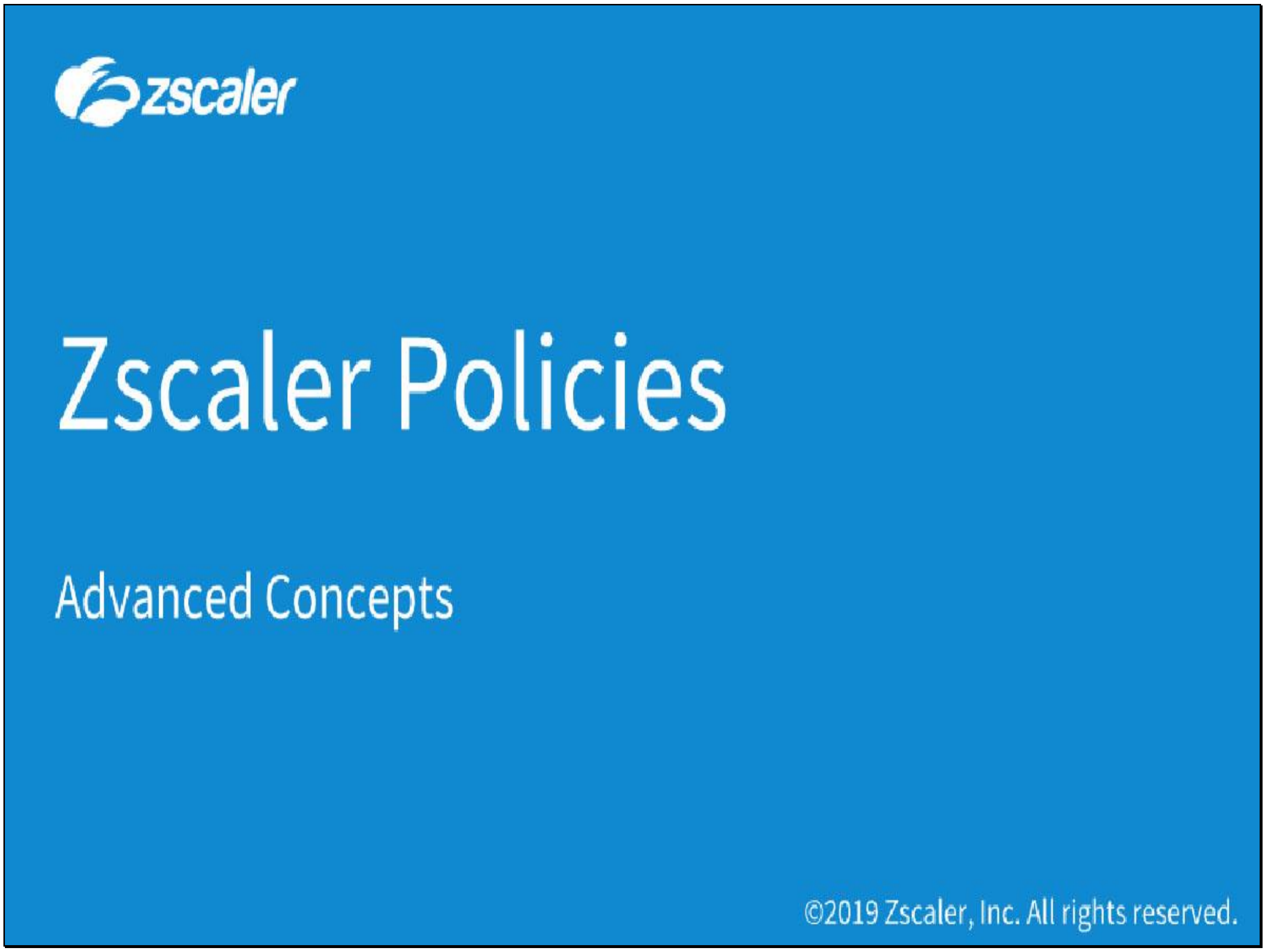
Slide 1 - Zscaler Policies



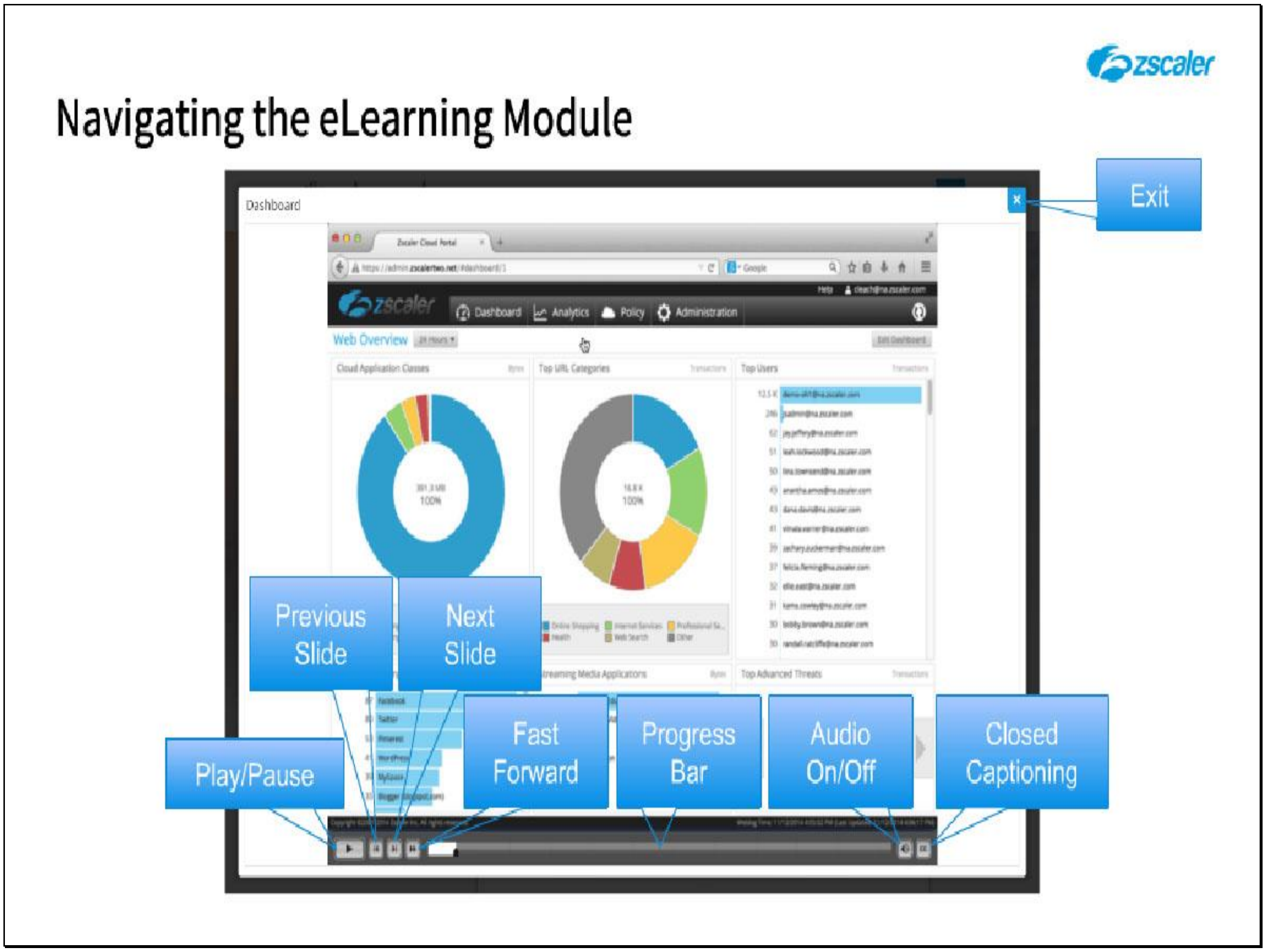
Zscaler Policies

Advanced Concepts

Slide notes

Welcome to the Zscaler Policies Advanced Concepts Module.

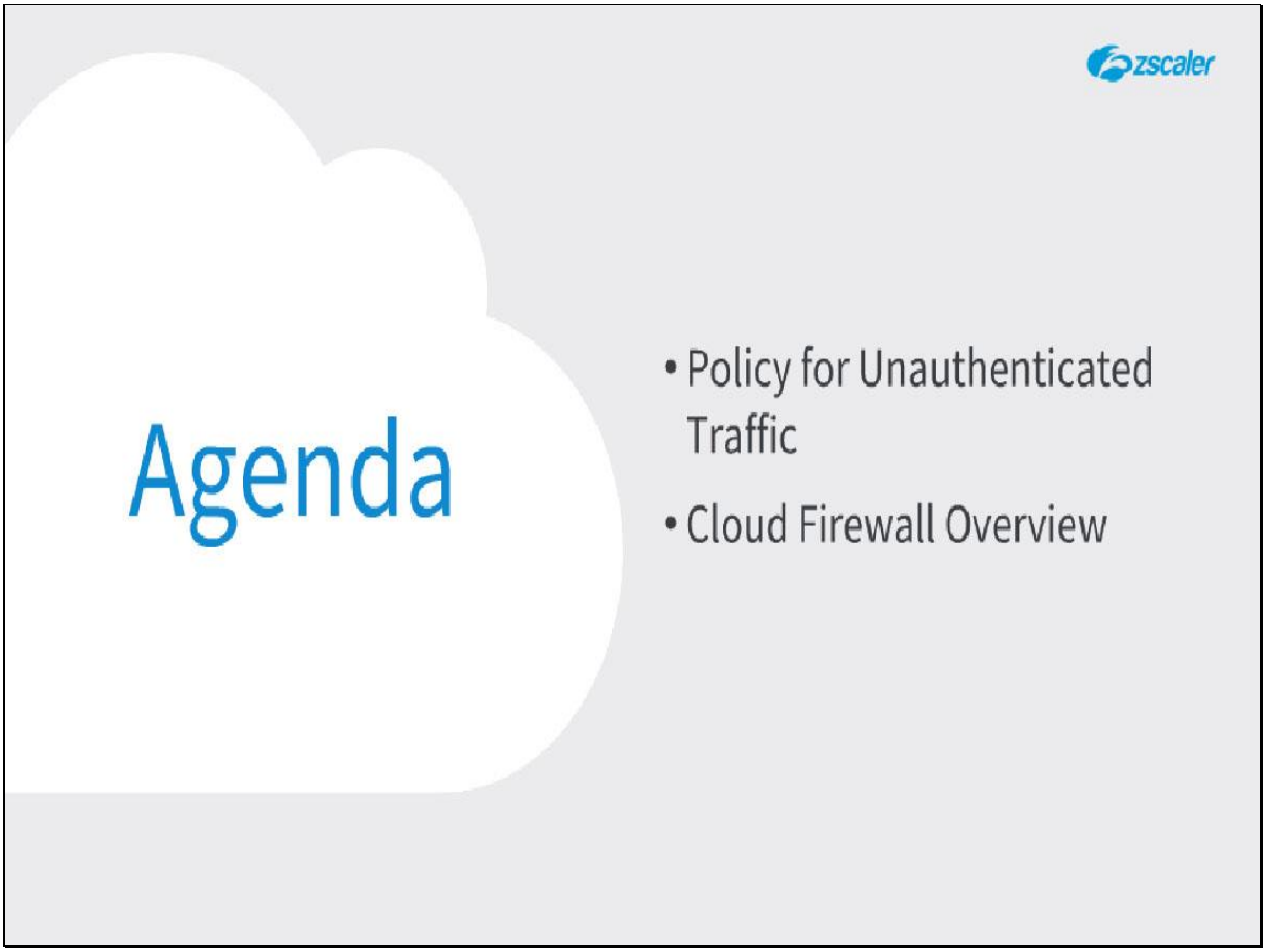
Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including play and pause, previous, 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

- Policy for Unauthenticated Traffic
- Cloud Firewall Overview

Slide notes

In this module, we will cover the application of policies to unauthenticated traffic and provide an overview of the Cloud Firewall capabilities.

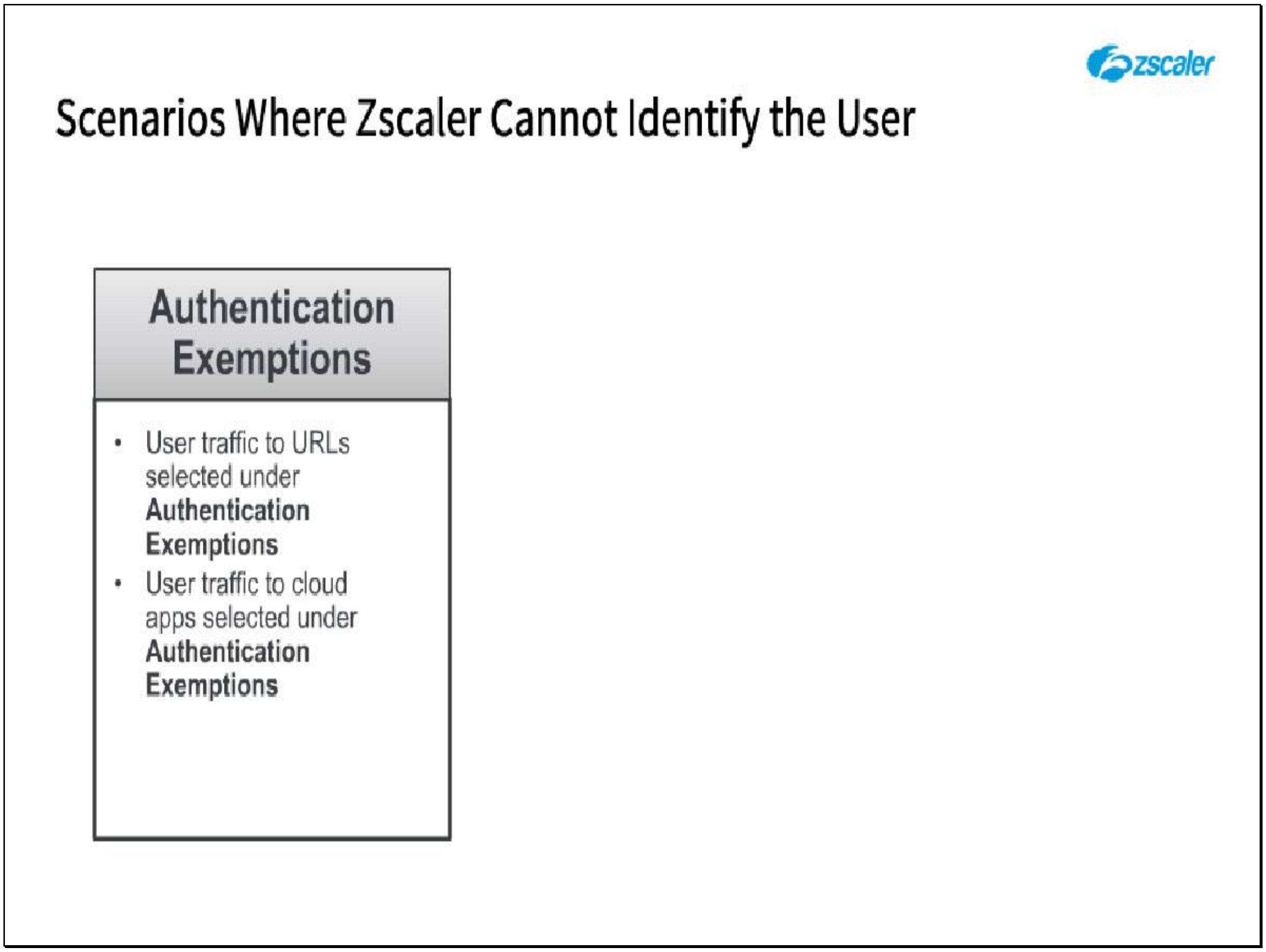
Slide 4 - Policy for Unauthenticated Traffic

Policy for Unauthenticated Traffic

Slide notes

In the next section, we will look at how to apply policy controls to unauthenticated traffic.

Slide 5 - Scenarios Where Zscaler Cannot Identify the User



Scenarios Where Zscaler Cannot Identify the User

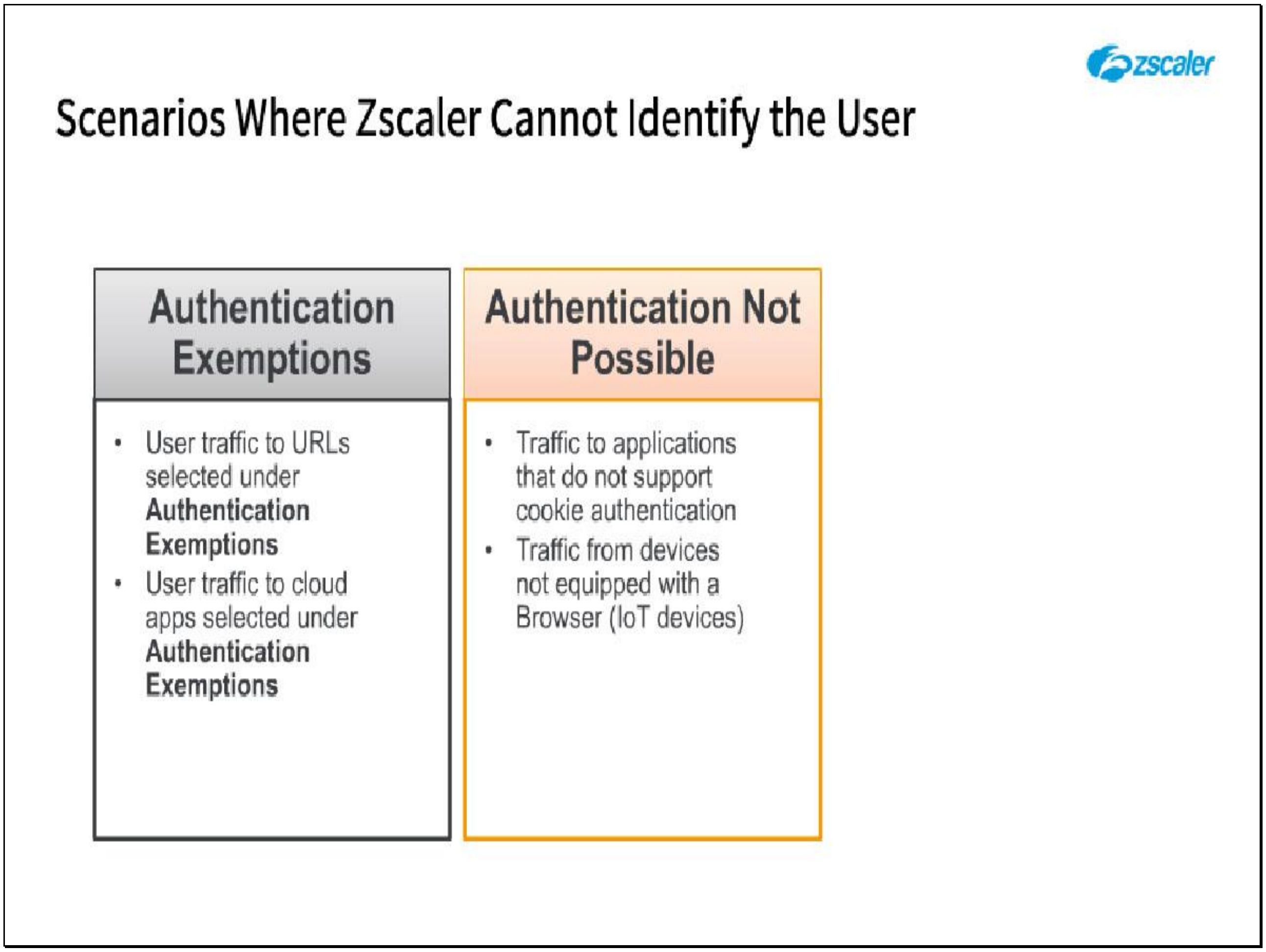
Authentication Exemptions

- User traffic to URLs selected under **Authentication Exemptions**
- User traffic to cloud apps selected under **Authentication Exemptions**

Slide notes

There may be scenarios in which the Zscaler service does not identify the user sending traffic to the service. For example, the service does not authenticate traffic to URLs or Cloud apps you have selected under the **Authentication Exemptions** option, in the **Advanced Settings**.

