AWS Verified Access
Request Verification Flow

1. With AWS IAM Identity Center – Initial Request

2. With AWS IAM Identity Center – After Initial Request

3. With AWS IAM Identity Center and Device Trust Provider – Initial Request

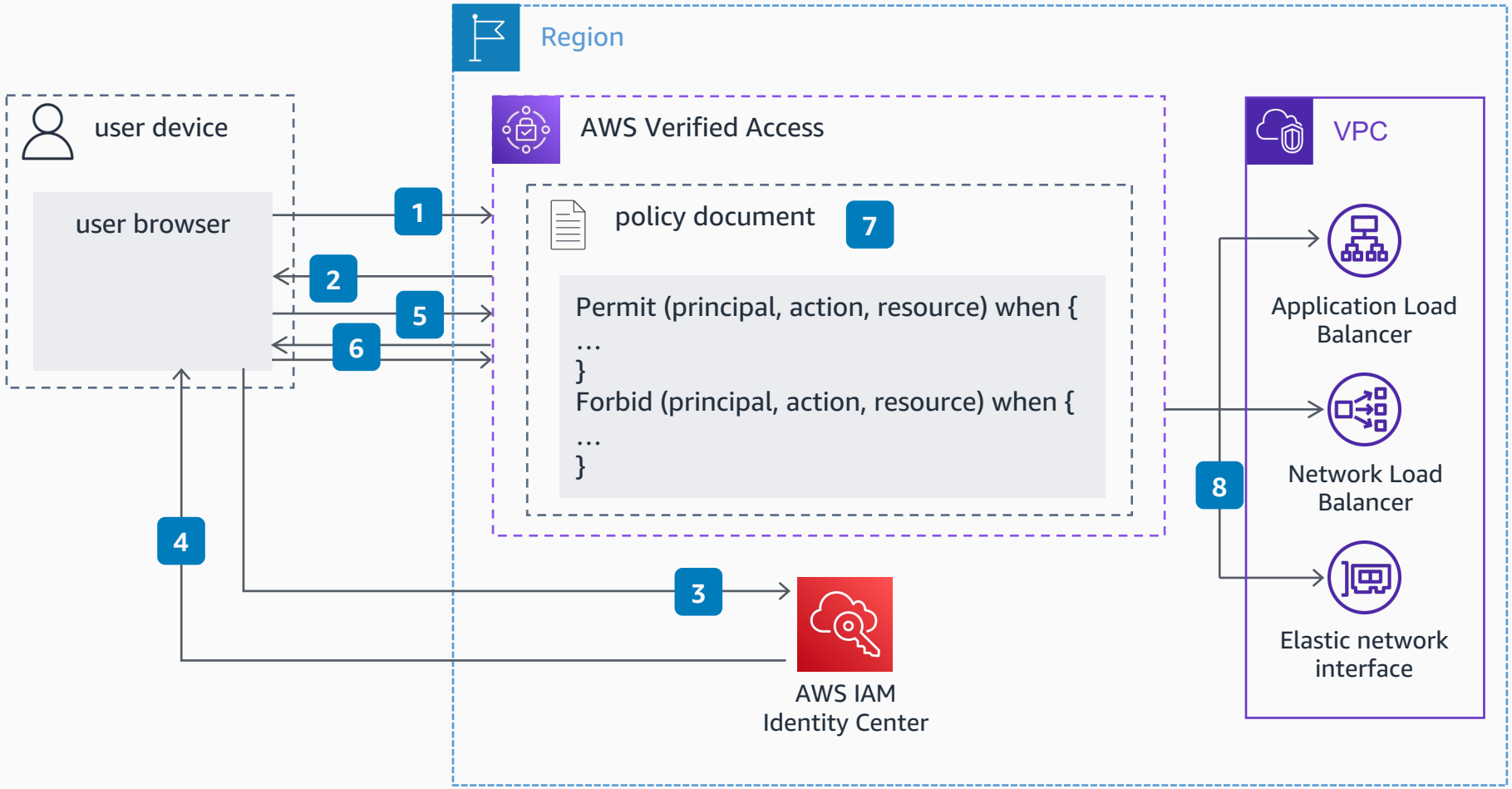
4. With AWS IAM Identity Center and Device Trust Provider – After Initial Request

