Your Network’s Security Shield powered by BGP Security

The High-Stakes Game of "Blind Trust"

The Internet wasn’t designed for bad actors; it was designed for academic collaboration. Its foundation—a web of interconnected Autonomous Systems—relies on a "trust-by-default" model that served us well until 2010 but has become a liability in the modern era. BGP’s fragility isn’t a bug; it is a function of the era in which the protocol was invented, where connectivity was between trusted systems and the intent was to enable access to a worldwide web.

We are now witnessing a high-stakes transition from this era of "blind trust" to one of "explicit verification." This change is driven in part by the value of the information that flows on top of the BGP transport fabric. Furthermore development of cloud networks have further increased the need to enhance security in the Internet since private information is maintained on the public cloud. To address the needs of the modern evolving network operators are re-engineering the backbone, shifting away from manual, error-prone configurations toward a resilient framework of cryptographic validation and automated deployment. It is a fundamental pivot toward true network resilience.

Your IP Address Needs a Digital Passport (RPKI)

To secure global routing, the industry is moving toward Resource Public Key Infrastructure (RPKI). Think of it as a digital passport system for IP addresses. RPKI adapts standard X.509 certificate fundamentals to verify the ownership of network identifiers like IP addresses and Autonomous System Numbers (ASNs).

Under this framework, resource owners obtain certificates from Regional Internet Registries (RIRs) like ARIN or RIPE NCC. These are used to generate a Route Origin Authorization (ROA)—a cryptographically signed statement specifying which ASNs are authorized to advertise specific IP blocks. These ROAs are stored in RIR repositories and synchronized globally via protocols like **rsync** or **RRDP** (RPKI Repository Delta Protocol). This moves the needle from "assuming" a route is legitimate to "verifying" it via proven digital ownership.

As the security experts at INCIBE-CERT, the Spanish National Cybersecurity Institute's Computer Emergency Response Team note:

"Given the lack of validation and verification mechanisms, malicious or incorrect information can be easily accepted and propagated by the Network, causing interruptions or malicious traffic diversions."

BGP Hijacking remains the ultimate "ghost in the machine." Because the Border Gateway Protocol (BGP) lacks intrinsic security, attackers can manipulate routes to redirect traffic to unauthorized destinations, leading to data interception or massive outages.

RPKI is the essential antidote, but the real magic happens at the router level via the **RPKI to Router Protocol (RPKI-RTR)**. This protocol allows routers to receive real-time validation data from "Waypoints" or RPKI validators. By comparing BGP advertisements against synchronized ROA data, routers can make informed decisions in milliseconds—dropping "Invalid" routes and prioritizing "Valid" ones. Organizations can even use tools like the "Is BGP Safe Yet?" portal to audit implementation and pressure providers toward better hygiene.

To maximize resilience, organizations are increasingly deploying their own proprietary RPKI validators. This mitigates external dependencies and allows ISPs to enforce internal routing policies with direct, first-party confirmation of validity.

Several powerful open-source validators are now the industry standard:

- **Routinator:** Created by NLnet Labs; noted for its high community activity and reliability.
- **FORT:** Developed by NIC Mexico; distinguished by its simplicity and lightweight footprint, perfect for resource-constrained environments.

TCP-AO: The Secret Handshake in BGP

BGP, which uses a TCP session, does not benefit directly from packet-level authentication. Authentication in BGP is a critical concern because BGP carries routing information all over the global public internet, creating a tempting target for route-status hackers, and, at the same time, making the authenticity of inter- and intra-AS routing information absolutely essential.

An initial attempt at TCP authentication in RFC 2385 added an MD5 signature to the TCP segment header. The TCP option Kind field value of 19 (decimal) indicated the presence of the MD5 signature in the TCP segment header. It did not take long before the restrictive nature of the length and type of the protection became apparent. Simply put, this method quickly became outdated. TCP-AO based on RFC 5925 replaced the older method with a more flexible and improved authentication technique, using TCP header option Kind 29 (decimal) to indicate use of the TCP authentication option (TCP-AO).

TCP-AO added:

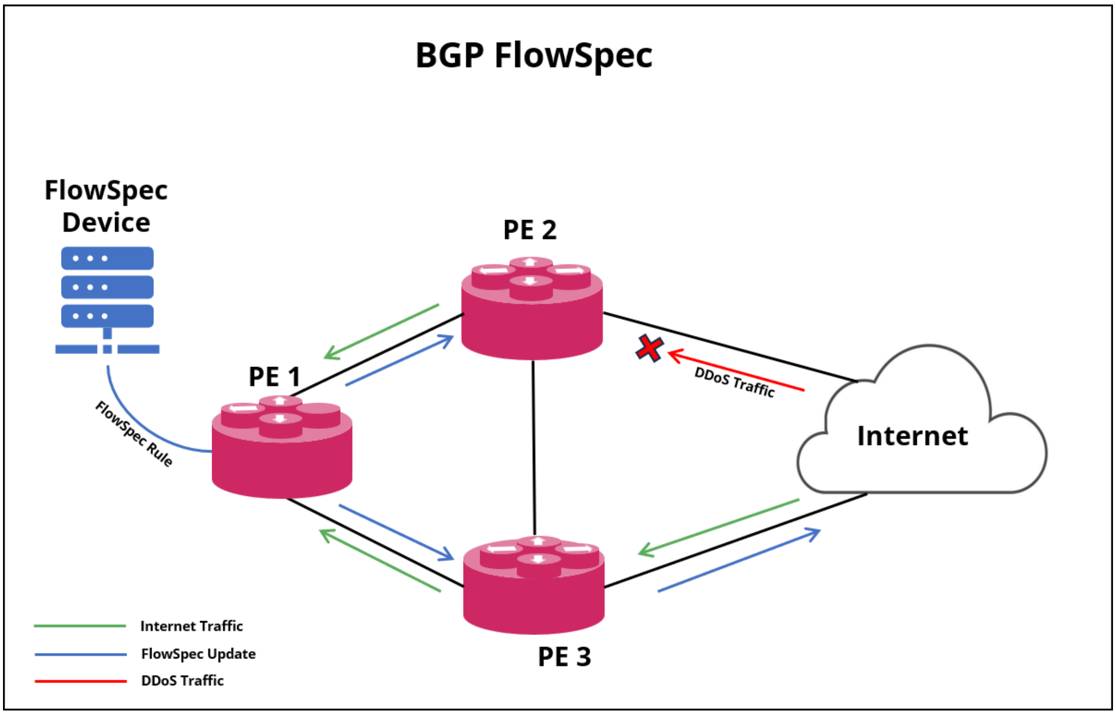
- • Stronger Message Authentication Codes (MACs)
- • Better protection against replays for the long-lived TCP sessions common between routers
- • A framework for the relationship between TCP authentication and security in general

TCP-AO is compatible with the use of TCP MD5 and it adds a layer of authentication that prevents spoofing attacks.

BGP Flow Spec: The Force Shield

BGP FlowSpec is an extension of the BGP protocol that allows for the dynamic propagation of more specific information than the traffic aggregate defined by an IP Prefix. This enables network administrators to control data traffic flow at any point in their network infrastructure. BGP FlowSpec can be used for various purposes, such as managing congestion or mitigating distributed denial-of-service (DDoS) attacks. Expanding routing information with FlowSpec allows the routing system to use the ACL (Access Control List) or firewall capabilities in the router's forwarding path.

The figure below shows a traffic scrubbing station capable of generating the FlowSpec rule in the event of a DDoS attack and sending the BGP FlowSpec update to the neighbouring devices. The device that can interpret this update can drop the DDoS traffic as it arrives.



FlowSpec helps to establish matching criteria for IP traffic packets encoded into BGP Network Layer Reachability Information (NLRI). The requirements can include various attributes and may or may not involve reachability information. Routers can use FlowSpec to forward, shape, classify, rate limit, filter, or redirect packets based on specific policies, allowing for rules that operate on multiple fields of the packet header.

BGP-GTSM: The body guard

BGP Generalized TTL Security Mechanism (GTSM) protects a BGP session by evaluating the Time to Live (TTL) value contained in the IP header of incoming BGP packets. TTL security is enabled using the ttl-security command on a single-hop BGP session. When TTL security is enabled on a BGP session the IP TTL values in packets is set to 255. To enable TTL security on a multihop BGP session, enable ttl-security and configure ttl-limit to match the expected TTL value.

Enabling Iron-clad Security without a Gold-Plated Price Tag

The good news is that Rtbrick Full Stack (RBFS) supports the Full Suite of BGP Security features providing a digital identity passport via RPKI, TCP-AO based secret handshake, BGP Flow Spec support for a force shield protecting the networks against DDoS attacks and finally GTSM as a body guard that protects the CPU.

Even better, RBFS runs on open switch hardware, so that operators can benefit from the cost effectiveness of merchant silicon without sacrificing carrier-grade performance, and still have a suite of contemporary BGP Security features. Automated RPKI and other enhancements ensure robust security in the edge and peering and enhance 'Sleep' at night factor. All of these features thus enable iron-clad security but without a gold-plated price tag.

Find Out More

Why don't you get in touch with us to find out more about how disaggregated networks could improve your backbone security?

RtBrick is replacing legacy network infrastructure with its Multiservice Edge Routing Software, a cloud-native Network Operating System that disaggregates traditional telco routing functions and runs on open switch hardware. RtBrick ends the vendor lock-in that comes with monolithic chassis-based systems, bringing operators significant cost savings, greater choice and ease of automation. RtBrick is a privately held company headquartered in California, with additional locations in Europe, India, and Taiwan.