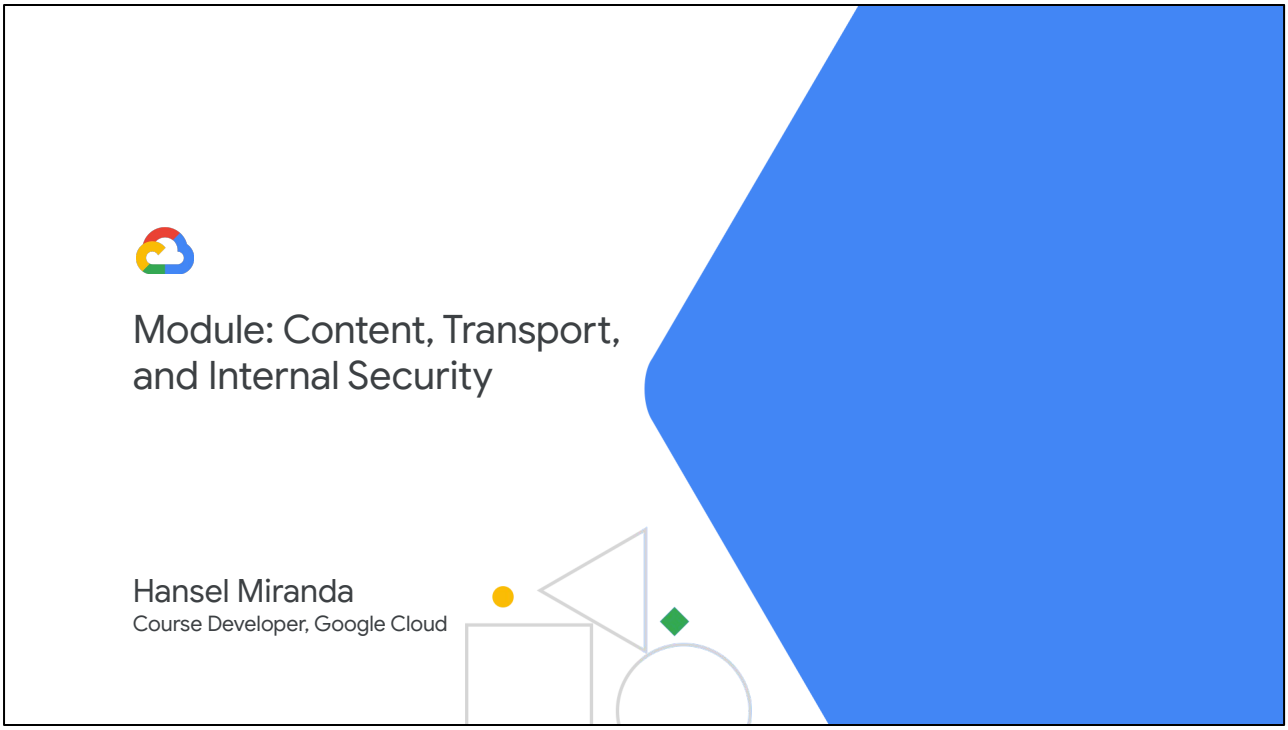


In the last module, you learned about authentication and authorization.

This module will teach you about content-based attacks, and the Apigee policies that can help protect your APIs against these attacks.

We will learn about transport security, and about features of Apigee that keep users of the Apigee console from seeing sensitive data when API calls are traced.

You will add JSON threat protection to your retail API proxy, and add a key value map to store backend credentials.

You will also complete a lab that uses the RegularExpressionThreatProtection policy, and a lab that uses the Apigee API to create a debug mask to mask variables while tracing an API proxy.

In this lecture you'll learn about content-based attacks against APIs and how Apigee can help you protect your APIs against them.

Content-based API attacks use malformed API requests to cause issues with APIs and backend services.

Some attacks use text fields to compromise data in the backend, either retrieving data that the user should not be permitted to get, or destroying data in backend databases.

Other attacks use JSON or XML payloads that are crafted specifically to cause problems for parsers. This type of attack can cause an application-level denial of service, where the API or backend service stops responding to requests.

Legacy services are often susceptible to these attacks. When services are designed to receive traffic only from inside the company network, developers may not pay much attention to content-based attacks. When you start using your legacy services to build your external APIs, though, all of a sudden your services are exposed to traffic from the internet.

It is a good practice to add protection against these attacks in your API proxies so that you can block the malicious data from reaching your backend services.

Apigee has policies that can help you create this level of protection in your proxies.

Tips for input validation

- Extract fields from payloads using JSONPath/XPath in the ExtractVariables policy.
- Validate required fields, field interactions, and regular expression patterns by using proxy conditions or JavaScript policies.
- Rewrite validation error messages from the backend.

You may need to use many different types of input validation for your APIs, and most of this validation can be done in the API proxy, reducing traffic to the backend that would be rejected anyway.

API payloads are often in JSON or XML format. Fields within your JSON and XML can be extracted using the JSONPath and XPath configuration within an ExtractVariables policy.

Required fields and field dependencies can be validated using boolean conditions.

Complex formatting patterns can also be checked by using regular expressions in conditions or by using a JavaScript policy.

If you choose not to validate all input at the proxy layer, make sure that you know all of the different error messages that might be returned by your backends and have a method for remapping each one to your consistent error format for your API.

Malicious input

- Malicious consumers may send inputs that contain dangerous strings.
  - Example: SQL injection code
    - You can perform malicious input checks in the proxy even if you expect the backend to check these also.
      - You still need to use best practices like parameterized queries and escaping/encoding data.
- The RegularExpressionProtection policy can be used to detect these types of attacks.

Blocking dangerous input at the API proxy layer helps protect your backend services from intentional attacks.

For example, a common attack on an API is a SQL injection attack, where the attacker creates inputs that have SQL code or comment characters embedded in them. These inputs can cause leakage or destruction of your backend database data if you do not block them.

The correct way to block SQL injection is to escape dangerous characters and not build SQL queries using concatenation. You should protect against SQL injection in your backend services.

However, blocking known bad requests will protect your APIs even if the backend is not inherently protected.

You can use the RegularExpressionProtection policy to block dangerous string patterns.

RegularExpressionProtection policy

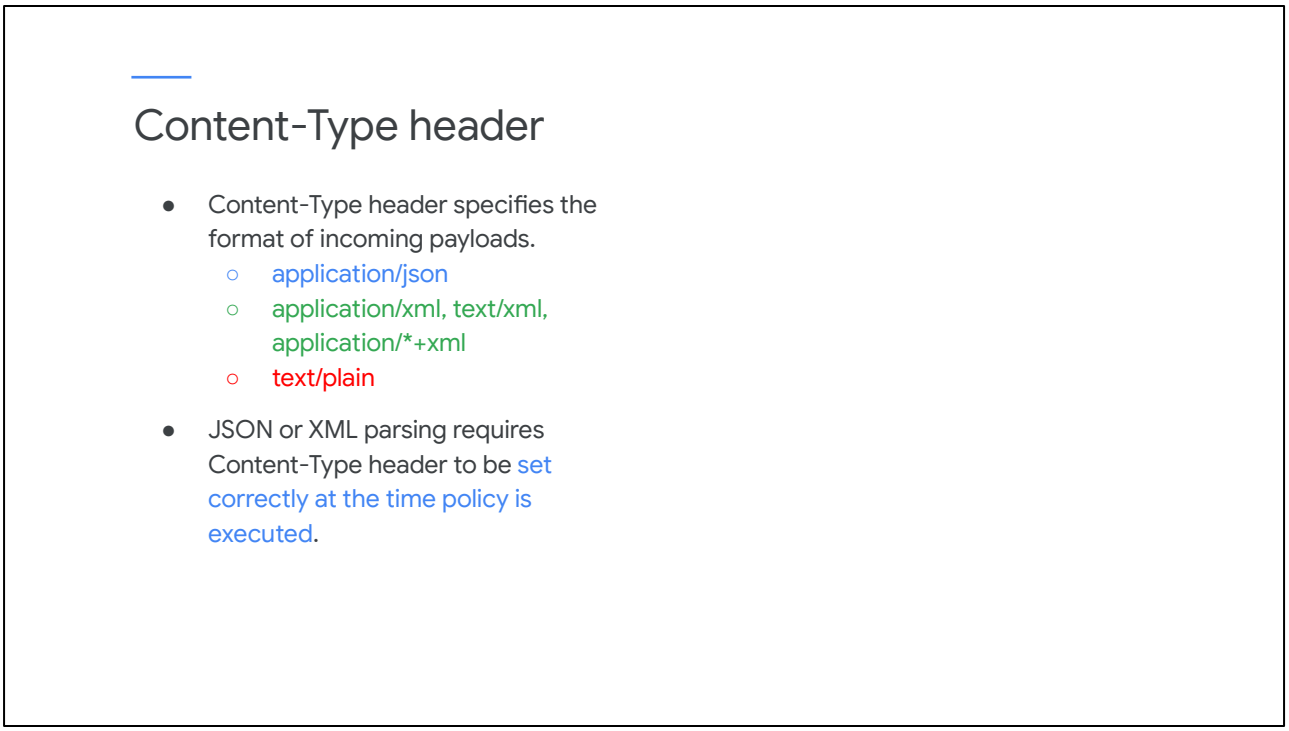
- Search for blocked patterns in any location (URI, payload, headers, query params, variables).
- If any specified regular expression matches the corresponding input field or variable, the message is considered a threat and is rejected.

```
<RegularExpressionProtection continueOnError="false"
 enabled="true" name="REP-InputProtection">
  <Source>request</Source>
  <IgnoreUnresolvedVariables>true</IgnoreUnresolvedVariables>
  <Variable name="request.content">
    <Pattern>[\s]*((delete)|(exec)|(drop\s*table)|(insert)|(shutdown)
|(update)|(\bor\b))</Pattern>
  </Variable>
  <JSONPayload>
    <JSONPath>
      <Expression>$.comment</Expression>
      <Pattern>[\s]*((delete)|(exec)|(drop\s*table)|(insert)
            |(shutdown)|(update)|(\bor\b))</Pattern>
    </JSONPath>
  </JSONPayload>
  <XMLPayload>
    ⋮
  </XMLPayload>
</RegularExpressionProtection>
```

The RegularExpressionProtection policy can be used to search for blocked patterns in the input request.

You can search inside variables or inside specific fields in an XML or JSON payload using XPath and JSONPath.

If any regular expression pattern in the policy matches the value in the corresponding location, the message is considered a threat, and the policy raises a fault. The API request should be rejected as a bad request.



Let's take a quick but important detour.

We've talked about using JSONPath and XPath to find specific fields inside a JSON or XML payload. How do your proxy's policies know whether the payload is JSON or XML?

You might say: if you see curly braces it's JSON, and angle brackets are XML. That's how humans tell the difference.

The proxy actually uses the Content-Type header.

The Content-Type header specifies which format is being used for the message. Apigee recognizes application/json as a JSON payload.

There are multiple formats for XML, including application/xml.

Text/plain indicates a plaintext payload.

As you use some of the powerful JSON and XML parsing functions in Apigee policies, remember that the Content-Type header must be set correctly at the time the policy is executed. For example, if you are trying to use JSONPath in a policy, and the Content-Type header is not application/json, that part of the policy will be silently skipped.

Content-Type header

- Content-Type header specifies the format of incoming payloads.
  - application/json
  - application/xml, text/xml, application/*+xml
  - text/plain
- JSON or XML parsing requires Content-Type header to be set correctly at the time policy is executed.

```
Payload:
{
  "message": "What format is this?"
}
```

Look at this example payload from an HTTP message. What format is it?

If you think it is a trick question, you're right.

It certainly looks like JSON, but we don't really know what the format is until we know what the content type is.

Content-Type header

- Content-Type header specifies the format of incoming payloads.
  - application/json
  - application/xml, text/xml, application/*+xml
  - text/plain
- JSON or XML parsing requires Content-Type header to be set correctly at the time policy is executed.

```
Content-Type: application/xml
Payload:
{
  "message": "This is invalid XML, NOT JSON!"
}
```

If the Content-Type is set to application/xml, this payload is invalid XML, not JSON.

If the Content-Type header is not set, the payload is also not considered JSON.

When creating an API that only uses JSON, you might want the default content type to be application/json when no Content-Type header is provided.

Content-Type header

- Content-Type header specifies the format of incoming payloads.
  - application/json
  - application/xml, text/xml, application/*+xml
  - text/plain
- JSON or XML parsing requires Content-Type header to be set correctly at the time policy is executed.

```
Content-Type: application/xml
Payload:
{
  "message": "This is invalid XML, NOT JSON!"
}
```

```
<Step>
  <Name>RF-ContentTypeInvalid</Name>
  <Condition>request.header.Content-Type != null AND
    request.header.Content-Type!="application/json"
  </Condition>
</Step>
<Step>
  <Name>AM-SetContentTypeToJSON</Name>
  <Condition>request.header.Content-Type == null
  </Condition>
</Step>
<!-- can now use JSON parsing -->
<Step>
  <Name>EV-ExtractFromJSON</Name>
</Step>
```

You can do this with a series of policies in a proxy.

The first condition is true if the content type header has a value and the content type is set to something other than application/json.

In this case, the caller has set a content type that is not allowed for this API.

The policy named RF-ContentTypeInvalid would raise a fault and cause an error to be returned for invalid content type.

Content-Type header

- Content-Type header specifies the format of incoming payloads.
  - application/json
  - application/xml, text/xml, application/*+xml
  - text/plain
- JSON or XML parsing requires Content-Type header to be set correctly at the time policy is executed.

```
Content-Type: application/xml
Payload:
{
  "message": "This is invalid XML, NOT JSON!"
}
```

```
<Step>
  <Name>RF-ContentTypeInvalid</Name>
  <Condition>request.header.Content-Type != null AND
    request.header.Content-Type!="application/json"
  </Condition>
</Step>
<Step>
  <Name>AM-SetContentTypeToJSON</Name>
  <Condition>request.header.Content-Type == null
  </Condition>
</Step>
<!-- can now use JSON parsing -->
<Step>
  <Name>EV-ExtractFromJSON</Name>
</Step>
```

The second condition is true if the Content-Type header is not set.

