


Slide 1 – Zscaler App: Best Practices for ZIA



The Zscaler App

ZIA Best Practices

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module for a look at some Zscaler App **Best Practices** for the ZIA service.

Slide 2 - Navigating the eLearning Module

The screenshot displays the ZPA Basic Administration interface, titled "Video: ZPA Basic Administration". The interface features a sidebar with navigation options: Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler. The main content area is divided into several sections: "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). Below these are "APPLICATIONS ACCESSED" and "TOP APPLICATIONS BY BANDWIDTH" lists. The interface also includes a "TOP ERROR" section and "TOP POLICY BLOCKS" (Access Policy Blocks, Timeout Policy Blocks, Access Denied Blocks). Navigation controls are highlighted with blue callouts: "Previous Slide", "Next Slide", "Play/Pause", "Progress Bar", "Audio On/Off", "Closed Captioning", and "Exit". The Zscaler logo is visible in the top right corner.

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

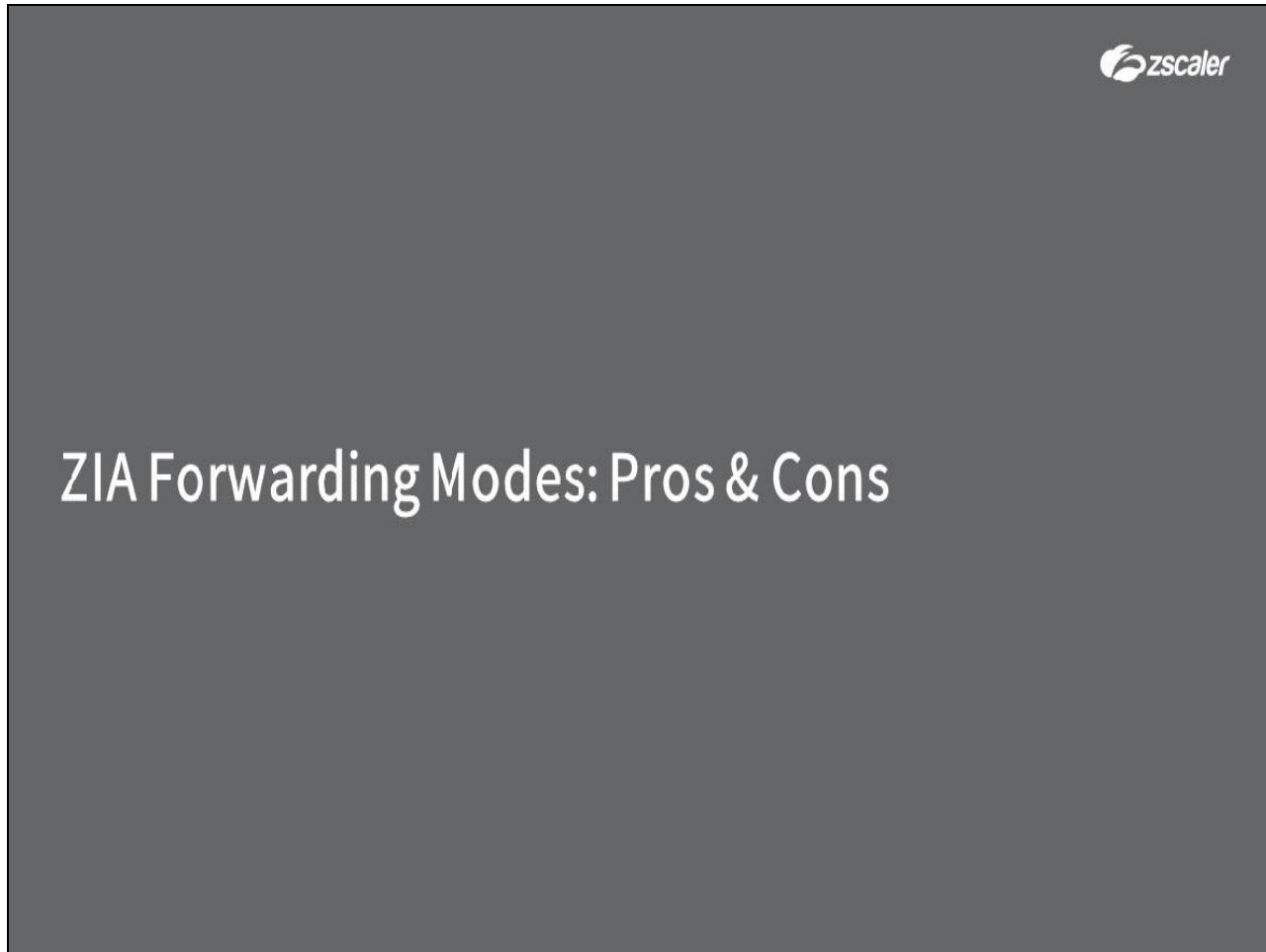
- ZIA Forwarding Modes: Pros & Cons
- What to Use When
- Zscaler App Best Practices:
 - Deployment
 - Authentication
 - General Use

Slide notes

In this module, we will cover the following topics:

- A look at some of the **Pros and Cons** of each of the Zscaler App forwarding modes:
- A look at **what forwarding mode to use when**;
- Then a look at some Zscaler App **Best Practices** in the areas of;
 - Deployment,
 - Authentication,
 - And General Usage guidelines.


Slide 4 - ZIA Forwarding Modes: Pros & Cons



Slide notes

The first topic that we will cover is a look at some of the **Pros and Cons** of each of the Z App forwarding modes.

Slide 5 - Zscaler App Modes: Advantages / Disadvantages



ZIA Forwarding Modes: Pros & Cons

Tunnel 1.0

- Secure ALL TCP port 80/443 traffic
- Interoperate with FW filter applications
- Interop with other proxy solutions
- Reasonable end user visibility


- Stream conversion
- Inbound FW rule
- No visibility into non-web traffic
- VPN co-existence
- ALG applications and 3rd party Proxy issues
- 60 minute App Portal policy interval
- Limited log visibility

Slide notes

One question you may have is; “why would I use one forwarding mode in preference to any other?”, we will try to throw some light onto this here, by listing some of the **Pros and Cons** of each of the various modes. First of all, for **Tunnel 1.0** mode:

- **Pros:** This mode can be used to secure ALL **TCP port 80/443** traffic, and this is regardless of the application that generated it (which means not just Web browser traffic). This mode is able to interoperate with both Firewall filter applications, and 3rd party proxy solutions. It also provides reasonable end user visibility to Zscaler, as the user must enroll into the App.
- **Cons:** The App must convert packets to a TCP stream before tunneling them to Zscaler, and as a result an inbound FW rule is required on the client host. This method only applies to TCP traffic on ports 80 and 443 which limits the ZIA security scanning and policy enforcement options. The App must be configured to fail open (using **Trusted Network** criteria) if a default route VPN is detected, and the host names or IPs of any VPN Gateways are required for split tunnel co-existence. This mode does not work well with apps that require an application level gateway (such as SIP) and bypasses must be defined for any 3rd party proxy solutions. Z App Portal policy changes are only propagated to the App when it checks in every 60 minutes, plus log visibility is limited.

