


Slide 1 – Zscaler App: Private Access – Under the Covers



The Zscaler App

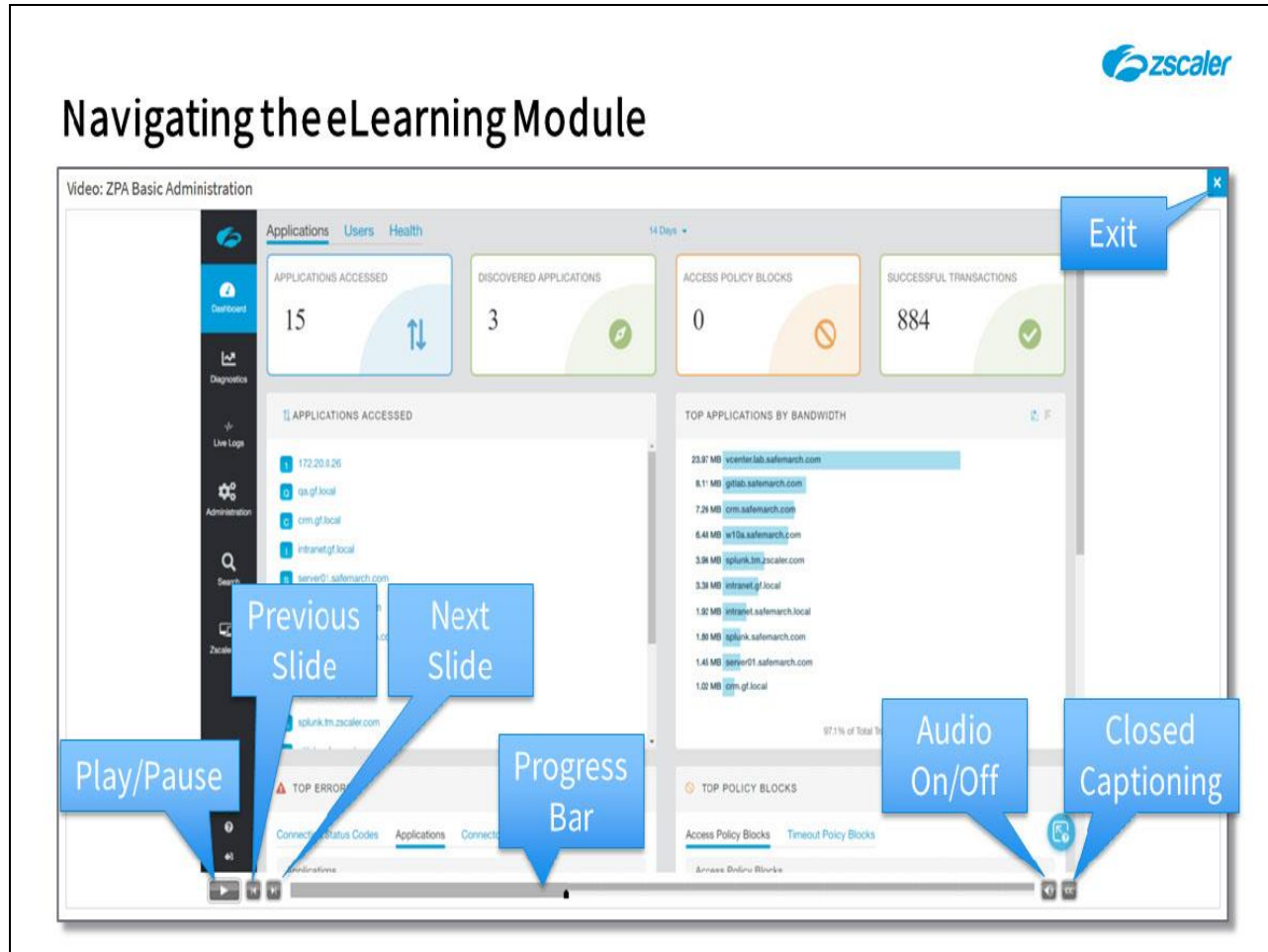
Private Access – Under the Covers

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module for a look under the covers at the Zscaler App for private access.

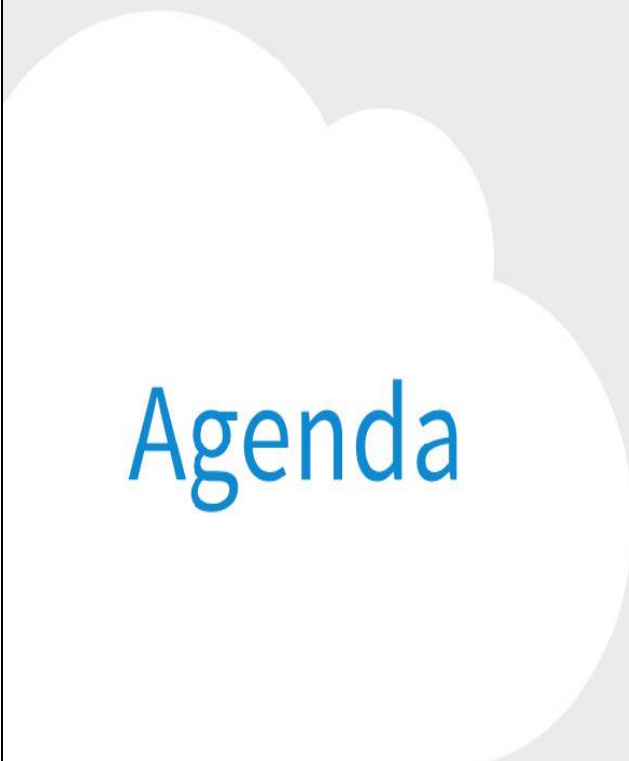

Slide 2 - Navigating the eLearning Module



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



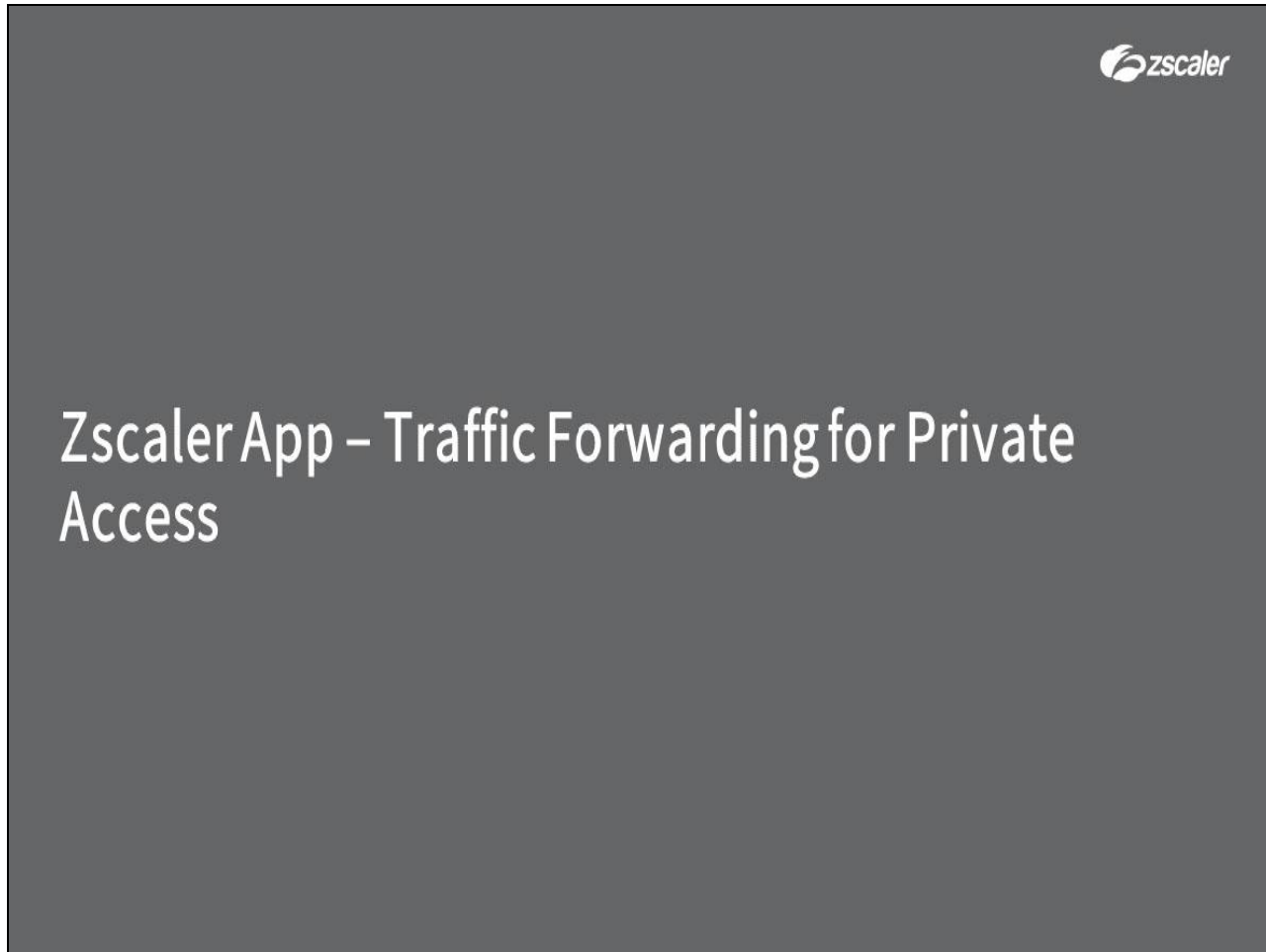
Agenda

- Zscaler App – Traffic Forwarding for Private Access
- Zscaler App – Platform Integration

