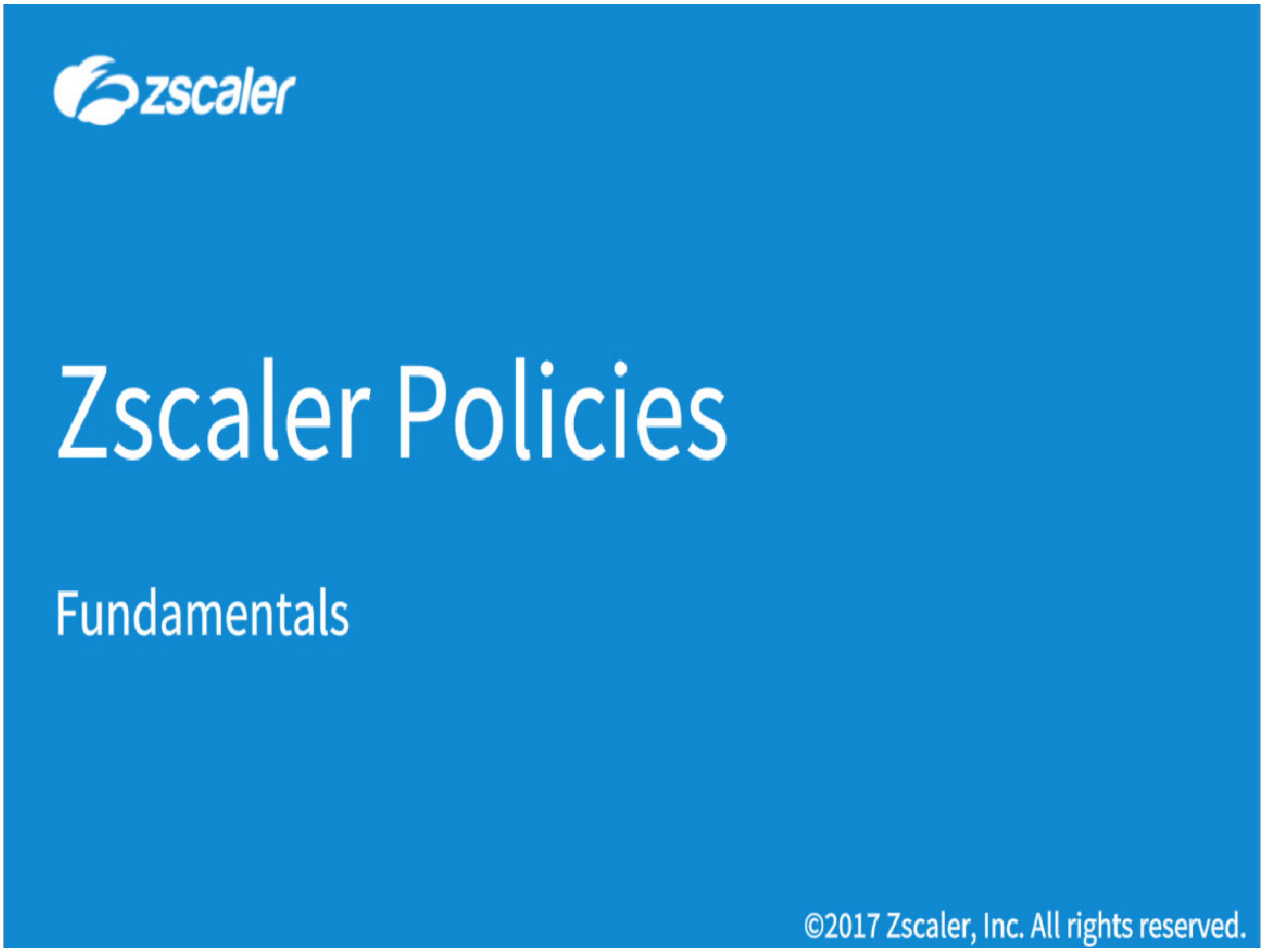
Slide 1 - Zscaler Policies



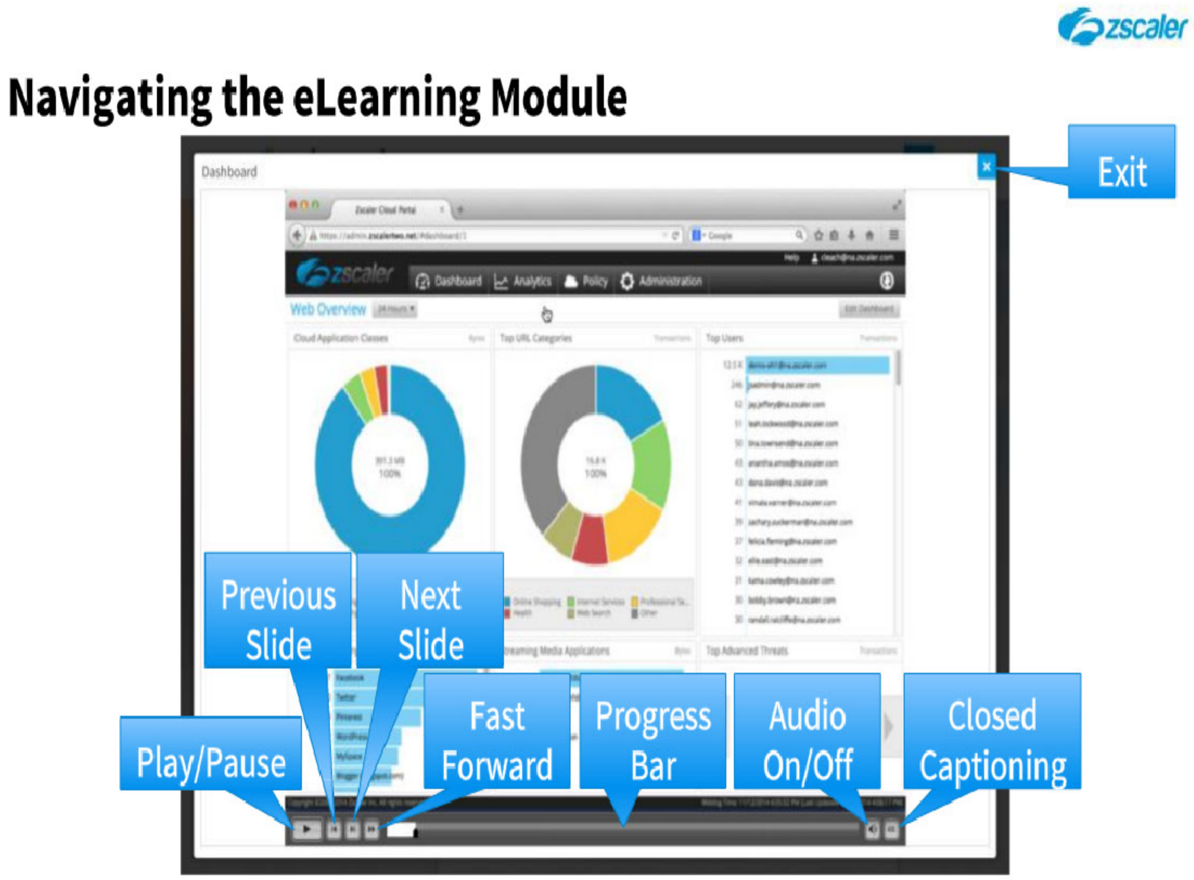
Zscaler Policies

Fundamentals

Slide notes

Welcome to the Zscaler Policy Fundamentals 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

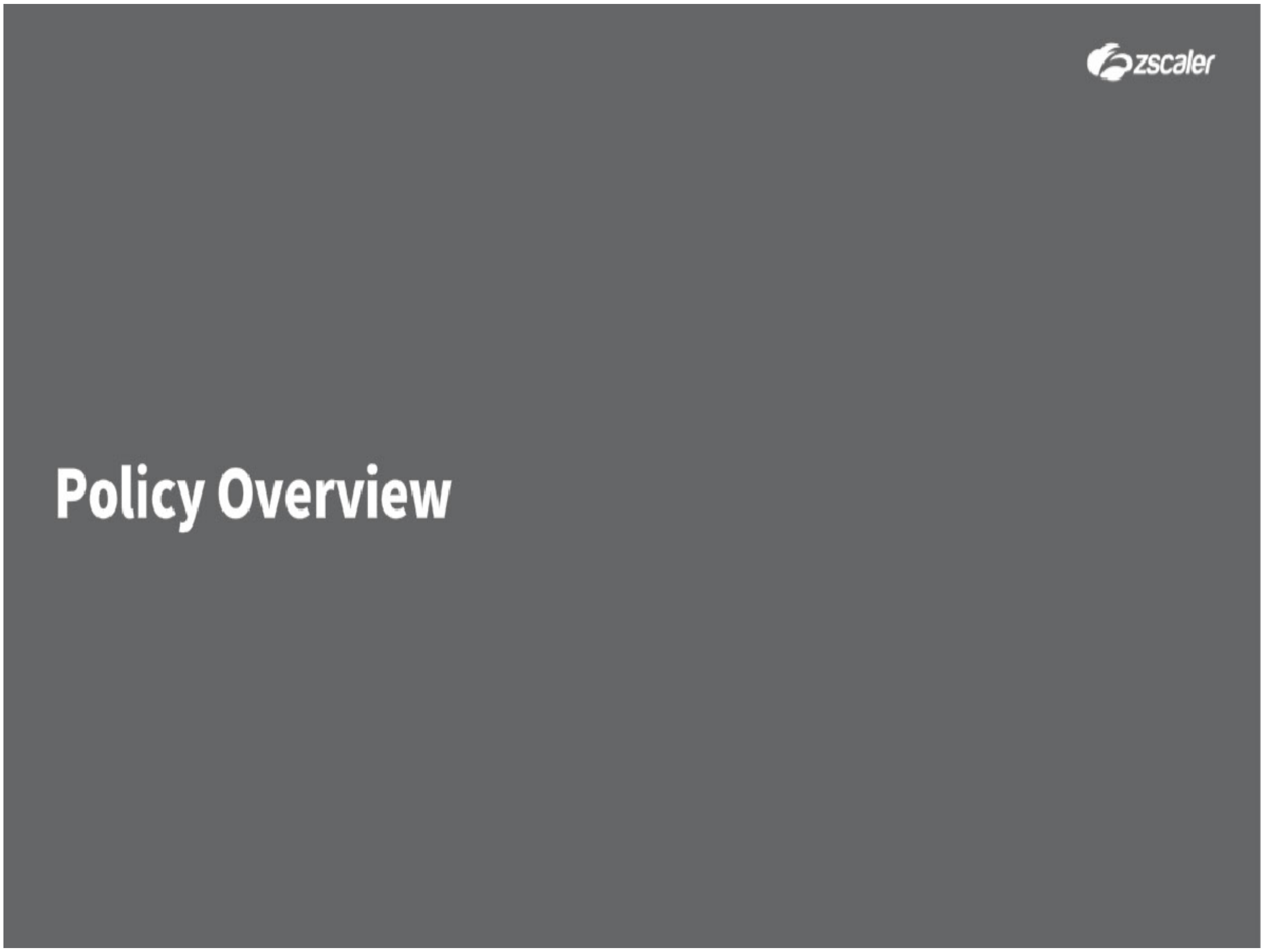
Agenda

- Policy Overview
- Policy Key Concepts

Slide notes

In this module, we will cover an overview of the Zscaler Policy capabilities and some Policy key concepts.

Slide 4 - Policy Overview

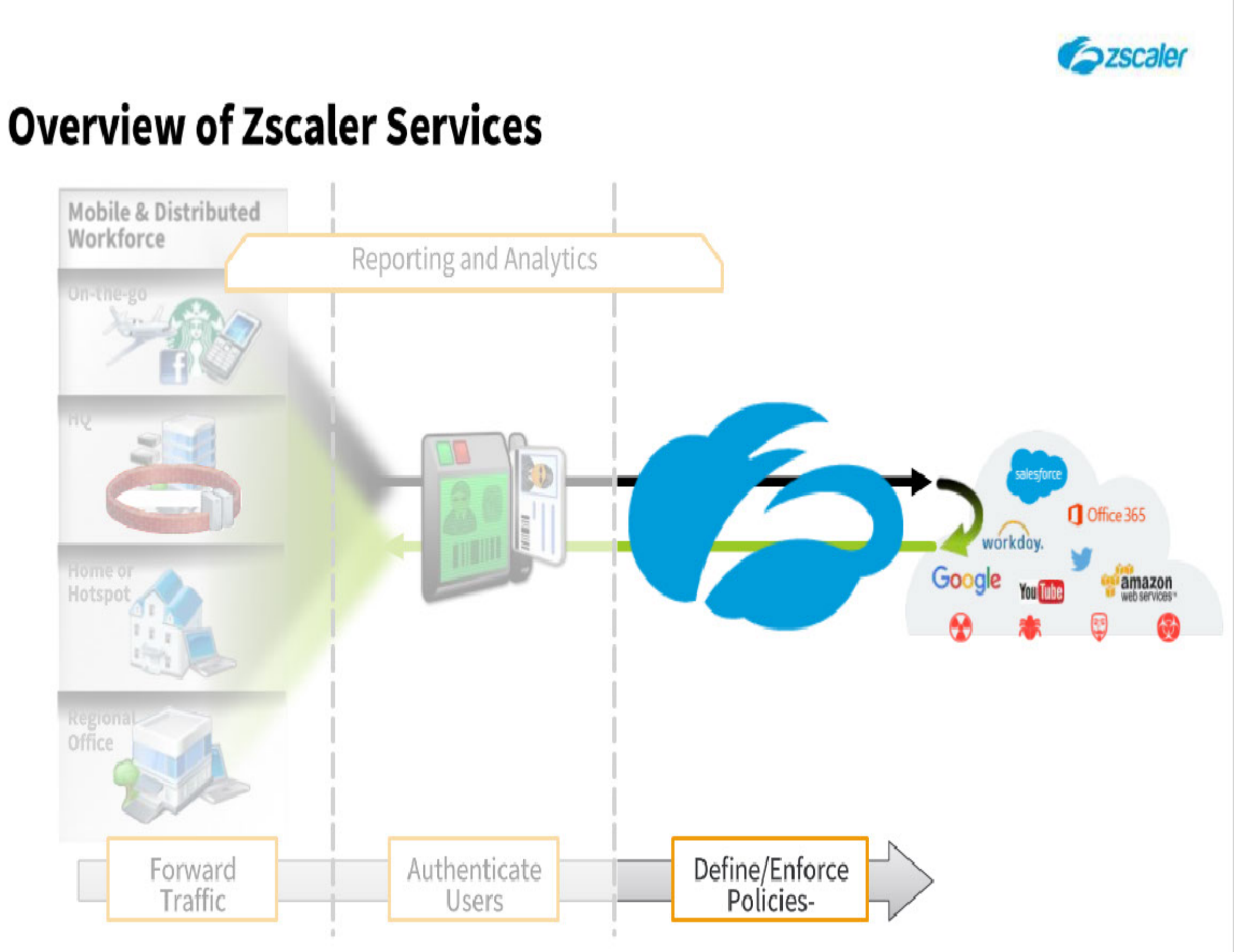


Policy Overview

Slide notes

The first topic we will cover is an overview of the Zscaler Policy capabilities.

