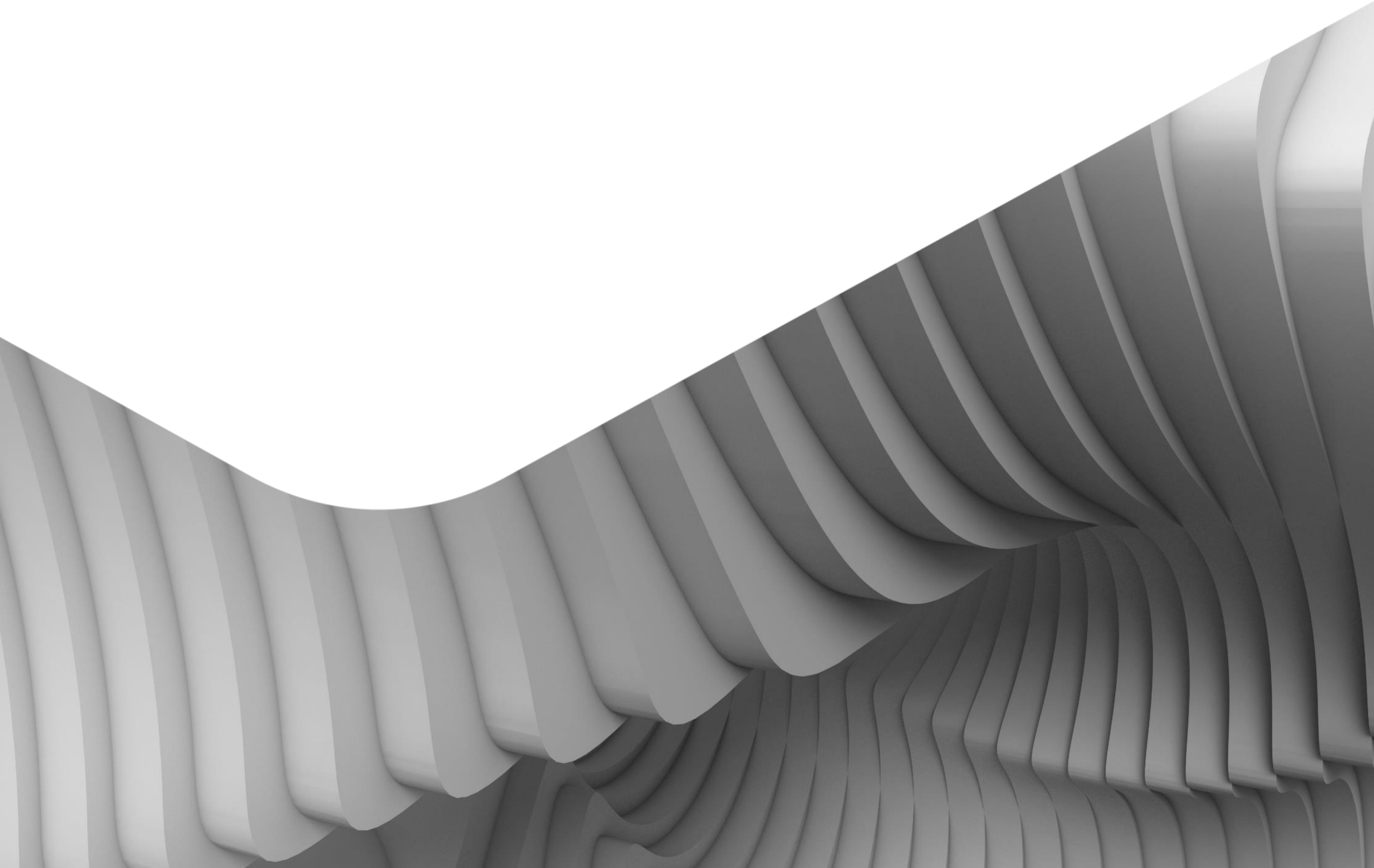
Kemp Zero Trust Access Gateway

Quick Start Guide



Overview

The Kemp Zero Trust Access Gateway (ZTAG) delivers a simple, flexible, and secure solution for providing the necessary access for users and applications to access backend systems while greatly reducing the exposure to today's threats. The Zero Trust Access Gateway architecture leverages the customer's existing Kemp load balancers to deliver this security model.