Slide notes

In this module, we will have a detailed look at how the Zscaler App forwards traffic for private access and at some host platform integration issues.

Slide 4 - Zscaler App – Traffic Forwarding for Private Access



Slide notes

The first topic that we will cover is a detailed look at how the Zscaler App forwards traffic for private access.

Slide 5 - 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

The screenshot shows the 'Add Forwarding Profile' dialog box. The 'WINDOWS DRIVER SELECTION' section is highlighted with a red box. It contains a 'Tunnel Driver Type' dropdown menu with two options: 'Route Based' (selected) and 'Packet Filter Based'. Below this, there are sections for 'FORWARDING PROFILE ACTION FOR ZIA' and 'VPN Trusted Network', each with radio button options for 'Tunnel', 'Tunnel With Local Proxy', 'Enforce Proxy', and 'None'. The 'Tunnel With Local Proxy' option is selected in both sections. At the bottom, there are 'Save' and 'Cancel' buttons.

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 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
- Route Based
 - Adds default route to send all traffic to Zscaler App
 - Adds DNS server proxy IPs

The screenshot shows the 'Add Forwarding Profile' dialog box in the Zscaler interface. The 'WINDOWS DRIVER SELECTION' section is highlighted with a red box, showing 'Route Based' selected. Other sections include 'PROFILE DEFINITION', 'TRUSTED NETWORK CRITERIA', and 'FORWARDING PROFILE ACTION FOR ZIA'.


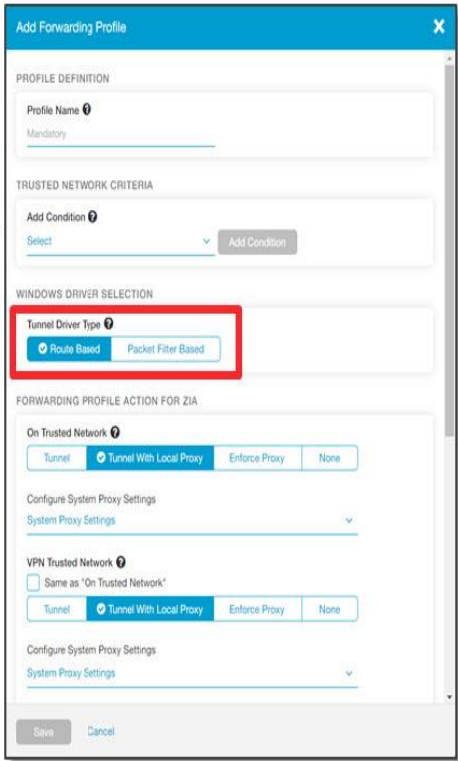
Slide notes

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, or other bypasses.

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
- 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

Slide notes

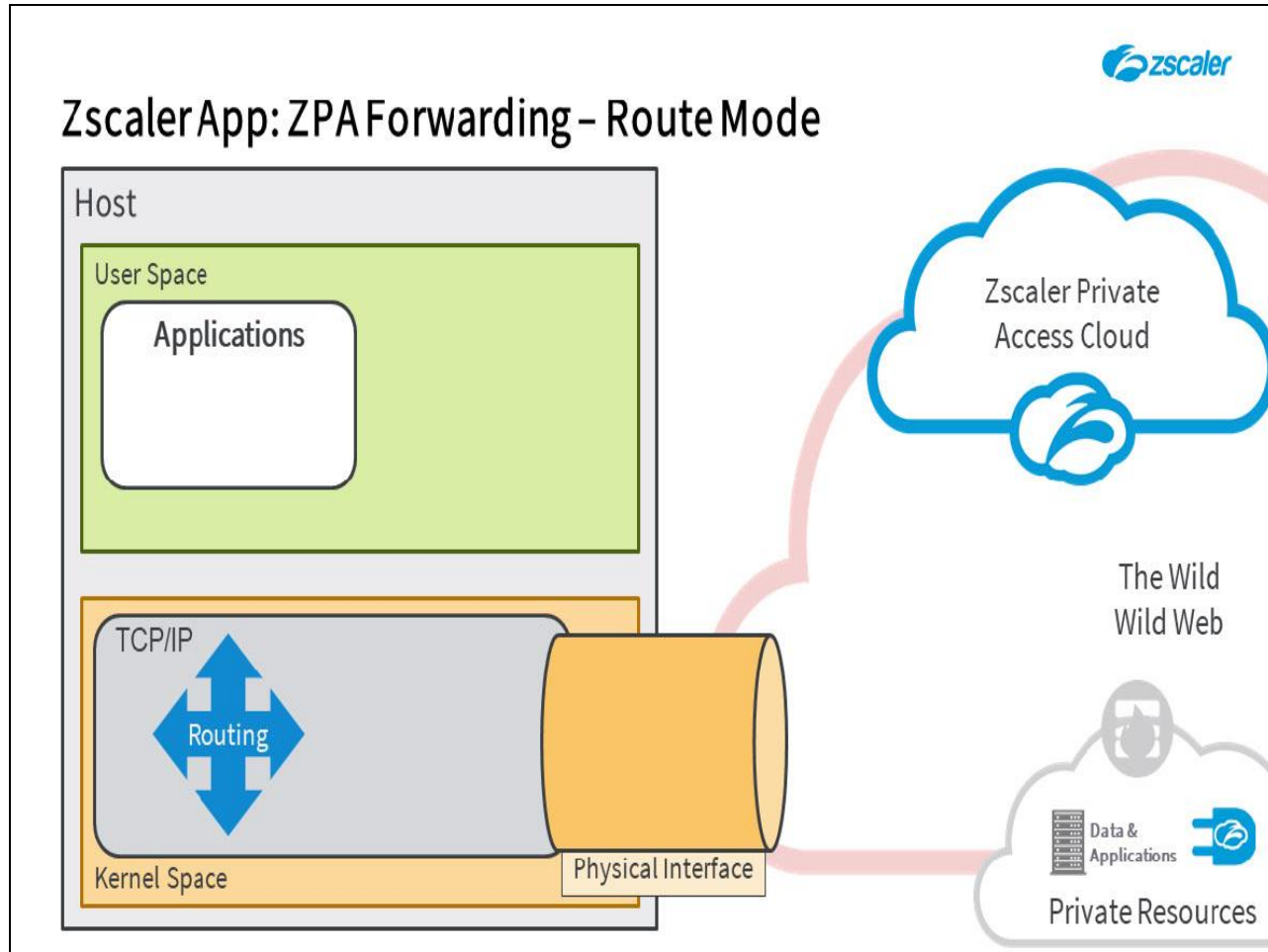
The **Packet Filter Based** driver is a high-performance packet filtering driver for the Windows platform that:

- 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 8 - Zscaler App: ZPA Forwarding

