificity Limit

Normally, ISPs neither announce nor accept routes for prefixes that are more specific than a certain level of specificity. For example, maximum acceptable prefix lengths are mentioned in existing practices as /24 for IPv4 [RIPE-399] and /48 for IPv6 [RIPE-532]. The level of specificity that is acceptable is decided by each AS operator and communicated with peers. In instances when Flowspec (see Section 5.5) [RFC5575] [Hares] [Ryburn] is used between adjacent ASes for DDoS mitigation, the two ASes may mutually agree to accept longer prefix lengths (e.g., a /32 for IPv4) but only for certain pre-agreed prefixes. That is, the announced more-specific prefix must be contained within a pre-agreed prefix.

> **Security Recommendation 22:** It is recommended that an eBGP router should set the specificity limit for each eBGP peer and reject prefixes that exceed the specificity limit on a per-peer basis.[8]

Some operators may choose to reject prefix announcements that are less-specific than /8 and /11 for IPv4 and IPv6, respectively.

### 4.4.5 Default Route

A route for the prefix 0.0.0.0/0 is known as the default route in IPv4, and a route for ::/0 is

[8] The specificity limit may be the same for all peers (e.g., /24 for IPv4 and /48 for IPv6).

known as the default route in IPv6. The default route is advertised or accepted only in specific customer-provider peering relations. For example, a transit provider and a customer that is a stub or leaf network may make this arrangement between them whereby the customer accepts the default route from the provider instead of the full routing table. In general, filtering the default route is recommended except in situations where a special peering agreement exists.

> **Security Recommendation 23:** The default route (0.0.0.0/0 in IPv4 and ::/0 in IPv6) should be rejected except when a special peering agreement exists that permits accepting it.

### 4.4.6 IXP LAN Prefixes

Typically, there is a need for the clients at an internet exchange point (IXP) to have knowledge of the IP prefix used for the IXP LAN which facilitates peering between the clients.

> **Security Recommendation 24:** An internet exchange point (IXP) should announce—from its route server to all of its member ASes—its LAN prefix or its entire prefix, which would be the same as or less specific than its LAN prefix. Each IXP member AS should, in turn, accept this prefix and reject any more-specific prefixes (of the IXP announced prefix) from any of its eBGP peers.

Implementing Security Recommendation 24 will ensure reachability to the IXP LAN prefix for each of the IXP members. It will also ensure that the Path Maximum Transmission Unit Discovery (PMTUD) will work between the members even in the presence of unicast Reverse Path Forwarding (uRPF). This is because the “packet too big” Internet Control Message Protocol (ICMP) messages sent by IXP members' routers may be sourced using an IP address from the IXP LAN prefix. See [RFC7454] for more details on this topic.

## 4.5 Prefix Filtering for Peers of Different Types

The inbound and outbound prefix filtering recommendations vary based on the type of peering relationship that exists between networks: lateral peer, transit provider, customer, or leaf customer (see definitions in Section 2.3). The different types of filters that apply are from the list described in Sections 4.4.1 through 4.4.6.

The security recommendations that follow apply to enterprises when they have eBGP peering with neighbor ASes. When an enterprise procures transit services from an ISP or hosted services (e.g., cloud, CDN, DNS, email) from hosted service providers, the security recommendations should be included in the respective service contracts.

### 4.5.1 Prefix Filtering with Lateral Peer

> **Security Recommendation 25:** **Inbound prefix filtering facing lateral peer** – The following prefix filters should be applied in the inbound direction:
>
> - Unallocated prefixes
> - Special-purpose prefixes
> - Prefixes that the AS originates

- Prefixes that exceed a specificity limit
- Default route
- IXP LAN prefixes

**Security Recommendation 26: Outbound prefix filtering facing lateral peer** – The appropriate outbound prefixes are those that are originated by the AS in question and those originated by its downstream ASes (i.e., the ASes in its customer cone). The following prefix filters should be applied in the outbound direction:

- Unallocated prefixes[9]
- Special-purpose prefixes
- Prefixes that exceed a specificity limit
- Default route
- IXP LAN prefixes
- Prefixes learned from AS's other lateral peers (see Security Recommendations in Section 4.9)
- Prefixes learned from AS's transit providers (see Security Recommendations in Section 4.9)

### 4.5.2 Prefix Filtering with Transit Provider

**Security Recommendation 27: Inbound prefix filtering facing transit provider** – **Case 1 (full routing table):** In general, when the full routing table is required from the transit provider, the following prefix filters should be applied in the inbound direction:[10]

- Unallocated prefixes
- Special-purpose prefixes
- Prefixes that the AS originates
- Prefixes that exceed a specificity limit
- IXP LAN prefixes

**Security Recommendation 28: Inbound prefix filtering facing transit provider** – **Case 2 (default route):** If the border router is configured only for the default route, then only the default route should be accepted from the transit provider and nothing else.

**Security Recommendation 29: Outbound prefix filtering facing transit provider:** The same outbound prefix filters should be applied as those for a lateral peer (see Section 4.5.1) except that the last two bullets are modified as follows:[11]

---

[9] Unallocated prefixes may be omitted if there is confidence that the inbound prefix filters are not letting them in.

[10] The default route is not included in this list. In some cases, a customer network prefers to receive the default route from a transit provider in addition to the full routing table.

[11] In conjunction with Security Recommendation 29, some policy rules may also be applied if a transit provider is not contracted (or chosen) to provide transit for some subset of outbound prefixes.

- Prefixes learned from AS's lateral peers (see Security Recommendations in Section 4.9)
- Prefixes learned from AS's other transit providers (see Security Recommendations in Section 4.9)

### 4.5.3 Prefix Filtering with Customer

**Inbound prefix filtering:** There are two scenarios that require consideration. **Scenario 1** is when there is full visibility of the customer and its cone of customers (if any) as well as knowledge of prefixes that originated from such a customer and its cone. The knowledge of prefixes can be based on direct customer knowledge, IRR data, and/or RPKI data (if that data is known to be in a complete and well-maintained state for the customer in consideration and its customer cone). The prefixes thus known for the customer and its customer cone are listed in the configuration of the eBGP router in question.

**Security Recommendation 30: Inbound prefix filtering facing customer in Scenario 1** – Only the prefixes that are known to be originated from the customer and its customer cone should be accepted, and all other route announcements should be rejected.

**Scenario 2** is when there is not a reliable knowledge of all prefixes originated from the customer and its cone of customers.

**Security Recommendation 31: Inbound prefix filtering facing customer in Scenario 2** – The same set of inbound prefix filters should be applied as those for a lateral peer (see Section 4.5.1).

**Security Recommendation 32: Outbound prefix filtering facing customer** – The filters applied in this case would vary depending on whether the customer wants to receive only the default route or the full routing table. If it is the former, then only the default route should be announced and nothing else. In the latter case, the following outbound prefix filters should be applied:[12]

- Special-purpose prefixes
- Prefixes that exceed a specificity limit

### 4.5.4 Prefix Filtering Performed in a Leaf Customer Network

A leaf customer network is one which is single-homed to a transit provider and has no lateral peers or customer ASes downstream.

**Security Recommendation 33: Inbound prefix filtering for leaf customer facing transit provider** – A leaf customer may request only the default route from its transit provider. In this case, only the default route should be accepted and nothing else. If the leaf customer requires the full routing table from the transit provider, then it should apply

[12] The default route filter may be added if the customer requires the full routing table but not the default route.

the following inbound prefix filters:

- Unallocated prefixes
- Special-purpose prefixes
- Prefixes that the AS (i.e., leaf customer) originates
- Prefixes that exceed a specificity limit
- Default route

**Security Recommendation 34: Outbound prefix filtering for leaf customer facing transit provider** – A leaf customer network should apply a very simple outbound policy of announcing only the prefixes it originates. However, it may additionally apply the same outbound prefix filters as those for a lateral peer (see Section 4.5.1) to observe extra caution.

### 4.6 Role of RPKI in Prefix Filtering

An ISP can retrieve (from RPKI registries) all available route origin authorizations (ROAs) corresponding to autonomous systems (ASes) that are known to belong in their customer cone (see definition in Section 2.3).[13] From the available ROAs, it is possible to determine the prefixes that can be originated from the ASes in the customer cone. As the RPKI registries become mature with increasing adoption, the prefix lists derived from ROAs will become useful for prefix filtering. Even in the early stages of RPKI adoption, the prefix lists (from ROAs) can help cross-check and/or augment the prefix filter lists that an ISP constructs by other means.

**Security Recommendation 35:** The ROA data (available from RPKI registries) should be used to construct and/or augment prefix filter lists for customer interfaces.[14]

### 4.7 AS Path Validation (Emerging/Future)

The IETF standard for BGP path validation (BGP-PV), namely BGPsec [RFC8205], is available but commercial vendor implementations are not currently available. Hence, this section briefly describes the technology and standards but does not make any security recommendations concerning BGP-PV.

As observed in Sections 4.3 and 4.3.1, BGP origin validation (BGP-OV) is necessary but, by itself, is insufficient for fully securing the prefix and AS path in BGP announcements. BGP path validation (BGP-PV) is additionally required to protect against prefix modifications and forged-origin attacks (see Section 4.3.1) as well as other AS-path attacks such as path shortening and Kapela-Pilosov attacks (see Section 2.2). There is significant interest in the networking community to secure the AS path in BGP updates so that a more comprehensive protection can be provided to BGP updates [RFC8205] [RFC8208] [RFC7353] [Huston2011] [RFC8374]. RFC

[13] The list of ASes in an AS's customer cone can be determined by forming the list of unique origin ASes in all BGP announcements received (i.e., currently in the Adj-RIB-ins [RFC4271]) on all customer interfaces at the AS under consideration (see Step 3 in Section 3.4 in [EFP-uRPF]). This can be done in the network management system (off the router).

[14] Security Recommendation 35 is possibly more applicable to smaller ISPs than larger ISPs.

8205 is the IETF standard that specifies the BGPsec protocol (i.e., the protocol for BGP path validation). Open-source prototype implementations of BGP-PV are available [NIST-SRx] [Parsons2] [Adalier2].

The basic principles of BGP-PV are illustrated in Figure 8.[15] An ROA signed by the owner of the prefix 10.1.0.0/16 attests that AS1 is authorized to originate the prefix. Further, each network operator that has deployed BGP-PV is given a resource certificate for their AS number, and the BGP-PV routers within the AS are given router certificates and private keys for signing updates. The certificates for all BGP-PV routers are retrieved by all participating ASes, and the public keys of all BGP-PV routers are expected to be available at each BGP-PV router. In Figure 8, AS1 uses its private key to generate its signature, SIG1-2, attesting that it sent a route for 10.1.0.0/16 to AS2. The target AS is included in the data that is under the signature. Likewise, AS2 signs the route to AS3 and so on. Each AS adds its signature as it propagates the update to its neighbors. The update includes the subject key identifier (SKI) for the public key of each AS in the path (i.e., the public key of the BGP-PV router in the AS). AS5 receives an update with four signatures (one corresponding to each hop). If all signatures verify correctly at AS 5, and the origin validation check also passes, then AS5 can be certain that the received update for 10.1.0.0/16 with AS path [AS1 (origin), AS2, AS3, AS4] is legitimate (i.e., not corrupted by prefix or path modifications along the way). For example, in Figure 8, AS6 would fail if it were to try to fake a connection to AS1 and announce a signed BGPsec update to AS5 (with a shorter path and a forged-origin AS1). This is because AS6 does not have an update signed to it directly from AS1.

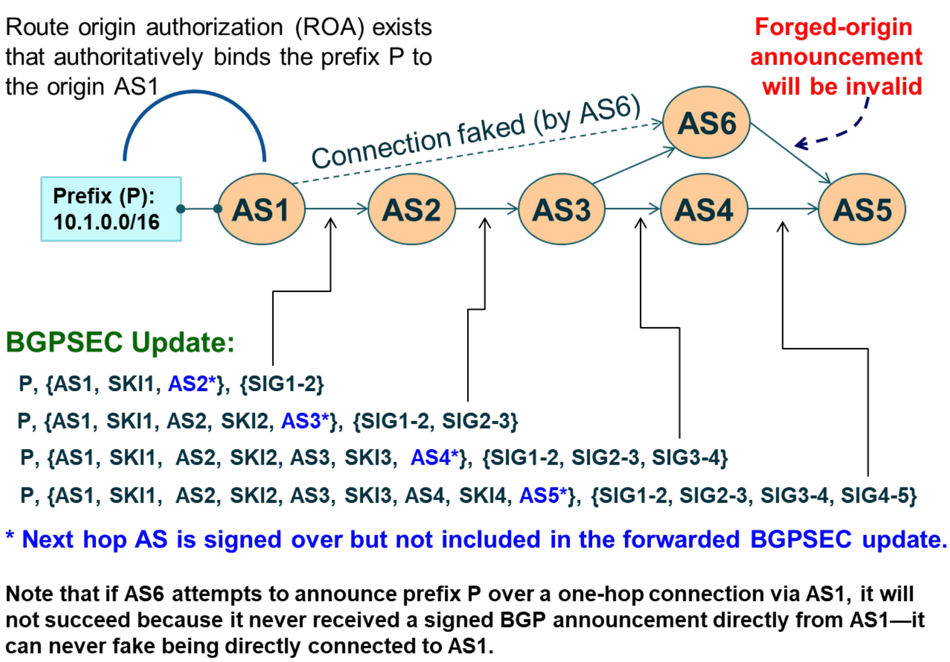



**Figure 8: Basic principle of signing/validating AS paths in BGP updates**

[15] See [RFC8205] for a detailed protocol specification.

