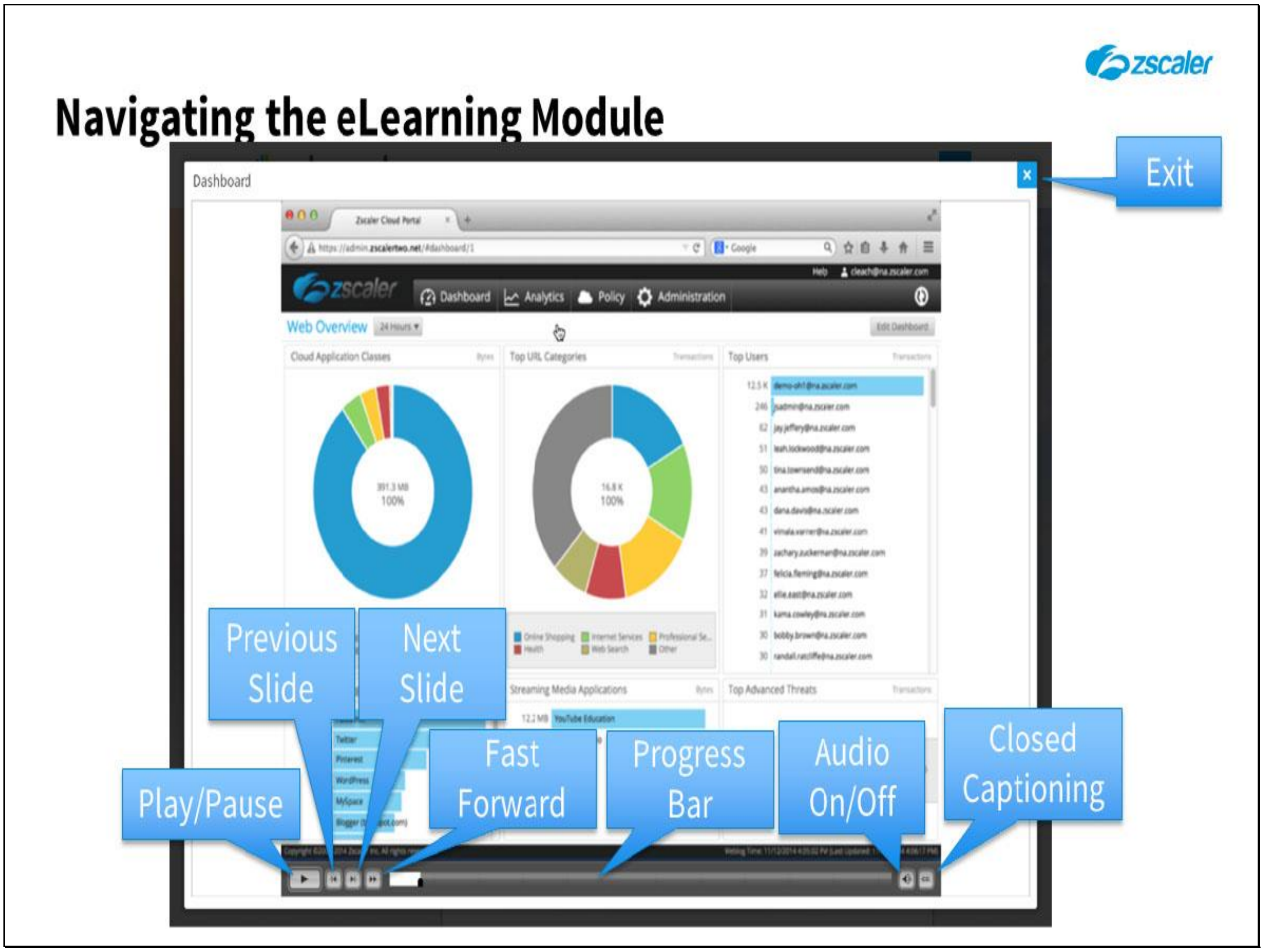
Slide 1 - Authentication

Authentication

Slide notes

Hello and thank you for viewing this eLearning module on Zscaler User Authentication in the Zscaler solution.

Slide 2 - Navigating the eLearning Module

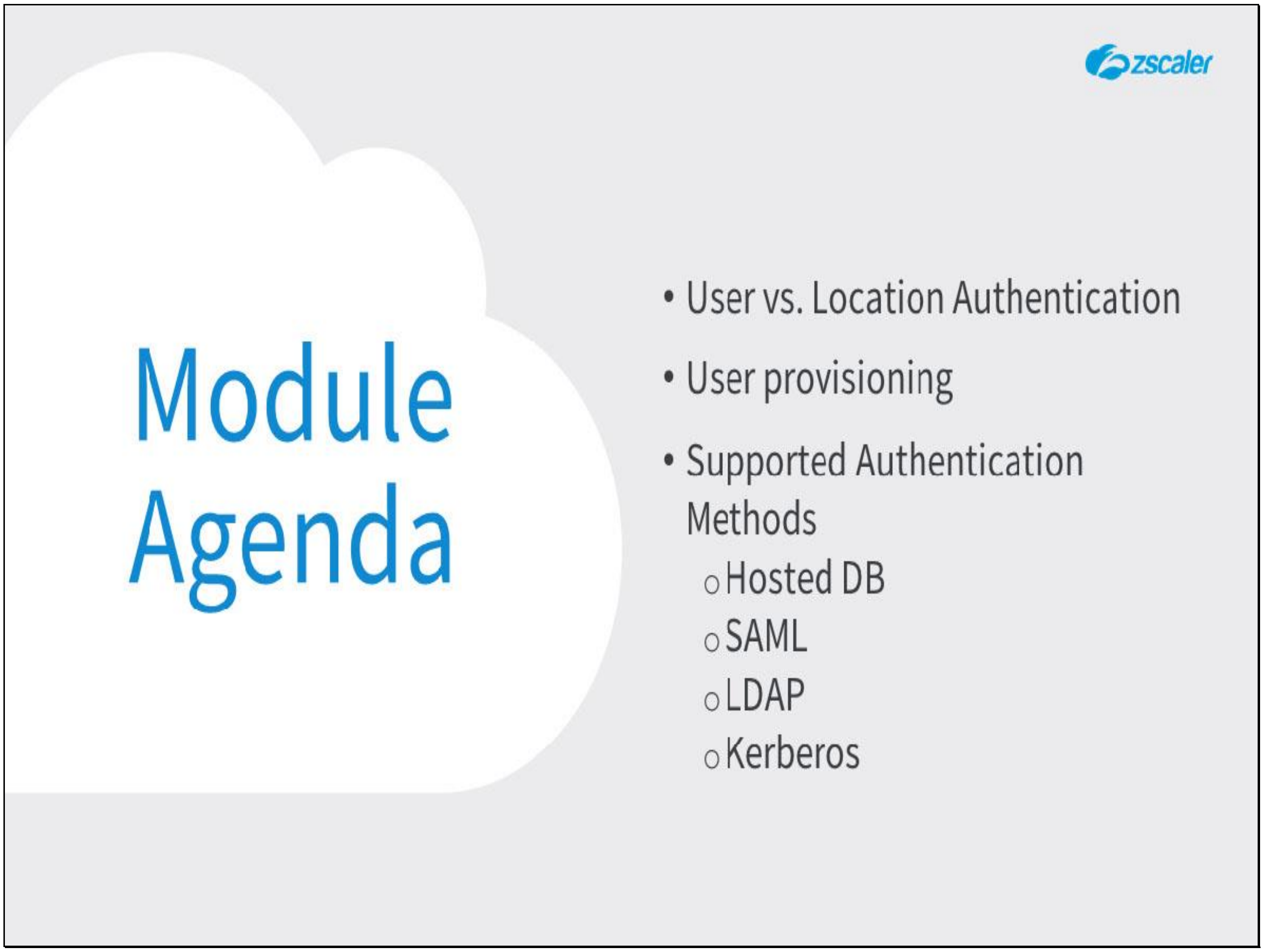


Navigating the eLearning Module

Slide notes

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and Next Slide, and Fast Forward. You can also mute the Audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button if you wish to exit.

Slide 3 - Understanding Authentication Methods with Zscaler



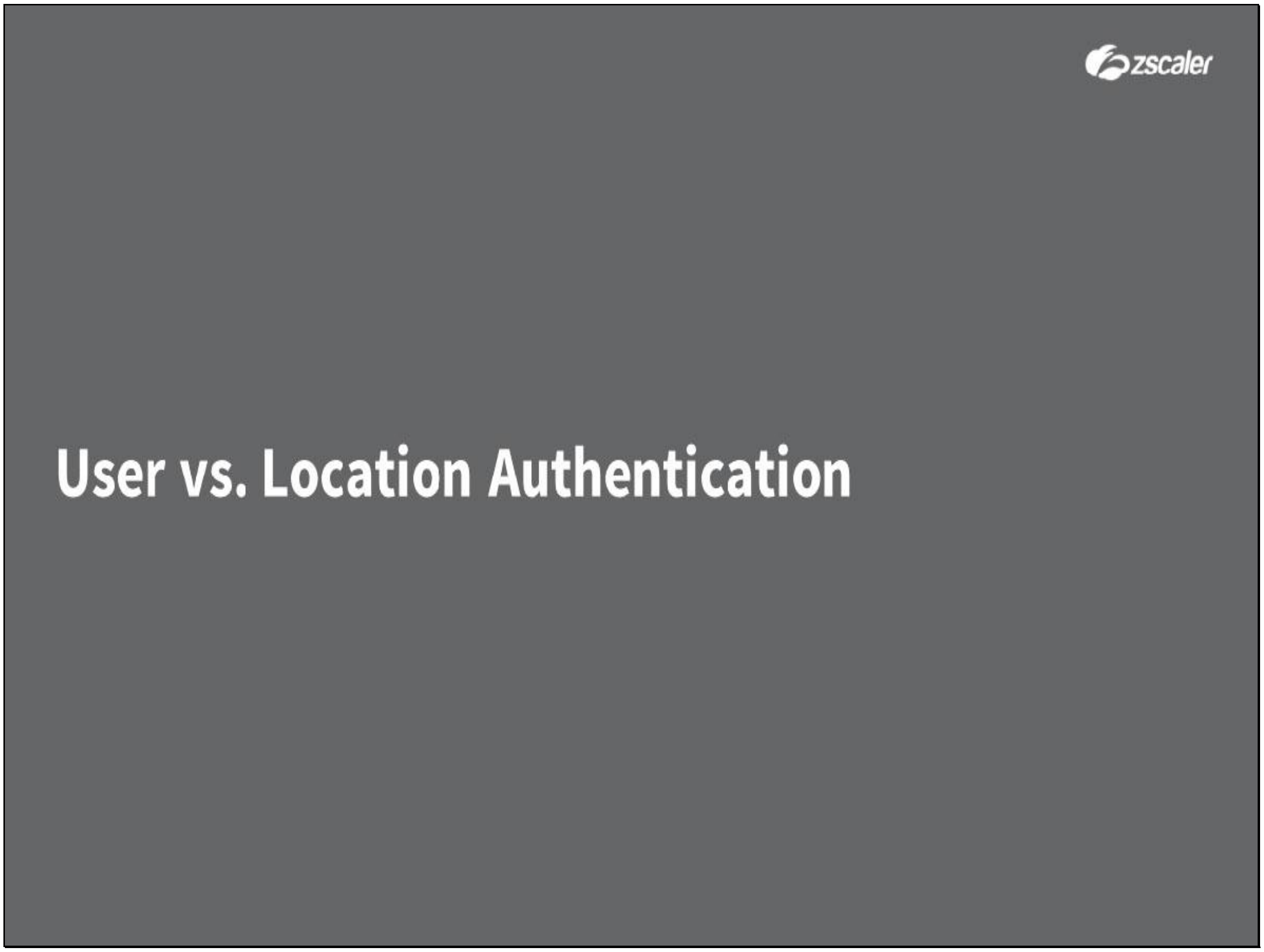
Module Agenda

- User vs. Location Authentication
- User provisioning
- Supported Authentication Methods
  - Hosted DB
  - SAML
  - LDAP
  - Kerberos

Slide notes

In this module we will look at user provisioning by authentication type, understanding the four types of authentication the Zscaler solution employs, and the authentication flow of each auth type.

Slide 4 - User vs. Location Authentication

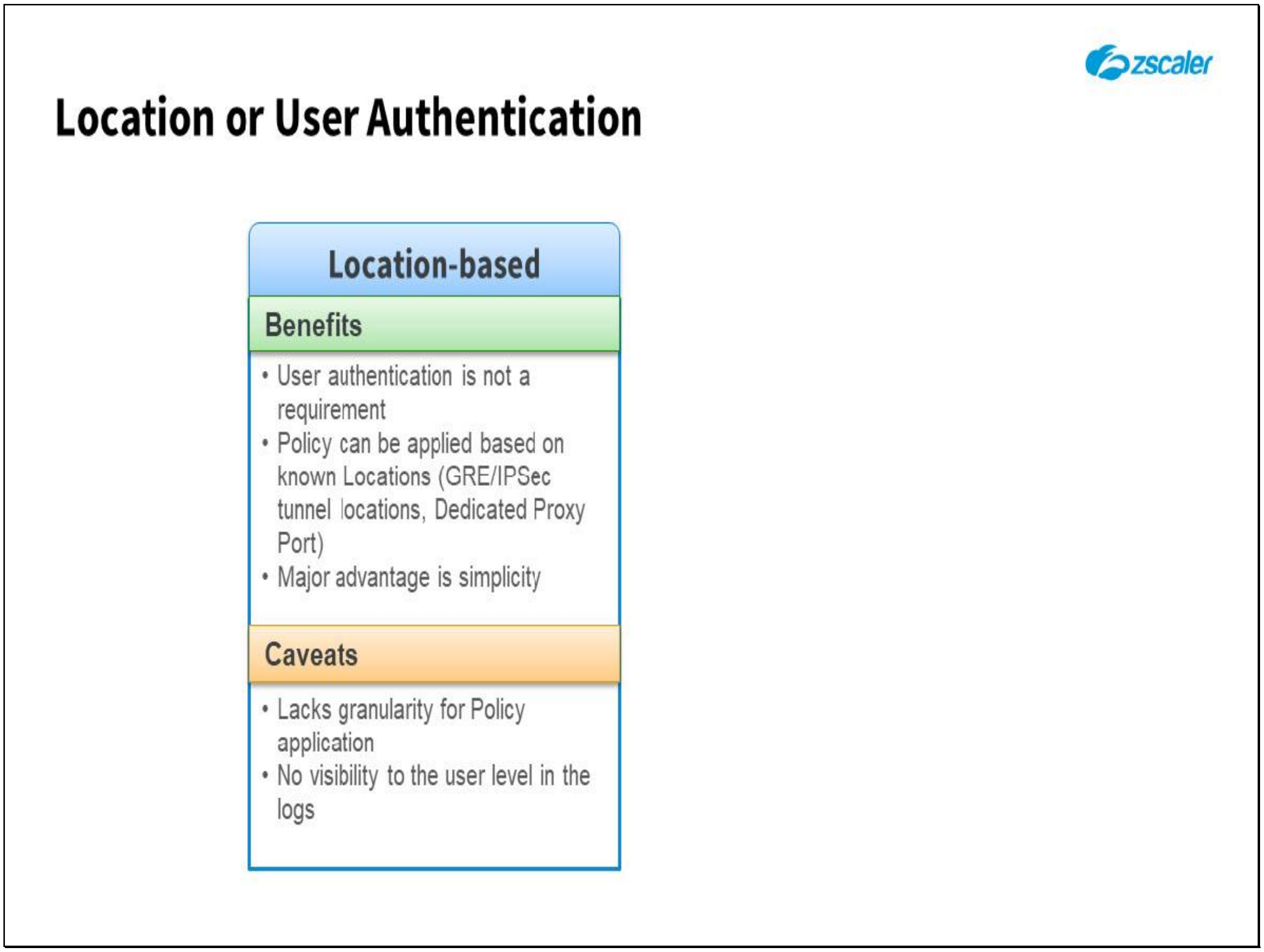


User vs. Location Authentication

Slide notes

Let's take a look at different methods for authenticating traffic; location and user auth and why we want to authenticate individual users.

Slide 5 - Location or User Authentication



Location or User Authentication

Location-based

Benefits

- User authentication is not a requirement
- Policy can be applied based on known Locations (GRE/IPSec tunnel locations, Dedicated Proxy Port)
- Major advantage is simplicity

Caveats

- Lacks granularity for Policy application
- No visibility to the user level in the logs

Slide notes

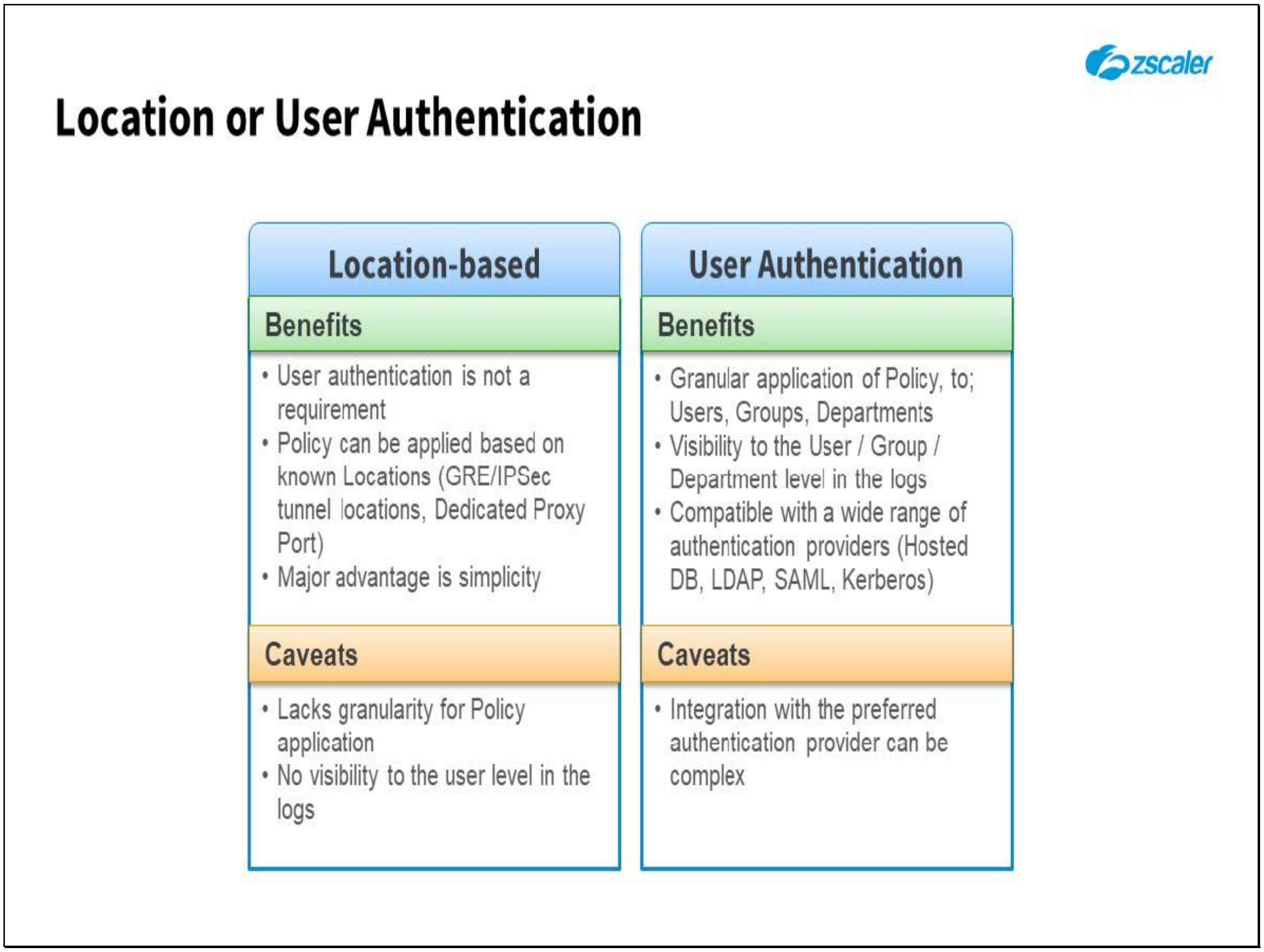
The first type of authentication in the Zscaler solution is **Location Authentication**. User authentication is not required in the Zscaler solution under specific circumstances; however, it is always desired. Policies can be applied to traffic if the traffic is originating from a **Known Location**. The location-based policy is applied to ALL traffic/users if user authentication is not applied.

Known Locations include:

- GRE tunnel, IPSec / VPN tunnel,
- Or the customer has purchased a Dedicated Proxy port from Zscaler – all traffic destined to that port is identified as **known** (this is a special case and user-auth is required). Dedicated Proxy port is discussed in ZCCP.

The benefit of Location auth is that it is simple to implement, and one policy controls all users where the challenges are a lack policy granularity by user type / organization. Location auth also lacks visibility into users for reporting.

Slide 6 - Location or User Authentication



Location or User Authentication

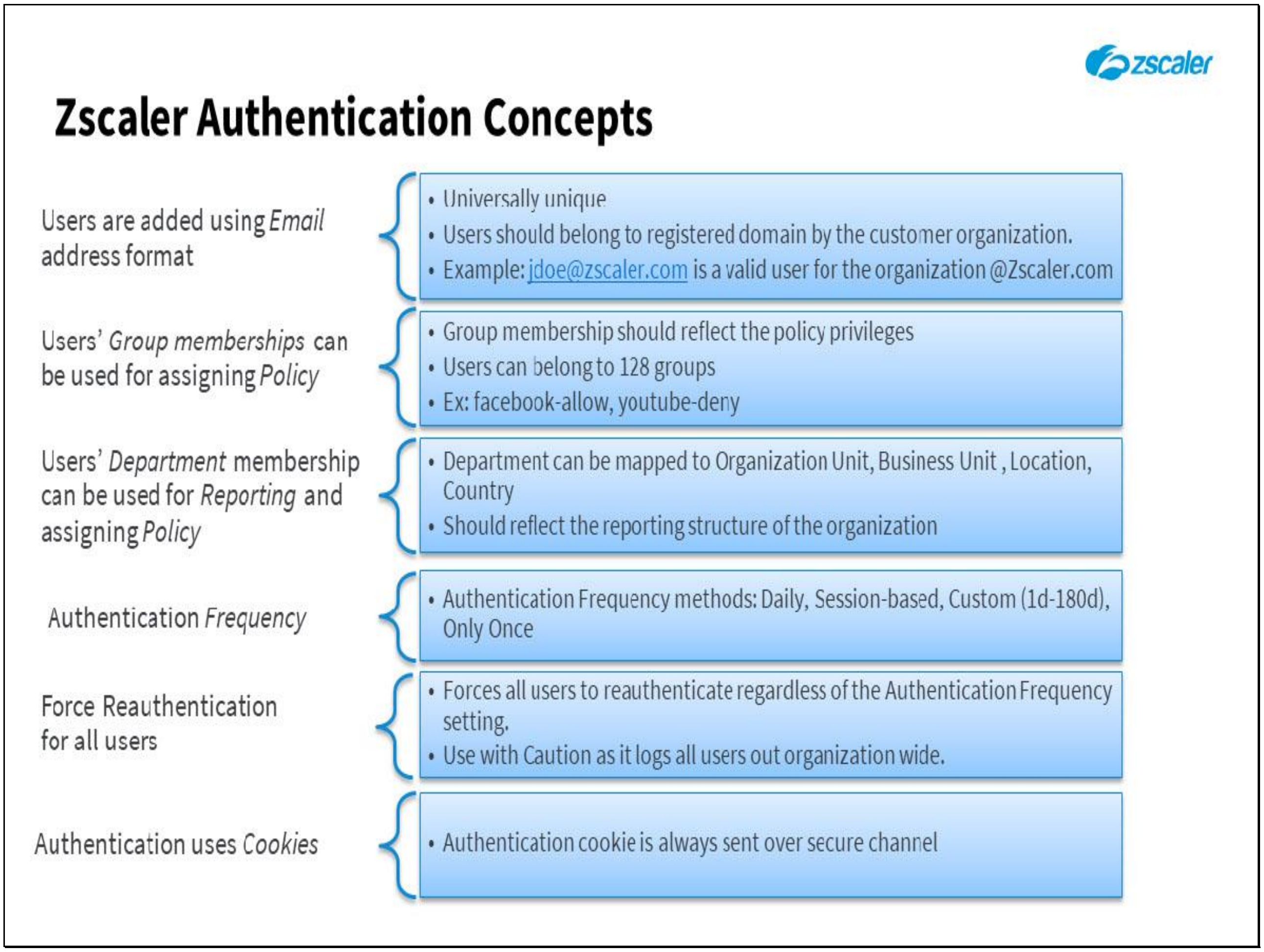
Location-based	User Authentication
Benefits	**Benefits**
• User authentication is not a requirement • Policy can be applied based on known Locations (GRE/IPSec tunnel locations, Dedicated Proxy Port) • Major advantage is simplicity	• Granular application of Policy, to; Users, Groups, Departments • Visibility to the User / Group / Department level in the logs • Compatible with a wide range of authentication providers (Hosted DB, LDAP, SAML, Kerberos)
Caveats	**Caveats**
• Lacks granularity for Policy application • No visibility to the user level in the logs	• Integration with the preferred authentication provider can be complex

Slide notes

Beyond location authentication Zscaler can also perform user authentication. User authentication provides the following benefits:

- Granular policy on individual users or users that are members of groups;
- Granular reporting on users / departments;
- Integrates with organization’s preferred authentication method.

Slide 7 - Zscaler Authentication Concepts



Zscaler Authentication Concepts

Users are added using *Email* address format

- Universally unique
- Users should belong to registered domain by the customer organization.
- Example: jdoe@zscaler.com is a valid user for the organization @Zscaler.com

Users' *Group memberships* can be used for assigning *Policy*

- Group membership should reflect the policy privileges
- Users can belong to 128 groups
- Ex: facebook-allow, youtube-deny

Users' *Department* membership can be used for *Reporting* and assigning *Policy*

- Department can be mapped to Organization Unit, Business Unit , Location, Country
- Should reflect the reporting structure of the organization

Authentication *Frequency*

- Authentication Frequency methods: Daily, Session-based, Custom (1d-180d), Only Once

Force Reauthentication for all users

- Forces all users to reauthenticate regardless of the Authentication Frequency setting.
- Use with Caution as it logs all users out organization wide.

Authentication uses *Cookies*

- Authentication cookie is always sent over secure channel

Slide notes

As mentioned in the previous slide it is beneficial to authenticate users into the system. Usernames are added as email addresses for the organization such that an employee of Zscaler, for example would have a username like jdoe@zscaler.com. Given that the user name is based off an email address it is unique. Individual users can be tied to Groups.

Individual users can be tied to Groups. The use of Groups greatly simplifies policy as a single policy, or groups of policies, can be tied to multiple users. A user can belong to up to 128 groups. Departments are used for reporting and policy and can be mapped to:

- Organization unit,
- Business unit,
- Location,
- Or country and should reflect the reporting structure of the organization.

