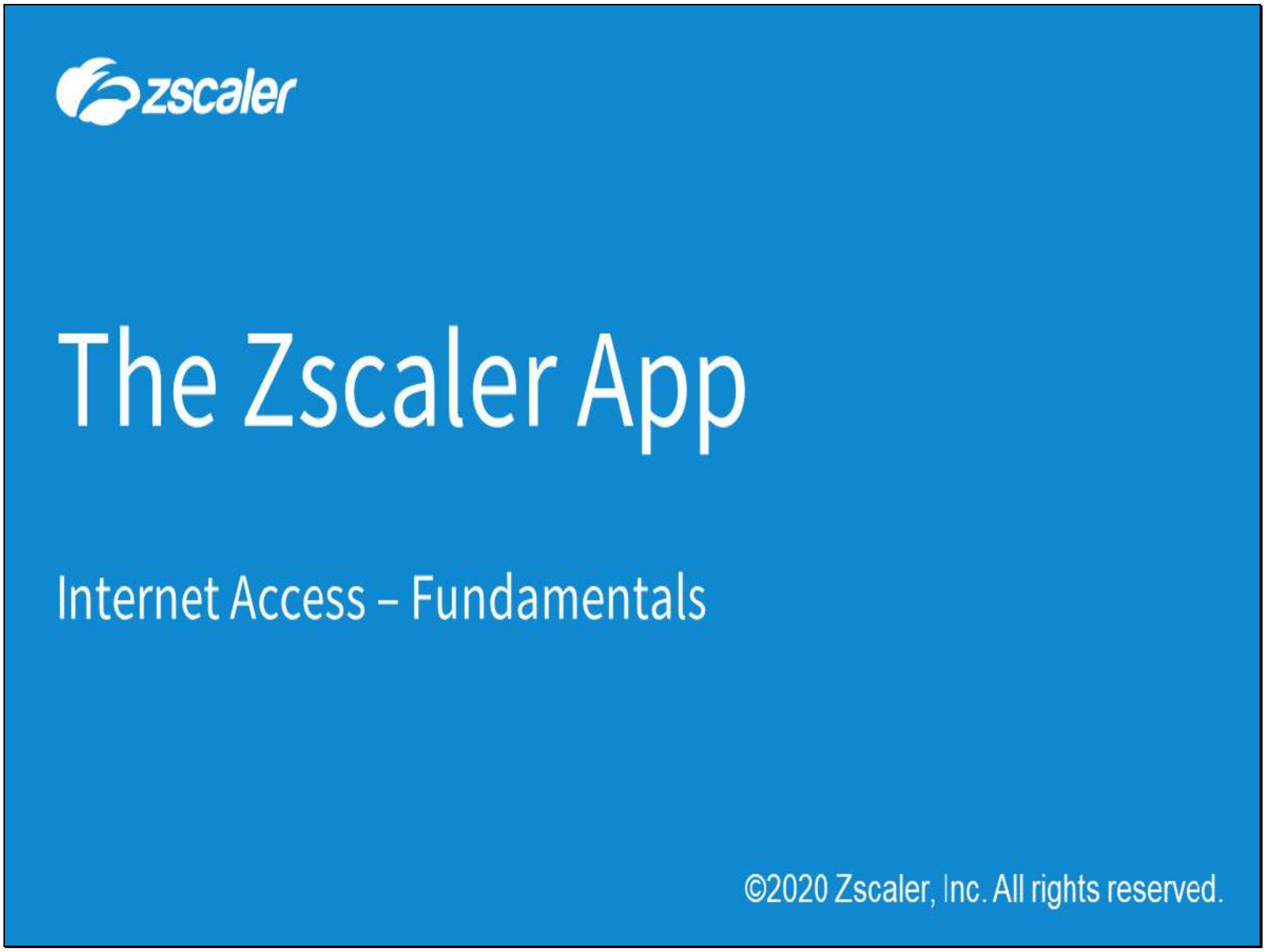
Slide 1 – The Zscaler App: IA Fundamentals



zscaler

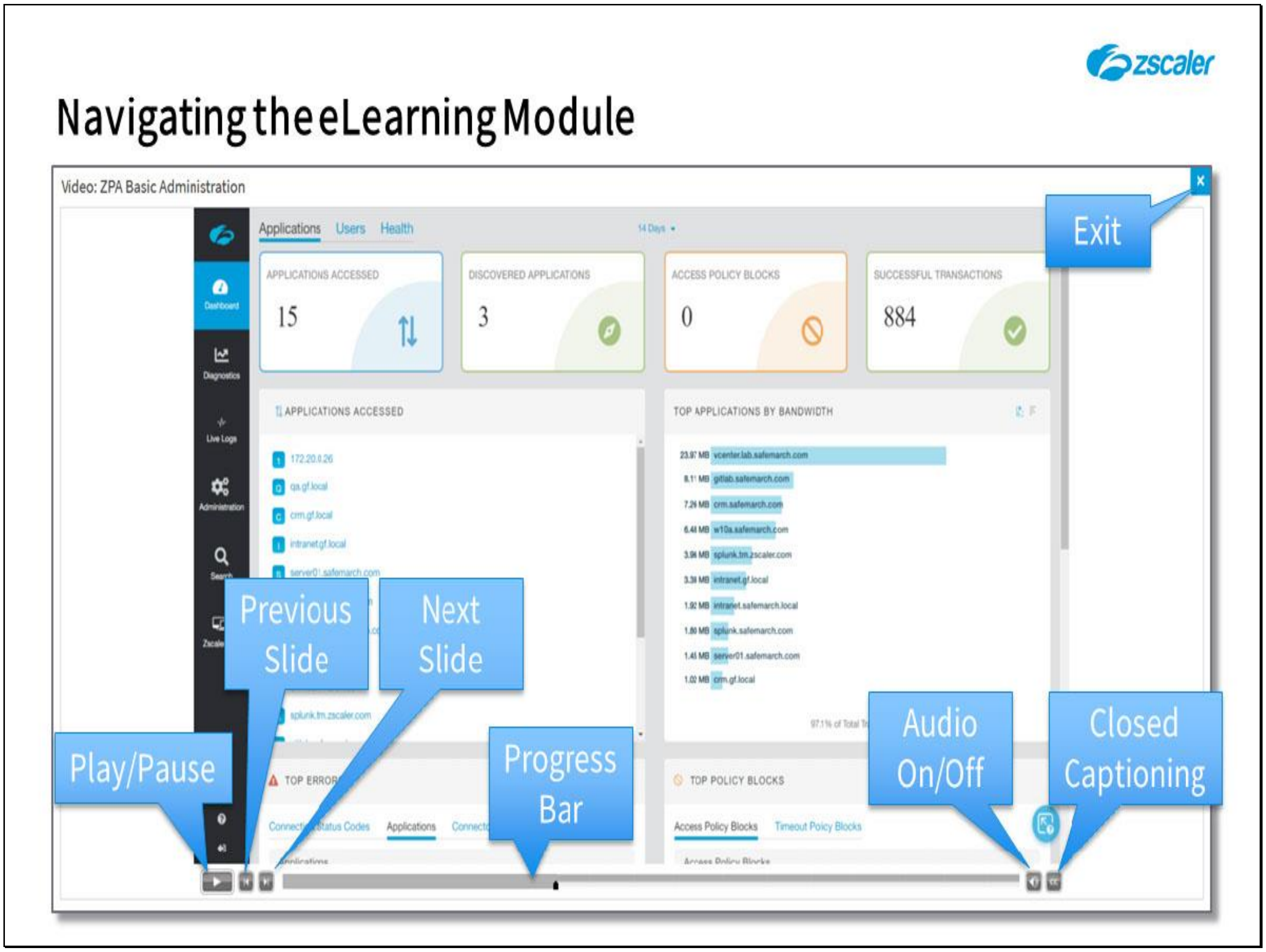
The Zscaler App

Internet Access – Fundamentals

Slide notes

Welcome to this training module on the Zscaler App Internet Access fundamentals.

Slide 2 - Navigating the eLearning Module



Navigating the eLearning Module

Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous**, and **Next** slide. 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 at the top to exit.

Slide 3 - Agenda

zscaler

Agenda

- Z App – ZIA: Deployment
- Z App – ZIA: Forwarding Modes
- Z App – ZIA: Silent Authentication with Zscaler App IdP
- Z App – ZIA: Provisioning and Enrollment Flow

Slide notes

In this module we will cover the following topics: The Zscaler App deployment process for Internet access; the Internet access forwarding modes available; the silent authentication option for Internet access using the Zscaler App Portal IdP; and the Zscaler App enrollment and provisioning flow for the ZIA service.

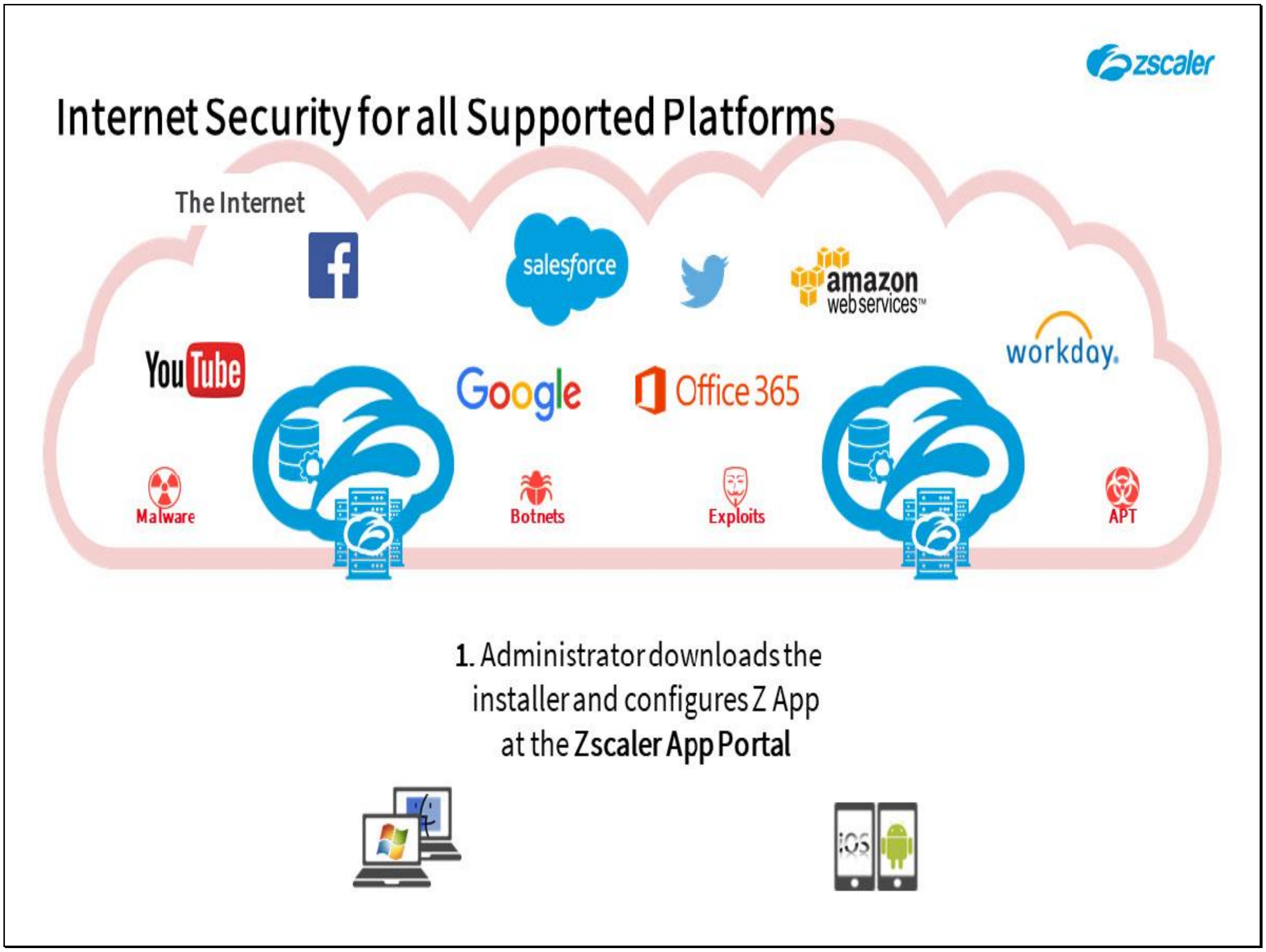
Slide 4 - Zscaler App – Architecture

Z App – ZIA: Deployment

Slide notes

The first topic that we will cover is a look at the Zscaler App deployment process for Internet access.

Slide 5 - Web Security for all Supported Platforms



Internet Security for all Supported Platforms

1. Administrator downloads the installer and configures Z App at the **Zscaler App Portal**

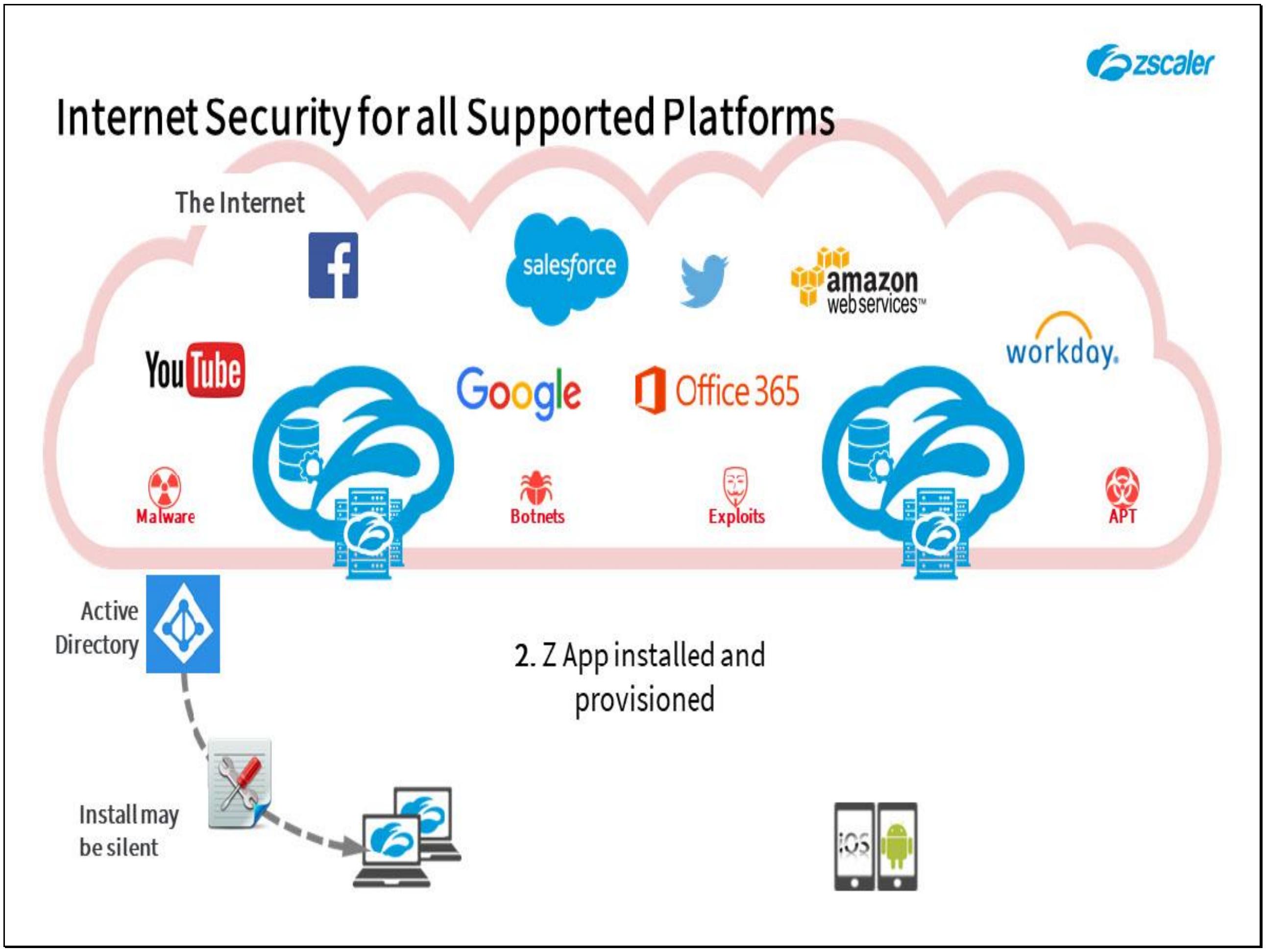
Slide notes

There are a number of steps to enabling Internet Security for your road warriors using the Zscaler App, as follows:

Step 1: An administrator must download the appropriate PC installation file for distribution and must configure appropriate App settings for the groups that will be using the App. For the ZIA service these include:

- **App Profile** and **Forwarding Profile** settings;
- **Notification** and **Support** settings;
- **Trusted Network** settings;
- **Zscaler App IdP** and **User Agent** settings.

Slide 6 - Web Security for all Supported Platforms



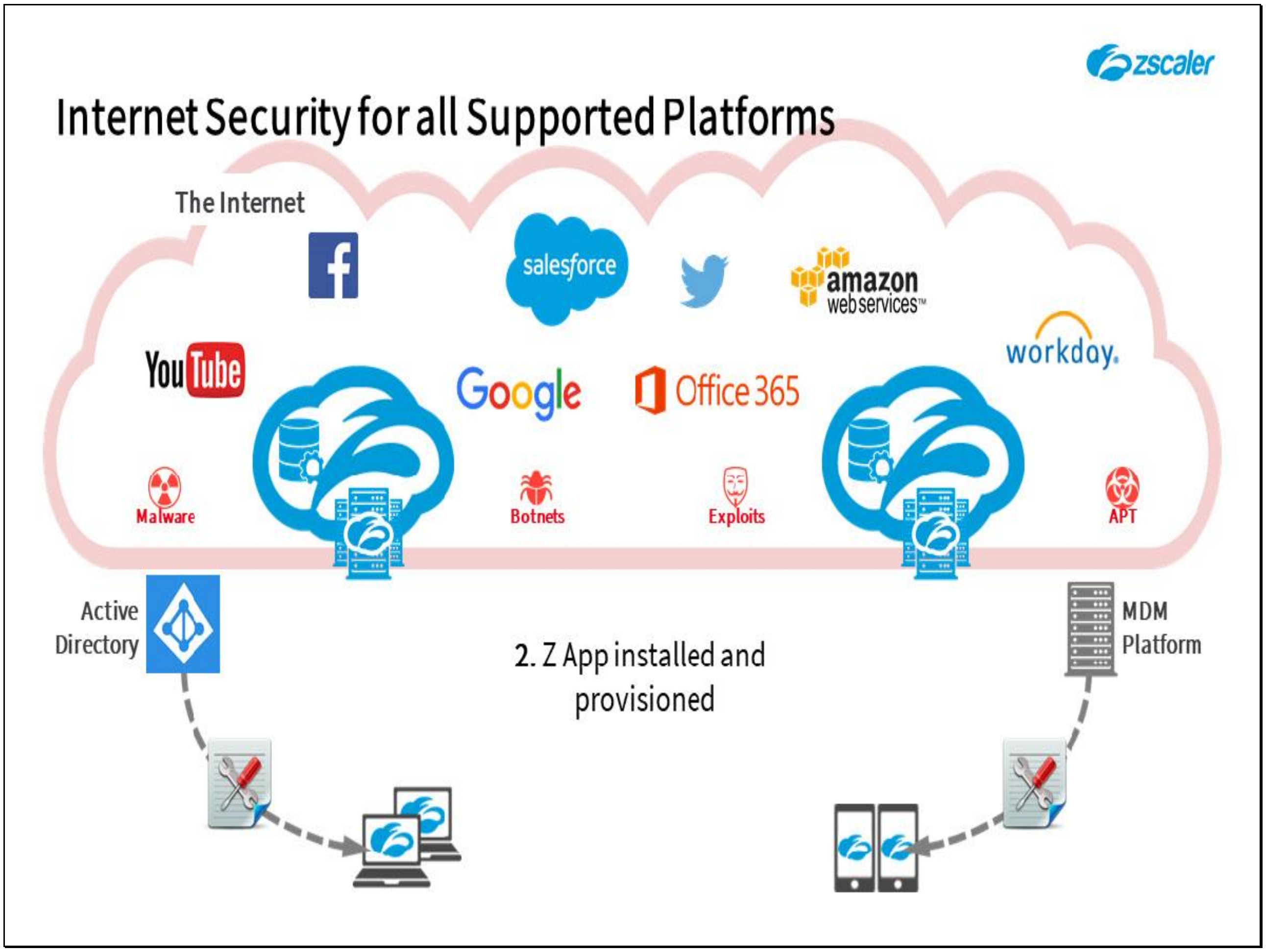
Internet Security for all Supported Platforms

2. Z App installed and provisioned

Slide notes

Step 2: The app must be distributed to the users that require it. For Windows users this can be done using an AD Group Policy Object (GPO) or Microsoft Intune, for Macs it can be done using Casper Suite or Tanium, or of course it can be installed manually. The install of the App can also be made silent, so the user is not aware that it is happening.

