Slide 1 - Zscaler Private Access

zscaler

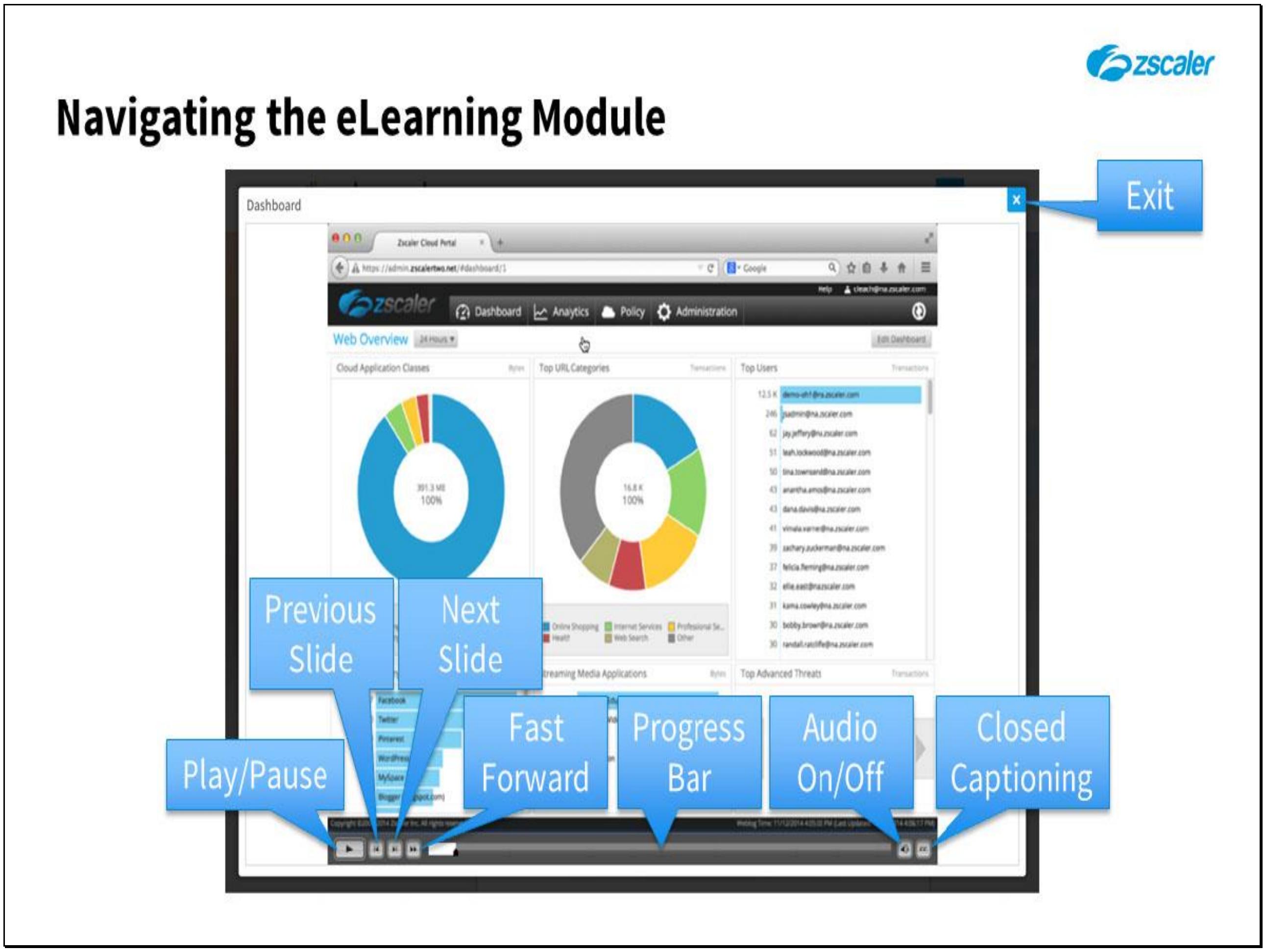
Zscaler Private Access

Architecture – Connector Deployment Options

Slide notes

Welcome to this training module that looks at some deployment options for ZEN Connectors.

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, next slide and fast forward. You can also mute the audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the ' X ' button at the top to exit.

Slide 3 - Agenda

Agenda

- Connector Deployment Recommendations
- Other Deployment Options

Slide notes

In this module we will first look at the recommended deployment for a ZEN Connector, and then at some other options available.

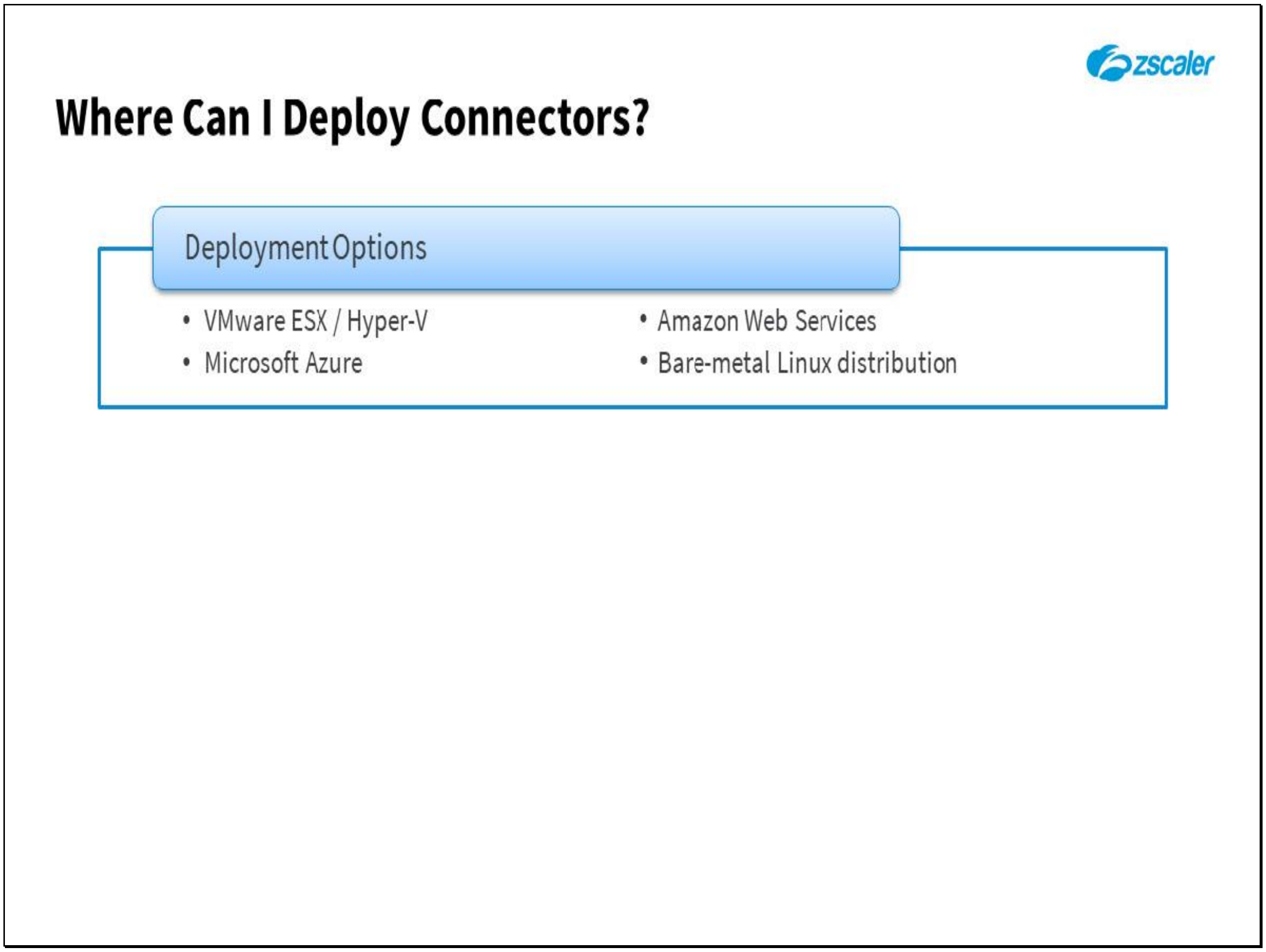
Slide 4 - Connector Deployment Recommendations

Connector Deployment Recommendations

Slide notes

The first topic we will cover is a look the recommended ZEN Connector deployment.

Slide 5 - Where Can I Deploy Connectors?



Where Can I Deploy Connectors?

Deployment Options

- VMware ESX / Hyper-V
- Microsoft Azure
- Amazon Web Services
- Bare-metal Linux distribution