The ECDSA-P256 algorithm is currently recommended for signing BGPsec updates between ASes that peer with each other [RFC8208]. Updates will have a larger size due to the addition of a 64-byte ECDSA P-256 signature for each hop. Also, the route processors in BGP-PV routers will be required to perform additional processing due to signing and verification of path signatures. The performance characterization of BGP-PV quantifying routing information base (RIB) size and routing convergence time has been reported in [Sriram1]. High performance implementations of the cryptographic operations (ECC signing and verifications) associated with BGPsec update processing are available [Adalier1] [Adalier2] [NIST-SRx]. Optimization algorithms for BGPsec update processing are proposed and analyzed in [Sriram2].

To reduce upgrade costs and encourage faster deployment, a leaf or stub AS is allowed to trust its upstream AS and negotiate to receive unsigned updates while it sends signed updates to the upstream AS [RFC8205].

The standards for BGP-PV are documented in IETF RFC's #8205 through #8210. When implementations based on these standards become available in commercial products, this document may be updated to recommend BGP-PV.

### 4.8 Checking AS Path for Disallowed AS Numbers

The AS path in an update received in eBGP is checked to make sure that there is no AS loop [RFC4271]. This is done by checking that the AS number of the local system does not appear in the received AS path. The AS path is also checked to ensure that AS numbers meant for special purposes [IANA-ASN-sp] are not present. Note that the special purpose ASN 23456 is allocated for AS_TRANS [RFC6793] and can be present in an AS_PATH in conjunction with an AS4_PATH [RFC 6793] in the update.

> **Security Recommendation 36:** The AS path in an update received in eBGP should be checked to ensure that the local AS number is not present. The AS path should also be checked to ensure that AS numbers meant for special purposes [IANA-ASN-sp] are not present.[16] In case of a violation, the update should be rejected.

### 4.9 Route Leak Solution

Section 2.3 described the route leaks problem space and noted that in RFC 7908 [RFC7908], the various types of route leaks are enumerated. Section 2.3 also defined some basic terms used in discussions of route leaks. Route leak solutions fall into two categories: intra-AS and inter-AS (across AS hops). Many operators currently use an intra-AS solution, which is done by tagging BGP updates from ingress to egress (within the AS) using a BGP community [NANOG-list]. The BGP community used is non-transitive because it does not propagate in eBGP (between ASes). Each BGP update is tagged on ingress to indicate that it was received in eBGP from a customer, lateral peer, or transit provider. Further, a route that originated within the AS is tagged to indicate the same. At the egress point, the sending router applies an egress policy that makes use of the tagging. Routes that are received from a customer are allowed on the egress to be

[16] Note that the special purpose ASN 23456 is allocated for AS_TRANS [RFC6793] and is allowed to be present in an AS_PATH in conjunction with an AS4_PATH [RFC 6793] in the update.

forwarded to any type of peer (e.g., customer, lateral peer, or transit provider). However, routes received from a lateral peer or transit provider are forwarded only to customers (i.e., they are not allowed to be forwarded to a lateral peer or transit provider). These ingress and egress policies are central to route leak prevention within an AS (intra-AS).

> **Security Recommendation 37:** An AS operator should have an ingress policy to tag routes internally (locally within the AS) to communicate from ingress to egress regarding the type of peer (customer, lateral peer, or transit provider) from which the route was received.

> **Security Recommendation 38:** An AS operator should have an egress policy to utilize the tagged information (in Security Recommendation 37) to prevent route leaks when routes are forwarded on the egress. The AS should not forward routes received from a transit provider to another transit provider or a lateral peer. Also, the AS should not forward routes received from a lateral peer to another lateral peer or a transit provider.

The above intra-AS solution for the prevention of route leaks can also be implemented using a BGP attribute (instead of BGP community). The advantage of an attribute-based solution [RouteLeak2] is that it can be made available in commercial routers as a standard feature, which in turn minimizes manual network operator actions. However, such a solution involves an update to the BGP protocol [RFC4271] and requires standardization, which takes time and is currently in progress in the IETF [RouteLeak2].

The second type of inter-AS solution is intended to work in eBGP across AS hops. With the inter-AS solution, the focus shifts to detection and mitigation in case a route leak has already occurred and started to propagate. If a leak indeed propagates out of an AS, then the peer AS or any AS along the subsequent AS path should be able to detect and stop it. A solution for inter-AS route leak detection and mitigation is also work in progress in the IETF [RouteLeak1] [RouteLeak3].

For robustness of the internet routing infrastructure, inter-AS route leak detection and mitigation capabilities will also need to be implemented in addition to the intra-AS prevention capability. When mechanisms for route leak detection and mitigation capabilities are standardized and become available in products, this document will be updated to include appropriate security recommendations to reflect the same.

### 4.10 Generalized TTL Security Mechanism (GTSM)

Time to Live (TTL) is an 8-bit field in each IP packet and is decremented by one on each hop. The Generalized TTL Security Mechanism (GTSM) [RFC5082] makes use of the TTL to provide an additional security mechanism for BGP messages. Typically, a BGP session runs between adjacent BGP routers, meaning BGP messages come from one hop away. Across such a BGP session, the sending router sets TTL to 255 on each BGP message, and the receiving router expects the incoming TTL to be 255 and rejects any BGP messages that have incoming TTL < 255. The expected TTL value in GTSM can be applied on a per-peer basis for each BGP session. In rare instances, if a BGP session with a specific peer is known to run over n hops, then the expected TTL for that session can be adjusted to a suitable value (255-n+1 in this case) in accordance with the number of hops. Thus, GTSM helps detect and reject spoofed BGP messages that may come from an attacker. Additional details regarding the operation of GTSM can be found in [RFC5082].

**Security Recommendation 39:** The Generalized TTL Security Mechanism (GTSM) [RFC5082] should be applied on a per-peer basis to provide protection against spoofed BGP messages.

# 5 Securing Against DDoS & Reflection Amplification – Solutions and Recommendations[17]

There are various existing techniques and recommendations for deterrence against DDoS attacks with spoofed addresses [BCP38] [BCP84] [NABCOP] [CSRIC4-WG5]. There are also some techniques used for preventing reflection amplification attacks [RRL] [TA14-017A], which are used to achieve greater impact in DDoS attacks. Employing a combination of these preventive techniques in enterprise and ISP border routers, hosted service provider networks, DNS/NTP servers, broadband and wireless access networks, and data centers provides the necessary protections against DDoS attacks.

## 5.1 Source Address Validation Techniques

Source address validation (SAV) is performed in network edge devices, such as border routers, cable modem termination systems (CMTS) [RFC4036], digital subscriber line access multiplexers (DSLAM), and packet data network gateways (PDN-GW) in mobile networks [Firmin]. Ingress/egress access control lists (ACLs) and unicast Reverse Path Forwarding (uRPF) are techniques employed for implementing SAV [BCP38] [BCP84] [ISOC] [RFC6092; REC-5, REC-6]. Ingress SAV applies to incoming (received) packets, and egress SAV applies to outgoing (transmitted) packets.

Definitions of terms used in this section such as transit provider, lateral peer, peering relationship (C2P, p2p), and customer cone were provided in Section 2.3. In addition, the Reverse Path Forwarding list (RPF list) is defined as the "list of permissible source-address prefixes for incoming data packets on a given interface."

### 5.1.1 SAV Using Access Control Lists

Ingress/egress access control lists (ACLs) are maintained with a list of acceptable (or alternatively, unacceptable) prefixes for the source addresses in the incoming/outgoing internet protocol (IP) packets. Any packet with a source address that does not match the filter is dropped. The ACLs for the ingress/egress filters need to be maintained to keep them up to date. Hence, this method may be operationally difficult or infeasible in dynamic environments, such as when a customer network is multi-homed, has address space allocations from multiple ISPs, or dynamically varies its BGP announcements (i.e., routing) for traffic engineering purposes.

Typically, the egress ACLs in access aggregation devices (e.g., CMTS, DSLAM, PDN-GW) permit source addresses only from the address spaces (prefixes) that are associated with the interface on which the customer network is connected. Ingress ACLs are typically deployed on border routers and drop ingress packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked "False" in column "Global" [IANA-v4-sp] [IANA-v6-sp], the enterprise's own prefixes, or the ISP's internal-use only prefixes).

---

[17] Parts of the material in this section related to the review of existing SAV/uRPF technology read like corresponding parts in [EFP-uRPF] since the authors worked on both documents in parallel and found it prudent to use the same or similar review material in both places. The IETF general rule is that original authors retain copyright. See https://trustee.ietf.org/reproduction-rfcs-faq.html.

### 5.1.2 SAV Using Strict Unicast Reverse Path Forwarding

***Terminology:*** In the figures (scenarios) in this section and the subsequent sections, the following terminology is used: "fails" means drops packets with legitimate source addresses; "works (but not desirable)" means passes all packets with legitimate source addresses but is oblivious to directionality; "works best" means passes all packets with legitimate source addresses with no (or minimal) compromise of directionality. Further, the notation Pi [ASn ASm ...] denotes a BGP update with prefix Pi and an AS_PATH as shown in the square brackets.

In the strict unicast Reverse Path Forwarding (uRPF) method, an ingress packet on an interface at the border router is accepted only if the forwarding information base (FIB) contains a prefix that encompasses the source address and packet forwarding for that prefix points to the interface in consideration. In other words, the selected best path for routing to that source address (if it were used as a destination address) should point to the interface under consideration. This method has limitations when a network or autonomous system is multi-homed, routes are not symmetrically announced to all transit providers, and there is asymmetric routing of data packets. As an example, asymmetric routing occurs (see Figure 9, Scenario 1) when a customer AS announces one prefix (P1) to one transit provider (ISP-a) and a different prefix (P2) to another transit provider (ISP-b) but routes data packets with source addresses in the second prefix (P2) to the first transit provider (ISP-a) or vice versa. Then data packets with a source address in prefix P2 that are received at AS2 directly from AS1 will be dropped. Further, data packets with a source address in prefix P1 that originate from AS1 and traverse via AS3 to AS2 will also be dropped at AS2.

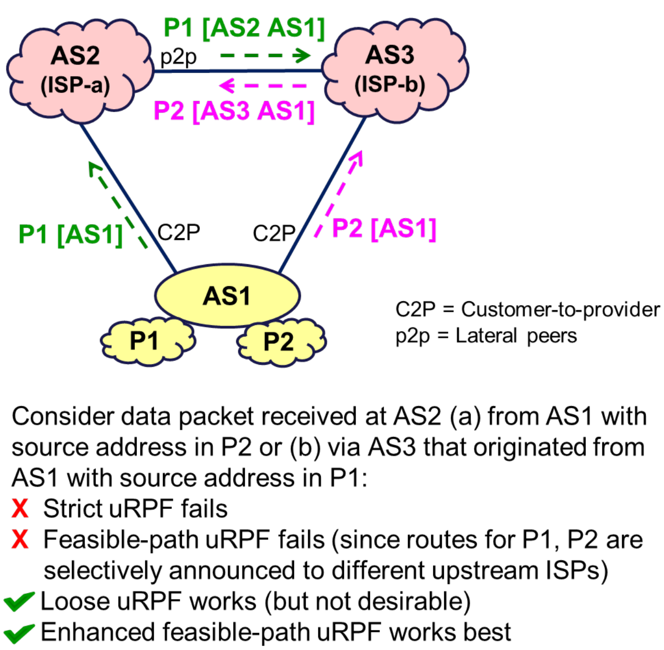



**Figure 9: Scenario 1 for illustration of efficacy of uRPF schemes**

### 5.1.3 SAV Using Feasible-Path Unicast Reverse Path Forwarding

The feasible-path uRPF helps partially overcome the problem identified with the strict uRPF in the multi-homing case. The feasible-path uRPF is similar to the strict uRPF, but in addition to inserting the best-path prefix, additional prefixes from alternative announced routes (on the interface under consideration) are also included in the RPF list (see definition at the top of Section 5.1). This method relies on either (a) announcements for the same prefixes (albeit some may be prepended to affect lower preference) propagating to all transit providers performing feasible-path uRPF checks or (b) announcement of an aggregate less-specific prefix to all transit providers while announcing more-specific prefixes (covered by the less-specific prefix) to different transit providers as needed for traffic engineering. As an example, in the multi-homing scenario (see Figure 10, Scenario 2), if the customer AS announces routes for both prefixes (P1, P2) to both transit providers (with suitable prepends if needed for traffic engineering), then the feasible-path uRPF method works. The feasible-path uRPF only works in this scenario if customer routes are preferred at AS2 and AS3 over a shorter non-customer route.