Slide 5 - Overview of Zscaler Services



Overview of Zscaler Services

Mobile & Distributed Workforce

Reporting and Analytics

Forward Traffic

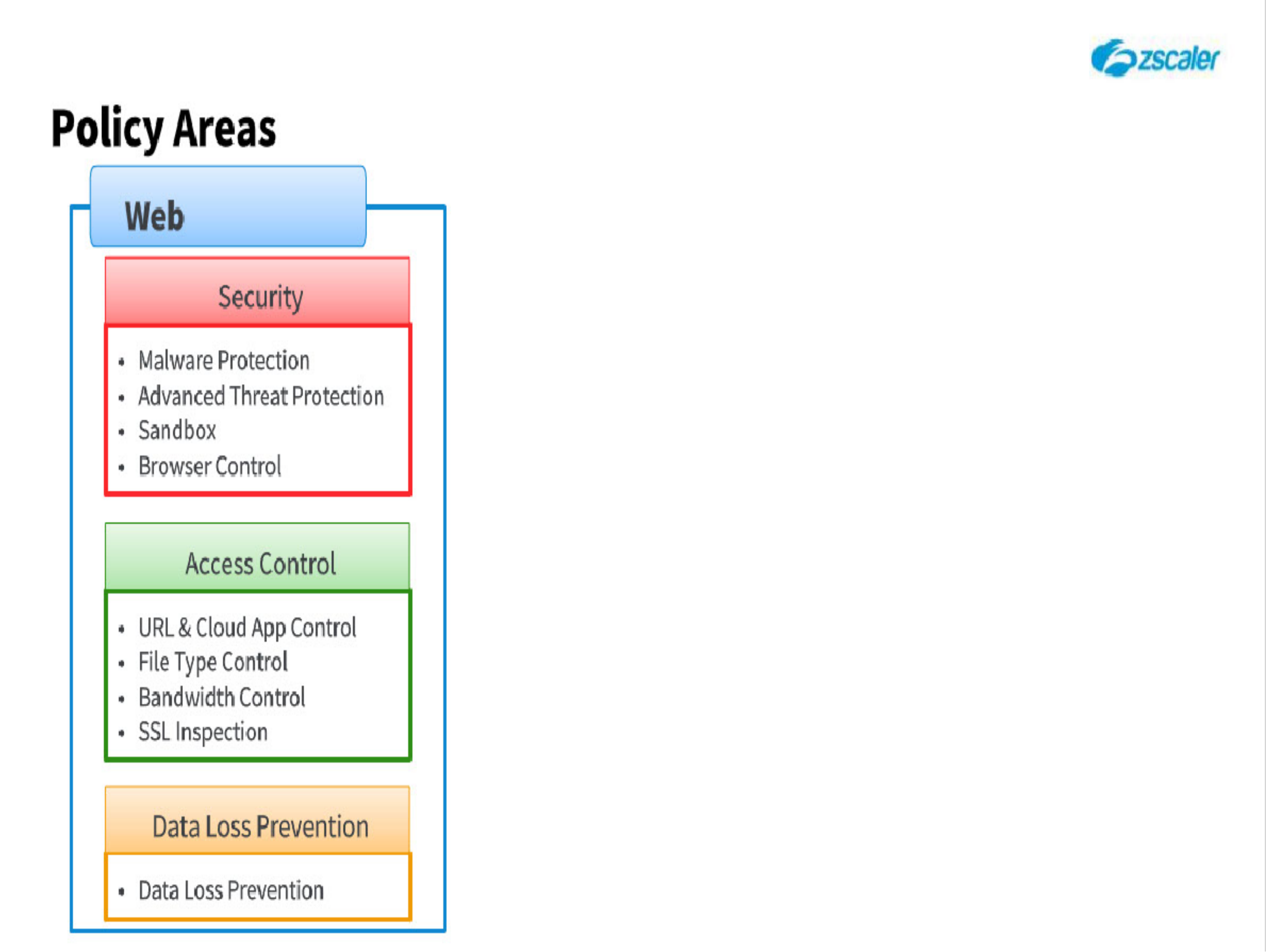
Authenticate Users

Define/Enforce Policies-

Slide notes

In this module we will focus on the Zscaler capabilities for defining and enforcing Policies for the traffic forwarded from locations and users. The Policy section of the admin portal is the real meat of the Zscaler service, this is where you define what access your users have, and how you protect your users and networks.

Slide 6 - Policy Areas



Policy Areas

Web

Security

- Malware Protection
- Advanced Threat Protection
- Sandbox
- Browser Control

Access Control

- URL & Cloud App Control
- File Type Control
- Bandwidth Control
- SSL Inspection

Data Loss Prevention

- Data Loss Prevention

Slide notes

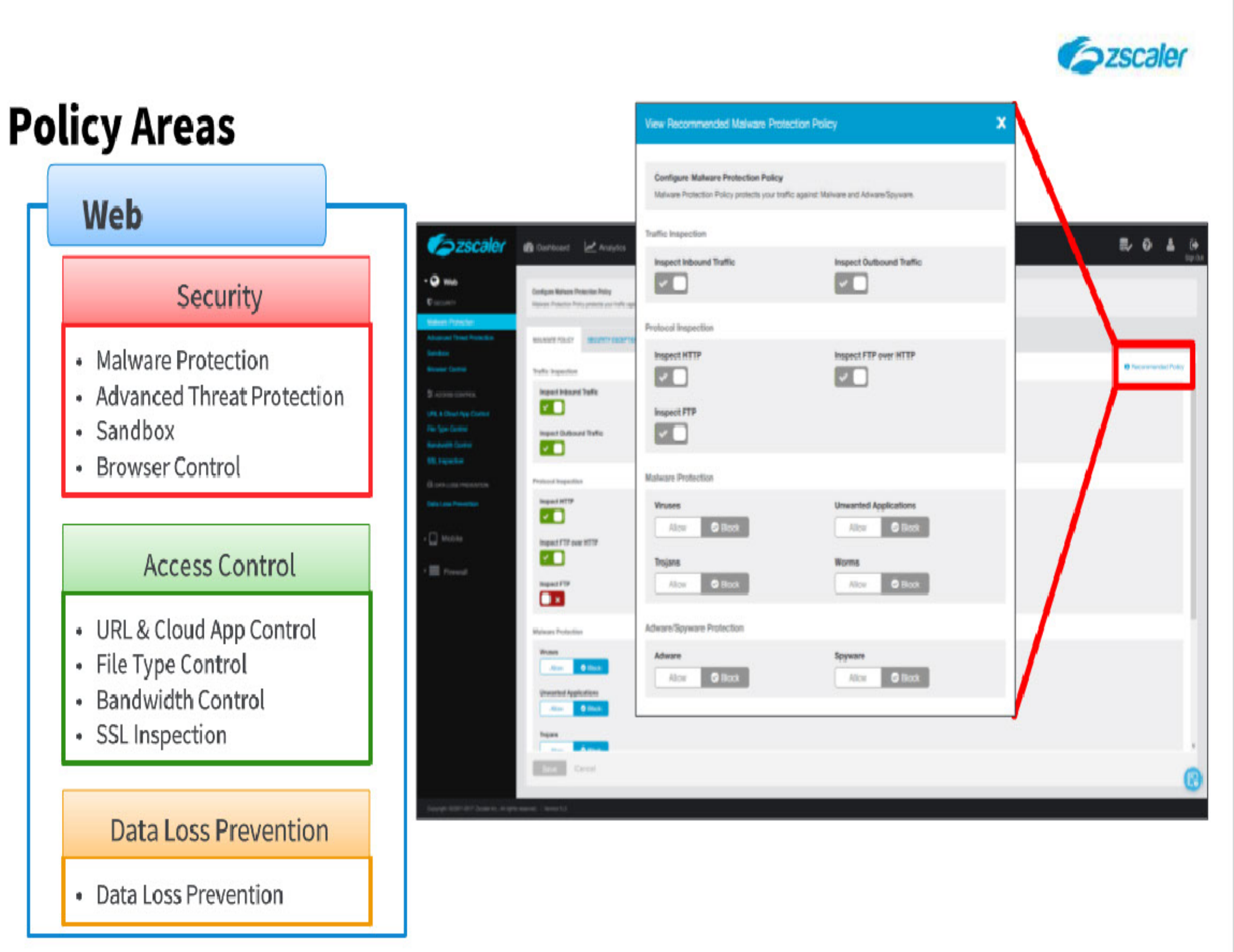
The Policy configuration area can be found by clicking on the **Policy** menu in the admin portal, the **Policy** menu is then broken down into the **Web**, **Mobile**, and **Firewall** areas. The **Web** policy area is the most extensive and allows the creation of **Security**, **Access Control**, and **Data Loss Prevention** policies.

The **Security** policies available to be configured are: **Malware Protection**, for configuring protection from viruses, Trojans, Worms, Adware, Spyware and other unwanted applications; **Advanced Threat Protection** (ATP), to detect and block malicious activity, spyware call-backs, or command and control traffic (CC); **Sandbox**, that allows the quarantining of suspect files for scanning in a protected sandbox environment; and **Browser Control**, that allows the specification of minimum Browser versions, and Browser vulnerability protections.

The A**ccess Control** policies available are: **URL & Cloud App Control**, that can be used to control access to destination Websites or applications; **File Type Control**, to specify the file types that may be uploaded, or downloaded; **Bandwidth Control**, for assigning maximum, and minimum bandwidth percentages for classes of traffic; and **SSL Inspection**, with settings and resources for intercepting and inspecting SSL traffic.

The **Data Loss Prevention** policy area allows the creation of policies to monitor, and if necessary block, the unauthorized exfiltration of data using Zscaler internal, or external DLP engines. It also allows the streaming of data to an on-site ICAP server for analysis.

Slide 7 - Policy Areas



Policy Areas

Web

Security

- Malware Protection
- Advanced Threat Protection
- Sandbox
- Browser Control

Access Control

- URL & Cloud App Control
- File Type Control
- Bandwidth Control
- SSL Inspection

Data Loss Prevention

- Data Loss Prevention

View Recommended Malware Protection Policy

Configure Malware Protection Policy

Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

Traffic Inspection

Inspect Inbound Traffic ✓

Inspect Outbound Traffic ✓

Protocol Inspection

Inspect HTTP ✓

Inspect FTP over HTTP ✓

Inspect FTP ✓

Malware Protection

Viruses: Allow [✓ Block]

Unwanted Applications: Allow [✓ Block]

Trojans: Allow [✓ Block]

Worms: Allow [✓ Block]

Adware/Spyware Protection

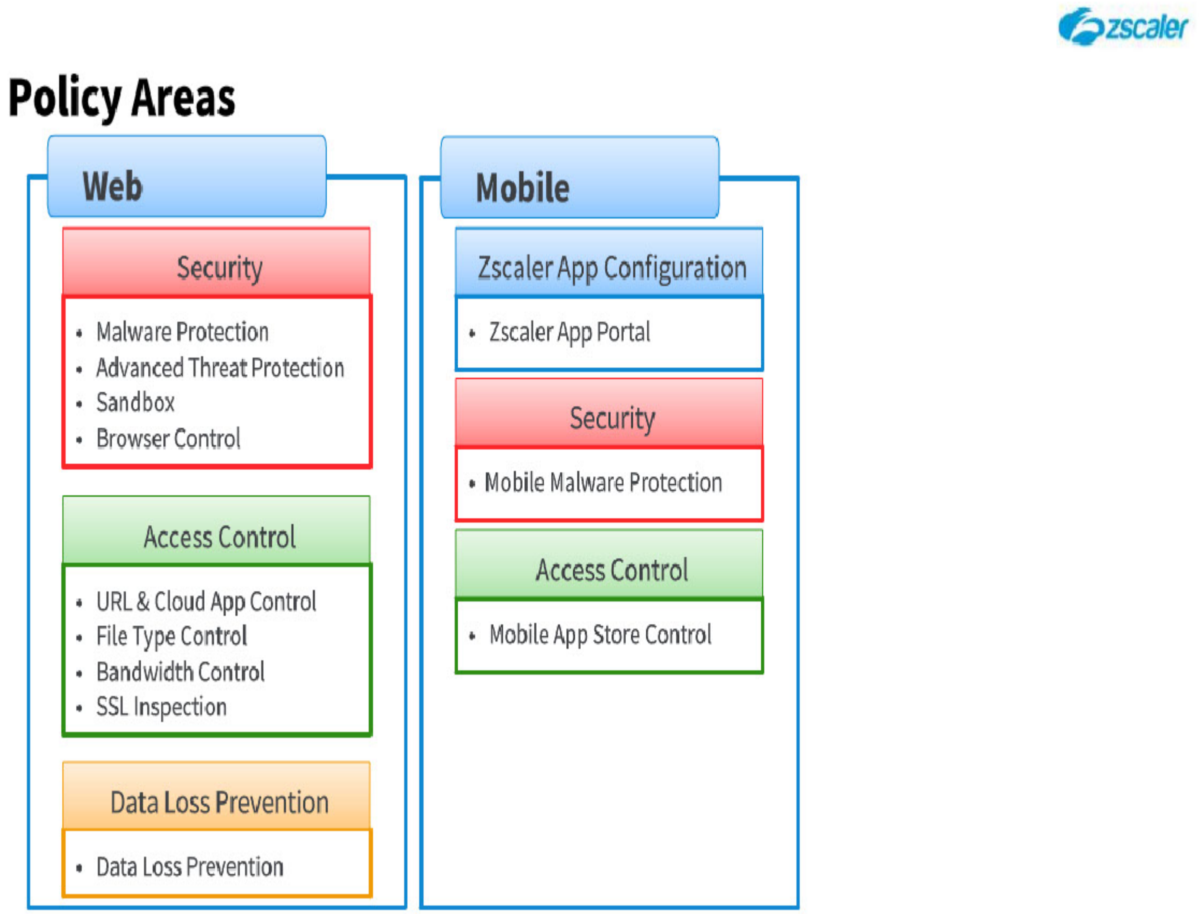
Adware: Allow [✓ Block]

Spyware: Allow [✓ Block]

Slide notes

Note, that brief Policy Information, and links to **Recommended Policy** settings are shown on each Policy page.

