

Slide 1 - ZCCP-IA



# ZCCP-IA

## Traffic Forwarding: Proxy Chaining and Port Forwarding

©2018 Zscaler, Inc. All rights reserved.

**Slide notes**

Thank you for viewing this eLearning module on Traffic forwarding to the Zscaler solution using Proxy Chaining and Port Forwarding.



## Slide 2 - Navigating the eLearning Module

## Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. The dashboard includes a navigation bar with links for Dashboard, Analytics, Policy, and Administration. The main content area displays several charts and tables, including 'Web Overview', 'Cloud Application Classes', 'Top URL Categories', and 'Top Users'. Overlaid on the screenshot are several blue callout boxes with white text, each pointing to a specific control on the dashboard. These controls are: 'Exit' (top right), 'Previous Slide' (left side), 'Next Slide' (right side), 'Play/Pause' (bottom left), 'Fast Forward' (bottom center-left), 'Progress Bar' (bottom center), 'Audio On/Off' (bottom center-right), and 'Closed Captioning' (bottom right).

**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 - Agenda**The slide features a light gray background with a large white cloud shape on the left side. The word "Agenda" is written in blue text inside the cloud. To the right of the cloud, there is a bulleted list of two items: "Proxy Chaining" and "Port Forwarding".

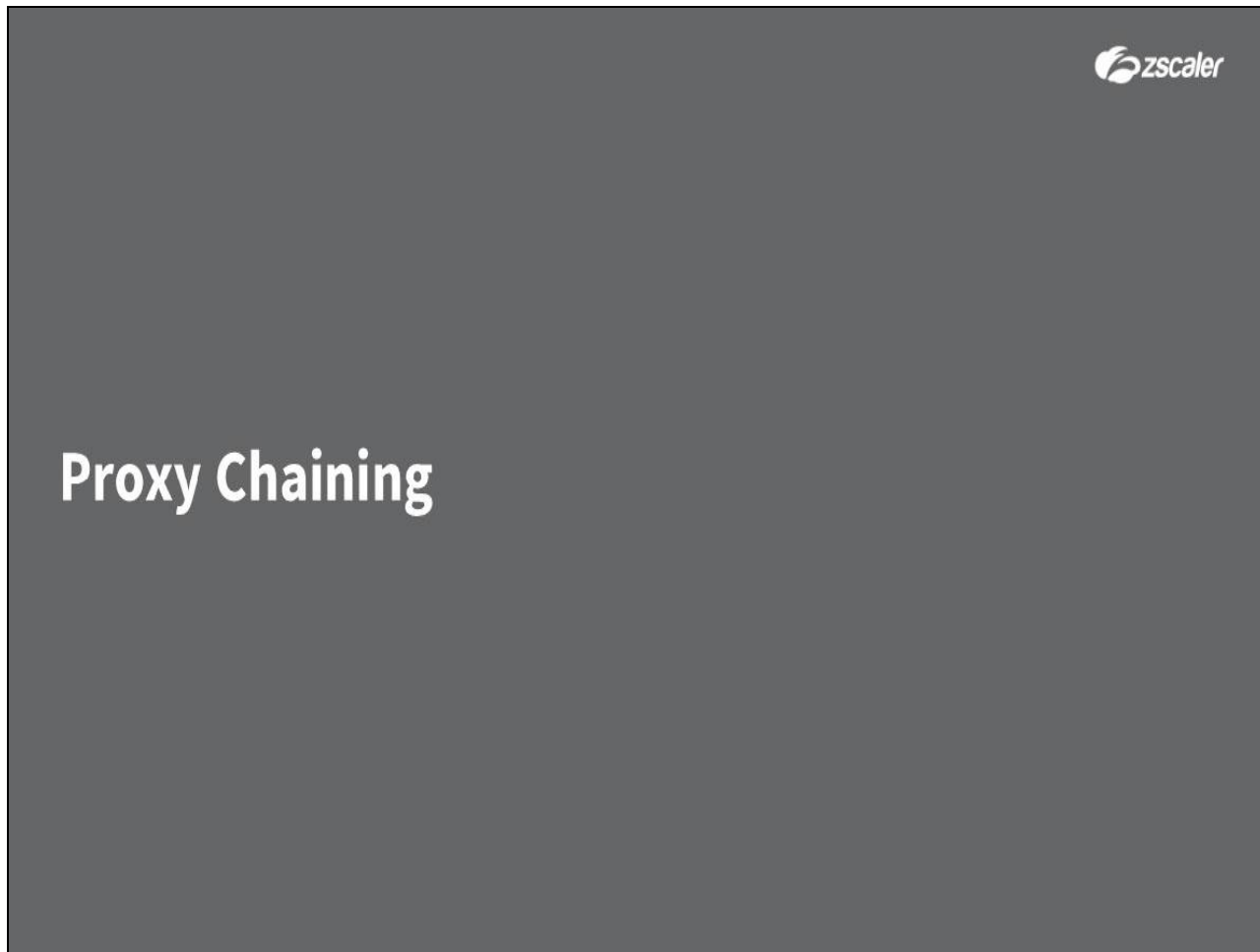
# Agenda

- Proxy Chaining
- Port Forwarding

**Slide notes**

During this session, we will examine Proxy Chaining and Port Forwarding to connect your locations to the Zscaler solution for proof of concept testing along with sample configurations.