User authentication frequency can be set to require the user to reauthenticate:

- Daily,

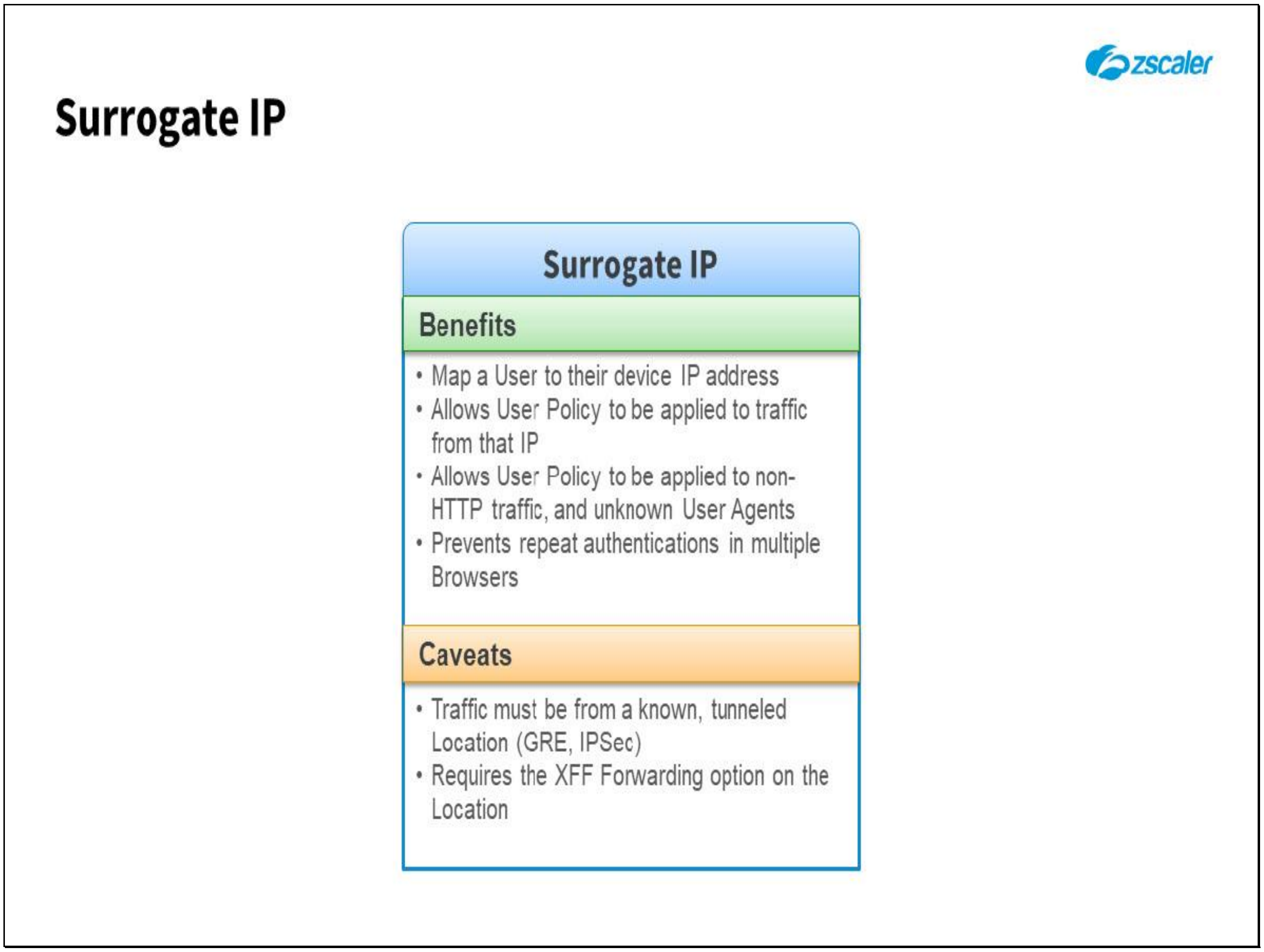
- Session based,
- A custom time period,
- Or only once.

While on the topic of Authentication Frequency there is an option to Force Reauthentication for all users. This action, if initiated by the Administrator, forces all users to reauthenticate by invalidating their authentication cookie.

This can be useful if the administrator just made changes to the Authentication Frequency or authentication method and would like them implemented immediately across all users. This can also be useful in more extreme circumstances where the administrator believes corporate passwords have been exploited and wants to force all users to immediately change their passwords rather than waiting for passwords to expire. This should be used with caution, however, as it logs all users out of the system Organization wide.

And last, authentication uses cookies. Cookies are always sent over a secure channel.

Slide 8 - Surrogate IP



Surrogate IP

Surrogate IP

Benefits

- Map a User to their device IP address
- Allows User Policy to be applied to traffic from that IP
- Allows User Policy to be applied to non-HTTP traffic, and unknown User Agents
- Prevents repeat authentications in multiple Browsers

Caveats

- Traffic must be from a known, tunneled Location (GRE, IPSec)
- Requires the XFF Forwarding option on the Location

Slide notes

In certain deployments from known locations, you can enable the Zscaler service to map a user to a device IP address, so it applies the user's policies, instead of the location's policies, to traffic that it cannot authenticate such as:

- Applications that do not support cookies such as Google Earth and Skydrive;
- HTTPS transactions that are not decrypted (SSL Interception is disabled);
- And transactions that use unknown user agents.

This mapping is called **Surrogate IP** and it allows the device IP to be mapped to the User. Non-HTTP Traffic can also have the user policy applied. Generally, a GRE tunnel or IPSec tunnel is required to support this feature. The main reason to use this feature is to authenticate unknown user agents and non-HTTP protocols.

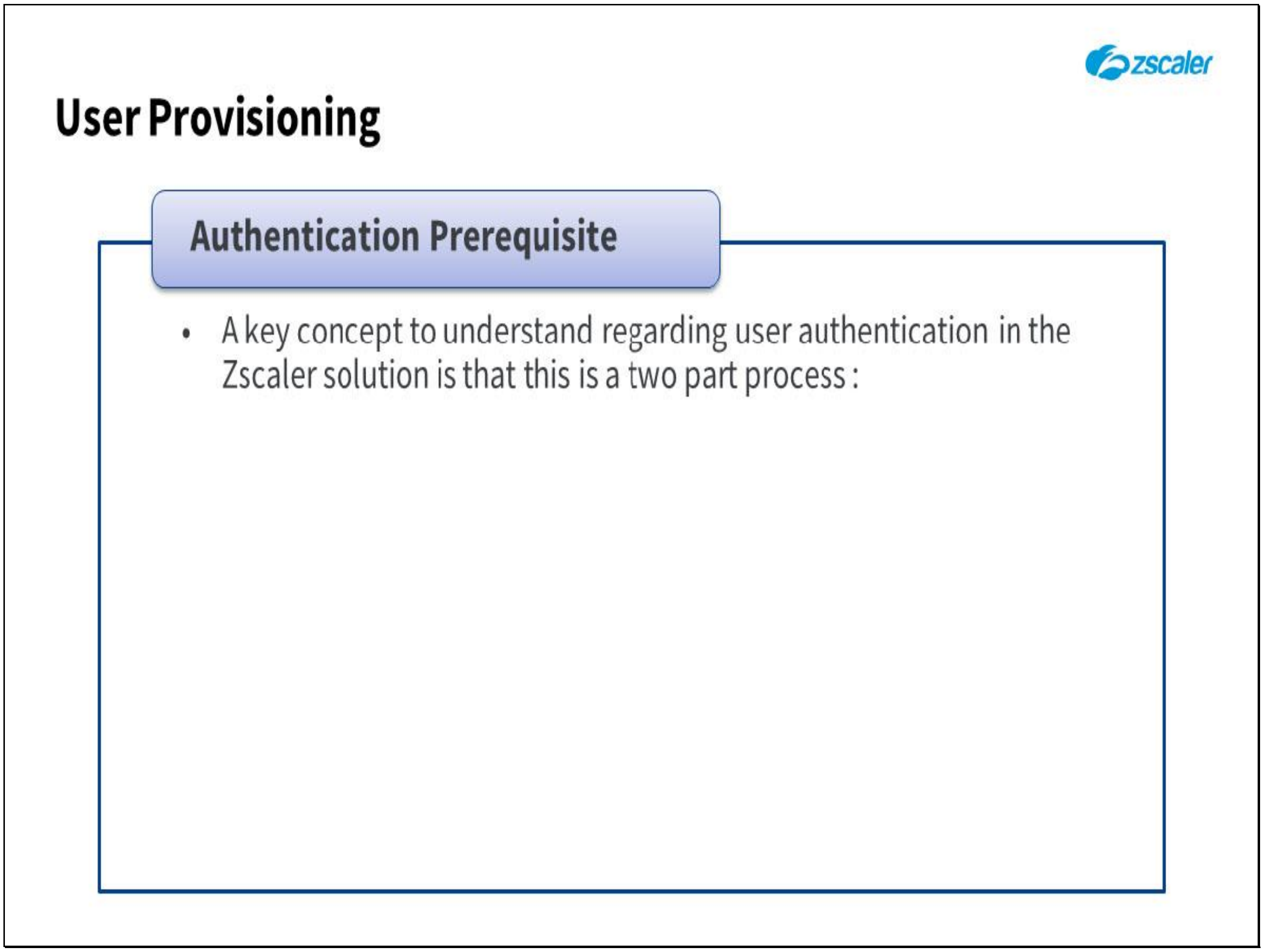
Also, when enabling the Surrogate IP Feature called **Enforce Surrogate IP for known browsers**, users will no longer need to login multiple times if using multiple different browsers such as Firefox, IE, and Chrome on the same machine providing for a smooth user experience. Without this feature users would be prompted to authenticate within each browser.

Slide 9 - User Provisioning

User Provisioning

Slide notes

Slide 10 - User Provisioning



User Provisioning

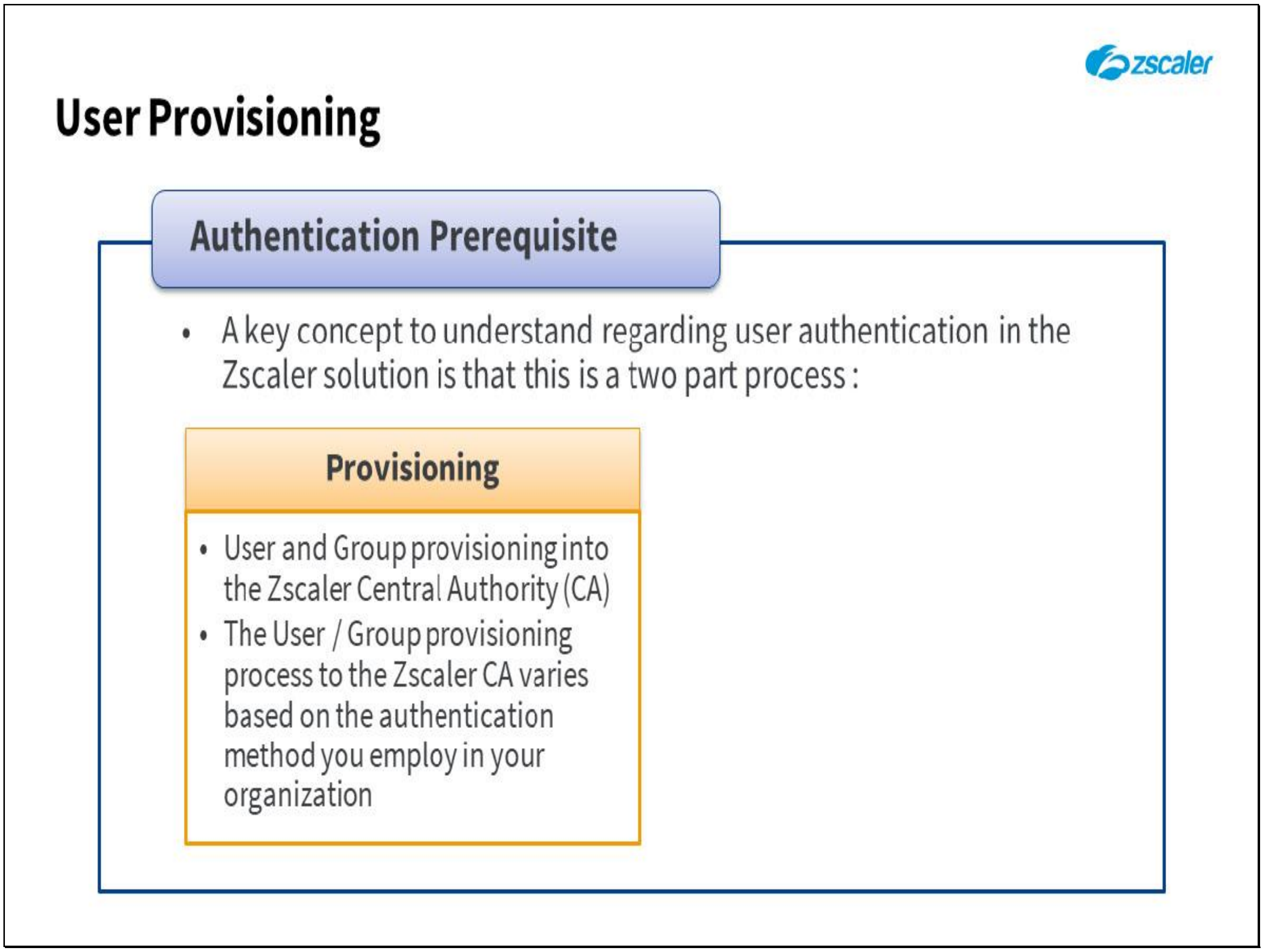
Authentication Prerequisite

- A key concept to understand regarding user authentication in the Zscaler solution is that this is a two part process :

Slide notes

A key concept to understand regarding user authentication in the Zscaler solution is that this is a two-part process.

Slide 11 - User Provisioning



User Provisioning

Authentication Prerequisite

- A key concept to understand regarding user authentication in the Zscaler solution is that this is a two part process :

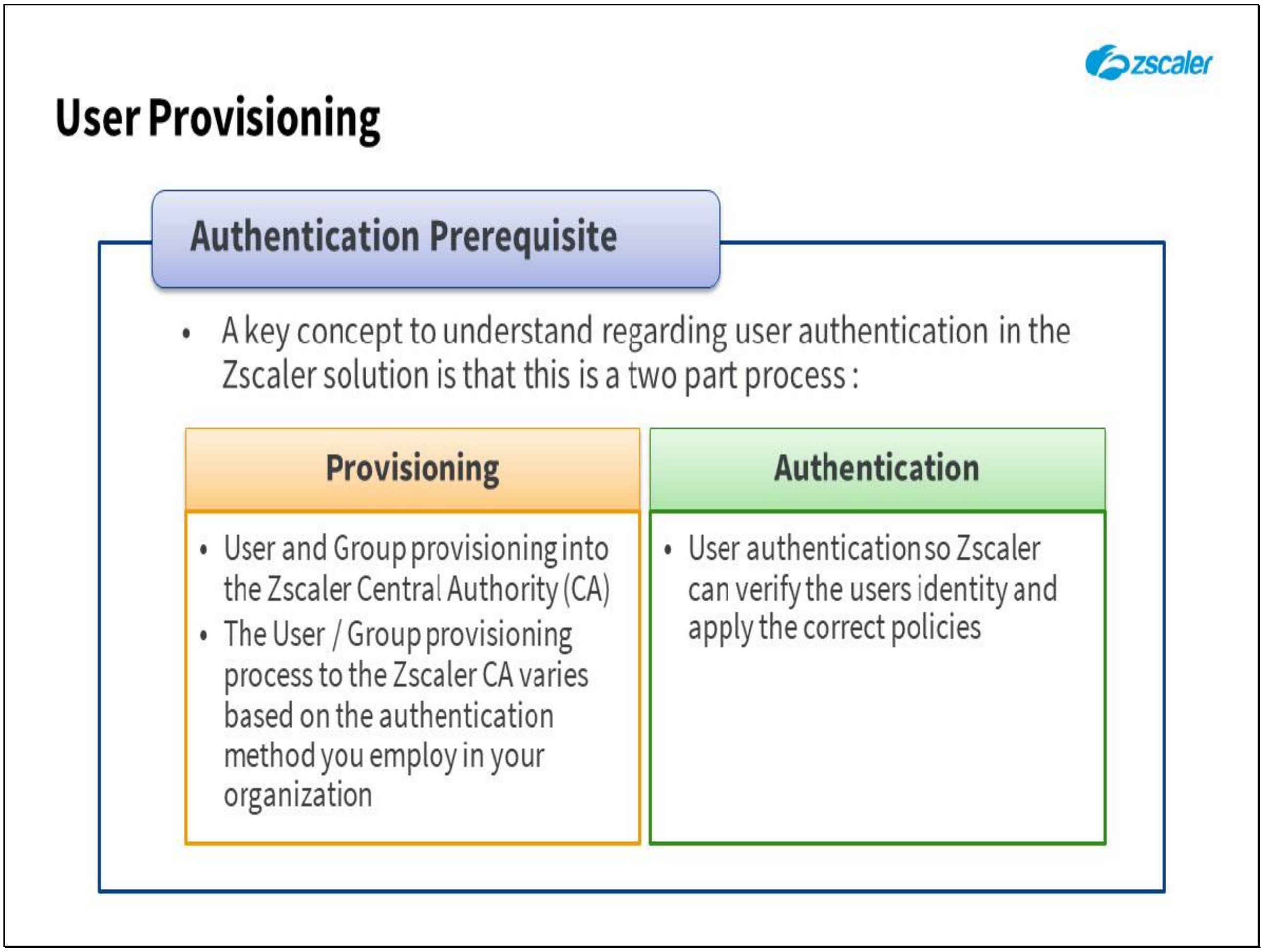
Provisioning

- User and Group provisioning into the Zscaler Central Authority (CA)
- The User / Group provisioning process to the Zscaler CA varies based on the authentication method you employ in your organization

Slide notes

User and Group membership information must be provisioned in the Zscaler Central Authority (CA). The User / Group provisioning process to the Zscaler CA varies based on the Authentication method you employ in your organization.

Slide 12 - User Provisioning



User Provisioning

Authentication Prerequisite

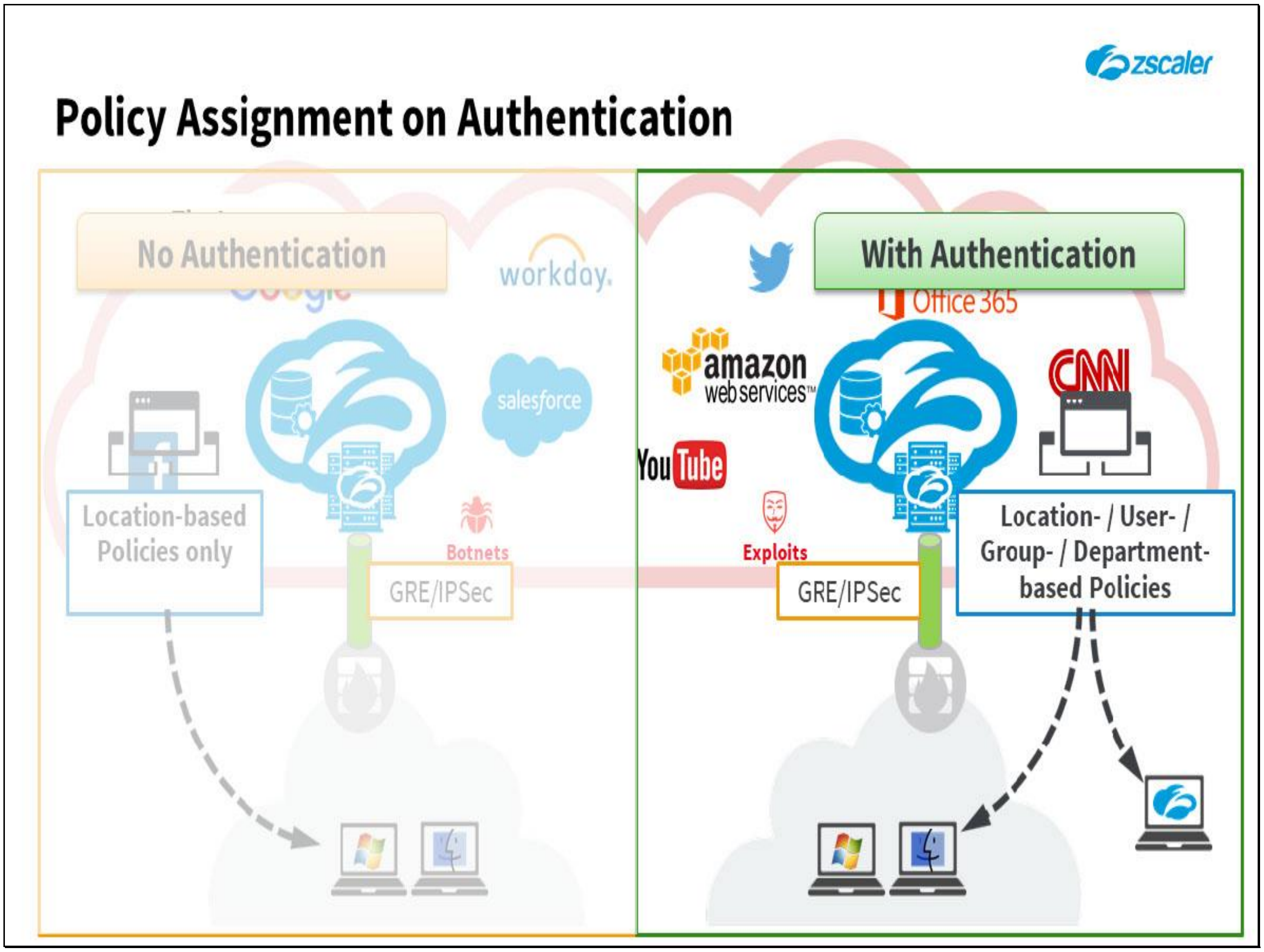
- A key concept to understand regarding user authentication in the Zscaler solution is that this is a two part process :

Provisioning	Authentication
• User and Group provisioning into the Zscaler Central Authority (CA) • The User / Group provisioning process to the Zscaler CA varies based on the authentication method you employ in your organization	• User authentication so Zscaler can verify the users identity and apply the correct policies

Slide notes

User Authentication is done so Zscaler can verify the user’s identity and apply the correct User policies.

Slide 13 - Provisioning and Authentication Flow



Policy Assignment on Authentication

Slide notes

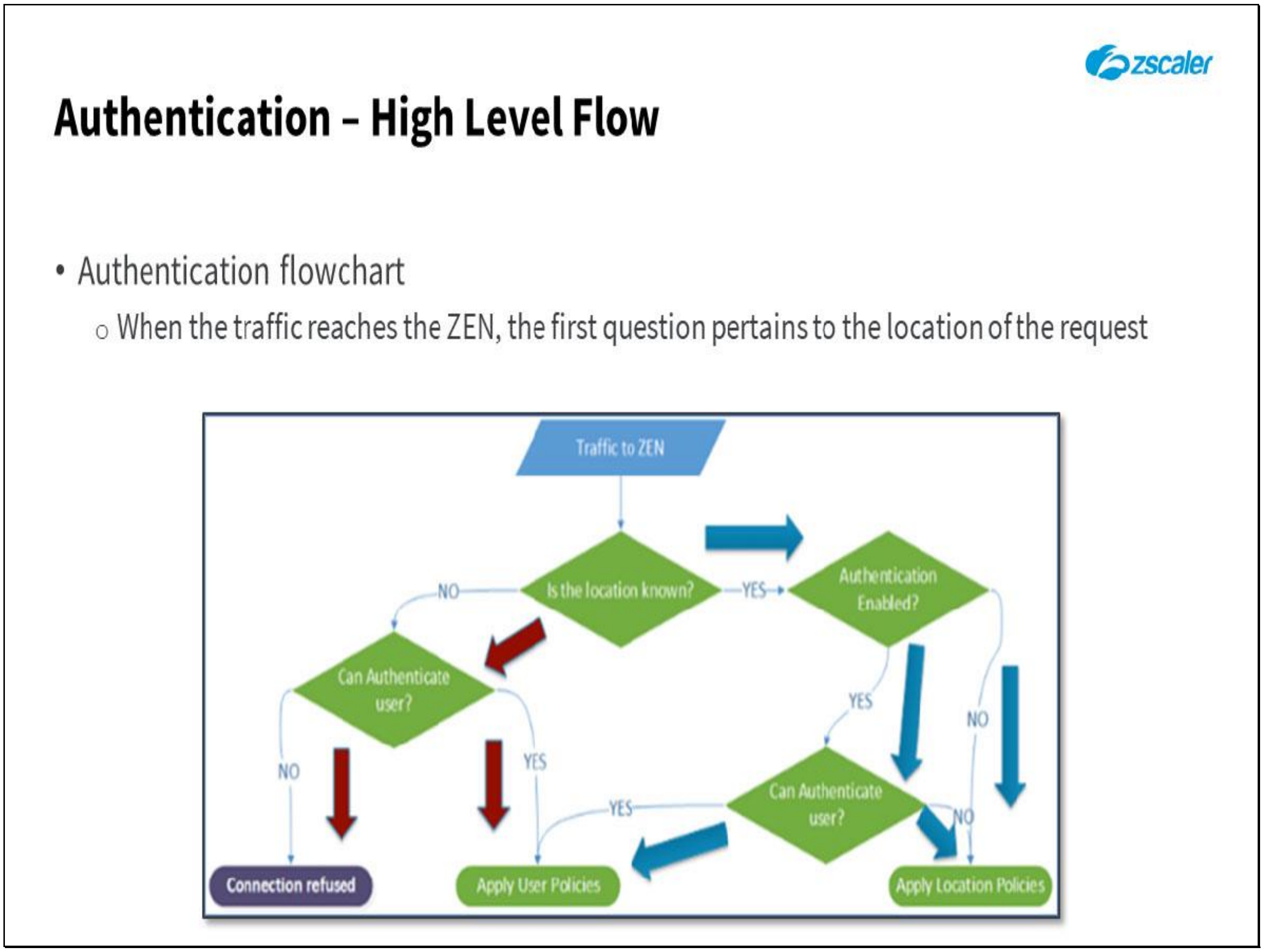
Once the user has authenticated the system sees the policy that has been assigned to the user, either directly or through their department or group memberships, which then determines the user's access privileges.

