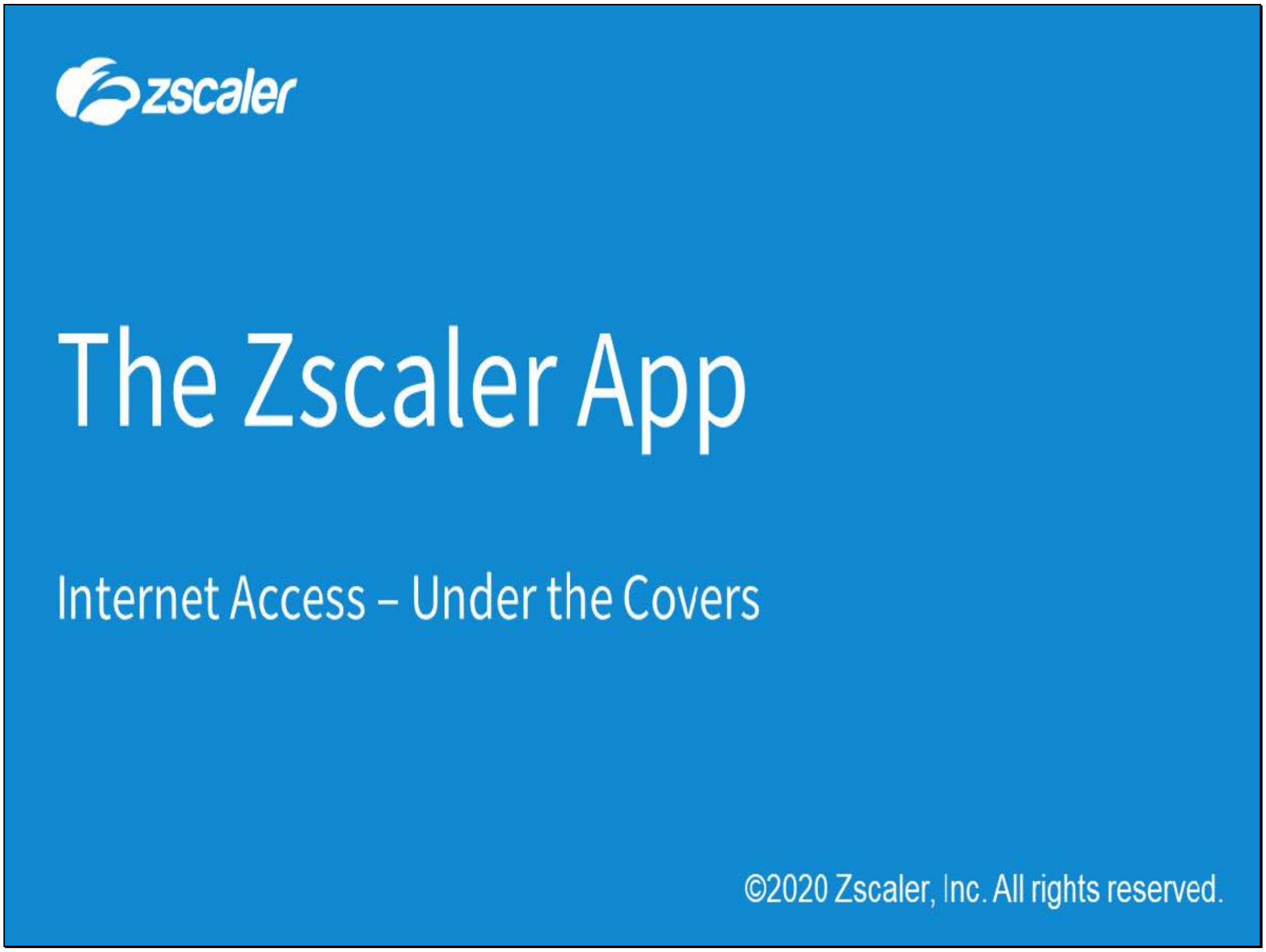
Slide 1 - Traffic Forwarding



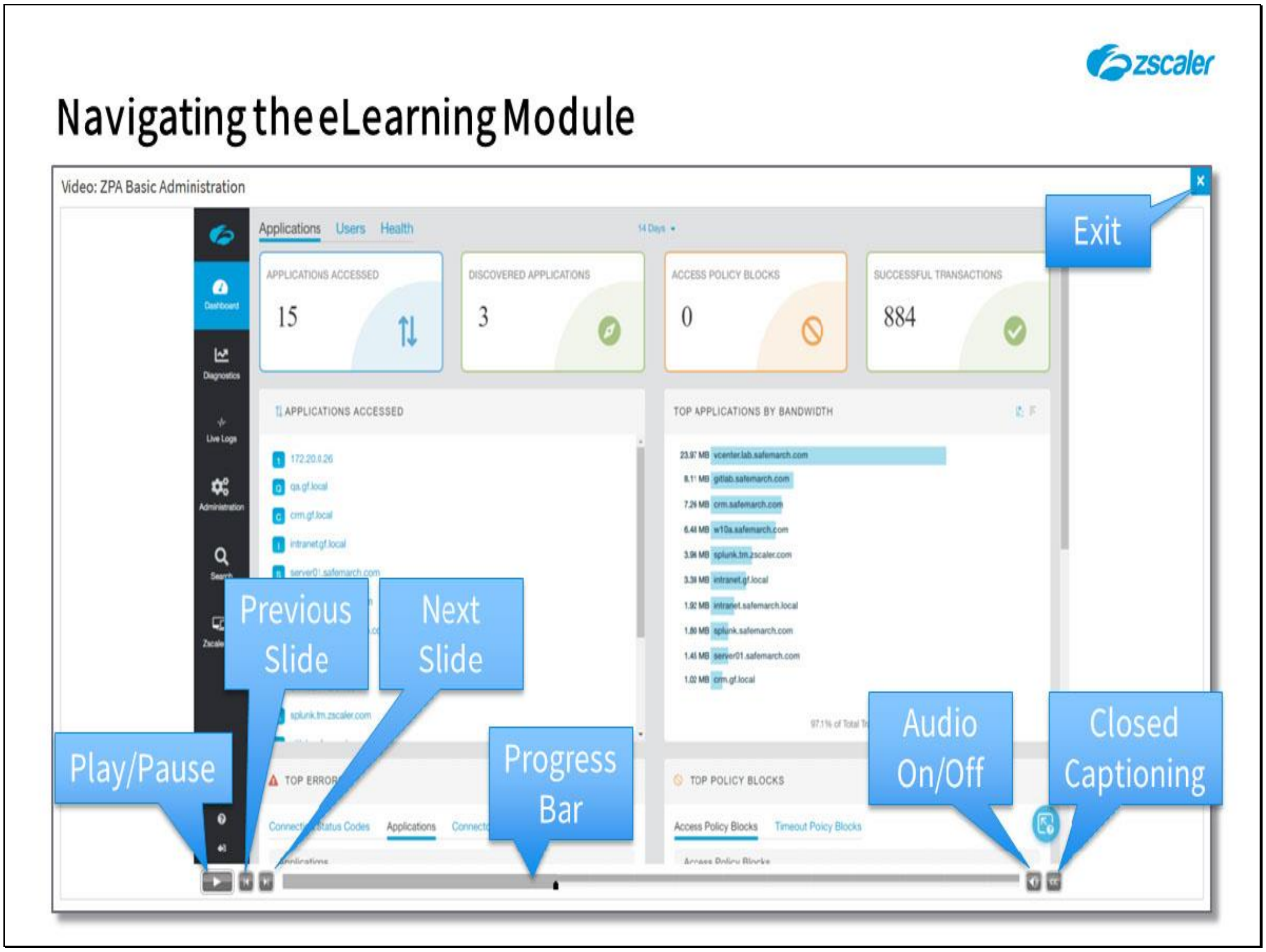
The Zscaler App

Internet Access – Under the Covers

Slide notes

Welcome to this training module for a look under the covers at the Zscaler App when used for the Internet Access service.

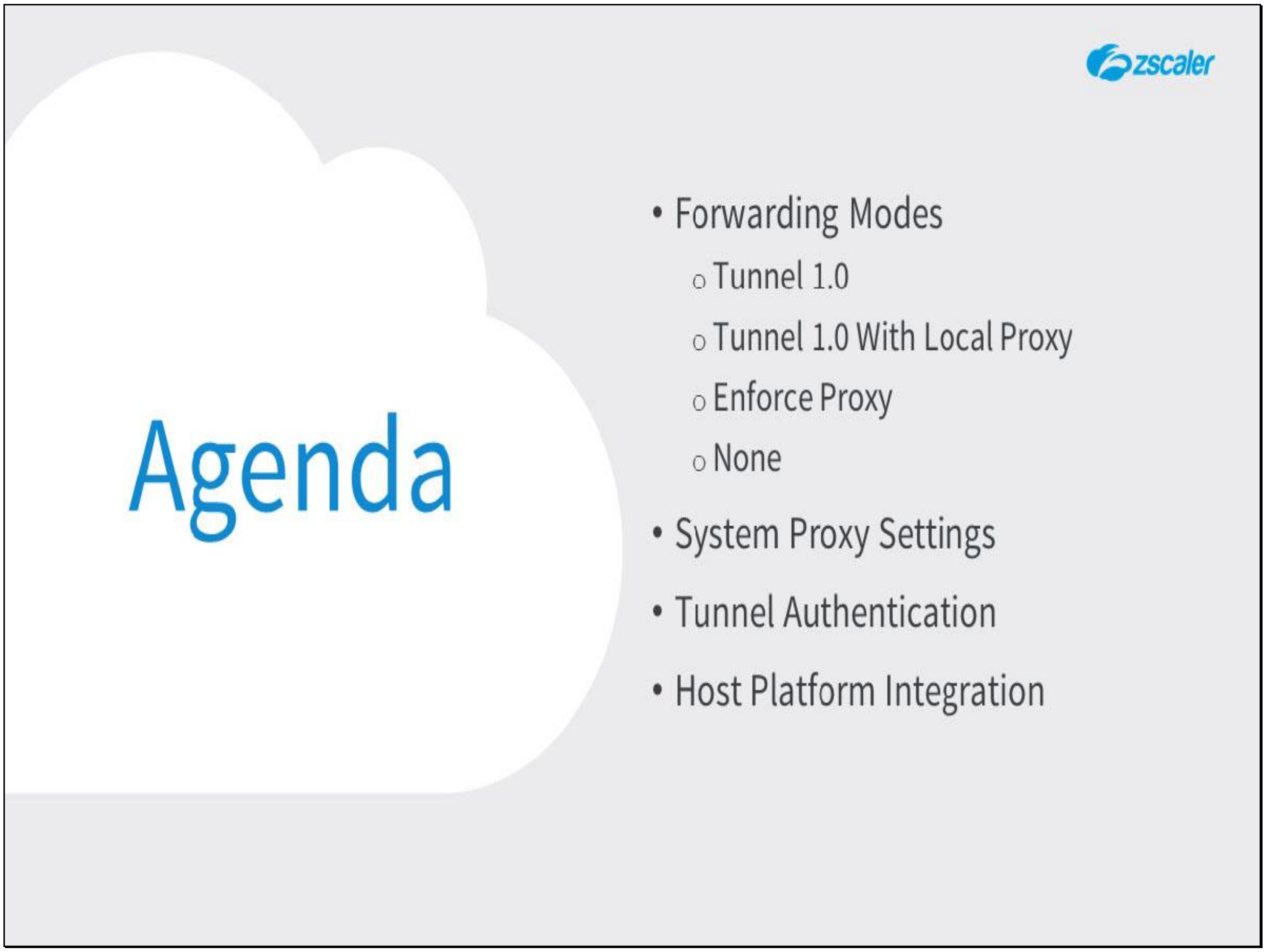
Slide 2 - Navigating the eLearning Module



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

- Forwarding Modes
  - Tunnel 1.0
  - Tunnel 1.0 With Local Proxy
  - Enforce Proxy
  - None
- System Proxy Settings
- Tunnel Authentication
- Host Platform Integration

Slide notes

In this module, we will cover the following topics: A detailed look at the Zscaler App forwarding modes (**Tunnel 1.0**, **Tunnel (1.0) With Local Proxy**, **Enforce Proxy**, and **None**); A look at the **System Proxy Settings** available for each of the forwarding modes; A look at how the ZIA Tunnels are authenticated; And at some host platform integration issues.

Note, we will look at the Tunnel 2.0 forwarding method in a separate module of this course.

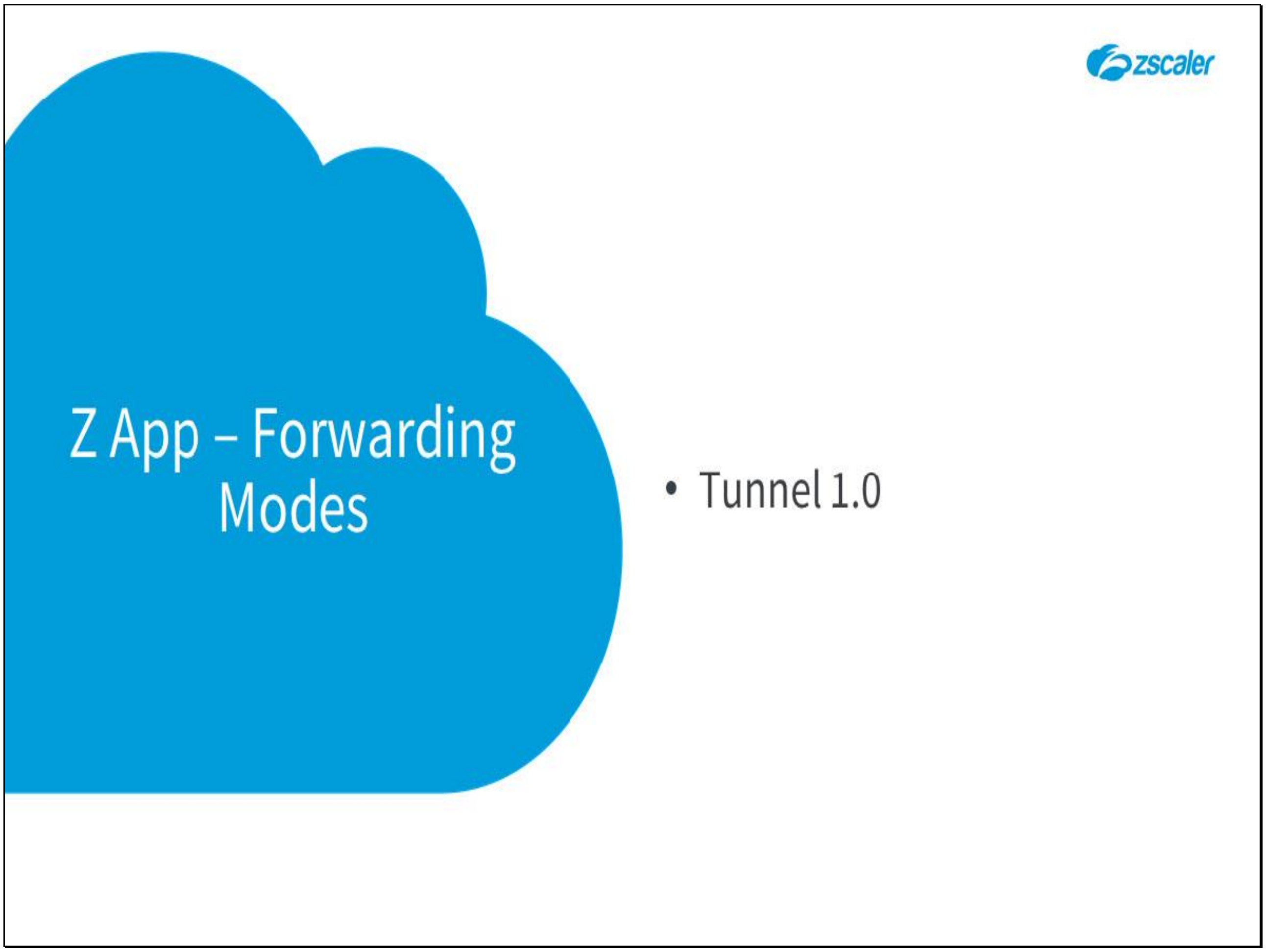
Slide 4 - Zscaler App – Forwarding Modes

Forwarding Modes

Slide notes

The first topic that we will cover is a detailed look at the forwarding modes available with the Zscaler App.

Slide 5 - Zscaler App – Forwarding Modes



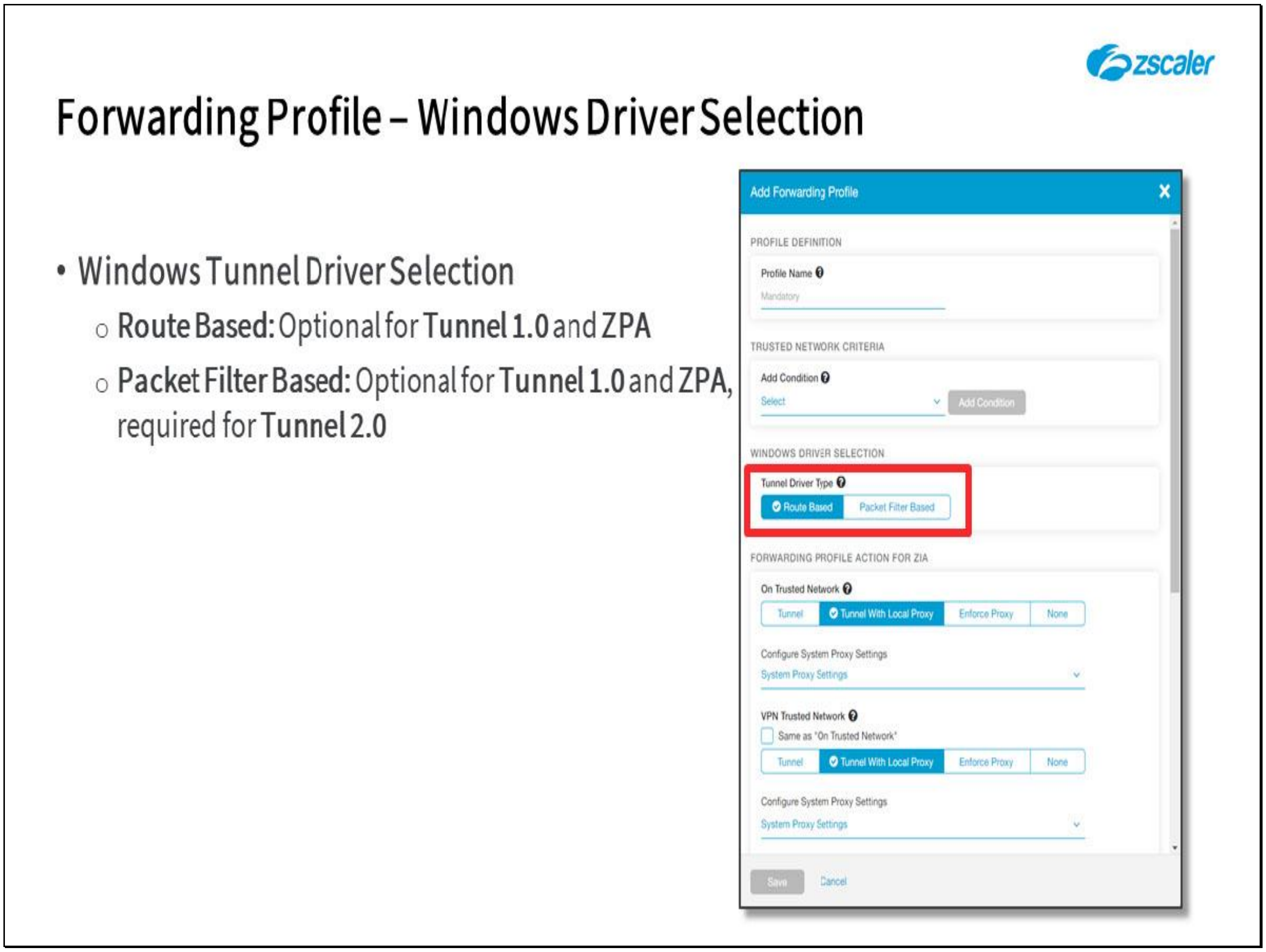
Z App – Forwarding Modes

- Tunnel 1.0

Slide notes

The first forwarding mode we will look at is **Tunnel 1.0**.

Slide 6 - Forwarding Profile – Windows Driver Selection



Forwarding Profile – Windows Driver Selection

- Windows Tunnel Driver Selection
  - **Route Based:** Optional for **Tunnel 1.0** and ZPA
  - **Packet Filter Based:** Optional for **Tunnel 1.0** and ZPA, required for **Tunnel 2.0**

Add Forwarding Profile

PROFILE DEFINITION

Profile Name: Mandatory

TRUSTED NETWORK CRITERIA

Add Condition: Select

WINDOWS DRIVER SELECTION

Tunnel Driver Type: [✓ Route Based] Packet Filter Based

FORWARDING PROFILE ACTION FOR ZIA

On Trusted Network: Tunnel [✓ Tunnel With Local Proxy] Enforce Proxy None

Configure System Proxy Settings: System Proxy Settings

VPN Trusted Network

□ Same as "On Trusted Network"

Tunnel [✓ Tunnel With Local Proxy] Enforce Proxy None

Configure System Proxy Settings: System Proxy Settings

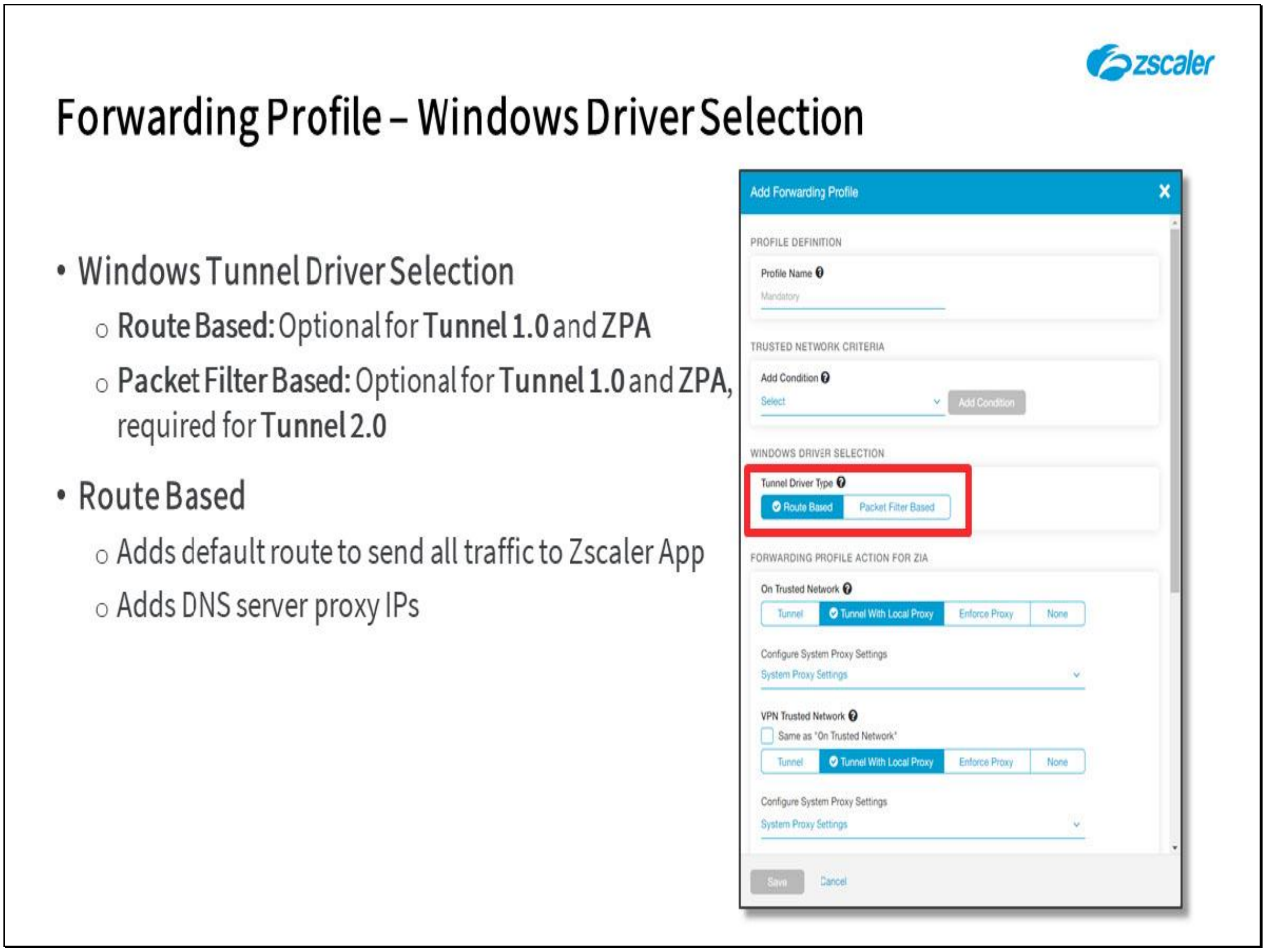
Slide notes

For the Windows platform, in the Zscaler App **Forwarding Profile**, you have the possibility to select the driver type to use for the **Tunnel** forwarding modes, whether **Route Based** or **Packet Filter Based**:

- The **Route Based** driver is an option for the **Tunnel 1.0** forwarding method for ZIA and for ZPA;
- The **Packet Filter Based** driver is an option for the **Tunnel 1.0** method and for ZPA but is required for the ZIA **Tunnel 2.0** method.

The default option in a **Forwarding Profile** currently, is to use the **Route Based** driver.