The Kemp Zero Trust Access Gateway delivers secure publishing of workloads using the following attributes:

- Authentication
- Group Membership
- Location
- HTTP Header
- Path

How it works

The Kemp Zero Trust Access Gateway provides administrators with a policy builder to implement granular least privileged access to resources published through the load balancer. A configuration file is used to clearly define the application as well as the access policy rules. This configuration file is called by a script that allows the administrator to choose different options during each run dependent on the use case being addressed. Example XML configuration files are provided to assist with the configuration of policies for each use case.

Supported Use Cases

The following are the supported use cases for Zero Trust Access Gateway while additional variations are being developed and released.

Source IP/Method/Path – This security policy although developed for object storage solutions is not limited for this workload. The traffic must match all three attributes to be permitted access to the published system.

Who – The source IP Address of the requestor.
What – The HTTP Method (GET, PUT, DELETE, etc.) being passed to the published system.
Where – The path of the object being requested or written, defined using regular expression (regex) for flexible implementations.

Authentication Header/Method/SourceIP– This security policy is also developed for object storage solutions but can be applied to other workloads. The Content Rules for this use case are as follows.

Who – The Authentication Header within the HTTP traffic.
What – The HTTP Method being passed to the published system.
Where – This is Source IP address from where the traffic originated.

SteeringGroup/Path/SourceIP– This security policy is designed for any application that performs pre-authentication on the Kemp Load Balancer. This utilizes the Kemp Edge Security Pack feature to determine a user's group membership in combination with the client's source IP address and the path within the application they request.

> Who – Group membership. This is an attribute that looks at the Active Directory group a user is a member of and directs them to a specific element of the published application.
> What – The path within the published application the user is trying to access. By defining this using regular expressions (regex), an application can be segmented to suit many scenarios
> Where – This is Source IP address from where the traffic originated from.

Trusted/ Untrusted Zone– This security policy also requires Kemp Edge Security Pack but determines the type of authentication that is required for a user based on group and location. Should the traffic match the attributes for a Trusted zone, the user is presented with a simple form to authenticate to the application, but should the traffic be identified as Untrusted, the user will be required to provide multi-factor authentication to gain access.

> Who – Permitted Group. This is a Kemp specific attribute that looks at the Active Directory group a user is a member of and permits or denies access dependent on their group membership.
> Where – This is Source IP address from where the traffic originated from.

Getting Started

Pre-Requisites

The Zero Trust Access Gateway does not require the user to have in-depth knowledge with Kemp products or PowerShell but some familiarity for each is recommended.

The components that make up the Kemp Zero Trust Access Gateway:

- Kemp LoadMaster or ECS Connection Manager
- Kemp Load Balancer PowerShell Module
- Zero Trust Policy Builder PowerShell Script
- Zero Trust Policy Builder Configuration File (XML)

Import Kemp PowerShell Module

1. **Download the Kemp PowerShell Module**

   The latest Kemp PowerShell Module can be found on the Support Website.

   https://support.kemptechnologies.com/hc/en-us/categories/200141477-Downloads

2. **Import the Kemp PowerShell Module** –

a) Copy the **Kemp.LoadBalancer.Powershell** folder to the relevant folder.
b) Install the module in a folder that is available in PSModulePath ($Env:PSModulePath).
c) Import the module to start using it:

Import-Module Kemp.LoadBalancer.Powershell

For the PowerShell commands to work, the API interface must be enabled on the LoadMaster. To enable it using the Web User Interface (WUI), go to **Certificates & Security** > **Remote Access** and select **Enable API Interface**

Download the Kemp Zero Trust Access Gateway Package

The latest Kemp ZTAG Package can be found on the Support Website.

https://support.kemptechnologies.com/hc/en-us/categories/200141477-Downloads

Unzip the ZTAG Package.

The package contains the following files:

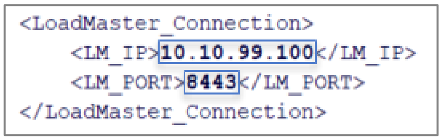
- ZTAG-Policy-Builder.ps1
- Config_AuthHeader.xml
- Config_SourceIP.xml
- Config_SteeringGroup.xml
- Config_Trusted_Zones.xml

Modify Configuration File for desired use case

The Zero Trust Policy Builder currently supports four (4) different use cases. Each is defined within a sample configuration XML file. These configuration files determine the state of the environment which is being secured.