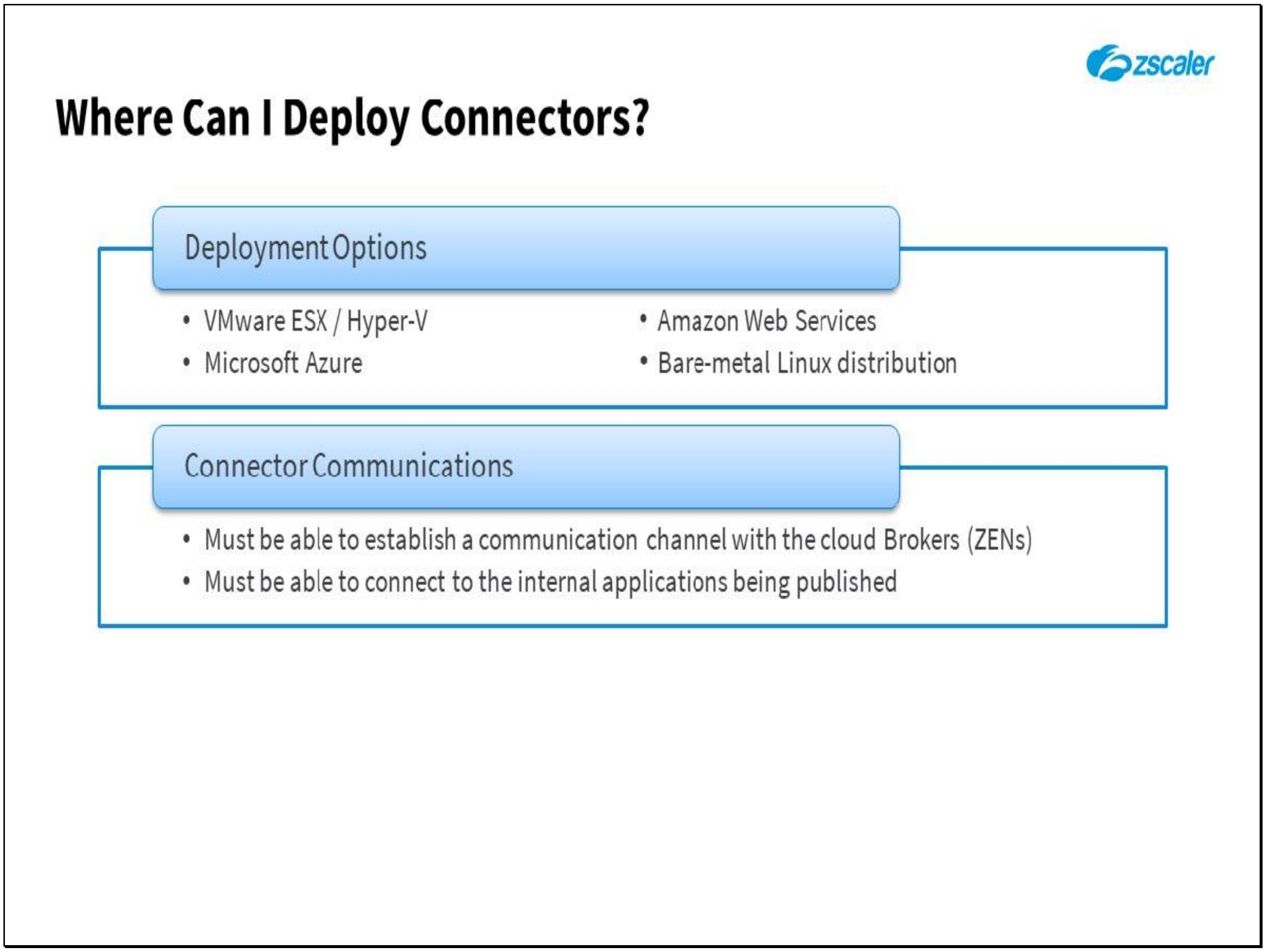
Slide notes

There are a number of platforms that support the deployment of a ZEN Connector, including:

- VMware ESX and Hyper-V;
- AWS;
- Microsoft Azure;
- Or even as an RDP deployed on a bare metal Linux box (real or virtual).

We recommend that you deploy the pre-built VMware package, as we have stripped down the underlying OS to pre-configure it, remove all unnecessary services, and harden it.

Slide 6 - Where Can I Deploy Connectors?



Where Can I Deploy Connectors?

Deployment Options

- VMware ESX / Hyper-V
- Microsoft Azure
- Amazon Web Services
- Bare-metal Linux distribution

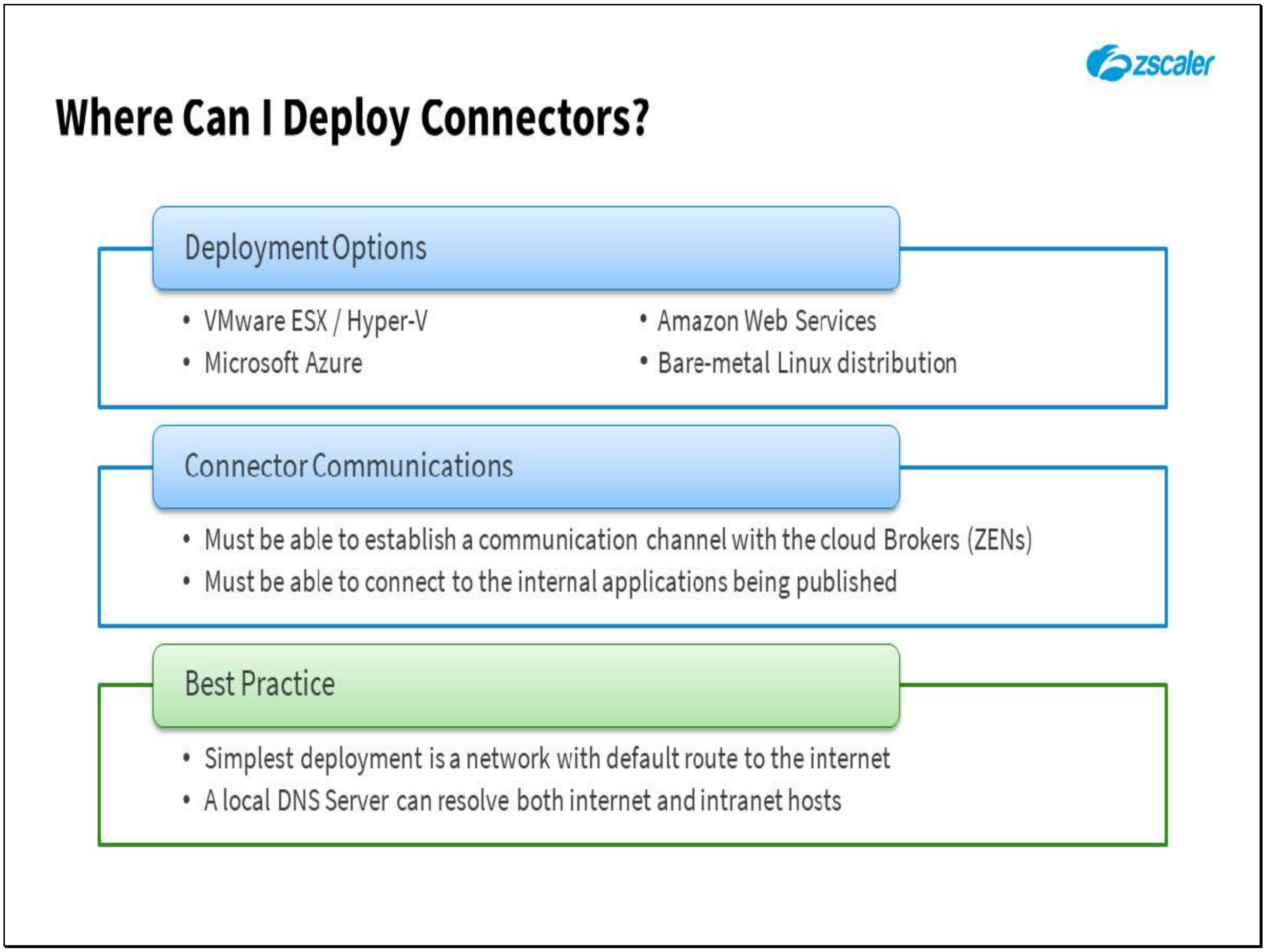
Connector Communications

- Must be able to establish a communication channel with the cloud Brokers (ZENs)
- Must be able to connect to the internal applications being published

Slide notes

External and internal communications from the Connector are critical for it to function. The Connector must be able to resolve and reach the external ZPA infrastructure hosts, and of course the internal applications that it is to provide connectivity to.

Slide 7 - Where Can I Deploy Connectors?



zscaler

Where Can I Deploy Connectors?

Deployment Options

- VMware ESX / Hyper-V
- Microsoft Azure
- Amazon Web Services
- Bare-metal Linux distribution

Connector Communications

- Must be able to establish a communication channel with the cloud Brokers (ZENs)
- Must be able to connect to the internal applications being published

Best Practice

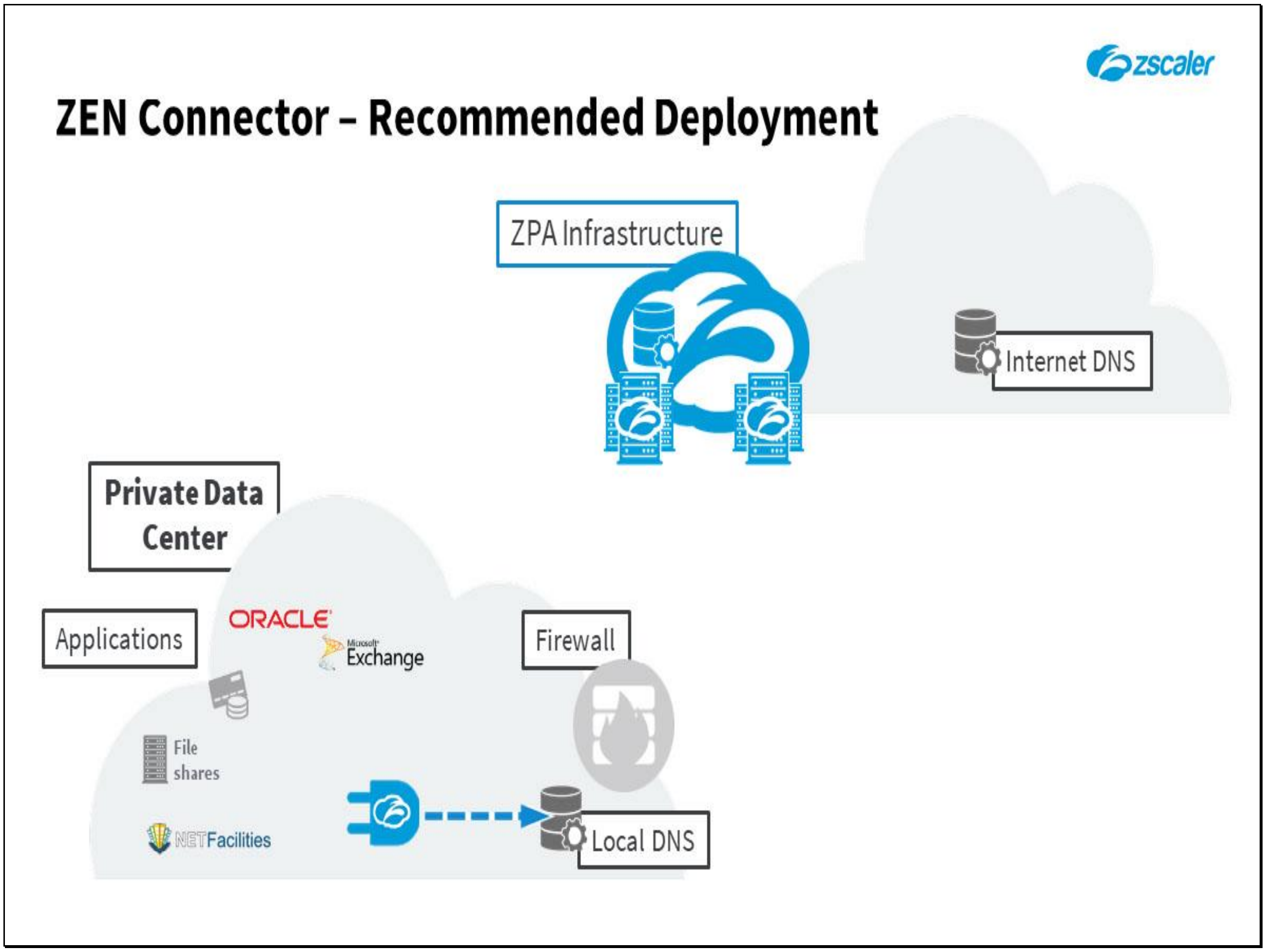
- Simplest deployment is a network with default route to the internet
- A local DNS Server can resolve both internet and intranet hosts

Slide notes

Our best practice recommendation, and the simplest deployment option for ZEN Connectors, is to place them on an internal network adjacent to the applications to be made available to end users with ZPA, ideally one with a default route to the Internet. Ideally the ZEN Connector can be pointed to a local DNS server that can manage the resolution of both internal and external hosts.