Slide 7 - Forwarding Profile – Windows Driver Selection



Forwarding Profile – Windows Driver Selection

- Windows Tunnel Driver Selection
  - **Route Based:** Optional for **Tunnel 1.0** and ZPA
  - **Packet Filter Based:** Optional for **Tunnel 1.0** and ZPA, required for **Tunnel 2.0**
- Route Based
  - Adds default route to send all traffic to Zscaler App
  - Adds DNS server proxy IPs

Add Forwarding Profile

PROFILE DEFINITION

Profile Name: Mandatory

TRUSTED NETWORK CRITERIA

Add Condition: Select

WINDOWS DRIVER SELECTION

Tunnel Driver Type: ● Route Based | Packet Filter Based

FORWARDING PROFILE ACTION FOR ZIA

On Trusted Network: Tunnel | ● Tunnel With Local Proxy | Enforce Proxy | None

Configure System Proxy Settings: System Proxy Settings

VPN Trusted Network

□ Same as "On Trusted Network"

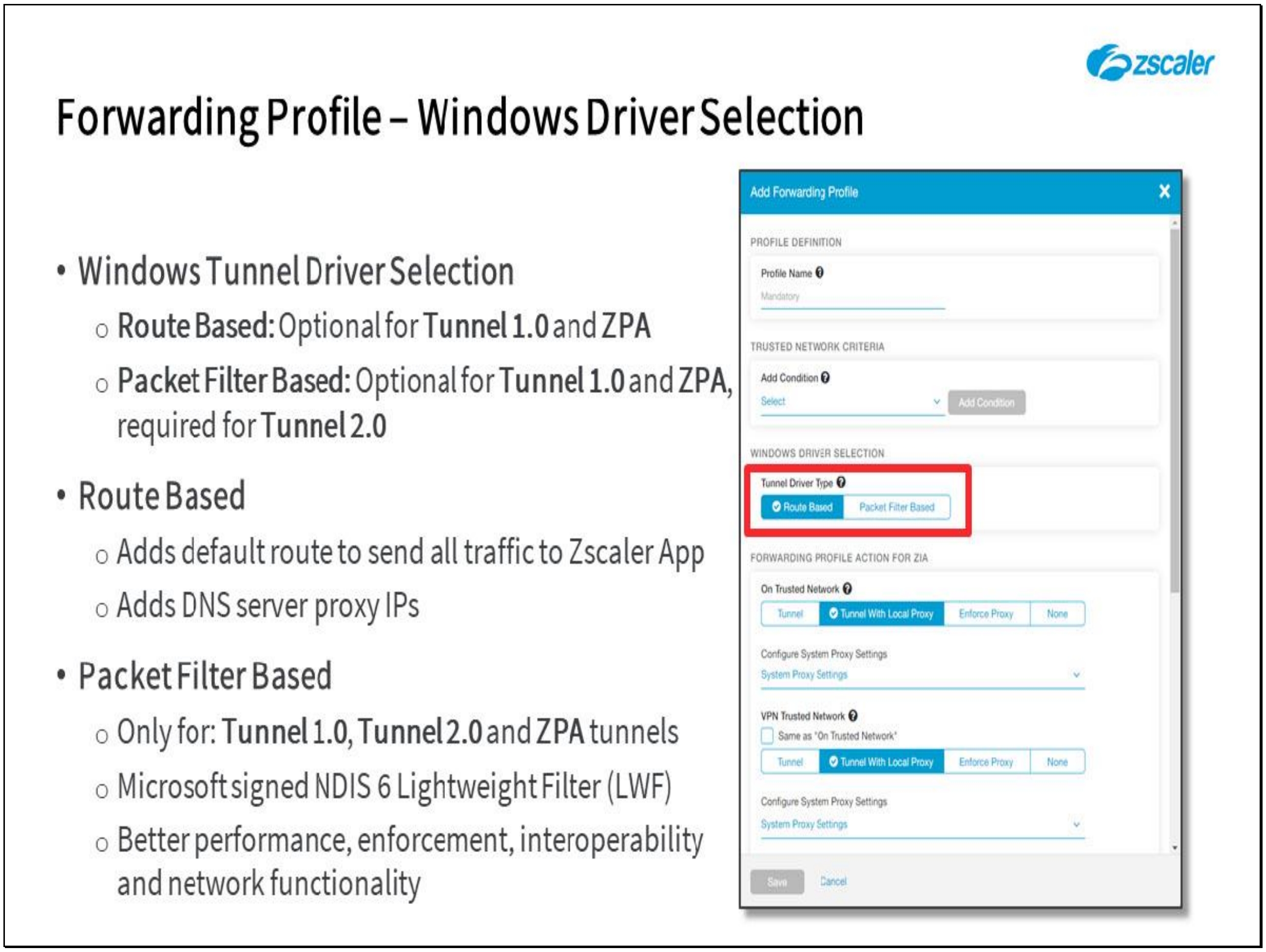
Tunnel | ● Tunnel With Local Proxy | Enforce Proxy | None

Configure System Proxy Settings: System Proxy Settings

Slide notes

Using the **Route Based** driver, Zscaler App sets up a default route to send all traffic into the App for processing. In addition, a set of priority DNS server IPs are added, to allow the proxying of DNS requests to the local DNS server. When necessary it also sets routes for any configured VPN gateways.

Slide 8 - Forwarding Profile – Windows Driver Selection



zscaler

Forwarding Profile – Windows Driver Selection

- Windows Tunnel Driver Selection
  - **Route Based:** Optional for **Tunnel 1.0** and **ZPA**
  - **Packet Filter Based:** Optional for **Tunnel 1.0** and **ZPA,** required for **Tunnel 2.0**
- Route Based
  - Adds default route to send all traffic to Zscaler App
  - Adds DNS server proxy IPs
- Packet Filter Based
  - Only for: **Tunnel 1.0, Tunnel 2.0** and **ZPA** tunnels
  - Microsoft signed NDIS 6 Lightweight Filter (LWF)
  - Better performance, enforcement, interoperability and network functionality

Add Forwarding Profile ✕

PROFILE DEFINITION

Profile Name: Mandatory

TRUSTED NETWORK CRITERIA

Add Condition: Select ⌄ [Add Condition]

WINDOWS DRIVER SELECTION

Tunnel Driver Type: [✓ Route Based] Packet Filter Based

FORWARDING PROFILE ACTION FOR ZIA

On Trusted Network: Tunnel [✓ Tunnel With Local Proxy] Enforce Proxy None

Configure System Proxy Settings: System Proxy Settings ⌄

VPN Trusted Network

☐ Same as "On Trusted Network"

Tunnel [✓ Tunnel With Local Proxy] Enforce Proxy None

Configure System Proxy Settings: System Proxy Settings ⌄

Save Cancel

Slide notes

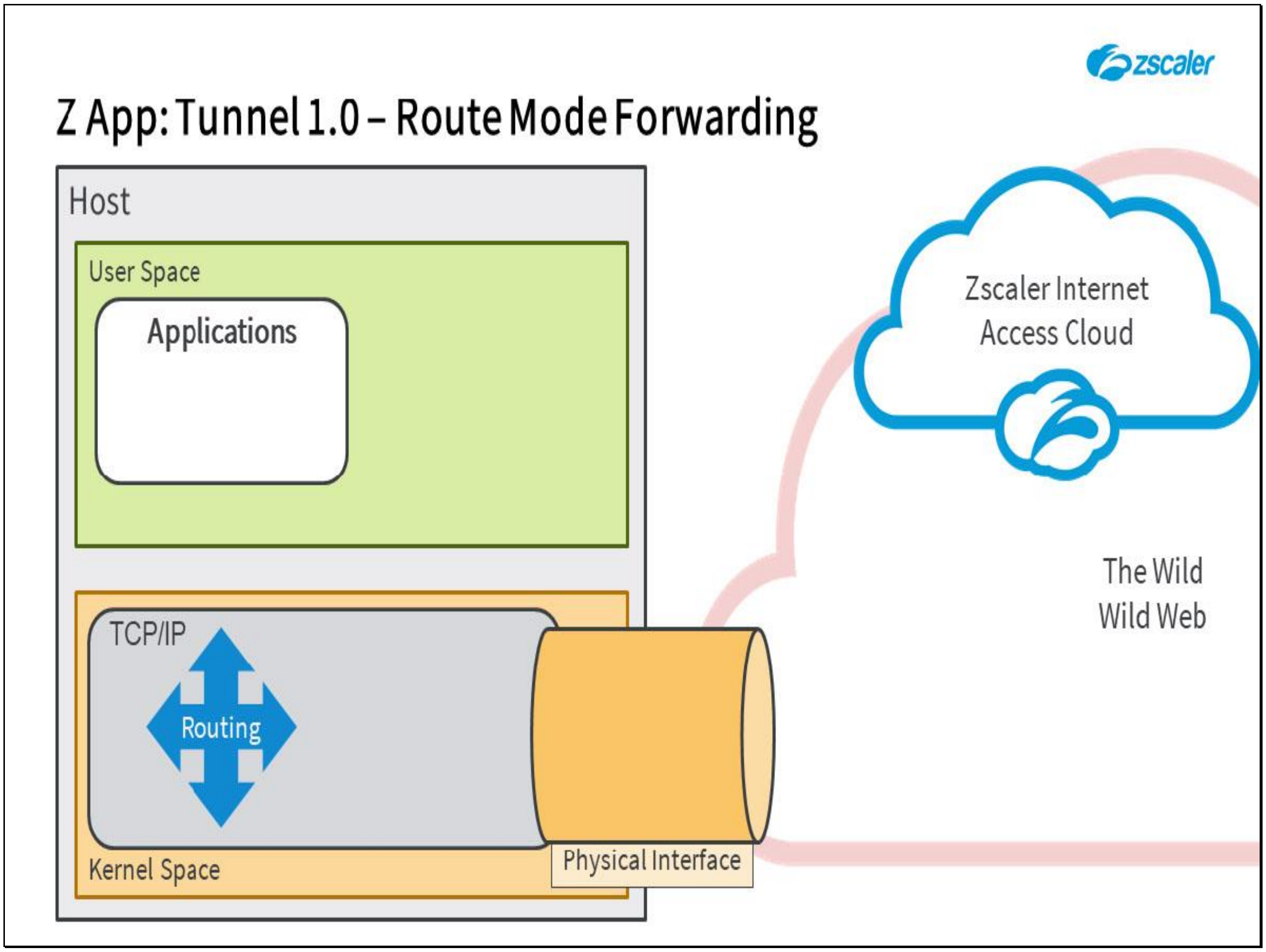
The **Packet Filter Based** driver is a high-performance packet filtering driver for the Windows platform that:

- Improves performance;
- Enables better enforcement on the platform;
- Allows for better interoperability;
- And improves overall network functionality.

The **Packet Filter Based** driver option allows Zscaler to transparently filter, view and modify raw network packets with minimal impact on network activity.

This driver is a Windows packet filter implemented using NDIS 6 Lightweight Filter (LWF) drivers which are tested and signed by Microsoft. When using the **Packet Filter Based** driver, the need for Zscaler to add routes and DNS Servers within the network stack is removed, the default route entry and other specific route entries are replaced by a TCP port **80**/**443** redirect filter, plus additional filters for any specified VPN gateway routes, the subnet for ZPA synthetic IP addresses (**100.64.0.0/16**) and any ZPA IP address routes. This removes the possibility for an end user to 'adjust' how the Zscaler App works by modifying or removing route entries.

Slide 9 - Zscaler App: Tunnel Mode



Z App: Tunnel 1.0 – Route Mode Forwarding

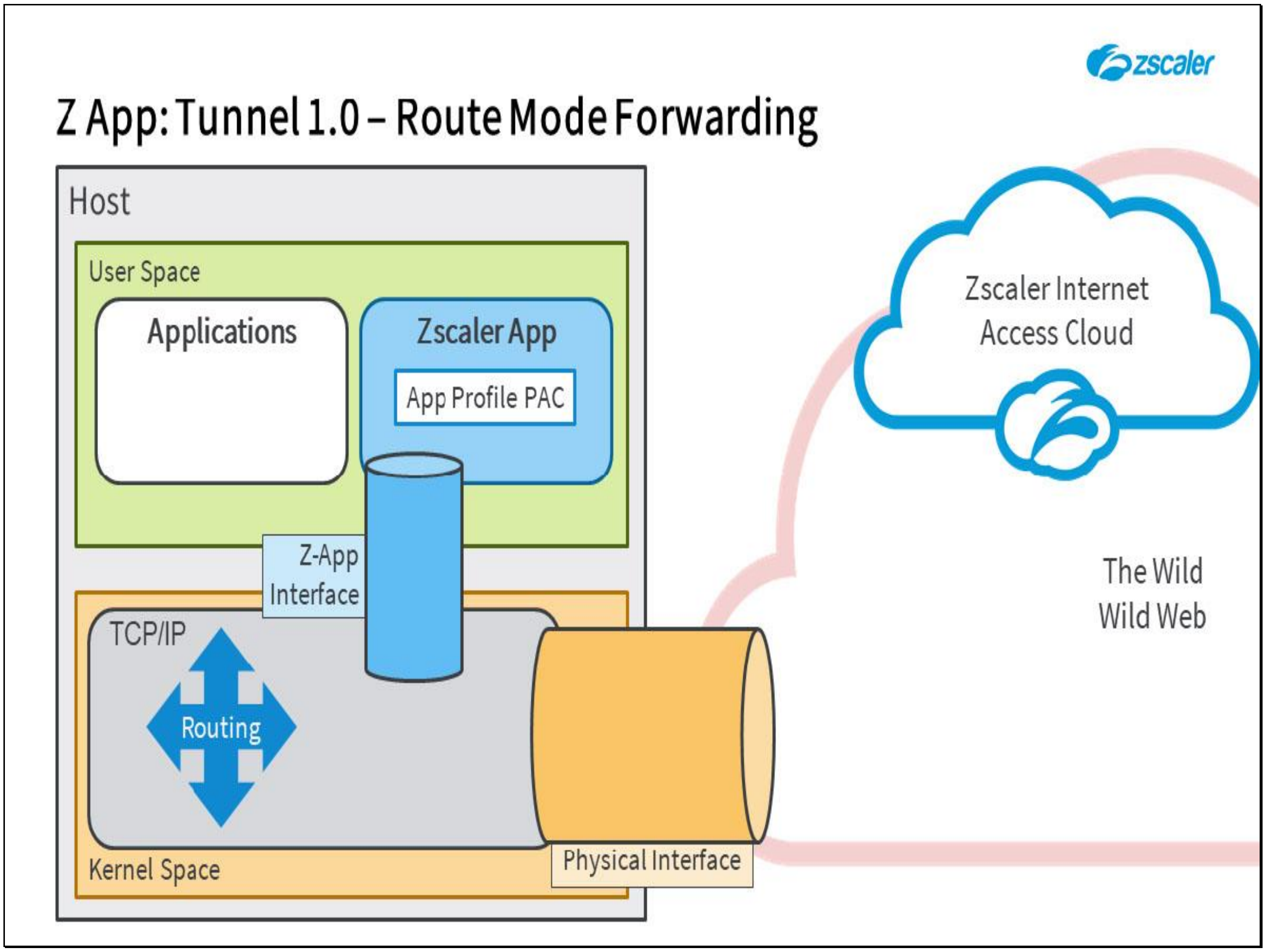
Slide notes

Let's talk through how the Zscaler App works in the default **Tunnel 1.0** mode, also referred to as 'route mode' as it sets up a default route to send all traffic to the App for processing. Note that route-based forwarding is the default forwarding method for **Tunnel 1.0** mode.

Here is a block diagram of the client device, with:

- The user space with applications;
- The kernel space with its TCP/IP stack and routing functionality;
- And the physical interface connecting the device to The Internet.

Slide 10 - Z App: Tunnel 1.0 – Route Mode Forwarding



zscaler

Z App: Tunnel 1.0 – Route Mode Forwarding

Host

User Space

Applications

Zscaler App

App Profile PAC

Z-App Interface

TCP/IP

Routing

Kernel Space

Physical Interface

Zscaler Internet Access Cloud

The Wild Wild Web

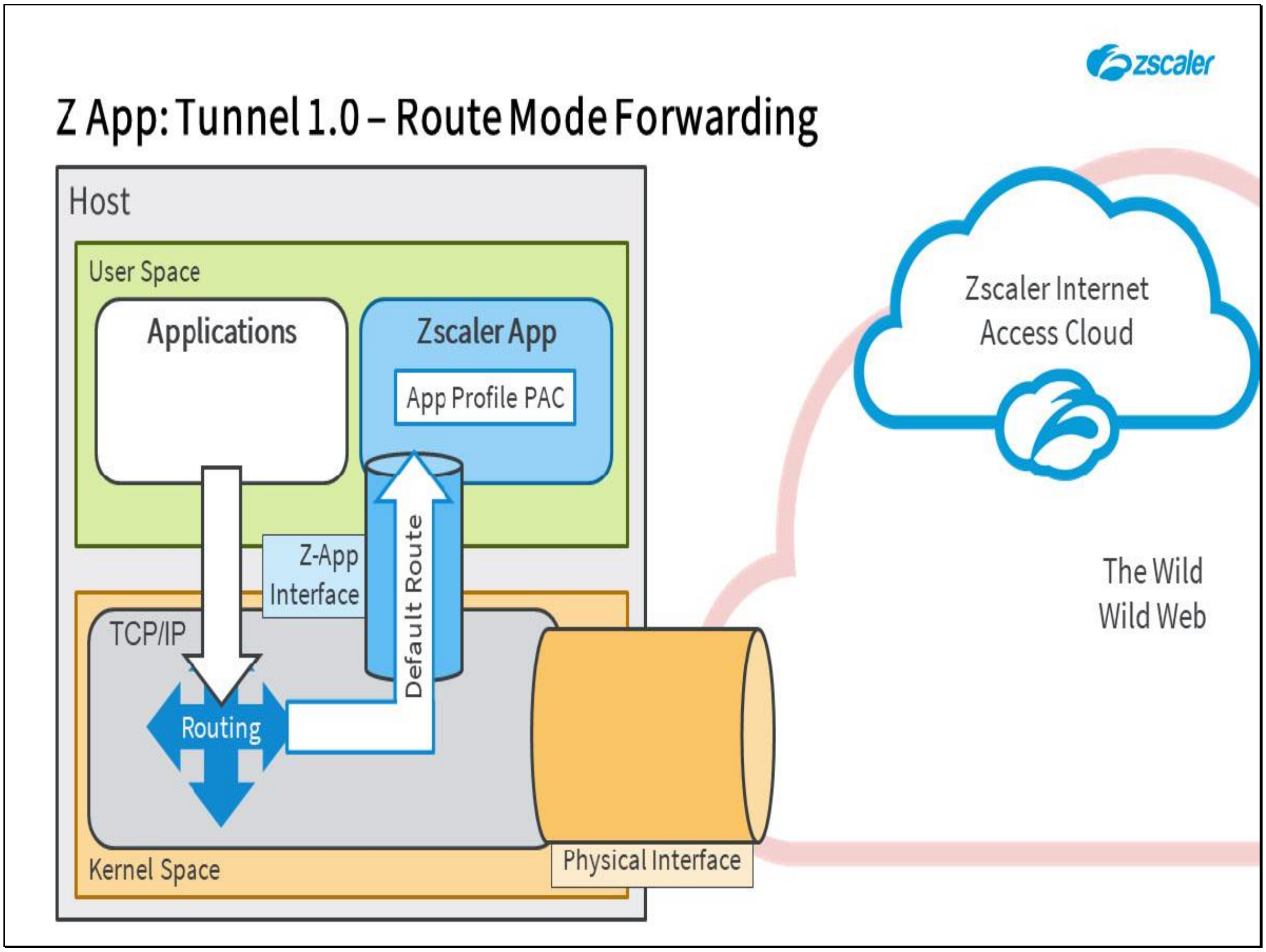
Slide notes

The App is of course installed in the user space, and it installs a virtual Ethernet network interface that is assigned a non-routable, synthetic IP address from the **100.64.0.0/16** range.

The Zscaler App refers to the PAC file specified in the **App Profile** applied to it for key configuration settings, most importantly - the ZENs to send traffic to (whether tunneled or proxied). A default PAC file is used in the default **App Profile** that uses the **{$GATEWAY}** and **{$SECONDARY_GATEWAY}** macros to allow the geo-location of the 2 closest healthy ZENs to forward traffic to.

You can also specify specific ZENs in a custom PAC file, which may also contain destinations that are to be bypassed by Zscaler App in all forwarding modes that use tunneling.

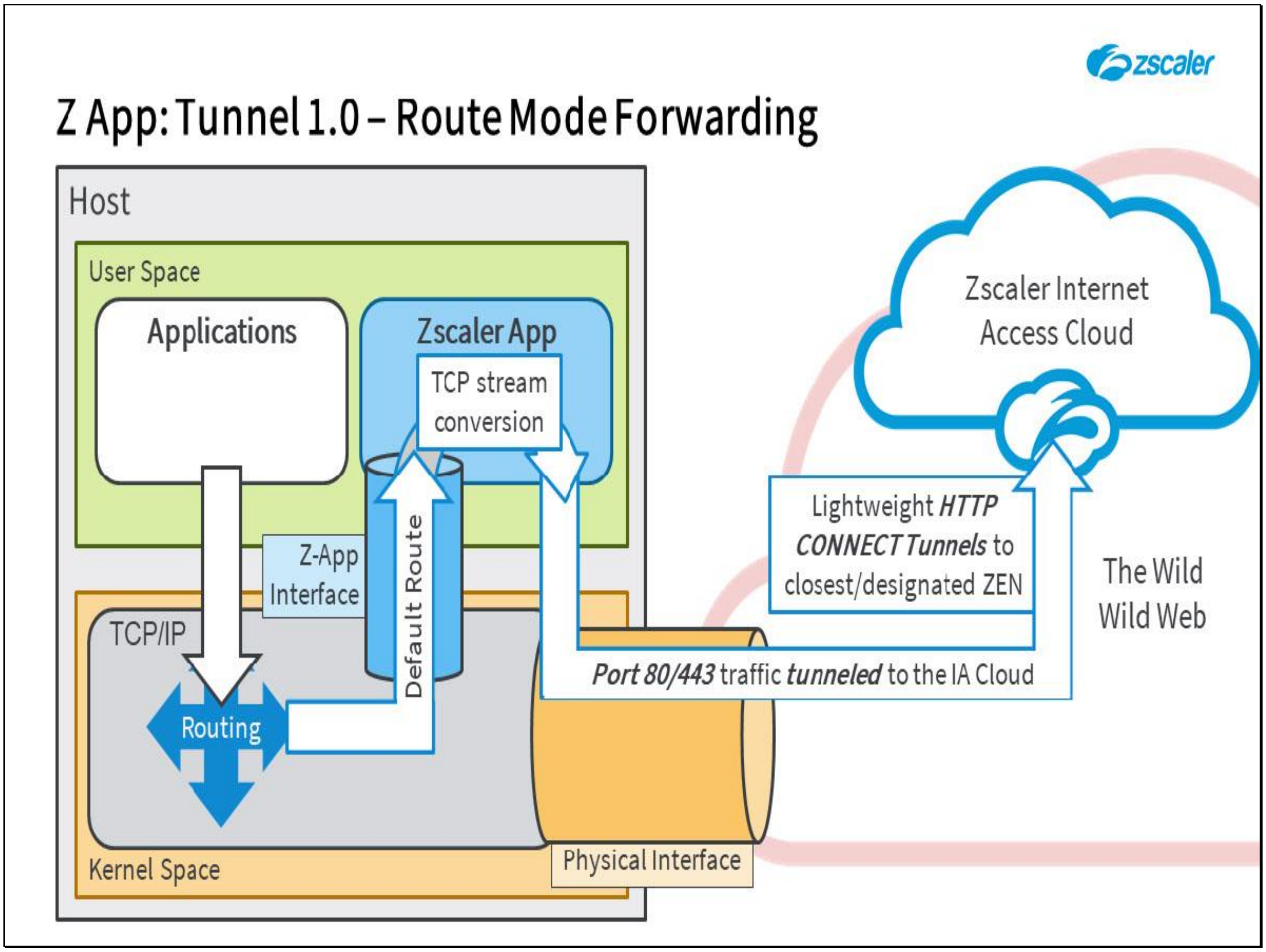
Slide 11 - Z App: Tunnel 1.0 – Route Mode Forwarding



Slide notes

During installation, the App also configures a default route to send ALL traffic to this interface, plus it configures three DNS servers on the IPs: **100.64.0.3**, **100.64.0.4**, and **100.64.0.5**.

Slide 12 - Z App: Tunnel 1.0 – Route Mode Forwarding



Z App: Tunnel 1.0 – Route Mode Forwarding

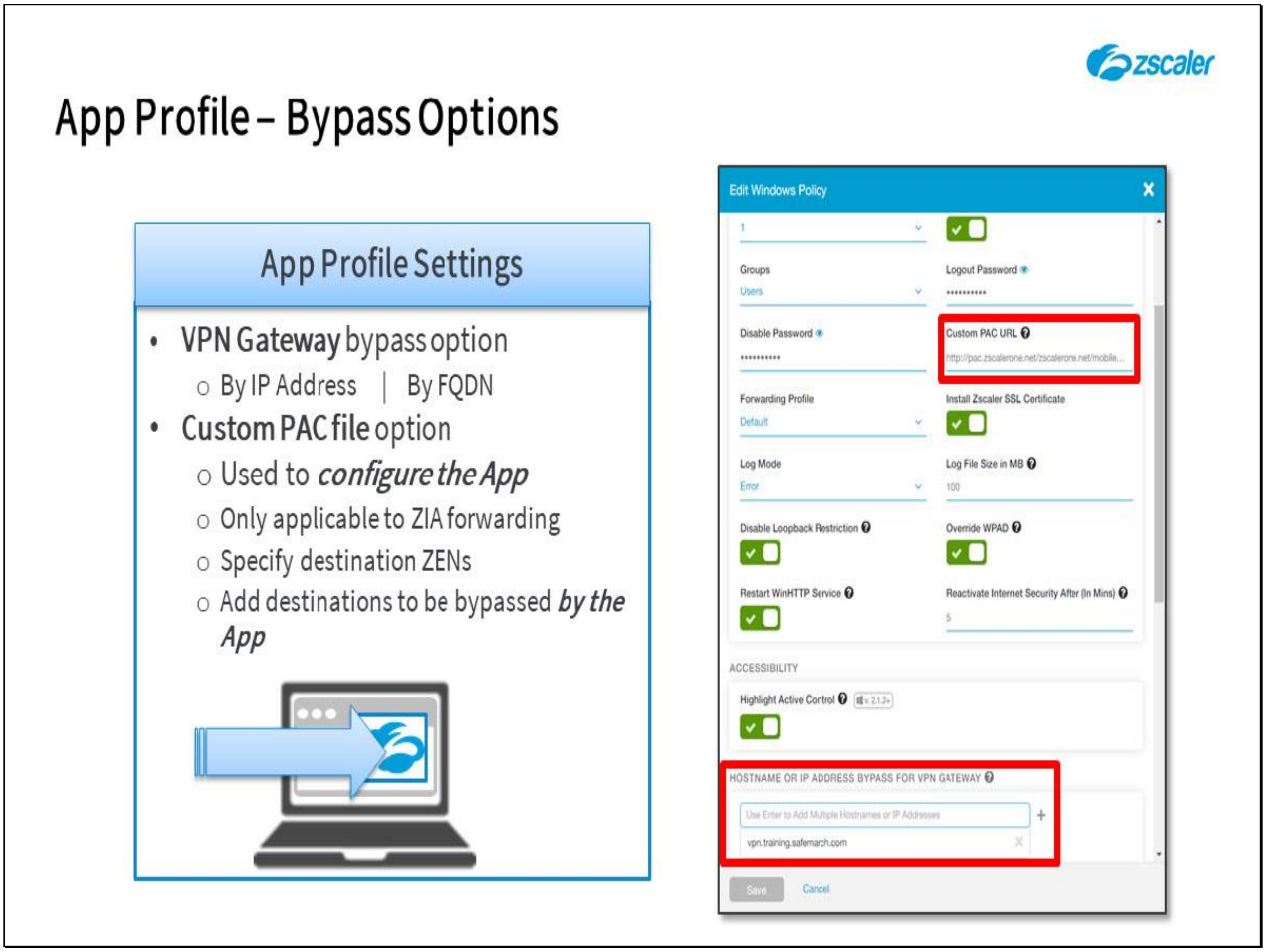
Slide notes

Which means that TCP port **80**, and **443** traffic (that is not bypassed) will be tunneled to Zscaler, either to the closest healthy ZEN, or to a ZEN specified in the PAC file applied to the App in the **App Profile**.

The tunnels are lightweight, unencrypted **HTTP CONNECT** tunnels established on destination port **443**, they are authenticated using the **Proxy Digest** method described later in this module. Packets to be forwarded to the Zscaler Cloud in this mode must first be converted to a TCP stream within the App.

Note that the traffic forwarded in the tunnels is not restricted to browser traffic; any TCP traffic sent to destination ports **80** or **443**, regardless of the application that generated it, will be tunneled to Zscaler.

Slide 13 - App Profile – Bypass Options



App Profile – Bypass Options

App Profile Settings

- VPN Gateway bypass option
  - By IP Address | By FQDN
- Custom PAC file option
  - Used to *configure the App*
  - Only applicable to ZIA forwarding
  - Specify destination ZENs
  - Add destinations to be bypassed *by the App*

Edit Windows Policy

1

☑

Groups: Users

Logout Password: **********

Disable Password: **********

Custom PAC URL: http://pac.zscalerone.net/zscalerone.net/mobile...

Forwarding Profile: Default

Install Zscaler SSL Certificate: ☑

Log Mode: Error

Log File Size in MB: 100

Disable Loopback Restriction: ☑

Override WPAD: ☑

Restart WinHTTP Service: ☑

Reactivate Internet Security After (In Mins): 5

ACCESSIBILITY

Highlight Active Control (v. 2.1.2+): ☑

HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY

Use Enter to Add Multiple Hostnames or IP Addresses

vpn.training.safemarch.com

Slide notes

An **App Profile** is applied to the Zscaler App on enrollment to configure App forwarding and other behavior, the default **App Profile** is used if no custom profile is applied to that user based on their group memberships.