Slide 6 - Scenarios Where Zscaler Cannot Identify the User



Scenarios Where Zscaler Cannot Identify the User

Authentication Exemptions

- User traffic to URLs selected under **Authentication Exemptions**
- User traffic to cloud apps selected under **Authentication Exemptions**

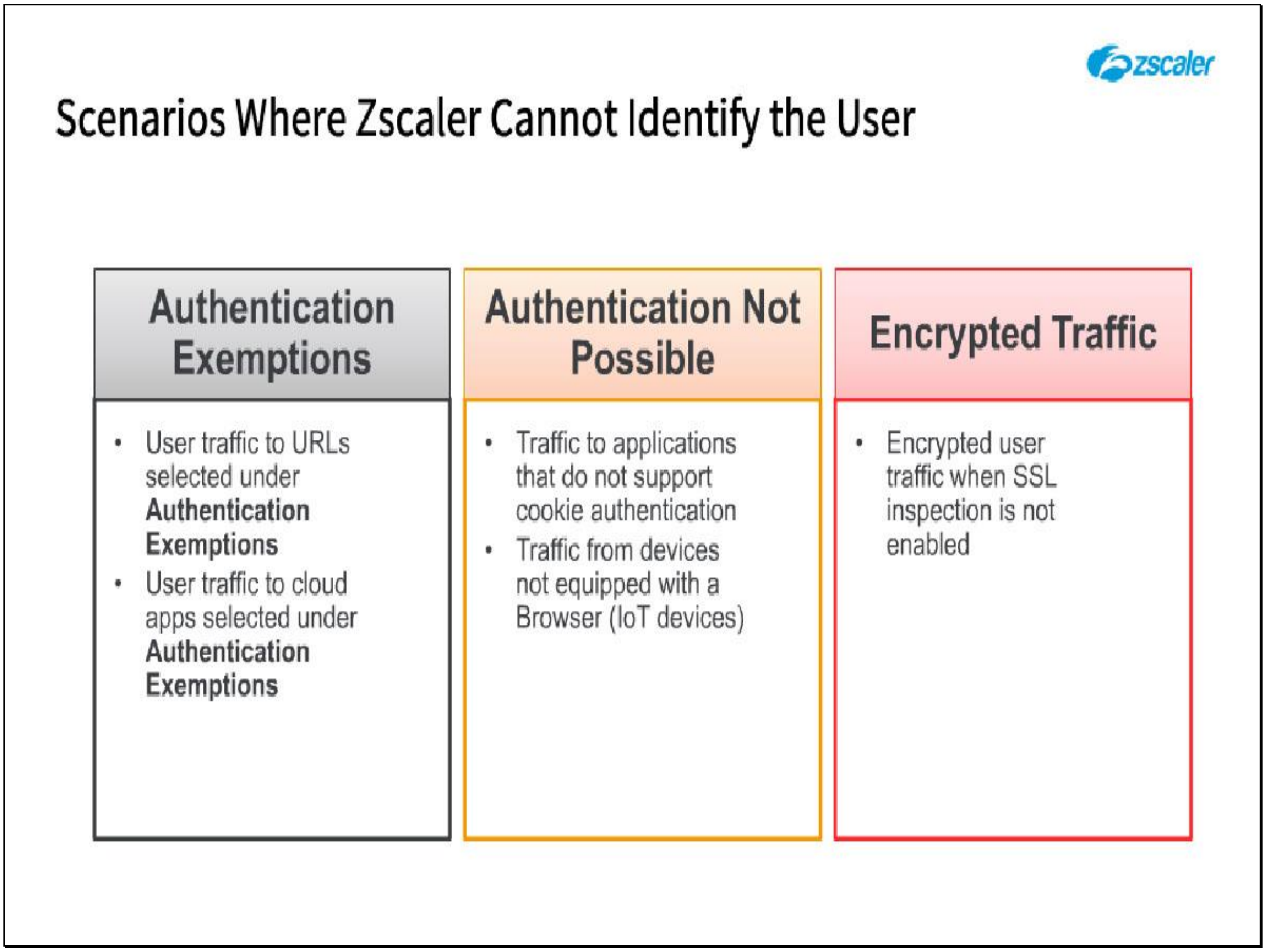
Authentication Not Possible

- Traffic to applications that do not support cookie authentication
- Traffic from devices not equipped with a Browser (IoT devices)

Slide notes

There are situations where authentication is just not possible, for example: for applications that do not support cookie-based authentication; or for devices that are just not equipped with a Web Browser, such as many of the Internet of Things (IoT) devices.

Slide 7 - Scenarios Where Zscaler Cannot Identify the User



Scenarios Where Zscaler Cannot Identify the User

Authentication Exemptions

- User traffic to URLs selected under **Authentication Exemptions**
- User traffic to cloud apps selected under **Authentication Exemptions**

Authentication Not Possible

- Traffic to applications that do not support cookie authentication
- Traffic from devices not equipped with a Browser (IoT devices)

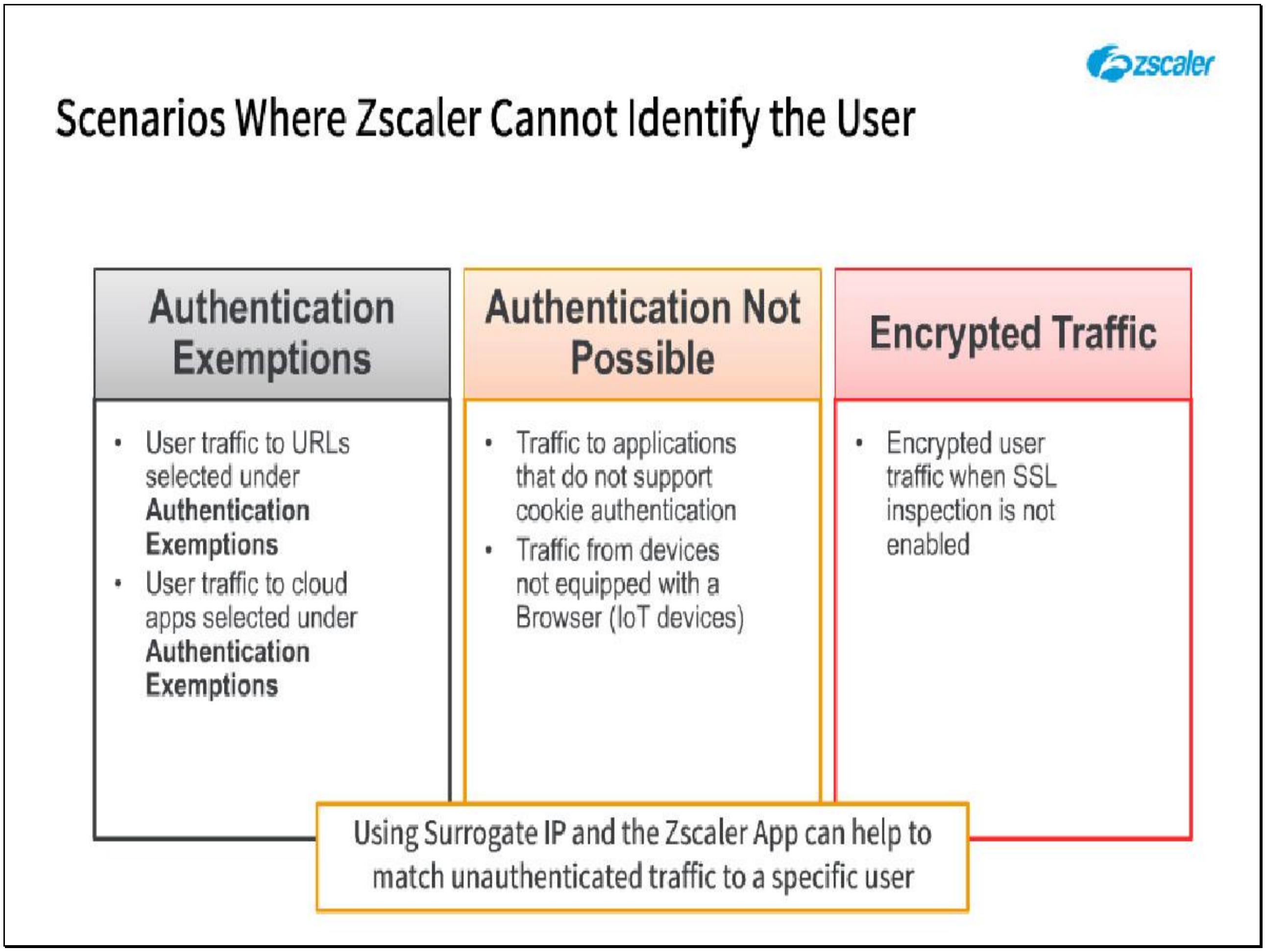
Encrypted Traffic

- Encrypted user traffic when SSL inspection is not enabled

Slide notes

Another example is encrypted traffic when SSL inspection is not enabled. If Zscaler is not inspecting SSL traffic, we are unable to identify the user generating an encrypted traffic stream.

Slide 8 - Scenarios Where Zscaler Cannot Identify the User



Scenarios Where Zscaler Cannot Identify the User

Authentication Exemptions

- User traffic to URLs selected under **Authentication Exemptions**
- User traffic to cloud apps selected under **Authentication Exemptions**

Authentication Not Possible

- Traffic to applications that do not support cookie authentication
- Traffic from devices not equipped with a Browser (IoT devices)

Encrypted Traffic

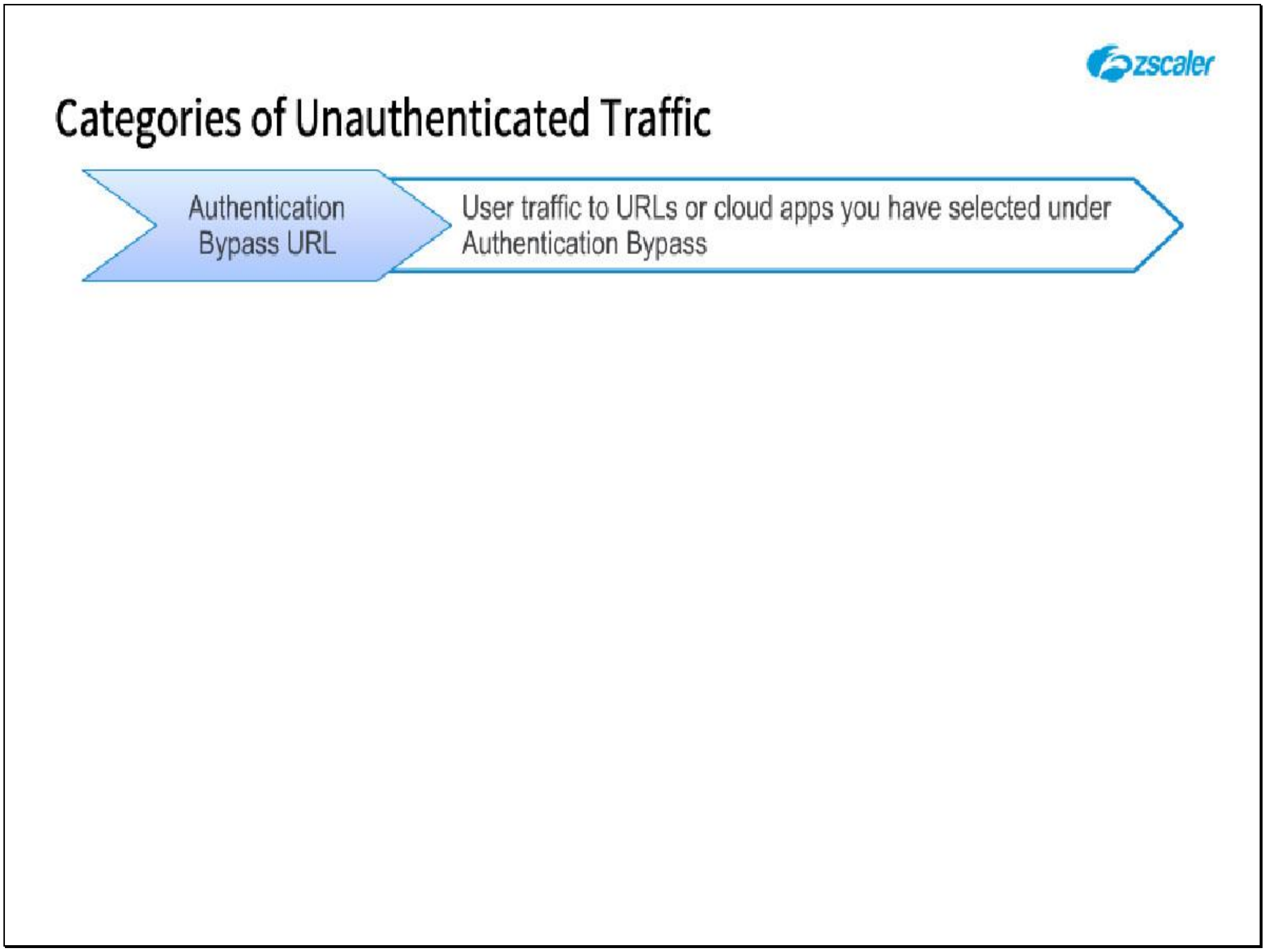
- Encrypted user traffic when SSL inspection is not enabled

Using Surrogate IP and the Zscaler App can help to match unauthenticated traffic to a specific user

Slide notes

Note that, most of these authentication issues can be resolved by enabling Surrogate IP in the location or sublocation. This creates a user-to-IP mapping each time authentication is validated (effectively each time a user visits a website). Although, note that this does require a single user per IP address, and that remote users will be excluded for the Surrogate IP option. Another way to prevent unauthenticated traffic is to use the Zscaler App, as it handles traffic authentication differently.

Slide 9 - Categories of Unauthenticated Traffic



zscaler

Categories of Unauthenticated Traffic

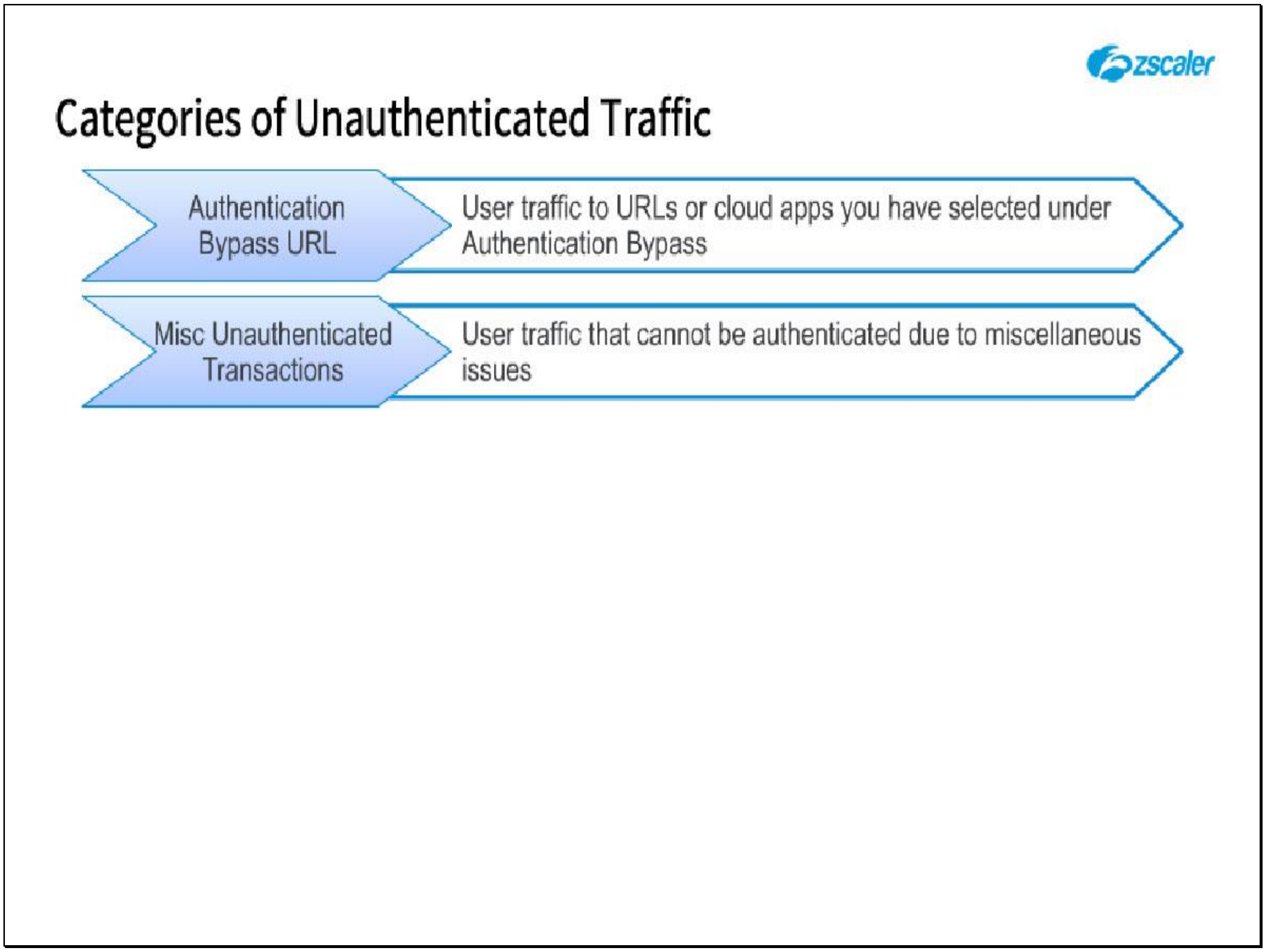
Authentication Bypass URL

User traffic to URLs or cloud apps you have selected under Authentication Bypass

Slide notes

There are several categories of unauthenticated traffic, the first of them being: **Authentication Bypass URL**. This is user traffic to URLs or cloud apps that you have added to the **Authentication Exemptions** list in the **Advanced Settings**.