Slide 6 - ZIA Forwarding Modes: Pros & Cons



ZIA Forwarding Modes: Pros & Cons

Tunnel 1.0

- Secure ALL TCP/UDP traffic (80/443 traffic)
- Interoperate with legacy firewall applications
- Interop with other proxy solutions
- Reasonable end user visibility

Tunnel (1.0) With Local Proxy

- Secure ALL HTTP/HTTPS traffic (also non-standard ports)
- Lightweight tunnels, no stream conversion
- Minimal VPN interop issues
- Reasonable end user visibility

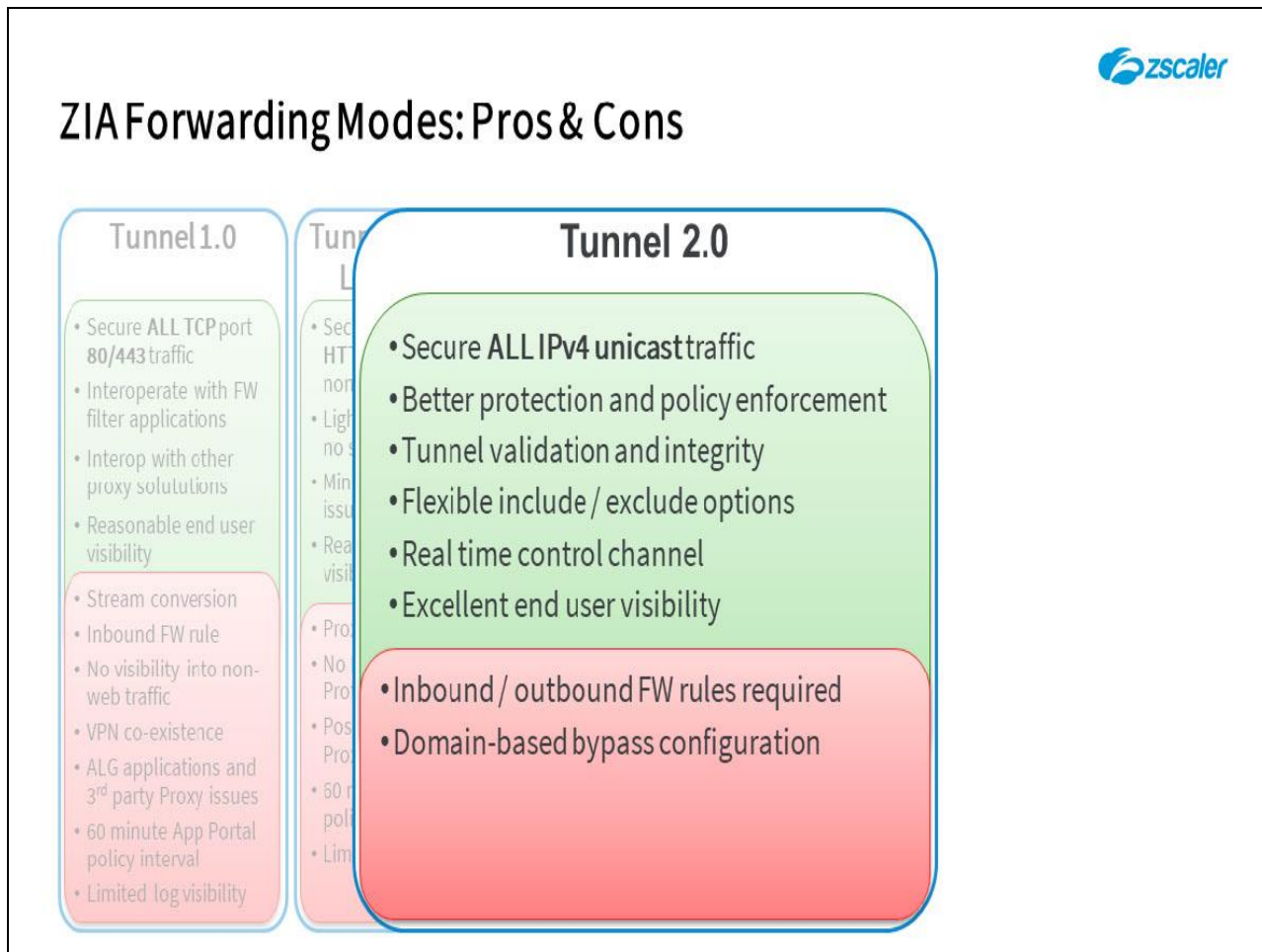
- Proxy traffic only
- No Browser Enhanced Protection
- Possible 3rd party Proxy issues
- 60 minute App Portal policy interval
- Limited log visibility

Slide notes

The **Tunnel with Local Proxy** mode (TWLP) **Pros** include:

- This mode can be used for all traffic that follows the proxy settings (which usually means **HTTP and HTTPS**), but regardless of destination port specified by the end user. This mode does not require any stream conversion, so provides a lighter weight tunneling solution. This mode has minimal interoperability issues with 3rd party systems. It also provides reasonable end user visibility to Zscaler.
- **Cons:** This mode can ONLY be used for traffic that follows the proxy definitions in the PAC files. Browser enhanced protection is not supported in this mode, plus you may see issues with 3rd party proxy solutions. As before, Z App Portal policy changes are only propagated to the App when it checks in every 60 minutes, and log visibility is limited.

