

**Slide 1 - Traffic Forwarding**



# ZCCA-IA

## Traffic Forwarding Overview

©2018 Zscaler, Inc. All rights reserved.

**Slide notes**

Welcome to the Traffic Forwarding Module.

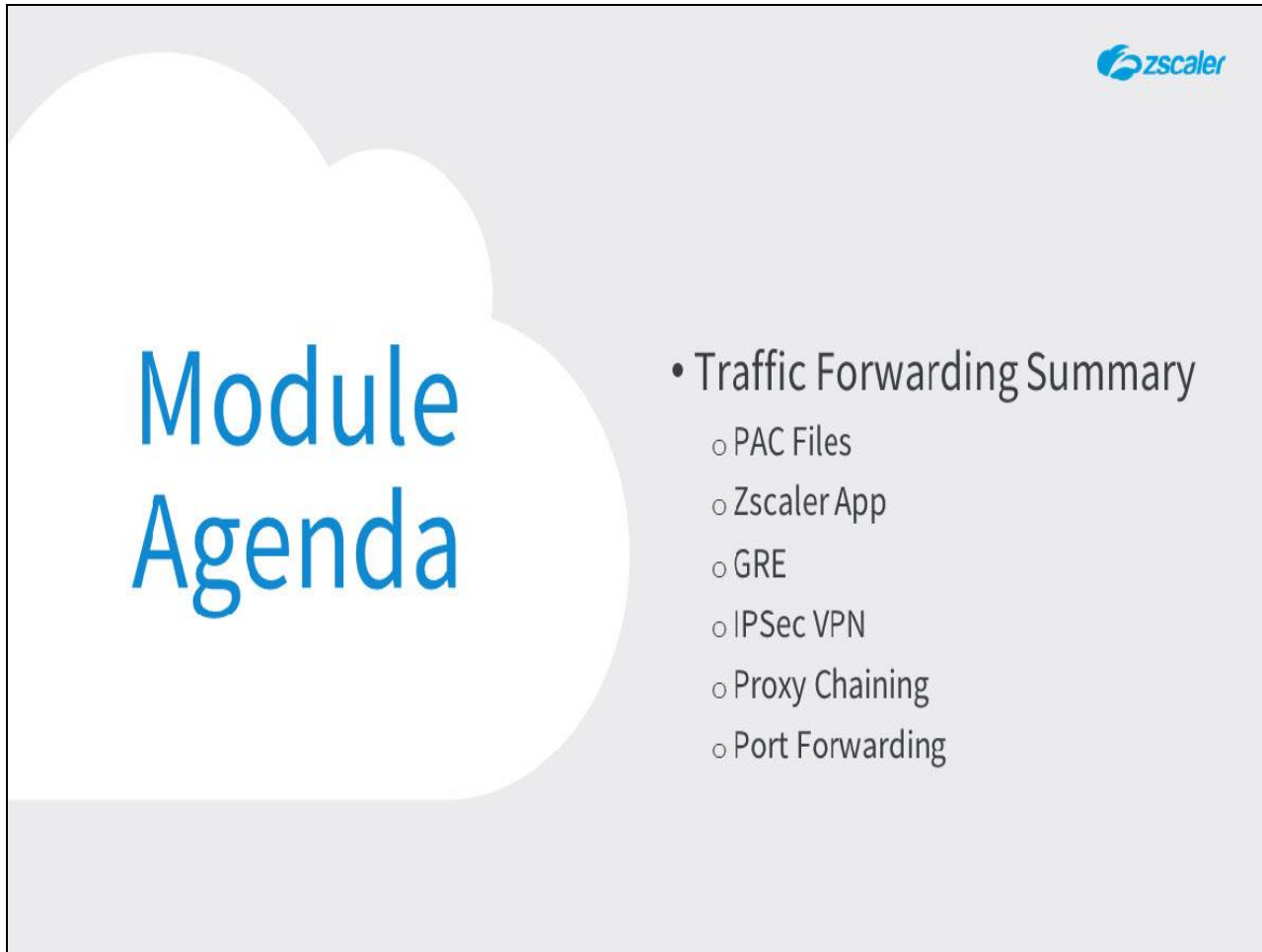
## Slide 2 - Navigating the eLearning Module

## Navigating the eLearning Module

The screenshot displays the Zscaler Cloud Portal dashboard. The dashboard includes sections for Cloud Application Classes, Top URL Categories, Top Users, Streaming Media Applications, and Top Advanced Threats. Overlaid on the dashboard are several blue callout boxes with white text, each pointing to a specific control on the video player interface. The controls include: 'Exit' (top right), 'Previous Slide' (left), 'Next Slide' (right), 'Play/Pause' (bottom left), 'Fast Forward' (bottom center), 'Progress Bar' (bottom center), 'Audio On/Off' (bottom right), and 'Closed Captioning' (bottom right). The Zscaler logo is visible in the top right corner of the dashboard.

**Slide notes**

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and 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 if you wish to exit.

**Slide 3 - Module Agenda**


The slide features a light gray background with a large white cloud shape on the left. Inside the cloud, the text "Module Agenda" is written in a large, blue, sans-serif font. To the right of the cloud, a bulleted list of topics is displayed. In the top right corner, the Zscaler logo is visible.

- Traffic Forwarding Summary
  - PAC Files
  - Zscaler App
  - GRE
  - IPSec VPN
  - Proxy Chaining
  - Port Forwarding


**Slide notes**







In this module we will cover a summary of Traffic Forwarding Methods including: PAC Files, Zscaler App, GRE Tunnel, IPSec VPN, Proxy Chaining, and Port Forwarding

## Slide 4 - Forwarding Methods Summary



## Forwarding Methods Summary

 = Possible but not recommended

User Type	GRE	IPSEC VPN	PAC File	Proxy Chain	Limited support Port Forward	Mobility platforms Secure Agent	Zscaler App
Main Office	✓	✓	✓	✓			
Small Office	✓	✓	✓				✓
Laptop			✓				✓
Desktop (home office)			✓				✓
Mobile IOS			✓			Deprecated	✓
Mobile Android			✓			Deprecated	✓

## Slide notes

This table shows the various methods to forward traffic to the Zscaler cloud. The green tick or check mark means that the combination of user or site and forwarding method is fully supported. The warning sign means that the combination of user or site and forwarding method, while technically possible, is not recommended for long-term production. For instance:

- Office locations can use GRE, IPSEC VPN, and PAC files or Zscaler App;
- Roaming users and home office users, should only use PAC files or Zscaler App.

