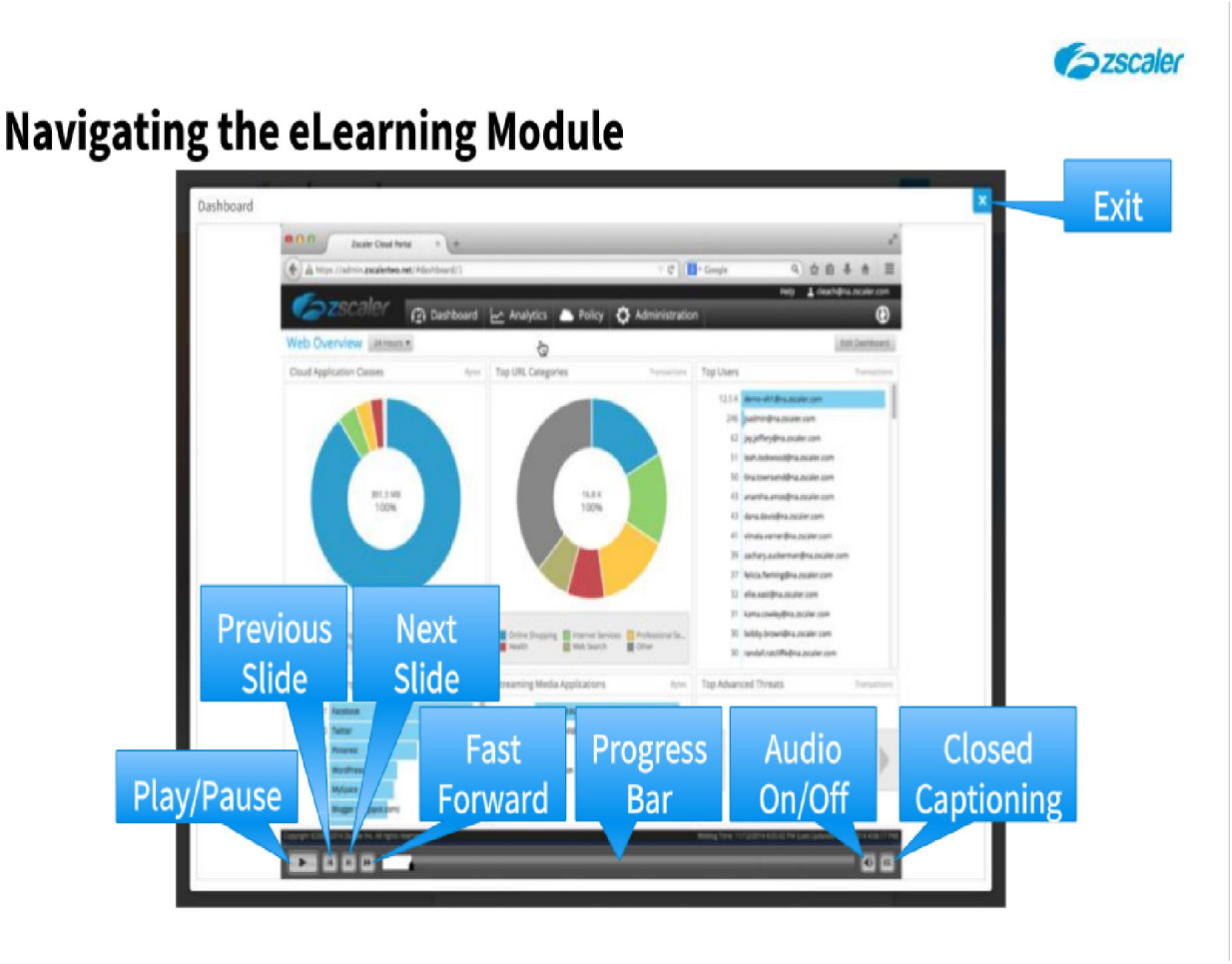
Slide 1 - Zscaler Internet Access

Slide notes

Welcome to this Zscaler Internet Access module on Configuring DNS Security and Optimization.

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 may also mute the audio or enable Closed Captioning to display a transcript of the narration on the screen. Finally, you can click the **X** button at the top to exit.

Slide 3 - Agenda

Slide notes

After completing this module you will be able to:

• Describe the services that Zscaler Internet Access provides for DNS traffic Security & Optimization;

• Configure ZIA DNS Control Policies;

• Configure ZIA DNS Tunneling Policies; and

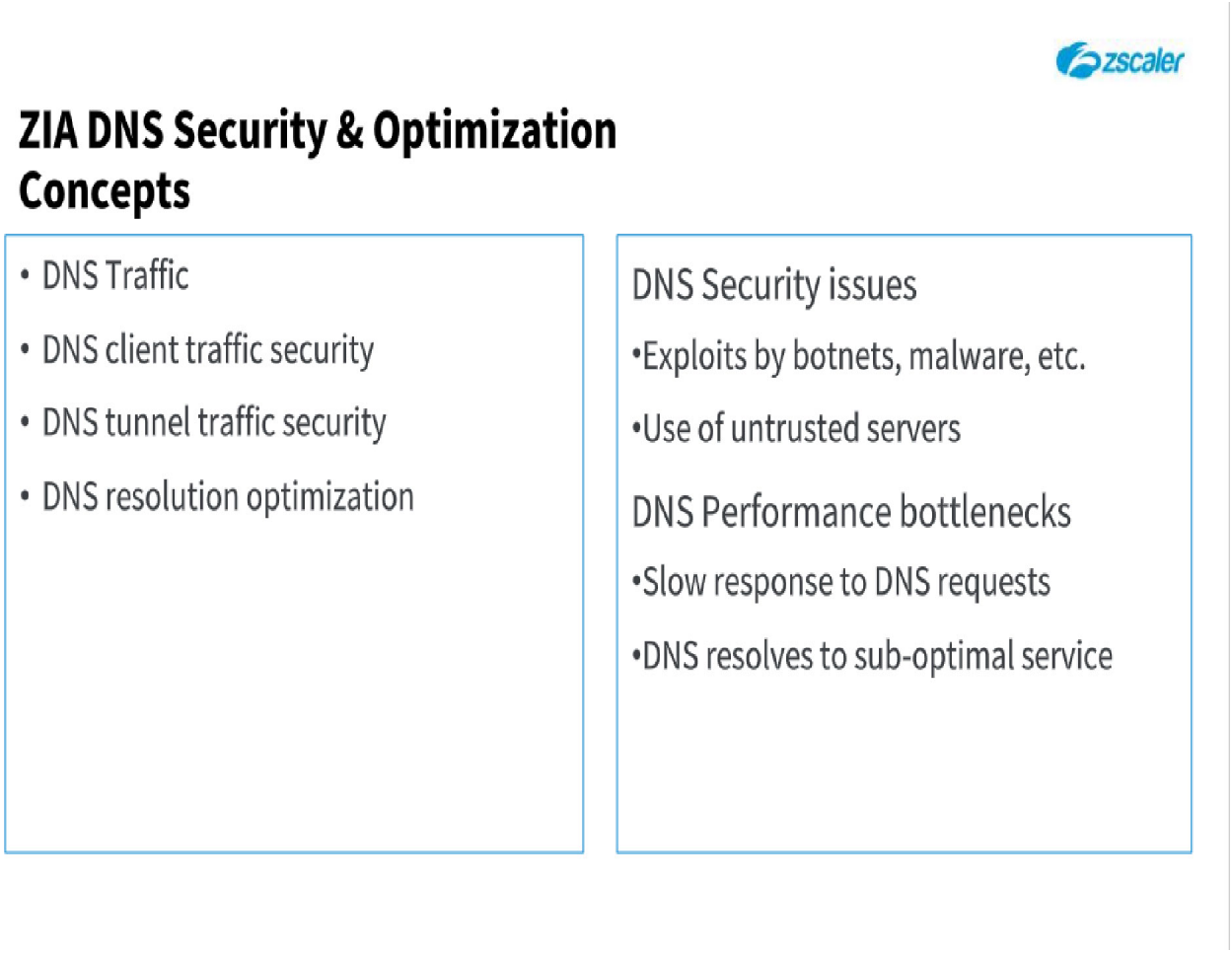
• Configure ZIA to optimize DNS Resolution

Slide 4 - ZIA DNS Security & Optimization

Slide notes

The Domain Name System, or DNS, is a critical part of the internet. Users depend on it to provide reliable and quick lookups to resolve names to IP address of hosts to connect to for service. In this part Zscaler Internet Access features are described that provide security of DNS results and help to optimize DNS performance.

Slide 5 - ZIA DNS Security & Optimization Concepts



Slide notes

To configure ZIA DNS security and optimization requires an understanding of :

• the different types of DNS traffic that may be inspected and controlled by ZIA;

• the policies that may be applied to protect DNS client traffic and data; and

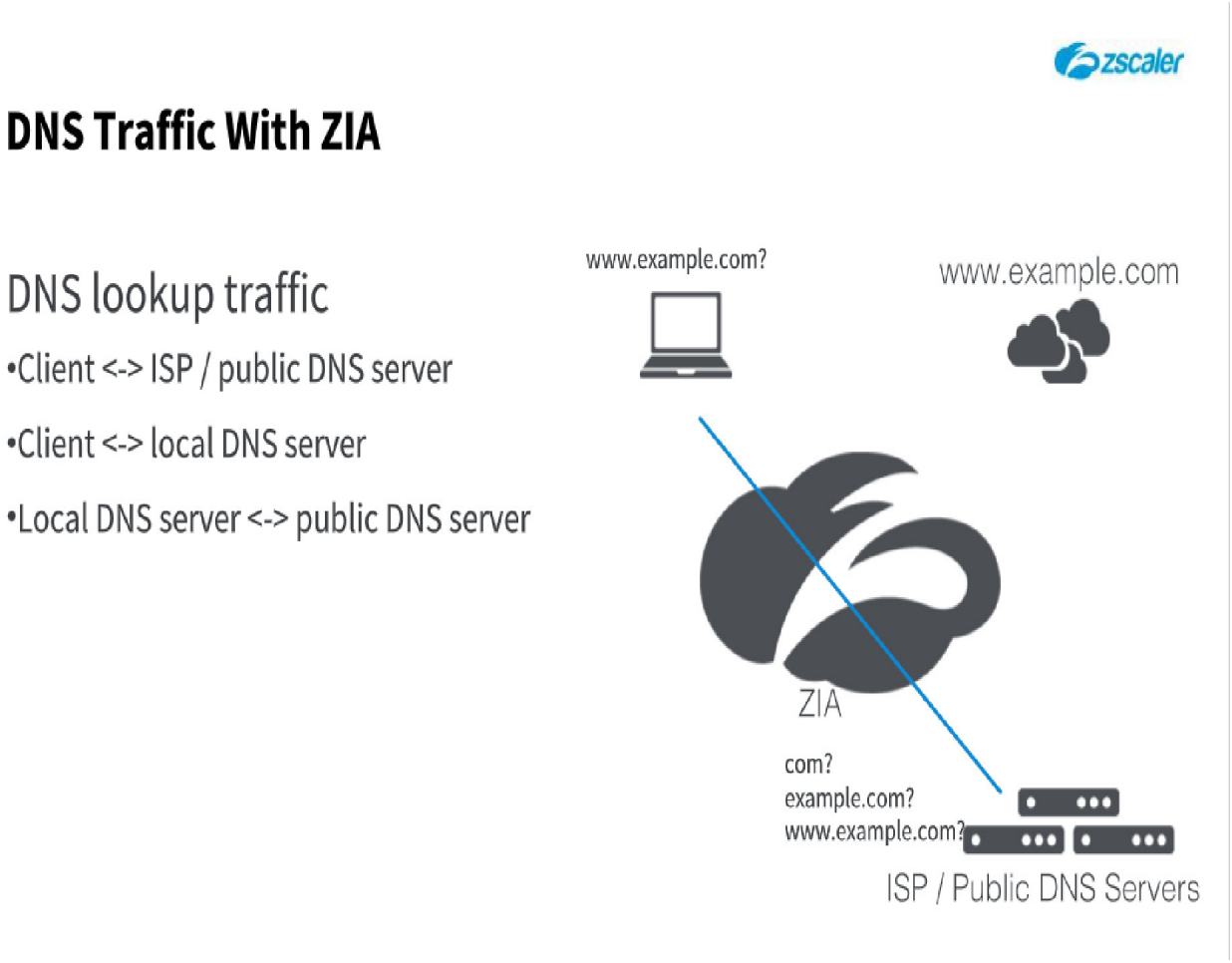
• the applications that may tunnel within DNS and the policies to control them.

DNS traffic is vulnerable to a number of potential security issues and performance bottlenecks.

From the security perspective, DNS can be exploited for malicious purposes such as botnet communication and to spread malware. The expense and effort that goes into securing DNS data may also be undermined by users receiving results from untrusted DNS servers.

From an Internet application performance perspective, name resolution is the first step that must complete in a request so any slowness in a DNS response diminishes the user experience. With clients and services being distributed to many different locations on the internet, DNS lookups may not resolve to a server that is geographically nearest the client or providing the fastest response to the client.

Slide 6 - DNS Traffic With ZIA

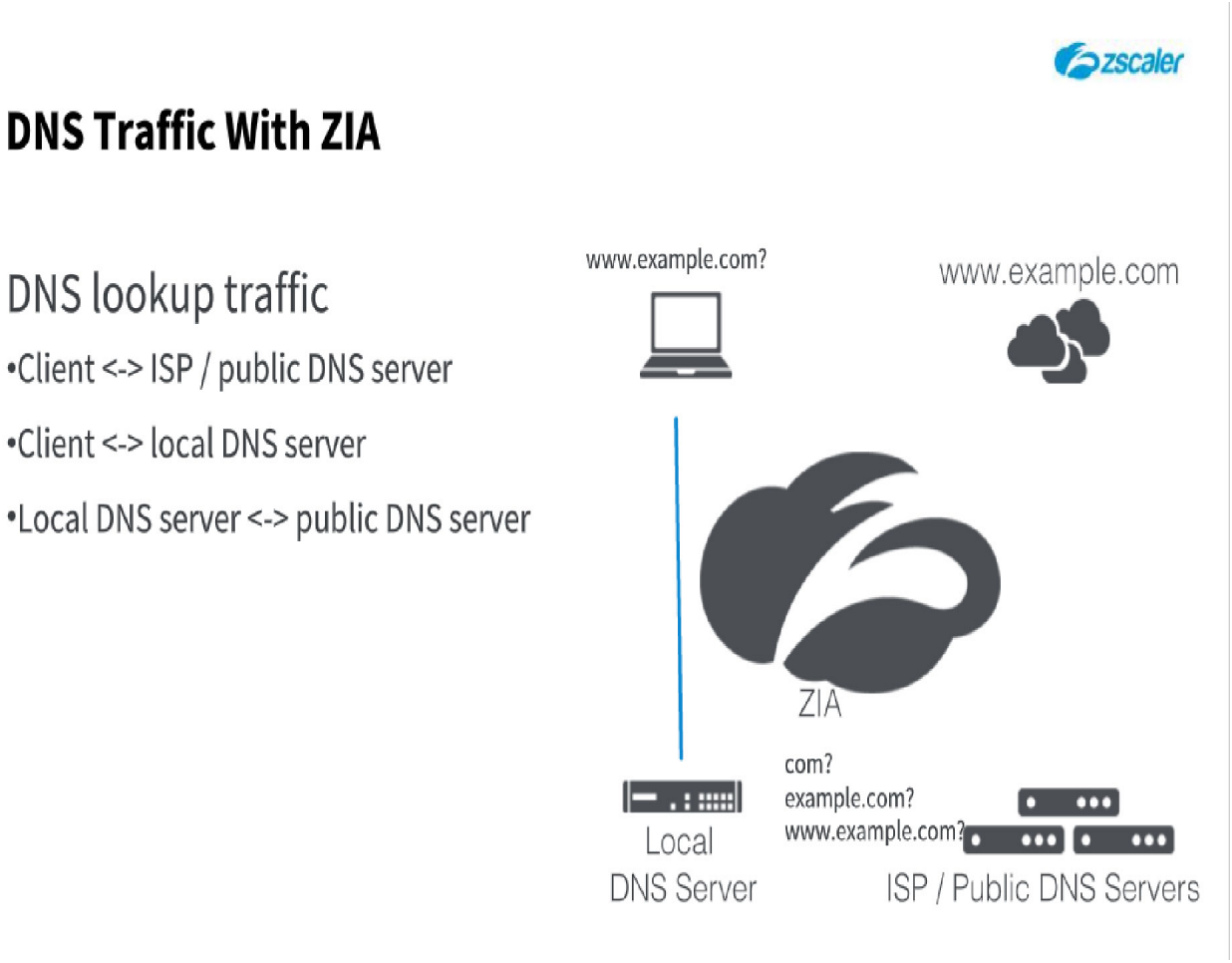


Slide notes

DNS lookup activity and applications tunneling through DNS are two primary sources of DNS traffic that flow through ZIA.

DNS lookup traffic comes from clients doing lookups on DNS servers provided by their ISP or through other public internet servers. This traffic passes through ZIA.

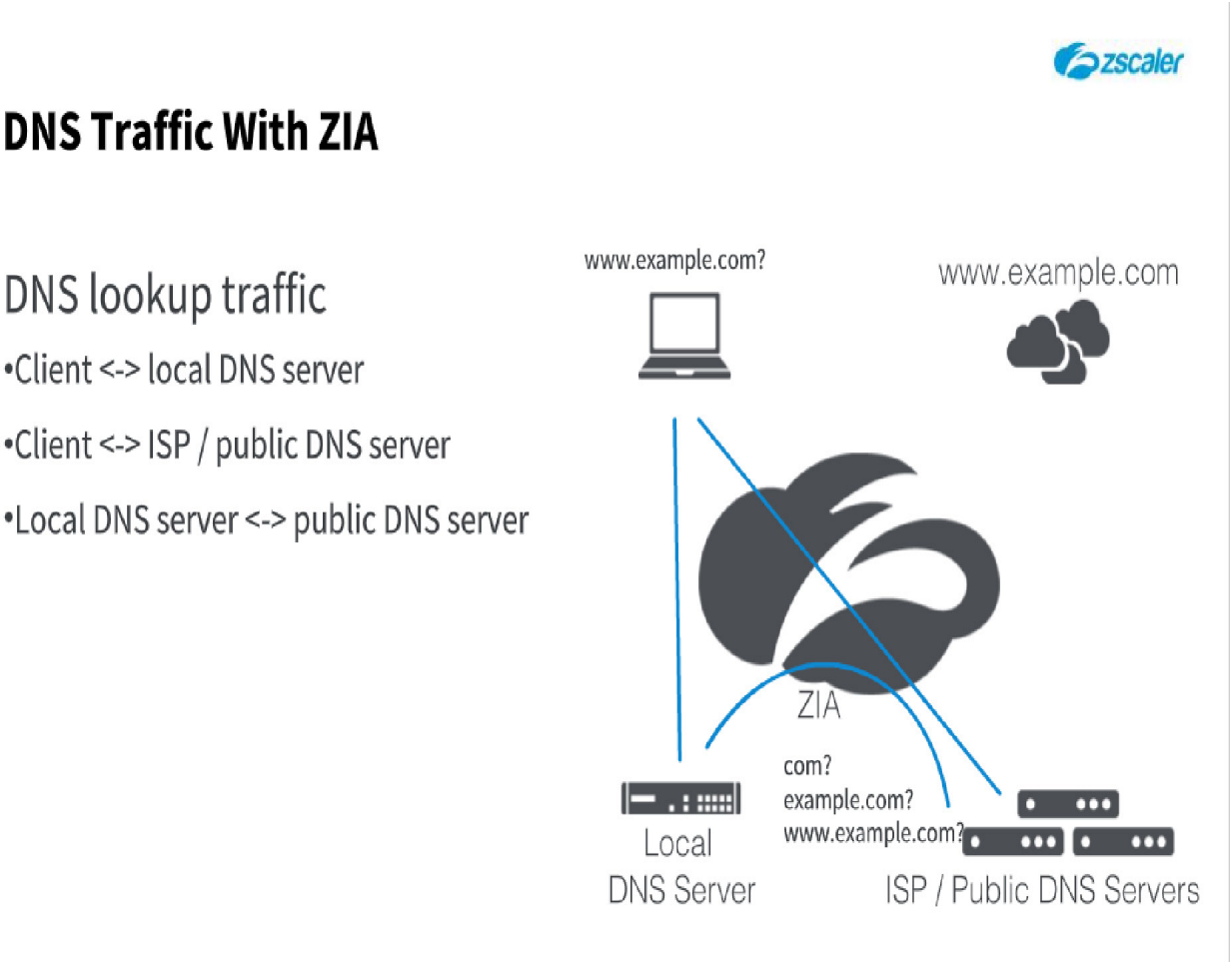
Slide 7 - DNS Traffic With ZIA



Slide notes

Organizations might configure client lookups to go to a local DNS server on the LAN or WAN, so this would not flow through ZIA.

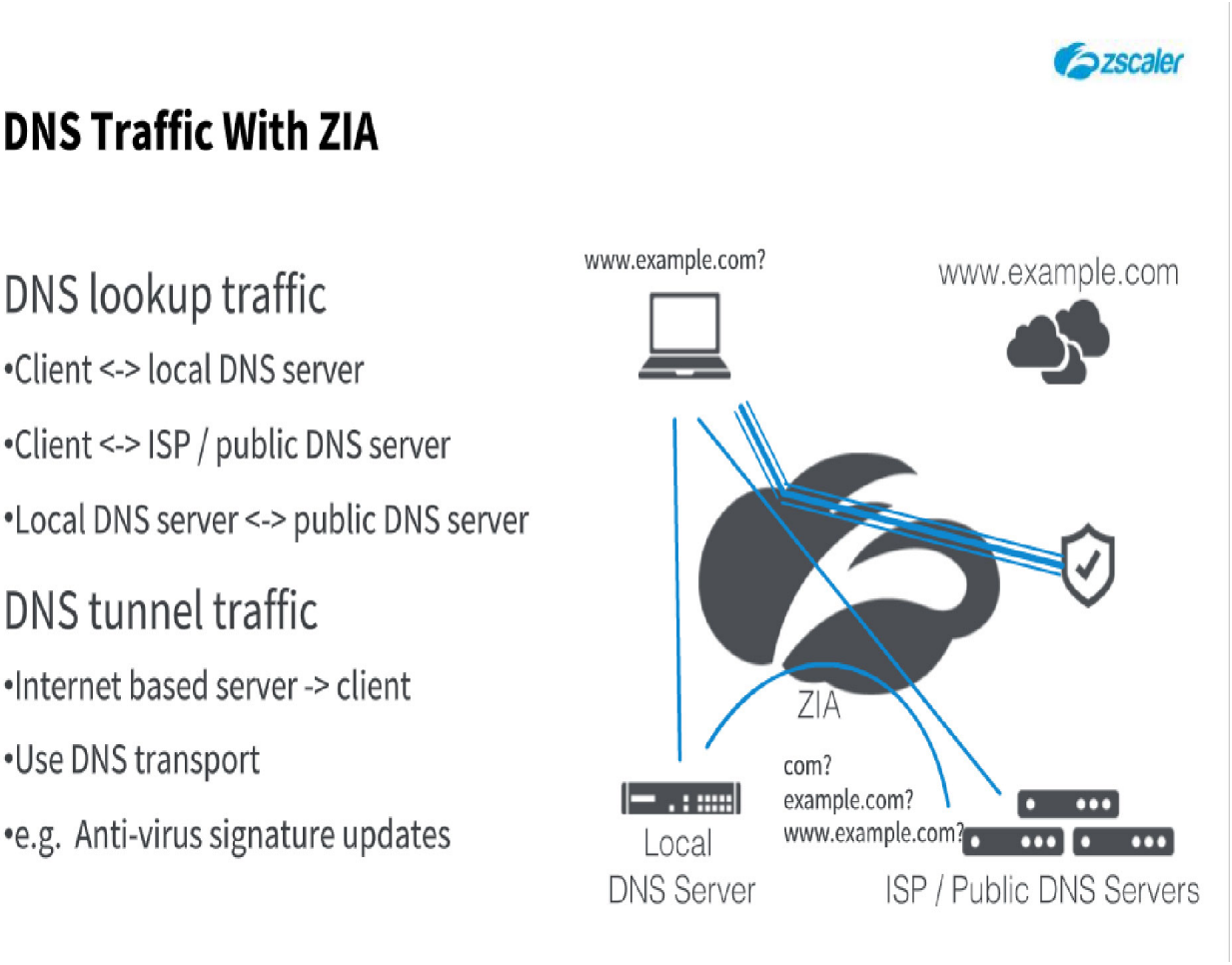
Slide 8 - DNS Traffic With ZIA



Slide notes

Recursive lookups to resolve host addresses through the DNS hierarchy of Root, Top Level Domain, and Authoritative servers on the internet would flow through ZIA. Depending how DNS is configured, this could either be between the local DNS server and external servers or directly from the client to internet DNS servers.

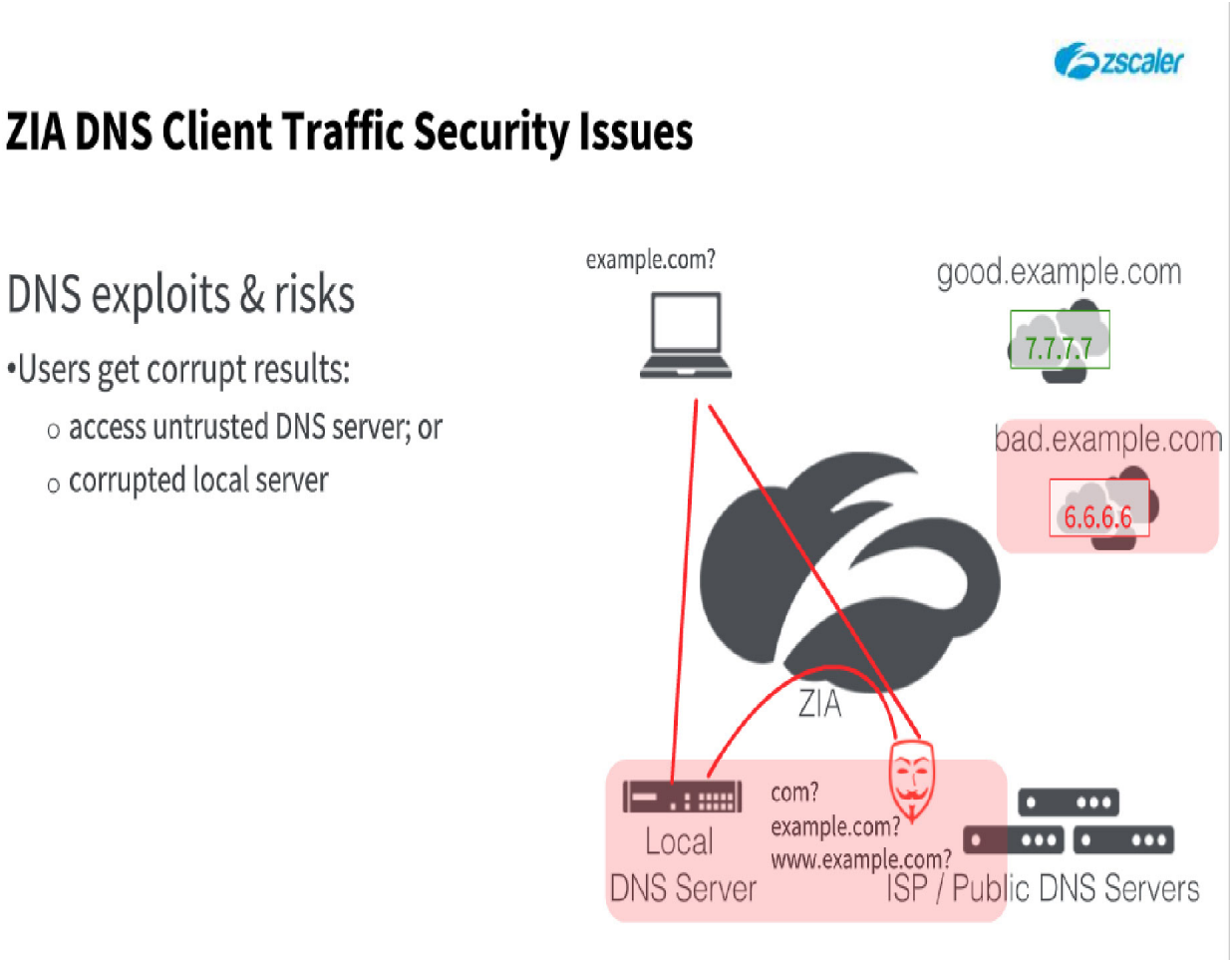
Slide 9 - DNS Traffic With ZIA



Slide notes

Since DNS traffic is critical, security policies are usually configured to allow DNS traffic to flow to the client and local DNS servers. This provides an opening for other applications to be able to tunnel through, encapsulated in packets that pass the security checks that allow incoming DNS. Tunneling might be done for productive reasons such as to carry updates for an anti-virus or similar security application.

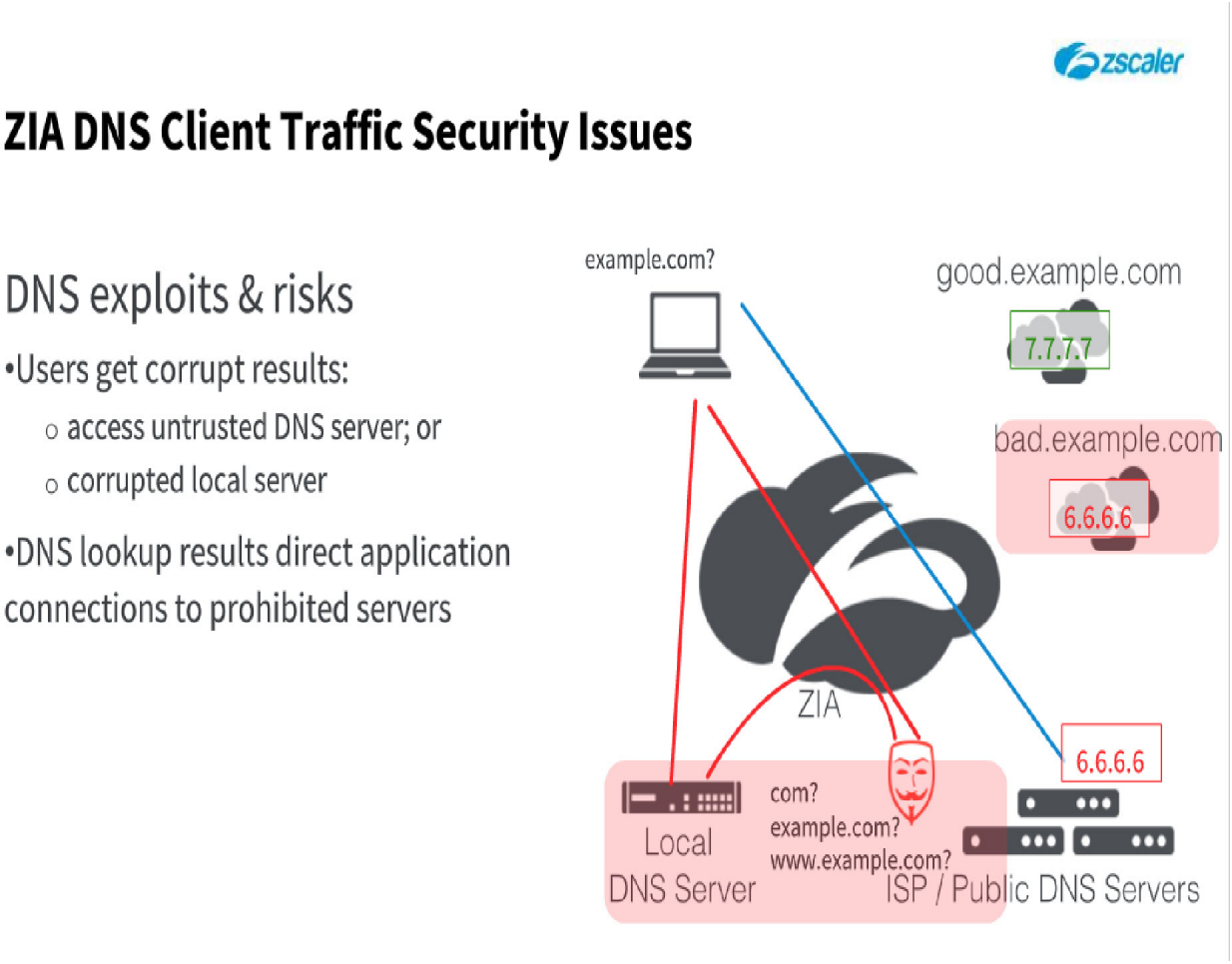
Slide 10 - ZIA DNS Client Traffic Security Issues



Slide notes

DNS security threats aim to corrupt DNS data that a client receives in response to lookups. This could be DNS queries made directly from clients to untrusted public DNS servers, or from the client to a local server that has been corrupted through its transactions with corrupted servers on the internet.
ZIA is in the path of both of these types of traffic, so malicious traffic can be detected and controlled.

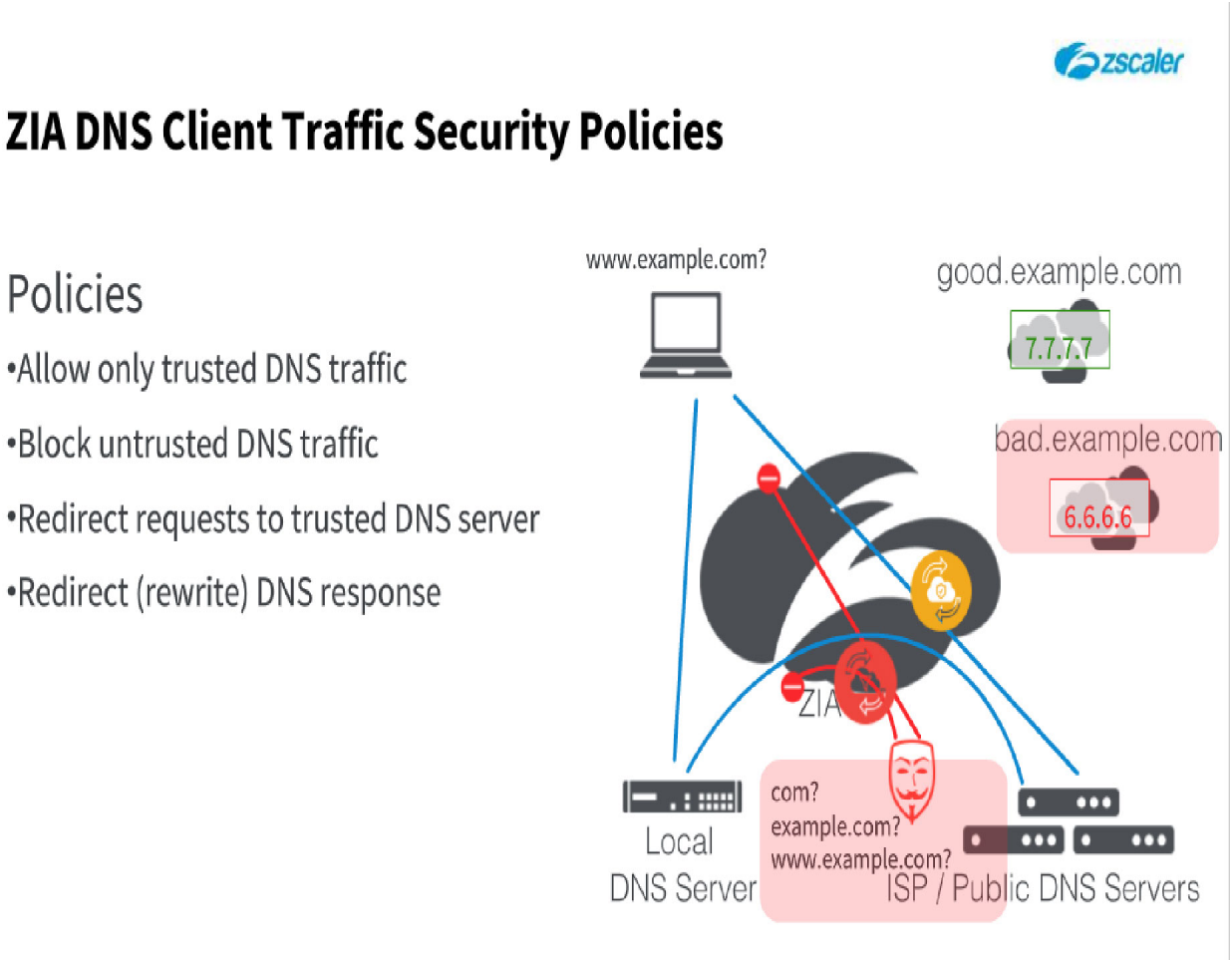
Slide 11 - ZIA DNS Client Traffic Security Issues



Slide notes

Another possible risk is that DNS lookup data, even from trusted sources, may be directing users to connect to services that are prohibited or unsanctioned. Prohibitions may be for security or organizational policy compliance based on factors such as location, ownership, or control of the servers.

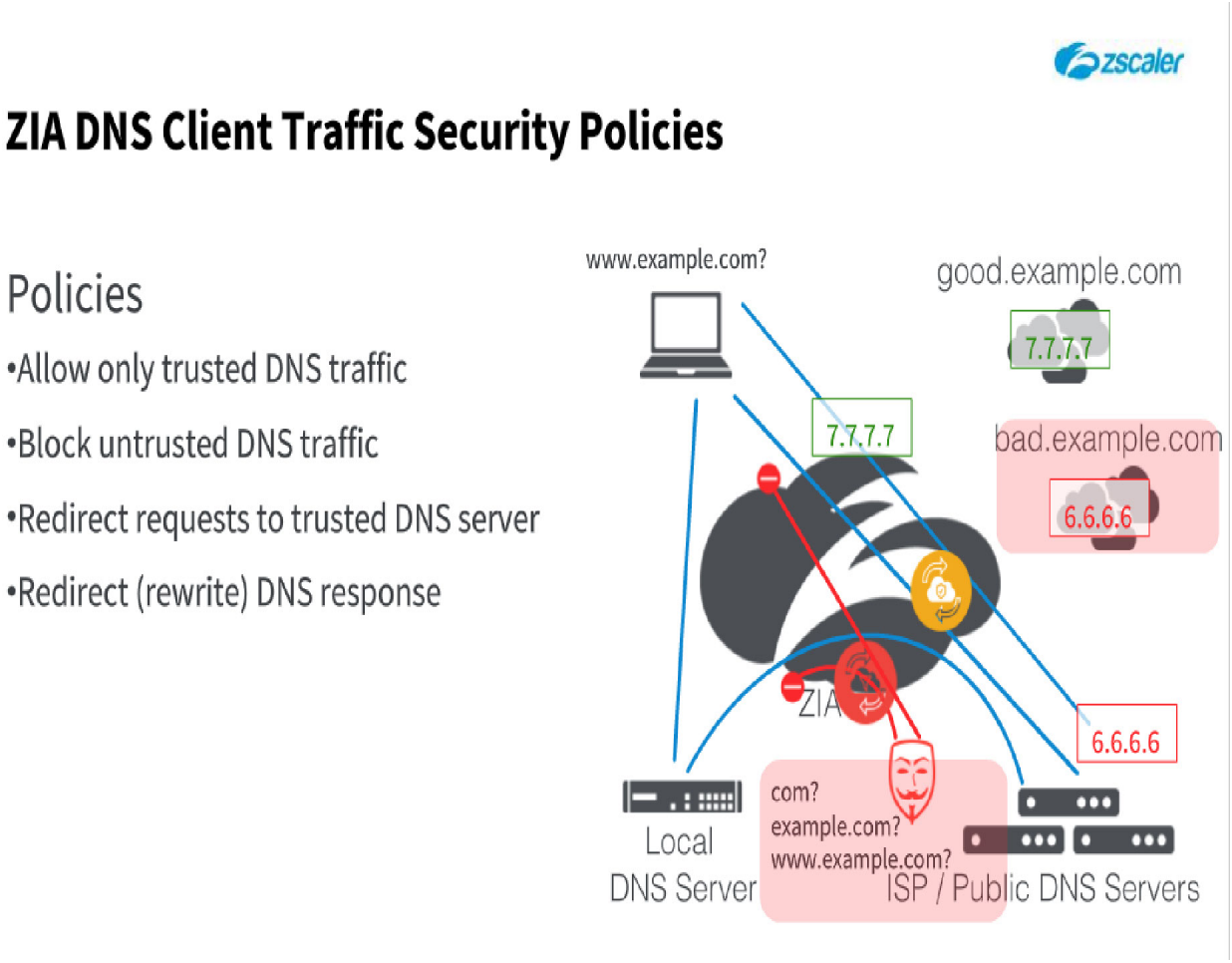
Slide 12 - ZIA DNS Client Traffic Security Policies



Slide notes

Policies may be configured to allow access to trusted DNS sources and to block untrusted traffic. Rules may also be configured to transparently redirect DNS requests to a trusted DNS server. This may be useful to help control users who ignore or are unaware of the risks of accessing data from untrusted sources, while ensuring that safe internet access is provided without any interruption.

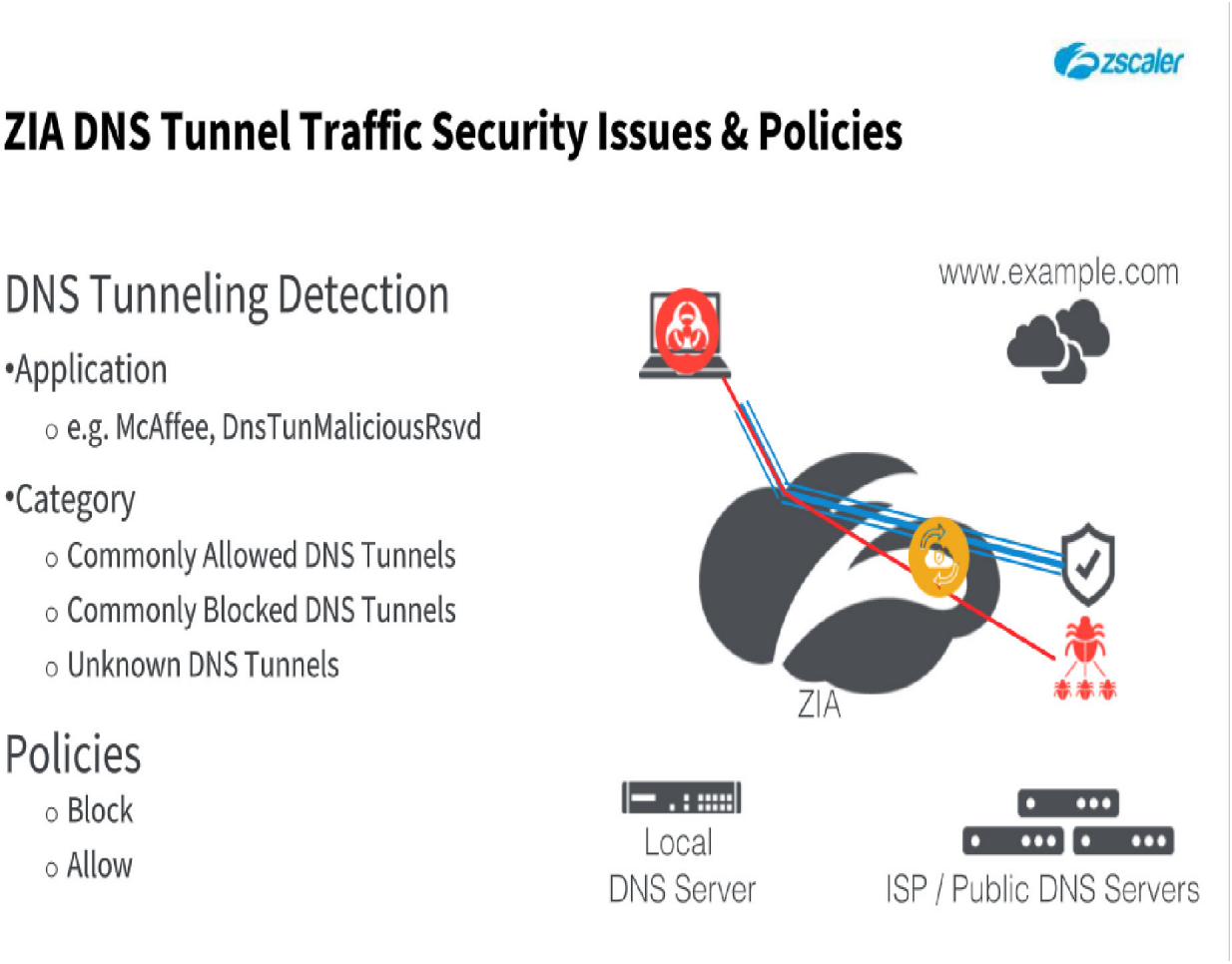
Slide 13 - ZIA DNS Client Traffic Security Policies



Slide notes

Results of a DNS response may also be rewritten by ZIA to change the IP that the client will be directed to connect to. This may be done by configuring a rule with an action to intercept the response and rewrite the destination IP address with a different value configured in ZIA.

Slide 14 - ZIA DNS Tunnel Traffic Security Issues & Policies



Slide notes

Where DNS tunnel traffic may need to be permitted to flow for legitimate productivity reasons, it may also be a target used to circumvent security. Exploits to control infected machines as part of an attacker's botnet are an example of the potential hazard that may be carried within DNS tunnels. ZIA DNS tunnel detection inspects DNS traffic to determine if traffic is being tunneled, and to classify that traffic by application.

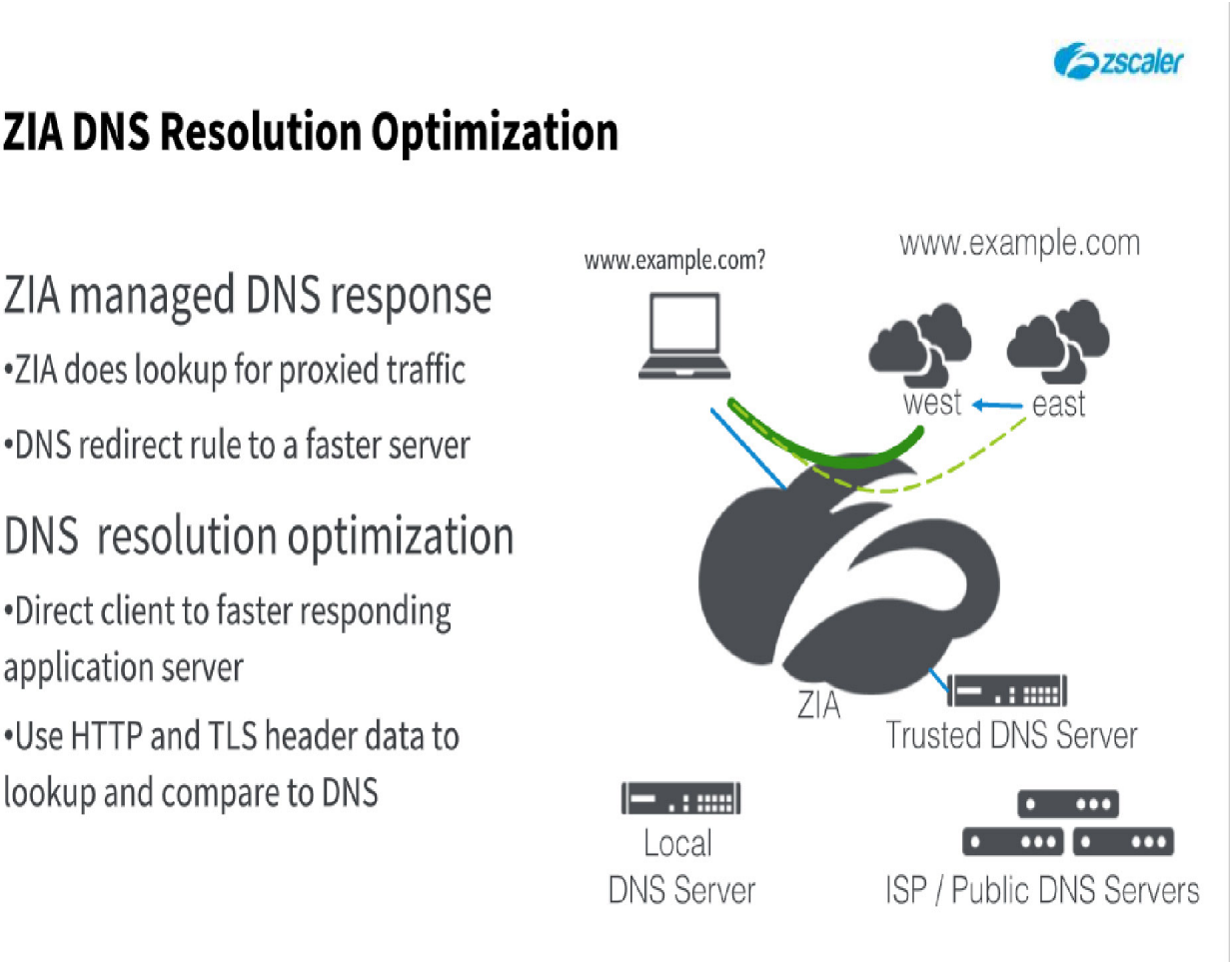
This classification may be used within DNS filtering rules to build policies that allow permitted DNS tunnels and block malicious DNS tunnels. To simplicy the configuration, traffic is classified in one of three categories:
Commonly allowed DNS tunnels; Comonly blocked DNS tunnels; and Unknown DNS tunnels.

