


Slide 1 - ZCCP-IA



# ZCCP-IA

Traffic forwarding – IPSec VPN

©2018 Zscaler, Inc. All rights reserved.

**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

## Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. At the top right is the Zscaler logo. Below it is a navigation bar with links: Dashboard, Analytics, Policy, and Administration. The main content area is titled 'Web Overview' and contains several charts and tables. Overlaid on the bottom of the dashboard are several blue callout boxes with white text, each pointing to a specific control on the video player interface. These controls include: 'Previous Slide', 'Next Slide', 'Fast Forward', 'Progress Bar', 'Audio On/Off', 'Closed Captioning', and 'Exit' (located at the top right of the video player window).

Dashboard

Zscaler Cloud Portal

Dashboard Analytics Policy Administration

Web Overview

Cloud Application Classes

Top URL Categories

Top Users

Previous Slide

Next Slide

Fast Forward

Progress Bar

Audio On/Off

Closed Captioning

Exit

**Slide notes**

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

**Slide 3 - Agenda**

# Agenda

- Understanding IPSec VPN
  - Technology Overview
- Connecting to Zscaler
  - VPN configuration

**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



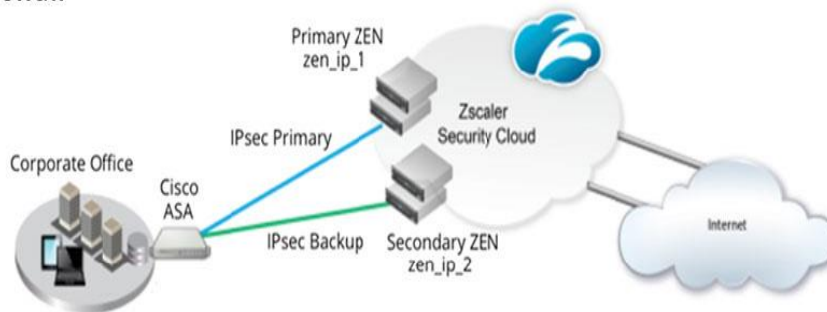
Slide notes

## Slide 5 - IPSec Overview



## IPSec Overview

- Internet Protocol Security (IPSec) is a protocol suite for authenticating, tunneling, and, optionally, encrypting IP traffic
  - IPSec is a common way to securely transport traffic between nodes in the network
  - IPSec VPNs can be used to forward all traffic from corporate and branch offices to Zscaler
  - IPSec VPNs require no configuration on PCs or laptops (unlike PAC files)
  - IPSec VPNs support tunneling from dynamic IP address branches, or from locations behind a NAT'd firewall

**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.



## IPSec Overview Cont.

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



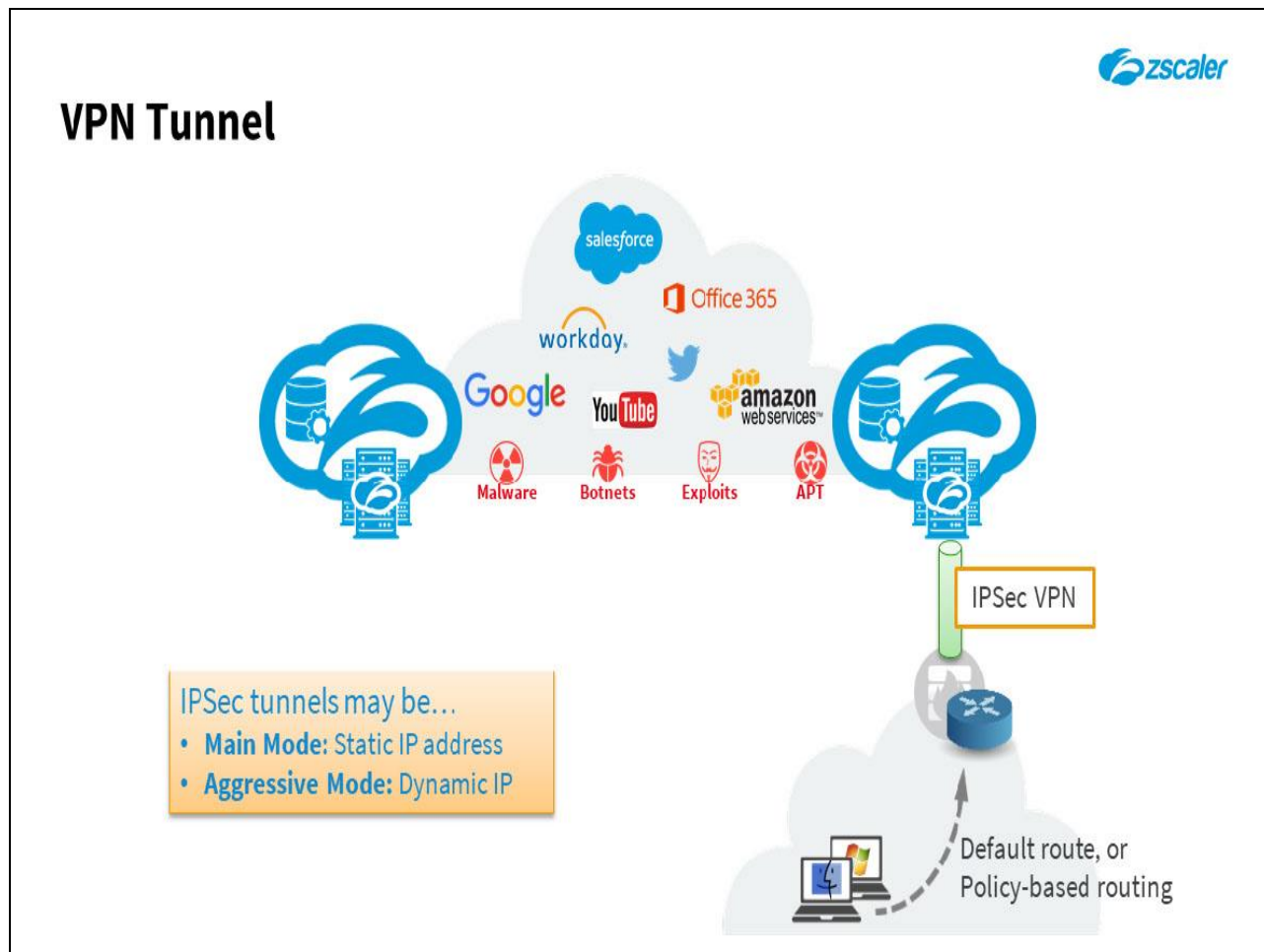
### Slide notes

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



## IPSec Modes

- Aggressive mode
  - IPSEC client has an IP address unknown to the concentrator
  - Authentication requires a known FQDN and knowledge of the pre-shared key
- Main mode
  - IPSEC client has an IP address known to the concentrator
  - Knowledge of the pre-shared key is sufficient for the concentrator to authenticate the client

