AWS Web Application Firewall (WAF)

Table of Contents

AWS Web Application Firewall (WAF)

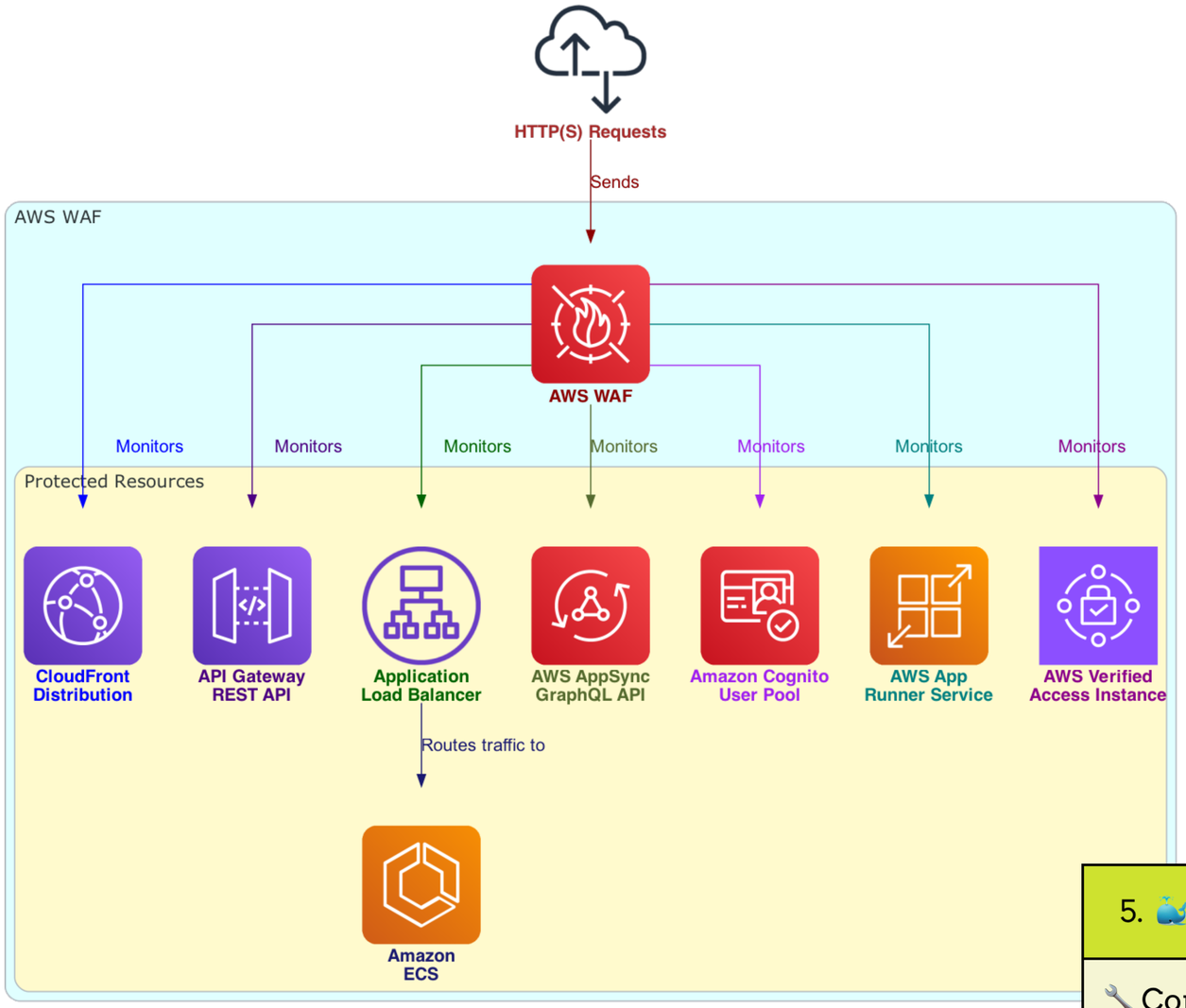
What is AWS Web Application Firewall (WAF)?

1. 🔍 Monitors HTTP(S) requests to protected resources

- 🌉 Web application firewall
- 🔒 Ensures security

2. 🌐 Supports 7 resource types

- ☁️ CloudFront distributions
- 🚏 API Gateway REST APIs
- ⚖️ Application Load Balancers
- 🕸️ AppSync GraphQL APIs
- 👥 Cognito user pools
- 🏃 App Runner services
- ✅ Verified Access instances



3. 🔑 Controls access to content

- 📋 Based on specified criteria
- 🌎 IP addresses
- 🔍 Query string values
- 🎛️ Granular control

4. 🚫 Responds with

- 📄 Requested content
- ⛔ HTTP 403 status code
- 🛠️ Custom response
- 🔒 Appropriate access control

5. 🐳 Protects applications hosted in ECS containers

- 🔧 Configure ECS with ALB + WAF
- 🚦 Routes, protects HTTP(S) layer 7 traffic
- 📦 Across tasks in service

How AWS WAF Works

1. 📝 Define a web access control list (ACL)