Commonly Allowed DNS Tunnels include tunnels that are using DNS tunneling for productive reasons. It is mostly composed of traffic from security services. Policies may be configured to selectively allow some or all of these tunnels.

Commonly Blocked DNS Tunnels includes tunnels that Zscaler has detected as malicious or that can cause a loss of productivity or data. Policies may be configured to block these tunnels.

Unknown DNS Tunnels includes all other tunnels that are not yet classified as commonly allowed or commonly blocked. The recommended best practice is to also block the Unknown DNS Tunnels category.

Slide 15 - ZIA DNS Resolution Optimization



Slide notes

DNS also plays a critical part in application performance and the user's experience. ZIA provides features to manage DNS responses and optimize the results to provide quick and reliable service. Options are available to use ZIA DNS lookup data for proxied traffic such as HTTP and HTTPS. Similarly, the DNS request redirect rules that were previously discussed in the context of DNS client traffic security may also be used to direct clients to reliable DNS servers that respond quickly.

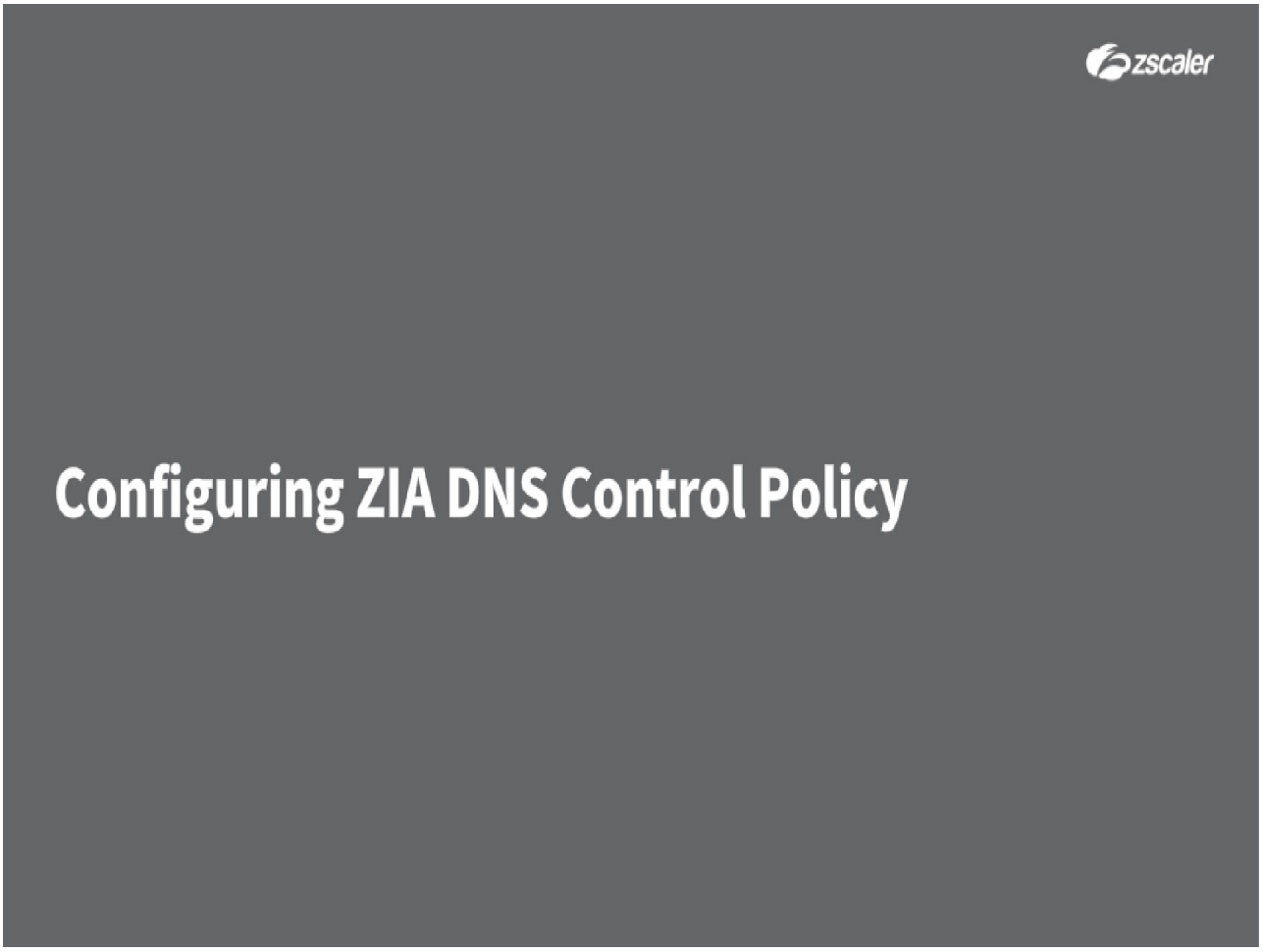
For HTTP and HTTPS proxied through ZIA, there is an additional level of optimization that may be enabled to improve upon the results returned through DNS. Zscaler proxy examines the HTTP header and TLS requests for information about the server hosts being connected to. ZIA will then separately lookup the hosts involved and direct the client to the IP based on a view that is optimized for the client's connections in terms of how and where they are connected. For example if DNS directs a client in the west to connect to a server in a data center in the east, ZIA can move the connection to a server in the west closer to the client.

Slide 16 - Exercises

Slide notes

Following is a series of short exercises to learn and practice the skills needed for configuring ZIA DNS Control and Tunneling Policies as well as DNS Resolution Optimization.
This section has been created as an interactive demo. You will be guided step by step to interact with the ZIA user interface by clicking and typing to navigate and configure ZIA. You may also use the Play button in the playback controls to advance to the next step.

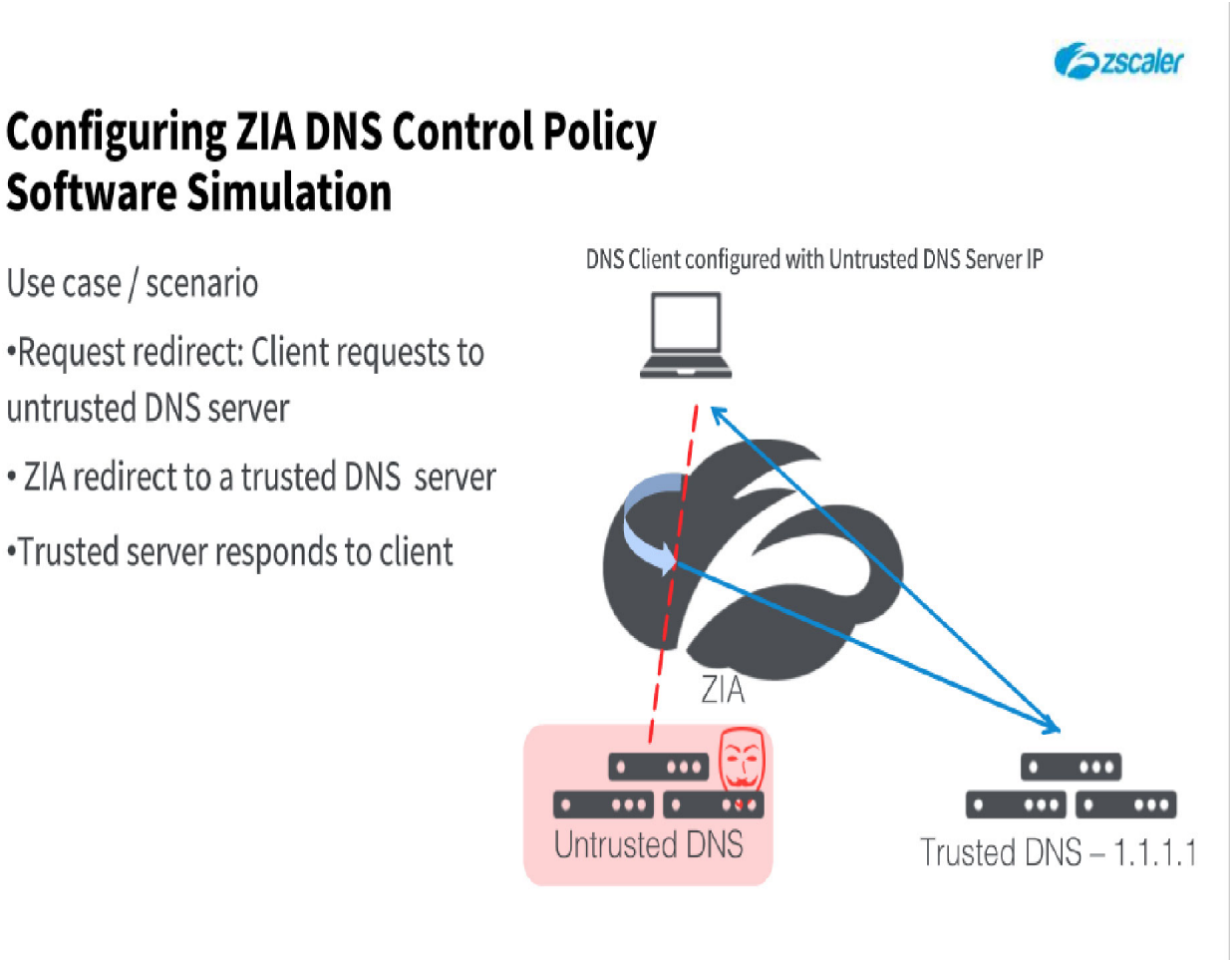
Slide 17 - Configuring ZIA DNS Control Policy



Slide notes

In this task you will configure a ZIA DNS Control Policy.

Slide 18 - Configuring ZIA DNS Control Policy Software Simulation

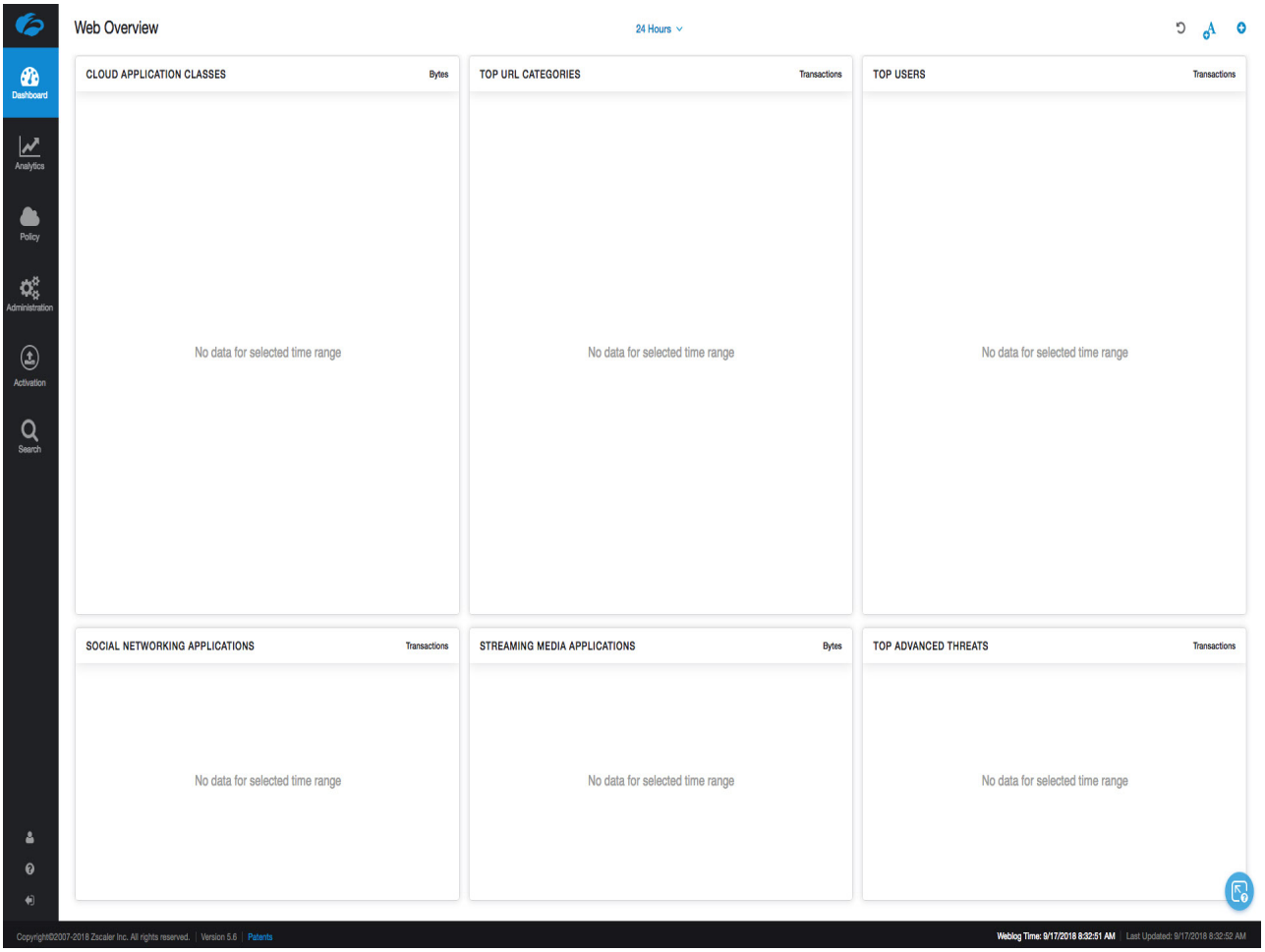


Slide notes

Consider the scenario where an organization's policy is for DNS traffic at a location to be directed to a trusted server. In this task you will configure a DNS filtering rule to redirect all DNS requests to the trusted DNS server. In this example 1.1.1.1 will be used as the trusted DNS server.

To configure a DNS control policy, follow these steps:

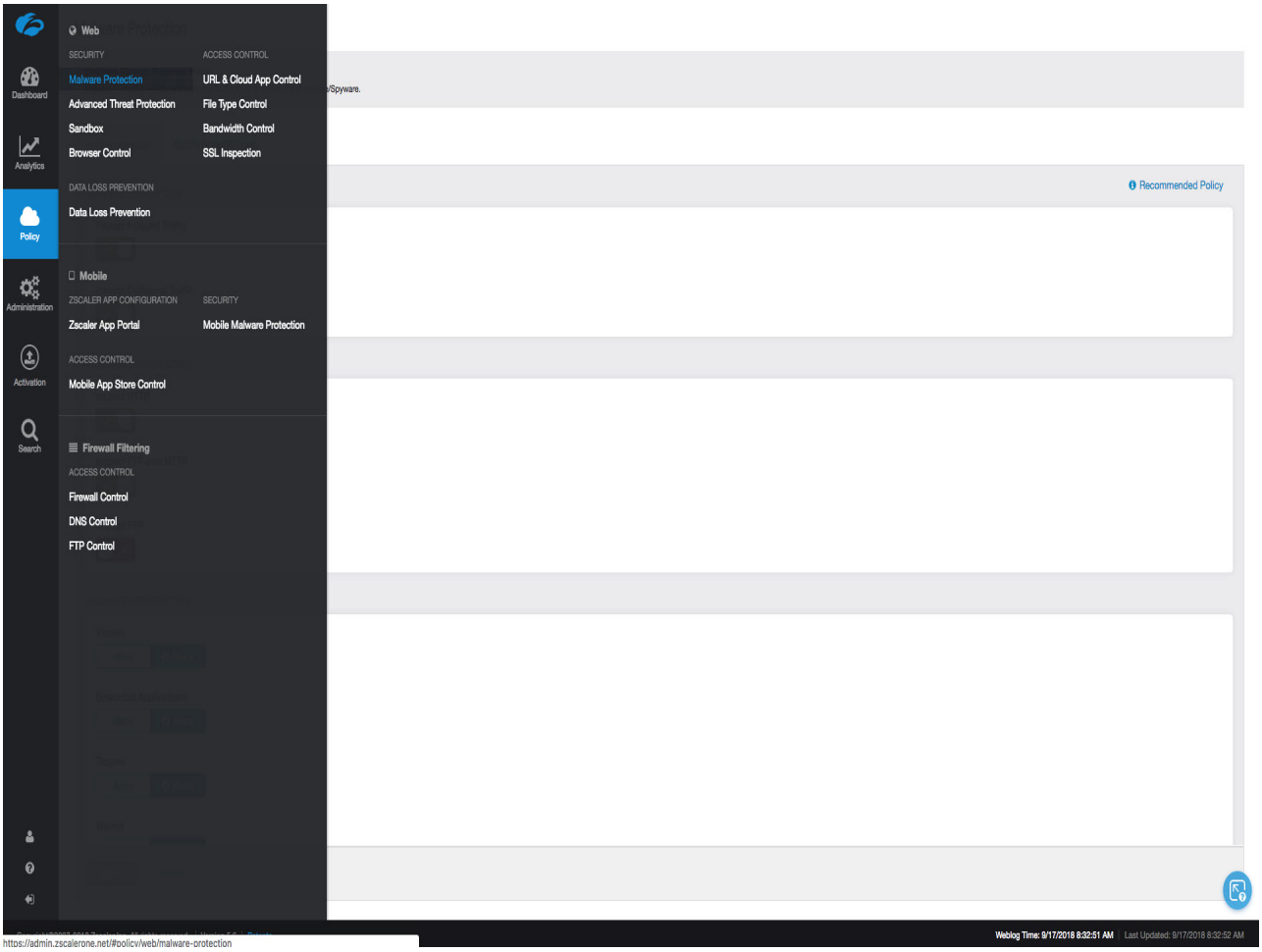
Slide 19 - Slide 19



Slide notes

Click to select from the **Policy** menu.

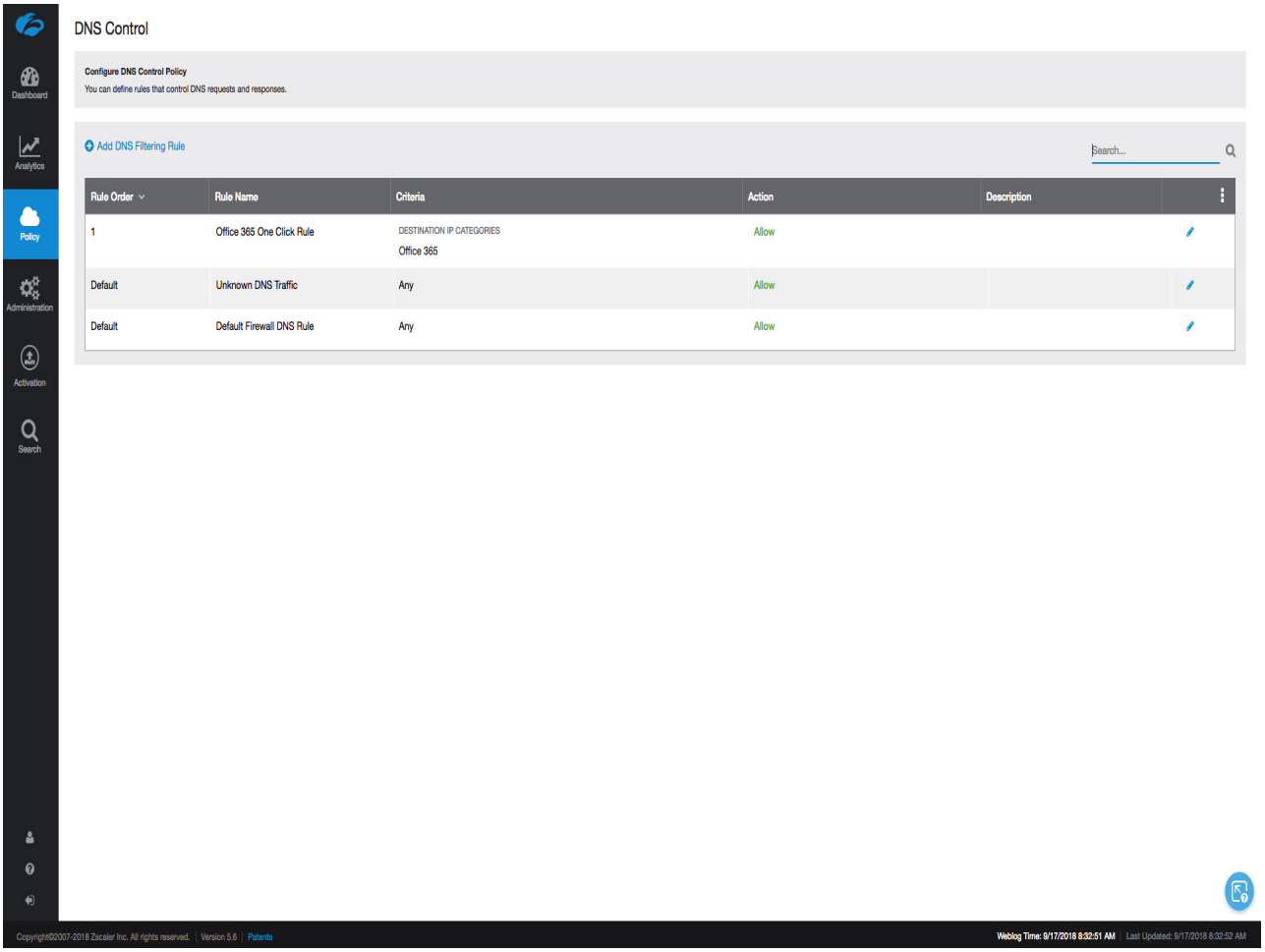
Slide 20 - Slide 20



Slide notes

Select **DNS Control** from the Firewall Filtering Access Controls sub-menu.

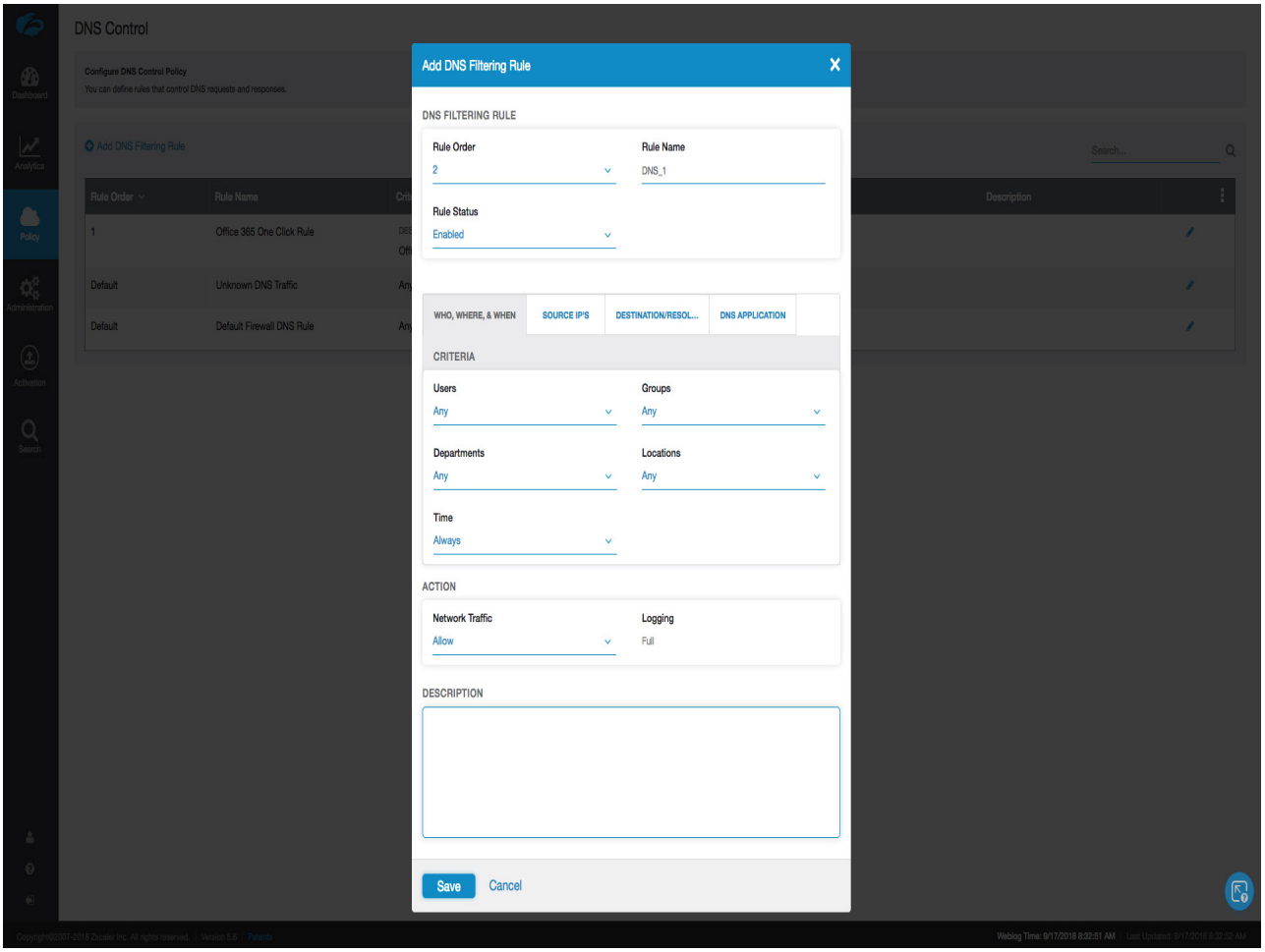
Slide 21 - Slide 21



Slide notes

On the **DNS Control** Page, click **Add DNS Filtering Rule**.

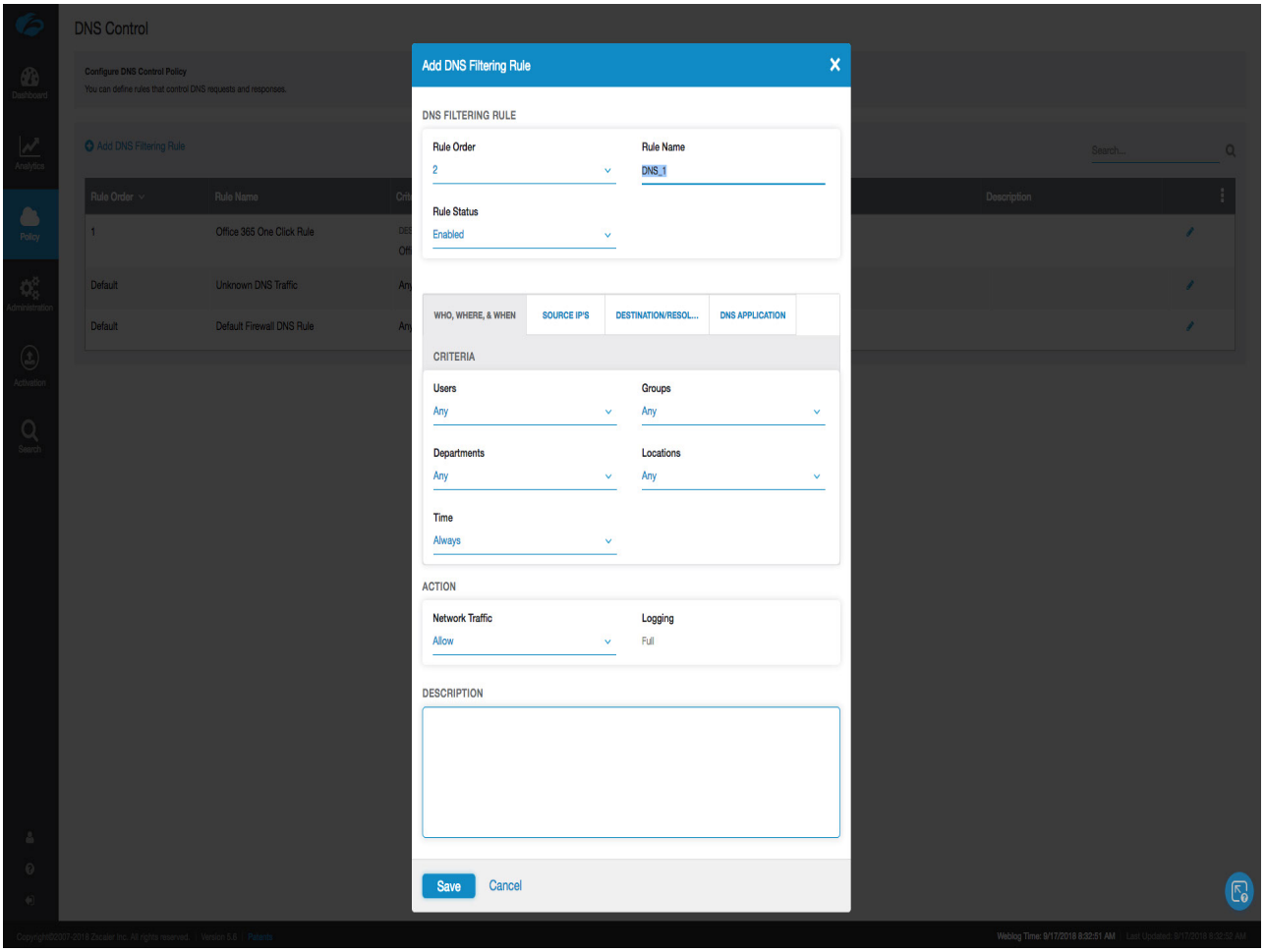
Slide 22 - Slide 22



Slide notes

Note that the rule order is automatically set to the next available number in the list. In this case as rule #2 it will placed below the Office 365 OneClick Rule. **Double-click** in the **Rule Name** field to enter a name.

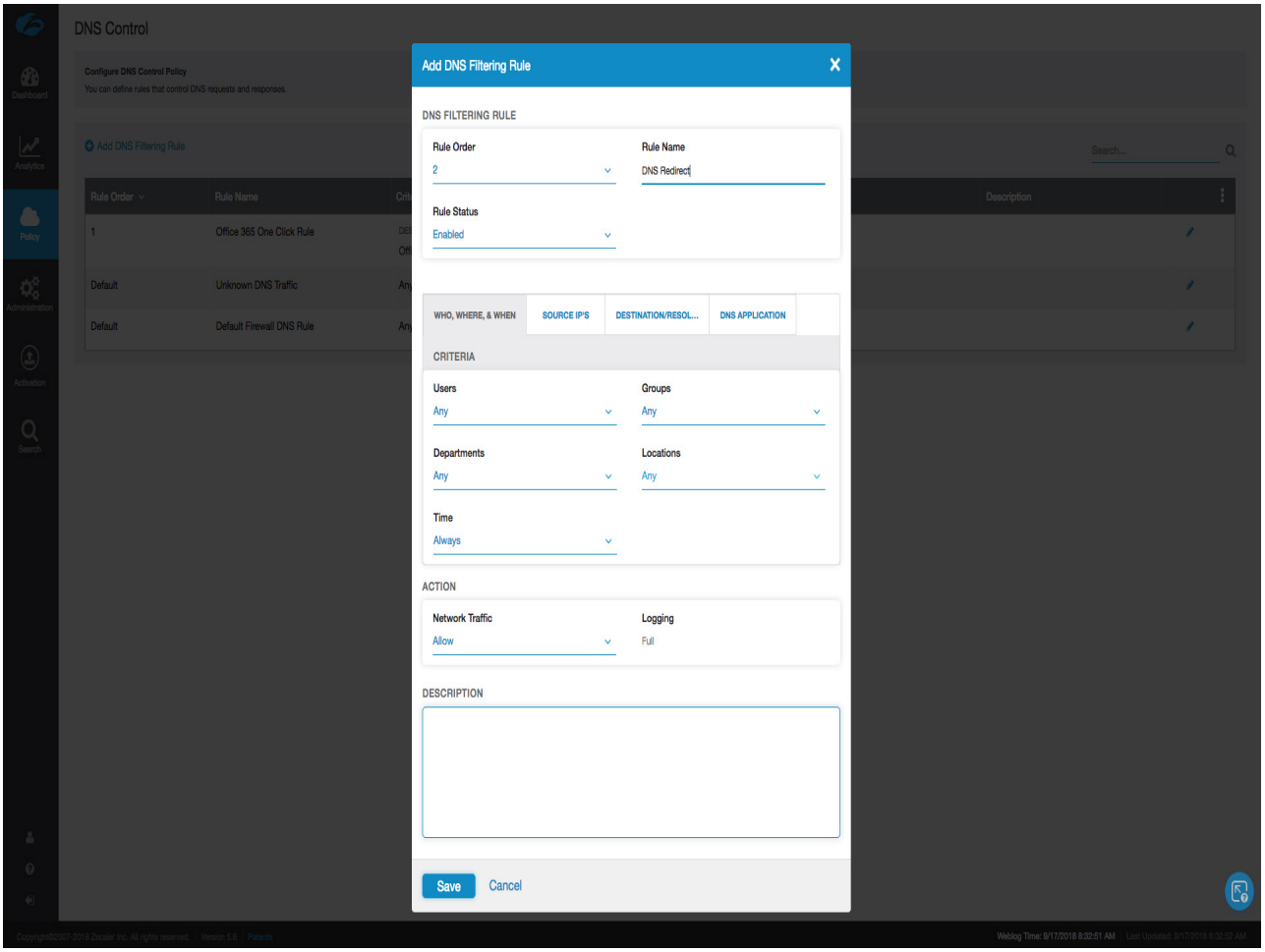
Slide 23 - Slide 23



Slide notes

Type the rule name **DNS Redirect** and hit **Enter**.

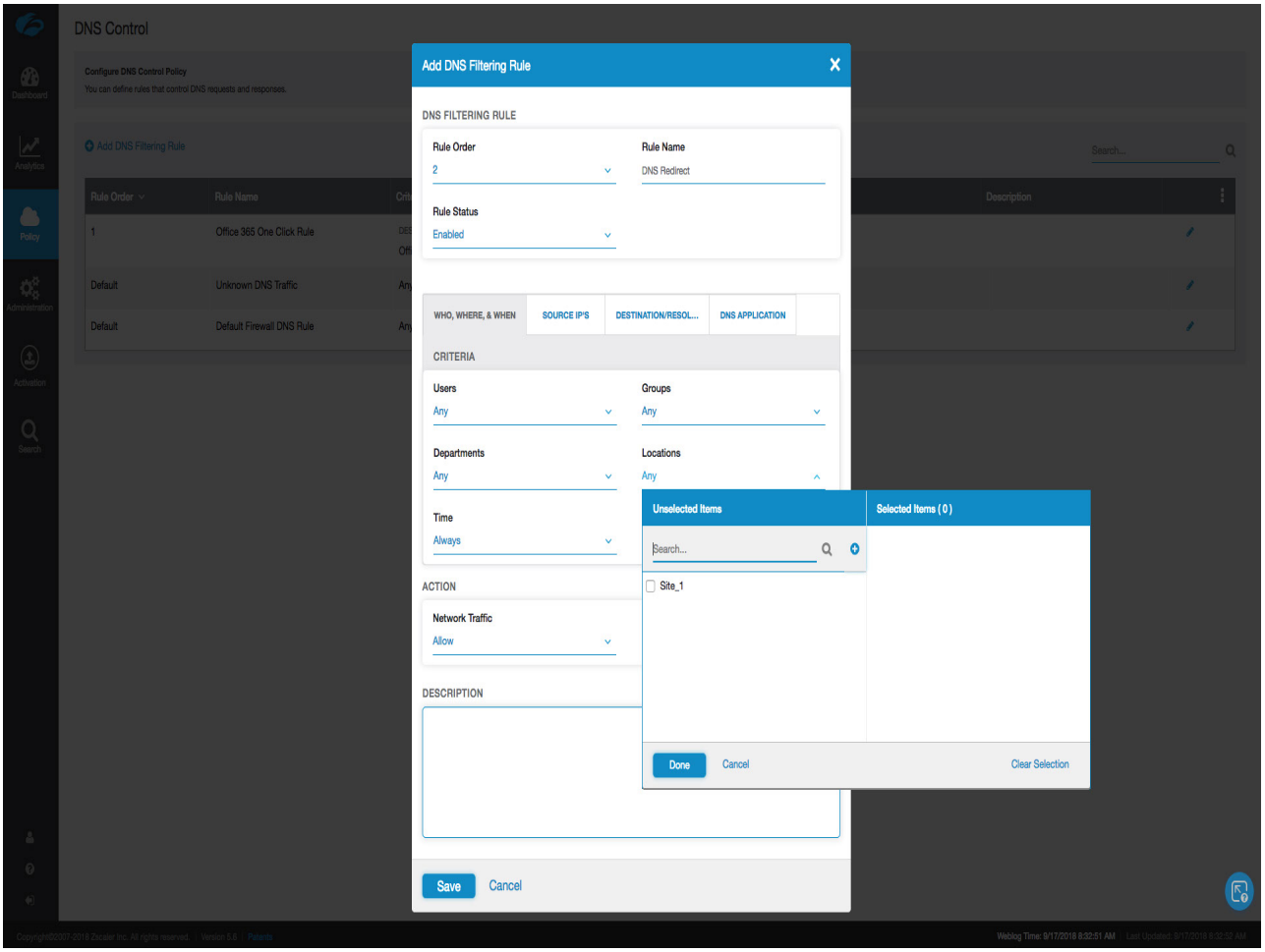
Slide 24 - Slide 24



Slide notes

In the **WHO, WHERE and WHEN** tab set the criteria for the location needing the policy. Click to view the **Locations** list.

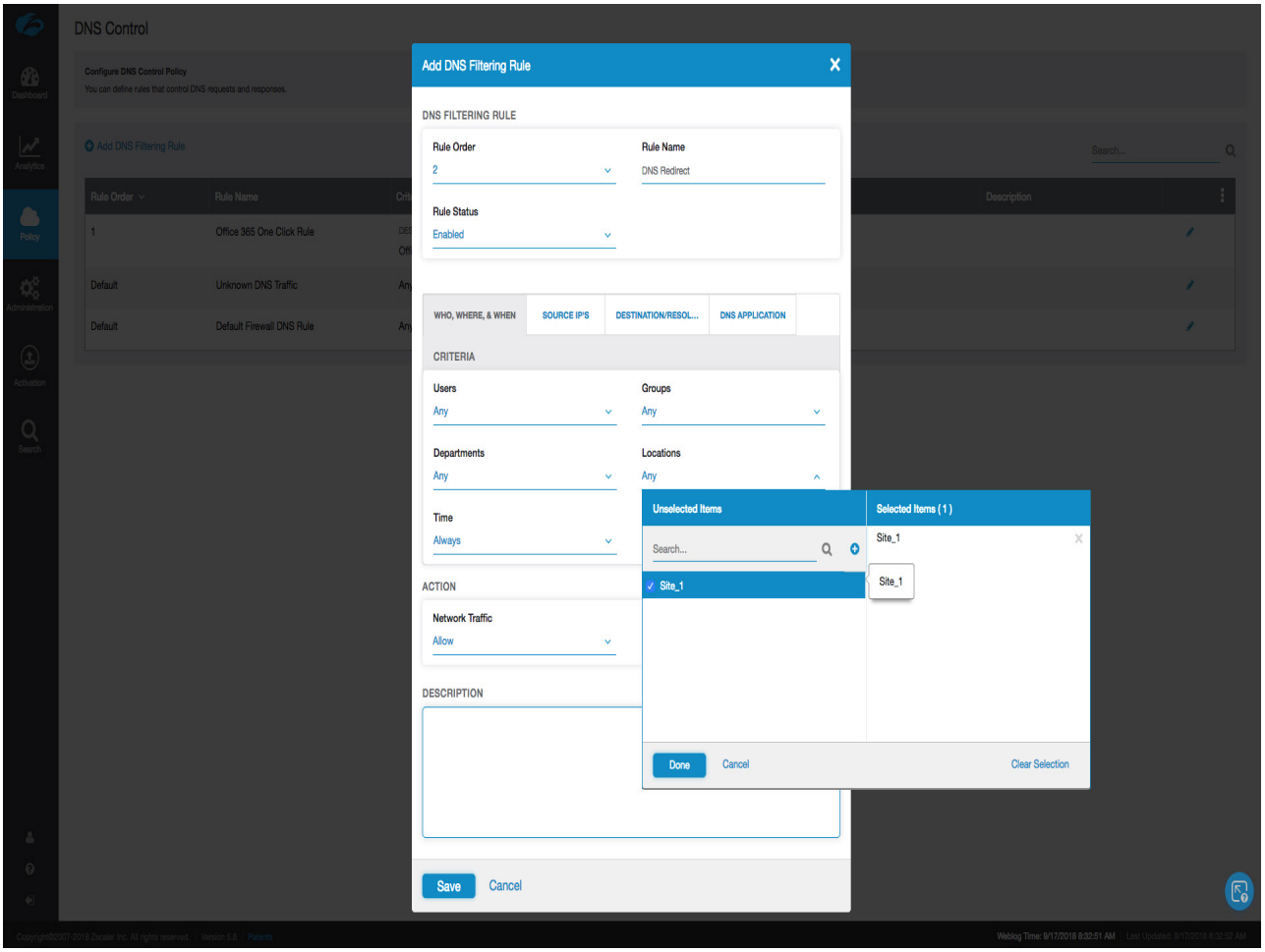
Slide 25 - Slide 25



Slide notes

Click the check box to set the rule to apply to **Site_1**.

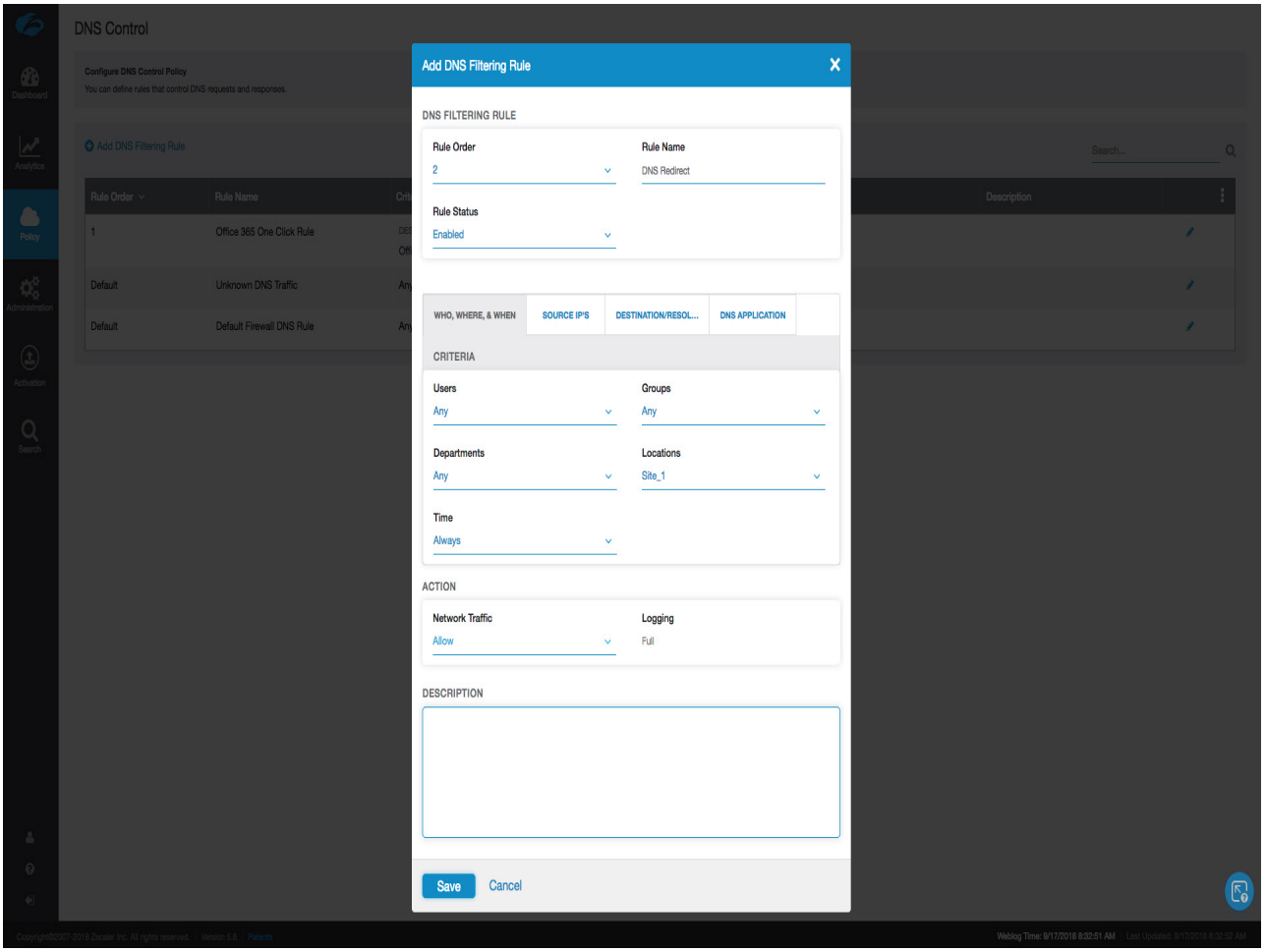
Slide 26 - Slide 26



Slide notes

This rule will be configured to only apply to Site_1, so click **Done**.