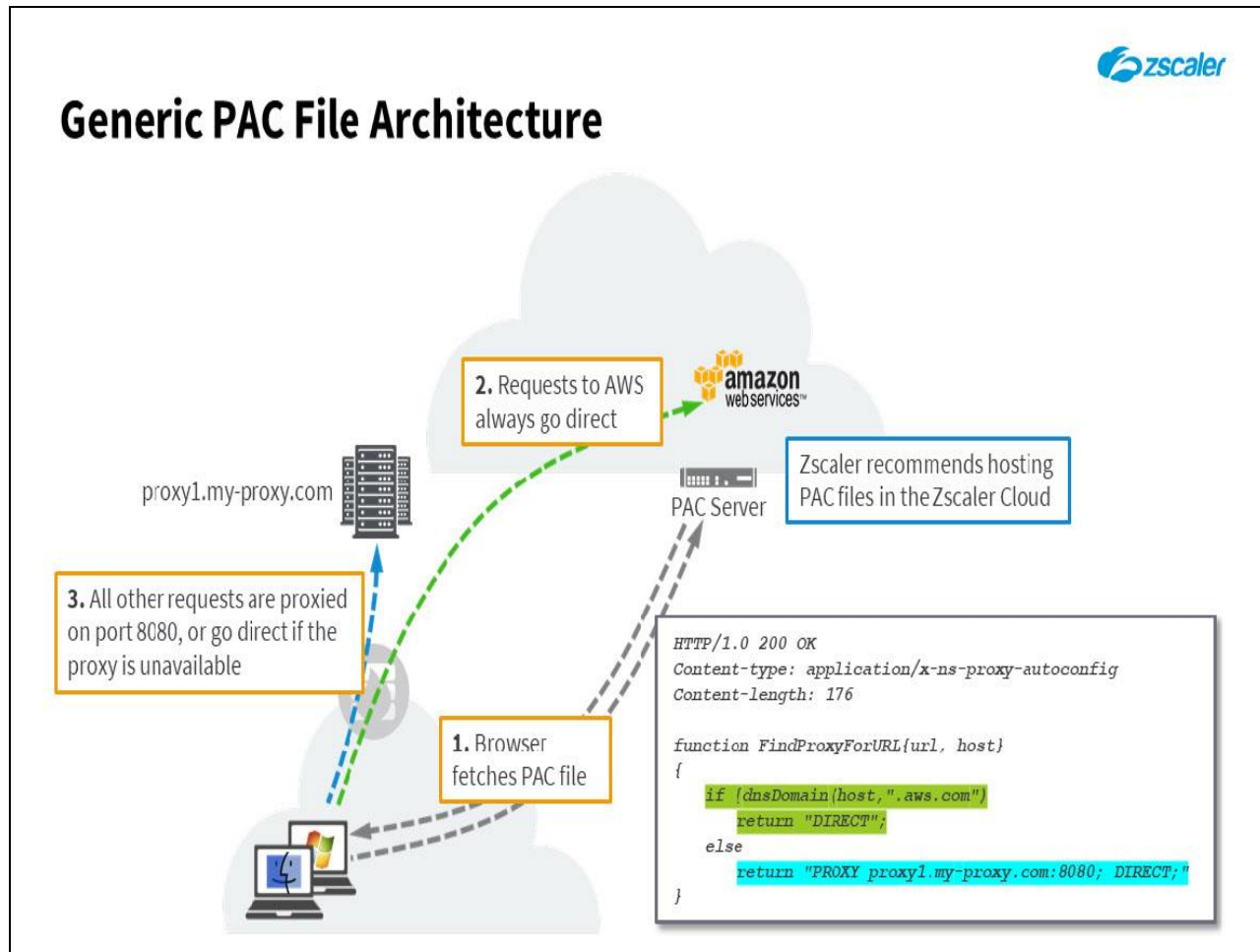
Proxy chaining involves forwarding traffic from one proxy server to another. This method leverages your existing proxy servers, with no additional changes to the network. It's a quick and easy way to forward your traffic to the Zscaler service for evaluation purposes and to add an additional layer of security to your network.

Although Zscaler supports proxy chaining, it is not recommended as a long-term solution in production environments. Multiple proxies add latency and depending on the proxy server used the options for redundant failover may be limited.

Port forwarding should only be used during the POC phase or initial roll out. It should not be used as long-term production methods as failover methods are limited.

The Zscaler App automatically creates a lightweight HTTP tunnel that connects the user's endpoint to Zscaler's cloud security platform with no need for PAC files or authentication cookies. The Zscaler Cloud Service delivers one-step enrollment, with multi-factor authentication support via SAML. Currently, the Z-App supports Windows and Mac OS X with support for Android and iOS.

## Slide 5 - Generic PAC File Architecture




## Slide notes

The PAC file is the only fully supported traffic forwarding method for roaming users and one of the most common for offices. The PAC file is, simply put, a java script, which instructs the browser to which proxy to connect, over which TCP port, etc. It can also instruct the browser to bypass the proxy for selected destinations or protocols.

Ideally, the customer hosts the PAC file on the PAC server in the Zscaler cloud. There are key features, such as precise geo-IP proxy configuration, which are only available when the PAC file resides on the Zscaler PAC server. The only caveat for hosting the PAC file in the Zscaler cloud, is to ensure that the firewall allows individual devices to connect to the PAC server and download the PAC file.

## Slide 6 - Zscaler Default PAC File



## Zscaler Default PAC File

```

function FindProxyForURL(url, host) {
    var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-9]|172\.3[01]|169\.254|192\.88\.99)\.([0-9.]+)$/;
    var resolved_ip = dnsResolve(host);

    /* Don't send non-FQDN or private IP auths to us */
    if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0", "255.255.255.0") ||
        privateIP.test(resolved_ip))
        return "DIRECT";

    /* FTP goes directly */
    if (url.substring(0,4) == "ftp:")
        return "DIRECT";

    /* Updates are directly accessible */
    if (((localHostOrDomainIs(host, "trust.zscaler.com")) ||
        (localHostOrDomainIs(host, "trust.zscaler.net")) ||
        (localHostOrDomainIs(host, "trust.zscalerone.net")) ||
        (localHostOrDomainIs(host, "trust.zscalertwo.net")) ||
        (localHostOrDomainIs(host, "trust.zscloud.net")) ) &&
        (url.substring(0,5) == "http:" || url.substring(0,6) == "https:"))
        return "DIRECT";

    /* Default Traffic Forwarding Forwarding to Zen port 80 but you can use port 9400 also */
    return "PROXY ${GATEWAY}:80 PROXY ${SECONDARY_GATEWAY}:80 DIRECT";
}

```

1
2
3

## Slide notes

This slide shows the default Zscaler PAC file. Each customer can create their own PAC file and host under their own profile in the Zscaler cloud. The most significant advantage of hosting the PAC file in the Zscaler cloud is the availability of the variables `${GATEWAY}` and `${SECONDARY_GATEWAY}`.