📜 Specifies rules and actions

🌐 Handles incoming HTTP(S) requests

2. 🔗 Associate ACL with web application resources

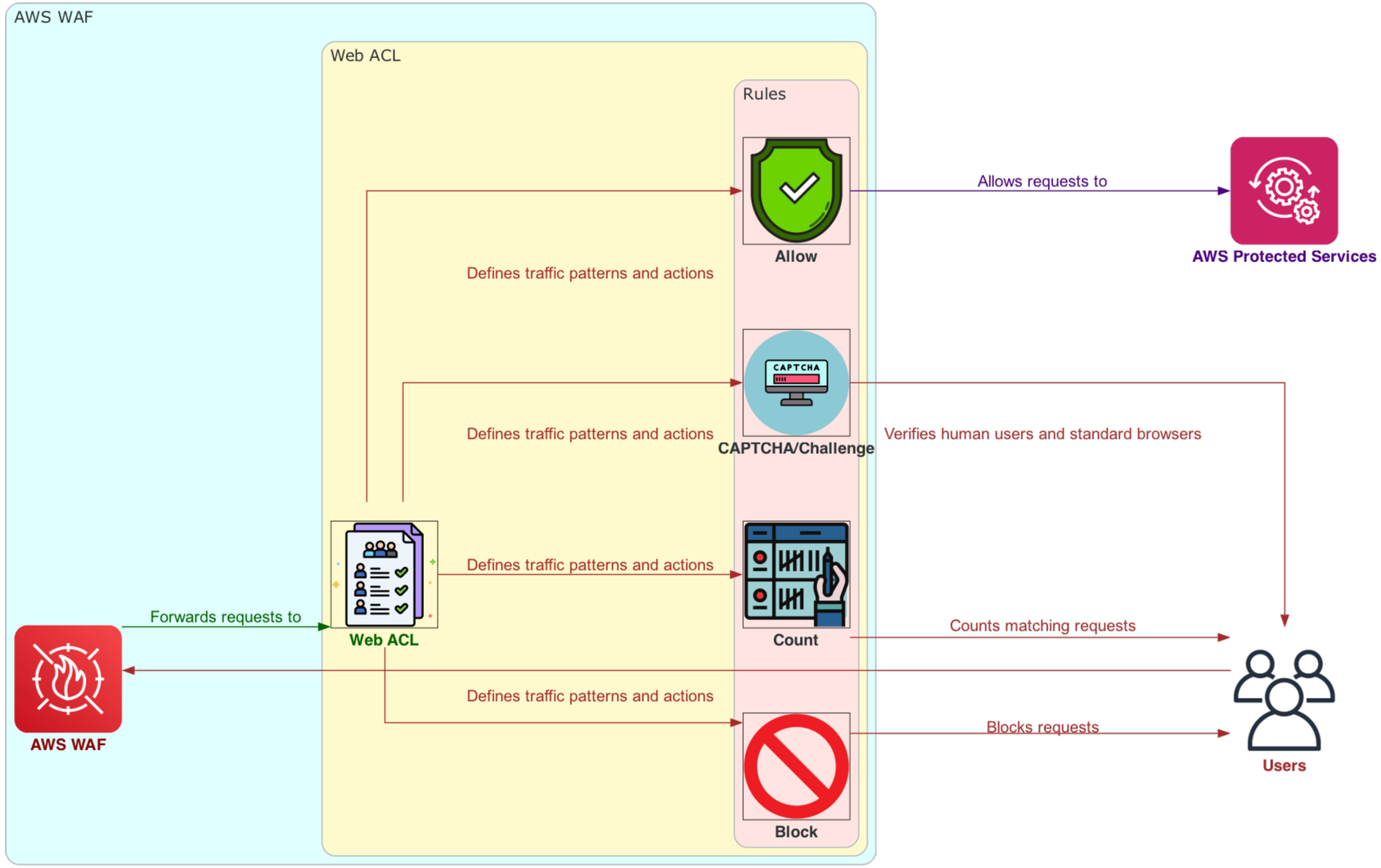
☁️ CloudFront distributions

⚖️ Application Load Balancers

3. 🔍 Inspect incoming requests using web ACL

🔁 Resources forward requests to WAF

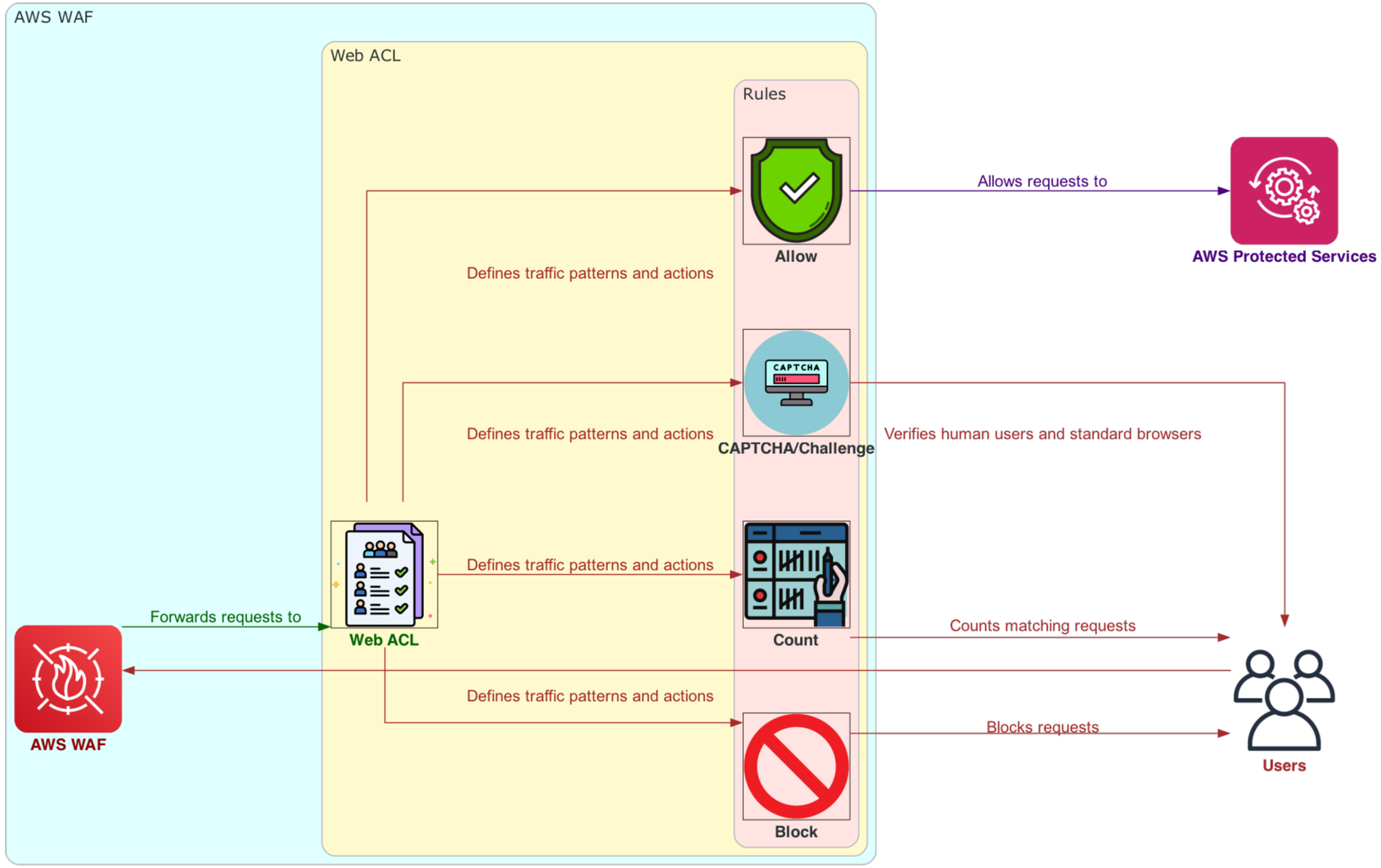
🕵️ WAF examines requests based on ACL rules