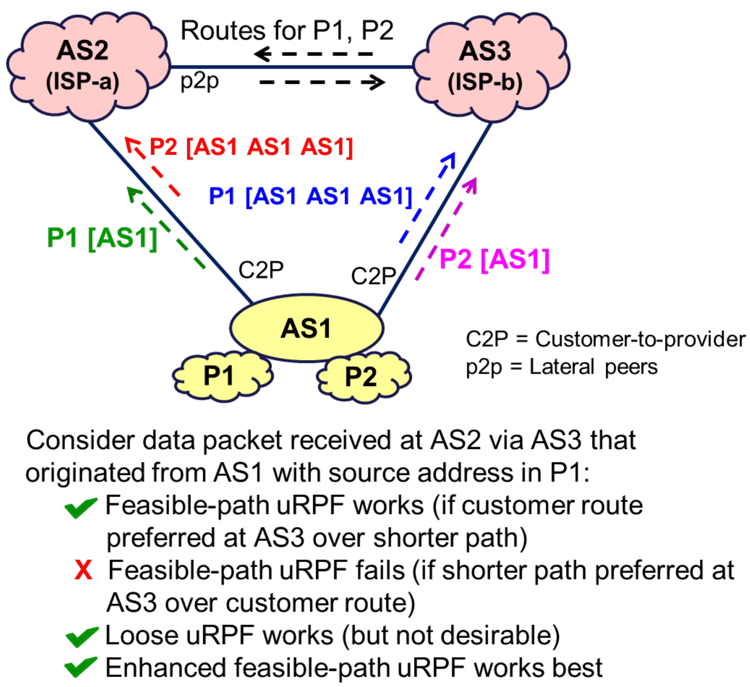



**Figure 10: Scenario 2 for illustration of efficacy of uRPF schemes**

However, the feasible-path uRPF method has limitations as well. One form of limitation naturally occurs when the recommendation of propagating the same prefixes to all routers is not heeded. Another form of limitation can be described as follows: in Scenario 2 (illustrated in Figure 10), it is possible that the second transit provider AS3 (ISP-b) does not propagate the prepended route (i.e., P1 [AS1 AS1 AS1]) to the first transit provider AS2 (ISP-a). This is because ISP-b's decision policy permits giving priority to a shorter route to prefix P1 via ISP-a over a longer route learned directly from the customer (AS1). In such a scenario, AS3 (ISP-b) would not send any route announcement for prefix P1 to AS2 (ISP-a). Then, a data packet originated from AS1 with a source address in prefix P1 that traverses via AS3 (ISP-b) will be dropped at AS2 (ISP-a).

### 5.1.4 SAV Using Loose Unicast Reverse Path Forwarding

In the loose unicast Reverse Path Forwarding (uRPF) method, an ingress packet at the border router is accepted only if the FIB has one or more prefixes that encompasses the source address. That is, a packet is dropped if no route exists in the FIB for the source address. Loose uRPF sacrifices directionality. This method is not very effective for preventing address spoofing. It only drops packets if the spoofed address is non-routable (e.g., belongs to obviously disallowed prefix blocks—prefixes marked “False” in column “Global” [IANA-v4-sp] [IANA-v6-sp], unallocated, or allocated but currently not routed). It may be noted that the method is more useful for IPv6 than IPv4.

### 5.1.5 SAV Using VRF Table

Virtual routing and forwarding (VRF) technology [RFC4364] [Juniper5] allows a router to maintain multiple routing table instances separate from the global routing information base (RIB). External BGP (eBGP) peering sessions send specific routes to be stored in a dedicated VRF table. The uRPF process queries the VRF table (instead of the FIB) for source address validation. A VRF table can be dedicated per eBGP peer and used for uRPF for only that peer, resulting in a strict mode operation. For implementing loose uRPF on an interface, the corresponding VRF table would be global (i.e., contains the same routes as in the FIB).

### 5.1.6 SAV Using Enhanced Feasible-Path uRPF (Emerging/Future)

The enhanced feasible-path uRPF (EFP-uRPF) method is currently a work in progress (soon to be RFC) in the IETF [EFP-uRPF]. It holds promise for providing a significant improvement in effectiveness and deployability over the feasible-path uRPF. This section briefly describes the technology and standards effort but does not make a security recommendation concerning the use of EFP-uRPF at this time.

EFP-uRPF adds greater flexibility and accuracy to uRPF operations than the existing uRPF methods discussed in Sections 5.1.2 through 5.1.5. The basic principle of the EFP-uRPF method for enhancing efficacy in multi-homing and asymmetric routing scenarios is as follows: if a route for prefix P1 is received on customer interface X and has origin AS1, and routes for P2 and P3 are received on other peering interfaces Y and Z but have the same origin AS1, then allow the flexibility that data packets with a source address in any of these three prefixes (P1, P2, P3) may be legitimately received on customer interface X. Thus, based on the common origin AS principle, the prefix list for allowable source addresses in data packets (i.e., the RPF list) is expanded to include all three prefixes (P1, P2, P3) for customer interface X. Further, the same principle is applied for determining the prefix list for allowable source addresses for each customer interface and possibly lateral peer interfaces.

As shown in Scenarios 1 and 2 (Figure 9 and Figure 10), the EFP-uRPF provides comparable or better performance than other uRPF methods for those scenarios. Scenario 3 (Figure 11) further illustrates that the EFP-uRPF method works best even in much more complex asymmetric routing scenarios. In Scenario 3 (Figure 11), the focus is on AS4 receiving data packets with a source address in {P1, P2, P3}. If EFP-uRPF is used, the operator (at AS4) can be assured that DDoS mitigation would work effectively, and none of those data packets would be subject to denial of service. The details concerning EFP-uRPF can be found in [EFP-uRPF]. Since it is still a work in progress, no security recommendations involving EFP-uRPF are offered here.

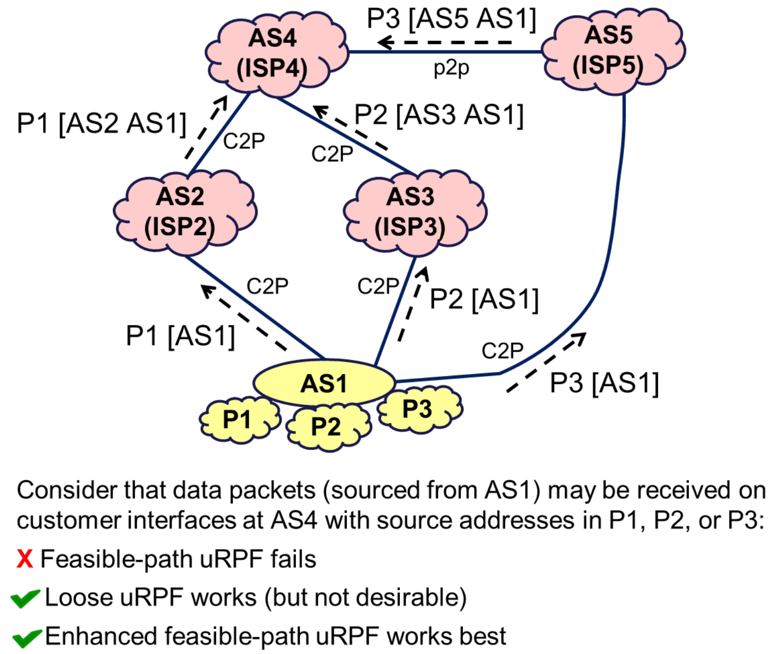



**Figure 11: Scenario 3 for illustration of efficacy of uRPF schemes**

### 5.1.7 More Effective Mitigation with Combination of Origin Validation and SAV

With the combination of BGP origin validation (BGP-OV) (see Section 4.3) and the SAV (uRPF) techniques discussed above, a stronger defense against address spoofing and DDoS is made possible. A determined DDoS attacker can subvert any of the uRPF methods by performing prefix hijacking followed by source address spoofing as illustrated in Figure 12. In the scenario in Figure 12, the attacker first compromises routers (or perhaps owns some of them) at AS98 and AS99, and then falsely announces a less-specific prefix (e.g., 10.1.0.0/21) encompassing the target's prefix (e.g., 10.1.0.0/22). It is assumed that there is currently no legitimate announcement of the less-specific prefix (10.1.0.0/21). The feasible-path uRPF (FP-uRPF) filters at AS5 and AS6 are effectively deceived, and the attacker possibly stays under the radar because the hijacked prefix is a less-specific prefix. The attacker would then be able to successfully perform address spoofing and DDoS with reflection amplification. To protect against this type of multipronged attack, the combination of BGP-OV (to prevent the hijacking) and FP-uRPF or EFP-uRPF (to prevent the address spoofing) should be employed. For this to work, the owners of the prefixes (10.1.0.0/22 and 10.1.0.0/21) should create ROAs, and all ASes (especially, AS5 and AS6) in Figure 12 should perform BGP-OV in addition to employing SAV using the FP-uRPF/EFP-uRPF method.

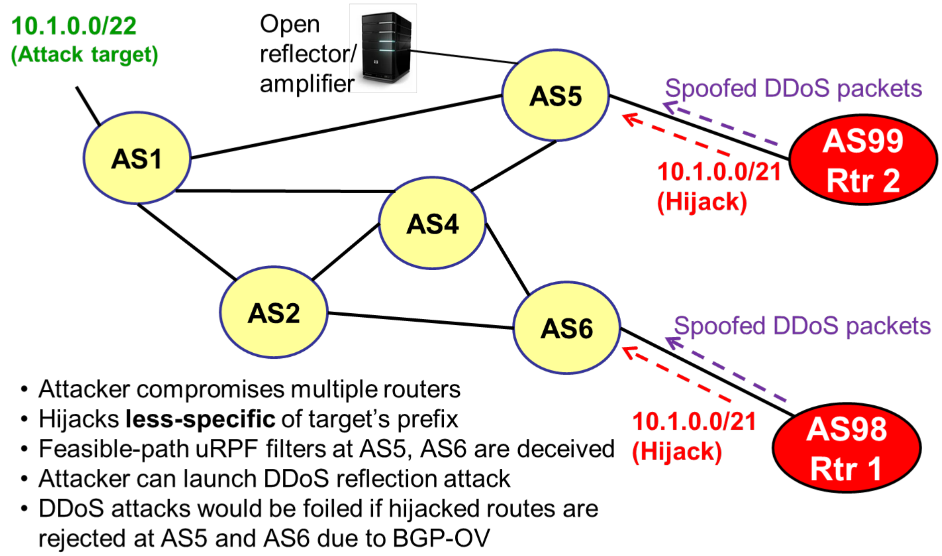



**Figure 12: Illustration of how origin validation complements SAV**

## 5.2 SAV Recommendations for Various Types of Networks

Three types of network scenarios are considered here, and SAV security recommendations are provided for each scenario. The network types are: 1) networks that have customers with directly connected allocated address space, such as broadband and wireless service providers; 2) enterprise networks; and 3) internet service providers (ISPs).

When a government agency or enterprise procures the services of a hosted service provider or transit ISP, the security recommendations listed here should be considered for inclusion in the service contracts as appropriate.

### 5.2.1 Customer with Directly Connected Allocated Address Space: Broadband and Wireless Service Providers

SAV with ACLs is relatively easy when a network served by an ISP's edge device (e.g., border router, CMTS, DSLAM, PDN-GW) is directly connected and using an IP address space that is suballocated by the ISP. Hence, SAV using the ACL method should always be used in such cases. For the egress packets (i.e., packets transiting via the edge device onto the internet), the source address must be within the allocated space. As an example, the Data Over Cable Service Interface Specification 3.1 (DOCSIS 3.1) standard for CMTS already incorporates this security check [DOCSIS] [Comcast] [RFC4036].

> **Security Recommendation 40:** BGP routers that have directly connected customers with suballocated address space, CMTS (or equivalent) in broadband access networks, and PDN-GW (or equivalent) in mobile networks should implement SAV using ACLs (Section 5.1.1). The BGP routers in this context may alternatively use the strict uRPF method (Section 5.1.2).

### 5.2.2 Enterprise Border Routers

The SAV security recommendations for enterprise border routers vary based on the egress/ingress nature of the data packets. Included here are recommendations concerning the routing control plane (BGP updates) as well.

> **Security Recommendation 41:** An enterprise border router that is multi-homed should always announce all of its address space to each of its upstream transit providers. This can be done in one of two ways: 1) announce an aggregate less-specific prefix to all transit providers and more-specific prefixes (covered by the less-specific prefix) to different transit providers as needed for traffic engineering, or 2) announce the same prefixes to each transit provider (albeit with suitable prepending for traffic engineering).[18]

> **Security Recommendation 42:** This is the exception case when the enterprise border router does not adhere to Security Recommendation 41 and instead selectively announces some prefixes to one upstream transit ISP and other prefixes to another upstream transit ISP. In this case, the enterprise should route data (by appropriate internal routing) such that the source addresses in the data packets towards each upstream transit ISP belong in the prefix or prefixes announced to that ISP.

> **Security Recommendation 43:** On the ingress side (i.e., for data packets received from the transit ISP), enterprise border routers should deploy loose uRPF (Section 5.1.4) and/or ACLs (Section 5.1.1) to drop packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked "False" in column "Global" [IANA-v4-sp] [IANA-v6-sp] and the enterprise's own prefixes).

> **Security Recommendation 44:** An enterprise (i.e., a leaf AS with or without multi-homing) should allow on the egress side (i.e., for data packets sent to the transit ISP) only those packets with source addresses that belong in their own prefixes.