Reviewed for technical accuracy February 22, 2023
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

AWS Verified Access Request Verification Flow

With AWS IAM Identity Center – Initial Request



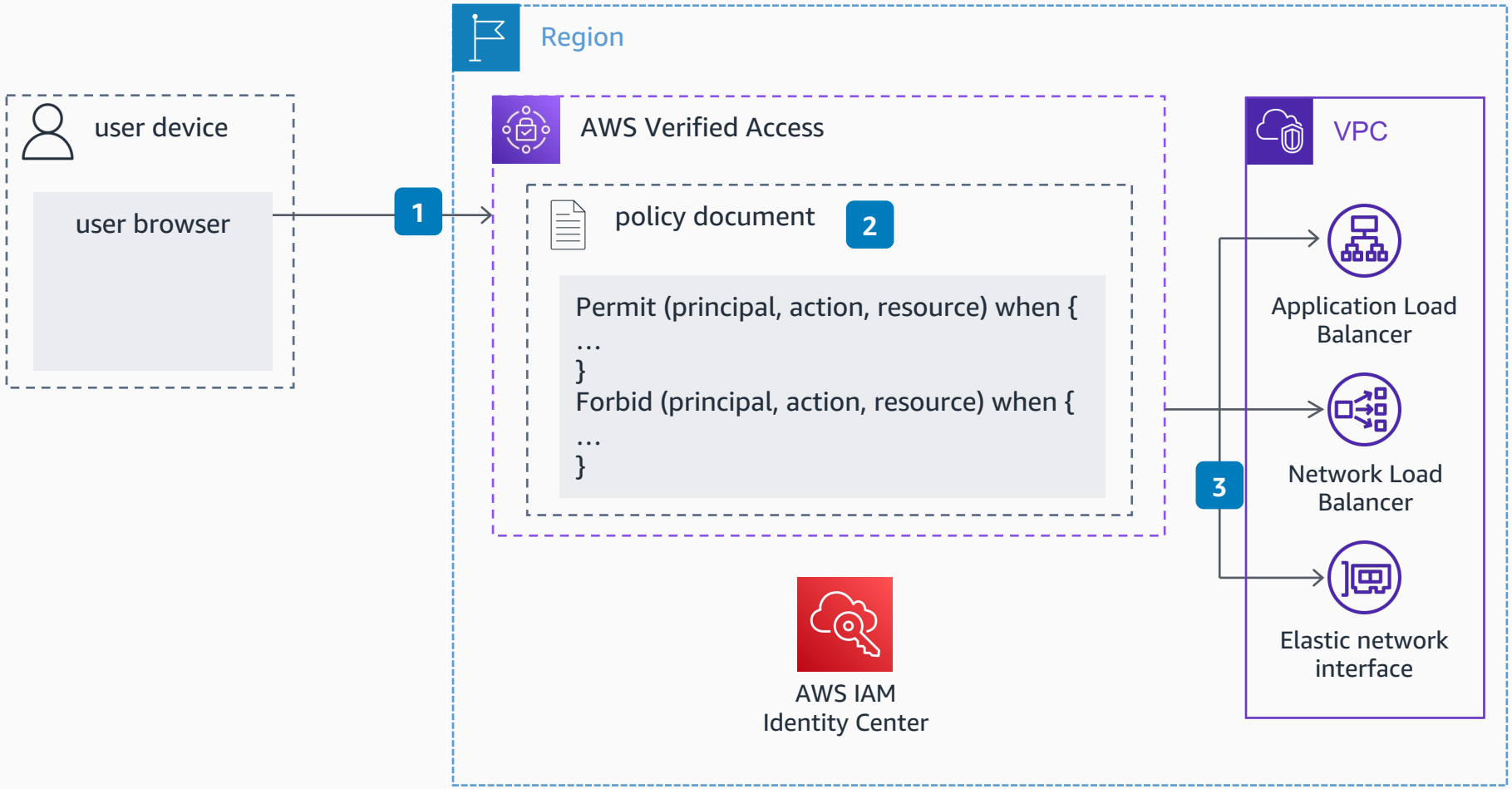
1. The initial request is made to the application domain hosted on an **AWS Verified Access** (AVA) endpoint. This request does not have an identity cookie.
2. The first redirect is made to the identity provider, **AWS IAM Identity Center**, to collect the user identity.
3. The browser redirects to the **IAM Identity Center** URL. The user completes the **IAM Identity Center** sign-in process.
4. **IAM Identity Center** redirects the user to the application domain to validate the identity token.
5. The browser sends the application domain endpoint the **IAM Identity Center** token, which **AVA** uses to set the user identity cookie.
6. **AVA** redirects the user with the user identity cookie to the original URI.
7. **AVA** receives the request with the user identity cookie. For each user request, **AVA** will validate the user request against the policy for the application using the identity of the user.
8. **AVA** proxies validated requests to application endpoints in the customer virtual private cloud (VPC).

