Usage of Proxies in Building Rules For Policies in Multicloud Defense

First Published: 2025-12-08

Usage of Proxies in Building Rules For Policies

Is This Document For You?

This document is intended for customers, security architects, and administrators who are new to the concept of building policies in Multicloud Defense. If you need to understand how to select and use proxies effectively to write security rules and policies, this document will help you navigate the concepts, scenarios, and related workflows.

Overview of Proxy and Proxy Types

There are mainly two proxies used in Multicloud Defense.

- Forward Proxy: A client is in your environment and initiates a connection to the server. This is an egress or east-west scenario. This proxy is positioned between the client and the server. This proxy is used for inspecting any outbound traffic. The are different types of forward proxies used in Multicloud Defense which are explained later in this section.
- Reverse Proxy: A client is outside your environment (in the Internet) and the server is within your environment, and you are protecting your server. This proxy is positioned in between your servers and the client, and is proxying the client requests to your backend servers. This proxy is used for inspecting any inbound traffic.

Forward proxies are further categorized into many types:

- Application Proxy (Layer 7): This proxy type handles HTTP/HTTPS/WebSocket traffic. It is specific to Layer 7 applications. It can inspect HTTP headers and content. The primary types of application proxies are:
  - WebSocket Forward Proxy – Handles WebSocket connections that are bi-directional communication channels such as gaming, chats, collaboration applications. Offers security for real-time applications.
  - HTTP Forward Proxy – Handles HTTP and HTTPS traffic. Suitable for web browsing and offers features such as filtering, caching, and anonymity.
- TLS Proxy: This proxy is used for TLS activation where this proxy is used to negotiate TLS.
- TCP Proxy (Layer 4): This proxy type handles only TCP/UDP traffic, forwards data without inspecting application content.

Guidelines For Usage of Proxies in Building Rules

The general guideline is to use proxies when you need to decrypt the traffic. It helps investigate for signature matches, deep packet inspection and more.

Use Cases For Proxies in Building Rules For Policies

Primarily, if you have more information on the traffic that you need to protect, it makes it easier to know which proxy to use. Here is a list of use cases for ideal usage of proxies along with reasons for use.

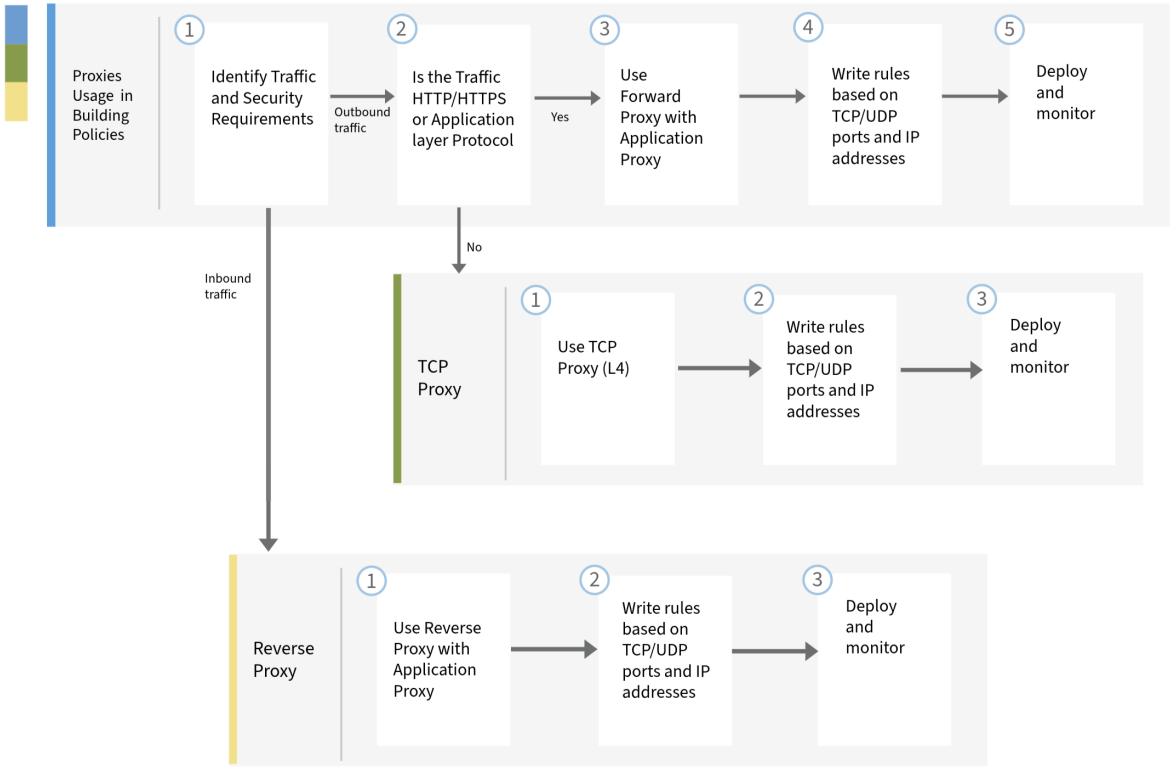
Table 1: Use Cases For Proxy Roles and Proxy Types

