

Slide 1 - Zscaler Private Access



Zscaler Private Access

Architecture – Best Practices

©2018 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on the Zscaler Private Access best practices.

Slide 2 - Navigating the eLearning Module

Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. At the top right is the Zscaler logo. Below it is a navigation bar with links: Dashboard, Analytics, Policy, and Administration. The main content area is titled 'Web Overview' and contains several charts and tables. Overlaid on the bottom of the dashboard are several blue callout boxes with white text, each pointing to a specific control on the video player interface. These controls include: 'Previous Slide', 'Next Slide', 'Fast Forward', 'Progress Bar', 'Audio On/Off', 'Closed Captioning', and an 'Exit' button at the top right corner of the dashboard window.

Dashboard

Exit

Previous Slide

Next Slide

Fast Forward

Progress Bar

Audio On/Off

Closed Captioning

Play/Pause

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 Best Practices
- Certificates Best Practices
- Authentication Best Practices
- Z-App Best Practices
- Application Best Practices
- Monitoring Best Practices
- LSS Best Practices

Slide notes

In this module we will look at best practices across the following areas: for ZEN Connector deployment and management; for certificate management; for authentication; for the Zscaler App; for the management of applications; for health and monitoring of the whole system; and for the Log Streaming Service.

Slide 4 - Connector Best Practices



Slide notes

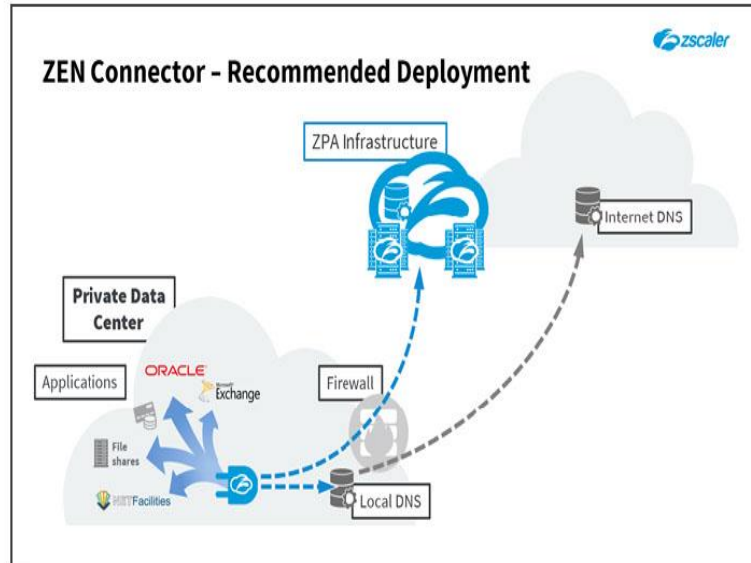
The first topic we will cover is a look at some Connector best practices.

Slide 5 - Connector Deployment Best Practices

Connector Deployment

• Network Topology

- Connector on an internal network segment
- Default route to internet
- Internal DNS server that can also resolve external hosts
- Unrestricted access to internal applications (also with ICMP)
- No proxies on the enrollment, or data path



Slide notes

As has been discussed elsewhere, our recommendations for ZEN Connector deployment are:


- Install the Connectors on an internal network segment, adjacent to the applications that they are to provide connectivity to;
- Ideally that network segment should be configured with a default route to the internet;
- The Connector should be configured to contact an internal DNS server capable of resolving hosts for all the applications that need to be supported, and for hosts on the internet;
- The Connectors should have unrestricted access to the applications, with no protocol or port limitations or restrictions, to include ICMP access;
- While an explicit proxy on the Connector enrollment and subsequent data path can be supported, it is certainly not recommended. Also remember that any attempt at SSL interception on the Connector's traffic will cause ZPA communications to fail (because of the certificate pinning).

Caution: ICMP access to UDP applications is a hard requirement, as it is used to determine the RTT to the application host (which is important for making load-balancing decisions). For TCP applications ICMP access is less critical although highly desirable.

Slide 6 - Connector Group Best Practices

Connector Group Configuration

- **Location-sensitive Applications**
(users must be associated to local AD DC)
 - Use location-based Connector Groups
 - Define the actual site location in the Connector Group configuration



Location-specific Connector Groups


Slide notes

For customers with 'location-sensitive' apps, such as Active Directory (AD) domain controllers used for DFS and other AD services, where the user needs to be associated to a local AD Domain Controller (DC), the following best practices apply:

- You must use location-based Connector Groups (meaning that all Connectors at site A are in Connector Group A, all Connectors at site B are in Connector Group B, etc.); this is to ensure that the user is always connected to an application instance that is local to them.
- You should statically define the actual site location (by locale name, street address, or latitude and longitude) in the Connector Group definition, as this is used to determine the geographically closest instance of an application.

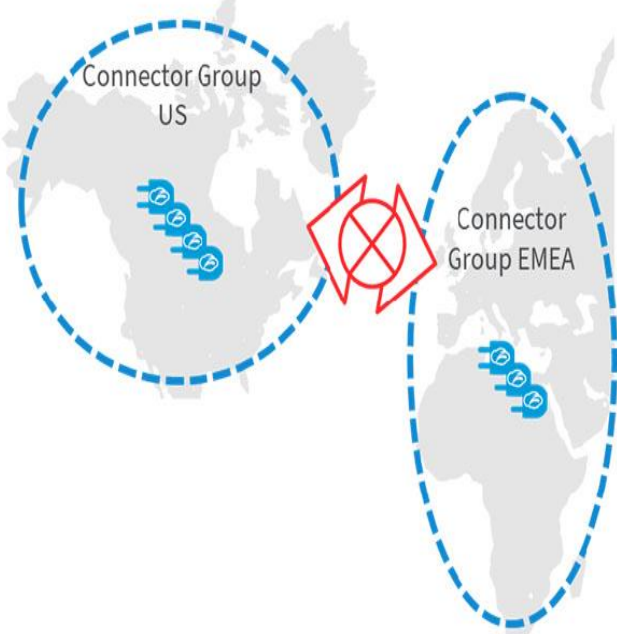
Note that this would be considered the 'normal' situation for Connector Group configurations.