**Slide 4 - Proxy Chaining**



**Slide notes**

Let's begin by taking a look at Proxy chaining and a sample configuration of Proxy Chaining.

## Slide 5 - About Proxy Chaining



## About Proxy Chaining

- Proxy chaining involves forwarding traffic from one proxy server to another

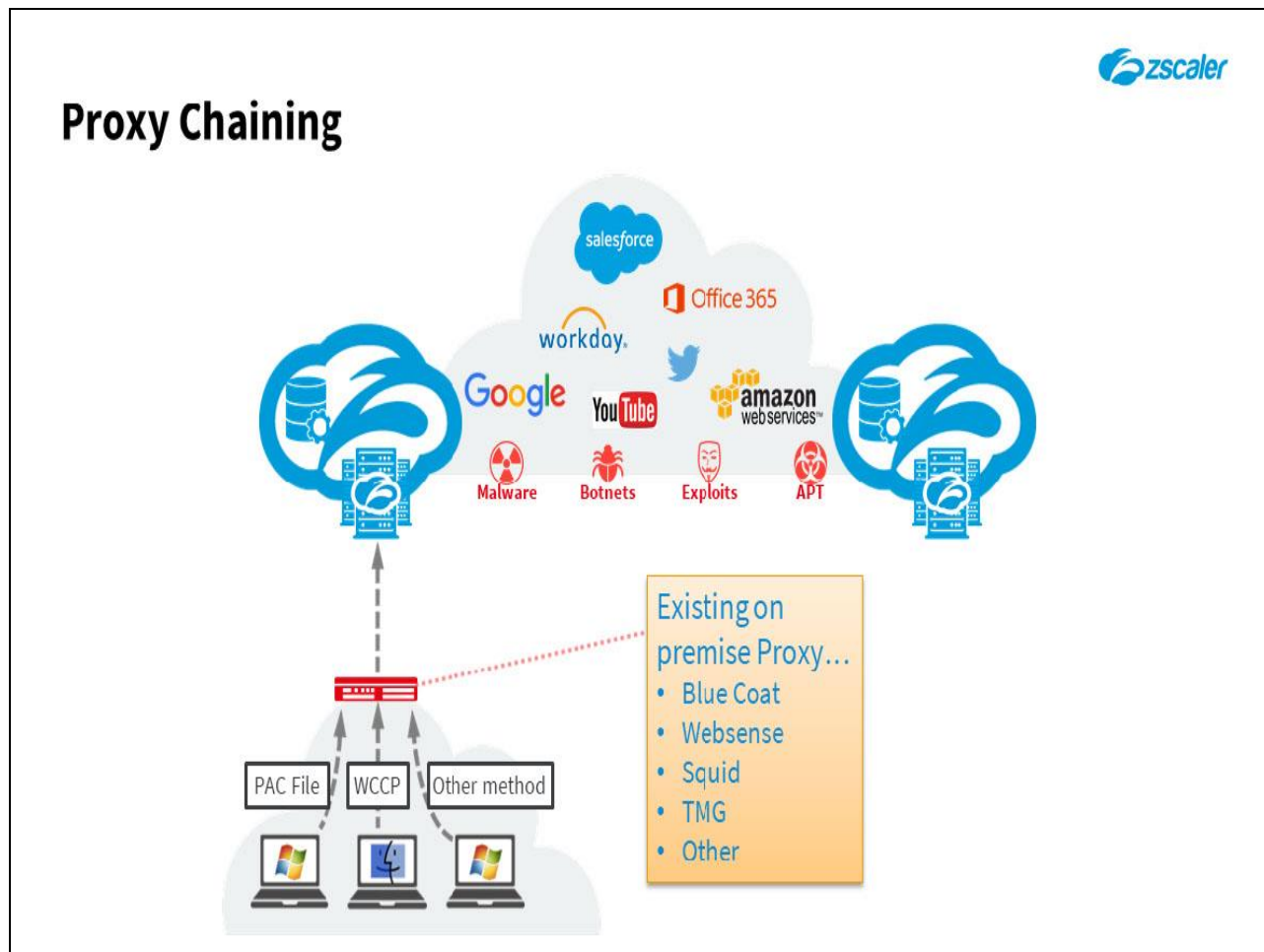
| Advantages                                                                                                                                                                                                       | Disadvantages                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Leverage existing proxy servers</li><li>No changes to the network</li><li>Quick and easy way to forward traffic to Zscaler</li><li>Ideal for evaluation purposes</li></ul> | <ul style="list-style-type: none"><li>Not recommended as a long-term solution</li><li>Manual failover only is available for proxy servers with failover support</li><li>Not recommended for production environments</li></ul> |

**Slide notes**

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.

Please note that Zscaler does not recommend proxy chaining as a long-term solution because proxy servers that support failover, generally support only manual failover, which is not recommended for production environments.