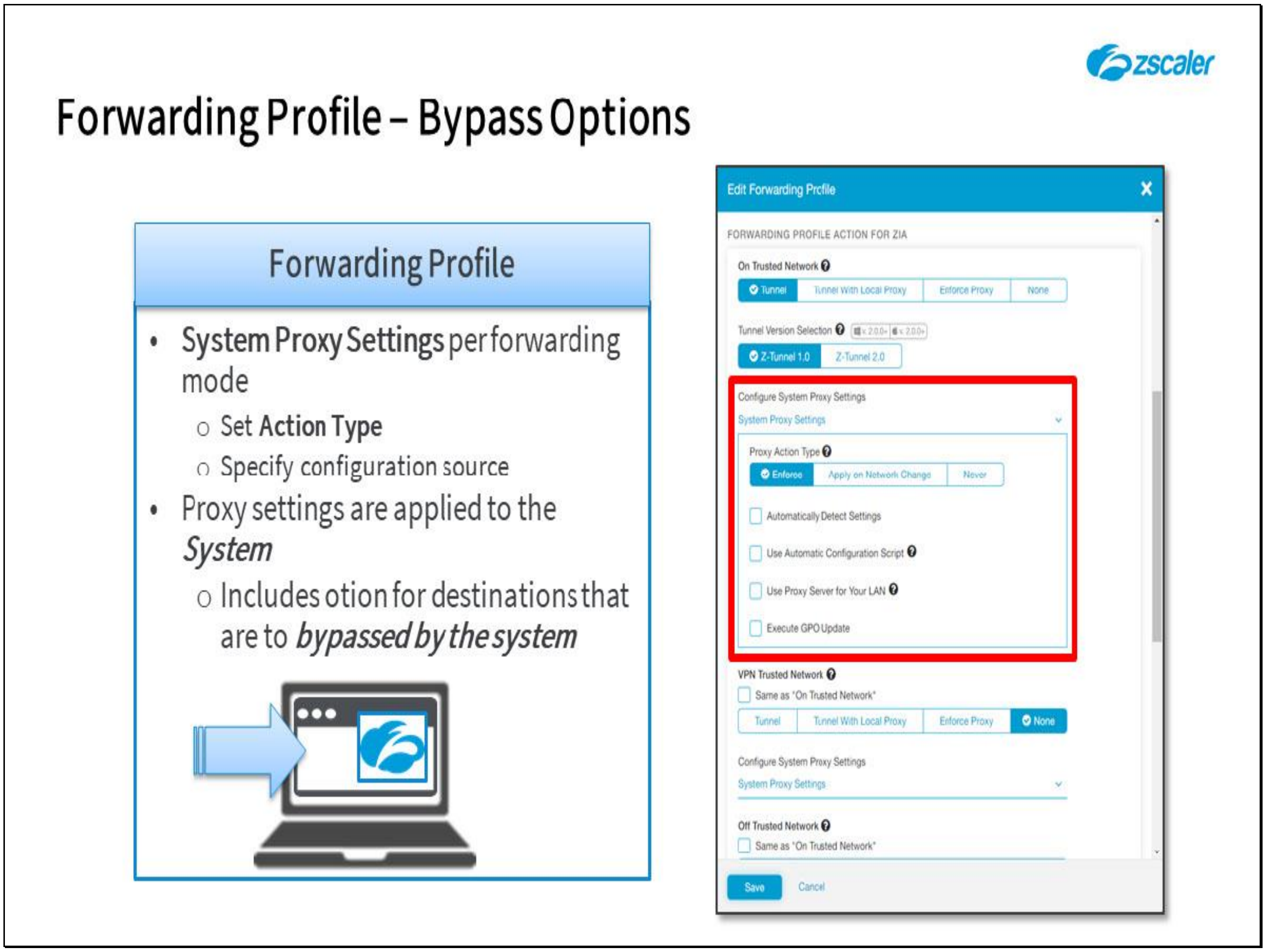
An option in the **App Profile** is to specify one or more **Hostname/IP Address Bypass for VPN Gateway**. If configured, specific routes for these destinations will be added to the system network settings, so Internet Access traffic for the IPs or FQDNs specified here will bypass the Zscaler App completely.

In addition, it is possible to apply a custom PAC file in an **App Profile**, which is used more as a configuration file for Zscaler App than as a conventional proxy auto-configuration file. This PAC file can be used for two purposes:

1. To specify the destination ZENs, if you do not want to use the default mechanism to geo-locate the closest;
2. Add destinations that are to be bypassed by the App itself in the forwarding modes that use tunnels.

As mentioned previously, the default **App Profile** PAC file uses the **{$GATEWAY}** and **{$SECONDARY_GATEWAY}** variables to geo-locate the closest ZIA ZENs, it contains no destination bypasses.

Slide 14 - Zscaler App PAC File Usage



Forwarding Profile – Bypass Options

Forwarding Profile

- **System Proxy Settings** per forwarding mode
  - Set **Action Type**
  - Specify configuration source
- Proxy settings are applied to the *System*
  - Includes otion for destinations that are to ***bypassed by the system***

Edit Forwarding Profile

FORWARDING PROFILE ACTION FOR ZIA

On Trusted Network: ● Tunnel | Tunnel With Local Proxy | Enforce Proxy | None

Tunnel Version Selection (v 2.0.0+ | v 2.0.0+): ● Z-Tunnel 1.0 | Z-Tunnel 2.0

Configure System Proxy Settings: System Proxy Settings

Proxy Action Type: ● Enforce | Apply on Network Change | Never

□ Automatically Detect Settings

□ Use Automatic Configuration Script

□ Use Proxy Server for Your LAN

□ Execute GPO Update

VPN Trusted Network

□ Same as "On Trusted Network"

Tunnel | Tunnel With Local Proxy | Enforce Proxy | ● None

Configure System Proxy Settings: System Proxy Settings

Off Trusted Network

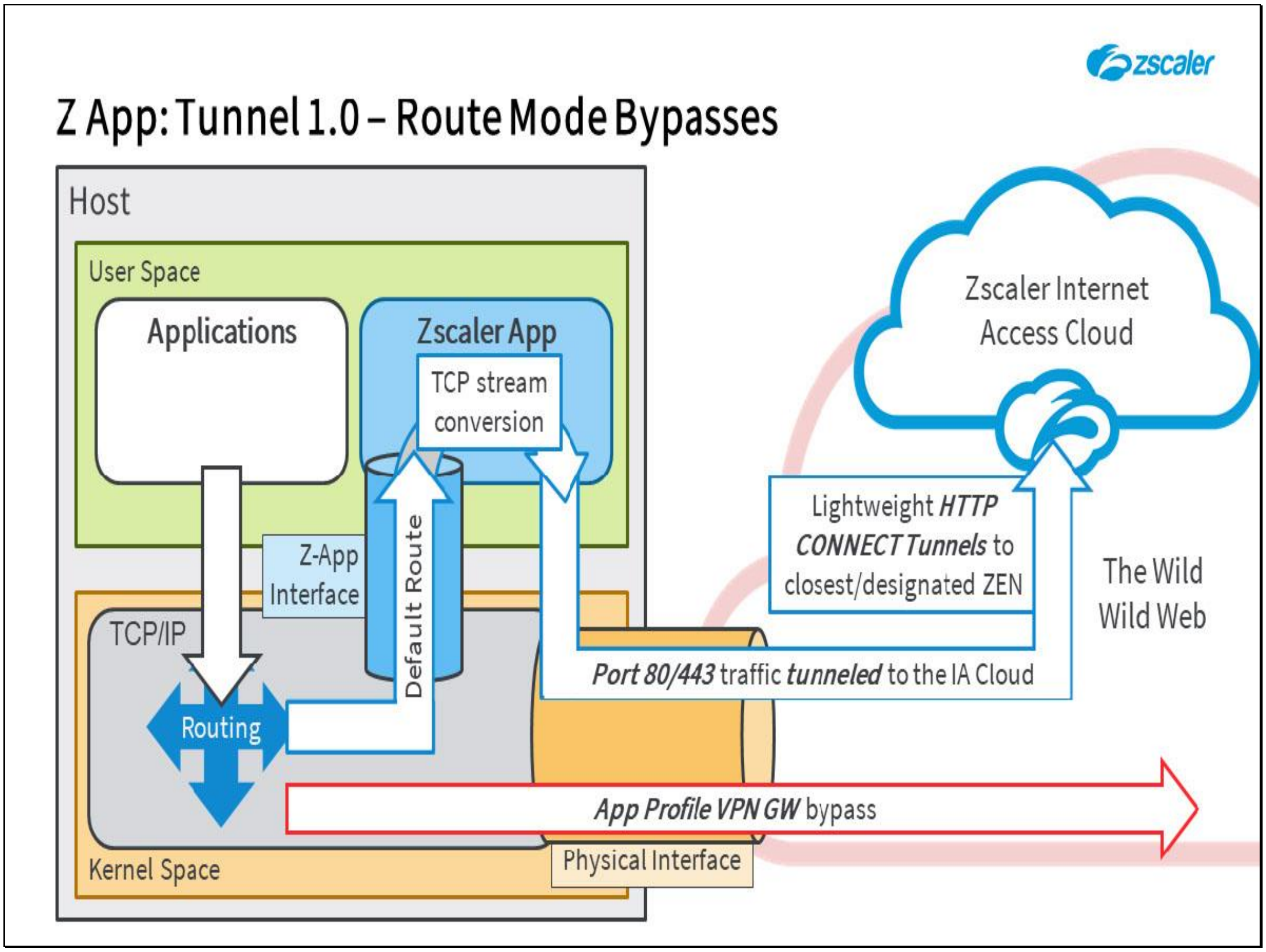
□ Same as "On Trusted Network"

Slide notes

In a **Forwarding Profile**, when configuring each of the forwarding methods, you have options for managing the **System Proxy Settings**. You can specify the **Action Type** (**Enforce**, **Apply on Network Change**, or **Never**), plus you can control the source for the system proxy configuration.

Any configuration specified here, typically in the form of a PAC file, is applied to the system to replace any configured proxy definitions and may include destinations to be bypassed. Any bypasses specified in these **Forwarding Profile** settings will not even be processed by the App. We will look at these options in more detail in a later section of this module.

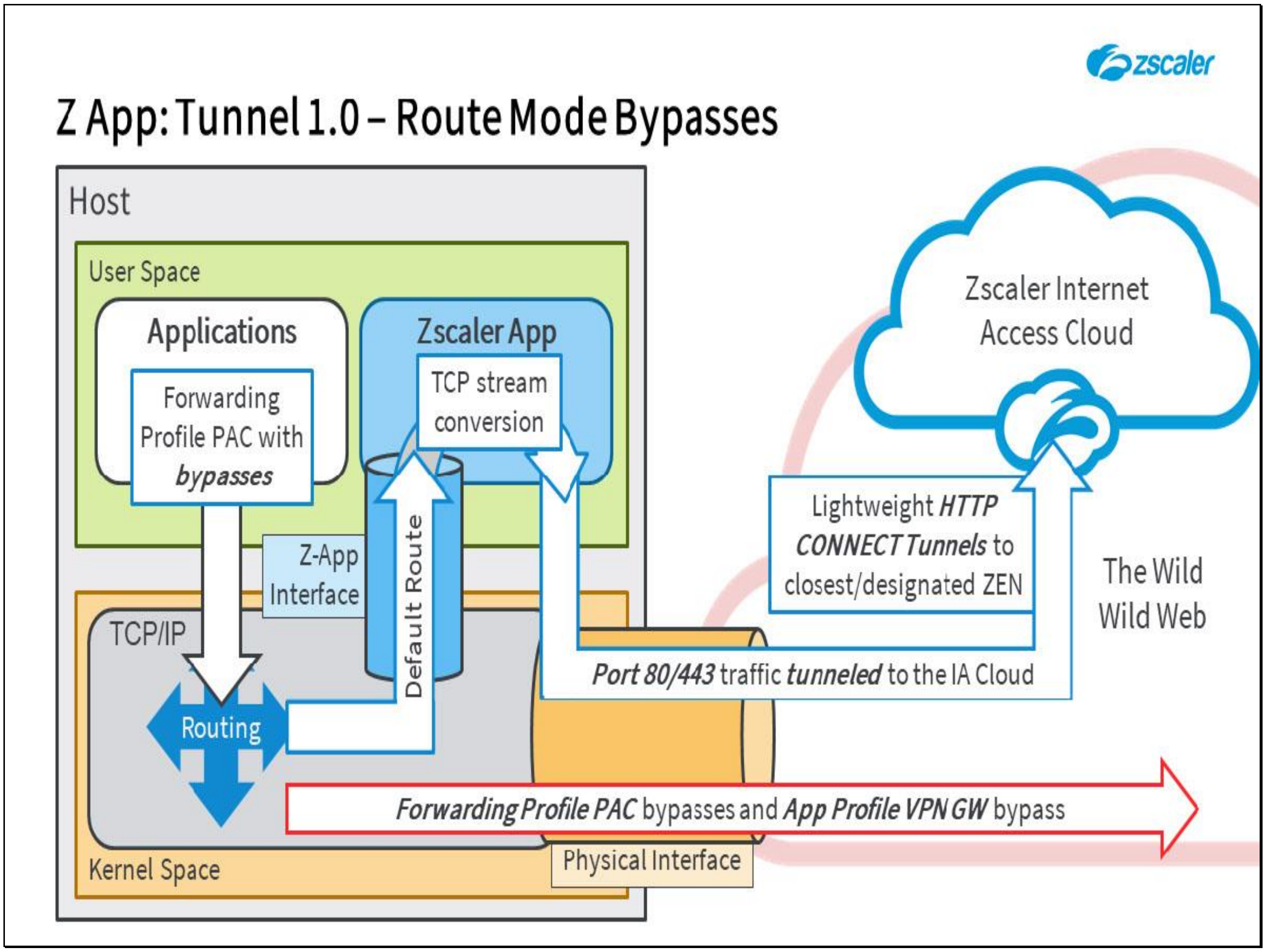
Slide 15 - Z App: Tunnel 1.0 – Route Mode Bypasses


zscaler
Z App: Tunnel 1.0 – Route Mode Bypasses
Host
User Space
Applications
Zscaler App
TCP stream conversion
Z-App Interface
Default Route
TCP/IP
Routing
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Lightweight HTTP CONNECT Tunnels to closest/designated ZEN
Port 80/443 traffic tunneled to the IA Cloud
The Wild Wild Web
App Profile VPN GW bypass

Slide notes

For the **App Profile VPN GW Bypass** field, typically you would add the hostnames or IPs of any VPN gateways that should receive traffic directly from the client device. Specific IP routes are added for any addresses specified, so traffic for any IPs or hosts specified in that field are not even processed by Zscaler App.

Slide 16 - Z App: Tunnel 1.0 – Route Mode Whitelisting



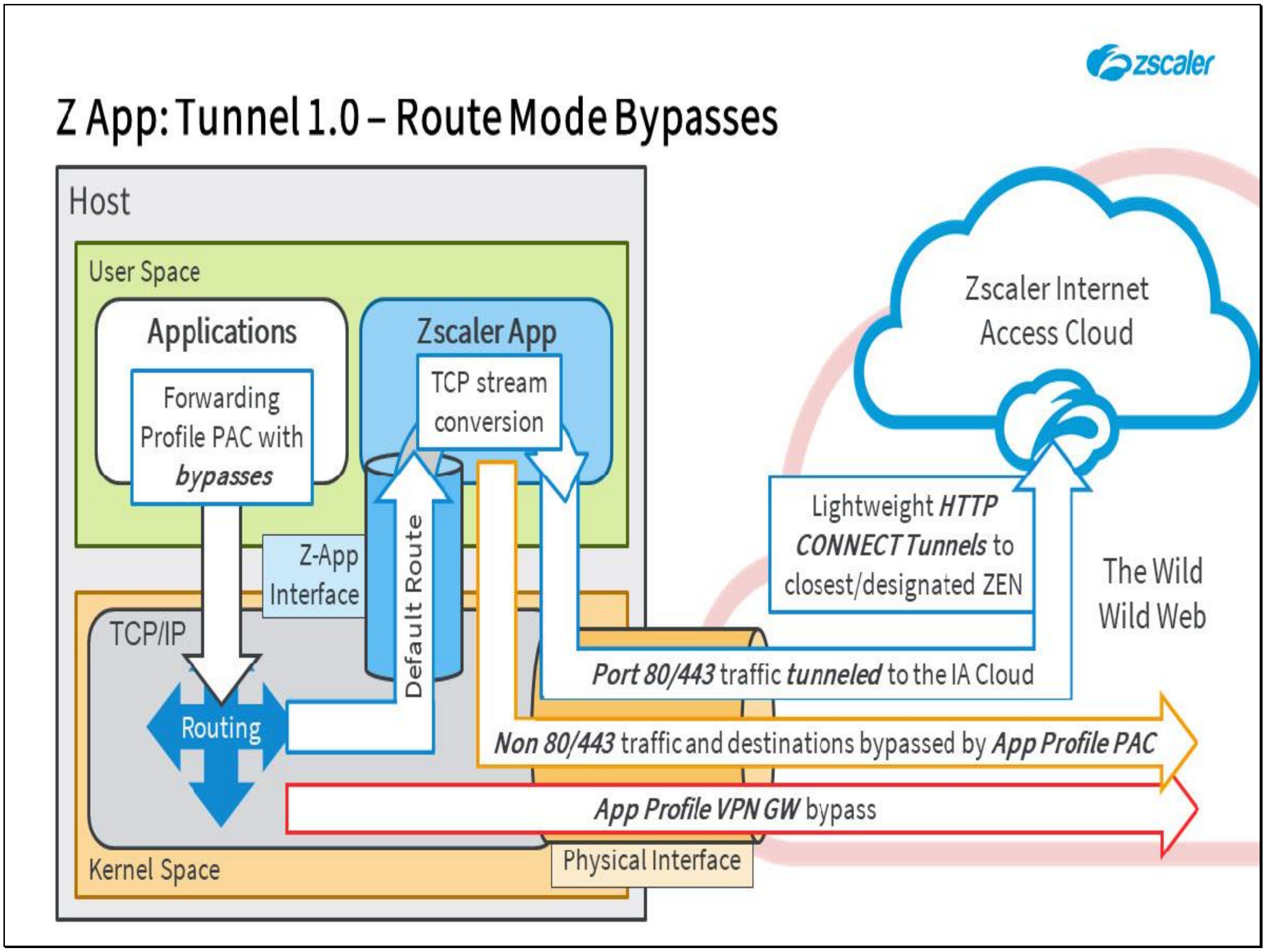
Z App: Tunnel 1.0 – Route Mode Bypasses

zscaler
Host
User Space
Applications
Forwarding Profile PAC with *bypasses*
Zscaler App
TCP stream conversion
Z-App Interface
Default Route
TCP/IP
Routing
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
Port 80/443 traffic *tunneled* to the IA Cloud
Forwarding Profile PAC bypasses and *App Profile VPN GW* bypass

Slide notes

If a system proxy configuration has been added in the applied **Forwarding Profile** that contains bypass destinations, this traffic will also be sent direct by the system proxy settings and not even be processed by the App.

Slide 17 - Z App: Tunnel 1.0 – Route Mode Bypasses



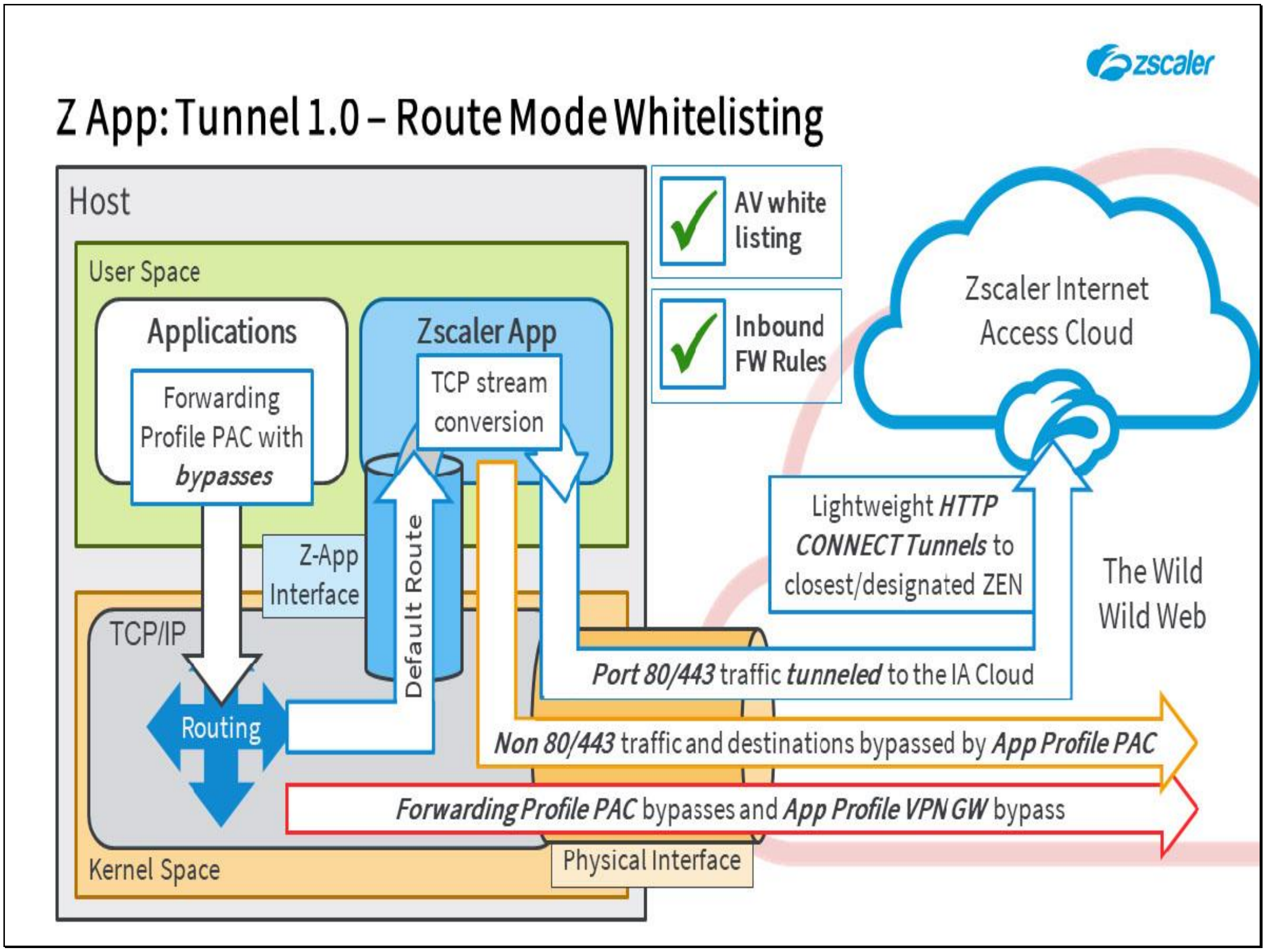
Z App: Tunnel 1.0 – Route Mode Bypasses

zscaler
Host
User Space
Applications
Forwarding Profile PAC with *bypasses*
Zscaler App
TCP stream conversion
Z-App Interface
Default Route
TCP/IP
Routing
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
Port 80/443 traffic *tunneled* to the IA Cloud
Non 80/443 traffic and destinations bypassed by *App Profile PAC*
App Profile VPN GW bypass

Slide notes

In this mode, any traffic that is NOT on TCP ports **80**/**443** is still processed by the App (because it is on the default route) but is simply forwarded directly through the physical interface. In addition, if traffic is for a destination that is listed as a bypass in the **App Profile** PAC file, that traffic is also processed by the App, but is simply forwarded directly.

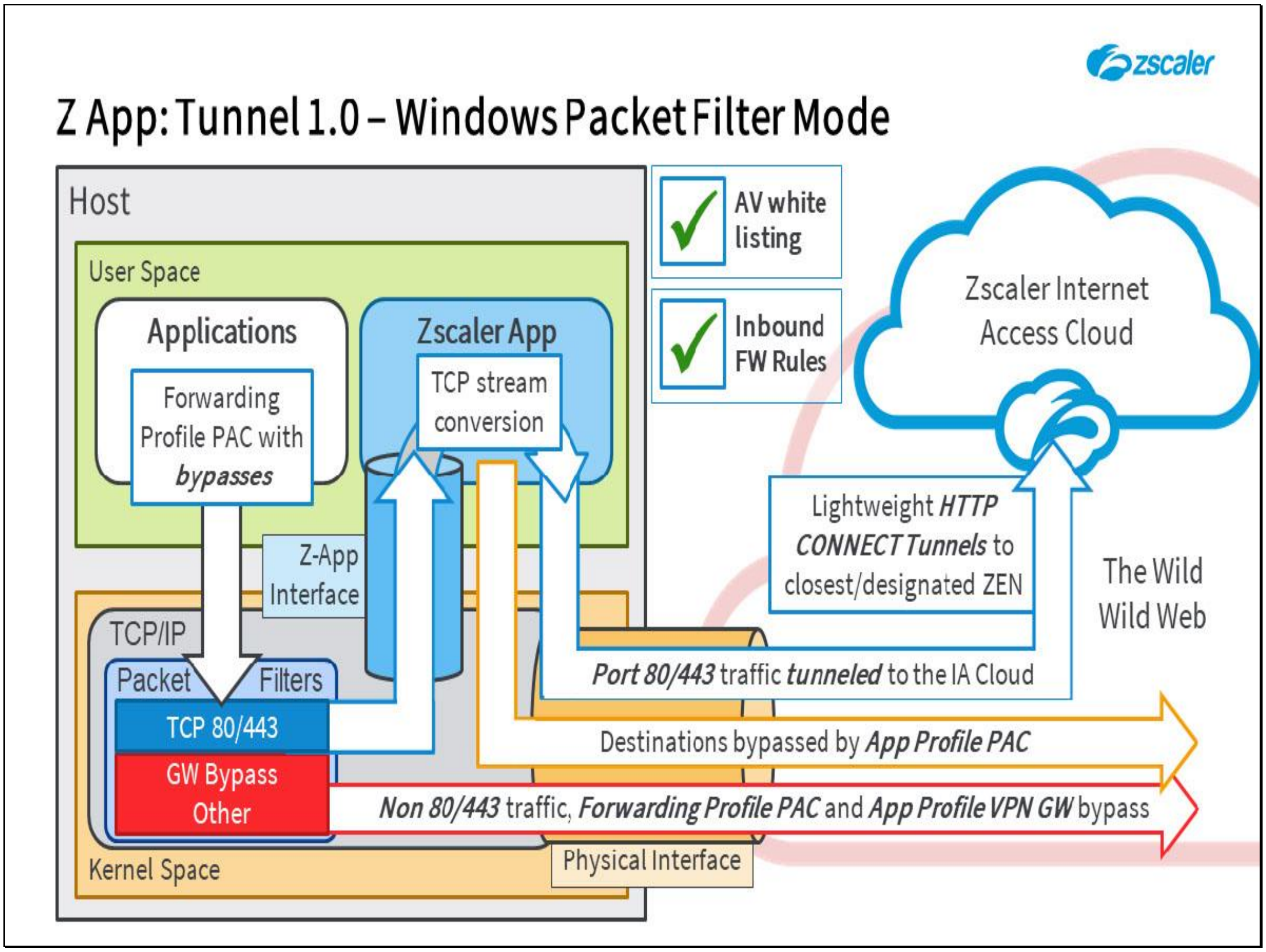
Slide 18 - Z App: Tunnel 1.0 – Route Mode Whitelisting


zscaler
Z App: Tunnel 1.0 – Route Mode Whitelisting
Host
User Space
Applications
Forwarding Profile PAC with *bypasses*
Zscaler App
TCP stream conversion
Z-App Interface
Default Route
TCP/IP
Routing
Kernel Space
Physical Interface
AV white listing
Inbound FW Rules
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
Port 80/443 traffic *tunneled* to the IA Cloud
Non 80/443 traffic and destinations bypassed by *App Profile PAC*
Forwarding Profile PAC bypasses and *App Profile VPN GW* bypass

Slide notes

The App needs to be white listed by any AV software installed on the host machine, and for **Tunnel 1.0** mode an inbound Firewall rule for all protocols and ports is required (because of the stream conversion).

