

Slide 1 - Zscaler Internet Access



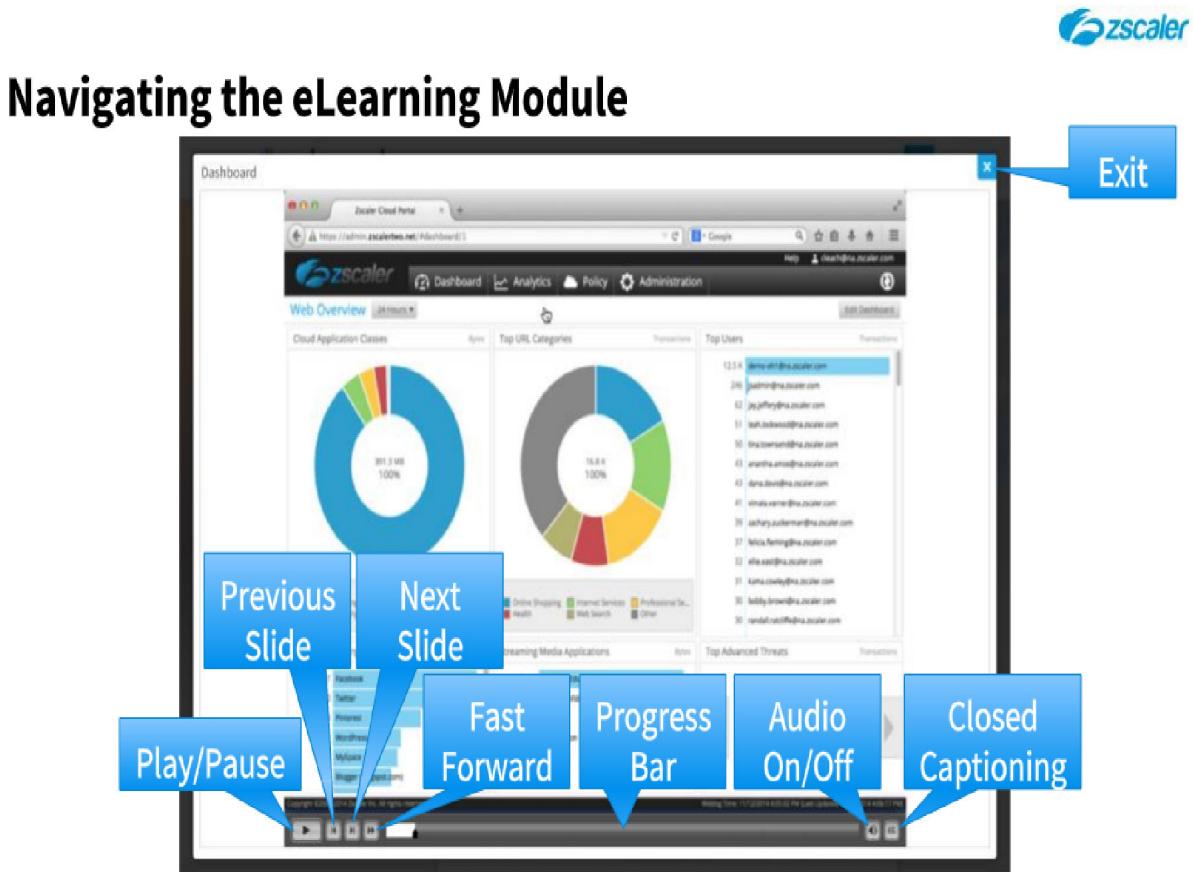
Zscaler Internet Access

Configuring DNS Security & Optimization

©2017 Zscaler, Inc. All rights reserved.

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

Agenda



- Describe ZIA DNS Security & Optimization
- Configure ZIA DNS Control Policy
- Configure ZIA DNS Tunneling Policy
- Configure ZIA DNS Resolution Optimization

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



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

ZIA DNS Security & Optimization Concepts

- DNS Traffic
- DNS client traffic security
- DNS tunnel traffic security
- DNS resolution optimization

DNS Security issues

- Exploits by botnets, malware, etc.
 - Use of untrusted servers
- ### DNS Performance bottlenecks
- Slow response to DNS requests
 - DNS resolves to sub-optimal service

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.

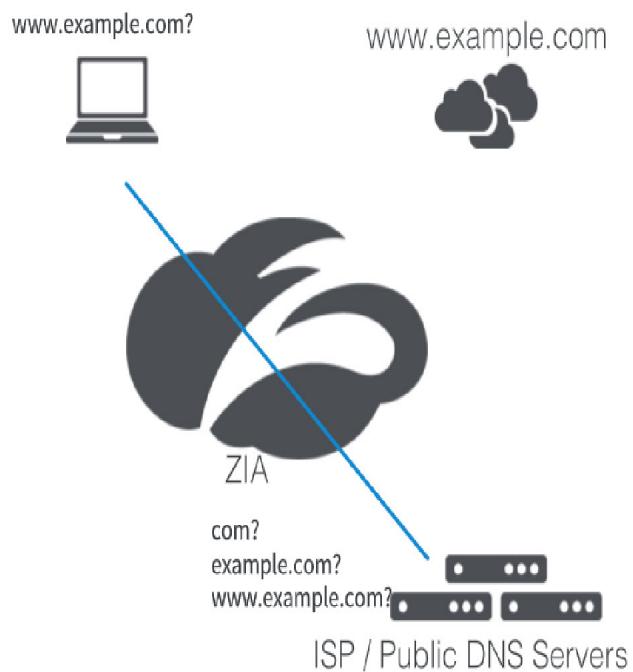
From an Internet application performance perspective, name resolution is the first step that must complete in a request so any slowness in a DNS response diminishes the user experience. With clients and services being distributed to many different locations on the internet, DNS lookups may not resolve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

Slide 6 - DNS Traffic With ZIA

DNS Traffic With ZIA

DNS lookup traffic

- Client <-> ISP / public DNS server
- Client <-> local DNS server
- Local DNS server <-> public DNS server

**Slide notes**

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

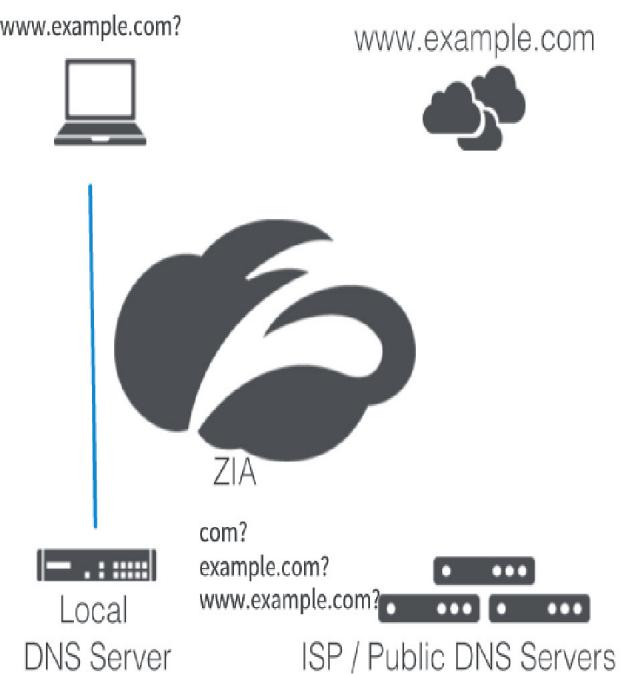
DNS lookup traffic comes from clients doing lookups on DNS servers provided by their ISP or through other public internet servers. This traffic passes through ZIA.

Slide 7 - DNS Traffic With ZIA

DNS Traffic With ZIA

DNS lookup traffic

- Client <-> ISP / public DNS server
- Client <-> local DNS server
- Local DNS server <-> public DNS server



Slide notes

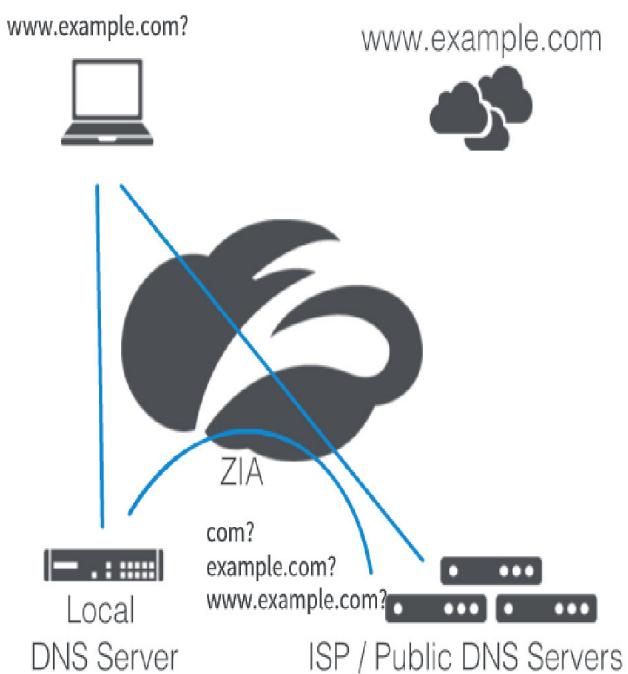
Organizations might configure client lookups to go to a local DNS server on the LAN or WAN, so this would not flow through ZIA.

Slide 8 - DNS Traffic With ZIA

DNS Traffic With ZIA

DNS lookup traffic

- Client <-> local DNS server
- Client <-> ISP / public DNS server
- Local DNS server <-> public DNS server

**Slide notes**

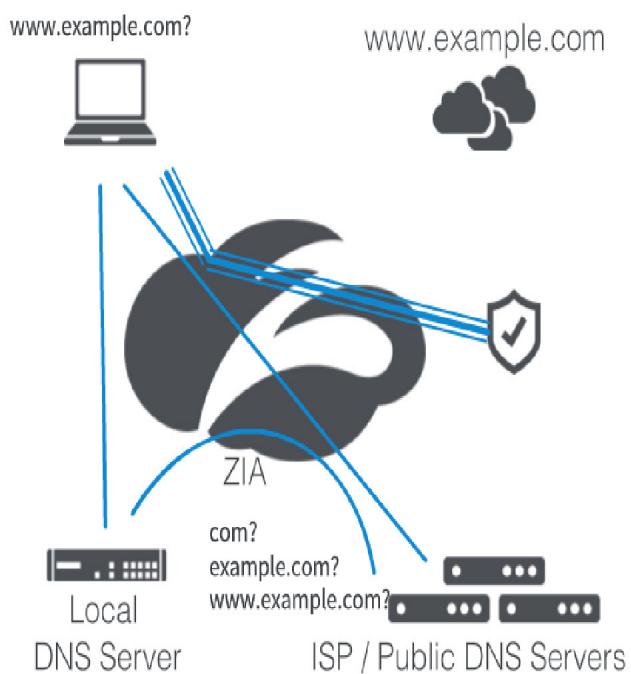
Recursive lookups to resolve host addresses through the DNS hierarchy of Root, Top Level Domain, and Authoritative servers on the internet would flow through ZIA. Depending how DNS is configured, this could either be between the local DNS server and external servers or directly from the client to internet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

Slide 9 - DNS Traffic With ZIA

DNS Traffic With ZIA

DNS lookup traffic

- Client <-> local DNS server
- Client <-> ISP / public DNS server
- Local DNS server <-> public DNS server



DNS tunnel traffic

- Internet based server -> client
- Use DNS transport
- e.g. Anti-virus signature updates