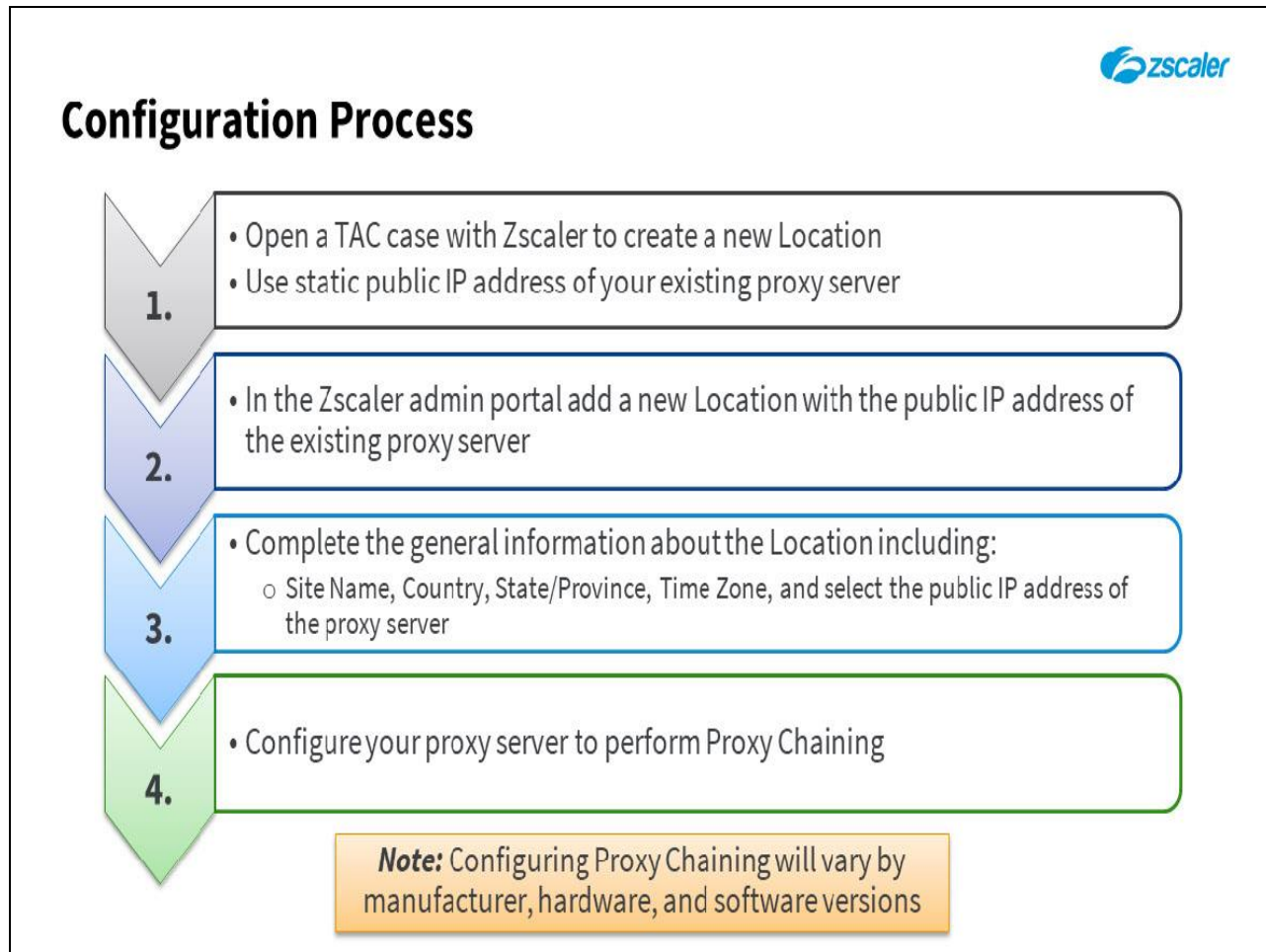
## Slide 6 - Proxy Chaining



## Slide notes

Proxy chaining is a very useful deployment option for Proof of Concept testing 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 configure a BlueCoat proxy to forward all HTTP or HTTPS traffic for a certain subnet, users, or category to Zscaler. Also, you can send all uncategorized traffic to Zscaler to immediately see all the items your other solution may be missing.

## Slide 7 - Configuration Process



## Slide notes

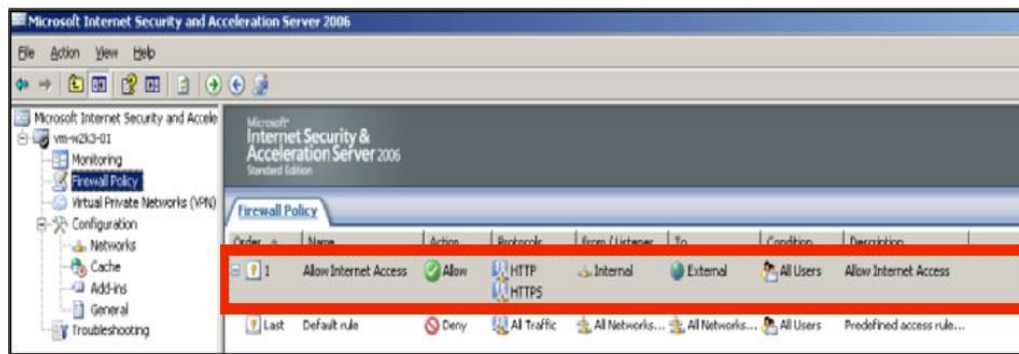
1. Begin by opening a TAC case with Zscaler to create a new location using the static public IP address of your proxy server performing Proxy Chaining.
2. Once the location has been created by TAC it is visible in the Zscaler Admin Portal. You can now add the new location using the public IP address of your proxy server.
3. Fill in the general information about the location including: **Site Name, Country, State/Province, Time Zone**, and choose the **Public IP Address** of your proxy server.
4. Configure your proxy server to perform Proxy Chaining.