In this case, you could use the policy AM-SetContentTypeToJSON to set the Content-Type header in the request to application/json.

Content-Type header

- Content-Type header specifies the format of incoming payloads.
  - application/json
  - application/xml, text/xml, application/*+xml
  - text/plain
- JSON or XML parsing requires Content-Type header to be set correctly at the time policy is executed.

```
Content-Type: application/xml
Payload:
{
  "message": "This is invalid XML, NOT JSON!"
}
```

```
<Step>
  <Name>RF-ContentTypeInvalid</Name>
  <Condition>request.header.Content-Type != null AND
    request.header.Content-Type!="application/json"
  </Condition>
</Step>
<Step>
  <Name>AM-SetContentTypeToJSON</Name>
  <Condition>request.header.Content-Type == null
  </Condition>
</Step>
<!-- can now use JSON parsing -->
<Step>
  <Name>EV-ExtractFromJSON</Name>
</Step>
```

Now that you have a valid content type, the EV-ExtractFromJSON ExtractVariables policy will be able to parse JSON.

Parsing attacks

- XML and JSON payloads can be crafted to overwhelm parsers.
- JSONThreatProtection and XMLThreatProtection policies use string-based evaluation of the payload instead of parsing the payload.
- These policies should be run before doing any JSON/XML parsing.

XML and JSON payloads can be crafted to overwhelm parsers, causing application-level denial of service attacks.

The JSON and XMLThreatProtection policies use string-based evaluation of the payload instead of loading it into a parser.

By using string-based evaluation of the payload, you can detect XML or JSON payloads that exceed configured limits and reject the request before you ever load it into a parser.

It is important to run these protection policies before you attempt to use JSON or XML parsing at all.

For example, you may want to validate fields within your JSON by using JSONPath in an ExtractVariables policy.

You should use the JSONThreatProtection policy to confirm that the payload is safe before parsing it.

JSONThreatProtection policy

- Specify limits on JSON structures and fields.
- These limits are checked without the use of a parser.

```
<JSONThreatProtection continueOnError="false" enabled="true"
name="JTP-ValidateJSON">
  <Source>request</Source>
  <ArrayElementCount>20</ArrayElementCount>
  <ContainerDepth>10</ContainerDepth>
  <ObjectEntryCount>15</ObjectEntryCount>
  <ObjectEntryNameLength>50</ObjectEntryNameLength>
  <StringValueLength>500</StringValueLength>
</JSONThreatProtection>
```

The JSONThreatProtection policy allows you to specify limits on your JSON, like how deep your JSON can be nested, or how many elements can be in an array.

The policy will check for these structural limits by scanning through the text of the JSON object, without parsing the JSON.

JSONThreatProtection policy

- Specify limits on JSON structures and fields.
- These limits are checked without the use of a parser.
- The first exceeded limit results in an error.
- Craft limits to allow all good requests through.

```
<JSONThreatProtection continueOnError="false" enabled="true"
name="JTP-ValidateJSON">
  <Source>request</Source>
  <ArrayElementCount>20</ArrayElementCount>
  <ContainerDepth>10</ContainerDepth>
  <ObjectEntryCount>15</ObjectEntryCount>
  <ObjectEntryNameLength>50</ObjectEntryNameLength>
  <StringValueLength>500</StringValueLength>
</JSONThreatProtection>
```

```
{
  "fault": {
    "faultstring": "JSONThreatProtection[JTP-ValidateJSON]: Execution failed.
reason: JSONThreatProtection[JTP-ValidateJSON]: Exceeded object entry name
length at line 2",
    "detail": {
      "errorcode": "steps.jsonthreatprotection.ExecutionFailed"
    }
  }
}
```

The first time a limit is exceeded, the policy will raise a fault, allowing you to reject the request.

Only the first error encountered in the JSON will be mentioned in the response.

It is important to set limits that allow legitimate JSON payloads through, so you don't reject requests as false positives.

XMLThreatProtection policy

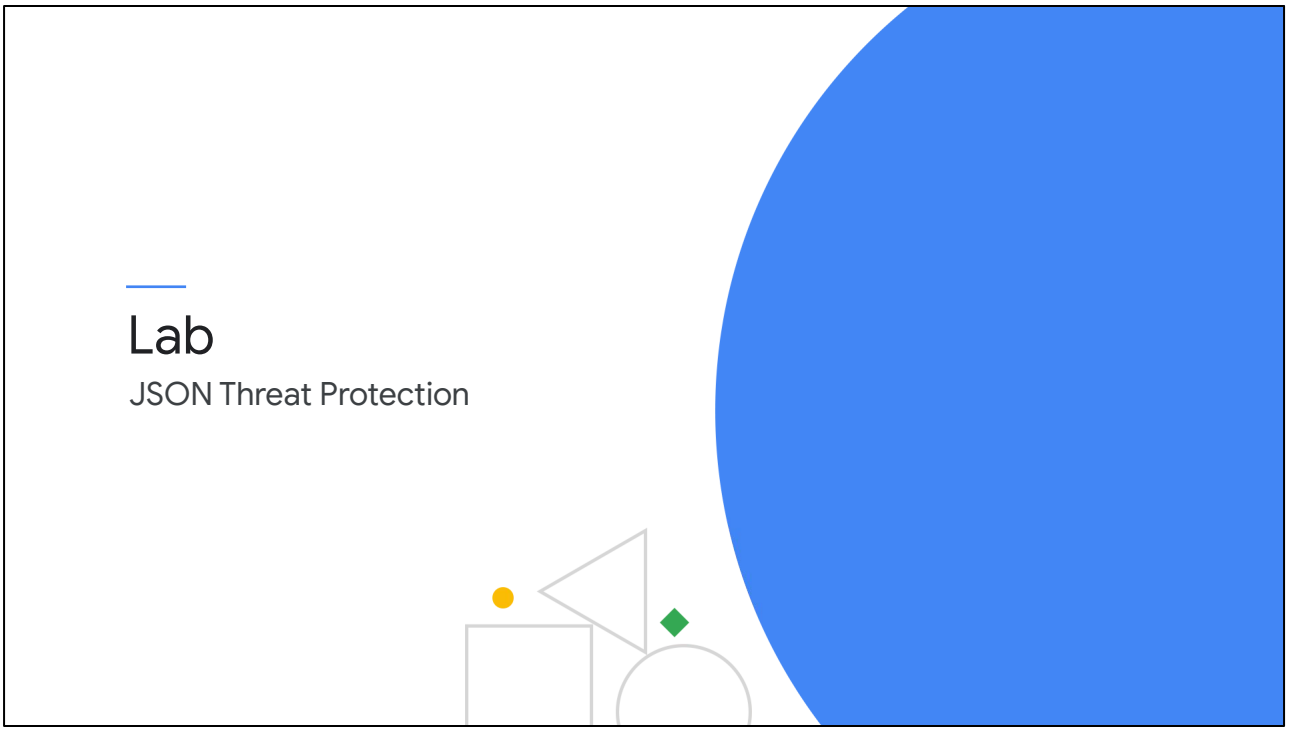
```
<XMLThreatProtection continueOnError="false" enabled="true" name="XTP-ValidateXML">
  <Source>request</Source>
  <NameLimits>
    <Element>10</Element>
    <Attribute>10</Attribute>
    <NamespacePrefix>10</NamespacePrefix>
    <ProcessingInstructionTarget>10</ProcessingInstructionTarget>
  </NameLimits>
  <StructureLimits>
    <NodeDepth>5</NodeDepth>
    <AttributeCountPerElement>2</AttributeCountPerElement>
    <NamespaceCountPerElement>3</NamespaceCountPerElement>
    <ChildCount includeComment="true" includeElement="true"
includeProcessingInstruction="true" includeText="true">3</ChildCount>
  </StructureLimits>
  <ValueLimits>
    <Text>15</Text>
    <Attribute>10</Attribute>
    <NamespaceURI>10</NamespaceURI>
    <Comment>10</Comment>
    <ProcessingInstructionData>10</ProcessingInstructionData>
  </ValueLimits>
</XMLThreatProtection>
```

- Functionality similar to JSONThreatProtection policy

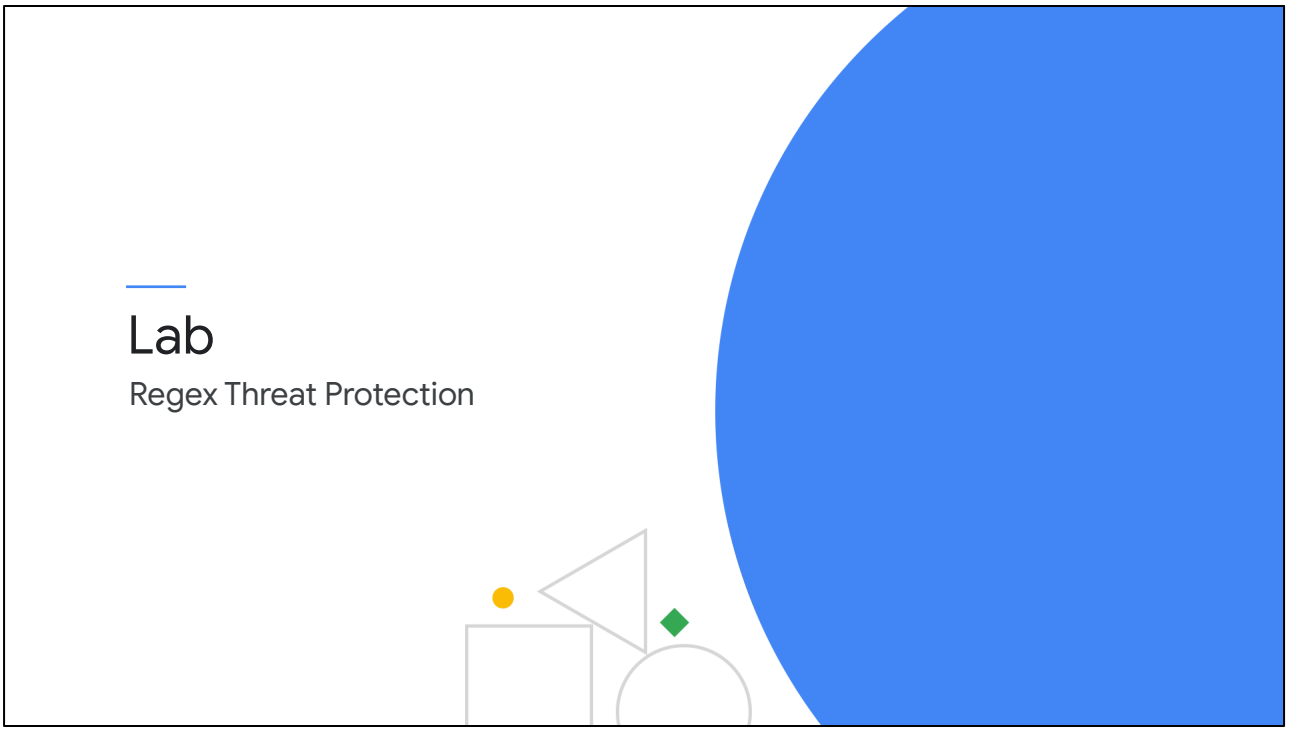
The XMLThreatProtection policy works exactly the same way as the JSONThreatProtection policy.

The XML payload is validated against configured limits without using a parser.

Note that the configuration elements are very different for XML, and there are many more options. This is because the XML and JSON formats are very different. The JSON format is simple, and the XML format is significantly more complex.



In this lab you add JSON threat protection to your retail API proxy. You will test with different payloads to see how the JSONThreatProtection policy's limits work.



In this lab you add a RegularExpressionThreatProtection policy to a new API proxy and test that the RegularExpressionThreatProtection policy rejects requests with data that matches the configured regular expressions.

During this lecture you will learn about Transport Layer Security, or TLS, which is the primary method of securing API requests and responses when sent across a network.

You'll learn about how TLS works, and how it is supported on Apigee. You'll also learn how to allow or deny traffic based on source IP address.

Transport layer security (TLS)

- Successor to Secure Sockets Layer (SSL).
  - SSL is deprecated
- Establishes encrypted http link between client and server (https).
- Certificates prove identity.
- All OAuth traffic must use TLS; recommended for all API traffic.

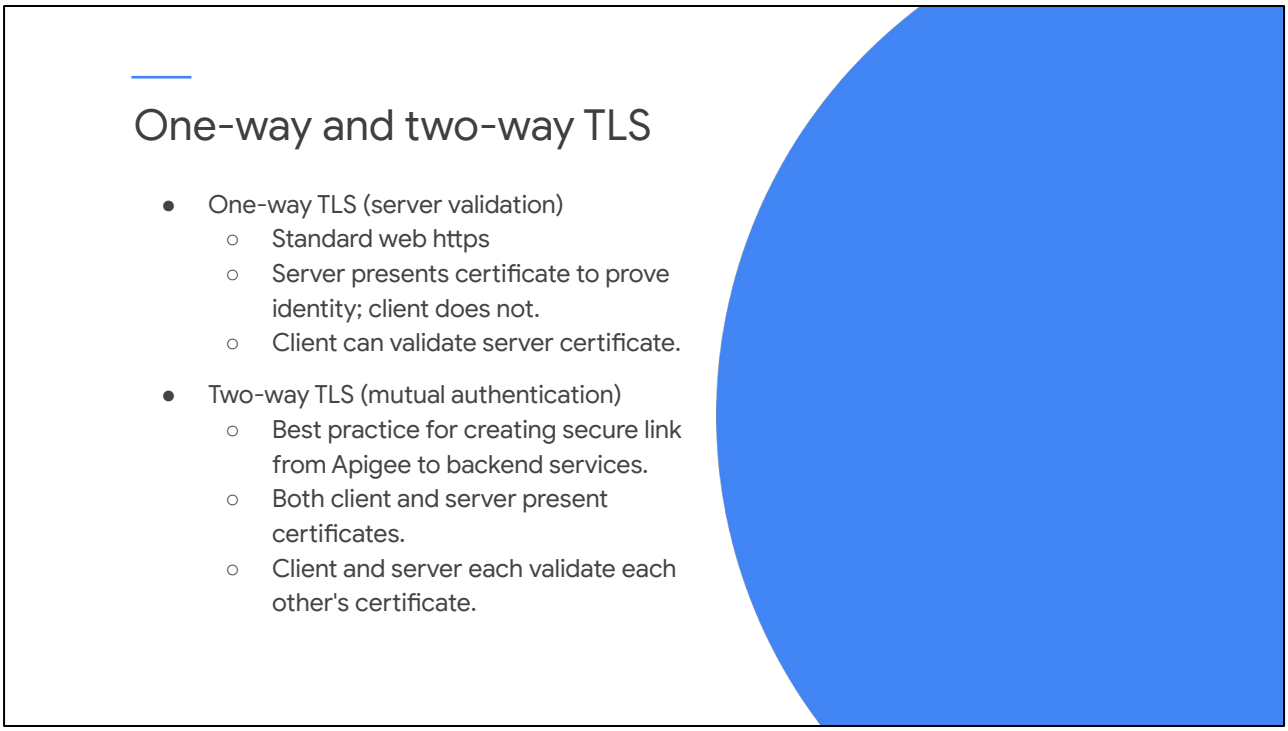
TLS is the successor to Secure Sockets Layer, also known as SSL.