Slide 10 - Categories of Unauthenticated Traffic



Categories of Unauthenticated Traffic

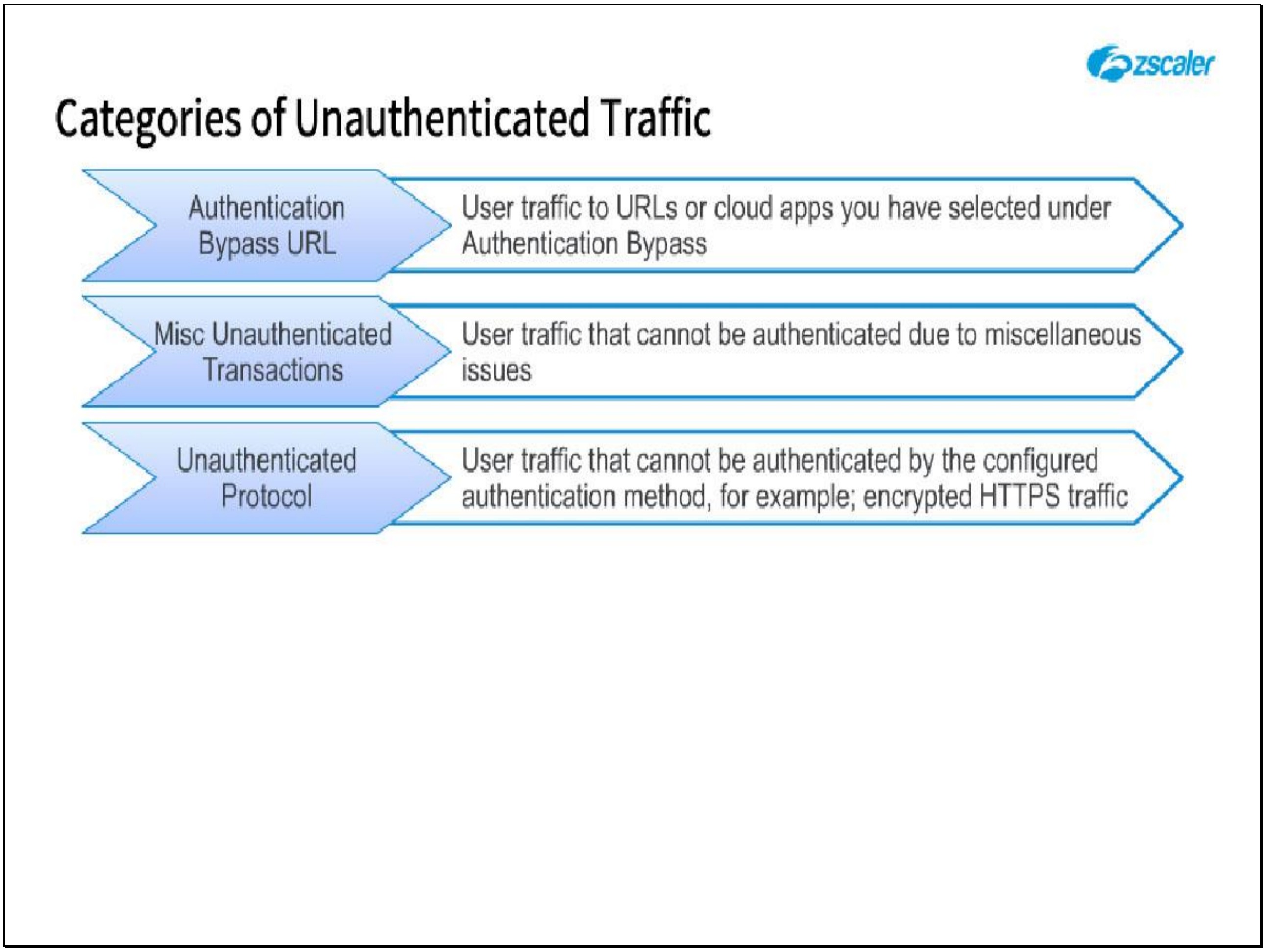
Authentication Bypass URL	User traffic to URLs or cloud apps you have selected under Authentication Bypass
Misc Unauthenticated Transactions	User traffic that cannot be authenticated due to miscellaneous issues

Slide notes

Next is the **Miscellaneous Unauthenticated Transactions** category, which is user traffic that cannot be authenticated due to miscellaneous issues.

Examples of this include: applications that don’t support HTTP redirects as used by cookie-based authentication; some Web traffic that doesn’t even use HTTP headers (such as Gstatic, or Github).

Slide 11 - Categories of Unauthenticated Traffic



zscaler

Categories of Unauthenticated Traffic

Authentication Bypass URL — User traffic to URLs or cloud apps you have selected under Authentication Bypass

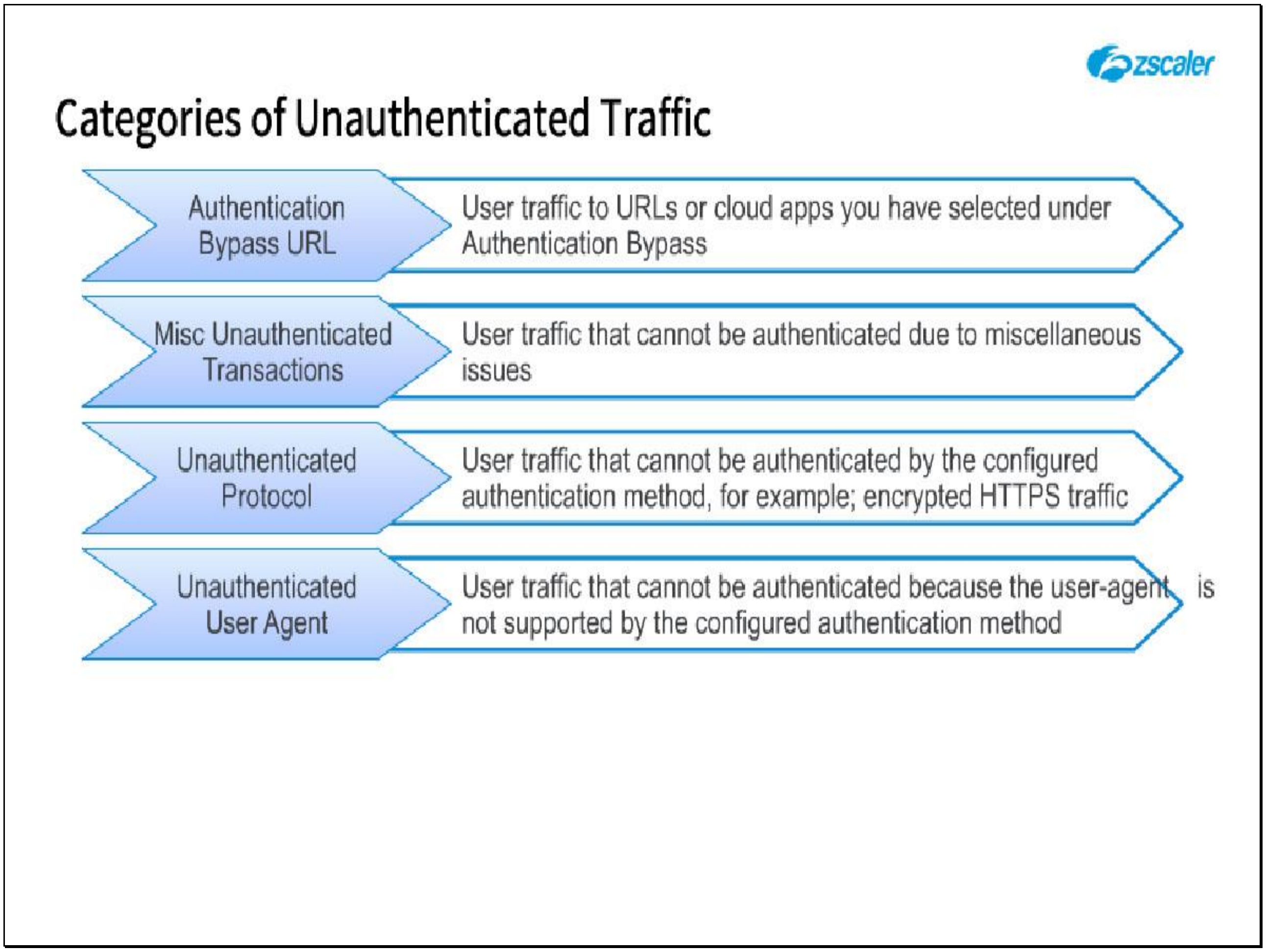
Misc Unauthenticated Transactions — User traffic that cannot be authenticated due to miscellaneous issues

Unauthenticated Protocol — User traffic that cannot be authenticated by the configured authentication method, for example; encrypted HTTPS traffic

Slide notes

The **Unauthenticated Protocol** category is user traffic that cannot be authenticated by the configured authentication method. Examples include: undecrypted HTTPS traffic; CONNECT requests prior to any HTTPS connection; FTP over HTTP.

Slide 12 - Categories of Unauthenticated Traffic



zscaler

Categories of Unauthenticated Traffic

Authentication Bypass URL — User traffic to URLs or cloud apps you have selected under Authentication Bypass

Misc Unauthenticated Transactions — User traffic that cannot be authenticated due to miscellaneous issues

Unauthenticated Protocol — User traffic that cannot be authenticated by the configured authentication method, for example; encrypted HTTPS traffic

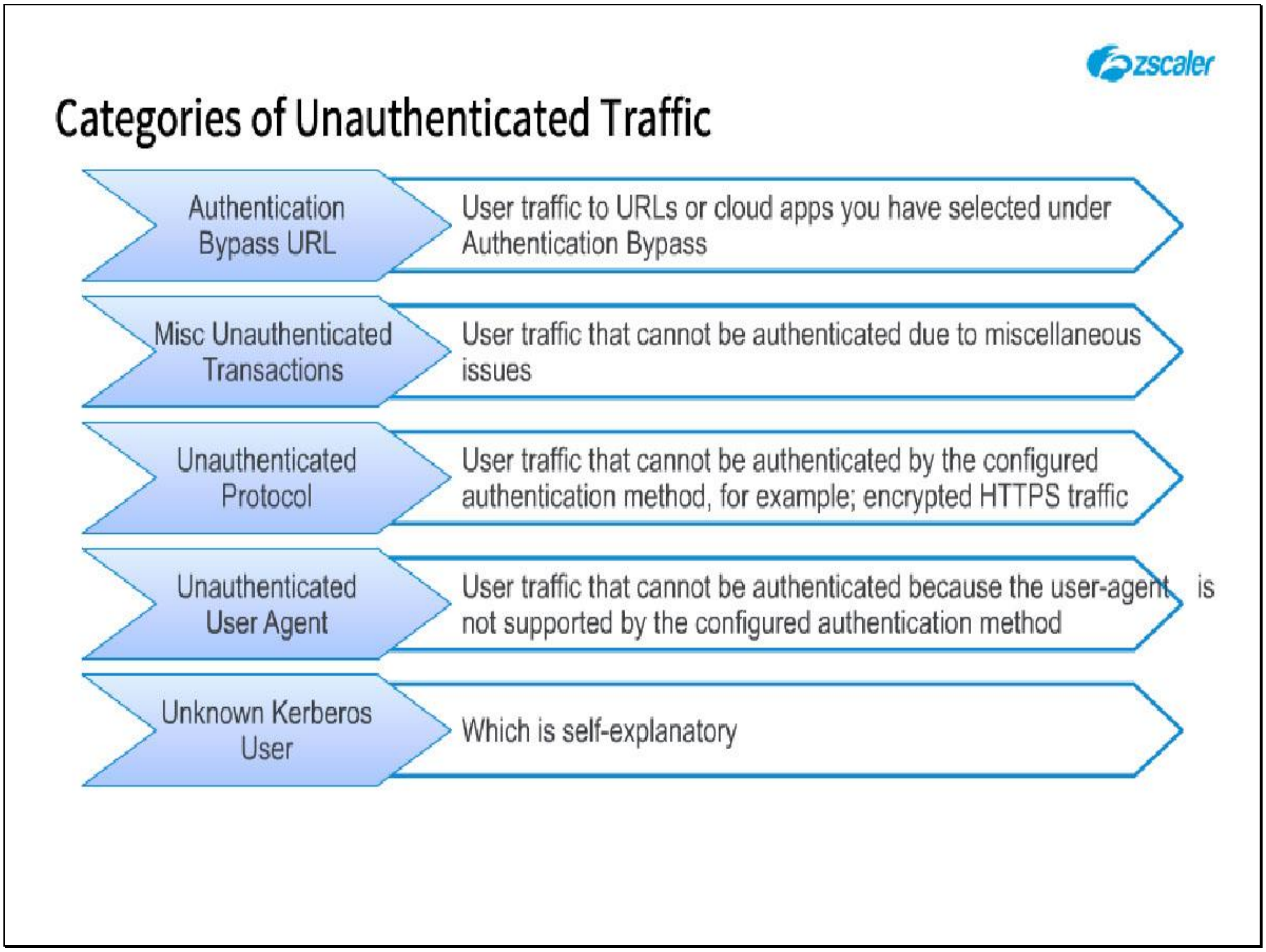
Unauthenticated User Agent — User traffic that cannot be authenticated because the user-agent is not supported by the configured authentication method

Slide notes

The **Unauthenticated User Agent** category is user traffic that cannot be authenticated because the user-agent is not supported by the configured authentication method.

Examples include: Traffic from desktop application such as Google Earth or Google Talk; Google Sync initialization; Microsoft related traffic (SharePoint lookups, Outlook auto discovery; Skype for Business).

Slide 13 - Categories of Unauthenticated Traffic



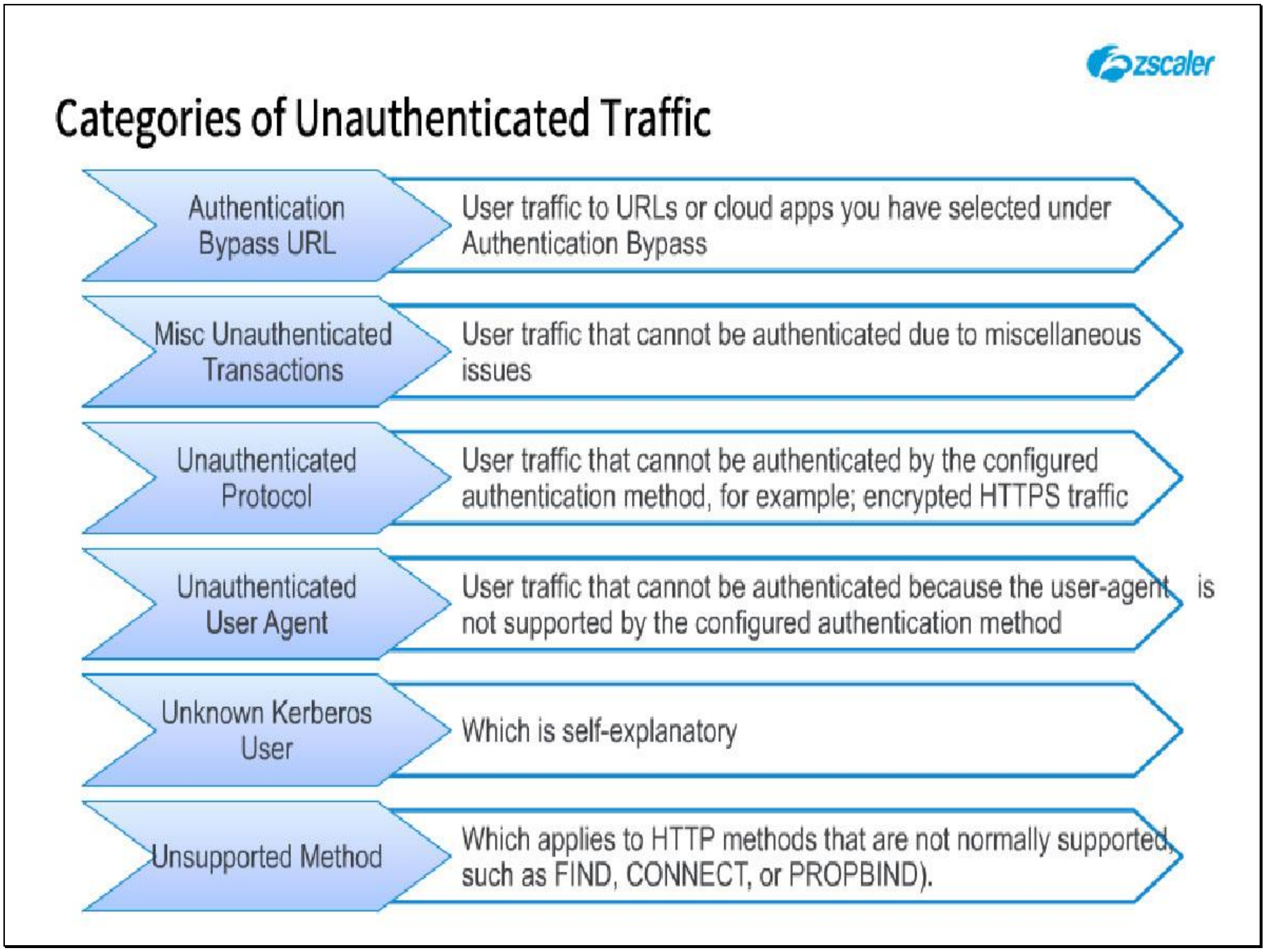
Categories of Unauthenticated Traffic

Authentication Bypass URL	User traffic to URLs or cloud apps you have selected under Authentication Bypass
Misc Unauthenticated Transactions	User traffic that cannot be authenticated due to miscellaneous issues
Unauthenticated Protocol	User traffic that cannot be authenticated by the configured authentication method, for example; encrypted HTTPS traffic
Unauthenticated User Agent	User traffic that cannot be authenticated because the user-agent is not supported by the configured authentication method
Unknown Kerberos User	Which is self-explanatory

Slide notes

The **Unknown Kerberos User** category is self-explanatory…

Slide 14 - Categories of Unauthenticated Traffic



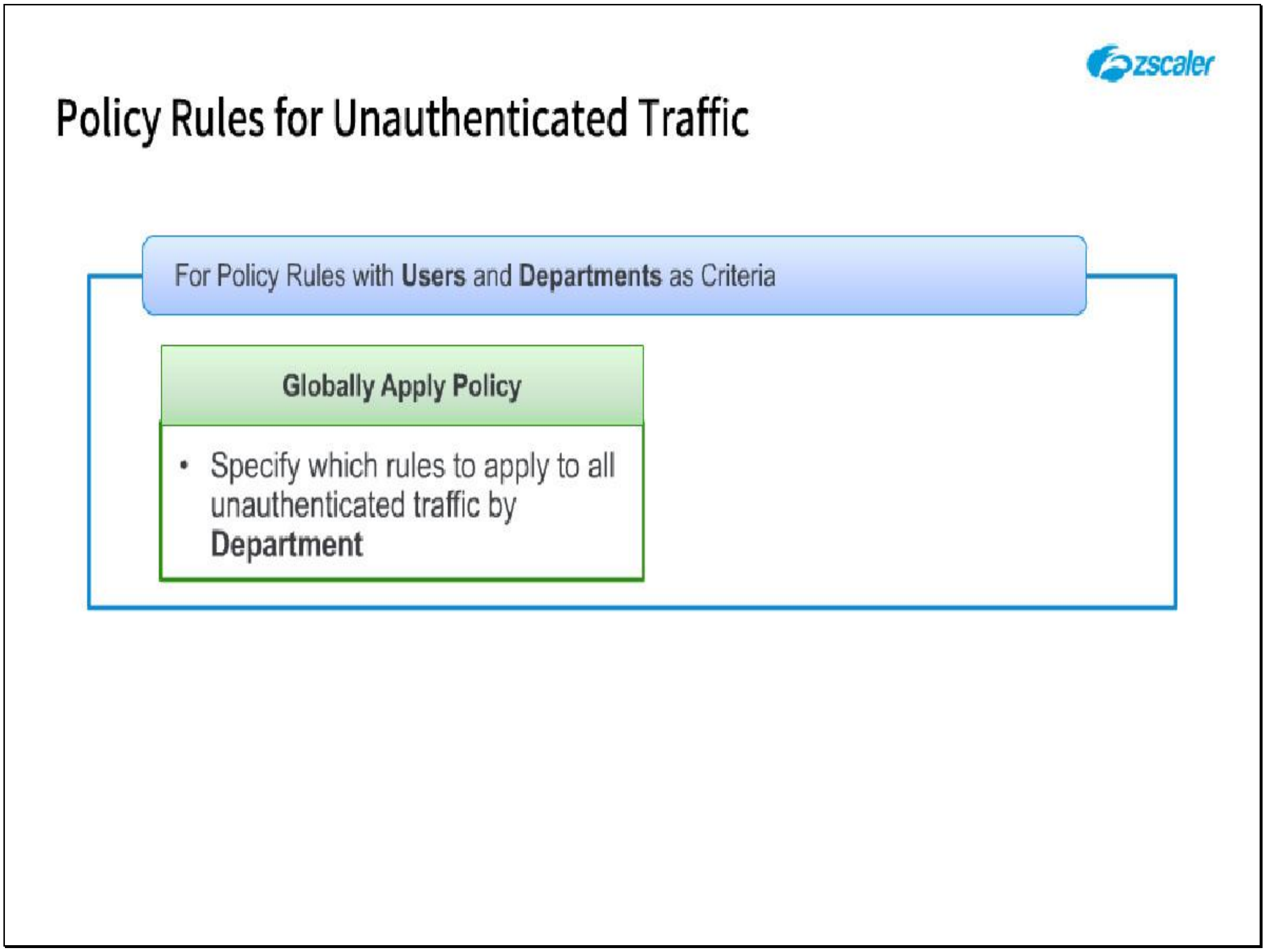
Categories of Unauthenticated Traffic

Authentication Bypass URL	User traffic to URLs or cloud apps you have selected under Authentication Bypass
Misc Unauthenticated Transactions	User traffic that cannot be authenticated due to miscellaneous issues
Unauthenticated Protocol	User traffic that cannot be authenticated by the configured authentication method, for example; encrypted HTTPS traffic
Unauthenticated User Agent	User traffic that cannot be authenticated because the user-agent is not supported by the configured authentication method
Unknown Kerberos User	Which is self-explanatory
Unsupported Method	Which applies to HTTP methods that are not normally supported, such as FIND, CONNECT, or PROPBIND).

