1. What is used to detect if a SAML assertion was modified after being issued?
   - ✓ Digital Signatures

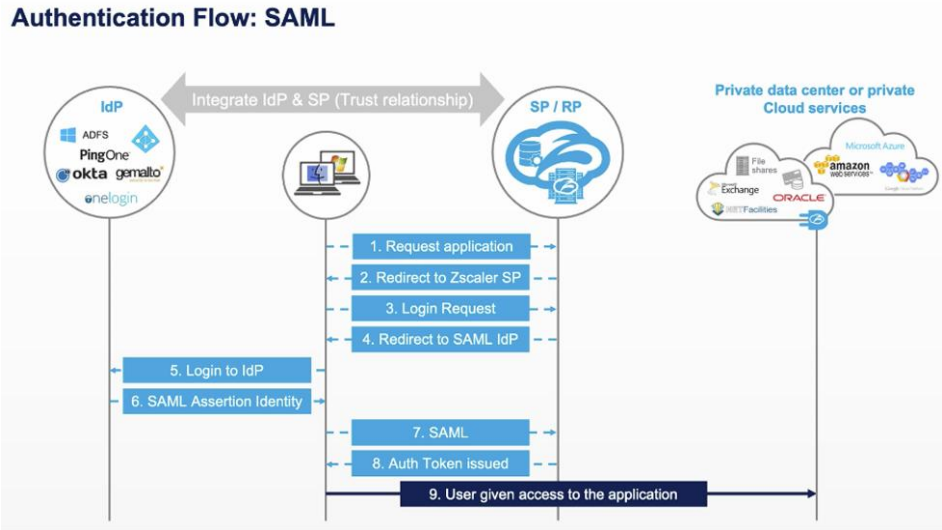
Zscaler Validates the SAML Assertion

Upon receiving the SAML assertion, **Zscaler verifies the digital signature** to confirm:

- The assertion is from a **trusted source**
- The data has **not been tampered with** during transmission

✓

2. How is a SAML assertion delivered to Zscaler?
   - ✓ The IdP sends it via an HTTP post directly to the SP via a backend API



✓

3. How does ZIA authenticate users? (3 Options)
   - ✓ SAML
   - ✓ SCIM
   - ✓ Hosted Database

4. How does ZPA authenticate end users?
   - ✓ SAML

5. What is the fastest way to change a user's access entitlements?
   - ✓ Send different attributes via SCIM

6. For Zscaler to enforce policy based on accessing devices, what method is best used by IdPs to share information about a user's accessing device?
   - ✓ SAML

7. Privileged Remote Access supports which protocols? (2 Option)
   - ✓ SSH
   - ✓ RDP

8. Which services can coexist on an Application Segment?
   - ✓ Isolation, Browser Access and Inspection

9. How often does the Zscaler Cient Connector check for software updates?
   - ✓ Every 2 hours

   Step 5: Software Update Check

   - **Frequency:** Every **2 hours**
   - **Action:** Performs checks for software updates to the Client Connector.
   - **Purpose:** To ensure the system has the latest enhancements and security patches.

   ✓

10. Browser Based Access enables what kinds of applications to be published?
    - ✓ HTTP
    - ✓ HTTPS

      Browser Access enables secure user authentication and application access through a **web browser**, eliminating the need for users to install **Zscaler Client Connector** on their devices. This feature is particularly useful in scenarios where installing the **Client Connector** is not feasible or desirable.

    ✓

11. What conditions exist for Trusted Network Detection?
    - ✓ DNS Search Domain
    - ✓ DNS Server
    - ✓ Hostname/IP

