

Slide 1 - Zscaler Policies



Zscaler Policies

Web – Security

©2018 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to the Zscaler Web ‘Security’ Policies Module.

Slide 2 - Navigating the eLearning Module

Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. Overlaid on the bottom of the screen are several blue callout boxes with white text, each pointing to a specific control on the interface:

- Previous Slide
- Next Slide
- Play/Pause
- Fast Forward
- Progress Bar
- Audio On/Off
- Closed Captioning
- Exit

The dashboard itself displays various metrics and charts, including a large donut chart showing 391.3 MB and 16.8 K transactions, and a list of top users.

Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including play and pause, previous, next slide and fast forward. You can also mute the audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the 'X' button at the top to exit.

Slide 3 - Agenda

Agenda

- Web Policy Overview
- Interactive Demo: Web Policy
- Security



Slide notes

In this module, we will cover: an overview of the Web policies available; and a detailed look at the available Web 'Security' policies.

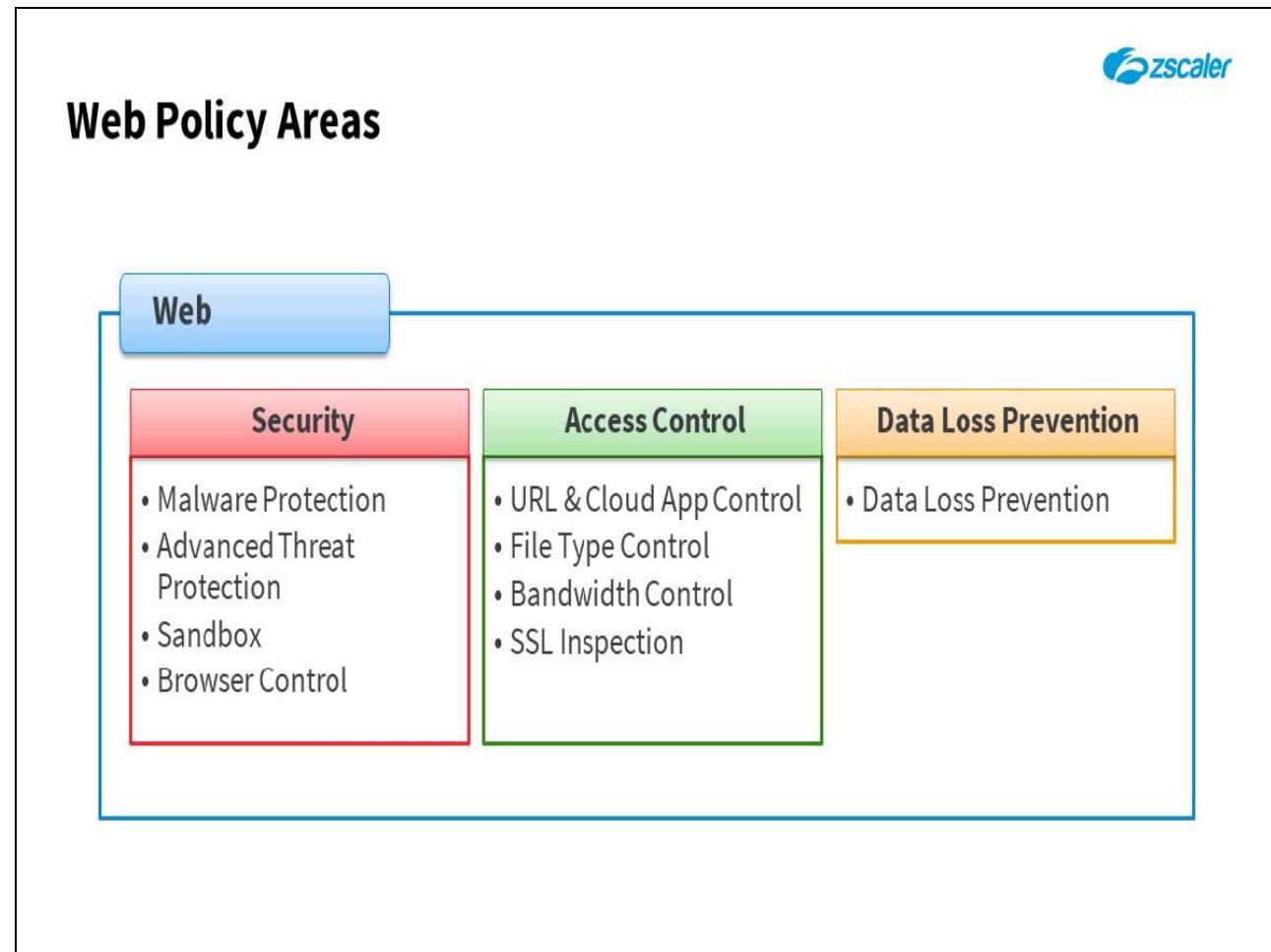
Slide 4 - Web Policy Overview



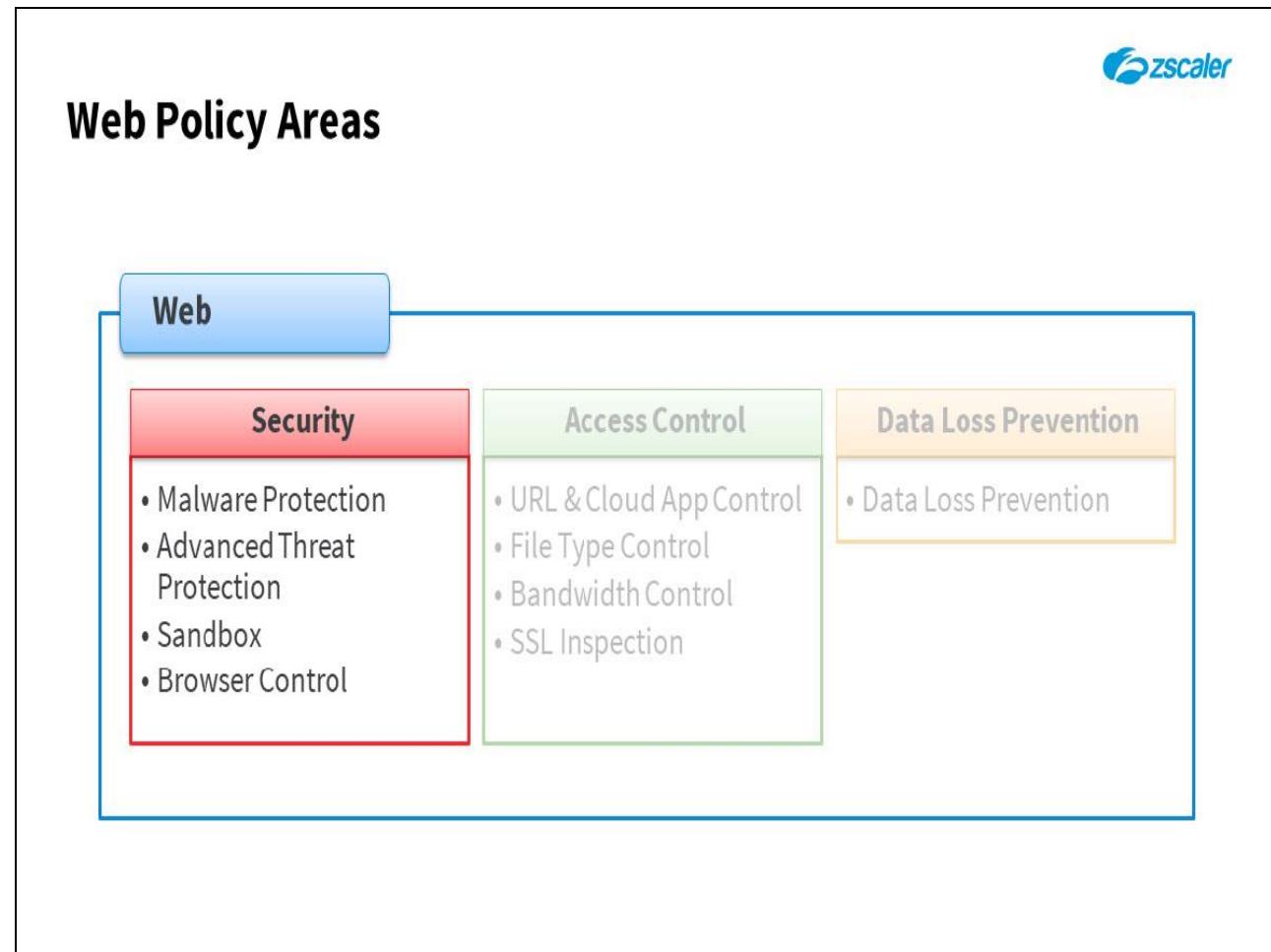
Web Policy Overview

Slide notes

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

Slide 5 - Web Policy Areas**Slide notes**

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

Slide 6 - Web Policy Areas**Slide notes**

In this module, we will look at each of the policies available in the 'Security' category and provide some recommendations for the policy settings.

Slide 7 - Interactive Demo: Web Policy – Security

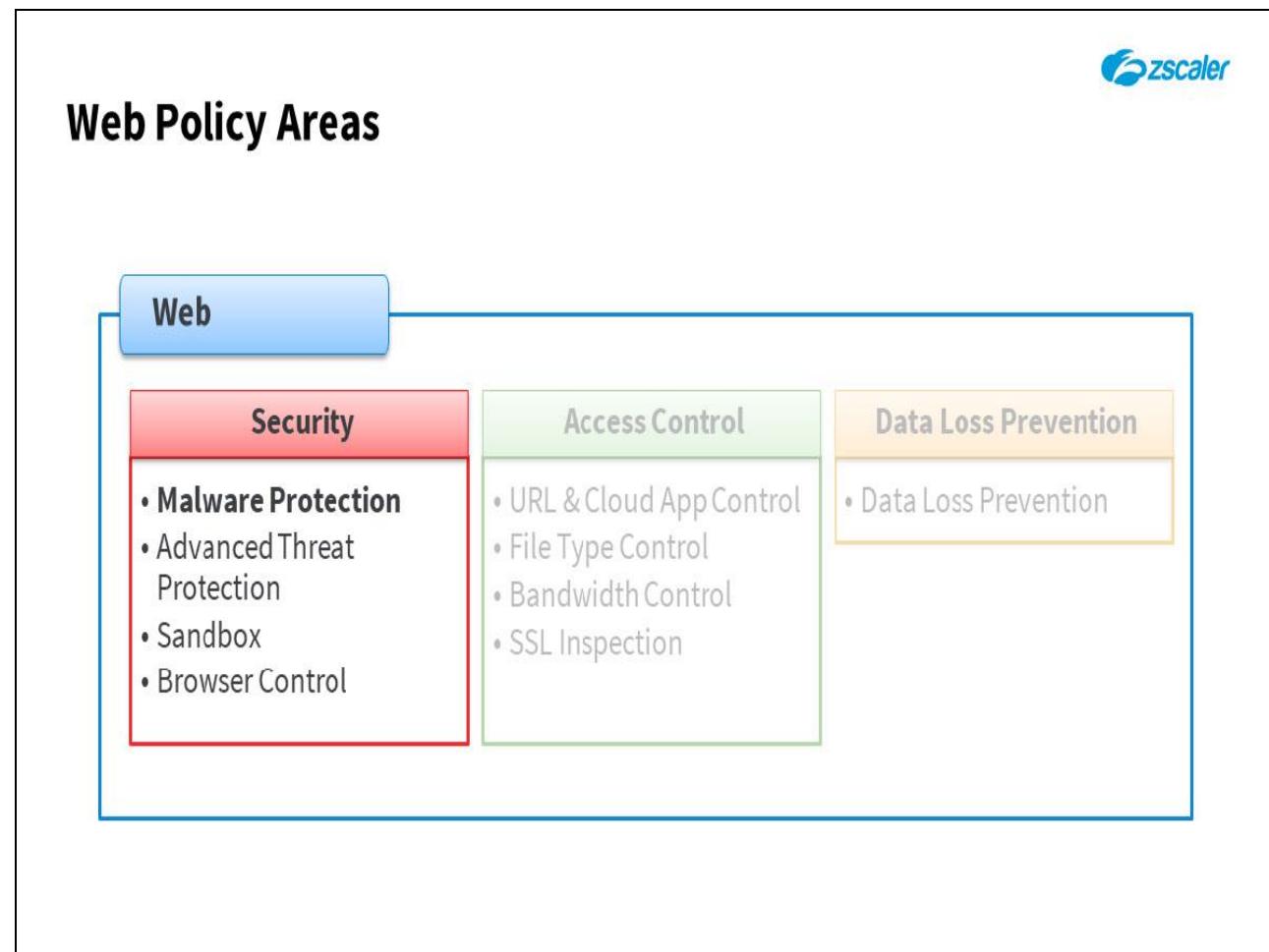


Interactive Demo: Web Policy – Security

Slide notes

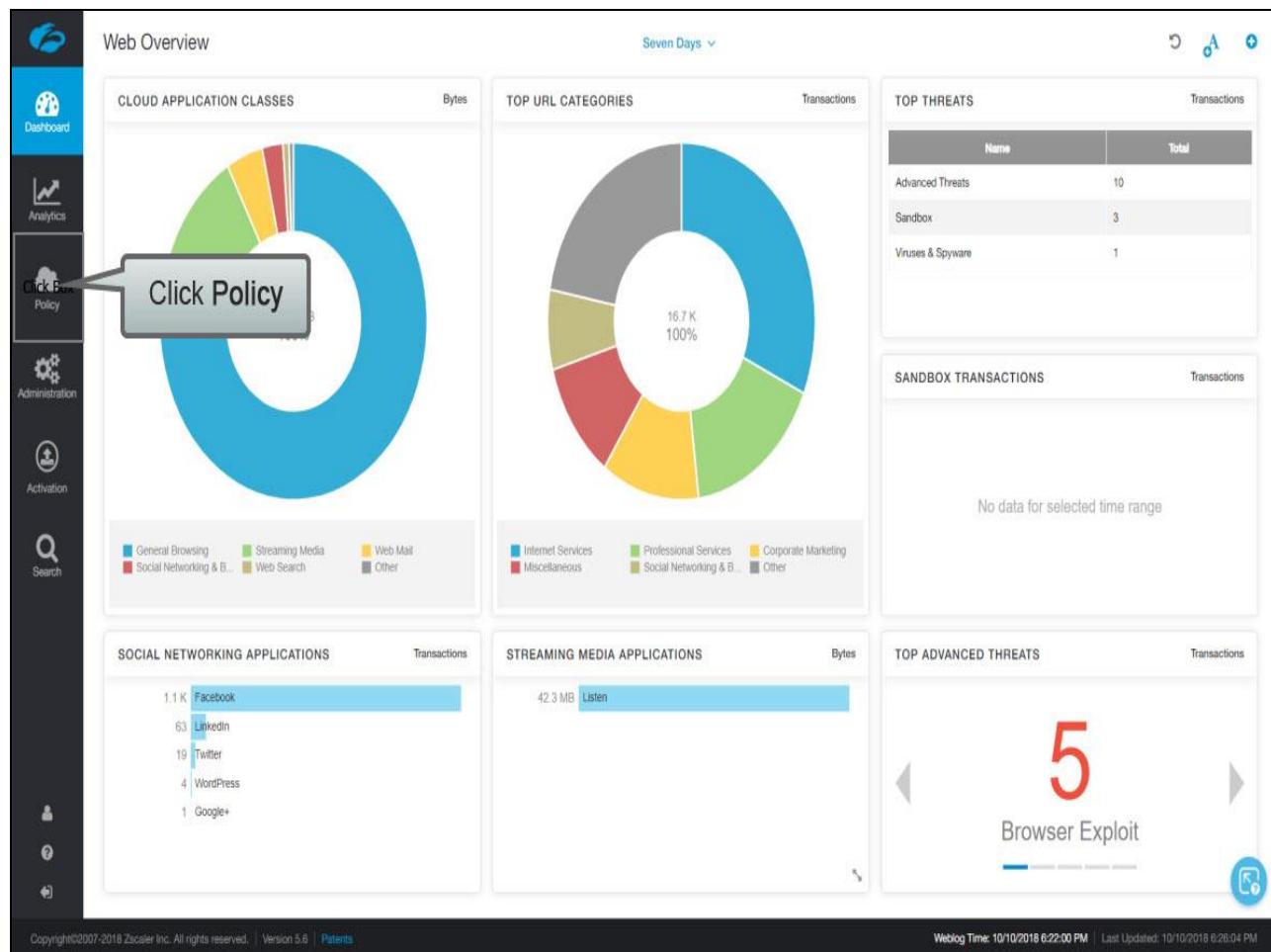
In the next section, we will have a detailed look at the Web ‘Security’ Policies.

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

Slide 8 - Web Policy Areas**Slide notes**

The first policy option that we will look at is 'Malware Protection'. This Policy protects your traffic against 'Malware', 'Adware', and 'Spyware'.

Slide 9 - Slide 9



Slide notes

To access the 'Malware Protection' policy settings, click 'Policy', ...

Slide 10 - Slide 10

The screenshot shows the Zscaler Policy interface. On the left sidebar, under the 'Web' section of the 'Policy' menu, there is a callout box highlighting the 'Malware Protection' option. The main dashboard displays several key metrics and charts:

- TOP URL CATEGORIES:** A donut chart showing traffic distribution across various categories. The data is as follows:

Category	Percentage
Internet Services	16.7 K (100%)
Miscellaneous	~20%
Professional Services	~20%
Social Networking & B.	~10%
Corporate Marketing	~10%
Other	~20%
- TOP THREATS:** A table showing the top threats identified over the last seven days.

Name	Total
Advanced Threats	10
Sandbox	3
Viruses & Spyware	1
- STREAMING MEDIA APPLICATIONS:** A chart showing bandwidth usage for streaming media applications, with 'Listen' being the active state at 42.3 MB.
- TOP ADVANCED THREATS:** A large red '5' indicating the count of browser exploits.

At the bottom of the interface, there is a footer bar with copyright information and a timestamp: "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Policies" and "Weblog Time: 10/10/2018 6:22:00 PM | Last Updated: 10/10/2018 6:28:04 PM".

Slide notes

...then from the 'Web' section of the 'Policy' menu, under the 'SECURITY' heading, click 'Malware Protection'.

Slide 11 - Slide 11

Malware Protection

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

MALWARE POLICY SECURITY EXCEPTIONS

TRAFFIC INSPECTION

Enable Traffic Inspection inbound and outbound

Inspect Inbound Traffic

Inspect Outbound Traffic

PROTOCOL INSPECTION

Inspect HTTP

Inspect FTP over HTTP

Inspect FTP

MALWARE PROTECTION

Viruses

Save Cancel

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

Weblog Time: 10/10/2018 6:22:00 PM | Last Updated: 10/10/2018 6:26:04 PM

Slide notes

The first section on the ‘MALWARE POLICY’ tab controls whether Zscaler inspects your traffic for Malware, and scanning is enabled by default for both outbound, and return traffic. If you disable these options, then Zscaler will not inspect your traffic for Malware at all.