Slide 8 - Policy Areas



Policy Areas

Web

Security

- Malware Protection
- Advanced Threat Protection
- Sandbox
- Browser Control

Access Control

- URL & Cloud App Control
- File Type Control
- Bandwidth Control
- SSL Inspection

Data Loss Prevention

- Data Loss Prevention

Mobile

Zscaler App Configuration

- Zscaler App Portal

Security

- Mobile Malware Protection

Access Control

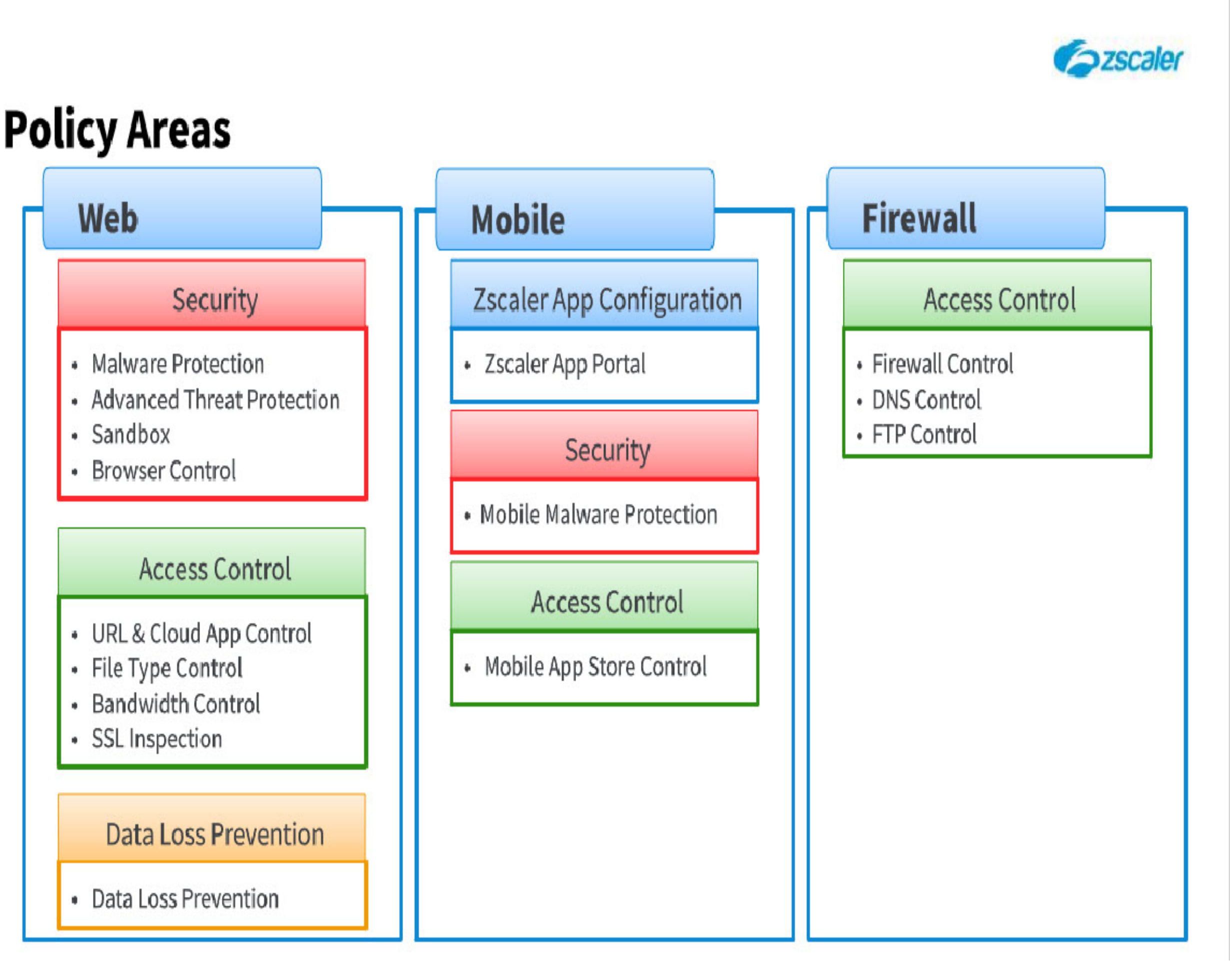
- Mobile App Store Control

Slide notes

The **Mobile** policy area also has three policy categories; **Zscaler App Configuration**, **Security**, and **Access Control**.

The **Zscaler App Configuration** category contains a link to the **Zscaler App Portal**, where configurations and policies for the Zscaler App, and secure agent for mobile can be defined. The **Security** category contains the ability to setup a policy for **Mobile Malware Protection**, and the **Access Control** category allows the definition of policy rules for **Mobile App Store Control**.

Slide 9 - Policy Areas



Policy Areas

Web

Security

- Malware Protection
- Advanced Threat Protection
- Sandbox
- Browser Control

Access Control

- URL & Cloud App Control
- File Type Control
- Bandwidth Control
- SSL Inspection

Data Loss Prevention

- Data Loss Prevention

Mobile

Zscaler App Configuration

- Zscaler App Portal

Security

- Mobile Malware Protection

Access Control

- Mobile App Store Control

Firewall

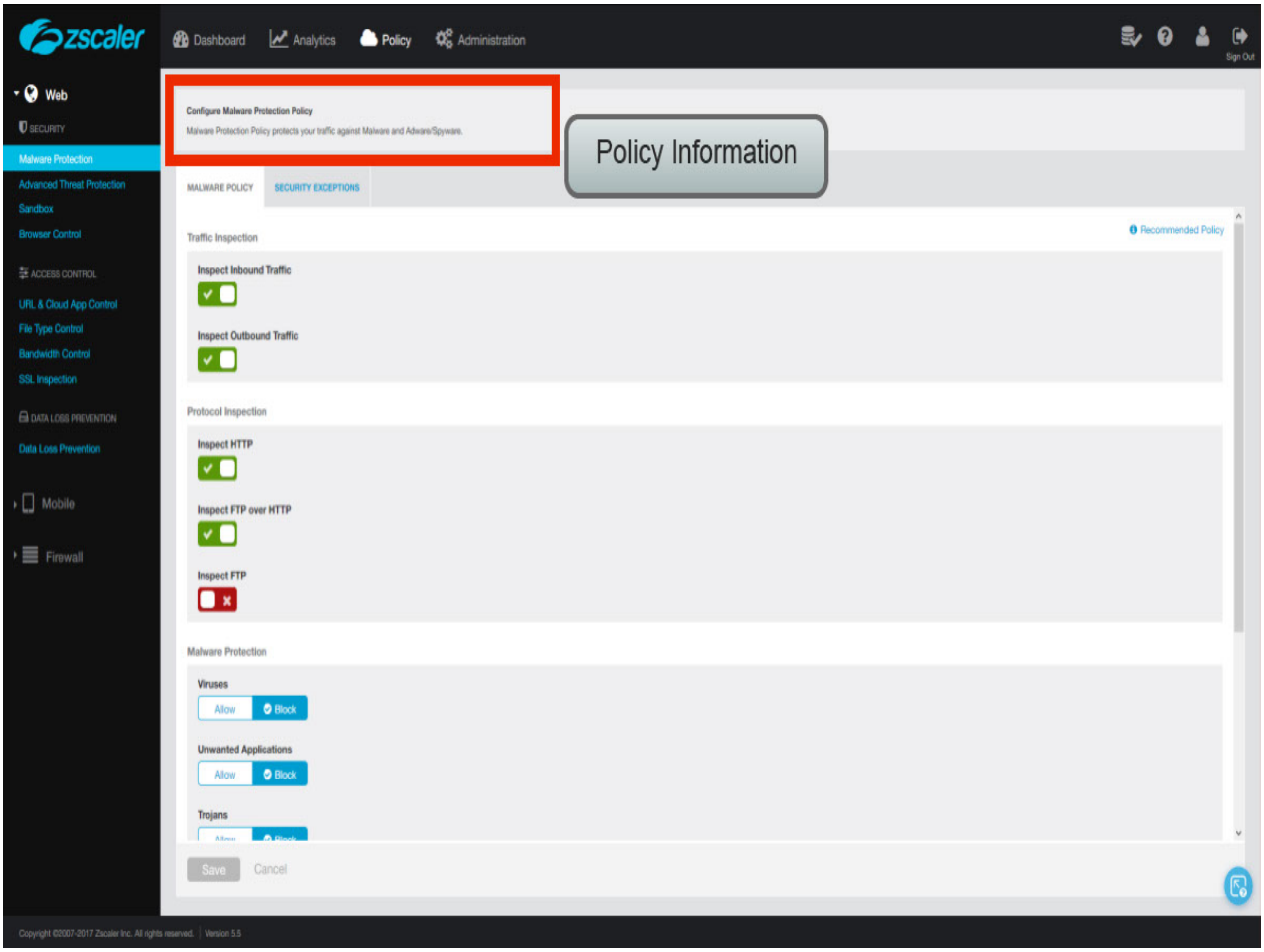
Access Control

- Firewall Control
- DNS Control
- FTP Control

Slide notes

The **Firewall** area contains **Access Control** policies allowing the configuration of **Firewall Control**, **DNS Control**, or **FTP Control** policies. Note that the **Firewall** policy configuration is for both the Basic, and Next Generation Firewall configuration, depending on your subscription.

Slide 10 - Slide 10



Configure Malware Protection Policy

Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

Traffic Inspection

Inspect Inbound Traffic ✓

Inspect Outbound Traffic ✓

Protocol Inspection

Inspect HTTP ✓

Inspect FTP over HTTP ✓

Inspect FTP ✗

Malware Protection

Viruses: Allow [✓ Block]

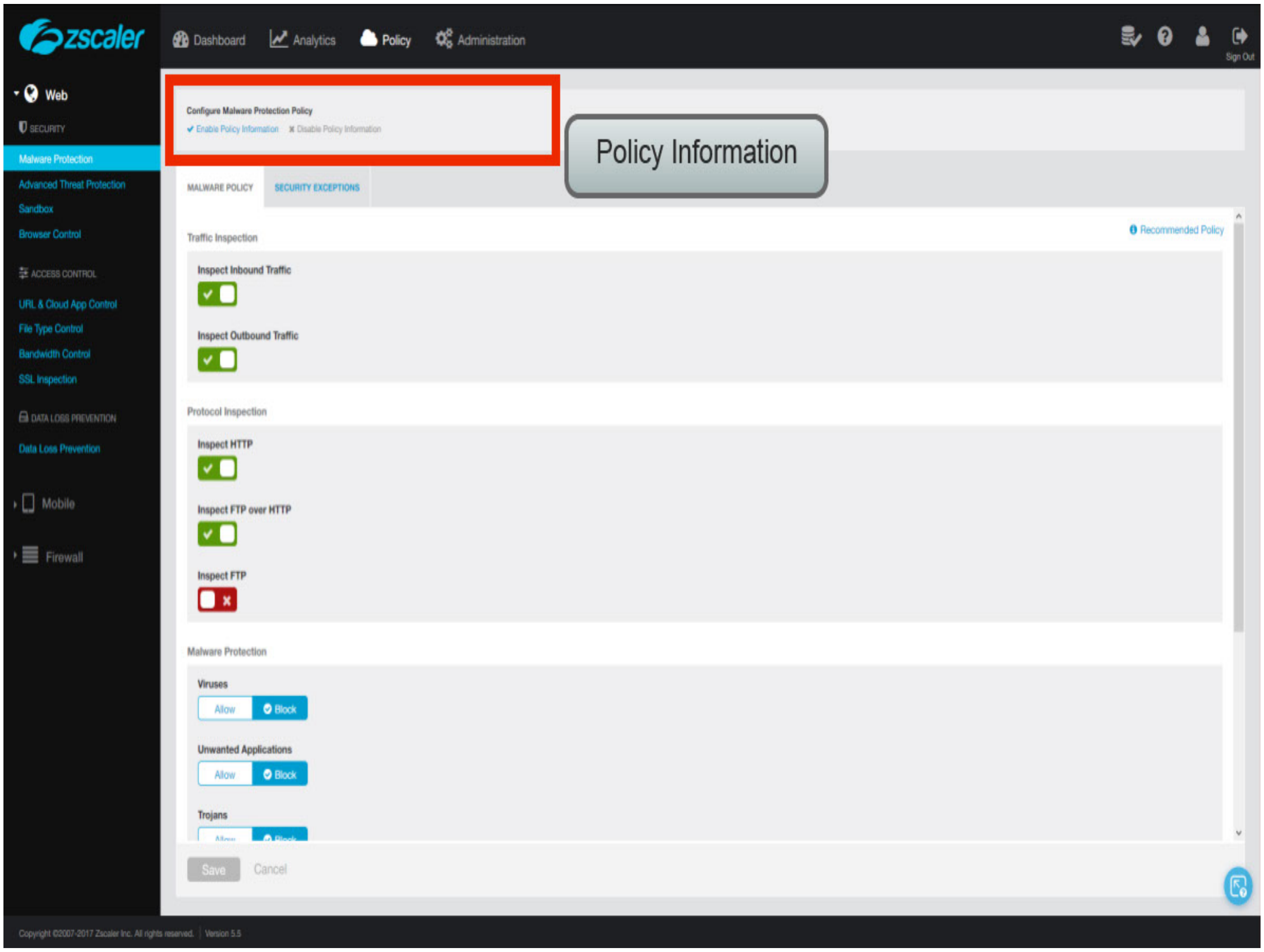
Unwanted Applications: Allow [✓ Block]

Trojans: Allow [✓ Block]

Slide notes

Brief Policy information is shown at the top of each Policy page, to describe the purpose of the Policy.

Slide 11 - Slide 11



Configure Malware Protection Policy

✔ Enable Policy Information ✖ Disable Policy Information

Traffic Inspection

Inspect Inbound Traffic ✓

Inspect Outbound Traffic ✓

Protocol Inspection

Inspect HTTP ✓

Inspect FTP over HTTP ✓

Inspect FTP ✗

Malware Protection

Viruses: Allow [✓ Block]

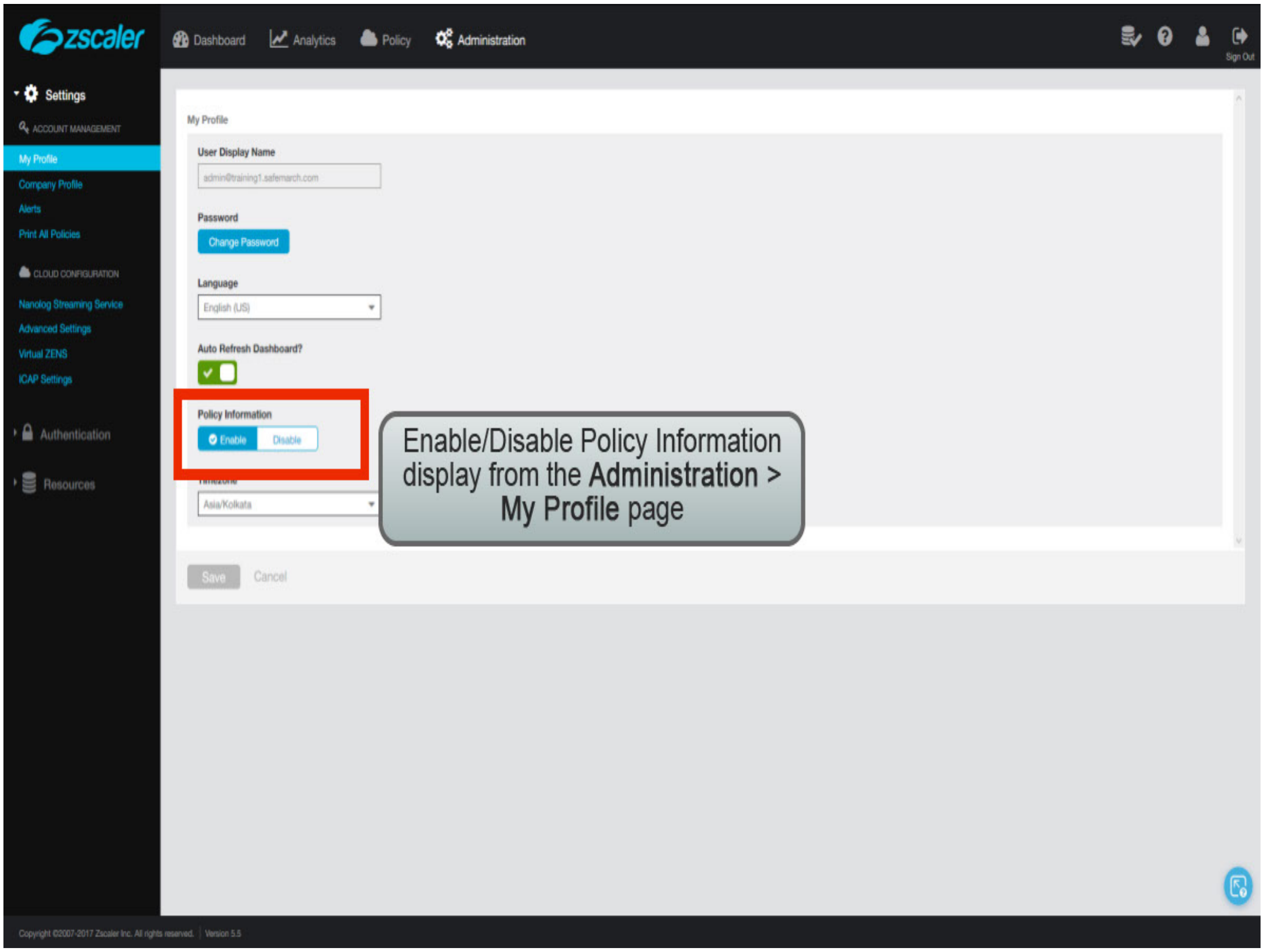
Unwanted Applications: Allow [✓ Block]

Trojans: Allow [✓ Block]

Slide notes

These notices can be turned off if necessary on each Policy page.