    ✓

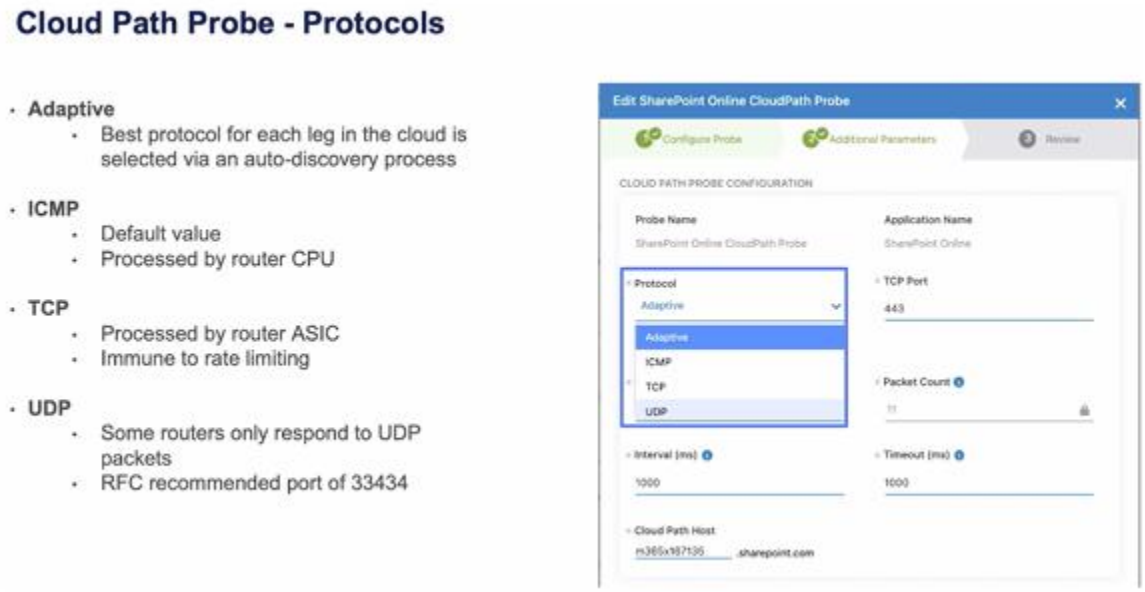
12. What are the acceptable actions for Firewall policy?
    - ✓ Allow
    - ✓ Block/Drop
    - ✓ Block/reset

13. The ZDX Web Probe provides the following metrics?
    - ✓ Page Fetch Time, DNS Time. Server Response Time and Availability

    ✓ There are two primary components of **application monitoring** in ZDX: the **Web Probe** and the **Cloud Path Probe**. The **Web Probe** is responsible for pulling objects from the server and collecting key metrics such as **page fetch time, DNS resolution time, server response time, and application availability**. These metrics help in determining how efficiently an application is

14. A Cloud Path supports the following protocols for probing (3 Options)
    - ✓ ICMP
    - ✓ TCP
    - ✓ UDP

    ✓



15. What functionalities in ZDX leverages machine learning to assist with automated root cause analysis?
    - ✓ Y-Engine

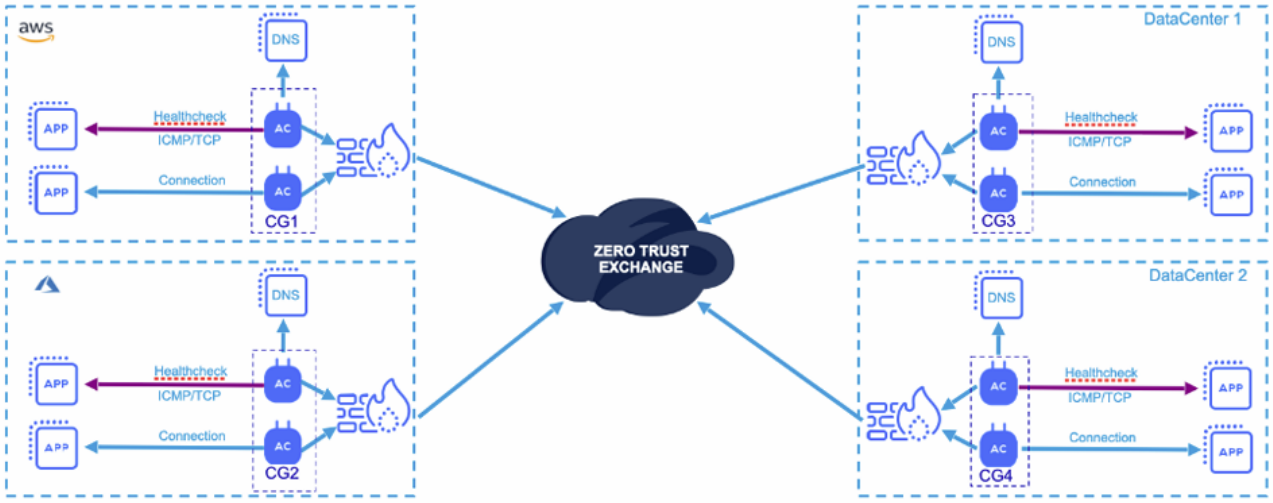
    ✓ **Automated Root Cause Analysis (Y-Engine)** – Leverage AI-powered analysis to quickly pinpoint the root cause of digital experience problems, minimizing troubleshooting time.