Use Case	Proxy Role	Proxy Type	Reason
HTTP/HTTPS traffic (web browsing, APIs)	Forward Proxy	Application Proxy (L7)	Enables deep inspection, URL filtering, and advanced security features for outbound web traffic.
WebSocket (bi-directional communication - chat, gaming, collaboration)	Forward Proxy	Application Proxy (L7)	Handles WebSocket handshake. Low latency, data exchange. Enables security, anonymity and content filtering.
TLS (corporate networks - detect malware, DDoS attacks, control website access and more)	Forward Proxy	Forward Proxy	Handles TLS handshake. Protects by inspecting encrypted traffic for security threats and protects using network policies.
Inbound web traffic to internal servers	Reverse Proxy	Application Proxy (L7)	Protects internal servers by inspecting and controlling inbound HTTP/HTTPS traffic.
Non-HTTP TCP/UDP traffic (database, mail)	Forward Proxy	TCP	Provides efficient Layer 4 inspection for non-HTTP protocols without full application-layer parsing.
Internal service-to-service communication	Forward Proxy	TCP	Low latency, high throughput inspection for internal TCP/UDP traffic.

Use Case	Proxy Role	Proxy Type	Reason
Advanced security policy requiring deep packet inspection	Forward Proxy	Application Proxy (L7)	Needed for granular security controls, threat detection, and protocol validation.
Simple L4 policy for allowing or blocking ports	Forward Proxy	TCP	Lightweight policy enforcement based on ports and IPs without deep inspection.

Workflow For Usage of Proxies in Building Rules For Policies

This workflow helps you identify the proxies to use, whether it is for inbound traffic or outbound traffic. Based on the traffic, you can determine the proxies that you need to choose to build your rules for policies.



Configure Proxies For Building Rules For Policies

Configure and set up your proxies for building rules for policies as shown here.

Procedure

Step 1 Identify your traffic and security requirements.

Step 2 If the traffic is outbound, check if the traffic is on HTTP/HTTPS or Application-layer Protocol.

a) If yes, use Forward Proxy with Application Proxy.
b) If no, use TCP Forward Proxy (L4).
c) Write rules based on TCP/UDP ports and IP addresses.
d) Deploy and monitor the traffic.

Step 3 If the traffic is inbound, use Reverse Proxy with Application Proxy.

a) Write rules based on TCP/UDP ports and IP addresses.
b) Deploy and monitor the traffic.

Troubleshooting For Proxies in Building Rules For Policies

Summary

Here are some common issues and ways to address them:

- If the traffic is not inspected as expected, verify that the proxy type selection matches the traffic type.
- Check the rule order and specificity to avoid conflicts.
- Confirm that advanced security profiles are attached only to supported proxy types.
- Review logs for errors or dropped packets that can indicate misconfiguration.

For support, contact Cisco Technical Assistance Center.

Additional Resources For Usage of Proxies in Building Rules For Policies

To know more about proxies and how you can use them in Multicloud Defense, here are a list of references:

- Create a Rule in a Ruleset in the Cisco Multicloud Defense User Guide
- Proxies in Multicloud Defense