Mod 8

**Mod 8 Anypoint Secuity**

1. Why should we use Anypoint Security when Mulesoft provides security through API Manager’s API policy?

Extra defence for api..

These policies are applied at api gateway rather than to the apis so it acts like an added security.

1. //Why is Anypoint security not available in deployment models other than RTF?
2. Can you explain the architecture of the Anypoint security?

Anypoint Security provides a layered approach to secure your application network. These layers work together to protect both the application network and the network’s individual nodes by controlling access to APIs, enforcing policies, and proxying all inbound or outbound traffic to mitigate external threats and attacks.

Anypoint is used with only RTF at present.

AS has got two services that are :.

Edge policies and Tokenisation

Edge policies consists of:

Ip whitelist policy:

The IP Whitelist policy allows you to create an explicit list of IP addresses that can access your deployed endpoints. IP addresses that aren’t on this white list are rejected.

DOS:

The Denial of Service (DoS) policy prevents attackers from flooding your network to prevent legitimate network traffic to your APIs. For example, malicious clients could send huge payloads designed to consume resources and bandwidth to your network.

When you create a DoS policy, you configure a time span and action to take when the [error types](https://docs.mulesoft.com/anypoint-security/dos-policy#error_types) you configure are encountered. If the policy encounters more errors than your configured threshold coming from the same IP address, the policy can either drop the connection silently (doesn’t attempt the TLS connection), or drop the connection immediately and return a 503 error

HTTP limit policy:

The HTTP Limits policy prevents an attacker from sending large messages that consume all your bandwidth.  
This policy checks TCP protocol message sizes and headers. This policy does not check content.

This policy applies to all the APIs behind your Edge inbound endpoint.

1. When should I go with Anypoint Security for securing my applications.?

When we need an extra security for our apis we go for this AS and also here there are some policies like http limit, dos etc we don’t get with api manager policies.

1. Can you provide some advantages and disadvantages of Anypoint security over API Manager’s API policies?

Adv--We have some advanced policies like http limit policy, dos, WAF, tokenisation

Dis -- available only with rtf and should have platinum or higher subscription.

1. // How can we enforce security policies in Anypoint Security?
2. Can you name some of the EDGE policies that can be applied in Anypoint Security?

Ip whitelist policy, DOS policy, http limit policy, WAF policy

1. //How do I whitelist certain ips using Anypoint security?

Listing of ips – explain the basic ip whitelisting

1. What is the use of Denial Of Service Policy in Anypoint Security?

* The Denial of Service (DoS) policy prevents attackers from flooding your network to prevent legitimate network traffic to your APIs.
* For example, malicious clients could send huge payloads designed to consume resources and bandwidth to your network.
* When you create a DoS policy, you configure a time span and action to take when the [error types](https://docs.mulesoft.com/anypoint-security/dos-policy#error_types) you configure are encountered.

If the policy encounters more errors than your configured threshold coming from the same IP address, the policy can either drop the connection silently or drop the connection immediately and return a 503 error.

1. What are the capabilities of EDGE policies?

Ip whitelist policy, DOS policy, http limit policy, WAF policy

Explain this in detail

1. What do you mean by Web Application Firewall Policy?
2. How do you prevent SQL Injection using Anypoint Security?
3. How do you manage your certificates in Anypoint Security?

Anypoint Security secrets manager uses secure vault technology to store and control access to private keys, passwords, certificates, and other secrets.

1. //What QoS policies are available in Anypoint Security?

http limit, DOS, WAF

1. What do you mean by Certificate Revocation List?

A **Certificate Revocation List** (**CRL**) is a **list** of digital **certificates** that have been **revoked** by the issuing **Certificate** Authority (CA) before their scheduled expiration date and should no longer be trusted.

1. How do you protect sensitive data using a Tokenization method in Anypoint Security?

Tokenisation can be applied on the sensitive data so that even if there is a breach the original data is no exposed.

Tokenization is a highly effective way to protect sensitive data. When you tokenize data, sensitive data elements are substituted with randomly generated non-sensitive data elements.

Examples of sensitive information that are suitable for tokenization protection include:

* Primary Account Number (PAN)
* Personally Identifiable Information (PII)
* Protected Health Information (PHI), or any information deemed sensitive

<https://docs.mulesoft.com/anypoint-security/tokenization>

1. How do tokens stored in Anypoint Security?
2. How do you retrieve the original values in the Tokenization method?

Revival is possible only with detokenisation method.

1. Can you provide some examples of you using tokenization in your project?

Okta token, sfdc token

1. In which scenario you will MASK sensitive information rather than Encrypting the information.

Logging and login – masking

Reuse the data – encryption

Don’t reuse --- masking

1. How do you encrypt sensitive information in Anypoint security?
2. What is the use of a Secrets manager in Anypoint Security?