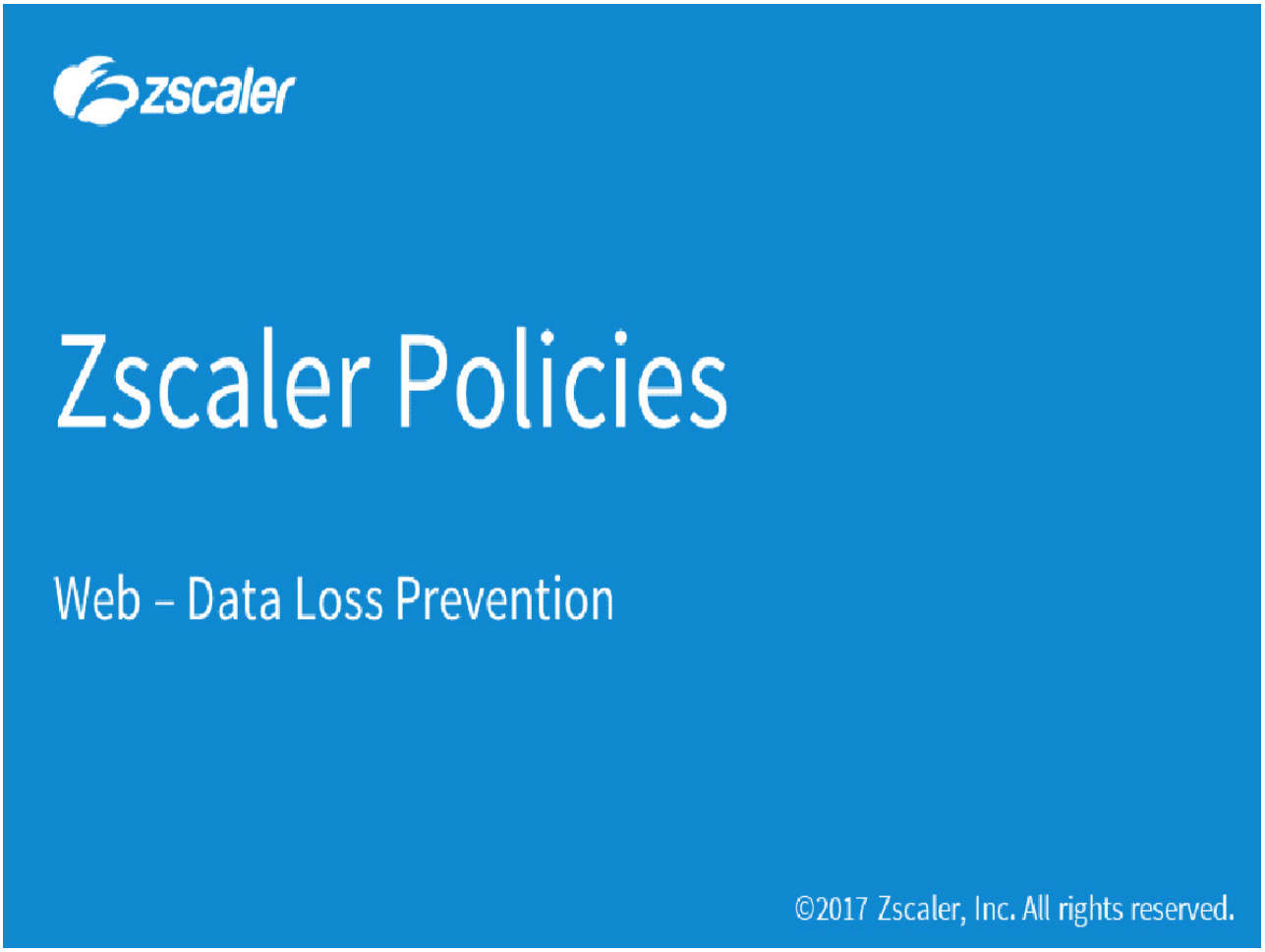
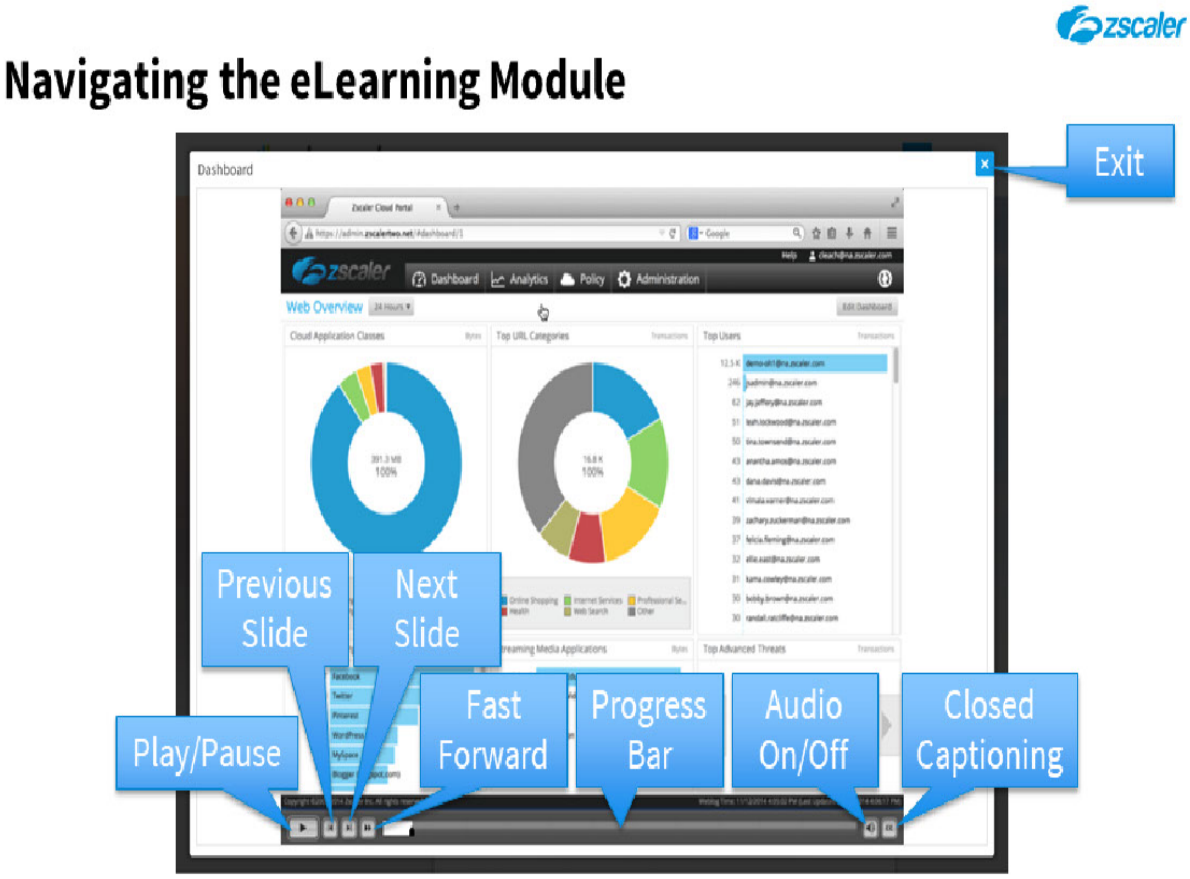
Slide 1 - Zscaler Policies



Slide notes

Welcome to the Zscaler Data Loss Prevention Policy Module.

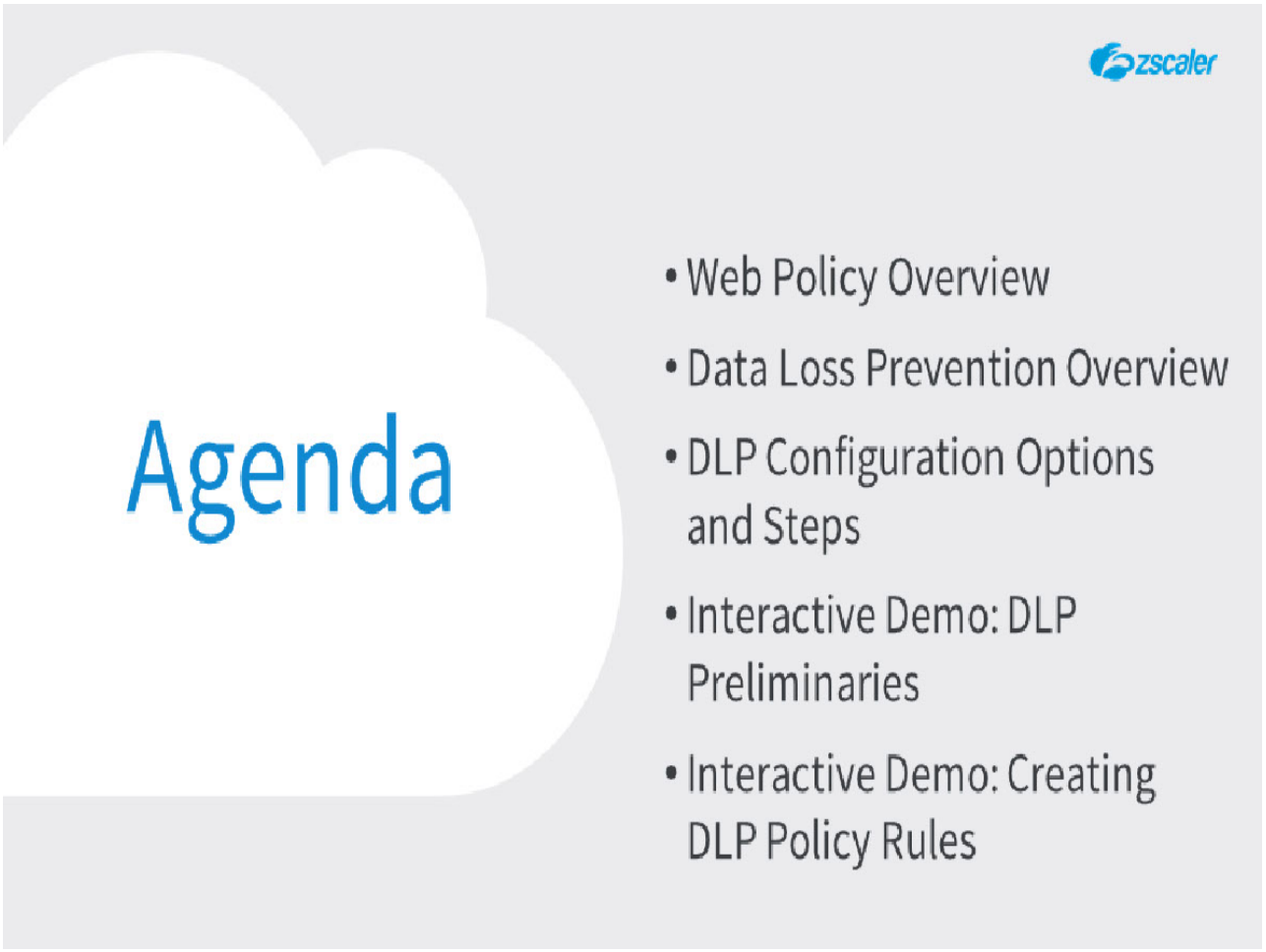
Slide 2 - Navigating the eLearning Module



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



Slide notes

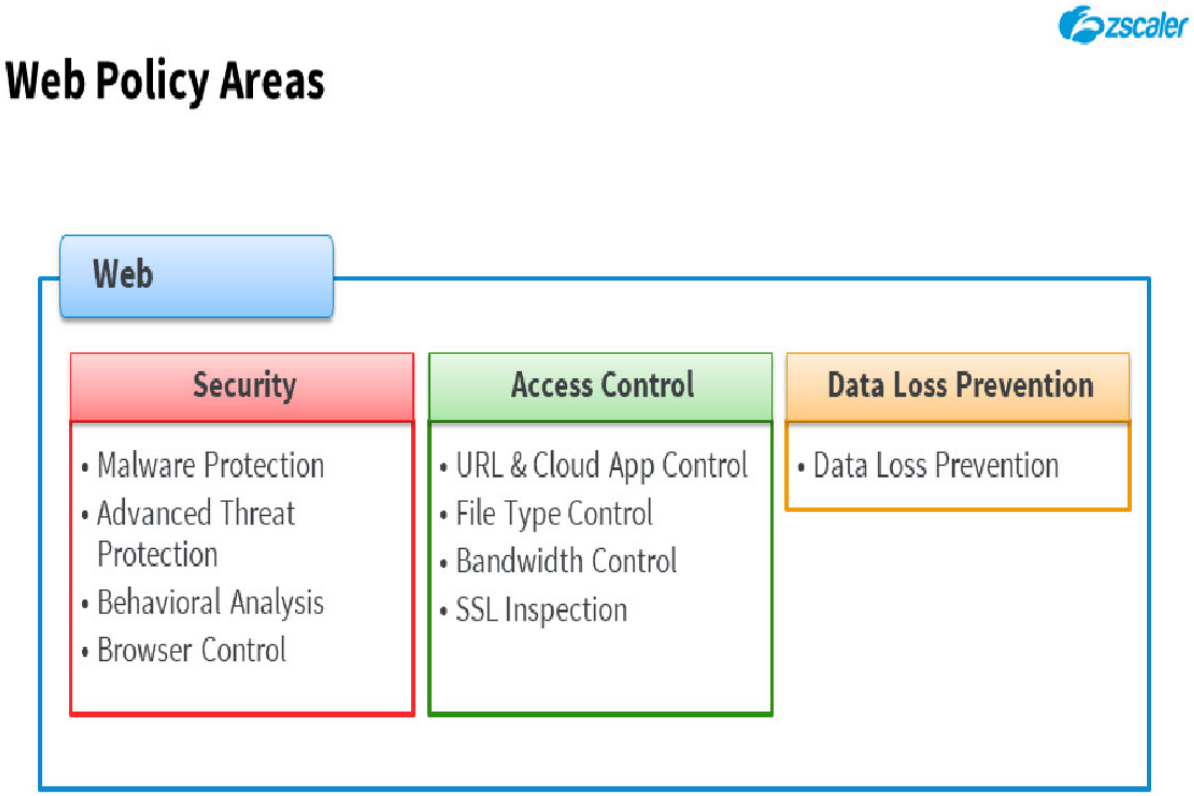
In this module, we will cover: an overview of the available Web policies; an overview of the Zscaler Data Loss Prevention (DLP) capabilities; a look at the Zscaler configuration options and steps for DLP; a detailed look at the preliminary configurations necessary to enforce DLP policy; and a detailed look at how to create DLP policy rules.

Slide 4 - Web Policy Overview

Slide notes

The first topic we will cover is an overview of the available Web policies.

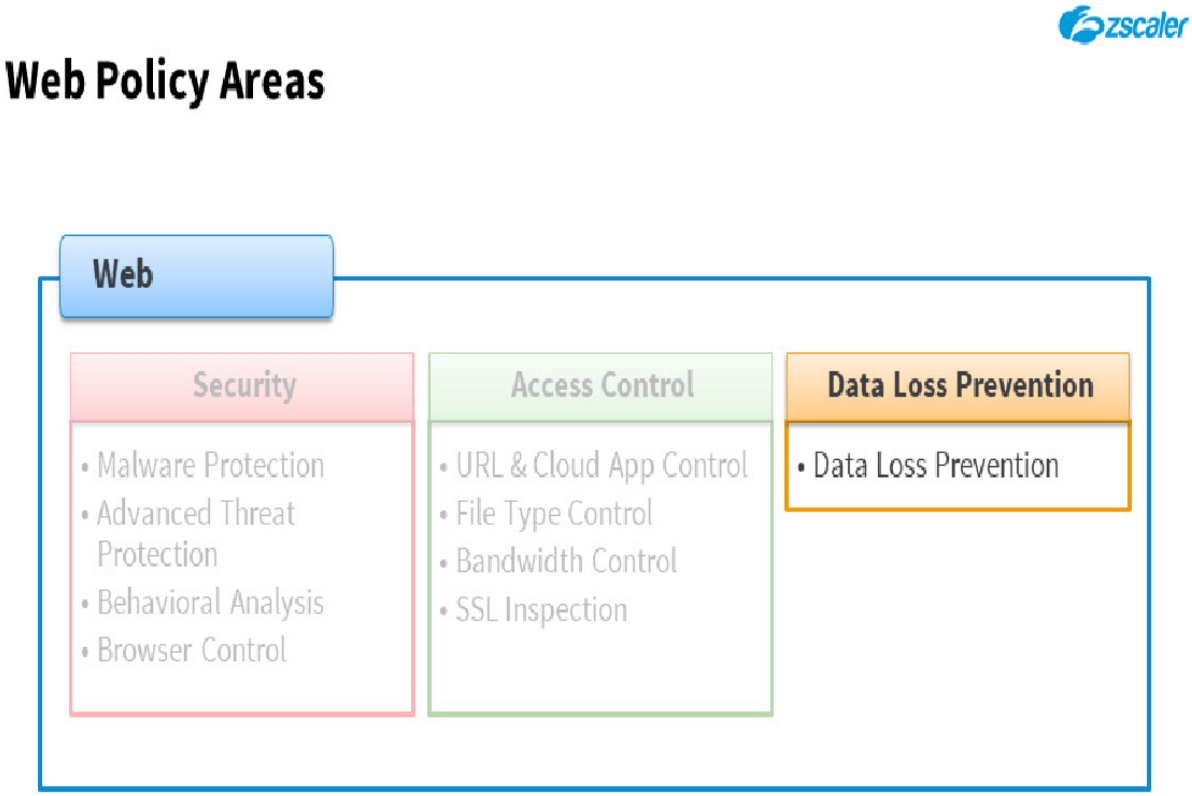
Slide 5 - Web Policy Areas



Slide notes

The Web policy area is the most extensive of the policy areas, and allows the creation of **Security**, **Access Control** and **Data Loss Prevention** policies.

Slide 6 - Web Policy Areas



Slide notes

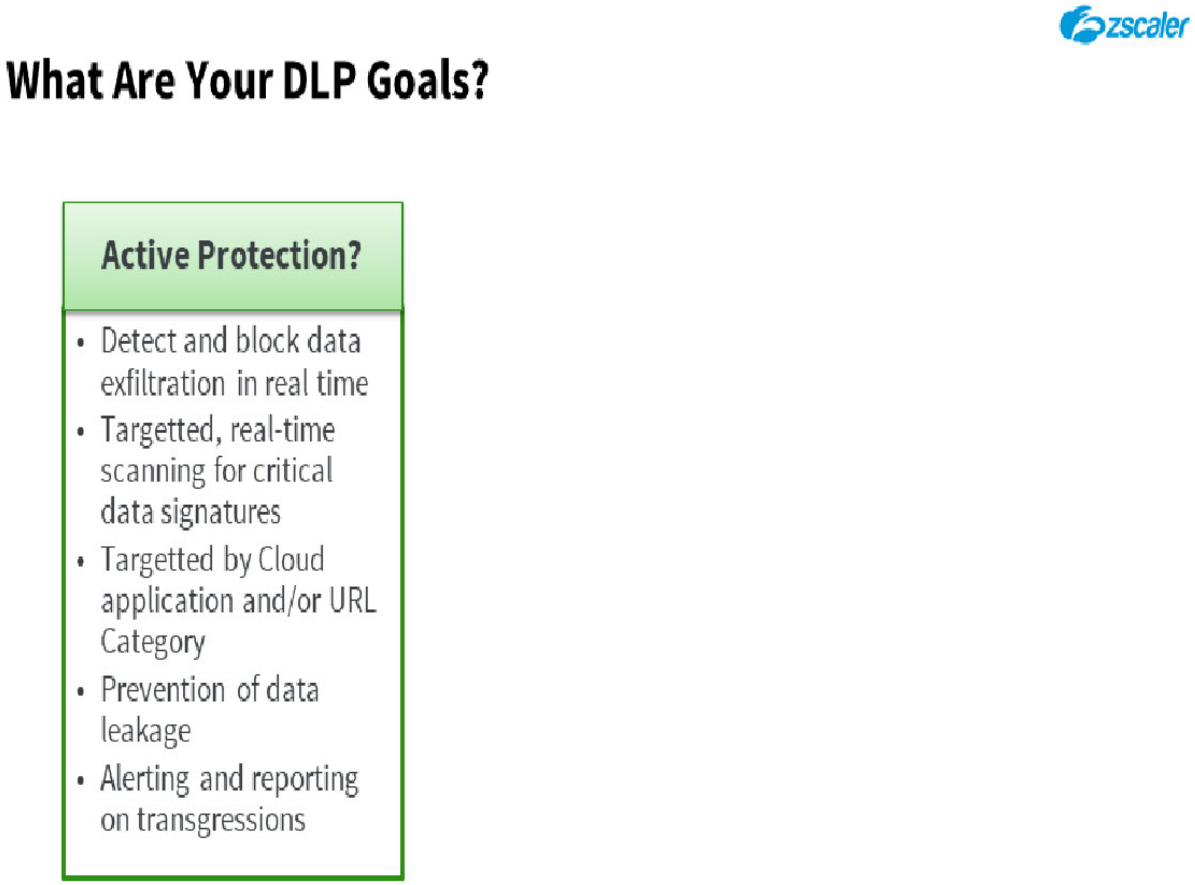
In this module, we will look in detail at the **Data Loss Prevention** category, and provide some recommendations for the policy settings.

Slide 7 - Web Policy Overview – DLP

Slide notes

The next topic we will cover is an overview of the Zscaler DLP capabilities.

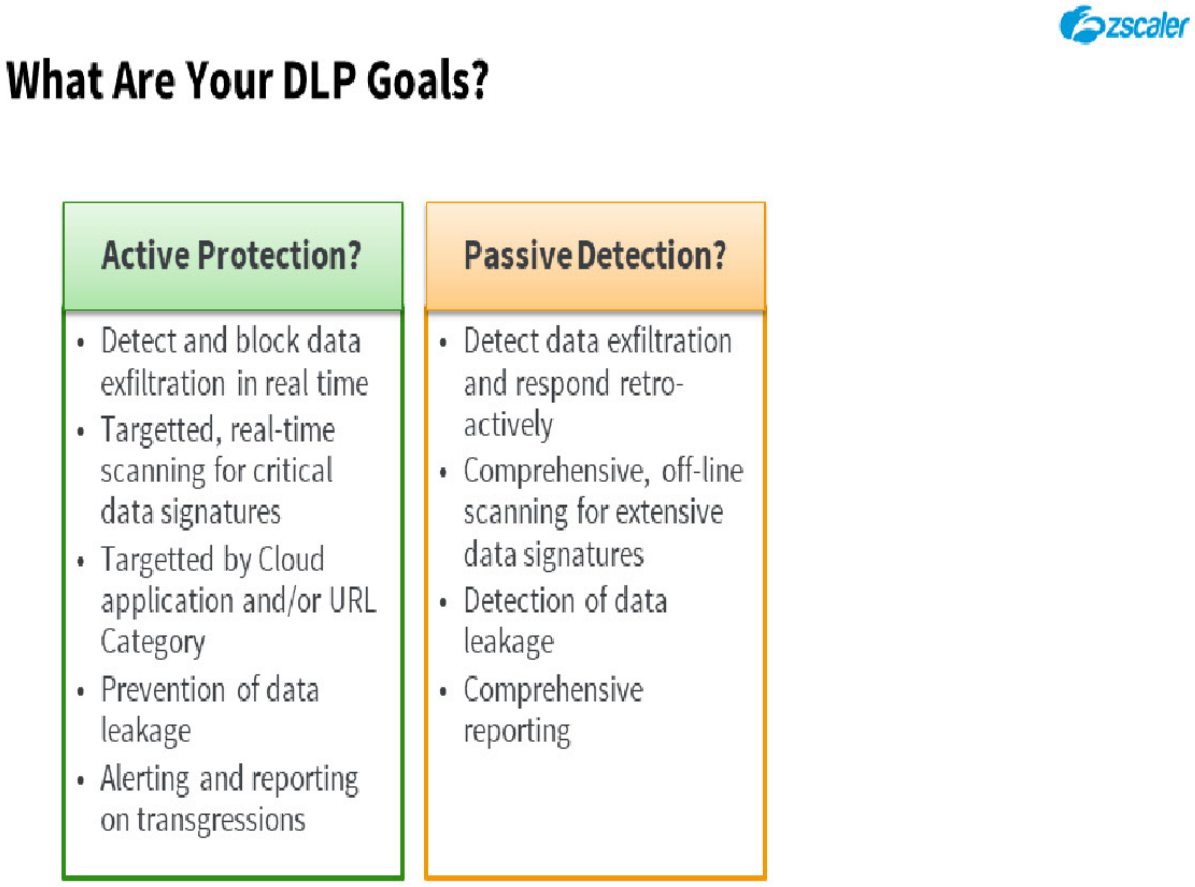
Slide 8 - What Are Your DLP Goals?



Slide notes

Before configuring DLP on Zscaler, you must have a clear understanding of what it is you want to achieve with this functionality. Do you need active, real-time protection? …with targeted traffic being scanned for critical data signatures on exit from the corporate environment, and any offending data blocked before it can leave the organization.

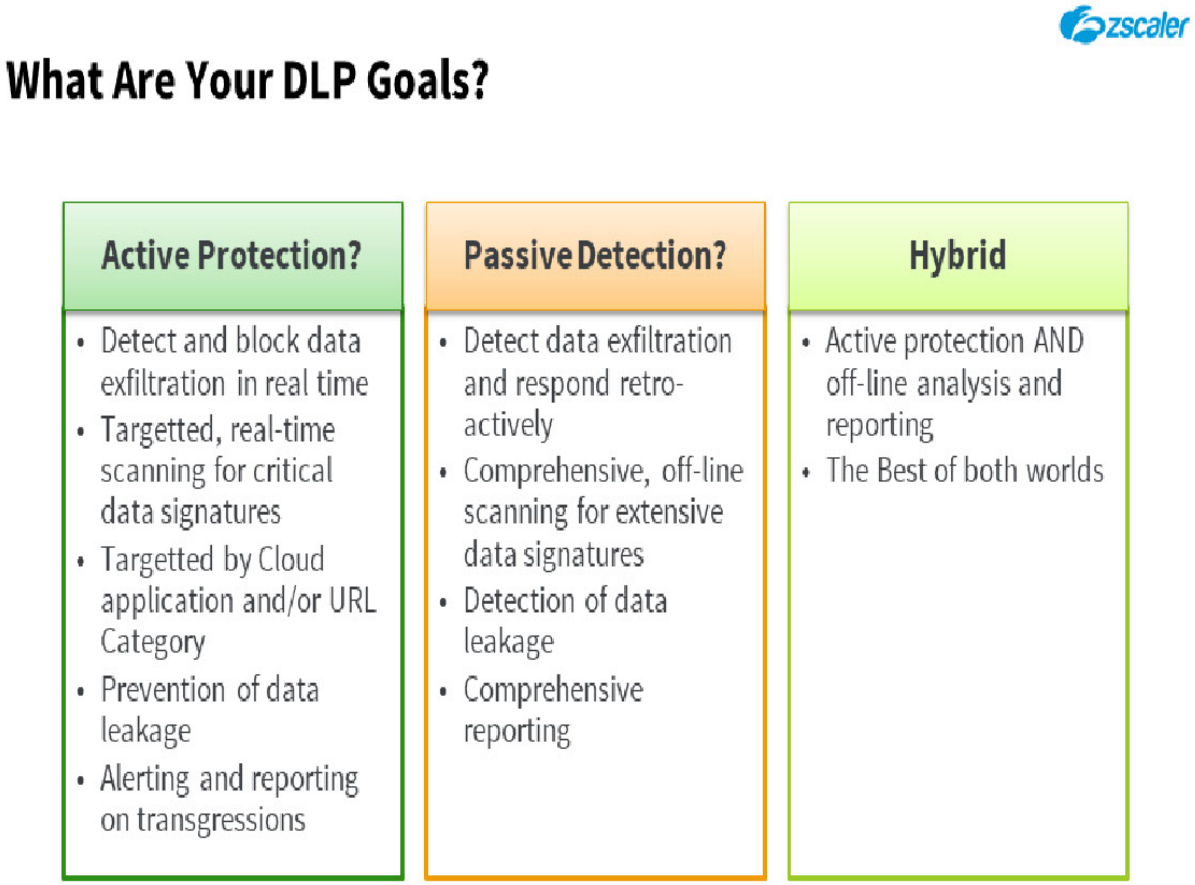
Slide 9 - What Are Your DLP Goals?



Slide notes

Or is it sufficient to passively monitor data on exit, and forward suspect transactions to an external system for off-line scanning with a more comprehensive set of data signatures ? Although this option only allows you to respond retro-actively to any suspected data exfiltration attempt.

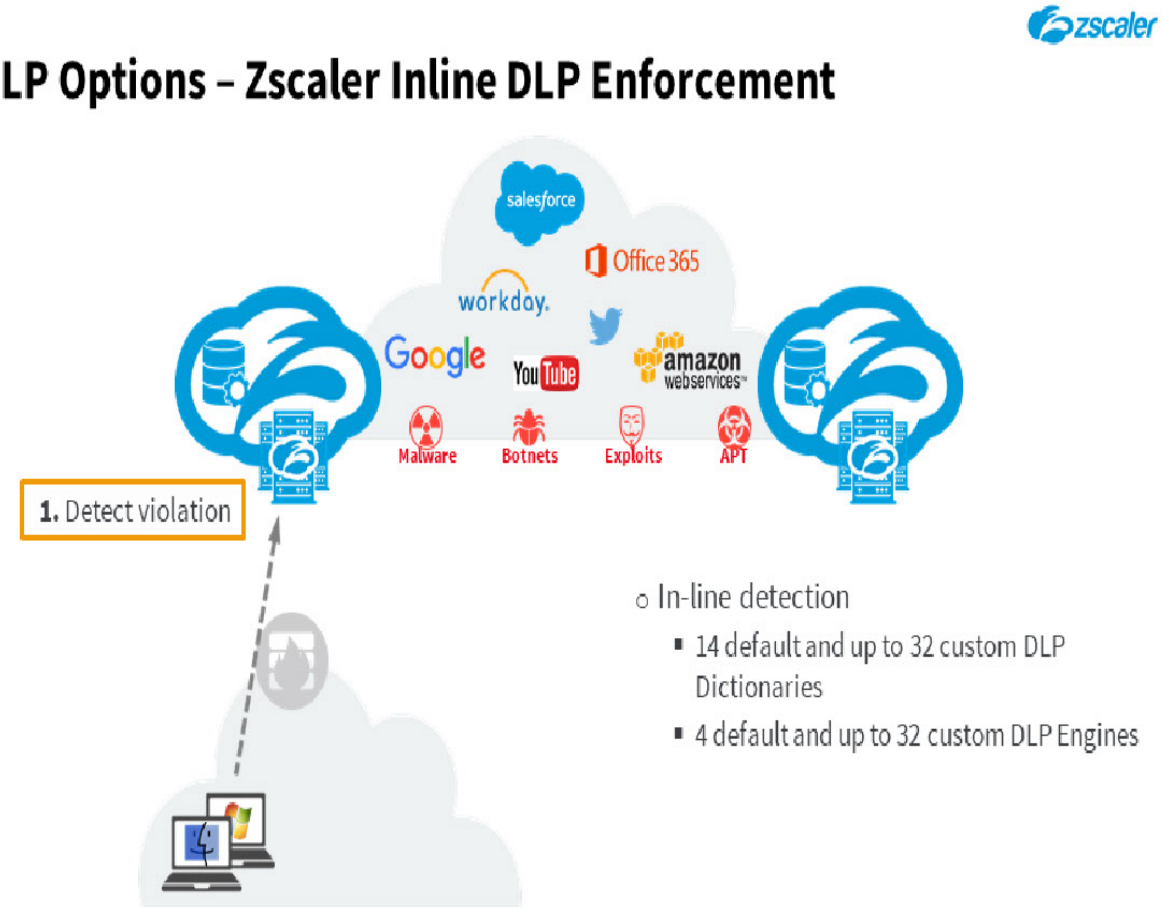
Slide 10 - What Are Your DLP Goals?



Slide notes

Or, do you need both capabilities? With real-time protection, AND detailed off-line scanning, analysis, and reporting.

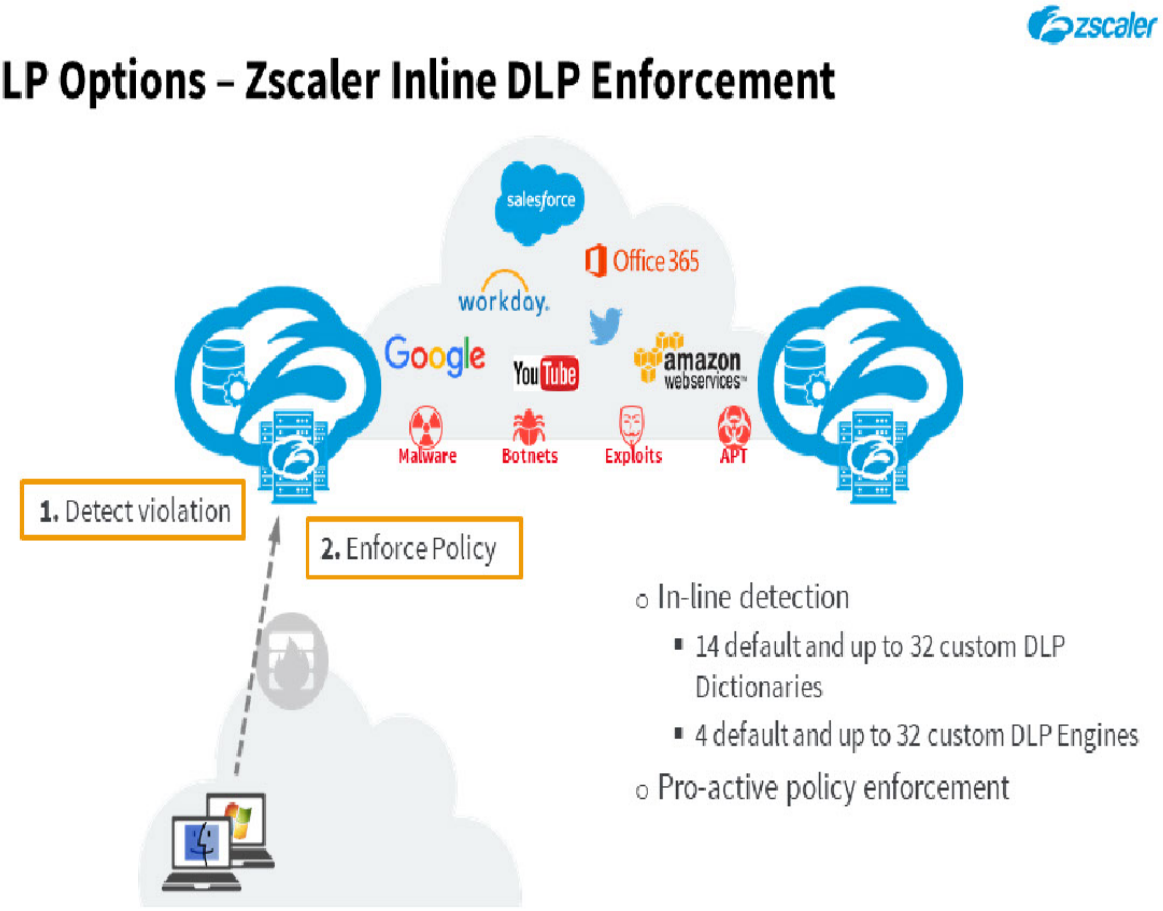
Slide 11 - DLP Options – Zscaler Inline DLP Enforcement



Slide notes

You can use Zscaler's DLP engines alone to scan for key data signatures in real-time as data exits the organization. You can create granular policy controls based on our 14 standard DLP **Dictionaries**, and 4 default **Engines**, or easily create custom definitions that you can tailor for your industry, and propagate through the Zscaler cloud in minutes.

