ace
Internet-Draft
Intended status: Informational
Expires: 23 January 2026

B. Chen
OpenNHP

22 July 2025

Network infrastructure Hiding Protocol
draft-opennhp-ace-nhp-00

Abstract

The Network infrastructure Hiding Protocol (NHP) is a cryptography-based session-layer protocol designed to implement Zero Trust principles by rendering protected network resources invisible to unauthorized entities. By requiring authentication before connection and operating at OSI layers 5 , NHP conceals IP addresses, ports, and domains from exposure to reconnaissance and automated exploitation, effectively reducing the attack surface. This draft defines the architecture, message format, and workflow of the NHP protocol, outlines its security objectives, and provides guidance for integration into modern network infrastructures and Zero Trust deployments.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://OpenNHP.github.io/ietf-rfc-nhp/draft-opennhp-ace-nhp.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-opennhp-ace-nhp/.

Discussion of this document takes place on the WG Working Group mailing list (mailto:ace@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ace/. Subscribe at https://www.ietf.org/mailman/listinfo/ace/.

Source for this draft and an issue tracker can be found at https://github.com/OpenNHP/ietf-rfc-nhp.

Status of This Memo

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

Copyright Notice

Table of Contents

1. Introduction

Since its inception in the 1970s, the TCP/IP networking model has prioritized openness and interoperability, laying the foundation for the modern Internet. However, this design philosophy also exposes systems to reconnaissance and attack.

Today, the cyber threat landscape has been dramatically reshaped by the rise of AI-driven attacks, which bring unprecedented speed and scale to vulnerability discovery and exploitation. Automated tools continuously scan the global network space, identifying weaknesses in real-time. As a result, the Internet is evolving into a "Dark Forest," where *visibility equates to vulnerability*. In such an environment, any exposed service becomes an immediate target.

The Zero Trust model, which mandates continuous verification and eliminates implicit trust, has emerged as a modern approach to cybersecurity. Within this context, the Network infrastructure Hiding Protocol (NHP) offers a new architectural element: authenticated-before-connect access at the session layer. Inspired by Single-Packet Authorization (SPA) and Software Defined Perimeter (SDP) technologies, NHP advances the concept further by using cryptographic protocols (e.g., Noise, ECC) to obfuscate infrastructure and enforce granular access control.

This document outlines the motivations behind NHP, its design objectives, message structures, integration options, and security considerations for adoption within Zero Trust frameworks.

2. Conventions and Definitions

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.

NHP: Network infrastructure Hiding Protocol SPA: Single-Packet Authorization SDP: Software Defined Perimeter OSI: Open Systems Interconnection model ZTA: Zero Trust Architecture ECC: Elliptic Curve Cryptography

3. Security Considerations

NHP is explicitly designed to prevent unauthorized discovery of network resources. It implements multiple layers of cryptographic protection and enforces access controls before any TCP or TLS handshake occurs. As a result:

* The risk of port scanning and IP enumeration is significantly reduced.

* Mutual authentication is performed at the session layer using asymmetric cryptography.

* NHP packet headers are designed to be indistinguishable from random noise to unauthenticated entities.

Potential threats include cryptographic downgrade attacks, traffic analysis, or exploitation of weak authentication mechanisms. Therefore, implementations must:

* Use strong ECC keys (e.g., Curve25519) and modern AEAD ciphers.

* Implement replay protection and rate limiting.

* Follow best practices for key management and endpoint hardening.

4. IANA Considerations

This document has no IANA actions.

5. 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/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Acknowledgments

This work builds upon foundational research from the Cloud Security Alliance (CSA) (https://cloudsecurityalliance.org/) and benefits from the collaborative support of the China Computer Federation (CCF) (https://www.ccf.org.cn/en/). The authors would also like to thank the OpenNHP (https://github.com/OpenNHP/opennhp) open source community for their contributions, testing, and feedback on early implementations of the Network infrastructure Hiding Protocol (NHP).

Author’s Address

Benfeng Chen
OpenNHP
Email: benfeng@gmail.com