Slide notes

…and finally, the **Unsupported Method** category, which applies to HTTP methods that are not normally supported, such as FIND, CONNECT, or PROPBIND.

Slide 15 - Policy Rules for Unauthenticated Traffic



Policy Rules for Unauthenticated Traffic

For Policy Rules with **Users** and **Departments** as Criteria

Globally Apply Policy

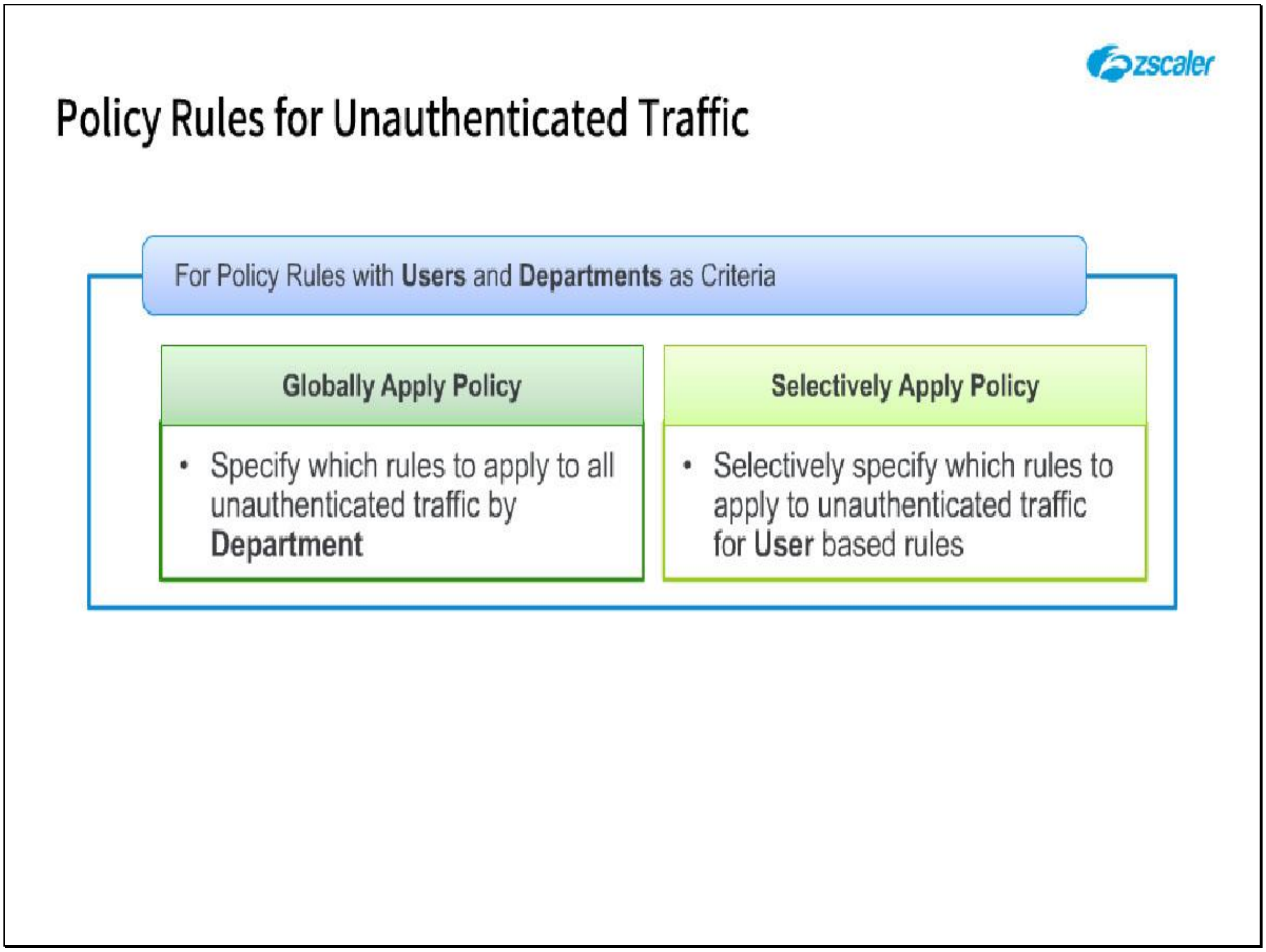
- Specify which rules to apply to all unauthenticated traffic by **Department**

Slide notes

For policies that support **User** and **Department** in the criteria, Zscaler allows you to specify which rules are applied to such unauthenticated traffic. For example, if your organization has changed the implicit **Allow All** rule for Web traffic to **Block** (to block all traffic that is not explicitly allowed in a preceding URL Filtering rule), the policy for unauthenticated traffic feature can help you ensure that the lack of authentication does not lead to the unwanted blocking of user traffic.

Once the feature is enabled on the **Administration > Advanced Settings** page, you can select whether a policy rule is also to apply to all unauthenticated traffic by **Department**…

Slide 16 - Policy Rules for Unauthenticated Traffic



Policy Rules for Unauthenticated Traffic

For Policy Rules with **Users** and **Departments** as Criteria

Globally Apply Policy

- Specify which rules to apply to all unauthenticated traffic by **Department**

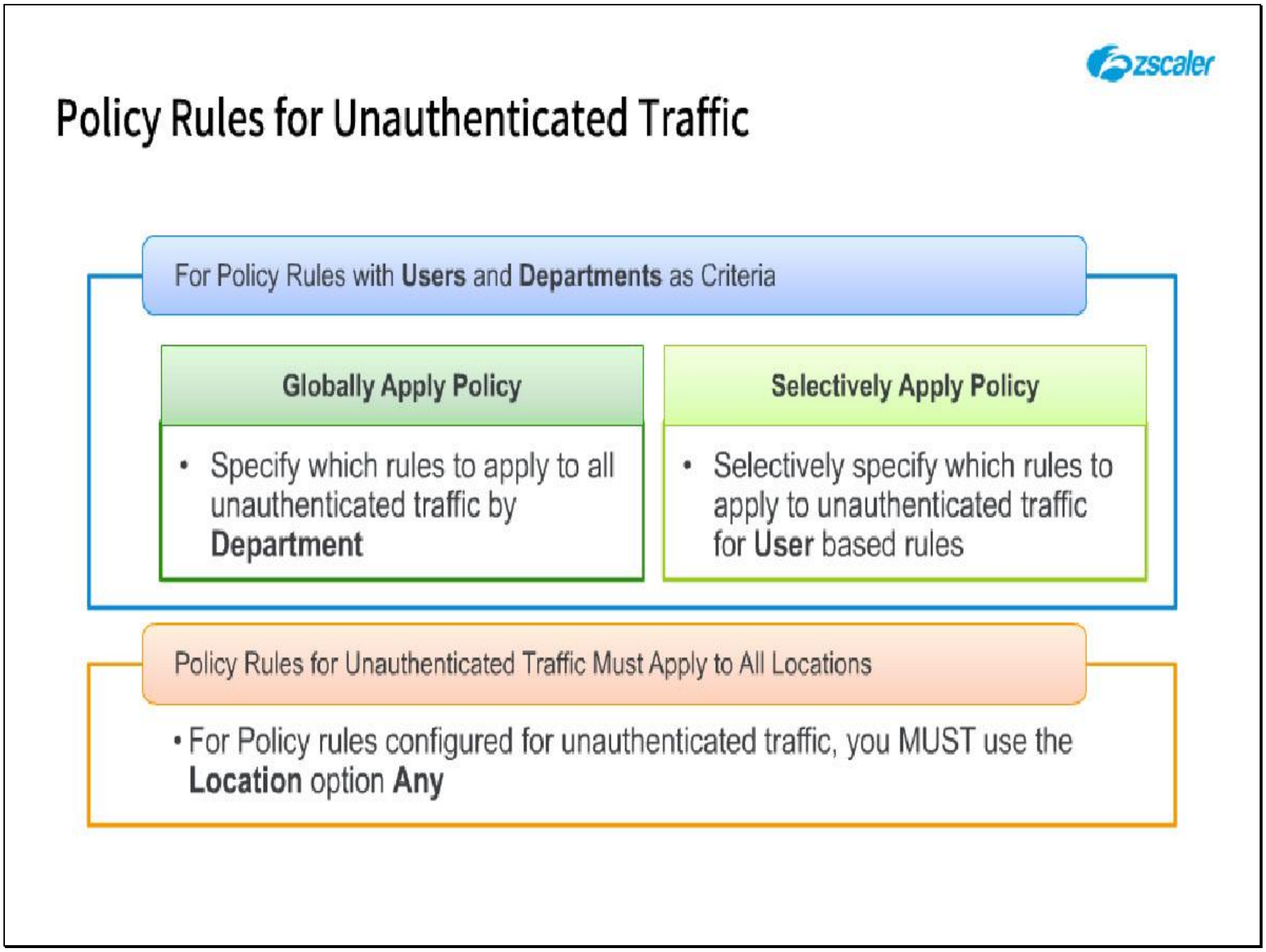
Selectively Apply Policy

- Selectively specify which rules to apply to unauthenticated traffic for **User** based rules

Slide notes

…or for more granularity you can select the types of unauthenticated traffic to which the policy rule applies under the **Users** criteria (for example, to apply a rule only when traffic is unauthenticated due to an **Authentication Exemption**).

Slide 17 - Policy Rules for Unauthenticated Traffic



Policy Rules for Unauthenticated Traffic

For Policy Rules with **Users** and **Departments** as Criteria

Globally Apply Policy

- Specify which rules to apply to all unauthenticated traffic by **Department**

Selectively Apply Policy

- Selectively specify which rules to apply to unauthenticated traffic for **User** based rules

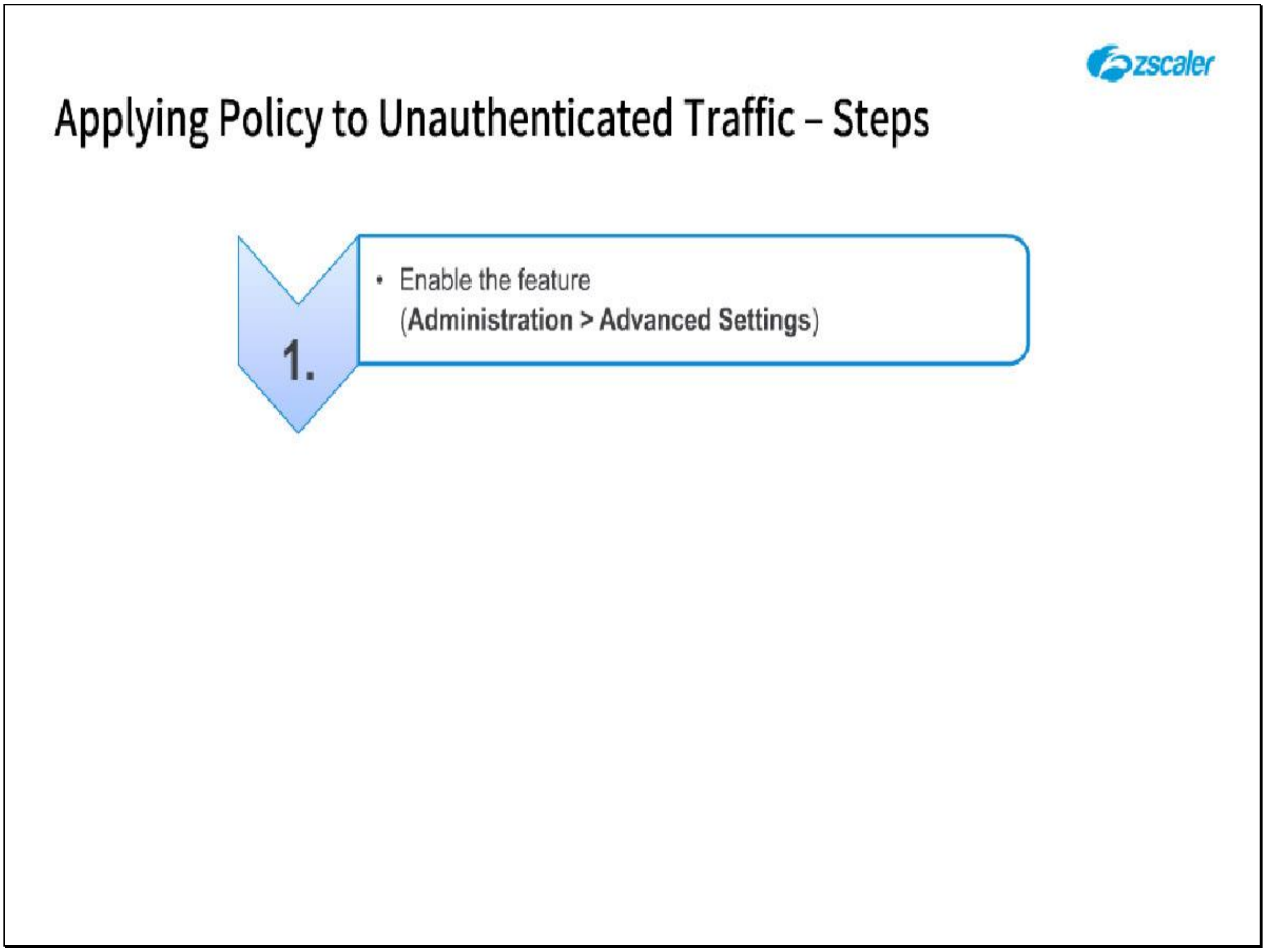
Policy Rules for Unauthenticated Traffic Must Apply to All Locations

- For Policy rules configured for unauthenticated traffic, you MUST use the **Location** option **Any**

Slide notes

Note, that any policy rule which applies to unauthenticated traffic must be applied to all locations; you cannot apply a rule to unauthenticated traffic and subsequently select to apply it to specific locations.

Slide 18 - Applying Policy to Unauthenticated Traffic – Steps



zscaler

Applying Policy to Unauthenticated Traffic – Steps

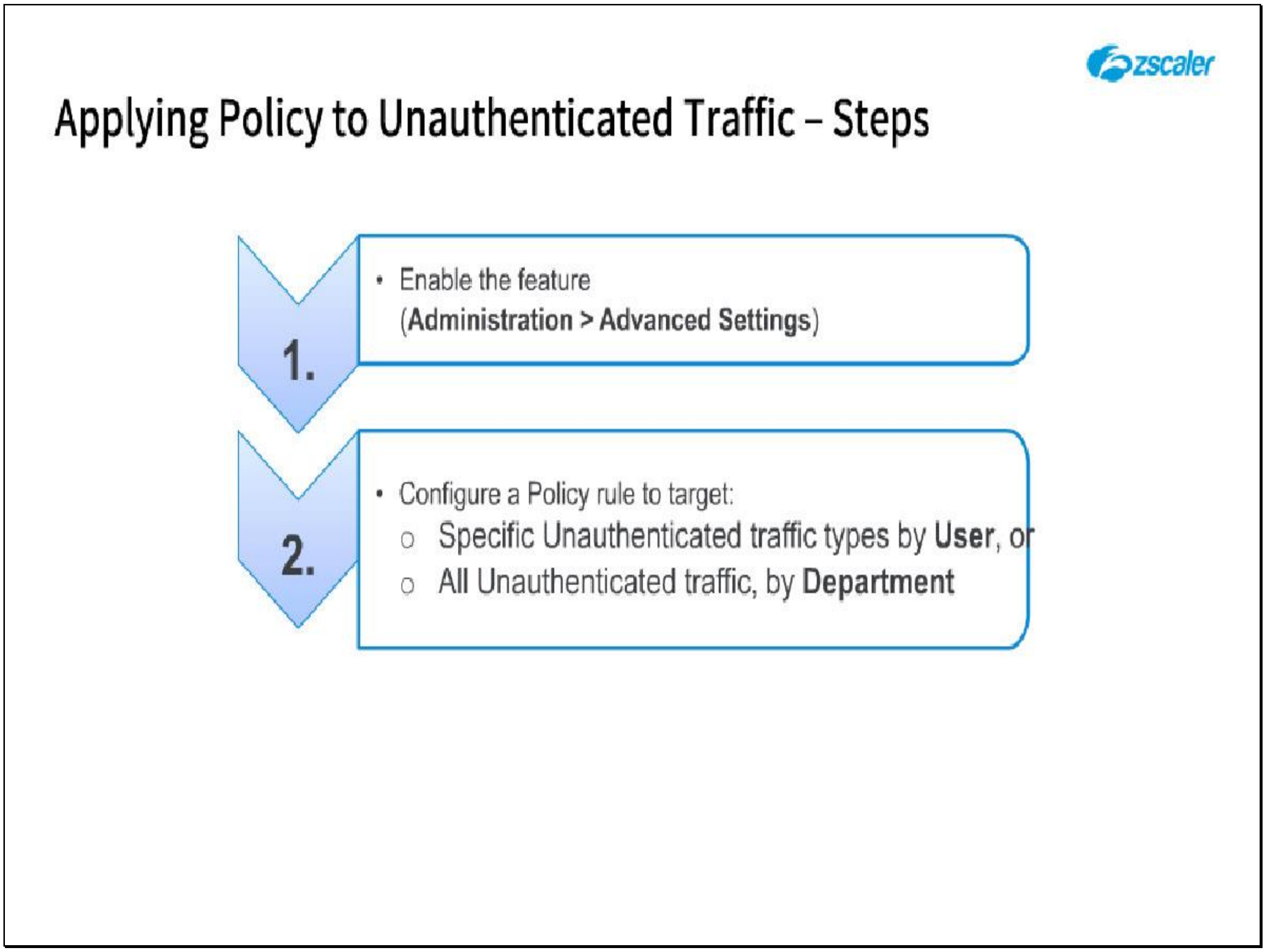
1.

- Enable the feature (**Administration > Advanced Settings**)

Slide notes

The steps for applying policy rules to unauthenticated traffic are: One - enable the feature on the **Administration > Advanced Settings** page, then save and activate the change.