Slide 12 - Slide 12

Malware Protection

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

MALWARE POLICY SECURITY EXCEPTIONS

TRAFFIC INSPECTION

Inspect Inbound Traffic

Inspect Outbound Traffic

PROTOCOL INSPECTION

Inspect HTTP

Inspect FTP over HTTP

Inspect FTP

MALWARE PROTECTION

Viruses

Save Cancel

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

Weblog Time: 10/10/2018 6:22:00 PM | Last Updated: 10/10/2018 6:26:04 PM

Slide notes

In the next section, you can specify which protocols to scan for Malware, the options being HTTP, FTP over HTTP, and native FTP. Note that this is a global setting, and also controls whether traffic is scanned for the Anti-Virus, Anti-Malware, Anti-Spyware, Advanced Threat Protection, and Sandbox policies.

Click to scroll to the bottom of this page.

Slide 13 - Slide 13

Malware Protection

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

MALWARE POLICY SECURITY EXCEPTIONS

MALWARE PROTECTION

Viruses Recommended Policy

Unwanted Applications

Trojans

Worms

ADWARE/SPYWARE PROTECTION

Adware

Spyware

Configure blocking of Malware, Adware, and Spyware

Save Cancel

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

Weblog Time: 10/10/2018 6:22:00 PM | Last Updated: 10/10/2018 6:26:04 PM

Slide notes

The other sections on this page allow you to allow or block various types of ‘Malware’, ‘Adware’, and ‘Spyware’, and by default all of these are enabled.

Slide 14 - Slide 14

The screenshot shows the Zscaler Malware Protection Policy configuration interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Malware Protection' and contains sections for 'MALWARE POLICY' and 'MALWARE PROTECTION'. Under 'MALWARE PROTECTION', there are categories for Viruses, Unwanted Applications, Trojans, and Worms, each with 'Allow' and 'Block' buttons. Below these is an 'ADWARE/SPYWARE PROTECTION' section with 'Adware' and 'Spyware' categories, also with 'Allow' and 'Block' buttons. At the bottom, there are 'Save' and 'Cancel' buttons. A callout box with the text 'Click SECURITY EXCEPTIONS' points to the 'SECURITY EXCEPTIONS' tab in the top navigation bar.

Slide notes

It is possible to configure exceptions to the 'Malware Protection' Policy, and this is done by clicking on the 'SECURITY EXCEPTIONS' tab.

Slide 15 - Slide 15

The screenshot shows the 'Malware Protection' section of the Zscaler interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Malware Protection' and contains a sub-section 'Configure Malware Protection Policy' which states: 'Malware Protection Policy protects your traffic against Malware and Adware/Spyware.' Below this are two tabs: 'MALWARE POLICY' (selected) and 'SECURITY EXCEPTIONS'. Under 'SECURITY EXCEPTIONS', there are two sections: 'Password-Protected Files' and 'Unscannable Files', each with 'Allow' and 'Block' buttons. A callout box highlights the 'Block or Allow special file types' section. At the bottom, there's a field for 'Do Not Scan Content from these URLs' with an 'Add Items' button, and 'Save' and 'Cancel' buttons.

Slide notes

Password protected .ZIP and .RAR files are allowed by default, but you can click 'Block' to stop users from uploading or downloading these types of file. In addition, 'Unscannable Files' are allowed by default, and you also have the option to block them.

Zscaler may not be able to scan some files due to an unrecognized file format, excessive size, or recursive compression. If you elect to block users from downloading or uploading unscannable files, Zscaler will notify the user that the password-protected or unknown file could not be scanned by the AV application, and that the entire transaction has failed.

Slide 16 - Slide 16

The screenshot shows the 'Malware Protection' section of the Zscaler interface. On the left sidebar, there are icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure Malware Protection Policy' and describes it as protecting traffic against Malware and Adware/Spyware. It has tabs for 'MALWARE POLICY' (selected) and 'SECURITY EXCEPTIONS'. Under 'SECURITY EXCEPTIONS', there are sections for 'Password-Protected Files' (with 'Allow' and 'Block' buttons) and 'Unscannable Files' (with 'Allow' and 'Block' buttons). A prominent red box highlights the 'Do Not Scan Content from these URLs' input field, which contains a placeholder 'http://www.google.com'. To the right of this field is a blue 'Add Items' button. Below this section, there are 'Save' and 'Cancel' buttons. A callout bubble with a grey border and white text says 'Add Do Not Scan URLs if necessary'. At the bottom of the page, there is copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and a timestamp: 'Weblog Time: 10/10/2018 6:22:00 PM | Last Updated: 10/10/2018 6:26:04 PM'.

Slide notes

There may be trusted Web sites of partners or vendors, whose webmail or file downloads might otherwise be blocked due to anti-virus, anti-spyware, or anti-malware policies. You can exempt these sites from inspection by adding them to the 'Do Not Scan Content from these URLs' list. Zscaler will allow users to download content from the URLs added here without inspecting the traffic.

Note that this is a global list, and traffic from any of the sites listed here will also bypass anti-virus, anti-malware, anti-spyware, 'Advanced Threat Protection', and 'Sandbox' checks. The syntax for adding URLs here is discussed in the 'Policy Fundamentals' module.

Slide 17 - Slide 17

The screenshot shows the 'Malware Protection' section of the Zscaler interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a title 'Malware Protection' and a sub-section 'Configure Malware Protection Policy' which states 'Malware Protection Policy protects your traffic against Malware and Adware/Spyware.' Below this are two tabs: 'MALWARE POLICY' (selected) and 'SECURITY EXCEPTIONS'. Under 'SECURITY EXCEPTIONS', there are sections for 'Password-Protected Files' and 'Unscannable Files', each with 'Allow' and 'Block' buttons. There is also a field 'Do Not Scan Content from these URLs' with an 'Add Items' button. At the bottom are 'Save' and 'Cancel' buttons. A callout box with a grey background and white text 'Click Recommended Policy' points to a blue link labeled 'Recommended Policy' located in the top right corner of the 'SECURITY EXCEPTIONS' section.

Slide notes

To view Zscaler recommendations for configuring 'Malware Protection' Policy settings, click the 'Recommended Policy' link.

Slide 18 - Slide 18

The screenshot shows the Zscaler Policy Management interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Malware Protection' and contains a 'Configure Malware Protection Policy' section. A 'View Recommended Malware Protection Policy' dialog box is overlaid on the screen. This dialog box contains several configuration sections:

- TRAFFIC INSPECTION:** Includes 'Inspect Inbound Traffic' (checked) and 'Inspect Outbound Traffic' (unchecked).
- PROTOCOL INSPECTION:** Includes 'Inspect HTTP' (checked) and 'Inspect FTP over HTTP' (unchecked).
- MALWARE PROTECTION:** Includes sections for 'Viruses' (checked 'Block'), 'Unwanted Applications' (checked 'Block'), 'Trojans' (checked 'Block'), and 'Worms' (checked 'Block').
- ADWARE/SPYWARE PROTECTION:** Includes sections for 'Adware' (checked 'Block') and 'Spyware' (checked 'Block').

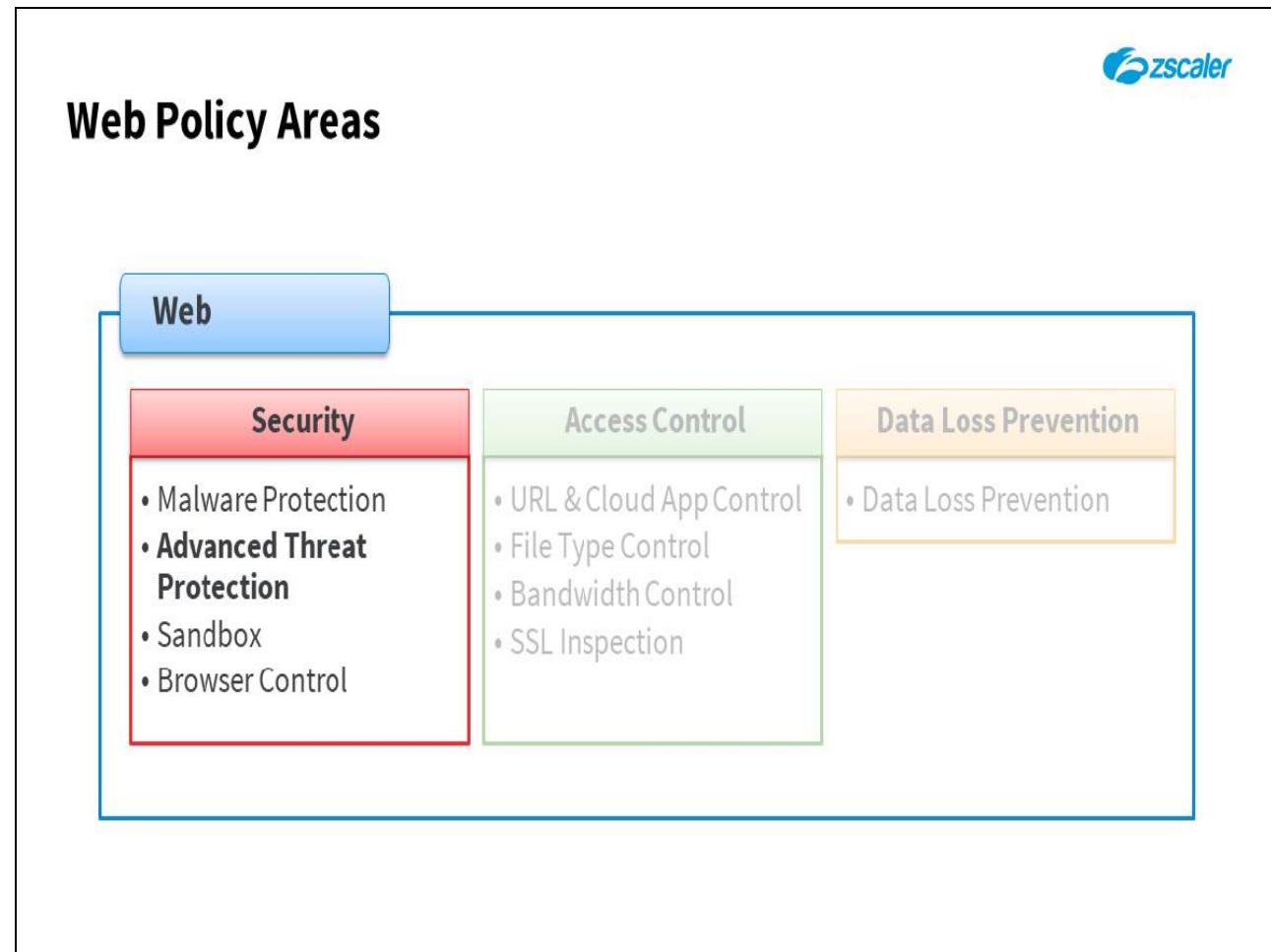
At the bottom of the dialog box, there's a 'Save' button and a 'Cancel' button. The background of the main interface shows a dark theme with some UI elements like a 'Recommended Policy' card.

Slide notes

The 'Malware Protection' Policy applies globally to all of your locations, and the recommended configuration is to:

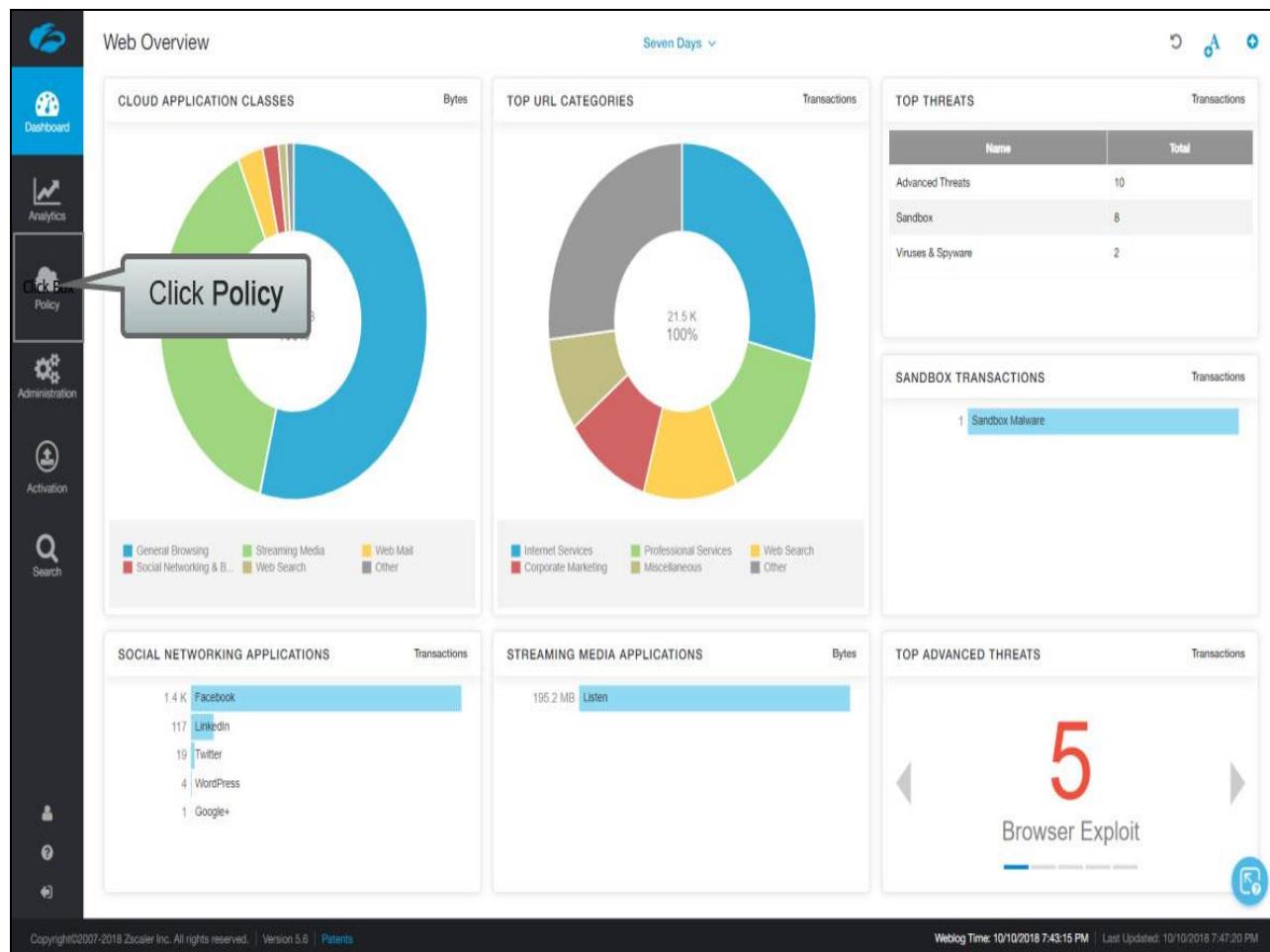
- Enable 'Traffic Inspection' in both directions, and 'Protocol Inspection' for all protocols;
- To set all 'Malware', 'Adware', and 'Spyware' types to 'Block'; with no 'Security Exceptions'.

Be sure to 'Save' and 'Activate' any changes you make to the Policy.

Slide 19 - Web Policy Areas**Slide notes**

The 'Advanced Threat Protection' Policy protects your traffic against 'Botnets', 'Malicious Active Content', 'Fraud', 'Unauthorized Communication', 'Cross-Site Scripting (XSS)', 'Suspicious Destinations', and 'Peer-to-Peer (P2P) File Sharing'.

Slide 20 - Slide 20



Slide notes

To access the 'Advanced Threat Protection' policy settings, click 'Policy', ...

Slide 21 - Slide 21

The screenshot shows the Zscaler Policy interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Activation, and Search. The main area is titled 'Web' under 'SECURITY'. It includes sections for Malware Protection (with 'Advanced Click Box Protection' highlighted), URL & Cloud App Control, File Type Control, Bandwidth Control, and SSL Inspection. Below this, there are sections for Mobile (Zscaler App Configuration, Zscaler App Portal, Mobile Malware Protection, Access Control, Mobile App Store Control), Firewall Filtering (Access Control, Firewall Control, DNS Control, FTP Control), and a general Firewall section.

The main dashboard displays several metrics:

- TOP URL CATEGORIES:** A donut chart showing 21.5 K transactions across categories: Internet Services (blue), Corporate Marketing (red), Professional Services (green), Web Search (yellow), and Miscellaneous (grey).
- TOP THREATS:** A table showing transactions for Advanced Threats (10), Sandbox (8), and Viruses & Spyware (2).
- SANDBOX TRANSACTIONS:** A table showing 1 transaction for 'Sandbox Malware'.
- TOP ADVANCED THREATS:** A section featuring a large red '5' and the text 'Browser Exploit'.

At the bottom, there's a footer with copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Patients'. To the right, it says 'Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM'.

Slide notes

...then from the 'Web' section of the 'Policy' menu, under the 'SECURITY' heading, click 'Advanced Threat Protection'.

Slide 22 - Slide 22

Advanced Threat Protection

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Transfer.

ADVANCED THREATS POLICY **SECURITY EXCEPTIONS**

SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)

Click to set a higher tolerance to risk

Recommended Policy

Low Risk | Moderate Risk | Click Box | High Risk

BOTNET PROTECTION

Command & Control Servers

Allow Block

Set your page risk tolerance

Command & Control Traffic

Allow Block

MALICIOUS ACTIVE CONTENT PROTECTION

Malicious Content & Sites

Allow Block

Vulnerable ActiveX Controls

Allow Block

Browser Exploits

Save Cancel

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

The ‘ADVANCED THREATS POLICY’ tab is broken into two main parts; the ‘Suspicious Content Protection (PageRisk™)’ slider at the top, and the options below it. Note that the page risk tolerance slider is independent of the ‘Block’/‘Allow’ settings below it.

Zscaler calculates the ‘Risk Index’ of a page in real-time by identifying malicious content within the page, such as; injected scripts, vulnerable ActiveX, zero-pixel iFrames, and so on. Simultaneously, Zscaler creates a ‘Domain Risk Index’ using data such as; hosting country, domain age, past results, and links to high-risk top-level domains. The ‘Page Risk’ and ‘Domain Risk’ scores are combined to produce a single Risk Index.

This score is then compared to the page risk tolerance value that you set in this policy. Any sites with a ‘Risk Index’ greater than the page risk tolerance index will be blocked. Click on the slider to set your preferred tolerance to risk.