Slide notes

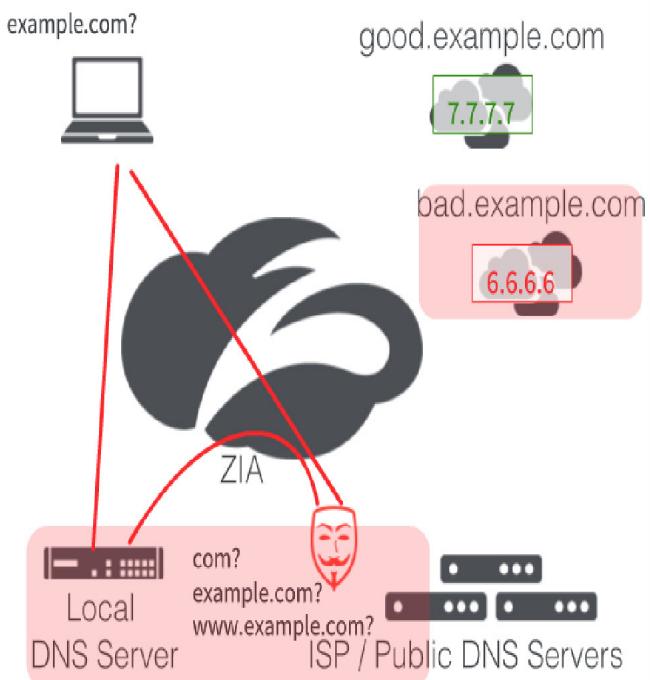
Since DNS traffic is critical, security policies are usually configured to allow DNS traffic to flow to the client and local DNS servers. This provides an opening for other applications to be able to tunnel through, encapsulated in packets that pass the security checks that allow incoming DNS. Tunneling 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

ZIA DNS Client Traffic Security Issues

DNS exploits & risks

- Users get corrupt results:
 - access untrusted DNS server; or
 - corrupted local server

**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.

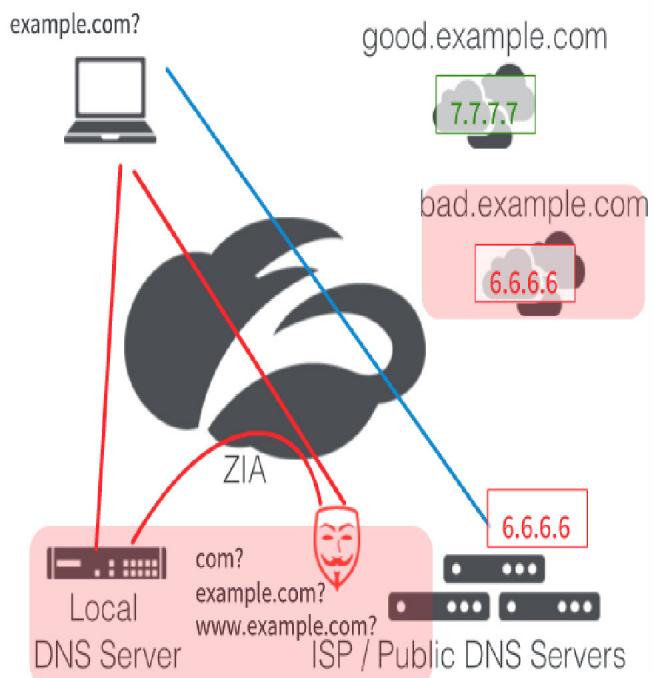
ZIA is in the path of both of these types of traffic, so malicious traffic can be detected and controlled.

Slide 11 - ZIA DNS Client Traffic Security Issues

ZIA DNS Client Traffic Security Issues

DNS exploits & risks

- Users get corrupt results:
 - access untrusted DNS server; or
 - corrupted local server
- DNS lookup results direct application connections to prohibited servers



Slide notes

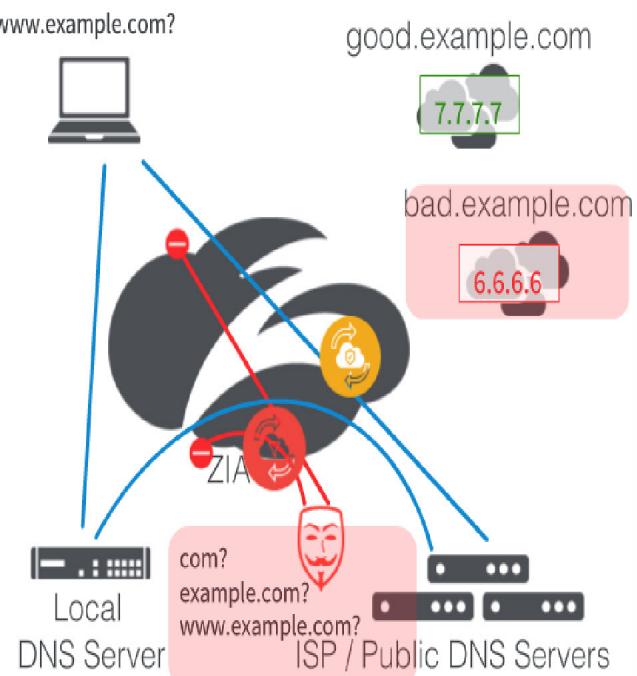
Another possible risk is that DNS lookup data, even from trusted sources, may be directing users to connect to services that are prohibited or unsanctioned. Prohibitions may be for security or organizational policy compliance based on factors such as location, ownership, or control of the servers.

Slide 12 - ZIA DNS Client Traffic Security Policies

ZIA DNS Client Traffic Security Policies

Policies

- Allow only trusted DNS traffic
- Block untrusted DNS traffic
- Redirect requests to trusted DNS server
- Redirect (rewrite) DNS response



Slide notes

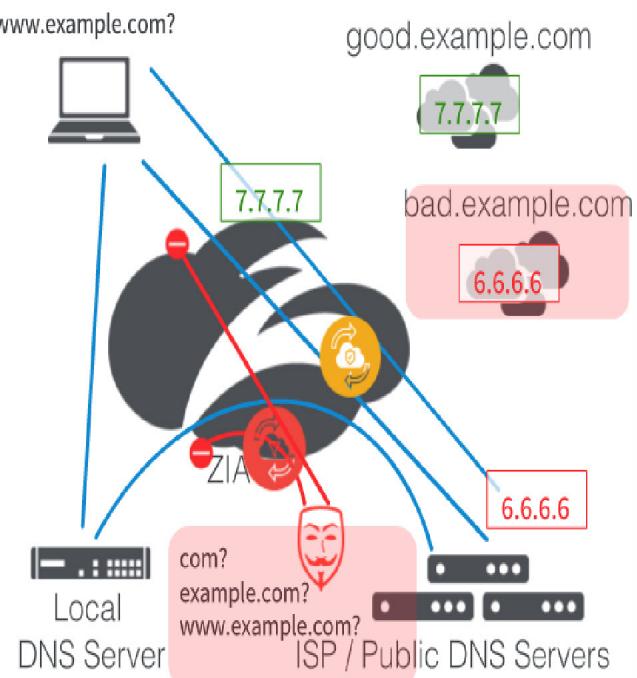
Policies may be configured to allow access to trusted DNS sources and to block untrusted traffic. Rules may also be configured to transparently redirect DNS requests to a trusted DNS server. This may be useful to help control users who ignore or are unaware of the risks of accessing data from untrusted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

Slide 13 - ZIA DNS Client Traffic Security Policies

ZIA DNS Client Traffic Security Policies

Policies

- Allow only trusted DNS traffic
- Block untrusted DNS traffic
- Redirect requests to trusted DNS server
- Redirect (rewrite) DNS response



Slide notes

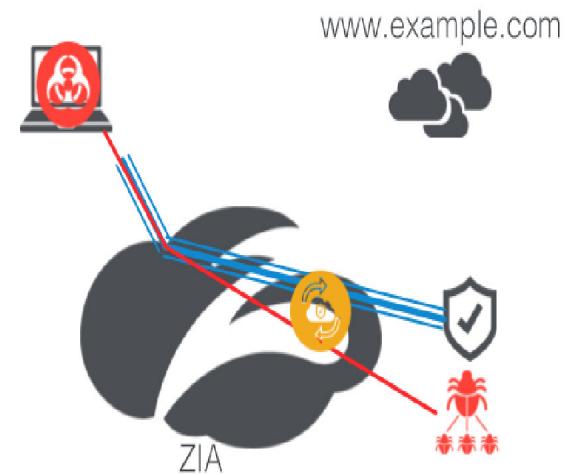
Results of a DNS response may also be rewritten by ZIA to change the IP that the client will be directed to connect to. This may be done by configuring a rule with an action to intercept the response and rewrite the destination IP address with a different value configured in ZIA.

Slide 14 - ZIA DNS Tunnel Traffic Security Issues & Policies

ZIA DNS Tunnel Traffic Security Issues & Policies

DNS Tunneling Detection

- Application
 - e.g. McAfee, DnsTunMaliciousRsvd
- Category
 - Commonly Allowed DNS Tunnels
 - Commonly Blocked DNS Tunnels
 - Unknown DNS Tunnels



Policies

- Block
- Allow

**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 simplify the configuration, traffic is classified in one of three categories: Commonly allowed DNS tunnels; Commonly 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

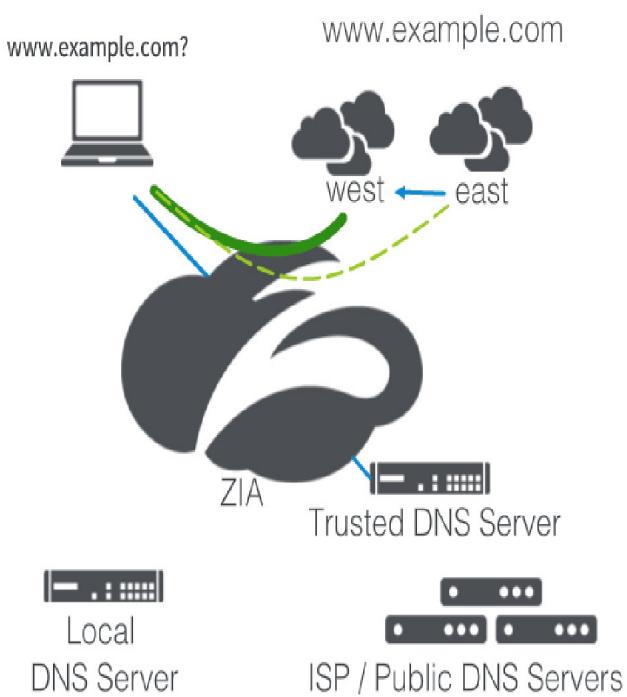
ZIA DNS Resolution Optimization

ZIA managed DNS response

- ZIA does lookup for proxied traffic
- DNS redirect rule to a faster server

DNS resolution optimization

- Direct client to faster responding application server
- Use HTTP and TLS header data to lookup and compare to DNS



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

Exercises



Configuring ZIA

- DNS Control Policy
- DNS Tunneling Policy
- DNS Resolution Optimization

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



Configuring ZIA DNS Control Policy

Slide notes

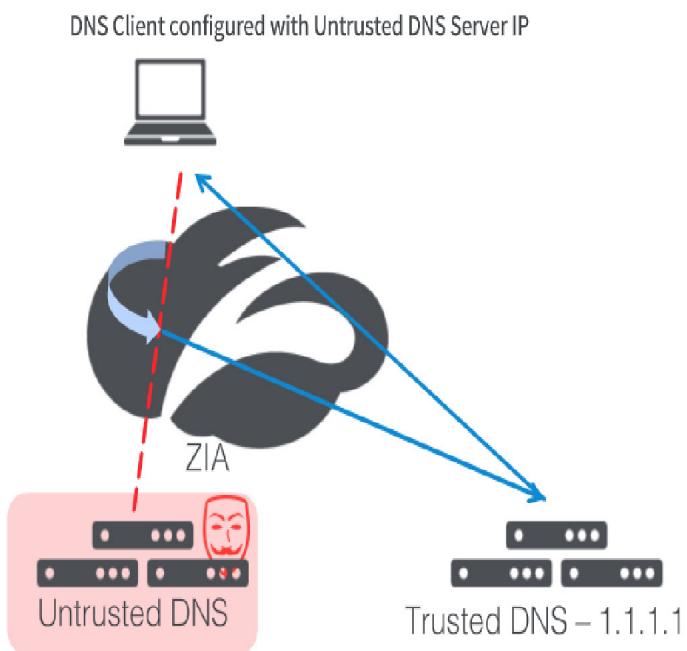
In this task you will configure a ZIA DNS Control Policy.