Slide 14 - Supported Authentication Methods

Supported Authentication Methods

Slide notes

Slide 15 - Authentication – High Level Flow



Authentication – High Level Flow

- Authentication flowchart
  - When the traffic reaches the ZEN, the first question pertains to the location of the request

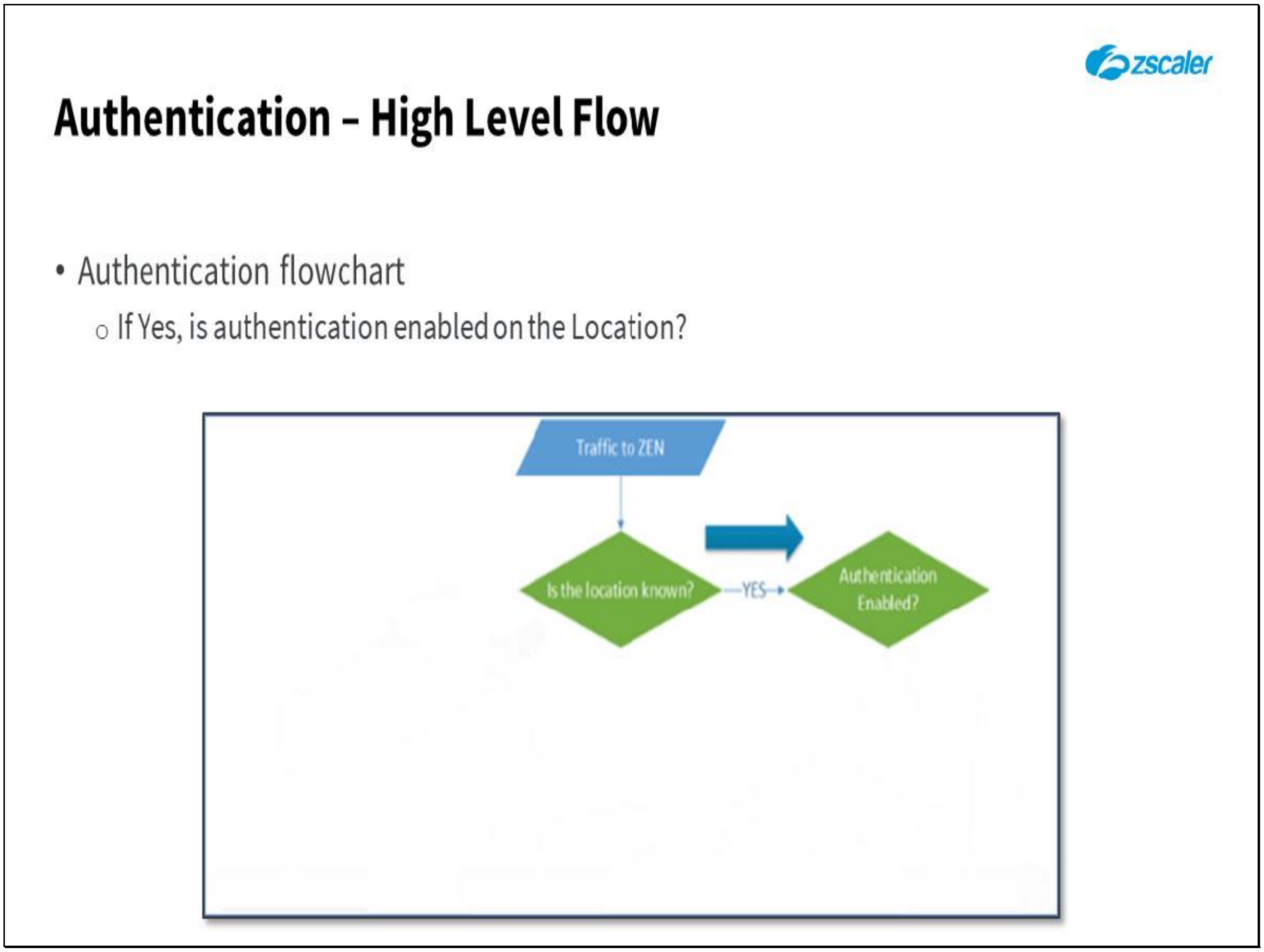
Slide notes

This flowchart represents, at a very high-level, the authentication process within the Zscaler cloud. When the traffic reaches the ZEN, the first determination pertains to the location of the request.

Is the user coming from a known location? Known locations are requests coming from static IP addresses or Dedicated Proxy Ports (TCP ports associated to a company account and mapped as a location for that organization). Aggressive mode IPSec VPN connections also count as known locations.

Let’s follow the flowchart starting with the case when the request comes from a known location (the blue arrows):

Slide 16 - Authentication – High Level Flow



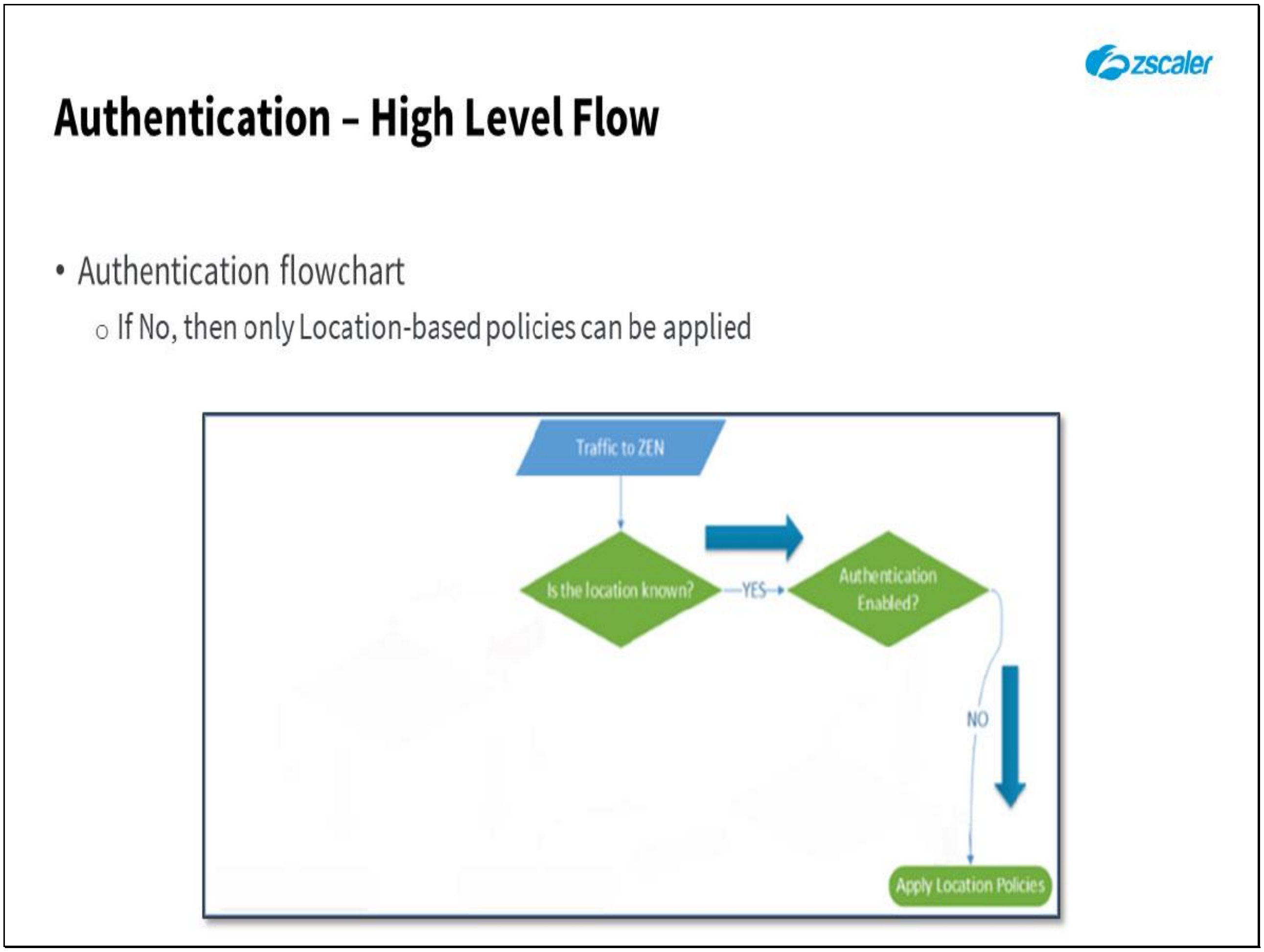
Authentication – High Level Flow

- Authentication flowchart
  - If Yes, is authentication enabled on the Location?

Slide notes

Traffic, or users, coming from a known location does not need to be authenticated. This is a decision than can be made on a per location basis. So, the first step is to determine if user authentication is to be enabled for that location.

Slide 17 - Authentication – High Level Flow



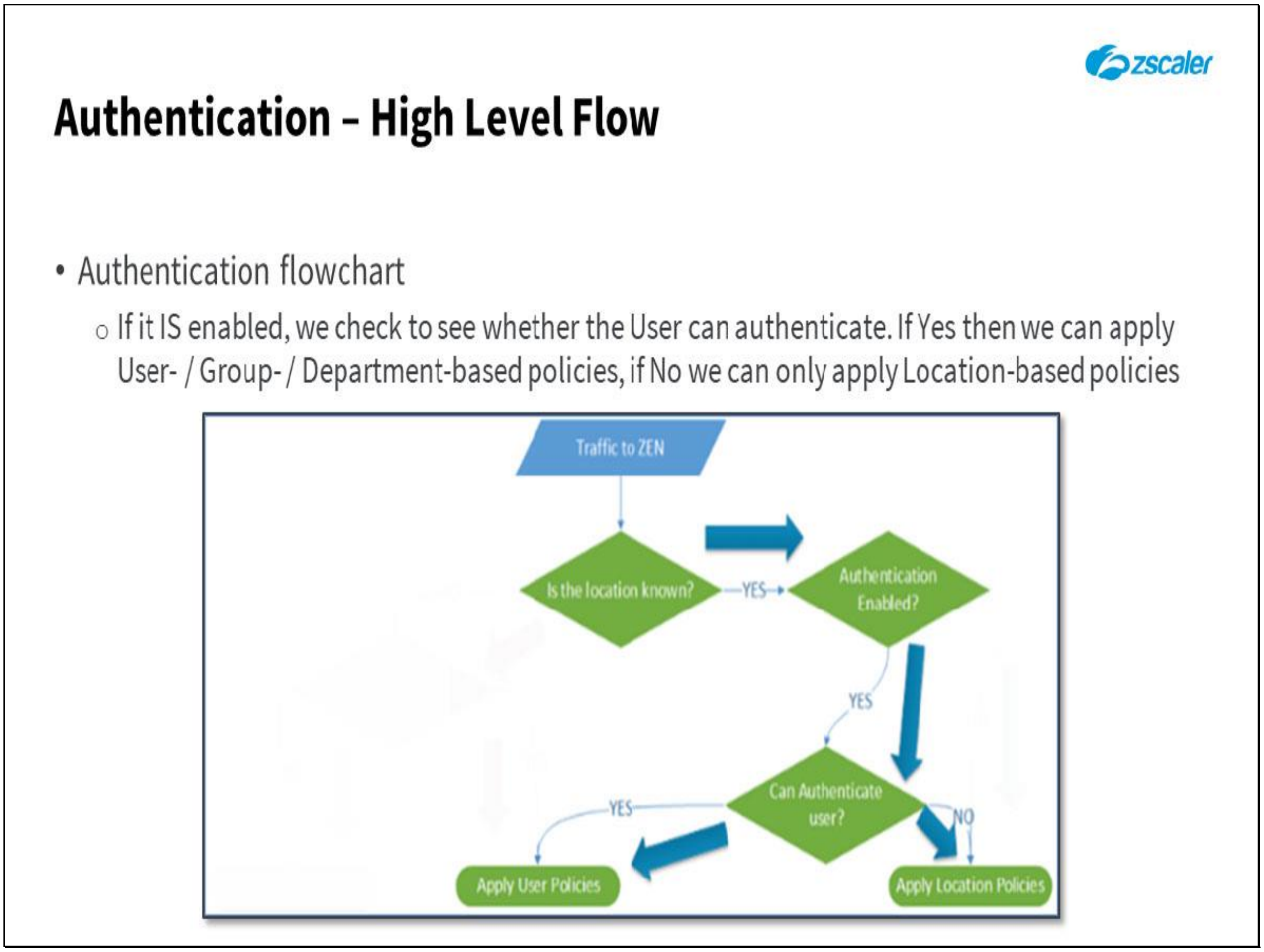
Authentication – High Level Flow

- Authentication flowchart
  - If No, then only Location-based policies can be applied

Slide notes

If authentication for that location is not required, then only location-specific policies will apply.

Slide 18 - Authentication – High Level Flow



Authentication – High Level Flow

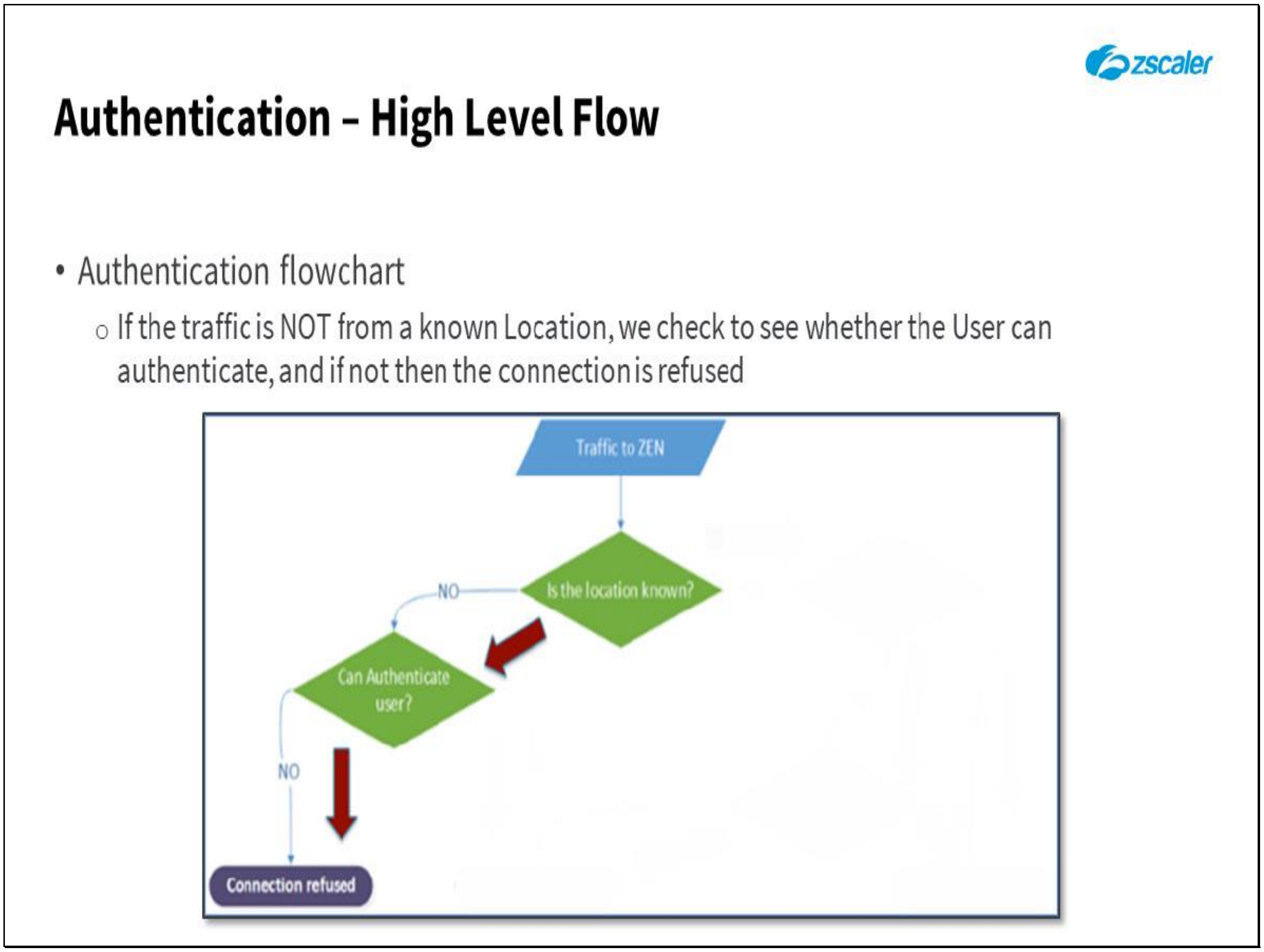
- Authentication flowchart
  - If it IS enabled, we check to see whether the User can authenticate. If Yes then we can apply User- / Group- / Department-based policies, if No we can only apply Location-based policies

Slide notes

If authentication is enabled and the user can authenticate, then both user-specific and location-specific policies will apply. If the user cannot authenticate, for instance the traffic is SSL and SSL Inspection is not enabled, then only location-specific polices apply for that request.

Now let's now look at the case where the user request comes from an unknown location (the red arrows):

Slide 19 - Authentication – High Level Flow



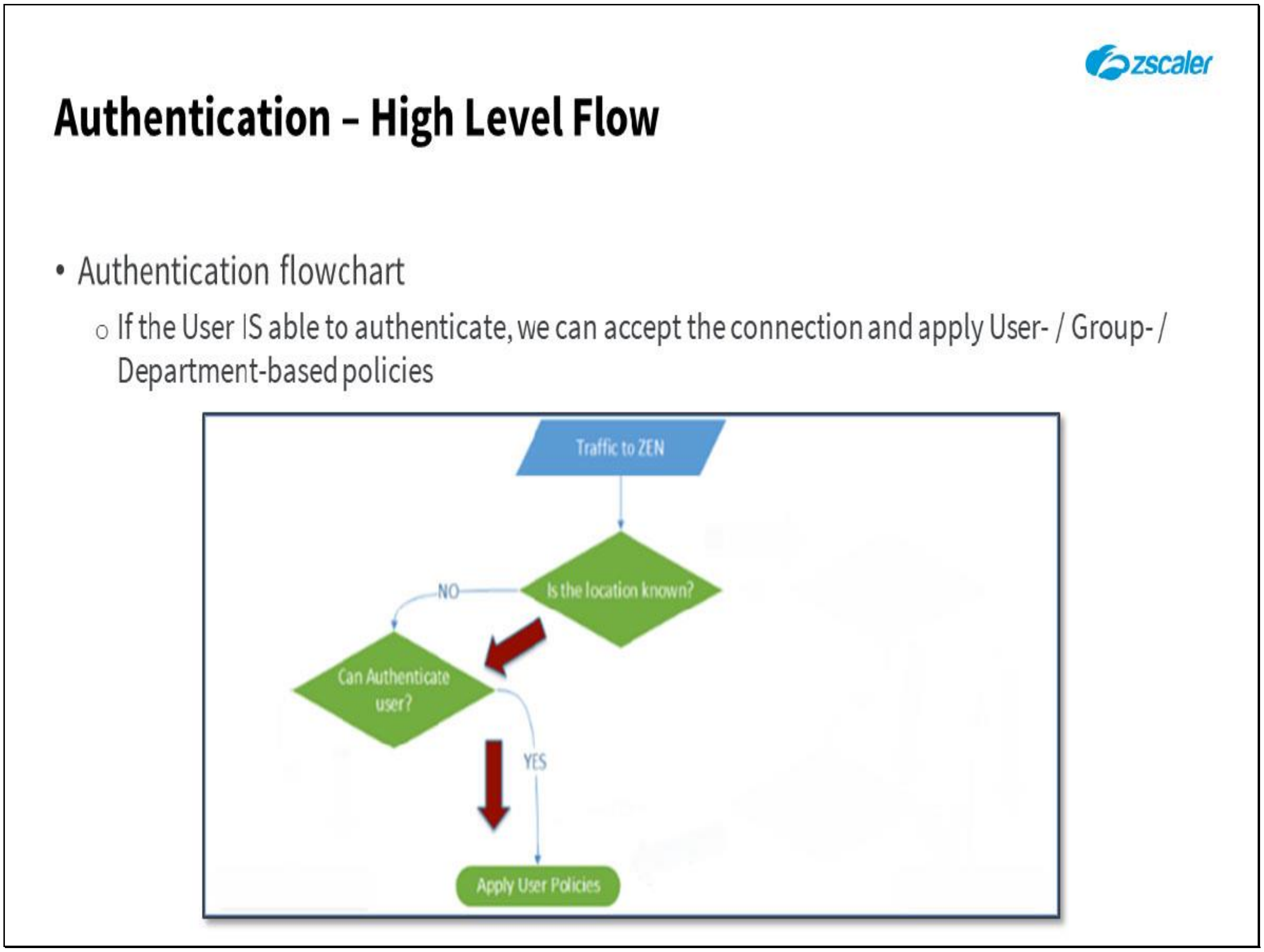
Authentication – High Level Flow

- Authentication flowchart
  - If the traffic is NOT from a known Location, we check to see whether the User can authenticate, and if not then the connection is refused

Slide notes

The first check Zscaler performs is simple: Can the user authenticate? If the user cannot authenticate because the protocol does not support authentication, or the user agent does not support cookies, or the credential provided are incorrect, then Zscaler refuses access.

Slide 20 - Authentication – High Level Flow



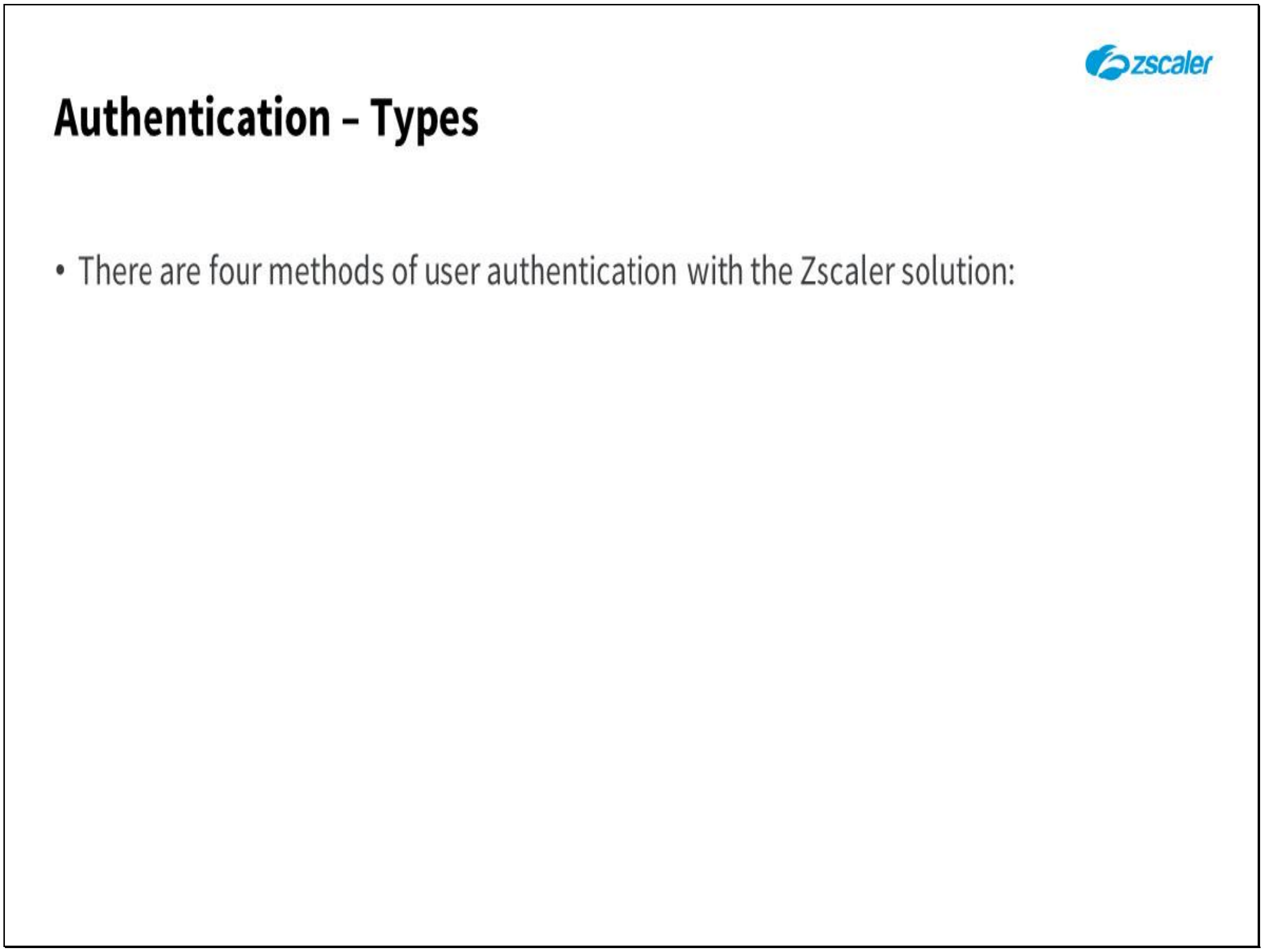
Authentication – High Level Flow

- Authentication flowchart
  - If the User IS able to authenticate, we can accept the connection and apply User- / Group- / Department-based policies

Slide notes

If the user can authenticate successfully, then user-specific policies apply to this transaction.