Slide 7 - ZIA Forwarding Modes: Pros & Cons

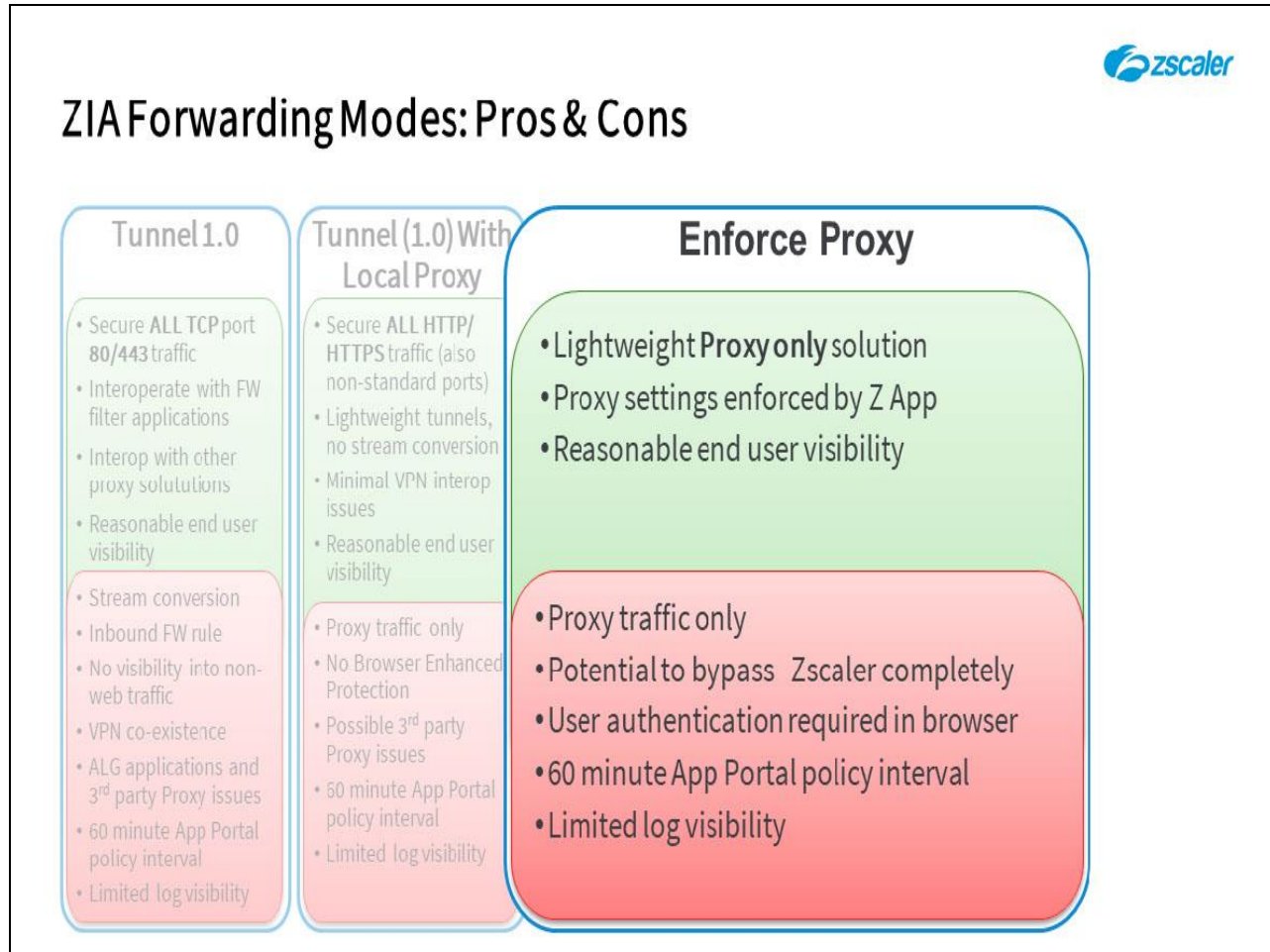


Slide notes

For Tunnel 2.0 the Pros are:

- It can be used to secure **ALL IPv4 unicast** traffic, regardless of protocol (TCP, UDP, or ICMP) and port. This method allows much better ZIA protection and policy enforcement, allowing us to also apply **Advanced Cloud Firewall** and **DLP** policies. Tunnels are established using secure protocols meaning that, while they are not encrypted, they do still provide for validation and integrity to prevent MitM attacks. There are extremely flexible **Include / Exclude** options, to control exactly what traffic gets sent to the ZIA service. A secure control channel is provided that allows the update of Z App Portal policies in real-time, plus end user visibility is excellent, with full logging of all activity.
- On the **Con** side: Inbound / outbound FW rules are required on the host platform and the addition of **Domain-based** bypass configurations is somewhat complicated.

Slide 8 - ZIA Forwarding Modes: Pros & Cons

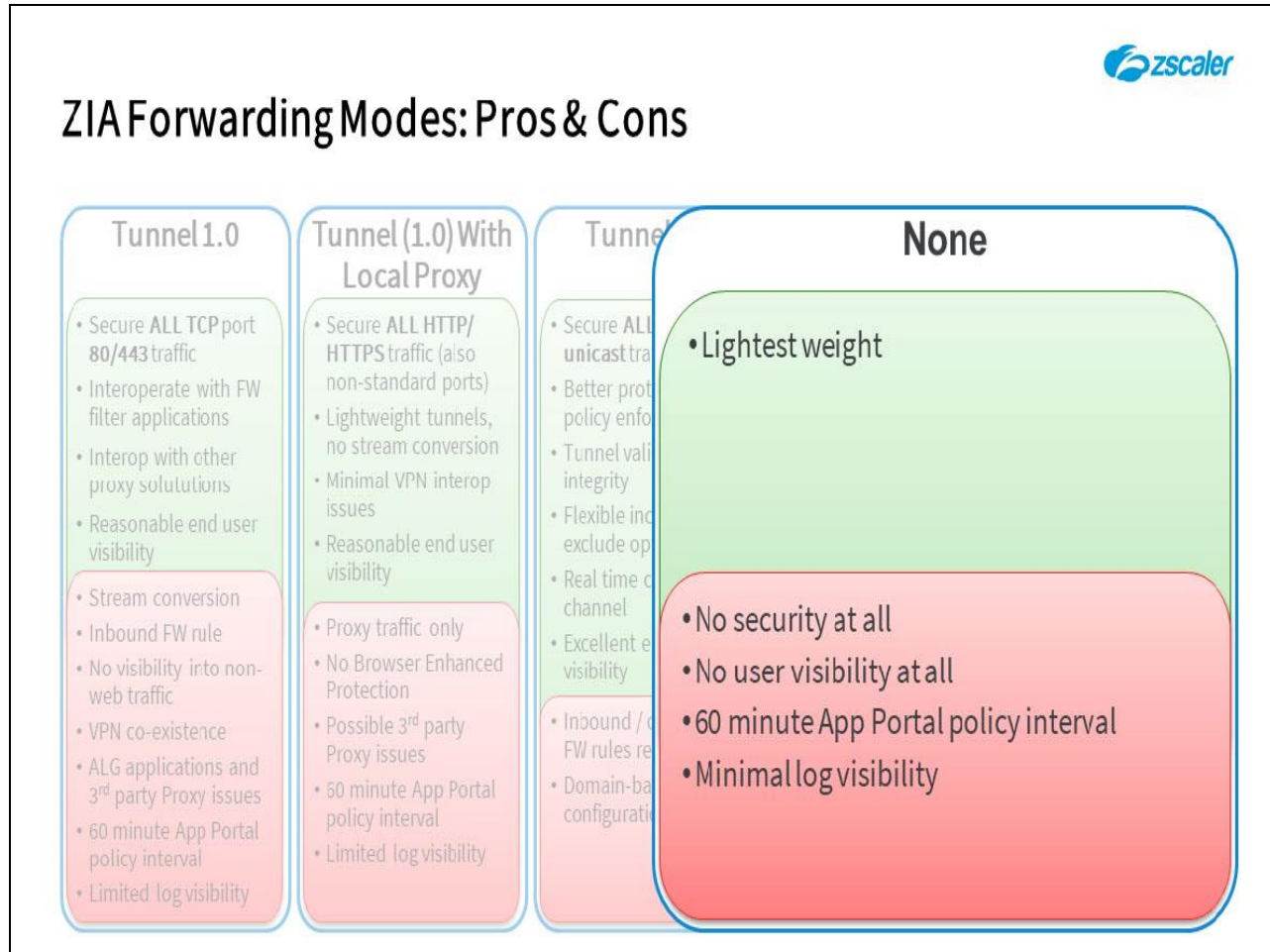


Slide notes

Pros for the Enforce Proxy mode are:

- This mode provides an extremely light weight solution, as no tunnels are ever established, the App is simply used to enforce what proxy configuration is applied to (or removed from) the system and makes sure that the PAC file is applied even if the user tries to remove it. It provides reasonable end user visibility to Zscaler, as users must authenticate to the ZIA service in the browser on their first connection.
- Cons:** Once again, this mode can ONLY be used for traffic that follows the proxy definitions in the PAC file. There is the possibility that Zscaler can be bypassed completely if the original system proxy definitions are retained. Users must authenticate into the App on first enrollment and again in the Web browser on first connection to the ZIA service. Once again, Z App Portal policy changes are only propagated to the App when it checks in every 60 minutes and log visibility is limited.

Slide 9 - ZIA Forwarding Modes: Pros & Cons




Slide notes

Finally, for the **None** mode the **Pros** are:

- This is the lightest weight mode of all, as the App is basically in fail open mode and does no traffic forwarding at all.
- The **Cons** of this mode are: The App cannot ensure traffic is forwarded to Zscaler to provide any level of protection, nor does Zscaler have any visibility into the traffic generated by the user. As before, Z App Portal policy changes are only propagated to the App when it checks in every 60 minutes and log visibility is minimal.