Slide 19 - Applying Policy to Unauthenticated Traffic – Steps



Applying Policy to Unauthenticated Traffic – Steps

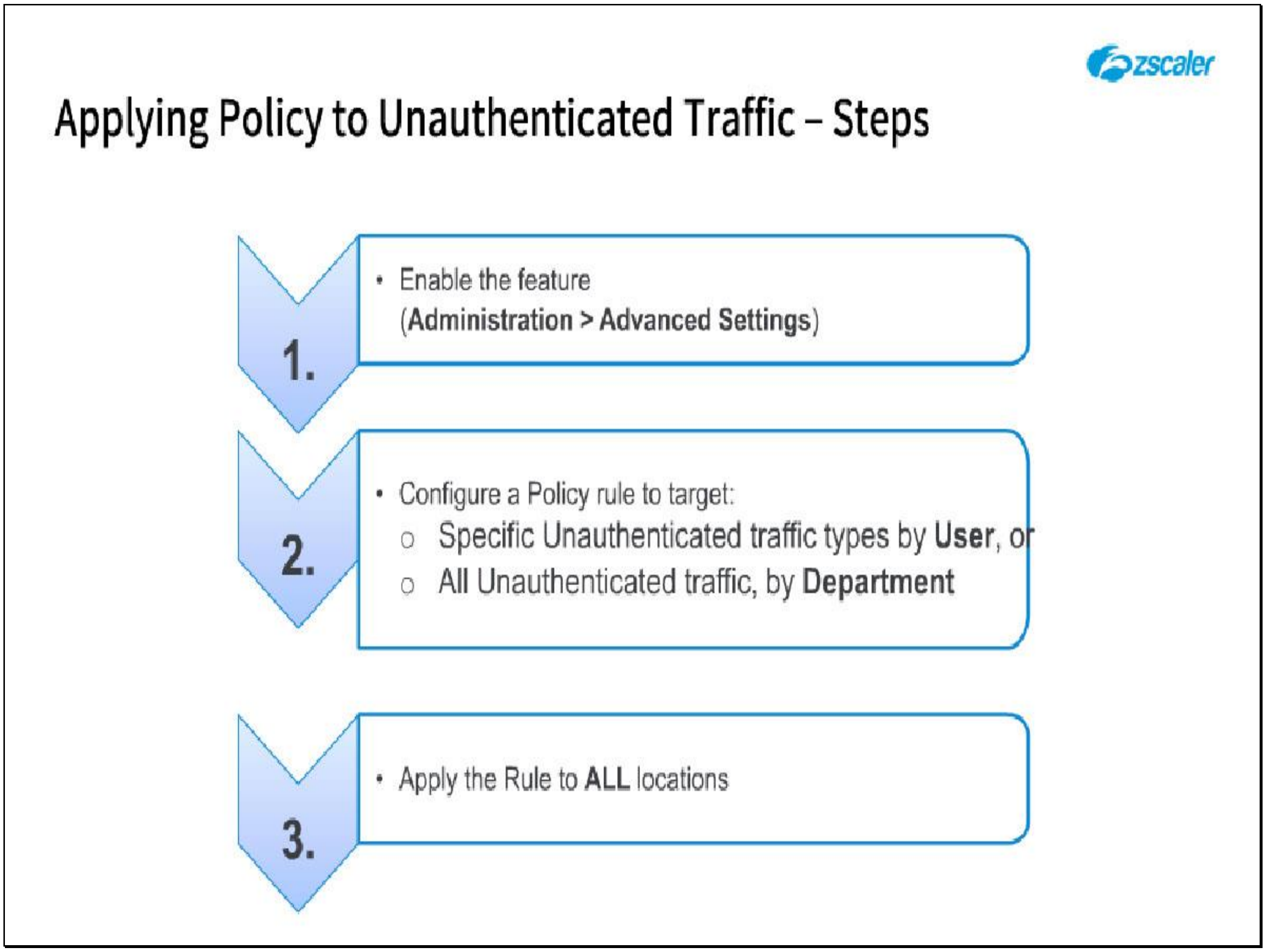
1.
- Enable the feature (**Administration > Advanced Settings**)

2.
- Configure a Policy rule to target:
  - Specific Unauthenticated traffic types by **User**, or
  - All Unauthenticated traffic, by **Department**

Slide notes

Two - having enabled the feature, you will find that the **Users** and **Departments** criteria within the policy rules configuration have been expanded to include **Special Users**, and **Special Departments**. These options can be used to target a policy rule against specific unauthenticated traffic types, or all unauthenticated transactions.

Slide 20 - Applying Policy to Unauthenticated Traffic – Steps



Applying Policy to Unauthenticated Traffic – Steps

1.
- Enable the feature (**Administration > Advanced Settings**)

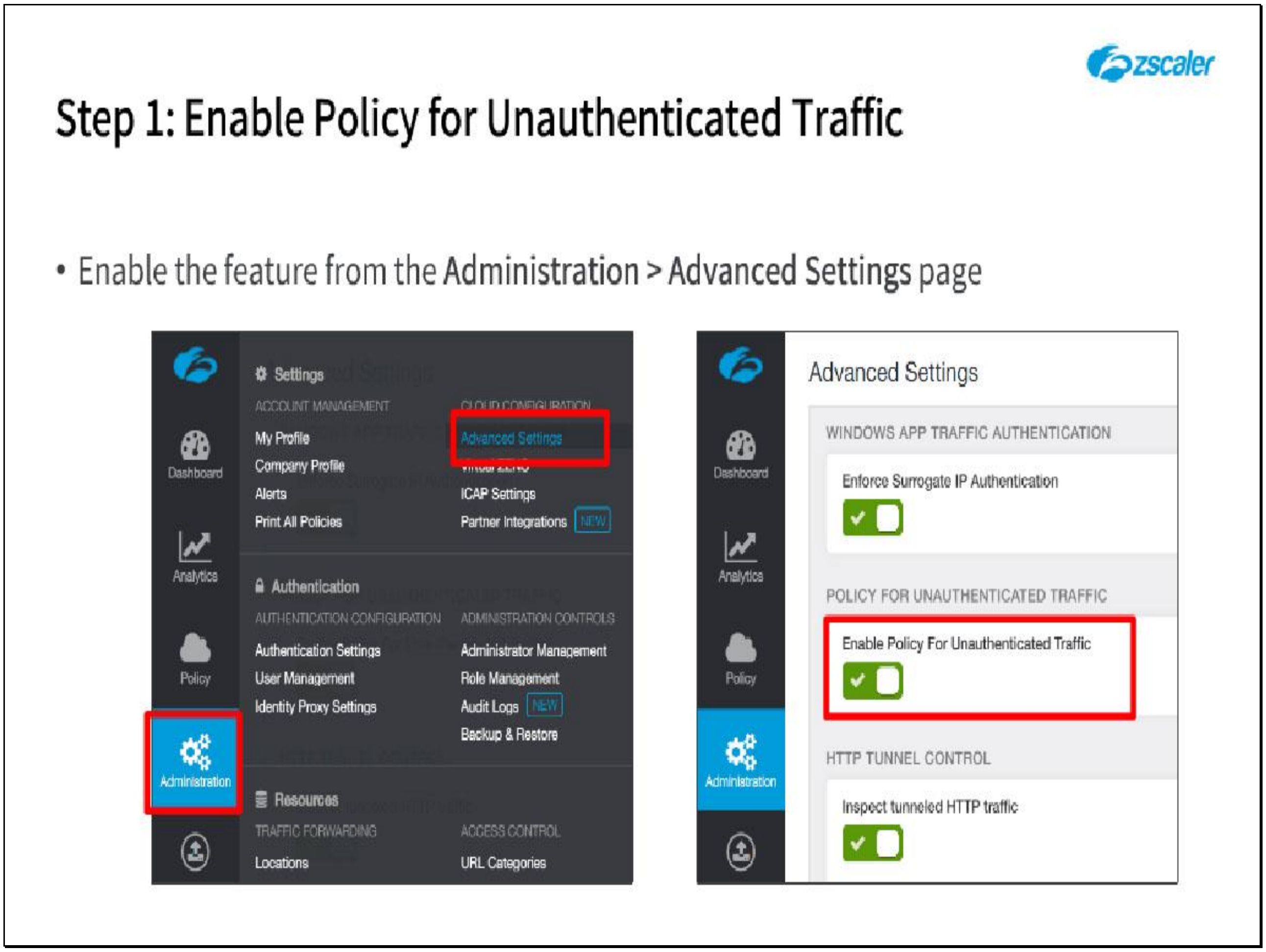
2.
- Configure a Policy rule to target:
  - Specific Unauthenticated traffic types by **User**, or
  - All Unauthenticated traffic, by **Department**

3.
- Apply the Rule to **ALL** locations

Slide notes

Three - any policy rule that contains an unauthenticated traffic configuration must also be configured to apply to **ALL** Locations.

Slide 21 - Step 1: Enable Policy for Unauthenticated Traffic



Step 1: Enable Policy for Unauthenticated Traffic

- Enable the feature from the Administration > Advanced Settings page

Advanced Settings

WINDOWS APP TRAFFIC AUTHENTICATION

Enforce Surrogate IP Authentication ✓

POLICY FOR UNAUTHENTICATED TRAFFIC

Enable Policy For Unauthenticated Traffic ✓

HTTP TUNNEL CONTROL

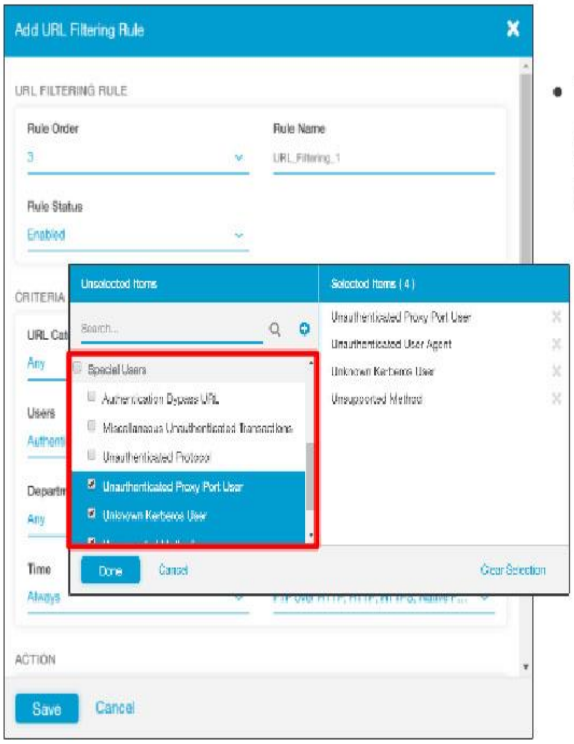
Inspect tunneled HTTP traffic ✓

Slide notes

To enable policy configurations for unauthenticated traffic, go to the **Administration > Advanced Settings** page, activate the **Enable Policy For Unauthenticated Traffic** option, then **Save** and **Activate** your changes.

Slide 22 - Unauthenticated Traffic Policy Rule Configuration

Unauthenticated Traffic Policy Rule Configuration



Add URL Filtering Rule

URL FILTERING RULE

Rule Order: 3

Rule Name: URL_Filtering_1

Rule Status: Enabled

CRITERIA

URL Cat: Any

Users: Authent

Departm: Any

Time: Always

Unselected Items

Special Users

- ☐ Authentication Bypass URL
- ☐ Miscellaneous Unauthenticated Transactions
- ☐ Unauthenticated Protocol
- ☑ Unauthenticated Proxy Port User
- ☑ Unknown Kerberos User

Selected Items (4)

- Unauthenticated Proxy Port User
- Unauthenticated User Agent
- Unknown Kerberos User
- Unsupported Method

ACTION

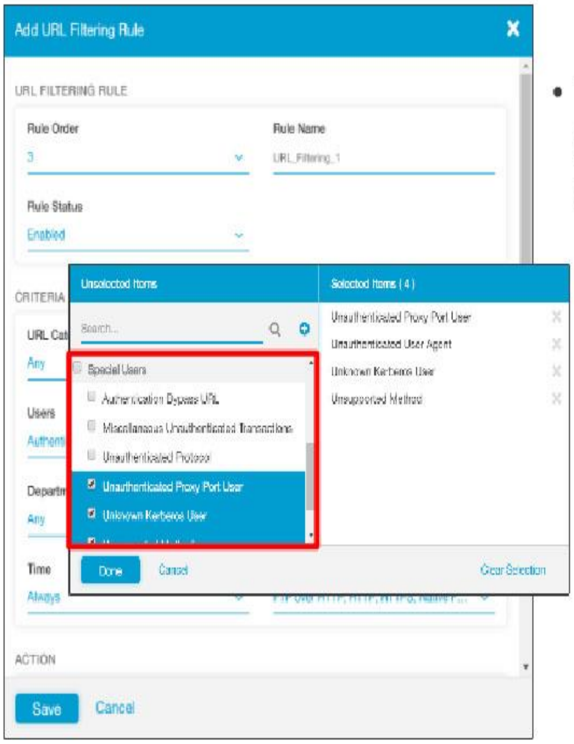
- To apply a rule to specific types of traffic, in the Users field select up to 4 of the Special Users:
  - Authentication Bypass URL
  - Miscellaneous Unauthenticated Transactions
  - Unauthenticated Protocol
  - Unauthenticated Proxy Port User
  - Unauthenticated User Agent
  - Unknown Kerberos User
  - Unsupported Method

Slide notes

Once the feature is enabled, within a policy rule configuration you will find that additional **Special Users** are listed within the **Users** field. These match the categories of unauthenticated traffic that we discussed earlier. You can select up to four of them to apply the policy to.

Slide 23 - Unauthenticated Traffic Policy Rule Configuration

Unauthenticated Traffic Policy Rule Configuration



Add URL Filtering Rule

URL FILTERING RULE

Rule Order: 3

Rule Name: URL_Filtering_1

Rule Status: Enabled

CRITERIA

URL Cat: Any

Users: Authent

Departm: Any

Time: Always

Unselected Items

- □ Special Users
  - □ Authentication Bypass URL
  - □ Miscellaneous Unauthenticated Transactions
  - □ Unauthenticated Protocol
  - ☑ Unauthenticated Proxy Port User
  - ☑ Unknown Kerberos User

Selected Items (4)

- Unauthenticated Proxy Port User
- Unauthenticated User Agent
- Unknown Kerberos User
- Unsupported Method

- To apply a rule to specific types of traffic, in the Users field select up to 4 of the Special Users:
  - Authentication Bypass URL
  - Miscellaneous Unauthenticated Transactions
  - Unauthenticated Protocol
  - Unauthenticated Proxy Port User
  - Unauthenticated User Agent
  - Unknown Kerberos User
  - Unsupported Method

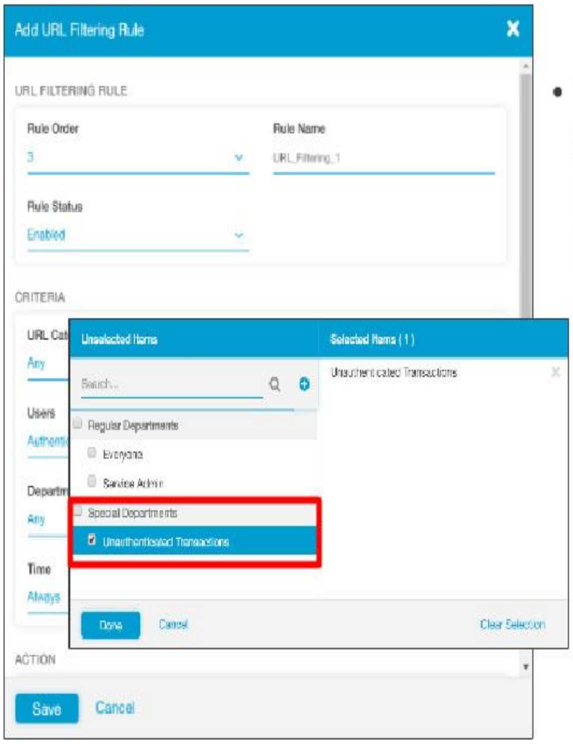
Note: these special users are NOT included in the **Any** option

Slide notes

One thing to note is that these special users are NOT included if you select the **Any** option in the **Users** field.

Slide 24 - Unauthenticated Traffic Policy Rule Configuration

Unauthenticated Traffic Policy Rule Configuration



Rule Order: 3
Rule Name: URL_Filtering_1
Rule Status: Enabled
URL Cat: Any
Users: Authenti
Departm: Any
Time: Always

□ Regular Departments
□ Everyone
□ Service Admin
□ Special Departments
☑ Unauthenticated Transactions

Selected Items (1): Unauthenticated Transactions

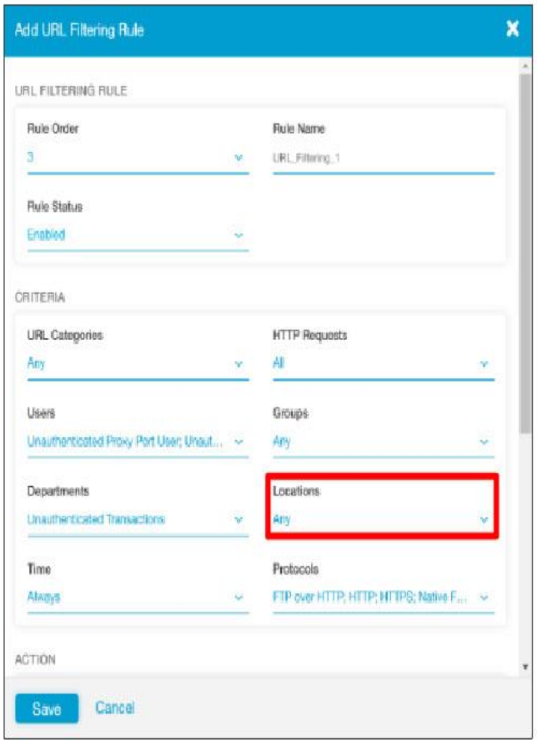
- To apply the rule to all unauthenticated traffic, in the **Departments** field select the **Unauthenticated Transactions** option under **Special Departments**

Slide notes

You will also find an additional **Special Departments** option under the policy rule configuration **Departments** field. Under **Special Departments**, select **Unauthenticated Transactions** if you want the rule to apply to ALL unauthenticated traffic.

Slide 25 - Unauthenticated Traffic Policy Rule Configuration

Unauthenticated Traffic Policy Rule Configuration



Add URL Filtering Rule

URL FILTERING RULE

Rule Order: 3

Rule Name: URL_Filtering_1

Rule Status: Enabled

CRITERIA

URL Categories: Any

HTTP Requests: All

Users: Unauthenticated Proxy Port User; Unaut...

Groups: Any

Departments: Unauthenticated Transactions

Locations: Any

Time: Always

Protocols: FTP over HTTP; HTTP; HTTPS; Native F...

ACTION

- For all rules that include options for unauthenticated traffic, select the Location option Any

Slide notes

Any rule that applies to unauthenticated traffic must apply to all locations, so in the **Locations** field you must select the **Any** option.

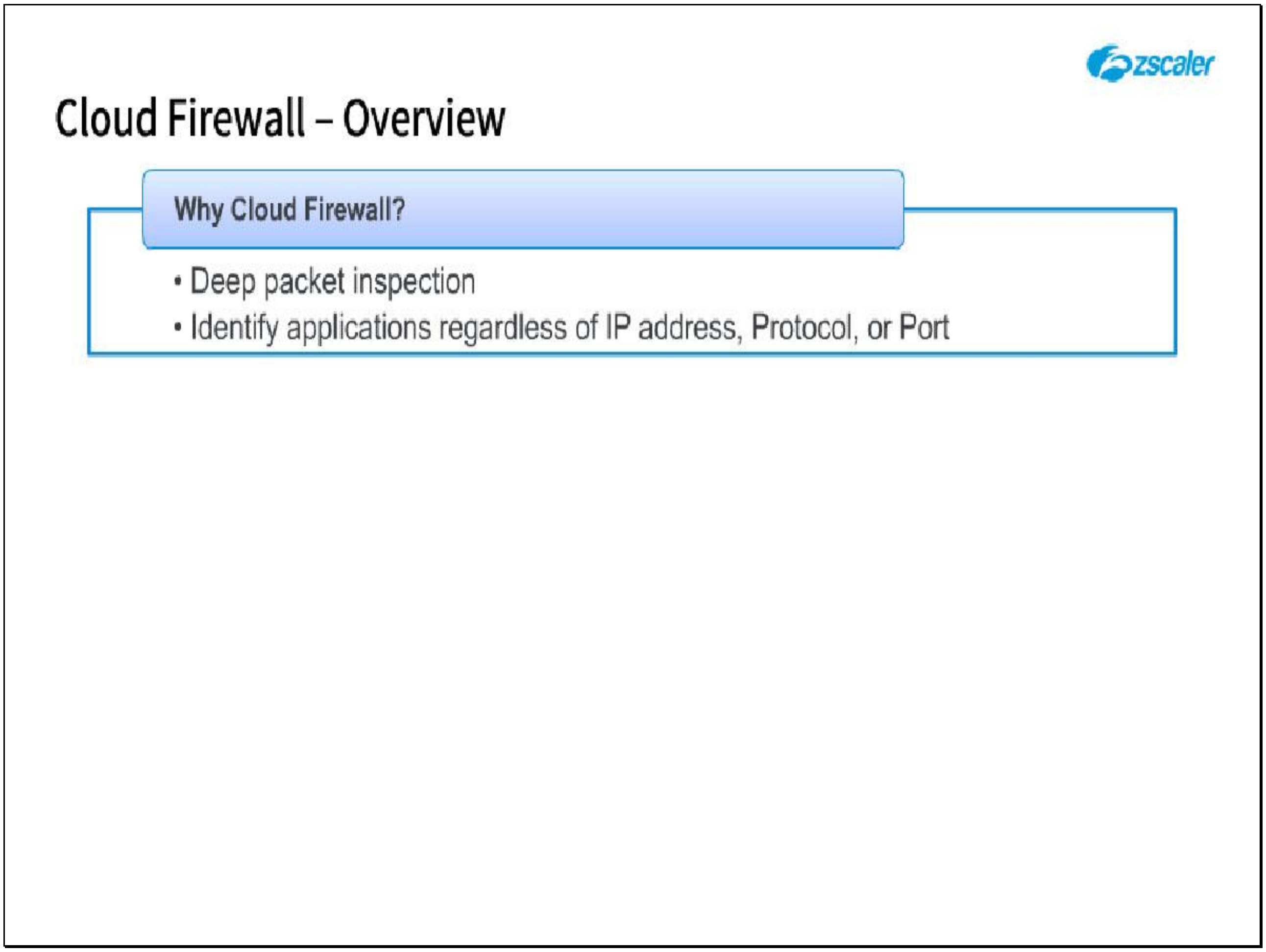
Slide 26 - Next Generation Firewall Overview

Cloud Firewall Overview

Slide notes

The final topic we will cover is an overview of the Zscaler Cloud Firewall.