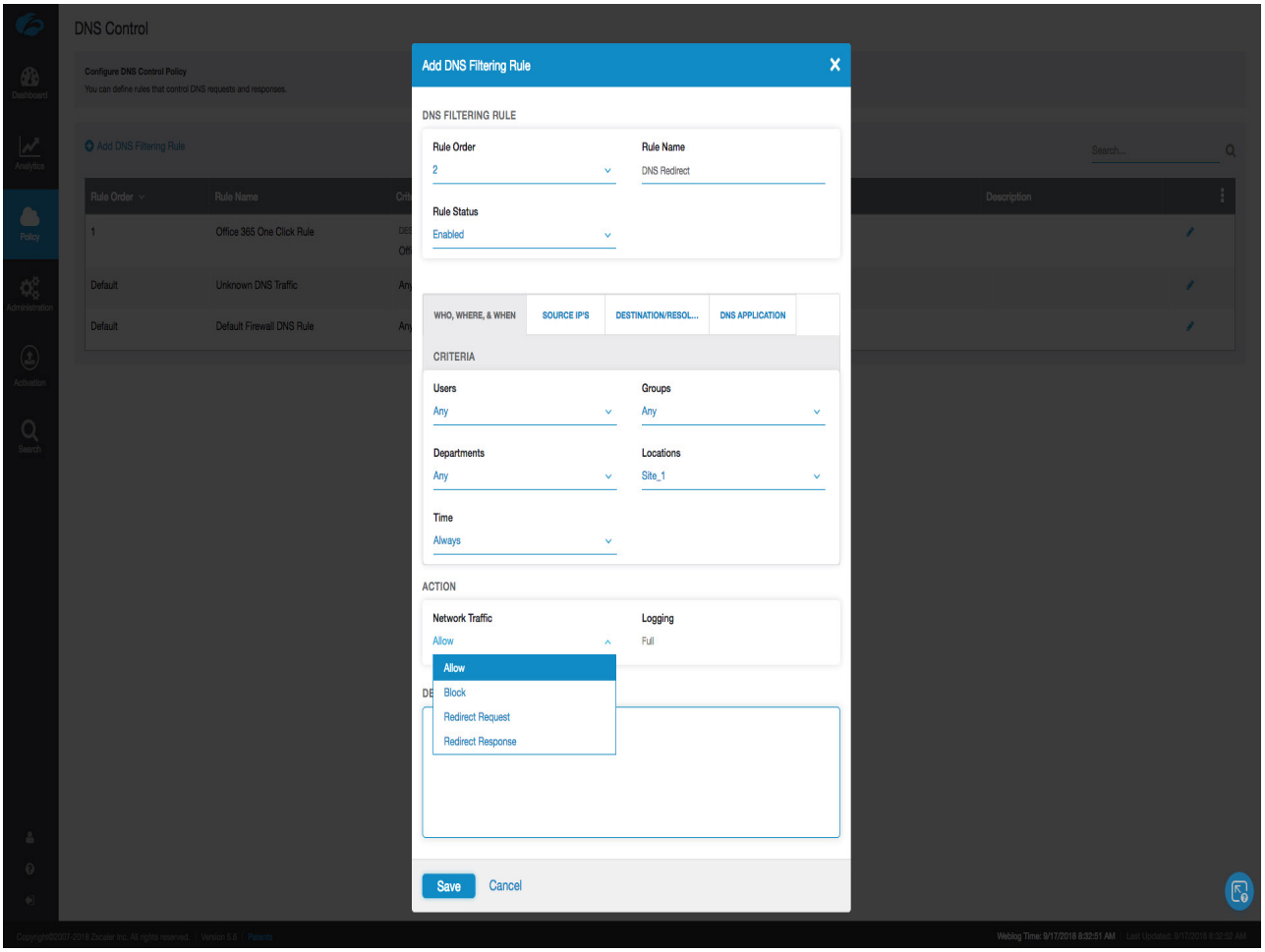
Slide 27 - Slide 27



Slide notes

All other criteria are left to default settings to apply to all DNS traffic at Site_1 with no other conditions. Click to select the **Network Traffic** Action setting.

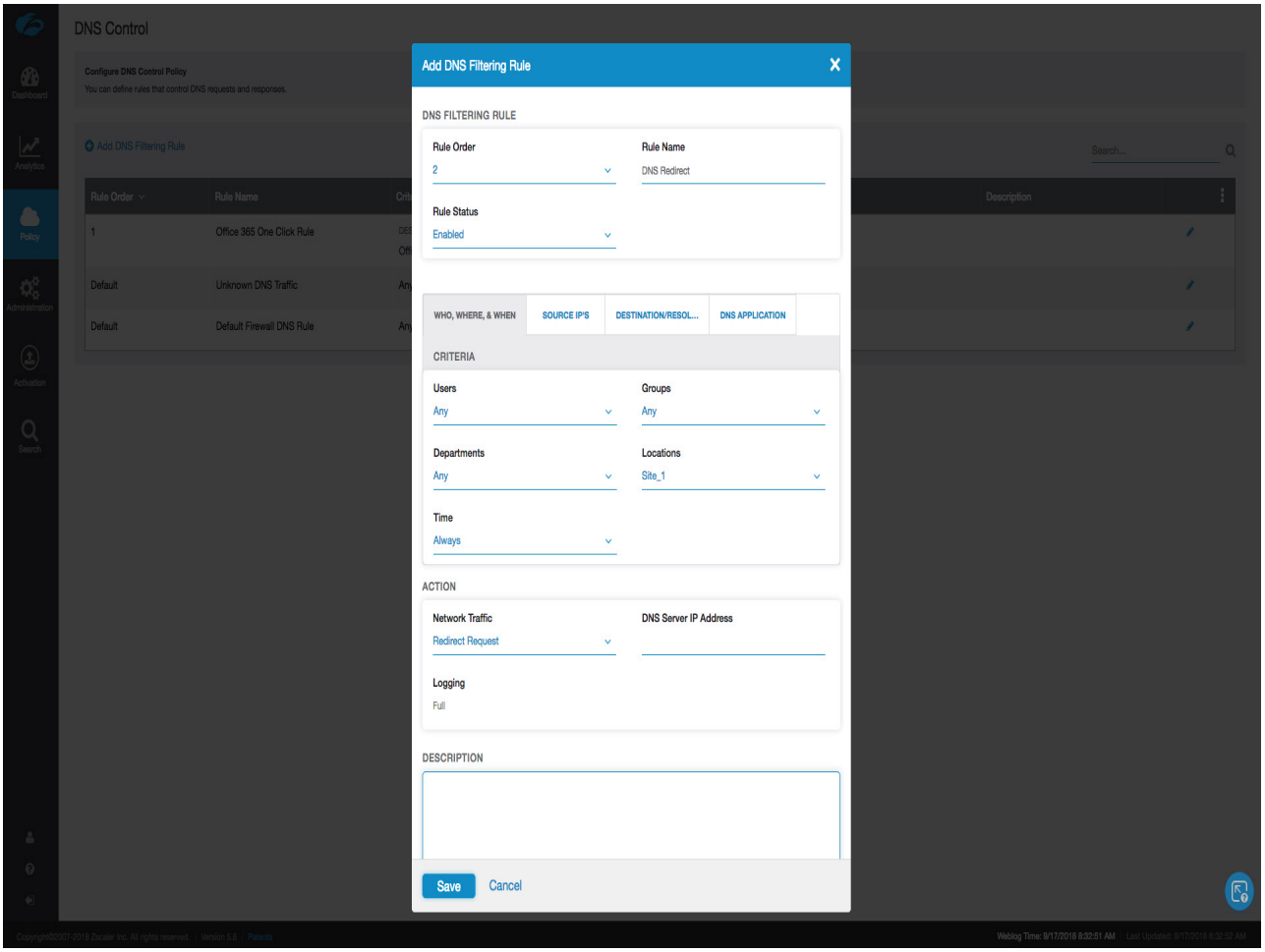
Slide 28 - Slide 28



Slide notes

Select the **Redirect Request** action.

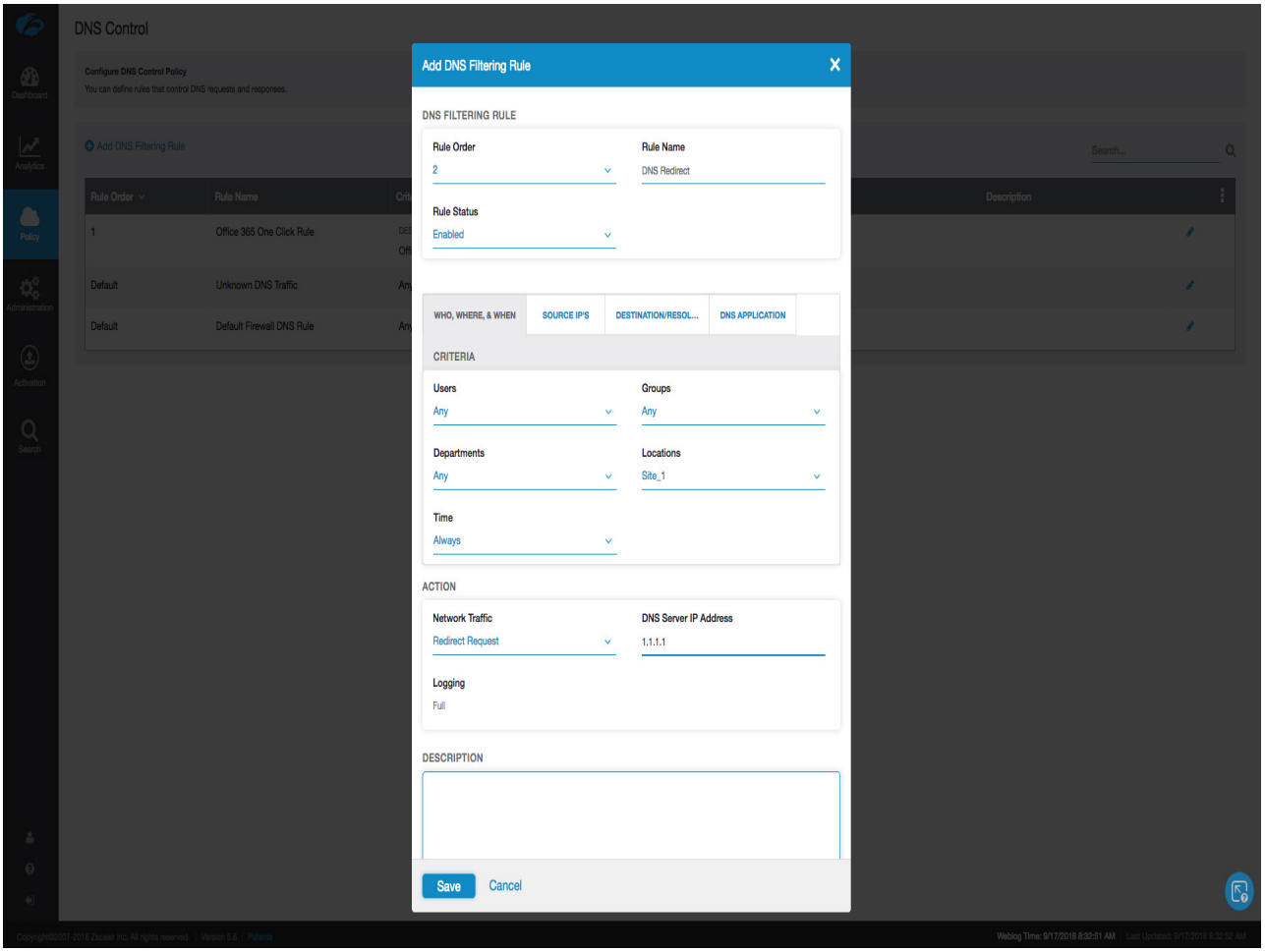
Slide 29 - Slide 29



Slide notes

Type **1.1.1.1** as the **DNS Server IP Address** to redirect requests to.

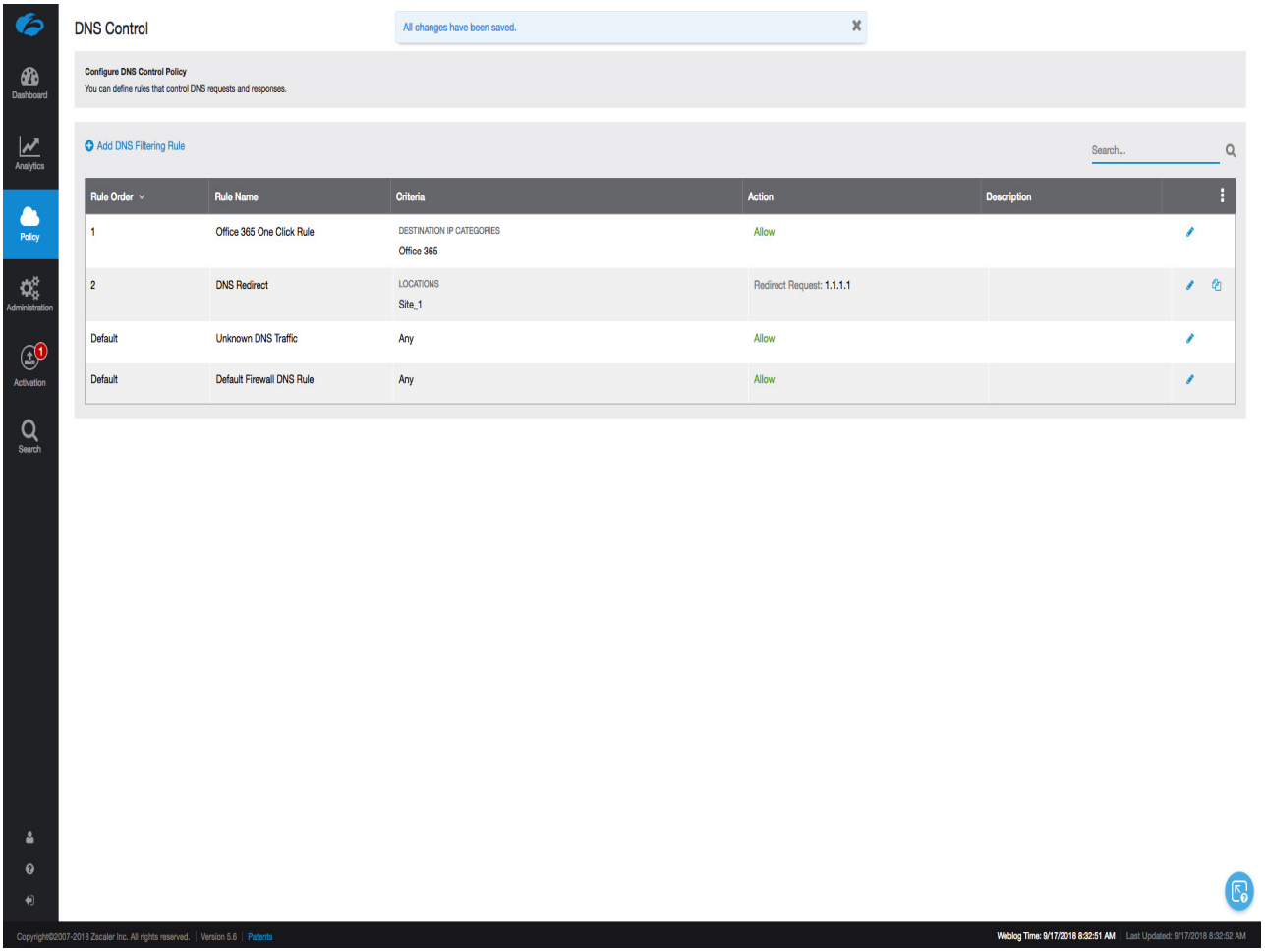
Slide 30 - Slide 30



Slide notes

Save the rule.

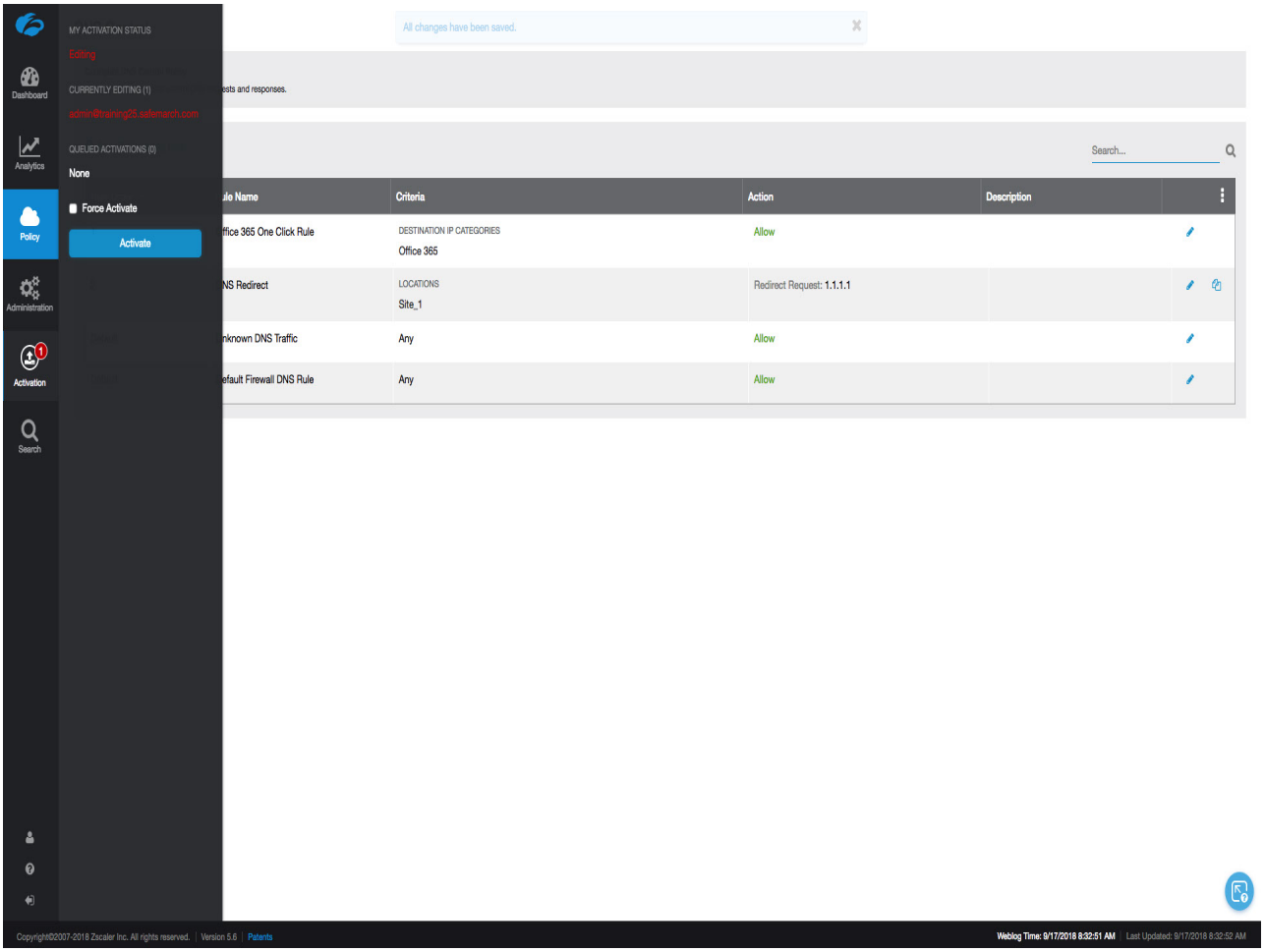
Slide 31 - Slide 31



Slide notes

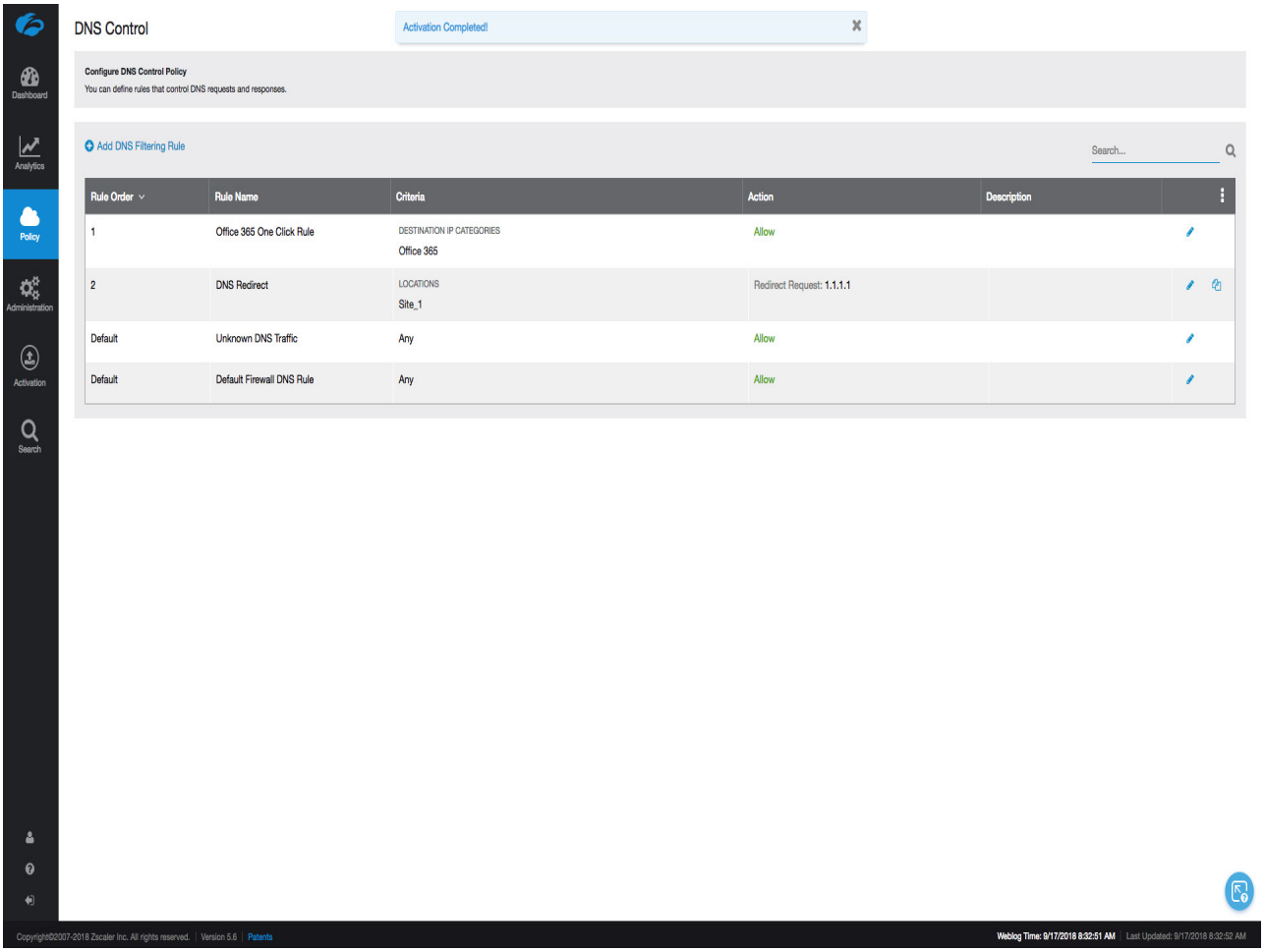
Check that the rule is added to the list and **Activate** the changes.

Slide 32 - Slide 32



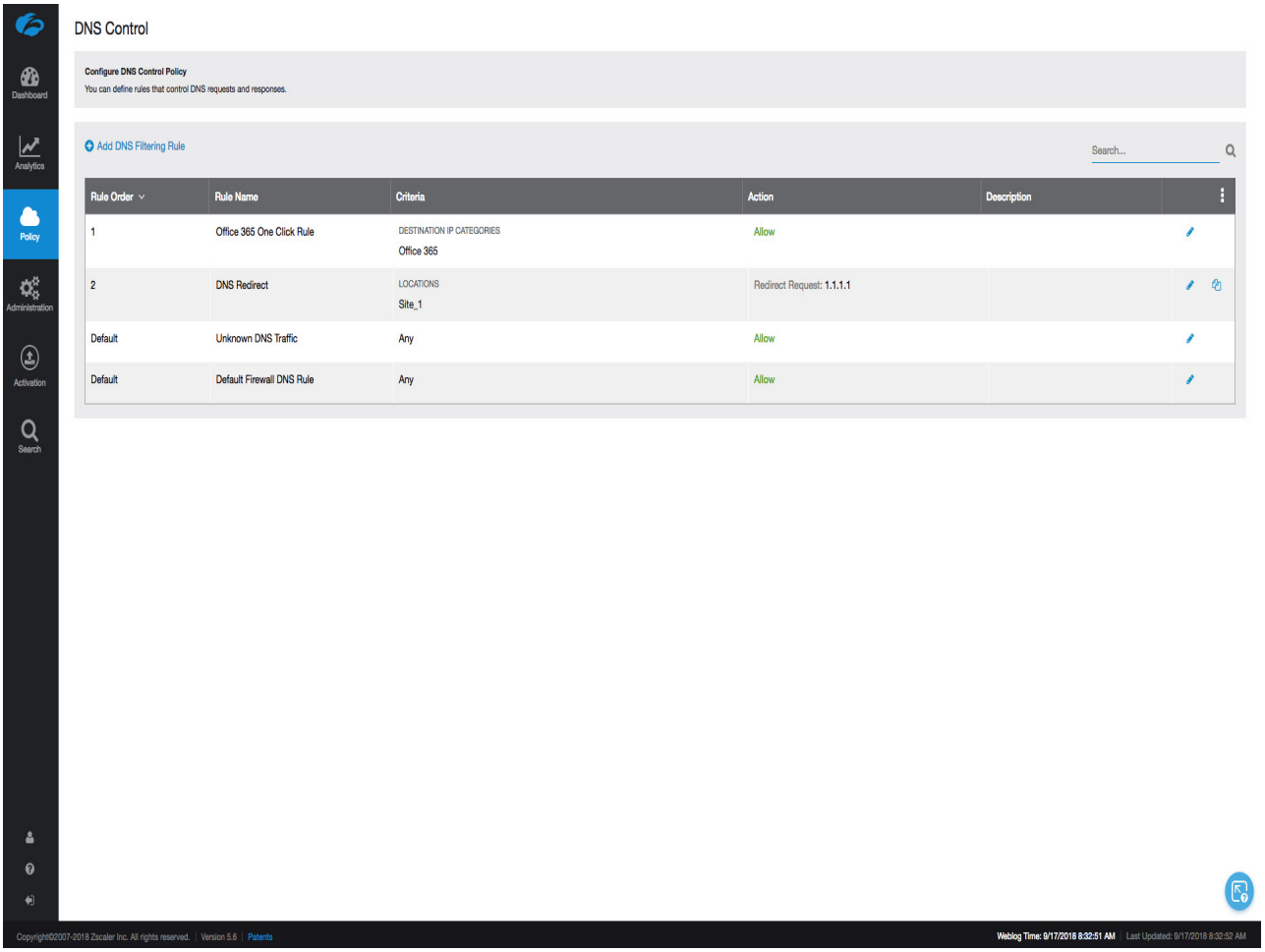
Slide notes

Slide 33 - Slide 33



Slide notes

Slide 34 - Slide 34



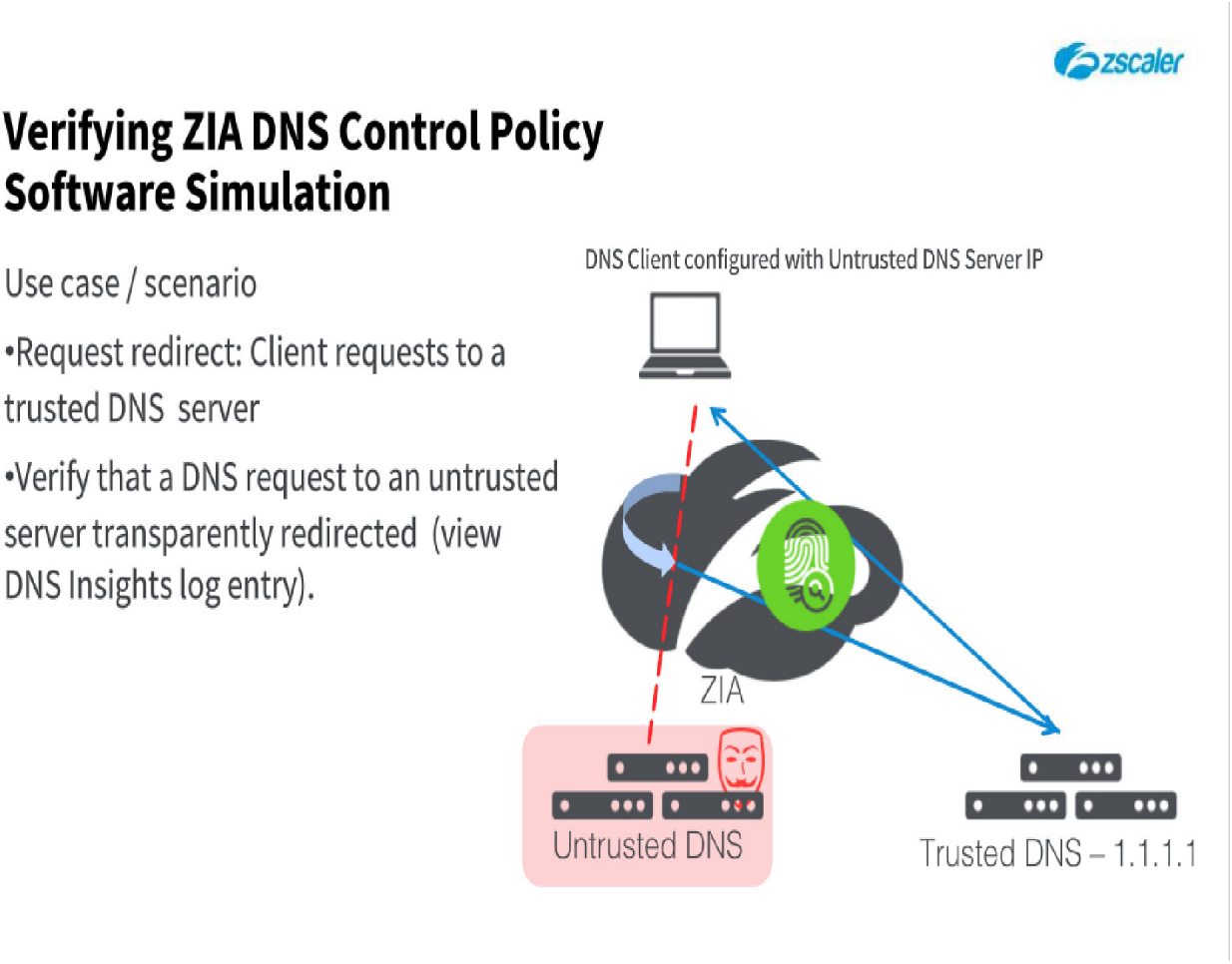
Slide notes

Slide 35 - Verifying DNS Control Policy

Slide notes

In this task you will verify that DNS Control Policy is being enforced.

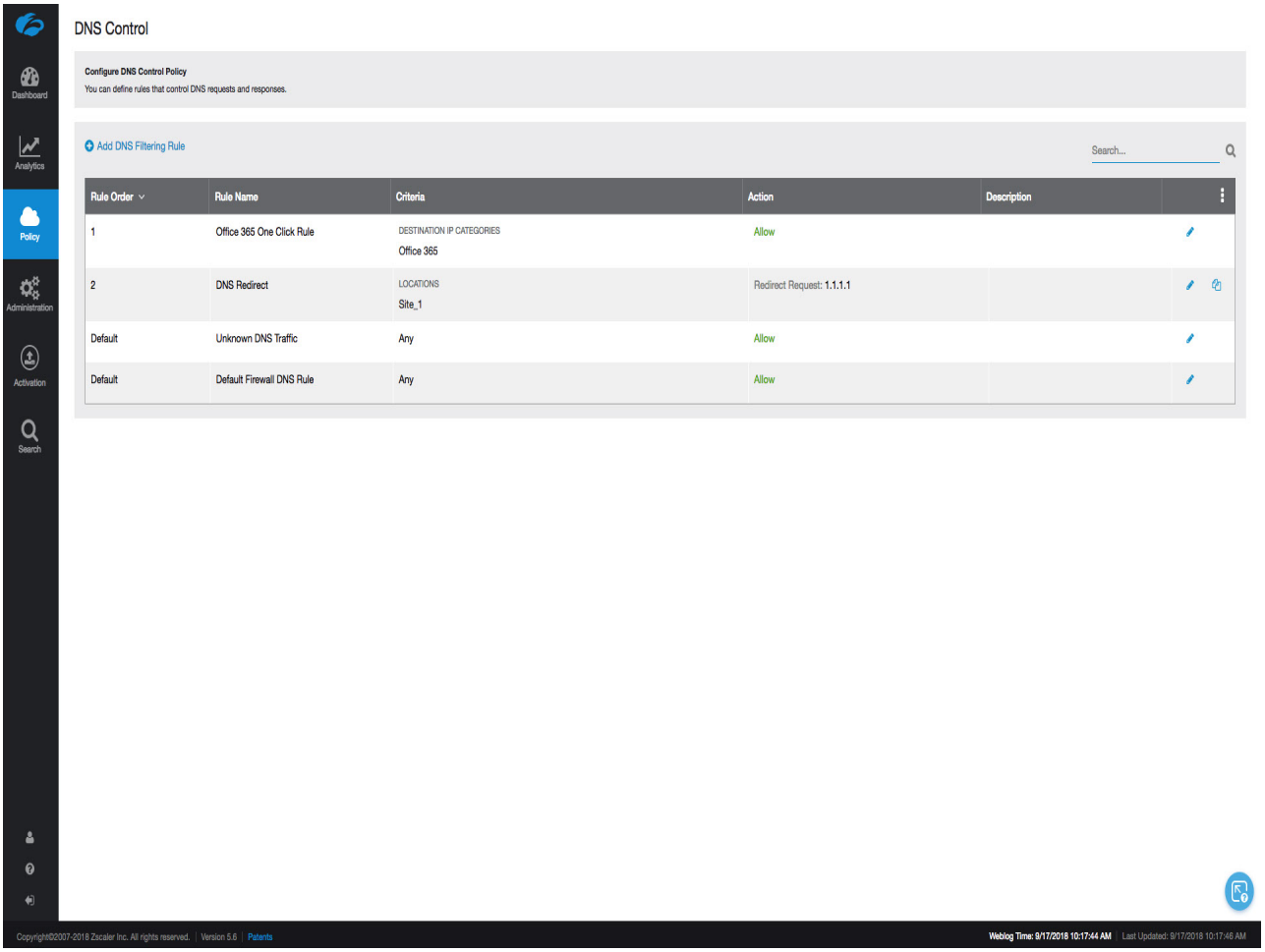
Slide 36 - Verifying ZIA DNS Control Policy Software Simulation



Slide notes

Consider the scenario where ZIA is configured with an active rule to direct DNS requests to a trusted server. In this task you will verify the redirection result by viewing the log entries in the DNS Insights analytics data.

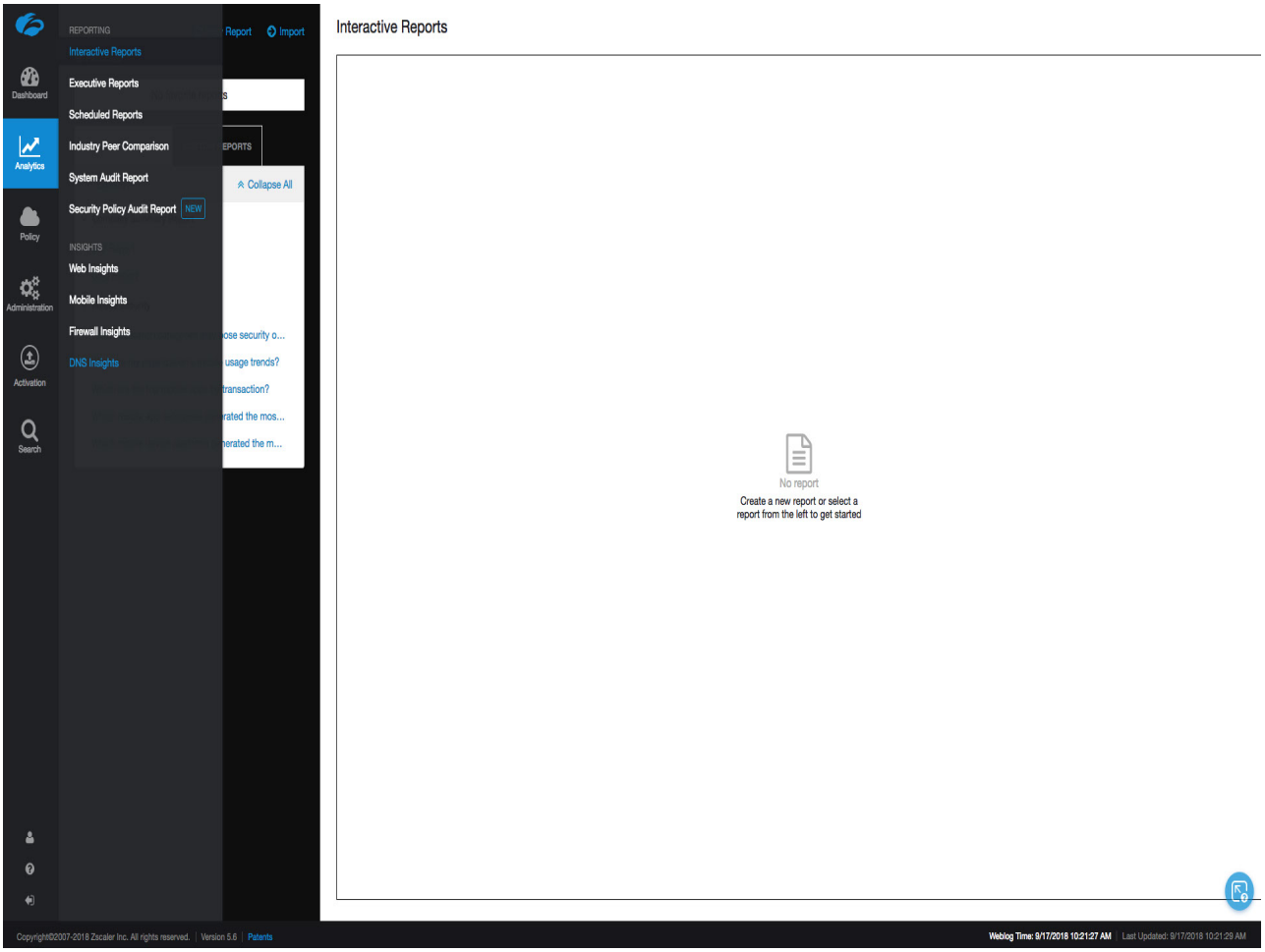
Slide 37 - Slide 37



Slide notes

With the rule now active its activity will be recorded in the logs. To verify that DNS requests are being redirected follow these steps:
Click to select from the **Analytics** menu.

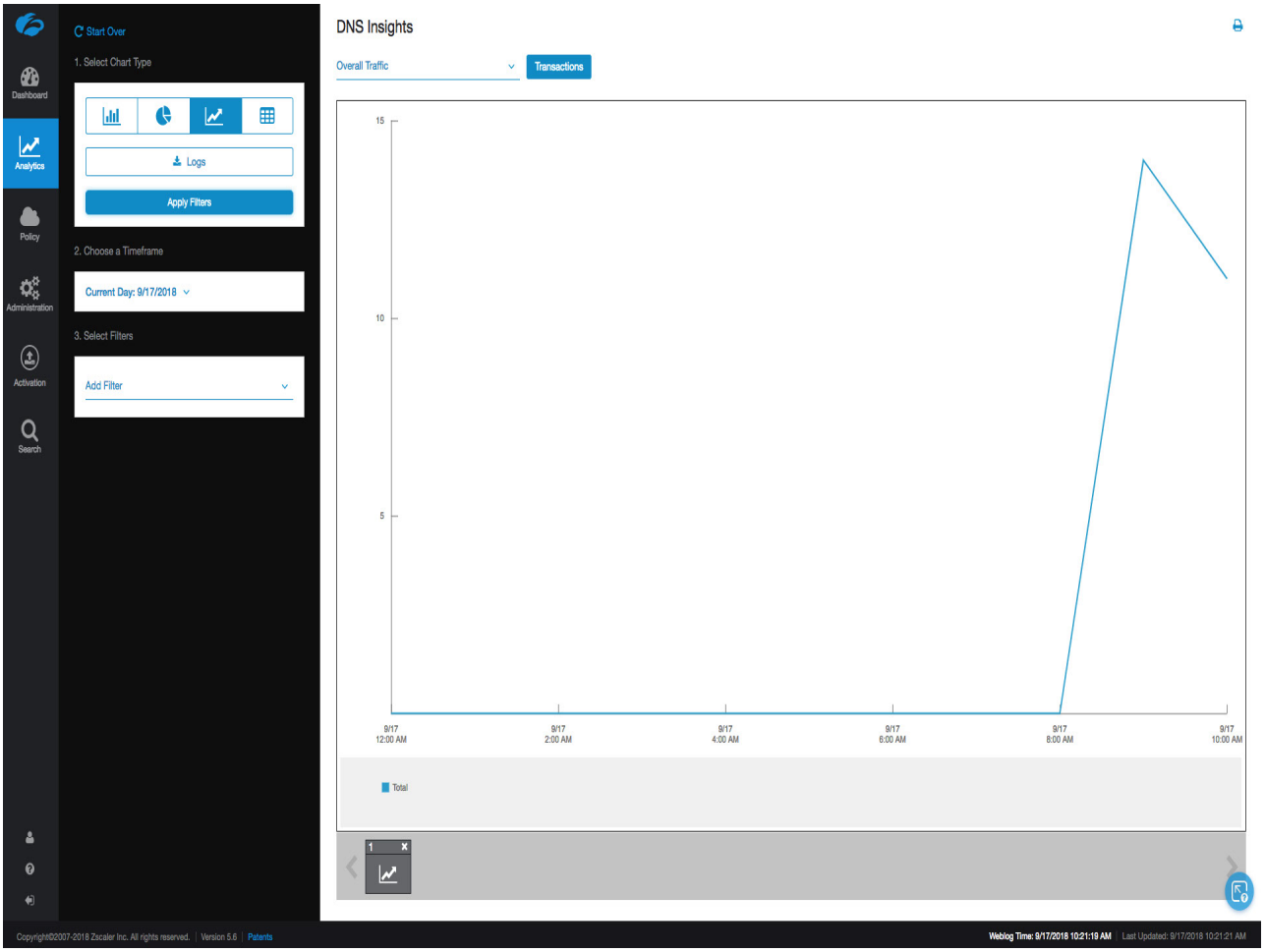
Slide 38 - Slide 38



Slide notes

Select to go to **DNS Insights** under the **INSIGHTS** group.

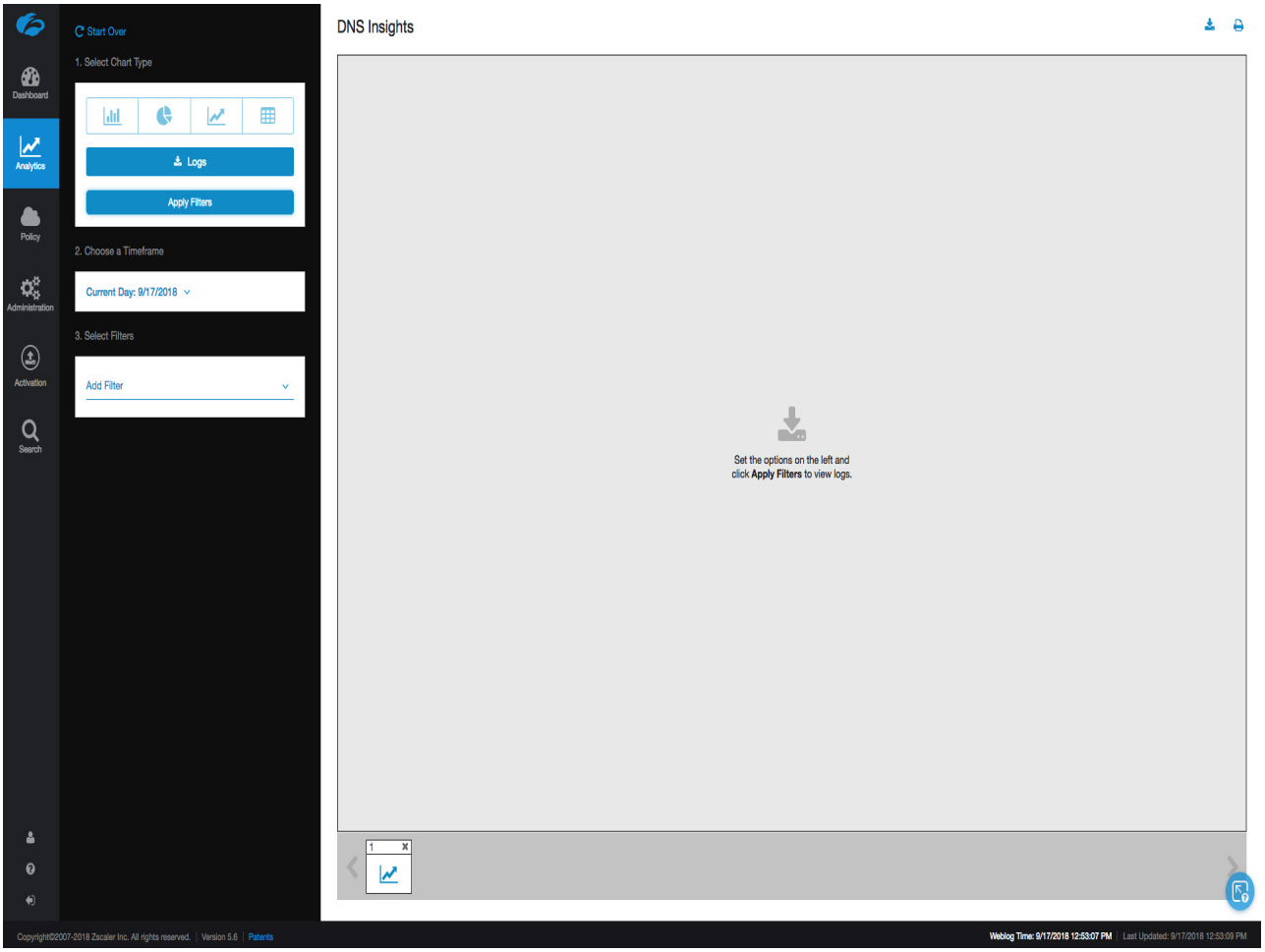
Slide 39 - Slide 39



Slide notes

To see detailed records of DNS transactions click the **Logs** button under the Chart Type selection item.