Slide 7 - Web Security for all Supported Platforms



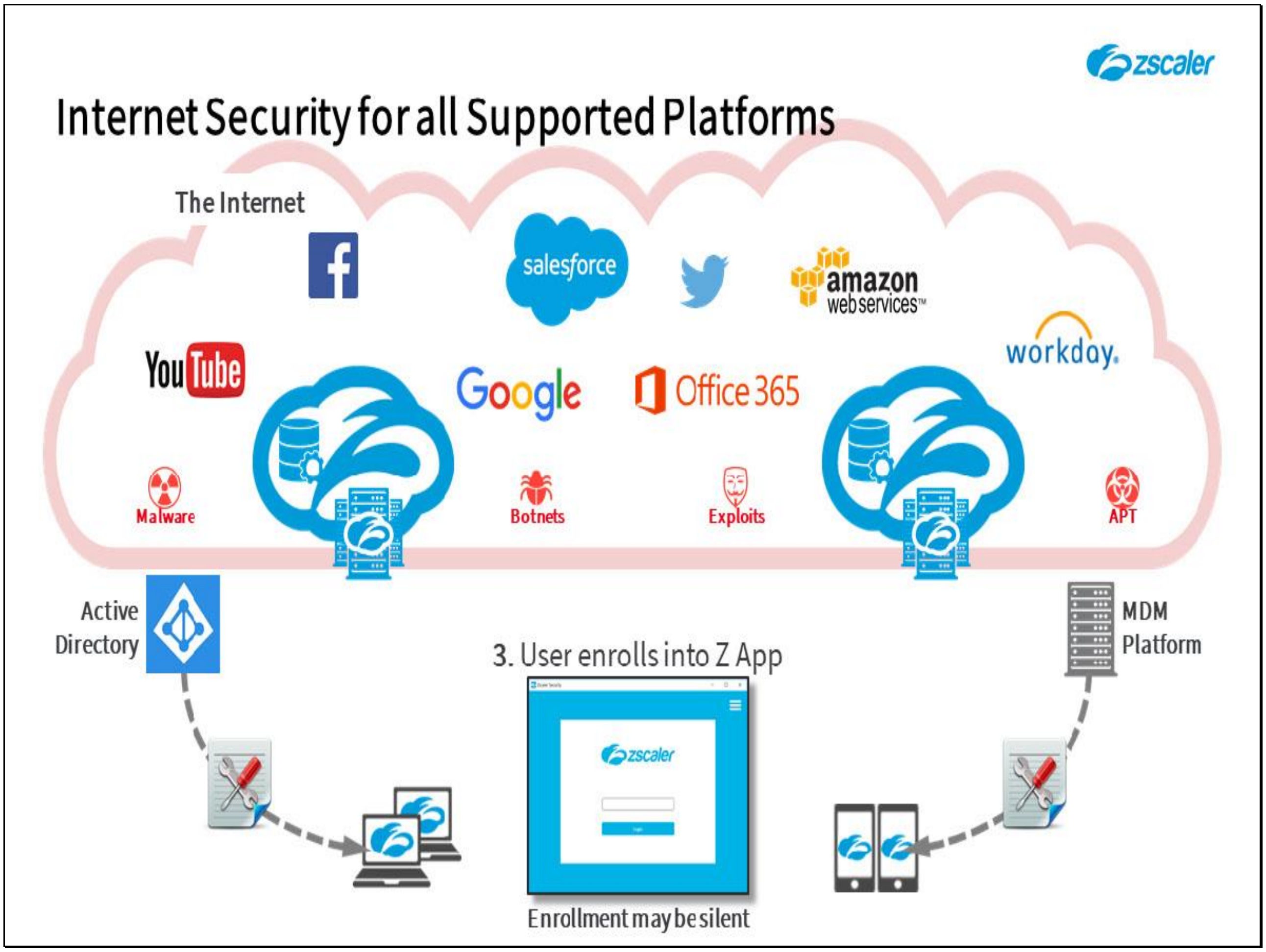
Internet Security for all Supported Platforms

2. Z App installed and provisioned

Slide notes

For Mobile devices, the installer is available on the public App Stores for your users to install themselves, or you can distribute it as a managed App using your preferred Mobile Device Management (MDM) platform, such as VMware’s Workspace ONE (previously known as AirWatch), MobileIron, or Microsoft Intune. If you push the App from an MDM manager, you have more control over how it is installed and configured on the end user’s device.

Slide 8 - Web Security for all Supported Platforms



Internet Security for all Supported Platforms

3. User enrolls into Z App

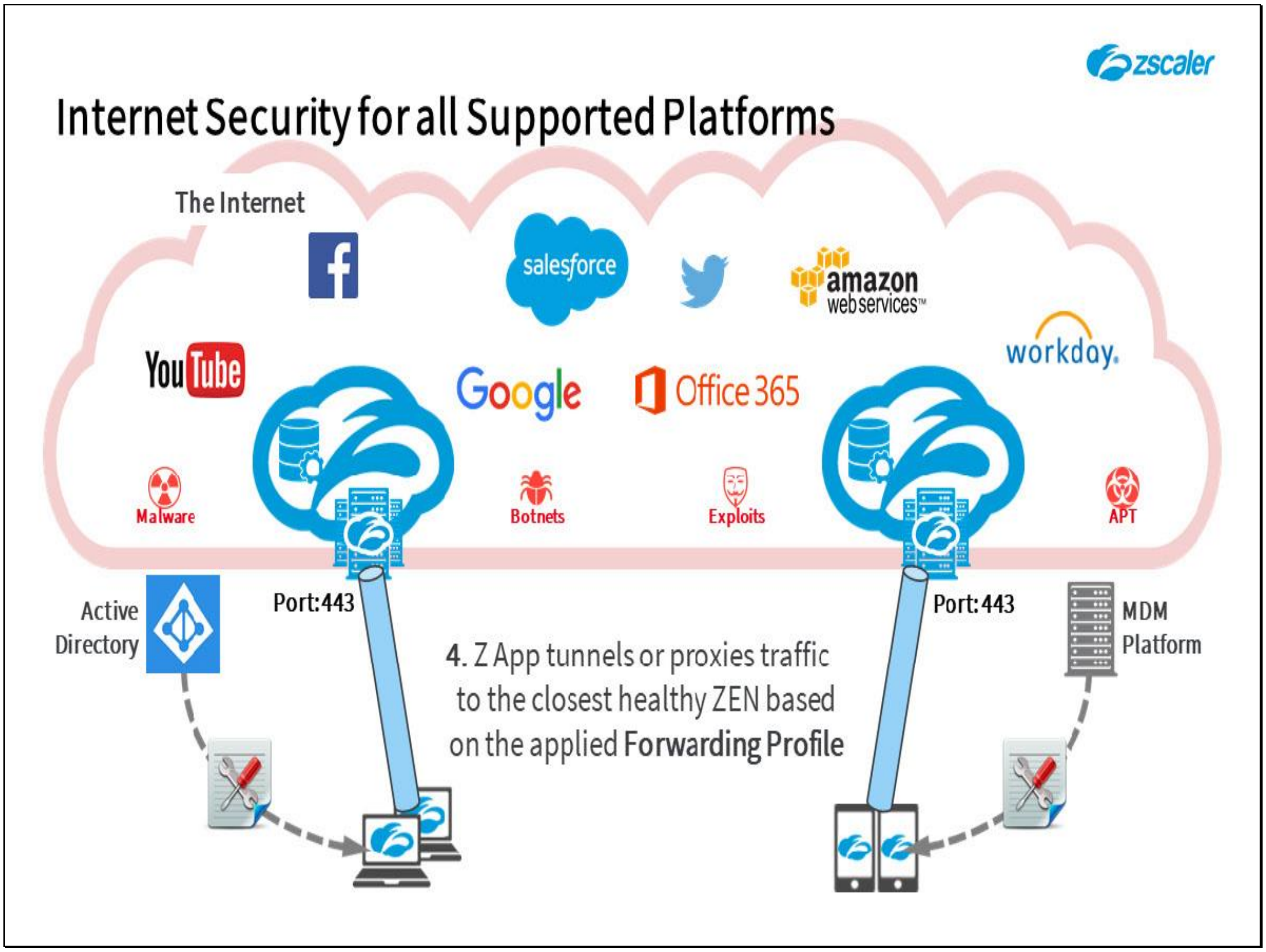
Enrollment may be silent

Slide notes

Step 3: After installation, the device user is prompted to enroll through the App. Currently this is a one-time enrollment process, that is coupled to the authentication method of your choice (although SAML is recommended). This enrollment can also be done silently based on the user's device login, either using Microsoft IWA or by using SAML and the **Zscaler App IdP**.

Note that, if the App is also to be used for access to private applications using the ZPA service, we recommend that you use SAML authentication and the same Identity Provider (IdP) to avoid the end user having to login twice.

Slide 9 - Web Security for all Supported Platforms



Internet Security for all Supported Platforms

4. Z App tunnels or proxies traffic to the closest healthy ZEN based on the applied **Forwarding Profile**

Slide notes

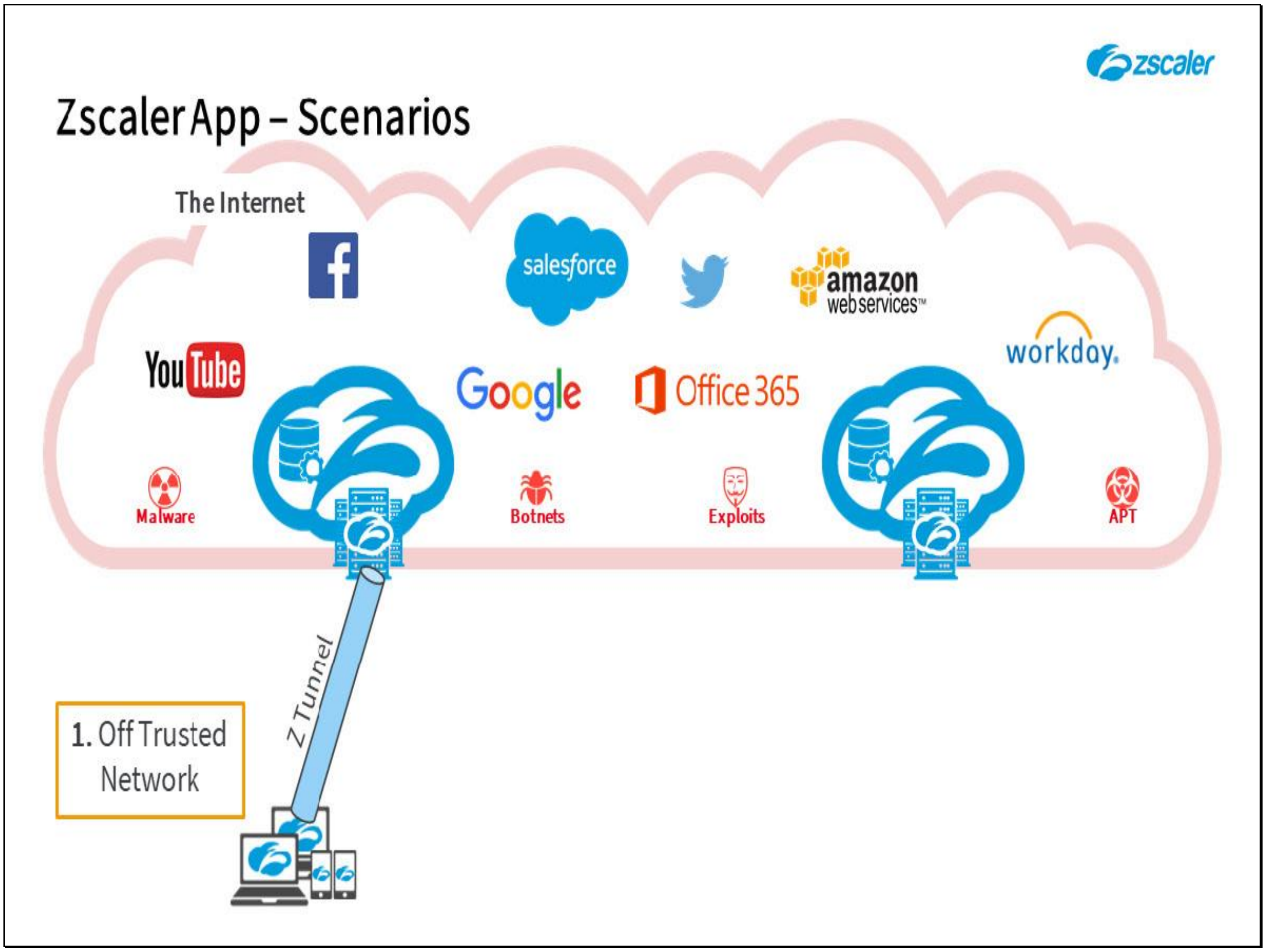
Step 4: After a successful enrollment, if used for Internet Security with the ZIA service, the App will forward traffic to the Zscaler Internet Access Cloud based on the settings in the applied **Forwarding Profile**. Options are:

1. To tunnel all port 80 and port 443 traffic in a **Tunnel 1.0** Z Tunnel to the local (or a designated) ZEN;
2. Send all HTTP/HTTPS traffic regardless of port into a **Tunnel 1.0** Z Tunnel;
3. Send all unicast IPv4 traffic regardless of port in a **Tunnel 2.0** Z Tunnel;
4. To apply the default or a specified PAC file;
5. Or to disable the app.

When **Tunnel 1.0** is used the tunnels are unencrypted, lightweight HTTP CONNECT tunnels established on destination port 443.

If you upgrade users to the 2.x version of the App, you may also use the **Tunnel 2.0** method to forward all unicast IPv4 traffic regardless of port using either DTLS or TLS.

Slide 10 - Zscaler App – Scenarios

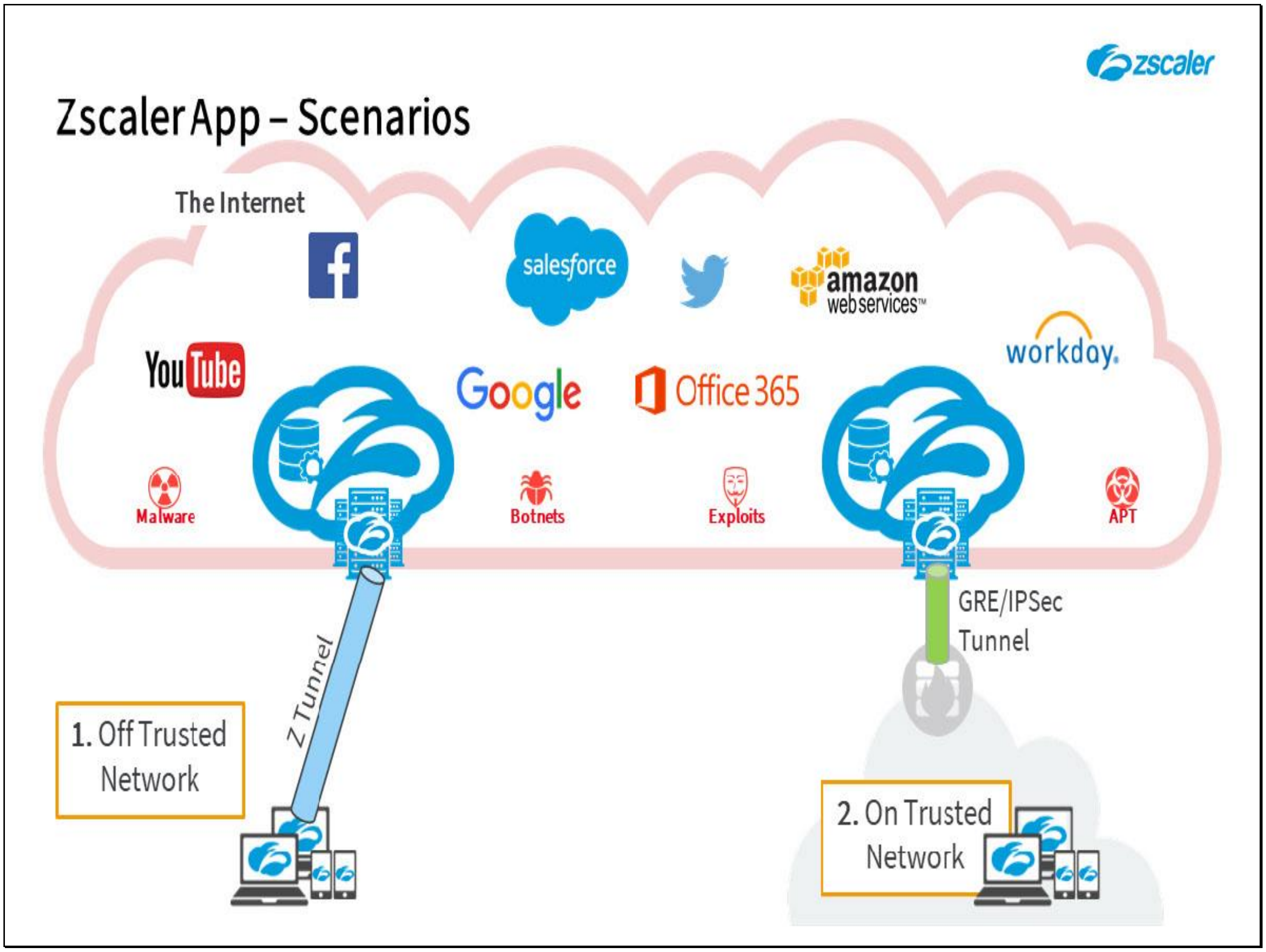


Slide notes

There are three primary forwarding scenarios for the Zscaler App used for Internet access, and the first of these is the classic Road Warrior scenario:

1. Where a user is connecting from outside any of your locations and is therefore not on a trusted network. It is for precisely this situation that the Zscaler App was developed, and it provides a mechanism to tunnel or proxy traffic from the client device to the Zscaler cloud to ensure the scanning and protection of your remote user's traffic.

Slide 11 - Zscaler App – Scenarios

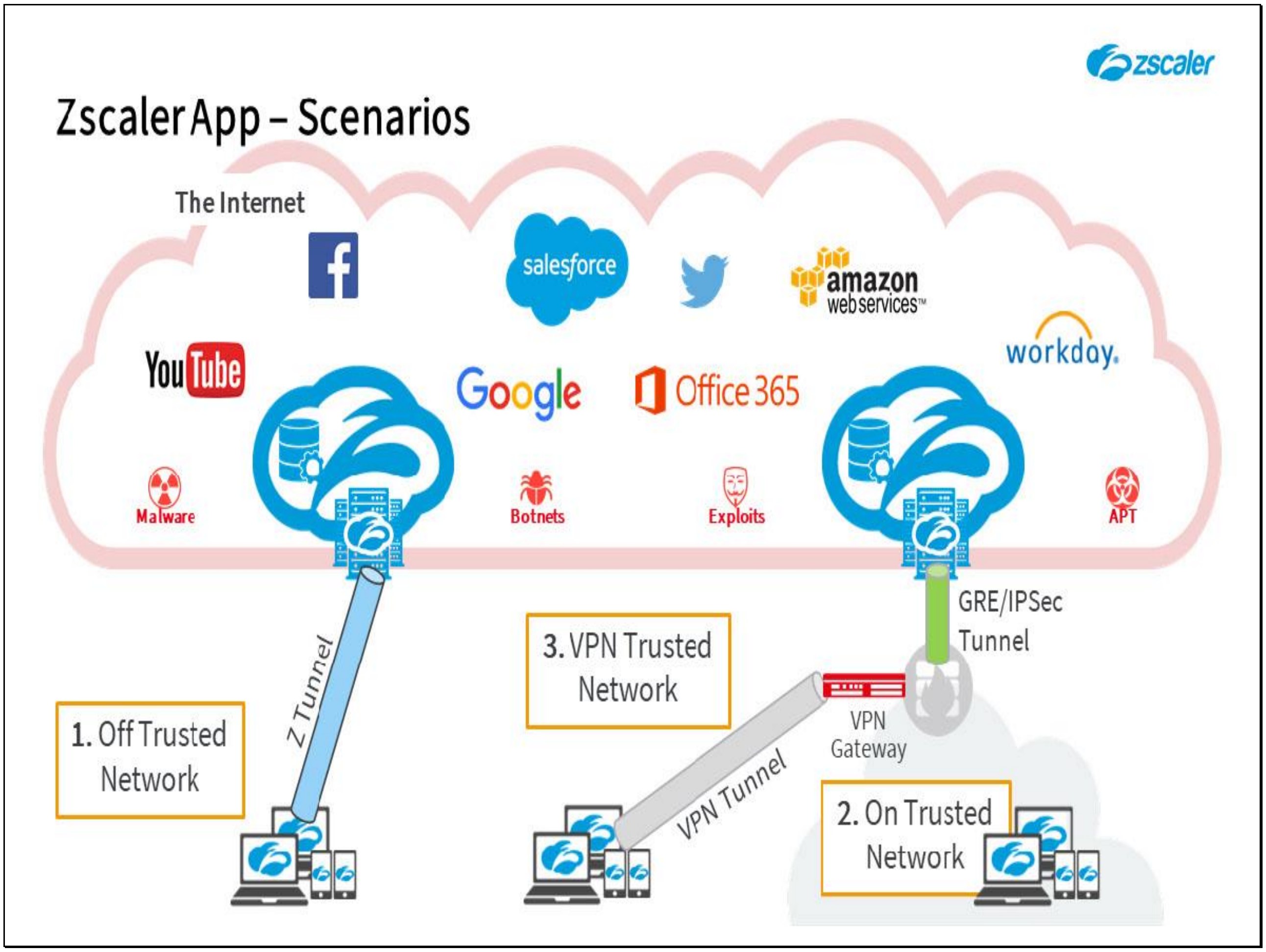


Slide notes

2. But what happens when your Road Warriors return to the office? If they connect to a trusted network at a location that connects to Zscaler anyway, is there any need for the app to tunnel traffic to Zscaler? Normally your offices will establish a GRE or IPSec tunnel to Zscaler, and all devices on the trusted network will have their traffic scanned and protected anyway.

   Note that the app has the ability to detect the network it is connected to, and can be configured to use different forwarding options, or even to disable itself depending on the network.