Slide 27 - Next Generation Firewall Overview



Cloud Firewall – Overview

Why Cloud Firewall?

- Deep packet inspection
- Identify applications regardless of IP address, Protocol, or Port

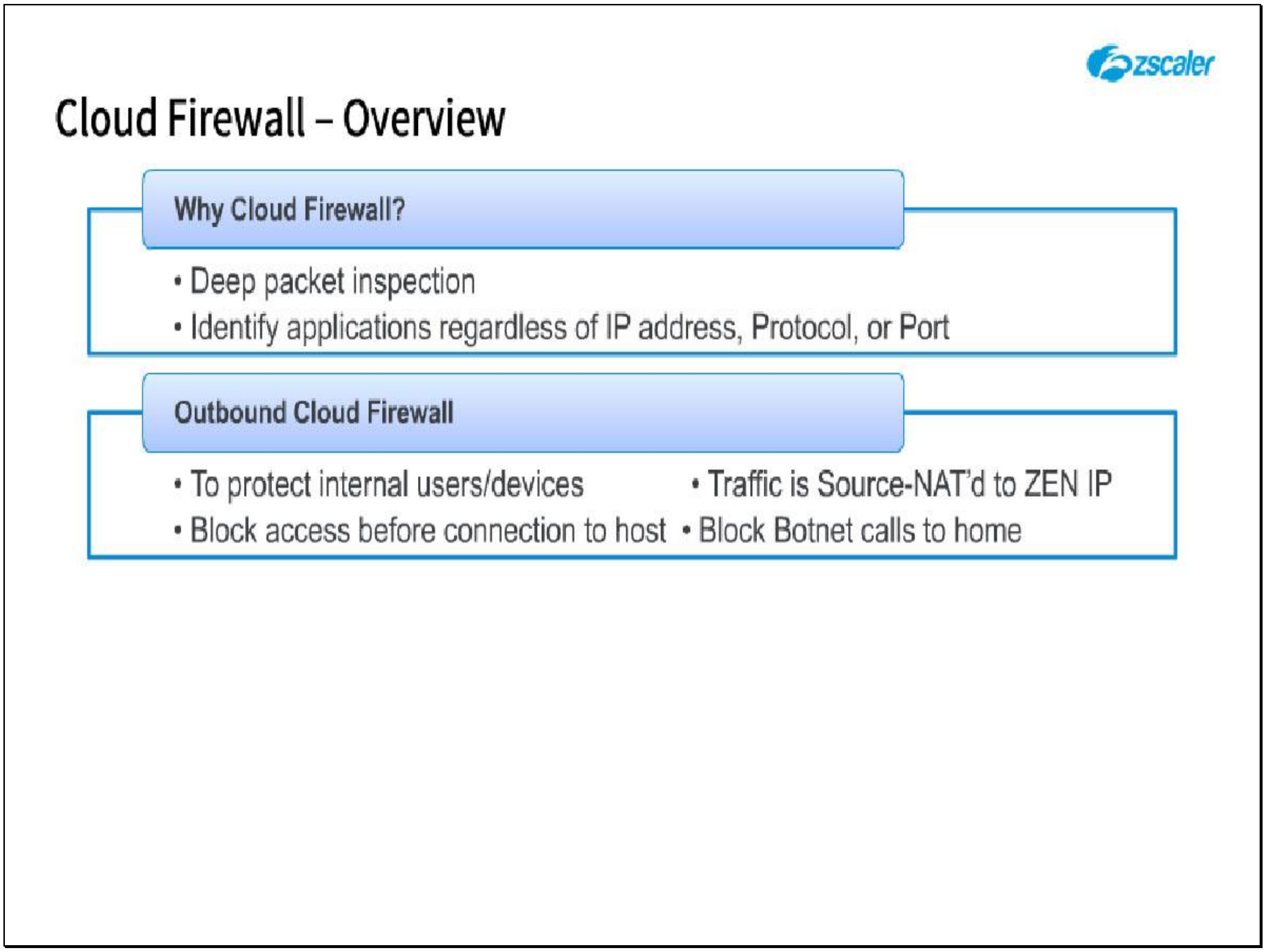
Slide notes

A traditional firewall allows you to write policies based on 5 tuples: Source IP, Destination IP, Protocol, Source Port, and Destination Port. However, in today's world of dynamic IP addresses and TCP/UDP ports, where applications like Skype or BitTorrent will use any available port to send traffic to a multitude of destinations, this approach simply doesn't work.

In contrast, Zscaler's Cloud Firewall uses deep packet inspection to identify applications regardless of IP address, port, or protocol. You can then combine this application-centric view of traffic with Zscaler's knowledge of your locations, users, and groups to write policies granting users, or groups of users access to the applications they need. The days of needing to look up which applications use which TCP and UDP ports are at an end.

This includes support for the QUIC and PPTP protocols, as well as better detection for Skype for Business (SfB) on both UDP and TCP, thanks to the synchronization we do with the Microsoft published IPs and ports for SfB.

Slide 28 - Next Generation Firewall Overview



Cloud Firewall – Overview

Why Cloud Firewall?

- Deep packet inspection
- Identify applications regardless of IP address, Protocol, or Port

Outbound Cloud Firewall

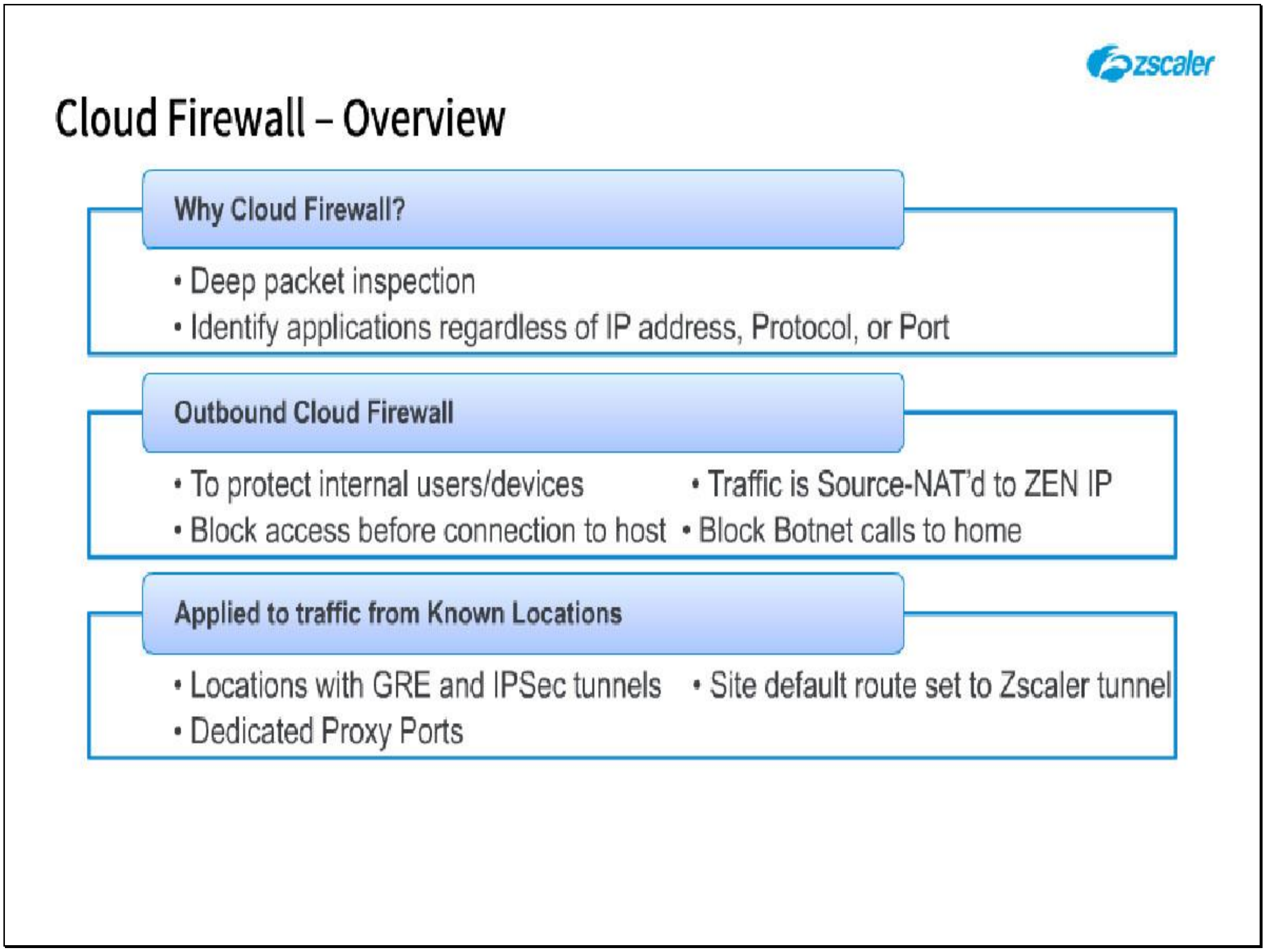
- To protect internal users/devices
- Block access before connection to host
- Traffic is Source-NAT'd to ZEN IP
- Block Botnet calls to home

Slide notes

Zscaler's Cloud Firewall allows you to protect and manage your organization's outbound Internet access against application-based threats across your entire distributed enterprise. This means that policies you write are based on connections or applications being initiated from inside your networks by your own users and devices. Any connections initiated from outside your networks will be blocked.

Further, all traffic will be Source-NAT'd to the IP address of the ZEN through which the traffic is flowing. With the Zscaler Cloud Firewall inspecting your outbound traffic, connections across the Internet to known malware sources are blocked, this includes botnet calls home meaning that the botnet malware will never be activated.

Slide 29 - Next Generation Firewall Overview



Cloud Firewall – Overview

Why Cloud Firewall?

- Deep packet inspection
- Identify applications regardless of IP address, Protocol, or Port

Outbound Cloud Firewall

- To protect internal users/devices
- Block access before connection to host
- Traffic is Source-NAT'd to ZEN IP
- Block Botnet calls to home

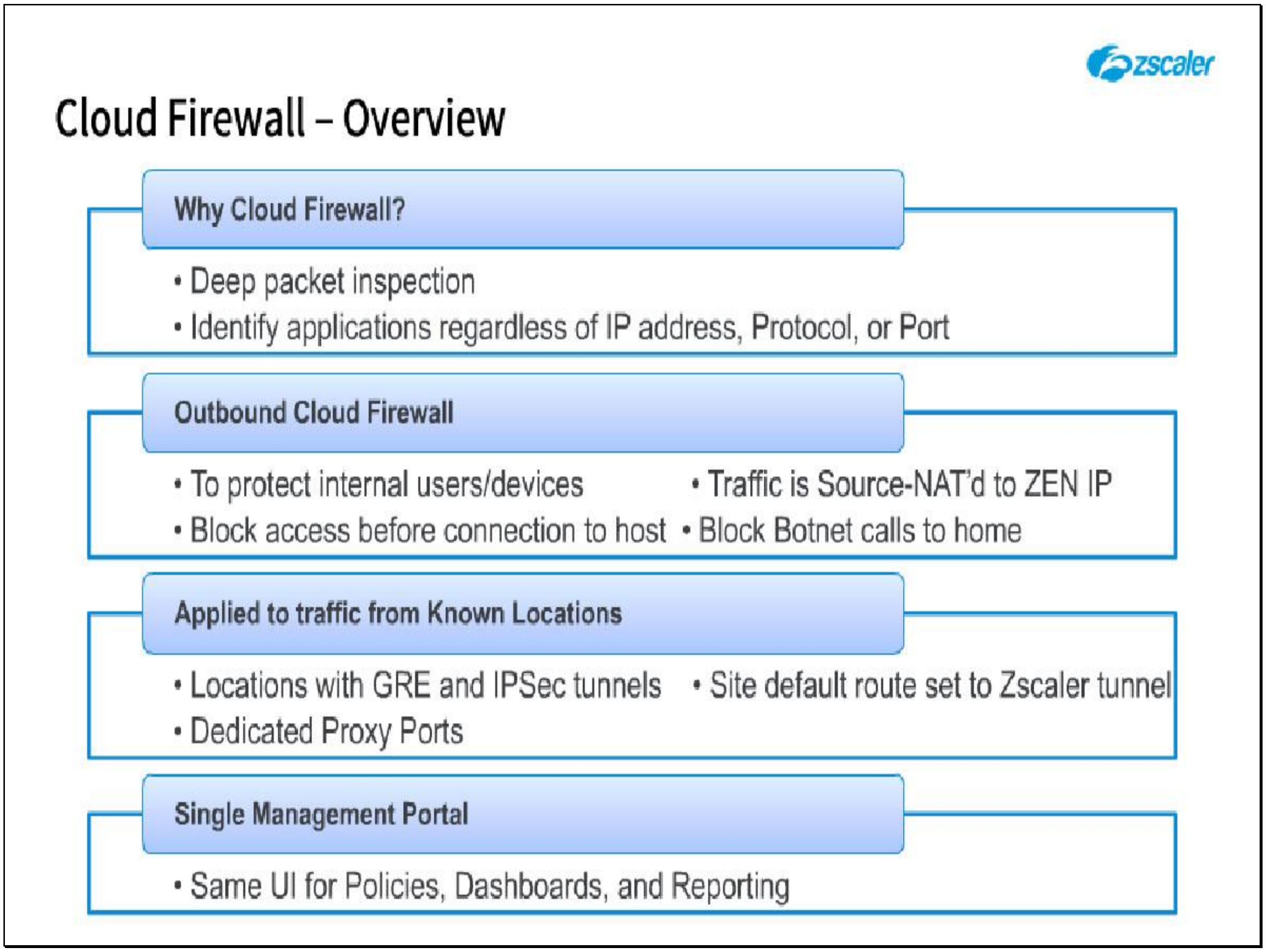
Applied to traffic from Known Locations

- Locations with GRE and IPSec tunnels
- Dedicated Proxy Ports
- Site default route set to Zscaler tunnel

Slide notes

Zscaler's Cloud Firewall is applied to traffic from known Locations. These are locations with a GRE or IPSec tunnel into Zscaler. With the addition of the Cloud Firewall, you can now simply set the site's default route to Zscaler and send all internet-bound traffic to Zscaler. Note that the Firewall can be enabled for your Dedicated Proxy Port users as well.

Slide 30 - Next Generation Firewall Overview



zscaler

Cloud Firewall – Overview

Why Cloud Firewall?

- Deep packet inspection
- Identify applications regardless of IP address, Protocol, or Port

Outbound Cloud Firewall

- To protect internal users/devices
- Block access before connection to host
- Traffic is Source-NAT'd to ZEN IP
- Block Botnet calls to home

Applied to traffic from Known Locations

- Locations with GRE and IPSec tunnels
- Dedicated Proxy Ports
- Site default route set to Zscaler tunnel

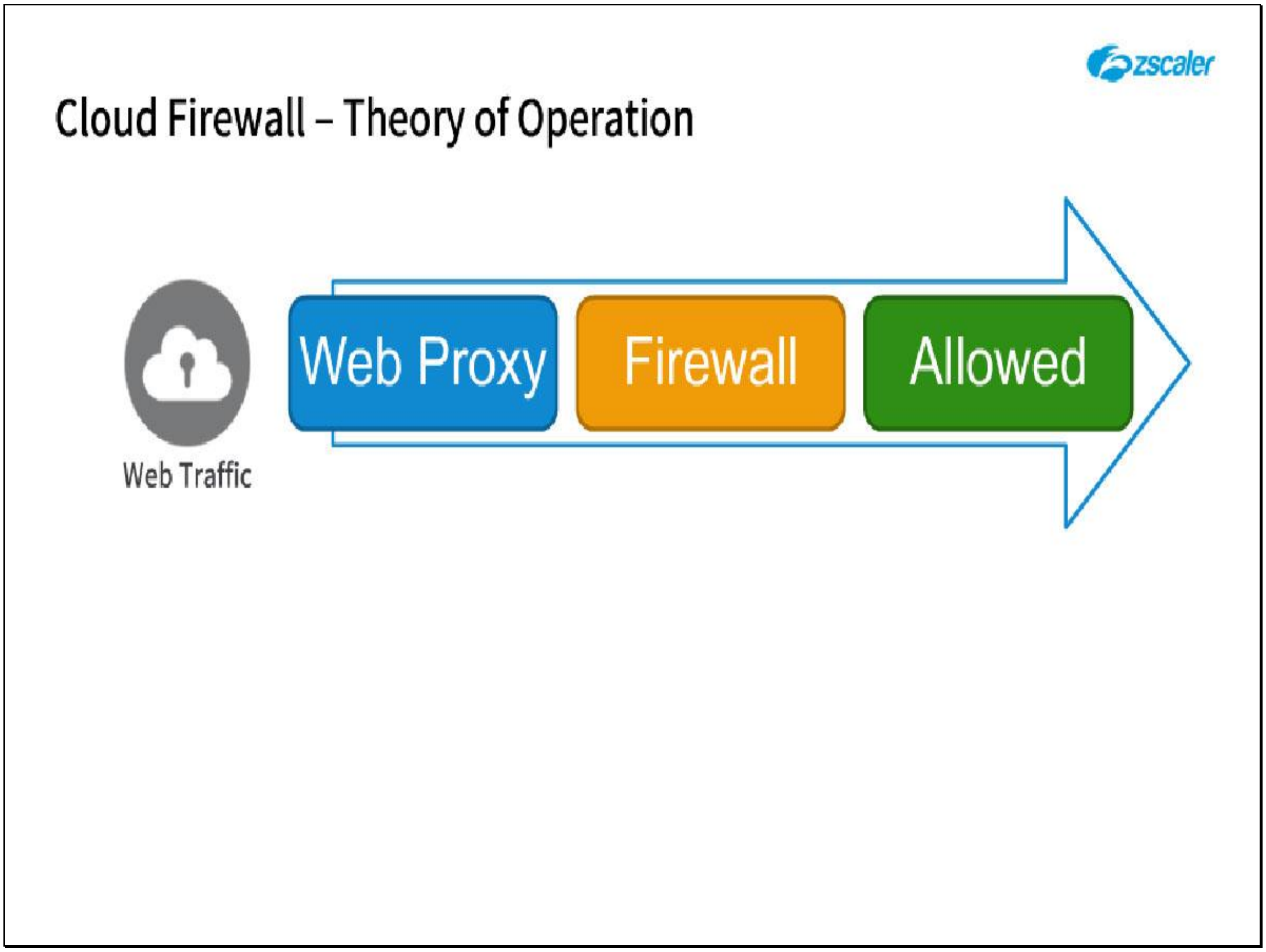
Single Management Portal

- Same UI for Policies, Dashboards, and Reporting

Slide notes

Finally, Zscaler's Cloud Firewall offers a single, unified user interface for creating and managing policies, dashboards, and reporting.