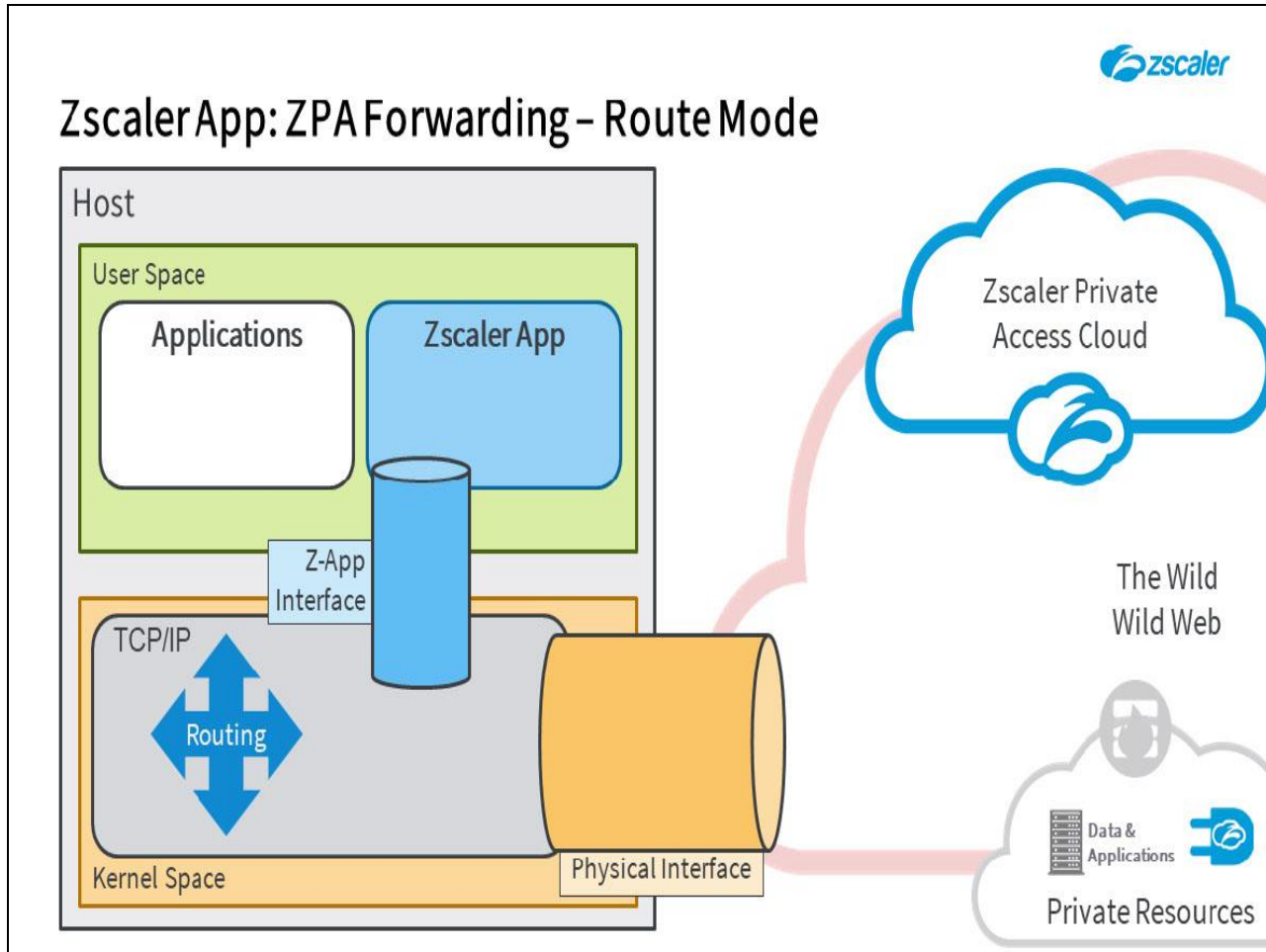


Slide notes

Let's talk through how the Zscaler App works on the host device for ZPA access to private applications:

- 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.

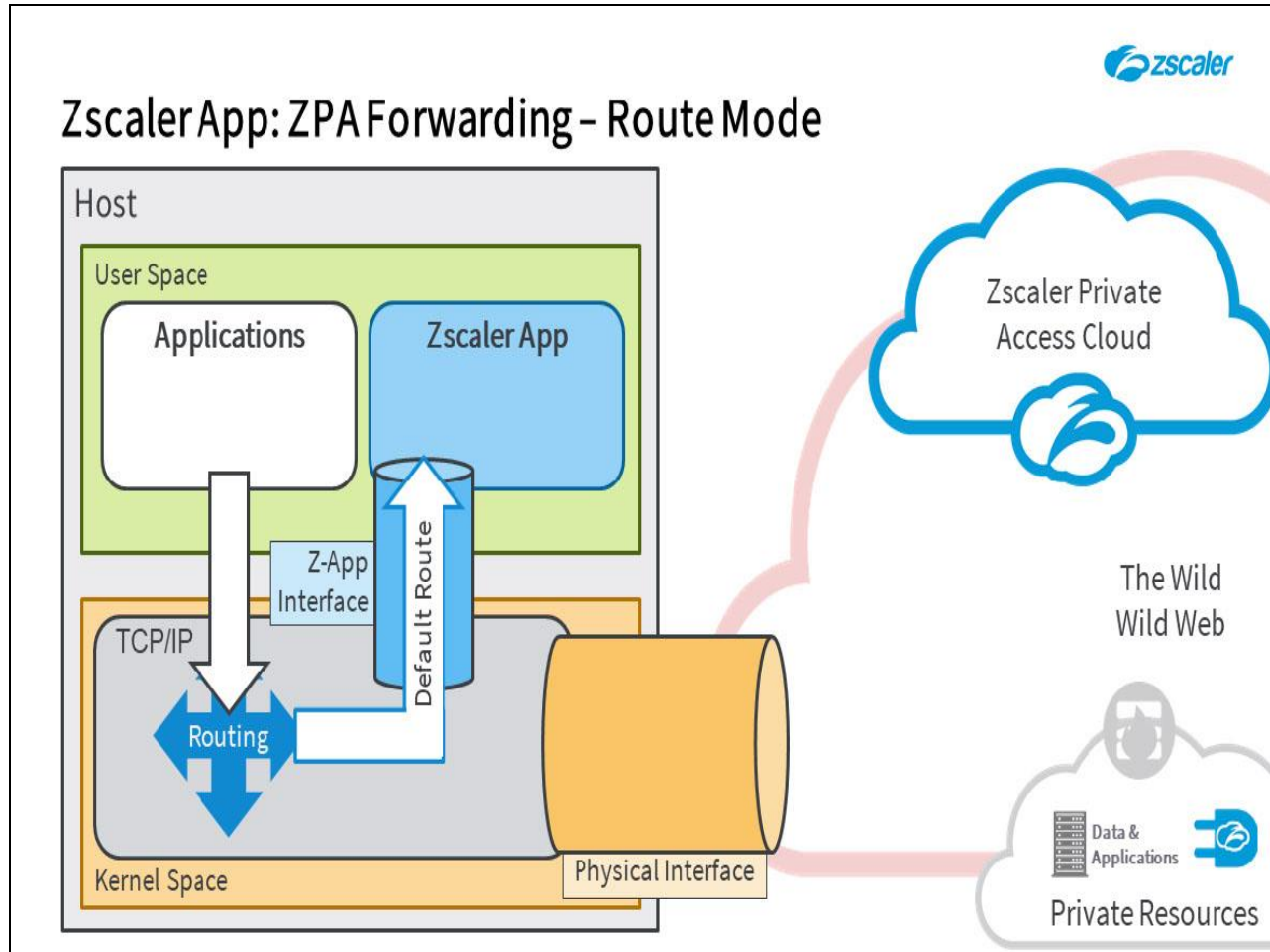
Slide 9 - Zscaler App: ZPA Forwarding



Slide notes

- The App is of course installed in the user space and it installs a virtual network interface that is assigned a non-routable, synthetic IP address (**100.64.0.2**).