Slide 7 - Connector Group Best Practices



Connector Group Configuration

- **Non-Location-sensitive Applications**
 - Single Connector Group may be used for dispersed geographies (e.g. US vs. EMEA)
 - Connectors in one Connector Group should NOT be able to reach Applications in another
 - Specify a 'center-of-mass' location in the Connector Group configuration (Note that Connectors will be geo-located based on egress IP address)



Slide notes

If a customer has no location-sensitive apps, and all UDP-based apps are ICMP-reachable, then the following best practices apply:

- You may use a single Connector Group per Geo (for example, all US Connectors are in a US Connector Group, all EMEA Connectors are in an EMEA Connector Group) to allow the system to choose an optimal path based on the RTT between the Connectors and application instances. In this case, the Connectors in one Geo should not be able to reach applications in another Geo (to avoid any possibility of sub-optimal path selection). Note that if you only have end users within a single Geo, then you should have all your Connectors in the one Connector Group.
- As a location (locale name, street address, or Latitude and Longitude) must be defined on the Connector Groups, it is recommended that you use a location that is 'center of mass' of the region in question. As an example, for the US Geo (including Alaska and Hawaii) use Belle Fourche, South Dakota (Lat. 44 58 02.07622(N) Long. 103 46 17.60283(W), which is considered as the geographic center of the US by the National Geographic Service (NGS). Note that this location definition does not impact optimum path selection.

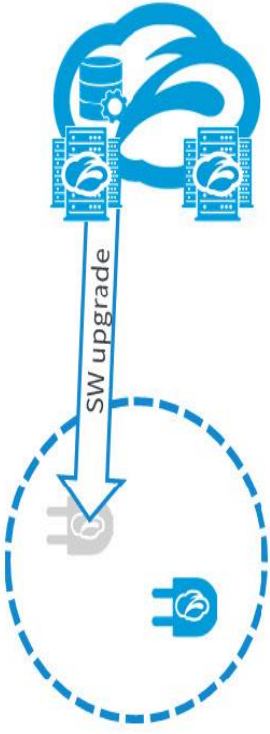
This should be the exception case, to provide a rational path selection for customers that don't have location-sensitive apps.

Slide 8 - Connector Capacity and Redundancy Best Practices




Connector Capacity and Redundancy

- **Connector Redundancy**
 - Connector Groups MUST contain at least two Connectors
 - This ensures application availability during Connector SW upgrades

**Slide notes**

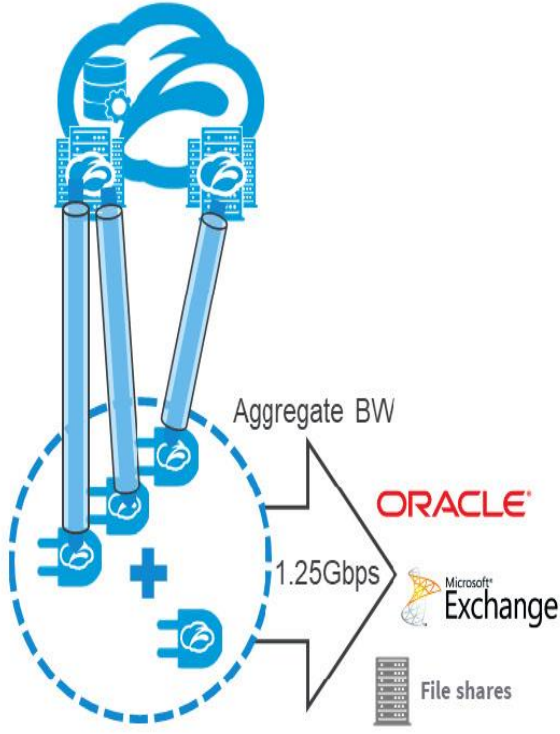
To ensure continuous availability, Connector Groups in a production environment MUST have a minimum of two Connectors. It is important to understand that while the rolling upgrade to Connectors within a Connector Group is taking place, one Connector can be out of service for a time as it reboots to apply the new SW.

Slide 9 - Connector Capacity and Redundancy Best Practices



Connector Capacity and Redundancy

- **Connector Capacity**
 - Implement Connectors with at least the minimum resource requirements
 - A Connector supports up to 500Mbps of data throughput
 - Add additional Connectors to provide the required capacity on an N+1 basis, e.g.
 - Application access requirement estimated at 1.25Gbps
 - Minimum Connectors required = 3 (1.5Gbps)
 - Minimum Connectors with N+1 redundancy = 4 (2Gbps)


Slide notes

Connectors must always be implemented with at least the minimum resource specifications for the host machine or virtual machine (VM), to ensure at least the specified capacity and throughput. Connector Groups in a production environment **SHOULD** be scaled to provide N+1 redundancy for estimated aggregate bandwidth required for application access. This will ensure that Connectors can provide enough bandwidth to service the anticipated user traffic, even during an upgrade window (when the rolling upgrade is taking one Connector out of service at a time).

Remember that each Connector can support up to 500Mbps of data throughput, so as an example, if your expected aggregate bandwidth requirement for application access is 1¼Gbps, you will need at least three Connectors to support that traffic. To provide the necessary redundancy to allow uninterrupted user access during a Connector upgrade window, add one more Connector.

Note: All Connectors (even the redundant Connectors) are managed in an active/active configuration, so adding a redundant Connector gives you excess capacity during normal operation and spreads the proffered load across all of the available Connectors.

Slide 10 - Certificates Best Practices



Slide notes

The next topic we will cover is a look at some best practices for the management of ZPA certificates.

Slide 11 - Certificates Best Practices – Self-Signed

Certificates Best Practices – Self-Signed

- **Self-Signed Certificates**


- Use the default set of certificates generated when first subscribing to ZPA

Name	Creation Date	Expiry Date	Common Name	
Client	Friday, March 09 2018 7:24:30 am	Saturday, March 05 2033 7:24:30 am	ptraining1.safemarch.com/Client	
Connector	Friday, March 09 2018 7:24:31 am	Saturday, March 05 2033 7:24:30 am	ptraining1.safemarch.com/Connector	
Root	Friday, March 09 2018 7:24:30 am	Sunday, March 01 2043 7:24:29 am	ptraining1.safemarch.com/Root	