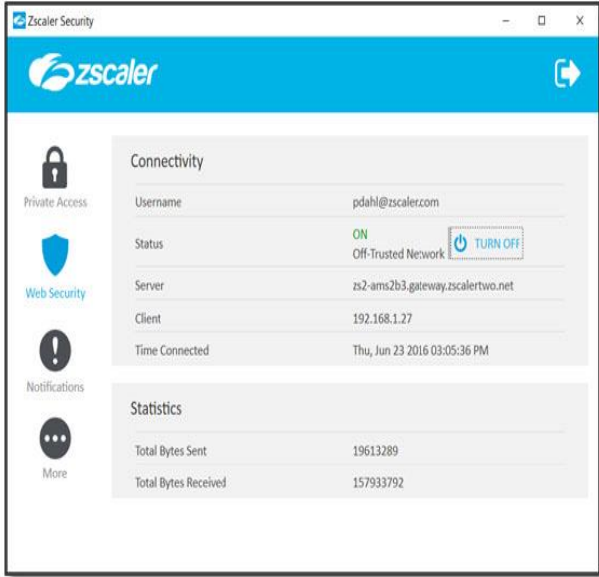
These variables tell the PAC server to insert the IP addresses of the closest ZENs based on the user's IP address. This PAC file is meaningless outside the context of the pac server. When the browser requests the PAC file from the pac server, the server substitutes the variables with the IP address of the geographically closest ZEN.

This determination is done based on the egress IP address of the client making the request. The key word `DIRECT` instructs the browser to connect directly to the Internet if both primary and secondary ZEN are unavailable.

**Slide 7 - Zscaler App – One App to Connect Them All**

## Zscaler App – One App to Connect Them All

- Free client SW for:
  - Secure Internet access (ZIA)
  - Connectivity to private applications (ZPA)
- Features:
  - Silent install options
  - One step end user enrollment
  - Enroll on up to 16 devices
  - Enforcement before enrollment
  - Privacy control for GDPR compliance
  - Installers for Windows, Mac, iOS, and Android
  - LWF driver for Windows



**Slide notes**

The Zscaler App, available at no additional charge, provides another method for forwarding traffic to The Zscaler Cloud to allow the enforcement of Zscaler Internet Security; one that is particularly well suited for your road warriors. The Zscaler App can be used both to scan and protect data sent to the Internet at large using the Zscaler Internet Access service (ZIA), and to provide access to private applications in your own Data Centers, or hosted in a private Cloud, using Zscaler Private Access (ZPA).


Some features of the app are:

- You can push it for silent install on PCs and mobile devices;
- There is a one-step enrollment process with the authentication method of your choice (SAML recommended), and on-going user verification using a device fingerprint captured during enrollment;
- The number of devices a user can enroll is configurable up to a maximum of 16;
- You have the ability to block access to the Internet before the user enrolls into the app;
- The collection of device owner information can be disabled, for compliance with GDPR requirements;



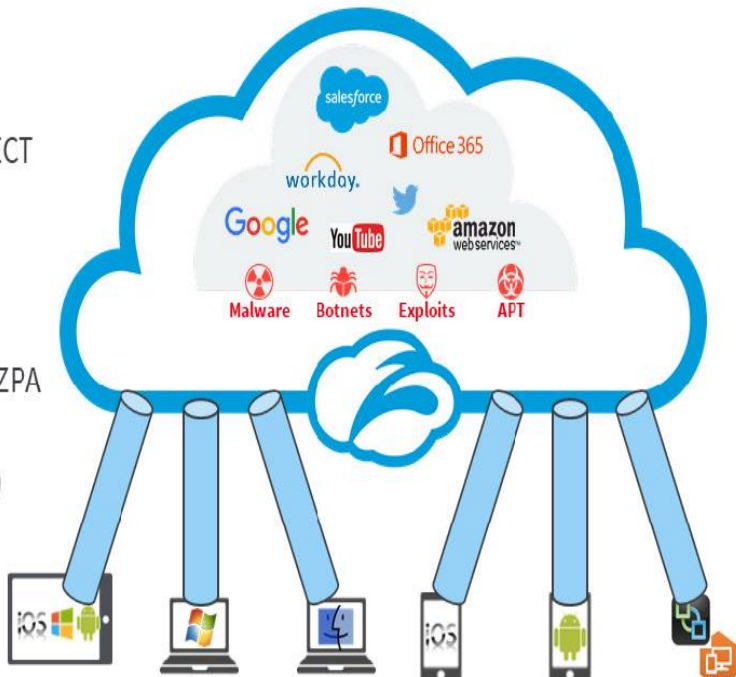
- Support for Windows and Mac PCs and mobile devices (iOS and Android), the app install file for PCs and Android is available for download from the Zscaler App Portal, and the mobile installers are available on the relevant public App Stores;
- A Lightweight Filter driver is available for Windows for better performance, enforcement and interoperability, and to allow packet captures.

## Slide 8 - Zscaler App – One App to Connect Them All



## Zscaler App – One App to Connect Them All

- Internet access capabilities (ZIA)
  - Configurable forwarding options
  - Optional lightweight HTTP CONNECT tunnels to Zscaler proxies
  - Custom PAC file options
- Private access capabilities (ZPA)
  - Secure Z tunnels/Microtunnels to ZPA infrastructure
  - Bring Your Own Encryption (BYOE) option
- Co-existence with VPN Clients
  - Full or split tunnel options




## Slide notes

For Internet access, the Zscaler App provides a number of forwarding options, including the ability to establish lightweight, unencrypted HTTP CONNECT tunnels to a local ZEN on the Zscaler Internet Access (ZIA) Cloud, or it can be configured simply to enforce a specified PAC file. You also have the option to specify a custom App configuration PAC file to identify one or more ZENs to send traffic to, or to specify destinations to be bypassed by the app.

For access to private resources, the app will establish TLS encrypted Z tunnels to the ZPA Cloud infrastructure, to allow end-to-end Microtunnels to the ZEN Connector virtual machines installed adjacent to the private applications. The option is available to also encrypt the Microtunnels using customer generated PKI, which gives the Zscaler infrastructure no possibility whatsoever to intercept or decrypt user traffic (the Bring Your Own Encryption (BYOE) option).

The Zscaler App can co-exist with popular VPN software on the client device, to allow either full or split-tunnel VPN configurations.

## Slide 9 - GRE Requirements



## GRE Requirements

- Static Routable IP
  - Notify Zscaler support of the IP and its geographic location
  - Support will give you the ZEN IP addresses and GRE parameters
- Compatible Device
  - Cisco Router (not available on ASA – use IPSec VPN instead)
  - Juniper
  - Fortinet
  - Vyatta
  - Many others