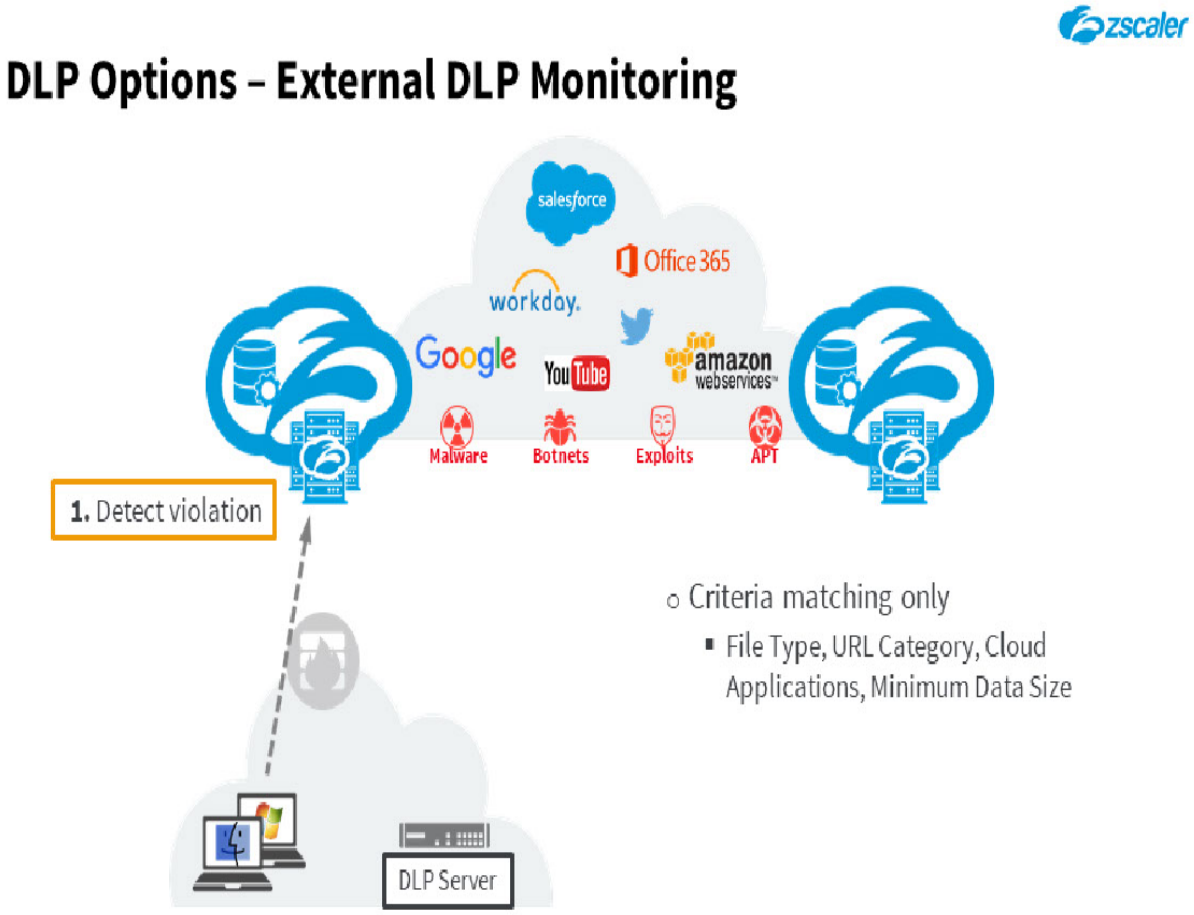
Slide 12 - DLP Options – Zscaler Inline DLP Enforcement



Slide notes

Using Zscaler DLP you can: allow transactions, or block them before the data has actually left the company; can notify your organization's auditor whenever a user's transaction triggers a DLP rule; plus, detailed logs are accessible for you in real time. With the Zscaler DLP solution you can ensure that you comply with industry, statutory, and regulatory criteria, such as HIPAA, PCI, and EU Data Privacy regulations.

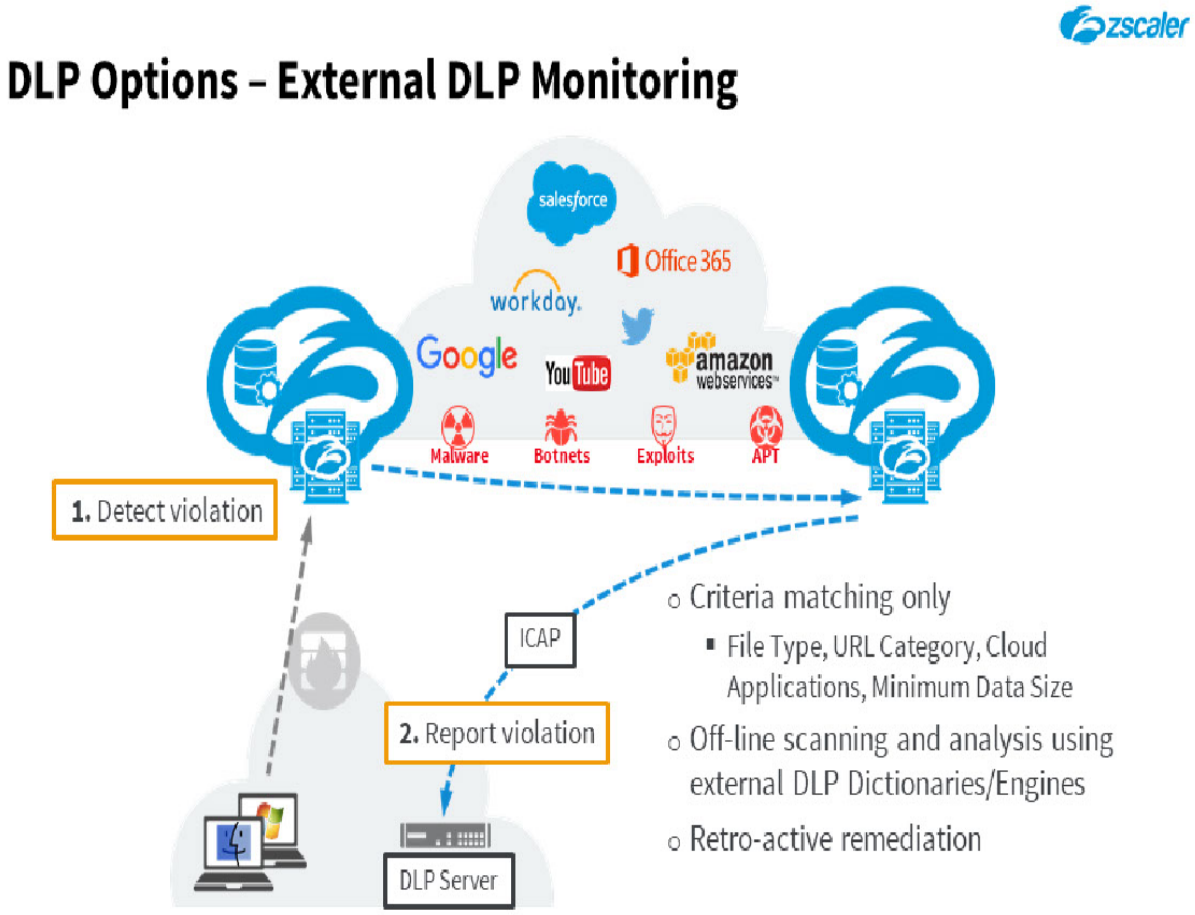
Slide 13 - DLP Options – External DLP Monitoring



Slide notes

Alternatively, you can configure Zscaler to simply detect a possible transgression and report it to an existing on-premise, or cloud-based DLP system using the Internet Content Adaptation Protocol (ICAP). In this scenario, Zscaler does not scan the content with its own DLP engines but simply acts as a filter, and triggers based on the configured criteria. Zscaler can also block traffic based on the criteria, although without the use of the Zscaler DLP engines, this would be a fairly hit-or-miss process.

Slide 14 - DLP Options – External DLP Monitoring



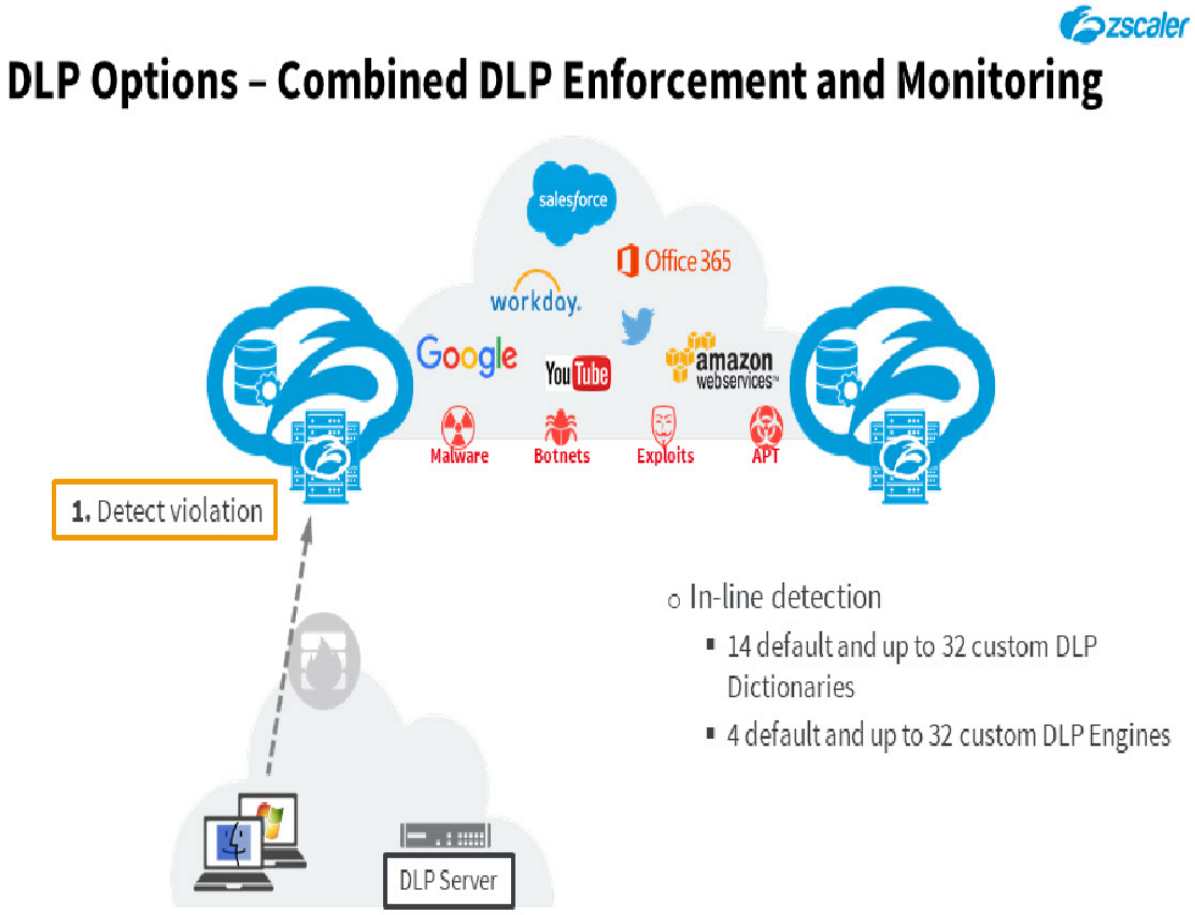
Slide notes

Suspect traffic is forwarded to your existing on premise (or cloud-based) DLP server, so that your organization can perform detailed analysis off-line as necessary, leveraging a comprehensive set of external DLP Dictionaries and Engines.

The forwarding is actually done through a ZEN on another cloud that we use for sending communications to your DLP servers, and to protect your organization's data, Zscaler recommends that you have the ZEN send the suspect transactions in encrypted form, using secure ICAP.

As many DLP servers can only read unencrypted information, Zscaler recommends installing an open-source application called stunnel. Once stunnel is installed on the DLP server, it can establish an SSL connection to the ZEN which can then send transaction information in encrypted form.

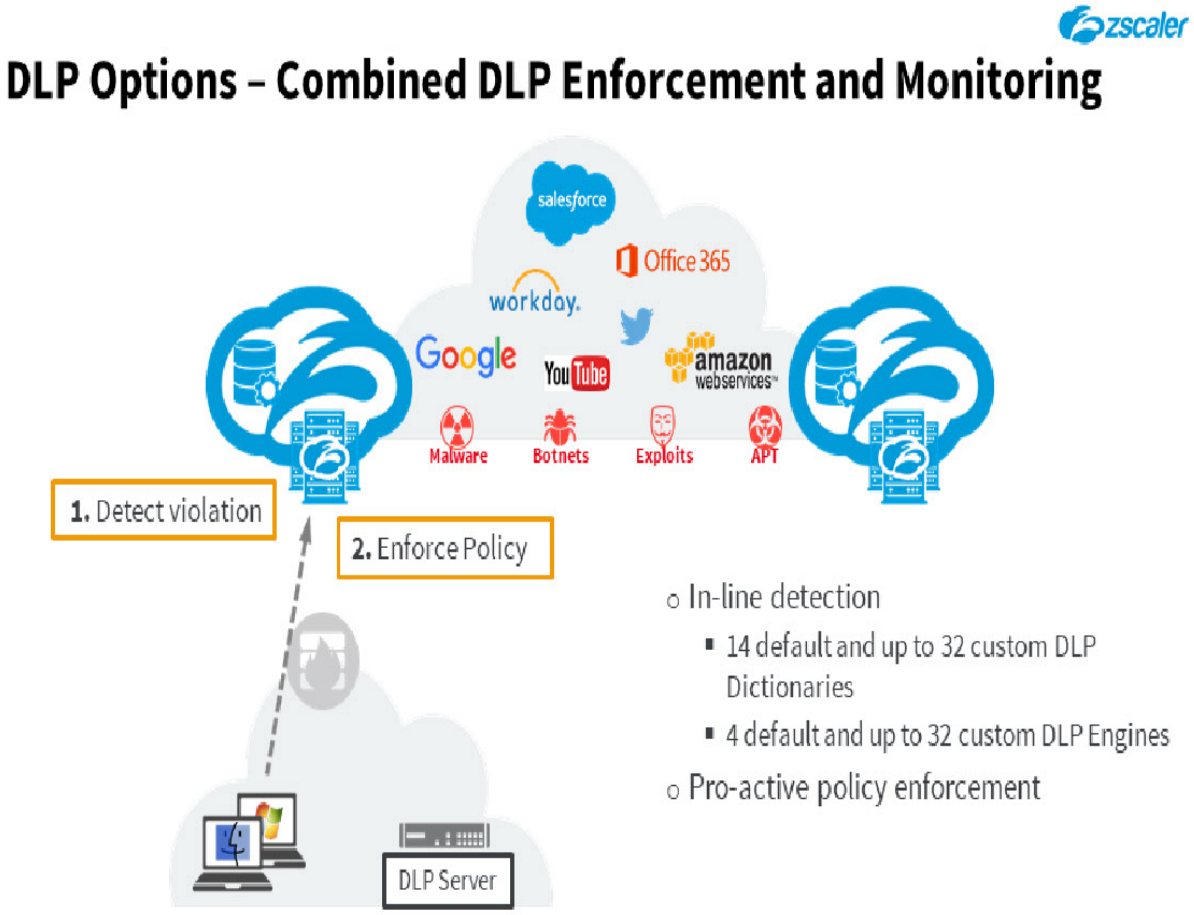
Slide 15 - DLP Options – Combined DLP Enforcement and Monitoring



Slide notes

For comprehensive DLP functionality, you can implement both models simultaneously; using Zscaler DLP Engines to scan in real time…

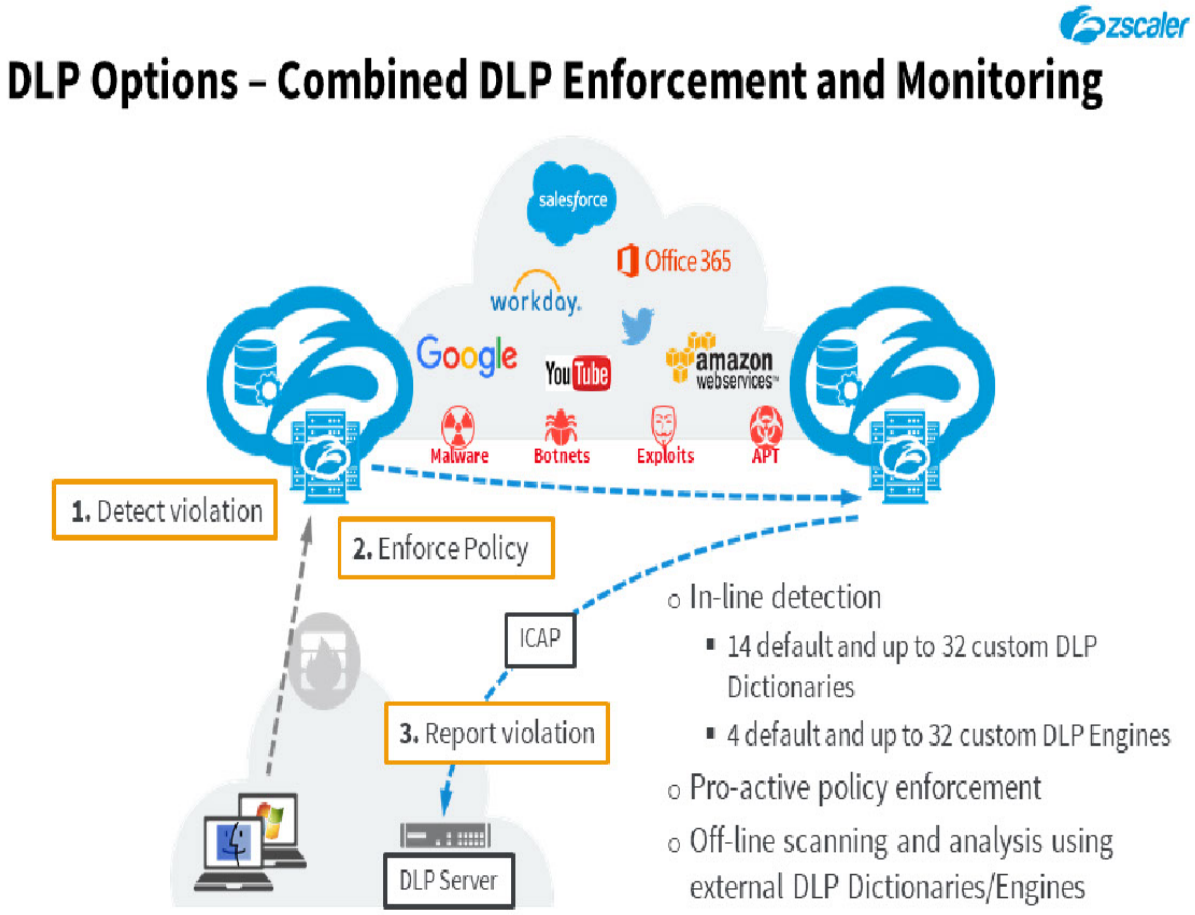
Slide 16 - DLP Options – Combined DLP Enforcement and Monitoring



Slide notes

…enforcing policy immediately;

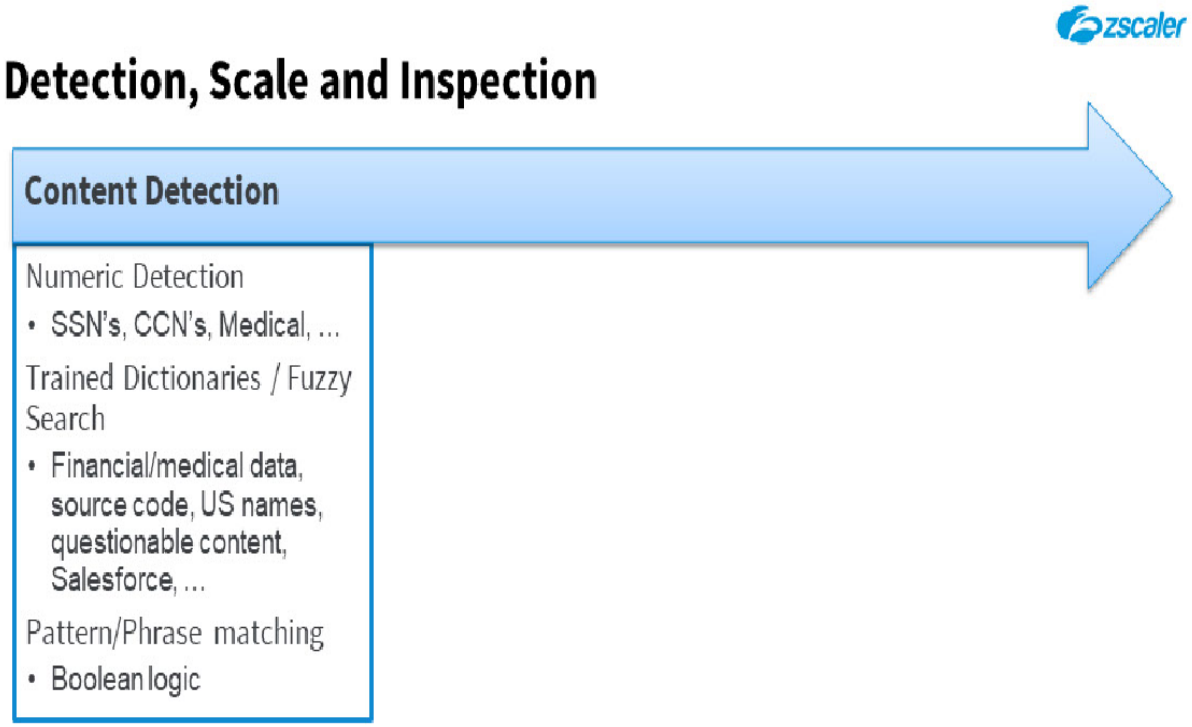
Slide 17 - DLP Options – Combined DLP Enforcement and Monitoring



Slide notes

…and forwarding any matching transactions to your on premise DLP solution for detailed analysis and reporting.

Slide 18 - Detection, Scale and Inspection

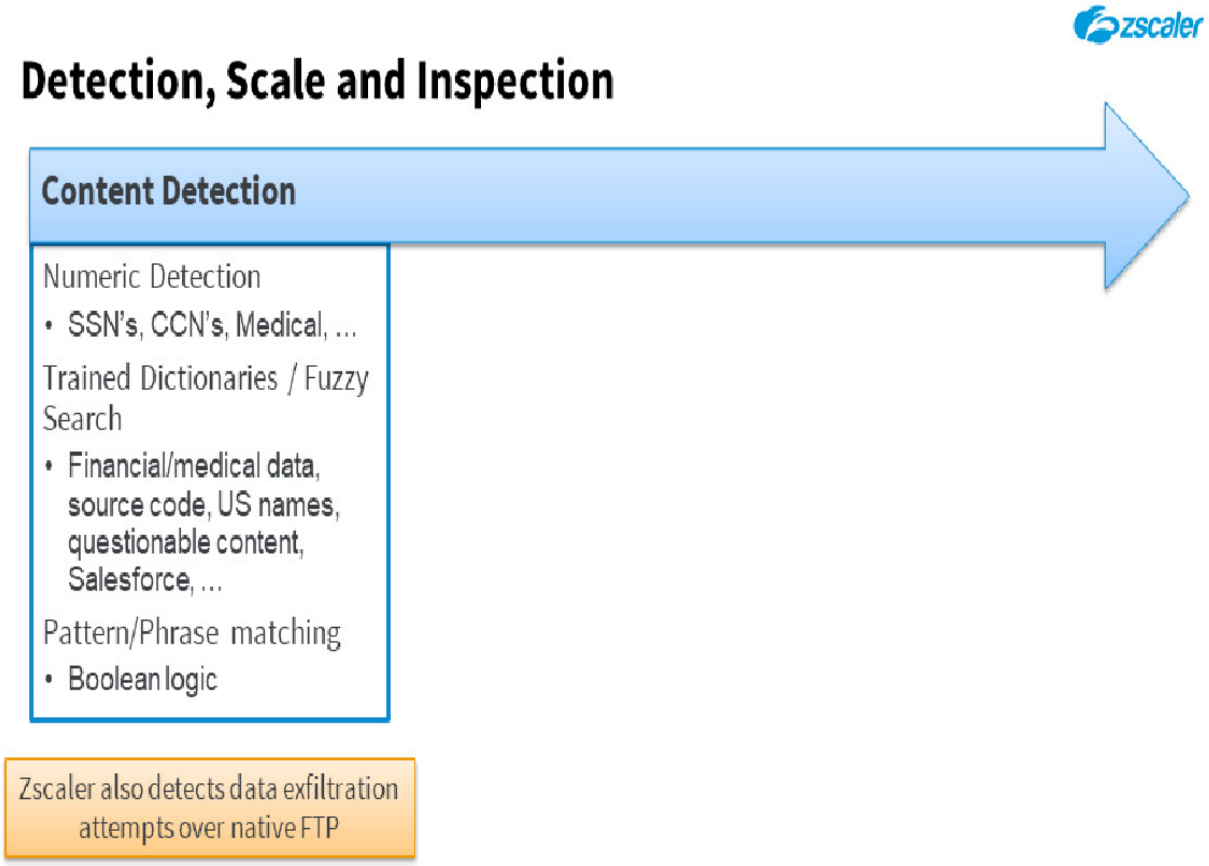


Slide notes

Zscaler DLP **Dictionaries** allow the detection of a wide range of data signatures, including; SSNs, CCN's, UK National Insurance numbers, Canadian CSIN's, and Singapore NRIC's.

Custom Dictionaries can be created with **fuzzy search** criteria to match financial, or medical data, source code, US names, questionable content, Salesforce data, or any other signatures that you care to define. Data patterns, specific phrases, or both may be defined in Zscaler dictionaries, and combined by a Boolean AND operation in a Zscaler **Engine**.

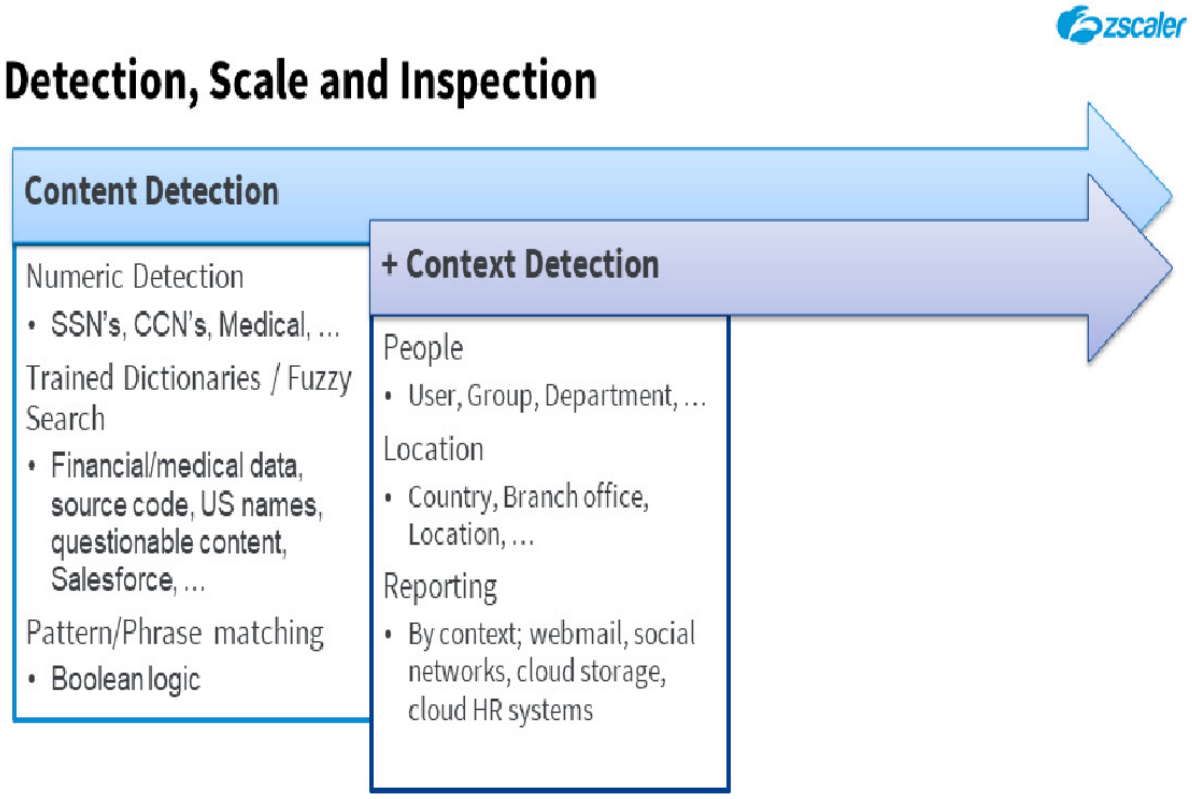
Slide 19 - Detection, Scale and Inspection



Slide notes

Note that Zscaler also detects attempts to exfiltrate data over the native FTP protocol.

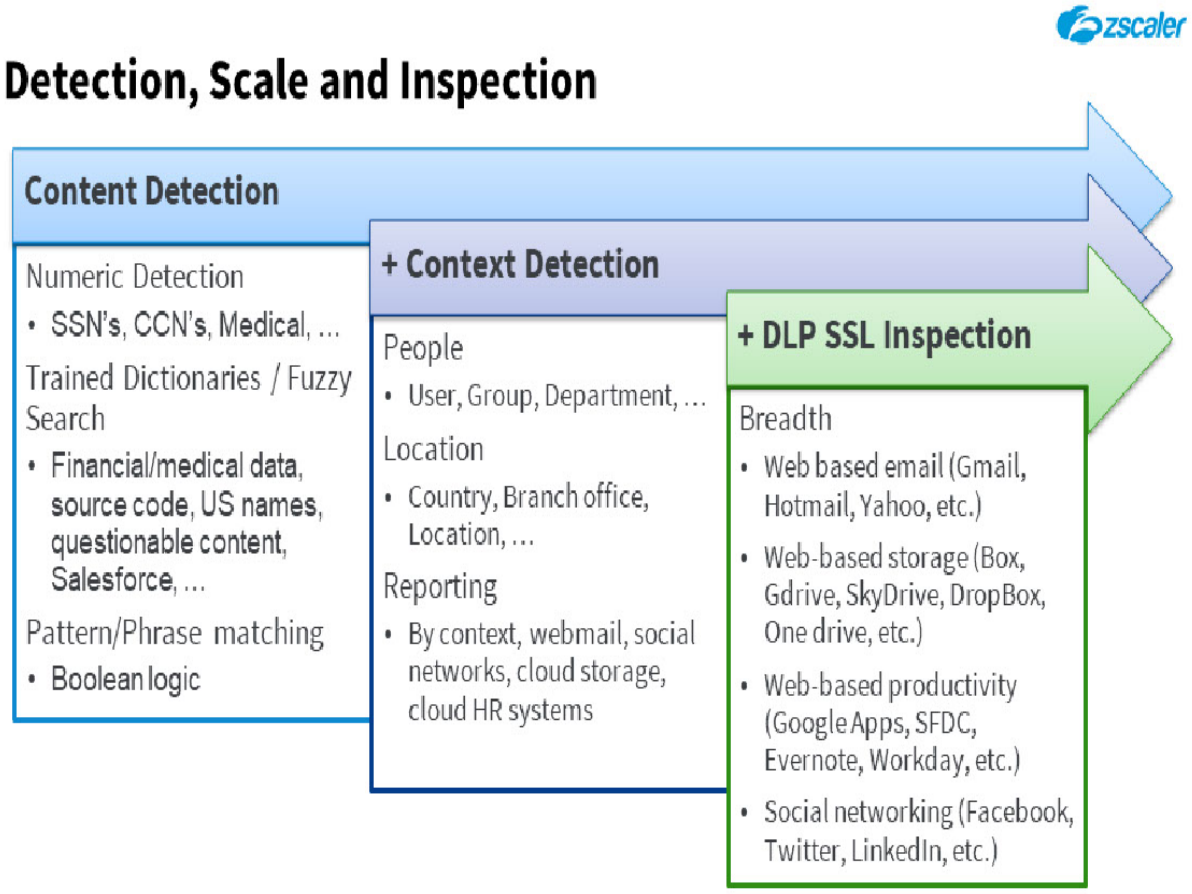
Slide 20 - Detection, Scale and Inspection



Slide notes

Both content, and context criteria can be combined in a Zscaler DLP policy rule to match keywords, phrases, or patterns generated by specific **Users**, **Groups**, **Departments** or **Locations**, and within defined **Time** intervals if necessary. Detailed reporting is available by cloud application (such as **Webmail**, **Social Networking**, **Cloud Storage**), and by context (**User**, **Group**, **Department** or **Location**).

Slide 21 - Detection, Scale and Inspection



Slide notes

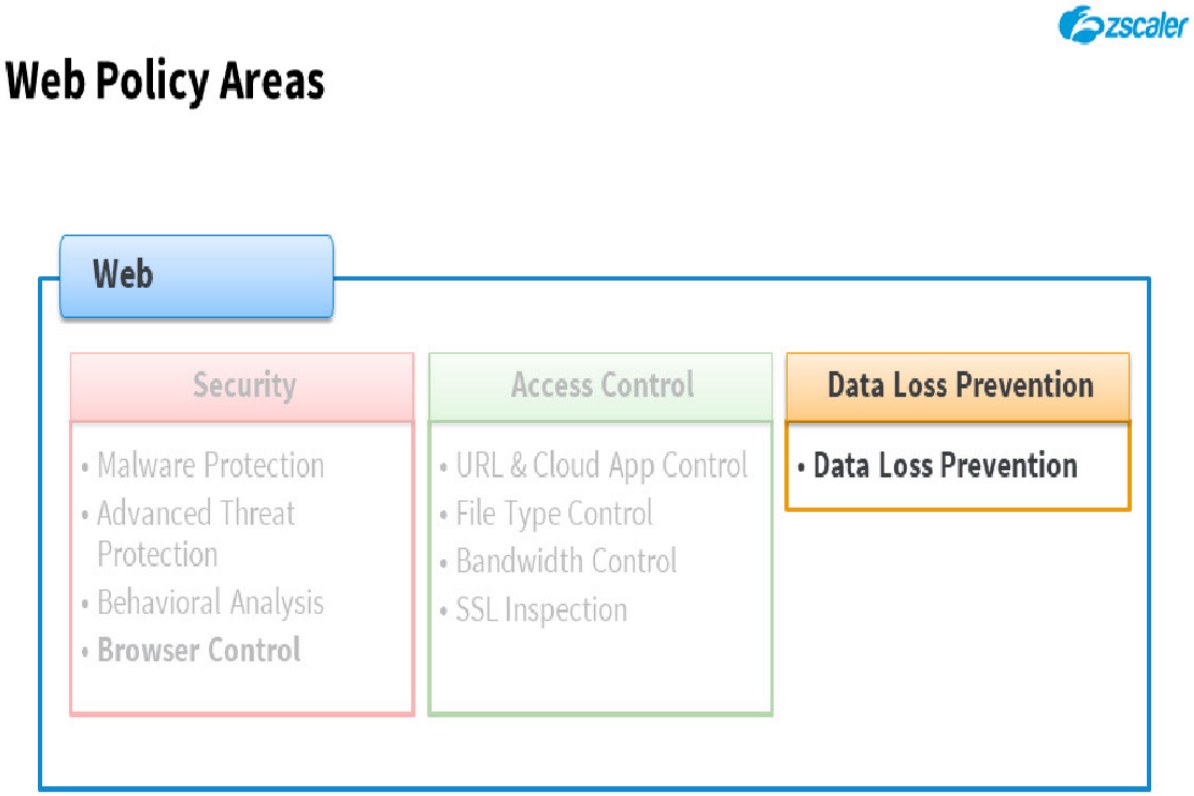
In addition, with SSL Inspection enabled, Zscaler DLP can detect data signatures and apply policy to all traffic, whether it is encrypted or not. We can inspect: Web-based email providers such as Gmail, Hotmail, or Yahoo; Web-based storage repositories such as Box, Google Drive, SkyDrive, Dropbox, or One drive; Web-based productivity tools like Google Apps, Salesforce.com, Evernote, Workday, or ServiceNow; and even Social Networking platforms like Facebook, LinkedIn, or Twitter.

Slide 22 - DLP Configuration Options and Steps

Slide notes

In the next section we will have a detailed look at the DLP configuration options and steps available on the Zscaler platform.

Slide 23 - Web Policy Areas

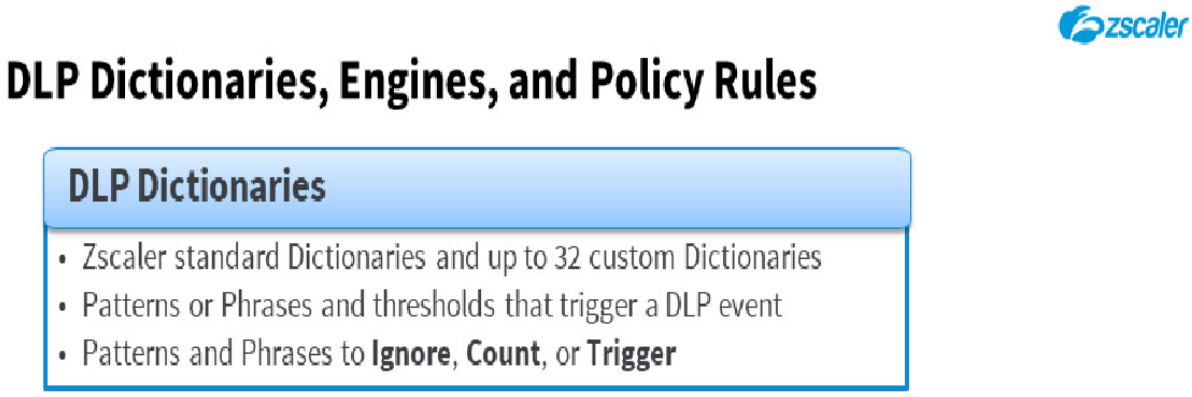


Slide notes

Data Loss Prevention Policy is a part of the Web policy configuration, and allows you to create rules to protect your organization from data loss.