It is important to note that ZEN Connectors do not require, and do not listen for inbound connections from the Internet, so there is no real need to locate them in the DMZ.

Slide 8 - ZEN Connector – Recommended Deployment

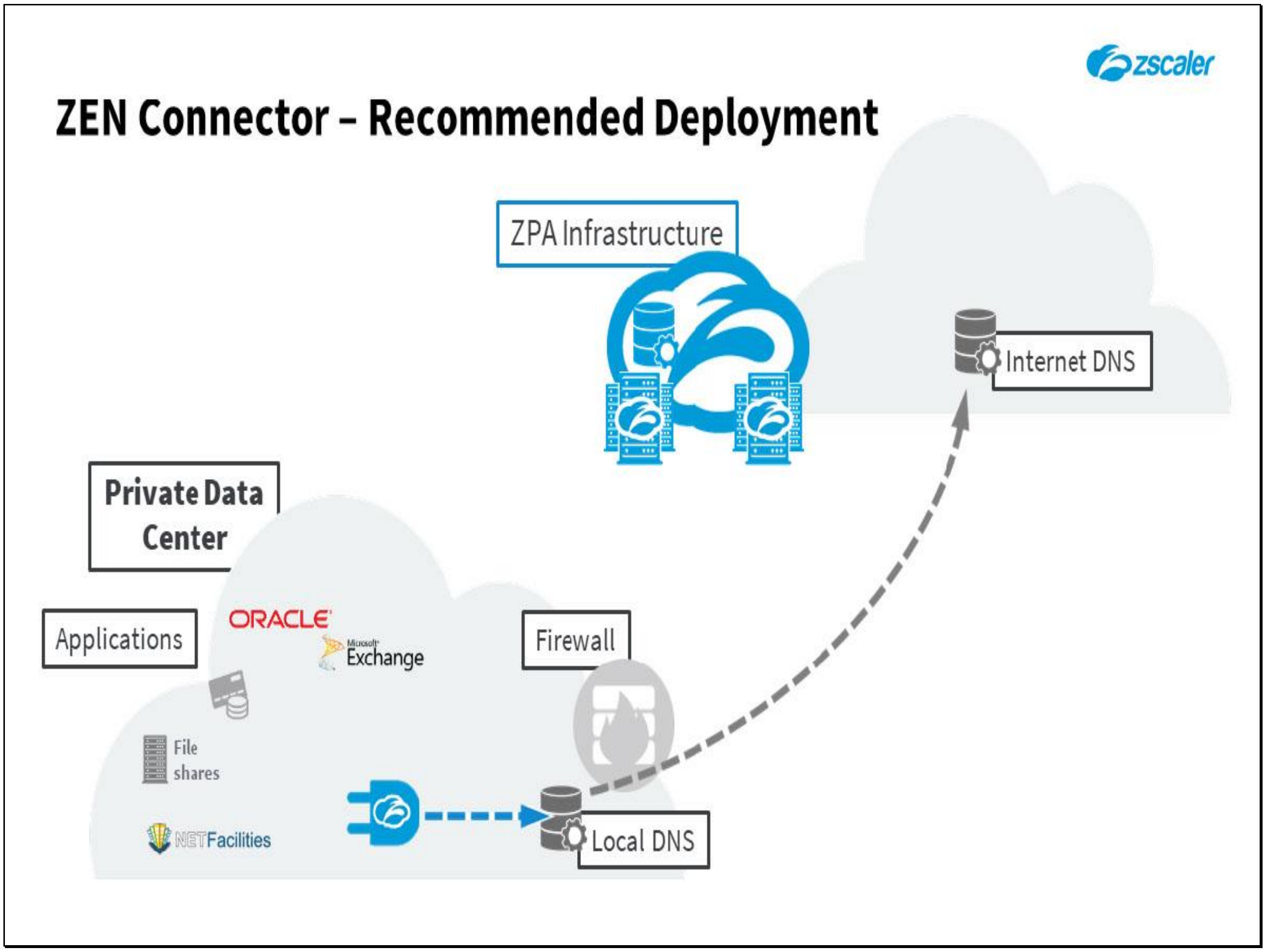


ZEN Connector – Recommended Deployment

Slide notes

To illustrate the recommended ZEN Connector deployment, here we see it deployed on an internal network that has a default route to the Internet. The Connector has been provided with the address of an internal DNS server, which can be done either through DHCP, or it may be statically defined on the Connector host OS.

Slide 9 - ZEN Connector – Recommended Deployment

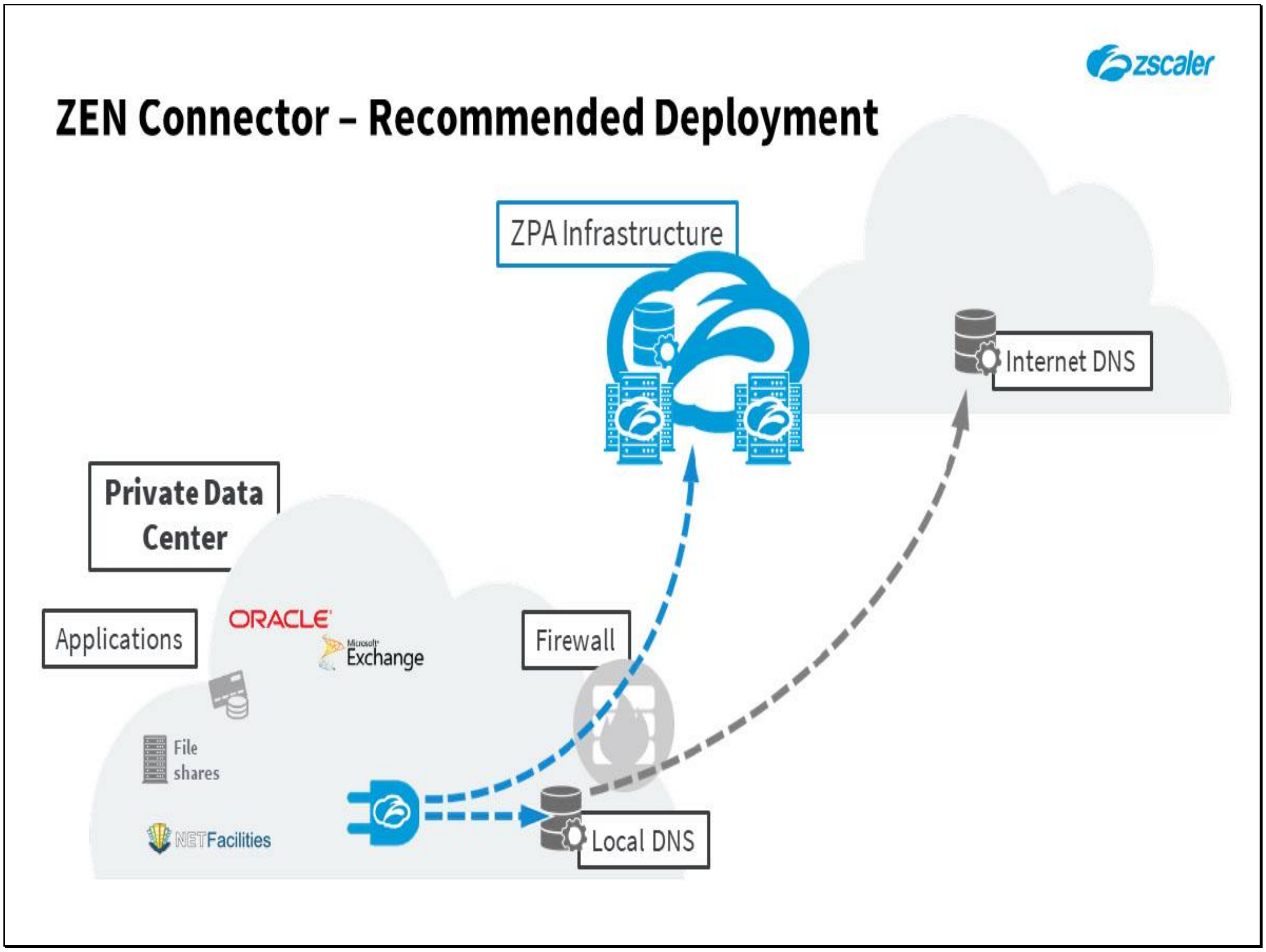


ZEN Connector – Recommended Deployment

Slide notes

The internal DNS server in this case, also has the ability to resolve external hosts, …