## 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.

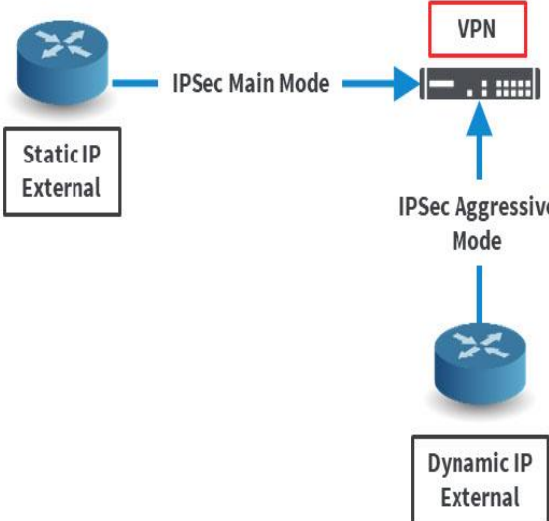
Main mode is used when the IP address of the device is known and is a fixed public IP such as that which would be configured on your Border Router or Firewall. Because Main mode uses the IP address as part of the exchange for identification, it cannot be used in a configuration where the IP address of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



## Slide 9 - IPSec Modes

## IPSec Modes

- Aggressive mode
  - IPSEC client has an IP address unknown to the concentrator
  - Authentication requires a known FQDN and knowledge of the pre-shared key
- Main mode
  - IPSEC client has an IP address known to the concentrator
  - Knowledge of the pre-shared key is sufficient for the concentrator to authenticate the client

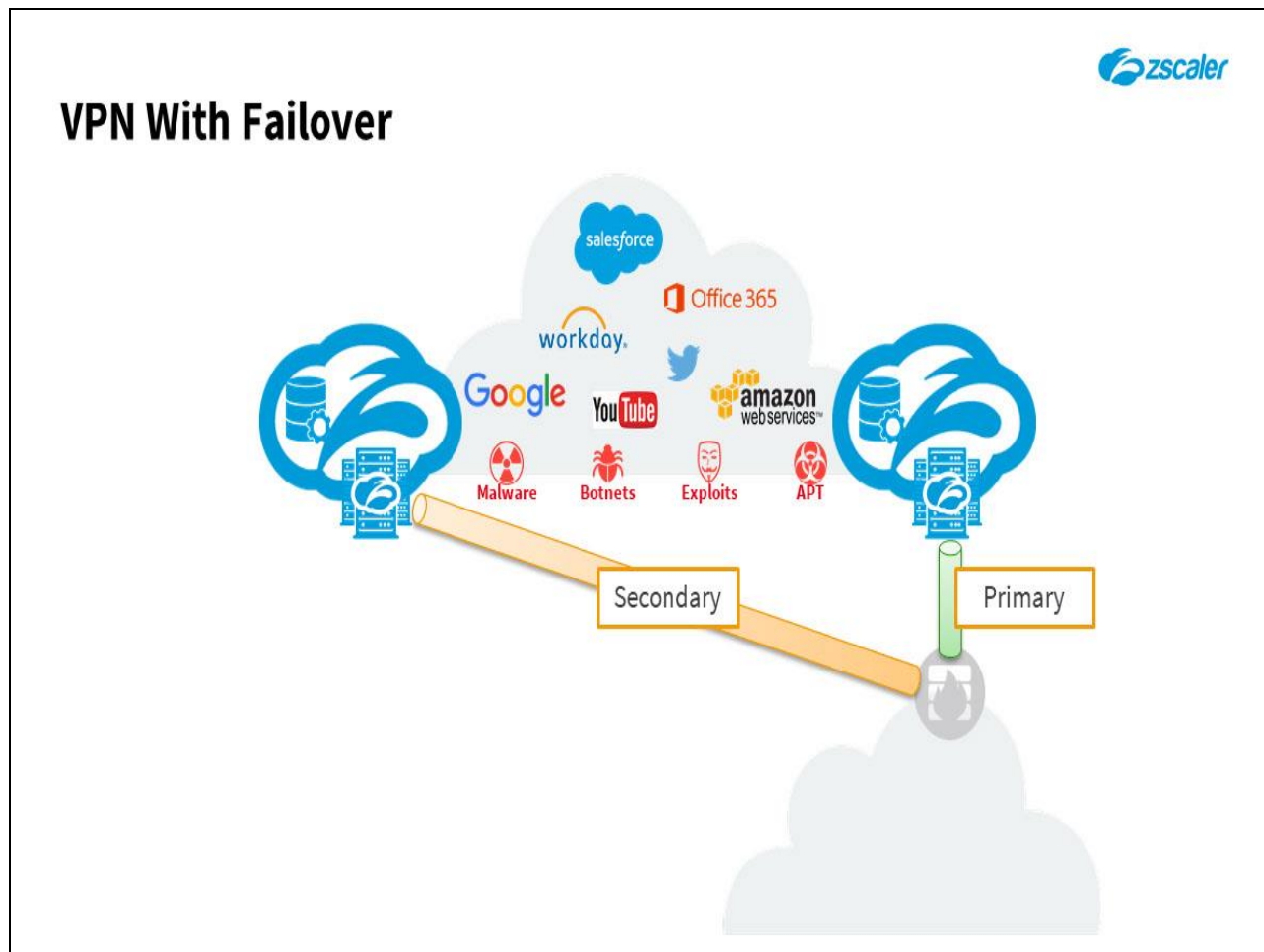


```
graph LR; R1[Router: Static IP External] -- "IPSec Main Mode" --> C[VPN Concentrator]; R2[Router: Dynamic IP External] -- "IPSec Aggressive Mode" --> C;
```

