What are Managed Rule Groups?

- **Managed Rule Groups** are collections of predefined rules designed to protect against specific security threats, such as common web vulnerabilities and attacks.
- These rule groups are **provided and maintained** by AWS or third-party vendors, ensuring that they are kept up-to-date with the latest security research and threat intelligence.
- Managed Rule Groups can be easily added to a **Web ACL** to provide protection without having to manually create custom rules.
- You can customize which rules in the group to enable or disable based on your specific needs.

How Managed Rule Groups Work in Web ACL

- Managed Rule Groups are applied by associating them with your Web ACL. Once applied, AWS WAF inspects incoming traffic based on the rules in the group.
- Managed rules are evaluated in the same way as custom rules within a Web ACL, meaning that the order of evaluation and actions (allow, block, count) are based on how you configure the Web ACL.
- You can selectively enable or disable individual rules within a managed rule group if certain rules are too restrictive or unnecessary for your use case.

Advantages of Using Managed Rule Groups

1. Simplified Security Management

- Managed Rule Groups offer a **turnkey solution** for application security, providing you with pre-built rulesets without needing in-depth security expertise to configure them.

2. Regular Updates

- These rules are automatically **updated by AWS or third-party vendors** to respond to new threats. This helps ensure that your application remains protected from evolving attack vectors without requiring constant manual rule updates.

3. Fast Deployment

- Managed Rule Groups allow you to quickly **apply comprehensive protections** to your application with minimal setup. This is particularly beneficial for teams that need rapid deployment and don't have the time or resources to develop custom security rules.

4. Comprehensive Coverage

- Managed Rule Groups cover a wide range of vulnerabilities and attack types, often aligned with best practices like **OWASP Top 10**. This provides protection against the most common threats facing web applications.

5. Cost Efficiency

- Managed Rule Groups save time and resources by reducing the need to manually create, configure, and update custom rules. In many cases, the cost of using these groups is outweighed by the reduction in administrative overhead.

Customization and Control

Even though Managed Rule Groups are predefined, AWS WAF allows you to **customize how these rule groups behave** in your Web ACL:

- **Enable/Disable Specific Rules**: Within a Managed Rule Group, individual rules can be turned on or off. This allows you to disable rules that might be too restrictive or cause false positives while keeping the rest of the group active.
- **Override Rule Actions**: You can modify the action for specific rules, such as changing a **Block** action to **Count** to observe how the rule behaves without blocking requests.
- **Rule Prioritization**: Managed rules are evaluated in the order defined in your Web ACL. You can control the order of evaluation by placing certain custom rules or managed rules before or after others.

Pricing for Managed Rule Groups

- **AWS Managed Rule Groups**: These are generally available as part of the standard AWS WAF pricing. You are charged based on the number of Web ACLs, the number of rules, and the number of requests processed.
- **Third-Party Managed Rule Groups**: Third-party rule groups from vendors typically come with additional charges. You may be billed for using the rule group in addition to the standard AWS WAF fees. Each vendor sets its own pricing structure.

Best Practices for Using Managed Rule Groups

- **Start with Managed Rule Groups**: If you’re new to AWS WAF or need rapid deployment, use AWS Managed Rule Groups to get baseline protection against common threats.
- **Monitor and Adjust**: Use the **Count** action on rules within Managed Rule Groups to observe their behavior before fully enabling them. This will help prevent false positives or unexpected blocks.
- **Combine with Custom Rules**: Use Managed Rule Groups for general protection and combine them with custom rules for more specific filtering based on your application's unique needs.
- **Regularly Review Rule Groups**: AWS and third-party vendors periodically update Managed Rule Groups. Review your Web ACLs regularly to ensure rules are still relevant and to incorporate any new protections that have been added.

Paid Managed Rule Groups:

1. Account Creation Fraud Prevention

- **Capacity**: 50
- **Description**: This rule group provides protection against the creation of fraudulent accounts on your application. Fraudulent accounts are often created for malicious purposes, such as exploiting promotional sign-ups, sending spam, or impersonating legitimate users. This rule group can block suspicious account creation attempts by analyzing request patterns commonly associated with automated scripts or fraudulent behavior.
- **Additional Fees**:
  - $10/month (prorated hourly).
  - Tiered fees for requests analyzed beyond the first 1 million requests, which are free.

2. Account Takeover Prevention

- **Capacity**: 50
- **Description**: Protects login endpoints from unauthorized access due to credential stuffing, brute force login attempts, and other login abuse scenarios. With account takeover prevention, you can safeguard user accounts by blocking suspicious login attempts and help mitigate fraud risks associated with compromised user credentials. This can help prevent unauthorized users from accessing sensitive areas of your application.
- **Additional Fees**:
  - $10/month (prorated hourly).