**Note:** If you are behind a NAT you will need 2 static IPs, one will be used as the Router's loopback address

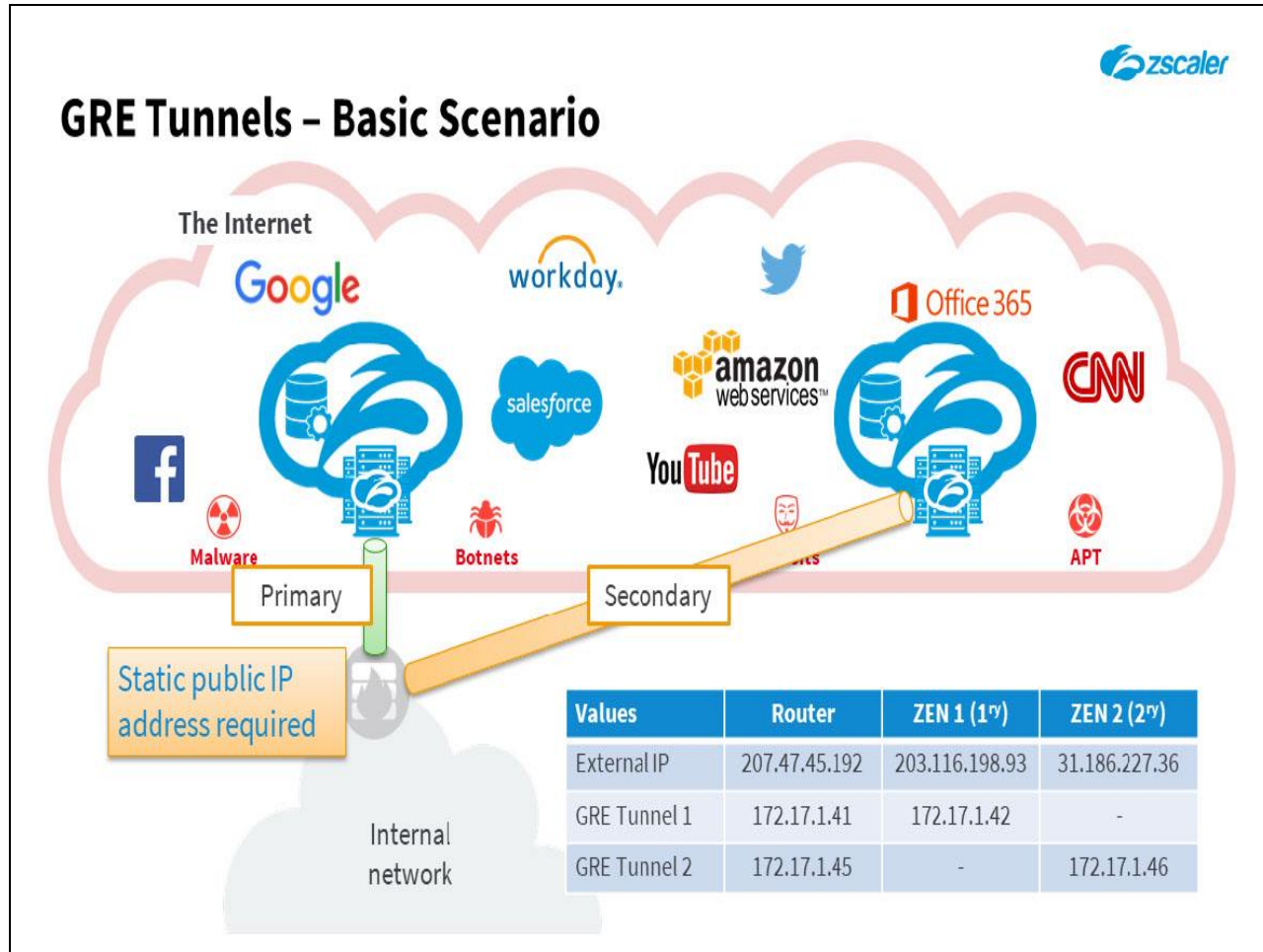
## Slide notes

Establishing a GRE tunnel between an edge device is the most common traffic forwarding method for offices. There are two key requirements for using GRE tunnels.

- 1) The edge device must have a static and routable IP address, uniquely assigned to the customer. For instance, most DSL or cable connections do not offer a static IP address. The fact that your IP has not changed in a long time does not qualify it as static IP. If the GRE device is behind a firewall, which performs NAT, you need to have two static and routable IP addresses allocated for that location.
- 2) You need to have a compatible edge device. The list of GRE enabled devices is long; if you have any Cisco (with the exception of ASA or PIX firewalls), or most Juniper, Fortinet devices, you can use GRE tunnels.

If you meet both requirements, you need to contact Zscaler support and have them associate the IP addresses to your account and enable them for GRE. This is a manual process that can only be achieved by contacting support. You should open a ticket from the administrative interface and request this operation to be done.

## Slide 10 - GRE Tunnels – Basic Scenario



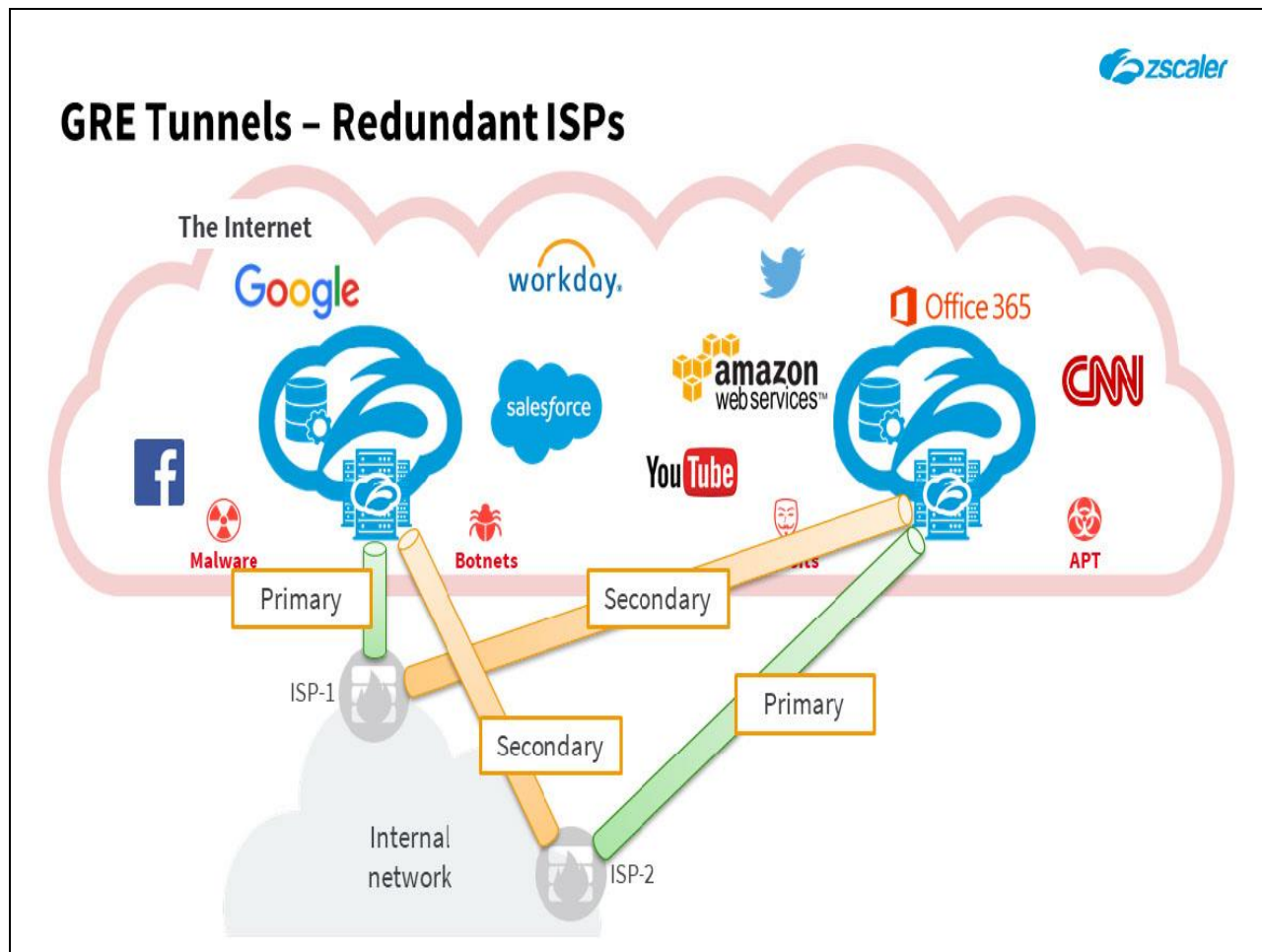
## Slide notes

This diagram shows the most basic GRE scenario. The GRE capable router is outside the firewall. The static and routable IP address of the device is 207.47.45.194. When you log in to the administrative interface and create a new location for this IP address, you see the remaining pieces of information needed to set up the tunnel.