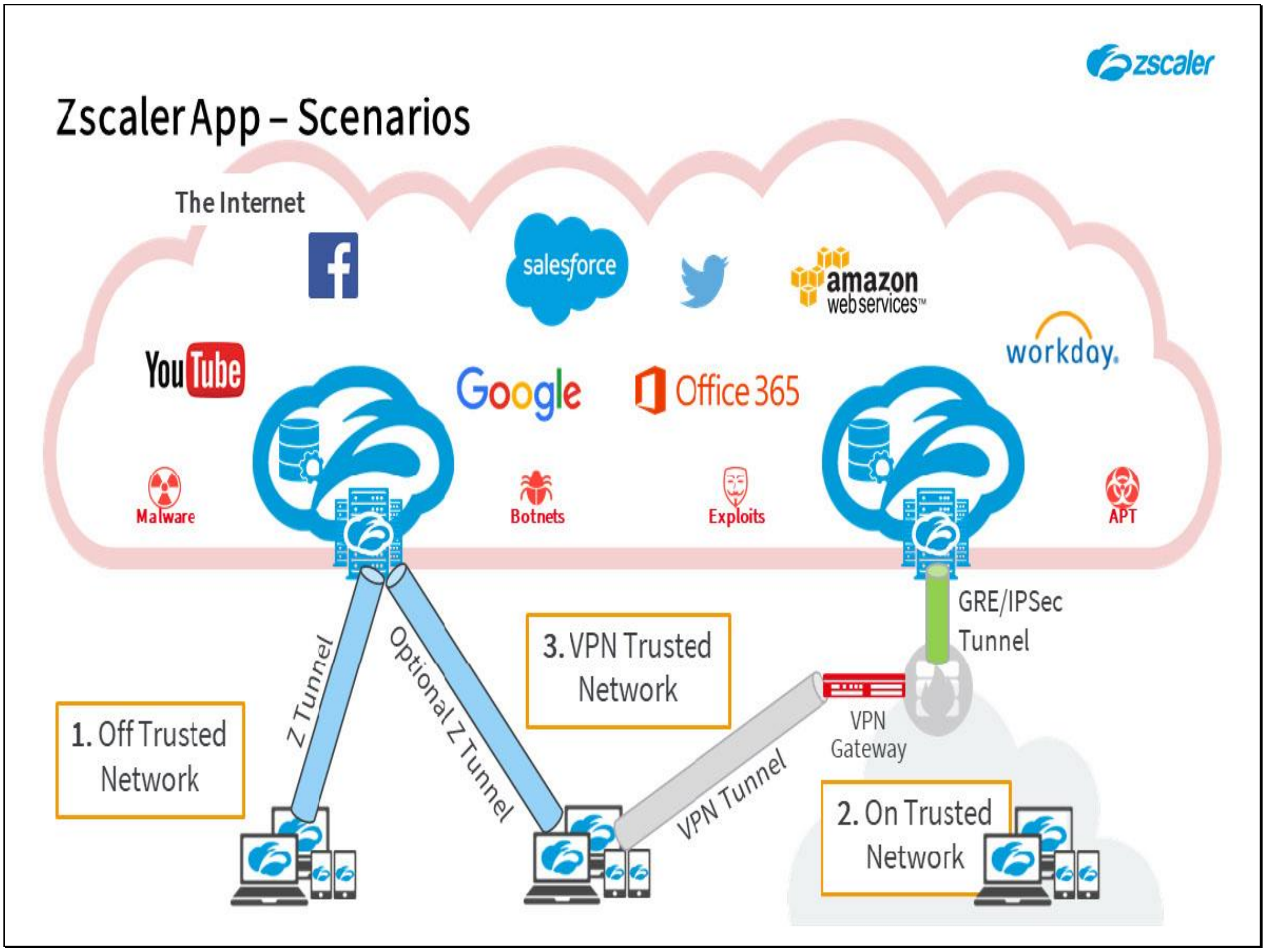
Slide 12 - Zscaler App – Scenarios



Slide notes

3. The third main scenario is when a Road Warrior who is out of the office, chooses to establish a VPN connection to a trusted network. There are two main options here, either the VPN is established for all traffic, in which case there is no real need for the Zscaler App to tunnel, …

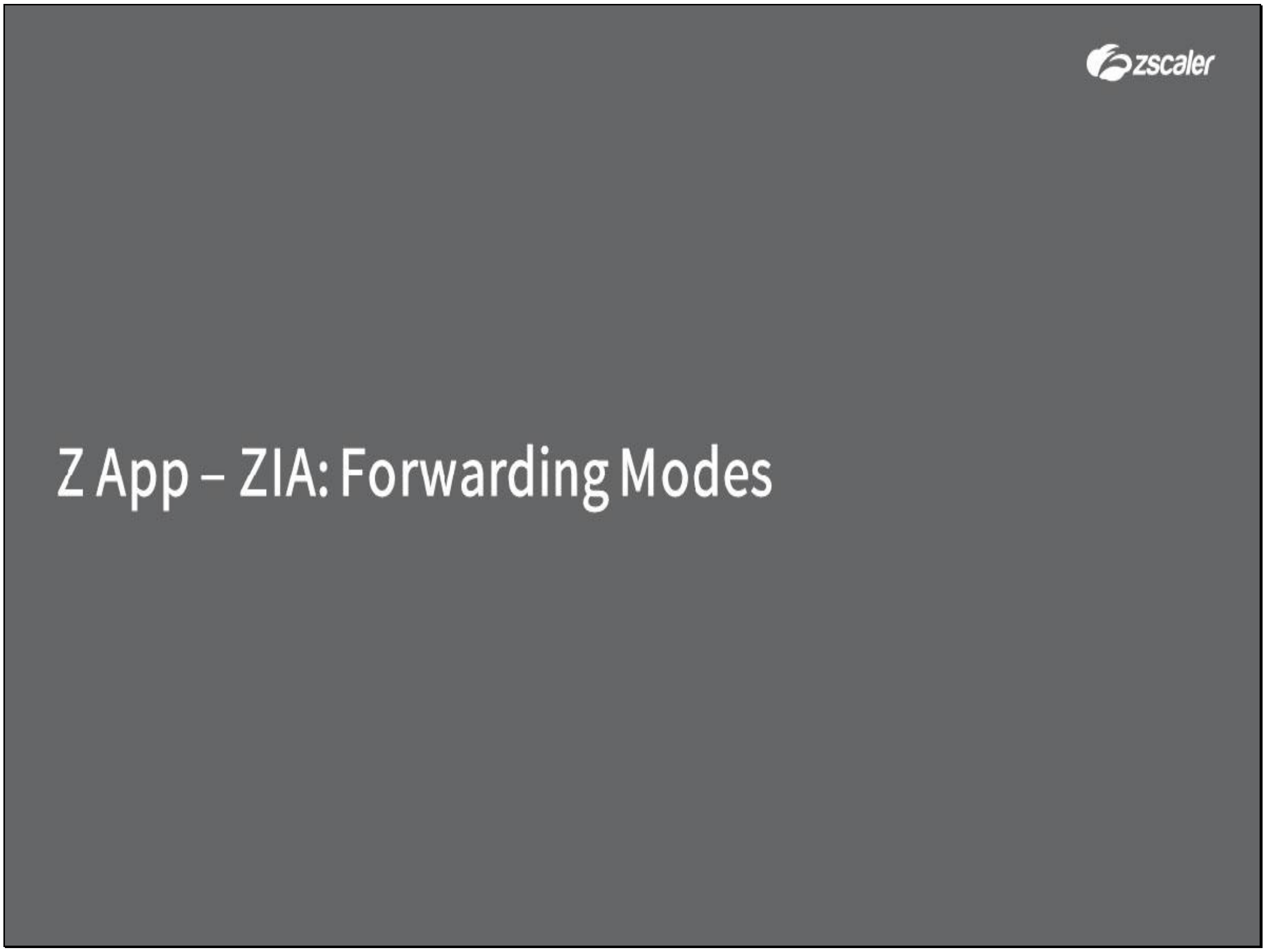
Slide 13 - Zscaler App – Scenarios



Slide notes

…or the VPN is only used for certain traffic, while Internet traffic goes direct. In this ‘split tunnel’ scenario, the Zscaler App can be used to tunnel or proxy the Internet bound traffic to Zscaler for scanning and protection.

Slide 14 - Zscaler App – Forwarding Modes



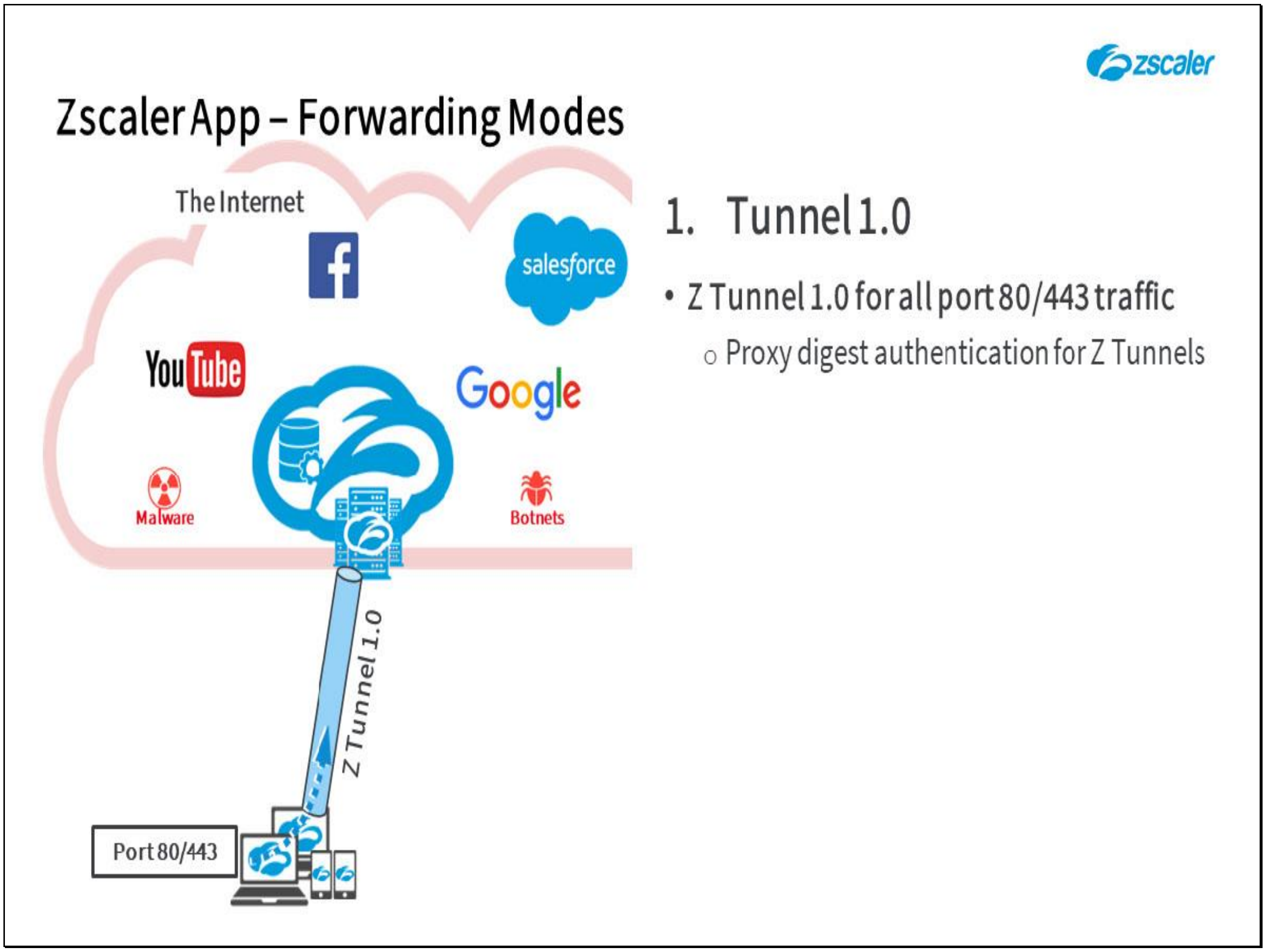
zscaler

Z App – ZIA: Forwarding Modes

Slide notes

The next topic that we will cover are the Zscaler App forwarding modes available.

Slide 15 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

1. Tunnel 1.0

- Z Tunnel 1.0 for all port 80/443 traffic
  - Proxy digest authentication for Z Tunnels

Slide notes

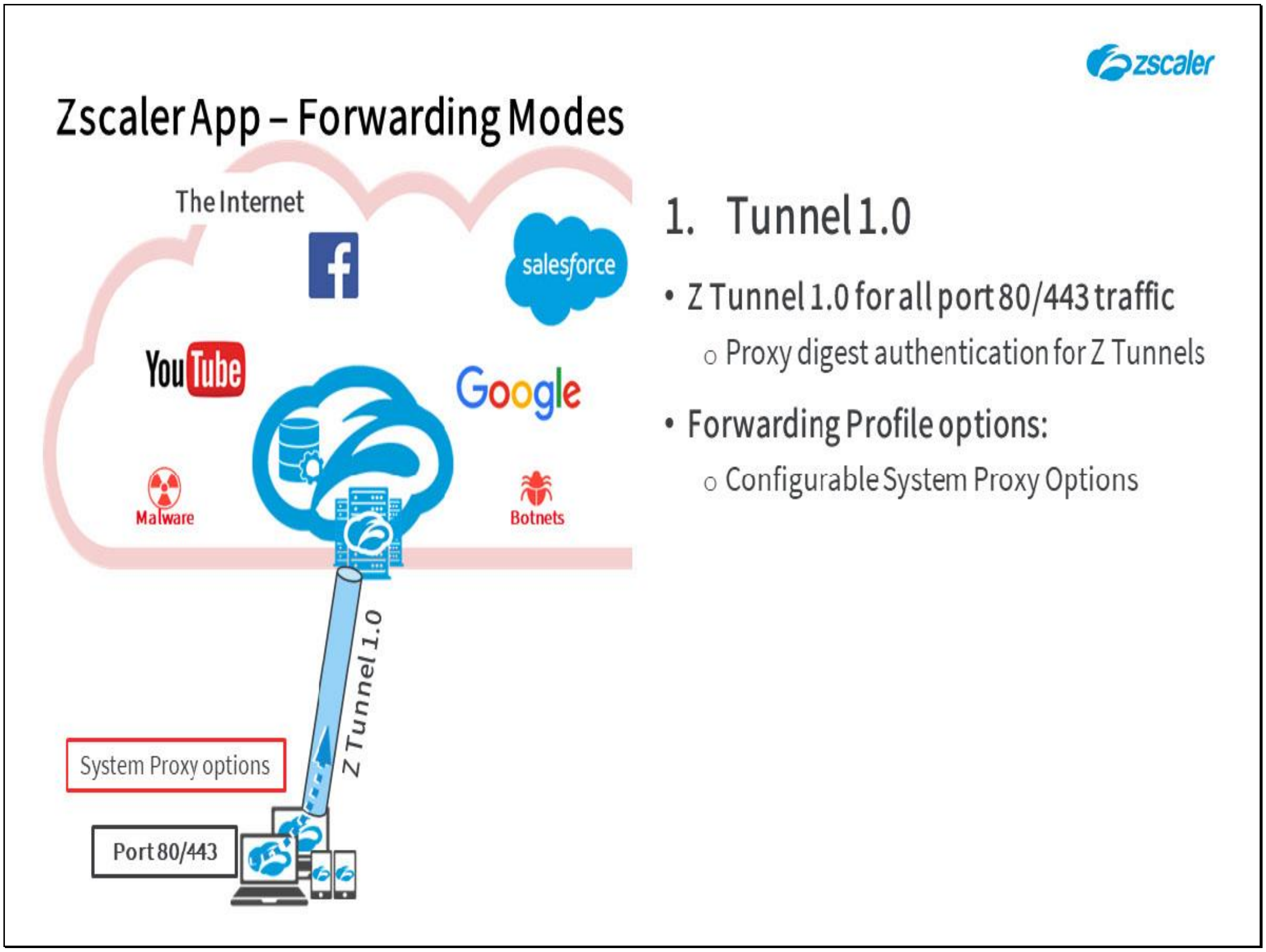
Regardless of the connection scenario (whether **On**, **Off**, or **VPN to** a trusted network), there are five forwarding options to choose from:

1. The first of these is simply to **Tunnel** using the 1.0 method, meaning that the app will establish a lightweight HTTP CONNECT tunnel on destination port 443 to the local (or a designated) ZEN, for all port 80 or port 443 traffic.

   Note that this need not necessarily be browser traffic only, any traffic generated by apps on the device that use ports 80 or 443 will also be forwarded to Zscaler in the Z Tunnel.

   The tunnels authenticate to the ZEN using proxy digest authentication, which we will look at in detail in the **Under the Covers** module.

Slide 16 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

1. Tunnel 1.0

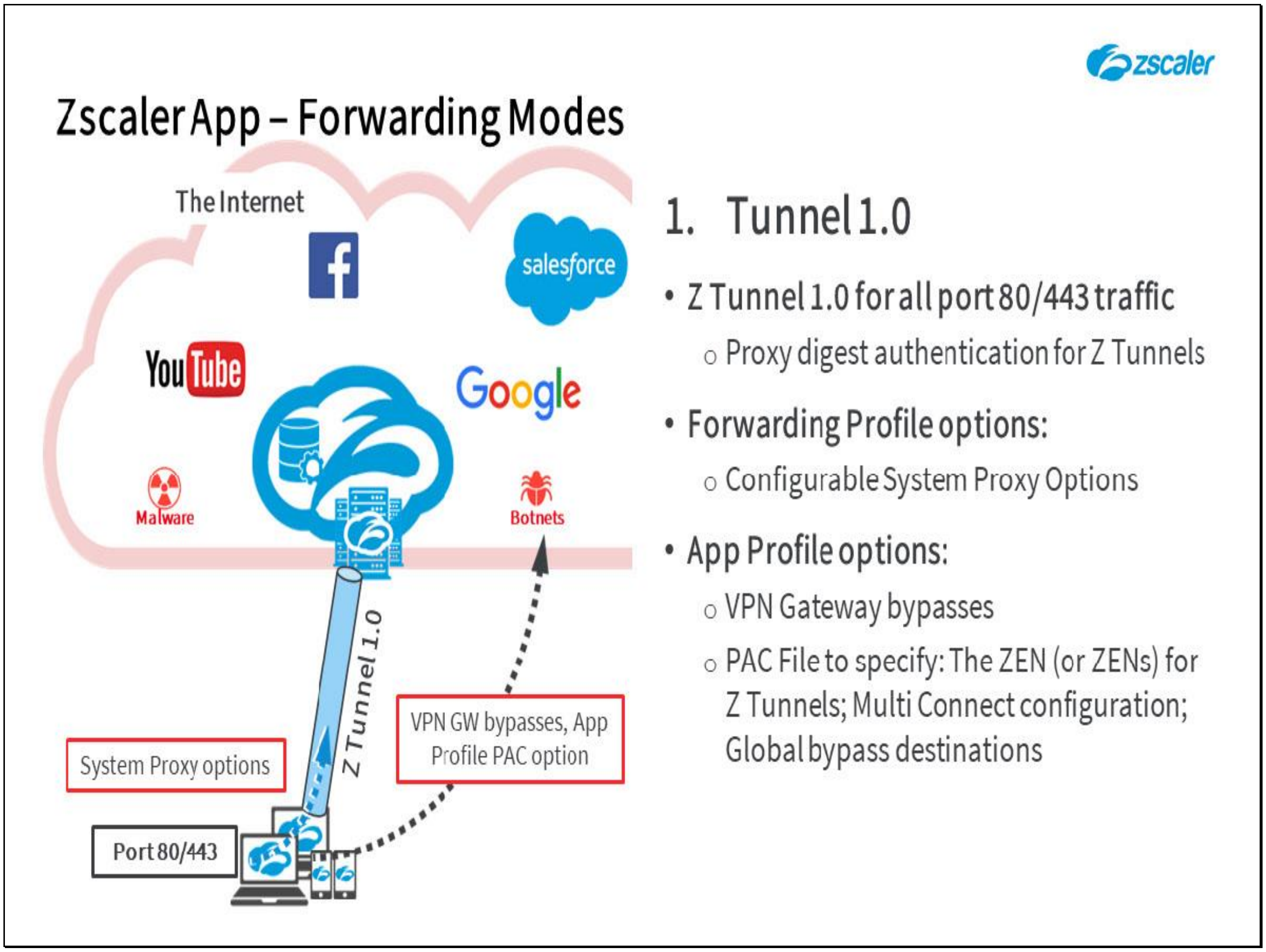
- Z Tunnel 1.0 for all port 80/443 traffic
  - Proxy digest authentication for Z Tunnels
- Forwarding Profile options:
  - Configurable System Proxy Options

Slide notes

The **Forwarding Profile** provides options for the management of any system proxy that might be locally defined in the browser settings, with options to always **Enforce** it, **Never** enforce it, or to **Apply on a Network Change**. Proxy settings may be:

- Automatically detected;
- Configured using a script;
- Set to use a local Proxy server on the LAN;
- Applied using a GPO update;
- Or any combination of these options.

Slide 17 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

1. Tunnel 1.0

- Z Tunnel 1.0 for all port 80/443 traffic
  - Proxy digest authentication for Z Tunnels
- Forwarding Profile options:
  - Configurable System Proxy Options
- App Profile options:
  - VPN Gateway bypasses
  - PAC File to specify: The ZEN (or ZENs) for Z Tunnels; Multi Connect configuration; Global bypass destinations

Slide notes

In the **App Profile** you have the option to specify **HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY**. Here you can specify one or more FQDNs or IP addresses for your corporate VPN gateways, traffic for these destinations is not even processed by the Zscaler App. Note that, while it is possible to add bypass destinations here other than your VPN gateways, this is not recommended.

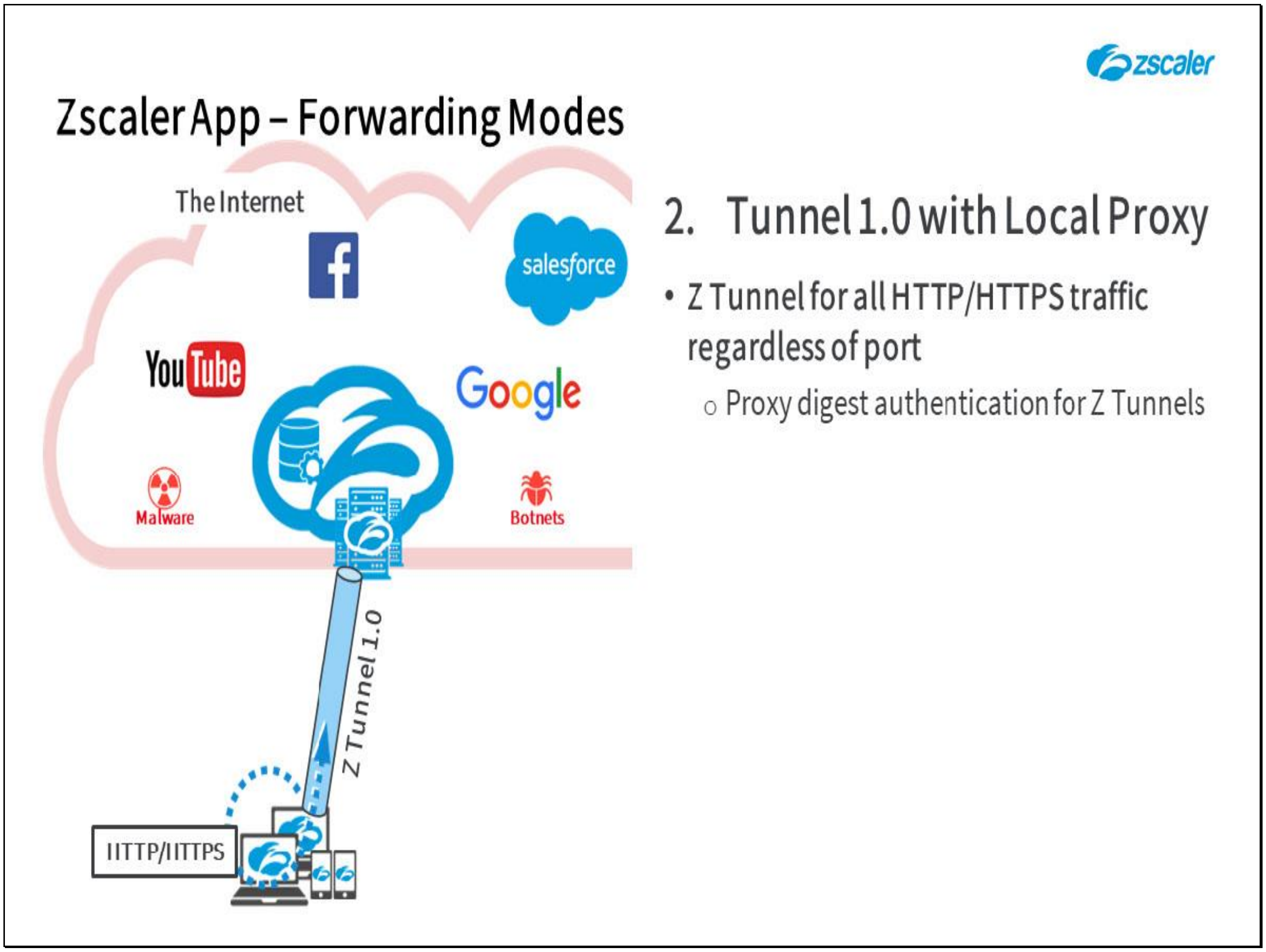
In the **App Profile** you also have the option to apply a custom PAC file that may be used for two purposes:

1. The first being to specify the ZEN (or ZENs) to establish tunnels to (for example a Service Edge or Virtual Service Edge). Logic can be added to this PAC file to specify an alternative ZEN to use under a specific set of circumstances, e.g. for internal destinations, or destination services that are only accessible if the request originates in a specific country (the Multi Connect feature).
2. The second purpose being to specify destinations that bypass the Zscaler cloud completely. As this PAC file is applied in all forwarding modes that use Z Tunnels, if there are 'global' bypass destinations that must be defined for all Z Tunnel modes, they should be added to this PAC file.