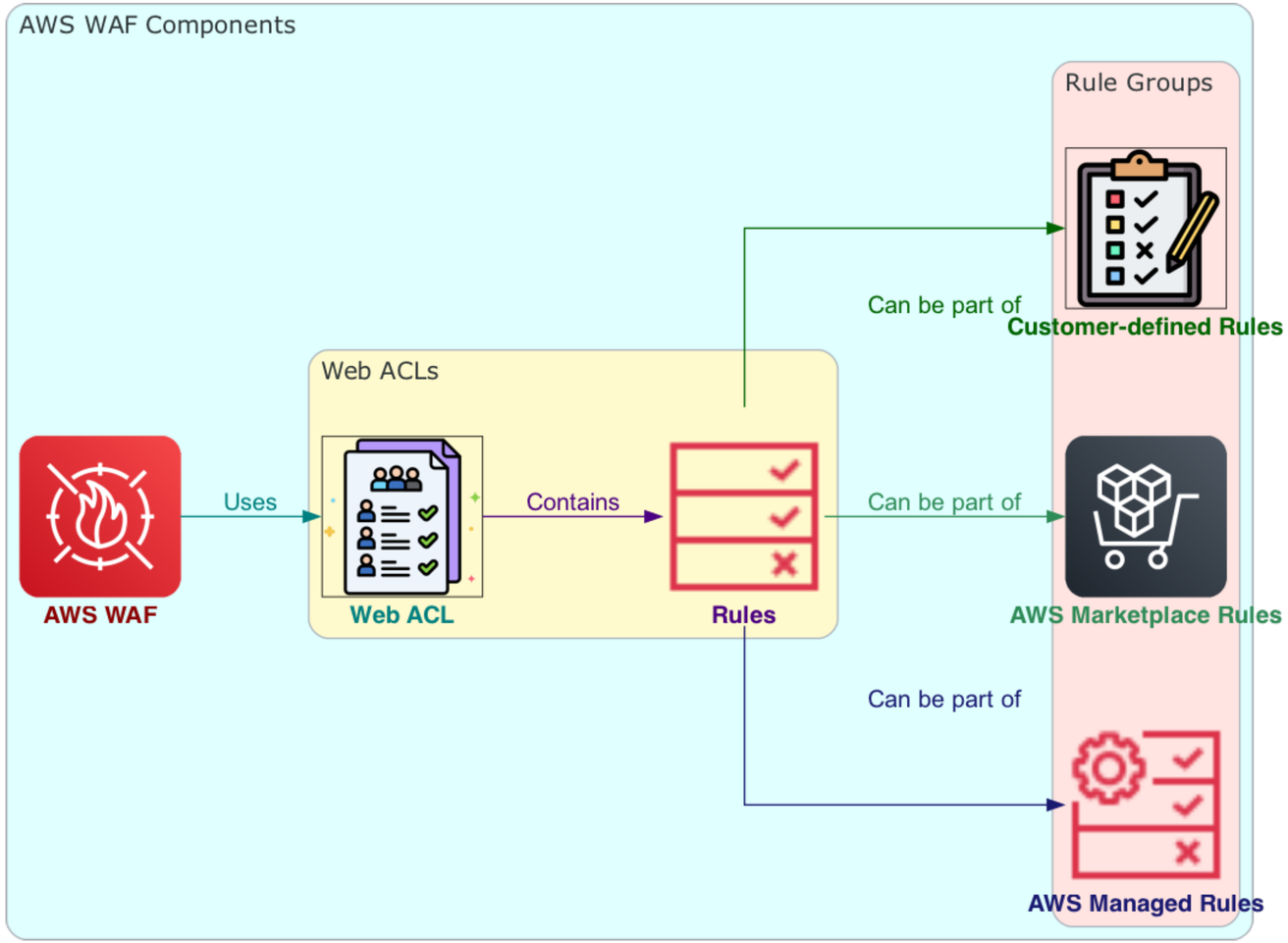
How AWS WAF Works

4. 📋 Create rules to define traffic patterns
🎯 Identify malicious or unwanted traffic

5. 🎯 Specify actions for matching requests	
✅ Allow	👍 Proceed to protected resource
🚫 Block	⛔ Prevent reaching protected resource
🔢 Count	📈 Track matching requests
	🚷 No additional action
🤖 Run CAPTCHA/challenge checks	🧩 Verify human users
	🖥️ Standard browser use
	🔒 Prevent automated attacks