Slide 19 - Z App: Tunnel 1.0 – Windows Packet Filter Mode



Z App: Tunnel 1.0 – Windows Packet Filter Mode

zscaler
Host
User Space
Applications
Forwarding Profile PAC with *bypasses*
Zscaler App
TCP stream conversion
Z-App Interface
TCP/IP
Packet Filters
TCP 80/443
GW Bypass Other
Kernel Space
AV white listing
Inbound FW Rules
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
Port 80/443 traffic *tunneled* to the IA Cloud
Destinations bypassed by *App Profile PAC*
Non 80/443 traffic, *Forwarding Profile PAC* and *App Profile VPN GW* bypass
Physical Interface

Slide notes

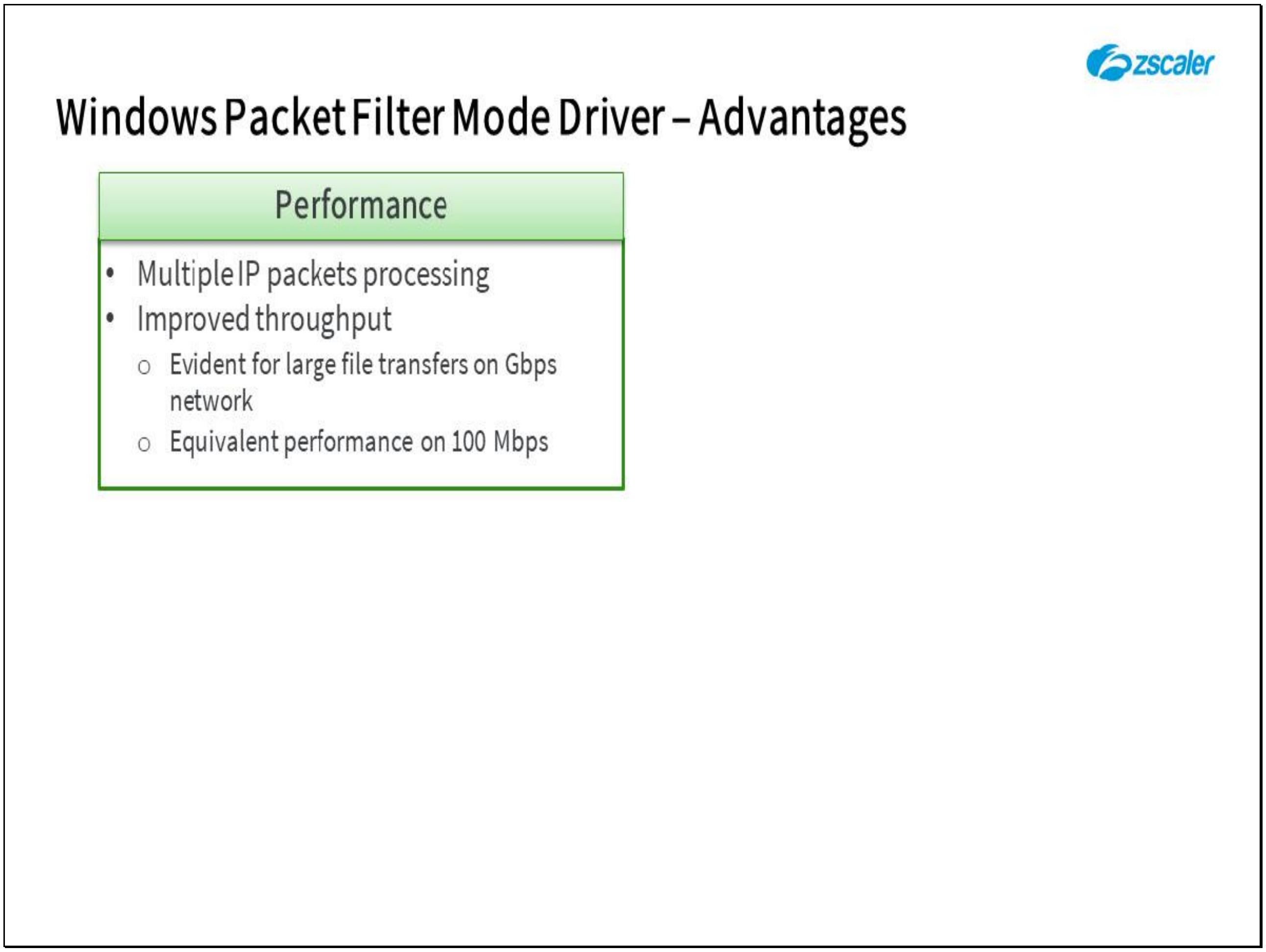
On Windows devices, with the **Packet Filter Based** driver enabled, there is no longer any need for Zscaler App to add a default, or any other route within the TCP/IP stack; what the driver uses instead is a set of Zscaler installed redirect filters. Filters are provided for:

- **TCP 80/443** traffic (to be converted to a stream and tunneled to the Zscaler Internet Access service);
- Any **VPN GW Bypasses** configured in the **App Profile**;
- The **100.64.0.0/16** subnet and any specific application IP addresses required by ZPA;
- Plus, some additional filters for local packet routing.

Traffic that does not match any of the filters or matches an explicit 'direct' filter (such as a VPN gateway), will be forwarded to the network through the physical interface without being processed by the App, as will any bypasses specified in the **Forwarding Profile** proxy settings. For the ZIA service, this includes all DNS traffic.

Destinations added as bypasses in the **App Profile** PAC file, will be processed by and forwarded directly by the App.

Slide 20 - Windows Packet Filter Mode Driver – Advantages



Windows Packet Filter Mode Driver – Advantages

Performance

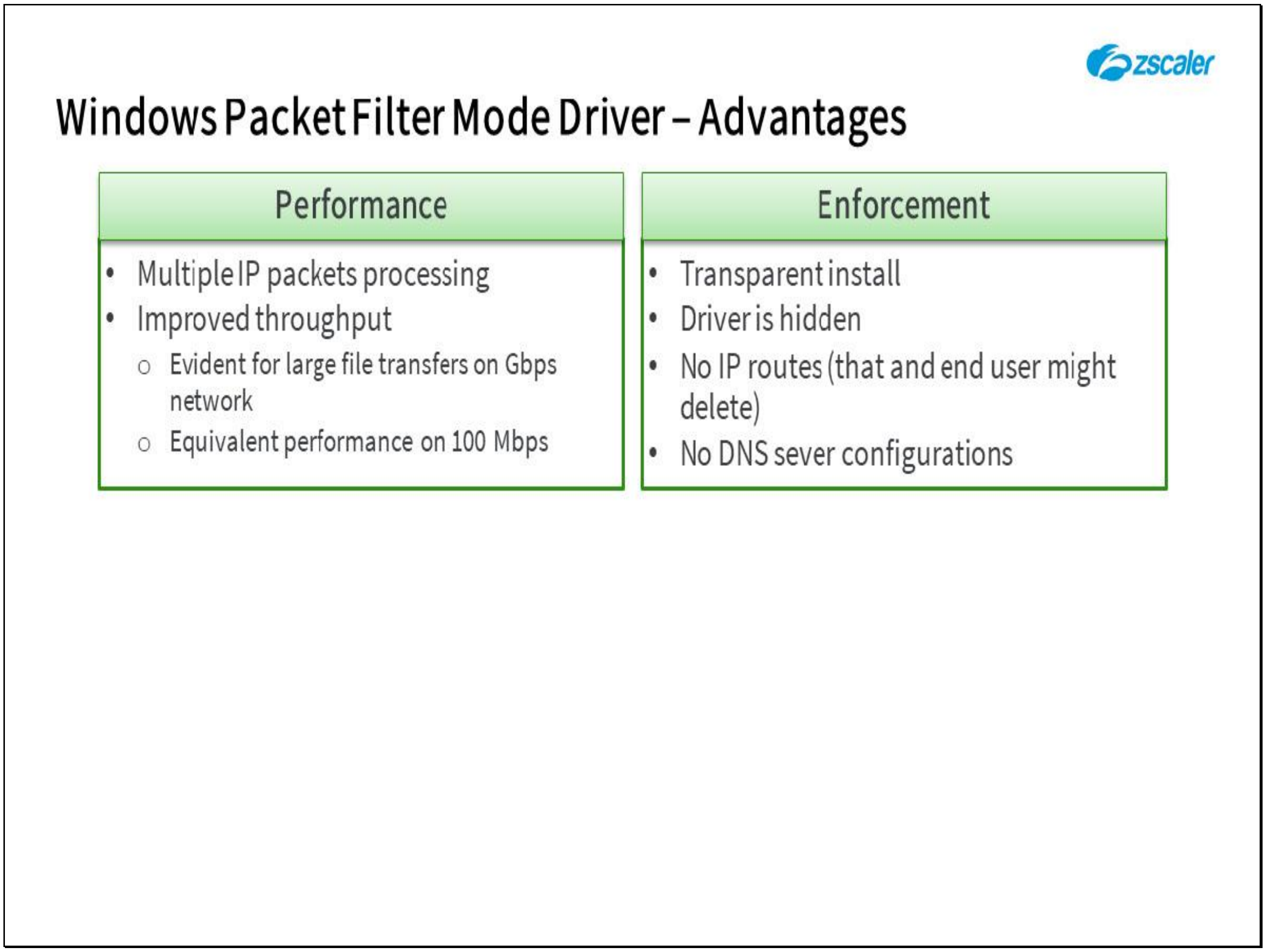
- Multiple IP packets processing
- Improved throughput
  - Evident for large file transfers on Gbps network
  - Equivalent performance on 100 Mbps

Slide notes

The advantages of Zscaler’s **Packet Filter Based** driver for the Windows platform include:

- **Performance improvements** - the **Packet Filter Based** driver reads multiple IP packets in single read call to have best throughput. The throughput difference between **Packet Filter Based** and regular **Route Based** driver can be easily seen when transferring a large file on a Gigabit network connection, on a slower network (<100 Mbps) performance is about the same as for the **Route Based** driver.

Slide 21 - Windows Packet Filter Mode Driver – Advantages



zscaler

Windows Packet Filter Mode Driver – Advantages

Performance

- Multiple IP packets processing
- Improved throughput
  - Evident for large file transfers on Gbps network
  - Equivalent performance on 100 Mbps

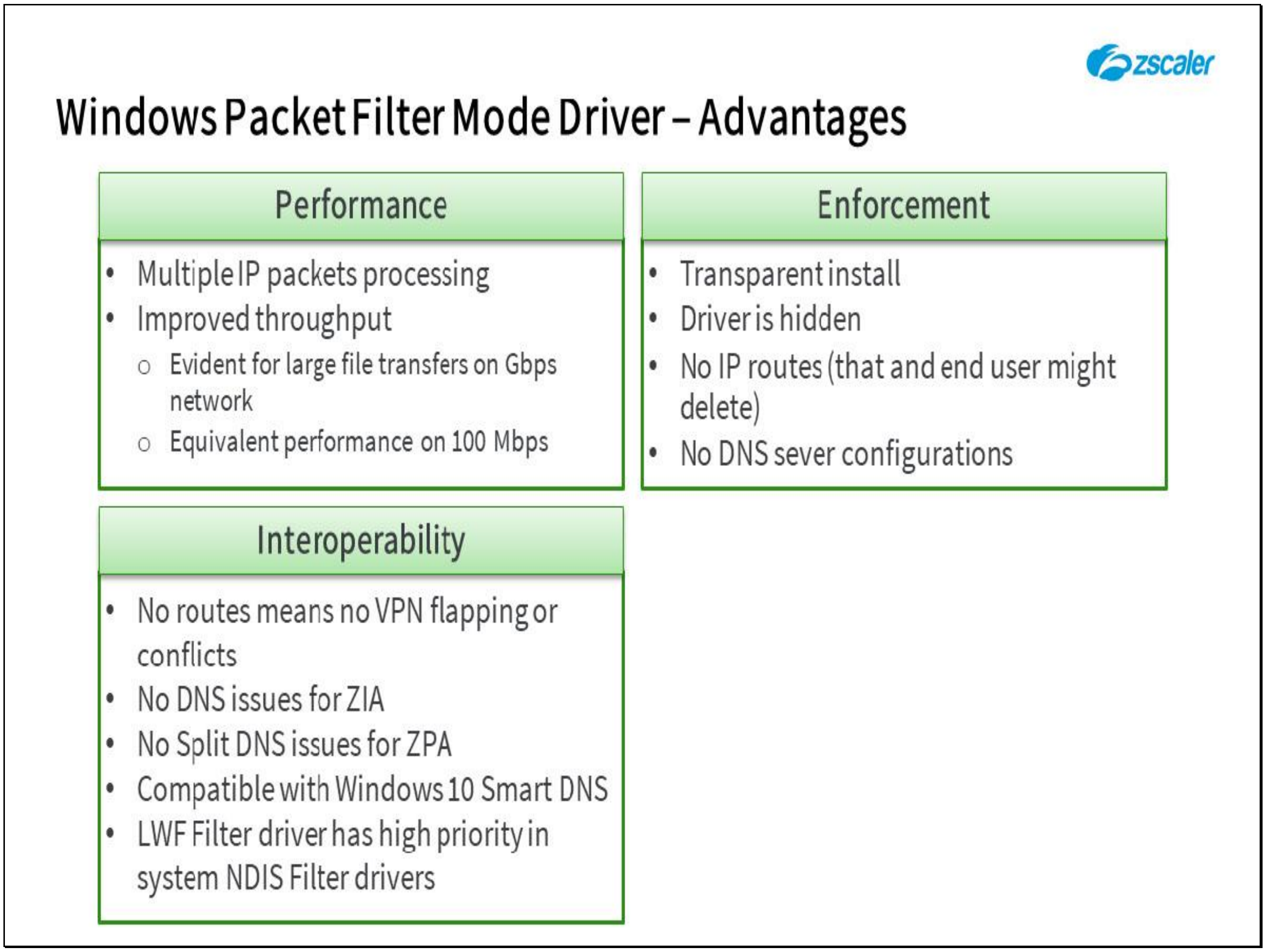
Enforcement

- Transparent install
- Driver is hidden
- No IP routes (that and end user might delete)
- No DNS sever configurations

Slide notes

- **Better enforcement** - The **Packet Filter Based** driver is installed transparently and is hidden, so it is not visible to an end user and cannot be uninstalled. It does not install any IP routes (so an end user can’t bypass Zscaler by deleting routes), nor does it install any DNS server configurations (so an end user cannot manipulate the DNS entries either).

Slide 22 - Windows Packet Filter Mode Driver – Advantages



Windows Packet Filter Mode Driver – Advantages

Performance

- Multiple IP packets processing
- Improved throughput
  - Evident for large file transfers on Gbps network
  - Equivalent performance on 100 Mbps

Enforcement

- Transparent install
- Driver is hidden
- No IP routes (that and end user might delete)
- No DNS sever configurations

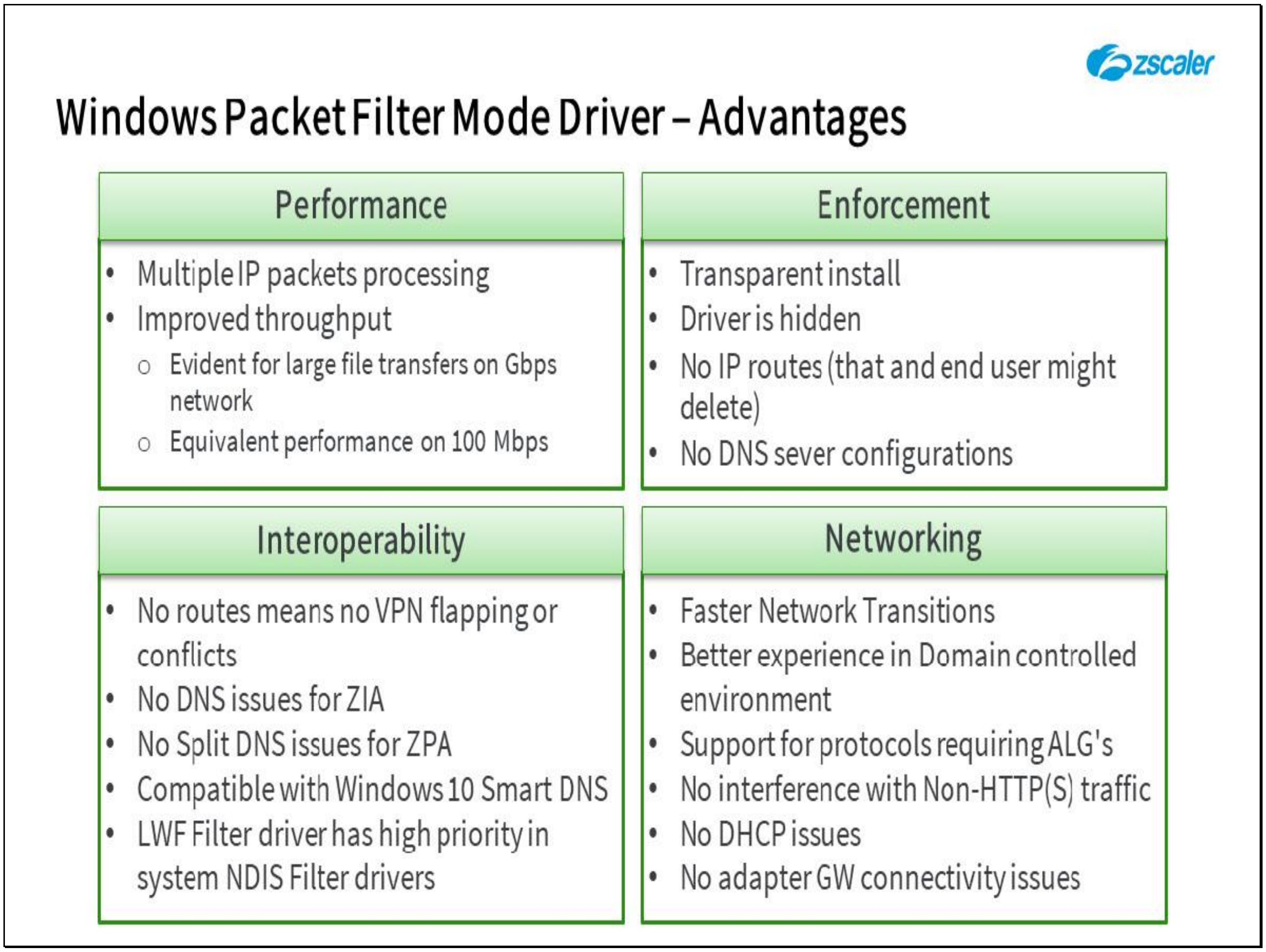
Interoperability

- No routes means no VPN flapping or conflicts
- No DNS issues for ZIA
- No Split DNS issues for ZPA
- Compatible with Windows 10 Smart DNS
- LWF Filter driver has high priority in system NDIS Filter drivers

Slide notes

- **Improved interoperability** - As there are no IP routes or DNS servers set on the system, this protects against VPN flapping issues due to route change events or conflicts between the different VPN routes. For the ZIA service, the **Packet Filter Based** driver does not even intercept DNS requests, so there is no possibility for DNS issues (e.g. split DNS problems), nor is there any need to disable the Smart DNS capability on Windows 10 for the ZPA service.

Slide 23 - Windows Packet Filter Mode Driver – Advantages



Windows Packet Filter Mode Driver – Advantages

Performance

- Multiple IP packets processing
- Improved throughput
  - Evident for large file transfers on Gbps network
  - Equivalent performance on 100 Mbps

Enforcement

- Transparent install
- Driver is hidden
- No IP routes (that and end user might delete)
- No DNS sever configurations

Interoperability

- No routes means no VPN flapping or conflicts
- No DNS issues for ZIA
- No Split DNS issues for ZPA
- Compatible with Windows 10 Smart DNS
- LWF Filter driver has high priority in system NDIS Filter drivers

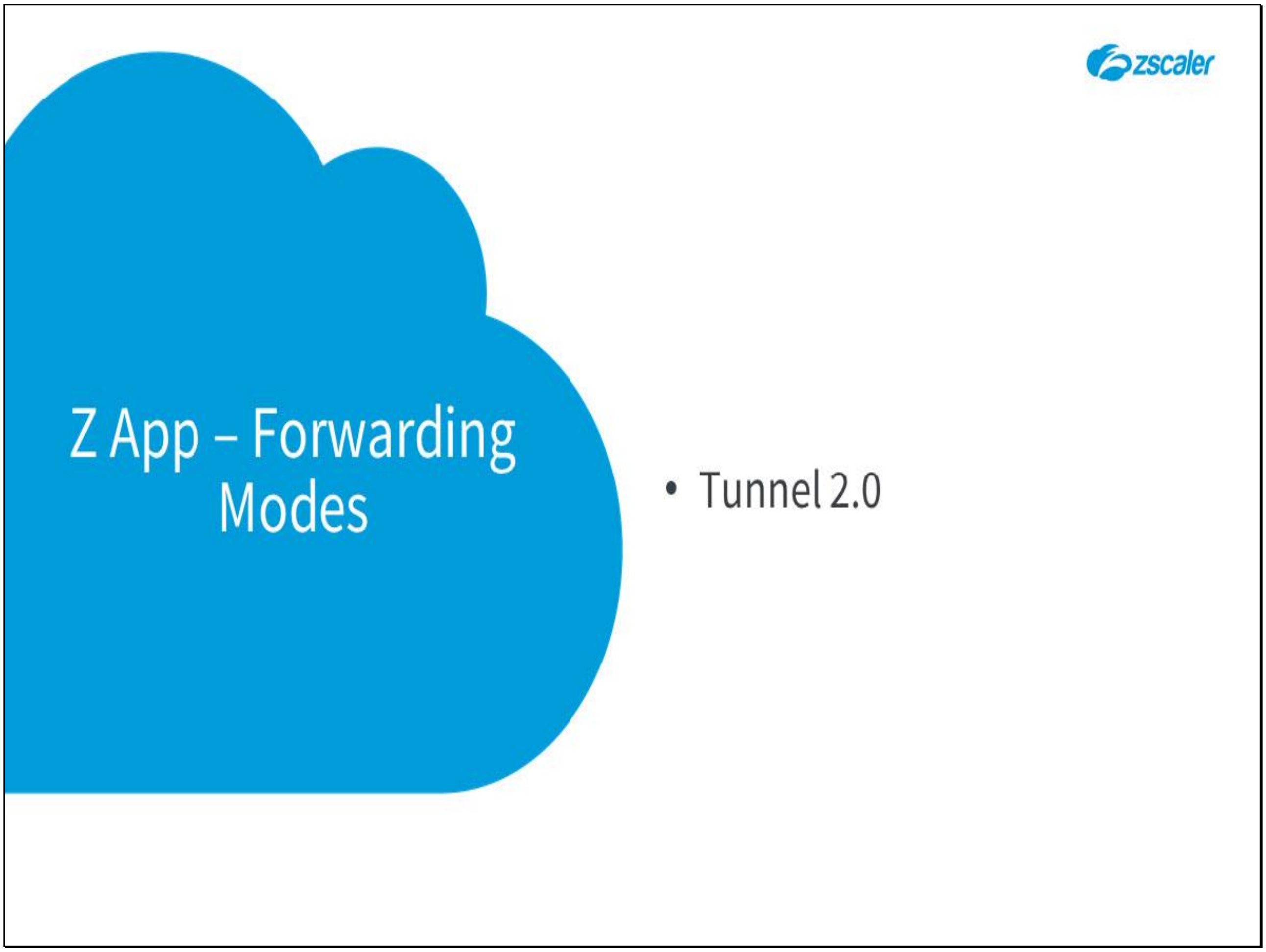
Networking

- Faster Network Transitions
- Better experience in Domain controlled environment
- Support for protocols requiring ALG's
- No interference with Non-HTTP(S) traffic
- No DHCP issues
- No adapter GW connectivity issues

Slide notes

- **Improved network functionality** - With:
  - Faster network transitions are possible, as the **Packet Filter Based** driver requires much less time to initialize and there are no delays waiting to add or delete routes;
  - A better experience in Domain controlled environments, as an end user will not experience issues such as the adapter not joining or leaving the domain;
  - Support for protocols requiring Application Layer Gateways (ALG), such as active-mode FTP and SIP (although note that as ZPA does not support ALG initiated connections, these protocols will still not work over ZPA);
  - The Zscaler App will not even process non-TCP:80/443 packet flows, which also results in fewer socket connections used by Z App;
  - No DHCP issues as Zscaler App will not interference with DHCP packets;
  - Plus, no adapter gateway related connectivity issues, such as Office activation, or Windows App Store connectivity issues.

Slide 24 - Zscaler App – Forwarding Modes



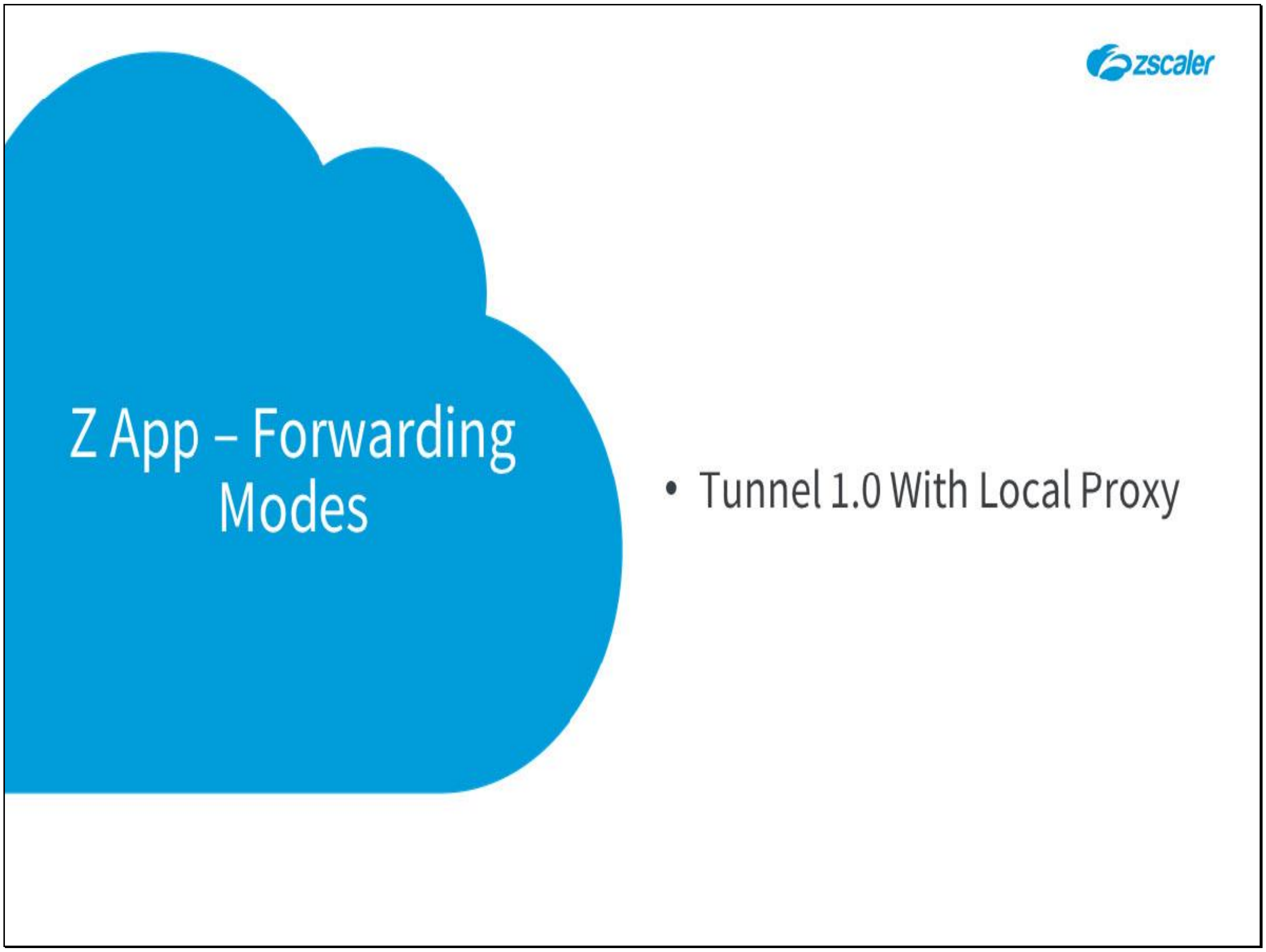
Z App – Forwarding Modes

- Tunnel 2.0

Slide notes

The next forwarding mode would be **Tunnel 2.0**, however we will deal with that option in a separate module of this course.