NOTE: Configuring Proxy Chaining will vary by manufacturer, hardware, and software versions.

**Slide 8 - Example Configuration – Microsoft ISA Server**

## Example Configuration – Microsoft ISA Server

- This example illustrates how to configure a Microsoft ISA server to redirect web traffic upstream to a ZEN
  - It is based on the deployment of a simple single network adapter
  - Client workstations on the internal network proxy to the ISA server
  - Rule configured to permit web access from the internal network to the Internet

**Slide notes**

This example illustrates how to configure a Microsoft ISA server to redirect web traffic upstream to Zscaler. Client workstations on the internal network have their browsers configured to proxy to the ISA server. It assumes you have configured the rule in the following figure to permit web access from the internal network to the Internet. This rule (number 1) allows both the HTTP and HTTPS traffic from the internal network to the external network for all users.

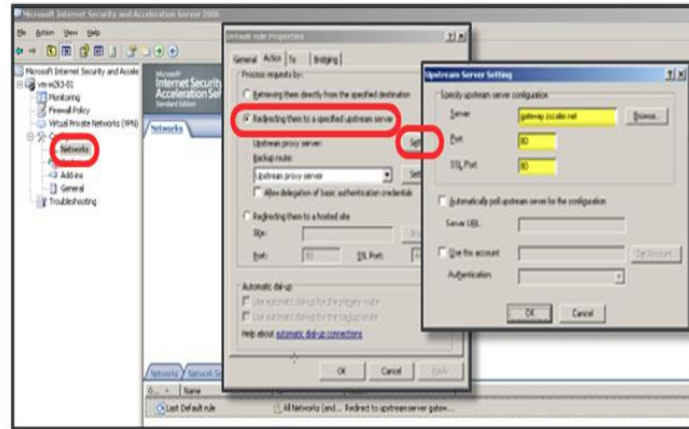


## Slide 9 - Example Configuration – Microsoft ISA Server

## Example Configuration – Microsoft ISA Server



- To configure web chaining on the Microsoft ISA Server:
  - Go to **Configuration > Networks**
  - Edit **Default Rule** (or create a new, higher rule)
  - On the rule's **Action** tab, select to process requests by **Redirecting them to a specified upstream server**
  - Click **Settings**
    - Server: gateway.<your assigned cloud>.net
    - Port : 80
    - SSL Port: 80



### Slide notes

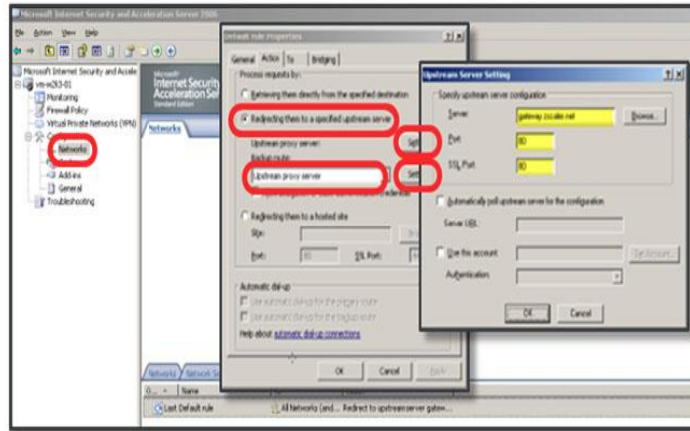
To configure web chaining on the Microsoft ISA Server: Go to the **Configuration > Networks** menu. Edit the **Default Rule** or create a new rule higher up in the Web chaining policy. On the rule's **Action** tab select: **Redirecting them to a specified upstream server**. Click **Settings**, and specify the Server as **gateway.<your assigned cloud>.net** (for example **gateway.zscaler.net**) and enter **80** in the **Port** and **SSL Port** fields.

## Slide 10 - Example Configuration – Microsoft ISA Server

## Example Configuration – Microsoft ISA Server



- Completing the configuration...
  - On the same tab, select to use a **Backup route: Upstream proxy server**
  - Click **Settings**
    - Server: secondary.gateway.<your assigned cloud>.net
    - Port : 80
    - SSL Port: 80



- All proxy connections to the Microsoft ISA Server will now be forwarded to a resilient pair of nodes on Zscaler

