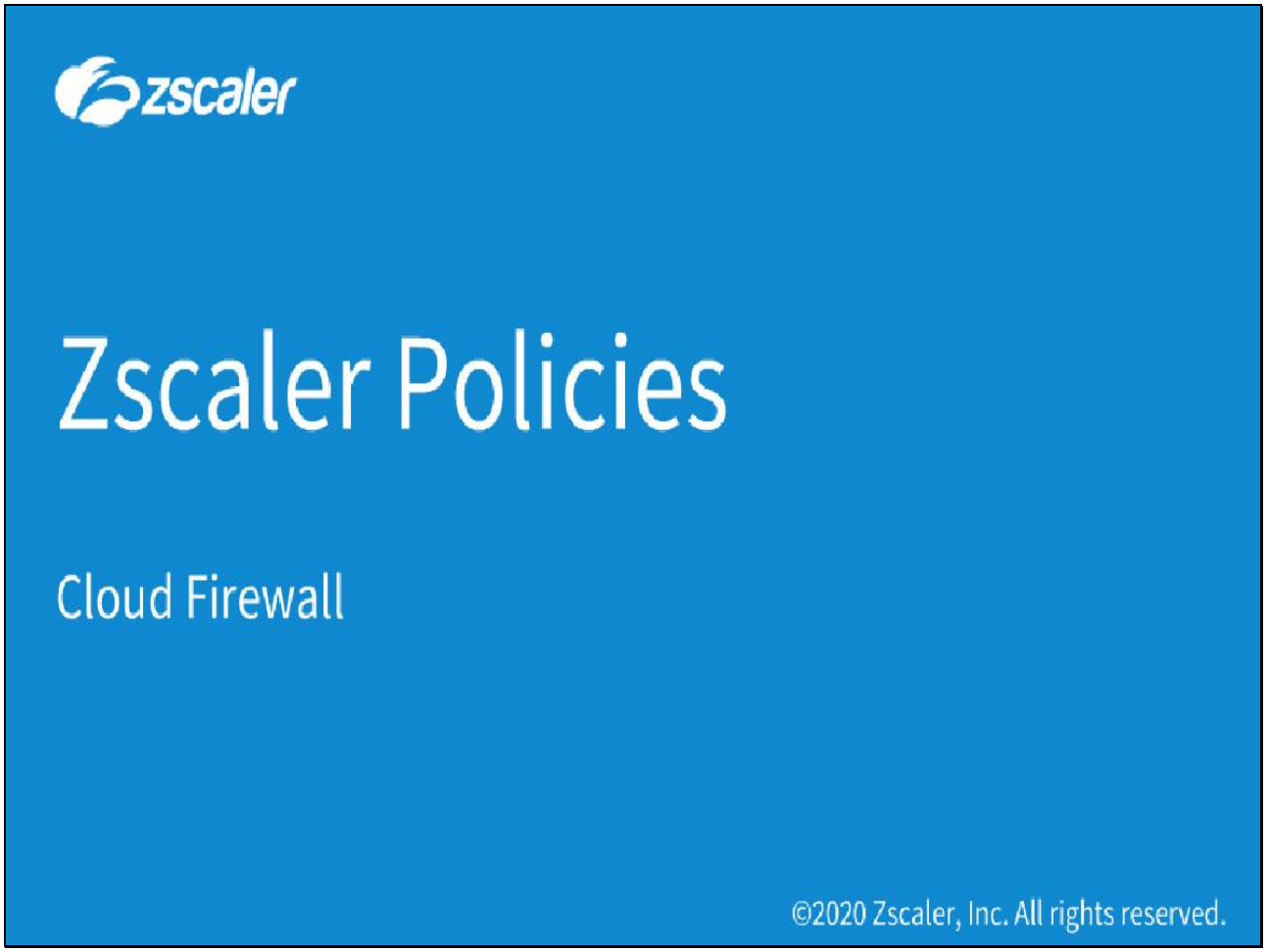
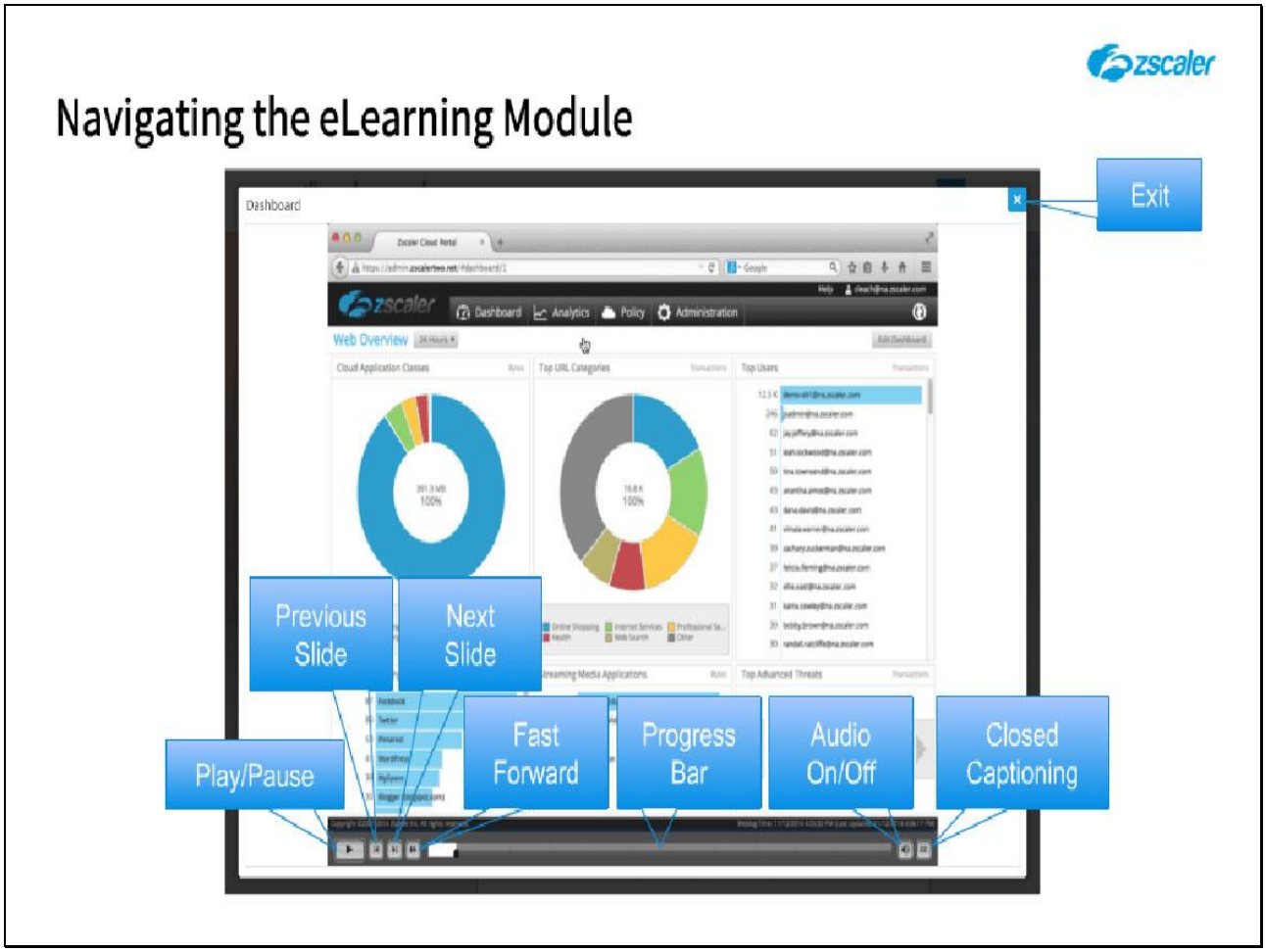
Slide 1 - Zscaler Policies



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

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

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.

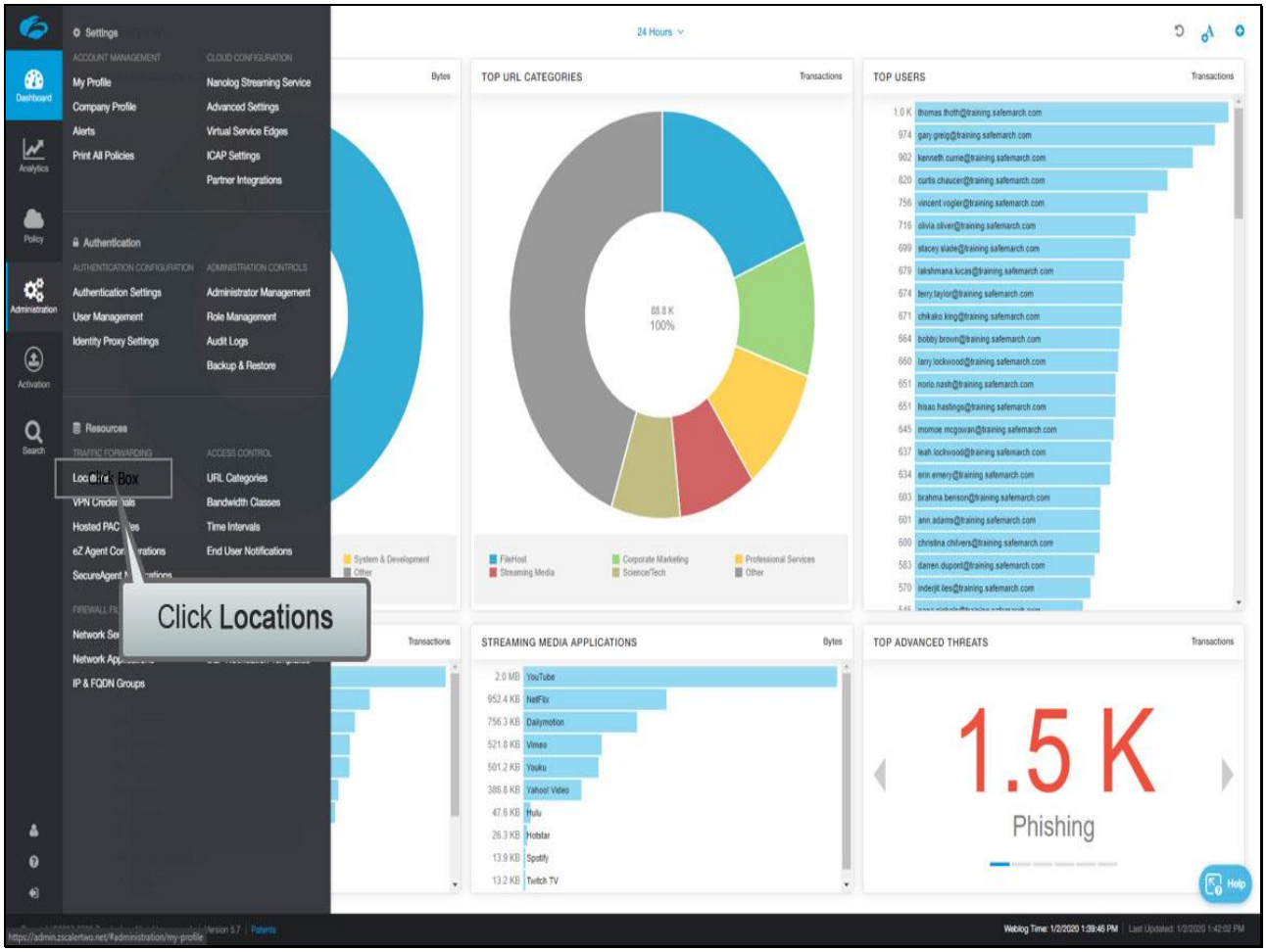
This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler admin portal UI. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

Slide 7 - Slide 7

Slide notes

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

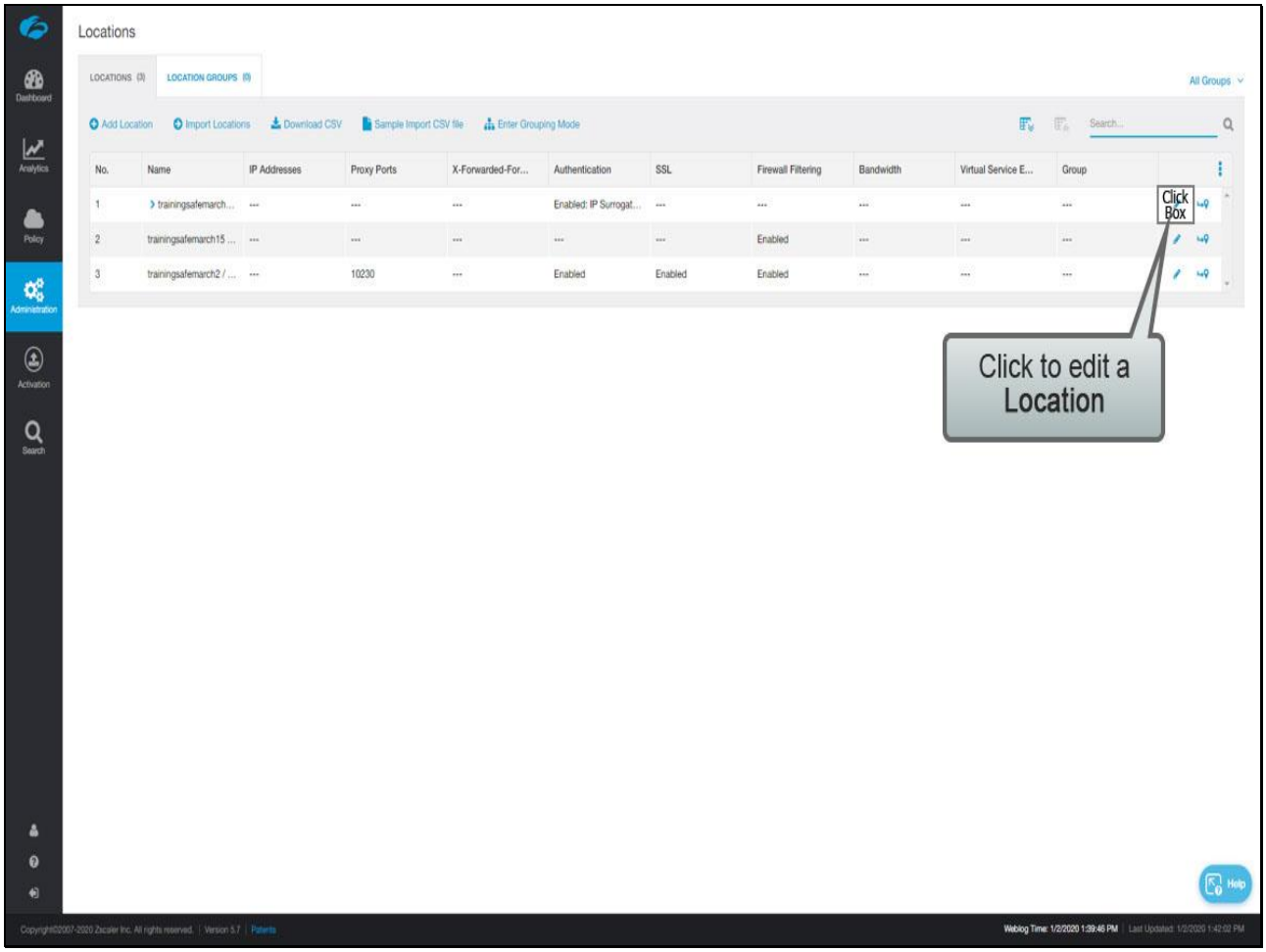
Slide 8 - Slide 8



Slide notes

Click **Locations**.

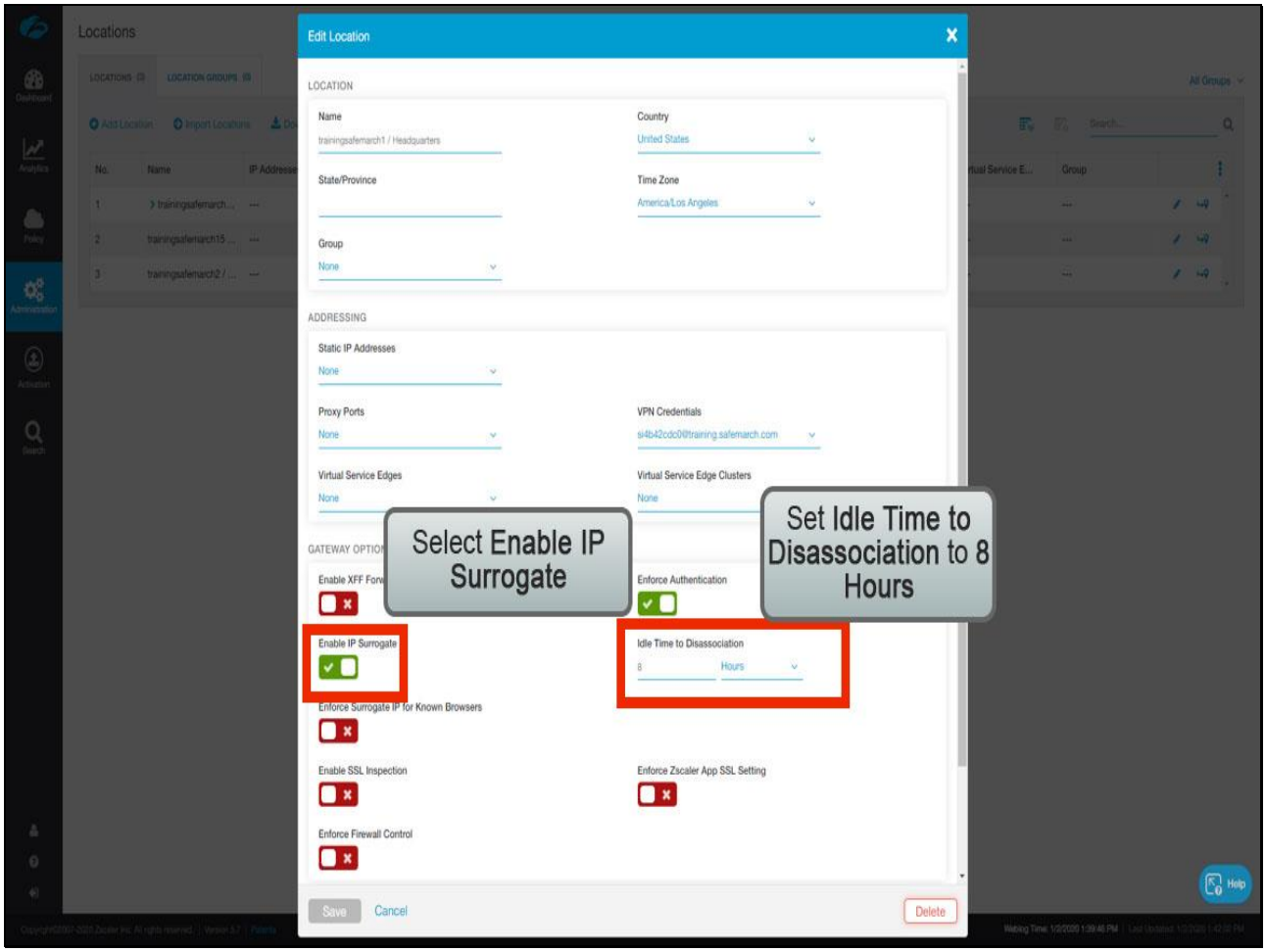
Slide 10 - Slide 10



Slide notes

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

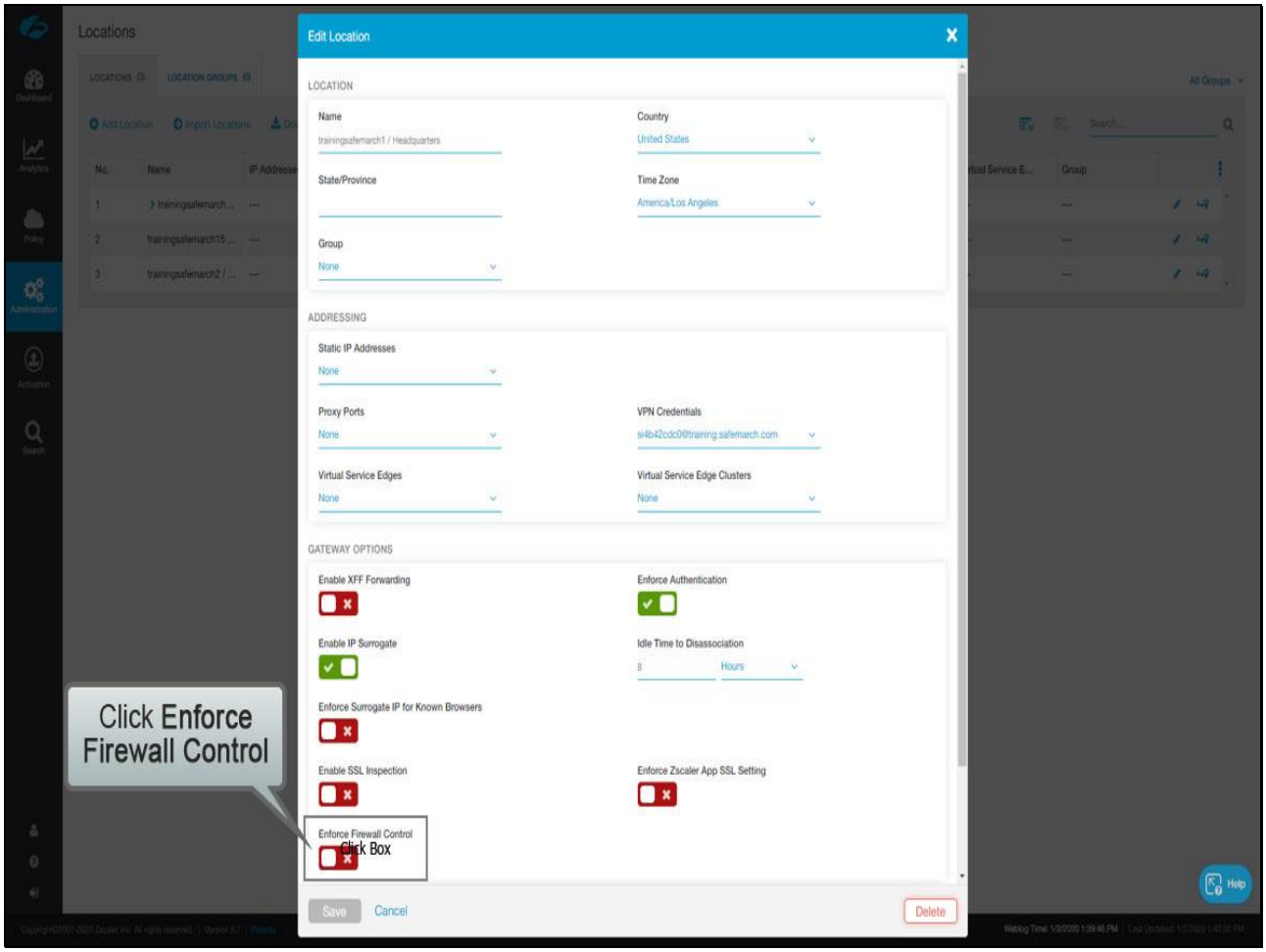
Slide 11 - Slide 11



Slide notes

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

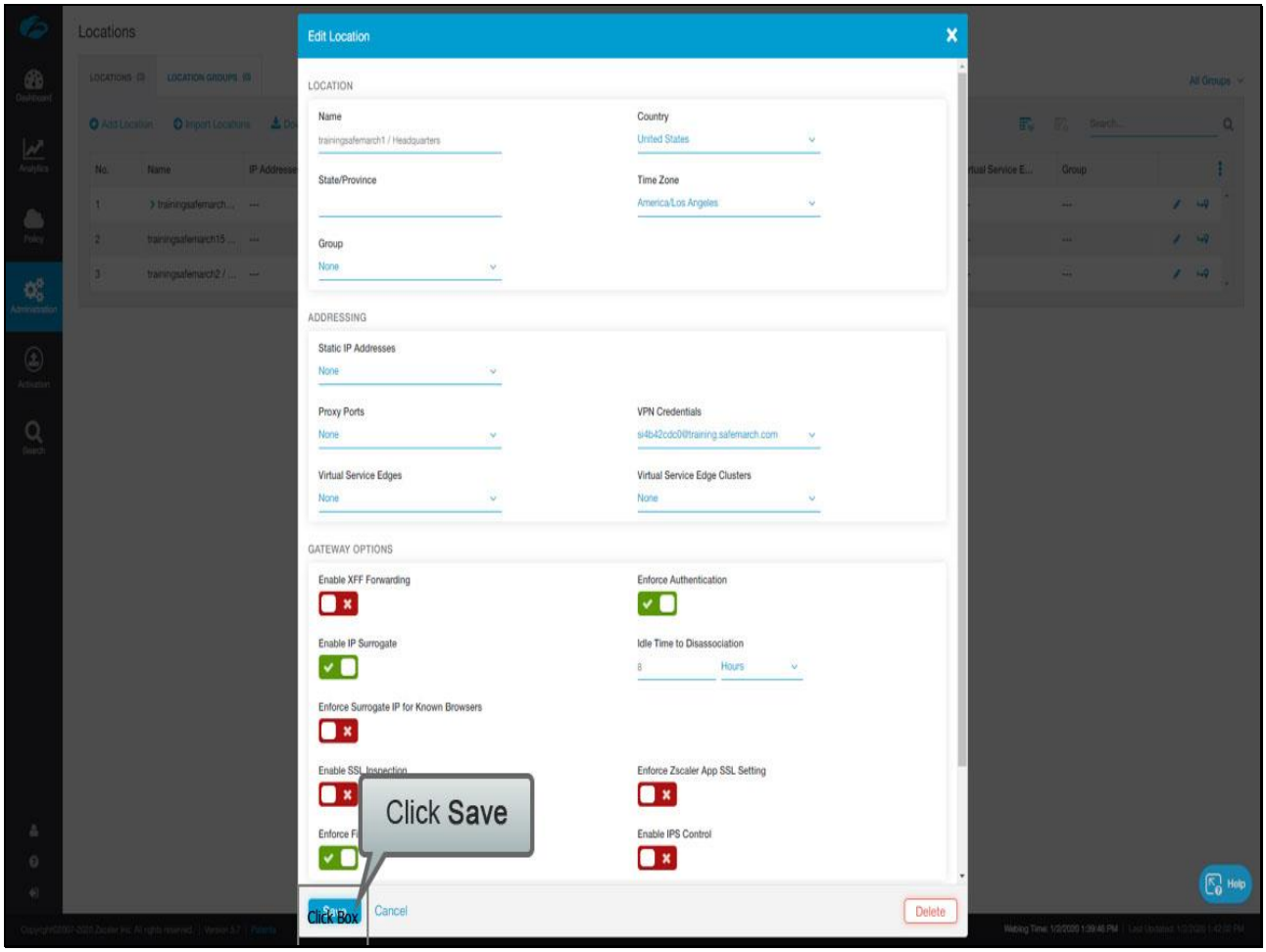
Slide 12 - Slide 12



Slide notes

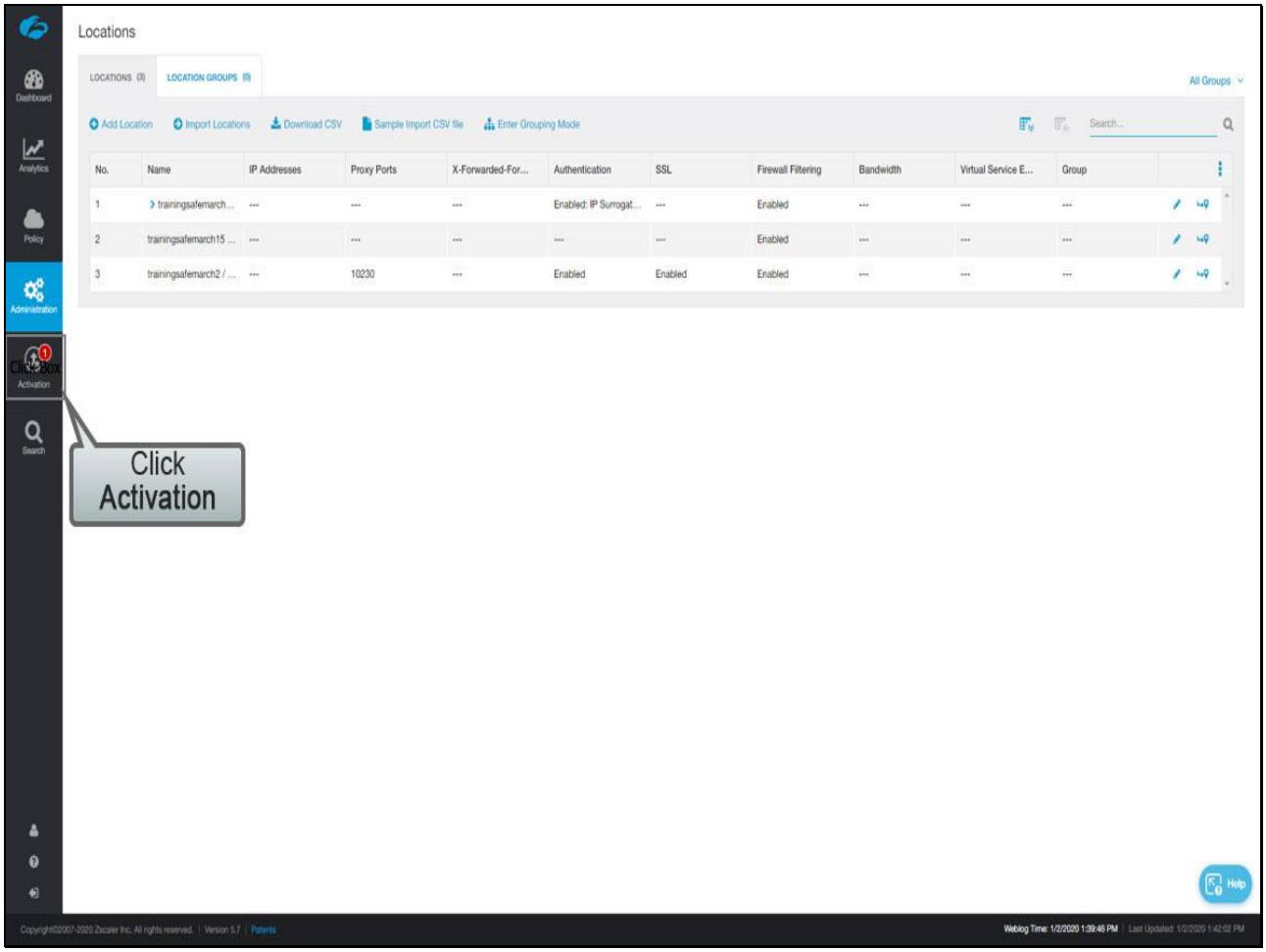
Enable the **Enforce Firewall Control** option and click **Save**.

Slide 13 - Slide 13



Slide notes

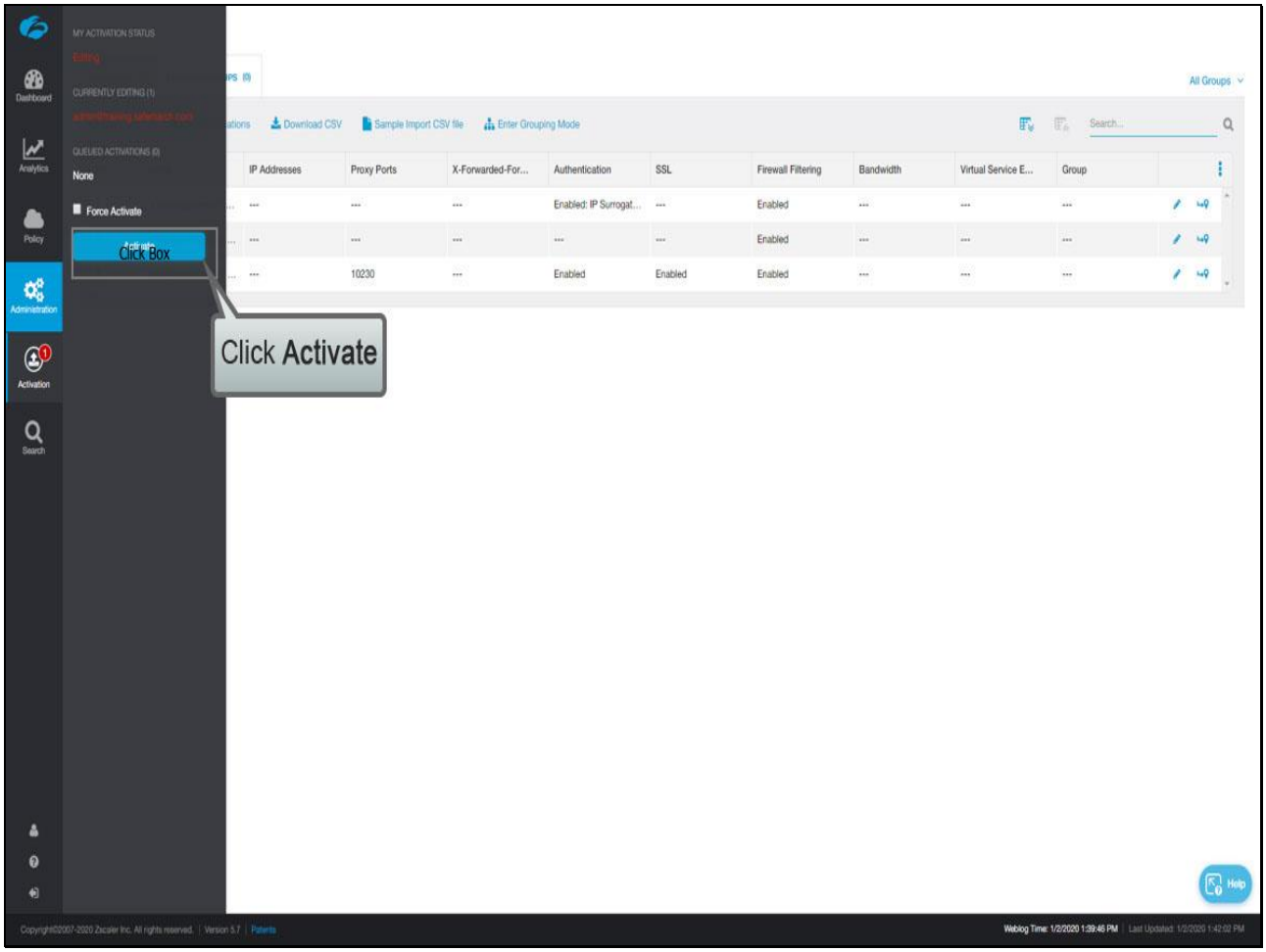
Slide 19 - Slide 19



Slide notes

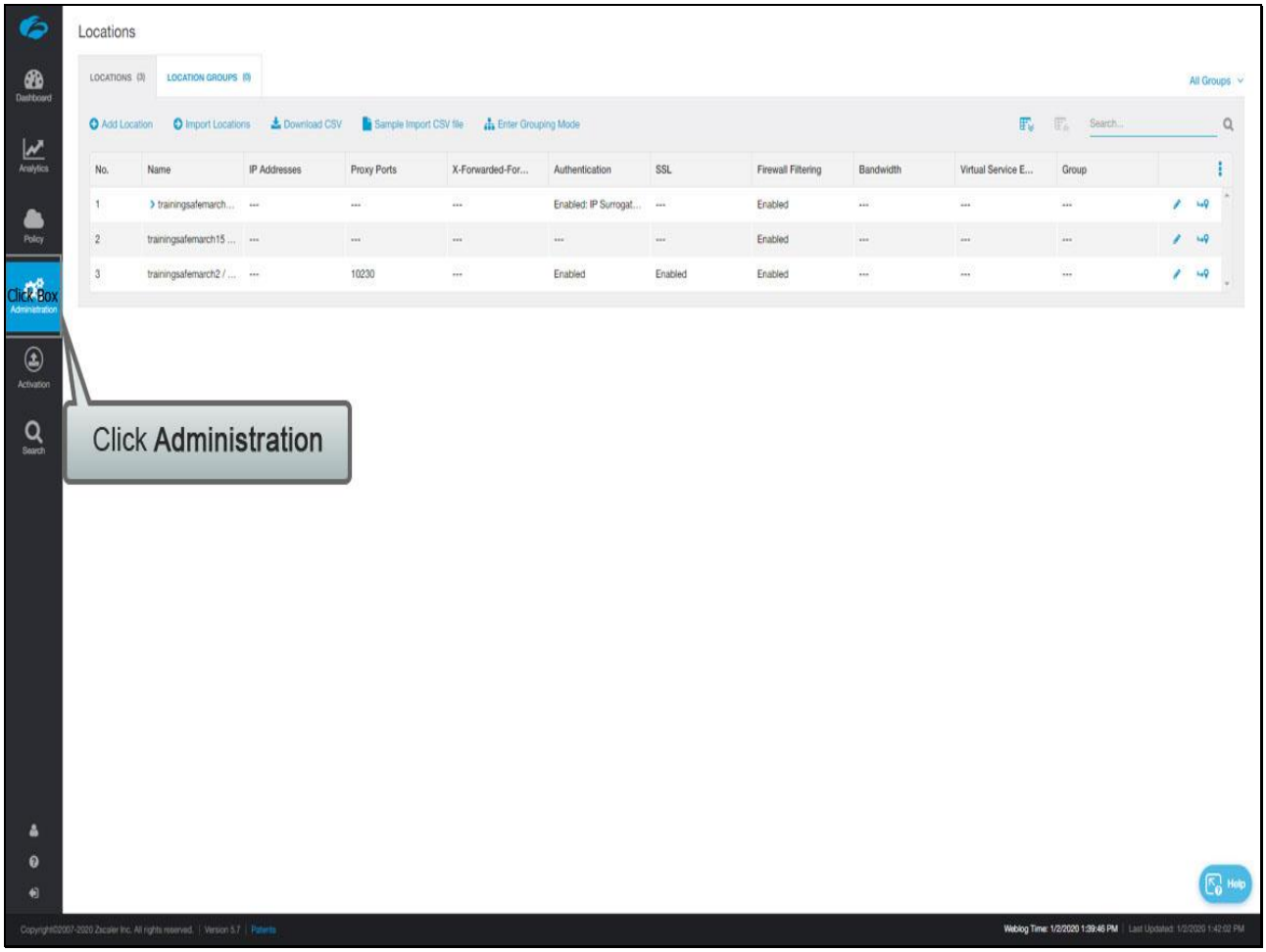
Then **Activate** your changes.

Slide 20 - Slide 20



Slide notes

Slide 26 - Slide 26



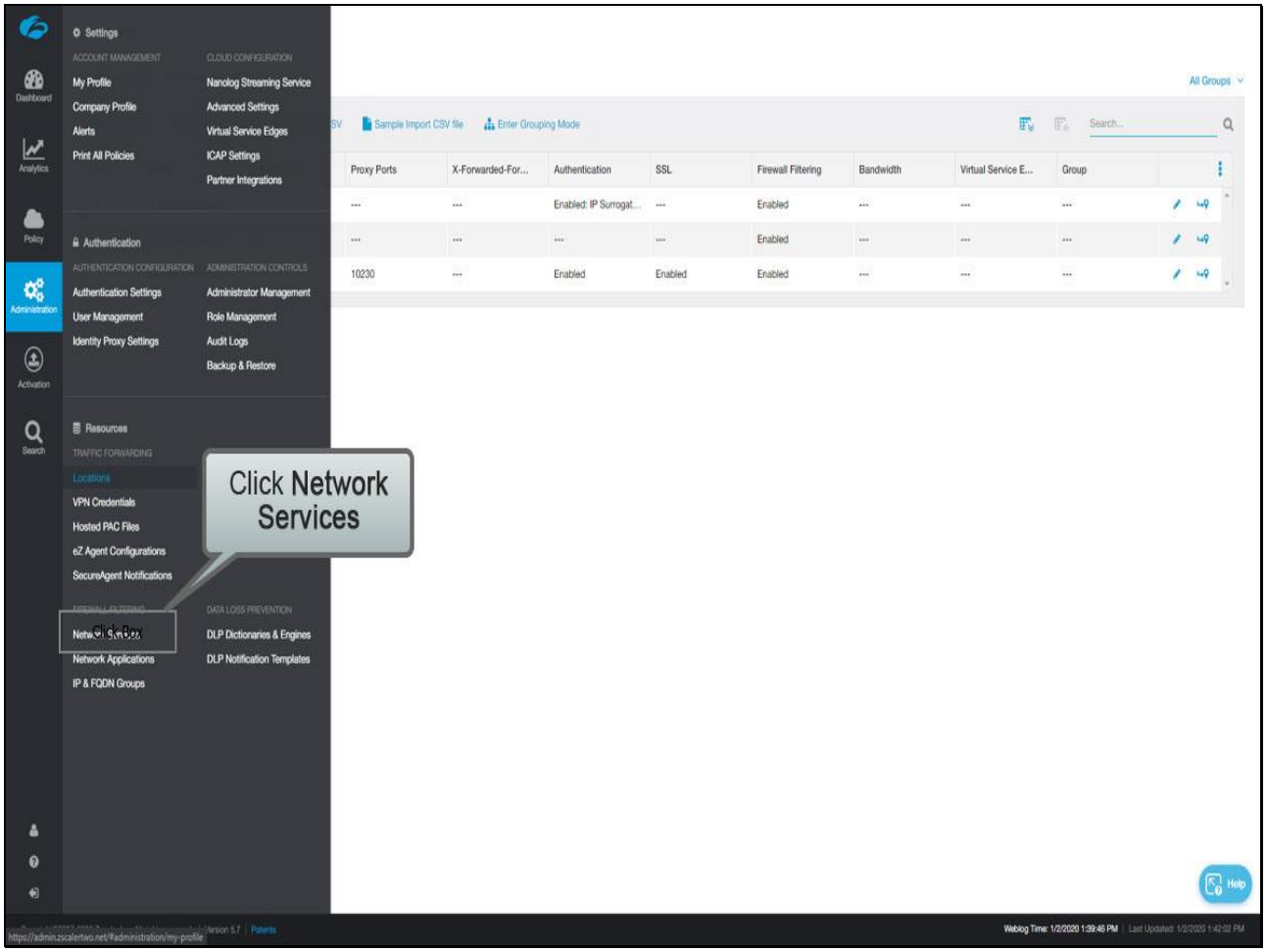
Slide notes

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

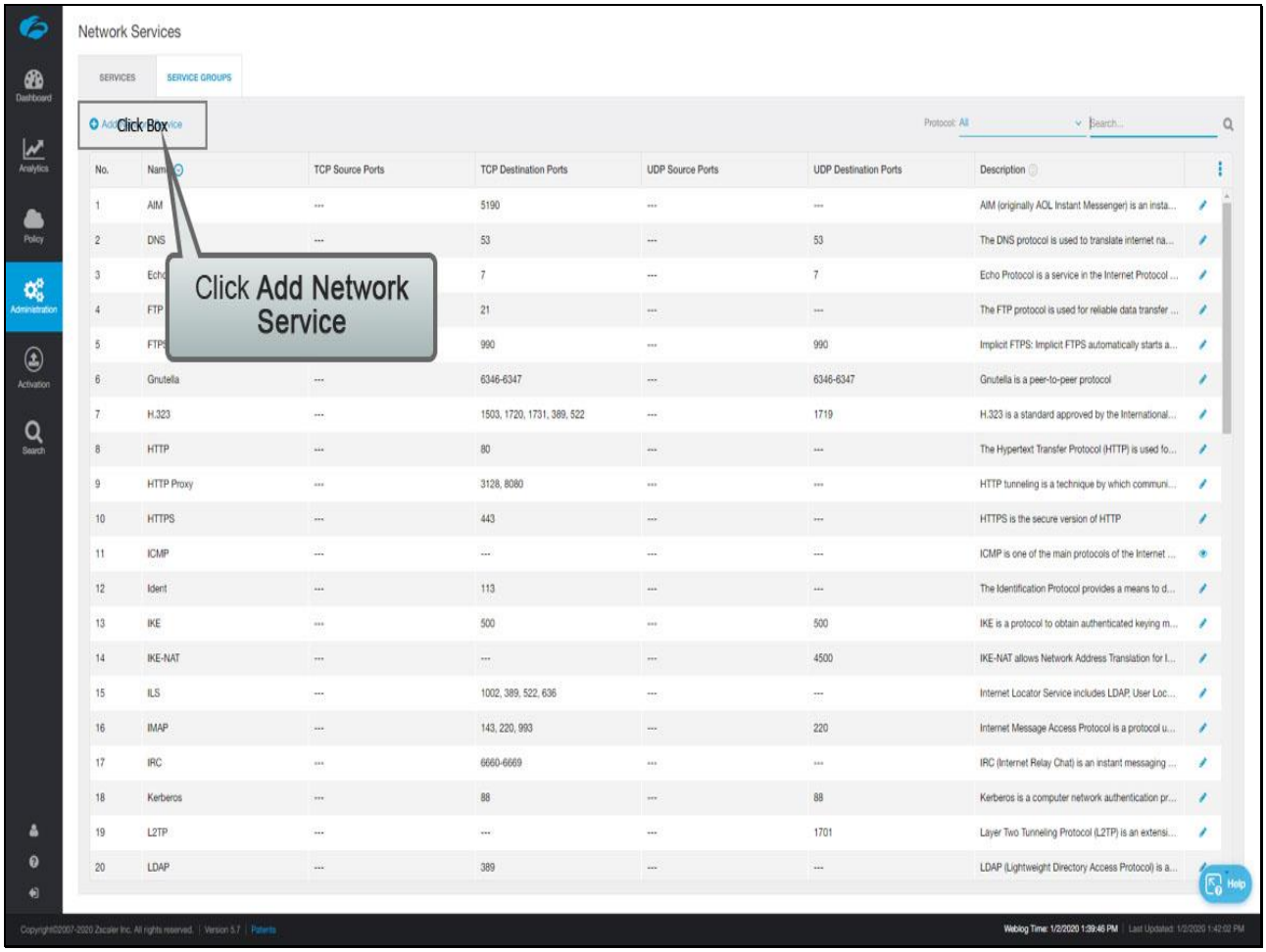
Slide 27 - Slide 27



Slide notes

click **Network Services**.

Slide 29 - Slide 29

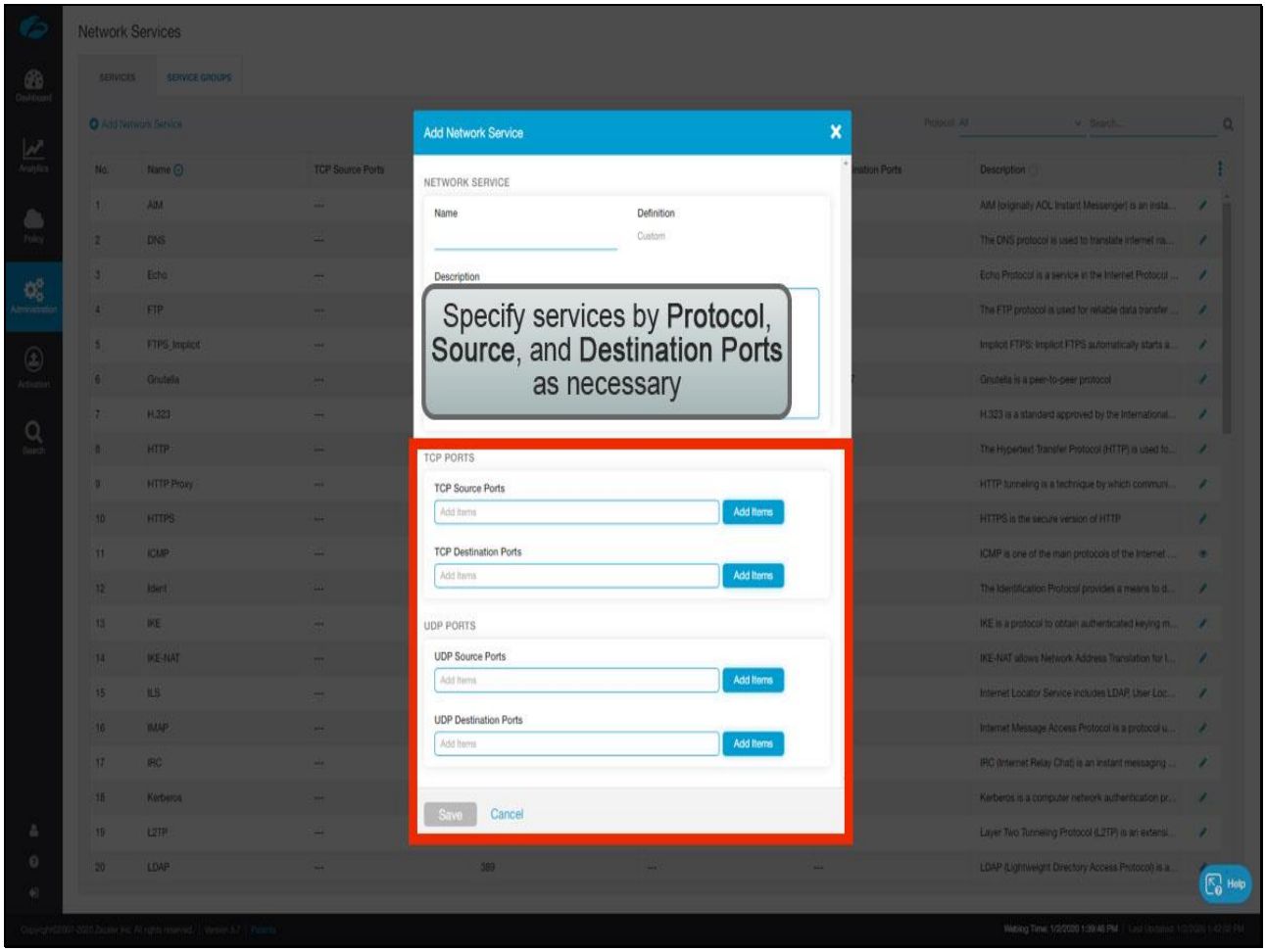


Slide notes

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

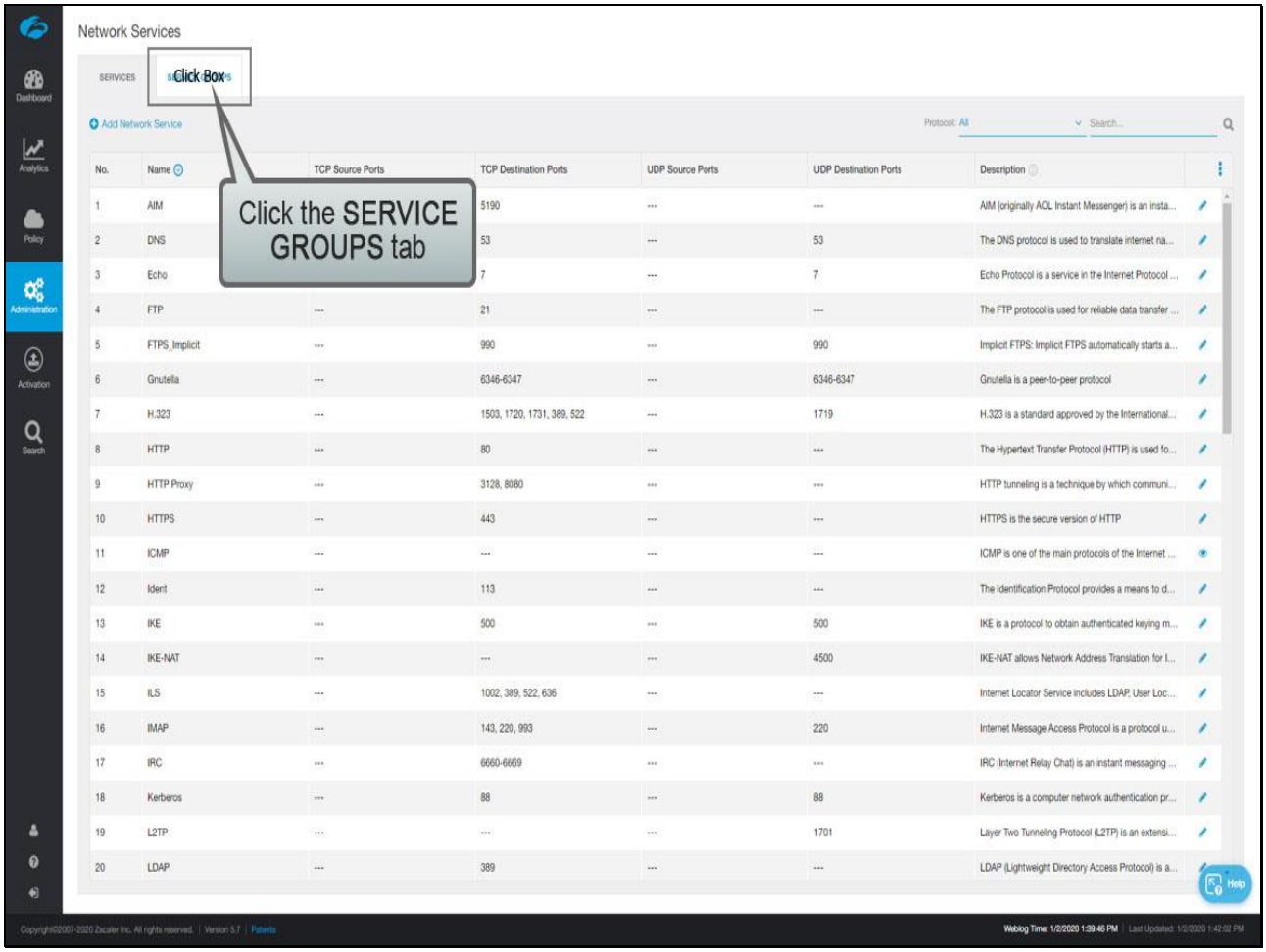


Slide notes

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.

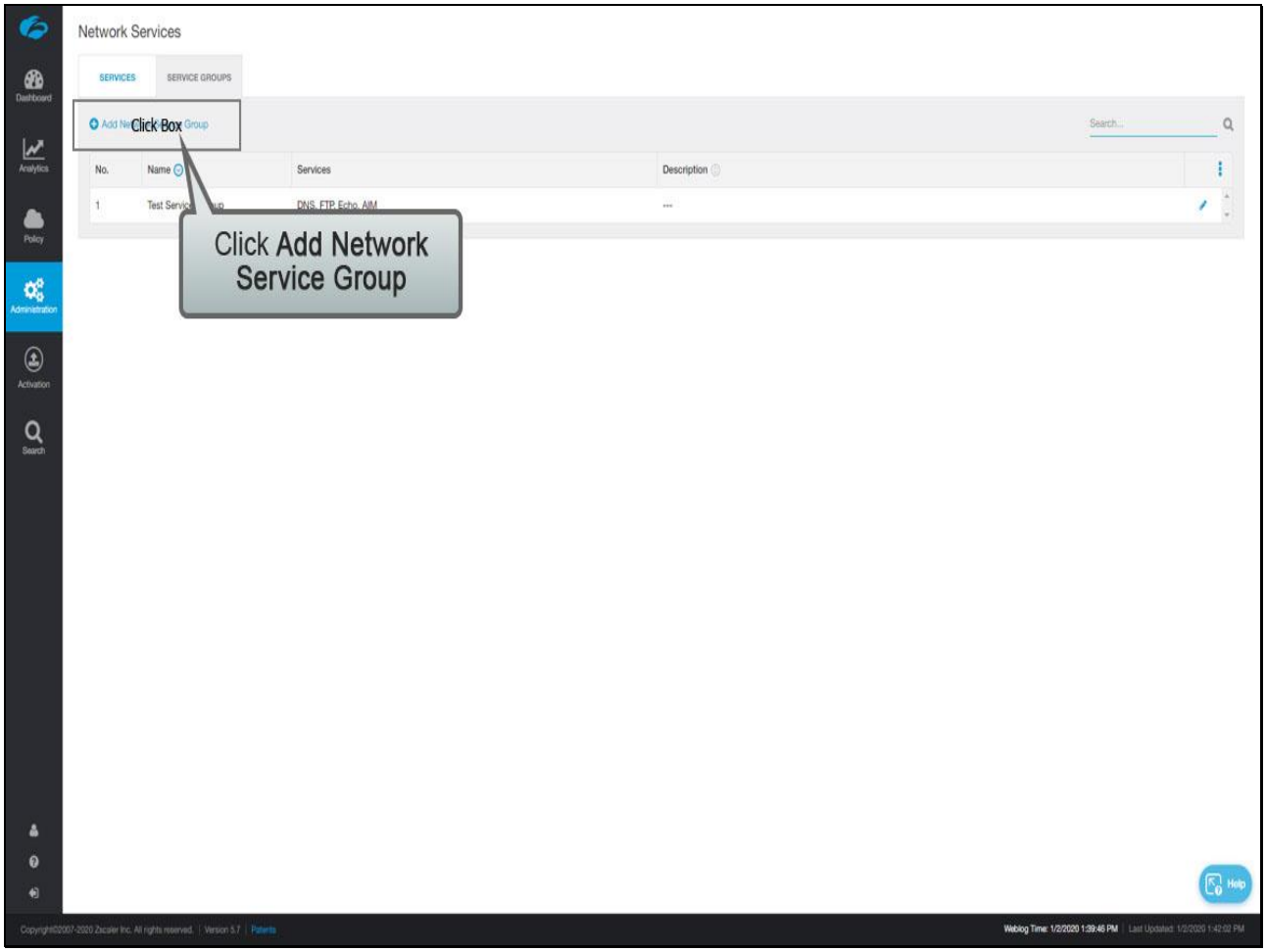
Slide 32 - Slide 32



Slide notes

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

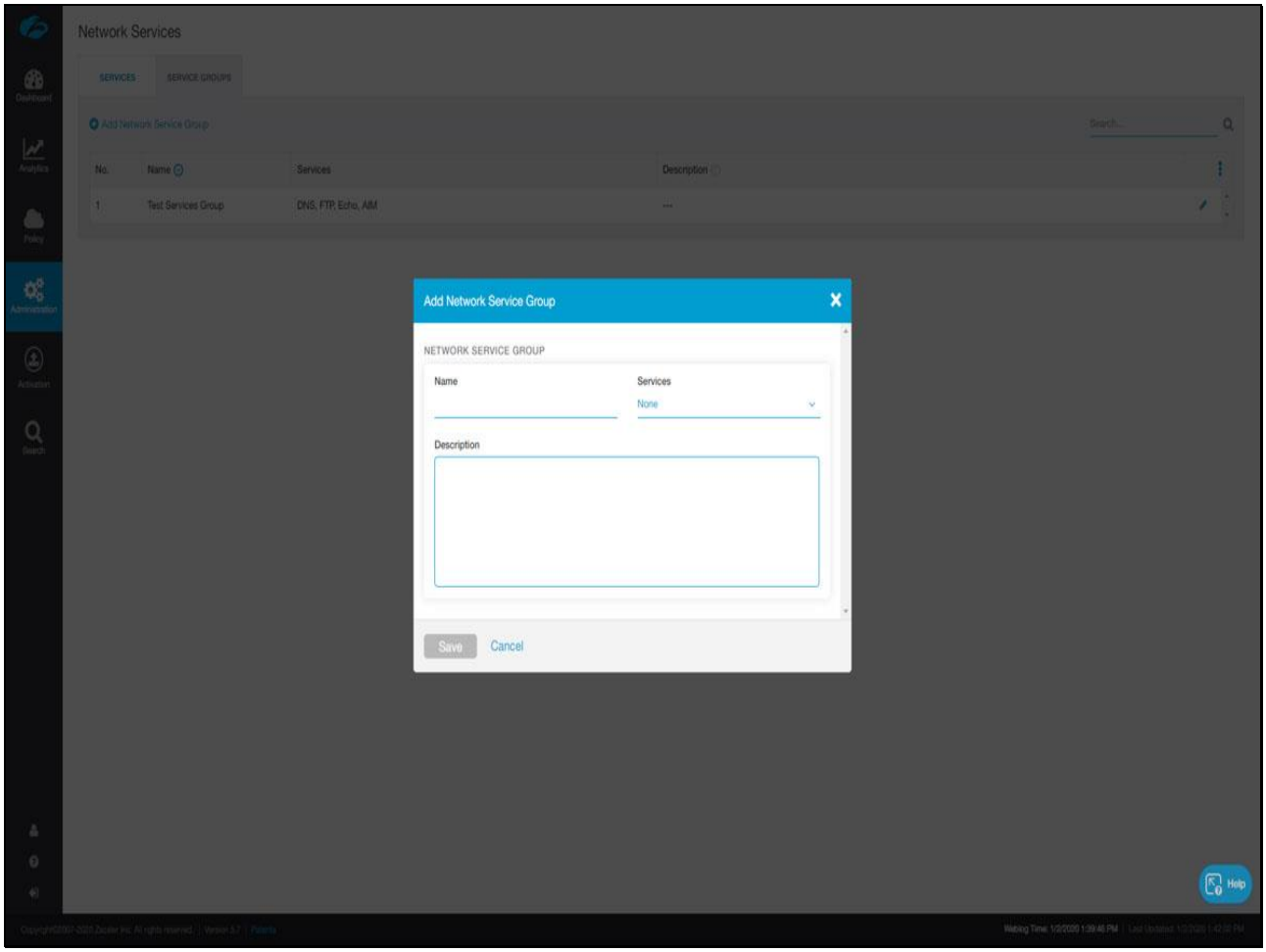
Slide 33 - Slide 33



Slide notes

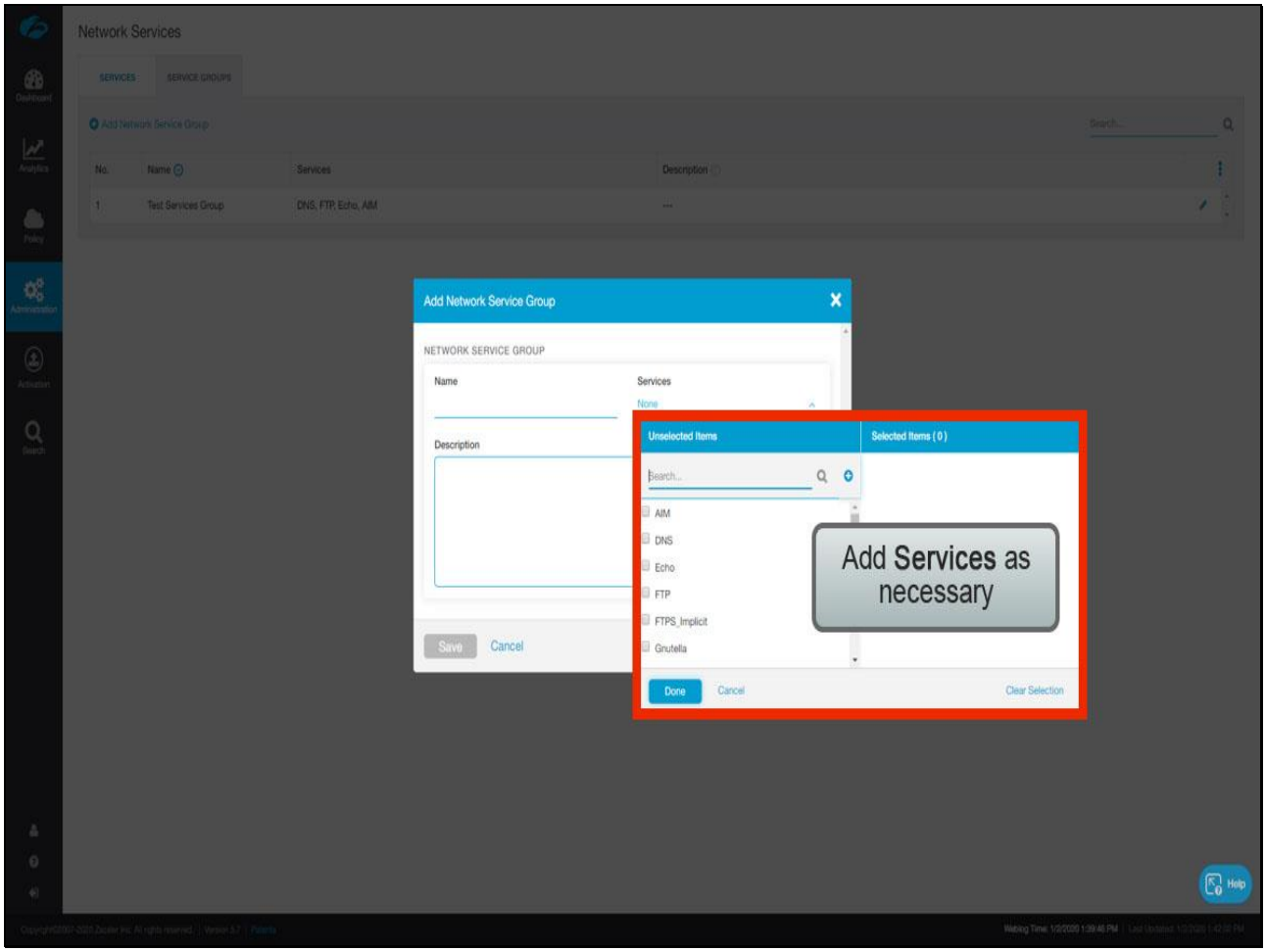
This is simply a way to apply rules to common sets of services. To add a network service group, click the **Add Network Service Group** link.

Slide 34 - Slide 34



Slide notes

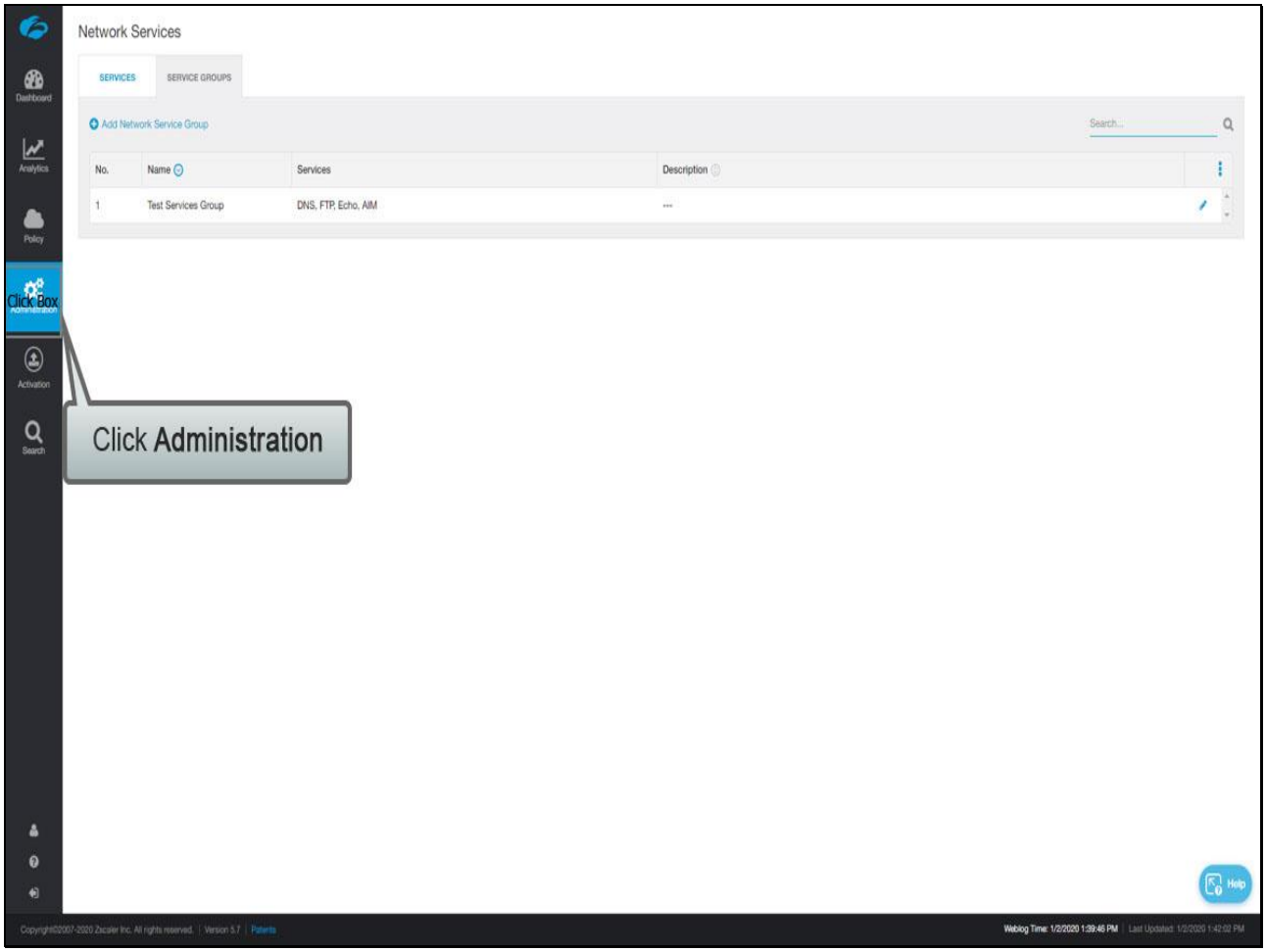
Slide 35 - Slide 35



Slide notes

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

Slide 37 - Slide 37

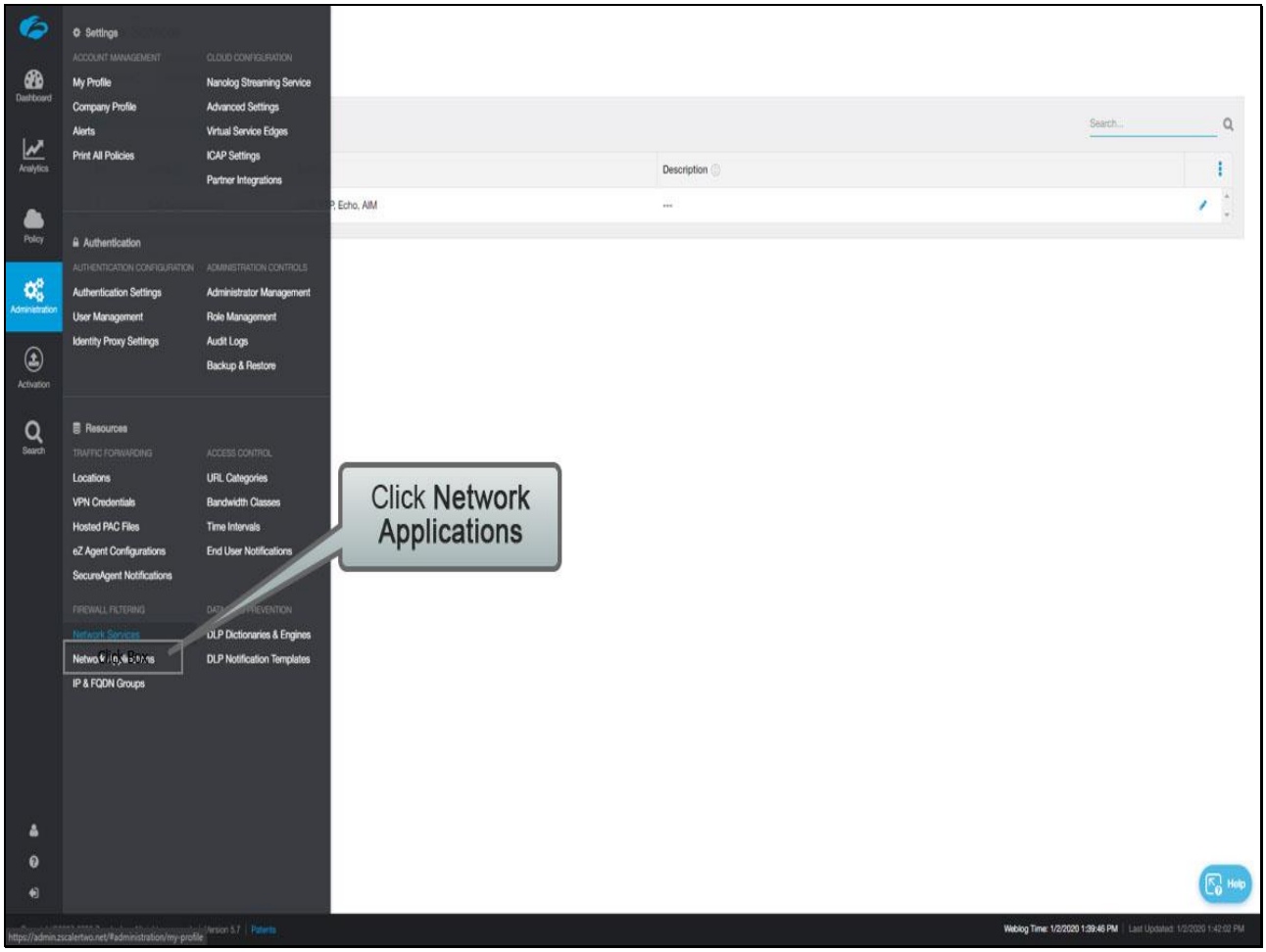


Slide notes

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.