Slide 10 - ZEN Connector – Recommended Deployment

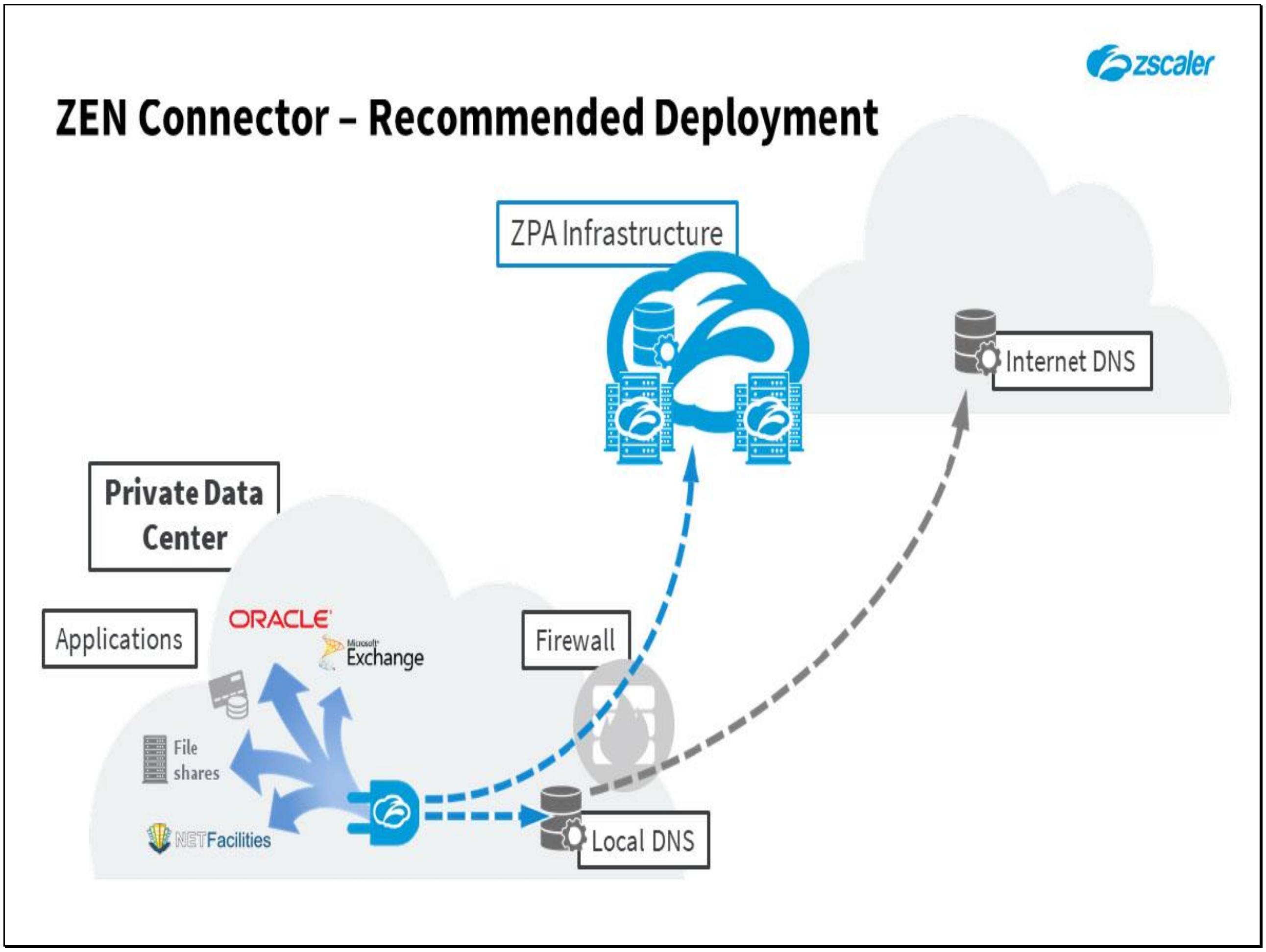


ZEN Connector – Recommended Deployment

Slide notes

…which allows the Connector to resolve and contact the ZPA infrastructure using TLS 1.2 on destination port 443.

Slide 11 - ZEN Connector – Recommended Deployment



ZEN Connector – Recommended Deployment

Slide notes

The DNS server will of course be able to resolve the hosts for the internal applications to be made available over ZPA through this Connector.

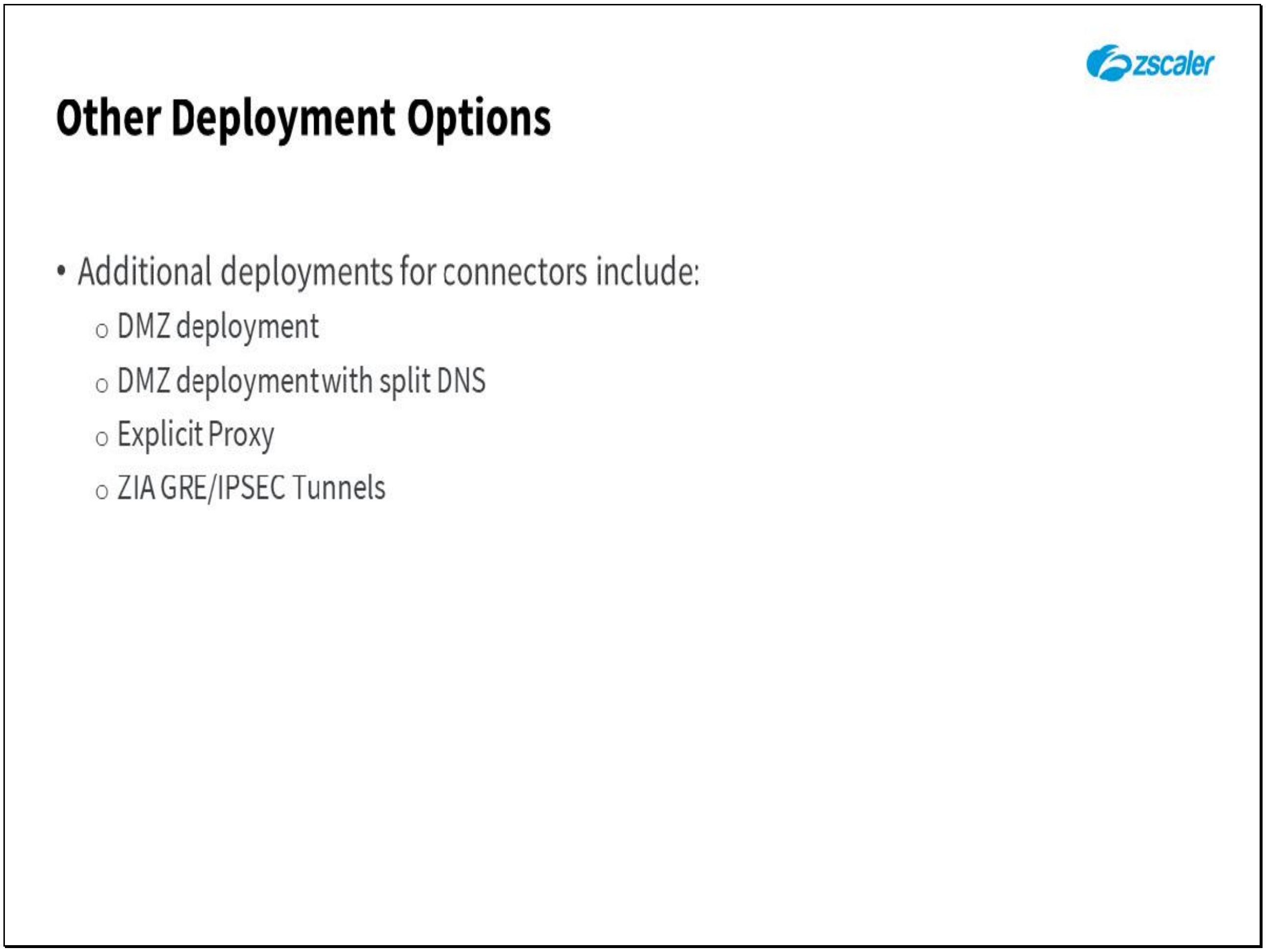
Slide 12 - Other Deployment Options

Other Deployment Options

Slide notes

The last topic we will cover is a look some of the options available for a ZEN Connector deployment.

Slide 13 - Other Deployment Options



Other Deployment Options

- Additional deployments for connectors include:
  - DMZ deployment
  - DMZ deploymentwith split DNS
  - Explicit Proxy
  - ZIA GRE/IPSEC Tunnels