Slide notes

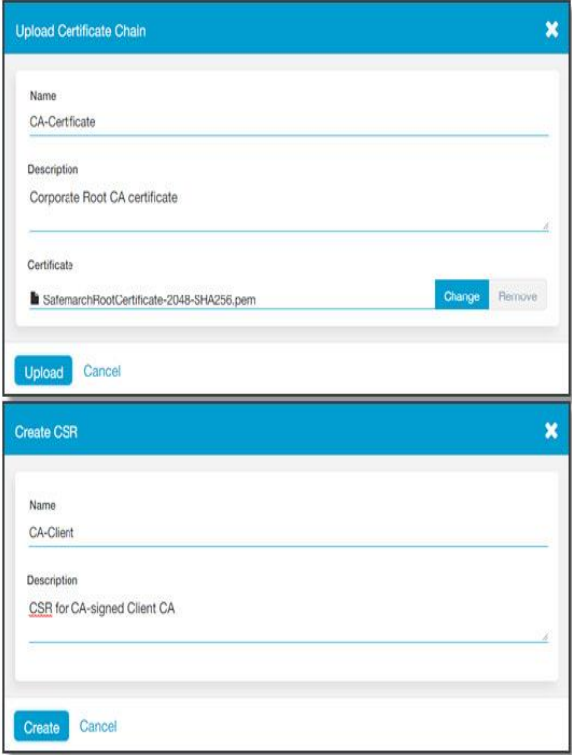
When you first subscribe to the ZPA service, Zscaler will provision a full set of self-signed Root, Client, and Connector certificates to your organization. They are listed on the Enrollment Certificates page in the ZPA Admin Portal, and are available for immediate use, there is no real need to generate your own set of self-signed certificates.

Slide 12 - Certificates Best Practices – BYOE



Certificates Best Practices – BYOE

- **Custom Certificates**
 - Upload your enterprise private Root CA certificate or certificate chain
 - Generate new Client and Connector certificates that use the new custom root certificate as parent
 - Manage the certificates through their lifetime
 - Note that this process is required to support double encryption



Slide notes

If you do not want to rely on the Zscaler self-signed certificates, or if you plan to deploy applications that use the double encryption feature, you will need to load custom certificates to the ZPA Admin Portal, signed by your own internal private root CA (the 'Bring Your Own Encryption' or BYOE option).

The process for this is:

1. Upload the root CA certificate, or certificate chain from your internal PKI at the ZPA Admin Portal.
2. Generate Certificate Signing Requests (CSRs) for Clients and Connectors and copy the CSR data (for an air-gapped private CA you will need to save this data to file). Note, this process also generates new sets of public/private keys, the private keys are securely stored on the ZPA CA; the public keys are included in the CSRs.
3. Take the CSR data (or files) to the appropriate internal private CA to be signed. This can be a Root CA, or an Intermediate CA that has signing authority.
4. Save the signed certificates to file and upload them to the ZPA Admin Portal for use as a new custom Client and Connector subordinate CAs.

Having uploaded your CA-signed Root certificate and generated new Client and Connector subsidiary CAs that are configured to use this new Root certificate as their parent, you then have a complete set of custom certificates for use across your ZPA infrastructure. Note: you will need to manage these certificates through their lifetime.

Slide 13 - Z-App Best Practices



Slide notes

The next topic we will cover are some Authentication best practices.

Slide 14 - Zscaler App Best Practices

IdP Advertised Over ZPA

- **Seamless SSO**
 - Advertising the IdP over ZPA can give end users a seamless SSO experience
- **Reauthentication Issues**
 - Set a per-application Timeout Policy for the IdP
 - Set the Authentication Timeout and Idle Timeout to **Never**

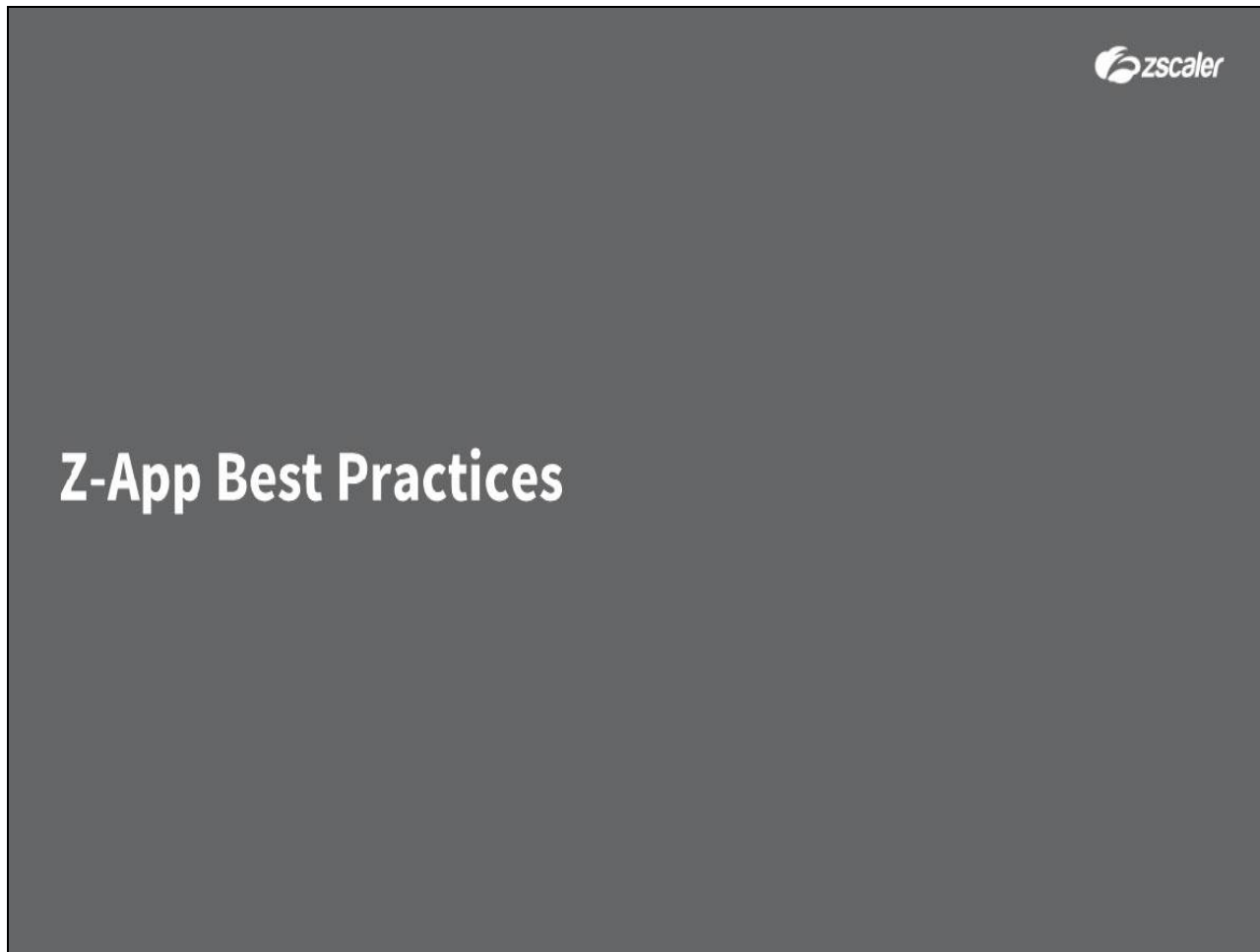
Slide notes

It is possible to protect the SAML IdP behind ZPA, which can improve end user experience by providing a seamless reauthentication. However, be aware that by default when the Reauthentication timer times out, end users will no longer be able to connect to the internal IdP as they are no longer authorized to access ZPA applications.

