VyOS Networks

SOLUTION BRIEF

RESOURCE PUBLIC KEY INFRASTRUCTURE (RPKI)

Overview

Routing protocols such as **Border Gateway Protocol (BGP)** are commonly deployed today with a strong reliance on trust. Any peer—either unintentionally or with malicious intent—can announce IP prefixes they don't own, potentially disrupting Internet traffic. To prevent this, many networks implement manually maintained filtering rules, which require human oversight whenever routing changes occur.

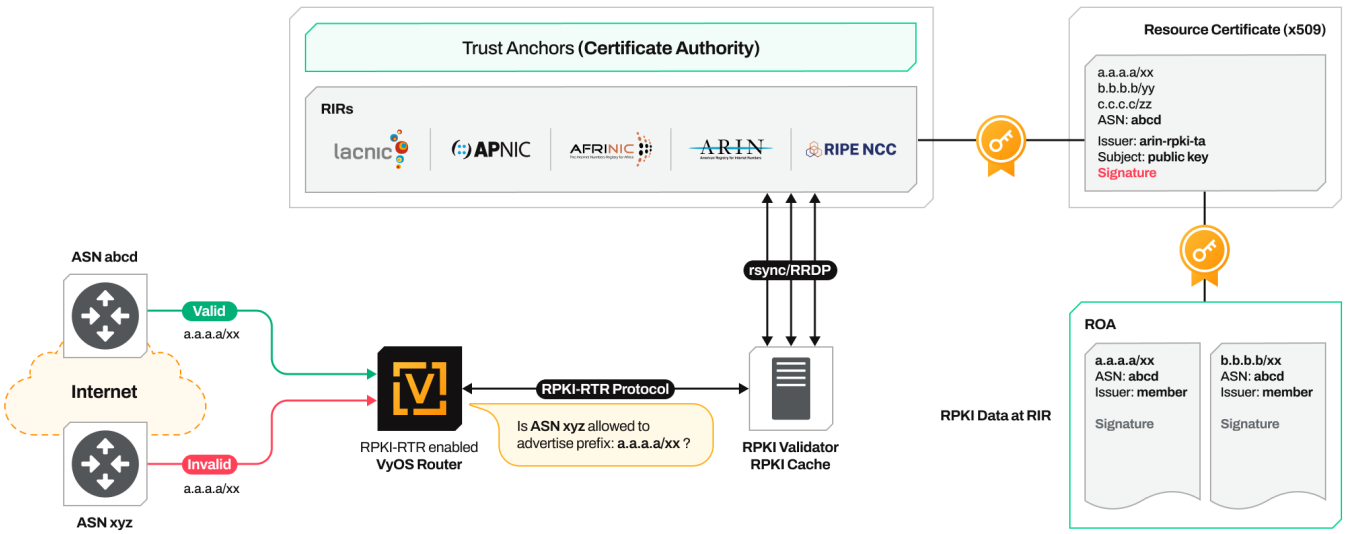
Resource Public Key Infrastructure (RPKI) addresses this issue by offering a cryptographic mechanism to validate prefix ownership, reducing the risk of incorrect route advertisements on the global Internet.

What is Resource Public Key Infrastructure (RPKI)?

Resource Public Key Infrastructure (RPKI) is a security framework designed to prevent IP route hijacking and improve the trustworthiness of **BGP (Border Gateway Protocol)** routing on the Internet. It uses cryptographic certificates to prove ownership of IP address blocks and Autonomous System Numbers (ASNs).

What is RPKI used for?

RPKI is used to create and validate **Route Origin Authorizations (ROAs)**, which specify which ASNs are authorized to originate routes to specific IP prefixes. When a BGP update is received, networks that use RPKI can check the validity of the origin AS number against the ROAs to ensure it is legitimate.



How is RPKI used?

- **Certificate Authorities (CAs)** issue digital certificates to IP address holders (e.g., RIRs like ARIN, RIPE).
- Organizations generate **ROAs**, stating which AS is allowed to advertise each prefix.
- Network operators deploy **RPKI validators** that fetch and verify ROAs.
- BGP routers use the validation results to mark prefixes as:
  - **Valid** (matches ROA)
  - **Invalid** (mismatch)
  - **Not Found** (no ROA exists)
- Routing policies can then be enforced to **prefer valid routes** and reject or deprioritize invalid ones.

How does RPKI benefit organizations?

- **Protects IP address space** from being hijacked or misused.
- **Improves routing security**, reducing the risk of traffic interception or blackholing due to incorrect BGP advertisements.
- **Enhances trust and reputation**, especially for ISPs, content providers, and enterprises with public-facing services.
- **Helps comply with security best practices** and industry expectations for BGP filtering and origin validation.

Summary of Key Components

Component	Role
ROA	Authorizes an ASN to announce a prefix
RPKI Validator	Fetches and verifies ROAs from CAs
BGP Router	Receives prefix info and validates it
RTR Protocol	Transports validated data to routers
Routing Policy	Decides what to do with valid/invalid routes

VyOS, being a fully open-source network operating system, supports **RPKI-based BGP origin validation**, making it a great option for organizations that want to enhance routing security without relying on expensive or proprietary solutions.

How VyOS Helps with RPKI

VyOS uses **FRRouting (FRR)** as its routing engine, which supports integration with external **RPKI validators** via the **RTR (RPKI-to-Router) protocol** (RFC 6810/6811).

Here's how it works with VyOS:

- **Configure VyOS to connect to an RPKI validator**, such as Routinator or rpki-client.
- **VyOS downloads validated ROAs** via RTR over TCP.
- **BGP announcements received by VyOS are validated** against ROAs.
- **Routing policy is applied** to:
  - Accept only **valid** routes.
  - Drop or de-preference **invalid** or **NotFound** routes.

Benefits of Using RPKI in VyOS

Benefit	Description
Routing Security	Prevents acceptance of BGP routes from unauthorized or malicious sources.
Open-Source & Cost-Effective	No licensing costs; full transparency and customization.
Flexibility	Can be deployed on-prem, in the cloud, or at the edge.
BGP Policy Control	Easily define route-maps and prefix-lists based on RPKI status.
Compliance & Best Practices	Aligns with MANRS (Mutually Agreed Norms for Routing Security) standards.

sales@vyos.io
vyos.io