Slide 21 - Slide 21



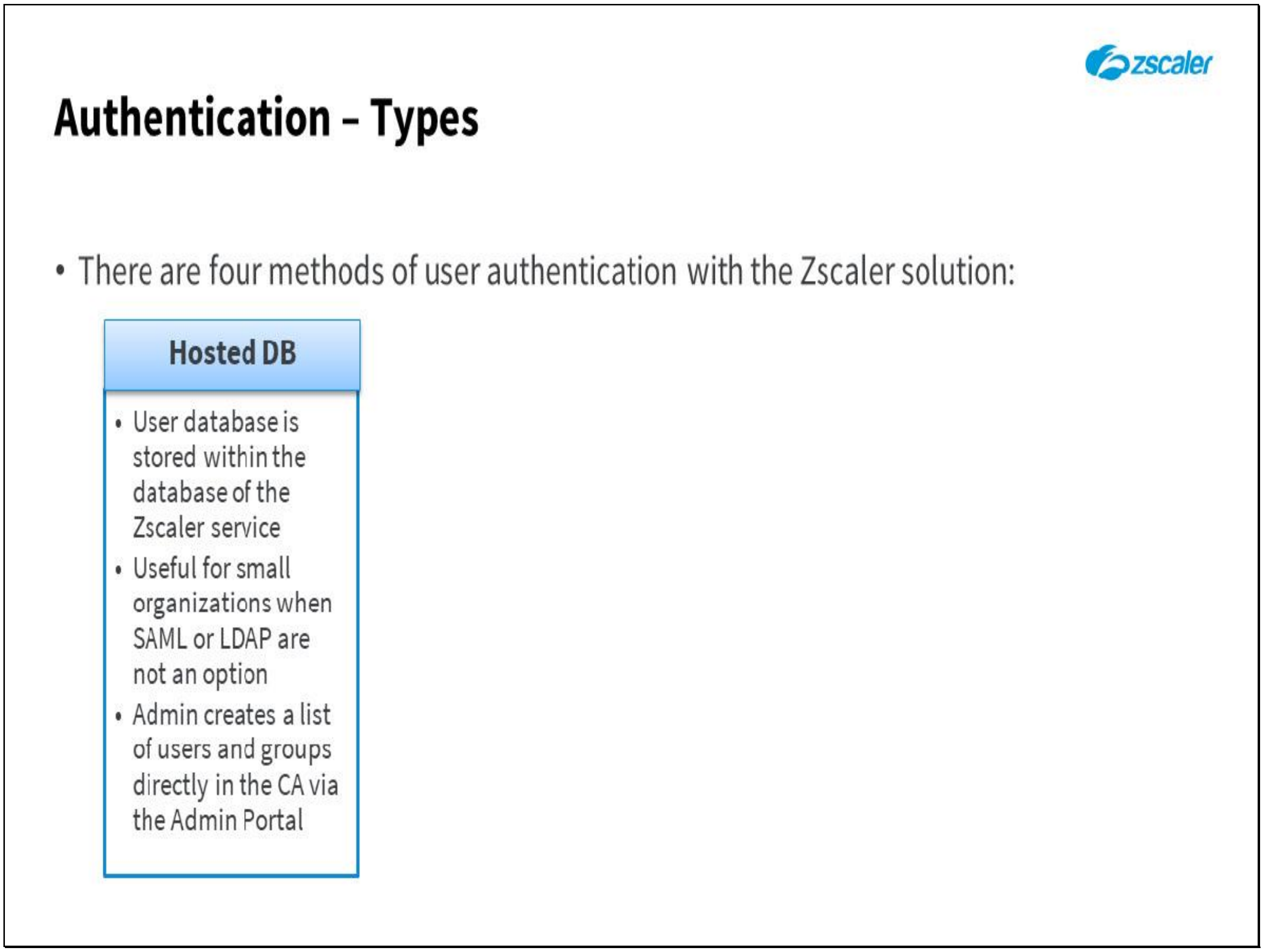
Authentication – Types

- There are four methods of user authentication with the Zscaler solution:

Slide notes

There are four methods of User authentication with the Zscaler solution:

Slide 22 - Authentication – Types



Authentication – Types

- There are four methods of user authentication with the Zscaler solution:

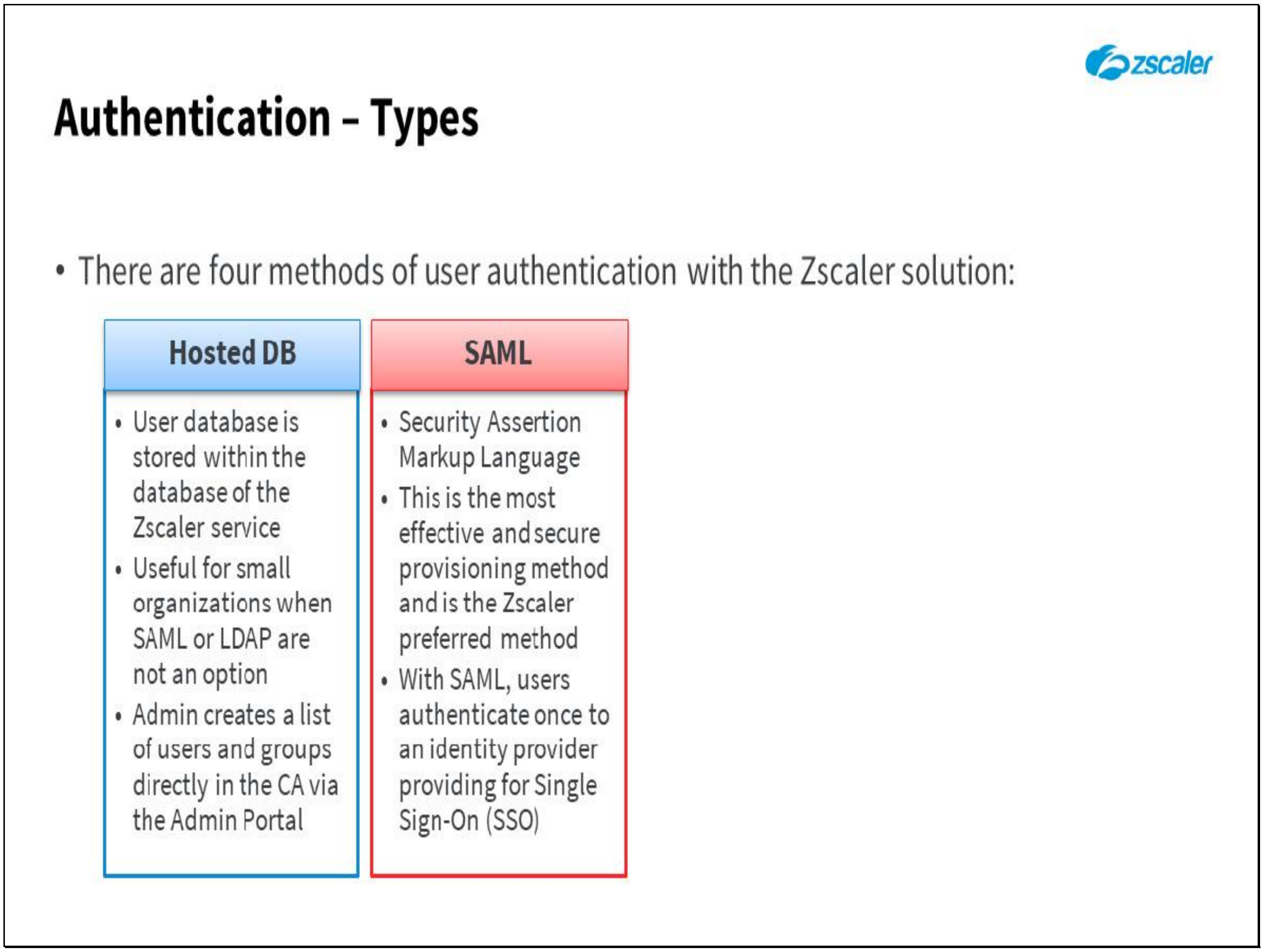
Hosted DB

- User database is stored within the database of the Zscaler service
- Useful for small organizations when SAML or LDAP are not an option
- Admin creates a list of users and groups directly in the CA via the Admin Portal

Slide notes

The first method is the Hosted Database. With the Hosted DB the User database with both username and password is stored within the database of the Zscaler service. This is useful for small organizations when SAML, LDAP, or Kerberos are not an option. The Admin creates a list of users and groups directly in the CA via the Admin Portal UI.

Slide 23 - Authentication – Types



Authentication – Types

- There are four methods of user authentication with the Zscaler solution:

Hosted DB

- User database is stored within the database of the Zscaler service
- Useful for small organizations when SAML or LDAP are not an option
- Admin creates a list of users and groups directly in the CA via the Admin Portal

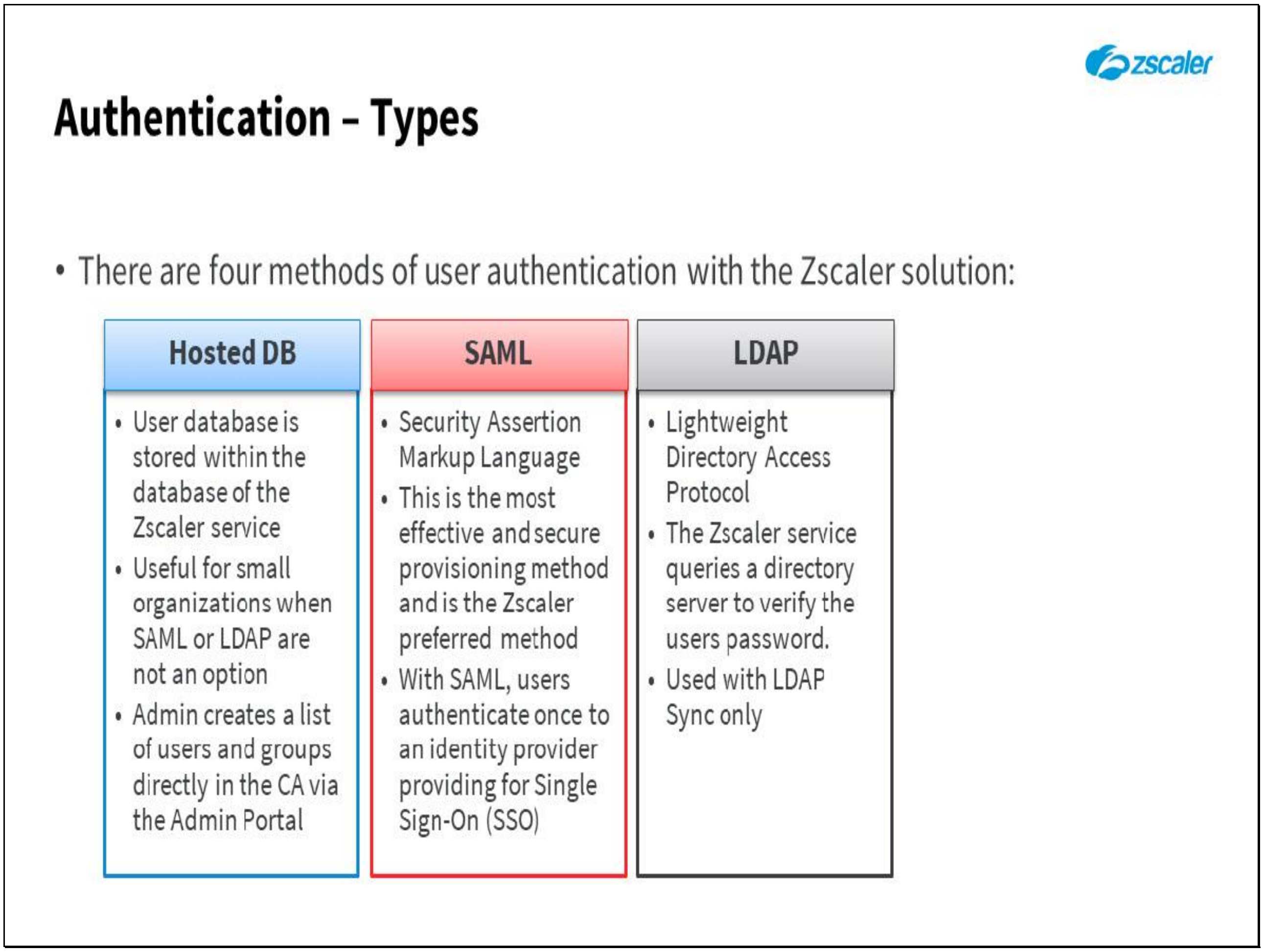
SAML

- Security Assertion Markup Language
- This is the most effective and secure provisioning method and is the Zscaler preferred method
- With SAML, users authenticate once to an identity provider providing for Single Sign-On (SSO)

Slide notes

SAML, or Security Assertion Markup Language, is the most effective and secure provisioning method. With SAML, users authenticate once to an identity provider providing for Single Sign-On (SSO).

Slide 24 - Authentication – Types



Authentication – Types

- There are four methods of user authentication with the Zscaler solution:

Hosted DB

- User database is stored within the database of the Zscaler service
- Useful for small organizations when SAML or LDAP are not an option
- Admin creates a list of users and groups directly in the CA via the Admin Portal

SAML

- Security Assertion Markup Language
- This is the most effective and secure provisioning method and is the Zscaler preferred method
- With SAML, users authenticate once to an identity provider providing for Single Sign-On (SSO)

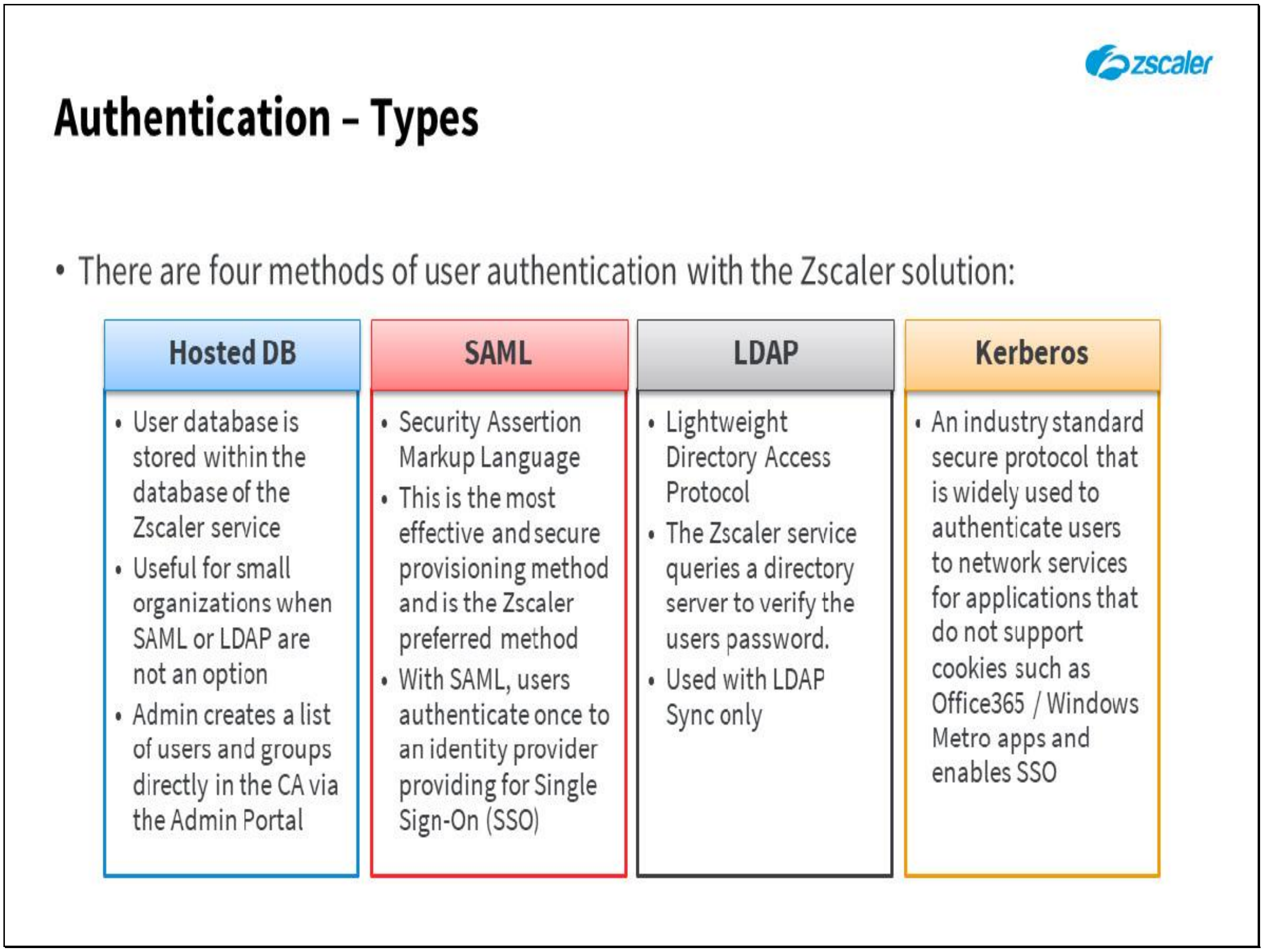
LDAP

- Lightweight Directory Access Protocol
- The Zscaler service queries a directory server to verify the users password.
- Used with LDAP Sync only

Slide notes

With LDAP or Lightweight Directory Access Protocol the Zscaler service queries a directory server to verify the user’s password. Used with LDAP Synch only.

Slide 25 - Authentication – Types



zscaler

Authentication – Types

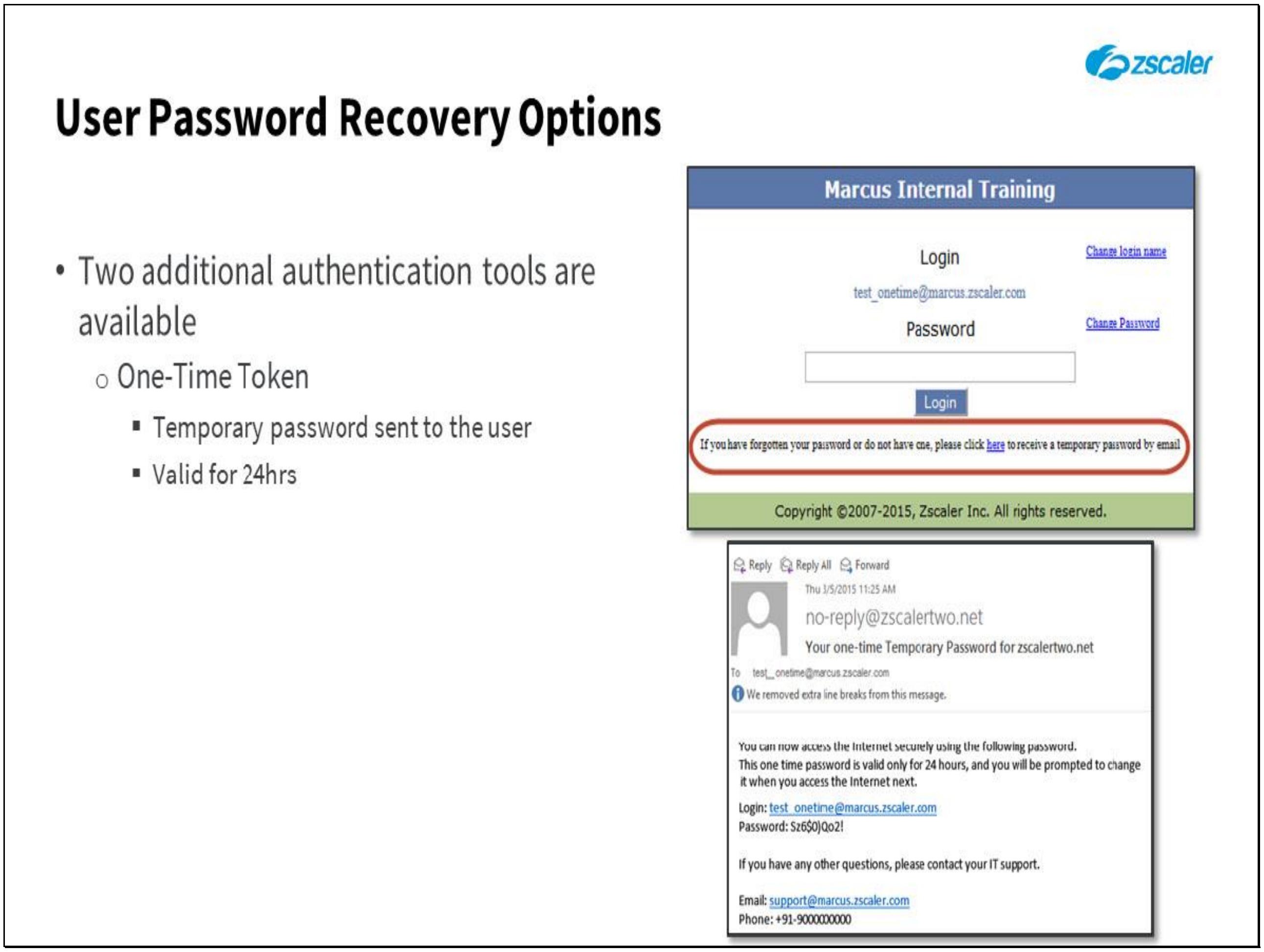
- There are four methods of user authentication with the Zscaler solution:

Hosted DB	SAML	LDAP	Kerberos
• User database is stored within the database of the Zscaler service • Useful for small organizations when SAML or LDAP are not an option • Admin creates a list of users and groups directly in the CA via the Admin Portal	• Security Assertion Markup Language • This is the most effective and secure provisioning method and is the Zscaler preferred method • With SAML, users authenticate once to an identity provider providing for Single Sign-On (SSO)	• Lightweight Directory Access Protocol • The Zscaler service queries a directory server to verify the users password. • Used with LDAP Sync only	• An industry standard secure protocol that is widely used to authenticate users to network services for applications that do not support cookies such as Office365 / Windows Metro apps and enables SSO

Slide notes

Kerberos is an industry standard secure protocol that is widely used to authenticate users to network services for applications that do not support cookies such as Office365 and enables SSO.

Slide 26 - User Password Recovery Options



User Password Recovery Options

- Two additional authentication tools are available
  - One-Time Token
    - Temporary password sent to the user
    - Valid for 24hrs

Marcus Internal Training

Login

test_onetime@marcus.zscaler.com

Password

If you have forgotten your password or do not have one, please click here to receive a temporary password by email

Copyright ©2007-2015, Zscaler Inc. All rights reserved.

Thu 3/5/2015 11:25 AM

no-reply@zscalertwo.net

Your one-time Temporary Password for zscalertwo.net

To test_onetime@marcus.zscaler.com

We removed extra line breaks from this message.

You can now access the Internet securely using the following password.
This one time password is valid only for 24 hours, and you will be prompted to change it when you access the Internet next.

Login: test_onetime@marcus.zscaler.com
Password: Sz6$0)Qo2!

If you have any other questions, please contact your IT support.

Email: support@marcus.zscaler.com
Phone: +91-900000000

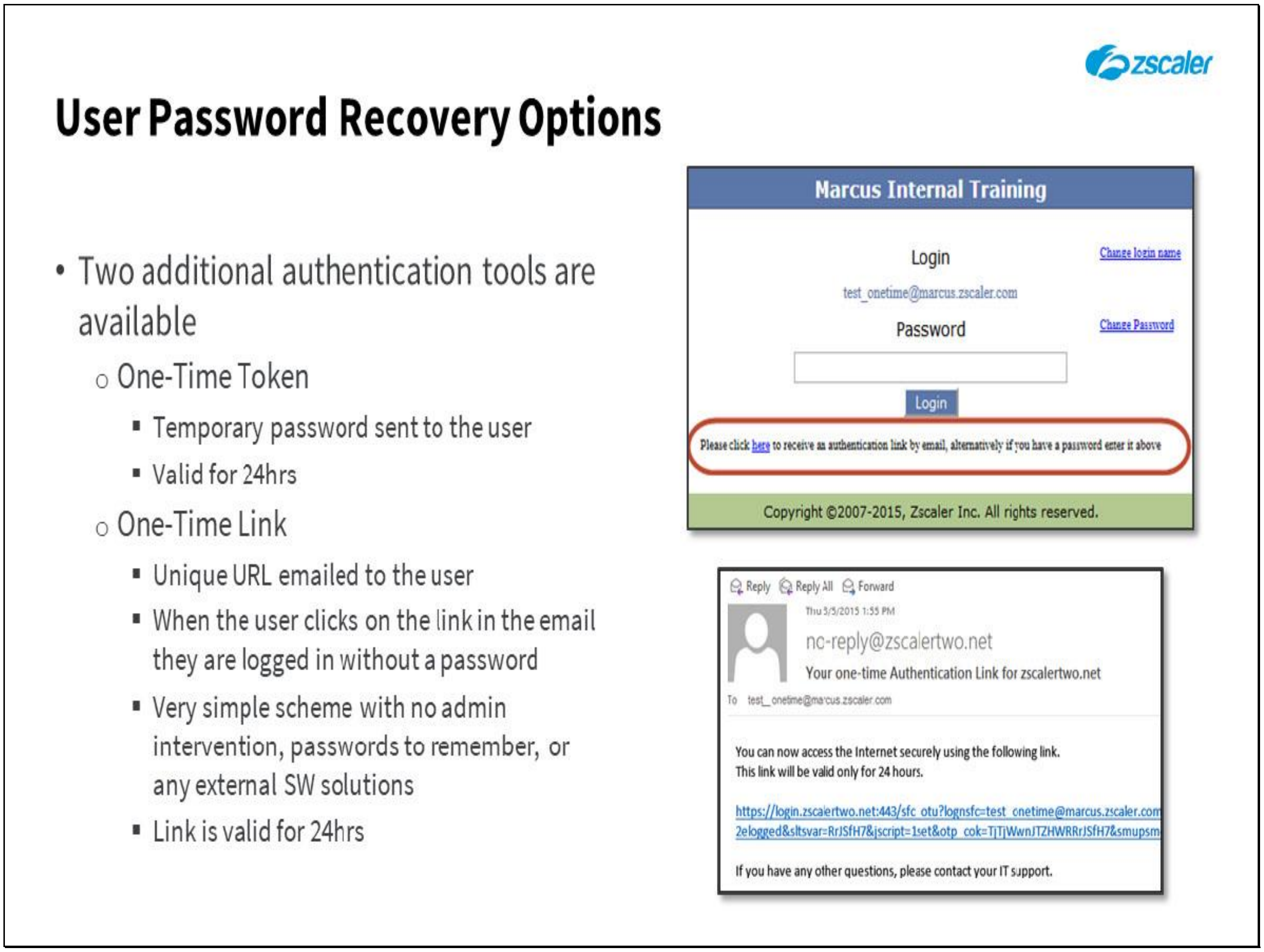
Slide notes

Two additional authentication tools are available. The purpose of these tools is to offload password management from the admin and allow the user to manage access.

1. The first is **One-Time Token**: The One-Time Token allows the end-users to recover a lost password via email without the Admin's intervention. The user simply clicks on the password recovery link on the bottom of the page.

   Note: this link will only appear if the feature is enabled. If the username is valid and an email address is tied to the account, the user will receive a temporary password via email.

Slide 27 - User Password Recovery Options



User Password Recovery Options

- Two additional authentication tools are available
  - One-Time Token
    - Temporary password sent to the user
    - Valid for 24hrs
  - One-Time Link
    - Unique URL emailed to the user
    - When the user clicks on the link in the email they are logged in without a password
    - Very simple scheme with no admin intervention, passwords to remember, or any external SW solutions
    - Link is valid for 24hrs

Marcus Internal Training

Login

test_onetime@marcus.zscaler.com

Change login name

Password

Change Password

Login

Please click here to receive an authentication link by email, alternatively if you have a password enter it above

Copyright ©2007-2015, Zscaler Inc. All rights reserved.

Thu 5/5/2015 1:55 PM

nc-reply@zscalertwo.net

Your one-time Authentication Link for zscalertwo.net

To test_onetime@marcus.zscaler.com

You can now access the Internet securely using the following link.
This link will be valid only for 24 hours.

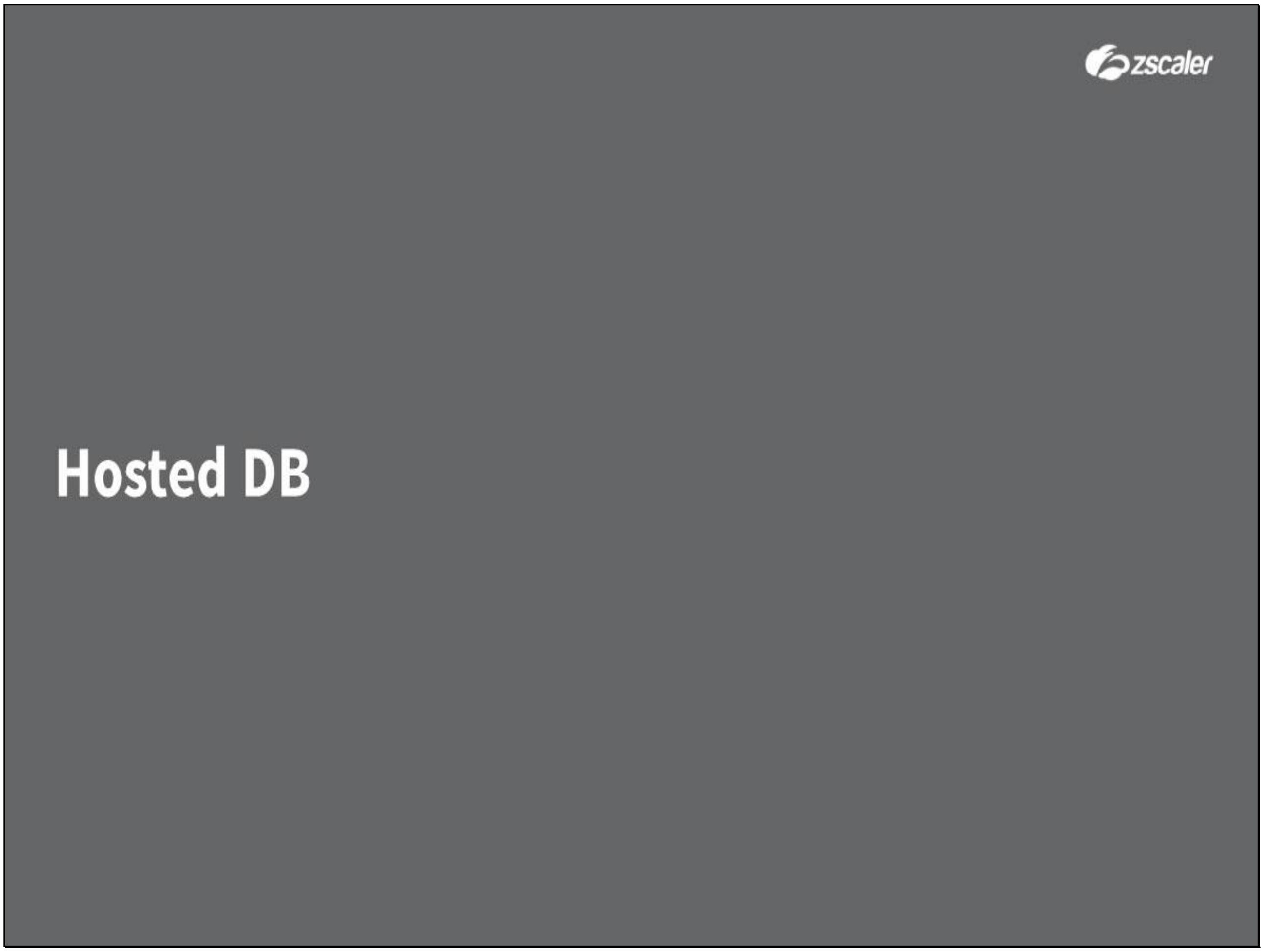
https://login.zscalertwo.net:443/sfc_otu?lognsfc=test_onetime@marcus.zscaler.com
2elogged&sltsvar=RrJSfH7&jscript=1set&otp_cok=TjTjWwnJTZHWRRrJSfH7&smupsm

If you have any other questions, please contact your IT support.