The solution to this 'chicken and egg' situation is to configure a per-application reauthentication timer just for the IdP, with both the 'Authentication Timeout' and 'Idle Timeout' set to 'Never'.

Caution: While this configuration can work under specific circumstances, it is not generally recommended.

Slide 15 - Z-App Best Practices



Slide notes

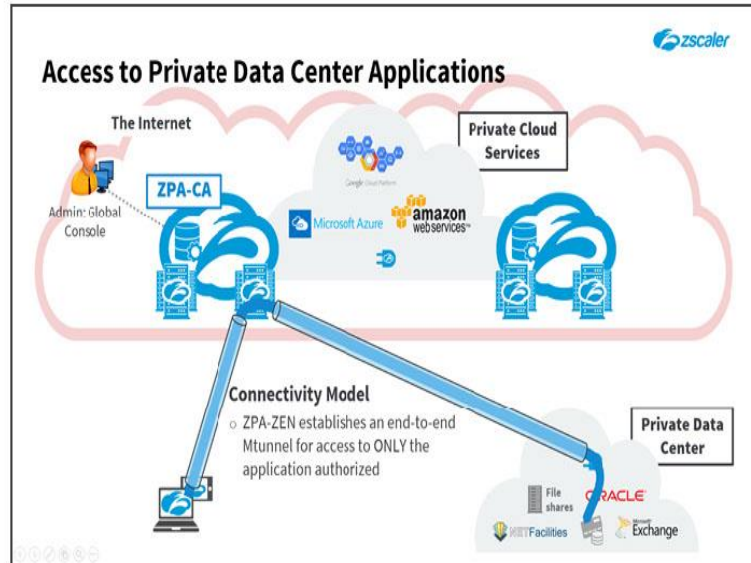
The next topic we will cover are some Zscaler App best practices.

Slide 16 - Zscaler App Enrollment

Zscaler App Enrollment

• Enrollment

- No proxies on the enrollment or data paths
- Make it as frictionless as possible for end users
 - Make install hidden
 - Provide Domain during App install
 - Provide App Profile during install



Slide notes

Similar to Connectors, it is not recommended for there to be any explicit proxies on the data path from a machine running the Zscaler App, plus any attempt to do SSL inspection on Zscaler App traffic will cause ZPA connectivity to fail.

The enrollment process for end users should be as frictionless as possible, and there are install options that can be used as the App is pushed to their device to achieve this. The recommended install process is:

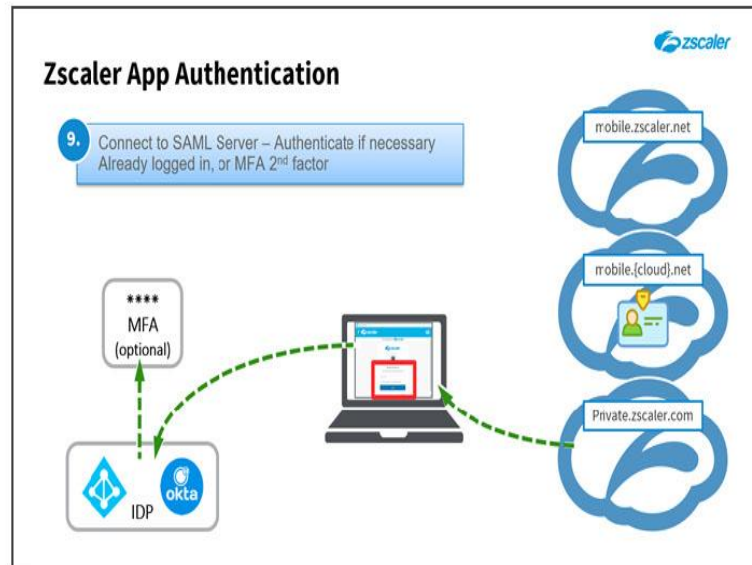
Push the App silently using your corporate AD, SCCM, or MDM; Use the silent installation option; Provide the domain to the App during installation (so users only need to provide their username to enroll); Provide the App Profile token during installation, to ensure the correct App Profile and related settings are automatically applied to the App.

Slide 17 - Zscaler App Best Practices

Zscaler App Authentication

- **ZPA and ZIA Coexistence**

- Use the same SAML IdP for authentication
- Add 2nd authentication factor if necessary

**Slide notes**

If the Zscaler App is used for both ZIA and ZPA, then it is recommended that ZIA enrollment also uses SAML, and the SAME IdP (to avoid the user being prompted twice for enrollment details). If necessary add a 2nd authentication factor for the ZPA enrollment, to provide more robust control of access to your private applications.

Slide 18 - Application Best Practices



Slide notes

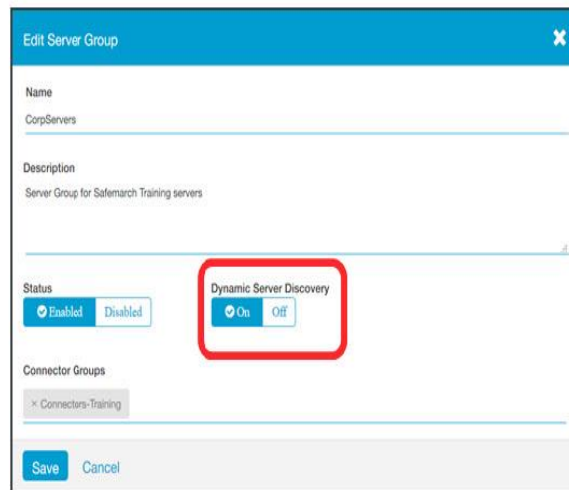
Next, we will look at some Application-related best practices.