## 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



## Zscaler Recommended Settings

- **IKE Phase 1** – Recommended Settings
  - Mode: Main for sites with static IP
  - Encryption Algorithm: **AES-128**, 3DES, DES
  - Authentication Algorithm: **SHA1-128**, MD5
  - DH Keys: Group 2
  - SA Lifetime: 24 hrs (86400 seconds)
  - Peer Authentication: PSK
- **IKE Phase 2** – Recommended Settings
  - Mode: Quick
  - Encryption Algorithm: **NULL/MD5**, AES-128/MD5
  - Authentication Algorithm: MD5
  - DH Group 2
  - SA Lifetime: 8 hrs (28800 seconds)
  - Perfect Forward Secrecy (PFS) : disabled

## 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

**Cloud Enforcement Node Ranges**

Looking for the latest changes? [Changing...](#)

Customers that have implemented private Cloud Enforcement Nodes in their environment: you may need to take into account additional address ranges not represented here. Customers should ensure that access is permitted to data center IP ranges. Allowing access to only specific IP addresses may result in a loss of service.

**Notes**


Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	VPN Host Name	Notes
<b>Africa</b> <a href="#">Copy IP Addresses</a>					
Capetown	196.23.154.64/27	capetown1.sme.zscalerone.net	196.23.154.78	RS	
Johannesburg	196.23.147.192/27	johannesburg1.sme.zscalerone.net	196.23.147.206	johannesburg1-vpn.zscalerone.net	RS
Lagos	197.236.241.224/27	lagos1.sme.zscalerone.net	197.236.241.234	lagos1-vpn.zscalerone.net	RS
<b>Europe</b> <a href="#">Copy IP Addresses</a>					
London W	80.155.80.0/29	london1.sme.zscalerone.net	80.155.80.28	london1-vpn.zscalerone.net	

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


## 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	<pre>crypto ikev1 enable Outside crypto ikev1 policy 1   encryption 3des   authentication pre-share   hash md5   group 2   lifetime 86400 exit</pre>
Link the VPN tunnel with the IKE configuration	<pre>group-policy Zscaler_GRP internal group-policy Zscaler_GRP attributes   vpn-tunnel-protocol ikev1 exit</pre>
Create tunnel group and set the pre-shared key	<pre>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</pre>
Configuring the ACL	<pre>object network flow_traffic   subnet 10.84.0.0 255.255.255.0 access-list Zscaler_map extended permit ip object flow_traffic any</pre>
IPSec configuration	<pre>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</pre>

## 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.

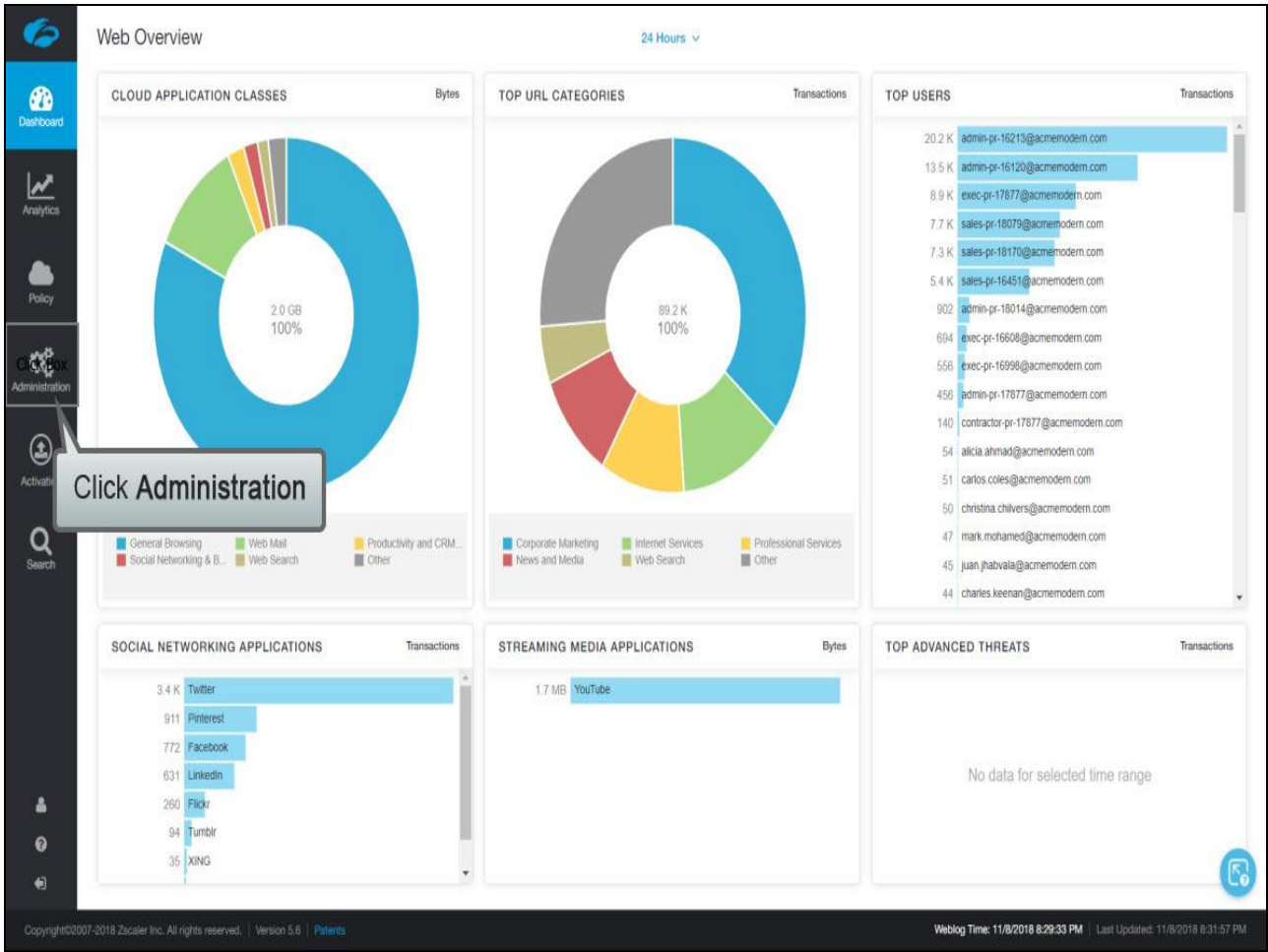
**Slide 15 - Connecting to Zscaler: Interactive Demo**