Slide 12 - Slide 12



My Profile

User Display Name: admin@training1.safemarch.com

Password: Change Password

Language: English (US)

Auto Refresh Dashboard? ✓

Policy Information: [✓ Enable] Disable

Timezone: Asia/Kolkata

Save Cancel

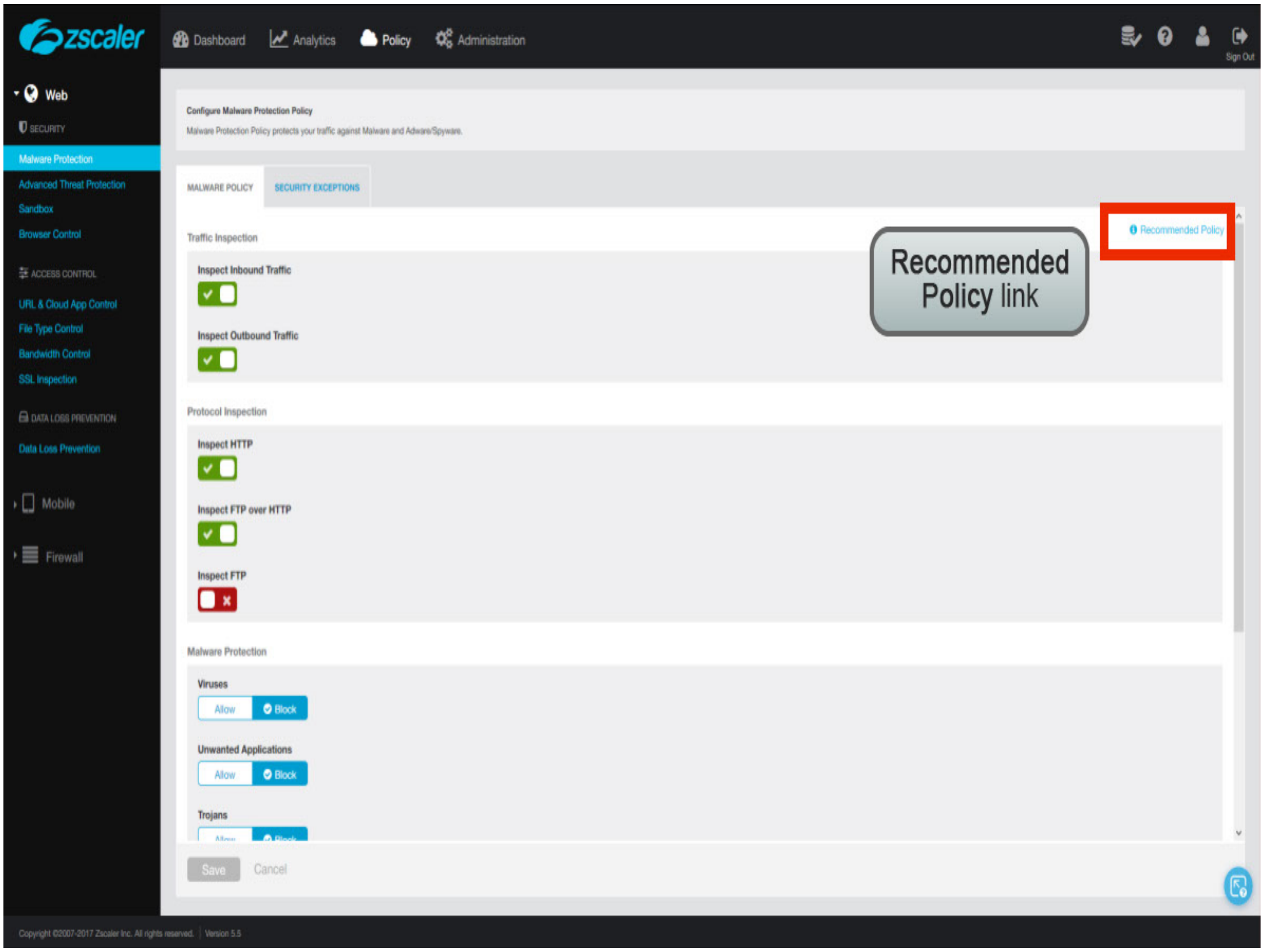
Enable/Disable Policy Information display from the **Administration** > My Profile page

Copyright ©2007-2017 Zscaler Inc. All rights reserved. | Version 5.5

Slide notes

You can enable, or disable the display of Policy information from the **Administration** > **My Profile** page.

Slide 13 - Slide 13



Configure Malware Protection Policy

Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

Traffic Inspection

Inspect Inbound Traffic ✓

Inspect Outbound Traffic ✓

Protocol Inspection

Inspect HTTP ✓

Inspect FTP over HTTP ✓

Inspect FTP ✗

Malware Protection

Viruses: Allow ● Block

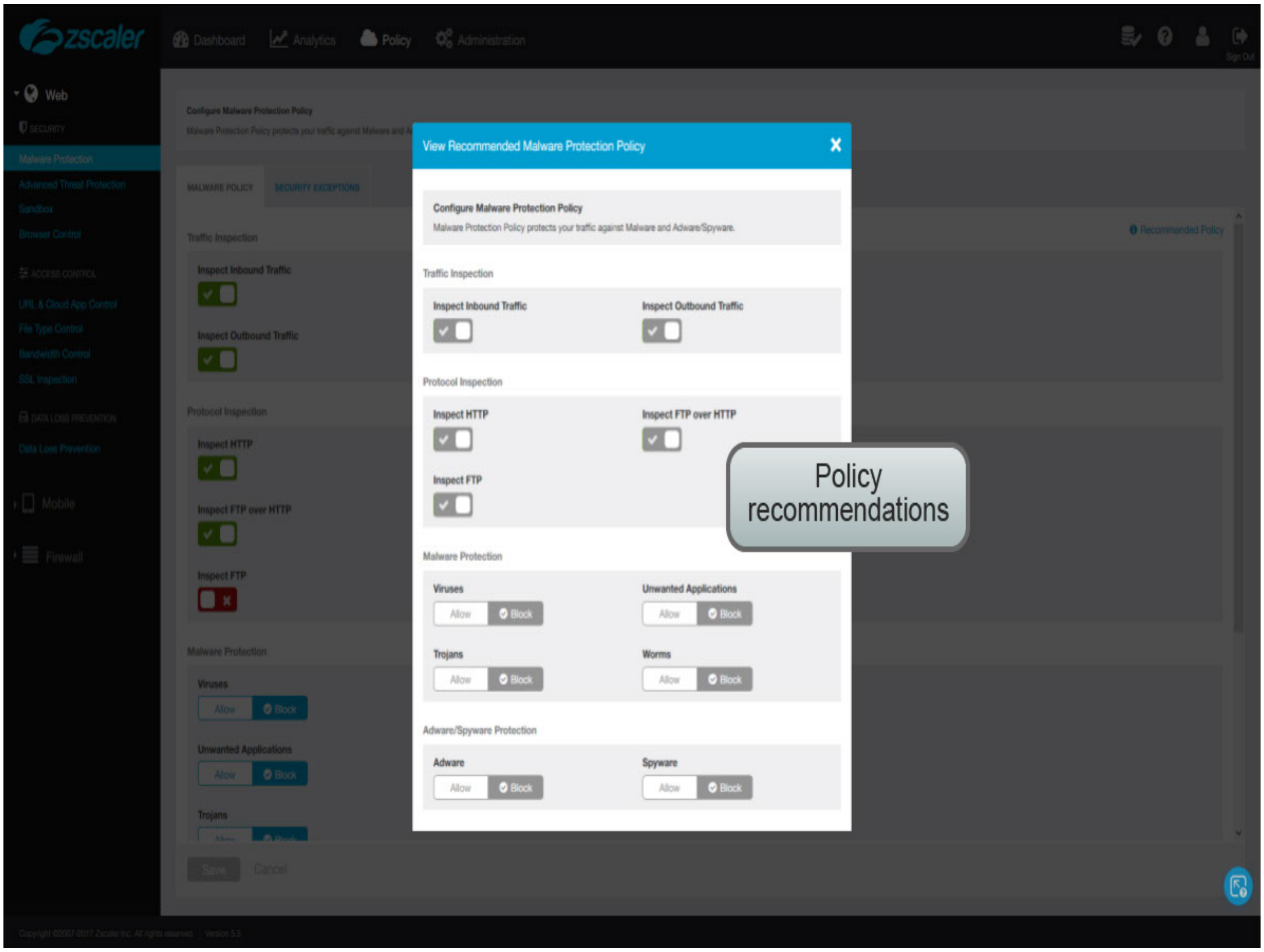
Unwanted Applications: Allow ● Block

Trojans: Allow ● Block

Slide notes

Each Policy page also has a **Recommended Policy** link

Slide 14 - Slide 14



View Recommended Malware Protection Policy

Configure Malware Protection Policy

Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

Traffic Inspection

- Inspect Inbound Traffic: ✓
- Inspect Outbound Traffic: ✓

Protocol Inspection

- Inspect HTTP: ✓
- Inspect FTP over HTTP: ✓
- Inspect FTP: ✓

Malware Protection

- Viruses: Allow [✓ Block]
- Unwanted Applications: Allow [✓ Block]
- Trojans: Allow [✓ Block]
- Worms: Allow [✓ Block]

Adware/Spyware Protection

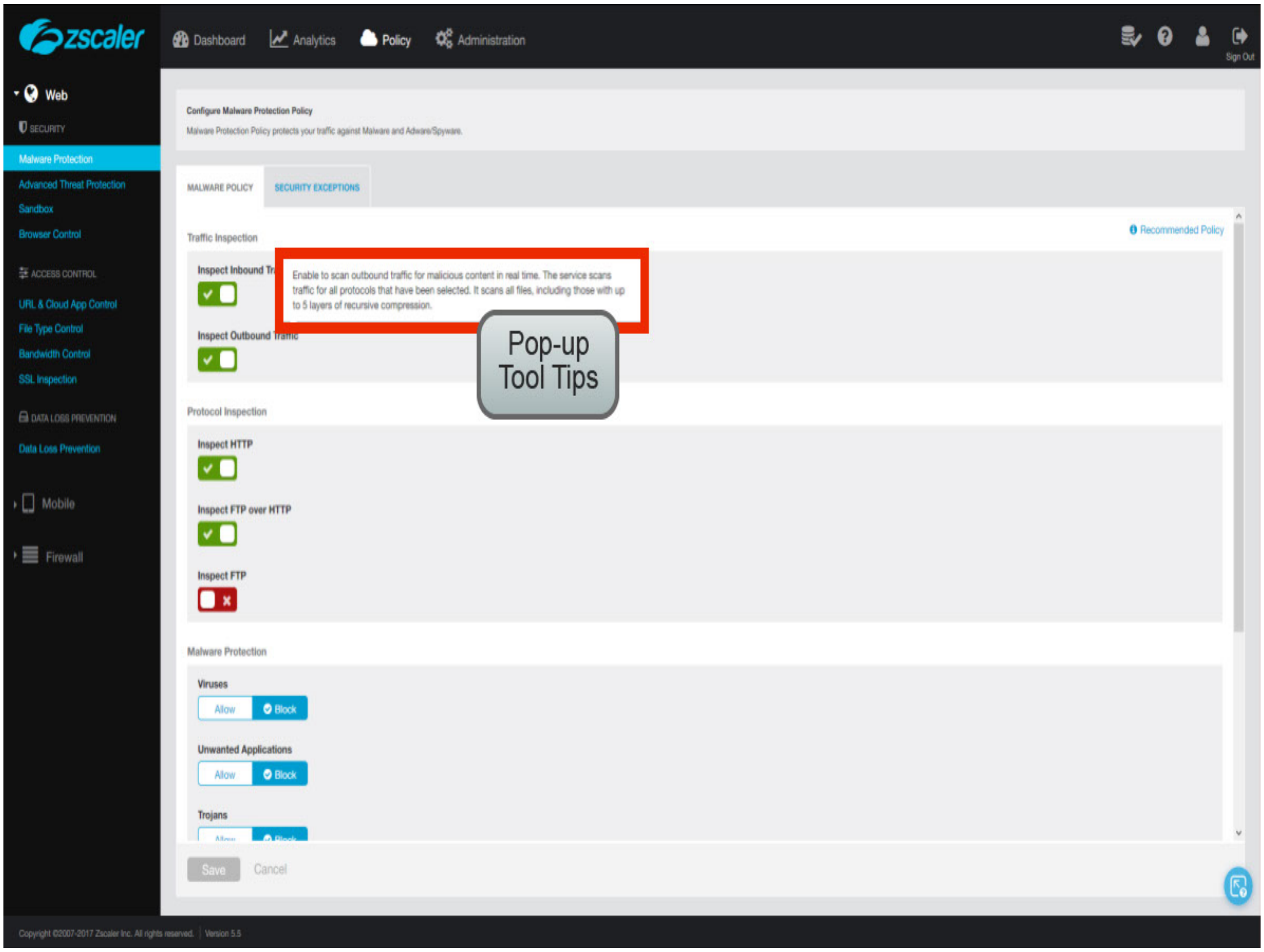
- Adware: Allow [✓ Block]
- Spyware: Allow [✓ Block]

Policy recommendations

Slide notes

which opens a window displaying Zscaler's recommended settings for the Policy in question.

Slide 15 - Slide 15



Configure Malware Protection Policy

Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

Traffic Inspection

Inspect Inbound Tr ✓

Enable to scan outbound traffic for malicious content in real time. The service scans traffic for all protocols that have been selected. It scans all files, including those with up to 5 layers of recursive compression.