    - Additional fees apply based on the volume of requests processed beyond 1 million free requests.

3. Bot Control

- **Capacity**: 50 (available in **Common** and **Targeted** levels)
- **Description**: AWS WAF Bot Control is designed to defend against automated bots that may scrape content, perform credential stuffing, or conduct DDoS attacks. This rule group allows you to monitor and control bot traffic using CloudWatch and apply specific actions to different bot types. Bot Control provides extensive insights into bot traffic, helping to minimize the impact on resources and ensuring legitimate traffic isn't affected.
- **Common Level**:
    - Basic bot traffic management.
    - $10/month (prorated) includes the first 1 million web requests, with additional costs per million requests beyond this.
    - $0.40 per thousand CAPTCHA attempts.
- **Targeted Level**:
    - Advanced bot mitigation.
    - Similar pricing to the common level, but with added costs for analysis of CAPTCHA and challenge attempts.

Free Rule Groups:

1. Admin Protection

- **Capacity**: 100
- **Description**: Helps block access to sensitive admin panels or pages (e.g., `/admin` or `/login`) to prevent unauthorized access to these critical endpoints. This rule group is useful for reducing the risk of administrative exploitation, particularly if you are running third-party software or have known exposed admin pages that attackers frequently target.

2. Amazon IP Reputation List

- **Capacity**: 25
- **Description**: Based on Amazon's threat intelligence, this rule group blocks requests originating from IP addresses associated with malicious activity, such as botnets, spam sources, or DDoS attack nodes. This rule group is particularly effective at blocking harmful traffic without manual configuration.

3. Anonymous IP List

- **Capacity**: 50
- **Description**: Blocks requests from IP addresses using anonymity services (e.g., VPNs, proxies, or the Tor network) that mask the true origin of the traffic. This rule group is valuable for applications that want to block traffic from anonymized sources, which are often associated with malicious activities.

4. Core Rule Set

- **Capacity**: 700
- **Description**: Provides a broad set of protections for web applications, including defenses against common vulnerabilities like SQL Injection (SQLi), Cross-Site Scripting (XSS), Local File Inclusion (LFI), and other OWASP Top 10 security risks. This general-purpose rule group is highly recommended for web applications that need basic protection against a wide range of attacks.

5. Known Bad Inputs

- **Capacity**: 200
- **Description**: This rule group focuses on blocking well-known malicious request patterns, which can help reduce the chances of attackers discovering vulnerabilities in your application. It identifies requests containing invalid inputs or patterns commonly used in exploitation attempts, such as malformed requests, illegal headers, and suspicious characters.

6. Linux Operating System

- **Capacity**: 200
- **Description**: Designed to block exploitation attempts targeting Linux environments, such as those leveraging Local File Inclusion (LFI) vulnerabilities, command injection, or privilege escalation. This rule group can help prevent malicious users from executing commands or accessing restricted files on Linux-based systems.

7. PHP Application

- **Capacity**: 100
- **Description**: Protects PHP-based applications from vulnerabilities specific to the PHP platform, such as Remote Code Execution (RCE) via insecure PHP functions, PHP Object Injection, or file inclusion attacks. This rule group helps prevent attackers from exploiting unsafe PHP code to execute arbitrary commands or compromise application integrity.

8. POSIX Operating System

- **Capacity**: 100
- **Description**: Focuses on blocking exploits aimed at POSIX-like operating systems (including Unix-based systems) by identifying patterns that indicate unauthorized file access or code execution. It targets vulnerabilities that could allow attackers to manipulate file permissions or escalate privileges.

9. SQL Database

- **Capacity**: 200
- **Description**: Provides SQL injection protection by blocking malicious queries targeting your database through vulnerabilities in SQL statements. This rule group is essential for applications that interact with relational databases and want to prevent unauthorized data access or manipulation through SQLi attacks.

10. Windows Operating System

- **Capacity**: 200
- **Description**: This rule group is designed to protect Windows-based web applications from known vulnerabilities, including those related to file access or command execution. It blocks requests that attempt to exploit PowerShell, Windows command line utilities, or other Windows-specific weaknesses.

Cloudbric Corp. Managed Rule Groups:

1. API Protection

- **Capacity**: 1200
- **Description**: Provides defense against the OWASP API Security Top 10 vulnerabilities. It focuses on protecting APIs from threats such as insecure object access, improper data exposure, and injection attacks, as well as payload validation for formats like XML, JSON, and YAML.