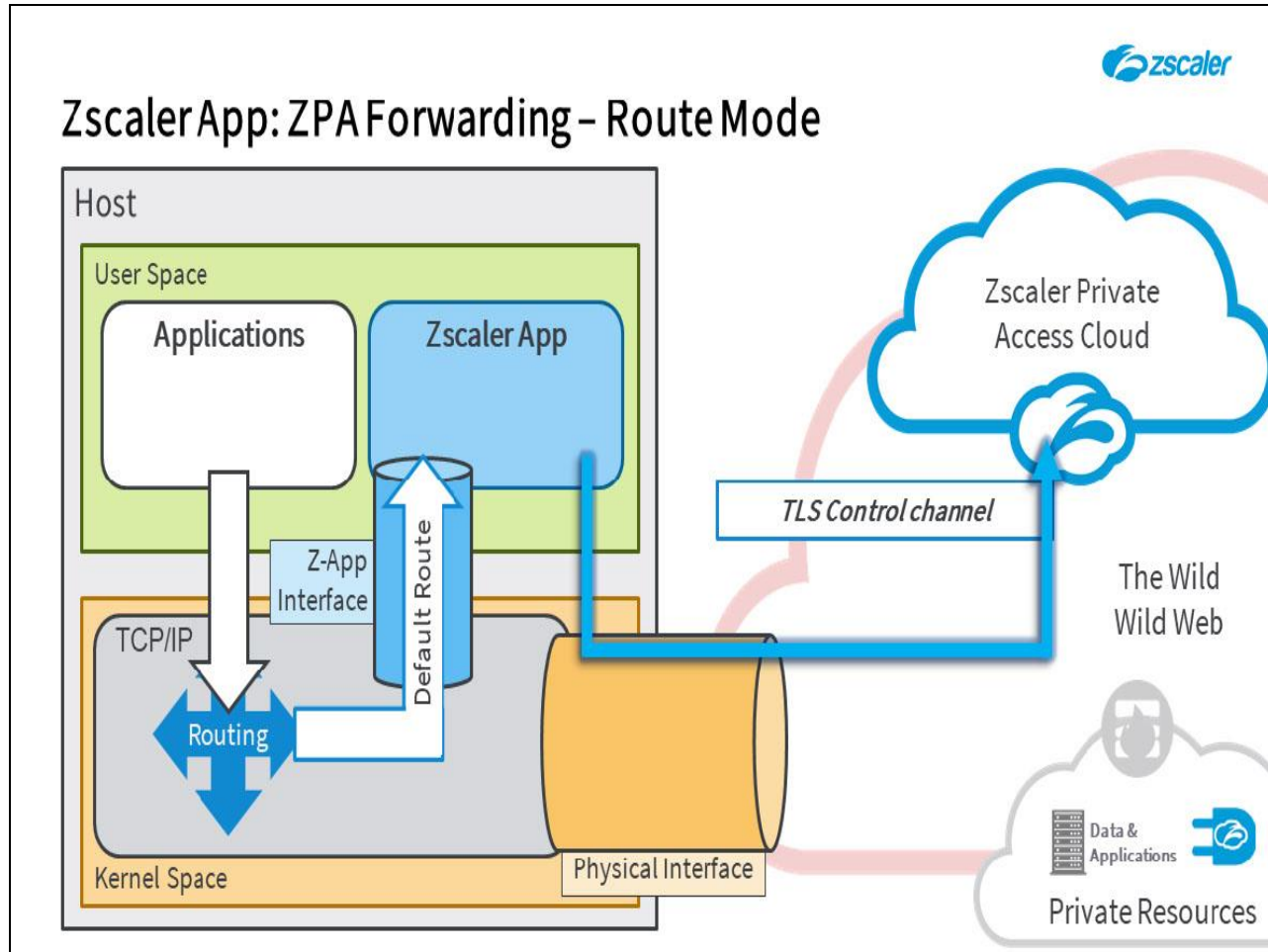
Slide 10 - Zscaler App: ZPA Forwarding



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**.

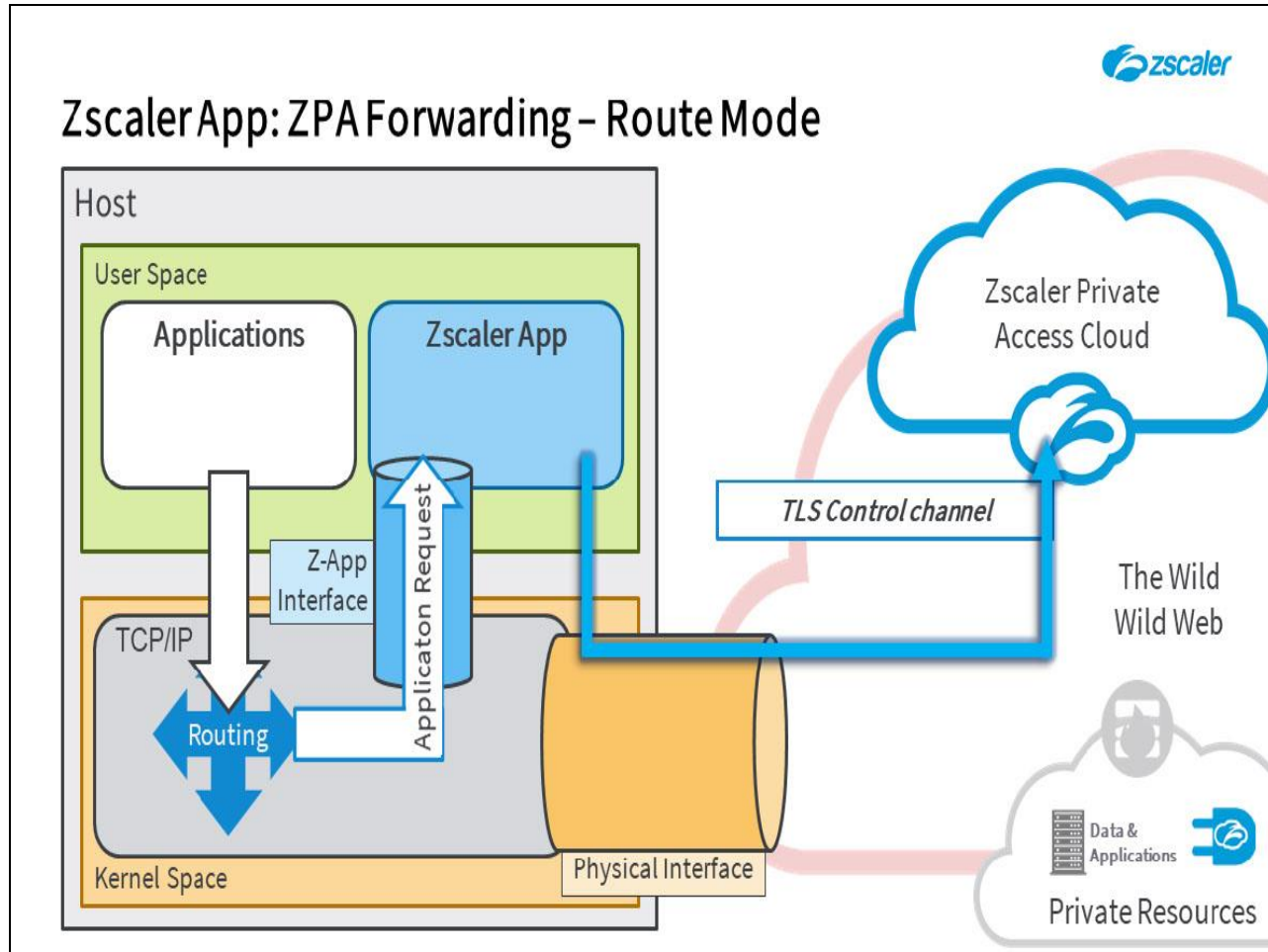
Slide 11 - Zscaler App: ZPA Forwarding – Route Mode



Slide notes

- Zscaler App will establish an encrypted TLS control channel to the closest ZPA Service Edge node, to allow the end user to authenticate to the ZPA service and for it to be notified by the ZPA-CA of the private applications available and of any applications that require double encryption.