Slide 19 - Application Best Practices

Server Group Configuration

- **Server Configuration**

- Use dynamic server discovery



The screenshot shows the 'Edit Server Group' dialog in the Zscaler interface. The 'Name' field is 'CorpServers' and the 'Description' is 'Server Group for Safemarch Training servers'. The 'Status' is 'Enabled'. The 'Dynamic Server Discovery' section, which is highlighted with a red rectangle, has the 'On' button selected. Below this, the 'Connector Groups' section shows 'Connectors-Training'. At the bottom, there are 'Save' and 'Cancel' buttons.

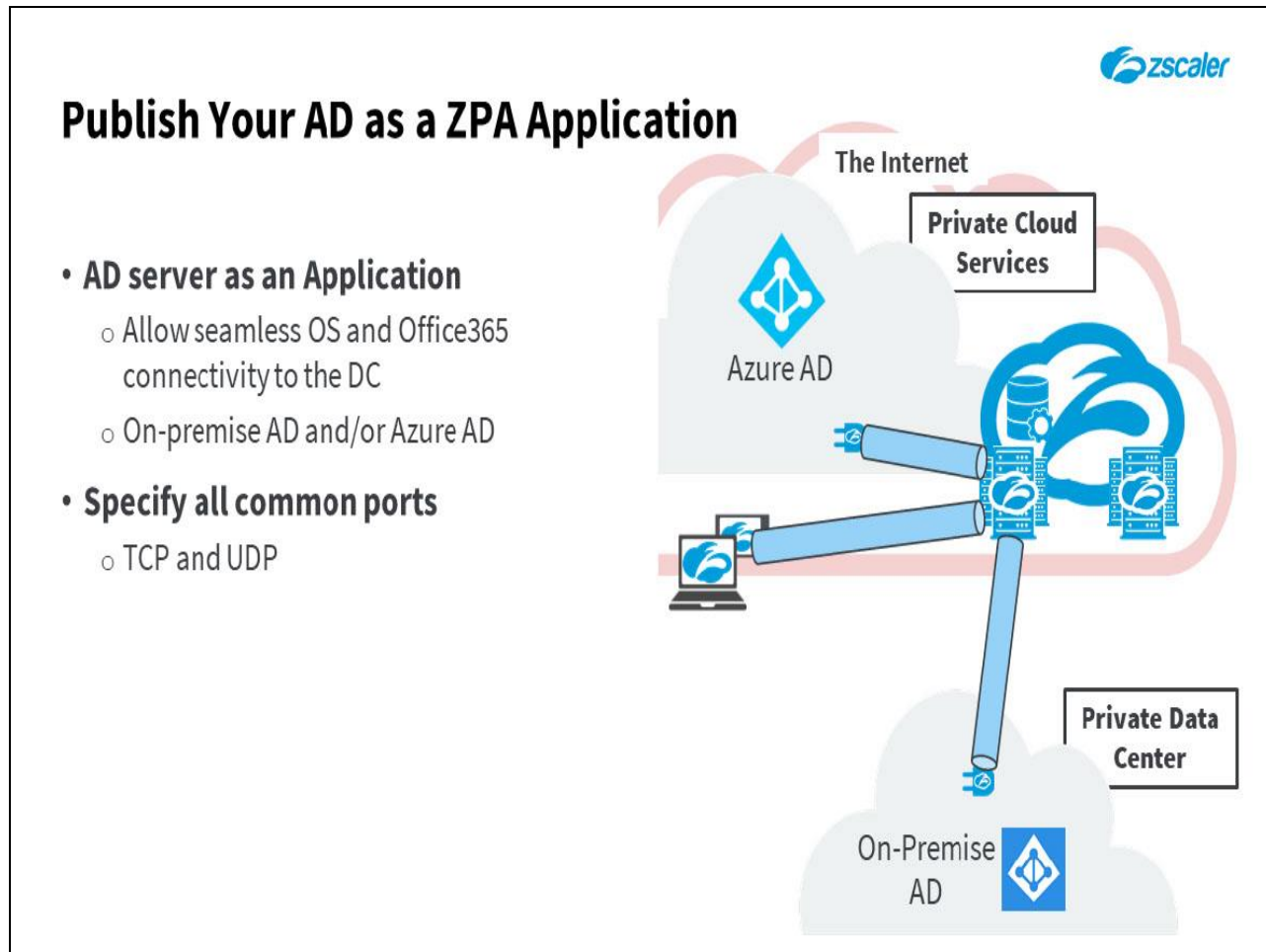
Slide notes

Wherever possible, use dynamic server discovery when defining creating ZPA Server Groups. This simplifies the configuration and allows ZPA to automatically detect the optimum server instance for each user request.

There are only two reasons to define servers statically:

1. To limit the potential pool of IP addresses that can serve a hostname request. For example, if you have DNS round-robin configured across 6 back-end servers for a given hostname, but you only want to allow a remote ZPA user to connect to a subset of them.
2. To override the user's request. For example, if the user wants to access the application 'foo.corpdomain.tld', and you want to route them to an IP address other than the IP address which is resolved by a DNS lookup of that hostname.


Slide 20 - Publish Your AD as a ZPA Application

**Slide notes**

Microsoft Office365 applications (e.g. Skype for Business) will often attempt to contact the AD Domain in the background, and if this is not possible the application will fail. We therefore recommend that you advertise your AD Domain Controller(s) over ZPA to allow all the background traffic to function correctly. This is particularly useful in a multi-domain environment, where a user might resolve their local AD for authentication, but also needs to contact the Global Catalog (GC) server in order to resolve cross-domain groups/access.

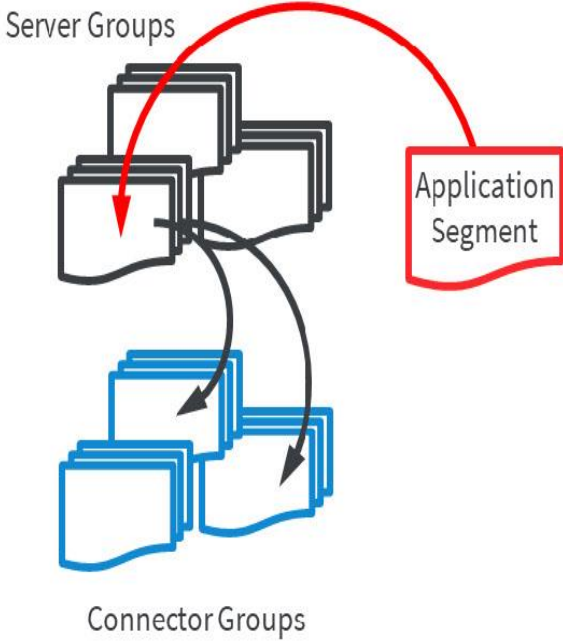
It is recommended that all of the ports listed as required by Microsoft be added to the application configuration for both TCP and UDP, as they have been known to switch between the transport layer protocols. Ports to add include: TCP/88, UDP/88; TCP/139, UDP/139; TCP/135, UDP 135; TCP/389, UDP/389; TCP/445, UDP/445; TCP/3268, UDP 3268; TCP/3269, UDP 3269.