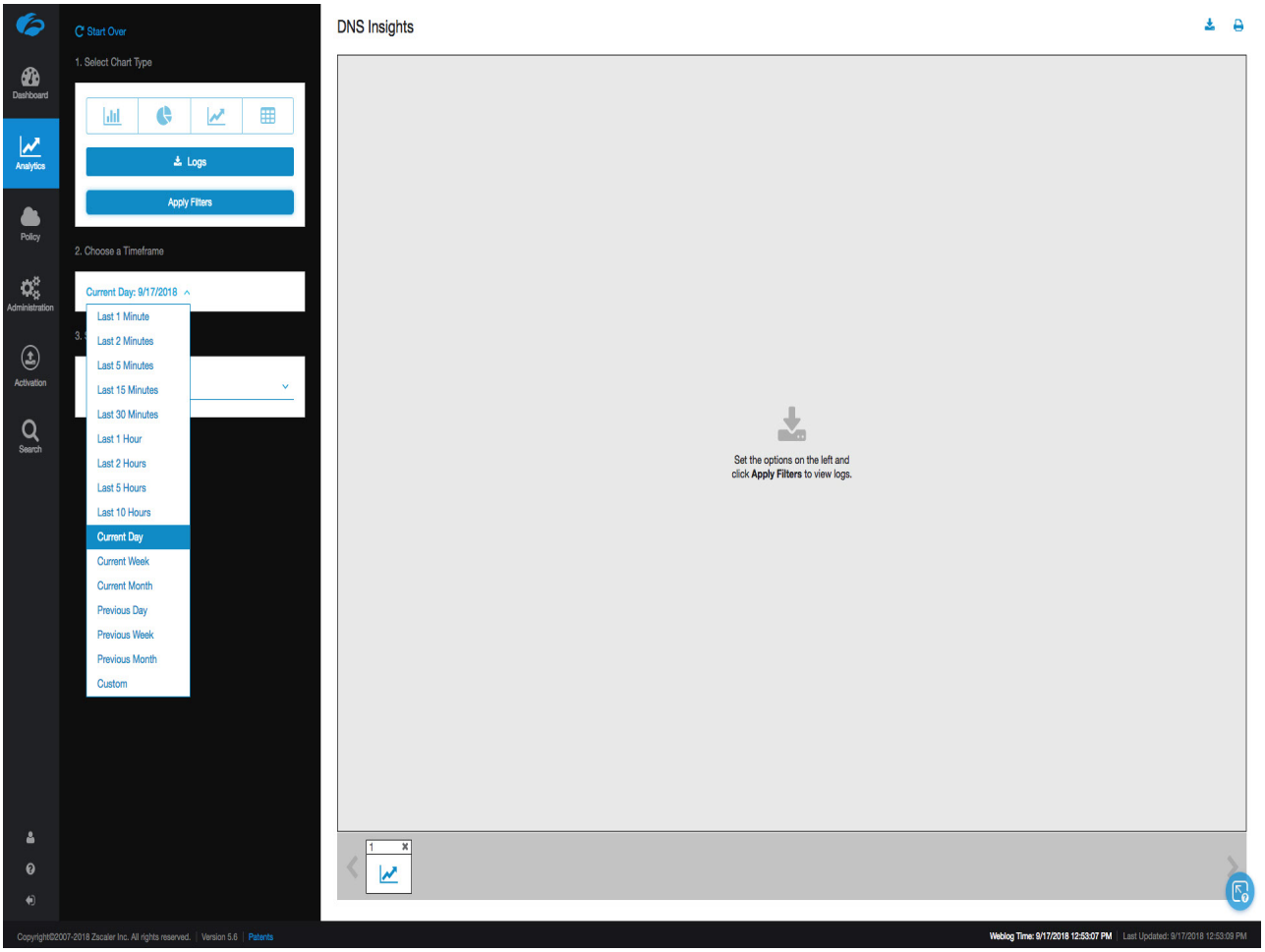
Slide 40 - Slide 40



Slide notes

Note that the **Timeframe** is set to the Current Day. Click the selected Timeframe to see more options.

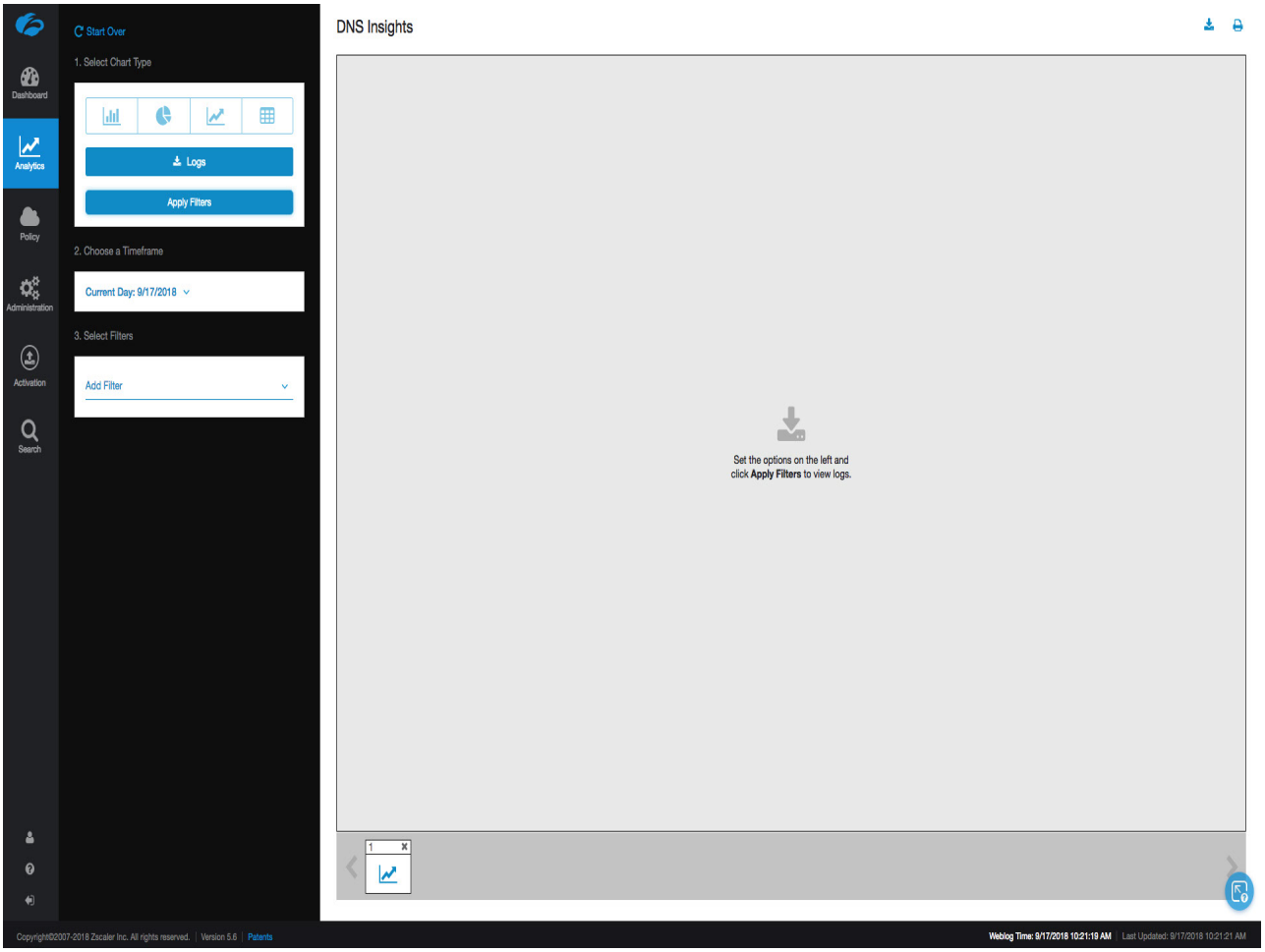
Slide 41 - Slide 41



Slide notes

When viewing logs there are several helpful preset time periods spanning recent minutes, hours, days or months. For this example select **Current Day**.

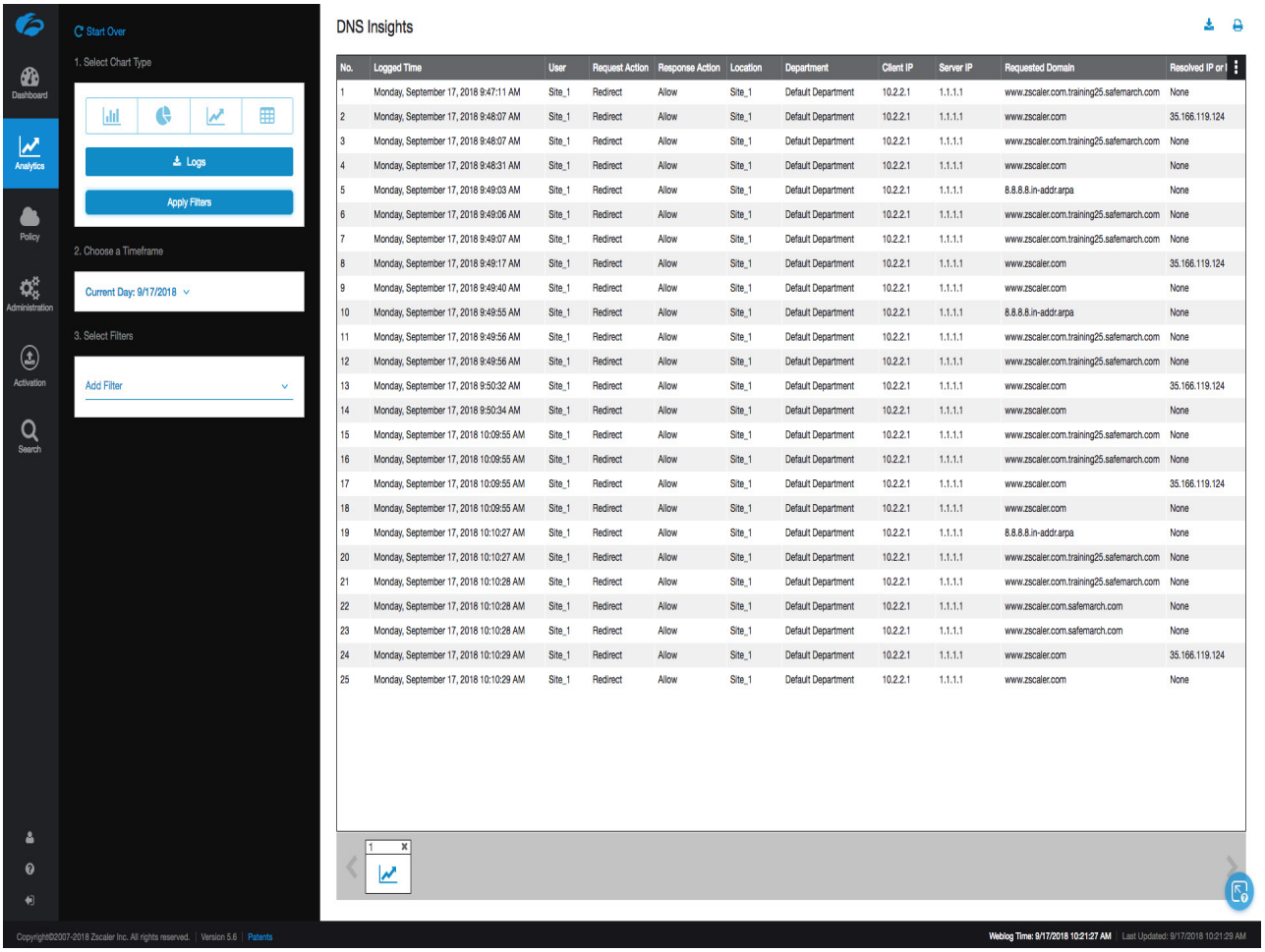
Slide 42 - Slide 42



Slide notes

No other filters will be set for this initial look. Click **Apply Filters** to view the logs.

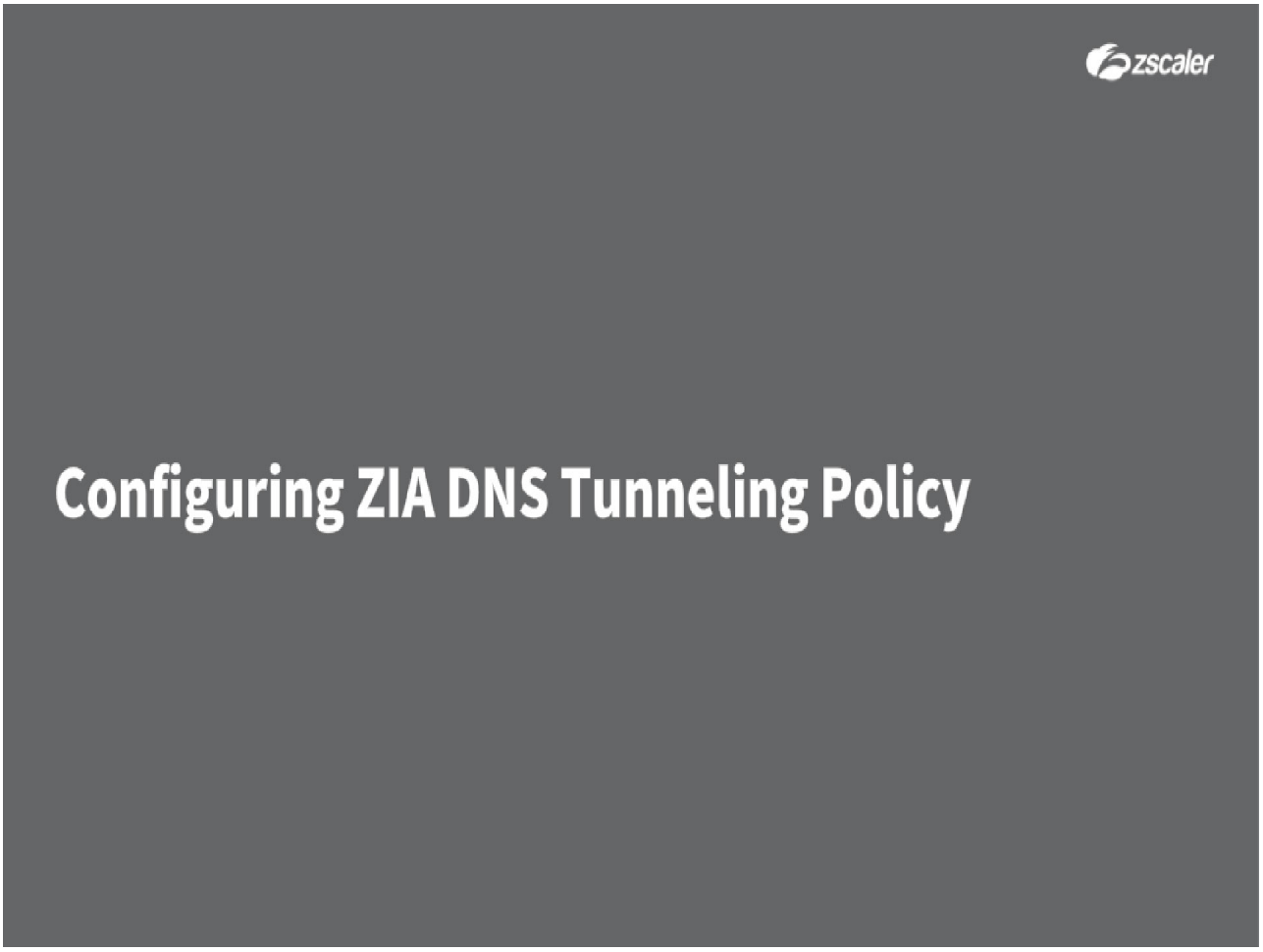
Slide 43 - Slide 43



Slide notes

Log entries show the expected result of **Request Action** of *Redirect*, with the **Location** of *Site_1*, and the **Server IP** of *1.1.1.1*. This verifies that Site_1 requests are being redirected as configured in the DNS Control rule.

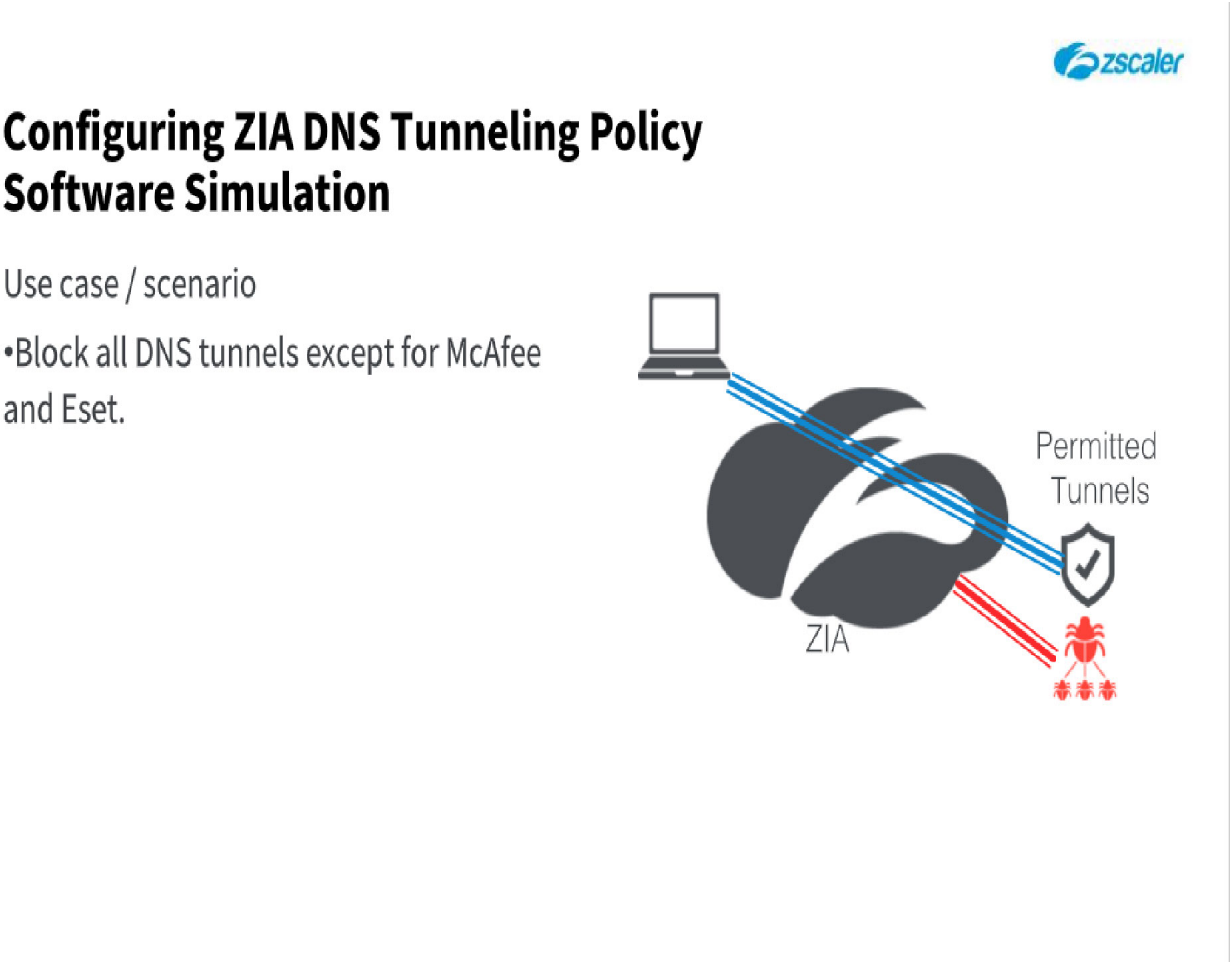
Slide 44 - Configuring ZIA DNS Tunneling Policy



Slide notes

In this task you will configure a ZIA DNS Tunneling Policy.

Slide 45 - Configuring ZIA DNS Tunneling Policy Software Simulation

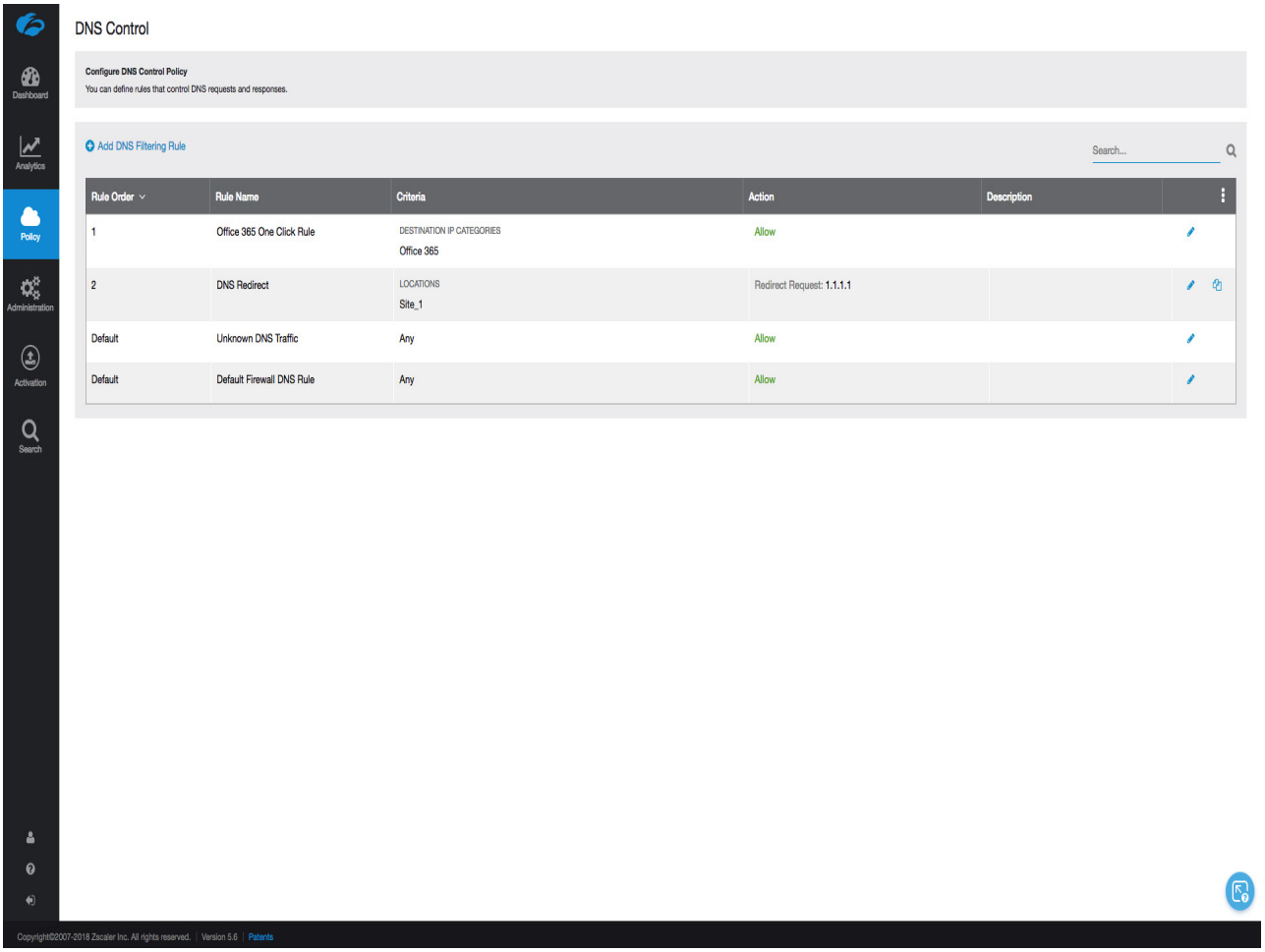


Slide notes

Consider the scenario where an organization's policy is to allow DNS tunnel traffic for only the McAfee and Eset anti-virus applications. You will configure two DNS Control rules. The first rule will block DNS tunnel traffic for a DNS Tunnel Application group that will be configured to include all DNS tunnels. The second rule will be placed higher in the list to allow DNS tunneling for the permitted applications.

To configure a DNS tunneling policy, follow these steps:

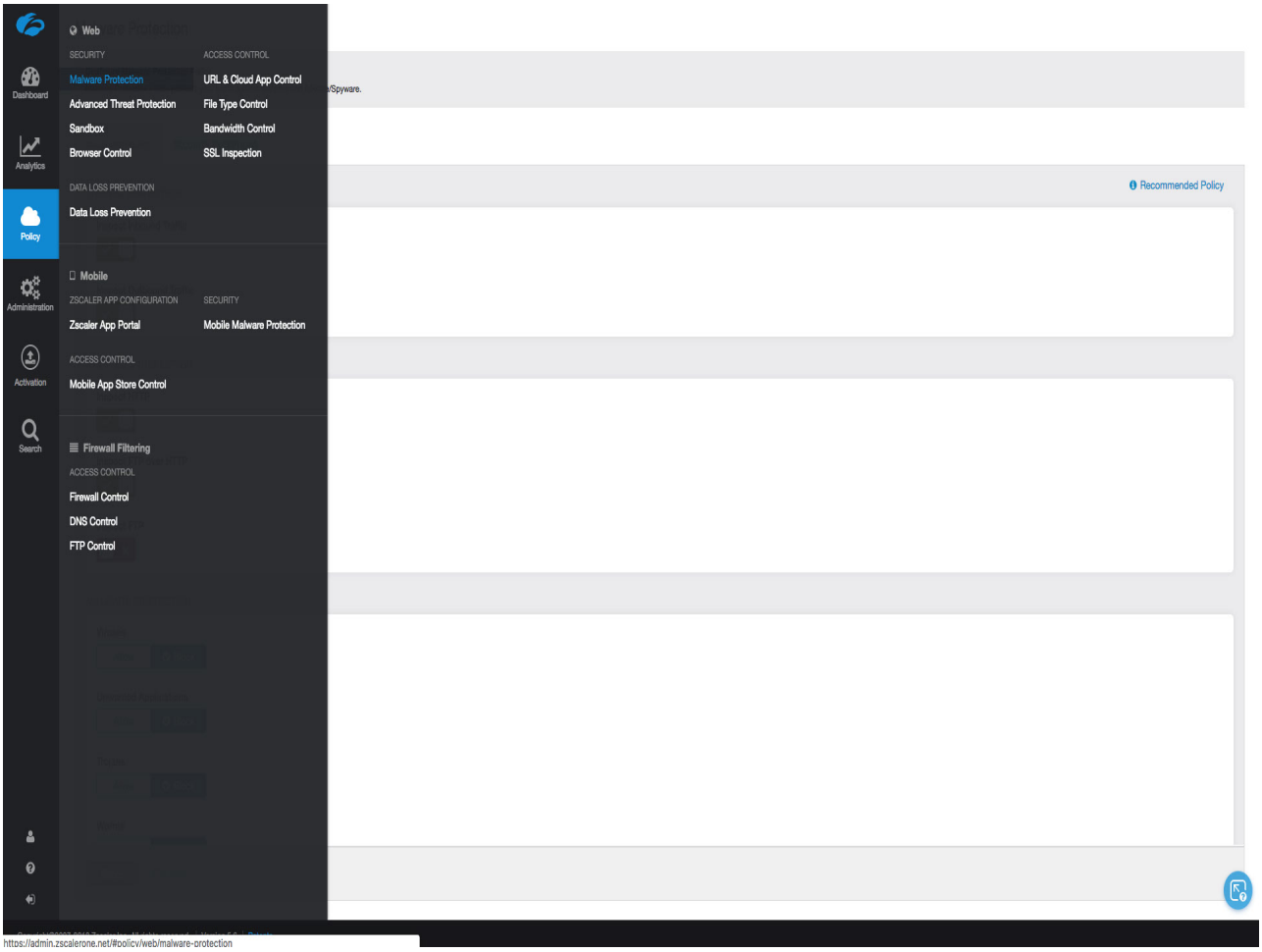
Slide 46 - Slide 46



Slide notes

Click to select from the **Policy** menu.

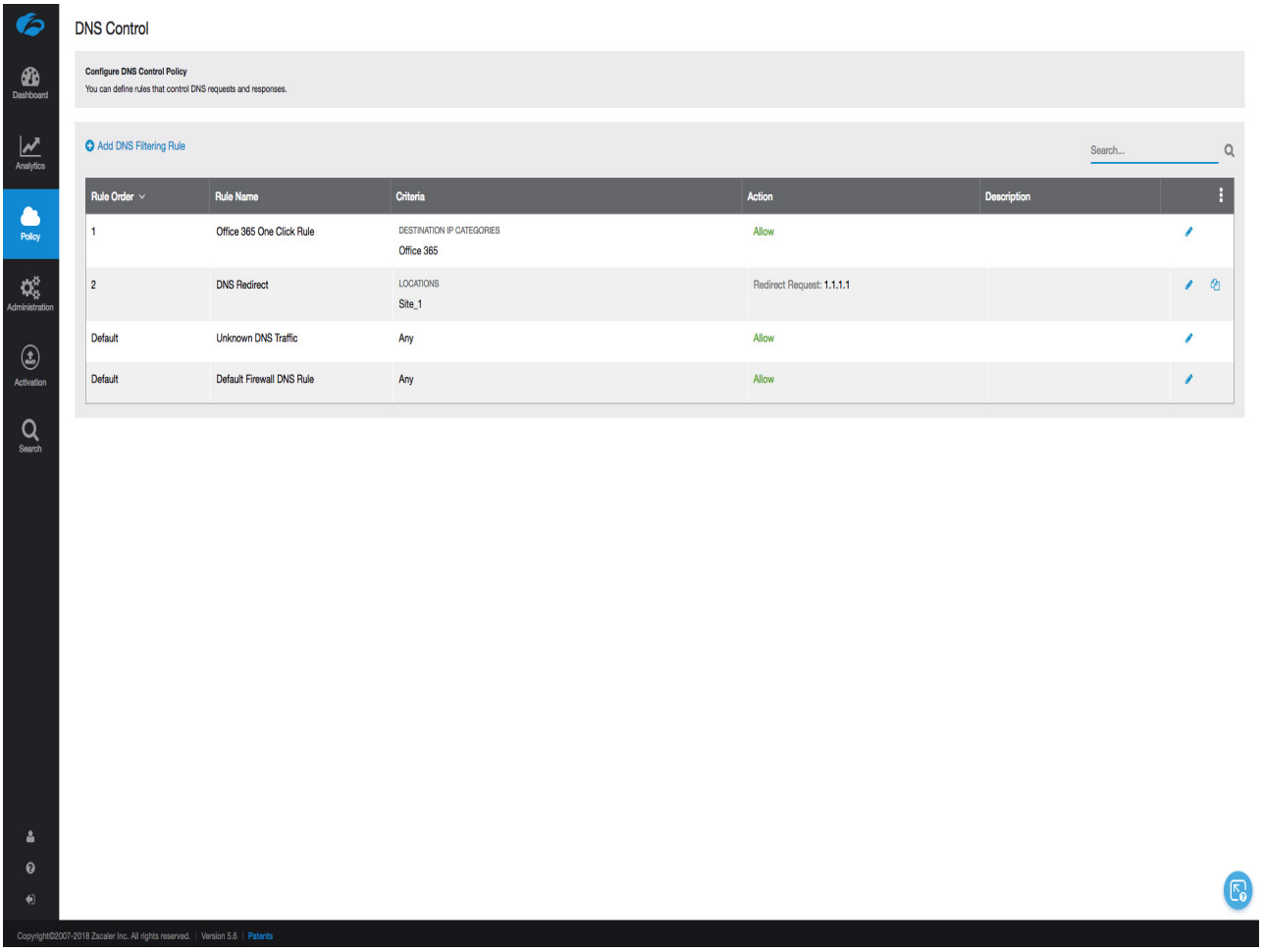
Slide 47 - Slide 47



Slide notes

Select **DNS Control** from the Firewall Filtering Access Controls sub-menu.

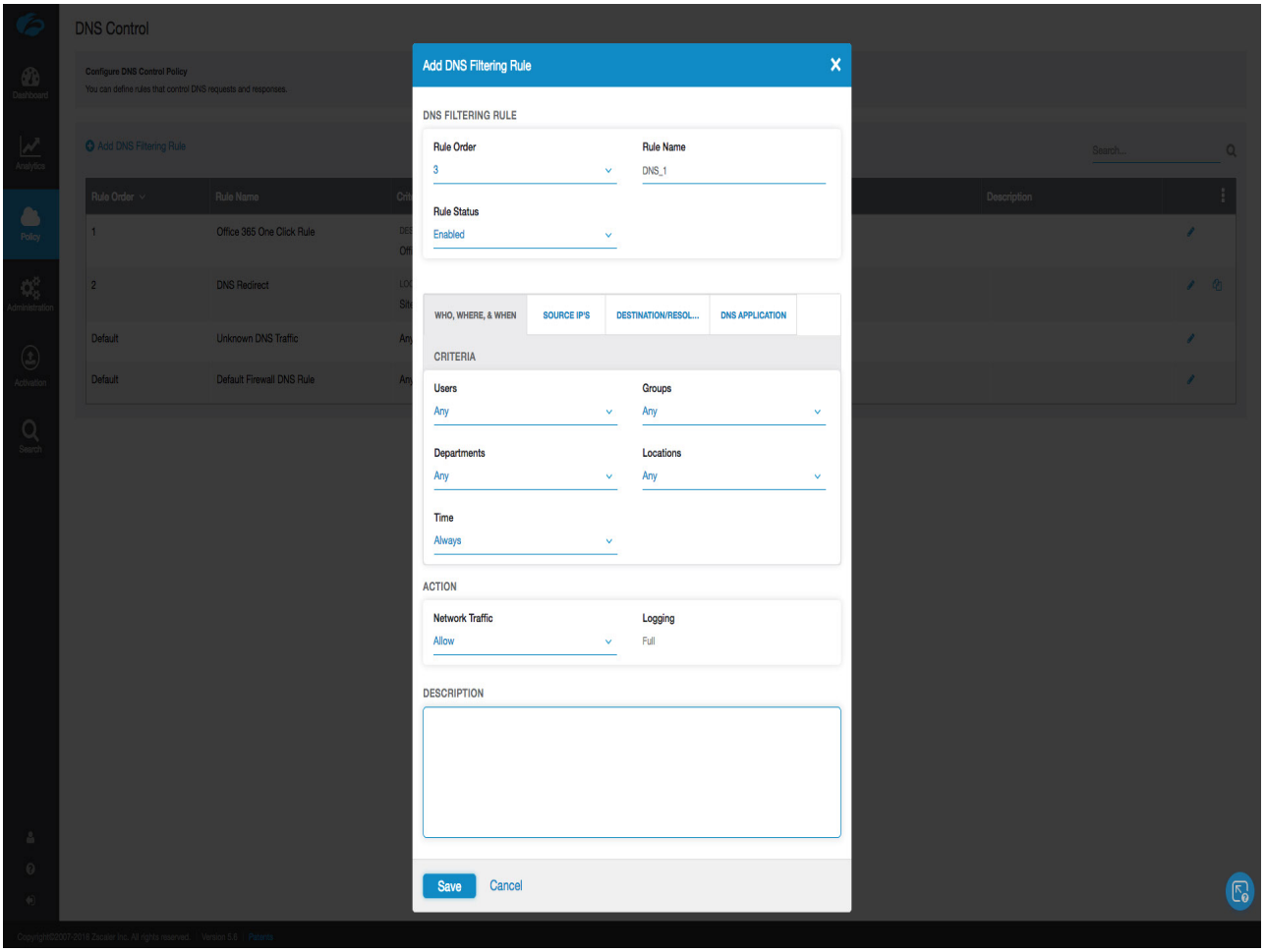
Slide 48 - Slide 48



Slide notes

On the **DNS Control** Page, click **Add DNS Filtering Rule**.

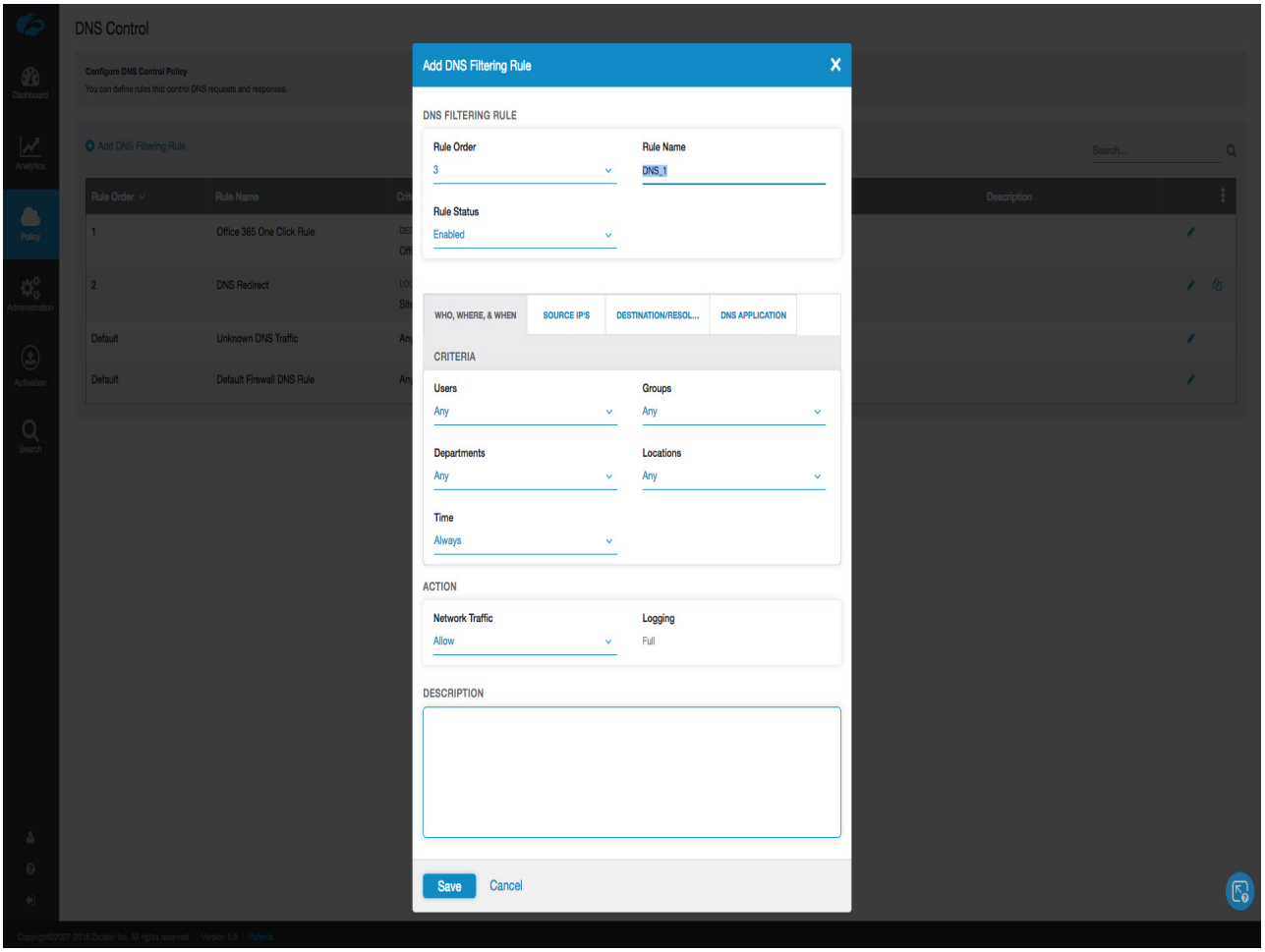
Slide 49 - Slide 49



Slide notes

Note that the rule order is automatically set to the next available number in the list. In this case as rule #3 it will be placed above the defaults rules. **Double-click** in the **Rule Name** field to select to change the system generated rule name.

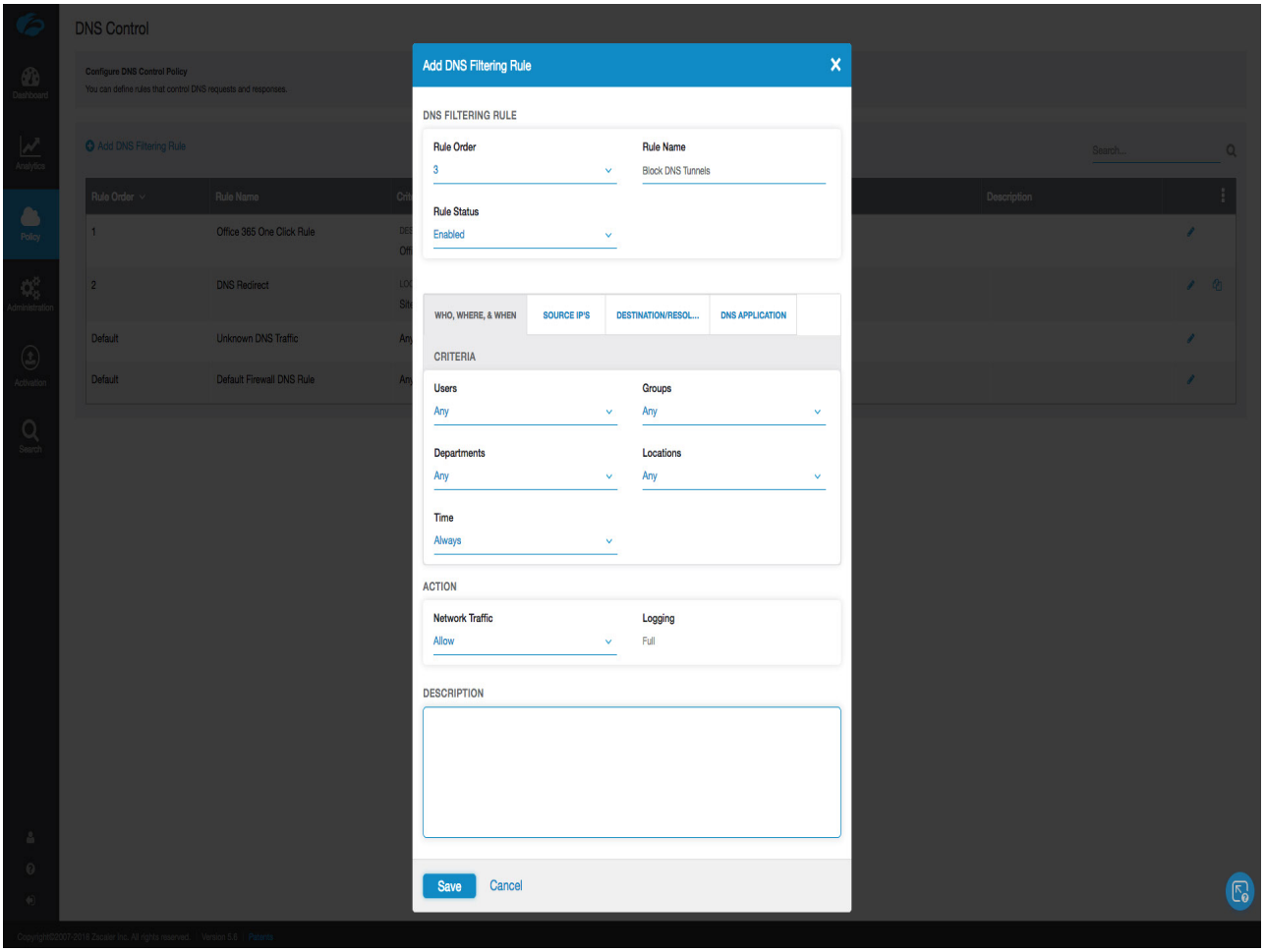
Slide 50 - Slide 50



Slide notes

Type the rule name **Block DNS Tunnels** and hit **Enter**.

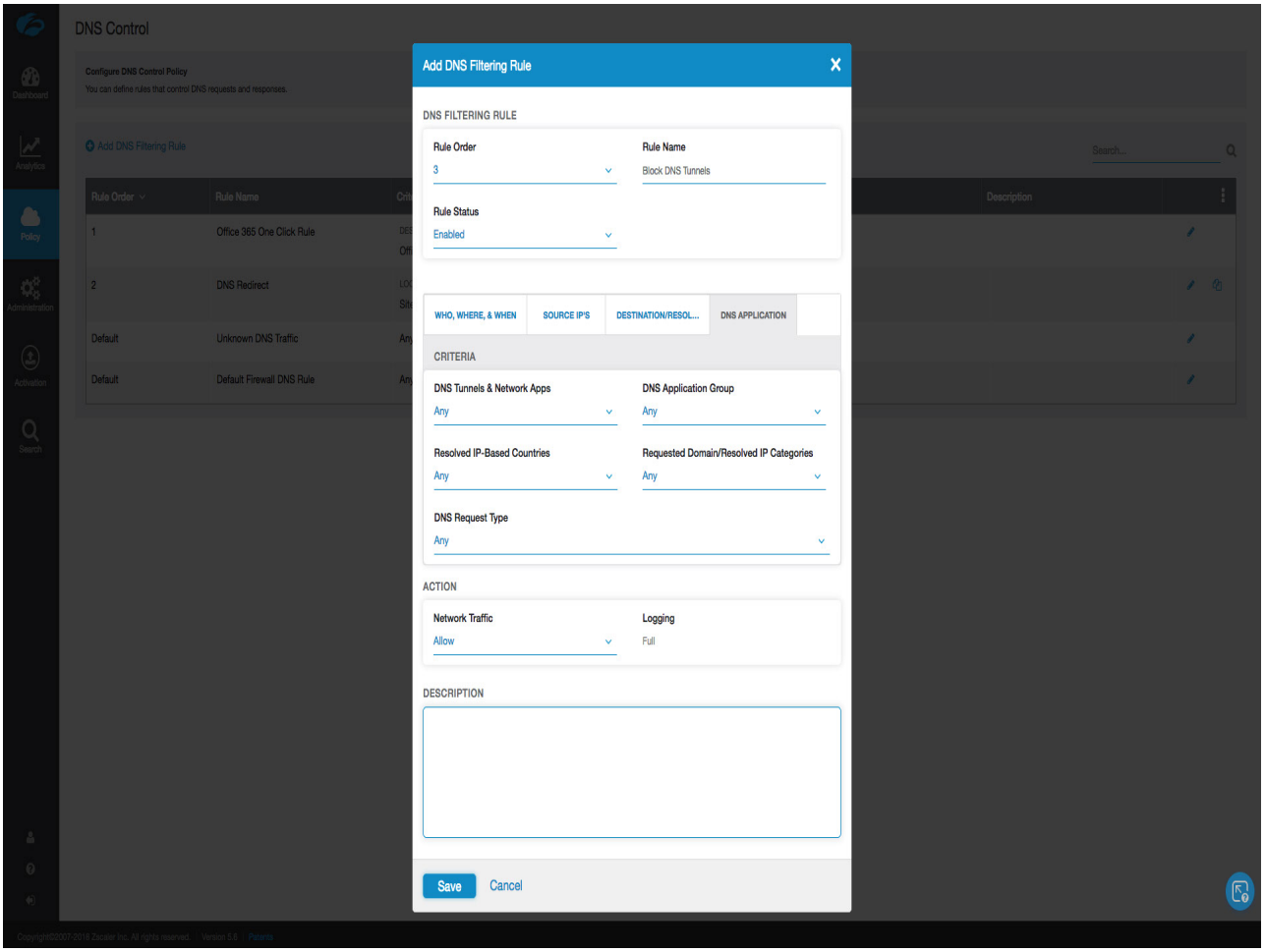
Slide 51 - Slide 51



Slide notes

This rule is to apply to tunnel traffic for all users at all locations, so the default settings for the **WHO, WHERE and WHEN** criteria will be used. Click the **DNS APPLICATION** tab to select the tunnels to block.