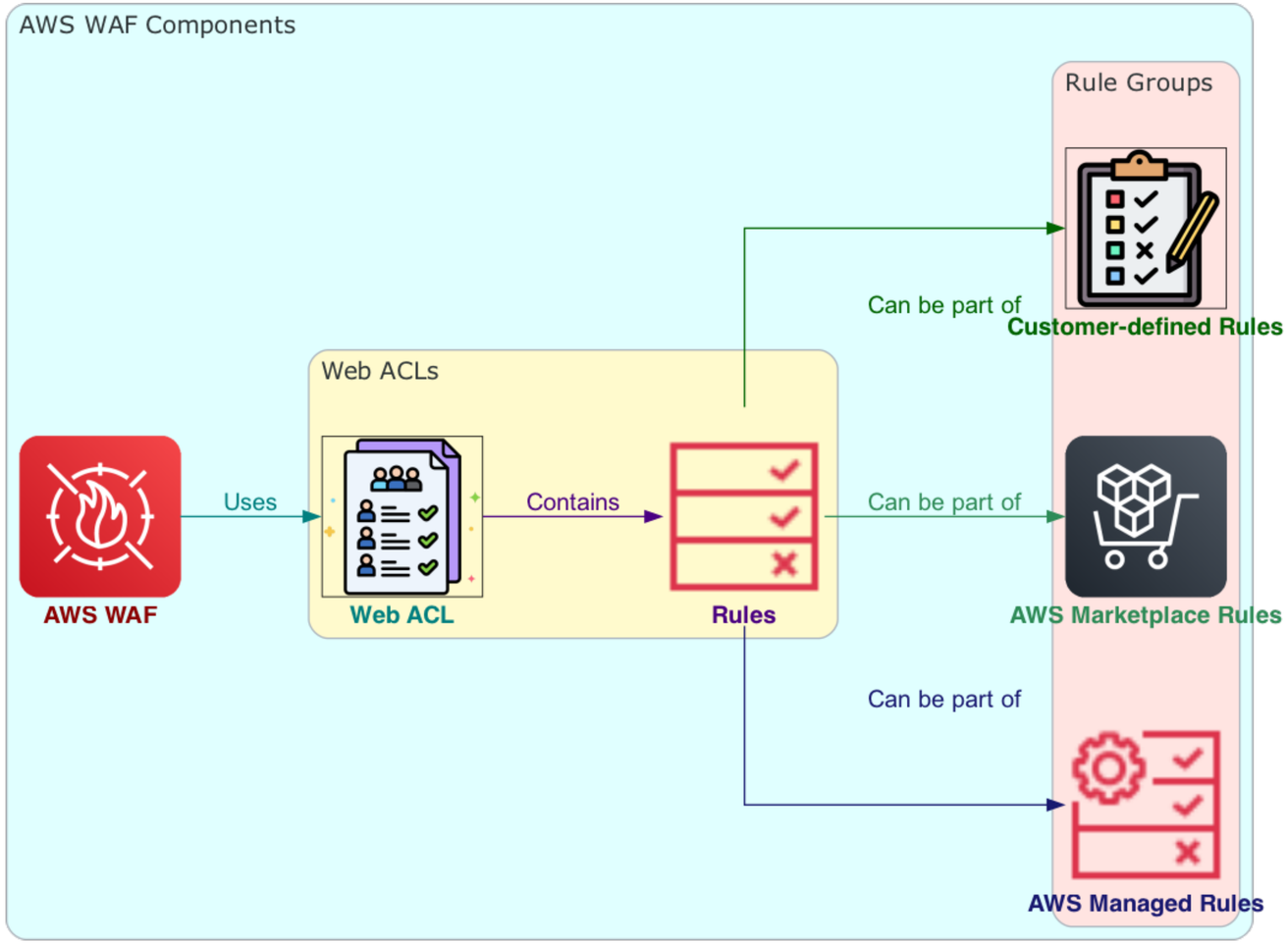
AWS WAF Components



1. 🛡️ Web ACLs	
🌐 Protect AWS resources	
📝 Define protection strategy	🧩 Add rules
🎯 Set default action	⛔ Block requests
	✅ Allow requests

2. 🔪 Rules		
📜 Contain statement	🔍 Define inspection criteria	
	🎬 Specify action on match	
⚖️ Configure actions	🚫 Block matching requests	
	👍 Allow matching requests	
	🔢 Count matching requests	
	🤖 Run bot controls	🧩 CAPTCHA puzzles
		🕵️ Silent client browser challenges