Slide 31 - Theory of Operation



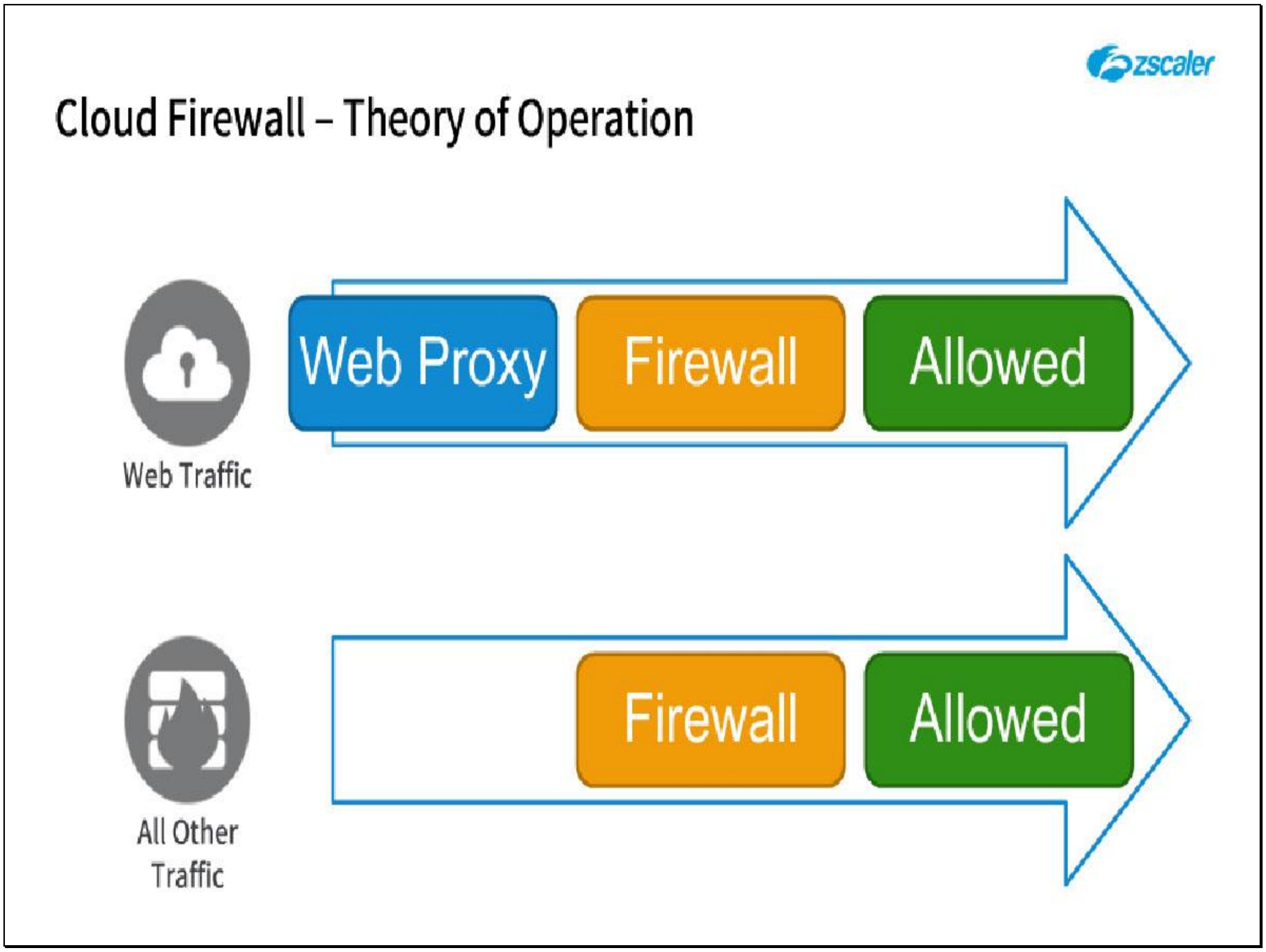
Cloud Firewall – Theory of Operation

Slide notes

When traffic arrives at the ZEN, Web traffic (usually on ports 80 and 443) is sent to the Web Proxy for security and policy checks. If allowed by the **URL & Cloud App Control Policy**, this traffic is also evaluated by the Cloud Firewall. Policy rules are applied top-down, with first-match, and a default **Allow All** at the end.

This means that Web traffic must be permitted by both modules in order to pass through the ZEN.

Slide 32 - Theory of Operation



zscaler

Cloud Firewall – Theory of Operation

Web Traffic

Web Proxy

Firewall

Allowed

All Other Traffic

Firewall

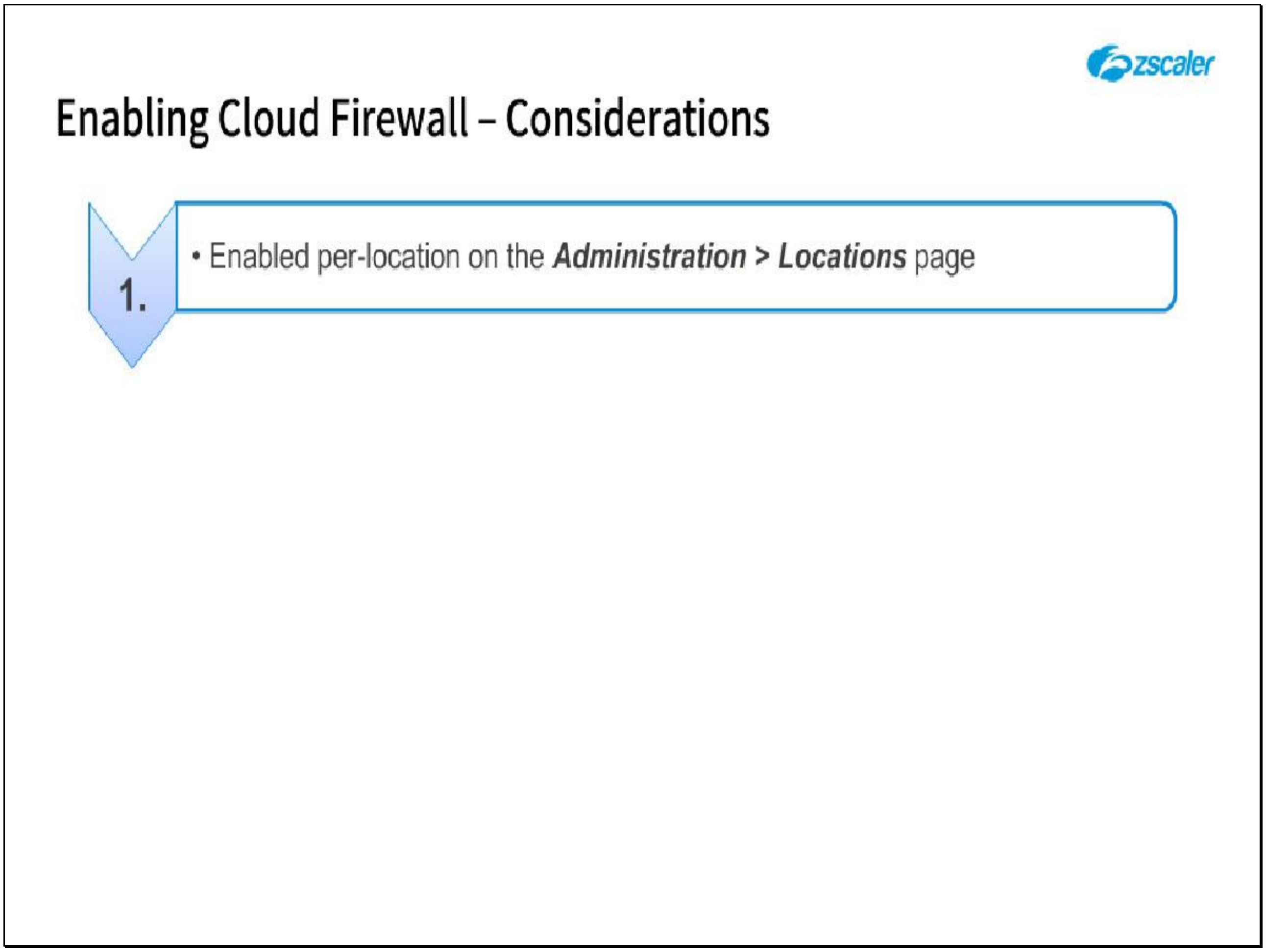
Allowed

Slide notes

Non-Web traffic is sent through the Cloud Firewall only. As with the Web proxy, rules are applied top-down, first match, with a default **Allow All** rule at the end. This decision was made so if an administrator enables the Firewall on a location traffic would continue to flow, even if no rules had been created.

A Zscaler best practice is to create a rule allowing DNS, HTTP, and HTTPS protocols, and then change the Default rule to **Block**. You would then create additional rules to permit the specific applications that you need.

Slide 33 - Enabling Next Generation Firewall



zscaler

Enabling Cloud Firewall – Considerations

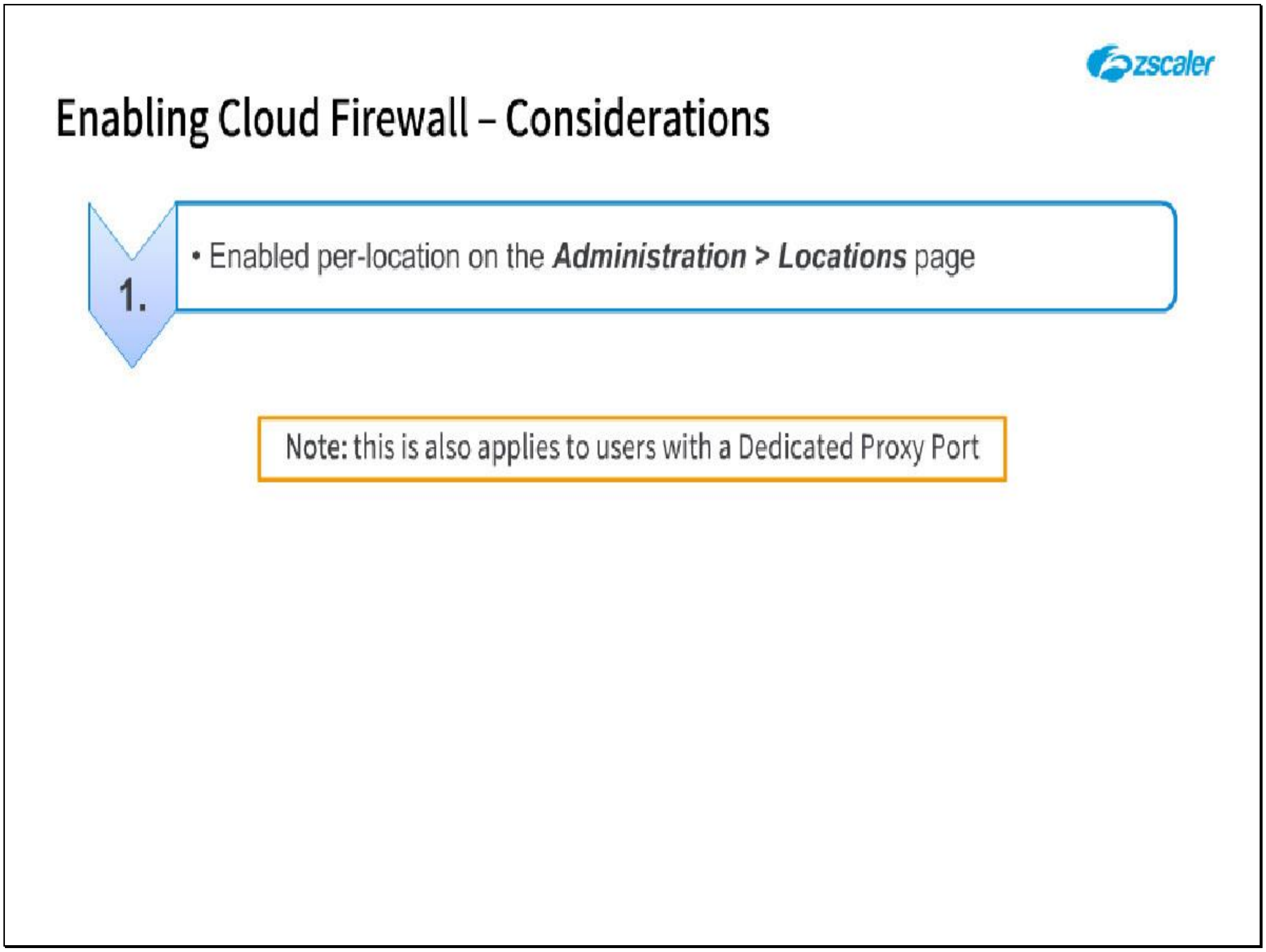
1.

- Enabled per-location on the ***Administration > Locations*** page

Slide notes

The Zscaler Cloud Firewall is enabled on a per-location basis, this is done on the **Locations** page under the **Administration** menu.

Slide 34 - Enabling Next Generation Firewall – Considerations



Enabling Cloud Firewall – Considerations

1.

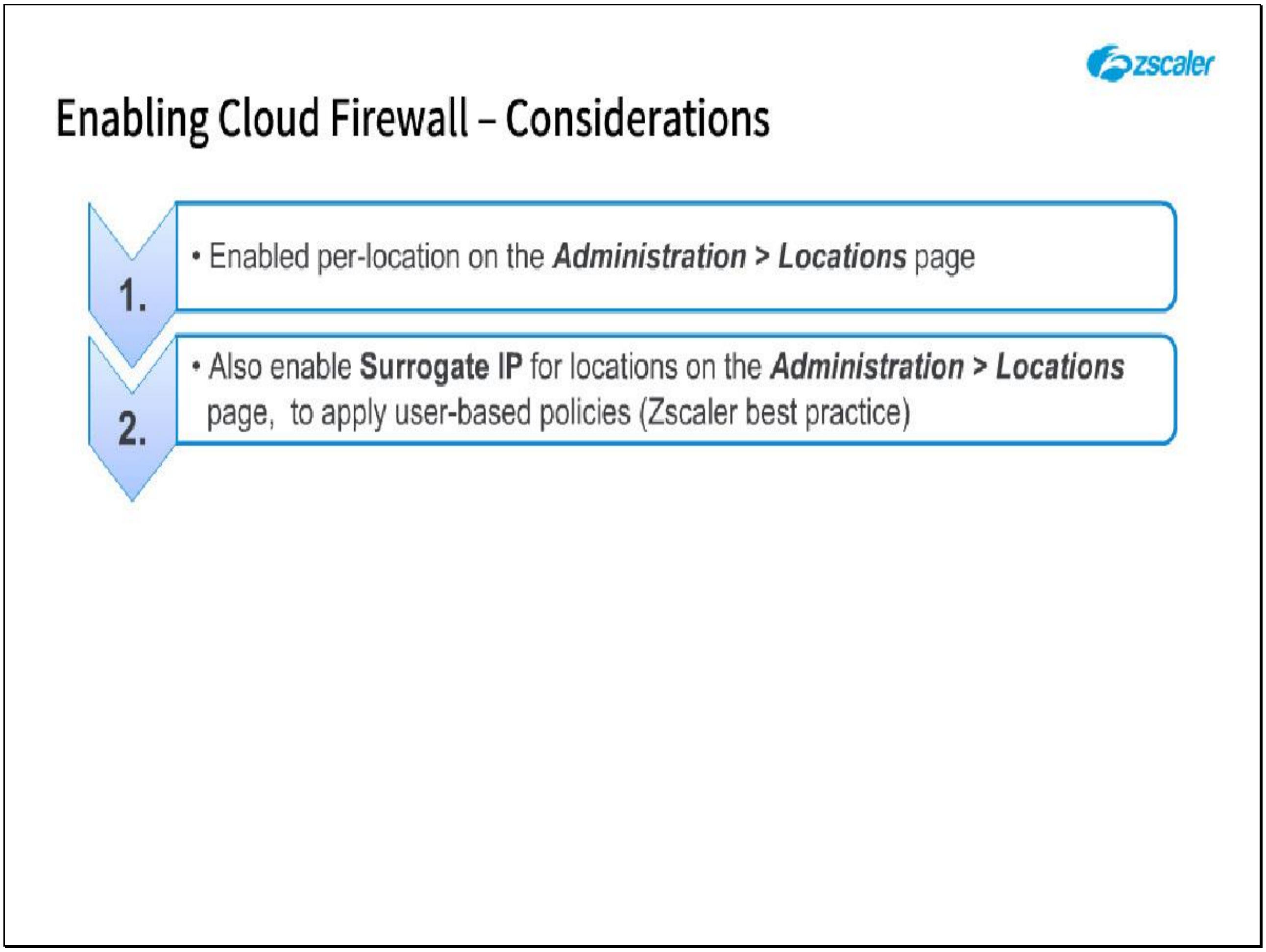
- Enabled per-location on the ***Administration > Locations*** page

Note: this is also applies to users with a Dedicated Proxy Port

Slide notes

Note, this is also where you go to enable the Firewall for Dedicated Proxy Ports.

Slide 35 - Enabling Next Generation Firewall



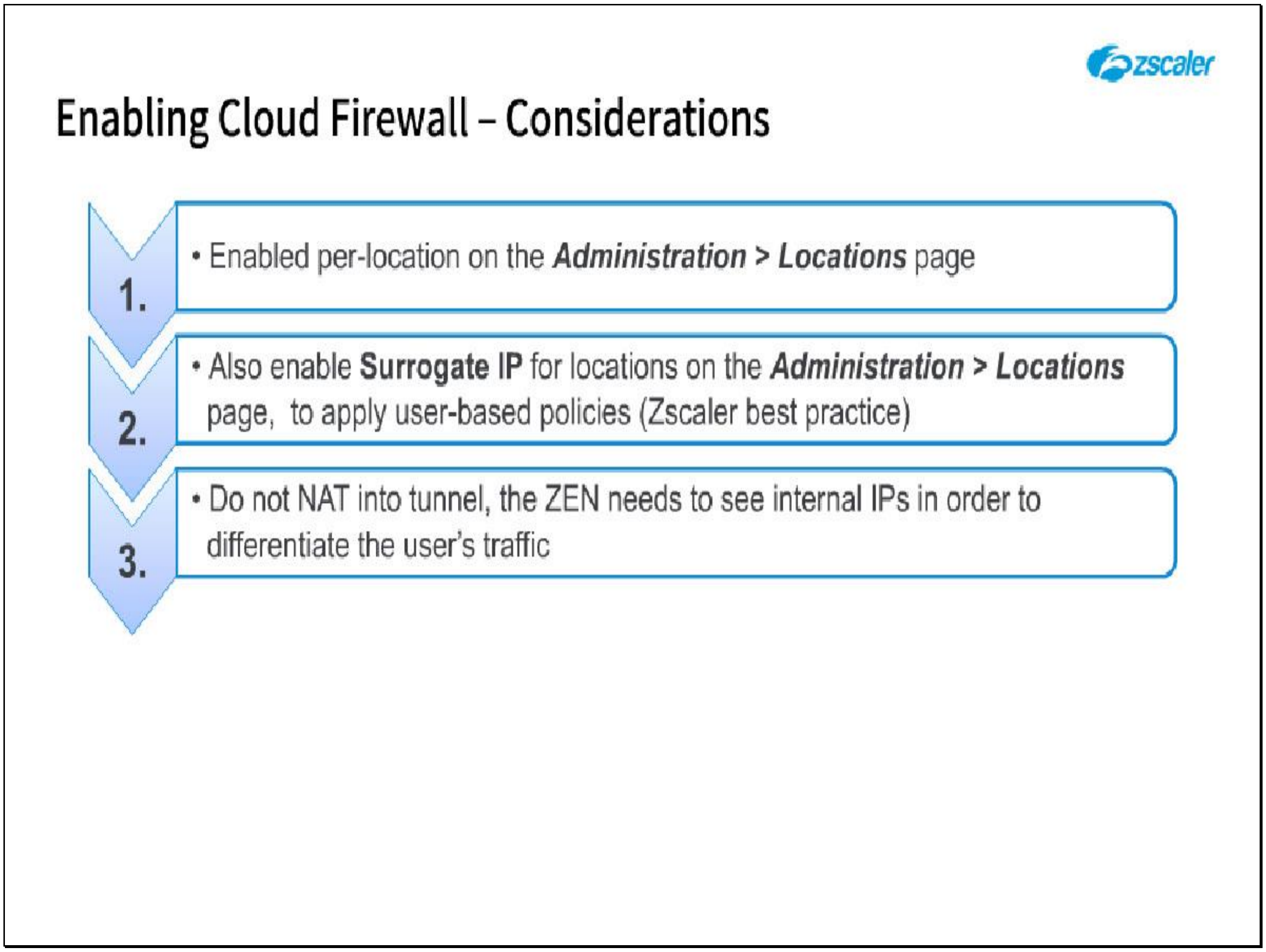
Enabling Cloud Firewall – Considerations

1. • Enabled per-location on the ***Administration > Locations*** page
2. • Also enable **Surrogate IP** for locations on the ***Administration > Locations*** page, to apply user-based policies (Zscaler best practice)

Slide notes

It is also recommended that you enable the **Surrogate IP** option on a per-location basis, which is also done from the **Locations** Page under the **Administration** menu. This feature maps IP addresses to users so that the system can apply user-based firewall policies.