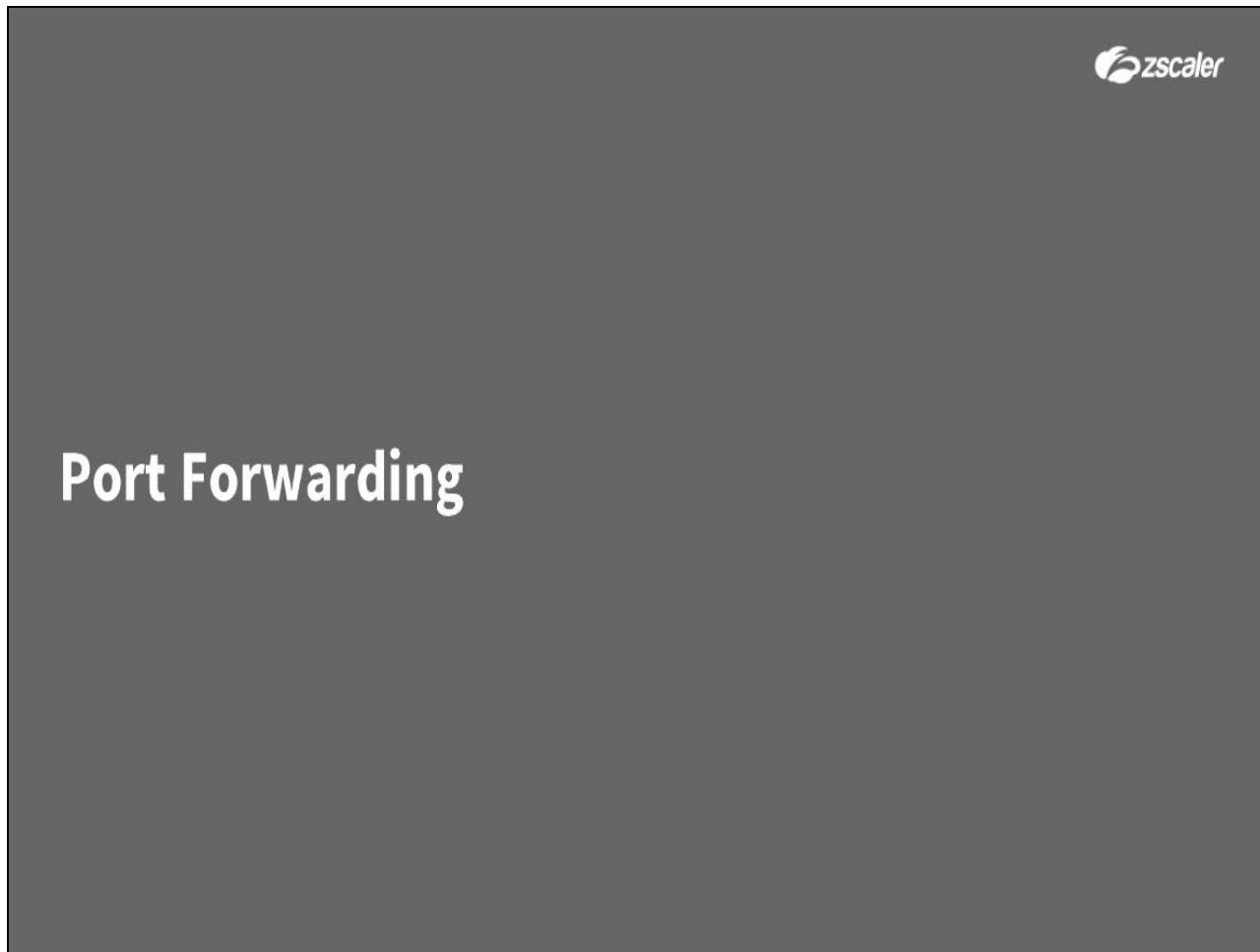
**Note:** both **gateway.-** and **secondary.gateway.<your assigned cloud>.net** are required for fault tolerance, Zscaler does not support configurations with only one proxy server

### Slide notes

On the same tab, under **Backup route** select **Upstream proxy server**. Click **Settings**, and specify the Server as **secondary.gateway.<your assigned cloud>.net** (for example **secondary.gateway.zscaler.net**) and enter **80** in the **Port** and **SSL Port** fields.

All proxy connections to the Microsoft ISA Server will now be forwarded to a resilient pair of nodes within the Zscaler service. Note that both **gateway.<your assigned cloud>.net** and **secondary.gateway.<your assigned cloud>.net** must be specified as the primary and secondary proxy servers to ensure fault tolerance. Zscaler does not support configurations with only one proxy server.

**Slide 11 - Port Forwarding**



**Slide notes**

Let's now take a quick look at Port Forwarding, and a sample configuration for Port Forwarding.

## Slide 12 - About Port Forwarding



## About Port Forwarding

- If your perimeter firewall supports forwarding protocols to another host, you can configure it to forward outgoing HTTP traffic to Zscaler

### Advantages

- This method leverages your existing firewall
- No additional changes to the network
- Quick and easy way to forward traffic to Zscaler for evaluation purposes