### 5.2.3 Internet Service Providers

The SAV security recommendations for ISPs vary based on the ingress/egress of packets as well as the relationship with the peer (e.g., customer, lateral peer, transit provider).

> **Security Recommendation 45:** On customer-facing interfaces, smaller ISPs should perform SAV on ingress packets by deploying the feasible-path uRPF (see Section 5.1.3). They should avoid using strict or loose uRPF as they are not effective, especially in the case of multi-homed customers. It is recognized that larger ISPs may use loose uRPF on customer interfaces.[19]

---

[18] By following Security Recommendation 41, the enterprise border router ensures that the transit ISP's border routers discard (due to uRPF) only those data packets from the enterprise that do not have source addresses belonging in any of the enterprise's announced prefixes. Thus, it also ensures that data packets from the enterprise that have source addresses belonging in any of the enterprise's announced prefixes are never denied.

[19] In the future, the enhanced feasible-path uRPF [EFP-uRPF] may be considered based on the availability of commercial implementation (see Section 5.1.6).

**Security Recommendation 46:** For feasible-path uRPF to work appropriately, a smaller ISP (especially one that is near the internet edge) should propagate all of its announced address space to each of its upstream transit providers. This can be done in one of two ways: 1) announce an aggregate less-specific prefix to all transit providers and announce more-specific prefixes (covered by the less-specific prefix) to different transit providers as needed for traffic engineering, or 2) announce the same prefixes to each transit provider (albeit with suitable prepending for traffic engineering).

**Security Recommendation 47:** ISPs should prefer customer routes over other (i.e., transit provider or lateral peer) routes. (This is also normal ISP policy in most cases.)[20]

**Security Recommendation 48:** On interfaces with lateral (i.e., non-transit) peers, smaller ISPs (near the edge of the internet) should perform SAV on ingress packets by deploying the feasible-path uRPF (see Section 5.1.3). They should avoid using strict or loose uRPF as they are not very effective for SAV on the lateral peer interfaces. It is recognized that larger ISPs may use loose uRPF on the interfaces with lateral peers.

**Security Recommendation 49:** On interfaces with transit providers, ISPs should perform SAV on ingress packets by deploying loose uRPF (see Section 5.1.4) and/or ACLs (see Section 5.1.1) to drop packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked "False" in column "Global" [IANA-v4-sp] [IANA-v6-sp] and the ISP's internal-use only prefixes).

**Security Recommendation 50:** On the egress side towards customers, lateral (i.e., non-transit) peers, and transit providers, the ISP's border routers should deploy ACLs (see Section 5.1.1) to drop packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked "False" in column "Global" [IANA-v4-sp] [IANA-v6-sp] and the ISP's internal-use only prefixes).

### 5.3 Role of RPKI in Source Address Validation

A method was described in Section 4.6 on how ISPs can use the ROAs in RPKI registries to assist with the construction of prefix filters. The same technique can be applied to constructing ACLs for SAV on each customer-facing interface. These ACLs can be used to cross-check and/or augment entries in the RPF lists corresponding to each customer-facing interface.

**Security Recommendation 51:** Smaller ISPs should use the ROA data (available from RPKI registries) to construct and/or augment ACLs/RPF lists for SAV for ingress packets on customer interfaces.

[20] Security Recommendation 46 is also one of the stability conditions on BGP policy for ensuring stable convergence of routing information [Gao-Rexford].

### 5.4 Monitoring UDP/TCP Ports with Vulnerable Applications and Employing Traffic Filtering

DDoS threats involving vulnerable applications using various UDP/TCP ports and IoT devices are continually evolving and varied (e.g., memcached DDoS reflection attacks and SSDP diffraction, etc. [Bjarnason]). Hence, traffic filtering methods mentioned in this section are not meant to be exhaustive.

Traffic monitoring and filtering based on specific User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) ports are done to deny traffic of certain application types that are not expected on a given interface under consideration [TA14-017A] [Acunetix] [ISC2] [Arbor]. In some cases, the applications may be legitimate, but the observed traffic volumes may be suspiciously high, in which case response rate limiting is applied [Redbarn] [ISC1].

In the case of the DNS (Port 53), the enterprise internal DNS resolver can limit the scope of clients from which it will accept requests. The clients normally come from within the same enterprise network where the DNS resolver resides. Hence, the DNS recursive resolver can maintain access lists in the configuration so that an otherwise open DNS resolver can be effectively “closed” [ISOC]. Another effective measure is for the authoritative DNS resolvers to monitor the rate of queries per source address and apply response rate limiting (RRL), which dampens the rate at which authoritative servers respond to high volumes of malicious queries [Redbarn] [ISC1].

Table 1, below, lists application layer protocols and their port numbers [TA14-017A] [Akamai]. The UDP-based applications have been identified as vulnerable to reflection/amplification attacks. In Table 1, the amplification factor listed for each protocol is the traffic volume multiplier that can be achieved by exploiting the reflection/amplification effect of that protocol run on UDP [TA14-017A] [Akamai]. Port assignment status is called “Official” if officially assigned by IANA; otherwise it is “Unofficial” [TCP-UDP-port].

1298 **Table 1: Common Applications and their TCP/UDP Port Numbers**

| Application Protocol | Bandwidth Amplification Factor | Port # | Port Assignment Status |
|---|---|---|---|
| Domain Name System (DNS) | 28 to 54 | 53, 853, 953 | Official |
| Network Time Protocol (NTP) | 557 | 123 | Official |
| Simple Network Management Protocol (SNMP), SNMPv2 | 6 | 161 | Official |
| NetBIOS Name/Datagram/Session | 4 | 137/138/139 | Official |
| Simple Service Discovery Protocol (SSDP); discovery of UPnP devices | 31 | 1900 | Official |
| Character Generation Protocol (CharGEN) | 359 | 19 | Official |
| Quote of the Day (QOTD) | 140 | 17 | Official |
| BitTorrent | 4 | 6881-6887; 6889-90; 6891-6900; etc. various ranges | Unofficial |
| Kad Network (Kademlia P2P overlay protocol) | 16 | 6419, 6429 | Unofficial |
| Quake Network Protocol | 64 | 15, 28, 27500-27900, 27901-27910, 27950, 27952, 27960-27969, etc. | Unofficial |
| Streaming Protocols (e.g., QuickTime) | | 6970-9999, etc. | Unofficial |
| Real-Time Streaming Protocol (RTSP); ms-streaming | | 554, 1755 | Official |
| Routing Information Protocol (RIP, RIPng) | 131 | 520, 521 | Official |
| Multicast DNS (mDNS) | 2 to 10 | 5353 | Official |
| Portmap/Remote Procedure Call (RPC)RPC | 7 to 28 | 111, 369 | Official |
| Lightweight Directory Access Protocol (LDAP); Connection-less LDAP (CLDAP) | 70 | 389 | Official |

1299

The following set of security recommendations pertain to vulnerable applications such as those listed in Table 1:

**Security Recommendation 52:** In BGP routers, allow peers to connect to only port 179. The standard port for receiving BGP session OPEN messages is port 179, so attempts by BGP peers to reach other ports are likely to indicate faulty configuration or potential malicious activity.

**Security Recommendation 53:** Disable applications or services that are unwanted in the network or system under consideration.

**Security Recommendation 54:** Deny traffic for any TCP/UDP ports for which the network or system under consideration does not support the corresponding applications. In some cases, an application or service is supported on some interfaces (e.g., customer or internal-facing interfaces) but not others (e.g., internet-facing interfaces). In such cases, the traffic with a port ID specific to the application under consideration should be denied on interfaces on which the application is not supported.

**Security Recommendation 55:** This recommendation is aimed at the detection of traffic overload and mitigating actions. The relevant mitigation techniques are response rate limiting (RRL) [ISC1] [Redbarn] and source-based remotely triggered black hole (S/RTBH) filtering enabled with Flowspec [RFC5575] (see Section 5.5). These techniques are applicable to open services/protocols such as those listed in Table 1, which are themselves vulnerable to DoS/DDoS attacks or may be exploited for reflection/amplification. The recommendation consists of multiple steps as follows [TA14-017A]:

- Monitor the rate of queries/requests per source address and detect if an abnormally high volume of responses is headed to the same destination (i.e., same IP address).
- Apply the response rate limiting (RRL) technique to mitigate the attack.[21]
- Using BGP messaging (Flowspec), create a remotely triggered black hole (RTBH) filter. This can be coordinated with the upstream ISP.
- Maintain emergency contact information for the upstream provider to coordinate a response to the attack.
- An upstream ISP should actively coordinate responses with downstream customers.

The security recommendations that follow below are specific to NTP and DNS:

**Security Recommendation 56:** Deny NTP monlist request traffic (by disabling the monlist command) altogether, or enforce that the requests come from valid (permitted) source addresses.

[21] The RRL technique is commonly used in DNS and dampens the rate at which authoritative servers respond to high volumes of malicious queries. It can also be applied in other applications (shown in Table 1) for dampening the response rate.

**Security Recommendation 57:** To limit exploitation, an enterprise internal DNS recursive resolver should limit the scope of clients from which it accepts requests. The clients normally come from within the same enterprise network where the DNS resolver resides. Hence, the DNS recursive resolver can maintain access lists in the configuration so that it is not open to the entire internet [ISOC] [TA14-017A].

**Security Recommendation 58:** An enterprise should block UDP/Port 53 and TCP/Port 53 for ingress and egress at the network boundary; exceptions to this include designated enterprise recursive resolvers that need to send queries and designated enterprise authoritative servers that must listen for queries.

Concerning Security Recommendation 58, the purpose of blocking on egress is to block stub resolvers (on hosts) from sending their own queries out to the Internet and instead make sure they use an enterprise recursive resolver. Likewise, the purpose of blocking on ingress is to block attacks or “rogue” recursive resolvers from being used in attacks by blocking traffic from reaching them.

DNS, LDAP, and other DDoS amplification protocols generate significant amounts of UDP fragment traffic. It is possible to reduce the impact of DDoS amplification traffic by rate limiting UDP fragments at an ISP’s peering edges.

**Security Recommendation 59:** An ISP should perform rate limiting of UDP fragment traffic at edge routers facing customers and lateral peers.

### 5.5 BGP Flow Specification (Flowspec)

Destination-based remotely triggered black-holing (D/RTBH) [RFC3882] [RFC7999] and source-based remotely triggered black-holing (S/RTBH) [RFC5635] (the latter in conjunction with uRPF) have been used as techniques for DDoS mitigation. However, with the standardization and vendor support of Flowspec [RFC5575] [RFC7674] [Hares] [Ryburn] [Cisco4] [Juniper4], the basic principles of D/RTBH and S/RTBH are significantly enhanced and can be operationally deployed in a fine-grained, dynamic, and efficient way. Operational experience with Flowspec for DDoS mitigation has been reported in [Levy2] [Compton].

In D/RTBH, a BGP message is sent to trigger the provider edge (PE) routers (within the victim’s AS or its transit provider AS) to block ingress traffic to the specified IP address where the affected server resides. In S/RTBH, a BGP message is sent to trigger the provider edge (PE) routers (within the victim’s AS or its transit provider AS) to block ingress traffic from the specified IP address that is the source address employed by the attacker. In S/RTBH, loose uRPF is used to filter traffic from the specified source address. In the BGP Flowspec mechanism, a flow specification NLRI is defined and used to convey information about filtering rules for traffic that should be discarded [RFC5575]. This mechanism allows an upstream AS to perform inbound filtering in their edge routers of traffic that a given downstream AS wishes to drop. Table 2 shows the information that can be included in BGP Flowspec [RFC5575].

**Table 2: BGP Flowspec types**

| | |
|---|---|
| Type 1 | Destination Prefix |
| Type 2 | Source Prefix |
| Type 3 | IP Protocol |
| Type 4 | Source or Destination Port |
| Type 5 | Destination Port |
| Type 6 | Source Port |
| Type 7 | ICMP Type |
| Type 8 | ICMP Code |
| Type 9 | TCP flags |
| Type 10 | Packet length |
| Type 11 | DSCP |
| Type 12 | Fragment Encoding |

Table 3 shows the extended community values that are defined to specify various types of actions [RFC5575] requested at the upstream AS.

**Table 3: Extended community values defined in Flowspec to specify various types of actions**

| Type | Extended Community | Encoding |
|---|---|---|
| 0x8006 | Traffic-rate (set to 0 to drop all traffic) | 2-byte as#, 4-byte float |
| 0x8007 | Traffic-action (sampling) | Bitmask |
| 0x8008 | Redirect to VRF (route target) | 6-byte route target |
| 0x8009 | Traffic-marking | DSCP value |

In the table above, VRF stands for "virtual routing and forwarding," and DSCP stands for "differentiated services code point". Flowspec facilitates flexible specification and communication (by downstream AS) of rules and actions for DDoS mitigation to be executed at edge routers in the upstream AS.

**Security Recommendation 60:** Edge routers should be equipped to perform destination-based remotely triggered black hole (D/RTBH) filtering and source-based remotely triggered black hole (S/RTBH) filtering.

**Security Recommendation 61:** Edge routers should be equipped to make use of BGP flow specification (Flowspec) to facilitate DoS/DDoS mitigation (in coordination between upstream and downstream autonomous systems).