Slide 23 - Slide 23

The screenshot shows the 'Advanced Threat Protection' section of the Zscaler web interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Configure Advanced Threat Protection Policy' and describes its purpose: 'Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.' Below this, there are tabs for 'ADVANCED THREATS POLICY' (selected) and 'SECURITY EXCEPTIONS'. The 'ADVANCED THREATS POLICY' tab contains several sections: 'SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)' with a slider set at 33 (highlighted with a red box); 'BOTNET PROTECTION' with 'Command & Control Servers' and 'Command & Control Traffic' settings; and 'MALICIOUS ACTIVE CONTENT PROTECTION' with 'Malicious Content & Sites', 'Vulnerable ActiveX Controls', and 'Browser Exploits' settings. A large callout box with the text 'Set your page risk tolerance' points to the slider. At the bottom, there are 'Save' and 'Cancel' buttons.

Slide notes

So to reiterate, the further you move this slider to the right, the more risk you are willing to accept. By default, the page risk tolerance is set to 33.

Slide 24 - Slide 24

The screenshot shows the 'Advanced Threat Protection' section of the Zscaler web interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Advanced Threat Protection' and contains a sub-section titled 'Configure Advanced Threat Protection Policy'. It explains that the policy protects against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. Below this are tabs for 'ADVANCED THREATS POLICY' (selected) and 'SECURITY EXCEPTIONS'. A 'SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)' section shows a risk scale from 'Low Risk' to 'High Risk' with a value of '33'. A red box highlights the 'BOTNET PROTECTION' section, which includes 'Command & Control Servers' and 'Command & Control Traffic' settings, both with 'Allow' and 'Block' buttons. A callout bubble points to the 'Block' button with the text: 'Block or Allow access to malware sites or activity as necessary'. Below this are sections for 'MALICIOUS ACTIVE CONTENT PROTECTION' (with 'Malicious Content & Sites', 'Vulnerable ActiveX Controls', and 'Browser Exploits' settings) and a 'Save' and 'Cancel' button at the bottom. The footer includes copyright information and a help link.

Slide notes

The rest of the page contains 'Block' or 'Allow' controls for: 'BOTNET PROTECTION', ...

Slide 25 - Slide 25

Advanced Threat Protection

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

ADVANCED THREATS POLICY SECURITY EXCEPTIONS

MALICIOUS ACTIVE CONTENT PROTECTION

Malicious Content & Sites

Vulnerable ActiveX Controls

Browser Exploits

File Format Vulnerabilities

Blocked Malicious URLs

Block or Allow access to malware sites or activity as necessary

Add Items

FRAUD PROTECTION

Known Phishing Sites

Suspected Phishing Sites

Save Cancel

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

...‘MALICIOUS ACTIVE CONTENT PROTECTION’, ...

Slide 26 - Slide 26

The screenshot shows the 'Advanced Threat Protection' section of the Zscaler web interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a header 'Configure Advanced Threat Protection Policy' with a sub-header 'Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.' Below this are tabs for 'ADVANCED THREATS POLICY' (selected) and 'SECURITY EXCEPTIONS'. Under 'MALICIOUS ACTIVE CONTENT PROTECTION', there are four sections: 'Malicious Content & Sites' (Allow/Block), 'Vulnerable ActiveX Controls' (Allow/Block), 'Browser Exploits' (Allow/Block), and 'File Format Vulnerabilities' (Allow/Block). A callout box highlights the 'Blocked Malicious URLs' field, which is a text input with a red border and a blue 'Add Items' button. Below this is the 'FRAUD PROTECTION' section with 'Known Phishing Sites' (Allow/Block) and 'Suspected Phishing Sites' (Save/Cancel) buttons. At the bottom, copyright information reads 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Policies' and 'Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM'.

Advanced Threat Protection

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

ADVANCED THREATS POLICY SECURITY EXCEPTIONS

MALICIOUS ACTIVE CONTENT PROTECTION

Malicious Content & Sites

Vulnerable ActiveX Controls

Browser Exploits

File Format Vulnerabilities

Blocked Malicious URLs

Add Items

Configuring a URL Black List if necessary

FRAUD PROTECTION

Known Phishing Sites

Suspected Phishing Sites

Save Cancel

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

...where it is also possible to set up a 'URL Black List'. Add any sites that you explicitly wish to block to the 'Blocked Malicious URLs' field. The syntax for adding URLs here is described in the 'Policy Fundamentals' module.

Slide 27 - Slide 27

Advanced Threat Protection

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

ADVANCED THREATS POLICY SECURITY EXCEPTIONS

FRAUD PROTECTION

Known Phishing Sites Block

Suspected Phishing Sites Block

Spyware Callback Block

Web Spam Block

Crypto Mining Block

Known Adware/Spyware sites Block

UNAUTHORIZED COMMUNICATION PROTECTION

IRC Tunneling

Save Cancel

Block or Allow access to malware sites or activity as necessary

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

The next sections are 'FRAUD PROTECTION', ...

Slide 28 - Slide 28

Advanced Threat Protection

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

ADVANCED THREATS POLICY SECURITY EXCEPTIONS

UNAUTHORIZED COMMUNICATION PROTECTION

IRC Tunneling: Allow Block

SSH Tunneling: Allow Block

Anonymizers: Allow Block

CROSS-SITE SCRIPTING (XSS) PROTECTION

Cookie Stealing: Allow Block

Potentially Malicious Requests: Allow Block

SUSPICIOUS DESTINATIONS PROTECTION

Blocked Countries: China; North Korea; Russia

Save Cancel

Block or Allow access to malware sites or activity as necessary

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

...‘UNAUTHORIZED COMMUNICATION PROTECTION’, ‘CROSS-SITE SCRIPTING (XSS) PROTECTION’, ...

Slide 29 - Slide 29

The screenshot shows the 'Advanced Threat Protection' section of the Zscaler web interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a title 'Advanced Threat Protection' and a sub-section 'Configure Advanced Threat Protection Policy'. It explains that the policy protects against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. Below this are tabs for 'ADVANCED THREATS POLICY' (selected) and 'SECURITY EXCEPTIONS'. Under 'ADVANCED THREATS POLICY', there are four sections: 'SUSPICIOUS DESTINATIONS PROTECTION' (highlighted with a red box and a callout bubble), 'P2P FILE SHARING PROTECTION', 'P2P ANONYMIZER PROTECTION', and 'P2P VOIP PROTECTION'. Each section contains a list of items and 'Allow' or 'Block' buttons. A 'Recommended Policy' button is in the top right. At the bottom are 'Save' and 'Cancel' buttons.

SUSPICIOUS DESTINATIONS PROTECTION

Blocked Countries
China; North Korea; Russia

P2P FILE SHARING PROTECTION

BitTorrent
Allow Block

P2P ANONYMIZER PROTECTION

Tor
Allow Block

P2P VOIP PROTECTION

Google Talk
Allow Block

Block or Allow access to malware sites or activity as necessary

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

...‘SUSPICIOUS DESTINATIONS PROTECTION’, plus a set of ‘P2P PROTECTION’ settings (for Peer-to-Peer connections).

We recommend leaving all these at the default ‘Block’ option, unless you have a specific need.

Slide 30 - Slide 30

The screenshot shows the Zscaler Advanced Threat Protection Policy configuration interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Advanced Threat Protection" and contains several sections:

- Configure Advanced Threat Protection Policy:** Describes what the policy protects against.
- ADVANCED THREATS POLICY:** Shows "Allow" and "Block" buttons. A callout box points to the "Block" button with the text "Click Blocked Countries".
- SUSPICIOUS DESTINATIONS PROTECTION:** Shows a dropdown menu with "Blocked Countries" and a list including "China, North Korea, Russia". A callout box points to this list with the text "Click Blocked Countries".
- P2P FILE SHARING PROTECTION:** Shows "BitTorrent" with "Allow" and "Block" buttons.
- P2P ANONYMIZER PROTECTION:** Shows "Tor" with "Allow" and "Block" buttons.
- P2P VOIP PROTECTION:** Shows "Google Talk" with "Allow" and "Block" buttons.

At the bottom are "Save" and "Cancel" buttons, and a "Help" icon. The footer includes copyright information and a timestamp.

Slide notes

In addition, you can block entire countries if necessary, based on the ISO3166 mapping of countries to their IP address space. This has the effect of blocking all traffic to, or from any IP addresses owned by the countries listed. To add a country to the block list, click in the 'Blocked Countries' field, ...

Slide 31 - Slide 31

The screenshot shows the Zscaler Advanced Threat Protection Policy configuration interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Advanced Threat Protection" and "Configure Advanced Threat Protection Policy". It describes the policy's purpose: "Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing." Below this, there are tabs for "ADVANCED THREATS POLICY" and "SECURITY EXCEPTIONS", with "SECURITY EXCEPTIONS" currently selected. Under "SECURITY EXCEPTIONS", there are "Allow" and "Block" buttons, and a "Recommended Policy" link. The main content area is titled "SUSPICIOUS DESTINATIONS PROTECTION" and shows a "Blocked Countries" section. A modal dialog is open, showing a list of countries under "Unselected Items" and "Selected Items (3)". The "Selected Items" list includes China, North Korea, and Russia. A tooltip "Click Belarus" points to the "Belarus" entry in the "Unselected Items" list. At the bottom of the modal are "Done", "Clear Selection", "Allow", and "Block" buttons, along with "Save" and "Cancel" buttons.

Slide notes

...and click to select the country, or countries to add (in this case 'Belarus').

Slide 32 - Slide 32

The screenshot shows the Zscaler web interface for configuring an Advanced Threat Protection Policy. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled "Advanced Threat Protection" and "Configure Advanced Threat Protection Policy". It describes the policy's purpose of protecting traffic against various threats. Below this, there are tabs for "ADVANCED THREATS POLICY" and "SECURITY EXCEPTIONS", with "SECURITY EXCEPTIONS" currently selected. A "Block" button is visible. A callout bubble points to a "Click Box" on the "Block" button with the text "Click Done". The "Suspicious Destinations Protection" section lists "Blocked Countries" with entries for China, North Korea, and Russia. A "Selected Items (4)" list includes Belarus, China, North Korea, and Russia. At the bottom, there are "Save" and "Cancel" buttons.

Slide notes

Note that 'Whitelisted URLs' take precedence over this list. If a white listed URL is hosted on a web server in a blocked country, the service will still allow users to download content from that site.

Having made changes to this policy, click 'Done', ...

Slide 33 - Slide 33

The screenshot shows the Zscaler Advanced Threat Protection policy configuration interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Advanced Threat Protection" and contains several sections:

- Configure Advanced Threat Protection Policy:** Describes what the policy protects against.
- ADVANCED THREATS POLICY:** Shows tabs for "Allow" and "Block". A "Recommended Policy" button is present.
- SUSPICIOUS DESTINATIONS PROTECTION:** Shows a dropdown menu with "Blocked Countries" containing "Belarus; China; North Korea; Russia".
- P2P FILE SHARING PROTECTION:** Shows a dropdown menu with "BitTorrent" and "Allow" and "Block" buttons.
- P2P ANONYMIZER PROTECTION:** Shows a dropdown menu with "Tor" and "Allow" and "Block" buttons.
- P2P VOIP PROTECTION:** Shows a dropdown menu with "Google" and "Allow" and "Block" buttons. A callout bubble points to the "Click Box" button with the text "Click Save".

At the bottom, there is copyright information: "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients". On the right, it says "Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM".

Slide notes

...then click 'Save'.

Slide 34 - Slide 34

The screenshot shows the 'Advanced Threat Protection' configuration page. At the top, a message says 'All changes have been saved.' Below it, a section titled 'Configure Advanced Threat Protection Policy' describes what the policy protects against. The main interface is divided into several sections:

- ADVANCED THREATS POLICY**: A tab labeled 'SECURITY EXCEPTIONS' is selected. It features a 'SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)' slider set at '33'. Below the slider are three categories: 'BOTNET PROTECTION', 'MALICIOUS ACTIVE CONTENT PROTECTION', and 'PUPPETEERING PROTECTION'. Each category has an 'Allow' or 'Block' button.
- BOTNET PROTECTION**: Includes settings for 'Command & Control Servers' and 'Command & Control Traffic', both with 'Allow' and 'Block' buttons.
- MALICIOUS ACTIVE CONTENT PROTECTION**: Includes settings for 'Malicious Content & Sites', 'Vulnerable ActiveX Controls', and 'Browser Exploits', all with 'Allow' and 'Block' buttons.
- PUPPETEERING PROTECTION**: This section is partially visible below the other categories.
- Buttons**: At the bottom left are 'Save' and 'Cancel' buttons. At the bottom right is a blue circular icon with a white 'Z'.

On the far left, a vertical sidebar lists navigation icons: Dashboard, Analytics, Policy, Administration, Activation, and Search. At the bottom of the page, there is copyright information and a timestamp.

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

Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM

Slide notes

Slide 35 - Slide 35

The screenshot shows the Zscaler Advanced Threat Protection Policy configuration interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation (which is highlighted with a red circle), and Search. The main content area is titled 'Advanced Threat Protection' and 'Configure Advanced Threat Protection Policy'. It explains that the policy protects against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. The 'SECURITY EXCEPTIONS' tab is selected. Under 'SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)', there is a risk slider set at 33, with markers for Low Risk, Moderate Risk, and High Risk. The 'BOTNET PROTECTION' section contains a 'Command & Control Traffic' section with 'Allow' and 'Block' buttons, where 'Block' is selected. The 'MALICIOUS ACTIVE CONTENT PROTECTION' section includes sections for 'Malicious Content & Sites', 'Vulnerable ActiveX Controls', and 'Browser Exploits', each with 'Allow' and 'Block' buttons, all set to 'Block'. At the bottom are 'Save' and 'Cancel' buttons, and a 'Logout' icon.

Slide notes

Then to activate your changes, click 'Activation', ...

Slide 36 - Slide 36

The screenshot shows the Zscaler Policy Web Security interface. On the left, a dark sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation (with a red notification badge), and Search. The main area has a light gray header with 'MY ACTIVATION STATUS' set to 'ON'. Below this, a section titled 'CURRENTLY EDITING (1)' shows a policy for 'admin@pilot.zscaler.com'. A 'SECURITY EXCEPTIONS' section indicates 'None'. A 'PROTECTION' section includes a 'Force Activate' checkbox and a 'Click Box' button, which is highlighted with a large blue rectangular callout containing the text 'Click Activate'. A risk slider is positioned between 'Low Risk' and 'High Risk', with the value '33' indicated. A 'Recommended Policy' button is also present. At the bottom, copyright information reads 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Policies' and a footer note says 'Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM'.

Slide notes

...and click 'Activate'.

Slide 37 - Slide 37

The screenshot shows the Zscaler Advanced Threat Protection Policy configuration interface. At the top, a message says "Activation Completed!" with a close button. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled "Configure Advanced Threat Protection Policy". It includes a brief description of what the policy protects against. Below this are tabs for "ADVANCED THREATS POLICY" (selected) and "SECURITY EXCEPTIONS". Under "ADVANCED THREATS POLICY", there's a section for "SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)" with a risk slider set at 33, ranging from Low Risk to High Risk. There are sections for "BOTNET PROTECTION" (with "Command & Control Servers" and "Command & Control Traffic" settings), "MALICIOUS ACTIVE CONTENT PROTECTION" (with "Malicious Content & Sites", "Vulnerable ActiveX Controls", and "Browser Exploits" settings), and a "Save" and "Cancel" button at the bottom right.

Slide notes

Slide 38 - Slide 38

The screenshot shows the Zscaler Advanced Threat Protection Policy configuration interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Advanced Threat Protection' and contains several tabs: 'ADVANCED THREATS POLICY', 'SUSPICIOUS CONTENT PROTECTION (PAGE 1 OF 2)', 'BOTNET PROTECTION', and 'MALICIOUS ACTIVE CONTENT PROTECTION'. Under 'ADVANCED THREATS POLICY', there is a 'SECURITY EXCEPTIONS' tab highlighted with a callout box containing the text 'Click SECURITY EXCEPTIONS'. Other sections include 'Command & Control Servers' (Allow or Block), 'Command & Control Traffic' (Allow or Block), 'Malicious Content & Sites' (Allow or Block), 'Vulnerable ActiveX Controls' (Allow or Block), and 'Browser Exploits'. At the bottom are 'Save' and 'Cancel' buttons, and a status bar at the bottom right indicates 'Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM'.

Slide notes

You can configure exceptions to the 'Advanced Threat Protection' Policy, and this is done by clicking on the 'SECURITY EXCEPTIONS' tab.

Slide 39 - Slide 39

The screenshot shows the 'Advanced Threat Protection' section of the Zscaler web interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a title 'Advanced Threat Protection' and a sub-section 'Configure Advanced Threat Protection Policy'. It explains that the policy protects against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. Below this are tabs for 'ADVANCED THREATS POLICY' (selected) and 'SECURITY EXCEPTIONS'. Under 'SECURITY EXCEPTIONS', there is a red box around a text input field labeled 'Do Not Scan Content from these URLs' and a button 'Add Items'. A callout box points to this area with the text 'Add Bypassed URLs if necessary'. In the top right corner, there is a link 'Click Recommended Policy' with a callout box pointing to it. At the bottom, there are 'Save' and 'Cancel' buttons. The footer contains copyright information 'Copyright©2007-2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Patients', along with a timestamp 'Weblog Time: 10/10/2018 7:43:15 PM | Last Updated: 10/10/2018 7:47:20 PM'.

Slide notes

In this case, only a 'Do Not Scan Content from these URLs' configuration can be added as an exception. Once again, the syntax for adding URLs here is exactly the same as for the 'Do Not Scan' list that we looked at under 'Malware Protection'.

To see Zscaler recommendations for configuring 'Advanced Threat Protection' Policy settings, click the 'Recommended Policy' link.

Slide 40 - Slide 40

The screenshot shows the 'View Recommended Advanced Threat Protection Policy' dialog box over a dark background. The dialog has a blue header bar with the title. Below it, there's a section titled 'Configure Advanced Threat Protection Policy' with a brief description. A horizontal slider for 'SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)' is set to 35, with 'Low Risk' on the left and 'High Risk' on the right. Under 'BOTNET PROTECTION', 'Command & Control Servers' and 'Command & Control Traffic' both have 'Block' selected. In 'MALICIOUS ACTIVE CONTENT PROTECTION', 'Malicious Content & Sites' and 'Vulnerable ActiveX Controls' both have 'Block' selected. Under 'FRAUD PROTECTION', 'Known Phishing Sites' and 'Suspected Phishing Sites' both have 'Block' selected. 'Spyware Callback' and 'Web Spam' also have 'Block' selected. 'Crypto Mining' and 'Known Adware/Spyware sites' both have 'Block' selected. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons. The background shows a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search, along with a footer with copyright information.

Slide notes

For the 'Advanced Threat Protection' Policy, Zscaler recommends that you:

- Set the page risk index to the 'Low Risk' area of the scale (the default level is 33);
- Block all of the advanced threats;
- And do not add any exceptions.