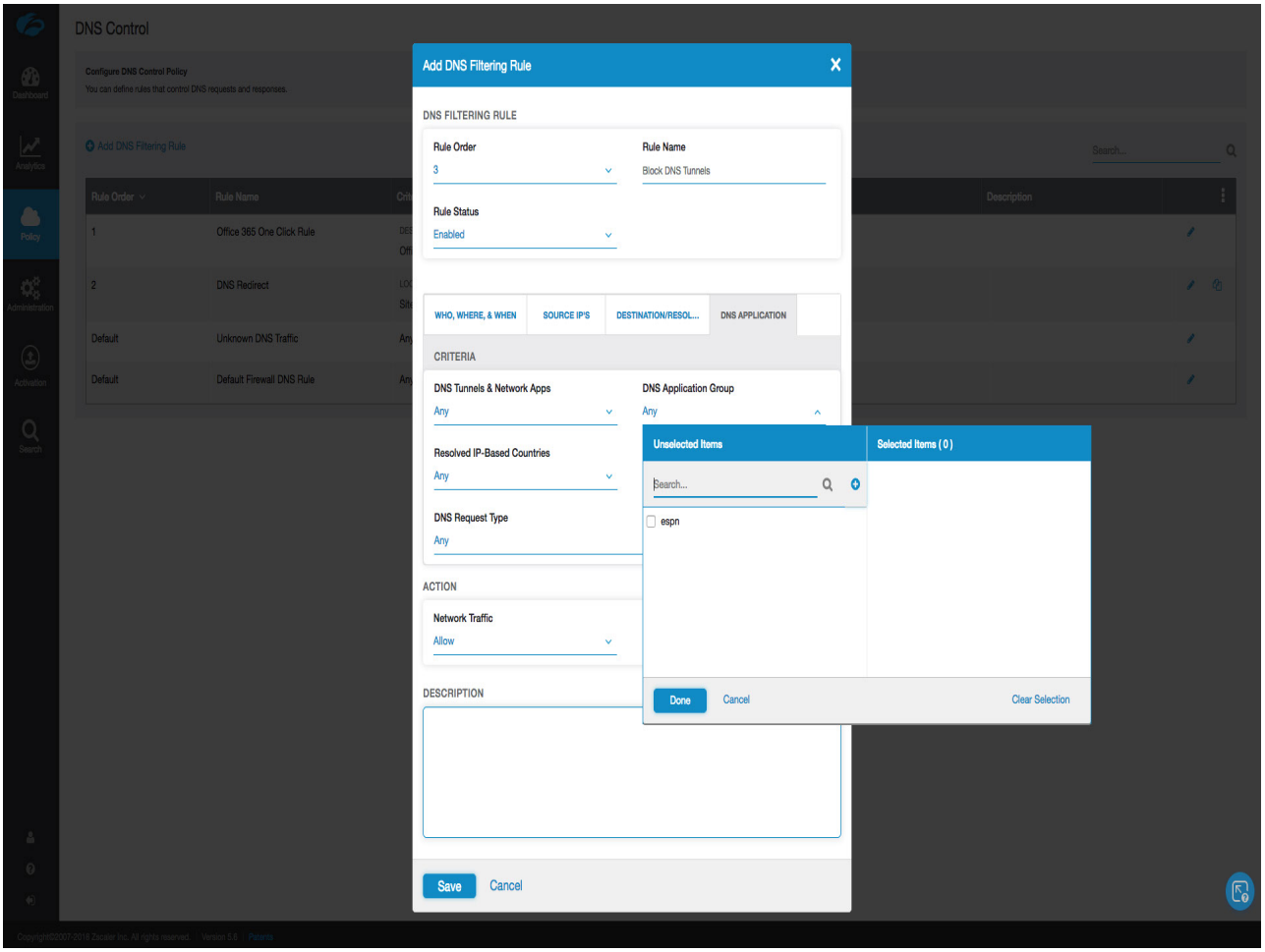
Slide 52 - Slide 52



Slide notes

Click to view the **DNS Application Groups**.

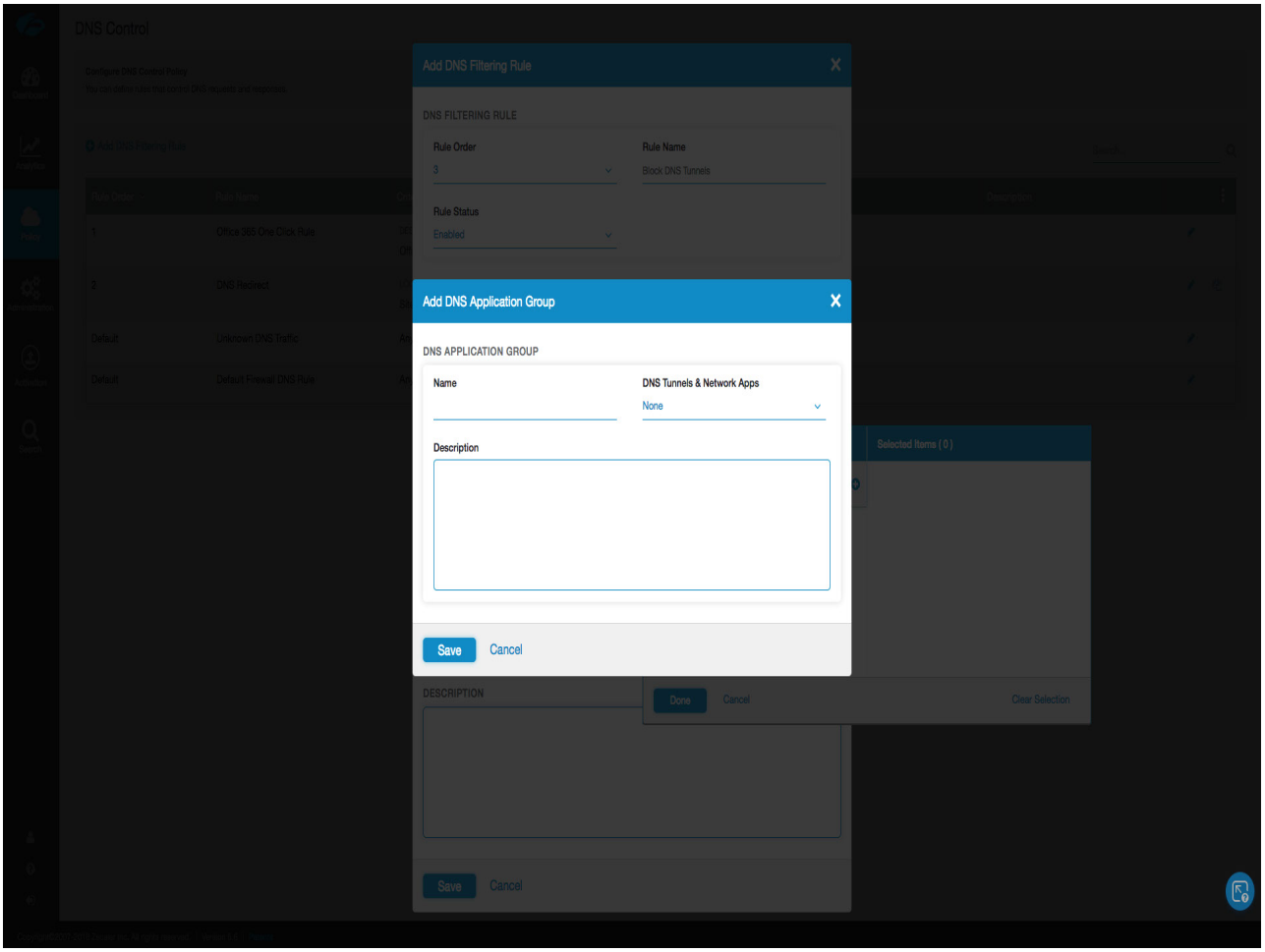
Slide 53 - Slide 53



Slide notes

Any previously configured **DNS Application Groups** will be displayed. **DNS Application Groups** may either be configured from the **Network Applications** item in the **Administration** menu or added here directly by clicking on the **+** symbol.

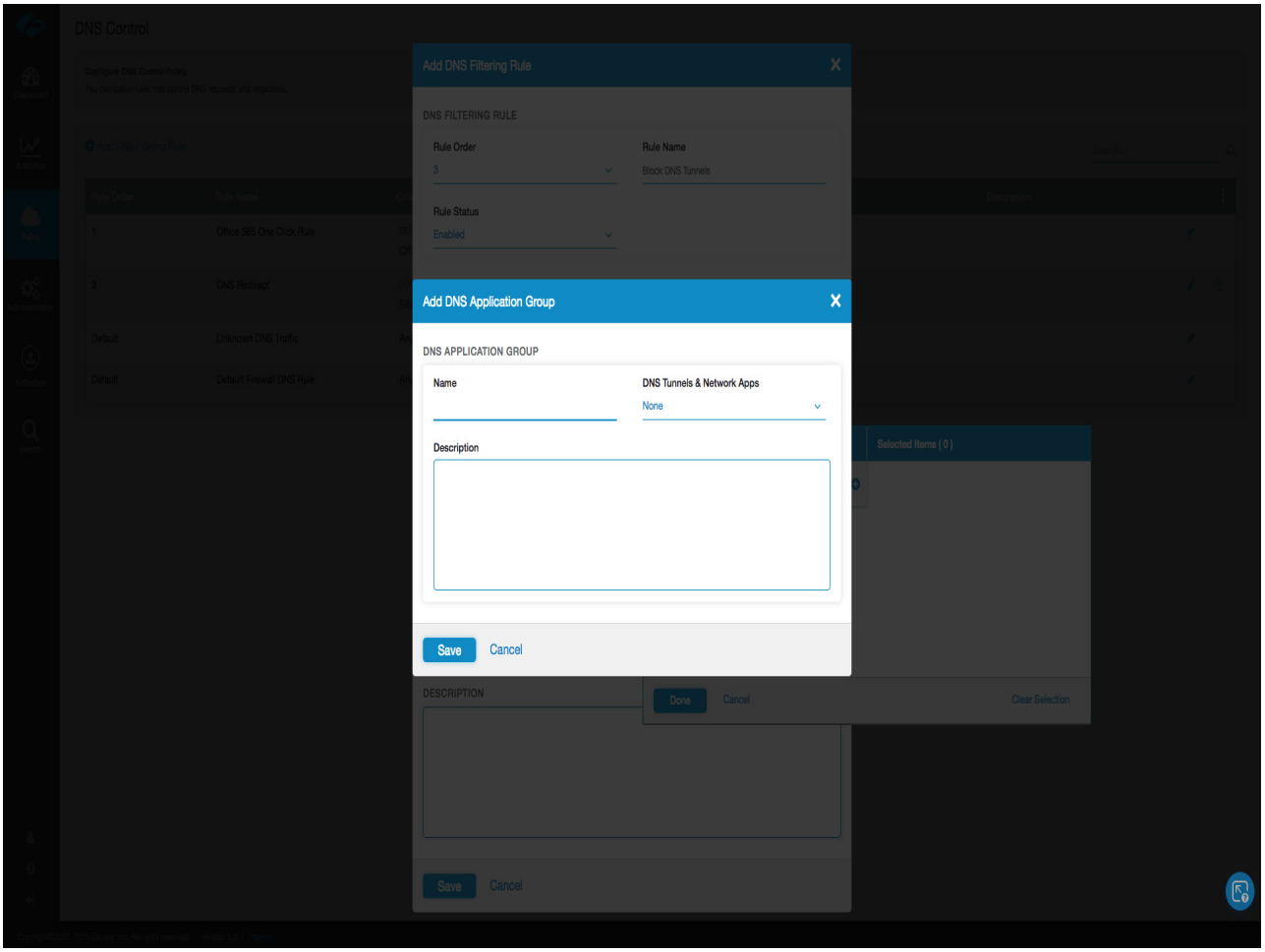
Slide 54 - Slide 54



Slide notes

Select to enter a **Name** for the new DNS Application Group.

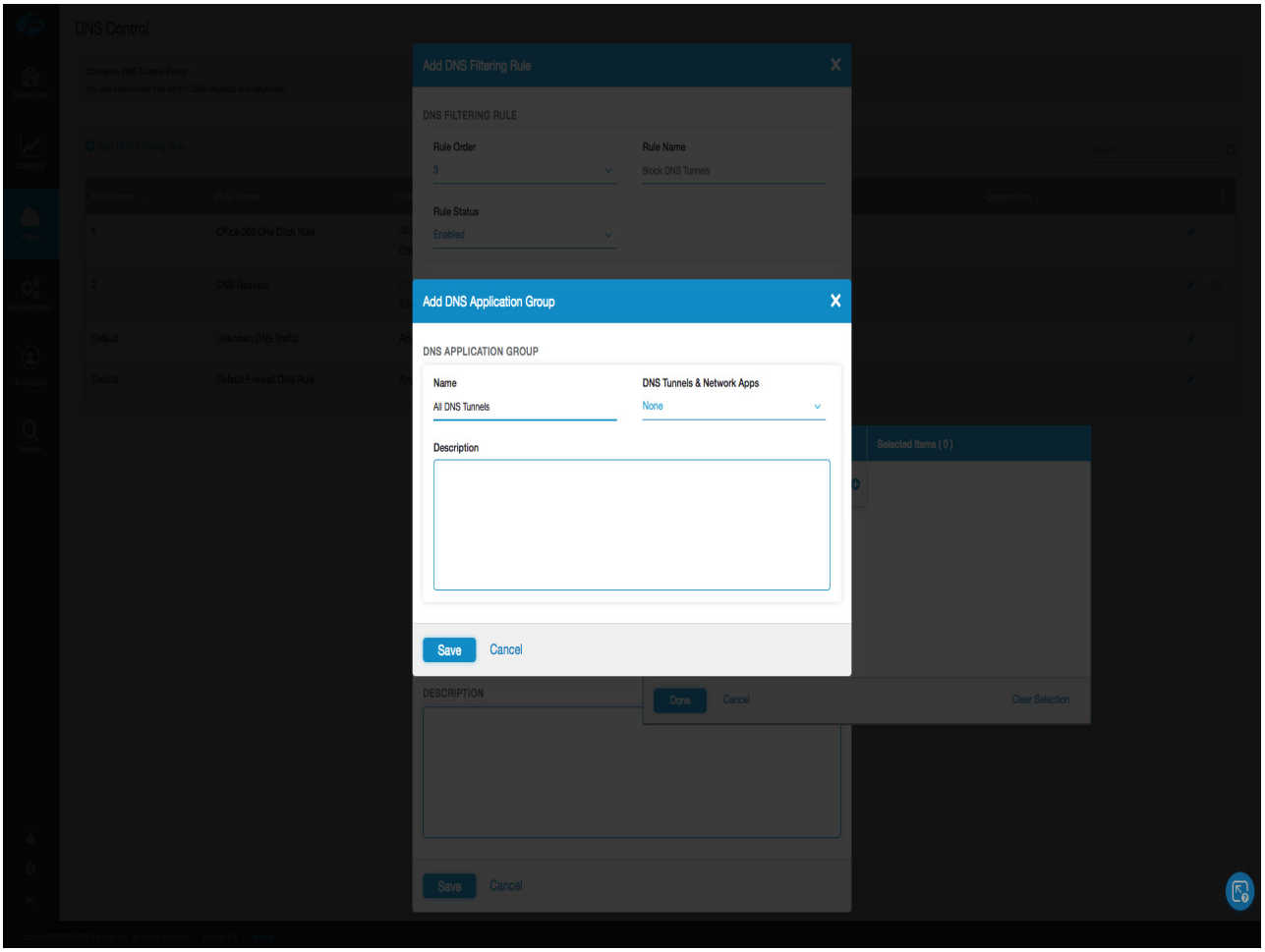
Slide 55 - Slide 55



Slide notes

Type **All DNS Tunnels** and hit enter.

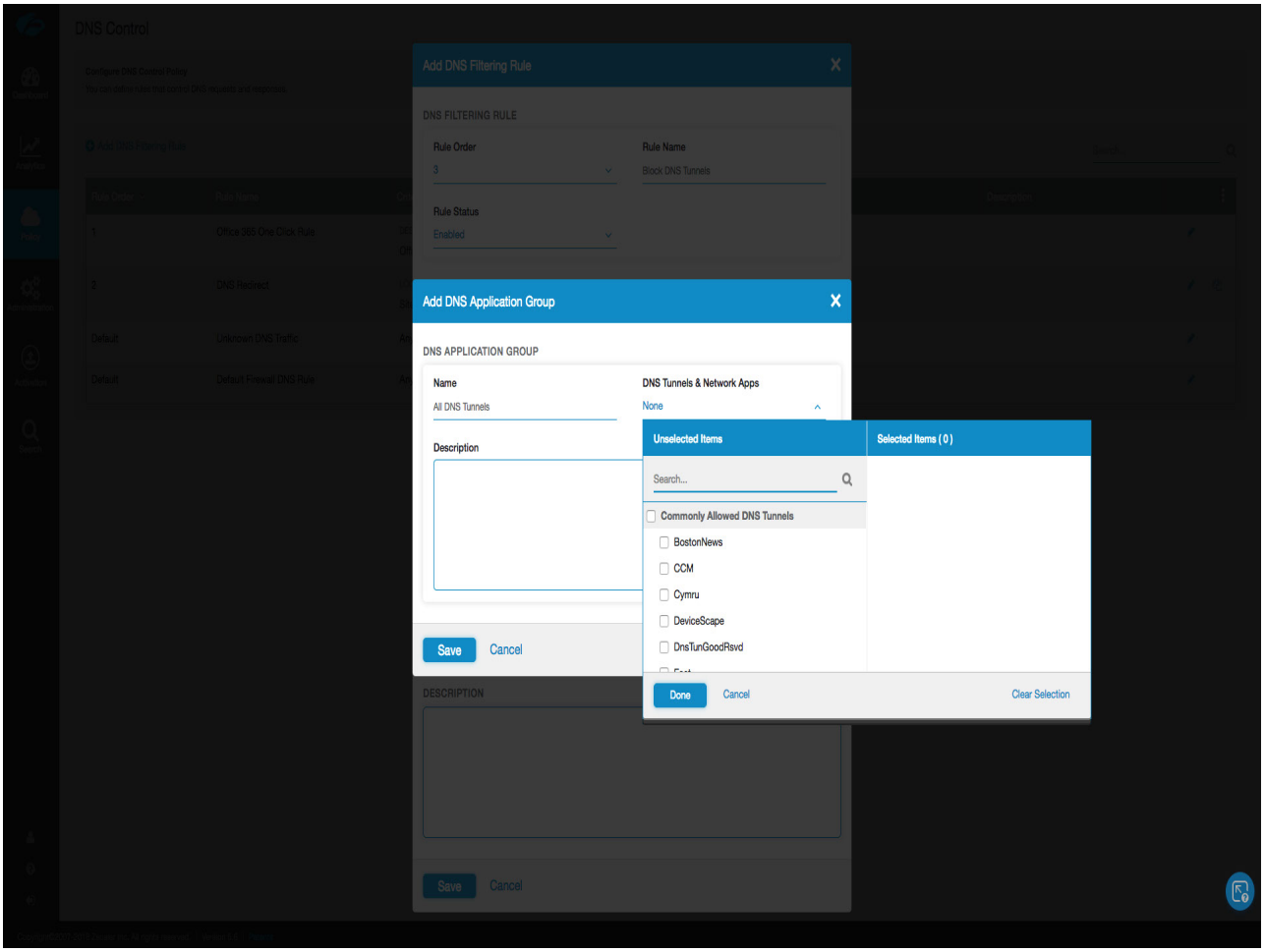
Slide 56 - Slide 56



Slide notes

Now add all of the DNS Tunnels to the group. Click to select from the **DNS Tunnels and Network Apps** list.

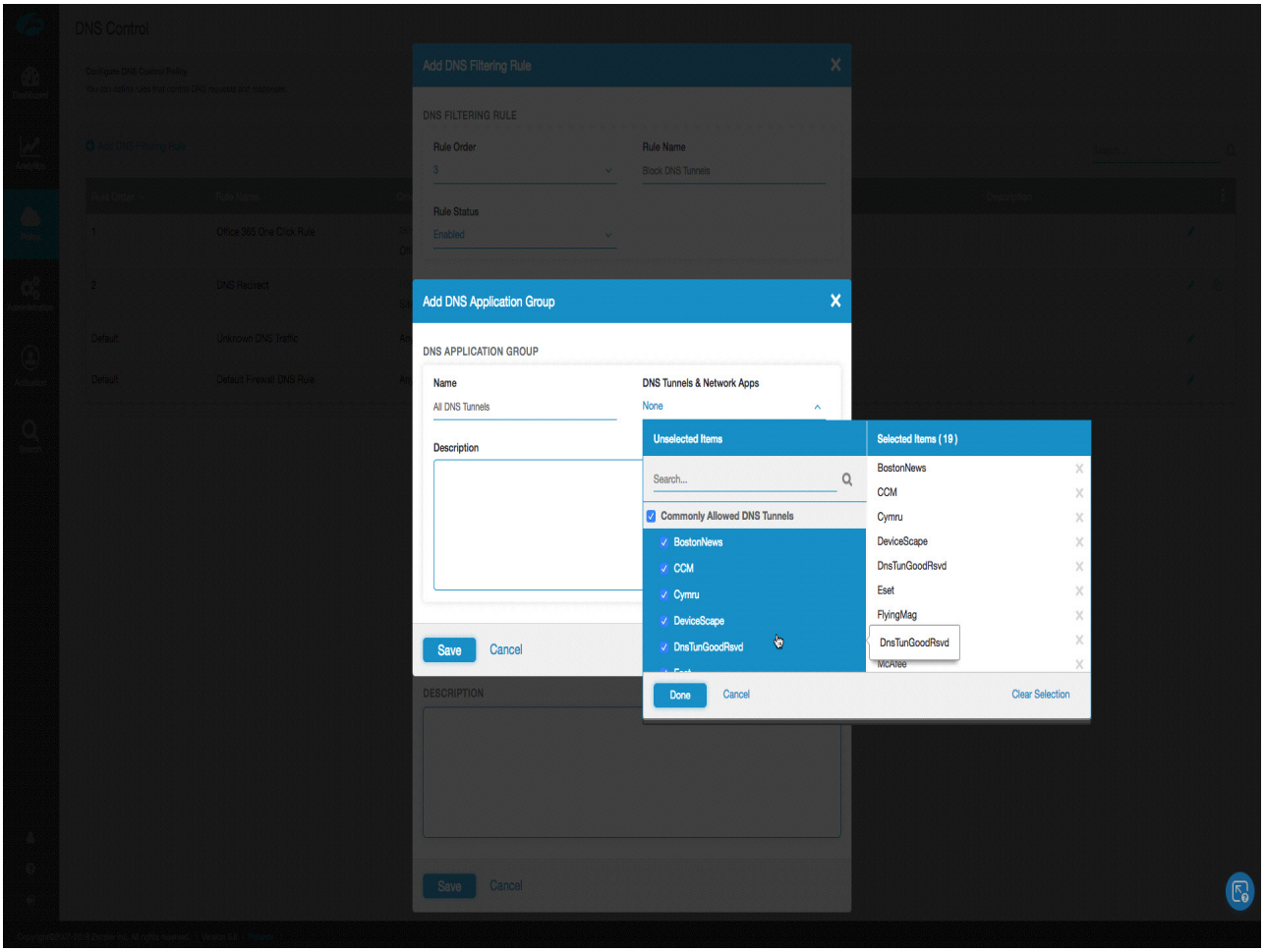
Slide 57 - Slide 57



Slide notes

Selecting a DNS tunnel category will add all of its tunnels to the **Selected Items** list. Click to include the items in the **Commonly Allowed DNS Tunnels** category.

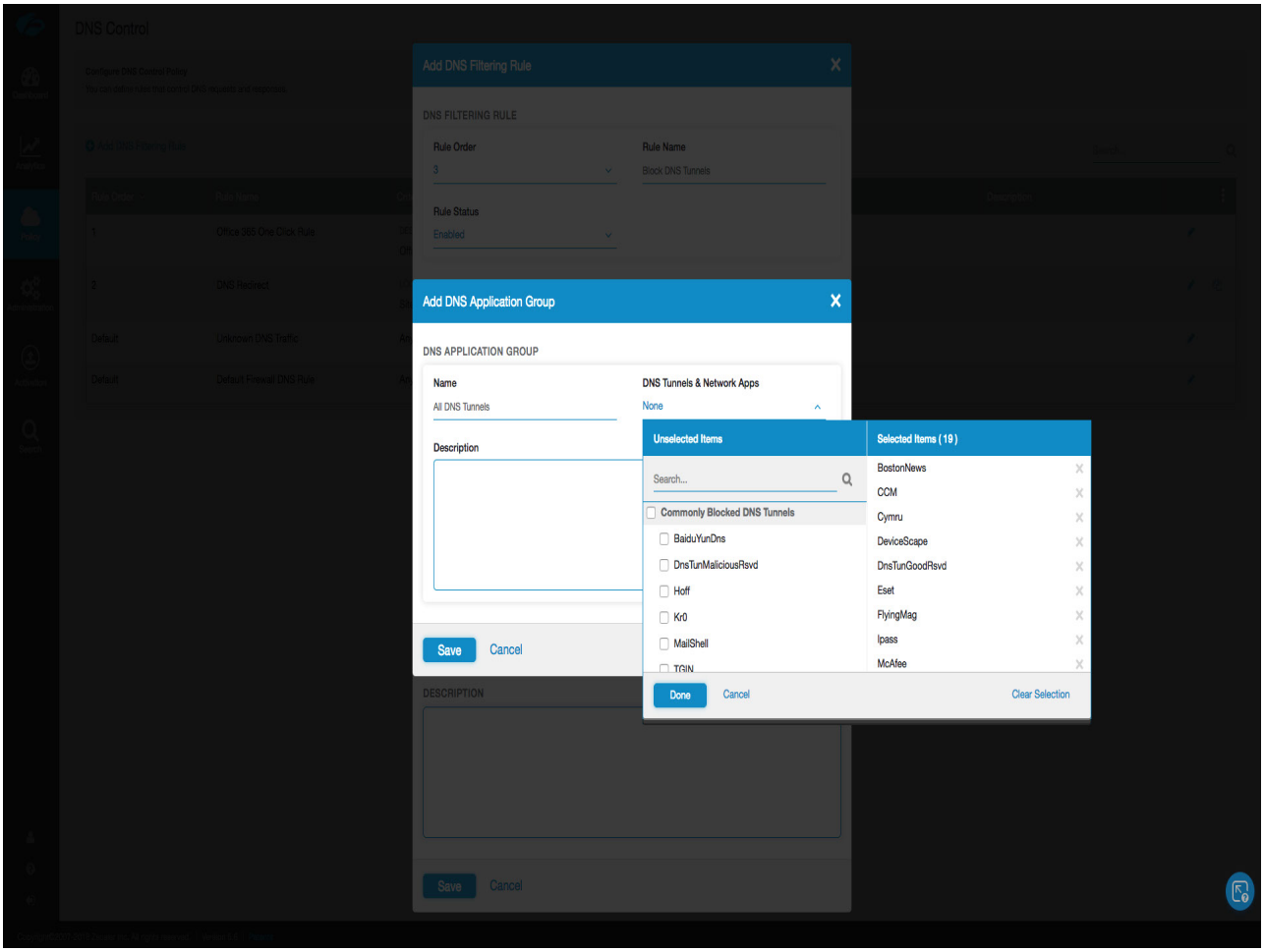
Slide 58 - Slide 58



Slide notes

Note that in this example 19 items were added to the **Selected Items** list.

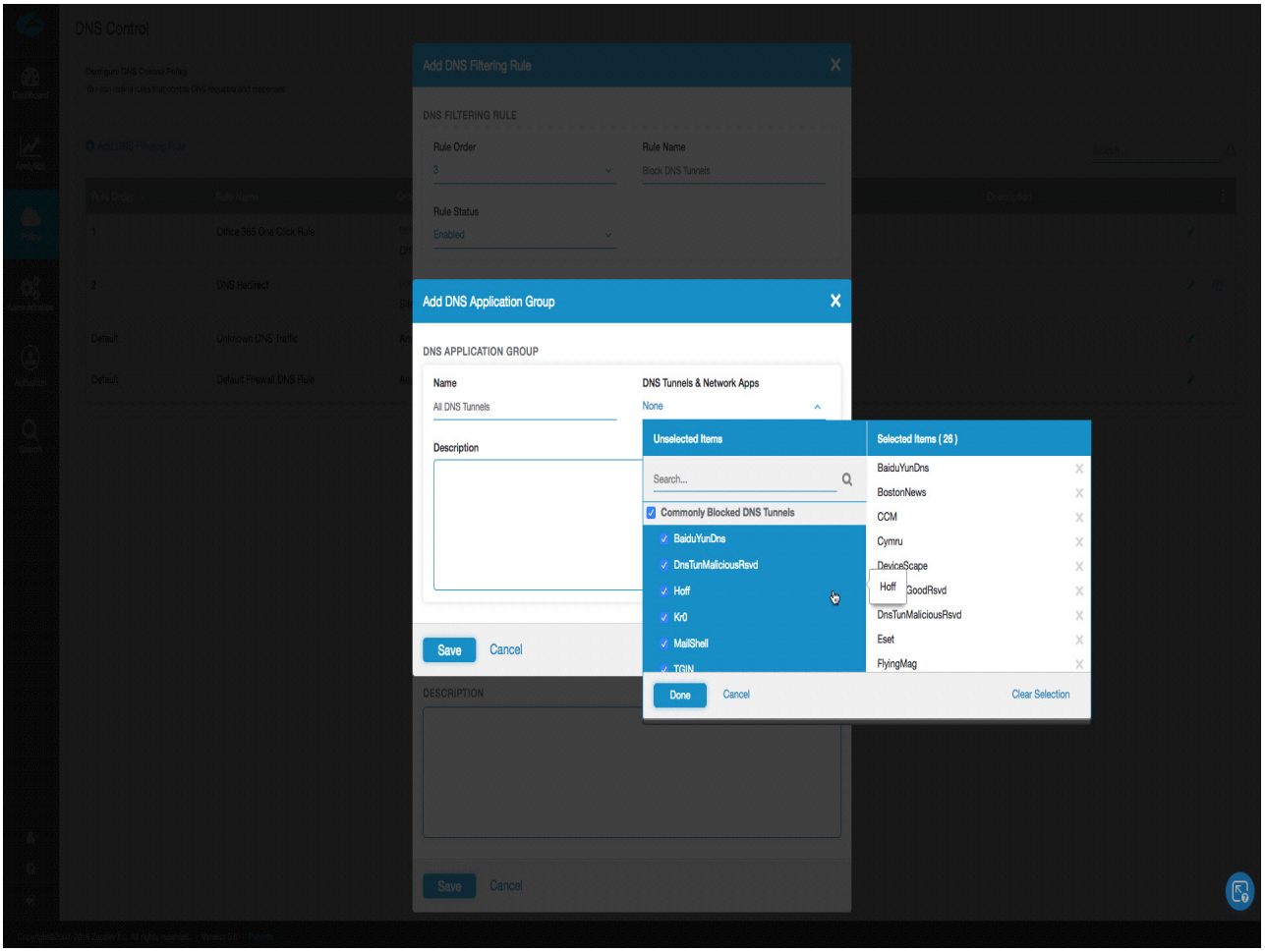
Slide 59 - Slide 59



Slide notes

Further down in the list find the **Commonly Blocked DNS Tunnels** and click to also include them in the selected items for the group.

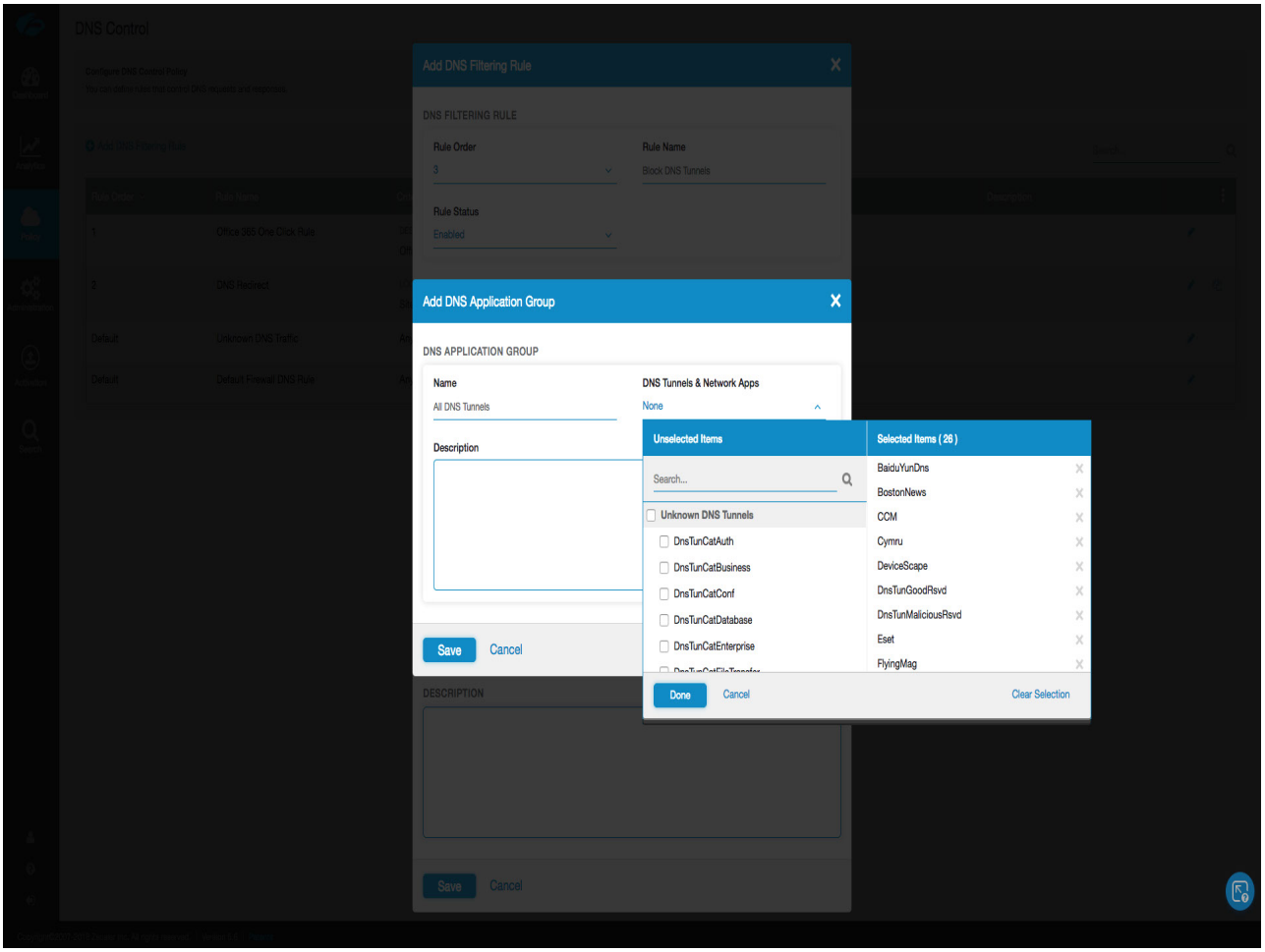
Slide 60 - Slide 60



Slide notes

Note that 7 more items were added to the **Selected Items** list.

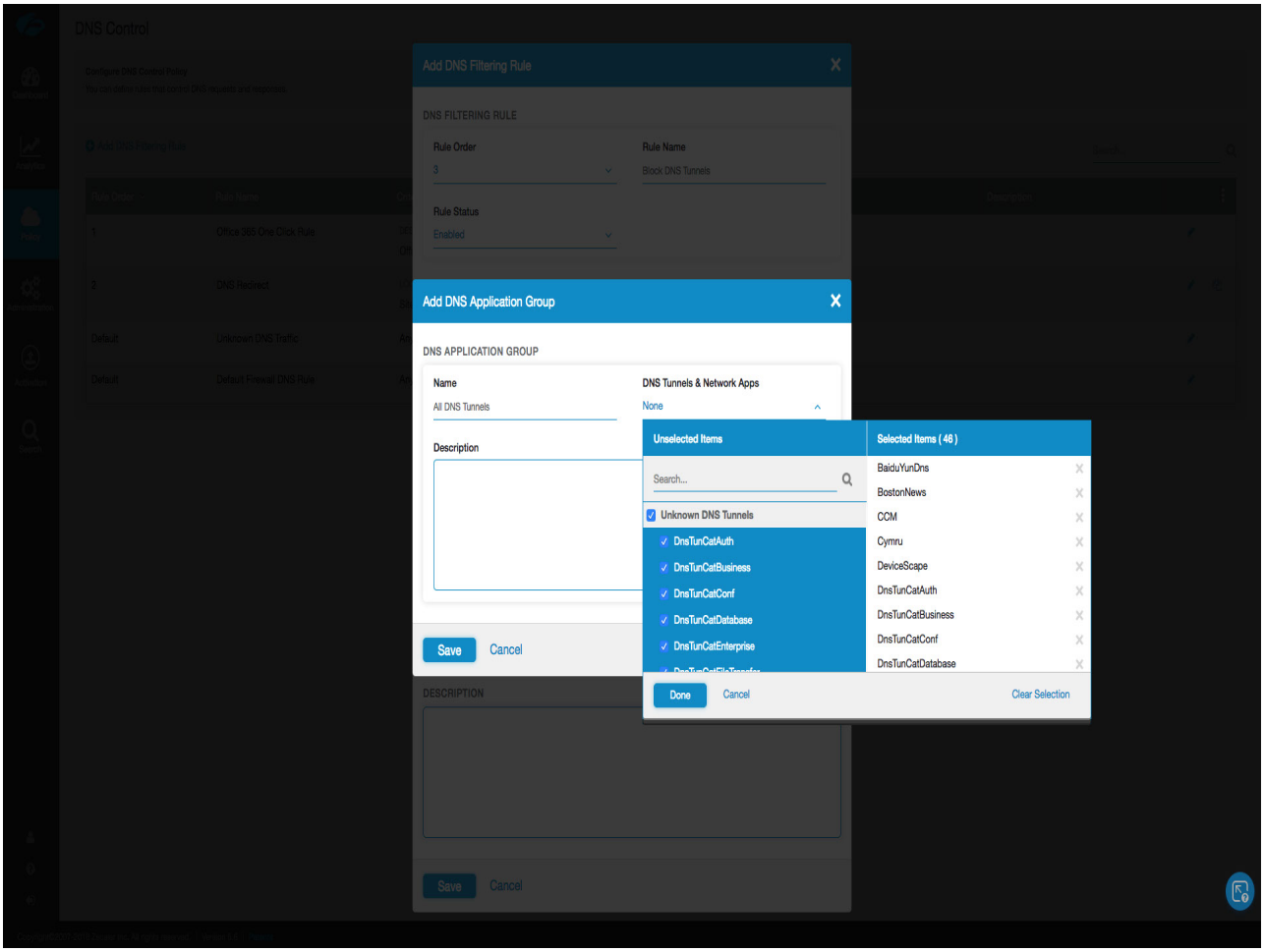
Slide 61 - Slide 61



Slide notes

Repeat to find and add the tunnels in the **Unknown DNS Tunnels** category to the selected items.

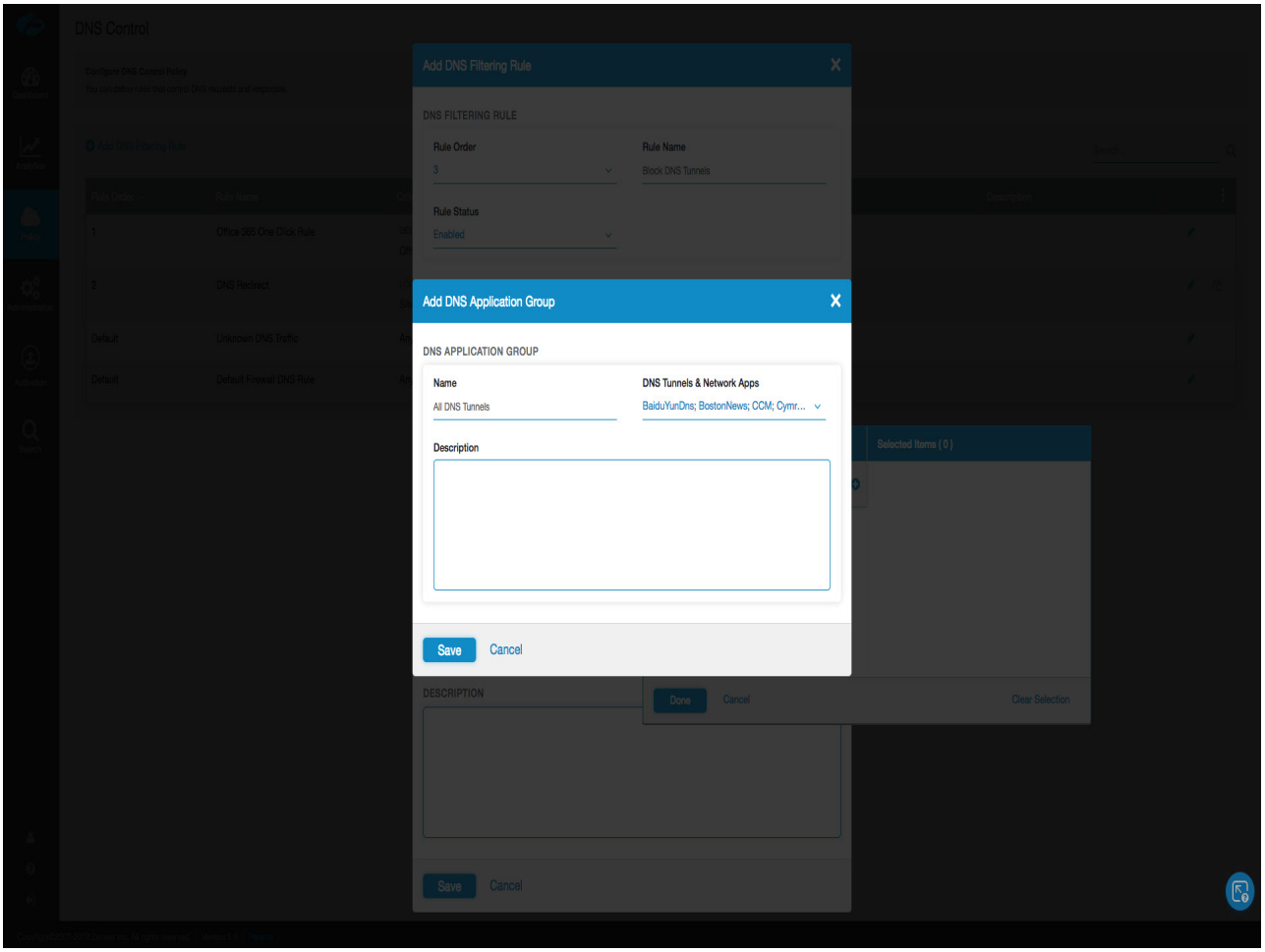
Slide 62 - Slide 62



Slide notes

Now that all DNS tunnels are included in the **Selected Items** list, click **Done**.

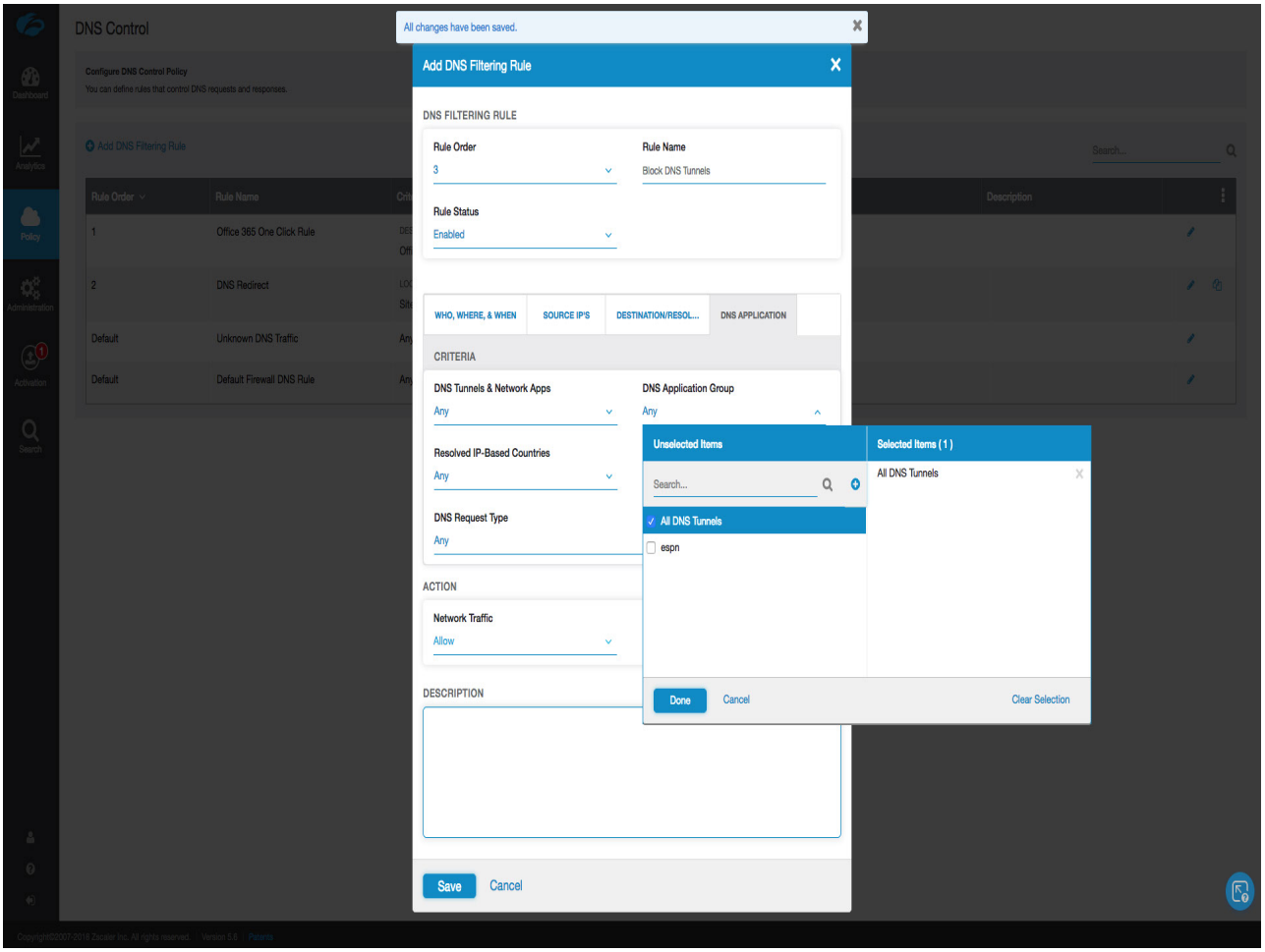
Slide 63 - Slide 63



Slide notes

Save this new **DNS Application Group**.

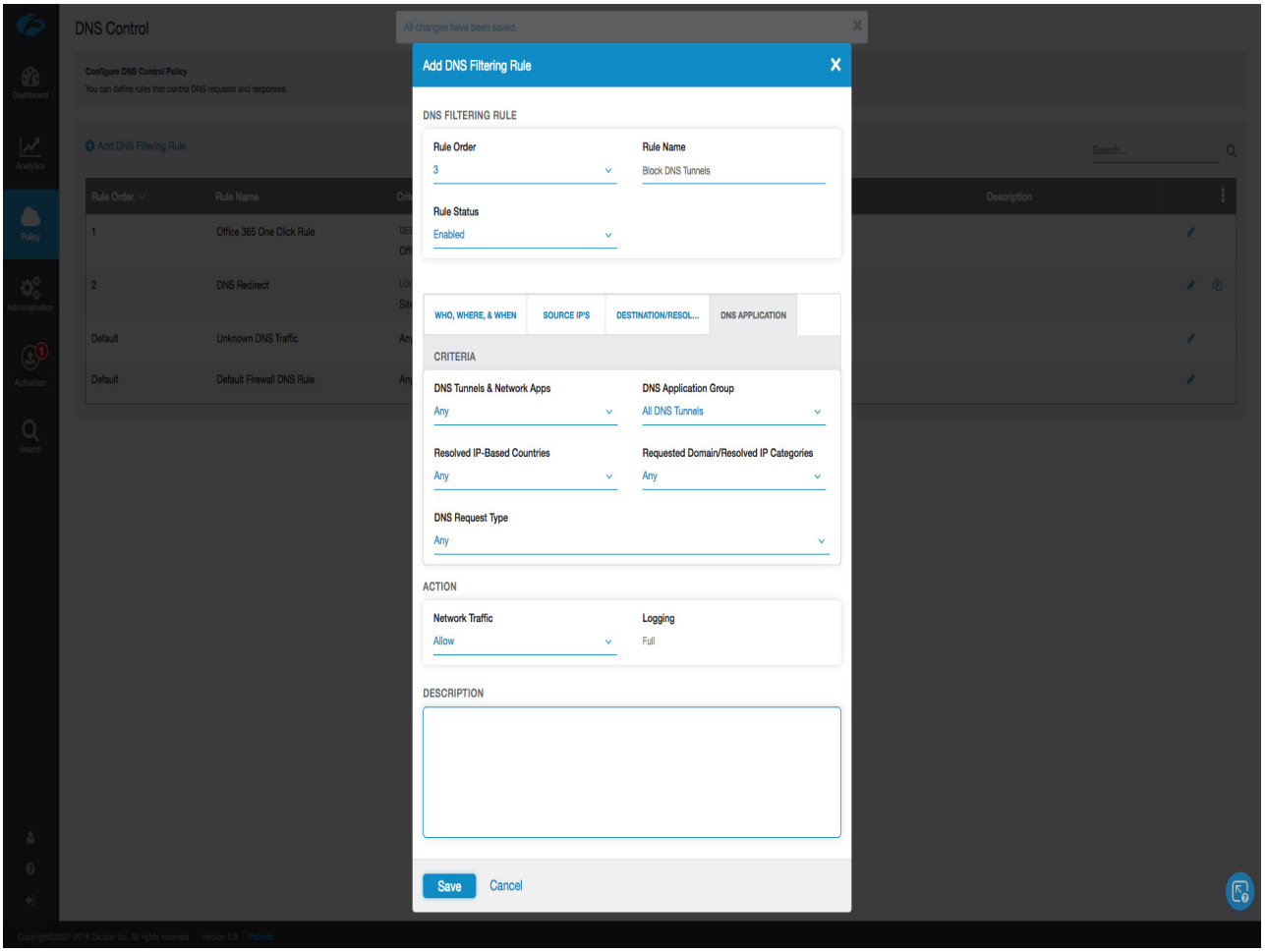
Slide 64 - Slide 64



Slide notes

The newly created **All DNS Tunnels** group is automatically selected, so click **Done**.