Slide 25 - Z App – Forwarding Modes



zscaler

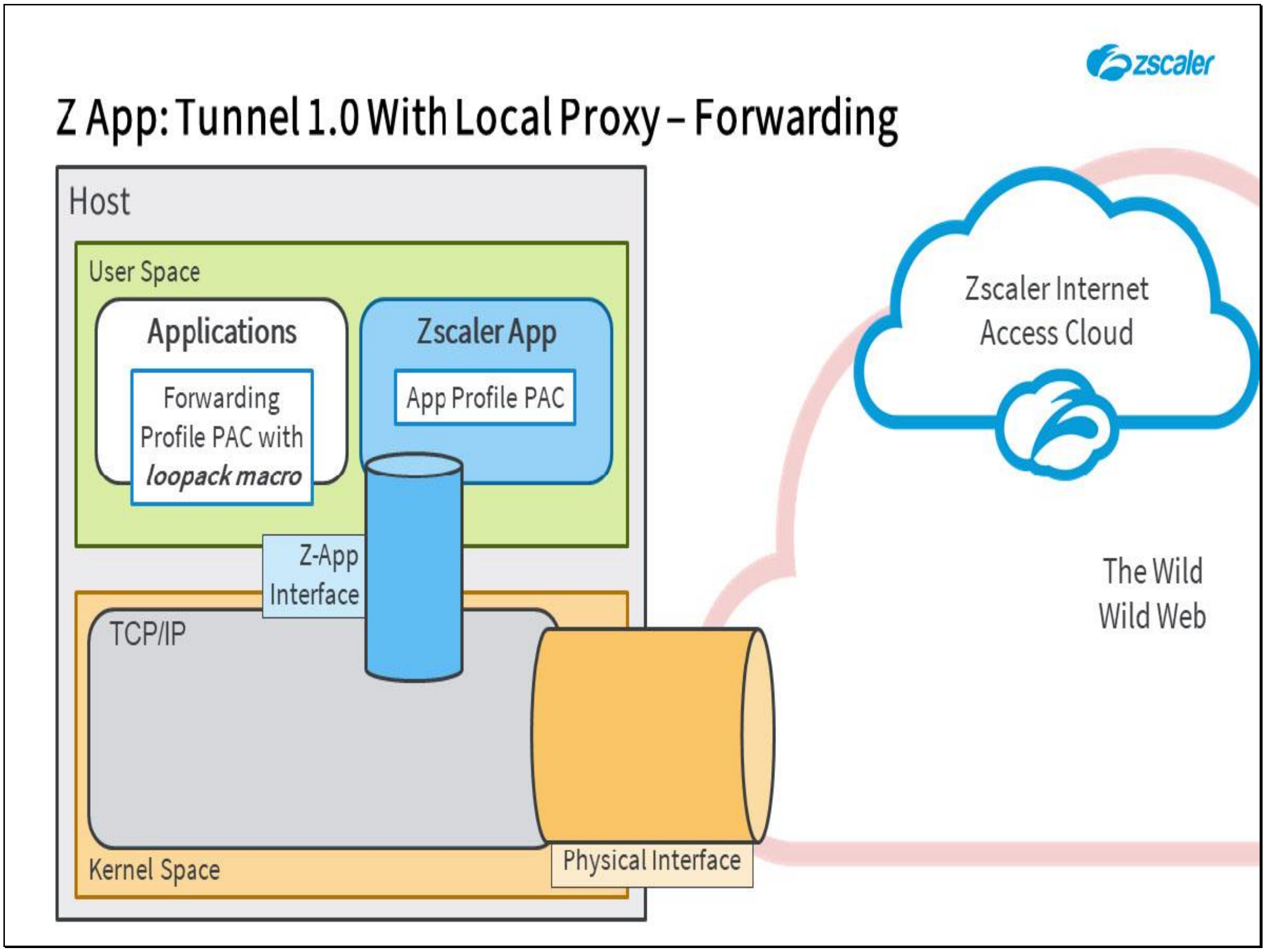
Z App – Forwarding Modes

- Tunnel 1.0 With Local Proxy

Slide notes

The next forwarding mode we will look at is **Tunnel (1.0) With Local Proxy** (**TWLP**).

Slide 26 - Z App: Tunnel 1.0 With Local Proxy – Forwarding



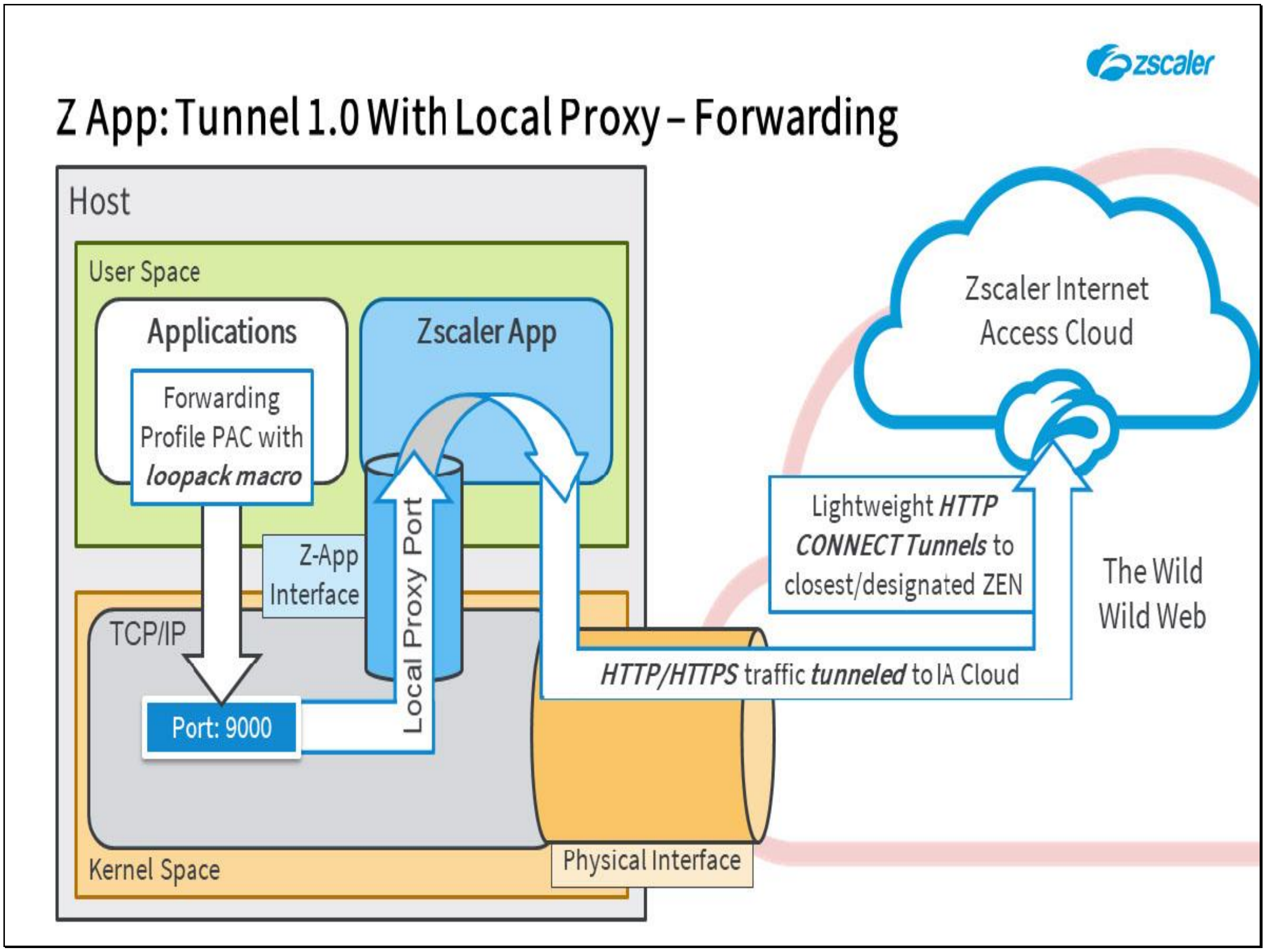
Slide notes

This mode does not use routing to identify traffic to be tunneled, it uses the local loopback proxy macro applied in the Zscaler default or in a custom **Forwarding Profile** PAC file, to forward traffic into the Zscaler App.

With this mode, if you choose to apply a custom PAC file, that file must contain either the gateway macro function **${ZAPP_LOCAL_PROXY}** as the destination (which is recommended), or a static loopback configuration with the correct port (e.g. **127.0.0.1:9000**). The port the App is to listen on can be configured through the Zscaler App Portal (defaults to **9000**).

Note that a custom **Forwarding Profile** PAC file is only required if you have specific traffic that is to be bypassed by the app. If you don't specify a custom PAC file, the Zscaler App automatically sets the system PAC settings to **http://127.0.0.1:9000/localproxy.pac**, this PAC file contains the loopback configuration.

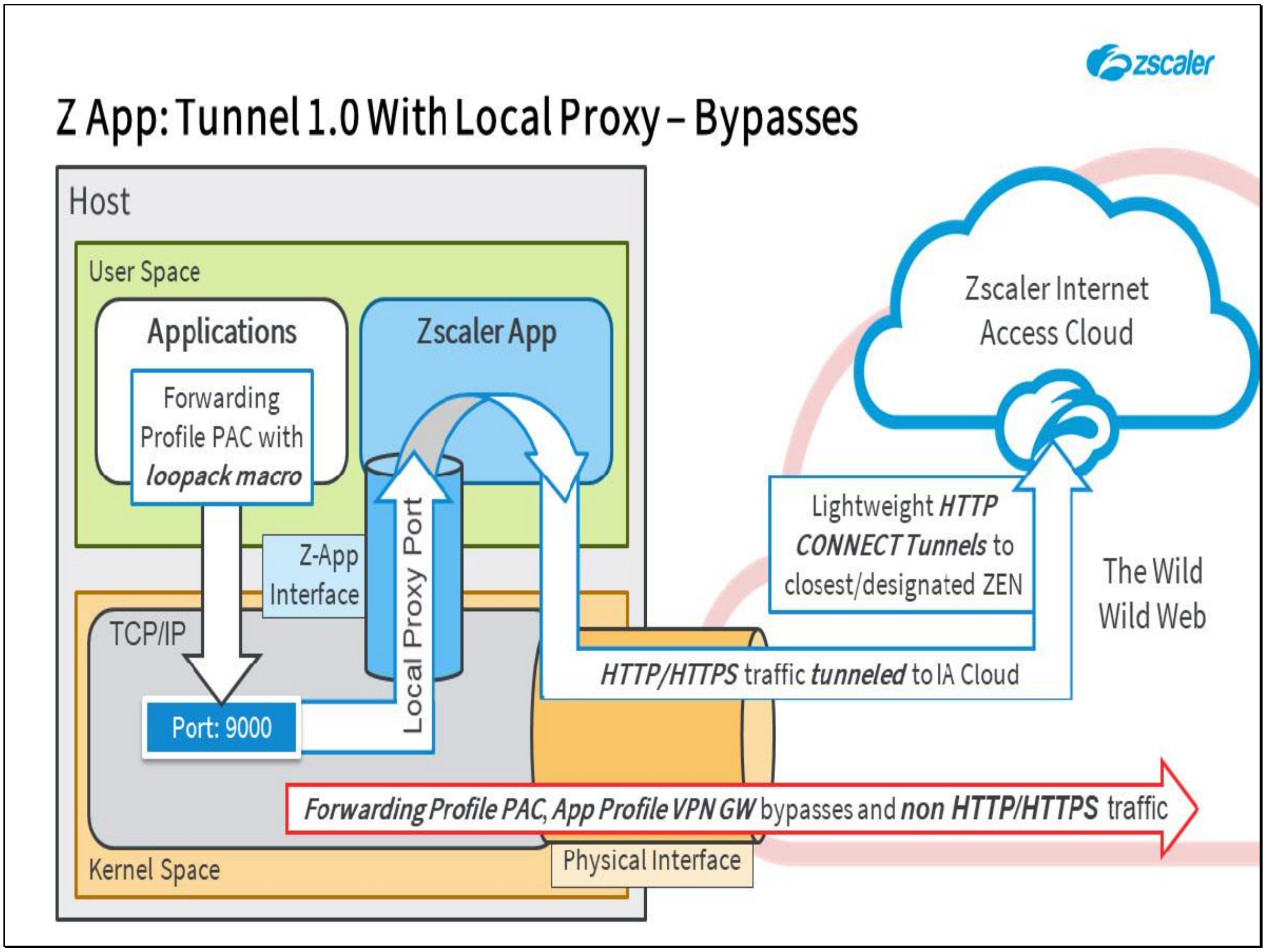
Slide 27 - Z App: Tunnel 1.0 With Local Proxy – Forwarding


zscaler
Z App: Tunnel 1.0 With Local Proxy – Forwarding
Host
User Space
Applications
Forwarding Profile PAC with *loopack macro*
Zscaler App
Z-App Interface
Local Proxy Port
TCP/IP
Port: 9000
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
HTTP/HTTPS traffic *tunneled* to IA Cloud
The Wild Wild Web

Slide notes

In this mode, only traffic that follows the proxy definition (which means **HTTP**/**HTTPS**) will be will be tunneled to either the closest ZEN, or the ZEN specified in the **App Profile** PAC file, although regardless of the destination port specified by the end user (so not only port **80** and **443**). Only the **Tunnel 1.0** method is supported in this mode, meaning unencrypted, lightweight **HTTP CONNECT** tunnels on destination port **443**.

Slide 28 - Z App: Tunnel 1.0 With Local Proxy – Bypasses



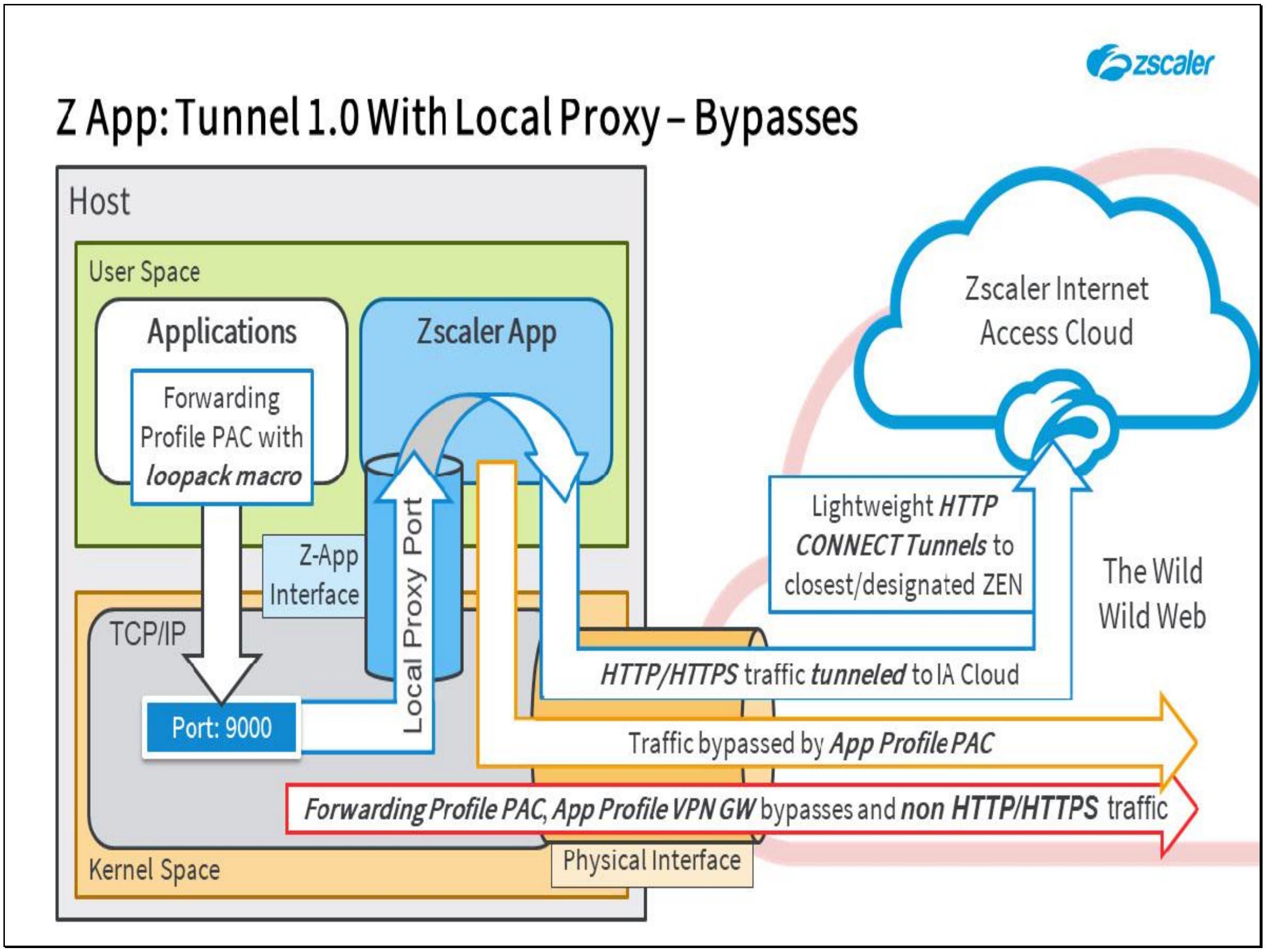
Z App: Tunnel 1.0 With Local Proxy – Bypasses

zscaler
Host
User Space
Applications
Forwarding Profile PAC with *loopack macro*
Zscaler App
Z-App Interface
Local Proxy Port
TCP/IP
Port: 9000
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
HTTP/HTTPS traffic ***tunneled*** to IA Cloud
Forwarding Profile PAC, App Profile VPN GW bypasses and **non HTTP/HTTPS** traffic

Slide notes

Traffic that does not follow the proxy settings will be sent directly to the physical interface, plus it is also possible to bypass the Zscaler App completely by configuring bypasses in the proxy settings applied by the **Forwarding Profile**.

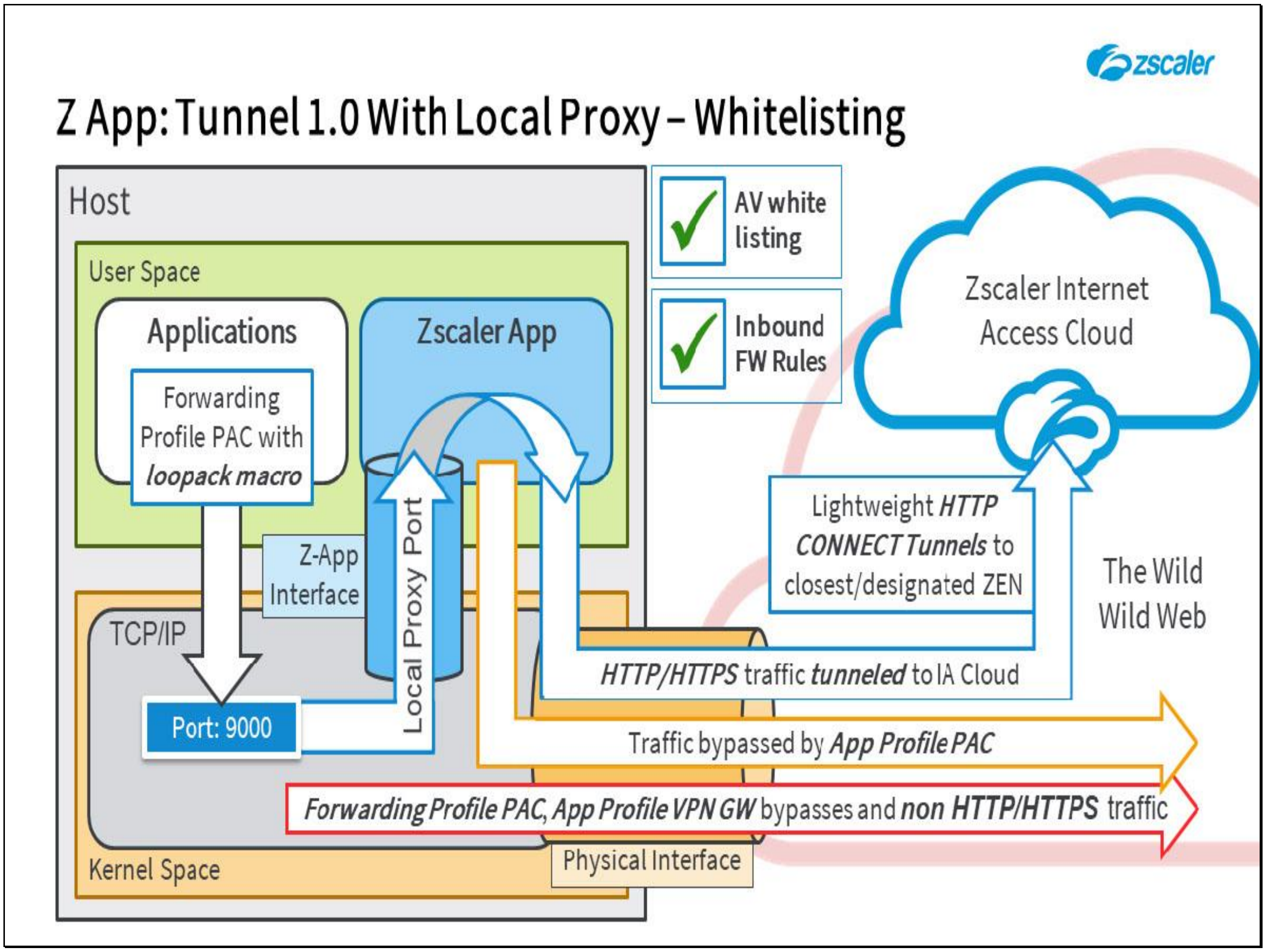
Slide 29 - Z App: Tunnel 1.0 With Local Proxy – Bypasses


zscaler
Z App: Tunnel 1.0 With Local Proxy – Bypasses
Host
User Space
Applications
Forwarding Profile PAC with *loopack macro*
Zscaler App
Z-App Interface
Local Proxy Port
TCP/IP
Port: 9000
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
HTTP/HTTPS traffic *tunneled* to IA Cloud
Traffic bypassed by *App Profile PAC*
Forwarding Profile PAC, App Profile VPN GW bypasses and *non HTTP/HTTPS* traffic

Slide notes

As with the route mode tunnels, the PAC file applied in the **App Profile** can also be used to define bypass destinations to ensure that traffic for them is sent direct by the App.

Slide 30 - Z App: Tunnel 1.0 With Local Proxy – Whitelisting



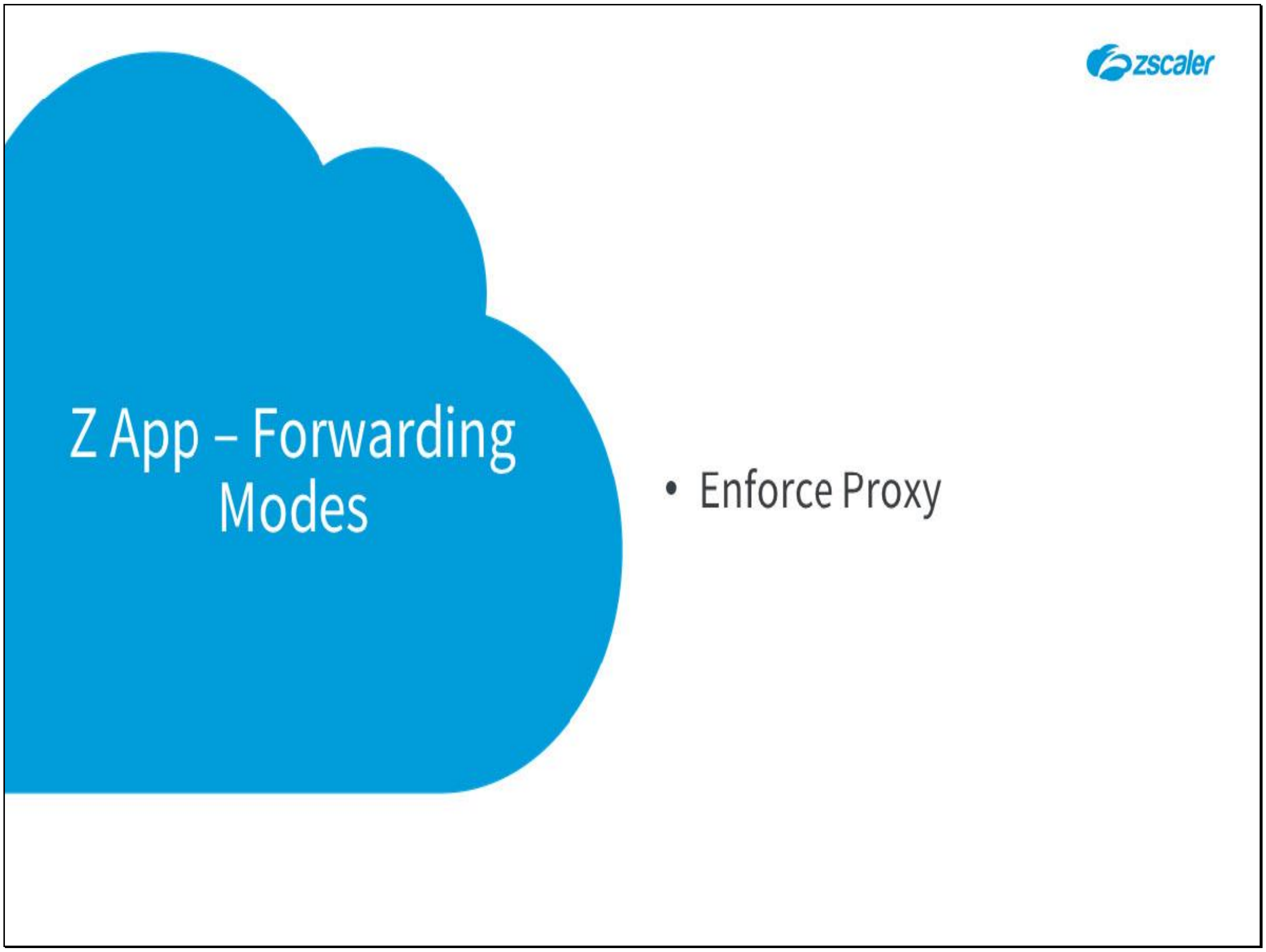
Z App: Tunnel 1.0 With Local Proxy – Whitelisting

zscaler
Host
User Space
Applications
Forwarding Profile PAC with *loopack macro*
Zscaler App
Z-App Interface
Local Proxy Port
TCP/IP
Port: 9000
Kernel Space
Physical Interface
AV white listing
Inbound FW Rules
Zscaler Internet Access Cloud
Lightweight *HTTP CONNECT Tunnels* to closest/designated ZEN
The Wild Wild Web
HTTP/HTTPS traffic *tunneled* to IA Cloud
Traffic bypassed by *App Profile PAC*
Forwarding Profile PAC, App Profile VPN GW bypasses and **non HTTP/HTTPS** traffic

Slide notes

As before, the App needs to be white listed by any AV software installed on the host machine, plus for this mode an inbound Firewall rule may be needed, to allow loopback communication on the appropriate port (e.g. **127.0.0.1:9000**).