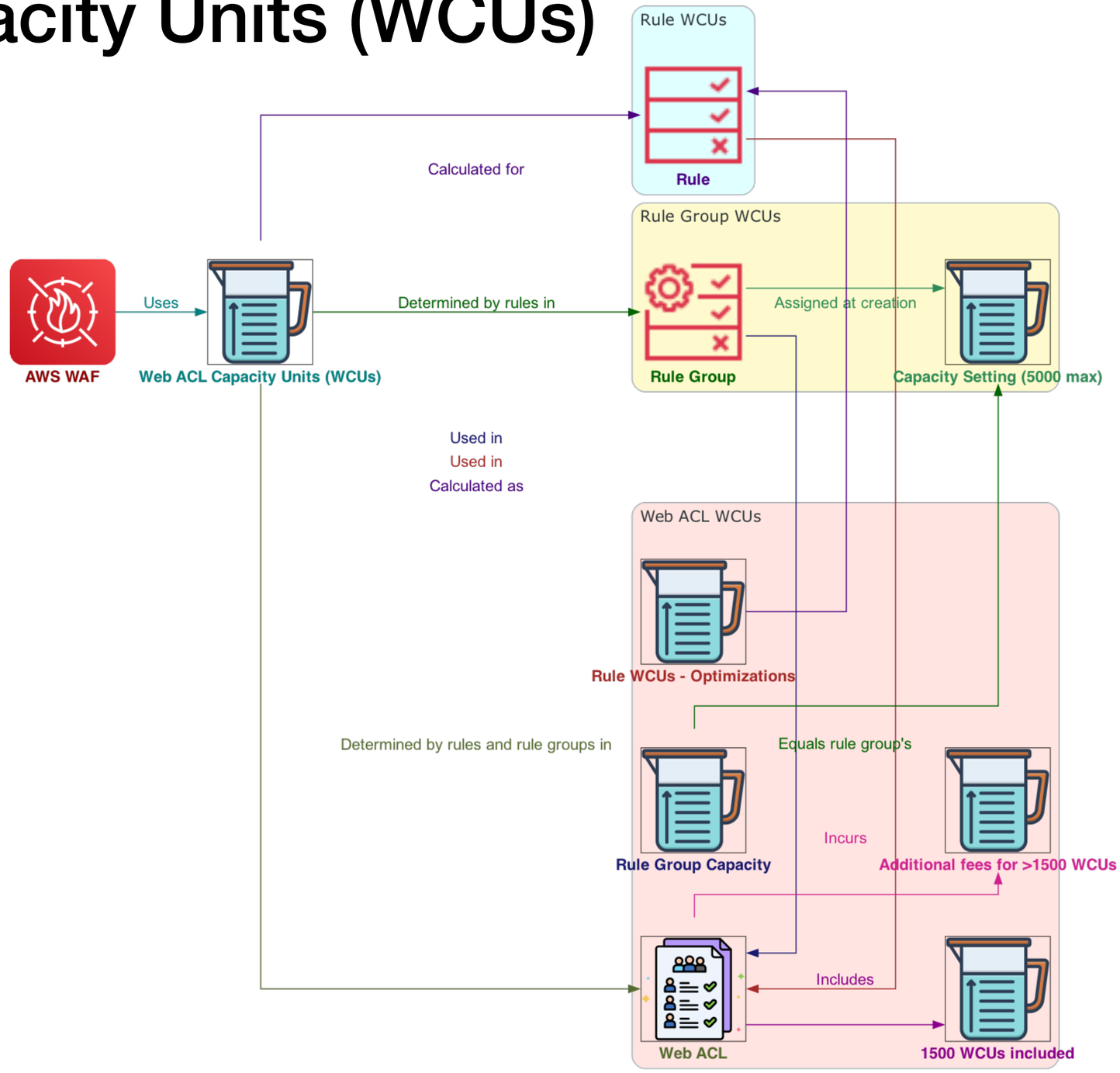
AWS WAF Components



3. 🗂️ Rule Groups	
📝 Define rules	🌐 Directly in Web ACL
	♻️ In reusable rule groups
🏷️ Managed rule groups	🅰️ AWS Managed Rules
	🛒 AWS Marketplace sellers
🙋 Customer-defined rule groups	

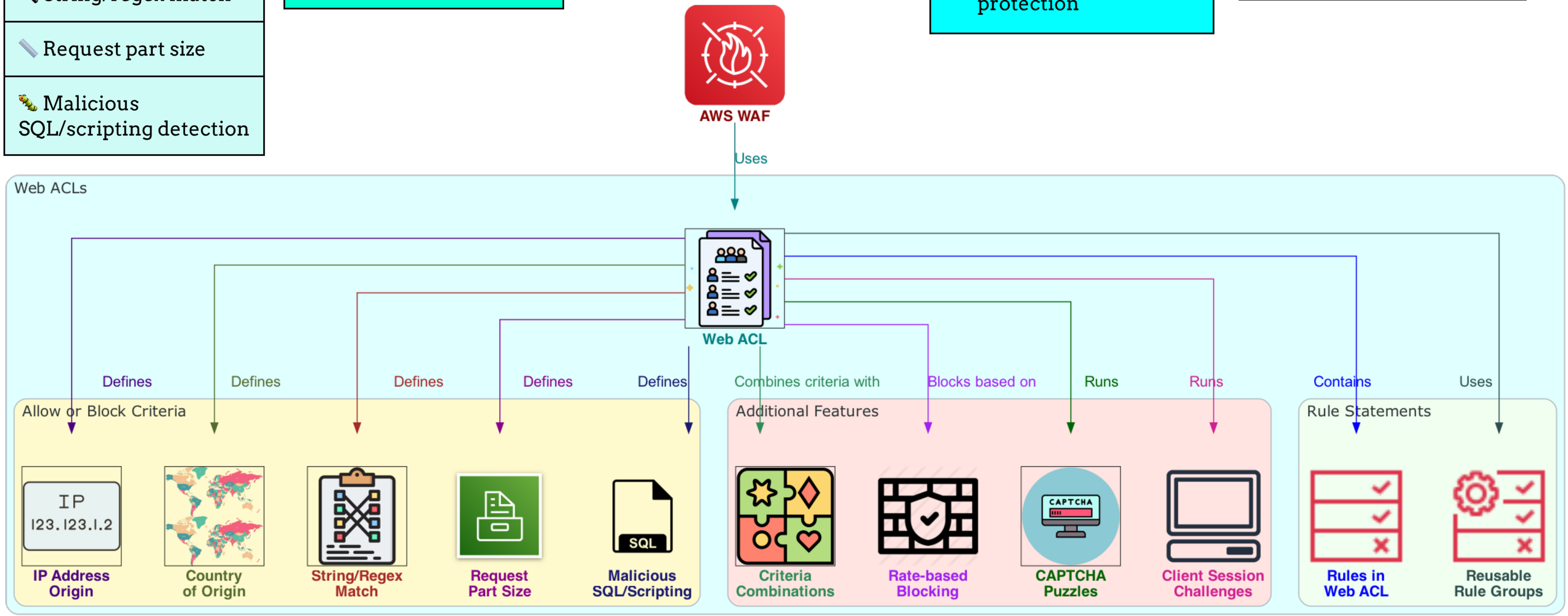
AWS WAF Web ACL Capacity Units (WCUs)

1. 🎛️ **Calculates, controls operating resources**: 🔪 For rules, rule groups, web ACLs
2. 🚦 **Enforces WCU limits**: ⚙️ When configuring rule groups, web ACLs
3. 🔍 **Does not affect web traffic inspection**
4. 🔪 **Rule WCUs**: 🆕 Calculated on rule creation/ update, 💰 Reflects rule's relative cost, 🔧 Simple rules use fewer WCUs, 🧩 Complex rules use more WCUs
5. 📂 **Rule Group WCUs**: 📋 Determined by rules inside group, 🔝 Maximum capacity: 5,000 WCUs, 🔒 Immutable capacity setting: 🆔 Assigned by owner at creation, 📦 Applies to managed, custom rule groups, 🔄 Modifications must stay within capacity
6. 🌐 **Web ACL WCUs**: 📋 Determined by rules, rule groups used, 💸 Rule group cost = capacity setting, 💸 Rule cost = calculated WCUs - optimizations, 🎟️ Basic price includes 1,500 WCUs, 💰 Additional fees for >1,500 WCUs: 🪜 Tiered pricing model