Zscaler technical support loads this information in the backend then provisions your IP address for GRE access. Each of your locations ( or IP addresses) can connect up to two separate ZENs for GRE. In this case, you can connect to ZENs with IP addresses 203.116.198.93 and 31.186.227.36. From the point of view of your router, there are two GRE tunnels. Each tunnel also has an internal IP address schema.

- The first GRE Tunnel goes from IP 207.47.45.192 to IP address 203.116.198.93. The near end tunnel IP address is 172.17.1.41, the far end tunnel IP address is 172.17.1.42.
- The second GRE Tunnel goes from IP 207.47.45.192 to IP address 31.186.227.36. The near end tunnel IP address is 172.17.1.45, the far end tunnel IP address is 172.17.1.46. The final step would be to configure your edge device to send all internet-bound traffic through the GRE tunnels.

## Slide 11 - GRE Tunnels – Redundant ISPs

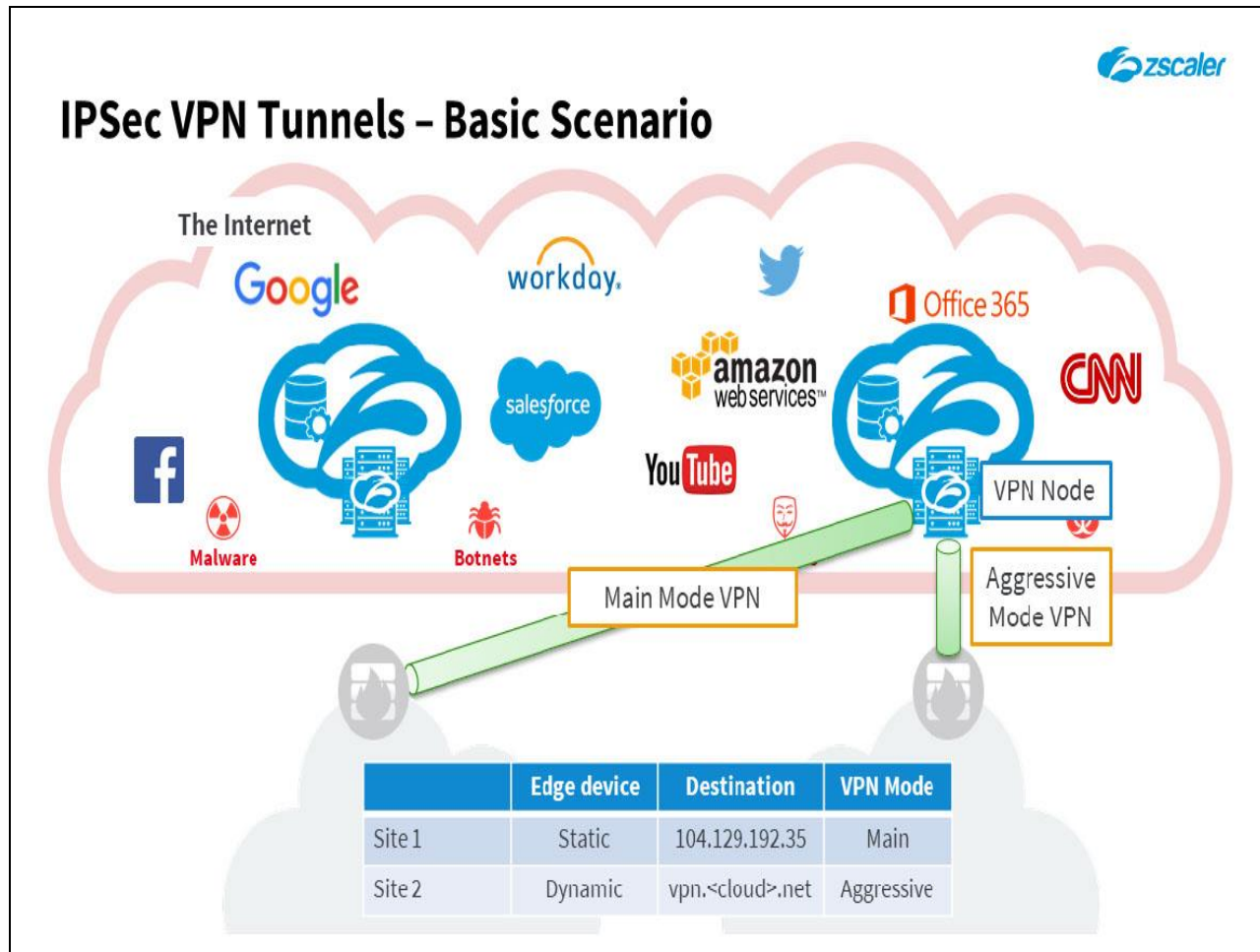


## Slide notes

Larger sites may have more than one egress point. From the Zscaler point of view, you can have many egress points. They can point to the same ZEN or to separate ZENs. That is immaterial. Zscaler sees the connection from one routable IP address to a ZEN pair. The configuration is the same as in the previous case.

You just need to create additional locations, register the IP addresses with Zscaler technical support, and configure your internal routing to get the traffic to the ZENs in whatever priority you wish.