When you hear someone talk about SSL, they are generally referring to TLS, because all versions of SSL have been deprecated due to vulnerabilities.

TLS establishes an encrypted link over http between a client and server. When you connect to a web page or API over https, you are using TLS.

TLS uses certificates with public and private keys to prove identity.

When we discussed OAuth, you learned that one of the firm requirements is that all OAuth traffic be sent using TLS, and, in fact, it is recommended to send all API traffic over TLS.



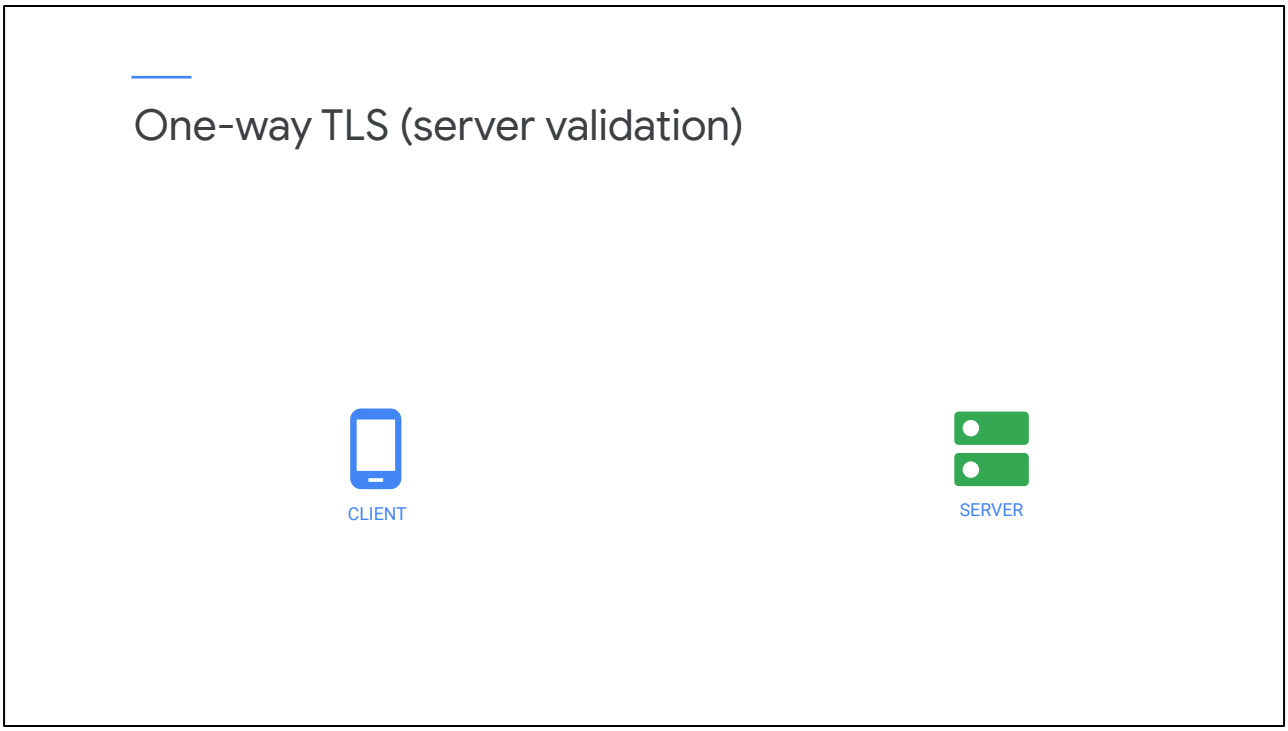
Two types of TLS connections can be made. They are commonly called one-way and two-way TLS.

One-way TLS, also called server validation, is probably very familiar to you. When you open a web page in your browser, and the request URL starts with https://, you are using one-way TLS. The server being contacted is required to present a certificate to the client to prove its identity.

For an API, we typically use something called a truststore on the client side to validate the certificate. For web requests, we trust the certificate because it has been signed by a trusted third-party certificate authority. Certificate authorities are outside the scope of this course.

Two-way TLS, also called mutual authentication, is the recommended method for securing the network connection between an Apigee proxy and the backend services it uses. Both the client and server present certificates, and each can validate the other's certificate.

Because your backend typically needs to let traffic through the firewall, it is important to validate that backend requests are coming from a legitimate source.



Let's look at one-way TLS, and how a client can trust a server.

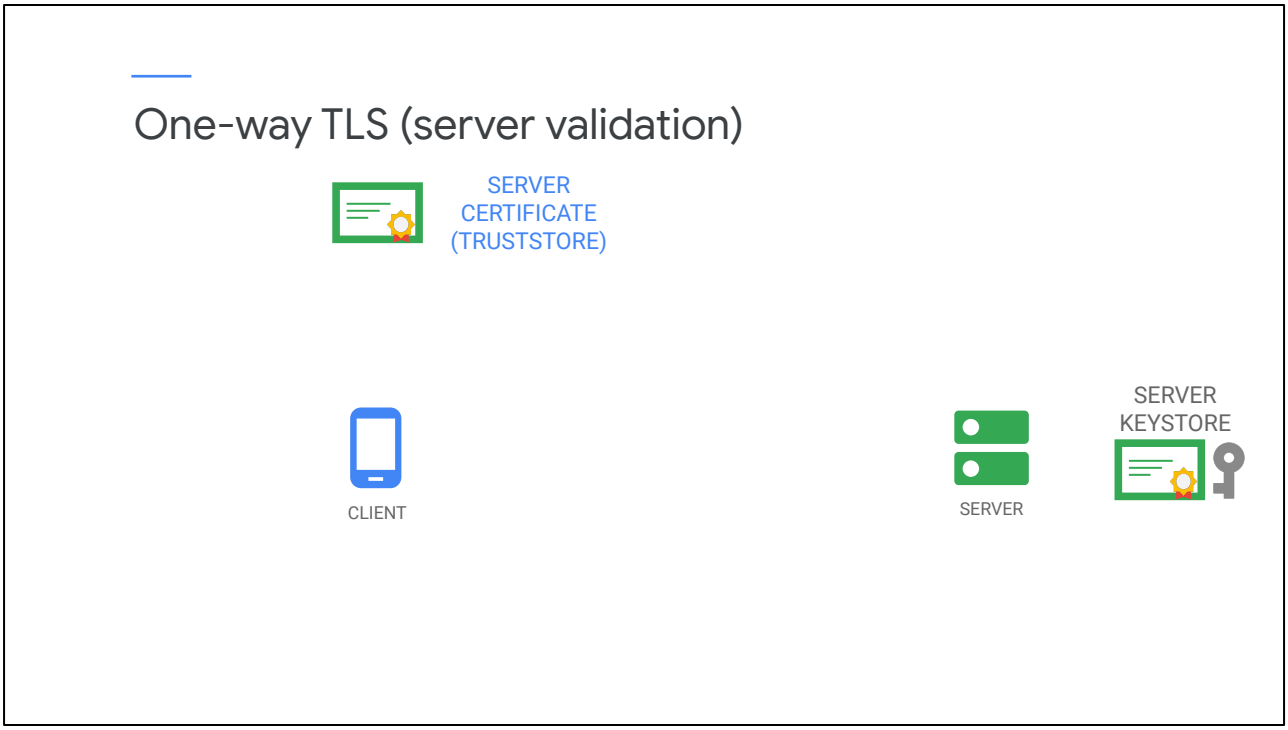
We are calling the participants the client and the server.

The client will initiate the request. Even though the client is represented in this diagram with a mobile device icon, the client could also be an Apigee proxy, with the server being a backend or third-party service.

One-way TLS (server validation)

For one-way TLS, the server will need to present a certificate to the client. This certificate, which contains a public key, will be stored in a keystore on the server side.

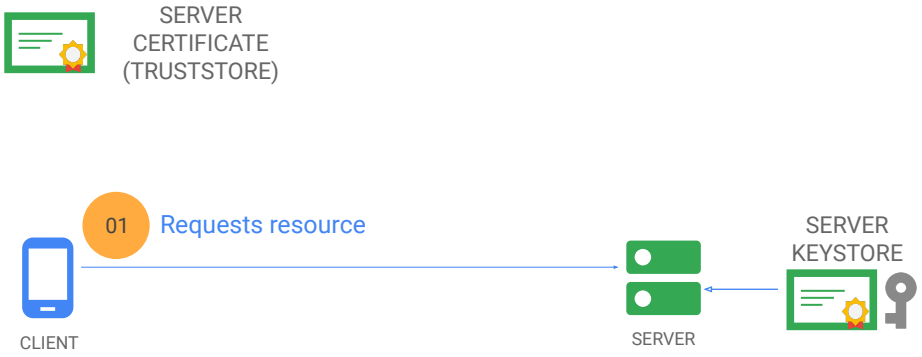
In addition, the keystore will contain the private key associated with the server certificate.



The client will need to validate the certificate from the server.

The server's certificate or chain of certificates can be stored in a truststore.

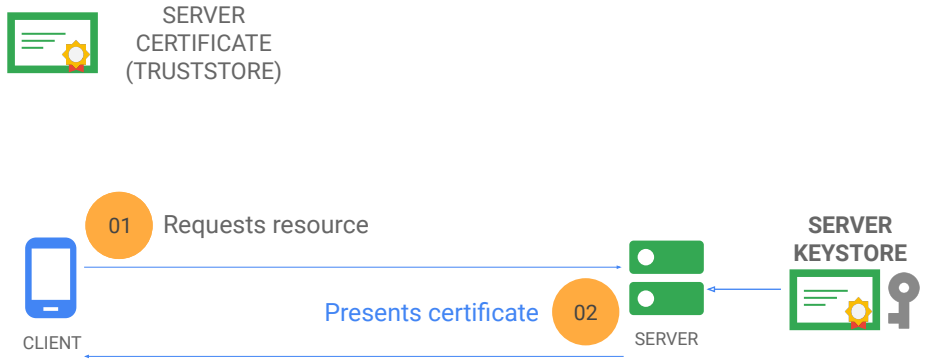
One-way TLS (server validation)



First, the client sends a request to access a resource on the server.

Before creating the encrypted connection, the server must prove its identity to the client.

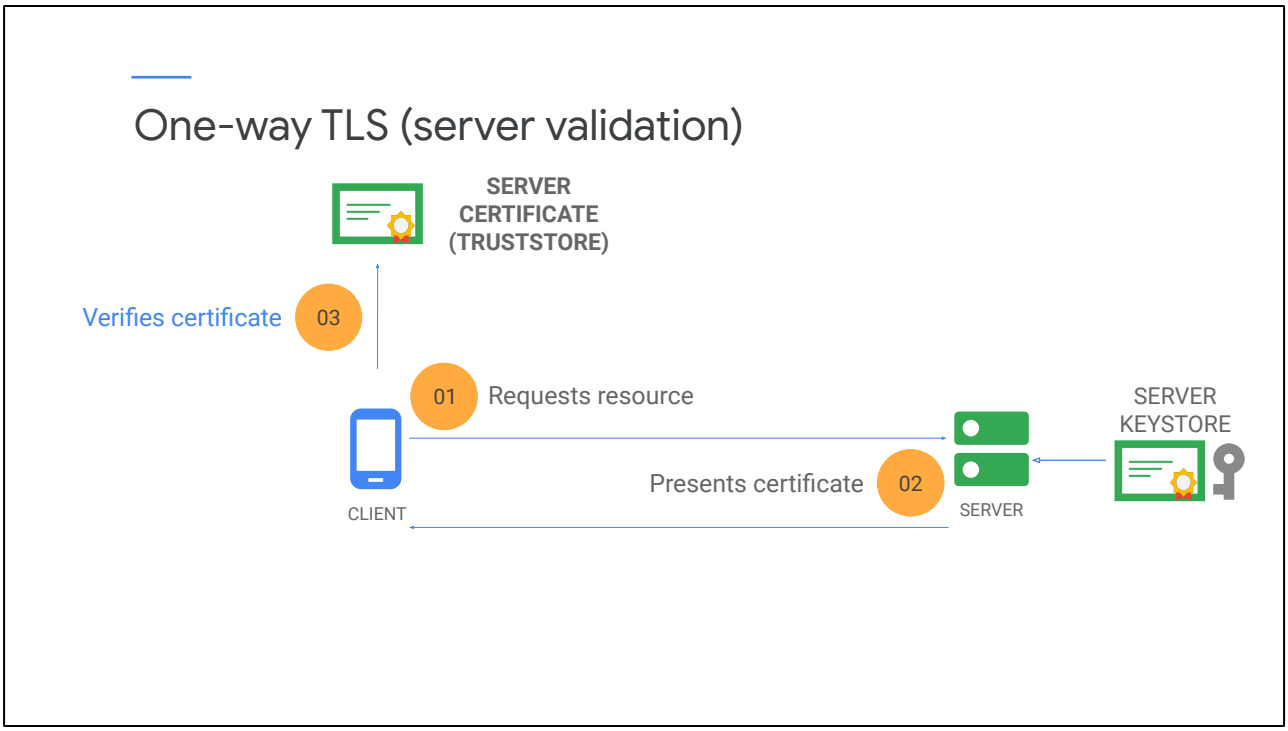
One-way TLS (server validation)



The server will present its certificate containing its public key to the client.