Corporate data can be leaked in different ways; through Webmail, cloud storage, social media, and a variety of other applications. To protect your organization from data loss, Zscaler provides you with the following options for DLP policy: you may use Zscaler DLP **Engines** only; forward information to your on premise (or cloud-based) DLP server using the ICAP protocol; or use a combination of both methods.

Slide 24 - DLP Dictionaries, Engines, and Policy Rules



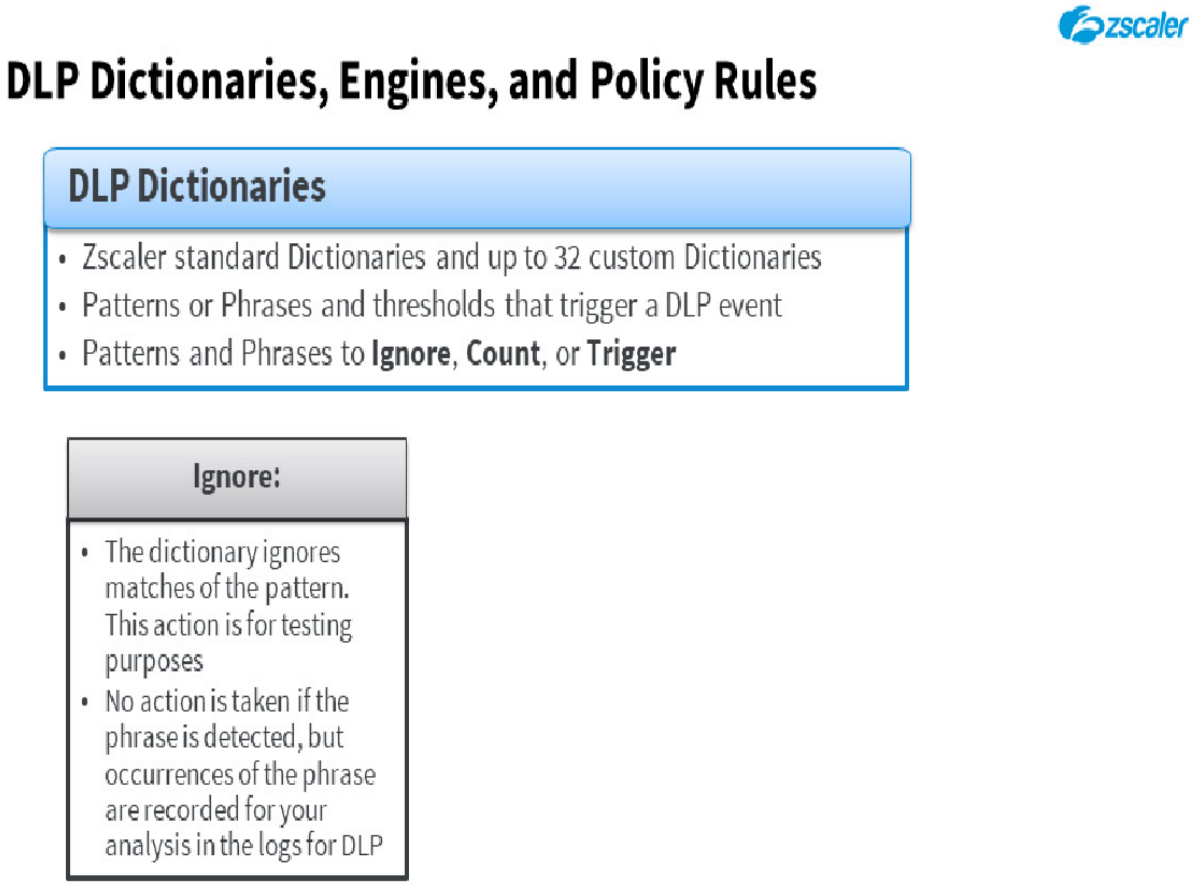
Slide notes

First of all, we need to look at the relationship between Zscaler DLP **Dictionaries**, **Engines**, and Policy Rules.

A DLP **Dictionary** contains a set of patented algorithms that are designed to detect specific kinds of information in your users' traffic. These predefined Dictionaries can be modified, and you can also create up to 32 additional, custom Dictionaries for content not covered by the standard dictionaries.

For each Dictionary, you can add custom phrases and alphanumeric patterns that represent the content you want to protect, and define the **Action** to be taken, whether to; **Ignore**, **Count**, or **Trigger**.

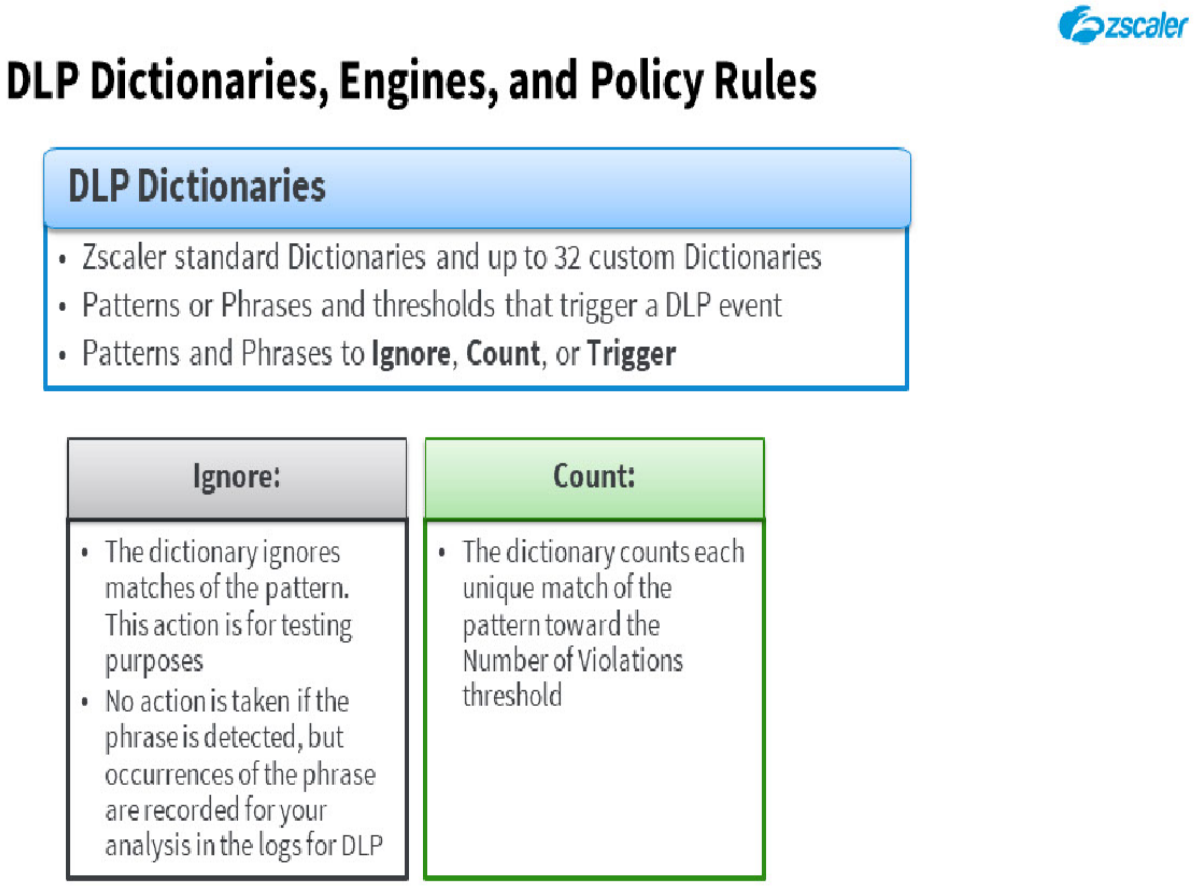
Slide 25 - DLP Dictionaries, Engines, and Policy Rules



Slide notes

The **Ignore** option is really there for testing purposes, no action is taken but the system will record any matches for analysis in the DLP Logs.

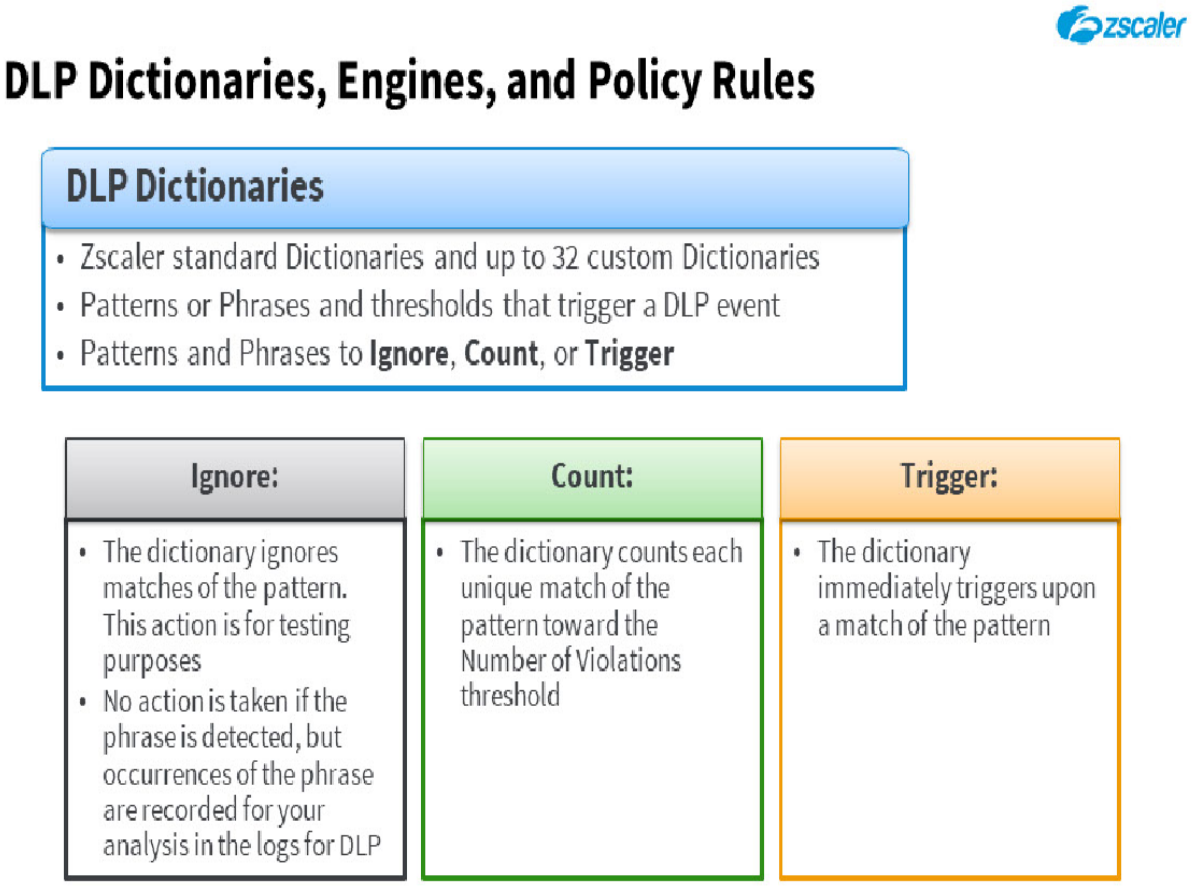
Slide 26 - DLP Dictionaries, Engines, and Policy Rules



Slide notes

The **Count** option adds each occurrence of a **Phrase** or **Pattern** to the violations total, and an event is triggered if the total reaches the specified **Number of Violations Threshold**.

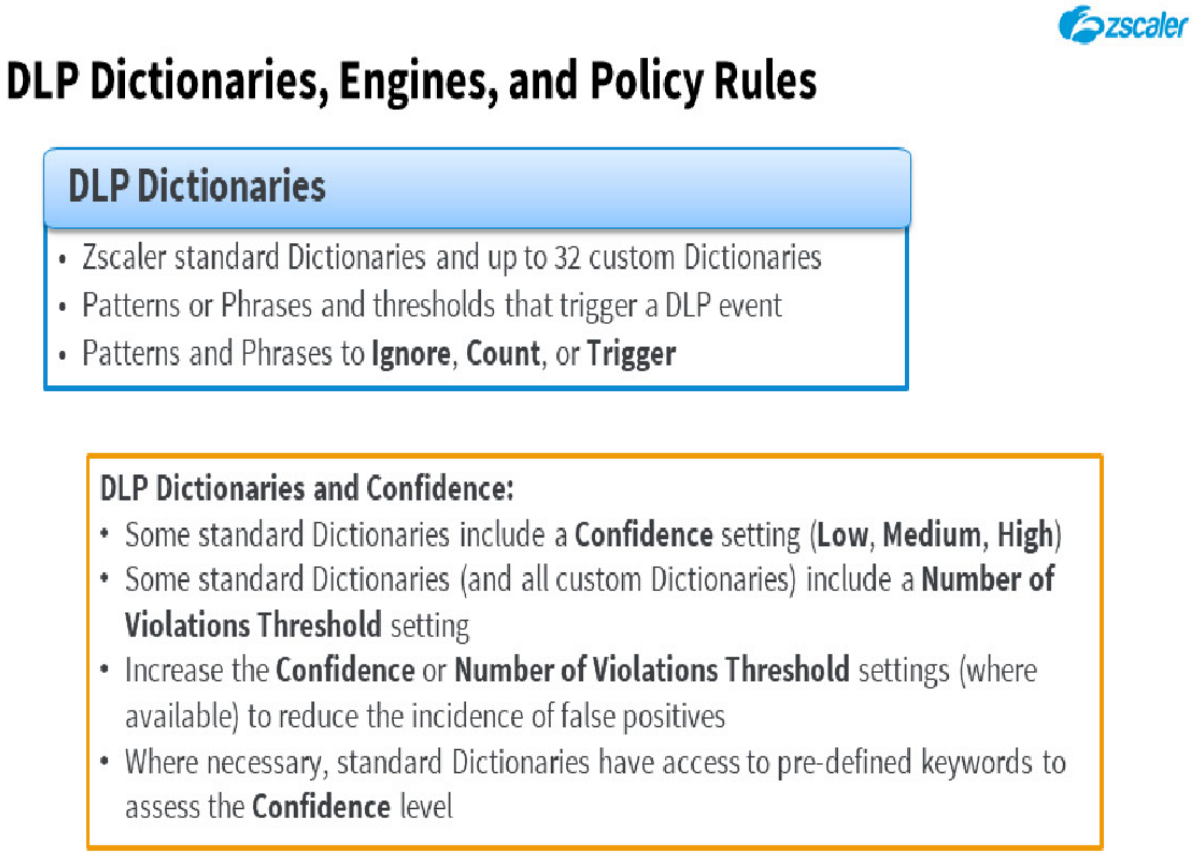
Slide 27 - DLP Dictionaries, Engines, and Policy Rules



Slide notes

The **Trigger** option, triggers an event immediately on detection of the **Phrase** or **Pattern**.

Slide 28 - DLP Dictionaries, Engines, and Policy Rules



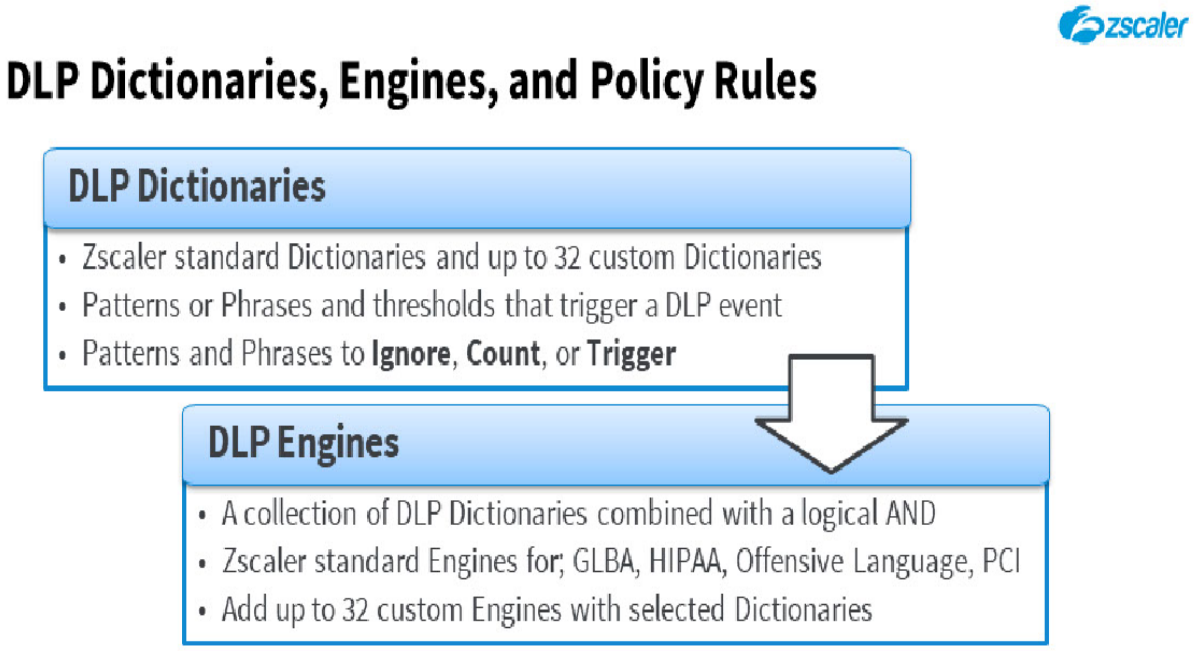
Slide notes

Some of the standard Dictionaries include a **Confidence** setting (**Low**, **Medium**, or **High**), plus some of the standard Dictionaries (and all your custom ones) also contain a **Number of Violations Threshold** configuration.

For the Standard Dictionaries these are set to default values, however these values can be fine-tuned to help to reduce the number of **false positives** triggered by the DLP Policy rules. The standard Dictionaries also have access to pre-defined keywords relevant to the type of Dictionary, that are used in assessing the **Confidence** level.

For example, the standard rule named **Credit Cards** is set to the Confidence level **Medium**, and requires **5 Violations** before it will trigger. If this still results in too many false positives, you have the option to either increase the **Number of Violations Threshold**, or the **Confidence** level.

Slide 29 - DLP Dictionaries, Engines, and Policy Rules

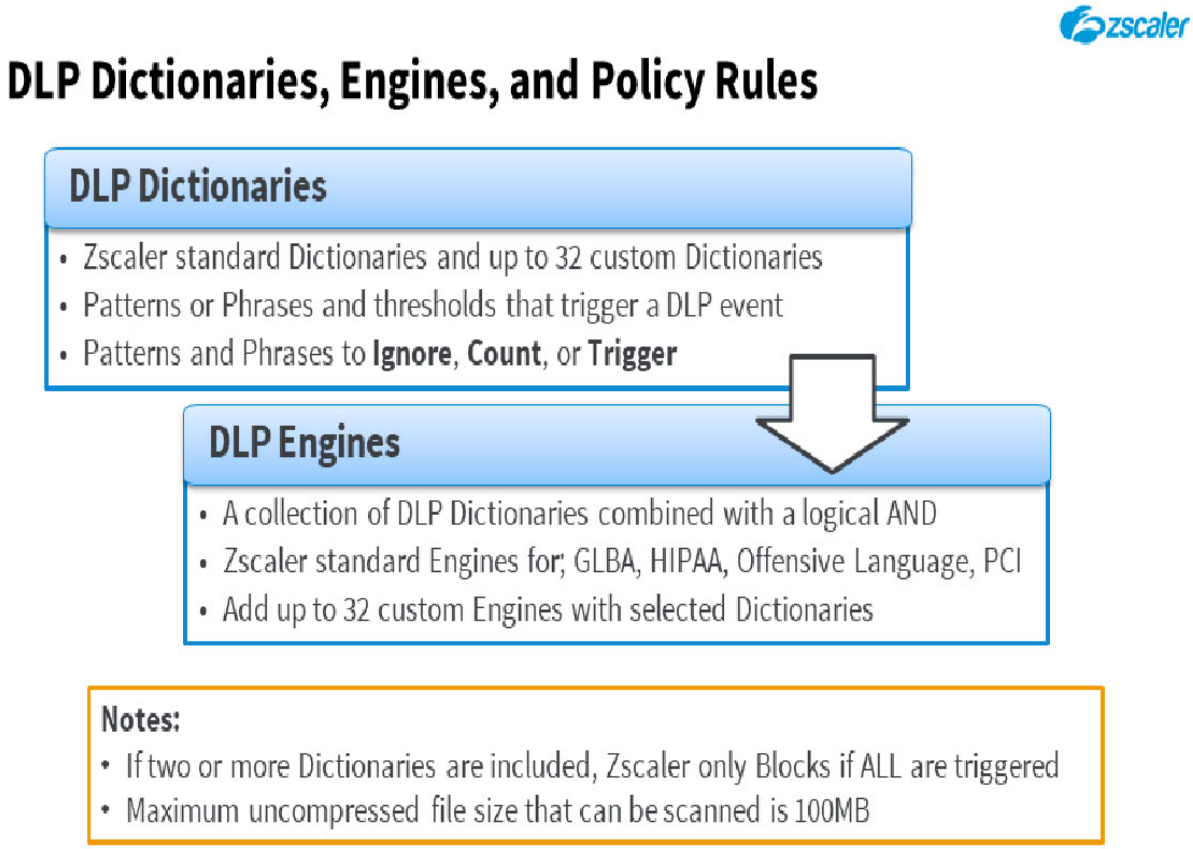


Slide notes

A DLP **Engine** is a collection of one or more DLP Dictionaries, and it is these Engines that you subsequently reference in your DLP Policy rules. By using a DLP Engine, you can create rules to detect content that encompasses more than one Dictionary.

For example, if your organization wants to protect social security AND credit card numbers simultaneously, you would create a rule using the PCI Engine, which contains the **Credit Cards** and **Social Security Numbers** Dictionaries.

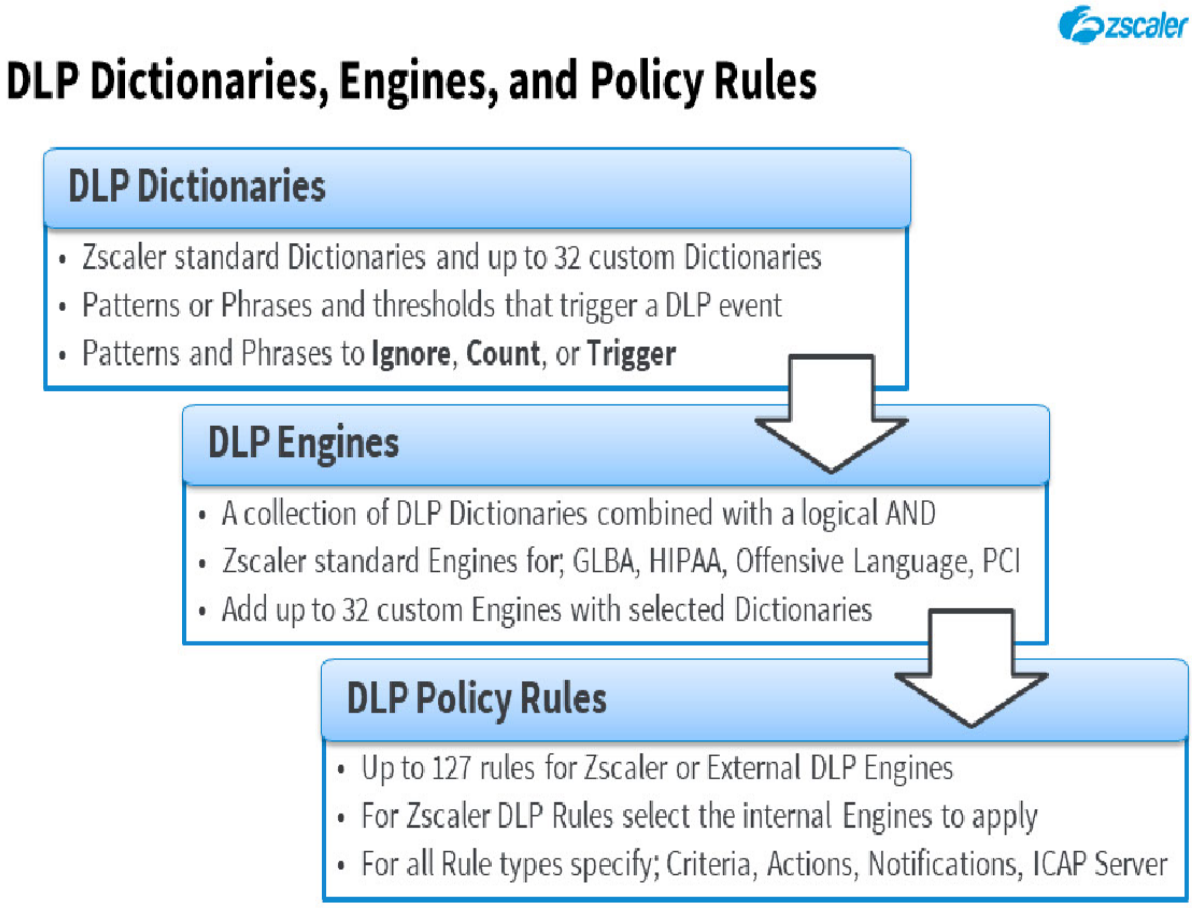
Slide 30 - DLP Dictionaries, Engines, and Policy Rules



Slide notes

Note that when a DLP Engine uses two or more Dictionaries, a logical **AND** operation is performed, so that Zscaler will only block content if ALL of the Dictionaries in the Engine are triggered. Also note that Zscaler DLP Engines can scan files with a maximum size of 100 MB.

Slide 31 - DLP Dictionaries, Engines, and Policy Rules

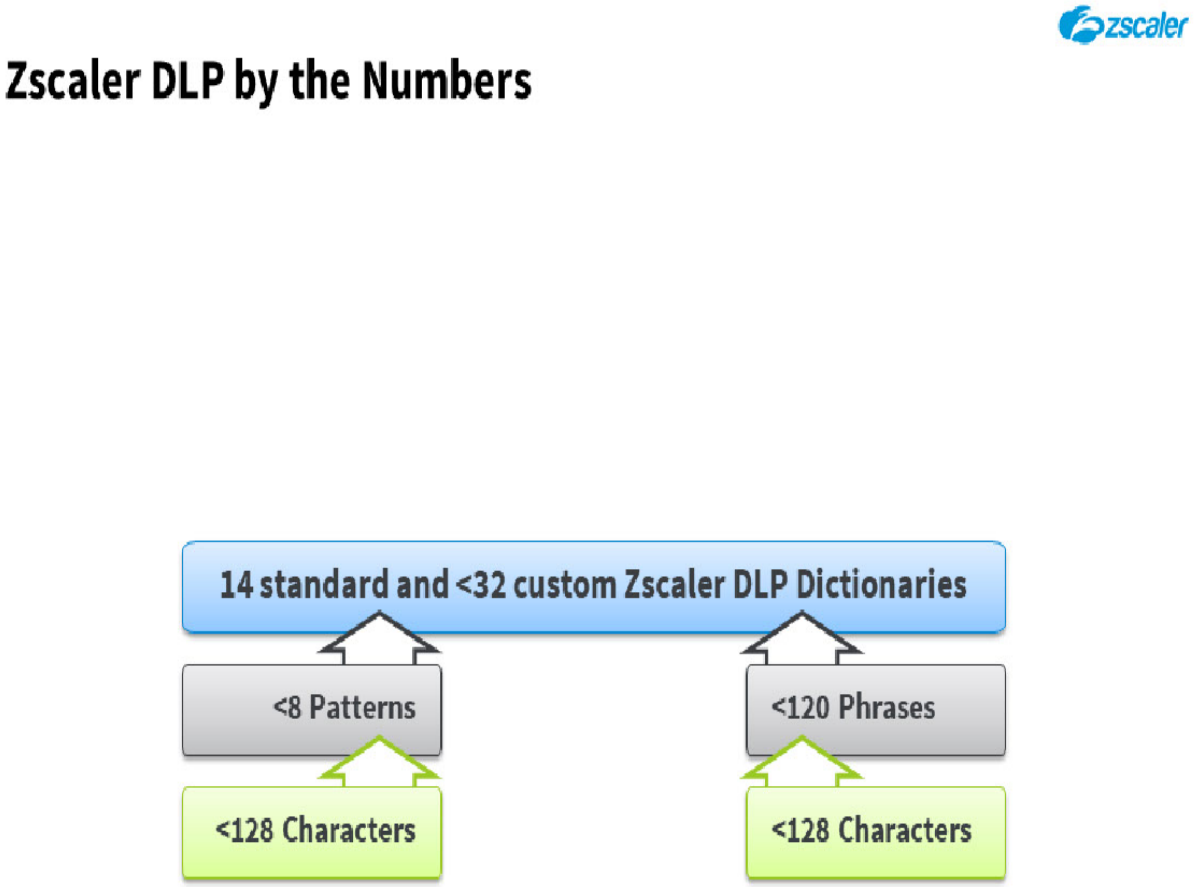


Slide notes

Having defined any custom DLP Dictionaries and/or Engines on the Zscaler platform, you can refer to the engines in a **Zscaler DLP Engine** Policy rule. This then allows you to detect matching data patterns, allow or block the transactions containing them, and notify your organization's auditor as required.

Plus, if you have an on-premise DLP solution, you can also forward content to it using secure ICAP so that external DLP Engines can perform further analysis of the data.

Slide 32 - Zscaler DLP by the Numbers

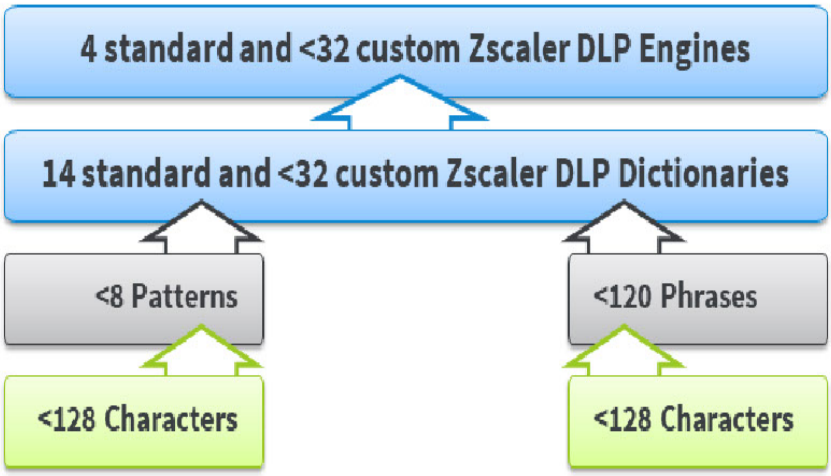


Slide notes

The Zscaler DLP environment provides 14 pre-defined DLP Dictionaries (for things like **Adult Content**, **Credit Cards**, and **Medical Information**), and we allow you to create up to 32 custom Dictionaries. Each of the custom Dictionaries may contain up to 120 **Phrases**, and/or up to 8 **Patterns**, with each **Phrase** or **Pattern** containing a maximum of 128 Characters.

Slide 33 - Zscaler DLP by the Numbers

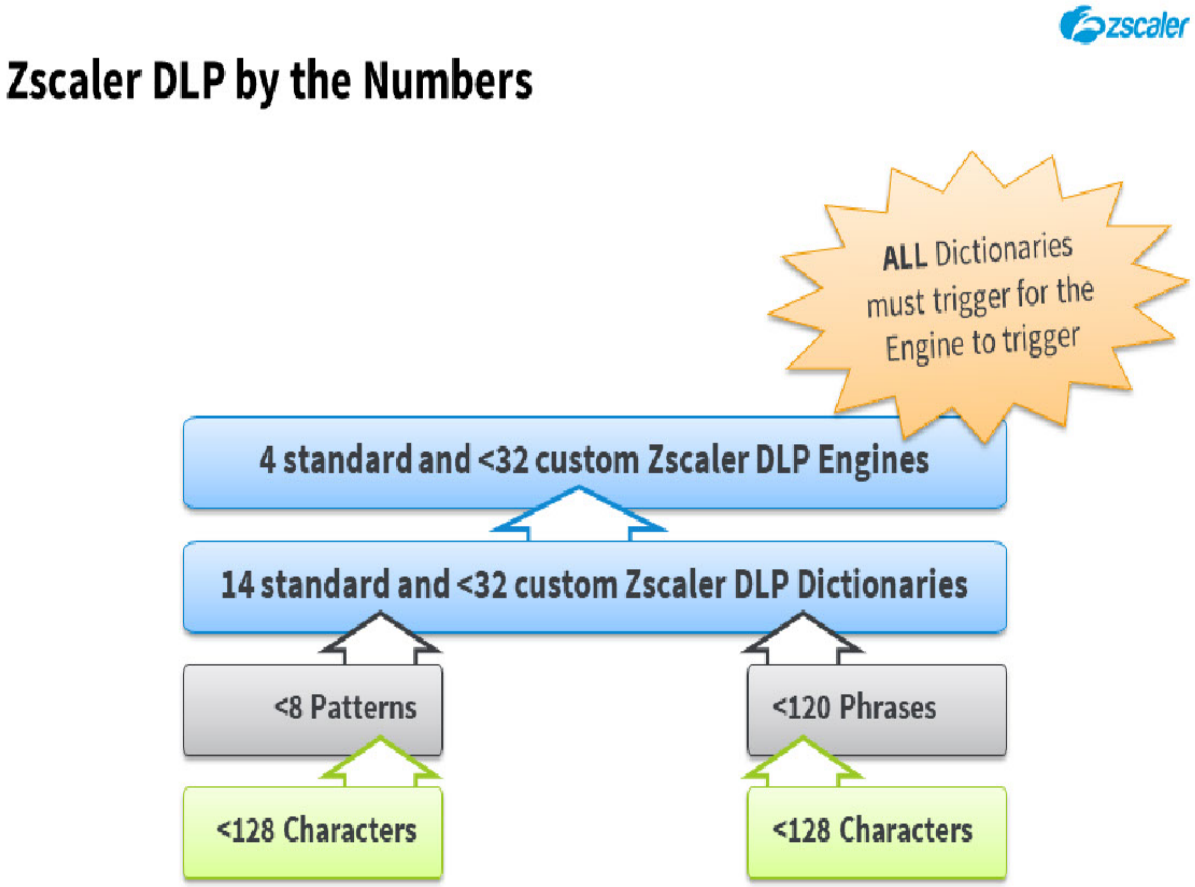
Zscaler DLP by the Numbers



Slide notes

We provide 4 standard DLP Engines for you (**GLBA**, **HIPAA**, **Offensive Language**, and **PCI**), and you may combine any of the DLP Dictionaries in up to 32 custom Engines.

Slide 34 - Zscaler DLP by the Numbers

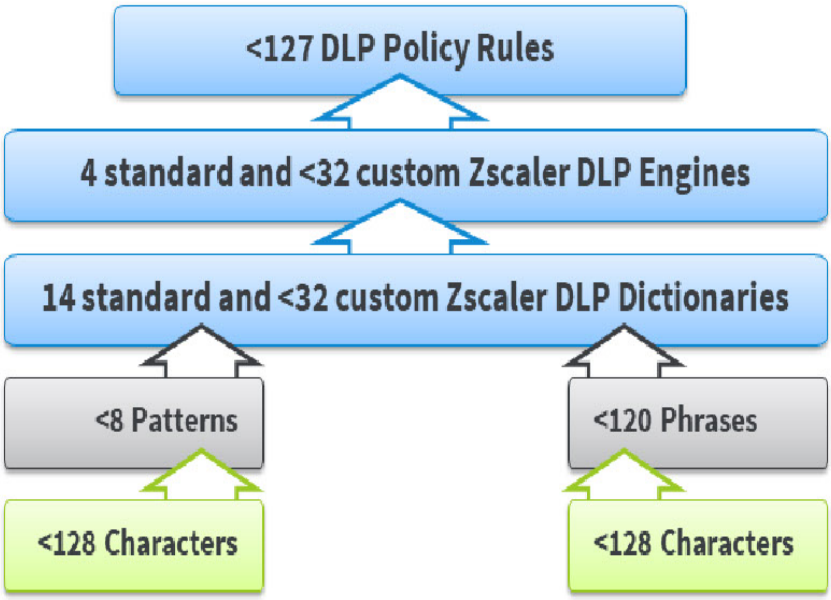


Slide notes

Note that all the Dictionaries added to an Engine must trigger for the Engine itself to trigger.