Slide notes

2. The next tool is **One-Time Link**: While similar to One-Time Token, in that it offloads password administration from the Admin to the user, it does so by simply providing the user a link, which replaces the user's password, via email.

Slide 28 - Hosted DB

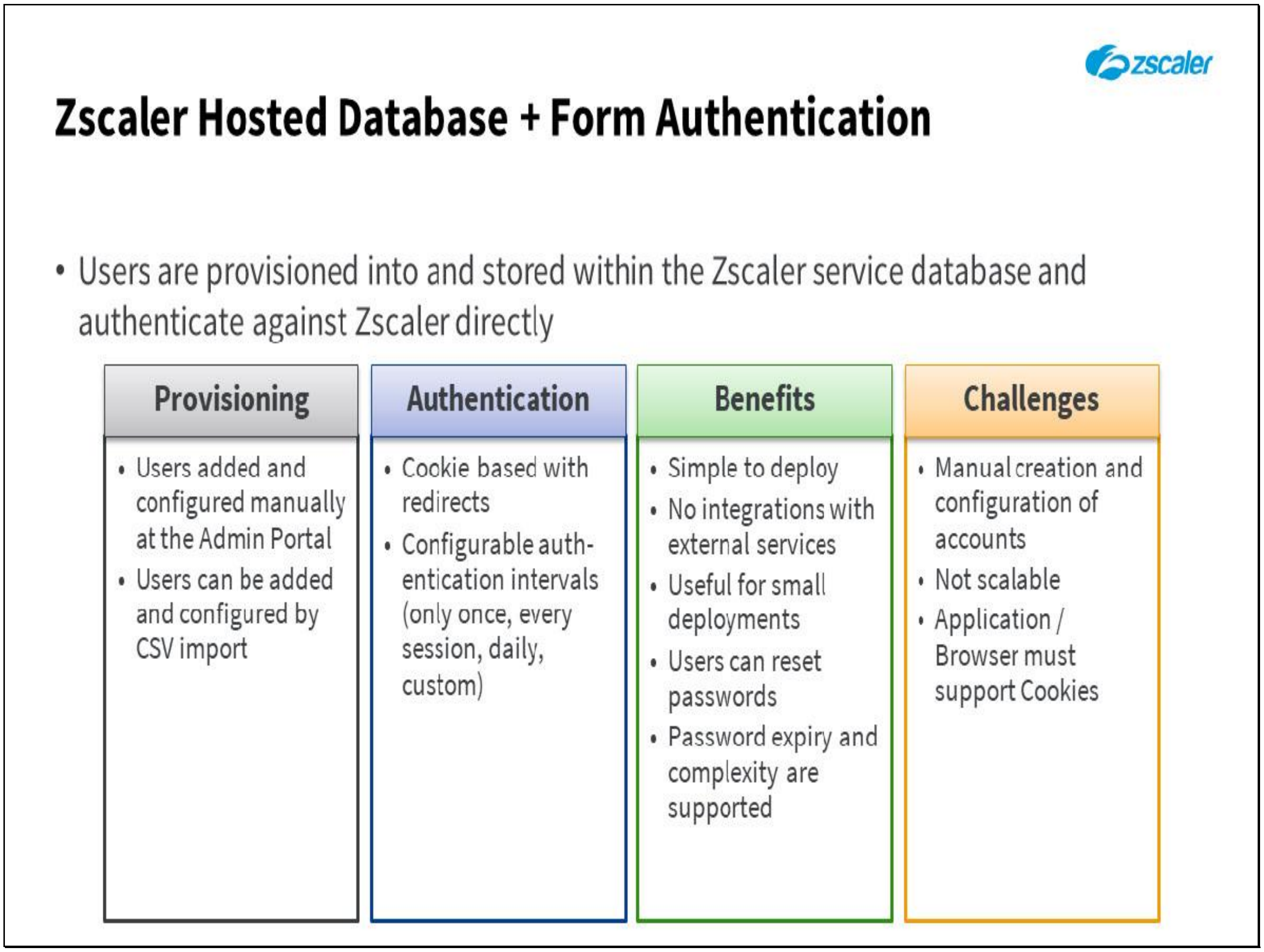


zscaler

Hosted DB

Slide notes

Slide 29 - Zscaler Hosted Database + Form Authentication



Zscaler Hosted Database + Form Authentication

- Users are provisioned into and stored within the Zscaler service database and authenticate against Zscaler directly

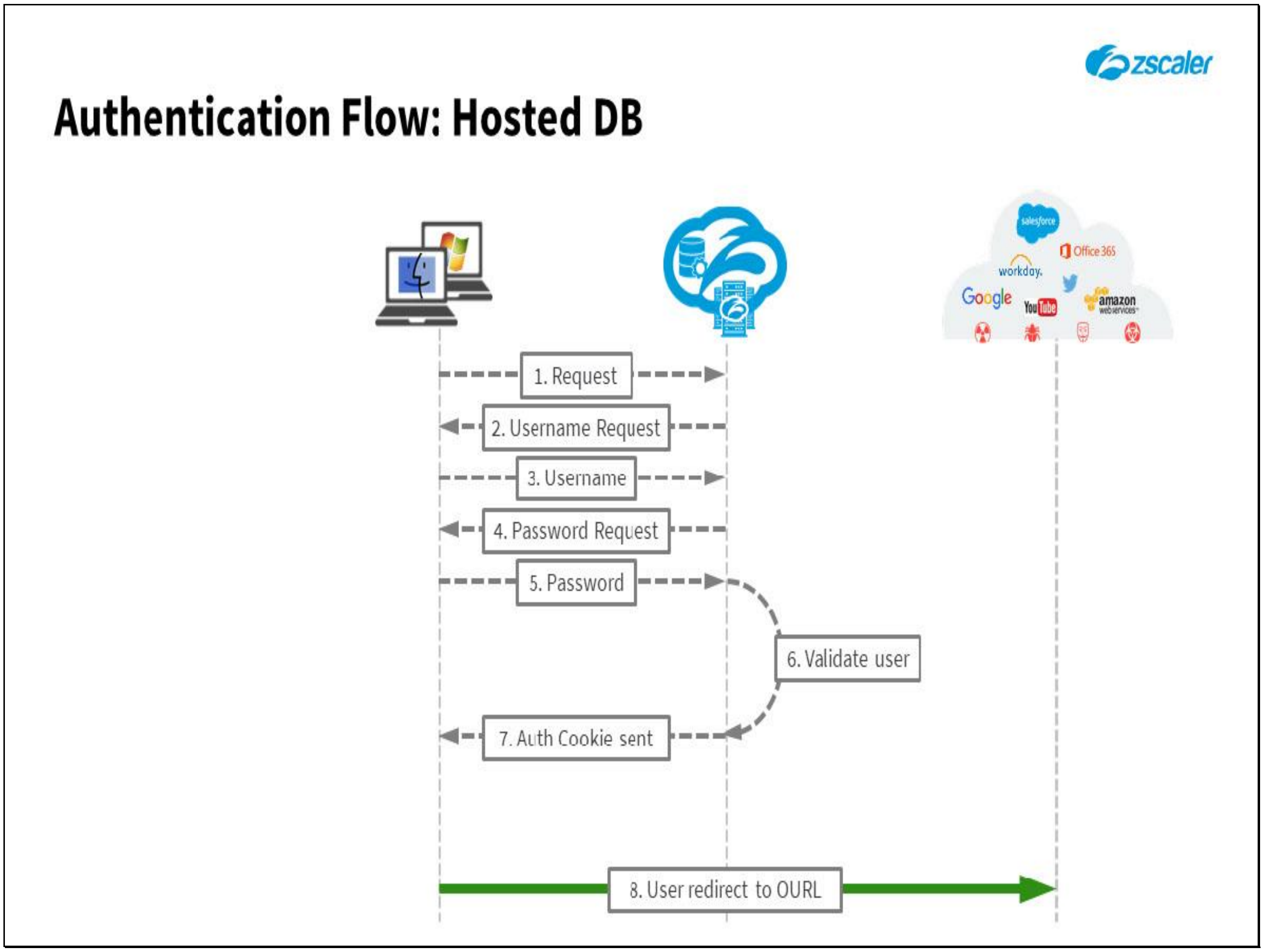
Provisioning	Authentication	Benefits	Challenges
• Users added and configured manually at the Admin Portal • Users can be added and configured by CSV import	• Cookie based with redirects • Configurable authentication intervals (only once, every session, daily, custom)	• Simple to deploy • No integrations with external services • Useful for small deployments • Users can reset passwords • Password expiry and complexity are supported	• Manual creation and configuration of accounts • Not scalable • Application / Browser must support Cookies

Slide notes

The first, and most basic authentication method supported by Zscaler is the Hosted database.

- User provisioning is a manual process by the administrator and requires the Admin to create the user accounts via the Admin Portal UI. The user list, alternatively, can be compiled in a CSV then uploaded to Zscaler.
- Authentication is cookie based with redirects and user authentication can be set to require the user to authenticate daily, only once, every session, or each time the browser closes or the cookies are deleted, or a custom time period.
- The benefits of the Hosted DB are that it is simple to implement. No external authentication methods to deploy. It is also useful in a small deployment with a limited number of users.
- The Challenges are that the Administrator must manually create each entry, manually, in the Admin Portal UI or upload a user list in CSV and this method does not scale as easily as other auth methods.

Slide 30 - Authentication Flow – Hosted DB



Authentication Flow: Hosted DB

1. Request

2. Username Request

3. Username

4. Password Request

5. Password

6. Validate user

7. Auth Cookie sent

8. User redirect to OURL

Slide notes

This image details the authentication process when the users are provisioned in a database hosted on Zscaler Cloud. Let’s walk through the process:

1. The user sends a request to Zscaler,
2. Zscaler sends the request for the username,
3. The user returns the username,
4. Zscaler sends the request for the password,
5. The user returns the password to Zscaler,
6. Zscaler validates the credentials against its database,
7. Zscaler sends the cookie to the user,
8. And last the user is redirected to its original URL request.

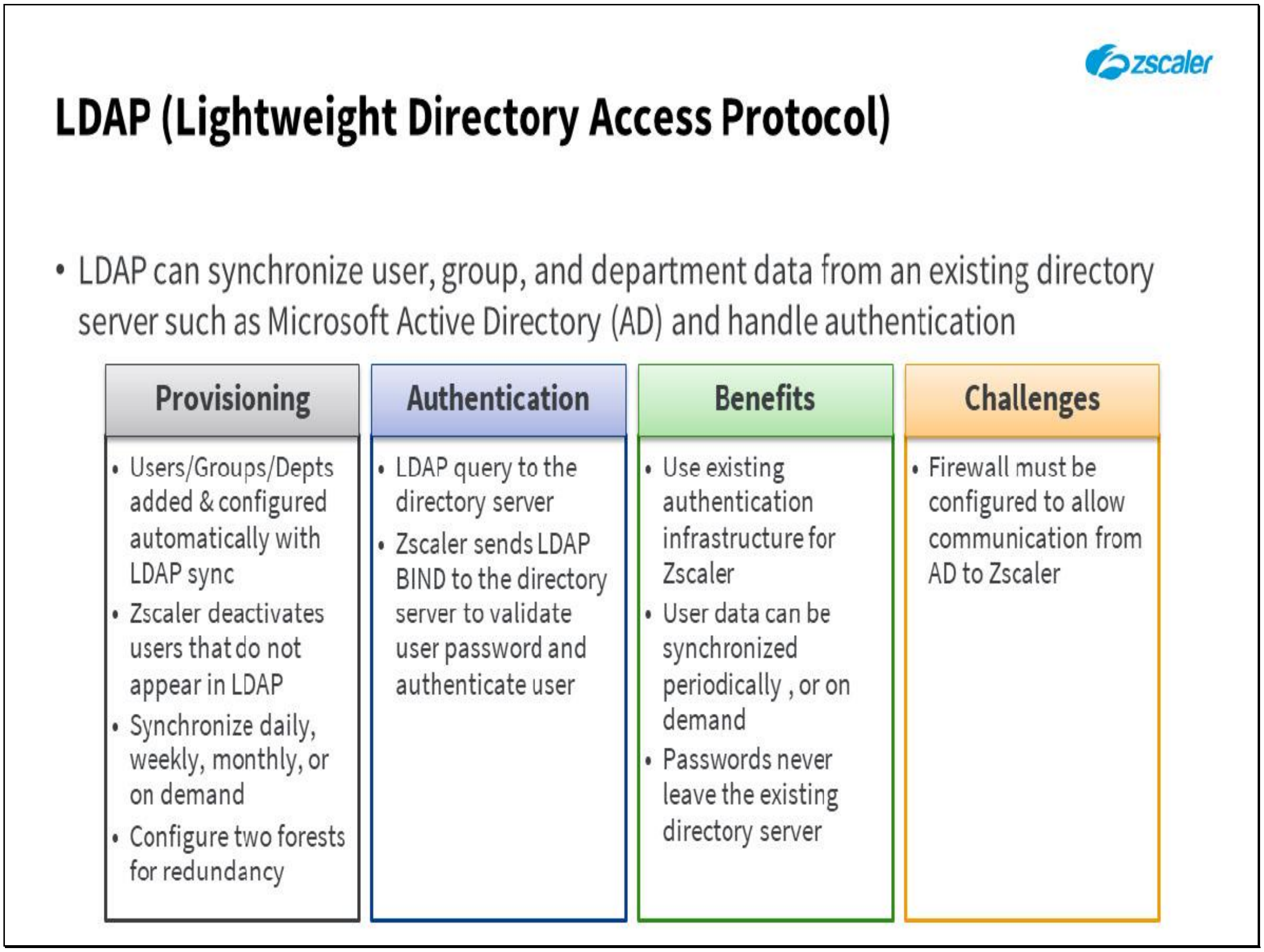
It is important to point out that all the authentication steps outlined above happen over SSL. No data is sent in clear at any point during the authentication phase.

Slide 31 - LDAP

LDAP

Slide notes

Slide 32 - LDAP (Lightweight Directory Access Protocol)



LDAP (Lightweight Directory Access Protocol)

- LDAP can synchronize user, group, and department data from an existing directory server such as Microsoft Active Directory (AD) and handle authentication

Provisioning	Authentication	Benefits	Challenges
• Users/Groups/Depts added & configured automatically with LDAP sync • Zscaler deactivates users that do not appear in LDAP • Synchronize daily, weekly, monthly, or on demand • Configure two forests for redundancy	• LDAP query to the directory server • Zscaler sends LDAP BIND to the directory server to validate user password and authenticate user	• Use existing authentication infrastructure for Zscaler • User data can be synchronized periodically , or on demand • Passwords never leave the existing directory server	• Firewall must be configured to allow communication from AD to Zscaler

Slide notes

LDAP, or lightweight directory access protocol, can synchronize user, group, and department data from an existing directory server such as Microsoft Active Directory (AD) to the Zscaler service. User and group information must be propagated from your directory service into Zscaler. Passwords however, are never copied over.

Using LDAP synchronization, the following items occur:

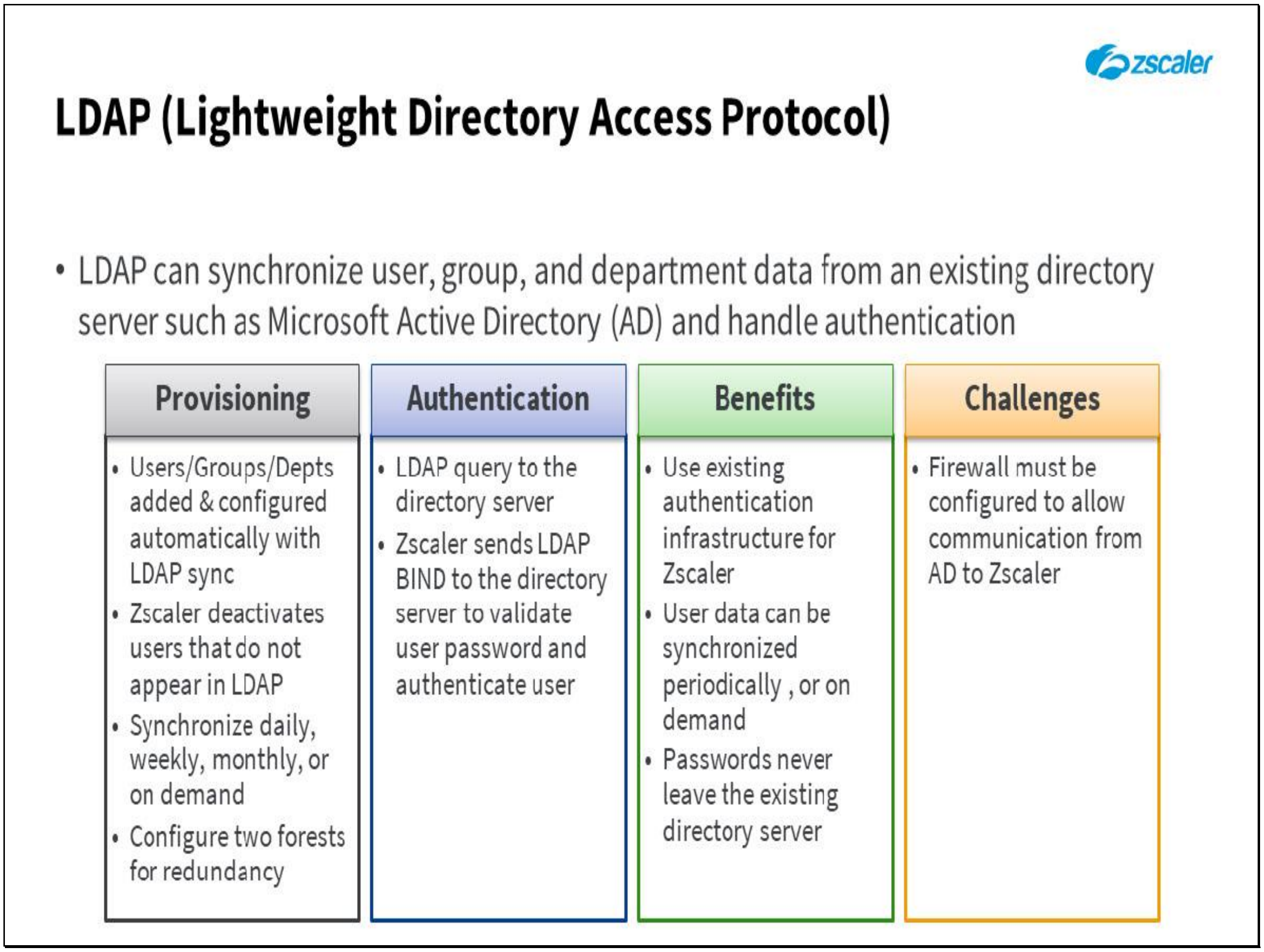
- Users are added to Zscaler via LDAP Sync with your Directory Server;
- Users, Groups, and Departments that are not in the Zscaler DB are automatically copied over from the Directory;
- Users that are in the Zscaler DB but not in the Directory Server are automatically deactivated.

If there is a discrepancy between the Zscaler DB and the Directory Server Zscaler will modify its information to match that on the Directory Server. Zscaler can synchronize from two forests in an organization. Database synchronization can be configured to synchronize: daily, weekly, monthly, or manually (now).

User Authentication is handled by your authentication server via Zscaler as follows:

- The Zscaler service performs an LDAP query to the directory server to authenticate users whose data was synchronized from a directory server
- It performs an LDAP BIND to the directory server to validate a user’s password and authenticate a user;
- Therefore, passwords are stored and maintained on the Directory Server and are never copied into the Zscaler service.

Slide 33 - LDAP (Lightweight Directory Access Protocol)



LDAP (Lightweight Directory Access Protocol)

- LDAP can synchronize user, group, and department data from an existing directory server such as Microsoft Active Directory (AD) and handle authentication

Provisioning	Authentication	Benefits	Challenges
• Users/Groups/Depts added & configured automatically with LDAP sync • Zscaler deactivates users that do not appear in LDAP • Synchronize daily, weekly, monthly, or on demand • Configure two forests for redundancy	• LDAP query to the directory server • Zscaler sends LDAP BIND to the directory server to validate user password and authenticate user	• Use existing authentication infrastructure for Zscaler • User data can be synchronized periodically , or on demand • Passwords never leave the existing directory server	• Firewall must be configured to allow communication from AD to Zscaler

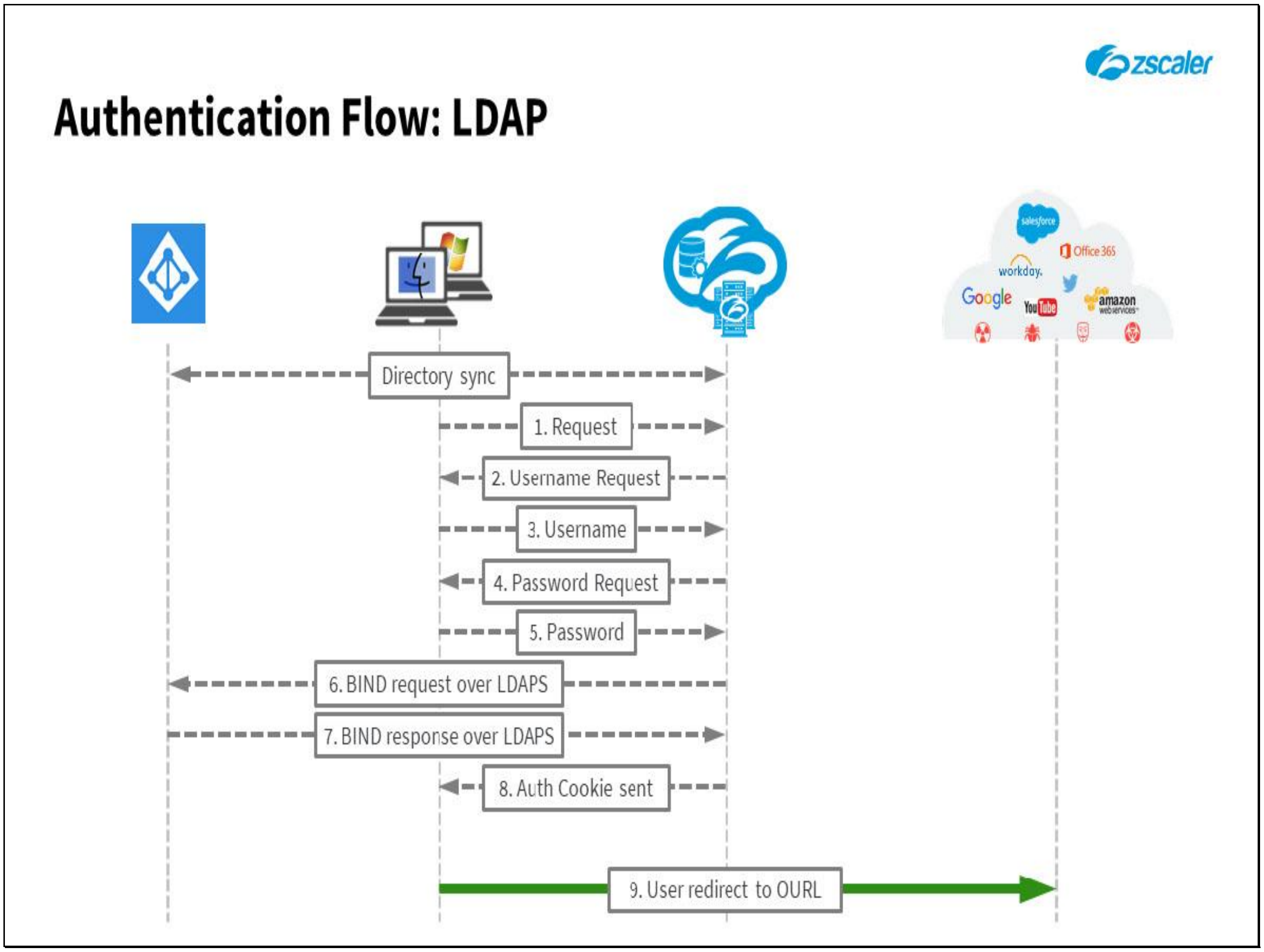
Slide notes

Let’s take a look at some of the attributes of LDAP for authentication:

- First, LDAP allows companies to use their existing authentication scheme with Zscaler;
- User data can be synchronized periodically or when requested;
- Passwords do not leave the organization - Zscaler only has the end-user identity.

Some of the challenges in implementing LDAP for an organization could be that the Firewall must be configured to allow communication with Zscaler.

Slide 34 - Authentication Flow – LDAP



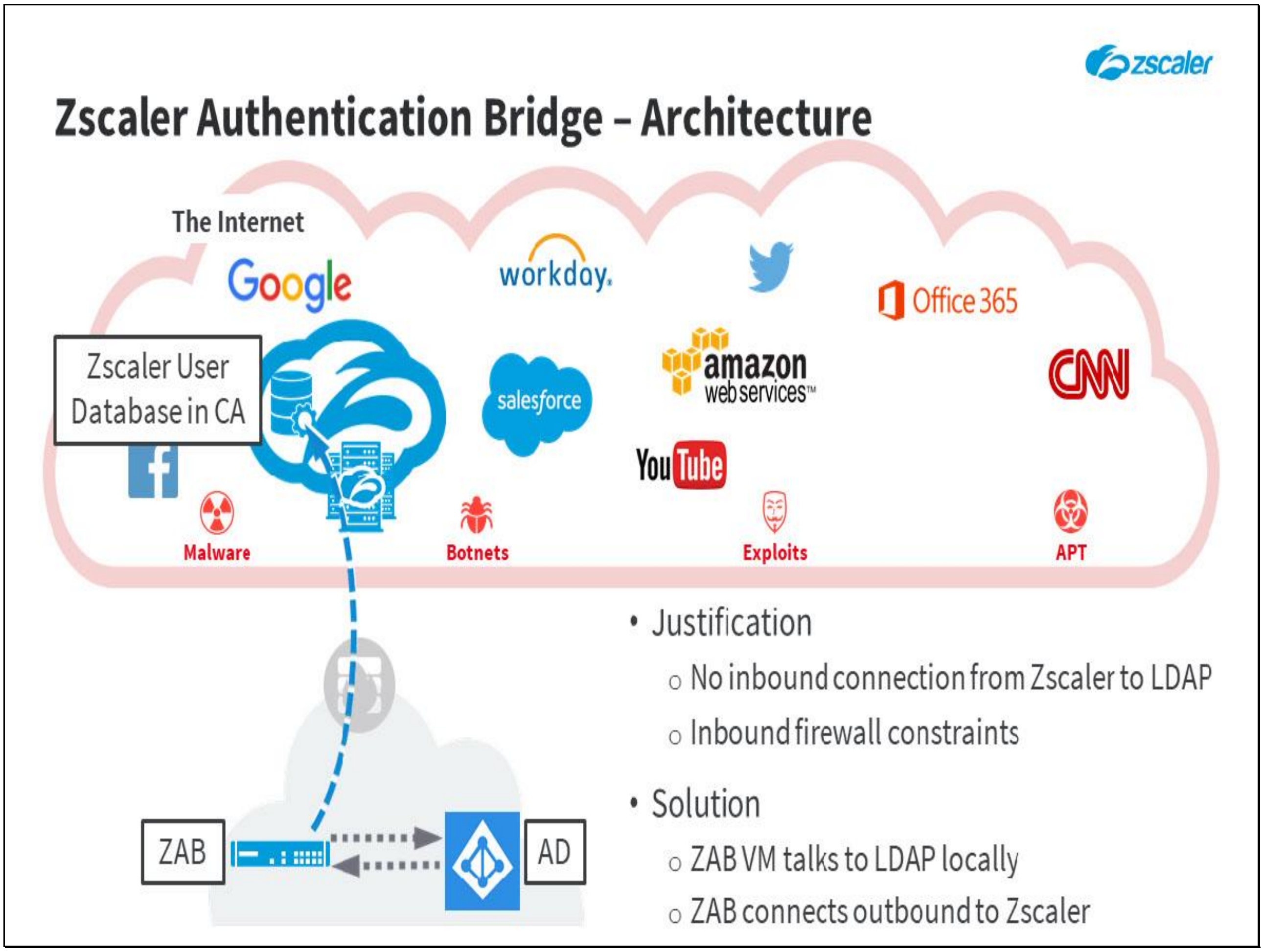
Authentication Flow: LDAP

Slide notes

As shown in the diagram below, when a synchronized user logs in to the Zscaler service it searches within its database by the login attribute and email address specified by the user. If Zscaler finds the user, it displays the password request form.