Slide 21 - Entity and Group Mappings Best Practices



Entity and Group Mappings Best Practices

- **Server Group ⇔ Connector Group Mapping**
 - Server Group per Connector Group servicing a set of applications
 - Map to multiple Connector Groups for redundancy
 - Use actual location based Connector Groups to ensure users connect to a local application instance
 - Use large Connector Groups to allow best path discovery
 - Closest Connector Group to the user will always be used


Slide notes


The Server Group to Connector Group mapping controls which Connectors will be queried for an application, only the Connectors that are members of a Connector Group associated with a Server Group that is mapped to an application will query on the private network for that application.

If an Application Segment is associated with multiple eligible Connector Groups, the service will choose the closest Connector Group to the user, based on geographic location of the client (from IP geo-location), and geographic location (latitude and longitude) configured on the Connector Group. The system will evaluate proximity using the geo-IP of the source address of the Connector presented to the ZPA ZEN. Note: If an Application Segment has only one Connector Group associated to its Server Group, that Connector Group will automatically be the closest.

The Server Group to Connector Group mapping can also help to minimize health checks. If you create multiple dynamic-discovery Server Groups to control which Connectors will be queried for dynamic-discovery for a given application, this will eliminate health checks by Connectors which cannot reach the app.


As previously mentioned in the Connector's best practice section, use location-based Connector groups for location-sensitive applications, but use large non location-based groups to allow for the best application discovery path.

Slide 22 - Applications Unsuitable for ZPA



Applications Unsuitable for ZPA

- **Internal DNS**
 - If corporate DNS is available over ZPA it prevents the Zscaler App recognizing ZPA applications



DNS port 53

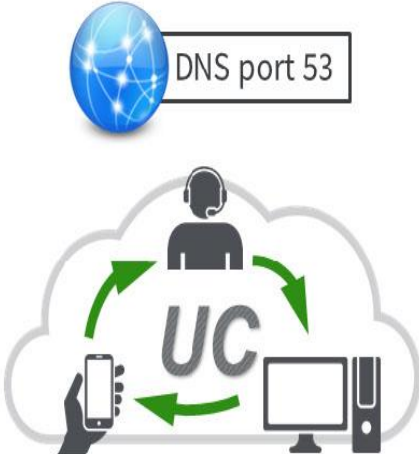
Slide notes

Some applications cannot be supported by ZPA due to architectural incompatibilities, one example is your internal DNS. If your corporate DNS server is accessible over ZPA, when a client requests an application by FQDN, this will be passed to your internal DNS and resolve to an IP address. The client device will then try to access the application on that IP instead of using ZPA.

Slide 23 - Applications Unsuitable for ZPA

Applications Unsuitable for ZPA

- **Internal DNS**
 - If corporate DNS is available over ZPA it prevents the Zscaler App recognizing ZPA applications
- **Unified Communications**
 - VoIP protocols (e.g. SIP) are architecturally unsuited to use ZPA
 - Peer-to-peer transport is not supported by ZPA
 - Real-time traffic over encrypted TCP connections would be sub-optimal

**Slide notes**

A whole application category that is unsuitable for transport over ZPA is the 'Unified Communications' class of application. Typically, these applications make extensive use of protocols designed for VoIP (e.g. SIP), where the server will try to facilitate a peer-to-peer connection for a voice or video call. As no Mtunnels exist between the peers, and ZPA does not use layer 3 routing mechanisms, this call setup will fail. In any case the transport of real-time streaming protocols would be encapsulated across SSL encrypted TCP connections giving sub-optimal voice and video performance.

Slide 24 - Applications Unsuitable for ZPA



Applications Unsuitable for ZPA

- **Internal DNS**

- If corporate DNS is available over ZPA it prevents the Zscaler App recognizing ZPA applications



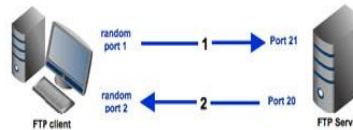
- **Unified Communications**

- VoIP protocols (e.g. SIP) are architecturally unsuited to use ZPA
- Peer-to-peer transport is not supported by ZPA
- Real-time traffic over encrypted TCP connections would be sub-optimal



- **Active-Mode FTP**

- Server call-back to the client is not supported on ZPA



Slide notes

Another example is active-mode FTP, where the FTP server calls the originating client back on a randomly chosen port in order to establish a data connection. As this return connection has no knowledge of the Mtunnel architecture, the server will be unable to route back to the client and the connection will fail.

Slide 25 - Monitoring Best Practices



Slide notes

The next topic we will cover are some ZPA monitoring best practices.

Slide 26 - Monitoring Best Practices

Health Check and Reporting

• Health Check Settings

- Under normal circumstances set 'Health Check' to 'Default' and 'Health Reporting' to 'On Access'
- For applications sensitive to unsolicited packets or passive FTP, set 'Health Check' to 'Off'

The screenshot shows the 'Edit Application' configuration page in the Zscaler interface. The application is named 'CIFS' and is currently 'Enabled'. The domain or IP address is '10.0.0.8'. The TCP port ranges are configured for 139 and 445. The UDP port ranges are empty. The 'Enable Double Encryption' is disabled. The 'Bypass When' is set to 'Never'. The 'Health Reporting' is set to 'On Access' (highlighted with a red box). The 'Health Check' is set to 'Default' (highlighted with a red box). The 'Server Groups' are 'CorpServers'. The 'Application Group' is 'CorpApps'. The 'Save' and 'Cancel' buttons are at the bottom.

Slide notes

Under normal circumstances we recommend that you set the 'Health Check' option within an Application Segment's configuration to 'Default', with the 'Health Reporting' option set to 'On Access'. This will provide effective monitoring of the application while it is being accessed and for 30 minutes following the last access request to it.