Slide 35 - Zscaler DLP by the Numbers

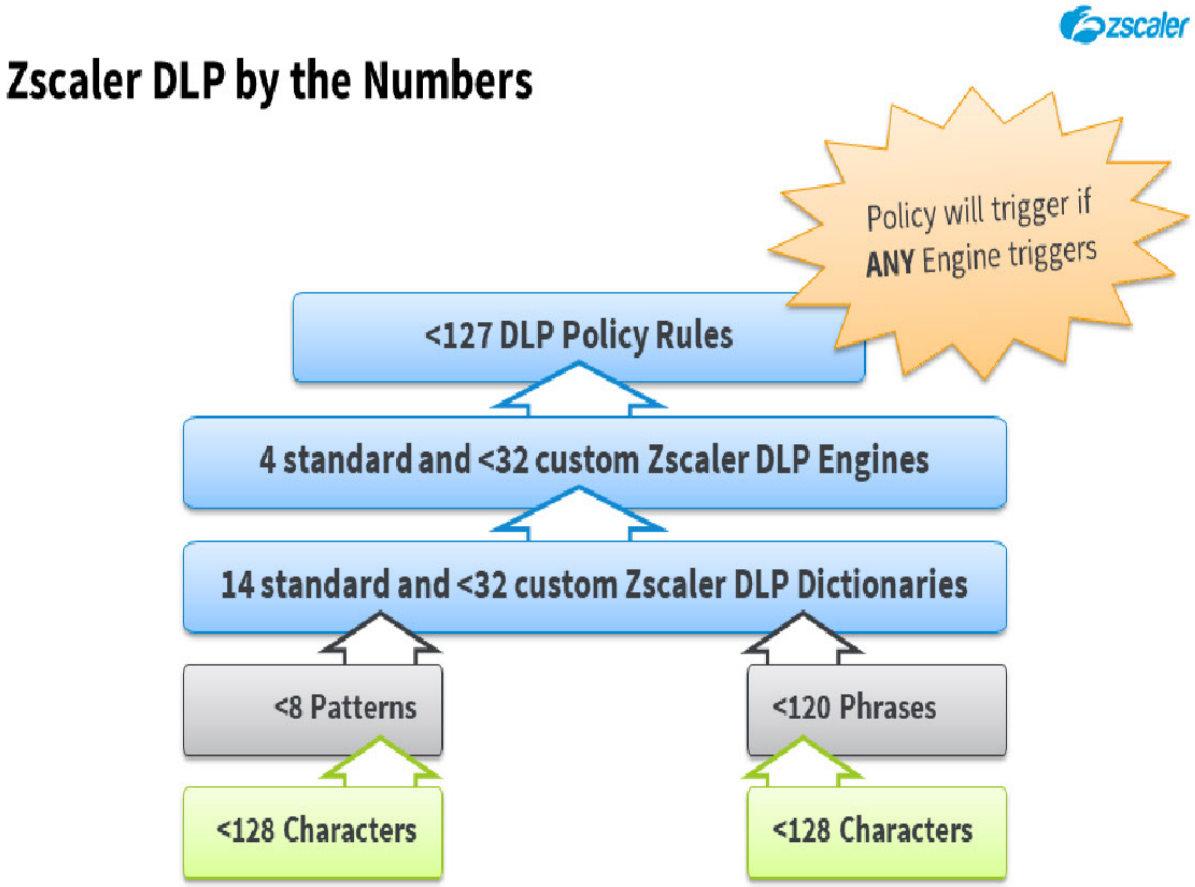
Zscaler DLP by the Numbers



Slide notes

Up to 127 DLP Policy rules may be created, and for the **Zscaler DLP Engine** rules, you may add whatever combination of the standard or custom Engines that meets your needs.

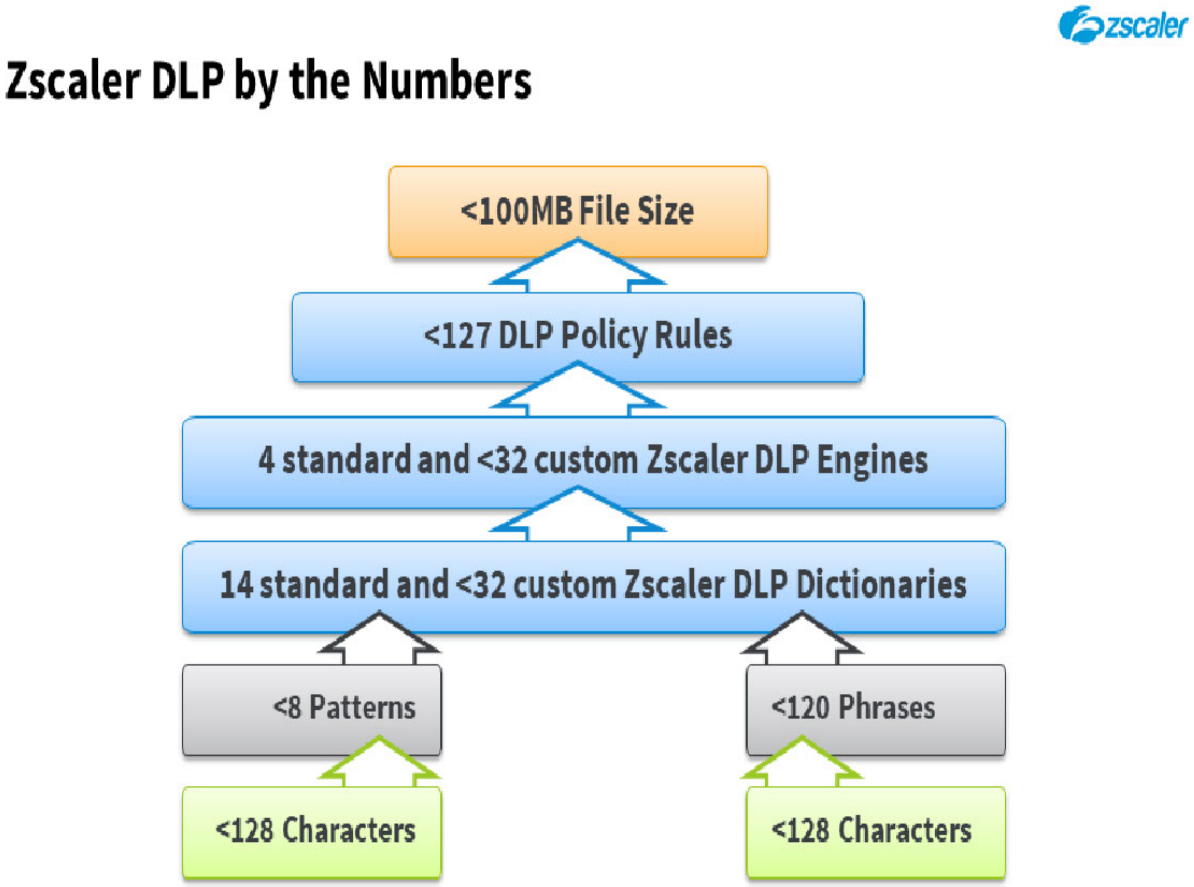
Slide 36 - Zscaler DLP by the Numbers



Slide notes

Note that the rule **Action** will be taken if any one of the added Engines triggers.

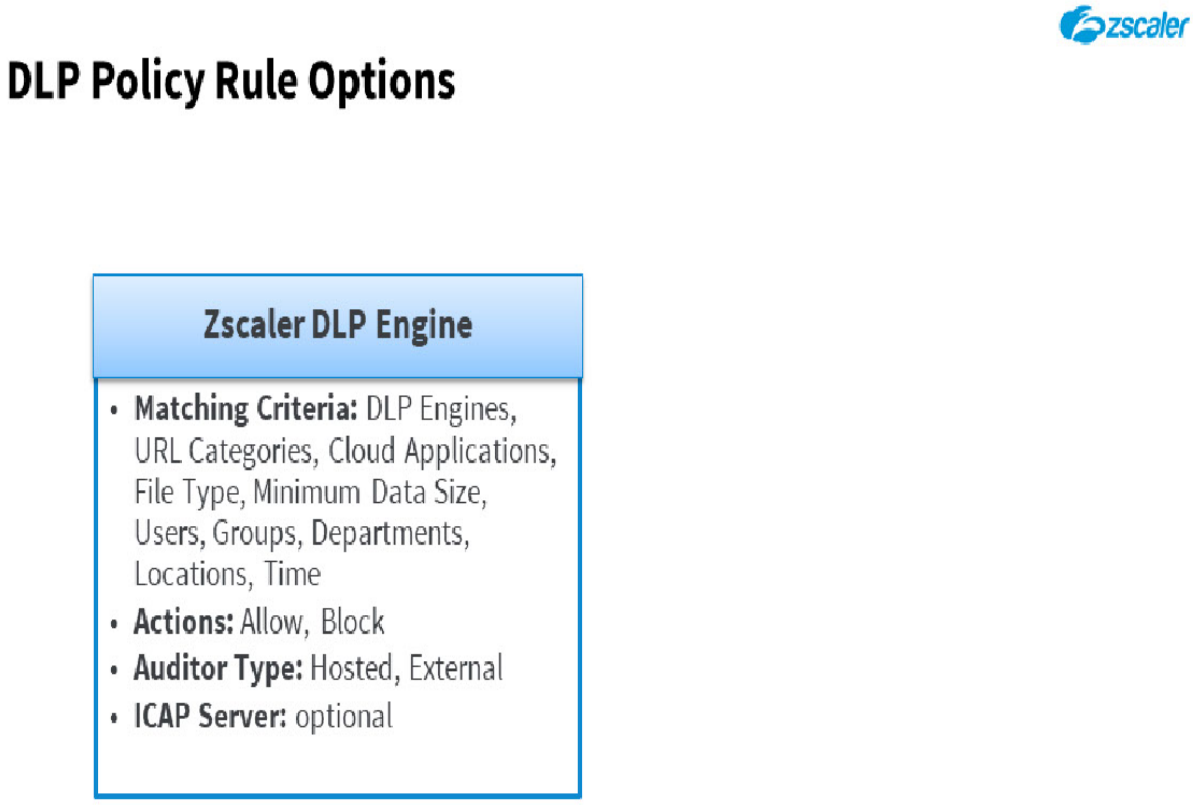
Slide 37 - Zscaler DLP by the Numbers



Slide notes

One thing to note is that the Zscaler DLP Engines can scan files with a maximum size of 100 MB. Or, for an archived file, the maximum size of an individual decompressed file is 50 MB.

Slide 38 - DLP Policy Rule Options



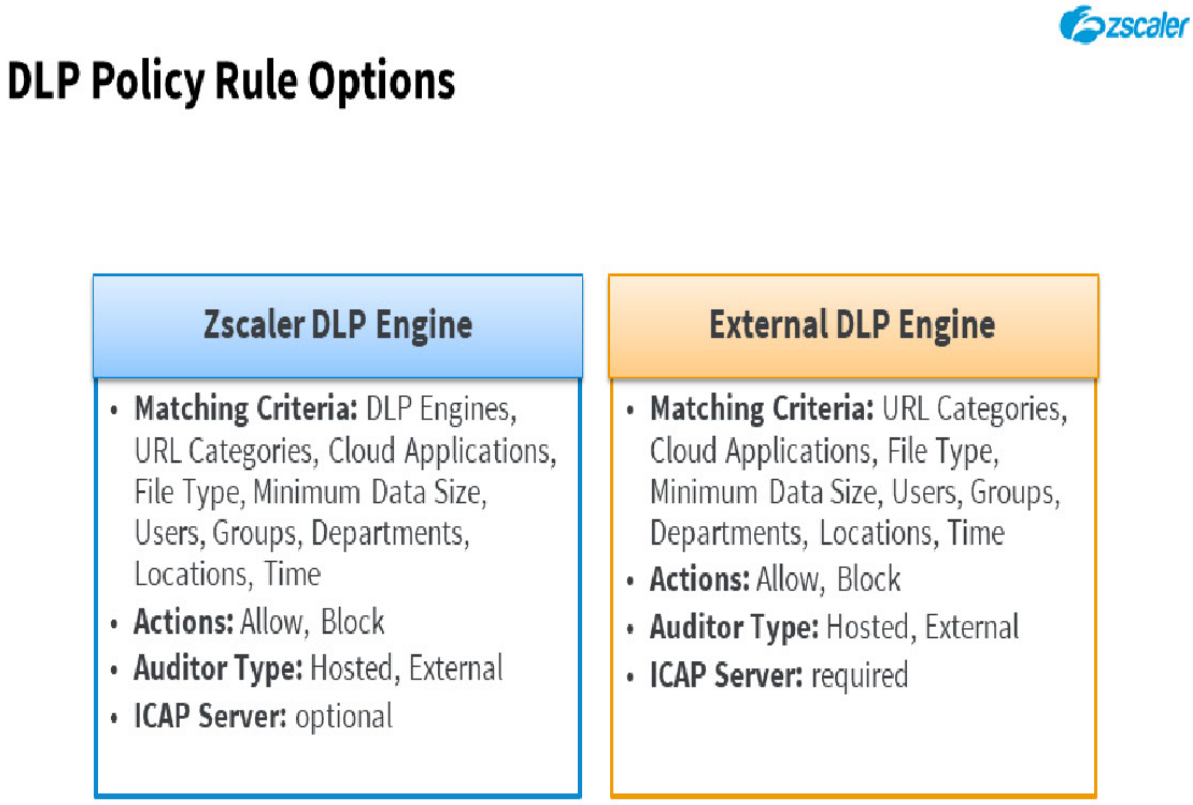
Slide notes

There are two main DLP Policy configuration options, whether to use Zscaler internal engines, or external engines. If you elect to go for the **Zscaler DLP Engine** option, you have the ability to match data signatures from the standard Zscaler DLP Engines, or any custom Engines that you created for specific purposes.

Other criteria that can be used are; any combination of the available **URL Categories**; any combination of the defined **Cloud Applications**; specific **File Types**; a minimum data size threshold; and all of the **standard** criteria (**Users**, **Groups**, **Departments**, **Locations**, and **Time**).

The actions available within a rule are to **Allow** or **Block**; you have the ability to set up notifications to either the hosted users, or to an external auditor; plus you have the option to specify an external ICAP server to send any matching transactions to.

Slide 39 - DLP Policy Rule Options

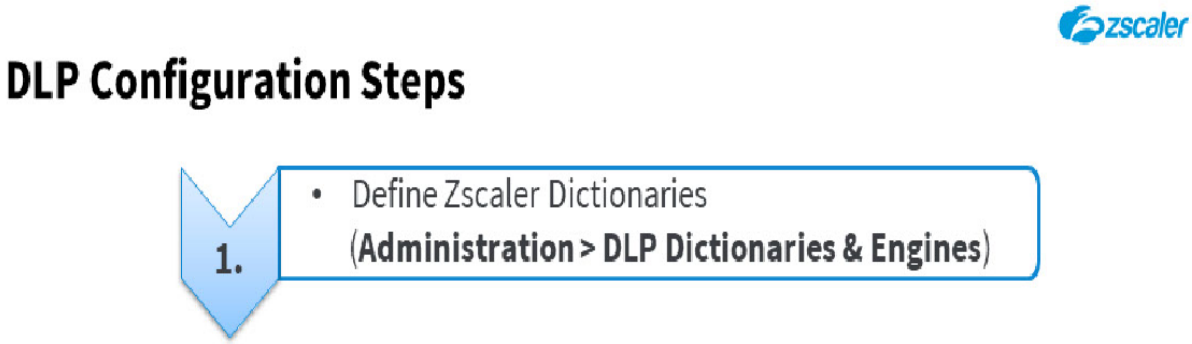


Slide notes

If you elect to go for the **External DLP Engine** option, Zscaler will act as a **coarse filter** for your external DLP server. The matching criteria that can be used are the same as for a Zscaler rule, with the exception of the **DLP Engines** option. Extensive scanning and analysis can be done by the external DLP system, using a comprehensive set of Dictionaries and Engines; although it is unable to block exfiltration attempts in real-time.

As with a Zscaler Engine, the available actions are to **Allow** or **Block**, you can send notifications to hosted users or an external auditor, and you must specify the external DLP server to send any matching transactions to.

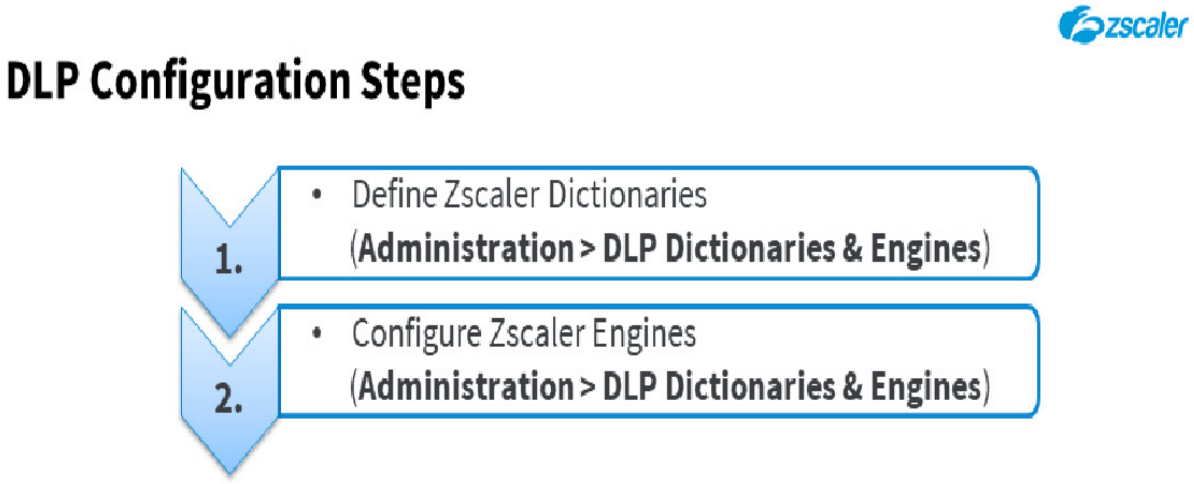
Slide 40 - DLP Configuration Steps



Slide notes

There are a number of steps to configure DLP functionality on the Zscaler platform, the first of them being to review, customize as necessary, or even create new DLP Dictionaries on the **Administration > DLP Dictionaries & Engines** page.

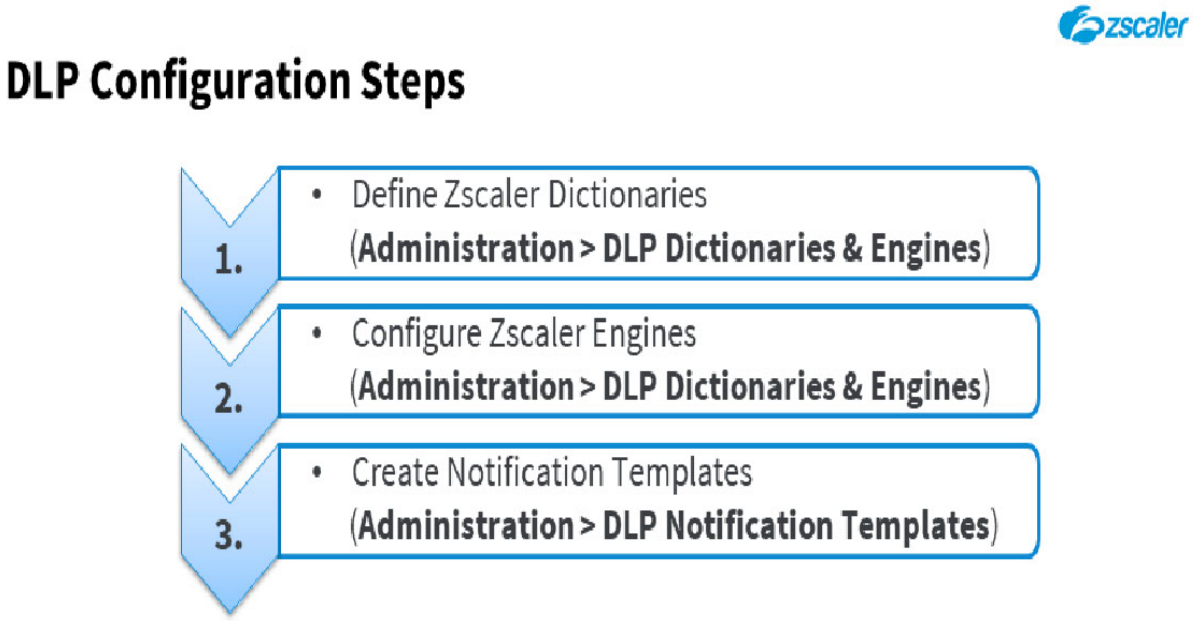
Slide 41 - DLP Configuration Steps



Slide notes

The next step is to review, customize as necessary, or even create new DLP Engines on the **Administration > DLP Dictionaries & Engines** page.

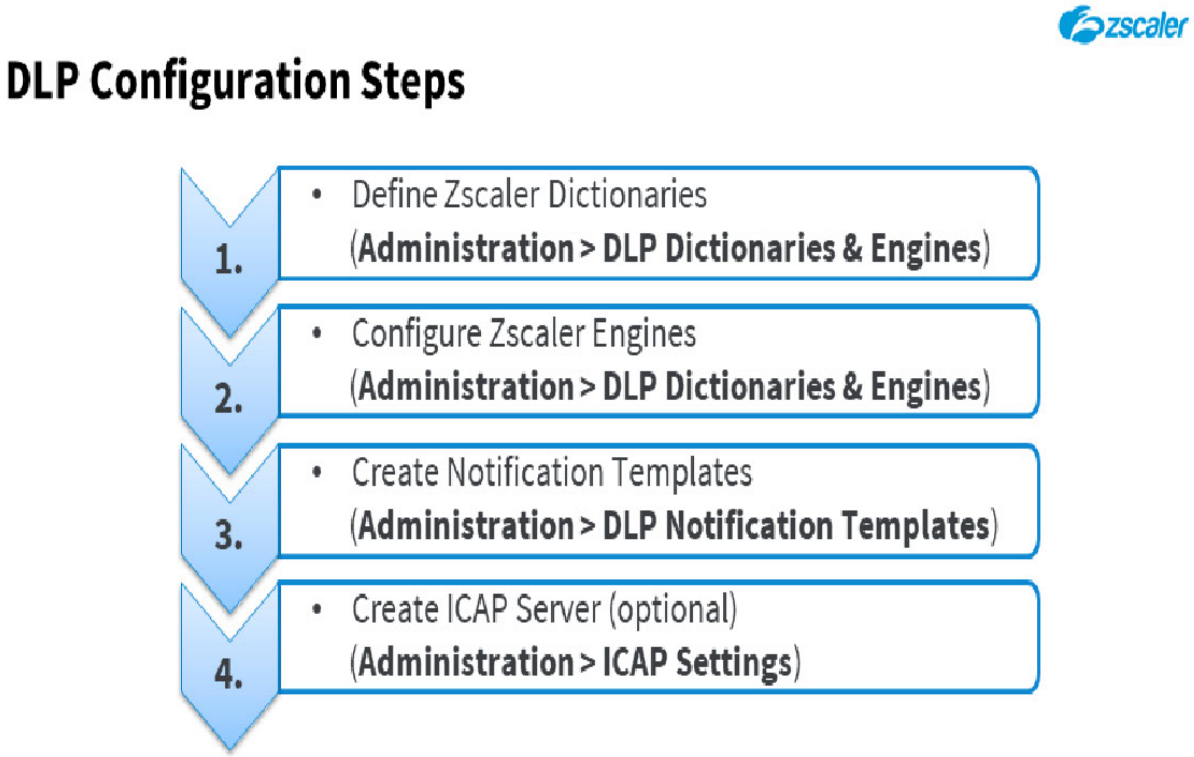
Slide 42 - DLP Configuration Steps



Slide notes

Next you may need to create or manage the DLP **Notification Templates** on the **Administration > DLP Notification Templates** page.

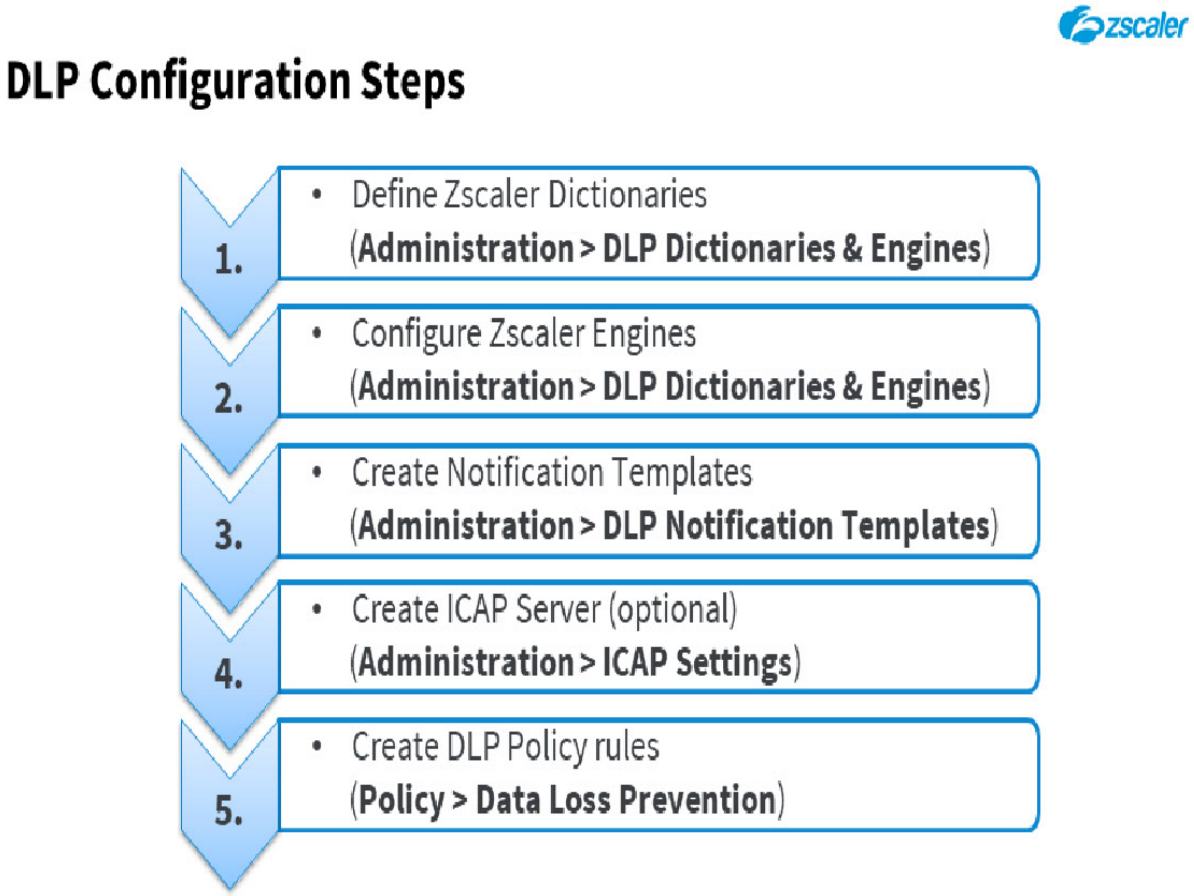
Slide 43 - DLP Configuration Steps



Slide notes

If you plan to send suspect transactions to an external DLP server using ICAP, you need to add the server to send them to on the **Administration > ICAP Settings** page.

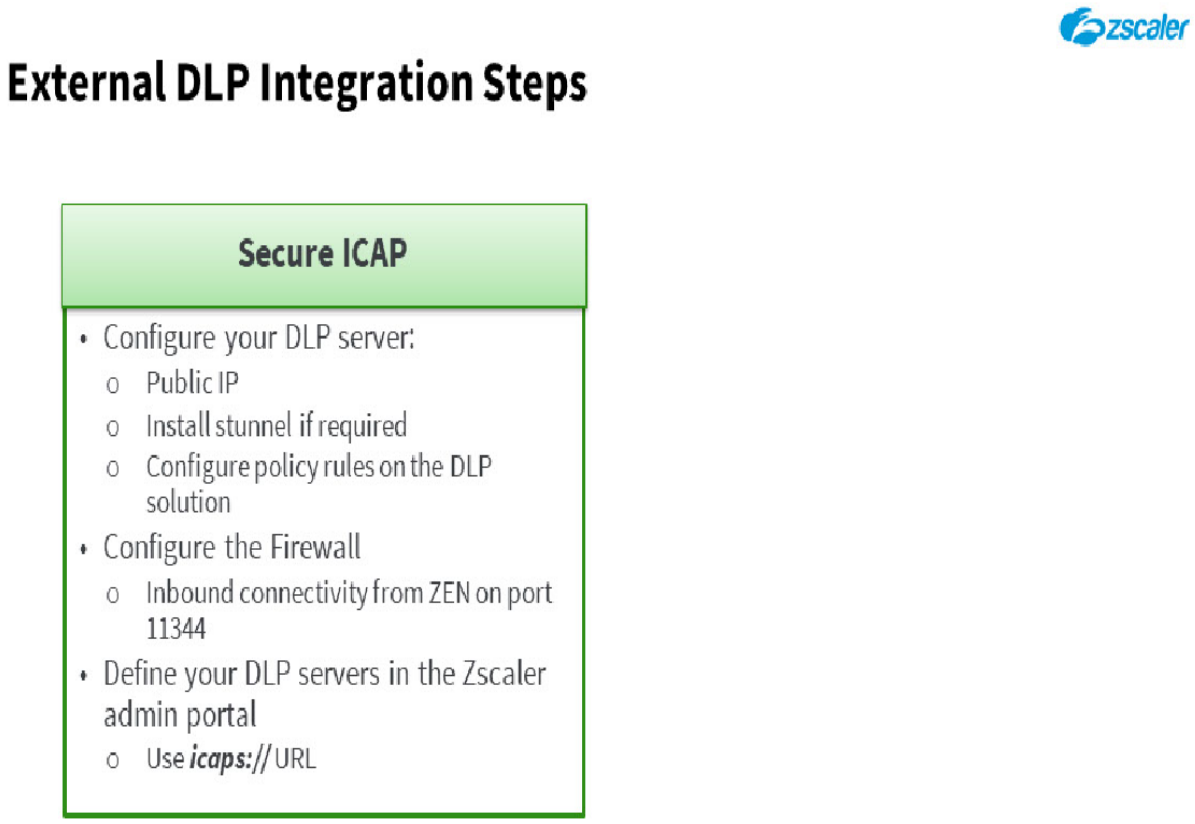
Slide 44 - DLP Configuration Steps



Slide notes

Finally, you can begin to define your DLP Policy rules, to reference the Engines, Templates, and servers that you have defined.

Slide 45 - External DLP Integration Steps

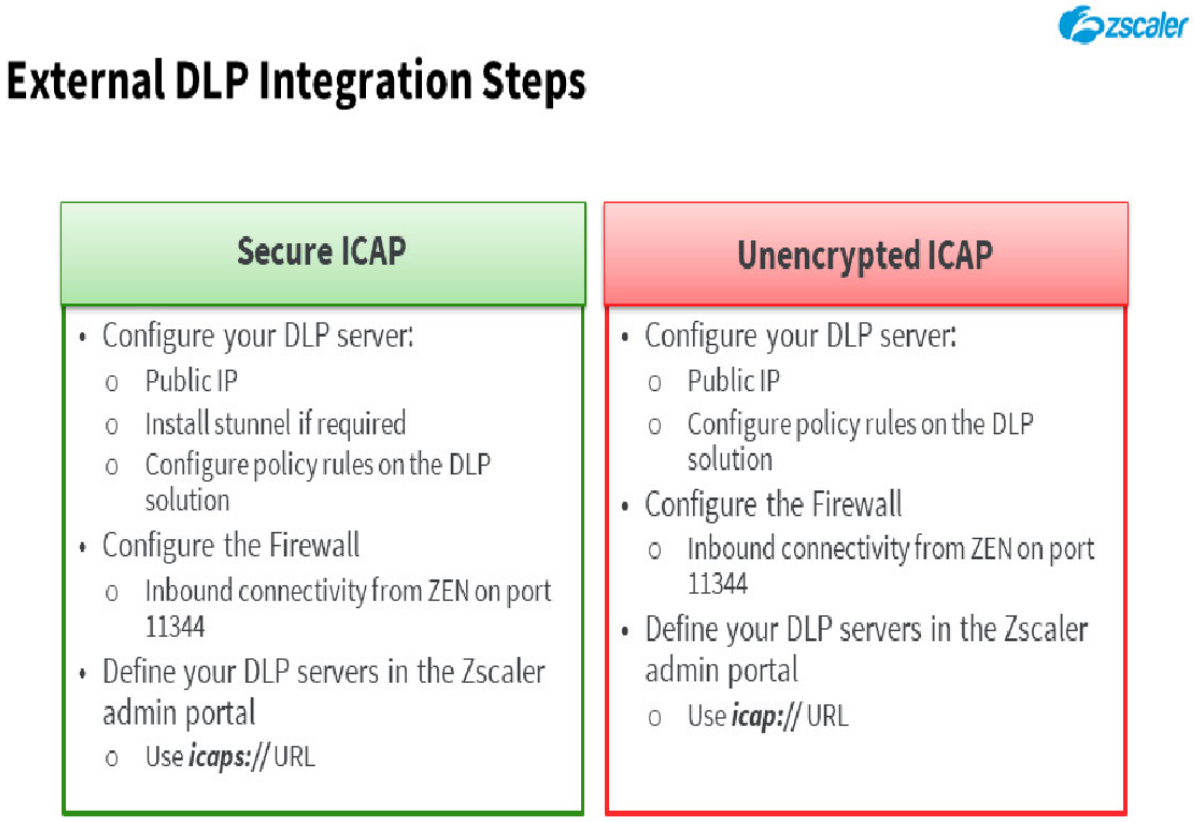


Slide notes

If you wish to send suspect transactions to an external DLP system securely, there are a number of integration steps that must be taken care of. Your DLP system must be available on a public IP address, and if it doesn't support secure ICAP natively we recommend that you install the open source **stunnel** application on the DLP appliance. You will of course also need to configure appropriate policy rules on the external system.

The Firewall in front of the DLP server must be configured to allow inbound connections from Zscaler, usually on port 11344. Then, as mentioned at step 4 in the previous slide, you must create the ICAP server in the Zscaler admin portal on the **Administration > ICAP Settings** page. When creating the ICAP server, the URL for the external system must be configured using the protocol definition **icaps://**.

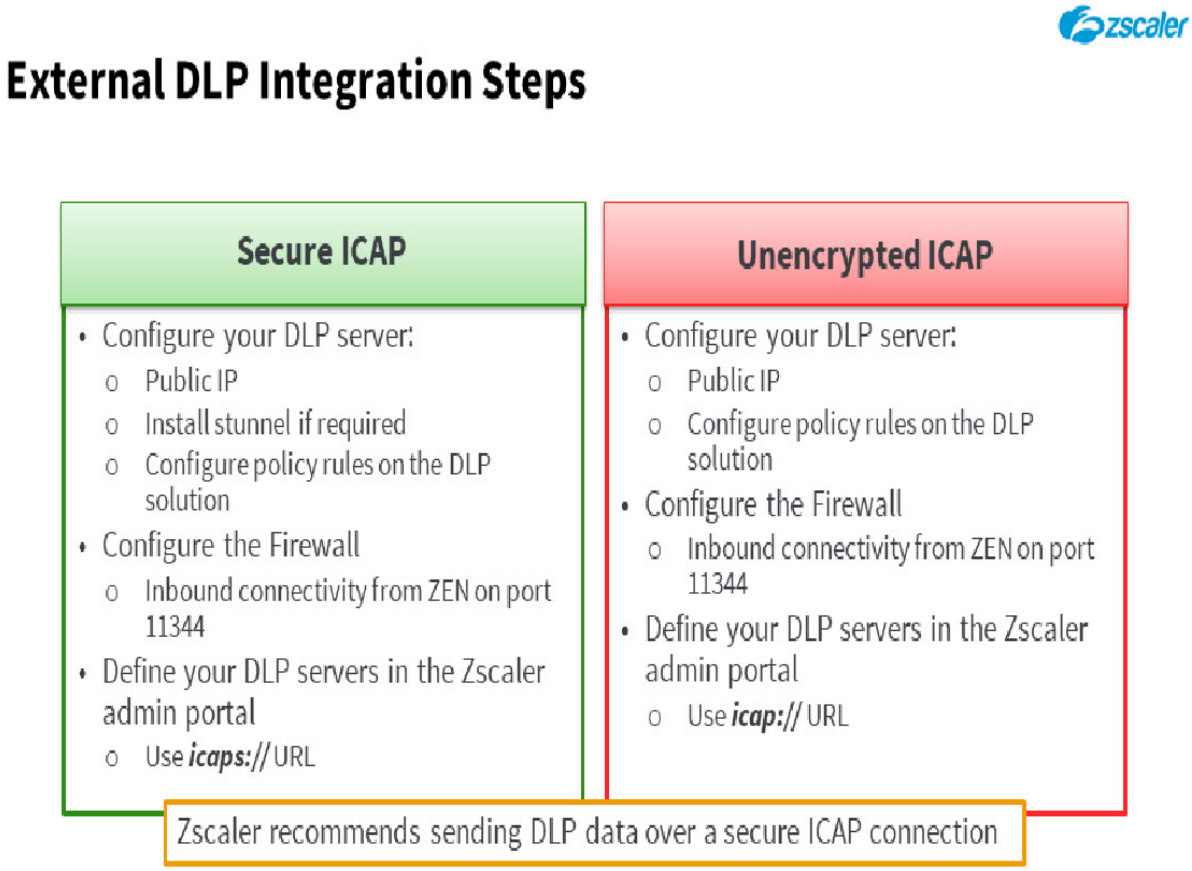
Slide 46 - External DLP Integration Steps



Slide notes

To send suspect transactions in an unencrypted form to your external DLP system; you can omit the installation of 'stunnel', and you need to configure the URL for the ICAP server in the Zscaler admin portal using the protocol definition **icap://**.

