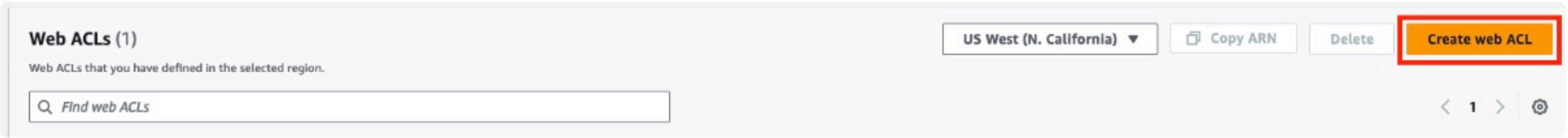
First step was to add a WAF to the ALB

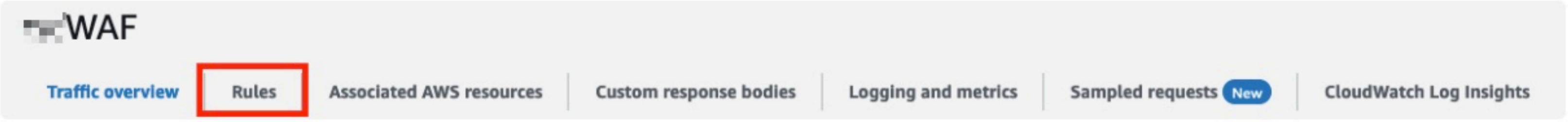


Web ACLs (1)

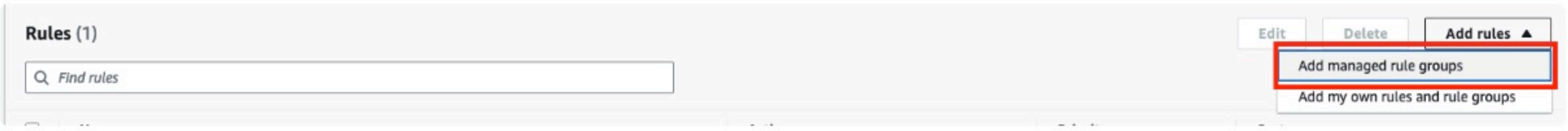
Web ACLs that you have defined in the selected region.

Find web ACLs

Second step was to add the AWS Core Rule Set to the WAF

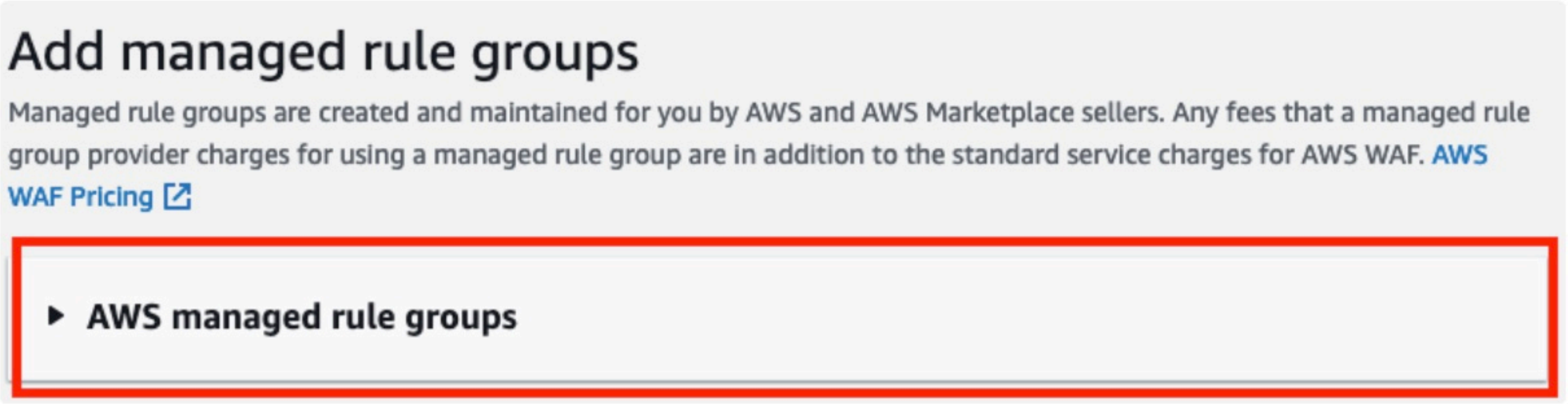


WAF



Rules (1)