Remember that you can also add SSL and authentication exemptions in the Admin Portal (which is the recommended way to ‘bypass’ these categories of traffic). Any bypasses that you add to this PAC file will be processed by the App but will not be forwarded to the Zscaler cloud.

Note, the app checks for updates to this PAC file every 15 minutes.

Slide 18 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

2. Tunnel 1.0 with Local Proxy

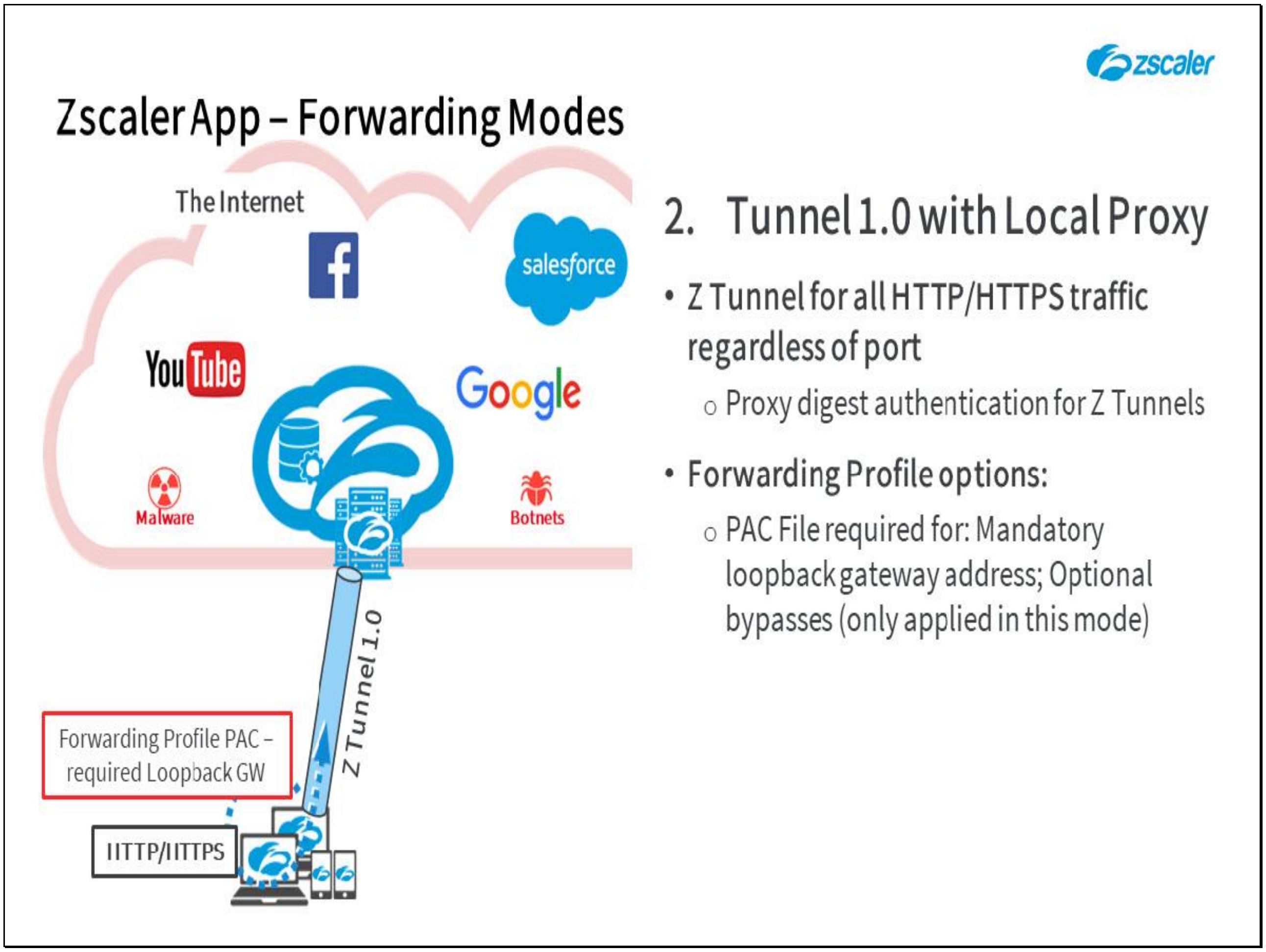
- Z Tunnel for all HTTP/HTTPS traffic regardless of port
  - Proxy digest authentication for Z Tunnels

Slide notes

2. The second (and default) forwarding option is the **Tunnel with Local Proxy** option, which can only be used with **Tunnel 1.0**. This method sets up a lightweight HTTP CONNECT tunnel with a loopback IP based socket for all traffic that follows the proxy (which normally means all **HTTP** and **HTTPS** traffic regardless of port). All other traffic is sent directly to the Internet. This option can be useful when the user is on a trusted VPN and the regular tunnel mode will not work.

   As Z Tunnels are used in this forwarding mode, the tunnels are once again transparently authenticated to the ZEN using proxy digest authentication.

Slide 19 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

Forwarding Profile PAC – required Loopback GW

HTTP/HTTPS

2. Tunnel 1.0 with Local Proxy

- Z Tunnel for all HTTP/HTTPS traffic regardless of port
  - o Proxy digest authentication for Z Tunnels
- Forwarding Profile options:
  - o PAC File required for: Mandatory loopback gateway address; Optional bypasses (only applied in this mode)

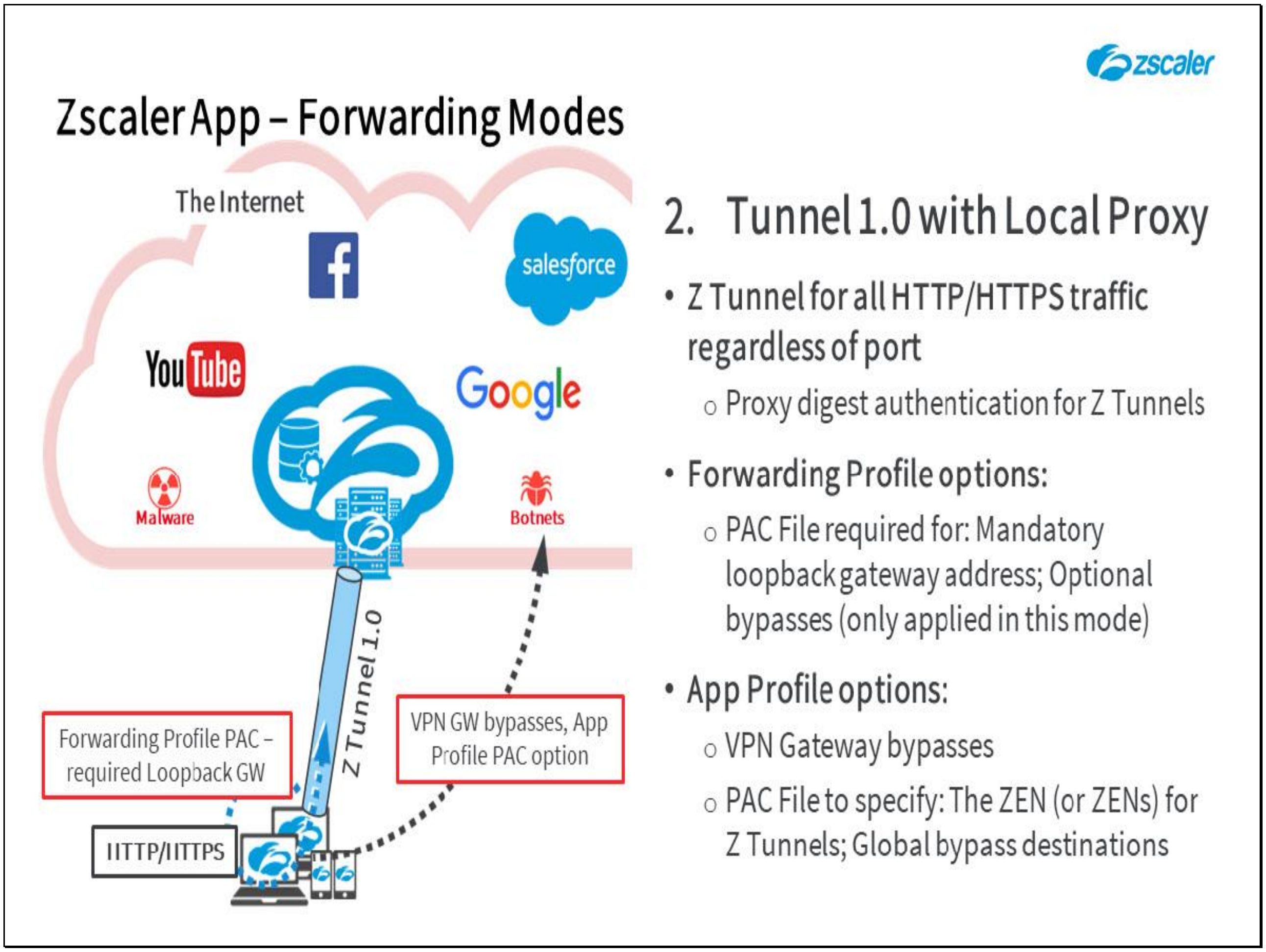
Slide notes

With this option, traffic that follows the proxy definition (primarily HTTP and HTTPS) will be forwarded to the loopback address on **port 9000** (although the port can be configured from the Zscaler App Portal if necessary). The Zscaler App will listen for traffic to proxy on the configured port and will tunnel it to the closest healthy ZEN (or to the ZEN specified in the **App Profile** PAC file).

In the **Forwarding Profile** you have the option to manually specify the URL for a custom PAC file, apply it by GPO update, or both. Any custom PAC file applied MUST use the gateway macro function **${ZAPP_LOCAL_PROXY}** to specify the forwarding destination. Note that if no custom PAC file is specified, the system will use a default PAC with the gateway macro defined.

This PAC file may also contain destinations to be bypassed by the Zscaler App, however note that this PAC file is ONLY applied in this forwarding mode, so if there are bypass destinations that must be defined ONLY for this mode, they can be added to this PAC file. This PAC file is also refreshed every 15 minutes.

Slide 20 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

Forwarding Profile PAC – required Loopback GW

VPN GW bypasses, App Profile PAC option

2. Tunnel 1.0 with Local Proxy

- Z Tunnel for all HTTP/HTTPS traffic regardless of port
  - Proxy digest authentication for Z Tunnels
- Forwarding Profile options:
  - PAC File required for: Mandatory loopback gateway address; Optional bypasses (only applied in this mode)
- App Profile options:
  - VPN Gateway bypasses
  - PAC File to specify: The ZEN (or ZENs) for Z Tunnels; Global bypass destinations

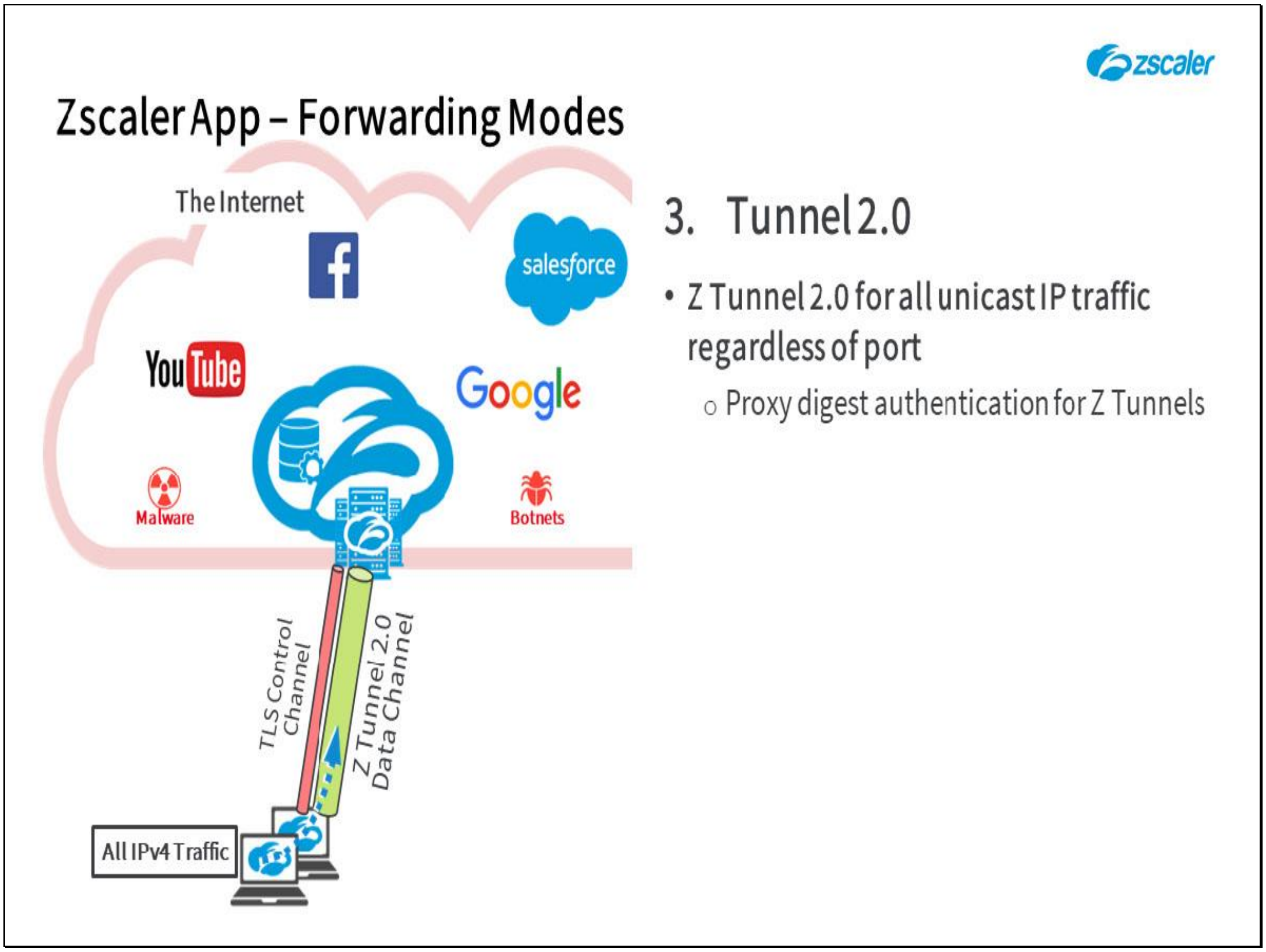
Slide notes

In the **App Profile**, you still have the option to specify:

- VPN GW bypasses;
- The ZEN (or ZENs) for the tunnels;
- Or PAC file global bypasses.

Remember, the PAC file here is applied in ALL forwarding modes that use Z Tunnels and should be used for ‘global’ bypass destinations that must be defined for all Z Tunnel forwarding modes.

Slide 21 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

3. Tunnel 2.0

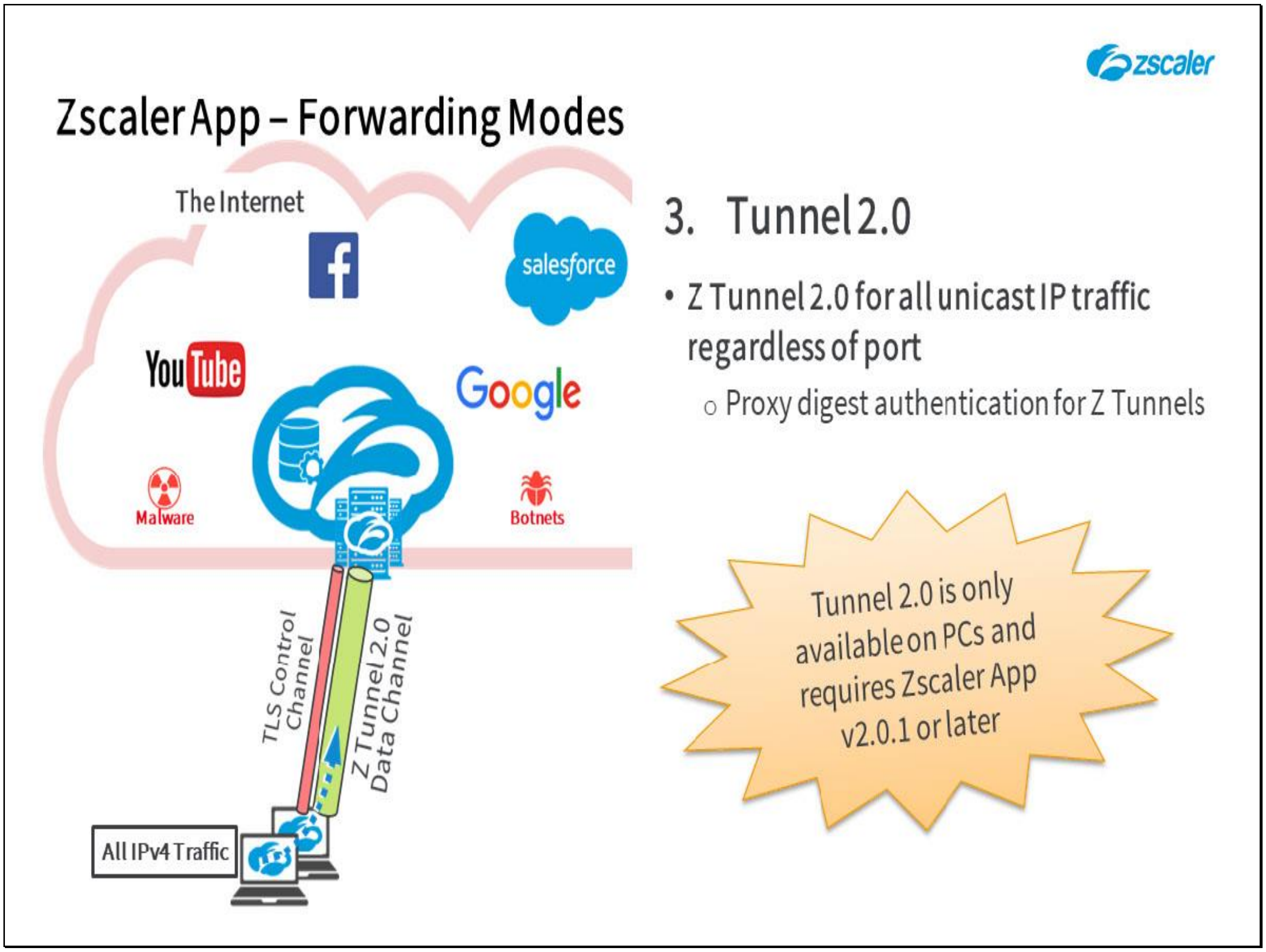
- Z Tunnel 2.0 for all unicast IP traffic regardless of port
  - Proxy digest authentication for Z Tunnels

Slide notes

3. The **Tunnel 2.0** option is a new tunneling mode for PCs, that supports the forwarding of all IPv4 unicast traffic types on just about any port. When using **Tunnel 2.0**, Z App will first establish a TLS tunnel to the closest healthy (or a specified) ZEN for use as a control channel. It will then set up data tunnels using **DTLS**, **TLS**, or the **Tunnel 1.0** method, depending on the configuration. By default, it will first try **DTLS**, if that does not work it will fall back to **TLS**, and if necessary, to **Tunnel 1.0**.

   Tunnel authentication is the same as for **Tunnel 1.0**, i.e. using Proxy Digest authentication.

Slide 22 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

3. Tunnel 2.0

- Z Tunnel 2.0 for all unicast IP traffic regardless of port
  - Proxy digest authentication for Z Tunnels

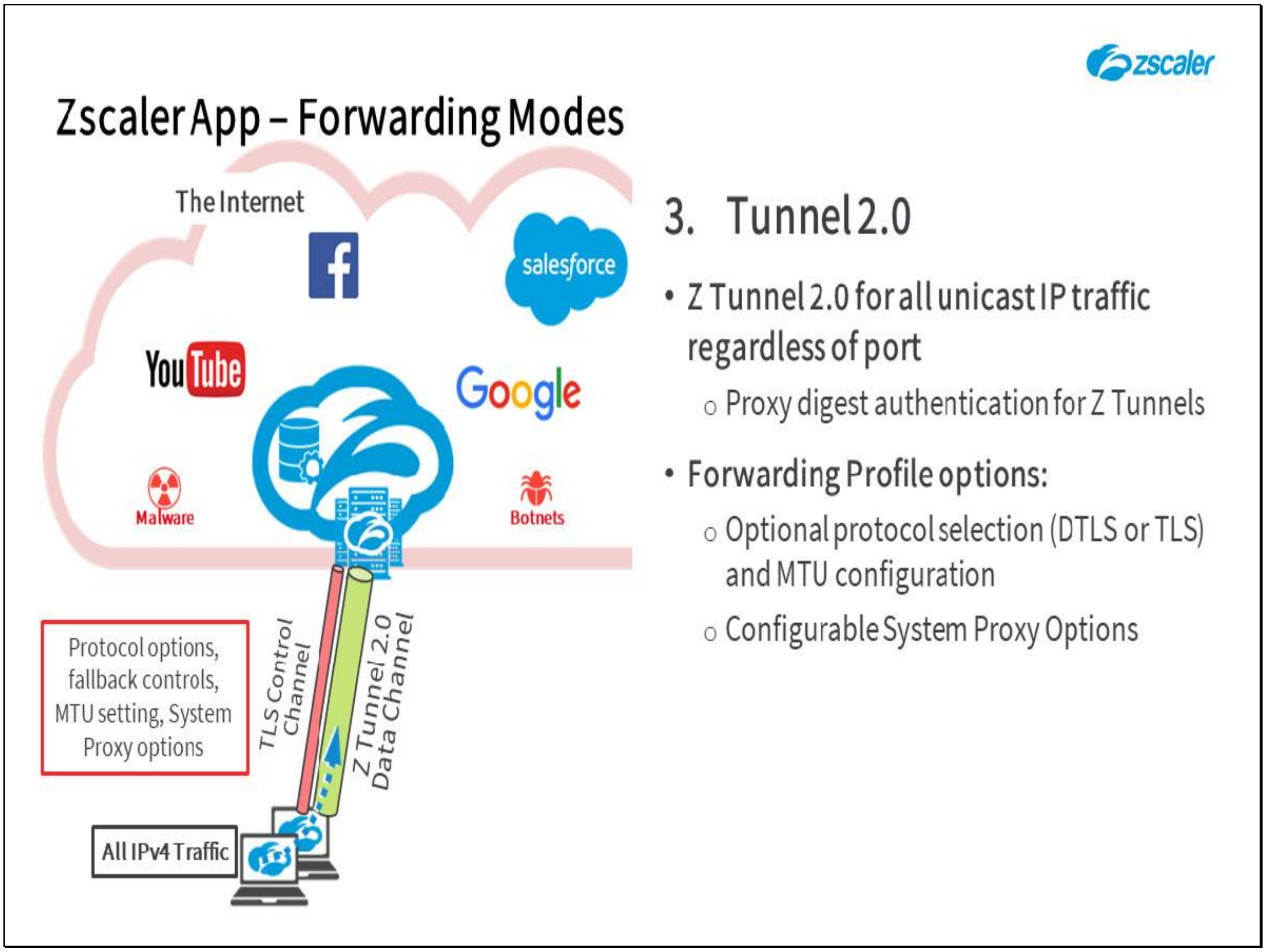
Tunnel 2.0 is only available on PCs and requires Zscaler App v2.0.1 or later

Slide notes

Note that **Tunnel 2.0** is only available on the PC platforms with the **Packet Filter Based** driver (on Windows), or the Zscaler App installed **TUN** driver (on Macs). It requires at least Zscaler App **v2.0.1**.