The certificate and public key are presented to any client connecting to the server, so the certificate is not a secret.

However, the server is the only entity that should have the associated private key.



The client will confirm that the certificate is the expected one by validating it against the truststore.

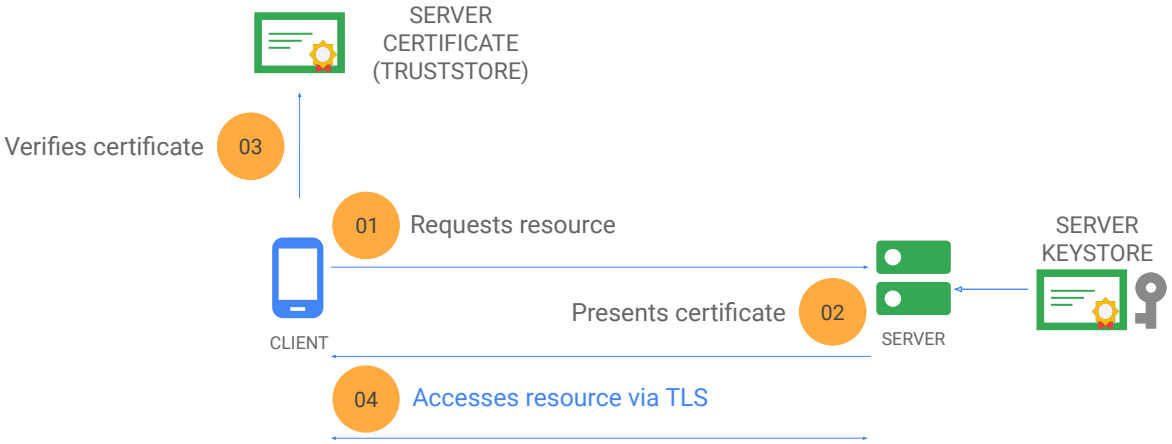
Note that a simplified, logical version of the communication between client and server is shown here; the actual TLS handshake is a bit more complex.

During this handshake, the client will typically encrypt some random data using the public key from the server certificate and send it to the server.

When the server proves to the client that it can decrypt the data, the client knows that the server must have the private key, and is therefore the legitimate holder of the certificate.

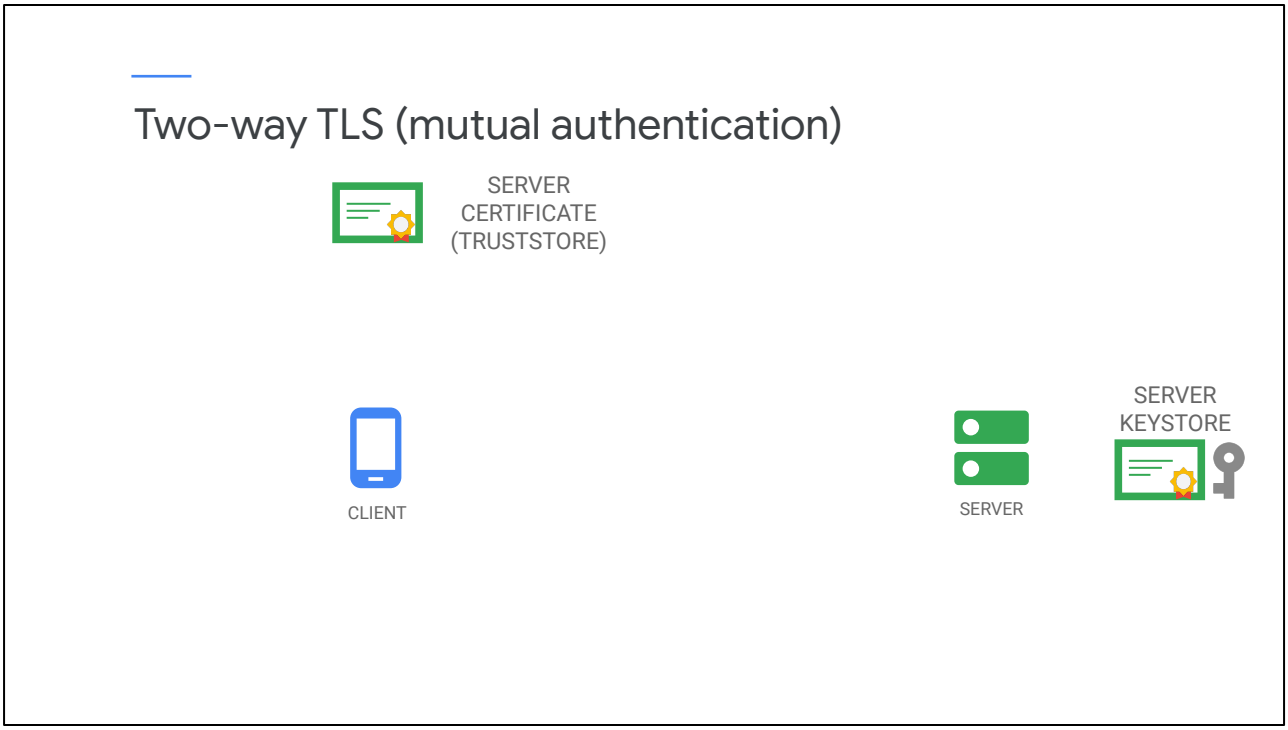
In addition to proving that the server has the private key, the two sides also negotiate the encryption cypher for the handshake and the symmetric keys that will be used to encrypt traffic across the network.

One-way TLS (server validation)



If the client is confident that the server is legitimate, the encrypted connection setup will be completed, and the client can access the resource via TLS.

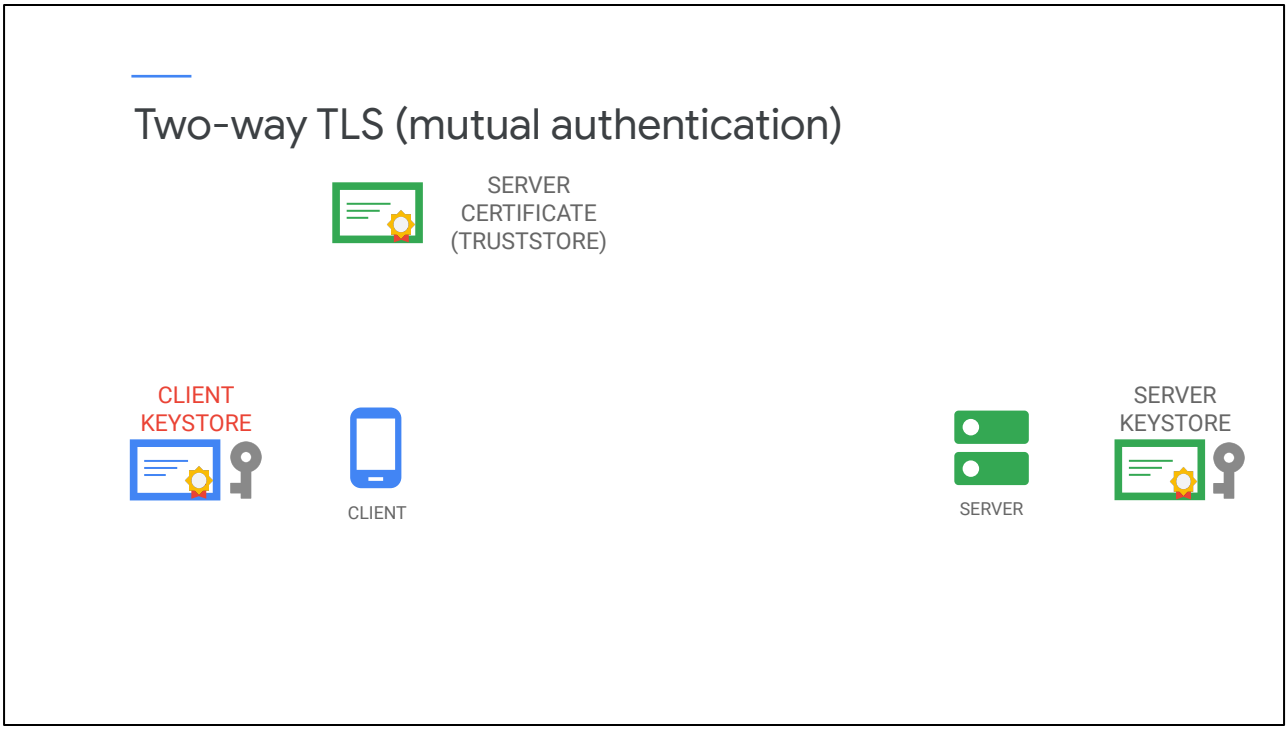
The TLS connection between client and server can remain up for future communication between client and server.



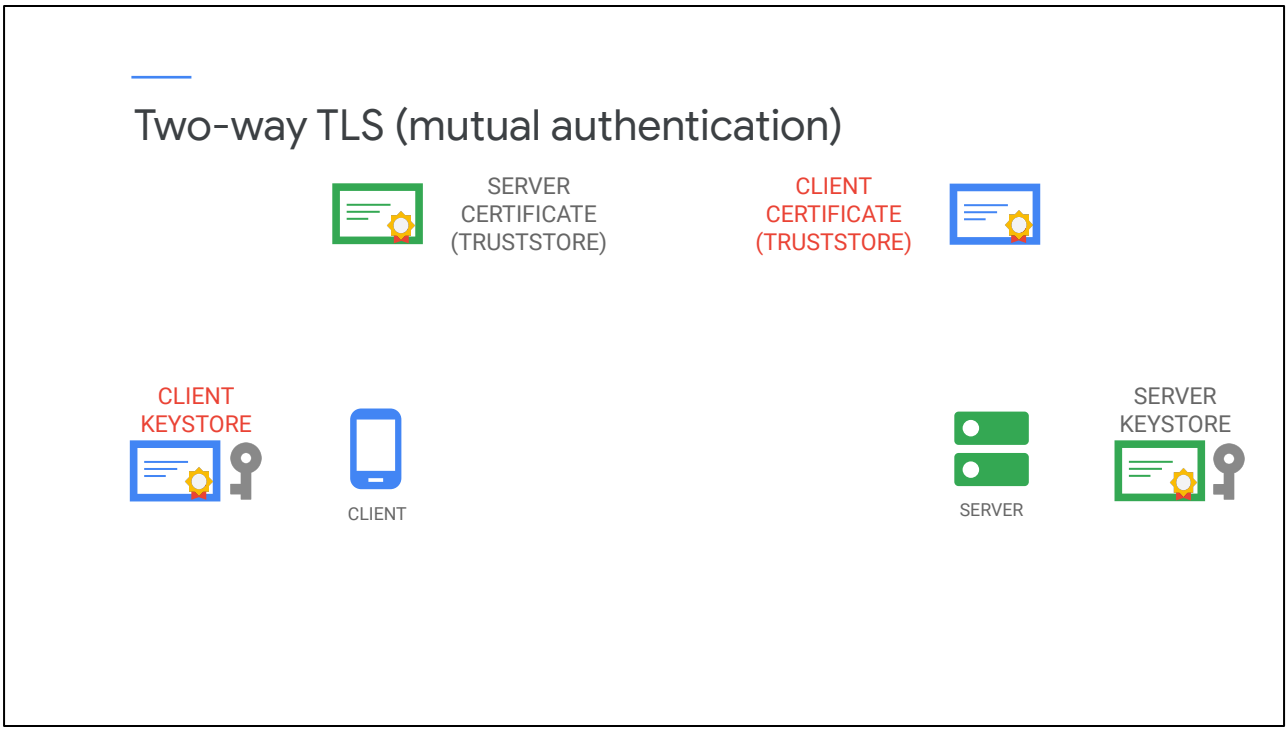
Let's see how two-way TLS is set up between client and server.

This two-way TLS is client validation layered on top of one-way TLS.