**Security Recommendation 62:** Edge routers in an AS providing RTBH filtering should have an ingress policy towards RTBH customers to accept routes more specific than /24 in IPv4 and /48 in IPv6. Additionally, the edge routers should accept a more specific route (in case of D/RTBH) only if it is subsumed by a less-specific route that the customer is authorized to announce as standard policy (i.e., the less-specific route has a registered IRR entry and/or an ROA). Further, the edge routers should not drop RTBH-related more-specific route advertisements from customers even though BGP origin validation may mark them as "Invalid."

**Security Recommendation 63:** A customer AS should make sure that the routes announced for RTBH filtering have NO_EXPORT, NO_ADVERTISE, or similar communities.

**Security Recommendation 64:** An ISP providing an RTBH filtering service to customers must have an egress policy that denies routes that have community tagging meant for triggering RTBH filtering. This is an additional safeguard in case NO_EXPORT, NO_ADVERTISE, or similar tagging fails.

**Security Recommendation 65:** An ISP providing an RTBH filtering service to customers must have an egress policy that denies prefixes that are longer than expected. This provides added safety in case NO_EXPORT, NO_ADVERTISE, or similar tagging fails.

# References


[Acunetix] "Prevention of NTP Reflection DDoS attacks based on CVE-2013-5211," Acunetix blog, September 2014. http://www.acunetix.com/blog/articles/ntp-reflection-ddos-attacks/

[Adalier1] M. Adalier, K. Sriram, O. Borchert, K. Lee, and D. Montgomery, "High Performance BGP Security: Algorithms and Architectures", North American Network Operators Group (NANOG 69), Washington D.C, February 2017. https://archive.nanog.org/sites/default/files/1_Sriram_High_Performance_Bgp_v1.pdf (slides) https://www.youtube.com/watch?v=Yp03po5WJP0 (video)

[Adalier2] M. Adalier, "Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256," NIST Workshop on ECC Standards, June 2015. http://csrc.nist.gov/groups/ST/ecc-workshop-2015/papers/session6-adalier-mehmet.pdf

[Akamai] J. Artega and W. Mejia, "CLDAP Reflection DDoS," Akamai Threat Advisory, April 2017. https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf

[APNIC1] G. Michaelson, "MyAPNIC RPKI service now supports AS0 ROA creation," APNIC technical note online, November 2018. https://blog.apnic.net/2018/11/09/myapnic-rpki-service-now-supports-as0-roa-creation/

[Arbor] "Worldwide Infrastructure Security Report," Vol. XI, Arbor Networks report (2016). https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

[ARIN1] "Using RPKI at ARIN to certify resources," ARIN online. https://www.arin.net/resources/rpki/using_rpki.html#hosted

[ARIN2] M. Kosters, "ARIN Provisioning in RPKI," NANOG 67, June 2016. https://archive.nanog.org/sites/default/files/Kosters.pdf

[ARTEMIS] Automatic and Real-Time dEtection and Mitigation (ARTEMIS) http://www.inspire.edu.gr/artemis/

[BCP38] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," BCP 38 (RFC 2827), May 2000. https://tools.ietf.org/html/bcp38

[BCP84] F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," BCP 84 (RFC 3704), March 2004, https://tools.ietf.org/html/bcp84

[BGPmon] BGPmon: https://bgpmon.net/

[BGPStream] BGPStream: https://bgpstream.caida.org/

[Bjarnason] S. Bjarnason, "Withstanding the Infinite: DDoS Defense in the Terabit Era," Presentation at NANOG-74, October 2018. https://pc.nanog.org/static/published/meetings/NANOG74/1789/20181001_Bjarnason_Withstanding_The_Infinite__v1.pdf

[Botnet-Roadmap] "A Road Map Toward Resilience Against Botnets," Joint US DoC/DHS report, November 2018. https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf

[Cisco1] "BGP—Origin AS Validation," http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/irg-origin-as.pdf

[Cisco2] "Understanding Unicast Reverse Path Forwarding," Cisco blog, http://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

[Cisco3] "Unicast reverse path forwarding enhancements for the internet service provider—internet service provider network edge," Cisco WP, http://www.cisco.com/c/dam/en_us/about/security/intelligence/urpf.pdf

[Cisco4] "Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide, Release 5.2.x – Chapter: Implementing BGP Flowspec," http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html

[Comcast] "Comcast network management: Preventing Network Spoofing," March 2014, http://networkmanagement.xfinity.com/index.php/faqs-on-preventing-network-spoofing

[Compton] R. Compton, T. Bowlby, T. Harris, P. Lotia, "eBGP Flowspec Peering for DDoS Mitigation," NANOG 75, February 2019. https://pc.nanog.org/static/published/meetings/NANOG75/1887/20190219_Compton_Ebgp_Flowspec_Peering_v1.pdf

[CSRIC4-WG5] CSRIC Working Group 5 Final Report: Remediation of Server-Based DDoS Attacks. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remedia tion_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf

[CSRIC4-WG6] "Long-Term Core Internet Protocol Improvements," Working Group 6 presentation, September 2015. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG6_Presentation_09242014.pdf

[CSRIC6-WG3] "Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols," March 2019. https://www.fcc.gov/files/csric6wg3finalreport030819pdf

[CSDE] "Cyber Crisis: Foundations of Multi-Stakeholder Coordination," Council for Secure Digital Economy (CSDE) report (2019). https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf

[CVE-2013-5211] "Vulnerability summary for CVE-2013-5211," (for vulnerability related to monlist feature in NTP), National Vulnerability Database, September 27, 2016. https://nvd.nist.gov/vuln/detail/CVE-2013-5211

[Cymru-bogon] "Bogon route server project: Bogons via BGP" http://www.team-cymru.org/bogon-reference-bgp.html

[Cymru-UTRS] Unwanted traffic removal service (UTRS), Team Cymru blog, http://www.team-cymru.com/utrs.html

[DOC-Botnet] U.S. Department of Commerce, U.S. Department of Homeland Security, "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," May 22, 2018. https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final

[DOCSIS] "DOCSIS® 3.1 Technology", CableLabs, https://www.cablelabs.com/technologies/docsis-3-1.

[EFP-uRPF] K. Sriram, D. Montgomery, and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Filtering," IETF Internet Draft, August 2019. https://datatracker.ietf.org/doc/draft-ietf-opsec-urpf-improvements/

[ENISA] "7 Steps to shore up the Border Gateway Protocol (BGP)", the EU Cybersecurity Agency, May 2019.

[Firmin] F. Firmin, "The Evolved Packet Core," 3GPP The Mobile Broadband Standard. https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

[FISMA2002] Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat. 2946. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[FISMA2014] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

[Gao-Rexford] Freedman, M., "Interdomain Routing Policy", Princeton University COS 461 Lecture Notes; Slides 25-27, Spring 2011, http://www.cs.princeton.edu/courses/archive/spr11/cos461/docs/lec17-bgp-policy.ppt

[goBGP] Use of Resource Public Key Infrastructure (RPKI) server to do Origin AS Validation in goBGP. https://github.com/osrg/gobgp/blob/master/docs/sources/rpki.md

[Hares] S. Hares, C. Loibl, R. Raszuk, D. McPherson, and M. Bacher, "Dissemination of Flow Specification Rules," IETF I.D. draft-ietf-idr-rfc5575bis (work in progress), June 2018. https://datatracker.ietf.org/doc/draft-ietf-idr-rfc5575bis/

[HelpNet] "DNS amplification attacks double in Q1 2018," Help Net Security blog, June 2018. https://www.helpnetsecurity.com/2018/06/14/dns-amplification-attacks-q1-2018/

[Huston2011] G. Huston and R. Bush, "Securing BGP," The Internet Protocol Journal, Volume 14, No. 2, June 2011. http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-52/142-bgp.html

[Huston2012] G. Huston, "Leaking Routes," Asia Pacific Network Information Centre (APNIC) Blog, March 2012, http://labs.apnic.net/blabs/?p=139/

[Huston2016] G. Huston, "Taking a Closer Look at the Recent DDoS Attacks and What It Means for the DNS," CircleID Blog, October 2016. http://www.circleid.com/posts/20161026_closer_look_at_recent_ddos_attacks_and_what_it_means_for_dns/

[IANA-ASN-sp] "Special-Purpose Autonomous System (AS) Numbers" IANA web page. https://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml

[IANA-v4-r] "IANA IPv4 Address Space Registry," IANA web page. http://www.iana.org/assignments/ipv4-address-space

[IANA-v6-r] "Internet Protocol Version 6 Address Space," IANA web page. http://www.iana.org/assignments/ipv6-address-space

[IANA-v4-sp] "IANA IPv4 Special-Purpose Address Registry," IANA web page. https://www.iana.org/assignments/iana-ipv4-special-registry

[IANA-v6-sp] "IANA IPv6 Special-Purpose Address Registry," IANA web page. http://www.iana.org/assignments/iana-ipv6-special-registry

[IETF-GROW] IETF Global Routing Operations (GROW) Working Group https://datatracker.ietf.org/wg/grow/documents/

[IETF-IDR] IETF Inter-Domain Routing (IDR) Working Group https://datatracker.ietf.org/wg/idr/documents/

[IETF-OPSEC] IETF Operational Security Capabilities for IP Network Infrastructure (OPSEC) Working Group https://datatracker.ietf.org/wg/opsec/documents/

[IETF-SIDR] IETF Secure Inter-Domain Routing (SIDR) Working Group https://datatracker.ietf.org/wg/sidr/documents/

[IETF-SIDROPS] IETF Secure Inter-Domain Routing Operations (SIDROPS) Working Group https://datatracker.ietf.org/wg/sidrops/documents/

[ISC1] "A Quick Introduction to Response Rate Limiting," ISC Knowledge Base blog. https://kb.isc.org/article/AA-01000/0/A-Quick-Introduction-to-Response-Rate-Limiting.html

[ISC2] "A Chargen-base DDoS? Chargen still a thing?" ISC blog, https://isc.sans.edu/forums/diary/A+Chargenbased+DDoS+Chargen+is+still+a+thing/15647

[ISOC] P. Vixie (Ed.), "Addressing the challenge of IP spoofing," ISOC report, September 2015. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf

[ISTR-2015] *Internet Security Threat Report 2015, Volume 20*, Symantec Corporation, Mountain View, CA, April 2015. https://www.symantec.com/content/en/us/enterprise/other_resources/2134

7933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

[ISTR-2016] *Internet Security Threat Report 2016, Volume 21*, Symantec Corporation, Mountain View, CA, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[ISTR-2017] *Internet Security Threat Report 2017, Volume 22*, Symantec Corporation, Mountain View, CA, April 2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[Juniper1] "Example: Configuring Origin Validation for BGP," Juniper blog, http://www.juniper.net/techpubs/en_US/junos12.2/topics/topic-map/bgp-origin-as-validation.html

[Juniper2] "Configuring Unicast RPF," Juniper blog, https://www.juniper.net/documentation/en_US/junos14.2/topics/usage-guidelines/interfaces-configuring-unicast-rpf.html

[Juniper3] "Example: Configuring Unicast Reverse-Path-Forwarding Check," Juniper blog, http://www.juniper.net/documentation/en_US/junos15.1/topics/topic-map/unicast-rpf.html

[Juniper4] "Example: Enabling BGP to Carry Flow-Specification Routes," Juniper TechLibrary. https://www.juniper.net/documentation/en_US/junos12.3/topics/example/routing-bgp-flow-specification-routes.html

[Juniper5] "Creating Unique VPN Routes Using VRF Tables," May 2019 https://www.juniper.net/documentation/en_US/junos/topics/topic-map/l3-vpns-routes-vrf-tables.html#id-understanding-virtual-routing-and-forwarding-tables

[Kapela-Pilosov] A. Pilosov and T. Kapela, "Stealing the Internet: An Internet-Scale Man in the Middle Attack", 16th Defcon Conference, August 2008, https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf .

[Levy1] M. Levy, "RPKI - The required cryptographic upgrade to BGP routing," Cloudflare blog, September 2018. https://blog.cloudflare.com/rpki/

[Levy2] N. Levy, D. Smith, and J. Schiel, "Bi-Lateral Security Management Framework (a.k.a. DDoS peering)," NANOG 71, October 2017. https://pc.nanog.org/static/published/meetings/NANOG71/1447/2017100

3_Levy_Operationalizing_Isp_v2.pdf

[Luckie] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy, "AS Relationships, Customer Cones, and Validation," Proceedings of the 2013 ACM Internet Measurement Conference (IMC), DOI 10.1145/2504730.2504735, October 2013. http://www.caida.org/~amogh/papers/asrank-IMC13.pdf

[MANRS] "Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide," Published by the Internet Society (ISOC), retrieved October 2019. https://www.manrs.org/isps/guide/

[MANRS2] "MANRS Observatory," Monitoring data published by Internet Society (ISOC), retrieved October 2019. https://observatory.manrs.org/#/overview

[maxlength] Y. Gilad, S. Goldberg, K. Sriram, J. Snijders, and B. Maddison, "The use of maxlength in the RPKI," IETF Internet Draft, April 2019. https://datatracker.ietf.org/doc/draft-ietf-sidrops-rpkimaxlen/

[Merit-RADb] "Merit RADb" (Merit Network Inc.) http://www.radb.net

[Mirai1] "Mirai: what you need to know about the botnet behind recent major DDoS attacks," Symantec Security Response, October 27, 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

[Mirai2] "Dyn Analysis Summary of Friday October 21 Attack," Dyn Company News, October 26, 2016. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[Murphy] S. Murphy, "RPKI Tutorial: Routing Security and RPKI", NANOG on the Road (NOTR), St. Louis, MO, November, 2015 https://www.nanog.org/sites/default/files/04-Murphy-StLouis.pdf

[NABCOP] "DDoS-DoS-attack-BCOP," North American BCOP, http://nabcop.org/index.php/DDoS-DoS-attack-BCOP

[Naik] A. Naik, "Internet Vulnerability Takes Down Google," ThousandEyes report, November 2018. https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/

[NANOG] "Practical BGP Origin Validation using RPKI: Vendor Support, Signing and Validation Services, and Operational Experience," NANOG Track (multiple presentations) at NANOG 67, Chicago, IL, June 2016. https://archive.nanog.org/meetings/nanog67/agenda

[NANOG-list] "Intra-AS messaging for route leak prevention," NANOG Email List - Discussion Thread, June 2016. http://mailman.nanog.org/pipermail/nanog/2016-June/thread.html#86348

[NCCoE-sidr] W. Haag, D. Montgomery, W.C. Barker, A. Tan, "Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation, Volume B," NIST Special Publication (SP) 1800-14B, August 2018. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/sidr-piir-nist-sp1800-14b-draft.pdf

[NIST-CSF] Cybersecurity Framework, National Institute of Standards and Technology [Web site], http://www.nist.gov/cyberframework/

[NIST-RIDR] "Robust Inter-Domain Routing," NIST RIDR project. https://www.nist.gov/programs-projects/robust-inter-domain-routing

[NIST-SRx] BGP Secure Routing Extension (BGP-SRx): Open source Origin Validation and BGPsec Path Validation implementations in Quagga. https://www-x.antd.nist.gov/bgpsrx/

[NIST-RPKI] "RPKI Deployment Monitor," NIST's online monitor with Global and Regional views. https://rpki-monitor.antd.nist.gov/

[NSA-BGP] "A guide to Border Gateway Protocol (BGP) Best Practices," NSA Technical Report, September 2018. https://apps.nsa.gov/iaarchive/library/reports/a-guide-to-border-gateway-protocol-bgp-best-practices.cfm

[Patel] K. Patel, "Cisco's Origin Validation Implementation," NANOG 67, June 2016. https://www.nanog.org/sites/default/files/Patel.pdf

[Parsons1] "Secure Your Routing Infrastructure," Parsons blog. http://www.securerouting.net/

[Parsons2] Open source Origin Validation and BGPsec Path Validation implementations in BIRD, Parsons blog. http://www.securerouting.net/tools/bird/

[PEO-13800] U.S. Presidential Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[Quilt] "The Quilt security cookbook," published by the Quilt community, https://www.nitrd.gov/nitrdgroups/images/d/db/Quilt-Network-Security-Cookbook-v7.pdf

[Redbarn] "Response Rate Limiting in the Domain Name System (DNS RRL)," Redbarn blog. http://www.redbarn.org/dns/ratelimits

[RFC2725] C. Villamizar, C. Alaettinoglu, D. Meyer, S. Murphy, "Routing Policy System Security," IETF RFC 2725, December 1999. https://tools.ietf.org/html/rfc2725

[RFC3882] D. Turk, "Configuring BGP to Block Denial-of-Service Attacks," IETF RFC 3882, September 2004. https://tools.ietf.org/rfc/rfc3882.txt

[RFC4012] L. Blunk, J. Damas, F. Parent, and A. Robachevsky, "Routing Policy Specification Language next generation (RPSLng)," IETF RFC 4012, March 2005. https://tools.ietf.org/html/rfc4012

[RFC4036] W. Sawyer, "Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modem Termination Systems for Subscriber Management", RFC 4036, DOI 10.17487/RFC4036, April 2005. https://www.rfc-editor.org/info/rfc4036

[RFC4271] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF RFC 4271, January 2006. https://tools.ietf.org/html/rfc4271

[RFC4364] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006. https://www.rfc-editor.org/info/rfc4364

[RFC5802] V. Gill, J. Heasley, D. Meyer, P. Savola, Ed., C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)," IETF RFC 5082, October 2007. https://tools.ietf.org/html/rfc5082

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile," IETF RFC 5280, May 2008. http://www.ietf.org/rfc/rfc5280.txt.

[RFC5575] P. Marques et al., "Dissemination of Flow Specification Rules," IETF RFC 5575, August 2009. https://tools.ietf.org/html/rfc5575

[RFC5635] W. Kumari and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, DOI 10.17487/RFC5635, August 2009. https://tools.ietf.org/html/rfc5635

[RFC6092] J. Woodyatt, "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service," IETF RFC 6092, January 2011. https://tools.ietf.org/html/rfc6092

[RFC6472] W. Kumari and K. Sriram, "Recommendation for Not Using AS_SET and AS_CONFED_SET in BGP," BCP 172 (RFC 6472), December 2011. https://tools.ietf.org/html/rfc6472

[RFC6480] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," RFC6480, February 2012. https://tools.ietf.org/html/rfc6480

[RFC6481] G. Huston, R. Loomans, and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, February 2012. https://tools.ietf.org/html/rfc6481

[RFC6482] M. Lepinski, S. Kent, and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012. https://tools.ietf.org/html/rfc6482

[RFC6483] G. Huston and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs) ", RFC 6483, February 2012. https://tools.ietf.org/html/rfc6483

[RFC6487] G. Huston, G. Michaelson, and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," RFC 6487, February 2012. https://tools.ietf.org/html/rfc6487

[RFC6492] G. Huston, R. Loomans, B. Ellacott, and R. Austein, "A Protocol for Provisioning Resource Certificates," RFC 6492, February 2012. https://tools.ietf.org/html/rfc6492

[RFC6810] R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol," RFC 6810, January 2013. https://tools.ietf.org/html/rfc6810

[RFC6811] P. Mohapatra, J. Scudder, D. Ward, R. Bush, and R. Austein, "BGP Prefix Origin Validation," IETF RFC 6811, January 2013. https://tools.ietf.org/pdf/rfc6811.pdf

[RFC7318] A. Newton and G. Huston, "Policy Qualifiers in Resource Public Key Infrastructure (RPKI) Certificates," RFC 7318, July 2014. https://tools.ietf.org/html/rfc7318

[RFC7353] S. Bellovin, R. Bush, and D. Ward, "Security Requirements for BGP Path Validation," IETF RFC 7353, August 2014. https://tools.ietf.org/html/rfc7353

[RFC7382] S. Kent, D. Kong, and K. Seo, "Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)," IETF RFC 7382, April 2015. https://tools.ietf.org/html/rfc7382

[RFC7454] J. Durand, I. Pepelnjak, and G. Doering, "BGP Operations and Security," IETF RFC 7454, February 2015. https://tools.ietf.org/html/rfc7454

[RFC7674] J. Haas, "Clarification of the Flowspec Redirect Extended Community," IETF RFC 7674, October 2015. https://tools.ietf.org/html/rfc7674

[RFC7908] K. Sriram, D. Montgomery, D. McPherson, E. Osterweil, and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, June 2016. https://tools.ietf.org/html/rfc7908

[RFC7909] R. Kisteleki and B. Haberman, "Securing Routing Policy Specification Language (RPSL) Objects with Resource Public Key Infrastructure (RPKI) Signatures," IETF RFC 7909, June 2016. https://tools.ietf.org/html/rfc7909

[RFC7935] G. Huston and G. Michaelson, "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure," IETF RFC 7935, August 2016. https://tools.ietf.org/html/rfc7935

[RFC7999] T. King, et al., "BLACKHOLE Community," IETF RFC 7999, October 2016. https://tools.ietf.org/html/rfc7999

[RFC8182] T. Bruijnzeels, O. Muravskiy, B. Webre, and R. Austein, "RPKI Repository Delta Protocol (RRDP)," IETF RFC 8182, July 2017. https://tools.ietf.org/html/rfc8182

[RFC8205] M. Lepinski (Ed.) and K. Sriram (Ed.), "BGPsec Protocol Specification," IETF RFC 8205, September 2017. https://tools.ietf.org/html/rfc8205

[RFC8208] S. Turner and O. Borchert, "BGPsec Algorithms, Key Formats, & Signature Formats," IETF RFC 8208, September 2017. https://tools.ietf.org/html/rfc8208

[RFC8210] R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1," IETF RFC 8210, September 2017. https://tools.ietf.org/html/rfc8210

[RFC8374] K. Sriram (Ed.), "BGPsec Design Choices and Summary of Supporting Discussions," IETF RFC 8374, April 2018. https://tools.ietf.org/html/rfc8374

[RIPE1] RIPE NCC Resource Certification: Using the RPKI System, https://www.ripe.net/manage-ips-and-asns/resource-management/certification/using-the-rpki-system

[RIPE2] RIPE NCC RPKI Validator, https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources

[RIPE3] "Router Configuration with JunOS and Cisco IOS," RIPE NCC blog, https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration

[RIPE-399] P. Smith, R. Evans, and M. Hughes, "RIPE-399 - RIPE Routing Working Group Recommendations on Route Aggregation", December 2006. https://www.ripe.net/publications/docs/ripe-399

[RIPE-532] P. Smith and R. Evans, "RIPE-532 - RIPE Routing Working Group Recommendations on IPv6 Route Aggregation", November 2011. https://www.ripe.net/publications/docs/ripe-532

[RouteLeak1] K. Sriram (Ed.) and A. Azimov (Ed.), "Methods for Detection and Mitigation of BGP Route Leaks", IETF Internet Draft, July 2019. https://datatracker.ietf.org/doc/draft-ietf-grow-route-leak-detection-mitigation/

[RouteLeak2] A. Azimov, E. Bogomazov, R. Bush, K. Patel, and K. Sriram, "Route Leak Prevention using Roles in Update and Open Messages", IETF Internet Draft, July 2019. https://datatracker.ietf.org/doc/draft-ietf-idr-bgp-open-policy/

[RouteLeak3] K. Sriram (Ed.), "Design Discussion of Route Leaks Solution Methods", IETF Internet Draft, August 2019. https://datatracker.ietf.org/doc/draft-sriram-idr-route-leak-solution-discussion/

[Rsync] Wiki page on the Rsync protocol. https://en.wikipedia.org/wiki/Rsync

[Rsync-RPKI] S. Kent and K. Sriram, "RPKI Rsync Download Delay Modeling," Presented at the IETF-86, IETF SIDR WG Meeting, March 2013. https://www.ietf.org/proceedings/86/slides/slides-86-sidr-1.pdf

[RTRlib] "An open-source C implementation of the RPKI/Router Protocol client," https://github.com/rtrlib and http://www.mi.fu-berlin.de/en/inf/groups/ilab/software/index.html

[Ryburn] J. Ryburn, "DDoS Mitigation using BGP Flowspec," NANOG 63, February 2015. https://archive.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf

[Scudder] J. Scudder, "RPKI on Juniper Routers," NANOG 67, June 2016. https://www.nanog.org/sites/default/files/Scudder.pdf

[SP800-53] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) 800-53 Revision 4, April 2013 (includes updates as of 01-22-2015). https://doi.org/10.6028/NIST.SP.800-53r4

[SP800-54] Kuhn DR, Sriram K, Montgomery D (2007) Border Gateway Protocol Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-54. https://doi.org/10.6028/NIST.SP.800-54

[SWIP] S. Whipple, "The SWIP Template Tutorial," ARIN VII, April 2001. https://www.arin.net/vault/participate/meetings/reports/ARIN_VII/PDF/tutorials/swip_arin.pdf

[Sriram1] K. Sriram, D. Montgomery, and R. Bush, "RIB Size and CPU Workload Estimation for BGPSEC," Presentation at the IETF-91 Joint IDR/SIDR WG Meeting, November 2014. http://www.ietf.org/proceedings/91/slides/slides-91-idr-17.pdf

[Sriram2] V.K. Sriram and D. Montgomery, "Design and analysis of optimization algorithms to minimize cryptographic processing in BGP security protocols," Computer Communications, volume 106, pages 75-85, July 2017. https://doi.org/10.1016/j.comcom.2017.03.007

[Symantec] C. Wueest, "Denial-of-service attacks – short but strong: DDoS amplification attacks continue to increase as attackers experiment with new protocols," Symantec Blog, October 2014. http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong

[ThousandEyes] ThousandEyes: BGP Route Monitoring https://www.thousandeyes.com/solutions/bgp-and-route-monitoring

[Winward] R. Winward, "Mirai – Inside of an IoT Botnet," NANOG 69, February 2017. https://www.nanog.org/sites/default/files/1_Winward_Mirai_The_Rise.pdf

[Wishnick] D. Wishnick and C. Yoo, "Overcoming Legal Barriers to RPKI Adoption," Presented at NANOG 74, October 2018. https://pc.nanog.org/static/published/meetings//NANOG74/daily/day_2.html#talk_1767

[TA16-288A] "Heightened DDoS Threat Posed by Mirai and Other Botnets," US-CERT alert TA16-288A, November 30, 2016. https://www.us-cert.gov/ncas/alerts/TA16-288A

[TA14-017A] "UDP-Based Amplification Attacks," US-CERT alert TA14-017A, January 17, 2014. https://www.us-cert.gov/ncas/alerts/TA14-017A

[TCP-UDP-port] "List of TCP and UDP ports," https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers .

[Toonk-A] Toonk, A., "What caused the Google service interruption", BGPMON Blog, March 2015, http://www.bgpmon.net/what-caused-the-google-service-interruption/ .

[Toonk-B] Toonk, A., "Massive route leak causes Internet slowdown", BGPMON Blog, June 2015, http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/ .

[Verisign1] "Verisign Releases Q4 2016 DDoS Trends Report: 167% Increase in Average Peak Attack from 2015 to 2016," CircleID blog post, February 2017. http://www.circleid.com/posts/20170214_verisign_releases_q4_2016_ddos_trends_report_167_increase/

[Verisign2] "Distributed Denial of Service Trends Report" by Verisign, Published quarterly. http://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml

[White] R. White, "Rethinking Path Validation," NANOG 66, February 2016. https://www.nanog.org/sites/default/files/White_Rethinking_Bgp_Path.pdf

[Zmijewski] E. Zmijewski, "Indonesia Hijacks the World", Dyn Research/Renesys Blog, April 2014, http://research.dyn.com/2014/04/indonesia-hijacks-world

# Appendix A—Consolidated List of Security Recommendations

Table 4 provides a consolidated list of the security recommendations from various sections throughout the document. If the "Enterprise" column is checked, it means that the security recommendation should be considered for implementation in enterprise and hosted service provider autonomous systems (ASes)—in some cases, action(s) to be performed by the AS operator, and in other cases, feature(s) that should be available in their BGP router(s). A similar statement applies for ISPs when the "ISP" column is checked. The "Open Servers" column pertains to providers of open internet services, such as DNS, DNSSEC, or NTP. When an enterprise outsources services, then the feature/service corresponding to a security recommendation that applies to them would in turn apply to their hosted service provider. An enterprise should always consider (in their service contract) whether their transit ISP meets security recommendations that are checked in the ISP column. There is no column in Table 4 corresponding to an internet exchange point (IXP), but the BGP (control plane) security recommendations for ISPs also apply to opaque IXPs (i.e., IXPs that insert their ASN in the AS path and operate BGP).

**Table 4: Consolidated List of the Security Recommendations**

| | Applicable to | | |
|---|---|---|---|
| **Security Recommendation** | **Enter-prise** | **ISP** | **Open Servers** |
| **BGP Origin Validation:** | | | |
| **Security Recommendation 1:** All internet number resources (e.g., address blocks and AS numbers) should be covered by an appropriate registration services agreement with an RIR, and all point-of-contact (POC) information should be up to date. The granularity of such registrations should reflect all sub-allocations to entities (e.g., enterprises within the parent organization, branch offices) that operate their own network services (e.g., internet access, DNS). | X | X | |
| **Security Recommendation 2:** In the case of address block (NetRange) registration in ARIN, the originating autonomous system (origin AS) should be included. See https://whois.arin.net/rest/net/NET-128-3-0-0-1/pft?s=128.3.0. | X | X | |
| **Security Recommendation 3:** Route objects corresponding to the BGP routes originating from an AS should be registered and actively maintained in an appropriate RIR's IRR. Enterprises should ensure that appropriate IRR information exists for all IP | X | X | |

| | | | |
|---|---|---|---|
| address space used directly and by their outsourced IT systems and services. | | | |
| **Security Recommendation 4:** Internet number resource holders with IPv4/IPv6 prefixes and/or AS numbers (ASNs) should obtain RPKI certificate(s) for their resources. | X | X | |
| **Security Recommendation 5:** Transit providers should provide a service where they create, publish, and manage subordinate resource certificates for address space and/or ASNs suballocated to their customers.<br><br>Note: Currently, RPKI services based on the hosted model and offered by RIRs are common. This security recommendation can be implemented in the hosted or delegated model based on service agreements with customers. | | X | |
| **Security Recommendation 6:** Resource holders should register ROA(s) in the global RPKI for all prefixes that are announced or intended to be announced on the public internet. | X | X | |
| **Security Recommendation 7:** Each transit provider should provide a service where they create, publish, and maintain ROAs for prefixes suballocated to their customers. Alternatively, as part of the service, customers can be allowed to create, publish, and maintain their ROAs in a repository maintained by the transit provider.<br><br>Note: This security recommendation can be implemented in the hosted or delegated model based on service agreements with customers. | | X | |
| **Security Recommendation 8:** If a prefix that is announced (or intended to be announced) is multi-homed and originated from multiple ASes, then one ROA per originating AS should be registered for the prefix (possibly in combination with other prefixes which are also originated from the same AS). | X | X | |
| **Security Recommendation 9:** When an ISP or enterprise owns multiple prefixes that include less-specific and more-specific prefixes, they should ensure that the more-specific prefixes have ROAs before creating ROAs for the subsuming less-specific prefixes. | X | X | |
| **Security Recommendation 10:** An ISP should wait until more specific prefixes announced from within their customer cone have ROAs prior to the creation of its own ROAs for subsuming | | X | |

| | | | |
|---|---|---|---|
| less-specific prefix(es). | | | |
| **Security Recommendation 11:** An ISP or enterprise should create an AS0 ROA for any prefix that is currently not announced to the public internet. However, this should be done only after ensuring that ROAs exist for any more-specific prefixes subsumed by the prefix that are announced or are intended to be announced. | X | X | |
| **Security Recommendation 12:** A BGP router should not send updates with AS_SET or AS_CONFED_SET in them (in compliance with BCP 172 [RFC6472]). | X | X | |
| **Security Recommendation 13:** ISPs and enterprises that operate BGP routers should also operate one or more RPKI-validating caches. | X | X | |
| **Security Recommendation 14:** A BGP router should maintain an up-to-date white list consisting of {prefix, maxlength, origin ASN} that is derived from valid ROAs in the global RPKI. The router should perform BGP-OV. | X | X | |
| **Security Recommendation 15:** In partial/incremental deployment state of the RPKI, the permissible {prefix, origin ASN} pairs for performing BGP-OV should be generated by taking the union of such data obtained from ROAs, IRR data, and customer contracts. | X | X | |
| **Security Recommendation 16:** BGP-OV results should be incorporated into local policy decisions to select BGP best paths.<br><br>Note: Exactly how BGP-OV results are used in path selection is strictly a local policy decision for each network operator. Typical policy choices include:<br><br>• Tag-Only – BGP-OV results are only used to tag/log data about BGP routes for diagnostic purposes.<br>• Prefer-Valid – Use local preference settings to give priority to valid routes. Note this is only a tie-breaking preference among routes with the exact same prefix.<br>• Drop-Invalid – Use local policy to ignore invalid routes in the BGP decision process. | X | X | |
| **Security Recommendation 17:** The maxlength in the ROA should not exceed the length of the most specific prefix (subsumed under the prefix in consideration) that is originated or intended to be originated from the AS listed in the ROA. | X | X | |

| | | | |
|---|---|---|---|
| **Security Recommendation 18:** If a prefix and select more-specific prefixes subsumed under it are announced or intended to be announced, then instead of specifying a maxlength, the prefix and the more-specific prefixes should be listed explicitly in multiple ROAs (i.e., one ROA per prefix or more-specific prefix).<br><br>Note: In general, the use of maxlength should be avoided unless all or nearly all more-specific prefixes up to a maxlength are announced (or intended to be announced) [maxlength]. | X | X | |
| **Prefix (Route) Filtering:** | | | |
| **Security Recommendation 19:** IPv6 routes should be filtered to permit only allocated IPv6 prefixes. Network operators should update IPv6 prefix filters regularly to include any newly allocated prefixes.<br><br>Note: If prefix resource owners regularly register AS0 ROAs (see Section 4.3) for allocated (but possibly currently unused) prefixes, then those ROAs could be a complementary source for the update of prefix filters. | X | X | |
| **Security Recommendation 20:** Prefixes that are marked “False” in column “Global” [IANA-v4-sp] [IANA-v6-sp] are forbidden from routing in the global internet and should be rejected if received from an external BGP (eBGP) peer. | X | X | |
| **Security Recommendation 21:** For single-homed prefixes (subnets) that are owned and originated by an AS, any routes for those prefixes received at that AS from eBGP peers should be rejected. | X | X | |
| **Security Recommendation 22:** It is recommended that an eBGP router should set the specificity limit for each eBGP peer and reject prefixes that exceed the specificity limit on a per-peer basis.<br><br>Note: The specificity limit may be the same for all peers (e.g., /24 for IPv4 and /48 for IPv6). | X | X | |
| **Security Recommendation 23:** The default route (0.0.0.0/0 in IPv4 and ::/0 in IPv6) should be rejected except when a special peering agreement exists that permits accepting it. | X | X | |
| **Security Recommendation 24:** An internet exchange point (IXP) should announce—from its route server to all of its member ASes—its LAN prefix or its entire prefix, which would be the | X | X | |

| | | | |
|---|---|---|---|
| same as or less specific than its LAN prefix. Each IXP member AS should, in turn, accept this prefix and reject any more-specific prefixes (of the IXP announced prefix) from any of its eBGP peers. | | | |
| **Security Recommendation 25: Inbound prefix filtering facing lateral peer** – The following prefix filters should be applied in the inbound direction:<br>• Unallocated prefixes<br>• Special-purpose prefixes<br>• Prefixes that the AS originates<br>• Prefixes that exceed a specificity limit<br>• Default route<br>• IXP LAN Prefixes | X | X | |
| **Security Recommendation 26: Outbound prefix filtering facing lateral peer** – The appropriate outbound prefixes are those that are originated by the AS in question and those originated by its downstream ASes (i.e., the ASes in its customer cone). The following prefix filters should be applied in the outbound direction:<br>• Unallocated prefixes<br>• Special-purpose prefixes<br>• Prefixes that exceed a specificity limit<br>• Default route<br>• IXP LAN prefixes<br>• Prefixes learned from AS's other peers<br>• Prefixes learned from AS's transit providers | X | X | |
| **Security Recommendation 27: Inbound prefix filtering facing transit provider – Case 1 (full routing table):** In general, when the full routing table is required from the transit provider, the following prefix filters should be applied in the inbound direction:<br>• Unallocated prefixes<br>• Special-purpose prefixes<br>• Prefixes that the AS originates<br>• Prefixes that exceed a specificity limit<br>• IXP LAN prefixes | X | X | |
| **Security Recommendation 28: Inbound prefix filtering facing transit provider – Case 2 (default route):** If the border router is configured for only the default route, then only the | X | X | |

| | | | |
|---|---|---|---|
| default route should be accepted from the transit provider and nothing else. | | | |
| **Security Recommendation 29: Outbound prefix filtering facing transit provider:** The same outbound prefix filters should be applied as those for a lateral peer (see Section 4.5.1) except that the last two bullets are modified as follows:<br><br>• Prefixes learned from AS's lateral peers<br>• Prefixes learned from AS's other transit providers<br><br>Note: In conjunction with the outbound prefix filtering security recommendation, some policy rules may also be applied if a transit provider is not contracted (or chosen) to provide transit for some subset of outbound prefixes. | X | X | |
| **Security Recommendation 30: Inbound prefix filtering facing customer in Scenario 1** (see Section 4.5.3) – Only the prefixes that are known to be originated from the customer and its customer cone should be accepted, and all other route announcements should be rejected. | | X | |
| **Security Recommendation 31: Inbound prefix filtering facing customer in Scenario 2** (see Section 4.5.3) – The same set of inbound prefix filters should be applied as those for a lateral peer (see Section 4.5.1). | | X | |
| **Security Recommendation 32: Outbound prefix filtering facing customer:** The filters applied in this case would vary depending on whether the customer wants to receive only the default route or the full routing table. If it is the former, then only the default route should be announced and nothing else. In the latter case, the following outbound prefix filters should be applied:<br><br>• Special-purpose prefixes<br>• Prefixes that exceed a specificity limit<br><br>Note: The default route filter may be added if the customer requires the full routing table but not the default route. | | X | |
| **Security Recommendation 33: Inbound prefix filtering for leaf customer facing transit provider** – A leaf customer may request only the default route from its transit provider. In this case, only the default route should be accepted and nothing else. If the leaf customer requires the full routing table from the transit provider, then it should apply the following inbound prefix filters: | X | | |