See the separate module on **Tunnel 2.0** for full details of this forwarding method.

Slide 23 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

Protocol options, fallback controls, MTU setting, System Proxy options

3. Tunnel 2.0

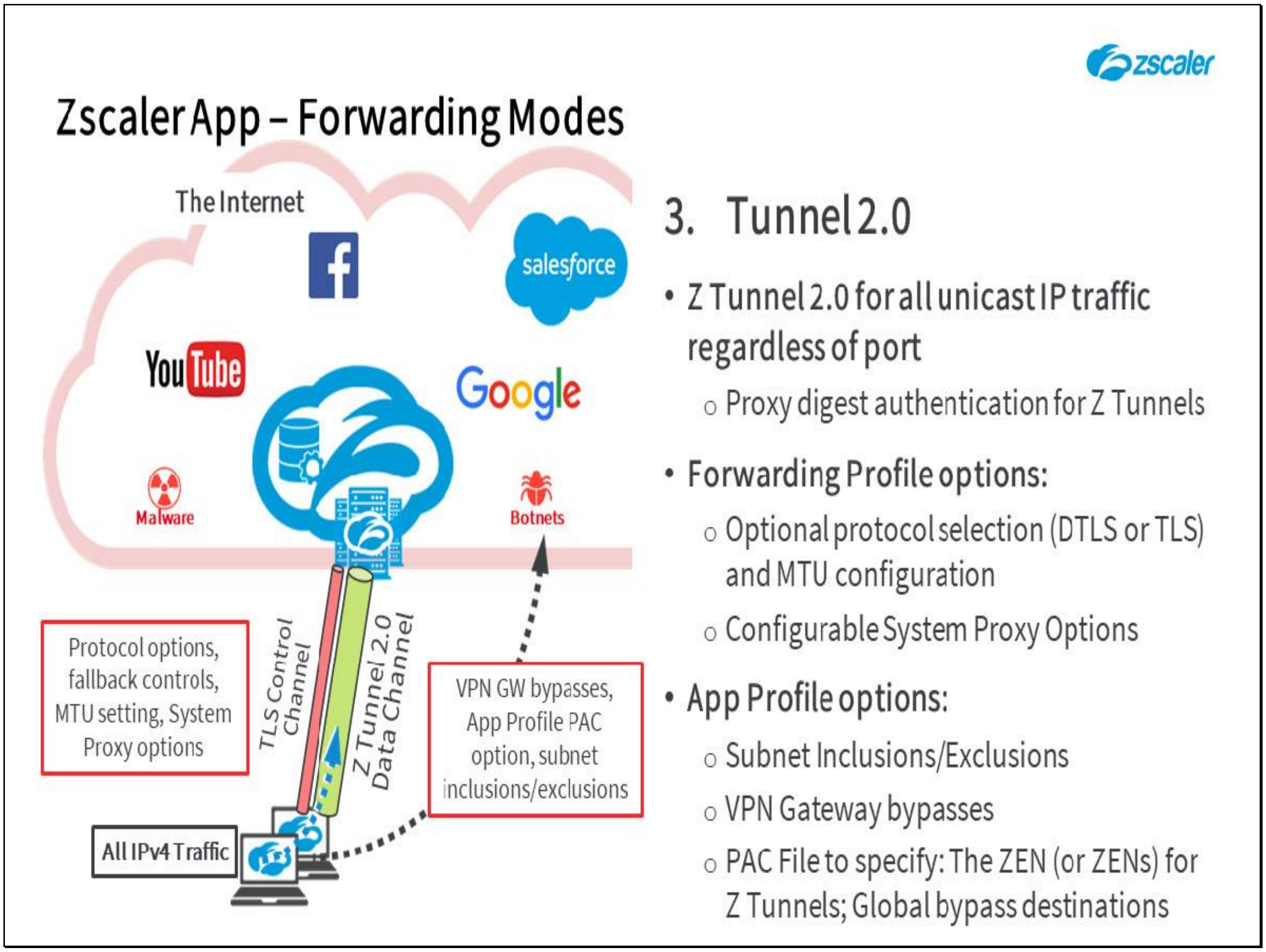
- Z Tunnel 2.0 for all unicast IP traffic regardless of port
  - Proxy digest authentication for Z Tunnels
- Forwarding Profile options:
  - Optional protocol selection (DTLS or TLS) and MTU configuration
  - Configurable System Proxy Options

Slide notes

In the **Forwarding Profile** you can configure the preferred tunneling behavior, whether to use **DTLS** or **TLS** by default, plus you can control the fall back process.

If necessary, you can also specify the MTU, although this should only be done if you see fragmentation issues using the default settings. You have the exact same Proxy configuration options as with **Tunnel 1.0**.

Slide 24 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

Protocol options, fallback controls, MTU setting, System Proxy options

VPN GW bypasses, App Profile PAC option, subnet inclusions/exclusions

3. Tunnel 2.0

- Z Tunnel 2.0 for all unicast IP traffic regardless of port
  - Proxy digest authentication for Z Tunnels
- Forwarding Profile options:
  - Optional protocol selection (DTLS or TLS) and MTU configuration
  - Configurable System Proxy Options
- App Profile options:
  - Subnet Inclusions/Exclusions
  - VPN Gateway bypasses
  - PAC File to specify: The ZEN (or ZENs) for Z Tunnels; Global bypass destinations

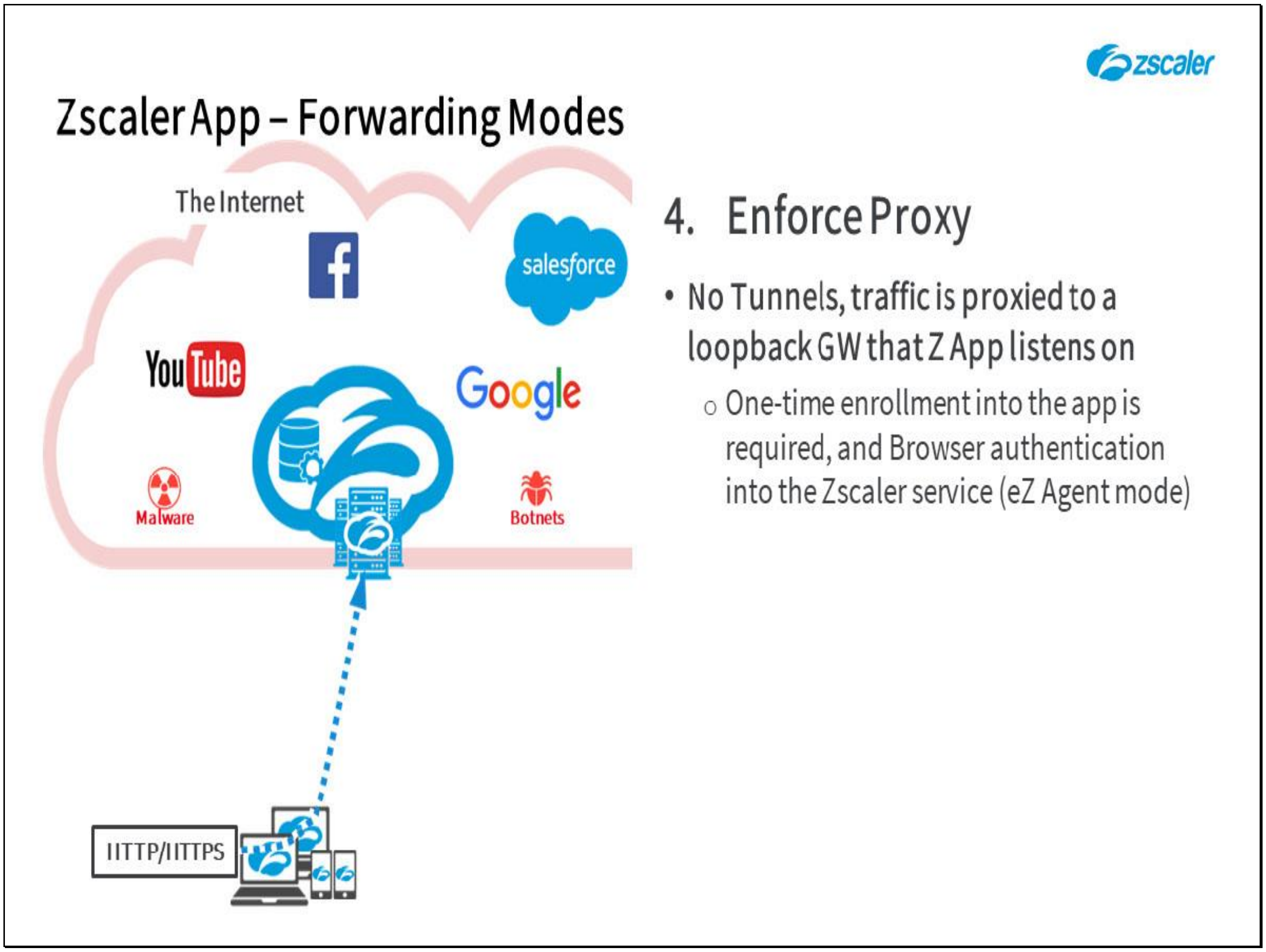
Slide notes

In the **App Profile** settings, in addition to the VPN gateway bypass option and the **App Profile** PAC file, you can also specify **Tunnel 2.0** network **Inclusions** and **Exclusions**. The order that these are applied is:

1. First the **VPN GW** bypasses;
2. Then the **Tunnel 2.0 Inclusions**/**Exclusions**;
3. And lastly the **App Profile** PAC file bypasses. This gives you a great deal of granularity in how you chose to forward, or bypass traffic based on the destination.

Although, note that if you plan to migrate from **Tunnel 1.0** to **Tunnel 2.0**, you will need to carefully plan the migration of your bypasses into the network **Inclusion**/**Exclusion** configuration.

Slide 25 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

4. Enforce Proxy

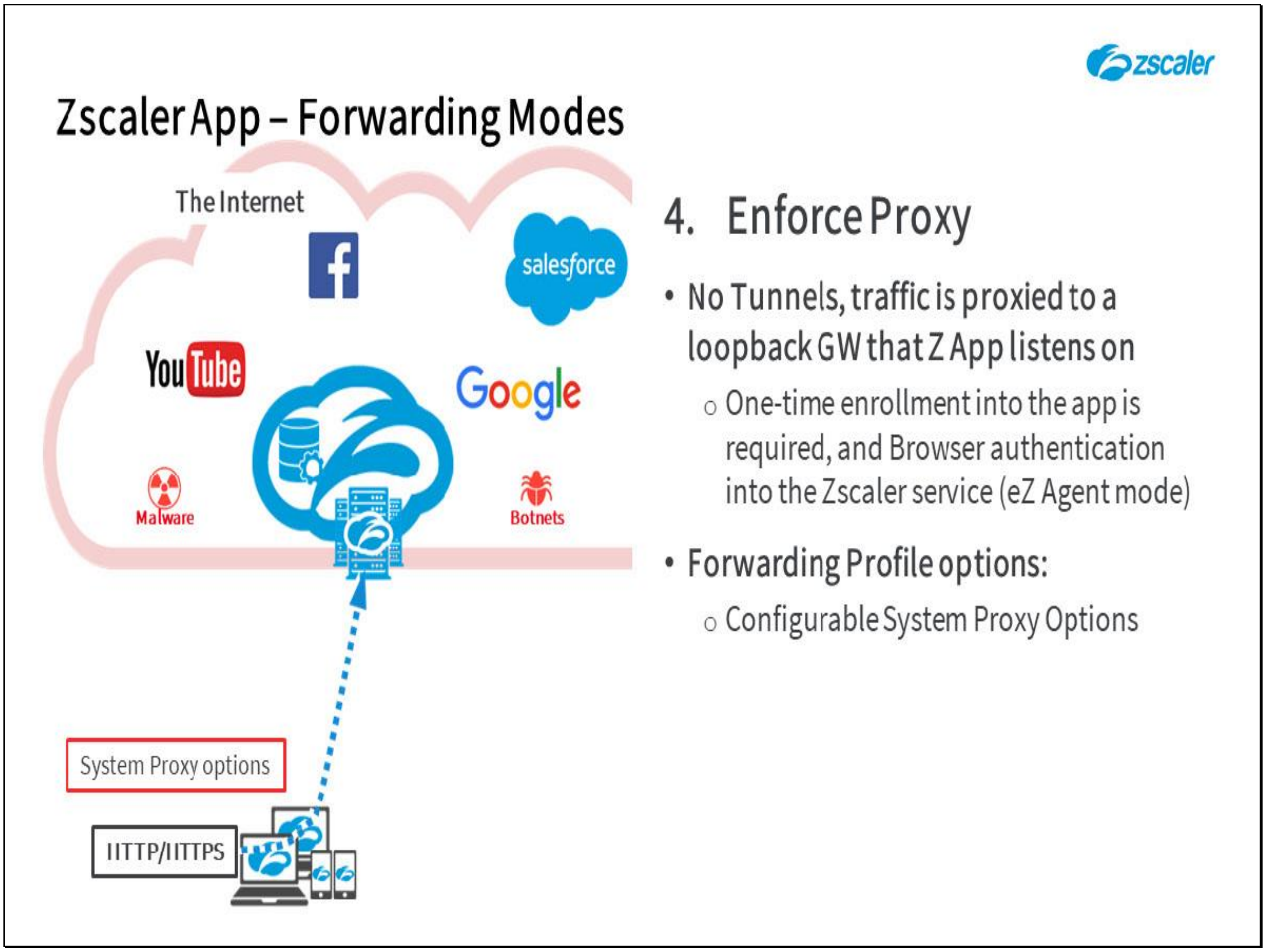
- No Tunnels, traffic is proxied to a loopback GW that Z App listens on
  - One-time enrollment into the app is required, and Browser authentication into the Zscaler service (eZ Agent mode)

Slide notes

4. The fourth forwarding option is the **Enforce Proxy** option, where the app enforces either the PAC file configured on the browser, or a specified PAC file; no Z Tunnels are used. If the device user re-configures the proxy settings, the app will immediately change them back and apply the specified PAC file.

   A one-time enrollment into the app is required and as this forwarding option equates to the legacy eZ Agent mode, authentication into the Zscaler Internet Access service in the browser will also be enforced. The requirement for a further authentication through the browser on connection to Zscaler can be suppressed with the right combination of Zscaler App install options (**--strictEnforcement**, and **--policyToken** options).

Slide 26 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

4. Enforce Proxy

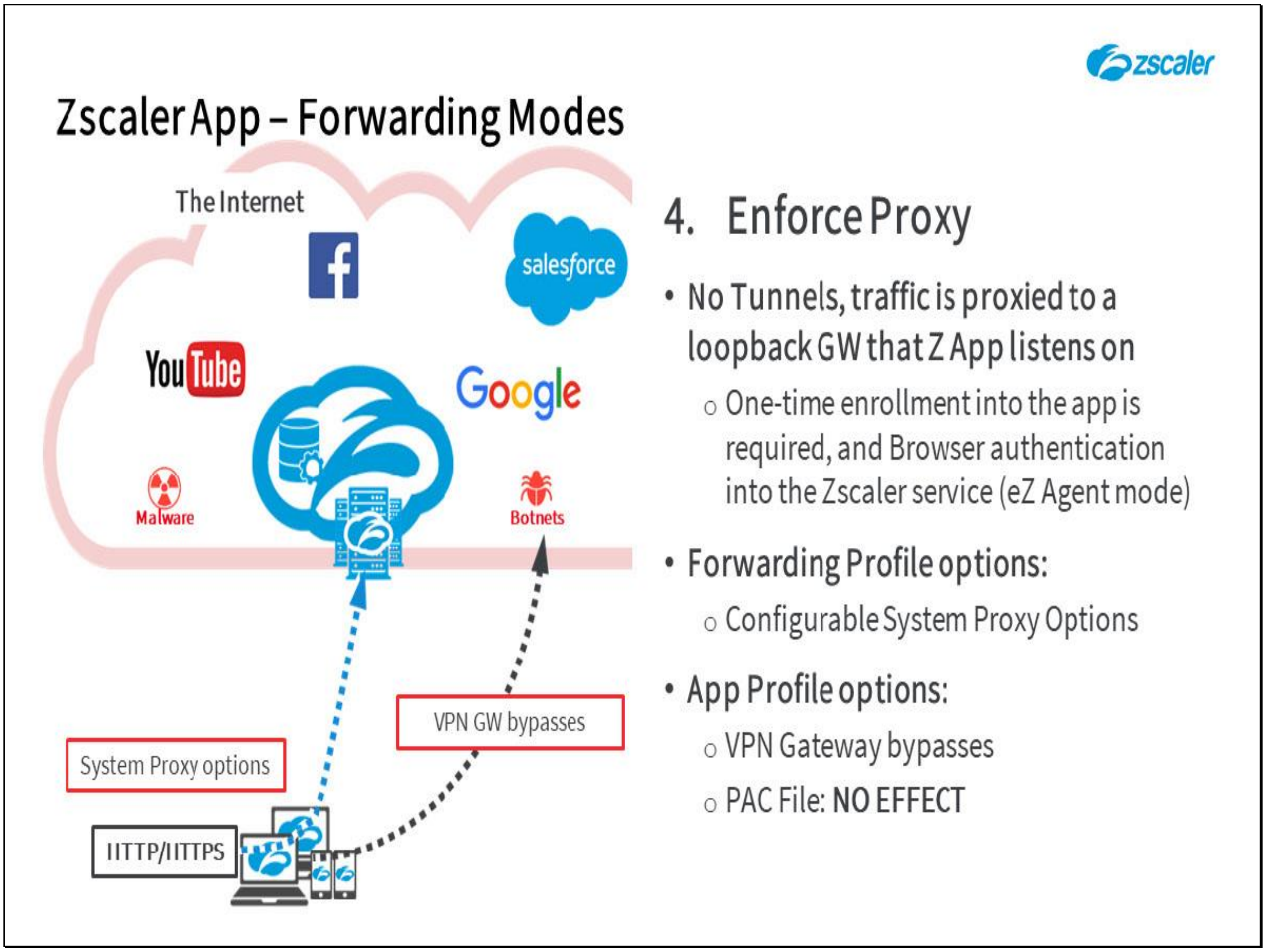
- No Tunnels, traffic is proxied to a loopback GW that Z App listens on
  - One-time enrollment into the app is required, and Browser authentication into the Zscaler service (eZ Agent mode)
- Forwarding Profile options:
  - Configurable System Proxy Options

Slide notes

Traffic to be forwarded to Zscaler, and traffic to be bypassed can be defined in the applied PAC file. With the **Enforce** option, the PAC file specified in the **Forwarding Profile** will be applied. The same Proxy settings as with the **Tunnel** method are available:

- Automatically detected;
- Configured using a script;
- Specified for the LAN;
- Applied by a GPO update;
- Or any combination of these options.

Slide 27 - Zscaler App – Forwarding Modes



zscaler

Zscaler App – Forwarding Modes

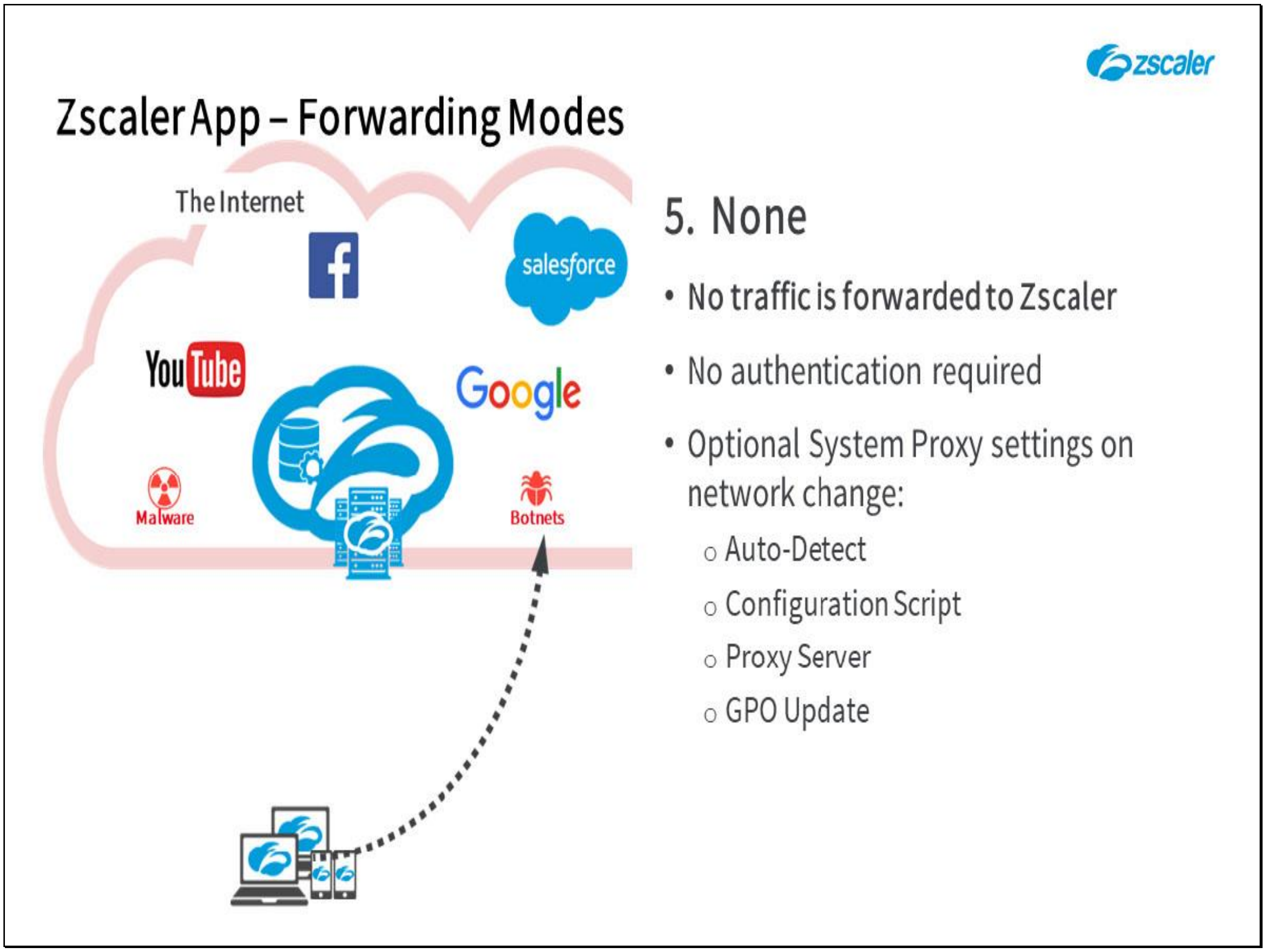
4. Enforce Proxy

- No Tunnels, traffic is proxied to a loopback GW that Z App listens on
  - One-time enrollment into the app is required, and Browser authentication into the Zscaler service (eZ Agent mode)
- Forwarding Profile options:
  - Configurable System Proxy Options
- App Profile options:
  - VPN Gateway bypasses
  - PAC File: **NO EFFECT**

Slide notes

Note that in this mode the App simply enforces the specified PAC file on the system but takes no part in the forwarding of traffic, this means that the PAC file applied in the **App Profile** has NO EFFECT in this mode. You still have the option to specify those VPN gateway bypasses, however.