16. What are the two probe types that are configured while configuring an application in the ZDX Administrator portal?
    - ✓ Web Probe and Cloud Path Robe
    - ✓ There are two primary components of **application monitoring** in ZDX: the **Web Probe** and the **Cloud Path Probe**. The **Web Probe** is responsible for pulling objects from the server and

17. What is the best practice for a cloud-gen firewall in terms of default rules?
    - ✓ Block everything and start allowing what your users need to access
    - ✓ **Zscaler's recommended best practice is to start with a Default Block Drop rule**, which aligns with cybersecurity best practices. This ensures that **all traffic is blocked by default**, and organizations can then **explicitly allow only the necessary applications and services**.

18. What are some actions that Zscaler's Firewall can take when rules trigger?
    - ✓ Allowed
    - ✓ Blocked / (Drop, Reset, ICMP)
    - ✓ **Action Types:**
      - **ALLOW**: Permits the transaction.
      - **BLOCK/DROP**: Silently drops traffic, potentially causing retransmissions.
      - **BLOCK ICMP**: Sends an ICMP "port unreachable" response.
      - **BLOCK/RESET**: Sends a **TCP reset**, forcibly closing the connection.

19. You have data centers in New York, San Francisco, London, and Hong Kong. Each data center hosts multiple applications, and all have internet connectivity. What is the minimum number of App Connectors you should deploy for production?
    - ✓ 8, 2 per Data Centers



For example, if an organization has a **data center in London, a data center in New York, an AWS instance in US West, and an Azure instance in EMEA Central**, then:

- These are **four separate locations**, each requiring its own **connector group**.
- Each location should have **at least two App Connectors**, totaling **eight connectors across all locations**.

✓

20. How often does Zscaler Client Connector download policy updates for the app profiles and forwarding profiles?
    - ✓ 80 minutes

Step 3: Policy Update Check

- **Frequency: Every** 80 minutes
- **Action:** Checks for policy updates from app profiles and forwarding profiles.
- **Purpose:** To promptly implement any changes in security policies.

✓

21. How often will Zscaler Client Connector download the PAC file of the app profiles and the forwarding profiles?
    - ✓ 15 Minutes

Step 2: PAC File Download

✓
- **Frequency**: Every 15 minutes
- **Action**: Periodic download of PAC files from app profiles and forwarding profiles.

✓
- **Purpose**: To keep the latest network routing configurations readily available

22. How often does ZDX probe an application?

✓ Every 5 Minutes

✓ To maintain real-time accuracy, ZDX **sends a probe to an application every five minutes**. Each measurement is assigned a numerical value between **1 and 100**,

23. What are the three levels of inspection for DLP?

✓ Magic Bytes

✓ Mime Type

✓ File Extension

✓ Zscaler DLP policies can block or allow specific file types from being uploaded to cloud applications. Instead of relying on file extensions (which can be modified), Zscaler performs three levels of inspection:

- **Magic Bytes Analysis:** Examines the file's first few bytes to determine its true format.
- **MIME Type Verification:** Ensures the file type aligns with its intended use.
- **File Extension Validation:** Confirms the correct extension usage.

