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 key that can be used for looking up attribute values. It may have one or more names as attributes, but these names are not the identity. An identity may be associated with different names in different identity services, but one of the attributes is a canonical name that is used within the ZPRnet for logging.

In ZPR, all flows of communication packets must be permissioned to travel through the network based on attributes of the identities associated with the endpoints of the flow. Since identity is used to decide whether to allow a flow, the identity's association with the endpoint must be authenticated. After authentication, an identity is used to look up attribute values from the ZPRnet's trusted sources that store attributes as name/value pairs associated with the identity. The permission to communicate depends on these attribute values.

Every endpoint, device, user or service in a ZPRnet has an identity that is unique within the ZPRnet.

2. Devices

There are always at least two network-connected devices involved in a communication flow, the transmitter and the receiver. Each of these has an identity and associated attributes. They may be physical devices such a processor, adaptor dongle or network interface card, or virtual devices such a software adaptor or a VNIC.

Conceptually, all authentication is accomplished by associating an identity with a device. How this is actually implemented will vary across implementations.

Devices are associated with a newly created identity each time a ZPRnet is configured.

Physical devices will usually authenticate their identity through hardware security modules or Trusted Platform Modules (TPMs) in the device that stores serial numbers and cryptographic keys. Virtual devices will usually authenticate through the operating system. The authentication ensures that the authentication attributes of the device match the attributes of the device identity.

3. Endpoints

The conceptual communicator that transmits or receives a flow of communication packets is called an ***endpoint.*** Since each endpoint has a device, it is tempting to think of the endpoint as the device, but different endpoints may use the same device. For example, if multiple services are associated with a single server, the device that is the server may have a different endpoint for each service. So, endpoints can have multiple associated elements that are involved in a communication flow.

The endpoint has an identity. The endpoint has a real or virtual device that connects to the network. It may also have a user and/or a service that can be involved in the communication

flow. More specifically, the endpoint is a 4-tuple of the endpoint identity, the identity of a network-connected device that handles the endpoint's flows, an optional user identity, and an optional service identity. These four identities are called ***elements*** of the endpoint. Whenever a new packet flow is initiated, ZPR will look for existing endpoints with elements that match the flow. If such an endpoint does not already exist, it will create one with a new identity.

At the time the packet is transmitted or received, an endpoint must be associated with an IP address or an address/ports combination. That address is an attribute value of the endpoint's device. The port numbers, if any, share an attribute value of the endpoint's service.

4. 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 device.

Not all communication can be uniquely associated with a user. An endpoint device may have no user, one user, or many users. In the case where the endpoint has one user, the communication can be associated with that user. In the case where the endpoint has multiple users, the communication can sometimes be associated with the user that is controlling the process that is communicating.

ZPR Policy Language (ZPL) can express policy statements that allow communication based on the source user and/or destination user, based on the attributes of that user. It can also express policy statements that allow communication regardless of whether or not that communication is associated with a user.

Users may have different names in different parts of the ZPR network, and the ZPR configuration file can specify a trusted source for the correspondence between these names. User names may be assigned identities at configuration time, or when they first communicate. Whenever ZPR encounters a user name, it checks to see to see if it has already assigned an identity to that user, and if not, it creates one. Authentications of a user's association with a flow may require the endpoint's device to communicate with an identity service, or it may be established through biometric devices, card readers, or user responses to security challenges.

5. Services

Services in ZPR also have identities and associated attributes. A least one of these attributes is usually a list of port numbers through which communication with the service can be initiated.

A service is typically an application that responds to requests. Services may also make requests to other services and accept responses.

Services may also have different names in different parts of the ZPR network, and the ZPR configuration file can specify a trusted source for the correspondence between these names. Service names may be assigned identities at configuration time. Whenever ZPR encounters a service name, it checks to see if it has already assigned an identity to that service, and if not, it creates one.

Services will typically be authenticated by cryptographic certificates that prove the association of the identity of the service with the device and with any optional port numbers.

6. Authentication of Identity

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 endpoint's communication. ZPR authentication policies specify the required method of authentication.

ZPL can make use of multiple user identity services in the same ZPR network. This is important for dealing with multiple clouds and customer locations where uses of the different attribute values can be authenticated differently. For example, users may authenticate their identity differently on different parts of the same ZPRnet, and they may even use different user names in different parts of the network.

7. Recursive Identity Attributes

ZPR allows, but does not require, values of attributes to be identities that must be authenticated before they are used to look up attribute values. For example, user names, device names, and service names are authenticatable identities, and they may have attribute values that are also identities.

8. Revision History

1. Revision as of May 19, 2025
    a. Eliminate any discussion of actors/agents.
    b. Call the devices endpoints.
    c. Allow entire system to be an endpoint.
    d. Clarify use of multiple authentication services.
2. Revision as of August 2025
    a. Add headings Devices and Recursive Identity Attributes.