It is recommended that Notepad++ or some other XML aware application is used when working with the ZTAG configuration files

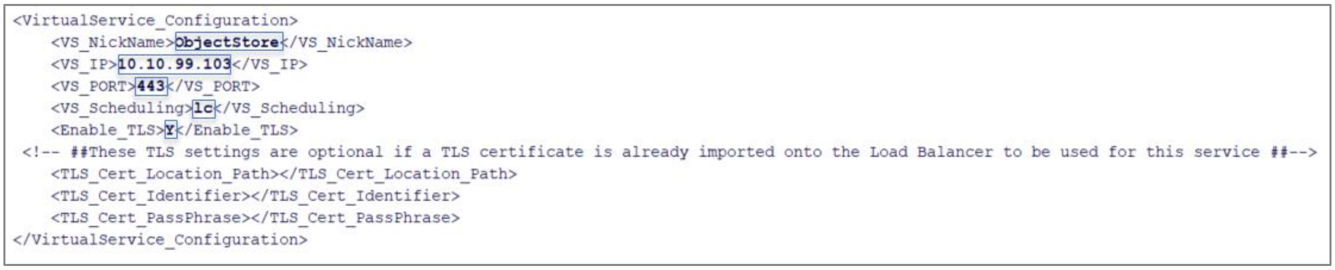
Open the desired sample configuration file. The XML files contain similar sections for the configuration of the Virtual Service that will be used to publish and secure the application/workload. Policy specific sections will be unique based on the use case.



```
<LoadMaster_Connection>
    <LM_IP>10.10.99.100</LM_IP>
    <LM_PORT>8443</LM_PORT>
</LoadMaster_Connection>
```

1. Modify the LoadMaster connection settings for the LoadMaster or ECS Connection Manager:
    - The LoadMaster or ECS Connection Manager IP Address

- The LoadMaster or ECS Connection Manager TCP Port

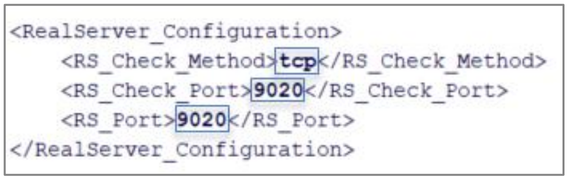


```
<VirtualService_Configuration>
    <VS_NickName>ObjectStore</VS_NickName>
    <VS_IP>10.10.99.103</VS_IP>
    <VS_PORT>443</VS_PORT>
    <VS_Scheduling>lc</VS_Scheduling>
    <Enable_TLS>Y</Enable_TLS>
 <!-- ##These TLS settings are optional if a TLS certificate is already imported onto the Load Balancer to be used for this service ##-->
    <TLS_Cert_Location_Path></TLS_Cert_Location_Path>
    <TLS_Cert_Identifier></TLS_Cert_Identifier>
    <TLS_Cert_PassPhrase></TLS_Cert_PassPhrase>
</VirtualService_Configuration>
```

2. Modify the Virtual Service configuration with settings based on workload requirements.
    - A Nickname (friendly name) to identify the workload being published
    - A Virtual IP Address to publish the workload
    - A Scheduling Method on how the distribution of the traffic to back-end systems should occur.
        - rr = round robin
        - wrr = weighted round robin
        - lc = least connection
        - wlc = weighted least connection
        - fixed = fixed weighting
        - adaptive = resource based (adaptive)
        - sh = source IP hash
        - dl = weighted response time
        - sdn-adaptive = resource based (SDN adaptive)
        - uhash = URL hash
    - Select whether SSL/TLS Acceleration should be enabled on the Virtual Service.
        - Y
        - N

    Optional – If a certificate is present on the LoadMaster/ ECS Connection Manager a prompt will be provided to select which certificate should be used in the configuration. A certificate can be uploaded and applied by entering the following parameters

    - Path/ location to the certificate file (PFX)
    - A friendly name or identifier for the certificate
    - The passphrase for importing the certificate

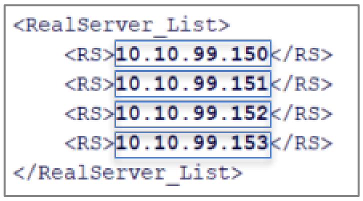


```
<RealServer_Configuration>
    <RS_Check_Method>tcp</RS_Check_Method>
    <RS_Check_Port>9020</RS_Check_Port>
    <RS_Port>9020</RS_Port>
</RealServer_Configuration>
```