| | | | |
|---|---|---|---|
| • Unallocated prefixes<br>• Special-purpose prefixes<br>• Prefixes that the AS (i.e., leaf customer) originates<br>• Prefixes that exceed a specificity limit<br>• Default route | | | |
| **Security Recommendation 34: Outbound prefix filtering for leaf customer facing transit provider** – A leaf customer network should apply a very simple outbound policy of announcing only the prefixes it originates. However, it may additionally apply the same outbound prefix filters as those for a lateral peer (see Section 4.5.1) to observe extra caution. | X | | |
| **Security Recommendation 35:** The ROA data (available from RPKI registries) should be used to construct and/or augment prefix filter lists for customer interfaces. | | X | |
| **Checking AS Path for Disallowed AS Numbers** | | | |
| **Security Recommendation 36:** The AS path in an update received in eBGP should be checked to ensure that the local AS number is not present. The AS path should also be checked to ensure that AS numbers meant for special purposes [IANA-ASN-sp] are not present. In case of a violation, the update should be rejected.<br><br>Note: The special purpose ASN 23456 is allocated for AS_TRANS [RFC6793] and is allowed to be present in an AS_PATH in conjunction with an AS4_PATH [RFC 6793] in the update. | X | X | |
| **Route Leak Mitigation:** | | | |
| **Security Recommendation 37:** An AS operator should have an ingress policy to tag routes internally (locally within the AS) to communicate from ingress to egress regarding the type of peer (customer, lateral peer, or transit provider) from which the route was received. | X | X | |
| **Security Recommendation 38:** An AS operator should have an egress policy to utilize the tagged information (in Security Recommendation 37) to prevent route leaks when routes are forwarded on the egress. The AS should not forward routes received from a transit provider to another transit provider or a | X | X | |

| | | | |
|---|---|---|---|
| lateral peer. Also, the AS should not forward routes received from a lateral peer to another lateral peer or a transit provider. | | | |
| **GTSM** | | | |
| **Security Recommendation 39:** The Generalized TTL Security Mechanism (GTSM) [RFC5082] should be applied on a per-peer basis to provide protection against spoofed BGP messages. | X | X | |
| **DDoS Mitigation (Anti-spoofing):** | | | |
| **Security Recommendation 40:** BGP routers that have directly connected customers with suballocated address space, CMTS (or equivalent) in broadband access networks, and PDN-GW (or equivalent) in mobile networks should implement SAV using ACLs (Section 5.1.1). The BGP routers in this context may alternatively use the strict uRPF method (Section 5.1.2). | | X | |
| **Security Recommendation 41:** An enterprise border router that is multi-homed should always announce all of its address space to each of its upstream transit providers. This can be done in one of two ways: 1) announce an aggregate less-specific prefix to all transit providers and more-specific prefixes (covered by the less-specific prefix) to different transit providers as needed for traffic engineering, or 2) announce the same prefixes to each transit provider (albeit with suitable prepending for traffic engineering). | X | | |
| **Security Recommendation 42:** This is the exception case when the enterprise border router does not adhere to Security Recommendation 41 and instead selectively announces some prefixes to one upstream transit ISP and other prefixes to another upstream transit ISP. In this case, the enterprise should route data (by appropriate internal routing) such that the source addresses in the data packets towards each upstream transit ISP belong in the prefix or prefixes announced to that ISP. | X | | |
| **Security Recommendation 43:** On the ingress side (i.e., for data packets received from the transit ISP), enterprise border routers should deploy loose uRPF (Section 5.1.4) and/or ACLs (Section 5.1.1) to drop packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked “False” in column “Global” [IANA-v4-sp] [IANA-v6-sp] and the enterprise’s own prefixes). | X | | |

| | | | |
|---|---|---|---|
| **Security Recommendation 44:** An enterprise (i.e., a leaf AS with or without multi-homing) should allow on the egress side (i.e., for data packets sent to the transit ISP) only those packets with source addresses that belong in their own prefixes. | X | | |
| **Security Recommendation 45:** On customer-facing interfaces, smaller ISPs should perform SAV on ingress packets by deploying the feasible-path uRPF (see Section 5.1.3). They should avoid using strict or loose uRPF as they are not effective, especially in the case of multi-homed customers. It is recognized that larger ISPs may use loose uRPF on customer interfaces. | | X | |
| **Security Recommendation 46:** For feasible-path uRPF to work appropriately, a smaller ISP (especially one that is near the internet edge) should propagate all of its announced address space to each of its upstream transit providers. This can be done in one of two ways: 1) announce an aggregate less-specific prefix to all transit providers and announce more-specific prefixes (covered by the less-specific prefix) to different transit providers as needed for traffic engineering, or 2) announce the same prefixes to each transit provider (albeit with suitable prepending for traffic engineering). | | X | |
| **Security Recommendation 47:** ISPs should prefer customer routes over other (i.e., transit provider or lateral peer) routes. (This is also normal ISP policy in most cases.)<br><br>Note: Following this recommendation facilitates a basis for adhering to Security Recommendation 45. It is also one of the stability conditions on BGP policy for ensuring stable convergence of routing information [Gao-Rexford]. | | X | |
| **Security Recommendation 48:** On interfaces with lateral (i.e., non-transit) peers, smaller ISPs (near the edge of the internet) should perform SAV on ingress packets by deploying the feasible-path uRPF (see Section 5.1.3). They should avoid using strict or loose uRPF as they are not very effective for SAV on the lateral peer interfaces. It is recognized that larger ISPs may use loose uRPF on the interfaces with lateral peers. | | X | |
| **Security Recommendation 49:** On interfaces with transit providers, ISPs should perform SAV on ingress packets by deploying loose uRPF (see Section 5.1.4) and/or ACLs (see Section 5.1.1) to drop packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked “False” in column “Global” [IANA-v4-sp] [IANA-v6-sp] | | X | |

| | | | |
|---|---|---|---|
| and the ISP's internal-use only prefixes). | | | |
| **Security Recommendation 50:** On the egress side towards customers, lateral (i.e., non-transit) peers, and transit providers, the ISP's border routers should deploy ACLs (see Section 5.1.1) to drop packets when the source address is spoofed (i.e., belongs to obviously disallowed prefix blocks—prefixes marked "False" in column "Global" [IANA-v4-sp] [IANA-v6-sp] and the ISP's internal-use only prefixes). | | X | |
| **Security Recommendation 51:** Smaller ISPs should use the ROA data (available from RPKI registries) to construct and/or augment ACLs/RPF lists for SAV for ingress packets on customer interfaces. | | X | |
| **Traffic Filtering (Monitoring UDP/TCP Ports with Vulnerable Applications):** | | | |
| **Security Recommendation 52:** In BGP routers, allow peers to connect to only port 179. The standard port for receiving BGP session OPEN messages is port 179, so attempts by BGP peers to reach other ports are likely to indicate faulty configuration or potential malicious activity. | X | X | |
| **Security Recommendation 53:** Disable applications or services that are unwanted in the network or system under consideration. | | | X |
| **Security Recommendation 54:** Deny traffic for any TCP/UDP ports for which the network or system under consideration does not support the corresponding applications. In some cases, an application or service is supported on some interfaces (e.g., customer or internal-facing interfaces) but not others (e.g., internet-facing interfaces). In such cases, the traffic with a port ID specific to the application under consideration should be denied on interfaces on which the application is not supported. | | | X |
| **Security Recommendation 55:** This recommendation is aimed at the detection of traffic overload and mitigating actions. The relevant mitigation techniques are response rate limiting (RRL) [ISC1] [Redbarn] and source-based remotely triggered black hole (S/RTBH) filtering enabled with Flowspec [RFC5575] (see Section 5.5). These techniques are applicable to open services/protocols such as those listed in Table 1, which are themselves vulnerable to DoS/DDoS attacks or may be exploited | | | X |

| | | | |
|---|---|---|---|
| for reflection/amplification. The recommendation consists of multiple steps as follows [TA14-017A]:<br><br>• Monitor the rate of queries/requests per source address and detect if an abnormally high volume of responses is headed to the same destination (i.e., same IP address).<br>• Apply the response rate limiting (RRL) technique to mitigate the attack.<br>• Using BGP messaging (Flowspec), create a remotely triggered black hole (RTBH) filter. This can be coordinated with the upstream ISP.<br>• Maintain emergency contact information for the upstream provider to coordinate a response to the attack.<br>• An upstream ISP should actively coordinate responses with downstream customers. | | | |
| **Security Recommendation 56:** Deny NTP monlist request traffic (by disabling the monlist command) altogether, or enforce that the requests come from valid (permitted) source addresses. | | | X |
| **Security Recommendation 57:** To limit exploitation, an enterprise internal DNS recursive resolver should limit the scope of clients from which it accepts requests. The clients normally come from within the same enterprise network where the DNS resolver resides. Hence, the DNS recursive resolver can maintain access lists in the configuration so that it is not open to the entire internet [ISOC] [TA14-017A]. | | | X |
| **Security Recommendation 58:** An enterprise should block UDP/Port 53 and TCP/Port 53 for ingress and egress at the network boundary; exceptions to this include designated enterprise recursive resolvers that need to send queries and designated enterprise authoritative servers that must listen for queries. (See explanation in Section 5.4.) | | | X |
| **Security Recommendation 59:** An ISP should perform rate limiting of UDP fragment traffic at edge routers facing customers and lateral peers. | | X | |
| **DDoS Mitigation (Remote Triggered Black Hole filtering, Flow specification):** | | | |
| **Security Recommendation 60:** Edge routers should be equipped to perform destination-based remotely triggered black hole (D/RTBH) filtering and source-based remotely triggered | X | X | |

| | | | |
|---|---|---|---|
| black hole (S/RTBH) filtering. | | | |
| **Security Recommendation 61:** Edge routers should be equipped to make use of BGP flow specification (Flowspec) to facilitate DoS/DDoS mitigation (in coordination between upstream and downstream autonomous systems). | X | X | |
| **Security Recommendation 62:** Edge routers in an AS providing RTBH filtering should have an ingress policy towards RTBH customers to accept routes more specific than /24 in IPv4 and /48 in IPv6. Additionally, the edge routers should accept a more specific route (in case of D/RTBH) only if it is subsumed by a less-specific route that the customer is authorized to announce as standard policy (i.e., the less-specific route has a registered IRR entry and/or an ROA). Further, the edge routers should not drop RTBH-related more-specific route advertisements from customers even though BGP origin validation may mark them as "Invalid." | | X | |
| **Security Recommendation 63:** A customer AS should make sure that the routes announced for RTBH filtering have NO_EXPORT, NO_ADVERTISE, or similar communities. | X | X | |
| **Security Recommendation 64:** An ISP providing an RTBH filtering service to customers must have an egress policy that denies routes that have community tagging meant for triggering RTBH filtering. This is an additional safeguard in case NO_EXPORT, NO_ADVERTISE, or similar tagging fails. | | X | |
| **Security Recommendation 65:** An ISP providing an RTBH filtering service to customers must have an egress policy that denies prefixes that are longer than expected. This provides added safety in case NO_EXPORT, NO_ADVERTISE, or similar tagging fails. | | X | |

## Appendix B— Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

| | |
|---|---|
| ACL | Access Control List |
| AfriNIC | African Network Information Center |
| APNIC | Asia-Pacific Network Information Centre |
| ARIN | American Registry for Internet Numbers |
| AS | Autonomous System |
| BGP | Broder Gateway Protocol |
| BGP-OV | BGP Origin Validation |
| BGP-PV | BGP Path Validation |
| BGPsec | Broder Gateway Protocol with Security Extensions |
| DA | Destination Address |
| DSCP | Differentiated Services Code Point |
| DHS | Department of Homeland Security |
| DoS | Denial of Service |
| DDoS | Distributed Denial of Service |
| DNS | Domain Name System |
| DNSSEC | Domain Name System Security Extensions |
| eBGP | External BGP |
| EFP-uRPF | Enhanced Feasible Path Unicast Reverse Path Forwarding |
| FIB | Forwarding Information Base |
| FISMA | Federal Information Security Modernization Act |
| Flowspec | Flow Specification |
| FP-uRPF | Feasible Path Unicast Reverse Path Forwarding |
| GTSM | Generalized TTL Security Mechanism |

| | |
|---|---|
| IANA | Internet Assigned Numbers Authority |
| iBGP | Internal BGP |
| ICMP | Internet Control Message Protocol |
| IETF | Internet Engineering Task Force |
| IGP | Internal Gateway Protocol |
| IRR | Internet Routing Registry |
| ISP | Internet Service Provider |
| IXP | Internet Exchange Point |
| LACNIC | Latin America and Caribbean Network Information Centre |
| maxlength | Maximum allowed length of a prefix specified in RAO |
| NCCoE | National Cybersecurity Center of Excellence |
| NIST SP | NIST Special Publication |
| NLRI | Network Layer Routing Information (synonymous with prefix) |
| NTP | Network Time Protocol |
| RFC | Request for Comments (IETF standards document) |
| RFD | Route Flap Damping |
| RIB | Routing Information Base |
| RIPE | Réseaux IP Européens |
| RIR | Regional Internet Registry |
| RITE | Resilient Interdomain Traffic Exchange |
| ROA | Route Origin Authorization |
| RPKI | Resource Public Key Infrastructure |
| RPKI-to-router protocol | RPKI cache to router protocol |
| RLP | Route Leak Protection |

| | |
|---|---|
| RRDP | RPKI Repository Delta Protocol |
| RTBH | Remotely Triggered Black-Holing |
| D/RTBH | Destination-based Remotely Triggered Black-Holing |
| S/RTBH | Source-based Remotely Triggered Black-Holing |
| SA | Source Address |
| SAV | Source Address Validation |
| SIDR | Secure Inter-Domain Routing |
| SIDR WG | Secure Inter-Domain Routing Working Group (in the IETF) |
| SSDP | Simple Service Discovery Protocol |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| UPnP | Universal Plug and Play |
| uRPF | Unicast Reverse Path Forwarding |