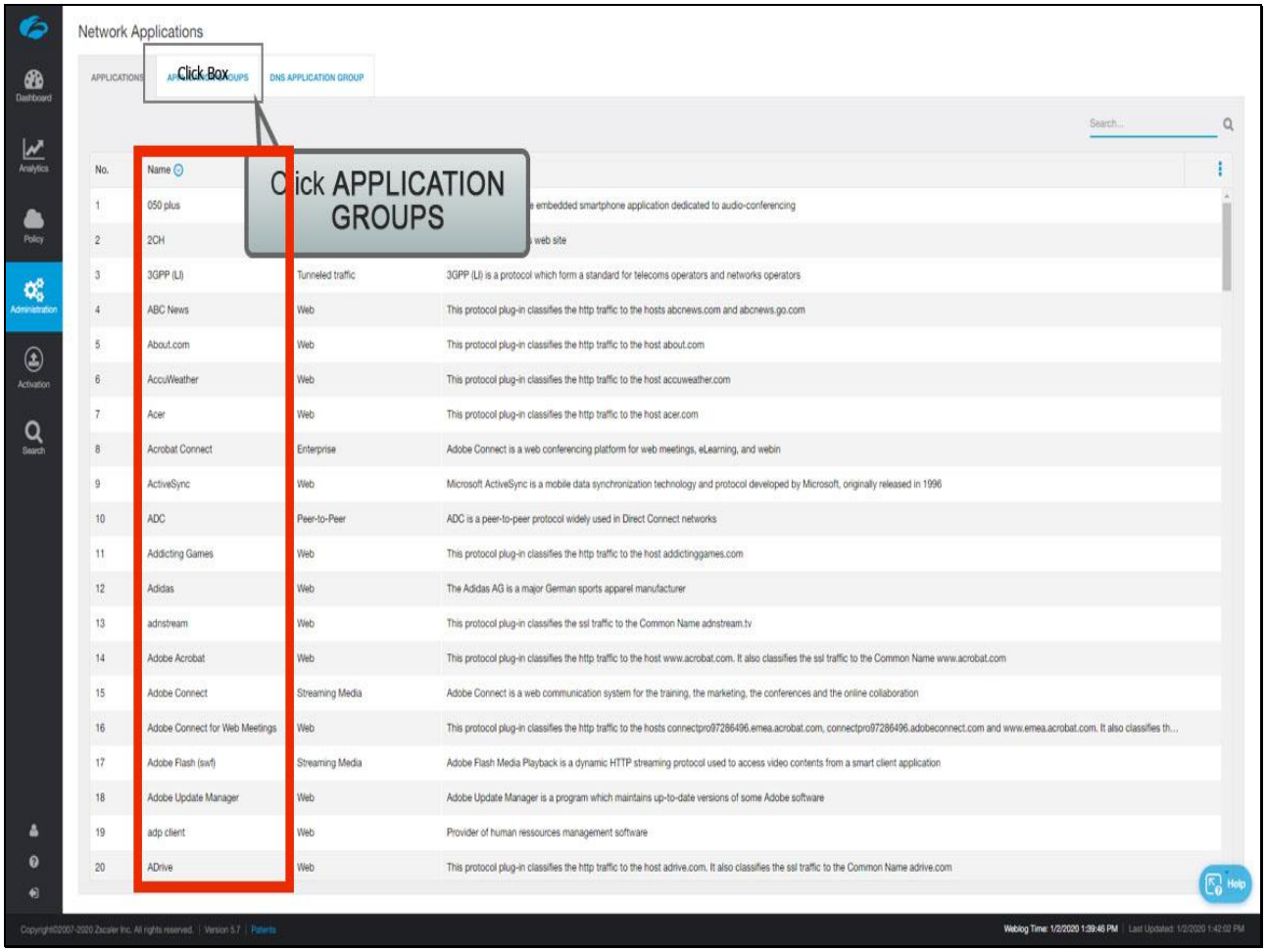
Now, let's click on **Network Applications**, as this is the meat of the Zscaler Cloud Firewall implementation.

Slide 38 - Slide 38



Slide notes

Slide 39 - Slide 39



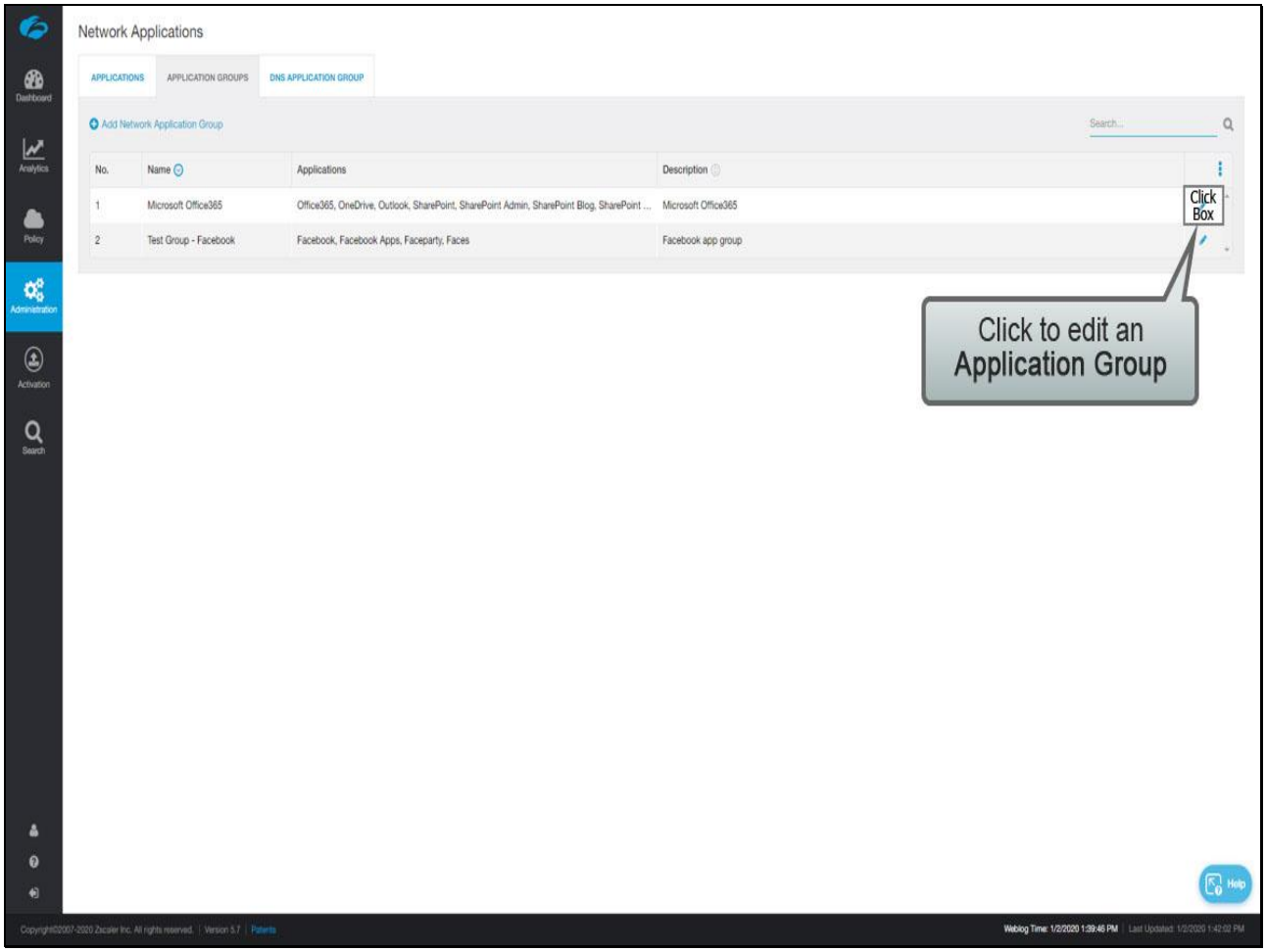
Slide notes

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.

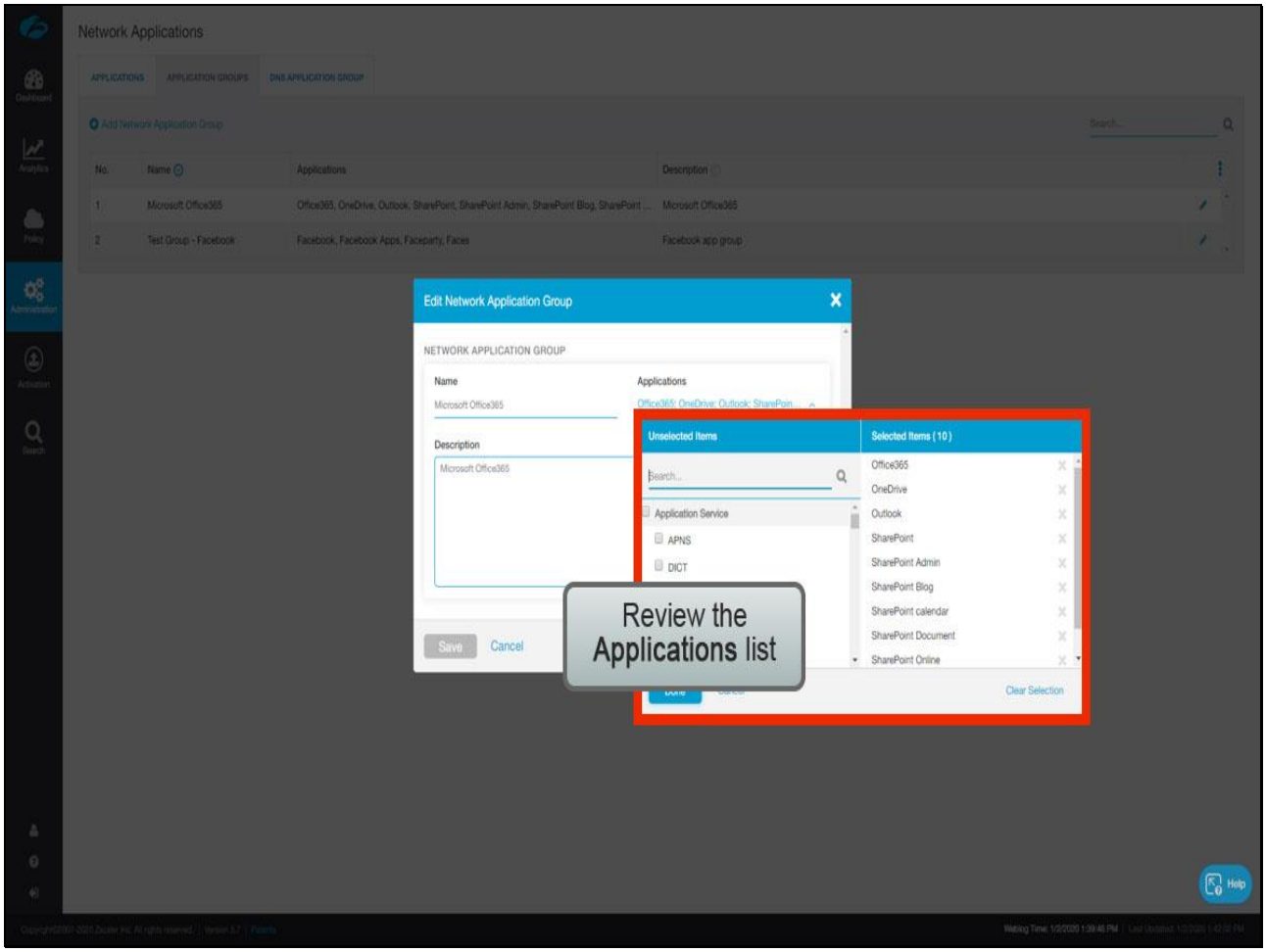
Slide 40 - Slide 40



Slide notes

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

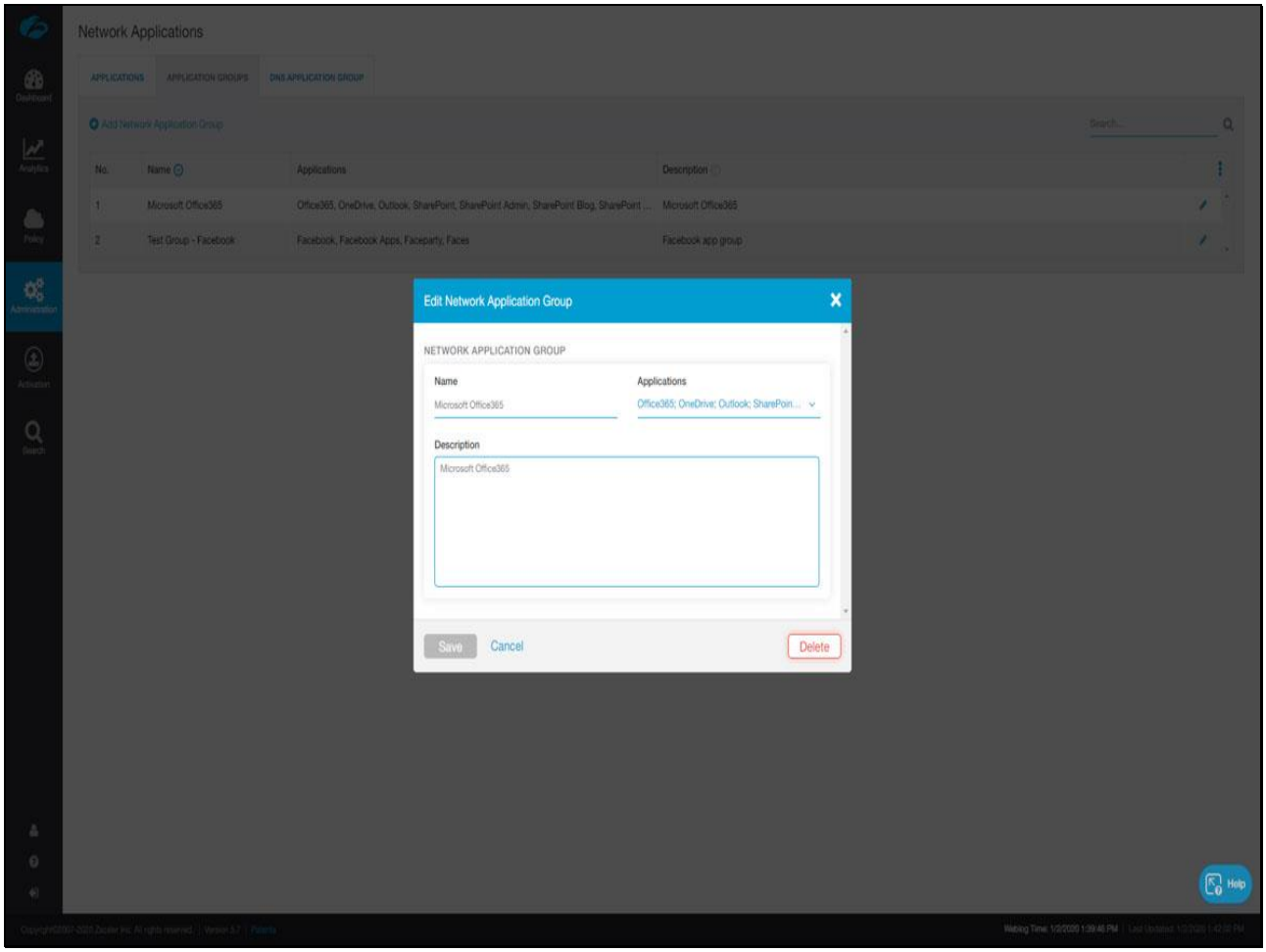
Slide 42 - Slide 42



Slide notes

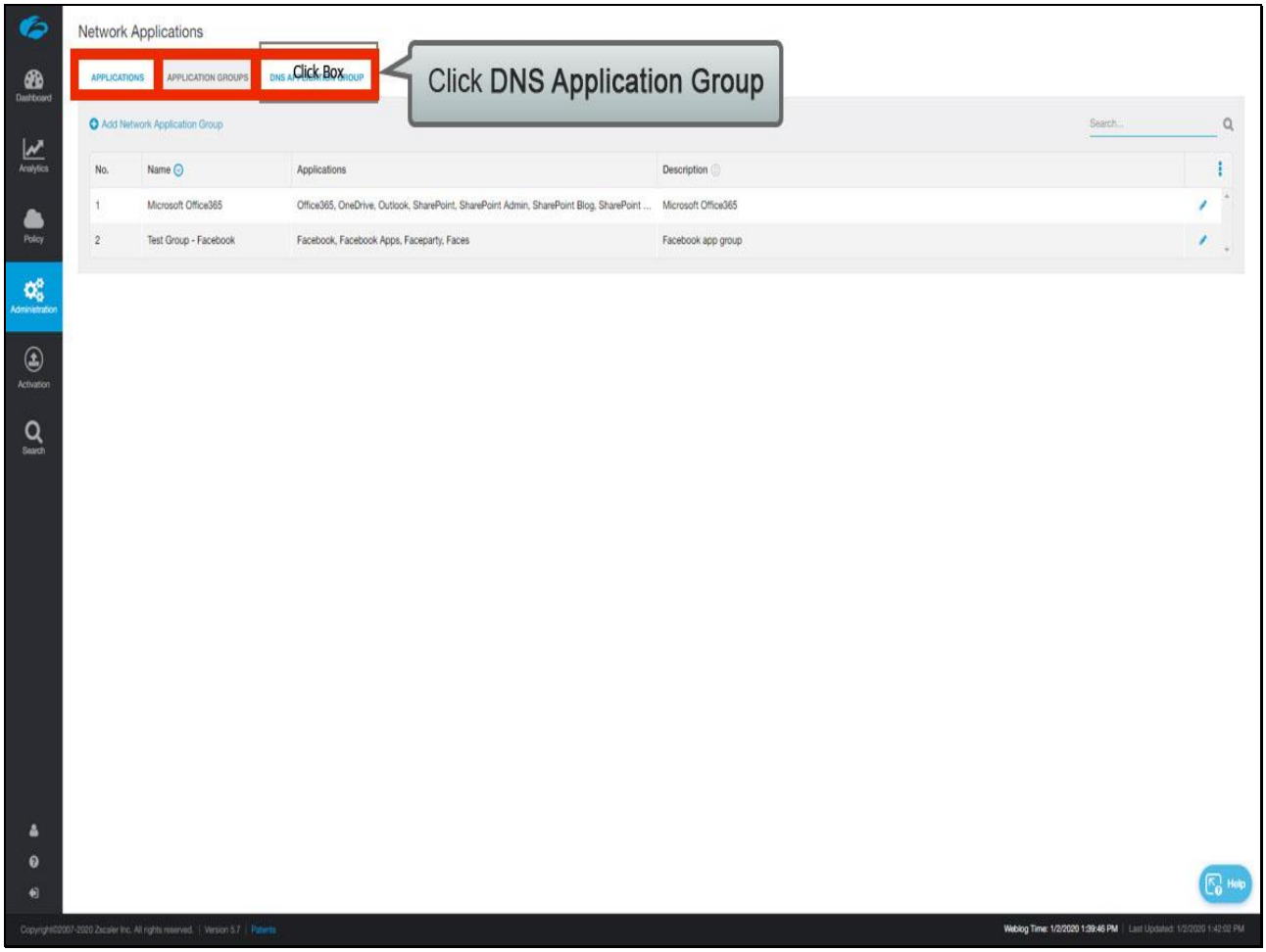
which contains all of the Office365 applications.

Slide 43 - Slide 43



Slide notes

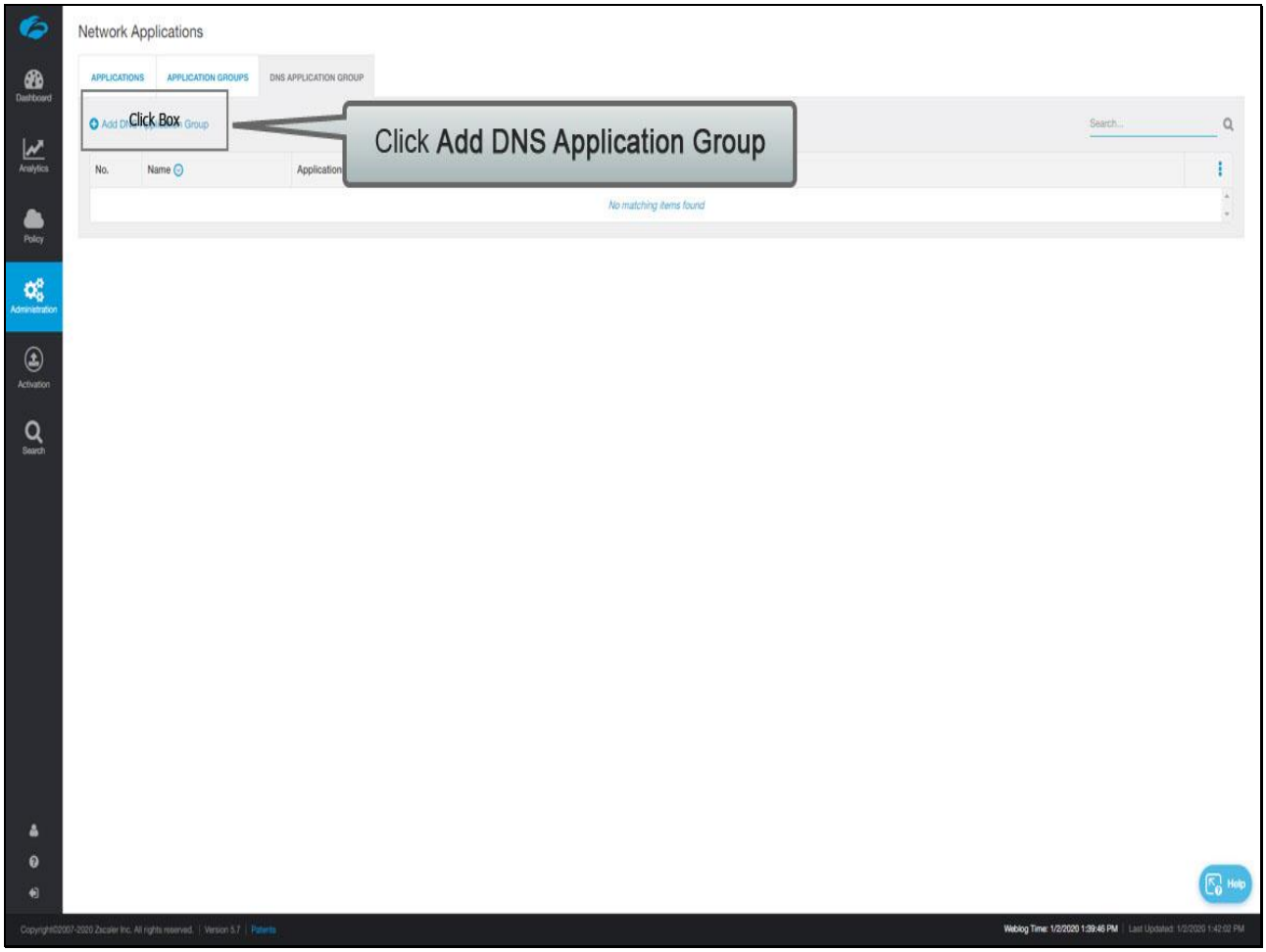
Slide 44 - Slide 44



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.

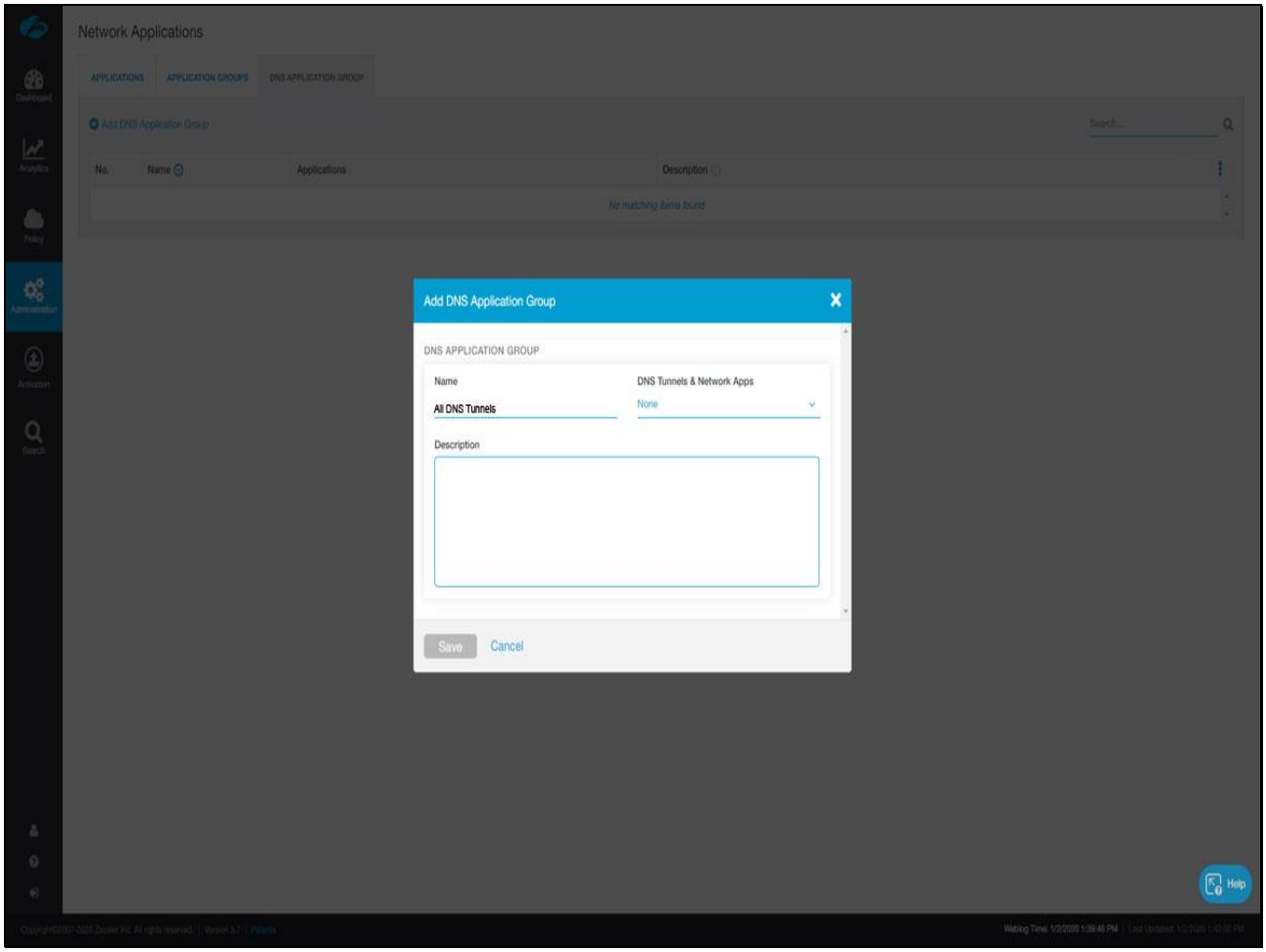
Slide 45 - Slide 45



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**.

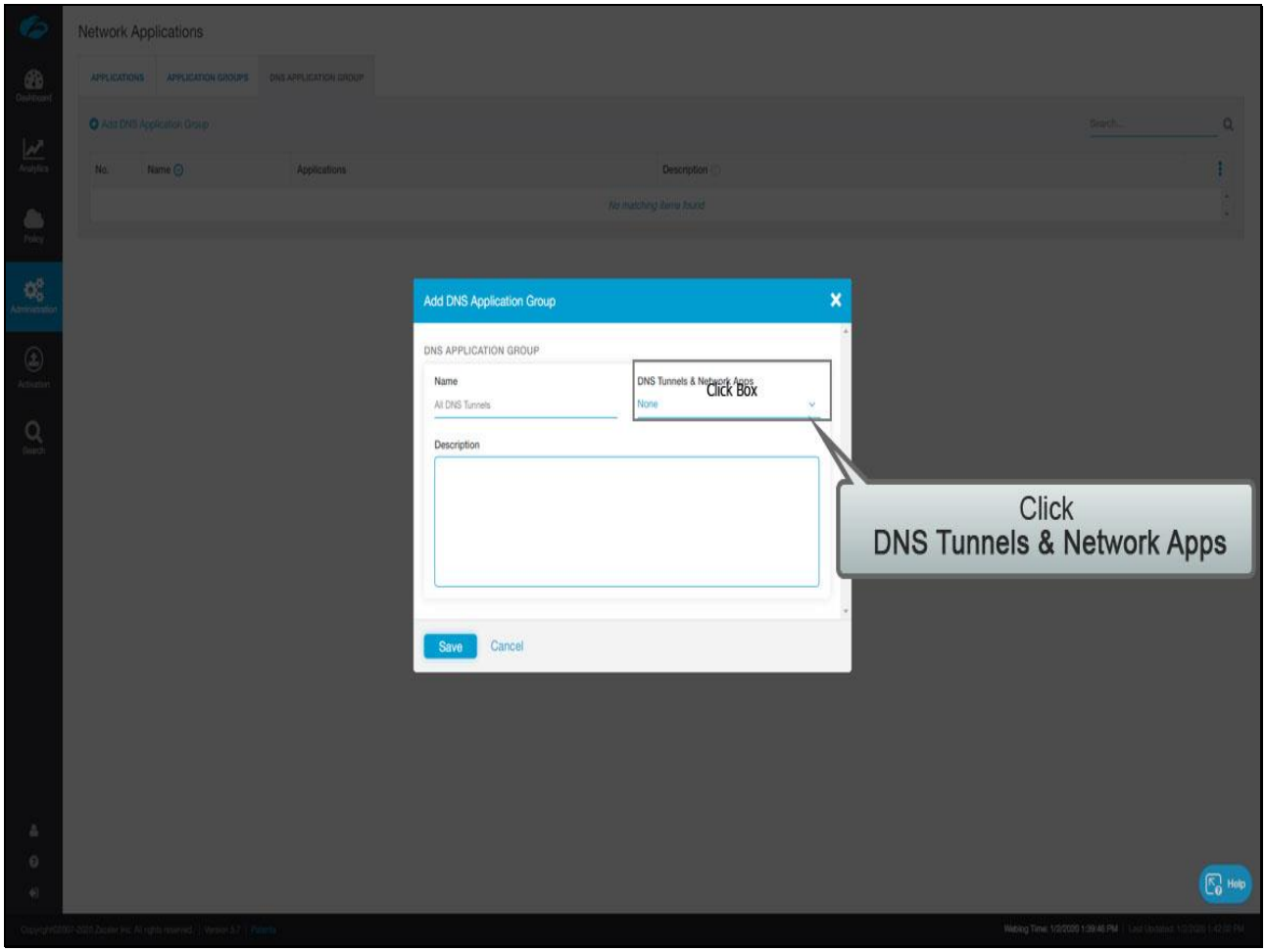
Slide 46 - Slide 46



Slide notes

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

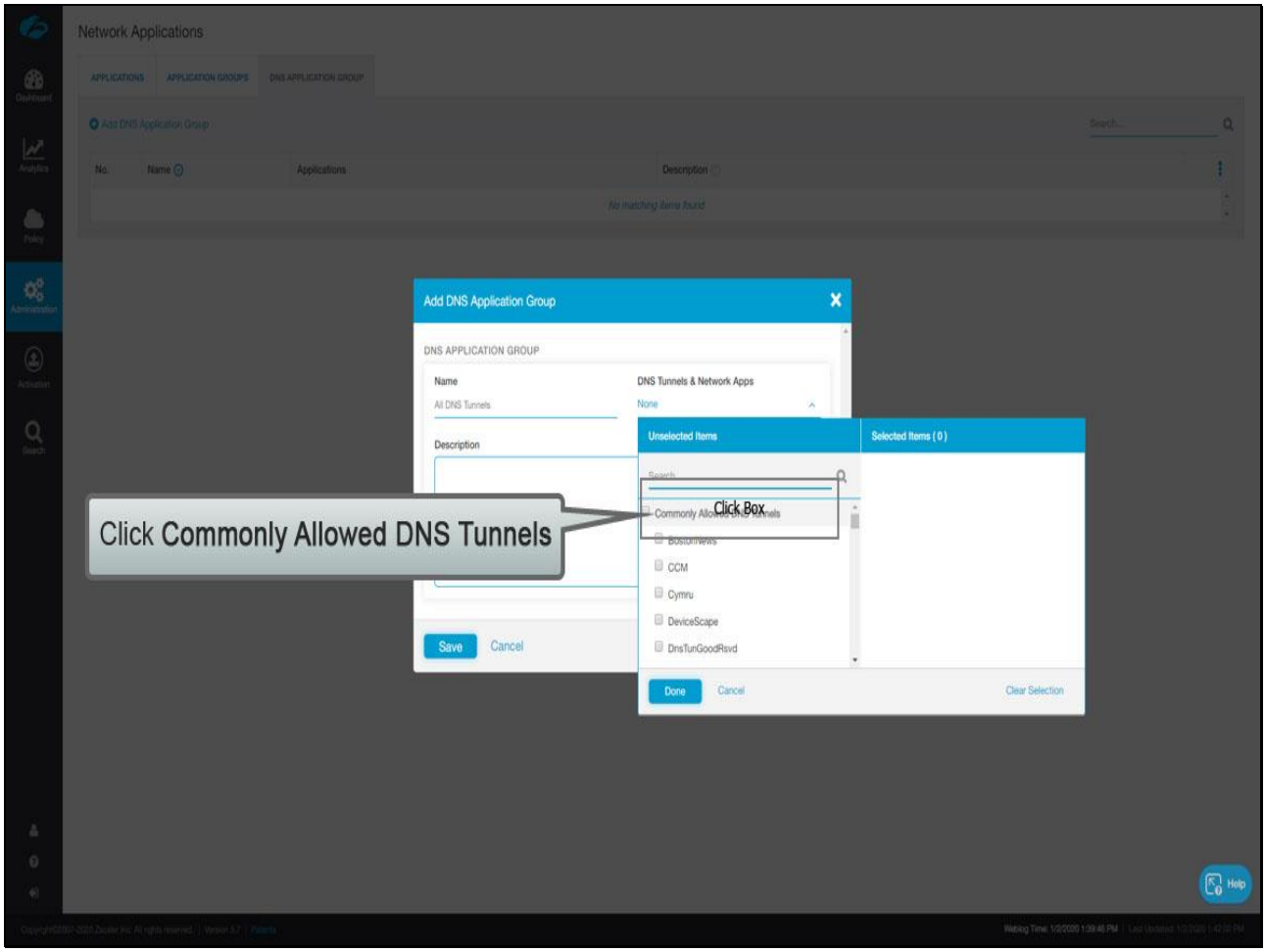
Slide 47 - Slide 47



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.

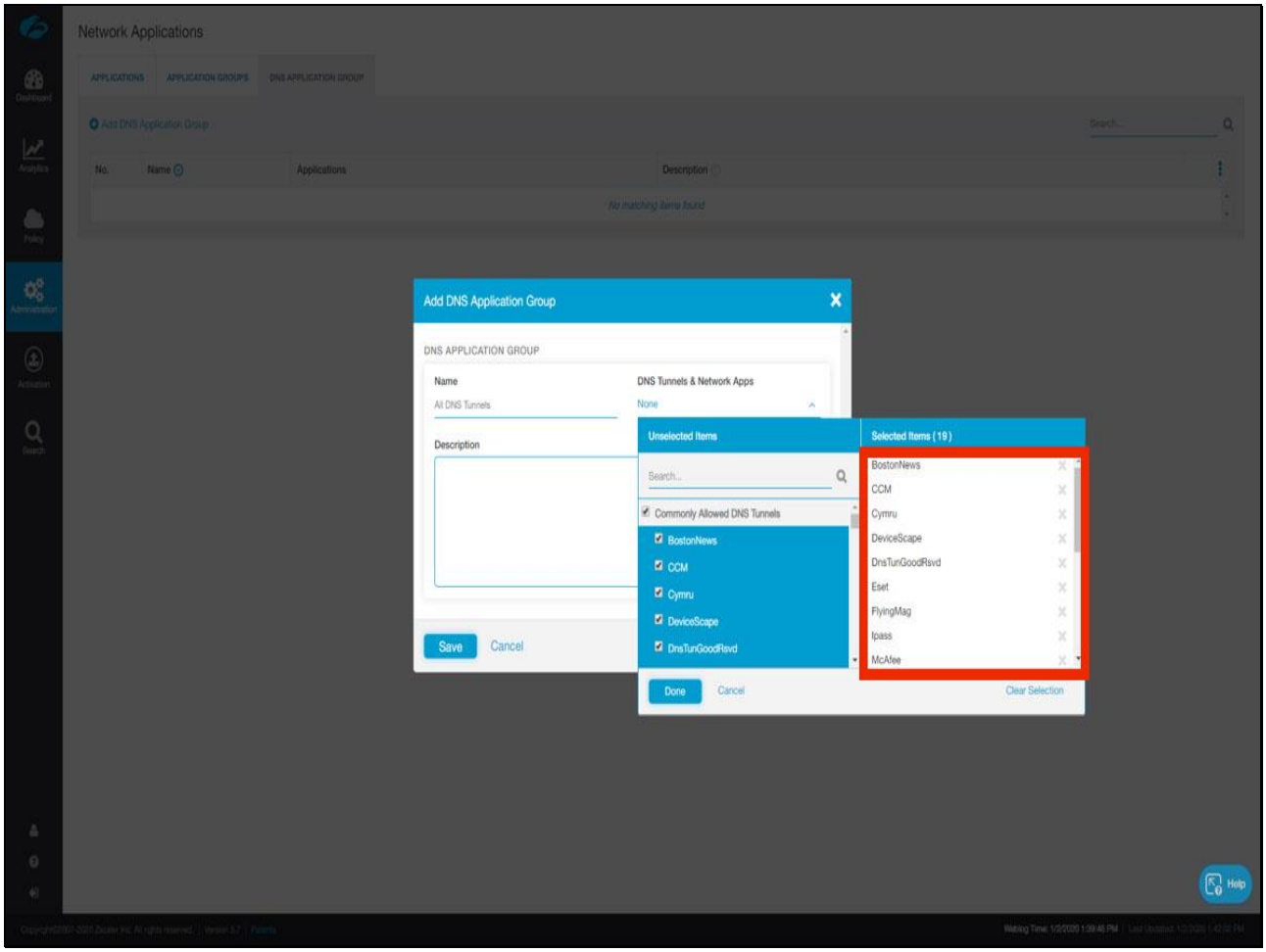
Slide 48 - Slide 48



Slide notes

Click **Commonly Allowed DNS Tunnels**.

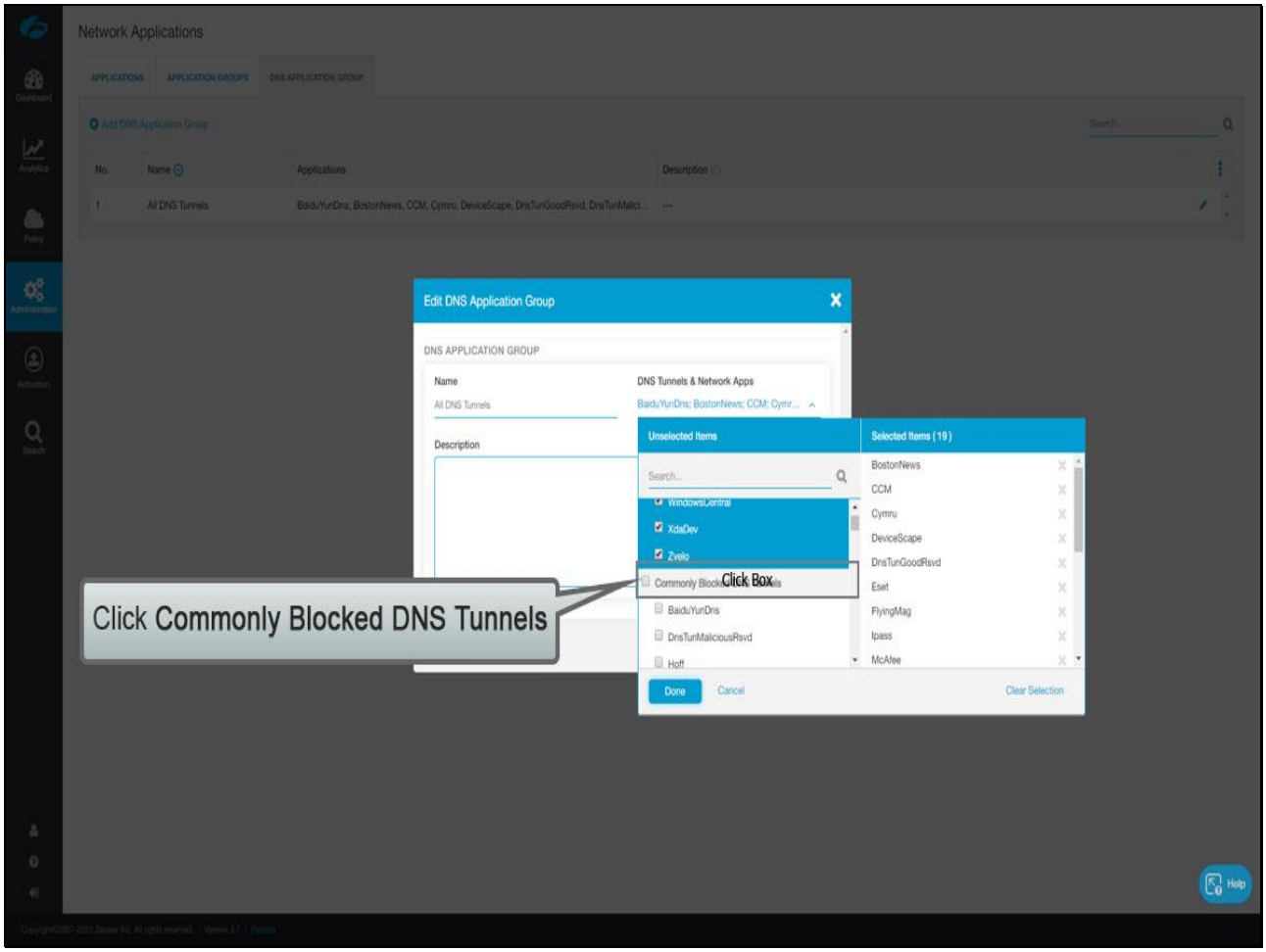
Slide 49 - Slide 49



Slide notes

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

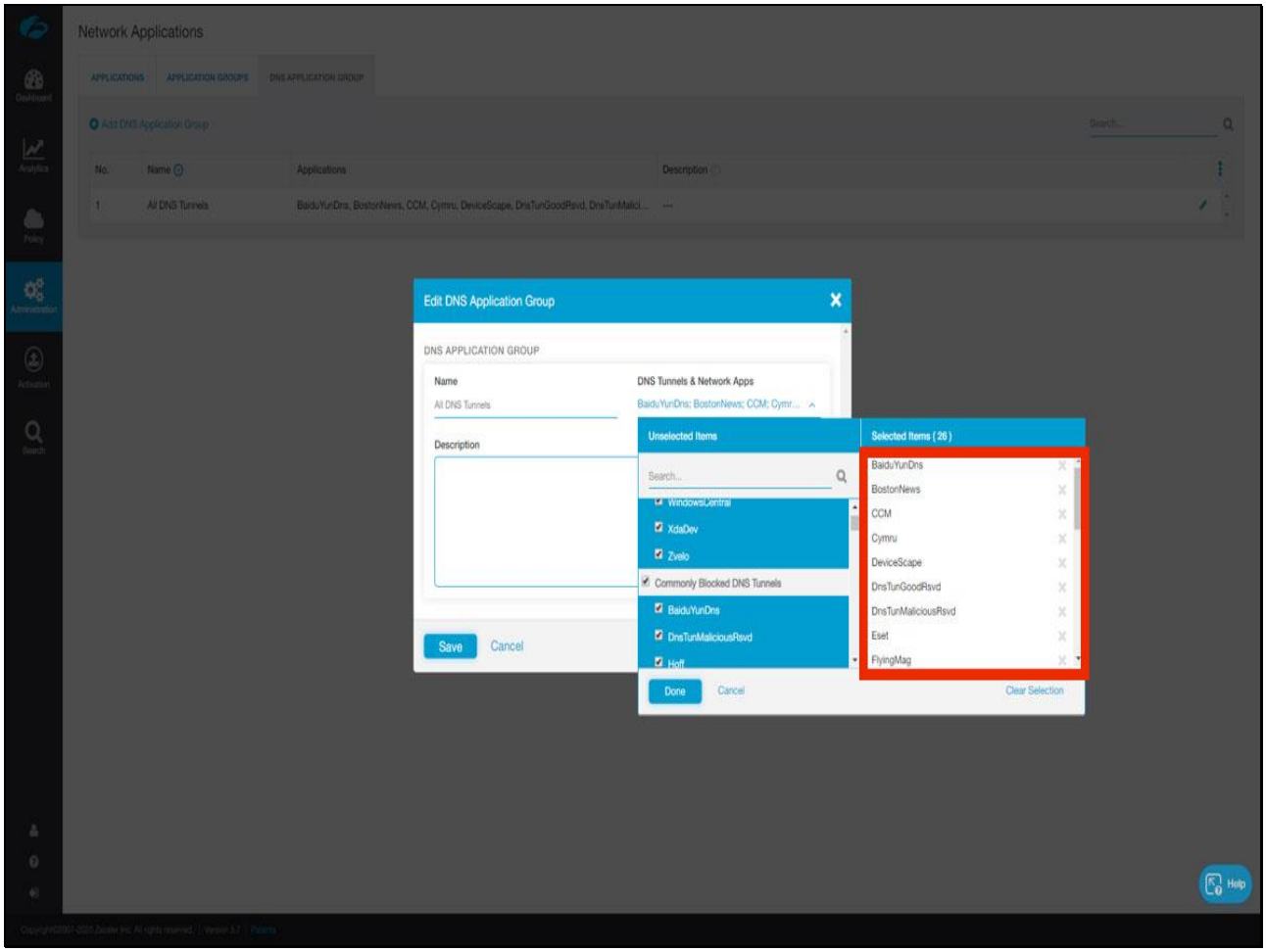
Slide 51 - Slide 51



Slide notes

Click **Commonly Blocked DNS Tunnels**.

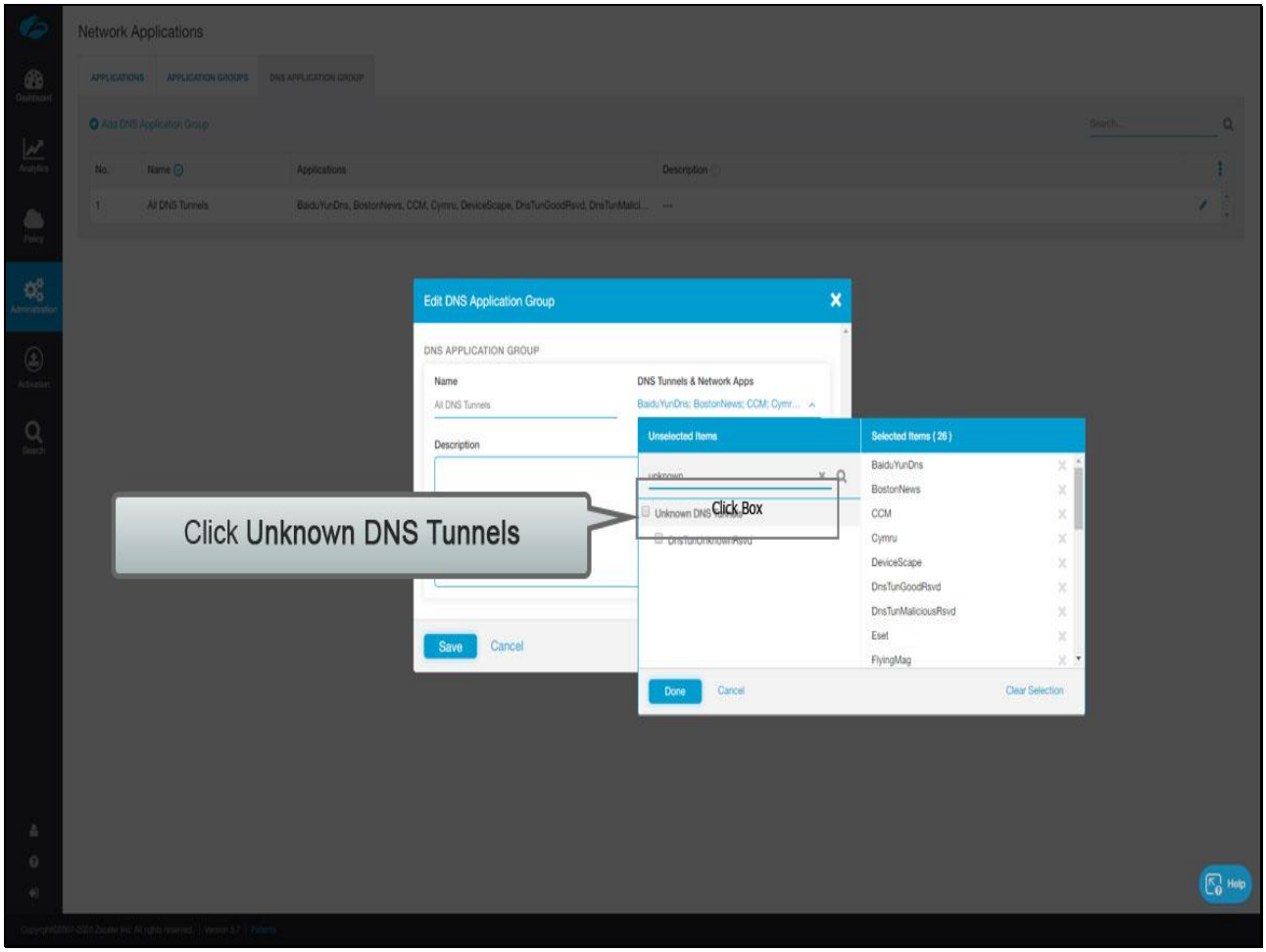
Slide 52 - Slide 52



Slide notes

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

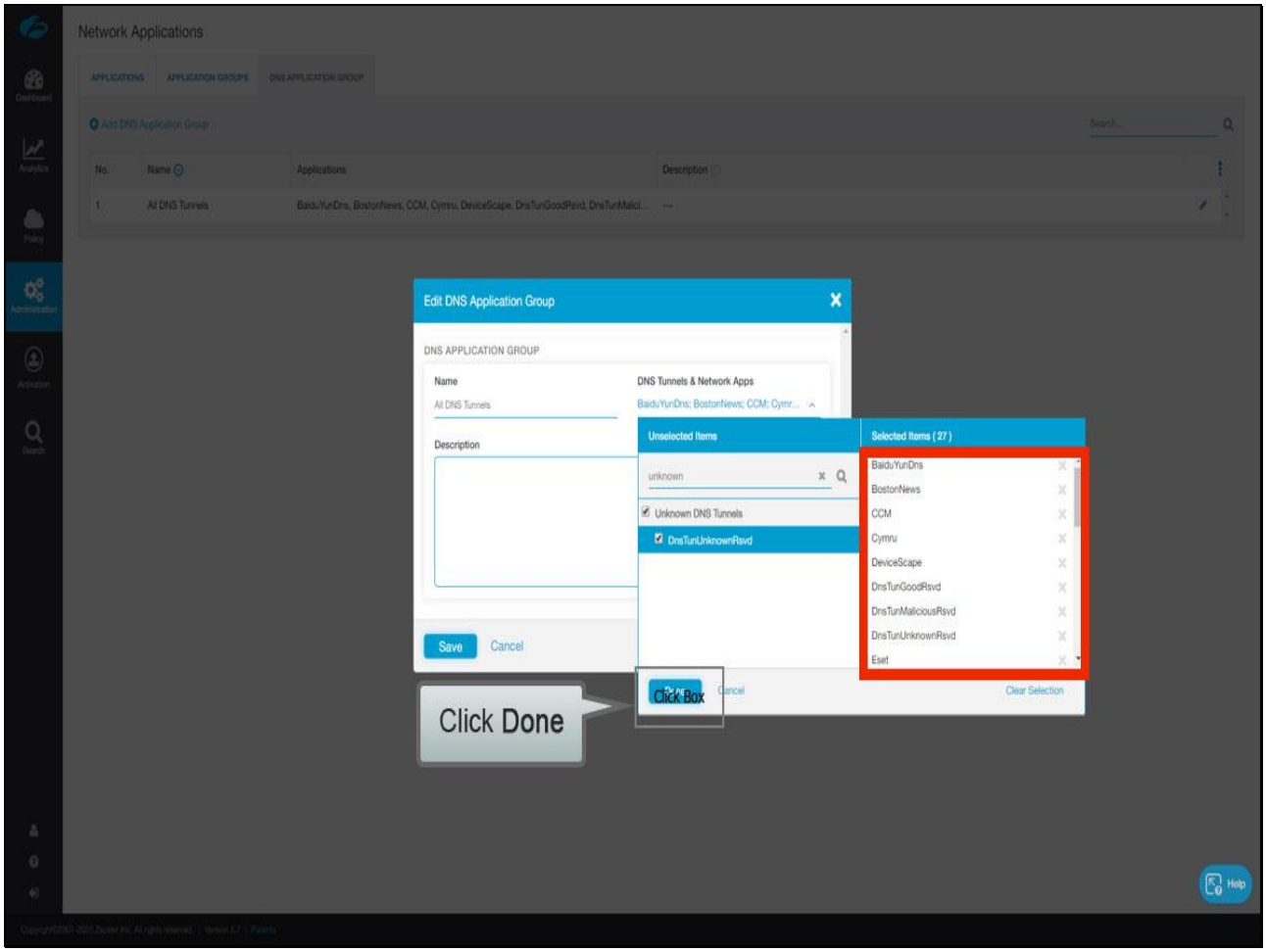
Slide 55 - Slide 55



Slide notes

Click **Unknown DNS Tunnels**.

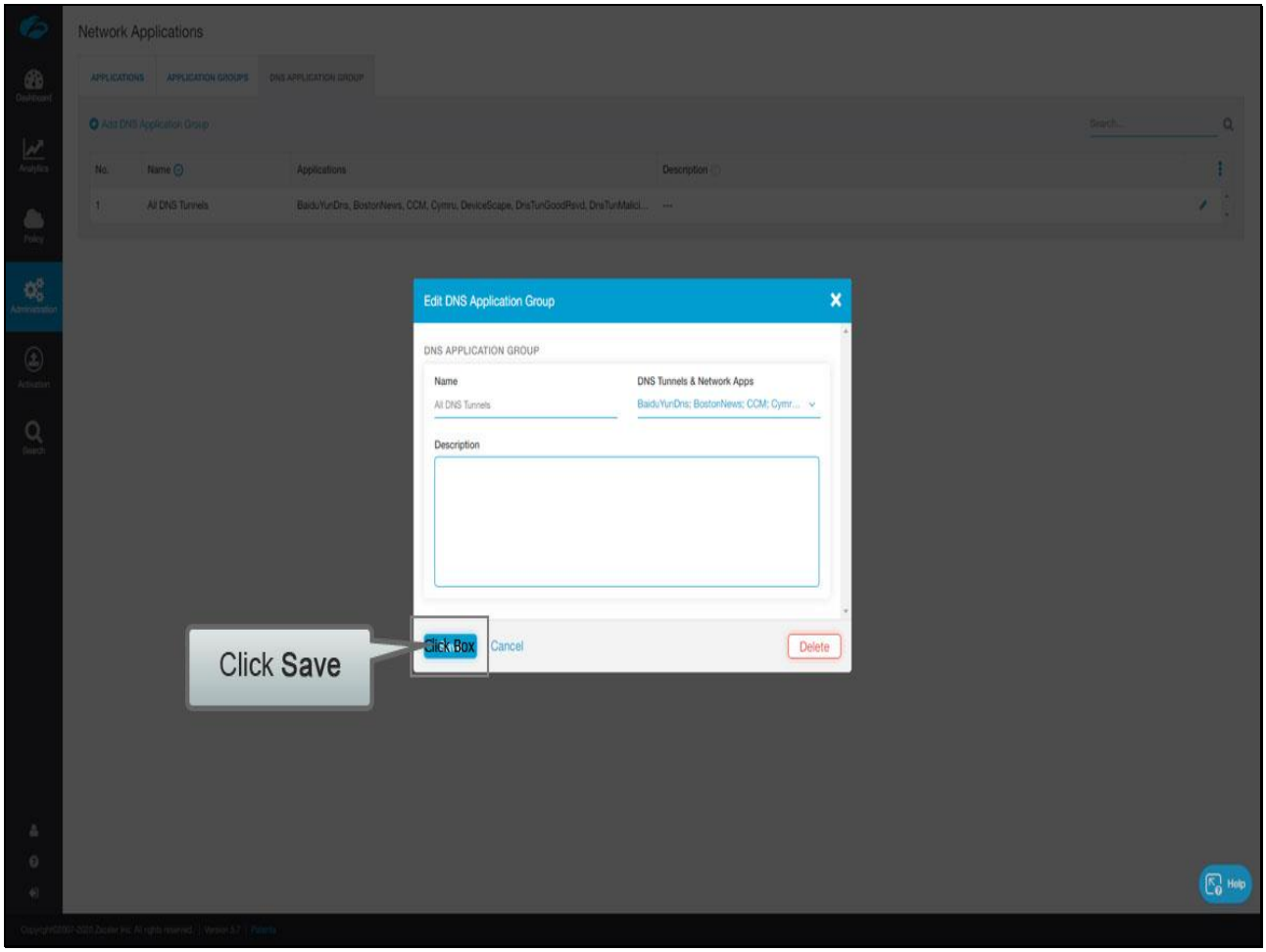
Slide 56 - Slide 56



Slide notes

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

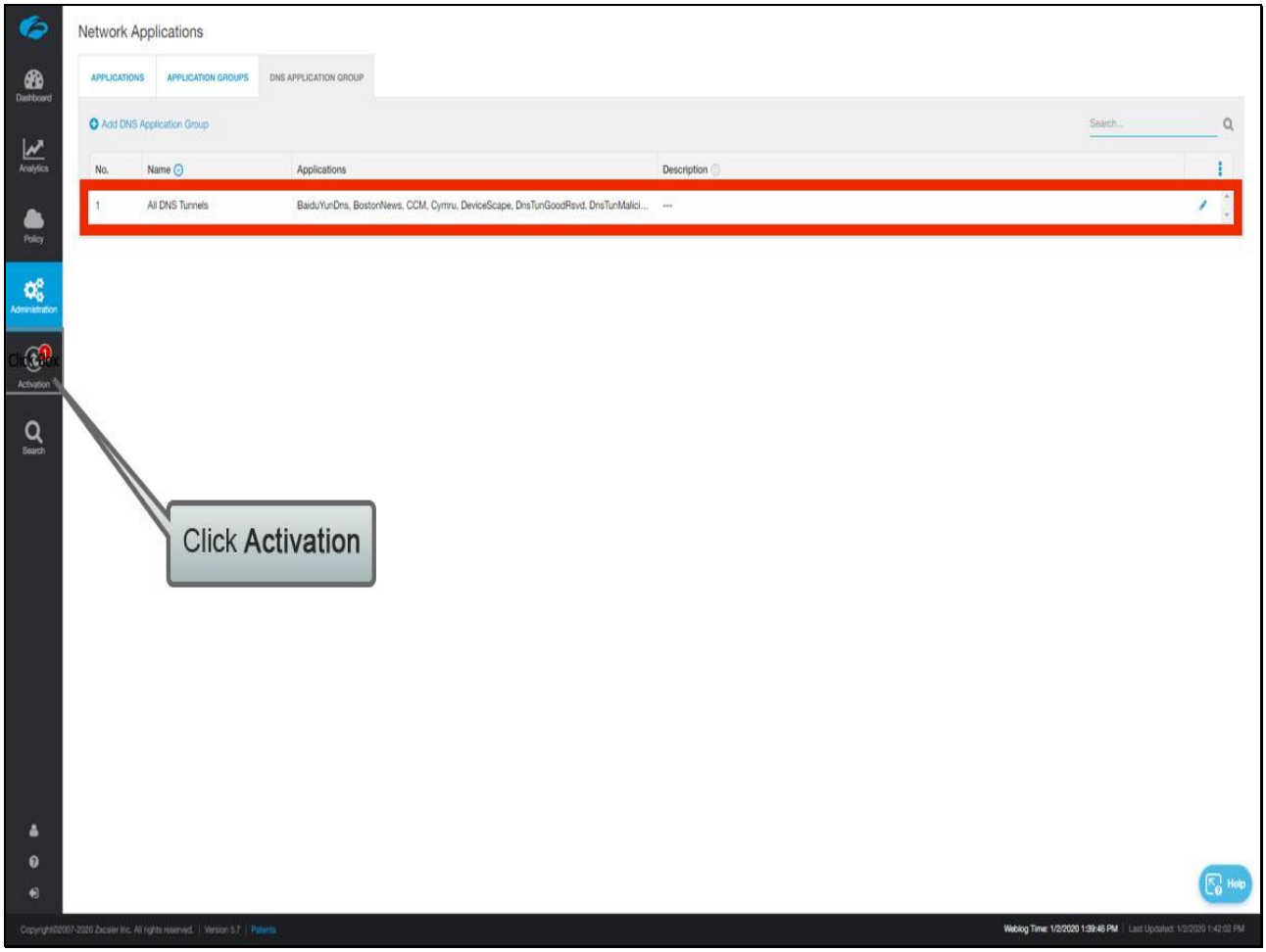
Slide 57 - Slide 57



Slide notes

Click **Save**.

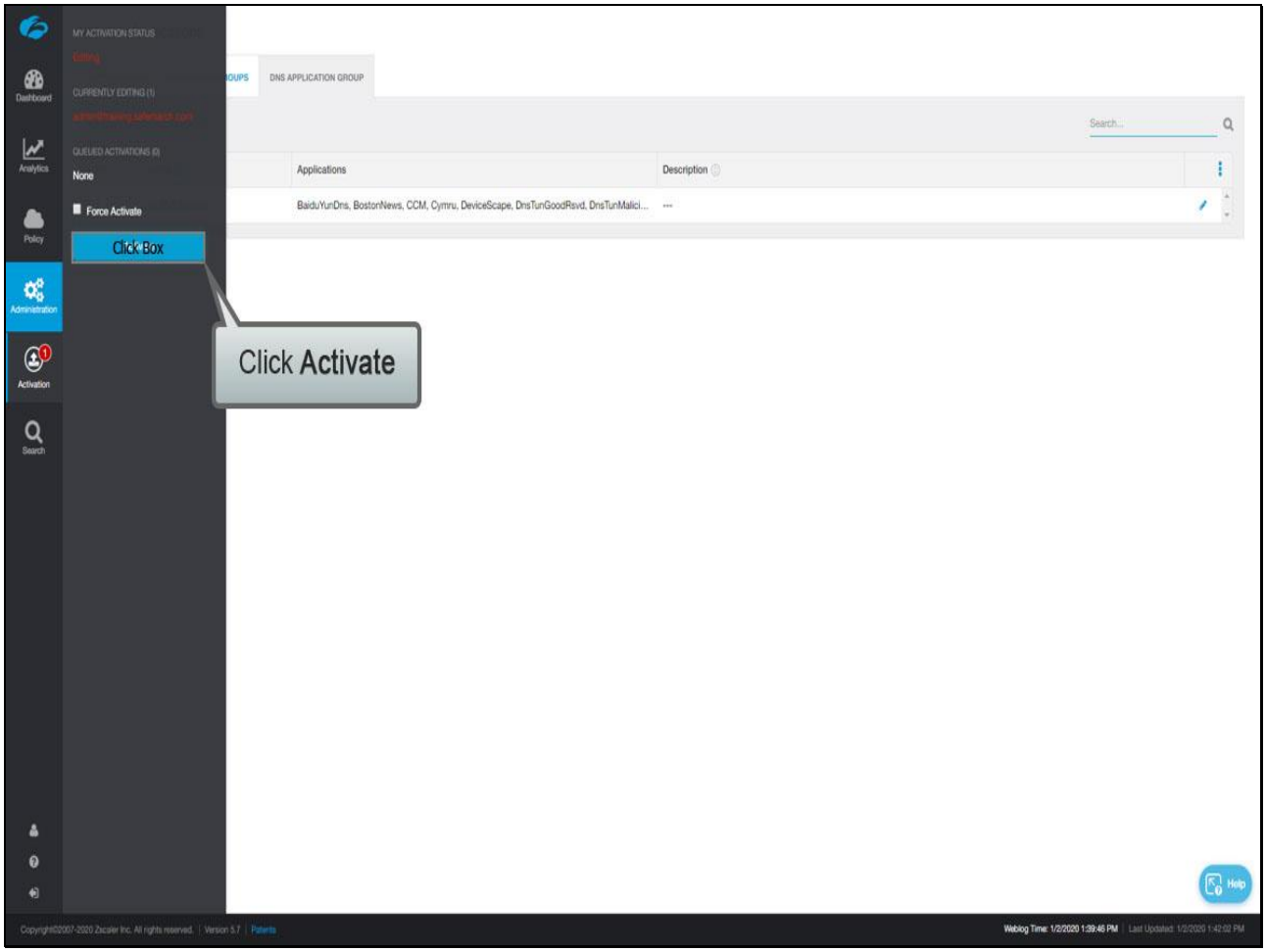
Slide 62 - Slide 62



Slide notes

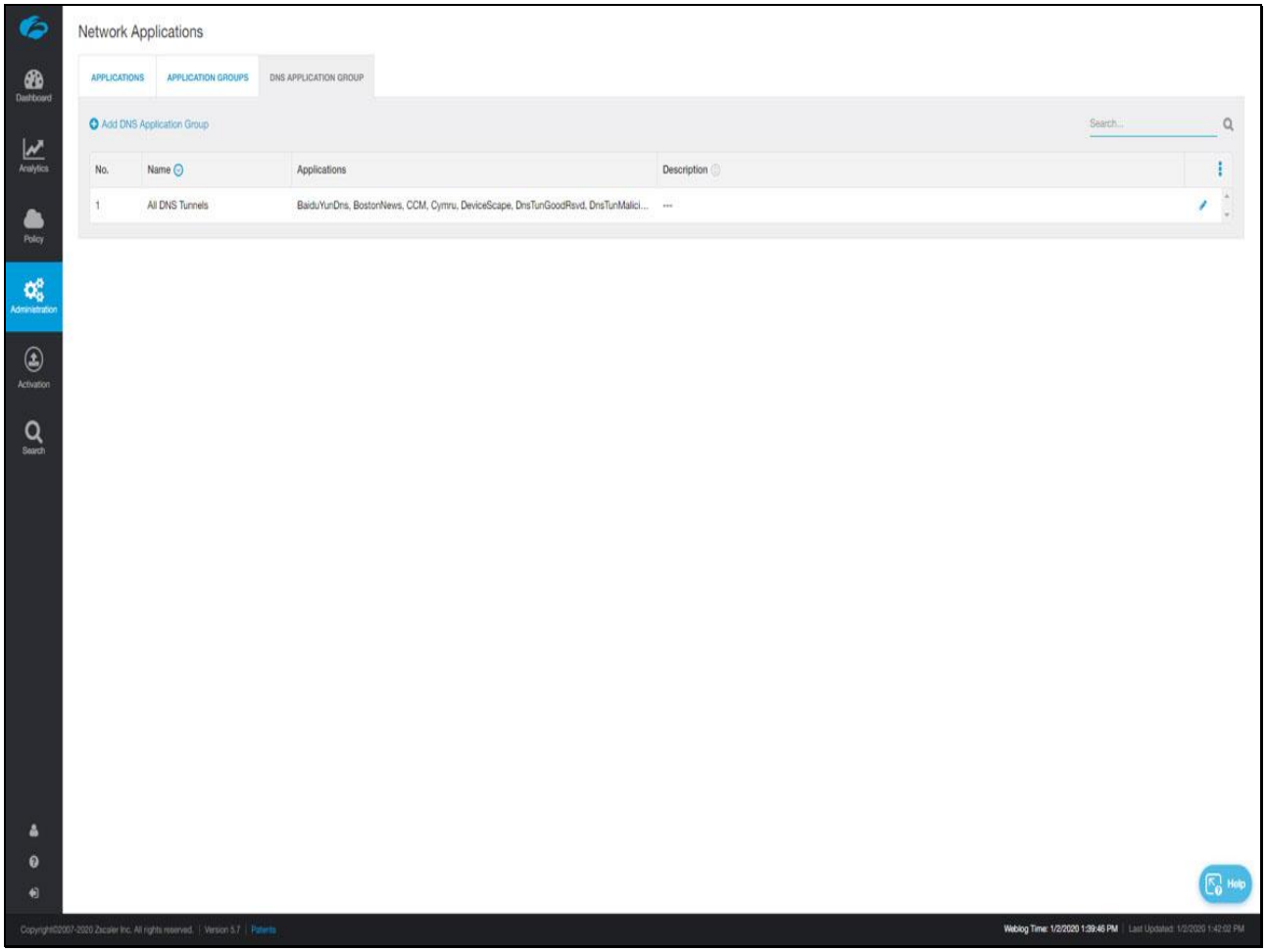
Verify that the new **DNS Application Group** has been added to the list. This DNS Application Group will be used in a later step to create a rule that will block DNS tunnel traffic. **Activate** the changes.

Slide 63 - Slide 63



Slide notes

Slide 68 - Slide 68



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.