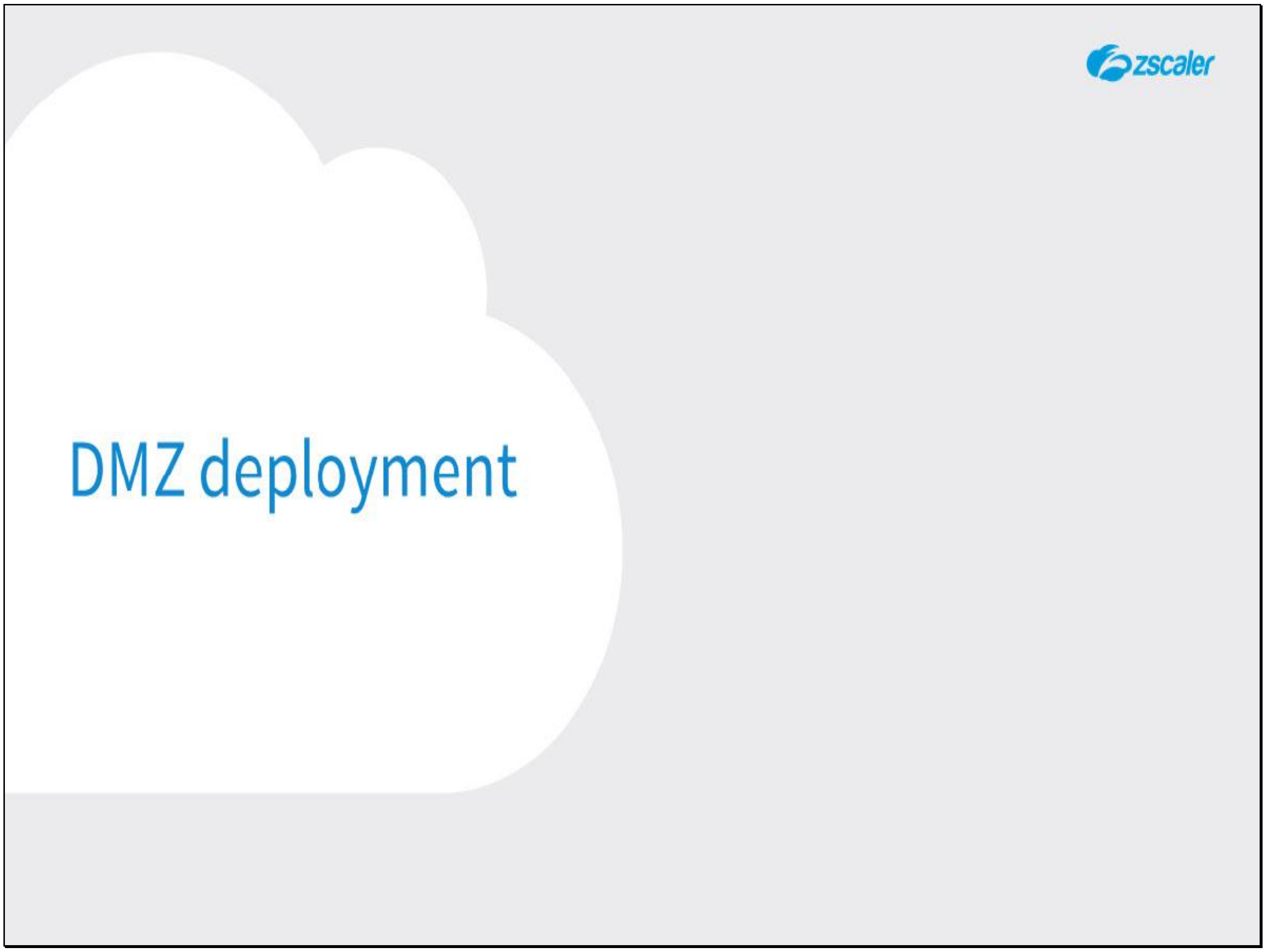
Slide notes

The additional deployment options we will look at are:

- Connector on the DMZ with firewall rules to access internal resources;
- Connector on the DMZ with a split DNS configuration;
- Connector tunneling via an explicit proxy;
- And Connector tunneling via a Zscaler Internet Access tunnel (GRE or IPSec).

Note that all of these options are sub-optimal and not recommended for production deployments, unless there are circumstances that dictate otherwise.

Slide 14 - DMZ deployment

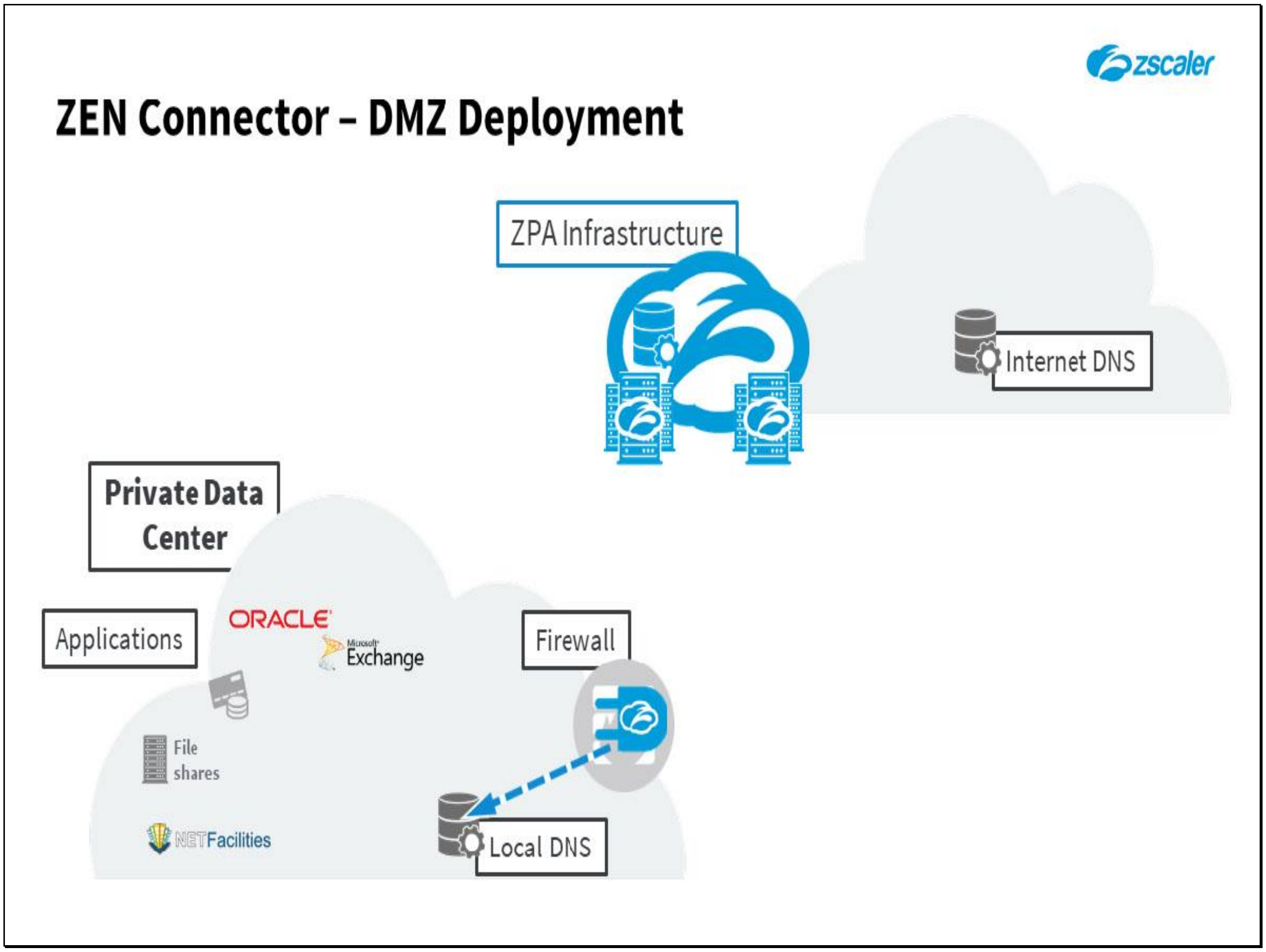


DMZ deployment

Slide notes

First, let’s look at the option of deploying Connectors in the DMZ.

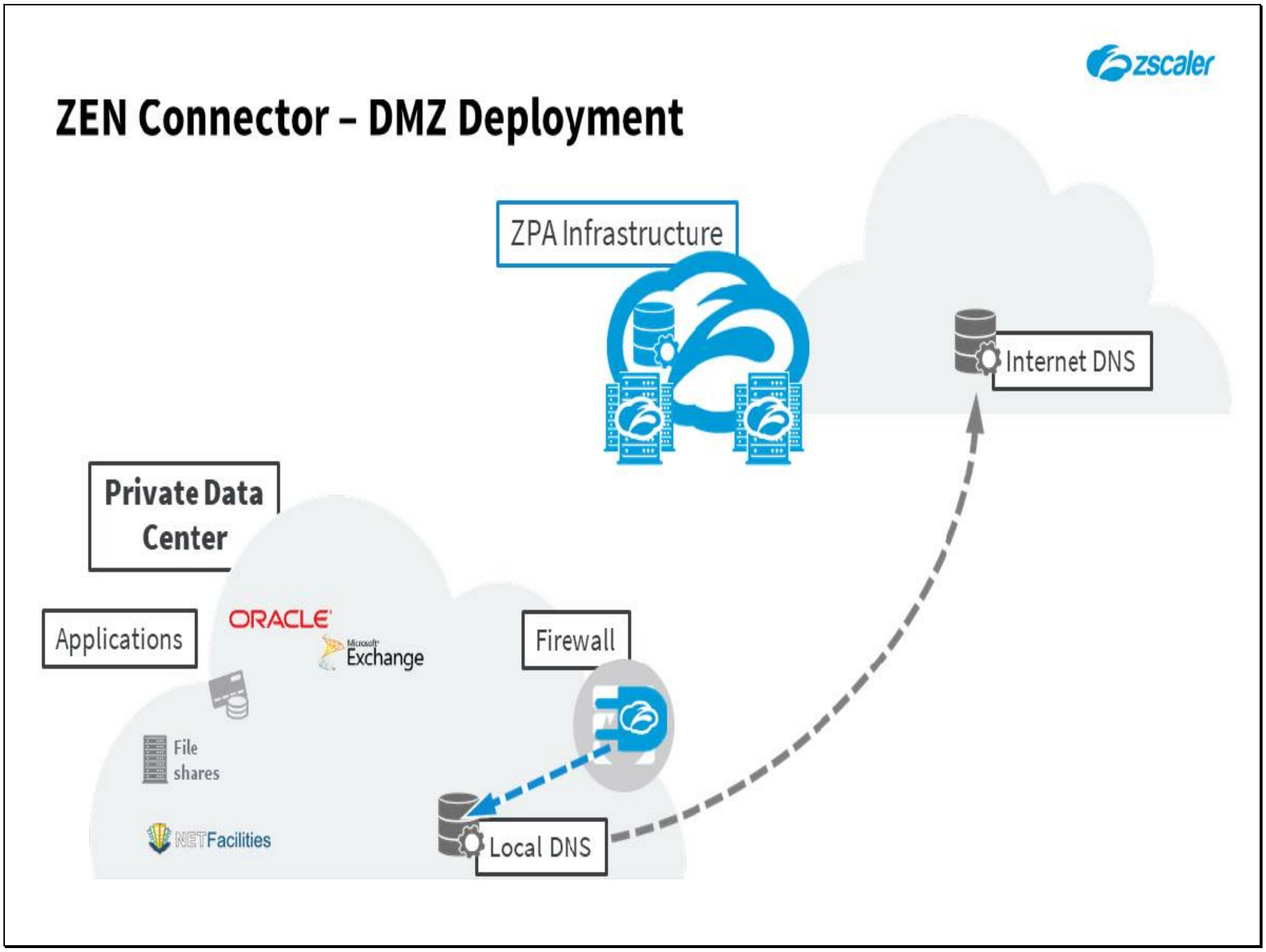
Slide 15 - ZEN Connector – DMZ Deployment



Slide notes

In this deployment model, the Connector is installed on the DMZ subnet of your corporate firewall. The Connector will of course need to be configured with a DNS server capable of resolving internal hosts, which may mean that DNS requests from the Connector will need to transit the internal firewall.