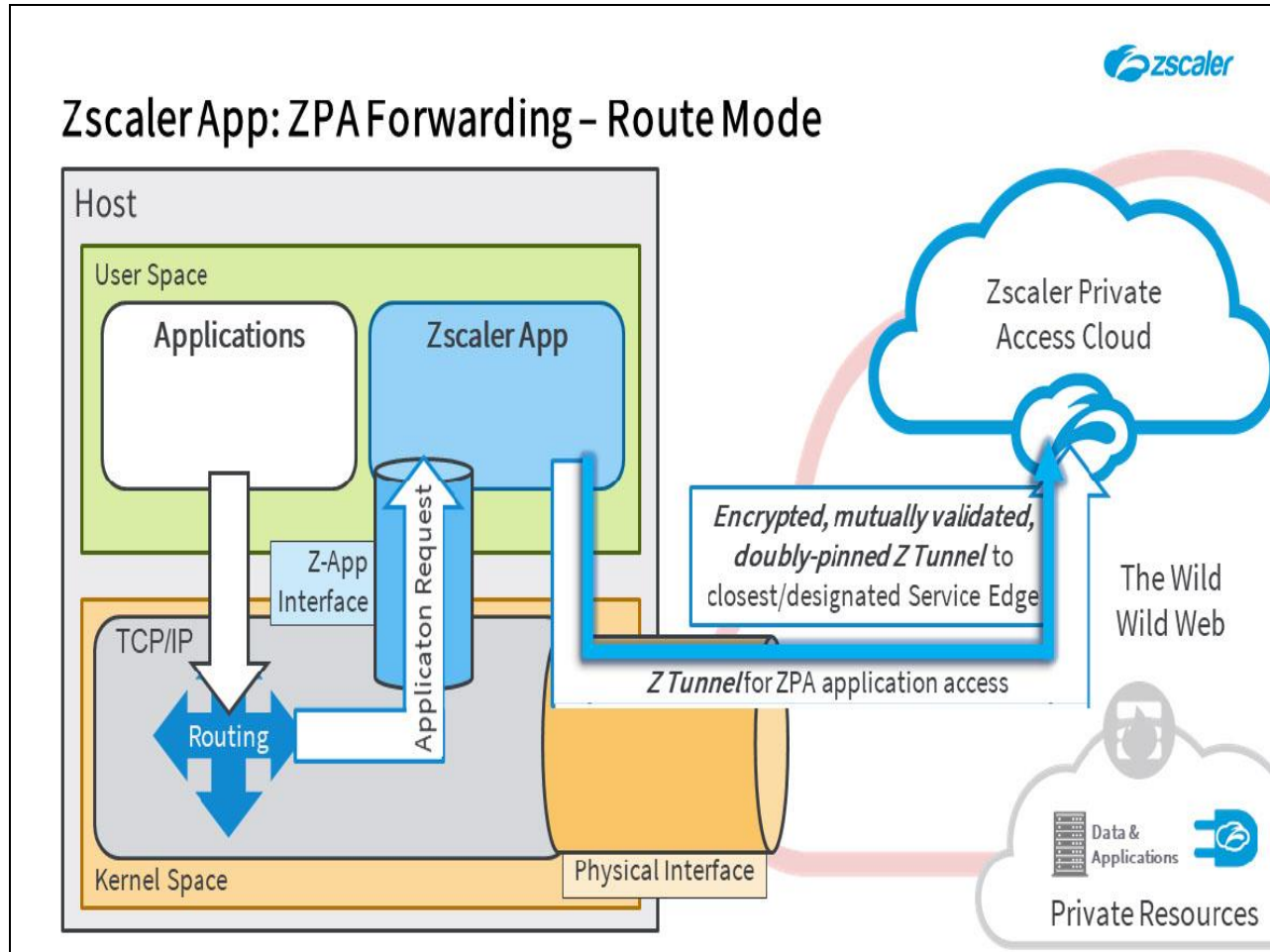
Slide 12 - Zscaler App: ZPA Forwarding



Slide notes

- The Zscaler App sees all outbound requests, including DNS requests, and can check whether they match the IP addresses or hostnames specified for the private applications defined in the ZPA Cloud.

Slide 13 - Zscaler App: ZPA Forwarding

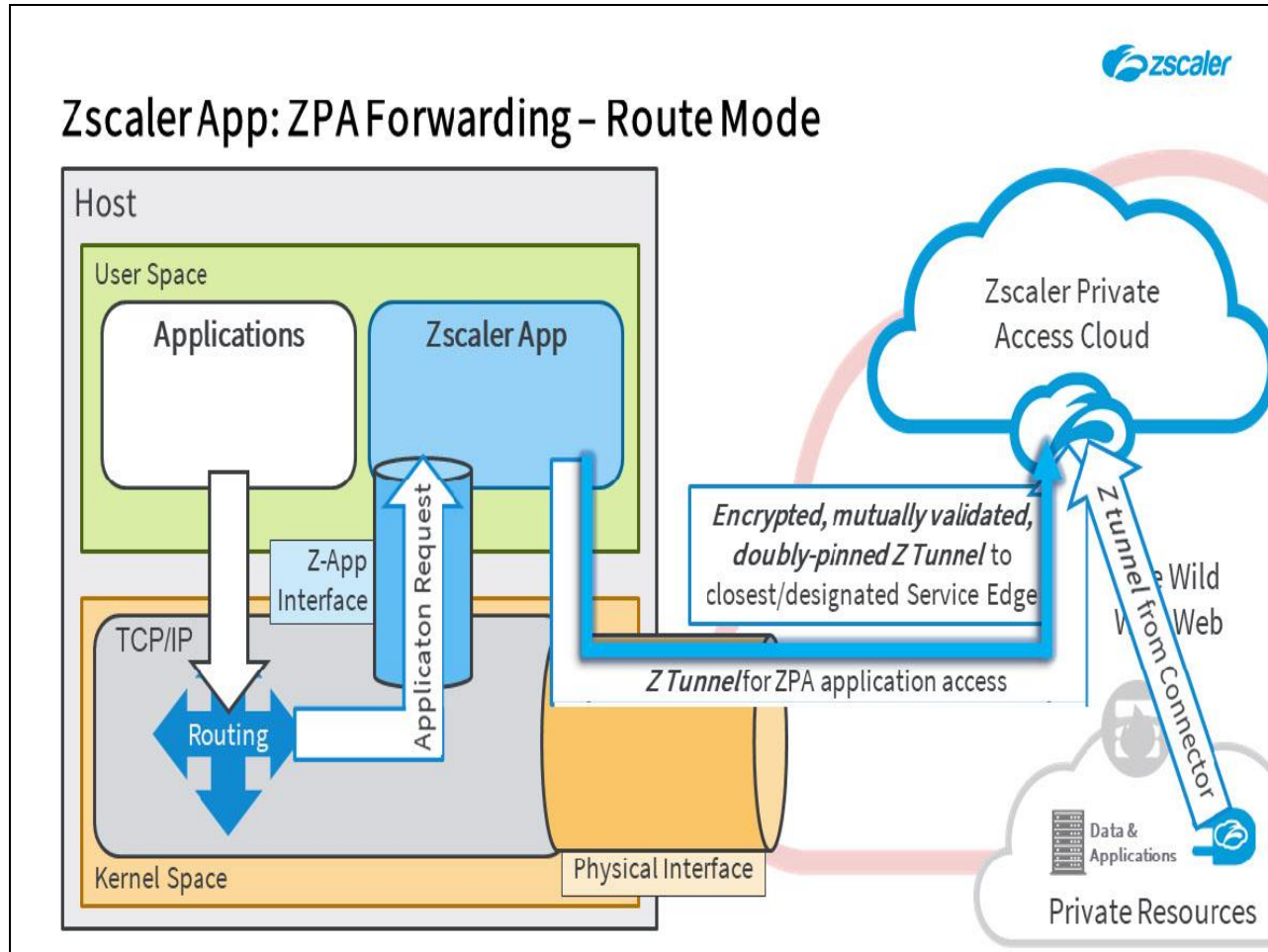


Slide notes

- If the request matches an application known to be available through ZPA, the Zscaler App will initiate a connection to that application.
 - It will first verify that the user is currently authenticated,
 - Is authorized to access the application,
 - That the application is available,
 - Then identify the best instance of it to connect to (if there are more than one).
 - The Zscaler App will establish an outbound **Z Tunnel** to the ZPA Service Edge that it is connected to.

Remember, **Z Tunnels** are encrypted TLS tunnels that are mutually validated and doubly-pinned, they are immune to MitM attacks.