Slide 18 - Configuring ZIA DNS Control Policy Software Simulation

Configuring ZIA DNS Control Policy Software Simulation

Use case / scenario

- Request redirect: Client requests to untrusted DNS server
- ZIA redirect to a trusted DNS server
- Trusted server responds to client



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

The screenshot shows the 'Web Overview' section of the Zscaler dashboard. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a title 'Web Overview' at the top, with a dropdown menu for '24 Hours'. Below this are six data cards arranged in a grid:

- CLOUD APPLICATION CLASSES**: Bytes. Status: No data for selected time range.
- TOP URL CATEGORIES**: Transactions. Status: No data for selected time range.
- TOP USERS**: Transactions. Status: No data for selected time range.
- SOCIAL NETWORKING APPLICATIONS**: Transactions. Status: No data for selected time range.
- STREAMING MEDIA APPLICATIONS**: Bytes. Status: No data for selected time range.
- TOP ADVANCED THREATS**: Transactions. Status: No data for selected time range.

At the bottom of the dashboard, there is a footer bar with copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents'. To the right of this is a timestamp: 'Weblog Time: 9/17/2018 8:32:51 AM'. Further to the right is a note: 'Last Updated: 9/17/2018 8:32:52 AM'. On the far right edge of the dashboard, there is a small circular icon with a blue border and a white 'Z' inside.

Slide notes

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

Slide 20 - Slide 20

The screenshot shows the Zscaler Policy Management interface. The left sidebar has a dark theme with various icons and sections:

- Web Protection** (selected):
 - SECURITY: Malware Protection, Advanced Threat Protection, Sandbox, Browser Control.
 - ACCESS CONTROL: URL & Cloud App Control, File Type Control, Bandwidth Control, SSL Inspection.
- Data Loss Prevention**: Data Loss Prevention.
- Policy**: Recommended Policy.
- Administration**: ZSCALER APP CONFIGURATION, Zscaler App Portal.
- Activation**: Mobile App Store Control.
- Search**: Firewall Filtering, ACCESS CONTROL, Firewall Control, DNS Control, FTP Control.

The main content area displays the "Web Protection" configuration page, which is currently empty. At the bottom, there is a URL bar showing <https://admin.zscalerone.net/#policy/web/malware-protection>, a timestamp of "Weblog Time: 9/17/2018 8:32:51 AM", and a note "Last Updated: 9/17/2018 8:32:52 AM".

Slide notes

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

Slide 21 - Slide 21

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' and contains a table of DNS filtering rules.

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		
Default	Unknown DNS Traffic	Any	Allow		
Default	Default Firewall DNS Rule	Any	Allow		

At the bottom of the page, there is a footer bar with copyright information, a timestamp, and a refresh icon.

Slide notes

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

Slide 22 - Slide 22

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "DNS Control" and has a sub-section "Configure DNS Control Policy". It lists existing rules: "Office 365 One Click Rule" (Rule Order 1, Enabled) and "Default Firewall DNS Rule" (Rule Order 2, Enabled). A modal window titled "Add DNS Filtering Rule" is open, prompting for new rule details. The "DNS FILTERING RULE" section includes fields for "Rule Order" (set to 2), "Rule Name" (set to "DNS_1"), and "Rule Status" (set to "Enabled"). The "CRITERIA" section defines users ("Any", "Any"), departments ("Any", "Any"), locations ("Any", "Any"), and time ("Always"). The "ACTION" section specifies "Network Traffic" ("Allow") and "Logging" ("Full"). A large "DESCRIPTION" field is present but empty. At the bottom of the modal are "Save" and "Cancel" buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default, Any), and 'Default Firewall DNS Rule' (Default, Any). A modal window titled 'Add DNS Filtering Rule' is open. It contains fields for 'Rule Order' (set to 2), 'Rule Name' (set to 'DNS_1'), and 'Rule Status' (set to 'Enabled'). Below these are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'WHO, WHERE, & WHEN' tab is selected. Under 'CRITERIA', there are dropdowns for 'Users' (Any) and 'Groups' (Any), 'Departments' (Any) and 'Locations' (Any), and a 'Time' dropdown set to 'Always'. The 'ACTION' section shows 'Network Traffic' (Allow) and 'Logging' (Full). A large 'DESCRIPTION' text area is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 24 - Slide 24

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default, Any), and 'Default Firewall DNS Rule' (Default, Any). A modal window titled 'Add DNS Filtering Rule' is open, prompting for a 'Rule Order' (set to 2), a 'Rule Name' (set to 'DNS Redirect'), and a 'Rule Status' (set to 'Enabled'). Below these are tabs for 'WHO, WHERE, & WHEN' (selected), 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'WHO, WHERE, & WHEN' tab is divided into 'CRITERIA' and 'ACTION' sections. Under 'CRITERIA', 'Users' and 'Groups' are both set to 'Any'. Under 'ACTION', 'Network Traffic' is set to 'Allow' and 'Logging' is set to 'Full'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default), and 'Default Firewall DNS Rule' (Default). A modal window titled 'Add DNS Filtering Rule' is open. In the 'DNS FILTERING RULE' section, 'Rule Order' is set to 2 and 'Rule Name' is 'DNS Redirect'. The 'Rule Status' is 'Enabled'. Below this, there are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'WHO, WHERE, & WHEN' tab is selected. Under 'CRITERIA', 'Users' and 'Groups' are both set to 'Any'. 'Departments' and 'Locations' are also set to 'Any'. A 'Time' dropdown shows 'Always'. Below this is the 'ACTION' section, where 'Network Traffic' is set to 'Allow'. The 'DESCRIPTION' section contains a large empty text area. At the bottom of the modal, there are 'Done', 'Cancel', and 'Clear Selection' buttons, along with 'Save' and 'Cancel' buttons at the very bottom.

Slide notes

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

Slide 26 - Slide 26

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various navigation icons: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default), and 'Default Firewall DNS Rule' (Default). The central part of the screen is a modal window titled 'Add DNS Filtering Rule'. Inside, you can set the 'Rule Order' to 2, give it a name like 'DNS Redirect', and enable it. Under 'WHO, WHERE, & WHEN', 'SOURCE IP'S is selected. In the 'CRITERIA' section, both 'Users' and 'Groups' are set to 'Any'. Under 'ACTION', 'Network Traffic' is selected with 'Allow' as the action. A modal window is overlaid on the main dialog, showing a list of selected items: 'Site_1' is listed under 'Selected Items (1)'. At the bottom of the main dialog, there are 'Done', 'Cancel', and 'Clear Selection' buttons, and at the very bottom, 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 27 - Slide 27

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "DNS Control" and has a sub-section "Configure DNS Control Policy". It lists three existing rules: "Office 365 One Click Rule" (Rule Order 1, Enabled), "Unknown DNS Traffic" (Default, Any), and "Default Firewall DNS Rule" (Default, Any). A modal window titled "Add DNS Filtering Rule" is open, prompting for a "Rule Order" (set to 2), a "Rule Name" (set to "DNS Redirect"), and a "Rule Status" (set to "Enabled"). The modal is divided into several sections: "WHO, WHERE, & WHEN" (with tabs for WHO, WHERE, WHEN, and AND/OR), "CRITERIA" (with tabs for Users, Groups, Departments, Locations, and Time), "ACTION" (with tabs for Network Traffic, Logging, and AND/OR), and "DESCRIPTION" (a large text area). At the bottom of the modal are "Save" and "Cancel" buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default), and 'Default Firewall DNS Rule' (Default). The central part of the screen is a modal window titled 'Add DNS Filtering Rule'. This window has several tabs: 'WHO, WHERE, & WHEN' (selected), 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Below these tabs are sections for 'CRITERIA' (Users: Any, Groups: Any, Departments: Any, Locations: Site_1) and 'ACTION' (Network Traffic: Allow, Logging: Full). A dropdown menu under 'ACTION' shows four options: 'Allow' (selected), 'Block', 'Redirect Request', and 'Redirect Response'. The 'Redirect Request' option is highlighted with a blue border. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Select the **Redirect Request** action.

Slide 29 - Slide 29

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default, Any), and 'Default Firewall DNS Rule' (Default, Any). A modal window titled 'Add DNS Filtering Rule' is open. It contains fields for 'Rule Order' (set to 2), 'Rule Name' (set to 'DNS Redirect'), 'Rule Status' (set to 'Enabled'), and tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'WHO, WHERE, & WHEN' tab is selected. Under 'CRITERIA', it shows 'Users' (Any) and 'Groups' (Any). Under 'Time', it shows 'Any' and 'Site_1'. Under 'ACTION', it shows 'Network Traffic' (set to 'Redirect Request') and 'DNS Server IP Address' (empty). Under 'Logging', it shows 'Full'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 30 - Slide 30

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'Unknown DNS Traffic' (Default, Any), and 'Default Firewall DNS Rule' (Default, Any). A modal window titled 'Add DNS Filtering Rule' is open. It contains fields for 'Rule Order' (set to 2), 'Rule Name' (set to 'DNS Redirect'), 'Rule Status' (set to 'Enabled'), and tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'WHO, WHERE, & WHEN' tab is selected. Under 'CRITERIA', it shows 'Users' set to 'Any' and 'Groups' set to 'Any'. Under 'Time', it shows 'Any' and 'Site_1'. Under 'ACTION', it shows 'Network Traffic' set to 'Redirect Request' and 'DNS Server IP Address' set to '1.1.1.1'. Under 'Logging', it shows 'Full'. A large 'DESCRIPTION' text area is present at the bottom of the modal. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

Copyright © 2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Projects

Weblog Time: 9/17/2018 8:32:51 AM | Last Updated: 9/17/2018 8:32:52 AM

Slide notes

Save the rule.

Slide 31 - Slide 31

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with a sub-instruction 'You can define rules that control DNS requests and responses.' A message at the top right says 'All changes have been saved.' Below this is a search bar with a magnifying glass icon. A table lists four DNS filtering rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		edit
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		edit info
Default	Unknown DNS Traffic	Any	Allow		edit
Default	Default Firewall DNS Rule	Any	Allow		edit

At the bottom, there are copyright notices: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents' and 'Weblog Time: 9/17/2018 8:32:51 AM Last Updated: 9/17/2018 8:32:52 AM'. A blue circular icon with a white 'Z' is also present.

Slide notes

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

Slide 32 - Slide 32

The screenshot shows the Zscaler DNS Security & Optimization 5.6 v1.0 interface. The left sidebar has icons for Dashboard, Analytics, Policy (selected), Administration, Activation (with a red notification dot), and Search. The main area shows 'MY ACTIVATION STATUS' with 'Editing' and 'CURRENTLY EDITING (1)' for 'admin@training20.salemerch.com'. A message says 'All changes have been saved.' Below is a table of rules:

Rule Name	Criteria	Action	Description	⋮
Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		edit
NS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		edit info
Unknown DNS Traffic	Any	Allow		edit
Default Firewall DNS Rule	Any	Allow		edit

At the bottom, it says 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents' and 'Weblog Time: 9/17/2018 8:32:51 AM Last Updated: 9/17/2018 8:32:52 AM'.