3. Modify the Real Server configuration with settings based on workload requirements.

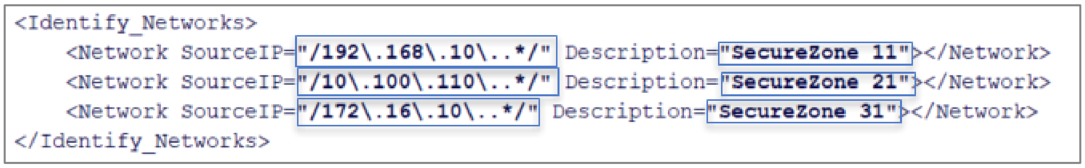
    Real Server Check Method

    - https
    - http
    - tcp



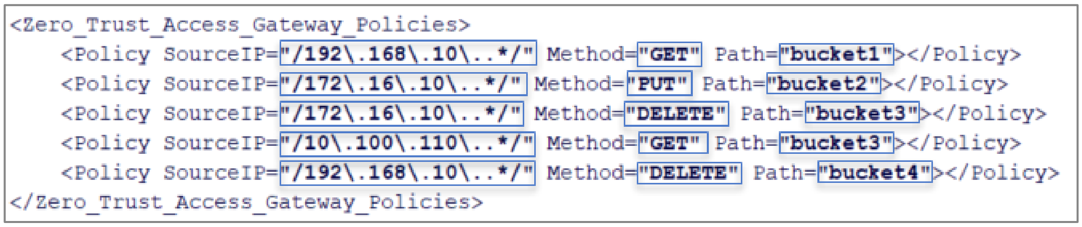
```
<RealServer_List>
    <RS>10.10.99.150</RS>
    <RS>10.10.99.151</RS>
    <RS>10.10.99.152</RS>
    <RS>10.10.99.153</RS>
</RealServer_List>
```

4. Modify the Real Server list with IP Address or FQDN of the back-end systems being published. Lines can be removed or added based on the number of Real Servers in the environment.



```
<Identify_Networks>
    <Network SourceIP="/192\.168\.10\..*/" Description="SecureZone 11"></Network>
    <Network SourceIP="/10\.100\.110\..*/" Description="SecureZone 21"></Network>
    <Network SourceIP="/172\.16\.10\..*/" Description="SecureZone 31"></Network>
</Identify_Networks>
```

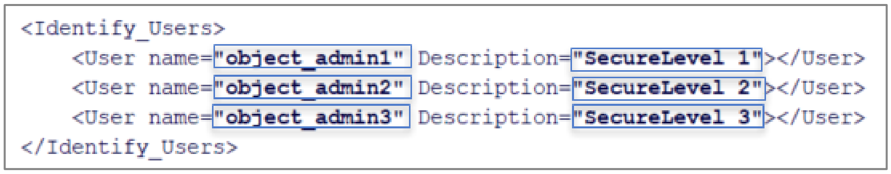
5. **SourceIP/Method/Path Only** - The SourceIP/Method/Path use case identifies where the traffic originates from based on IP Address. This section defines the networks and description for each within an environment.
    - Source IP Address using Regular Expression (RegEx) to identify the networks in the environment.
    - Description (friendly name) of the networks in the environment.



```
<Zero_Trust_Access_Gateway_Policies>
    <Policy SourceIP="/192\.168\.10\..*/" Method="GET" Path="bucket1"></Policy>
    <Policy SourceIP="/172\.16\.10\..*/" Method="PUT" Path="bucket2"></Policy>
    <Policy SourceIP="/172\.16\.10\..*/" Method="DELETE" Path="bucket3"></Policy>
    <Policy SourceIP="/10\.100\.110\..*/" Method="GET" Path="bucket3"></Policy>
    <Policy SourceIP="/192\.168\.10\..*/" Method="DELETE" Path="bucket4"></Policy>
</Zero_Trust_Access_Gateway_Policies>
```

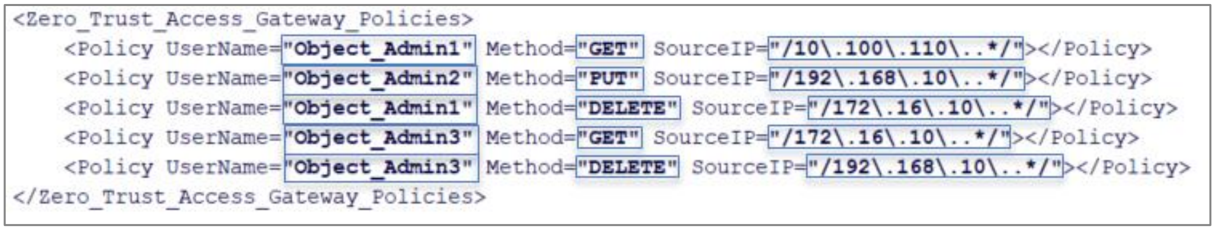
6. **SourceIP/Method/Path Only** - The policy section is where the security settings are configured. Lines can be added or removed depending on the number of rules that should be applied in the policy.
    - Source IP Address to apply the security policy to.
    - The method that should be permitted for the defined path/ bucket.
        - GET
        - PUT
        - DELETE
        - POST
    - The path or bucket to apply the security policy to.