**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

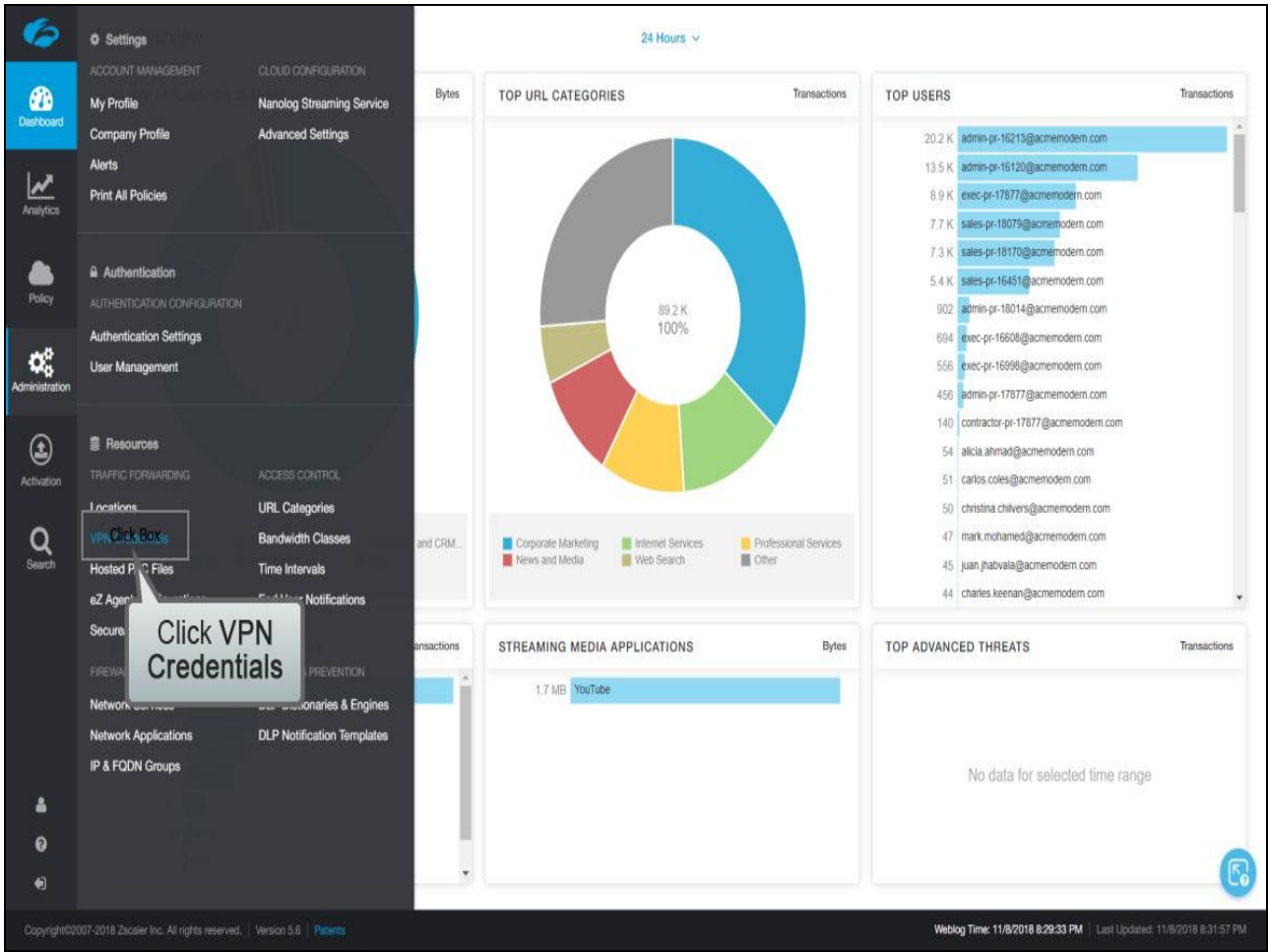


Slide notes

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



Slide 17 - Slide 17



Slide notes

Then **VPN Credentials**.

## Slide 18 - Slide 18

VPN Credentials

[Add VPN Credential](#) [Import VPN Credentials](#) [Sample Import CSV file](#) Authentication Type: All Search...

No.	User/Certificate ID	Authentication Type	Location	Comments
No matching items found				

Click Add VPN Credentials

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents Weblog Time: 11/8/2018 8:23:07 PM Last Updated: 11/8/2018 8:24:15 PM

## Slide notes

Click **Add VPN Credentials**.

## Slide 19 - Slide 19

VPN Credentials

+ Add VPN Credential + Import VPN Credentials Sample Import CSV file

Authentication Type: All Search...

No.	User/Certificate ID	Location	Comments
-----	---------------------	----------	----------

**Add VPN Credential**

VPN CREDENTIAL

Authentication Type

☒ FQDN ☐ XAUTH Click Box

User ID

Click IP

New Pre-Shared Key

Comments

Save Cancel

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

## Slide notes

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

## Slide 20 - Slide 20

The screenshot shows the Zscaler VPN Credentials management interface. The 'Add VPN Credential' modal is open, displaying the 'VPN CREDENTIAL' form. The 'Authentication Type' is set to 'IP'. The 'IP Address' dropdown menu is open, showing 'NONE' as the selected option. A callout box points to the dropdown with the text 'Click in the IP Address field'. The background shows a table of existing credentials with columns for No., User/Certificate ID, Location, and Comments. The footer includes copyright information for Zscaler Inc. and the version number 5.6.

VPN Credentials

+ Add VPN Credential + Import VPN Credentials Sample Import CSV file

Authentication Type: All Search...