Slide notes

Slide 33 - Slide 33

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with a sub-instruction 'You can define rules that control DNS requests and responses.' A message box at the top right says 'Activation Completed!' with a close button. Below this is a table titled 'Add DNS Filtering Rule' with columns: Rule Order, Rule Name, Criteria, Action, Description, and a more options icon. The table lists four rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		edit
2	DNS Redirect	LOCATIONS Site,1	Redirect Request: 1.1.1.1		edit info
Default	Unknown DNS Traffic	Any	Allow		edit
Default	Default Firewall DNS Rule	Any	Allow		edit

At the bottom, there are copyright notices: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents' and 'Weblog Time: 9/17/2018 8:32:51 AM Last Updated: 9/17/2018 8:32:52 AM'. A blue circular icon with a white 'Z' is also present.

Slide notes

Slide 34 - Slide 34

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' Below this is a search bar with placeholder 'Search...' and a magnifying glass icon.

Add DNS Filtering Rule

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		Edit
2	DNS Redirect	LOCATIONS Site,1	Redirect Request: 1.1.1.1		Edit Preview
Default	Unknown DNS Traffic	Any	Allow		Edit
Default	Default Firewall DNS Rule	Any	Allow		Edit

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Weblog Time: 9/17/2018 8:32:51 AM Last Updated: 9/17/2018 8:32:52 AM

Slide notes

Slide 35 - Verifying DNS Control Policy



Verifying DNS Control Policy

Slide notes

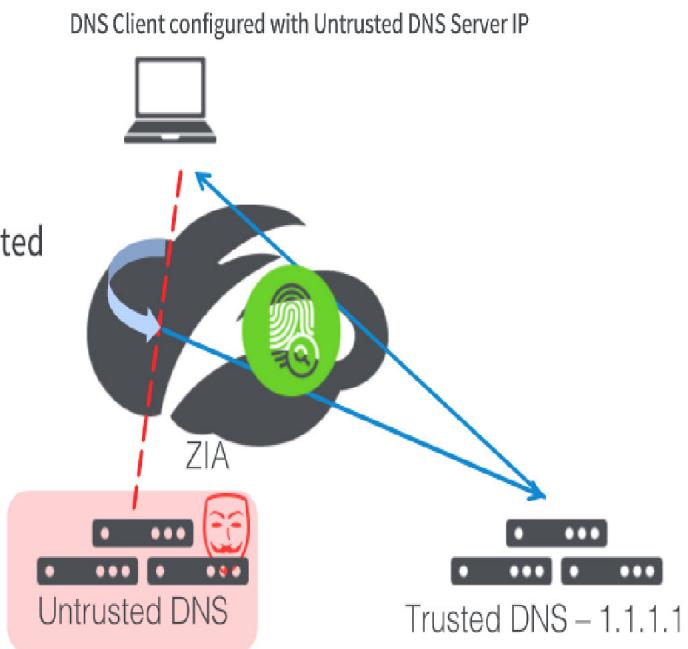
In this task you will verify that DNS Control Policy is being enforced.

Slide 36 - Verifying ZIA DNS Control Policy Software Simulation

Verifying ZIA DNS Control Policy Software Simulation

Use case / scenario

- Request redirect: Client requests to a trusted DNS server
- Verify that a DNS request to an untrusted server transparently redirected (view DNS Insights log entry).



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

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' Below this is a table titled 'Add DNS Filtering Rule' with columns: Rule Order, Rule Name, Criteria, Action, Description, and a more options icon. There are four rows in the table:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		
2	DNS Redirect	LOCATIONS Site,1	Redirect Request: 1.1.1.1		
Default	Unknown DNS Traffic	Any	Allow		
Default	Default Firewall DNS Rule	Any	Allow		

At the bottom of the interface, there are copyright information ('Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents'), a timestamp ('Weblog Time: 9/17/2018 10:17:44 AM'), and a last updated timestamp ('Last Updated: 9/17/2018 10:17:46 AM'). A blue circular icon with a white question mark is located in the bottom right corner.

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.

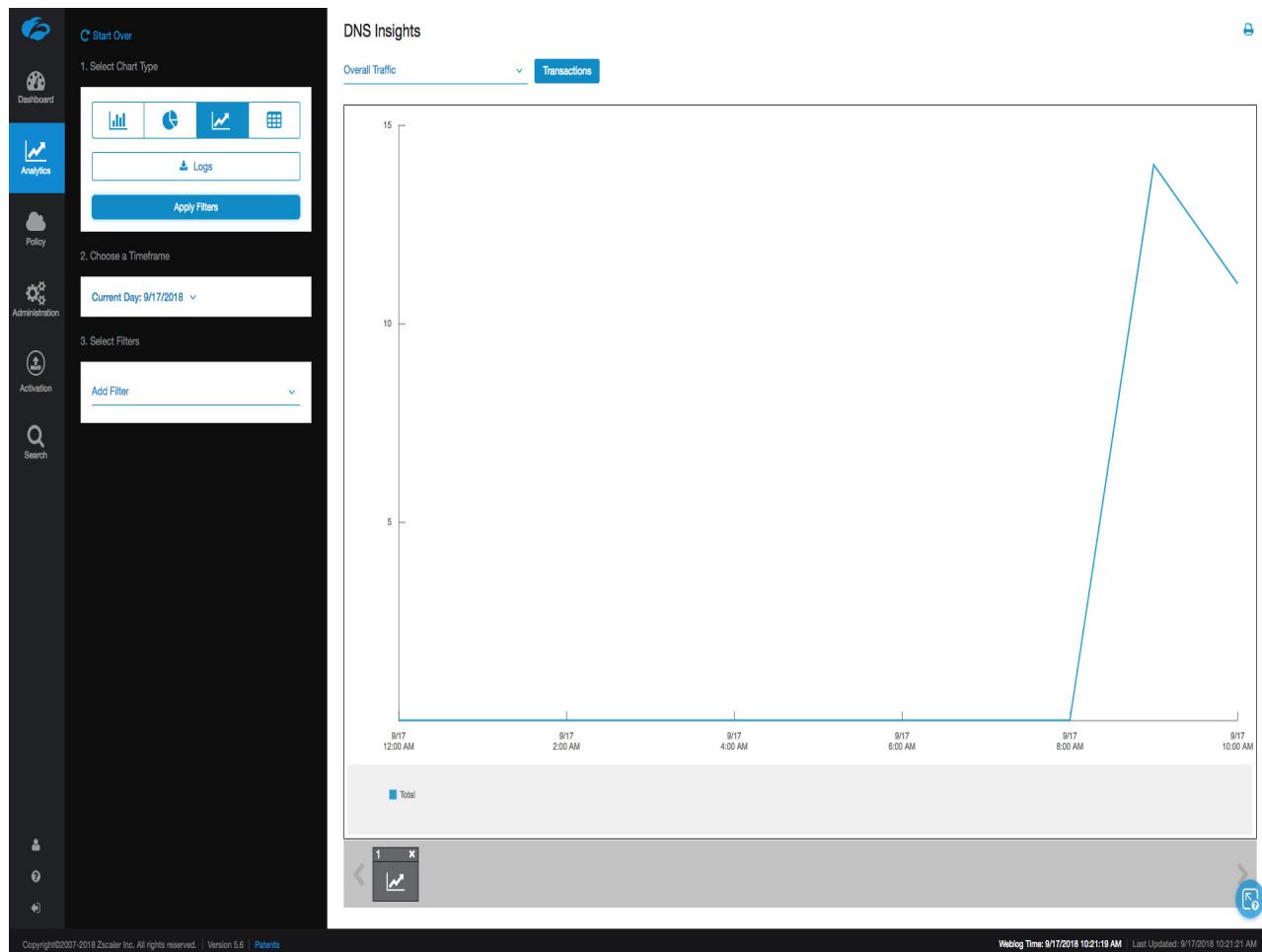
Slide 38 - Slide 38

The screenshot shows the Zscaler interface with the 'REPORTING' tab selected. On the left, a sidebar lists various report categories: Dashboard, Analytics, Policy, Administration, Activation, and Search. Under 'INSIGHTS', there are sections for Web Insights, Mobile Insights, Firewall Insights, and DNS Insights. The 'DNS Insights' section is currently active, showing a sub-menu with options like 'Security Policy Audit Report' (marked as NEW) and 'DNS Usage Trends'. The main content area is titled 'Interactive Reports' and displays a message: 'No report. Create a new report or select a report from the left to get started.' A small 'Report' and 'Import' button is visible at the top of this area.

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

The screenshot shows the Zscaler DNS Security & Optimization 5.6 v1.0 interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "DNS Insights". It has three steps on the left: 1. Select Chart Type (with four chart icons), 2. Choose a Timeframe (set to "Current Day: 9/17/2018"), and 3. Select Filters (with an "Add Filter" dropdown). A large central area is labeled "Set the options on the left and click Apply Filters to view logs." with a download icon. At the bottom, there is a small window showing a chart and navigation arrows, along with copyright and log information.

Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Weblog Time: 9/17/2018 12:53:07 PM Last Updated: 9/17/2018 12:53:09 PM

Slide notes

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

Slide 41 - Slide 41

The screenshot shows the ZCCIA-IA interface with the following details:

- Left Sidebar:** Contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search.
- Main Area:** Titled "DNS Insights". It includes a "Start Over" button and a "Logs" section with four chart types: Bar, Line, Area, and Grid. A "Logs" button and "Apply Filters" button are also present.
- Timeframe Selection:** A dropdown menu titled "Choose a Timeframe" with the current selection "Current Day: 9/17/2018". Other options include "Last 1 Minute", "Last 2 Minutes", "Last 5 Minutes", "Last 15 Minutes", "Last 30 Minutes", "Last 1 Hour", "Last 2 Hours", "Last 5 Hours", "Last 10 Hours", "Current Day" (selected), "Current Week", "Current Month", "Previous Day", "Previous Week", "Previous Month", and "Custom".
- Content Area:** A large empty box with a download icon and the text "Set the options on the left and click Apply Filters to view logs."
- Bottom Navigation:** Includes a search bar, a "1" indicator, and a refresh/circular arrow icon.
- Footer:** Copyright information "Copyright 2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents" and log time "Weblog Time: 9/17/2018 12:53:07 PM Last Updated: 9/17/2018 12:53:09 PM".

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

The screenshot shows the Zscaler DNS Security & Optimization 5.6 v1.0 interface. On the left is a dark sidebar with various icons and sections: Dashboard, Analytics (selected), Policy, Administration, Activation, and Search. The main area is titled "DNS Insights". It has three steps on the left: 1. Select Chart Type (with four chart icons), 2. Choose a Timeframe (set to "Current Day: 9/17/2018"), and 3. Select Filters (with an "Add Filter" dropdown). A large central area is currently empty with a download icon and the text "Set the options on the left and click **Apply Filters** to view logs." At the bottom, there's a navigation bar with a back arrow, a forward arrow, and a refresh icon.