AWS WAF Web Access Control Lists (Web ACLs)

1. 🎯 Allow or block requests based on criteria
   - 🌐 IP address origin
   - 🌍 Country of origin
   - 🔍 String/regex match
   - 📏 Request part size
   - 🦠 Malicious SQL/scripting detection
2. 🧩 Combine criteria using logical operators
3. 🔢 Block/count requests exceeding rate limit
4. 🤖 Run CAPTCHA and client challenges
5. 📋 Define rules
   - 🌐 In web ACL
   - 🗃️ In reusable rule groups
6. 🔤 Rules evaluated in listed order
7. 🔗 Associate web ACL with resources for protection



AWS WAF Rule and Rule Group Actions in Web ACLs

1. 🚦 Allow and Block: Terminating actions

- 🛑 Stop processing on match
- 🚫 Block prevents resource from receiving request

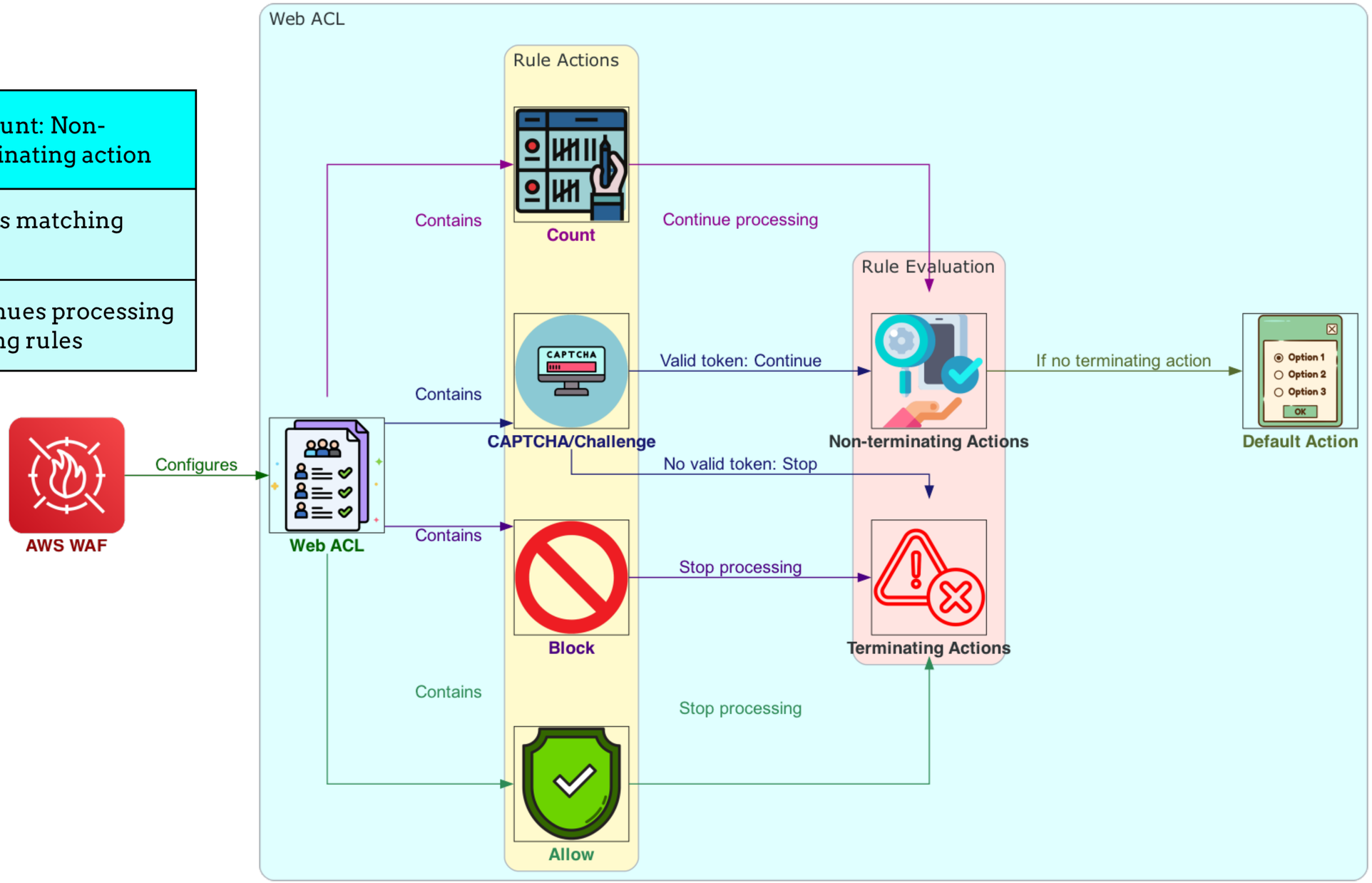
2. 🔢 Count: Non-terminating action

- 📋 Counts matching requests
- ▶️ Continues processing remaining rules

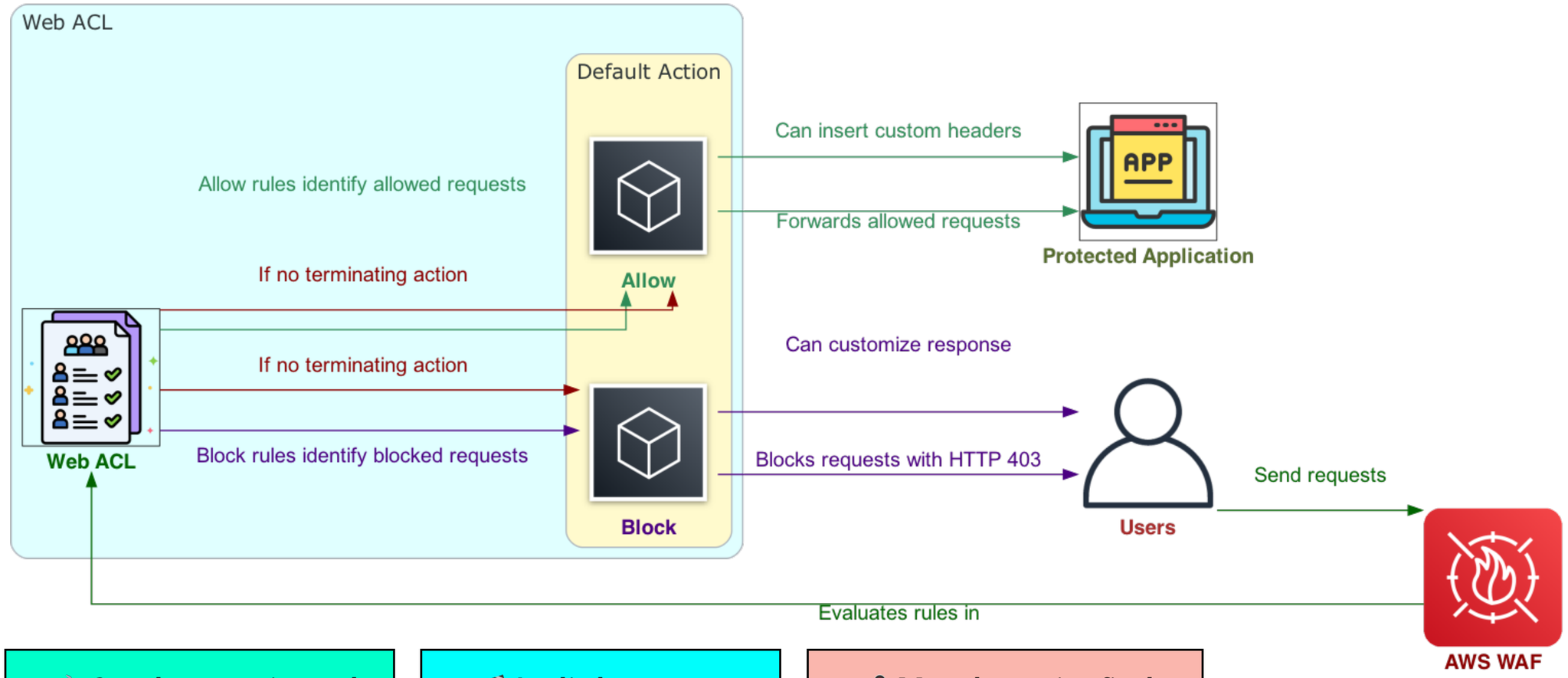
3. 🤖 CAPTCHA and Challenge: Terminating or non-terminating

- ✅ Valid token: Behaves like Count
- ❌ No valid token: Terminates evaluation, sends challenge