Some applications may be sensitive to unsolicited health check packets, or (as for passive-mode FTP) the health-check packet may consume the listening socket on the server. For these applications, set the 'Health Check' option to 'None'.

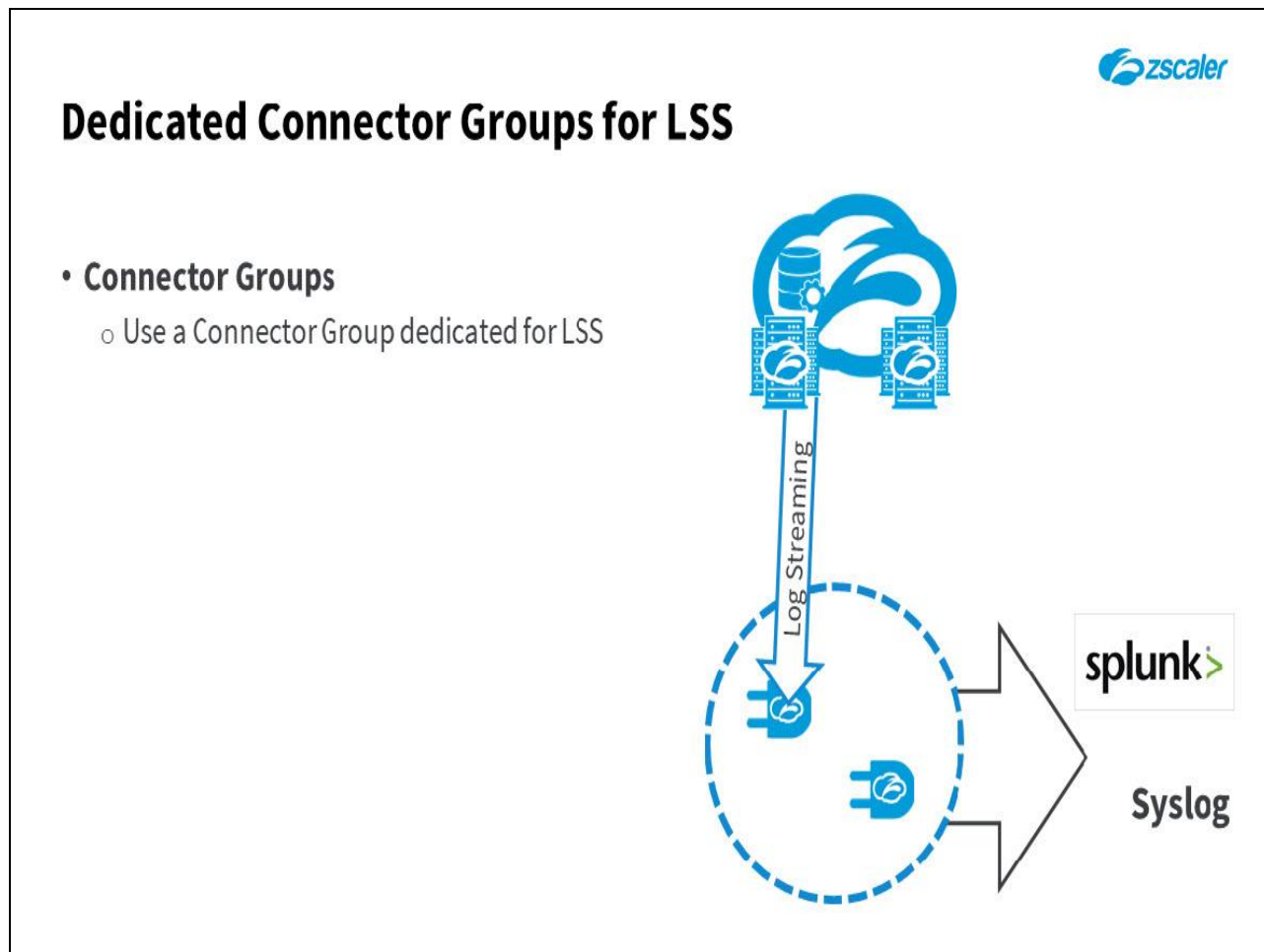
Slide 27 - LSS Best Practices



Slide notes

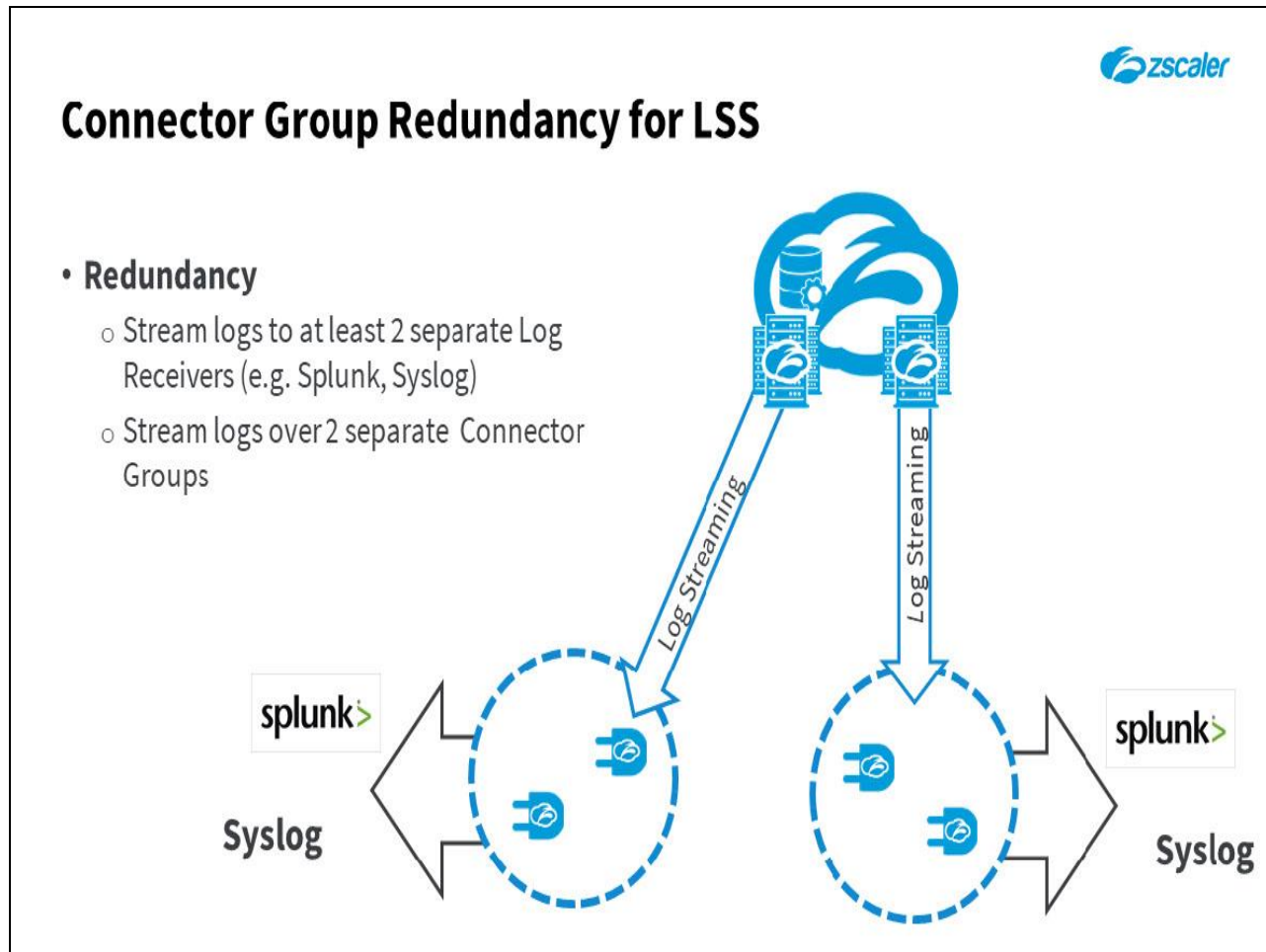
Finally, let's look at some ZPA Log Streaming Service best practices.