Slide 36 - Enabling Next Generation Firewall



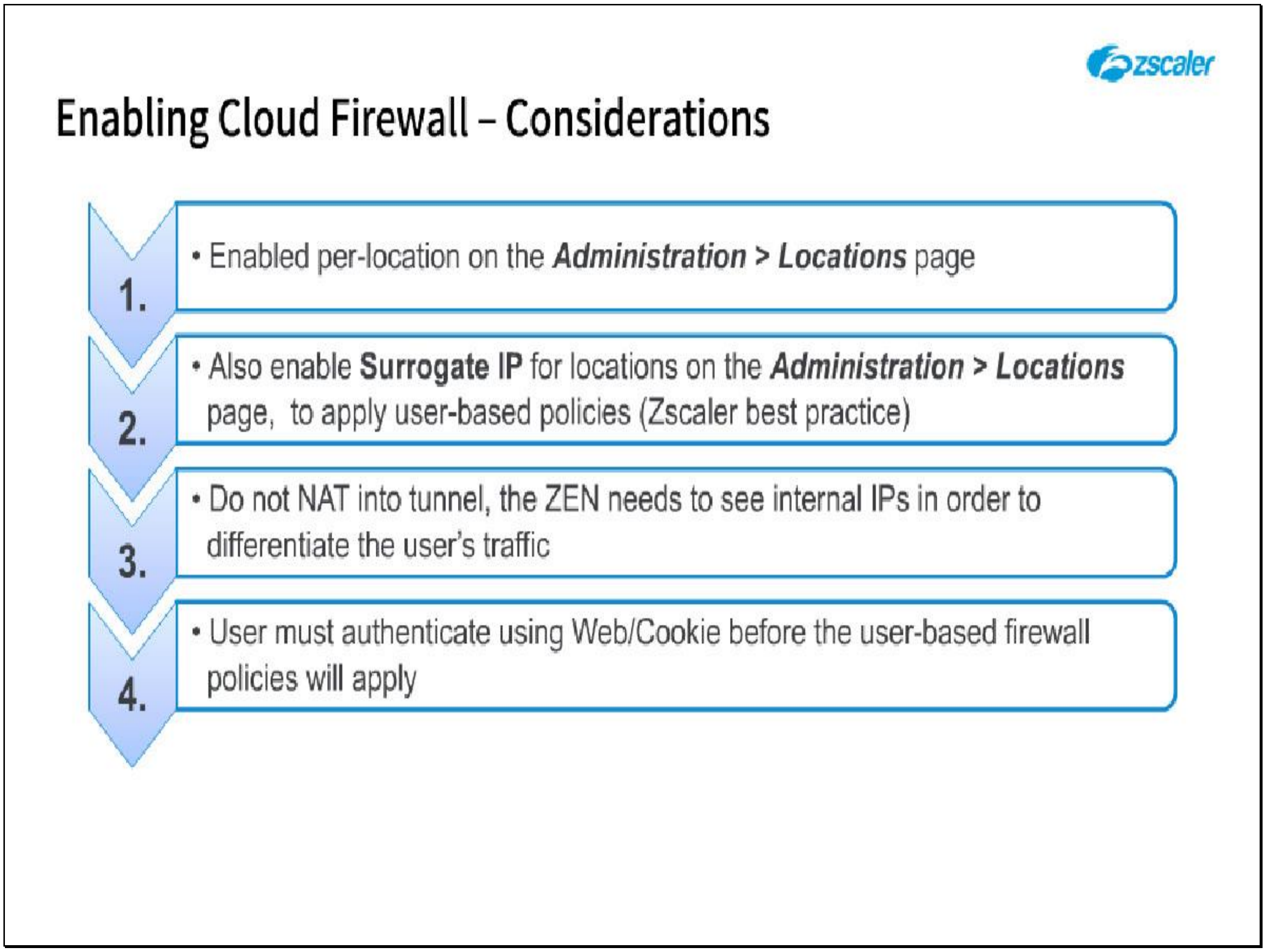
Enabling Cloud Firewall – Considerations

1. • Enabled per-location on the ***Administration > Locations*** page
2. • Also enable **Surrogate IP** for locations on the ***Administration > Locations*** page, to apply user-based policies (Zscaler best practice)
3. • Do not NAT into tunnel, the ZEN needs to see internal IPs in order to differentiate the user's traffic

Slide notes

It is recommended that you do not NAT traffic into the GRE or IPSec tunnels, as this would cause all users to have the same source IP address coming into the ZEN, and Zscaler would have no way to differentiate traffic from different users.

Slide 37 - Enabling Next Generation Firewall



Enabling Cloud Firewall – Considerations

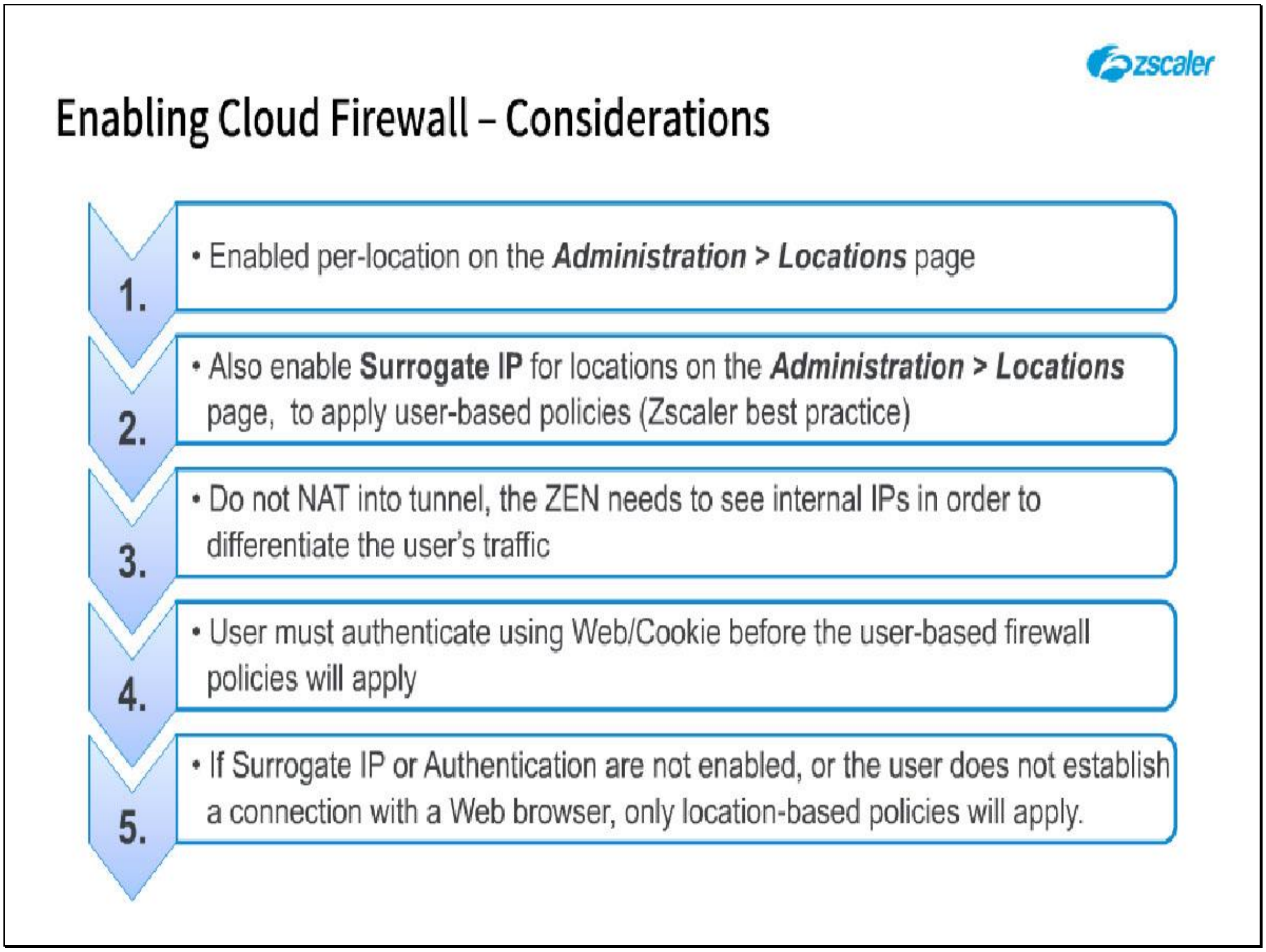
1. • Enabled per-location on the ***Administration > Locations*** page
2. • Also enable **Surrogate IP** for locations on the ***Administration > Locations*** page, to apply user-based policies (Zscaler best practice)
3. • Do not NAT into tunnel, the ZEN needs to see internal IPs in order to differentiate the user's traffic
4. • User must authenticate using Web/Cookie before the user-based firewall policies will apply

Slide notes

There is also a caveat if you want to apply user-based Firewall policies. While the HTTP protocol has provisions for authenticating users to a proxy, other applications going through the Firewall do not. Think of an instant messaging app, or streaming music or movies from a dedicated app like iTunes. There is no way for the ZEN to prompt the user to authenticate in order to apply user-based policies like there is with a Web browser.

So, in this case, a user must first authenticate to the ZEN through a Web browser in order to establish a user identity. With the surrogate IP feature mentioned above, the ZEN then temporarily maps the user's IP address to the user and can apply both user and location-based policies to the user's traffic.

Slide 38 - Enabling Next Generation Firewall



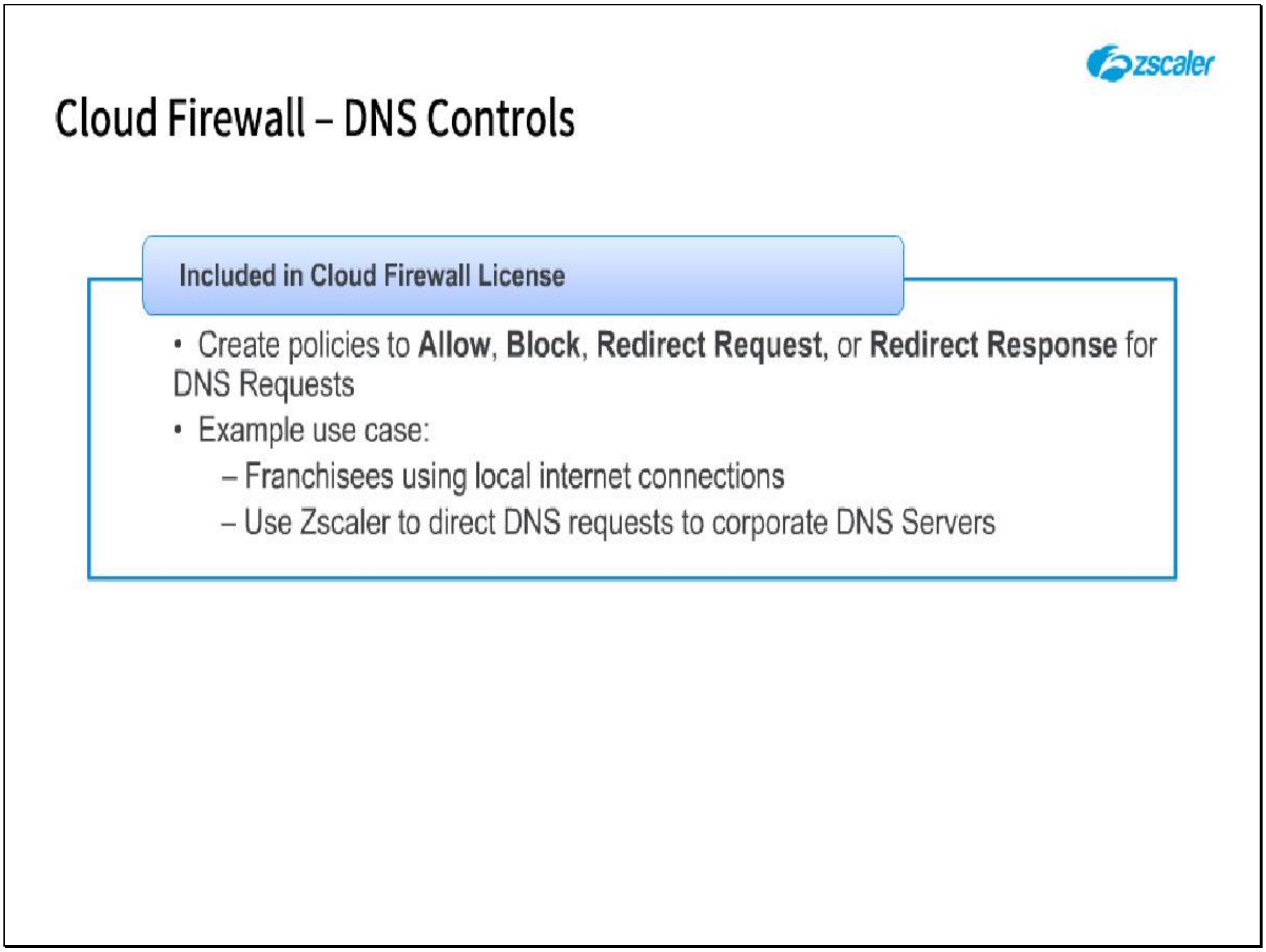
Enabling Cloud Firewall – Considerations

1. • Enabled per-location on the ***Administration > Locations*** page
2. • Also enable **Surrogate IP** for locations on the ***Administration > Locations*** page, to apply user-based policies (Zscaler best practice)
3. • Do not NAT into tunnel, the ZEN needs to see internal IPs in order to differentiate the user's traffic
4. • User must authenticate using Web/Cookie before the user-based firewall policies will apply
5. • If Surrogate IP or Authentication are not enabled, or the user does not establish a connection with a Web browser, only location-based policies will apply.

Slide notes

If Surrogate IP and authentication are not enabled, or the user does not first establish a connection with a Web browser, then only location-based policies can be applied.

Slide 39 - DNS Controls



Cloud Firewall – DNS Controls

Included in Cloud Firewall License

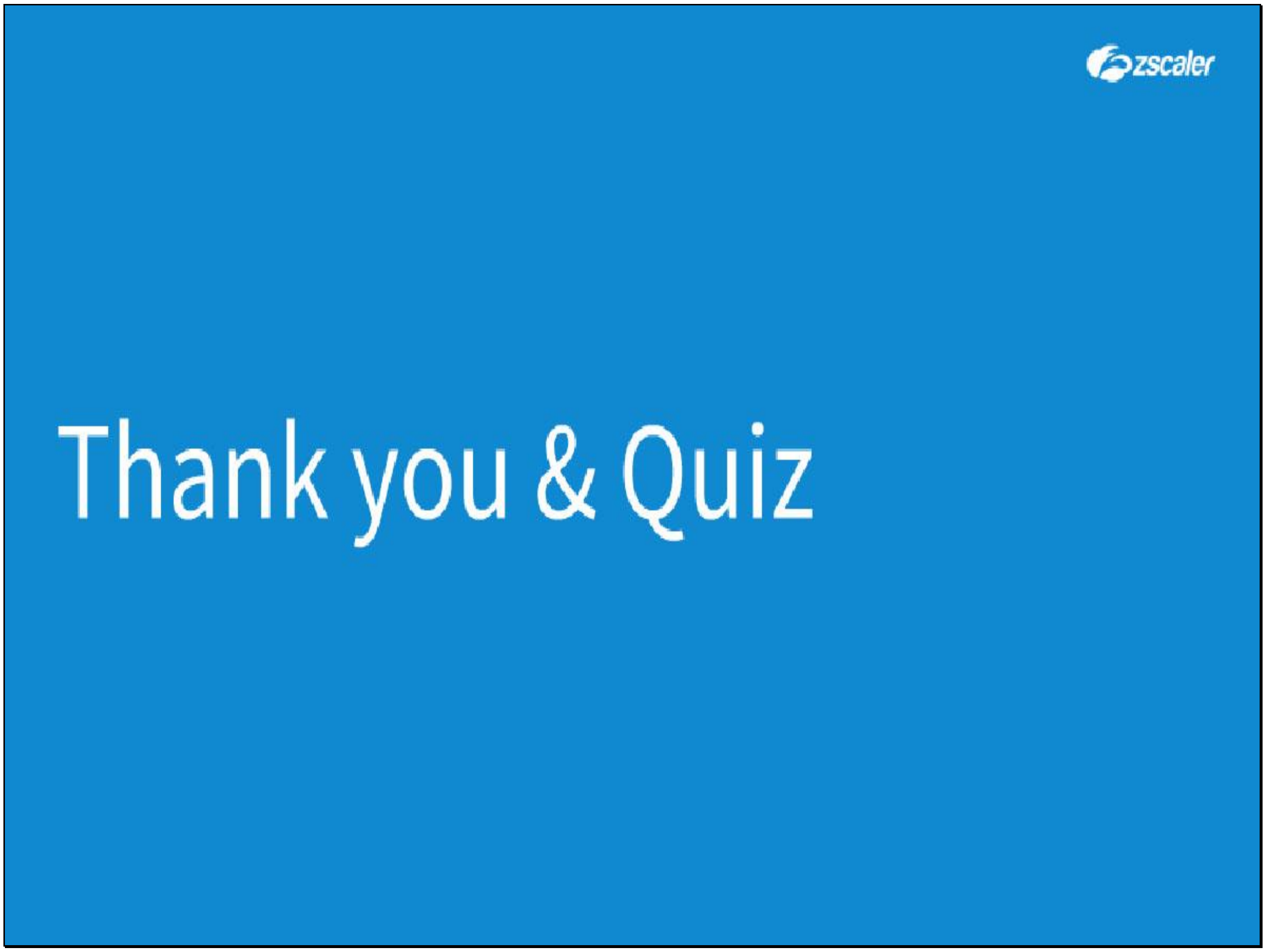
- Create policies to **Allow**, **Block**, **Redirect Request**, or **Redirect Response** for DNS Requests
- Example use case:
  - Franchisees using local internet connections
  - Use Zscaler to direct DNS requests to corporate DNS Servers

Slide notes

The **DNS Controls** page allow you to control how DNS traffic is handled between your users and the Internet. You can create policies to **Allow**, **Block**, **Redirect Request**, or **Redirect Response** for DNS requests.

One example use case is a company that has franchisees that are not under direct control of the company. These franchisees buy local commodity internet service to access resources back at corporate. For security reasons, it would be a good idea to make sure that DNS requests for corporate resources are not subject to DNS hijacking or poisoning. One way to prevent this would be to redirect all DNS requests for corporate resources to use corporate DNS servers instead of the local ISP.

Slide 40 - 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.