# Trust boundaries

Previously, you learned that perimeter protection refers to the security measures implemented at the edge of a network or system to defend against unauthorized access and cyber threats. You also learned that trust boundaries are vital because they define the network points where the trust level changes, like the transition from a trusted internal network to an untrusted external network.

In this reading, you'll first dive deeper into trust boundaries and learn how to identify them in an infrastructure. Then, you'll also learn how to use firewalls to control network traffic. Last, you'll learn some best practices to help effectively implement and maintain controls to enforce trust boundary rules.

## What are trust boundaries?

According to the U.S. National Institute of Standards and Technology, in the context of a cloud ecosystem, a trust boundary encompasses all resources and identifies a logical and dynamic border between the supporting subsystems and the cloud-based information system from the cloud consumer's perspective. The boundary is dynamic because it adapts to a cloud ecosystem's changes, like when resources are provisioned or decommissioned. It also adapts to changes made by data resting or securely traveling. For example, a boundary where data flows or passes between two different systems is usually a trust boundary.

## Identify trust boundaries throughout an infrastructure

To identify an infrastructure's trust boundaries, consider these recommendations:

- **Identify all of the assets in your infrastructure**, including hardware, software, data, and networks.
- **Classify your assets based on their sensitivity and criticality** to help you prioritize your trust boundary efforts.
- **Chart all of the ways that your assets interact with each other,** including data flows, network traffic, and user access.
- **Locate any points in the interaction between your assets where the level of trust changes;** these are your trust boundaries.

Examples of assets with trust boundaries in an infrastructure can include:

- The public internet and your internal network
- Different security zones within your internal network, like the development zone, the

testing zone, and the production zone
- Different applications or services
- Different users or groups of users
- Different operating systems or hardware platforms

## Firewalls can control network traffic in the cloud

Most cloud providers have firewall systems that enable you to control inbound and outbound traffic. You can set your network to let your virtual machine (VM) instances make outgoing requests and receive established responses by using egress rules. You can allow all protocols and ports, or restrict your traffic to only the ports and protocols that meet your needs. This helps ensure only the traffic you need has access to get through to your network. Restricting traffic follows the principle of least privilege, which helps to reduce the risk of unauthorized access.

### VPC Firewall Rules

Virtual private cloud (VPC) firewall rules let you deny or allow connections to or from VM instances in your VPC network. VPC firewall rules that you enable are enforced, and help protect your VM instances regardless of their operating system and configuration.

## Best practices to enforce trust boundary rules

Once you've identified your trust boundaries, you can start to implement and maintain controls to enforce your policies. Some best practices are to:

- **Enforce firewall rules for your VPCs**, allowing only the specific traffic you need.
    - Use firewalls and other network security devices to control traffic between different trust zones.
    - Set the rules that limit traffic to just the protocols and ports you allow.
- **Implement least privilege access with strong authentication and authorization rules,** so that users and applications only have the access they need.
    - With hierarchical firewall policies in place, you can define rules on an organizational or folder level that apply to lower levels of the resource hierarchy.
    - Use service accounts in regular VPC firewall rules—which are rules you define at the network level and apply to all instances in the network—by specifying the service account in the source or destination filter of the firewall rule.
        - This will enable you to control network access based on the identity of the application or instance, instead of just the IP address. A couple of rule examples are restricting access and specifying only service accounts that can access specific VMs on your network.
    - **Keep rules based on IP addresses to a minimum.** It's easier to track a single rule that allows traffic to a range of 16 virtual machines than to track 16 separate rules.
- **Monitor your infrastructure for suspicious activity** and respond promptly to any incidents.

## Key takeaways

As a cloud security professional, you'll use trust boundaries to help protect your cloud infrastructure as a measure to a more secure and stable digital future.

You'll also use cloud firewalls to help protect your cloud infrastructure's boundaries by specifying what network traffic can enter your cloud environment. This will enable you to control traffic in and out of your network's boundaries.