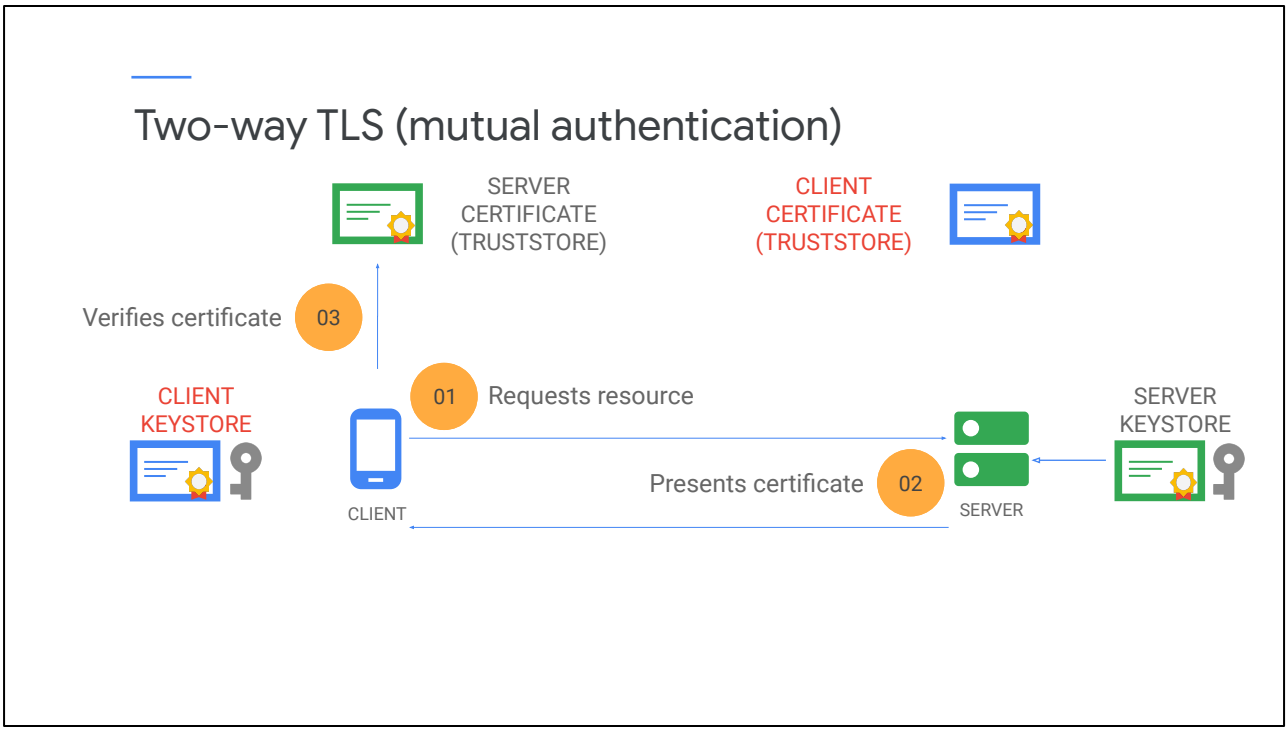
We still have the server's keystore and the client's truststore as before.



In addition, the client will need to present a certificate and encrypt using its private key, so there will be a client keystore.

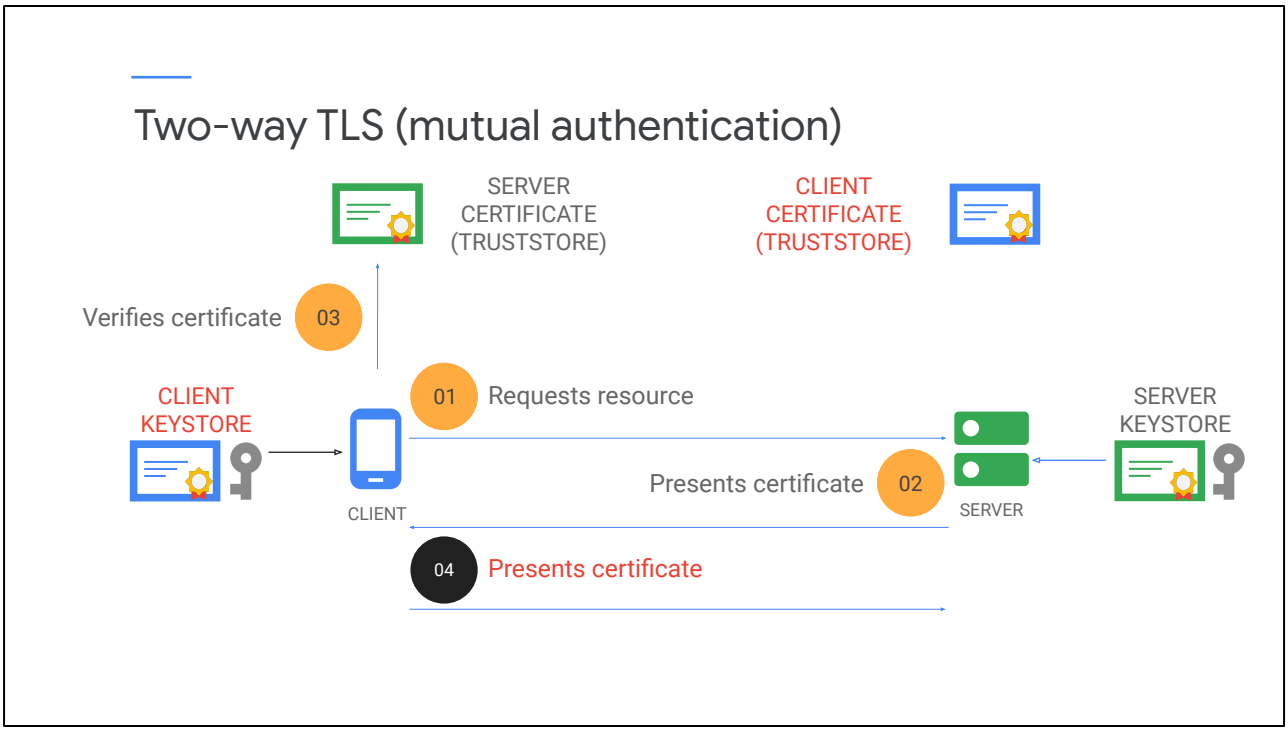


The server will need to validate that client certificate, so it will have a truststore.



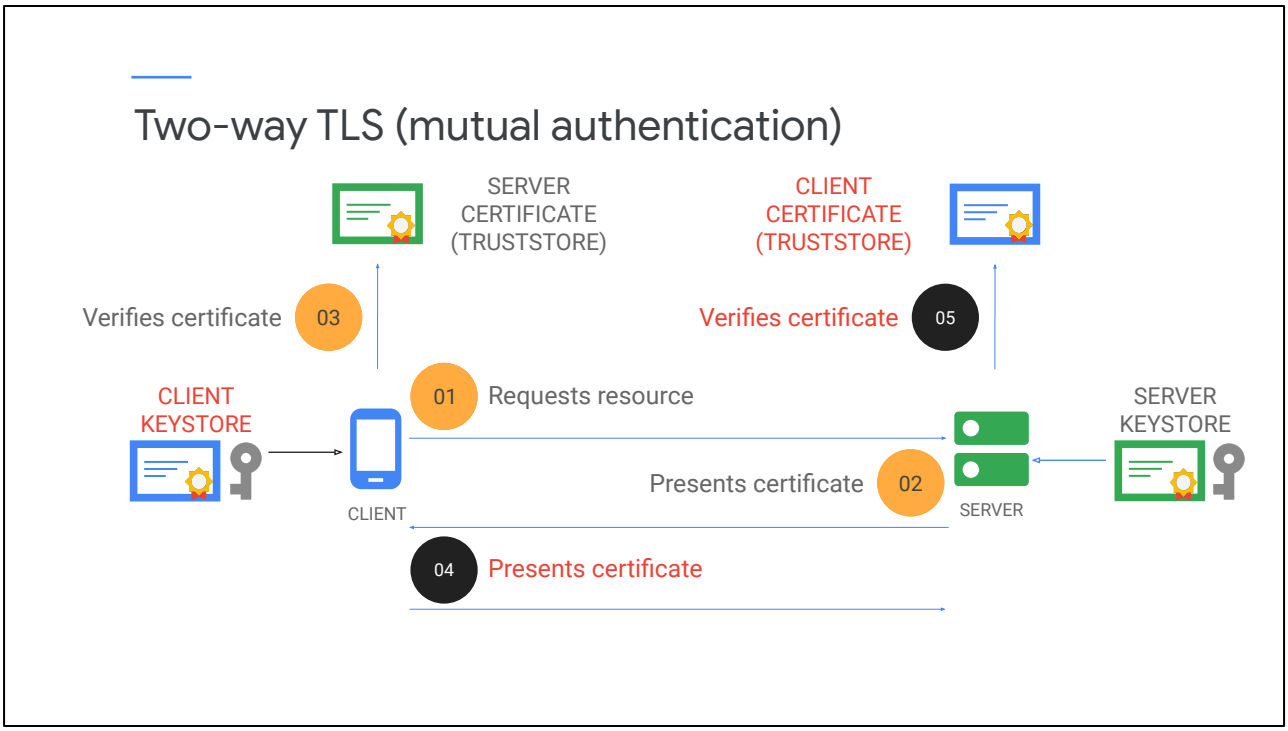
Steps 1 through 3 of the interaction are the same as before.

The client requests a resource, and the server presents its certificate and proves it has the private key.



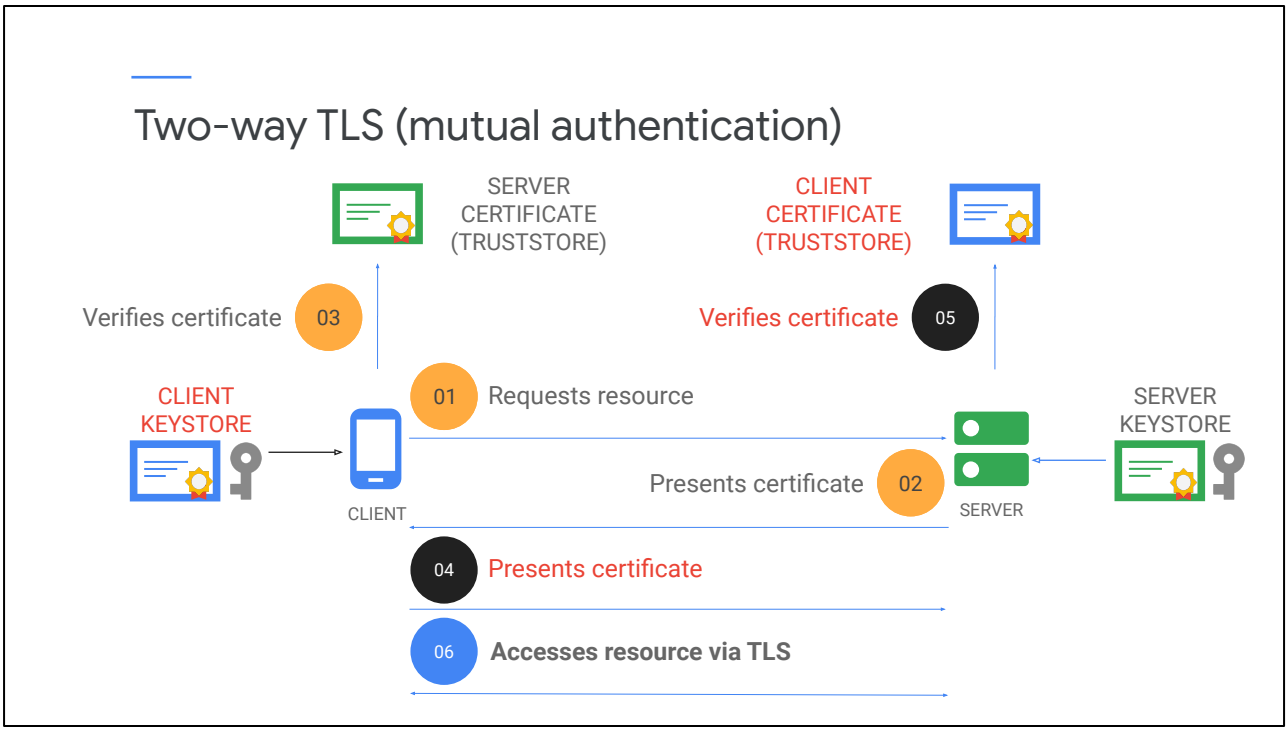
After the client is convinced of the authenticity of the server, the client needs to prove its identity.

The client takes its certificate from the keystore and presents it to the server.



The server will validate the client's certificate against its trust store.

During the handshake, the validity of the associated private key will also be proven.



Once each side is convinced of the other's identity, the encrypted TLS connection setup can complete, and the client can securely access resources on the server.

Keystores and truststores

- Keystore:
  - Stores certificates to be presented to remote server.
  - Also stores private key to prove identity.
- Truststore:
  - Stores certificates to compare with remote certificates.

On Apigee, you'll create keystores to store certificates and private keys to prove the Apigee proxy's identity over secure connections.

You'll also create truststores to store certificates that are expected from remote participants, so the proxy can verify that it is communicating with the correct participant.

Keystores and truststores

- Keystore:
  - Stores certificates to be presented to remote server.
  - Also stores private key to prove identity.
- Truststore:
  - Stores certificates to compare with remote certificates.
- Configuring TLS for Apigee
  - App ➔ Apigee
    - Configured on load balancer in Google Cloud project
  - Apigee ➔ Backend
    - Configured in target endpoints/target servers
    - Uses truststore (one- and two-way) and keystore (two-way only)

For incoming traffic, TLS should be configured on a load balancer in the Google Cloud project.

For Apigee communication with a backend, the TLS configuration will be set up in the TargetEndpoint in the proxy or in a TargetServer configuration referenced by the proxy.

For one-way or two-way TLS, a truststore is used to store trusted backend certificates.

For two-way TLS, an Apigee keystore is used to store the private keys and the certificates to be presented to the backend service.

References

```
<TrustStore>ref://truststore-reference</TrustStore>
<TrustStore>truststore-name</TrustStore>
```

- A keystore or truststore may be specified by using a keystore or truststore name or a reference.
- References are variables containing the name of the keystore or truststore.
- If a reference is not used, a proxy must be undeployed and redeployed to change the keystore or truststore for a target.
  - To change a keystore or truststore for a virtual host, servers must be rebooted.
- References allow key and certificate rotation without downtime.

When you use a keystore or truststore on Apigee, you have two choices: specify by using the keystore or truststore name, or by using a reference.

A reference is a variable containing the name of a keystore or truststore. References are configured within the scope of an environment.

If you use a name in your proxies instead of a reference, changes to the certificates and private keys will only be picked up after the proxy is undeployed and redeployed.

With a reference, a new keystore or truststore with the new certificates and keys can be created, and the reference can be updated on the fly without downtime for your proxies.

Rotating keys and certificates is a best practice, so we recommend that you always use references.

Configuring one-way or two-way TLS for targets

- By default, backend certificate will not be validated.
- To validate a backend certificate, include truststore with target certs.

```
<HTTPTargetConnection>
  <URL>https://internal-test.example.org/store</URL>
  <SSLInfo>
    <Enabled>true</Enabled>
    <TrustStore>ref://backend-truststore</TrustStore>
  </SSLInfo>
</HTTPTargetConnection>
```

When you create a target definition, either in a proxy or in a target server, the backend certificate will not be validated by default. This means that Apigee will not validate that the certificate has expired, that the certificate's common name matches the hostname in the URL, or that it has been signed by a trusted certificate authority.

