TCP Maintenance and Minor Extensions (TCPM)
Internet-Draft
Intended status: Informational
Expires: 4 April 2026

K.W. Bedford
Juniper Networks

1 October 2025

Applicability of TCP-AO for Securing NETCONF and gNMI
draft-bedford-tcpm-ao-for-gnmi-netconf-00

Abstract

This document analyzes the applicability of the TCP Authentication Option (TCP-AO) to secure TCP-based network management protocols, specifically NETCONF and gNMI. It describes deployment profiles in which TCP-AO provides per-connection integrity and peer authentication with low operational overhead, either as an alternative to or in combination with TLS/SSH. This document gives guidance on key management (e.g., static keys and operational "key chains") and documents expected behaviors and benefits. No new protocol bits are defined and there are no IANA actions.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 April 2026.

Copyright Notice

Table of Contents

1. Introduction and Motivation

The TCP Authentication Option (TCP-AO) [RFC5925] provides connection-oriented integrity and peer authentication for TCP segments with cryptographic agility [RFC5926]. TCP-AO has seen deployment primarily with routing/control protocols; however, its applicability to network management and telemetry protocols is under-documented.

This document specifies practical applicability guidance for using TCP-AO with two widely used TCP-based management protocols: NETCONF [RFC6241] (commonly over SSH [RFC6242] or TLS [RFC7589]) and gNMI (as specified by the OpenConfig community, see [OC-GNMI]). TCP-AO can be used: (a) as a lightweight hop-by-hop integrity mechanism when TLS/SSH are operationally impractical; or (b) in defense-in-depth alongside TLS/SSH to harden the TCP substrate against spoofed resets and option tampering.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. TCP-AO Recap

TCP-AO (TCP option kind 29; see TCP specification [RFC9293]) protects selected TCP header fields, options, and payload using per-connection traffic keys derived from a Master Key Tuple (MKT). It supports algorithm agility and hitless rekey via KeyIDs, as specified in [RFC5925] and [RFC5926]. TCP-AO provides integrity and peer authentication only; it does not provide confidentiality. When confidentiality is required, it SHOULD be used in combination with an encryption mechanism such as TLS.

4. Limitations of Existing Solutions (TLS/SSH and IPsec)

TLS/SSH:

* Provide end-to-end confidentiality and rich authentication, but require PKI, certificate lifecycle management, and consistent trust-store operations across heterogeneous fleets.

* Do not protect the underlying TCP control plane itself against certain transport-level disruptions (e.g., off-path resets or option tampering on unencrypted segments prior to keying).

IPsec:

* Offers strong security properties but introduces per-SA policy management, NAT traversal considerations, and often coarser granularity (per-host/per-subnet) than operators desire for per-connection management channels.

In contrast, TCP-AO offers a lightweight, hop-by-hop protection model with explicit per-connection association and zero-loss rekey semantics.

5. Applicability to NETCONF

NETCONF servers typically listen on TCP port 830 (SSH) or use TLS per [RFC7589]. Operators MAY deploy TCP-AO to protect the underlying TCP transport for NETCONF sessions when:

* TLS/SSH are unavailable or impractical (e.g., brownfield devices lacking PKI support), OR

* Additional hardening of the TCP substrate is desired in defense-in-depth.

Guidance:

* AO policies SHOULD be enforced only between authorized client and server peers (e.g., NMS subnets).

* Operators SHOULD configure overlapping MKTs (key chains) to enable predictable, hitless rekeys for long-lived sessions.

* Where confidentiality is required, AO SHOULD be combined with TLS/SSH; AO by itself does not encrypt management content.

6. Applicability to gNMI

gNMI commonly runs over TCP with gRPC and often with TLS. Streaming telemetry subscriptions can be long-lived and bandwidth-efficient, but the control channel remains sensitive to spoofed resets and tampering on the TCP path.

Guidance:

* AO MAY be applied beneath gNMI (with or without TLS) to provide hop-by-hop transport integrity and to resist TCP control-plane disruption.

* When TLS is used for confidentiality/authentication, AO provides additional assurance that TCP segments (including control flags and negotiated options) are authenticated.

7. Key Management and Deployment

Static keys vs. dynamic keys:

* Operators MAY deploy static MKTs (pre-shared keys) at moderate scale. To avoid outages during rotation, operators SHOULD use key chains with overlapping lifetimes and planned KeyID transitions.

* TCP-AO does not define in-band key management; dynamic keying occurs out-of-band. Existing automation systems (e.g., via NETCONF/TLS or gNMI/TLS) MAY distribute and rotate MKTs securely.

Algorithm selection:

* Implementations MUST follow [RFC5926] for required MACs/KDFs. Operators SHOULD prefer modern, efficient MACs consistent with implementation guidance.

Deployment notes:

* TCP-AO is not compatible with address/port translation; the peers' IP addresses and ports are part of the authenticated context.

* TCP-AO slightly reduces available MSS due to option bytes; PMTUD SHOULD be verified on management paths.

8. Security Considerations

TCP-AO provides integrity and peer authentication at the transport layer and mitigates off-path spoofing, forged resets, and tampering with protected TCP options and payload. It does not provide confidentiality; when secrecy is required, AO SHOULD be combined with TLS. Key hygiene is critical: per-peer unique MKTs SHOULD be used, rotated regularly, and tracked operationally. Algorithm agility as defined in [RFC5926] SHOULD be maintained.

9. IANA Considerations

This document has no IANA actions.

10. Appendix A. Non-Normative Notes and Examples

* Example policy: require AO on TCP/830 (NETCONF) and the gNMI port from NMS subnets; maintain two MKTs with 24-hour overlap for monthly rotations.

* Lab validation: capture AO presence with a packet analyzer (TCP option kind 29) and test negative cases (wrong KeyID, wrong MAC) to verify expected failures.

11. Acknowledgments

The author thanks reviewers and operators who provided early feedback on applicability and deployment considerations.

12. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option", RFC 5926, June 2010, <https://www.rfc-editor.org/info/rfc5926>.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC7589] Badra, M. and J. Schoenwaelder, "Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication", RFC 7589, April 2015, <https://www.rfc-editor.org/info/rfc7589>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9293] Eddy, W., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, August 2022, <https://www.rfc-editor.org/info/rfc9293>.

13. Informative References

[OC-GNMI] Group, O. W., "gNMI Specification", GitHub repository, 2025, <https://github.com/openconfig/gnmi>.

Author’s Address

Kenneth Wignarajah Bedford
Juniper Networks
Basingstoke
United Kingdom
Email: kbedford@juniper.net