24. To ensure Zero Trust, users should not be connected to _____, but to the application

✓ Network

✓ *Zero Trust Segmentation with Zscaler*

Rather than granting broad network access, **Zscaler applies Zero Trust segmentation**, allowing users to connect only to the **specific applications they need—without ever being placed on the network**. By eliminating network access, organizations remove the ability to **discover, probe, or move laterally** to unauthorized applications and resources.

25. Is URL filtering or Cloud App Control better suited to control access to specific web applications?

✓ Cloud App Control

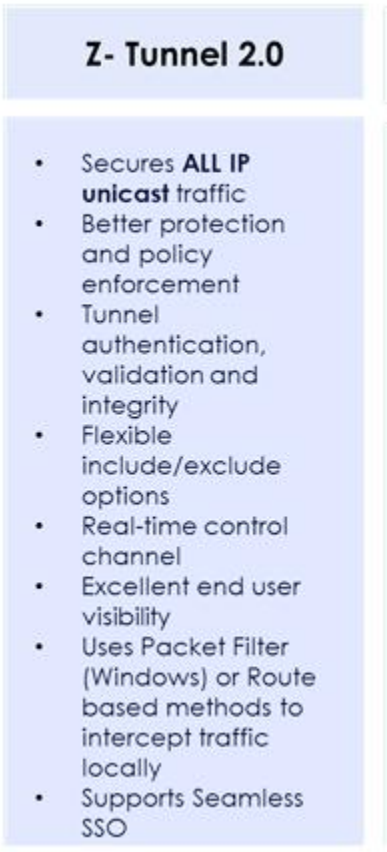
26. What signifies Land Mine in Cybersecurity?

✓ **Decoys placed across cloud environments, endpoints, networks, and Active Directory** serve as **landmines**, detecting **ransomware at every phase of the attack chain**. The presence of decoys alone discourages ransomware from spreading further.

27. What enables zero trust to be properly implemented and enforced between an originator and the destination application?

✓ Access is granted without sharing the network between the originator and destination application

28. In support of data privacy about TLS/SSL inspection, when you subscribe to ZIA, you enter into what kind of agreement?
    - ✓ Acceptable Use Policy
    - ✓ Before deploying **SSL inspection**, it is critical to align organizational stakeholders and ensure there is agreement on its purpose. SSL inspection is not about monitoring user activity but rather about safeguarding the business from malware, preventing data leaks, and protecting corporate reputation. Defining an **acceptable use policy (AUP)** and establishing clear user notifications help set expectations and transparency around its implementation.

29. Which ZIA forwarding modes secure all IP unicast Traffic?
    - ✓ Z-Tunnel Mode 2.0
    - ✓ 

30. What is the name of the feature that allows the platform to apply URL filtering even when a Cloud App Control Policy explicitly permits a transaction?
    - ✓ Allow Cascading
    - ✓ As noted above, **Cloud App Control rules override URL Filtering** when an application is explicitly allowed. However, **Allow Cascading to URL Filtering** is an advanced setting that enables both policies to be enforced simultaneously.

31. What is the preferred method for authentication in a OneAPI environment?
    - ✓ OIDC

32. From a user perspective, Zscaler bandwidth control performs traffic **shaping** and buffering on what direction of traffic?
    - ✓ Outbound Traffic is Shaped. Inbound or localhost traffic is unshaped.
    - ✓

	Policing	Shaping
Goal	Drop excess traffic beyond set limit. (typical UTM boxes). Also called "rate limit."	Delay (buffer) above committed rate traffic in a queue for later transmit
Direction	Inbound and outbound	Outbound
Bursts	Transmitted as is with sawtooth. Drop excess	Smooths out traffic rate, buffer excess
TCP traffic behavior	Drops causes TCP retransmits (YouTube resets) — choppy video	Minimizes TCP retransmits by buffering — smoothens YouTube at 480p vs 720p.
Queuing	Not performed	Queuing is performed with high memory buffers
Commonly used	Delay sensitive traffic (UDP, voice)	Delay insensitive traffic that can bear latency

33. What is the main purpose of sandbox functionality?
    - ✓ Identify Zero Day Threats
    - ✓ **Cloud Sandbox** with **AI/ML-based behavioral analysis** detects and blocks zero-day malware before it reaches users.