Slide notes

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

Slide 43 - Slide 43

The screenshot shows the Zscaler interface with the following sections:

- Start Over**: A button to reset the dashboard.
- Dashboard**: A summary section with various metrics and links.
- Analytics**: A chart showing traffic trends.
- Policy**: A section for managing security policies.
- Administration**: A section for system management.
- Activation**: A section for activating licenses.
- Search**: A search bar for finding specific logs.
- DNS Insights**: The main log viewer with the following details:
 - Logs**: A button to view logs.
 - Apply Filters**: A button to apply specific filters to the logs.
 - Choose a Timeframe**: A dropdown set to "Current Day: 9/17/2018".
 - Select Filters**: A dropdown menu for filtering logs.
 - Table Headers**: No. (Log ID), Logged Time, User, Request Action, Response Action, Location, Department, Client IP, Server IP, Requested Domain, Resolved IP or URL.
 - Table Data** (25 rows):

No.	Logged Time	User	Request Action	Response Action	Location	Department	Client IP	Server IP	Requested Domain	Resolved IP or URL
1	Monday, September 17, 2018 9:47:11 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
2	Monday, September 17, 2018 9:48:07 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	35.166.119.124
3	Monday, September 17, 2018 9:48:07 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
4	Monday, September 17, 2018 9:48:31 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	None
5	Monday, September 17, 2018 9:49:03 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	8.8.8.in-addr.arpa	None
6	Monday, September 17, 2018 9:49:06 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
7	Monday, September 17, 2018 9:49:07 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
8	Monday, September 17, 2018 9:49:17 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	35.166.119.124
9	Monday, September 17, 2018 9:49:40 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	None
10	Monday, September 17, 2018 9:49:55 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	8.8.8.in-addr.arpa	None
11	Monday, September 17, 2018 9:49:56 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
12	Monday, September 17, 2018 9:49:56 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
13	Monday, September 17, 2018 9:50:32 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	35.166.119.124
14	Monday, September 17, 2018 9:50:34 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	None
15	Monday, September 17, 2018 10:09:55 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
16	Monday, September 17, 2018 10:09:55 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
17	Monday, September 17, 2018 10:09:55 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	35.166.119.124
18	Monday, September 17, 2018 10:09:55 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	None
19	Monday, September 17, 2018 10:10:27 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	8.8.8.in-addr.arpa	None
20	Monday, September 17, 2018 10:10:27 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
21	Monday, September 17, 2018 10:10:28 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.training25.safemarch.com	None
22	Monday, September 17, 2018 10:10:28 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.safemarch.com	None
23	Monday, September 17, 2018 10:10:28 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com.safemarch.com	None
24	Monday, September 17, 2018 10:10:29 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	35.166.119.124
25	Monday, September 17, 2018 10:10:29 AM	Site_1	Redirect	Allow	Site_1	Default Department	10.2.2.1	1.1.1.1	www.zscaler.com	None
 - Logs**: A small preview window showing a single log entry.
 - Filter**: A dropdown menu for applying filters.
 - Timeframe**: A dropdown menu for selecting timeframes.
 - Logs**: A button to view logs.
 - Apply Filters**: A button to apply filters.
 - Start Over**: A button to start over.

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



Configuring ZIA DNS Tunneling Policy

Slide notes

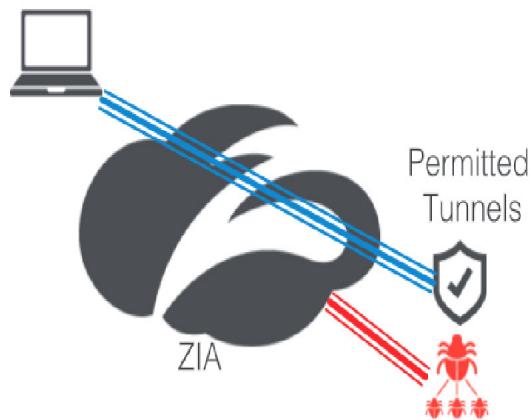
In this task you will configure a ZIA DNS Tunneling Policy.

Slide 45 - Configuring ZIA DNS Tunneling Policy Software Simulation

Configuring ZIA DNS Tunneling Policy Software Simulation

Use case / scenario

- Block all DNS tunnels except for McAfee and Eset.



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

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy (highlighted in blue), Administration, Activation, and Search. The main area has a title 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' Below this is a search bar with placeholder 'Search...' and a magnifying glass icon. A button labeled 'Add DNS Filtering Rule' with a plus sign icon is visible. The central part of the screen displays a table of DNS filtering rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		Edit
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		Edit Preview
Default	Unknown DNS Traffic	Any	Allow		Edit
Default	Default Firewall DNS Rule	Any	Allow		Edit

At the bottom of the main area, there is a copyright notice: 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents'. To the right of the notice is a blue circular icon with a white 'Z' and a gear symbol.

Slide notes

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

Slide 47 - Slide 47

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with various icons and links: Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main content area is titled "Policy" and contains several sections: "Web Protection" (with sub-links: Malware Protection, Advanced Threat Protection, Sandbox, Browser Control, URL & Cloud App Control, File Type Control, Bandwidth Control, SSL Inspection), "Data Loss Prevention" (with sub-link: Data Loss Prevention), "Mobile" (with sub-links: ZSCALER APP CONFIGURATION, Zscaler App Portal, Mobile Malware Protection, ACCESS CONTROL, Mobile App Store Control), "Firewall Filtering" (with sub-links: Firewall Control, DNS Control, FTP Control), and "Access Control" (with sub-links: Web, Downloaded Applications, DNS, Remote Access, Network). A "Recommended Policy" button is located in the top right of the main content area. The URL in the browser bar is https://admin.zscalerone.net/#policy/web/malware-protection.

Slide notes

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

Slide 48 - Slide 48

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' and contains a table of DNS filtering rules.

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		Edit
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		Edit Preview
Default	Unknown DNS Traffic	Any	Allow		Edit
Default	Default Firewall DNS Rule	Any	Allow		Edit

At the bottom of the page, there is a copyright notice: 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents' and a blue circular icon with a white 'Z'.

Slide notes

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

Slide 49 - Slide 49

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists several existing rules:

- Rule Order 1: Office 365 One Click Rule, Enabled, Destination: Off-Site
- Rule Order 2: DNS Redirect, Enabled, Destination: Local Site
- Default: Unknown DNS Traffic, Any
- Default: Default Firewall DNS Rule, Any

A modal window titled 'Add DNS Filtering Rule' is open. It has the following configuration:

- DNS FILTERING RULE**
 - Rule Order: 3
 - Rule Name: DNS_1
 - Rule Status: Enabled
- WHO, WHERE, & WHEN** tab selected (SOURCE IP'S, DESTINATION/RESOL..., DNS APPLICATION tabs available)
- CRITERIA**
 - Users: Any, Groups: Any
 - Departments: Any, Locations: Any
 - Time: Always
- ACTION**
 - Network Traffic: Allow
 - Logging: Full
- DESCRIPTION**: An empty text area.

At the bottom of the modal are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), 'Unknown DNS Traffic' (Default, Enabled), and 'Default Firewall DNS Rule' (Default, Enabled). A modal window titled 'Add DNS Filtering Rule' is open. It contains fields for 'Rule Order' (set to 3), 'Rule Name' (set to 'DNS_1'), 'Rule Status' (set to 'Enabled'), and tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'CRITERIA', there are dropdowns for 'Users' (Any) and 'Groups' (Any), 'Departments' (Any) and 'Locations' (Any), and a 'Time' dropdown set to 'Always'. Under 'ACTION', there are dropdowns for 'Network Traffic' (Allow) and 'Logging' (Full). A large 'DESCRIPTION' text area is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 51 - Slide 51

The screenshot shows the Zscaler DNS Control interface. On the left, there is a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists several existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), 'Unknown DNS Traffic' (Default, Any), and 'Default Firewall DNS Rule' (Default, Any). A modal window titled 'Add DNS Filtering Rule' is open in the center. It has a 'DNS FILTERING RULE' section with 'Rule Order' set to 3, 'Rule Name' to 'Block DNS Tunnels', and 'Rule Status' to 'Enabled'. Below this are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP's', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'DNS APPLICATION' tab is currently selected. The 'CRITERIA' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Full'. At the bottom of the modal is a large empty box for 'DESCRIPTION' and two buttons: 'Save' and 'Cancel'.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), 'Unknown DNS Traffic' (Default, Enabled), and 'Default Firewall DNS Rule' (Default, Enabled). A modal window titled 'Add DNS Filtering Rule' is open in the center. The modal has tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'WHO, WHERE, & WHEN', 'Rule Order' is set to 3 and 'Rule Name' is 'Block DNS Tunnels'. 'Rule Status' is 'Enabled'. In the 'CRITERIA' section, 'DNS Tunnels & Network Apps' and 'Resolved IP-Based Countries' both have 'Any' selected. Under 'DNS Request Type', 'Any' is selected. In the 'ACTION' section, 'Network Traffic' is set to 'Allow' and 'Logging' is set to 'Full'. There's a large 'DESCRIPTION' text area at the bottom. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 53 - Slide 53

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and shows a list of existing DNS filtering rules. One rule is selected, and a modal dialog box is open for 'Add DNS Filtering Rule'. The dialog box has tabs for WHO, WHERE, & WHEN, SOURCE IP's, DESTINATION/RESOL..., and DNS APPLICATION. Under DESTINATION/RESOL..., there are dropdowns for 'DNS Tunnels & Network Apps' (set to Any) and 'DNS Application Group' (set to Any). A modal window titled 'Unselected Items' lists 'espn' with a checkbox next to it. At the bottom of the dialog box are buttons for Done, Cancel, Clear Selection, Save, and Cancel.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for "Rule Order" (set to 3), "Rule Name" (set to "Block DNS Tunnels"), and "Rule Status" (set to "Enabled").
- Add DNS Application Group**: This window has a "Name" field (left empty) and a dropdown menu for "DNS Tunnels & Network Apps" (set to "None"). There's also a "Description" text area and a "Save" button.

At the bottom of the interface, there's a "DESCRIPTION" section with a "Save" and "Cancel" button, and a "Done" button above the "Cancel" button in the top right corner of the modal windows.

Slide notes

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

Slide 55 - Slide 55

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for "Rule Order" (set to 3), "Rule Name" (Block DNS Tunnels), and "Rule Status" (Enabled). It also includes a search bar and a "Done" button at the bottom.
- Add DNS Application Group**: This window has fields for "Name" (DNS Tunnels & Network Apps) and "Description". A dropdown menu shows "None" selected. At the bottom are "Save" and "Cancel" buttons.

Below these modals, a "DESCRIPTION" section is visible with "Done", "Cancel", and "Clear Selection" buttons. The bottom of the screen shows a footer with the text "Copyright 2018 Zscaler Inc. All rights reserved. / Version 5.6 / Page 1".

Slide notes

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

Slide 56 - Slide 56

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for "Rule Order" (set to 3), "Rule Name" (set to "Block DNS Tunnels"), and "Rule Status" (set to "Enabled").
- Add DNS Application Group**: This window has a "Name" field set to "All DNS Tunnels" and a "DNS Tunnels & Network Apps" dropdown set to "None". There's also a "Description" text area and "Save" and "Cancel" buttons.

At the bottom of the screen, there's a large, semi-transparent "DESCRIPTION" box with its own "Save" and "Cancel" buttons, likely a placeholder for additional configuration or notes.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, there's a table listing existing DNS filtering rules. Two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for Rule Order (set to 3), Rule Name (Block DNS Tunnels), and Rule Status (Enabled). It also includes a search bar and a 'Done' button.
- Add DNS Application Group**: This window has a 'Name' field set to 'All DNS Tunnels'. Below it is a 'DNS Tunnels & Network Apps' dropdown set to 'None'. A large 'Unselected Items' section lists several options under 'Commonly Allowed DNS Tunnels', each with a checkbox. Some options are checked (e.g., BostonNews, CCM, Cymru, DeviceScape, OnsTunGoodRsvd). There are 'Save' and 'Cancel' buttons at the bottom.

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

The screenshot shows the Zscaler DNS Control interface. In the background, there's a list of existing DNS filtering rules, including "Office 365 One Click Rule" (Rule Order 1) and "DNS Redirect" (Rule Order 2). A new rule is being created with the following details:

- Rule Order:** 3
- Rule Name:** Block DNS Tunnels
- Rule Status:** Enabled

A modal window titled "Add DNS Application Group" is open, showing a list of items under "Selected Items (19)". The list includes:

- BostonNews
- CCM
- Cymru
- DeviceScape
- DnsTunGoodRsvd
- Eset
- FlyingMag
- Mcafee

The "Unselected Items" section contains a checkbox for "Commonly Allowed DNS Tunnels" and a list of items:

- BostonNews
- CCM
- Cymru
- DeviceScape
- DnsTunGoodRsvd
- Eset
- FlyingMag
- Mcafee

At the bottom of the modal, there are "Done", "Cancel", and "Clear Selection" buttons.

