Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 30 August 2025

M. Chen
L. Su
China Mobile

26 February 2025

the service model of NASR
draft-chen-nasr-service-model-00

Abstract

This document describes the service model of Network Attestation for Secure foRwarding (NASR). It lists security capabilities and characteristics of connectivity services that operators can offer and clients can choose from.

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 30 August 2025.

Table of Contents

1. Introduction 2
2. Abbreviations 2
3. NASR service model 2
3.1. Service model from user 2
3.1.1. Source 3
3.1.2. Destination 3
3.1.3. Trusted Path Provision 3
3.2. service model to user 5
3.3. Service result model to user 5
3.4. Interaction process 5
4. IANA Considerations 6
5. Security Considerations 6
Authors' Addresses 7

1. Introduction

The NASR goal is to allow clients to choose desired security attributes of his received network service, achieving dependable forwarding by routing on top of only devices that satisfies certain security requirements. NASR then provides proof that packets or flows have traversed a network path with defined security properties.

The service model enables users to specify their security requirements. The network service provider translates these requirements into network configurations, which are then used to prepare the network for transmission. After delivering the service, the provider returns proof of compliance to the user.

2. Abbreviations

The following abbreviations are used in this document.

NVF: Network Functions Virtualization.

IDS: Intrusion Detection System.

IPS: Intrusion Prevention System.

PoT: Proof of Transit.

SLA: Service Level Expectation.

3. NASR service model

3.1. Service model from user

3.1.1. Source

Users can send requests for service creation, modification and deletion by specifying details such as destination, service type, and security requirements. For example, they define the destination IP, choose the type of service, and set security requirements like integrity, confidentiality, authentication and availability security features.

The parameters from Users to Providers may involve: source device ID (with unique identifier), service type, destination device ID, security provision, Trusted Path Provision, etc. The detailed parameters for destination and Trusted Path Provision are showed below.

3.1.2. Destination

Destination: Used to indicate the destination of the visit, such as IP address.

Path: a list of selected router ID list or IP addresses list on Path.

Sevice type: used to indicate the type of data, such as eMBB data, mMTC data or uRLLC data.

Geographic: used to indicate users’ requirements for geographic location or restrictions, a customer may request certain geographic limits are applied to how the provider routes traffic for the network forwarding, due to policy reasons or security considerations, For example, some countries have regulations that explicitly prohibit data from leaving the country. In such cases, customers may request certain geographic limits be applied to how the provider routes traffic for network forwarding.

3.1.3. Trusted Path Provision

ISPs can provide secure forwarding service by selecting a trusted path for users, including choosing trusted routers that can provide the security services required by the user;

The trusted path provision includes but is not limited to the following parameters.

Node Type: NFV or Hardware, this field is used to identify whether the node is of hardware type or virtualization software type, different node types have different security configurations.

Node Security Configuration: the node’s basic security configuration baseline possessed by the node(such as router) itself, include security hardening, attack perception and so on. The security configuration baseline is represented using vectors or sets.

for example:
+ Account management and authentication authorization
+ Password management
+ Access control
+ Service and Protocol Management
+ Log and Audit
+ System Security
+ Physical security
+ Data protection
+ ...

L2/L3 Security Feature: used to identify whether to enable authentication and encryption on L2 or L3. L2 authentication can be based on the device’s MAC address and encryption can use MACsec; L3 can provide end-to-end authentication and encryption, such as VPN. They can be configured through Boolean values.

for example:
+ L2 authentication: true
+ L2 encryption: false
+ L3 authentication: true
+ L3 encryption: false
+ ...

Connection Reliability Feature: Maximal occupancy level, Isolation, Diversity.<RFC 9543>. The maximal occupancy level specifies the number of flows to be admitted and optionally a maximum number of countable resource units (e.g., IP or MAC addresses). Isolation refers to the division of traffic , a customer may request that its traffic is isolated from the other network traffic supported by the same provider. Diversity allows connections based on different underlying network constructions.

Security Services Configuration: Security services that can be provided based on traffic, such as firewall,IDS/IPS,attack-mitigation(anti-DDos), access control, Integrity Protection. Each type of security service requires two SLE parameters, processing latency and performance of security capabilities.

for example:
+ Security service type: anti-ddos
+ processing latency: 2ms
+ performance of security capabilities: 40G
+ ...

3.2. service model to user

When users are very proficient in security configuration and requirements, they can directly fill in a fixed format list, the operator can provide feedback on whether the requirements are met; Users may not be security experts, they will propose vague security requirements, and the ISP generates one or more fixed format lists for users to choose from, there is an additional interaction process with the user here.

3.3. Service result model to user

Path attestation result: after generating a path that meets the specific forwarding requirements of the user, it is used to record the initial path attestation result as a baseline for future verification, contains at least four fields: Identity, initial attestation result, verification reference and auxiliary information (e.g., node type along the path, isolation, firewall, IDS/IPS, etc.).