Slide 41 - Slide 41

The screenshot shows the 'Advanced Threat Protection' configuration page. A modal window titled 'View Recommended Advanced Threat Protection Policy' is open, displaying various threat protection settings with 'Allow' or 'Block' buttons:

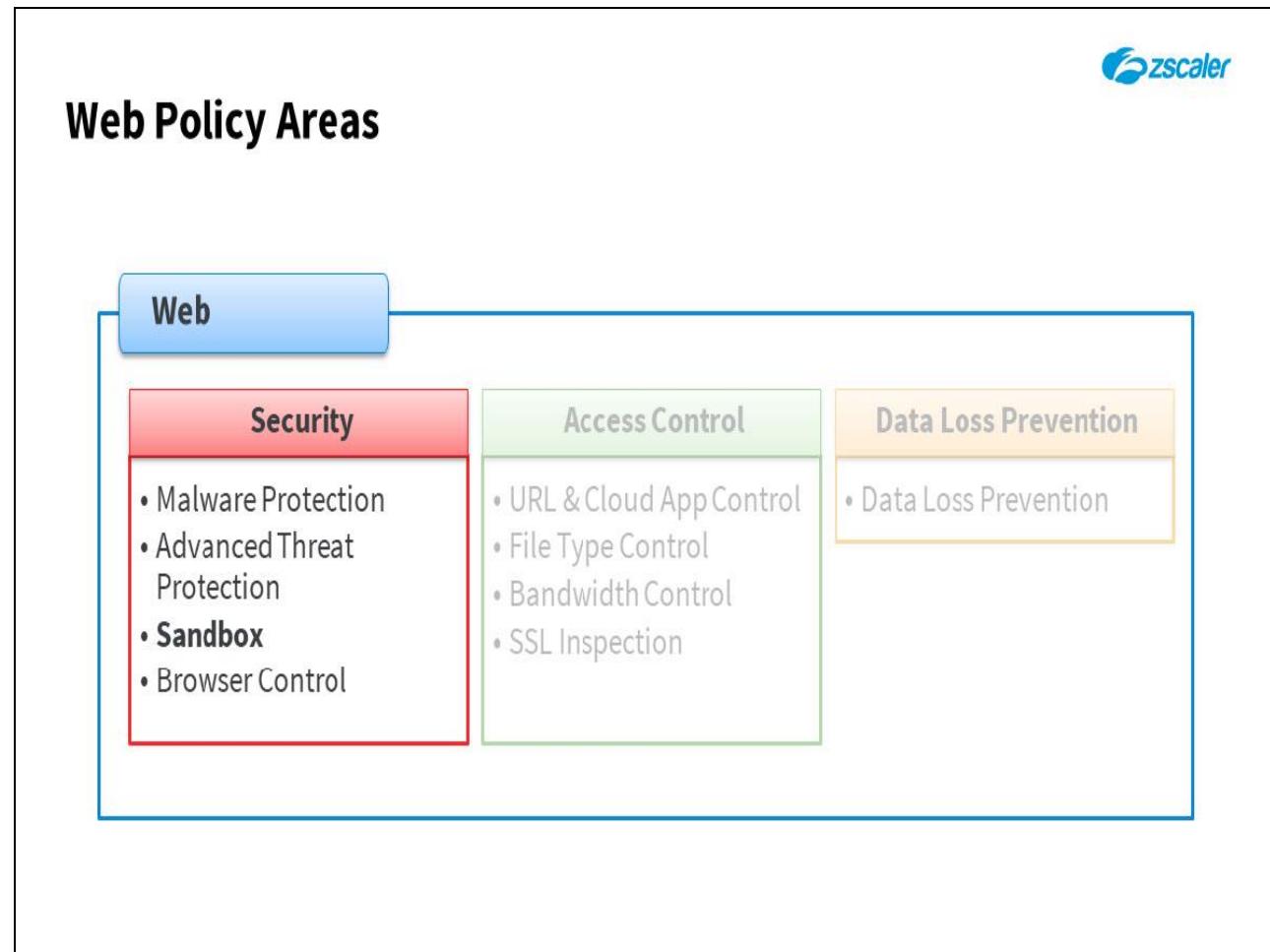
- Crypto Mining:** Block (selected)
- Known Adware/Spyware sites:** Block (selected)
- UNAUTHORIZED COMMUNICATION PROTECTION:**
 - IRC Tunneling:** Block (selected)
 - SSH Tunneling:** Block (selected)
 - Anonymizers:** Block (selected)
- CROSS-SITE SCRIPTING (XSS) PROTECTION:**
 - Cookie Stealing:** Block (selected)
 - Potentially Malicious Requests:** Block (selected)
- P2P FILE SHARING PROTECTION:**
 - BitTorrent:** Block (selected)
- P2P ANONYMIZER PROTECTION:**
 - Tor:** Block (selected)
- P2P VOIP PROTECTION:**
 - Google Talk:** Block (selected)

At the bottom of the modal, there is a note: 'Recommended Policy'.

On the left sidebar, other policy categories like 'ADVANCED THREATS POLICY', 'SECURITY EXCEPTIONS', and 'Do Not Scan Content from these URLs' are visible. At the bottom of the sidebar, there are links for 'Copyright © 2018 Zscaler Inc. All rights reserved.' and 'Version 5.6'.

Slide notes

One thing to note though, some peer-to-peer applications like Google Talk, or Skype would need to be explicitly enabled in this policy.

Slide 42 - Web Policy Areas**Slide notes**

The 'Sandbox' Policy allows the creation of rules for the scanning and execution of files in a Zscaler sandbox environment, to be sure that any malicious content is 'detonated' safely. This provides an additional layer of security against 0-day, and Advanced Persistent Threats (APTs).

Sandbox policy rules are evaluated in the order listed, and rule evaluation stops at the first match. There is a default 'Allow and Scan' rule for all the Sandbox categories.

A detailed report on any files found to be malicious is available through the logs, a 'SANDBOX PATIENT 0 EVENTS' widget is available on the 'Security' Dashboard, plus email alerts on any discovered 0 Day threats can be configured.

Slide 43 - What is Zscaler Sandbox?

What is Zscaler Sandbox?



In-Line Zero-Day Malware Protection

- Always in-line, for all users, everywhere
- Consistent policy enforcement – all users, all devices
- Inspect all files, including on SSL encrypted connections
- Uses the latest threat intelligence
- Immediately block new threats as they are discovered
- Observes and defeats malware evasion techniques
- Sandbox all unknown traffic and files from suspicious locations

Slide notes

The Zscaler Cloud Sandbox service allows you to detect and neutralize even ‘Zero-Day’ threats. Because Zscaler’s Sandbox service is in-line, it sits between your users and the internet no matter where they connect from, to analyze unknown files for zero-day and advanced threats. Cover every user regardless of location from the cloud, whether on or off network everyone gets the exact same protection, without cumbersome VPNs or costly MPLS links. We can even inspect incoming files on SSL encrypted connections to ensure we detect and neutralize all inbound zero-day threats.

As with all our services we make use the latest threat intelligence, plus we can detect previously unreported threats by ‘detonating’ an unknown file in our sandbox environment, to see what it does and what traffic it may generate (e.g. botnet communications or attempted data extraction). We even recognize and neutralize attempts by malware to evade sandbox detection. All unknown files from suspicious locations will be sandboxed, including the blocking of all executable files.

Slide 44 - What is Zscaler Sandbox?

What is Zscaler Sandbox?



In-Line Zero-Day Malware Protection

- Always in-line, for all users, everywhere
- Consistent policy enforcement – all users, all devices
- Inspect all files, including on SSL encrypted connections
- Uses the latest threat intelligence
- Immediately block new threats as they are discovered
- Observes and defeats malware evasion techniques
- Sandbox all unknown traffic and files from suspicious locations

One out of every 300 files sent to Sandbox is new, detonated, and found to be malicious (Fall 2018)

Slide notes

Note that currently (Fall 2018), we find that 1 in every 300 files sent to our Cloud Sandbox, are found to be malicious when detonated.

Slide 45 - Sandbox Subscription Levels and Threat Score

Sandbox Subscription Levels and Threat Score

Standard

- Included with Business Suite
- Limited file types:
.exe, .dll
- Maximum file size restriction: **2MB**
- No policy control
- No quarantine
- No reporting

Slide notes

The 'Standard' Sandbox subscription is included with our 'Business Suite' and provides a basic level of protection against zero-day threats:

- Only the .exe and .dll file types from 'suspicious' URL categories are scanned and blocked, the suspicious categories being: 'Misc./unknown', 'Nudity', 'Pornography', 'Web host', 'File host', 'Shareware download', and 'Anonymizer'.
- The maximum size of file that can be scanned is 2MB;
- Policy control rules cannot be created;
- There is no option to apply the 'Quarantine' action (scan and detonate the file before it is downloaded);
- And there is no detailed Sandbox reporting.

Slide 46 - Sandbox Subscription Levels and Threat Score

Sandbox Subscription Levels and Threat Score

Standard	Advanced
<ul style="list-style-type: none">Included with Business SuiteLimited file types: .exe, .dllMaximum file size restriction: 2MBNo policy controlNo quarantineNo reporting	<ul style="list-style-type: none">Additional subscriptionAll available file types: .exe, .dll, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .rar, .rtf, .zip, suspicious scripts in .zipMaximum file Size: 20MB (50MB for .apk)Granular policy controlQuarantine optionFull IOC and Patient 0 reporting/alerting

Slide notes

The 'Advanced' Sandbox subscription provides a much more comprehensive level of zero-day protection:

- The file types that can be scanned are: .exe, .dll, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .rar, .rtf, .zip, plus any suspicious scripts within a .zip file.
- The maximum file size that can be scanned is 20MB (or 50MB for Android .apk files);
- Granular Sandbox policy rules can be created and assigned, and the 'Quarantine' action is available within them.
- Plus, there is full 'Indicator of Compromise' (IOC) reporting, as well as a 'Patient 0' widget on the 'Security' Dashboard for full visibility into newly discovered threats. Email alerts for any newly discovered 0 Day threats can be enabled and configured from the 'Administration > Alerts' page.

Slide 47 - Sandbox Subscription Levels and Threat Score

Sandbox Subscription Levels and Threat Score

Standard

- Included with Business Suite
 - Limited file types:
 .exe, .dll
 - Maximum file size restriction: **2MB**
 - No policy control
 - No quarantine
 - No reporting
- Sandbox Threat Scoring (Out of 100)

Advanced

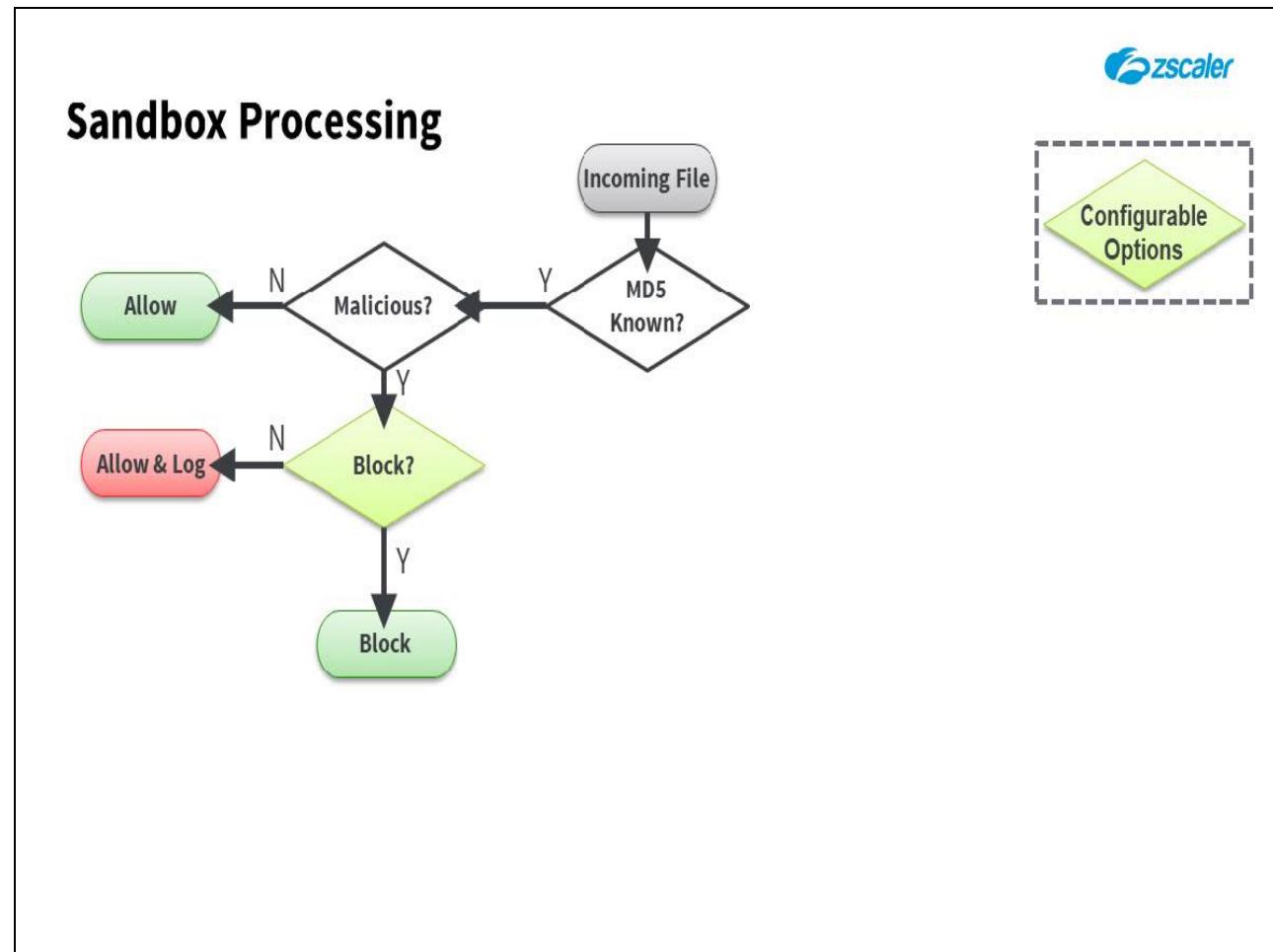
- Additional subscription
- All available file types:
 .exe, .dll, .jar, .pdf, .swf, .doc(x),
 .xls(x), .ppt(x), .apk, .rar, .rtf, .zip,
 suspicious scripts in .zip
- Maximum file Size: **20MB** (50MB for .apk)
- Granular policy control
- Quarantine option
- Full IOC and **Patient 0** reporting/alerting

Benign ↘ 40 ↗ Suspicious, not blocked ↘ 70 ↗ Malicious, blocked

Slide notes

Under the covers, the Sandbox makes decisions about files based on a hard-coded ‘Risk Score’ (in addition to the configurable ‘Page Risk Score’ in the ‘Advanced Threat Protection’ policy). A file’s ‘Risk Score’ is out of ‘100’ and it is determined when analyzing the file. Anything that scores above ‘70’ is deemed ‘Malicious’ and will be blocked and black-listed; anything that scores below ‘40’ is considered ‘Benign’ and will be white-listed; anything in between is considered ‘Suspicious’ but will not be automatically blocked.

Slide 48 - Sandbox Processing



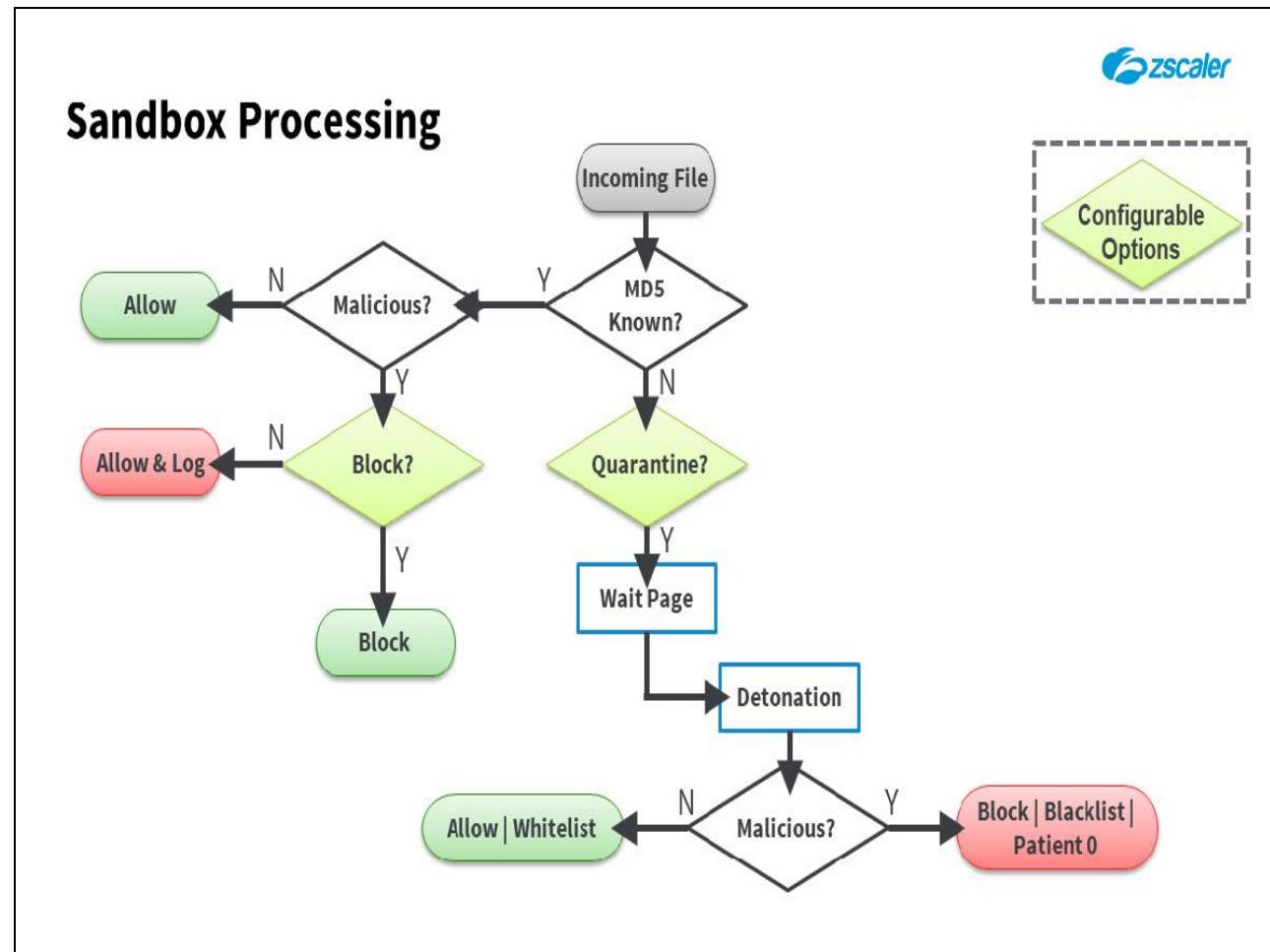
Slide notes

The processing flow for our Cloud Sandbox starts when we detect an incoming file, and if the MD5 hash for the file is already known, we can make an immediate forwarding decision:

- If it is already known to be benign, we will simply allow the download;
- If it is known to be malicious you can configure the behavior, whether to simply block (the safest option), or to allow it to proceed and log the event.

If you allow and log malicious files then the service can be considered to be an 'Intrusion Detection System' only (IDS), rather than a full 'Intrusion Prevention System' (IPS).

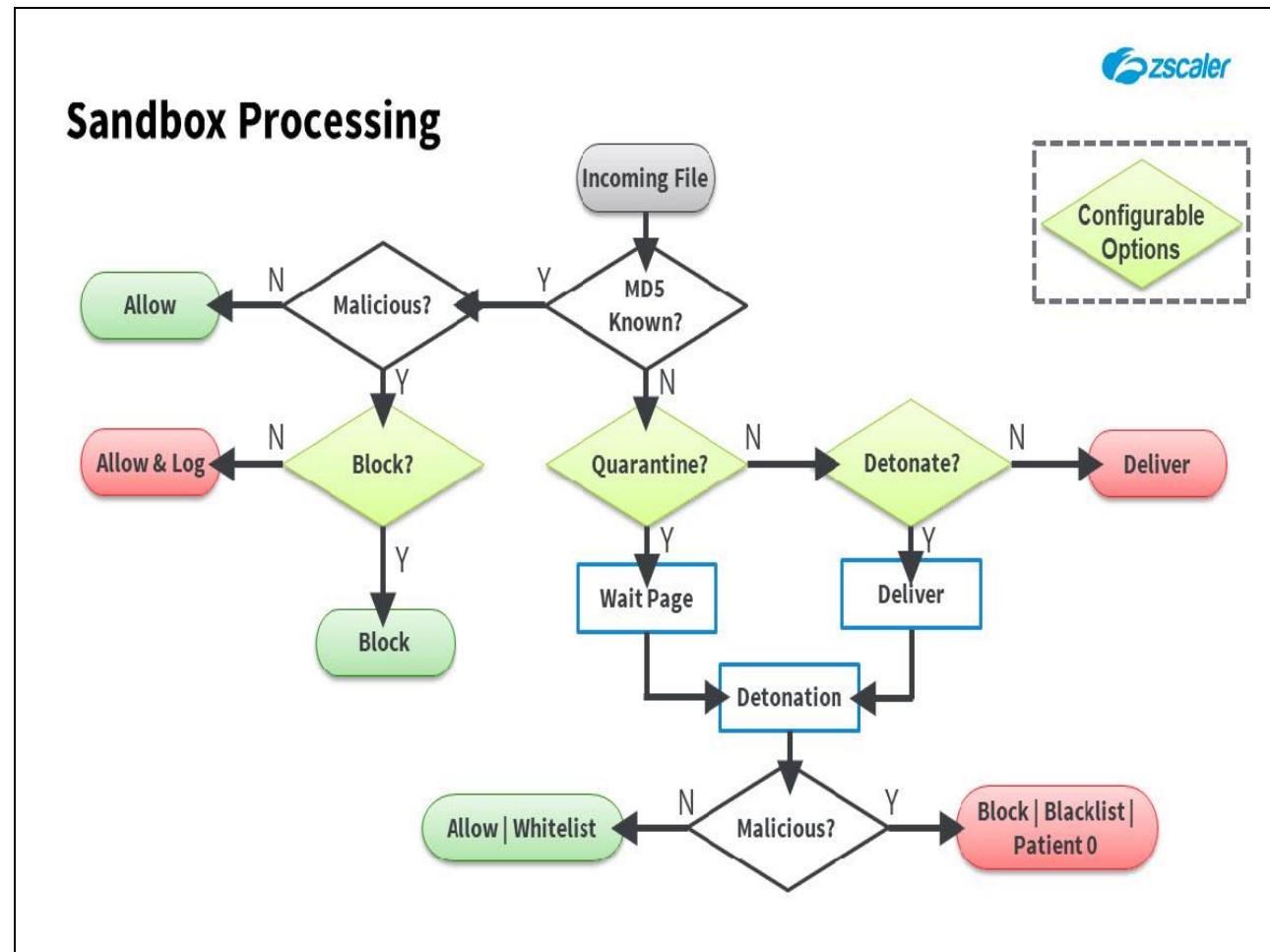
Slide 49 - Sandbox Processing



Slide notes

If the MD5 hash for the file is not known, you have the option whether or not to 'Quarantine' the file, i.e. block the download until the file has been proven to be benign. If you enable the 'Quarantine' option, we will display a 'Wait' page to the end user while we detonate and analyze the file. This page is refreshed at intervals and if the file is found to be OK, it will be automatically delivered. If it is found to be malicious, it will be blocked and black-listed, and a report will be posted to the 'Patient 0' widget on the 'Security' Dashboard.

Slide 50 - Sandbox Processing



Slide notes

If you elect not to use the 'Quarantine' option, you can decide whether or not to Sandbox it at all, and if not, we simply deliver the file. Note that this would be considered a risky option, as there is no way to know whether the file is safe.

If you elect to analyze the file, we will detonate it as before although the file will be delivered to the end user regardless, while we proceed with detonation and analysis. If the file is retrospectively found to be benign, all well and good; if it is found to be malicious, it will be blocked for subsequent downloads, black-listed and a report will be posted to the 'Patient 0' widget on the 'Security' Dashboard.

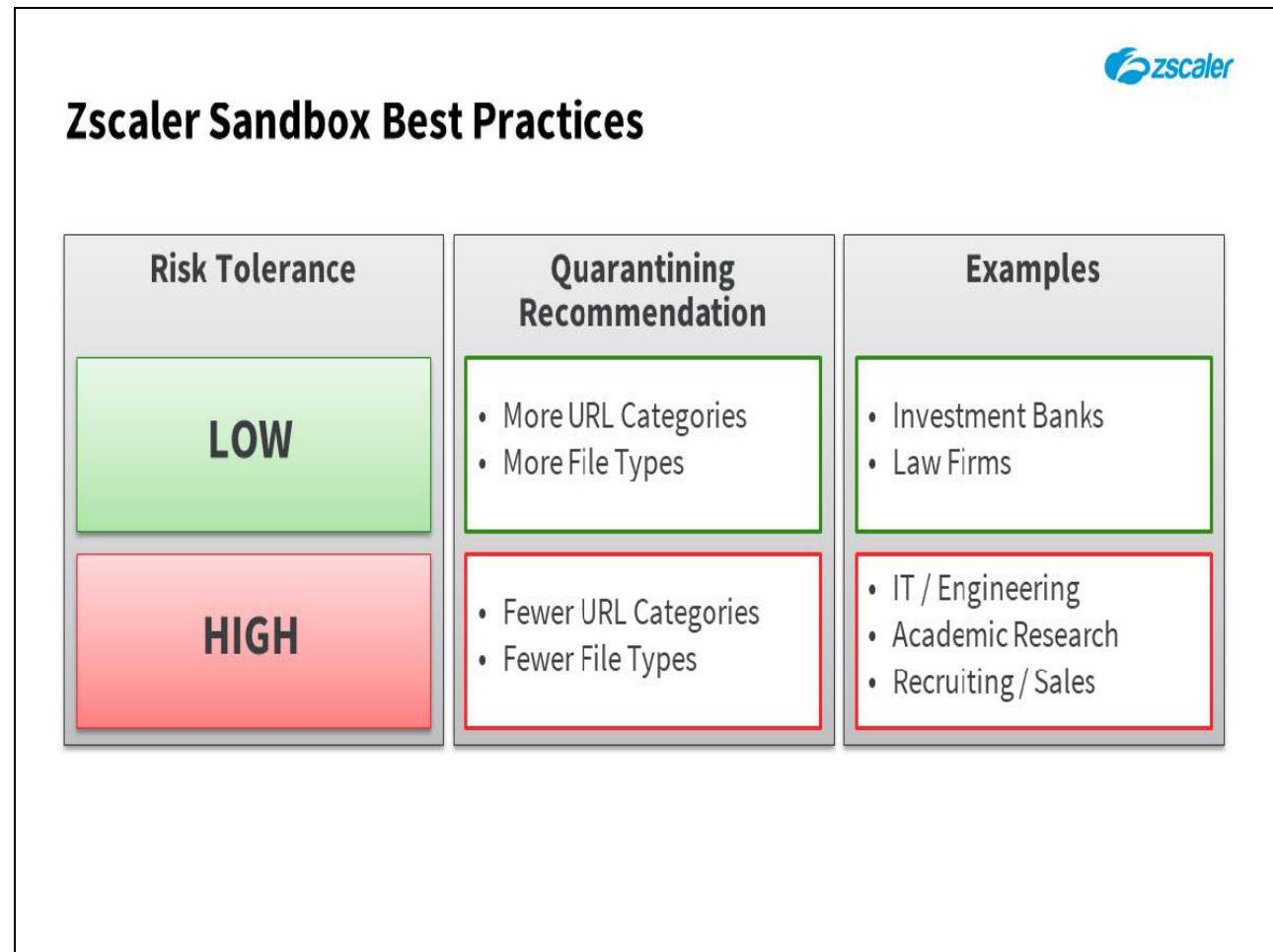
Slide 51 - Zscaler Sandbox Best Practices

Zscaler Sandbox Best Practices

Risk Tolerance	Quarantining Recommendation	Examples
LOW	<ul style="list-style-type: none">• More URL Categories• More File Types	<ul style="list-style-type: none">• Investment Banks• Law Firms

Slide notes

Best practices for the Zscaler Cloud Sandbox are really determined by the tolerance to risk of the customer. Some people are very risk averse (i.e. have low risk tolerance, such as Investment Banks, or Law firms), and they would probably require many more URL Categories and file types to be analyzed.

Slide 52 - Zscaler Sandbox Best Practices**Slide notes**

Other organizations have a high tolerance for risk (such as IT or Engineering groups, Academic Research organizations, Recruiting or Sales organizations). These customers can probably get away with analyzing fewer URL categories and file types.

Slide 53 - Zscaler Sandbox Best Practices

Zscaler Sandbox Best Practices



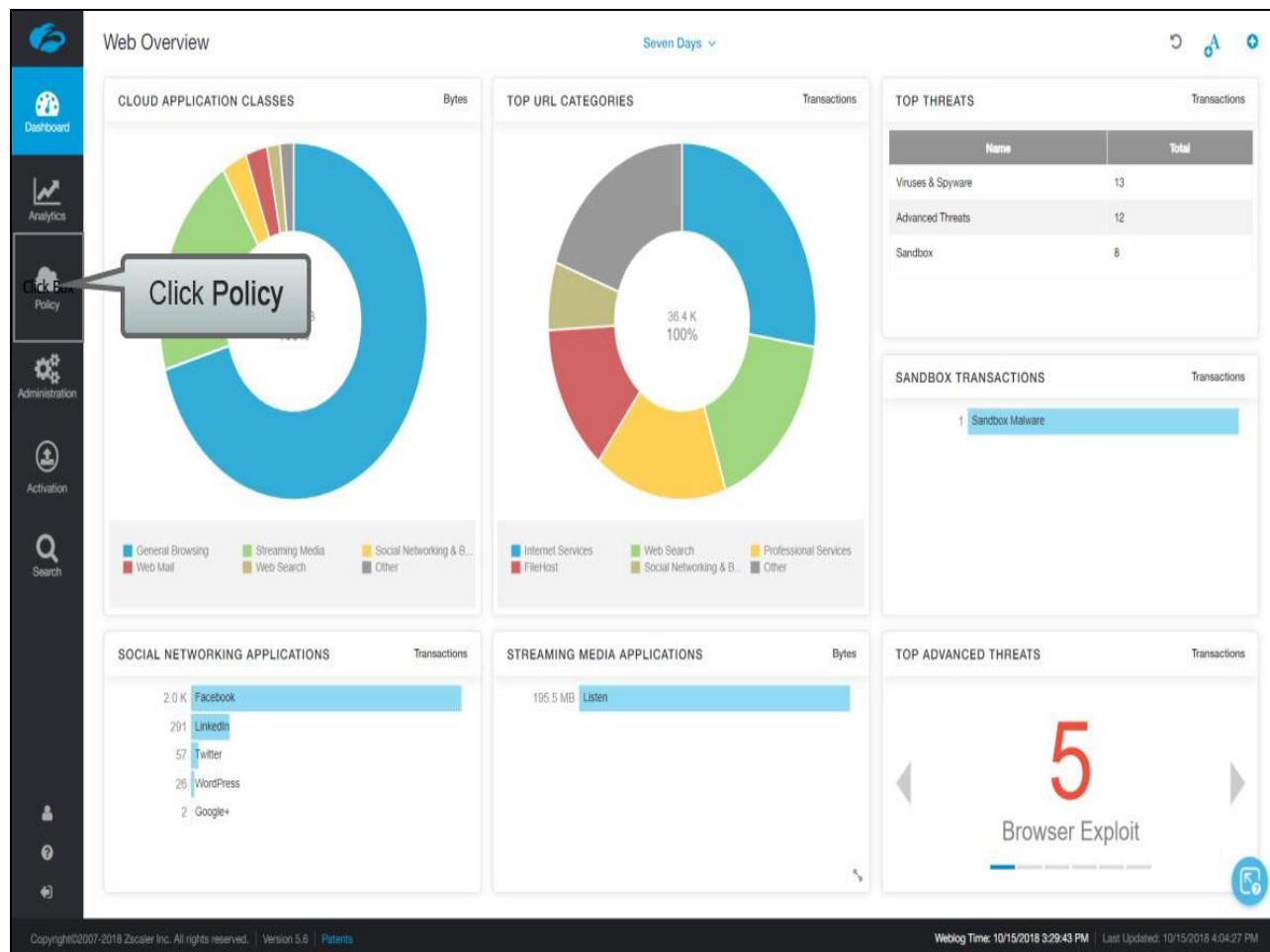
Risk Tolerance	Quarantining Recommendation	Examples
LOW	<ul style="list-style-type: none">More URL CategoriesMore File Types	<ul style="list-style-type: none">Investment BanksLaw Firms
HIGH	<ul style="list-style-type: none">Fewer URL CategoriesFewer File Types	<ul style="list-style-type: none">IT / EngineeringAcademic ResearchRecruiting / Sales

Consider also the risk tolerance of departments within an organization

Slide notes

Note that the tolerance for risk may well not be consistent throughout an organization, and the Sandbox configuration allows for customized rules per-user group, per-department, or even per-location.

Slide 54 - Slide 54



Slide notes

To access the 'Sandbox' policy settings, click 'Policy', ...

Slide 55 - Slide 55

The screenshot shows the Zscaler Policy interface. On the left sidebar, under the 'Web' section, there is a 'Click Box' button which is highlighted with a callout pointing to a 'Click Sandbox' box. The main dashboard area displays several charts and tables. One chart is a donut chart titled 'TOP URL CATEGORIES' showing transaction volumes for different categories. Another chart is a bar chart titled 'STREAMING MEDIA APPLICATIONS'. A table titled 'TOP THREATS' lists 'Viruses & Spyware' (13), 'Advanced Threats' (12), and 'Sandbox' (8). A table titled 'TOP ADVANCED THREATS' shows a large red number '5' and the text 'Browser Exploit'. The bottom of the screen shows copyright information and a timestamp.

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

Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM

Slide notes

...then from the 'Web' section of the 'Policy' menu, under the 'SECURITY' heading, click 'Sandbox'.

Slide 56 - Slide 56

The screenshot shows the Zscaler Policy Web Security interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Sandbox" and contains a "Configure Sandbox Policy" section with a note that "Sandbox supports the scanning and execution of files." Below this is a table titled "Add Sandbox Rule". The table has columns for "Rule Order", "Rule Name", "Criteria", "Action", and "Description". There is one row in the table:

Rule Order	Rule Name	Criteria	Action	Description
Default	BA 1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anony...	Allow and scan First Time Block Subsequent Downloads	Default Rule Created during the ... Click Box

A callout box with the text "Click to Edit the default rule" points to the "Click Box" icon in the "Description" column of the table. At the bottom of the page, there is a footer with copyright information and a timestamp.

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

Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM

Slide notes

There is a default Sandbox policy rule, click to edit it, ...

Slide 57 - Slide 57

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Administration, Activation, and Search. The main area is titled 'Sandbox' and contains a sub-section 'Configure Sandbox Policy' which states 'Sandbox supports the scanning and execution of files.' Below this is a table with two rows: 'Default' and 'BA 1'. A modal window titled 'Edit Sandbox Rule' is open over the table. The modal has a header 'Default rule criteria' and a section 'CRITERIA' with tabs for 'File Types', 'URL Categories', 'Sandbox Categories', and 'Protocols'. Under 'Sandbox Categories', there's a list of items: 'Sandbox Adware', 'Sandbox Malware/Botnet', and 'Sandbox P2P/Anonymizer'. These three items are highlighted with a red box and labeled 'Sandbox Categories (configurable)'. At the bottom of the modal, there are 'Done' and 'Cancel' buttons.

Slide notes

...this policy is configured by default, to analyze suspicious Windows executable files (.exe) and dynamic link libraries (.dll) of traffic from URLs in suspicious URL categories. By default, the three 'Sandbox Categories' ('Sandbox Adware', 'Sandbox Malware/Botnet' and 'Sandbox P2P/Anonymizer') are enabled for analysis, although you can disable them if you choose.

Slide 58 - Slide 58

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Administration, Activation, and Search. The main area is titled 'Sandbox' and contains a sub-section 'Configure Sandbox Policy' with the note 'Sandbox supports the scanning and execution of files.' Below this is a table for 'Sandbox Rules' with columns 'Rule Order', 'Rule Name', and 'Description'. A rule named 'BA 1' is selected. A modal window titled 'Edit Sandbox Rule' is open, showing 'CRITERIA' and 'ACTION' sections. In the 'ACTION' section, under 'First-Time Action', there are 'Allow and scan', 'Block', and 'Action for Subsequent Downloads'. A callout box highlights the 'Action for Subsequent Downloads' section, which is set to 'Block'. The 'Allow' option is also visible. At the bottom of the modal are 'Save' and 'Cancel' buttons. The status bar at the bottom of the screen shows 'Copyright © 2018 Zscaler Inc. All rights reserved | Version 5.6 | Policies' and 'Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 3:29:37 PM'.

Slide notes

In most case the Zscaler service will have seen a file before and it will be examined with no delay to the user. However, if it is a new file and appears suspicious, Zscaler allows the download to proceed but will take the file and execute it in a sandbox to see what it does. The 'Action for Subsequent Downloads' is set by default to 'Block', although the 'Allow' option can be selected instead if you choose.

If you change the default rule, be sure to save and activate it!

Slide 59 - Slide 59

The screenshot shows the Zscaler Policy Web Security interface. On the left, there is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Sandbox' and contains a sub-section titled 'Configure Sandbox Policy' which states 'Sandbox supports the scanning and execution of files.' Below this is a table titled 'Click Add Sandbox Rule'.

Rule Order	Rule Name	Criteria	Action	Description
Default		SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anony... FILE TYPES Windows Executables (exe, exe64); ZIP (zip); Windows Library (dll6... URL CATEGORIES Suspicious Destinations	Allow and scan First Time Block Subsequent Downloads	Default Rule Created during the ...

A callout box with a blue arrow points to the 'Add Click Box Rule' link in the top-left corner of the table header. The bottom of the screen displays copyright information and a timestamp.

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

Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM

Slide notes

To add a new 'Sandbox' Policy rule, click on the 'Add Sandbox Rule' link.

Slide 60 - Slide 60

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Administration, Activation, and Search. The main area is titled 'Sandbox' and has a sub-section 'Configure Sandbox Policy' which says 'Sandbox supports the scanning and execution of files.' There's a button '+ Add Sandbox Rule' and a table with two rows: 'Default' and 'BA_1'. The 'BA_1' row has 'Rule Order' set to 1, 'Rule Name' set to BA_1, and 'Rule Status' set to Enabled. A callout bubble highlights these three fields with the text 'Manage Rule Order, Rule Name, and Rule Status'. Below this, there's a 'CRITERIA' section with dropdowns for File Types (None), URL Categories (Any), Users (Any), Groups (Any), Departments (Any), Locations (Any), Sandbox Categories (Sandbox Aware; Sandbox Malware/Bot...), and Protocols (FTP over HTTP; HTTP; HTTPS; Native FTP). There's also an 'ACTION' section with 'First-Time Action' set to 'Allow and scan' and 'Action for Subsequent Downloads' set to 'Block'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows a list of rules with columns for 'Rule Order', 'Rule Name', and 'Description'. The first rule in the list is 'Default Rule Created during the ...'.

Slide notes

You must specify the ‘Rule Order’, ‘Rule Name’, and ‘Status’, remembering that rules are read from the top down, and evaluation stops at the first match.

Slide 61 - Slide 61

Configure standard criteria as necessary

Slide notes

When adding a new ‘Sandbox’ rule, you can be as general or as specific as you need with the standard target criteria to target the rule based on any combination of:

- ‘URL Categories’;
- ‘Users’;
- ‘Groups’;
- ‘Departments’;
- ‘Locations’;
- Or ‘Protocols’.

Note that we will talk about the ‘URL Categories’ shortly, when looking at the ‘URL & Cloud App Control’ Policy.

Slide 62 - Slide 62

Select File Types to be scanned

Slide notes

With a basic subscription, the only file types that can be selected for scanning are executables, and .DLL files, up to 2MB in size.

With the Advanced Cloud Sandbox subscription, there is no file size restriction, and the files that can be scanned include:

- ‘Archive’ files (.RAR, .ZIP, and .ZIP with suspicious Script Files);
- ‘Executables’ (including Windows library files);
- ‘Microsoft Office’ files (with all the Excel, PowerPoint, RTF and Word file formats, including the macro enabled versions of these formats);
- ‘Mobile’ files, specifically Android application packages (.APKs);
- ‘Other Documents’, which includes .PDF documents;
- And ‘Web Content’, such as Adobe Flash and Java applets.

Slide 63 - Slide 63

Sandbox

Configure Sandbox Policy
Sandbox supports the scanning and execution of files.

Add Sandbox Rule

Rule Order: 1 Rule Name: BA_1

Rule Status: Enabled

CRITERIA

File Types: Adobe Flash; Android Application Packa...

Users: Any

Departments: Any

Sandbox Categories: Sandbox Aware; Sandbox Malware/Bot...

ACTION

First-Time Action: Allow and scan

DESCRIPTION

Save Cancel

Configure URL Categories as necessary

Unselected Items Selected Items (32)

- Search...
Done Cancel Clear Selection
- Illegal or Questionable
- Anonymizer
- Computer Hacking
- Copyright Infringement
- Mature Humor
- Other Illegal or Questionable
- Adult Sex Education
- Adult Themes
- Anonymizer
- Computer Hacking
- Copyright Infringement
- Gambling
- K-12 Sex Education
- Lingerie/Bikini
- Mature Humor

Default Rule Created during the ...

Slide notes

Typically, you would target a rule against the 'Legal Liability' URL Categories, although you are free to select any appropriate categories.

Slide 64 - Slide 64

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Sandbox' and has a sub-section 'Configure Sandbox Policy' which states 'Sandbox supports the scanning and execution of files.' Below this is a button 'Add Sandbox Rule'. The central part of the screen shows a list of rules with columns for 'Rule Order' (Default) and 'Rule Name' (BA_1). A modal window titled 'Add Sandbox Rule' is open. Inside, under the 'Sandbox RULE' section, there's a 'Rule Status' table with two columns: 'Unselected Items' and 'Selected Items (3)'. The 'Selected Items' column lists 'Sandbox Adware', 'Sandbox Malware/Botnet', and 'Sandbox P2P/Anonymizer', each with a small 'X' icon to remove them. Below this table is a callout box with the text 'Configure Sandbox Categories as necessary'. At the bottom of the modal are 'Done', 'Cancel', and 'Clear Selection' buttons. The background of the main interface shows a list of rules with descriptions like 'Default Rule Created during the ...'. At the bottom of the page, there's a footer with copyright information: 'Copyright © 2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Policies'.

Slide notes

You can also target a rule against any combination of the three 'Sandbox' Categories:

- 'Sandbox Adware';
- 'Sandbox Malware/Botnet';
- Or 'Sandbox P2P/Anonymizer'.

Slide 65 - Slide 65

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Administration, Activation, and Search. The main area is titled 'Sandbox' and contains a sub-section 'Configure Sandbox Policy' with a note that it supports scanning and execution of files. A button '+ Add Sandbox Rule' is visible. In the center, a modal window titled 'Add Sandbox Rule' is open. It has sections for 'Sandbox Rule' (Rule Order: 1, Rule Name: BA_1, Rule Status: Enabled), 'Criteria' (File Types: Adobe Flash; Android Application Packa..., Users: Any, Departments: Any), 'Sandbox Categories' (Sandbox Aware; Sandbox Malware/Bot...), 'Action' (First-Time Action: Allow and scan, Action for Subsequent Downloads: Block), and 'Description' (a large text input field). At the bottom of the modal are 'Save' and 'Cancel' buttons. A callout bubble with the text 'Configure Protocols as necessary' points to the 'Selected Items (4)' section of the protocol selection dropdown. This dropdown shows four items: 'FTP over HTTP', 'HTTP', 'HTTPS', and 'Native FTP', each with a checked checkbox. The 'Selected Items (4)' section also includes a search bar and 'Done' and 'Cancel' buttons.

Slide notes

You can specify the 'Protocols' the rule is to be applied to, any combination of; 'FTP over HTTP', 'HTTP', 'HTTPS', or 'Native FTP'.

Slide 66 - Slide 66

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Sandbox' and has a sub-section 'Configure Sandbox Policy' which states 'Sandbox supports the scanning and execution of files.' There's a button 'Add Sandbox Rule'. Below it, a table lists a single rule: 'Default' with 'Rule Name' 'BA_1'. The 'ACTION' section of the dialog box is highlighted with a red box. It shows three options for 'First-Time Action': 'Allow and do not scan', 'Allow and scan' (selected), and 'Quarantine'. A callout bubble says 'Configure the preferred First Time Action'.

Slide notes

Specify the action to be taken when Zscaler sees a file for the first time, the options here being:

- ‘Allow and do not scan’;
- ‘Allow and scan’;
- Or ‘Quarantine’.

The decision to be made here is whether you want to make the user wait while Zscaler scans the file, the typical delay for scanning being less than 10 minutes. If you choose to quarantine the file, then while the file is being scanned the user will see a ‘Please Wait’ message. This message will be automatically refreshed at intervals while the file is ‘detonated’ in the Sandbox.

Slide 67 - Slide 67

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Sandbox' and has a sub-section 'Configure Sandbox Policy' which says 'Sandbox supports the scanning and execution of files.' There's a button to 'Add Sandbox Rule'. In the center, a modal window titled 'Add Sandbox Rule' is open. It has a section for 'Sandbox RULE' where 'Rule Order' is set to 1 and 'Rule Name' is 'BA_1', with 'Enabled' status selected. Below that is a 'CRITERIA' section with various filters like 'File Types', 'Users', 'Departments', 'Sandbox Categories', 'Groups', 'Locations', and 'Protocols'. At the bottom is an 'ACTION' section with a dropdown for 'First-Time Action' set to 'Quarantine'. A sub-menu titled 'Action for Subsequent Downloads' is open, showing 'Allow' and 'Block' options, with 'Block' highlighted by a red box. A tooltip at the bottom left of the modal says 'Configure the preferred Action for Subsequent Downloads'. The footer of the page includes copyright information and a timestamp.

Slide notes

Then specify what Zscaler should do on subsequent downloads of the file, whether to; 'Block', or 'Allow'.

Slide 68 - Slide 68

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Sandbox' and has a sub-section 'Configure Sandbox Policy' which says 'Sandbox supports the scanning and execution of files.' There's a button to 'Add Sandbox Rule'. In the center, a modal window titled 'Add Sandbox Rule' is open. It has a tab 'Sandbox Rule' selected. Inside, there are sections for 'Rule Order' (set to 1), 'Rule Name' (BA_1), 'Rule Status' (Enabled), 'CRITERIA' (File Types: Adobe Flash; Android Application Packa..., URL Categories: Adult Sex Education; Adult Themes; Ano..., Users: Any, Groups: Any, Departments: Any, Locations: Any, Sandbox Categories: Sandbox Aware; Sandbox Malware/Bot..., Protocols: FTP over HTTP; HTTP; HTTPS; Native FTP), 'ACTION' (First-Time Action: Quarantine, Action for Subsequent Downloads: Block), and a 'DESCRIPTION' field. At the bottom left of the modal, there's a blue button labeled 'Click Box' with a callout bubble pointing to it, and a 'Cancel' button.

Slide notes

Having configured the Cloud Sandbox policy rule as necessary, click 'Save'.

Slide 69 - Slide 69

The screenshot shows the Zscaler Policy-Web-Security interface with the 'Sandbox' tab selected. The main area displays the 'Configure Sandbox Policy' section, which states that 'Sandbox supports the scanning and execution of files.' Below this is a table titled 'Add Sandbox Rule'.

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	BA_1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anony...	Quarantine First Time Block Subsequent Downloads		Edit Delete
FILE TYPES Microsoft Word (doc, docx, docm, dotx, etc.); Microsoft PowerPoi...					
URL CATEGORIES Other Adult Material; Adult Themes; Lingerie/Bikini; Nudity; Porno...					
PROTOCOLS FTP over HTTP; Native FTP; HTTPS; HTTP					
Default	BA_1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anon...	Allow and scan First Time Block Subsequent Downloads	Default Rule Created during th...	Edit
FILE TYPES Windows Executables (exe, exe64); ZIP (zip); Windows Library (dll...					
URL CATEGORIES Suspicious Destinations					

At the bottom left, there is a copyright notice: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'. At the bottom right, it says 'Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM'.

Slide notes

Slide 70 - Slide 70

Sandbox

Configure Sandbox Policy
Sandbox supports the scanning and execution of files.

Add Sandbox Rule

Rule Order Rule Name Criteria Action Description

1	BA_1	<p>SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anony...</p> <p>FILE TYPES Microsoft Word (doc, docx, docm, dotx, etc.); Microsoft PowerPoi...</p> <p>URL CATEGORIES Other Adult Material; Adult Themes; Lingerie/Bikini; Nudity; Porno...</p> <p>PROTOCOLS FTP over HTTP; Native FTP; HTTPS; HTTP</p>	<p>Quarantine First Time Block Subsequent Downloads</p>	
Default	BA_1	<p>SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anon...</p> <p>FILE TYPES Windows Executables (exe, exe64); ZIP (zip); Windows Library (dll...</p> <p>URL CATEGORIES Suspicious Destinations</p>	<p>Allow and scan First Time Block Subsequent Downloads</p>	Default Rule Created during th...

Activation

Search

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

Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM

Slide notes

...and 'Activate' your changes.

Slide 71 - Slide 71

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation (which is selected and has a red notification badge), and Search. The main area is titled "CURRENTLY EDITING (1)" and shows a list of activations. A large blue button labeled "Click Box" is highlighted with a callout bubble containing the text "Click Activate". The table lists two activation rules:

	Criteria	Action	Description
SANDBOX CATEGORIES	Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anony...	Quarantine First Time Block Subsequent Downloads	
FILE TYPES	Microsoft Word (doc, docx, docm, dotx, etc.); Microsoft PowerPoi...		
URL CATEGORIES	Other Adult Material; Adult Themes; Lingerie/Bikini; Nudity; Porno...		
PROTOCOLS	FTP over HTTP; Native FTP; HTTPS; HTTP		
SANDBOX CATEGORIES	Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anon...	Allow and scan First Time Block Subsequent Downloads	Default Rule Created during th...
FILE TYPES	Windows Executables (exe, exe64); ZIP (zip); Windows Library (dll...		
URL CATEGORIES	Suspicious Destinations		

At the bottom, there are copyright and log-in information: "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients". To the right, it says "Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM".

Slide notes

Slide 72 - Slide 72

The screenshot shows the Zscaler Policy interface with the 'Sandbox' tab selected. A message at the top right says 'Activation Completed!'. On the left, a sidebar lists various policy categories: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area displays a table of 'Sandbox Rule' configurations.

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	BA_1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anony... FILE TYPES Microsoft Word (doc, docx, docm, dotx, etc.); Microsoft PowerPoi... URL CATEGORIES Other Adult Material; Adult Themes; Lingerie/Bikini; Nudity; Porno... PROTOCOLS FTP over HTTP; Native FTP; HTTPS; HTTP	Quarantine First Time Block Subsequent Downloads	Default Rule Created during th...	Edit Delete
Default	BA_1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anon... FILE TYPES Windows Executables (exe, exe64); ZIP (zip); Windows Library (dll... URL CATEGORIES Suspicious Destinations	Allow and scan First Time Block Subsequent Downloads	Default Rule Created during th...	Edit

At the bottom, there are copyright notices: 'Copyright©2007-2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Patients'. To the right, it says 'Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM'.

Slide notes

Slide 73 - Slide 73

The screenshot shows the Zscaler Policy Management interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Sandbox' and contains a table for 'Configure Sandbox Policy'. The table has columns for Rule Order, Rule Name, Criteria, Action, and Description. There are two rows: one for 'BA_1' and one for 'Default'. A callout box with the text 'Click Recommended Policy' points to the 'Action' column of the 'BA_1' row. The 'Action' column for 'BA_1' shows 'Allow and scan First Time' and 'Block Subsequent Downloads'. The 'Default' row shows 'Default Rule Created during th...'. At the bottom of the interface, there is a footer with copyright information and a timestamp.

Rule Order	Rule Name	Criteria	Action	Description
1	BA_1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anon... FILE TYPES Microsoft Word (doc, docx, docm, dotx, etc.); Microsoft	Allow and scan First Time Block Subsequent Downloads	Default Rule Created during th...
Default	BA_1	SANDBOX CATEGORIES Sandbox Adware; Sandbox Malware/Botnet; Sandbox P2P/Anon... FILE TYPES Windows Executables (exe, exe64); ZIP (zip); Windows Library (dll... URL CATEGORIES Suspicious Destinations		

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

Weblog Time: 10/15/2018 3:29:43 PM | Last Updated: 10/15/2018 4:04:27 PM

Slide notes

To see Zscaler recommendations for configuring ‘Sandbox’ Policy settings, click the ‘Recommended Policy’ link.

Slide 74 - Slide 74

The screenshot shows the Zscaler Policy interface with the 'Sandbox' policy selected. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays the 'Sandbox' policy details. A modal window titled 'View Recommended Sandbox Policy' is open, showing the following configuration:

Rule Order	Role Name	Description
1	BA_1	Configure Sandbox Policy Sandbox supports the scanning and execution of files.

SANDBOX RULE

Rule Order:	Rule Status:
1	Enabled

CRITERIA

File Types:	Select all file types for sandboxing	URL Categories:	Any
Users:	Any	Groups:	Any
Departments:	Any	Locations:	Any
Sandbox Categories:	Any	Protocols:	Any

ACTION

Action:	First Time Action:
Block	Allow and scan

At the bottom of the modal, there is a note: "Default Rule Created during th...". The footer of the page includes copyright information: "Copyright © 2018 Zscaler Inc. All rights reserved." and "Version 5.6 | Policies". It also shows the "Last Updated: 10/15/2018 8:04:37 PM" and a timestamp "Weblog Time: 10/15/2018 3:29:43 PM".

Slide notes

For the 'Sandbox' Policy Zscaler recommends that you:

- Analyze all 'File Types' of traffic from any 'URL Categories', that match any of the 'Sandbox Categories';
- That you 'Block' files known to contain Adware, Botnets & Malware, or Anonymizers or P2P clients;
- And that you 'Allow and scan' files seen for the first time.

Slide 75 - Slide 75

The screenshot shows a web page from Zscaler. At the top, it says "pete.zscaler". Below that is a yellow-bordered box containing the following text:

⚠ We're checking this file for a potential security risk.

The file you attempted to download is being analyzed for your protection. It is not blocked. The analysis can take up to 10 minutes, depending on the size and type of the file.

If safe, your file downloads automatically.

If unsafe, the file will be blocked.

You tried to download: <http://securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe>

See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@pete.zscaler.com

Q01

At the bottom left, it says "Waiting for securitytest.zsdemo.com..."

Slide notes

For the end user experience, when the 'Quarantine' action is selected, they will see and 'End User Notification' (EUN) message while the file is being detonated. This page will refresh at intervals, ...