Slide 28 - LSS Best Practices

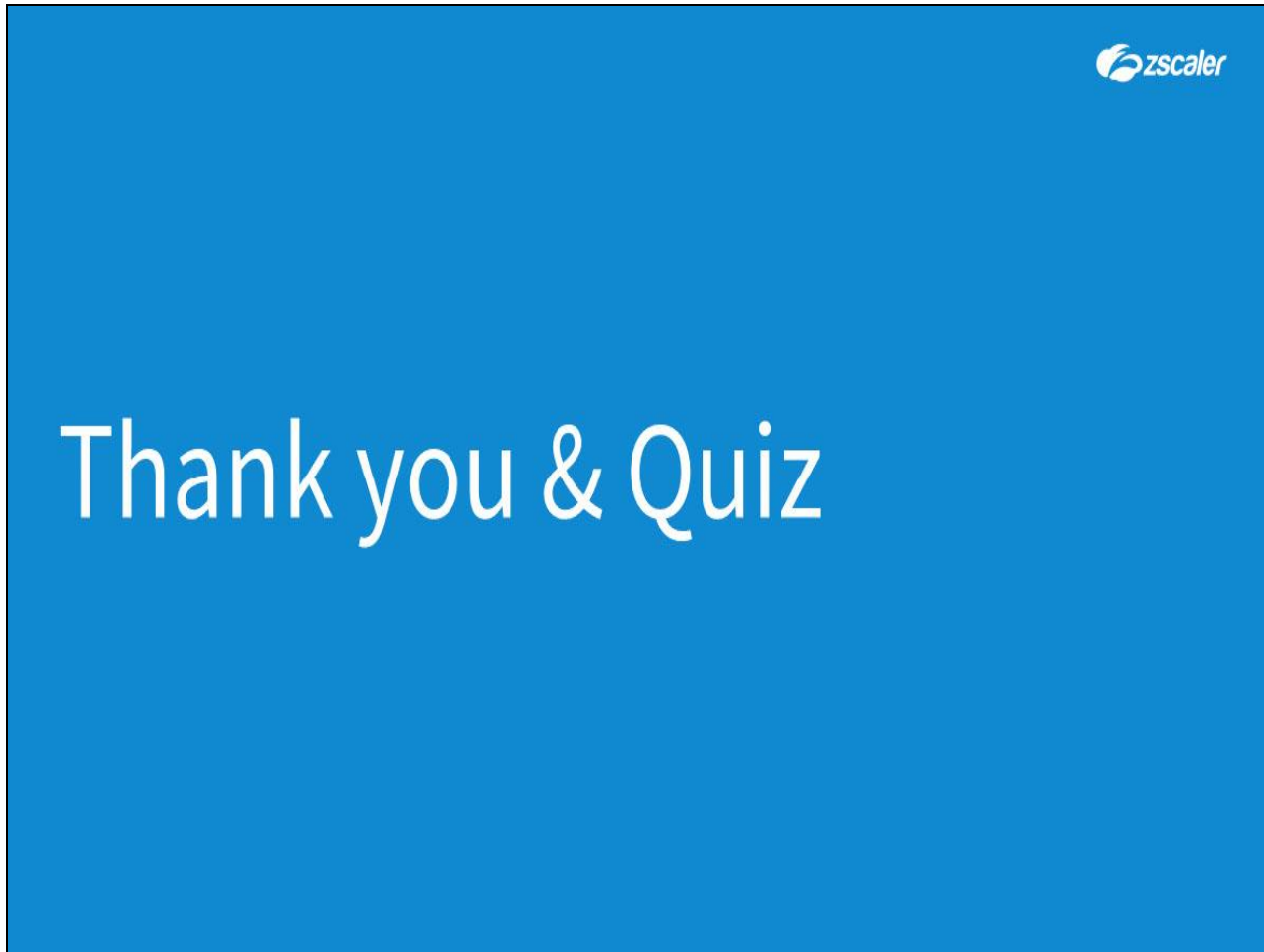
**Slide notes**

Remember, the ZPA Log Streaming Service (LSS) makes use of the Connector infrastructure for the delivery of logs to your local SIEM, and you need to select a Connector Group to send the logs to. This could be a regular Connector Group that also supports application access, however for production deployments we strongly recommend that you install Connectors adjacent to your SIEM and add them to a group dedicated to receiving the logs. Otherwise a burst of user traffic that consumes the available bandwidth through a Connector, could disrupt log streaming (which is best effort application) resulting in some loss of logs.

Slide 29 - LSS Best Practices

**Slide notes**

For the purposes of redundancy, we also recommend that you stream LSS logs to at least 2 log receivers, preferably at separate physical locations. Use separate Connector Groups for each log receiver destination.

Slide 30 - 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.