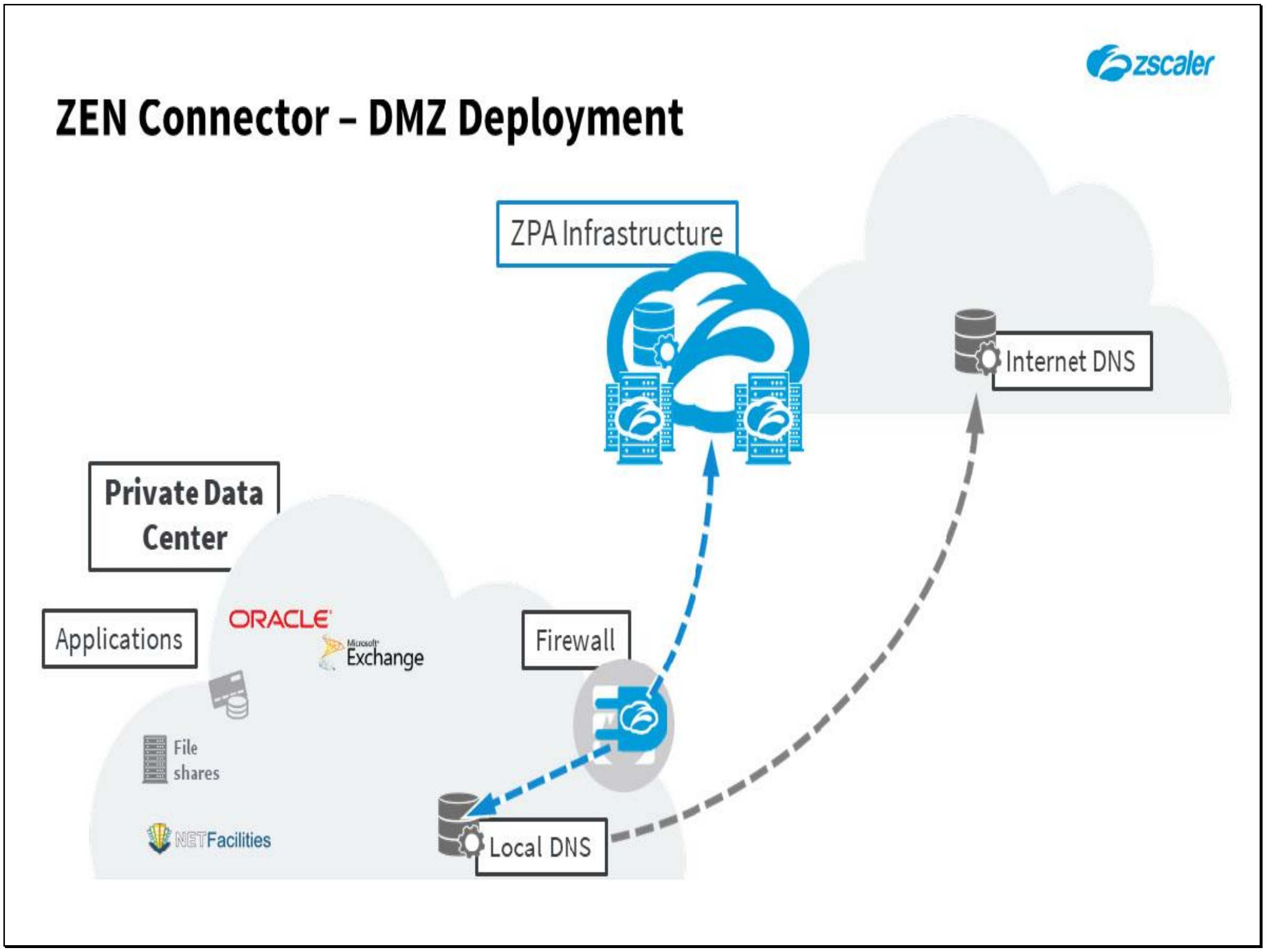
Slide 16 - ZEN Connector – DMZ Deployment



Slide notes

The internal DNS server should ideally also be able to resolve externally, so the Connector can find the IP addresses for the ZPA infrastructure, …

Slide 17 - ZEN Connector – DMZ Deployment

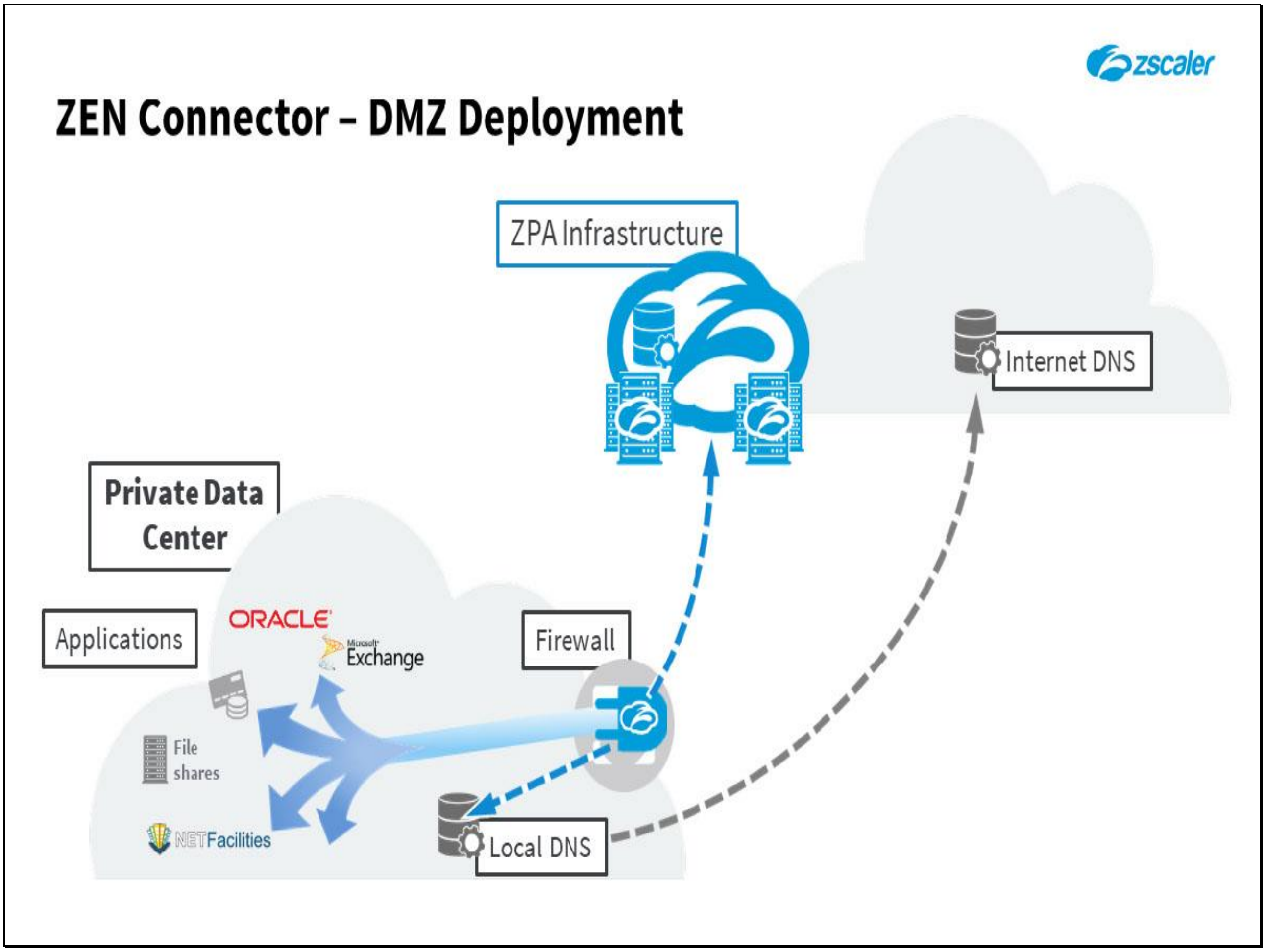


ZEN Connector – DMZ Deployment

Slide notes

…that it needs to enroll with, and tunnel to.

Slide 18 - ZEN Connector – DMZ Deployment



Slide notes

Of course, with the Connector in the DMZ, it must transit the interior firewall in order to reach the private applications that it needs to provide access for. This will require firewall configuration to allow communications from the Connector to these internal applications, to include all the protocols and ports necessary for application connections to work (including ICMP for UDP applications).

As a reminder, the Connector is not a traditional appliance that is listening for inbound connections from the Internet; it only ever establishes connections in the outbound direction. As a consequence, there is no real need for the ZEN Connectors to be deployed in your corporate DMZ, it is perfectly acceptable (and simpler) to install them on the internal network. Configuring the internal firewall is an unnecessary complication, and an additional opportunity for misconfigurations.