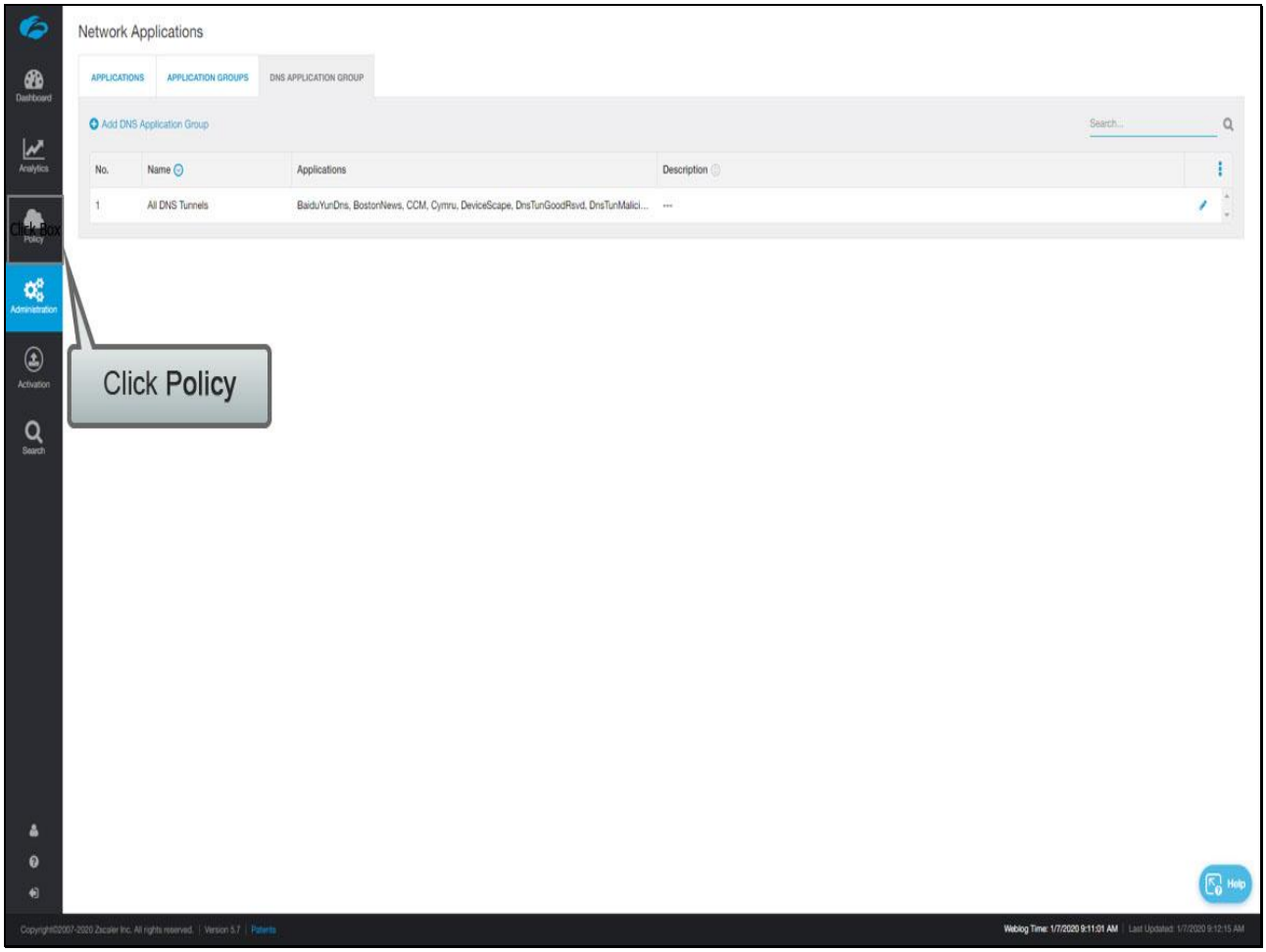
This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler Admin Portal UI. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

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

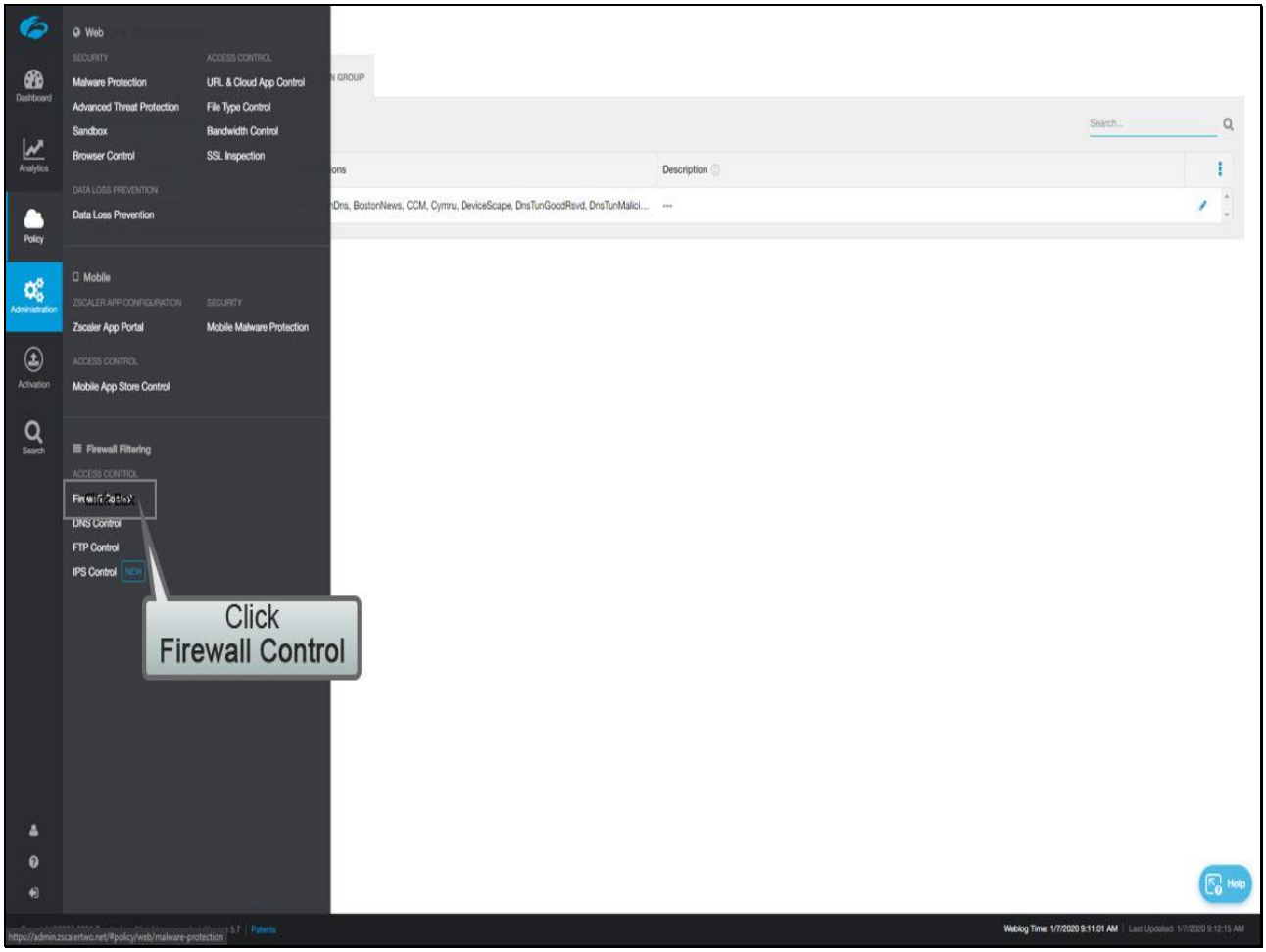


Slide notes

select **Firewall Control**.

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

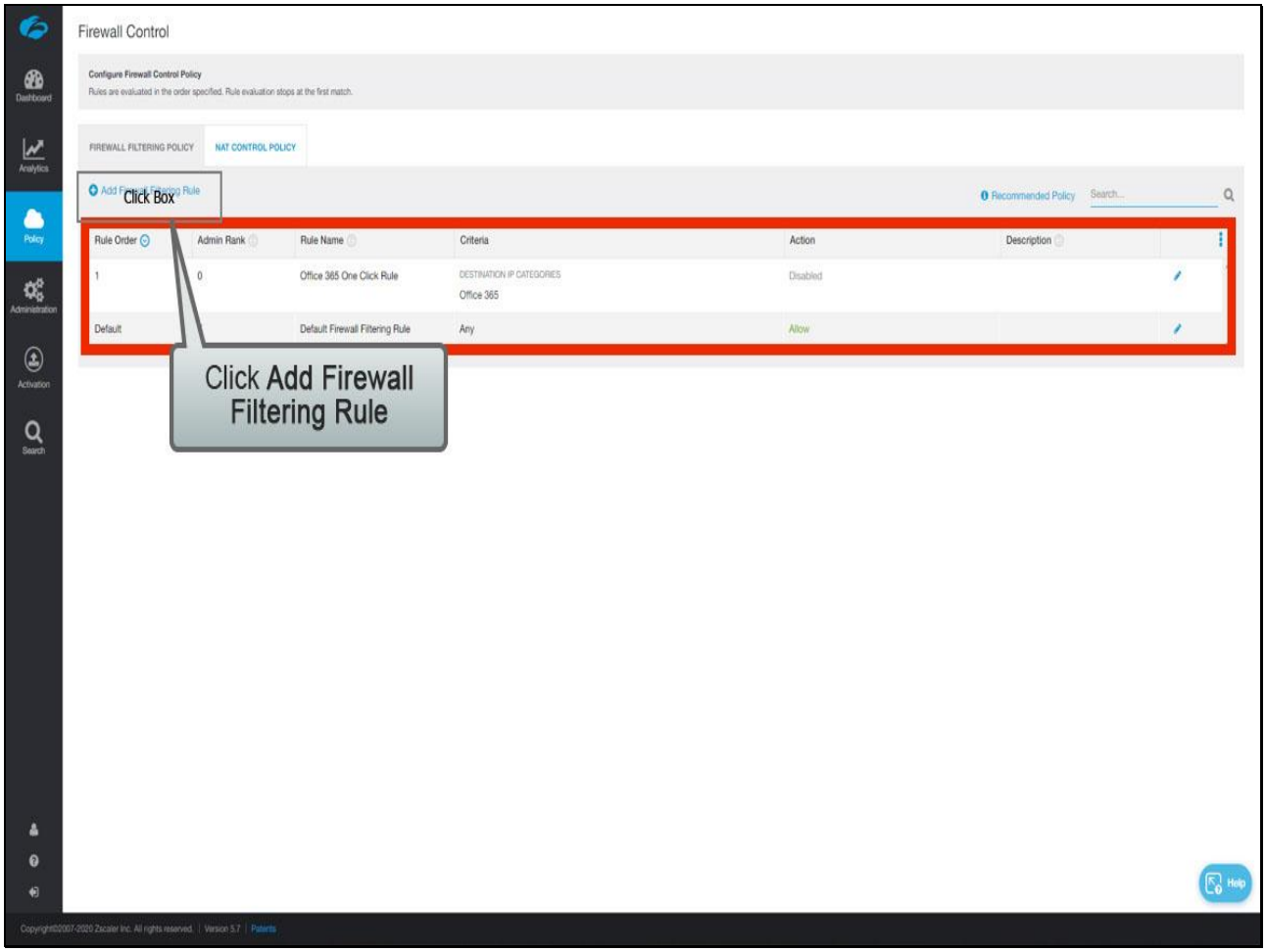
Slide 72 - Slide 72



Slide notes

Click **Firewall Control.**

Slide 74 - Slide 74



Slide notes

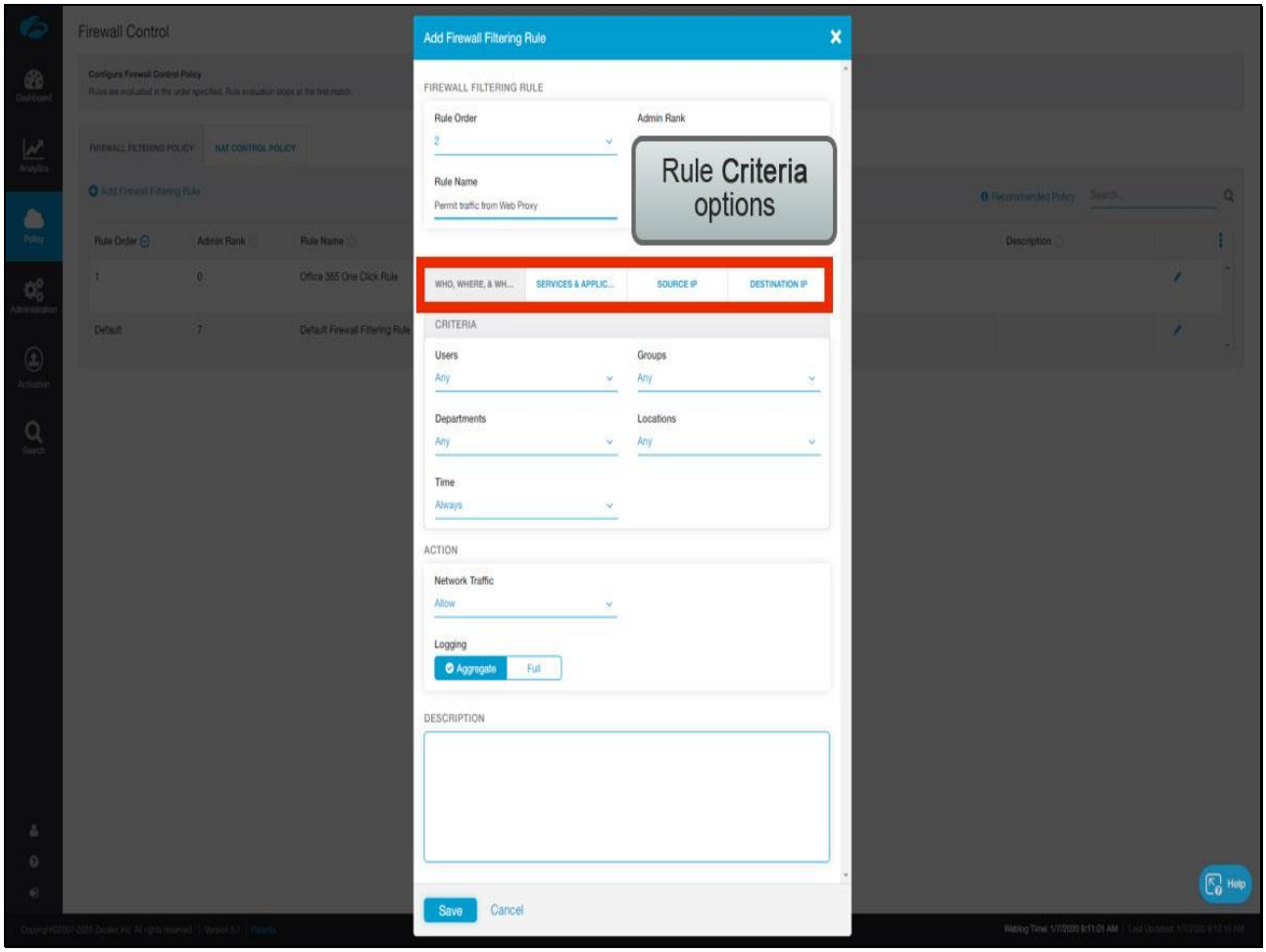
Here, you can create up to 1024 Firewall policy rules, and you can see a couple of default rules have been added for you. The first rule listed here is a system generated rule for Microsoft Office 365 traffic. This rule is added automatically at position 1 when you enable the Microsoft Office **One Click**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

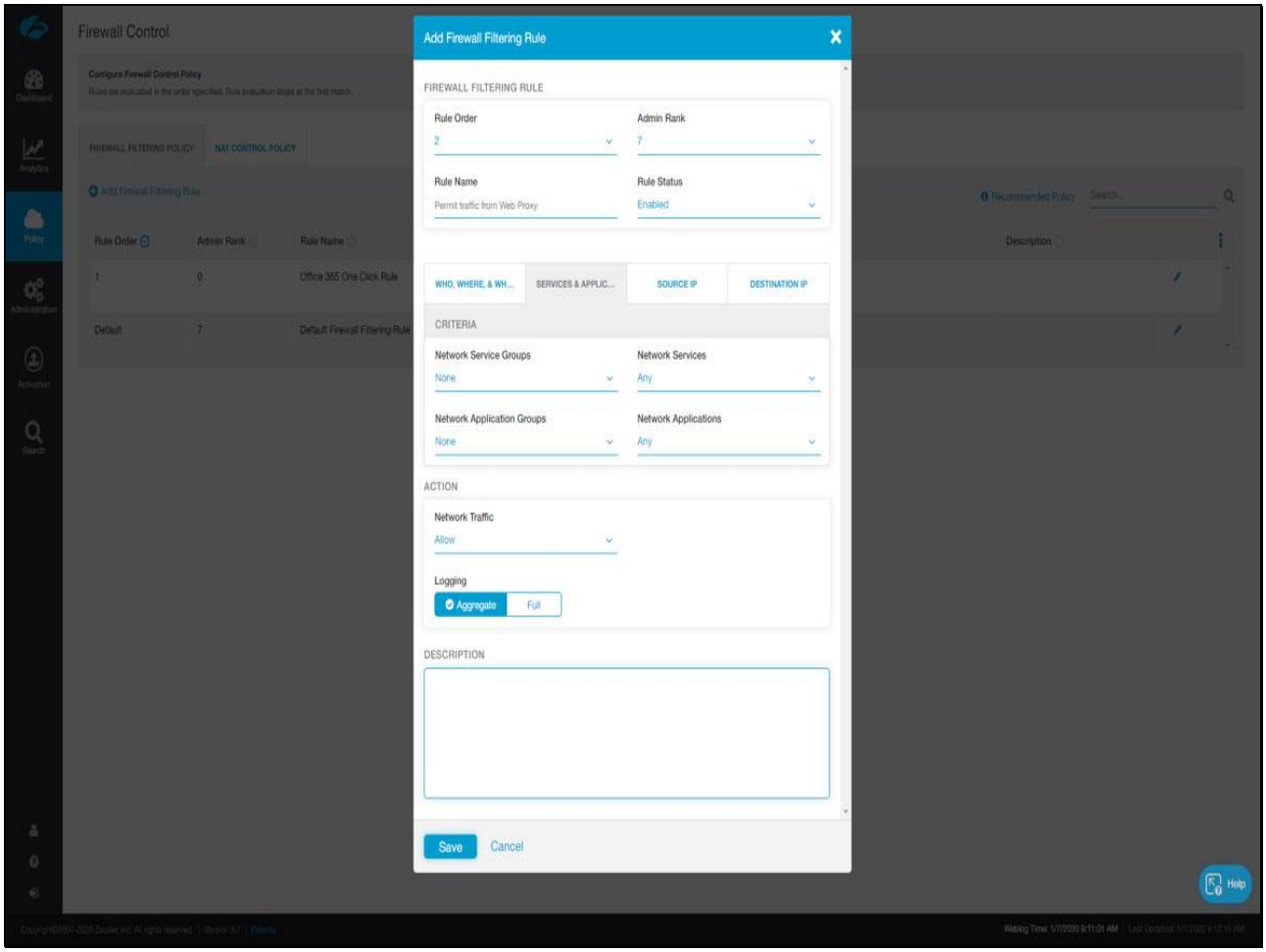


Slide notes

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.

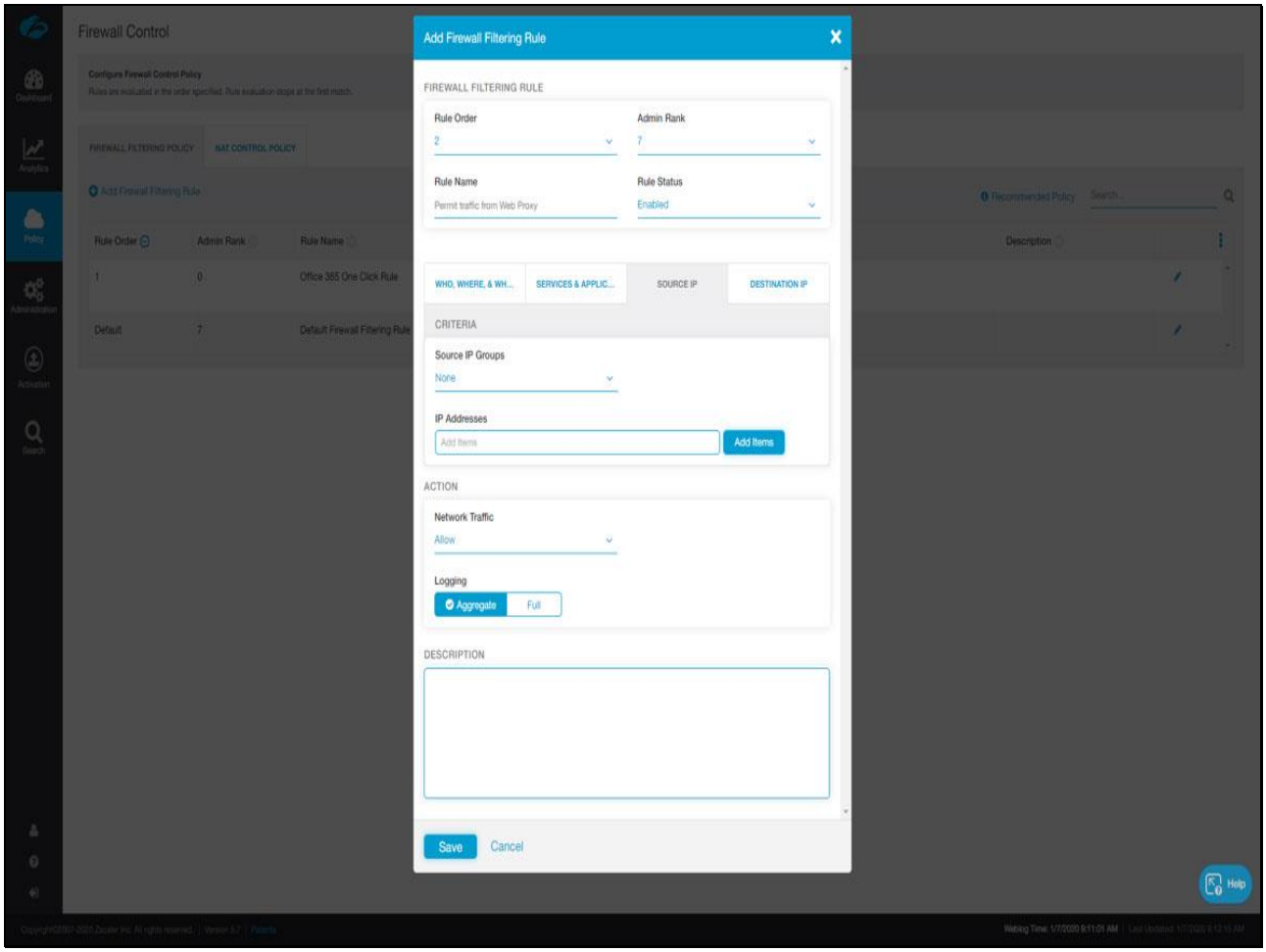
Slide 80 - Slide 80



Slide notes

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

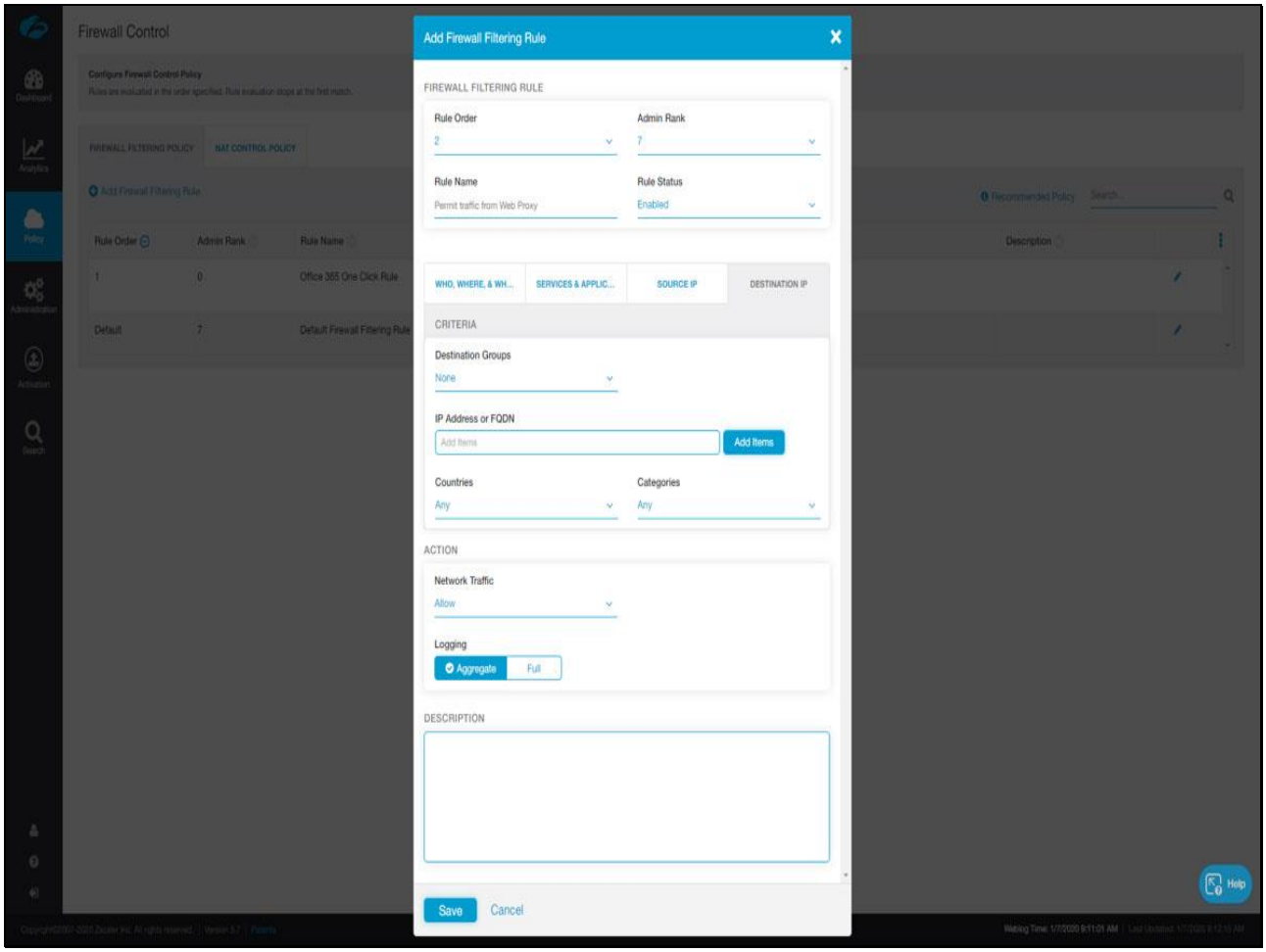
Slide 81 - Slide 81



Slide notes

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

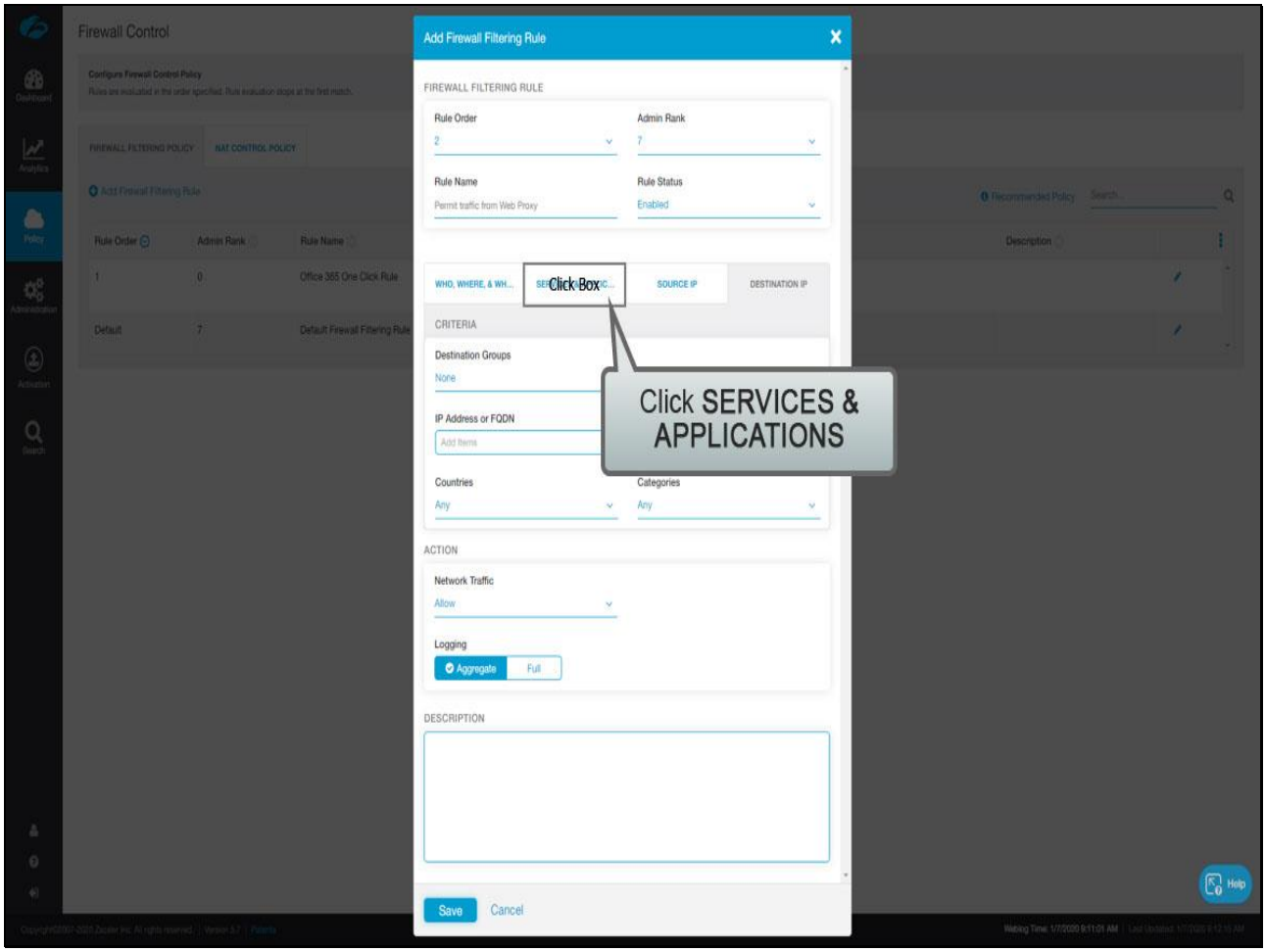
Slide 82 - Slide 82



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**.

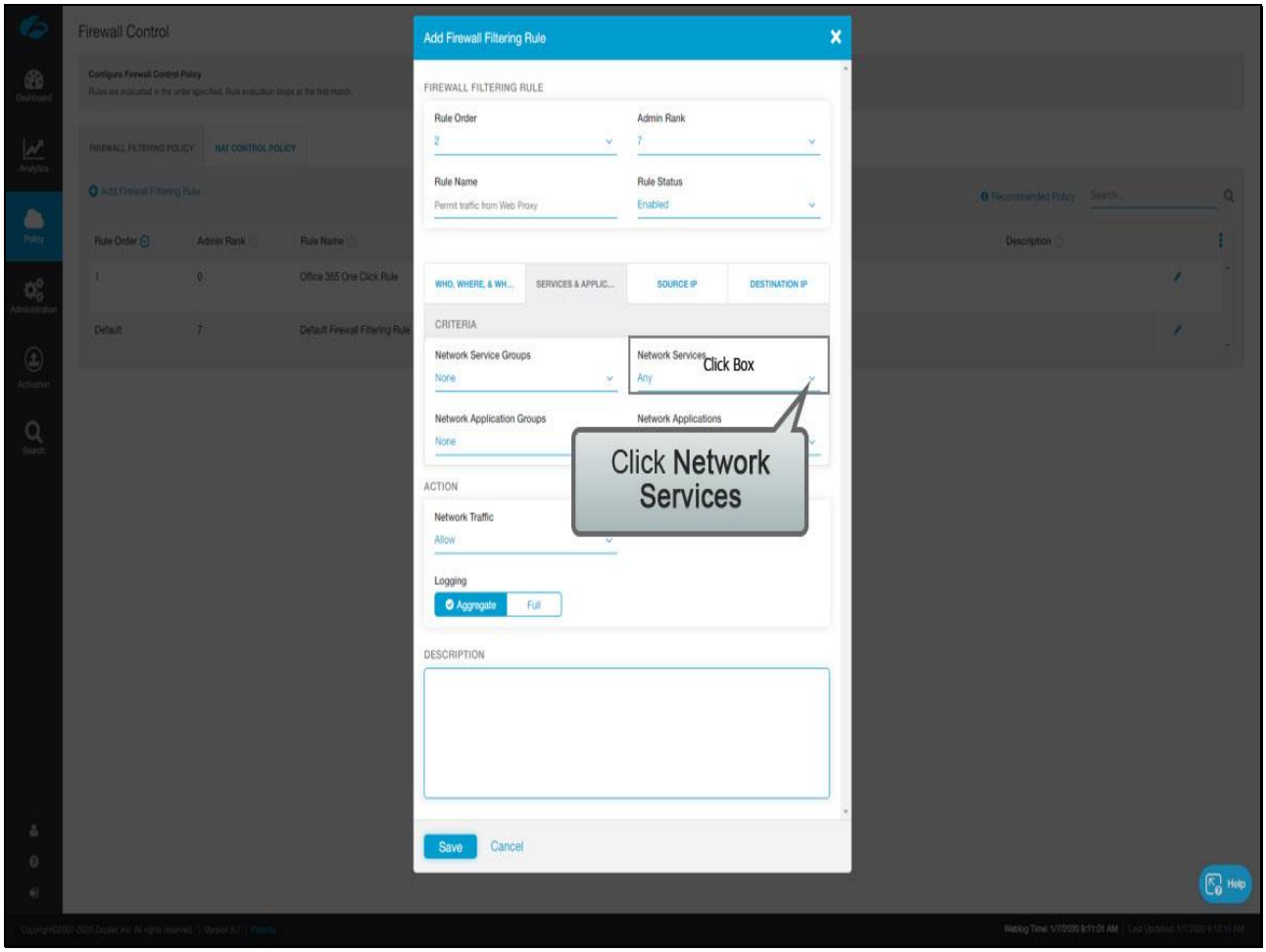
Slide 83 - Slide 83



Slide notes

Click the **SERVICES & APPLICATIONS** tab.

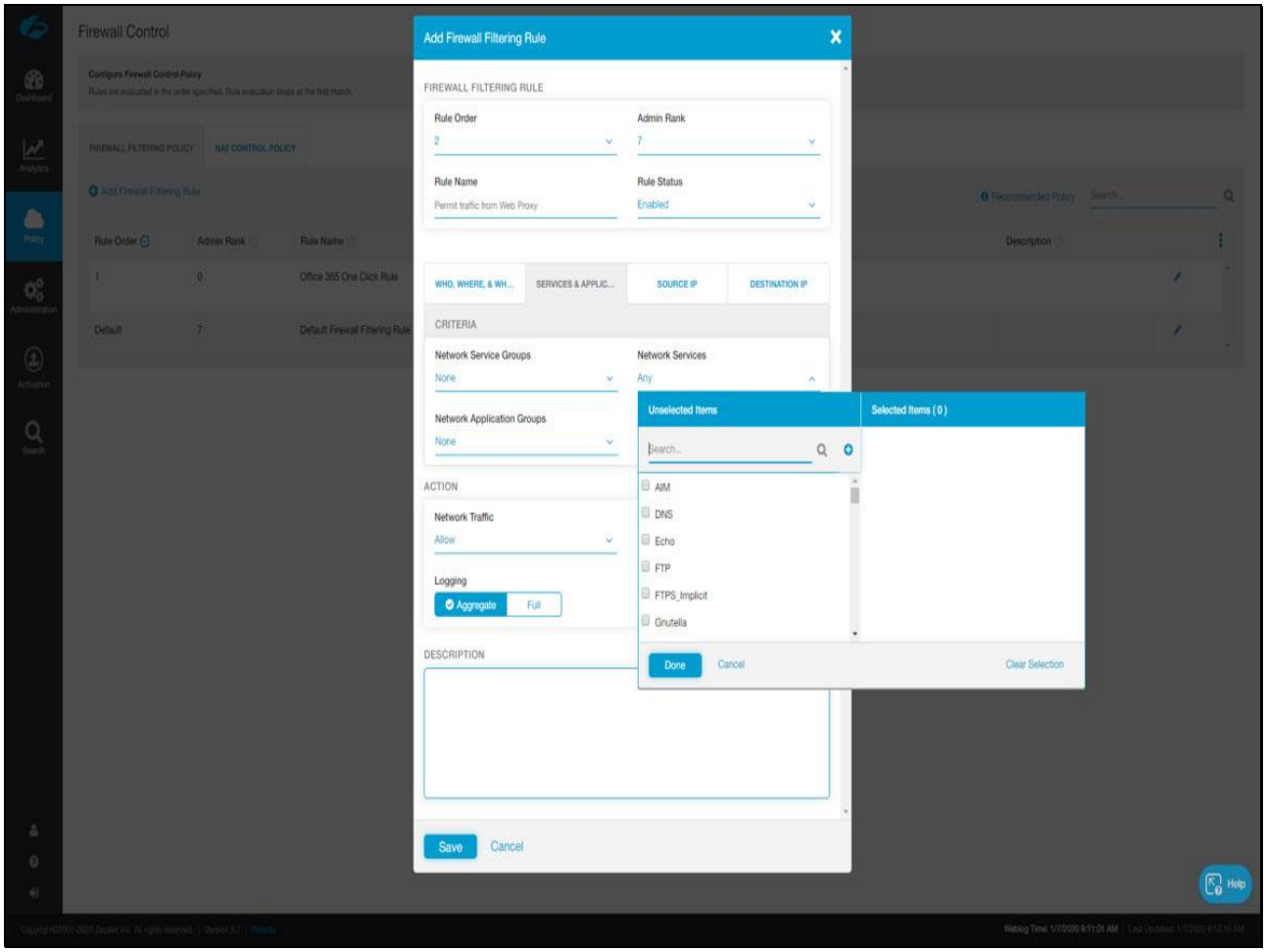
Slide 84 - Slide 84



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

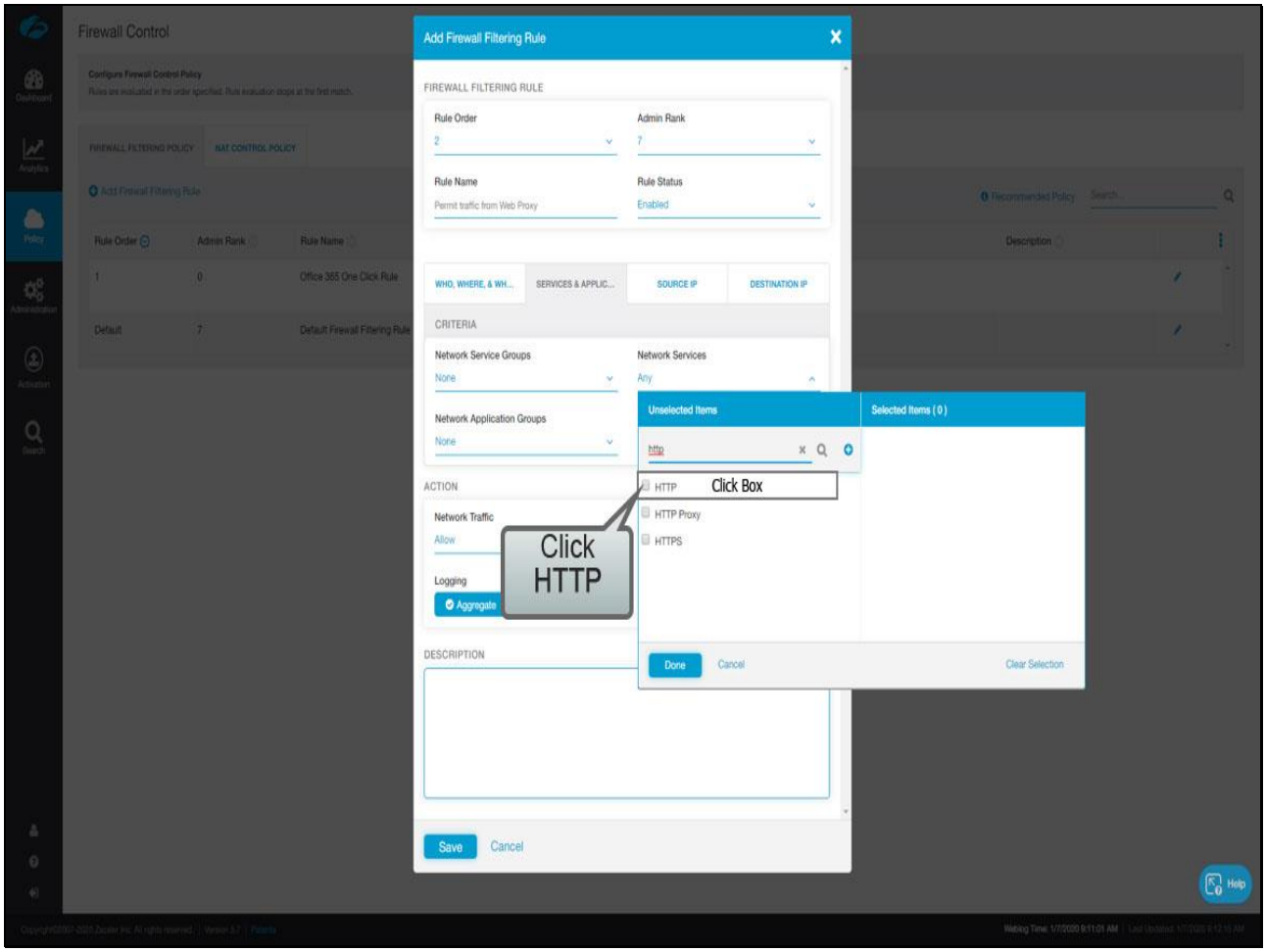
Slide 85 - Slide 85



Slide notes

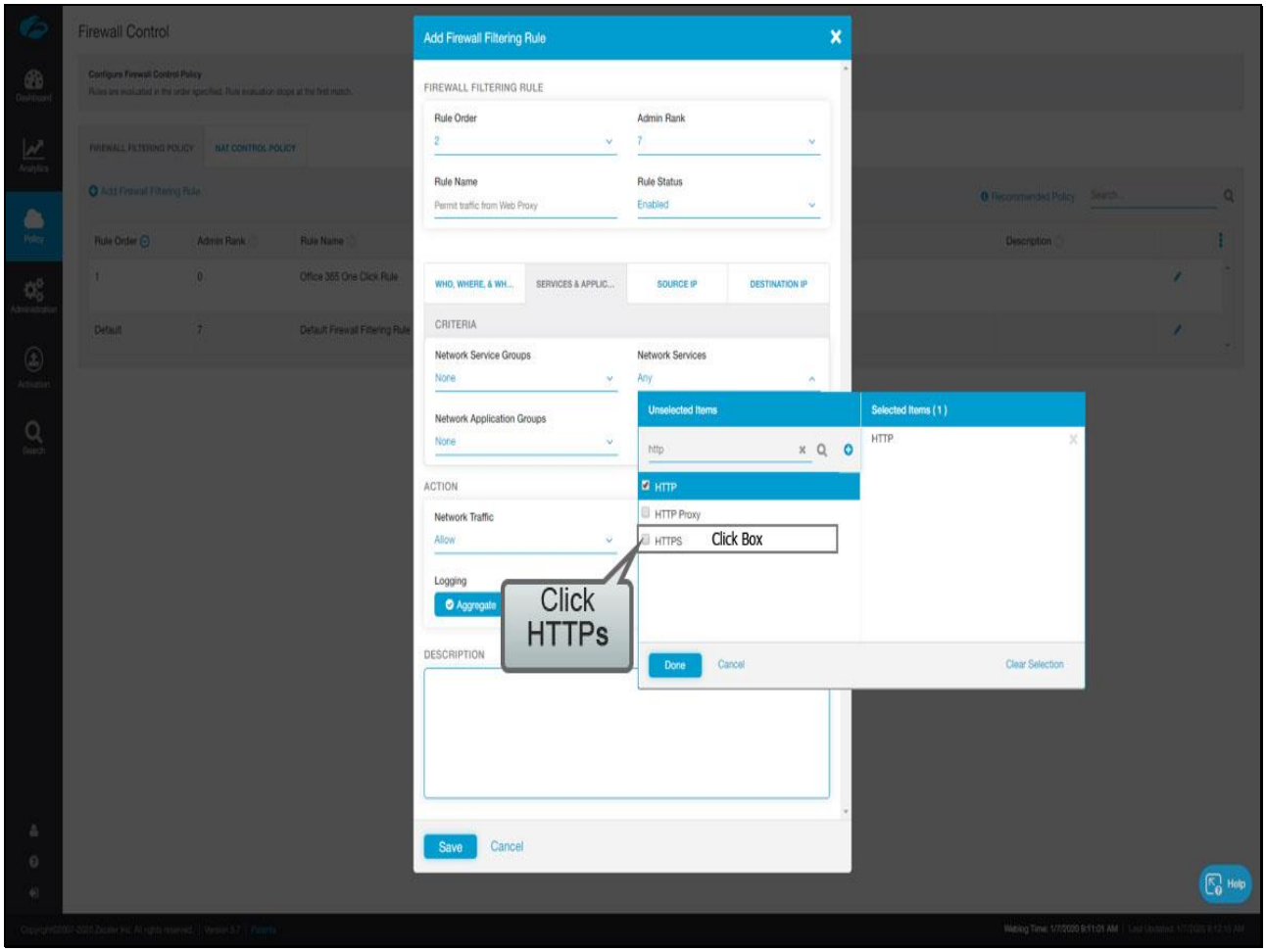
select **HTTP** and **HTTPS**, then click **Done**.

Slide 87 - Slide 87



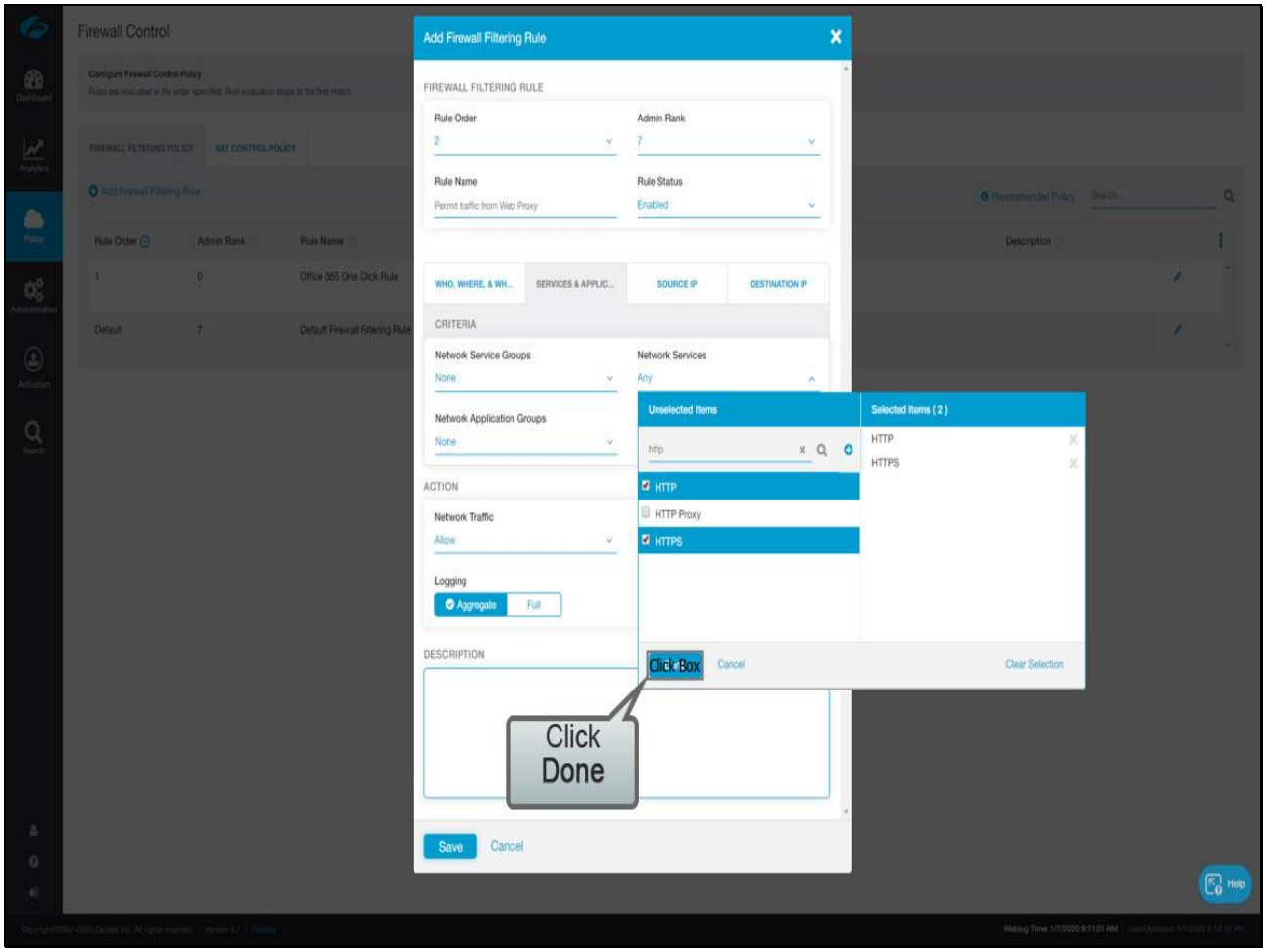
Slide notes

Slide 88 - Slide 88



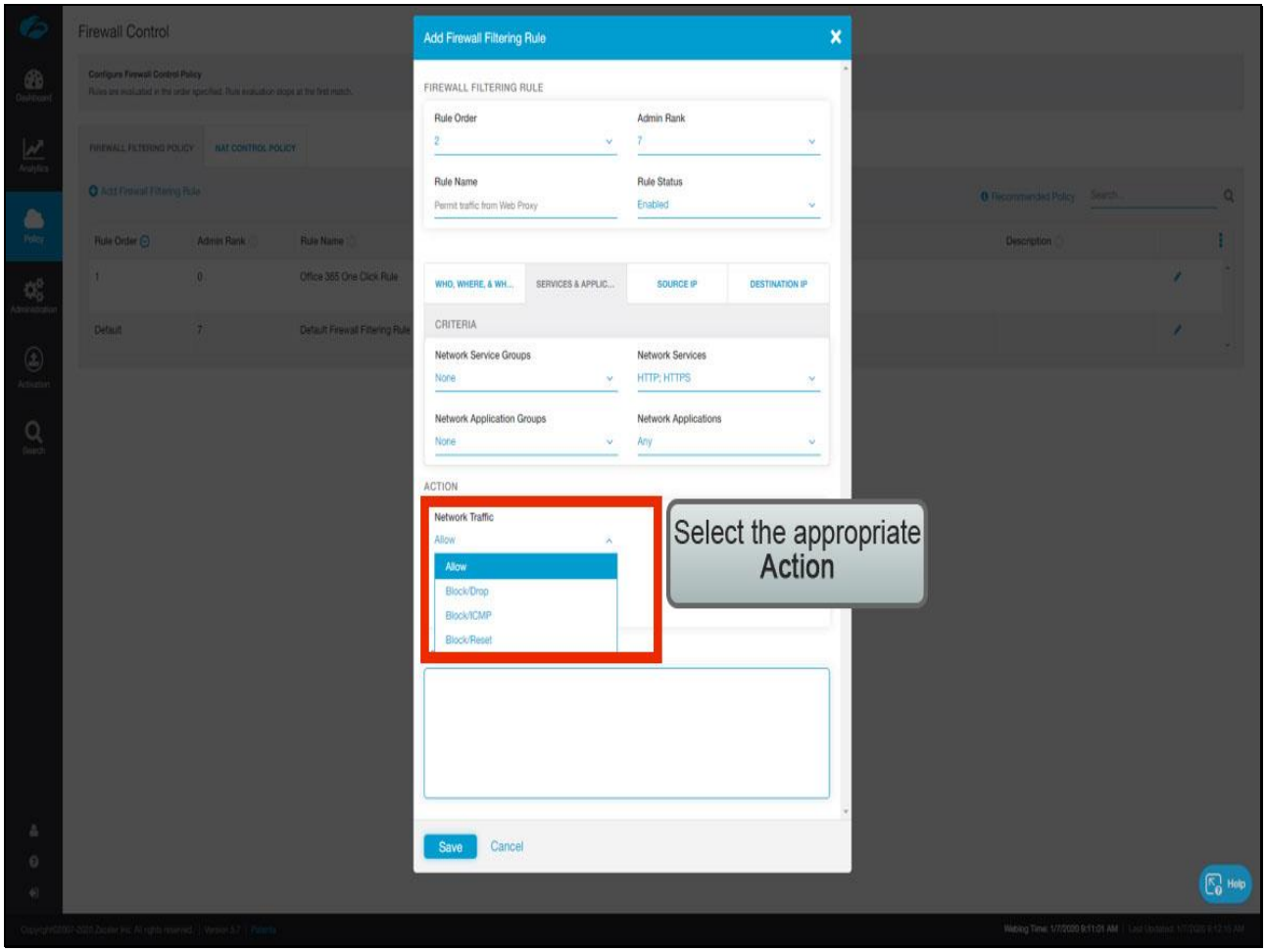
Slide notes

Slide 89 - Slide 89



Slide notes

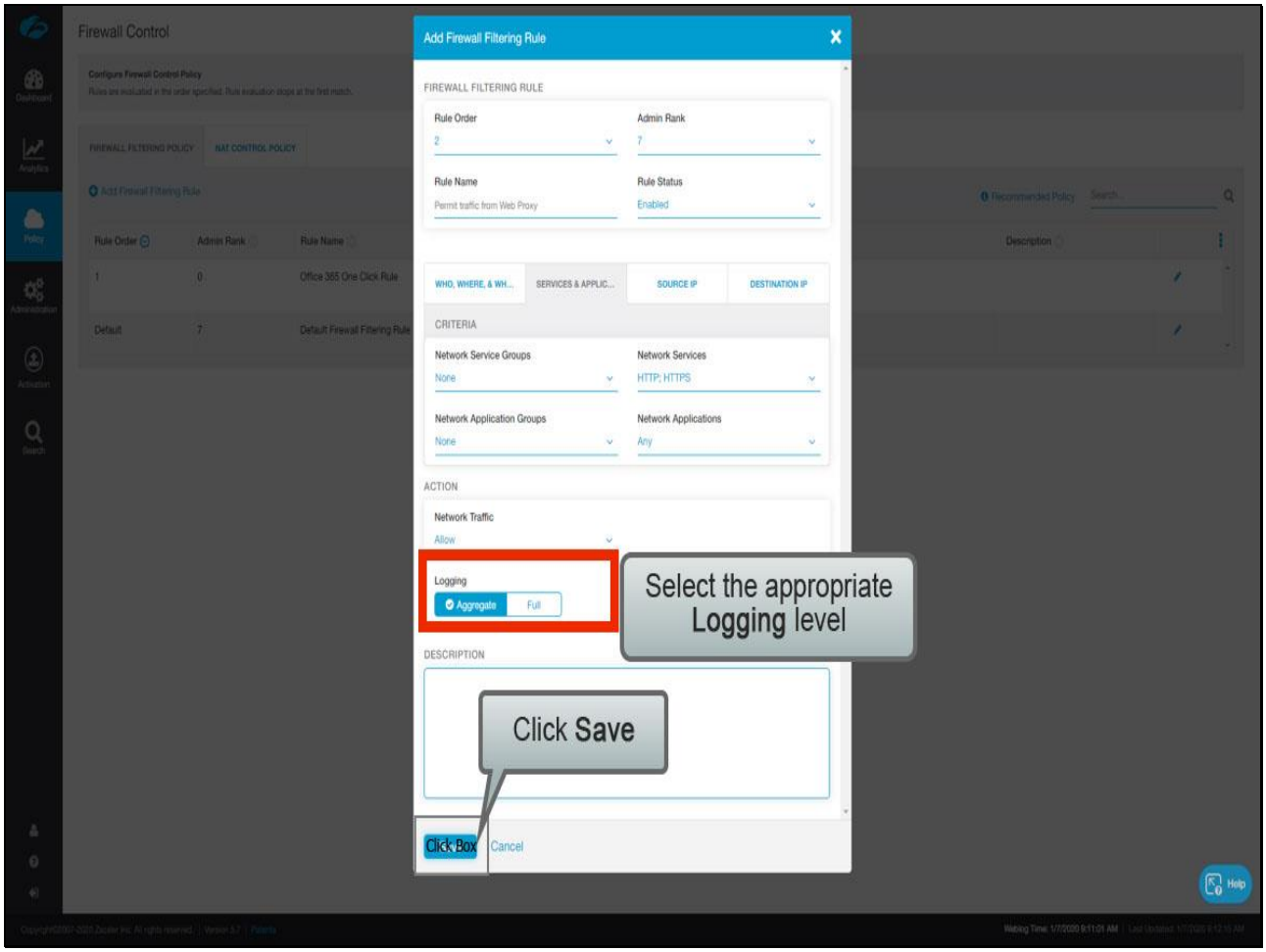
Slide 91 - Slide 91



Slide notes

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

Slide 92 - Slide 92

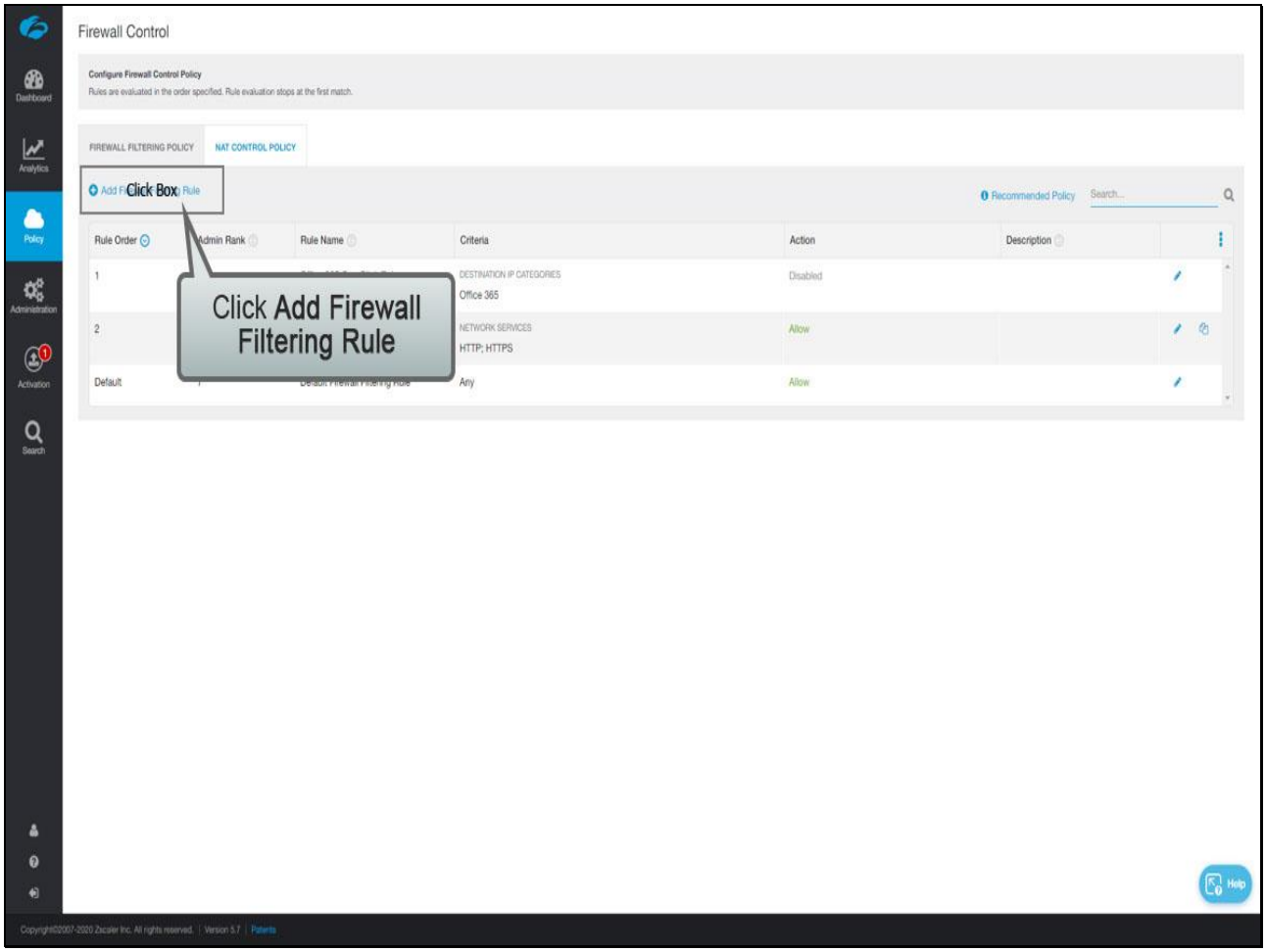


Slide notes

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**.

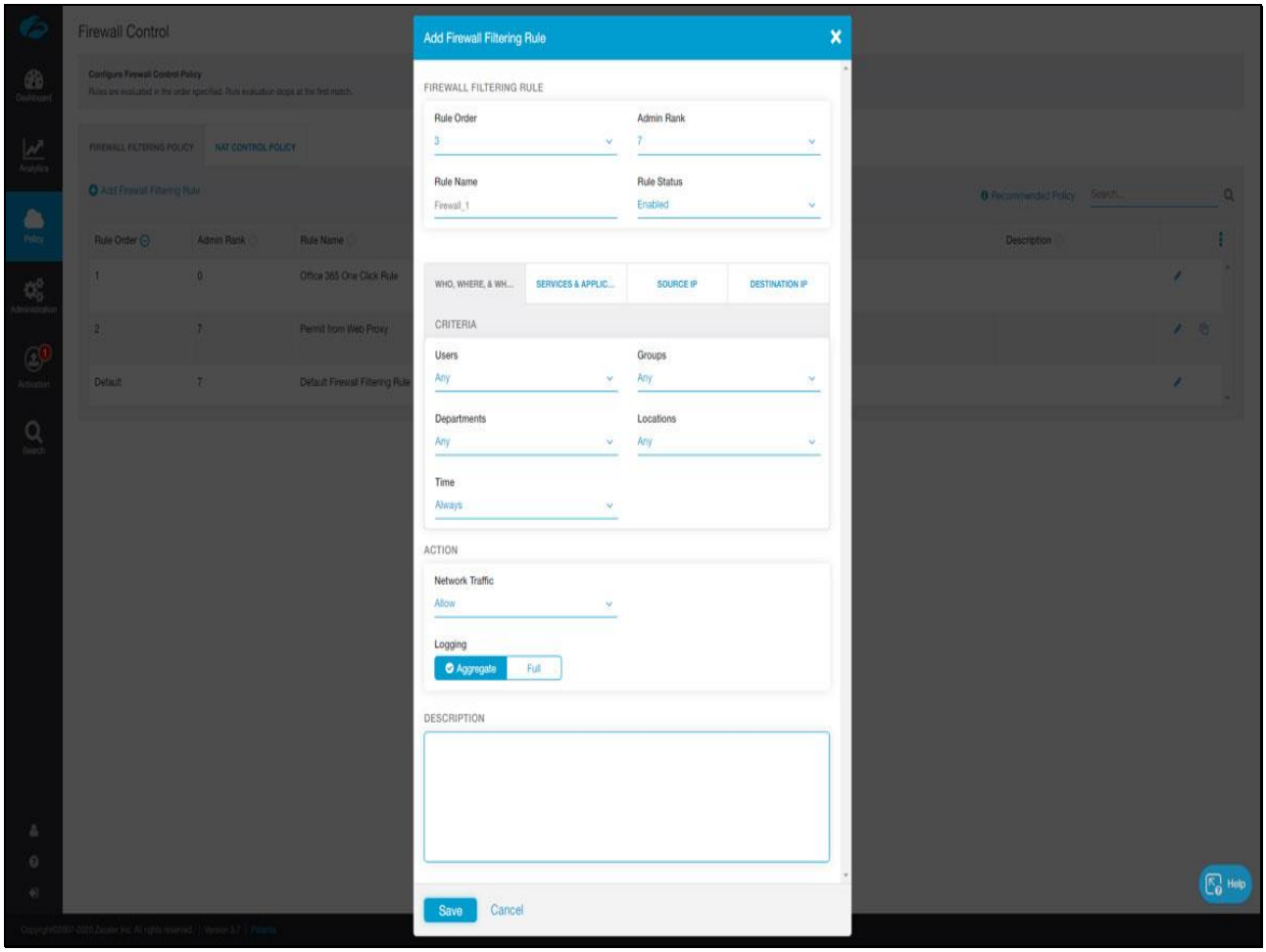
Slide 97 - Slide 97



Slide notes

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

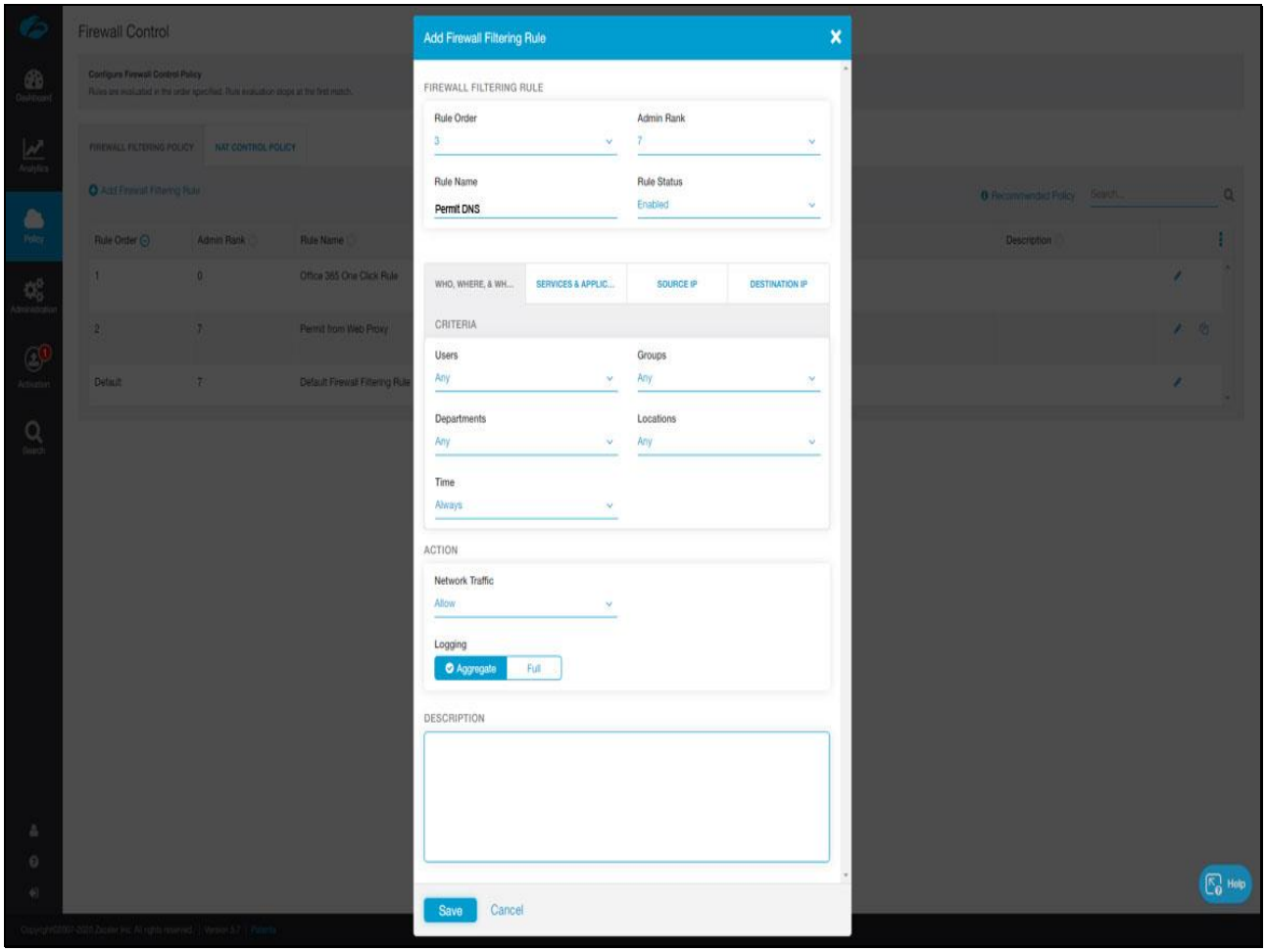
Slide 98 - Slide 98



Slide notes

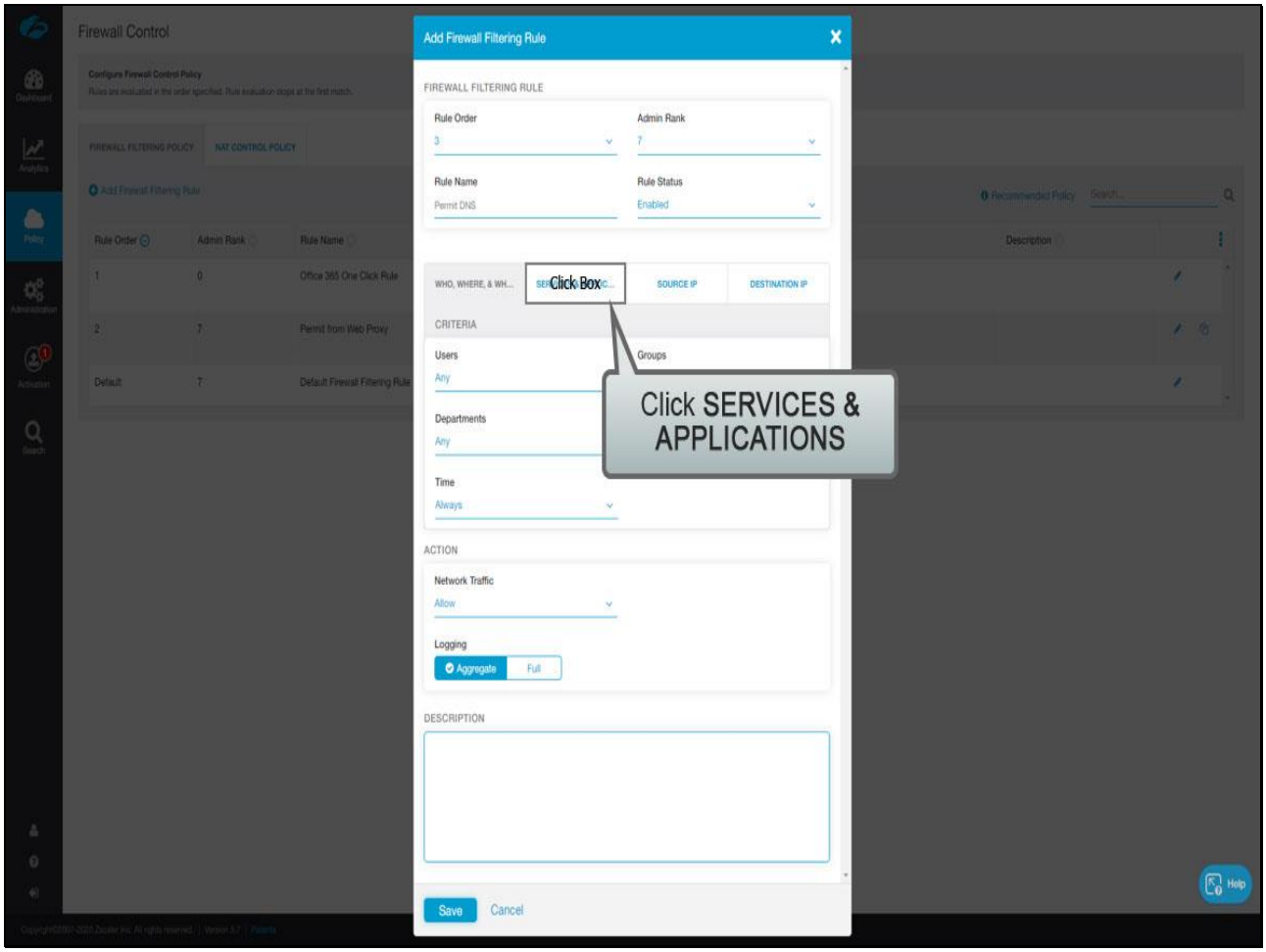
For ‘Rule Name’ we will use Permit DNS. Click the **Services & Applications** tab.

Slide 99 - Slide 99



Slide notes

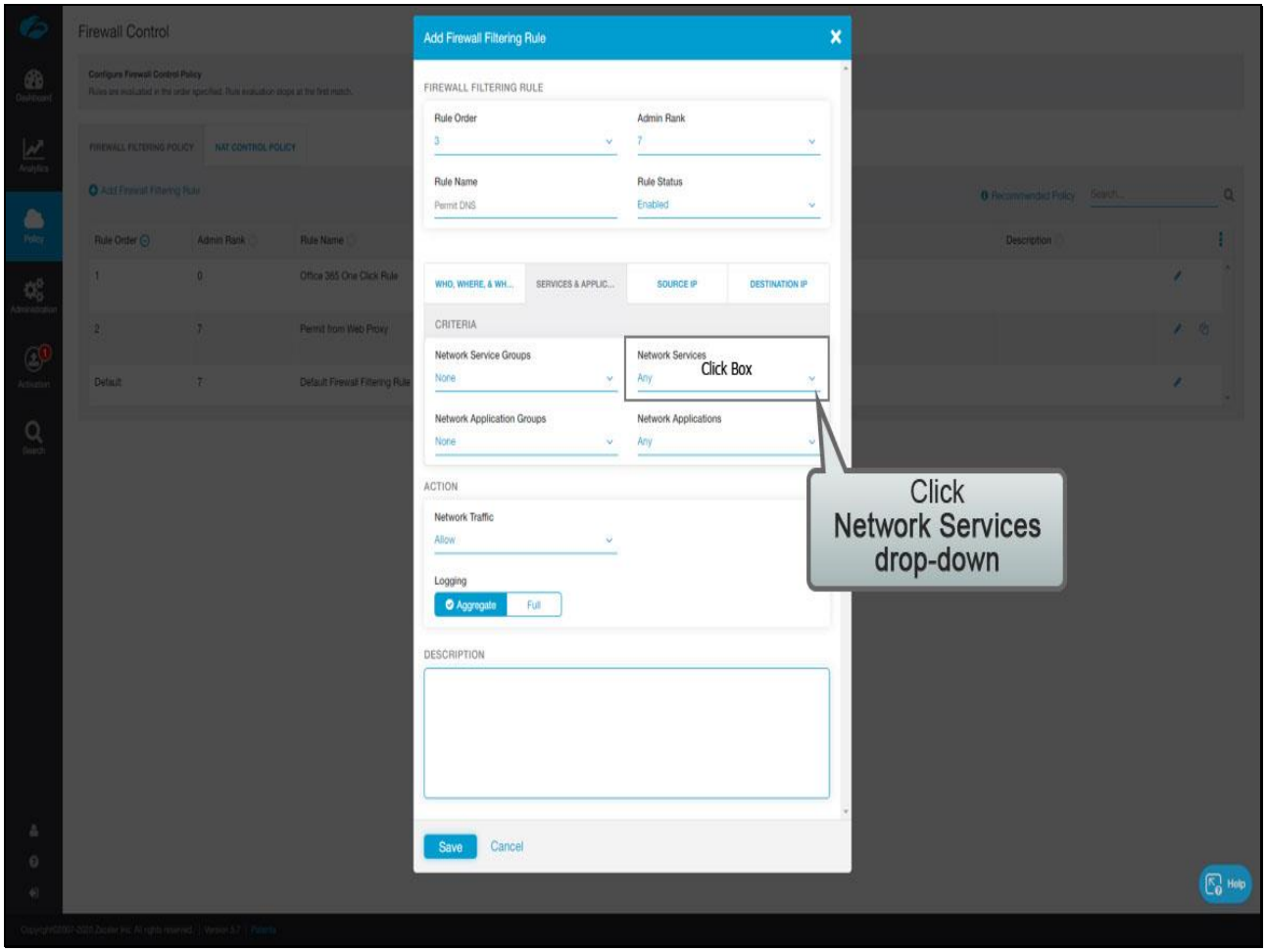
Slide 100 - Slide 100



Slide notes

Click the **Services & Applications** tab.

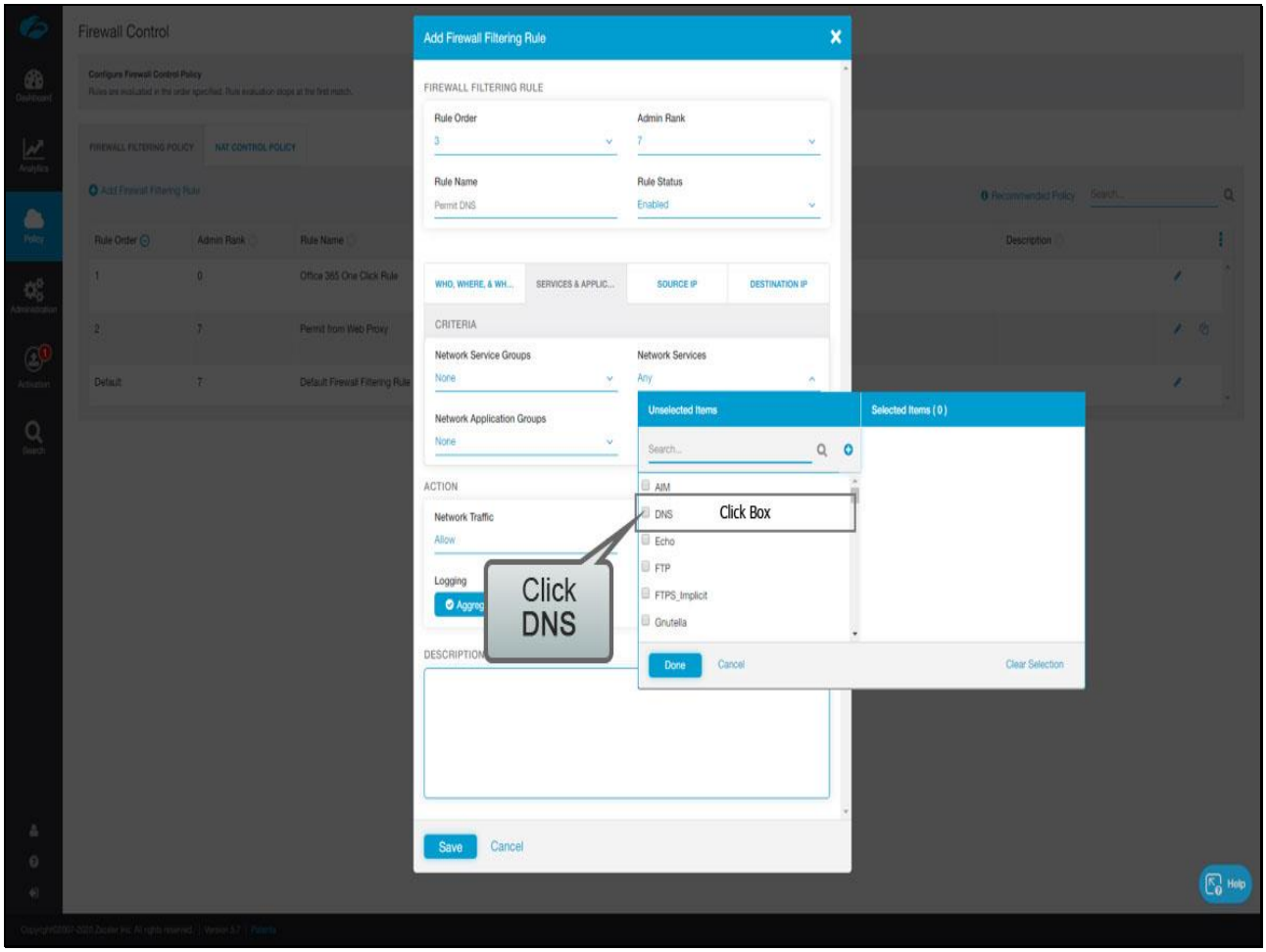
Slide 101 - Slide 101



Slide notes

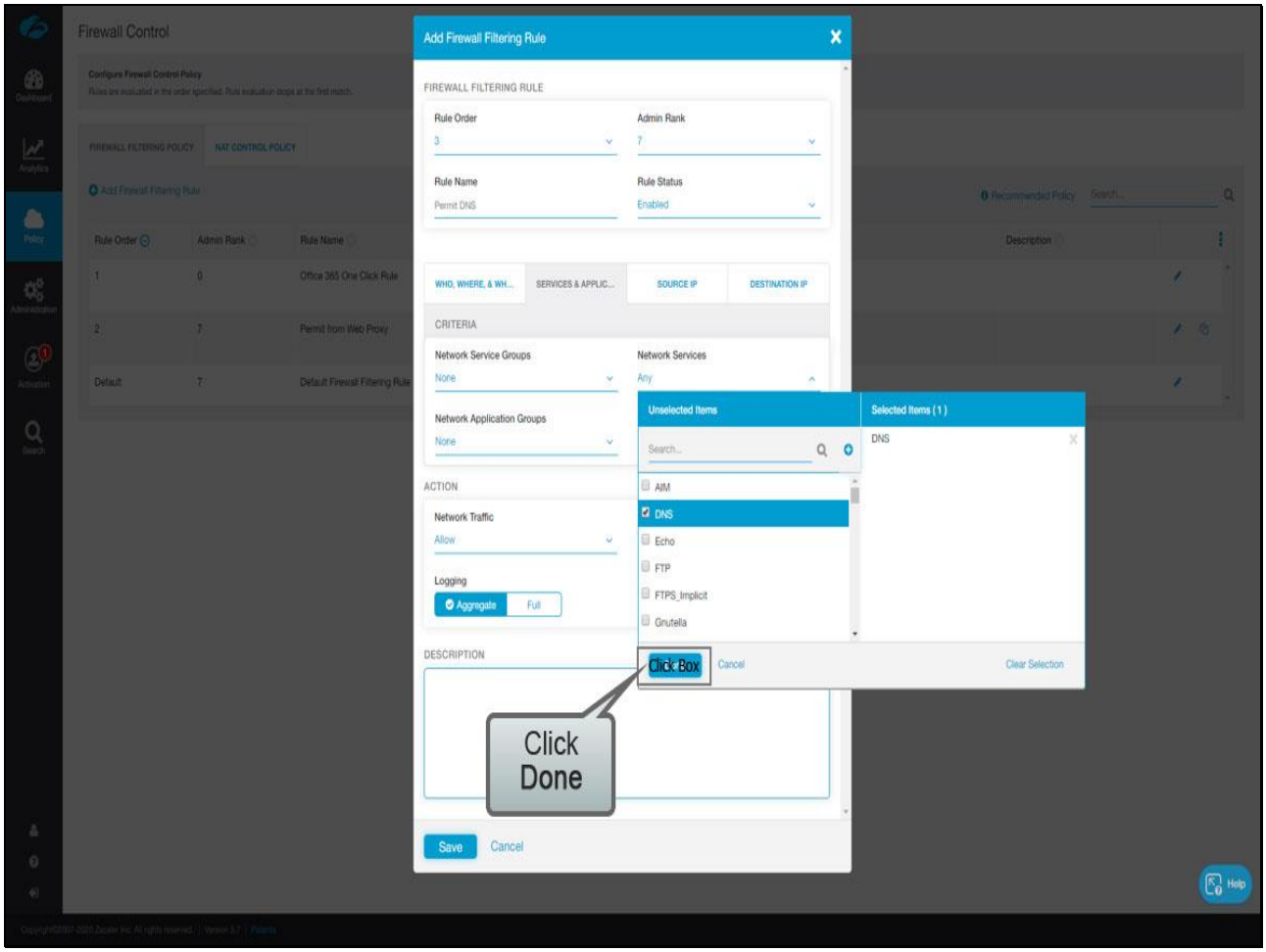
From the **Network Services** drop-down, select **DNS**, then click **Done**.

Slide 102 - Slide 102



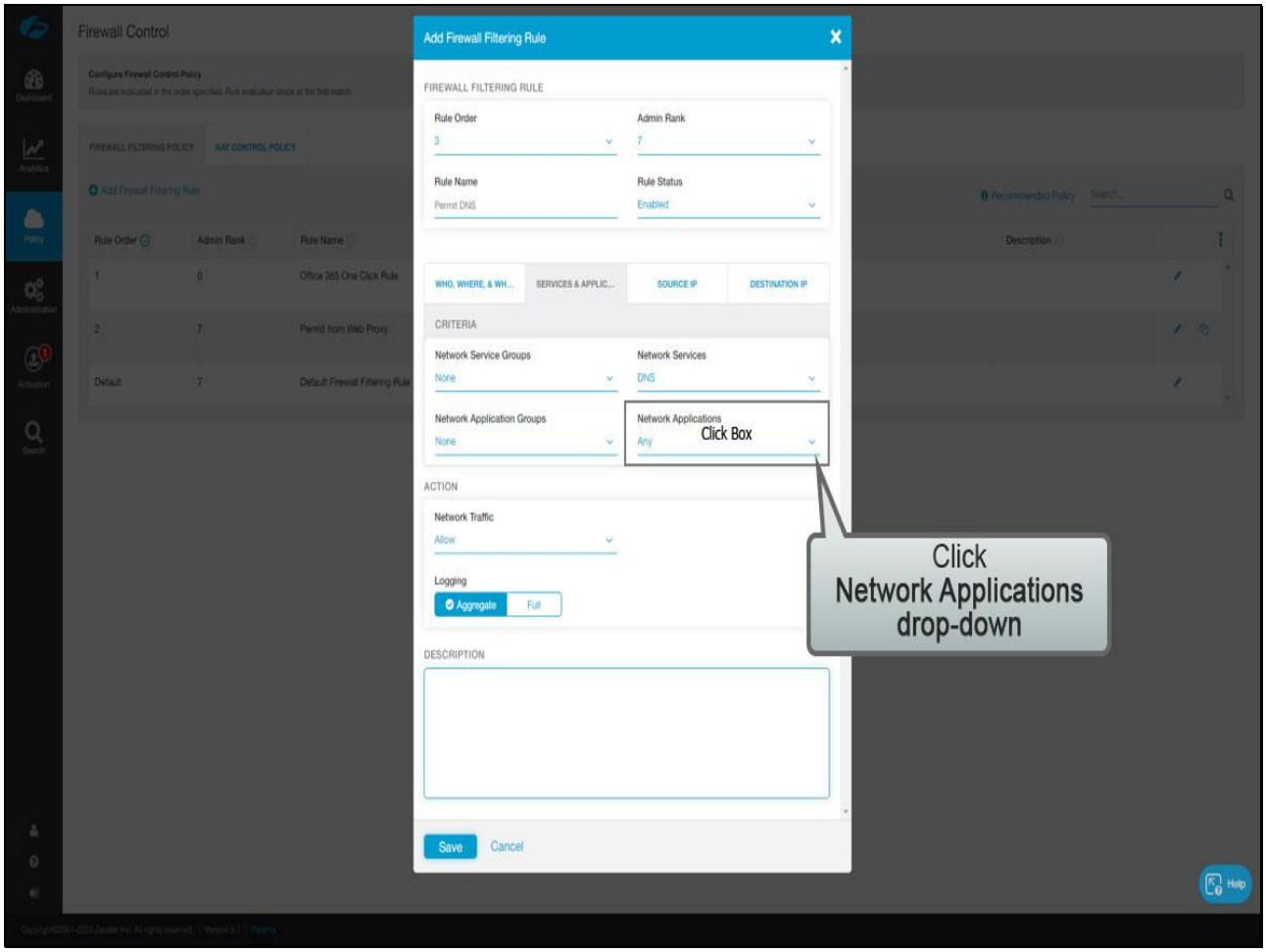
Slide notes

Slide 104 - Slide 104



Slide notes

Slide 105 - Slide 105

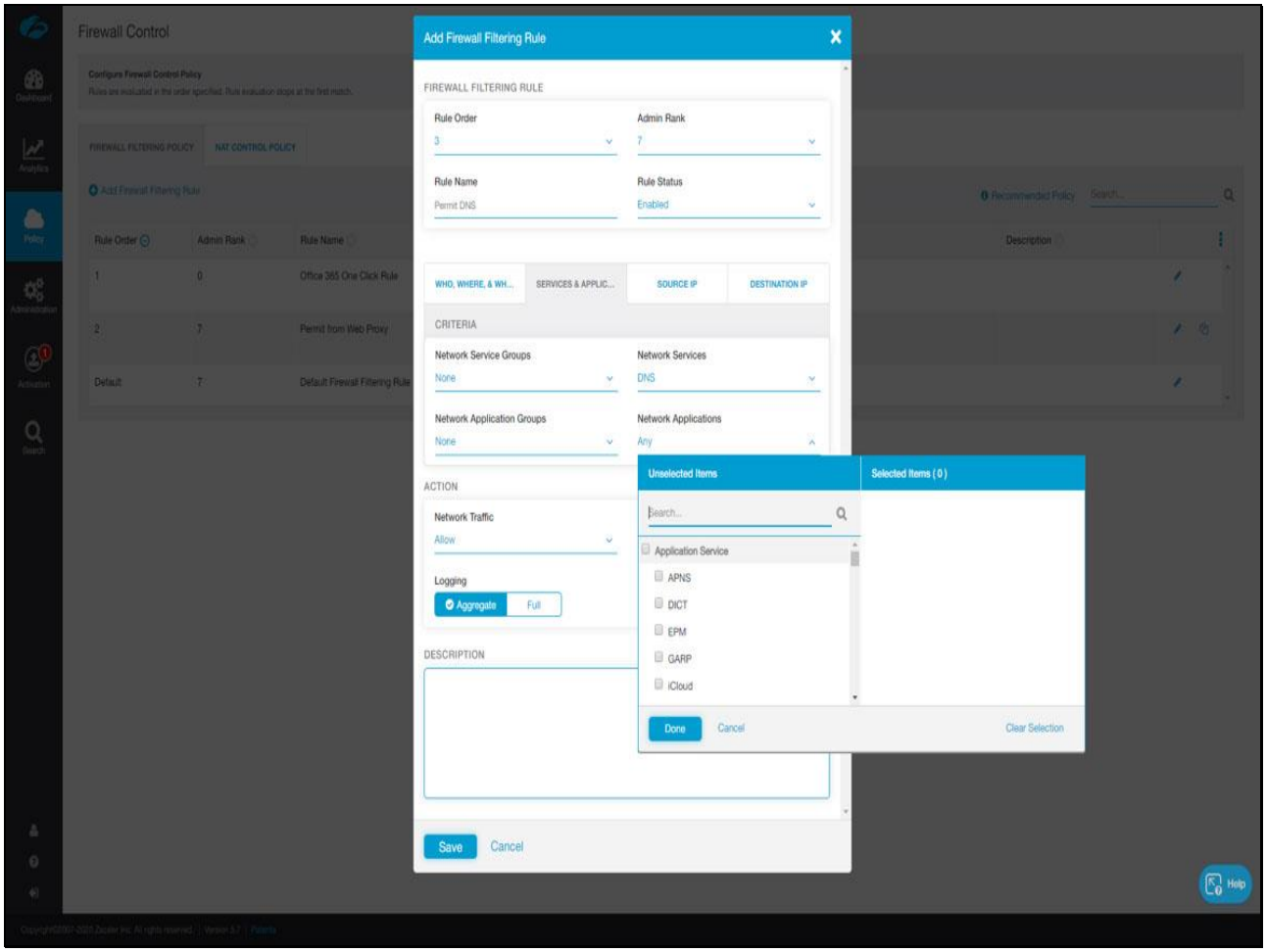


Slide notes

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

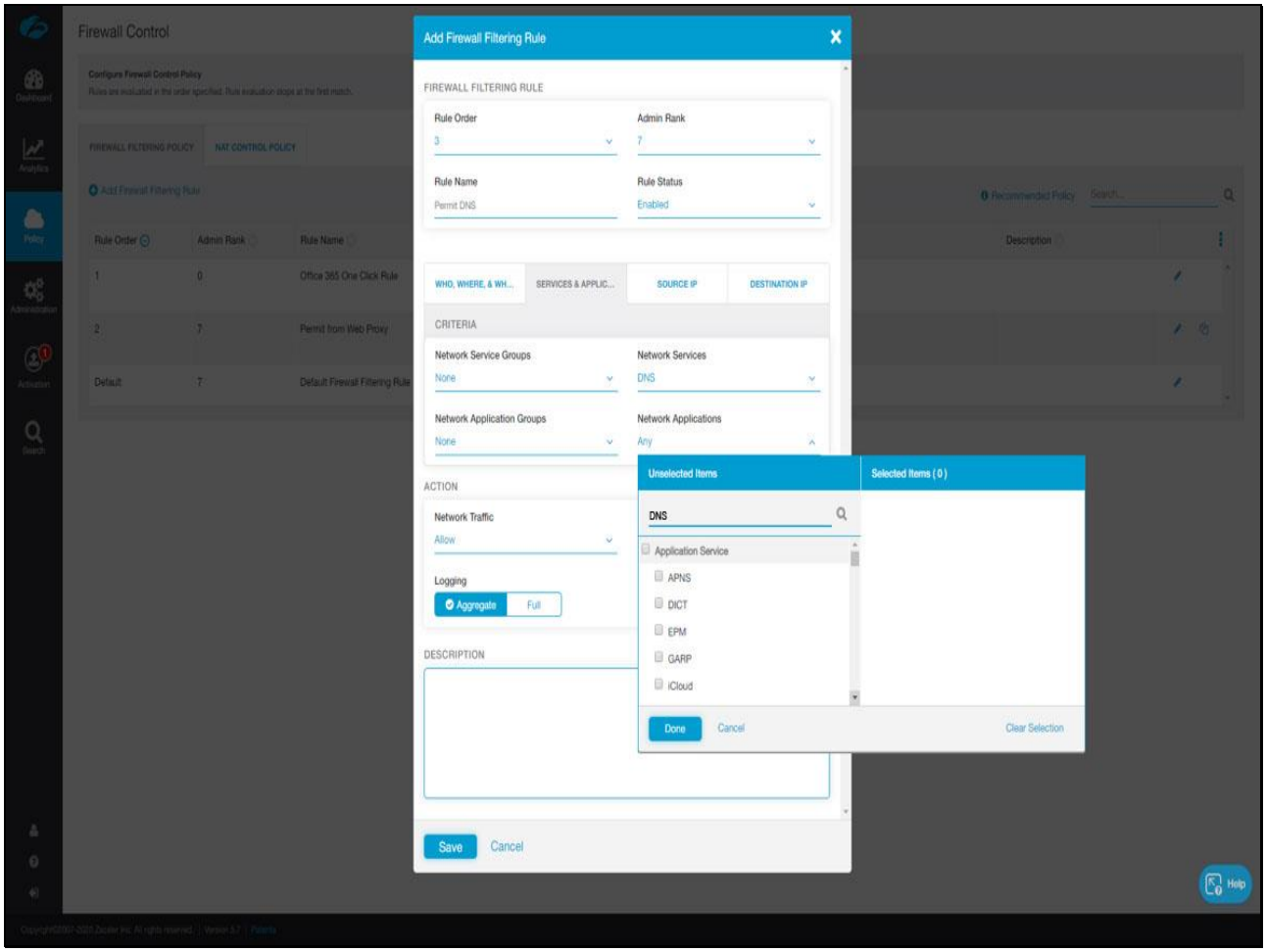
Slide 106 - Slide 106



Slide notes

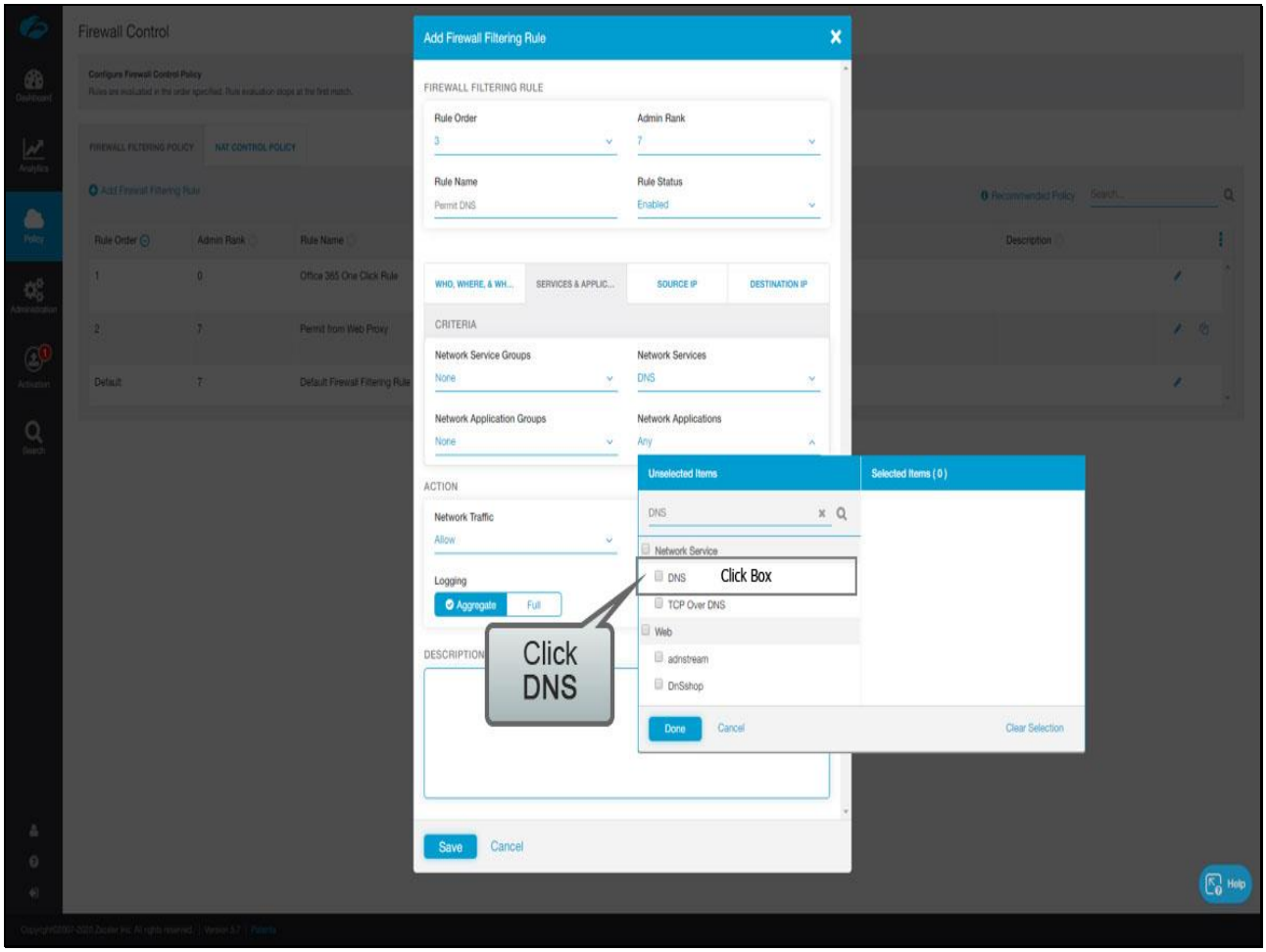
select **DNS**, then **Done**, then save this rule.

Slide 107 - Slide 107



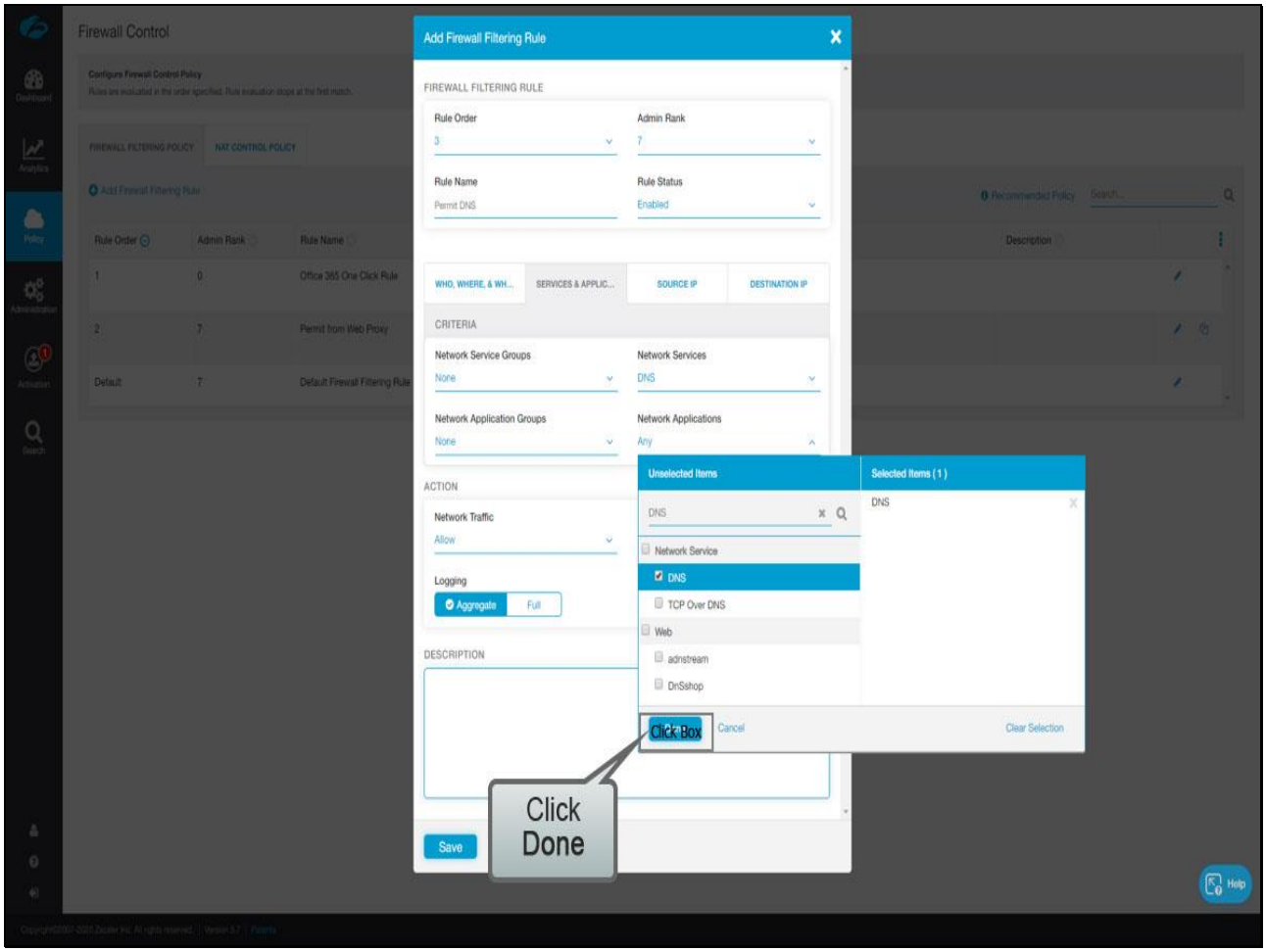
Slide notes

Slide 108 - Slide 108



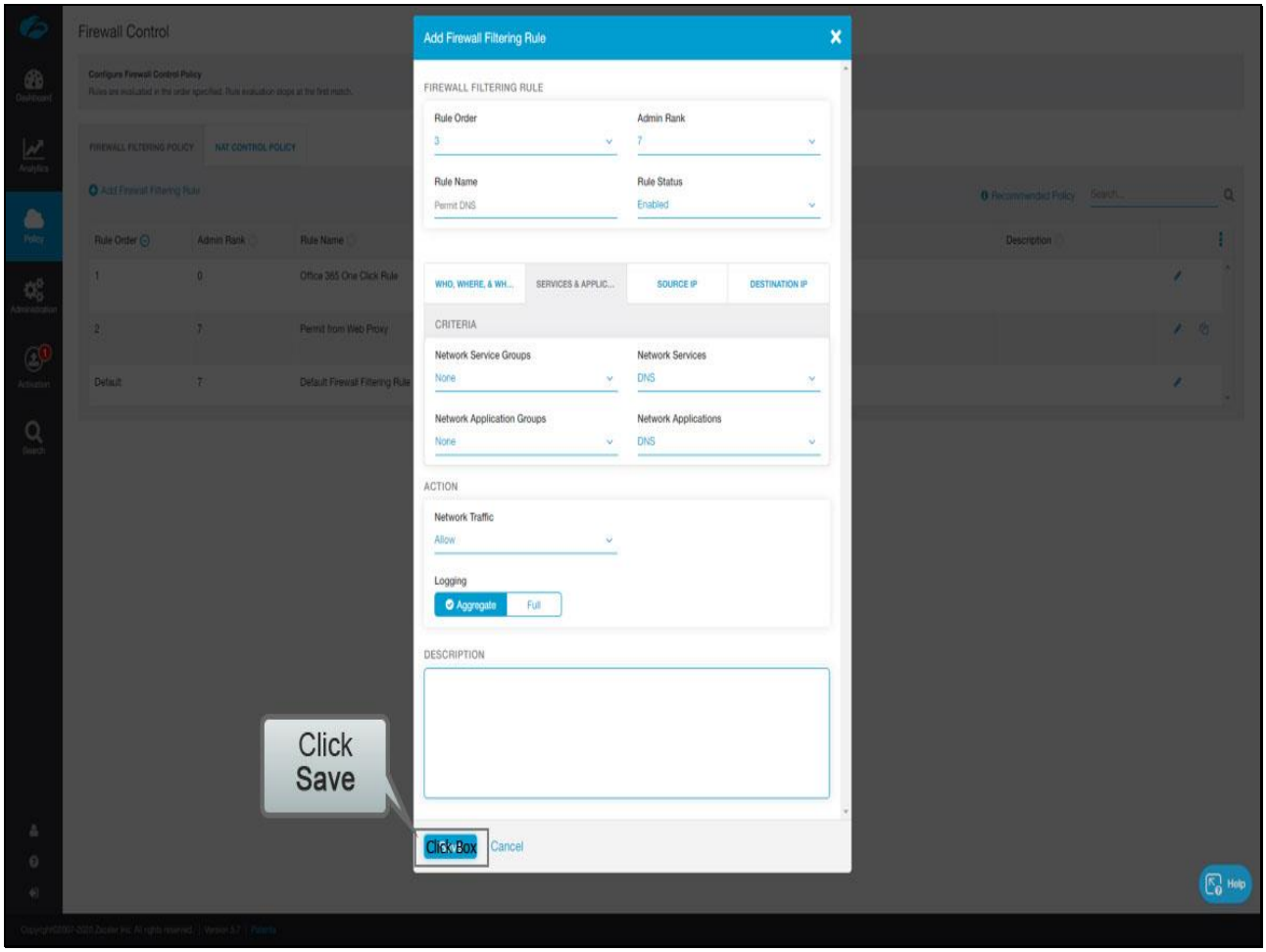
Slide notes

Slide 109 - Slide 109



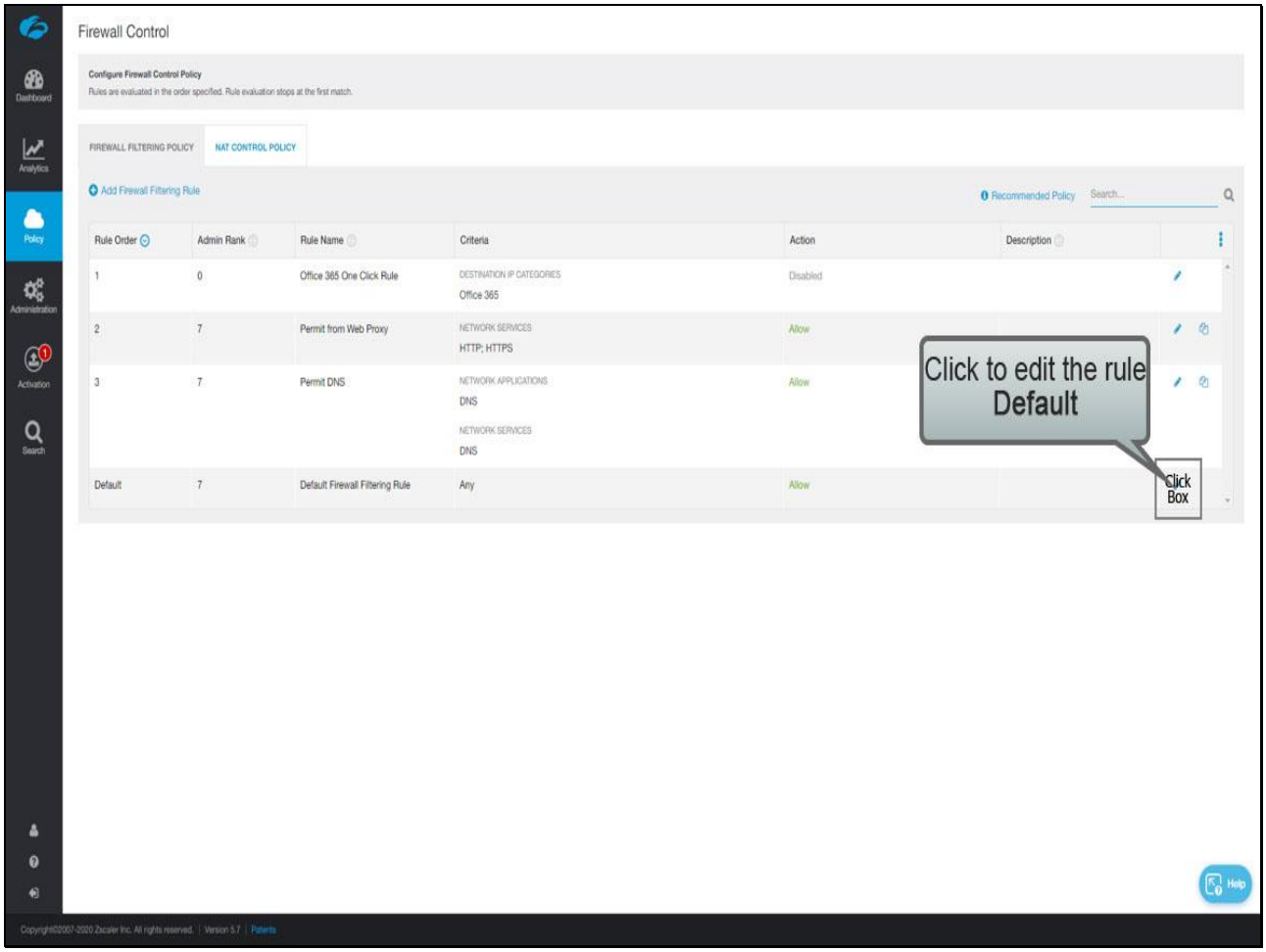
Slide notes

Slide 110 - Slide 110



Slide notes

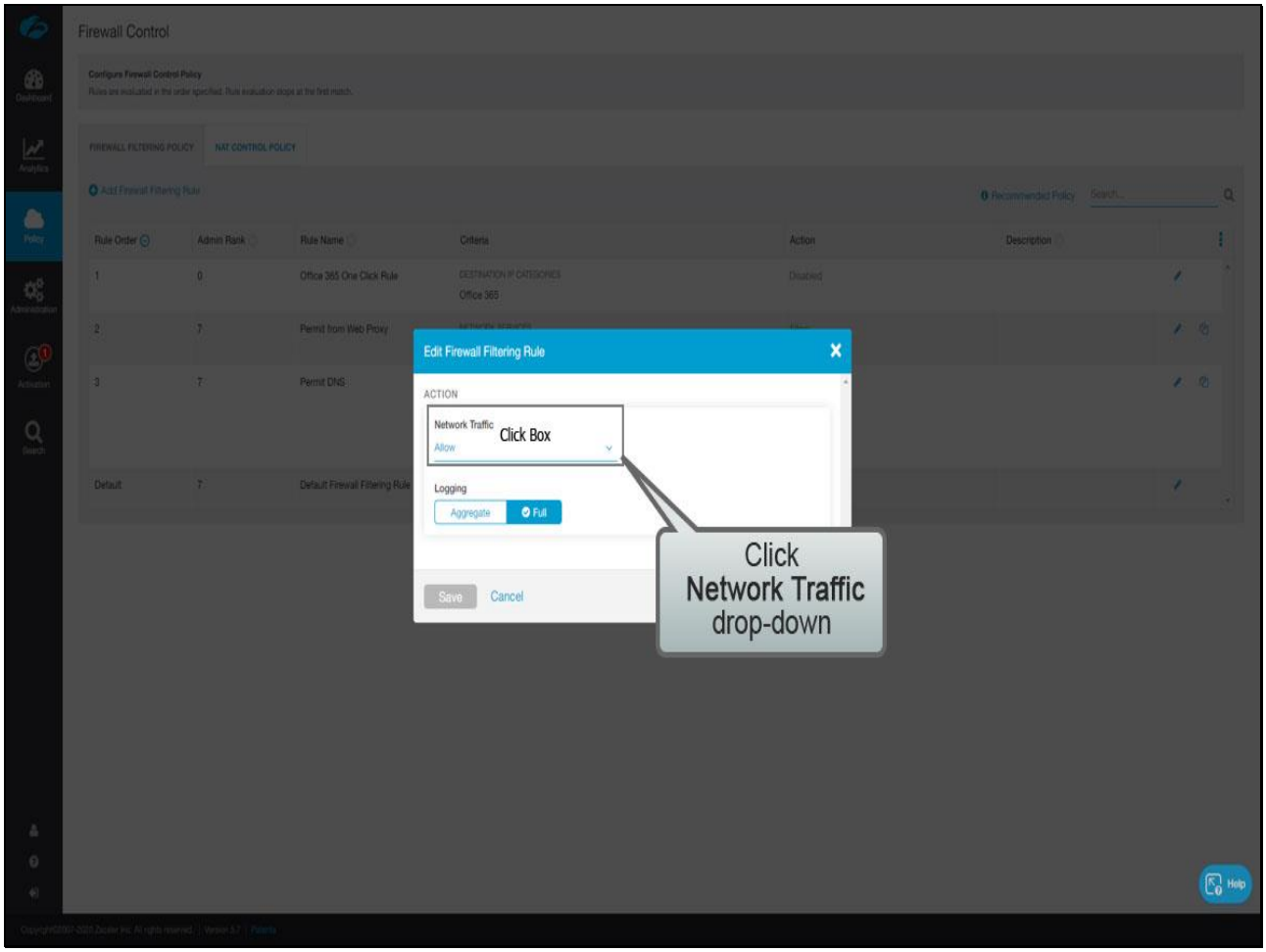
Slide 115 - Slide 115



Slide notes

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

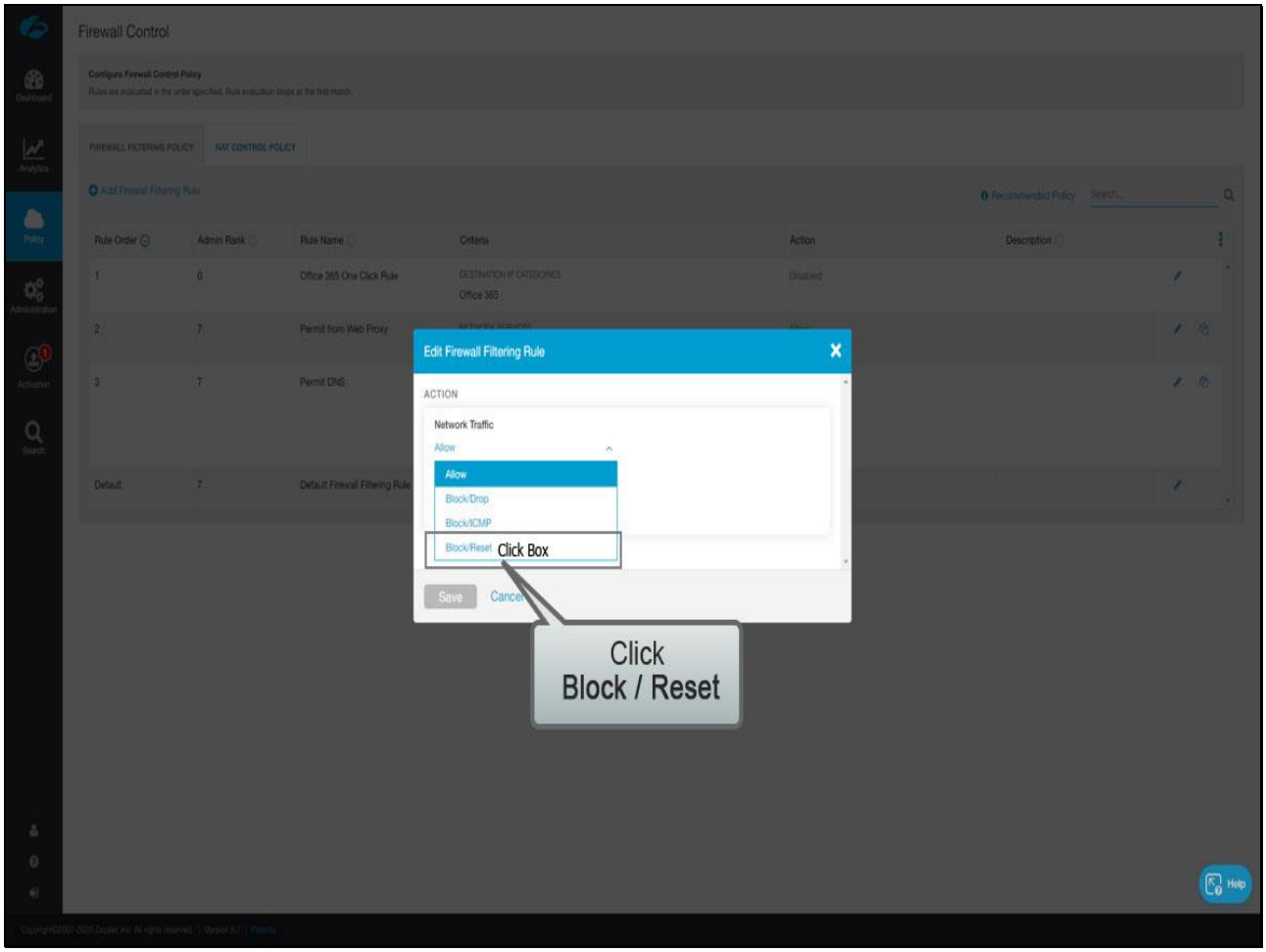
Slide 116 - Slide 116



Slide notes

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

Slide 117 - Slide 117

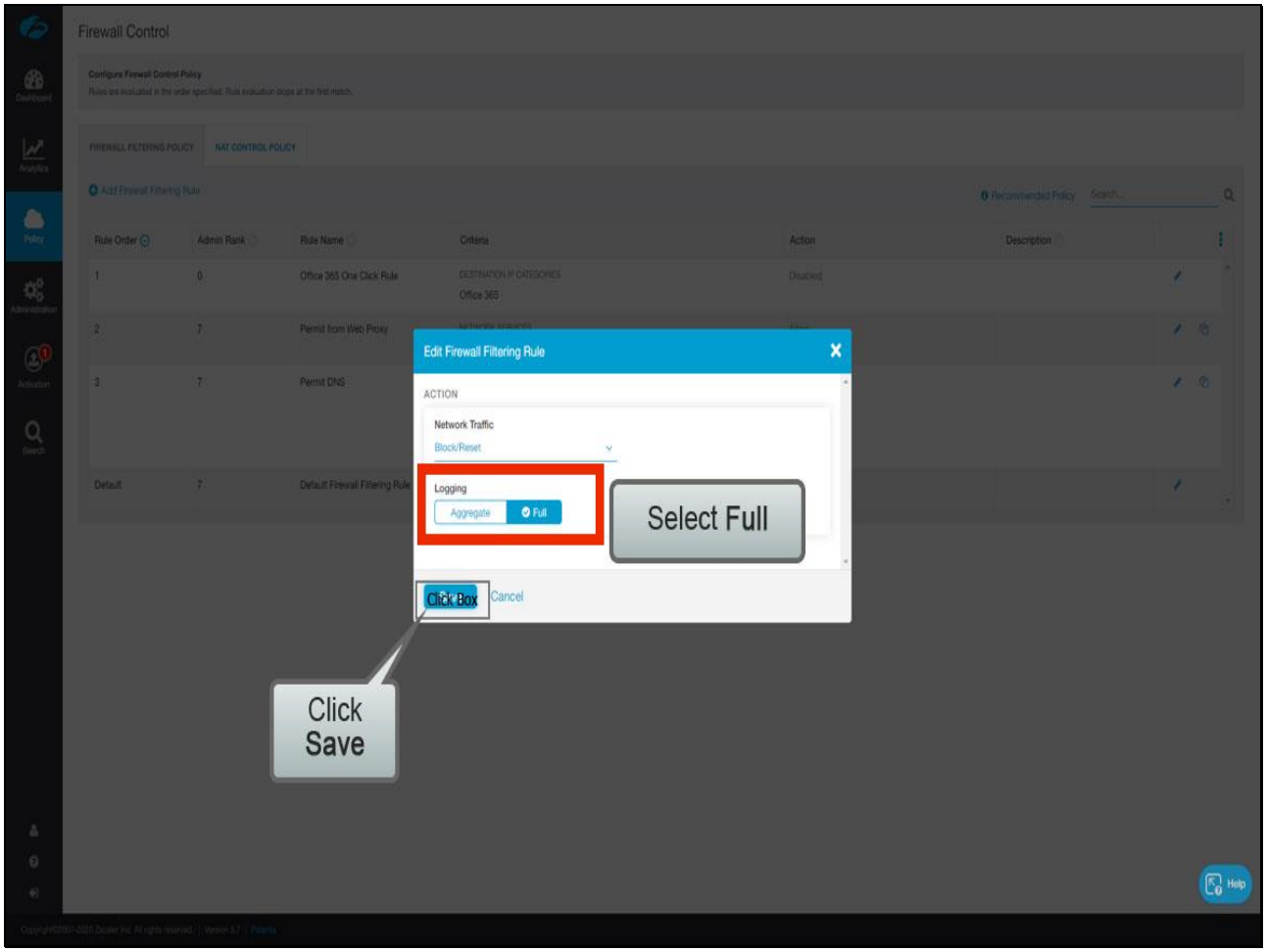


Slide notes

...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**.

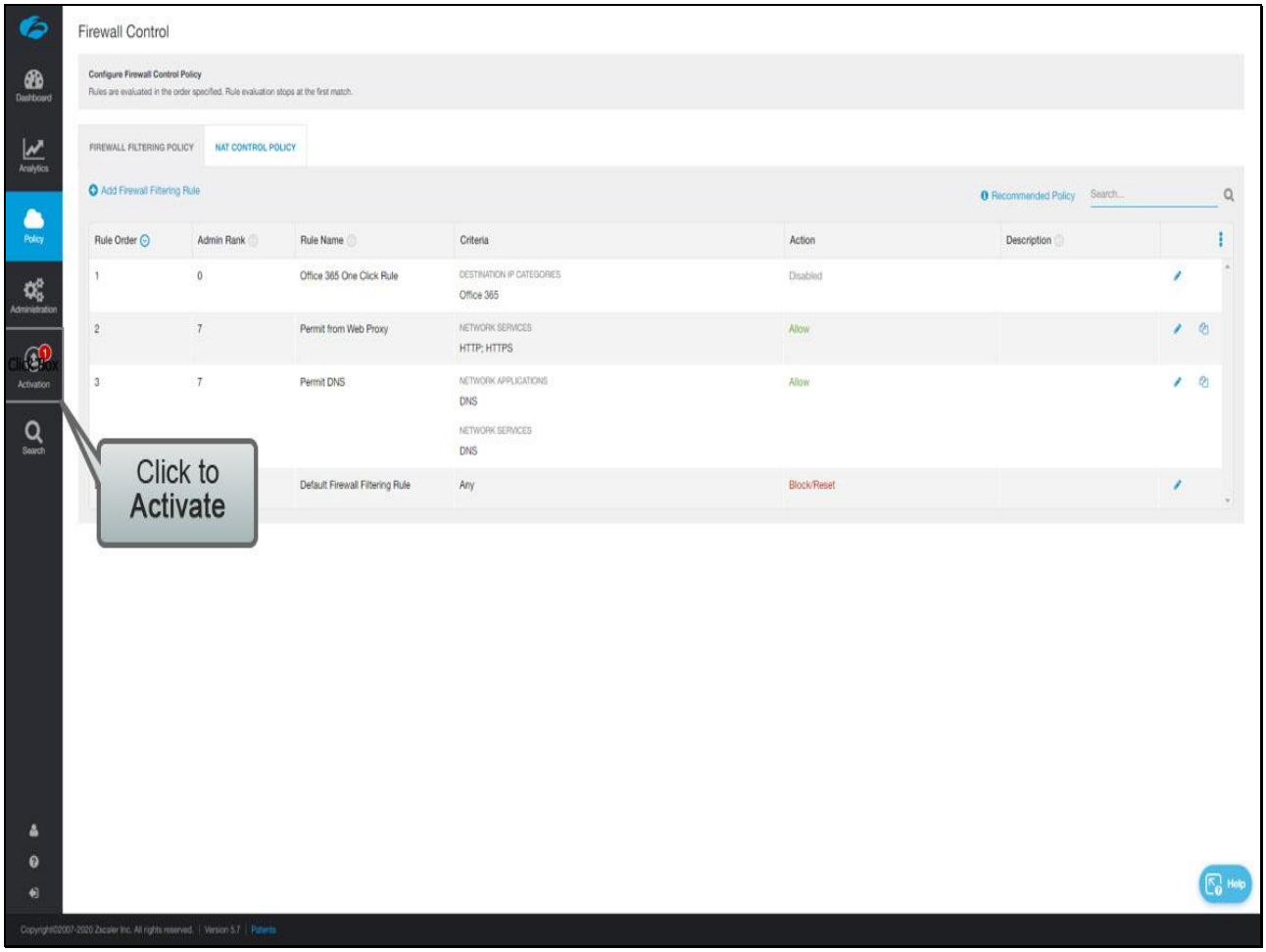
Slide 118 - Slide 118



Slide notes

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

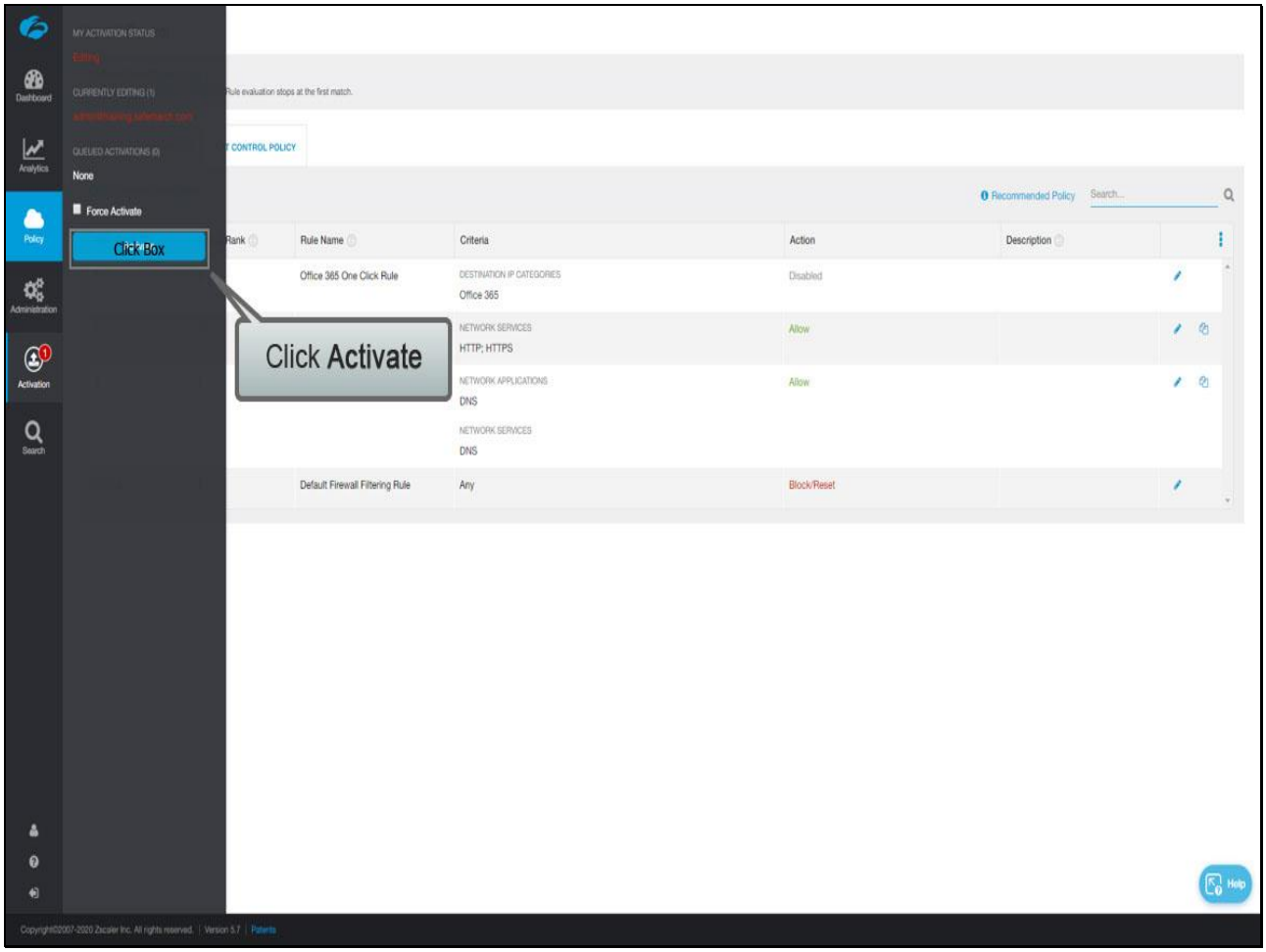
Slide 122 - Slide 122



Slide notes

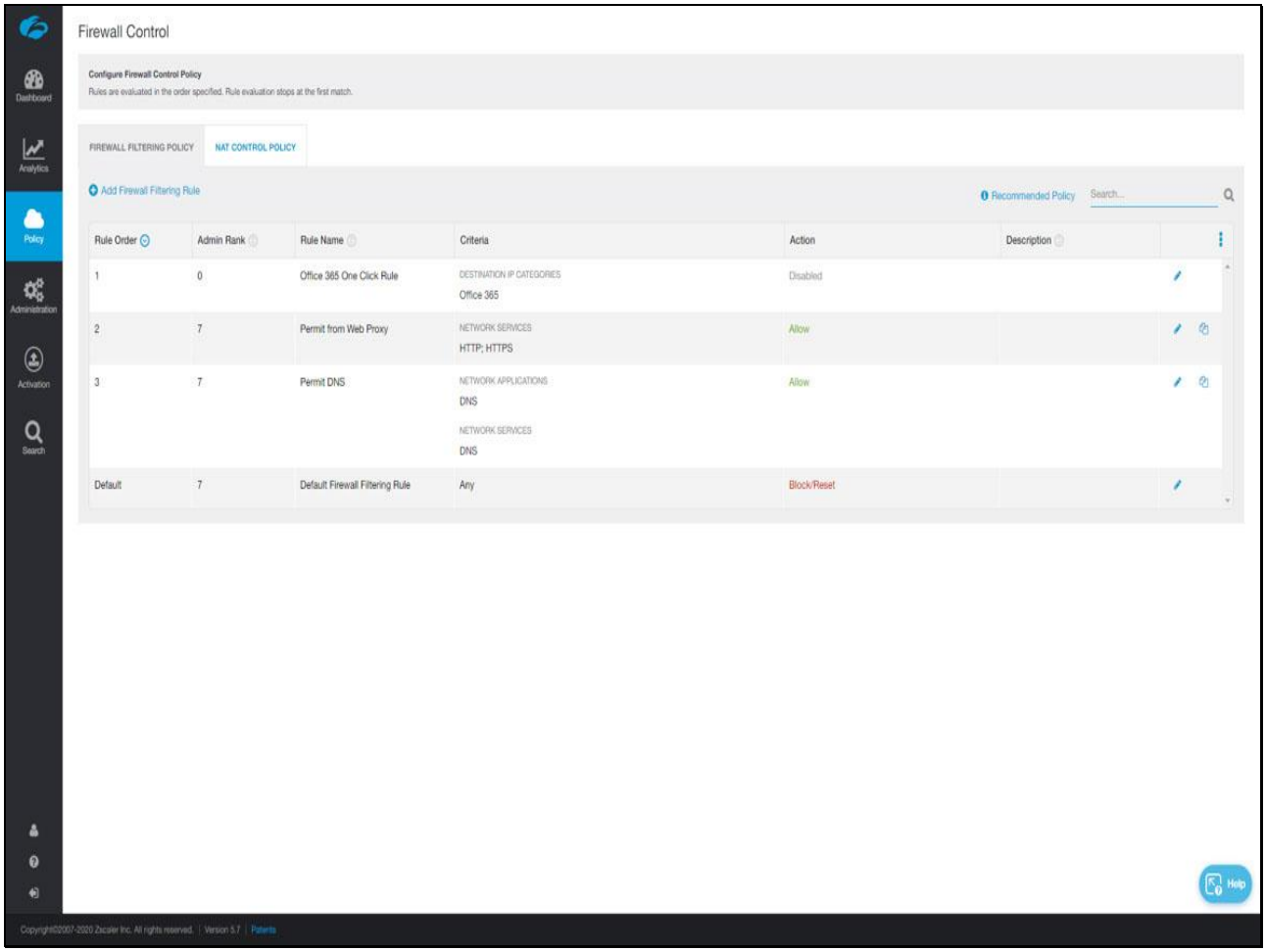
Then **Activate** your changes.

Slide 123 - Slide 123



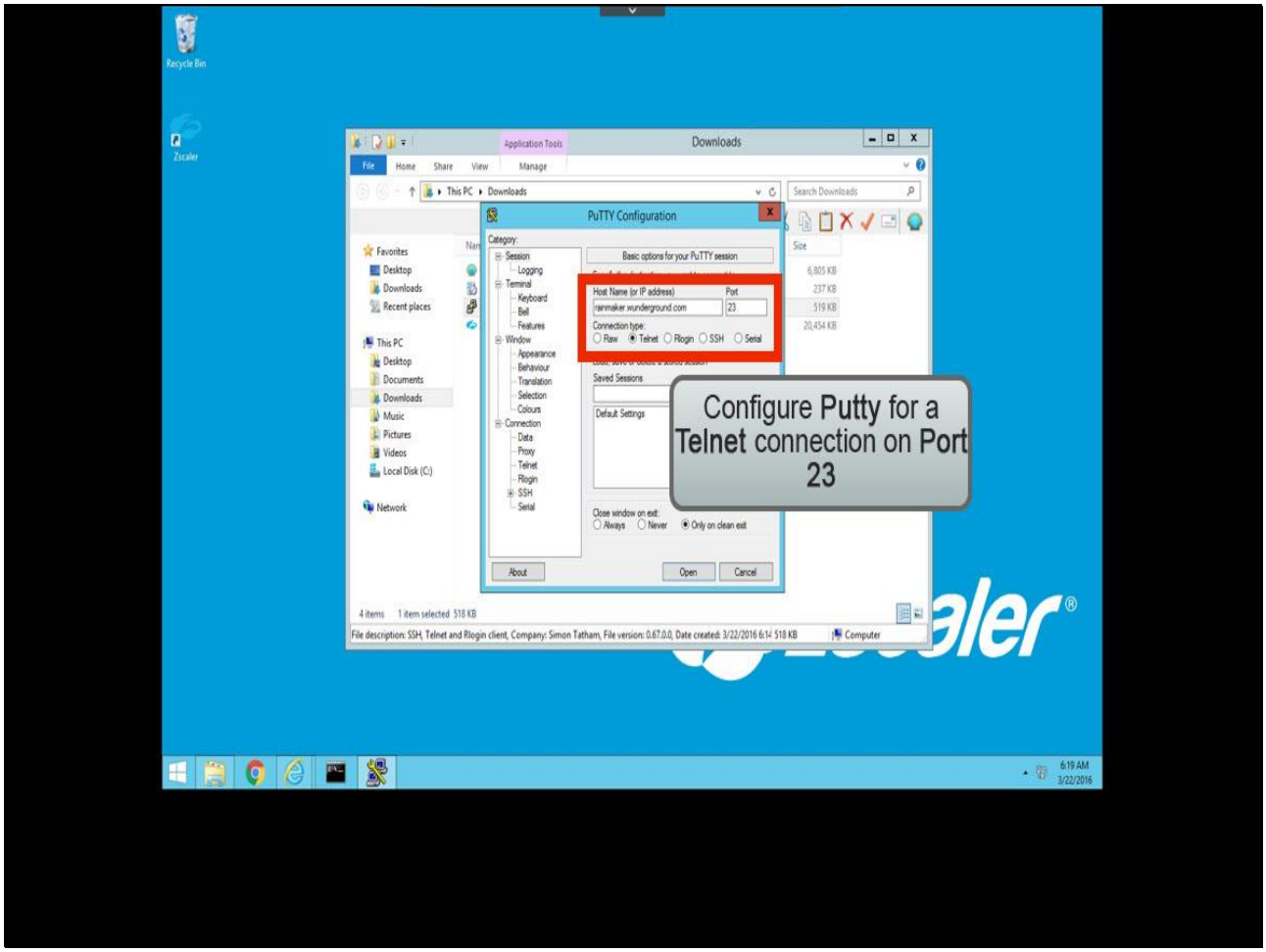
Slide notes

Slide 126 - Slide 126



Slide notes

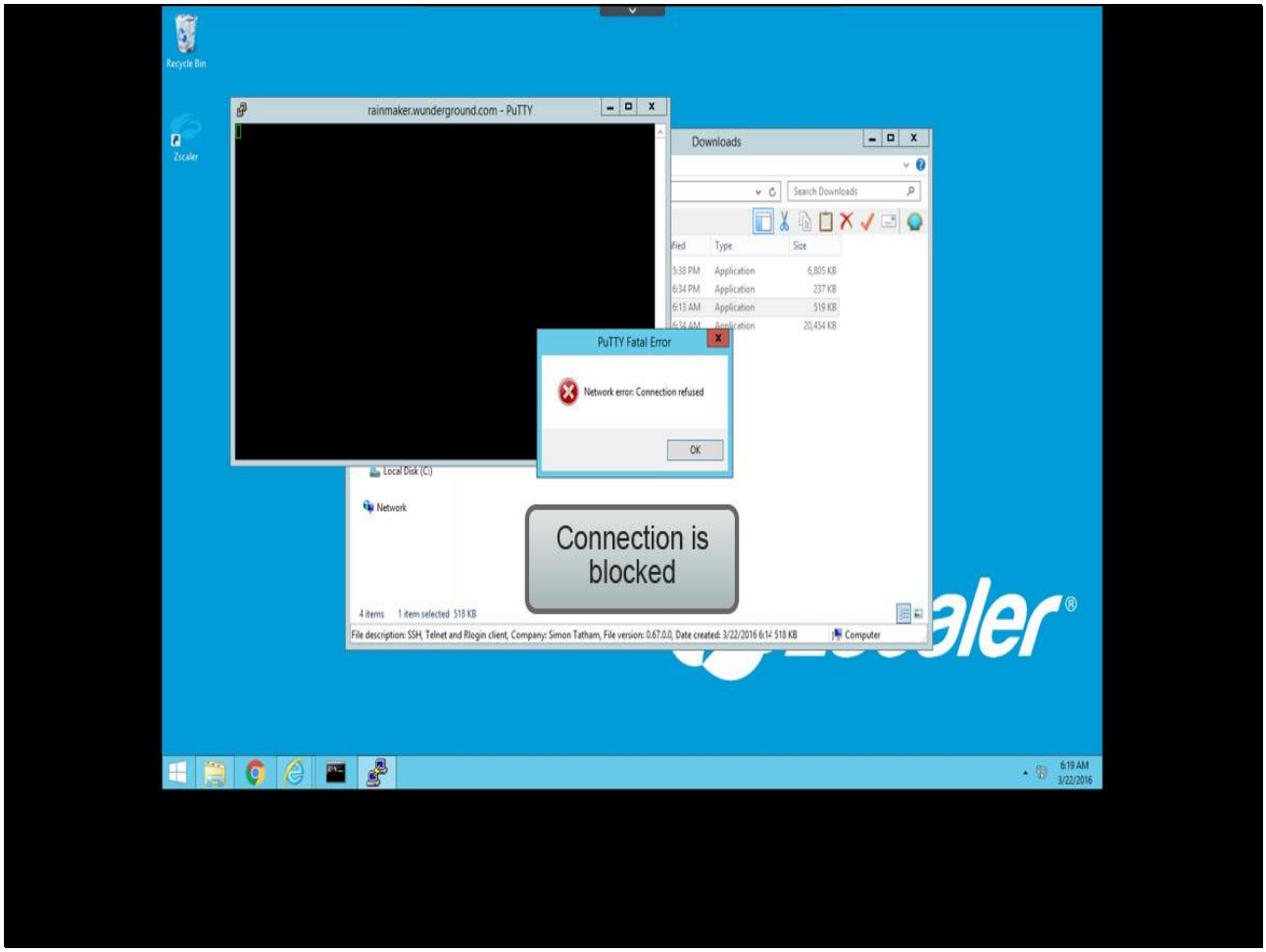
Slide 127 - Slide 127



Slide notes

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

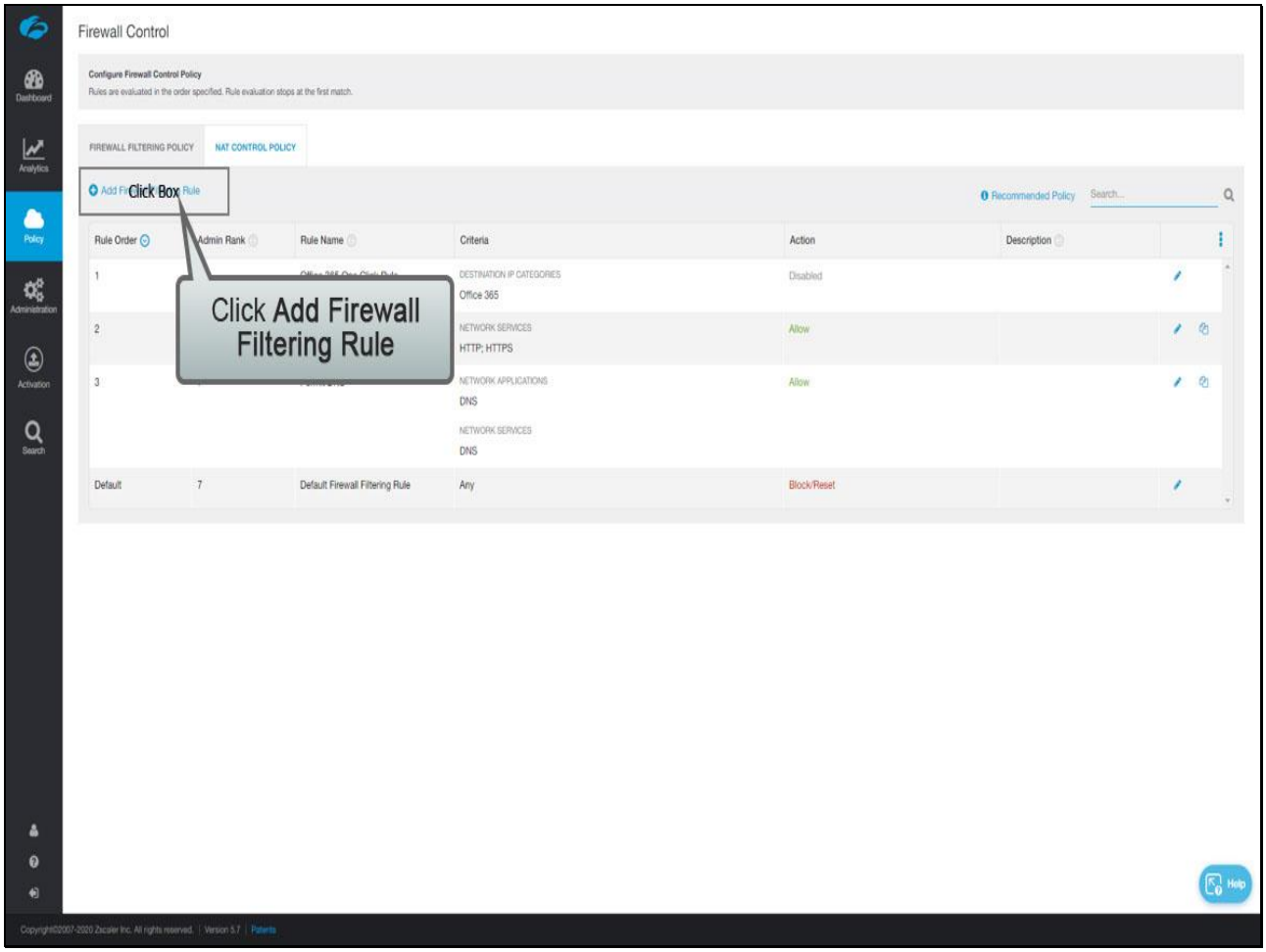
Slide 128 - Slide 128



Slide notes

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

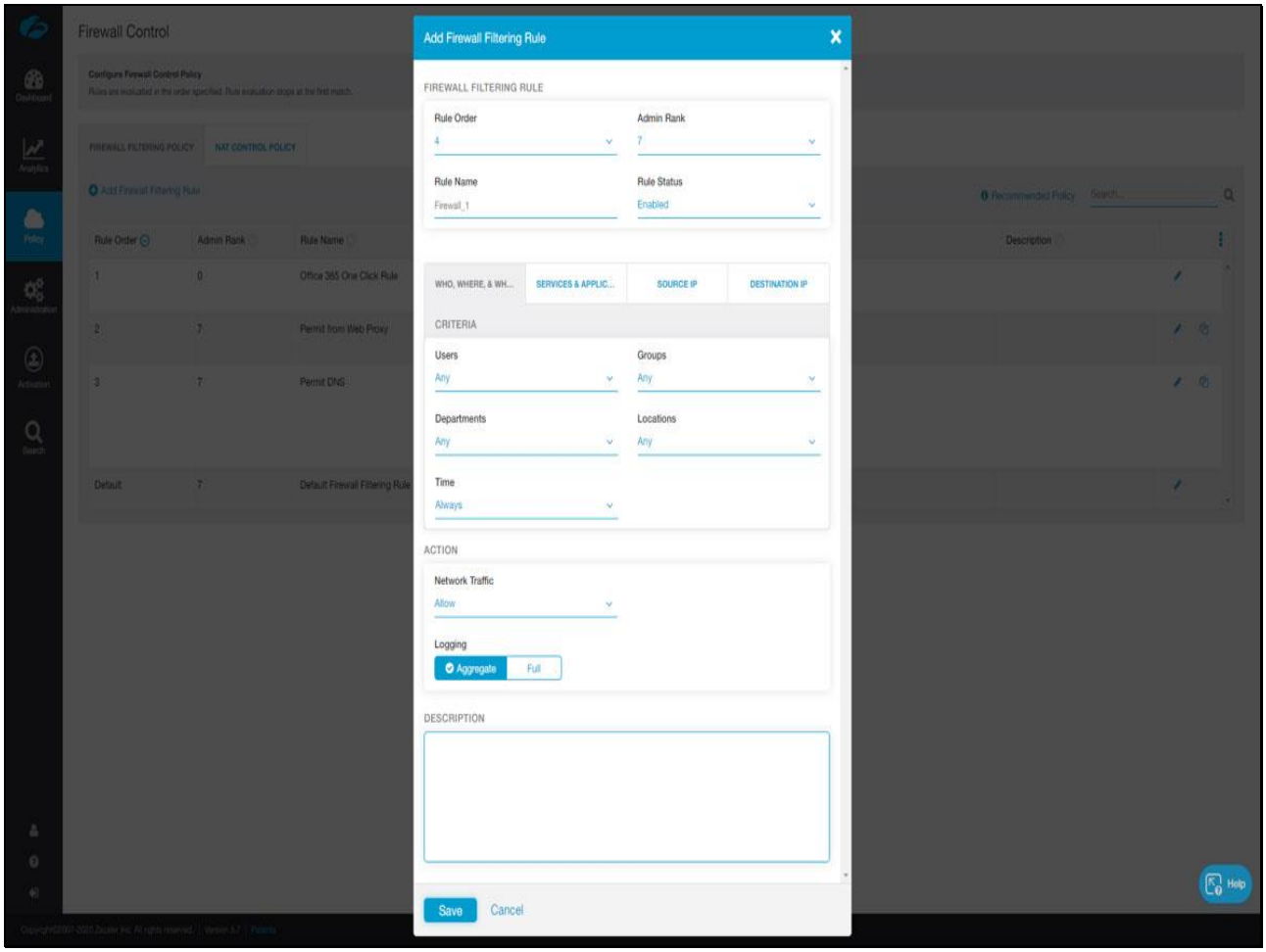
Slide 129 - Slide 129



Slide notes

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

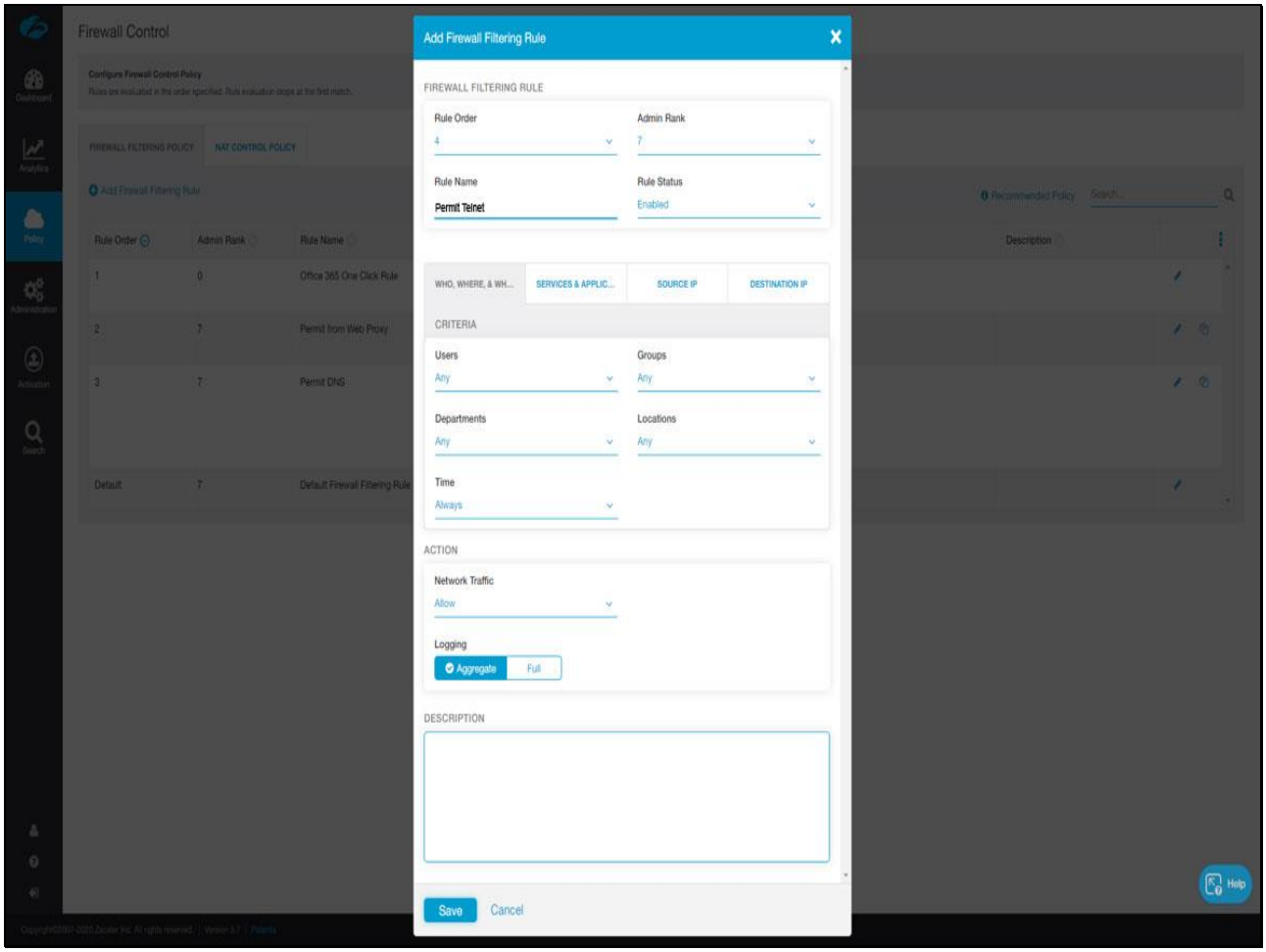
Slide 130 - Slide 130



Slide notes

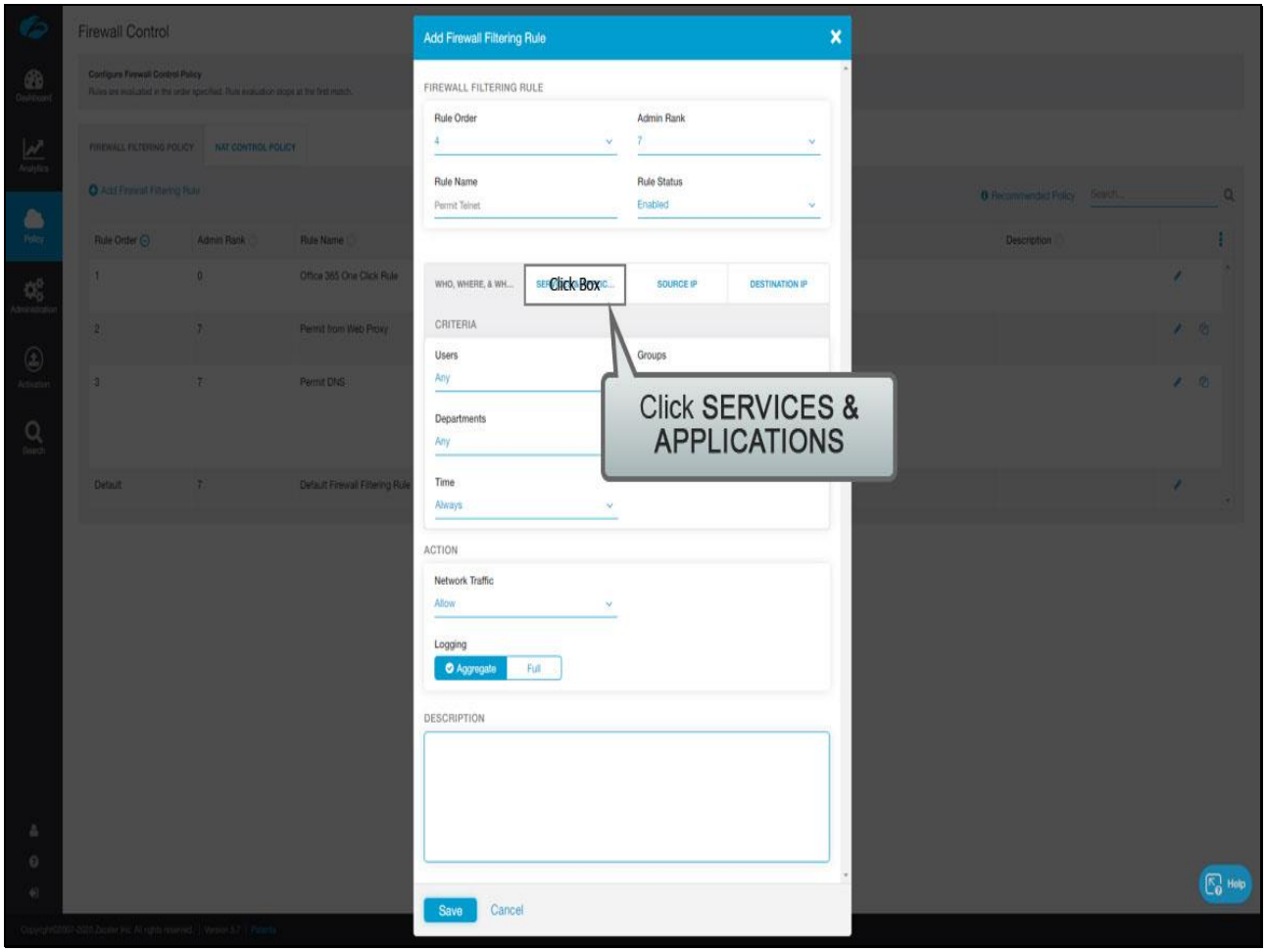
We'll name this rule **Permit Telnet**...

Slide 131 - Slide 131



Slide notes

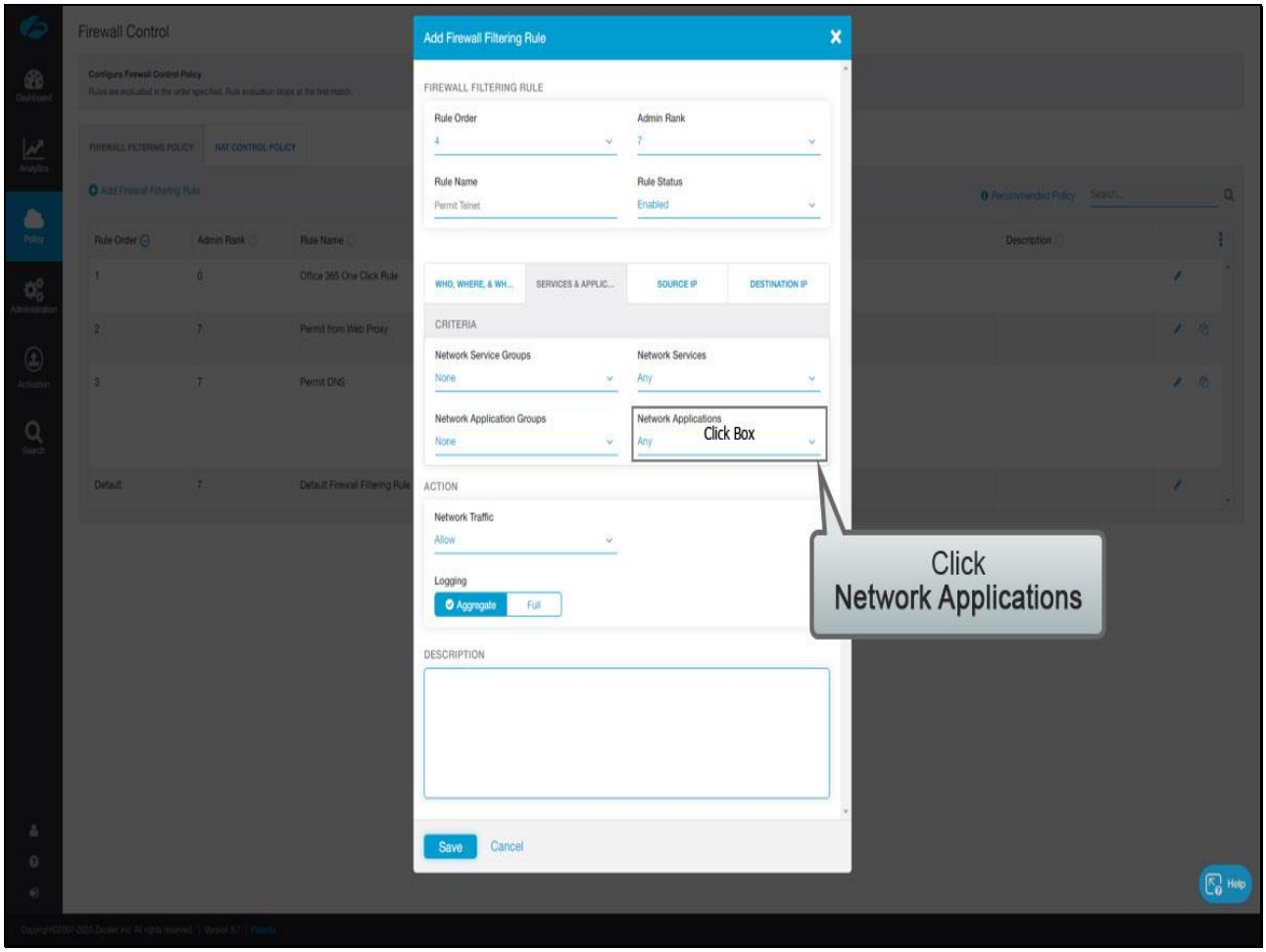
Slide 132 - Slide 132



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

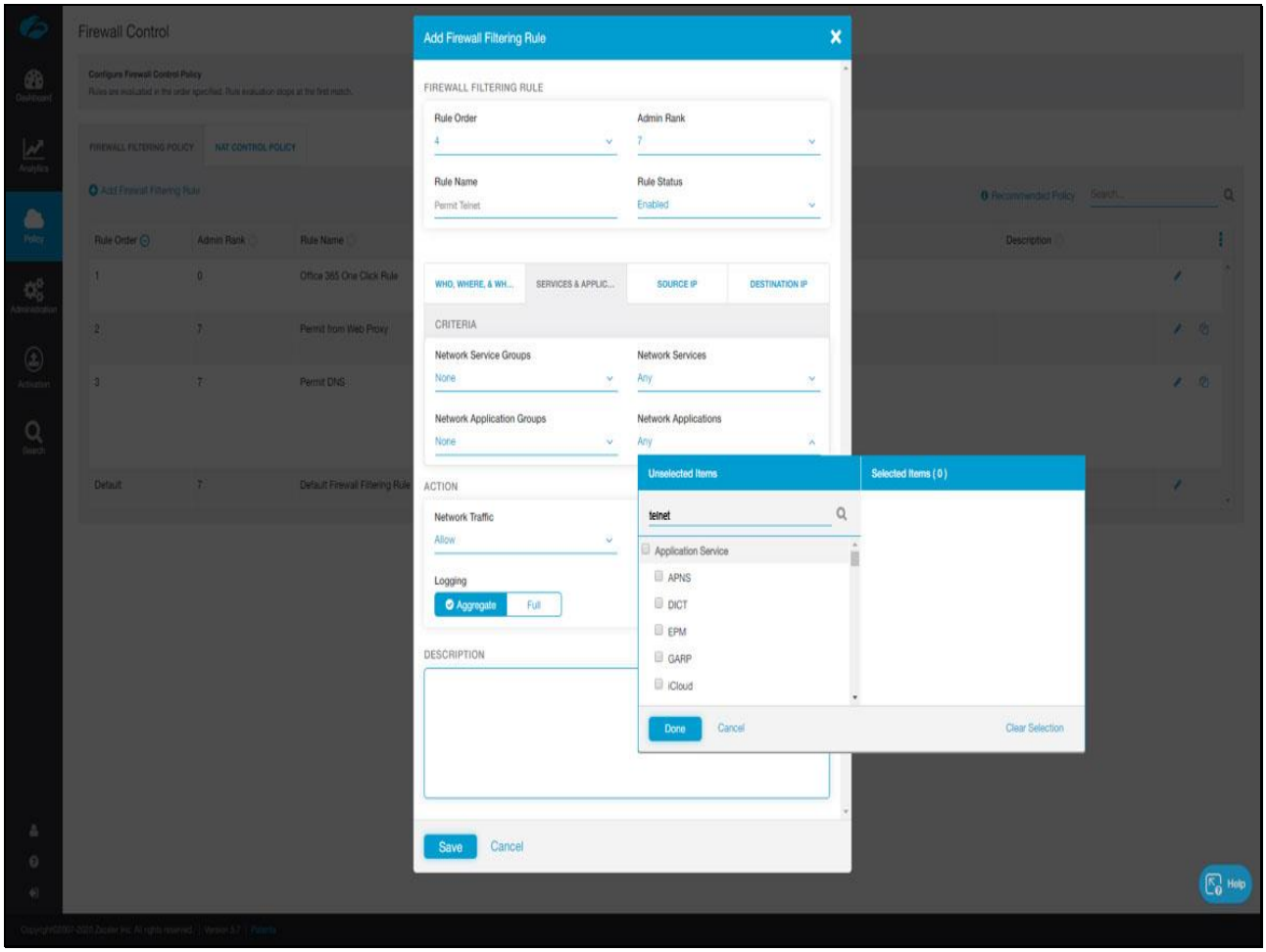


Slide notes

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.

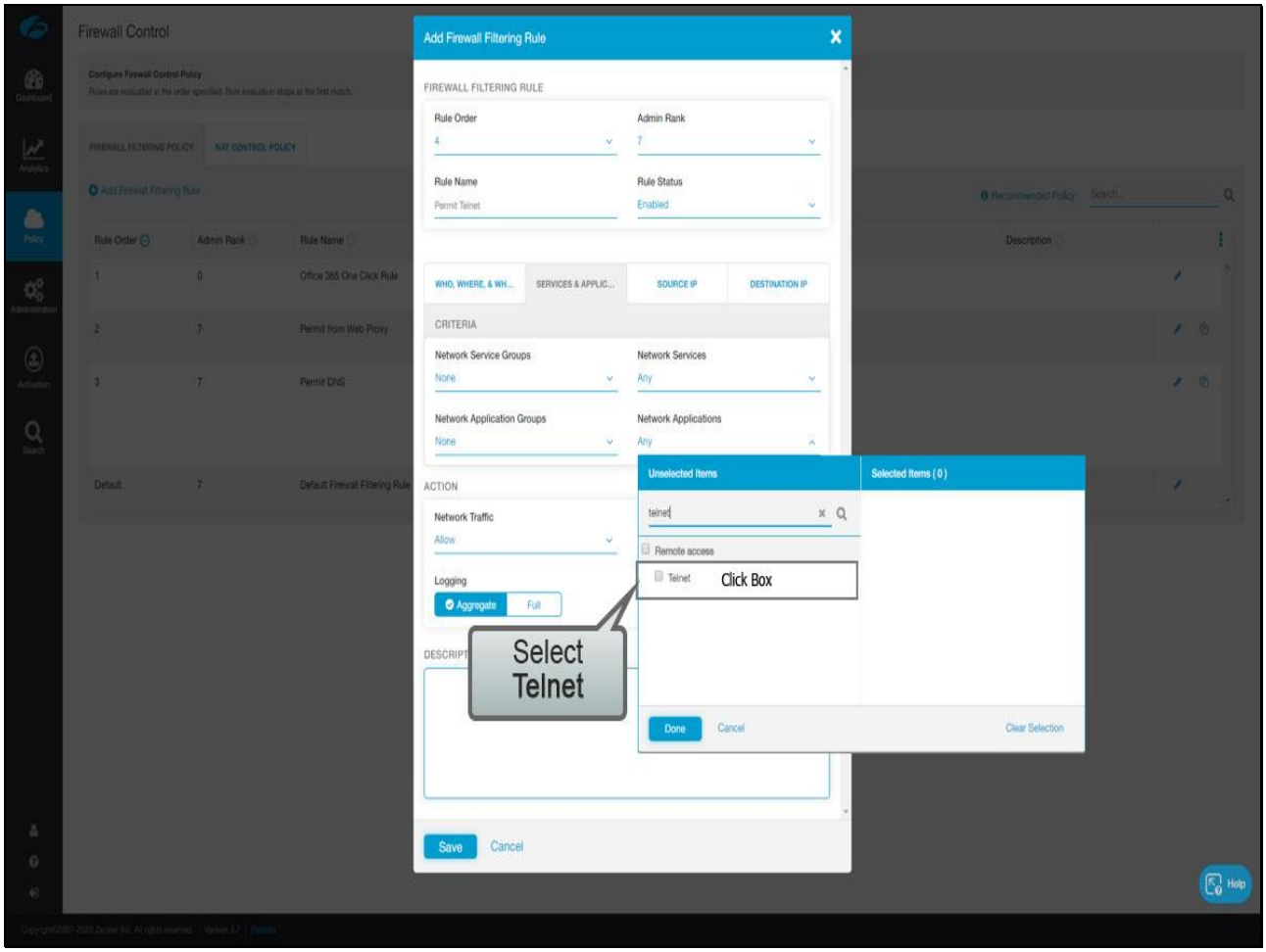
Instead, we'll use the **Network Applications** criteria to match Telnet. The result of this is that the Telnet application will now be allowed regardless of Layer 4 port. Click to expand the **Network Applications** list.

Slide 135 - Slide 135



Slide notes

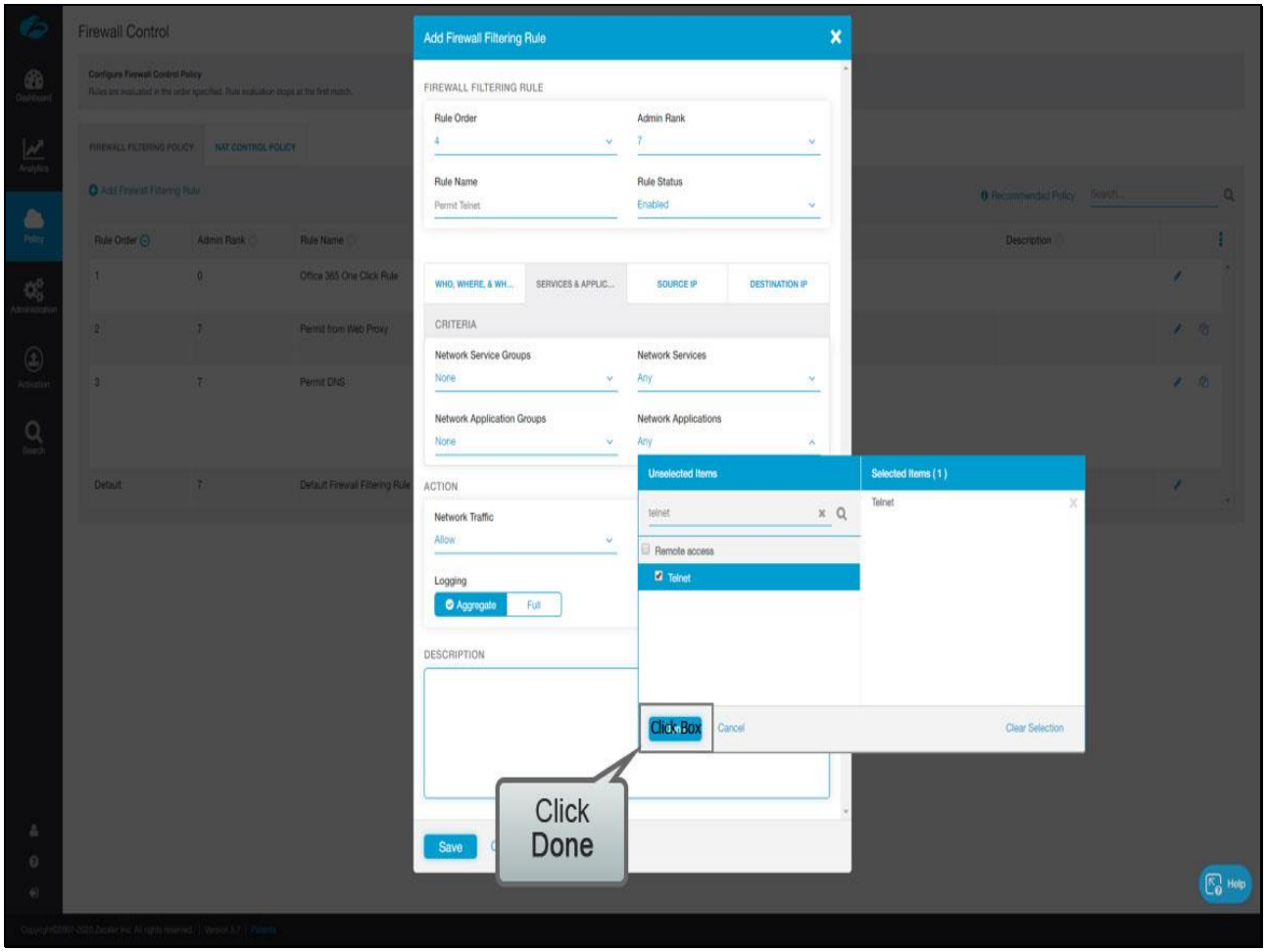
Slide 136 - Slide 136



Slide notes

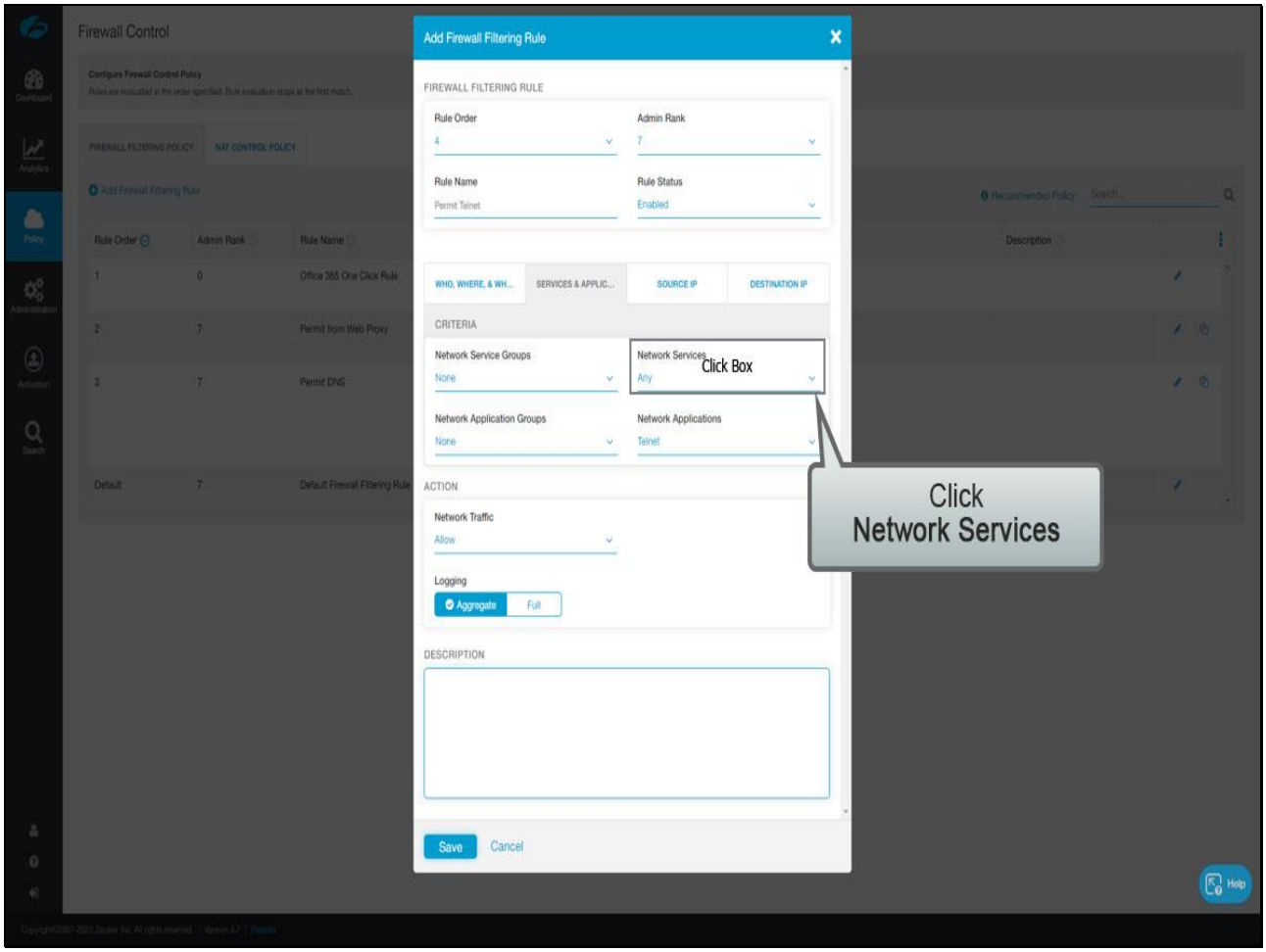
Select **Telnet** and click **Done**.

Slide 137 - Slide 137



Slide notes

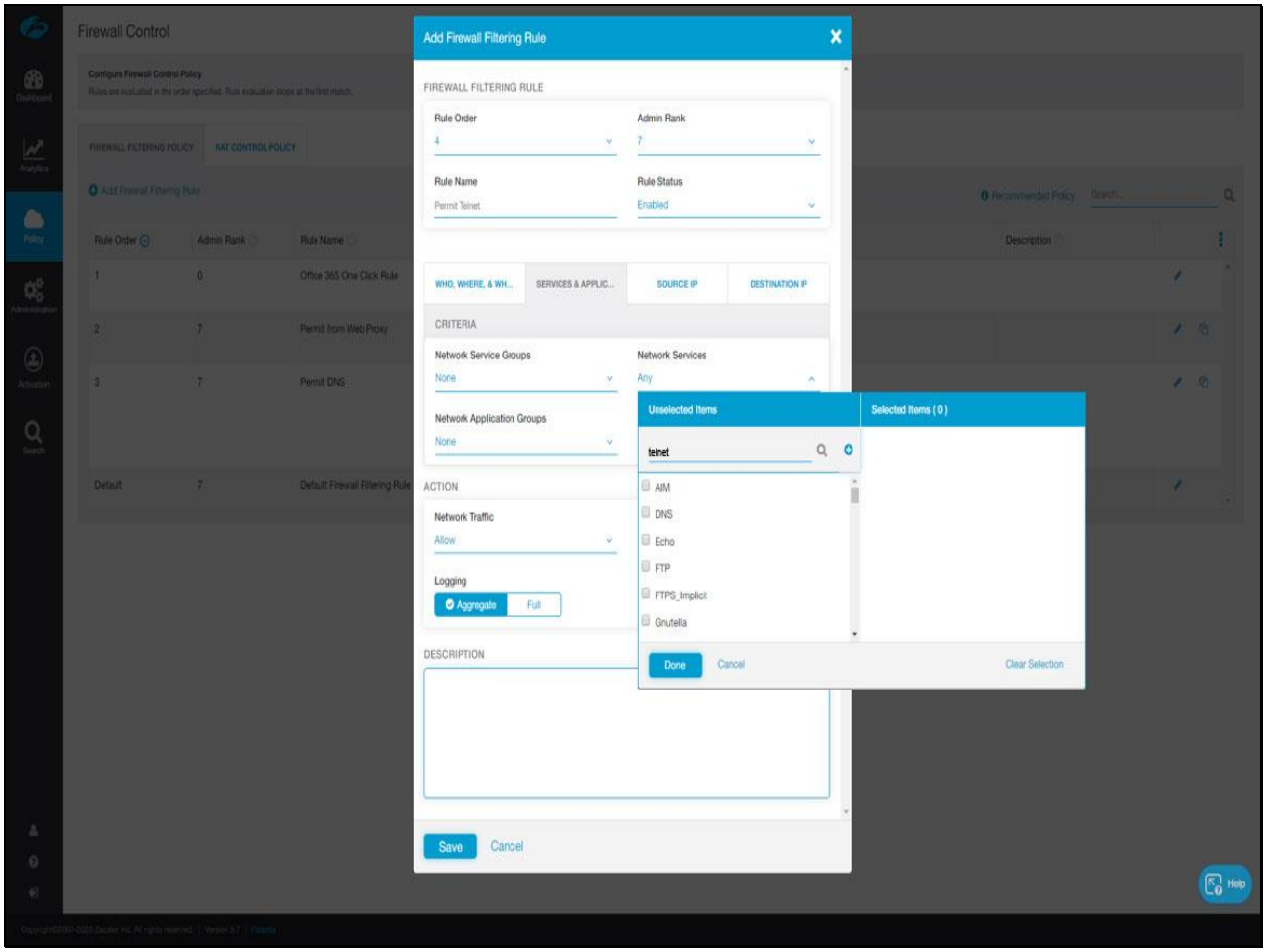
Slide 138 - Slide 138



Slide notes

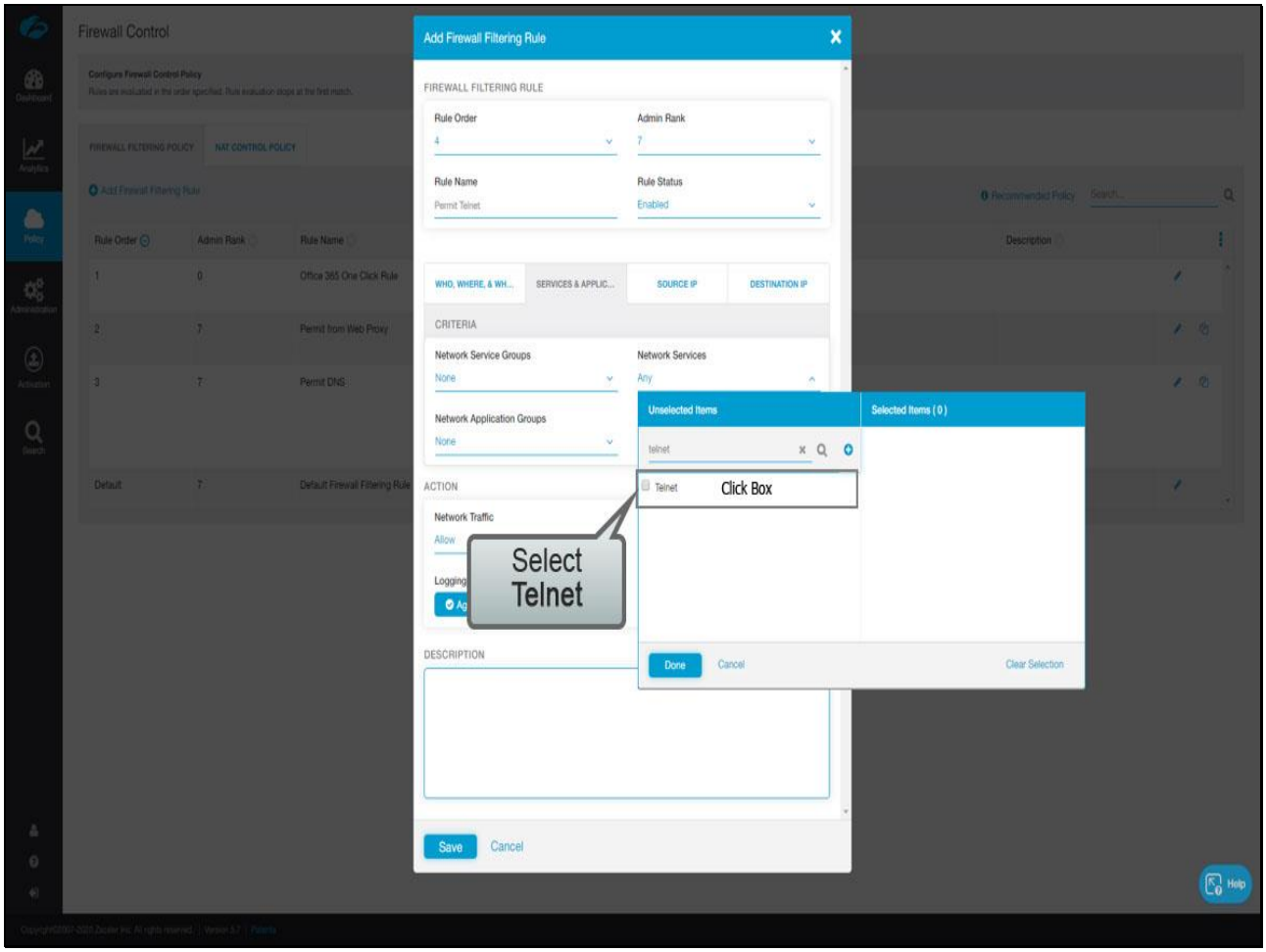
If you also want to restrict the Layer 4 ports that are used, you need to combine a **Network Services** configuration with the **Network Applications** rule. Click **Network Services**

Slide 140 - Slide 140



Slide notes

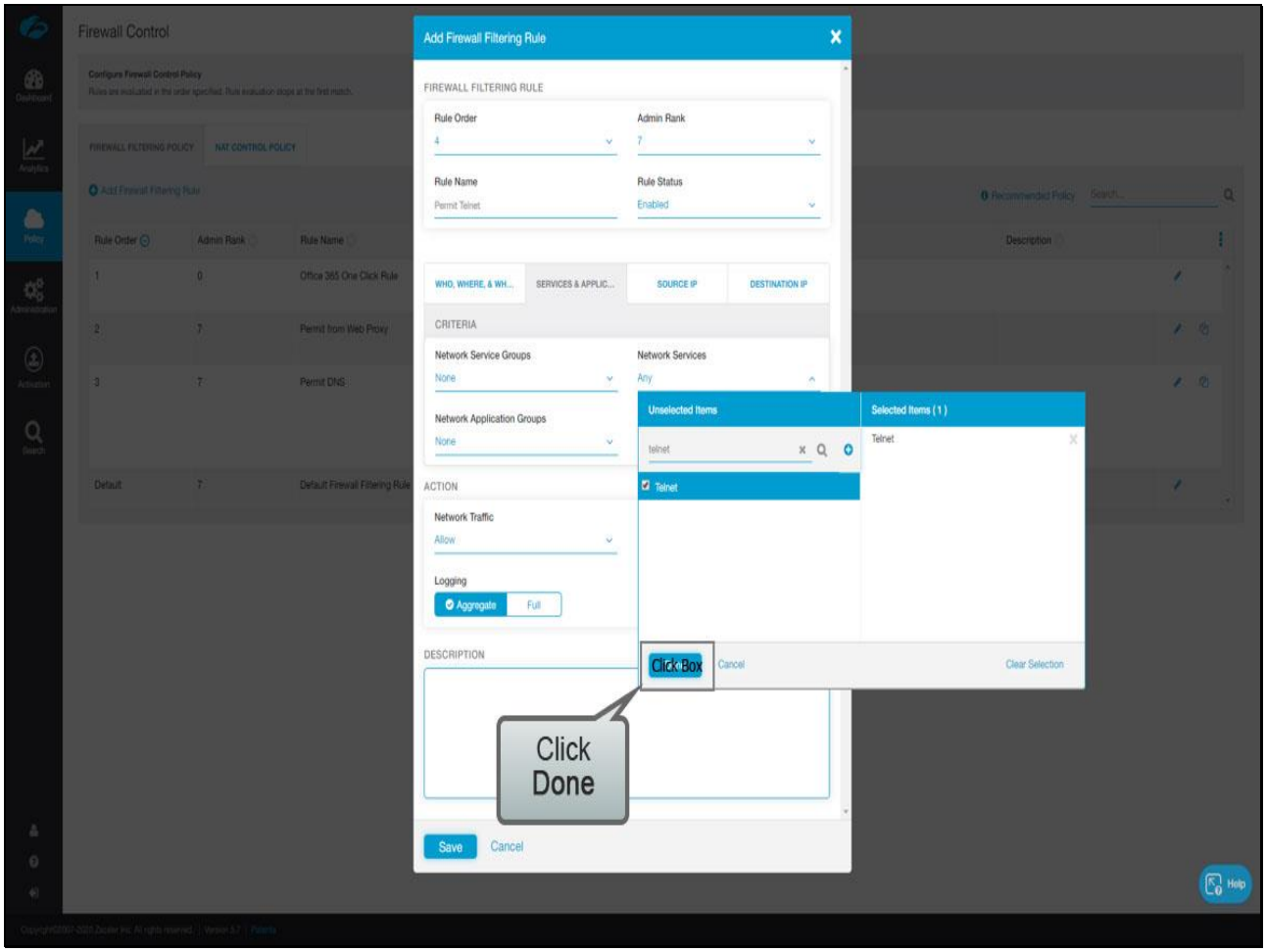
Slide 141 - Slide 141



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.

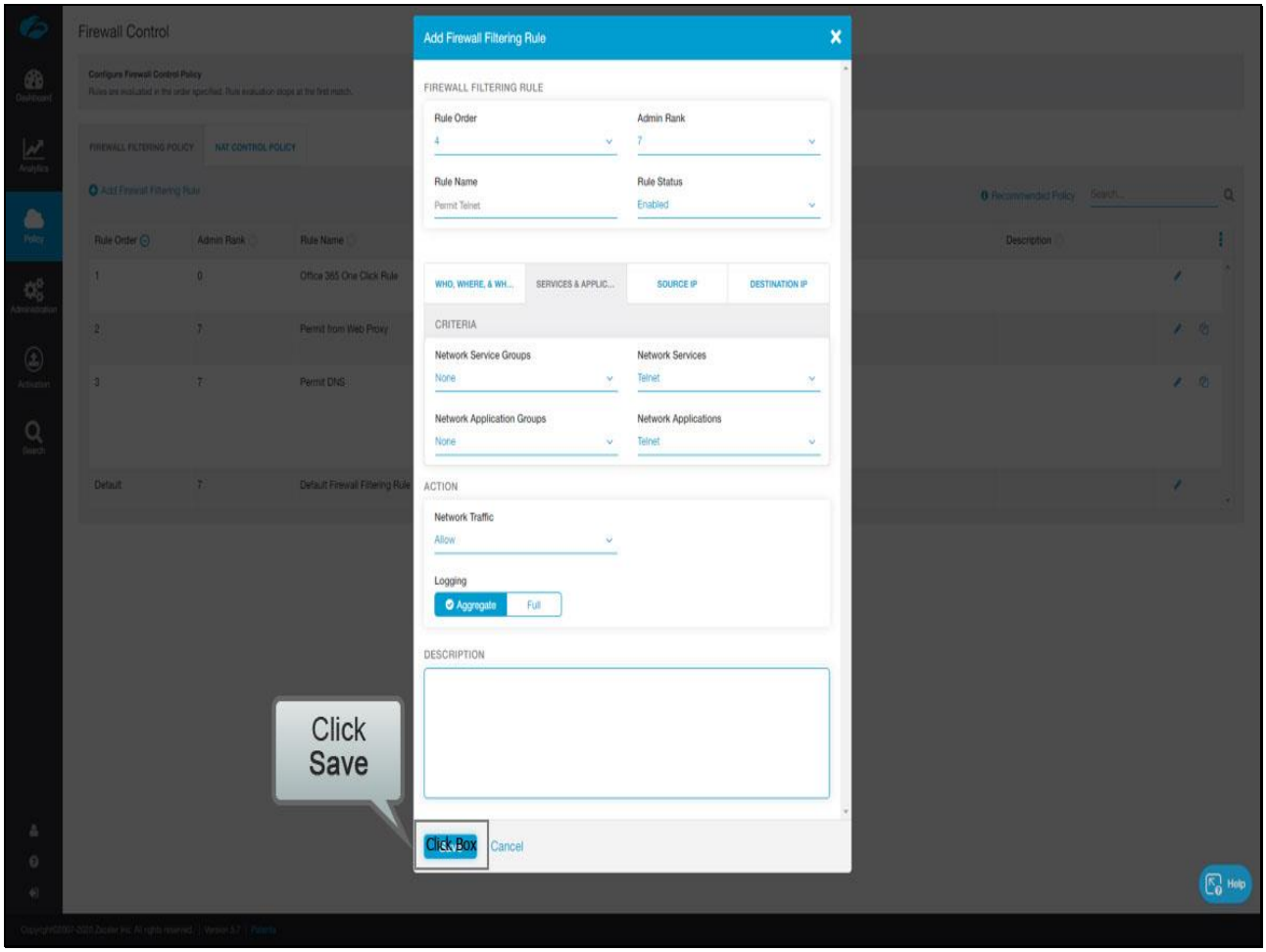
Slide 142 - Slide 142



Slide notes

Click **Done** to select Telnet.

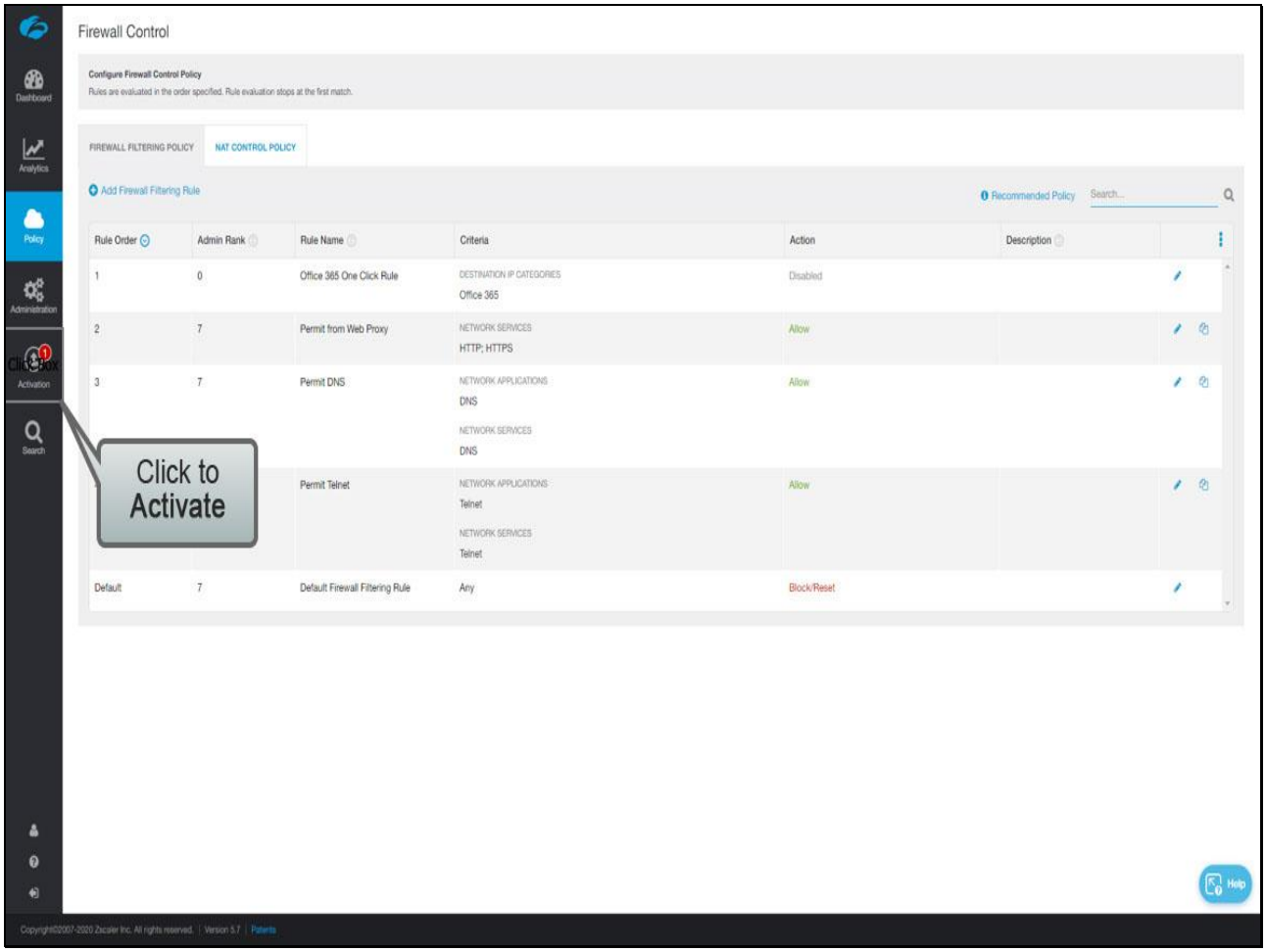
Slide 143 - Slide 143



Slide notes

Click **Save**.

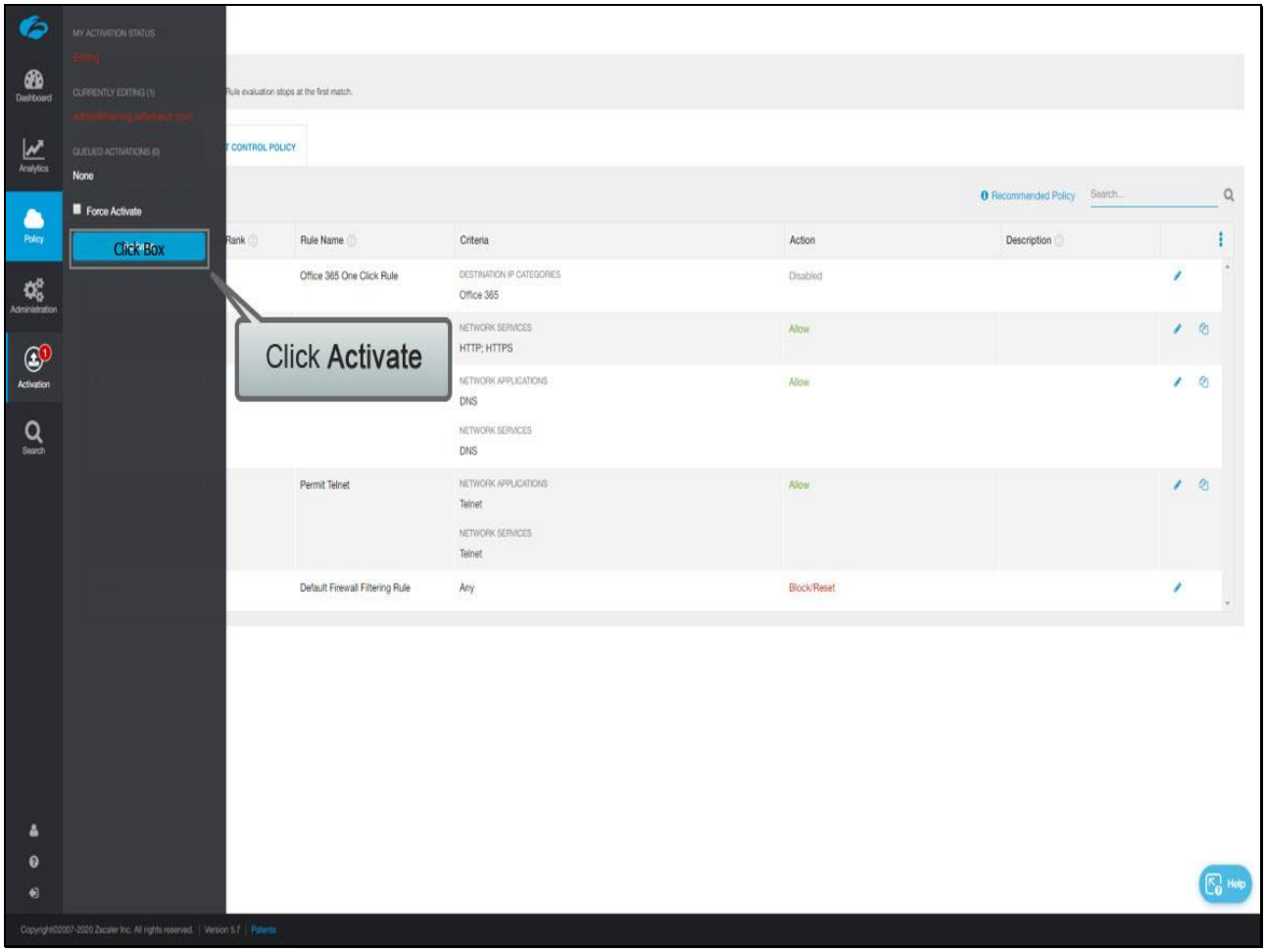
Slide 148 - Slide 148



Slide notes

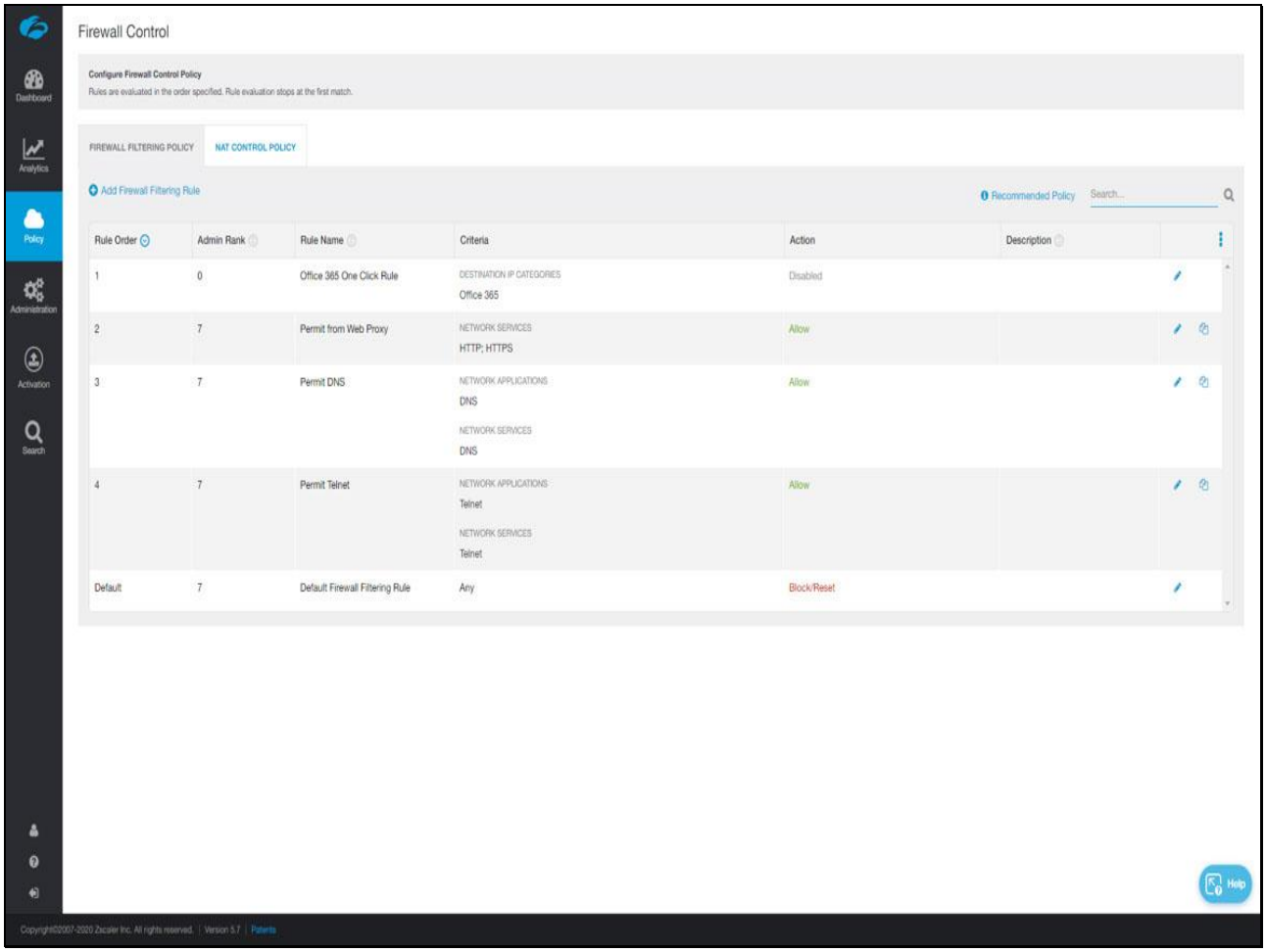
then **Activate** your changes.

Slide 149 - Slide 149



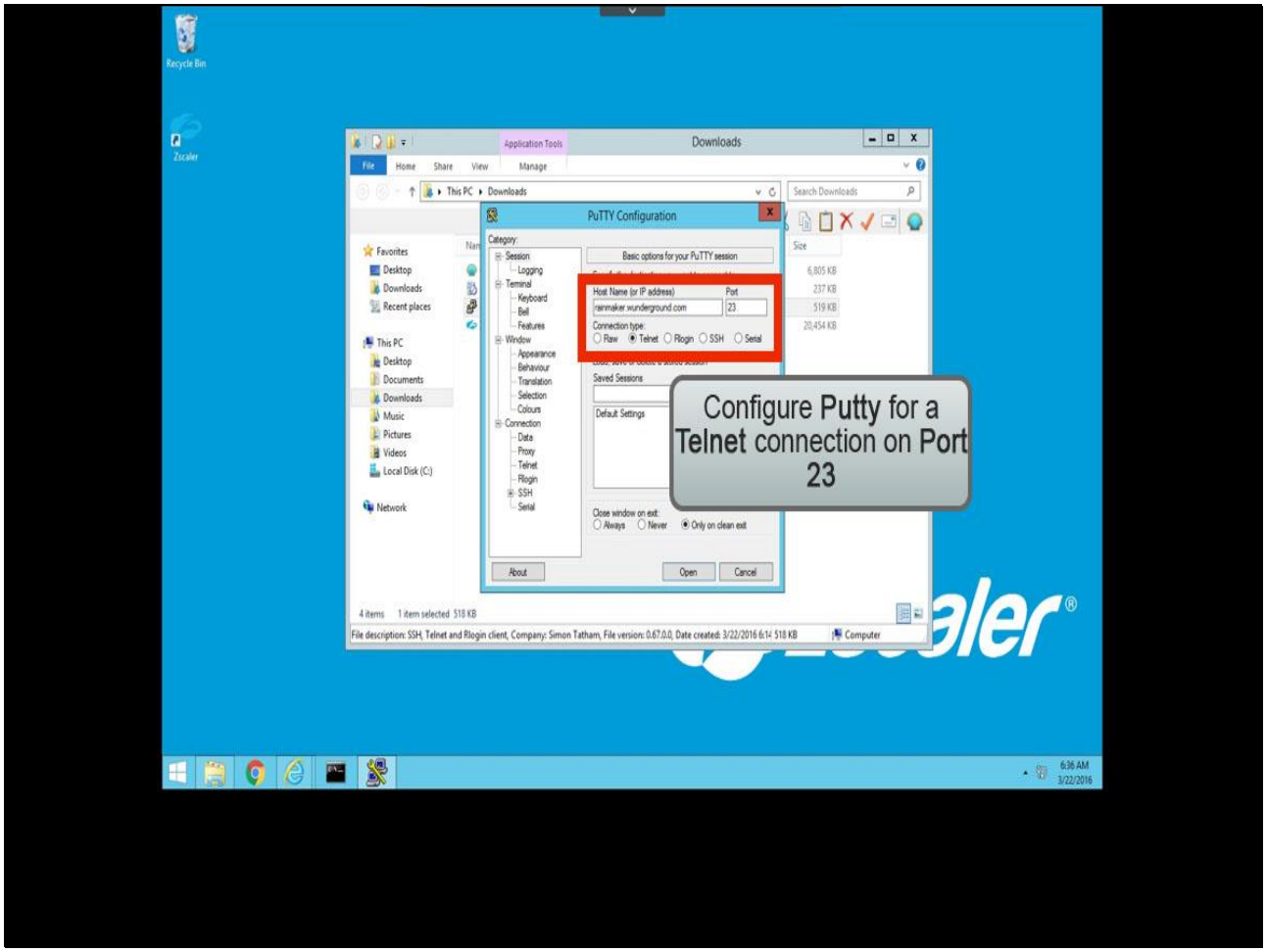
Slide notes

Slide 152 - Slide 152



Slide notes

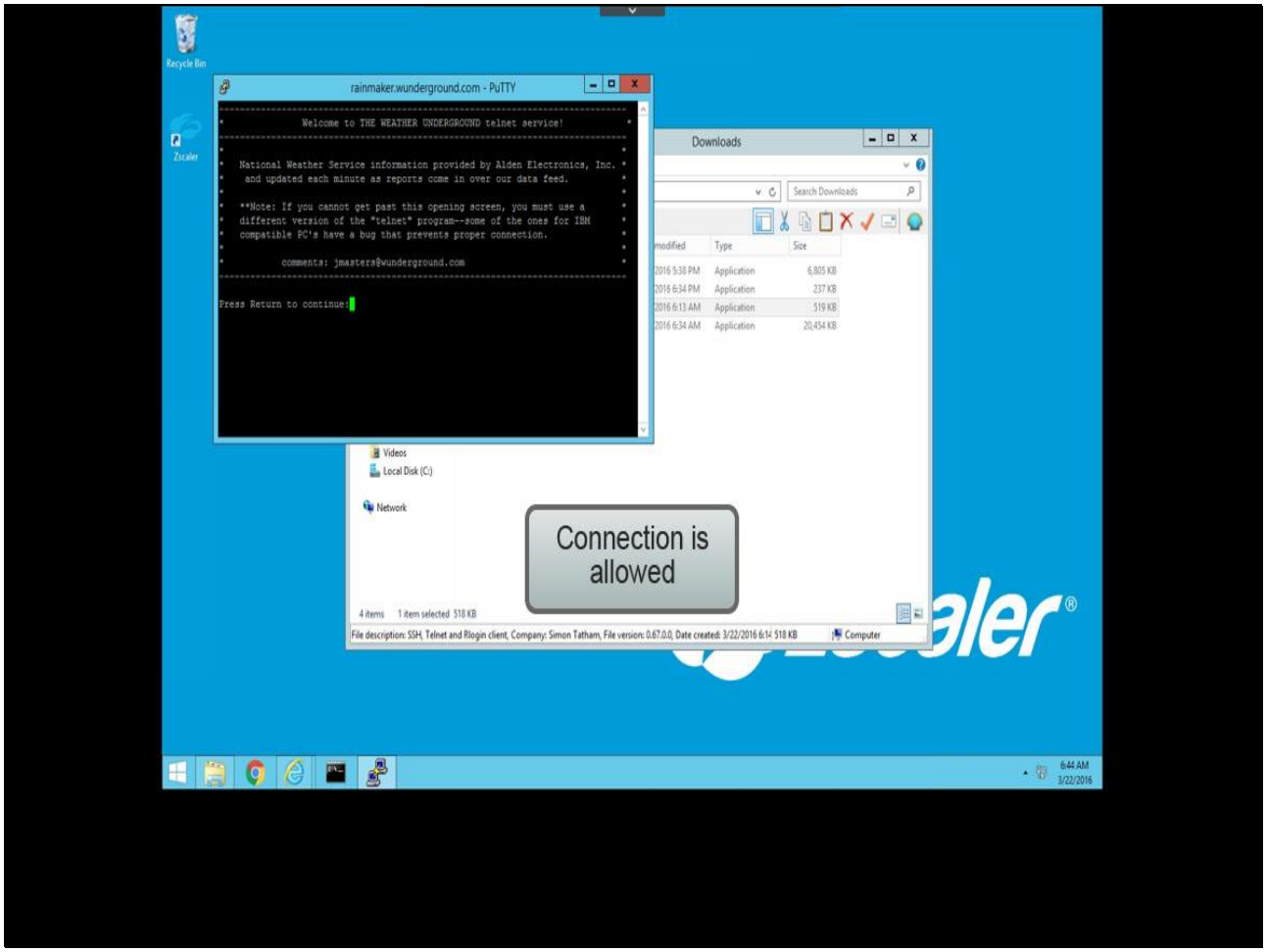
Slide 153 - Slide 153



Slide notes

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

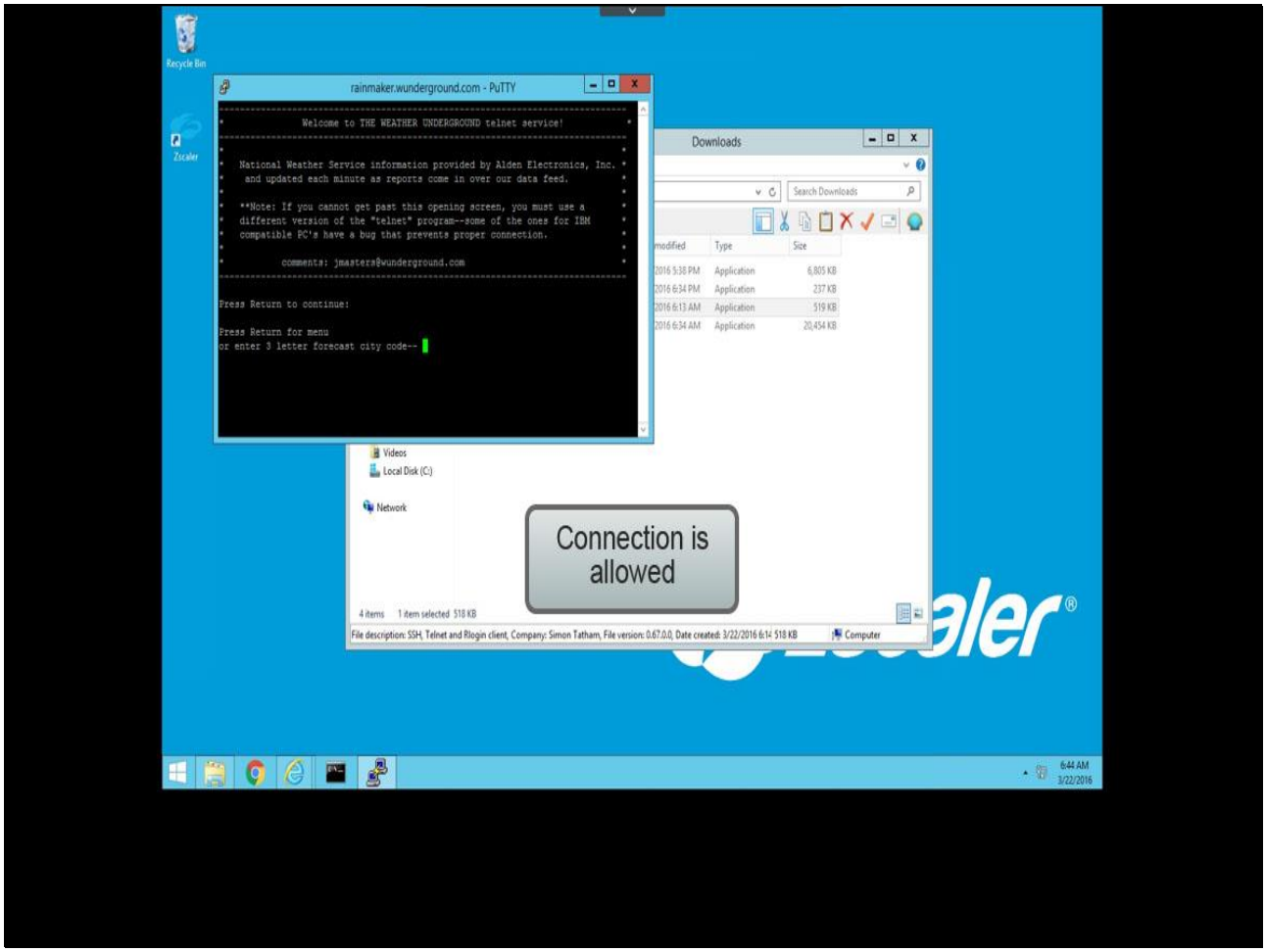
Slide 154 - Slide 154



Slide notes

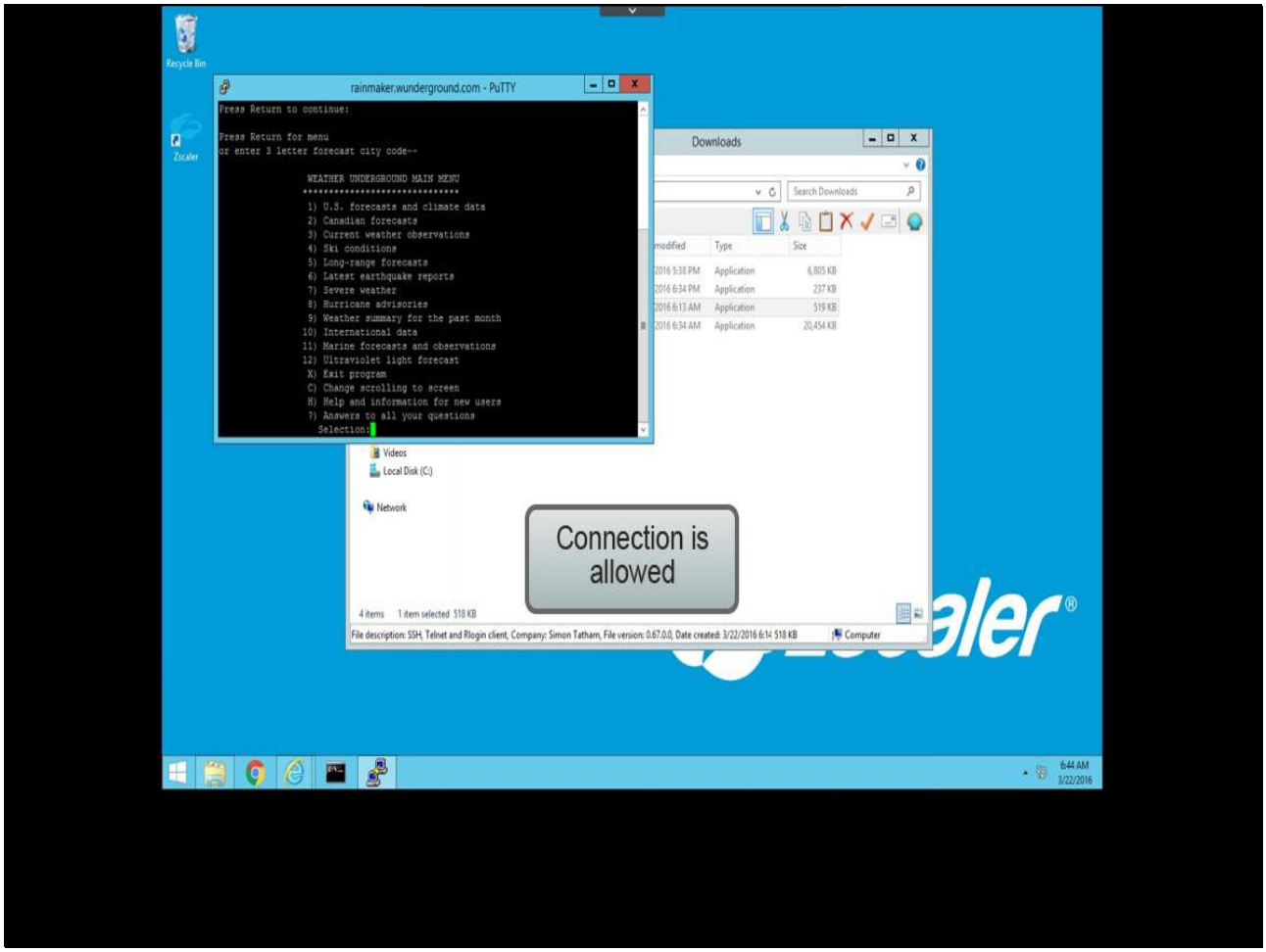
And as you can see, Telnet using port 23 is being allowed.

Slide 155 - Slide 155



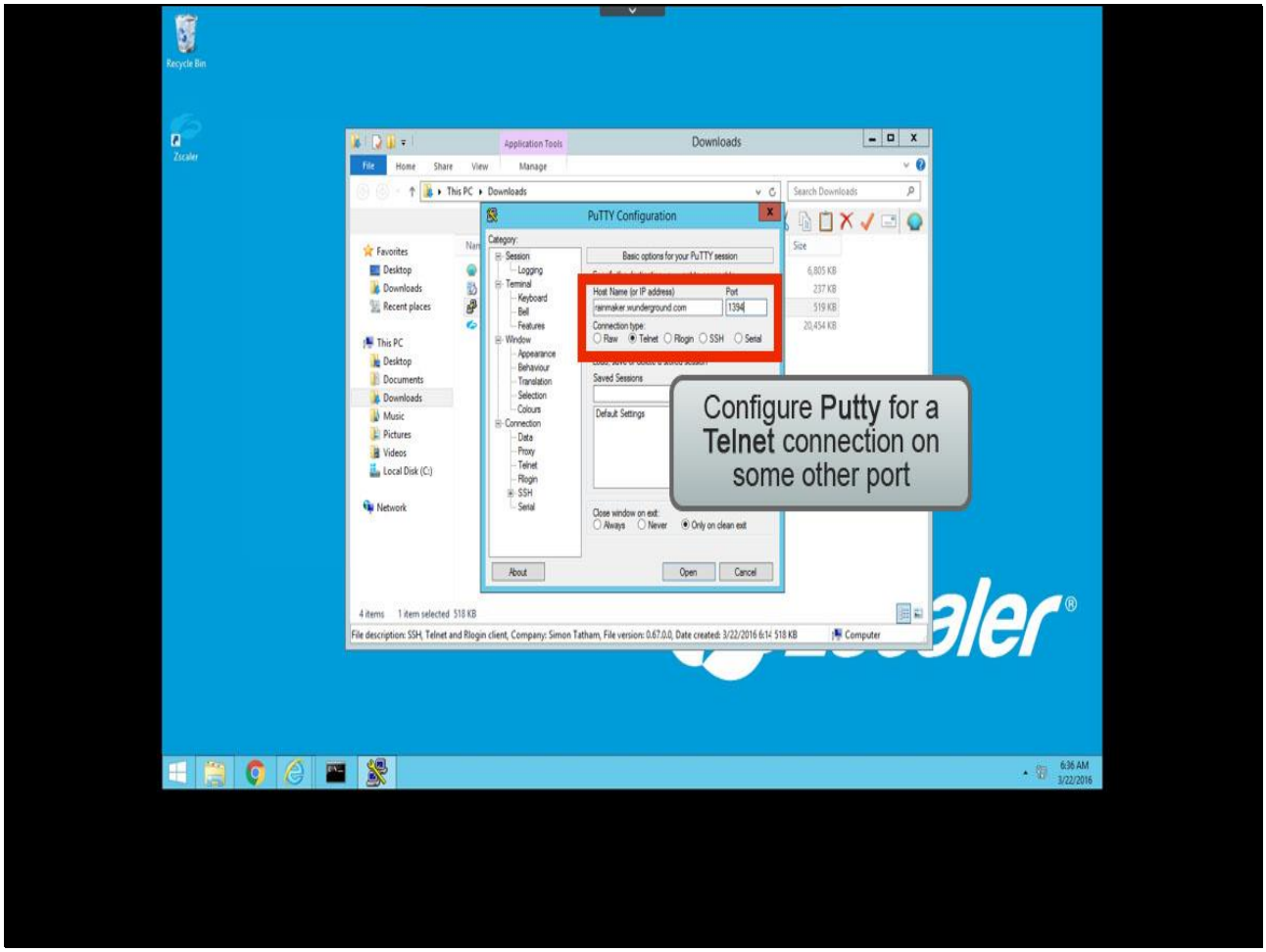
Slide notes

Slide 156 - Slide 156



Slide notes

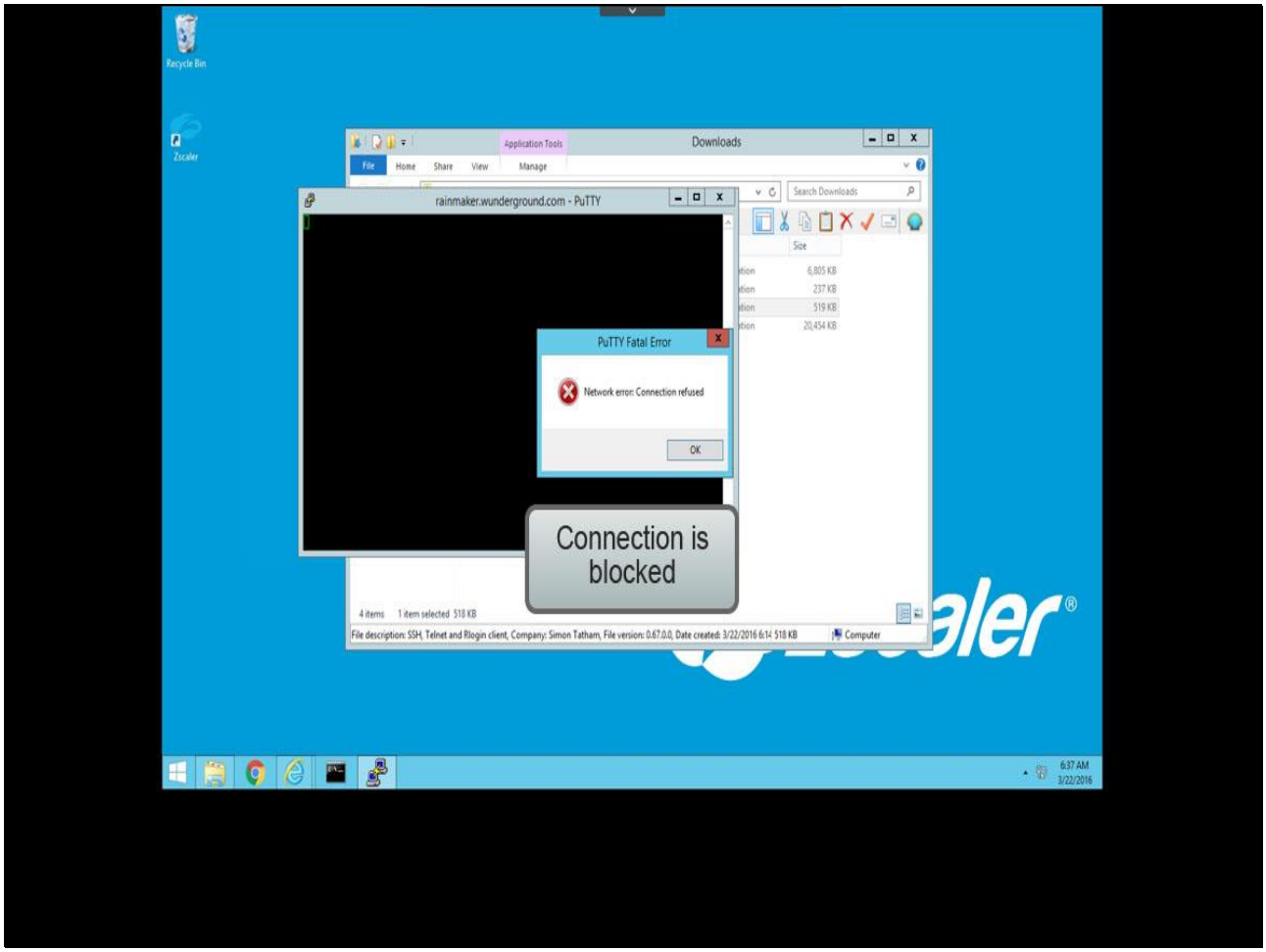
Slide 157 - Slide 157



Slide notes

But if we try to Telnet over some other port

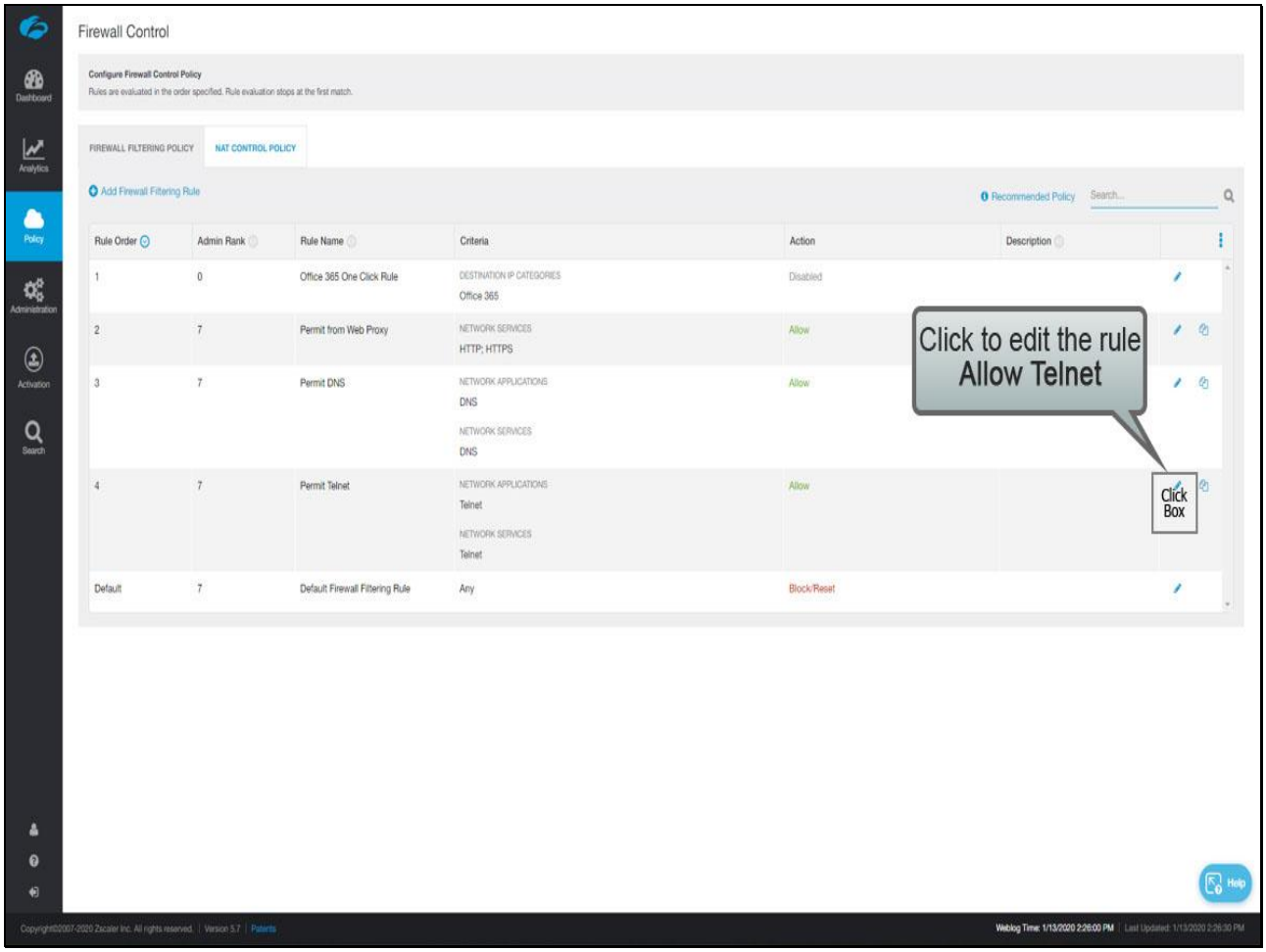
Slide 158 - Slide 158



Slide notes

it is still being blocked.

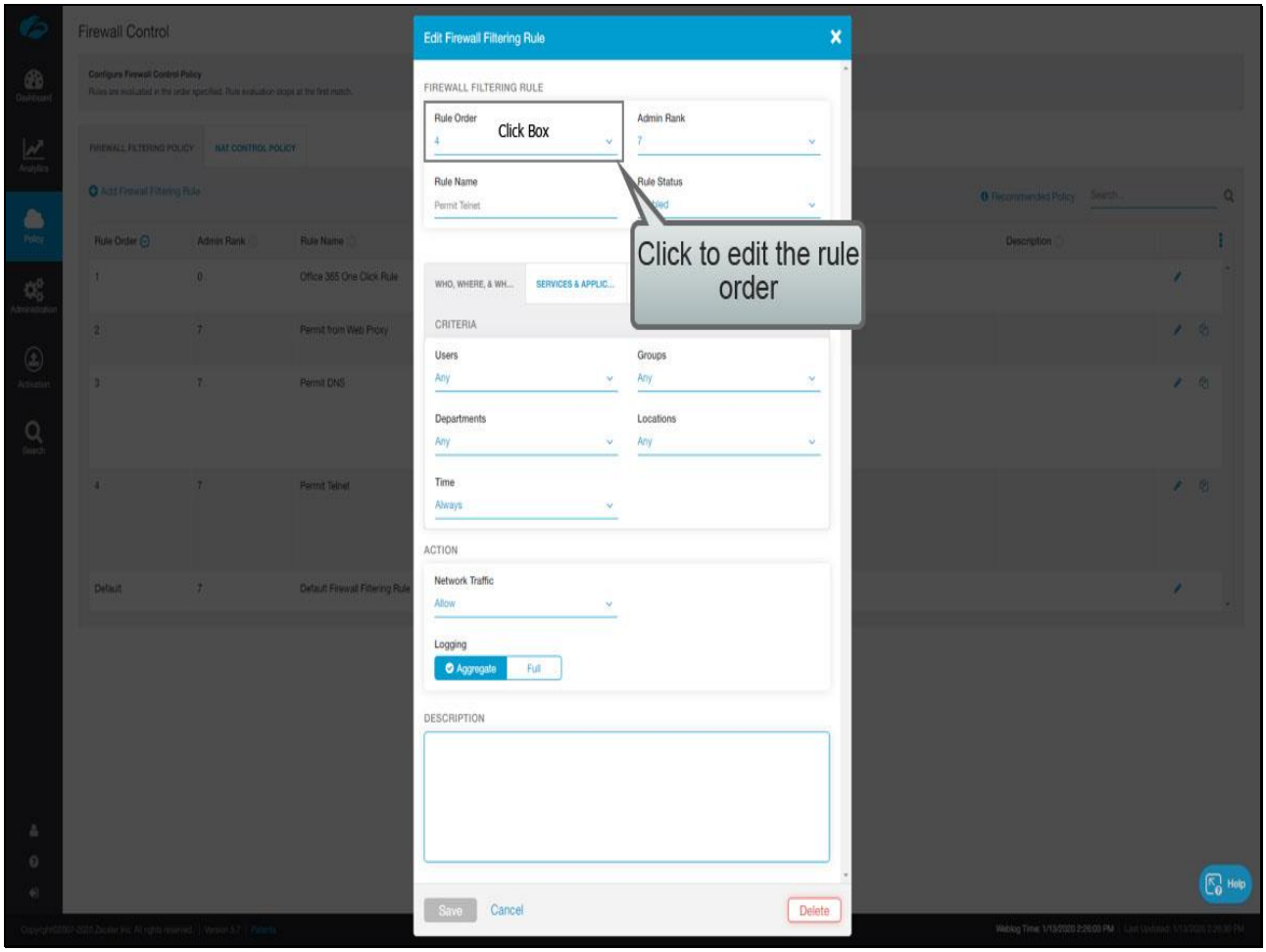
Slide 159 - Slide 159



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.

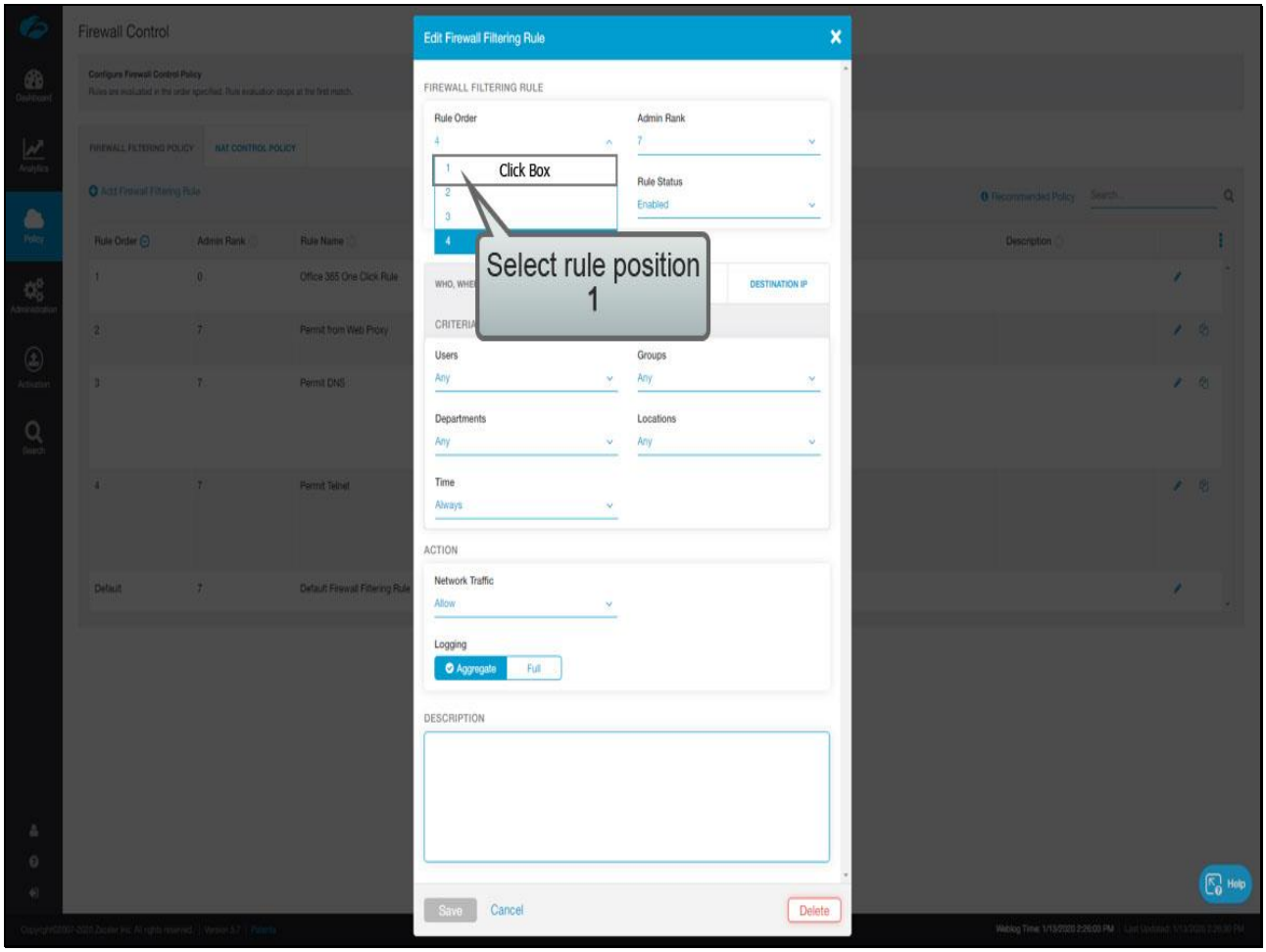
Slide 160 - Slide 160



Slide notes

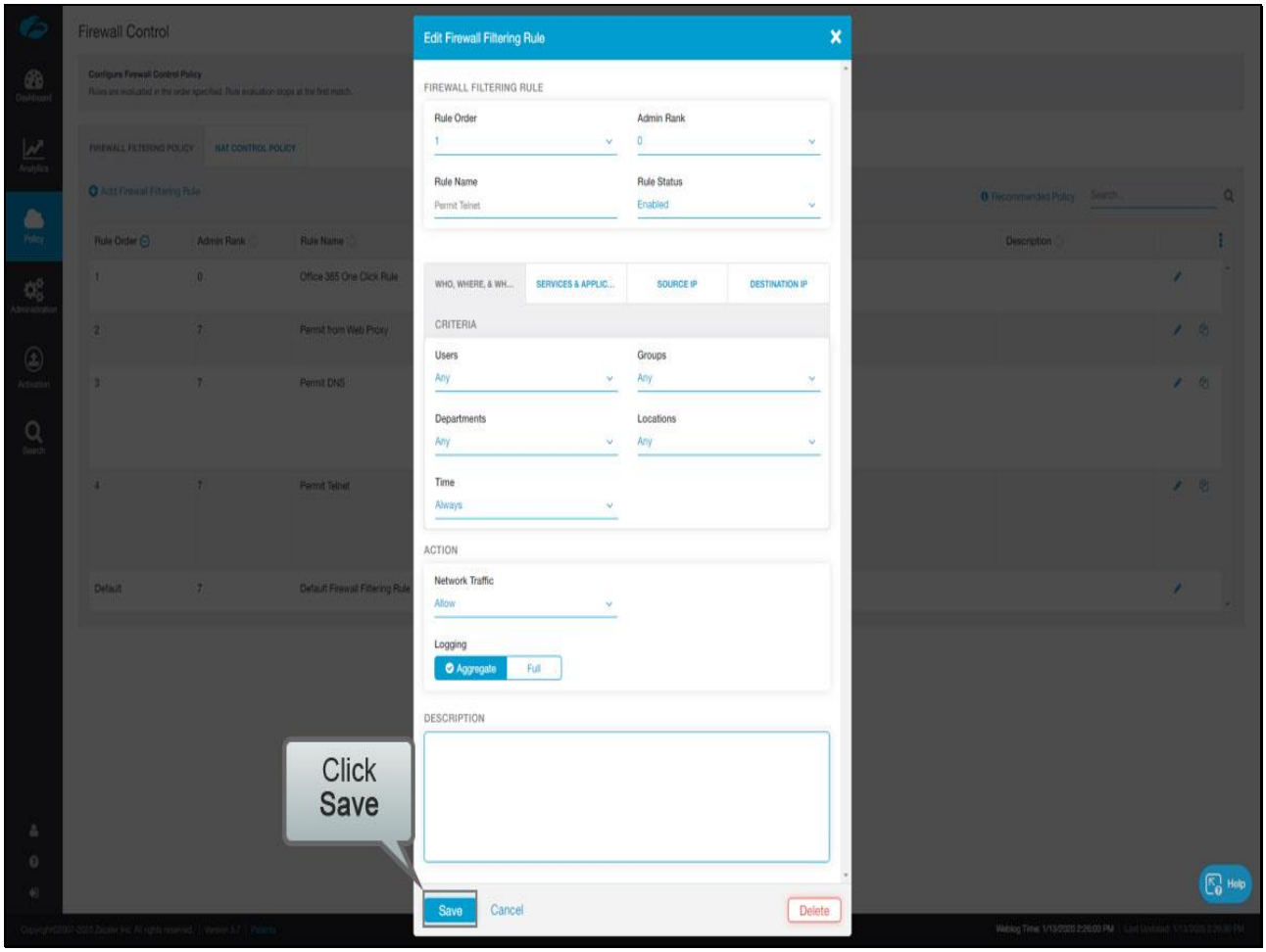
Select the correct **Rule Order** from the drop-down list (we will put this rule to number 1), click **Save**

Slide 161 - Slide 161



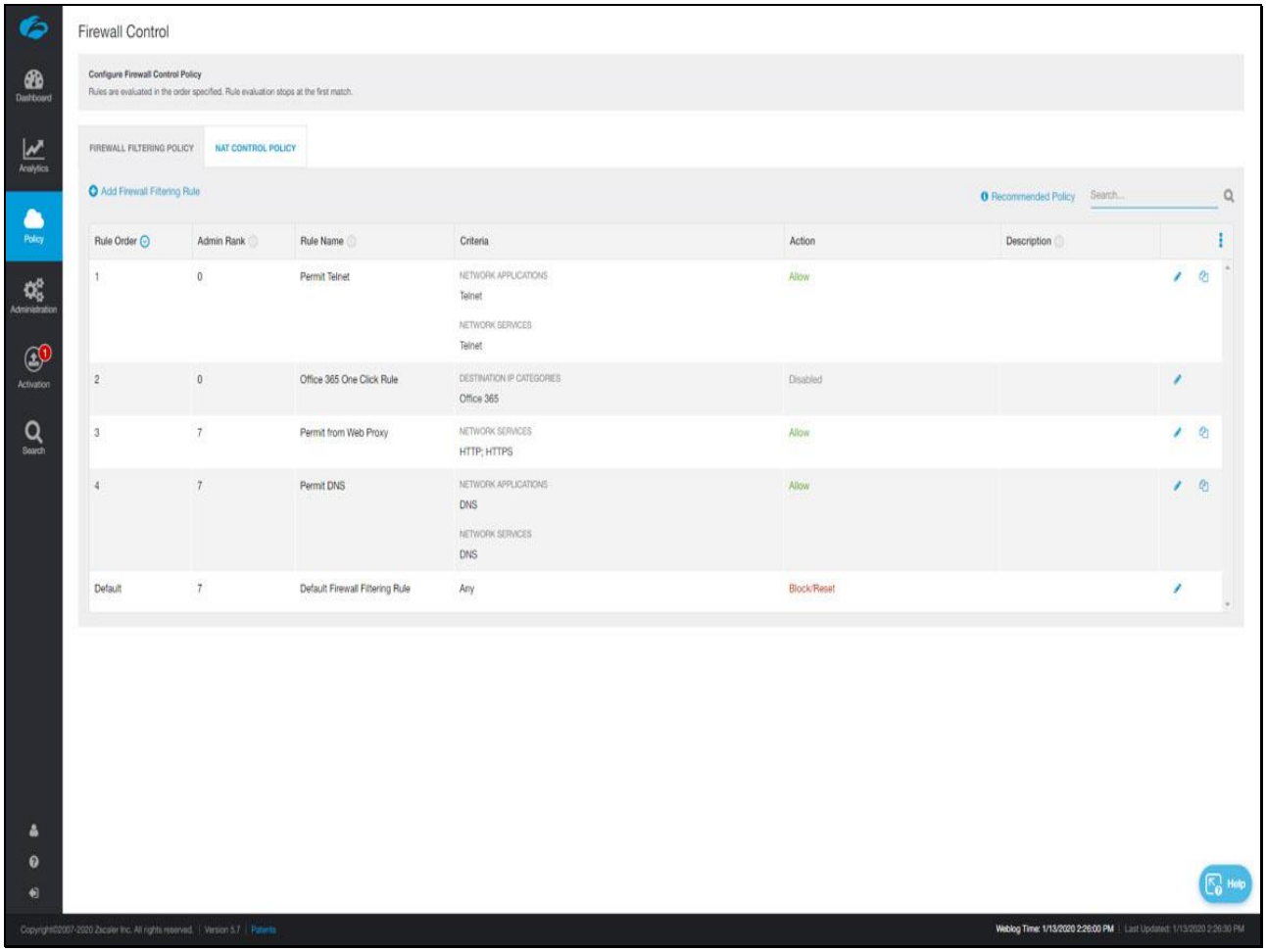
Slide notes

Slide 163 - Slide 163



Slide notes

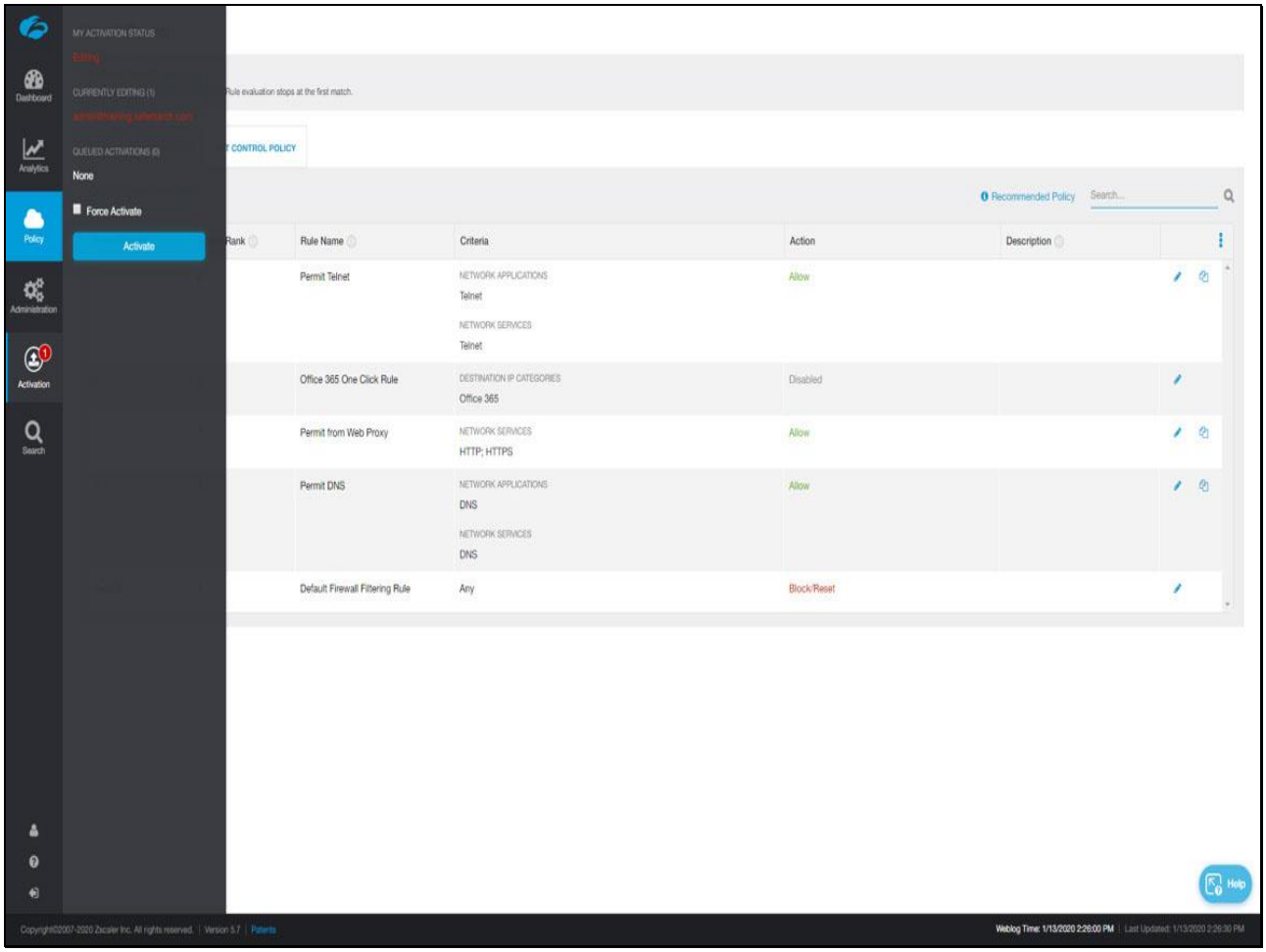
Slide 169 - Slide 169



Slide notes

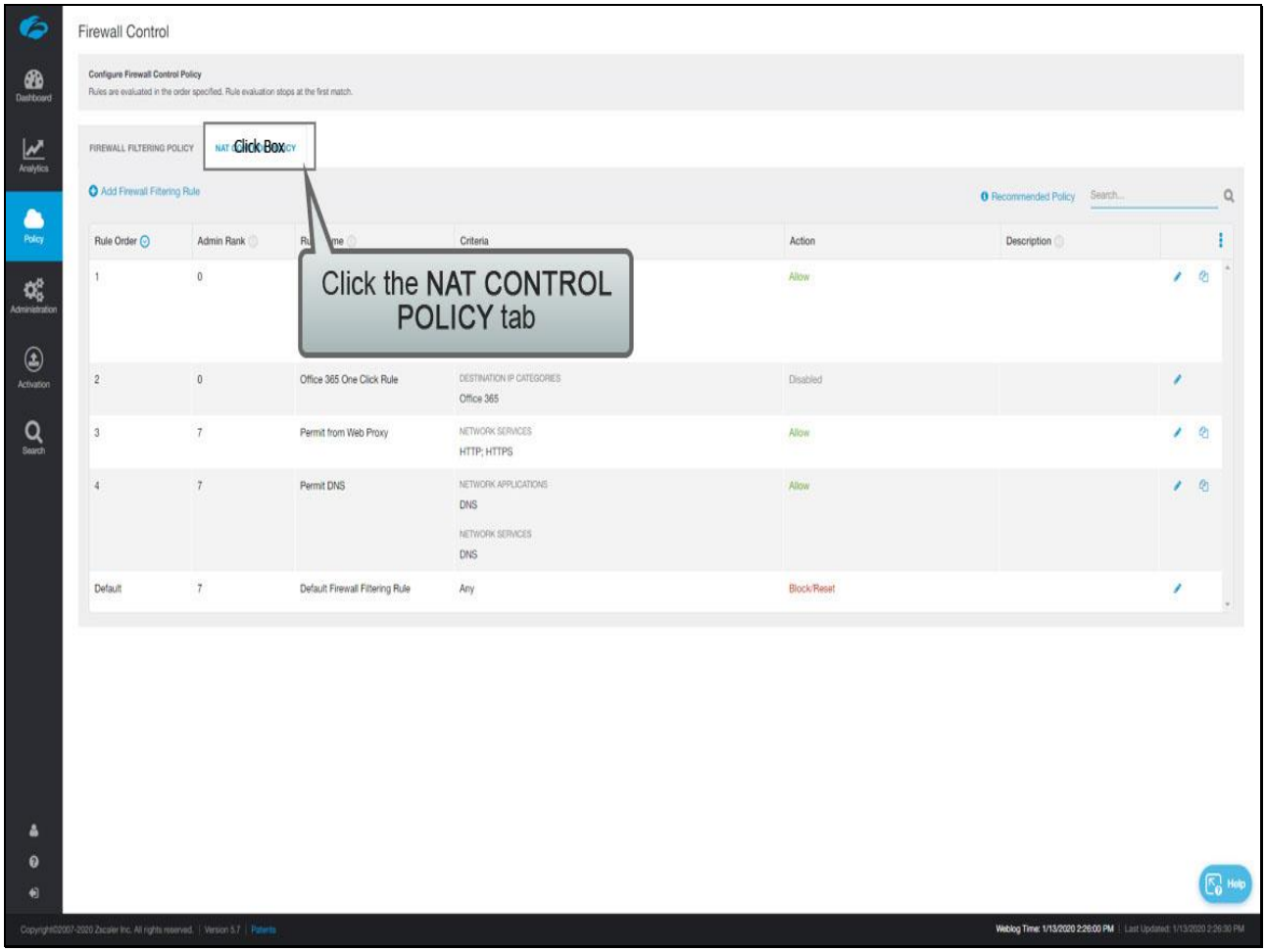
then **Activate** your changes.

Slide 170 - Slide 170



Slide notes

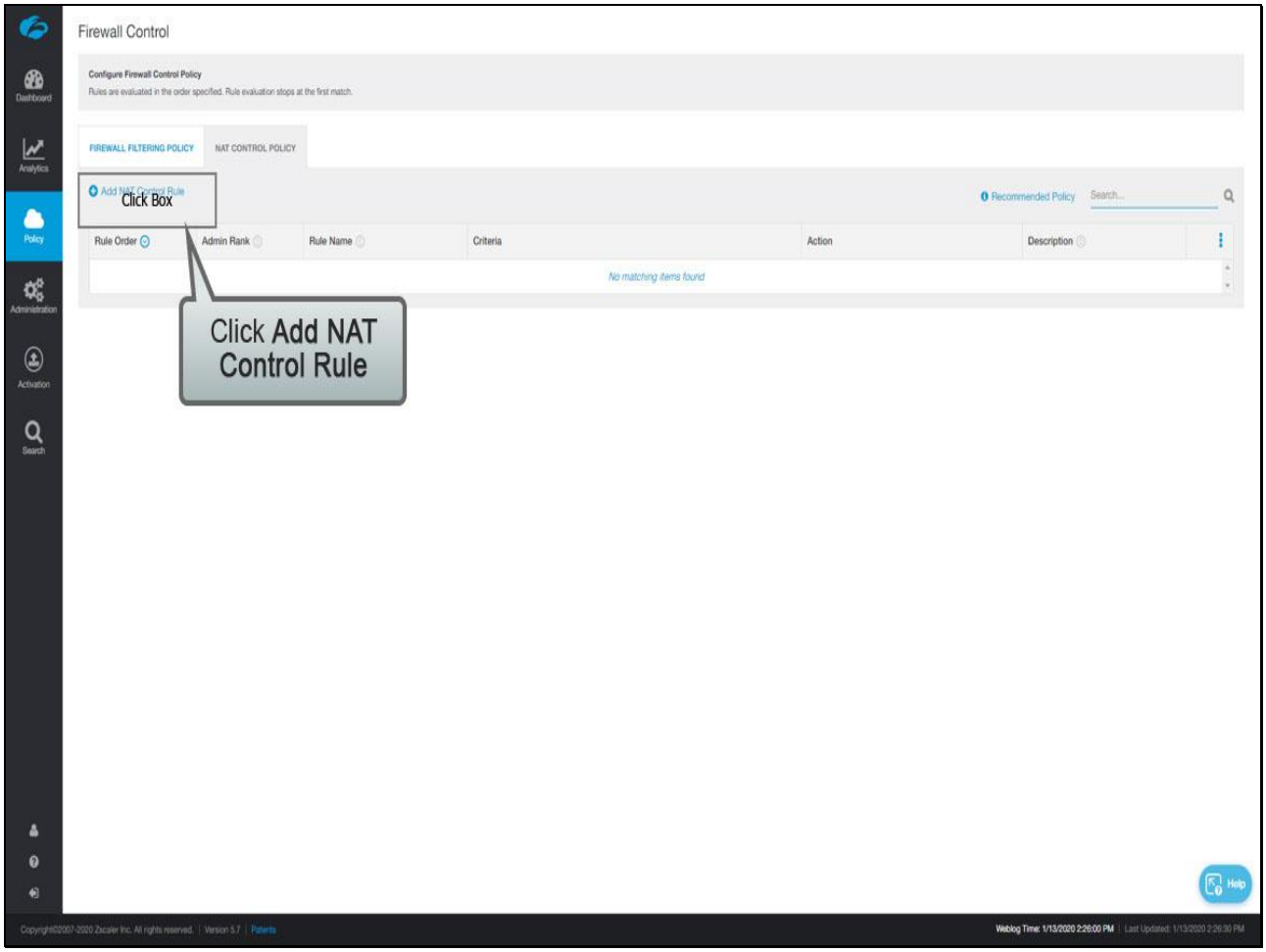
Slide 174 - Slide 174



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.

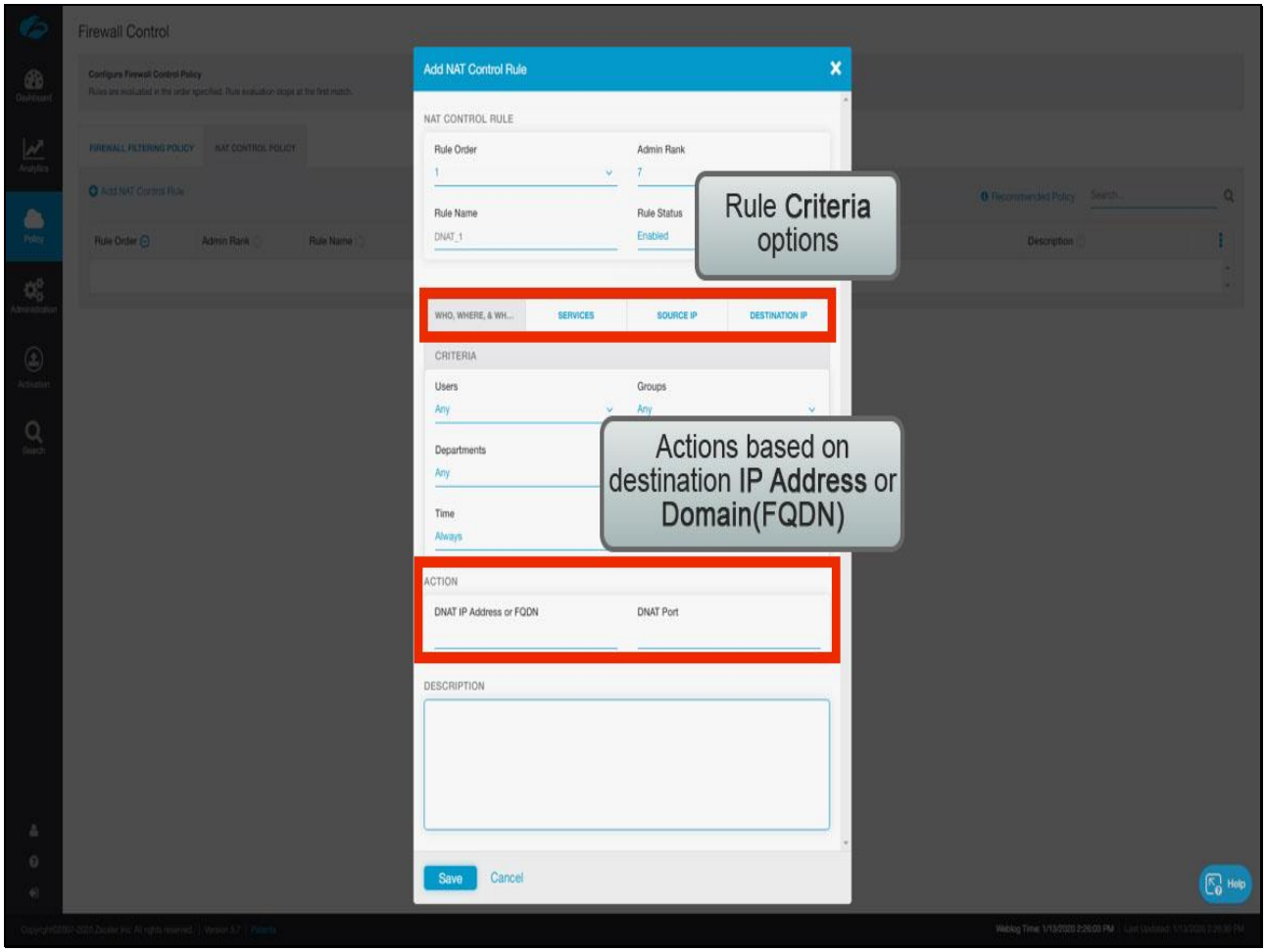
Slide 175 - Slide 175



Slide notes

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

Slide 176 - Slide 176

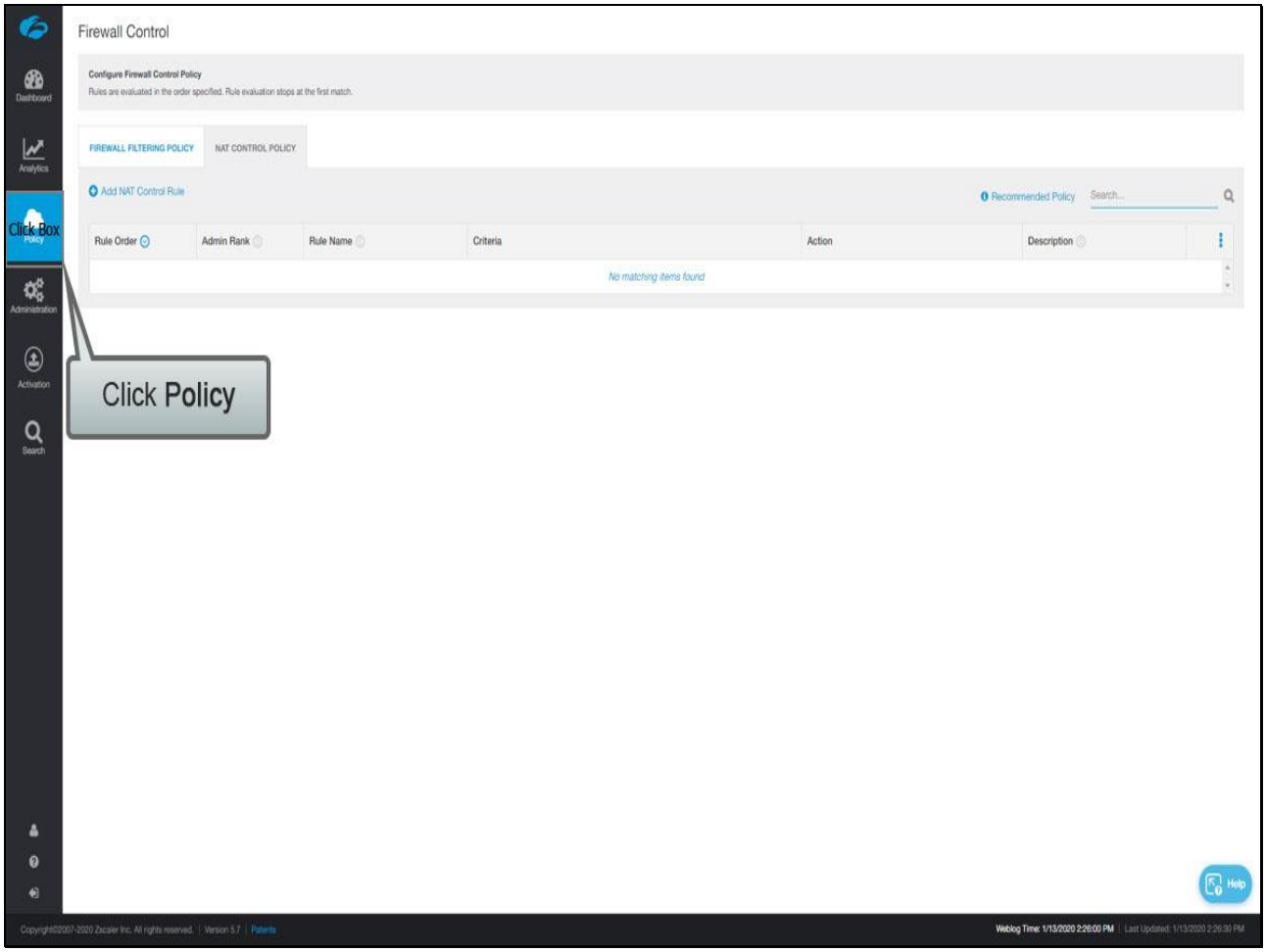


Slide notes

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.

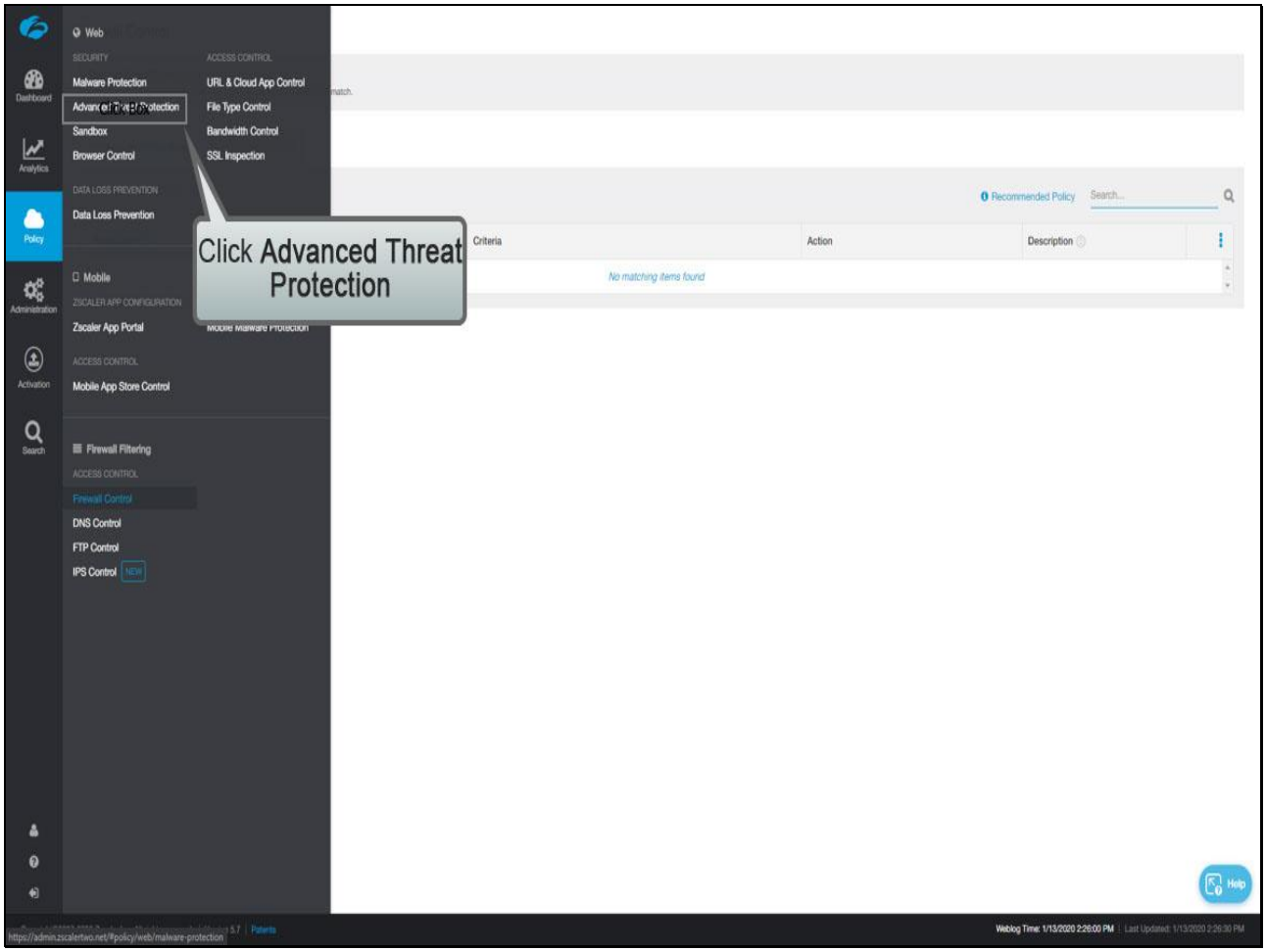
Slide 177 - Slide 177



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

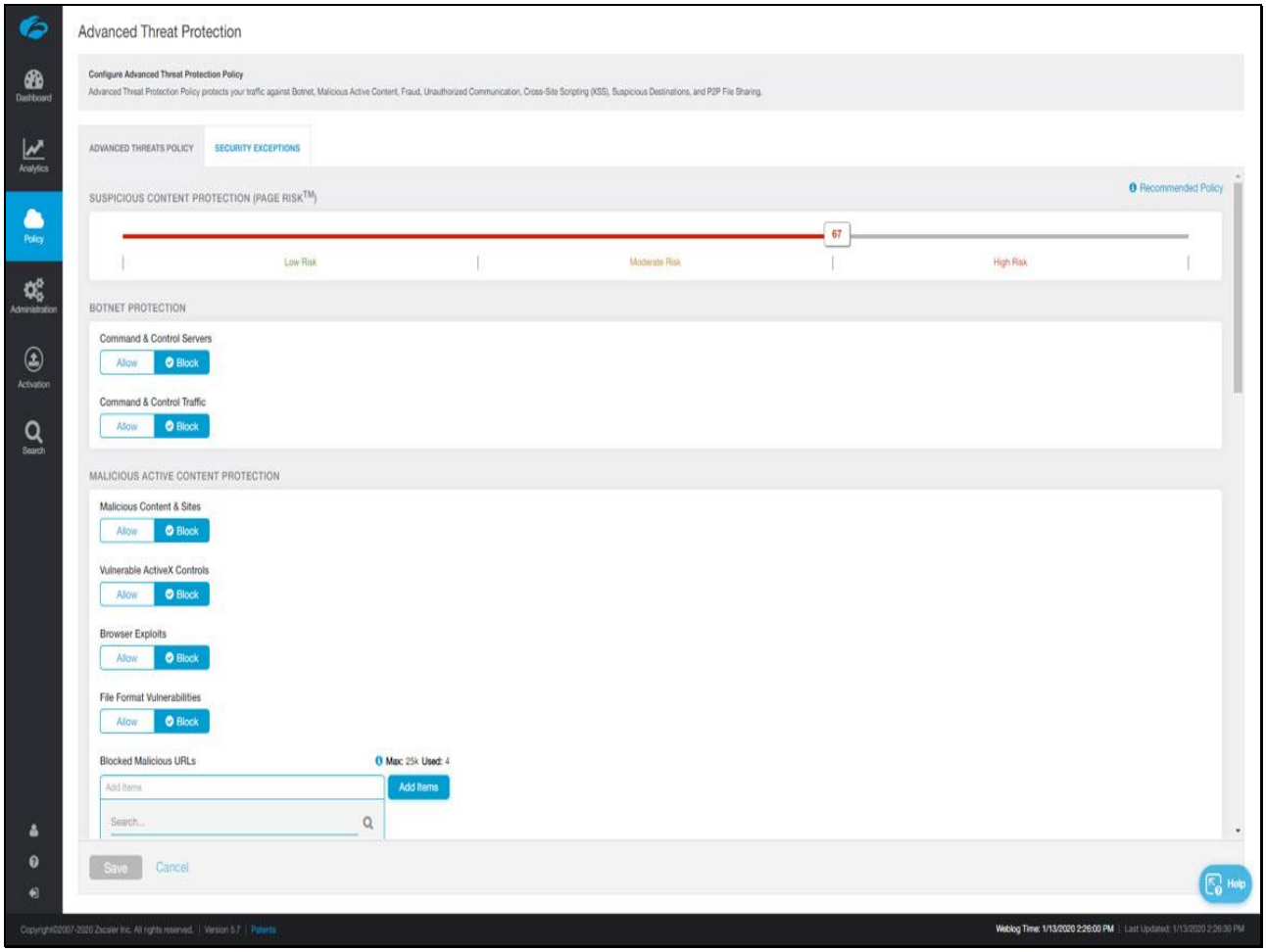
Slide 178 - Slide 178



Slide notes

select **Advanced Threat Protection**.

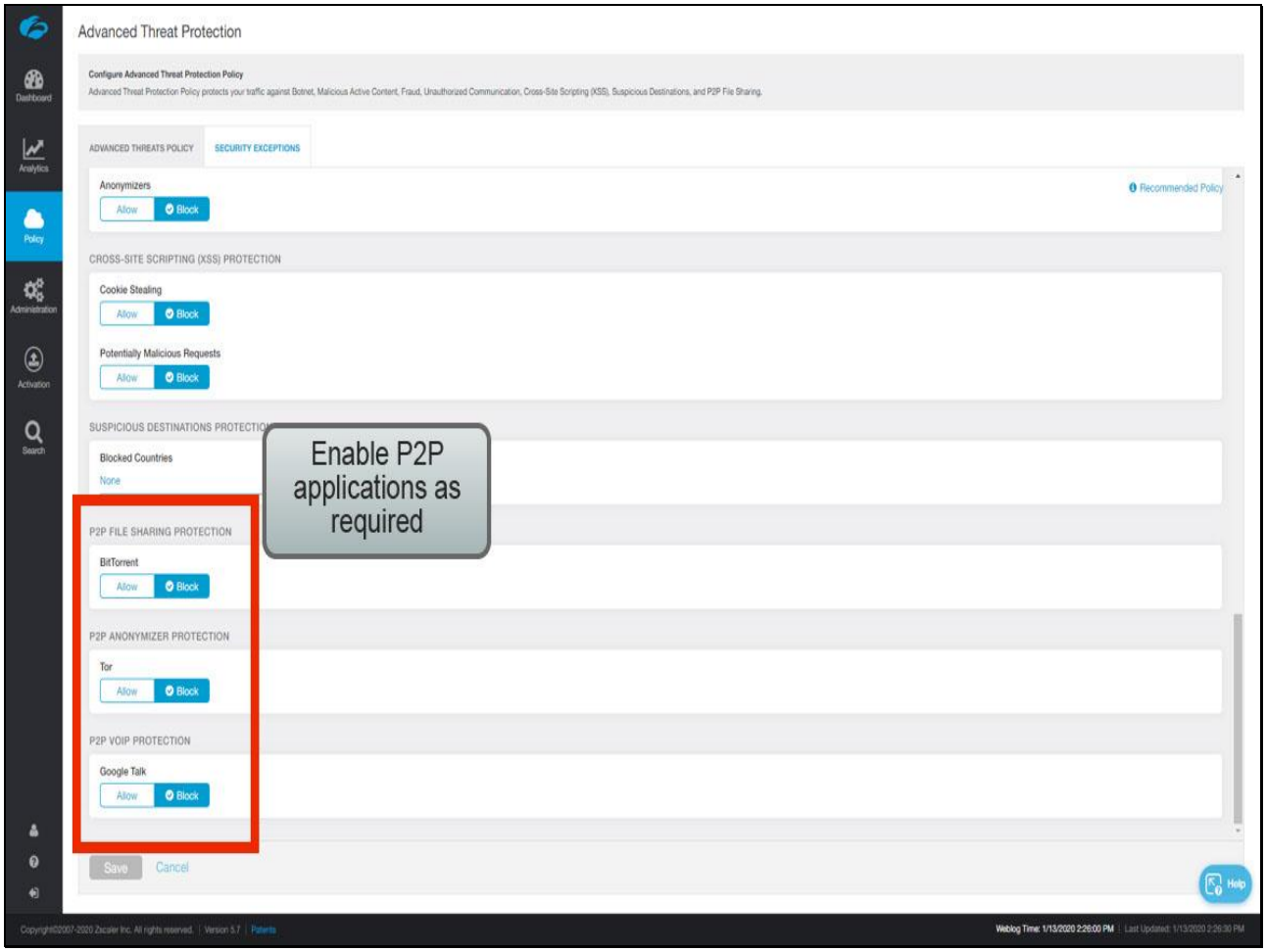
Slide 179 - Slide 179



Slide notes

Scroll down to the bottom of the page.

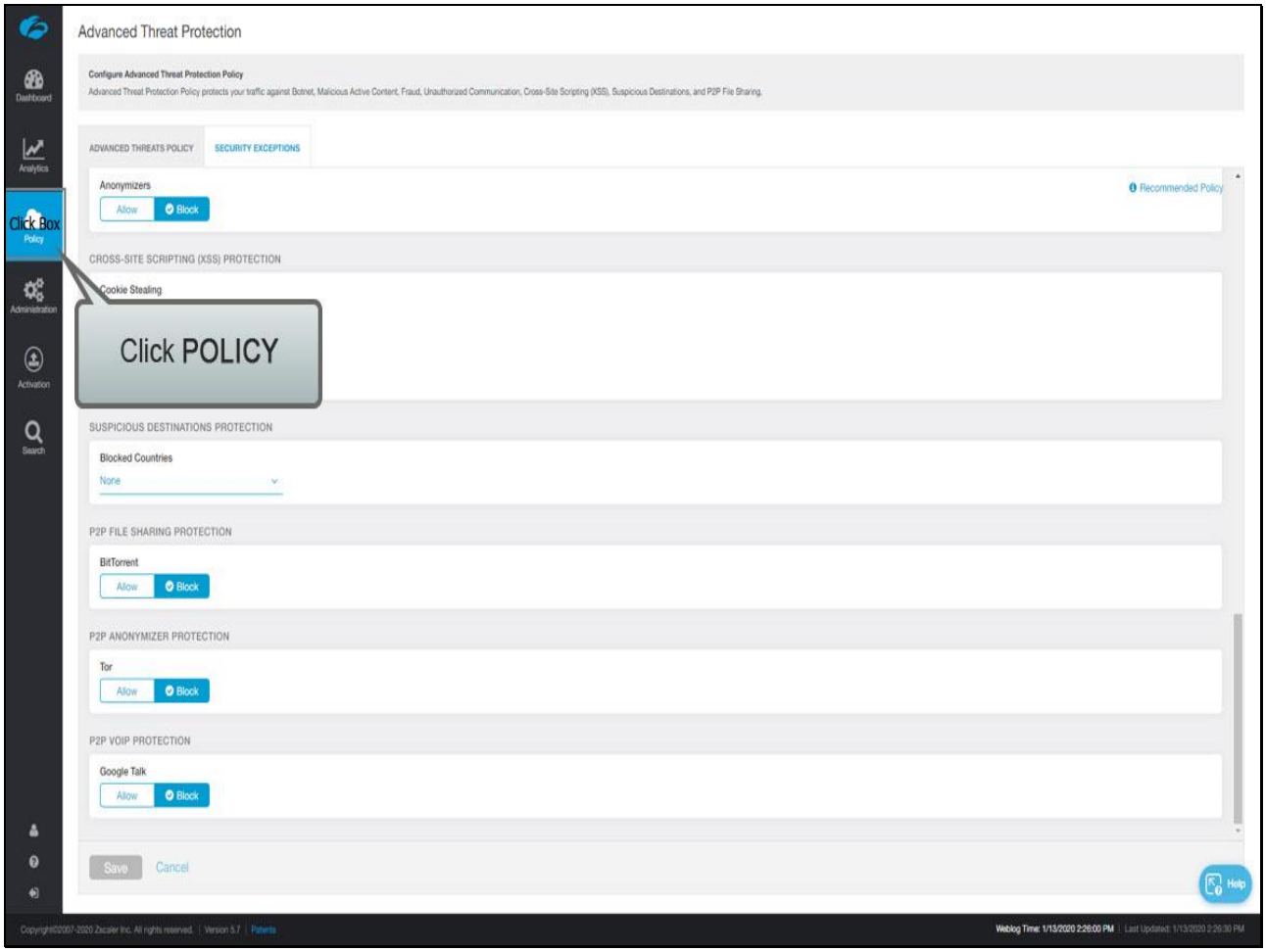
Slide 181 - Slide 181



Slide notes

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

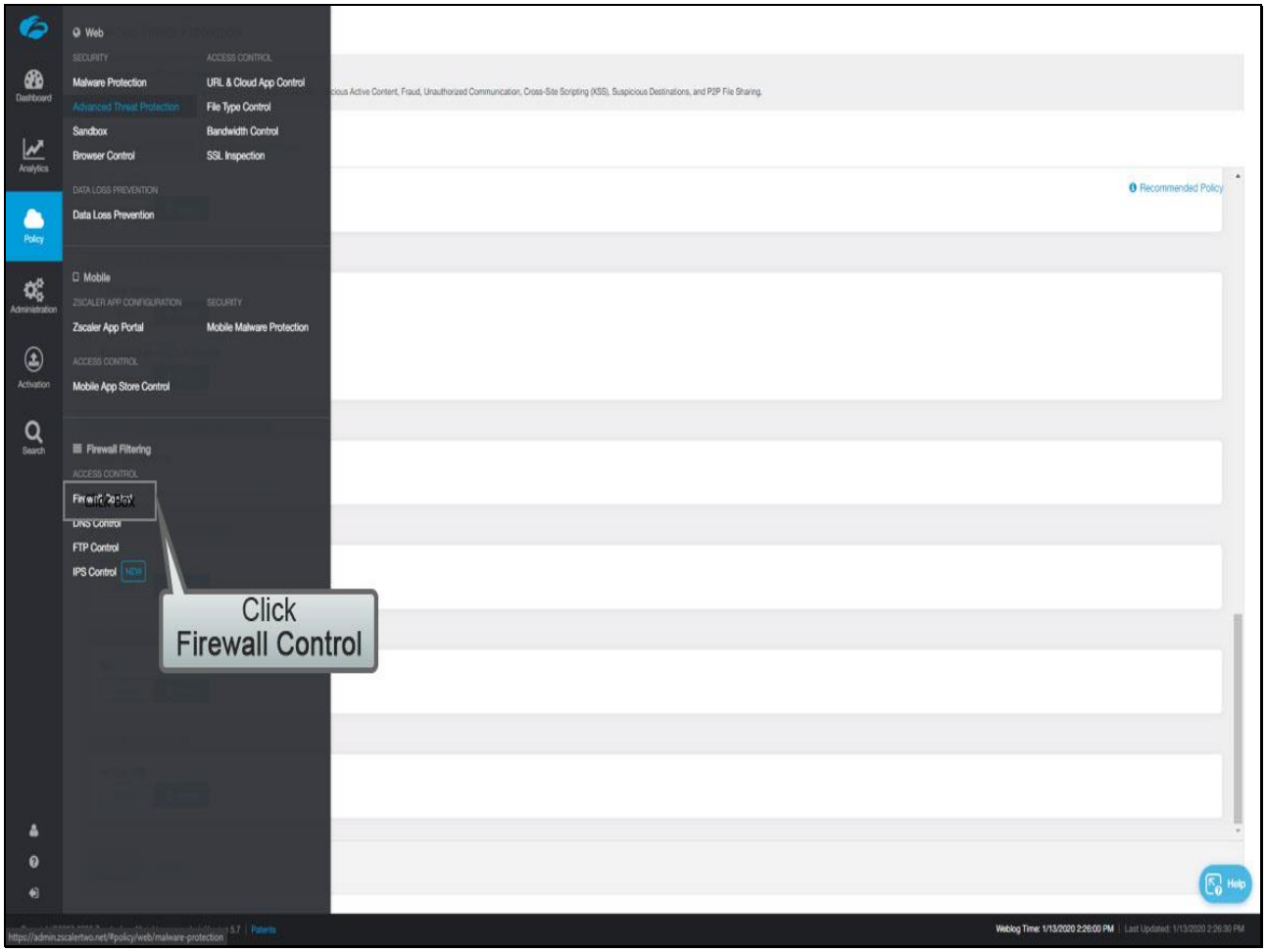
Slide 182 - Slide 182



Slide notes

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

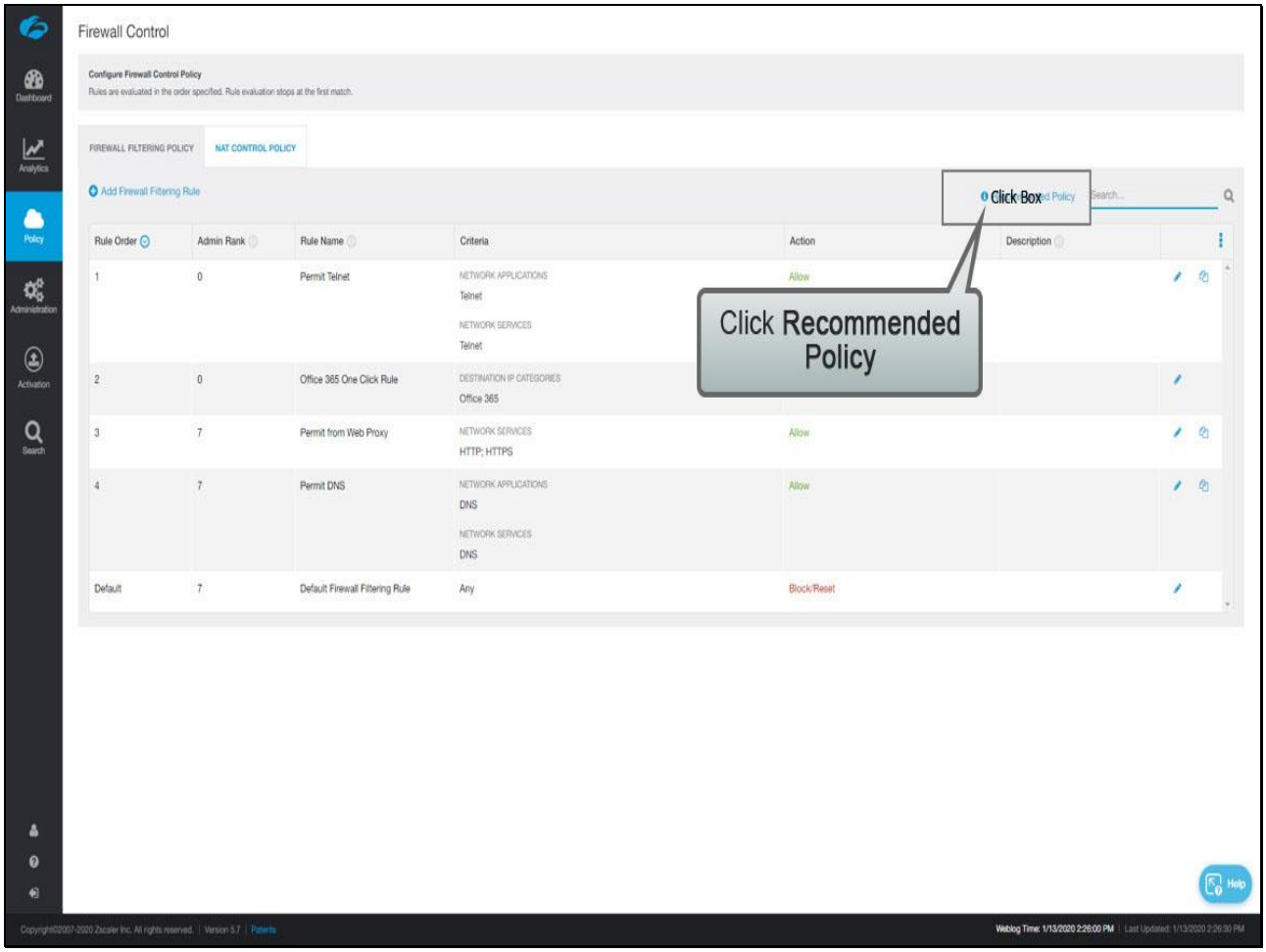
Slide 183 - Slide 183



Slide notes

Click **Firewall Control.**

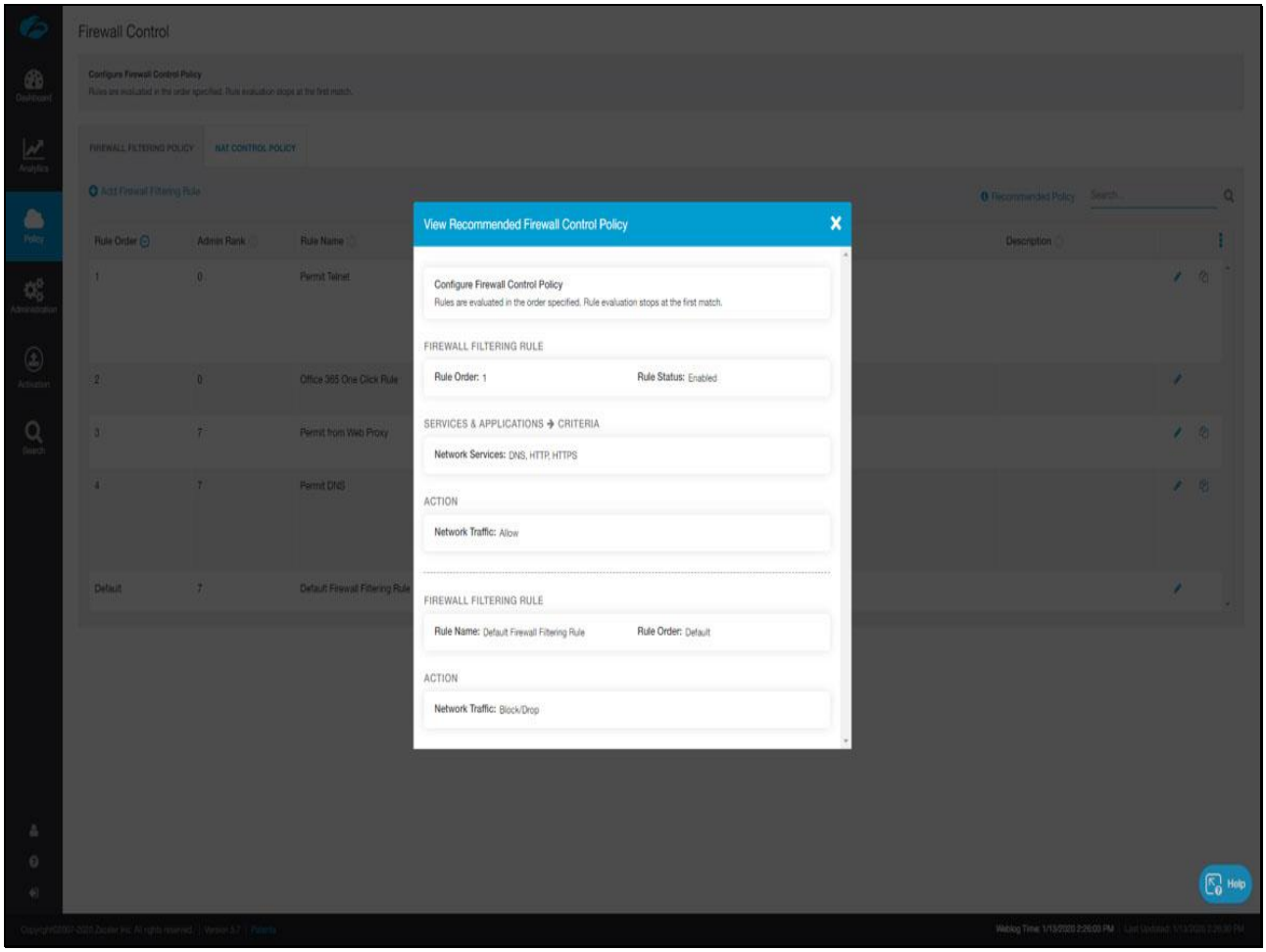
Slide 185 - Slide 185



Slide notes

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

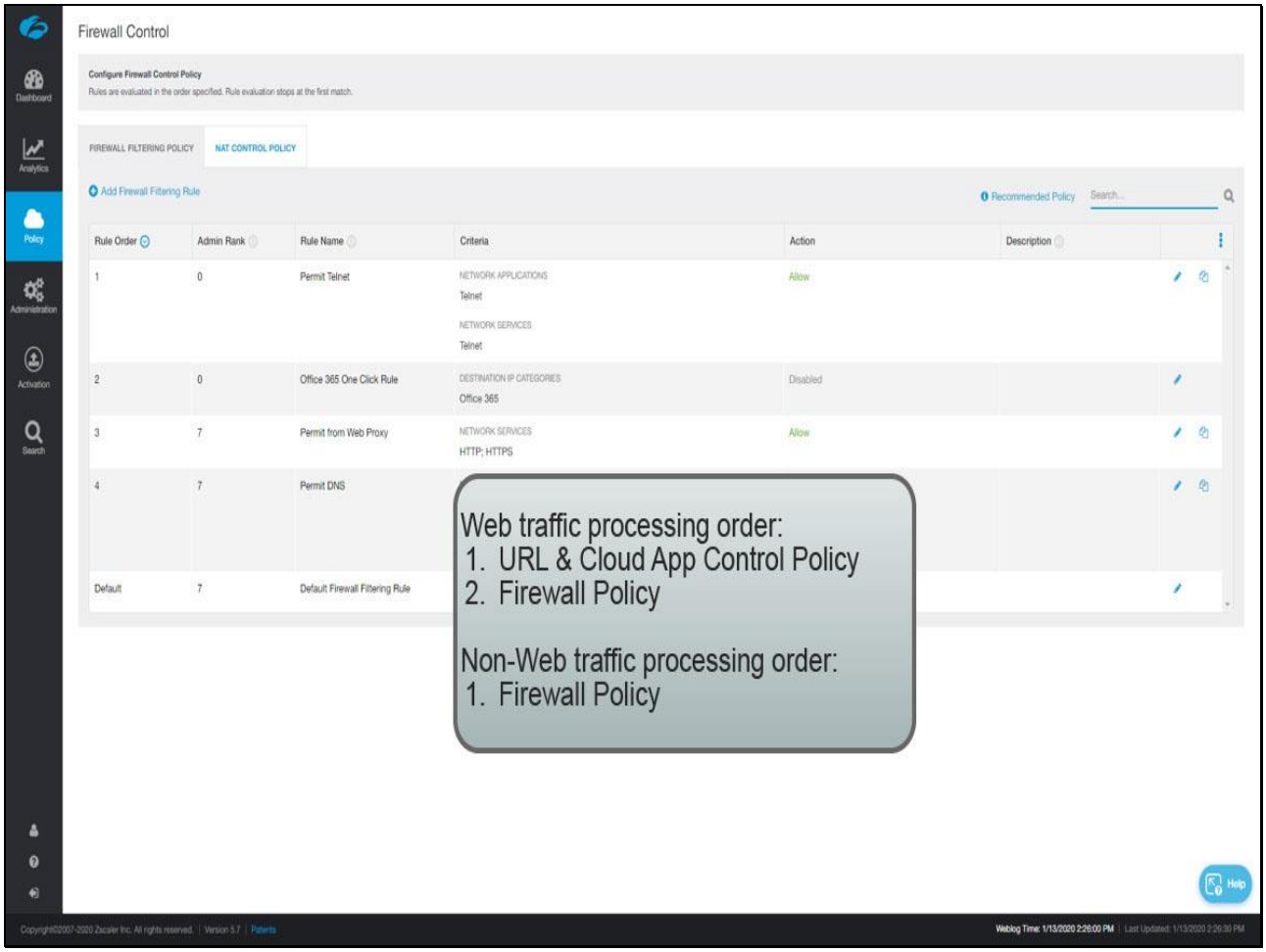
Slide 186 - Slide 186



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

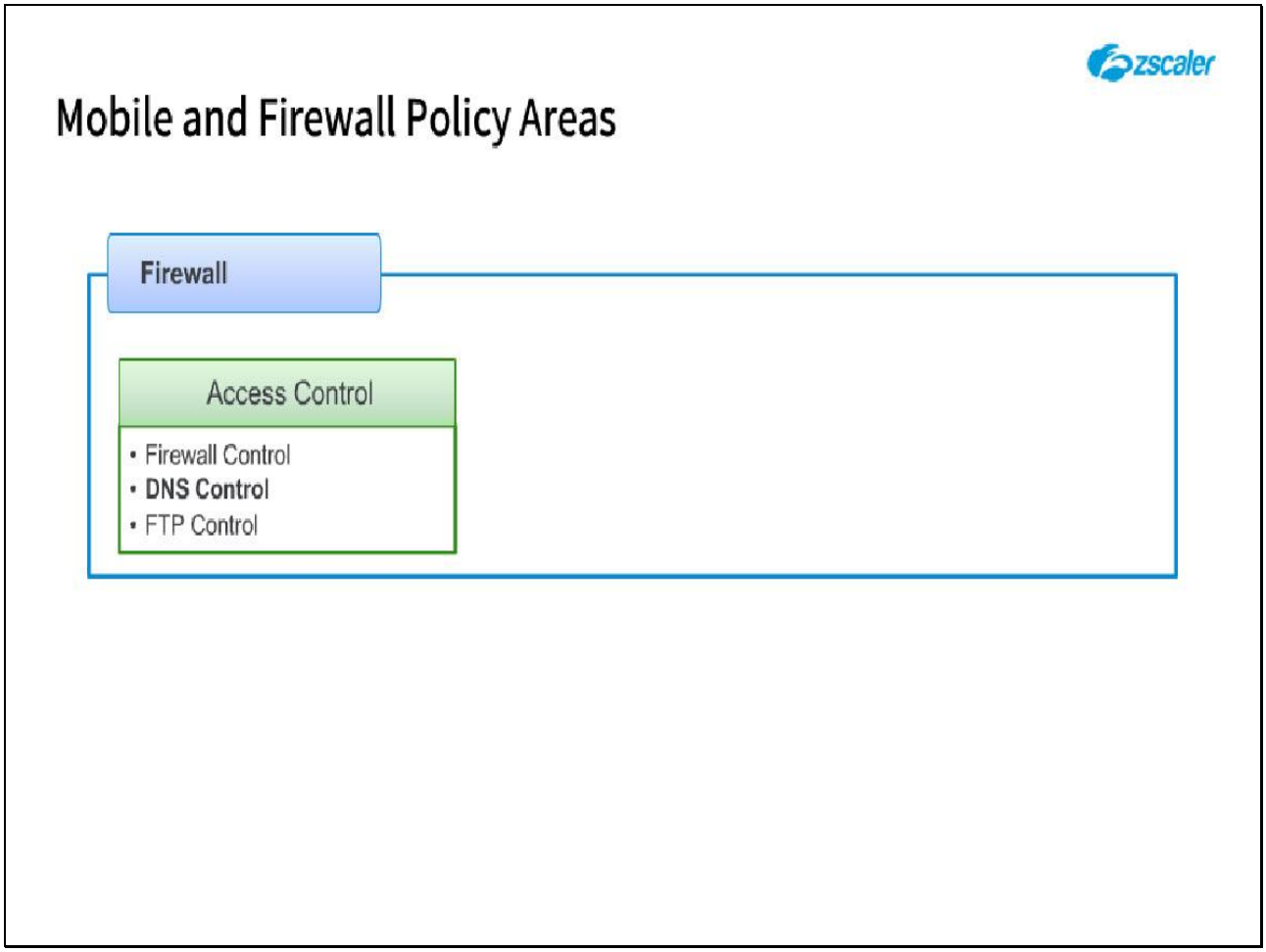


Slide notes

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.

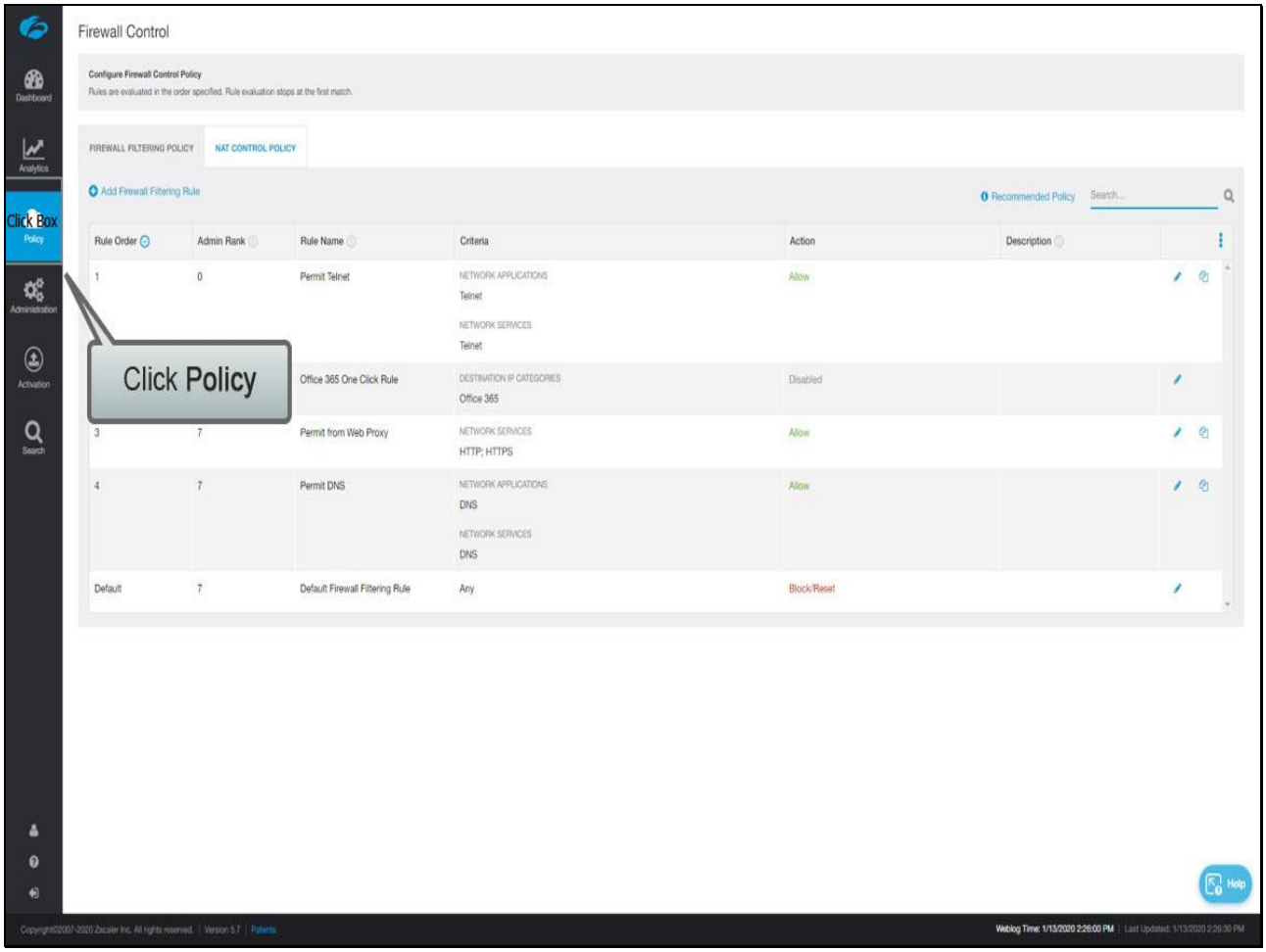
Slide 188 - Mobile and Firewall Policy Areas



Slide notes

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

Slide 189 - Slide 189



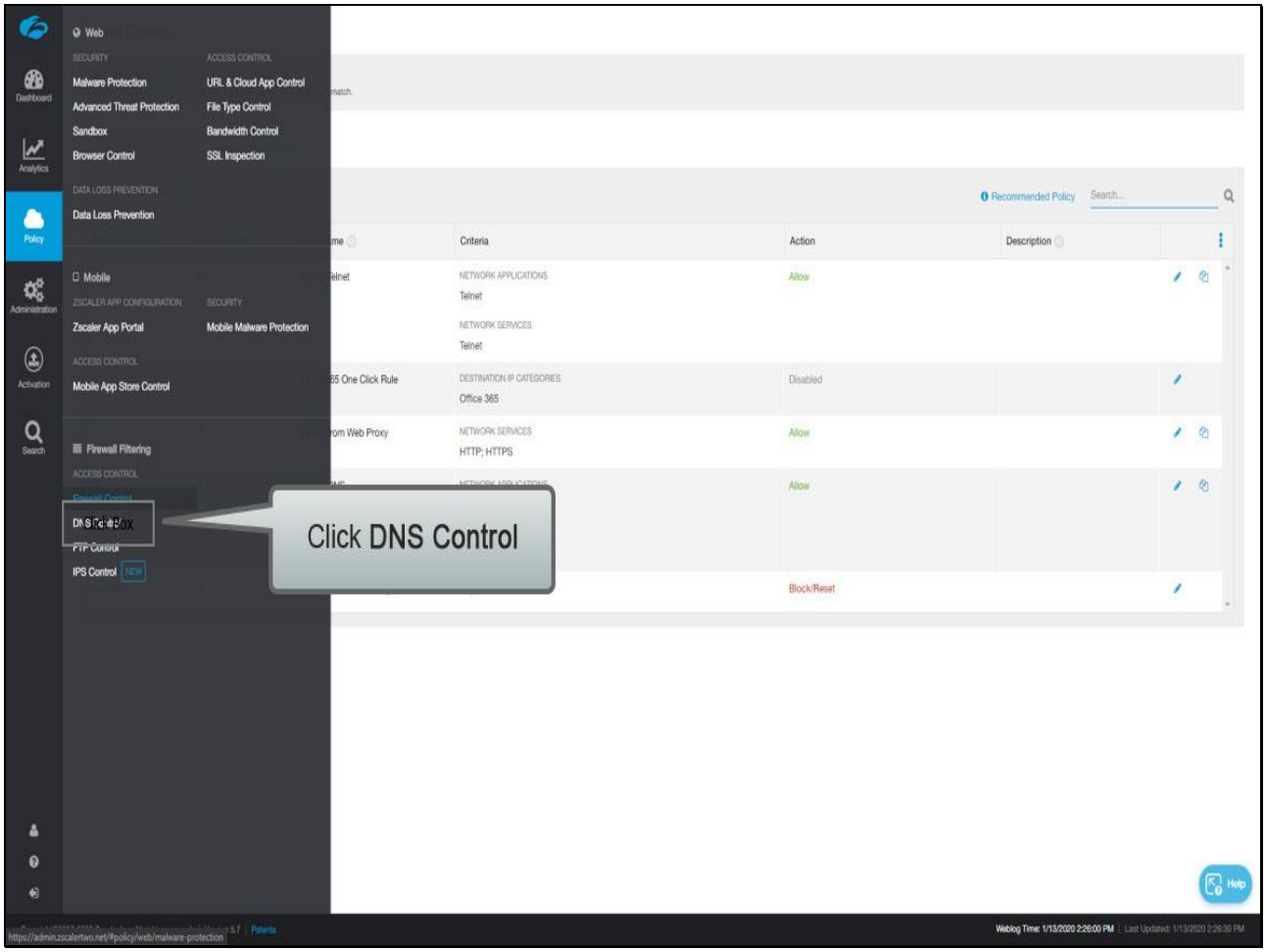
Slide notes

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**.

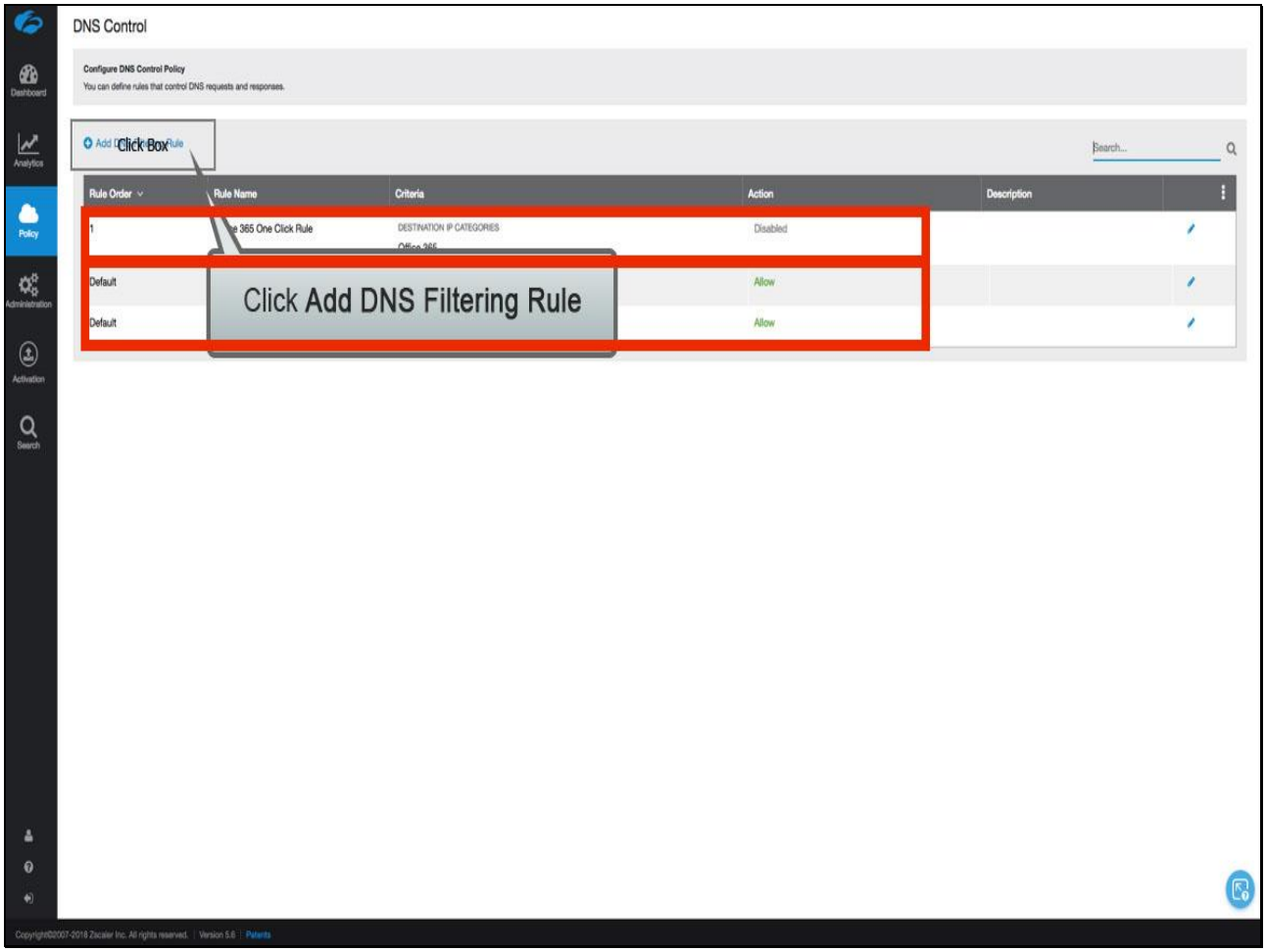
Slide 190 - Slide 190



Slide notes

And then click on **DNS Control**.

Slide 192 - Slide 192



Slide notes

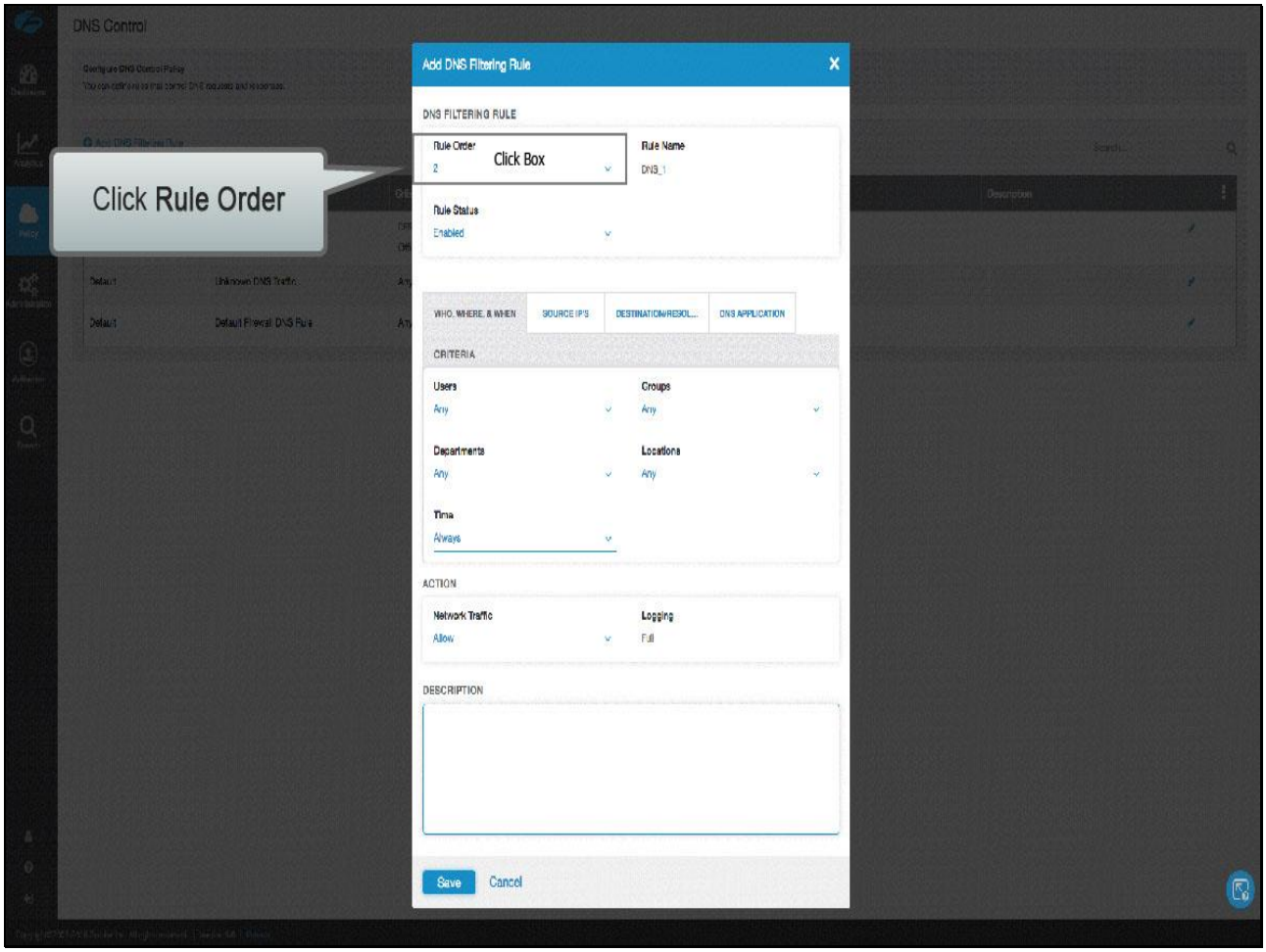
Here a system generated rule for Microsoft Office 365 traffic was added automatically at position 1 when the Microsoft Office **One Click** feature was enabled. The rule is currently in the disabled state, because **One Click** was later disabled.

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**.

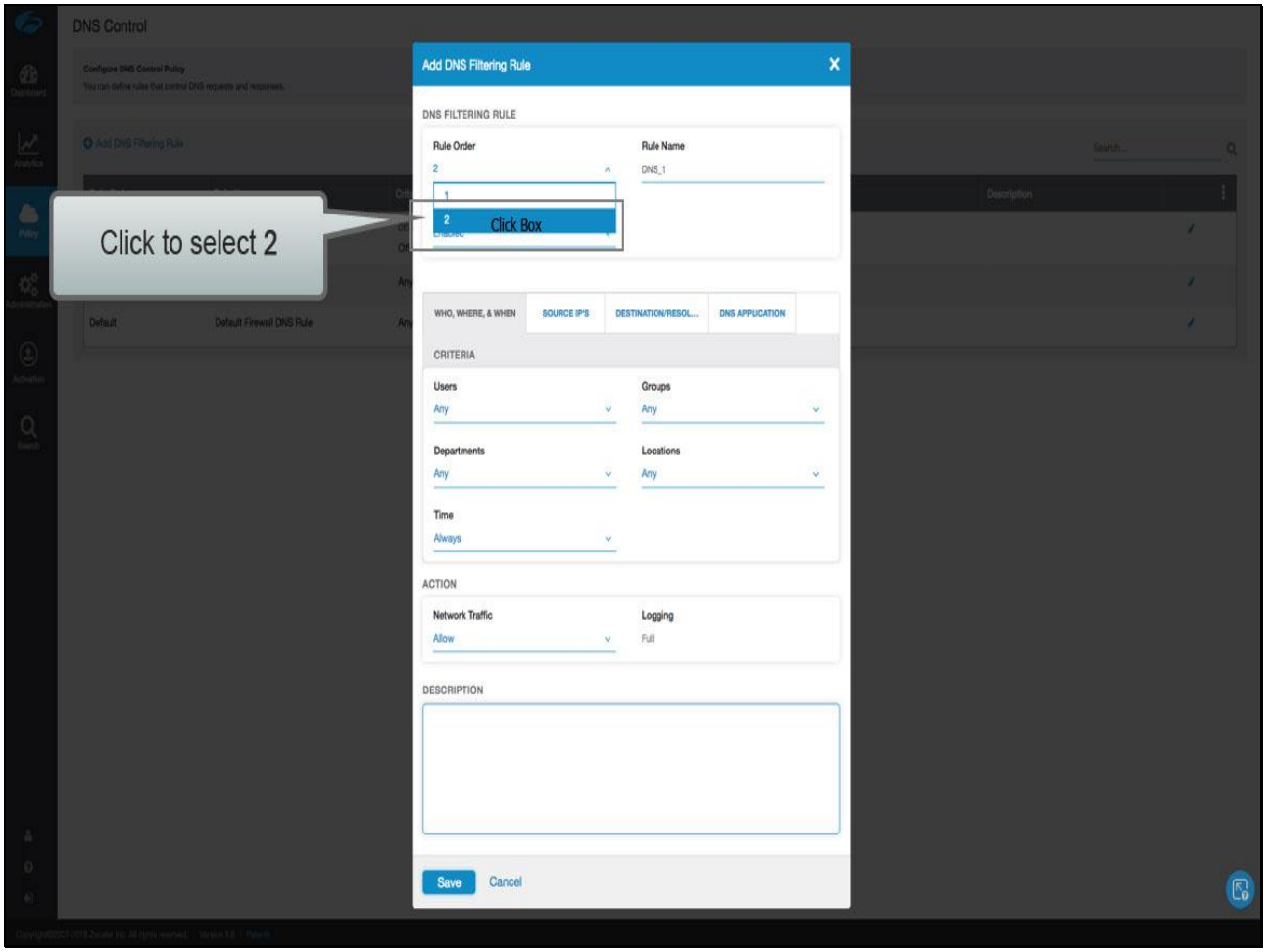
Slide 193 - Slide 193



Slide notes

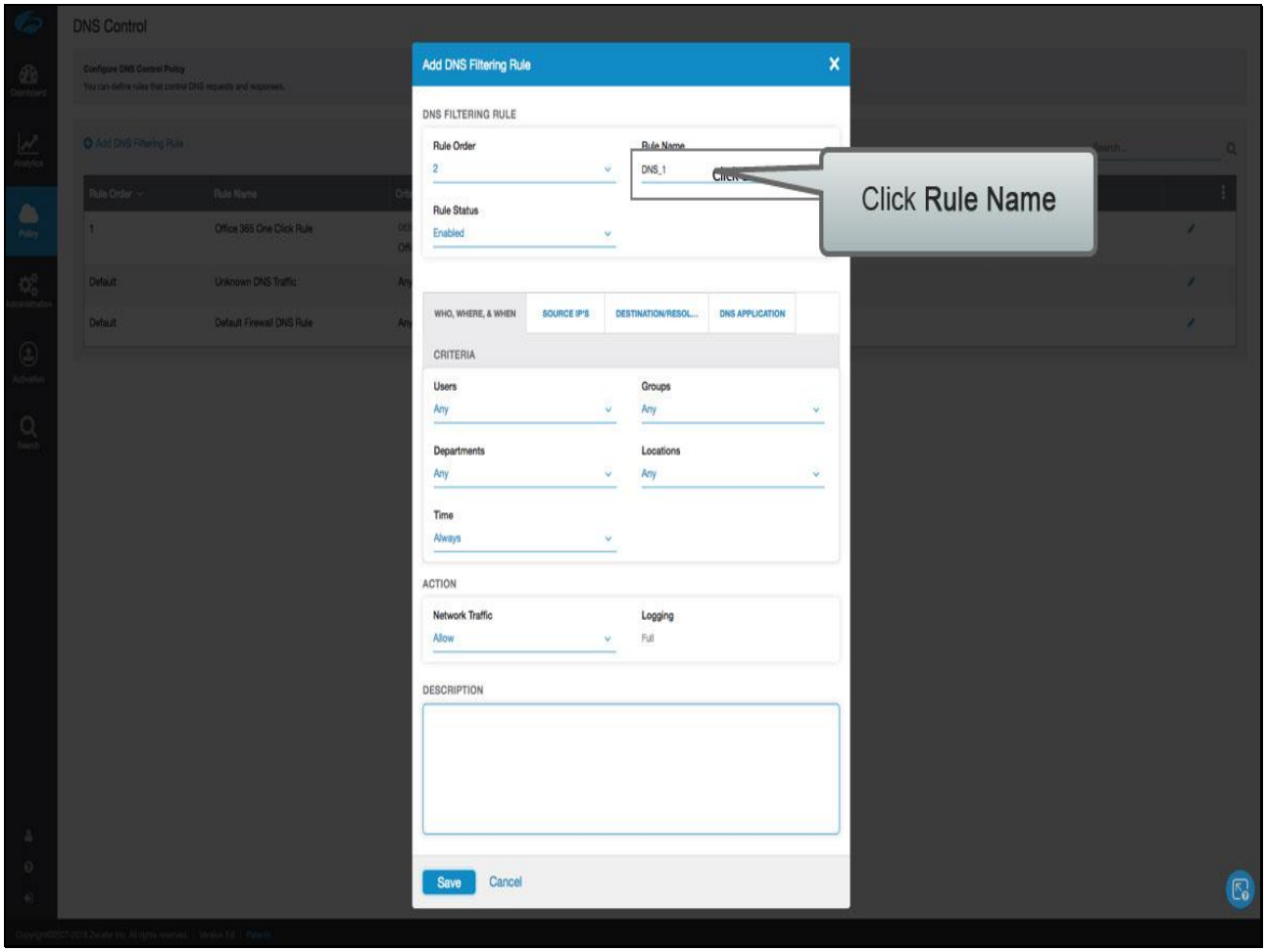
Specify **Rule Order**, **Rule Name**, and **Rule Status**.

Slide 194 - Slide 194



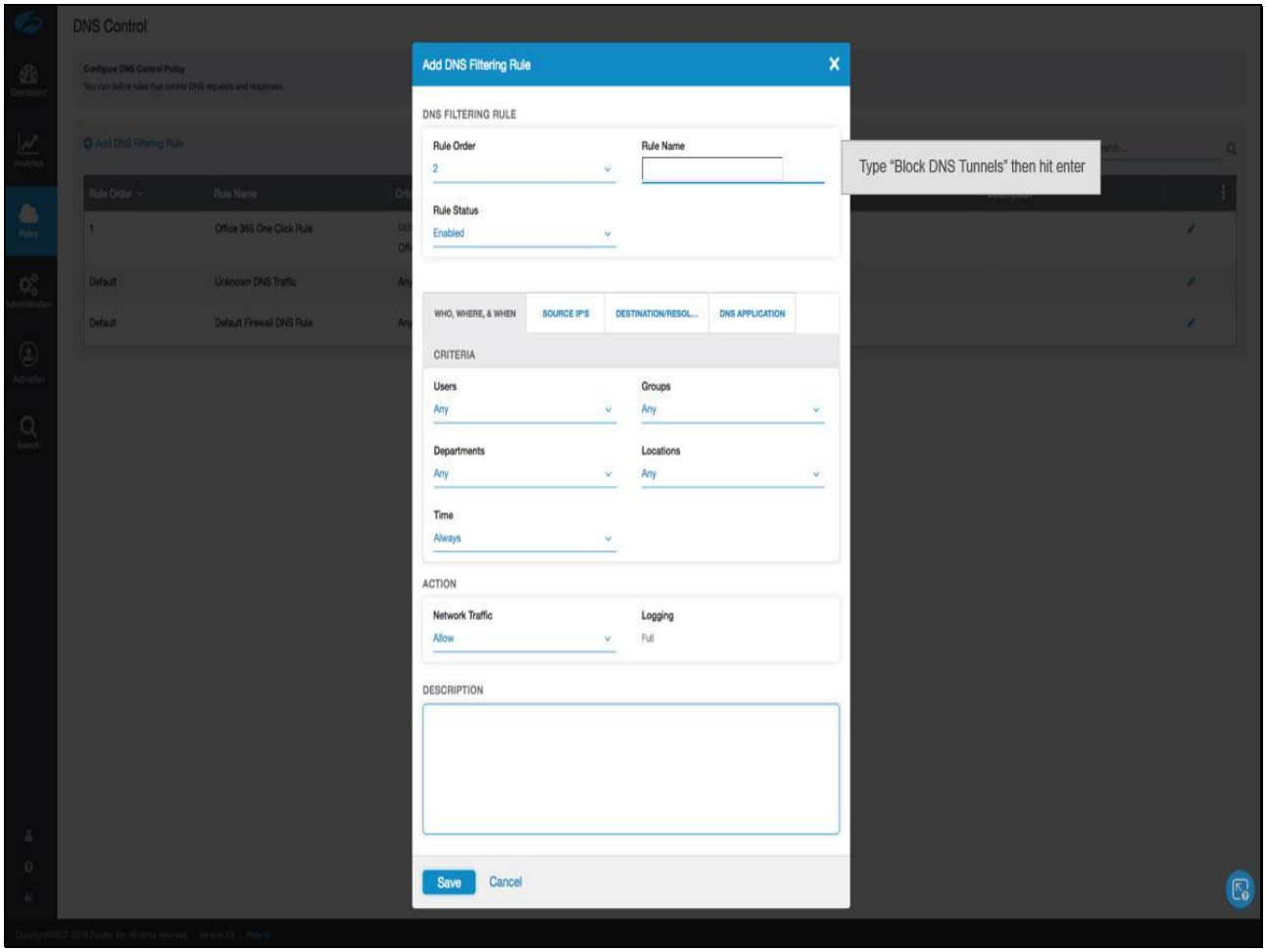
Slide notes

Slide 195 - Slide 195



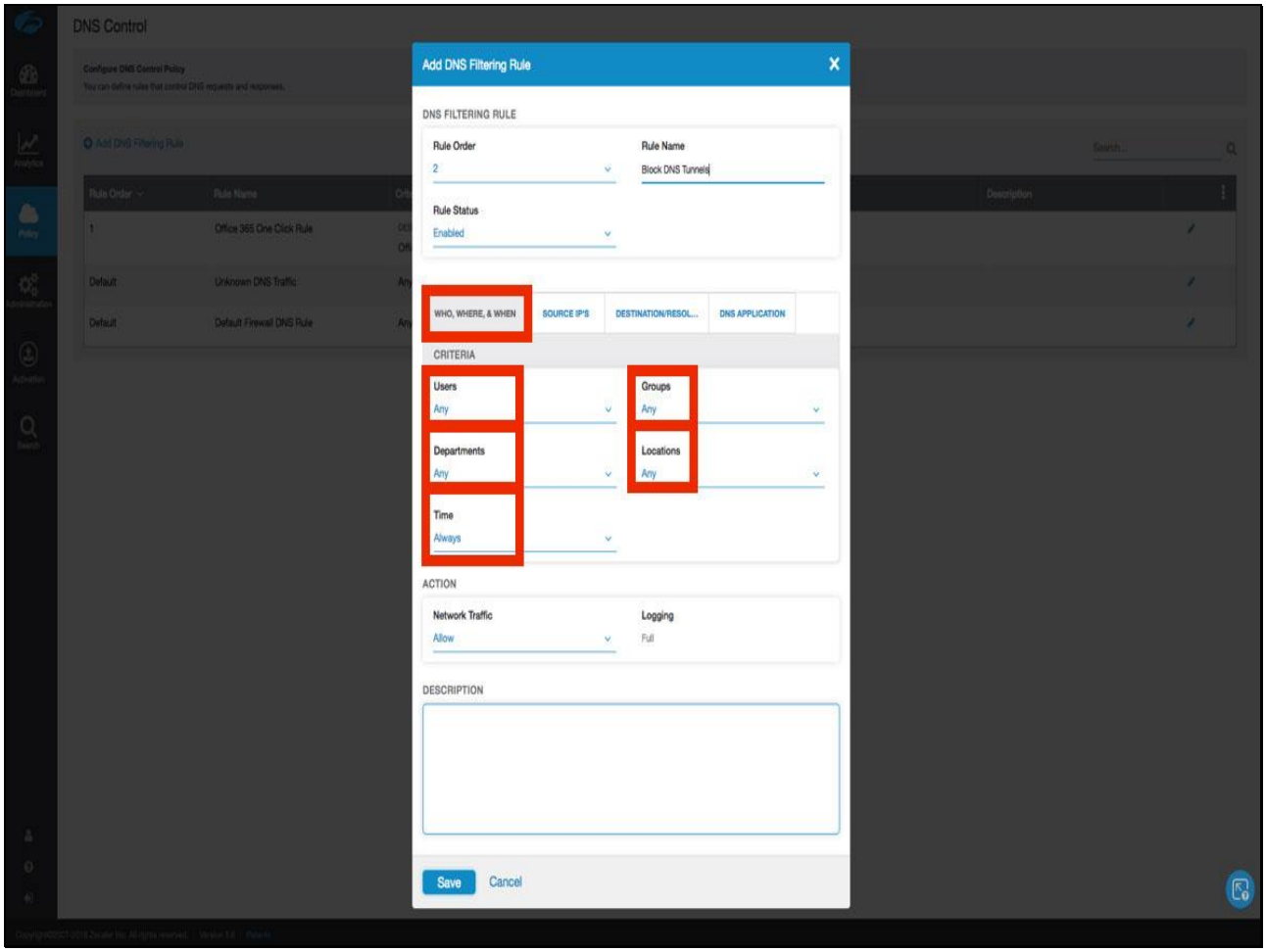
Slide notes

Slide 196 - Slide 196



Slide notes

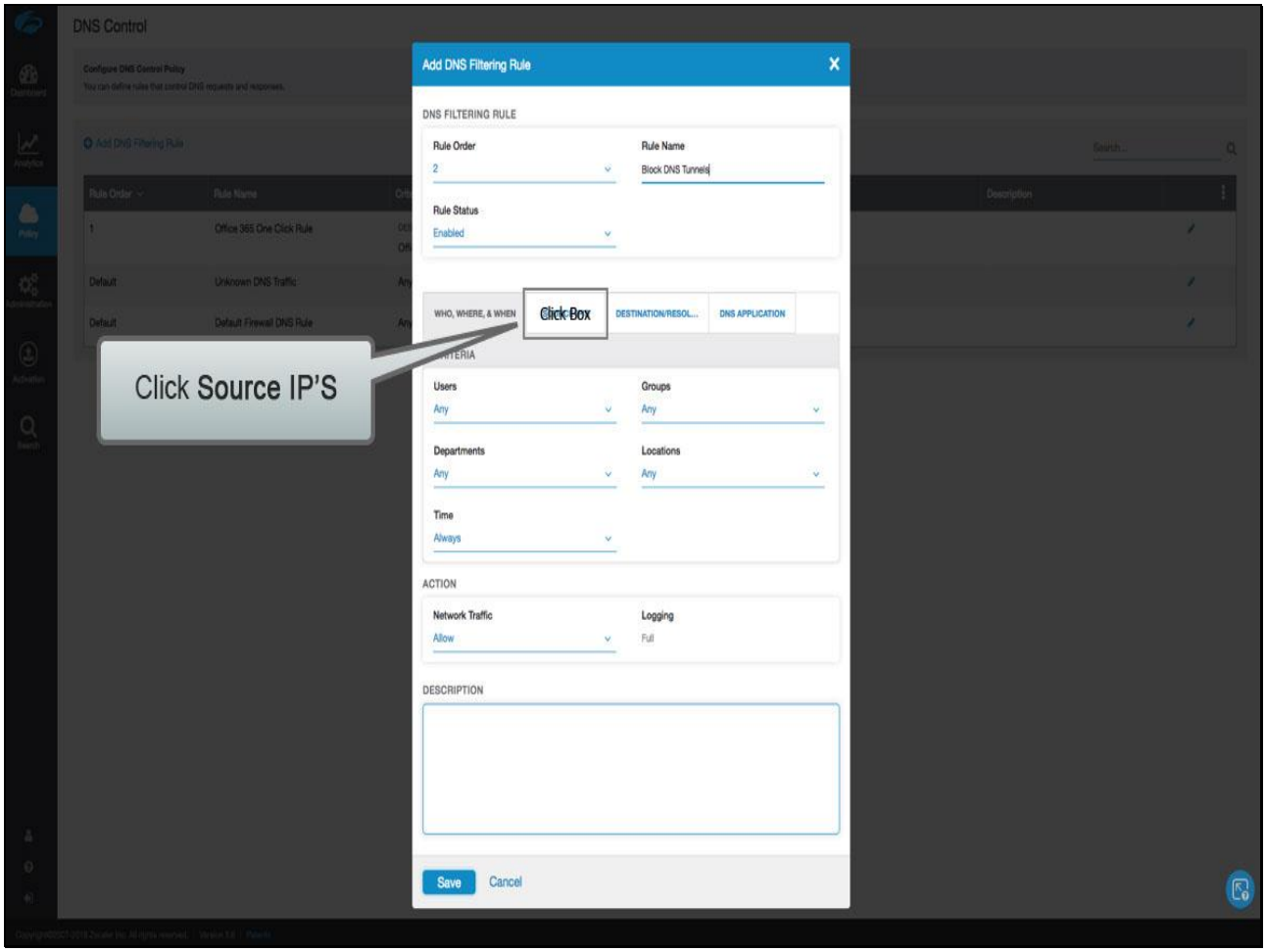
Slide 197 - Slide 197



Slide notes

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

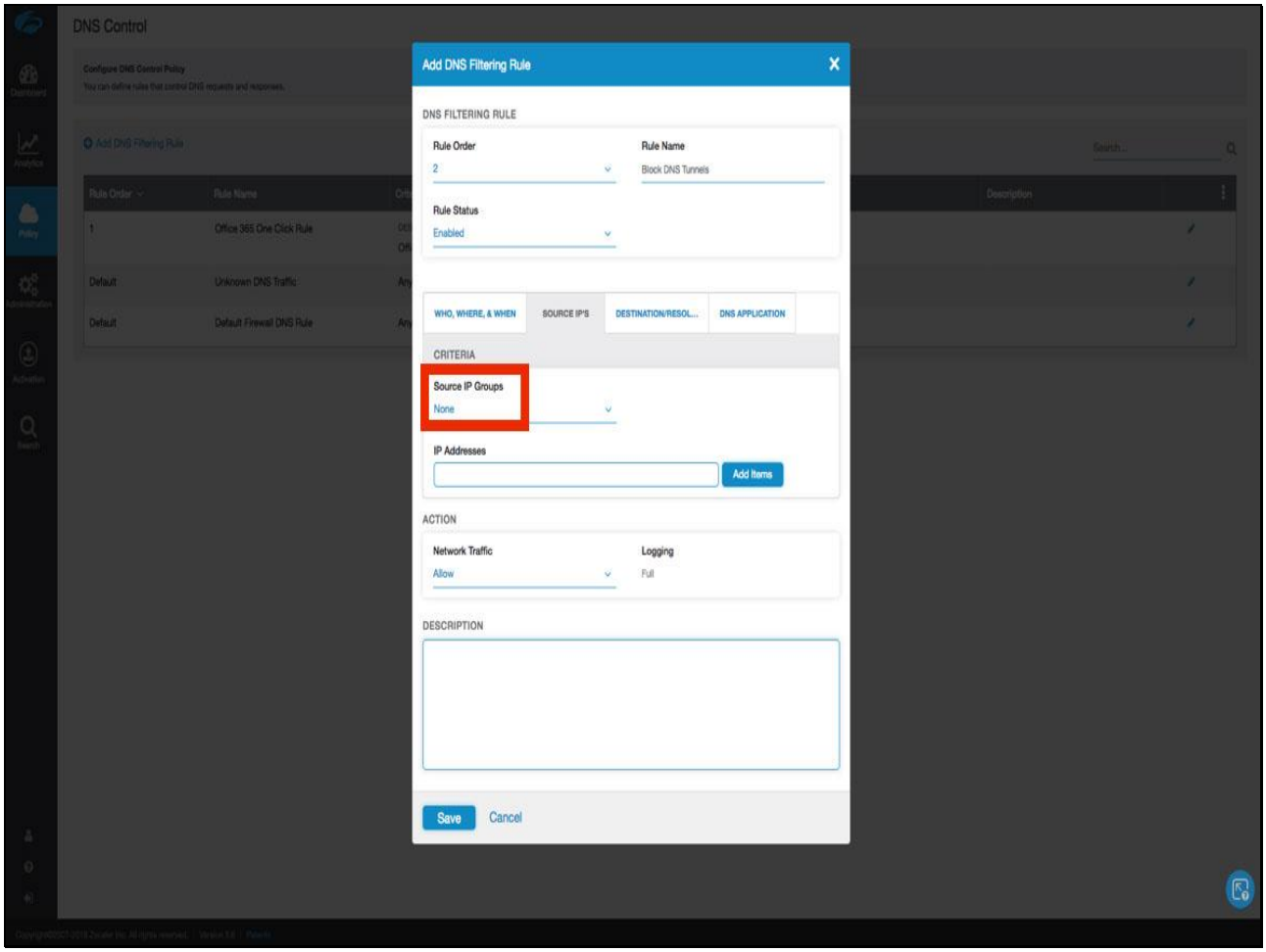
Slide 198 - Slide 198



Slide notes

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

Slide 199 - Slide 199

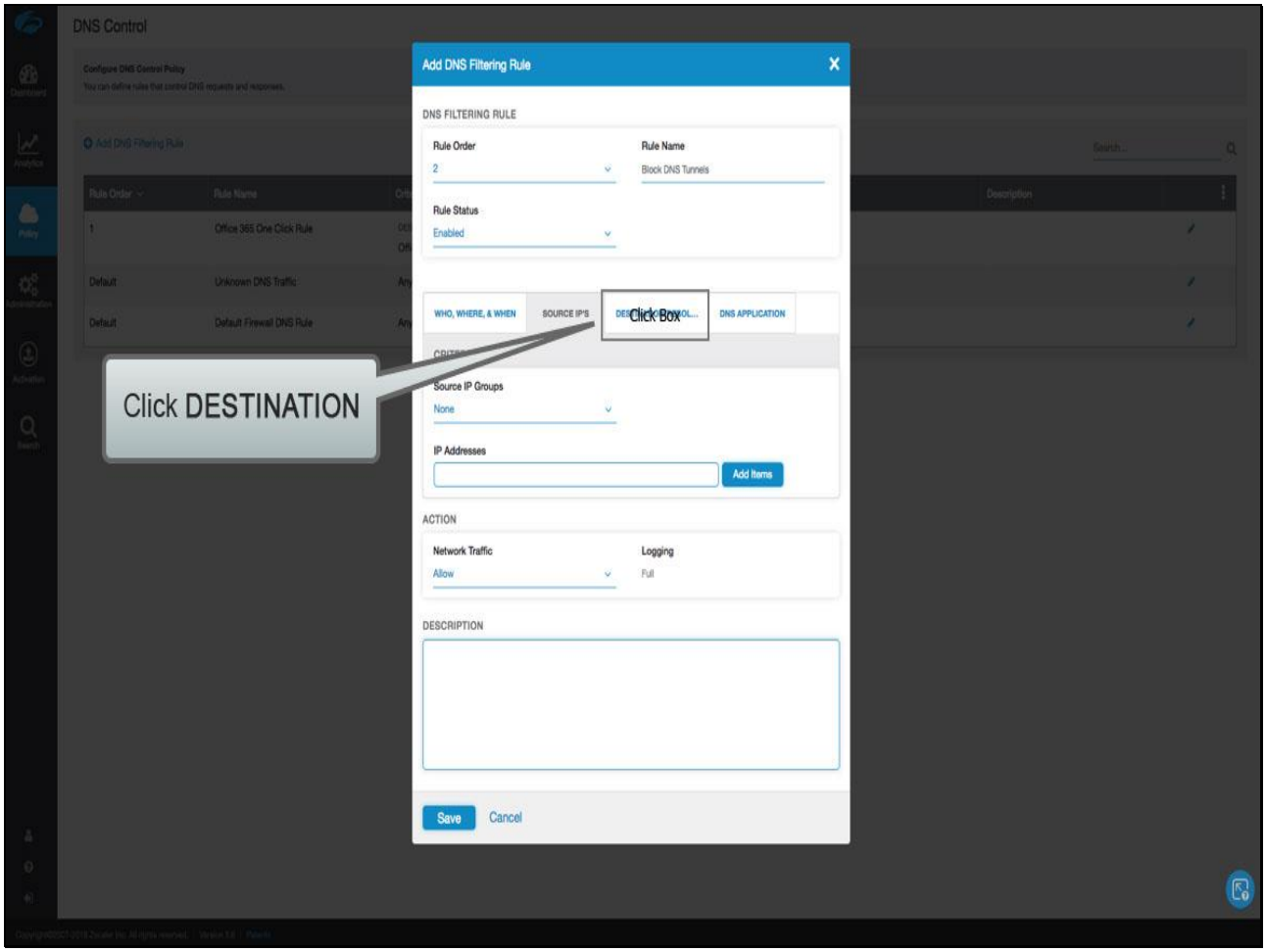


Slide notes

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.

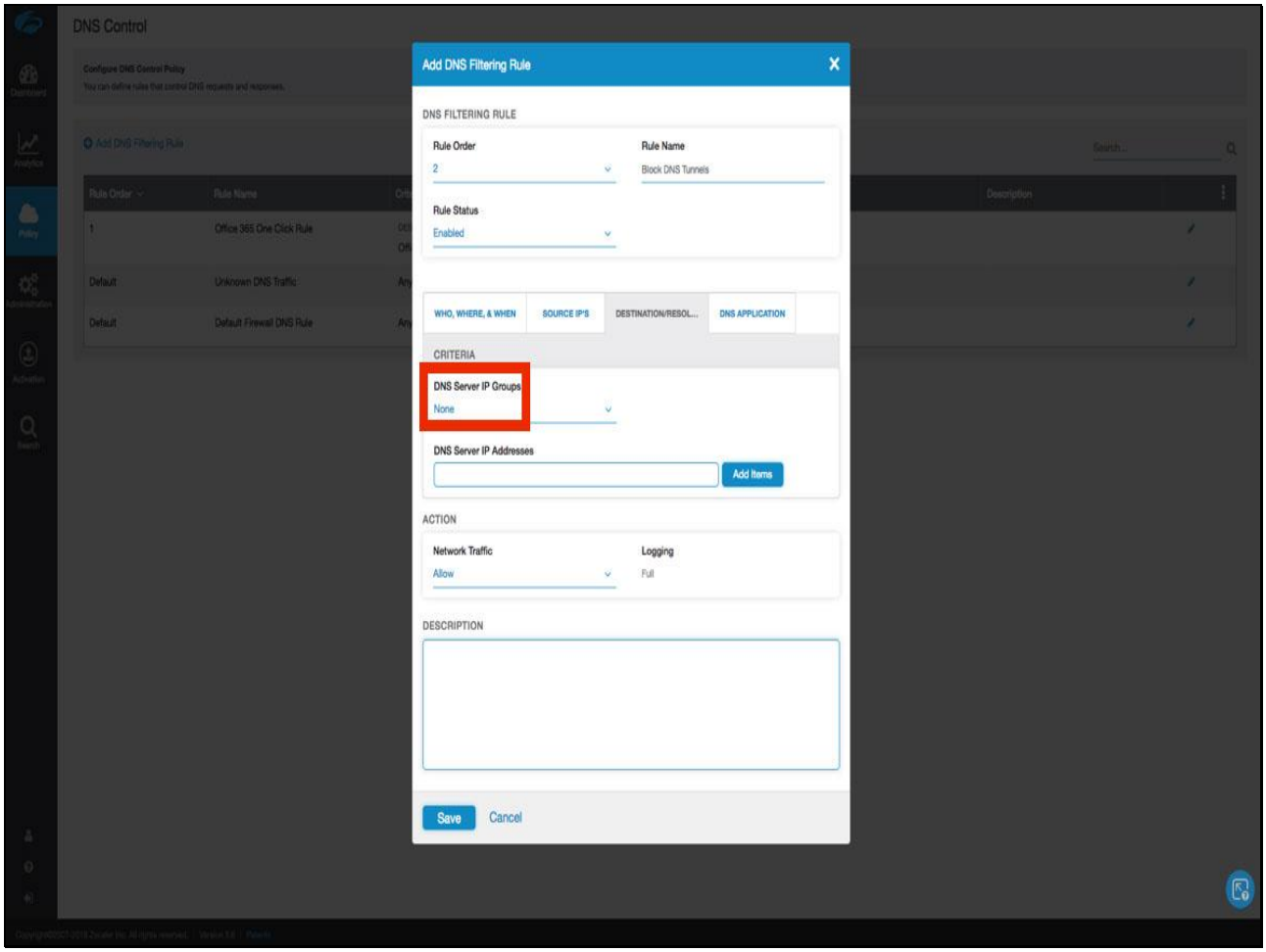
Slide 200 - Slide 200



Slide notes

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

Slide 201 - Slide 201

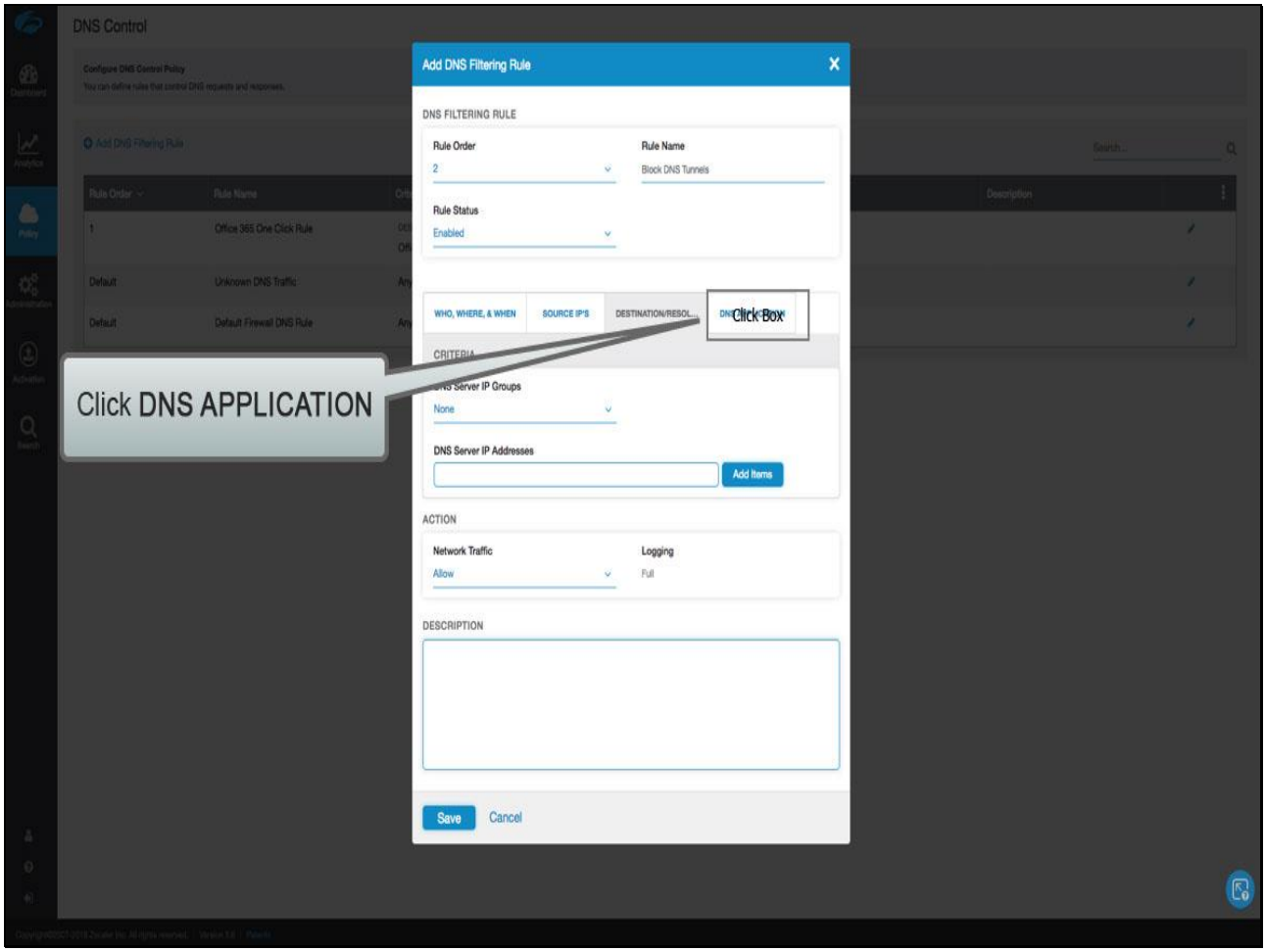


Slide notes

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.

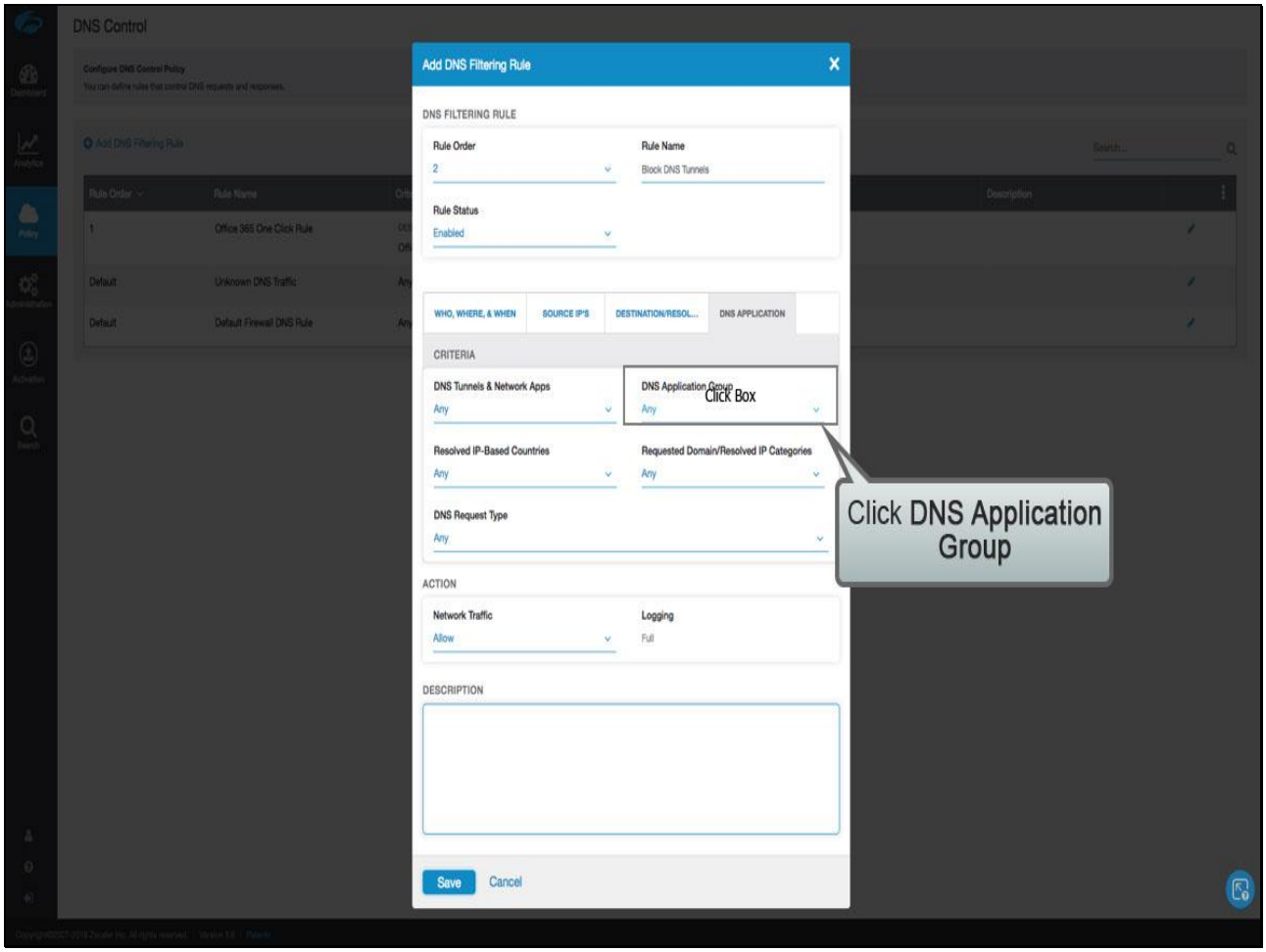
Slide 202 - Slide 202



Slide notes

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

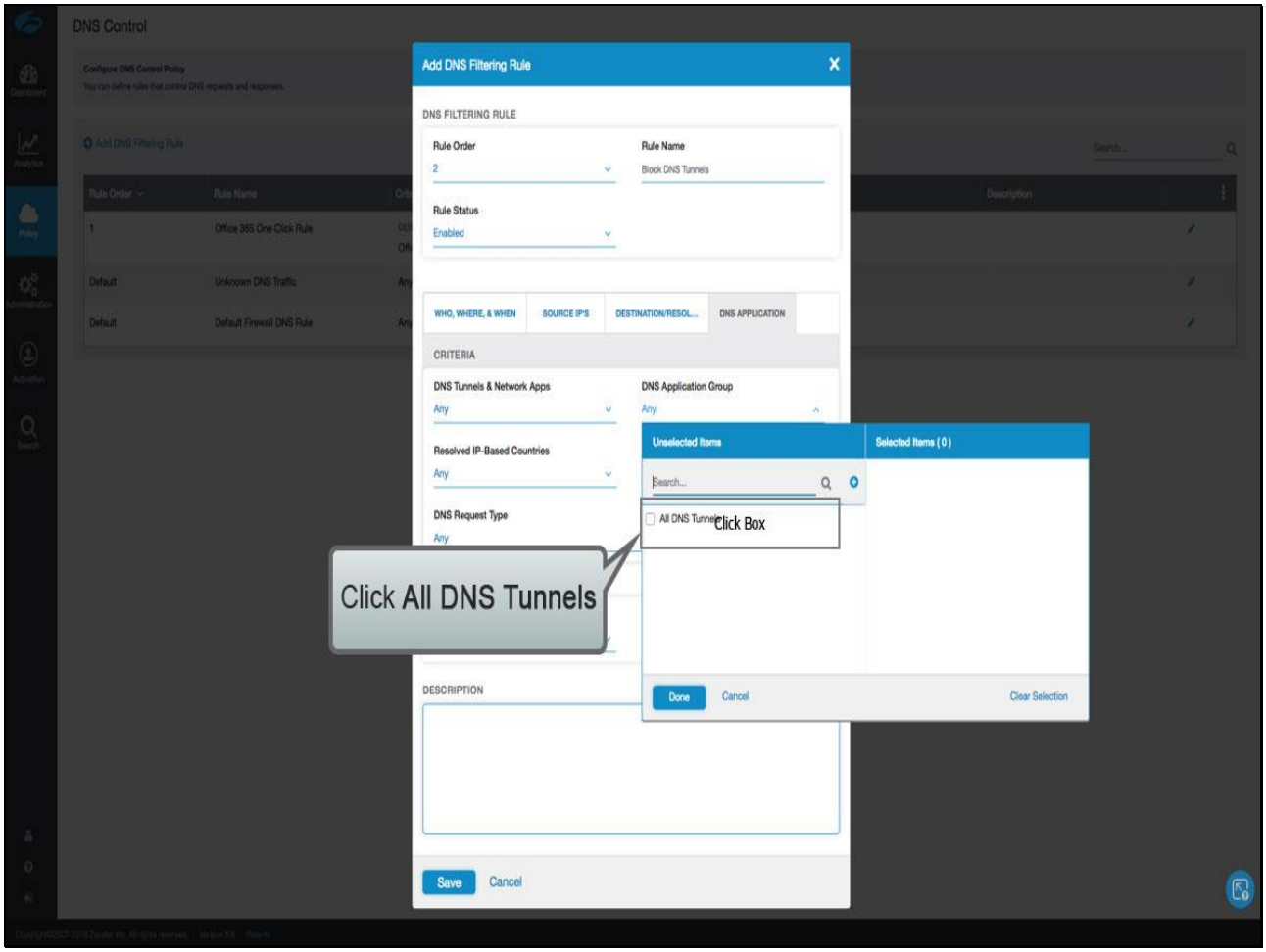
Slide 203 - Slide 203



Slide notes

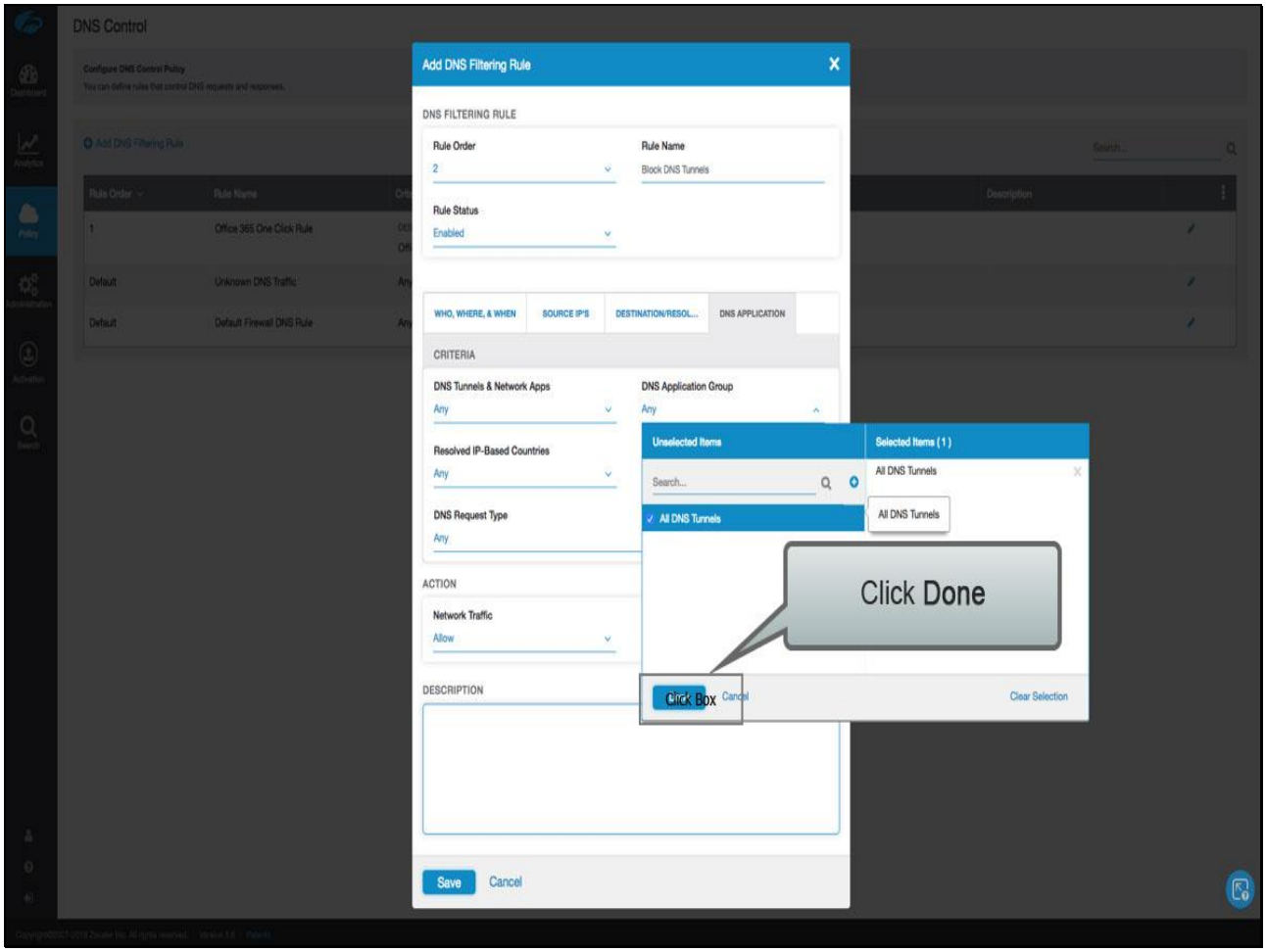
Configure **DNS APPLICATION** to apply to the DNS Application Group added earlier for **All DNS Tunnels**.

Slide 204 - Slide 204



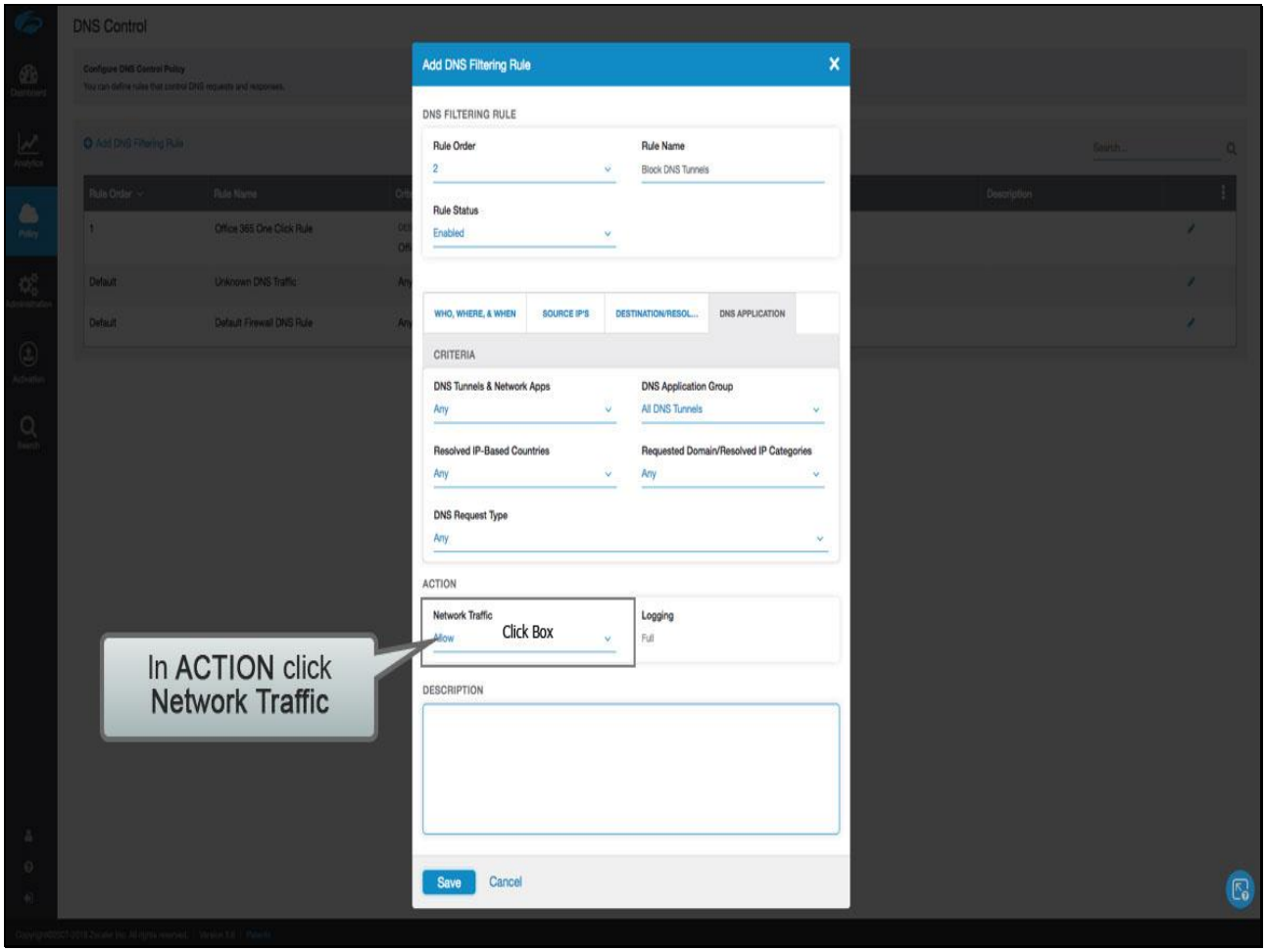
Slide notes

Slide 205 - Slide 205



Slide notes

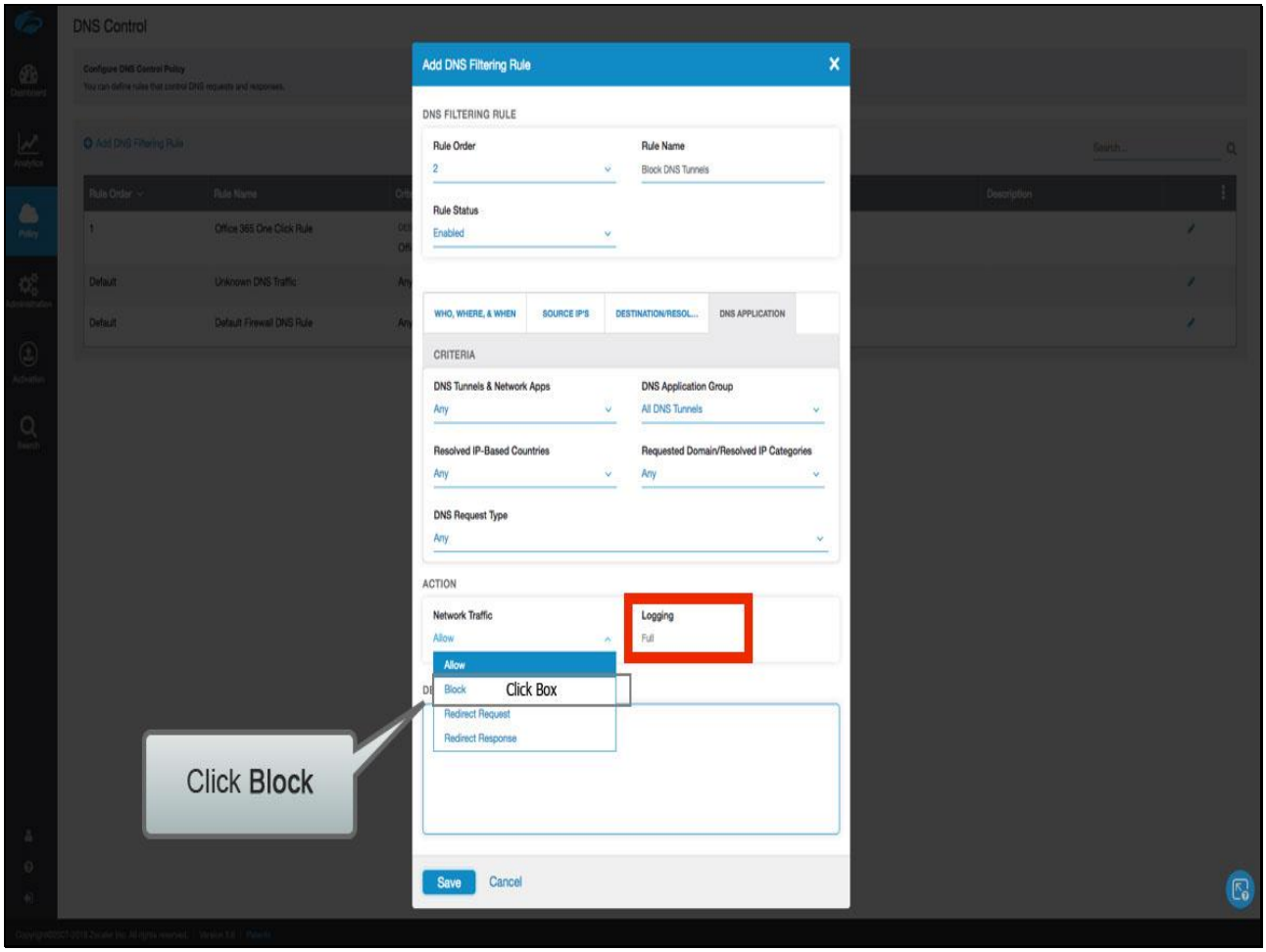
Slide 206 - Slide 206



Slide notes

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

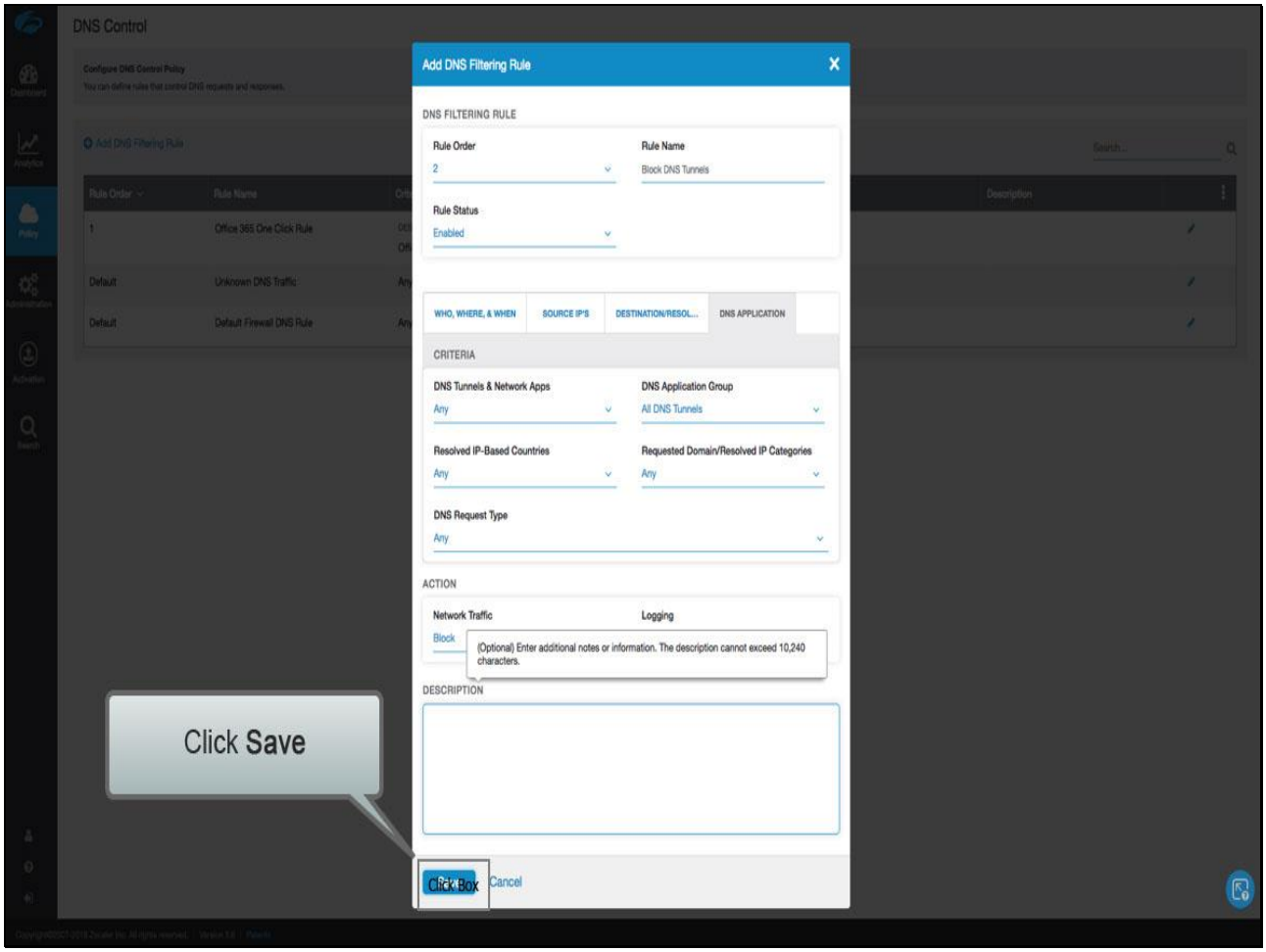
Slide 207 - Slide 207



Slide notes

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

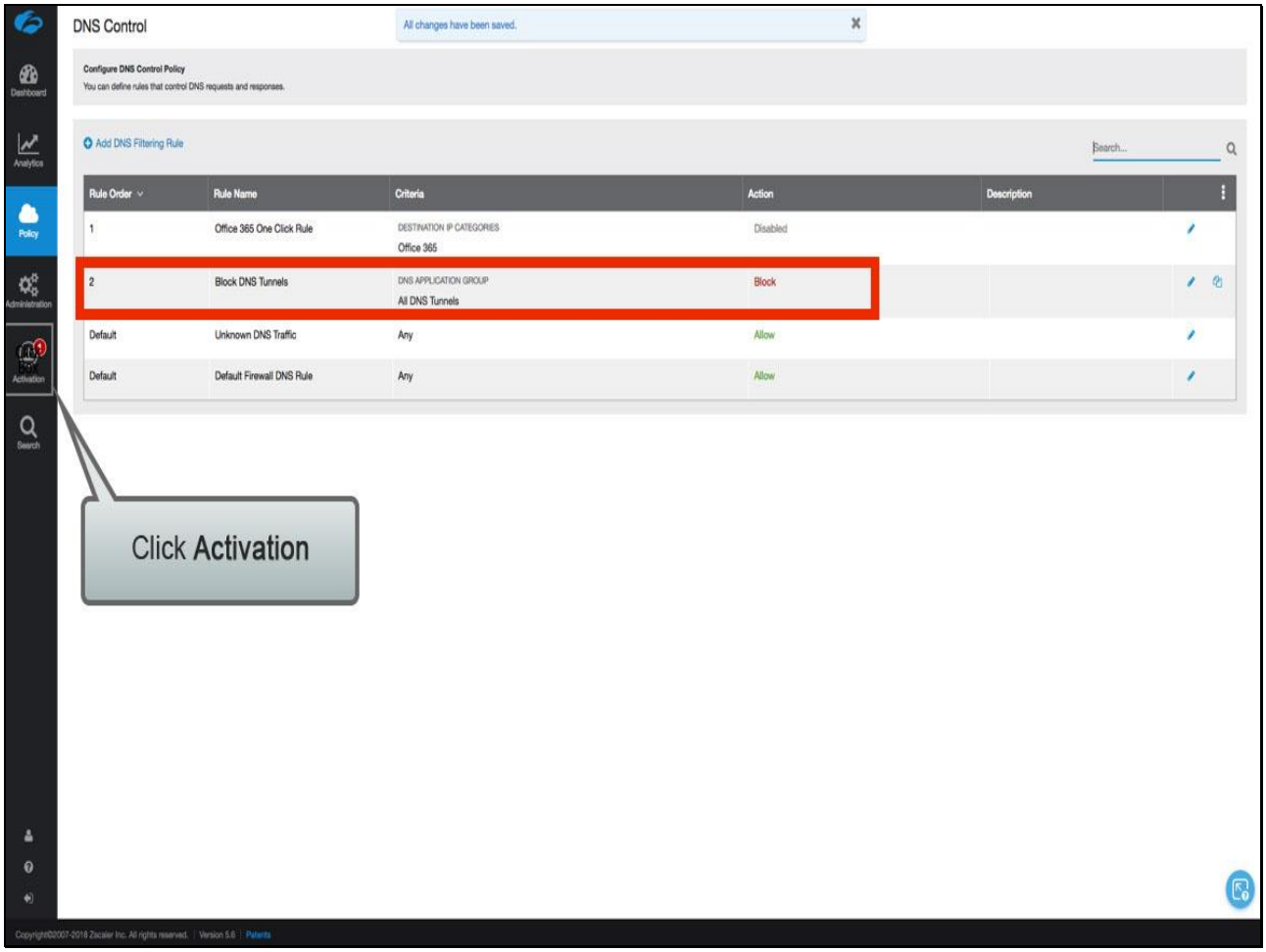
Slide 208 - Slide 208



Slide notes

Click **Save**.

Slide 209 - Slide 209



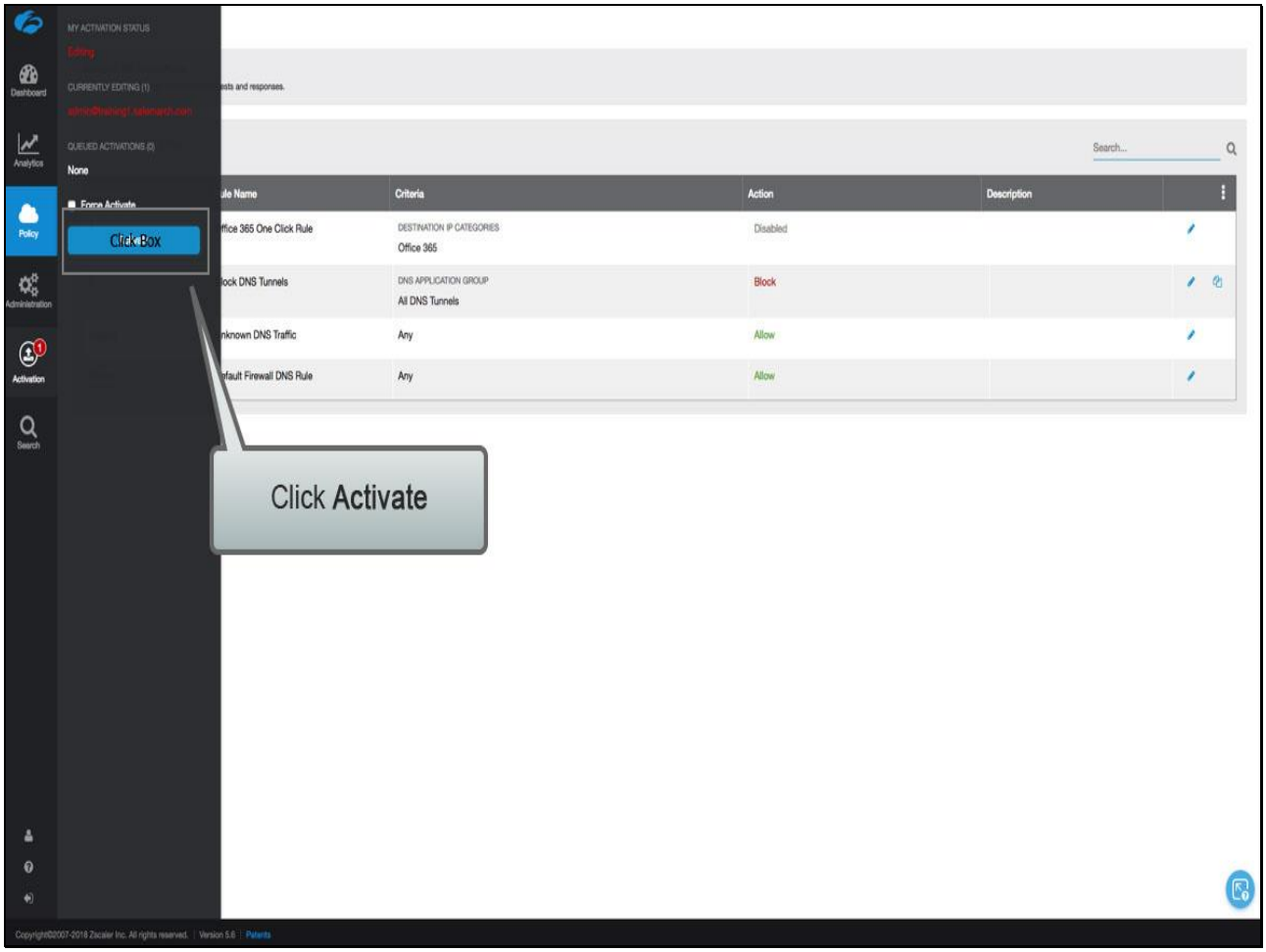
Slide notes

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.

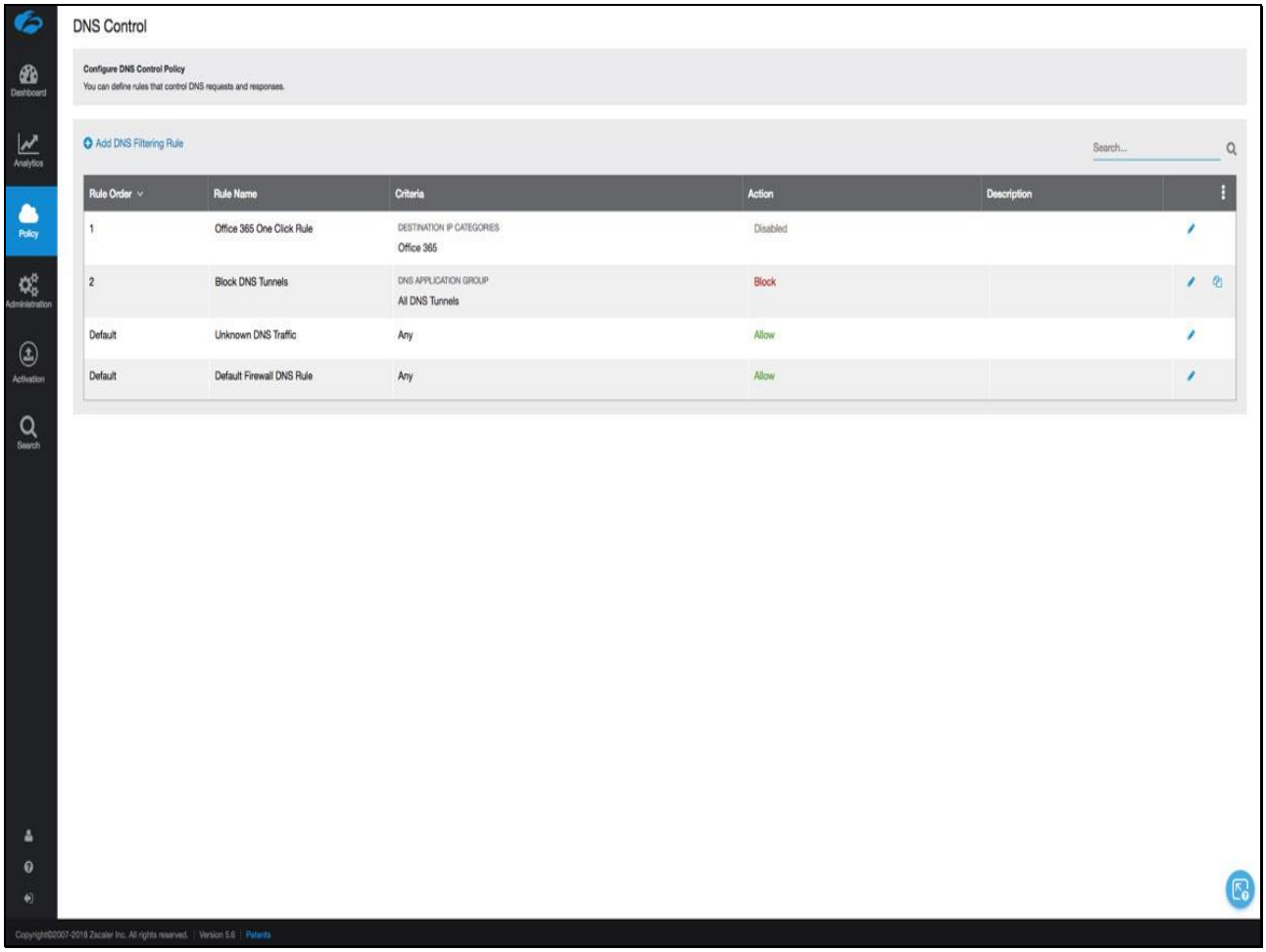
And **Activate** the changes.

Slide 210 - Slide 210



Slide notes

Slide 211 - Slide 211



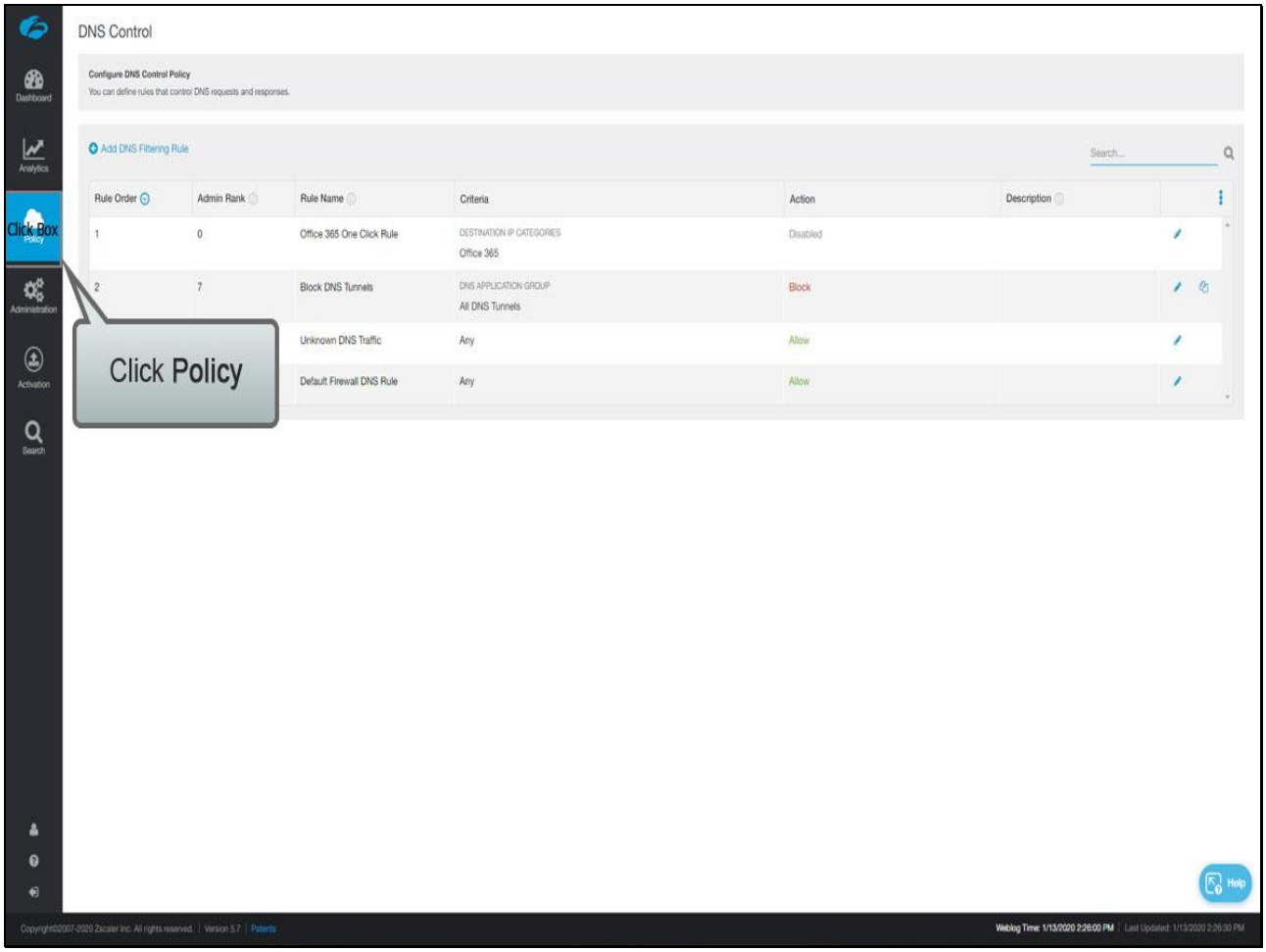
Slide notes

Slide 212 - Mobile and Firewall Policy Areas

Slide notes

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

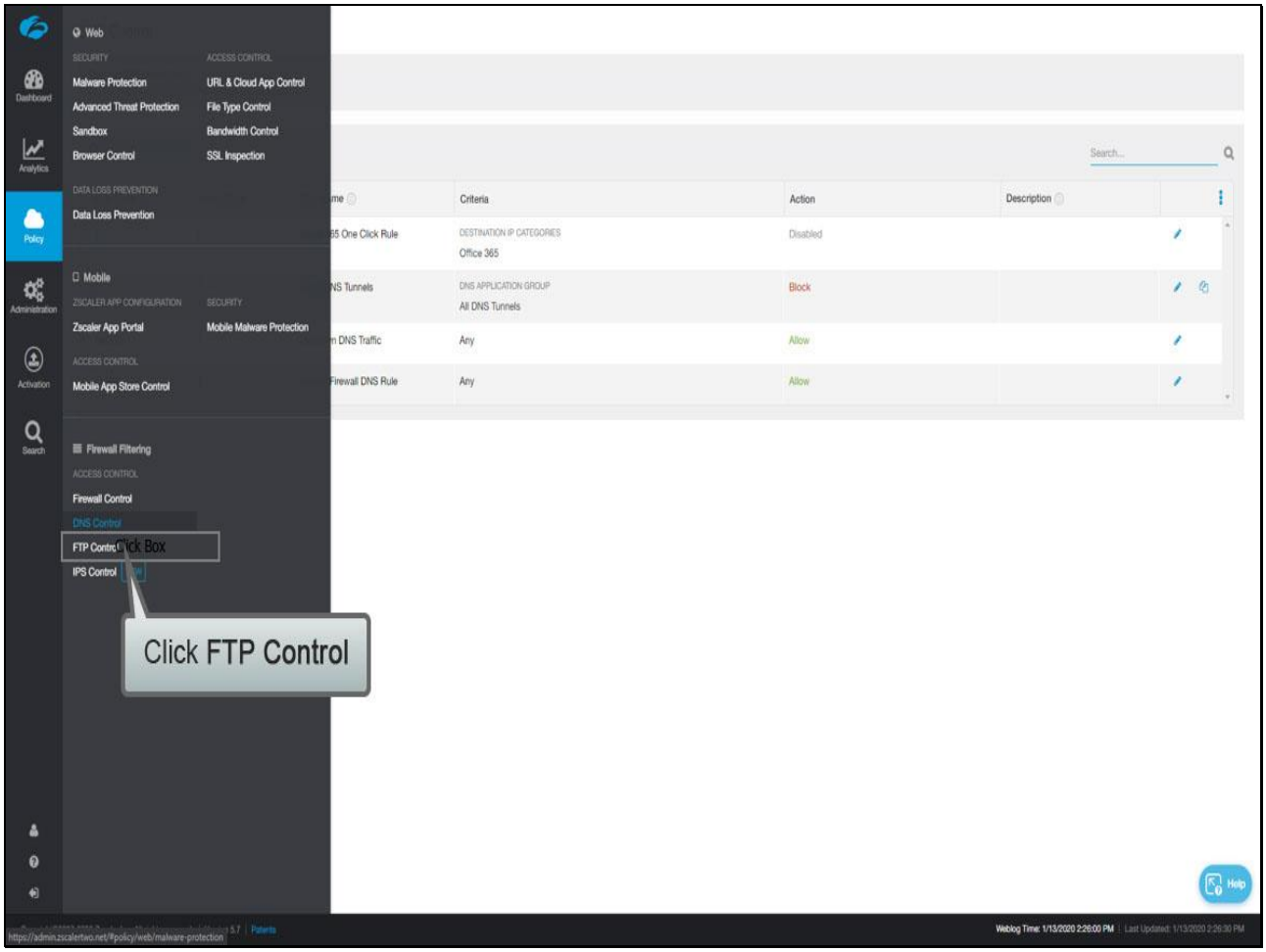
Slide 213 - Slide 213



Slide notes

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

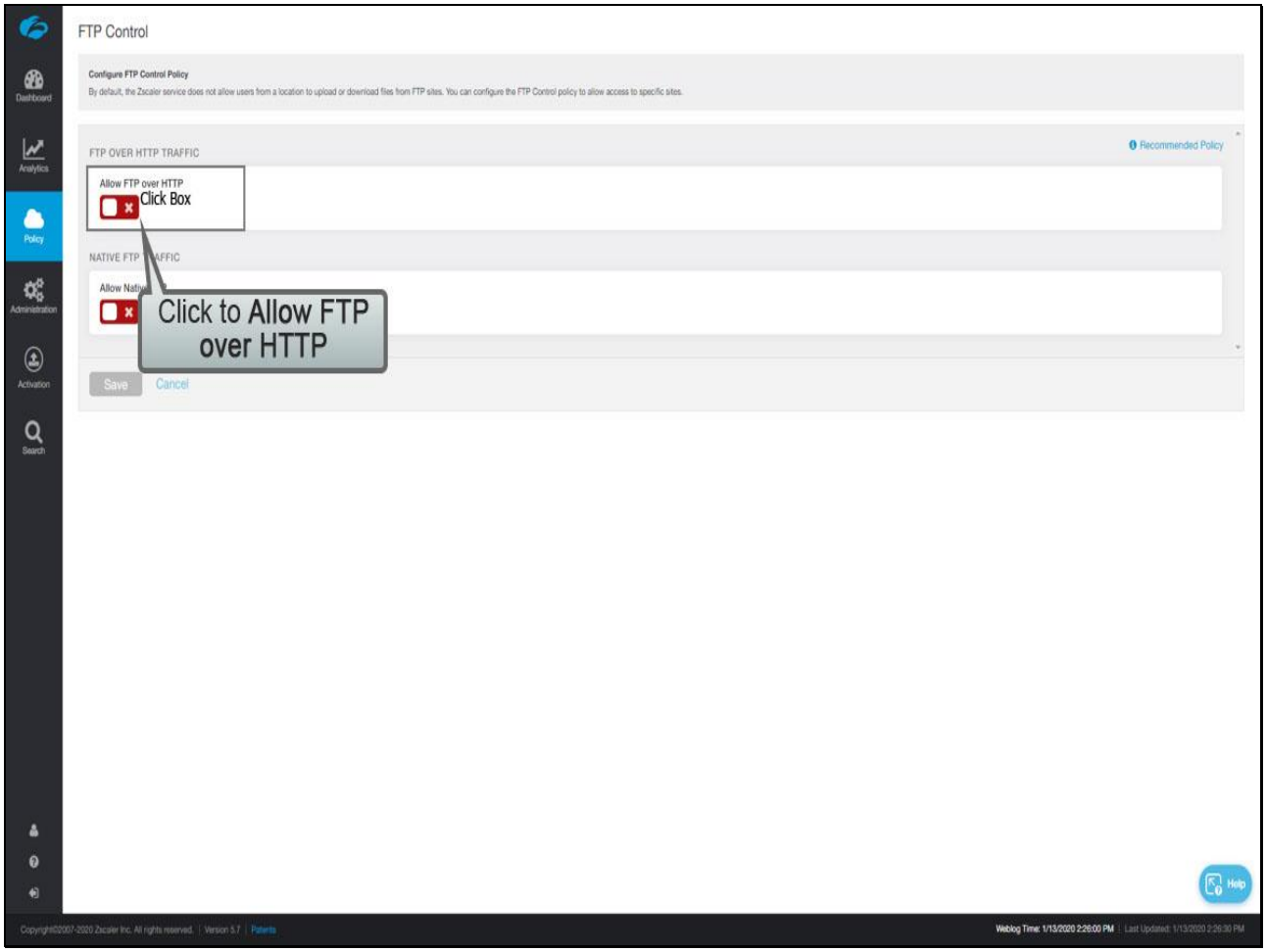
Slide 214 - Slide 214



Slide notes

Click on **FTP Control**.

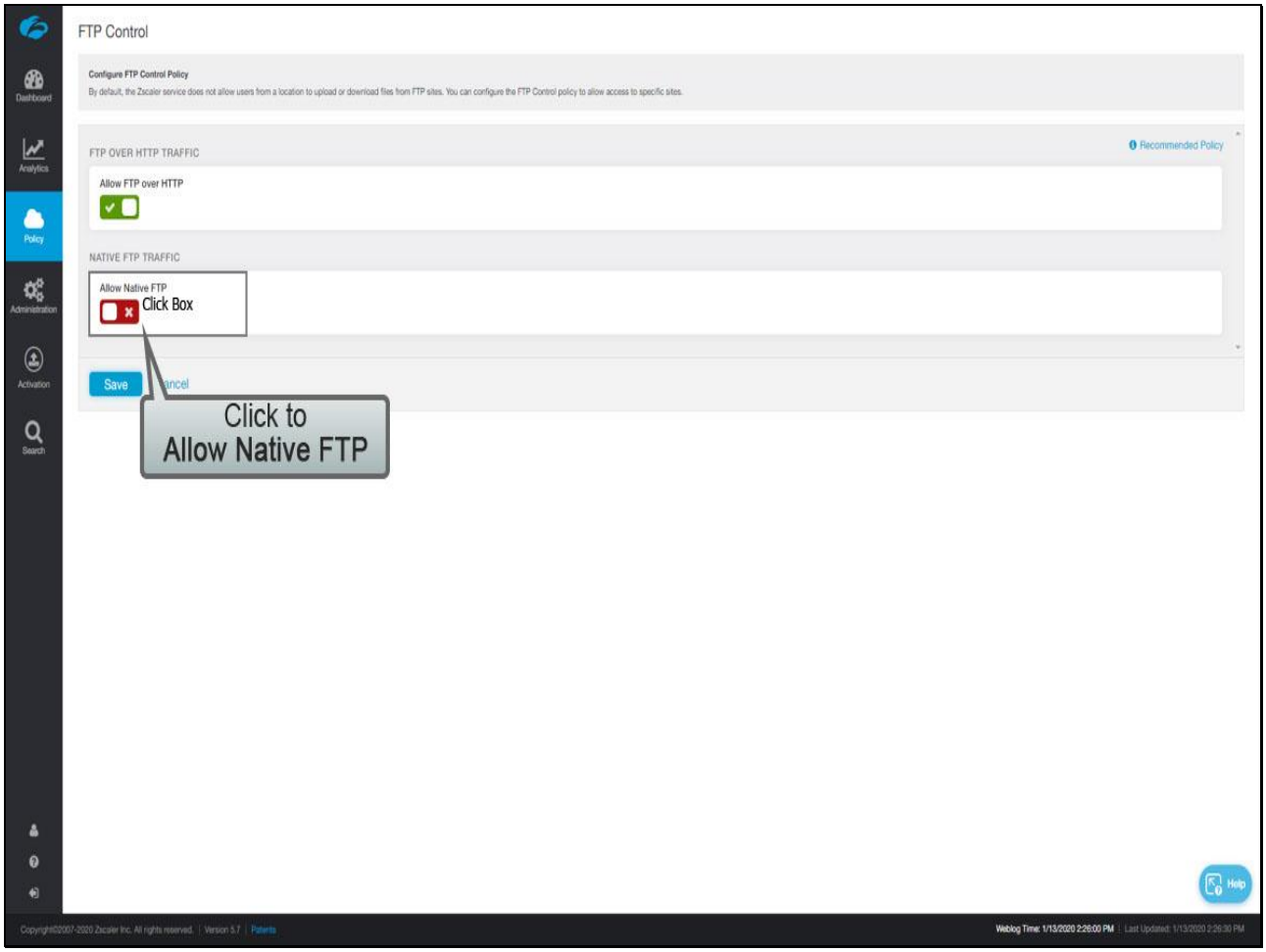
Slide 216 - Slide 216



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.

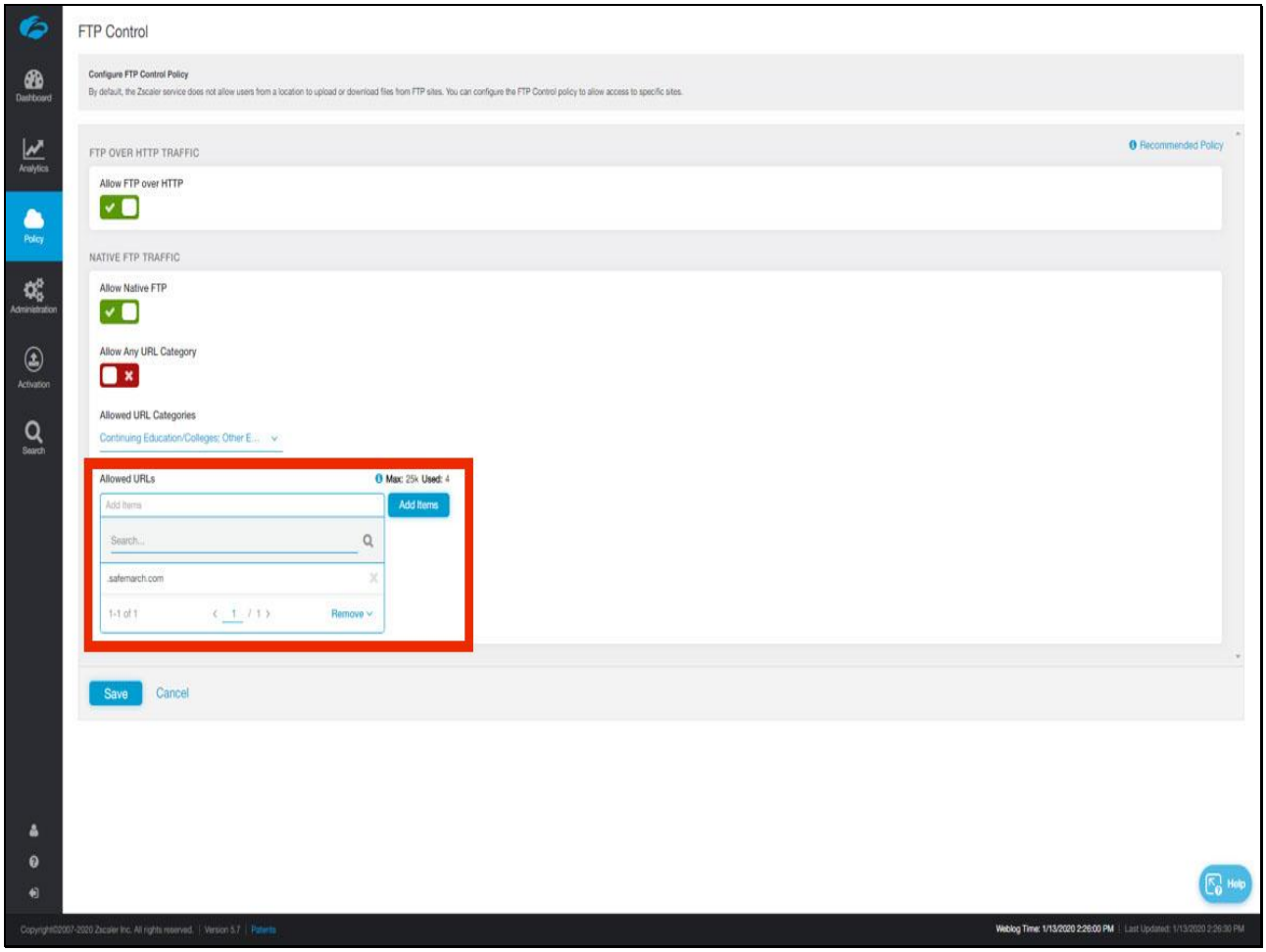
Slide 217 - Slide 217



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

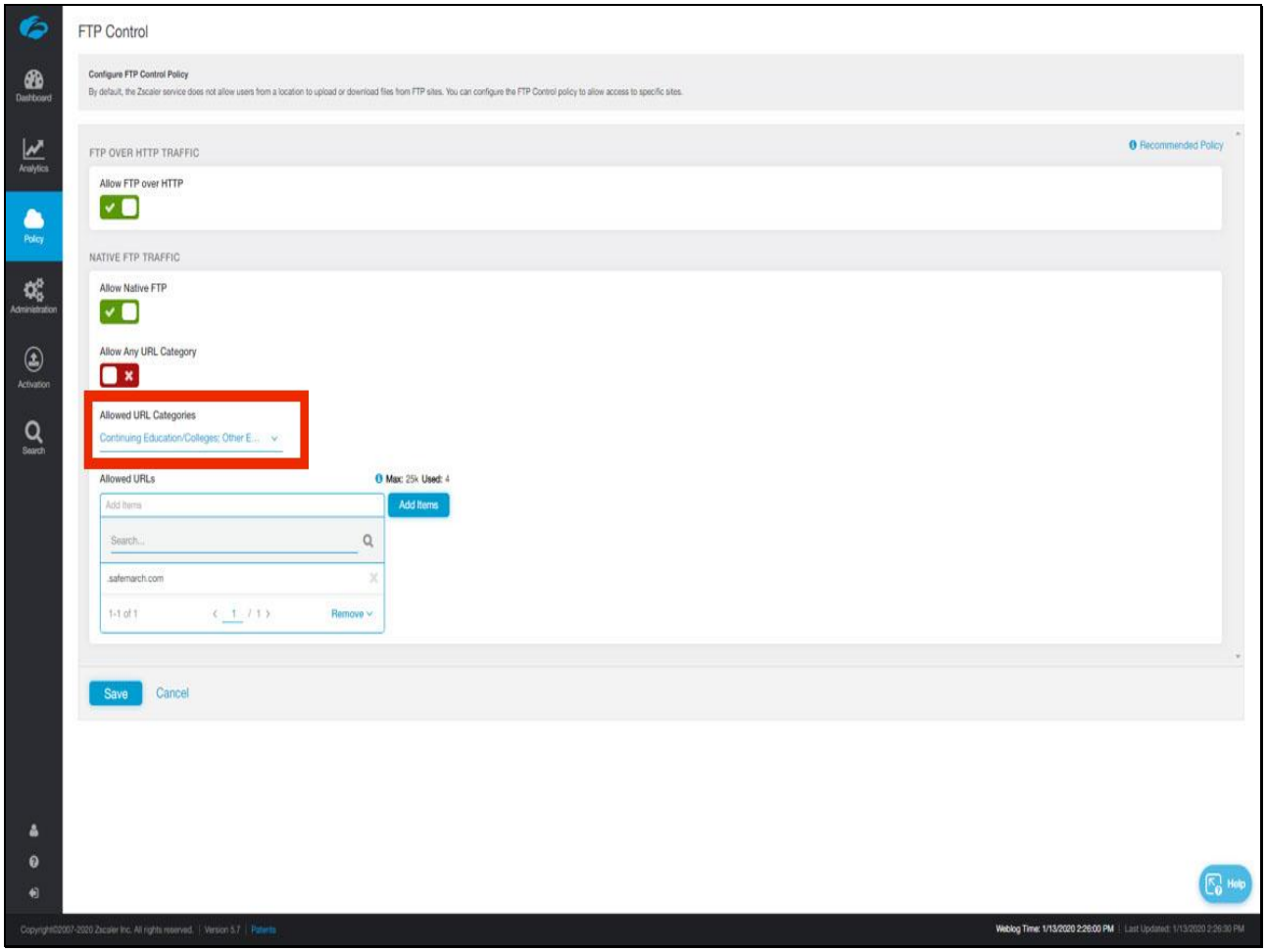


Slide notes

You may add specific URLs.

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

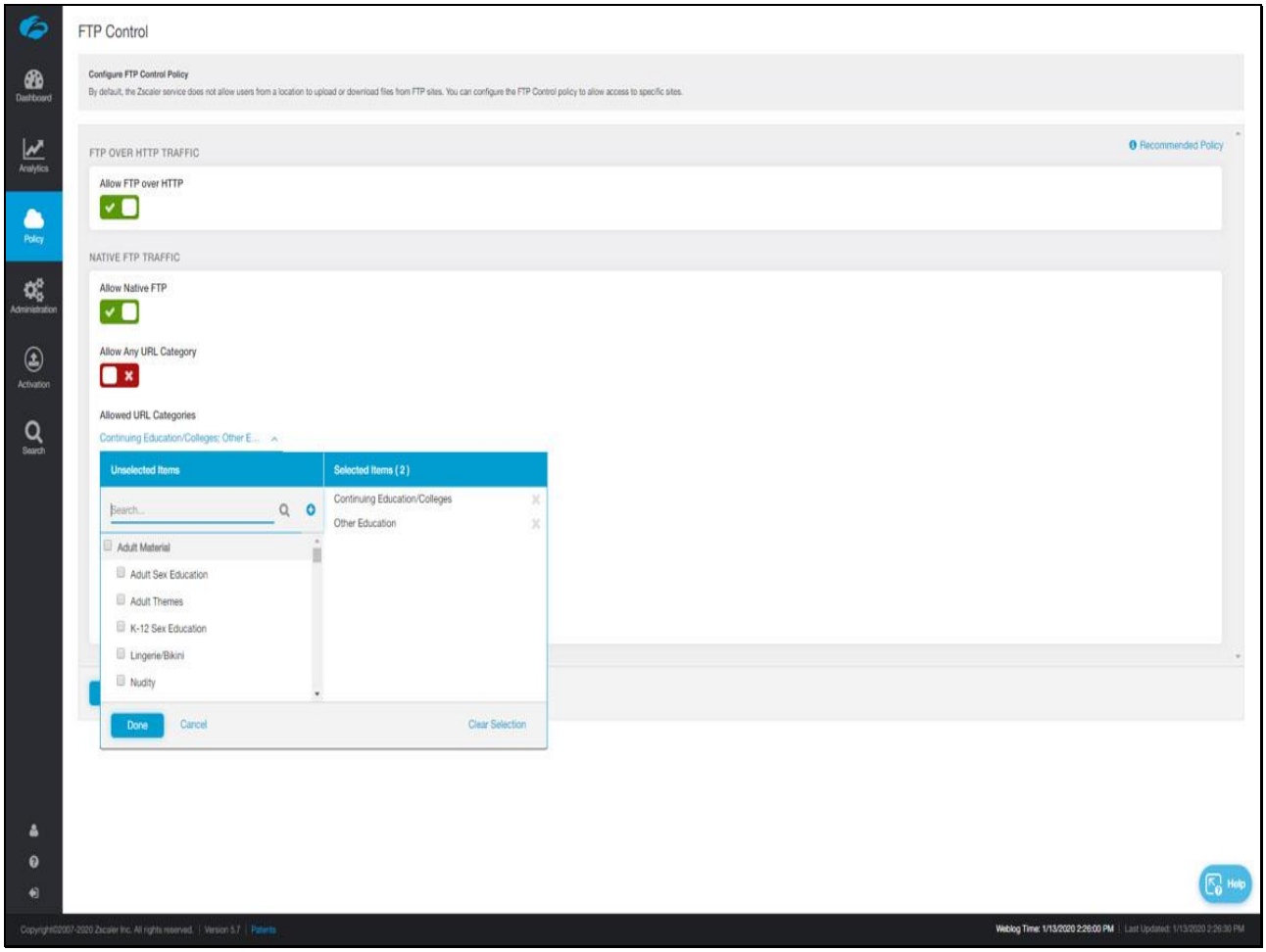
Slide 219 - Slide 219



Slide notes

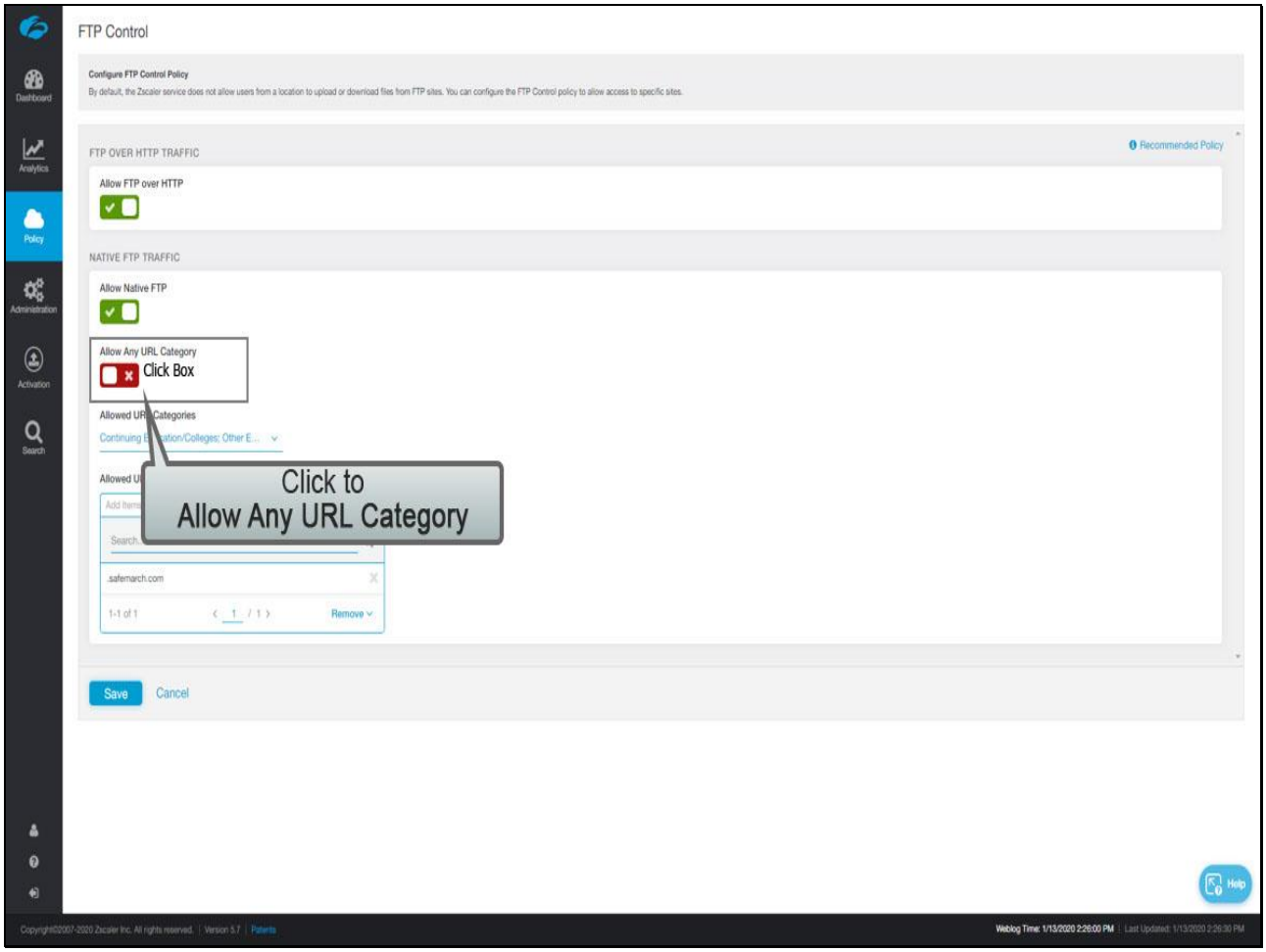
or entire URL Categories that should be allowed. Alternatively, you can permit native FTP to any URL Category

Slide 220 - Slide 220



Slide notes

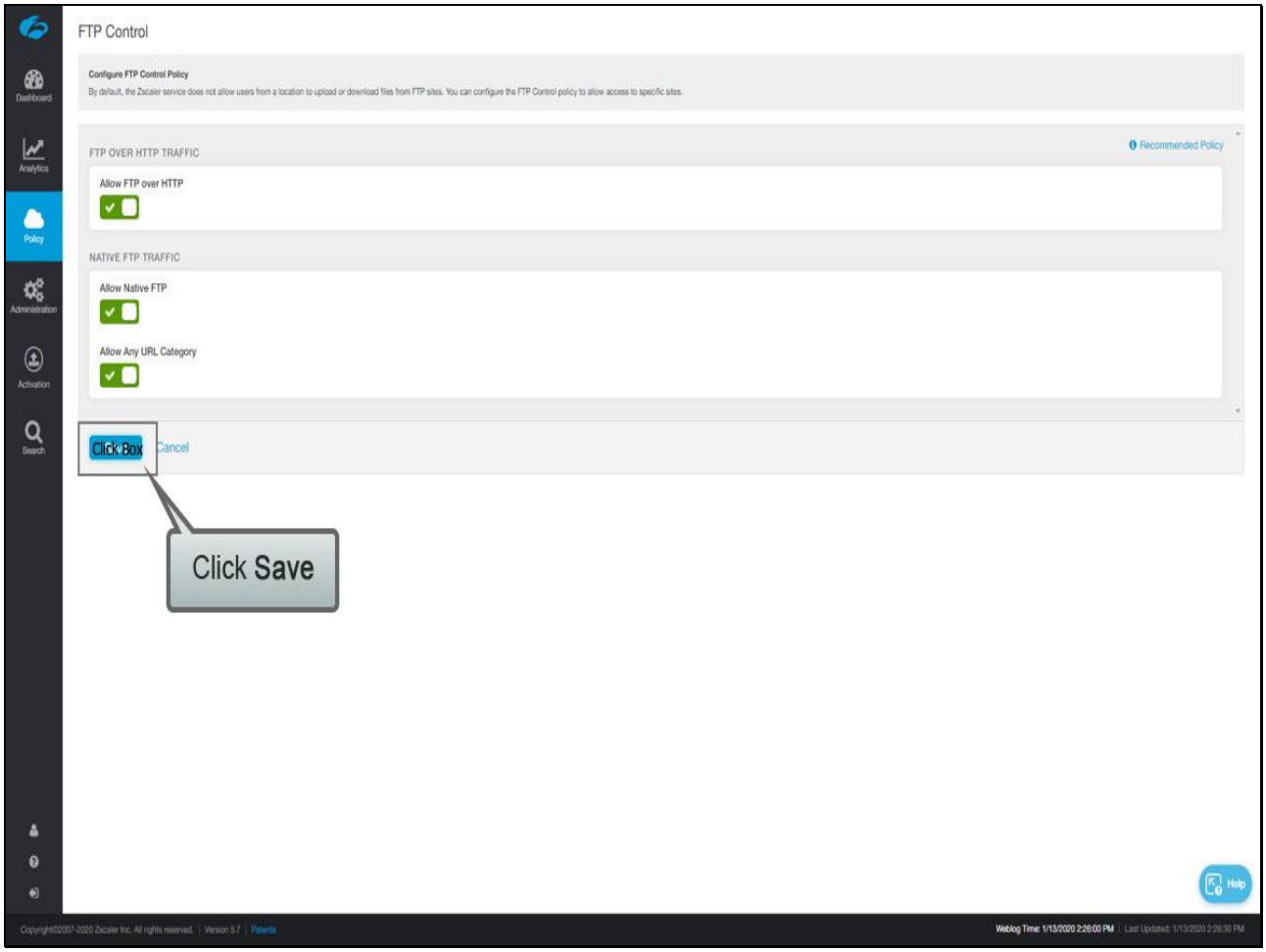
Slide 221 - Slide 221



Slide notes

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

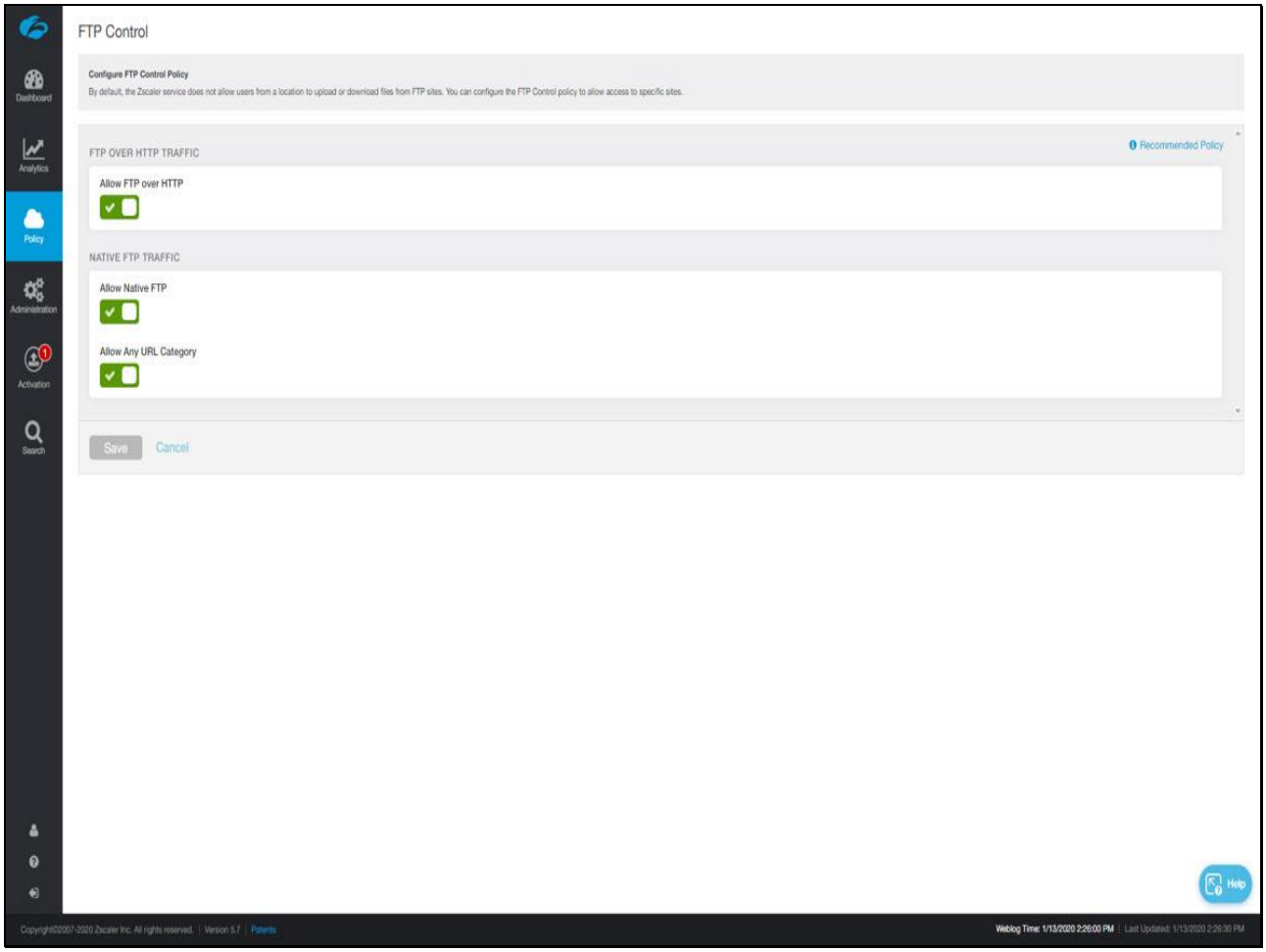
Slide 222 - Slide 222



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**.

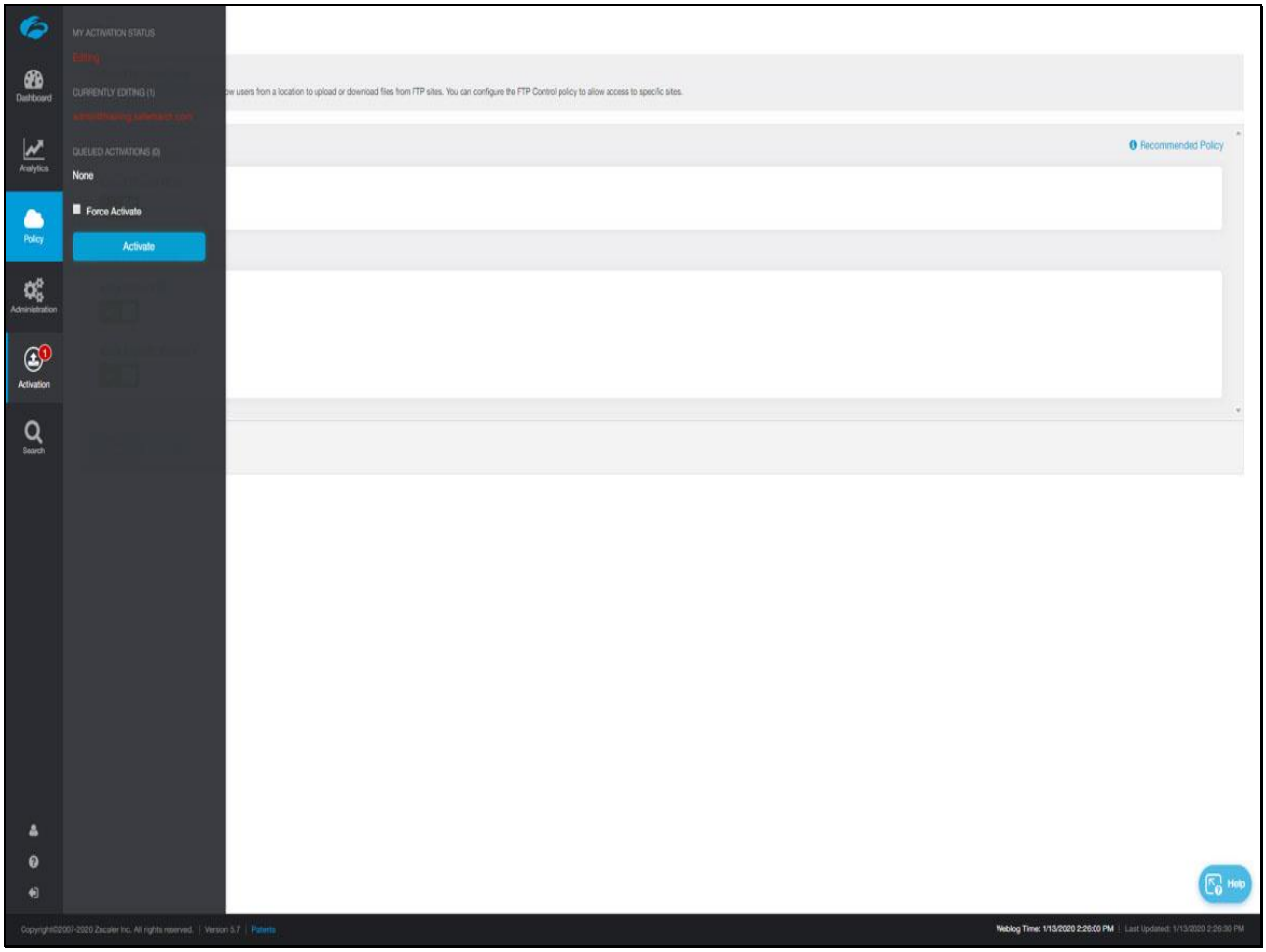
Slide 227 - Slide 227



Slide notes

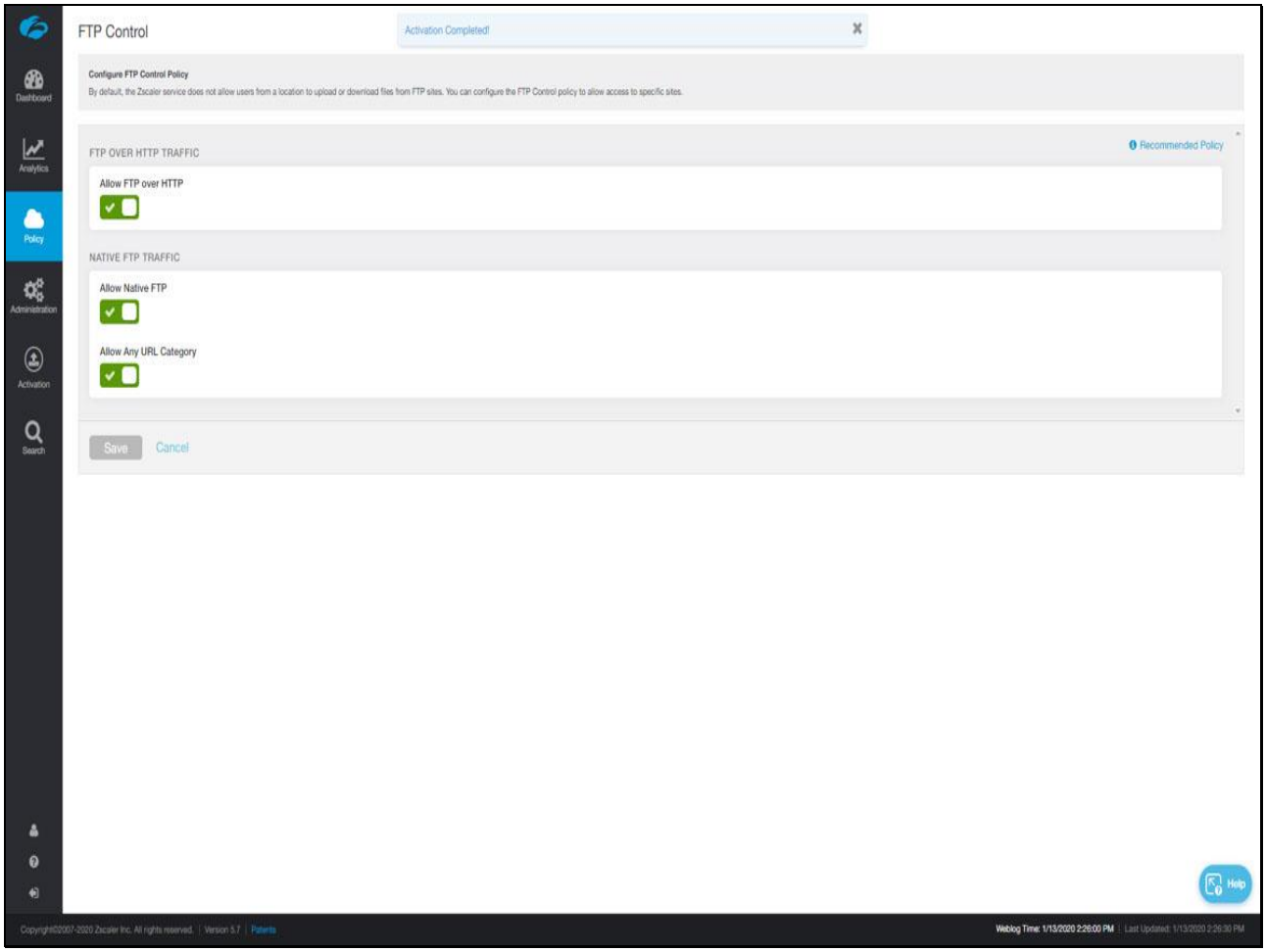
and **Activate** your changes.

Slide 228 - Slide 228



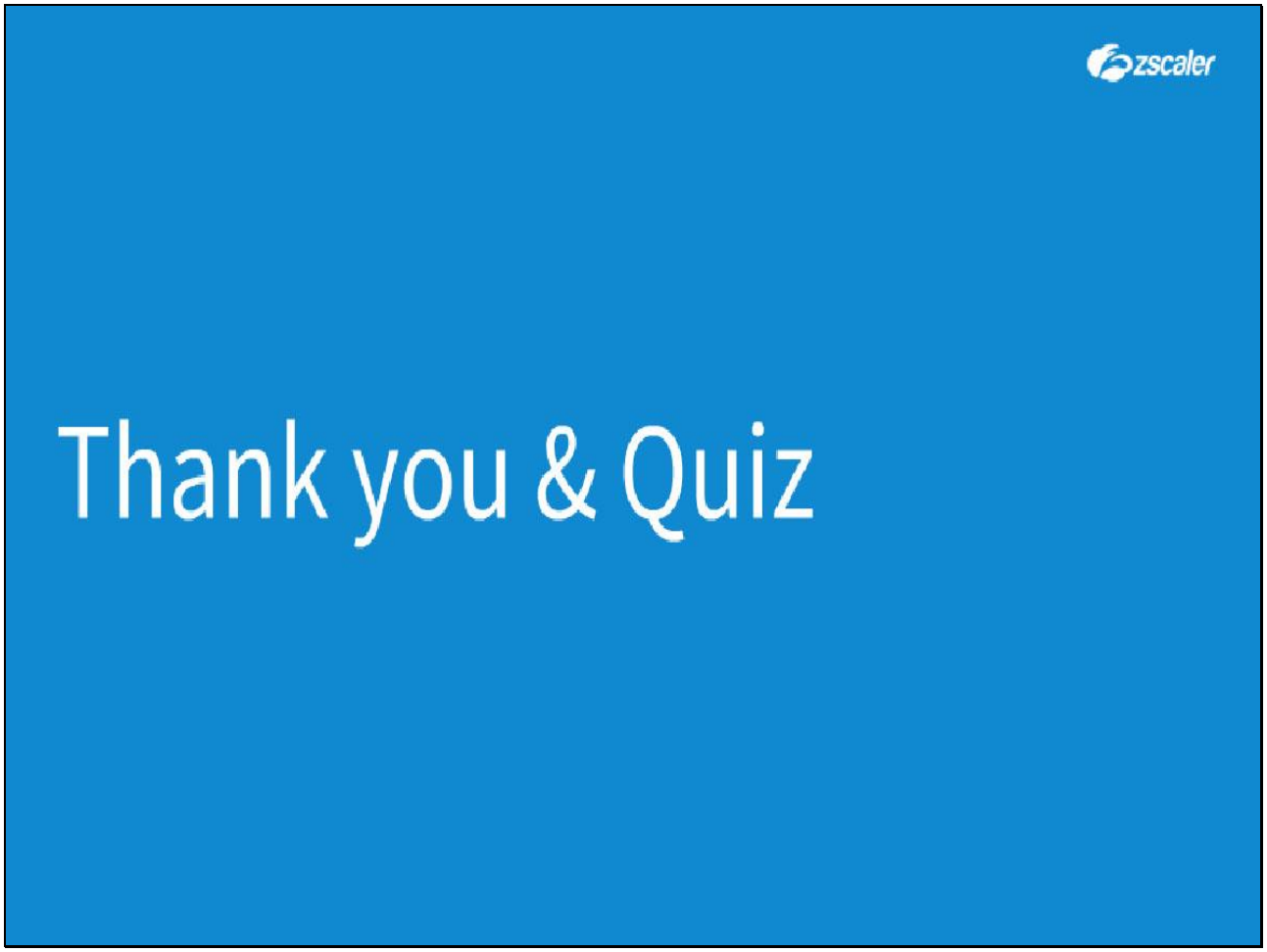
Slide notes

Slide 229 - Slide 229



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.