ZPR's Concept of Identity

Danny Hillis, May 2025
(Updated May 19, 2025)

1. Identity

In Zero-trust Packet Routing (ZPR), an identity is a retrieval key that is used for looking up attributes, which are name/value pairs associated with the identity. The identity is associated with an individual endpoint, user or service.

Every endpoint, user or service in a ZPR network (ZPRnet) has an identity that is unique within the ZPRnet. User Identity is usually associated with username tied to credentials (e.g., passwords, tokens, certificates) and often managed via systems like LDAP or Active Directory. Device Identity is usually a device ID associated with a MAC address, certificate, or hardware identifier such as Trusted Platform Modules (TPMs). A Service Identity is associated with a service name, usually tied to the service by cryptographic certificates.

An identity may be associated with multiple names through attribute values, but these names should not be confused with the retrieval key that is the identity.

2. Endpoints

In ZPR, an endpoint is the device that implements the interface between ZPR protocols and standard IP protocols. The endpoint may be a virtual device (software adapter, vNIC), a physical interface device (adapter dongle, NIC) that connects to the ZPRnet or an entire host or client device (sever, desktop). The essential purpose of the ZPRnet is to enable endpoints to communicate when, and only when, such communication is authorized by policy.

It is only possible to treat the entire host or client as an endpoint if it presents a single ZPR interface to the ZPRnet. For systems with multiple ZPRnet interfaces, such as a server with several ZPRnet NICs, it is necessary to treat each interface as an endpoint.

There are always at least two endpoints involved in a packet flow. Each endpoint has an identity with associated attributes. Flows can be authorized based on attributes of either or both endpoints of the flow.

3. Users

A user is a person or authority that can be associated with a communication flow. Each user also has an identity and associated attributes, just like each endpoint. Flows can also be authorized based on attributes of the users involved in the flow.

Users can only be associated with a flow through an endpoint. An endpoint may have zero, one, or multiple users. In the case where the endpoint has one user, the endpoint's communication can be associated with that user. In the case where the endpoint has multiple users, the endpoint is sometimes able to associate a packet flow with a single user. If a single user cannot be associated with the flow, then no permissions that depend on user attributes will apply.

When a single user can be associated with a flow, ZPR can enforce policies based on the attributes of the source user and/or destination user. When no user can be associated with a flow, ZPR can only authorize the flow based on policies that do not depend on user attributes.

Users may use different names in different parts of the ZPRnet, but ZPR can be configured to map multiple names to the same user identity.

4. Services

Services in ZPR are applications that listen for communications packets and respond and/or act on them. Services may also initiate communication to other services. Services can have identities and associated attributes, and flows can be authorized based on attributes of any service with identity involved in the flow.

Flows can only be associated with a service through the endpoint. Typically, each service served by an endpoint has a list of port numbers as an attribute value, so the endpoint can determine which service is involved in the flow by examining the packets' port numbers.

Services may also have different names in different parts of the ZPRnet, and a ZPRnet can be configured to map these names to the same identity.

At the time the packet is transmitted or received, both the source and destination endpoints must be associated with an IP address. That address is an attribute value of the endpoint, but ZPR policies are not normally based on IP addresses.

5. Authentication of Identity

Conceptually, all authentication is accomplished by confirming the association of an identity with an endpoint, user, or service. How this is implemented will vary across implementations.

It's important to keep in mind that authenticating identity means not just authenticating that it is a valid identity but also authenticating that it is associated with the authorized packet flow. In the case of an endpoint, this means authenticating the physical or virtual device itself. In the case of a user or service, the association must be made through the endpoint.

The authentication also ensures that certain attribute values of the identity, known as identity attributes, match the attributes of the device, user, or service being authenticated. For example, an endpoint serial number might be an identity attribute of an endpoint.

Authentications of any user's identity association with a flow may require the endpoint to communicate with an identity service, or it may be established through biometric devices, card readers, or user responses to security challenges. ZPR can make use of multiple identity authentication services in the same ZPRnet. This is important for dealing with multiple clouds and customer locations where some identities are authenticated on different services than others.

Services will typically be authenticated by cryptographic certificates that prove the association of the identity of the service with the endpoint. The certificate includes or references the authorized port numbers as claims, allowing verification that the service is legitimately operating on its claimed ports. This creates a binding between the service identity, its endpoint, and the specific ports it uses.

6. Revision History

1. Revision as of May 19, 2025
   1.1 Eliminate any discussion of actors/agents.
   1.2 Call the devices endpoints.
   1.3 Allow entire system to be an endpoint.
   1.4 Clarify use of multiple authentication services.