Slide notes

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

Slide 59 - Slide 59

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, there's a table listing existing DNS filtering rules. A modal window titled "Add DNS Filtering Rule" is open, showing fields for Rule Order (set to 3), Rule Name ("Block DNS Tunnels"), and Rule Status ("Enabled"). Below this, another modal window titled "Add DNS Application Group" is open, showing a table of "DNS APPLICATION GROUP". It has a "Name" field set to "All DNS Tunnels" and a "Description" field which is empty. To the right of the table is a list of "Unselected Items" and "Selected Items (19)". The "Selected Items" list includes items like BostonNews, CCM, Cyru, DeviceScape, DnsTunGoodRsvd, Eset, FlyingMag, Ipass, and McAfee. At the bottom of the modal are "Done", "Cancel", and "Clear Selection" buttons.

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

The screenshot shows the Zscaler DNS Control interface. In the background, there's a list of existing DNS filtering rules, including "Office 365 One Click Rule" (Rule Order 1) and "DNS Redirect" (Rule Order 2). A new rule is being created with the following details:

- Rule Order:** 3
- Rule Name:** Block DNS Tunnels
- Rule Status:** Enabled

A modal window titled "Add DNS Application Group" is open, showing a list of items under "Selected Items (28)". The items listed are:

- BaiduYunDns
- BostonNews
- CCM
- Cymru
- DeviceScape
- Hoff
- GoodRsvd
- DnsTunMaliciousRsvd
- Eset
- FlyingMag

The "Unselected Items" section contains many other items, including:

- Community Blocked DNS Tunnels
- BaiduYunDns
- DnsTunMaliciousRsvd
- Hoff
- Kd
- MailShell
- TGIN

At the bottom of the modal, there are "Done" and "Cancel" buttons.

Slide notes

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

Slide 61 - Slide 61

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for "Rule Order" (set to 3), "Rule Name" (Block DNS Tunnels), and "Rule Status" (Enabled). It also includes a search bar and a "Done" button.
- Add DNS Application Group**: This window has a "Name" field set to "All DNS Tunnels" and a "DNS Tunnels & Network Apps" dropdown set to "None". Below these are sections for "Description" and "Selected Items (28)". The "Selected Items" table lists 28 items, including BaiduYunDns, BostonNews, CCM, Cymru, DeviceScape, DnsTunGoodRsvd, DnsTunMaliciousRsvd, Eset, FlyingMag, and others. There are "Unselected Items" and "Selected Items" tabs, a search bar, and "Done" and "Cancel" buttons.

Slide notes

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

Slide 62 - Slide 62

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for "Rule Order" (set to 3), "Rule Name" (set to "Block DNS Tunnels"), and "Rule Status" (set to "Enabled").
- Add DNS Application Group**: This window has a "Name" field set to "All DNS Tunnels". Below it is a table titled "DNS APPLICATION GROUP" with two columns: "Unselected Items" and "Selected Items (48)". The "Unselected Items" column lists various DNS tunnel names like "Unknown DNS Tunnels", "DnsTunCatAuth", etc. The "Selected Items" column lists the same items with a checkmark next to each. At the bottom of this window are "Done", "Cancel", and "Clear Selection" buttons.

At the bottom of the main dashboard, there are "Save" and "Cancel" buttons.

Slide notes

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

Slide 63 - Slide 63

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons and a main dashboard area. In the center, two modal windows are open:

- Add DNS Filtering Rule**: This window has fields for "Rule Order" (set to 3), "Rule Name" (Block DNS Tunnels), and "Rule Status" (Enabled). It also includes a search bar and a "Done" button.
- Add DNS Application Group**: This window has a "Name" field containing "All DNS Tunnels" and a "DNS Tunnels & Network Apps" dropdown menu listing "BaiduYunDns; BostonNews; CCM; Oy...". It features a "Description" text area and "Save" and "Cancel" buttons.

At the bottom of the interface, there's a "DESCRIPTION" section with "Save" and "Cancel" buttons, and a "Selected Items (0)" list.

Slide notes

Save this new DNS Application Group.

Slide 64 - Slide 64

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), 'Unknown DNS Traffic' (Default, Any), and 'Default Firewall DNS Rule' (Default, Any). A modal window titled 'Add DNS Filtering Rule' is open. In the 'DNS FILTERING RULE' section, the 'Rule Order' is set to 3, the 'Rule Name' is 'Block DNS Tunnels', and the 'Rule Status' is 'Enabled'. The 'DESTINATION/RESOL...' tab is selected under 'WHO, WHERE, & WHEN'. In the 'CRITERIA' section, 'DNS Tunnels & Network Apps' is set to 'Any' and 'DNS Application Group' is also set to 'Any'. A dropdown menu shows 'Unselected Items' with 'All DNS Tunnels' checked and 'espn' unchecked. The 'ACTION' section shows 'Network Traffic' and 'Allow'. The 'DESCRIPTION' field is empty. At the bottom of the modal are 'Done', 'Cancel', and 'Clear Selection' buttons, along with 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 65 - Slide 65

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A modal window titled 'Add DNS Filtering Rule' is open. Inside the modal, there are fields for 'Rule Order' (set to 3), 'Rule Name' (Block DNS Tunnels), and 'Rule Status' (Enabled). Below these are sections for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'CRITERIA', there are dropdowns for 'DNS Tunnels & Network Apps' (Any), 'DNS Application Group' (All DNS Tunnels), 'Resolved IP-Based Countries' (Any), and 'Requested Domain/Resolved IP Categories' (Any). The 'DNS Request Type' is set to Any. In the 'ACTION' section, 'Network Traffic' is set to 'Allow' and 'Logging' is set to 'Full'. At the bottom of the modal, there are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and shows a table of existing rules. One rule is highlighted: 'Office 365 One Click Rule' (Rule Order 1, Enabled). Another rule is shown: 'DNS Redirect' (Rule Order 2, Enabled). Below these are two default rules: 'Unknown DNS Traffic' (Default, Any) and 'Default Firewall DNS Rule' (Default, Any). The central part of the screen is a modal window titled 'Add DNS Filtering Rule'. It has a 'DNS FILTERING RULE' section with 'Rule Order' set to 3 and 'Rule Name' set to 'Block DNS Tunnels'. The 'Rule Status' is set to 'Enabled'. Below this are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'CRITERIA', there are sections for 'DNS Tunnels & Network Apps' (Any, All DNS Tunnels), 'Resolved IP-Based Countries' (Any, Any), and 'DNS Request Type' (Any). The 'ACTION' section shows 'Network Traffic' with 'Allow' selected and 'Logging' set to 'Full'. A dropdown menu for 'Action' shows options: 'Allow' (selected), 'Block', 'Redirect Request', and 'Redirect Response'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Slide 67 - Slide 67

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and contains a table of existing DNS filtering rules. A modal window titled 'Add DNS Filtering Rule' is open in the center. The modal has several sections: 'DNS FILTERING RULE' (Rule Order: 3, Rule Name: Block DNS Tunnels, Rule Status: Enabled), 'CRITERIA' (DNS Tunnels & Network Apps: Any, DNS Application Group: All DNS Tunnels; Resolved IP-Based Countries: Any, Requested Domain/Resolved IP Categories: Any; DNS Request Type: Any), 'ACTION' (Network Traffic: Block, Logging: Full), and 'DESCRIPTION' (a large text input field). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

And **Save** the rule.

Slide 68 - Slide 68

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' A search bar at the top right has the placeholder 'Search...'. Below is a table listing DNS filtering rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		Edit Delete
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		Edit Delete
3	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		Edit Delete
Default	Unknown DNS Traffic	Any	Allow		Edit
Default	Default Firewall DNS Rule	Any	Allow		Edit

At the bottom left, there is a copyright notice: 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents'. On the bottom right is a blue circular icon with a white 'Z' and a gear.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and contains a table of existing DNS filtering rules. A modal window titled 'Add DNS Filtering Rule' is open in the center. The modal has several sections: 'DNS FILTERING RULE' (Rule Order: 4, Rule Name: DNS_1, Rule Status: Enabled), 'WHO, WHERE, & WHEN' (selected tab), 'CRITERIA' (Users: Any, Groups: Any, Departments: Any, Locations: Any), 'ACTION' (Network Traffic: Allow, Logging: Full), and 'DESCRIPTION' (an empty text area). At the bottom of the modal are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists several existing DNS filtering rules:

Rule Order	Rule Name	Description
1	Office 365 One Click Rule	DESIRED STATE: OFF
2	DNS Redirect	LOCATION: Site
3	Block DNS Tunnels	DNS APPLICATION: All
Default	Unknown DNS Traffic	Any
Default	Default Firewall DNS Rule	Any

A modal window titled 'Add DNS Filtering Rule' is open. It has a 'DNS FILTERING RULE' section with 'Rule Order' set to 4 and 'Rule Name' set to 'DNS_1'. Below this are tabs for 'WHO, WHERE, & WHEN' (selected), 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'CRITERIA' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), 'Locations' (Any), and 'Time' (Always). The 'ACTION' section shows 'Network Traffic' with 'Allow' selected and 'Logging' with 'Full' selected. A large 'DESCRIPTION' text area is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, prompting for rule details. The 'Rule Order' is set to 3, and the 'Rule Name' is 'DNS_1'. The 'Rule Status' is 'Enabled'. The 'Criteria' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). The 'Time' dropdown is set to 'Always'. The 'Action' section shows 'Network Traffic' with 'Allow' selected and 'Logging' with 'Full' selected. There's a large 'DESCRIPTION' text area at the bottom of the modal. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 72 - Slide 72

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open. It contains fields for 'Rule Order' (set to 3), 'Rule Name' (set to 'DNS_1'), 'Rule Status' (set to 'Enabled'), and a 'Criteria' section. The 'Criteria' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). Below this is a 'Time' dropdown set to 'Always'. The 'Action' section shows 'Network Traffic' (Allow) and 'Logging' (Full). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 73 - Slide 73

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, prompting for a 'Rule Order' (set to 3), 'Rule Name' ('Allow Productive Tunnels'), and 'Rule Status' ('Enabled'). The 'CRITERIA' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Full'. A large 'DESCRIPTION' text area is present at the bottom of the modal. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 74 - Slide 74

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, prompting for a 'Rule Order' (set to 3) and a 'Rule Name' ('Allow Productive Tunnels'). The 'Rule Status' is set to 'Enabled'. The 'CRITERIA' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). The 'Time' dropdown is set to 'Always'. The 'ACTION' section shows 'Network Traffic' (Allow) and 'Logging' (Full). A large 'DESCRIPTION' text area is present at the bottom of the modal. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 75 - Slide 75

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, prompting for a 'Rule Order' (set to 3), a 'Rule Name' ('Allow Productive Tunnels'), and a 'Rule Status' ('Enabled'). The modal also includes tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'CRITERIA', it lists 'DNS Tunnels & Network Apps' (Any) and 'DNS Application Group' (Any). It also includes sections for 'Resolved IP-Based Countries' and 'Requested Domain/Resolved IP Categories', both set to 'Any'. The 'DNS Request Type' is set to 'Any'. In the 'ACTION' section, 'Network Traffic' is set to 'Allow' and 'Logging' is set to 'Full'. A large 'DESCRIPTION' text area is present at the bottom of the modal. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open. It contains fields for 'Rule Order' (set to 3), 'Rule Name' ('Allow Productive Tunnels'), and 'Rule Status' ('Enabled'). Below these are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'CRITERIA', there are dropdowns for 'DNS Tunnels & Network Apps' (set to 'Any') and 'DNS Application Group' (set to 'Any'). A search bar at the top of the modal shows 'mca'. The 'Unselected Items' section lists 'Commonly Allowed DNS Tunnels', 'McAfee', 'Web', and 'Comcast'. Buttons at the bottom of the modal include 'Done', 'Cancel', 'Clear Selection', 'Save', and 'Cancel'.