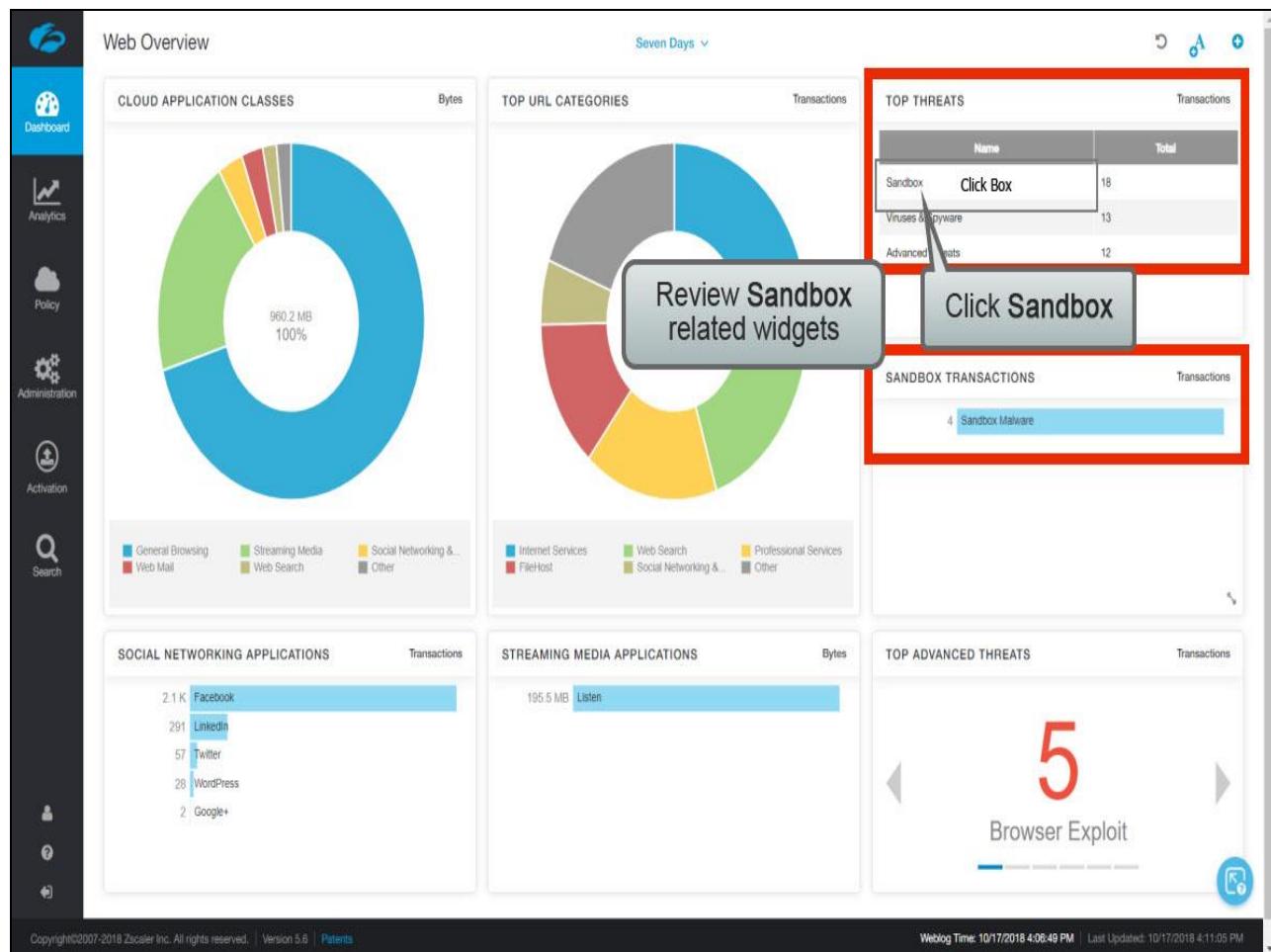
Slide 76 - Slide 76

The screenshot shows a red-bordered alert window from Zscaler. At the top, it says "pete.zscaler". Inside the window, there is a red circular icon with a white exclamation mark followed by the text "We found a security threat." Below this, a section titled "Website blocked" is shown with the message "You tried to visit: <http://securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe>". Further down, it states "Threat found: Sandbox Malware" and provides a link "See our internet use policy.". At the bottom of the window, there is a footer bar with the text "Need help? Contact our support team at +91-9000000000, support@pete.zscaler.com" and the Zscaler logo followed by the text "Your organization has selected Zscaler to protect you from internet threats".

Slide notes

...and if the file is found to be malicious a 'Block' EUN will be shown. If the file is found to be OK, it will simply be delivered.

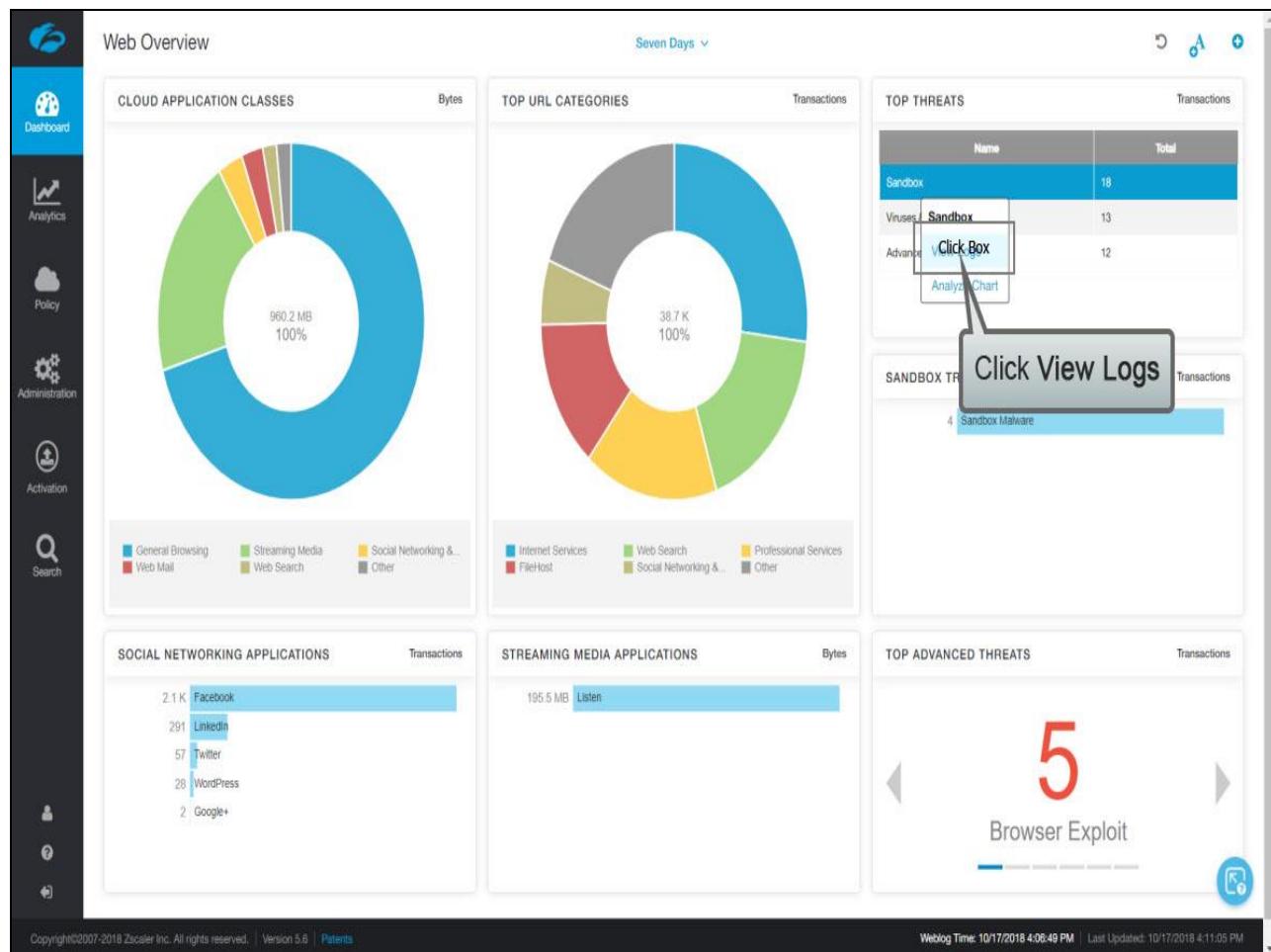
Slide 77 - Slide 77



Slide notes

An administrator with access to the Zscaler Admin Portal Dashboards, can review the Sandbox widgets on the 'Web Overview' Dashboard, and can drill down for full details. For example, in the 'Top Threats' widget, click 'Sandbox', ...

Slide 78 - Slide 78



Slide notes

...then click 'View Logs'.

Slide 79 - Slide 79

The screenshot shows the Zscaler Web Insights interface. On the left is a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has three sections: 1. Select Chart Type (with Log icon highlighted), 2. Choose a Timeframe (Custom: 10/10/2018 12:00:00 AM - 10/17/20...), and 3. Select Filters (User: All, Threat Class: Sandbox, Threat Name Search, Show Delayed Logs, Add Filter). To the right is a table titled "Web Insights" with columns: No., Logged Time, User, URL, and Policy Action. The table lists 18 rows of log entries. A callout bubble with the text "Click to scroll through the fields" points to the table.

No.	Logged Time	User	URL	Policy Action
1	Wednesday, October 10, 2018 5:58:12 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3640.exe	Quarantined
2	Wednesday, October 10, 2018 5:58:18 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3640.exe	Quarantined
3	Wednesday, October 10, 2018 6:11:22 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3640.exe	Quarantined
4	Wednesday, October 10, 2018 7:15:48 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3642.exe	Quarantined
5	Wednesday, October 10, 2018 7:15:54 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3642.exe	Quarantined
6	Wednesday, October 10, 2018 7:18:12 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3642.exe	Quarantined
7	Wednesday, October 10, 2018 7:25:27 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3642.exe	Quarantined
8	Wednesday, October 10, 2018 7:38:39 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3642.exe	Sandbox bloc...
9	Monday, October 15, 2018 5:39:36 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/exe_kryptik_46527d53a046ebc4e4...	Sandbox bloc...
10	Monday, October 15, 2018 5:42:00 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/exe_kryptik_46527d53a046ebc4e4...	Sandbox bloc...
11	Monday, October 15, 2018 5:43:14 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3656.exe	Allowed
12	Monday, October 15, 2018 5:43:34 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3657.exe	Allowed
13	Monday, October 15, 2018 5:44:06 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3658.exe	Allowed
14	Monday, October 15, 2018 5:46:39 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe	Quarantined
15	Monday, October 15, 2018 5:46:46 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe	Quarantined
16	Monday, October 15, 2018 5:49:20 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe	Quarantined
17	Monday, October 15, 2018 5:53:51 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe	Quarantined
18	Monday, October 15, 2018 5:59:09 PM	pdahl@pete.zscaler.com	securitytest.zsdemo.com/ba-demo/quarantine/compiled/3659.exe	Sandbox bloc...

Slide notes

Scroll through the data fields for the file, ...

Slide 80 - Slide 80

The screenshot shows the Zscaler Web Insights interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has three sections: 1. Select Chart Type (with Log selected), 2. Choose a Timeframe (Custom: 10/10/2018 12:00:00 AM - 10/17/20...), and 3. Select Filters (User set to All, Threat Class set to Sandbox). The right side displays a table titled 'Web Insights' with columns: Met..., Response Code, Received Bytes, Sent Bytes, Agent, Server Trans. Time (ms), Client T..., MD5, and File Name. A callout box points to the 'MD5' column, containing the value 'cbc6d41a5f2Click.Box(2547a0a178'. The table contains numerous rows of log data.

Met...	Response Code	Received Bytes	Sent Bytes	Agent	Server Trans. Time (ms)	Client T...	MD5	File Name
403 - Forbidden	18,008	508	Firefox (62.0)	613	619		cbc6d41a5f2Click.Box(2547a0a178	3640.exe
403 - Forbidden	18,008	534	Firefox (62.0)	581	581		6603041139c402421388c2-7d9a178	3640.exe
403 - Forbidden	18,008	508	Firefox (62.0)	563	570		cbc6d41a5f2102f9213e82547a0a178	3640.exe
403 - Forbidden	18,008	567	Safari Unkno...	794			7785ac4726be9a747	3642.exe
403 - Forbidden	18,008	583	Safari Unkno...	803			7785ac4726be9a747	3642.exe
403 - Forbidden	18,008	505	Safari Unkno...	1074			7785ac4726be9a747	3642.exe
403 - Forbidden	18,008	567	Safari Unkno...	828	836		7785ac4726be9a747	3642.exe
403 - Forbidden	14,256	567	Safari Unkno...	799	799		1952aad637d4ddff7785ac4726be9a747	3642.exe
403 - Forbidden	14,337	623	Safari Unkno...	1803	1803		celf4323ba4d4eb9de984dcbe3fa139f	exe_httpbrow...
403 - Forbidden	14,315	541	Safari Unkno...	4455	4458		46527d53a046ebc4e4ca08843af47a13	exe_kryptik_4...
200 - OK	22,321	479	Safari Unkno...	747	755		c957d37fbf626b87esta970n7d92642a	3656.exe
200 - OK	22,321	479	Safari Unkno...	760	768		40bad9bb47c596c4018c50fdeab3ffbc	3657.exe
200 - OK	22,321	479	Safari Unkno...	726	802		7445b9d69b75be8cf1c3e1ddaa5b21972	3658.exe
403 - Forbidden	18,008	567	Safari Unkno...	1101	1109		5cb30c84c64a3321bb035e19609cfaf5	3659.exe
403 - Forbidden	18,008	583	Safari Unkno...	1131	1235		5cb30c84c64a3321bb035e19609cfaf5	3659.exe
403 - Forbidden	18,008	583	Safari Unkno...	1095	1157		5cb30c84c64a3321bb035e19609cfaf5	3659.exe
403 - Forbidden	18,008	567	Safari Unkno...	1131	1147		5cb30c84c64a3321bb035e19609cfaf5	3659.exe
403 - Forbidden	14,256	567	Safari Unkno...	1115	1115		5cb30c84c64a3321bb035e19609cfaf5	3659.exe

Slide notes

...to find the 'MD5' field. To see a detailed Sandbox report on a file, click the link for its MD5 hash.

Slide 81 - Slide 81

SANDBOX DETAIL REPORT

Report ID (MD5): cbc6d41a5f2b202f3213e82547a0a178

CLASSIFICATION

Class Type: Malicious
Category: Malware & Botnet Detected: a variant of MSIL/Spy.Agent.GN trojan

Threat Score: 76 (High Risk)

VIRUS AND MALWARE

- A Variant Of: A Variant Of

NETWORKING

- Checks The Public IP Address Of The Machine
- Downloads Files From Web Servers Via HTTP
- Performs DNS Lookups
- Sample HTTP Request Are All Non Existing, Likely The Sample Is No Longer Working
- Tries To Download Non-Existing HTTP Data
- URLs Found In Memory Or Binary Data

STEALTH

- Disables: A Long Time (Installer Files Shows These)
- Debuggers
- Number Of Window / User Specific System Calls
- Amount Of Sleeps In A Loop

SPREADING

INFORMATION LEAKAGE

No suspicious activity detected

EXPLOITING

PERSISTENCE

SYSTEM SUMMARY

DOWNLOAD SUMMARY

ORIGIN

FILE PROPERTIES

PROCESS SUMMARY

DROPPED FILES

SCREENSHOTS

NETWORK PACKETS

File Type: Windows Executable

suspicious activity detected

T Certificates

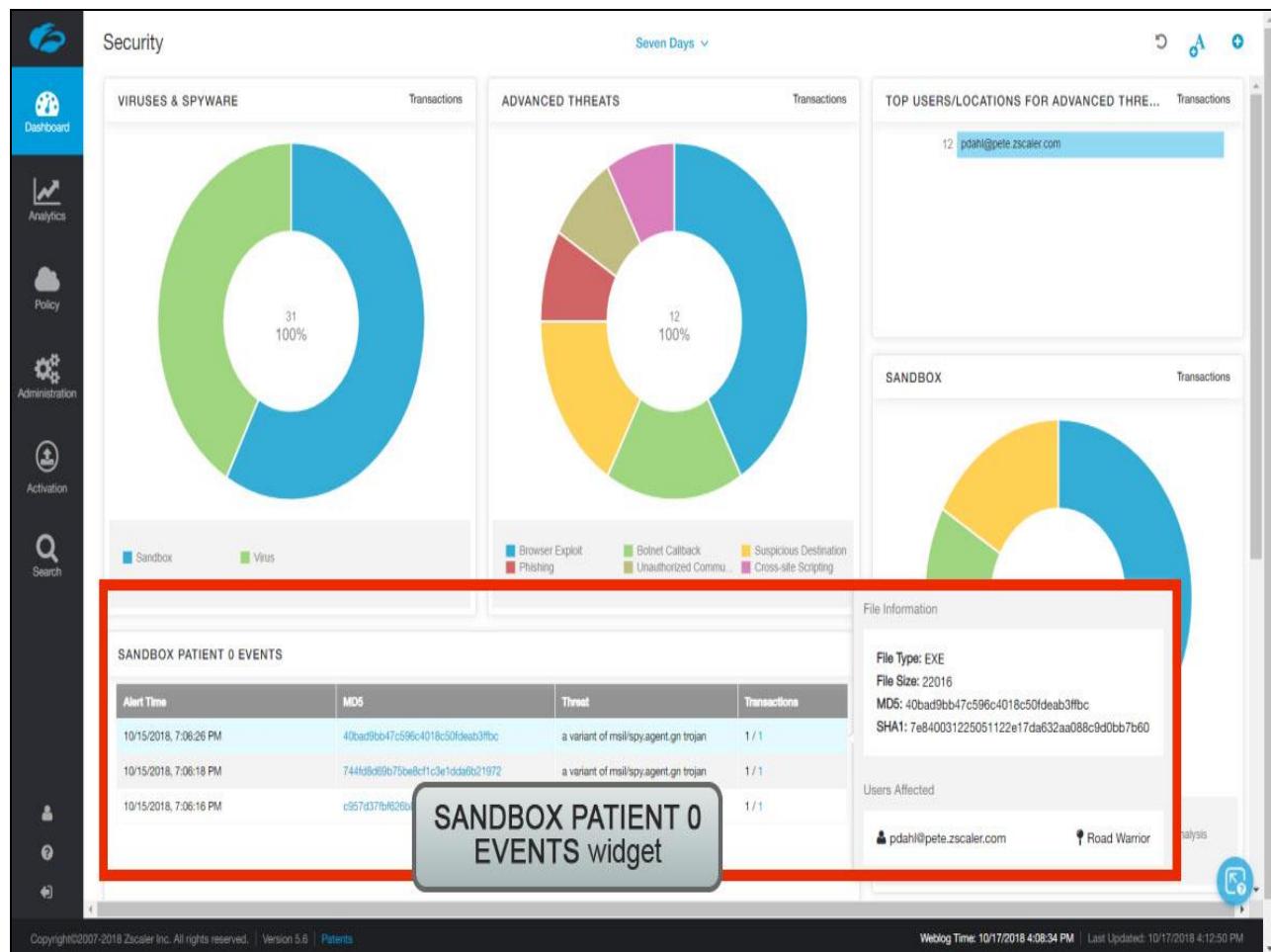
Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Weblog Time: 10/17/2018 4:07:25 PM | Last Updated: 10/17/2018 4:11:43 PM