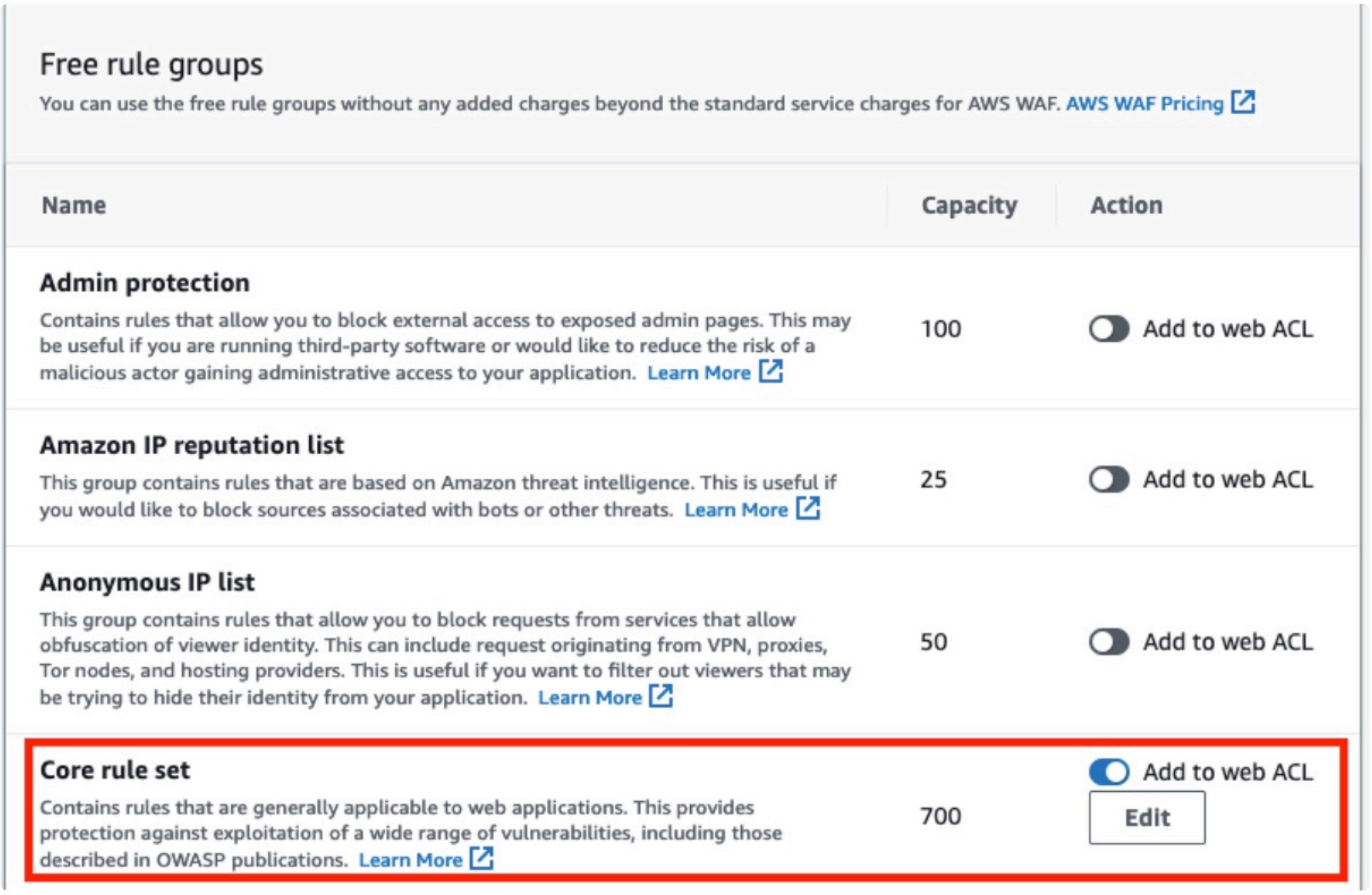
Find rules



Add managed rule groups

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. AWS WAF Pricing

▶ **AWS managed rule groups**

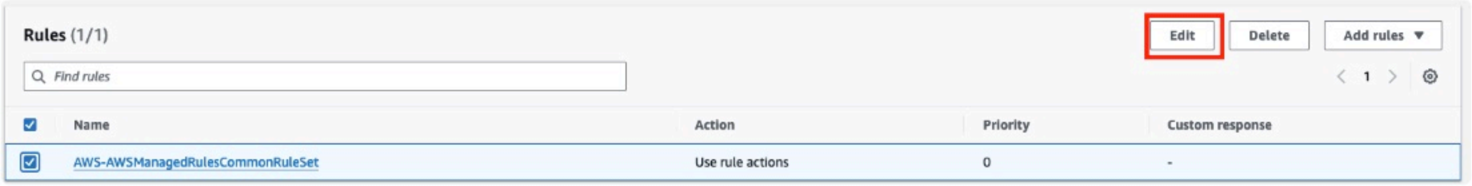


Free rule groups

You can use the free rule groups without any added charges beyond the standard service charges for AWS WAF. AWS WAF Pricing