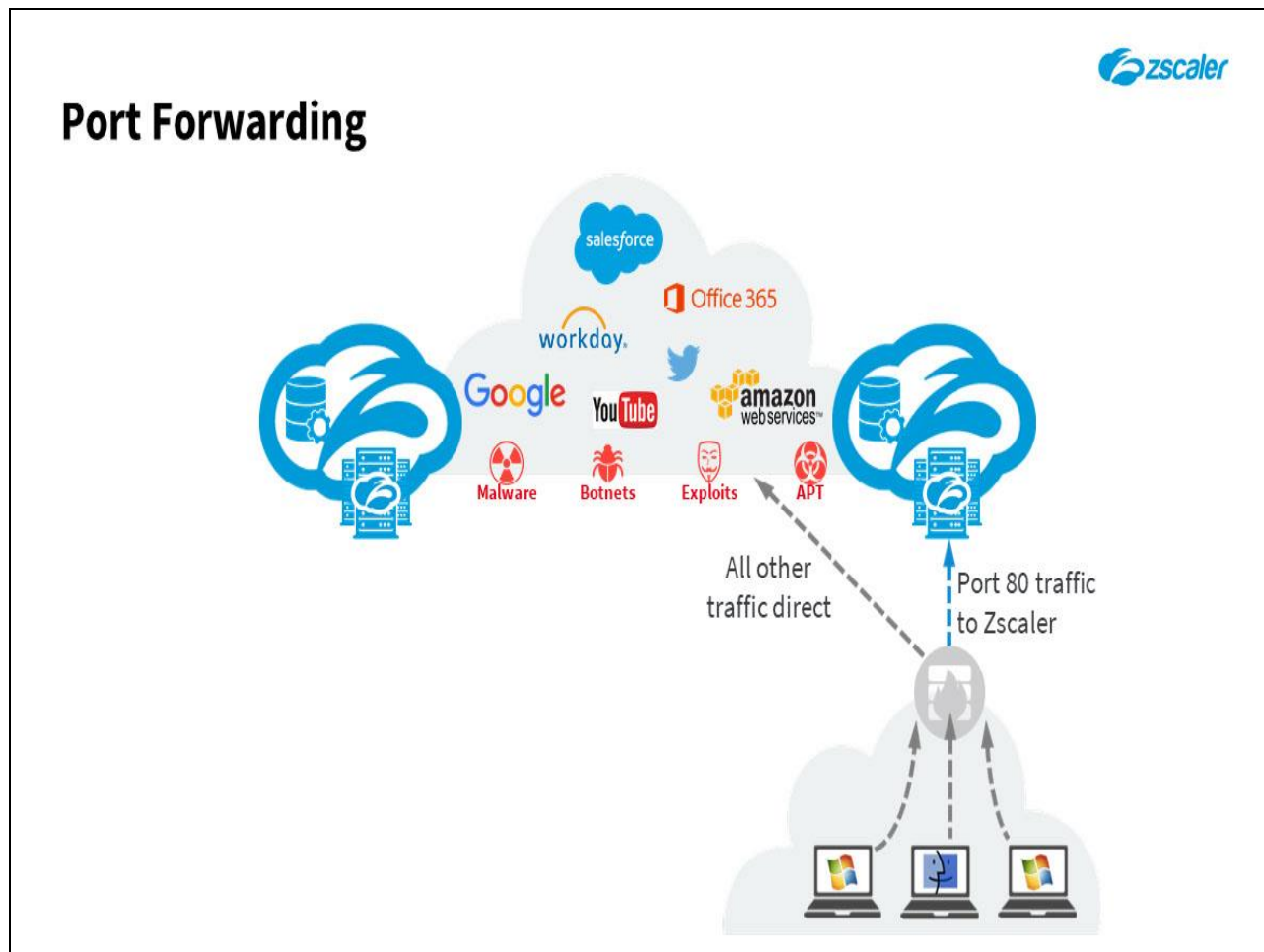
### Disadvantages

- Not recommended as a long-term solution
- Does not support HTTPS traffic or automatic failover

### Slide notes

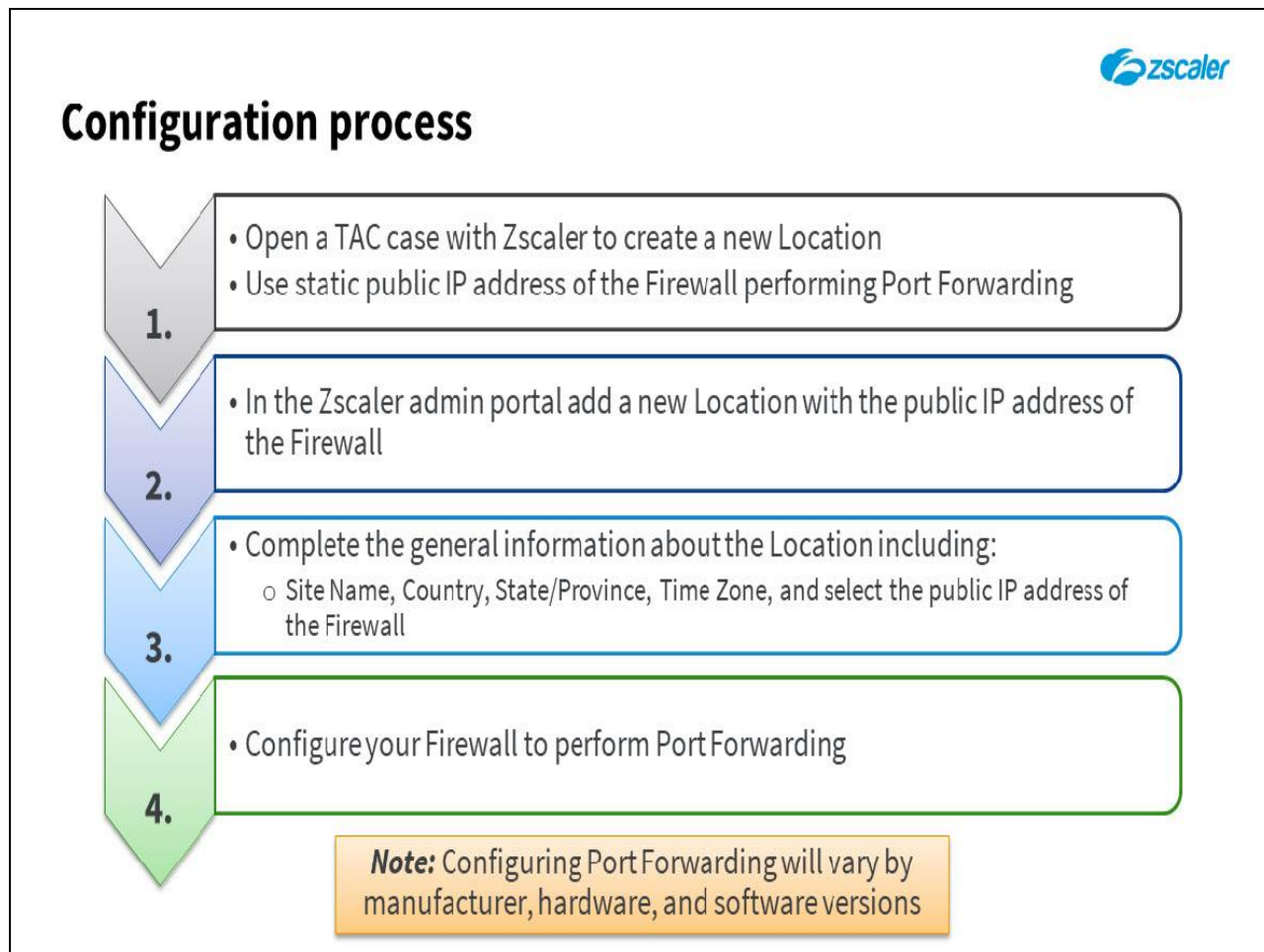
If your perimeter firewall supports forwarding protocols to another host, you can configure it to forward outgoing HTTP traffic to Zscaler. This method leverages your existing firewall, with no additional changes to the network. It's a quick and easy way to forward your traffic to the Zscaler service for evaluation purposes. Zscaler does not recommend port forwarding as a long-term solution because it does not support HTTPS traffic or automatic failover.