Slide 19 - DMZ deployment with split DNS

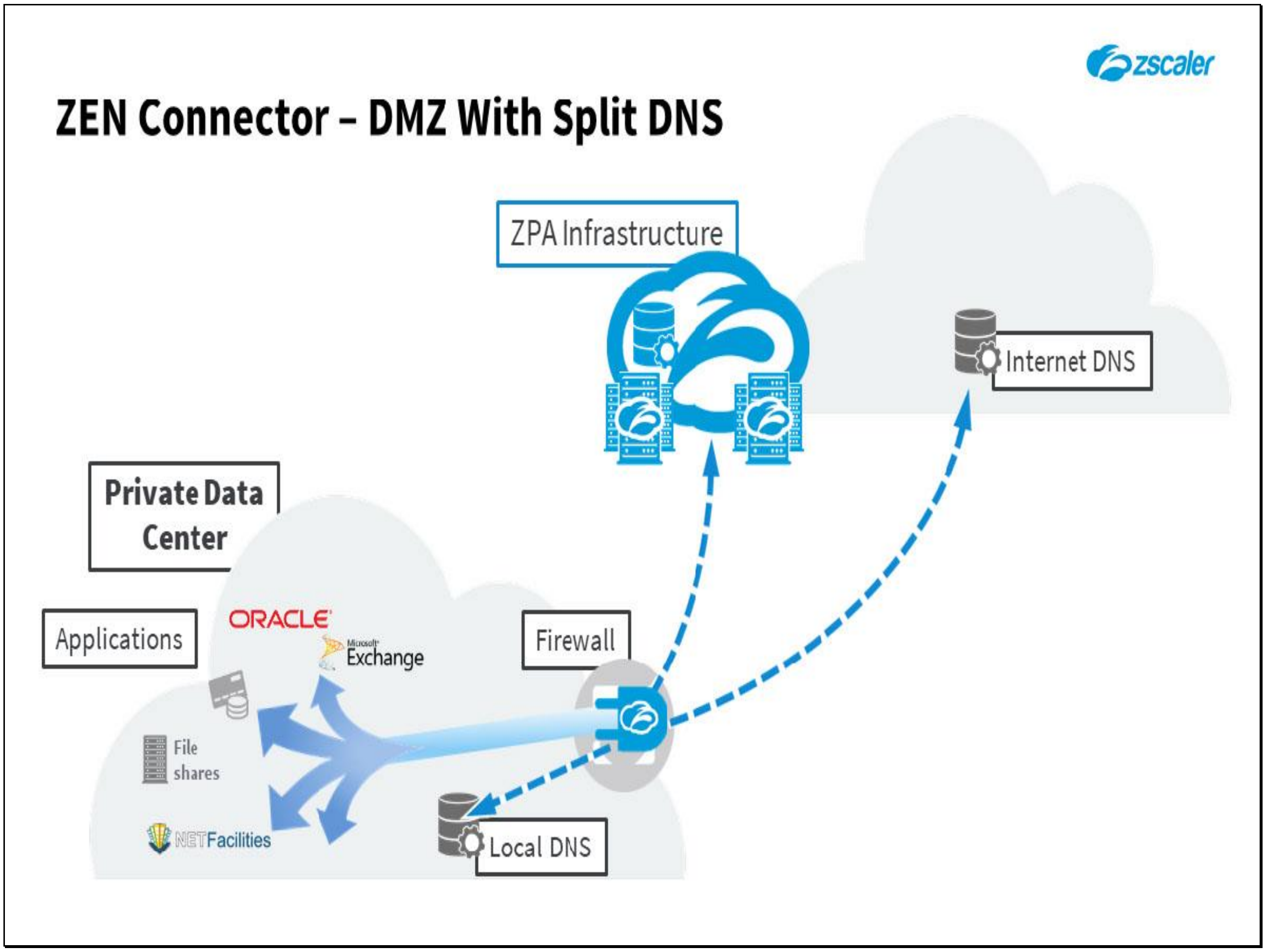
zscaler

DMZ deployment with split DNS

Slide notes

Next, let’s look at the DMZ option with split DNS.

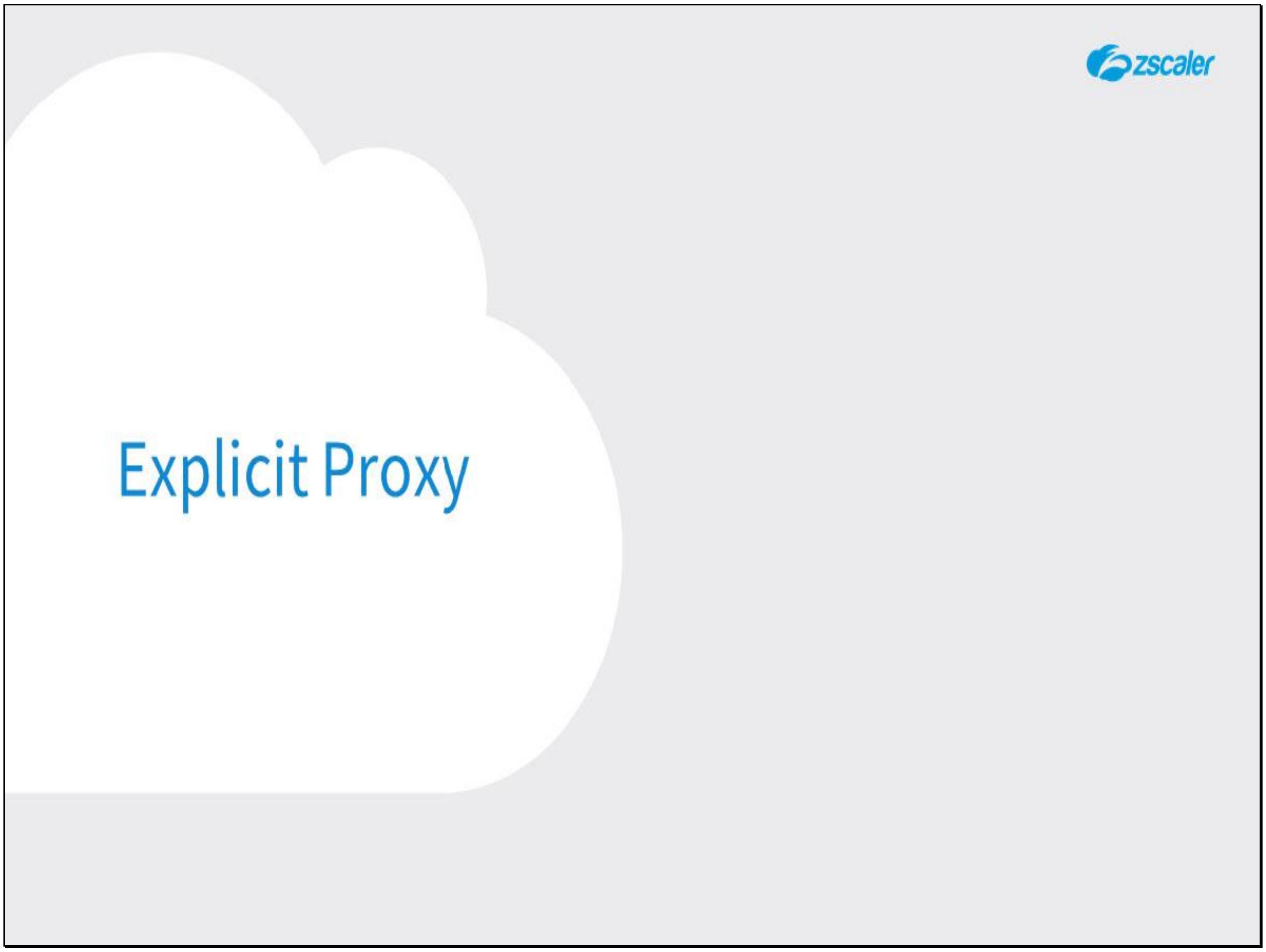
Slide 20 - ZEN Connector – DMZ With Split DNS



Slide notes

This model is very similar to the simple DMZ deployment option we just looked at, however in this case a DNS solution such as ‘unbound’ can be used to resolve against different internal and external DNS servers. In this case, not only do you need to worry about the rules at the internal firewall, you also need to configure the DNS environment correctly.

Slide 21 - Explicit Proxy

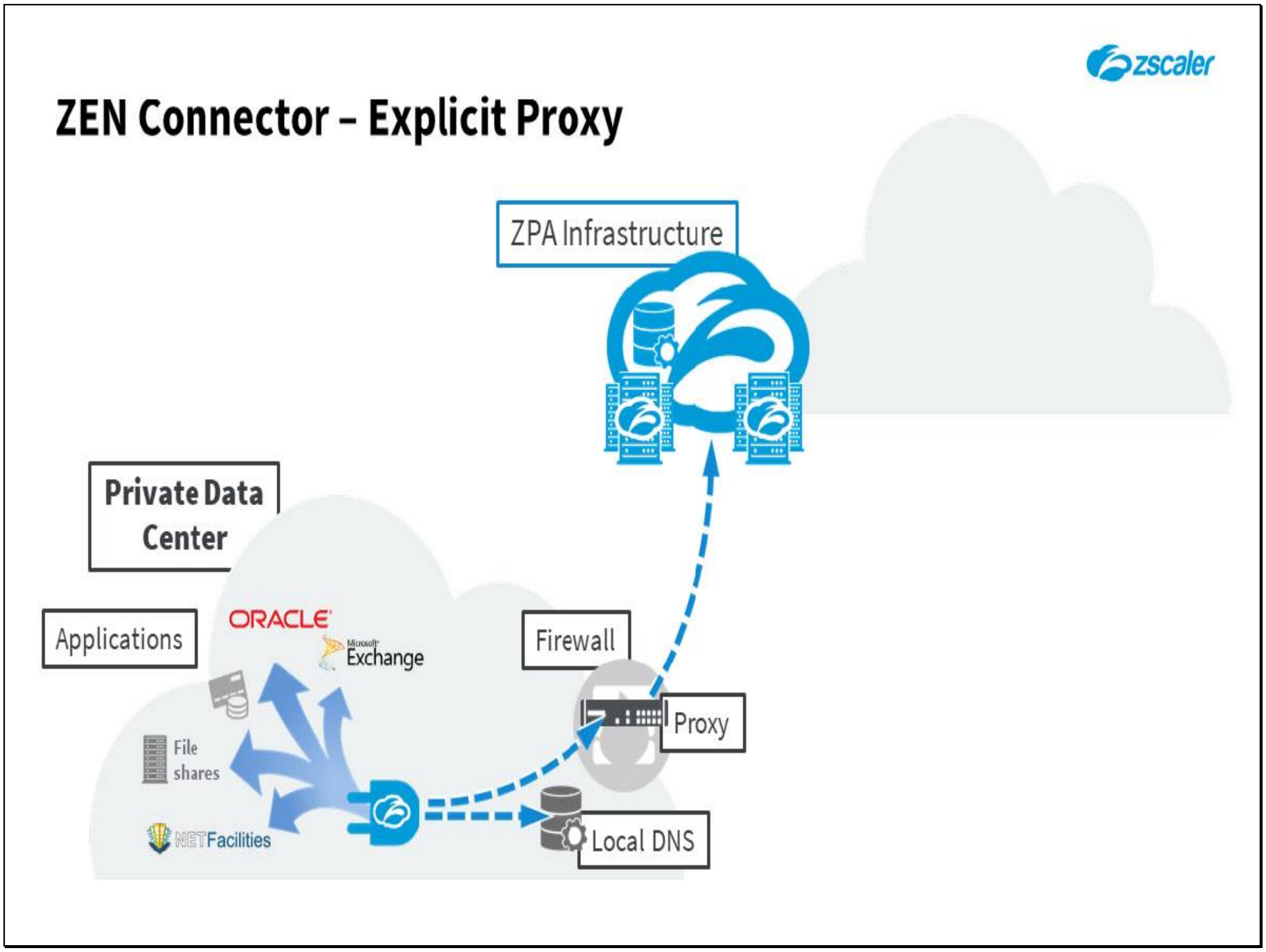


Explicit Proxy

Slide notes

Next, we'll look at the option for Connectors communicating via an explicit proxy.