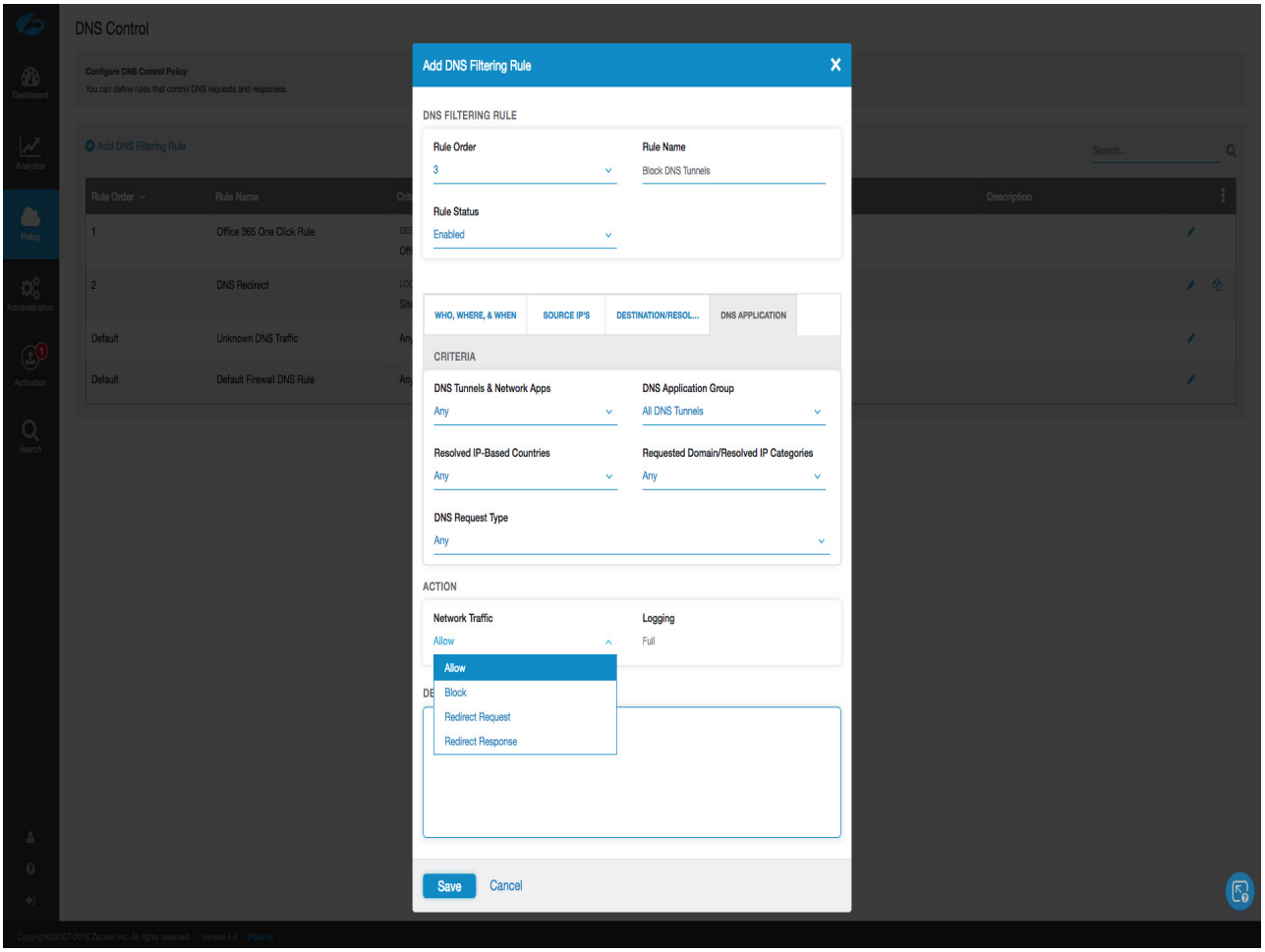
Slide 65 - Slide 65



Slide notes

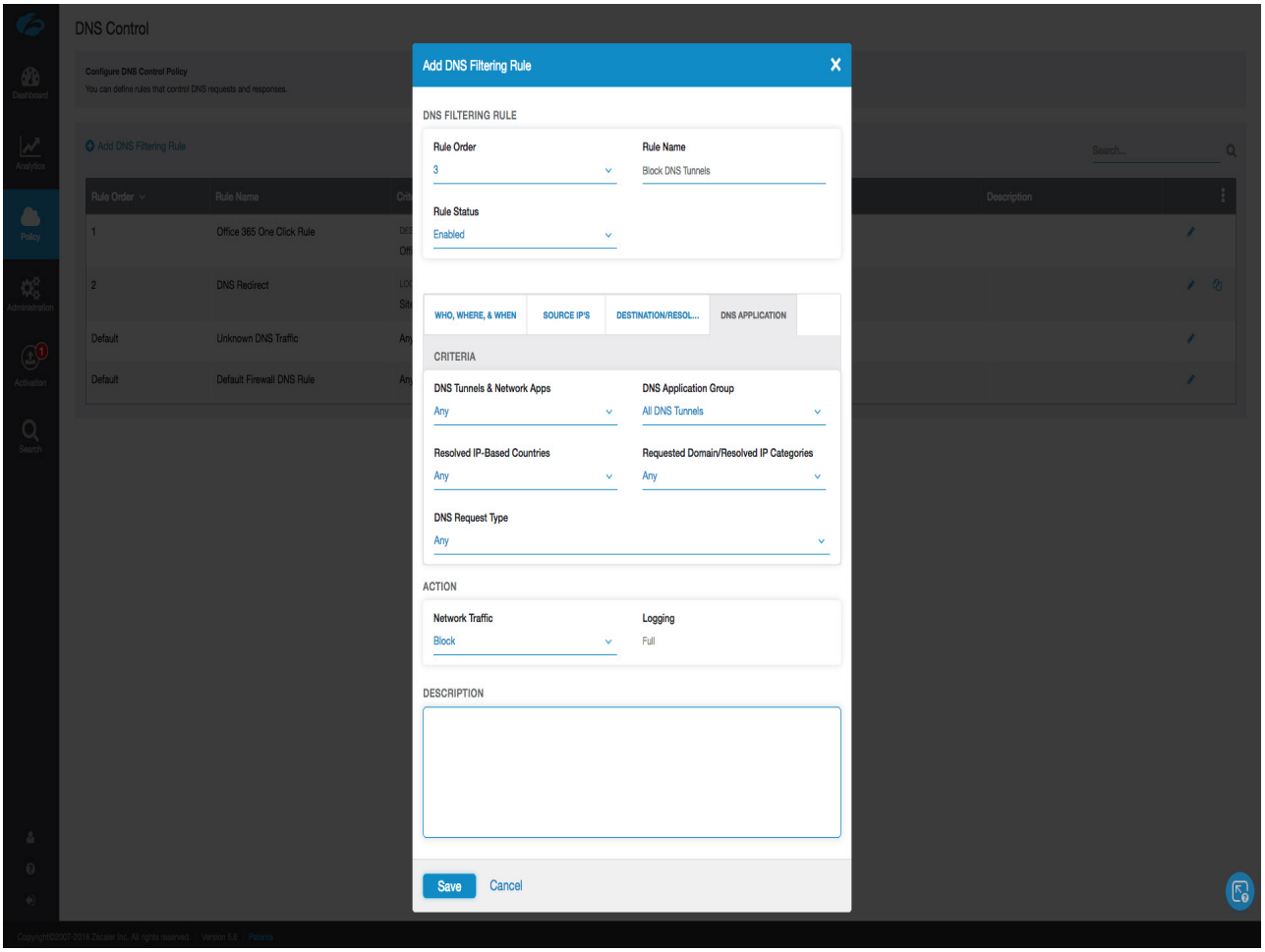
The default **Network Traffic** action is to allow this traffic, so click to select the **Action** to **Block** this traffic.

Slide 66 - Slide 66



Slide notes

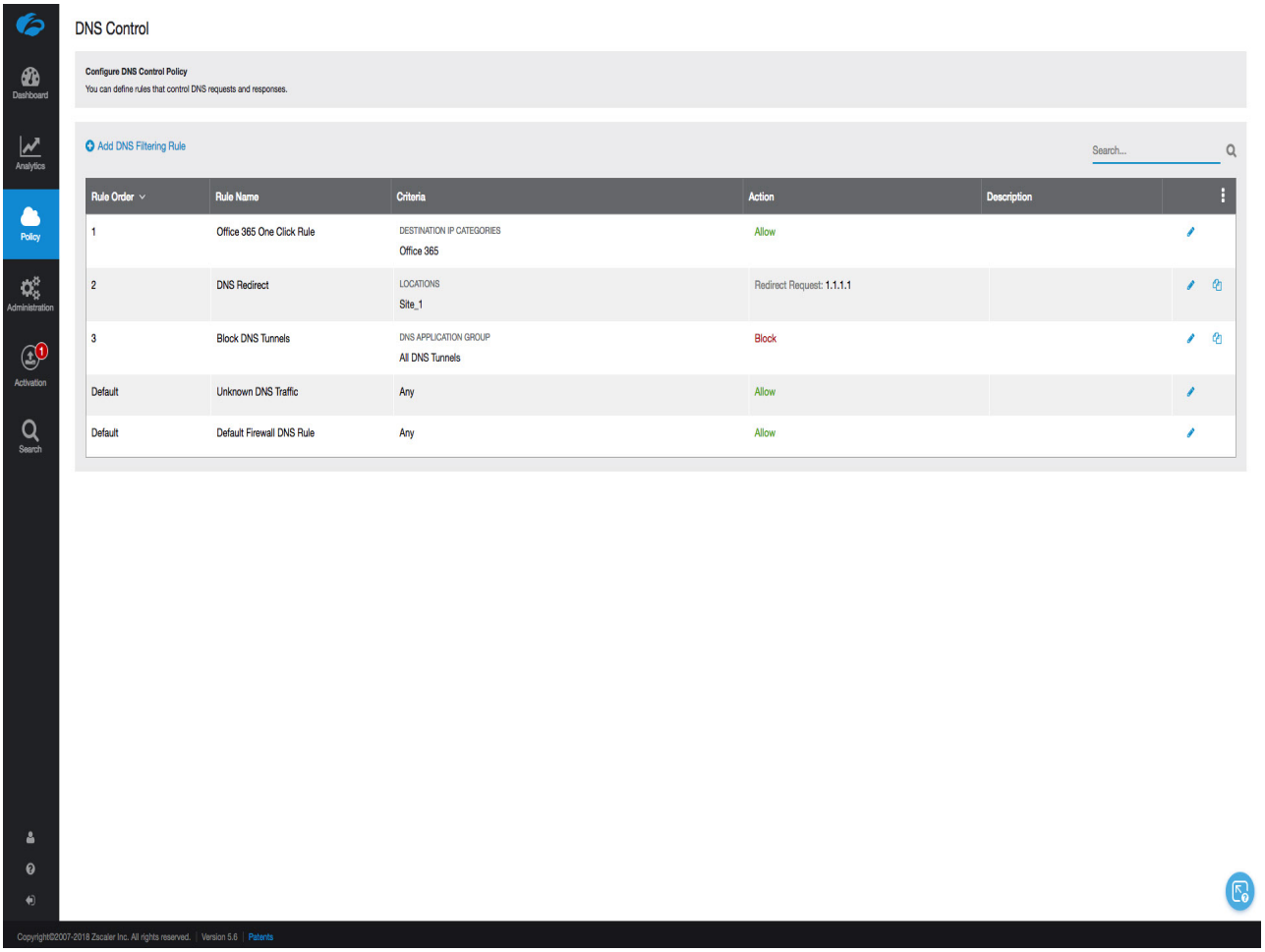
Slide 67 - Slide 67



Slide notes

And **Save** the rule.

Slide 68 - Slide 68

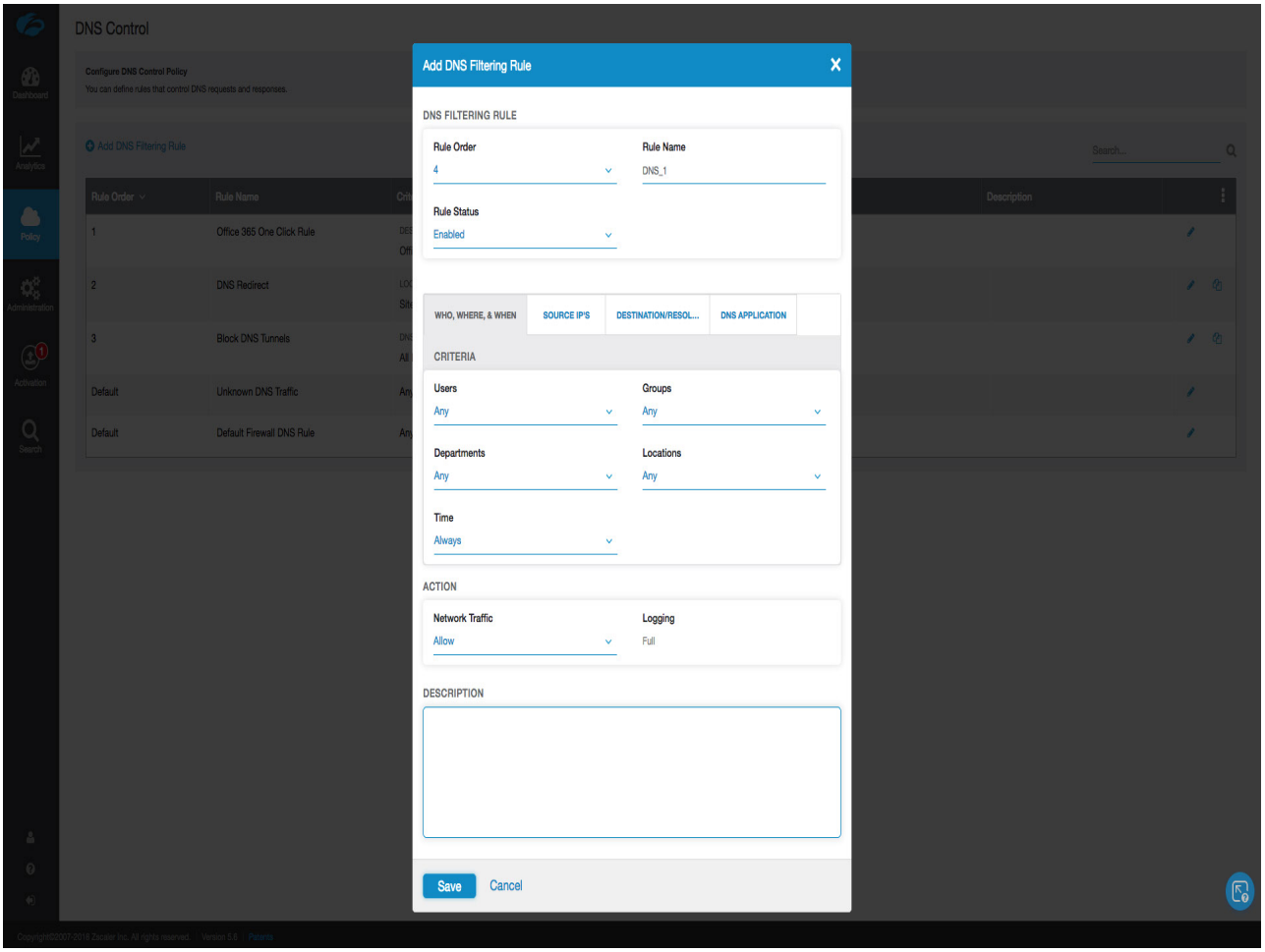


Slide notes

Verify that the rule is added to the list to block all DNS Tunnels.

Next add another DNS Filtering Rule that will go above this rule to permit the DNS tunnels for McAfee and Eset updates.

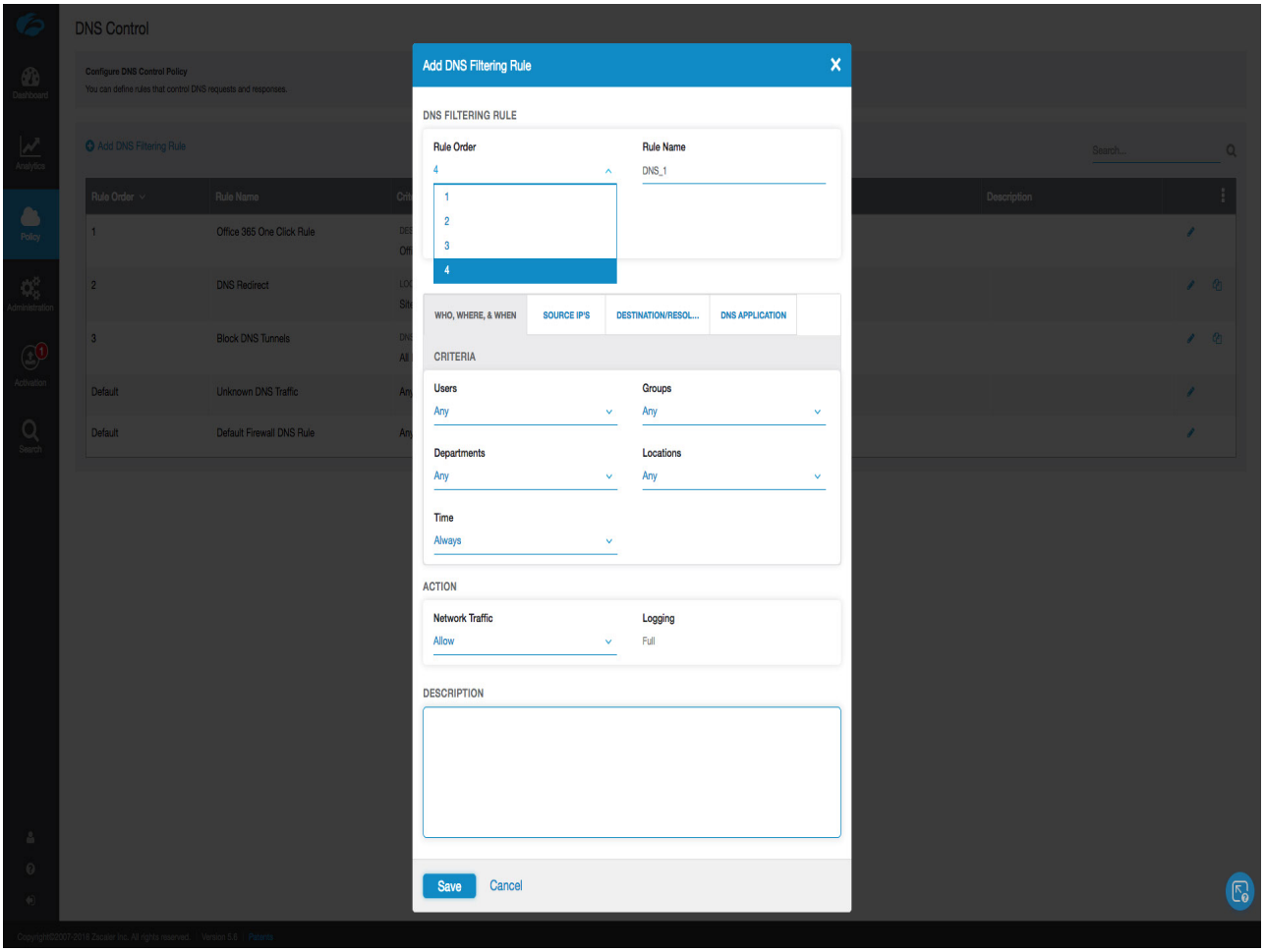
Slide 69 - Slide 69



Slide notes

The system defaults would place to set this new rule at the bottom of the list above the default rules. To place it above the **Block DNS Tunnels** rule, click to change the **Rule Order**.

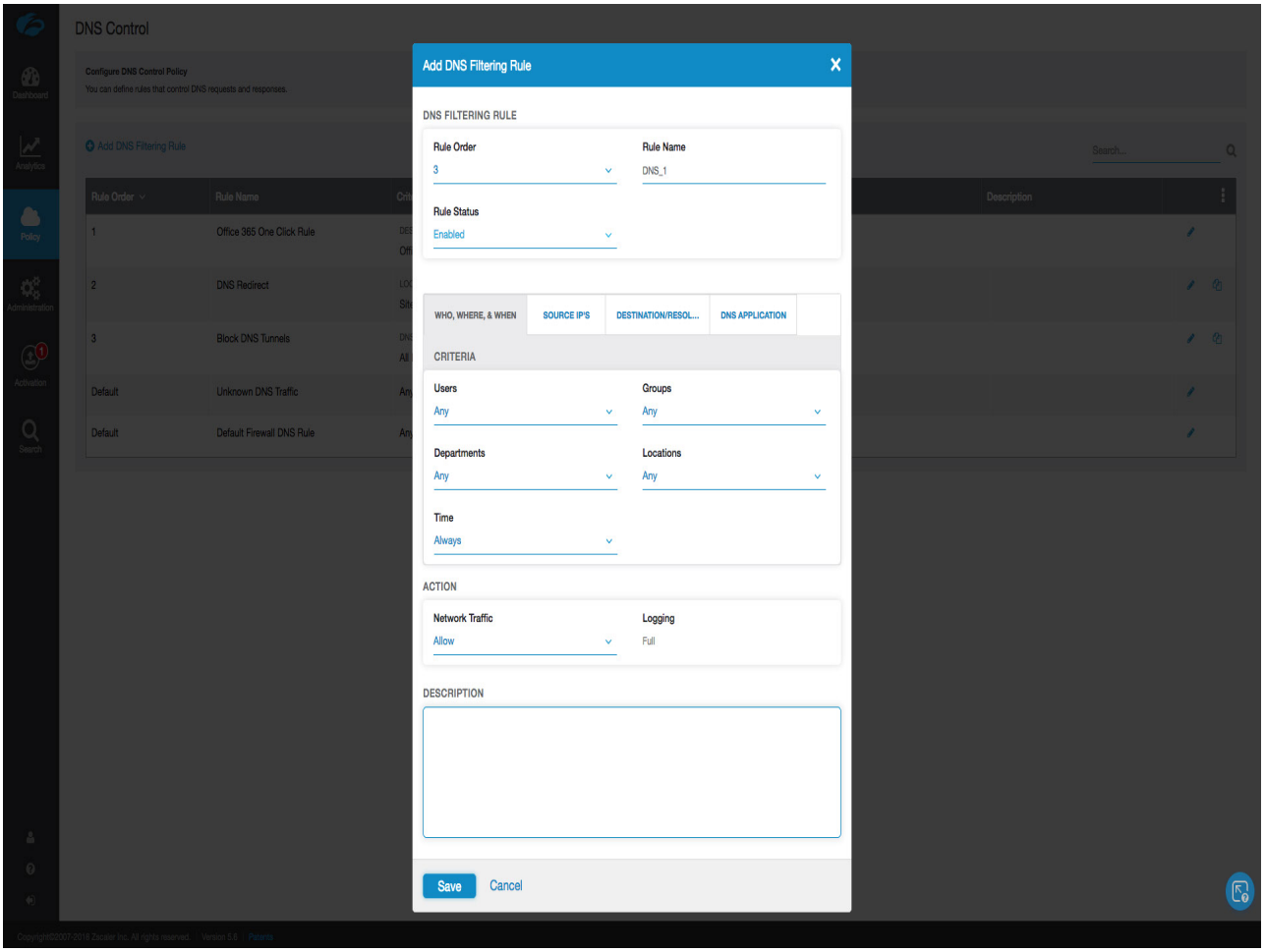
Slide 70 - Slide 70



Slide notes

Select to place this rule in position #**3** which will insert it above the current #3 **Block DNS Tunnels**, which will move to #4.

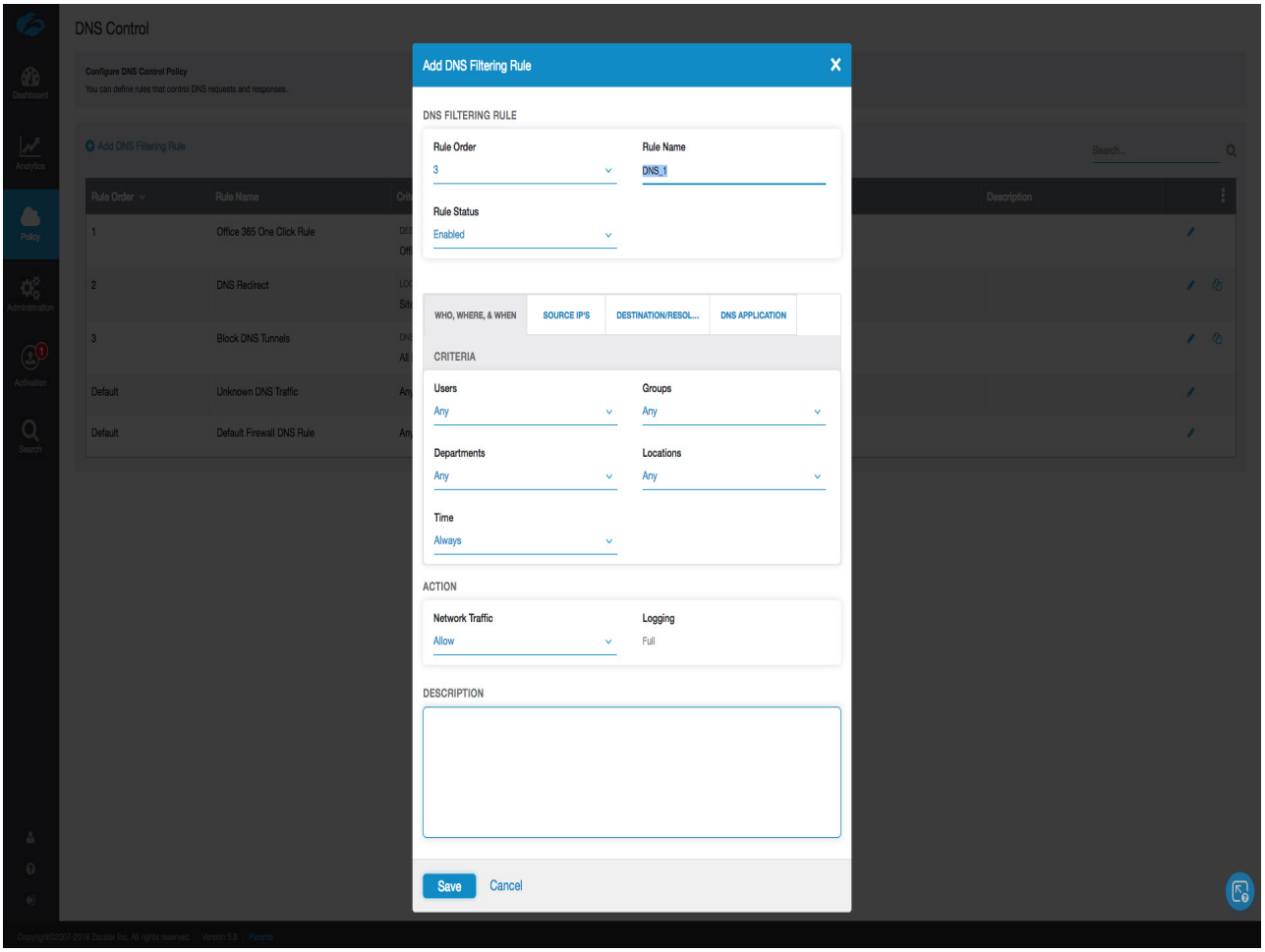
Slide 71 - Slide 71



Slide notes

Double click to select to change the **Rule Name**.

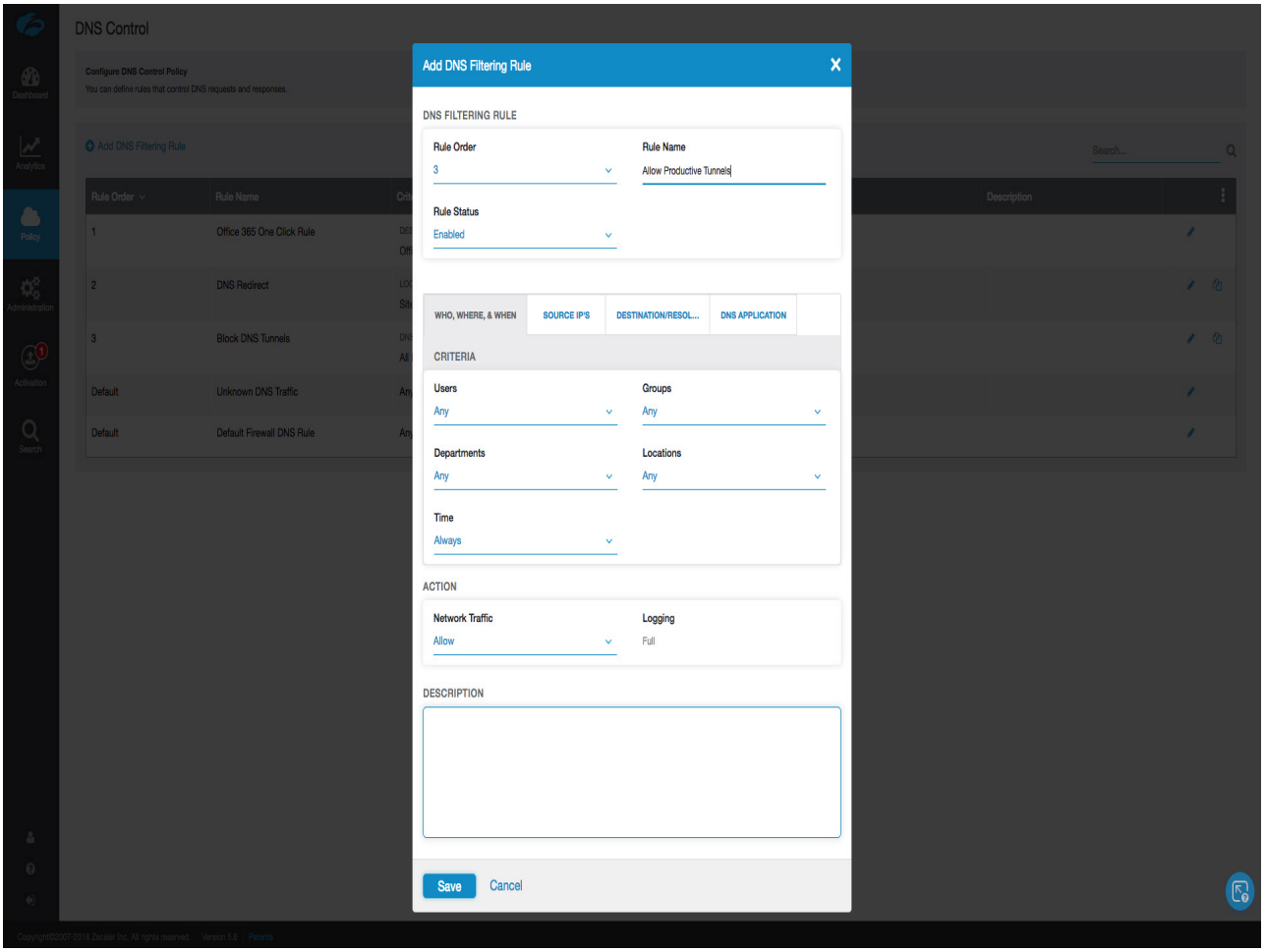
Slide 72 - Slide 72



Slide notes

Type **Allow Productive Tunnels** and hit enter.

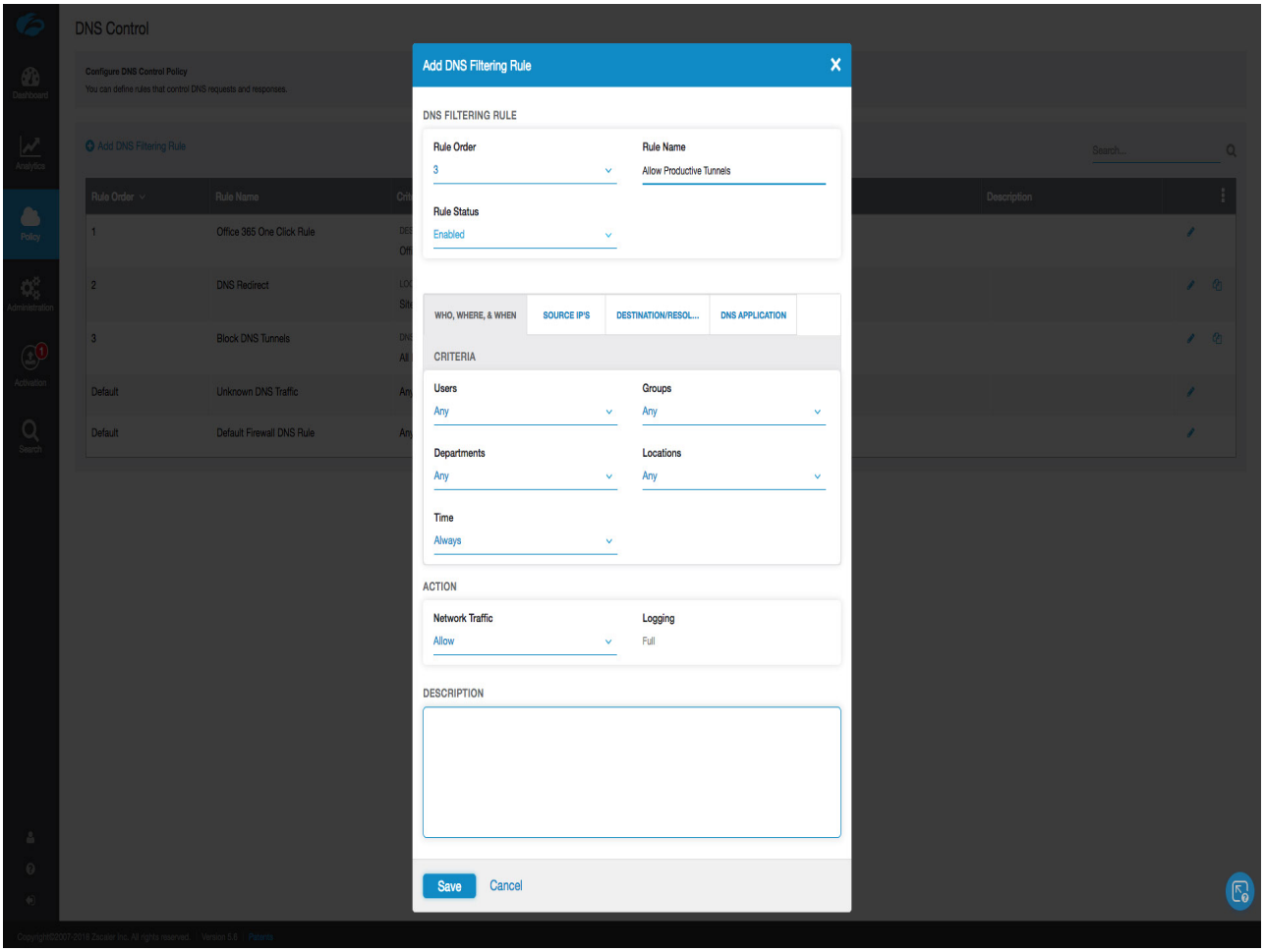
Slide 73 - Slide 73



Slide notes

Similar to the previous rule the default criteria will be used to apply to all users and locations.

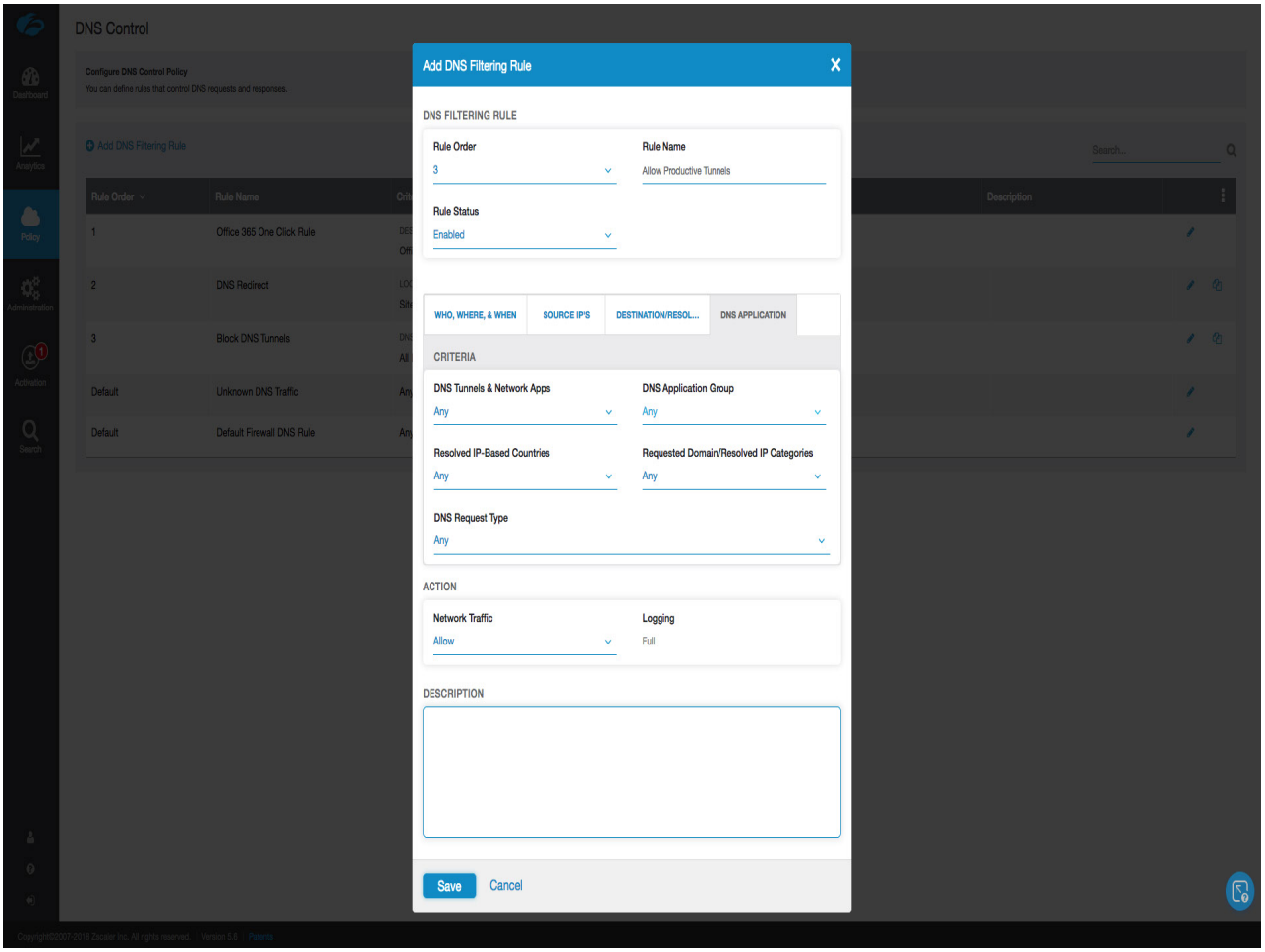
Slide 74 - Slide 74



Slide notes

Click the **DNS APPLICATIONS** to include the permitted DNS tunnels.

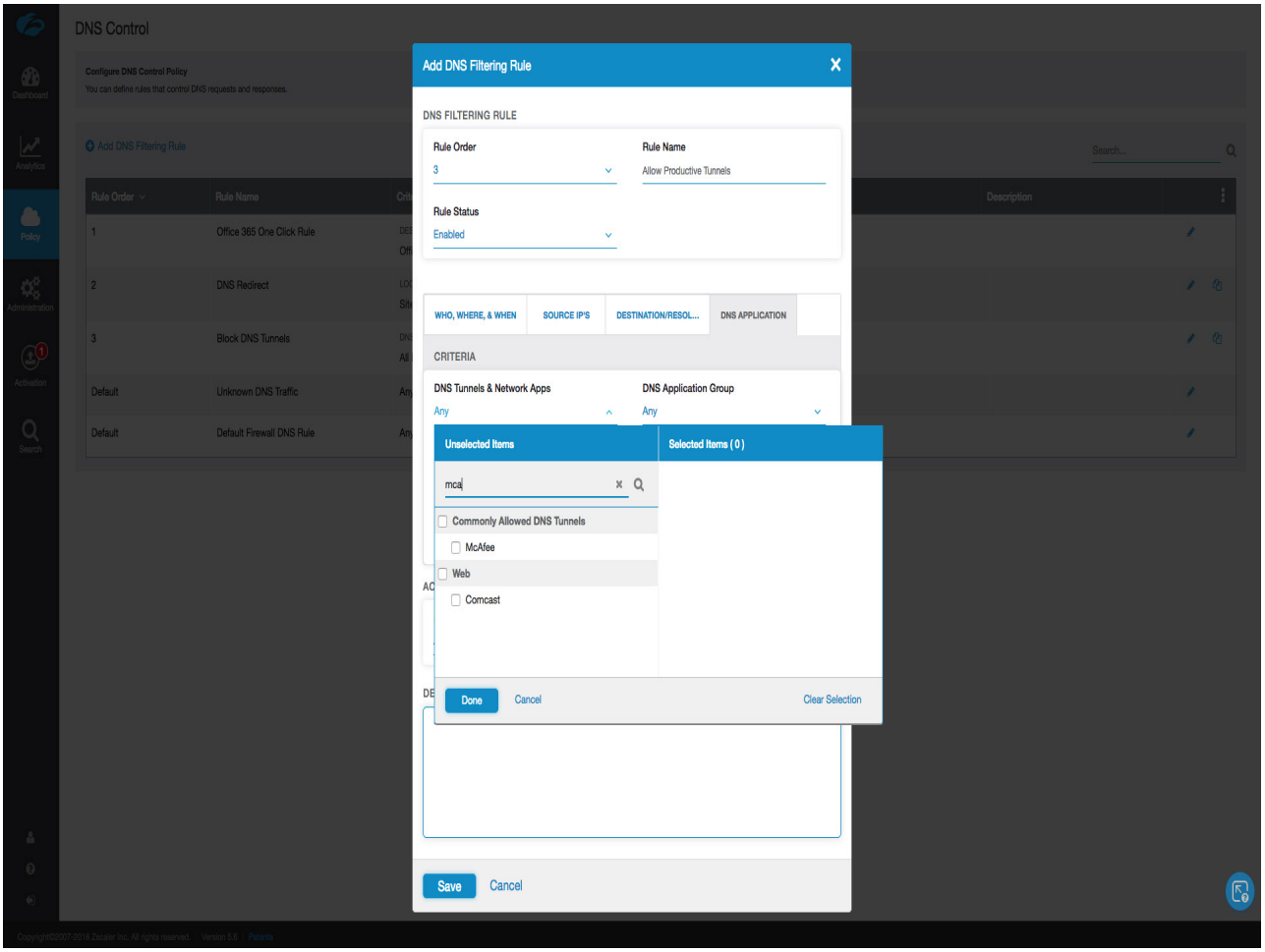
Slide 75 - Slide 75



Slide notes

The two tunnels to allow could be added by creating another **DNS Application Group**, or in this example they will be included individually from the **DNS Tunnels and Network Apps** list**.**

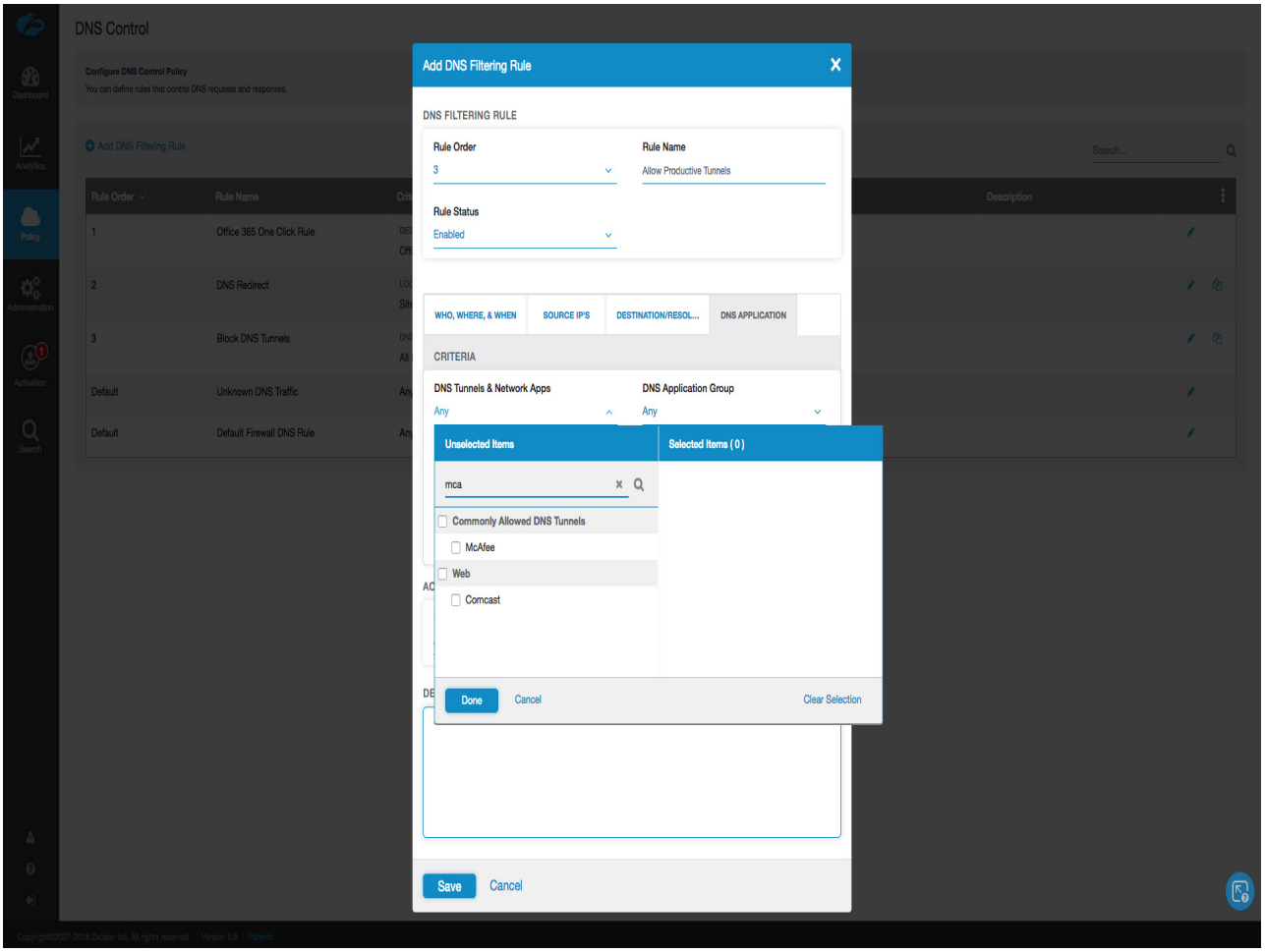
Slide 76 - Slide 76



Slide notes

The selection dialog box includes a search field for quickly locating specific items in the list. As the first few letters of McAfee are typed the list will filter to show matching items.