When the user submits the password request form, Zscaler retrieves the Distinguished Name and tries to perform an LDAP Bind to the directory sever using the Distinguished Name and password of the user. If the LDAP Bind succeeds, user authentication is successful.

Slide 35 - Zscaler Authentication Bridge – Architecture



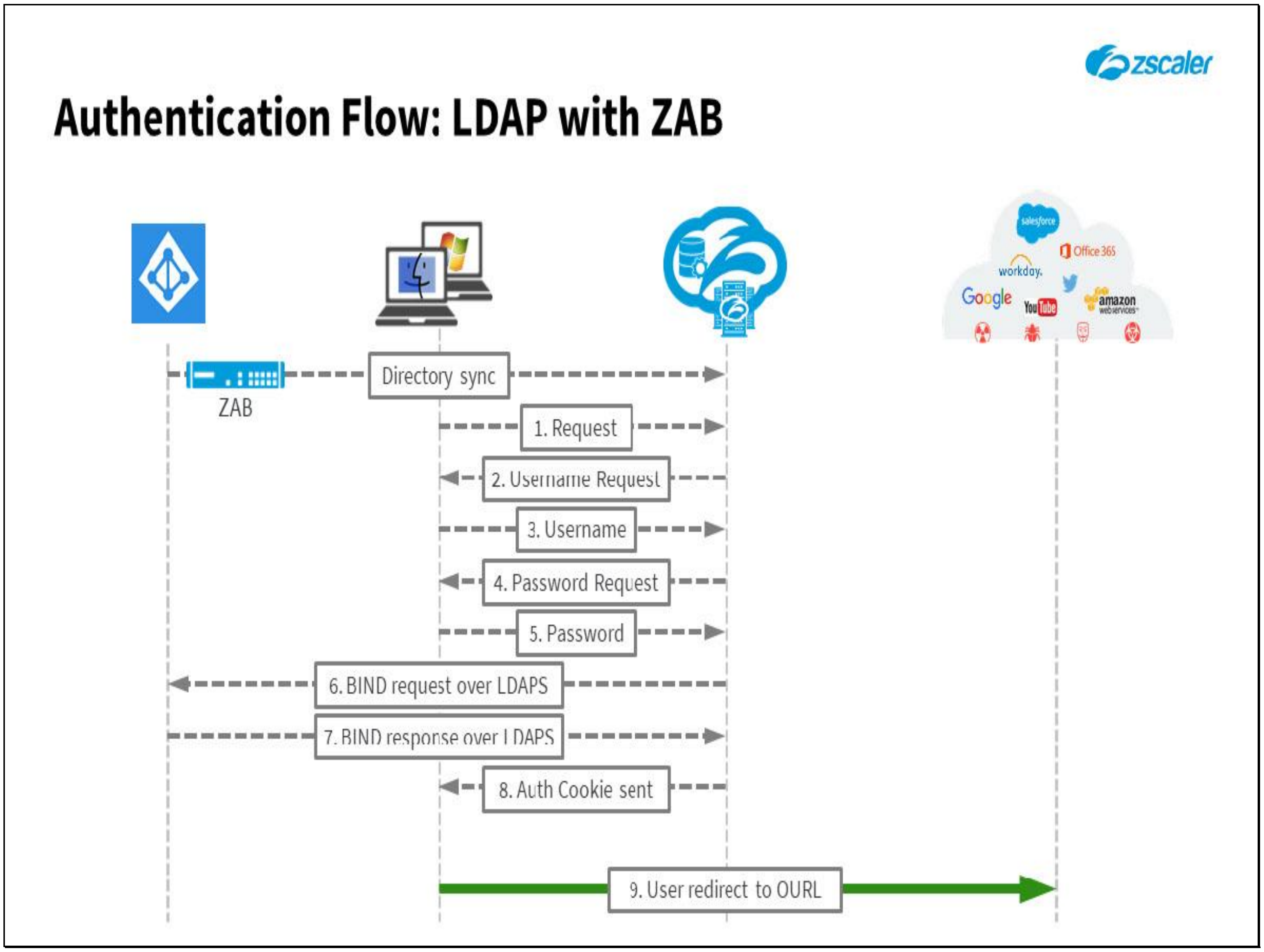
Zscaler Authentication Bridge – Architecture

- Justification
  - No inbound connection from Zscaler to LDAP
  - Inbound firewall constraints
- Solution
  - ZAB VM talks to LDAP locally
  - ZAB connects outbound to Zscaler

Slide notes

If your organization cannot allow the Zscaler service to connect directly to your internal directory servers or if you want to bypass any inbound firewall constraints on your network, your organizations can install an on-site Zscaler Authentication Bridge (ZAB). The ZAB is a VM that communicates with your internal directory servers. The Zscaler service communicates only with the ZAB, which then queries your directory server.

Slide 36 - Authentication Flow – LDAP with Zscaler Authentication Bridge



zscaler

Authentication Flow: LDAP with ZAB

ZAB

Directory sync

1. Request

2. Username Request

3. Username

4. Password Request

5. Password

6. BIND request over LDAPS

7. BIND response over LDAPS

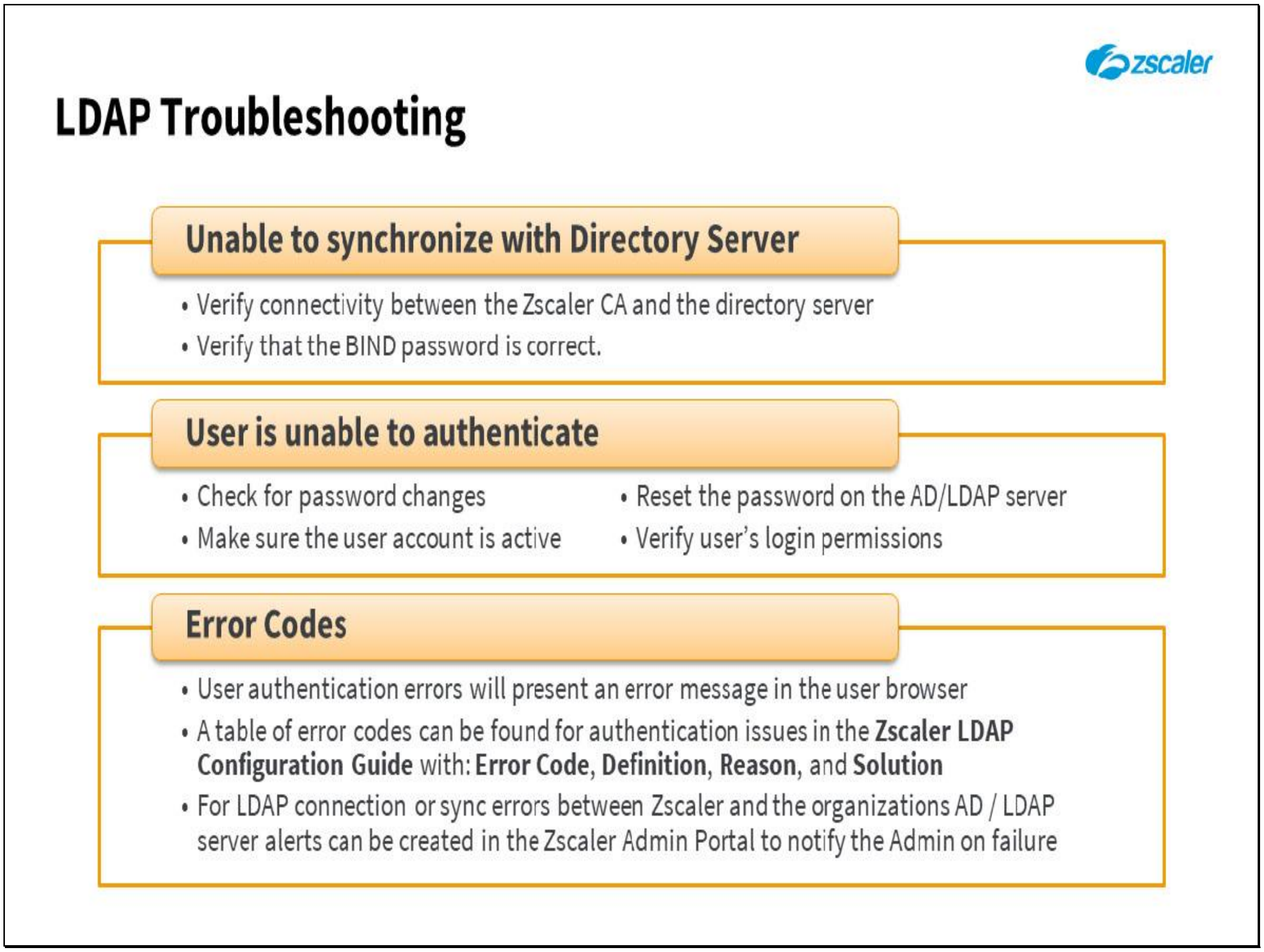
8. Auth Cookie sent

9. User redirect to OURL

Slide notes

When adding the Zscaler Authentication Bridge, or ZAB, user provisioning information is no longer direct between the customers AD. Rather, AD communicates with the ZAB and the ZAB communicates with the Zscaler service.

Slide 37 - LDAP Troubleshooting



LDAP Troubleshooting

Unable to synchronize with Directory Server

- Verify connectivity between the Zscaler CA and the directory server
- Verify that the BIND password is correct.

User is unable to authenticate

- Check for password changes
- Make sure the user account is active
- Reset the password on the AD/LDAP server
- Verify user's login permissions

Error Codes

- User authentication errors will present an error message in the user browser
- A table of error codes can be found for authentication issues in the **Zscaler LDAP Configuration Guide** with: **Error Code**, **Definition**, **Reason**, and **Solution**
- For LDAP connection or sync errors between Zscaler and the organizations AD / LDAP server alerts can be created in the Zscaler Admin Portal to notify the Admin on failure

Slide notes

Here is a short list of troubleshooting tips for LDAP related issues.

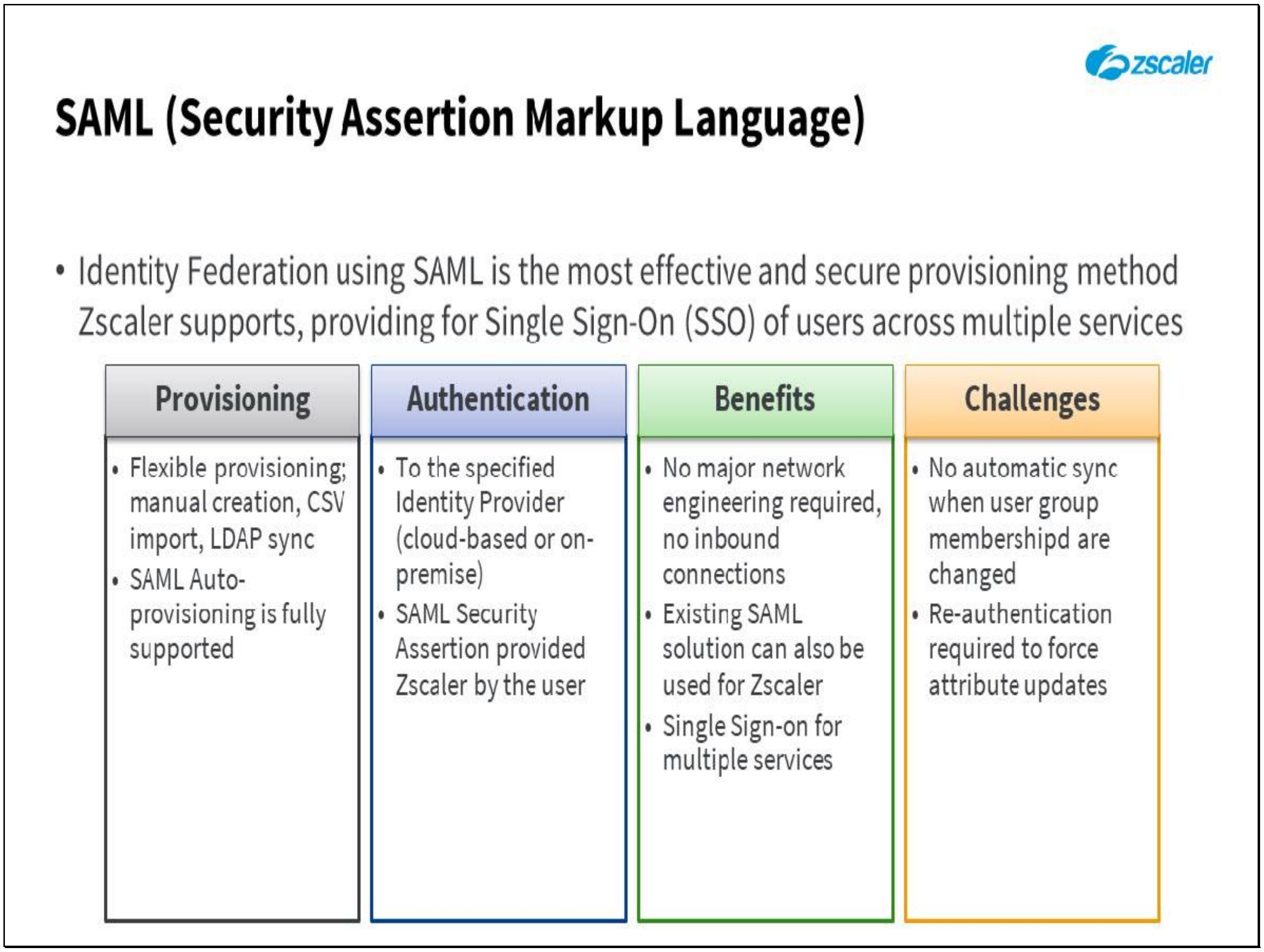
- First, if the Zscaler service is unable to synchronize with the Directory Server. Verify connectivity between the Zscaler CA server and the directory server and verify that the BIND password is correct.
- If a user is unable to authenticate verify the password the user is attempting. If the user is attempting to use an old password reset the password on the AD/LDAP server.
- Check error codes that the Zscaler service presents. A table of error codes can be found for authentication issues in the **Zscaler LDAP Configuration Guide** and lists the Error code, Definition, reason, and Solution.

Slide 38 - SAML

SAML

Slide notes

Slide 39 - SAML (Security Assertion Markup Language)



SAML (Security Assertion Markup Language)

- Identity Federation using SAML is the most effective and secure provisioning method Zscaler supports, providing for Single Sign-On (SSO) of users across multiple services

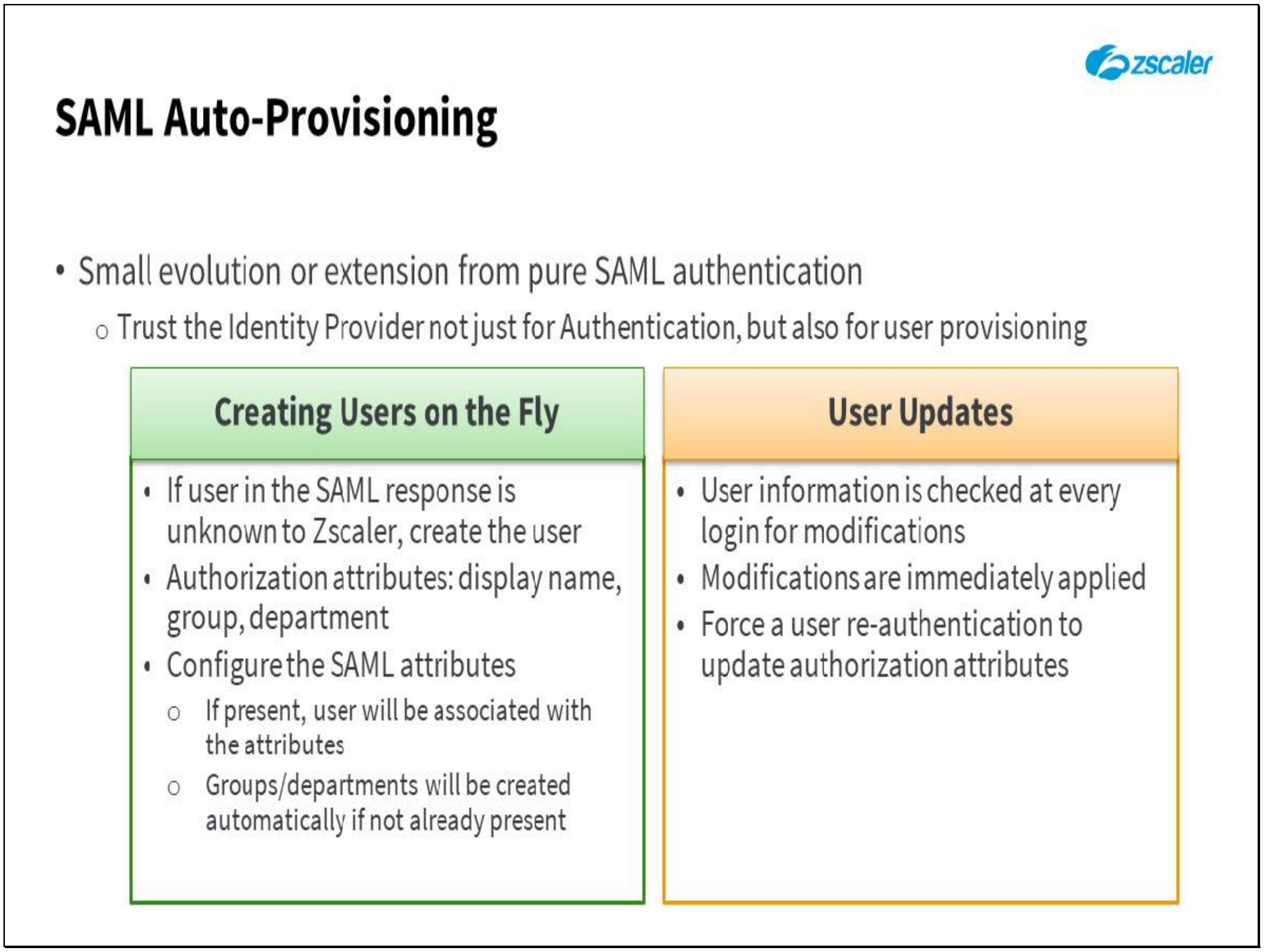
Provisioning	Authentication	Benefits	Challenges
• Flexible provisioning; manual creation, CSV import, LDAP sync • SAML Auto-provisioning is fully supported	• To the specified Identity Provider (cloud-based or on-premise) • SAML Security Assertion provided Zscaler by the user	• No major network engineering required, no inbound connections • Existing SAML solution can also be used for Zscaler • Single Sign-on for multiple services	• No automatic sync when user group membershipd are changed • Re-authentication required to force attribute updates

Slide notes

The preferred method of Authentication with the Zscaler service is SAML or **Security Assertion Markup Language**. This is the most effective and secure provisioning method of the supported options and provides for Single Sign-On of users across multiple services.

- User and Group provisioning, when using SAML can be done using a CSV or manually import the users in the Zscaler database, via LDAP sync, or via SAML auto-provisioning.
- User authentication is via an **Identity Provider**, or idP such as Okta or Microsoft ADFS as part of the SAML response posted to the Service Provider, in this case Zscaler.
- The Benefits of SAML at that no considerable network changes are required as no ports need to be opened for inbound connections from Zscaler to your Directory Server.
- One of the Challenges of SAML can be in the use of SAML auto-provisioning. If the user Group membership changes in Directory server, the Zscaler user database does not automatically sync with the idP. As such the user’s login is still valid and the user remains logged in with their old privileges till it re-authenticates to the Zscaler service. This will cause re-authentication and the user will be a member of the new group. For more information contact TAC.

Slide 40 - SAML Auto-Provisioning



SAML Auto-Provisioning

- Small evolution or extension from pure SAML authentication
  - Trust the Identity Provider not just for Authentication, but also for user provisioning

Creating Users on the Fly

- If user in the SAML response is unknown to Zscaler, create the user
- Authorization attributes: display name, group, department
- Configure the SAML attributes
  - If present, user will be associated with the attributes
  - Groups/departments will be created automatically if not already present

User Updates

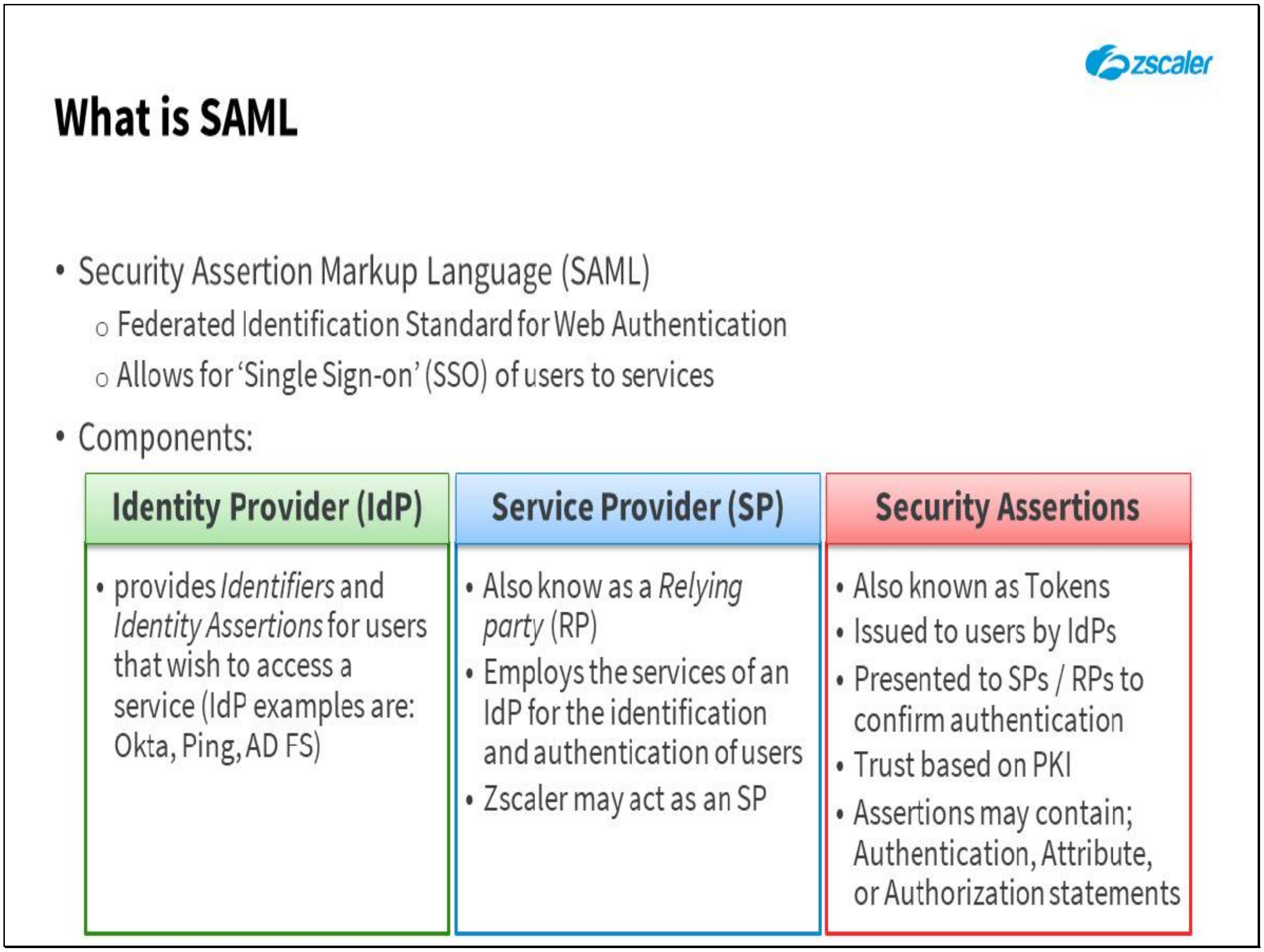
- User information is checked at every login for modifications
- Modifications are immediately applied
- Force a user re-authentication to update authorization attributes

Slide notes

SAML auto-provisioning is a proprietary evolution of SAML deployed by many vendors. The use of SAML auto provisioning enables the system to import user information as it is seen as part of the authentication request. User attributes can also be imported such as display name, group, and department membership.

Each time a user logs in to the Zscaler system the user information seen as part of the authentication is checked against the information that may already be contained in the Zscaler cloud. If different, Zscaler will update its records.