In order to validate the backend certificate, you must configure a truststore, preferably using a reference. This truststore must contain the server's certificate or a certificate chain. If the server's certificate is signed by a third party, you would need to upload the entire certificate chain, up to the root certificate authority, or CA, certificate.

Unlike a web browser, Apigee does not implicitly trust any certificate authorities.

Configuring one-way or two-way TLS for targets

- By default, backend certificate will not be validated.
- To validate a backend certificate, include truststore with target certs.
- Use a keystore and key alias to present a client certificate to the backend to prove the identity of the proxy.

```
<HTTPTargetConnection>
  <URL>https://internal-test.example.org/store</URL>
  <SSLInfo>
    <Enabled>true</Enabled>
    <TrustStore>ref://backend-truststore</TrustStore>
  </SSLInfo>
</HTTPTargetConnection>
```

```
<HTTPTargetConnection>
  <URL>https://internal-test.example.org/store</URL>
  <SSLInfo>
    <Enabled>true</Enabled>
    <TrustStore>ref://backend-truststore</TrustStore>
    <ClientAuthEnabled>true</ClientAuthEnabled>
    <KeyStore>ref://proxy-keystore</KeyStore>
    <KeyAlias>edgeKey</KeyAlias>
  </SSLInfo>
</HTTPTargetConnection>
```

It is typically recommended to have the server validate the proxy's identity using two-way TLS.

The truststore is configured the same way as for one-way TLS. In addition, the target's ClientAuthEnabled element should be set to true, and a keystore and key alias should be configured.

The keystore contains the certificate and private key. You should configure the keystore as a reference.

The KeyAlias is the name of the certificate and key within the keystore. Multiple certificate and key pairs can be stored in the same keystore by using different key alias names.

Key aliases cannot be specified by reference, so a new keystore should use the same key alias name when used for certificate rotation.

AccessControl policy

```
<AccessControl continueOnError="false" enabled="true"
name="AC-WhitelistIPs">
  <ClientIPVariable>request_ip</ClientIPVariable>
  <IPRules noRuleMatchAction="DENY">
    <MatchRule action="ALLOW">
      <SourceAddress mask="20">172.217.32.0</SourceAddress>
      <SourceAddress mask="16">173.194.0.0</SourceAddress>
    </MatchRule>
    <MatchRule action="ALLOW">
      <!-- use app custom attributes for CIDR -->
      <SourceAddress mask="verifyapikey.VK-VerifyKey.app_cidr_mask">
{verifyapikey.VK-VerifyKey.app_cidr_addr}</SourceAddress>
    </MatchRule>
  </IPRules>
</AccessControl>
```

- IP allow/deny lists for ranges of IPs.
- Specify one or more rules to be evaluated in order.
- noRuleMatchAction specifies default functionality.
- ClientIPVariable may be used to specify the IP address to check.

An additional method to restrict incoming connections to your API proxies is to use the AccessControl policy.

Allow and deny rules for IP addresses and IP address ranges can be specified, and they are evaluated in order.

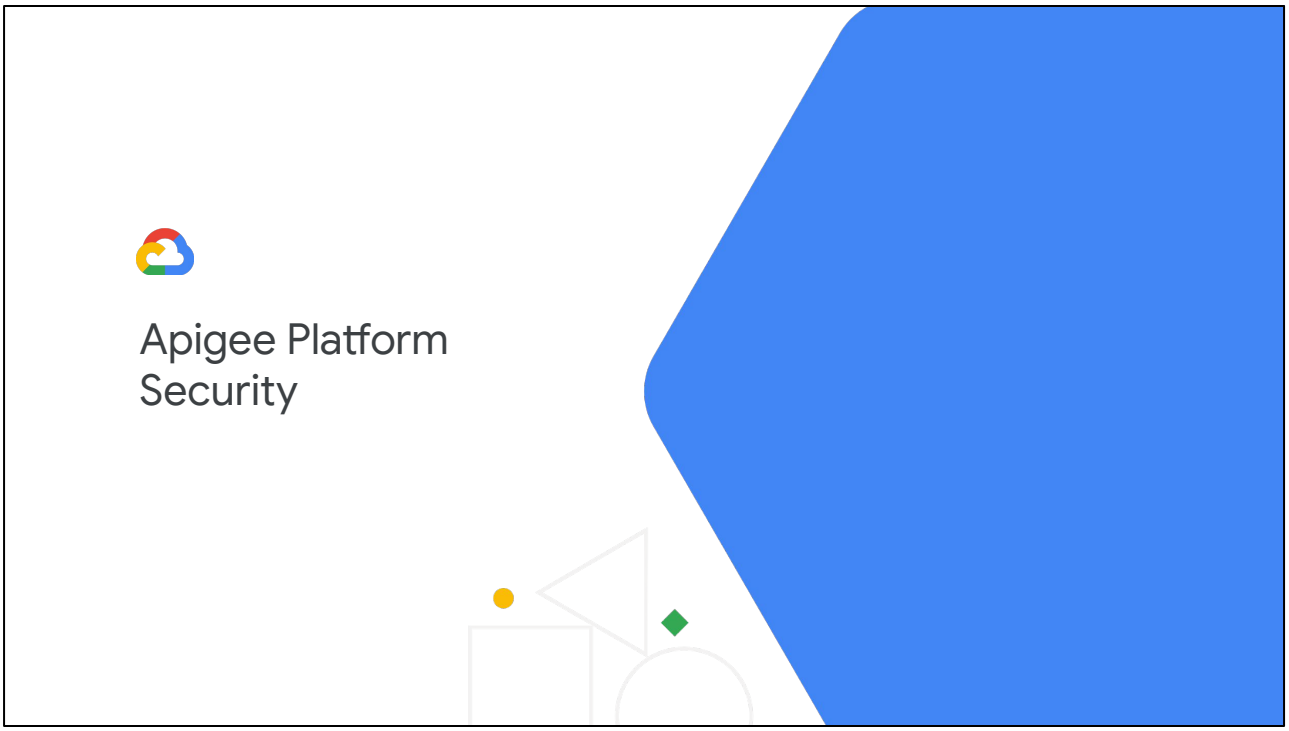
The action of the first matching rule determines whether the traffic is allowed or denied.

Address and address ranges in rules can be hardcoded in the policy or specified using variables.

The noRuleMatchAction element specifies whether the default behavior is to allow or deny traffic if none of the rules match.

Note that the IP address that is validated may be found in a header, like the X-Forwarded-For header, rather than using the actual connected IP address. If Apigee is fronted by a load balancer, the connection IP address would be from the load balancer and not the original request. Load balancers and proxies typically add the upstream IP address to the X-Forwarded-For header.

Alternatively, you can specify the client IP to be verified in the ClientIPVariable element.



You've learned quite a bit about securing APIs from external threats.

Now we'll discuss platform security, which protects internal access.

Cloud Identity and Access Management, or IAM, is used to grant access to an Apigee organization to Google Cloud user accounts using Apigee roles.

Data masking and private variables can be used to prevent sensitive data from being visible while live traffic is being traced.

And key value maps can be used to store and use configuration data like credentials without allowing users of the Apigee platform to see the values.

Users

- Apigee users are managed using Cloud Identity and Access Management (IAM) users in the customer-managed project.
- In IAM, access control is managed by defining who has what access for which resource.
- The Apigee organization, as well as the entities it contains, are resources within the customer-managed project.

Apigee users are managed using Google Cloud's Identity and Access Management, or IAM.

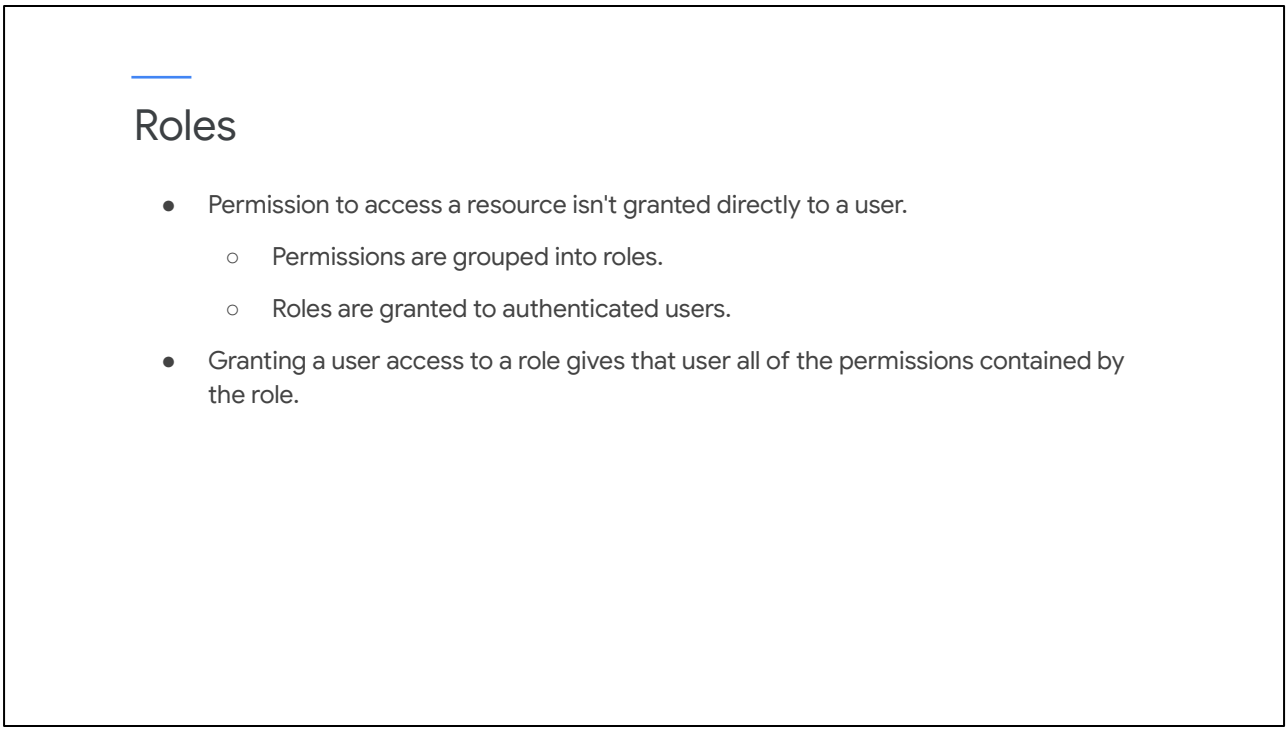
Apigee users are configured as user accounts within the customer-managed project that is tied to the Apigee organization.

In Cloud IAM, we think of access control as defining who has what access for which resource.

The Apigee org is tied, one-to-one, with the customer-managed project that was used to create it.

The Apigee org, and the entities it contains, are resources within the customer-managed project.

When we refer to an Apigee user, we are referring to an authenticated user account that can access an organization and some or all of the entities within the organization.



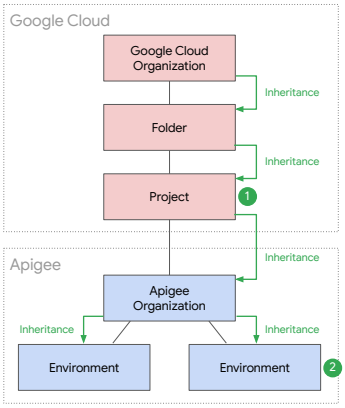
Permission to access a specific resource in Google Cloud is not granted directly to a user. This could be a maintenance nightmare if we needed to specifically grant permissions for each resource to each user.

Instead, permissions are grouped into roles, and then a role may be granted to an authenticated user.

A role can therefore be thought of as a collection of permissions. Granting a user access to a role specifically provides the user with all of the permissions contained by the role.

Role inheritance

- Any Apigee roles attached to the project are automatically available for the organization and contained environments.
- Within the Apigee console, environment-specific roles may be given to IAM users that are defined at the project level.



Within Google Cloud, the resource hierarchy is made up of organizations, folders, and projects. For most companies, the root of the resource hierarchy is a Google Cloud organization. Inside that organization is a hierarchy of folders and projects. Folders can only be created in an organization or inside other folders. Projects can also be created without an organization, in which case the project is the root element. Resources are created inside projects.

Organizations, folders, and projects provide places to attach and inherit roles. Permissions at a higher level in the hierarchy are inherited by lower level entities. For example giving a user a role in a folder provides those role permissions for any projects and resources the folder contains. All Google Cloud resources, like virtual machines, databases, and Apigee, are contained in a project.

An Apigee organization is contained in a single customer project. Environments for that Apigee organization are contained in the organization. A Google Cloud organization and an Apigee organization are different. In this course, when we refer to an organization, we are referring to an Apigee organization, unless otherwise specified.

The inheritance pattern for Apigee follows the inheritance of the resource hierarchy. Roles that are given in a project are automatically inherited for the Apigee organization, and any roles inherited by the Apigee organization are inherited by its environments. There are two locations in which Apigee roles are attached.

The first location is at the project level. Any Apigee roles attached to the project are automatically available for the organization and all contained environments.

The second location is in a specific environment. Within the Apigee console, environment-specific roles can be given to IAM users defined at the Project level. The access given in an environment is the union of the access provided at the organization and the specific environment.

Apigee roles

- Several pre-defined roles for specific types of Apigee users
  - Apigee Organization Admin: full read-write access
  - Apigee Read-only Admin: full read-only access
  - Apigee API Admin: developer who creates and tests API proxies
  - Apigee Developer Admin: manages API products, developers, apps, and keys
  - Apigee Environment Admin: deploys and undeploys API proxies
- Project Owner has Organization Admin access
- Can create custom roles to support the Principle of Least Privilege

There are several pre-defined roles created for Apigee users.

An Organization Admin, or Org Admin, has full read-write access to the organization. A Read Only Admin has full read access.

An API Admin has the correct privileges for a developer who creates and tests proxies. This role provides the ability to edit proxies, shared flows, and key value maps.