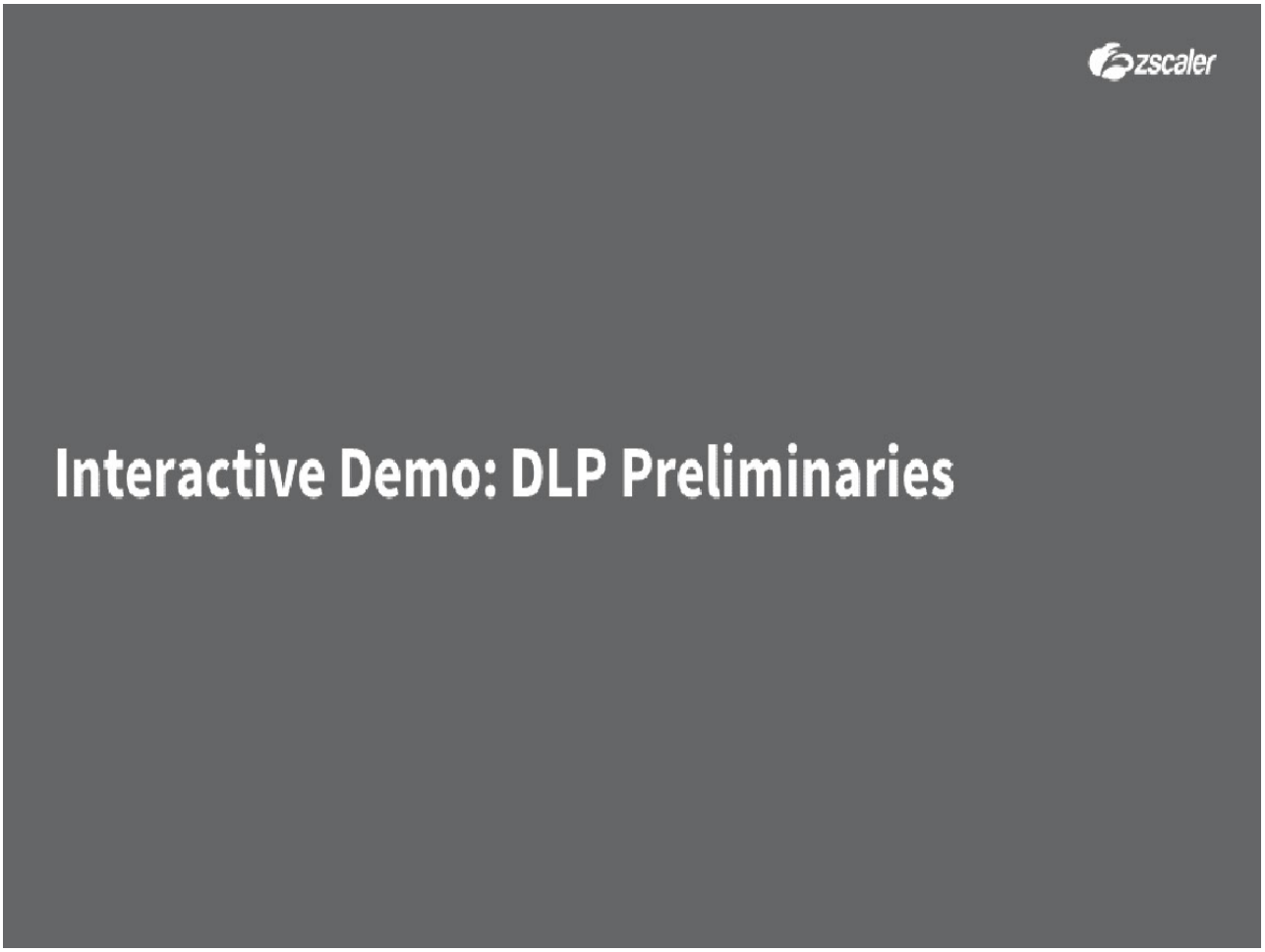
Slide 47 - External DLP Integration Steps



Slide notes

Note that Zscaler recommends using secure ICAP to transfer data to your external DLP system.

Slide 48 - Interactive Demo: DLP Preliminaries

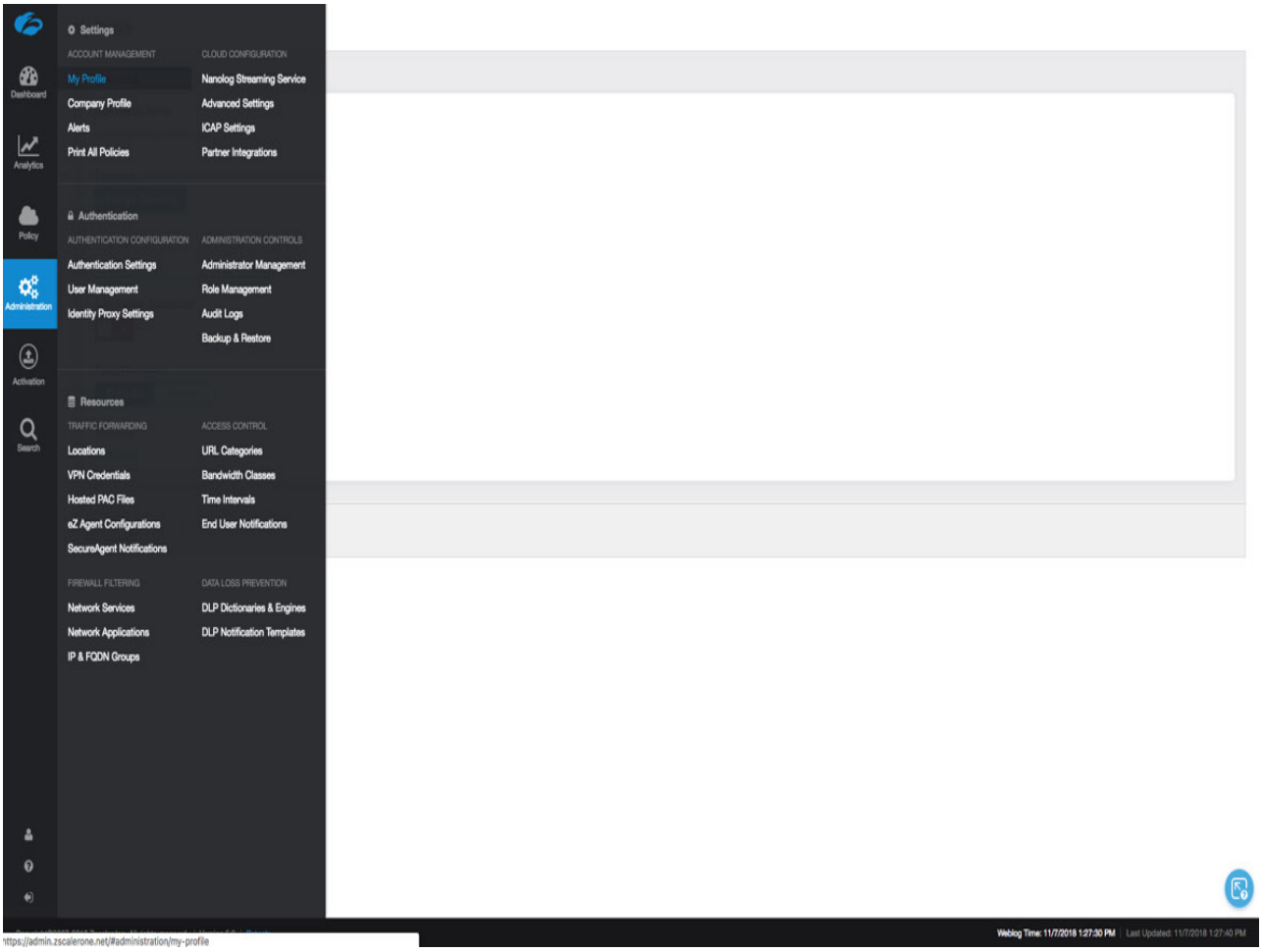


Slide notes

In the next section, we will have a detailed look at the DLP preliminary configurations on the Zscaler admin portal.

This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler App Portal UI. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

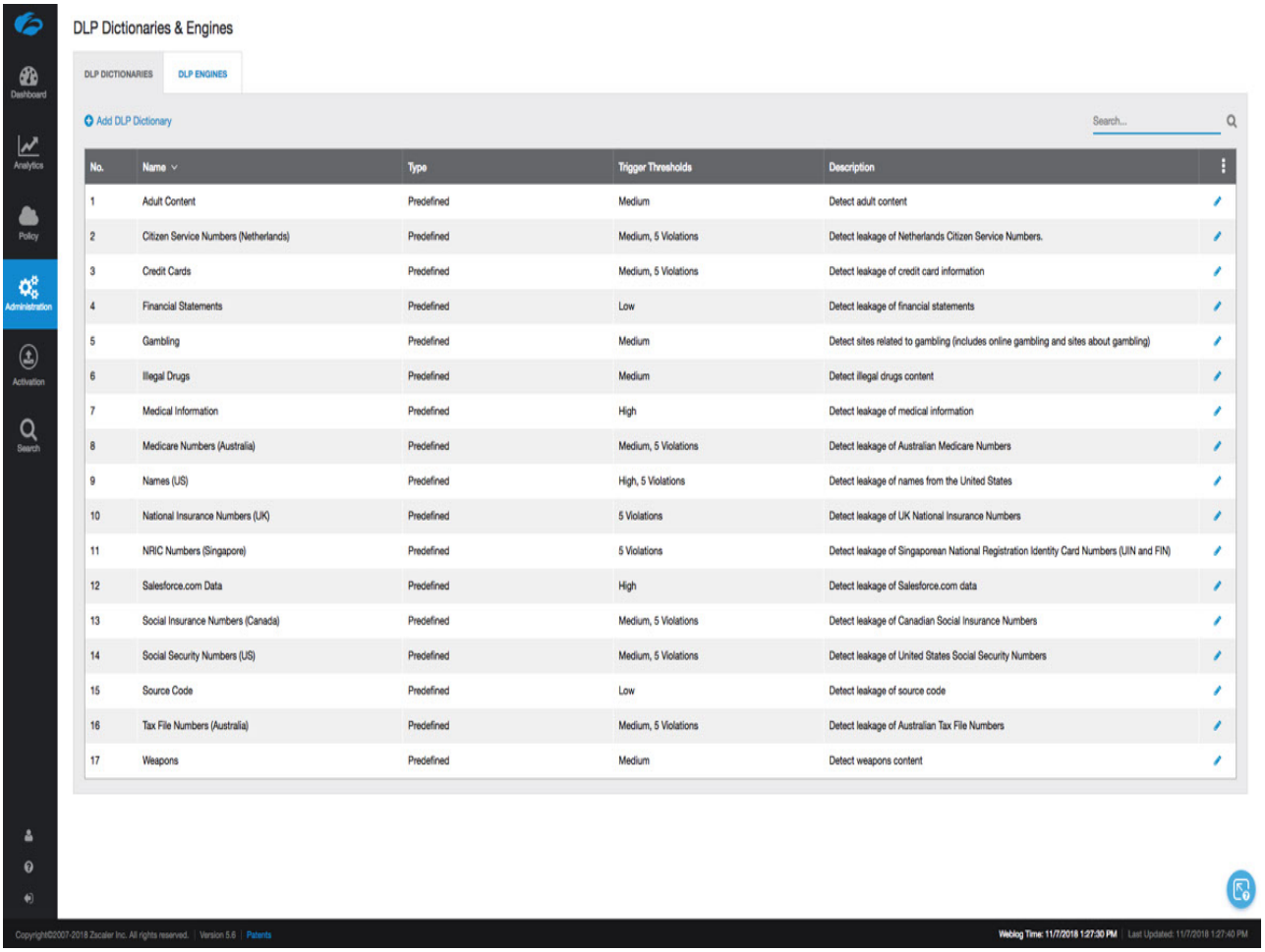
Slide 49 - Slide 49



Slide notes

To manage DLP Dictionaries and Engines, from the **Administration** menu, under **Resources**, click **DLP Dictionaries and Engines**.

Slide 50 - Slide 50



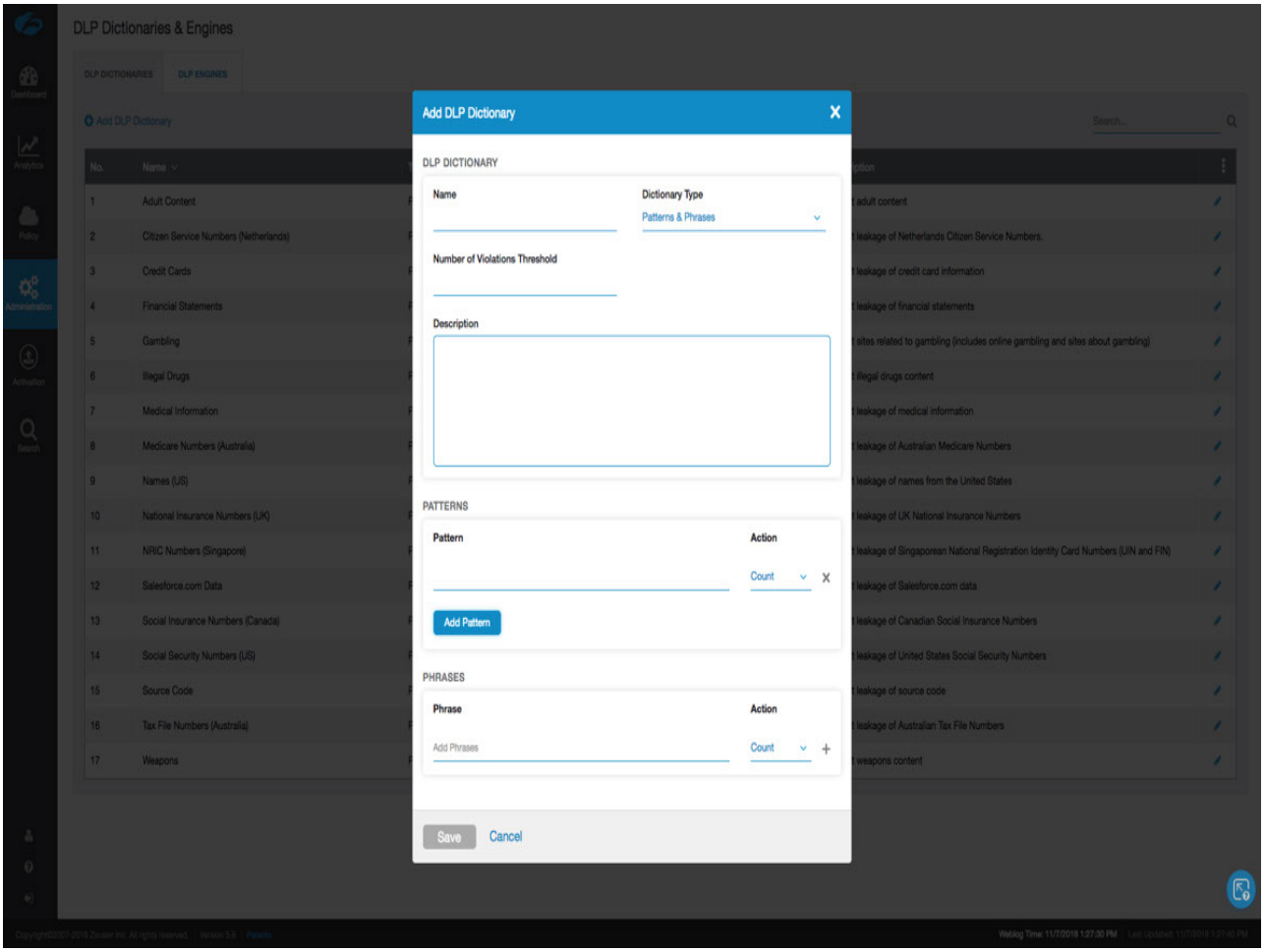
No.	Name	Type	Trigger Thresholds	Description
1	Adult Content	Predefined	Medium	Detect adult content
2	Citizen Service Numbers (Netherlands)	Predefined	Medium, 5 Violations	Detect leakage of Netherlands Citizen Service Numbers.
3	Credit Cards	Predefined	Medium, 5 Violations	Detect leakage of credit card information
4	Financial Statements	Predefined	Low	Detect leakage of financial statements
5	Gambling	Predefined	Medium	Detect sites related to gambling (includes online gambling and sites about gambling)
6	Illegal Drugs	Predefined	Medium	Detect illegal drugs content
7	Medical Information	Predefined	High	Detect leakage of medical information
8	Medicare Numbers (Australia)	Predefined	Medium, 5 Violations	Detect leakage of Australian Medicare Numbers
9	Names (US)	Predefined	High, 5 Violations	Detect leakage of names from the United States
10	National Insurance Numbers (UK)	Predefined	5 Violations	Detect leakage of UK National Insurance Numbers
11	NRIC Numbers (Singapore)	Predefined	5 Violations	Detect leakage of Singaporean National Registration Identity Card Numbers (UIN and FIN)
12	Salesforce.com Data	Predefined	High	Detect leakage of Salesforce.com data
13	Social Insurance Numbers (Canada)	Predefined	Medium, 5 Violations	Detect leakage of Canadian Social Insurance Numbers
14	Social Security Numbers (US)	Predefined	Medium, 5 Violations	Detect leakage of United States Social Security Numbers
15	Source Code	Predefined	Low	Detect leakage of source code
16	Tax File Numbers (Australia)	Predefined	Medium, 5 Violations	Detect leakage of Australian Tax File Numbers
17	Weapons	Predefined	Medium	Detect weapons content

Slide notes

A DLP Dictionary contains a set of patented algorithms that are designed to detect specific kinds of information in your users' traffic, and Zscaler provides a set pre-defined Dictionaries. The default **Tigger Thresholds** (number of violations and the **Confidence** setting) are indicated, and you can modify these by editing a Dictionary.

To add a Dictionary of your own, to detect content relevant to your organization, click the **Add DLP Dictionary** link.

Slide 51 - Slide 51

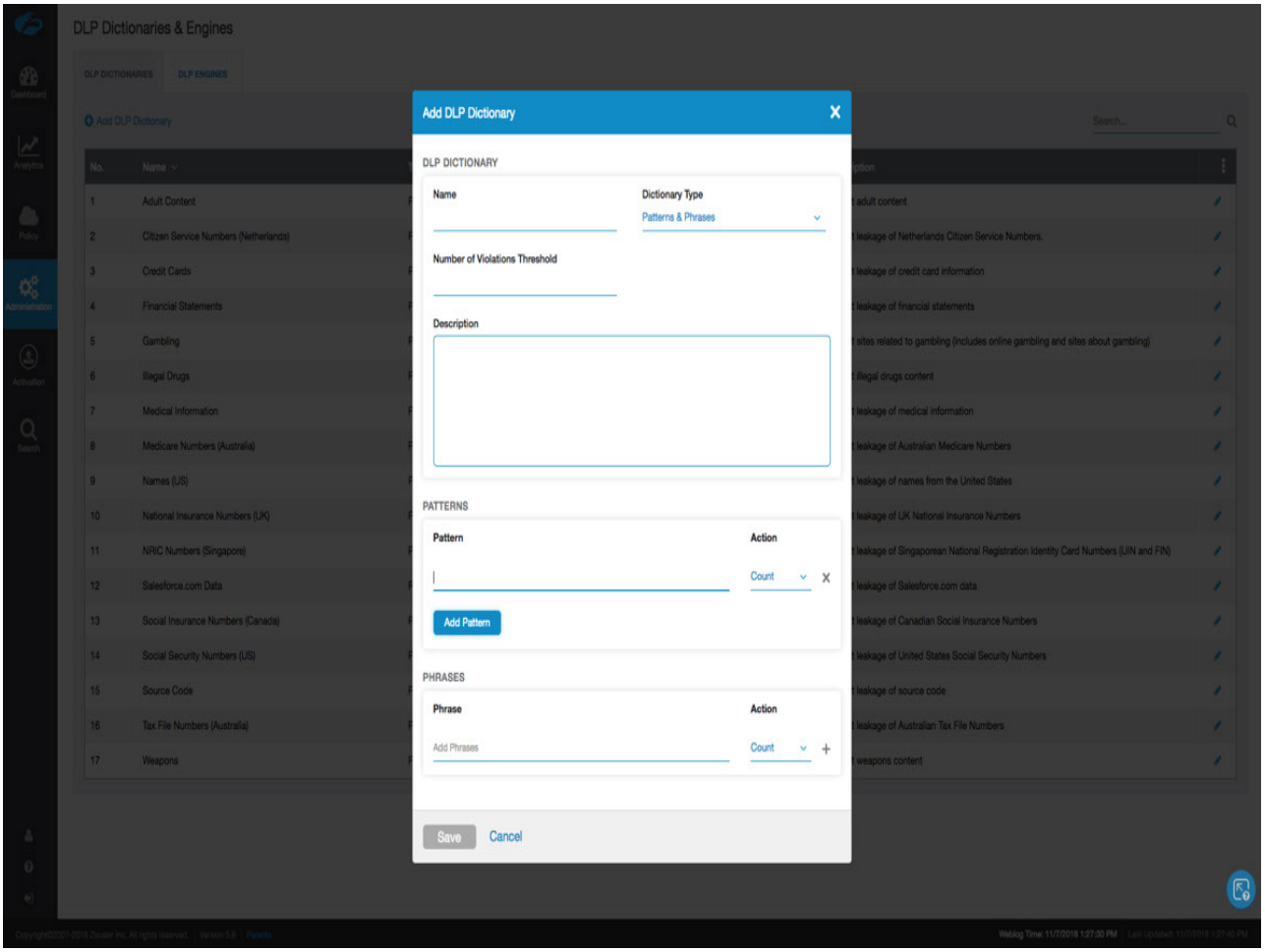


Slide notes

You can create a maximum of 32 custom DLP Dictionaries. You must name them and set the **Number of Violations Threshold**, which is the number of violations that is to trigger the Dictionary.

The Dictionary triggers only if it finds more violations than the number specified here, and you may enter any value here up to 10,000.

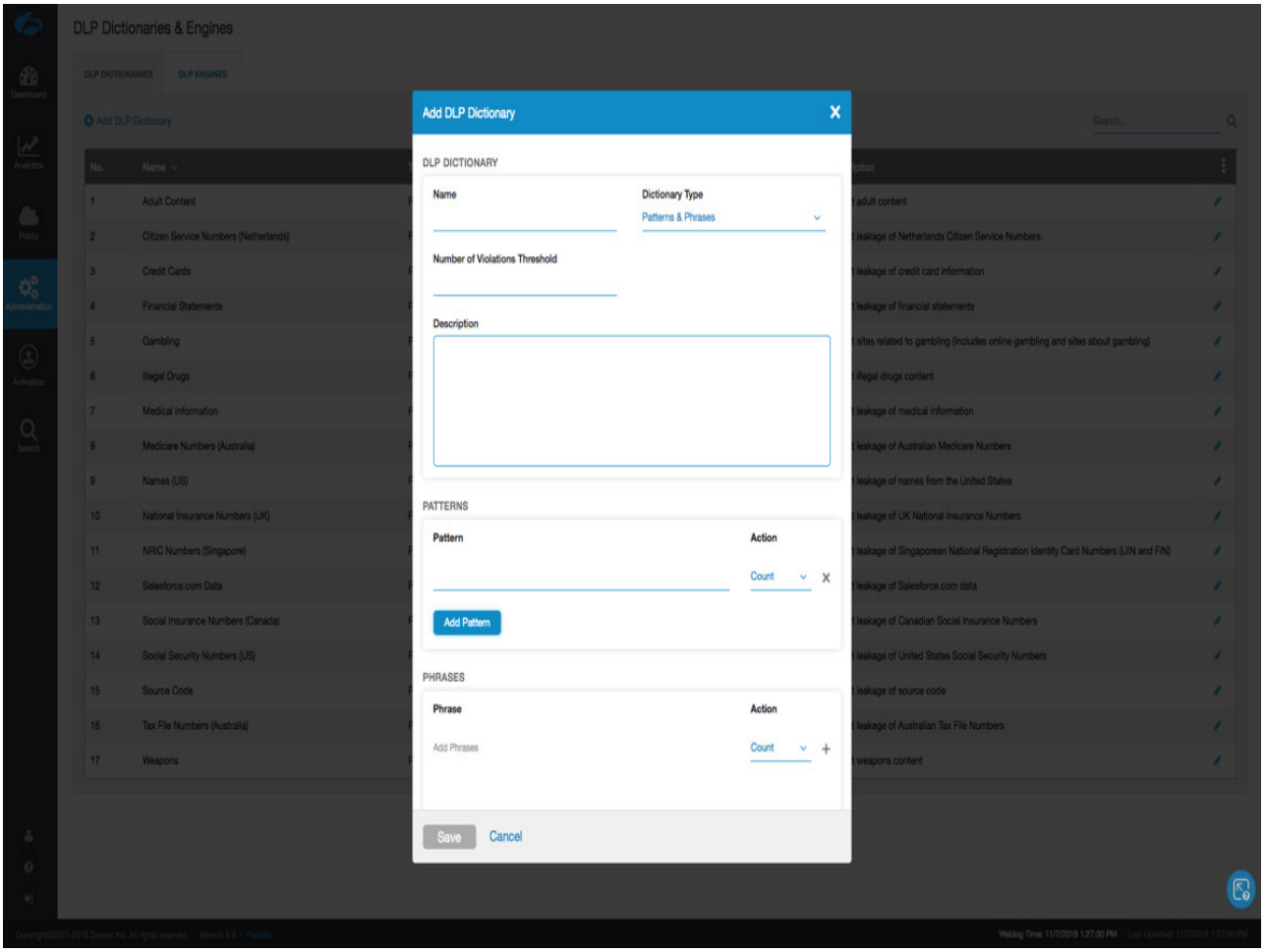
Slide 52 - Slide 52



Slide notes

You can add up to 8 alphanumeric **Patterns** that represent the content you want to protect, and which the Dictionary is to detect. You can use a subset of the POSIX Extended Regular Expression (ERE) syntax to create the Patterns to match.

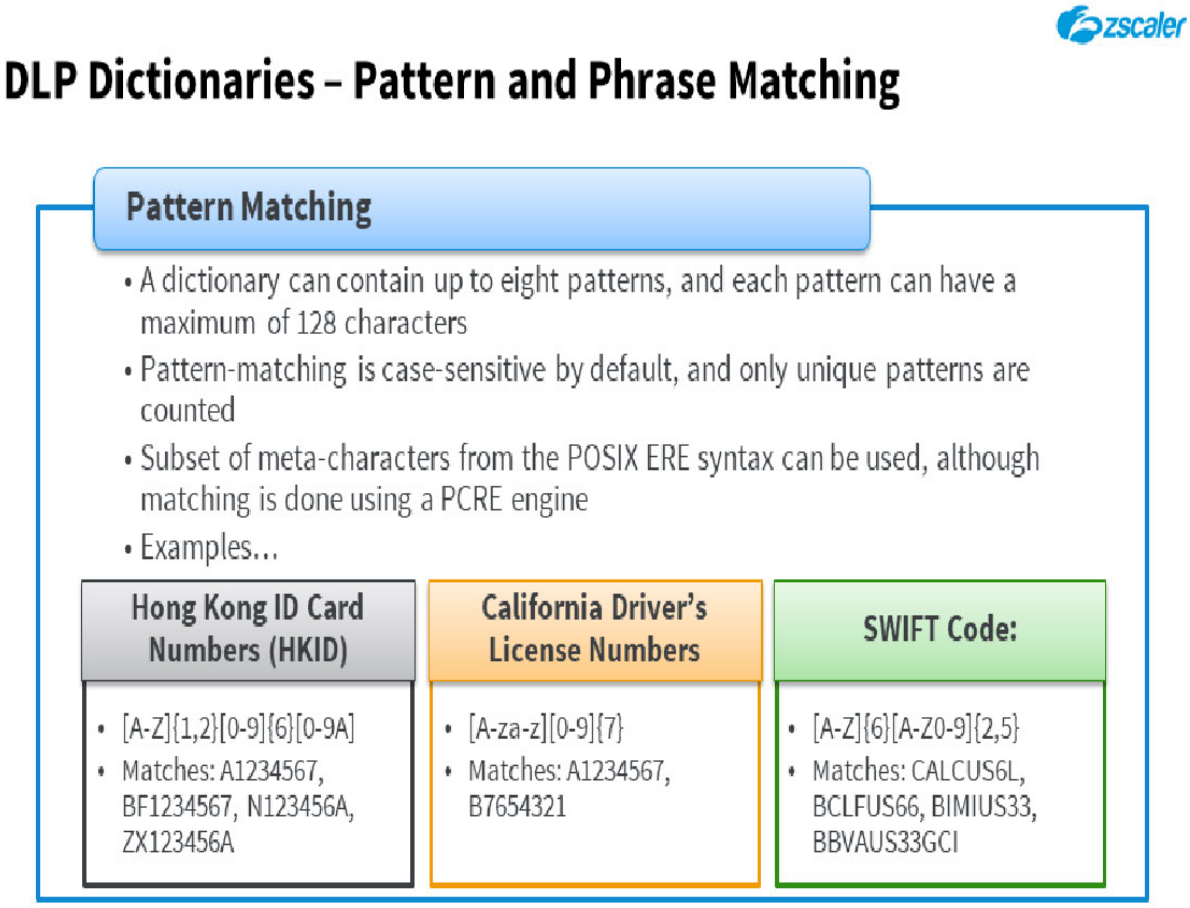
Slide 53 - Slide 53



Slide notes

You may also add up to 120 exact **Phrases** that the Dictionary is to detect.

Slide 54 - DLP Dictionaries – Pattern and Phrase Matching



Slide notes

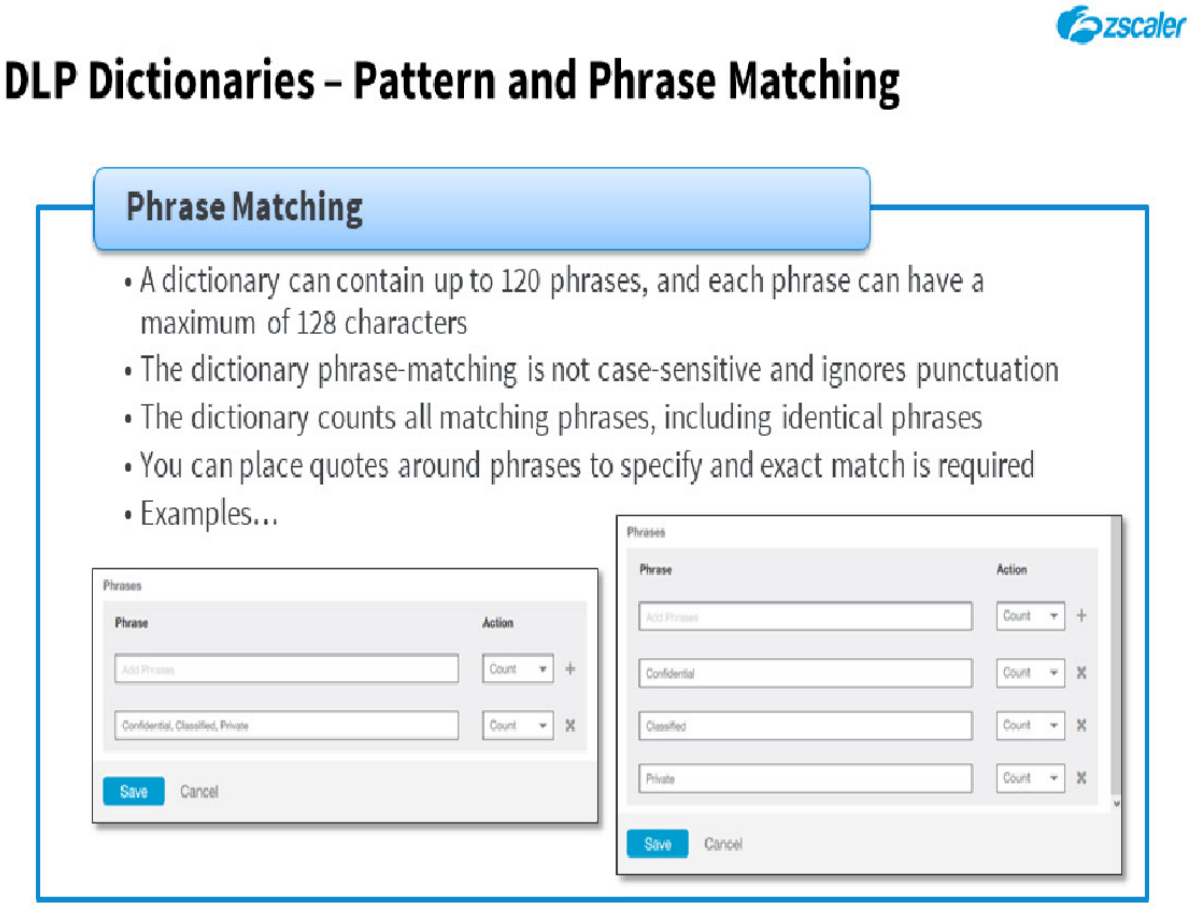
You can use alphanumeric **Patterns** to configure custom dictionaries that match a wide variety of data types. For example, you can define Patterns to detect data such as; US phone numbers, driver's license numbers, or credit card numbers for specific issuers (a number of sample Patterns are provided below).

General guidelines for Patterns include the following: a dictionary can contain up to eight Patterns; each Pattern can have a maximum of 128 characters; Pattern-matching is case-sensitive by default; only unique Patterns are counted – a specific text matching the Pattern is counted only once, regardless of how many times it actually appears in the content;

the custom Dictionary accepts a subset of the POSIX ERE syntax (see the on-line documentation for details); although matching is done using a PCRE engine for flexibility and speed.

Some simple examples of the Pattern matching syntax are shown here, for Hong Kong ID Card numbers, California driver's license numbers, and SWIFT codes. Full details of the regular expressions supported with comprehensive examples are available on the support Web site.