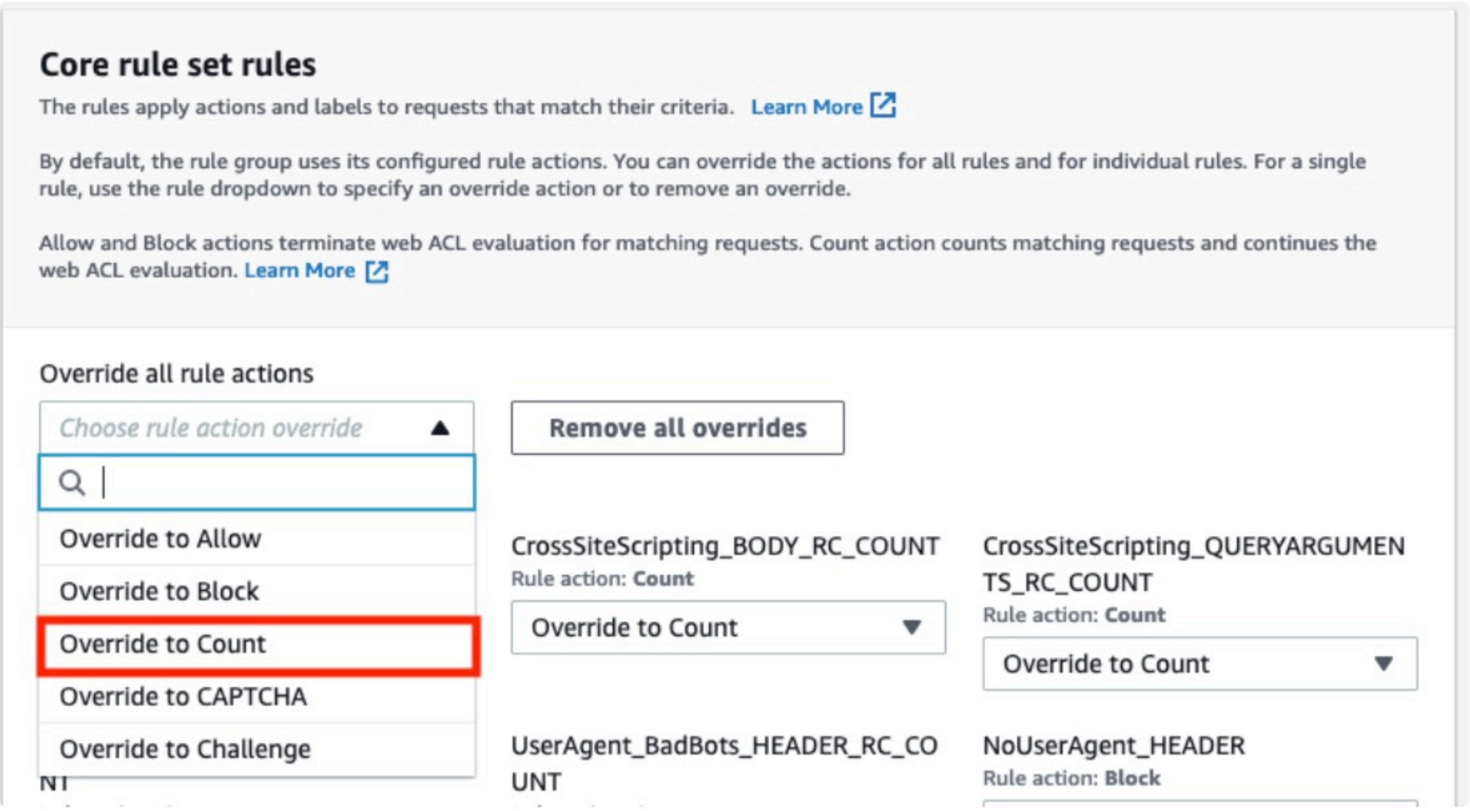
Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. Learn More	100	○ Add to web ACL
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. Learn More	25	○ Add to web ACL
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application. Learn More	50	○ Add to web ACL
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. Learn More	700	● Add to web ACL Edit