No.	User/Certificate ID	Location	Comments
-----	---------------------	----------	----------

**Add VPN Credential**

VPN CREDENTIAL

Authentication Type

FQDN XAUTH **IP**

IP Address

NONE Click Box

New Pre-Shared Key Confirm New Pre-Shared Key

Comments

Save Cancel

Copyright © 2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Privacy Weblog Time: 11/8/2018 8:23:07 PM Last Updated: 11/8/2018 8:24:15 PM

## Slide notes

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

## Slide 21 - Slide 21

The screenshot displays the Zscaler VPN Credentials management interface. A modal dialog titled "Add VPN Credential" is open, allowing the user to configure a new credential. The dialog includes the following sections:

- Authentication Type:** Three radio buttons are present: "FQDN", "XAUTH", and "IP". The "IP" option is selected.
- IP Address:** A dropdown menu is currently set to "NONE". Below it is a search box with the text "Search...". A list of IP addresses is displayed, with "184.170.227.129" highlighted. A callout box points to this entry with the text "Click Box".
- Form New Pre-Shared Key:** A text input field for entering a pre-shared key.
- Comments:** A large text area for adding comments.
- Buttons:** "Save" and "Cancel" buttons are located at the bottom of the dialog.

The background interface shows a table of existing VPN credentials with columns for "No.", "User/Certificate ID", "Authentication Type", "IP Address", "Pre-Shared Key", and "Comments". The footer of the interface contains copyright information: "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Privacy" and system status: "Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM".

## Slide notes

## Slide 22 - Slide 22

The screenshot shows the Zscaler VPN Credentials management interface. A modal window titled "Add VPN Credential" is open, allowing the user to add a new VPN credential. The interface includes a sidebar with navigation options like Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area shows a table of existing credentials and a modal for adding new ones.

**Add VPN Credential**

VPN CREDENTIAL

Authentication Type: ☐ FQDN ☐ XAUTH ☒ IP

IP Address: 184.170.227.129

**Enter a suitable New Pre-Shared Key and confirm**

New Pre-Shared Key:

Confirm New Pre-Shared Key:

Comments:

**Save** **Cancel**

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

Weblog Time: 11/9/2018 8:23:07 PM | Last Updated: 11/9/2018 8:24:15 PM

## Slide notes

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

## Slide 23 - Slide 23

The screenshot shows the 'Add VPN Credential' dialog box in the Zscaler VPN Credentials management interface. The dialog box is titled 'Add VPN Credential' and has a close button (X) in the top right corner. It contains the following fields and options:

- Authentication Type:** Three radio buttons are present: 'FQDN', 'XAUTH', and 'IP'. The 'IP' button is selected.
- IP Address:** A text field containing the value '184.170.227.129'.
- New Pre-Shared Key:** A text field with a red border, containing a masked key (\*\*\*\*\*).
- Confirm New Pre-Shared Key:** A text field with a red border, containing a masked key (\*\*\*\*\*).
- Comments:** A large text area for additional notes.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

A grey callout box with the text 'Enter a suitable New Pre-Shared Key and confirm' is positioned over the key fields. The background interface shows a table with columns 'No.', 'User/Certificate ID', and 'Comments', and a sidebar with navigation icons for Dashboard, Analytics, Policy, Administration, Activation, and Search.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Privacy  
Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

## Slide notes

Then confirm the new pre-shared key.

## Slide 24 - Slide 24

VPN Credentials

+ Add VPN Credential + Import VPN Credentials Sample Import CSV file

Authentication Type: All Search...

No.	User/Certificate ID	Authentication Type	Location	Comments
-----	---------------------	---------------------	----------	----------

**Add VPN Credential**

VPN CREDENTIAL

Authentication Type

☐ FQDN ☐ XAUTH ☒ IP

IP Address

184.170.227.129

New Pre-Shared Key

\*\*\*\*\*

Confirm New Pre-Shared Key

\*\*\*\*\*

Comments

Click Save

Click Save Cancel

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

## Slide notes

Then click **Save**.



Slide 25 - Slide 25

Dashboard

Analytics

Policy

Administration

Activation

Search

VPN Credentials

All changes have been saved.

Add VPN Credential

Import VPN Credentials

Sample Import CSV file

Authentication Type: All

Search...

No.	User/Certificate ID	Authentication Type	Location	Comments	
1	184.170.227.129	IP	---	---	

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

Slide notes

Slide 26 - Slide 26

Dashboard

Analytics

Policy

**Click Box Administration**

Activate

Search

VPN Credentials

Messages have been sent.

Add VPN Credential

Import VPN Credentials

Sample Import CSV file

Authentication Type: All

Search...

No.	User/Certificate ID	Authentication Type	Location	Comments	
1	184.170.227.129	IP	---	---	


Click Administration

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

Slide notes

Slide 27 - Slide 27



Dashboard


Analytics


Policy


Administration

Activation

Search







Settings

ACCOUNT MANAGEMENT

My Profile

Company Profile

Alerts

Print All Policies

Authentication

AUTHENTICATION CONFIGURATION

Authentication Settings

User Management

Identity Proxy Settings

Resources

TRAFFIC FORWARDING

Loc Click Box

VPN Credentials

Hosted P...

eZ Age...

Secure...

FIREWALL FILTERING

Network Services

Network Applications

IP & FQDN Groups

CLOUD CONFIGURATION

Nanolog Streaming Service

Advanced Settings

Virtual ZENS

ICAP Settings

Partner Integrations

ADMINISTRATION CONTROLS

Administrator Management

Role Management

Audit Logs

Backup & Restore

ACCESS CONTROL

URL Categories

Bandwidth Classes

Time Intervals

DATA LOSS PREVENTION

DLP Dictionaries & Engines

DLP Notification Templates

Sample Import CSV file

Authentication Type: All

Search...

Authentication Type	Location	Comments	
IP	Site_1	---	

Click Locations

5.6

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

Weblog Time: 11/8/2018 9:05:17 PM | Last Updated: 11/8/2018 9:05:27 PM

Slide notes

Next, click on **Locations**, ...

## Slide 28 - Slide 28

Locations

LOCATIONS (0) LOCATION GROUPS (0) All Groups ▾

Click Box... Add Location Download... Sample Im... Enter Gro...

Search...

No.	Name	IP Addresses	Proxy Ports	X-Forwards...	Authentication	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	
No matching items found											

Click Add Location

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

## Slide notes

...click **Add Location**, ...

