Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 5 May 2026

Q. Yuan
J. Mao
B. Liu
N. Geng
X. Shang
Q. Gao
Z. Li
Huawei Technologies
1 November 2025

Use cases of the AI Network Security Agent
draft-yuan-rtgwg-security-agent-usecase-00

Abstract

Core network devices like routers fulfill dual roles of data forwarding and security protection. However, escalating threats (e.g., zero-day vulnerabilities, DDoS attacks) expose limitations of traditional security— relying on static ACLs, signature-based detection, and manual configuration— causing delayed responses, high false positives, and protection gaps. This paper proposes AI Network Security Agents: intelligent software components leveraging machine learning, behavioral analysis, and real-time data fusion, with three core capabilities (adaptive learning, automation, distributed collaboration) to shift security from passive to intelligent. Four key scenarios are outlined: dynamic defense against unknown threats via baselines and tracing; ACL optimization via intent parsing; configuration security via baseline checks and simulation; and collaborative defense via intelligence aggregation and linked responses. AI Agents turn routers into active security orchestrators, enhancing threat protection and operational efficiency.

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 5 May 2026.

Table of Contents

1. Introduction

Routers and other core network devices serve as the foundational backbone of modern digital infrastructures, responsible for both data forwarding across network segments and the critical security functions of protecting traffic integrity, confidentiality, and availability. However, the escalating sophistication of cyber threats—ranging from stealthy zero-day exploits and large-scale DDoS assaults to persistent APT infiltrations—has exposed inherent limitations in traditional network security mechanisms. Dependent on static access control lists (ACLs), signature-based threat detection, and manual configuration workflows, legacy systems lack the agility to keep pace with dynamic threat landscapes, often leading to delayed threat responses, high false-positive rates, and unavoidable protection gaps. This document explores how integrating AI Agents into network devices addresses these limitations, transforming passive defense into an intelligent, adaptive security framework.

2. Requirements Language

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 RFC 2119[RFC2119].

3. Usage Scenarios of the AI Network Security Agent

After integrating AI Agents into network devices, their core security capabilities are upgraded from passive defense to an intelligent, adaptive protection system. Below are the key usage scenarios, elaborated with technical details and practical use cases:

3.1. Dynamic Defense Against Zero-Day Vulnerabilities and Unknown Threats

Traditional signature-based detection fails to address zero-day Vulnerabilities (e.g., new APT campaigns). AI Agents enable real-time threat identification and mitigation through behavioral analytics and adaptive learning:

3.1.1. Behavioral Pattern Recognition

Embedded AI Agents in network devices can analyze system calls, network traffic features, and file operations to establish a "normal behavior baseline." For instance, if a device suddenly sends encrypted data to multiple unknown IPs (a sign of data exfiltration), the AI Agent triggers isolation within minutes to prevent lateral spread.

3.1.2. Attack Chain Tracing

Leveraging knowledge graphs, AI Agents can correlate multi-source logs (Syslog, traffic logs) to map attack paths. For example, during a supply chain attack, the agent can identify abnormal ARP requests and failed SSH logins in device logs, pinpoint the attack pivot, and block further infiltration.

3.1.3. Zero-Day Vulnerability Prediction

Trained on historical vulnerability data and code features, AI Agents can forecast potential attack surfaces. For example, they scan device configurations to flag weak passwords or unclosed high-risk ports, generating actionable risk reports.

3.2. Dynamic ACL Rule Optimization and Intelligent Policy Management

Manual ACL configuration is error-prone and rigid. AI Agents automate policy creation and adjustment via intent-based parsing and reinforcement learning:

3.2.1. Policy Intent Translation

Users describe security requirements in natural language (e.g., "Block the Sales department from accessing finance servers"), and the AI Agent converts this into valid ACL rules.

3.2.2. Traffic Behavior Learning

AI Agents can continuously analyze network traffic to optimize ACL rules dynamically. For example, during peak video conference hours, the agent adjusts QoS policies to prioritize critical app bandwidth while identifying DDoS attacks disguised as video streams.

3.2.3. Policy Conflict Detection

Using knowledge graphs, AI Agents can real-time validate logical conflicts in ACL rules. If rules like "Allow all HTTP traffic" and "Block specific IPs" overlap, the agent flags the inconsistency and recommends priority adjustments.

3.3. Device Configuration Security

Manual configuration audits are inefficient. AI Agents boost network security via automated compliance checks and intelligent repairs:

3.3.1. Configuration Baseline Verification

AI Agents can use pre-defined security templates to scan device configurations, flagging risks like weak passwords or unencrypted management interfaces.

3.3.2. Configuration Change Validation

After a user submits a configuration change (e.g., modifying NAT policies), the AI Agent simulates post-deployment network behavior to verify functionality—ensuring internal devices can still access the public network—and generates a validation report.

3.4. Threat Intelligence Sharing and Global Collaborative Defense

Traditional security deployments operate in silos, limiting effectiveness against cross-network threats. AI Agents enable cross-device/vendor protection via multi-source data fusion and automated response orchestration:

3.4.1. Intelligence Aggregation

AI Agents integrate feeds from sources like CISA and VirusTotal to update threat signatures in real time. If a malicious IP is flagged as a phishing source by multiple feeds, the agent automatically adds blocking rules across all routers in the network.

3.4.2. Linked Attack Response

When one router detects an attack, the AI Agent notifies upstream/downstream devices for coordinated defense. For example, if a branch router detects an APT attack, the agent coordinates with the headquarters firewall to block the attack IP and alerts endpoint security tools for virus scans.

3.4.3. Security Posture Prediction

Using historical attack data and network topology, AI Agents forecast potential attack paths. If a network faces cross-VLAN infiltration risks, the agent pre-deploys access control policies on core routers to block lateral movement.

4. Conclusion

The integration of AI Agents into core network devices represents a pivotal advancement in network security, addressing the inherent inflexibility of traditional defense mechanisms. By enabling dynamic threat detection, intelligent policy management, automated configuration security, and collaborative defense, AI Agents transform routers from passive traffic handlers into proactive security orchestrators. These capabilities not only enhance protection against emerging threats like zero-day vulnerabilities but also streamline operational efficiency by reducing manual intervention. While challenges remain— such as optimizing AI model performance for resource-constrained devices and mitigating adversarial attacks— future developments in edge AI and self-healing algorithms will further strengthen this framework. Ultimately, AI-enhanced network security devices provide organizations with a resilient, scalable foundation to navigate the evolving cyber threat landscape, ensuring the reliability and security of critical digital infrastructures.

5. Security Considerations

TBD.

6. IANA Considerations

TBD.

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Quan Yuan
Huawei Technologies
Beijing
100095
China
Email: yuanquan25@huawei.com

Jianwei Mao
Huawei Technologies
Beijing
100095
China
Email: maojianwei@huawei.com

Bing Liu
Huawei Technologies
Beijing
100095
China
Email: leo.liubing@huawei.com

Nan Geng
Huawei Technologies
Beijing
100095
China
Email: gengnan@huawei.com

Xiaotong Shang
Huawei Technologies
Beijing
100095
China
Email: shangxiaotong@huawei.com

Qiangzhou Gao
Huawei Technologies
Beijing
100095
China
Email: gaoqiangzhou@huawei.com

Zhenbin
Huawei Technologies
Beijing
100095
China
Email: robinli314@163.com