Inspect Outbound Traffic ✓

Protocol Inspection

Inspect HTTP ✓

Inspect FTP over HTTP ✓

Inspect FTP ✗

Malware Protection

Viruses: Allow [✓ Block]

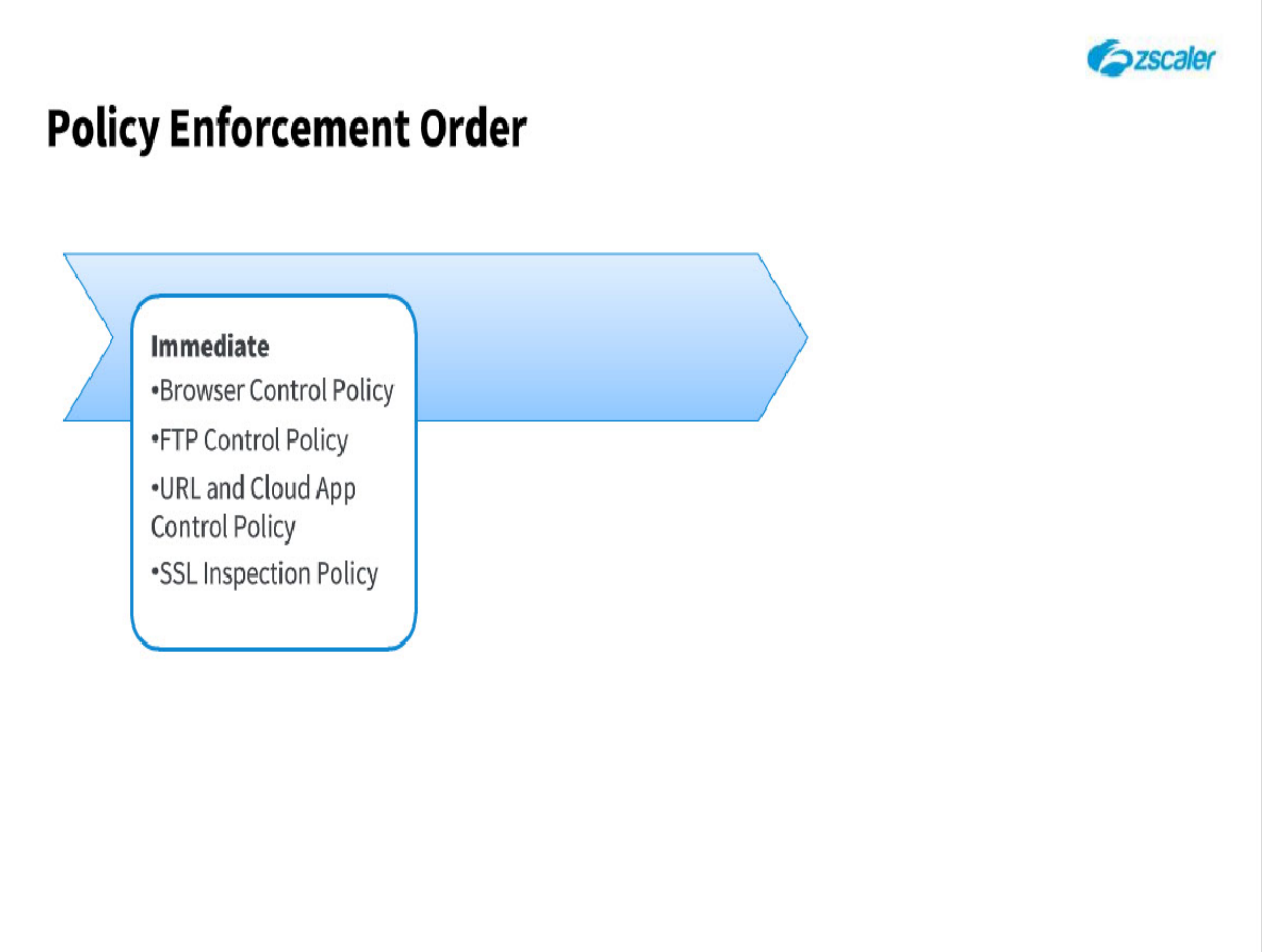
Unwanted Applications: Allow [✓ Block]

Trojans: Allow [✓ Block]

Slide notes

In addition, if you mouseover the name of an item in the admin portal, information for that setting will be shown in a pop-up Tool Tip.

Slide 16 - Policy Enforcement Order



Policy Enforcement Order

Immediate

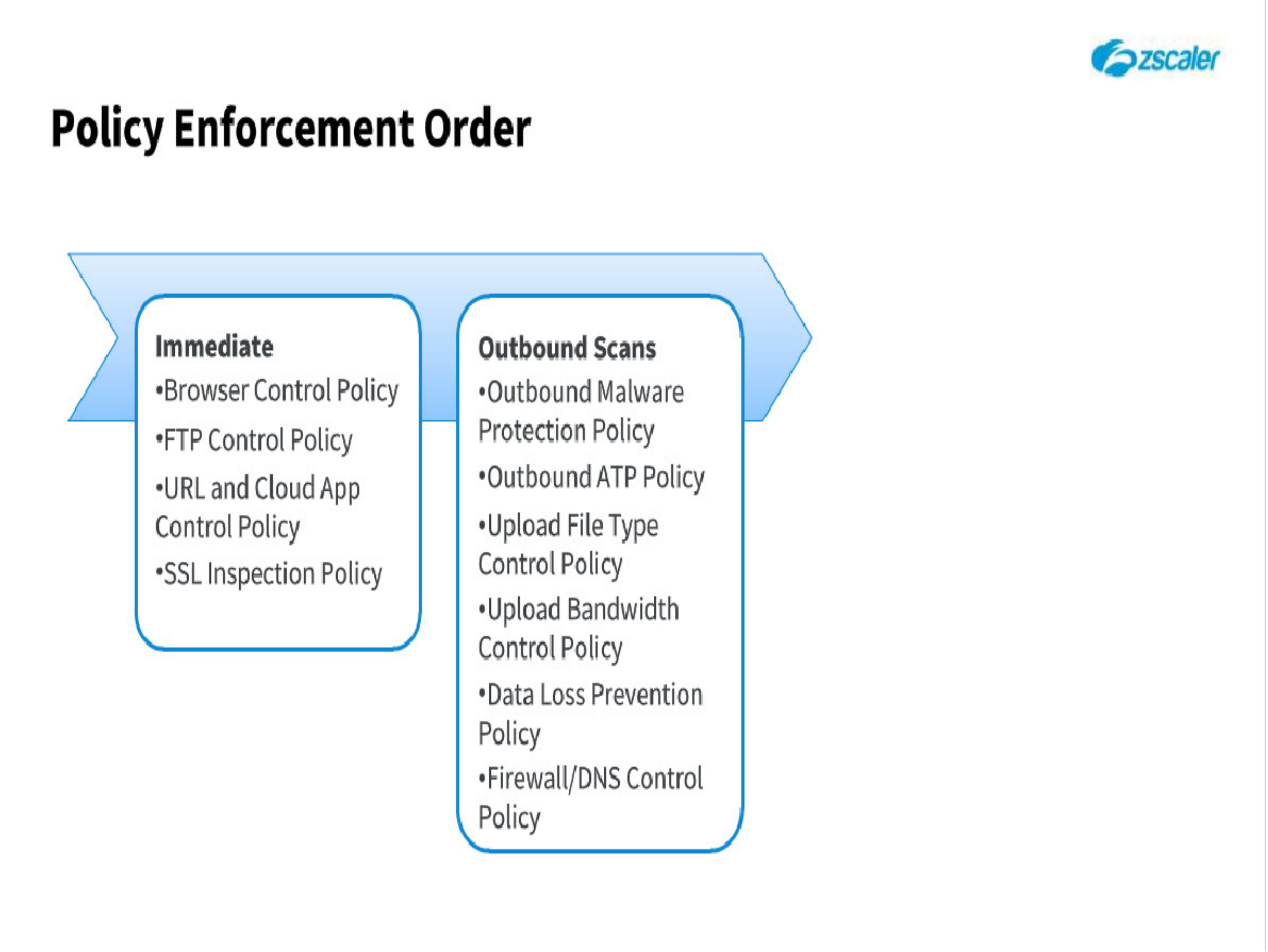
- •Browser Control Policy
- •FTP Control Policy
- •URL and Cloud App Control Policy
- •SSL Inspection Policy

Slide notes

Some of the policies that you can define are implemented immediately a connection request from a client device reaches the ZEN. If the Browser used does not match the **Browser Control** policy, we can block access; if FTP requests are disallowed by an **FTP Control** policy, they can be immediately blocked;

if the Cloud App request, or the URL match filters setup up in a **URL & Cloud App Control** policy, the user can be blocked or warned straight away; and of course, if Zscaler is to inspect SSL traffic, we must terminate the inbound connection before we can do anything else.

Slide 17 - Policy Enforcement Order



Policy Enforcement Order

Immediate

- Browser Control Policy
- FTP Control Policy
- URL and Cloud App Control Policy
- SSL Inspection Policy

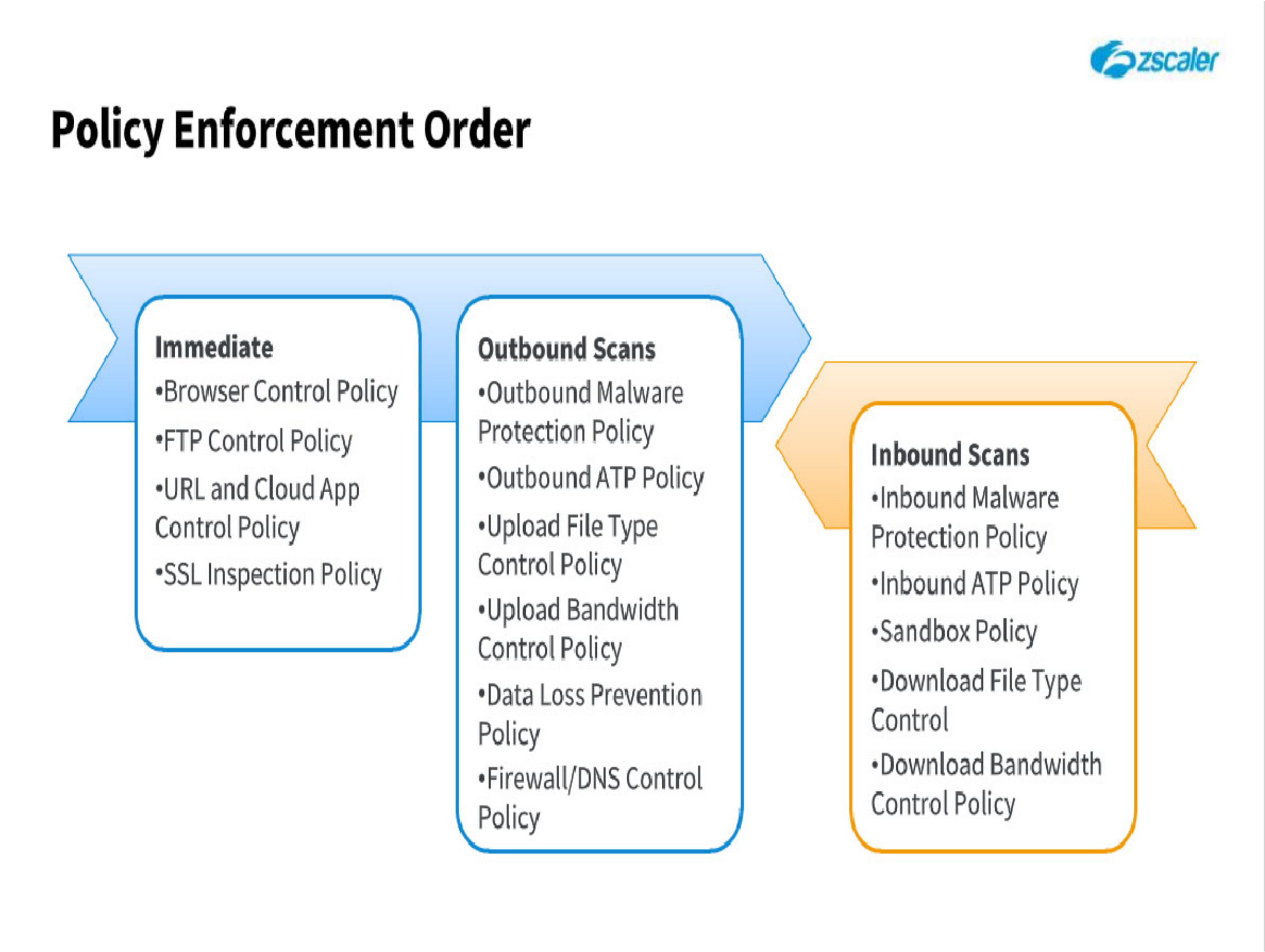
Outbound Scans

- Outbound Malware Protection Policy
- Outbound ATP Policy
- Upload File Type Control Policy
- Upload Bandwidth Control Policy
- Data Loss Prevention Policy
- Firewall/DNS Control Policy

Slide notes

If the outbound request is allowed to proceed, we can then move on to perform the outbound scans to check for other policy matches, this includes scans for: **Malware Protection**; **Advanced Threat Protection**; **File Type Control**; **Bandwidth Control**; **Data Loss Prevention**; as well as **Firewall** and **DNS Control** policies.

Slide 18 - Policy Enforcement Order



zscaler

Policy Enforcement Order

Immediate
- Browser Control Policy
- FTP Control Policy
- URL and Cloud App Control Policy
- SSL Inspection Policy

Outbound Scans
- Outbound Malware Protection Policy
- Outbound ATP Policy
- Upload File Type Control Policy
- Upload Bandwidth Control Policy
- Data Loss Prevention Policy
- Firewall/DNS Control Policy

Inbound Scans
- Inbound Malware Protection Policy
- Inbound ATP Policy
- Sandbox Policy
- Download File Type Control
- Download Bandwidth Control Policy

Slide notes

Once the connection is established to the destination server or host, policies are applied to the return traffic, including: **Malware Protection**; **Advanced Threat Protection**; **Cloud Sandbox**; **File Type Control**; and **Bandwidth Control**.

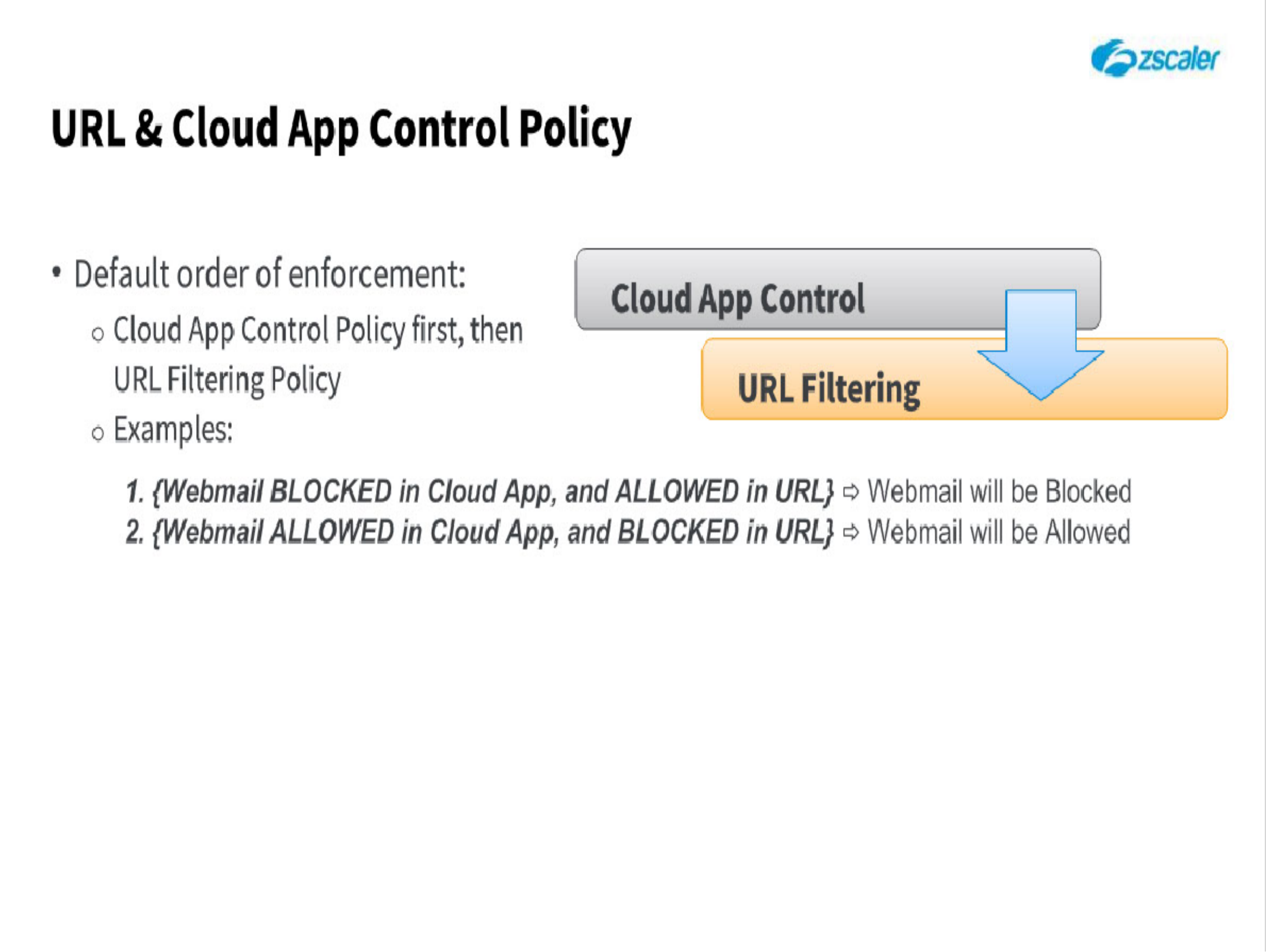
Slide 19 - Policy Key Concepts

Policy Key Concepts

Slide notes

Before we start writing policies there are some key concepts that we need to understand around how policies are applied to users and devices.