## Slide 29 - Slide 29

**Add Location**

**LOCATION**

Name:

Country:

State/Province:

Time Zone:

Group:

**ADDRESSING**

Static IP Addresses:

Proxy Ports:

Virtual ZENS:

VPN Credentials:

Virtual ZEN Clusters:

**GATEWAY OPTIONS**

Enable XFF Forwarding: ☐ ☒

Enable AUP: ☐ ☒

Enforce Authentication: ☐ ☒

Save Cancel

Configure LOCATION information as necessary

## Slide notes

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

## Slide 30 - Slide 30

**Add Location**

**LOCATION**

Name: Site\_1

State/Province:

Group: None

Country: NONE

Country dropdown options: United Arab Emirates, United Kingdom, United States, United States Minor Outlying Islands

**ADDRESSING**

Static IP Addresses: None

Proxy Ports: None

Virtual ZENS: None

VPN Credentials: None

Virtual ZEN Clusters: None

**GATEWAY OPTIONS**

Enable XFF Forwarding: ☐ X

Enable AUP: ☐ X

Enforce Authentication: ☐ X

Buttons: Save, Cancel

Callout: Configure LOCATION information as necessary

## Slide notes

## Slide 31 - Slide 31

**Locations**

LOCATIONS (0)

+ Add Location...

No. Name

**Add Location**

**LOCATION**

Name: Site\_1

Country: United States

State/Province: CA

Time Zone: NONE

Group: None

**ADDRESSING**

Static IP Addresses: None

Click Box

Click in the Static IP Addresses field

Configure LOCATION information as necessary

Proxy Ports: None

VPN Credentials: None

Virtual ZEN: None

Virtual ZEN Clusters: None

**GATEWAY OPTIONS**

Enable XFF Forwarding: ☐

Enforce Authentication: ☐

Enable AUP: ☐

Save Cancel

## Slide notes

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

## Slide 32 - Slide 32

**Add Location**

**LOCATION**

Name: Site\_1

Country: United States

State/Province: CA

Time Zone: America/Los Angeles

Group: None

**ADDRESSING**

Static IP Addresses: None

Unselected Items	Selected Items (0)
Search...	

Click to select the correct IP Address

Done Cancel Clear Selection

Save Cancel

## Slide notes



## Slide 33 - Slide 33

**Add Location**

**LOCATION**

Name: Site\_1

Country: United States

State/Province: CA

Time Zone: America/Los Angeles

Group: None

**ADDRESSING**

Static IP Addresses

None

Unselected Items	Selected Items (1)
Search...	184.170.227.129
<input checked="" type="checkbox"/> 184.170.227.129	

Click Done

Click Box Cancel Clear Selection

Save Cancel

Secondary Destination Internal ...

172.17.20.52 - 172.17.20.55

Export

## Slide notes

Then click **Done**.

## Slide 34 - Slide 34

**Locations**

LOCATIONS (0)

+ Add Location

No. Name

**Add Location**

**LOCATION**

Name: Site\_1

Country: United States

State/Province: CA

Time Zone: America/Los Angeles

Group: None

**ADDRESSING**

Static IP Addresses: 184.170.227.129

Proxy Ports: None

VPN Credentials: None

**GRE Tunnel Information**

No.	Tunnel Source...	Primary Desti...	Secondary D...	Primary Destination Internal Ra...	Secondary Destination Internal ...
1	184.170.227.129	199.168.151.8	197.156.241.234	172.17.20.48 - 172.17.20.51	172.17.20.52 - 172.17.20.55

Virtual ZENS: None

Virtual ZEN Clusters: None

**GATEWAY OPTIONS**

Save Cancel

Click in the VPN Credentials field

Click Box

## Slide notes

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

## Slide 35 - Slide 35

**Locations**

LOCATIONS (0)

+ Add Location

No. Name

**Add Location**

**LOCATION**

Name: Site\_1

Country: United States

State/Province: CA

Time Zone: America/Los Angeles

Group: None

**ADDRESSING**

Static IP Addresses: 184.170.227.129

Proxy Ports: None

VPN Credentials: None

**GRE Tunnel Information**

No.	Tunnel Source...	Primary Desti...	Secondary D...	Pre...
1	184.170.227.129	199.168.151.8	197.156.241.234	184.170.227.129

Virtual ZENS: None

**GATEWAY OPTIONS**

Save Cancel

**Unselected Items** | **Selected Items (0)**

Search...

Click Box

Click to select the correct VPN Credentials

Done Cancel Clear Selection

## Slide notes

...and select the IP address of the site.

## Slide 36 - Slide 36

**Add Location**

**LOCATION**

Name: Site\_1

Country: United States

State/Province: CA

Time Zone: America/Los Angeles

Group: None

**ADDRESSING**

Static IP Addresses: 184.170.227.129

Proxy Ports: None

VPN Credentials: None

**GRE Tunnel Information**

No.	Tunnel Source...	Primary Desti...	Secondary D...	P...
1	184.170.227.129	199.168.151.8	197.156.241.234	17

Virtual ZENS: None

**GATEWAY OPTIONS**

Save Cancel

**Unselected Items**

Search...

184.170.227.129

**Selected Items (1)**

184.170.227.129

Click Done

Click Box Cancel Clear Selection

## Slide notes

Then click **Done**, ...

Slide 37 - Slide 37

Locations

LOCATIONS (0)

Add Locati...

Dashboard

Analytics

Policy

Administration

Activation

Search

Locations

LOCATIONS (0)

Add Locati...

No.

Name

Add Location

LOCATION

Name

Site\_1

Country

United States

State/Province

CA

Time Zone

America/Los Angeles

Group

None

ADDRESSING

Static IP Addresses

184.170.227.129

Proxy Ports

None

VPN Credentials

184.170.227.129

GRE Tunnel Information

No.

Tunnel Sourc...

Primary Desti...

Secondary D...

Primary Destination Internal Ra...

Secondary Destination Internal ...

1

184.170.227.129

199.168.151.8

197.156.241.234

172.17.20.48 - 172.17.20.51

172.17.20.52 - 172.17.20.55

Virtual ZENS

None

Virtual ZEN Clusters

None

GATEWAY OPTIONS

Save

Cancel

Scroll down...