Slide 28 - Zscaler App – Forwarding Modes



Zscaler App – Forwarding Modes

5. None

- No traffic is forwarded to Zscaler
- No authentication required
- Optional System Proxy settings on network change:
  - Auto-Detect
  - Configuration Script
  - Proxy Server
  - GPO Update

Slide notes

5. The final forwarding configuration is the **None** option, where the Zscaler App forwards no traffic to Zscaler at all. You have the option to never apply a proxy configuration, or to apply one on a network change. If the network changes, the same Proxy settings as with the **Tunnel** method are available: Automatically detected; configured using a script; use a local Proxy server on the LAN; apply it using a GPO update; or any combination of these options.

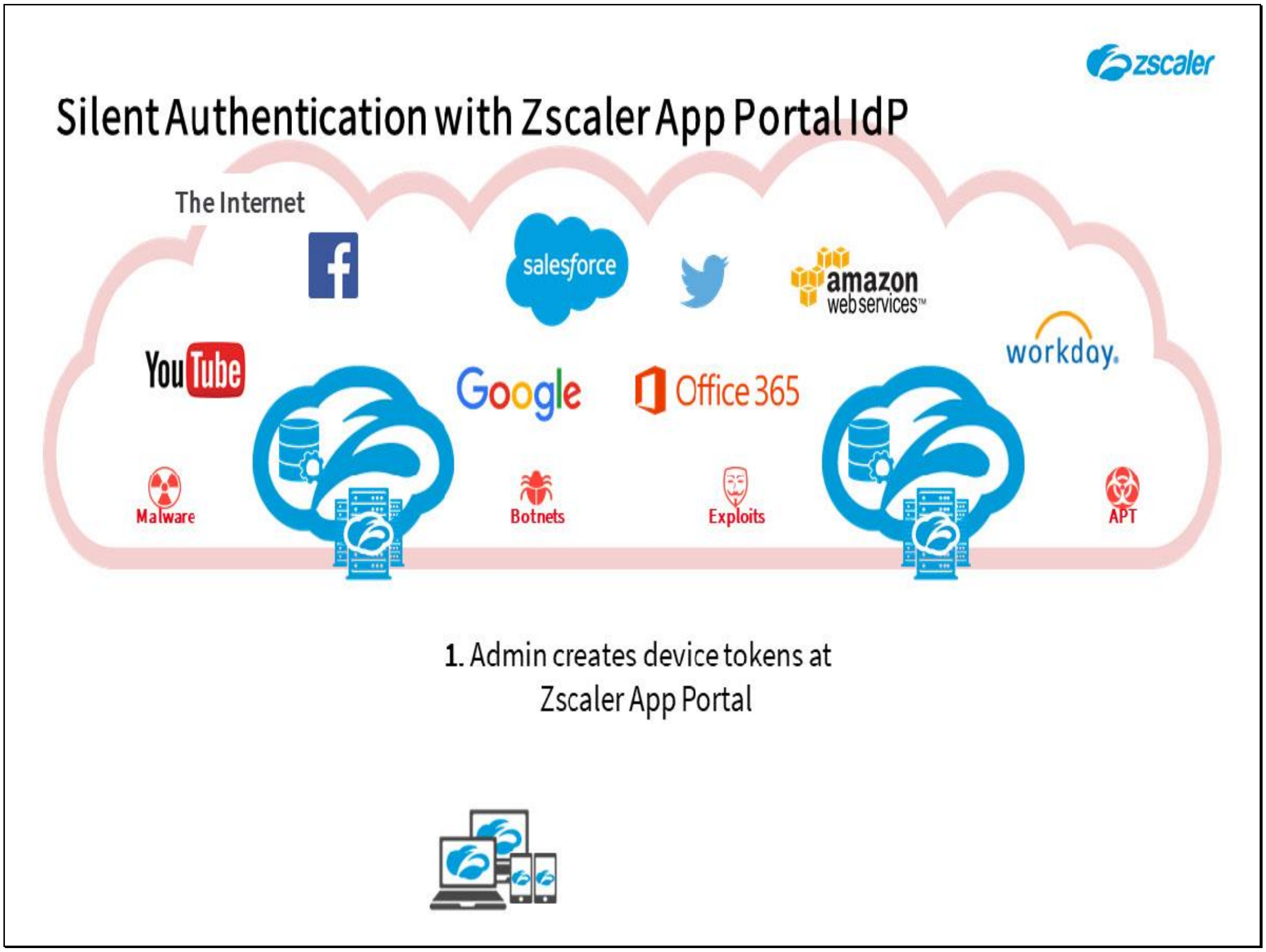
Slide 29 - Zscaler App – Silent Authentication with Zscaler App IdP

Z App – ZIA: Silent Authentication with Zscaler App IdP

Slide notes

The next topic that we will cover is an overview of the process for end user silent authentication using the Zscaler App IdP.

Slide 30 - Silent Authentication with Zscaler Mobile Portal IdP



Silent Authentication with Zscaler App Portal IdP

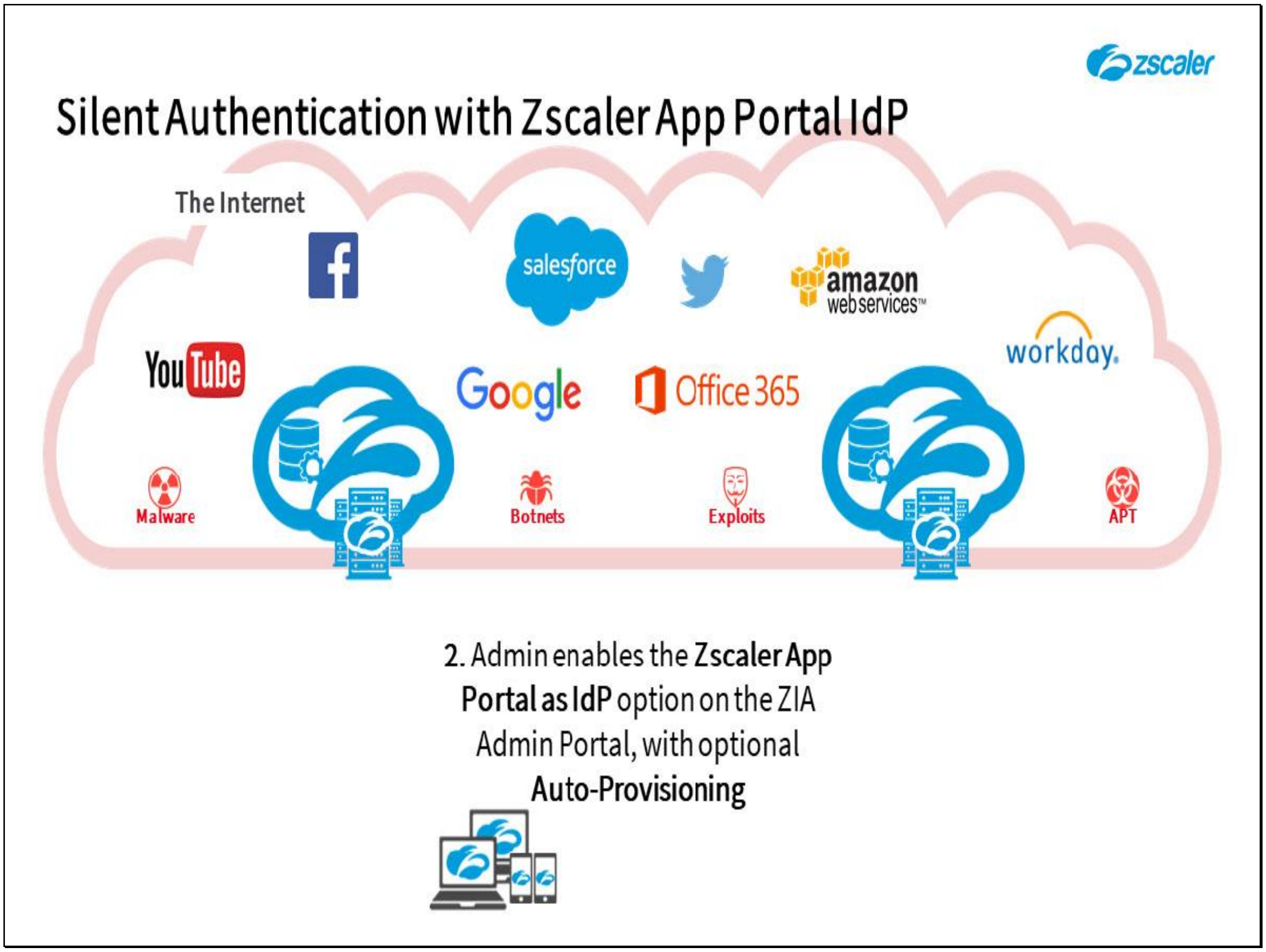
1. Admin creates device tokens at Zscaler App Portal

Slide notes

The Zscaler App Portal can also be used as a SAML Identity Provider to facilitate a silent user authentication into the Zscaler App. The steps to configuring this are:

1. Create device tokens at the Zscaler App Portal on the **Administration > Zscaler App IdP** page. You will need to copy the token values for use when installing the app. Note that currently you may create a maximum of 8 tokens.

Slide 31 - Silent Authentication with Zscaler Mobile Portal IdP



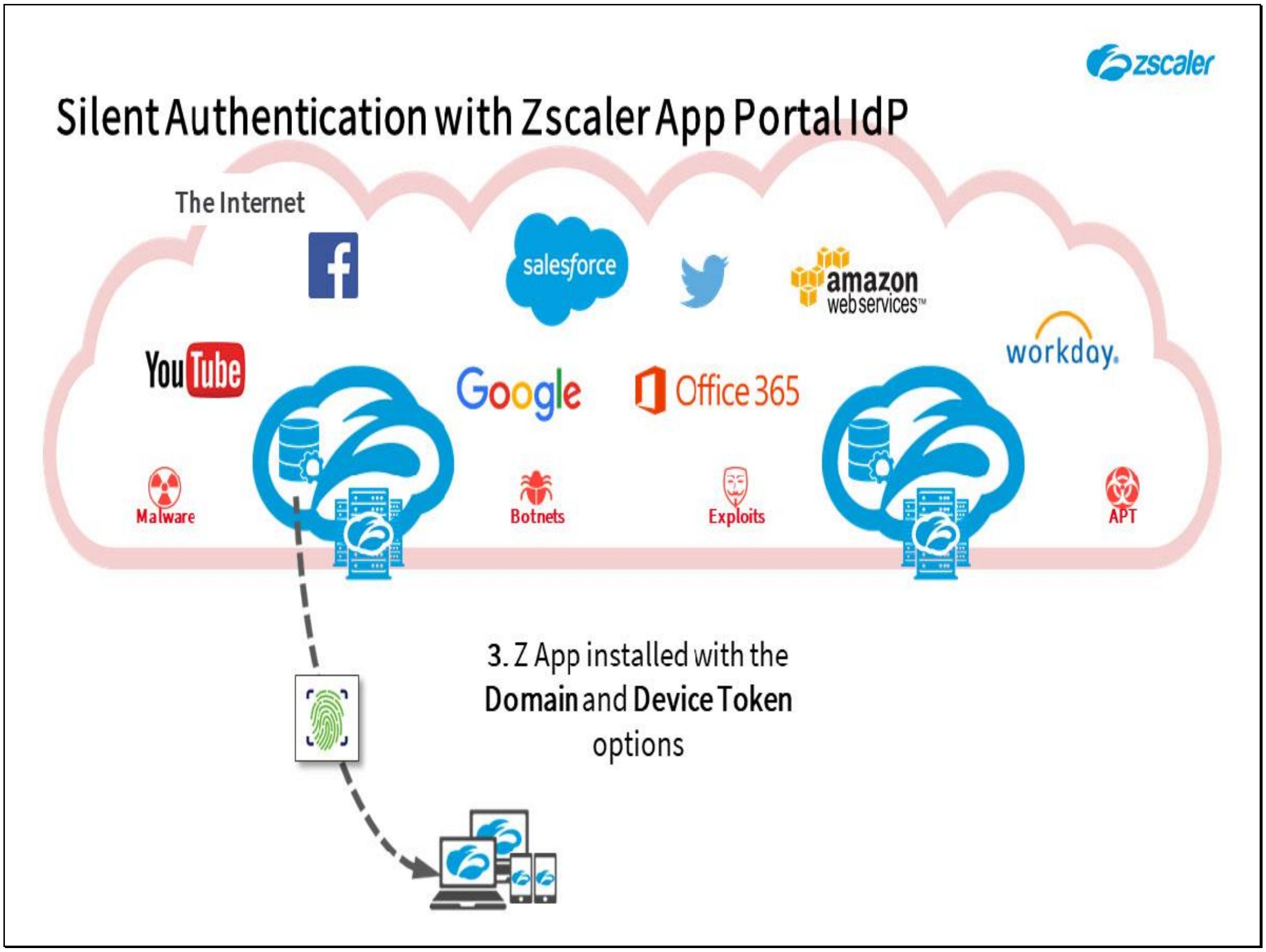
Silent Authentication with Zscaler App Portal IdP

2. Admin enables the **Zscaler App Portal as IdP** option on the ZIA Admin Portal, with optional **Auto-Provisioning**

Slide notes

2. The administrator must use the **Add Zscaler App Portal as IdP** option in the ZIA Admin Portal under **Administration > Authentication Settings > IDENTITY PROVIDERS**, to add the Zscaler App Portal as an IdP option, either with or without **SAML Auto-Provisioning**.

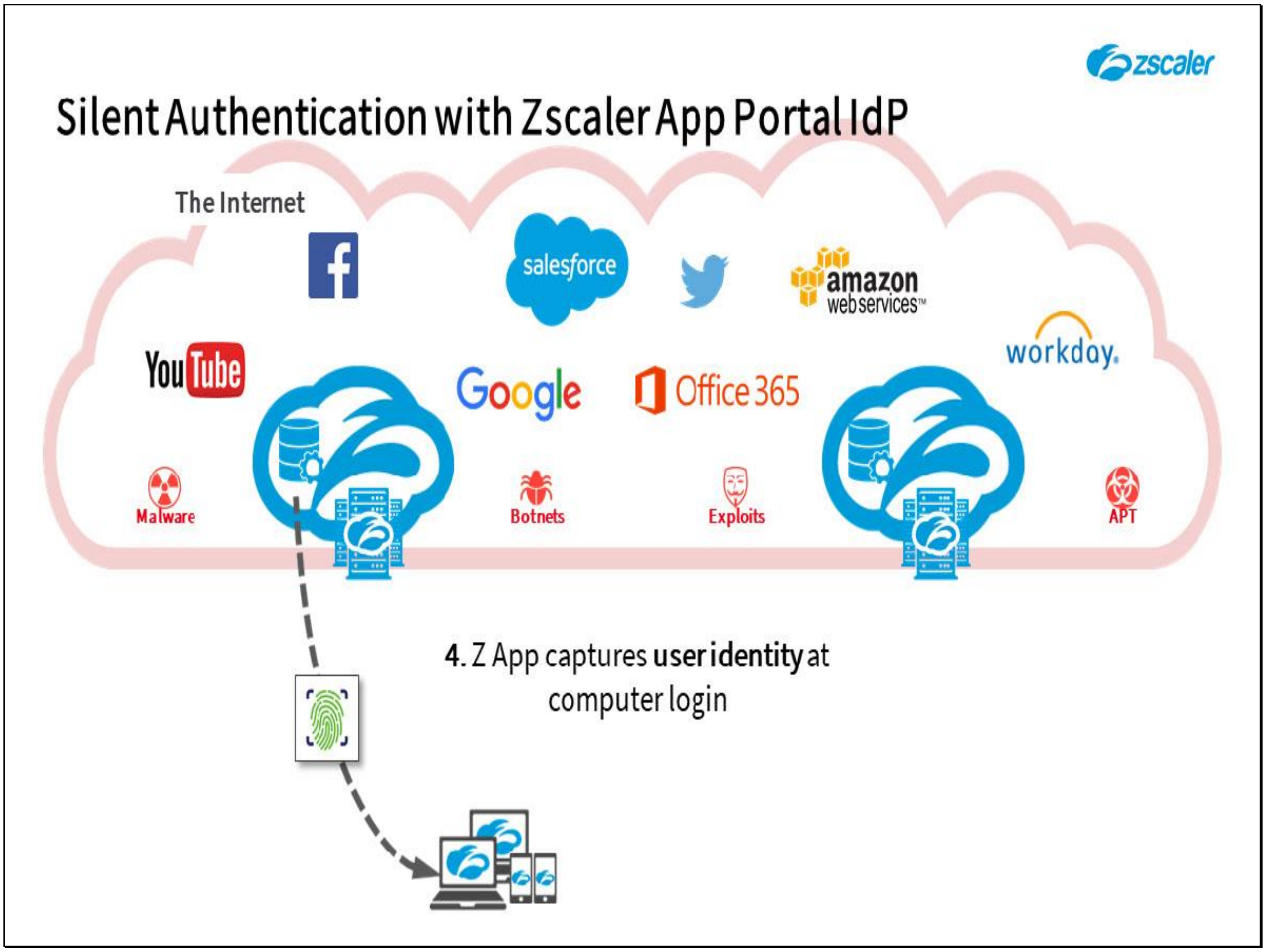
Slide 32 - Silent Authentication with Zscaler Mobile Portal IdP



Slide notes

3. The App must be installed with both the **--deviceToken**, and the **--userDomain** command line options.

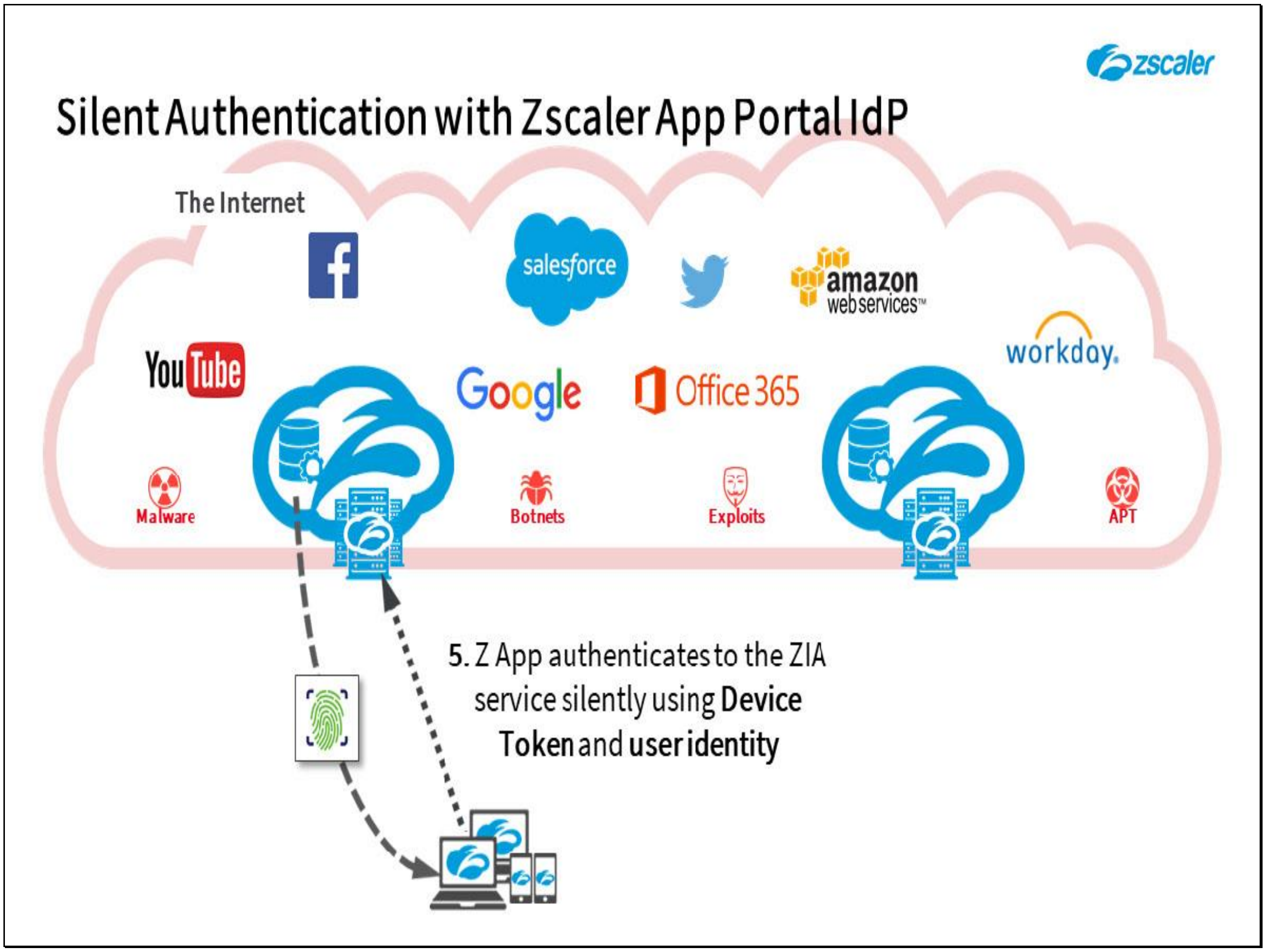
Slide 33 - Silent Authentication with Zscaler Mobile Portal IdP