Slide 10 - ZIA Forwarding Modes: Pros & Cons



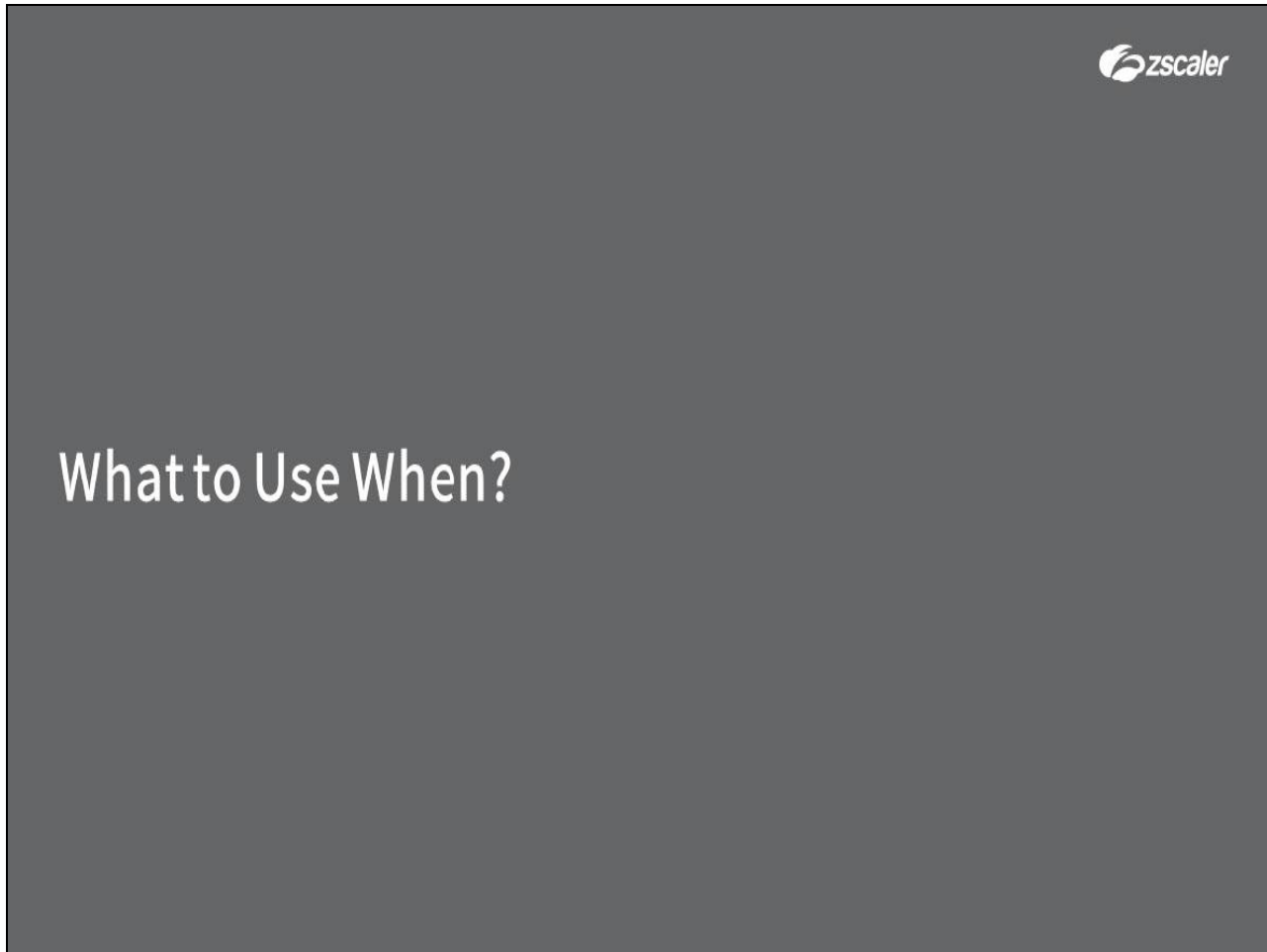
ZIA Forwarding Modes: Pros & Cons

Tunnel 1.0	Tunnel (1.0) With Local Proxy	Tunnel 2.0	Enforce PAC	None
<ul style="list-style-type: none"> Secure ALL TCP port 80/443 traffic Interoperate with FW filter applications Interop with other proxy solutions Reasonable end user visibility 	<ul style="list-style-type: none"> Secure ALL HTTP/HTTPS traffic (also non-standard ports) Lightweight tunnels, no stream conversion Minimal VPN interop issues Reasonable end user visibility 	<ul style="list-style-type: none"> Secure ALL IPv4 unicast traffic Better protection and policy enforcement Tunnel validation and integrity Flexible include / exclude options Real time control channel Excellent end user visibility 	<ul style="list-style-type: none"> Lightweight Proxy only solution Proxy settings enforced by Z App Reasonable end user visibility 	<ul style="list-style-type: none"> Lightest weight
<ul style="list-style-type: none"> Stream conversion Inbound FW rule No visibility into non-web traffic VPN co-existence ALG applications and 3rd party Proxy issues 60 minute App Portal policy interval Limited log visibility 	<ul style="list-style-type: none"> Proxy traffic only No Browser Enhanced Protection Possible 3rd party Proxy issues 60 minute App Portal policy interval Limited log visibility 	<ul style="list-style-type: none"> Inbound / outbound FW rules required Domain-based bypass configuration 	<ul style="list-style-type: none"> Proxy traffic only Potential to bypass Zscaler completely User authentication required in browser 60 minute App Portal policy interval Limited log visibility 	<ul style="list-style-type: none"> No security at all No user visibility at all 60 minute App Portal policy interval Minimal log visibility

Slide notes

Just for completeness, here are all the **Pros** and **Cons** side by side.


Slide 11 - What to Use When?



Slide notes

The next topic that we will cover is a look at some suggestions for **what forwarding mode to use when**.

Slide 12 - What to Use When?



What to Use When?


	Tunnel 1.0	TWLP	Tunnel 2.0	Enforce Proxy	None
Forward all standard Web traffic	✓	✓	✓	✓	
Forward all Web traffic on non-standard ports		✓	✓	✓	
Forward all non-Web traffic			✓		
Transparent forwarding (include non-proxy aware apps)	✓		✓		
Unified authentication (include non-SAML aware apps)	✓	✓	✓		

Slide notes

Hopefully, this matrix will assist you in choosing the optimum forwarding mode based on your situation. Please note though, that what we discuss here are general scenario guidelines, your detailed situation may dictate a selection other than those presented here:

- The forwarding modes that support all Web traffic on the standard ports (80 and 443) are **Tunnel** (both 1.0 and 2.0), **TWLP** and **Enforce Proxy**.
- If you wish to forward Web traffic on non-standard ports, then you would need **TWLP**, **Tunnel 2.0** or **Enforce Proxy**.
- If you need to forward data other than simple Web traffic, you will need **Tunnel 2.0**.
- If you need to transparently forward traffic, including from non-proxy aware applications, then you will need **Tunnel** mode (1.0 or 2.0).
- To support application traffic from applications that are not SAML aware, you will need **Tunnel** mode again (1.0 or 2.0), or **TWLP** mode.

Slide 13 - What to Use When?



What to Use When?

	Tunnel 1.0	TWLP	Tunnel 2.0	Enforce Proxy	None
Manage client local IP policies			✓		
Manage IP-layer bypasses/exclusions/inclusions			✓		
Support for no default route environment	✓	✓	✓	✓	
Co-exist with default route VPN on MacOS		✓			
No ZIA scanning required (e.g. on trusted network)					✓

Slide notes

- If you need to be able to manage client local IP policies,
- Or if you need to manage detailed IP-layer destination inclusions or exclusions, then you will need **Tunnel 2.0**.
- For no-default route environments, you can use any of the forwarding modes that use tunnels or the **Enforce Proxy** mode.
- For optimum co-existence with default route VPN clients, particularly on the Mac platform, you will need **TWLP**.
- Finally, for those situations where you do not need to forward traffic to Zscaler (e.g. because the device is on a **Trusted Network**), you have the **None** option.