Slide notes

Page 37 of 48

## Slide 38 - Slide 38

**Add Location**

184.170.227.129

Proxy Ports: None

VPN Credentials: 184.170.227.129

GRE Tunnel Information

No.	Tunnel Sourc...	Primary Desti...	Secondary D...	Primary Destination Internal Ra...	Secondary Destination Internal ...
1	184.170.227.129	199.168.151.8	197.156.241.234	172.17.20.48 - 172.17.20.51	172.17.20.52 - 172.17.20.55

Virtual ZENS: None

Virtual ZEN Clusters: None

**GATEWAY OPTIONS**

Enable XFF Forwarding: ☐

Enable AUP: ☐

Enable SSL Scanning: ☐

Enforce Authentication: ☐

Enforce Firewall Control: ☐

**BANDWIDTH CONTROL**

Enforce B...: ☐

**Click Save**

Click Box Cancel

## Slide notes

...and then **Save**.

Slide 39 - Slide 39

Dashboard

Analytics

Policy

Administration

Activation

Search

Locations

All changes have been saved.

LOCATIONS (1)

LOCATION GROUPS (0)

All Groups

Add Locati...

Import Lo...

Download...

Sample Im...

Enter Gro...

Filter

Export

Search...

No.	Name	IP Addresses	Proxy Ports	X-Forward...	Authenticat...	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	
1	Site_1	184.170.227.129	---	---	---	---	---	---	---	---	

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

Slide notes

## Slide 40 - Slide 40

The screenshot shows the Zscaler Administration console interface. The left sidebar contains navigation icons for Dashboard, Analytics, Policy, Administration, and Activation. The Activation icon is highlighted with a red notification badge and a callout box that says "Click Activation". The main content area displays the "Locations" page, which includes a table of locations and a "LOCATION GROUPS" tab. The table has columns for No., Name, IP Addresses, Proxy Ports, X-Forwarded, Authentication, SSL, Firewall Filter, Bandwidth, Virtual ZENS, and Group. A single location, "Site\_1", is listed with IP addresses 184.170.227.129. The footer of the console shows copyright information for Zscaler Inc. and the version number 5.6.

No.	Name	IP Addresses	Proxy Ports	X-Forwarded	Authentication	SSL	Firewall Filter	Bandwidth	Virtual ZENS	Group
1	Site_1	184.170.227.129	---	---	---	---	---	---	---	---

## Slide notes

Then **Activate** your changes...



Slide 41 - Slide 41

MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

admin@bushneg1.zscaler.com

QUEUED ACTIVATIONS (0)

None

☐ Force Activate

Click Box

Dashboard

Analytics

Policy

Administration

Activation

Search

Groups (0)

All Groups

Download... Sample Im... Enter Gro...

Search...

IP Addresses	Proxy Ports	X-Forward...	Authenticat...	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	
184.170.227.129	---	---	---	---	---	---	---	---	

Click Activate

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

Slide notes

Slide 42 - Slide 42

Dashboard

Analytics

Policy

Administration

Activation

Search

Locations

Activation Completed!

LOCATIONS (1)

LOCATION GROUPS (0)

All Groups

Add Locati...

Import Lo...

Download...

Sample Im...

Enter Gro...

Filter

Export

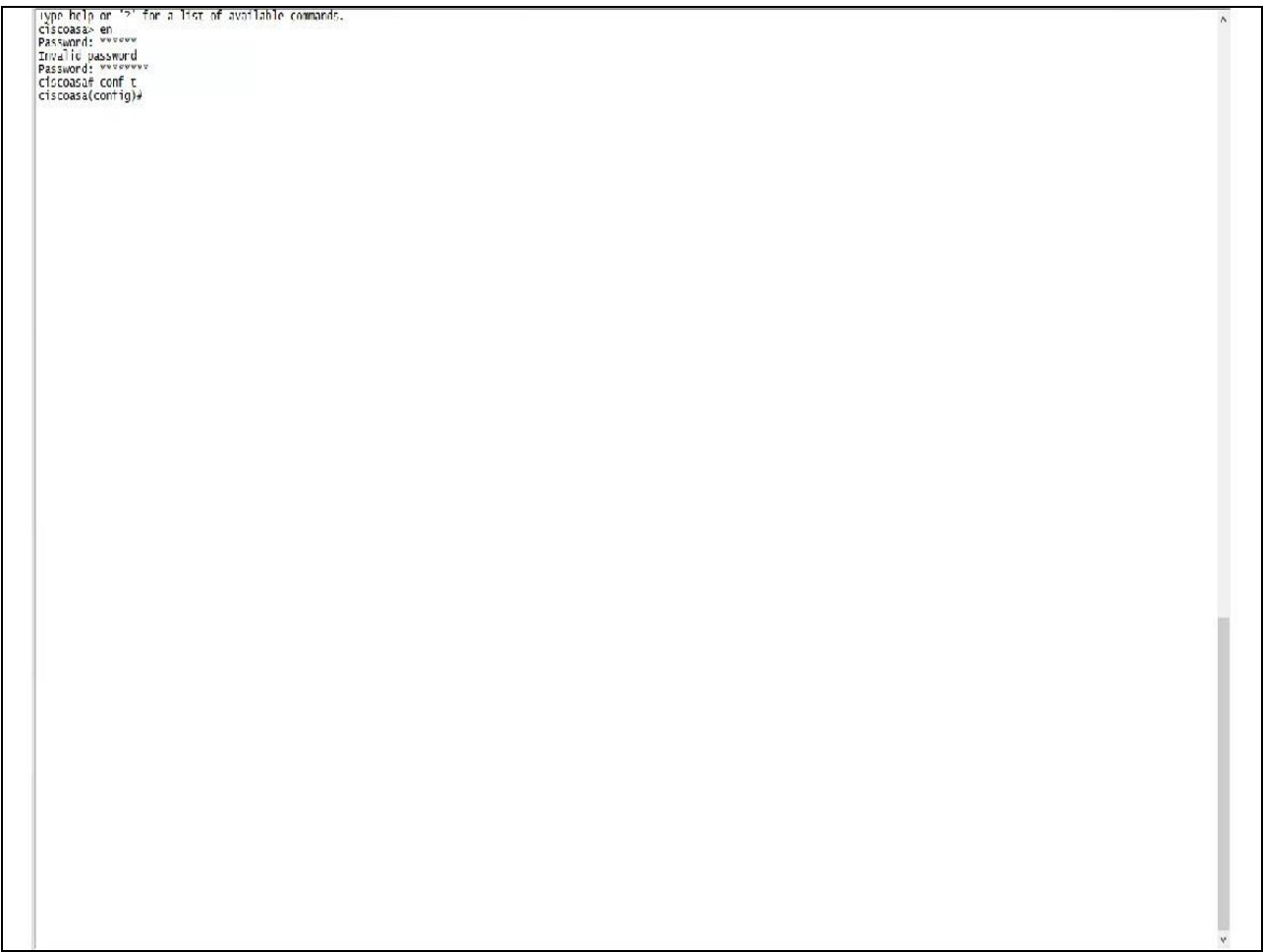
Search...