Reviewed for technical accuracy February 22, 2023
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

AWS Verified Access Request Verification Flow

With AWS IAM Identity Center – After Initial Request



1. The initial request to the application domain hosted on an **AVA** endpoint, which does have a user identity cookie.
2. For each user request, **AVA** will validate the user request against the policy for the application using the identity of the user.
3. **AVA** proxies validated requests to application endpoints in the customer VPC.

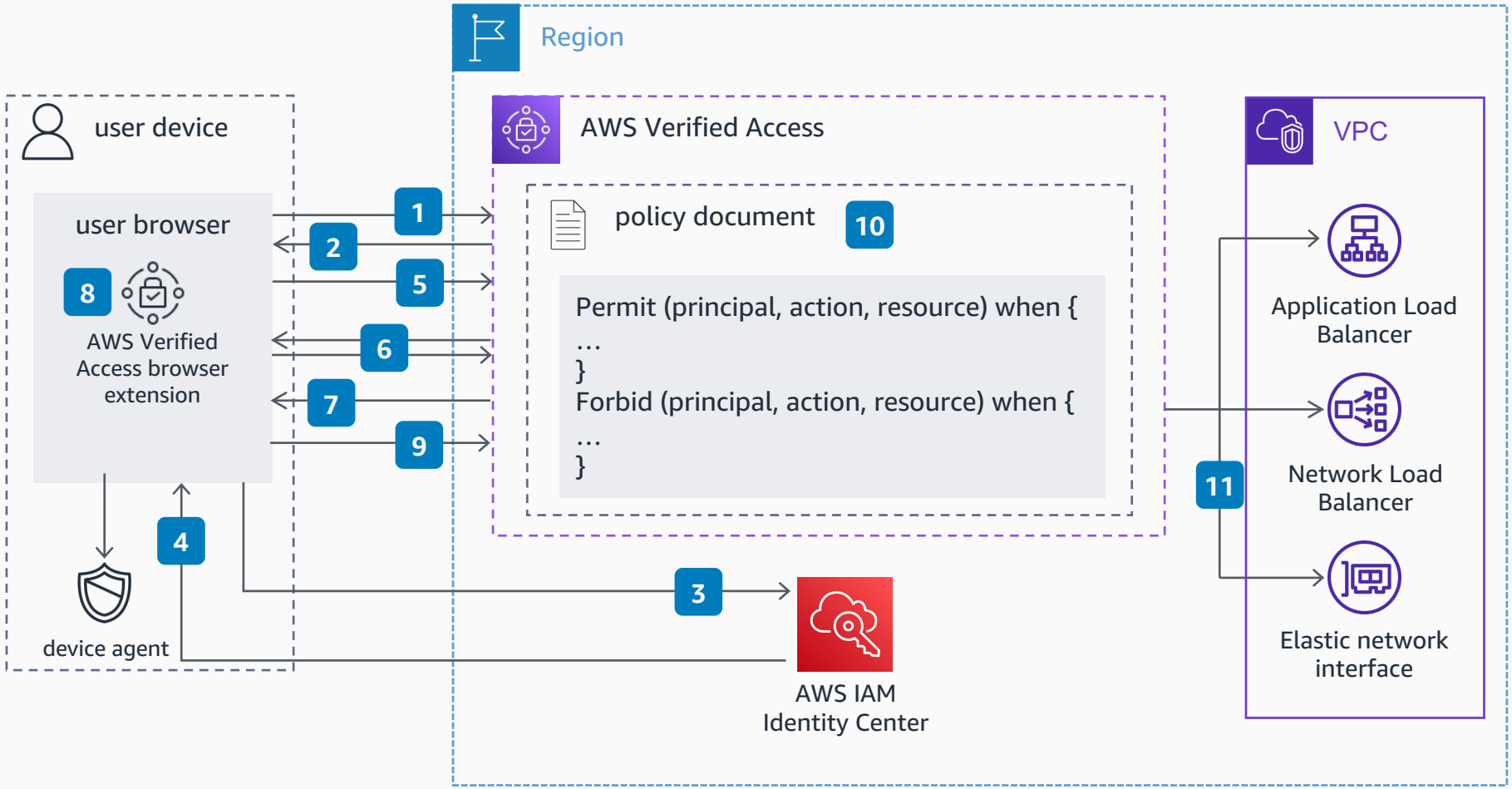
Note: The identity cookie will have a lifetime associated with it. When that lifetime expires, the user will need to re-authenticate with **IAM Identity Center**.