Slide 31 - Zscaler App – Forwarding Modes



zscaler

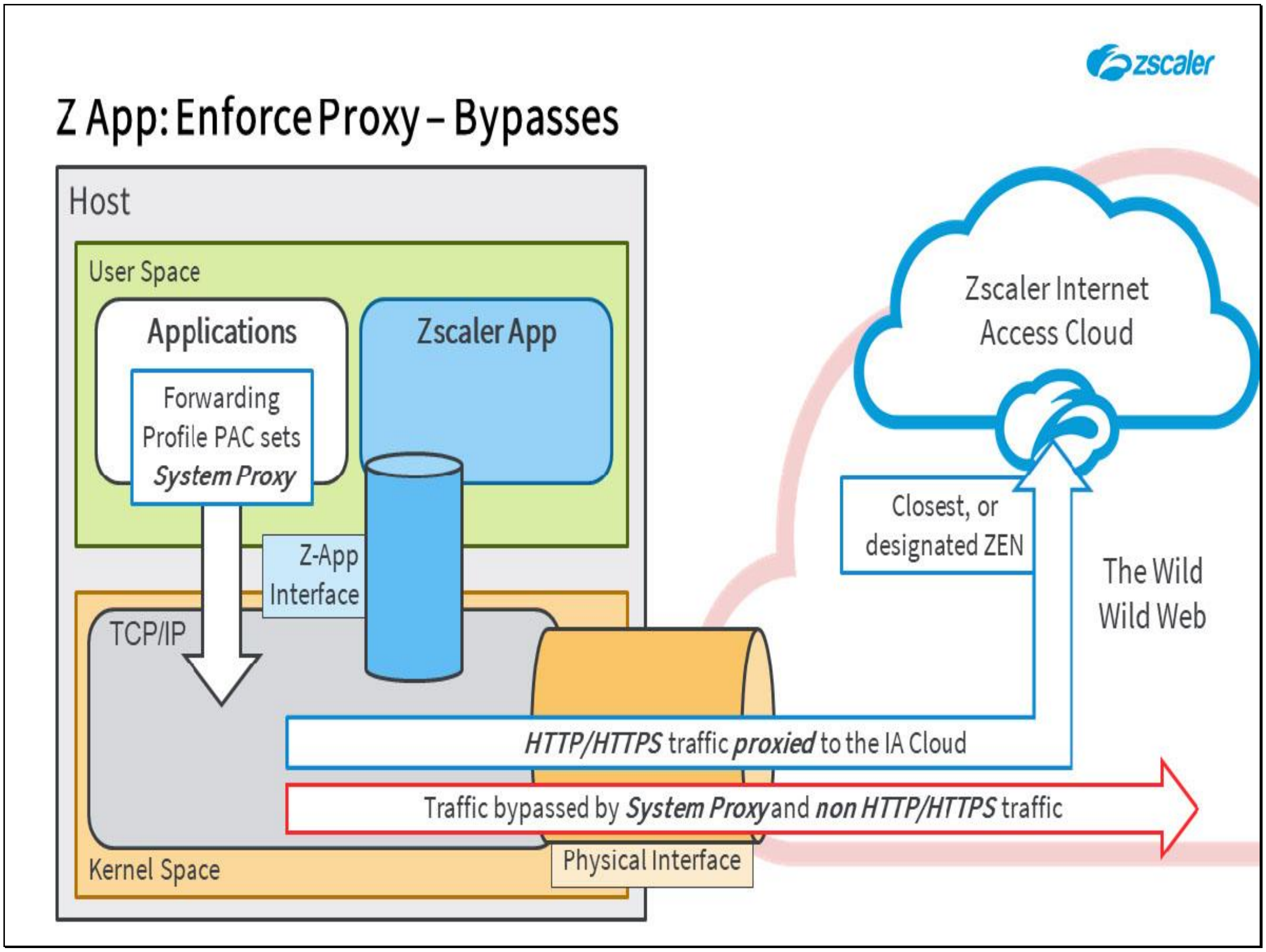
Z App – Forwarding Modes

- Enforce Proxy

Slide notes

The next forwarding mode we will look at is **Enforce Proxy**.

Slide 32 - Z App: Enforce Proxy – Bypasses



Z App: Enforce Proxy – Bypasses

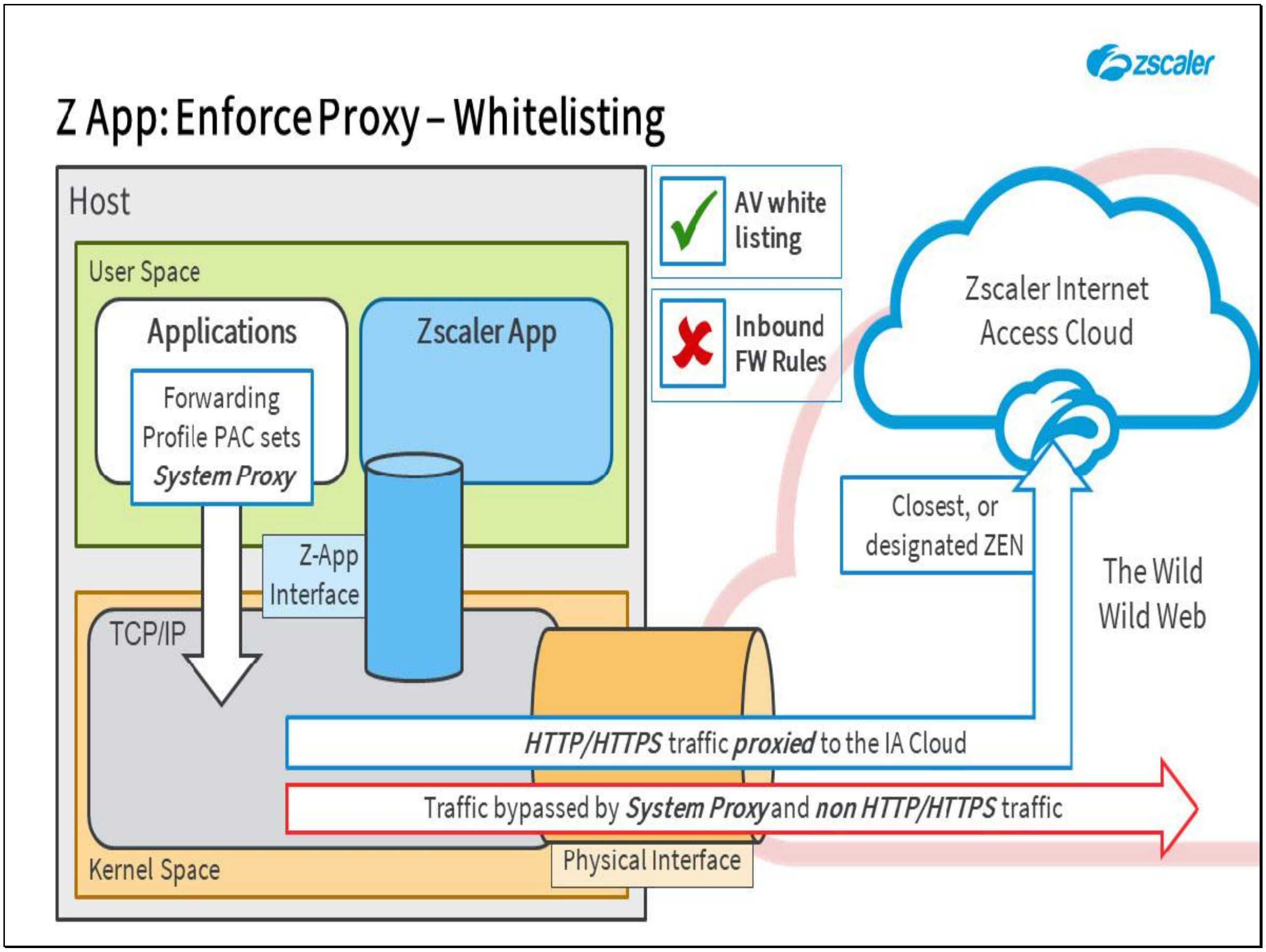
zscaler
Host
User Space
Applications
Forwarding Profile PAC sets *System Proxy*
Zscaler App
Z-App Interface
TCP/IP
Kernel Space
Physical Interface
Zscaler Internet Access Cloud
Closest, or designated ZEN
The Wild Wild Web
HTTP/HTTPS traffic *proxied* to the IA Cloud
Traffic bypassed by *System Proxy* and *non HTTP/HTTPS* traffic

Slide notes

In the **Enforce Proxy** mode, no tunnels are established by Zscaler App at all. In this mode the App is used simply to control what proxy configuration is applied to or removed from the system, ...and it is the proxy settings that defines whether traffic is to be proxied to Zscaler, or whether it is to go direct. If traffic is proxied, it will be sent to either the closest or to a ZEN designated in the PAC file applied.

Note that, as no tunnels are used in this mode, the **App Profile** PAC file is not used at all.

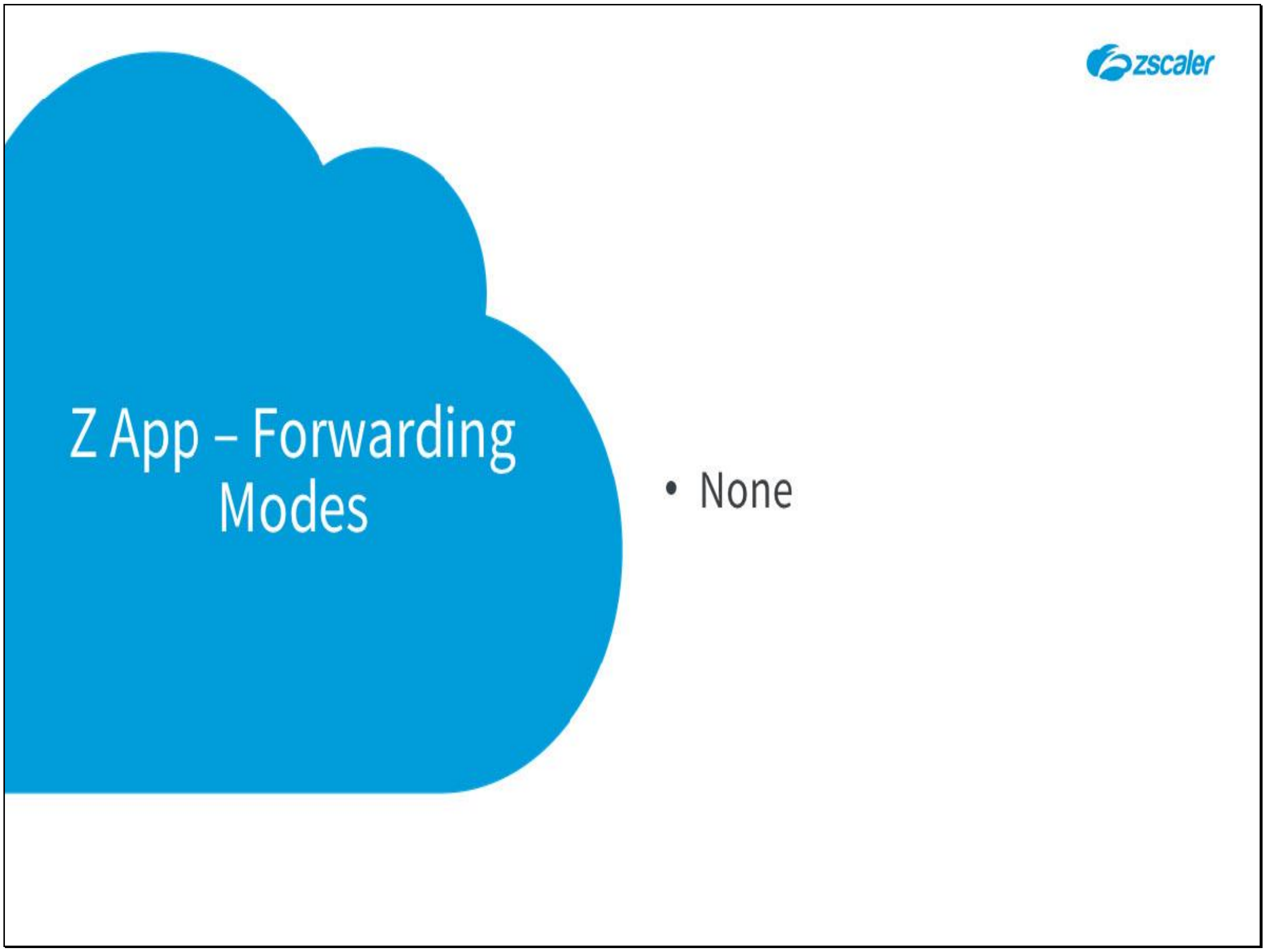
Slide 33 - Z App: Enforce Proxy – Whitelisting


zscaler
Z App: Enforce Proxy – Whitelisting
Host
User Space
Applications
Forwarding Profile PAC sets *System Proxy*
Zscaler App
Z-App Interface
TCP/IP
Kernel Space
Physical Interface
✓ AV white listing
✗ Inbound FW Rules
Zscaler Internet Access Cloud
Closest, or designated ZEN
The Wild Wild Web
HTTP/HTTPS traffic *proxied* to the IA Cloud
Traffic bypassed by *System Proxy* and *non HTTP/HTTPS* traffic

Slide notes

As before, the App needs to be white listed by any AV software installed on the host machine, however for this mode no inbound Firewall rules are required.

Slide 34 - Zscaler App – Forwarding Modes



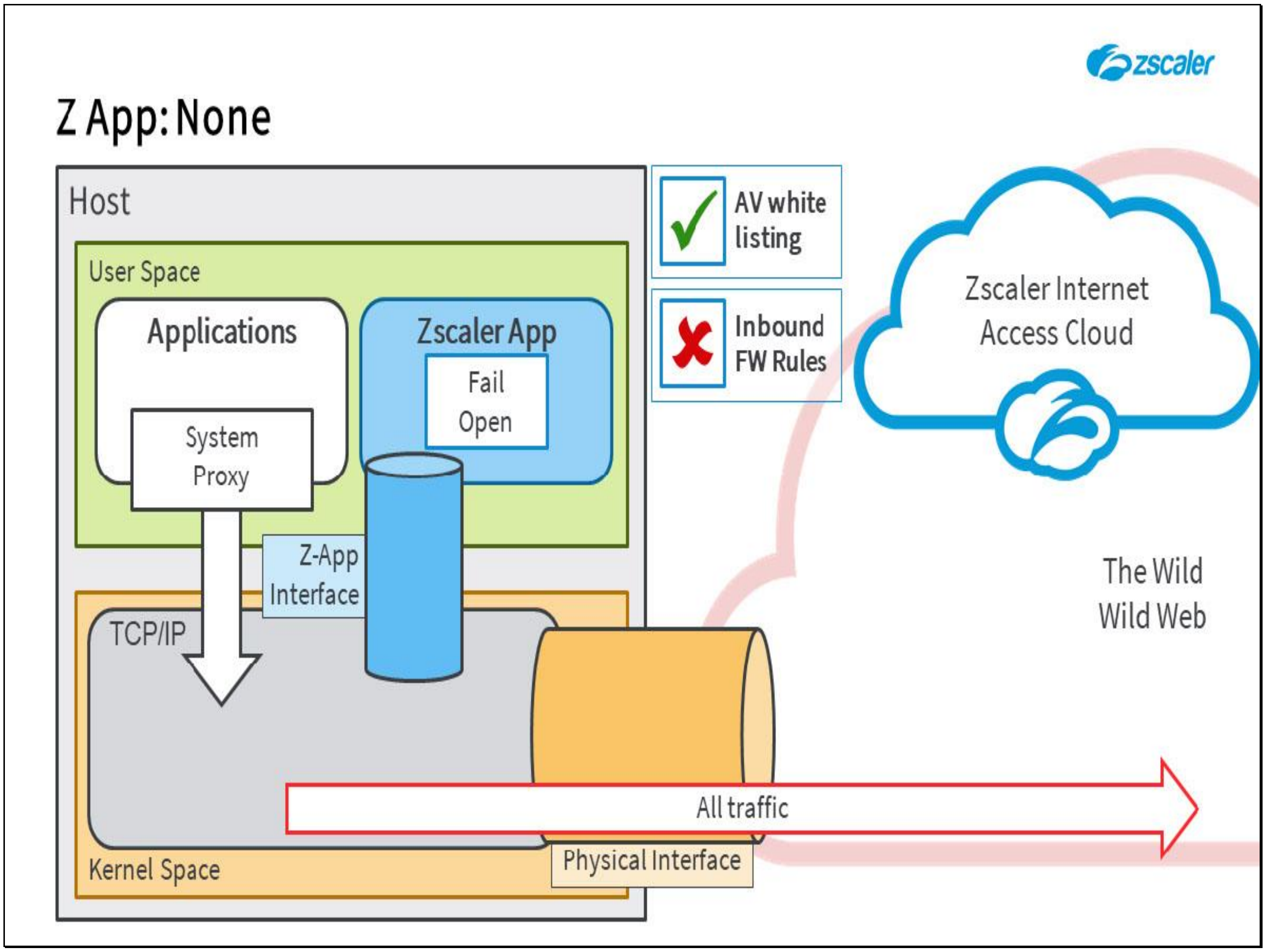
Z App – Forwarding Modes

- None

Slide notes

The last forwarding mode available is the **None** mode.

Slide 35 - Z App: None



Slide notes

If the App is set to the **None** mode, it is essentially in fail open mode and takes no part in the forwarding of traffic. The App still needs to be white listed by any AV software installed on the host machine, although no inbound Firewall rules are required.

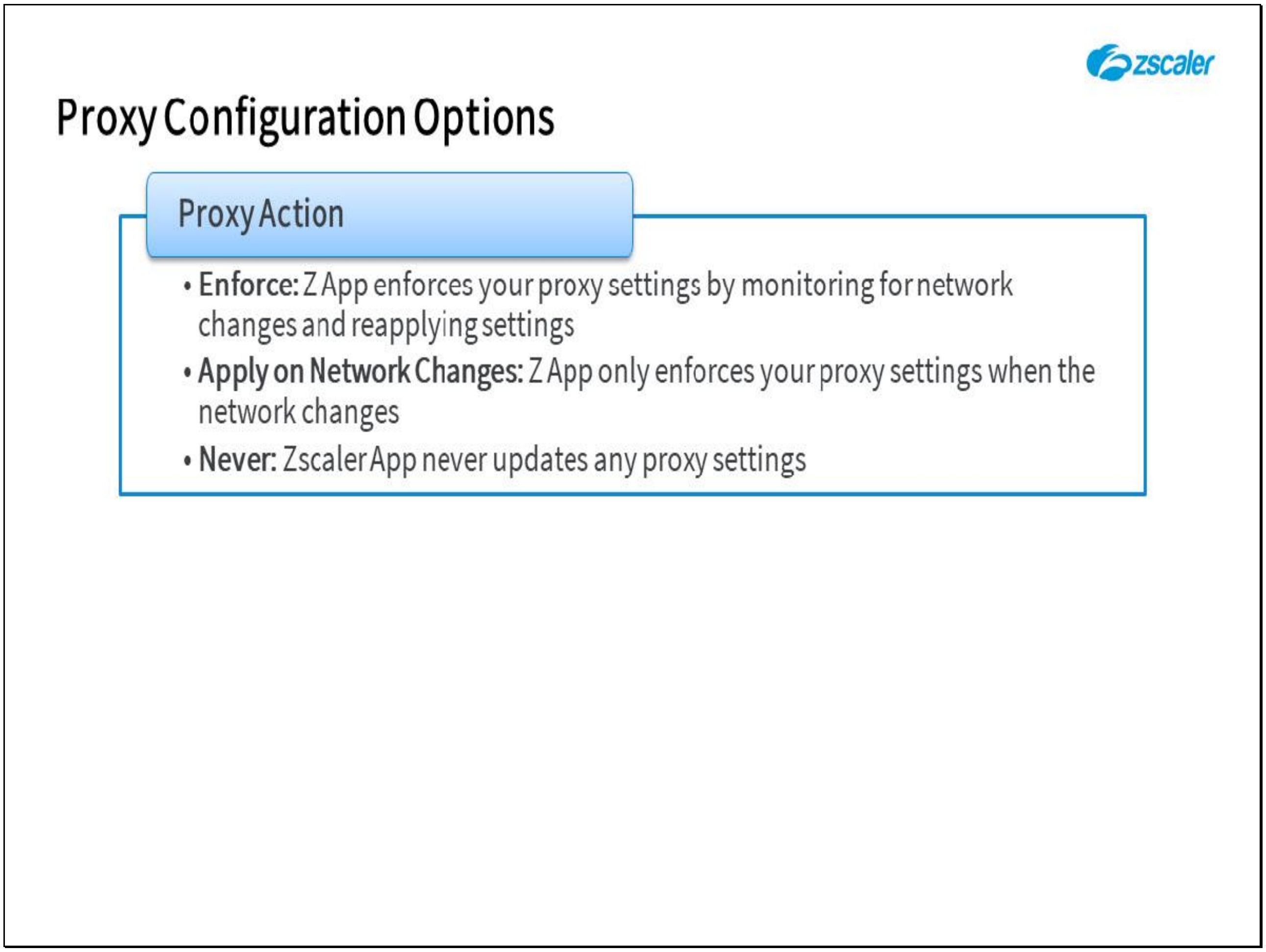
Slide 36 - App Profile PAC File – Adding Multiple ZENs

System Proxy Settings

Slide notes

The next topic that we will cover is a look at the **System Proxy Settings** available for each of the forwarding modes.

Slide 37 - Proxy Configuration Options



Proxy Configuration Options

Proxy Action

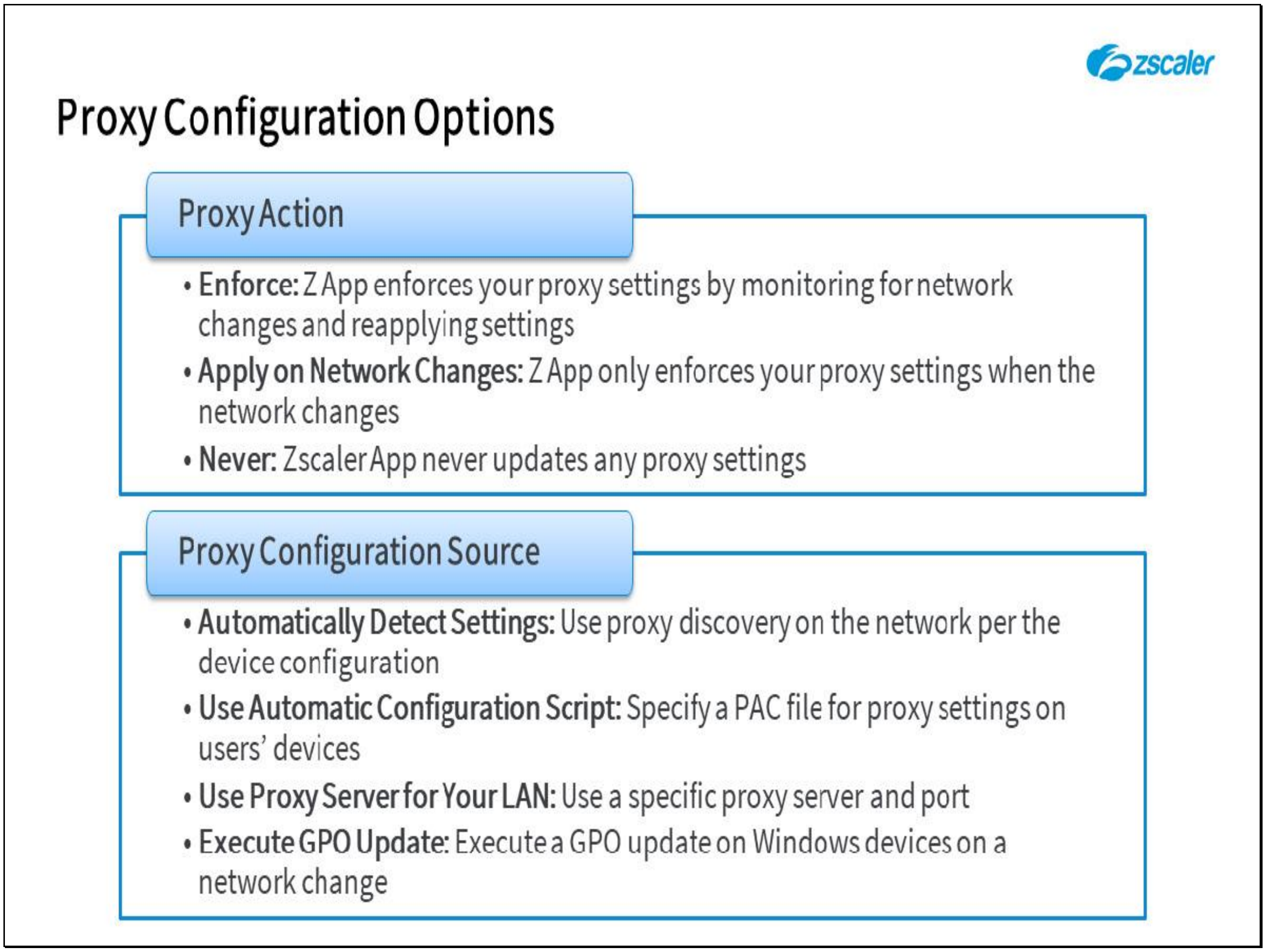
- **Enforce:** Z App enforces your proxy settings by monitoring for network changes and reapplying settings
- **Apply on Network Changes:** Z App only enforces your proxy settings when the network changes
- **Never:** Zscaler App never updates any proxy settings

Slide notes

Depending which forwarding mode you select for the ZIA service though Zscaler App, you will have options in the **Forwarding Profile** for configuring **System Proxy Settings**. The full set of **Proxy Action** options available are:

- **Enforce** - Zscaler App enforces your proxy settings by monitoring for network changes and reapplying settings when necessary, because of this Z App can ensure that users cannot tamper with their proxy settings;
- **Apply on Network Changes** - Z App only enforces your proxy settings when the network changes, it does not monitor for proxy change afterward;
- **Never** - Zscaler App never updates any proxy settings.