No.	Name	IP Addresses	Proxy Ports	X-Forward...	Authenticat...	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	
1	Site_1	184.170.227.129	---	---	---	---	---	---	---	---	

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

Weblog Time: 11/8/2018 8:23:07 PM | Last Updated: 11/8/2018 8:24:15 PM

Slide notes

**Slide 43 - Slide 43**A screenshot of a Cisco ASA command-line interface. The text shows the user entering 'en' to enter enable mode, followed by a password prompt 'Password: ' where 'ciscoasa' is entered. Then, the user enters 'conf t' to enter configuration mode, and the prompt changes to 'ciscoasa(config)#'.

```
type help or '?' for a list of available commands.  
ciscoasa> en  
Password: ciscoasa  
Invalid password  
Password: ciscoasa  
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: *****
Invalidate 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 104.120.192.35 type ipsec-l2l
ciscoasa(config)# tunnel-group 104.120.192.35 general-attributes
ciscoasa(config-tunnel-general)# default-group-policy Zscaler_GRP
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)# tunnel-group 104.120.192.35 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

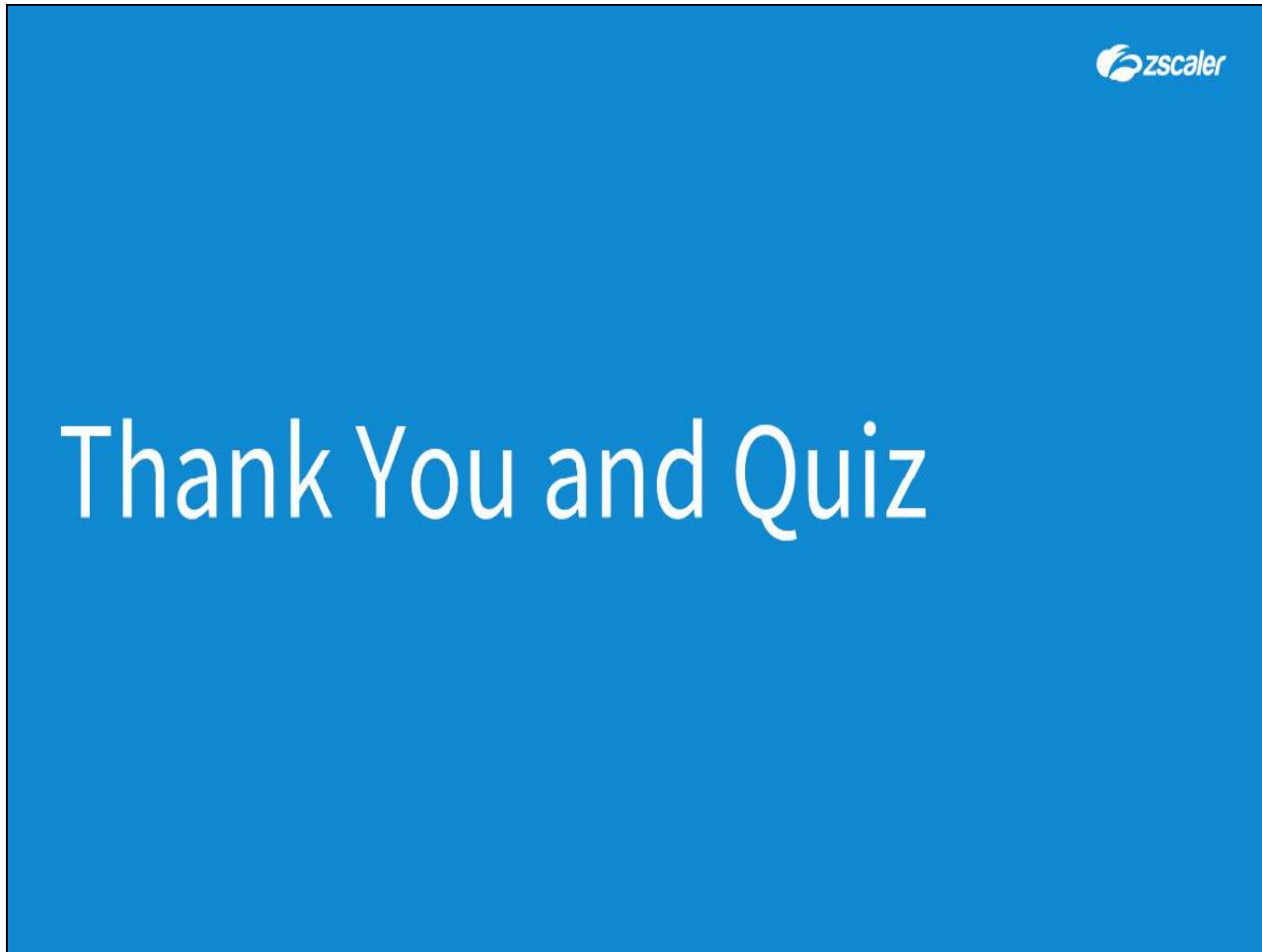
Configure the ACL to forward traffic into the tunnel.

## 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 104.120.192.35 type ipsec-l2l
ciscoasa(config)# tunnel-group 104.120.192.35 general-attributes
ciscoasa(config-tunnel-general)# default-group-policy ZScaler_GRP
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)# tunnel-group 104.124.192.35 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.