Slide 55 - DLP Dictionaries – Pattern and Phrase Matching



Slide notes

You can add to your custom Dictionaries **Phrases** that represent content you want to protect for your organization. General guidelines for Phrases include the following: a Dictionary can contain up to 120 Phrases; each Phrase can have a maximum of 128 characters;

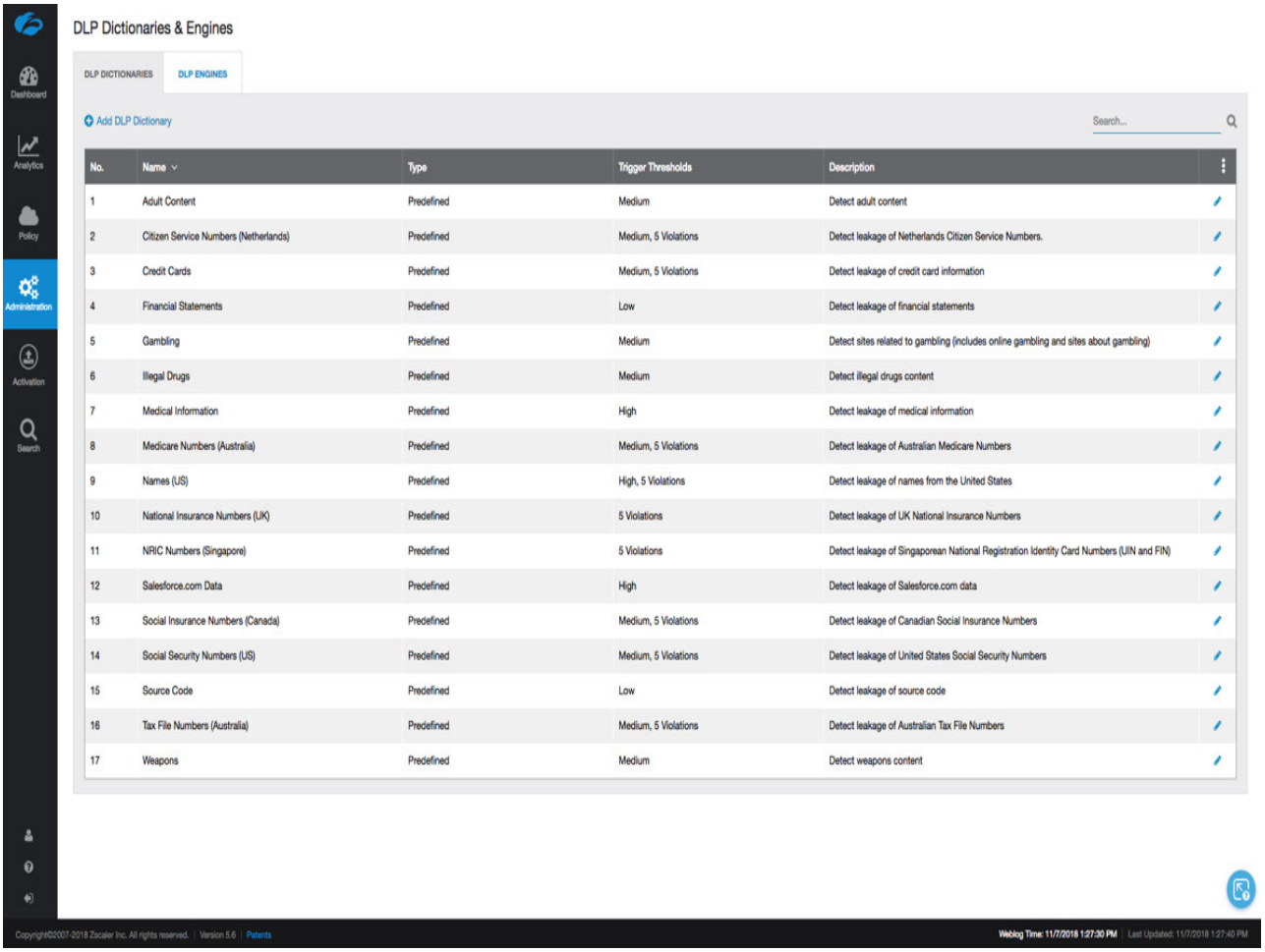
the Dictionary Phrase-matching is not case-sensitive and ignores punctuation; the Dictionary counts all matching Phrases, including identical Phrases; you can place quotes around Phrases to specify that the Dictionary detect only Phrases that exactly match the Phrase in the order given within the quotes.

The Zscaler service uses fuzzy matching techniques to ensure that Phrases do not go undetected by Dictionaries because of capitalization or spacing discrepancies and the existence of noise words (such as spurious words or HTML tags) between words.

Sometimes this fuzzy matching results in the matching of Phrases from an irrelevant context and can cause false positives. In such cases, quotes or double quotes can be placed around the words of a Phrase to disable fuzzy matching and match only the Phrase within the quotes.

In the examples shown, each line is treated as a separate Phrase, so on the left the rule will only trigger if a Phrase contains all three words. In the example on the right each word is treated as a separate Phrase.

Slide 56 - Slide 56

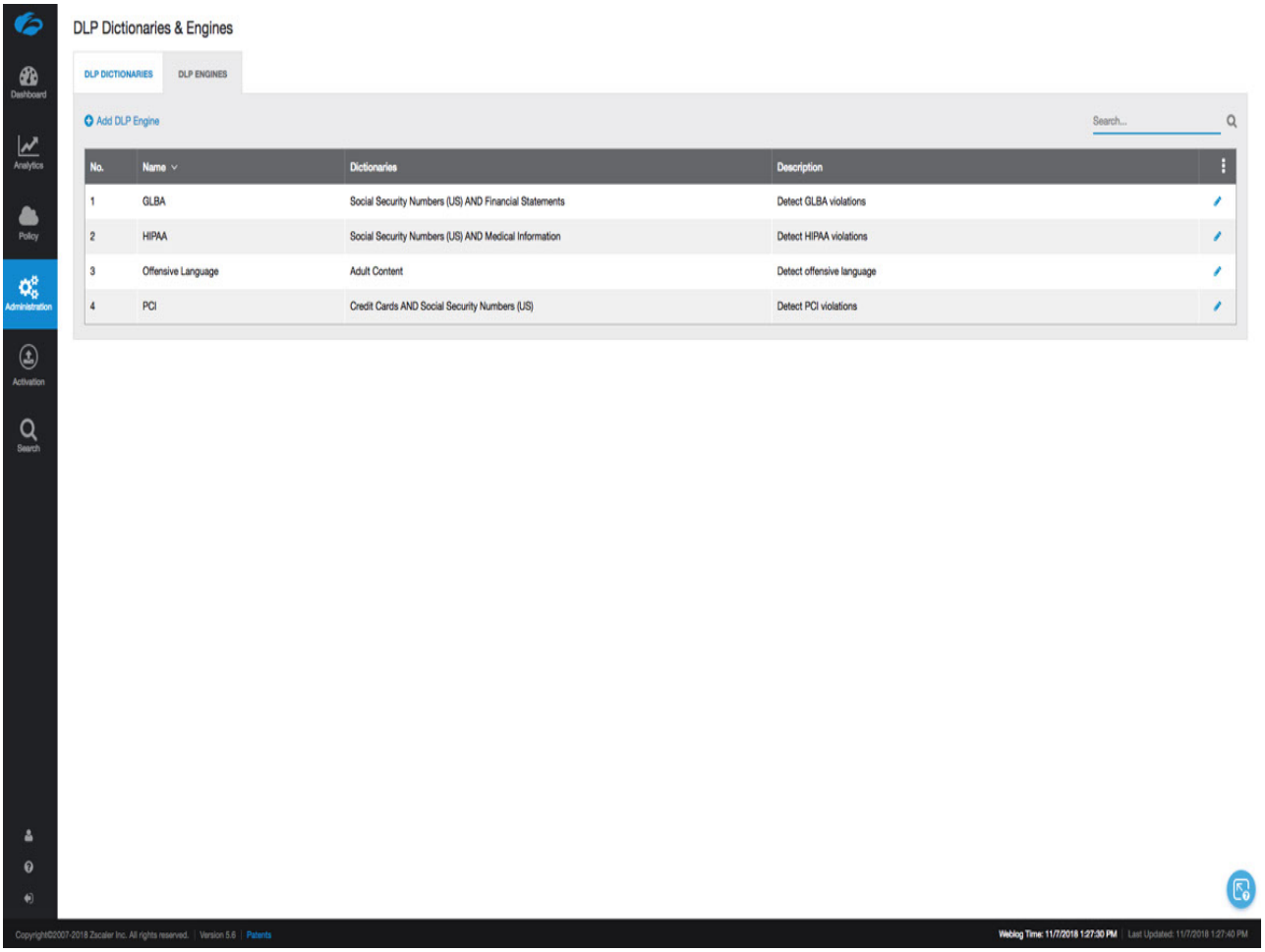


No.	Name	Type	Trigger Thresholds	Description
1	Adult Content	Predefined	Medium	Detect adult content
2	Citizen Service Numbers (Netherlands)	Predefined	Medium, 5 Violations	Detect leakage of Netherlands Citizen Service Numbers.
3	Credit Cards	Predefined	Medium, 5 Violations	Detect leakage of credit card information
4	Financial Statements	Predefined	Low	Detect leakage of financial statements
5	Gambling	Predefined	Medium	Detect sites related to gambling (includes online gambling and sites about gambling)
6	Illegal Drugs	Predefined	Medium	Detect illegal drugs content
7	Medical Information	Predefined	High	Detect leakage of medical information
8	Medicare Numbers (Australia)	Predefined	Medium, 5 Violations	Detect leakage of Australian Medicare Numbers
9	Names (US)	Predefined	High, 5 Violations	Detect leakage of names from the United States
10	National Insurance Numbers (UK)	Predefined	5 Violations	Detect leakage of UK National Insurance Numbers
11	NRIC Numbers (Singapore)	Predefined	5 Violations	Detect leakage of Singaporean National Registration Identity Card Numbers (UIN and FIN)
12	Salesforce.com Data	Predefined	High	Detect leakage of Salesforce.com data
13	Social Insurance Numbers (Canada)	Predefined	Medium, 5 Violations	Detect leakage of Canadian Social Insurance Numbers
14	Social Security Numbers (US)	Predefined	Medium, 5 Violations	Detect leakage of United States Social Security Numbers
15	Source Code	Predefined	Low	Detect leakage of source code
16	Tax File Numbers (Australia)	Predefined	Medium, 5 Violations	Detect leakage of Australian Tax File Numbers
17	Weapons	Predefined	Medium	Detect weapons content

Slide notes

The DLP Dictionaries are not used directly; they must be referred to from a DLP **Engine**. To manage these, click the **DLP Engines** tab.

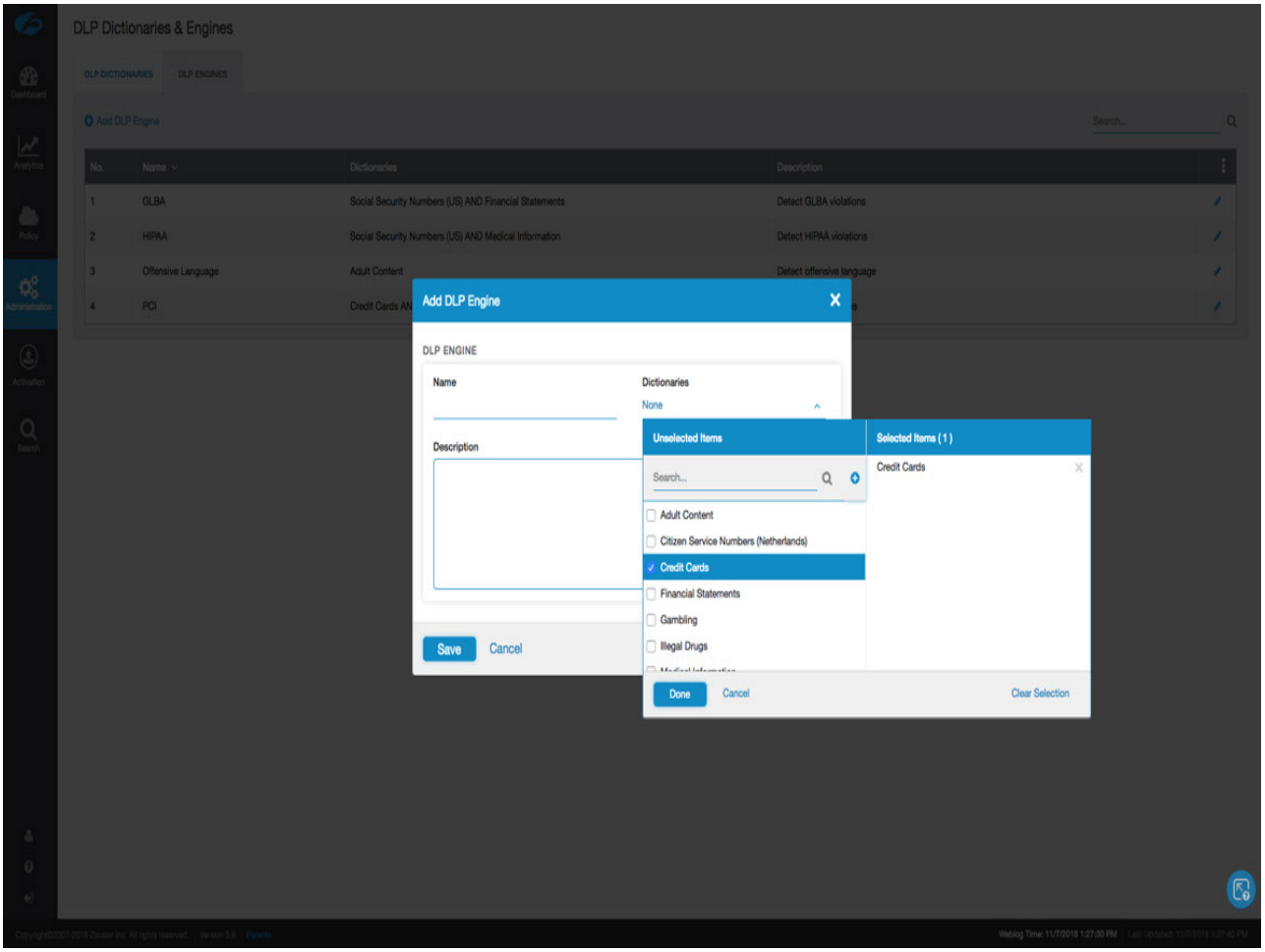
Slide 57 - Slide 57



Slide notes

A DLP Engine is a collection of one or more DLP Dictionaries. When you define your DLP Policy rules, you must reference the DLP Engines, rather than DLP Dictionaries directly. By using a DLP Engine, you can create rules to detect content that encompasses more than one Dictionary. Zscaler provides four predefined Engines: **HIPAA**; **GLBA**; **PCI**; and **Offensive Language**. To add your own custom DLP Engine, click the **Add DLP Engine** link.

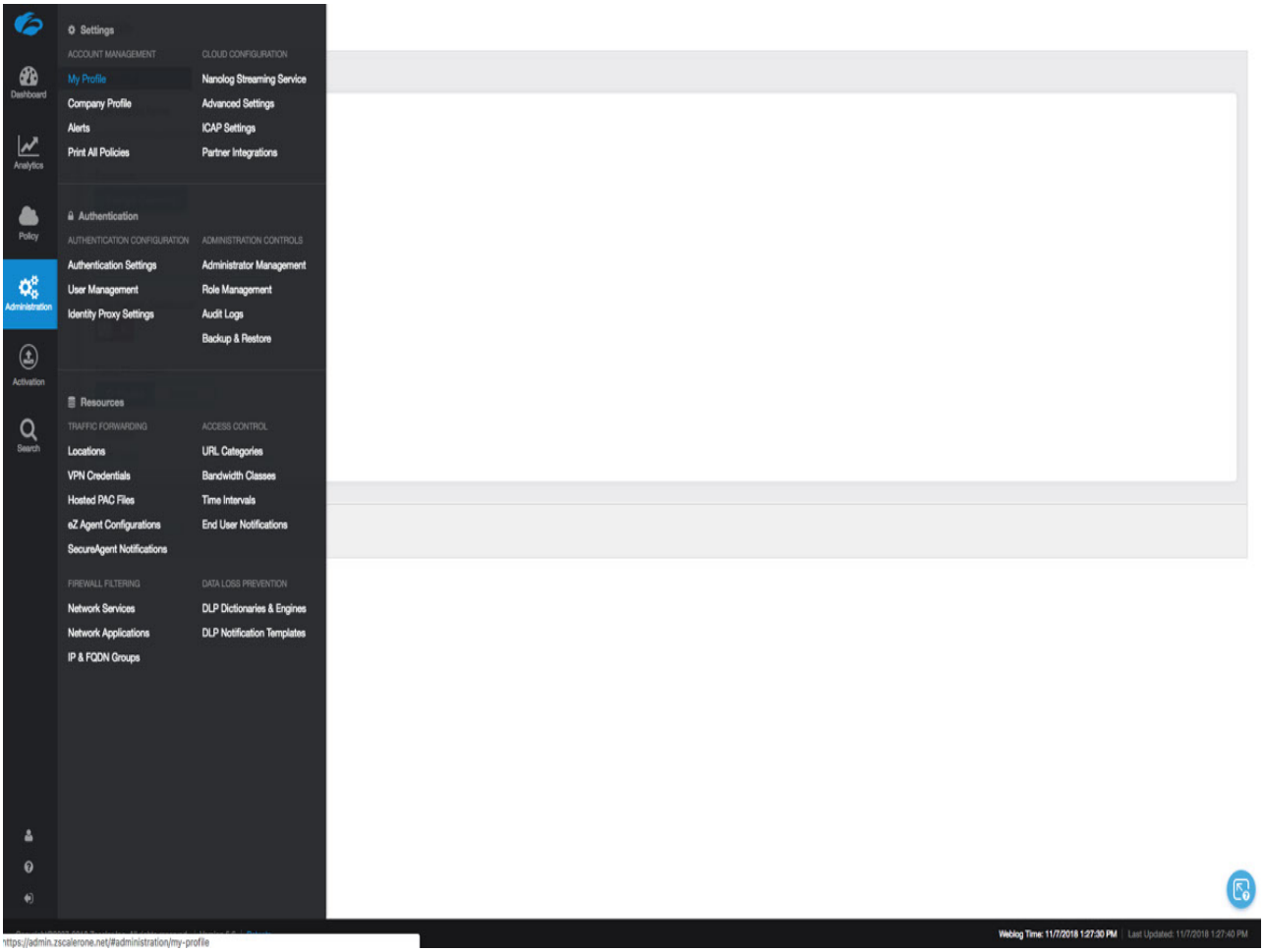
Slide 58 - Slide 58



Slide notes

You must give your Engine a **Name**, then select the combination of DLP **Dictionaries** that you want it to enforce. Note that all the Dictionaries added to an Engine must trigger in order for the Engine to trigger.

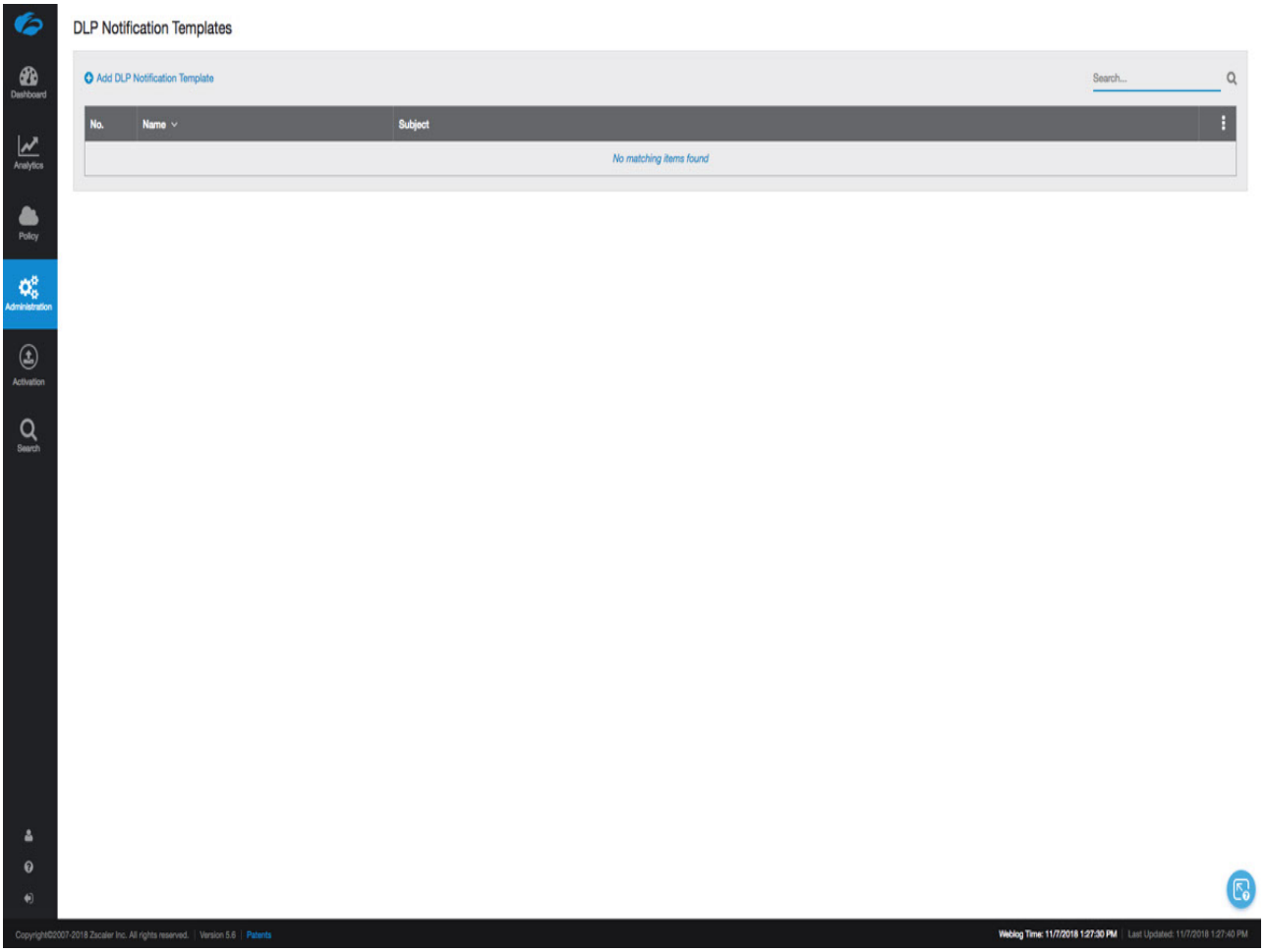
Slide 59 - Slide 59



Slide notes

To manage notification templates for DLP, click on **DLP Notification** templates.

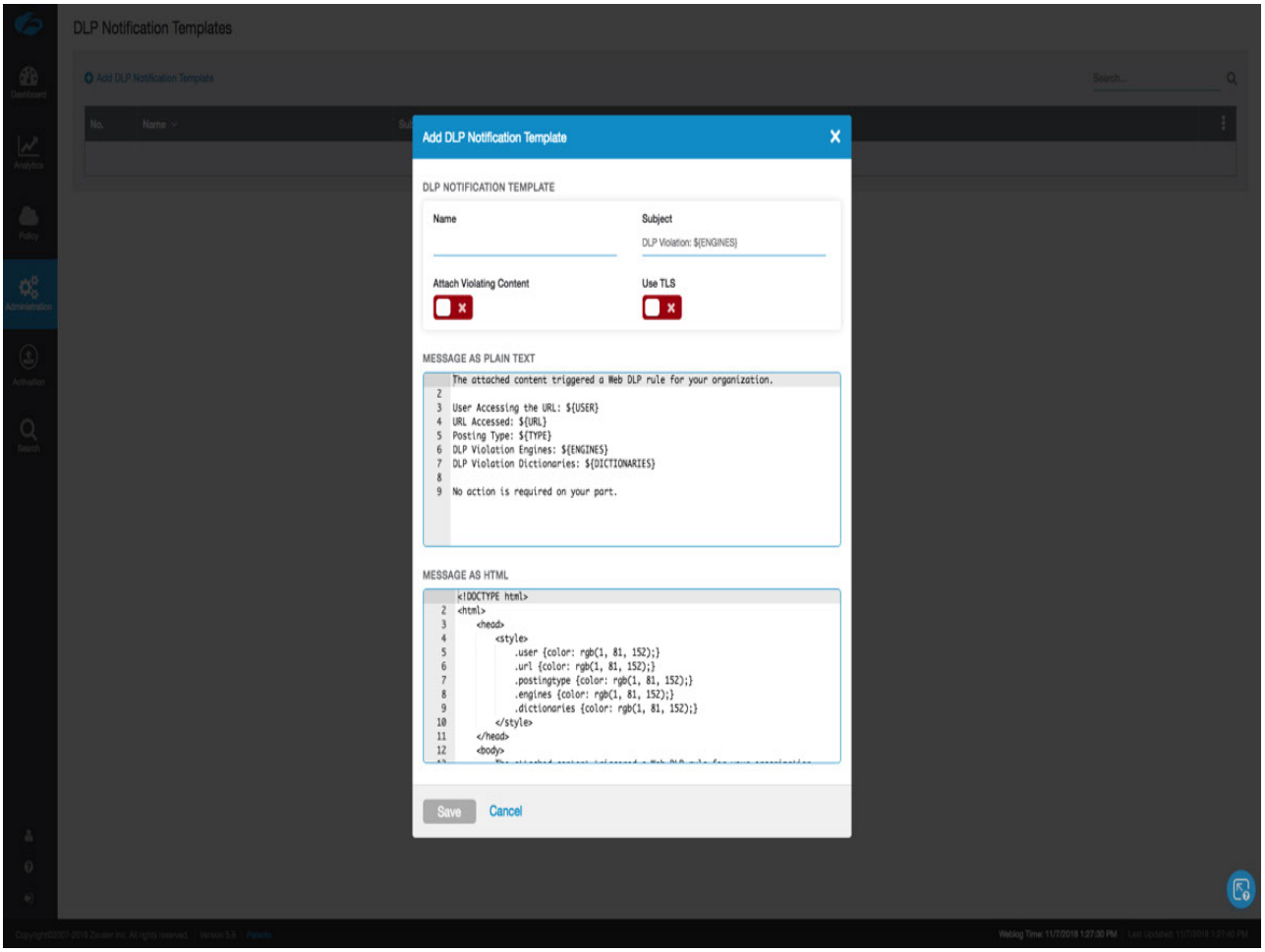
Slide 60 - Slide 60



Slide notes

You can create templates for the email notifications that are sent to your organization's auditors when a DLP Policy triggers. When configuring DLP Policy rules, you can reference one of the templates you configure here. There are no default templates, to create one click the **Add DLP Notification Template** link.

Slide 61 - Slide 61

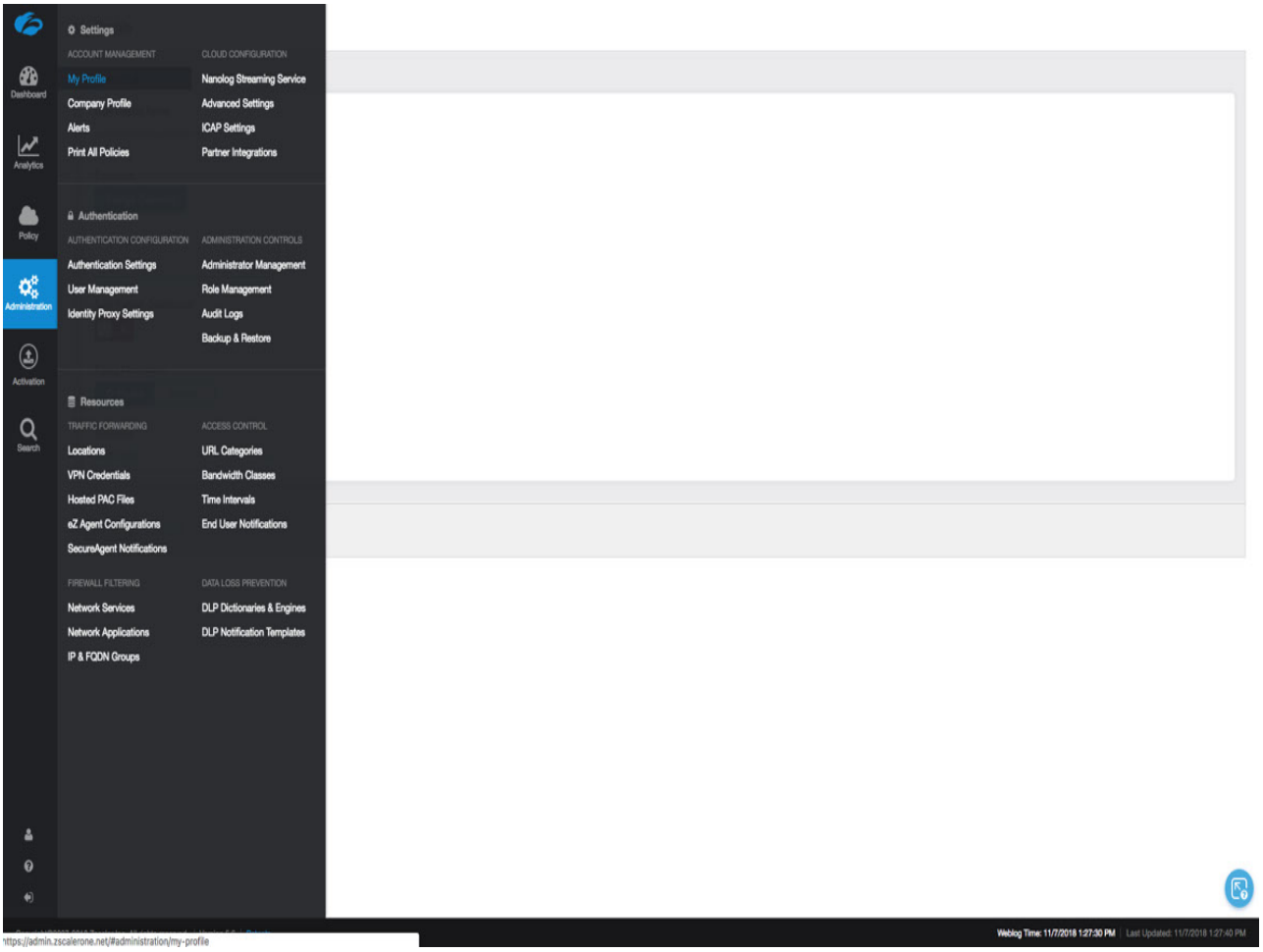


Slide notes

Name the template, specify an email **Subject**, and optionally elect to **Attach Violating Content**, or **Use TLS**. In the **Message as Plain Text**, or **Message as HTML** sections, you can create a customized message detailing why the content was blocked.

This message is delivered by email to the auditor when a DLP Policy triggers (whether or not it blocks the content). There are also a number of macros that may be used within the message text.

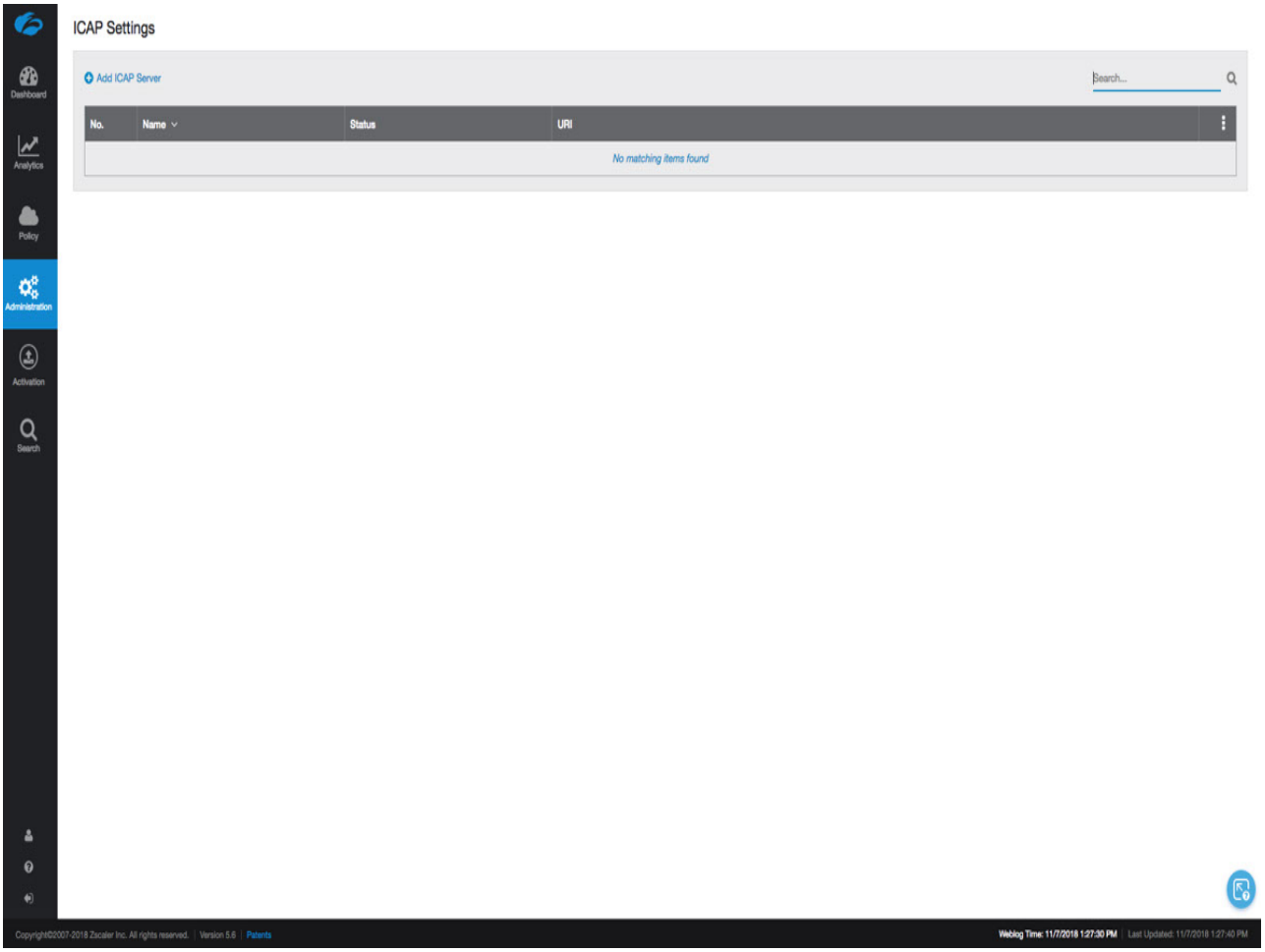
Slide 62 - Slide 62



Slide notes

To add an **ICAP Server**, from the **Administration** menu click **ICAP Settings**…

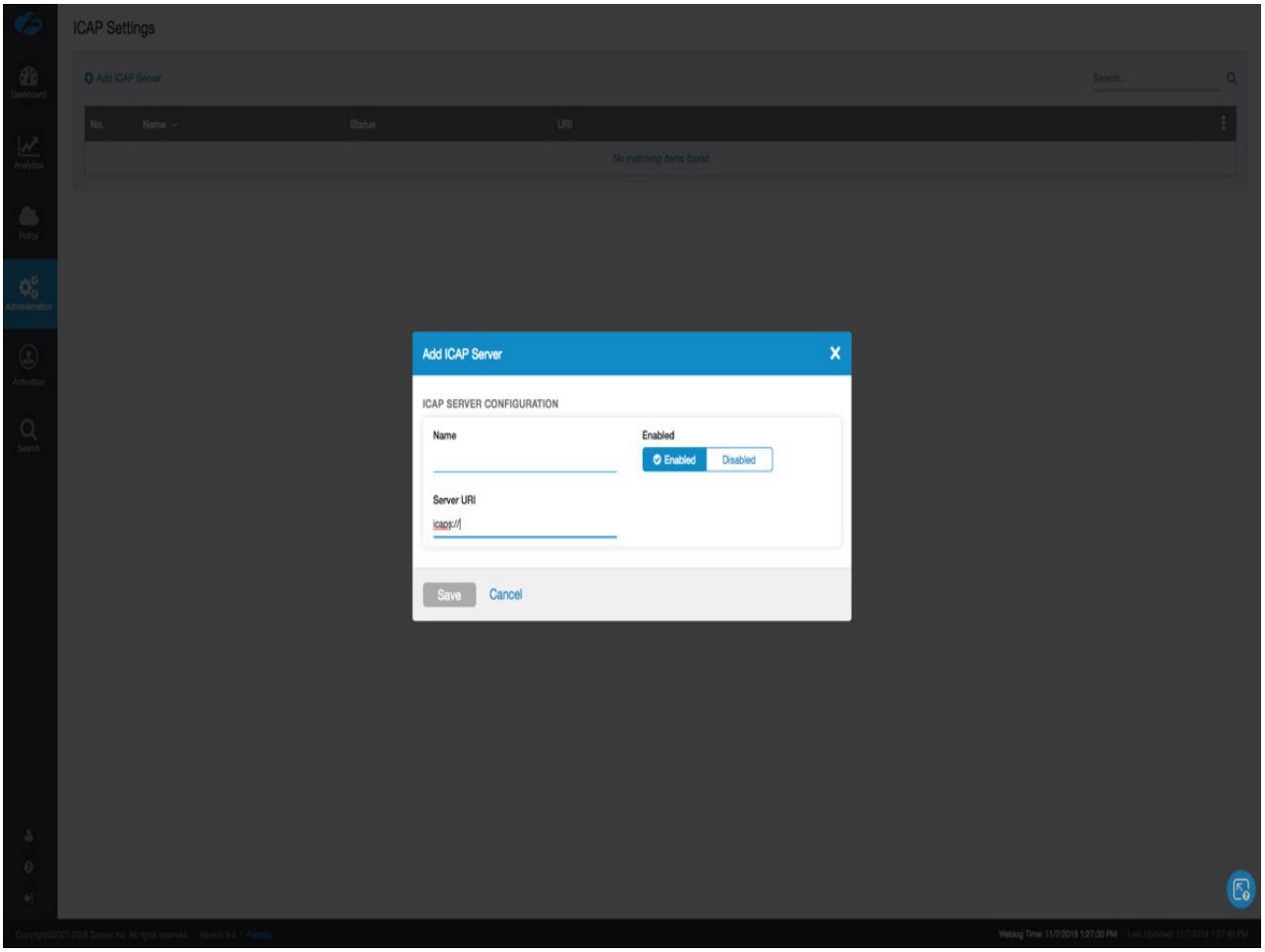
Slide 63 - Slide 63



Slide notes

...then click **Add ICAP Server**.