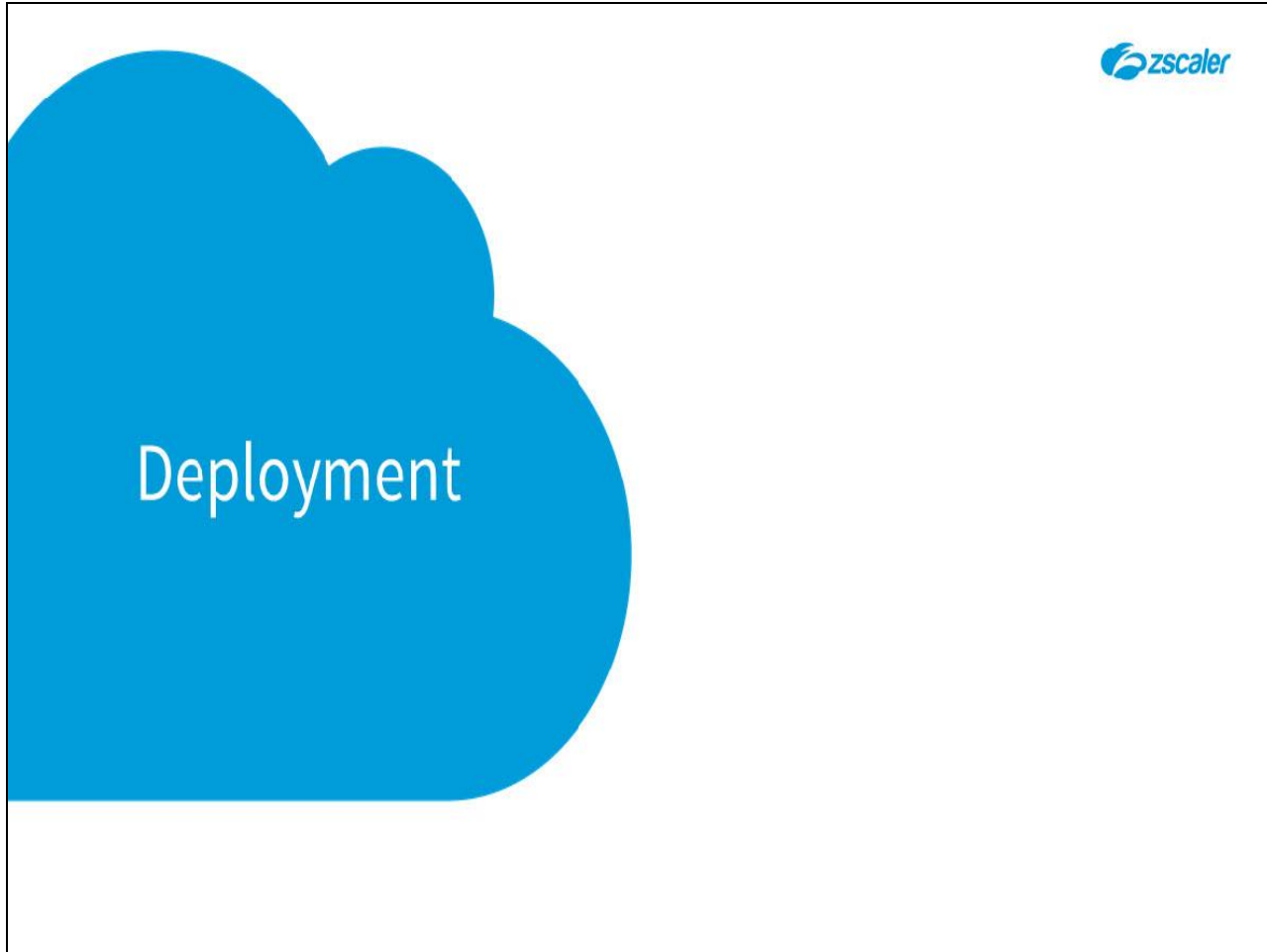
Slide 14 - Zscaler App Best Practices:



Slide notes

The final topic that we will cover is a look at some Zscaler App **Best Practices** when used to connect to the ZIA service.

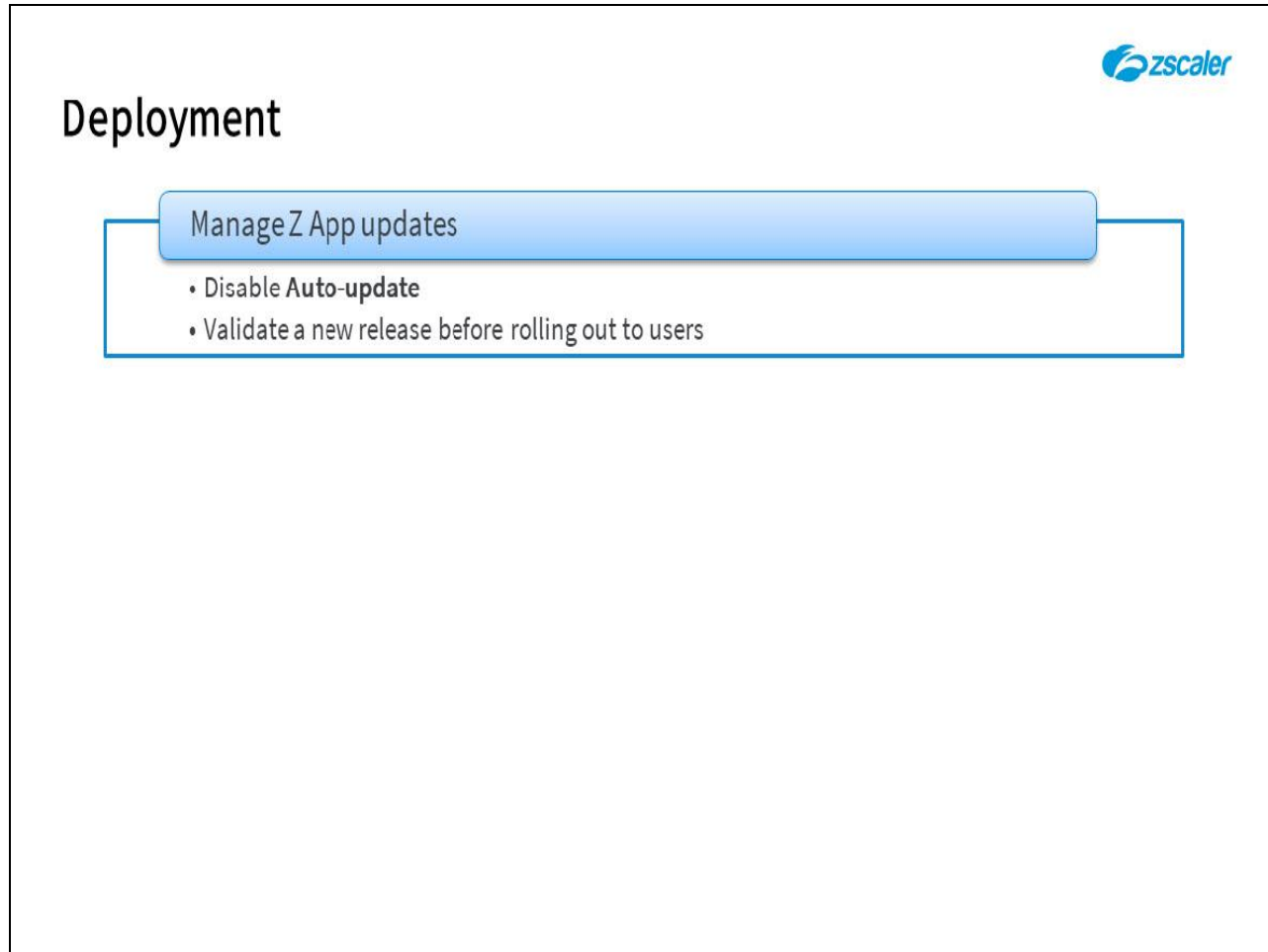
Slide 15 - Deployment



Slide notes


To start with, we'll look at best practices for Z App deployment.