Slide 38 - Proxy Configuration Options



Proxy Configuration Options

Proxy Action

- **Enforce:** Z App enforces your proxy settings by monitoring for network changes and reapplying settings
- **Apply on Network Changes:** Z App only enforces your proxy settings when the network changes
- **Never:** Zscaler App never updates any proxy settings

Proxy Configuration Source

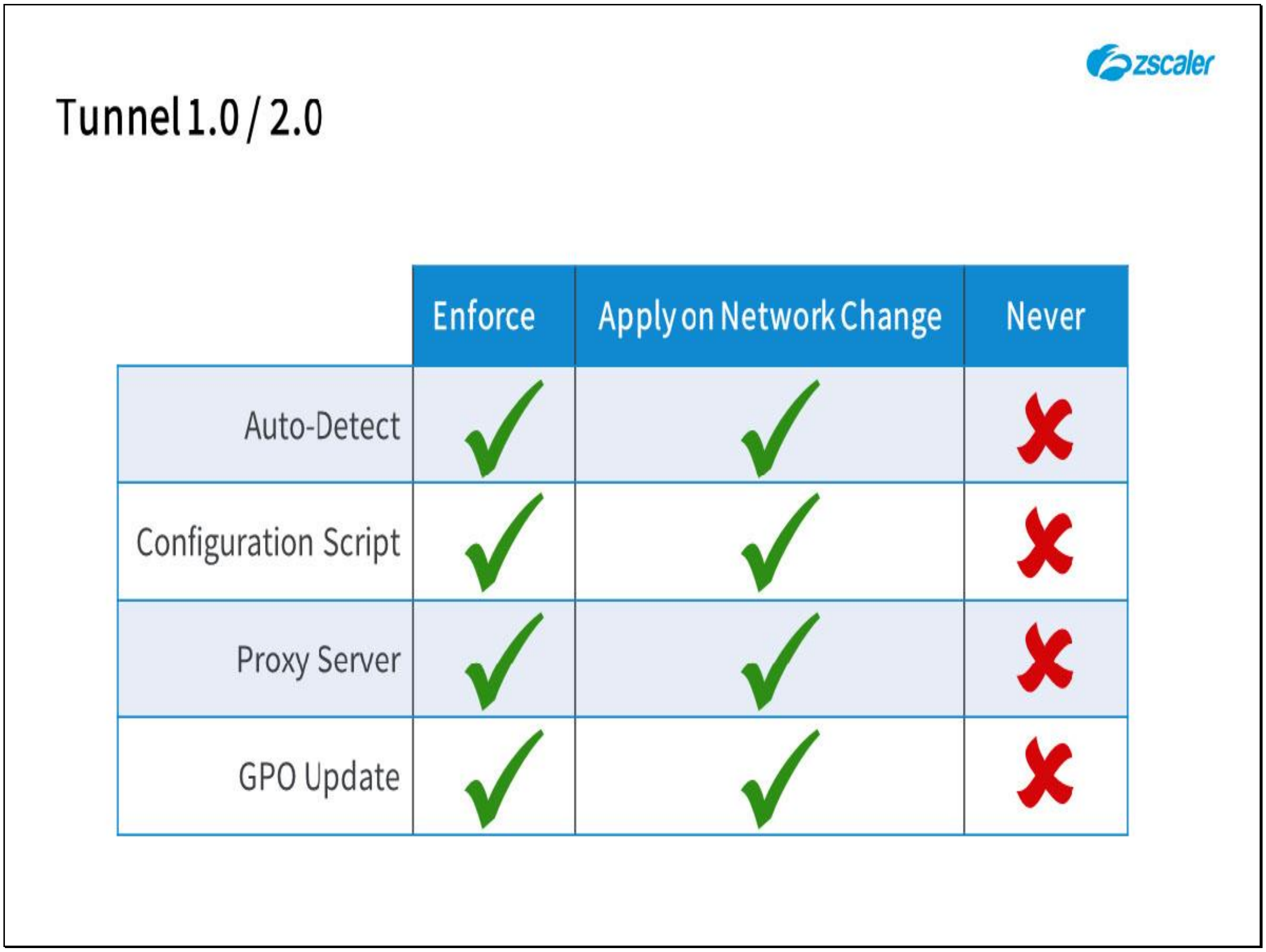
- **Automatically Detect Settings:** Use proxy discovery on the network per the device configuration
- **Use Automatic Configuration Script:** Specify a PAC file for proxy settings on users' devices
- **Use Proxy Server for Your LAN:** Use a specific proxy server and port
- **Execute GPO Update:** Execute a GPO update on Windows devices on a network change

Slide notes

Depending on your configuration, you may also have options for the source of the proxy configuration settings. You may choose one or more of the following options:

- **Automatically Detect Settings** - select this option if you want the users' devices to use proxy discovery on the local network;
- **Use Automatic Configuration Script** - select this option if you want to use a PAC file to specify automatic proxy settings on users' devices, the App fetches the PAC file at the specified URL and enforces your chosen proxy settings;
- **Use Proxy Server for Your LAN** - select this option if you want to use a specific proxy server (specified by IP, FQDN, or URL) and port, there is also a **Bypass Proxy Server for Local Addresses** option to bypass local resources;
- **Execute GPO Update** - select this option if you want to execute the GPO update command on Windows devices.

Slide 39 - Tunnel 1.0 / 2.0



Tunnel 1.0 / 2.0

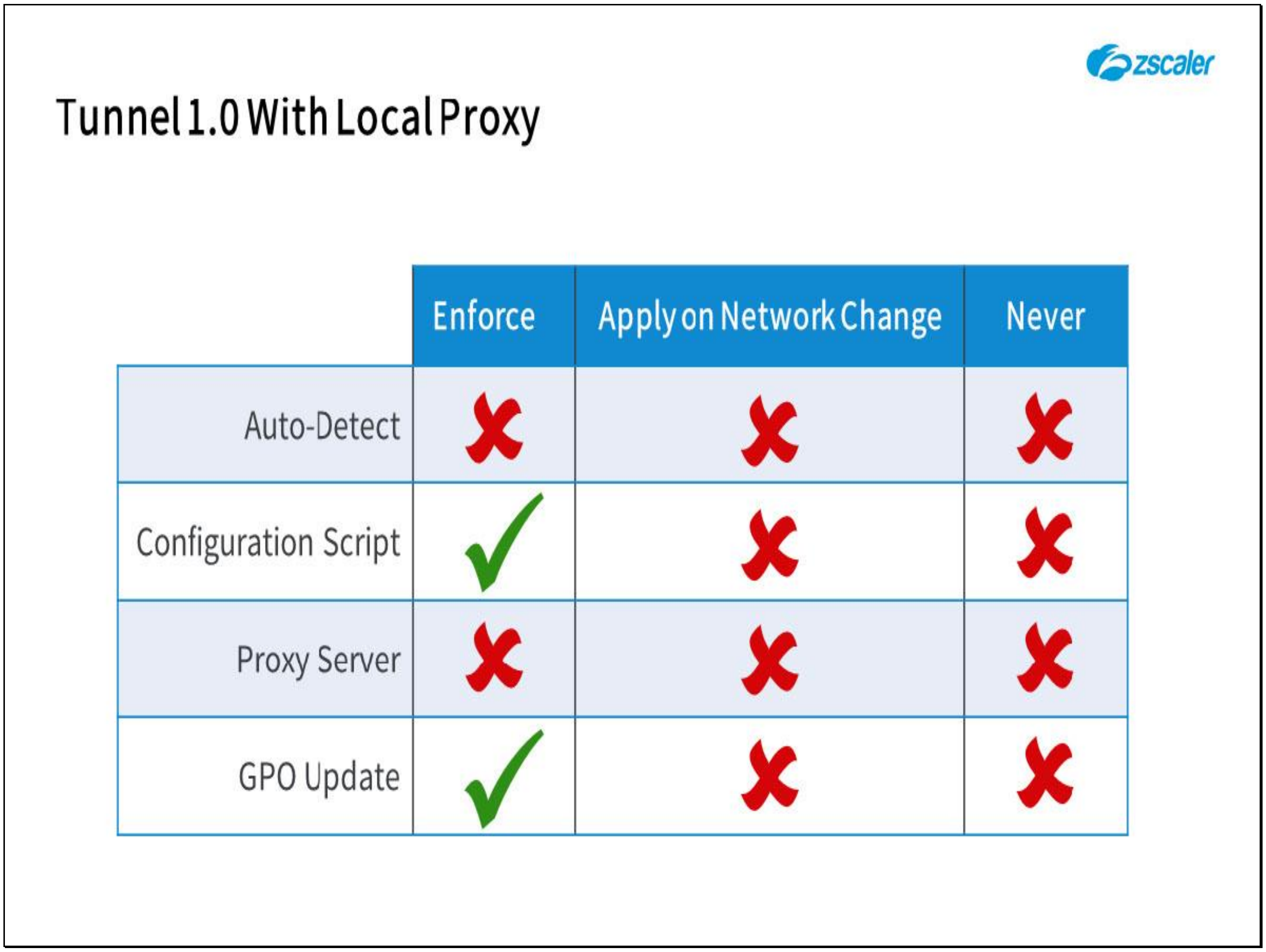
	Enforce	Apply on Network Change	Never
Auto-Detect	✓	✓	✗
Configuration Script	✓	✓	✗
Proxy Server	✓	✓	✗
GPO Update	✓	✓	✗

Slide notes

For the **Tunnel** options, this table represents the available configuration choices, for the **Enforce** and **Apply on Network Change** options, you may configure a mix of any of the proxy settings sources. For the **Never** option, there is nothing to be configured.

Note, while it is possible to configure multiple sources for the proxy configuration settings, it is probably better to pick one of them. Configuring multiple sources could lead to ‘contention’ between them which may lead to unexpected consequences.

Slide 40 - Tunnel 1.0 With Local Proxy



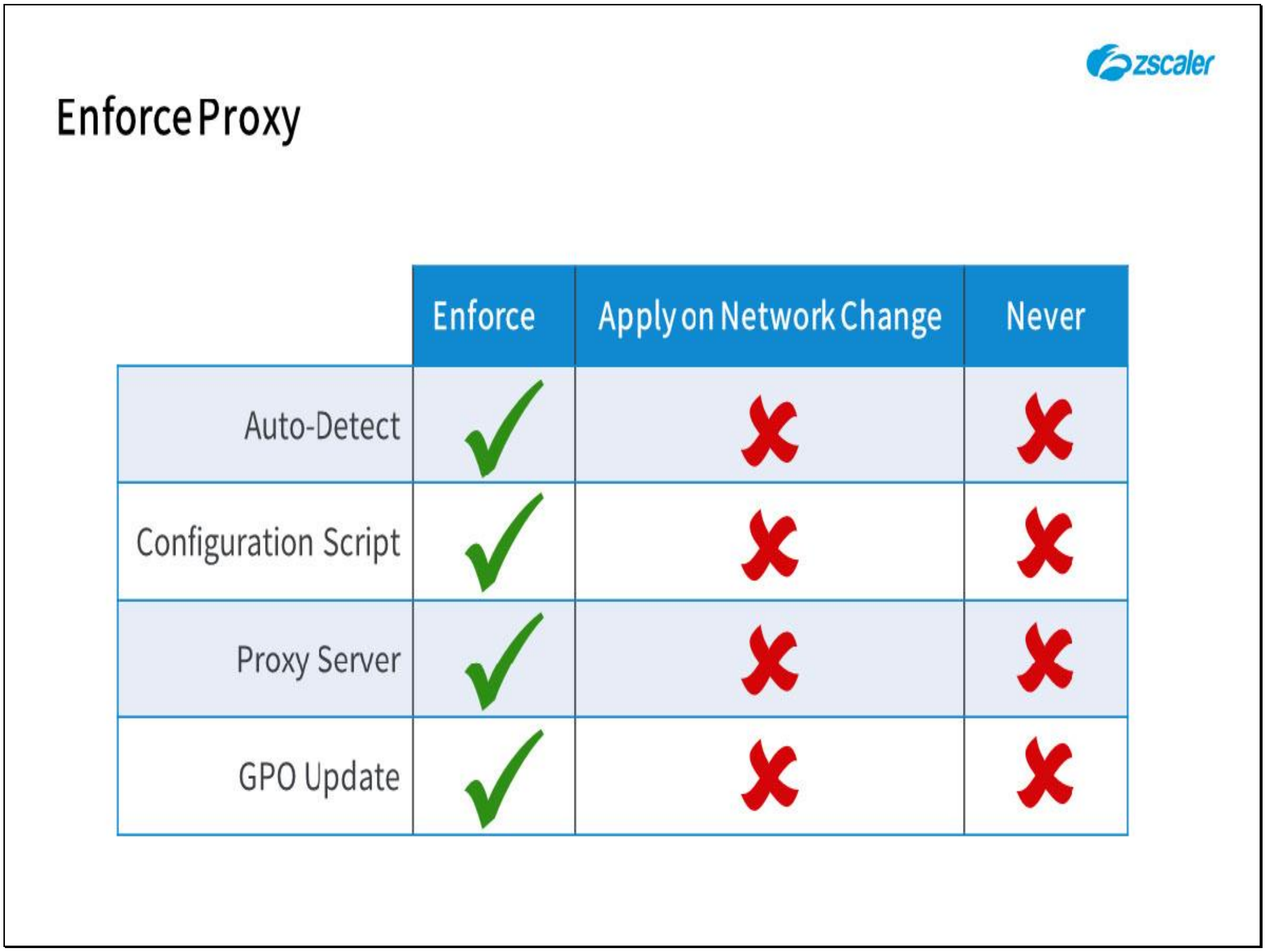
Tunnel 1.0 With Local Proxy

	Enforce	Apply on Network Change	Never
Auto-Detect	✗	✗	✗
Configuration Script	✓	✗	✗
Proxy Server	✗	✗	✗
GPO Update	✓	✗	✗

Slide notes

For the **TWLP** mode, the only proxy configuration options you have are to **Enforce** using a **Configuration Script** (which is required) and the option to do a **GPO Update** when necessary. Remember, any PAC file applied in this mode MUST contain either the gateway macro function **${ZAPP_LOCAL_PROXY}** as the destination (which is recommended), or a static loopback configuration with the correct port (e.g. **127.0.0.1:9000**).

Slide 41 - Enforce Proxy



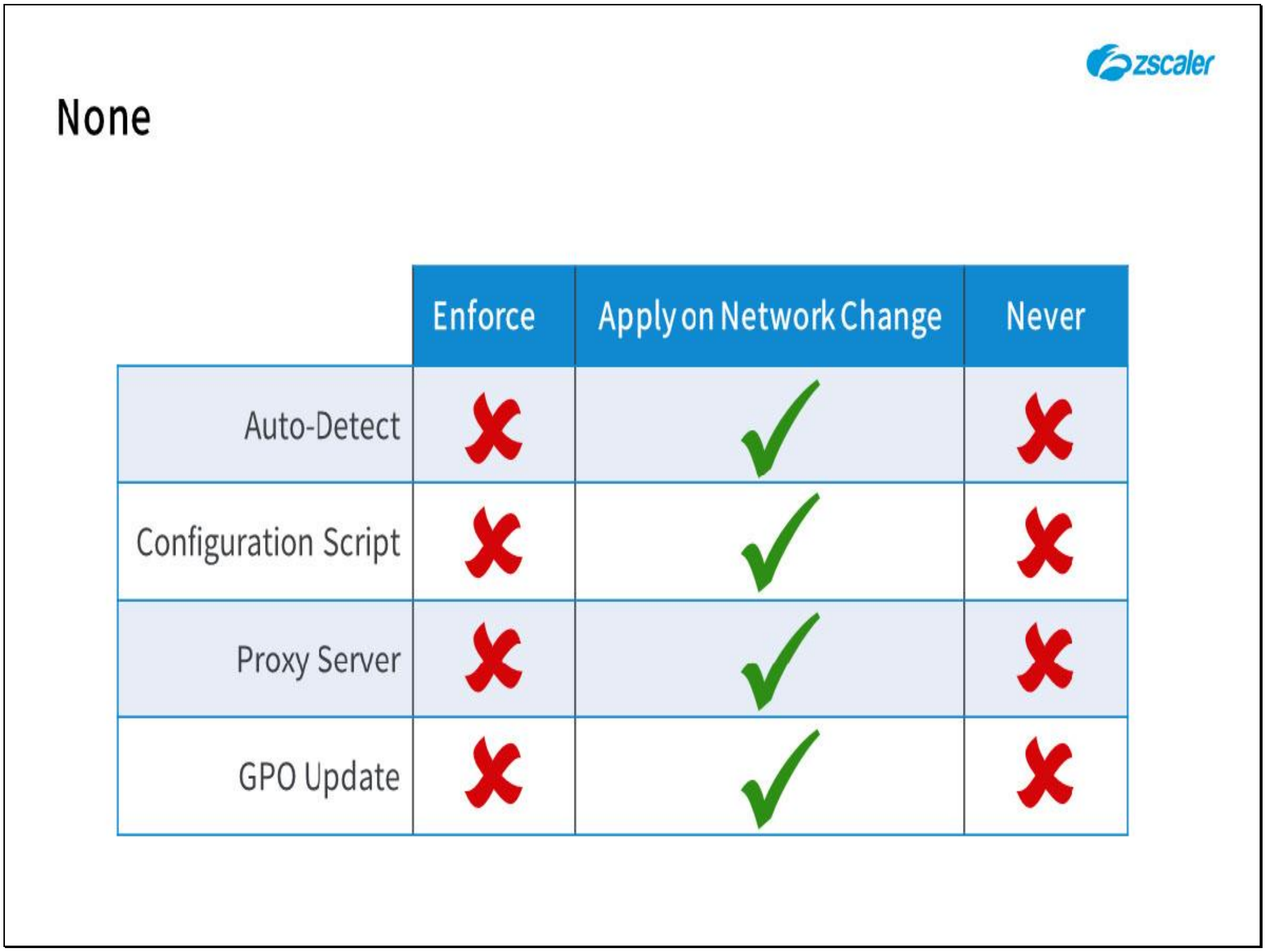
Enforce Proxy

	Enforce	Apply on Network Change	Never
Auto-Detect	✓	✗	✗
Configuration Script	✓	✗	✗
Proxy Server	✓	✗	✗
GPO Update	✓	✗	✗

Slide notes

The **Enforce Proxy** forwarding mode gives you all the available options for enforcing the proxy settings. The **Apply on Network Change** and **Never** options are unavailable.

Slide 42 - None



None

	Enforce	Apply on Network Change	Never
Auto-Detect	✗	✓	✗
Configuration Script	✗	✓	✗
Proxy Server	✗	✓	✗
GPO Update	✗	✓	✗

Slide notes

Finally, for the **None** forwarding mode, the only proxy configuration settings available are for the **Apply on Network Change** option.

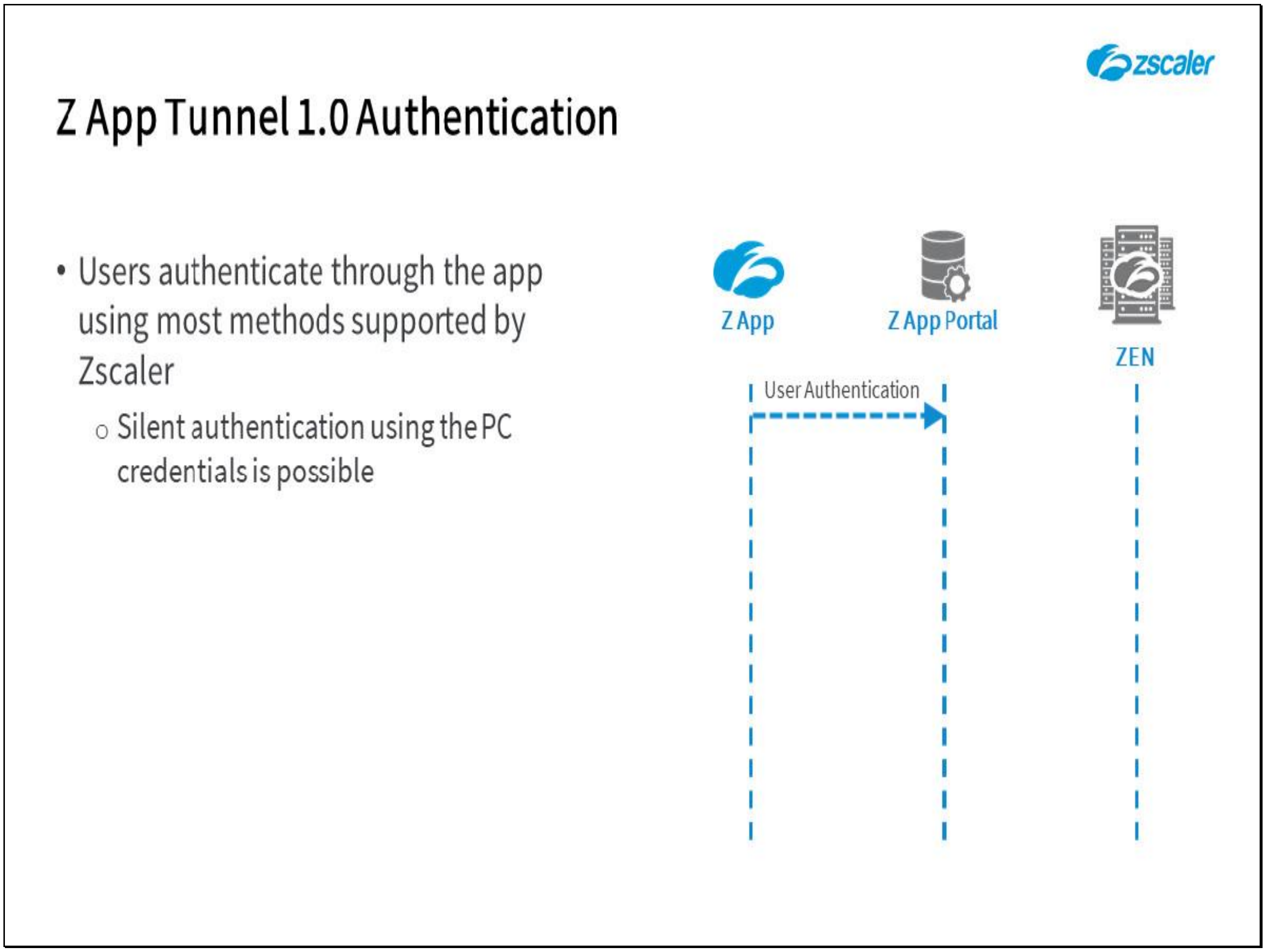
Slide 43 - Zscaler App – Tunnel Authentication

Tunnel Authentication

Slide notes

The next topic that we will cover is a look at how tunnels used for forwarding traffic to the ZIA service are authenticated.

Slide 44 - Z-App Authentication



zscaler

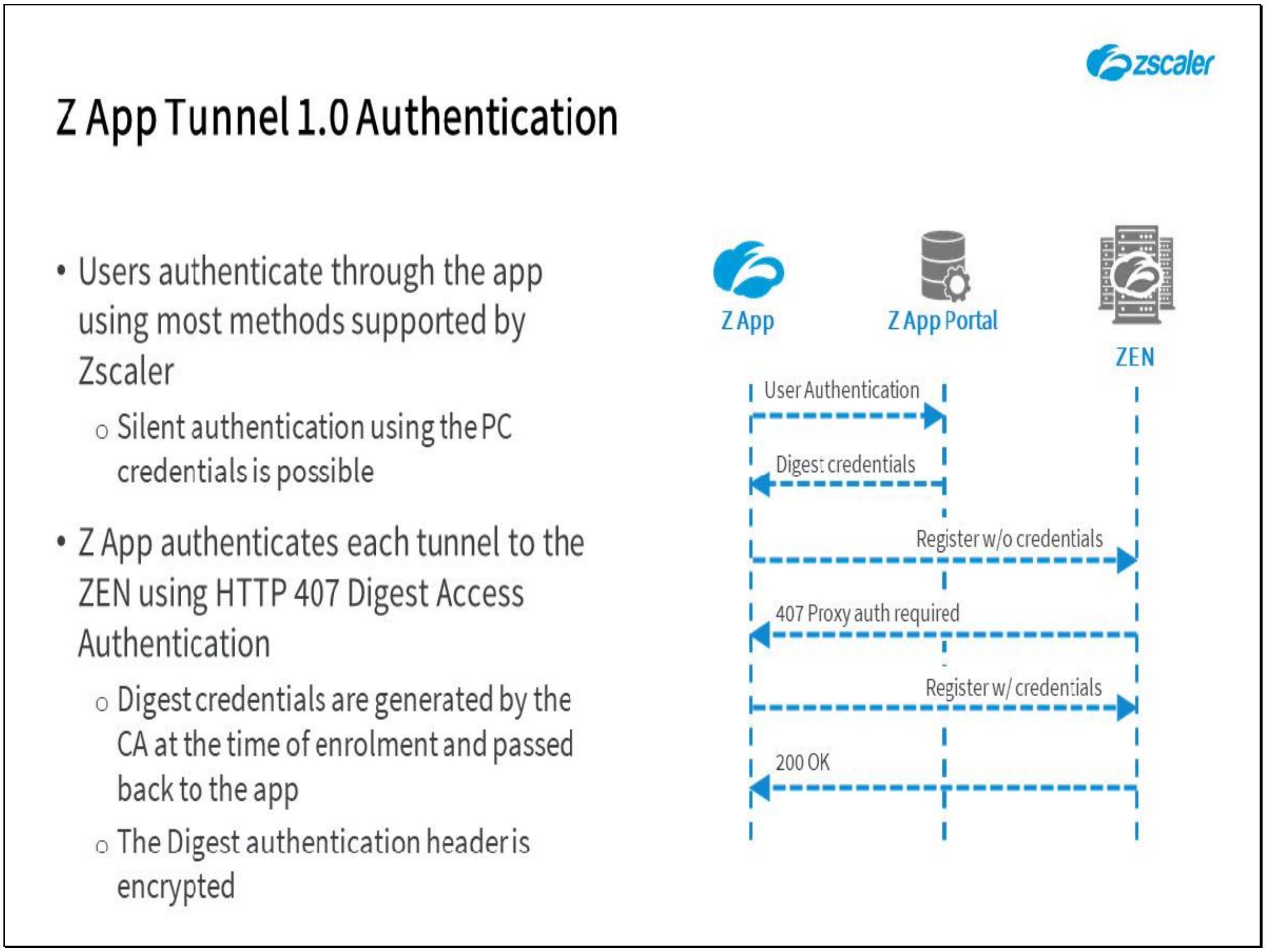
Z App Tunnel 1.0 Authentication

- Users authenticate through the app using most methods supported by Zscaler
  - o Silent authentication using the PC credentials is possible

Slide notes

On enrollment, users authenticate through the Zscaler App using just about any method supported by Zscaler. A silent authentication is also possible, based on the user’s PC login credentials.

Slide 45 - Z-App Authentication



Z App Tunnel 1.0 Authentication

- Users authenticate through the app using most methods supported by Zscaler
  - Silent authentication using the PC credentials is possible
- Z App authenticates each tunnel to the ZEN using HTTP 407 Digest Access Authentication
  - Digest credentials are generated by the CA at the time of enrolment and passed back to the app
  - The Digest authentication header is encrypted

Slide notes

The Zscaler App uses RFC 2617 **Proxy Digest Authentication** to authenticate ZIA Tunnels to the ZEN, with the encrypted digest credentials being provided to the App following user authentication. When establishing a Tunnel to the ZEN the client is challenged with a **407** (Proxy Authentication Required) response message, to which it responds with the supplied digest credentials.

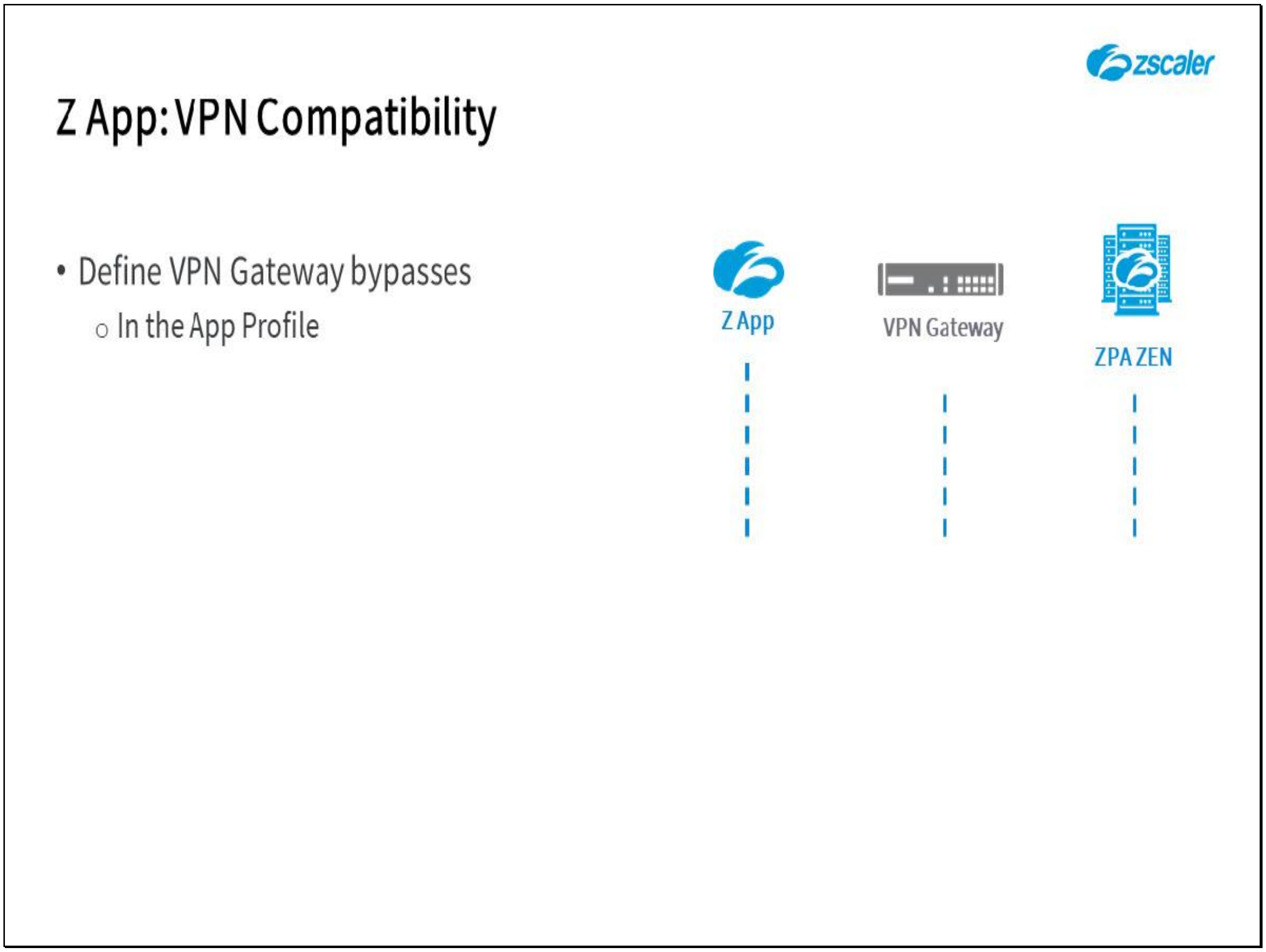
Slide 46 - Zscaler App – Platform Integration Issues

Host Platform Integration

Slide notes

The last topic that we will cover is a look at some host platform integration issues.