## Slide 12 - IPSec VPN Tunnels – Basic Scenario

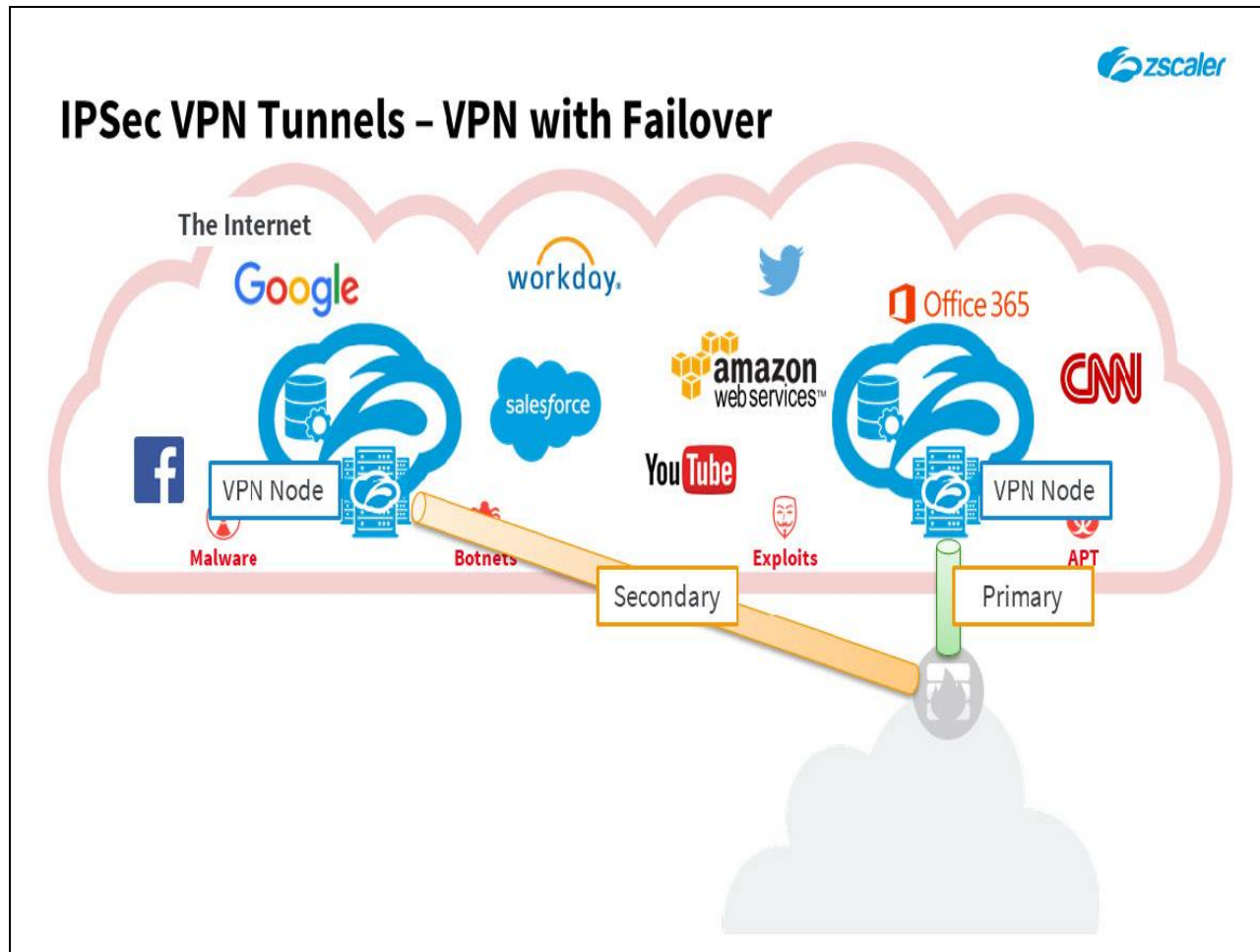
**Slide notes**

IPSEC VPN represents another common deployment scenario for offices. Zscaler supports aggressive mode and main mode VPN access. In order to use main mode VPN, you need to have a static and routable IP address associated to your VPN edge device.

You need to contact technical support and open a ticket via the administrative interface to have the IP address provisioned to your account, similar to GRE. If your site is using dynamic IP addressing and your edge device supports it you can use aggressive mode. This does not require you to have support provision your IP address in the system.



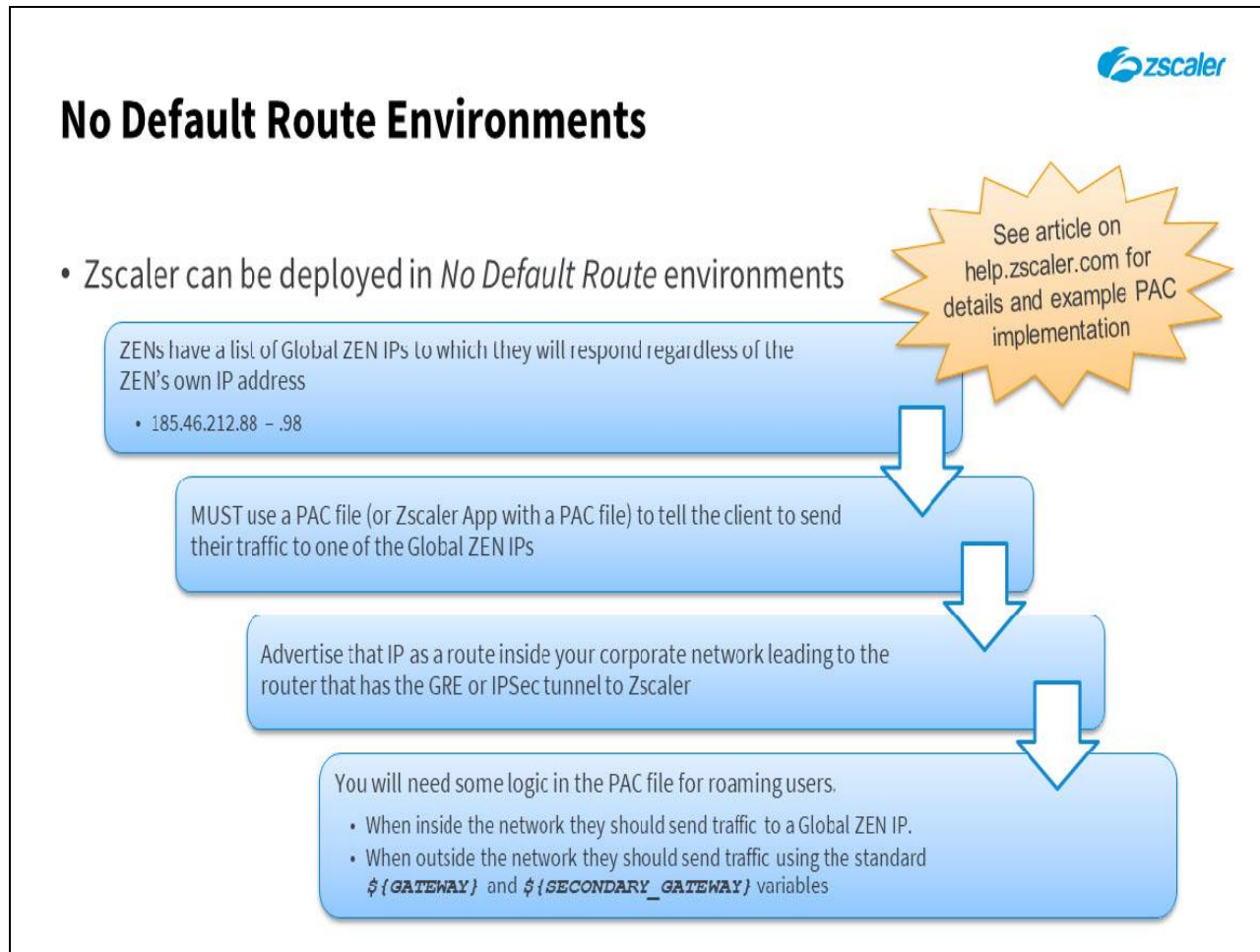
## Slide 13 - IPSec VPN Tunnels - VPN with Failover



## Slide notes

You should always configure your VPN device with at least two tunnels for fault tolerance. You can have more than two tunnels, for example, if you have multiple Internet connections at a location.