Slide 64 - Slide 64



Slide notes

Give the Server a **Name**, and specify the URL for the Server, then **Save** the configuration and **Activate** it. Remember, for secure ICAP the protocol for the URL must be ‘icaps://’, for insecure ICAP the protocol must be defined as ‘icap://’.

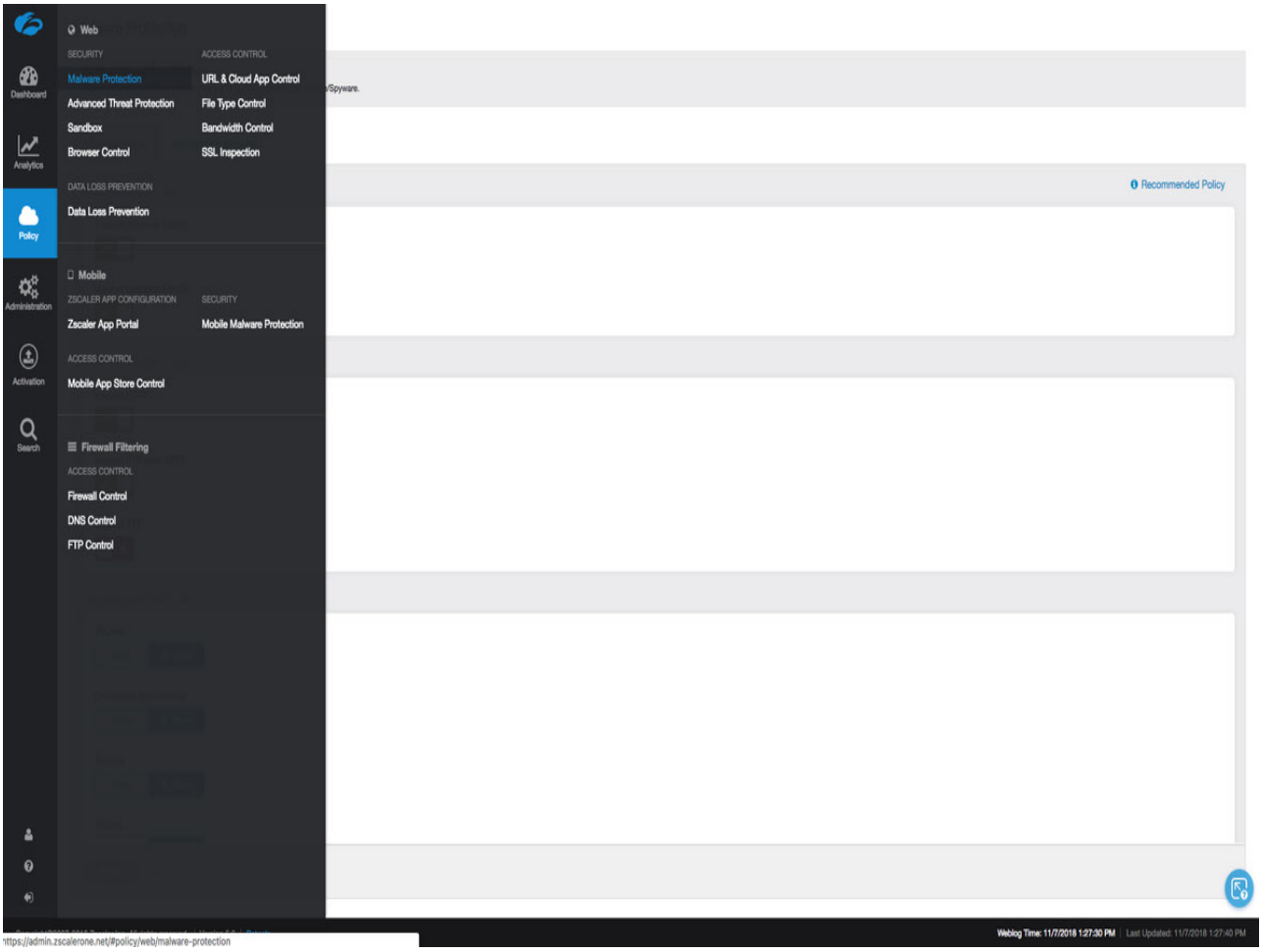
Slide 65 - Interactive Demo: DLP Policy

Slide notes

In the next section, we will have a detailed look at creating DLP Policies.

This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler App Portal UI. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

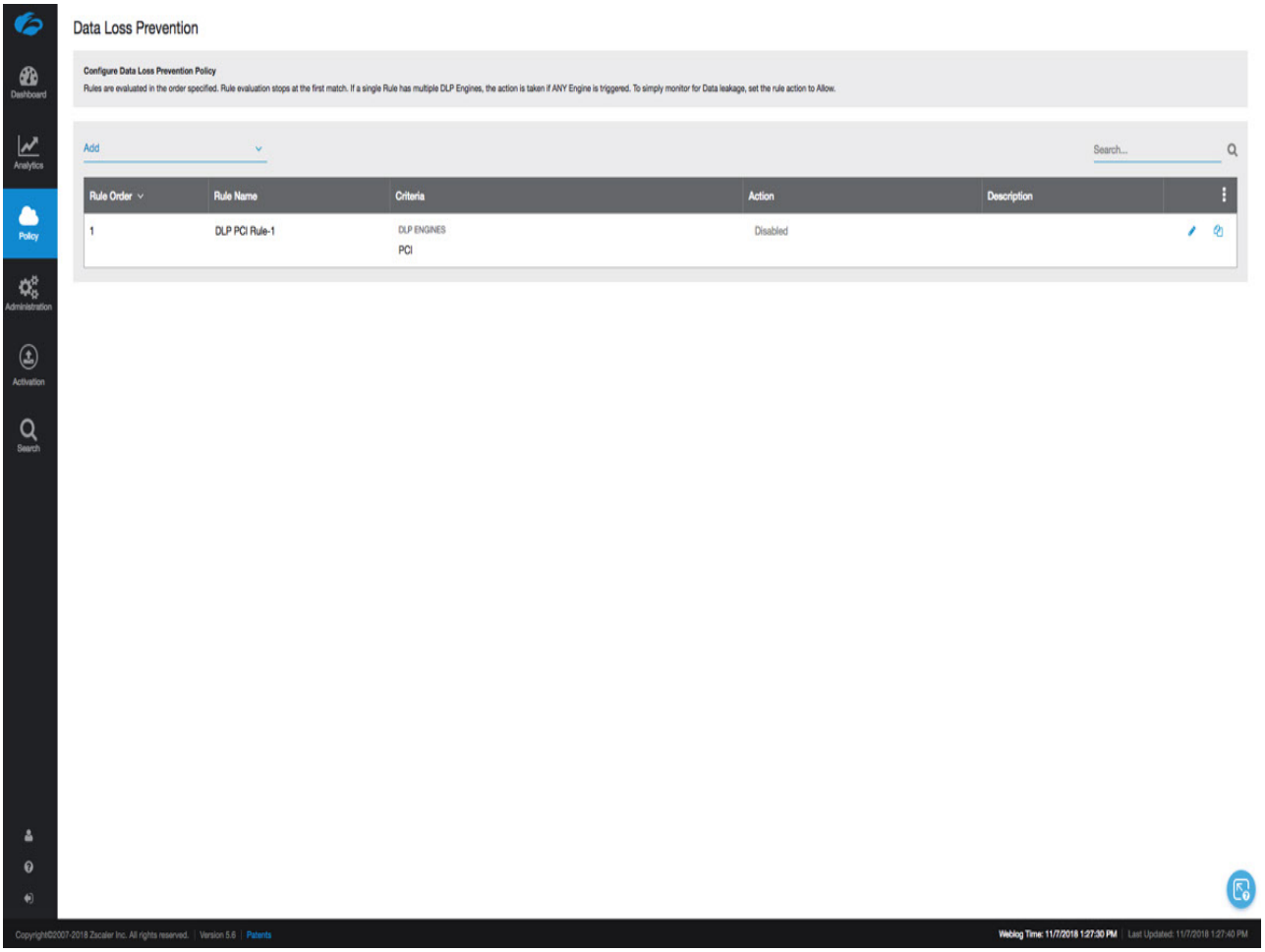
Slide 66 - Slide 66



Slide notes

To configure **Data Loss Prevention** Policy rules, from the **Policy** menu click **Data Loss Prevention**.

Slide 67 - Slide 67

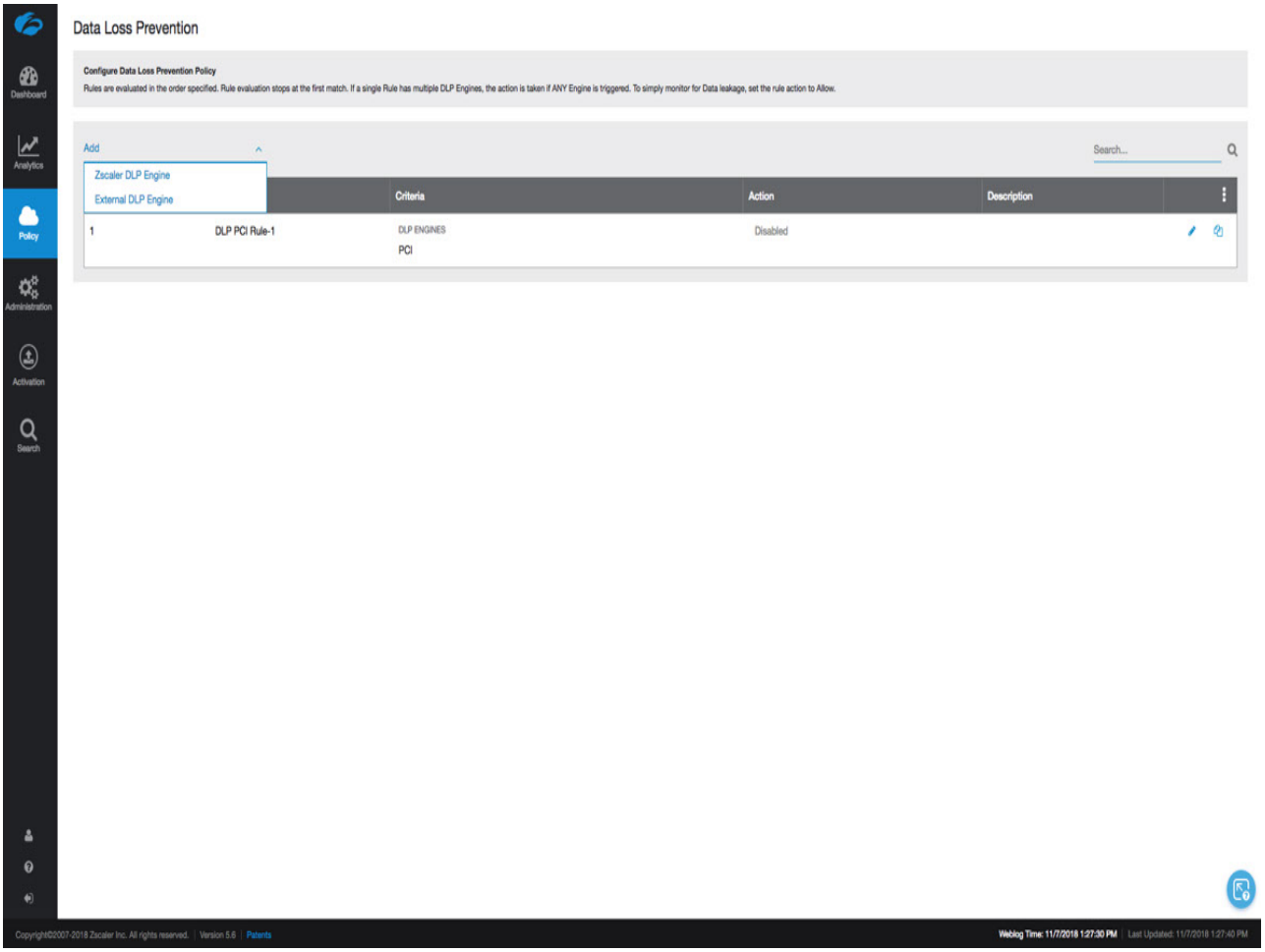


Slide notes

Corporate data can be leaked in many different ways, through Webmail, cloud storage, social media, File Transfer Protocol, and a variety of other applications. To protect your organization from data loss, Zscaler allows you to set up rules with the following options for DLP Policy: the use of Zscaler DLP Engines only; or the use of an external DLP ICAP server.

Rules are evaluated in the order specified, and rule evaluation stops at the first match, no rules are applied by default. If a single rule has multiple DLP Engines selected, the specified action is taken if ANY Engine is triggered. To simply monitor for data leakage, set the rule action to **Allow**. To add a new rule, click the **Add** field at the top.

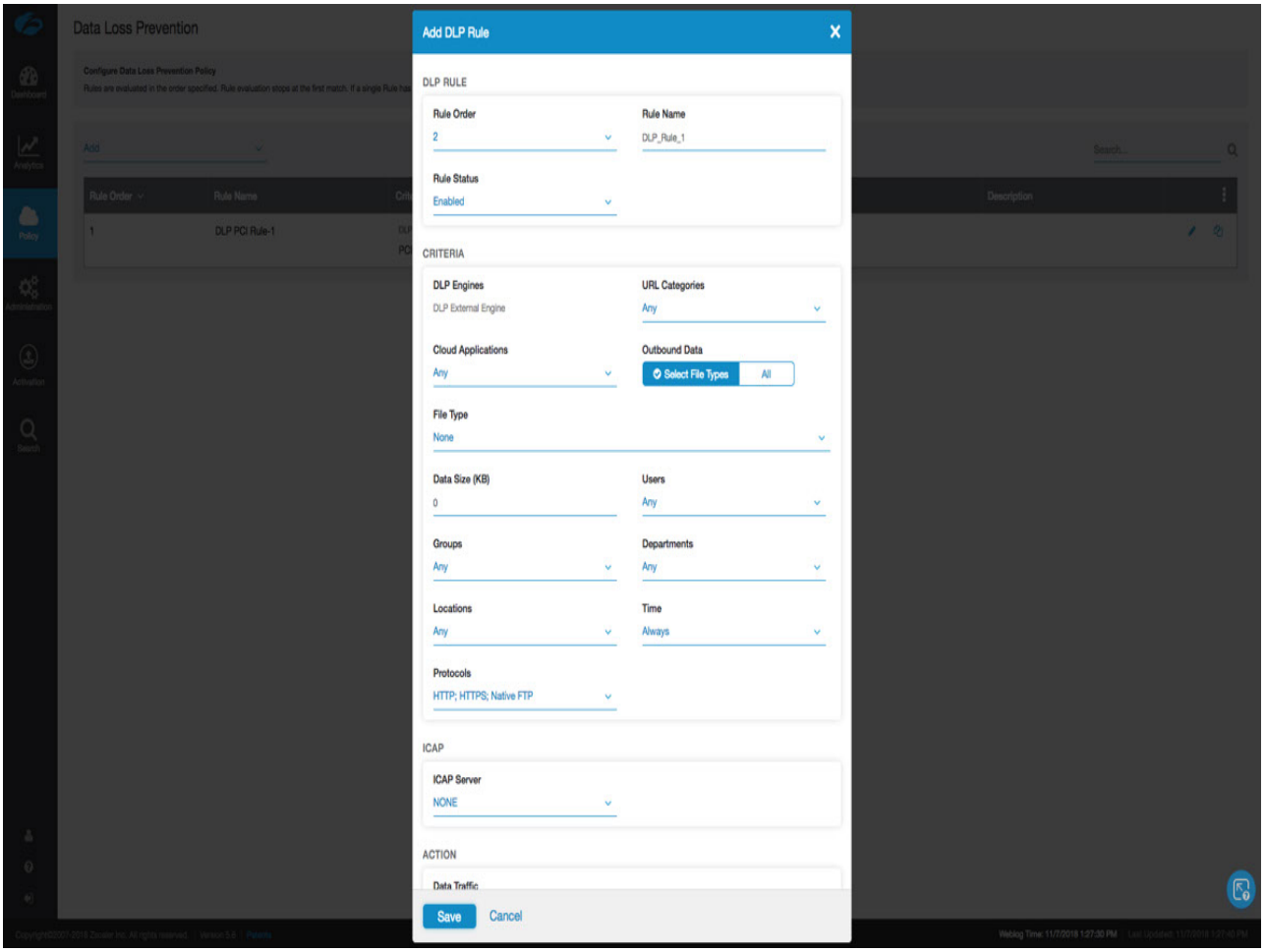
Slide 68 - Slide 68



Slide notes

If all you want to do is to forward data to an on premise DLP server, click the **External DLP Engine** option.

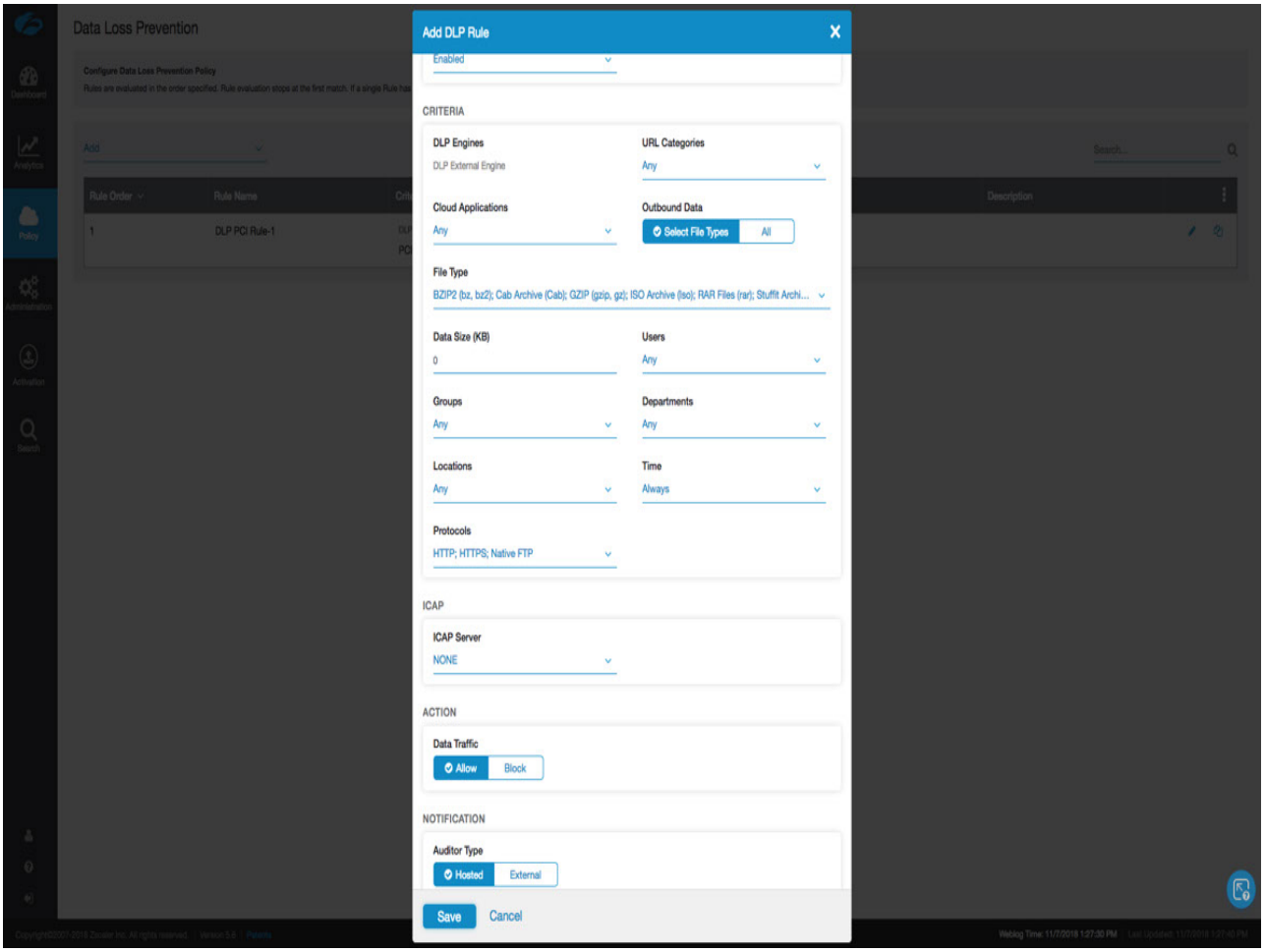
Slide 69 - Slide 69



Slide notes

Set the **Rule Order** and **Rule Status**, and specify the **Rule Name**. You have the option to accept the default name of the rule, or to edit it to provide a meaningful custom name.

Slide 70 - Slide 70

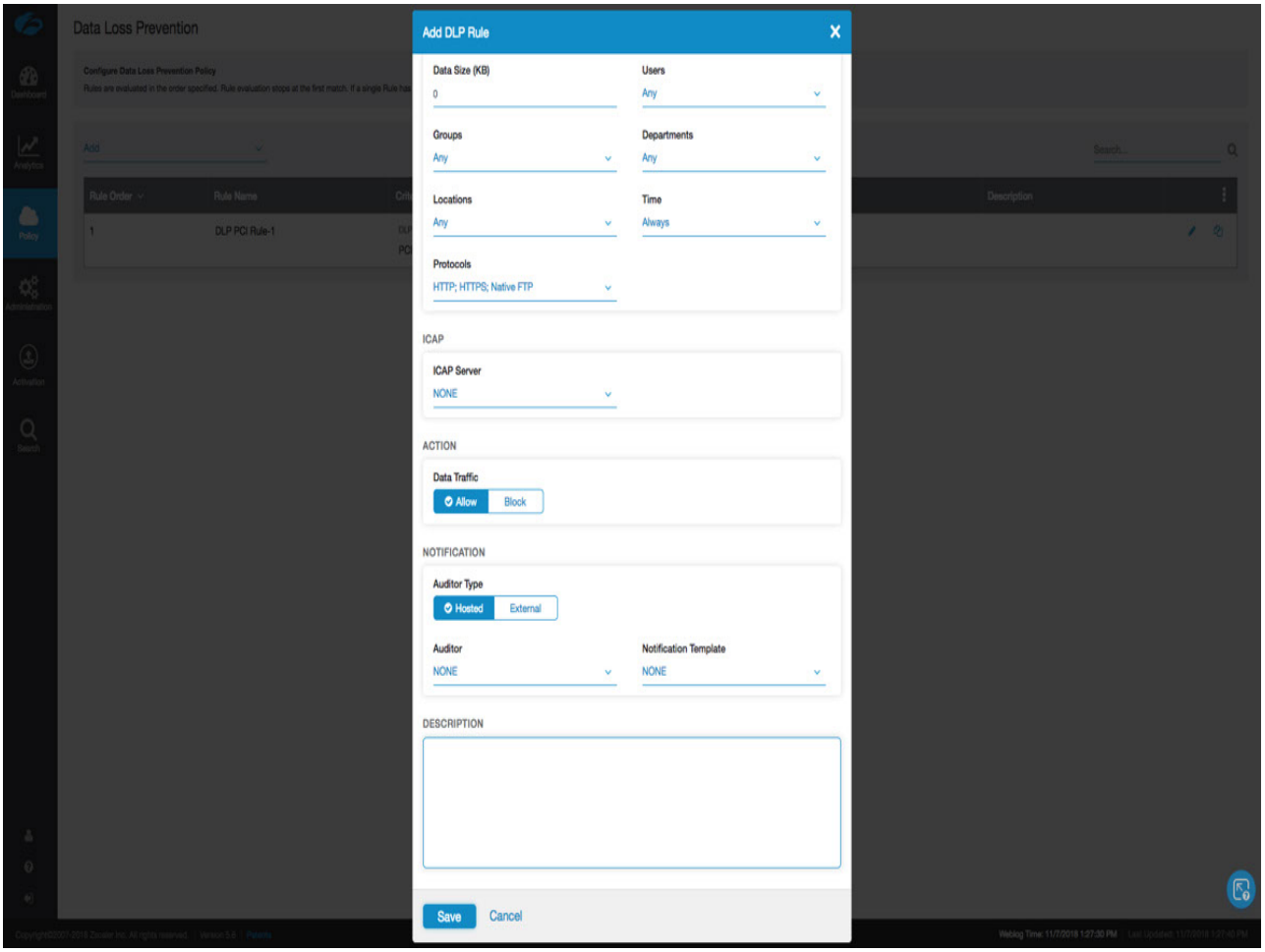


Slide notes

Configure the target **Criteria** as required, in this case the criteria available are: **URL Categories**; **Cloud Applications**; **File Type**; **Data Size (KB)**; **Users**; **Groups**; **Departments**; **Locations**; and **Time**.

Note that for the 'Outbound Data' criteria, you may either select **All**, or use the **Select File Type** option to select specific types of file to be scanned.

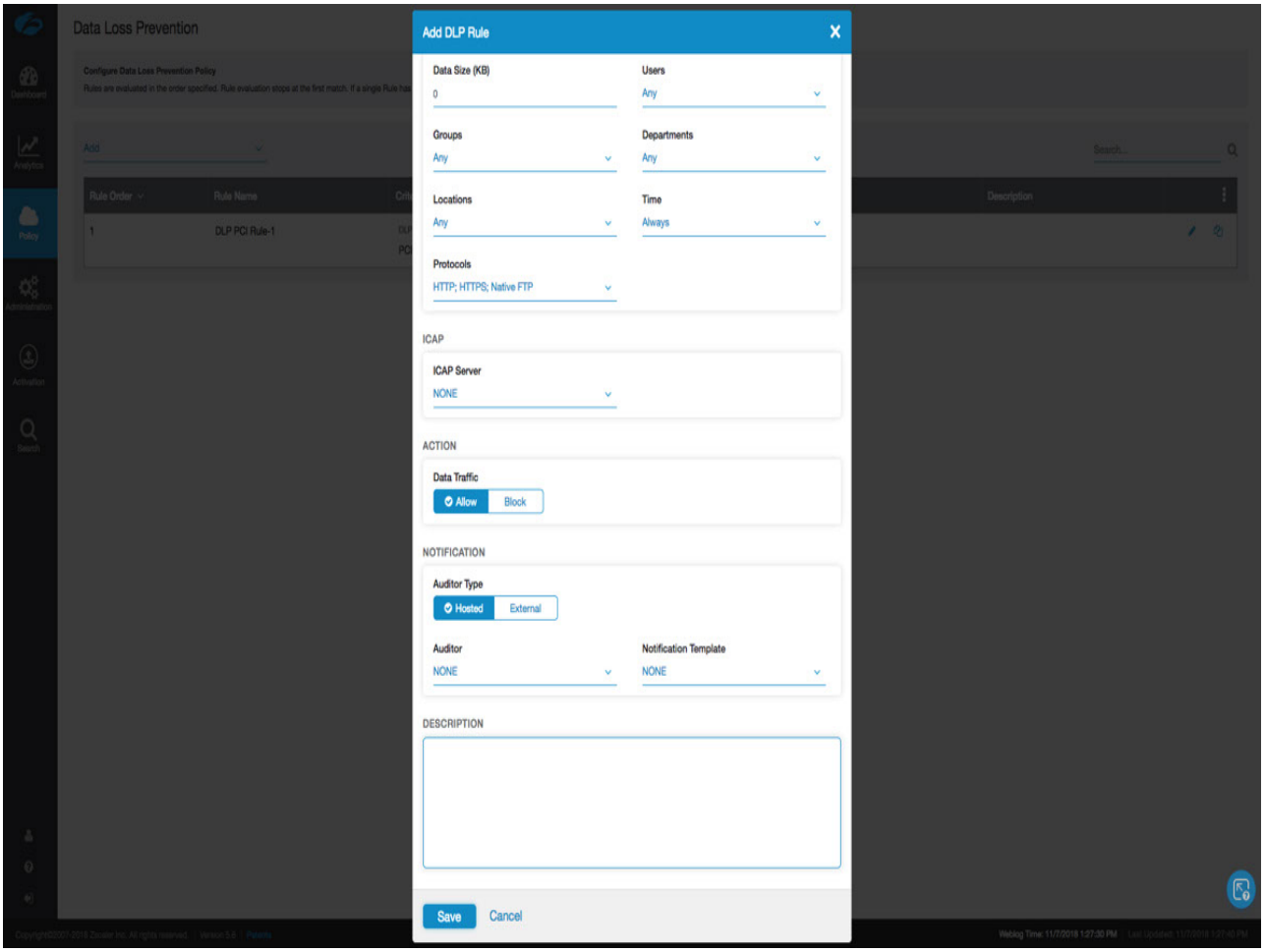
Slide 71 - Slide 71



Slide notes

For an **External DLP Engine** rule, you must send data to an on premise (or cloud-based) **ICAP Server**, select the server here to send the data to. ICAP Servers must have been added previously, as we described in the earlier section.

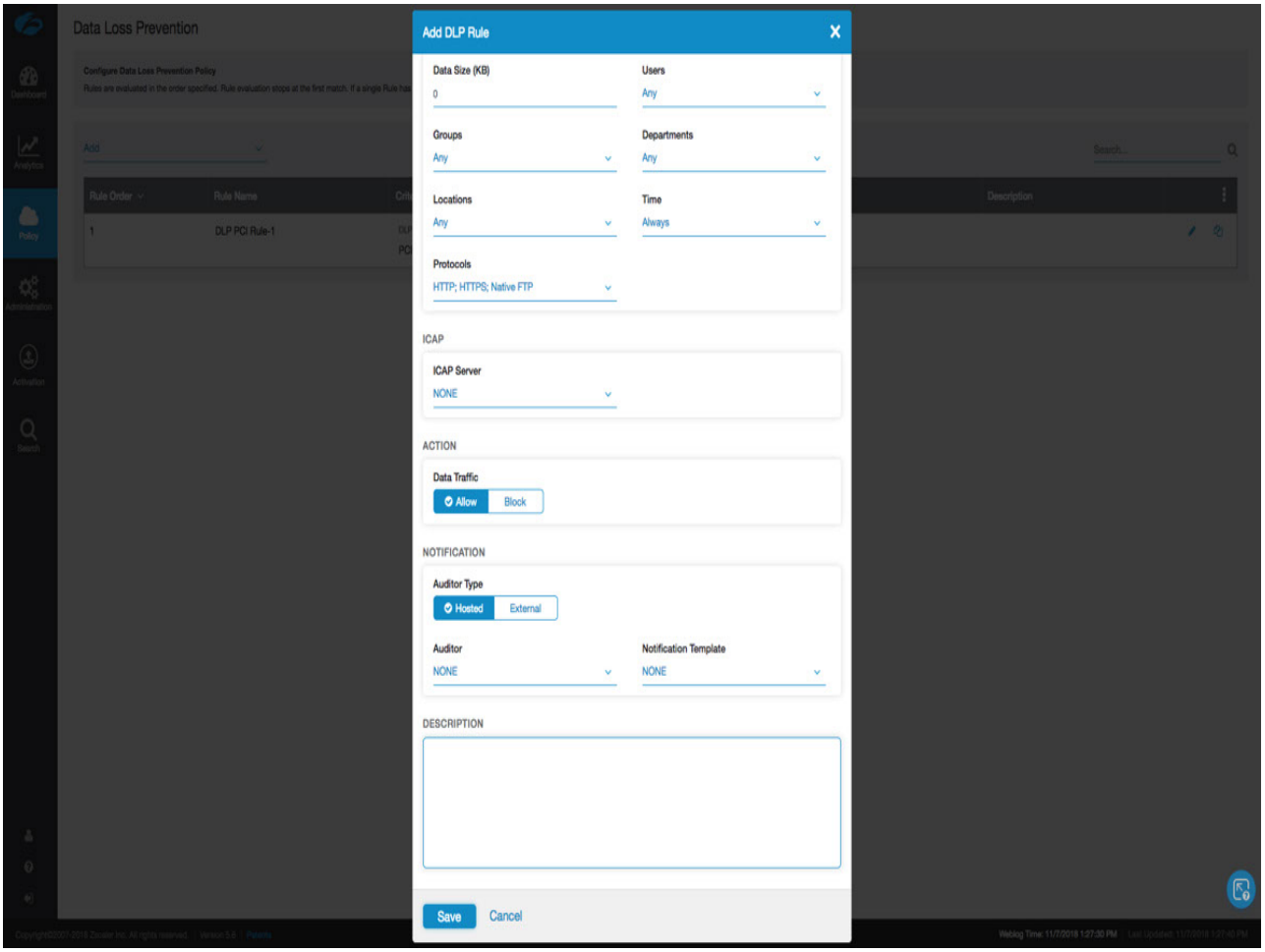
Slide 72 - Slide 72



Slide notes

The only **Actions** available for this type of rule are **Allow**, or **Block** traffic that matches the rule. If you select **Allow**, the service will allow but log the transaction, and if you select **Block**, the service will block and log the transaction.

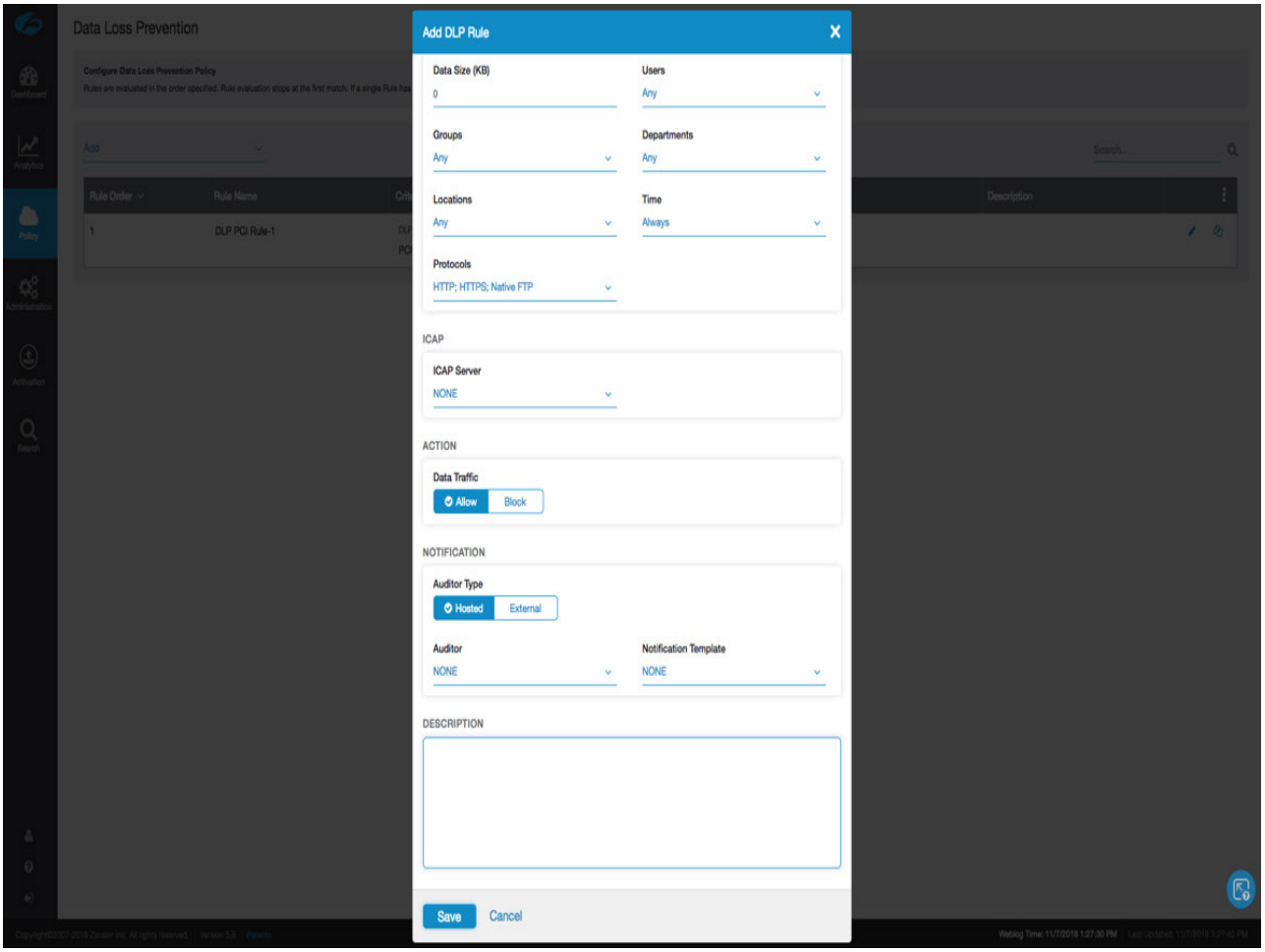
Slide 73 - Slide 73



Slide notes

You can configure an email **Notification** for the rule, to be sent to a **Hosted** auditor (just select the user to send mail to), or to an **External** auditor (an email address is required). You must also select a **Notification Template** from the dropdown menu, from the templates that you created earlier.

