## Module 8: Anypoint Security

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

It is separate service provided for RTF deployment. These are out of box policies.

Anypoint Security provides advanced defense for your APIs and integrations. **Protect sensitive data, stop threats at the edge, and automatically enforce security best** practices to protect and govern your application network

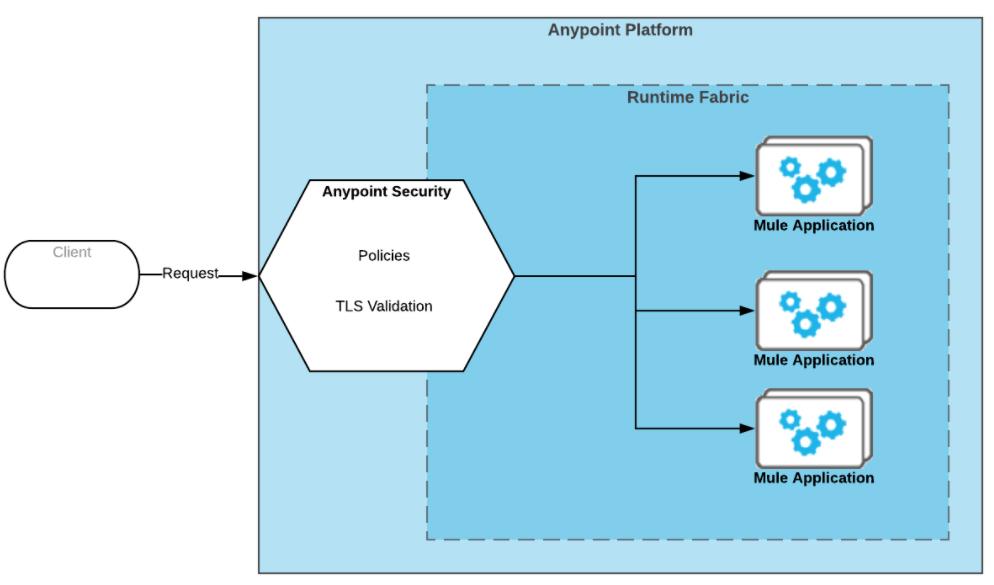
While API Manager’s API policy only provides base level security of each APIs

AS enables security by design

Holistic security from API design, API deployment and API management

1. Why is Anypoint security not available in deployment models other than RTF?

Anypoint security is additional features customer can get when implementing RTF.

1. 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 Security provides you with a dedicated endpoint to detect attacks and validate traffic without taxing your network implementations.

It provides two services. One at the perimeter of network called as **edge policies**. These policies helps to identify threats at the network perimeter . It is implemented on Kubertenes which is outside of mule infrastructure and do not impact the APIs. The second service runs inside the network known **as tokenization service**. It ensures that the sensitive data are secured. It ensures the security via masking, tokenization and encryption.

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

If we want to secure and govern our application using Mulesoft security services then we can use anypoint security.

If organizations don’t have proper resource and infrastructure to maintain their own security management and wants to go for out of box services then they should go for Anypoint Security for securing their applications.

Example:

At JetBlue, they need to use customer credit card in flight and out of flight as well. They needed data security as well as compliance with security laws.

Three important agends: customers data are secure at transit and at rest, maintain credit card information integrity, and provide valid credit card numbers to external partner like expedia, and hotels.com as required.

Solution: All airline ticket booking along with addons like hotels, car rentals would go through their ESG tokenization proxy. They implemented anypoint security to tokenize and detokenize the credit card. Only partner with

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

Advantages:

* Provides security for sensitive data
* Gives flexibility to tokenize specific data: partial or fully
* You can use the **Any point Security policies to manage all traffic to your Runtime Fabric**, and leverage **API Manager policies** to apply specific behaviors to specific APIs.
* Ensures security compliance rules

Disadvantages

* Need to pay more to get the service.
* Must have RTF installed and customer should subscribe for platinium or higher

1. How can we enforce security policies in Anypoint Security?

* We can enforce security policies in Anypoint Security by adding security at network level. The policies that can be implemented at edge are IP Whitlelist Policy, DoS, HTTP limit policy, and WAF

1. Can you name some of the EDGE policies that can be applied in Anypoint Security?

* The edge policies that are applied in the anypoint security are:
  + **IP White list Policy**:
  + **Denial of Service Policy**:
  + **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. You can Configure the maximum sizes for message, path header and trailers. f you want to filter specific HTTP methods, configure them in the **Allowed HTTP Request Methods** field.  
    Allowed methods are: GET, POST, PATCH, HEAD, TRACE, OPTIONS, DELETE, and PUT.
  + **Web Application Firewall (WAF) policy**

1. How do I whitelist certain IPs using Anypoint security?

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.