2. Anonymous IP Protection

- **Capacity**: 90
- **Description**: Blocks malicious requests originating from anonymous IP addresses (VPNs, proxies, DNS proxies, etc.), which are often used by attackers to hide their identity.

3. Bot Protection Rule Set

- **Capacity**: 150
- **Description**: Mitigates risks from malicious bots, such as credential stuffing and account takeover attempts, while allowing legitimate bot traffic (e.g., search engine crawlers).

4. Malicious IP Reputation Rule Set

- **Capacity**: 6
- **Description**: Uses a comprehensive IP reputation database to block requests from IP addresses known for malicious activities such as spam, DDoS, or other forms of attack.

5. OWASP Top 10 Rule Set

- **Capacity**: 1400
- **Description**: Protects against the OWASP Top 10 vulnerabilities, including SQL injection, XSS, and other web application security risks.

6. Tor IP Detection Rule Set

- **Capacity**: 6
- **Description**: Identifies and blocks requests from IP addresses associated with the Tor network, often used by attackers to remain anonymous while launching attacks.

Cyber Security Cloud Inc. Managed Rule Groups:

1. API Gateway/Serverless Protection

- **Capacity**: 1000
- **Description**: Designed for protecting serverless and API Gateway environments from OWASP API Security Top 10 risks. This includes protections against data exposure, insecure endpoints, and malicious API traffic.

2. High-Security OWASP Set

- **Capacity**: 1000
- **Description**: Offers comprehensive coverage of OWASP Top 10 vulnerabilities for applications that need enhanced security, particularly for business-critical applications.

F5 Managed Rule Groups:

1. API Security Rules

- **Capacity**: 1000
- **Description**: Focuses on defending APIs against a variety of threats, including injection attacks (SQLi, XML External Entity Injection), server-side request forgery, and improper data validation. It ensures that APIs can handle common payload formats safely.

2. Bot Protection Rules

- **Capacity**: 1000
- **Description**: Protects web applications from automated attacks carried out by malicious bots, such as credential stuffing, web scraping, and brute force login attempts.

3. Common Vulnerabilities & Exposures (CVE) Rules

- **Capacity**: 1000
- **Description**: Defends against known CVEs by blocking exploitation attempts of popular platforms like Apache, PHP, Node.js, and others.

4. Web Exploits OWASP Rules

- **Capacity**: 1000
- **Description**: Protects against the OWASP Top 10 web application security risks, with a focus on preventing exploitation via SQL injection, cross-site scripting, and command injection.

Fortinet Managed Rule Groups:

1. API Security

- **Capacity**: 1000
- **Description**: Protects APIs against various OWASP API vulnerabilities, focusing on input validation, improper authentication, and request tampering.

2. OWASP Top 10 - The Complete Ruleset

- **Capacity**: 1000
- **Description**: Comprehensive coverage for OWASP Top 10 vulnerabilities across web applications, including SQLi, XSS, CSRF, and security misconfigurations.

GeoGuard Managed Rule Groups:

1. IP Advanced Protection (Web ACL Pricing)

- **Capacity**: 100
- **Description**: Protects against geolocation fraud by detecting IPs using VPNs, proxies, or other tools that mask the true IP address.

2. IP Advanced Protection (Per Request Pricing)

- **Capacity**: 200
- **Description**: Similar to the Web ACL pricing but billed per request, offering a more granular cost structure.

Imperva Managed Rule Groups:

IP Reputation

- **Capacity**: 200
- **Description**: Protects against IP addresses with poor reputations (often associated with malicious activities). It uses an extensive IP blacklist to block threats.

ThreatSTOP Managed Rule Groups:

1. Enhanced OFAC Sanctions Compliance

- **Capacity**: 5
- **Description**: Helps businesses comply with OFAC sanctions by blocking traffic associated with sanctioned entities and their subsidiaries.

2. Core Threats

- **Capacity**: 10
- **Description**: Blocks inbound threats such as brute force attacks, web server exploits, and DDoS attempts, helping reduce fraud and security risks.

3. ITAR and OFAC Rules

- **Capacity**: 5
- **Description**: Provides compliance with the U.S. International Traffic in Arms Regulations (ITAR) and OFAC by blocking sanctioned traffic.

4. New and Active HTTP Threats

- **Capacity**: 2
- **Description**: Protects against active and newly identified HTTP-based threats, including attempts to exploit vulnerabilities like Shellshock, Apache Struts, and SSH brute force attacks.