Slide 47 - Zscaler App: VPN Compatibility



zscaler

Z App: VPN Compatibility

- Define VPN Gateway bypasses
  - In the App Profile

Z App

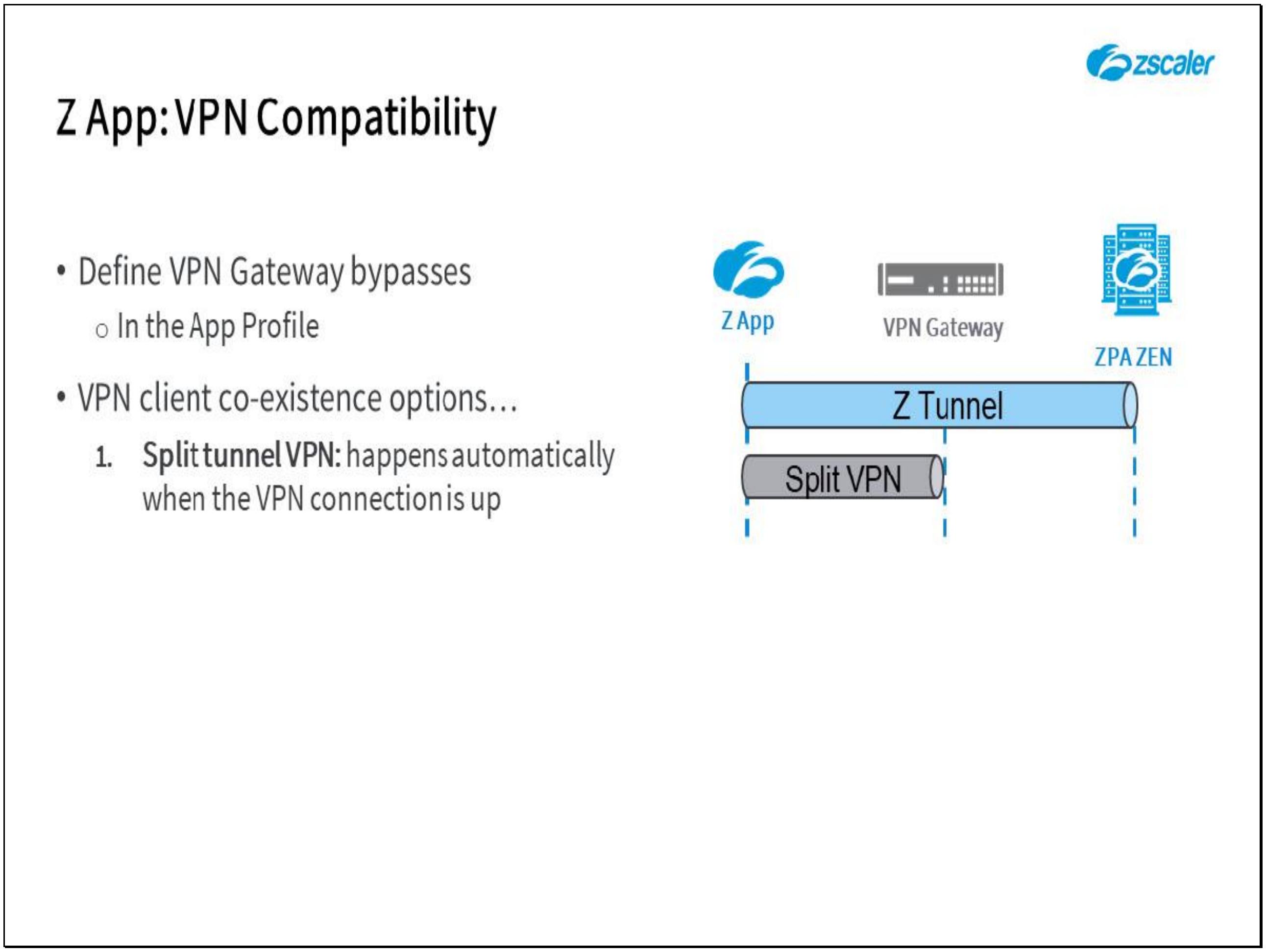
VPN Gateway

ZPA ZEN

Slide notes

There are two methods for the Zscaler App to co-exist with 3rd party VPN software on the client devices; split tunnel VPN, and full VPN. In either case you need to define the Hostnames, or IP addresses for the VPN Gateways as bypasses in the **App Profile** that you apply to your users.

Slide 48 - Zscaler App: VPN Compatibility



zscaler

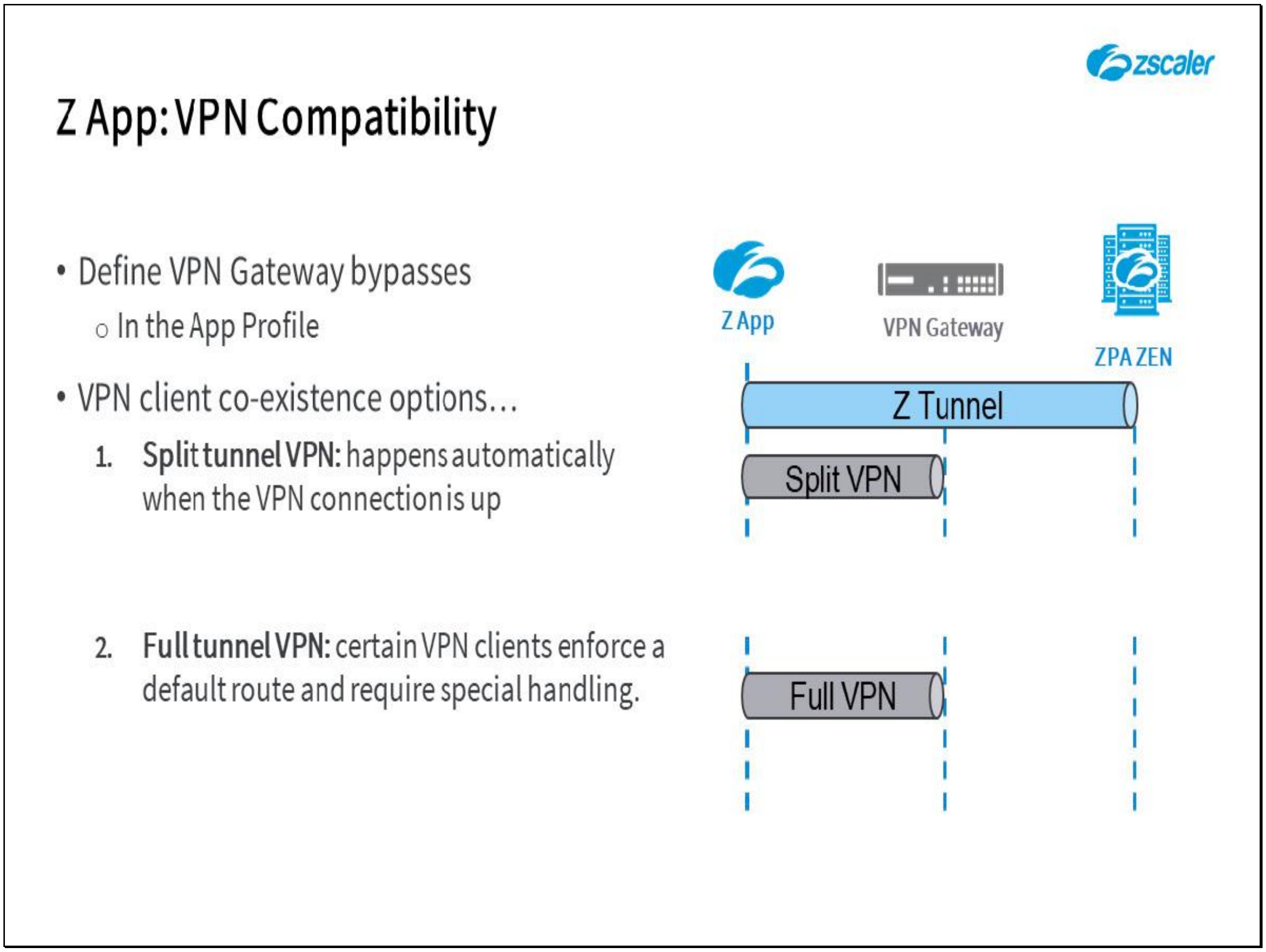
Z App: VPN Compatibility

- Define VPN Gateway bypasses
  - In the App Profile
- VPN client co-existence options…
  1. **Split tunnel VPN:** happens automatically when the VPN connection is up

Slide notes

Split tunneling happens automatically when the VPN connection is up, the VPN client creates a more specific route on top of the Zscaler default route. This results in the split tunnel configuration, where traffic sent to the VPN gateway is bypassed by the App and goes direct, while other Internet bound traffic is tunneled by the App to Zscaler.

Slide 49 - Zscaler App: VPN Compatibility



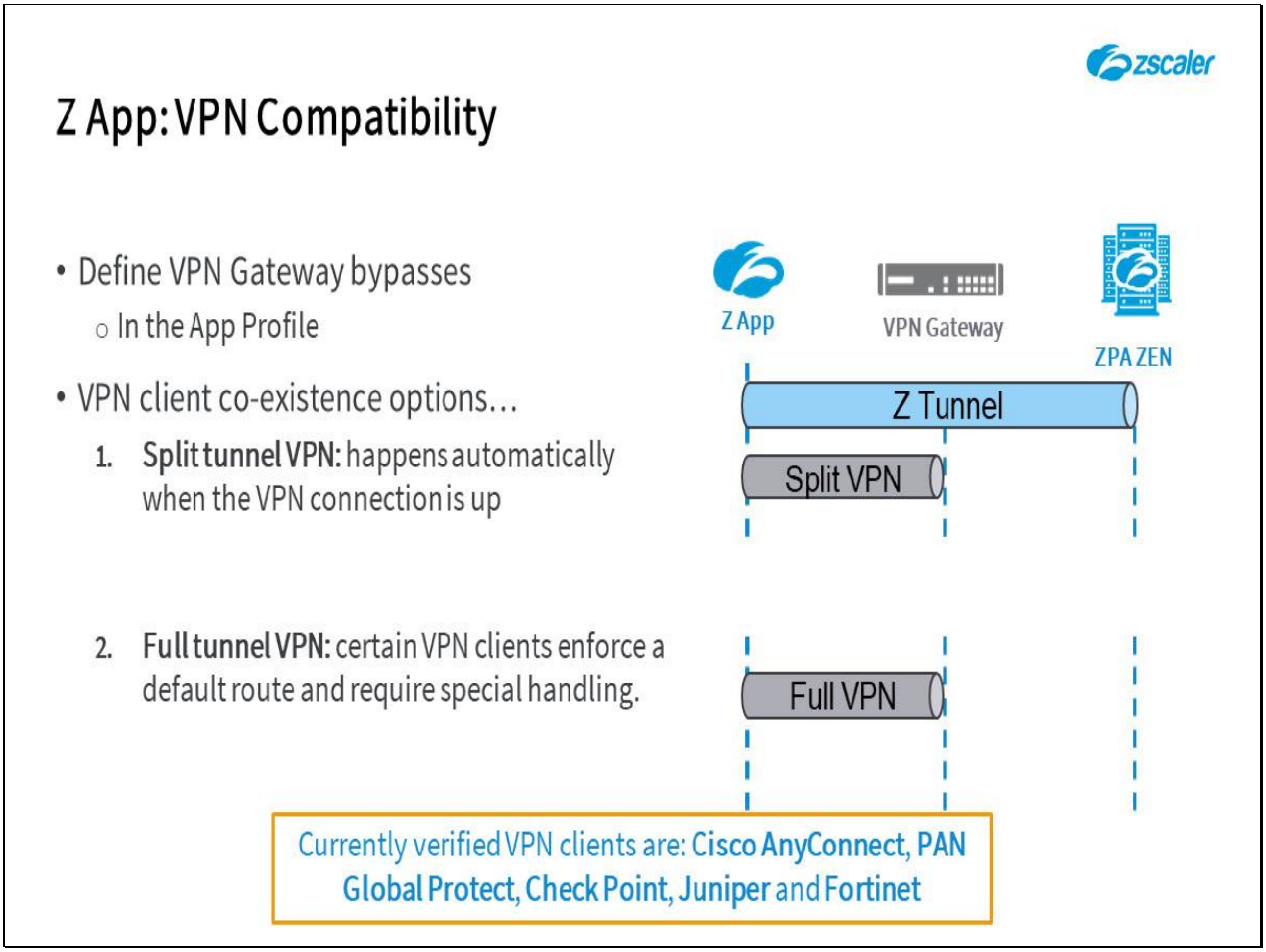
Z App: VPN Compatibility

- Define VPN Gateway bypasses
  - In the App Profile
- VPN client co-existence options…
  1. **Split tunnel VPN:** happens automatically when the VPN connection is up
  2. **Full tunnel VPN:** certain VPN clients enforce a default route and require special handling.

Slide notes

Some VPN client software tunnel ALL traffic to the specified VPN gateway, and usually specifies a default route to achieve this. The Zscaler App detects the presence of a default route VPN and goes into fail open mode, meaning that no traffic will be tunneled by the App.

Slide 50 - Zscaler App: VPN Compatibility



zscaler

Z App: VPN Compatibility

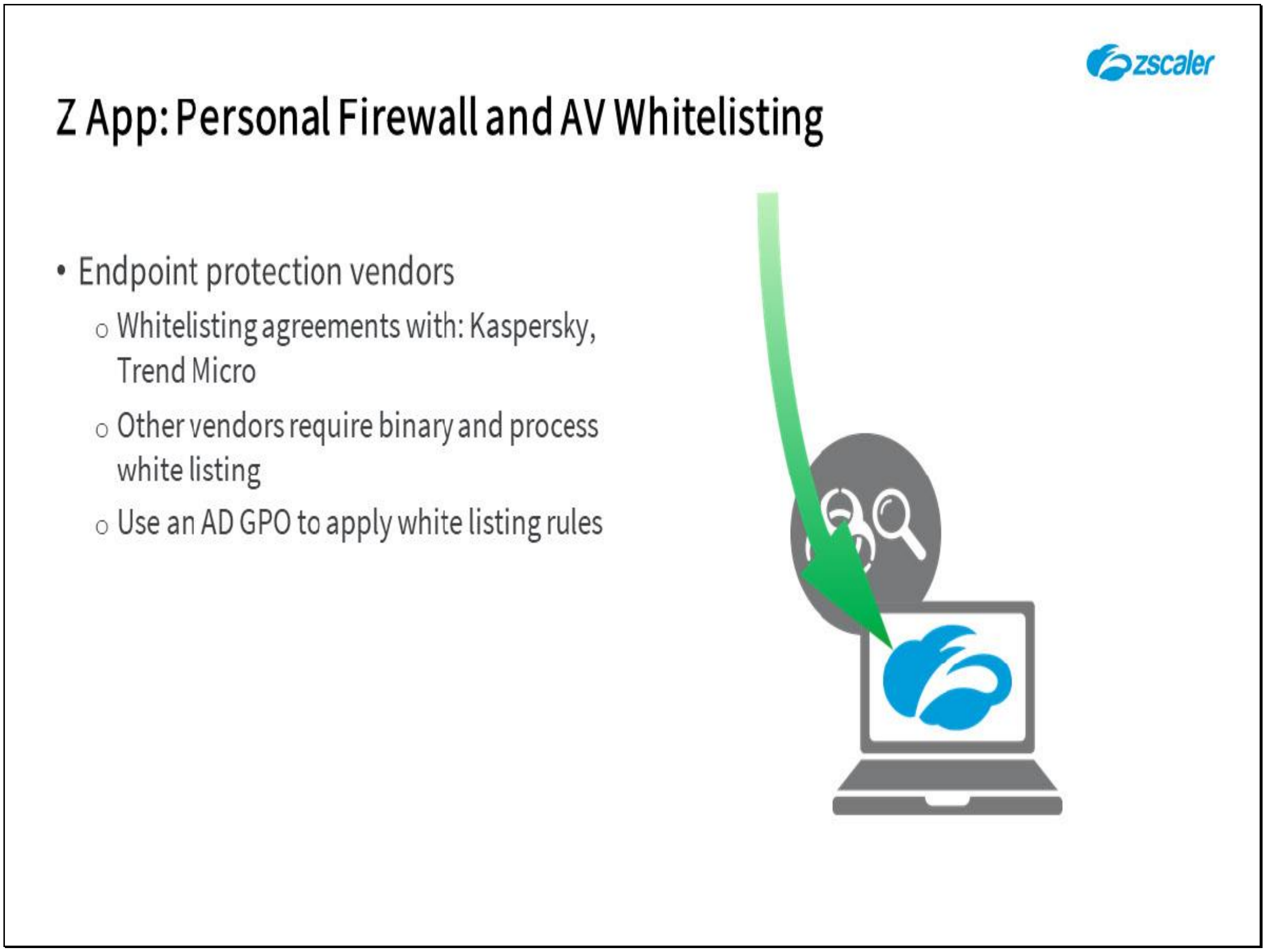
- Define VPN Gateway bypasses
  - In the App Profile
- VPN client co-existence options…
  1. **Split tunnel VPN:** happens automatically when the VPN connection is up
  2. **Full tunnel VPN:** certain VPN clients enforce a default route and require special handling.

Currently verified VPN clients are: **Cisco AnyConnect, PAN Global Protect, Check Point, Juniper** and **Fortinet**

Slide notes

Corporate VPN clients that have been tested and verified so far are: **Cisco AnyConnect**, **PAN Global Protect**, **Check Point** also the **Juniper** and **Fortinet** VPN clients.

Slide 51 - Zscaler App: Personal Firewall and AV Whitelisting



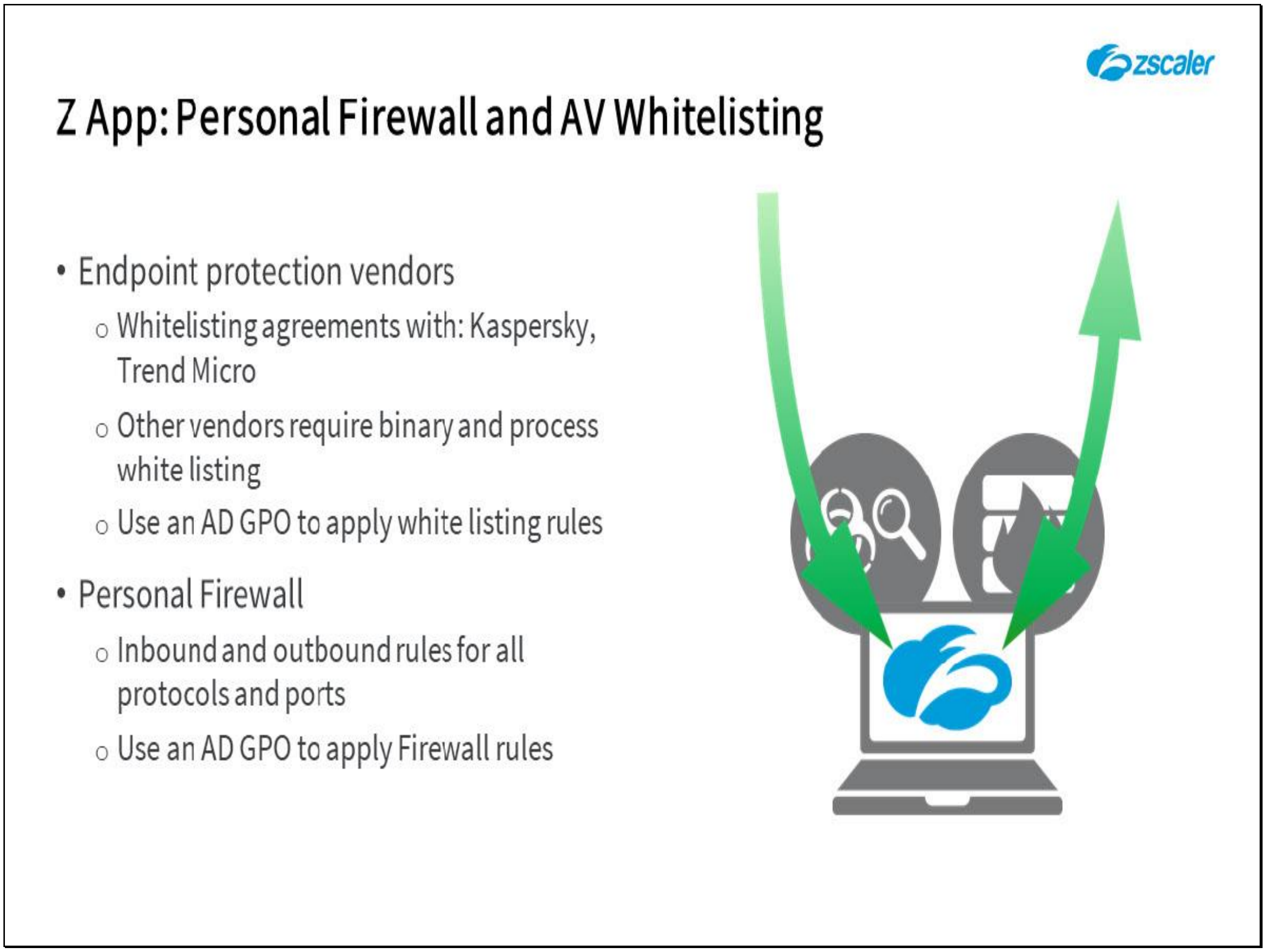
Z App: Personal Firewall and AV Whitelisting

- Endpoint protection vendors
  - Whitelisting agreements with: Kaspersky, Trend Micro
  - Other vendors require binary and process white listing
  - Use an AD GPO to apply white listing rules

Slide notes

For some endpoint protection products like anti-virus and personal firewall, you may need to perform additional whitelisting of Zscaler App binaries and processes to ensure full Zscaler App functionality. White listing agreements are in place with some endpoint protection vendors (such as Kaspersky, and Trend Micro), or you can use GPO to define rules to allow the required processes. See the on-line documentation for full details.

Slide 52 - Zscaler App: Personal Firewall and AV Whitelisting



Z App: Personal Firewall and AV Whitelisting

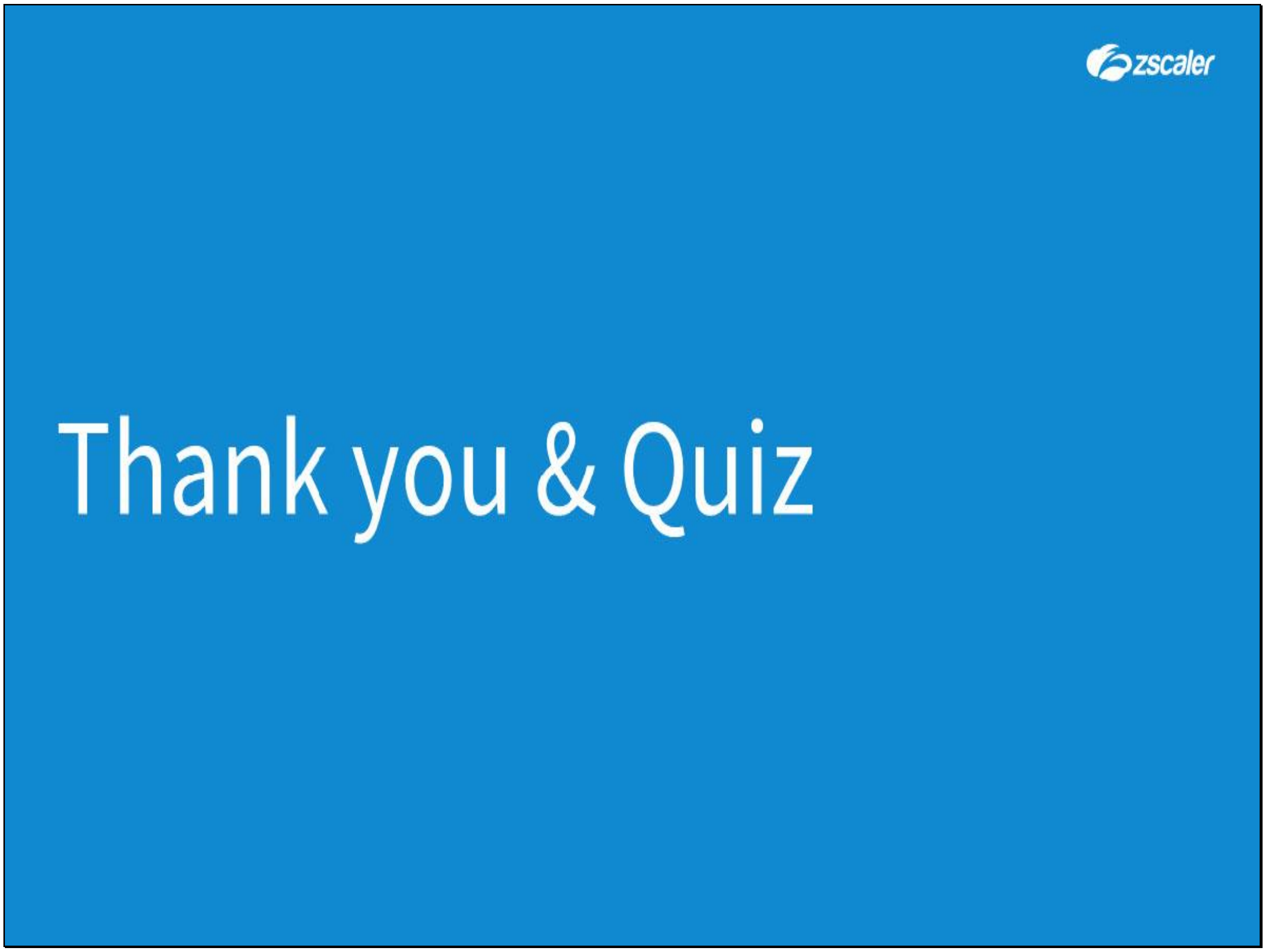
- Endpoint protection vendors
  - Whitelisting agreements with: Kaspersky, Trend Micro
  - Other vendors require binary and process white listing
  - Use an AD GPO to apply white listing rules
- Personal Firewall
  - Inbound and outbound rules for all protocols and ports
  - Use an AD GPO to apply Firewall rules

Slide notes

In addition, you may need to add firewall rules on your end point protection for various Zscaler App executables for all ports, protocols, and network types, although the App does try to add them automatically.

If you have a GPO-managed or AV-managed host firewall, you may configure inbound and outbound firewall rules on your endpoint protection product for Zscaler App processes for; all ports, protocols, and network interfaces.

Slide 53 - 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.