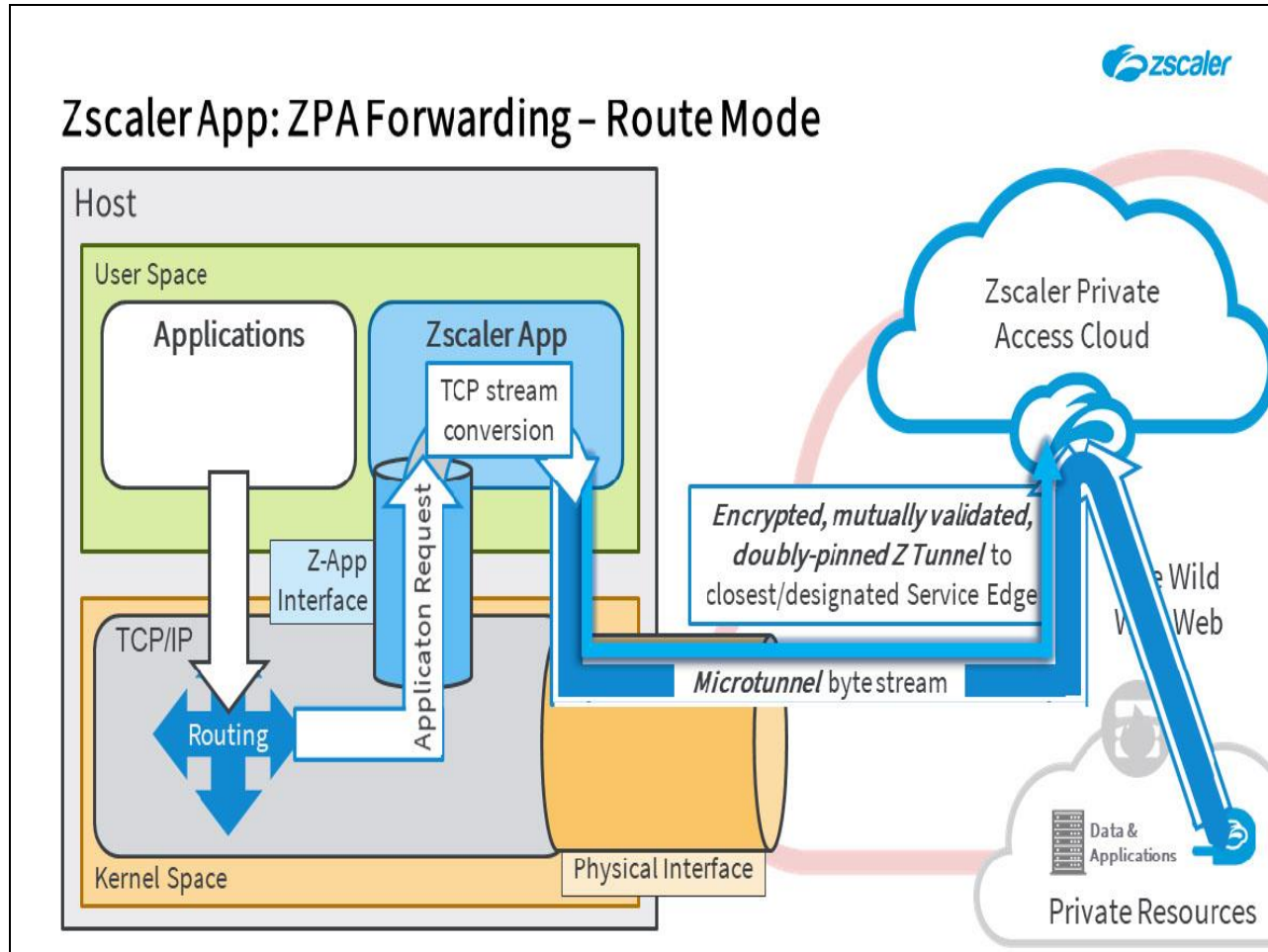
Slide 14 - Zscaler App: ZPA Forwarding



Slide notes

- The ZPA CA will identify the optimum App Connector for this connection and will notify it to establish a **Z Tunnel** to the same ZPA Service Edge.

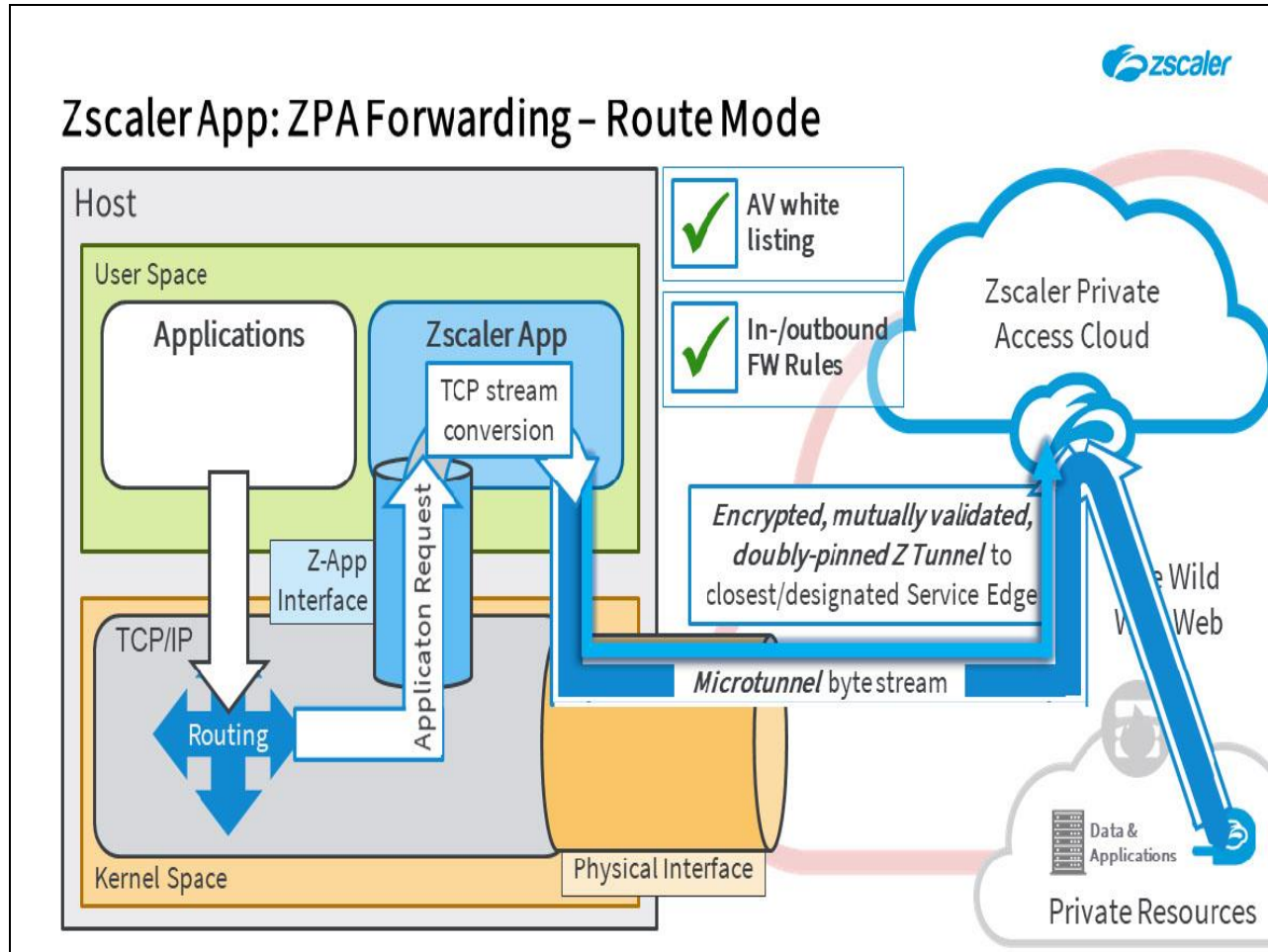
Slide 15 - Zscaler App: ZPA Forwarding



Slide notes

- An end-to-end **Microtunnel** is established within the **Z Tunnels** and the Zscaler App converts the outbound packets to a byte stream which it sends into the **Microtunnel**. Return traffic from the private application travels on the reciprocal path, for the App to deliver to the originating host application. Note that both UDP and TCP unicast traffic are supported over IPv4 on just about any destination port.