Slide 16 - Install



The slide is titled "Deployment" and features the Zscaler logo in the top right corner. A blue box titled "Manage Z App updates" contains two bullet points: "• Disable Auto-update" and "• Validate a new release before rolling out to users".

Deployment



Manage Z App updates


- Disable Auto-update
- Validate a new release before rolling out to users

Slide notes

First and foremost, you need to be sure to control exactly what version of the App gets installed to your end user's devices. Ideally, you would always like the latest version available, to be sure to have all the latest bug fixes and any new features. However, it is probably not a good idea to install the new version blindly. We would recommend that you turn off the automatic Z App updates and only ever deploy versions that are known to be good *in your environment*.

This may well mean that you need to test each new version of the App prior to pushing it to your installed end user base.

Slide 17 - Install




Deployment

- Manage Z App updates
 - Disable **Auto-update**
 - Validate a new release before rolling out to users
- Manage Z App Permissions, Processes and Firewall Rules
 - Use GPO if necessary to configure **Firewall Rules**

Slide notes

Be sure to review all the Z App requirements for the devices that you will be deploying it to, in terms of the **Permissions**, **Processes** and **Firewall Rules** required. If any of these are already under the control of some management system (e.g. AD GPO rules), be sure to update those rules to account for the Z App requirements.

Slide 18 - Install




Deployment

- Manage Z App updates
 - Disable **Auto-update**
 - Validate a new release before rolling out to users
- Manage Z App Permissions, Processes and Firewall Rules
 - Use GPO if necessary to configure **Firewall Rules**
- Use the `--cloudName`, `--userDomain` and `--policyToken` switches on install
 - Automatically assign ZIA **Cloud**, user **Domain** and **App Profile** to be applied
 - This ties the App to the corporate domain

Slide notes

Wherever possible, use the available command line switches when installing the App, such as `--cloudName`, `--userDomain` and `--policyToken`. This improves the end user enrollment experience as they will be immediately redirected to the appropriate SAML IdP. This also ties the Z App installation to your domain (so end users are unable to enter some other domain during enrollment) and automatically applies the appropriate **App Profile** (with all the correct App settings and the correct **Forwarding Profile** for the users).

Slide 19 - Install



Deployment


- Manage Z App updates
 - Disable **Auto-update**
 - Validate a new release before rolling out to users
- Manage Z App Permissions, Processes and Firewall Rules
 - Use GPO if necessary to configure **Firewall Rules**
- Use the `--cloudName`, `--userDomain` and `--policyToken` switches on install
 - Automatically assign ZIA **Cloud**, user **Domain** and App **Profile** to be applied
 - This ties the App to the corporate domain
- Where possible ensure silent install and enrollment into the App
 - For the end users, ...it should just work

Slide notes

Taking this a stage further, where possible configure a silent end user enrollment into the App; from the end user perspective “it should just work”. A silent enrollment for ZIA can be achieved using the **Zscaler App Portal IdP**, or you can use the options available with your chosen 3rd party SAML IdP.

Under some circumstances, a silent enrollment into the App for ZIA service can still be achieved with a non-SAML authentication method.

Slide 20 - Install



Deployment


Ensure Z App is not competing for control of the System Proxy Settings

- No WPAD, no GPO, no local proxy server

Slide notes

Ensure that Zscaler App is not competing with some other proxy configuration method (WPAD, GPO pushed PAC files, or local proxy server). Ideally, Z App should be in control of what proxy settings are applied, in the form of PAC files.

Slide 21 - Install



Deployment


- Ensure Z App is not competing for control of the System Proxy Settings
 - No WPAD, no GPO, no local proxy server
- Start small and scale up
 - Pilot, then wider testing, then general deployment (<1,000 in a batch)

Slide notes

Start your deployment small and scale up. Do a pilot deployment first, targeting a small group of ideally tech-savvy users. Once you have confirmed the configurations and methods you require, you can then start to do a wider deployment.

We would recommend that you enroll **no more than 1,000** Z App end users at a time.

Slide 22 - Install




Deployment

- Ensure Z App is not competing for control of the System Proxy Settings
 - No WPAD, no GPO, no local proxy server
- Start small and scale up
 - Pilot, then wider testing, then general deployment (<1,000 in a batch)
- Use the .EXE installer during local testing
 - To avoid SCCM/GPO version mismatches

Slide notes

When testing on a local machine, use the **.EXE** installer for preference. This will avoid any potential clashes with a SCCM or GPO pushed installer.