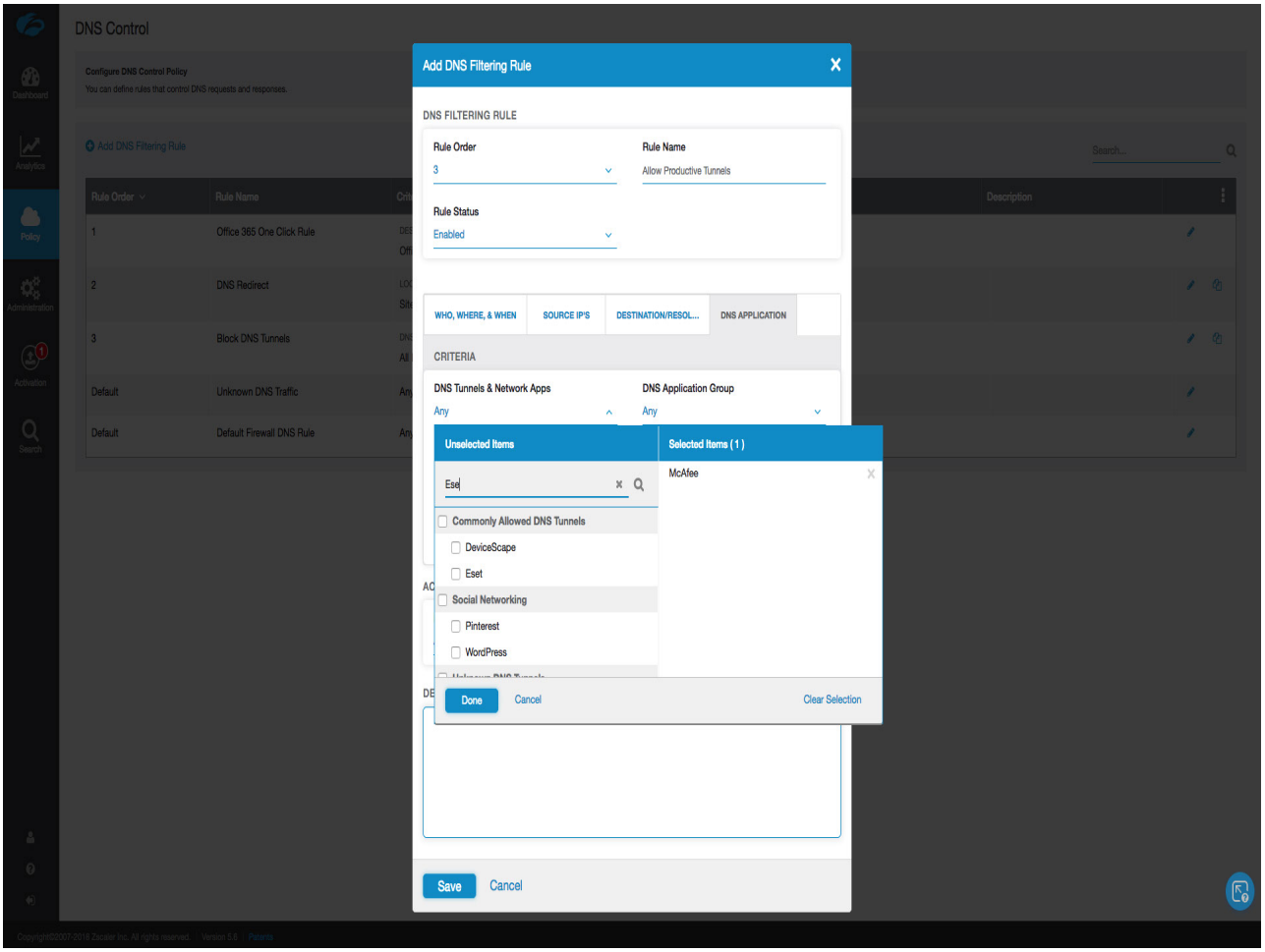
Slide 77 - Slide 77



Slide notes

Click to include **McAfee**

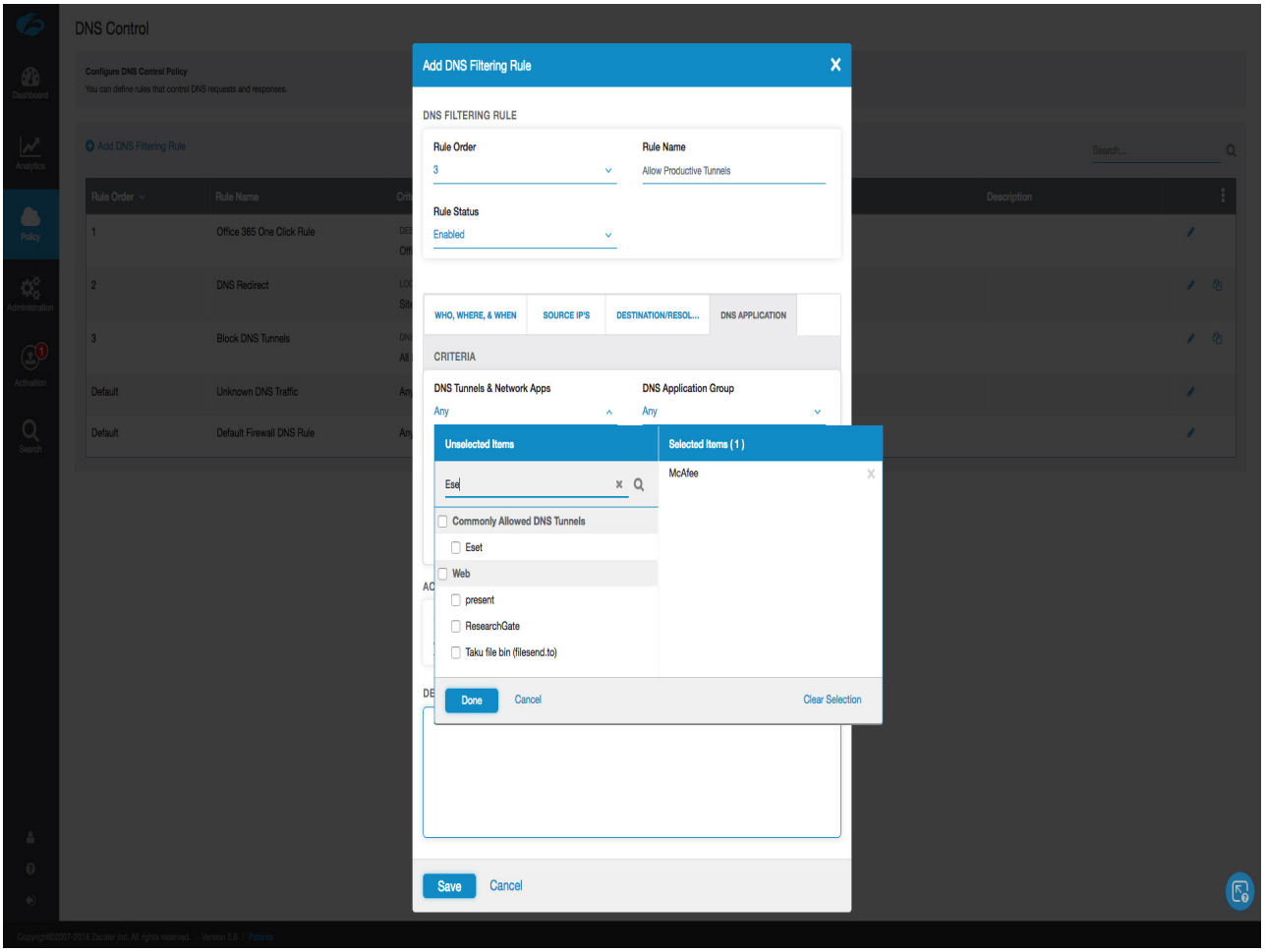
Slide 78 - Slide 78



Slide notes

Similarly the **Eset** tunnel may be found.

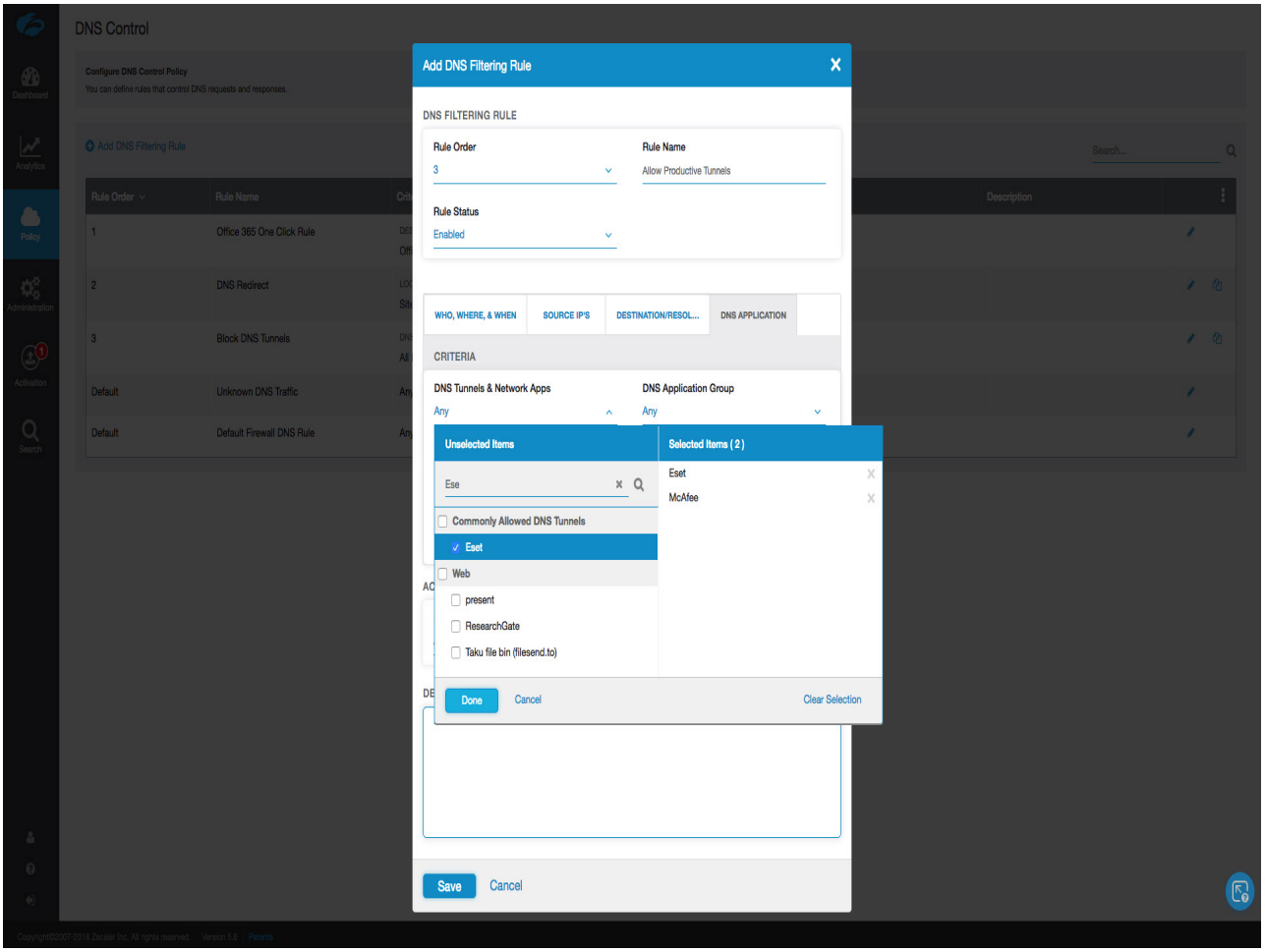
Slide 79 - Slide 79



Slide notes

Click to add **Eset** to the selected items for this rule.

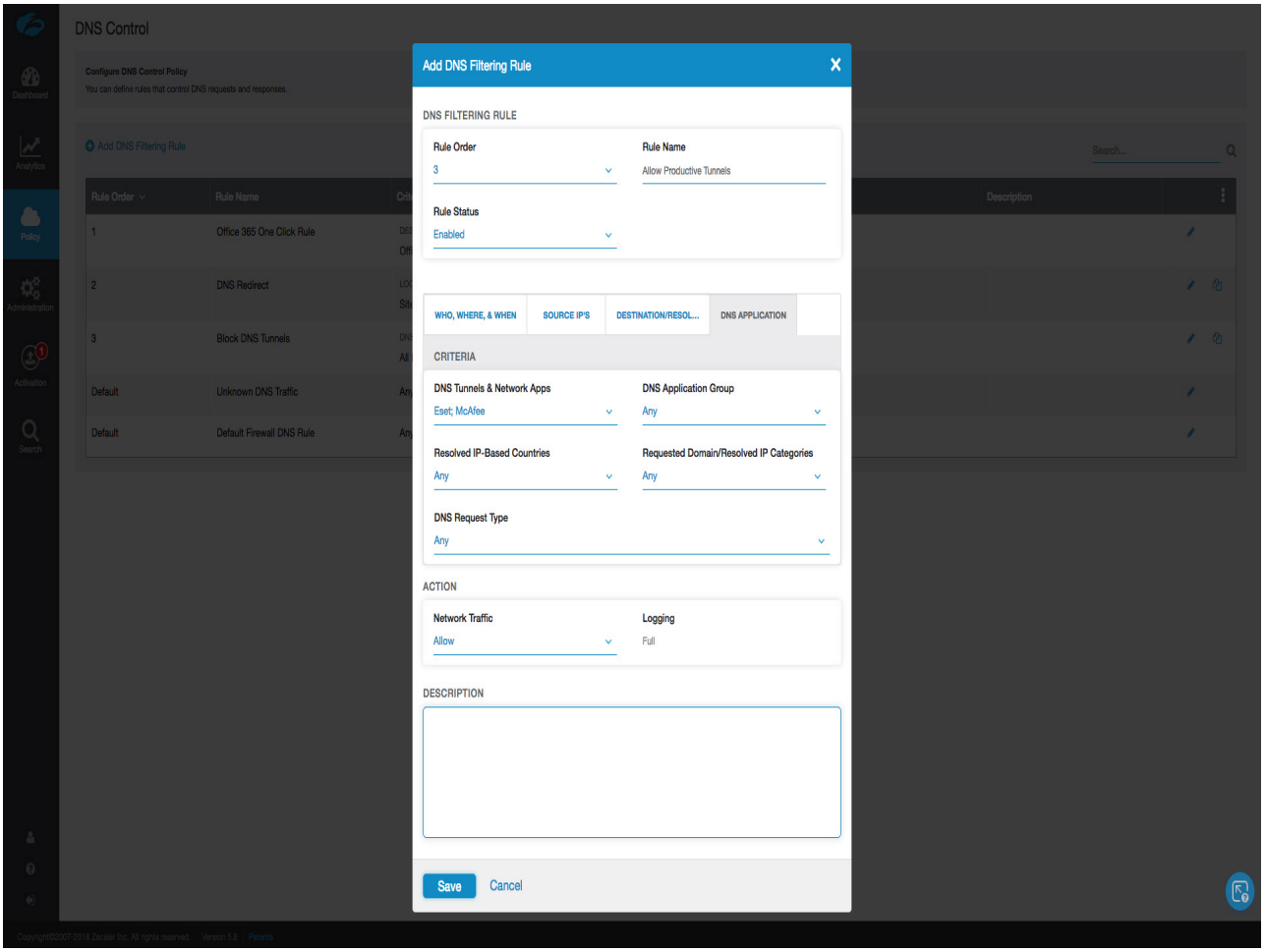
Slide 80 - Slide 80



Slide notes

Click **Done** to save the two selected tunnel items.

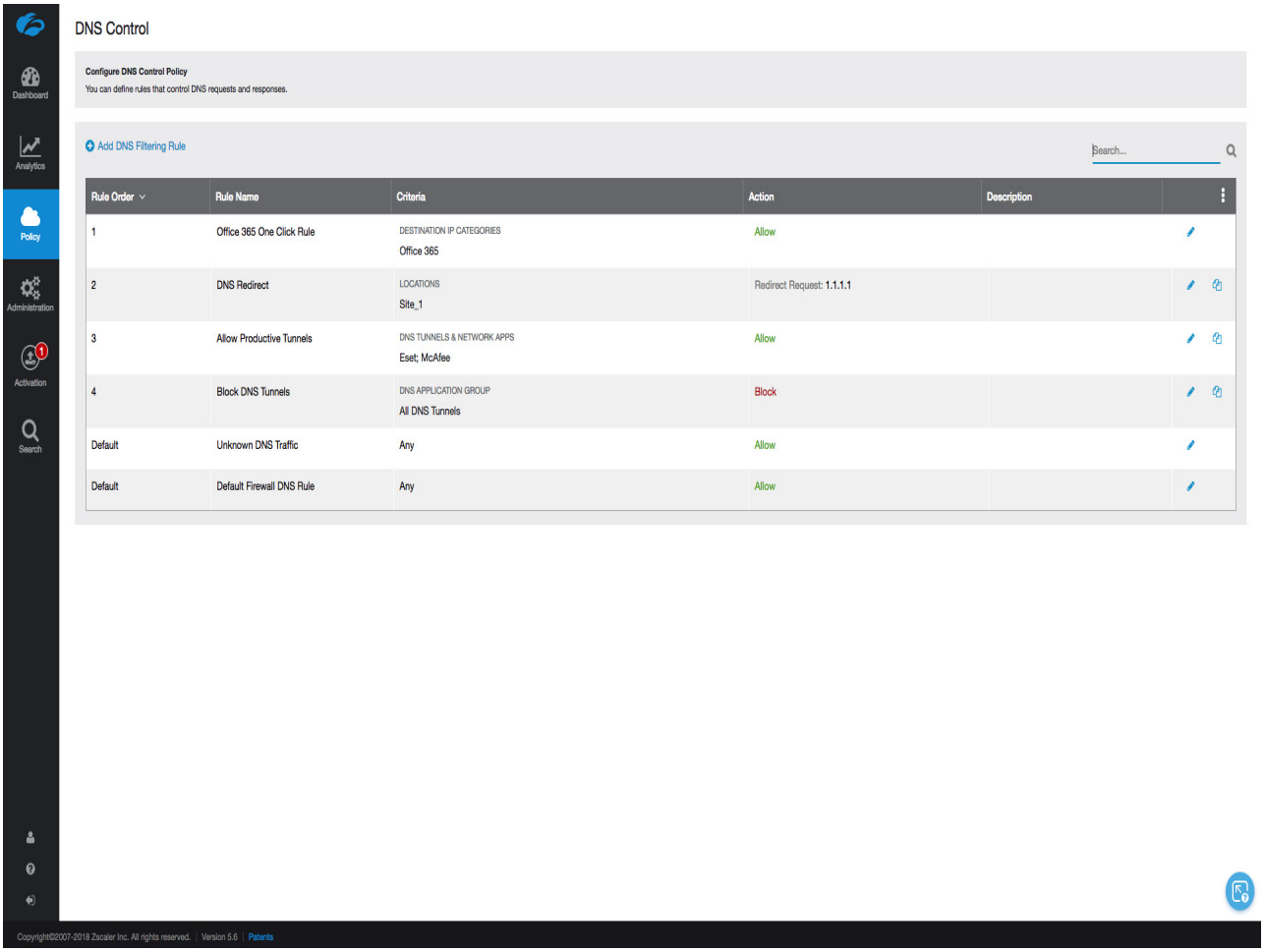
Slide 81 - Slide 81



Slide notes

Allow is set as the default action. Click to **Save** the rule.

Slide 82 - Slide 82

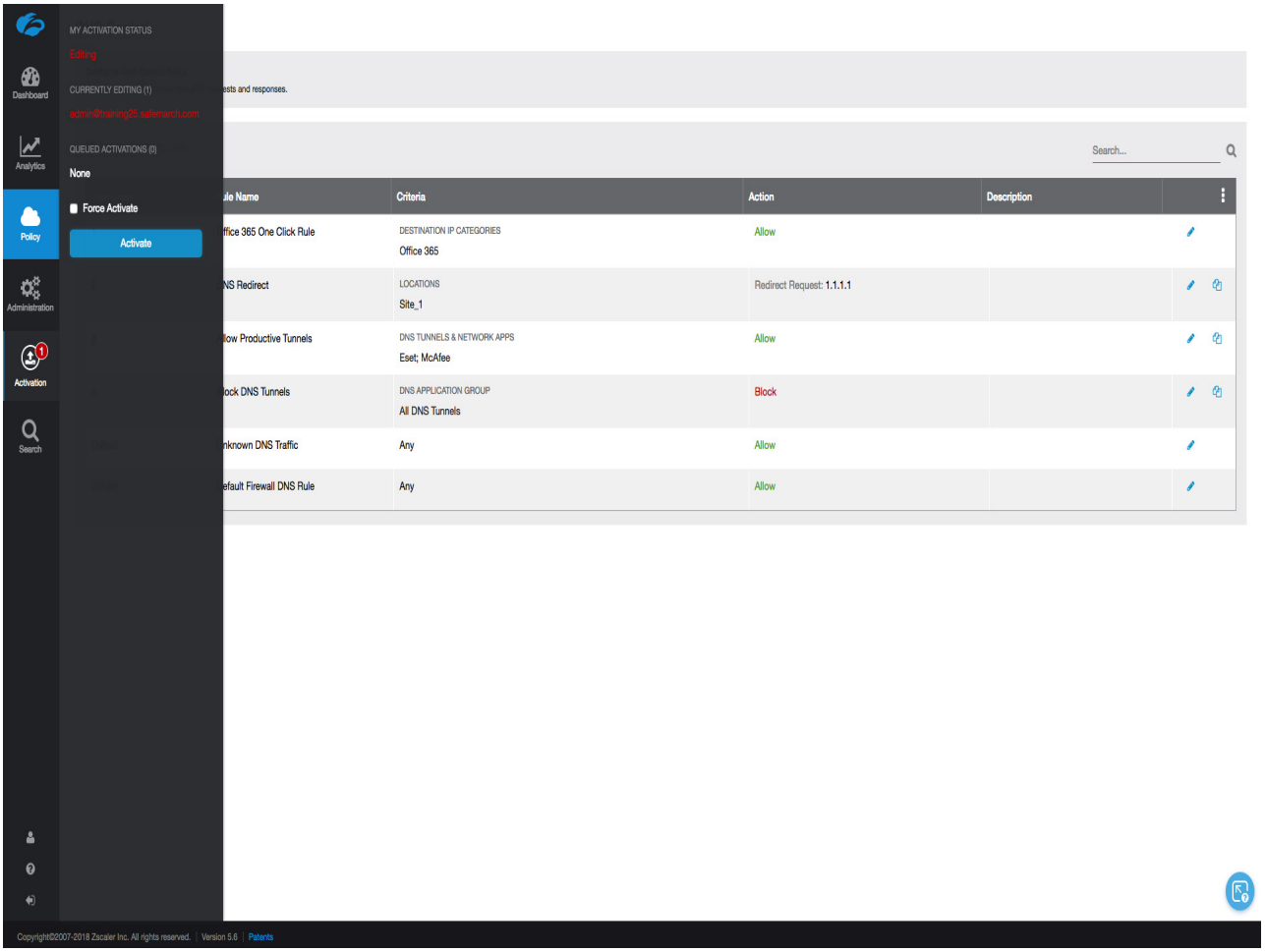


Slide notes

Verify that the **Allow Productive Tunnels** rule has been added in the list above the **Block DNS Tunnels** rule. In this order any McAfee or Eset DNS tunnels will match rule #3 and be allowed. All other DNS tunnels will match rule #4 so will be blocked.

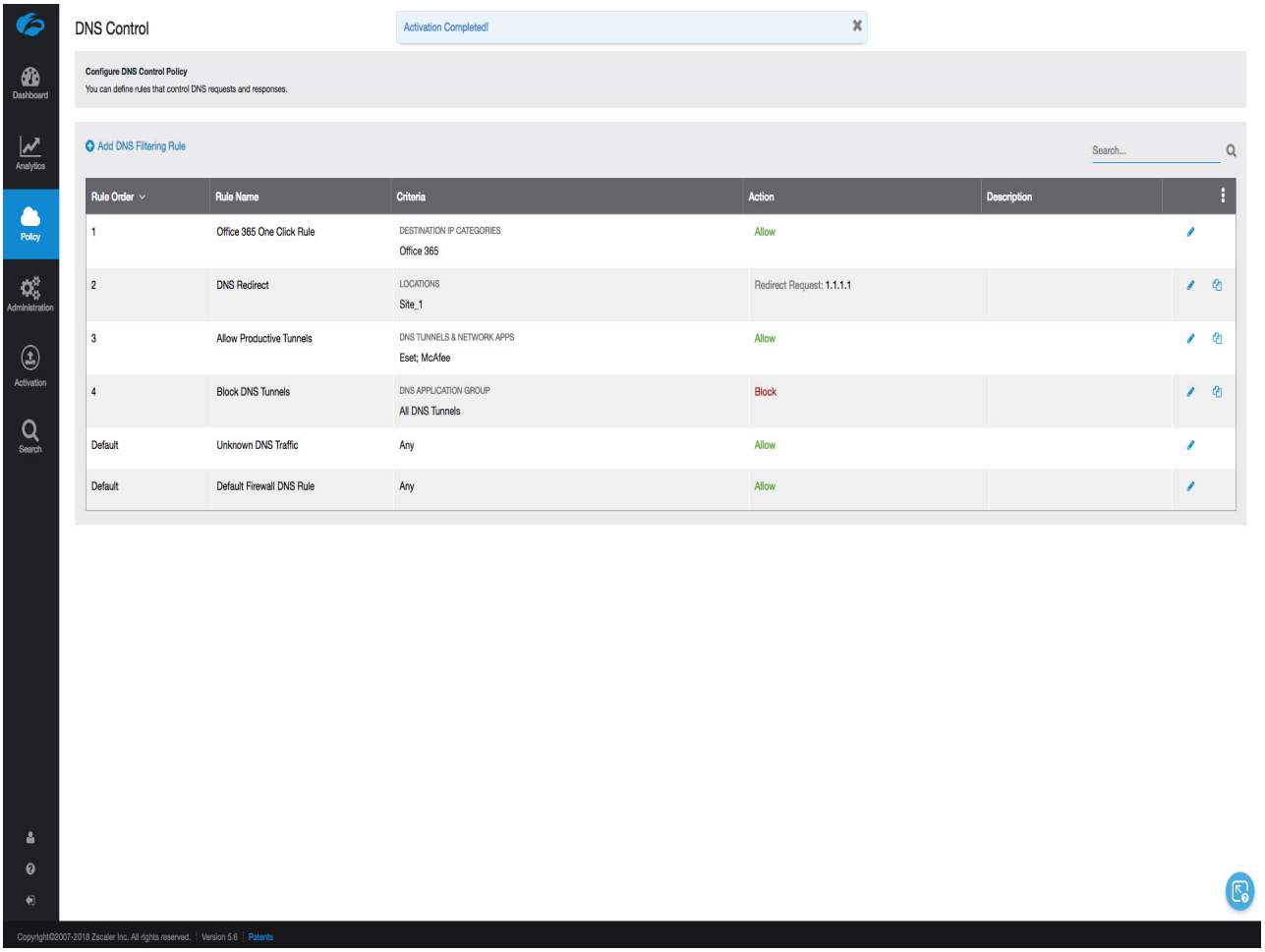
Activate the changes.

Slide 83 - Slide 83



Slide notes

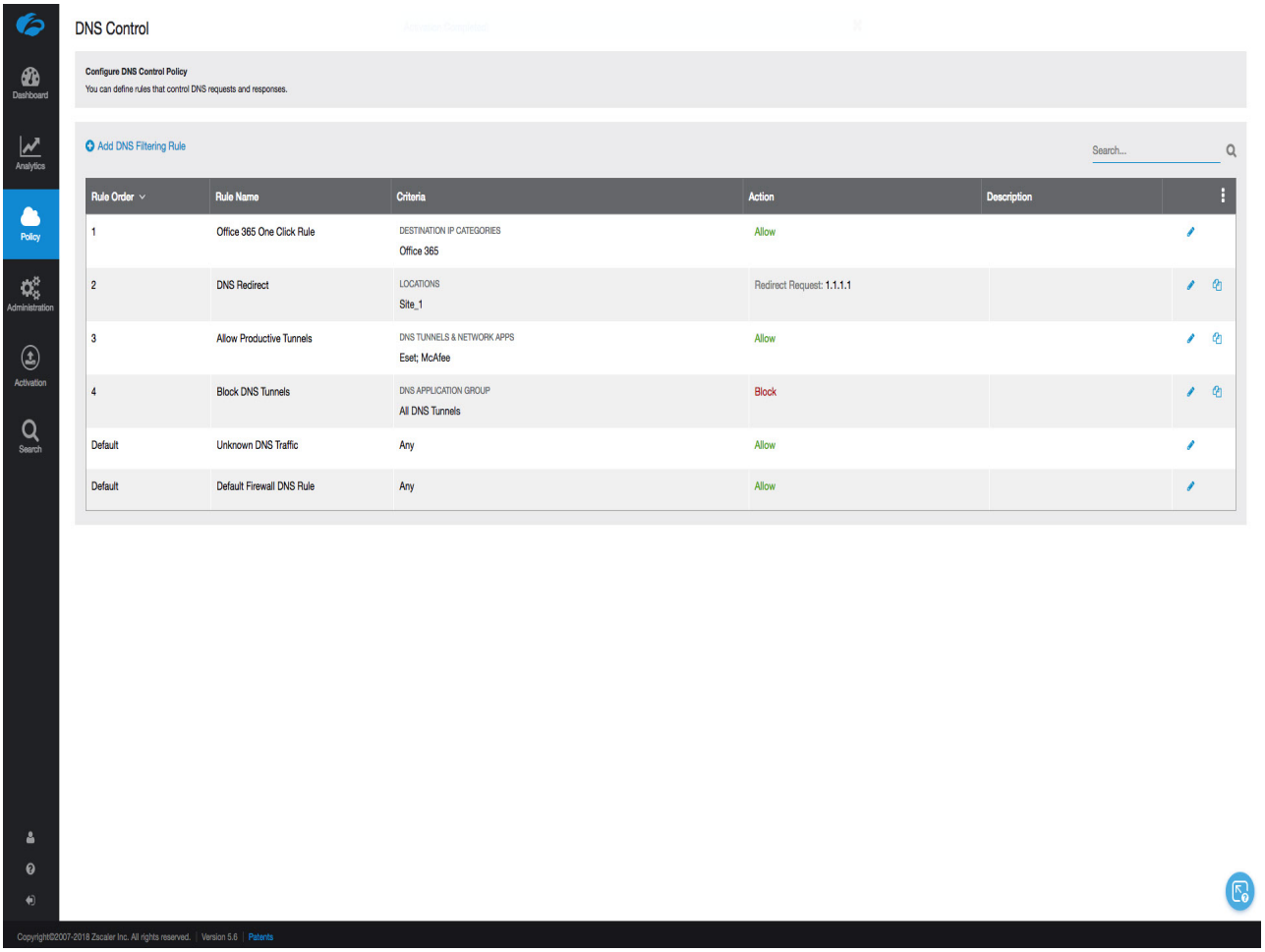
Slide 84 - Slide 84



Slide notes

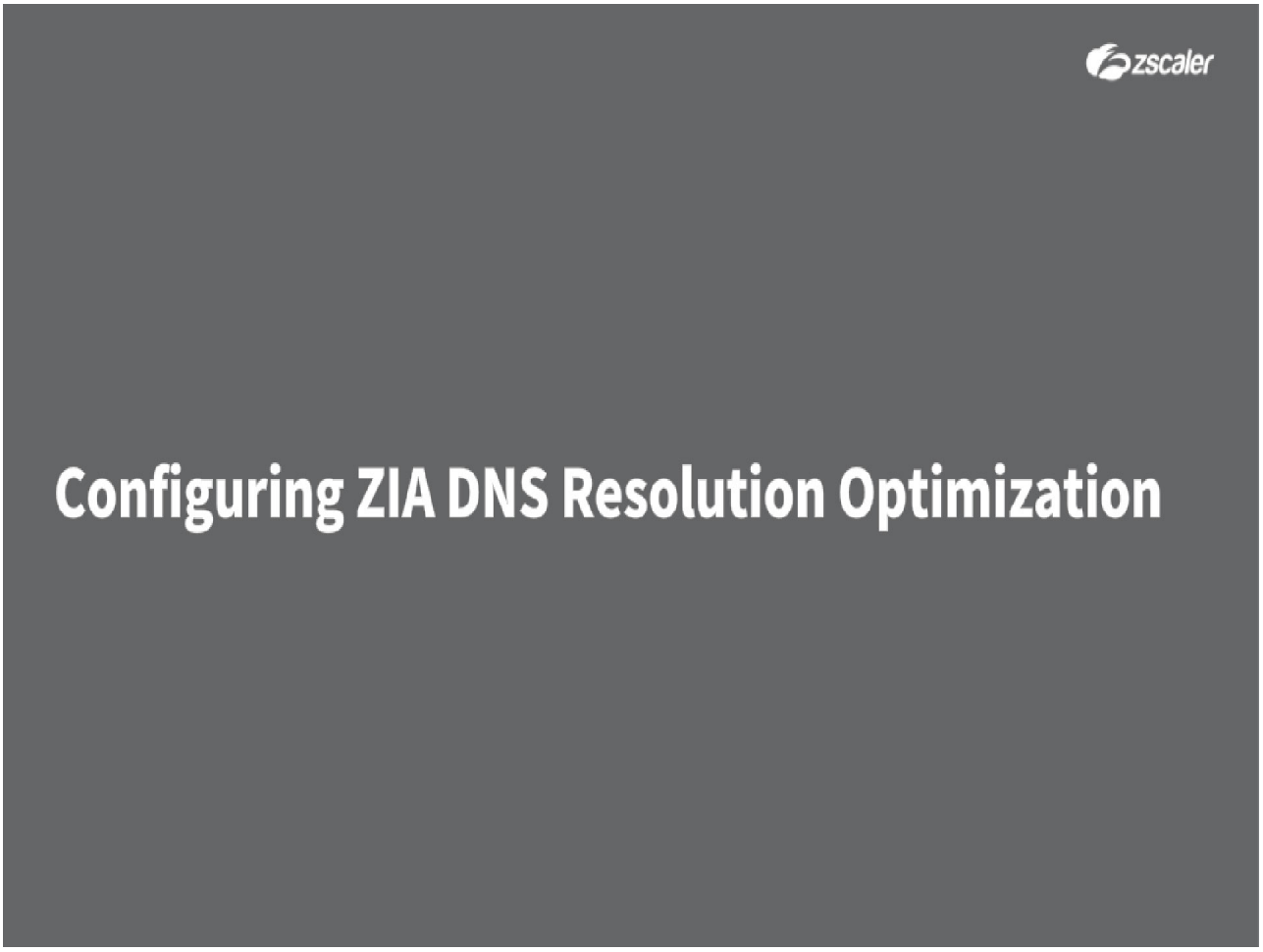
Now that the DNS rules are active, their enforcement may be verified as shown in the previous task for examining the **DNS Insights** log **Analytics** data.

Slide 85 - Slide 85



Slide notes

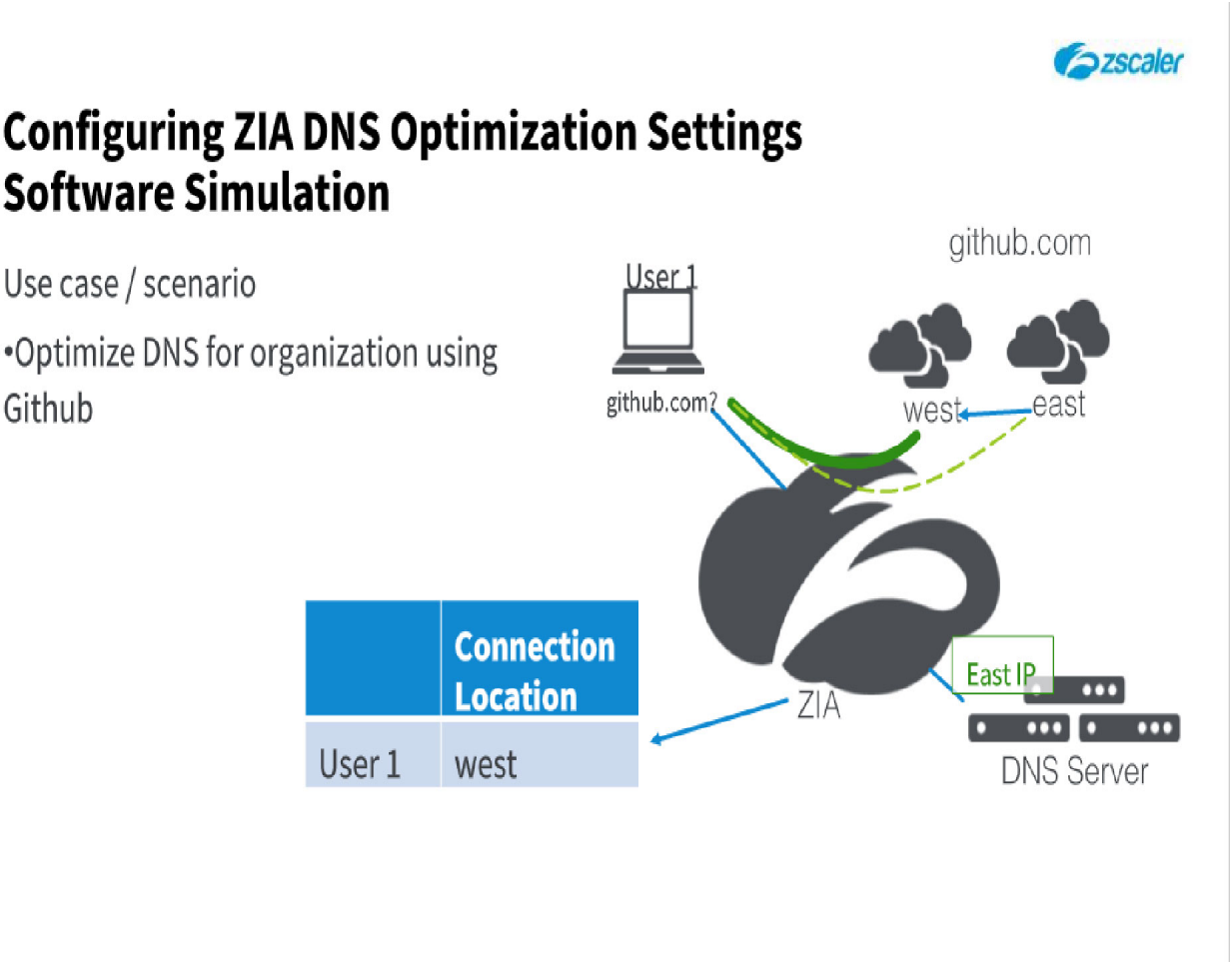
Slide 86 - Configuring ZIA DNS Resolution Optimization



Slide notes

In this task you will configure ZIA for DNS Resolution Optimization.

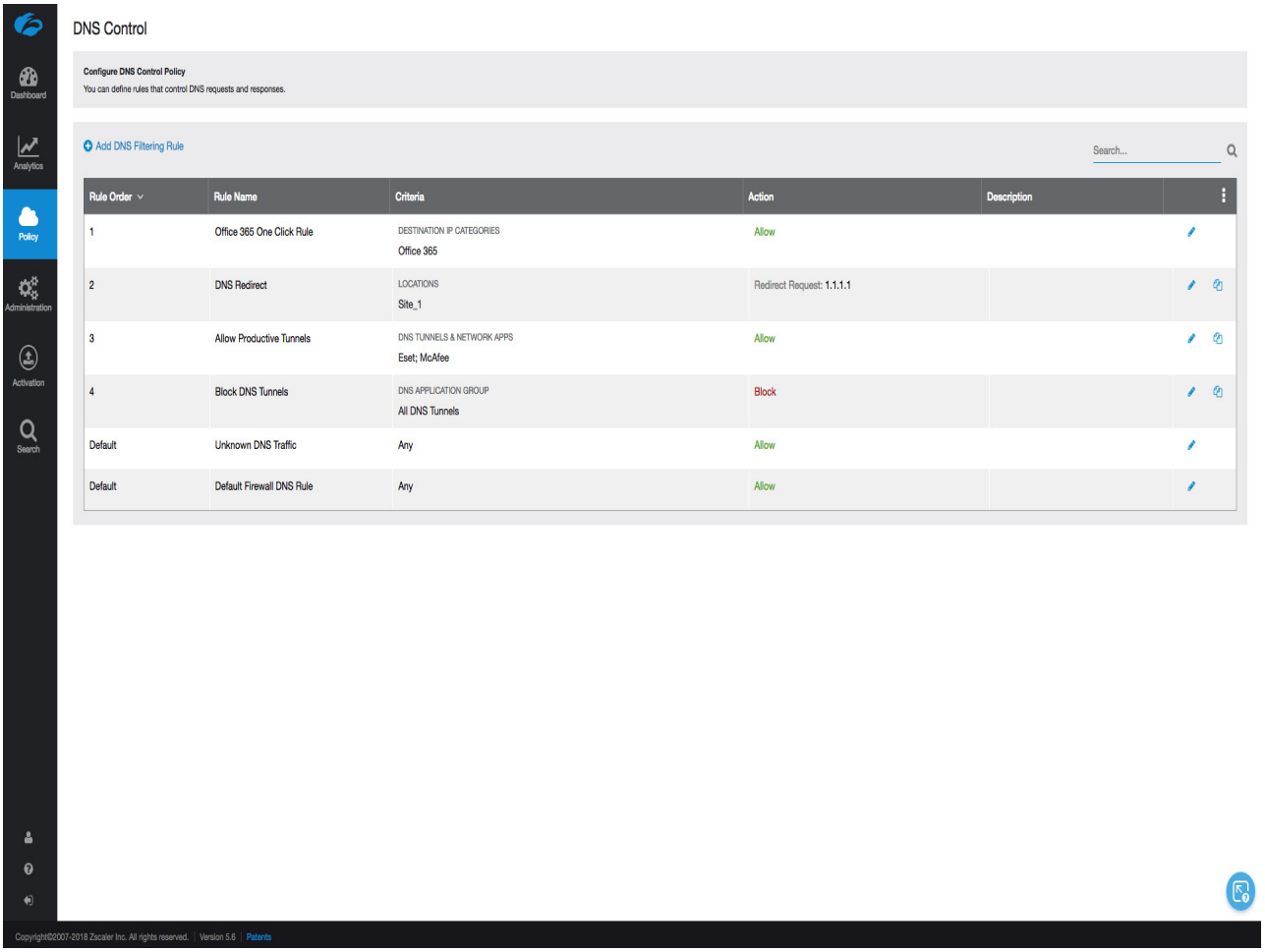
Slide 87 - Configuring ZIA DNS Optimization Settings Software Simulation



Slide notes

Consider the scenario where an organization is using Github. DNS resolution is not setup to take geolocation into consideration. Users in the west end up connected to Github servers in the east. ZIA needs to improve on this by using its awareness of where the user is connecting to the cloud and updating the results to direct the client to a closer server. You will configure ZIA to optimize the DNS resolution for Github. You will enable DNS Resolution Optimization and configure the settings to optimize for the Github Cloud Application.
To configure DNS Resolution Optimization, follow these steps:

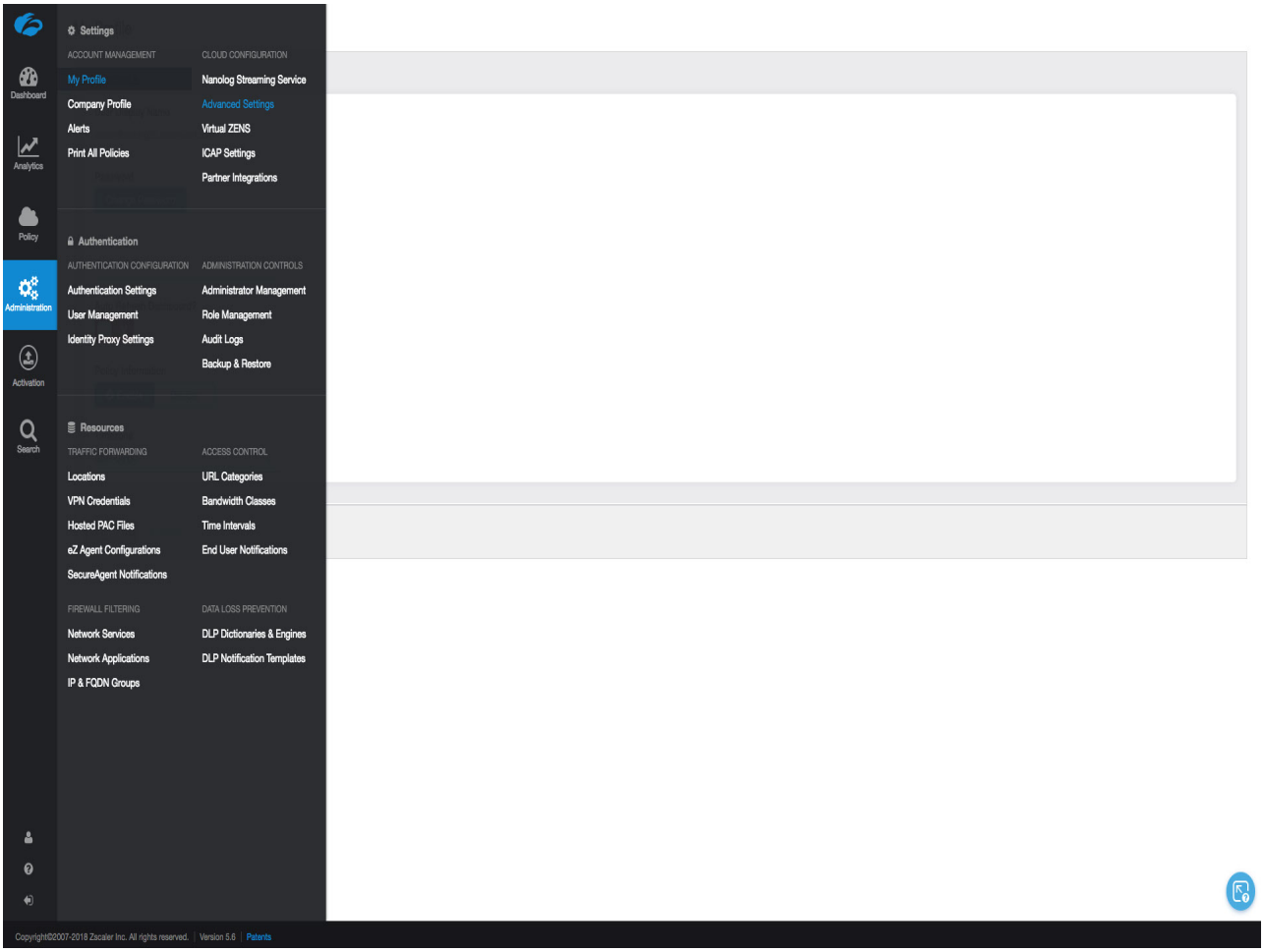
Slide 88 - Slide 88



Slide notes

Click to select the **Administration** menu.