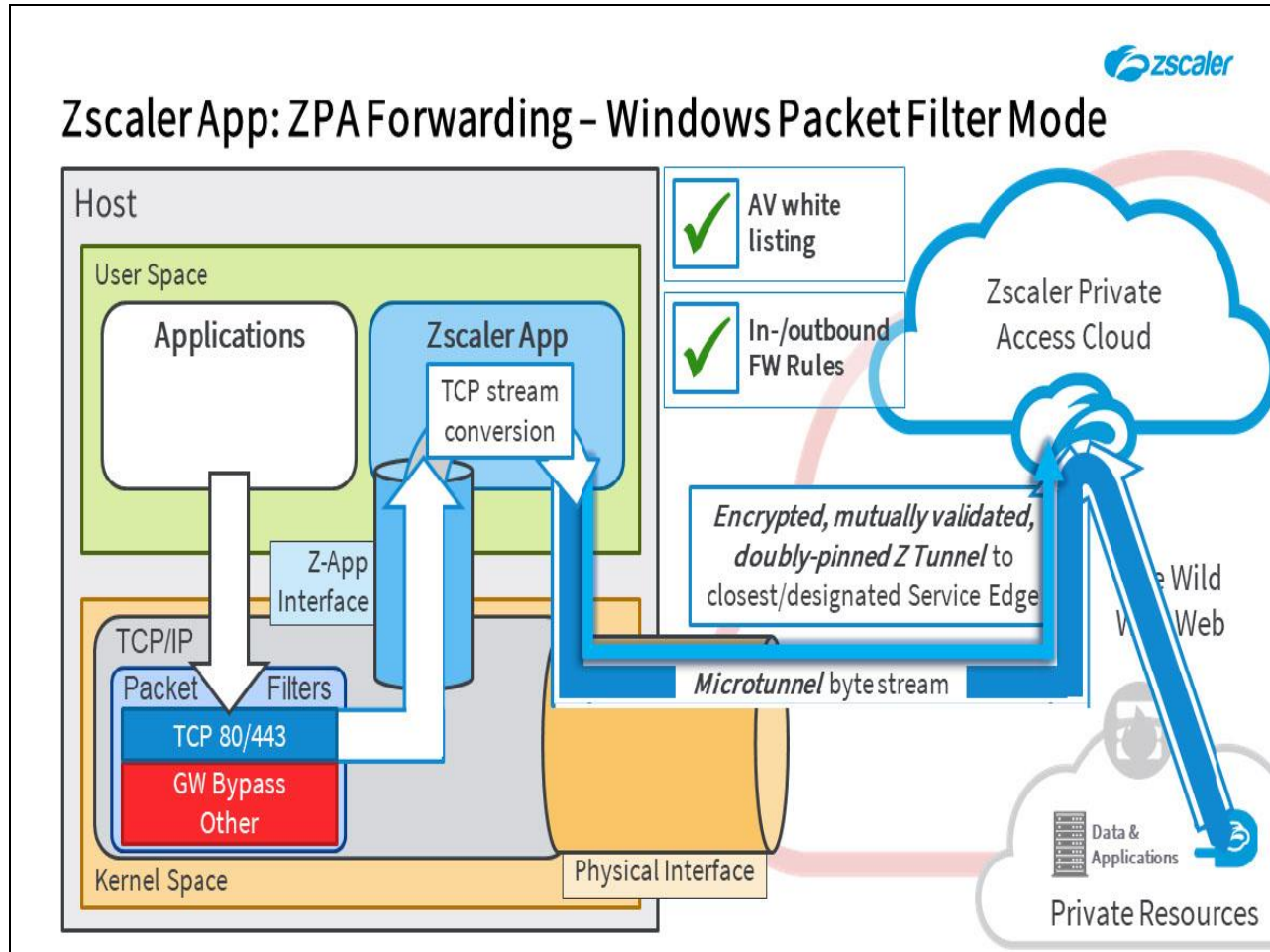
Slide 16 - Zscaler App: ZPA Forwarding



Slide notes

- The App needs to be whitelisted by any AV software installed on the host machine and for ZPA forwarding, inbound and outbound Firewall rules for all protocols and ports are required (because of the stream conversion).

Slide 17 - Z App: Tunnel 1.0 – Windows Packet Filter Mode




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 IP addresses required by ZPA;
- Any destinations listed as bypasses in the **App Profile** PAC file;
- Plus, some additional filters for local packet routing.

For the ZPA service, traffic that matches the **100.64.0.0/16** filter or a specific ZPA IP address filter, is forwarded to the Zscaler App which processes it as for any other ZPA traffic, as discussed in the preceding slides.

Slide 18 - Windows Packet Filter Mode Driver – Advantages



Windows Packet Filter Mode Driver – Advantages


Performance

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 19 - Windows Packet Filter Mode Driver – Advantages




Windows Packet Filter Mode Driver – Advantages

Performance	Enforcement
<ul style="list-style-type: none">• Multiple IP packets processing• Improved throughput<ul style="list-style-type: none">○ Evident for large file transfers on Gbps network○ Equivalent performance on 100 Mbps	<ul style="list-style-type: none">• Transparent install• Driver is hidden• No IP routes (that an end user might delete)• No DNS server 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 20 - Windows Packet Filter Mode Driver – Advantages



Windows Packet Filter Mode Driver – Advantages


Performance	Enforcement
<ul style="list-style-type: none">• Multiple IP packets processing• Improved throughput<ul style="list-style-type: none">○ Evident for large file transfers on Gbps network○ Equivalent performance on 100 Mbps	<ul style="list-style-type: none">• Transparent install• Driver is hidden• No IP routes (that an end user might delete)• No DNS server configurations

Interoperability
<ul style="list-style-type: none">• 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 21 - Windows Packet Filter Mode Driver – Advantages




Windows Packet Filter Mode Driver – Advantages

Performance	Enforcement
<ul style="list-style-type: none">• Multiple IP packets processing• Improved throughput<ul style="list-style-type: none">○ Evident for large file transfers on Gbps network○ Equivalent performance on 100 Mbps	<ul style="list-style-type: none">• Transparent install• Driver is hidden• No IP routes (that an end user might delete)• No DNS server configurations
Interoperability	Networking
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

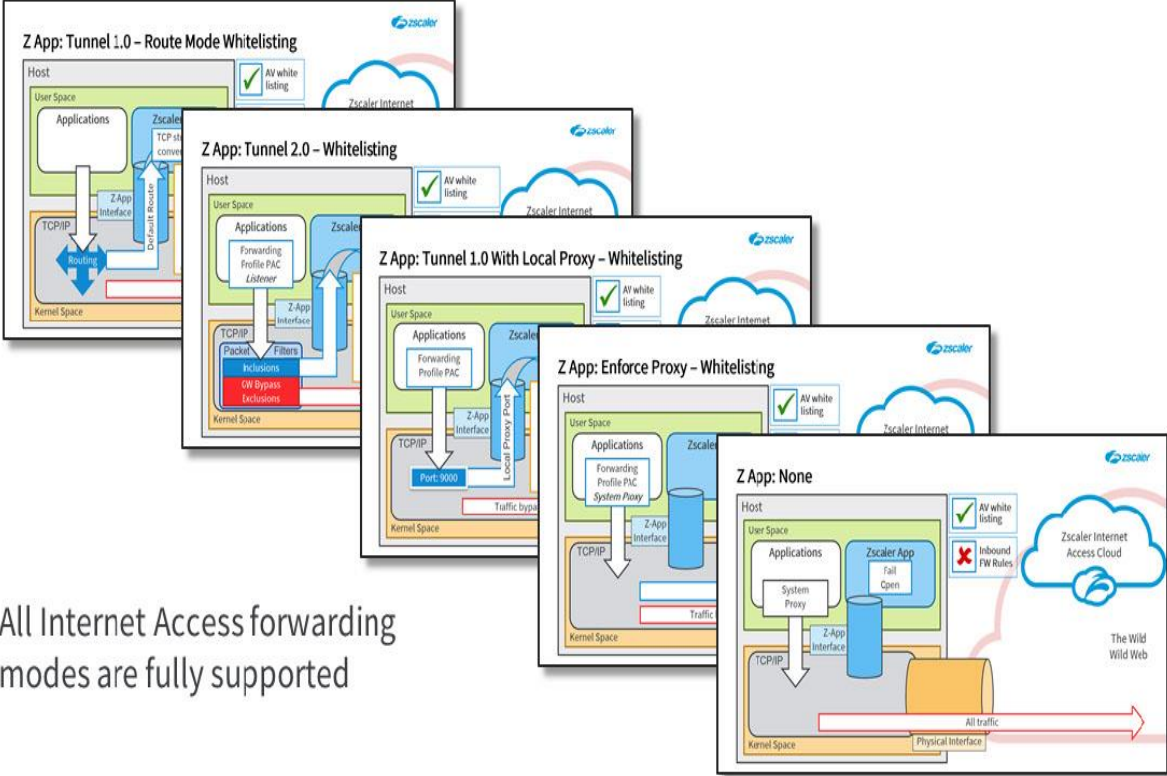
Slide notes

- **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 interfere with DHCP packets;
 - Plus, no adapter gateway related connectivity issues, such as Office activation, or Windows App Store connectivity issues.