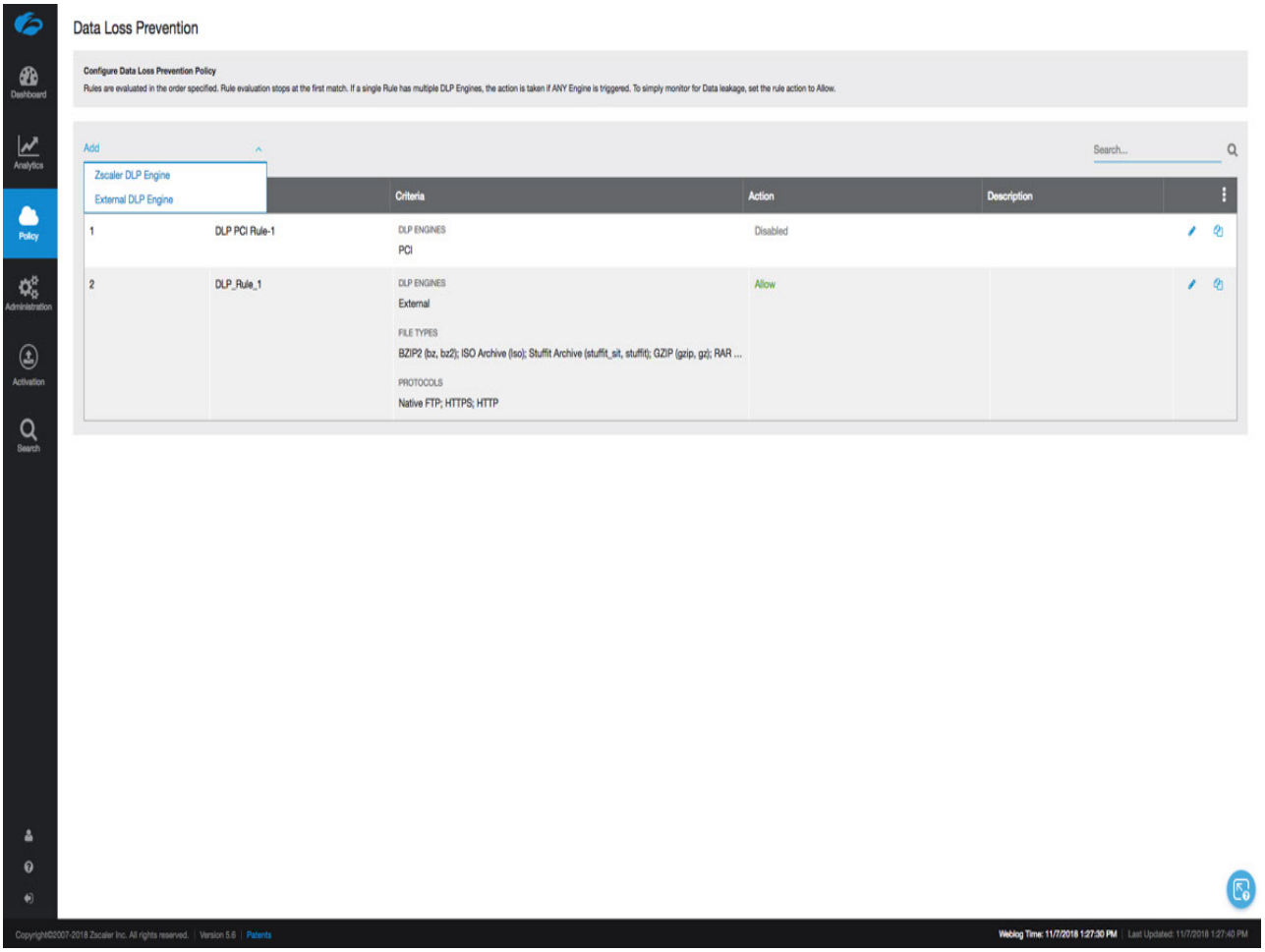
Slide 74 - Slide 74



Slide notes

Once you have fully configured the rule, click **Save**, then **Activate** your changes.

Slide 75 - Slide 75

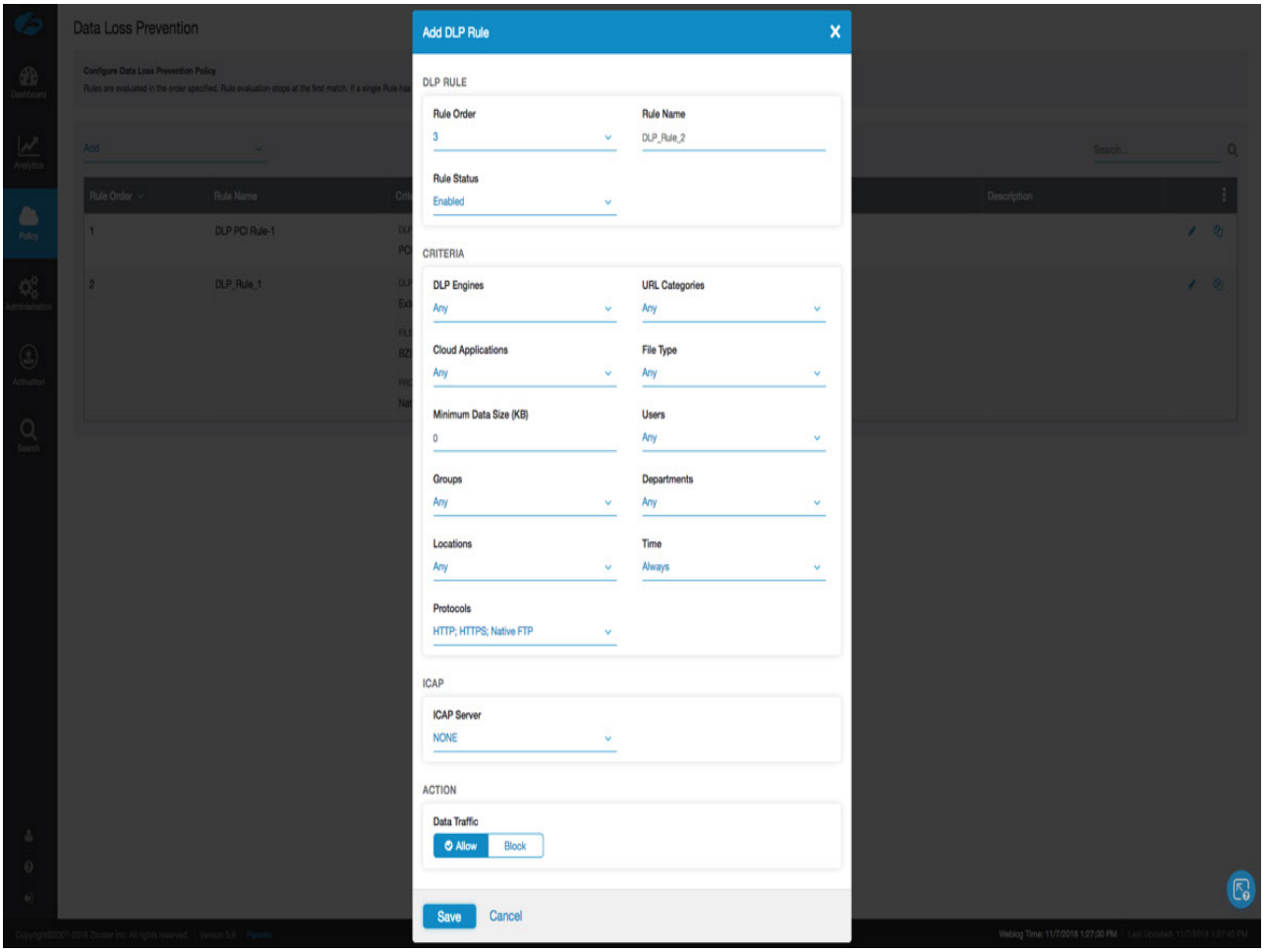


Slide notes

If all you want to do is to forward data to an on premise DLP server, click the **External DLP Engine** option.

To create a **Zscaler DLP Engine** Policy rule, from the **Add** field, click the **Zscaler DLP Engine** option.

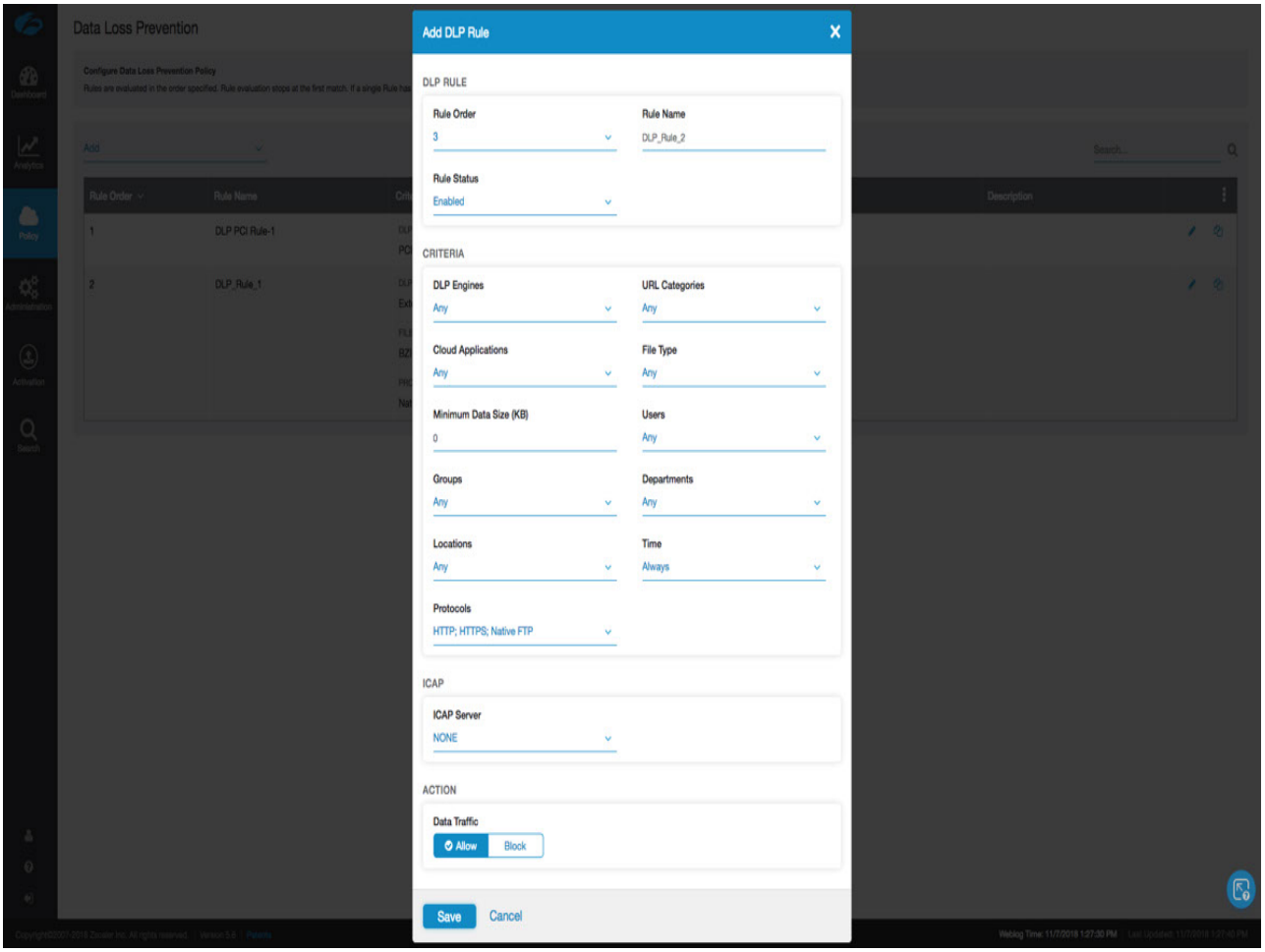
Slide 76 - Slide 76



Slide notes

As before, set the **Rule Order**, **Rule Status**, and **Rule Name**.

Slide 77 - Slide 77

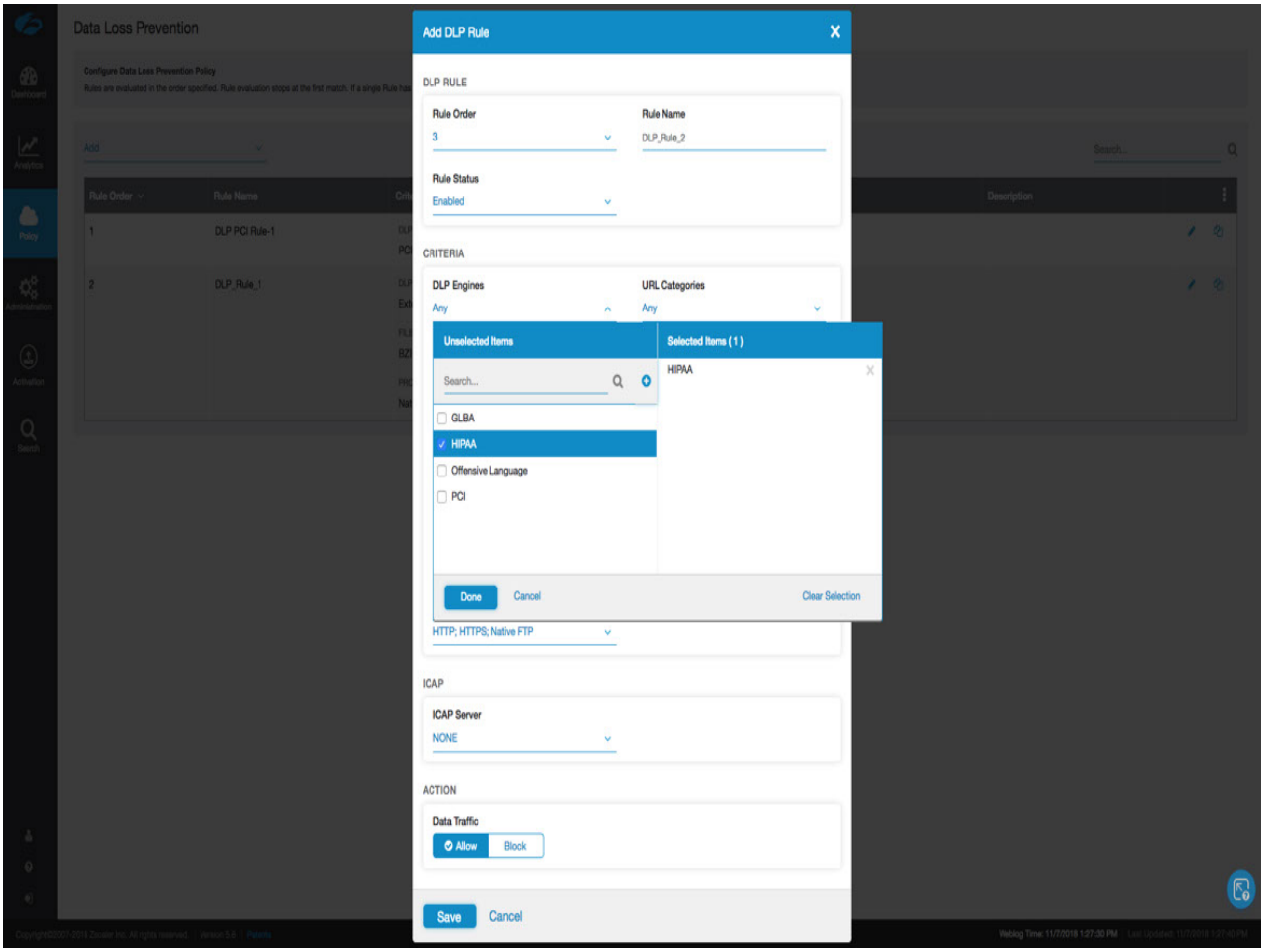


Slide notes

The only significant difference to an **External DLP Engine** Policy rule, is in the **Criteria** section where the **DLP Engines** are available to be selected as well as all the other criteria.

This gives Zscaler the unique ability to make intelligent decisions about when to block traffic, or alert an auditor, based on the Zscaler standard Dictionaries, or the custom Dictionaries that you created.

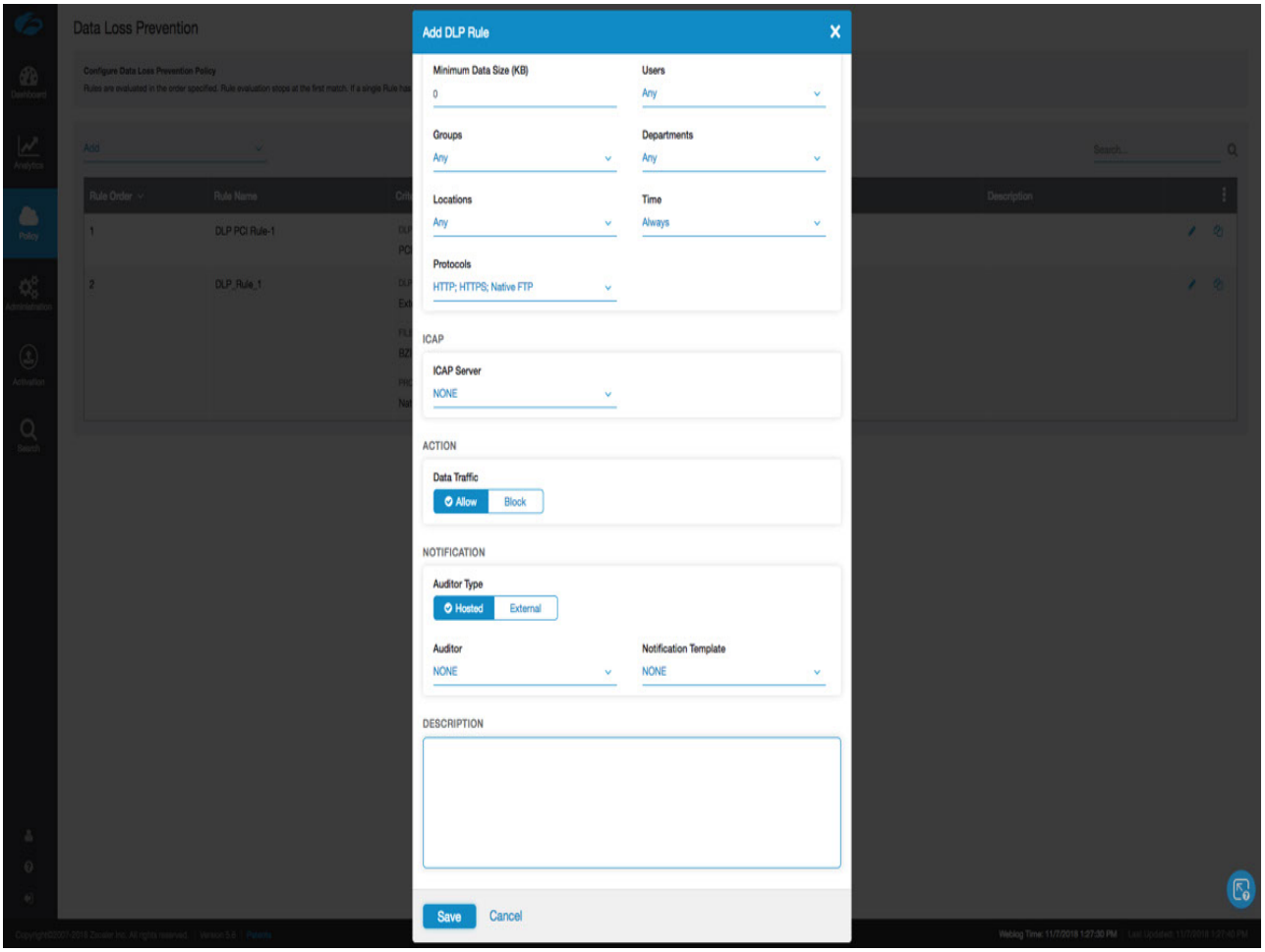
Slide 78 - Slide 78



Slide notes

Select from the Zscaler standard Engines, or those that you added yourself, as discussed previously. Note that the rule **Action** will be taken if any one of the added Engines triggers.

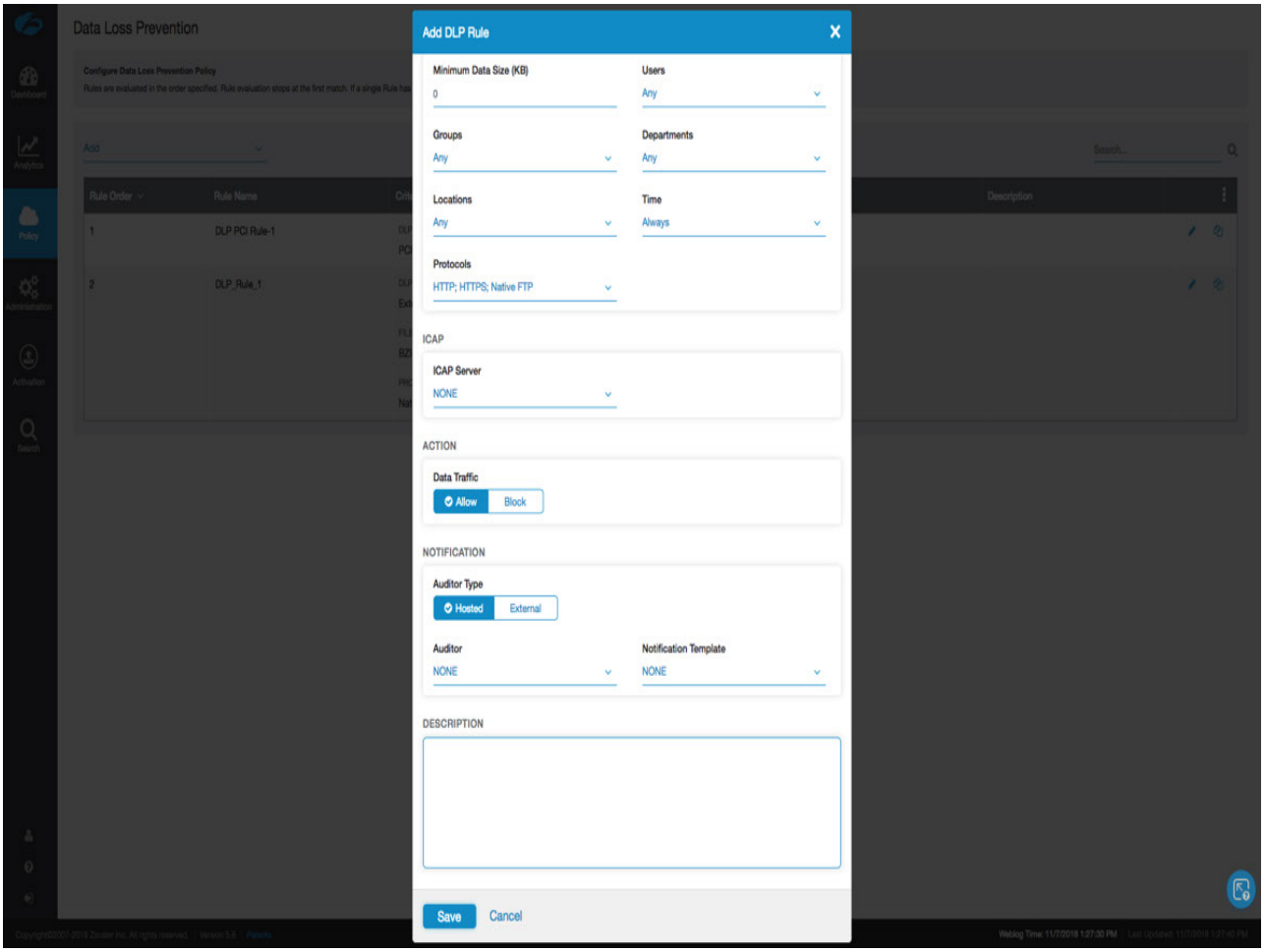
Slide 79 - Slide 79



Slide notes

For a **Zscaler DLP Engine** Policy rule you may also elect to send data to an on premise **ICAP Server**, although in this case this is optional.

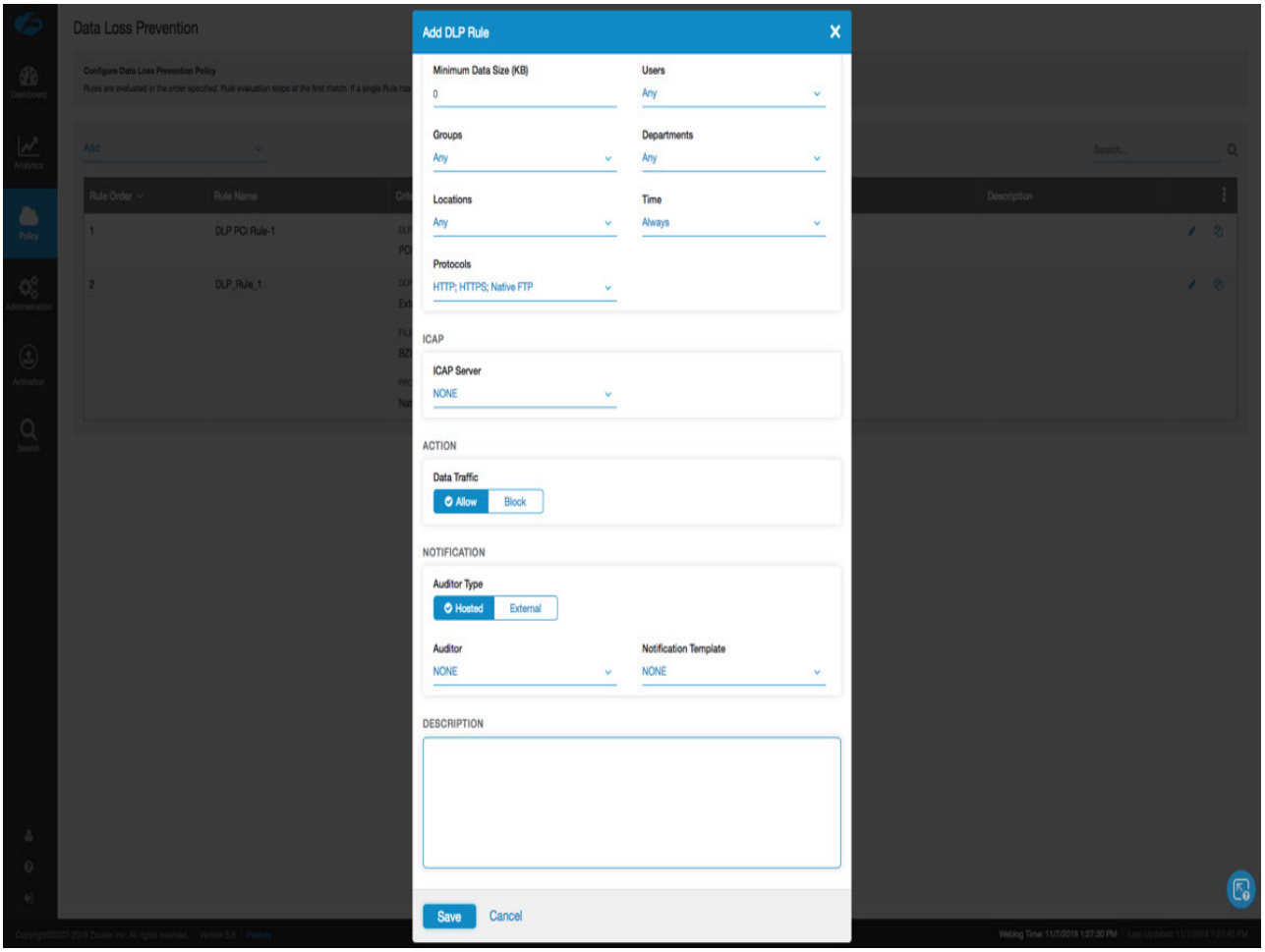
Slide 80 - Slide 80



Slide notes

Once again, the **Actions** available are **Allow**, or **Block** traffic that matches the rule. As before, if you select **Allow**, the service will allow but log the transaction, and if you select **Block**, the service will block and log the transaction.

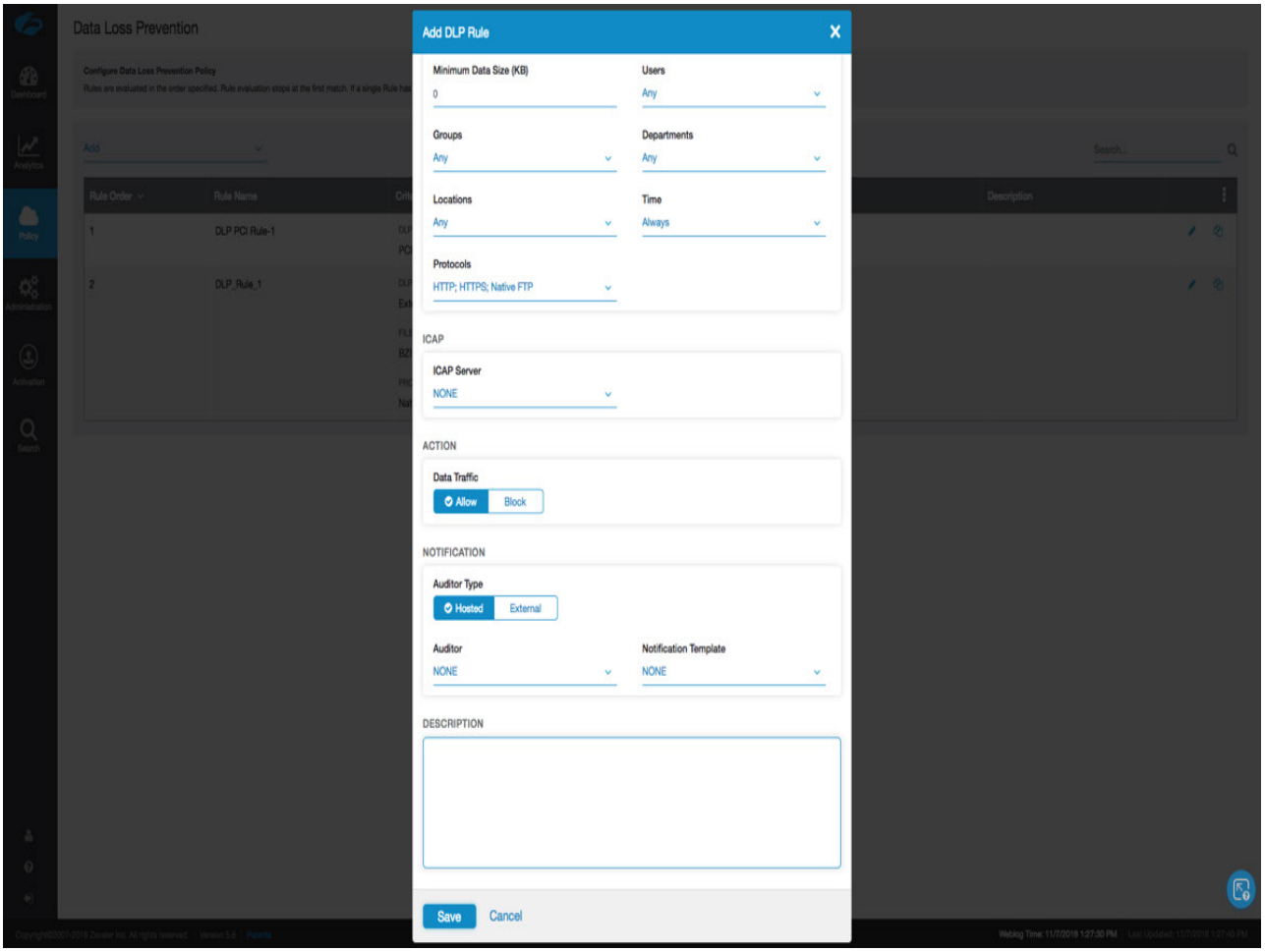
Slide 81 - Slide 81



Slide notes

The same options to configure an email **Notification** is available, to be sent to a **Hosted** or **External** auditor. As before, you must also select a **Notification Template** from the dropdown menu, from the templates that you created on the **Administration > DLP Notification Templates** page.

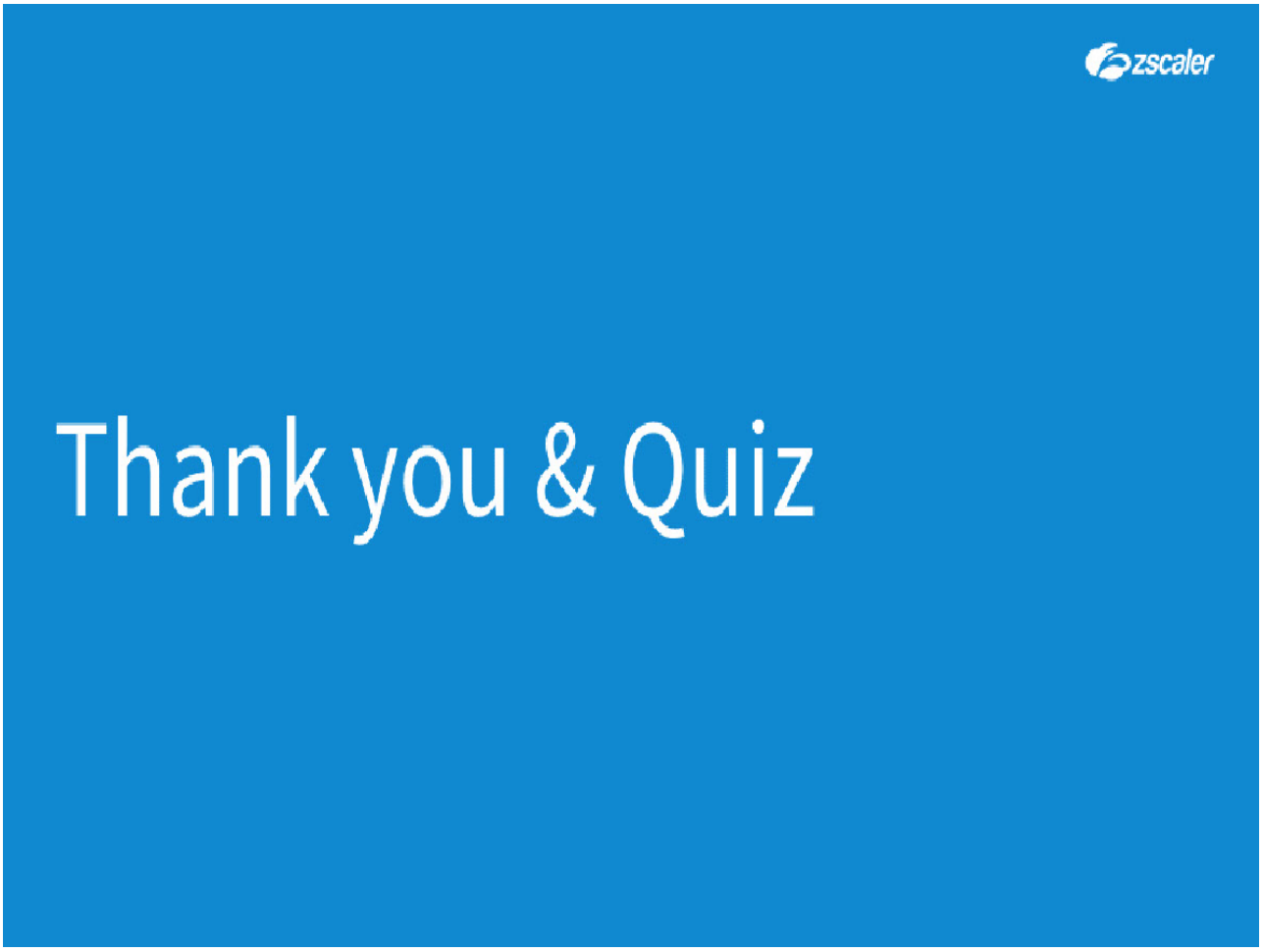
Slide 82 - Slide 82



Slide notes

Once you have fully configured the rule, click **Save**, then **Activate** your changes.

Slide 83 - 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.