Slide 41 - What is SAML



What is SAML

- Security Assertion Markup Language (SAML)
  - Federated Identification Standard for Web Authentication
  - Allows for 'Single Sign-on' (SSO) of users to services
- Components:

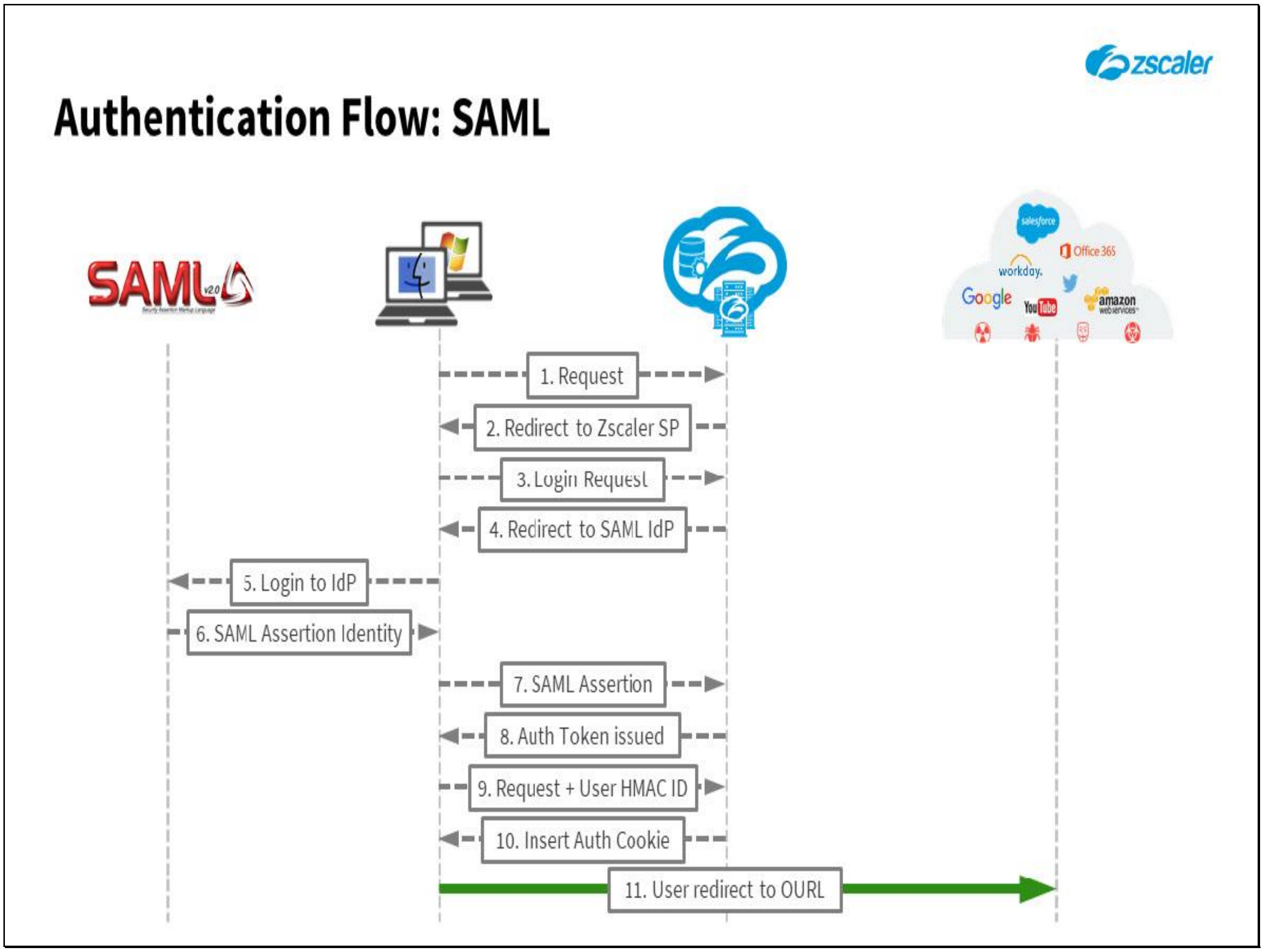
Identity Provider (IdP)	Service Provider (SP)	Security Assertions
• provides *Identifiers* and *Identity Assertions* for users that wish to access a service (IdP examples are: Okta, Ping, AD FS)	• Also know as a *Relying party* (RP) • Employs the services of an IdP for the identification and authentication of users • Zscaler may act as an SP	• Also known as Tokens • Issued to users by IdPs • Presented to SPs / RPs to confirm authentication • Trust based on PKI • Assertions may contain; Authentication, Attribute, or Authorization statements

Slide notes

There are three major components in a SAML deployment: The Service Provider (SP), such as Zscaler; the Identity Provider (IdP), such as Okta, ADFS, One Login, and SiteMinder; and the client, which is the Web browser on the user's PC. As mentioned previously, SAML enables single sign-on (SSO) such that the user authenticates to one service then, without an addition authentication, is able to access resources at another service.

SAML enables Web SSO through the communication of an authentication assertion from the first site, to the second site that, if confident of the origin of the assertion, can chose to login the users as if they had authenticated directly.

Slide 42 - Authentication Flow – SAML



Authentication Flow: SAML

1. Request
2. Redirect to Zscaler SP
3. Login Request
4. Redirect to SAML IdP
5. Login to IdP
6. SAML Assertion Identity
7. SAML Assertion
8. Auth Token issued
9. Request + User HMAC ID
10. Insert Auth Cookie
11. User redirect to OURL

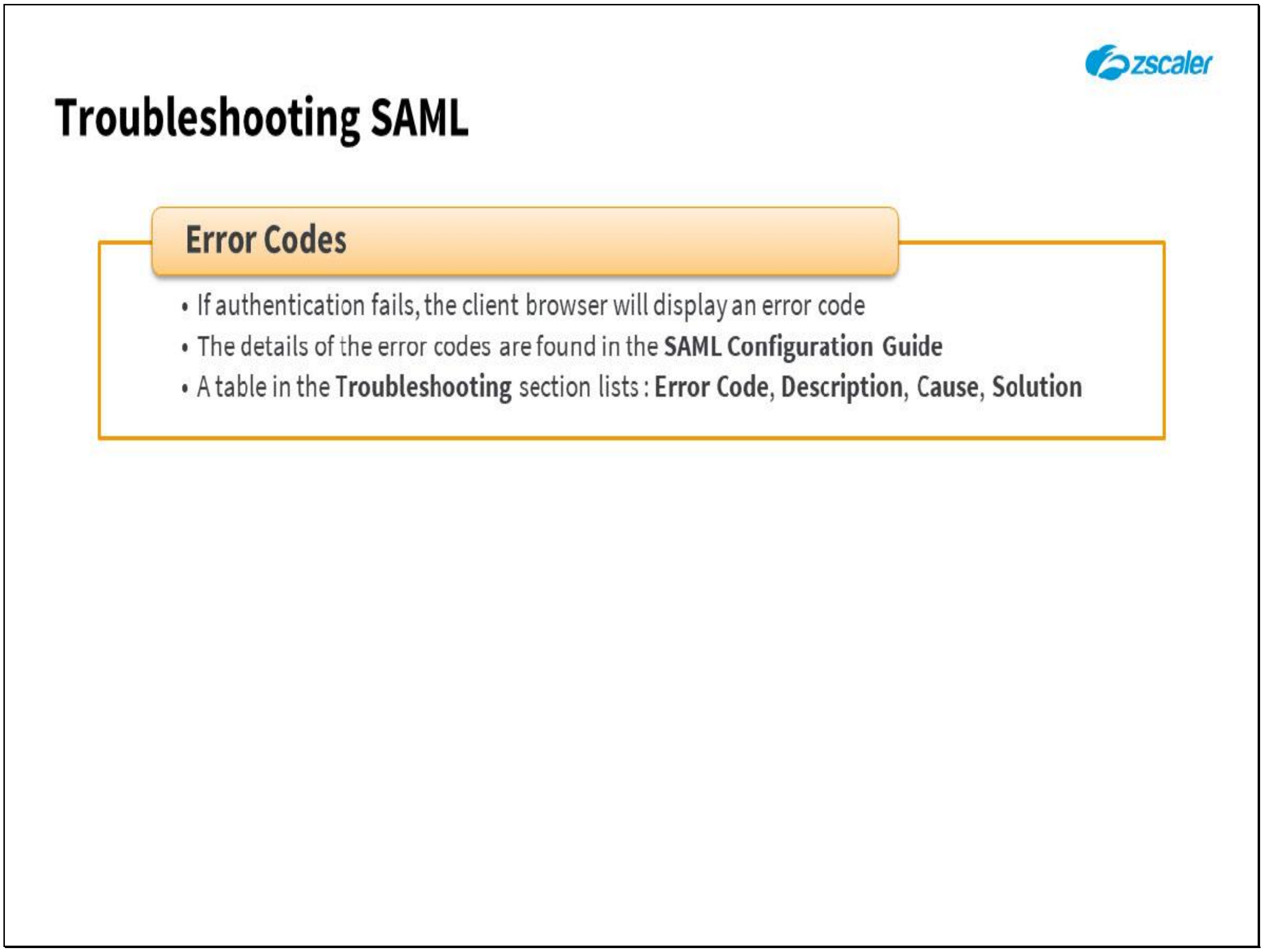
Slide notes

SAML authentication does not require the SAML server, or Identity provider and the Zscaler cloud to exchange any data directly. It is a token-based authentication mechanism by which Zscaler trusts the user request that is correctly signed by the Identity Provider.

The process is as follows:

1. The user makes an initial HTTP request,
2. Zscaler redirects the user to the Zscaler cloud for authentication,
3. The user sends its username to Zscaler,
4. Zscaler returns the URL for the IdP (SAML server),
5. The user authenticates into the IdP,
6. The IdP gives the user the SAML Assertion identity (which is basically a token to present to Zscaler),
7. The user sends the IdP Assertion to Zscaler,
8. – 10. Zscaler issues an authentication token to the user,
11. The user is now authenticated and Zscaler sends an Auth cookie.

Slide 43 - Troubleshooting SAML



Troubleshooting SAML

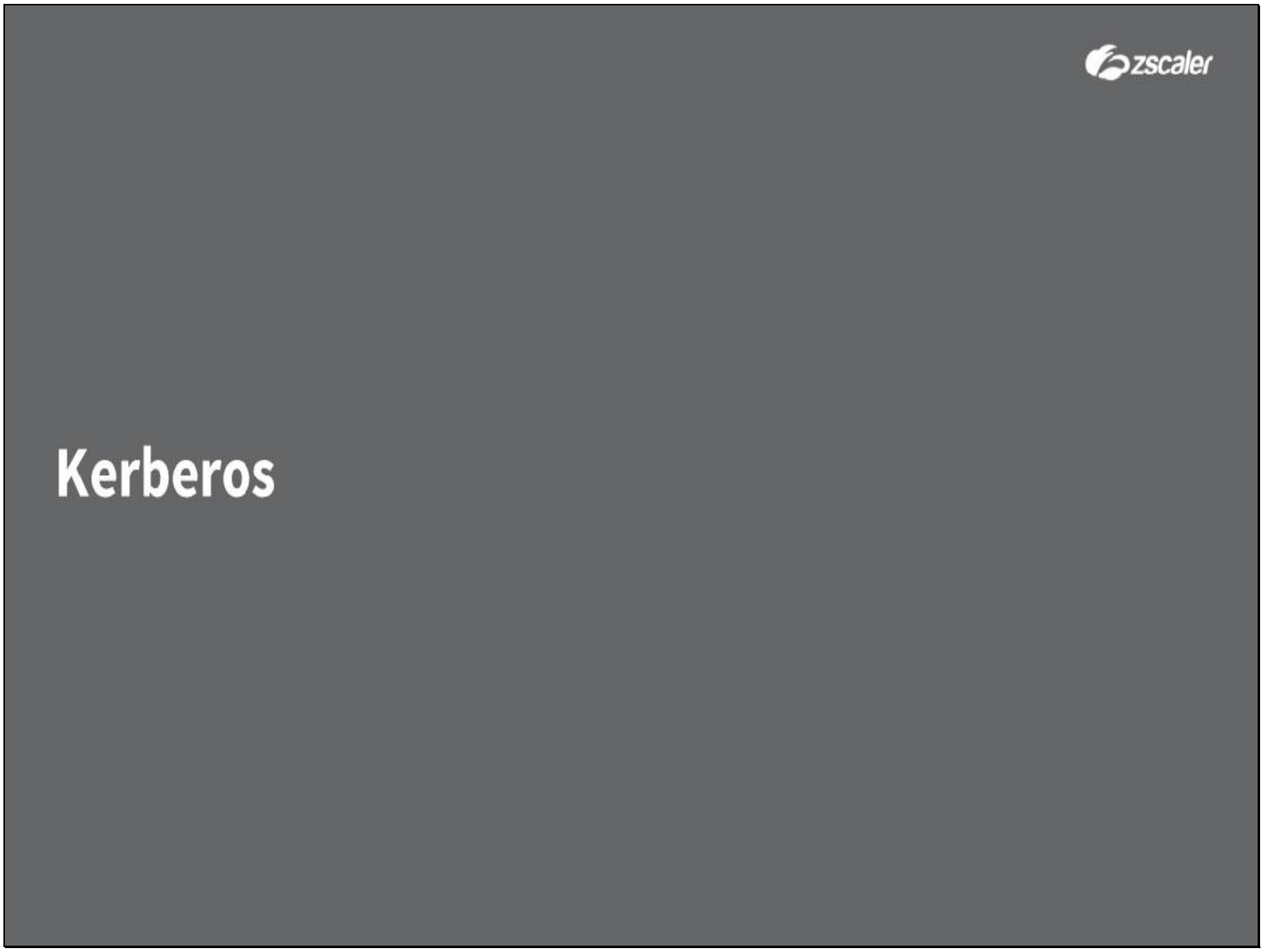
Error Codes

- If authentication fails, the client browser will display an error code
- The details of the error codes are found in the **SAML Configuration Guide**
- A table in the **Troubleshooting** section lists : **Error Code**, **Description**, **Cause**, **Solution**

Slide notes

With SAML if user authentication fails, the client browser will display an error code. The details of the error codes are found in the Troubleshooting section of the SAML Configuration Guide. A table in the Troubleshooting section lists the following: error code, description, cause, solution.

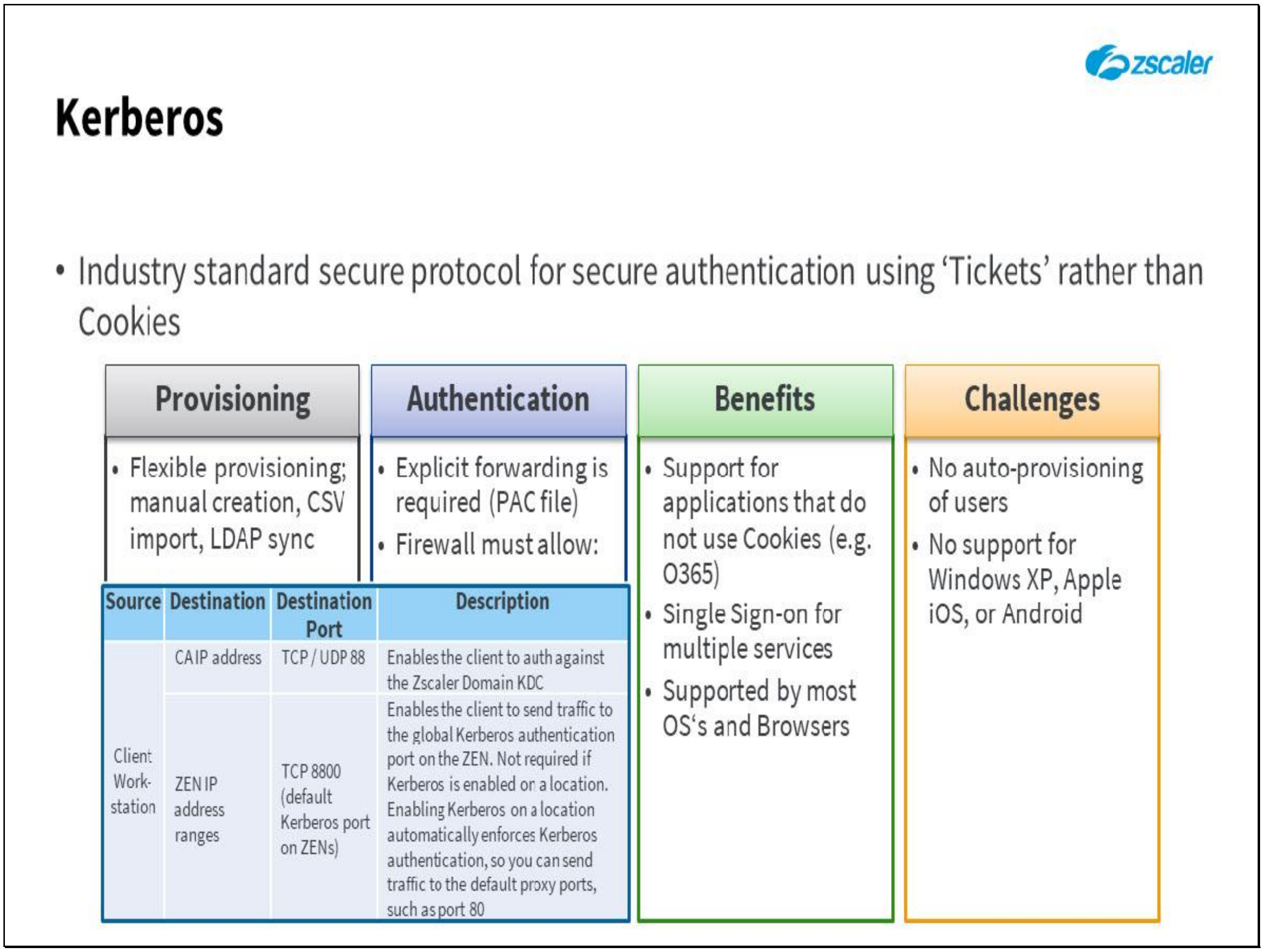
Slide 44 - Kerberos



Kerberos

Slide notes

Slide 45 - Kerberos



Kerberos

- Industry standard secure protocol for secure authentication using 'Tickets' rather than Cookies

Provisioning

- Flexible provisioning; manual creation, CSV import, LDAP sync

Authentication

- Explicit forwarding is required (PAC file)
- Firewall must allow:

Source	Destination	Destination Port	Description
Client Work-station	CA IP address	TCP / UDP 88	Enables the client to auth against the Zscaler Domain KDC
	ZEN IP address ranges	TCP 8800 (default Kerberos port on ZENs)	Enables the client to send traffic to the global Kerberos authentication port on the ZEN. Not required if Kerberos is enabled on a location. Enabling Kerberos on a location automatically enforces Kerberos authentication, so you can send traffic to the default proxy ports, such as port 80

Benefits

- Support for applications that do not use Cookies (e.g. O365)
- Single Sign-on for multiple services
- Supported by most OS's and Browsers

Challenges

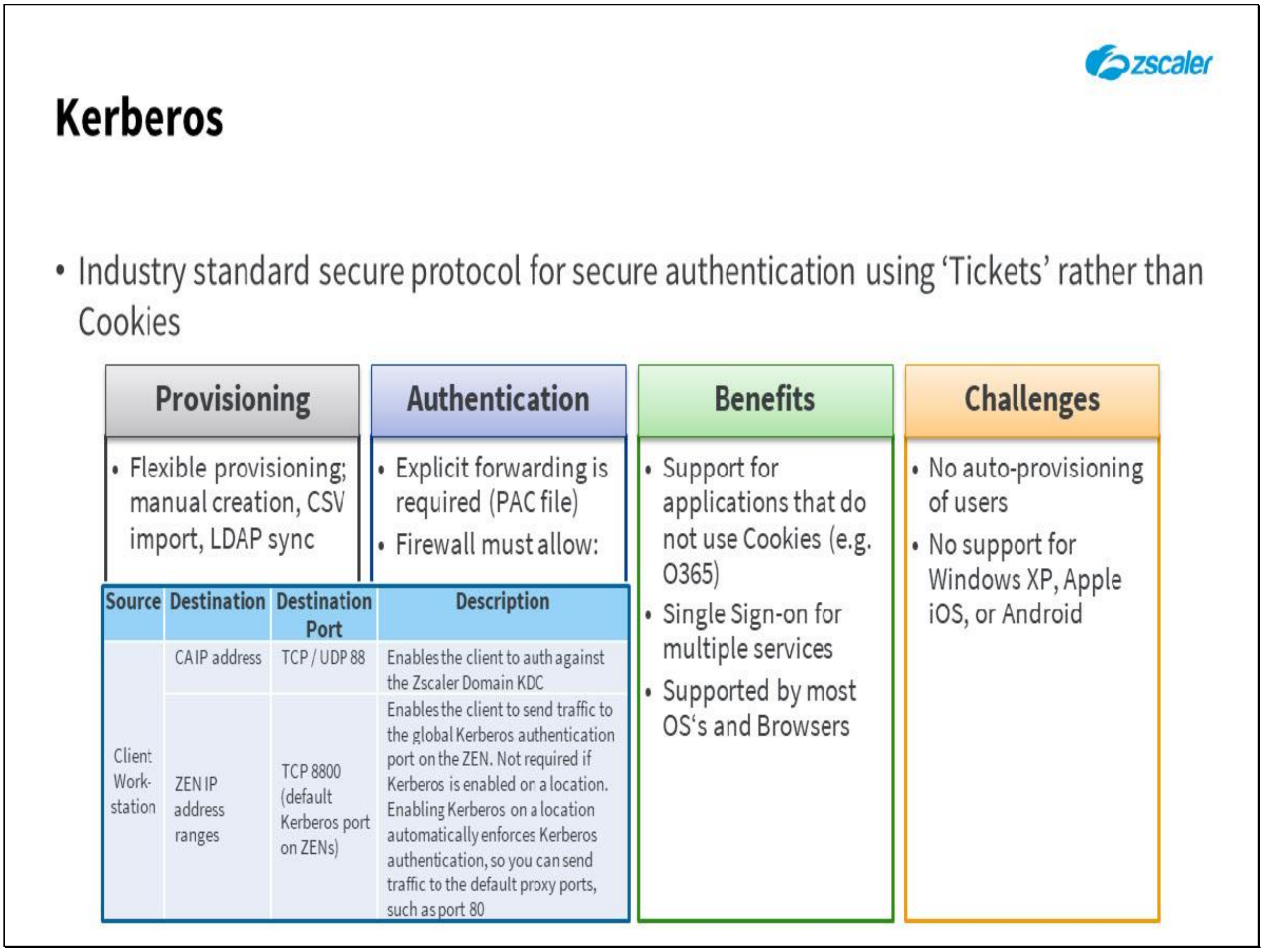
- No auto-provisioning of users
- No support for Windows XP, Apple iOS, or Android

Slide notes

Zscaler supports authentication using Kerberos, an industry standard secure protocol. Unlike the other supported authentication mechanisms, Kerberos does not use cookies for authentication. It is a ticket-based authentication protocol that is widely used to authenticate users to network services.

- Users and their groups must be provisioned on the Zscaler service as with the other authentication methods discussed previously. Users are provisioned either manually in the Admin Portal UI or by synchronizing user data from an AD or LDAP server. Unlike SAML the user cannot be provisioned automatically at the time of login.
- For user Authentication the use of PAC file is required. Ensure that your Firewall allows the following connections:
  - From the Client Workstation to the CA IP open TCP /UDP port 88 – this enables the client to authenticate against the Zscaler Domain KDC.
  - Also, from the client workstation to the ZEN IP address ranges open TCP port 8800 – this enables the client to send traffic to the global Kerberos authentication port on the ZEN (not required if Kerberos is enabled on a location – enabling Kerberos on a location automatically enforces Kerberos authentication, so you can send traffic to the default proxy ports, such as port 80).

Slide 46 - Kerberos



Kerberos

- Industry standard secure protocol for secure authentication using 'Tickets' rather than Cookies

Provisioning

- Flexible provisioning; manual creation, CSV import, LDAP sync

Authentication

- Explicit forwarding is required (PAC file)
- Firewall must allow:

Source	Destination	Destination Port	Description
Client Work-station	CA IP address	TCP / UDP 88	Enables the client to auth against the Zscaler Domain KDC
	ZEN IP address ranges	TCP 8800 (default Kerberos port on ZENs)	Enables the client to send traffic to the global Kerberos authentication port on the ZEN. Not required if Kerberos is enabled on a location. Enabling Kerberos on a location automatically enforces Kerberos authentication, so you can send traffic to the default proxy ports, such as port 80

Benefits

- Support for applications that do not use Cookies (e.g. O365)
- Single Sign-on for multiple services
- Supported by most OS's and Browsers

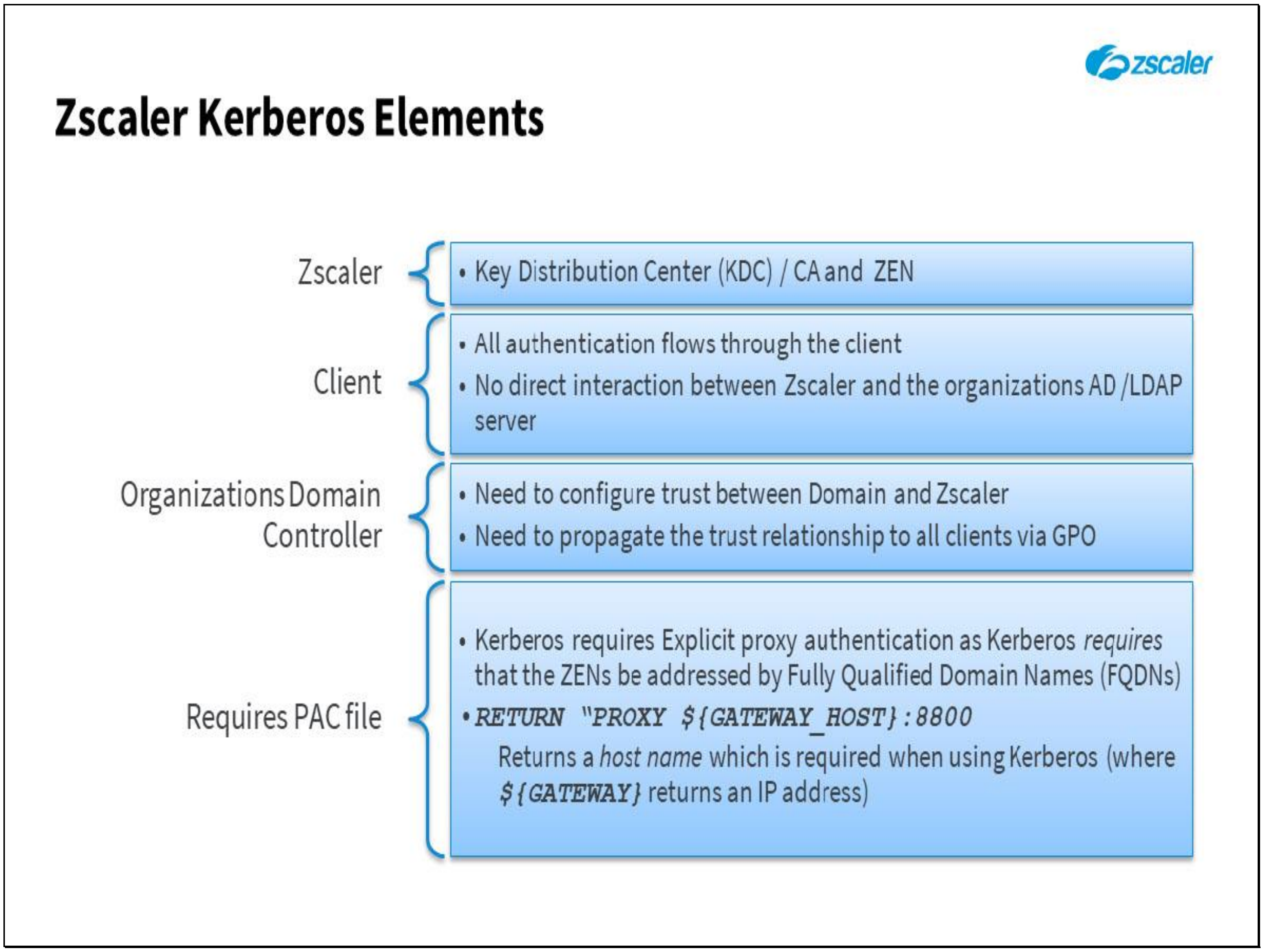
Challenges

- No auto-provisioning of users
- No support for Windows XP, Apple iOS, or Android

Slide notes

- Kerberos Benefits are that it does not use Cookies which enables the Zscaler service to authenticate users when they use applications that do not support cookies, such as Office 365. It also enables Single Sign-On - users auth once to their corporate domain then are no longer prompted for username/password for additional sites. Most modern OS and browsers support Kerberos.
- The Challenges are that the Zscaler service does not support Kerberos on Windows XP, Apple iOS, or Android and provisioning must be configured to import user accounts.