Slide 22 - Zscaler App: Internet Access Forwarding



Zscaler App: Internet Access Forwarding



- All Internet Access forwarding modes are fully supported

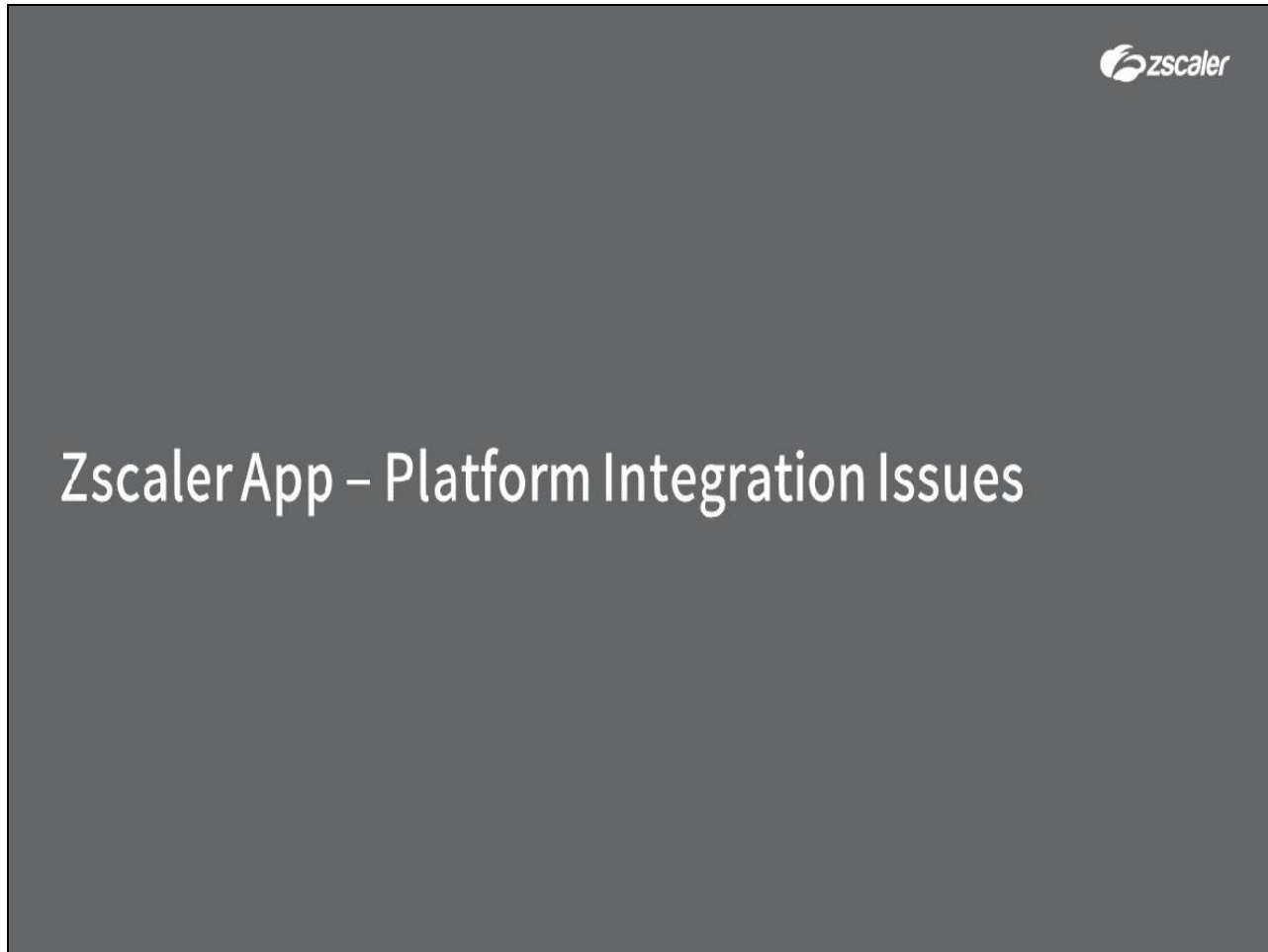
Slide notes

If the Zscaler App is also used for Internet Access, then any of the available forwarding modes can be specified for Internet Security forwarding;

- Tunnel 1.0,
- Tunnel 2.0,
- Tunnel (1.0) With Local Proxy,
- Enforce Proxy,
- And None.

See the **Zscaler App - Under the Covers** module in the **ZCCP-IA** content for full details.

Slide 23 - Zscaler App – Platform Integration Issues



Slide notes

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

Slide 24 - Zscaler App: Personal Firewall and AV Whitelisting



Zscaler 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 25 - Zscaler App: Personal Firewall and AV Whitelisting



Zscaler App: Personal Firewall and AV Whitelisting

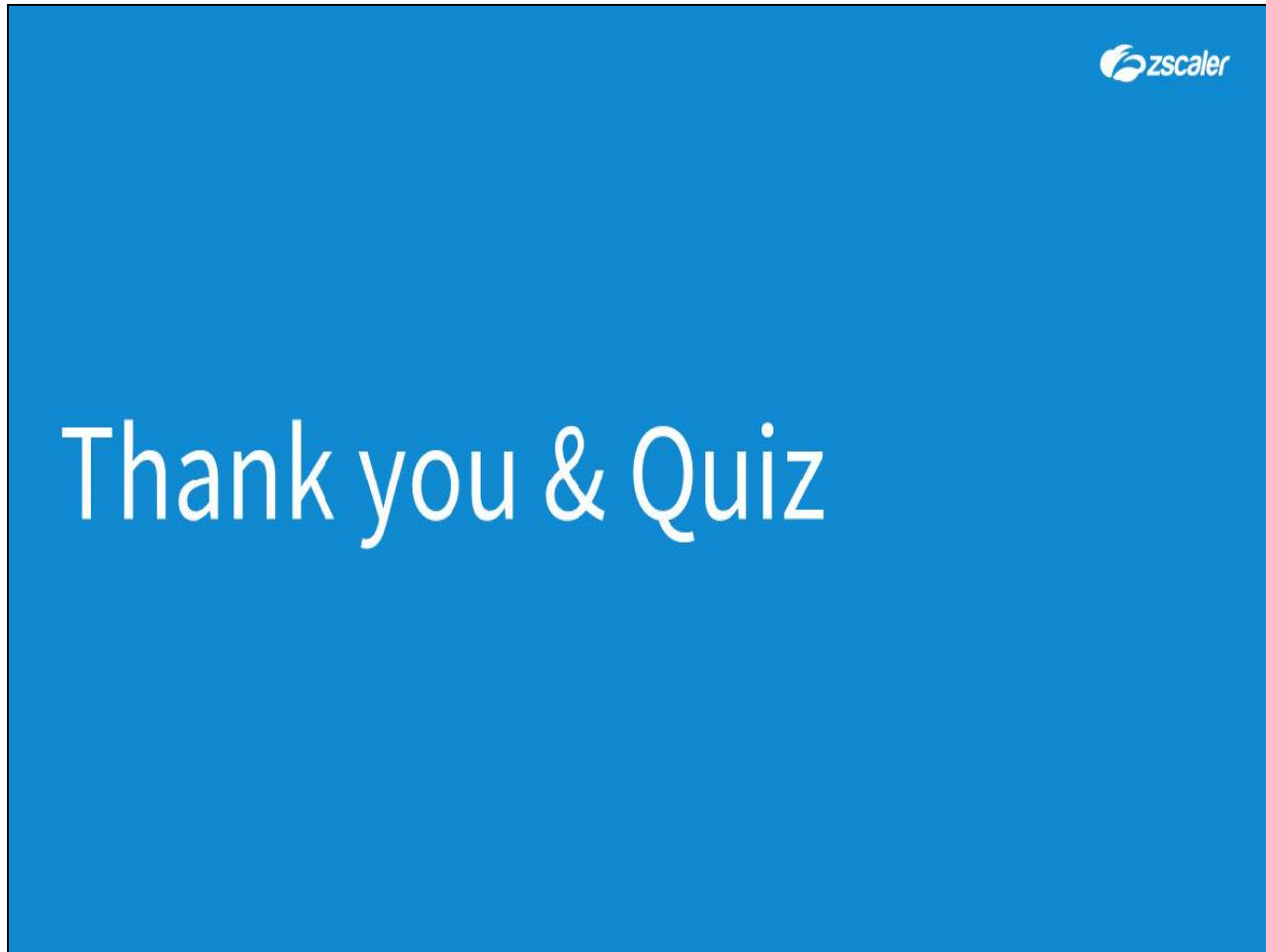
- Endpoint protection vendors
 - Whitelisting agreements with: Kaspersky, Trend Micro
 - Other vendors require binary and process white listing
 - Use an AD GPO to apply white listing rules
- Personal Firewall
 - Inbound and outbound rules for all protocols and ports
 - Use an AD GPO to apply Firewall 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 26 - 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.

What follows is a short 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.