Forwarding Path validation result: formed during the actual forwarding process both in-situ and out-of-band modes, it will be verified with path attestation result, contains at least two fields: Identity, attestation results and auxiliary information (e.g., node type along the path, isolation, firewall, IDS/IPS, etc.).

Service provision result: as security services can be provided, after the service is provided, need to provide service proof to the user, contains at least two fields: Identity, Service type, Service security details which may include satisfaction of data integrity, encryption mechanisms, authentication methods and availability percentage (for example, 99.999%), etc.

3.4. Interaction process

The service model is used between customers and networks, the customer sends security requirements to the ISP, and the network analyzes and selects the path based on the user’s security requirements, which are confirmed by the customer. The network orchestrator configures the network nodes and enables forwarding and service. After forwarding and service are completed, the proof of transit are fed back to the orchestrator, which generates a service result model and finally sends it to the customer.

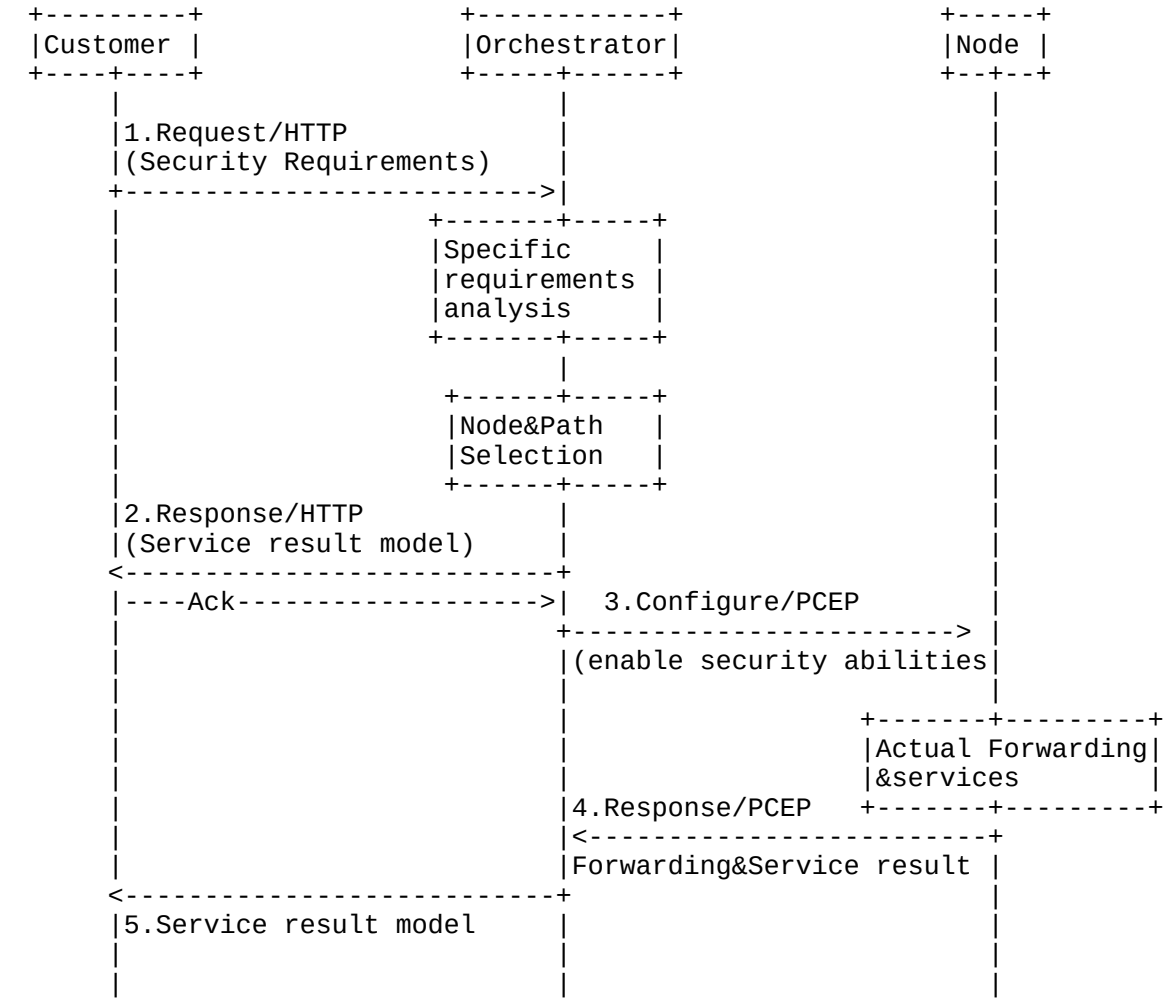

Figure1: Interaction diagram of service model

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

There is a risk of tampering for Path attestation result and Forwarding Path validation result, especially in the scenario of third-party auditing, it is required that both data transmission and storage cannot be tampered with.

Authors' Addresses

Meiling Chen
China Mobile
BeiJing
China
Email: chenmeiling@chinamobile.com

Li Su
China Mobile
BeiJing
China
Email: suli@chinamobile.com