4. 🎯 Default action applied if no terminating action



🎯 The Web ACL Default Action in AWS WAF



1. 🔧 Set when creating and configuring a web ACL

🔑 Crucial in determining request handling

2. 🎬 Applied to requests without a terminating action

🚫 After all rule evaluations

🔲 Terminating action stops evaluation

3. 🚦 Must determine final disposition of the request

✅ Allow or block the request

🔚 Always a terminating action

4. ✅ Allow default action

🔓 Allows most users

🚫 Block rules identify requests to block

📩 Can insert custom headers before forwarding

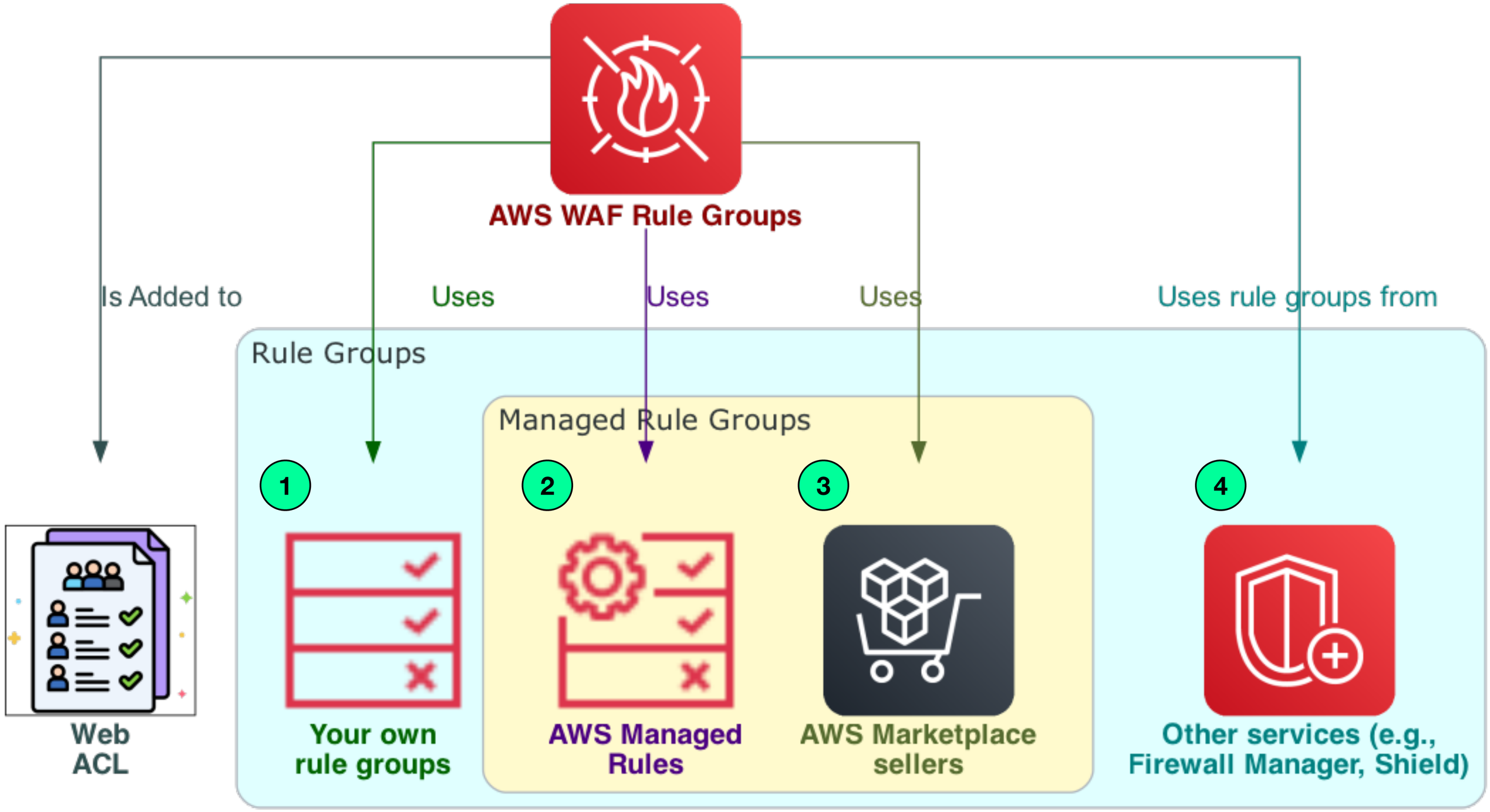
5. ⛔ Block default action

🚫 Prevents most users

✅ Allow rules identify requests to allow

🔢 Default HTTP 403 response, customizable

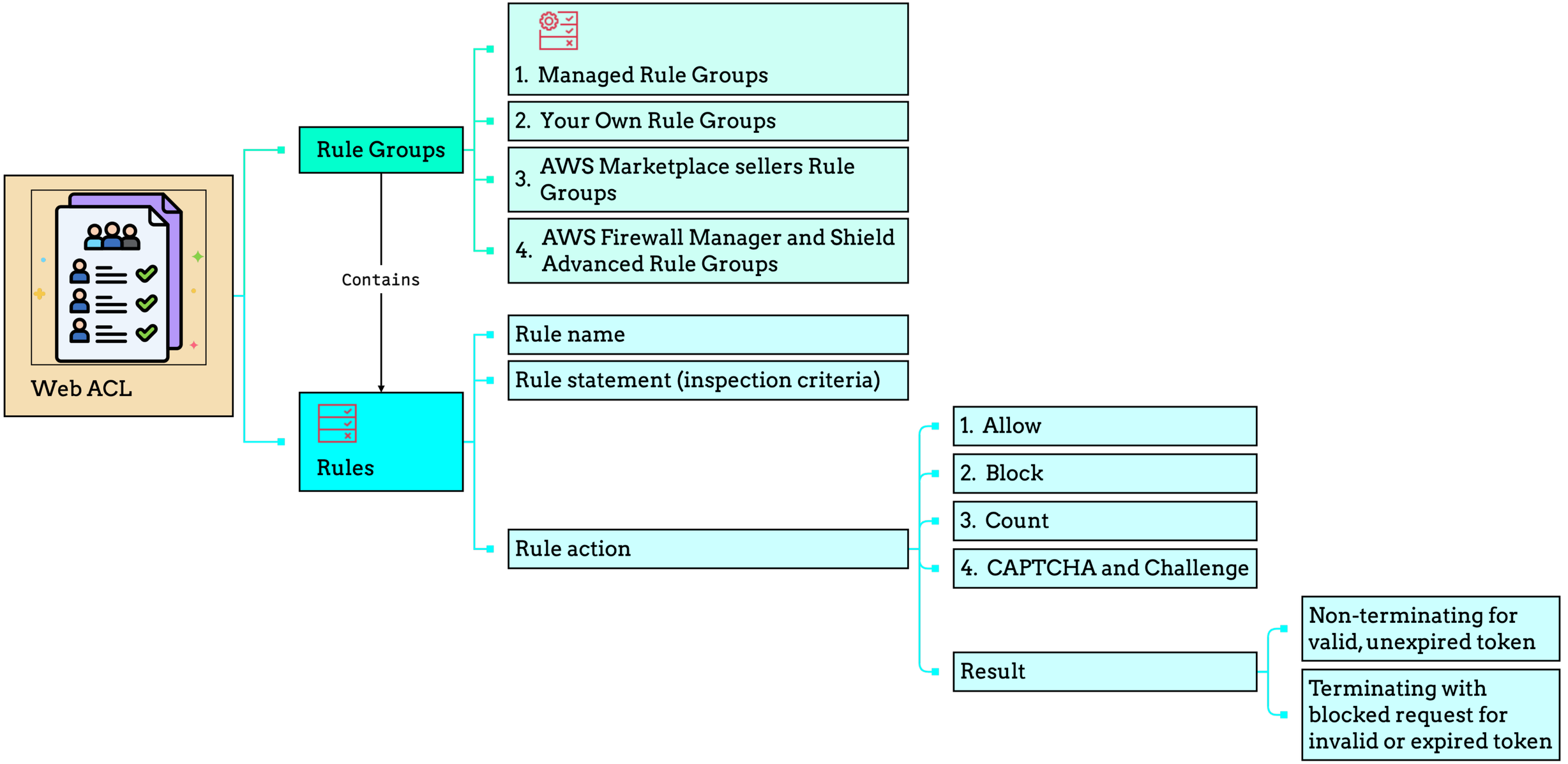
AWS WAF Rule Groups



Differences between Rule Groups and Web ACLs

Aspect	Rule Groups	Web ACLs
Containment	Can't contain rule group reference statements.	Can contain rule group reference statements.
Reusability	Can be reused in multiple web ACLs by adding a rule group reference statement to each web ACL.	Can't be reused.
Default Actions	Don't have default actions.	Have default actions for each rule or rule group included.
Association with AWS Resources	Not directly associated with AWS resources.	Directly associated with AWS resources.
Capacity	Fixed WCU setting that must be set at creation.	System-defined maximum capacity of 5,000 web ACL capacity units (WCUs).
Similarity	Rule groups and web ACLs both contain rules, which are defined in the same manner in both places.	Rule groups and web ACLs both contain rules, which are defined in the same manner in both places.

Relationship between Web ACL, Rule Groups and Rules



Thanks for Watching