Slide notes

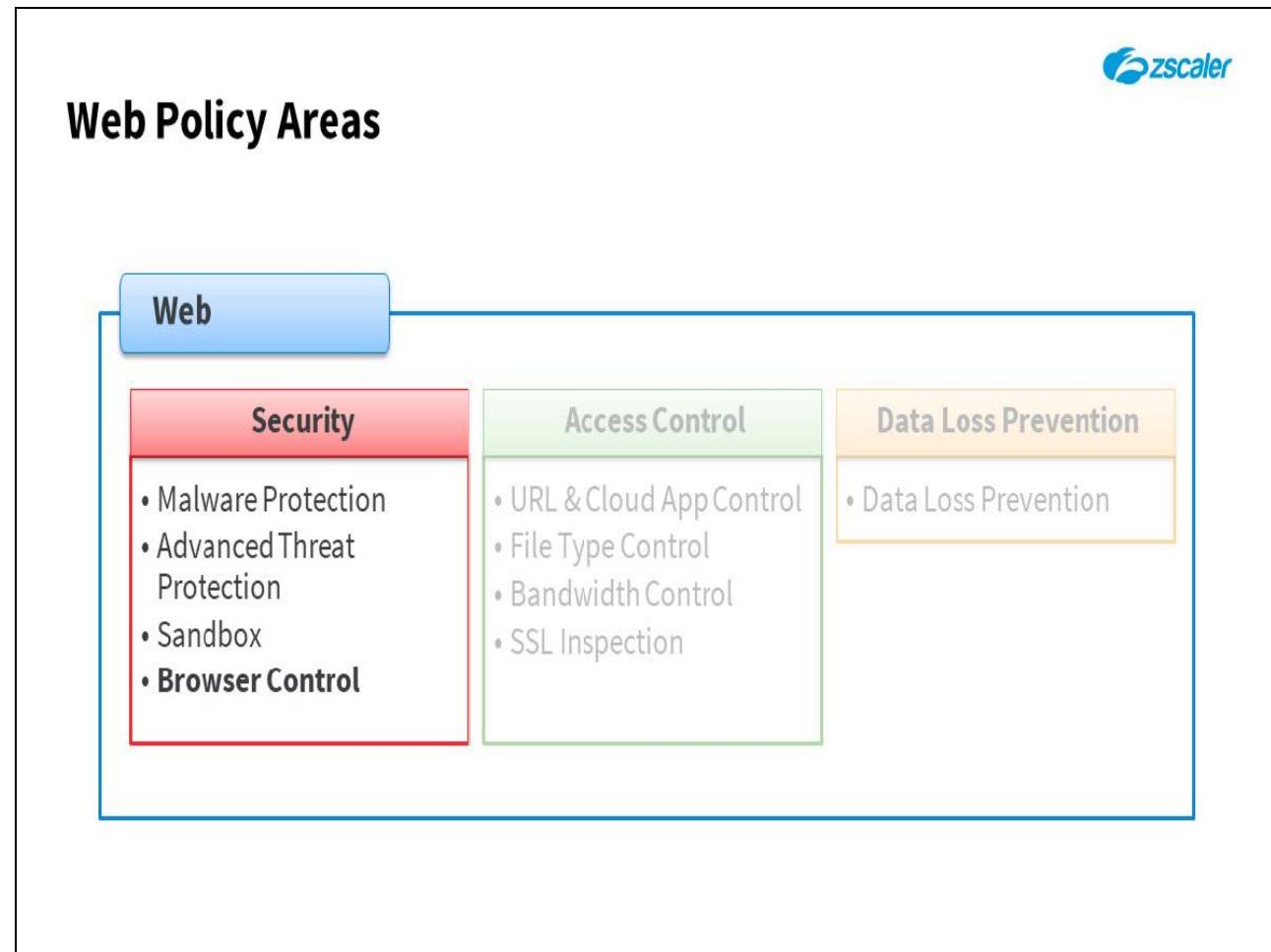
The Sandbox details report for a file has full details on the behaviors observed when the file was detonated, including sections on: 'CLASSIFICATION', 'VIRUS AND MALWARE', 'SECURITY BYPASS', 'NETWORKING', 'STEALTH', 'SPREADING', 'INFORMATION LEAKAGE', 'EXPLOITING', 'PERSISTENCE', 'SYSTEM SUMMARY', 'DOWNLOAD SUMMARY', 'ORIGIN', 'FILE PROPERTIES', 'PROCESS SUMMARY', 'DROPPED FILES', 'SCREENSHOTS', and 'NETWORK PACKETS'.

Slide 82 - Slide 82



Slide notes

In addition, the 'Security' Dashboard now has a 'SANDBOX PATIENT 0 EVENTS' widget, that provides full details for any '0 Day' threats discovered by the Zscaler Cloud Sandbox.

Slide 83 - Web Policy Areas**Slide notes**

The 'Browser Control' Policy can be used to block older Browsers with known vulnerabilities that increase the security risk for your organization.

Slide 84 - Slide 84



Slide notes

To access the 'Browser Control' policy settings, click 'Policy', ...

Slide 85 - Slide 85

The screenshot shows the Zscaler Policy interface. On the left sidebar, under the 'Web' section, there is a callout box highlighting the 'Browser Control' option under the 'SECURITY' heading. The main dashboard area displays several charts and tables. One chart is a donut chart titled 'TOP URL CATEGORIES' showing transaction volumes for different categories. Another chart shows 'STREAMING MEDIA APPLICATIONS' with a single entry for 'Listen'. A table titled 'TOP THREATS' lists 'Advanced Threats' (10), 'Sandbox' (8), and 'Viruses & Spyware' (2). A section titled 'TOP ADVANCED THREATS' features a large red '5' and the text 'Browser Exploit'. The bottom of the screen includes copyright information and a timestamp.

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

Weblog Time: 10/10/2018 8:45:17 PM | Last Updated: 10/10/2018 8:49:22 PM

Slide notes

...then from the 'Web' section of the 'Policy' menu, under the 'SECURITY' heading, click 'Browser Control'.

Slide 86 - Slide 86

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Browser Control' and contains a sub-section titled 'Configure Browser Control Policy'. It includes a note: 'Older browsers with known vulnerabilities increase the security risk for an organization. Allowing a limited set of browsers reduces risk.' Below this is a 'BROWSER VULNERABILITY PROTECTION' section with an 'Enable Checks & User Notification' button, which is highlighted with a red box and a callout bubble saying 'Click to Checks & User Notification'. There's also a 'Recommended Policy' link. At the bottom of the main panel are 'Save' and 'Cancel' buttons. The footer of the page contains copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 10/10/2018 8:45:17 PM | Last Updated: 10/10/2018 8:49:22 PM'.

Slide notes

To enable and configure browser 'Checks & User Notification', click to enable this option.

Slide 87 - Slide 87

The screenshot shows the 'Browser Control' configuration page. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Configure Browser Control Policy' with a note about reducing security risk by limiting browsers. It includes sections for 'BROWSER VULNERABILITY PROTECTION' and 'BROWSER BLOCKING'. In the 'BROWSER VULNERABILITY PROTECTION' section, there is a 'How Often to Check' dropdown menu with options 'NONE' and 'Click Box', where 'Click Box' is selected. A callout box with the text 'Click How Often to Check' points to this dropdown. Other settings include 'Disable Notifications for Browsers' (disabled) and 'Disable Notifications for Applications' (set to 'None'). At the bottom, there are 'Save' and 'Cancel' buttons.

Slide notes

To set a frequency to check end user browsers, click in the 'How often to Check' field, ...

Slide 88 - Slide 88

Browser Control

Configure Browser Control Policy
Older browsers with known vulnerabilities increase the security risk for an organization. Allowing a limited set of browsers reduces risk.

BROWSER VULNERABILITY PROTECTION

Enable Checks & User Notification

Select How Often to Check

How Often to Check

- NONE
- Daily
- Monthly
- Weekly

Disable Notification for Plugins

None

Disable Notification for Applications

None

BROWSER BLOCKING

Allow All Browsers

Save Cancel

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

Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM

Slide notes

...and select the required frequency ('Daily', 'Monthly' or 'Weekly').

Slide 89 - Slide 89

The screenshot shows the 'Browser Control' section of the Zscaler interface. On the left, a vertical sidebar lists icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure Browser Control Policy' with a note about reducing security risk by limiting browsers. Under 'BROWSER VULNERABILITY PROTECTION', a red box highlights the 'Enable Checks & User Notification' checkbox, which is checked. A callout bubble says: 'Configure other BROWSER VULNERABILITY PROTECTION settings as required'. Other settings shown include 'How Often to Check' (Weekly), 'Disable Notification for Browsers' (unchecked), 'Disable Notification for Plugins' (None), and 'Disable Notification for Applications' (None). Under 'BROWSER BLOCKING', the 'Allow All Browsers' checkbox is checked. At the bottom are 'Save' and 'Cancel' buttons.

Slide notes

Configure other 'BROWSER VULNERABILITY PROTECTION' settings as required, for example you can choose to 'Disable Notification for Browsers', ...

Slide 90 - Slide 90

The screenshot shows the Zscaler Policy interface under the 'Browser Control' section. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays 'BROWSER VULNERABILITY PROTECTION' settings, including 'Enable Checks & User Notification' (checked), 'How Often to Check' (set to 'Weekly'), and 'Disable Notification for Browsers' (unchecked). A modal dialog is open for 'Disable Notification for Plugins', with a red box highlighting the 'Unselected Items' list. A callout bubble contains the text 'Select Plugins to disable notifications for'. The list of plugins includes: .NET, Adobe Acrobat, Adobe Flash, DivX, Google Gears, and Java. At the bottom of the dialog are 'Done' and 'Cancel' buttons, and a 'Clear Selection' link.

Slide notes

...you can select individual plugins to disable notifications for, ...

Slide 91 - Slide 91

Select Applications to disable notifications for

Done Cancel Clear Selection

Allow All Browsers

Slide notes

...or you can select applications to disable notifications for.

Slide 92 - Slide 92

The screenshot shows the Zscaler Policy interface with the 'Policy' tab selected. The main area is titled 'Browser Control' and contains a section for 'Configure Browser Control Policy'. It includes a note about reducing security risk by allowing a limited set of browsers. Below this is a 'BROWSER VULNERABILITY PROTECTION' section with settings for 'Enable Checks & User Notification' (checked), 'How Often to Check' (set to 'Weekly'), 'Disable Notification for Browsers' (unchecked), 'Disable Notification for Plugins' (set to 'None'), and a dropdown for 'Disable Network' which is currently set to 'None'. A large callout box with a green border and white background points to the 'Allow All Browsers' checkbox in the 'BROWSER' section. The 'Allow All Browsers' checkbox is checked and has a green border around it. The callout box contains the text 'Click to disable Allow All Browsers'. At the bottom of the screen, there are 'Save' and 'Cancel' buttons, and a status bar at the bottom right indicates the 'Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM'.

Slide notes

The next section allows you to specify which Browsers and Browser versions are permitted, although the default is to allow all Browsers. The Browsers available to select are: 'Microsoft Browsers' (IE and Edge); 'Chrome'; 'Firefox'; 'Safari'; and 'Opera'.

To configure browser restrictions, click to disable the 'Allow All Browsers' option, ...

Slide 93 - Slide 93

The screenshot shows the 'Browser Control' section of the Zscaler interface. It includes settings for 'Disable Notification for Plugins' and 'Disable Notification for Applications'. The 'BROWSER BLOCKING' section is highlighted with a red box around the dropdown menus for various browsers. A callout bubble points to this area with the text 'Configure Browser Blocking as required'. The 'Allow All Browsers' toggle switch is turned off. The dropdown menus for each browser show 'None' selected. At the bottom are 'Save' and 'Cancel' buttons.

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

Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM

Slide notes

Slide 94 - Slide 94

The screenshot shows the 'Browser Control' section of the Zscaler Policy Web Security interface. On the left, a vertical sidebar lists icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has two sections: 'Disable Notification for Plugins' and 'Disable Notification for Applications', both set to 'None'. Below this is the 'BROWSER BLOCKING' section. It includes a toggle switch for 'Allow All Browsers' (which is off) and a dropdown menu for 'Microsoft Browsers' currently set to 'None'. A modal dialog is open, titled 'Configure Browser Blocking as required'. This dialog lists browser versions in two columns: 'Unselected Items' (IE8, IE9, Microsoft Edge Browser 12, Microsoft Edge Browser 14) and 'Selected Items (4)' (IE10, IE11, Microsoft Edge Browser 12, Microsoft Edge Browser 14). Each item in the selected list has a red 'X' icon to its right. At the bottom of the dialog are 'Done', 'Cancel', 'Clear Selection', and 'Save' buttons. The entire 'Selected Items' section is highlighted with a red border. The footer of the page includes copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and a timestamp: 'Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM'.

Slide notes

...configure the Browser versions that you wish to block, ...

Slide 95 - Slide 95

The screenshot shows the Zscaler Policy Web Security interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Browser Control' and contains two sections: 'Disable Notification for Plugins' (set to 'None') and 'Disable Notification for Applications' (set to 'None'). Below this is the 'BROWSER BLOCKING' section, which includes an 'Allow All Browsers' toggle (disabled) and dropdown menus for Microsoft Browsers (set to 'IE10; IE11; Microsoft Edge Browser 12; ...'), Chrome (set to 'None'), Firefox (set to 'None'), Safari (set to 'None'), and Opera (set to 'None'). At the bottom of the configuration window are 'Click Box' and 'Cancel' buttons. A callout bubble with the text 'Click Save' points to the 'Click Box' button. The footer of the interface includes copyright information (Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients), a weblog time (Weblog Time: 10/10/2018 8:49:25 PM), and a last update time (Last Updated: 10/10/2018 8:53:30 PM).

Slide notes

...then 'Save' the configuration, ...

Slide 96 - Slide 96

The screenshot shows the Zscaler Browser Control Policy configuration page. At the top, a message box says "All changes have been saved." On the left, a sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "BROWSER VULNERABILITY PROTECTION". It includes sections for "Enable Checks & User Notification" (checkbox checked), "How Often to Check" (set to "Weekly"), "Disable Notification for Browsers" (checkbox unchecked), "Disable Notification for Plugins" (checkbox unchecked), and "Disable Notification for Applications" (checkbox unchecked). Below these is the "BROWSER BLOCKING" section with "Allow All Browsers" (checkbox checked) and a dropdown menu for "Microsoft Browsers" containing "IE10; IE11; Microsoft Edge Browser 12; ...". At the bottom are "Save" and "Cancel" buttons, and a "Logout" link.

A modal dialog box is overlaid on the page, titled "Alert". It contains the text "Click Save" in a large font, followed by a smaller note: "All the older browser versions will be blocked when the 'Older Versions' checkbox is selected." A blue rectangular box highlights the "Click Save" button.

Slide notes

...and click 'OK' to clear the warning message.

Slide 97 - Slide 97

The screenshot shows the 'Browser Control' configuration page. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation (which is selected), and Search. The main content area is titled 'Configure Browser Control Policy' and includes a note about reducing security risk by limiting supported browsers. The 'BROWSER VULNERABILITY PROTECTION' section contains settings for 'Enable Checks & User Notification' (checked) and 'How Often to Check' (set to 'Weekly'). Below this are sections for 'Disable Notification for Browsers' (set to 'None') and 'Disable Notification for Applications' (set to 'None'). The 'BROWSER BLOCKING' section has 'Allow All Browsers' disabled. Under 'Microsoft Browsers', a dropdown menu lists 'IE10; IE11; Microsoft Edge Browser 12; ...'. At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Slide notes

Then Activate your changes.

Slide 98 - Slide 98

The screenshot shows the Zscaler Policy Web Security interface. On the left, there's a vertical navigation bar with icons for Dashboard, Analytics, Policy (selected), Administration, Activation (with a red notification dot), and Search. The main content area is titled 'CURRENTLY EDITING (1)' and shows a policy for 'admin@policies.zscaler.com'. It includes sections for 'PROTECTION' (set to 'None') and 'FORCE ACTIVATION' (checkbox labeled 'Force Activate' with a blue 'Click Box' overlay). A large callout bubble with the text 'Click Activate' points to the 'Click Box' on the 'Force Activate' checkbox. The bottom of the screen displays copyright information ('Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients') and a timestamp ('Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM').

Slide notes

Slide 99 - Slide 99

The screenshot shows the Zscaler Policy Web Security interface under the 'Browser Control' section. A message at the top says 'Activation Completed!'. On the left, a sidebar lists navigation options: Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main content area is titled 'BROWSER VULNERABILITY PROTECTION' and includes the following settings:

- Enable Checks & User Notification:** Enabled (green checkmark).
- How Often to Check:** Set to 'Weekly'.
- Disable Notification for Browsers:** Disabled (red X).
- Disable Notification for Plugins:** Set to 'None'.
- Disable Notification for Applications:** Set to 'None'.

Below this is the 'BROWSER BLOCKING' section:

- Allow All Browsers:** Enabled (green checkmark).
- Microsoft Browsers:** A dropdown menu lists 'IE10; IE11; Microsoft Edge Browser 12; ...'.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Page footer: Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Policies | Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM

Slide notes

Slide 100 - Slide 100

The screenshot shows the Zscaler Policy Management interface with the 'Policy' tab selected in the sidebar. The main page is titled 'Browser Control' under 'Configure Browser Control Policy'. It includes sections for 'BROWSER VULNERABILITY PROTECTION' and 'BROWSER BLOCKING'. A callout box highlights the 'Recommended Policy' link located in the top right corner of the 'BROWSER VULNERABILITY PROTECTION' section. The interface also features a 'Save' and 'Cancel' button at the bottom.

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

Weblog Time: 10/10/2018 8:49:25 PM | Last Updated: 10/10/2018 8:53:30 PM

Slide notes

To see Zscaler recommendations for configuring 'Browser Control' Policy settings, click the 'Recommended Policy' link.

Slide 101 - Slide 101

The screenshot shows the Zscaler Policy Management interface with the 'Browser Control' policy selected. A modal window titled 'View Recommended Browser Control Policy' is overlaid on the main screen. The modal contains the following configuration options:

- BROWSER VULNERABILITY PROTECTION**
 - Enable Checks & User Notification:
 - How Often to Check: Weekly
 - Disable Notification for Browsers:
 - Disable Notification for Plugins:
 - Disable Notification for Applications:
- BROWSER BLOCKING**
 - Allow All Browsers:
- Microsoft Browsers**
 - iE10;iE11;Microsoft Edge Browser 12;...

At the bottom of the modal, there are 'Save' and 'Cancel' buttons. The background of the main interface shows the policy configuration sections: 'Configure Browser Control Policy' (with a note about older browsers increasing security risk), 'BROWSER VULNERABILITY PROTECTION' (with the same note), and 'BROWSER BLOCKING' (with the 'Allow All Browsers' setting). The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search.

Slide notes

For the 'Browser Control' Policy Zscaler recommends that you disable checks and user notification and allow all Browsers.

Slide 102 - Thank you & Quiz



Thank you & Quiz

Slide notes

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

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