## Slide 13 - Port Forwarding

**Slide notes**

Port forwarding is a very useful tool to setup a quick Proof of concept test, 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 HTTP traffic to Zscaler. You should ultimately plan for GRE or Site-to-Site VPN for production deployments.

## Slide 14 - Configuration process



## Slide notes

1. Begin by opening a TAC case with Zscaler to create a new location using the static public IP address of your firewall performing Port Forwarding.
2. Once the location has been created by TAC it is visible in the Zscaler Admin Portal. You can now add the new location using the public IP address of the firewall.
3. Fill in the general information about the location including: **Site Name, Country, State/Province, Time Zone**, and choose the **Public IP Address** of your firewall.
4. Configure your firewall to perform Port Forwarding.

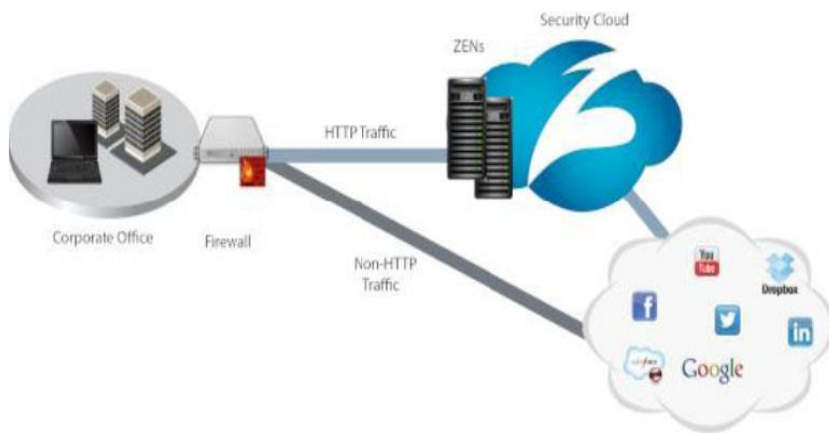
NOTE: Configuring Port Forwarding will vary by manufacturer, hardware, and software versions.

## Slide 15 - Example Configuration – Juniper SSG5 firewall



## Example Configuration – Juniper SSG5 firewall

- Configure a Juniper SSG5 firewall to forward HTTP traffic to Zscaler
  - Redirect traffic from the inside interface with destination port 80 to the Zscaler IP address on port 80



### Slide notes

The following example illustrates how to configure a Juniper SSG5 firewall to forward HTTP traffic to the Zscaler service. It redirects traffic from the inside interface with destination port 80 to the Zscaler IP address on port 80.

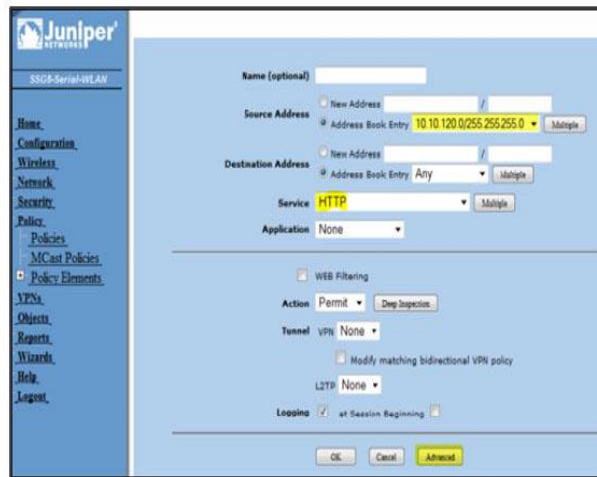


## Slide 16 - Config example



## Example Configuration – Juniper SSG5 firewall

- Go to **Policies > Policy** and create a new policy from the **Trust to the Untrust** zone
  - Click **New** then configure the policy
  - Port **80** originating from the 10.10.120.x network will be translated and forwarded
  - Click **Advanced**



### Slide notes

Go to **Policies > Policy** and create a new policy from the **Trust to the Untrust Zone**. Click **New** then configure the policy. As shown in the following figure port **80** originating from the **10.10.120.x** network will be translated and forwarded. Next, click **Advanced**.