Slide 23 - Install



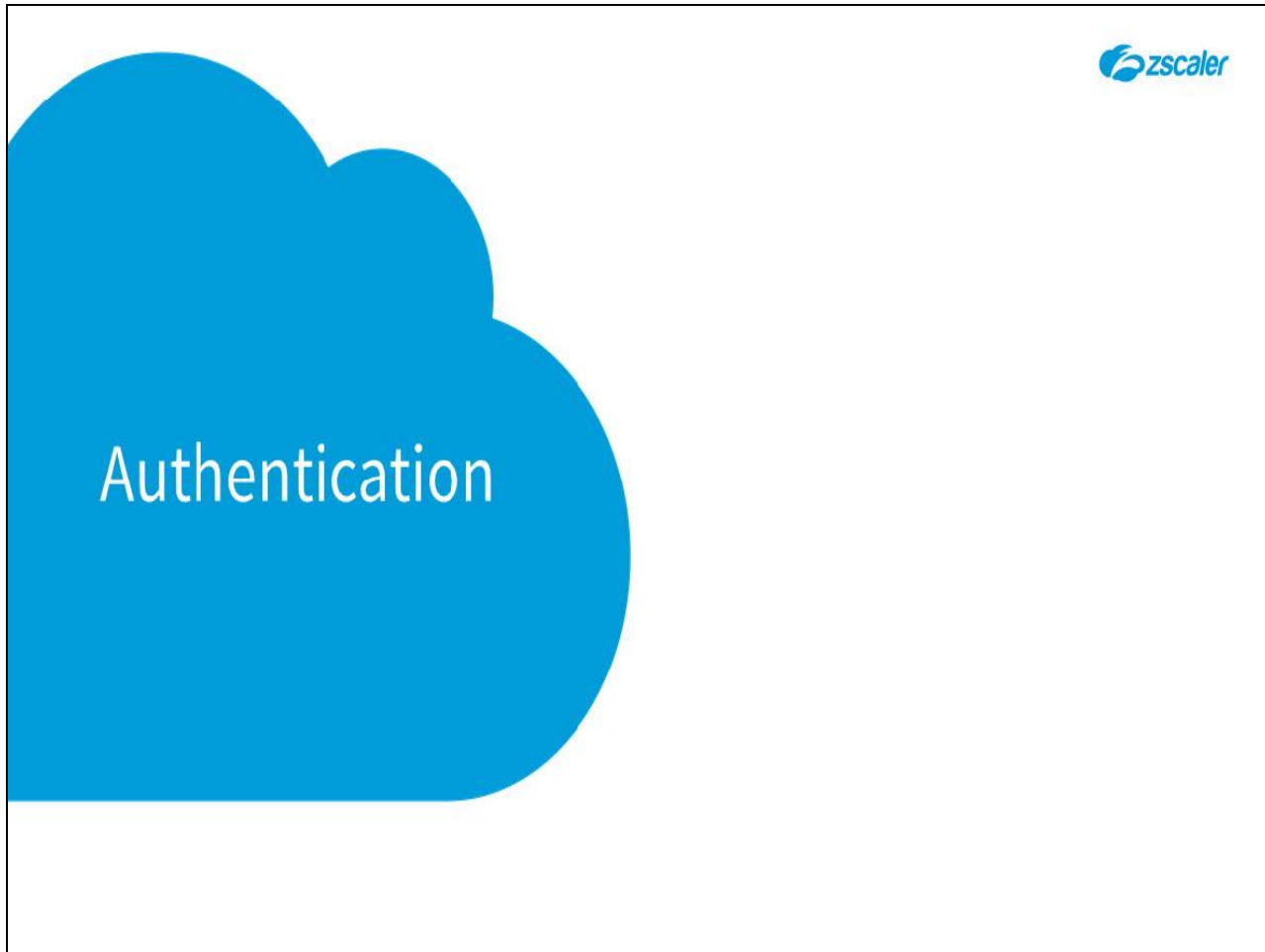
Deployment

- Ensure Z App is not competing for control of the System Proxy Settings
 - No WPAD, no GPO, no local proxy server
- Start small and scale up
 - Pilot, then wider testing, then general deployment (<1,000 in a batch)
- Use the .EXE installer during local testing
 - To avoid SCCM/GPO version mismatches
- Set Device Threshold to 8
 - Reduce the number of devices a single end user can enroll the App onto
 - Use the Device Cleanup option to enforce the limit

Slide notes

Set the **Device Threshold** to 8 and ensure it is enforced through the **Device Cleanup** configuration. This will ensure that users cannot install and enroll Z App on more than the specified number of devices.

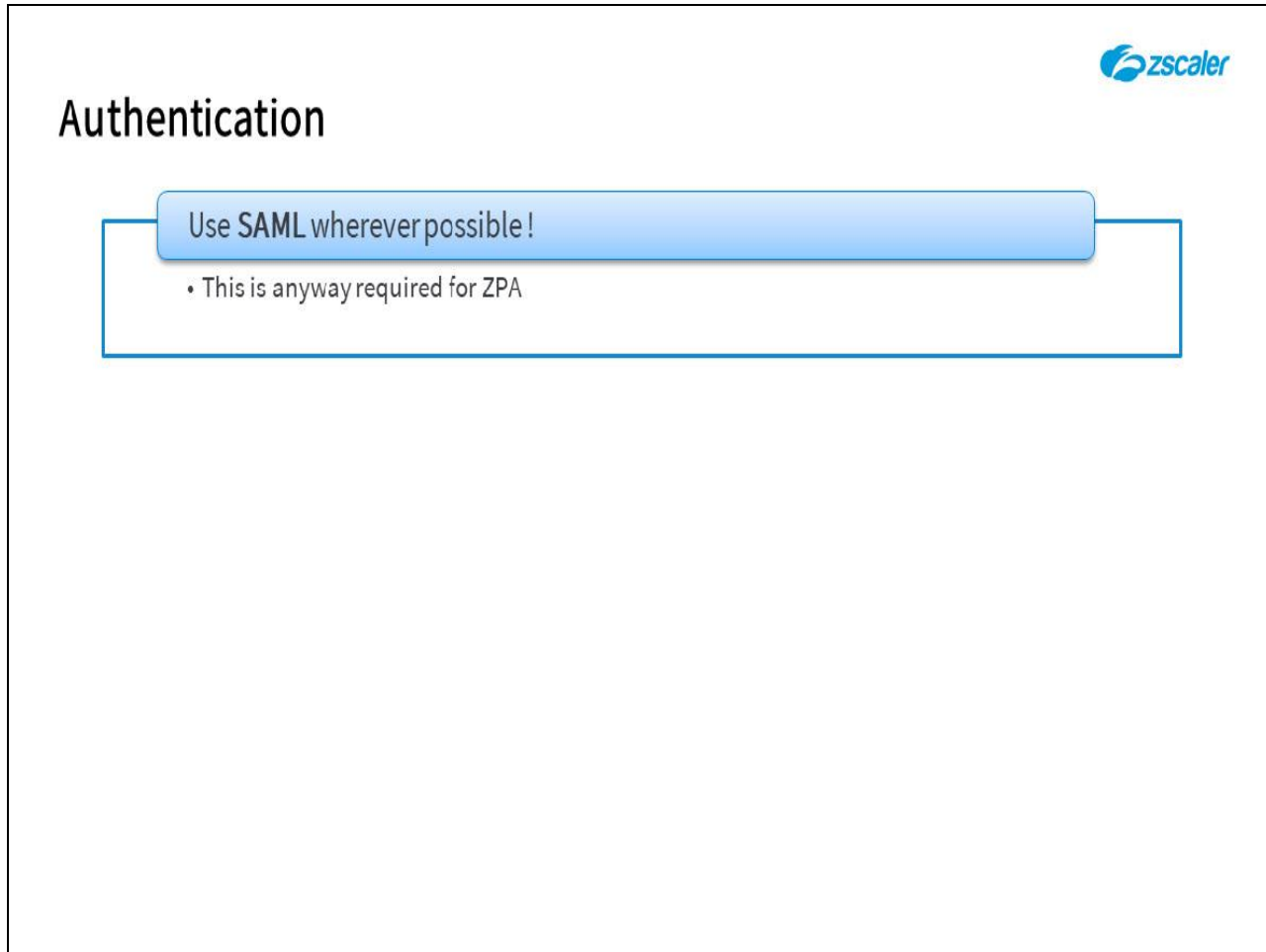
Slide 24 - Authentication



Slide notes


Now let's talk about some Authentication best practices.

Slide 25 - Authentication



The slide features the Zscaler logo in the top right corner. The main title 'Authentication' is positioned on the left. A blue callout box with a white border contains the text 'Use SAML wherever possible !' and a bullet point below it stating '• This is anyway required for ZPA'.

Authentication



Use SAML wherever possible !


- This is anyway required for ZPA

Slide notes

Wherever possible, use SAML authentication! It is anyway usually the simplest form of authentication to configure and, depending on your chosen IdP, can support advanced authentication options (silent authentication, certificate-based authentication, multi-factor authentication (MFA)).

It is also the authentication method required if you plan to use Z App for ZPA as well.

Slide 26 - Authentication




Authentication

- Use **SAML** wherever possible !
 - This is anyway required for ZPA
- If required - Configure MFA on the **SAML IdP**
 - Be sure to test it

Slide notes

Configure and test MFA on your IdP, preferably before deploying Z App. Make sure this works prior to authenticating Z App users.

Slide 27 - Authentication



Authentication

- Use **SAML** wherever possible !
 - This is anyway required for ZPA
- If required - Configure **MFA** on the **SAML IdP**
 - Be sure to test it
- Provisioning
 - Azure, Okta, PingOne, Centrify – use **SCIM** for dynamic user attribute updates (limited scope)
 - ADFS or other SAML IdP – use **Auto-Provisioning**

Slide notes

For end user provisioning to the ZIA database, if you are using Azure AD, Okta, PingOne or Centrify, we recommend that you configure **SCIM** – to ensure that end user details will be updated dynamically on adds, moves or changes. For ADFS, or any other SAML IdP, we recommend that you use SAML **Auto-Provisioning**, to at least add users automatically when they first enroll through Z App.