Slide notes

4. Once installed, the App captures the user’s identity, from the device login.

Slide 34 - Silent Authentication with Zscaler Mobile Portal IdP

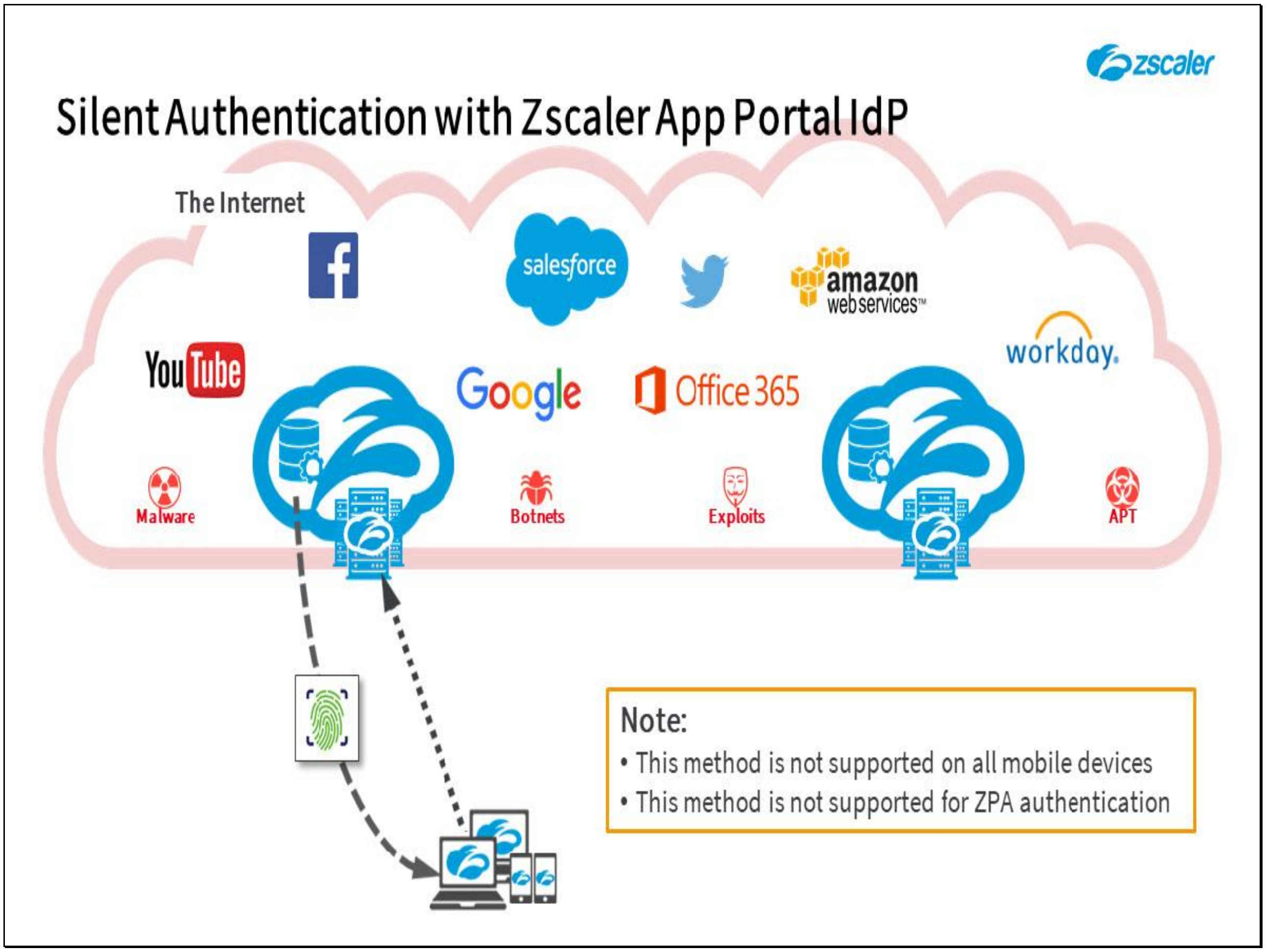


5. Z App authenticates to the ZIA service silently using **Device Token** and **user identity**

Slide notes

5. Then authenticates the user to the Zscaler IdP silently, using the **user identity** captured at device login, and the **Device Token** provisioned during the installation. The user does not need to respond to any Zscaler App prompts or provide a password in order to enroll to the Internet Security service.

Slide 35 - Silent Authentication with Zscaler Zscaler App Portal IdP



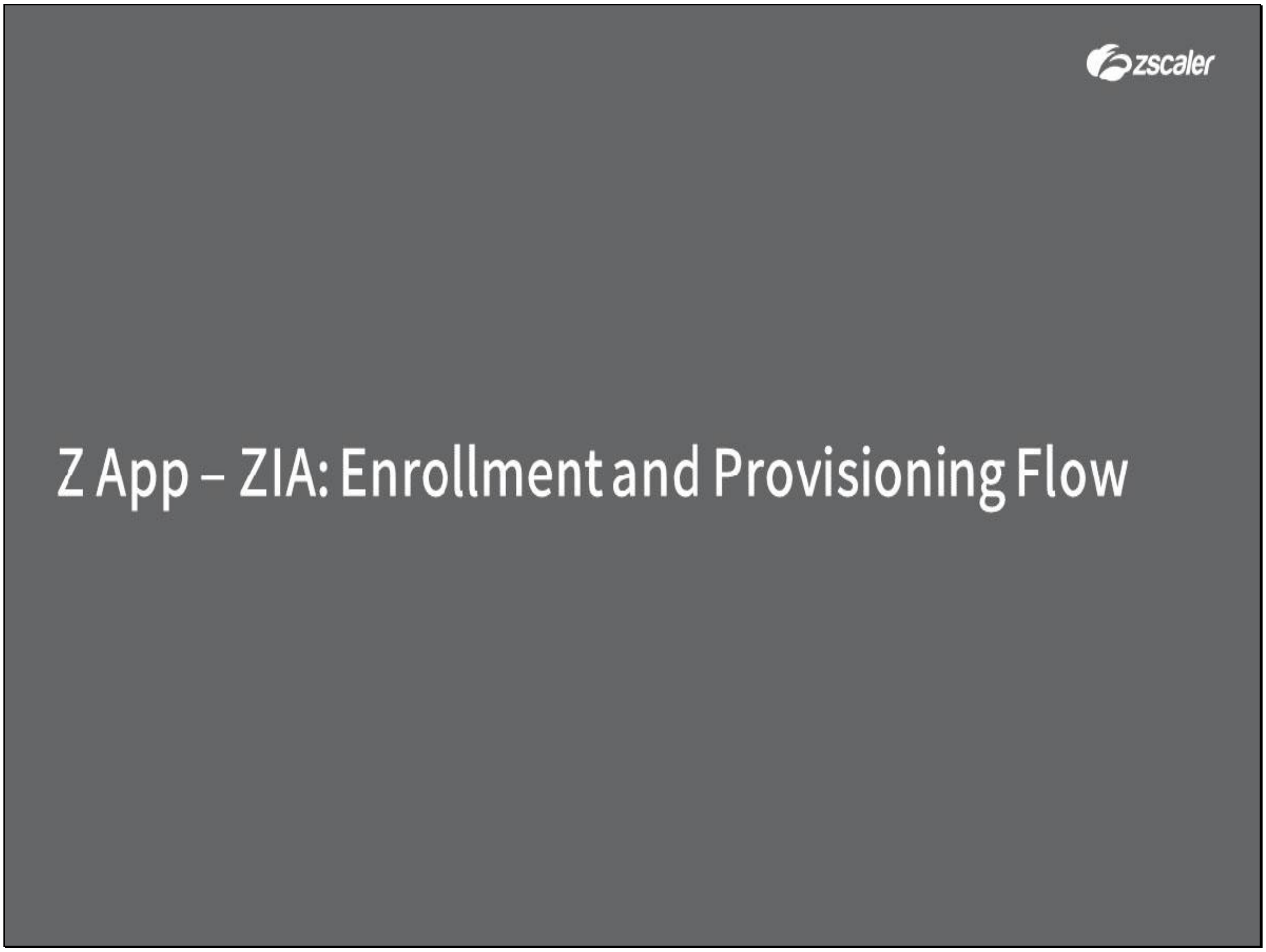
Note:

- This method is not supported on all mobile devices
- This method is not supported for ZPA authentication

Slide notes

Note that this authentication option is not supported on all mobile platforms, although it can be used with managed iOS devices. Nor is this method supported for authentication to the ZPA service.

Slide 36 - Zscaler App – Provisioning and Enrollment Flow



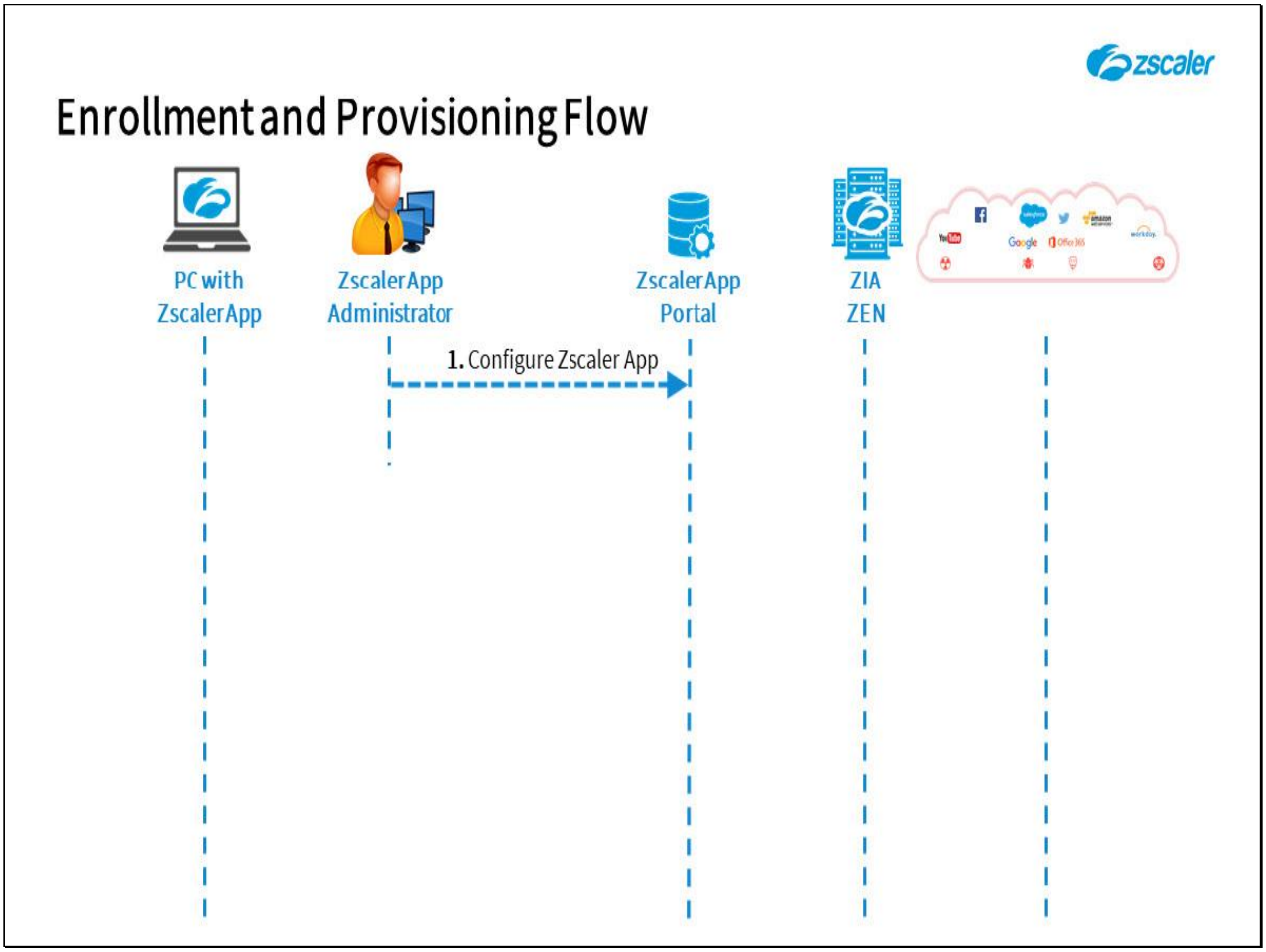
zscaler

Z App – ZIA: Enrollment and Provisioning Flow

Slide notes

The final topic that we will cover is the provisioning and enrollment flow for the Zscaler App.

Slide 37 - Provisioning and Enrollment Flow



Enrollment and Provisioning Flow

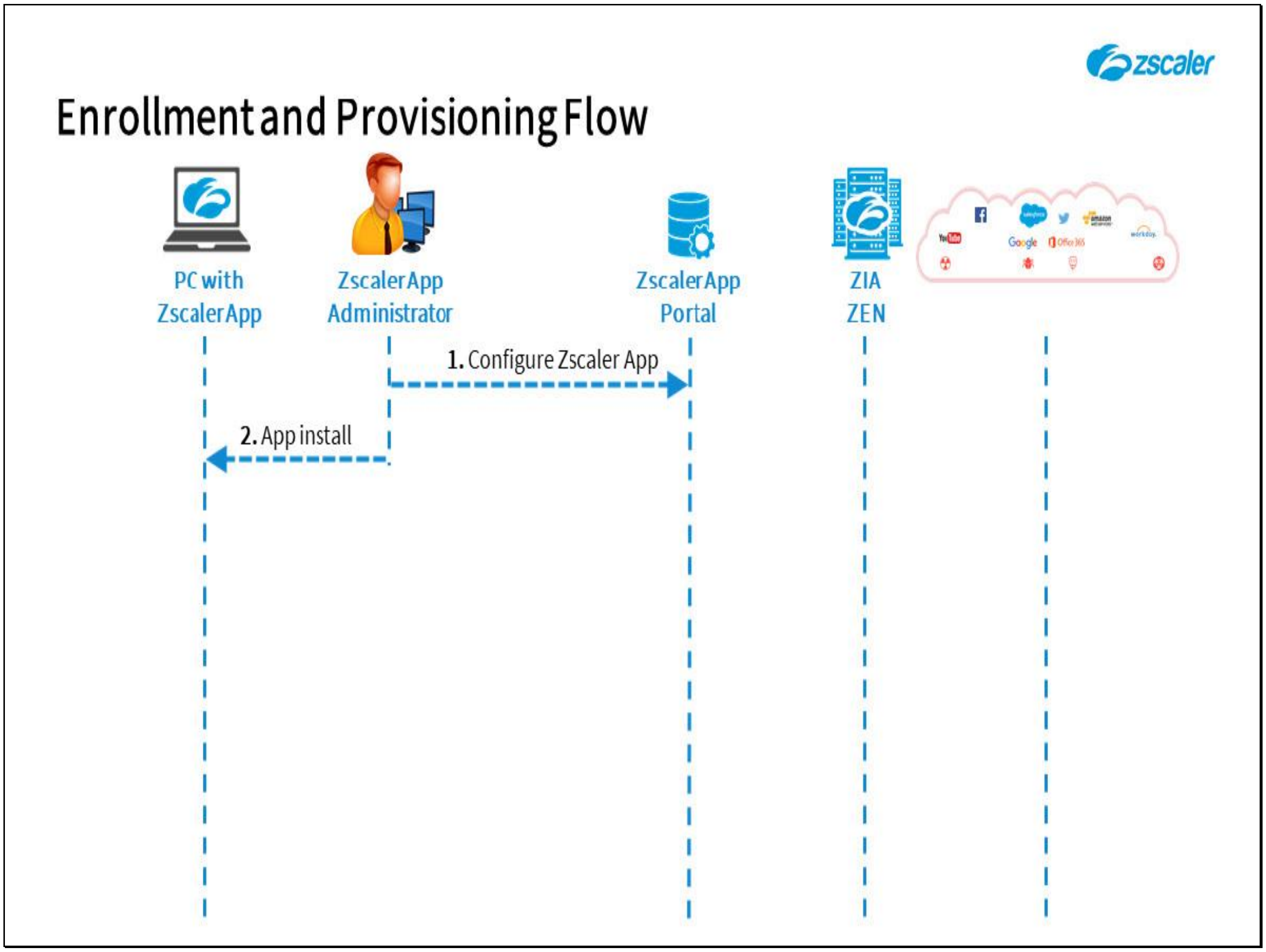
Slide notes

The enrollment and provisioning flow for the Zscaler App used for the ZIA service is as follows:

Step 1: An administrator configures appropriate app settings for the users or groups in **App Profiles**, and optionally one or more **Forwarding Profiles**. There are additional miscellaneous configuration options, such as:

- **Zscaler App Notifications**;
- **Trusted Networks**;
- **Zscaler App Support**;
- **User Agent**;
- And the **Zscaler App IdP** configurations.

Slide 38 - Provisioning and Enrollment Flow

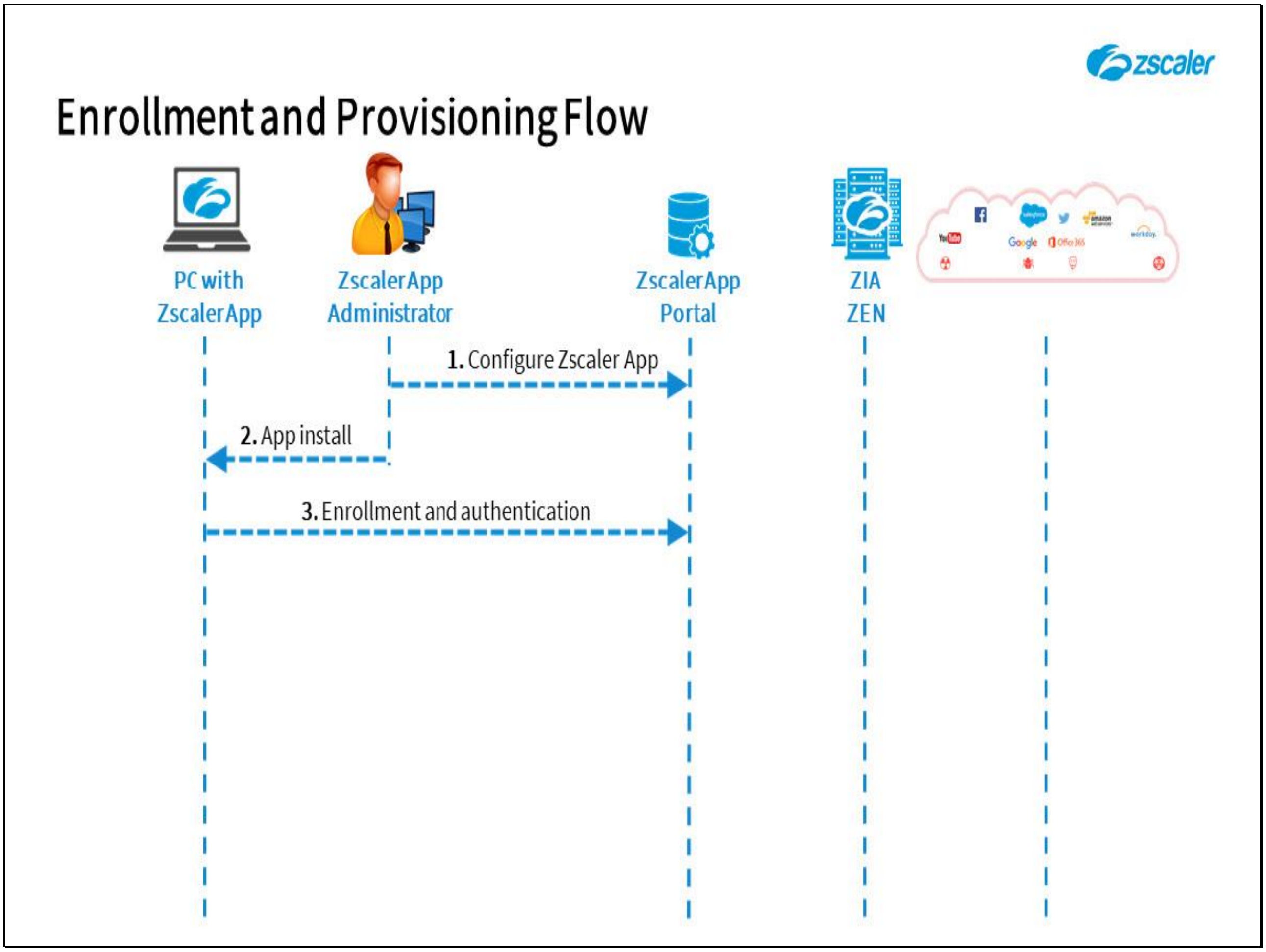


Enrollment and Provisioning Flow

Slide notes

Step 2: The Admin ensures the distribution and installation of the app to those users that require it. This is often done by silently pushing the app to those devices that need it using AD, or for mobile devices, an MDM solution.

Slide 39 - Provisioning and Enrollment Flow

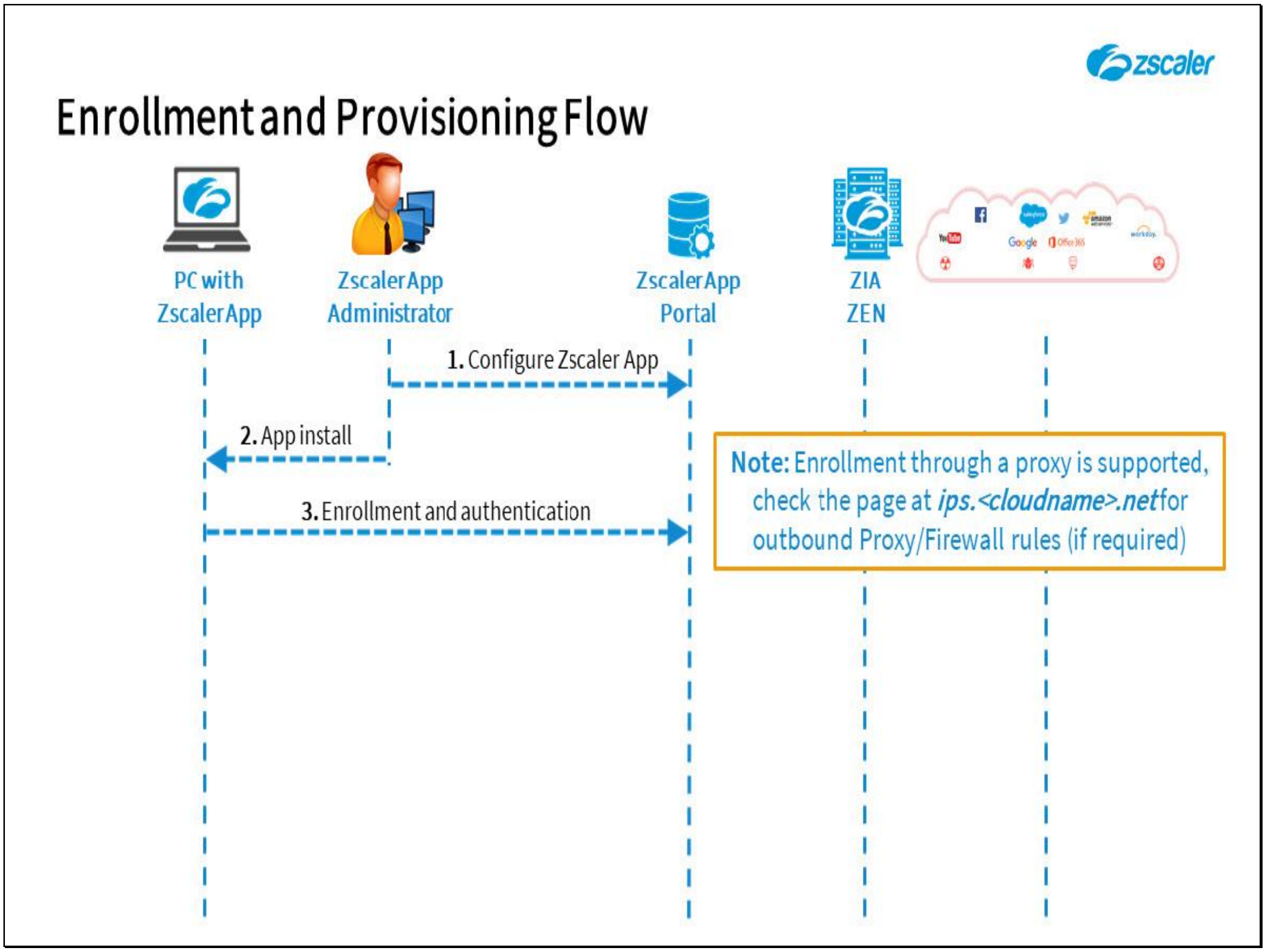


Enrollment and Provisioning Flow

Slide notes

Step 3: The device user is prompted to enroll through the app. The need for user interaction here can be suppressed, with a silent enrollment based on the device login. When auto-enrollment is enabled, the app waits for the network to be available before starting the auto-enrollment process.

