

Slide 1 - Zscaler Policies



Zscaler Policies

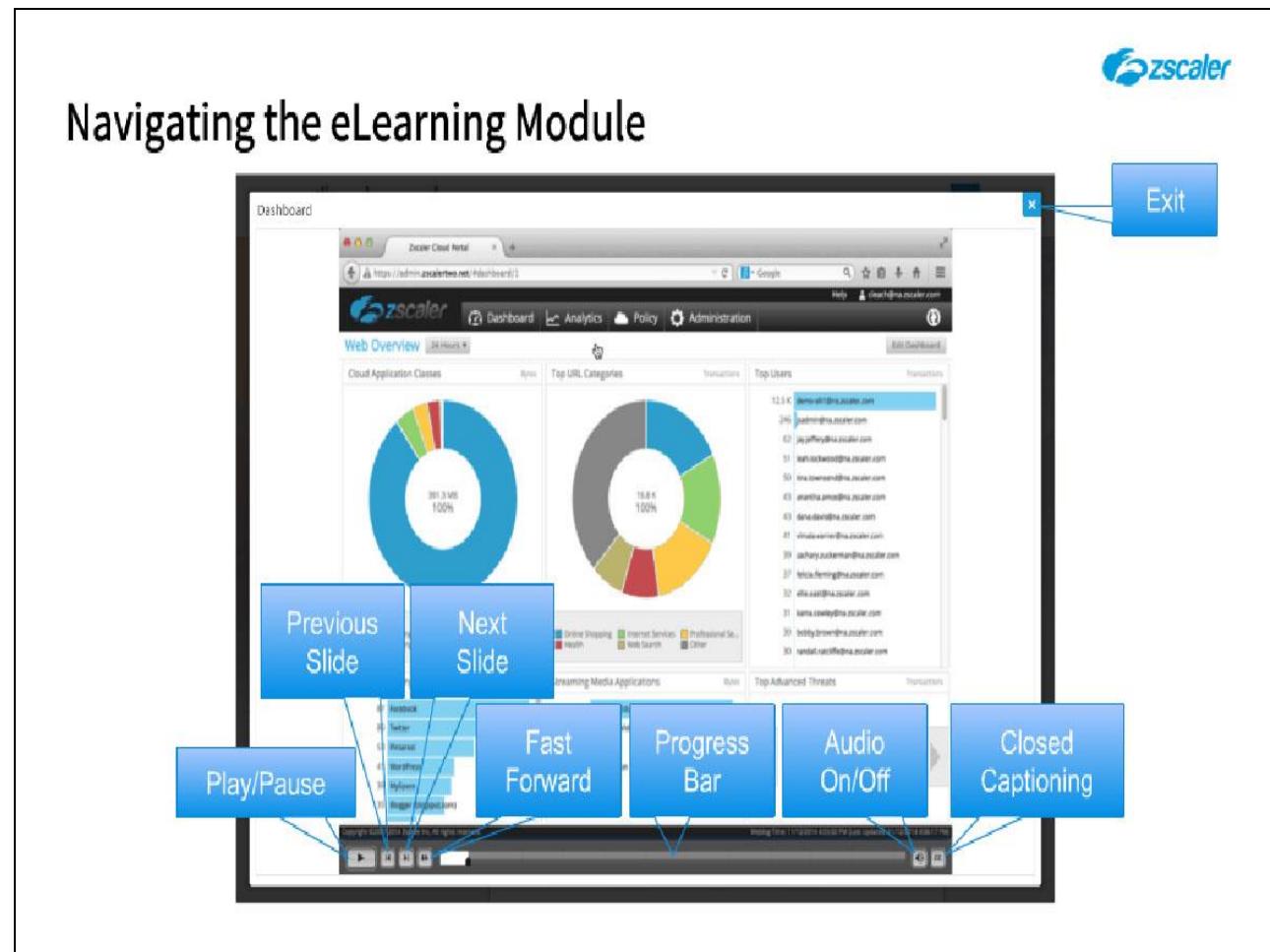
Cloud Firewall

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to the Zscaler Cloud Firewall Policies Module.

Slide 2 - Navigating the eLearning Module



Slide notes

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

Slide 3 - Agenda

Agenda



- Firewall Policy Overview
- Interactive Demo: Firewall Preliminaries
- Interactive Demo: Creating Firewall Policy

Slide notes

In this module, we will cover: an overview of the Firewall policies available; a detailed look at the configurations necessary to enable the Cloud Firewall; and a detailed look at creating Firewall, DNS Control, and FTP Control policies.

Slide 4 - Mobile and Firewall Policy Overview

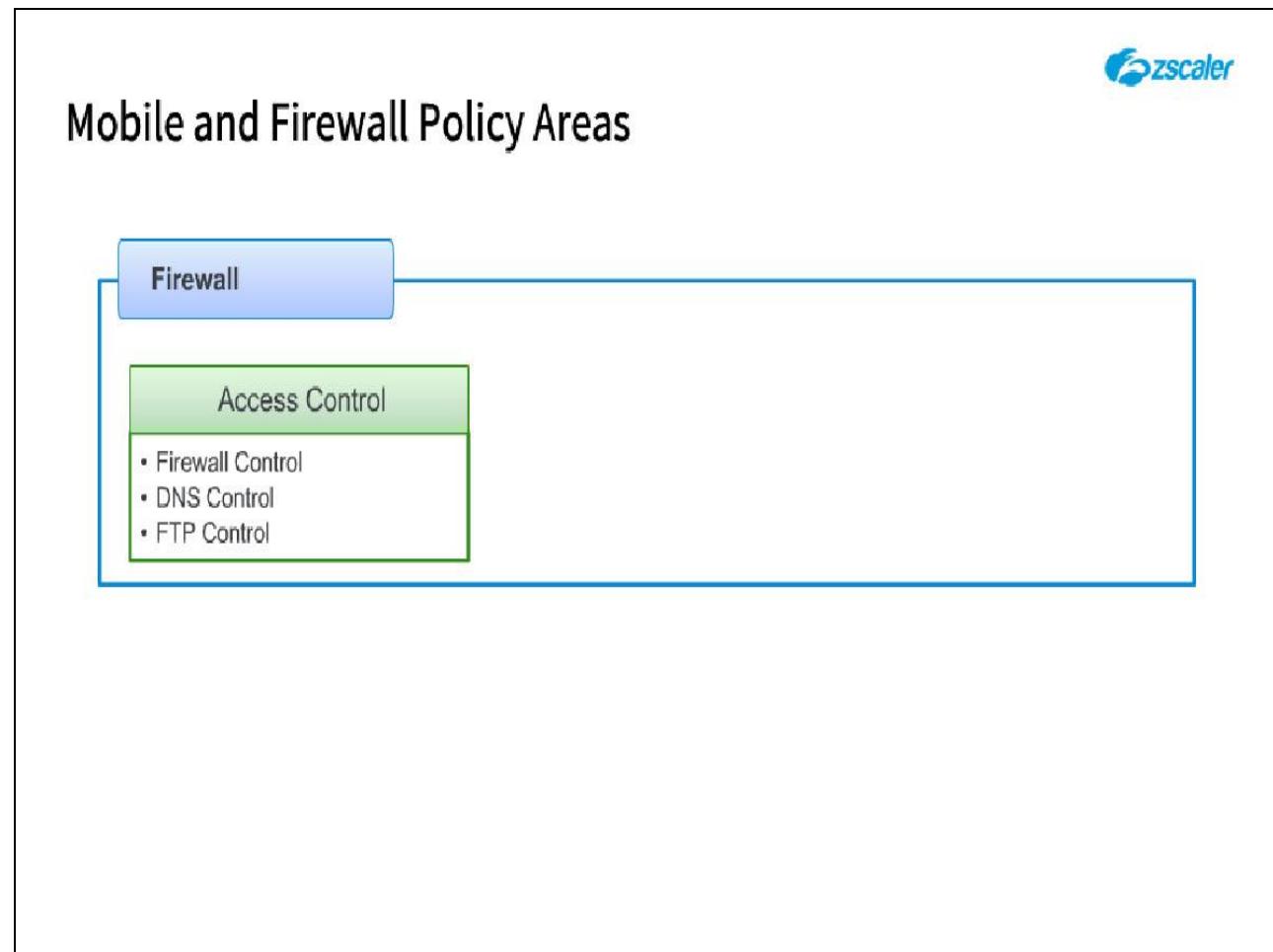


Firewall Policy Overview

Slide notes

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

Slide 5 - Mobile and Firewall Policy Areas



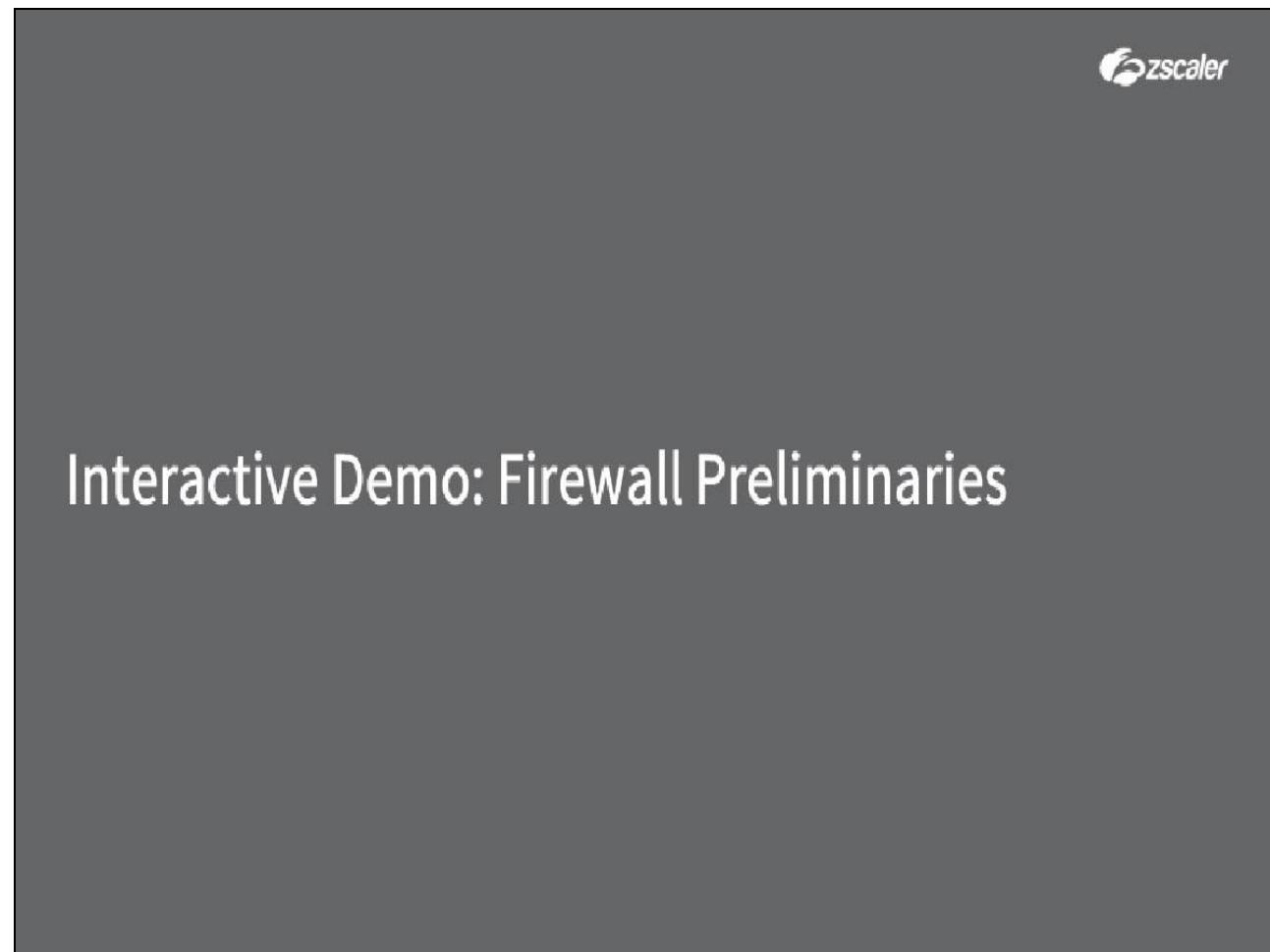
Slide notes

The Firewall policy area allows the configuration of **Access Control** policies for the Zscaler **Basic** and **Advanced** Cloud Firewall capability. In this module we will look at each of the policies available in each section and provide some recommendations for the policy settings.

Note that, with a **Basic** Cloud Firewall subscription, you can only create Firewall rules using the 5 well-known **tuples**: source and destination IP addresses; source and destination ports; and protocol.

With an **Advanced** Cloud Firewall subscription, you can make use of the Zscaler default **Network Services**, and **Network Application** definitions, or create your own custom services.

Slide 6 - Interactive Demo: Firewall Policy



Slide notes

In the next section, we will have a detailed look at the Firewall Policy area, and in particular examine the preliminary configurations required to enable the Zscaler Cloud Firewall.

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 7 - Slide 7



Slide notes

First, we'll enable the Cloud Firewall for an existing location. From the **Administration** menu, click **Locations**.

Slide 8 - Slide 8



Slide notes

Click Locations.

Slide 10 - Slide 10

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration (which is selected), Activation, and Search. The main area is titled 'Locations' and contains a table with three rows of location data. The columns include No., Name, IP Addresses, Proxy Ports, X-Forwarded-For..., Authentication, SSL, Firewall Filtering, Bandwidth, Virtual Service E..., Group, and three edit icons. A callout box with the text 'Click to edit a Location' points to the edit icon for the first location. The bottom of the screen shows copyright information and a help icon.

No.	Name	IP Addresses	Proxy Ports	X-Forwarded-For...	Authentication	SSL	Firewall Filtering	Bandwidth	Virtual Service E...	Group
1	> trainingsafemarch...	---	---	---	Enabled: IP Surrogat...	---	---	---	---	---
2	trainingsafemarch15 ...	---	---	---	---	Enabled	---	---	---	---
3	trainingsafemarch2 / ...	---	10230	---	Enabled	Enabled	Enabled	---	---	---

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies Weblog Time: 1/2/2020 1:39:46 PM Last Updated: 1/2/2020 1:42:22 PM Help

Slide notes

Click the **Edit** icon for the Location where you want to enable the Cloud Firewall.

Slide 11 - Slide 11

The screenshot shows the 'Edit Location' dialog box. In the 'Gateway Options' section, the 'Enable IP Surrogate' checkbox is selected (green). To the right, the 'Idle Time to Disassociation' dropdown is set to '8 Hours'. A callout bubble highlights these settings with the instructions: 'Select Enable IP Surrogate' and 'Set Idle Time to Disassociation to 8 Hours'.

Slide notes

In the **Gateway Options** section, select the **Enable IP Surrogate** option, and set the idle time to 8 hours.

Slide 12 - Slide 12

Locations

LOCATION

Name: trainingzafemarch1 / Headquarters

Country: United States

State/Province:

Time Zone: America/Los Angeles

Group: None

ADDRESSING

Static IP Addresses: None

Proxy Ports: None

VPN Credentials: si4b42cdc0@training.zafemarch.com

Virtual Service Edges: None

Virtual Service Edge Clusters: None

GATEWAY OPTIONS

Enable XFF Forwarding:

Enable IP Surrogate:

Enforce Surrogate IP for Known Browsers:

Enable SSL Inspection:

Enforce Firewall Control: Click Box

Enforce Authentication:

Idle Time to Disassociation: 8 Hours

Enforce Zscaler App SSL Setting:

Save Cancel Delete Help

Slide notes

Enable the **Enforce Firewall Control** option and click **Save**.

Slide 13 - Slide 13

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Locations' and shows a list of existing locations: 'trainingzafemarch1 / Headquarters' (No. 1), 'trainingzafemarch15' (No. 2), and 'trainingzafemarch07' (No. 3). A modal window titled 'Edit Location' is open, allowing the configuration of a new location. The 'LOCATION' section includes fields for Name (set to 'trainingzafemarch1 / Headquarters'), Country (set to 'United States'), State/Province, Time Zone (set to 'America/Los Angeles'), and Group (set to 'None'). The 'ADDRESSING' section includes fields for Static IP Addresses (set to 'None'), Proxy Ports (set to 'None'), VPN Credentials (set to 'si4b42cdc0@training.zafemarch.com'), and Virtual Service Edges (set to 'None'). The 'GATEWAY OPTIONS' section includes checkboxes for various features: 'Enable XFF Forwarding' (unchecked), 'Enforce Authentication' (checked), 'Enable IP Surrogate' (checked), 'Idle Time to Disassociation' (set to 8 hours), 'Enforce Surrogate IP for Known Browsers' (unchecked), 'Enable SSL Inspection' (unchecked), 'Enforce Zscaler App SSL Setting' (unchecked), 'Enforce FIPS' (checked), and 'Enable IPS Control' (unchecked). A large 'Click Save' button is overlaid on the standard 'Save' button at the bottom of the dialog. The status bar at the bottom right indicates a 'Working Time: 1/13/2020 1:39:46 PM | Last Updated: 1/13/2020 1:42:35 PM'.

Slide notes

Slide 19 - Slide 19

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, ClickBox (with a red notification badge), and Search. The main content area is titled 'Locations' and displays a table of location settings. The table has columns for No., Name, IP Addresses, Proxy Ports, X-Forwarded-For..., Authentication, SSL, Firewall Filtering, Bandwidth, Virtual Service E..., Group, and actions. Three rows are listed:

No.	Name	IP Addresses	Proxy Ports	X-Forwarded-For...	Authentication	SSL	Firewall Filtering	Bandwidth	Virtual Service E...	Group
1	> trainingsafemarch...	---	---	---	Enabled: IP Surrogat...	---	Enabled	---	---	---
2	trainingsafemarch15 ...	---	---	---	---	---	Enabled	---	---	---
3	trainingsafemarch2 / ...	---	10230	---	Enabled	Enabled	Enabled	---	---	---

A callout box with the text 'Click Activation' points to the 'Activation' button in the ClickBox sidebar. The ClickBox sidebar also includes a 'Search' icon. At the bottom of the screen, there are copyright and help information.

Slide notes

Then **Activate** your changes.

Slide 20 - Slide 20

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, a dark sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation (which is highlighted in blue), and Search. The main area is titled 'MY ACTIVATION STATUS' and shows 'CURRENTLY EDITING (1)' with the URL 'admin@zscaler.com'. Below this, 'QUEUED ACTIVATIONS (0)' is listed as 'None'. A 'Force Activate' button is visible. A large 'Click Box' is overlaid on the interface, pointing to the 'Force Activate' button. The main content area displays a table with columns: IP Addresses, Proxy Ports, X-Forwarded-For..., Authentication, SSL, Firewall Filtering, Bandwidth, Virtual Service E..., Group, and three more columns represented by ellipses (...). The table has three rows. The first row shows 'Enabled: IP Surrogat...' under Authentication. The second row shows 'Enabled' under Authentication. The third row shows 'Enabled' under Authentication and 'Enabled' under SSL.

Slide notes

Slide 26 - Slide 26

The screenshot shows the Zscaler Cloud Firewall interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Click Box (highlighted in blue), Activation, Search, and other navigation links. The main content area is titled 'Locations' and displays a table of location settings. The table has columns for No., Name, IP Addresses, Proxy Ports, X-Forwarded-For..., Authentication, SSL, Firewall Filtering, Bandwidth, Virtual Service E..., Group, and actions. Three rows are listed:

No.	Name	IP Addresses	Proxy Ports	X-Forwarded-For...	Authentication	SSL	Firewall Filtering	Bandwidth	Virtual Service E...	Group
1	> trainingsafemarch...	---	---	---	Enabled: IP Surrogat...	---	Enabled	---	---	---
2	trainingsafemarch15 ...	---	---	---	---	---	Enabled	---	---	---
3	trainingsafemarch2 / ...	---	10230	---	Enabled	Enabled	Enabled	---	---	---

A callout box with the text 'Click Administration' points to the 'Administration' icon in the sidebar. The bottom of the screen shows copyright information and a help icon.

Slide notes

Traffic from this location will now begin flowing through the Cloud Firewall module.

Creating and managing Cloud Firewall policies is very similar to creating **Cloud Application Control** and **URL Filtering** policies.

But before we do that, let's look at the various ways Zscaler classifies traffic for the firewall; **Network Services**, and **Network applications**. From the **Administration** menu

Slide 27 - Slide 27

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, there is a navigation sidebar with various icons and links. A callout bubble points to the 'Network Services' link under the 'TRAFFIC FORWARDING' section. The main content area displays a table of proxy ports with columns for Proxy Ports, X-Forwarded-For..., Authentication, SSL, Firewall Filtering, Bandwidth, Virtual Service E..., Group, and actions. The table has three rows of data. At the bottom of the page, there is a URL bar showing the address https://admin.zscaler.net/administration/my-profile and a status bar indicating the Weblog Time and Last Updated.

Proxy Ports	X-Forwarded-For...	Authentication	SSL	Firewall Filtering	Bandwidth	Virtual Service E...	Group	
---	---	Enabled: IP Surrogat...	---	Enabled	---	---	---	
---	---	---	---	Enabled	---	---	---	
10230	---	Enabled	Enabled	Enabled	---	---	---	

Callout text: Click Network Services

URL: https://admin.zscaler.net/administration/my-profile

Weblog Time: 1/2/2020 1:39:46 PM Last Updated: 1/2/2020 1:42:22 PM

Slide notes

click Network Services.

Slide 29 - Slide 29

The screenshot shows the 'Network Services' section of the Zscaler interface. The table lists various network services with columns for No., Name, TCP Source Ports, TCP Destination Ports, UDP Source Ports, UDP Destination Ports, and Description. An annotation with a callout box and the text 'Click Add Network Service' points to the 'Add Click Box' button in the top-left corner of the table header.

No.	Name	TCP Source Ports	TCP Destination Ports	UDP Source Ports	UDP Destination Ports	Description
1	AIM	...	5190	AIM (originally AOL Instant Messenger) is an insta...
2	DNS	...	53	...	53	The DNS protocol is used to translate internet na...
3	Echo		7	...	7	Echo Protocol is a service in the Internet Protocol ...
4	FTP		21	The FTP protocol is used for reliable data transfer ...
5	FTPS		990	...	990	Implicit FTPS: Implicit FTPS automatically starts a...
6	Gnutella	...	6346-6347	...	6346-6347	Gnutella is a peer-to-peer protocol
7	H.323	...	1503, 1720, 1731, 389, 522	...	1719	H.323 is a standard approved by the International ...
8	HTTP	...	80	The Hypertext Transfer Protocol (HTTP) is used fo...
9	HTTP Proxy	...	3128, 8080	HTTP tunneling is a technique by which commun...
10	HTTPS	...	443	HTTPS is the secure version of HTTP
11	ICMP	ICMP is one of the main protocols of the Internet ...
12	Ident	...	113	The Identification Protocol provides a means to d...
13	IKE	...	500	...	500	IKE is a protocol to obtain authenticated keying m...
14	IKE-NAT	4500	IKE-NAT allows Network Address Translation for I...
15	ILS	...	1002, 389, 522, 636	Internet Locator Service includes LDAP, User Loc...
16	IMAP	...	143, 220, 993	...	220	Internet Message Access Protocol is a protocol u...
17	IRC	...	6660-6669	IRC (Internet Relay Chat) is an instant messaging ...
18	Kerberos	...	88	...	88	Kerberos is a computer network authentication pr...
19	L2TP	1701	Layer Two Tunneling Protocol (L2TP) is an extensi...
20	LDAP	...	389	LDAP (Lightweight Directory Access Protocol) is a...

Slide notes

This is the pre-defined list of applications and the well-known port numbers used, which can be used to write traditional firewall policies where you specify a TCP or UDP port.

They can also be combined with applications to limit how a policy is applied, and we'll talk more about that later. You can create custom services by clicking the **Add Network Service** link.

Slide 30 - Slide 30

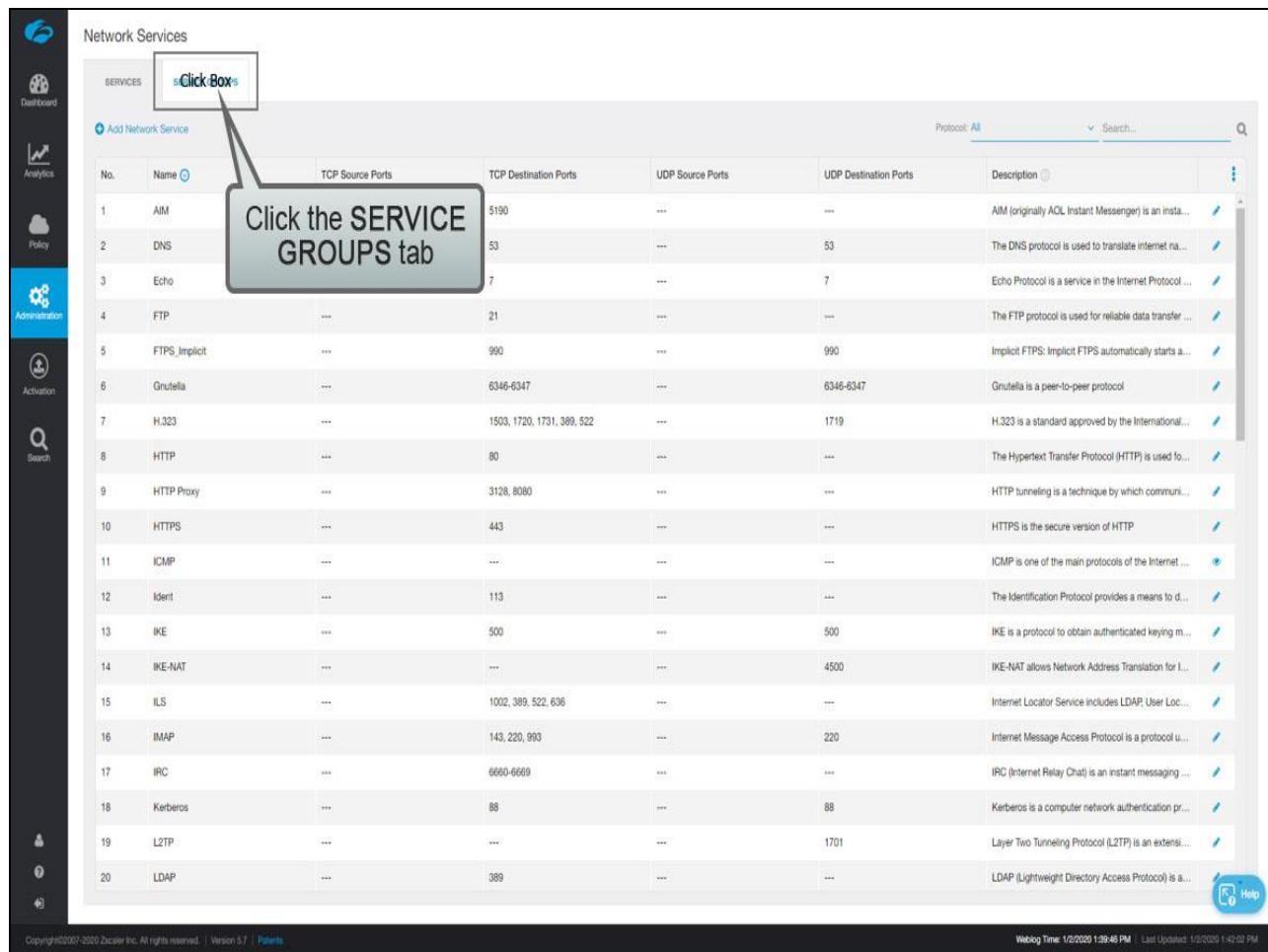
Specify services by Protocol, Source, and Destination Ports as necessary

Slide notes

Services can be specified by Layer 4 protocol (TCP or UDP), and by any combination of source, or destination Ports.

You can create network services with overlapping ports for the same protocols and add these network services to the **Firewall Control** policy rules. For example, FTP on port 21 is a standard network service, a custom network service that includes port 21 can now also be defined.

Slide 32 - Slide 32



The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Network Services' and contains a table of network services. The table has columns for No., Name, TCP Source Ports, TCP Destination Ports, UDP Source Ports, UDP Destination Ports, and Description. A callout box with the text 'Click the SERVICE GROUPS tab' points to the tab in the top navigation bar.

No.	Name	TCP Source Ports	TCP Destination Ports	UDP Source Ports	UDP Destination Ports	Description
1	AIM	5190	---	---	---	AIM (originally AOL Instant Messenger) is an instant messaging protocol developed by America Online.
2	DNS	53	---	---	53	The DNS protocol is used to translate internet names and addresses into IP addresses.
3	Echo	7	---	---	7	Echo Protocol is a service in the Internet Protocol suite.
4	FTP	---	21	---	---	The FTP protocol is used for reliable data transfer between computers.
5	FTPS_Implicit	---	990	---	990	Implicit FTPS: Implicit FTPS automatically starts a secure connection.
6	Gnutella	---	6346-6347	---	6346-6347	Gnutella is a peer-to-peer protocol.
7	H.323	---	1600, 1720, 1731, 389, 522	---	1719	H.323 is a standard approved by the International Telecommunication Union.
8	HTTP	---	80	---	---	The Hypertext Transfer Protocol (HTTP) is used for transmitting files over the web.
9	HTTP Proxy	---	3128, 8080	---	---	HTTP tunneling is a technique by which communication is carried out through an HTTP proxy.
10	HTTPS	---	443	---	---	HTTPS is the secure version of HTTP.
11	ICMP	---	---	---	---	ICMP is one of the main protocols of the Internet.
12	Ident	---	113	---	---	The Identification Protocol provides a means to determine the user identity.
13	IKE	---	500	---	500	IKE is a protocol to obtain authenticated keying material.
14	IKE-NAT	---	---	---	4500	IKE-NAT allows Network Address Translation for IPsec.
15	ILS	---	1002, 389, 522, 636	---	---	Internet Locator Service includes LDAP, User Location, and DNS.
16	IMAP	---	143, 220, 993	---	220	Internet Message Access Protocol is a protocol used for reading emails.
17	IRC	---	6660-6669	---	---	IRC (Internet Relay Chat) is an instant messaging protocol.
18	Kerberos	---	88	---	88	Kerberos is a computer network authentication protocol.
19	L2TP	---	---	---	1701	Layer Two Tunneling Protocol (L2TP) is an extension of PPTP.
20	LDAP	---	389	---	---	LDAP (Lightweight Directory Access Protocol) is a directory access protocol.

Copyright © 2000-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies | Weblog Time: 1/2/2020 1:39:46 PM | Last Updated: 1/2/2020 1:42:22 PM | Help

Slide notes

You can also group network services by clicking the **Service Groups** tab.

Slide 33 - Slide 33

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration (which is selected), Activation, and Search. The main area is titled 'Network Services' and has tabs for 'SERVICES' (selected) and 'SERVICE GROUPS'. A large callout box with the text 'Click Add Network Service Group' points to the 'Add Network Service Group' button, which is highlighted with a blue border. Below the table, there is a note: 'This is simply a way to apply rules to common sets of services. To add a network service group, click the Add Network Service Group link.' At the bottom of the screen, there is a footer with copyright information and help links.

Slide notes

This is simply a way to apply rules to common sets of services. To add a network service group, click the **Add Network Service Group** link.

Slide 34 - Slide 34

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Services". It has two tabs: "SERVICES" (selected) and "SERVICE GROUPS". Below the tabs, there is a search bar and a button for "Add Network Service Group". A table lists one service group: "Test Services Group" with services "DNS, FTP, Echo, AIM". The "Add Network Service Group" dialog is open in the center. It has fields for "Name" (set to "None") and "Services" (dropdown menu). There is also a "Description" text area and "Save" and "Cancel" buttons at the bottom.

Slide notes

Slide 35 - Slide 35

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Network Services' and shows a table with one row: 'Test Services Group' with services 'DNS, FTP, Echo, AIM'. A modal window titled 'Add Network Service Group' is open. It has fields for 'Name' (empty) and 'Description' (empty). Below these is a 'Services' section with a 'None' button. A large red box highlights the 'Selected Items (0)' section, which contains a search bar and a list of services: AIM, DNS, Echo, FTP, FTPS_Implicit, and Grutella. At the bottom of this section are 'Done' and 'Cancel' buttons, and a 'Clear Selection' link. A callout box with a red border and white text says 'Add Services as necessary'.

Slide notes

Add the **Services** required and **Save** the configuration.

Slide 37 - Slide 37

The screenshot shows the 'Network Services' section of the Zscaler Cloud Firewall interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Click Administration (which is highlighted with a gray box and labeled 'Click Administration'), Activation, Search, and other less visible options. The main area displays a table titled 'Add Network Service Group'. The table has columns for 'No.', 'Name', 'Services', and 'Description'. A single row is present with 'No.' 1, 'Name' 'Test Services Group', 'Services' 'DNS, FTP, Echo, AIM', and 'Description' '...'. There are also 'Edit' and 'Delete' buttons for this row. A search bar at the top right is empty. At the bottom of the page, there is a footer with copyright information and a help icon.

Slide notes

This is simply a way to apply rules to common sets of services. To add a network service group, click the **Add Network Service Group** link.

Now, let's click on **Network Applications**, as this is the meat of the Zscaler Cloud Firewall implementation.

Slide 38 - Slide 38

The screenshot shows the Zscaler Policy-Cloud Firewall Administration interface. On the left, there is a navigation sidebar with various icons and sections: Dashboard, Analytics, Policy, Administration (which is selected and highlighted in blue), Activation, Search, and Help. The main content area is titled "Network Applications". It contains sections for "CLOUD CONFIGURATION" (Nanolog Streaming Service, Advanced Settings, Virtual Service Edges, ICAP Settings, Partner Integrations) and "AUTHENTICATION" (Authentication Settings, User Management, Identity Proxy Settings). Below these are sections for "TRAFFIC FORWARDING" (Locations, VPN Credentials, Hosted PAC Files, e2 Agent Configurations, SecureAgent Notifications), "DATA LOSS PREVENTION" (DLP Dictionaries & Engines, DLP Notification Templates), and "FIREWALL FILTERING" (Network Services, IP & FQDN Groups). A callout box with the text "Click Network Applications" points to the main title of the section.

Slide notes

Slide 39 - Slide 39

The screenshot shows the Zscaler Cloud Firewall interface under the 'Network Applications' section. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays a table of applications. At the top of the table, there are tabs: 'APPLICATIONS' (which is selected), 'APPLICATION GROUPS' (highlighted with a red box and a callout bubble saying 'Click APPLICATION GROUPS'), and 'DNS APPLICATION GROUP'. The table has columns for 'No.', 'Name', 'Protocol', and 'Description'. The 'APPLICATION GROUPS' tab is currently active, showing a list of 20 applications. The bottom right corner of the interface has a 'Help' icon.

No.	Name	Protocol	Description
1	050 plus	Web	An embedded smartphone application dedicated to audio-conferencing
2	2CH	Web	A Chinese video sharing website
3	3GPP (U)	Tunneled traffic	3GPP (U) is a protocol which form a standard for telecoms operators and networks operators
4	ABC News	Web	This protocol plug-in classifies the http traffic to the hosts abcnews.com and abcnews.go.com
5	About.com	Web	This protocol plug-in classifies the http traffic to the host about.com
6	AccuWeather	Web	This protocol plug-in classifies the http traffic to the host accuweather.com
7	Acer	Web	This protocol plug-in classifies the http traffic to the host acer.com
8	Acrobat Connect	Enterprise	Adobe Connect is a web conferencing platform for web meetings, eLearning, and webin...
9	ActiveSync	Web	Microsoft ActiveSync is a mobile data synchronization technology and protocol developed by Microsoft, originally released in 1996
10	ADC	Peer-to-Peer	ADC is a peer-to-peer protocol widely used in Direct Connect networks
11	Addicting Games	Web	This protocol plug-in classifies the http traffic to the host addictinggames.com
12	Adidas	Web	The Adidas AG is a major German sports apparel manufacturer
13	adistream	Web	This protocol plug-in classifies the ssl traffic to the Common Name adistream.tv
14	Adobe Acrobat	Web	This protocol plug-in classifies the http traffic to the host www.acrobat.com. It also classifies the ssl traffic to the Common Name www.acrobat.com
15	Adobe Connect	Streaming Media	Adobe Connect is a web communication system for the training, the marketing, the conferences and the online collaboration
16	Adobe Connect for Web Meetings	Web	This protocol plug-in classifies the http traffic to the hosts connectpro097286496.emea.acrobat.com, connectpro097286496.adobeconnect.com and www.emea.acrobat.com. It also classifies th...
17	Adobe Flash (swf)	Streaming Media	Adobe Flash Media Playback is a dynamic HTTP streaming protocol used to access video contents from a smart client application
18	Adobe Update Manager	Web	Adobe Update Manager is a program which maintains up-to-date versions of some Adobe software
19	adp client	Web	Provider of human resources management software
20	ADrive	Web	This protocol plug-in classifies the http traffic to the host adrive.com. It also classifies the ssl traffic to the Common Name adrive.com

Slide notes

This is a list of applications that are recognized by the Cloud Firewall engine. These applications can be detected regardless of the Layer 4 port or protocol being used.

You'll notice many of the applications listed here are part of the **Web** category. This allows another level of policy enforcement beyond what's available in the **Cloud Application Control and URL Filtering Policies**.

As with **Network Services** you can also group **Network Applications** into **Application Groups** to simplify your ruleset. Click the **APPLICATION GROUPS** tab.

Slide 40 - Slide 40

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for "APPLICATIONS", "APPLICATION GROUPS", and "DNS APPLICATION GROUP". Under "APPLICATION GROUPS", there is a section titled "Add Network Application Group" with a search bar. Below this is a table with two rows:

No.	Name	Applications	Description
1	Microsoft Office365	Office365, OneDrive, Outlook, SharePoint, SharePoint Admin, SharePoint Blog, SharePoint ...	Microsoft Office365
2	Test Group - Facebook	Facebook, Facebook Apps, Faceparty, Faces	Facebook app group

A callout box with the text "Click to edit an Application Group" points to the edit icon (pencil icon) in the header of the Microsoft Office365 row. The bottom of the screen shows copyright information and a help icon.

Slide notes

As you can see there is a default application group for Microsoft Office365 applications. Click the **Edit** icon to view the group

Slide 42 - Slide 42

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Network Applications' and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. Under APPLICATIONS, there are two entries: 'Microsoft Office365' and 'Test Group - Facebook'. The 'Edit Network Application Group' dialog is open for 'Microsoft Office365'. It has fields for 'Name' (set to 'Microsoft Office365') and 'Description' (set to 'Microsoft Office365'). Below these are two lists: 'Unselected Items' (which is empty) and 'Selected Items (10)' (which contains the list of applications mentioned in the callout). A red box highlights the 'Selected Items (10)' list, and a callout bubble with the text 'Review the Applications list' points to it.

Slide notes

which contains all of the Office365 applications.

Slide 43 - Slide 43

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications". It has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-tab "Add Network Application Group" is selected. Below this, a table lists two application groups:

No.	Name	Applications	Description
1	Microsoft Office365	Office365, OneDrive, Outlook, SharePoint, SharePoint Admin, SharePoint Blog, SharePoint ...	Microsoft Office365
2	Test Group - Facebook	Facebook, Facebook Apps, Faceparty, Faces	Facebook app group

A modal window titled "Edit Network Application Group" is open, showing the details for the "Microsoft Office365" group. It includes fields for Name (Microsoft Office365), Applications (Office365; OneDrive; Outlook; SharePoin...), and Description (Microsoft Office365). At the bottom of the modal are "Save" and "Cancel" buttons, with "Delete" highlighted by a red box.

Slide notes

Slide 44 - Slide 44

Network Applications

APPLICATIONS APPLICATION GROUPS DNS GROUP Click Box

Add Network Application Group

No.	Name	Applications	Description
1	Microsoft Office365	Office365, OneDrive, Outlook, SharePoint, SharePoint Admin, SharePoint Blog, SharePoint ...	Microsoft Office365
2	Test Group - Facebook	Facebook, Facebook Apps, Faceparty, Faces	Facebook app group

Search... Q

Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies Weblog Time: 1/2/2020 1:39:46 PM Last Updated: 1/2/2020 1:42:22 PM

Slide notes

In addition to applications and application groups, DNS application groups may also be configured for use in rules to control traffic identified by DNS Tunneling Detection. Click the **DNS Application Group** tab.

Slide 45 - Slide 45

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration (which is selected), Activation, Search, and other management functions. The main area is titled 'Network Applications' and shows three tabs: APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. The APPLICATION GROUPS tab is selected. A sub-tab 'DNS APPLICATION GROUP' is also visible. In the center, there is a table with columns 'No.', 'Name', and 'Application'. A callout box with the text 'Click Add DNS Application Group' points to the 'Add DNS Application Group' button located in the top-left corner of the table area. The status bar at the bottom indicates 'Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies' and 'Weblog Time: 1/2/2020 1:39:46 PM Last Updated: 1/2/2020 1:42:22 PM'.

Slide notes

A common use case would be to add a **DNS Application Group** for use in a rule to block DNS tunnel traffic. To add a **DNS Application Group**, follow these steps: Click **Add DNS Application Group**.

Slide 46 - Slide 46

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for "APPLICATIONS", "APPLICATION GROUPS", and "DNS APPLICATION GROUP". A sub-header says "Add DNS Application Group". Below it, there's a search bar and a table with columns "No.", "Name", "Applications", and "Description". A message at the bottom of the table says "No matching items found". In the center, a modal window titled "Add DNS Application Group" is open. It has fields for "Name" (containing "All DNS Tunnels") and "DNS Tunnels & Network Apps" (set to "None"). There's also a "Description" field which is empty. At the bottom of the modal are "Save" and "Cancel" buttons. The footer of the page includes copyright information ("Copyright © 2019 Zscaler Inc. All rights reserved. | Version 5.7 | Products") and a help icon.

Slide notes

In the **Add DNS Application Group** window, type a name for the group.

Slide 47 - Slide 47

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Network Applications' and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-menu 'Add DNS Application Group' is open. The 'Name' field is populated with 'All DNS Tunnels'. A dropdown menu labeled 'DNS Tunnels & Network Apps' is expanded, showing 'None' as the current selection. A callout bubble points to this dropdown with the instruction 'Click DNS Tunnels & Network Apps'. The 'Description' field is empty. At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows a list of applications with a search bar and a message 'No matching items found'.

Slide notes

Take a look at the DNS tunnels that are identified and how they are grouped in categories. Click **DNS Tunnels & Network Apps** and select and examine the three tunnel categories.

Slide 48 - Slide 48

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A search bar at the top right says "Search...". Below the tabs, there's a table with columns "No.", "Name", "Applications", and "Description". A message at the bottom of the table says "No matching items found". In the center, a modal window titled "Add DNS Application Group" is open. It has fields for "Name" (set to "All DNS Tunnels") and "Description". Below these are two tabs: "Unselected Items" and "Selected Items (0)". The "Unselected Items" tab contains a list of checkboxes, one of which is highlighted with a red border and a callout box pointing to it. The callout box contains the text "Click Commonly Allowed DNS Tunnels". At the bottom of the modal are "Save" and "Cancel" buttons. The footer of the page includes copyright information ("Copyright © 2019 Zscaler Inc. All rights reserved. | Version 5.7 | Products") and a help icon.

Slide notes

Click Commonly Allowed DNS Tunnels.

Slide 49 - Slide 49

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-header says "Add DNS Application Group". Below it, there's a search bar and a table with columns for No., Name, Applications, and Description. A message says "No matching items found". Overlaid on this is a modal window titled "Add DNS Application Group". It has fields for "Name" (set to "All DNS Tunnels") and "Description". On the right side of the modal is a large red box highlighting a list of selected items under "Selected Items (19)". The list includes: BostonNews, CCM, Cymru, DeviceScope, DnsTunGoodRvrd, Esxt, FlyingMag, Ipass, and McAfee. There are also other items like Commonly Allowed DNS Tunnels, BostonNews, CCM, Cymru, DeviceScope, and DnsTunGoodRvrd which are unselected. At the bottom of the modal are "Done" and "Cancel" buttons, and a "Clear Selection" link.

Slide notes

Tunnels in this category use DNS tunneling for productive reasons such as updates coming from security services.

Slide 51 - Slide 51

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A modal window titled "Edit DNS Application Group" is open, showing a list of applications under "DNS APPLICATION GROUP". The "Name" field is set to "All DNS Tunnels" and the "Description" field is empty. The "Unselected Items" list contains several applications, and the "Selected Items (19)" list contains 19 items, including "BostonNews", "CCM", "Cymru", "DeviceScape", "DnsTunGoodRvrd", "Esxt", "FlyingMag", "Ipass", and "McAfee". A callout box points to the "Selected Items" list with the text "Click Commonly Blocked DNS Tunnels".

Slide notes

Click Commonly Blocked DNS Tunnels.

Slide 52 - Slide 52

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A modal window titled "Edit DNS Application Group" is open. It shows a table with two columns: "Unselected Items" and "Selected Items (26)". The "Selected Items" column contains a list of 26 items, many of which are checked. A red box highlights this list. At the bottom of the modal are "Done" and "Cancel" buttons.

Slide notes

Tunnels in this category are those detected by Zscaler as malicious or can cause a loss of productivity or data.

Slide 55 - Slide 55

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Network Applications' and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-section titled 'Add DNS Application Group' is visible. Below it, a table lists one application group named 'All DNS Tunnels' with the description 'BaiduYunDns; BostonNews; CCM; Cymru; DeviceScape; DnsTunGoodRsvd; DnsTunMalici...'. A modal window titled 'Edit DNS Application Group' is open. It contains a 'DNS APPLICATION GROUP' section with 'Name' set to 'All DNS Tunnels' and 'Description' empty. Below this is a list of items divided into 'Unselected Items' and 'Selected Items (26)'. The 'Unselected Items' list includes 'Unknown DNS Tunnels' (with a checked checkbox), 'Click Box', and 'dnsTununknownRsv'. The 'Selected Items' list includes BaiduYunDns, BostonNews, CCM, Cymru, DeviceScape, DnsTunGoodRsvd, DnsTunMaliciousRsvd, Eset, and FlyingMag. At the bottom of the modal are 'Save' and 'Cancel' buttons, along with 'Done' and 'Clear Selection' buttons.

Slide notes

Click Unknown DNS Tunnels.

Slide 56 - Slide 56

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-section titled "Add DNS Application Group" is visible. Below it, a table lists one item: "All DNS Tunnels" with applications "BaiduYunDns, BostonNews, CCM, Cymru, DeviceScape, DnsTunGoodRsvd, DnsTunMalici...". A search bar and a refresh button are also present.

A modal window titled "Edit DNS Application Group" is open. It contains a "DNS APPLICATION GROUP" section with a "Name" field set to "All DNS Tunnels" and a "Description" field. To the right is a list of items divided into "Unselected Items" and "Selected Items (27)". The "Selected Items" list is highlighted with a red border and contains the following items:

- BaiduYunDns
- BostonNews
- CCM
- Cymru
- DeviceScape
- DnsTunGoodRsvd
- DnsTunMaliciousRsvd
- DnsTunUnknownRsvd
- Eset

At the bottom of the modal are "Save" and "Cancel" buttons, and a "Click Box" button with a speech bubble pointing to it containing the text "Click Done".

Slide notes

Tunnels in this category are detected but not yet classified in the previous two categories. Click **Done**.

Slide 57 - Slide 57

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Network Applications" and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-section titled "Add DNS Application Group" is visible. Below it, a table lists one item: "No. Name Applications Description" with "1 All DNS Tunnels" and "BaiduYunDns; BostonNews; COM; Cymrus; DeviceScope; DnsTunGoodRaid; DnsTunMalic..." under Applications. A search bar and a refresh button are at the top right of this table. In the center, a modal window titled "Edit DNS Application Group" is open. It contains fields for "Name" (set to "All DNS Tunnels") and "DNS Tunnels & Network Apps" (a dropdown menu). There's also a "Description" field which is currently empty. At the bottom of the modal are buttons for "Click Box" (highlighted with a blue box), "Cancel", and "Delete". A large gray callout box with the text "Click Save" points to the "Click Box" button.

Slide notes

Click Save.

Slide 62 - Slide 62

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, ClickBox (with an activation count of 1), Search, and other management tools. The main area is titled 'Network Applications' and has tabs for APPLICATIONS, APPLICATION GROUPS, and DNS APPLICATION GROUP. Under 'DNS APPLICATION GROUP', there's a table with one row:

No.	Name	Applications	Description
1	All DNS Tunnels	BaiduYunDns, BostonNews, CCM, Cymru, DeviceScape, DnsTunGoodRev, DnsTunMalici...	...

A grey callout box with the text 'Click Activation' is positioned over the 'Activation' link in the table row for the 'All DNS Tunnels' group. At the bottom of the interface, there are copyright notices for Zscaler Inc. (2007-2020) and a timestamp: Weblog Time: 1/2/2020 1:39:46 PM Last Updated: 1/2/2020 1:42:22 PM.

Slide notes

Verify that the new **DNS Application Group** has been added to the list. This DNS Application Group will be used in a later step to create a rule that will block DNS tunnel traffic. **Activate** the changes.

Slide 63 - Slide 63

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a dark sidebar contains icons for Dashboard, Analytics, Policy, Administration (selected), Activation (with a red notification dot), and Search. A 'Click Box' is overlaid on the 'Activation' button. The main content area shows a table titled 'DNS APPLICATION GROUP' with columns for Applications and Description. The Applications column lists several entries, including 'BaiduYunDns', 'BostonNews', 'CCM', 'Cymru', 'DeviceScape', 'DnsTunGoodRvrd', 'DnsTunMalici...', and an ellipsis (...). A search bar and a help icon are also visible.

Slide notes

Slide 68 - Slide 68

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration (which is selected), Activation, Search, and Help. The main content area is titled "Network Applications". It has three tabs: APPLICATIONS (selected), APPLICATION GROUPS, and DNS APPLICATION GROUP. A sub-section titled "DNS APPLICATION GROUP" is shown, with a button to "Add DNS Application Group". A table lists one entry: "No. 1 Name All DNS Tunnels Applications BaiduYunDns, BostonNews, CCM, Cymru, DeviceScape, DnsTunGoodRvrd, DnsTunMalici... Description ...". There is a search bar at the top right and a help icon at the bottom right.

Slide notes

Slide 69 - Interactive Demo: Creating NGFW Policy

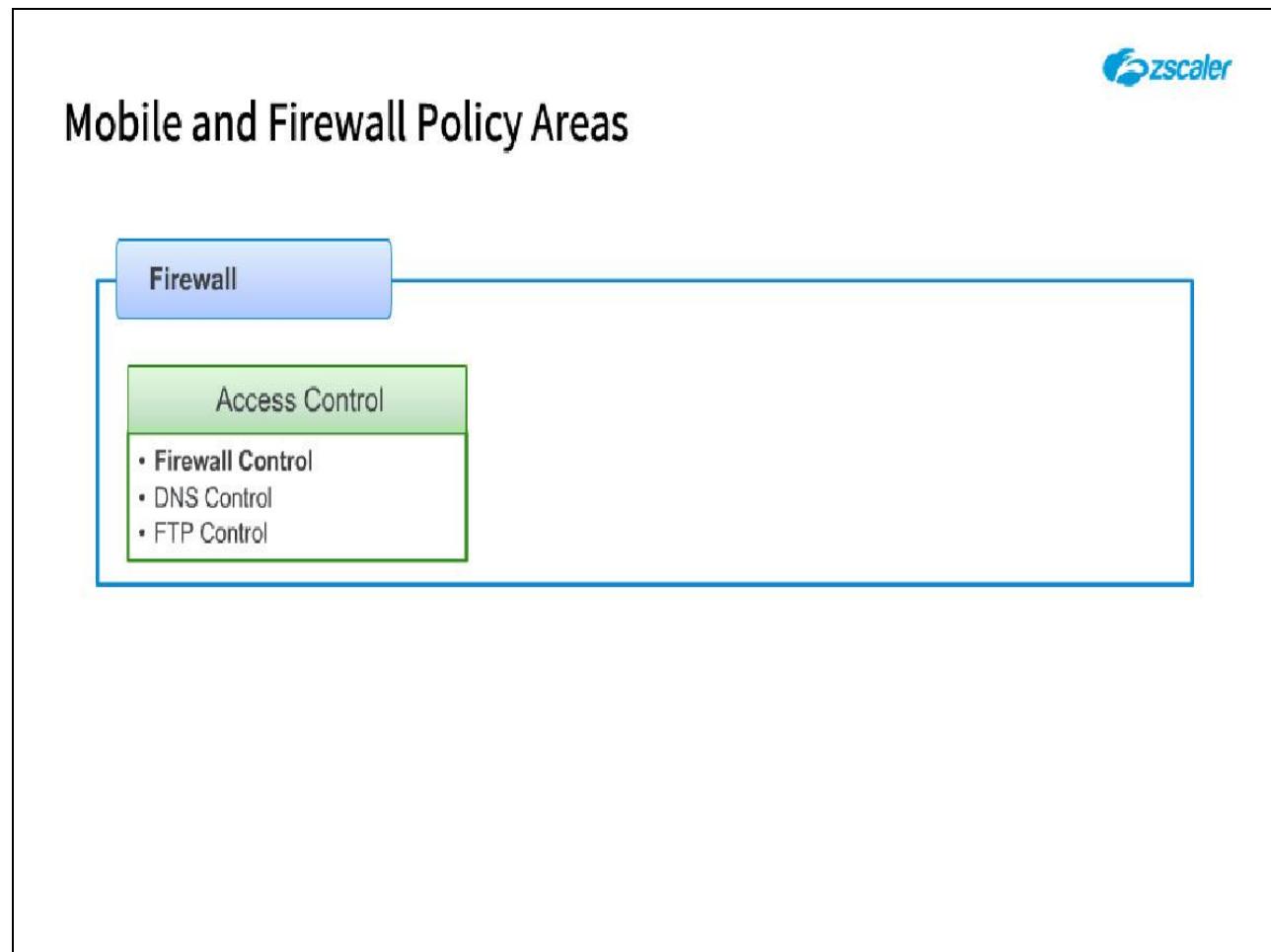


Slide notes

In the next section we will have a detailed look at the Firewall Policy area, and in particular examine the Cloud Firewall capabilities of the Zscaler system.

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 70 - Mobile and Firewall Policy Areas



Slide notes

In this first section, we'll look at the **Firewall Control** policies.

Slide 71 - Slide 71

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a vertical navigation bar lists several options: Dashboard, Analytics, Click Box Policy (which is highlighted in blue), Administration (selected), Activation, Search, and other icons. A callout box with the text "Click Policy" points to the "Administration" icon. The main content area is titled "Network Applications" and shows a table for "DNS APPLICATION GROUP". The table has columns for No., Name, Applications, and Description. One entry is listed: "1 All DNS Tunnels" with applications including "BaiduYunDns, BostonNews, CCM, Cymru, DeviceScape, DnsTunGoodRvrd, DnsTunMalici...". There are also "Add DNS Application Group" and search/filter buttons.

Slide notes

select Firewall Control.

Now, let's turn to our **Firewall** Policy ruleset. From the **Policy** menu

Slide 72 - Slide 72

The screenshot shows the Zscaler Policy-Cloud Firewall interface. The left sidebar contains several sections: SECURITY (Malware Protection, Advanced Threat Protection, Sandbox, Browser Control), ACCESS CONTROL (URL & Cloud App Control, File Type Control, Bandwidth Control, SSL Inspection), DATA LOSS PREVENTION (Data Loss Prevention), POLICY (Mobile, ZSCALER APP CONFIGURATION, Zscaler App Portal, Mobile Malware Protection, Mobile App Store Control), and ADMINISTRATION (Activation, Search). A callout box with the text "Click Firewall Control" points to the "Firewall Control" link under the ACCESS CONTROL section. The main pane displays a table with columns for ID, Name, Description, and Actions. The URL in the address bar is <https://admin.zscaler.net/policy/web/malware-protection>.

Slide notes

Click Firewall Control.

Slide 74 - Slide 74

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section 'Configure Firewall Control Policy'. It says 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this are two tabs: 'FIREWALL FILTERING POLICY' (selected) and 'NAT CONTROL POLICY'. Under the 'FIREWALL FILTERING POLICY' tab, there's a table with columns: Rule Order, Admin Rank, Rule Name, Criteria, Action, and Description. The first row shows a rule named 'Office 365 One Click Rule' with 'DESTINATION IP CATEGORIES' set to 'Office 365', 'Action' as 'Disabled', and 'Description' as 'Default'. The second row is a 'Default Firewall Filtering Rule' with 'Criteria' as 'Any' and 'Action' as 'Allow'. A large callout box with a grey background and black text points to the 'Add Firewall Filtering Rule' button, which is located above the table and has a blue outline. The bottom of the screen shows a copyright notice: 'Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies' and a 'Help' icon.

Slide notes

Here, you can create up to 1024 Firewall policy rules, and you can see a couple of default rules have been added for you. The first rule listed here is a system generated rule for Microsoft Office 365 traffic. This rule is added automatically at position 1 when you enable the Microsoft Office **One Click** feature. You can see here that the rule is currently in the disabled state, as **One Click** has subsequently been disabled.

You can also see the default **Allow All** rule here. Let's follow the Zscaler best practice of changing the default rule to **Block**.

However, before we do that, remember that traffic flowing through the Web proxy still needs to be allowed by the Firewall. If we switched the default rule to block, then all traffic would stop flowing in any locations where the Firewall is enabled.

So, we first need to add a couple rules to allow traffic coming from the Web proxy. We do that by creating a rule to allow the HTTP and HTTPS protocols, and another to allow DNS. Click the **Add Firewall Filtering Rule** link.

Slide 78 - Slide 78

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Firewall Control, Analytics, Policy, Administration, Activation, and Search. The main area shows a list of rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0) and 'Default Firewall Filtering Rule' (Rule Order 2, Admin Rank 7). A modal window titled 'Add Firewall Filtering Rule' is open. Inside, the 'Rule Criteria options' section is highlighted with a red box. It contains tabs for 'WHO, WHERE, & WHEN...', 'SERVICES & APPLICATIONS...', 'SOURCE IP', and 'DESTINATION IP'. Below these tabs is a 'CRITERIA' section with dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). There's also a 'Time' dropdown set to 'Always'. Under 'ACTION', there's a 'Network Traffic' dropdown set to 'Allow' and a 'Logging' section with 'Aggregate' and 'Full' options. At the bottom of the modal is a 'DESCRIPTION' text area and a 'Save' button.

Slide notes

For the **Rule Name** we will use **Permit traffic from Web Proxy**. In the **Criteria** section you'll see a difference from the Web proxy rules in that there are multiple tabs.

The first tab, labelled **WHO, WHERE, & WHEN**, defines to whom the rule will apply. As with **Cloud Application and URL Filtering** rules, the **User**, **Group**, and **Department** fields all use a logical **OR** function; while the **Where** and **Time** fields use a logical **AND**. This rule will apply to the entire organization, so we don't need to change any criteria here.

Slide 80 - Slide 80

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a table of existing rules. One rule is selected: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0). A modal window titled 'Add Firewall Filtering Rule' is open over the main interface. This modal has several sections: 'FIREWALL FILTERING RULE' (Rule Order 2, Admin Rank 7), 'CRITERIA' (Network Service Groups: None, Network Services: Any; Network Application Groups: None, Network Applications: Any), 'ACTION' (Network Traffic: Allow), 'Logging' (Aggregate selected), and 'DESCRIPTION' (an empty text area). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

The **SERVICES & APPLICATIONS** tab allows the selection of network services, or network applications (from those lists that we looked at earlier).

Slide 81 - Slide 81

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a table of existing rules. One rule is selected: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0). A modal window titled 'Add Firewall Filtering Rule' is open over the main interface. This modal has several tabs: 'WHO, WHERE, & WH...', 'SERVICES & APPLIC...', 'SOURCE IP', and 'DESTINATION IP'. Under 'CRITERIA', there's a dropdown for 'Source IP Groups' set to 'None'. Below that is a section for 'IP Addresses' with a 'Add Items' button. Under 'ACTION', there's a dropdown for 'Network Traffic' set to 'Allow'. Under 'Logging', there are two options: 'Aggregate' (selected) and 'Full'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

The **SOURCE IPs** tab allows the specification of specific IP addresses, or the selection of a **Source IP Group**.

Slide 82 - Slide 82

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains tabs for 'FIREWALL FILTERING POLICY' (selected) and 'NAT CONTROL POLICY'. A sub-section titled 'Configure Firewall Control Policy' with the note 'Rules are evaluated in the order specified. Thus evaluation stops at the first match.' is visible. Below this, a table lists rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0) and 'Default Firewall Filtering Rule' (Rule Order Default, Admin Rank 7). A large modal window titled 'Add Firewall Filtering Rule' is open. It has several tabs: 'WHO, WHERE, & WH...' (selected), 'SERVICES & APPLIC...', 'SOURCE IP', and 'DESTINATION IP'. Under 'WHO, WHERE, & WH...', fields include 'Rule Order' (2), 'Admin Rank' (7), 'Rule Name' (Permit traffic from Web Proxy), and 'Rule Status' (Enabled). The 'CRITERIA' section includes 'Destination Groups' (None), 'IP Address or FQDN' (Add Items), 'Countries' (Any), and 'Categories' (Any). The 'ACTION' section includes 'Network Traffic' (Allow) and 'Logging' (Aggregate selected). The 'DESCRIPTION' section is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

...and the **DESTINATION IPs** tab allows the specification of specific IP addresses or FQDNs, the selection of **Destination IP Groups**, **IP-Based Countries**, and/or **IP Categories**.

Slide 83 - Slide 83

The screenshot shows the Zscaler Policy-Cloud Firewall Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0) and 'Default Firewall Filtering Rule' (Rule Order Default, Admin Rank 7). A modal window titled 'Add Firewall Filtering Rule' is open. Inside, under the 'WHO: WHERE, & WHAT' tab, there's a section for 'Services & Applications'. A callout bubble with the text 'Click SERVICES & APPLICATIONS' points to this section. Other tabs in the modal include 'Click Box', 'Source IP', and 'Destination IP'. The modal also contains sections for 'CRITERIA', 'ACTION', and 'DESCRIPTION', along with 'Save' and 'Cancel' buttons.

Slide notes

Click the **SERVICES & APPLICATIONS** tab.

Slide 84 - Slide 84

Firewall Control

Add Firewall Filtering Rule

FIREWALL FILTERING RULE

Rule Order: 2 Admin Rank: 7

Rule Name: Permit traffic from Web Proxy Rule Status: Enabled

WHO, WHERE, & WHAT SERVICES & APPLICATIONS SOURCE IP DESTINATION IP

CRITERIA

Network Service Groups: None Network Services: Any

Network Application Groups: None Network Applications: Any

ACTION

Network Traffic: Allow

Logging: Aggregate, Full

DESCRIPTION

Save Cancel

Slide notes

Since we are creating a rule based on selected protocols, we will use the **Network Services** criteria. Click the **Network Services** drop-down

Slide 85 - Slide 85

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0) and 'Default Firewall Filtering Rule' (Rule Order Default, Admin Rank 7). A modal window titled 'Add Firewall Filtering Rule' is open. In the 'FIREWALL FILTERING RULE' section, 'Rule Order' is set to 2 and 'Admin Rank' is set to 7. The 'Rule Name' is 'Permit traffic from Web Proxy' and 'Rule Status' is 'Enabled'. Below this, there are tabs for 'WHO, WHERE, & WHO...' (selected), 'SERVICES & APPLICATIONS...', 'SOURCE IP', and 'DESTINATION IP'. The 'CRITERIA' section includes dropdowns for 'Network Service Groups' (set to 'None') and 'Network Application Groups' (set to 'None'). To the right, there's a list of network services with checkboxes: AIM, DNS, Echo, FTP, FTPS_Implicit, and Grutella. Under 'Selected Items (0)', there are 'Done', 'Cancel', and 'Clear Selection' buttons. At the bottom of the modal are 'Save' and 'Cancel' buttons. The status bar at the bottom of the screen shows 'Copyright © 2020 Zscaler Inc. All rights reserved. | Version 5.7 | Products' and 'Working Time: 1/12/2020 9:11:05 AM | Last Updated: 1/12/2020 9:12:15 AM'.

Slide notes

select HTTP and HTTPS, then click Done.

Slide 87 - Slide 87

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a sidebar lists various policy categories: Firewall Control, Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays a list of existing rules, including 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0) and 'Default Firewall Filtering Rule' (Rule Order Default, Admin Rank 7). A modal window titled 'Add Firewall Filtering Rule' is open, prompting for a rule name ('Permit traffic from Web Proxy') and status ('Enabled'). The 'ACTION' section allows setting traffic to 'Allow' or 'Deny' and enables 'Logging' with 'Aggregate' selected. A callout box highlights the 'HTTP' checkbox in a dropdown menu for selecting network services. The 'DESCRIPTION' field is empty, and at the bottom, there are 'Save' and 'Cancel' buttons.

Slide notes

Slide 88 - Slide 88

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of rules. One rule is selected: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0). A modal window titled 'Add Firewall Filtering Rule' is open. In the 'CRITERIA' section, under 'Network Service Groups', 'None' is selected. Under 'Network Services', 'Any' is selected. A callout box with the text 'Click HTTPS' points to the 'HTTPS' checkbox in a list of selected items. Other items in the list include 'HTTP' (checked) and 'HTTP Proxy'. At the bottom of the modal, there are 'Done', 'Cancel', and 'Clear Selection' buttons. The 'Save' button is at the very bottom of the main interface.

Slide notes

Slide 89 - Slide 89

Firewall Control

Add Firewall Filtering Rule

FIREWALL FILTERING RULE

Rule Order: 2 Admin Rank: 7

Rule Name: Permit traffic from Web Proxy Rule Status: Enabled

WHO, WHERE, & WHO... SERVICES & APPLICATIONS SOURCE IP DESTINATION IP

CRITERIA

Network Service Groups: None Network Services: Any

Unselected Items Selected Items (2)

http x Q HTTP HTTPS

HTTP Proxy HTTPS

ACTION

Network Traffic: Allow

Logging: Aggregate

DESCRIPTION

Click Box Click Done Cancel Clear Selection

Save Cancel

Copyright © 2020 Zscaler Inc. All rights reserved. | Version 5.7 | Products | Help | Working Time: 1/14/2020 9:11:05 AM | Last Updated: 1/14/2020 9:11:05 AM

Slide notes

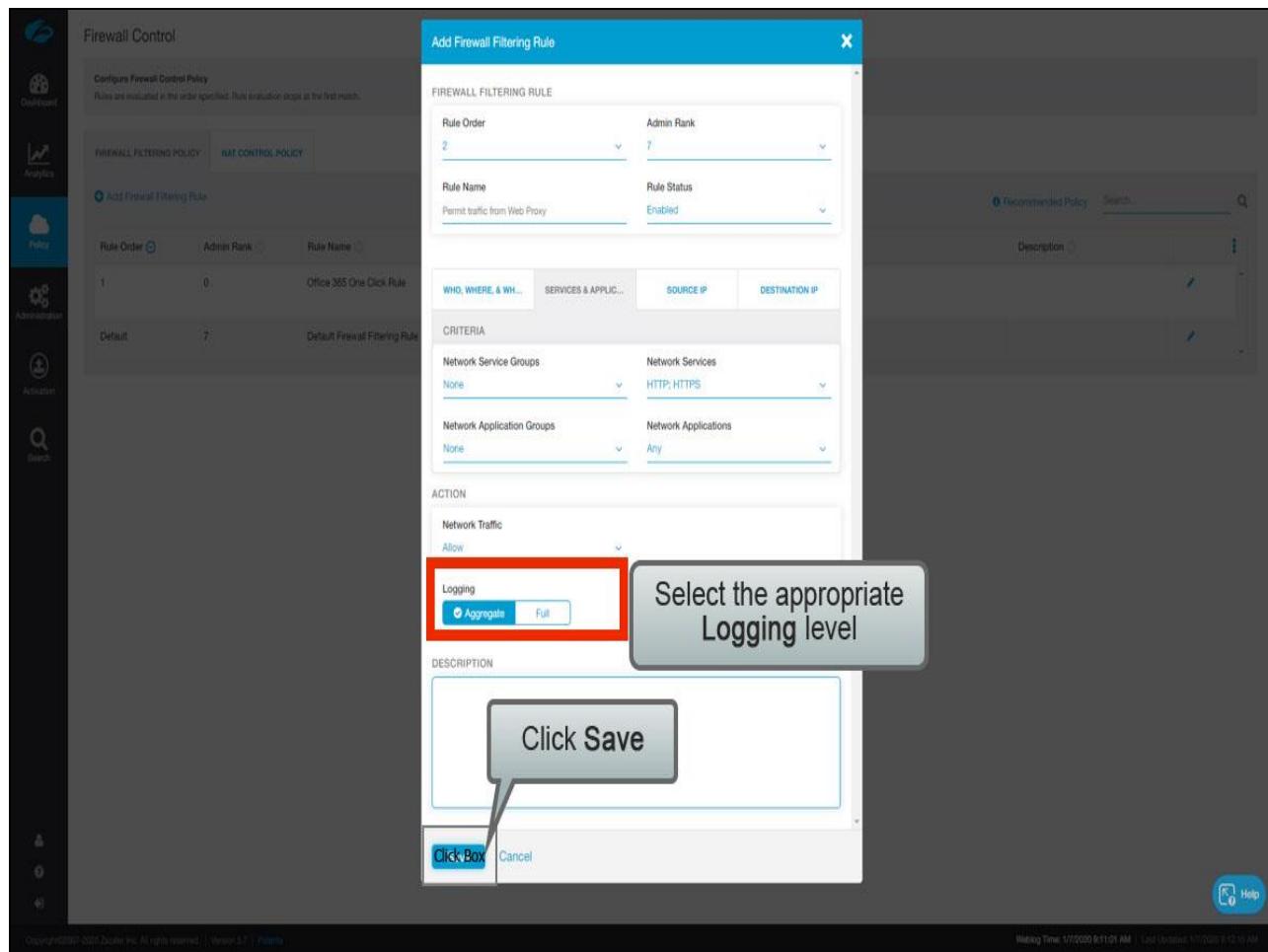
Slide 91 - Slide 91

Select the appropriate Action

Slide notes

The default **Action** is to **Allow**, so we'll leave that.

Slide 92 - Slide 92



Slide notes

For logging you have two options that relate to how traffic is logged; **Hourly Stats**, or **Full**. **Hourly Stats** provide aggregated logs every hour for traffic that triggers the rule; **Full** logging logs every session that triggers the rule. The best practice is to use **Hourly Stats** for **Allow** rules, and **Full** logging for **Block** rules.

Our rule is intended to be organization-wide so we won't need to set any source or destination IP restrictions. Click **Save**.

Slide 97 - Slide 97

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section 'Configure Firewall Control Policy'. It states: 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this, there are two tabs: 'FIREWALL FILTERING POLICY' (which is selected) and 'NAT CONTROL POLICY'. In the 'FIREWALL FILTERING POLICY' section, there's a button labeled 'Add Firewall Filtering Rule' with a blue icon. A callout box with a black border and white text 'Click Add Firewall Filtering Rule' points to this button. To the right of the button is a search bar with placeholder text 'Search...' and a magnifying glass icon. The main table lists firewall rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description	Actions
1			DESTINATION IP CATEGORIES Office 365	Disabled		
2			NETWORK SERVICES HTTP; HTTPS	Allow		
Default			Any	Allow		

At the bottom of the interface, there's a copyright notice: 'Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Patients' and a 'Help' button.

Slide notes

We now need to add a rule to allow DNS. Click the **Add Firewall Filtering Rule** link.

Slide 98 - Slide 98

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

- Office 365 One Click Rule (Rule Order 1, Admin Rank 0)
- Permit from Web Proxy (Rule Order 2, Admin Rank 7)
- Default Firewall Filtering Rule (Rule Order Default, Admin Rank 7)

A modal window titled 'Add Firewall Filtering Rule' is open. It has several sections:

- FIREWALL FILTERING RULE**:
 - Rule Order: 3
 - Admin Rank: 7
 - Rule Name: Firewall_1
 - Rule Status: Enabled
- WHO, WHERE, & WHEN**:
 - Services & Applications tab is selected.
 - Source IP and Destination IP fields are empty.
- CRITERIA**:
 - Users: Any
 - Groups: Any
 - Departments: Any
 - Locations: Any
 - Time: Always
- ACTION**:
 - Network Traffic: Allow
 - Logging: Aggregate (selected)
- DESCRIPTION**: A large text input field.

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

Slide notes

For 'Rule Name' we will use Permit DNS. Click the **Services & Applications** tab.

Slide 99 - Slide 99

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section 'Configure Firewall Control Policy'. It lists two rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0) and 'Permit from Web Proxy' (Rule Order 2, Admin Rank 7). A third rule, 'Default Firewall Filtering Rule', is listed with Rule Order 7, Admin Rank 7. The central part of the screen is a modal window titled 'Add Firewall Filtering Rule'.

Firewall Filtering Rule

Rule Order: 3 **Admin Rank:** 7

Rule Name: Permit DNS **Rule Status:** Enabled

WHO, WHERE, & WH... **SERVICES & APPLIC...** **SOURCE IP** **DESTINATION IP**

CRITERIA

Users: Any **Groups:** Any

Departments: Any **Locations:** Any

Time: Always

ACTION

Network Traffic: Allow

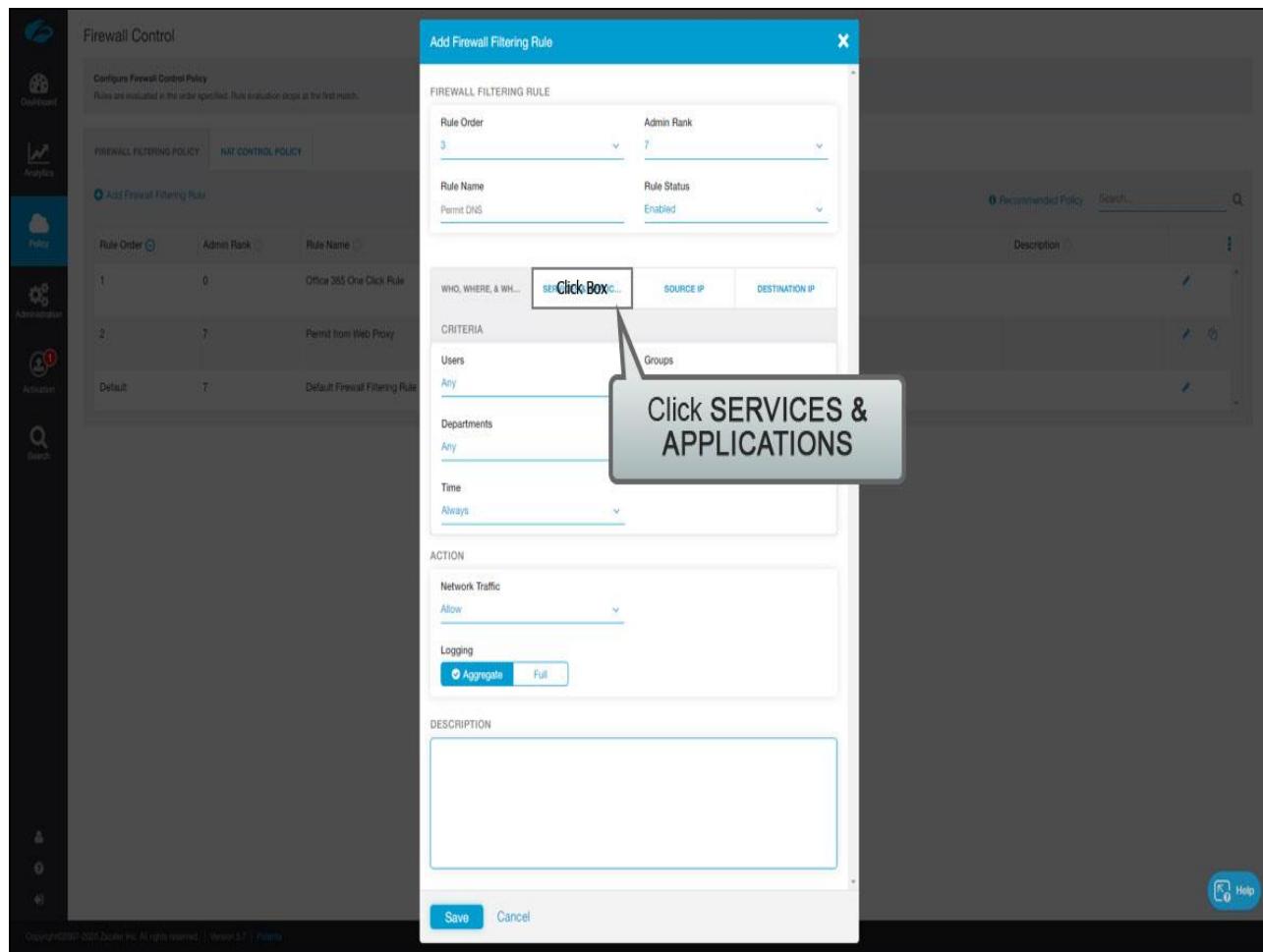
Logging: Aggregate (selected) Full

DESCRIPTION

Buttons: Save Cancel

Slide notes

Slide 100 - Slide 100



Slide notes

Click the Services & Applications tab.

Slide 101 - Slide 101

Firewall Control

Add Firewall Filtering Rule

FIREWALL FILTERING RULE

Rule Order: 3 Admin Rank: 7

Rule Name: Permit DNS Rule Status: Enabled

WHO, WHERE, & WHAT

SERVICES & APPLICATIONS

SOURCE IP DESTINATION IP

CRITERIA

Network Service Groups: None Network Services: Click Box

Network Application Groups: None Network Applications: Any

ACTION

Network Traffic: Allow

Logging: Aggregate

DESCRIPTION

Save Cancel

Click Network Services drop-down

Slide notes

From the **Network Services** drop-down, select **DNS**, then click **Done**.

Slide 102 - Slide 102

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules:

- Office 365 One Click Rule (Rule Order 1, Admin Rank 0)
- Permit from Web Proxy (Rule Order 2, Admin Rank 7)
- Default Firewall Filtering Rule (Rule Order Default, Admin Rank 7)

A modal window titled 'Add Firewall Filtering Rule' is open. It has tabs for 'FIREWALL FILTERING POLICY' and 'NAT CONTROL POLICY'. The 'FIREWALL FILTERING POLICY' tab is selected. Inside, there are fields for 'Rule Order' (set to 3), 'Admin Rank' (set to 7), 'Rule Name' (set to 'Permit DNS'), and 'Rule Status' (set to 'Enabled').

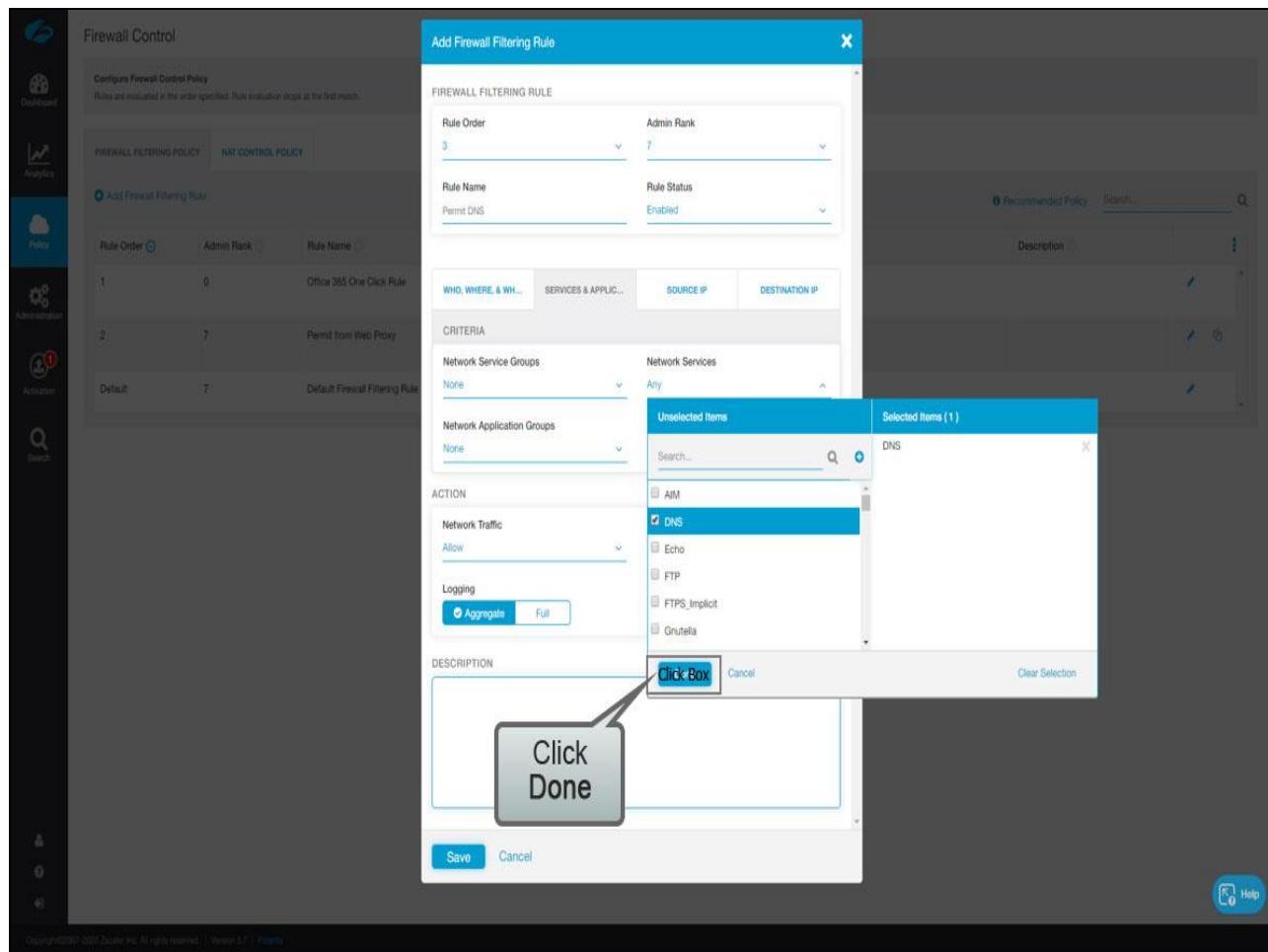
The 'CRITERIA' section includes dropdowns for 'Network Service Groups' (set to 'None') and 'Network Services' (set to 'Any'). Below these are sections for 'ACTION' (set to 'Network Traffic' and 'Allow') and 'Logging' (set to 'Aggreg').

The 'DESCRIPTION' field is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

A callout box with the text 'Click DNS' points to the 'DNS' option in a dropdown menu for selecting network services. The dropdown also lists AIM, Click Box, Echo, FTP, FTPS_Implicit, and Grutella. There are 'Unselected Items' and 'Selected Items (0)' sections at the bottom of the dropdown.

Slide notes

Slide 104 - Slide 104



Slide notes

Slide 105 - Slide 105

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0), 'Permit from Web Proxy' (Rule Order 2, Admin Rank 7), and 'Default Firewall Filtering Rule' (Rule Order Default, Admin Rank 7). A modal window titled 'Add Firewall Filtering Rule' is open. It has sections for 'FIREWALL FILTERING RULE' (Rule Order 3, Admin Rank 7, Rule Name 'Permit DNS', Rule Status 'Enabled'), 'CRITERIA' (Network Service Groups 'None', Network Services 'DNS', Network Application Groups 'None', Network Applications 'Click Box'), 'ACTION' (Network Traffic 'Allow'), 'Logging' (Aggregate selected), and 'DESCRIPTION' (empty). At the bottom are 'Save' and 'Cancel' buttons. A callout bubble with the text 'Click Network Applications drop-down' points to the 'Click Box' option in the Network Applications dropdown.

Slide notes

Now if we were to save this rule, we would be opening TCP and UDP port 53 since we only selected the **Network Services** protocol. This could allow other applications to ride over these ports, which we don't want to happen, so we're going to also select DNS from the **Network Applications** drop down as well.

If we combine **Network Services** and **Network Applications** criteria, this will have the effect of only allowing the DNS application to use TCP and UDP port 53. We'll talk more about how these two criteria coexist later in the module. Click the **Network Applications** drop-down

Slide 106 - Slide 106

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains tabs for 'FIREWALL FILTERING POLICY' and 'NAT CONTROL POLICY'. A message says 'Configure Firewall Control Policy' and 'Rules are evaluated in the order specified. Evaluation stops at the first match.' Below this, there's a table of existing rules:

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
Default	7	Default Firewall Filtering Rule

A modal window titled 'Add Firewall Filtering Rule' is open. It has sections for 'FIREWALL FILTERING RULE' (Rule Order: 3, Admin Rank: 7, Rule Name: Permit DNS, Rule Status: Enabled), 'CRITERIA' (Network Service Groups: None, Network Services: DNS; Network Application Groups: None, Network Applications: Any), 'ACTION' (Network Traffic: Allow), and 'DESCRIPTION' (a large text area). At the bottom are 'Save' and 'Cancel' buttons. A dropdown menu is open under 'Selected Items (0)' containing a list of application services: APNS, DICT, EPM, GARP, and iCloud. The 'Done' button is highlighted.

Slide notes

select **DNS**, then **Done**, then save this rule.

Slide 107 - Slide 107

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains tabs for 'FIREWALL FILTERING POLICY' and 'NAT CONTROL POLICY'. A sub-section titled 'Configure Firewall Control Policy' is visible. In the center, a modal window titled 'Add Firewall Filtering Rule' is open. The modal has several sections: 'FIREWALL FILTERING RULE' (Rule Order: 3, Admin Rank: 7), 'WHO, WHERE, & WHEN' (Rule Name: Permit DNS, Rule Status: Enabled), 'SERVICES & APPLICATIONS' (Network Service Groups: None, Network Services: DNS), 'SOURCE IP' (Network Application Groups: None, Network Applications: Any), and 'DESTINATION IP'. Below these is an 'ACTION' section (Network Traffic: Allow) and a 'Logging' section (Aggregate selected). A 'DESCRIPTION' field is also present. At the bottom of the modal are 'Save' and 'Cancel' buttons. A 'Help' button is located in the bottom right corner of the modal. The background shows a list of existing firewall rules.

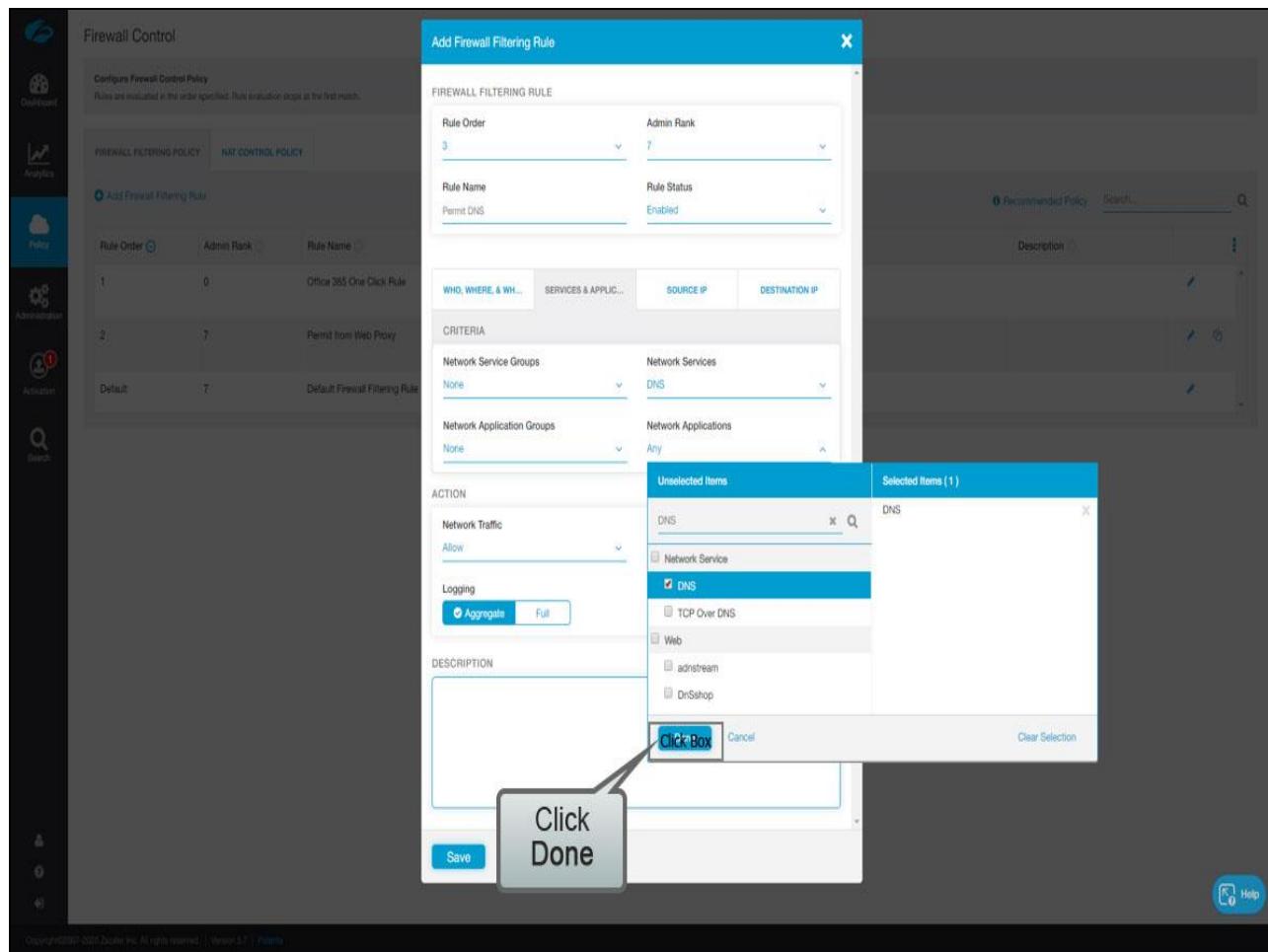
Slide notes

Slide 108 - Slide 108

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0), 'Permit from Web Proxy' (Rule Order 2, Admin Rank 7), and 'Default Firewall Filtering Rule' (Default, Admin Rank 7). A modal window titled 'Add Firewall Filtering Rule' is open. In the 'CRITERIA' section, under 'Network Service Groups', 'None' is selected. Under 'Network Applications', 'Any' is selected. In the 'ACTION' section, 'Network Traffic' is set to 'Allow'. The 'Logging' section has 'Aggregate' selected. A callout box with the text 'Click DNS' points to the 'DNS' option in a dropdown menu for selecting network services. The 'Selected Items (0)' section is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Slide 109 - Slide 109



Slide notes

Slide 110 - Slide 110

Firewall Control

Configure Firewall Control Policy
Rules are evaluated in the order specified. Evaluation stops at the first match.

FIREWALL FILTERING POLICY NAT CONTROL POLICY

Add Firewall Filtering Rule

Rule Order Admin Rank Rule Name

WHO, WHERE, & WHAT SERVICES & APPLICATIONS SOURCE IP DESTINATION IP

CRITERIA

Network Service Groups Network Services

Network Application Groups Network Applications

ACTION

Network Traffic Allow

Logging

Aggregate Full

DESCRIPTION

Click Box Cancel

Click Save

Slide notes

Slide 115 - Slide 115

The screenshot shows the Zscaler Firewall Control interface under the 'Firewall Control' section. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure Firewall Control Policy' with the note 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this, there are two tabs: 'FIREWALL FILTERING POLICY' (selected) and 'NAT CONTROL POLICY'. A sub-header 'Add Firewall Filtering Rule' is present. The main content is a table listing rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
3	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
Default	7	Default Firewall Filtering Rule	Any	Allow	

A large callout box with a dark gray background and white text points to the 'Default' row in the table. The text inside the box reads 'Click to edit the rule Default'. A smaller box labeled 'Click Box' is located at the bottom right of the callout.

Slide notes

Now, we can change the default rule to **Block**, click the **Edit** button for that rule.

Slide 116 - Slide 116

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of firewall rules. One rule is selected, and a modal window titled 'Edit Firewall Filtering Rule' is open. The modal has tabs for 'ACTION' and 'Logging'. Under 'ACTION', there's a dropdown menu currently set to 'Allow'. A callout bubble with the text 'Click Network Traffic drop-down' points to this dropdown. The background shows other rules in the list, such as 'Office 365 One Click Rule' and 'Permit from Web Proxy'.

Slide notes

Click the **Network Traffic** drop-down...

Slide 117 - Slide 117

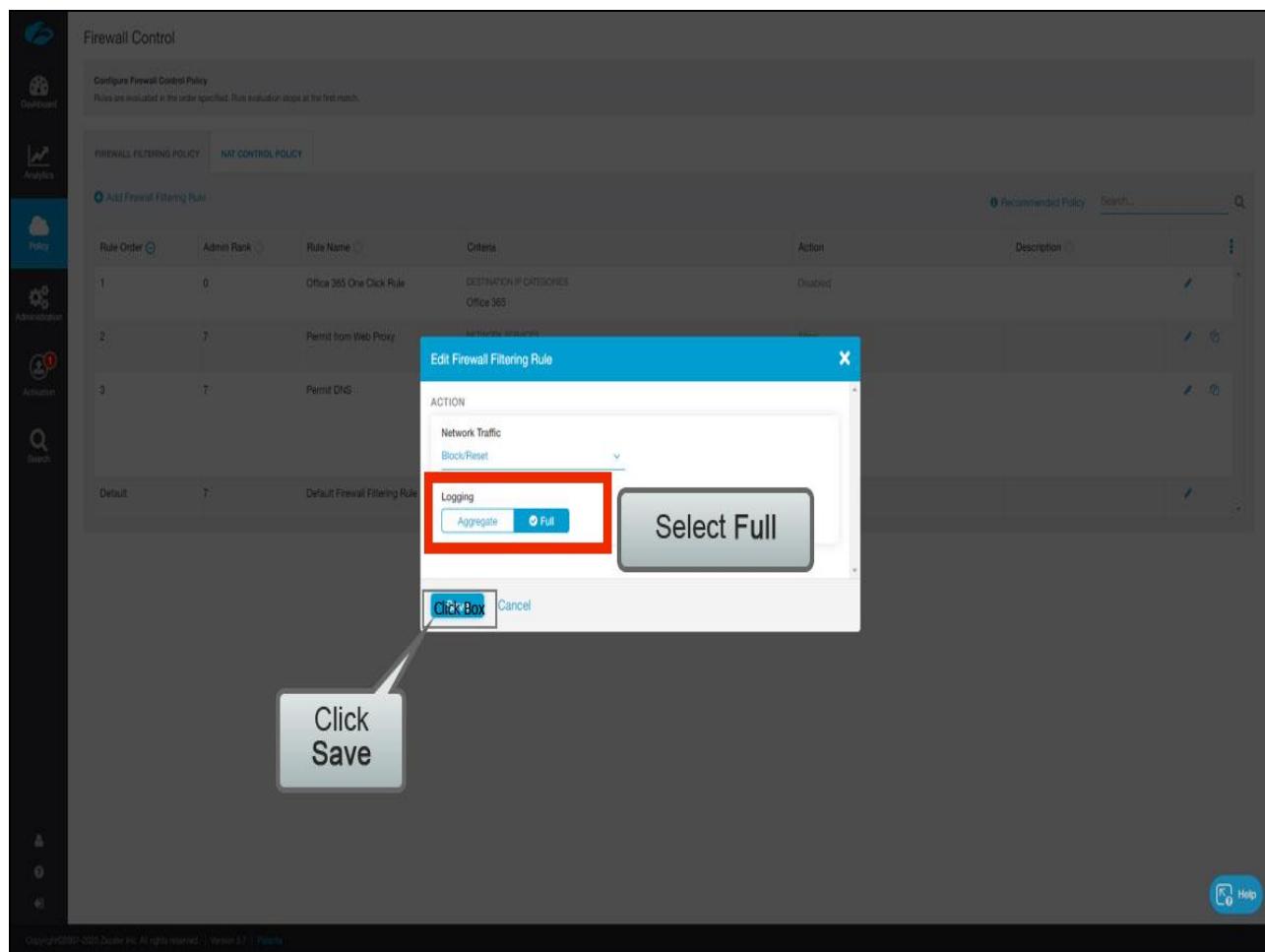
The screenshot shows the Zscaler Firewall Control interface. On the left, there's a vertical sidebar with icons for Firewall Control, Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and has tabs for 'FIREWALL FILTERING POLICY' and 'NAT CONTROL POLICY'. Under 'FIREWALL FILTERING POLICY', there's a table of rules. One rule is selected, and a modal window titled 'Edit Firewall Filtering Rule' is open. The 'ACTION' dropdown menu is expanded, showing options: Allow, Block/Drop, Block/ICMP, and Block/Reset. The 'Block/Reset' option is highlighted with a blue border and a callout box pointing to it. The callout box contains the text 'Click Block / Reset'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

...and you will see that you have 3 different options for **Block**; **Drop**, **ICMP**, and **Reset**.

Drop is self-explanatory, the traffic that matches this rule is simply dropped. This can however result in a poor user experience, as the blocked application may simply hang and the user may not know why it's not working. The **ICMP** option sends an ICMP Error message, and the **Reset** option sends a Layer 4 reset. For our rule click **Block/Reset**.

Slide 118 - Slide 118



Slide notes

Because this is now a **Block** rule, the best practice is to do full logging, so select **Full**, then click **Save**.

Slide 122 - Slide 122

The screenshot shows the Zscaler Firewall Control interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Click & Go Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section 'Configure Firewall Control Policy' with the note 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this are two tabs: 'FIREWALL FILTERING POLICY' (selected) and 'NAT CONTROL POLICY'. A table lists the following rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
3	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
Default Firewall Filtering Rule				Block/Reset	

A callout box with the text 'Click to Activate' is positioned over the bottom right corner of the table. At the bottom right of the interface is a 'Help' button.

Slide notes

Then **Activate** your changes.

Slide 123 - Slide 123

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a dark sidebar contains icons for Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. A blue box highlights the 'Click Box' button under the Policy section. A large callout box labeled 'Click Activate' points to this button. The main pane displays a table of firewall rules. The first rule is 'Office 365 One Click Rule' with criteria 'DESTINATION IP CATEGORIES Office 365' and action 'Disabled'. The second rule is 'HTTP; HTTPS' with criteria 'NETWORK SERVICES HTTP; HTTPS' and action 'Allow'. The third rule is 'DNS' with criteria 'NETWORK SERVICES DNS' and action 'Allow'. The fourth rule is 'Default Firewall Filtering Rule' with criteria 'Any' and action 'Block/Reset'. At the top right of the main pane, there is a 'Recommended Policy' button and a search bar.

Rank	Rule Name	Criteria	Action	Description
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2		NETWORK SERVICES HTTP; HTTPS	Allow	
3		NETWORK SERVICES DNS	Allow	
4	Default Firewall Filtering Rule	Any	Block/Reset	

Slide notes

Slide 126 - Slide 126

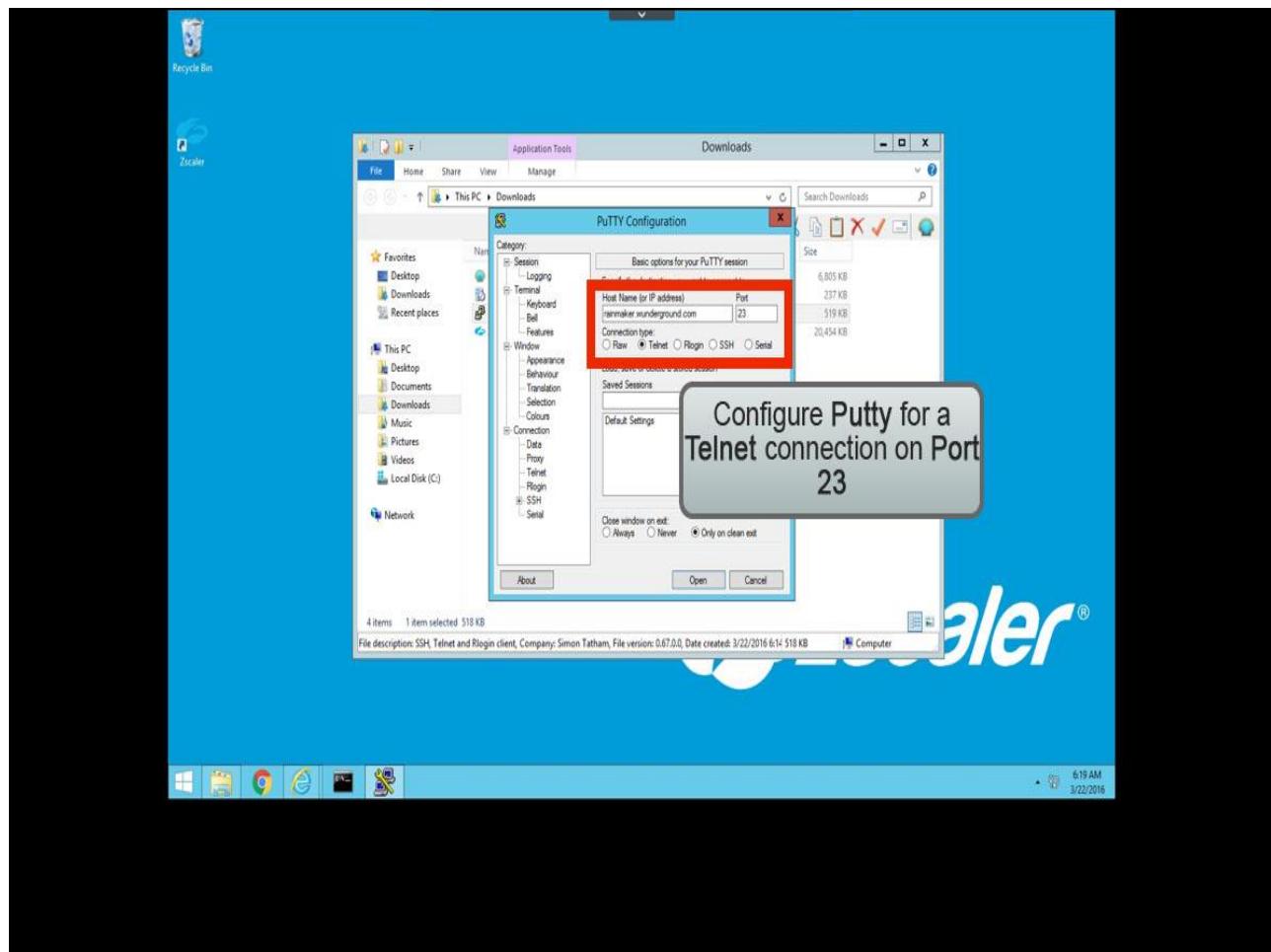
The screenshot shows the Zscaler Policy-Cloud Firewall Control interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Firewall Control" and "Configure Firewall Control Policy". It states: "Rules are evaluated in the order specified. Rule evaluation stops at the first match." Below this, there are two tabs: "FIREWALL FILTERING POLICY" (selected) and "NAT CONTROL POLICY". A button "Add Firewall Filtering Rule" is visible. The main content is a table listing rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description	Actions
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled		
2	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow		
3	7	Permit DNS	NETWORK APPLICATIONS DNS	Allow		
Default		7	Default Firewall Filtering Rule	Any	Block/Reset	

At the bottom right of the main area is a "Help" button. The footer contains the text "Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies".

Slide notes

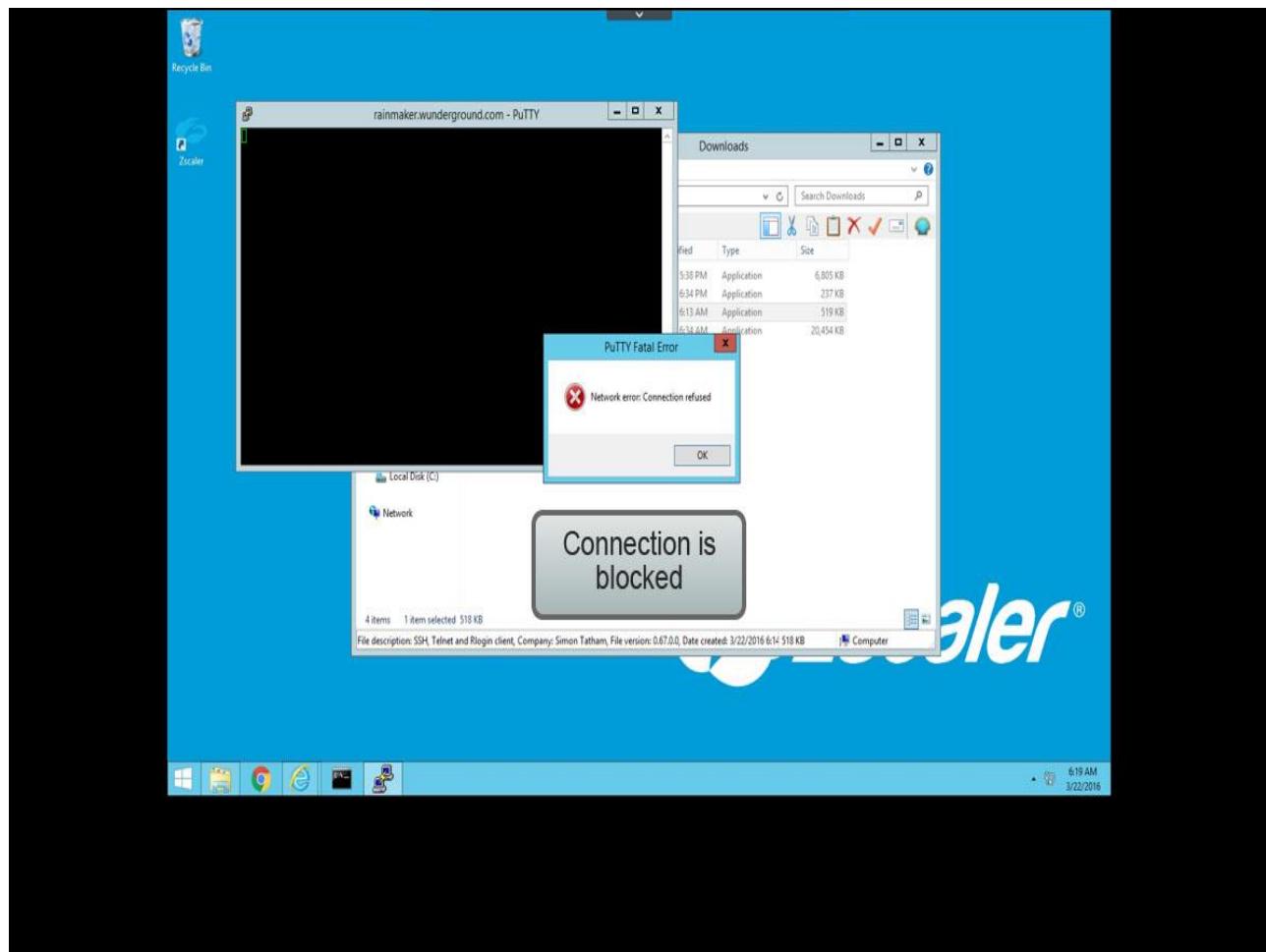
Slide 127 - Slide 127



Slide notes

Now let's test our policy by trying a Telnet connection from a client machine at the Location, using Putty.

Slide 128 - Slide 128



Slide notes

As you can see, Telnet is blocked. Let's create a rule to allow it.

Slide 129 - Slide 129

The screenshot shows the Zscaler Firewall Control interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section titled 'Configure Firewall Control Policy'. It states: 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this, there are two tabs: 'FIREWALL FILTERING POLICY' (which is selected) and 'NAT CONTROL POLICY'. A large table displays existing firewall rules. The first rule, numbered 1, has the following details:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	Office 365 Outbound	Office 365	DESTINATION IP CATEGORIES Office 365	Disabled	
2			NETWORK SERVICES HTTP; HTTPS	Allow	
3			NETWORK APPLICATIONS DNS	Allow	
Default	7	Default Firewall Filtering Rule	Any	Block/Reset	

A callout box with the text 'Click Add Firewall Filtering Rule' points to the 'Add Firewall Rule' button located in the top-left corner of the rule table.

Slide notes

On the Firewall Control page, click the **Add Firewall Filtering Rule** link.

Slide 130 - Slide 130

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

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
Default	7	Default Firewall Filtering Rule

A modal window titled 'Add Firewall Filtering Rule' is open. It contains fields for 'Rule Order' (set to 4) and 'Admin Rank' (set to 7). The 'Rule Name' is 'Firewall_1' and the 'Rule Status' is 'Enabled'. The 'CRITERIA' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Aggregate'. The 'DESCRIPTION' section has a large empty text area. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

We'll name this rule **Permit Telnet...**

Slide 131 - Slide 131

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

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
Default	7	Default Firewall Filtering Rule

A modal window titled 'Add Firewall Filtering Rule' is open. It contains fields for 'Rule Order' (set to 4) and 'Admin Rank' (set to 7). The 'Rule Name' is 'Permit Telnet' and the 'Rule Status' is 'Enabled'. The 'CRITERIA' section includes dropdowns for 'Users' (Any), 'Groups' (Any), 'Departments' (Any), and 'Locations' (Any). The 'Time' dropdown is set to 'Always'. The 'ACTION' section has a 'Network Traffic' dropdown set to 'Allow' and a 'Logging' section with 'Aggregate' selected. The 'DESCRIPTION' section is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Slide 132 - Slide 132

Firewall Control

Configure Firewall Control Policy
Rules are evaluated in the order specified. Evaluation stops at the first match.

FIREWALL FILTERING POLICY NAT CONTROL POLICY

Add Firewall Filtering Rule

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
Default	7	Default Firewall Filtering Rule

WHO, WHERE, & WHO... **Click Box** SOURCE IP DESTINATION IP

CRITERIA

Users: Any Groups

Departments: Any

Time: Always

ACTION

Network Traffic: Allow

Logging: Aggregate Full

DESCRIPTION

Save Cancel

Copyright © 2019 Zscaler Inc. All rights reserved. | Version 5.7 | Products

Help

Slide notes

as this rule will apply to everyone, leave the first criteria tab alone. Click the **Services and Applications** tab.

Slide 133 - Slide 133

Firewall Control

Add Firewall Filtering Rule

FIREWALL FILTERING RULE

Rule Order: 4 Admin Rank: 7

Rule Name: Permit Telnet Rule Status: Enabled

WHO, WHERE, & WHO

SERVICES & APPLICATIONS

SOURCE IP DESTINATION IP

CRITERIA

Network Service Groups: None Network Services: Any

Network Application Groups: None Network Applications: Click Box

ACTION

Network Traffic: Allow

Logging: Aggregate, Full

DESCRIPTION

Save Cancel

Click Network Applications

Slide notes

At this point we have a choice; we could match Telnet using the **Network Services** criteria. However, network services simply match the port and protocol assigned to it, so if we select Telnet here Zscaler will simply allow TCP port 23 connections. This means any application could ride over TCP port 23 which is not what we want.

Instead, we'll use the **Network Applications** criteria to match Telnet. The result of this is that the Telnet application will now be allowed regardless of Layer 4 port. Click to expand the **Network Applications** list.

Slide 135 - Slide 135

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

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS

A modal window titled 'Add Firewall Filtering Rule' is open. It has tabs for 'FIREWALL FILTERING POLICY' and 'NAT CONTROL POLICY'. The 'FIREWALL FILTERING POLICY' tab is selected. Inside, you can set 'Rule Order' (4), 'Admin Rank' (7), 'Rule Name' (Permit Telnet), and 'Rule Status' (Enabled). The 'CRITERIA' section includes dropdowns for 'Network Service Groups' (None) and 'Network Applications' (Any). The 'ACTION' section shows 'Network Traffic' set to 'Allow'. Under 'Logging', there are 'Aggregate' and 'Full' options, with 'Aggregate' selected. The 'DESCRIPTION' field is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

A search bar at the top right says 'Recommended Policy' and 'Search...'. A help icon is in the bottom right corner of the modal.

Slide notes

Slide 136 - Slide 136

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

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
Default	7	Default Firewall Filtering Rule

A modal window titled 'Add Firewall Filtering Rule' is open. It has tabs for 'FIREWALL FILTERING POLICY' and 'NAT CONTROL POLICY'. The 'FIREWALL FILTERING POLICY' tab is selected. Inside, there are fields for 'Rule Order' (set to 4), 'Admin Rank' (set to 7), 'Rule Name' (set to 'Permit Telnet'), and 'Rule Status' (set to 'Enabled').

The 'CRITERIA' section includes dropdowns for 'Network Service Groups' (None) and 'Network Applications' (Any). Below that is an 'ACTION' section with 'Network Traffic' set to 'Allow'.

At the bottom of the modal is a 'DESCRIPTION' field and a 'Save' button. A callout box points to the 'Click Box' button in the 'Selected Items' list of a modal overlay.

The overlay modal has tabs for 'Unselected Items' and 'Selected Items (0)'. In the 'Selected Items' tab, there is a search bar with 'telnet' typed in, a 'Clear Selection' button, and a 'Done' button. There is also a 'Remote access' checkbox and a 'Telet' button.

Slide notes

Select **Telnet** and click **Done**.

Slide 137 - Slide 137

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing firewall rules:

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS

A new rule is being added with the following details:

- Rule Order:** 4
- Admin Rank:** 7
- Rule Name:** Permit Telnet
- Criteria:**
 - Network Service Groups: None
 - Network Applications: Any
- Action:**
 - Network Traffic: Allow
 - Logging: Aggregate
- Description:** (Empty)

A modal dialog titled 'Click Box' is open, showing a list of items:

- Unselected Items: telnet
- Selected Items (1): Telnet

A callout box with the text 'Click Done' points to the 'Done' button at the bottom right of the modal.

Slide notes

Slide 138 - Slide 138

Click Network Services

Slide notes

If you also want to restrict the Layer 4 ports that are used, you need to combine a **Network Services** configuration with the **Network Applications** rule. Click **Network Services**

Slide 140 - Slide 140

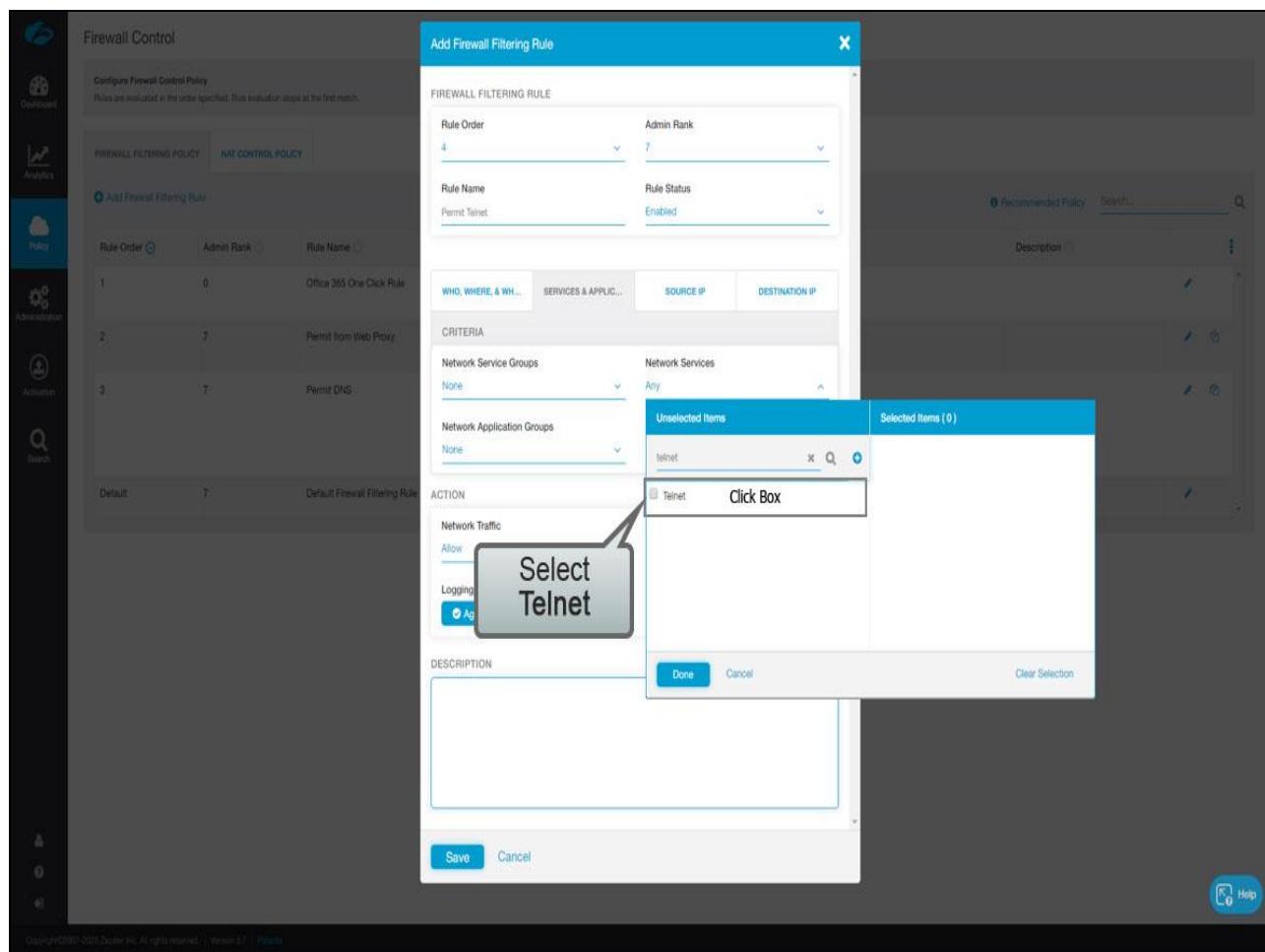
The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules:

- Rule Order 1, Admin Rank 0, Rule Name 'Office 365 One Click Rule'
- Rule Order 2, Admin Rank 7, Rule Name 'Permit from Web Proxy'
- Rule Order 3, Admin Rank 7, Rule Name 'Permit DNS'
- Default, Admin Rank 7, Rule Name 'Default Firewall Filtering Rule'

A modal window titled 'Add Firewall Filtering Rule' is open. It has fields for 'Rule Order' (set to 4) and 'Admin Rank' (set to 7). The 'Rule Name' is 'Permit Telnet' and the 'Rule Status' is 'Enabled'. The 'CRITERIA' section includes 'WHO, WHERE, & WHEN' (disabled), 'SERVICES & APPLICATIONS' (disabled), 'SOURCE IP' (disabled), and 'DESTINATION IP' (disabled). The 'Network Service Groups' dropdown is set to 'None'. The 'Network Services' dropdown is set to 'Any'. A 'Selected Items' list on the right contains 'telnet'. Other options in the list include AIM, DNS, Echo, FTP, FTPS_Implicit, and Grubella. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Slide 141 - Slide 141



Slide notes

...and select **Telnet**. The behavior here is different to Zscaler's standard rule criteria. **Network Services** and **Network Applications** are combined using a logical AND function, which means traffic must match BOTH criteria in order to trigger the rule. As a result, if we select Telnet in both **Network Services** and **Network Applications**, Telnet will only be allowed over TCP port 23.

Slide 142 - Slide 142

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of existing rules: 'Office 365 One Click Rule' (Rule Order 1, Admin Rank 0), 'Permit from Web Proxy' (Rule Order 2, Admin Rank 7), 'Permit DNS' (Rule Order 3, Admin Rank 7), and 'Default Firewall Filtering Rule' (Rule Order Default, Admin Rank 7). The current step is 'Add Firewall Filtering Rule' (Rule Order 4, Admin Rank 7). The 'FIREWALL FILTERING RULE' configuration includes:

- WHO, WHERE, & WHEN:** Rule Name: Permit Telnet.
- CRITERIA:** Network Service Groups: None; Network Services: Any.
- ACTION:** Network Traffic: Allow.
- Logging:** Aggregate.

A modal window titled 'Click Box' is overlaid on the screen, showing a list of unselected items ('Telnet') and one selected item ('Telnet'). The 'Selected Items (1)' list contains 'Telnet'. At the bottom of the 'Click Box' are 'Click Done' and 'Cancel' buttons, with 'Click Done' being highlighted by a callout bubble.

Slide notes

Click Done to select Telnet.

Slide 143 - Slide 143

The screenshot shows the Zscaler Policy-Cloud Firewall Control interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area shows a list of firewall rules:

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
Default	7	Default Firewall Filtering Rule

A modal window titled "Add Firewall Filtering Rule" is open in the center. It contains fields for Rule Order (set to 4), Admin Rank (set to 7), Rule Name (set to Permit Telnet), and Rule Status (set to Enabled). The "CRITERIA" section includes Network Service Groups (None) and Network Applications (Telnet). The "ACTION" section shows Network Traffic set to Allow. The "DESCRIPTION" field is empty. At the bottom of the modal, there are "Click Box" and "Cancel" buttons.

Slide notes

Click Save.

Slide 148 - Slide 148

The screenshot shows the Zscaler Firewall Control interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Click & Go Activation, and Search. The main area is titled 'Firewall Control' and contains a table of 'FIREWALL FILTERING POLICY' rules. The table has columns for Rule Order, Admin Rank, Rule Name, Criteria, Action, and Description. There are four rows of rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
3	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	

Below the table, there is a row for the 'Default' rule with an 'Any' criteria and an 'Allow' action. At the bottom right of the table area is a blue 'Block/Reset' button. A callout box with the text 'Click to Activate' is positioned over the first row of the table.

Slide notes

then **Activate** your changes.

Slide 149 - Slide 149

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a sidebar menu includes options like Dashboard, Analytics, Policy (selected), Activation, and Search. The main area displays a table of firewall rules. A large callout box labeled "Click Activate" points to the "Force Activate" button in the sidebar. The table has columns for Rank, Rule Name, Criteria, Action, and Description.

Rank	Rule Name	Criteria	Action	Description
	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
		NETWORK SERVICES HTTP; HTTPS	Allow	
		NETWORK APPLICATIONS DNS	Allow	
		NETWORK SERVICES DNS		
	Permit Telnet	NETWORK APPLICATIONS Telnet	Allow	
		NETWORK SERVICES Telnet		
	Default Firewall Filtering Rule	Any	Block/Reset	

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | [Patents](#)

Slide notes

Slide 152 - Slide 152

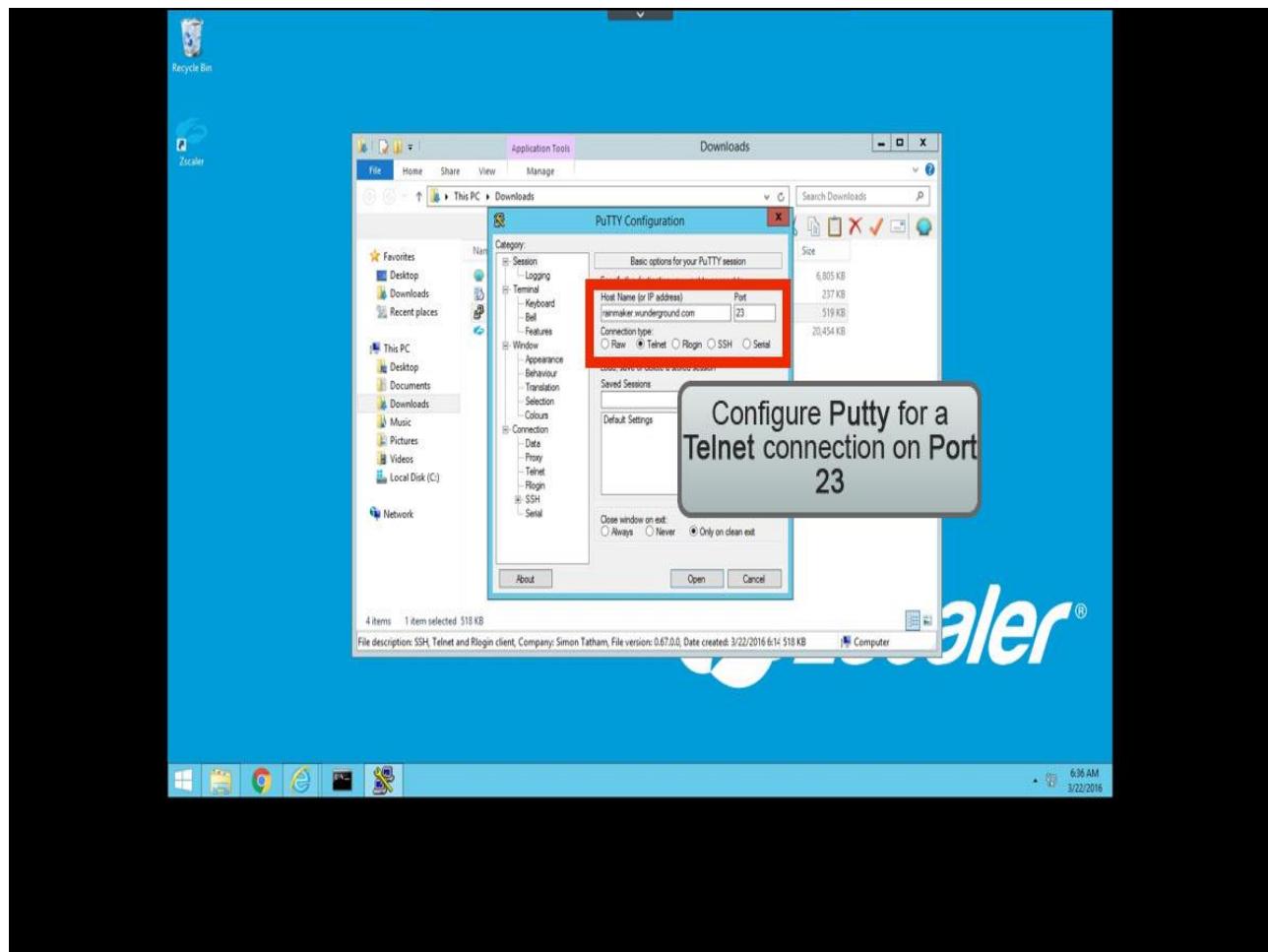
The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. The left sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Firewall Control" and shows a table of Firewall Filtering Rules. The table has columns for Rule Order, Admin Rank, Rule Name, Criteria, Action, and Description. There are 5 rows in the table:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
3	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
4	7	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow	
Default		Default Firewall Filtering Rule	Any	Block/Reset	

At the bottom of the interface, there is a "Help" button.

Slide notes

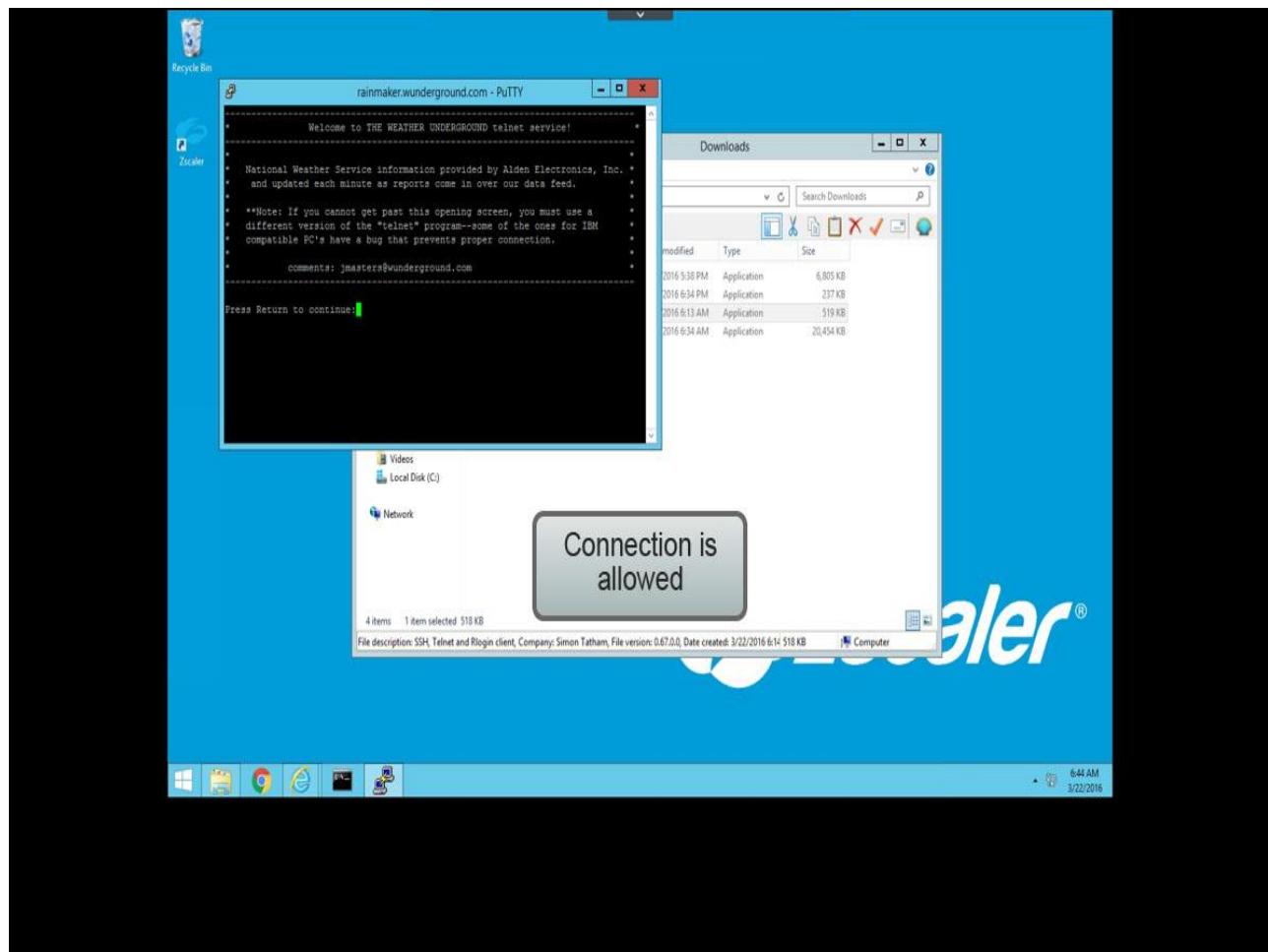
Slide 153 - Slide 153



Slide notes

Now let's test that Telnet is open using Putty.

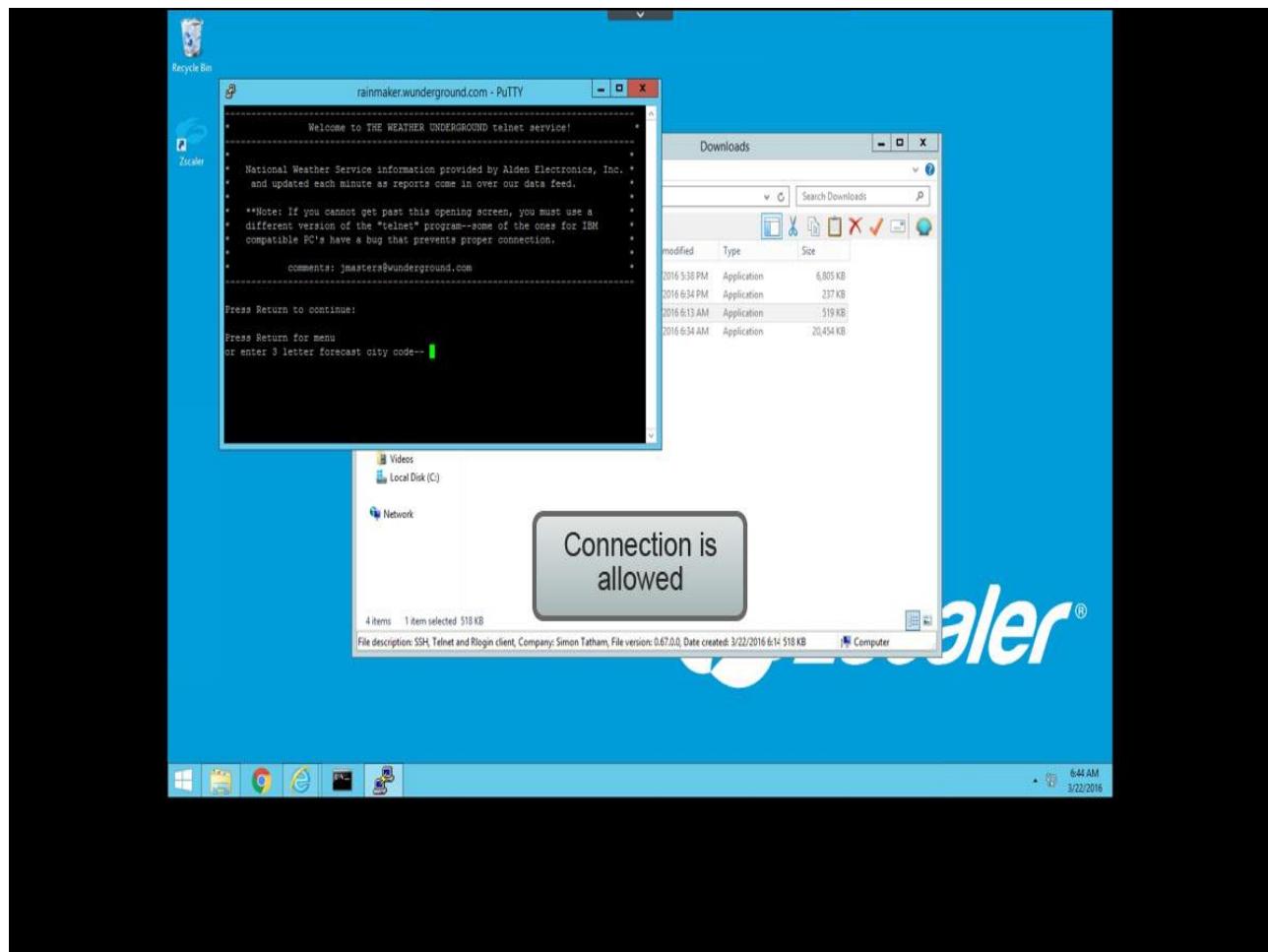
Slide 154 - Slide 154



Slide notes

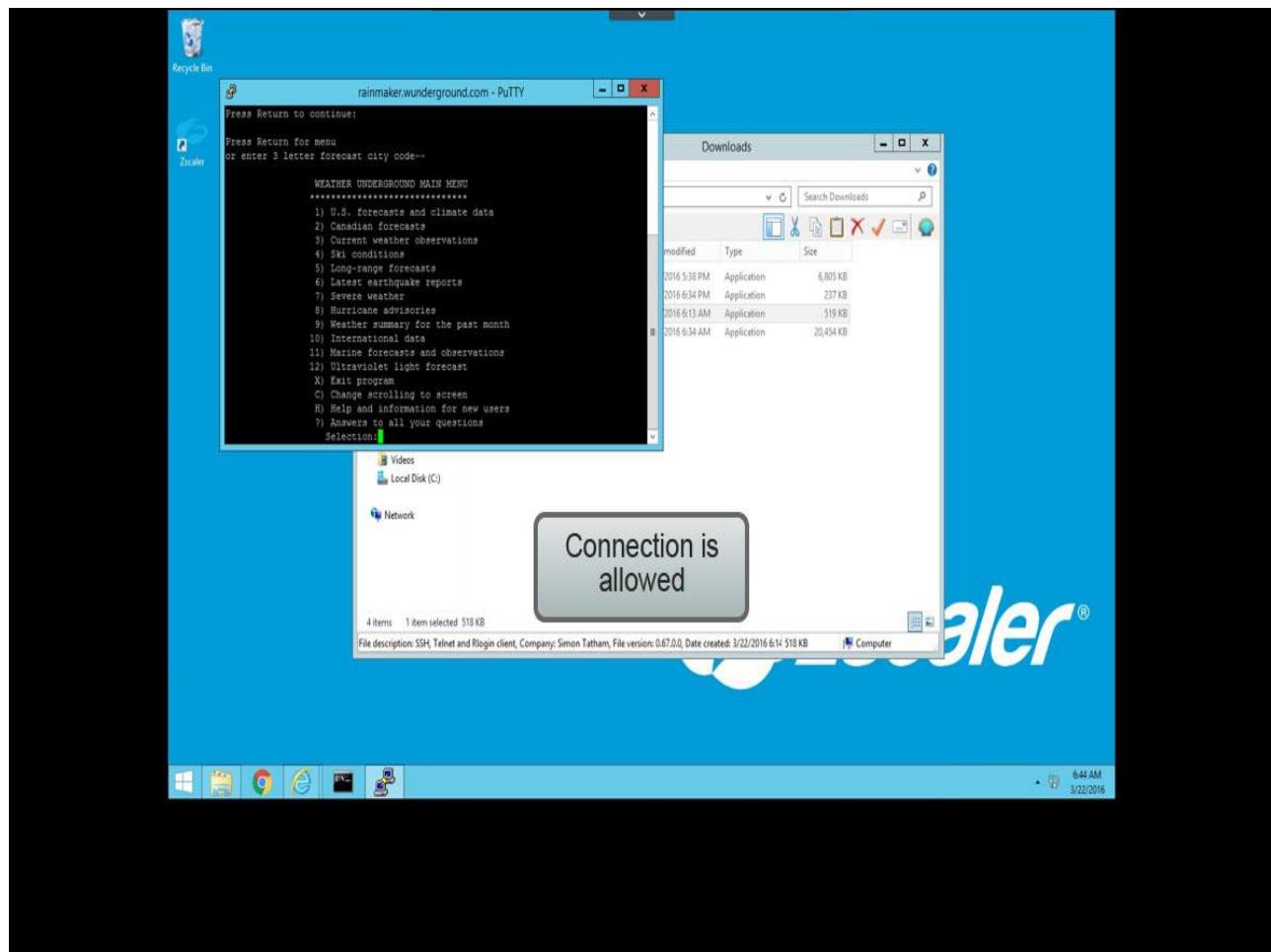
And as you can see, Telnet using port 23 is being allowed.

Slide 155 - Slide 155



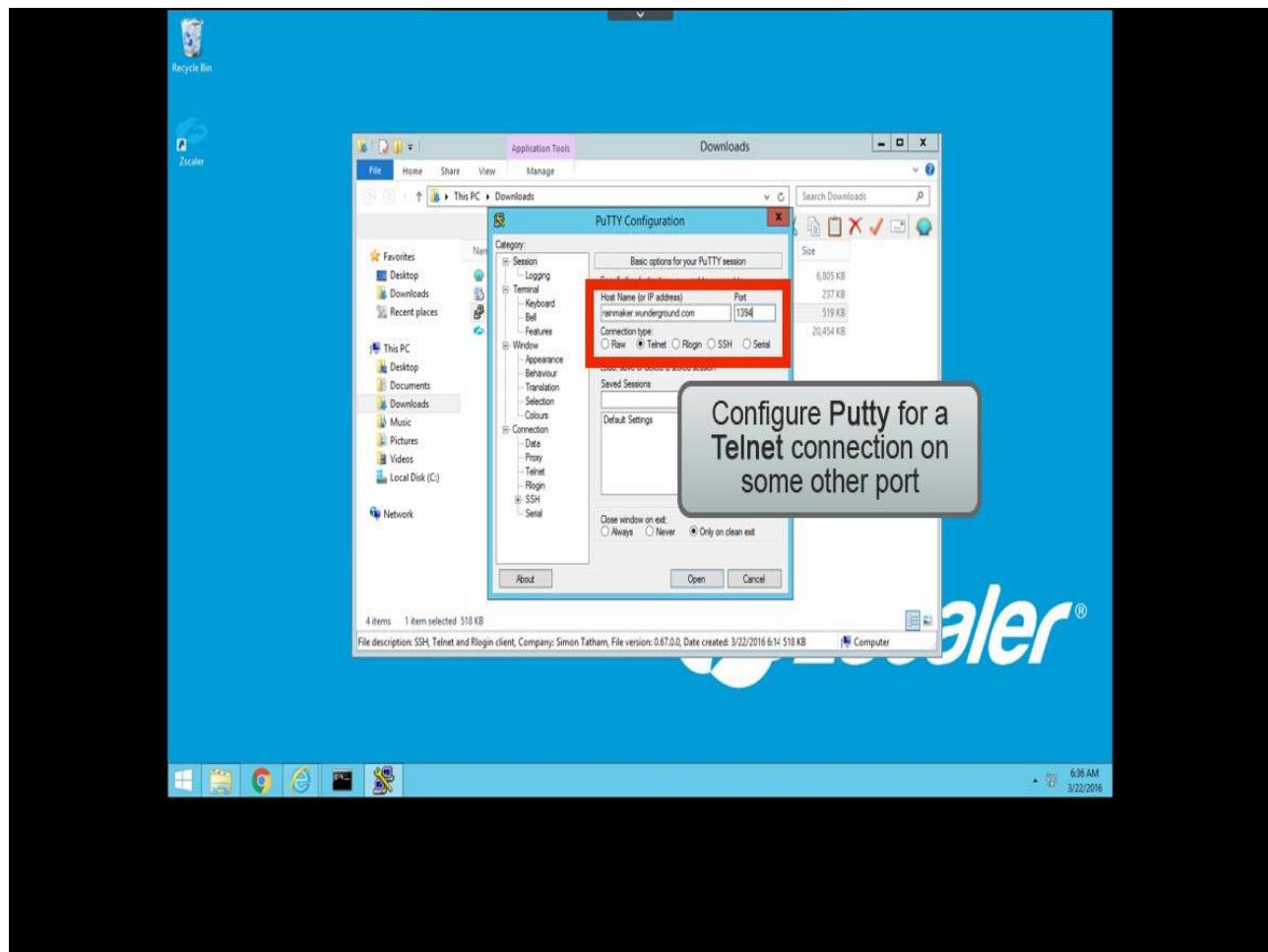
Slide notes

Slide 156 - Slide 156



Slide notes

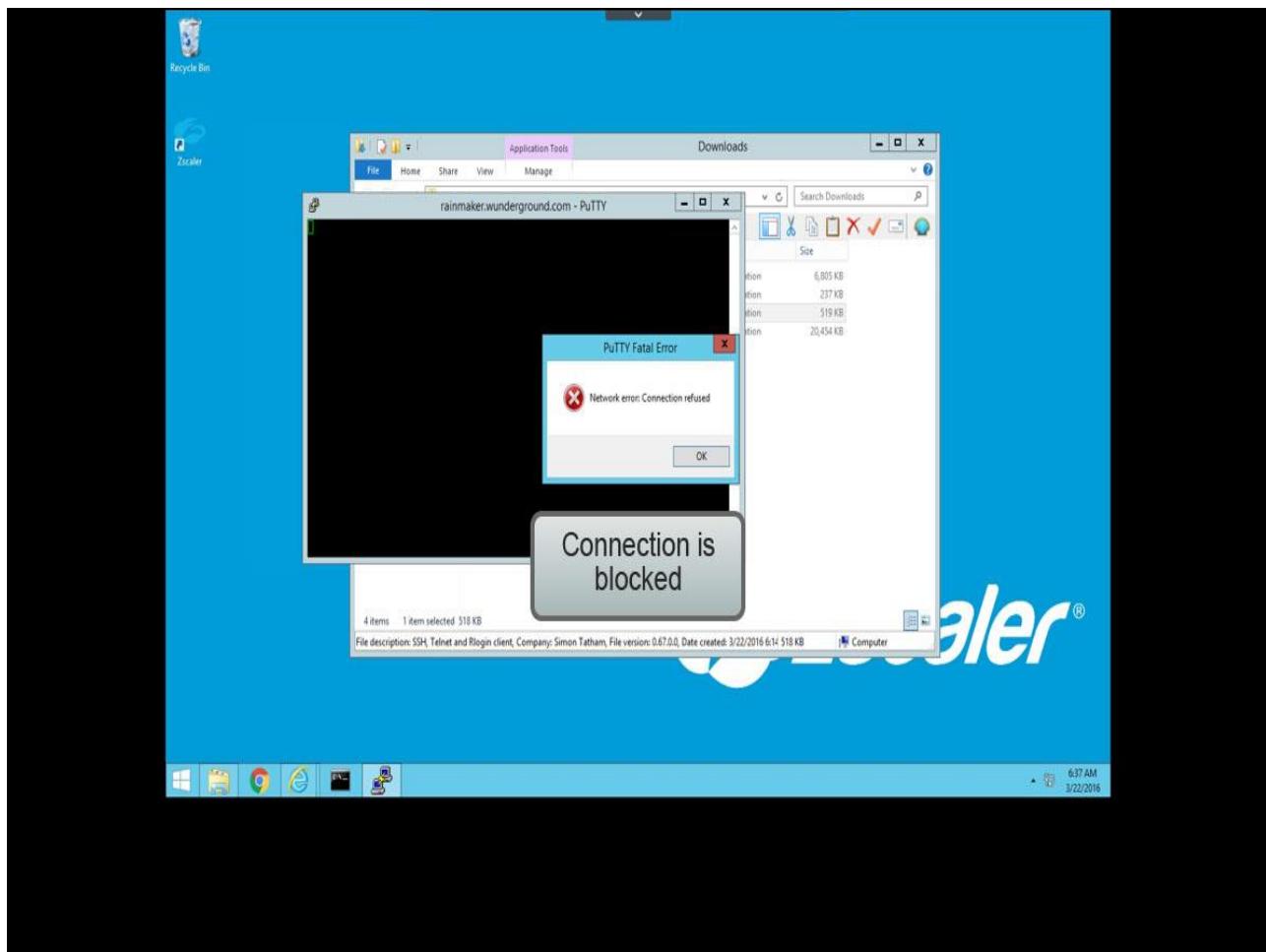
Slide 157 - Slide 157



Slide notes

But if we try to Telnet over some other port

Slide 158 - Slide 158



Slide notes

it is still being blocked.

Slide 159 - Slide 159

The screenshot shows the Zscaler Firewall Control Policy interface. On the left, a sidebar lists various navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section 'Configure Firewall Control Policy' with the note 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this, there are two tabs: 'FIREWALL FILTERING POLICY' (selected) and 'NAT CONTROL POLICY'. A button 'Add Firewall Filtering Rule' is visible. The main content is a table of rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	7	Permit from Web Proxy	NETWORK SERVICES HTTP, HTTPS	Allow	
3	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
4	7	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow	
Default	7	Default Firewall Filtering Rule	Any	Block/Reset	

A callout bubble with the text 'Click to edit the rule Allow Telnet' points to the fourth rule. A 'Click Box' icon is located in the bottom right corner of the interface.

Slide notes

As a further best practice, rules should always be listed from the most, to the least specific. So, let's change the order of the rule we just created to move it above the Web Proxy rule. Click **Edit** on that rule.

Slide 160 - Slide 160

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and shows a list of Firewall Filtering Rules:

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
4	7	Permit Telnet
Default		

A modal window titled 'Edit Firewall Filtering Rule' is open, showing the configuration for a rule named 'Click Box'. The 'Rule Order' dropdown is set to '4' and has a tooltip 'Click to edit the rule order'. The modal includes sections for 'CRITERIA', 'ACTION', and 'DESCRIPTION'. At the bottom, there are 'Save', 'Cancel', and 'Delete' buttons.

Slide notes

Select the correct **Rule Order** from the drop-down list (we will put this rule to number 1), click **Save**

Slide 161 - Slide 161

Firewall Control

Configure Firewall Control Policy
Rules are evaluated in the order specified. Evaluation stops at the first match.

FIREWALL FILTERING POLICY NAT CONTROL POLICY

Add Firewall Filtering Rule

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
4	7	Permit Telnet
Default 7 Default Firewall Filtering Rule		

WHO, WHERE

CRIERIA

DESTINATION IP

Users Groups

Departments Locations

Time

ACTION

Network Traffic

Allow

Logging

Aggregate Full

DESCRIPTION

Save Cancel Delete

Copyright © 2019 Zscaler Inc. All rights reserved. | Version 5.7 | Products | Help | Weblog Time: 1/15/2020 2:26:00 PM | Last Updated: 10:33:2019 2:26:00 PM

Slide notes

Slide 163 - Slide 163

Firewall Control

Configure Firewall Control Policy
Rules are evaluated in the order specified. Thus evaluation stops at the first match.

FIREWALL FILTERING POLICY NAT CONTROL POLICY

Add Firewall Filtering Rule

Rule Order	Admin Rank	Rule Name
1	0	Office 365 One Click Rule
2	7	Permit from Web Proxy
3	7	Permit DNS
4	7	Permit Telnet
Default 7 Default Firewall Filtering Rule		

WHO, WHERE, & WHEN SERVICES & APPLICATIONS SOURCE IP DESTINATION IP

CRITERIA

Users Groups
Any Any

Departments Locations
Any Any

Time
Always

ACTION

Network Traffic
Allow

Logging
Aggregate Full

DESCRIPTION

Click Save

Save Cancel Delete

Copyright © 2019 Zscaler Inc. All rights reserved. | Version 5.7 | Products | Help | Weblog Time: 1/15/2020 2:26:00 PM | Last Updated: 10:33:2020 2:26:00 PM

Slide notes

Slide 169 - Slide 169

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Firewall Control" and shows a table of rules. The table has columns: Rule Order, Admin Rank, Rule Name, Criteria, Action, Description, and three edit icons. There are five rows of rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow	
2	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
3	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
4	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
Default	7	Default Firewall Filtering Rule	Any	Block/Reset	

At the bottom, there are copyright information (Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies) and a help icon.

Slide notes

then **Activate** your changes.

Slide 170 - Slide 170

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, a dark sidebar contains icons for Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main area is titled 'MY ACTIVATION STATUS' with 'Editing' status. It shows 'CURRENTLY EDITING (1)' with a link to 'www.thinkingaboutit.com'. Below that is 'QUEUED ACTIVATIONS (0)' with 'None' listed. A 'Force Activate' button is present. The central part of the screen is the 'RULE CONTROL POLICY' editor. At the top, it says 'Rule evaluation stops at the first match.' Below is a table with columns: Rank, Rule Name, Criteria, Action, and Description. The table contains the following rules:

Rank	Rule Name	Criteria	Action	Description
	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow	
	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
	Default Firewall Filtering Rule	Any	Block/Reset	

At the bottom of the editor, there are 'Recommended Policy' and a search bar. A 'Help' icon is located in the bottom right corner.

Slide notes

Slide 174 - Slide 174

The screenshot shows the Zscaler Firewall Control interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a table for 'FIREWALL FILTERING POLICY'. The table has columns for Rule Order, Admin Rank, Rule Name, Criteria, Action, Description, and Edit/Delete icons. There are five rows: 1. Rule Order 1, Admin Rank 0, Rule Name 'Click Box CY', Criteria 'DESTINATION IP CATEGORIES Office 365', Action 'Allow'. 2. Rule Order 2, Admin Rank 0, Rule Name 'Office 365 One Click Rule', Criteria 'NETWORK SERVICES HTTP; HTTPS', Action 'Disabled'. 3. Rule Order 3, Admin Rank 7, Rule Name 'Permit from Web Proxy', Criteria 'NETWORK APPLICATIONS DNS', Action 'Allow'. 4. Rule Order 4, Admin Rank 7, Rule Name 'Permit DNS', Criteria 'NETWORK SERVICES DNS', Action 'Allow'. 5. Default, Admin Rank 7, Rule Name 'Default Firewall Filtering Rule', Criteria 'Any', Action 'Block/Reset'. A callout box with the text 'Click the NAT CONTROL POLICY tab' points to the 'NAT Click Box' tab in the top navigation bar.

Slide notes

You can also create rules that enable the Zscaler firewall to perform destination NAT, and redirect traffic to specific IP addresses, and if necessary, ports. To do this click the **NAT CONTROL POLICY** tab.

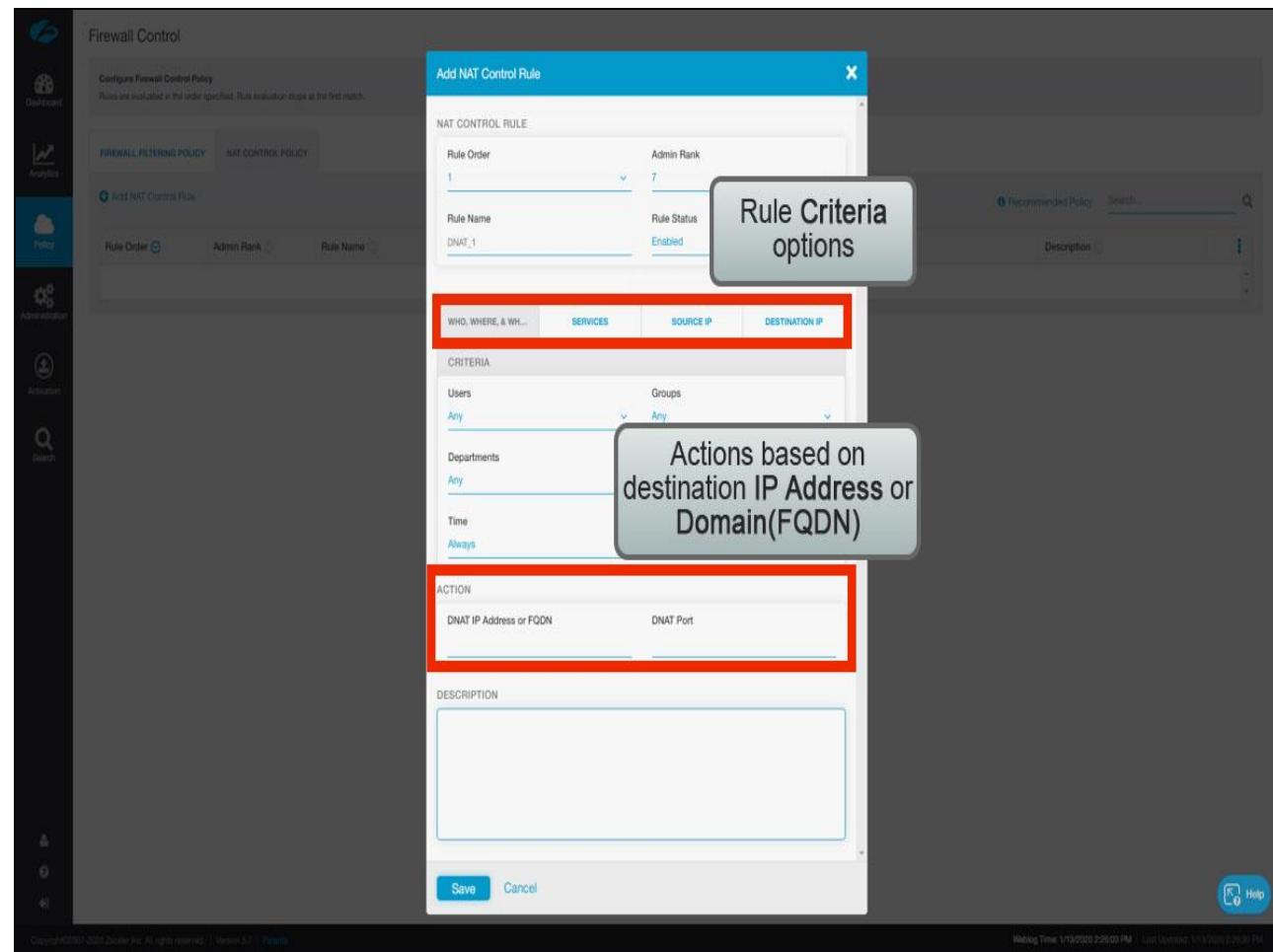
Slide 175 - Slide 175

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a sub-section titled 'Configure Firewall Control Policy'. It states: 'Rules are evaluated in the order specified. Rule evaluation stops at the first match.' Below this, there are two tabs: 'FIREWALL FILTERING POLICY' (which is selected) and 'NAT CONTROL POLICY'. A large callout box with the text 'Click Add NAT Control Rule' points to a blue button labeled 'Add NAT Control Rule'. To the right of the button is a search bar with the placeholder 'Search...' and a magnifying glass icon. At the bottom of the page, there is a footer with copyright information: 'Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies'. On the far right of the footer is a 'Help' icon.

Slide notes

To add a NAT Control Policy, click the **Add NAT Control Rule** link.

Slide 176 - Slide 176



Slide notes

You can add a rule in a similar way to adding a Firewall rule, and the same criteria tabs are available. Although, note that this type of policy does not support **Network Applications** as a criteria.

To support domains with multiple destination IP addresses or with destination IP addresses that may change, you can configure the actions for your NAT Control rules using FQDNs instead of IP addresses if necessary.

Slide 177 - Slide 177

The screenshot shows the Zscaler Firewall Control interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Click-Box Policy (which is selected), Administration, Activation, and Search. The main area is titled "Firewall Control" and contains a sub-section titled "Configure Firewall Control Policy". It says, "Rules are evaluated in the order specified. Rule evaluation stops at the first match." Below this are two tabs: "FIREWALL FILTERING POLICY" (selected) and "NAT CONTROL POLICY". There's a button to "Add NAT Control Rule". A search bar includes a "Recommended Policy" dropdown and a search input field. A table below has columns for "Rule Order", "Admin Rank", "Rule Name", "Criteria", "Action", and "Description". A message at the bottom of the table says "No matching items found". At the bottom right of the main area is a "Help" icon. The footer of the page includes copyright information: "Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies" and "Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM".

Slide notes

One final note. Some peer-to-peer applications like Tor, BitTorrent, Google Talk, etc., must also be enabled under **Advanced Threat Protection**. From the **Policy** menu

Slide 178 - Slide 178

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left sidebar, under the 'Web' category, 'Malware Protection' is selected, highlighted with a red box. A callout bubble points to this selection with the text 'Click Advanced Threat Protection'. Other options in the sidebar include 'Sandbox', 'Browser Control', 'SSL Inspection', 'Data Loss Prevention', 'Mobile App Store Control', 'Firewall Filtering', 'DNS Control', 'FTP Control', and 'IPS Control'. The main content area shows a table with columns 'Criteria', 'Action', and 'Description'. A message at the top right says 'No matching items found'. The bottom of the screen displays the URL 'https://admin.zscaler.net/policy/web/malware-protection' and the timestamp 'Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM'.

Slide notes

select Advanced Threat Protection.

Slide 179 - Slide 179

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. The left 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 explains that the policy protects traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. The "ADVANCED THREATS POLICY" tab is selected, showing a "SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)" section with a risk slider set at "Moderate Risk". Below this are sections for "BOTNET PROTECTION" (allow or block Command & Control Servers and Traffic), "MALICIOUS ACTIVE CONTENT PROTECTION" (allow or block Malicious Content & Sites, Vulnerable ActiveX Controls, Browser Exploits, and File Format Vulnerabilities), and a "Blocked Malicious URLs" list with a search bar and "Add Items" button. At the bottom are "Save" and "Cancel" buttons, and a "Help" icon.

Slide notes

Scroll down to the bottom of the page.

Slide 181 - Slide 181

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

Anonymizers Recommended Policy

CROSS-SITE SCRIPTING (XSS) PROTECTION

Cookie Stealing

Potentially Malicious Requests

SUSPICIOUS DESTINATIONS PROTECTION

Blocked Countries None

P2P FILE SHARING PROTECTION

BitTorrent

P2P ANONYMIZER PROTECTION

Tor

P2P VOIP PROTECTION

Google Talk

Save Cancel Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM

Slide notes

Enable any P2P applications that are required and click **Save**.

Slide 182 - Slide 182

The screenshot shows the 'Advanced Threat Protection' section of the Zscaler Click Box Policy configuration. A large, semi-transparent gray box labeled 'Click POLICY' is overlaid on the interface. The main content area includes sections for 'ADVANCED THREATS POLICY' (with tabs for 'ANONYMIZERS' showing 'Allow' and 'Block' options), 'CROSS-SITE SCRIPTING (XSS) PROTECTION' (with 'Cookie Stealing' listed), 'SUSPICIOUS DESTINATIONS PROTECTION' (with 'Blocked Countries' set to 'None'), 'P2P FILE SHARING PROTECTION' (with 'BitTorrent' listed), 'P2P ANONYMIZER PROTECTION' (with 'Tor' listed), and 'P2P VOIP PROTECTION' (with 'Google Talk' listed). At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Slide notes

Now, let's turn to our **Firewall** Policy ruleset. From the **Policy** menu

Slide 183 - Slide 183

The screenshot shows the Zscaler Policy Cloud interface. On the left, a dark sidebar contains various navigation links: Web, Security, Access Control, Malware Protection (selected), Advanced Threat Protection, Sandbox, URL & Cloud App Control, File Type Control, Data Loss Prevention (selected), Data Loss Prevention, Mobile (selected), Zscaler App Configuration, Zscaler App Portal, Mobile Malware Protection, Activation, and Search. A callout bubble points to the 'Firewall Control' link under the 'ACCESS CONTROL' section of the sidebar. The main content area displays a summary of Malware Protection features, including protection against various Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. A 'Recommended Policy' button is visible in the top right corner of the main content area.

Slide notes

Click Firewall Control.

Slide 185 - Slide 185

The screenshot shows the Zscaler Firewall Control Policy configuration page. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Firewall Control' and contains a table of rules. A callout box with a blue border and white text points to the second rule, which is highlighted with a red box. The rule is labeled 'Office 365 One Click Rule' and has an 'Allow' action. A 'Click Recommended Policy' button is overlaid on the callout box.

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow	
2	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365		
3	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
4	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow	
Default	7	Default Firewall Filtering Rule	Any	Block/Reset	

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies | Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM | Help

Slide notes

To view Zscaler recommended settings for Firewall Control Policy, click the **Recommended Policy** link.

Slide 186 - Slide 186

The screenshot shows the Zscaler Firewall Control interface. On the left, a sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Firewall Control" and shows a "Recommended Policy". A modal window titled "View Recommended Firewall Control Policy" is open, displaying the following rules:

Rule Order	Admin Rank	Rule Name
1	0	Permit Telnet
2	0	Office 365 One Click Rule
3	7	Permit from Web Proxy
4	7	Permit DNS
Default	7	Default Firewall Filtering Rule

Each rule has a "FIREWALL FILTERING RULE" section with "Rule Order" and "Rule Status: Enabled". The "Default Firewall Filtering Rule" also includes a "SERVICES & APPLICATIONS → CRITERIA" section listing "Network Services: DNS, HTTP, HTTPS". The "ACTION" section for all rules is set to "Allow" except for the Default rule, which is set to "Block/Drop".

Slide notes

It is difficult for Zscaler to recommend Firewall Policy settings, as each organization will have their own needs. However, it is recommended that if you create rule to allow specific classes of traffic, that you then change the Default rule to **Block**.

Slide 187 - Slide 187

The screenshot shows the Zscaler Firewall Control interface. On the left is a navigation sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Firewall Control" and contains a table of filtering rules. The table has columns for Rule Order, Admin Rank, Rule Name, Criteria, Action, and Description. There are four rows of rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow	
2	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
3	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
4	7	Permit DNS			
Default	7	Default Firewall Filtering Rule			

A callout box contains the following text:

Web traffic processing order:
1. URL & Cloud App Control Policy
2. Firewall Policy

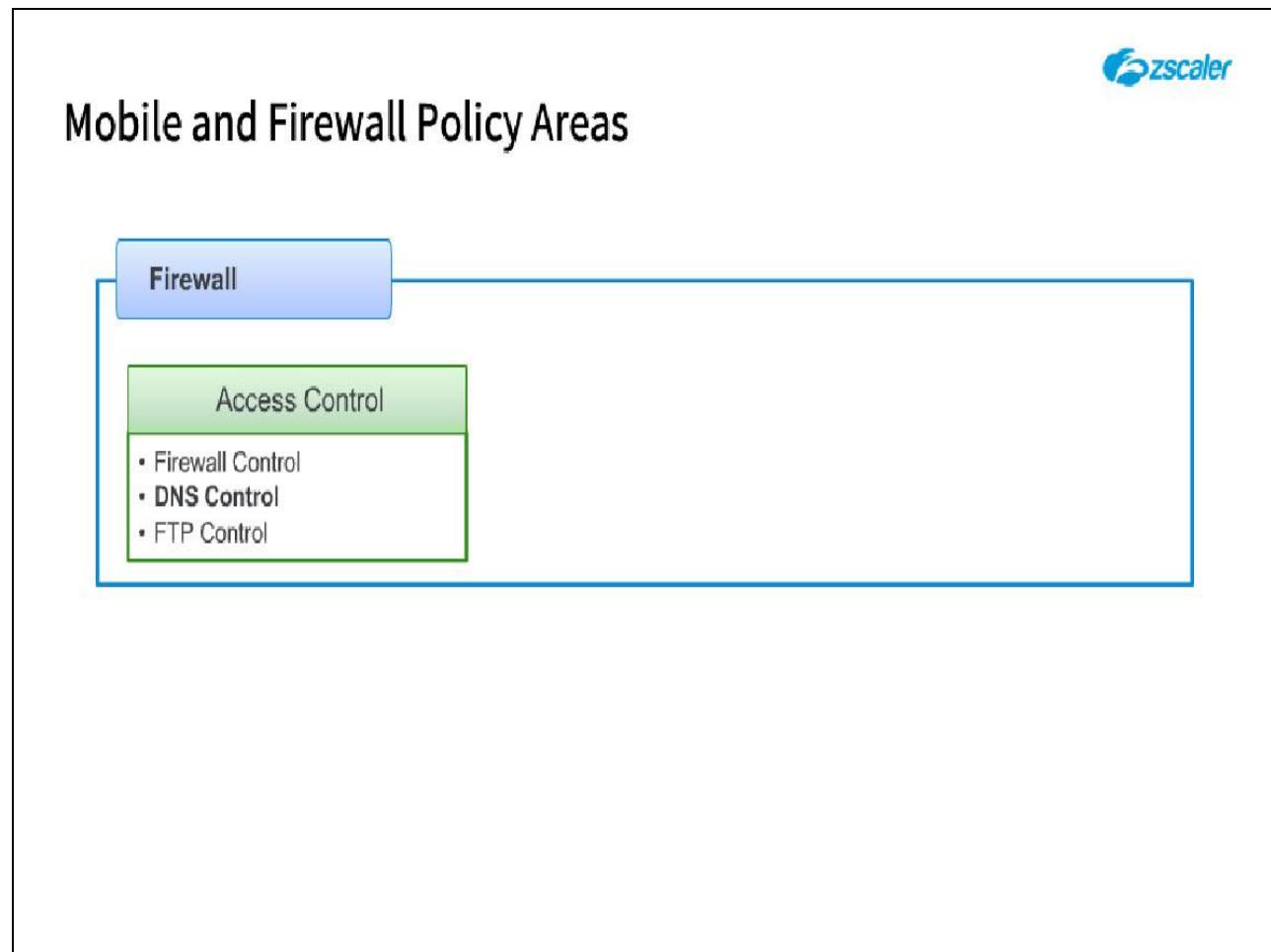
Non-Web traffic processing order:
1. Firewall Policy

Slide notes

If Firewall rules are configured, when the ZEN receives outbound Web traffic from your organization it sends the traffic to its Web module for policy evaluation; if the traffic violates a Web policy, it blocks the transaction; if the traffic does not violate any Web policies, it then sends the traffic to the Firewall module for policy evaluation. If the traffic violates a Firewall policy, the ZEN blocks the transaction; if the traffic does not violate any Firewall policies, the traffic is allowed to proceed to the Internet.

When the ZEN receives outbound non-Web traffic going to ports other than 80/443, it sends the traffic directly to the Firewall module for policy evaluation. If the traffic violates a Firewall policy, it blocks the transaction; if the traffic does not violate any Firewall policies, it allows the traffic to proceed to the Internet.

Slide 188 - Mobile and Firewall Policy Areas



Slide notes

Next, let's look at the **DNS Control** policy options.

Slide 189 - Slide 189

Firewall Control

Configure Firewall Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

FIREWALL FILTERING POLICY **NAT CONTROL POLICY**

Add Firewall Filtering Rule **Recommended Policy** **Search...**

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description	Actions
1	0	Permit Telnet	NETWORK APPLICATIONS Telnet NETWORK SERVICES Telnet	Allow		
3	7	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled		
4	7	Permit from Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow		
Default	7	Permit DNS	NETWORK APPLICATIONS DNS NETWORK SERVICES DNS	Allow		
		Default Firewall Filtering Rule	Any	Block/Reset		

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | [Patents](#)

Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM

Slide notes

If Firewall rules are configured, when the ZEN receives outbound Web traffic from your organization it sends the traffic to its Web module for policy evaluation; if the traffic violates a Web policy, it blocks the transaction; if the traffic does not violate any Web policies, it then sends the traffic to the Firewall module for policy evaluation. If the traffic violates a Firewall policy, the ZEN blocks the transaction; if the traffic does not violate any Firewall policies, the traffic is allowed to proceed to the Internet.

When the ZEN receives outbound non-Web traffic going to ports other than 80/443, it sends the traffic directly to the Firewall module for policy evaluation. If the traffic violates a Firewall policy, it blocks the transaction; if the traffic does not violate any Firewall policies, it allows the traffic to proceed to the Internet.

Click on Policy.

Slide 190 - Slide 190

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left sidebar, under the 'Policy' section, there is a 'DNS Control' button highlighted with a red box and a callout bubble containing the text 'Click DNS Control'. The main pane displays a table of policy rules:

Name	Criteria	Action	Description
Mobile	NETWORK APPLICATIONS Telnet	Allow	
ZSCALER APP CONFIGURATION	SECURITY Mobile Malware Protection		
Zscaler App Portal	Mobile Malware Protection		
ACCESS CONTROL			
Mobile App Store Control			
Firewall Filtering			
DNS Control	DESTINATION IP CATEGORIES Office 365	Disabled	
From Web Proxy	NETWORK SERVICES HTTP; HTTPS	Allow	
ACCESS CONTROL			
Domain Control	NETWORK APPLICATIONS	Allow	
Block/Reset			

At the bottom of the interface, there is a URL bar showing the address <https://admin.zscaler.net/policy/web/malware-protection>, a timestamp 'Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM', and a 'Help' button.

Slide notes

And then click on DNS Control.

Slide 192 - Slide 192

The screenshot shows the 'DNS Control' section of the Zscaler interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' A button labeled 'Add Click Box Rule' is highlighted with a red box and an arrow pointing to it. Below this, a table lists rules:

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Microsoft 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled		
Default	Click Add DNS Filtering Rule		Allow		
Default			Allow		

At the bottom of the interface, there is a copyright notice: 'Copyright © 2007-2018 Zscaler Inc. All rights reserved. | Version 5.8 | Policies'.

Slide notes

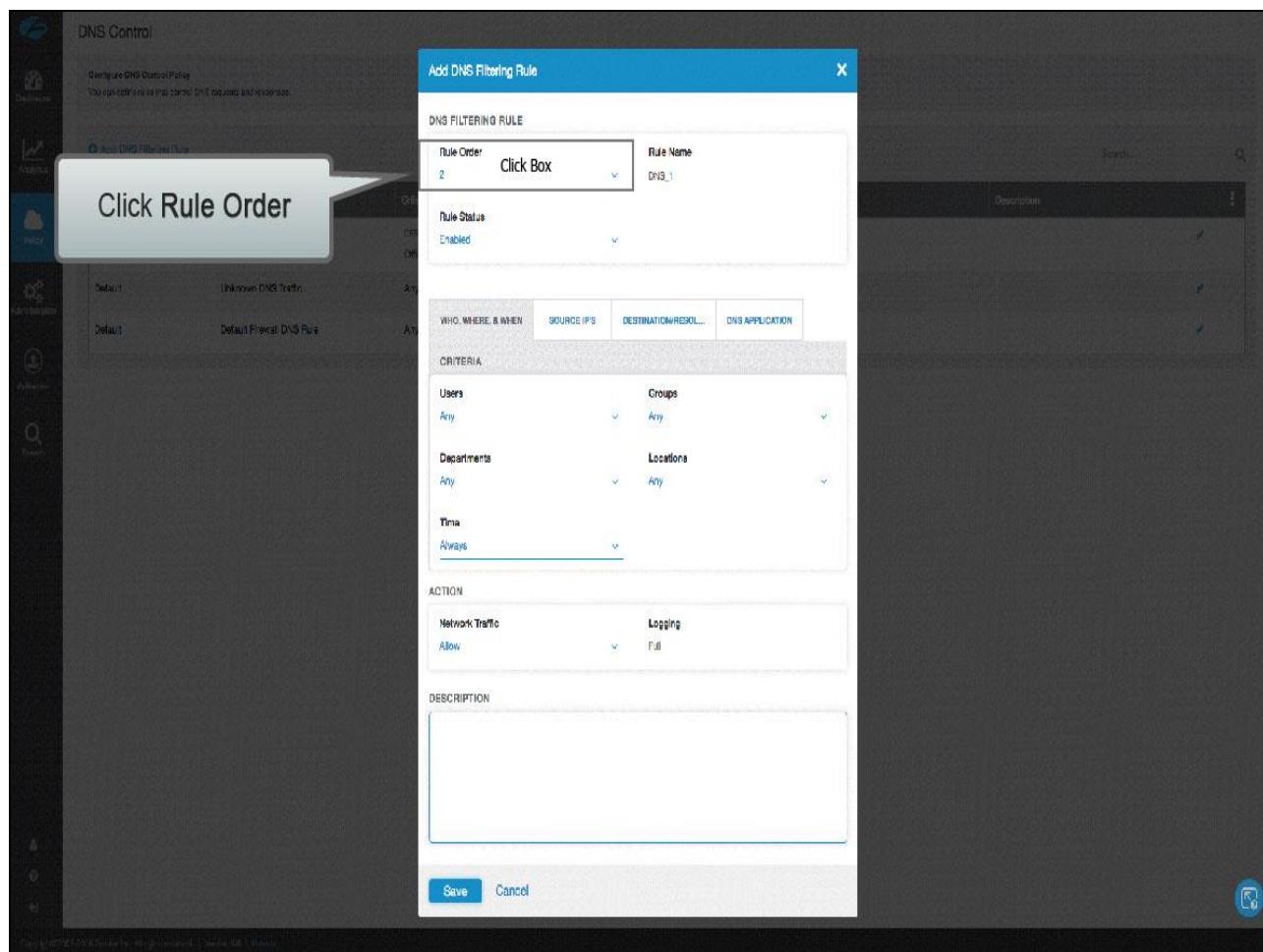
Here a system generated rule for Microsoft Office 365 traffic was added automatically at position 1 when the Microsoft Office **One Click** feature was enabled. The rule is currently in the disabled state, because **One Click** was later disabled.

There are also two default **Allow** rules.

DNS Control policy rules may be added to allow or block DNS requests, redirect requests to a different DNS server, redirect DNS responses by substituting a preconfigured IP address into a DNS response, and allowing or blocking DNS Tunnel traffic.

A common use case would be to protect against the use of DNS Tunnel traffic for malicious purposes. To add a rule to block all DNS Tunnel traffic follow these steps. Click **Add DNS Filtering Rule**.

Slide 193 - Slide 193



Slide notes

Specify Rule Order, Rule Name, and Rule Status.

Slide 194 - Slide 194

Click to select 2

DNS Control

Add DNS Filtering Rule

DNS FILTERING RULE

Rule Order: 2

Rule Name: DNS_1

WHO, WHERE, & WHEN

SOURCE IP/S

DESTINATION/RESOL...

DNS APPLICATION

CRITERIA

Users: Any

Groups: Any

Departments: Any

Locations: Any

Time: Always

ACTION

Network Traffic: Allow

Logging: Full

DESCRIPTION

Save Cancel

Slide notes

Slide 195 - Slide 195

The screenshot shows the Zscaler Policy-Cloud Firewall interface under the 'DNS Control' section. On the left, there's a sidebar with various icons for Dashboards, Analytics, Policy, Application, Activation, and Search. The main area displays a list of existing DNS filtering rules:

Rule Order	Rule Name	Description
1	Office 365 One Click Rule	Office 365
Default	Unknown DNS Traffic	Any
Default	Default Firewall DNS Rule	Any

A modal window titled 'Add DNS Filtering Rule' is open in the center. It contains fields for 'Rule Order' (set to 2), 'Rule Name' (set to 'DNS_1'), 'Rule Status' (set to 'Enabled'), and sections for 'CRITERIA' (Users, Departments, Time) and 'ACTION' (Network Traffic, Logging). A large 'DESCRIPTION' text area is empty. At the bottom are 'Save' and 'Cancel' buttons.

A callout bubble with the text 'Click Rule Name' points to the 'Rule Name' input field in the modal.

Slide notes

Slide 196 - Slide 196

The screenshot shows the Zscaler Policy-Cloud Firewall interface with the 'DNS Control' tab selected. On the left, there's a sidebar with various icons for Dashboards, Analytics, Policy, Application, Activation, and Search. The main area displays a table of existing DNS filtering rules:

Rule Order	Rule Name	Condition
1	Office 365 One Click Rule	Office 365
Default	Unknown DNS Traffic	Any
Default	Default Firewall DNS Rule	Any

A modal window titled 'Add DNS Filtering Rule' is open in the center. It contains fields for 'Rule Order' (set to 2), 'Rule Name' (with a placeholder 'Type "Block DNS Tunnels" then hit enter'), 'Rule Status' (set to Enabled), and 'Criteria' and 'Action' sections. The 'Criteria' section includes dropdowns for Users (Any), Groups (Any), Departments (Any), Locations (Any), and Time (Always). The 'Action' section includes dropdowns for Network Traffic (Allow) and Logging (Full). A large 'DESCRIPTION' text area is present at the bottom of the modal.

Slide notes

Slide 197 - Slide 197

The screenshot shows the 'Add DNS Filtering Rule' dialog box over a dark background of the ZCC Cloud Firewall interface. The dialog is divided into several sections:

- DNS FILTERING RULE:** Contains fields for 'Rule Order' (set to 2), 'Rule Name' (set to 'Block DNS Tunnels'), and 'Rule Status' (set to 'Enabled').
- CRITERIA:** This section is highlighted with a red box and contains four dropdowns:
 - Users:** Set to 'Any'
 - Groups:** Set to 'Any'
 - Departments:** Set to 'Any'
 - Locations:** Set to 'Any'
- ACTION:** Contains two dropdowns:
 - Network Traffic:** Set to 'Allow'
 - Logging:** Set to 'Full'
- DESCRIPTION:** An empty text area.

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

Slide notes

Configure **WHO, WHERE, & WHEN** with the default settings for Any Users, Groups, Departments, and Locations, and the Time as Always.

Slide 198 - Slide 198

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for DNS, Analytics, Policy, Optimization, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists existing rules: 'Office 365 One Click Rule' (Rule Order 1), 'Unknown DNS Traffic' (Default), and 'Default Firewall DNS Rule' (Default). A modal window titled 'Add DNS Filtering Rule' is open. Inside, the 'DNS FILTERING RULE' section includes fields for 'Rule Order' (set to 2), 'Rule Name' ('Block DNS Tunnels'), and 'Rule Status' ('Enabled'). The 'WHO, WHERE, & WHEN' section contains a 'Click Box' button, which is highlighted with a callout bubble containing the text 'Click Source IP'S'. Below this are sections for 'DESTINATION/RESOL...' and 'DNS APPLICATION'. The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Full'. The 'DESCRIPTION' section is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Configure **SOURCE IP'S** with the default setting of None for Source IP Groups to apply to all.

Slide 199 - Slide 199

The screenshot shows the Zscaler Policy-Cloud Firewall interface with the 'DNS Control' tab selected. On the left, there's a sidebar with various icons for Dashboards, Analytics, Policy, Optimization, Activation, and Search. The main area displays a table of existing DNS filtering rules:

Rule Order	Rule Name	Description
1	Office 365 One Click Rule	Office 365
Default	Unknown DNS Traffic	Any
Default	Default Firewall DNS Rule	Any

A modal window titled 'Add DNS Filtering Rule' is open in the center. It contains the following fields:

- DNS FILTERING RULE**
 - Rule Order: 2
 - Rule Name: Block DNS Tunnels
 - Rule Status: Enabled
- CRITERIA**
 - Source IP Groups: A dropdown menu set to 'None', which is highlighted with a red box.
 - IP Addresses: An input field containing a placeholder 'IP Addresses' with a 'Add Items' button.
- ACTION**
 - Network Traffic: Set to 'Allow'
 - Logging: Set to 'Full'
- DESCRIPTION**
 - A large text area for entering a description, currently empty.

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

Slide notes

Configure **DESTINATION** with the Server IP Groups default of None to apply to all.

Configure **SOURCE IP'S** with the default setting of None for Source IP Groups to apply to all.

Slide 200 - Slide 200

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for DNS, Analytics, Policy, Optimization, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists three existing rules: 'Office 365 One Click Rule', 'Unknown DNS Traffic', and 'Default Firewall DNS Rule'. A modal window titled 'Add DNS Filtering Rule' is open. Inside, under the 'WHO, WHERE, & WHEN' tab, there's a 'SOURCE IP'S' section with a dropdown menu. A callout bubble with the text 'Click DESTINATION' points to this dropdown. Other tabs in the modal include 'DESTINATION' (which is highlighted) and 'DNS APPLICATION'. The 'DESTINATION' tab contains sections for 'Source IP Groups' (set to 'None'), 'IP Addresses' (an empty input field), and 'DESCRIPTION' (an empty text area). The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Full'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Configure **DESTINATION** with the Server IP Groups default of None to apply to all.

Slide 201 - Slide 201

The screenshot shows the Zscaler Cloud Firewall interface under the 'DNS Control' section. A modal window titled 'Add DNS Filtering Rule' is open. In the 'DNS FILTERING RULE' section, the 'Rule Order' is set to 2 and the 'Rule Name' is 'Block DNS Tunnels'. The 'Rule Status' is 'Enabled'. Under the 'CRITERIA' section, the 'DNS APPLICATION' tab is selected, and the 'DNS Server IP Groups' dropdown is set to 'None'. Below this, there is a 'DNS Server IP Addresses' input field with an 'Add Items' button. The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Full'. The 'DESCRIPTION' section has a large empty text area. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Configure **DNS APPLICATION** to apply to the DNS Application Group added earlier for **All DNS Tunnels**.

Configure **DESTINATION** with the Server IP Groups default of None to apply to all.

Slide 202 - Slide 202

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboards, Analytics, Policy, Application, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists three existing rules: 'Office 365 One Click Rule', 'Unknown DNS Traffic', and 'Default Firewall DNS Rule'. A modal window titled 'Add DNS Filtering Rule' is open. Inside, the 'DNS FILTERING RULE' section includes fields for 'Rule Order' (set to 2), 'Rule Name' ('Block DNS Tunnels'), and 'Rule Status' ('Enabled'). Below this is a 'WHO, WHERE, & WHEN' section with tabs for 'WHO', 'WHERE', and 'WHEN'. A callout bubble with the text 'Click DNS APPLICATION' points to the 'WHO' tab. Other sections include 'CRITERIA' (with 'DNS Server IP Groups' set to 'None' and 'DNS Server IP Addresses' empty), 'ACTION' (with 'Network Traffic' set to 'Allow' and 'Logging' to 'Full'), and 'DESCRIPTION' (an empty text area). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Configure **DNS APPLICATION** to apply to the DNS Application Group added earlier for **All DNS Tunnels**.

Slide 203 - Slide 203

The screenshot shows the 'DNS Control' section of the Zscaler Policy-Cloud Firewall. On the left, there's a sidebar with various icons for Dashboards, Analytics, Policy, Application, Activation, and Search. The main area displays a table of existing DNS filtering rules:

Rule Order	Rule Name	Description
1	Office 365 One Click Rule	Office 365
Default	Unknown DNS Traffic	Any
Default	Default Firewall DNS Rule	Any

A modal window titled 'Add DNS Filtering Rule' is open. It has a 'DNS FILTERING RULE' header. Inside, there are fields for 'Rule Order' (set to 2), 'Rule Name' (set to 'Block DNS Tunnels'), and 'Rule Status' (set to 'Enabled'). The 'DNS APPLICATION' tab is selected under the 'CRITERIA' section. A callout bubble with the text 'Click DNS Application Group' points to the 'DNS Application Group' dropdown, which currently shows 'Any'. Other criteria listed include 'DNS Tunnels & Network Apps' (Any), 'Resolved IP-Based Countries' (Any), and 'Requested Domain/Resolved IP Categories' (Any). The 'ACTION' section shows 'Network Traffic' set to 'Allow' and 'Logging' set to 'Full'. The 'DESCRIPTION' section is empty. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

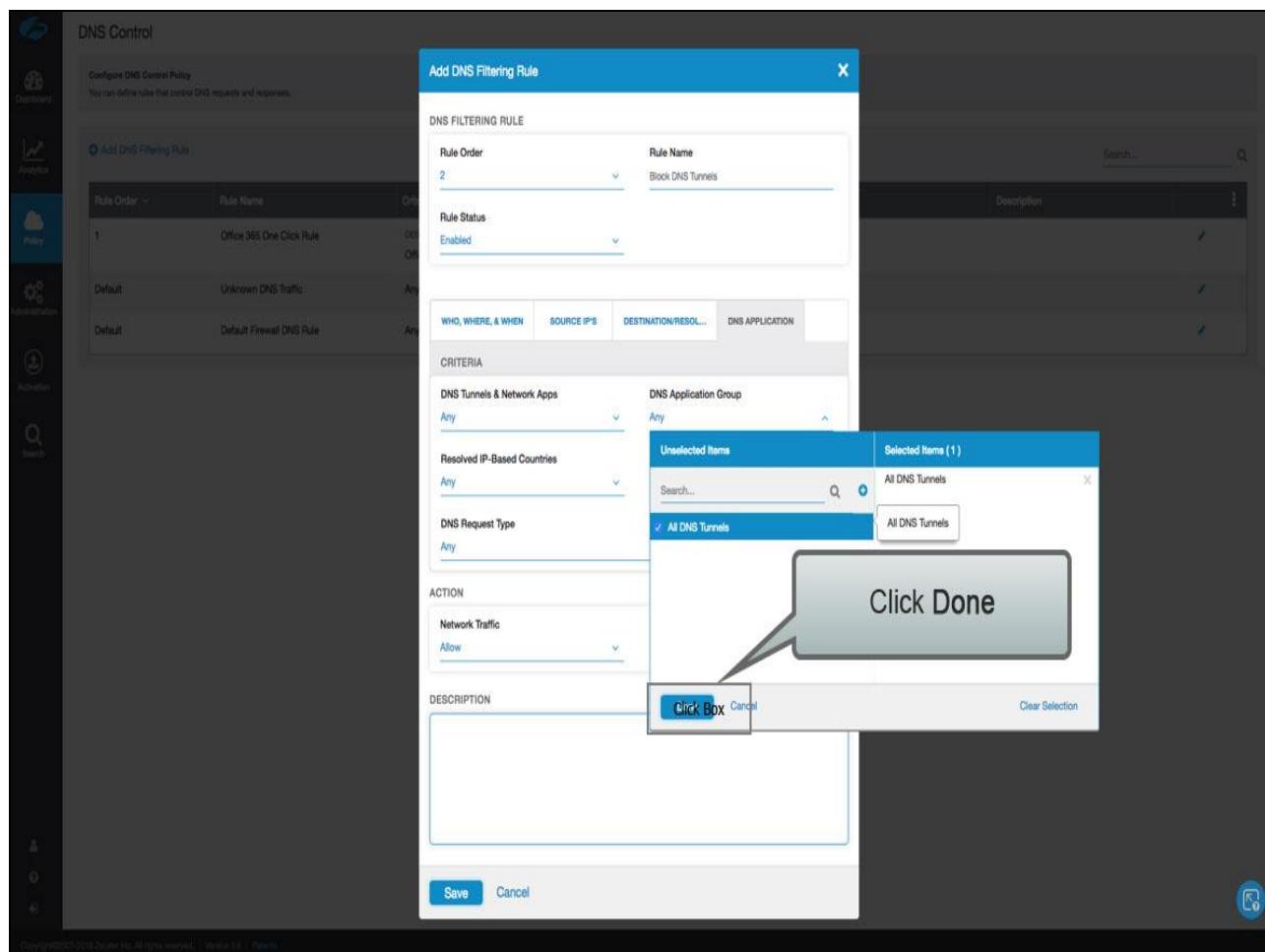
Configure **DNS APPLICATION** to apply to the DNS Application Group added earlier for **All DNS Tunnels**.

Slide 204 - Slide 204

The screenshot shows the Zscaler Policy-Cloud Firewall DNS Control interface. On the left, there's a sidebar with various icons for Dashboards, Analytics, Policy, Optimization, Activation, and Search. The main area is titled 'DNS Control' and has a sub-section 'Configure DNS Control Policy'. It lists three existing rules: 'Office 365 One Click Rule', 'Unknown DNS Traffic', and 'Default Firewall DNS Rule'. A modal window titled 'Add DNS Filtering Rule' is open. In the 'DNS FILTERING RULE' section, the 'Rule Order' is set to 2 and the 'Rule Name' is 'Block DNS Tunnels'. The 'Rule Status' is 'Enabled'. Below this, there are tabs for 'WHO, WHERE, & WHEN', 'SOURCE IP/S', 'DESTINATION/RESOL...', and 'DNS APPLICATION'. The 'DNS APPLICATION' tab is selected, showing criteria for 'DNS Tunnels & Network Apps' (set to 'Any'), 'Resolved IP-Based Countries' (set to 'Any'), and 'DNS Request Type' (set to 'Any'). A callout box with the text 'Click All DNS Tunnels' points to the 'All DNS Tunnels' checkbox in the 'DNS Tunnels & Network Apps' dropdown. A secondary callout box points to the 'Click Box' checkbox. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons, and a 'Done' button at the top right of the modal.

Slide notes

Slide 205 - Slide 205



Slide notes

Slide 206 - Slide 206

In ACTION click Network Traffic

Slide notes

Set the Action to **Block** Network Traffic. Note that **Full** logging of any matches is enabled by default.

Slide 207 - Slide 207

The screenshot shows the Zscaler Cloud Firewall DNS Control interface. On the left, there's a sidebar with various icons for DNS, Analytics, Policy, Application, Activation, and Search. The main area is titled 'DNS Control' and shows a list of existing DNS filtering rules. One rule is selected: 'Office 365 One Click Rule' (Rule Order 1, Enabled). A new rule is being added with the name 'Block DNS Tunnels' and Rule Order 2. The 'DNS APPLICATION' tab is active under the 'CRITERIA' section, which includes filters for DNS Tunnels & Network Apps (Any), Resolved IP-Based Countries (Any), and Requested Domain/Resolved IP Categories (Any). In the 'ACTION' section, the 'Allow' button is highlighted with a red box, and a callout bubble says 'Click Block'. Below the 'Allow' button is a 'Click Box' containing 'Block', 'Redirect Request', and 'Redirect Response' options. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Slide notes

Note that full logging of any matches is enabled by default.

Slide 208 - Slide 208

Click Save

Block

(Optional) Enter additional notes or information. The description cannot exceed 10,240 characters.

Slide notes

Click Save.

Slide 209 - Slide 209

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

Rule Order	Rule Name	Criteria	Action	Description
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block	
Default	Unknown DNS Traffic	Any	Allow	
Default	Default Firewall DNS Rule	Any	Allow	

A callout bubble with the text 'Click Activation' points to the activation icon (a pencil icon) next to the 'Block DNS Tunnels' rule.

Slide notes

Verify that the new DNS Control rule has been added to the list. With this rule enabled all DNS tunnel traffic will be blocked.

Additional DNS Control rules could be added above this rule to allow specific DNS tunnels if needed for productive reasons such as updates coming in for an Anti-virus application.

And **Activate** the changes.

Slide 210 - Slide 210

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy (highlighted in blue), Administration, Activation, and Search. The main area displays a table of firewall rules:

Rule Name	Criteria	Action	Description
Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block	
Unknown DNS Traffic	Any	Allow	
Default Firewall DNS Rule	Any	Allow	

A large blue button labeled "Click Box" is overlaid on the left side of the table. A callout bubble with the text "Click Activate" points to this button. At the bottom left, there's a copyright notice: "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.8 - Policies".

Slide notes

Slide 211 - Slide 211

The screenshot shows the 'DNS Control' section of the Zscaler Policy-Cloud Firewall interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Configure DNS Control Policy' with the sub-instruction 'You can define rules that control DNS requests and responses.' A search bar at the top right includes a magnifying glass icon.

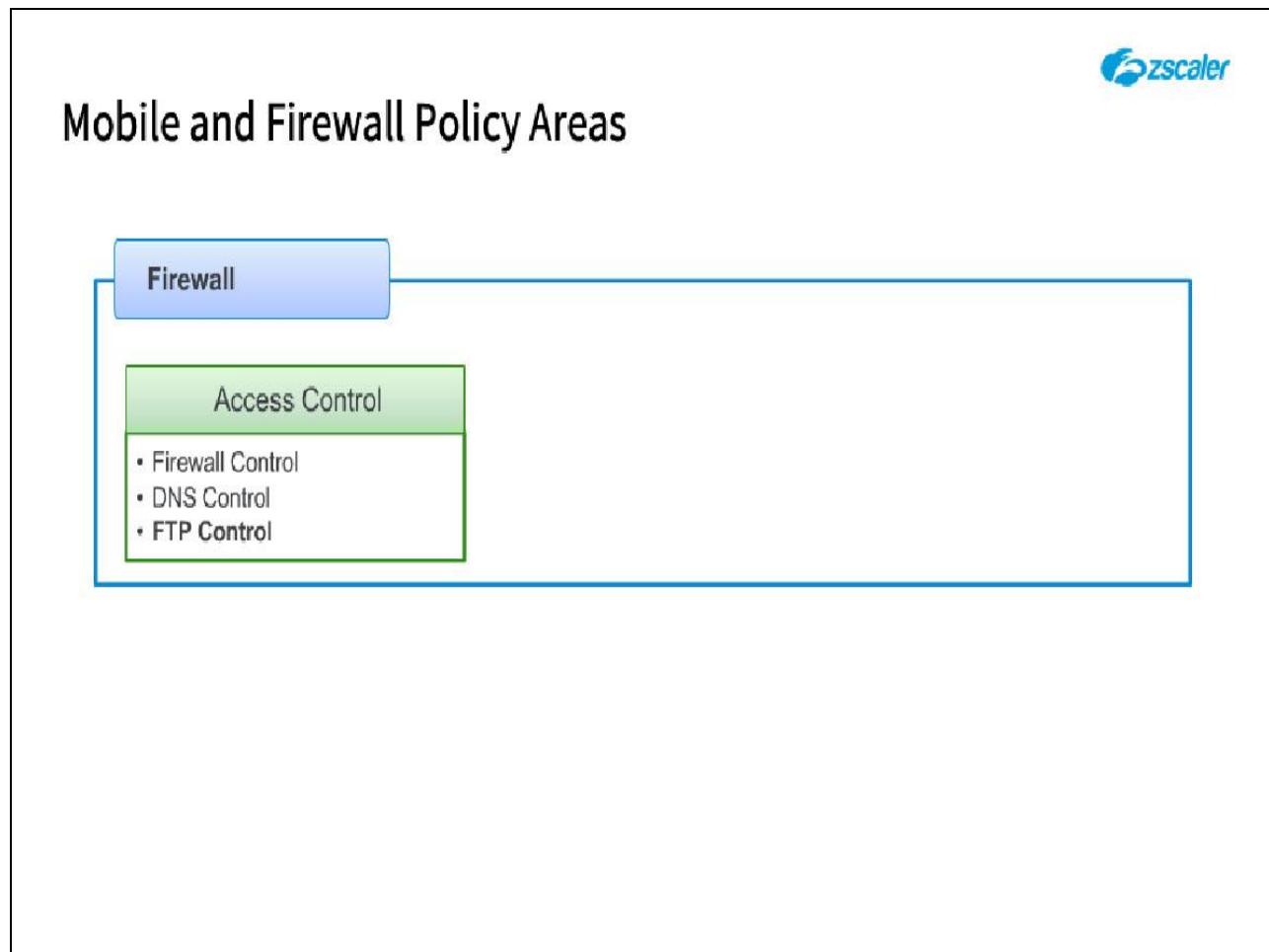
Add DNS Filtering Rule

Rule Order	Rule Name	Criteria	Action	Description	⋮
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled		
2	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block		
Default	Unknown DNS Traffic	Any	Allow		
Default	Default Firewall DNS Rule	Any	Allow		

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.8 | [Patents](#)

Slide notes

Slide 212 - Mobile and Firewall Policy Areas



Slide notes

Finally, let's look at the **FTP Control** policy options.

Slide 213 - Slide 213

The screenshot shows the Zscaler Cloud Firewall interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Click Box Policy (which is highlighted with a callout box labeled "Click Policy"), Administration, Activation, and Search. The main content area is titled "DNS Control" and "Configure DNS Control Policy". It displays a table of DNS filtering rules:

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
1	0	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
2	7	Block DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block	
		Unknown DNS Traffic	Any	Allow	
		Default Firewall DNS Rule	Any	Allow	

At the bottom of the page, there are copyright and help links.

Slide notes

Now, let's turn to our **Firewall** Policy ruleset. From the **Policy** menu

Slide 214 - Slide 214

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left sidebar, under the 'Policy' section, there is a 'Firewall Control' menu item with a sub-item 'FTP Control'. A callout box with the text 'Click FTP Control' points to the 'FTP Control' link. The main content area displays a table of rules for 'Data Loss Prevention' and 'Mobile' categories. The table has columns for 'Name', 'Criteria', 'Action', and 'Description'. A search bar is at the top right of the main content area.

Name	Criteria	Action	Description
Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Disabled	
DNS Tunnels	DNS APPLICATION GROUP All DNS Tunnels	Block	
Open DNS Traffic	Any	Allow	
Firewall DNS Rule	Any	Allow	

Slide notes

Click on **FTP Control**.

Slide 216 - Slide 216

The screenshot shows the Zscaler Policy-Cloud Firewall interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy (which is selected), Administration, Activation, and Search. The main content area is titled 'FTP Control' and contains the 'Configure FTP Control Policy' section. It states: 'By default, the Zscaler service does not allow users from a location to upload or download files from FTP sites. You can configure the FTP Control policy to allow access to specific sites.' Below this are two sections: 'FTP OVER HTTP TRAFFIC' and 'NATIVE FTP TRAFFIC'. In the 'FTP OVER HTTP TRAFFIC' section, there is a red-bordered checkbox labeled 'Allow FTP over HTTP Click Box'. In the 'NATIVE FTP TRAFFIC' section, there is another red-bordered checkbox labeled 'Allow Native Click Box'. A large gray callout box with a black border and white text 'Click to Allow FTP over HTTP' points to the first checkbox. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. A 'Help' button is located in the bottom right corner of the main window.

Slide notes

By default, the Zscaler service does not allow users from a location to upload or download files from FTP sites. You have the option here to enable FTP over HTTP.

Slide 217 - Slide 217

FTP Control

Configure FTP Control Policy

By default, the Zscaler service does not allow users from a location to upload or download files from FTP sites. You can configure the FTP Control policy to allow access to specific sites.

FTP OVER HTTP TRAFFIC

Allow FTP over HTTP

NATIVE FTP TRAFFIC

Allow Native FTP Click Box

Save Cancel

Help

Slide notes

You also have options for managing the specific sites available to your end users with the native FTP protocol.

Slide 218 - Slide 218

The screenshot shows the 'FTP Control' configuration page. Under 'FTP OVER HTTP TRAFFIC', 'Allow FTP over HTTP' is checked. Under 'NATIVE FTP TRAFFIC', 'Allow Native FTP' is checked and 'Allow Any URL Category' is unchecked. In the 'Allowed URLs' section, a red box highlights the list area which contains 'safemarch.com'. The interface includes a search bar, pagination (1-1 of 1), and buttons for 'Save' and 'Cancel'. The bottom of the screen shows copyright information and a help icon.

Slide notes

You may add specific URLs.

You also have options for managing the specific sites available to your end users with the native FTP protocol.

Slide 219 - Slide 219

The screenshot shows the 'FTP Control' configuration page. Under 'FTP OVER HTTP TRAFFIC', 'Allow FTP over HTTP' is checked. Under 'NATIVE FTP TRAFFIC', 'Allow Native FTP' is checked. The 'Allowed URL Categories' section is highlighted with a red box, containing a dropdown menu with options like 'Continuing Education/Colleges: Other E...' and 'Business/Educational'. The 'Allowed URLs' section shows a table with one item: 'safemarch.com'. At the bottom, there are 'Save' and 'Cancel' buttons.

Slide notes

or entire URL Categories that should be allowed. Alternatively, you can permit native FTP to any URL Category

Slide 220 - Slide 220

The screenshot shows the 'FTP Control' configuration page within the Zscaler Policy-Cloud Firewall Student Guide. The left sidebar includes icons for Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main content area has a header 'Configure FTP Control Policy' with a note about default settings. It contains two sections: 'FTP OVER HTTP TRAFFIC' (with 'Allow FTP over HTTP' checked) and 'NATIVE FTP TRAFFIC' (with 'Allow Native FTP' checked). Below these are sections for 'Allow Any URL Category' (unchecked) and 'Allowed URL Categories'. A modal dialog is open, titled 'Allowed URL Categories', showing a list of categories. The 'Unselected Items' list includes 'Adult Material' with sub-options like 'Adult Sex Education', 'Adult Themes', 'K-12 Sex Education', 'Lingerie/Bikini', and 'Nudity'. The 'Selected Items (2)' list contains 'Continuing Education/Colleges' and 'Other Education'. At the bottom of the dialog are 'Done', 'Cancel', and 'Clear Selection' buttons. The footer of the page includes copyright information (Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies) and a help icon.

Slide notes

Slide 221 - Slide 221

The screenshot shows the 'FTP Control' configuration page. It includes sections for 'FTP OVER HTTP TRAFFIC' (with 'Allow FTP over HTTP' checked) and 'NATIVE FTP TRAFFIC' (with 'Allow Native FTP' checked). A prominent feature is the 'Allow Any URL Category' checkbox, which is highlighted with a red border and a callout box containing the text 'Click to Allow Any URL Category'. Below this section, there's a list of allowed URLs, with 'safemarch.com' being the only entry. At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Slide notes

Alternatively, you can permit native FTP to any URL Category.

Slide 222 - Slide 222

The screenshot shows the 'FTP Control' configuration page. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy (which is selected), Administration, Activation, and Search. The main content area has a title 'Configure FTP Control Policy' with a note: 'By default, the Zscaler service does not allow users from a location to upload or download files from FTP sites. You can configure the FTP Control policy to allow access to specific sites.' It contains two sections: 'FTP OVER HTTP TRAFFIC' (with 'Allow FTP over HTTP' checked) and 'NATIVE FTP TRAFFIC' (with 'Allow Native FTP' and 'Allow Any URL Category' both checked). At the bottom right of the dialog is a 'Save' button. A large callout box with a grey border and a dark grey background contains the text 'Click Save' and points to the 'Save' button.

Slide notes

and to other specific URLs that you enter here. Having made any changes to the FTP Control policy, be sure to click **Save**.

Slide 227 - Slide 227

The screenshot shows the 'FTP Control' configuration page within the Zscaler Policy-Cloud Firewall interface. On the left, a vertical navigation bar lists several sections: Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main content area is titled 'FTP Control' and contains the following sections:

- Configure FTP Control Policy**: A note stating that by default, the Zscaler service does not allow users from a location to upload or download files from FTP sites. It allows configuring the FTP Control policy to allow access to specific sites.
- FTP OVER HTTP TRAFFIC**: Contains a single setting: 'Allow FTP over HTTP' with a checked checkbox.
- NATIVE FTP TRAFFIC**: Contains three settings:
 - 'Allow Native FTP' with a checked checkbox.
 - 'Allow Any URL Category' with a checked checkbox.

At the bottom of the configuration panel are 'Save' and 'Cancel' buttons. In the bottom right corner of the main window, there is a 'Help' icon.

Slide notes

and **Activate** your changes.

Slide 228 - Slide 228

The screenshot shows the Zscaler Policy-Cloud Firewall Student Guide interface. The left sidebar contains navigation links: Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main content area is titled "FTP Control" and describes its function: "Allow users from a location to upload or download files from FTP sites. You can configure the FTP Control policy to allow access to specific sites." It shows a list of currently editing sites: "www.thinkingunlocked.com". Below this is a section for "QUEUED ACTIVATIONS (0)" with a note "None". A "Force Activate" checkbox is present, and a large blue "Activate" button is highlighted. On the right side, there is a "Recommended Policy" section with a "View" button. At the bottom of the page, there is a footer with copyright information: "Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 5.7 | Policies" and a timestamp: "Weblog Time: 1/13/2020 2:26:00 PM | Last Updated: 1/13/2020 2:26:30 PM". A "Help" button is located in the bottom right corner.

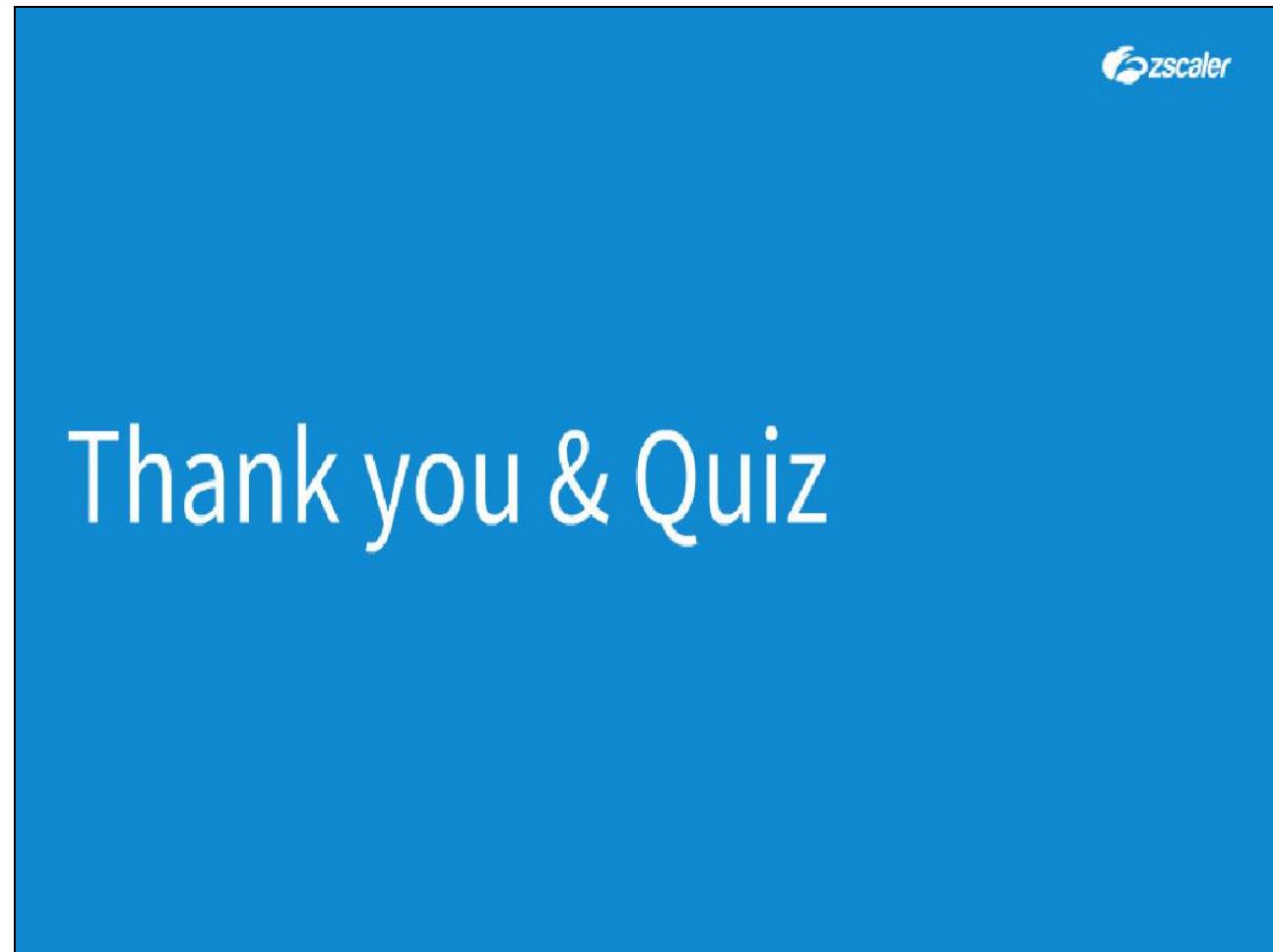
Slide notes

Slide 229 - Slide 229

The screenshot shows the 'FTP Control' configuration page within the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy (selected), Administration, Activation, and Search. The main content area has a header 'Activation Completed!' and a sub-header 'Configure FTP Control Policy'. It states: 'By default, the Zscaler service does not allow users from a location to upload or download files from FTP sites. You can configure the FTP Control policy to allow access to specific sites.' The 'FTP OVER HTTP TRAFFIC' section contains the 'Allow FTP over HTTP' checkbox, which is checked. The 'NATIVE FTP TRAFFIC' section contains two checkboxes: 'Allow Native FTP' (checked) and 'Allow Any URL Category' (checked). A 'Recommended Policy' button is located in the top right corner of this section. At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon in the bottom right corner.

Slide notes

Slide 232 - 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.