Slide 47 - Zscaler Kerberos Elements



Zscaler Kerberos Elements

Zscaler
- Key Distribution Center (KDC) / CA and ZEN

Client
- All authentication flows through the client
- No direct interaction between Zscaler and the organizations AD /LDAP server

Organizations Domain Controller
- Need to configure trust between Domain and Zscaler
- Need to propagate the trust relationship to all clients via GPO

Requires PAC file
- Kerberos requires Explicit proxy authentication as Kerberos *requires* that the ZENs be addressed by Fully Qualified Domain Names (FQDNs)
- ***RETURN "PROXY ${GATEWAY_HOST}:8800***

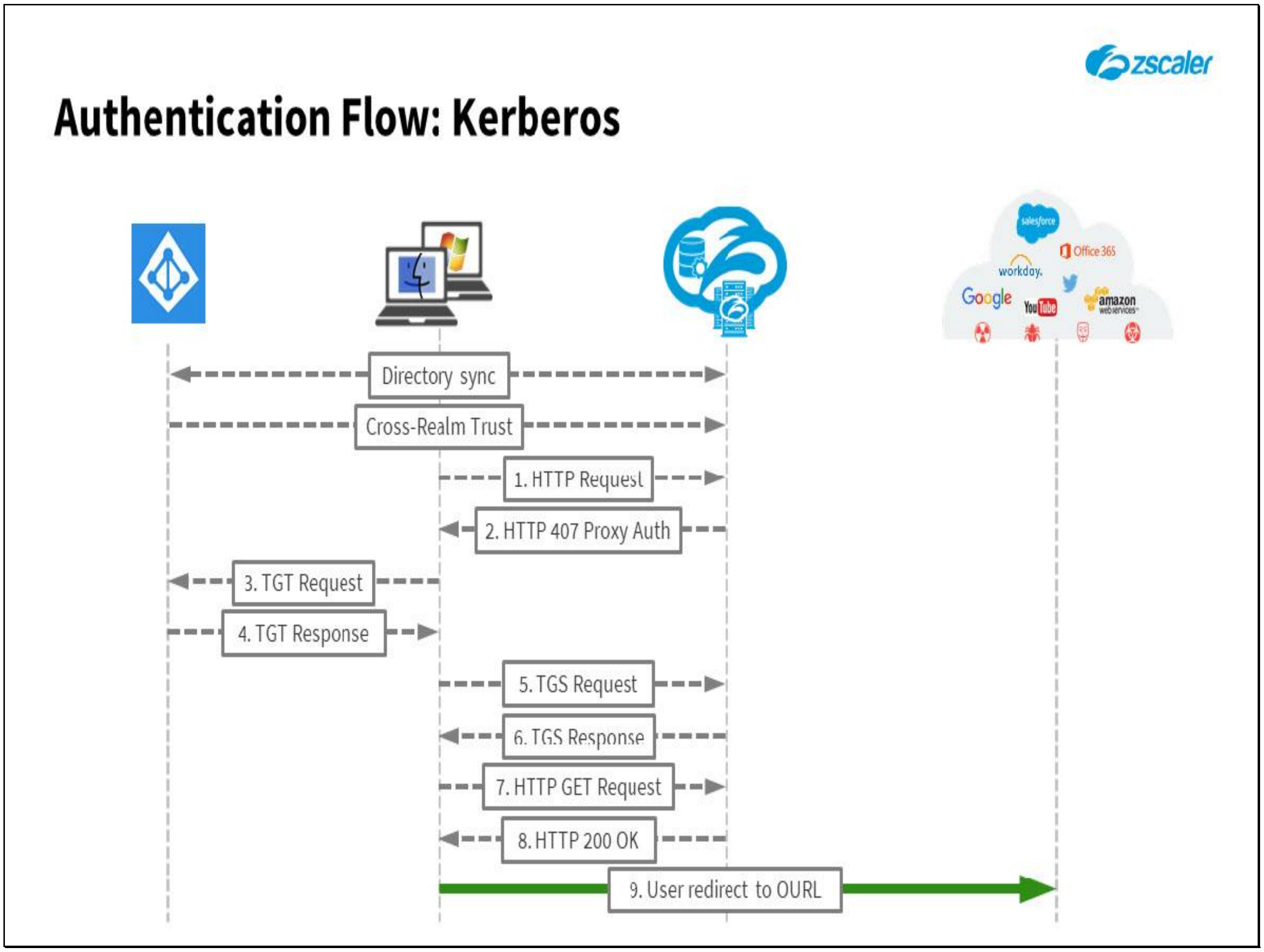
  Returns a *host name* which is required when using Kerberos (where ***${GATEWAY}*** returns an IP address)

Slide notes

Components of Kerberos in a Zscaler solution are as follows:

- On the Zscaler side is the Key Distribution Center (or KDC), the CA and ZEN;
- The Client, all authentication flows through the client, there is no direct interaction between Zscaler and the organizations AD / LDAP server;
- Last is the company's Domain Controller which needs to accept cross Trust requests from the Zscaler Domain on port **88**, you will need to configure the trust between the Domain and Zscaler.
- And the PAC file Kerberos requires Explicit proxy authentication as Kerberos requires that the ZENs be addressed as Fully Qualified Domain Names (FQDNs). To accomplish this, a PAC file is used with the variable **GATEWAY_HOST** which returns a hostname (which is required when using Kerberos), while the variable **GATEWAY** returns an IP address.

Slide 48 - Authentication Flow – Kerberos



Authentication Flow: Kerberos

Directory sync

Cross-Realm Trust

1. HTTP Request

2. HTTP 407 Proxy Auth

3. TGT Request

4. TGT Response

5. TGS Request

6. TGS Response

7. HTTP GET Request

8. HTTP 200 OK

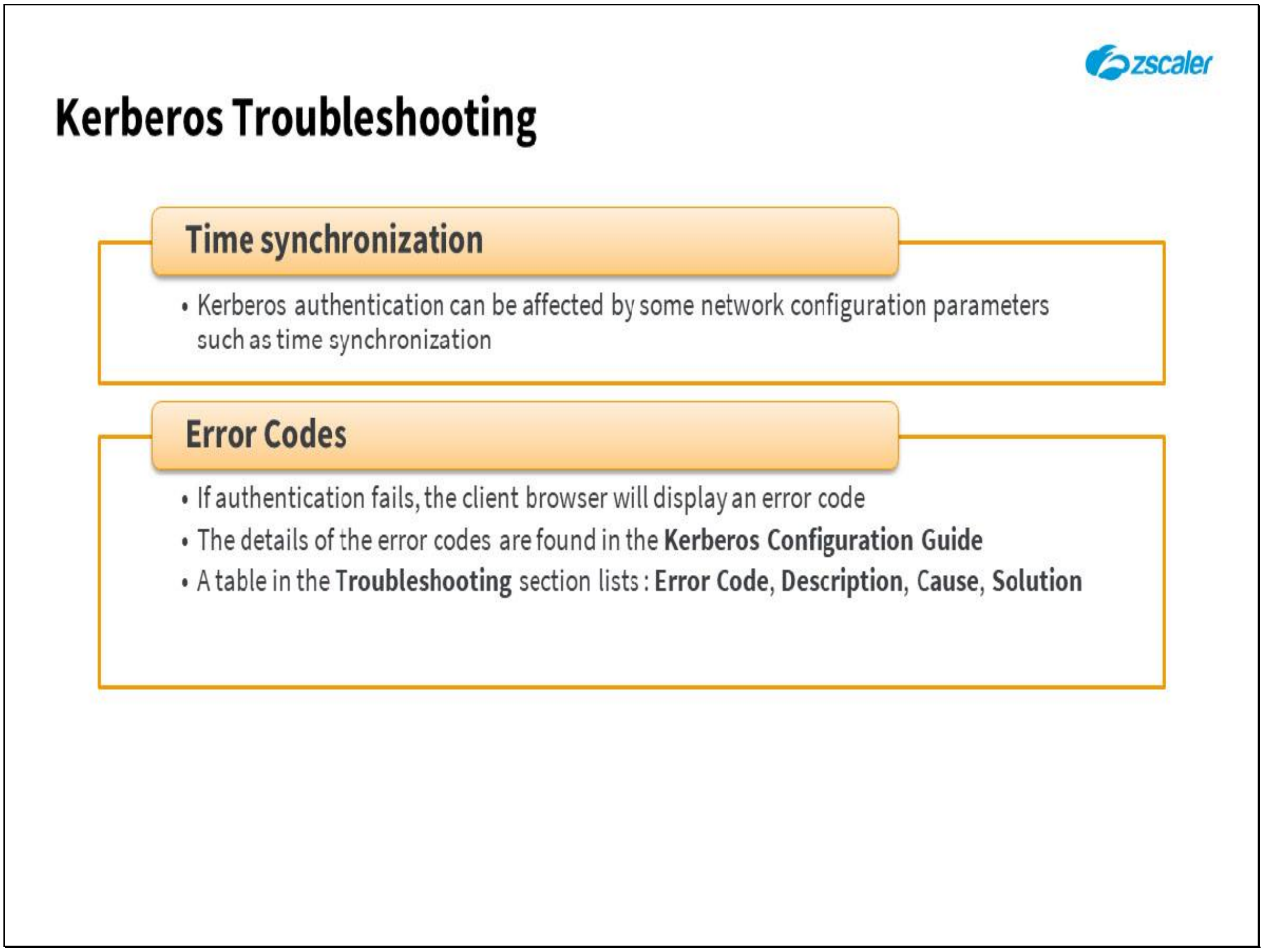
9. User redirect to OURL

Slide notes

The Kerberos authentication flow is as follows:

1. The client posts an HTTP request to the Zscaler,
2. Zscaler sends **HTTP 407 - proxy -Authenticate: Negotiate**,
3. The client sends a **Ticket Granting Ticket Request** (or TGT request) to the company domain,
4. The company domain sends a **TGT Response** back to the client,
5. The client sends a **Ticket Granting Service Request** (or TGS request) to the KDC which is Zscaler,
6. The KDC sends a **TGS Response** back to the client,
7. The client sends an **HTTP Get Request Proxy Authorization: Negotiate (TGS)** to Zscaler,
8. Zscaler sends back **HTTP 200 Ok** and the client is authenticated.

Slide 49 - Kerberos Troubleshooting



Kerberos Troubleshooting

Time synchronization

- Kerberos authentication can be affected by some network configuration parameters such as time synchronization

Error Codes

- If authentication fails, the client browser will display an error code
- The details of the error codes are found in the **Kerberos Configuration Guide**
- A table in the **Troubleshooting** section lists : **Error Code**, **Description**, **Cause**, **Solution**

Slide notes

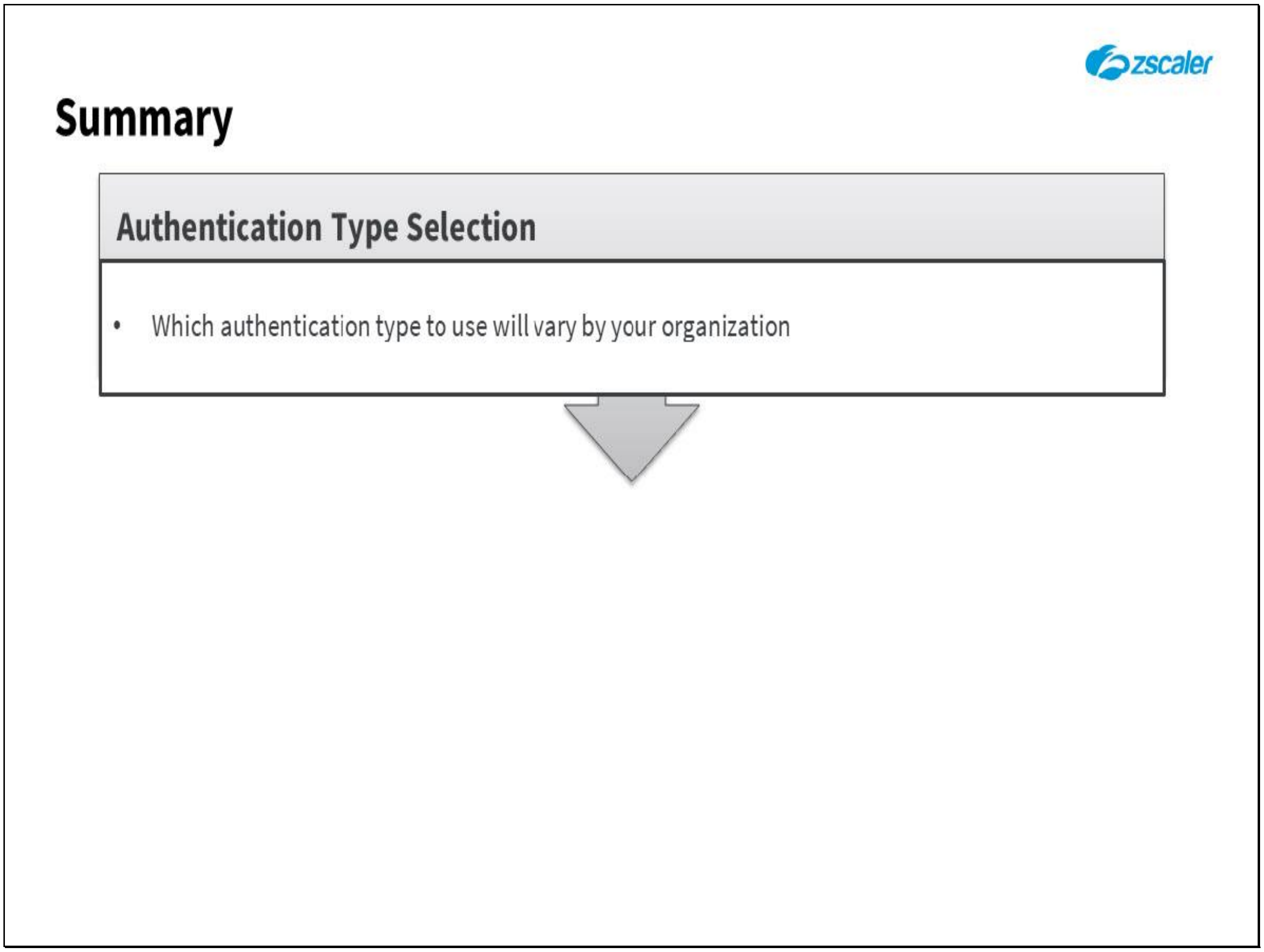
Kerberos authentication can be affected by some network configuration parameters such as time synchronization. If authentication fails, the client browser displays an error code. The details of the error codes are found in the Troubleshooting section of the Kerberos Configuration Guide. A table in the Troubleshooting section lists the following: error code, description, cause, solution.

Slide 50 - Summary

Summary

Slide notes

Slide 51 - Summary



Summary

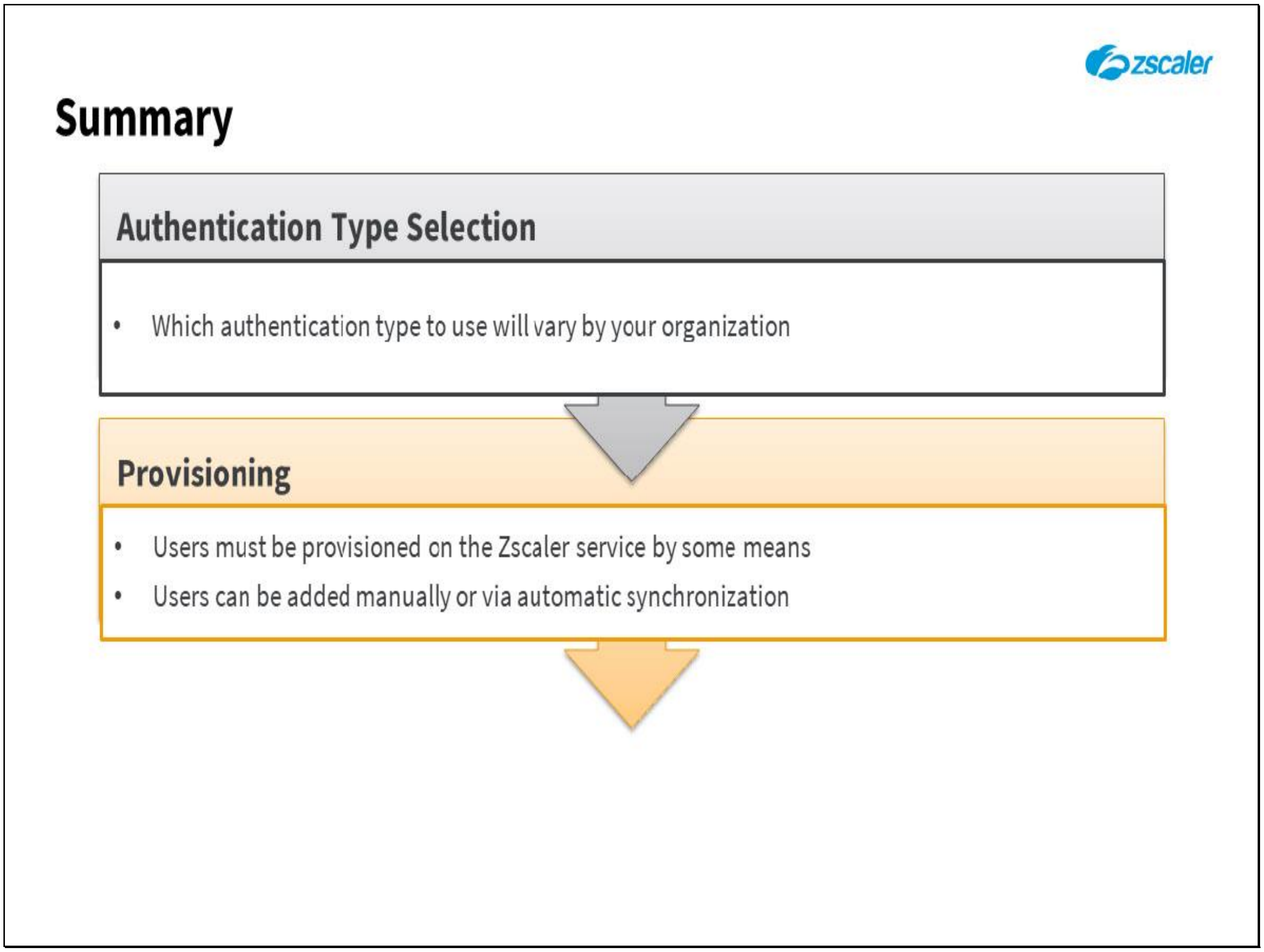
Authentication Type Selection

- Which authentication type to use will vary by your organization

Slide notes

To summarize, which authentication type to use will vary by your organization.

Slide 52 - Summary



Summary

Authentication Type Selection

- Which authentication type to use will vary by your organization

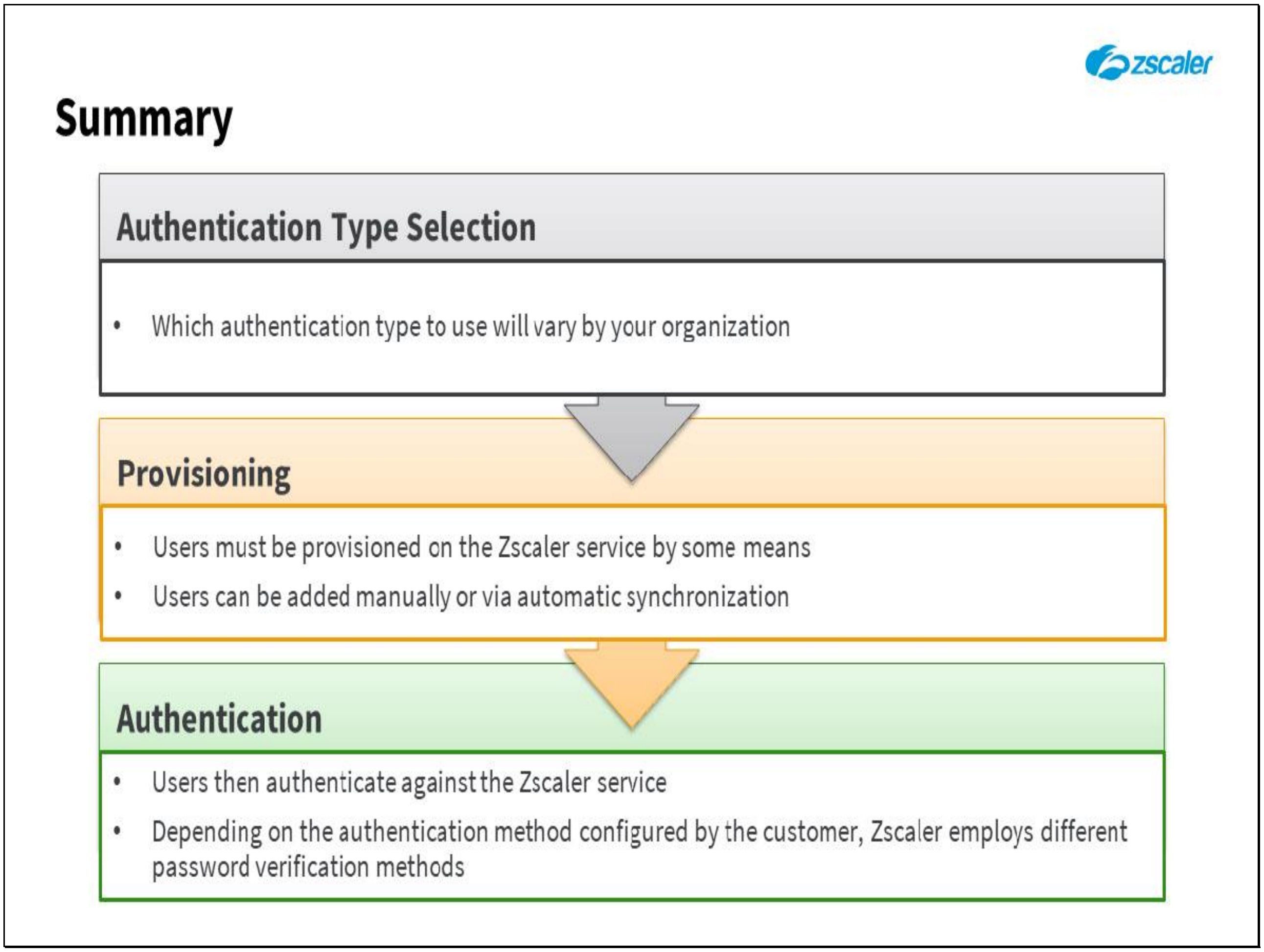
Provisioning

- Users must be provisioned on the Zscaler service by some means
- Users can be added manually or via automatic synchronization

Slide notes

Users must be provisioned on the Zscaler service by some means. Users can be added manually or via automatic synchronization.

Slide 53 - Summary



Summary

Authentication Type Selection

- Which authentication type to use will vary by your organization

Provisioning

- Users must be provisioned on the Zscaler service by some means
- Users can be added manually or via automatic synchronization

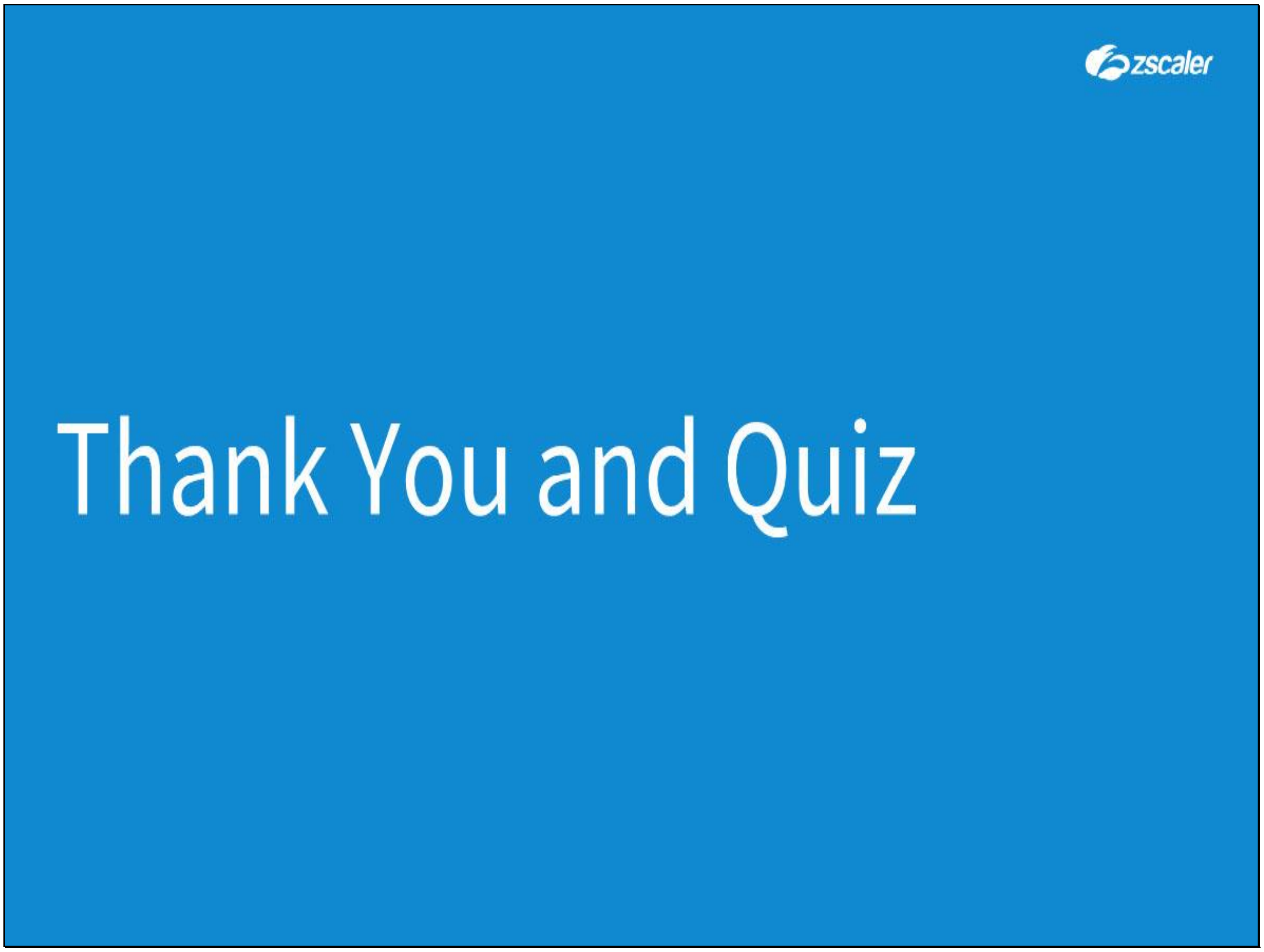
Authentication

- Users then authenticate against the Zscaler service
- Depending on the authentication method configured by the customer, Zscaler employs different password verification methods

Slide notes

Users then authenticate against the Zscaler service and, depending on the auth method configured by the customer, Zscaler employs different password verification methods.

Slide 54 - Thank You and Quiz



Thank You and Quiz

Slide notes

This completes the Understanding Authentication Methods module. We hope this module has been useful to you and thank you for your time.

What will follow is a short quiz to test your knowledge of the material presented during this module. Click the **X** in the upper right corner of the window to close this module then launch the quiz. You may retake the quiz as many times as necessary to pass.