Slide 40 - Provisioning and Enrollment Flow



Enrollment and Provisioning Flow

PC with ZscalerApp

ZscalerApp Administrator

ZscalerApp Portal

ZIA ZEN

1. Configure Zscaler App

2. App install

3. Enrollment and authentication

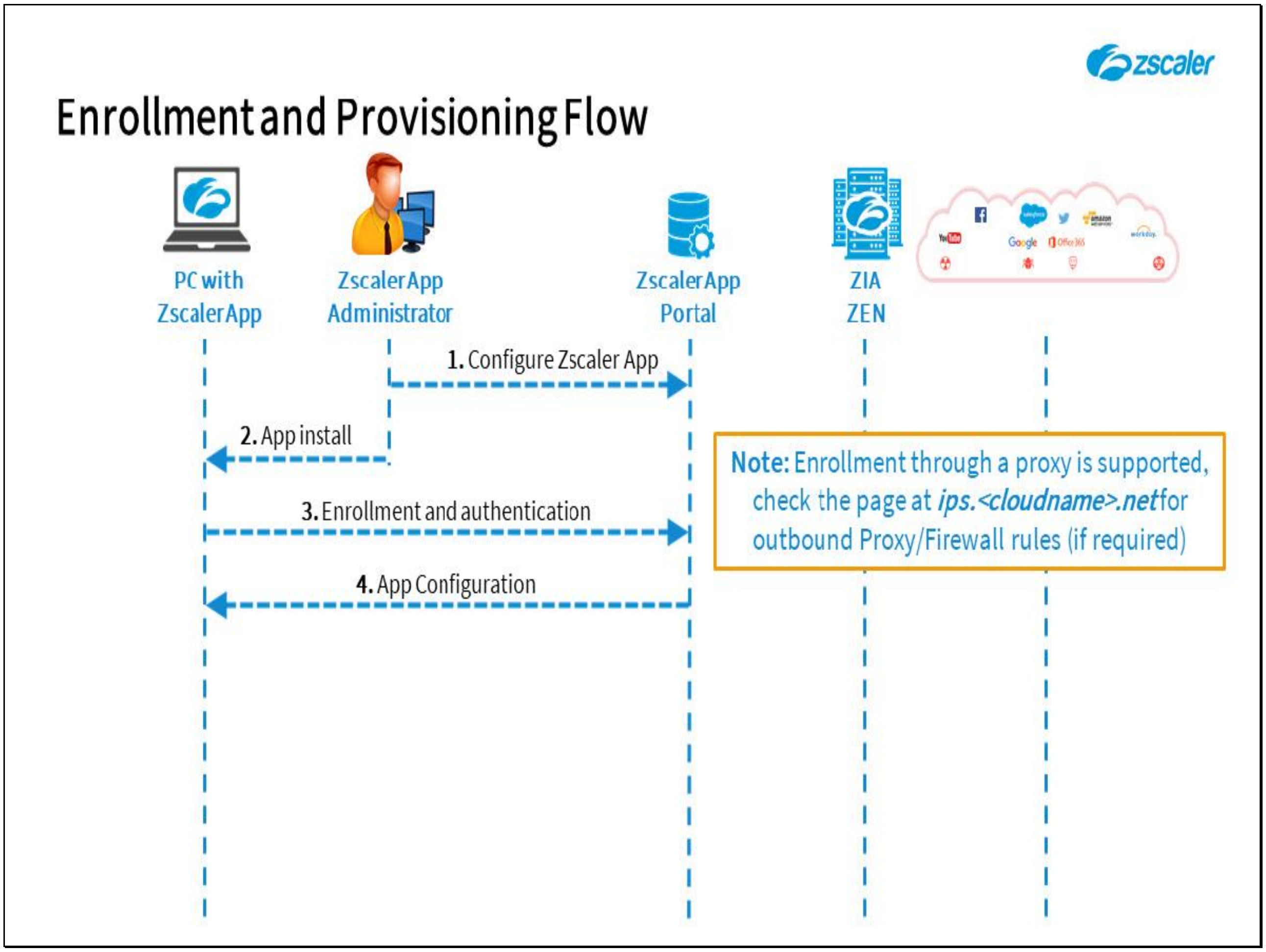
Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required)

Slide notes

Note that, the app tries to enroll direct first, if that fails it then tries using the system proxy settings. For enrollment through a Proxy, or from behind a Firewall there are some destinations that may need to be opened in the outbound direction, including authentication bypasses.

Check the page at **ips.< cloudname >.net** for details (for example **ips.zscalertwo.net**).

Slide 41 - Provisioning and Enrollment Flow



zscaler

Enrollment and Provisioning Flow

PC with ZscalerApp

ZscalerApp Administrator

ZscalerApp Portal

ZIA ZEN

1. Configure Zscaler App

2. App install

3. Enrollment and authentication

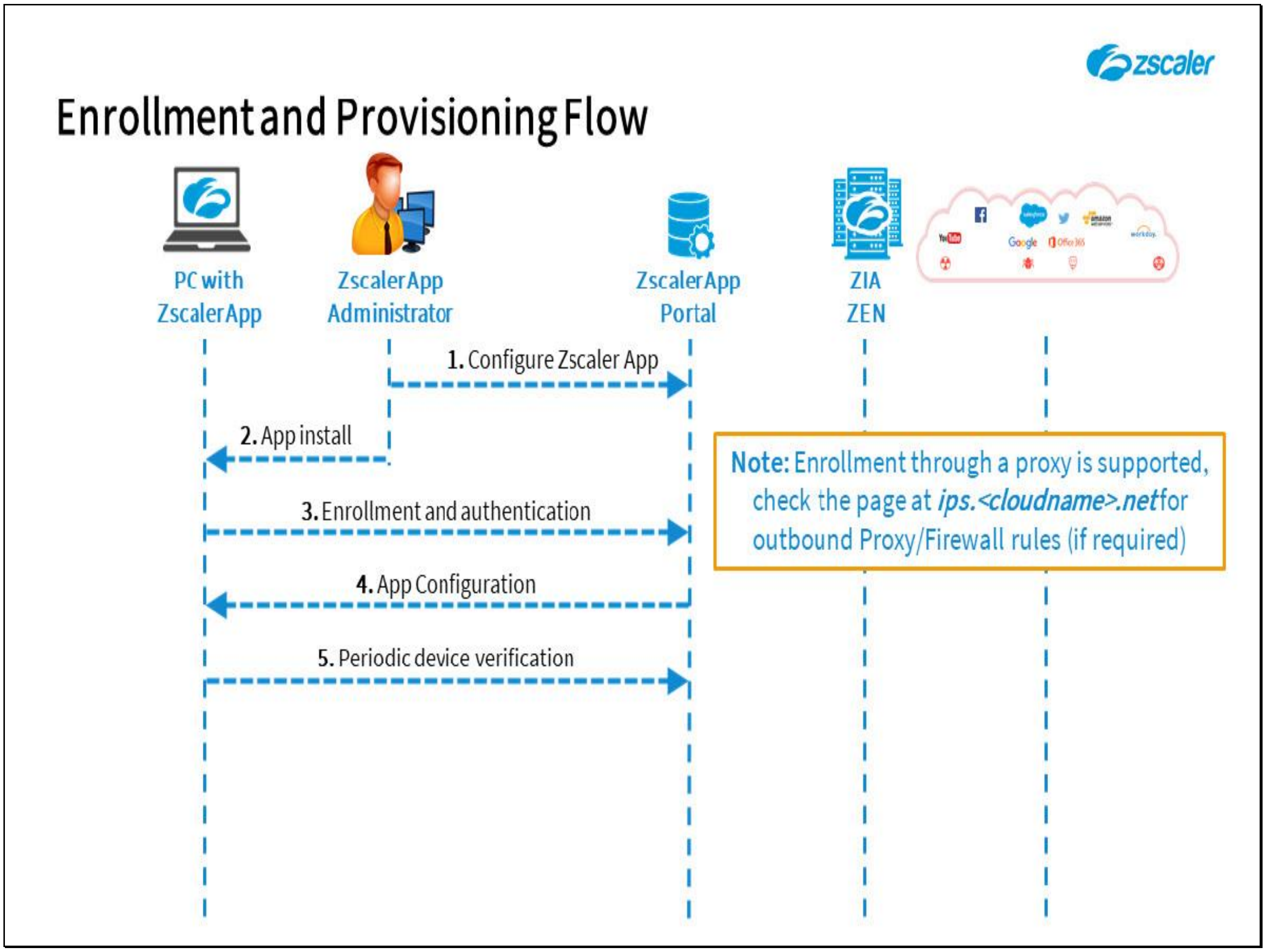
4. App Configuration

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required)

Slide notes

Step 4: On a successful enrollment, the app is provisioned and configured by the matching profiles, this includes the provisioning of the digest credentials required to establish the Z Tunnels.

Slide 42 - Provisioning and Enrollment Flow



Enrollment and Provisioning Flow

1. Configure Zscaler App
2. App install
3. Enrollment and authentication
4. App Configuration
5. Periodic device verification

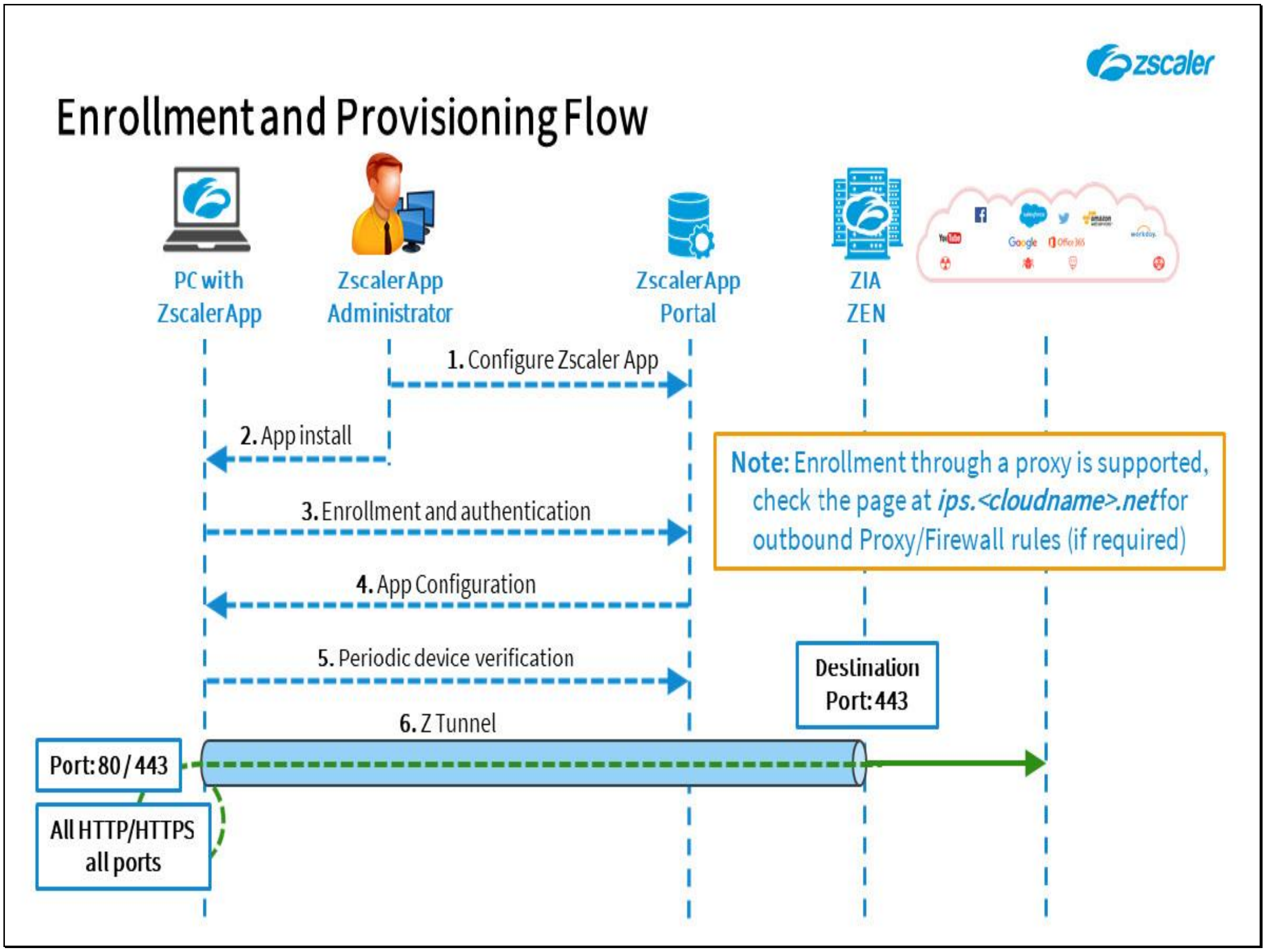
Note: Enrollment through a proxy is supported, check the page at ***ips.<cloudname>.net***for outbound Proxy/Firewall rules (if required)

Slide notes

Step 5: The app sends device information to Zscaler that includes a fingerprint of the device for security and reporting purposes.

The App subsequently checks in: Every 15 minutes to check for **App Profile** and **Forwarding Profile** PAC file updates; every 60 minutes for profile/policy updates and to refresh the device fingerprint; and every 2 hours for new SW. The user can also manually force a check in for Policy or PAC file updates from within the app.

Slide 43 - Provisioning and Enrollment Flow



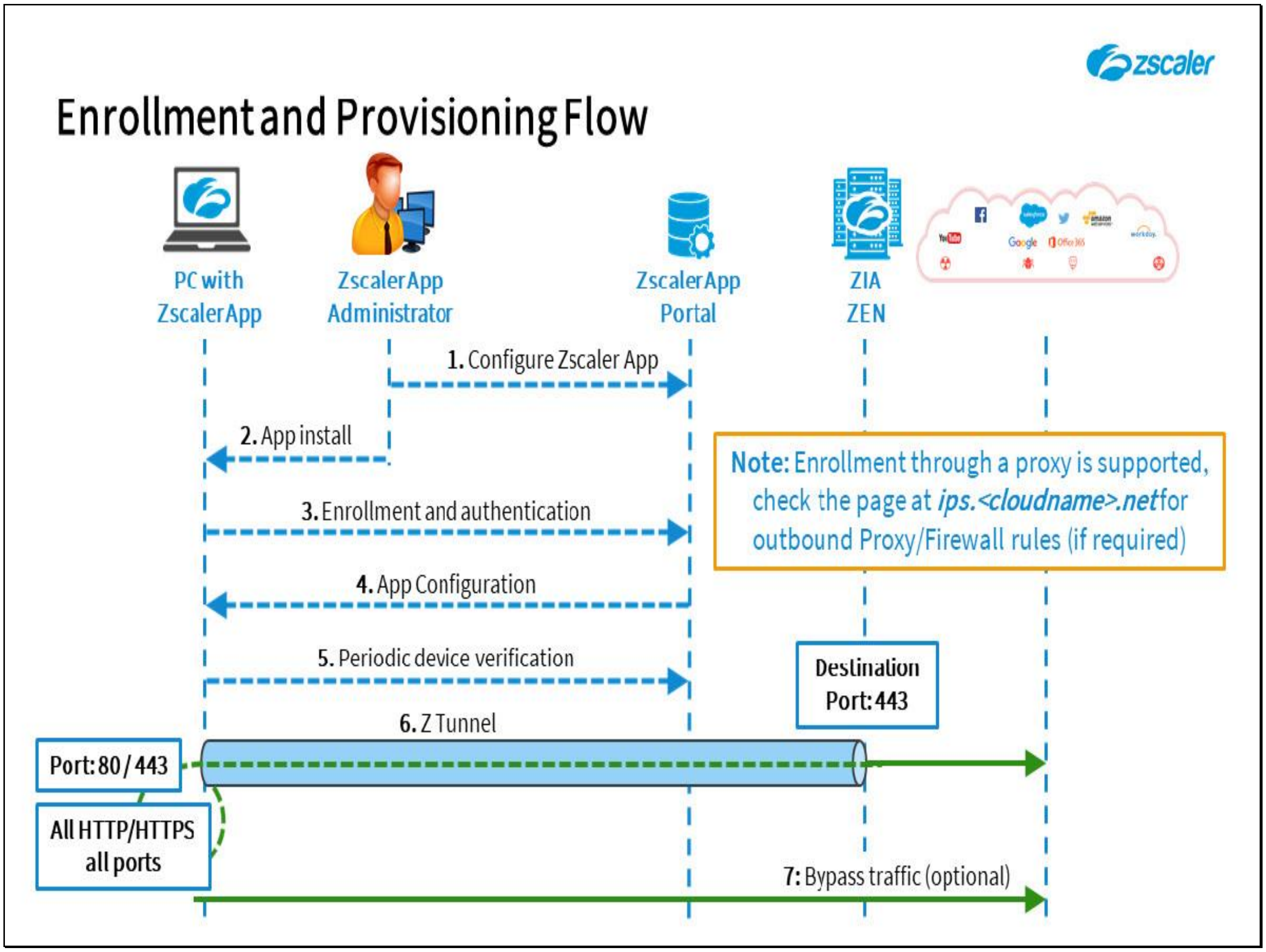
Enrollment and Provisioning Flow

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required)

Slide notes

Step 6: Traffic from the client device will be tunneled or proxied depending on the forwarding model defined by the applied **Forwarding Profile**. If Z Tunnels are required, they will be established as necessary on destination port 443 to the local, or to a specified ZEN, and authenticated using the digest credentials provided to the app at step 4.

Slide 44 - Provisioning and Enrollment Flow



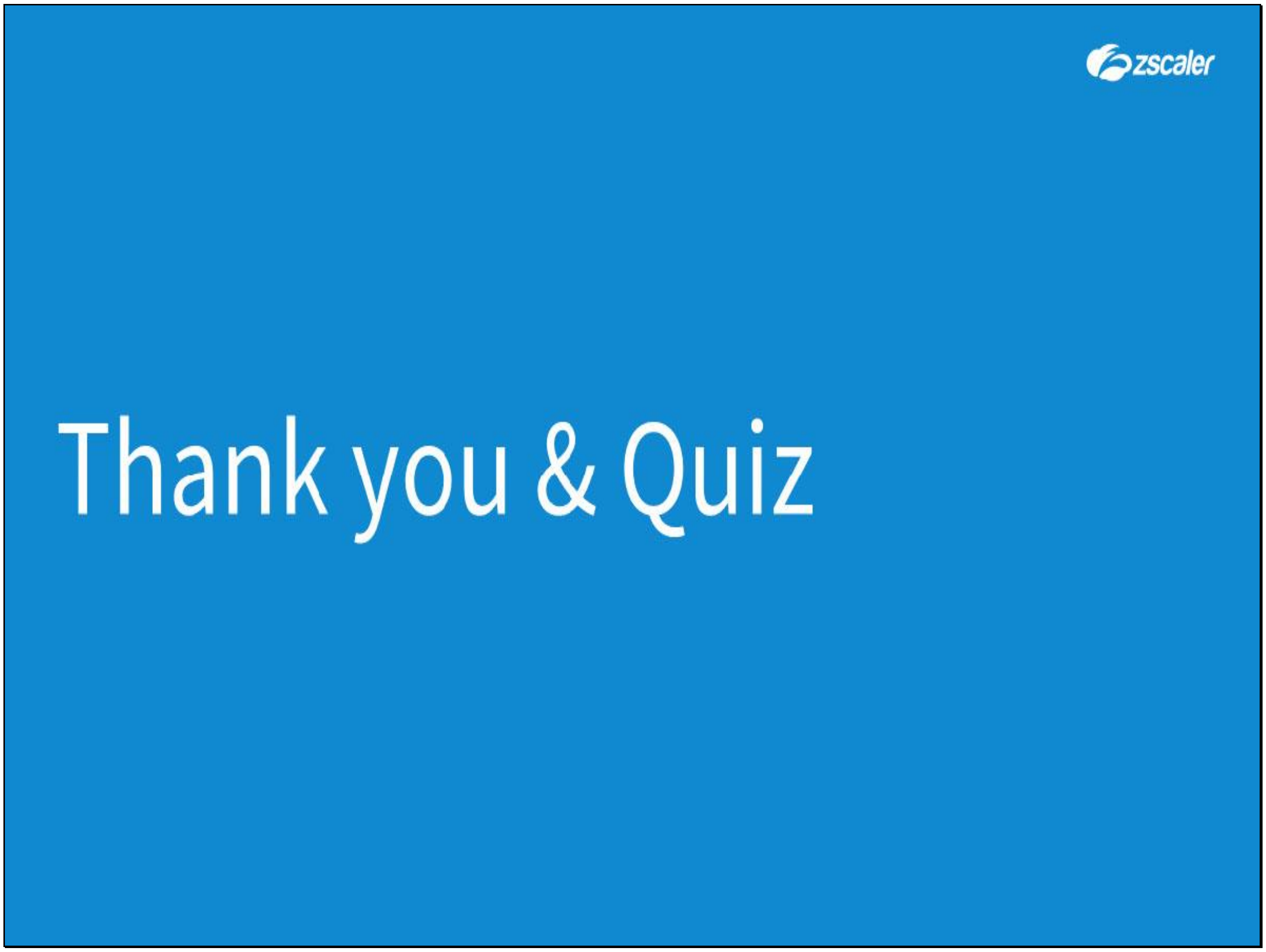
Enrollment and Provisioning Flow

Note: Enrollment through a proxy is supported, check the page at ***ips.<cloudname>.net*** for outbound Proxy/Firewall rules (if required)

Slide notes

Step 7: If bypasses have been defined and deployed to the app using a custom PAC file, traffic for the bypass destinations will be forwarded direct. The app checks every 15 minutes for **App Profile** PAC file updates and caches the file so that the local bypass sites will be reachable, even if there is a general Internet outage.

Slide 45 - Thank you & Quiz



Thank you & Quiz

Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

Click the **X** at top right to close this interface, then launch the quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.