Slide 20 - URL & Cloud App Control Policy



URL & Cloud App Control Policy

- Default order of enforcement:
  - Cloud App Control Policy first, then URL Filtering Policy
  - Examples:
    1. *{Webmail BLOCKED in Cloud App, and ALLOWED in URL}* ⇨ Webmail will be Blocked
    2. *{Webmail ALLOWED in Cloud App, and BLOCKED in URL}* ⇨ Webmail will be Allowed

Cloud App Control
URL Filtering

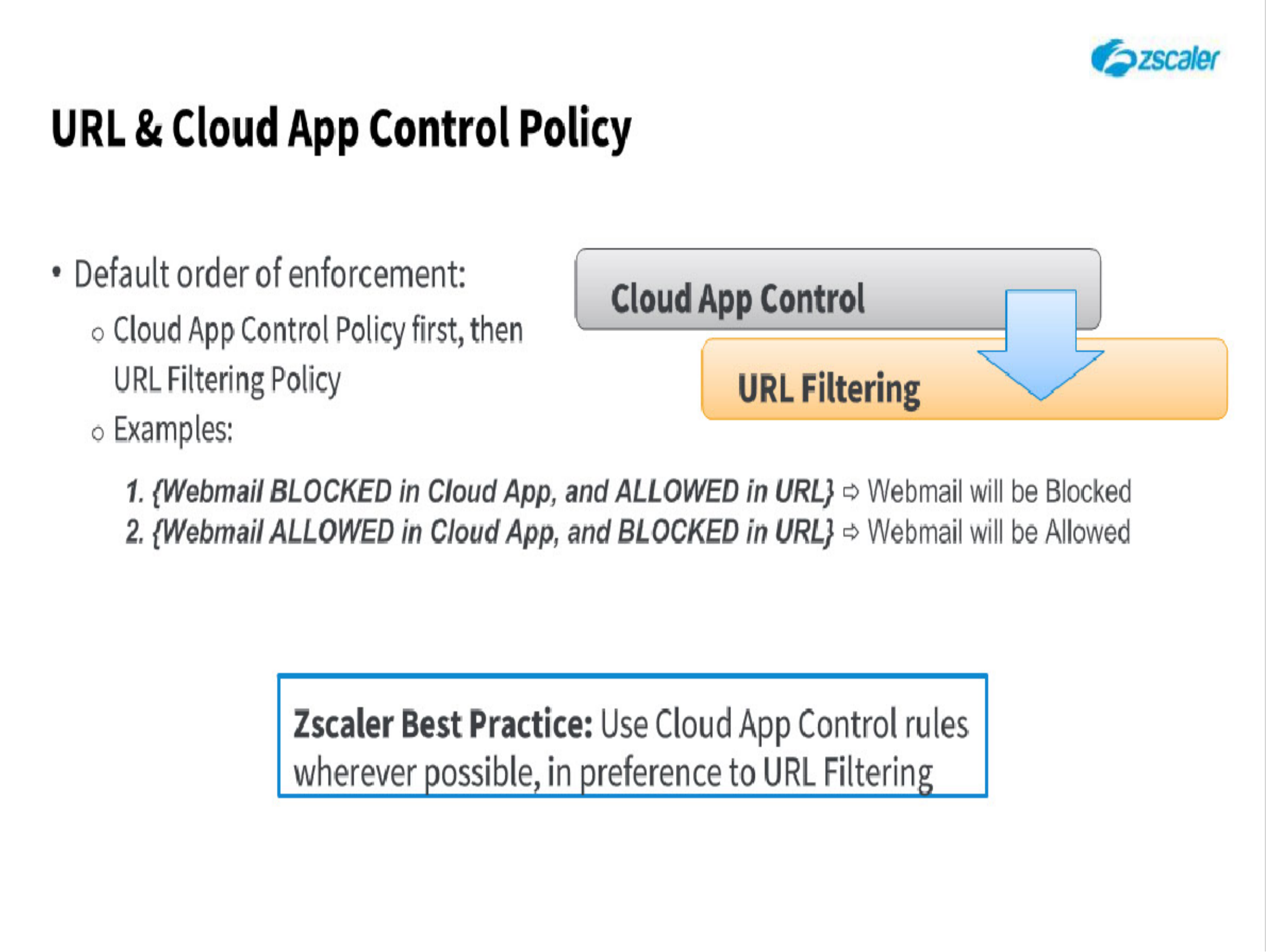
Slide notes

The **URL Filtering & Cloud App Control** pages are where you will probably spend most of your time, as this is where you will define what kinds of sites and applications your users are allowed to use. There are a couple things to note here: firstly, by default the policies are evaluated like a firewall, top-down, first match, with an implicit 'Allow All' at the end; secondly, that the **Cloud App Control** policies are evaluated first, and then the **URL Filtering** policies.

What does this mean in practice? Let's say that you block Webmail access in the **Cloud App Control Policy**, then in the **URL Filtering Policy** you allow Webmail. What will be the result? Webmail will be blocked because the **Cloud App Policy** is processed first. Conversely, what if you allow Webmail in the **Cloud App Control Policy,** and block it under **URL Filtering**?

This time Webmail will be allowed, because once the system sees the allow in the **Cloud App Policy**, that traffic will be permitted and no further rules will be processed. We will talk more about how important it is to order your rules correctly as we go through the rest of this module.

Slide 21 - URL & Cloud App Control Policy



URL & Cloud App Control Policy

- Default order of enforcement:
  - Cloud App Control Policy first, then URL Filtering Policy
  - Examples:

Cloud App Control
URL Filtering

1. *{Webmail BLOCKED in Cloud App, and ALLOWED in URL}* ⇨ Webmail will be Blocked
2. *{Webmail ALLOWED in Cloud App, and BLOCKED in URL}* ⇨ Webmail will be Allowed

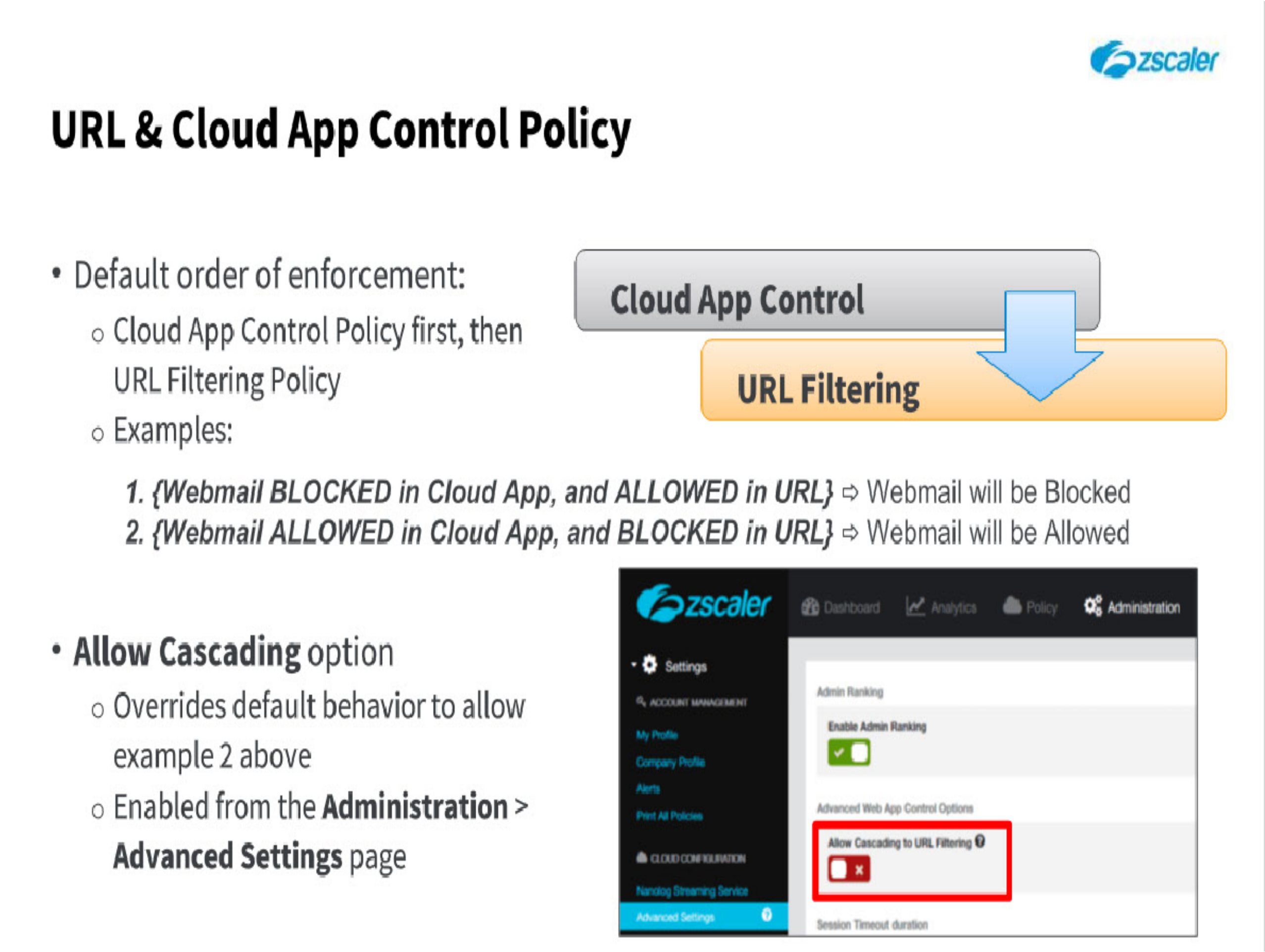
Zscaler Best Practice: Use Cloud App Control rules wherever possible, in preference to URL Filtering

Slide notes

When trying to block, or allow a specific site or app, always check first to see if it is listed under 'Cloud App Control', and use that to allow or block. Only if the site or app is not listed in **Cloud App Control** should you create a **URL Filter**, as this will save you from creating custom categories to block individual sites.

It also gives you the benefit of Zscaler keeping the filters up to date - for example, if you want to block YouTube and use a **Cloud App Control Policy** to do so, it doesn't matter what URL the user uses to access YouTube, we will block or allow regardless of the URL called.

Slide 22 - URL & Cloud App Control Policy



URL & Cloud App Control Policy

- Default order of enforcement:
  - Cloud App Control Policy first, then URL Filtering Policy
  - Examples:

1. *{Webmail BLOCKED in Cloud App, and ALLOWED in URL}* ⇨ Webmail will be Blocked
2. *{Webmail ALLOWED in Cloud App, and BLOCKED in URL}* ⇨ Webmail will be Allowed

- **Allow Cascading** option
  - Overrides default behavior to allow example 2 above
  - Enabled from the **Administration** > **Advanced Settings** page

Admin Ranking

Enable Admin Ranking ✓

Advanced Web App Control Options

Allow Cascading to URL Filtering ✗

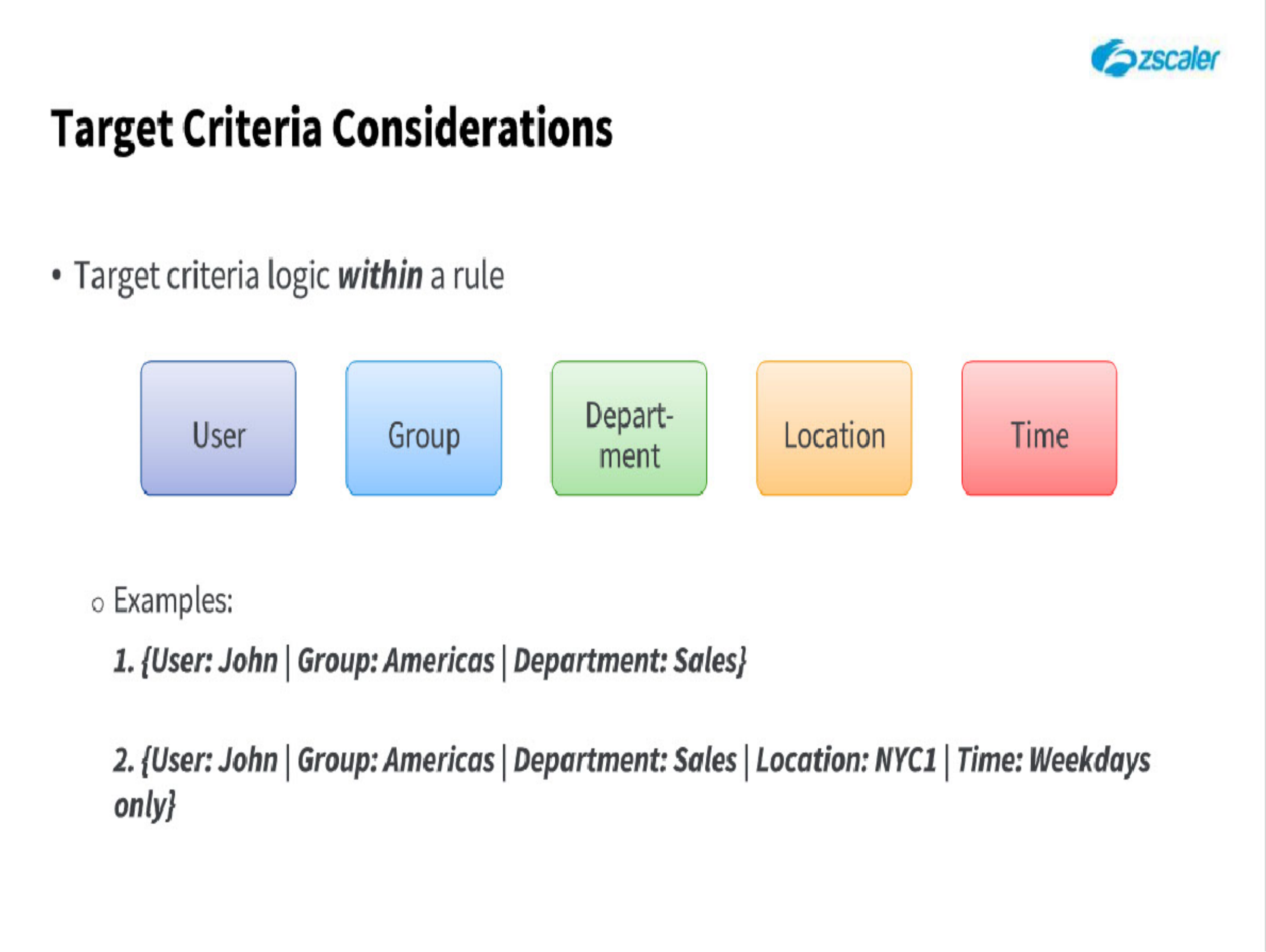
Session Timeout duration

Slide notes

This default behavior can be modified if necessary using the **Allow Cascading to URL Filtering** option in the **Advanced Settings**. This removes the **first match** condition when evaluating **Cloud Apps and URL Filtering**, and allows you to enforce both types of rule.