A Developer Admin manages app developer access, editing API products, app developers, apps, and app keys.

An Environment Admin manages API proxy deployments and environments, providing edit access to entities like shared flows, flow hooks, key value maps, and target servers. In addition, the Environment Admin can deploy and undeploy API proxies.

Note that the owner of a project has full read-write access like an Org Admin.

Google recommends the Principle of Least Privilege, where a user is only given the minimum set of privileges necessary to complete their job. If one of the pre-defined roles does not provide the correct level of access, you can create a custom role containing only the permissions you need for that role.

Data masking

- Trace tool allows users to see data being accessed during API calls, including sensitive data.
- Data masking can block fields from being viewed.
- Data masking is configured using the DebugMask Apigee API.
- Remember to mask sensitive data!

Use of the Apigee trace tool is vital for troubleshooting issues with your API. However, the user tracing live API traffic can, by default, see all of the fields that are being accessed during the API calls. This data can include sensitive user data, including names, passwords, or credit card numbers. A user can also see credentials that are being used to communicate with backend services. When you download a trace log, those values will also be in the trace file.

Data masking can block configured data from being visible in live trace or trace files. You specify certain patterns of field or variable names, and matching data will be masked using a series of asterisks.

Data masking is a feature that cannot be controlled using the Apigee console. Data masks are set up using the DebugMask Apigee API. Data masks are configured at the environment level, and these masks will be active for all APIs in the environment.

Data masks are not visible in the console, so API teams sometimes forget about them. Protecting data is an important part of your API security, so you should create data masks for your environments and ideally store the data masks in source control.

DebugMask singleton

PATCH /v1/organizations/{org}/environments/{env}/debugmask

```
{
  "name": "organizations/myorg/environments/myenv/debugmask",
  "requestJSONPaths": [ "$.logonPassword", "$.ccNumber" ],
  "variables": [ "password" ],
  "responseJSONPaths: [ "$.username" ]
}
```

Request Content

Body	{"logonPassword":"**********","lastName":"Smith","fi

A DebugMask is a singleton object in an Apigee environment.

Data masks are created by patching the singleton object, which is named "debugmask."

The payload for the DebugMask contains a list of variables and JSONPath or XPath expressions for API requests or responses. In this case, one of the masked fields is the logonPassword at the root level of an incoming JSON request.

When tracing, you'll see the masked value replaced with asterisks. A downloaded trace file will also have the data masked.

Private variables

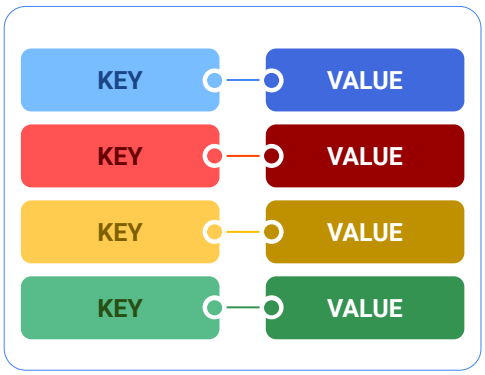
- *private.{varname}* is a private variable.
- Used like any other variable, but values do not show up in trace when created or accessed.
- When a private variable is assigned to another variable, the value is visible in the new variable.

Another way to hide sensitive information while tracing is to use private variables. A private variable is created by using a prefix of "private dot" in the variable name. So, private.password is a private variable.

A private variable can be used like any other variable, but, when an API is traced, the data value of a private variable is automatically masked.

Note that when you assign a private variable to another variable, the value will be visible when the non-private variable is accessed.

Key Value Maps (KVMs)



- Storage for non-expiring data retrieved at runtime.
- Keys and values are strings.
- Typically environment-scoped.
  - Ideal for environment-specific configuration
- Create or delete KVMs using Apigee API or console.
- Read/update/delete KVM entries via policy only.

Key value maps, or KVMs, are used to store non-expiring configuration data for use by proxies at runtime. You can think of a KVM as a replacement for a property file.

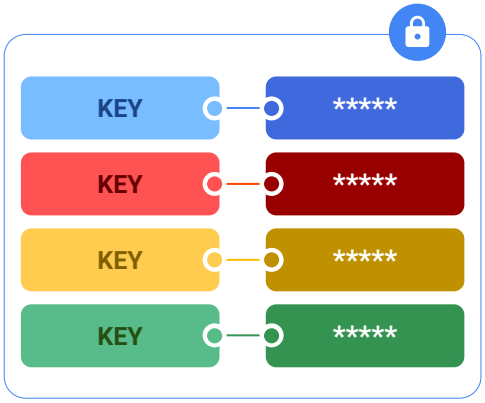
Both the key and the value for a key value map entry must be a string. You can convert the value to another data type, like a number, inside the proxy.

KVMs can be scoped to an organization, an environment, or a specific proxy, but environment-scoped KVMs are the most common. The Apigee console only allows you to create environment-scoped KVMs. KVMs are ideal for environment-specific configuration.

You can create or delete KVMs using the Apigee API or the Apigee console.

You can only add, update, or delete KVM entries using the KeyValueMapOperations policy.

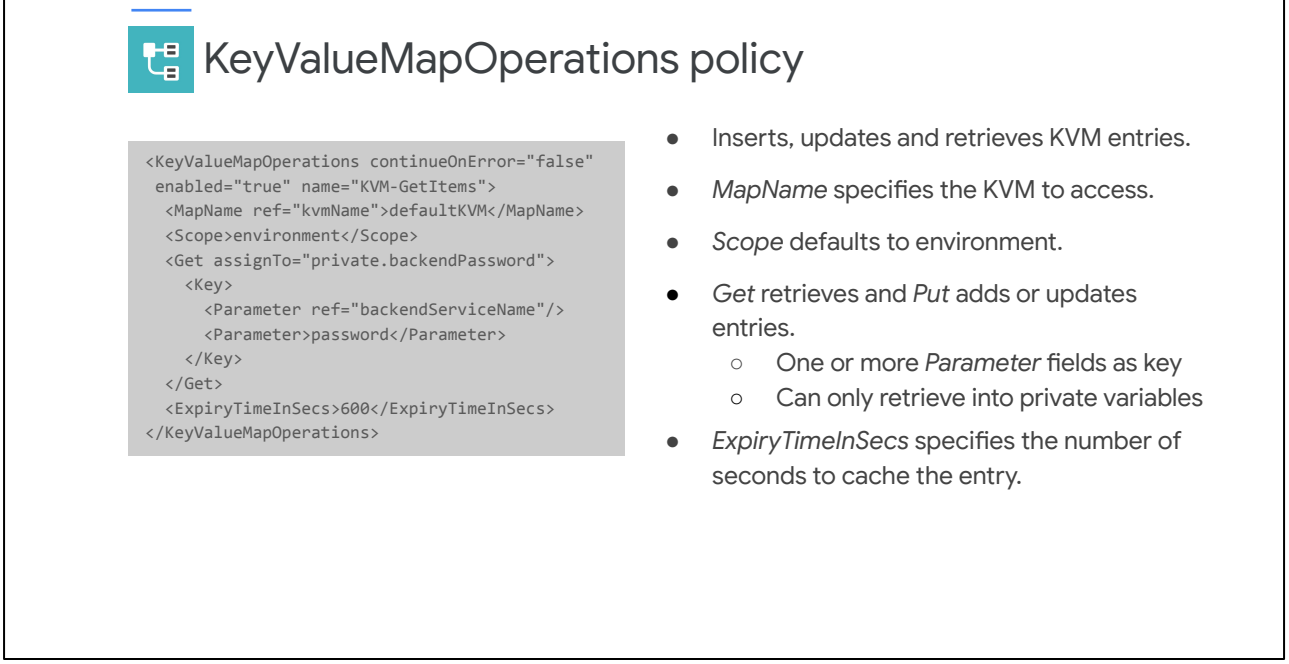
KVMs are encrypted



- Safe for sensitive data, like backend credentials.
- Can only retrieve values into private variables.

The key value map values are encrypted, so KVMs are safe for sensitive data, like backend credentials.

Because KVMs often do store sensitive data, you can only retrieve values into private proxy variables.



The KeyValueMapOperations policy can be used to access and update KVM data from within a proxy.

This policy can insert, update, or retrieve data from KVMs.

The MapName field specifies the KVM to access. The name can be specified from a variable or as a hardcoded value. In this case, the variable "kvmName" is checked first, and if the variable does not exist or is empty, then the string "defaultKVM" will be the name of the KVM.

Scope can be used to select an organization, environment, or API proxy-scoped key value map. The default scope, if not specified, is environment.

Entries are added or updated using a Put element, and retrieved by using a Get element.

One or more parameter fields are specified as your key, and each of these fields can be hardcoded or read from a variable. In the example, the backend service name is coming from a variable, but password is a hardcoded string.

Remember, when retrieving data from a KVM, you must use assign the KVM entry value to a private variable, or the policy will throw a runtime error.

Expiry time in seconds specifies how long to cache the retrieved or updated entry. In

this case, the entry is cached for 600 seconds. If the next Get for the matching entry happens within 600 seconds, or 10 minutes, a cached value will be used rather than reading from the database. Cached reads are significantly quicker than those from the database, but database changes may not be picked up until the cache entry has expired. If the entry is read from cache, the expiration time will not be extended.

Property sets

- Custom collection of key/value pairs for use in API proxies
- Property sets are specified using .properties files
- Used for non-expiring data that should not be hardcoded in an API proxy
- Can be scoped to an API proxy or to all API proxies deployed in an environment
  - Updating an API proxy-scoped property set requires redeployment
- Accessed using flow variables (propertyset.*property_set_name.property_name*)

```
# test.properties
status_message=The API is experiencing no outages.
loglevel=debug
```

Like a Key Value Map, a property set can be used to store a custom collection of key/value pairs that can be used by API proxies.

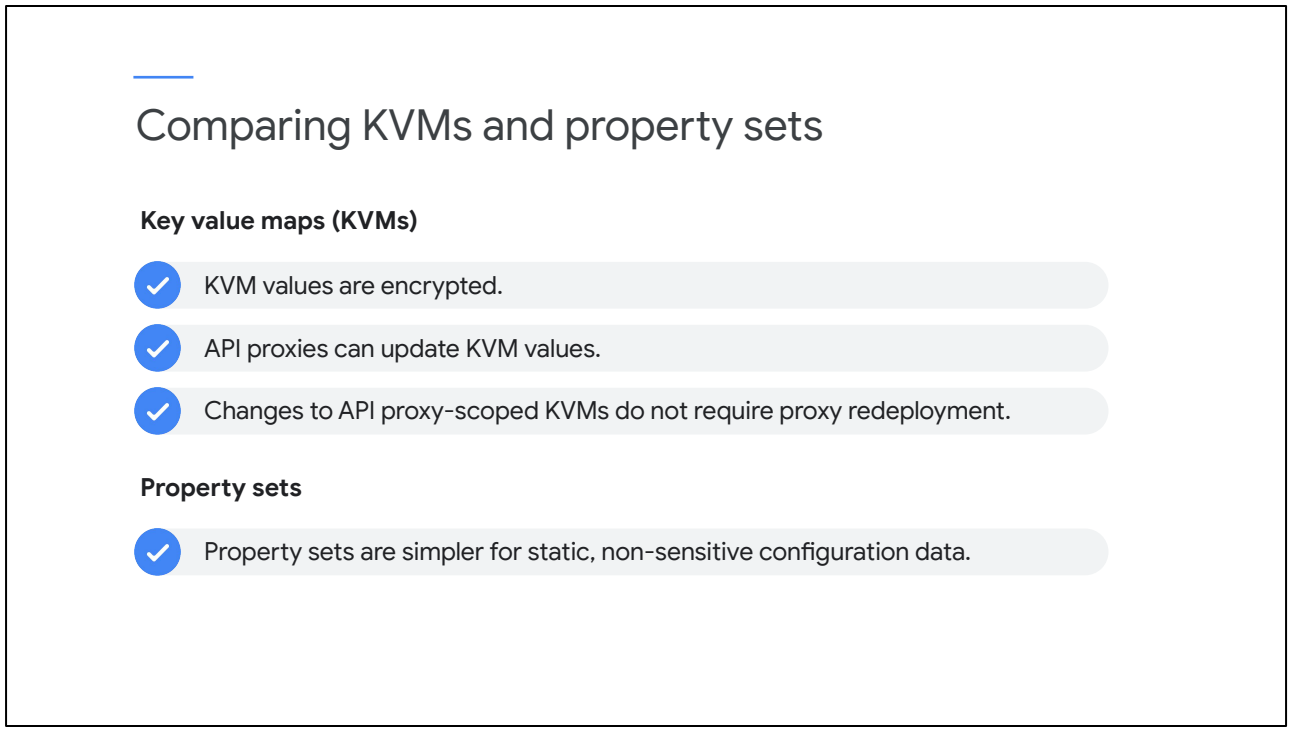
A property set is implemented using a .properties file. This standard format is used to specify key value pairs. Comments can be added to the file for readability.

Property sets should be used for static, non-expiring data. Unlike the values in a Key Value map, property set values cannot be updated dynamically by an API proxy.

Property sets can be specified at an environment or API proxy level. Environment-scoped property sets can be used to provide different values depending on the environment in which the API proxy is deployed. Changes to an environment-scoped property will be picked up by an API proxy without redeployment. For an API proxy-scoped property set, the keys and values can only be changed when the API proxy is redeployed.

The values in a property set are accessed by referencing flow variables in the API proxy. For example, a property named loglevel in a property set named test.properties could be accessed using the flow variable propertyset.test.loglevel.