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

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and contains a table of existing DNS filtering rules:

Rule Order	Rule Name	Description
1	Office 365 One Click Rule	DESIRED STATE: OFF
2	DNS Redirect	LOCKED STATE: Site
3	Block DNS Tunnels	DNS APPLICATION: All
Default	Unknown DNS Traffic	Any
Default	Default Firewall DNS Rule	Any

A modal window titled 'Add DNS Filtering Rule' is open. It has fields for 'Rule Order' (set to 3), 'Rule Name' (set to 'Allow Productive Tunnels'), and 'Rule Status' (set to 'Enabled'). Below these are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'DNS APPLICATION', there's a section for 'DNS Tunnels & Network Apps' with dropdowns for 'Any' under both 'DNS Application Group' and 'Any'. A search bar at the top right of the modal shows 'mca'. At the bottom of the modal are 'Done', 'Cancel', and 'Clear Selection' buttons, along with a 'Save' button at the very bottom.

Slide notes

Click to include **McAfee**

Slide 78 - Slide 78

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, showing a 'DNS FILTERING RULE' section with 'Rule Order' set to 3, 'Rule Name' as 'Allow Productive Tunnels', and 'Rule Status' as 'Enabled'. Below this is a 'CRITERIA' section with 'DNS Tunnels & Network Apps' and 'DNS Application Group' both set to 'Any'. A dropdown menu for selecting items shows 'Eset' selected. At the bottom of the modal are 'Done', 'Cancel', 'Clear Selection', 'Save', and 'Cancel' buttons.

Slide notes

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

Slide 79 - Slide 79

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists several existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), 'Block DNS Tunnels' (Rule Order 3, Enabled), 'Unknown DNS Traffic' (Default, Enabled), and 'Default Firewall DNS Rule' (Default, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, showing a 'DNS FILTERING RULE' configuration. The 'Rule Order' is set to 3, the 'Rule Name' is 'Allow Productive Tunnels', and the 'Rule Status' is 'Enabled'. In the 'CRITERIA' section, under 'DNS Tunnels & Network Apps', both 'DNS Tunnels' and 'DNS Application Group' dropdowns are set to 'Any'. A modal window titled 'Selected Items (1)' is displayed, listing 'Eset' with a checked checkbox. At the bottom of the 'Add DNS Filtering Rule' dialog, there are 'Done', 'Cancel', 'Clear Selection', 'Save', and 'Cancel' buttons.

Slide notes

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

Slide 80 - Slide 80

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open. Inside, a 'DNS FILTERING RULE' section includes fields for 'Rule Order' (set to 3), 'Rule Name' ('Allow Productive Tunnels'), and 'Rule Status' ('Enabled'). Below this is a 'CRITERIA' section with tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP'S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. Under 'DNS APPLICATION', there's a table with columns 'DNS Tunnels & Network Apps' and 'DNS Application Group'. The 'Unselected Items' table contains 'Eset' and 'McAfee'. The 'Selected Items (2)' table also contains 'Eset' and 'McAfee'. At the bottom of the modal are 'Done', 'Cancel', and 'Clear Selection' buttons, with 'Done' being highlighted. At the very bottom of the interface is a footer with copyright information.

Slide notes

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

Slide 81 - Slide 81

The screenshot shows the Zscaler DNS Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. A table lists existing rules: 'Office 365 One Click Rule' (Rule Order 1, Enabled), 'DNS Redirect' (Rule Order 2, Enabled), and 'Block DNS Tunnels' (Rule Order 3, Enabled). A modal window titled 'Add DNS Filtering Rule' is open, prompting for a 'Rule Order' (set to 3), 'Rule Name' ('Allow Productive Tunnels'), and 'Rule Status' ('Enabled'). The 'CRITERIA' section includes fields for 'DNS Tunnels & Network Apps' (selected: 'Eset; McAfee'), 'DNS Application Group' (selected: 'Any'), 'Resolved IP-Based Countries' (selected: 'Any'), and 'Requested Domain/Resolved IP Categories' (selected: 'Any'). The 'DNS Request Type' is set to 'Any'. The 'ACTION' section shows 'Network Traffic' (selected: 'Allow') and 'Logging' (selected: 'Full'). The 'DESCRIPTION' field is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 82 - Slide 82

Rule Order	Rule Name	Criteria	Action	Description	
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		
3	Allow Productive Tunnels	DNS TUNNELS & NETWORK APPS Eset; McAfee	Allow		
4	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		
Default	Unknown DNS Traffic	Any	Allow		
Default	Default Firewall DNS Rule	Any	Allow		

Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

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

The screenshot shows the Zscaler interface with the following details:

- Left Sidebar:** Includes icons for Dashboard, Analytics, Policy (selected), Administration, Activation (with a red notification dot), and Search.
- Top Bar:** Shows "MY ACTIVATION STATUS" as "Editing" and "CURRENTLY EDITING (1)" with the email "admin@training2@safermarch.com".
- Table:** Displays a list of DNS rules. The columns are "Rule Name", "Criteria", "Action", "Description", and "More".

Rule Name	Criteria	Action	Description	More
Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		Edit Delete
NS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		Edit Delete
Allow Productive Tunnels	DNS TUNNELS & NETWORK APPS Eset; McAfee	Allow		Edit Delete
Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		Edit Delete
Unknown DNS Traffic	Any	Allow		Edit
Default Firewall DNS Rule	Any	Allow		Edit
- Bottom Bar:** Shows copyright information "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents" and a "Logout" icon.

Slide notes

Slide 84 - Slide 84

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with a sub-instruction 'You can define rules that control DNS requests and responses.' A message box at the top right says 'Activation Completed!' with a close button. Below this is a table titled 'Add DNS Filtering Rule' with columns: Rule Order, Rule Name, Criteria, Action, Description, and three more columns represented by ellipsis (...). The table lists six rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		
3	Allow Productive Tunnels	DNS TUNNELS & NETWORK APPS Eset; McAfee	Allow		
4	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		
Default	Unknown DNS Traffic	Any	Allow		
Default	Default Firewall DNS Rule	Any	Allow		

At the bottom left, there's a copyright notice: 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents'. On the bottom right is a blue circular icon with a white 'Z' and a gear.

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

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The 'Policy' option is selected and highlighted in blue.

The main content area is titled 'Configure DNS Control Policy'. It displays a table of existing rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		Edit Delete
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		Edit Delete
3	Allow Productive Tunnels	DNS TUNNELS & NETWORK APPS Eset; McAfee	Allow		Edit Delete
4	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		Edit Delete
Default	Unknown DNS Traffic	Any	Allow		Edit
Default	Default Firewall DNS Rule	Any	Allow		Edit

At the bottom of the page, there is a footer bar with the text 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.6 | Patents' and a small circular icon with a question mark.

Slide notes

Slide 86 - Configuring ZIA DNS Resolution Optimization



Configuring ZIA DNS Resolution Optimization

Slide notes

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

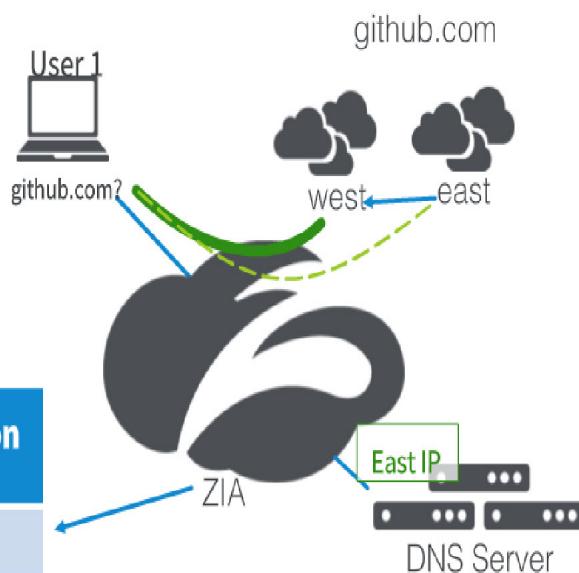
Slide 87 - Configuring ZIA DNS Optimization Settings Software Simulation

Configuring ZIA DNS Optimization Settings Software Simulation

Use case / scenario

- Optimize DNS for organization using Github

	Connection Location
User 1	west



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

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The 'Administration' icon is highlighted. The main area is titled 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' A search bar at the top right contains the placeholder 'Search...'. Below the search bar is a table titled 'Add DNS Filtering Rule' with the following columns: Rule Order, Rule Name, Criteria, Action, Description, and a three-dot menu. The table contains six rows of rules:

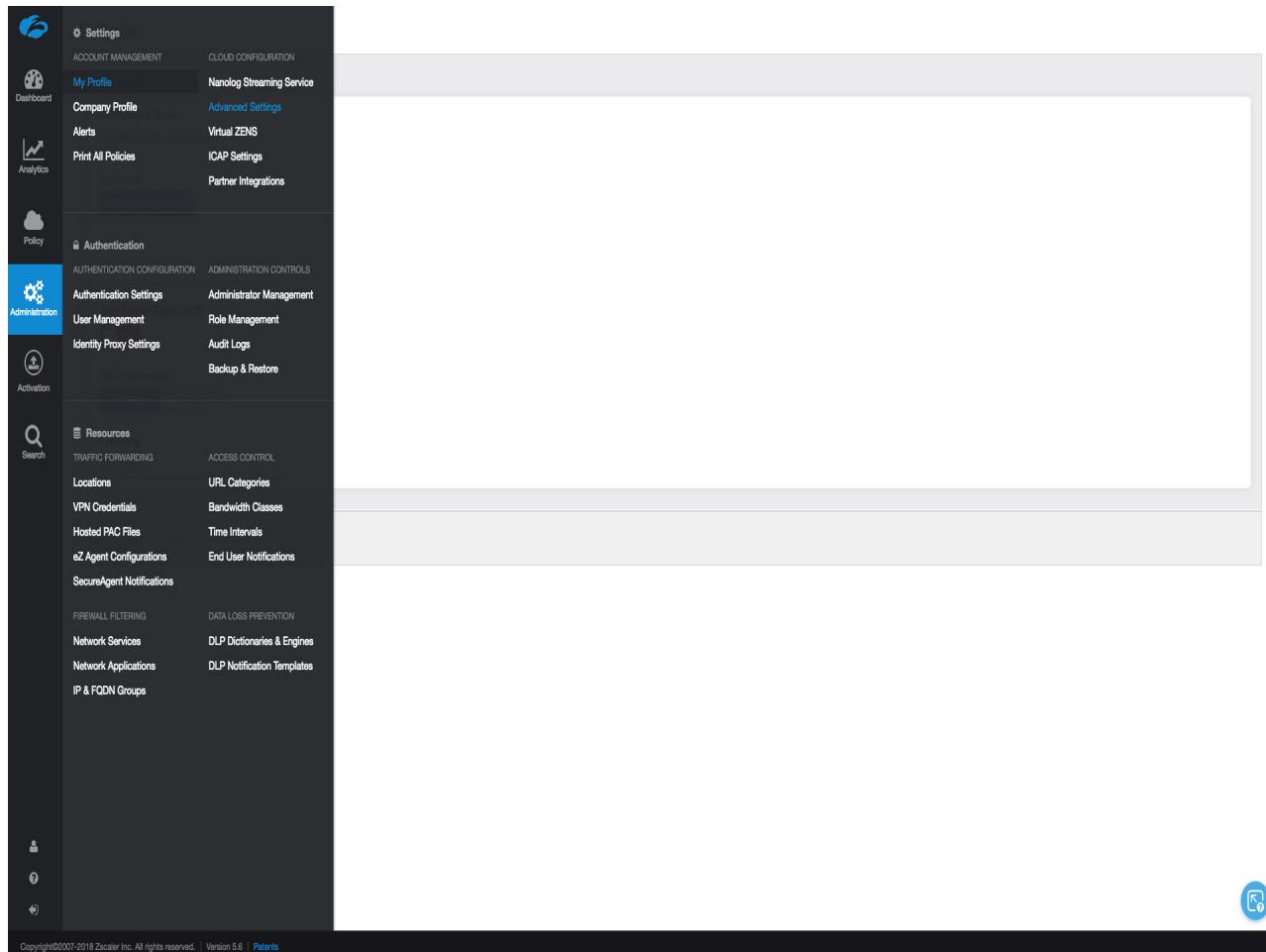
Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow		
2	DNS Redirect	LOCATIONS Site_1	Redirect Request: 1.1.1.1		
3	Allow Productive Tunnels	DNS TUNNELS & NETWORK APPS Eset; McAfee	Allow		
4	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		
Default	Unknown DNS Traffic	Any	Allow		
Default	Default Firewall DNS Rule	Any	Allow		

At the bottom left, there is a copyright notice: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)'. At the bottom right is a blue circular icon with a white 'Z' and a small '6'.