We will check first for **Cloud Apps**, then also evaluate the **URL Filtering** rules even if there was a **Cloud App** match. In the second of the examples above, this would have the effect of ensuring that Webmail is blocked, even though the **Cloud App** rule allows it.

Slide 23 - Target Criteria Considerations



zscaler

Target Criteria Considerations

- Target criteria logic ***within*** a rule

User | Group | Depart-ment | Location | Time

  - Examples:

    1. {User: John | Group: Americas | Department: Sales}

    2. {User: John | Group: Americas | Department: Sales | Location: NYC1 | Time: Weekdays only}

Slide notes

When you are creating Policy rules, you have the option to apply them to the entire organization, or to a subset of users based on a variety of criteria. The first criteria, **Users**, is pretty self-explanatory, you can enter specific usernames in the policy and it will only apply to those users. Next you have the option to select **Groups**, or **Departments**, these are dependent on the authentication method that you use.

For instance, if you are using LDAP to authenticate users, you must tell Zscaler what attribute in your directory structure should be used for the **Group** and **Department** fields, although configuring those fields is beyond the scope of this module. Once those fields are defined then the groups and departments will show up in the drop-down list when you're building policy rules.

Note that to able to use the **User**, **Group**, or **Department** options for targeting policy, or for filtering Logs, users must authenticate to Zscaler.

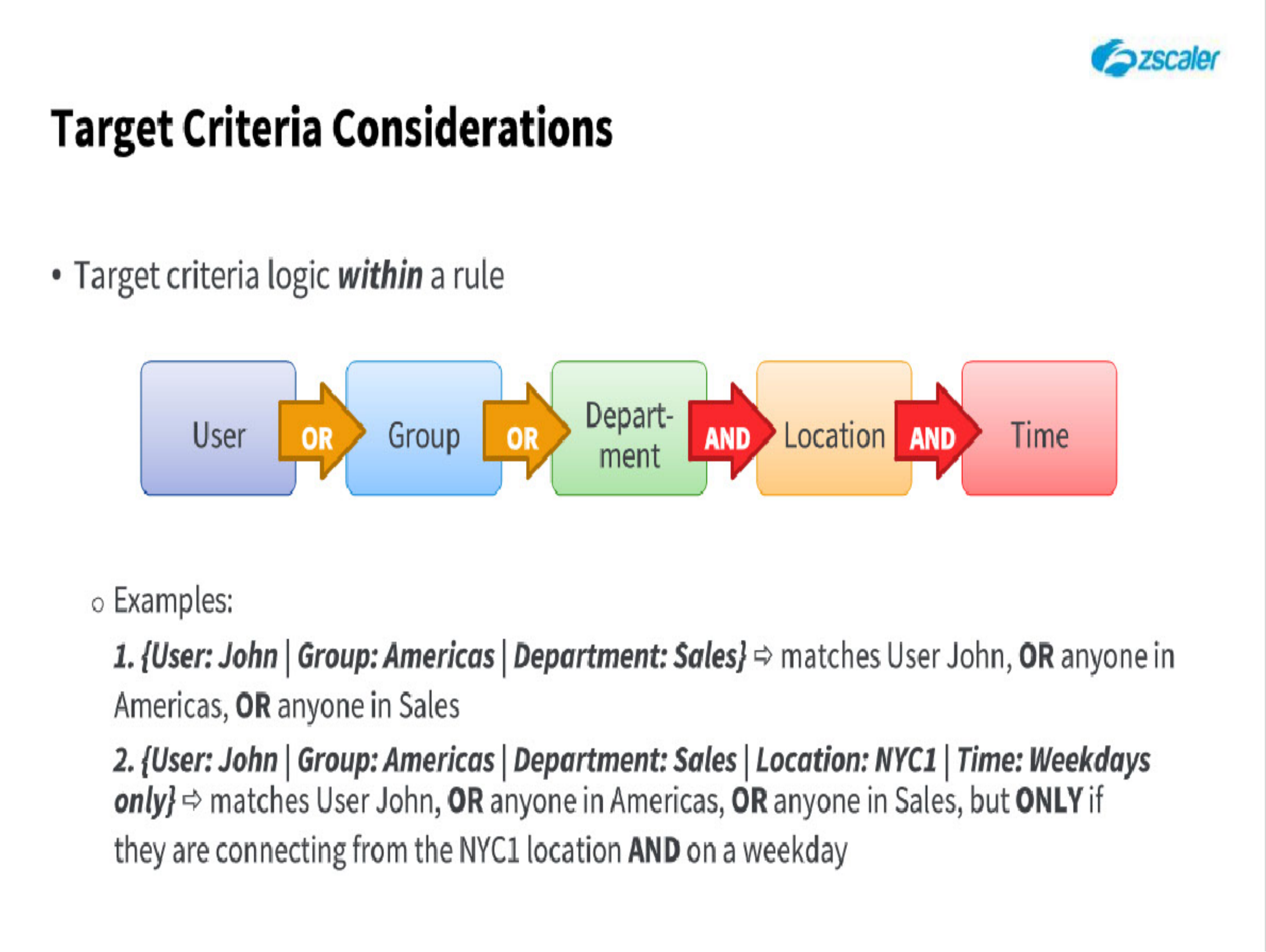
Locations allow you to assign policy based on specific sites. A **Location** can be a site that has a direct connection via GRE or VPN to the Zscaler cloud, such as a branch office, headquarters site, or even a dedicated TCP proxy port if one was purchased. When a user is coming in through one of these methods we consider them to be from a **Known Location** and you can set policy based on the user's location.

You will also see a **Location** with the name **Road Warrior**, this location applies to all users who are not connecting to the Zscaler service from a known location, so these are effectively your roaming users.

The next option is **Time**, although using timeframes can be tricky especially when applied to your roaming users. The system will apply a timeframe based on the time zone of the ZEN through which the user is connecting.

For known locations, the ZENs are generally statically assigned and so you know the time zone of the ZEN to which you're connecting. But for roaming users the ZEN through which they are connecting may or may not be in the same time zone and so the system may not behave in the way the user is expecting.

Slide 24 - Target Criteria Considerations



Target Criteria Considerations

- Target criteria logic ***within*** a rule

User **OR** Group **OR** Depart-ment **AND** Location **AND** Time

- Examples:

  1. {User: John | Group: Americas | Department: Sales} ⇨ matches User John, **OR** anyone in Americas, **OR** anyone in Sales

  2. {User: John | Group: Americas | Department: Sales | Location: NYC1 | Time: Weekdays only} ⇨ matches User John, **OR** anyone in Americas, **OR** anyone in Sales, but **ONLY** if they are connecting from the NYC1 location **AND** on a weekday

Slide notes

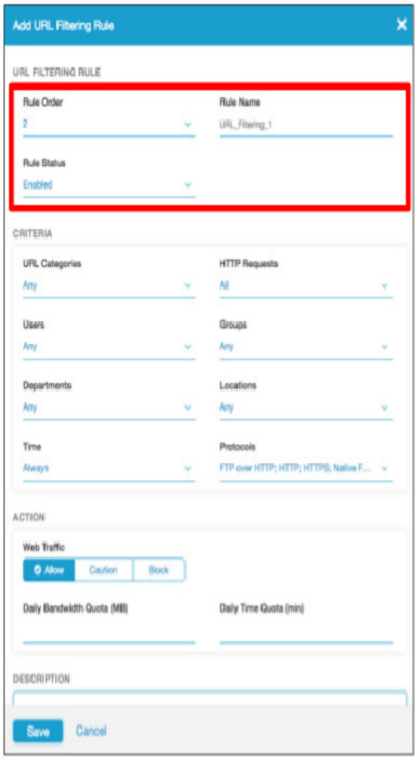
It is critical that you understand how the who, where, and when logic is applied when creating policy rules. The logic is shown here: the **User**, **Group**, and **Department** fields all use a logical **OR** function; but the **Location**, and **Time** fields use a logical **AND**. Let's look at a couple examples to demonstrate this.

In the first example, we create a rule that lists User **John**, Group **Americas**, and Department **Sales**. In this example, the rule will match User **John**, **OR** anyone in the Group **Americas**, **OR** anyone in the Department **Sales**.

In the second example, we create a rule that lists User **John**, Group **Americas**, Department **Sales**, Location **NYC1**, and Time **any weekday**. In this example the rule will match User **John**, **OR** anyone in the **Americas** Group, **OR** anyone in the **Sales** Department, but ONLY if they are connecting from the **NYC1** location on a weekday. If **John**, or a user in the **Americas** Group, or **Sales** Department connects from a different location, or at the weekend then this rule will not apply.

Slide 25 - Policy Rule – Configuration

Policy Rule – Configuration



Add URL Filtering Rule

URL FILTERING RULE

- Rule Order: 2
- Rule Name: URL_Filtering_1
- Rule Status: Enabled

CRITERIA

- URL Categories: Any
- HTTP Requests: All
- Users: Any
- Groups: Any
- Departments: Any
- Locations: Any
- Time: Always
- Protocols: FTP over HTTP; HTTP; HTTPS; Native F...

ACTION

- Web Traffic: ● Allow ○ Caution ○ Block
- Daily Bandwidth Quota (MB):
- Daily Time Quota (min):

DESCRIPTION

- Rule Order
  - Rules are evaluated top-down, first-match, with an implicit ***Allow All*** at the end
  - Best practice: Most specific to least specific, e.g.

    Users > **Groups** > **Departments** > **Organization**
- Admin Rank
  - When enabled, prevents a lower rank admin overriding a configuration from a higher rank
- Rule Name
  - A unique name for the rule
- Rule Status
  - **Enabled** or **Disabled**

Slide notes

Several policy types allow you to add rules using a dialog similar to that shown here. The policies that use this type of configuration include: **Cloud Sandbox**; **URL & Cloud App Control**; **File Type Control**; **Bandwidth Control**; **Mobile App Store Control**; **Firewall Control**; and **DNS Control**.

The first section at the top controls the status and positioning of this rule. The **Rule Order** field, defines where this rule is positioned in relation to your other rules, and remember rules are read from the top (rule 1) downwards, with a first match logic, and a default **Allow All** at the bottom.

Zscaler best practice is to list your rules from the MOST specific criteria, to the LEAST specific, for example if you are creating rules based on individuals or organizational groups, you would need to list the rules targeting users first, then rules for groups, then departments, and finally a general rule for the entire organization.

Admin Rank is a feature associated with role-based administration, although this is disabled by default. **Admin Rank** allows you to create a hierarchy among admins and ensure that policies and settings configured by admins with higher rank cannot be overridden by admins with lower rank. The highest rank, 0, belongs to the super admin, for each additional role you create, you can assign an admin rank between 1 (high) and 7 (low).

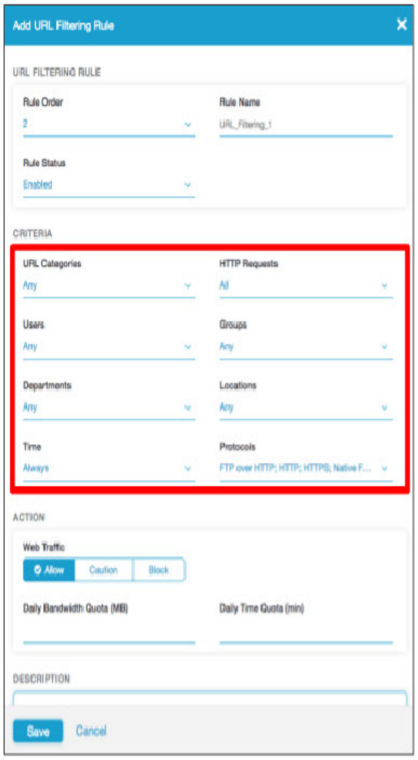
Each rule must be assigned unique name, although we automatically assign names by default. You can of course edit the default names as necessary.

Policy rules will only be applied if the rule is enabled, although this is the default status when you create a rule. To stop a rule being applied, without actually deleting the rule, set it to the Disabled status.

Slide 26 - Policy Rule – Criteria

zscaler

Policy Rule – Criteria



Add URL Filtering Rule

URL FILTERING RULE

Rule Order: 2

Rule Name: URL_Filtering_1

Rule Status: Enabled

CRITERIA

URL Categories: Any

HTTP Requests: All

Users: Any

Groups: Any

Departments: Any

Locations: Any

Time: Always

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

ACTION

Web Traffic: ● Allow ○ Caution ○ Block

Daily Bandwidth Quota (MB)

Daily Time Quota (min)

DESCRIPTION

- Target criteria to identify who the Policy applies to
  - **Users**
  - **Groups**
  - **Departments**
  - **Time**
  - **Locations** (known vs. road warrior)
- Policy specific criteria, such as…
  - **URL Categories**
  - **HTTP Requests**
  - **Cloud Applications**
  - **File Types**
  - **Sandbox Categories**
  - **Protocols**

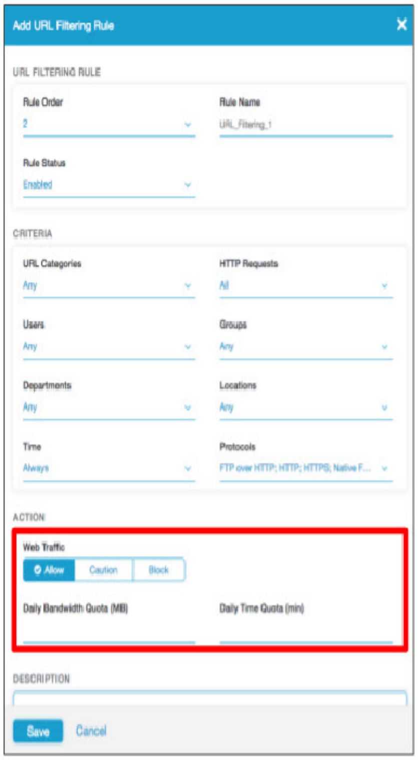
Slide notes

The **Criteria** section of the policy rule configuration allows you to specify the target criteria for the rule. Some criteria are common to most rule types, such as the **User**, **Group**, **Department**, **Location**, and **Time** options.

Other criteria are specific to the type of policy that you are creating a rule for, such as: **URL Categories**, **HTTP Requests**, or **Cloud Applications** for **URL & App Control Policy** rules; or **File Types** for a **File Type Control Policy** rules; or **Sandbox Categories** for **Sandbox Policy** rules.