Final Step is to set every rule other than GenericFLI_URIPATH to Count in order to preserve existing Nexus functionality



Rules (1/1)

☑	Name	Action	Priority	Custom response
☑	AWS-AWSManagedRulesCommonRuleSet	Use rule actions	0	-



Core rule set rules

The rules apply actions and labels to requests that match their criteria. Learn More

By default, the rule group uses its configured rule actions. You can override the actions for all rules and for individual rules. For a single rule, use the rule dropdown to specify an override action or to remove an override.

Allow and Block actions terminate web ACL evaluation for matching requests. Count action counts matching requests and continues the web ACL evaluation. Learn More

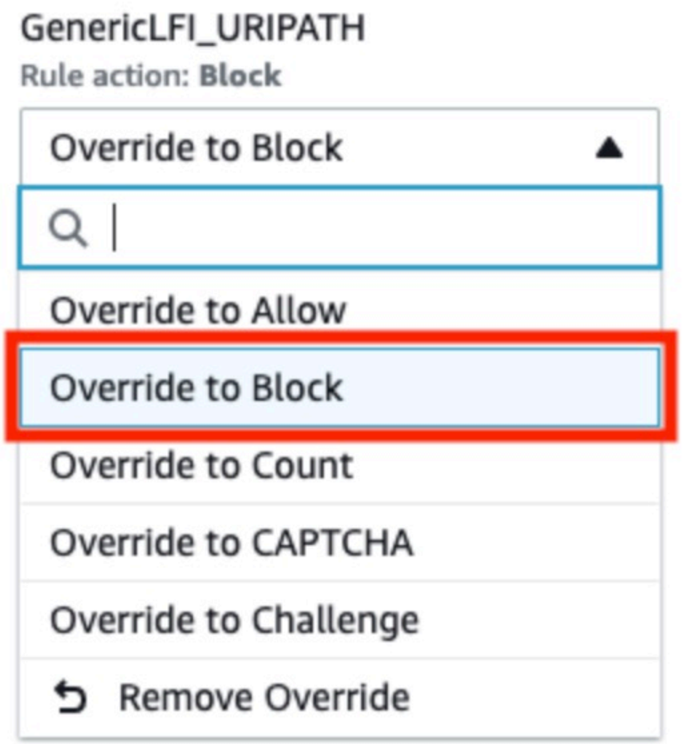
Override all rule actions

CrossSiteScripting_BODY_RC_COUNT
Rule action: **Count**
Override to Count

CrossSiteScripting_QUERYARGUMENTS_RC_COUNT
Rule action: **Count**
Override to Count

UserAgent_BadBots_HEADER_RC_COUNT

NoUserAgent_HEADER
Rule action: **Block**



GenericLFI_URIPATH
Rule action: **Block**
Override to Block