Reviewed for technical accuracy February 22, 2023
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

AWS Verified Access Request Verification Flow

With AWS IAM Identity Center and Device Trust Provider – Initial Request



Note: The local device agent is continuously gathering device posture information. The browser extension transmits up-to-date information for each request to an **AVA**-wrapped endpoint.

1:5 Steps 1-5 are the same as in the first use case ("With AWS IAM Identity Center – Initial Request").

6 The browser extension detects the 302 redirect, but does not know the application domain is an **AVA** domain. No device information cookie is added.

When **AVA** expects device information but does not receive it, it redirects the user to the device validation domain. **AVA** will repeat steps 3-6, but **IAM Identity Center** will bypass sign-in as cookies from previous sign-in are found.

7 The device validation domain sends a 302 redirect. This tells the browser extension it should pass the device information cookie to the application domain.

8 The browser extension extracts the application domain from the redirect and adds it to the cache of trusted **AVA** domains. It sets the device information cookie on the application domain.

9 The browser extension allows the redirect to continue.

10 **AVA** receives a response with a user identity cookie and device information cookie. For each user request, AVA will validate the user request against the policy for the application using the identity of the user and device posture.

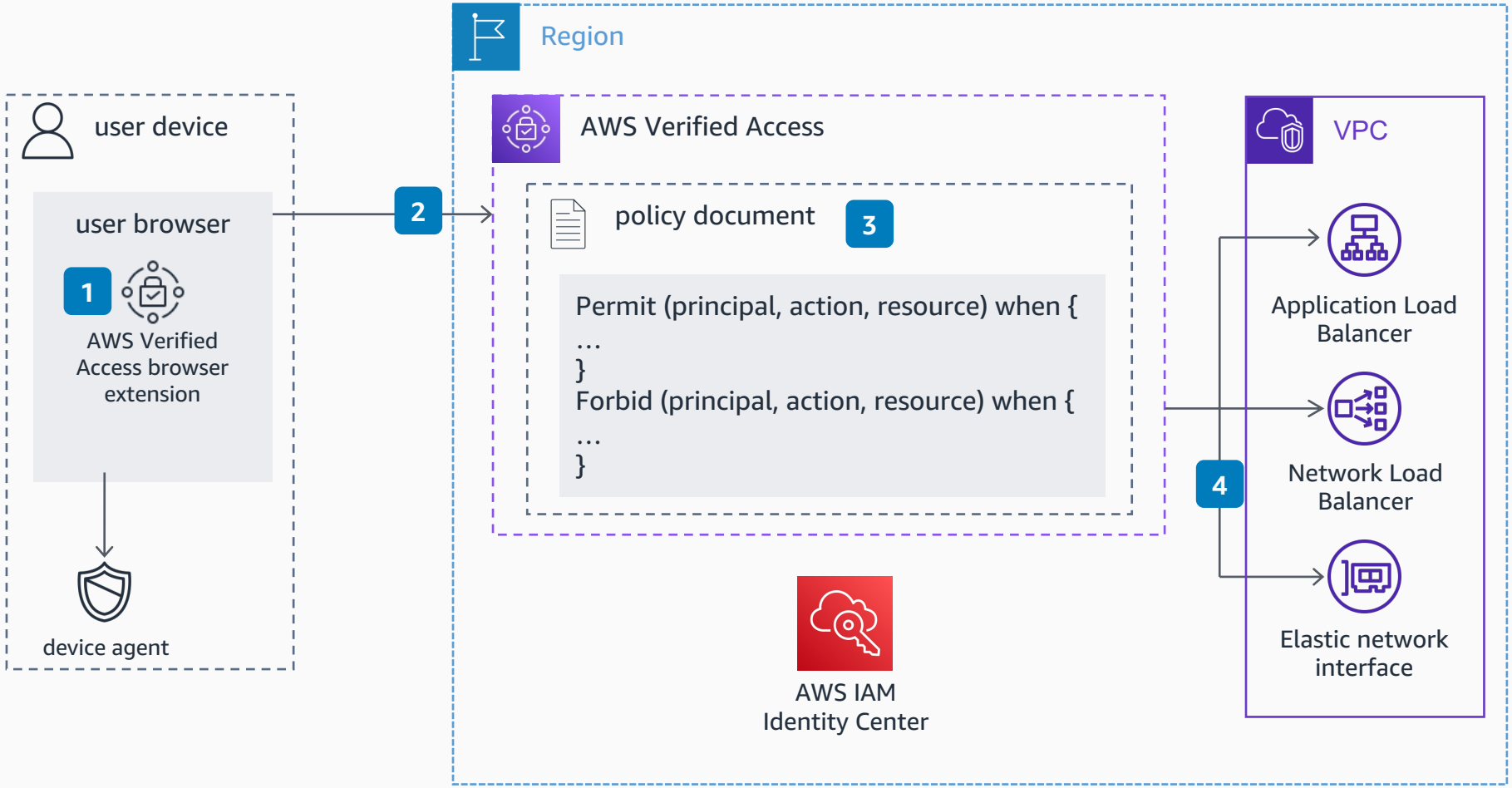
11 **AVA** proxies validated requests to application endpoints in the customer VPC.

Reviewed for technical accuracy February 22, 2023
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

AWS Verified Access Request Verification Flow

With AWS IAM Identity Center and Device Trust Provider – After Initial Request



Note: The local device agent is continuously gathering device posture information. The browser extension transmits up-to-date information for each request to an **AVA**-wrapped endpoint.

1. Because the application domain is in the browser extension application domain allow-list, the browser extension sets the device information cookie.
2. When the user sends the initial request to the **AVA** endpoint, the identity cookie and device information cookie are included with the request to the application domain.
3. **AVA** receives a response with a user identity cookie and device information cookie. For each user request, **AVA** will validate the user request against the policy for the application using the identity of the user and device posture.
4. **AVA** proxies validated requests to application endpoints in the customer VPC.

Note: The identity cookie will have a lifetime associated with it. When that lifetime expires, a user will need to re-authenticate with **IAM Identity Center**.

Reviewed for technical accuracy February 22, 2023
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture