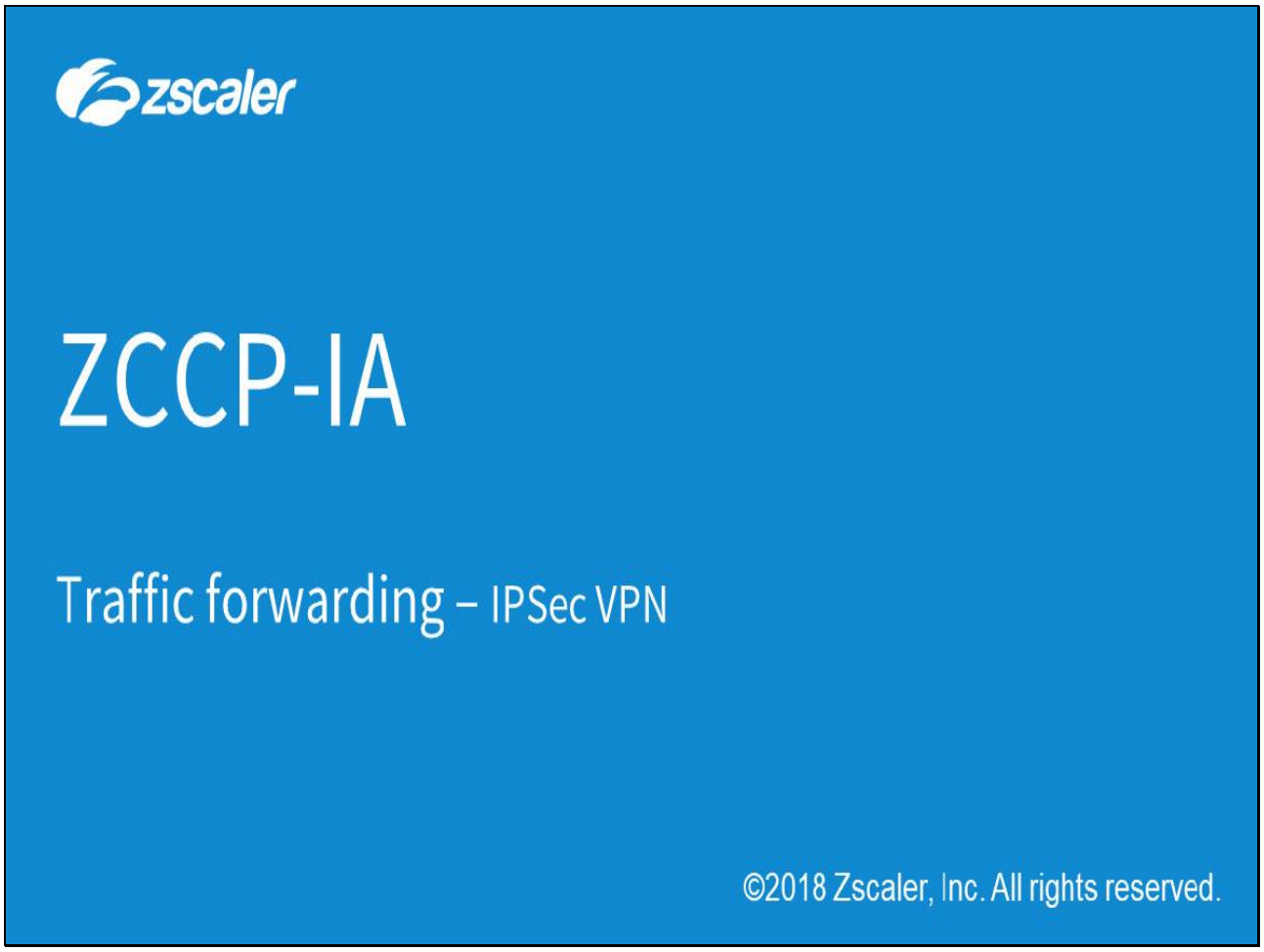
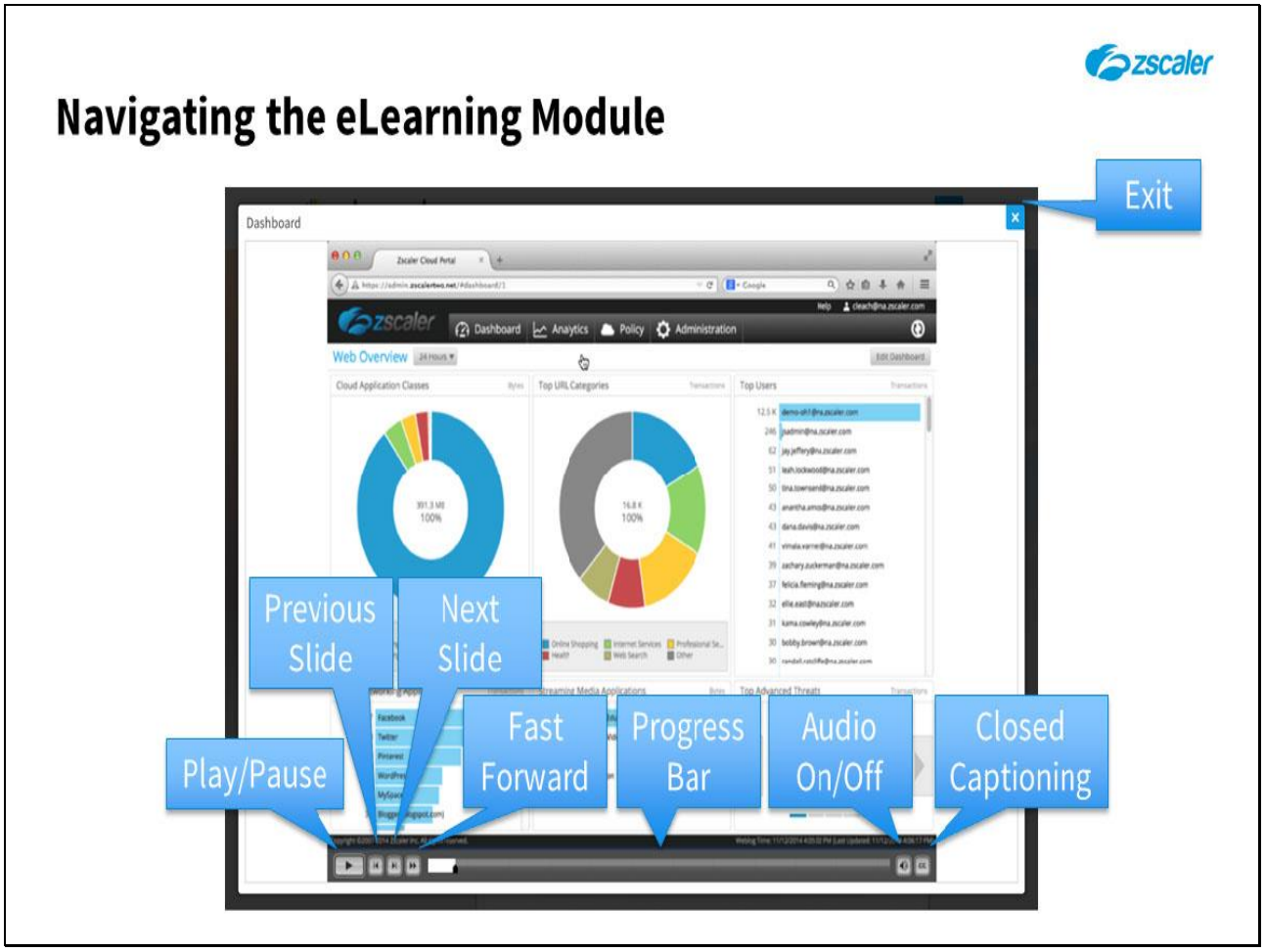
Slide 1 - ZCCP-IA



Slide notes

Thank you for viewing this eLearning module on Traffic forwarding to the Zscaler solution using IPSec / VPN.

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

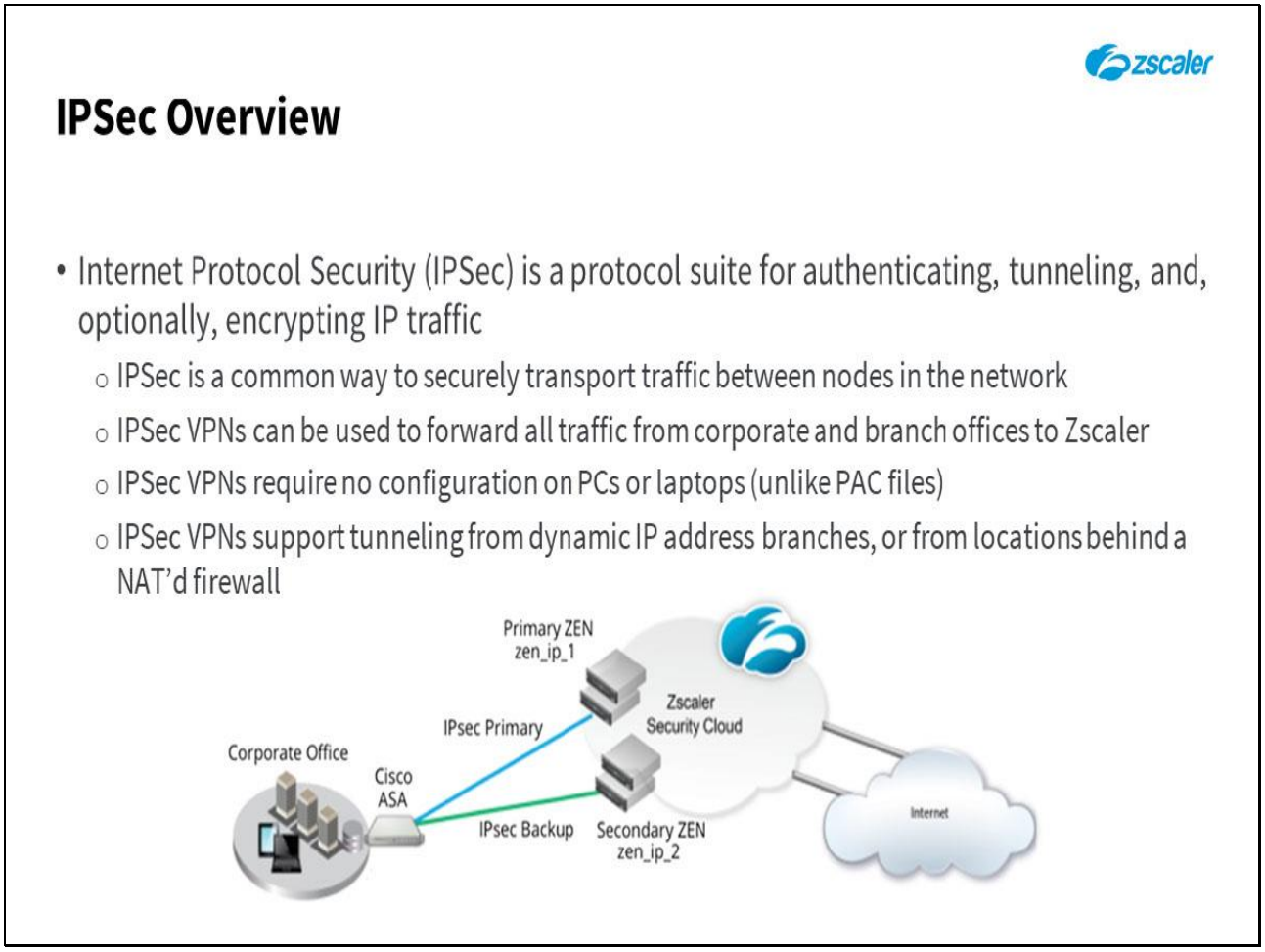
Slide notes

During this session we will examine and understand IPSec and how to configure a location to use IPSec to forward traffic to Zscaler.

Slide 4 - Understanding IPSec VPN

Slide notes

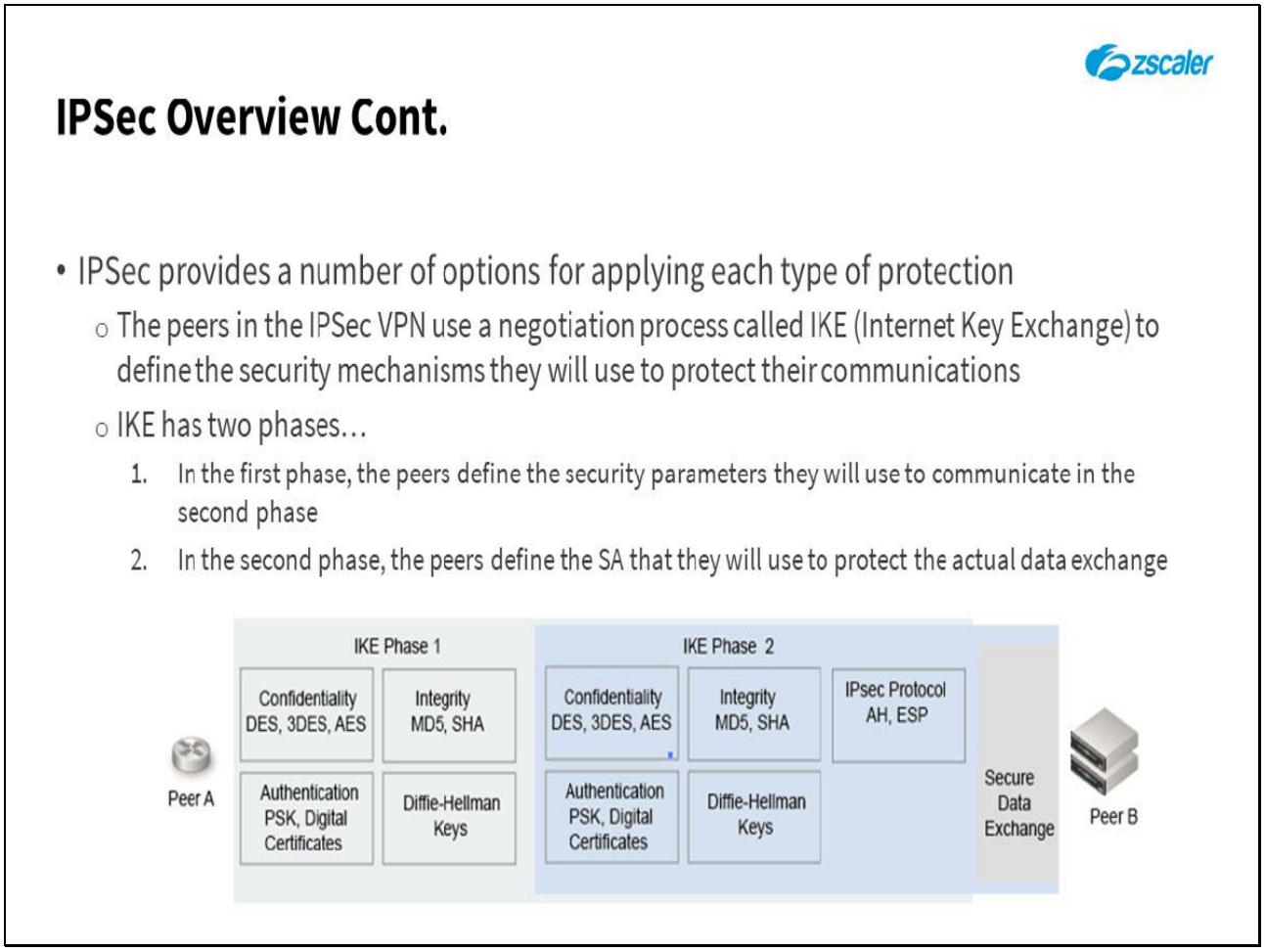
Slide 5 - IPSec Overview



Slide notes

Internet Protocol Security (IPsec) is a protocol suite for authenticating, tunneling, and, optionally, encrypting IP traffic. Using IPsec is a common way to securely transport traffic between one point to another point in the network. You can use IPsec VPNs to forward all traffic from your corporate network and branch offices to the Zscaler service. IPsec VPNs require no configuration on PCs or laptops, like PAC files. IPsec VPNs also support tunneling from dynamic IP address branches or from locations behind a NAT firewall.

Slide 6 - IPSec Overview Cont.



Slide notes

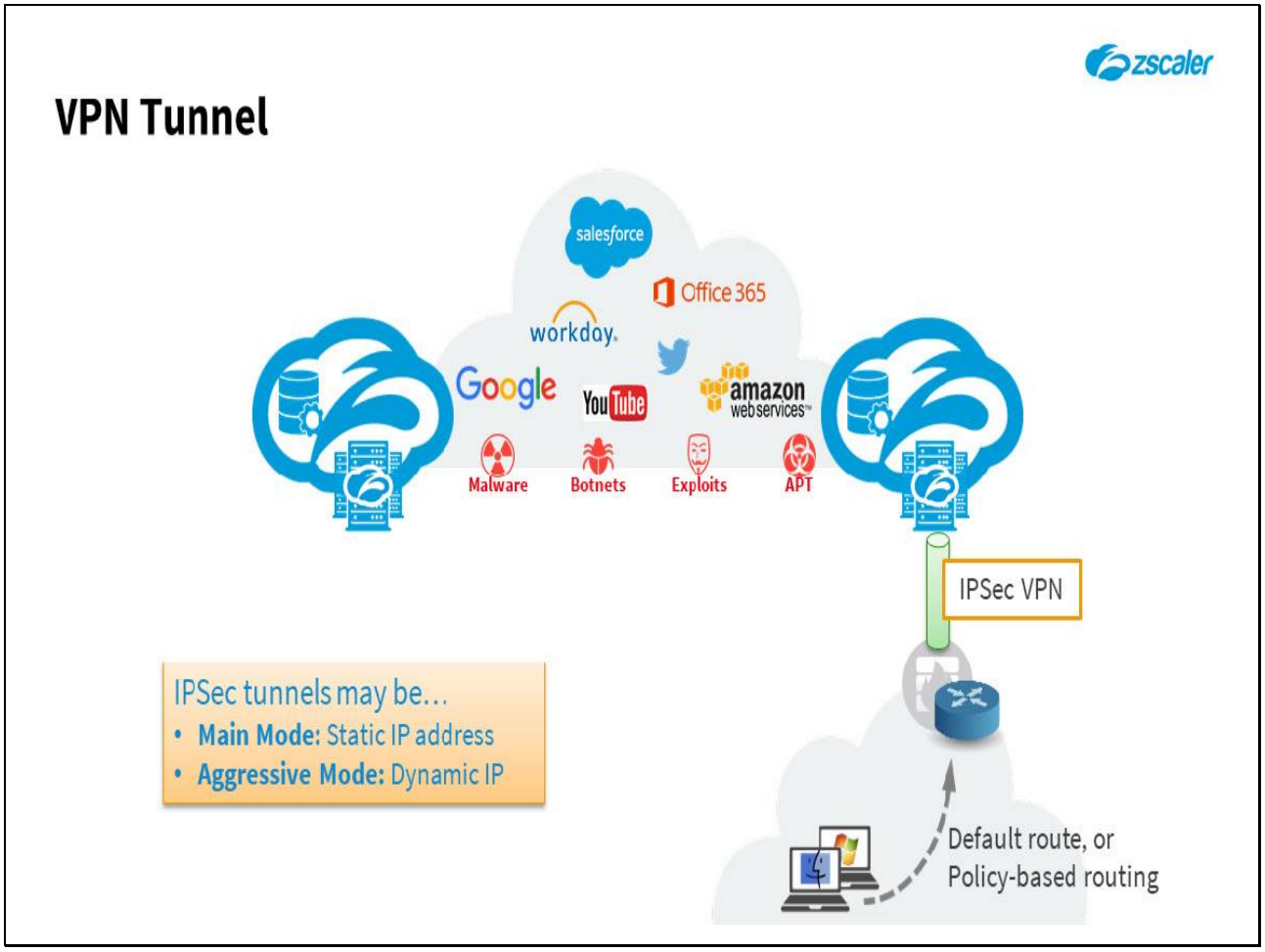
As shown in the following figure, IPSec provides a number of options for applying each type of protection. The peers in the IPsec VPN use a negotiation process called IKE (Internet Key Exchange) to define the security mechanisms they will use to protect their communications. IKE has two phases.

1. In the first phase, the peers define the security parameters they will use to communicate in the second phase. This collection of security parameters is called a security association (SA).

2. In the second phase, the peers define the SA that they will use to protect the actual data exchange.

For details on the inner workings of IPSec please review RFC 6071.

Slide 7 - VPN Tunnel

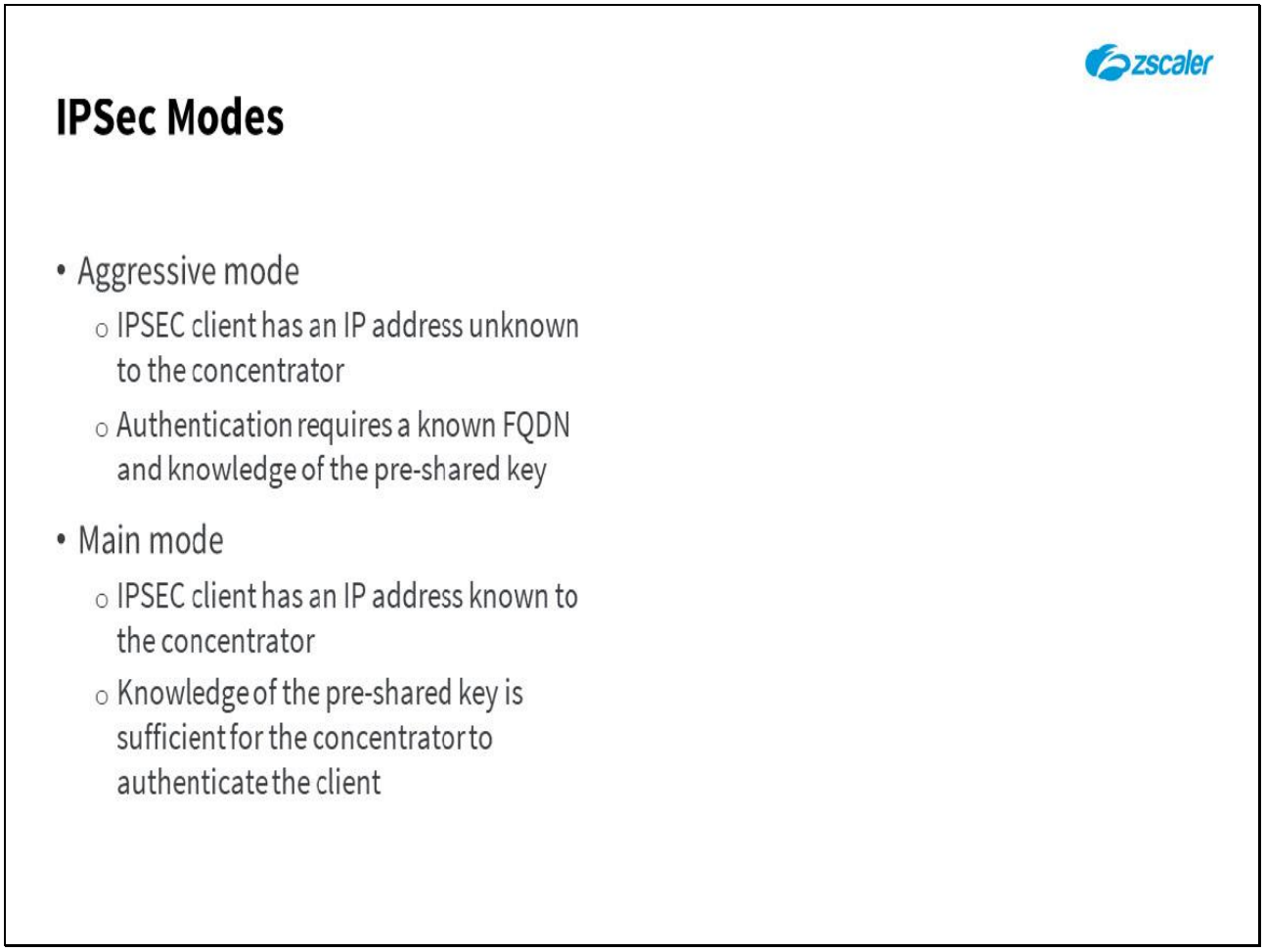


Slide notes

As shown in the diagram VPN tunnels can be created between the locations firewall or the border router. Redundant VPN tunnels can be created to protect against hardware or network failure. Once the tunnels are up, traffic must be redirected to Zscaler using the default route to send all traffic through the tunnel or Policy Based Routing to send only specific networks up the tunnel. This will be completely transparent to the user and no browser configuration settings are required.

When the Zscaler receives the traffic, it decides if this is traffic from a known location and if authentication is required. Configured policies are enforced and traffic is forwarded on to the Origin Server. Zscaler reports the traffic information and the metadata to the NanoLog Cluster for storage. Zscaler only deals with tokenized identifiers and is not aware of user or company names

Slide 8 - IPSec Modes

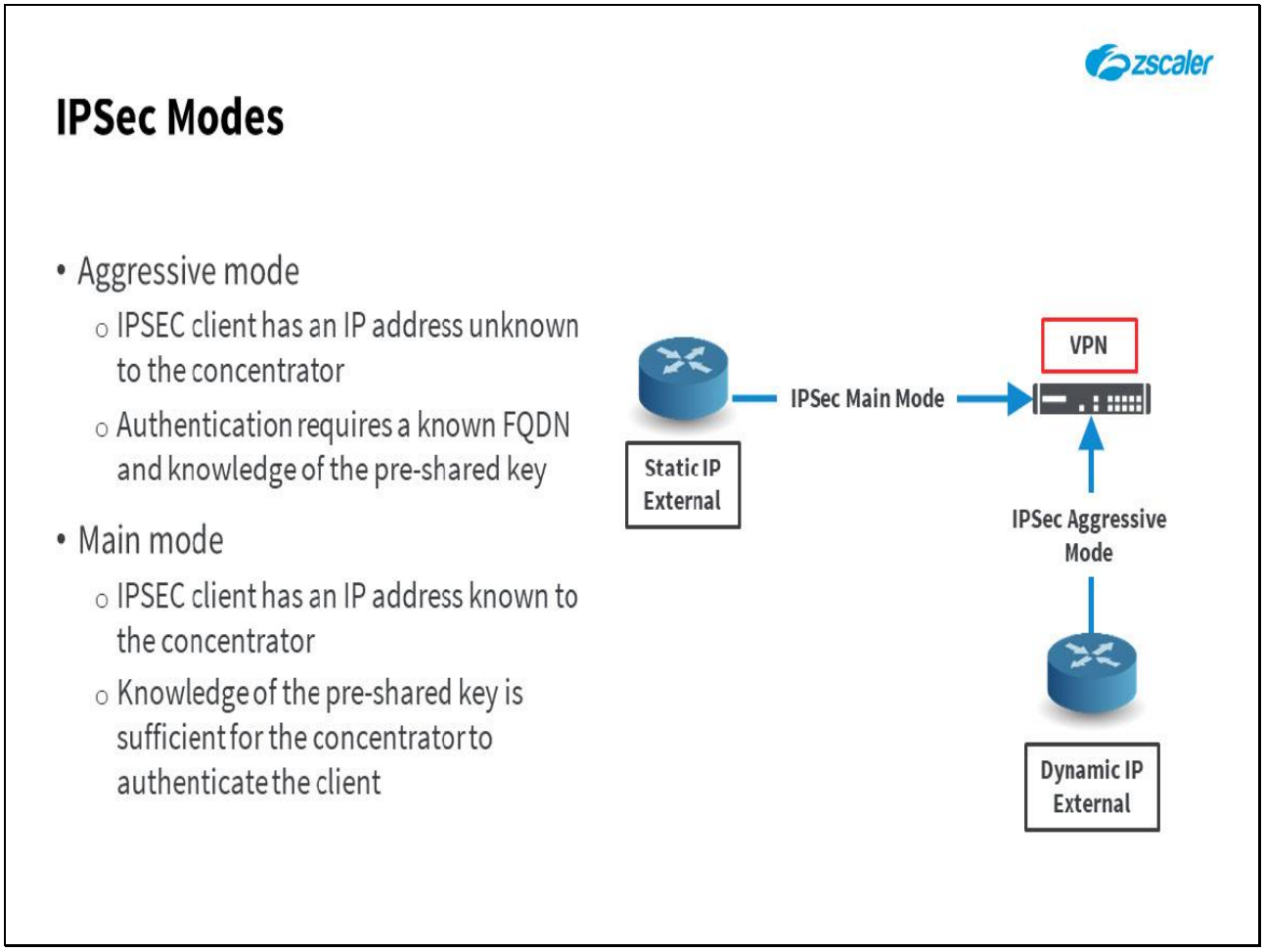


Slide notes

IPSec has two different modes that can be used depending on how the router or firewall is assigned its IP address. Aggressive mode is used when the IP address of the remote device is not known such as when an ISP provides the router an IP via DHCP. With Aggressive mode a Fully Qualified Domain name and pre-shared key must be configured.

Main mode is used when the IP address of the device is known and is a fixed public IP such as that which would be configured on your Border Router or Firewall. Because Main mode uses the IP address as part of the exchange for identification, it cannot be used in a configuration where the IP address of the peer may change.

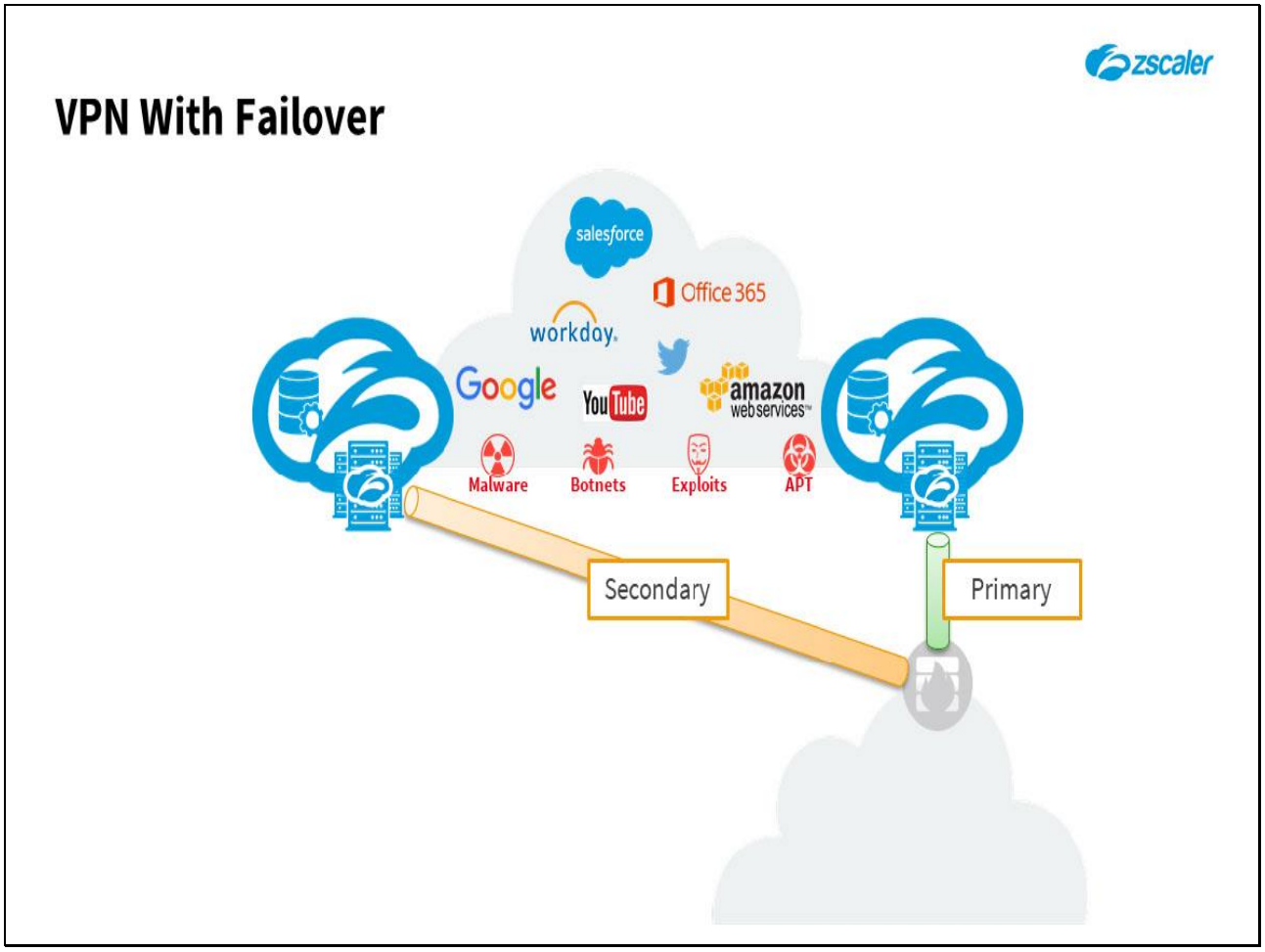
Slide 9 - IPSec Modes



Slide notes

As mentioned previously, IPSec can be configured in one of two ways, Main mode or Aggressive mode. Main mode would be used for a location with a fixed public IP such as what would be found at a large office and Aggressive mode may be used for a smaller site where the IP address for the router is assigned via DHCP by the ISP.

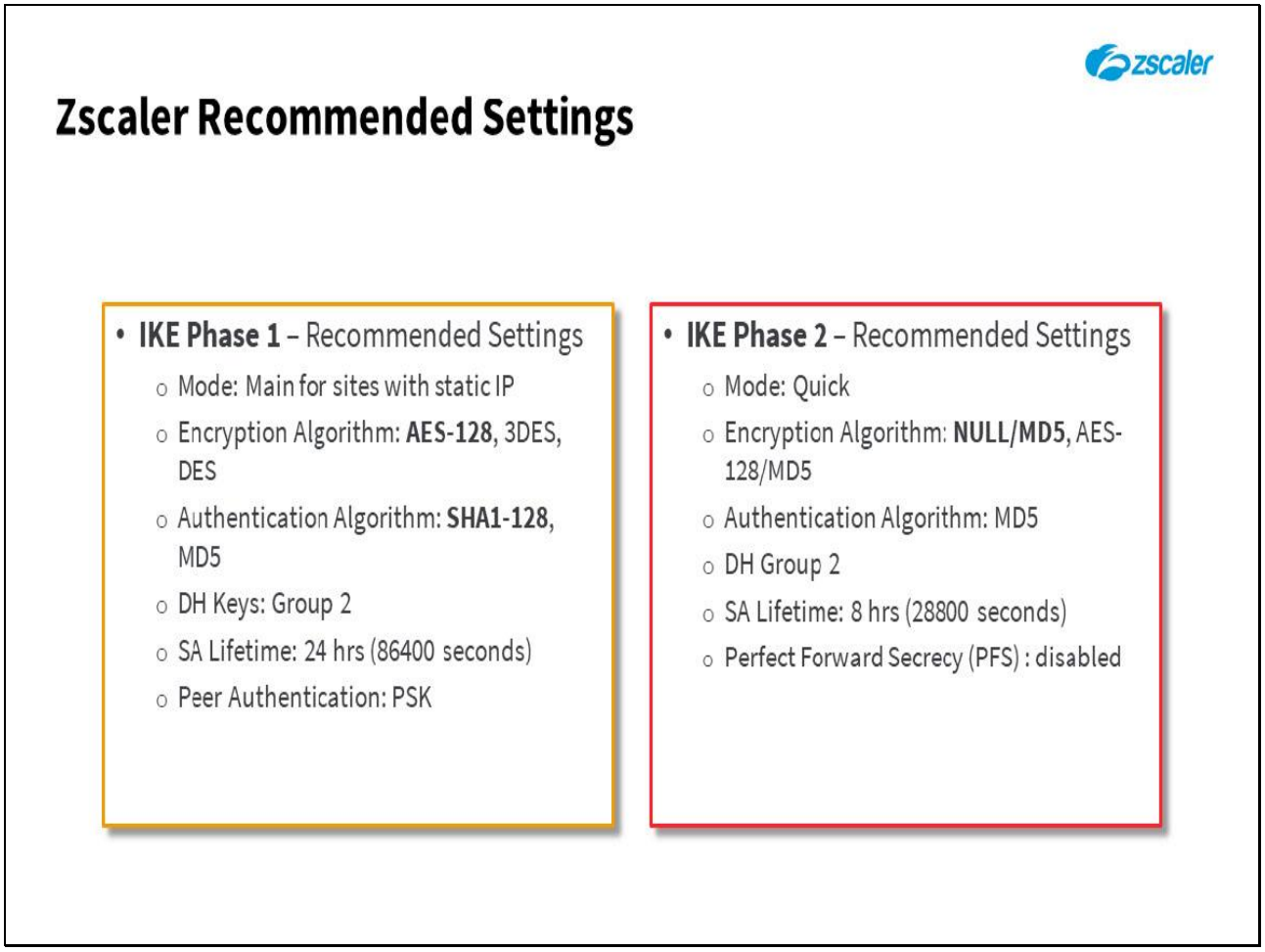
Slide 10 - VPN With Failover



Slide notes

In this example the IPSec tunnel is being built between the customer's router and both a primary and backup tunnel are configured for redundancy. Check with your router documentation to be sure that redundant tunnels is supported. As we discussed in the previous Traffic Forwarding module with GRE tunnels TAC provides the IP addressing information in response to a TAC case you submit requesting a location be defined.

Slide 11 - Zscaler Recommended Settings



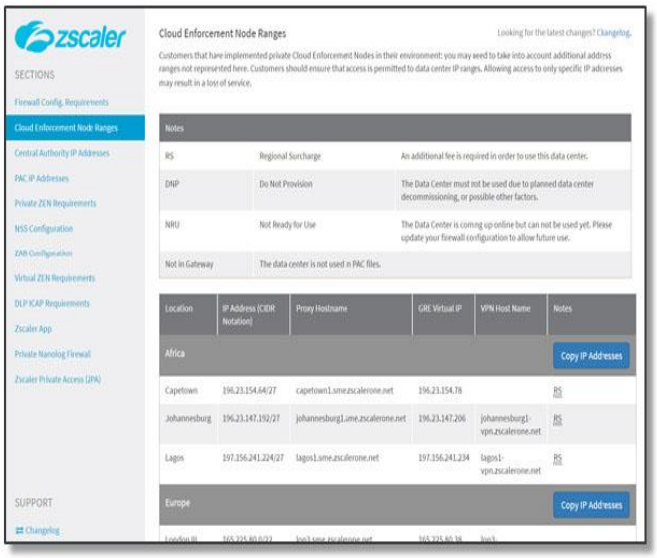
Slide notes

Here are the recommended settings when configuring IPSec VPNs. Please note that for Phase 2, the encryption algorithm should be set to ‘null’ with MD5 hash.

Slide 12 - Pre-requisite Tasks

Pre-requisite Tasks

- Contact TAC and provide the static public IP for the site
- Visit: https://ips.<your assigned Zscaler cloud>.net/cenr
  - Find the site closest to your location or the one with the least latency (TAC may suggest which site)
  - Ping the FQDN of the Zscaler VPN node you selected to obtain the IP address
  - Use the IP address during the site router configuration



Slide notes

There are a few tasks you will need to complete before configuring your site. First, contact TAC, create a TAC case and provide the static public IP address for the site. TAC will then create the location, so it will appear in the Admin Portal. Next, visit **https://ips.<your assigned Zscaler cloud>.net/cenr.html**. Once on this webpage find the site closest to your location or the one with the best performance based on latency. TAC may suggest which site to connect to as well.

PING the fully qualified domain name of the Zscaler VPN node you selected to obtain its' IP address. You will use the IP address during the configuration of the site's router.

Slide 13 - VPN (Aggressive Mode) – Cisco ASA Configuration 9.0

VPN (Aggressive Mode) – Cisco ASA Configuration 9.0

Task	Command
Internet Key Exchange (IKE) configuration	crypto ikev1 enable <outside_vlan_name> crypto ikev1 policy 1 encryption 3des authentication pre-share hash md5 group 2 lifetime 86400 exit
Link the VPN tunnel with the IKE configuration	group-policy <group name string> internal group-policy <group name string> attributes vpn-tunnel-protocol ikev1 exit
Create tunnel group and set the pre-shared key	tunnel-group <Zscaler VPN IP> type ipsec-l2l tunnel-group <Zscaler VPN IP> general-attributes default-group-policy <group name string> exit tunnel-group <Zscaler VPN IP> ipsec-attributes ikev1 pre-shared-key <PSK string> exit
Configuring the ACL	object network <IP_object_name> subnet <subnet> <subnet_mask> access-list <ACL name> extended permit ip object <IP object name> any
IPSec configuration	crypto ipsec ikev1 transform-set <name> esp-null esp-md5-hmac crypto ipsec security-association lifetime seconds 28800 crypto map <map_name> 65000 match address <ACL_name> crypto map <map_name> 65000 set connection-type originate-only crypto map <map_name> 65000 set peer <Zscaler_VPN_IP> crypto map <map_name> 65000 set ikev1 phase1-mode aggressive crypto map <map_name> 65000 set ikev1 transform-set <ipsec_transform_name> crypto map <map_name> interface <outside_vlan_name>

Slide notes

Here is a sample configuration of a Cisco ASA running version 9.0. Please note, syntax may vary depending on the version of software on your ASA. For further configuration information see the Cisco ASA Configuration Guide.

- Begin configuring the VPN tunnel in the ASA by first configuring IKE.
- Next Link the VPN tunnel with the IKE configuration
- Create the tunnel group and set the pre-shared key.
- Configure the ACL to forward traffic into the tunnel
- And last, the IPSec configuration

Take a moment to review the configuration.

Slide 14 - Cisco ASA Configuration – Completed With Policy Names

Cisco ASA Configuration – Completed With Policy Names

Task	Command

Internet Key Exchange (IKE) configuration	`crypto ikev1 enable Outside`
	`crypto ikev1 policy 1`
	`encryption 3des`
	`authentication pre-share`
	`hash md5`
	`group 2`
	`lifetime 86400`
	`exit`

Link the VPN tunnel with the IKE configuration	`group-policy Zscaler_GRP internal`
	`group-policy Zscaler_GRP attributes`
	`vpn-tunnel-protocol ikev1`
	`exit`

Create tunnel group and set the pre-shared key	`tunnel-group 104.129.192.35 type ipsec-l2l`
	`tunnel-group 104.129.192.35 general-attributes`
	`default-group-policy Zscaler_GRP`
	`exit`
	`tunnel-group 104.129.192.35 ipsec-attributes`
	`ikev1 pre-shared-key Admin-123!`
	`exit`

Configuring the ACL	`object network flow_traffic`
	`subnet 10.84.0.0 255.255.255.0`
	`access-list Zscaler_map extended permit ip object flow_traffic any`

IPSec configuration	`crypto ipsec ikev1 transform-set transform_zen esp-null esp-md5-hmac`
	`crypto ipsec security-association lifetime seconds 28800`
	`crypto map zen_vpn_map 65000 match address Zscaler_map`
	`crypto map zen_vpn_map 65000 set connection-type originate-only`
	`crypto map zen_vpn_map 65000 set peer 104.129.192.35`
	`crypto map zen_vpn_map 65000 set ikev1 phase1-mode aggressive`
	`crypto map zen_vpn_map 65000 set ikev1 transform-set transform_zen`
	`crypto map zen_vpn_map interface Outside`

Slide notes

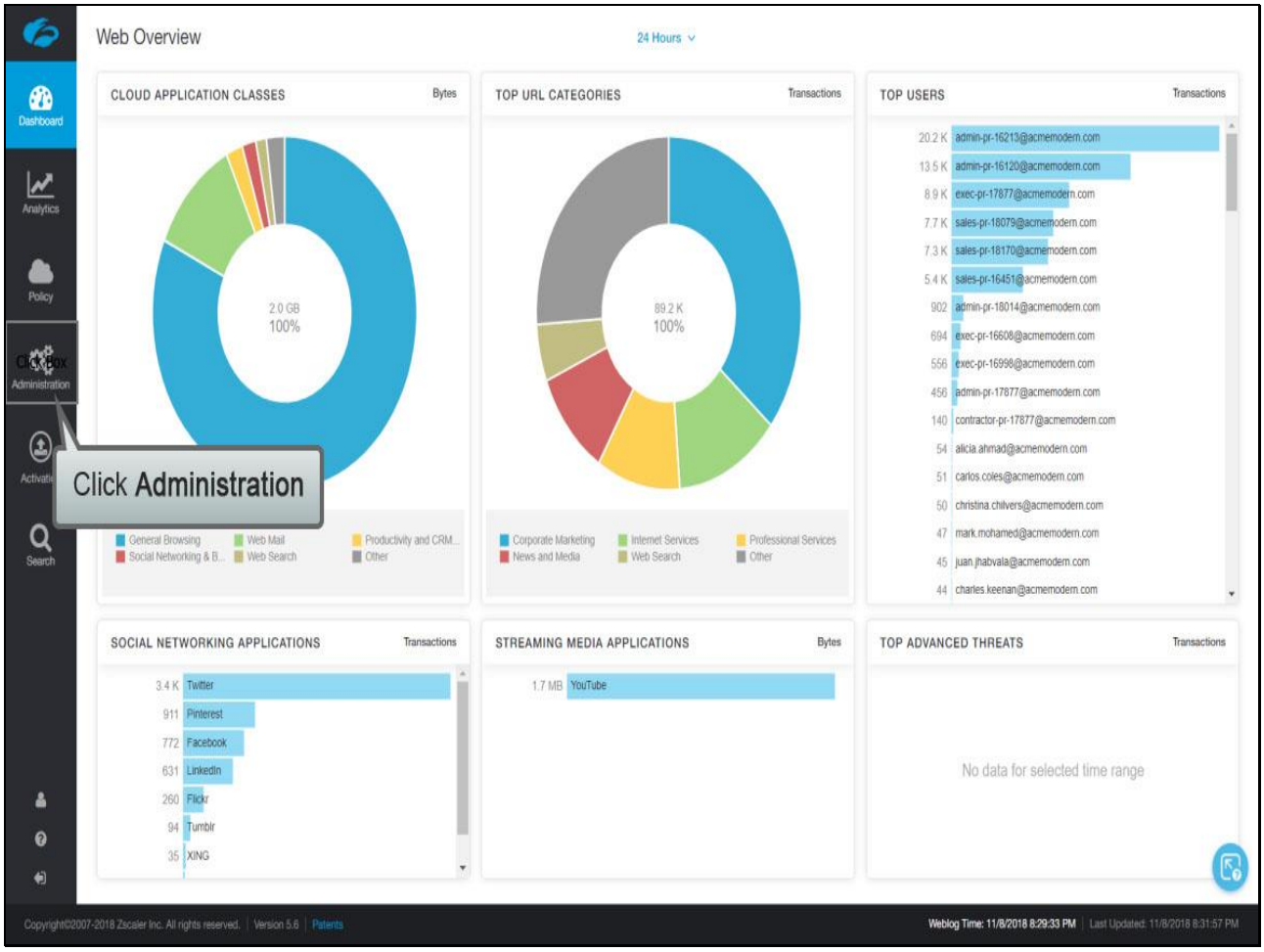
Here is the same configuration but with the policy names completed. Take a moment to review the config to see how the policies are nested or linked.

Slide 15 - Connecting to Zscaler: Interactive Demo

Slide notes

During this demonstration you will see the steps needed to configure a single VPN tunnel from a Cisco ASA to the Zscaler solution.

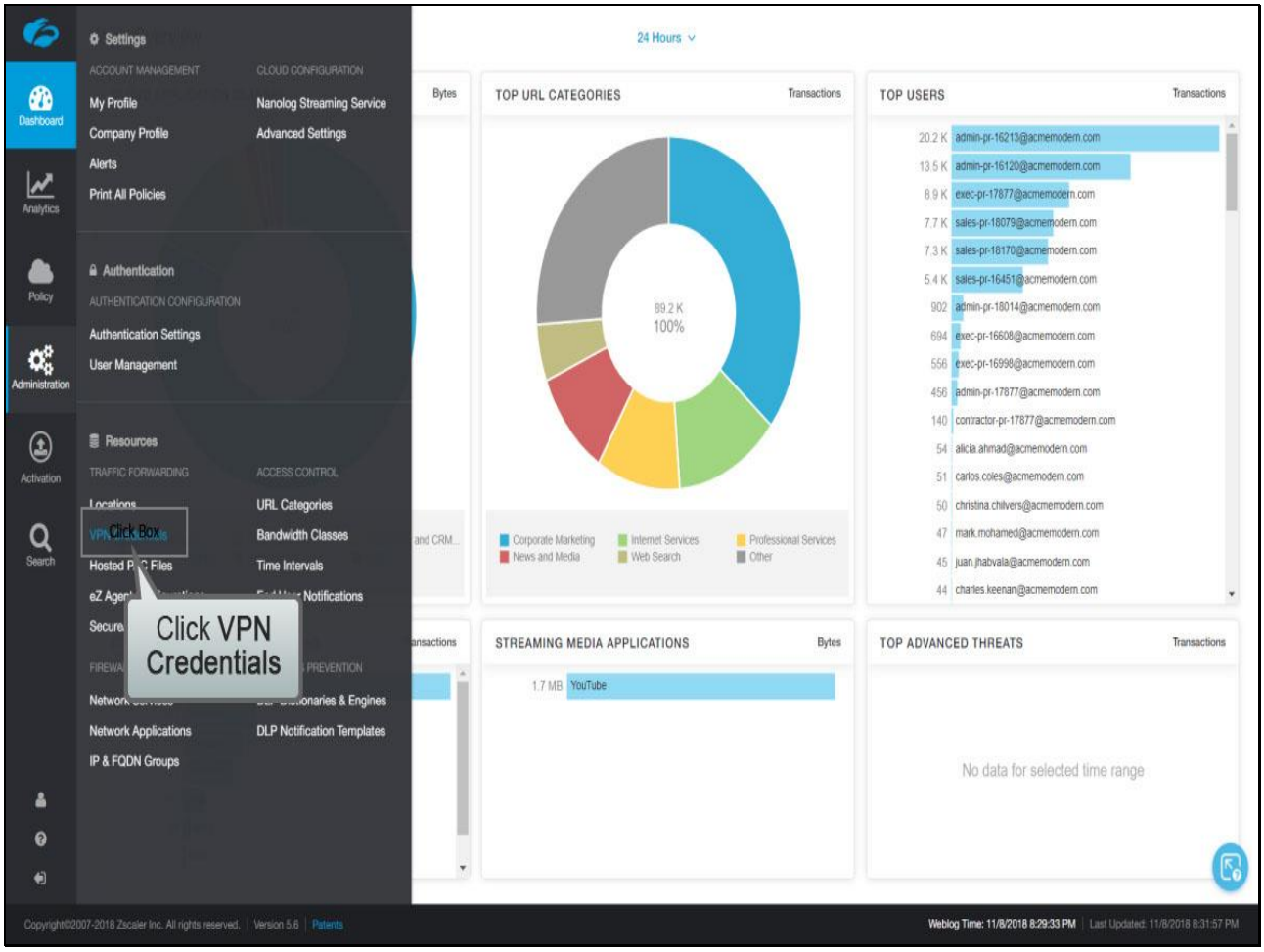
Slide 16 - Slide 16



Slide notes

Begin in the Admin Portal under **Administration**.

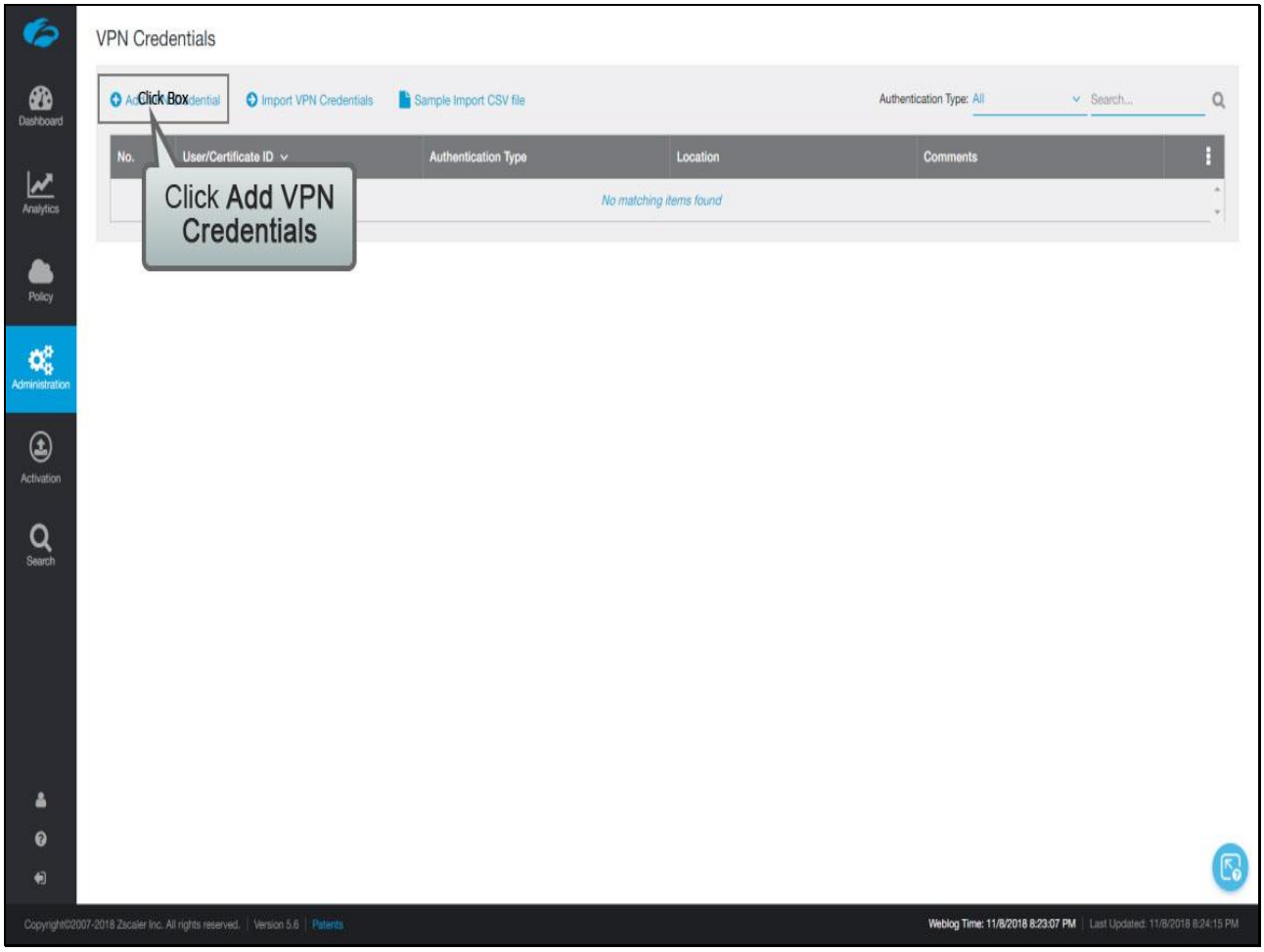
Slide 17 - Slide 17



Slide notes

Then **VPN Credentials**.

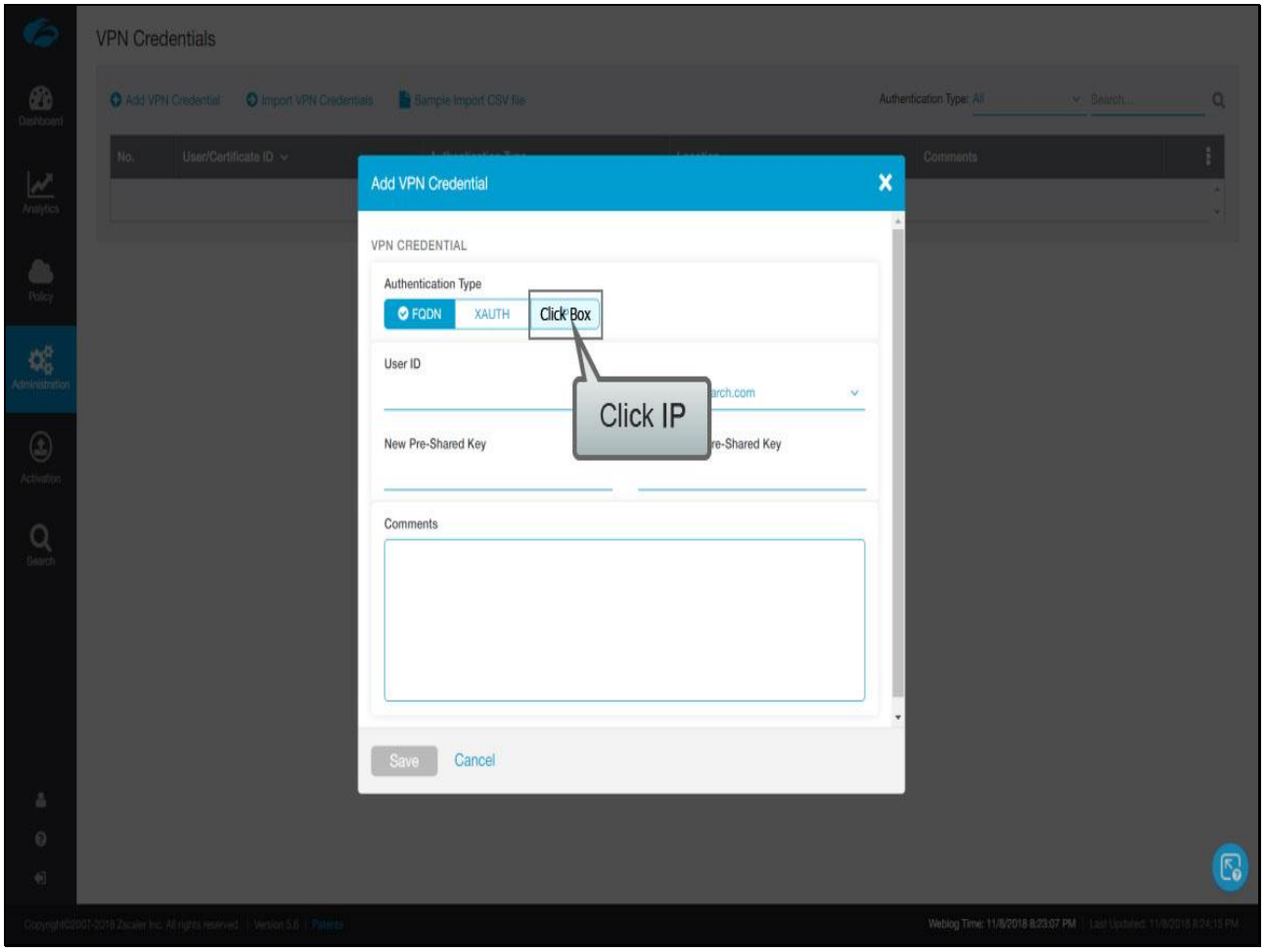
Slide 18 - Slide 18



Slide notes

Click **Add VPN Credentials**.

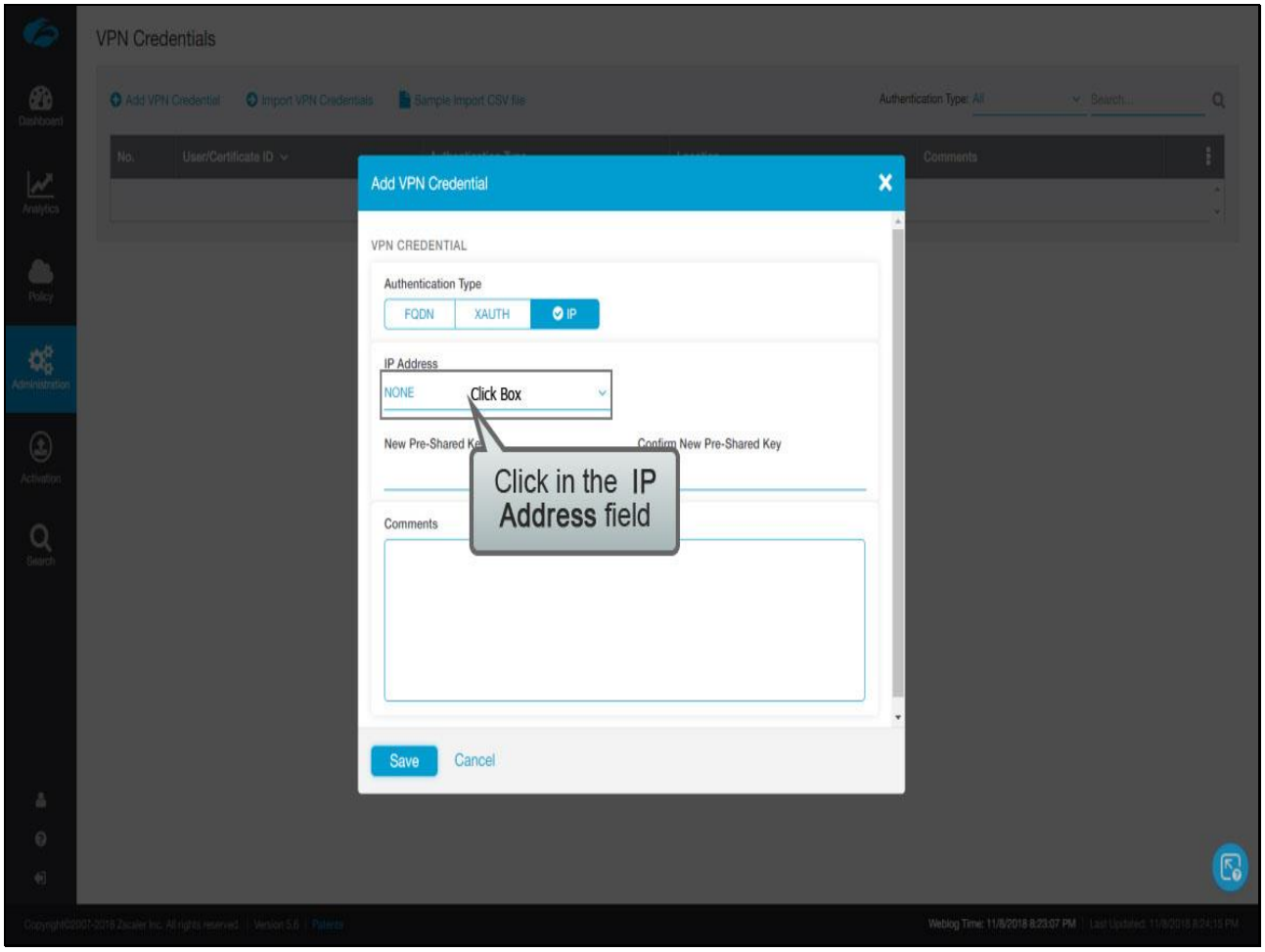
Slide 19 - Slide 19



Slide notes

Next to **Authentication Type**, select **IP**.

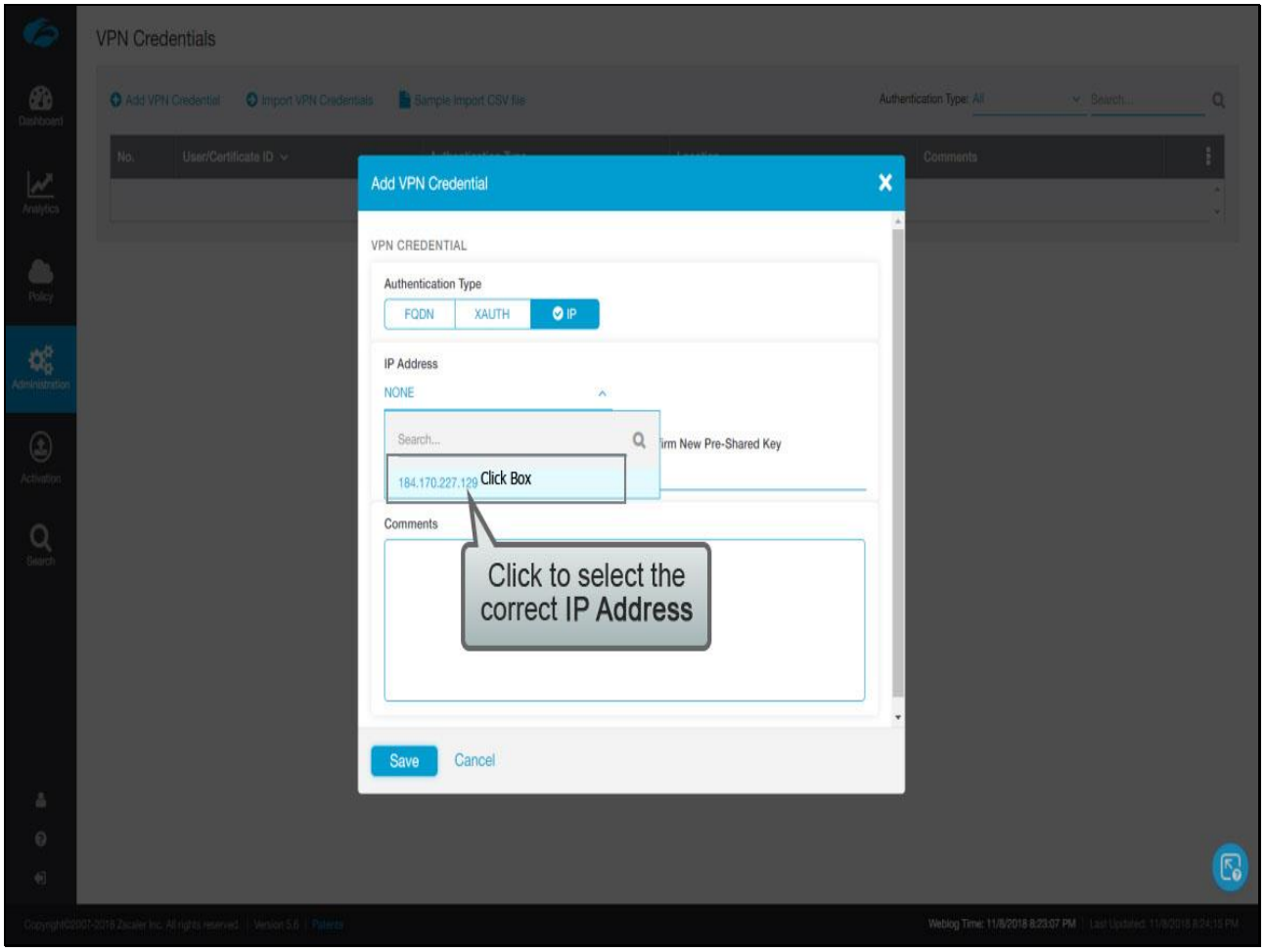
Slide 20 - Slide 20



Slide notes

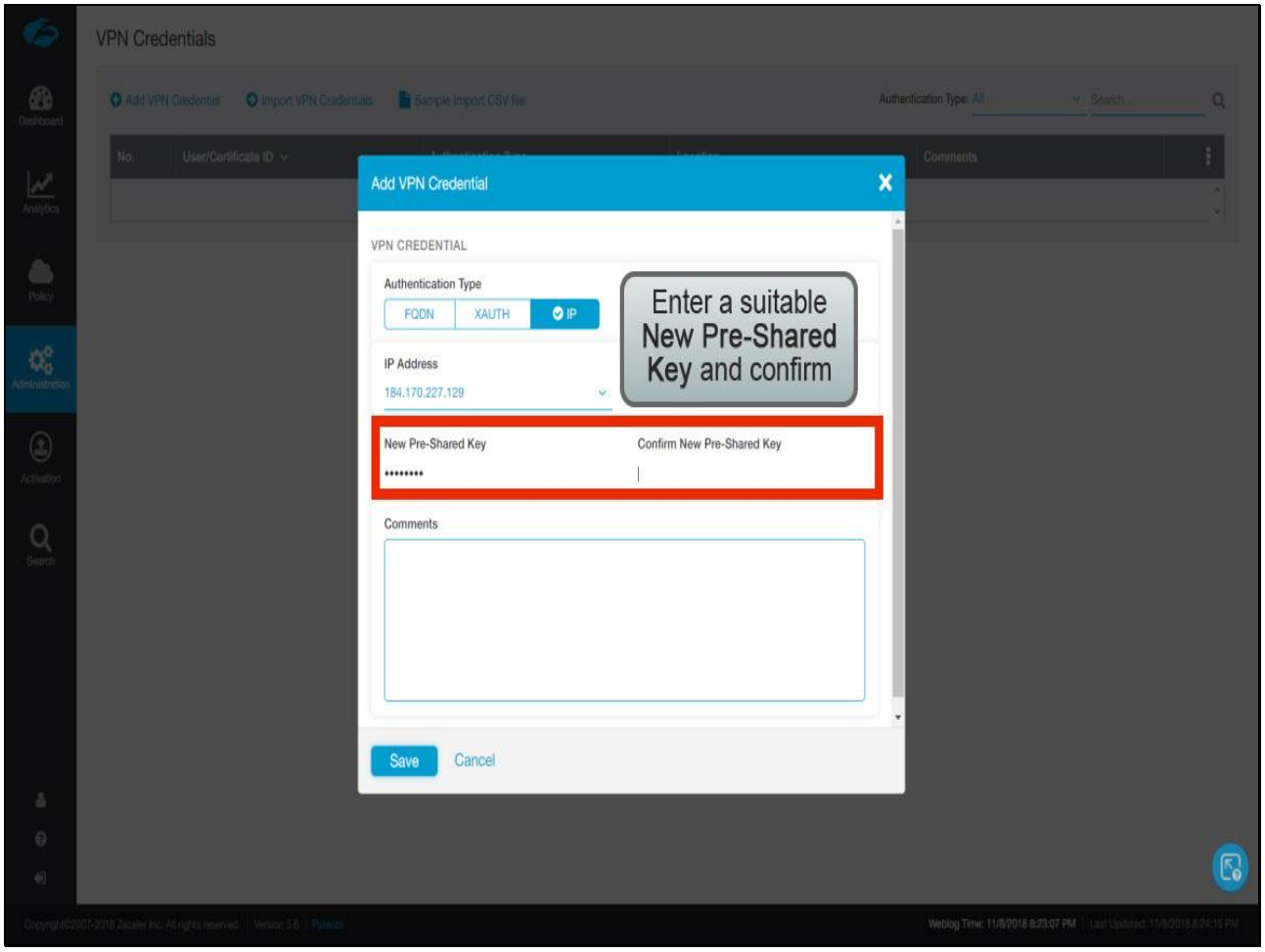
From the **IP Address** drop-down list select the location.

Slide 21 - Slide 21



Slide notes

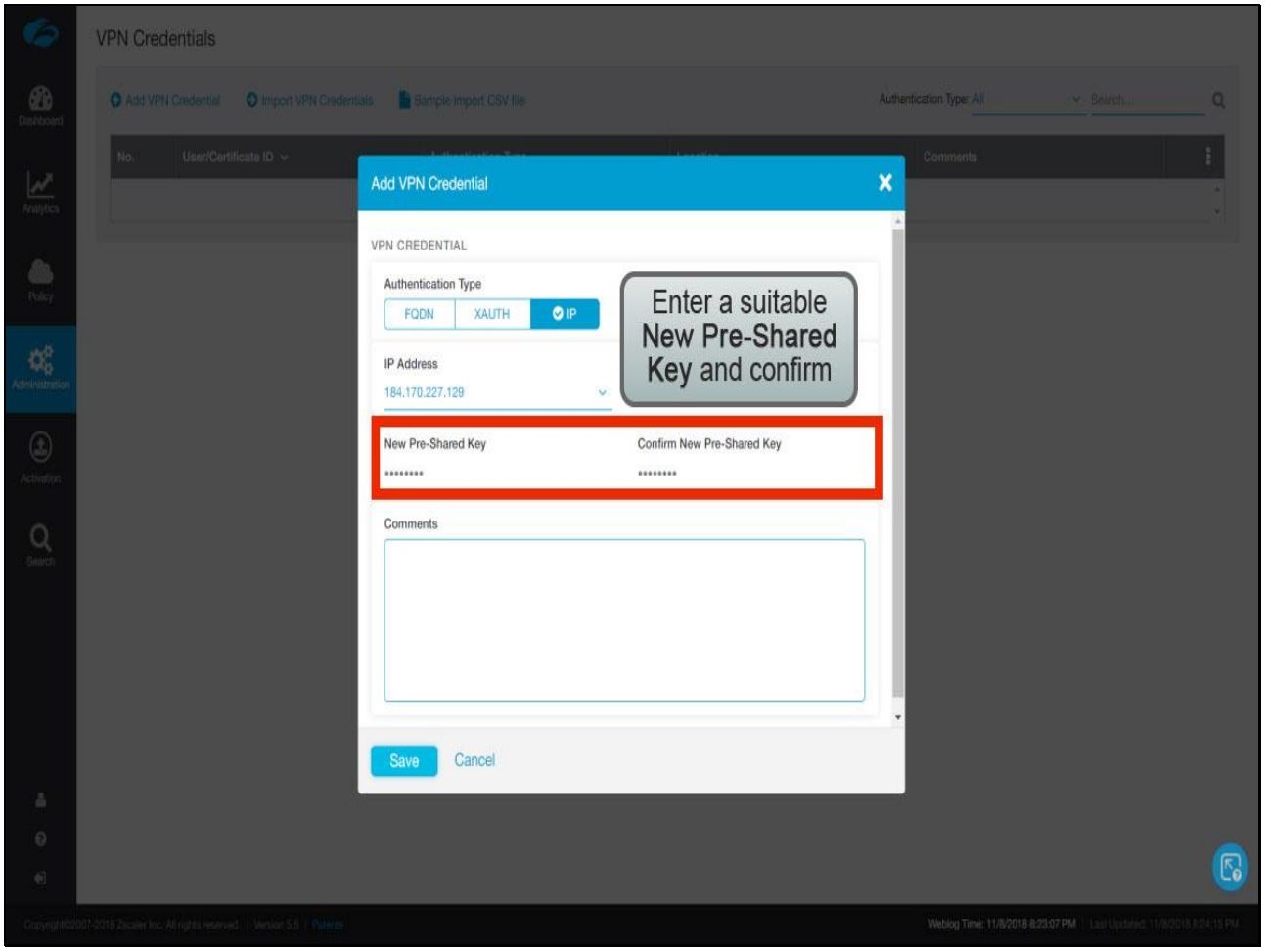
Slide 22 - Slide 22



Slide notes

Type in the **New Pre-Shared Key** for the VPN tunnel.

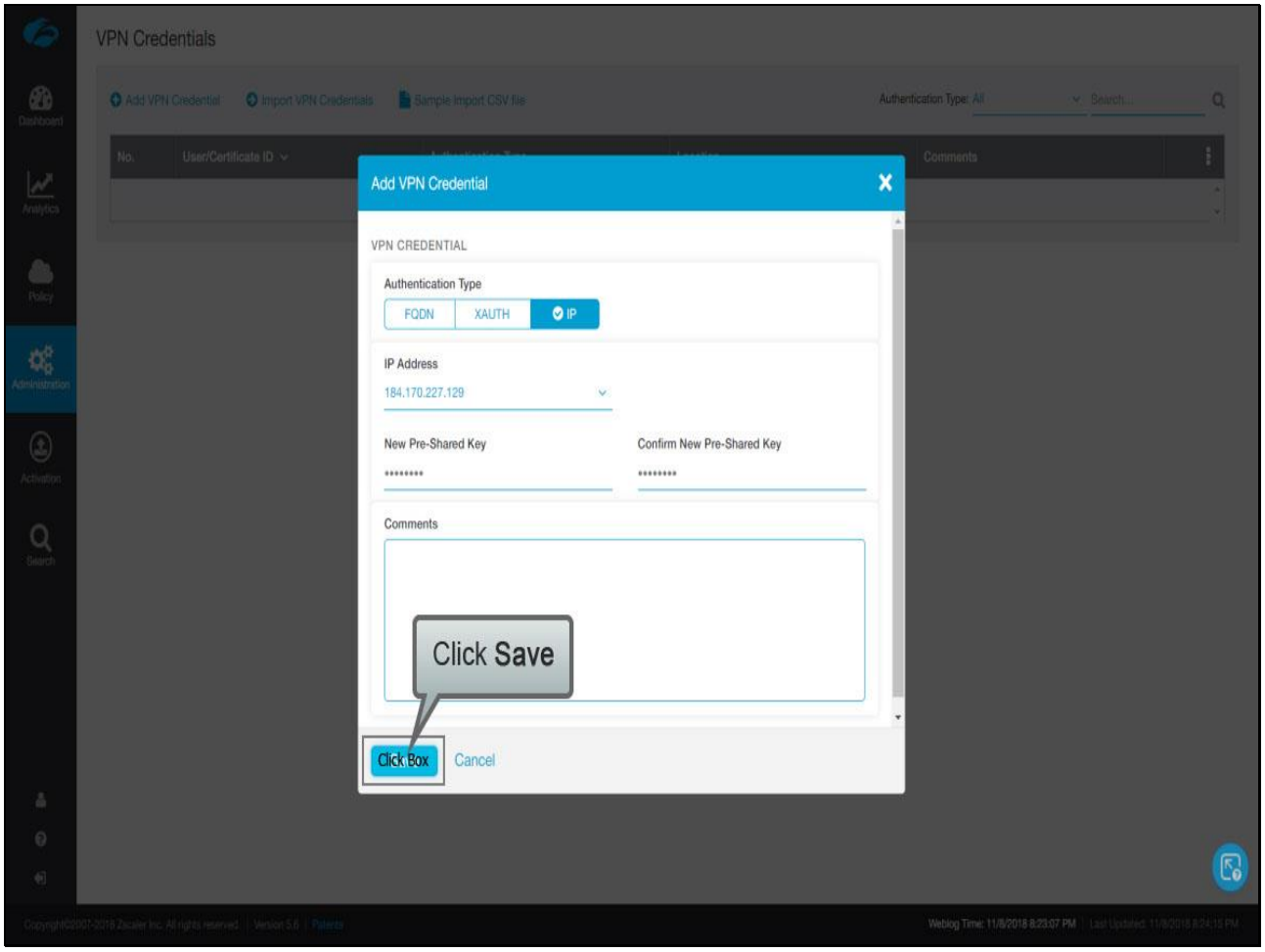
Slide 23 - Slide 23



Slide notes

Then confirm the new pre-shared key.

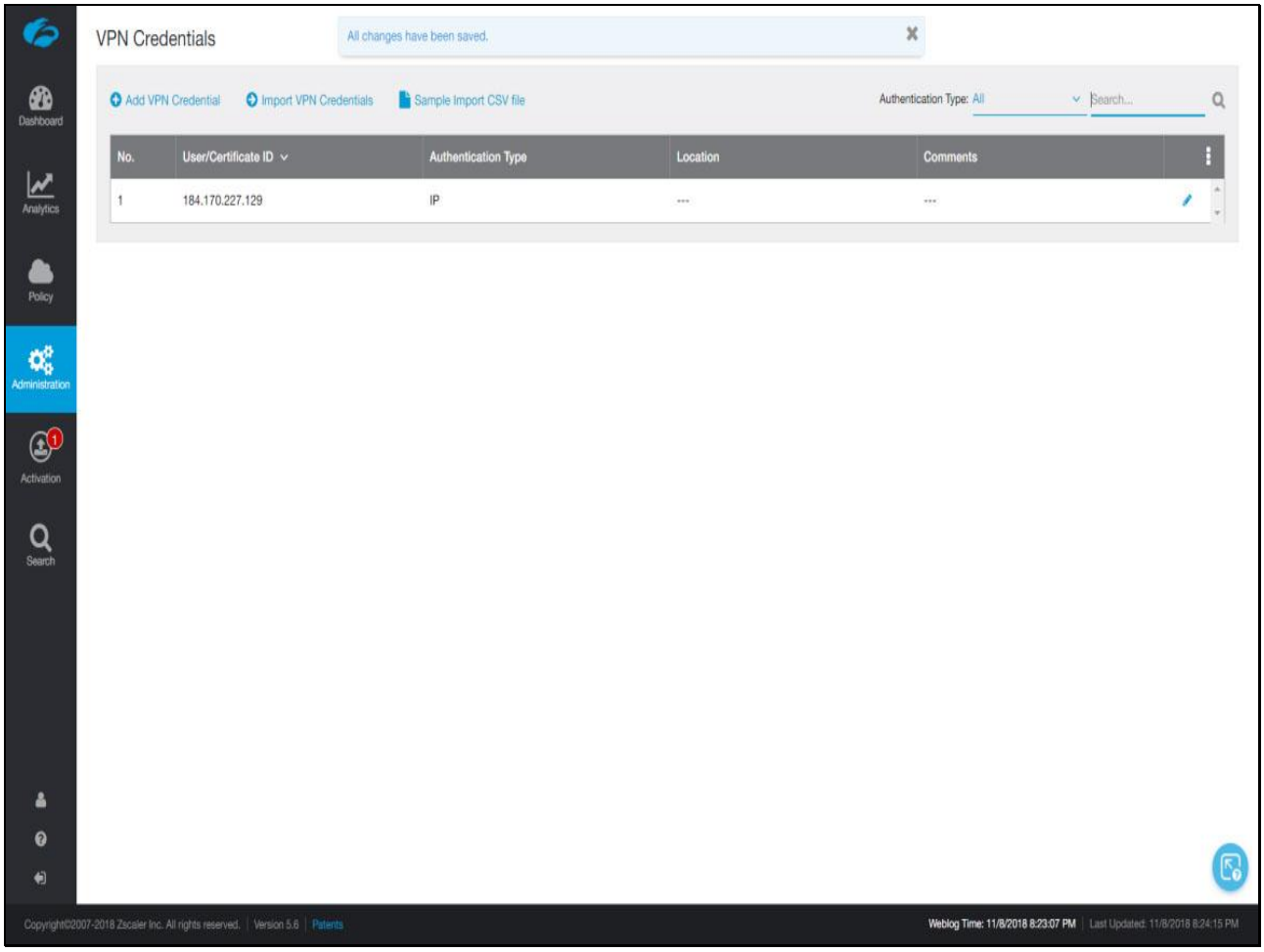
Slide 24 - Slide 24



Slide notes

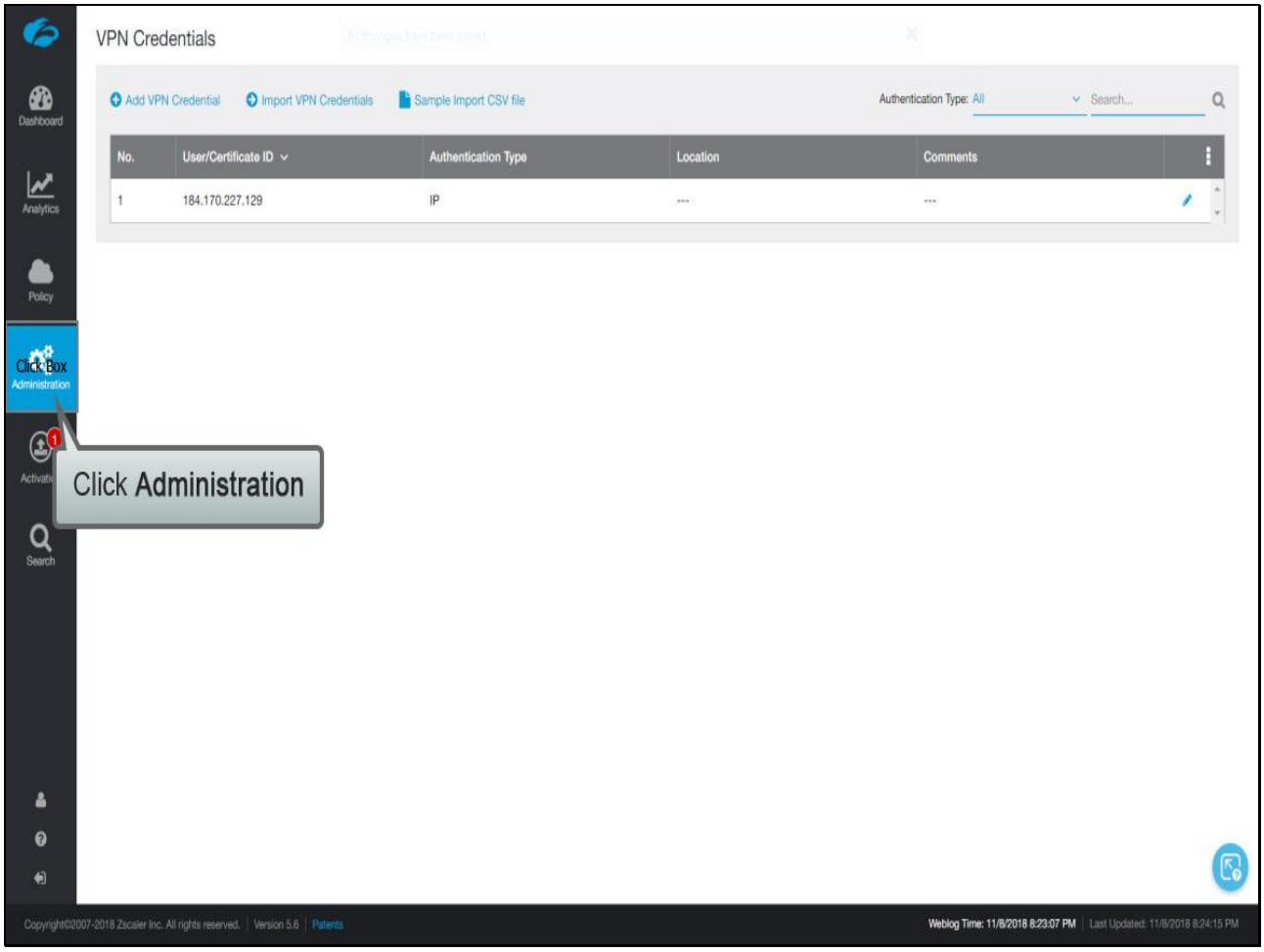
Then click **Save**.

Slide 25 - Slide 25



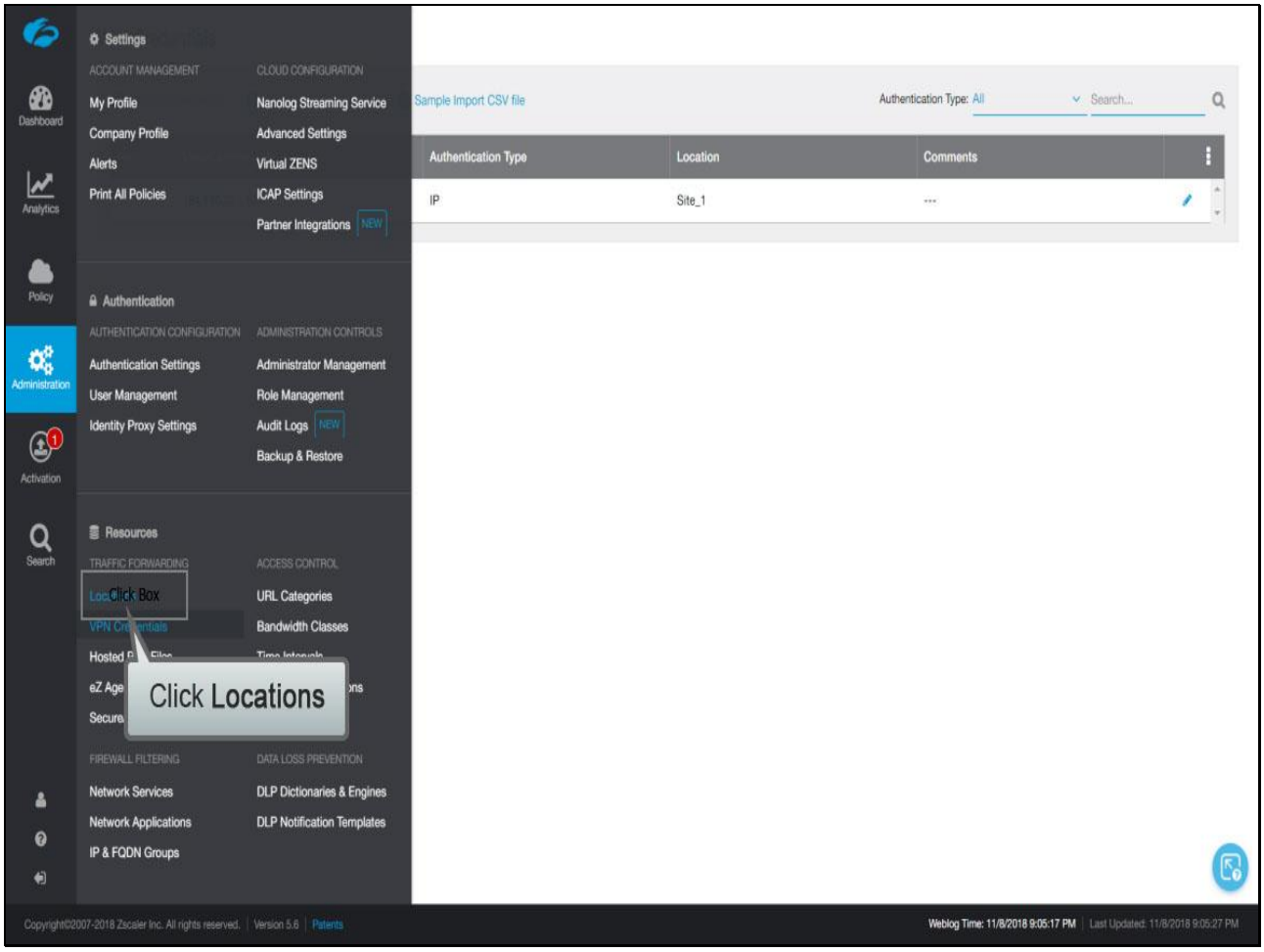
Slide notes

Slide 26 - Slide 26



Slide notes

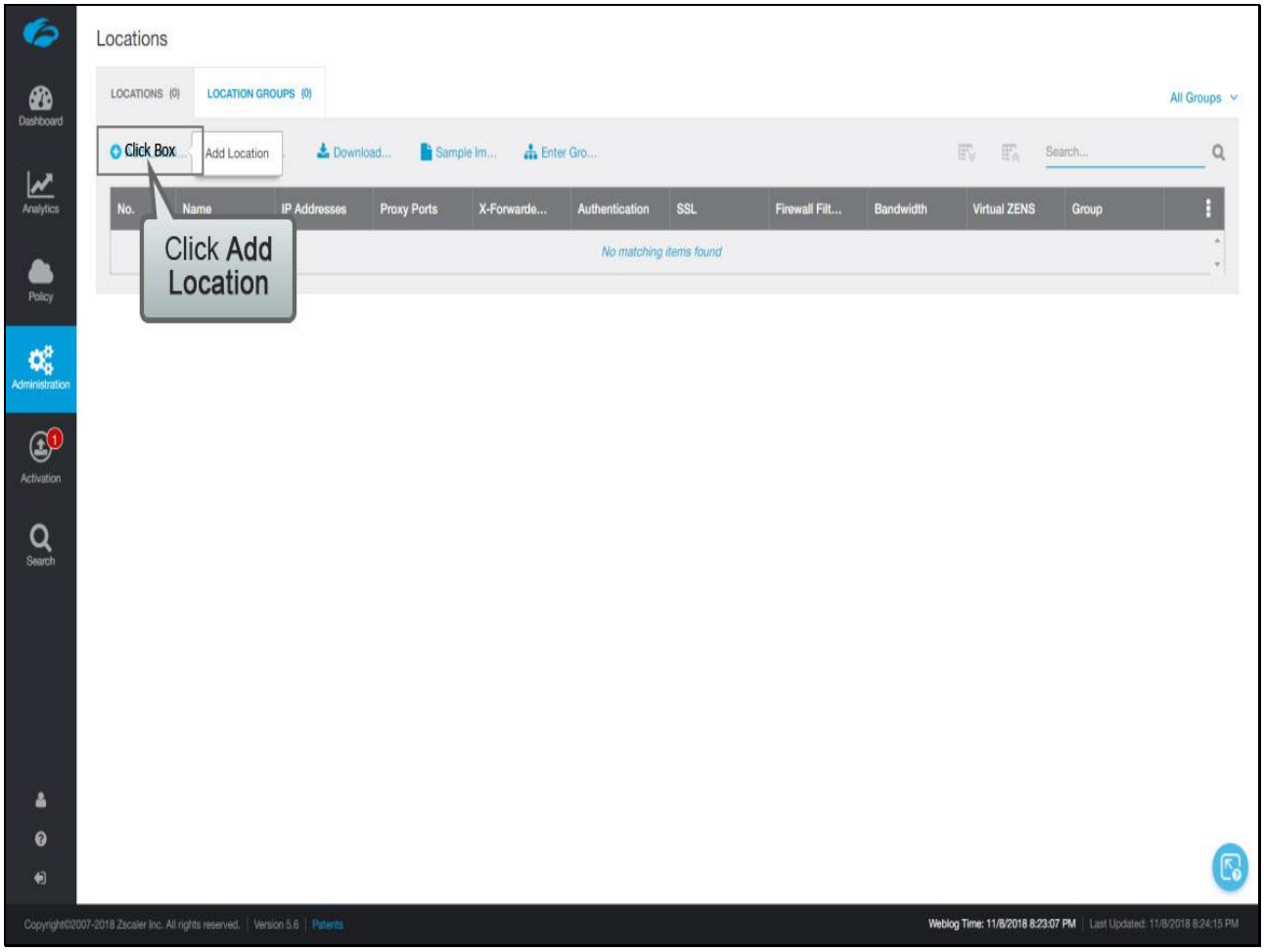
Slide 27 - Slide 27



Slide notes

Next, click on **Locations**, …

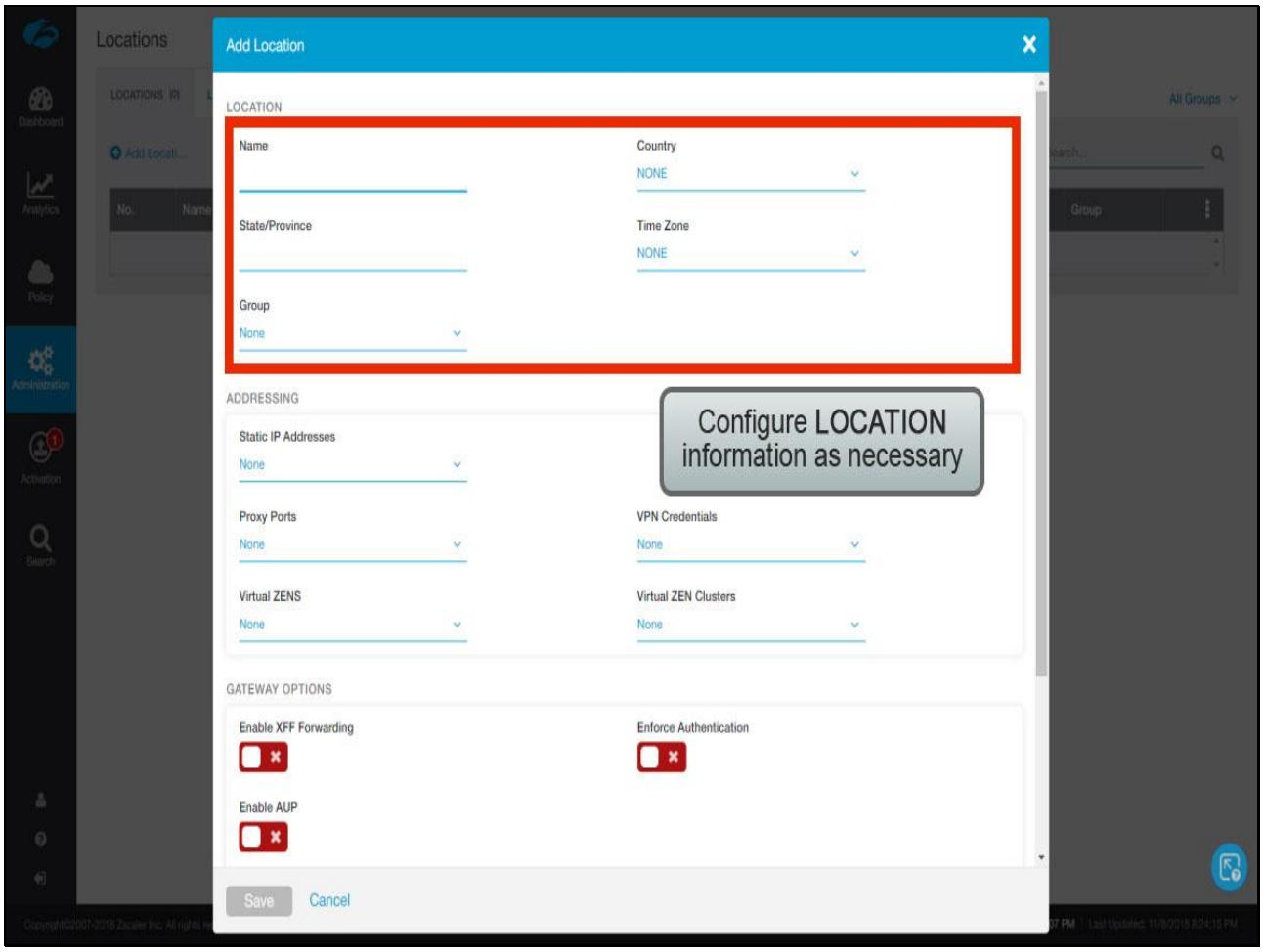
Slide 28 - Slide 28



Slide notes

…click **Add Location**, …

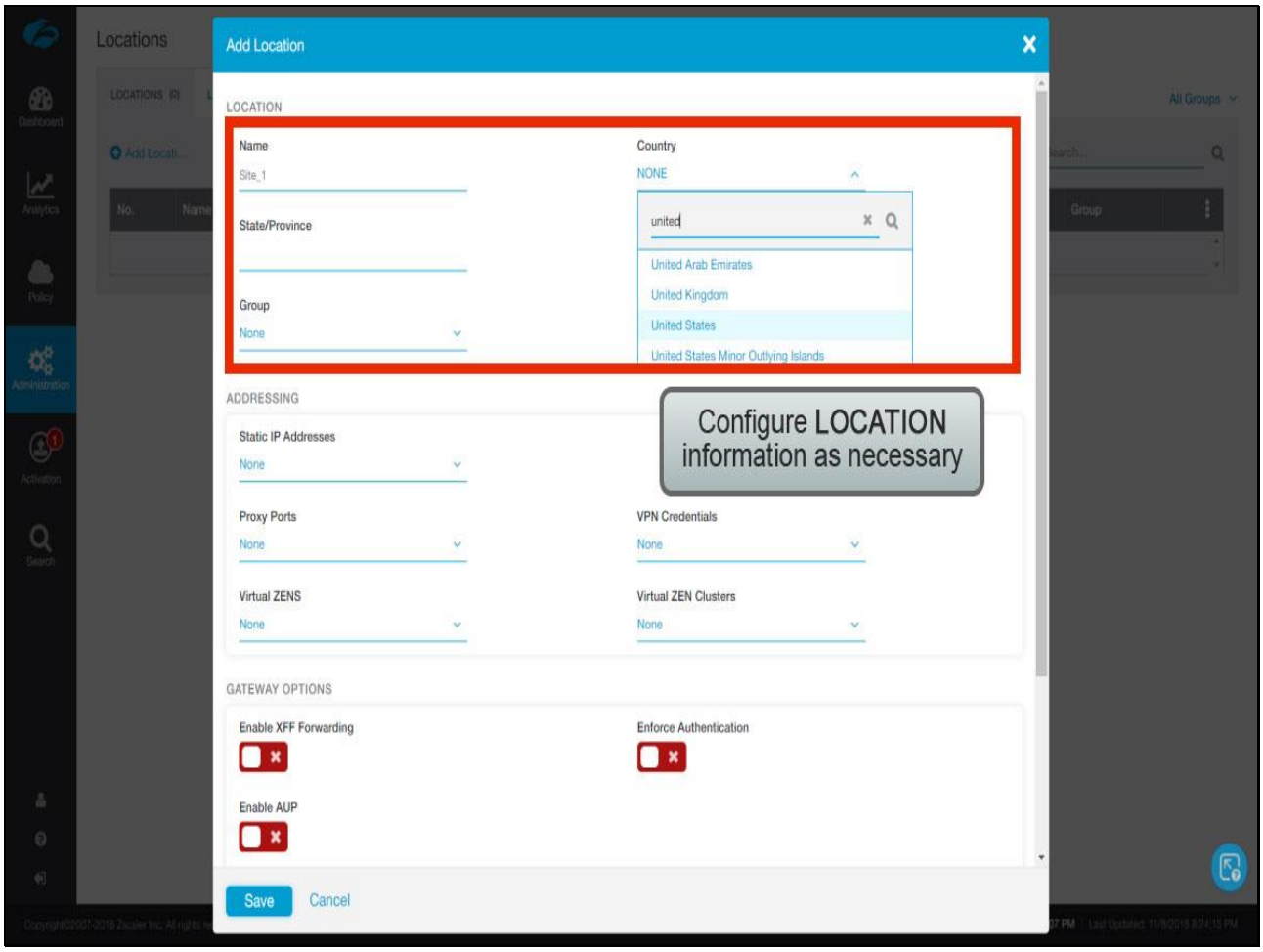
Slide 29 - Slide 29



Slide notes

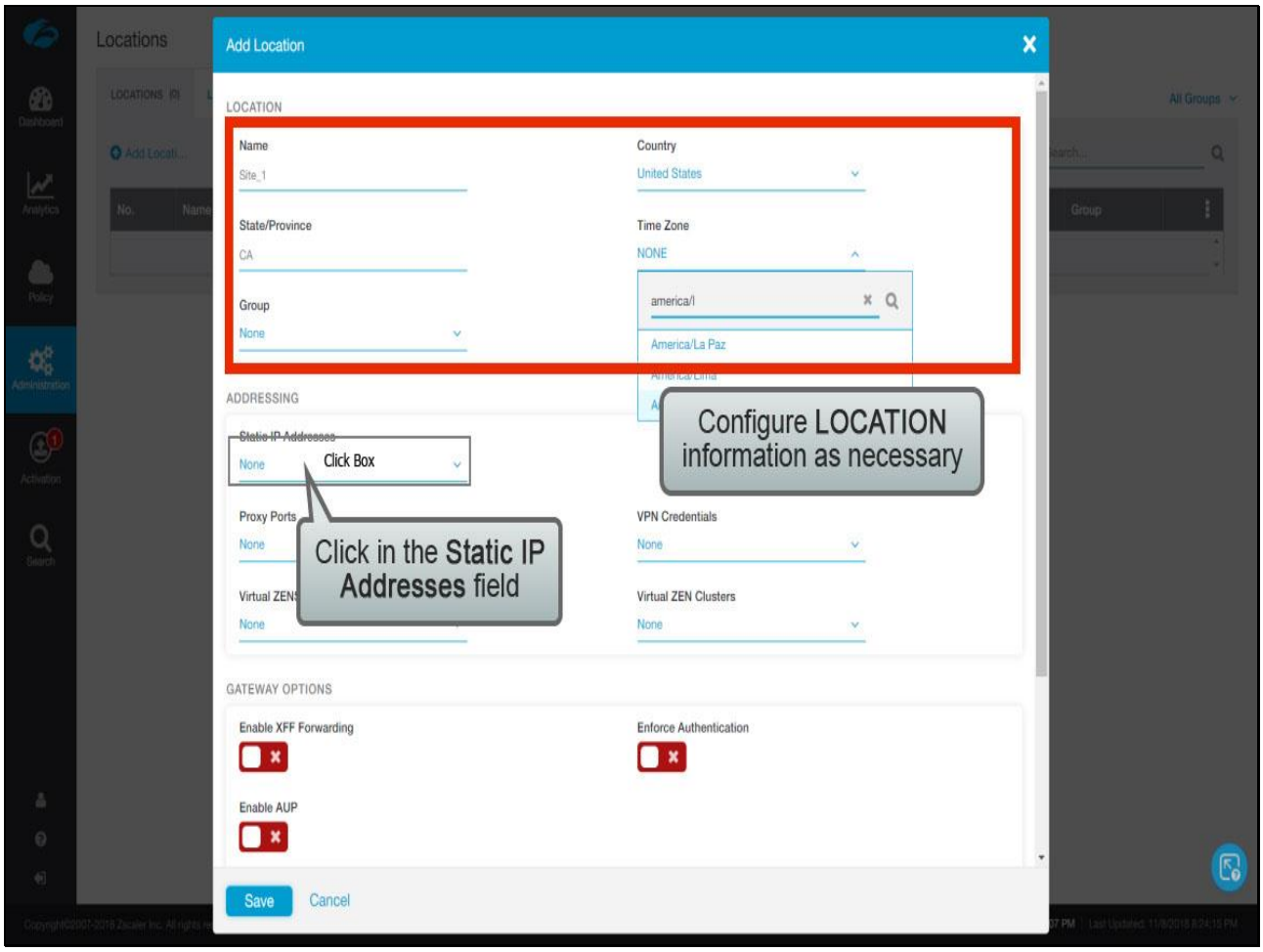
…provide a name for the Location and the **LOCATION** information.

Slide 30 - Slide 30



Slide notes

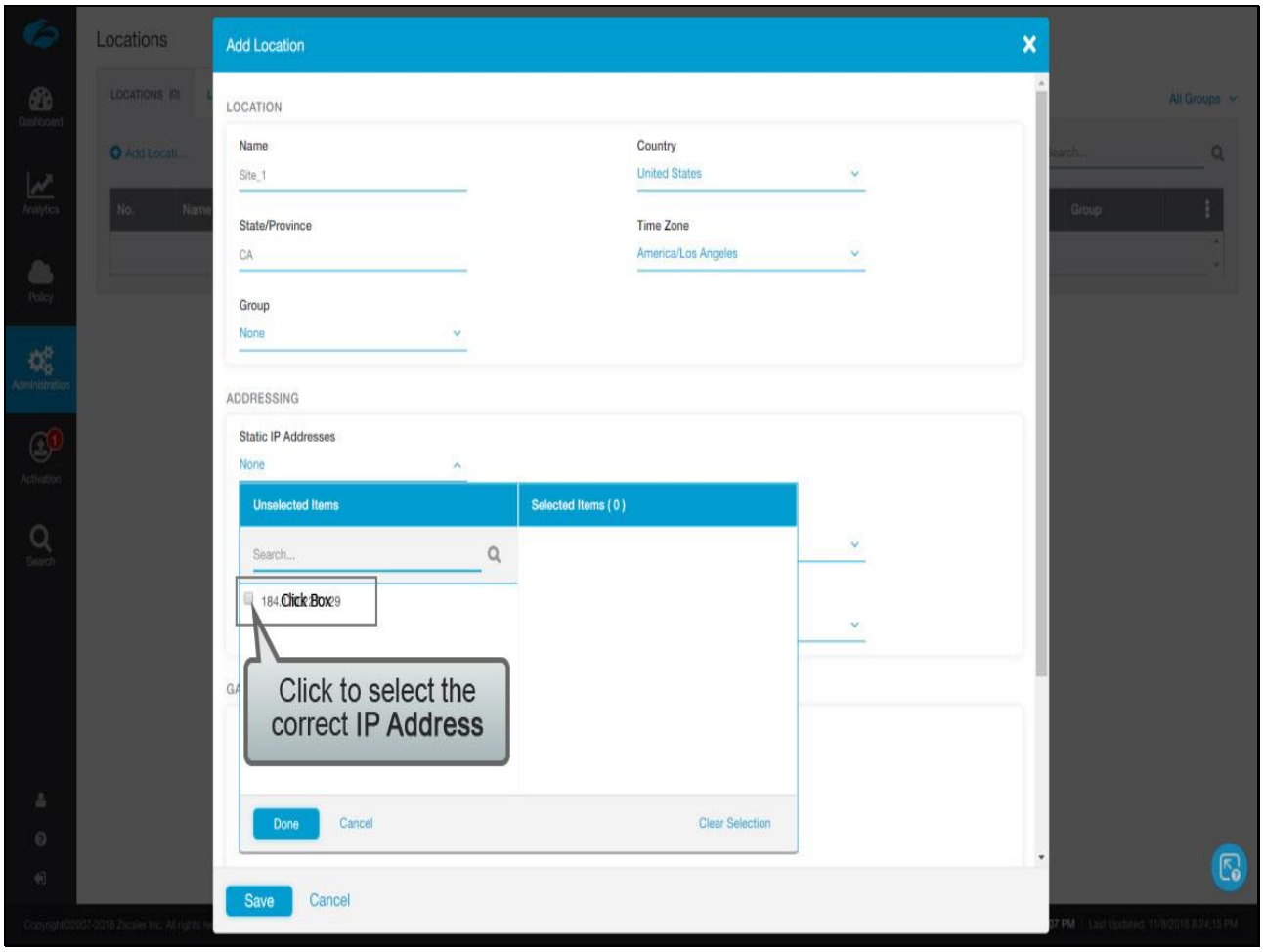
Slide 31 - Slide 31



Slide notes

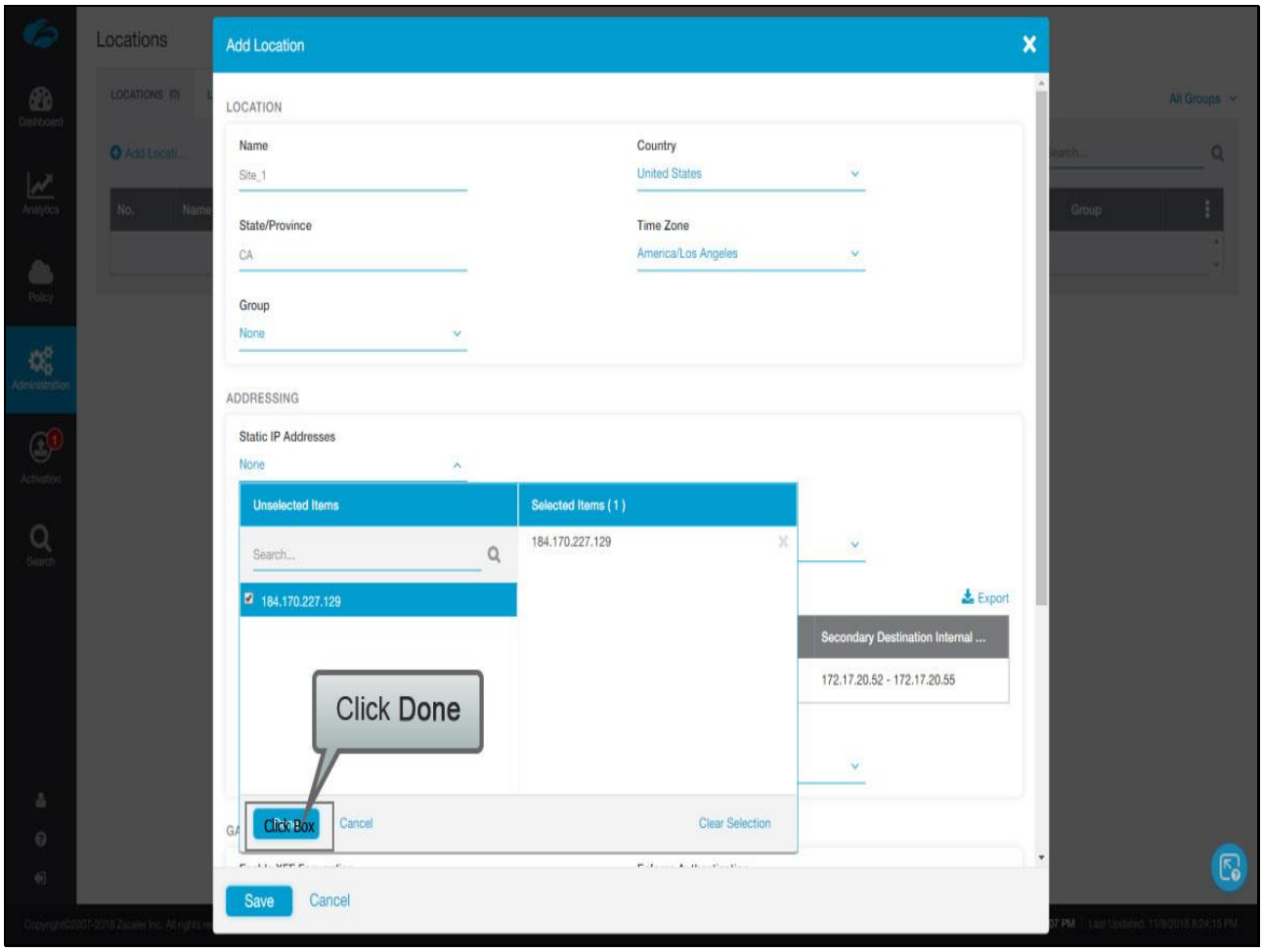
Under the **ADDRESSING** configuration select the **Static IP Address** of the new location from the drop-down.

Slide 32 - Slide 32



Slide notes

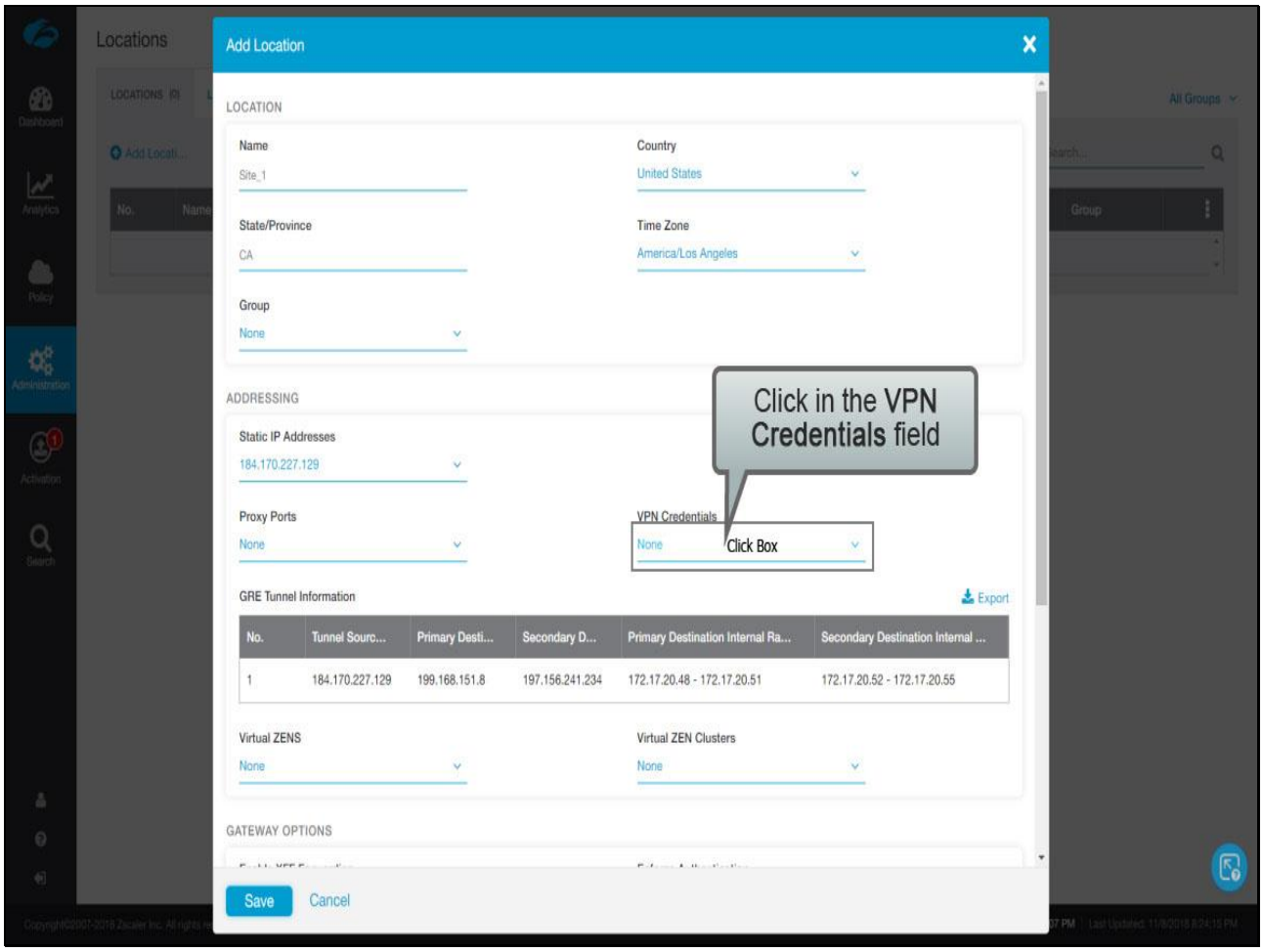
Slide 33 - Slide 33



Slide notes

Then click **Done**.

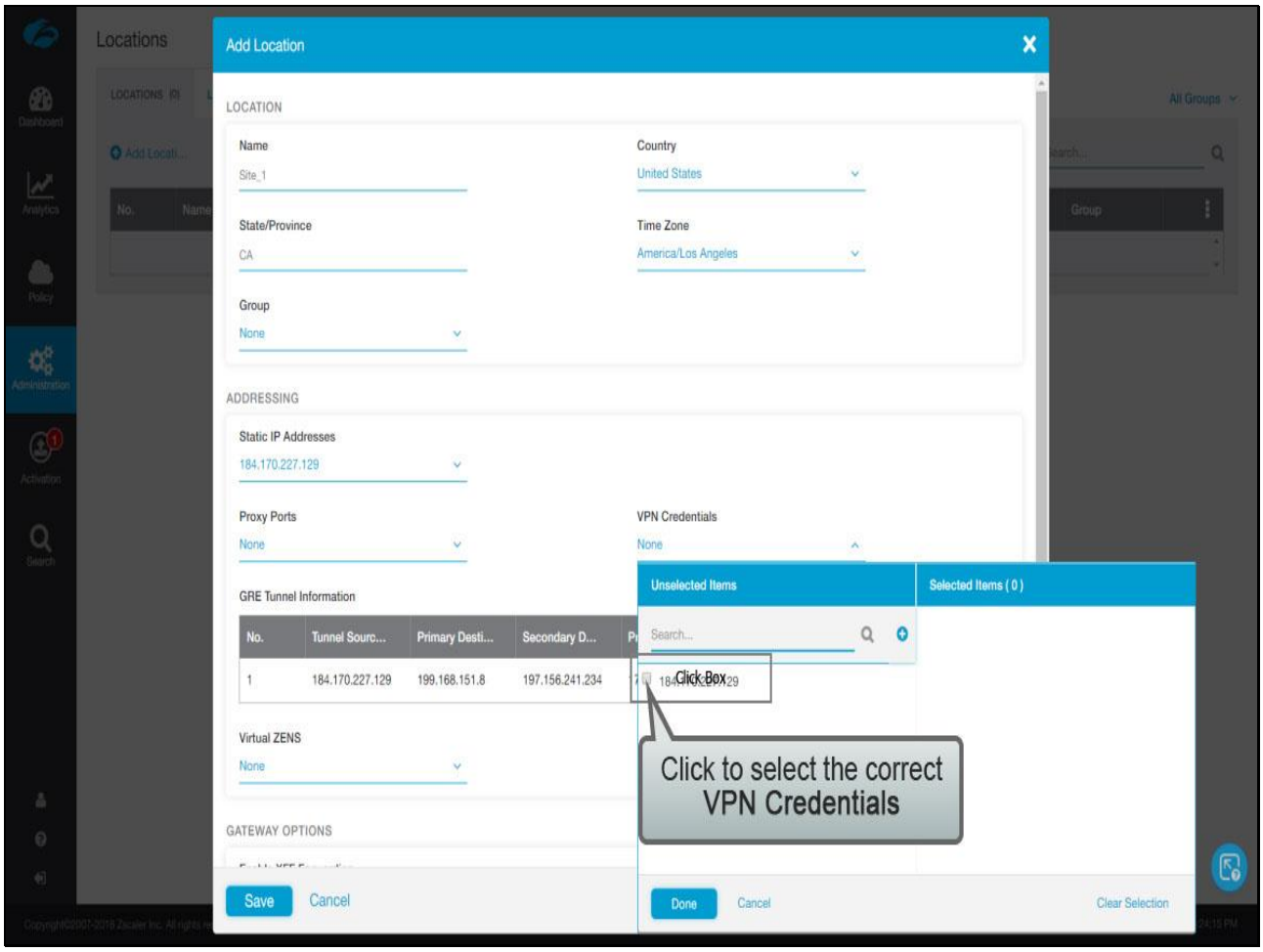
Slide 34 - Slide 34



Slide notes

Select the **VPN Credentials** drop-down box, …

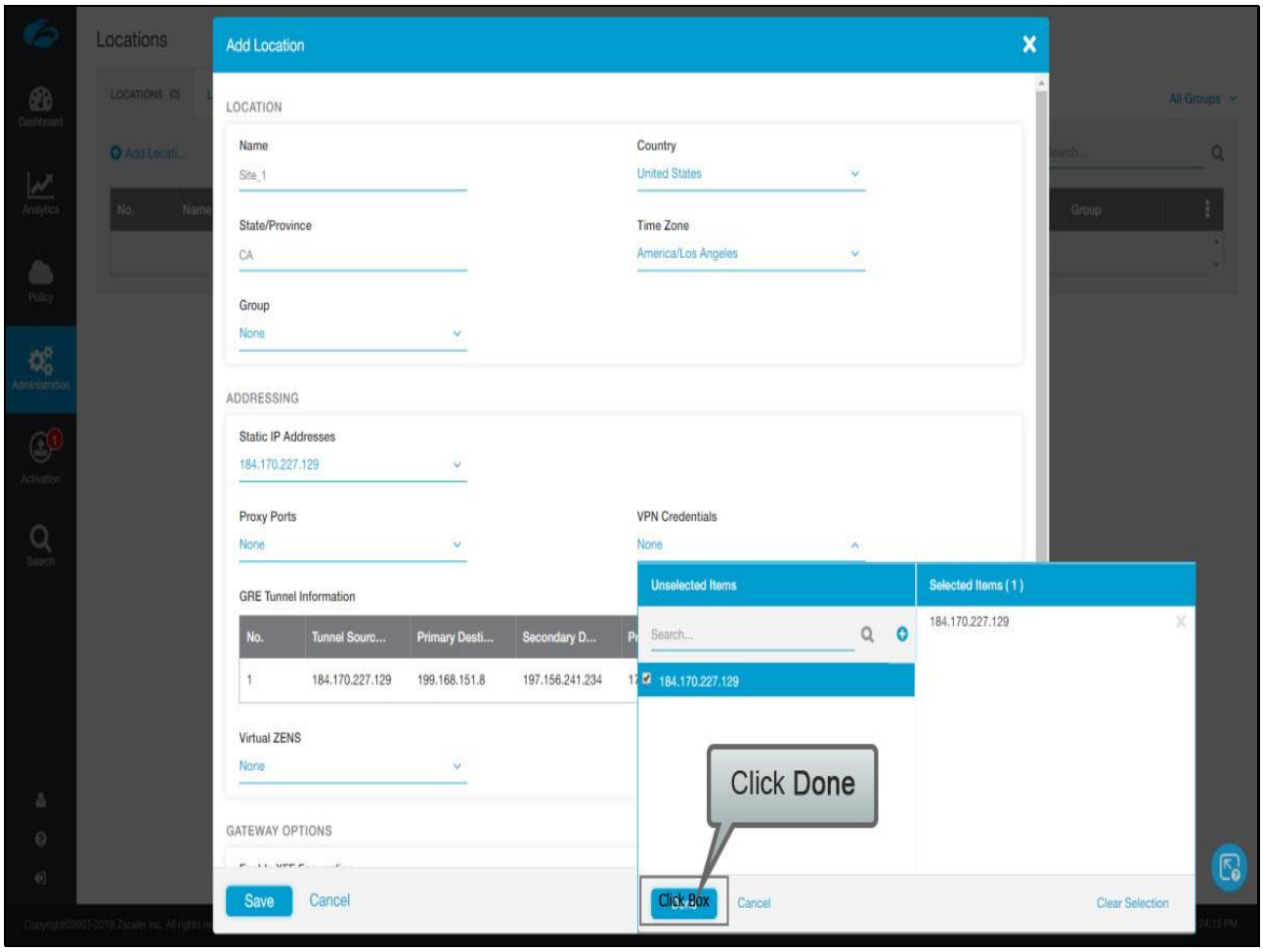
Slide 35 - Slide 35



Slide notes

…and select the IP address of the site.

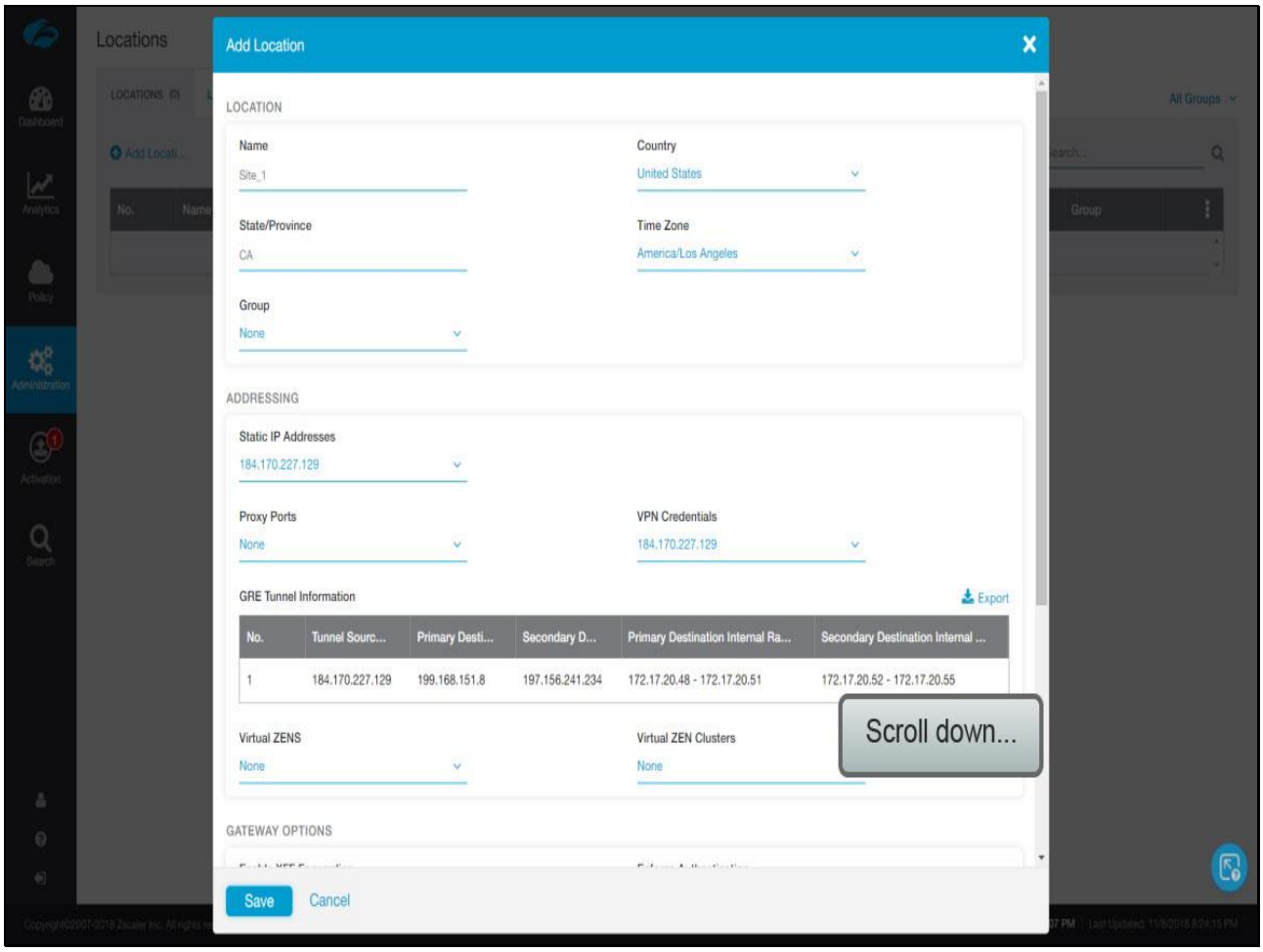
Slide 36 - Slide 36



Slide notes

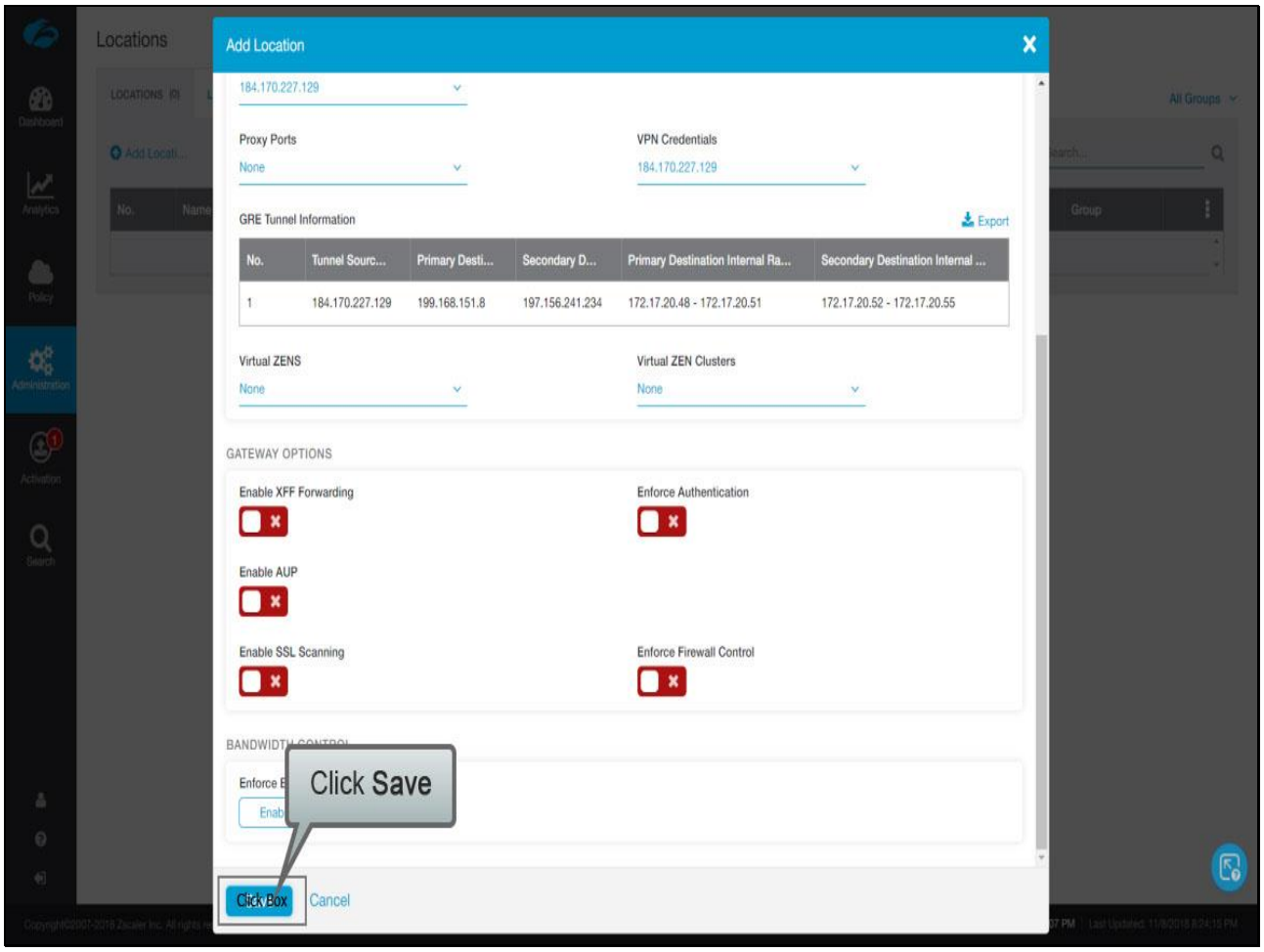
Then click **Done**, …

Slide 37 - Slide 37



Slide notes

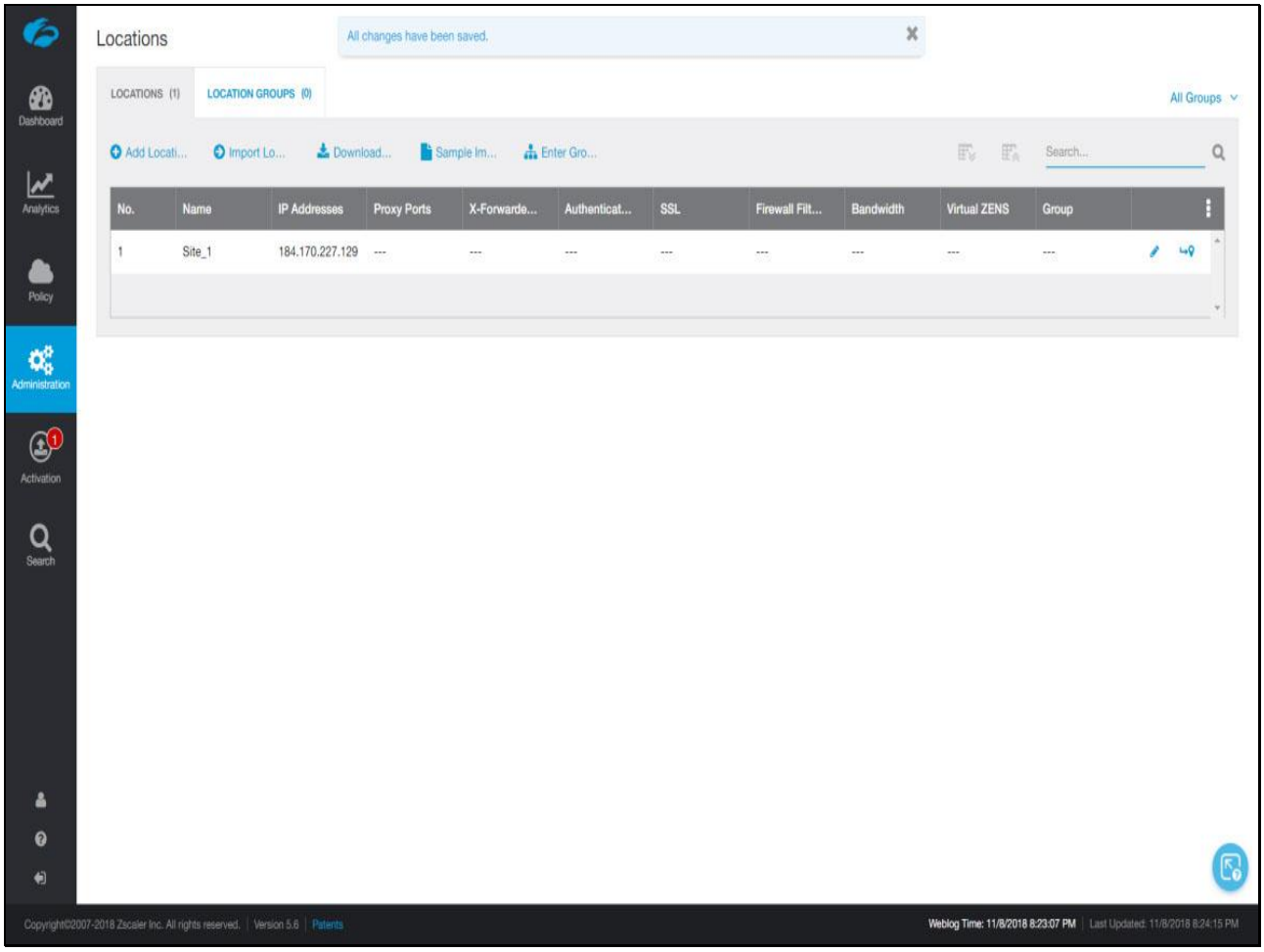
Slide 38 - Slide 38



Slide notes

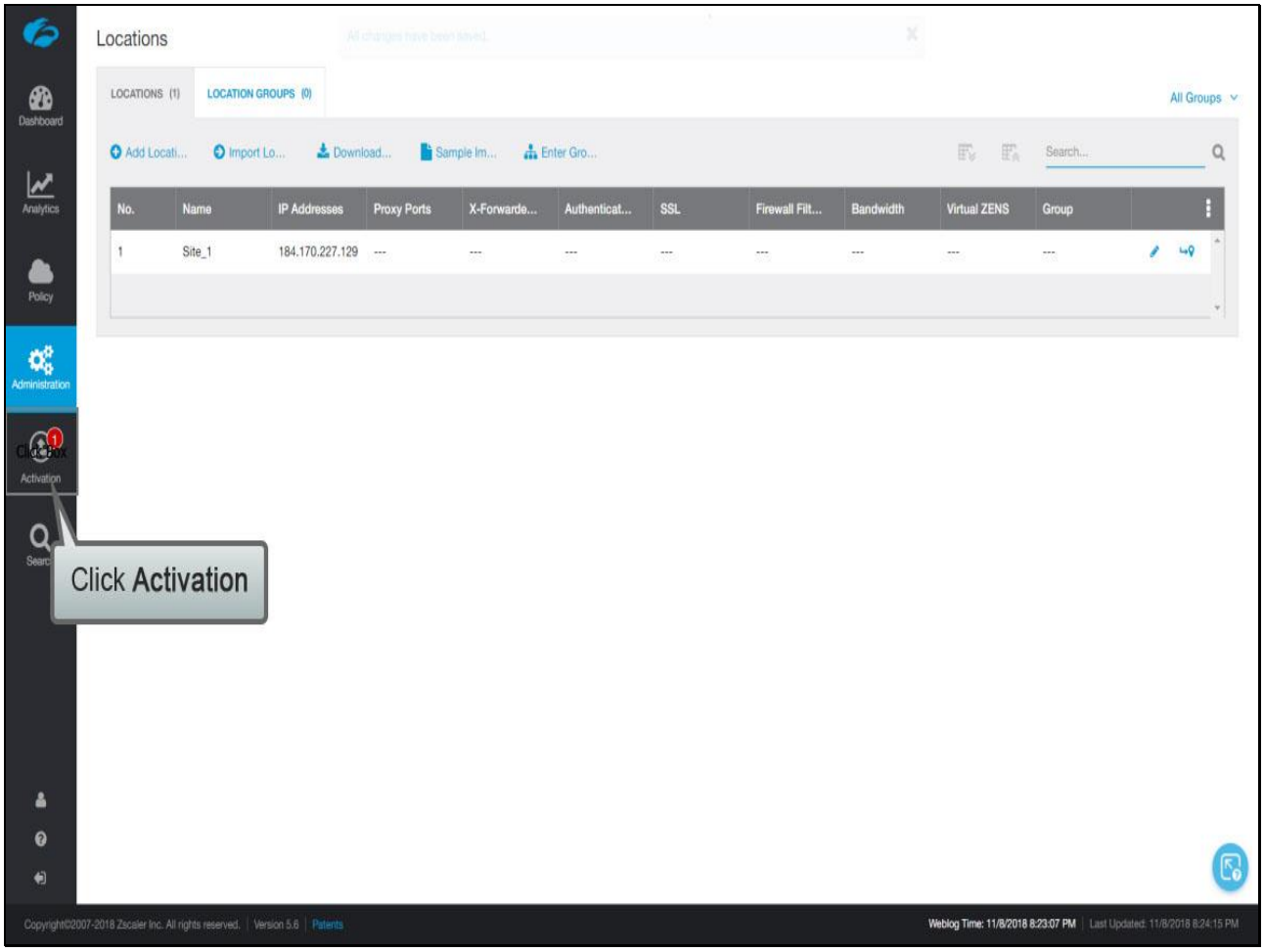
…and then **Save**.

Slide 39 - Slide 39



Slide notes

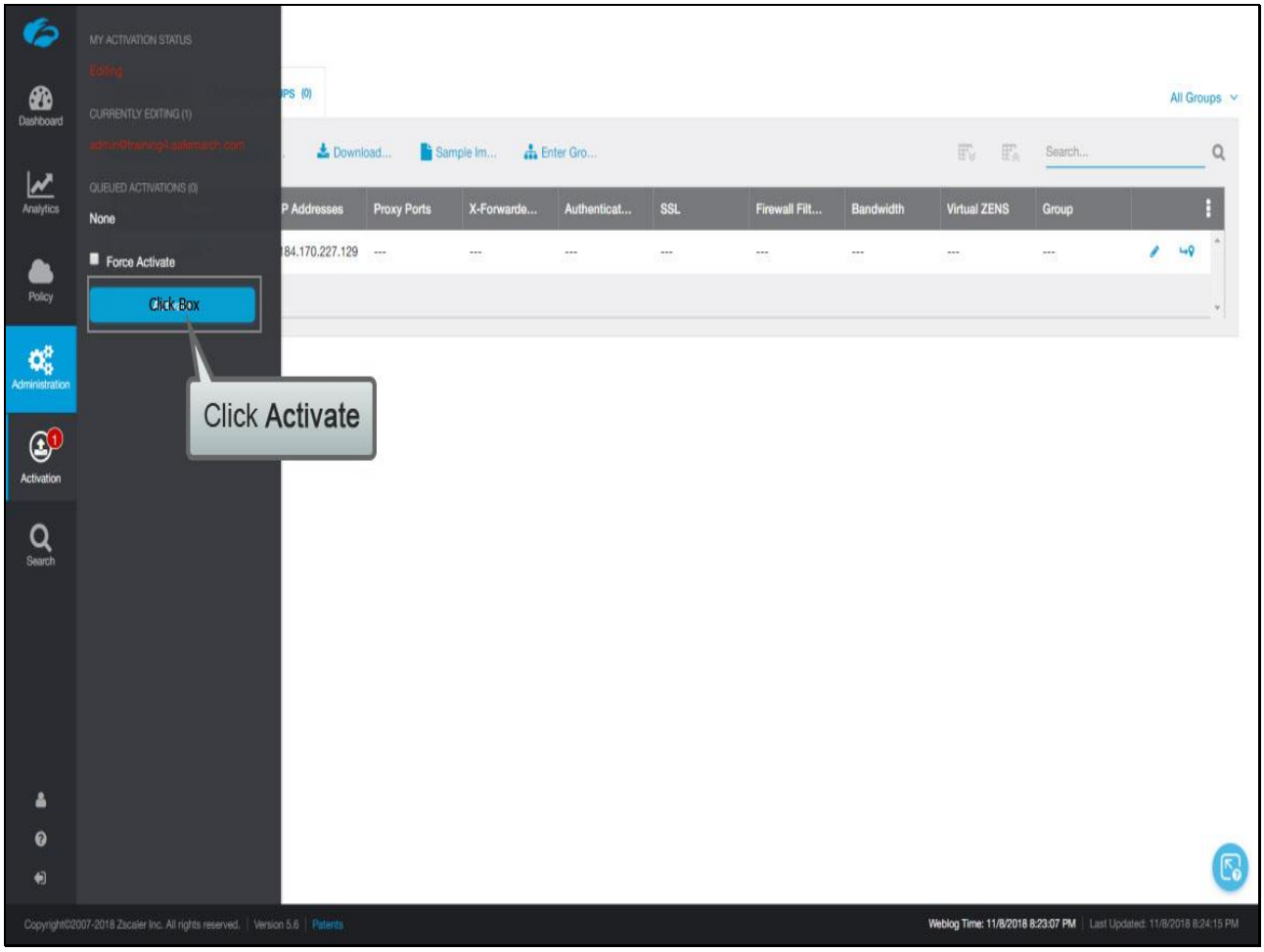
Slide 40 - Slide 40



Slide notes

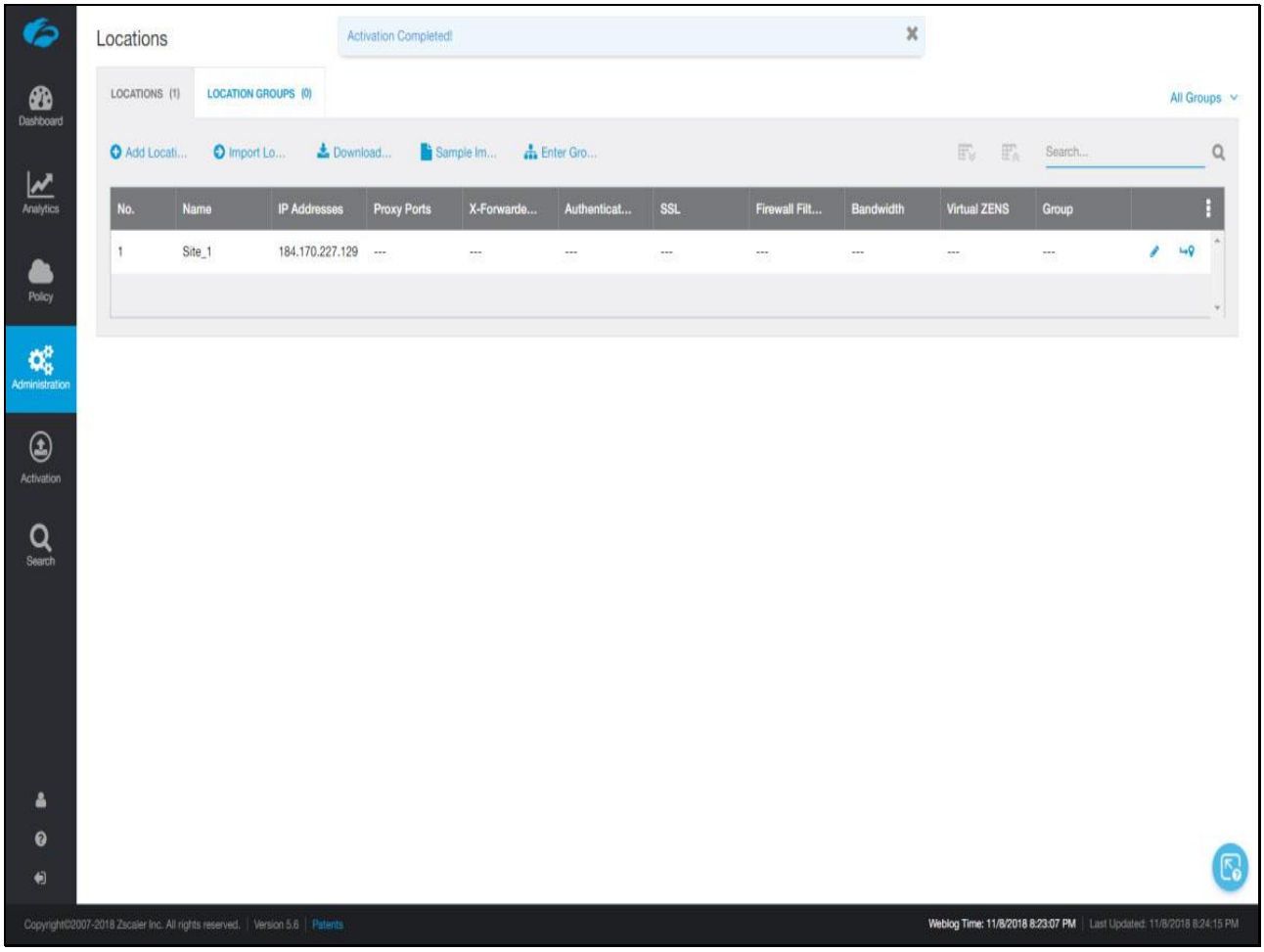
Then **Activate** your changes…

Slide 41 - Slide 41



Slide notes

Slide 42 - Slide 42



Slide notes

Slide 43 - Slide 43

```
Type help or '?' for a list of available commands.
ciscoasa> en
Password: ******
Invalid password
Password: ********
ciscoasa# conf t
ciscoasa(config)#
```

Slide notes

Begin configuring the VPN tunnel in the ASA by first configuring IKE.

Slide 44 - Slide 44

```
Type help or '?' for a list of available commands.
ciscoasa> en
Password: ******
Invalid password
Password: ********
ciscoasa# conf t
ciscoasa(config)# crypto ikev1 enable Outside
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)#      encryption 3des
ciscoasa(config-ikev1-policy)#      authentication pre-share
ciscoasa(config-ikev1-policy)#      hash md5
ciscoasa(config-ikev1-policy)#      group 2
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)#
```

Slide notes

Next, link the VPN tunnel with the IKE configuration.

Slide 45 - Slide 45

```
Type help or '?' for a list of available commands.
ciscoasa> en
Password: ********
ciscoasa# conf t
ciscoasa(config)# crypto ikev1 enable Outside
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)#      encryption 3des
ciscoasa(config-ikev1-policy)#      authentication pre-share
ciscoasa(config-ikev1-policy)#      hash md5
ciscoasa(config-ikev1-policy)#      group 2
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# group-policy Zscaler_GRP internal
ciscoasa(config)# group-policy Zscaler_GRP attributes
ciscoasa(config-group-policy)#      vpn-tunnel-protocol ikev1
ciscoasa(config-group-policy)# exit
ciscoasa(config)#
```

Slide notes

Next, create the Tunnel Group and set the pre-shared key.

Slide 46 - Slide 46

```
Type help or '?' for a list of available commands.
ciscoasa> en
Password: ********
ciscoasa# conf t
ciscoasa(config)# crypto ikev1 enable Outside
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)#      encryption 3des
ciscoasa(config-ikev1-policy)#      authentication pre-share
ciscoasa(config-ikev1-policy)#      hash md5
ciscoasa(config-ikev1-policy)#      group 2
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# group-policy Zscaler_GRP internal
ciscoasa(config)# group-policy Zscaler_GRP attributes
ciscoasa(config-group-policy)#      vpn-tunnel-protocol ikev1
ciscoasa(config-group-policy)# exit
ciscoasa(config)# tunnel-group 104.129.192.35 type ipsec-l2l
ciscoasa(config)# tunnel-group 104.129.192.35 general-attributes
ciscoasa(config-tunnel-general)#      default-group-policy Zscaler_GRP
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)# tunnel-group 104.129.192.35 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 pre-s
ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key Admin-123!
ciscoasa(config-tunnel-ipsec)# exit
ciscoasa(config)#
```

Slide notes

Configure the ACL to forward traffic into the tunnel.

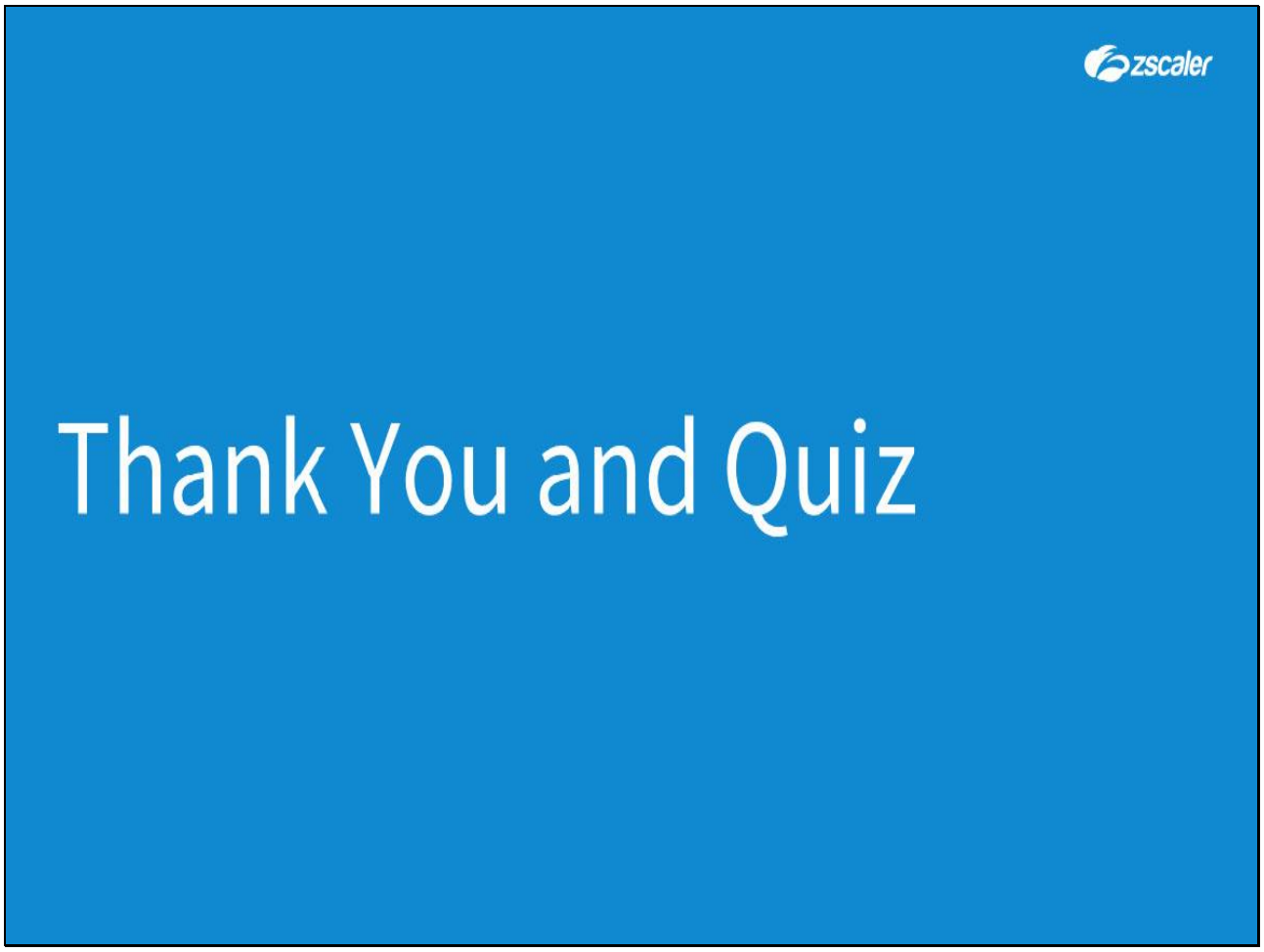
Slide 47 - Slide 47

```
ciscoasa(config)# crypto ikev1 enable Outside
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)#      encryption 3des
ciscoasa(config-ikev1-policy)#      authentication pre-share
ciscoasa(config-ikev1-policy)#      hash md5
ciscoasa(config-ikev1-policy)#      group 2
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# group-policy Zscaler_GRP internal
ciscoasa(config)# group-policy Zscaler_GRP attributes
ciscoasa(config-group-policy)#      vpn-tunnel-protocol ikev1
ciscoasa(config-group-policy)# exit
ciscoasa(config)# tunnel-group 104.129.192.35 type ipsec-l2l
ciscoasa(config)# tunnel-group 104.129.192.35 general-attributes
ciscoasa(config-tunnel-general)#        default-group-policy Zscaler_GRP
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)# tunnel-group 104.129.192.35 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#        ikev1 pre-shared-key Admin123!
ciscoasa(config-tunnel-ipsec)# exit
ciscoasa(config)# object network flow-traffic
ciscoasa(config-network-object)#        subnet 10.84.0.0 255.255.255.0
ciscoasa(config-network-object)# access-list Zscaler_map extended permit ip obj
ciscoasa(config)#
```

Slide notes

And last, the IPSec configuration. Once configured use the following commands to verify the tunnel is up. Begin using **show isakmp sa** and note the IKE peer address and the state is Active. Next, use the command **show ipsec sa** and note that the tunnel is established.

Slide 48 - Thank You and Quiz



Slide notes

This completes the Traffic Forwarding using IPSec VPN tunnels module. We hope this module has been useful to you and thank you for your time.

What will follow is a short quiz to test your knowledge of the material presented in this module. You may retake the quiz as many times as necessary to pass.