[More details on property sets are at:
https://cloud.google.com/apigee/docs/api-platform/cache/property-sets]



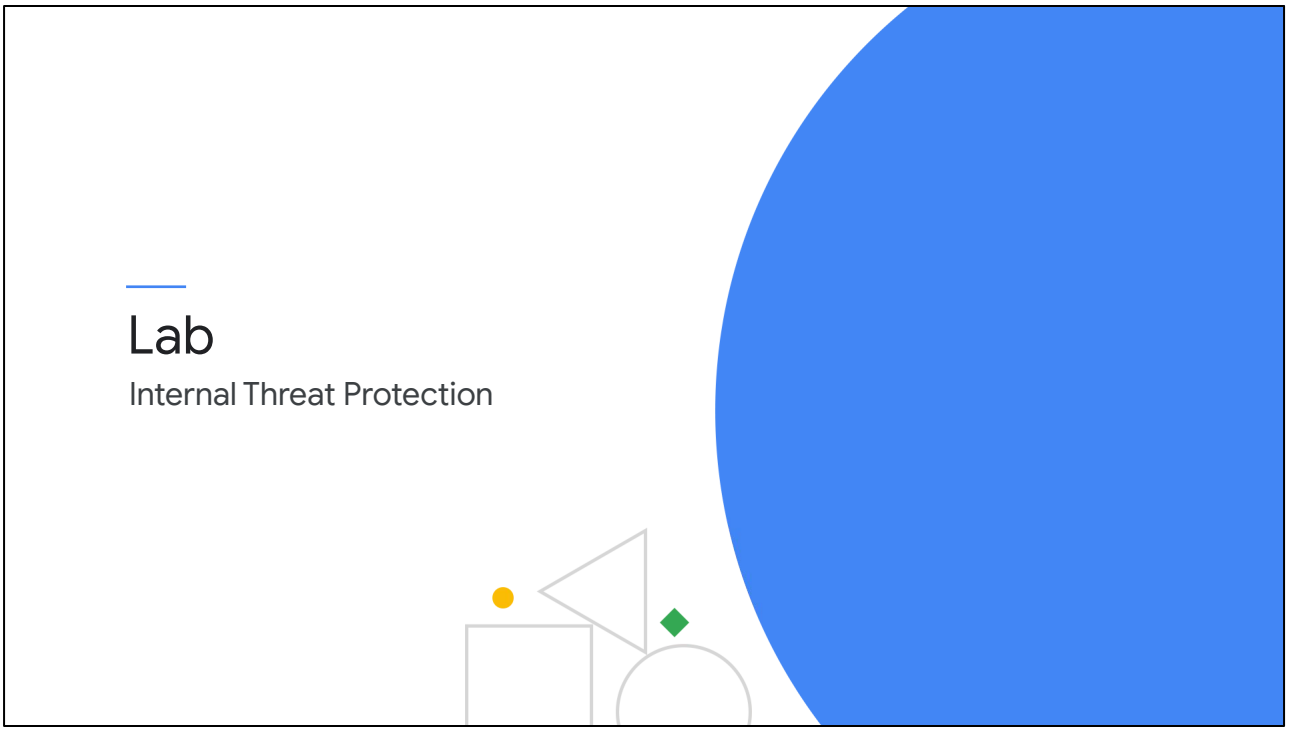
Key Value Maps and property sets serve similar purposes. They are both used to store configuration data, but there are key differences.

KVM values are encrypted. This can be important when storing sensitive data like backend service passwords or API keys. Property set values are stored in plaintext.

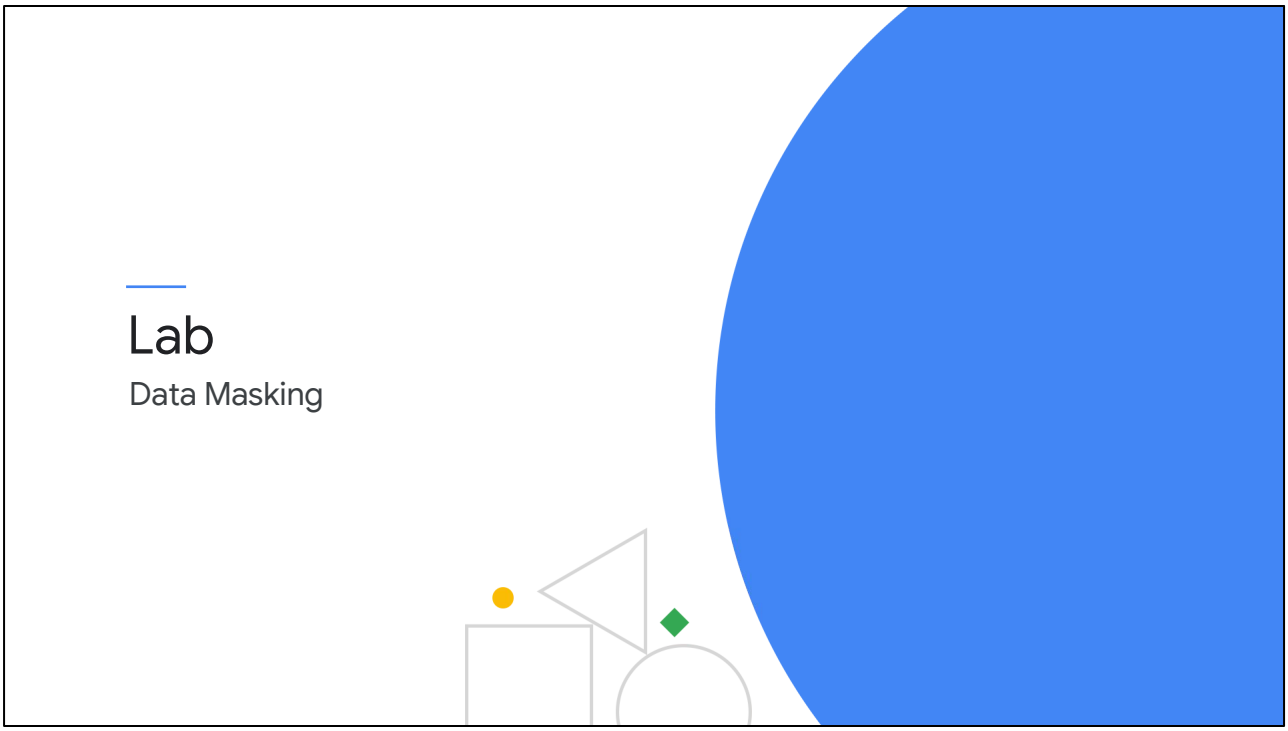
KVM values can be changed dynamically. The KeyValueMapOperations policy can be used to update a value during the execution of an API call. Property set values cannot be updated dynamically by an API proxy.

Changes to values in KVMs are picked up by an API proxy without redeployment. API proxy-scoped property sets can only be changed by redeploying the API proxy.

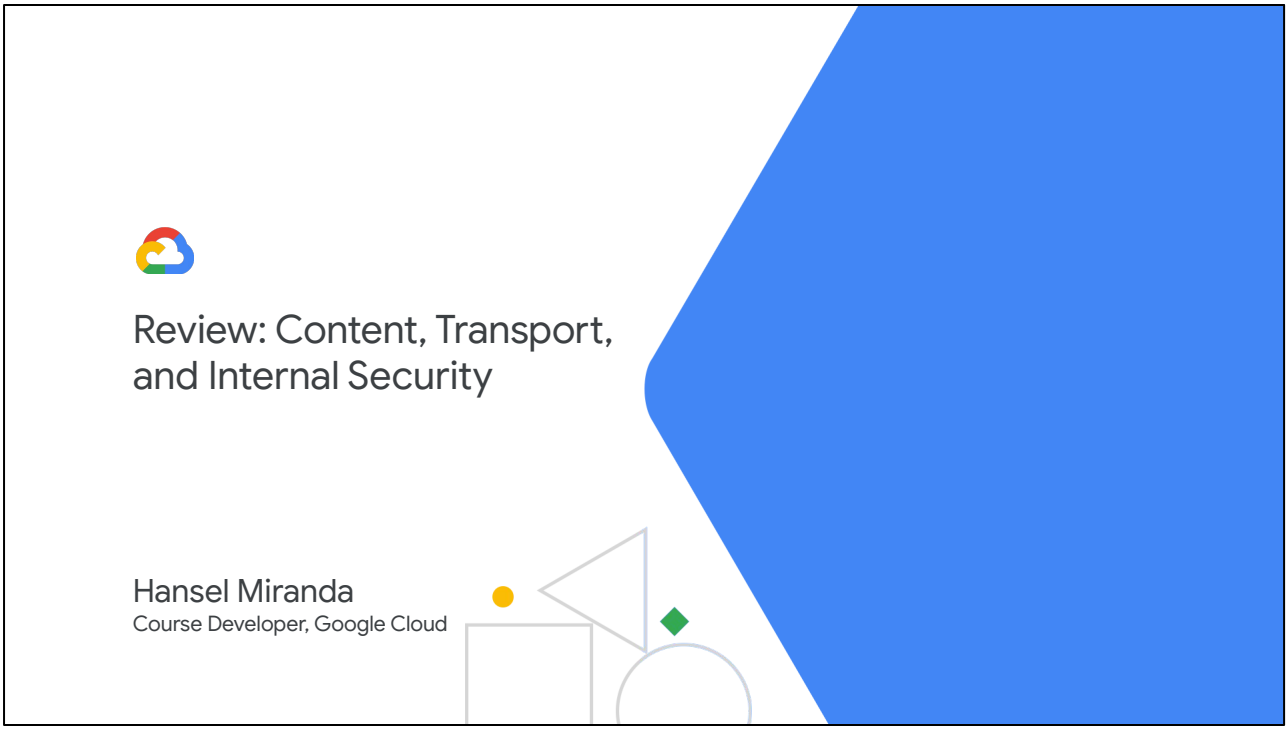
Even though KVMs have more features, property sets are usually better than KVMs for storing static, non-sensitive configuration data. Property set keys and values are easier to create and maintain than KVM entries. Because they are static and non-sensitive, it is often appropriate to check in .properties files to code repositories.



In this lab you protect backend credentials from being exposed in the Apigee management UI. You create a key value map and add the credentials to it. You will use those credentials in your proxy to create a Basic Authentication header for calls to the backend.



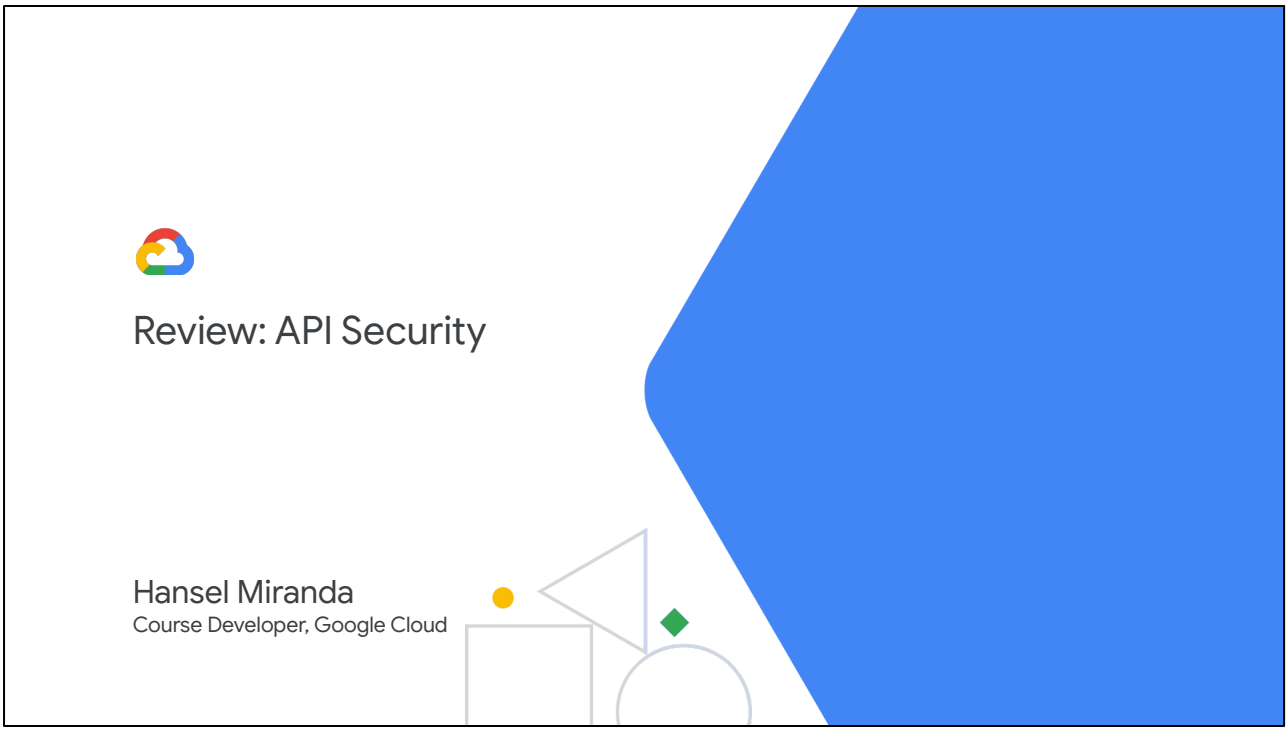
In this lab you learn how to protect against internal access of sensitive data by using private variables and data masking.



In this module, you learned how to protect your API proxies against content-based attacks, and how to keep users from seeing sensitive data while tracing API calls in the Apigee console.

You learned about transport security, and how to use TLS for communicating between client apps and Apigee and backend services.

You also completed labs using threat protection policies, key value maps, and data masking.



Thank you for taking the API Security course.

During this course you learned about the different types of security concerns your APIs must protect against.

We learned about many aspects of OAuth, including the OAuth grant type flows and when we would use each grant type.

You learned about JWT tokens and federated security.

We discussed content-based attacks, and learned about the threat protection policies that can be used to protect against these attacks.

And you learned about Apigee features that can limit internal access to features and mask data for the users of the Apigee console.

Next, we recommend you continue with the next course in this series, API Development and Operations on Google Cloud's Apigee API Platform.

In the API Development and Operations course, you'll learn about API mediation, traffic management, caching, and fault handling, and add these to your retail API proxy.

You will also create a developer portal, and publish your API product for use by app

developers.

We will learn about message logging and analytics, CI/CD, and deployment options for Apigee.

We hope to see you in the next course!