## Slide 14 - No Default Route Environments



## Slide notes

Before we leave tunnels, a quick note on No Default Route networks. Most Zscaler deployments with tunnels use a default route to send traffic to the router that has an active tunnel to Zscaler. This makes the deployment transparent to users. Internet-bound traffic simply follows the default route to Zscaler. However, some networks are set up with no default route.

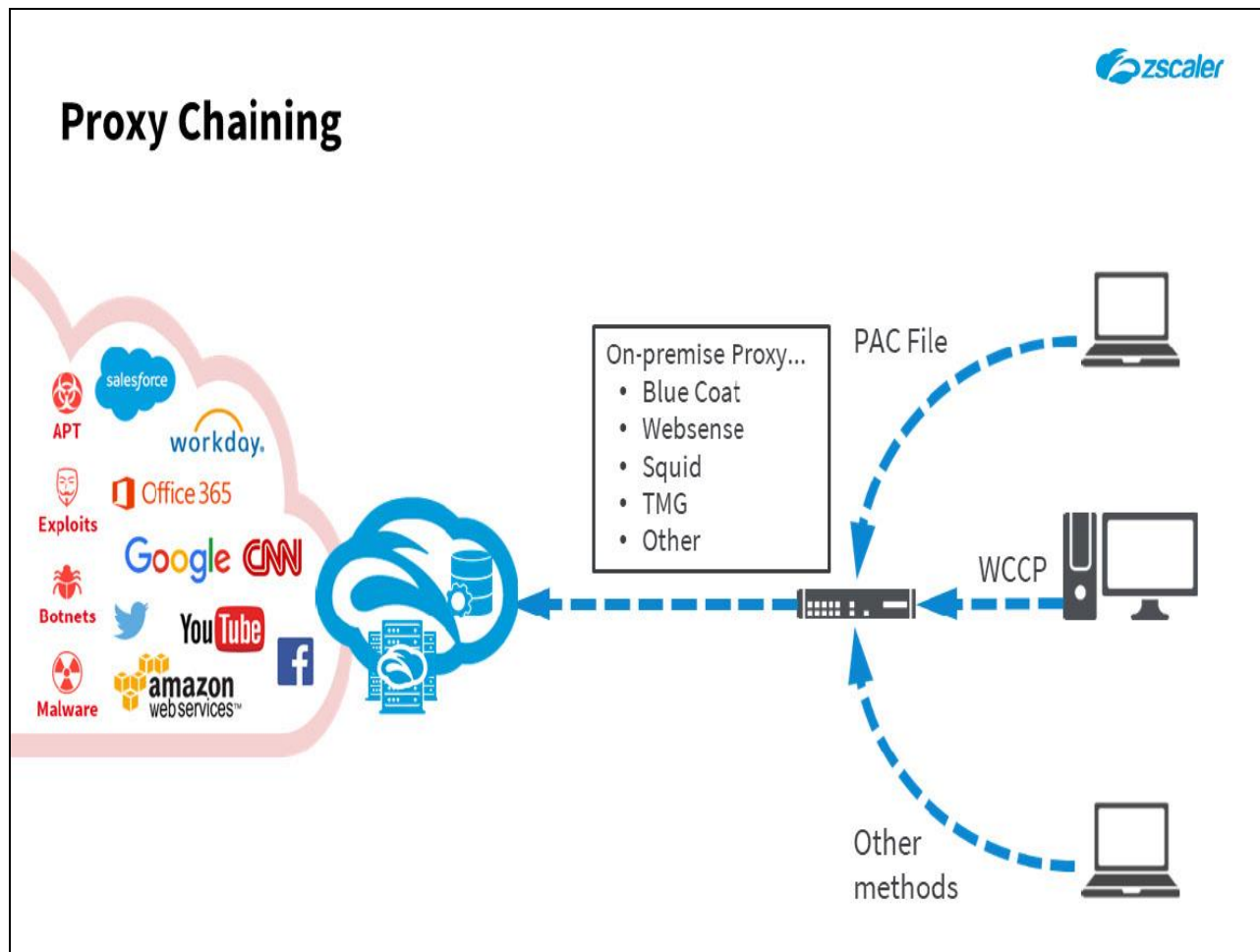
In these networks there must be an explicit route created for traffic destined for Zscaler. The way we handle this is via the use of Global ZEN IPs. These are a range of IP addresses to which a ZEN will respond regardless of its own IP. In this environment you must use a PAC file or Zscaler App with a PAC file to tell the client to send their traffic to one of the Global ZEN IPs.

You would then advertise a route for that Global ZEN IP inside your corporate network leading to the router with the tunnel to Zscaler. If you have users that roam outside the corporate network, you will need to add some logic to the PAC file. When they are inside the corporate network, they should send their traffic to the Global ZEN IP.



When they are outside the network, they should use the standard GATEWAY and SECONDARY\_GATEWAY variables to find the nearest ZEN IP. For more information and an example PAC file check out the No Default Route article on [help.zscaler.com](http://help.zscaler.com)