Slide 27 - Policy Rule – Actions

Policy Rule – Actions



Add URL Filtering Rule

URL FILTERING RULE

Rule Order: 2

Rule Name: URL_Filtering_1

Rule Status: Enabled

CRITERIA

URL Categories: Any

HTTP Requests: All

Users: Any

Groups: Any

Departments: Any

Locations: Any

Time: Always

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

ACTION

Web Traffic: ● Allow

Daily Bandwidth Quota (MB)

Daily Time Quota (min)

DESCRIPTION

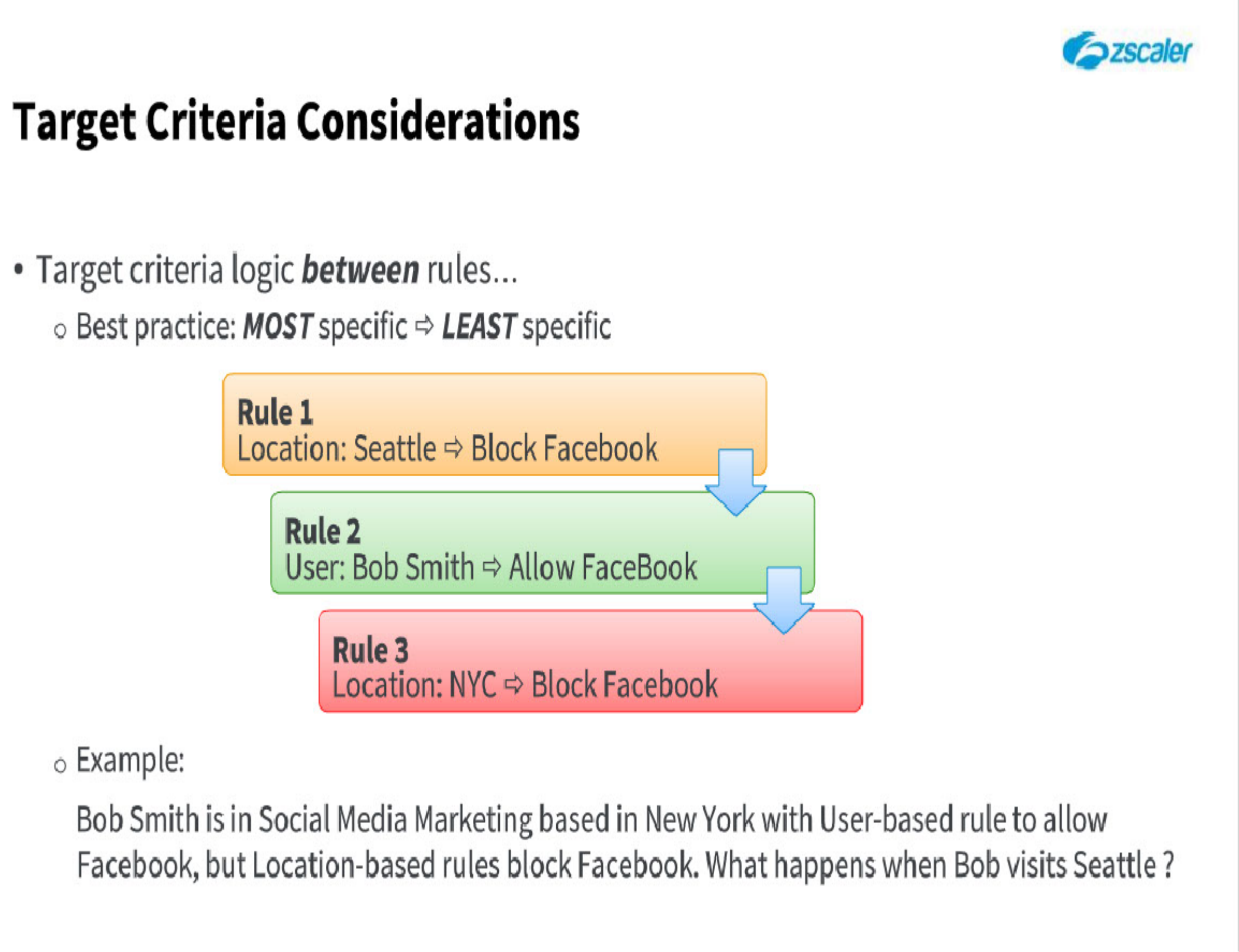
- Allow
  - Allow traffic as normal
- Caution
  - Display a caution End User Notification (EUN) page, but allow if they elect to proceed
- Block
  - Block access and display a caution End User Notification (EUN) page
- Other
  - Other actions may be available depending on the Policy type

Slide notes

The options available in the **Actions** section of a policy rule configuration depend very much on the type of policy, although the **Allow**, **Caution**, and **Block** options are available in most cases. The **Allow** option of course, permits the connection to proceed, the **Block** option blocks access and displays an **End User Notification** (EUN) page, and the **Caution** option will also display an EUN page before allowing access to the requested site.

The EUN may be the Zscaler default page, which may be customized, or you can redirect users to a specific URL to allow the use of a custom EUN. Other actions may be available depending on the type of policy.

Slide 28 - Target Criteria Considerations



Target Criteria Considerations

- Target criteria logic ***between*** rules…
  - Best practice: ***MOST*** specific ⇨ ***LEAST*** specific

Rule 1
Location: Seattle ⇨ Block Facebook

Rule 2
User: Bob Smith ⇨ Allow FaceBook

Rule 3
Location: NYC ⇨ Block Facebook

  - Example:

    Bob Smith is in Social Media Marketing based in New York with User-based rule to allow Facebook, but Location-based rules block Facebook. What happens when Bob visits Seattle ?

Slide notes

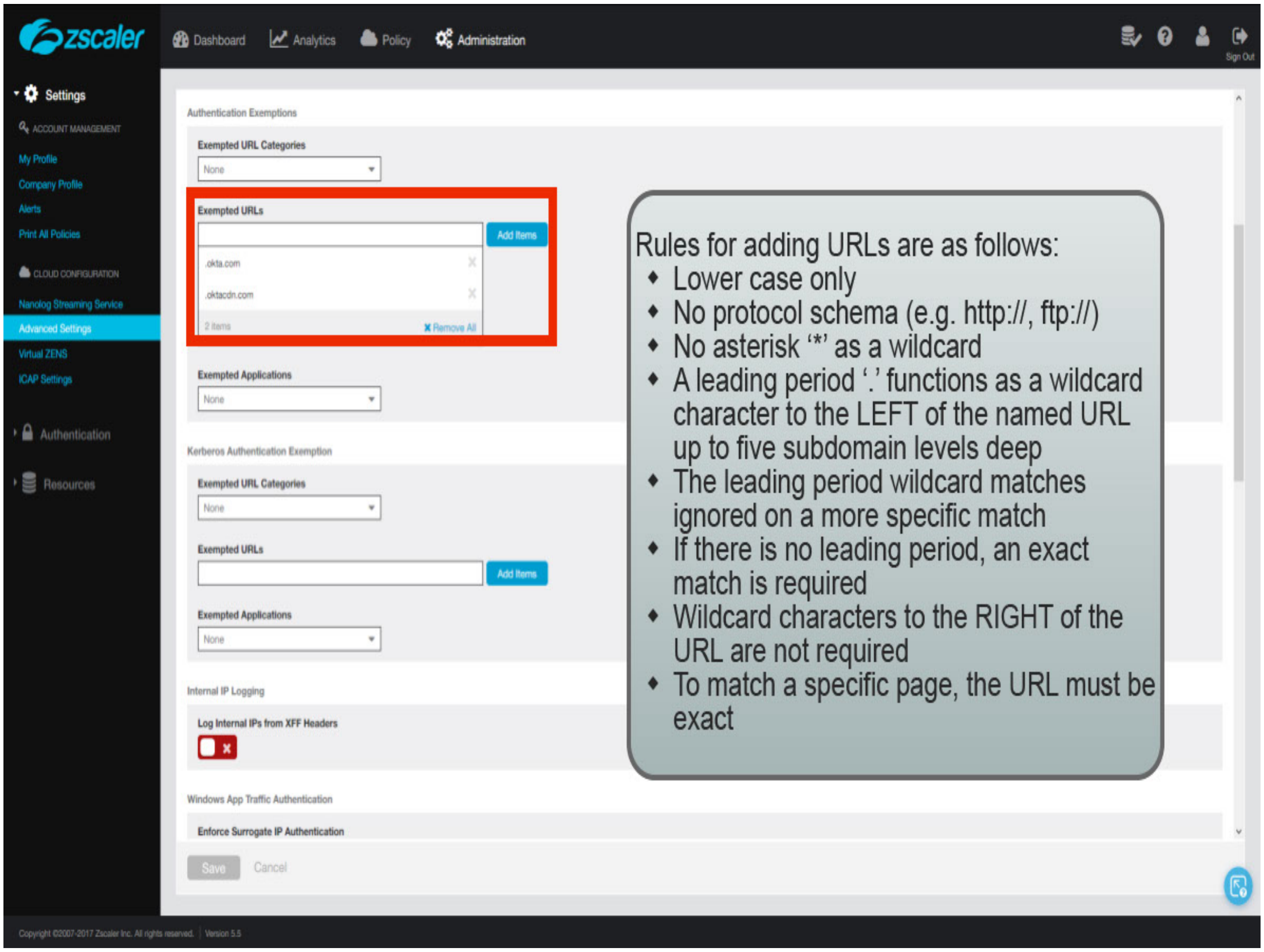
The last item we’ll cover here is the ordering of your rules. Remember that the rules are processed from the top down, with a first match logic, and a default ‘Allow All’ at the bottom. So just like when building Firewall rules, you want your most-specific rules at the top, and your least-specific rules at the bottom.

Here is an example that illustrates the importance of the ordering of your rules. You may have rules that are out of order and everything working fine, until you have a user that moves from one site to another. In this case, Bob Smith works in Social Media Marketing and is based in New York, and there is a specific rule granting Bob access to Social Media.

There are also more general rules blocking all Social Media access from particular locations, in this case New York (where Bob is based) and Seattle. However, the general rule for Seattle is listed before the specific rule for Bob.

Everything will work fine as long as Bob is in New York, but what will happen if Bob visits the Seattle office? Since Bob’s location is now Seattle, the general rule blocking Social Media access will trigger and block access for Bob. This illustrates why you need to have the most specific rules listed up front, also that you’ll typically want your location-based rules at the end.

Slide 29 - Slide 29



Authentication Exemptions

Exempted URL Categories: None

Exempted URLs:
.okta.com
.oktacdn.com
2 items

Exempted Applications: None

Kerberos Authentication Exemption

Exempted URL Categories: None

Exempted URLs

Exempted Applications: None

Internal IP Logging

Log Internal IPs from XFF Headers ✗

Windows App Traffic Authentication

Enforce Surrogate IP Authentication

Rules for adding URLs are as follows:
- Lower case only
- No protocol schema (e.g. http://, ftp://)
- No asterisk '*' as a wildcard
- A leading period '.' functions as a wildcard character to the LEFT of the named URL up to five subdomain levels deep
- The leading period wildcard matches ignored on a more specific match
- If there is no leading period, an exact match is required
- Wildcard characters to the RIGHT of the URL are not required
- To match a specific page, the URL must be exact

Slide notes

Finally, a note about adding domains in the various fields where this is possible, for example in the Authentication Exemption configuration. The rules for adding URLs are as follows: URLs must be entered in lower case only.

Do not include the protocol schema (e.g. http://, ftp://).

Do not use an asterisk ***** as a wildcard.

A leading period (**.**) functions as a wildcard character to the LEFT of the named URL up to five subdomain levels deep. For example, the entry **.example.com** also applies to: **whitelists.atlanta.example.com** and s**erv3.serv2.serv1.atlanta.example.com**.

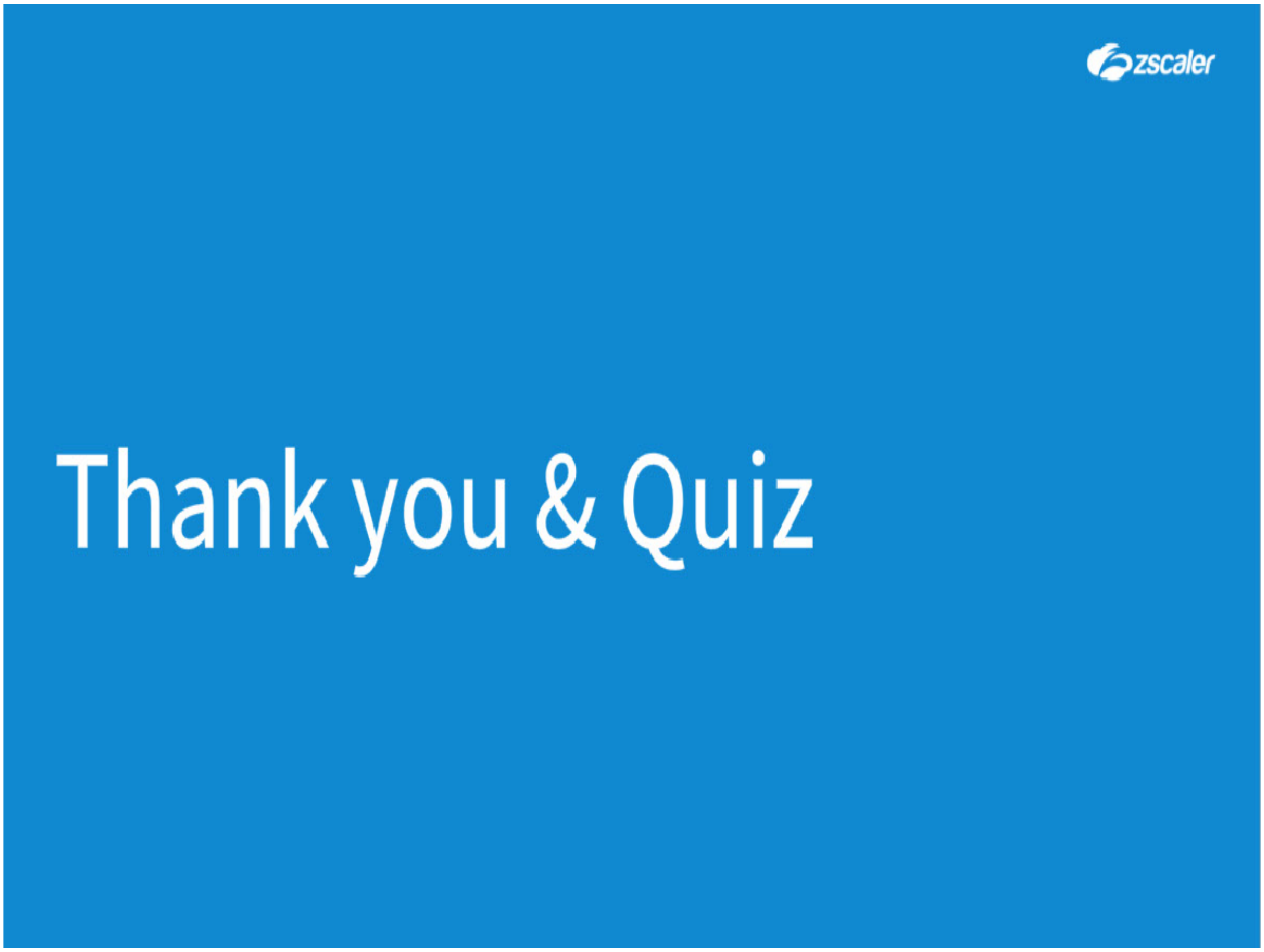
The leading period wildcard matches will be ignored if there is a more specific match.

If there is no leading period, the Domain/Subdomain must match exactly.

Wildcard characters to the RIGHT of the URL are not required, as they are assumed. For example, the URL entry **www.safemarch.com** will apply to: **safemarch.com:10443**, **safemarch.com/index.htm**, and **safemarch.com/work/mail?=next**.

To match a specific page, the URL must be exact, for example: **www.mydomain.com/resources/ftp.htm**.

Slide 30 - Thank you & Quiz



zscaler

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.