Slide 28 - General Use



Slide notes

Finally some general Z App best practices.

Slide 29 - General



General


Test destination responses thoroughly before general roll-out

- Make sure it works for all required destinations

Slide notes

Test access to all required destinations through the ZIA service prior to a general roll-out. Make sure you can reach all the destinations that you know your end users will need!

Slide 30 - General




General

- Test destination responses thoroughly before general roll-out
 - Make sure it works for all required destinations
- Use **Packet Filter Based** driver on Windows
 - For better performance, enforcement, interoperability, network functionality

Slide notes

Use the **Packet Filter Based** driver for the Windows platform, for better performance, enforcement, interoperability and network functionality.

Slide 31 - General




General

- Test destination responses thoroughly before general roll-out
 - Make sure it works for all required destinations
- Use **Packet Filter Based** driver on Windows
 - For better performance, enforcement, interoperability, network functionality
- Use **Tunnel 2.0** where you can
 - To provide better security for more applications

Slide notes

Where possible use the **Tunnel 2.0** forwarding method, as it provides better security, policy enforcement and end user visibility.

Slide 32 - General



General


- Test destination responses thoroughly before general roll-out
 - Make sure it works for all required destinations
- Use **Packet Filter Based** driver on Windows
 - For better performance, enforcement, interoperability, network functionality
- Use **Tunnel 2.0** where you can
 - To provide better security for more applications
- Use Z App to install Zscaler (or custom) **Root CA Cert** – also to Firefox
 - For trust to Zscaler when doing SSL inspection

Slide notes

Use the Z App install to also install the required **Root CA Certificate** for SSL inspection, whether that is the Zscaler root certificate or a custom root certificate.

Be sure to enable the Firefox support option as well, so this certificate will be installed to the Firefox certificate store too.

Slide 33 - General



General

SSL Inspection: Enable for PCs, Disable for Mobiles


- Or enable selectively for Mobiles

Slide notes

Enable SSL inspection for Z App on your PC platforms, but leave it disabled on Mobiles (for now). This is due to the certificate pinning commonly used by the developers of mobile applications.

Alternatively, you may enable SSL Inspection for Mobiles and manage exemptions in the **SSL Inspection Policy** configuration.

Slide 34 - General



General

SSL Inspection: Enable for PCs, Disable for Mobiles

- Or enable selectively for Mobiles


Use the Host Name > IP Address matching for Trusted Networks

- Other methods can be suspect

Slide notes

When configuring **Trusted Networks** in the Zscaler App Portal, use the **Host Name to IP Address** matching criteria for preference, as this can be a more reliable method of identifying the network.

Slide 35 - General




General

- SSL Inspection: Enable for PCs, Disable for Mobiles
 - Or enable selectively for Mobiles
- Use the Host Name > IP Address matching for Trusted Networks
 - Other methods can be suspect
- Reduce the Captive Portal Timer
 - To minimize the time spent unprotected

Slide notes

Reduce the **Captive Portal** timeout value from its default value of 10 minutes. This will help to minimize the periods where Z App is not in control of traffic forwarding on the devices.

Slide 36 - General



General

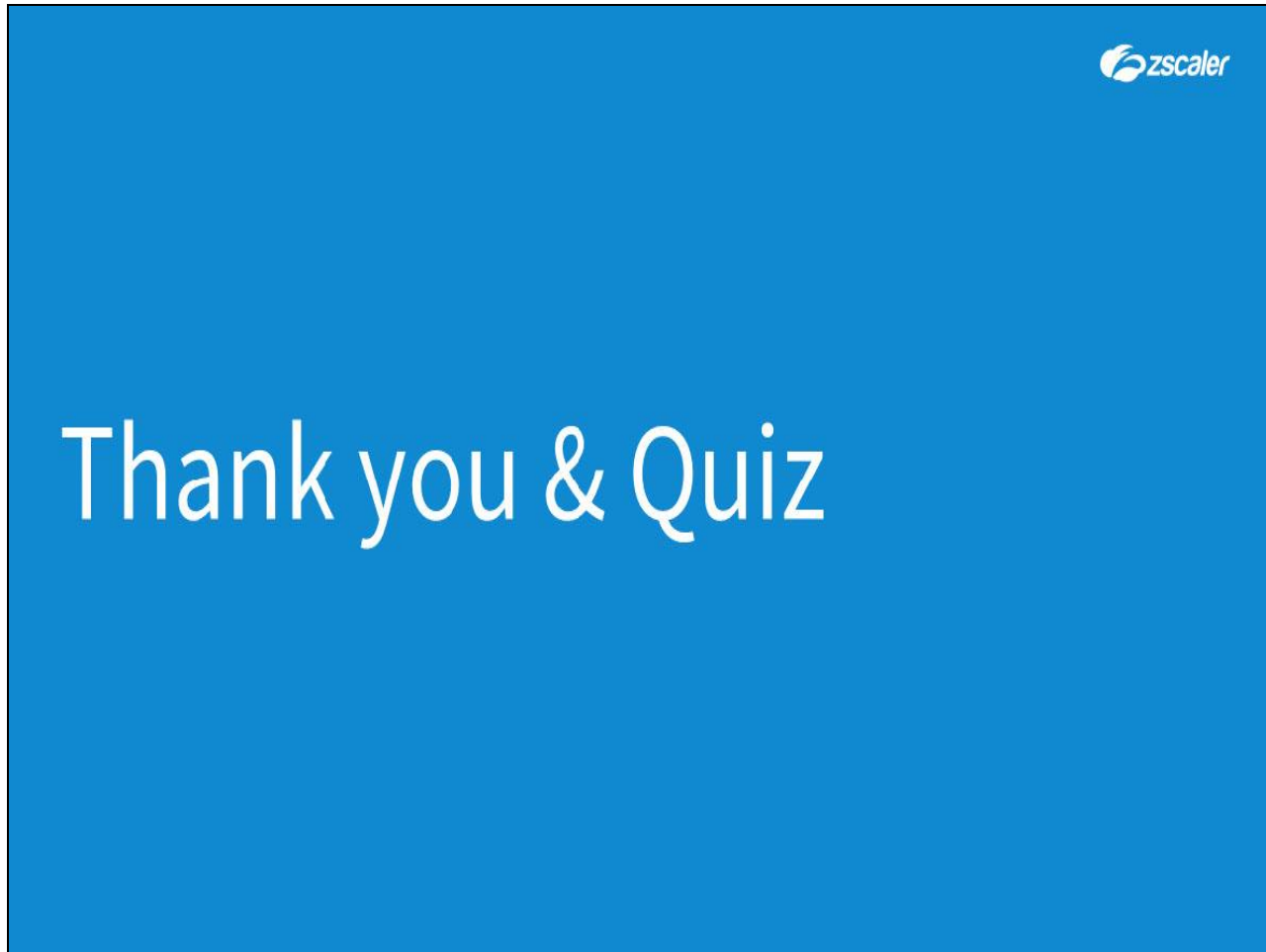
- SSL Inspection: Enable for PCs, Disable for Mobiles**
 - Or enable selectively for Mobiles
- Use the Host Name > IP Address matching for Trusted Networks**
 - Other methods can be suspect
- Reduce the Captive Portal Timer**
 - To minimize the time spent unprotected
- Keep End User Control to a minimum**
 - No user access to: **Logging, Support Access, Restart and Repair**
 - To minimize end user influence over the App environment

Slide notes

Try to keep end user controls within the App to a minimum, to avoid any opportunity for them to 'tinker' with the settings.

You can hide the logging controls, disable support access in the App and prevent the end user from restarting or repairing the services.

Slide 37 - 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.