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

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar has 'Administration' selected. The main content area contains several sections:

- ADMIN RANKING**: A toggle switch labeled 'Enable Admin Ranking' is turned off.
- ADVANCED WEB APP CONTROL OPTIONS**: A toggle switch labeled 'Allow Cascading to URL Filtering' is turned off.
- ADMIN UI SESSION TIMEOUT**: A text input field for 'Session Timeout Duration (In Minutes)' is set to 30.
- AUTHENTICATION EXEMPTIONS**:
 - 'Exempted URL Categories' dropdown is set to 'None'.
 - 'Exempted URLs' input field is empty, with a 'Add Items' button.
 - 'Exempted Applications' dropdown is set to 'None'.
- SSL EXEMPTIONS**: A toggle switch labeled 'Enable policies for SSL global exempted domains' is turned off.
- KERBEROS AUTHENTICATION EXEMPTION**:
 - 'Exempted URL Categories' dropdown is set to 'None'.
 - 'Exempted URLs' input field is empty.

At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon with a refresh symbol.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

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

Slide 91 - Slide 91

The screenshot shows the 'Advanced Settings' page of the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Advanced Settings'.

- Block tunneling to non-HTTP/HTTPS ports:** A checkbox is checked.
- SERVICES FORWARDED TO HTTP WEB PROXY:**
 - HTTP Services:** A dropdown menu shows 'HTTP' selected.
 - HTTPS Services:** A dropdown menu shows 'HTTPS' selected.
- SERVICES APPLICABLE TO DNS TRANSACTION POLICIES:**
 - DNS Services:** A dropdown menu shows 'DNS' selected.
- SERVICES FORWARDED TO FTP PROXY:**
 - FTP Services:** A dropdown menu shows 'FTP' selected.
- AUTO PROXY FORWARDING FOR NON-DEFINED PORTS:** Buttons for HTTP, HTTPS, FTP, and DNS are shown, all with checked checkboxes.
- OFFICE 365 ONE CLICK EXCEPTION CONFIGURATION:** A checkbox is unchecked.
- SETTINGS FOR DNS OPTIMIZATION** (with a 'NEW' badge):
 - Optimize DNS Resolution:** A checkbox is checked.

At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon with a refresh symbol.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

Enable **Optimize DNS Resolution**.

Slide 92 - Slide 92

The screenshot shows the 'Advanced Settings' section of the Zscaler interface. It includes the following sections:

- Block tunneling to non-HTTP/HTTPS ports:** A toggle switch is set to .
- SERVICES FORWARDED TO HTTP WEB PROXY:** Includes dropdown menus for **HTTP Services** (set to **HTTP**) and **HTTPS Services** (set to **HTTPS**).
- SERVICES APPLICABLE TO DNS TRANSACTION POLICIES:** Includes dropdown menus for **DNS Services** (set to **DNS**).
- SERVICES FORWARDED TO FTP PROXY:** Includes dropdown menu for **FTP Services** (set to **FTP**).
- AUTO PROXY FORWARDING FOR NON-DEFINED PORTS:** Shows checkboxes for **HTTP** (, , ,) and **DNS** (, , ,) respectively.
- OFFICE 365 ONE CLICK EXCEPTION CONFIGURATION:** Includes a toggle switch for **Enable Office 365 One Click Configuration** () and a note: "Enable if Domain name resolved IP should be overridden by Zscaler service based on ZEN's proximity. By default, ZEN will not override Domain resolved IP for outbound 80/443 connections. This setting is applicable only with Transparent mode connectivity to ZEN." Below this is a checkbox for **Optimize DNS Resolution** () and a link for **Optimize These URL Categories**.
- Buttons:** **Save** and **Cancel**.

At the bottom left, it says "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents".

Slide notes

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

Slide 93 - Slide 93

The screenshot shows the 'Advanced Settings' page under 'DNS'. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has tabs for 'FTP Services' (selected) and 'DNS'. Under 'AUTO PROXY FORWARDING FOR NON-DEFINED PORTS', 'HTTP', 'HTTPS', and 'DNS' are checked. Under 'OFFICE 365 ONE CLICK EXCEPTION CONFIGURATION', 'Enable Office 365 One Click Configuration' is checked. The 'SETTINGS FOR DNS OPTIMIZATION' section contains several dropdown menus and input fields:

- 'Optimize DNS Resolution': 'Optimize'
- 'Optimize These URL Categories': 'None'
- 'Optimize These Cloud Applications': 'None'
- 'Optimize These FQDN': Input field with 'Add Items' button
- 'Do Not Optimize These URL Categories': 'None'
- 'Do Not Optimize These Cloud Applications': 'None'
- 'Do Not Optimize These FQDN': Input field with 'Add Items' button

At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon with a gear and a checkmark.

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

Advanced Settings

FTP Services

FTP

AUTO PROXY FORWARDING FOR NON-DEFINED PORTS

HTTP

HTTPS

FTP

DNS

OFFICE 365 ONE CLICK EXCEPTION CONFIGURATION

Enable Office 365 One Click Configuration

SETTINGS FOR DNS OPTIMIZATION [NEW](#)

Optimize DNS Resolution

Optimize These URL Categories

None

Optimize These Cloud Applications

None

Unselected Items Selected Items (0)

git

Collaboration and Online Meetings

Acrobat Connect

Active Collaboration

GotoMeeting

GotoWebinar

HipChat

Microsoft Teams

Zoom

Done Cancel Clear Selection

Save Cancel

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

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

Slide 95 - Slide 95

The screenshot shows the 'Advanced Settings' page of the Zscaler interface. The 'DNS Optimization' section is active, displaying a search bar with 'git' and a list of selected items. The 'Selected Items (0)' list contains 'System & Development' and 'Github'. At the bottom, there are 'Done', 'Cancel', 'Clear Selection', 'Save', and 'Cancel' buttons.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

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

Slide 96 - Slide 96

The screenshot shows the Zscaler interface with the 'Advanced Settings' tab selected. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays various configuration sections: 'FTP Services' (with 'FTP' selected), 'AUTO PROXY FORWARDING FOR NON-DEFINED PORTS' (HTTP, HTTPS, FTP, DNS all checked), 'OFFICE 365 ONE CLICK EXCEPTION CONFIGURATION' (checkbox checked), and 'SETTINGS FOR DNS OPTIMIZATION' (checkbox checked). A modal window is open over the main content, titled 'SETTINGS FOR DNS OPTIMIZATION'. It contains a list of selected items: 'Unselected Items' (git) and 'Selected Items (1)' (Github). Below the list are buttons for 'Done', 'Cancel', 'Clear Selection', 'Save', and 'Cancel'. At the bottom of the interface, there's a footer with copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents'.

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

The screenshot shows the 'Advanced Settings' page under 'DNS'. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has tabs for 'FTP Services' (selected) and 'DNS'. Under 'AUTO PROXY FORWARDING FOR NON-DEFINED PORTS', 'HTTP', 'HTTPS', and 'DNS' are checked, while 'FTP' is not. Under 'OFFICE 365 ONE CLICK EXCEPTION CONFIGURATION', 'Enable Office 365 One Click Configuration' is checked. The 'SETTINGS FOR DNS OPTIMIZATION' section contains fields for 'Optimize DNS Resolution' (checked), 'Optimize These URL Categories' (set to 'None'), 'Optimize These Cloud Applications' (set to 'Github'), 'Optimize These FQDN' (empty input field with 'Add Items' button), 'Do Not Optimize These URL Categories' (set to 'None'), 'Do Not Optimize These Cloud Applications' (set to 'None'), and 'Do Not Optimize These FQDN' (empty input field with 'Add Items' button). At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon with a gear and a refresh symbol.

Slide notes

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

Slide 98 - Slide 98

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar has 'Administration' selected. The main content area contains several sections:

- ADMIN RANKING**: A section with a toggle switch labeled 'Enable Admin Ranking'.
- ADVANCED WEB APP CONTROL OPTIONS**: A section with a toggle switch labeled 'Allow Cascading to URL Filtering'.
- ADMIN UI SESSION TIMEOUT**: A section with a 'Session Timeout Duration (In Minutes)' input field set to 30.
- AUTHENTICATION EXEMPTIONS**: A section with dropdown menus for 'Exempted URL Categories' (set to 'None') and 'Exempted URLs' (with an 'Add Items' button).
- SSL EXEMPTIONS**: A section with a toggle switch labeled 'Enable policies for SSL global exempted domains'.
- KERBEROS AUTHENTICATION EXEMPTION**: A section with dropdown menus for 'Exempted URL Categories' (set to 'None') and 'Exempted URLs'.

At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon with a refresh symbol.

Slide notes

And **Activate** the changes.

Slide 99 - Slide 99

The screenshot shows the Zscaler Activation interface. The left sidebar has tabs for Dashboard, Analytics, Policy, Administration (selected), Activation (with a red notification dot), and Search. The main content area shows the following:

- MY ACTIVATION STATUS:** Editing, CURRENTLY EDITING (1) admin@training25.zsclearn.com
- QUEUED ACTIVATIONS (0):** None
- OPTIONS:** Force Activate, Activate button
- Session Timeout Details (minutes):** Session timeout is set to 10 minutes.
- Exempted URLs (Categories):** A dropdown menu with options like All, General, and Specific.
- Exempted URLs (URLs):** An input field with placeholder "Add URL" and an "Add Items" button.
- Non-exempted URLs (Categories):** A dropdown menu with options like All, General, and Specific.
- Non-exempted URLs (URLs):** An input field with placeholder "Add URL".
- EXEMPTION:** A section with a checkbox for "Allow passover for DNS, even for exempted domains".
- Generalized URL Categories:** A dropdown menu with options like All, General, and Specific.
- Forward URLs:** A dropdown menu with options like All, General, and Specific.

A message bar at the top right says "All changes have been saved." with a close button. The bottom footer includes copyright information: Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#).

Slide notes

Slide 100 - Slide 100

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar has icons for Dashboard, Analytics, Policy, Administration (selected), Activation, and Search. The main content area has sections for Admin Ranking, Advanced Web App Control Options, Admin UI Session Timeout, Authentication Exemptions, SSL Exemptions, and Kerberos Authentication Exemption. Each section contains configuration fields like checkboxes, dropdowns, and text inputs. A 'Save' button is at the bottom left, and a blue circular icon with a gear and refresh symbol is at the bottom right.

Advanced Settings

ADMIN RANKING

Enable Admin Ranking

ADVANCED WEB APP CONTROL OPTIONS

Allow Cascading to URL Filtering

ADMIN UI SESSION TIMEOUT

Session Timeout Duration (In Minutes)

AUTHENTICATION EXEMPTIONS

Exempted URL Categories

Exempted URLs Add Items

Exempted Applications

SSL EXEMPTIONS

Enable policies for SSL global exempted domains

KERBEROS AUTHENTICATION EXEMPTION

Exempted URL Categories

Exempted URLs

Save Cancel

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

Slide 101 - Thank you & Quiz

Thank you & Quiz

Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

Click the **X** at top right to close this interface, then launch the quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary to pass.