If you have an IP Whitelist policy assigned, you need to whitelist all IP addresses that are coming through your exposed endpoint..

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

This policy prevents attackers from flooding your network to prevent legitimate network traffic to your APIs. 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

For example, malicious clients could send huge payloads designed to consume resources and bandwidth to your network

Since the source of the request is based on the IP address**, if an an attacker spoofs** the source IP address, the DoS Policy cannot prevent the attack.

1. What are the capabilities of EDGE policies?

* Allows a policy be implemented in API Gateway so that any threats n/w threats are detected at the API gateways
  + **IP White list Policy**:
  + **Denial of Service Policy**: In this you can define rules for authentication and QoS that creates the feedback loop between the edge and individual API to ensure the security implementation adapts new threats
  + **HTTP Limit policy:** The HTTP Limits policy prevents an attacker from sending large messages that consume all your bandwidth. This policy checks message size and headers but not the content
  + **Web Application Firewall (WAF) policy**: You can implement WAF for all APIs contained with perimeter you define. This protects your api from threats like SQL injection, cross side scripting and any of the oath top 10 attack pattern

1. What do you mean by Web Application Firewall Policy?

A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet . The Web Application Firewall (WAF) security policy is available for request and response traffic to provide protection at the Web application level. Policies are grouped into the major threat categories for requests and responses.

**Example**: When the WAF policy detects errors, it triggers the thresholds configured in the DoS, which can be optionally configured to take actions such as shaping or blocking traffic for an IP address from a malicious source.

1. How do you prevent SQL Injection using Anypoint Security?

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands

**To prevent SQL injection In anypoint security we can enable the SQL injection rule in WAF policy**

**General SQL injection security**

The select operation introduced by the connector allows to use a parametrized SQL query, like in the following XML snippet:

<set-variable variableName="table" value="PLANET"/>

<db:select config-ref="dbConfig">

<db:sql>#["SELECT \* FROM $(vars.table) WHERE name = :name"]</db:sql>

<db:input-parameters>

#[{'name' : payload}]

</db:input-parameters>

</db:select>

By using prepared statements with parameterized queries and [white list input validation](https://stackoverflow.com/questions/3559621/blacklisting-vs-whitelisting-in-forms-input-filtering-and-validation) you can avoid some/most types of attacks

1. How do you manage your certificates in Anypoint Security?

To manage the certificate the Anypoint Security has a feature called Secure Manager which is used to store the certificates securely in a secure vault.

1. What QoS policies are available in Anypoint Security?

The QoS policies that are available in Anypoint Security are:

* DoS
* WAF
* Http limit

Policies category in API Manager: <https://medium.com/@pkurimella/mulesoft-policies-govern-and-manage-apis-efficiently-5dee0d7656db>

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?

If , a tokenization format is created with the credit card data domain and assigned to the tokenization service. A tokenization policy is applied to the API gateway.

When a payload that contains credit card numbers in the payload is sent, the request is redirected to the API gateway that has the tokenization policy applied.

A connection is established between the API gateway and the tokenization service. The tokenization service receives the credit card information, transforms the data into tokens, and returns the tokenized data to the API gateway. The API gateway replaces the credit card number with the tokenized data and the request is sent to the app.

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

The original values are retrieved using detokenization policy. This is conducted under strict security controls.

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

In the MyTrain project we can tokenize the personal information’s like email, and tokens needed to configure salesforce and okta connector. This provides security even if someone is able to breach the policy they do not get access to the original data

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

For logging and login where we don’t want user or anyone to see the sensitive data. In such case we can use masking

1. How do you encrypt sensitive information in Anypoint security?

We can encrypt the sensitive in formation in anypoint using encryption techniques, tokenization service or masking.

To encrypt information we can implement either symmetric or asymmetric encryption

For assymmetic encryption we can use – TrusStore, KeyStore, Certificates

For symmetric encryption we can use – password, symmetric keys, S3 credentials, Blob

1. What is the use of a Secrets manager in Anypoint Security?

* The secrets manager is used to write, read, and manage your secrets, keys, and Transport Layer Security (TLS) certificates within a unique source that allows access to other authorized platform services on your behalf.
* This is the central and secure repository to manage the secrets

https://nl.devoteam.com/en/blog-post/how-to-secure-properties-and-hide-encryption-key-in-cloudhub-mule-4/