## Slide 15 - Proxy Chaining

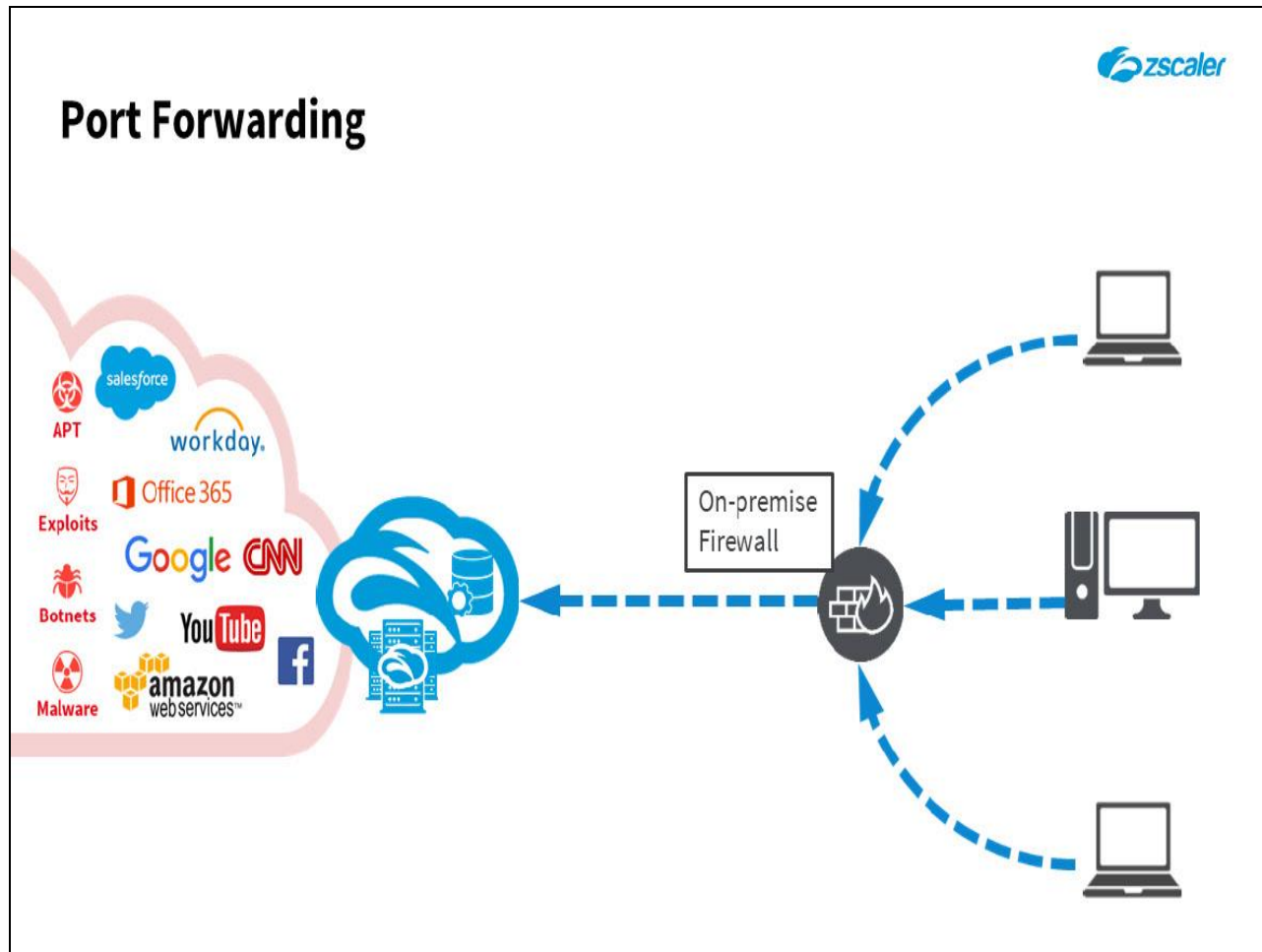


## Slide notes

Proxy chaining is a very useful deployment option for a Proof of Concept or POC where you already have a proxy solution deployed. This enables you to realize the value of Zscaler without any significant configuration changes. For instance, you can setup a BlueCoat proxy to forward all traffic for a certain subnet, users, or category to Zscaler.

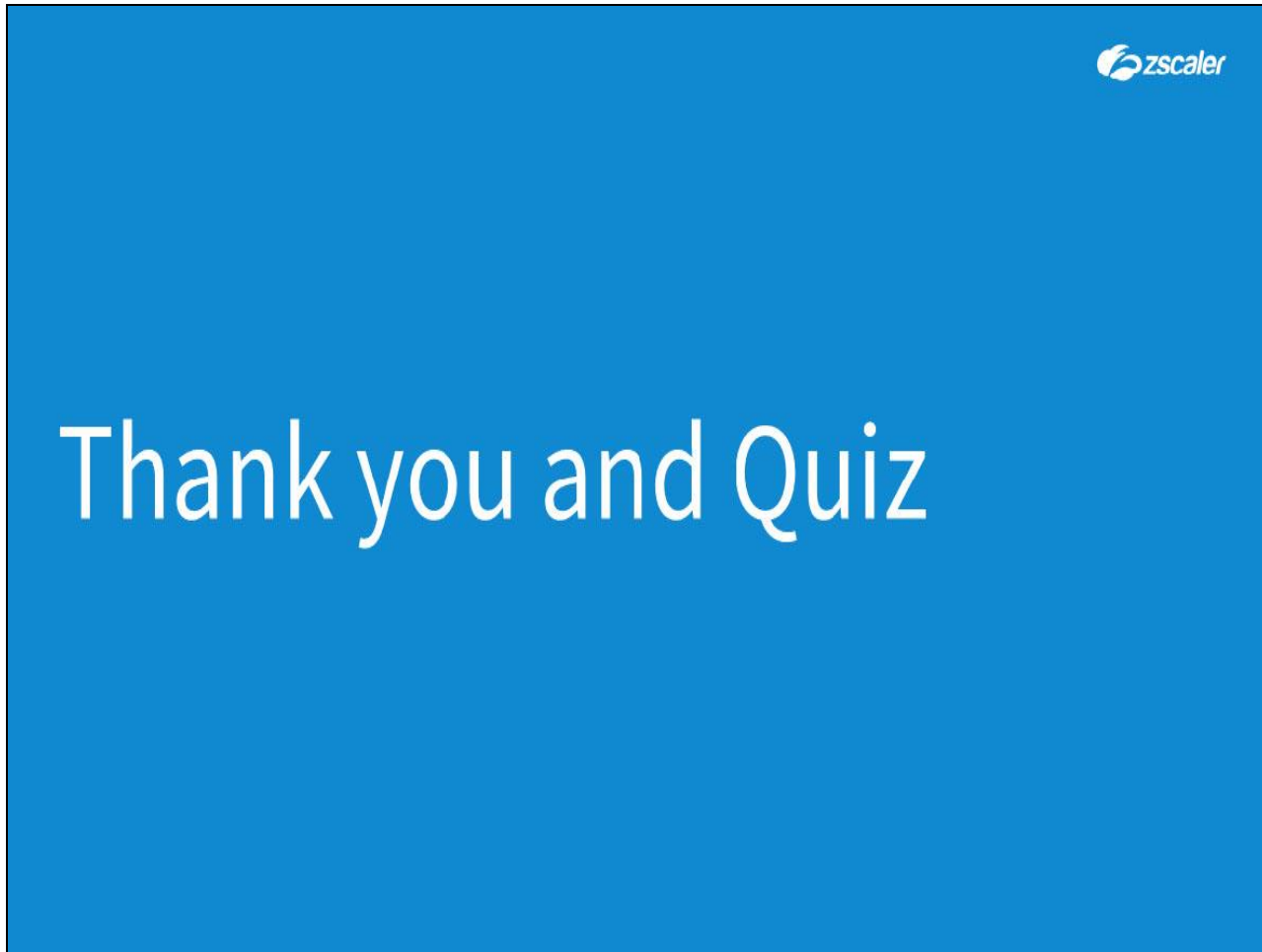
Also, you can send all uncategorized traffic to Zscaler and begin to immediately use its superior threat analysis engine.

## Slide 16 - Port Forwarding



## Slide notes

Port forwarding is a very useful tool to setup a quick POC, but it is not very efficient and may overload some older routers or firewalls. In essence, you need to instruct the edge device to forward all traffic that has port 80 or 443 destination to the closest ZEN. You should plan for GRE or Site-to-Site VPN for a production deployment.

**Slide 17 - Thank you and Quiz****Slide notes**

This completes the Zscaler Traffic Forwarding Overview 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 during this module. Click the **X** in the upper right corner of the window to close this module then launch the quiz. You may retake the quiz as many times as necessary to pass.