## Slide 17 - Config example cont.



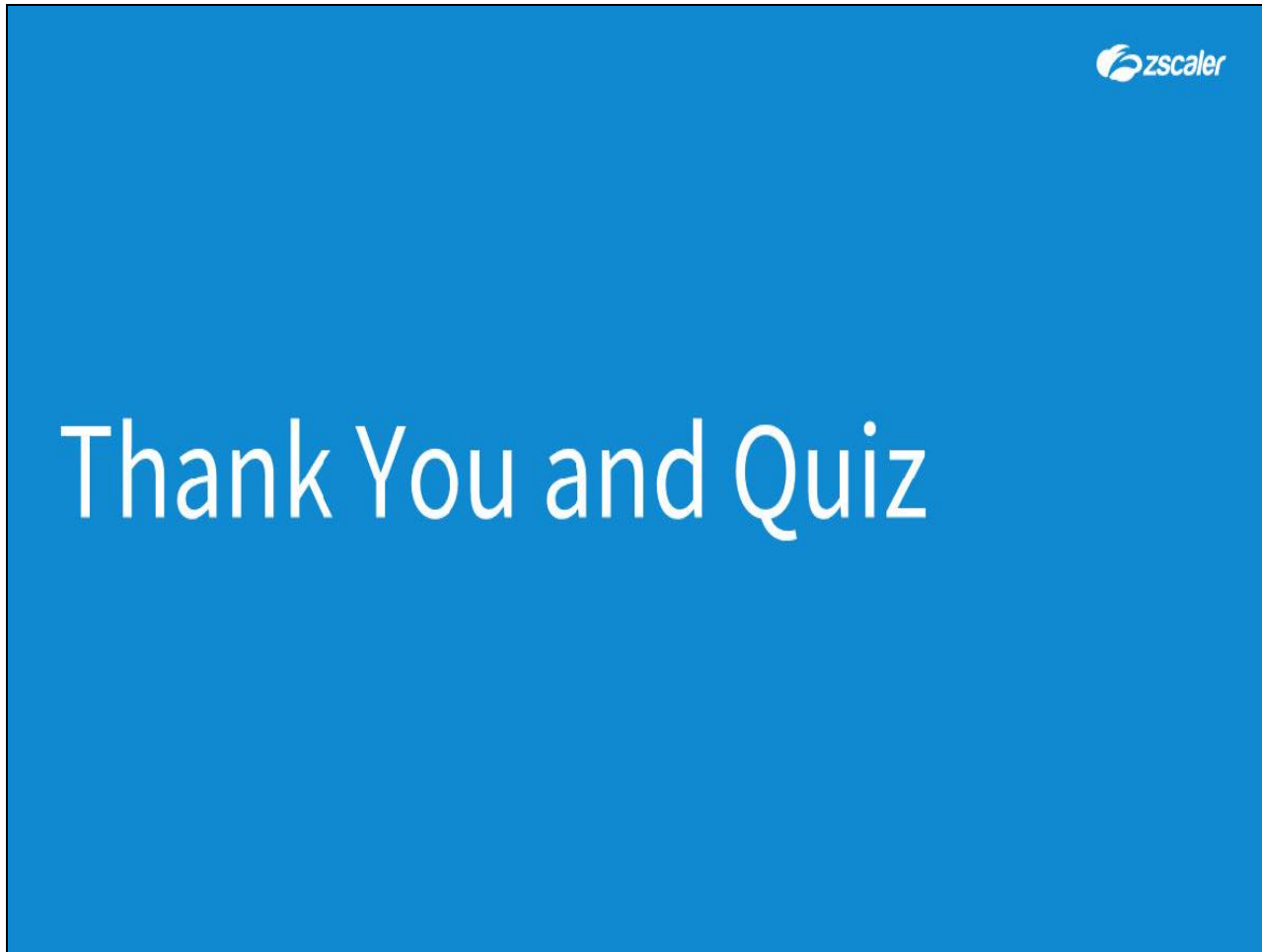
## Example Configuration – Juniper SSG5 firewall

- In the Advanced settings:
  - Set the **Translate to IP** to your assigned Zscaler node
  - Configure the **Map to Port** to **80**
  - Click **OK** to create the policy, then **OK** to exit advanced settings
- The completed policy will look similar to the figure below:

| ID | Source                    | Destination | Service | Action          | Options | Configure         | Enable                              | Move |
|----|---------------------------|-------------|---------|-----------------|---------|-------------------|-------------------------------------|------|
| 2  | 10.10.120.0/255.255.255.0 | Any         | HTTP    | Translate to IP |         | Edit Clone Remove | <input checked="" type="checkbox"/> | ↕ ⇄  |
| 1  | Any                       | Any         | ANY     | Allow           |         | Edit Clone Remove | <input checked="" type="checkbox"/> | ↕ ⇄  |

### Slide notes

After clicking **Advanced**, complete the following, and then click **OK** to exit Advanced Policy Settings: **Translate to IP:** **<your assigned Zscaler node>**, **Map to Port: 80**. Click **OK** to create the policy. The completed policy will look similar to the figure below.

**Slide 18 - Thank You and Quiz****Slide notes**

This completes the Traffic Forwarding with Proxy Chaining or Port Forwarding 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.