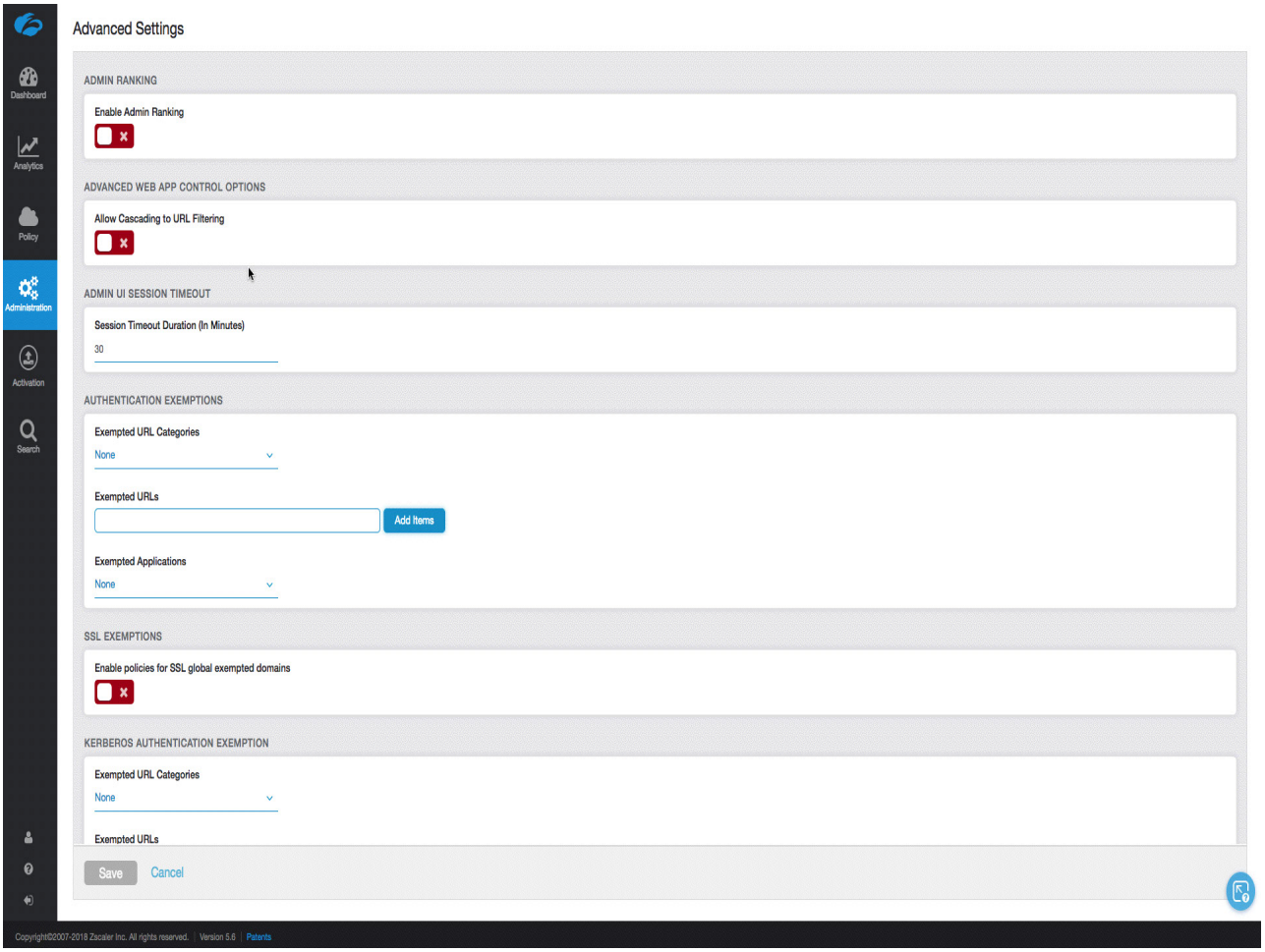
Slide 89 - Slide 89



Slide notes

Select **Advanced Settings** in the **Cloud Configuration** group of the **Settings** sub-menu.

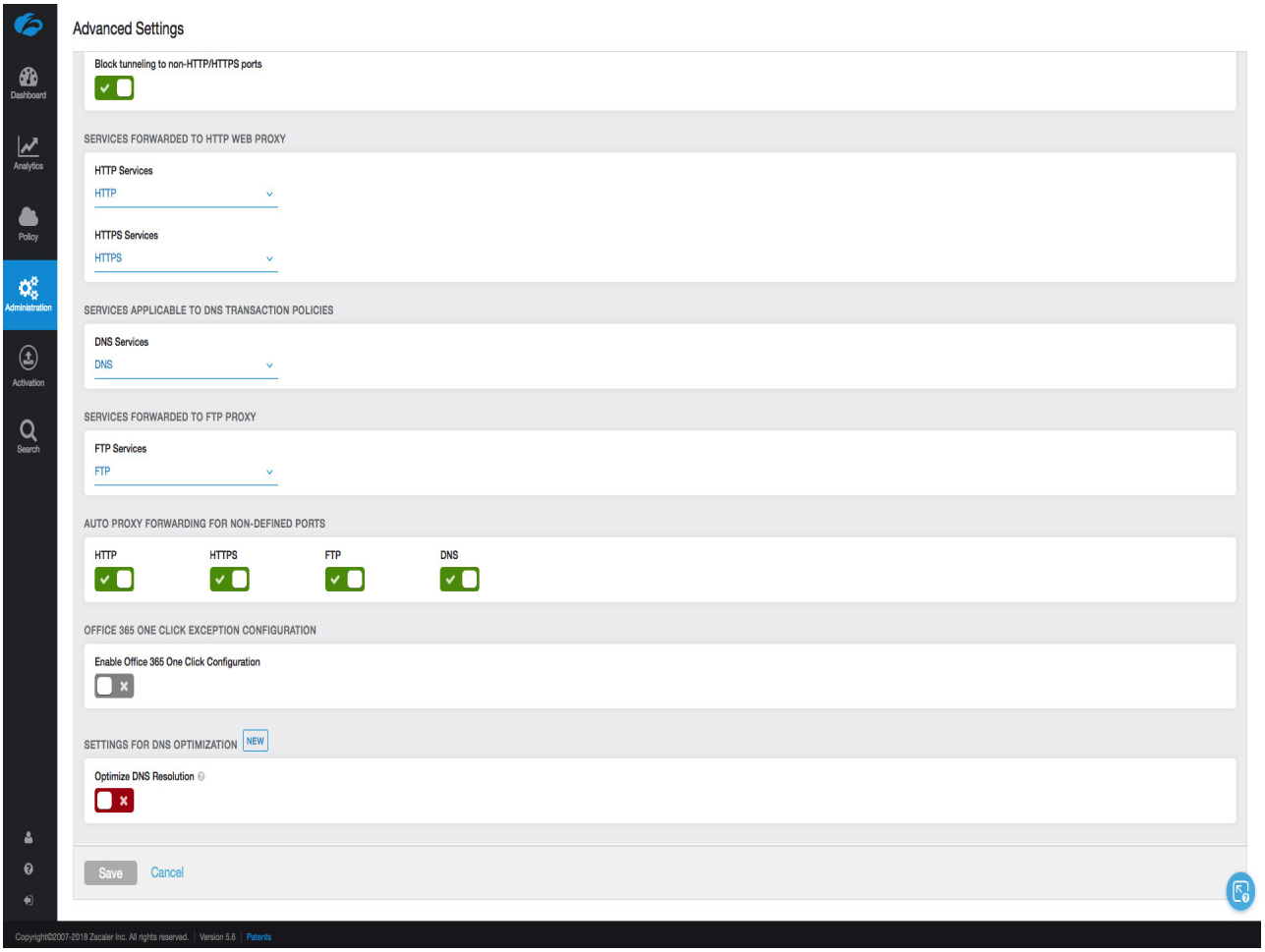
Slide 90 - Slide 90



Slide notes

It may be needed to scroll to locate the **Settings for DNS Optimization**.

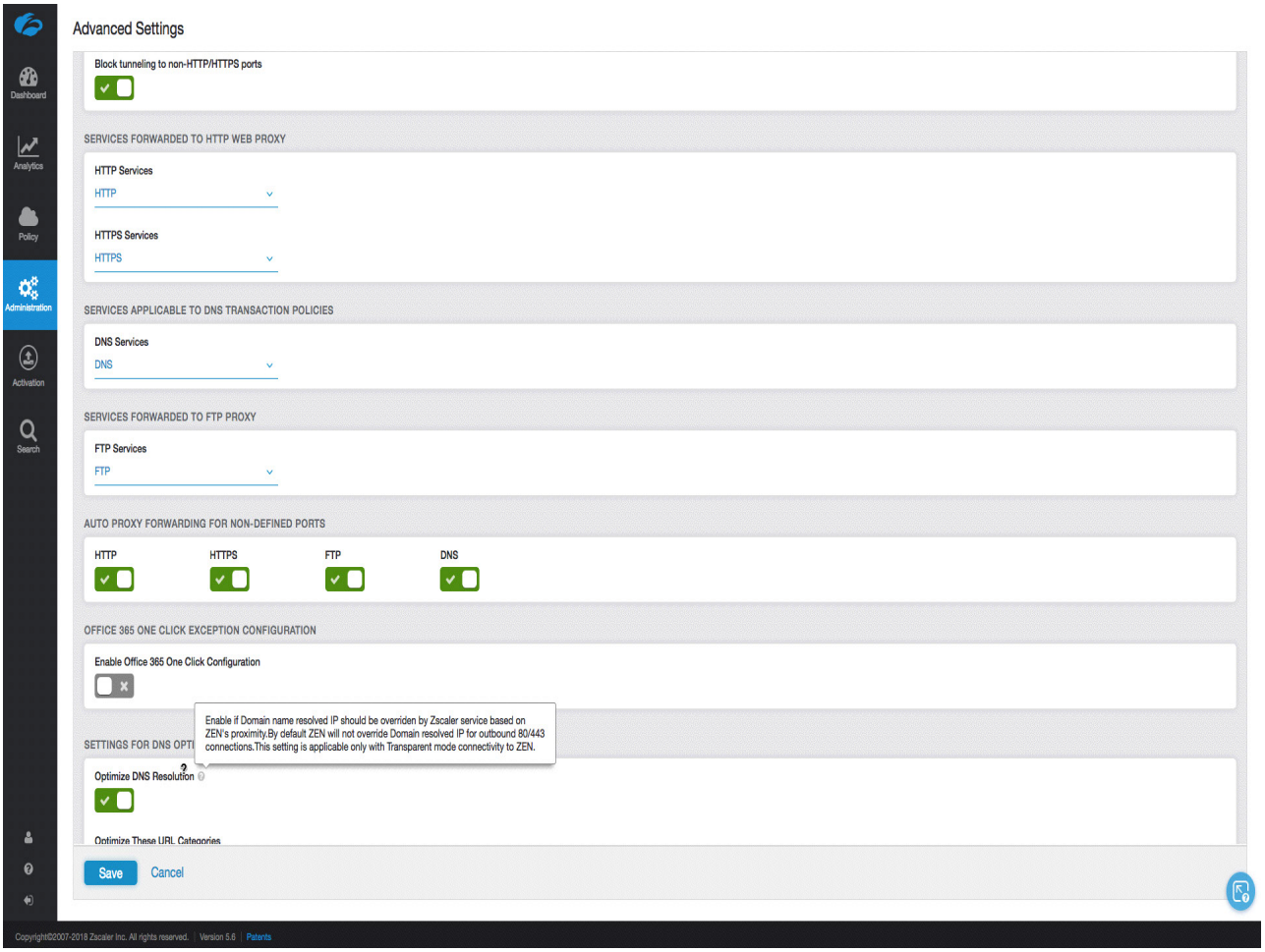
Slide 91 - Slide 91



Slide notes

Enable **Optimize DNS Resolution**.

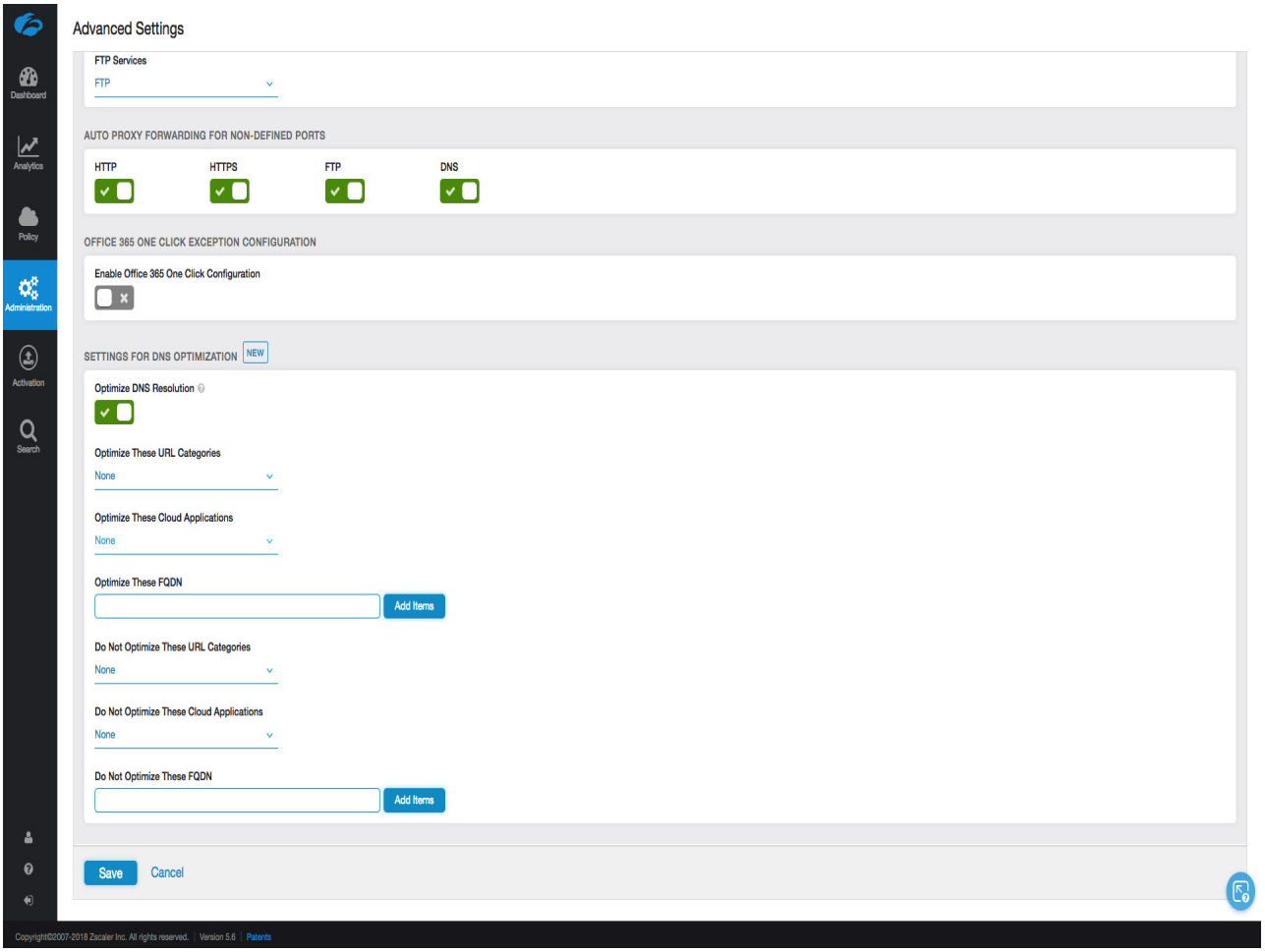
Slide 92 - Slide 92



Slide notes

And scroll as needed to view the detailed **Settings for DNS Optimization**.

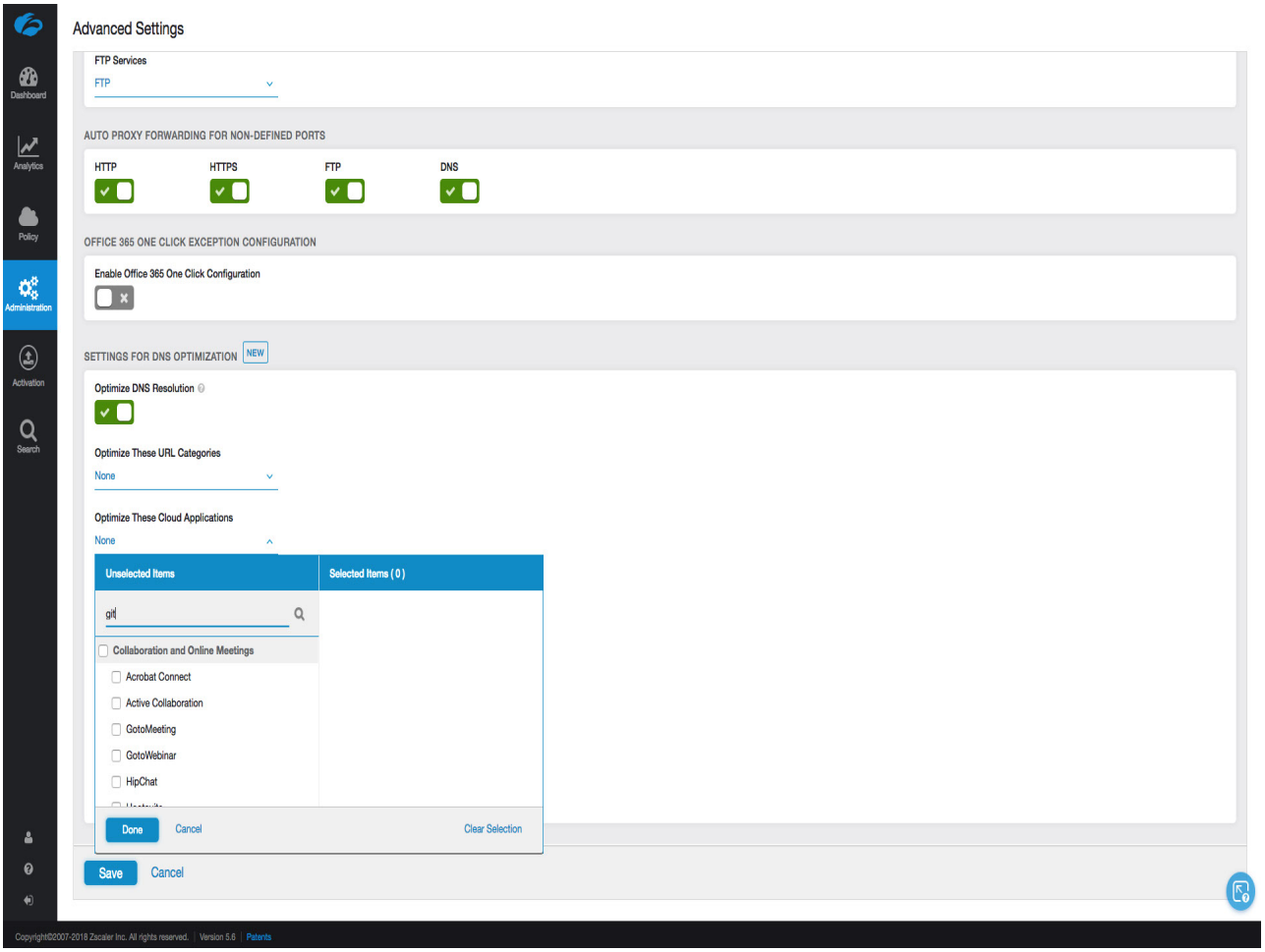
Slide 93 - Slide 93



Slide notes

URL Categories, **Cloud Applications**, and Fully Qualified Domain Names (**FQDN**) may be configured in the **Optimize These** lists**.**
Exclusions may be configured in the corresponding **Do Not Optimize** lists.
In this example select to include **Github** in the **Optimize These Cloud Applications** list.

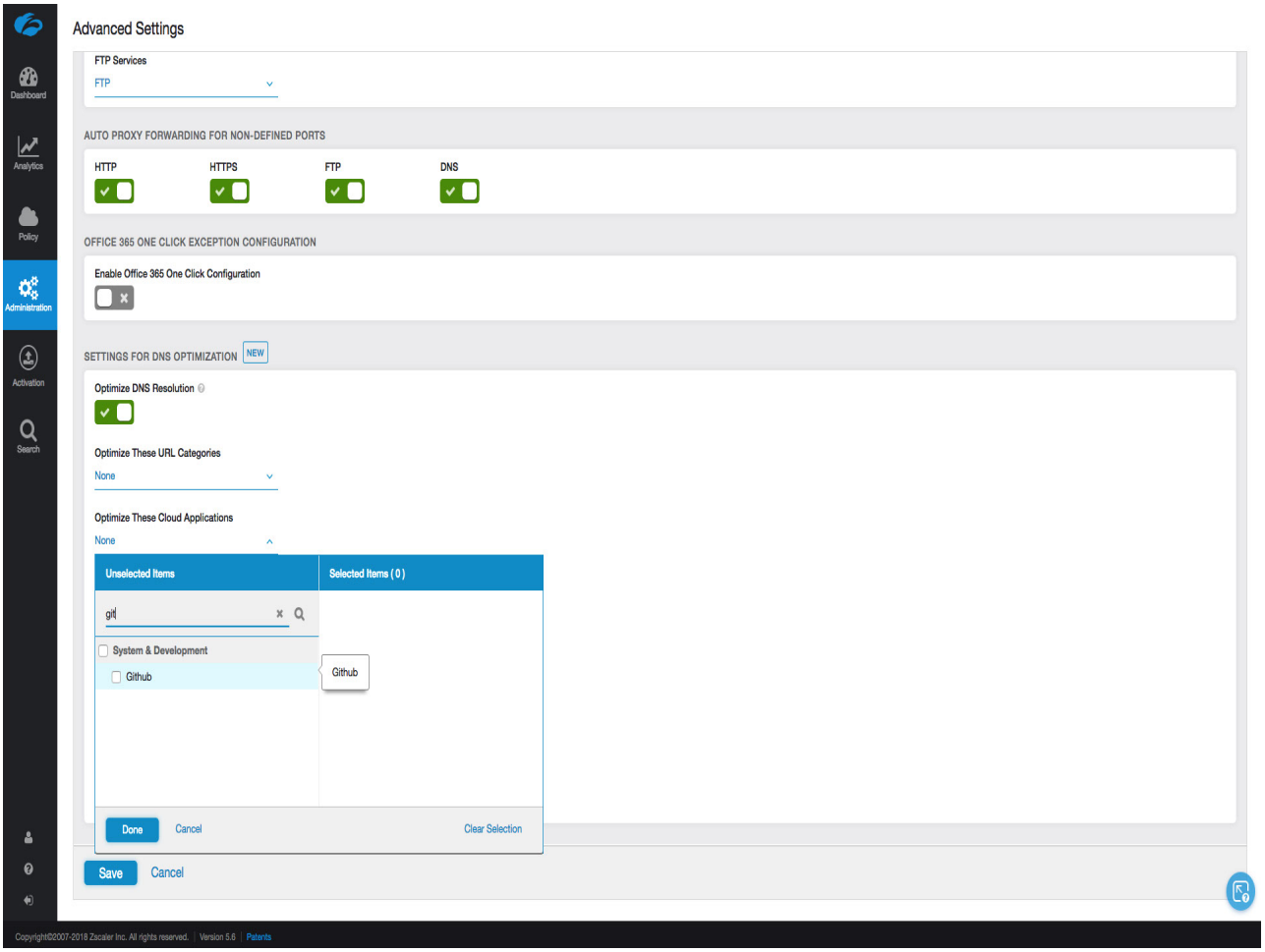
Slide 94 - Slide 94



Slide notes

To find a cloud application type the first few letters of its name in the **Search** box.

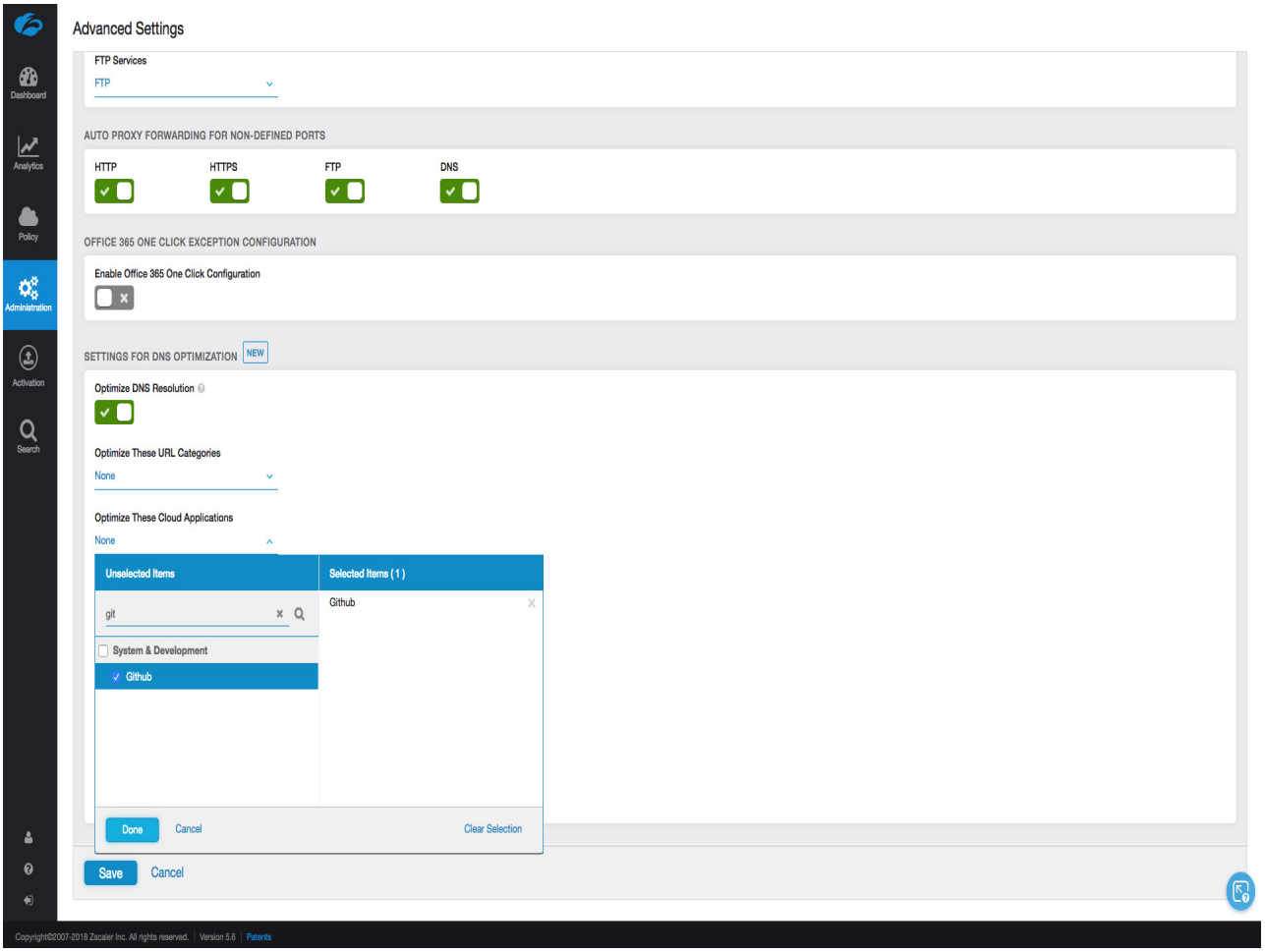
Slide 95 - Slide 95



Slide notes

Click the check box to include **Github**.

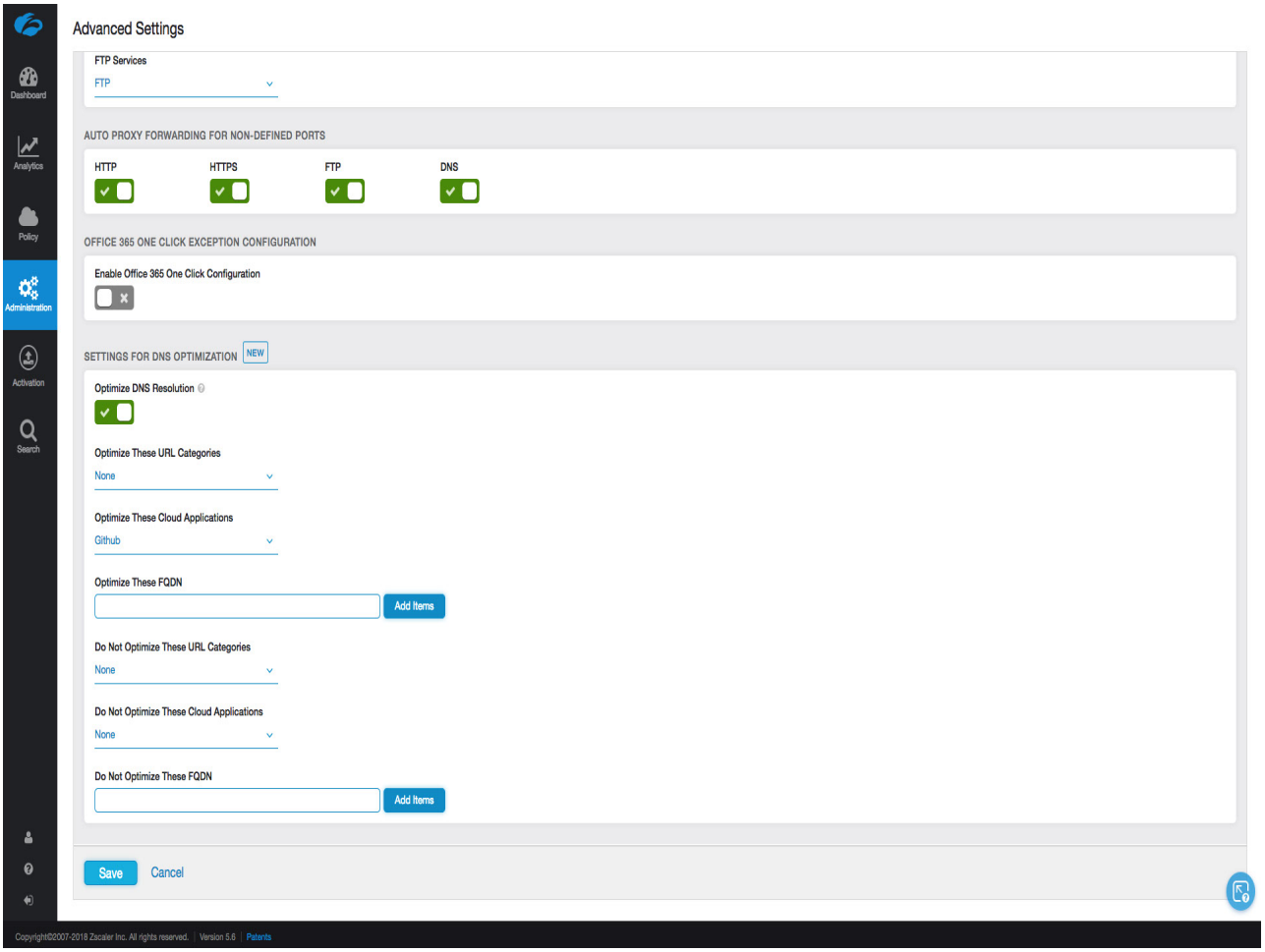
Slide 96 - Slide 96



Slide notes

Github is added to the **Selected Items** list. Other cloud applications could be added, but since this scenario specifically addresses DNS optimization for **Github**, click **Done**.

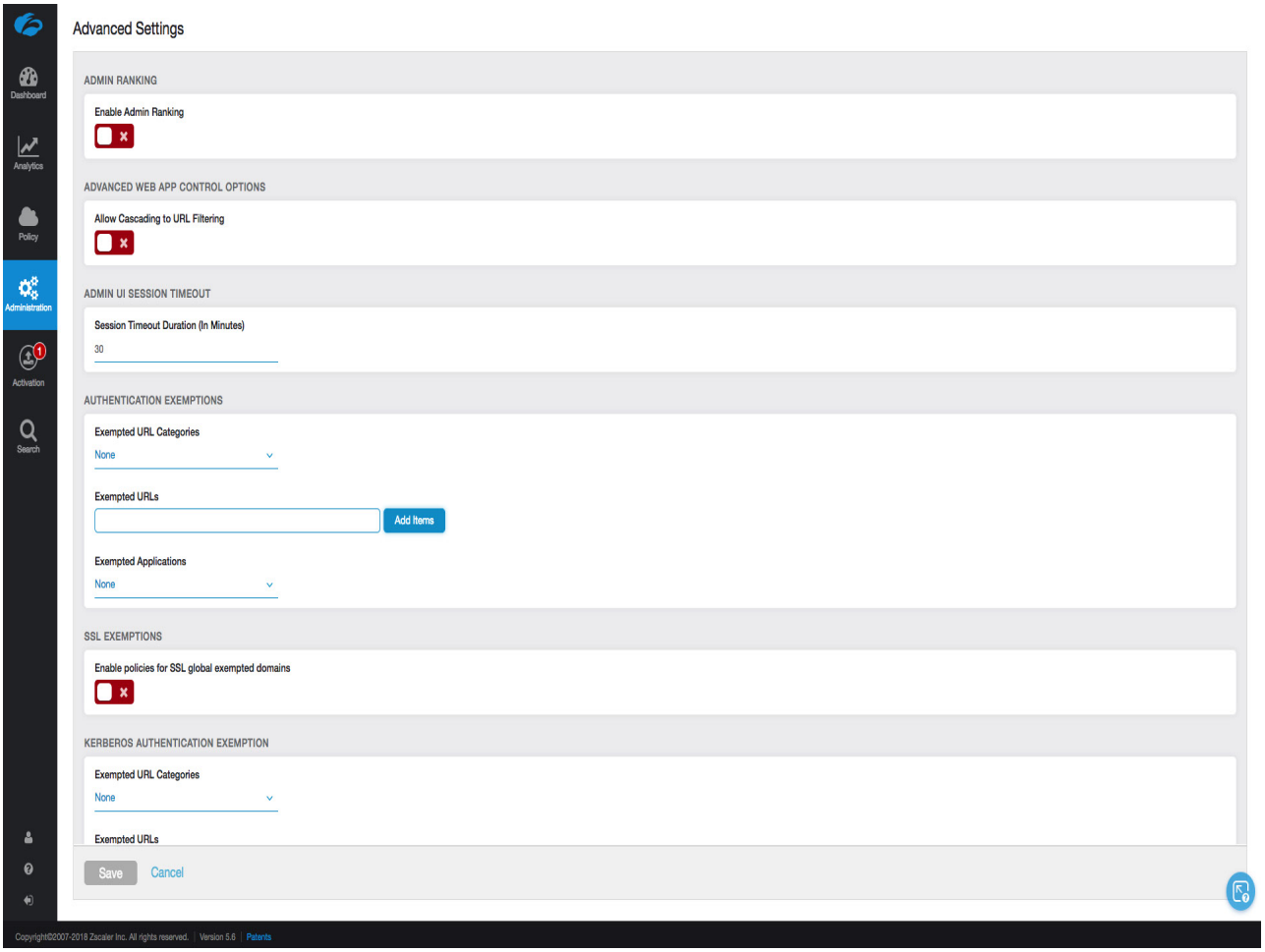
Slide 97 - Slide 97



Slide notes

And **Save** the configured **SETTINGS FOR DNS OPTIMIZATION**.

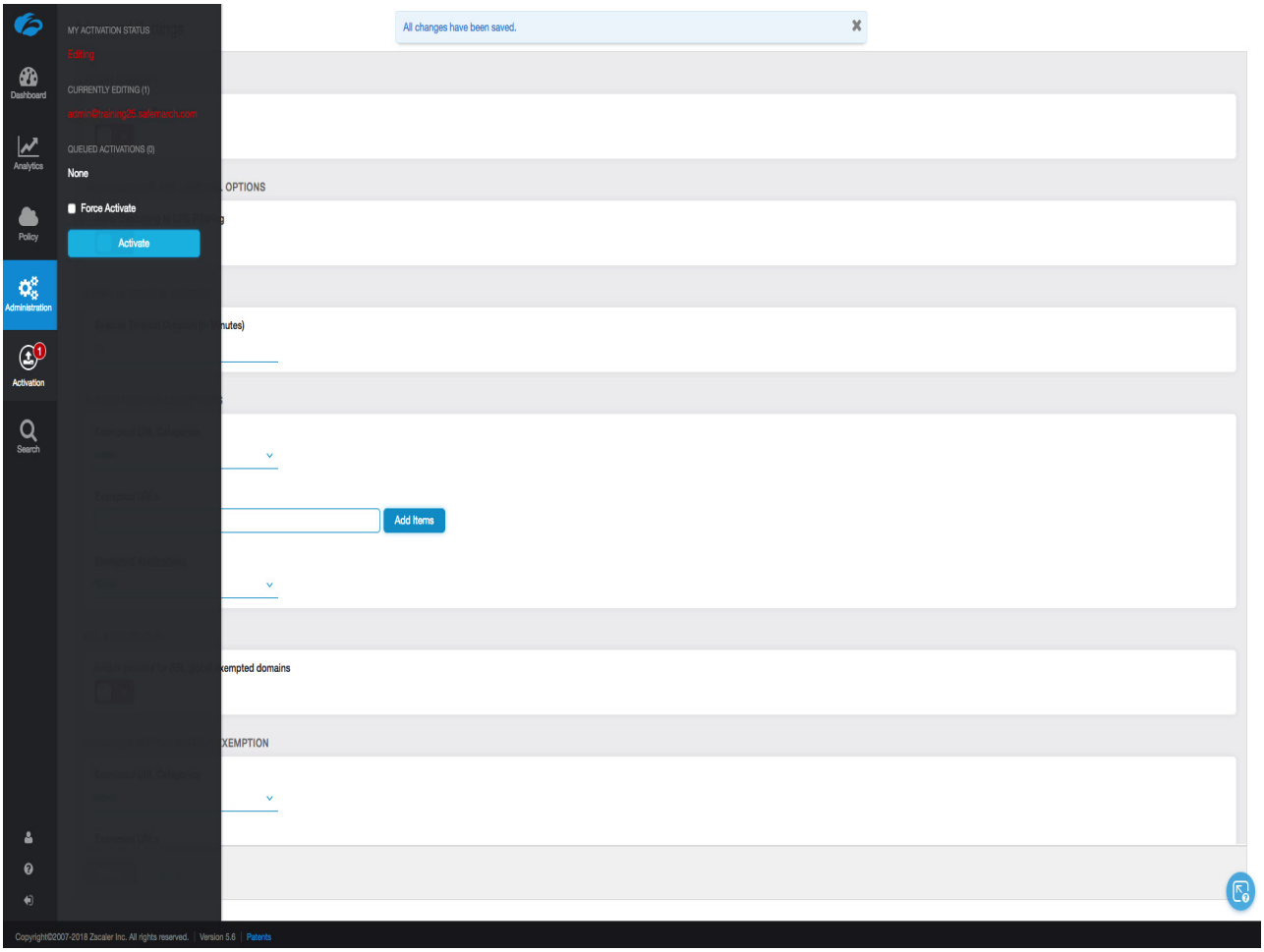
Slide 98 - Slide 98



Slide notes

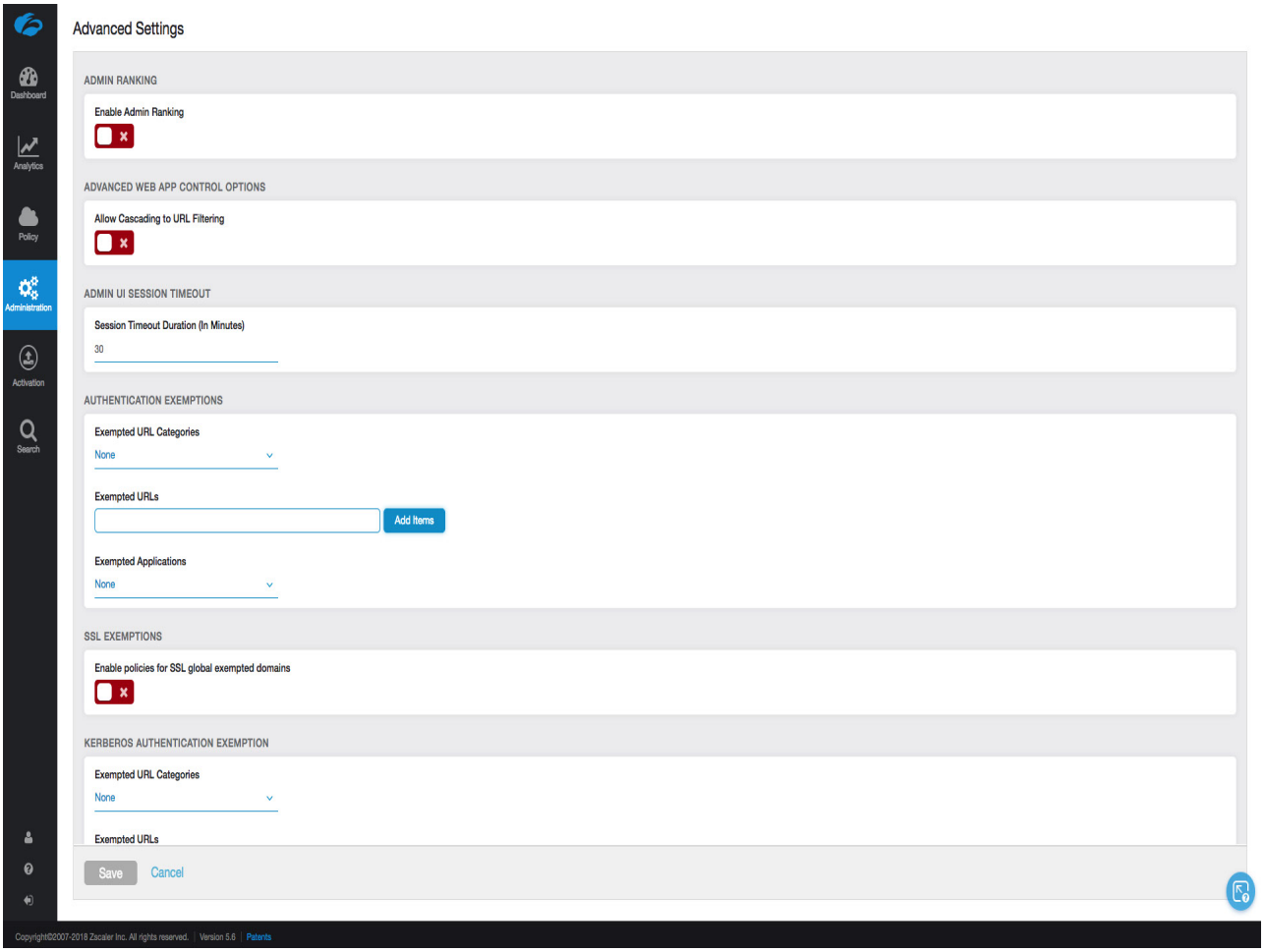
And **Activate** the changes.

Slide 99 - Slide 99



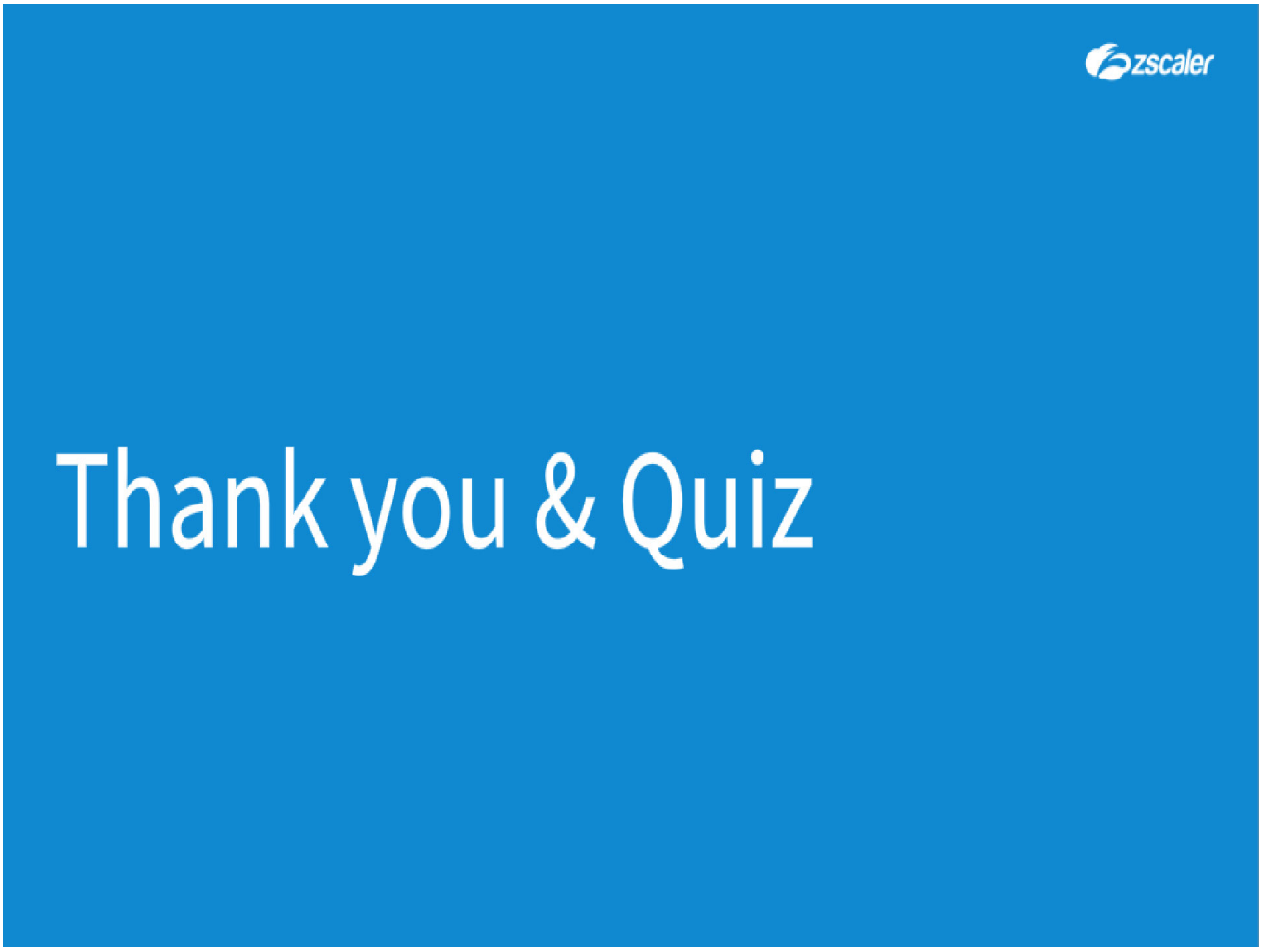
Slide notes

Slide 100 - Slide 100



Slide notes

Slide 101 - 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 to pass.