Slide 22 - ZEN Connector – Explicit Proxy



ZEN Connector – Explicit Proxy

Slide notes

In this instance, the Connector is explicitly configured (at the CLI) to connect via some 3rd party proxy solution. While this is possible and is a supported configuration (as long as the proxy does no SSL interception), it is not a recommended deployment scenario.

Remember that the Connector tunnels are always validated in both directions and are doubly pinned. Any attempt to intercept these connections will result in the failure to establish any tunnels to the ZPA infrastructure and consequently ZPA connectivity will fail.

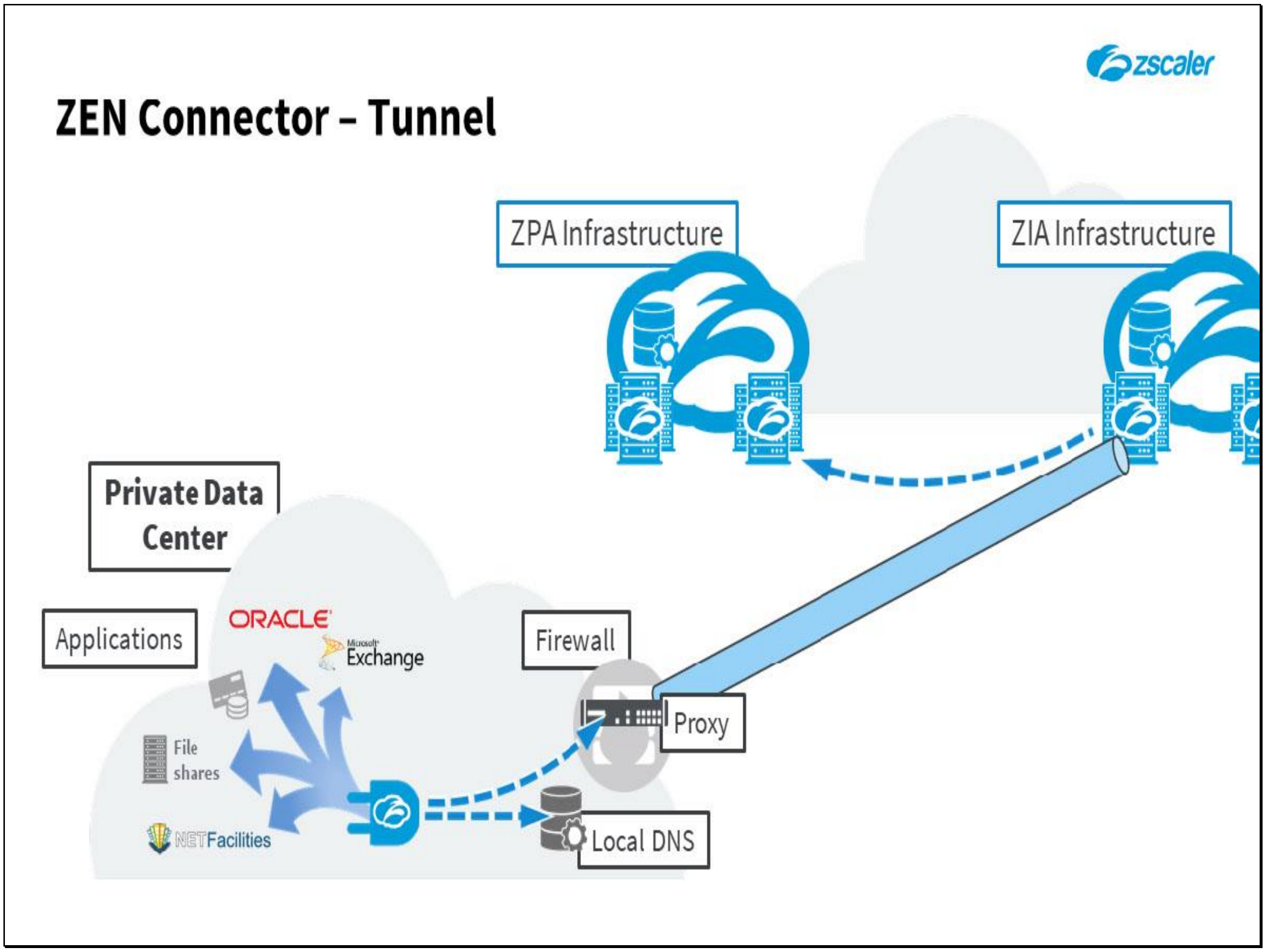
Slide 23 - ZIA GRE/IPSEC Tunnels

ZIA GRE/IPSEC Tunnels

Slide notes

Finally, let’s look at the option for Connectors to connect via an existing ZIA tunnel.

Slide 24 - ZEN Connector – Tunnel



ZEN Connector – Tunnel

ZPA Infrastructure

ZIA Infrastructure

Private Data Center

Applications

Firewall

Proxy

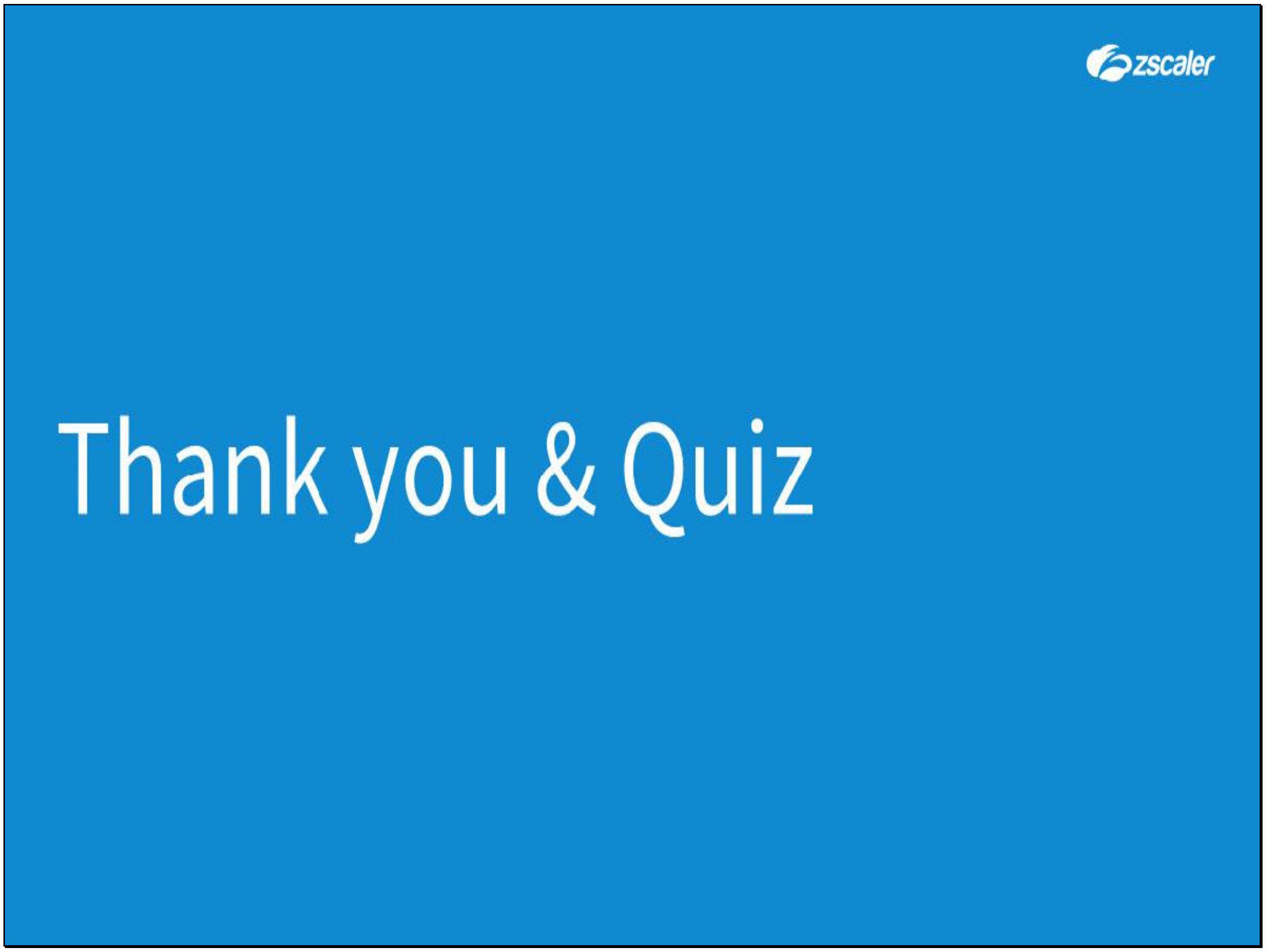
Local DNS

Slide notes

In this situation, with an edge device of some description that is already tunneling traffic to Zscaler for Internet security scanning, ZPA traffic may also be routed through these tunnels. However, as should be obvious from the diagram, this results in highly sub-optimal routing and consequently latency and response time issues for your end users. There can also be MTU issues, and unexpected timeouts that additionally affect performance. Also note that SSL inspection for ZPA tunnel traffic is not supported at all, for the same reason as for a 3rd party proxy.

This scenario may be an option for an existing ZIA customer who wishes to run a ZPA proof of concept without any major infrastructure changes. It would be strongly recommended that in production routing rules are applied to ensure that ZPA traffic goes direct to the Internet, without the need to tunnel it to the ZIA cloud.

Slide 25 - 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.

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.