Any Source IP Addresses that are applied here **must** be identified in the Identify_Network section for the SourceIP use case above



```
<Identify_Users>
    <User name="object_admin1" Description="SecureLevel 1"></User>
    <User name="object_admin2" Description="SecureLevel 2"></User>
    <User name="object_admin3" Description="SecureLevel 3"></User>
</Identify_Users>
```

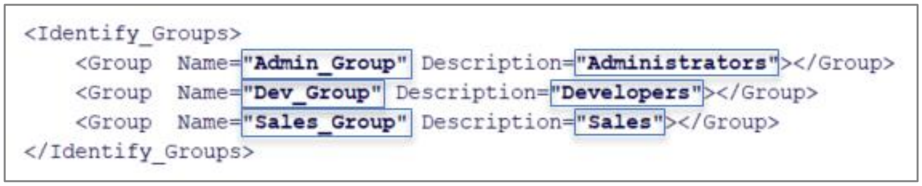
7. **AuthHeader/Method/ SourceIP Only** - The AuthHeader/Method/SourceIP use case identifies who is accessing the workload with the user account that appears in the Authentication Header. This section defines the user accounts or Object IDs and description for each within an environment.
    - Username to identify the account or object ID in the environment.
    - Description (friendly name) of the user account in the environment.



```
<Zero_Trust_Access_Gateway_Policies>
    <Policy UserName="Object_Admin1" Method="GET" SourceIP="/10\.100\.110\..*/"></Policy>
    <Policy UserName="Object_Admin2" Method="PUT" SourceIP="/192\.168\.10\..*/"></Policy>
    <Policy UserName="Object_Admin1" Method="DELETE" SourceIP="/172\.16\.10\..*/"></Policy>
    <Policy UserName="Object_Admin3" Method="GET" SourceIP="/172\.16\.10\..*/"></Policy>
    <Policy UserName="Object_Admin3" Method="DELETE" SourceIP="/192\.168\.10\..*/"></Policy>
</Zero_Trust_Access_Gateway_Policies>
```

8. **AuthHeader/Method/ SourceIP Only** - The policy section is where the security settings are configured. Lines can be added or removed depending on the number of rules that should be applied in the policy.
    - Username to apply the security policy to.
    - The method that should be permitted for the defined path/ bucket.
        - GET
        - PUT
        - DELETE
        - POST
    - The source IP Address as to where the traffic originates from using Regular Expression (RegEx).

Any Usernames that are applied here **must** be identified in the Identify_Users section for the SteeringGroup use case above

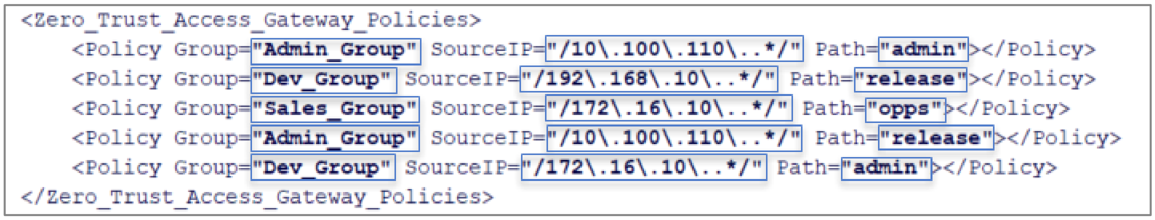


```
<Identify_Groups>
    <Group  Name="Admin_Group" Description="Administrators"></Group>
    <Group  Name="Dev_Group" Description="Developers"></Group>
    <Group  Name="Sales_Group" Description="Sales"></Group>
</Identify_Groups>
```

9. **SteeringGroup/SourceIP/Path Only** -The SteeringGroup/SourceIP/Path use case identifies who is accessing the workload with the Active Directory Group they are a member of. This section defines the Active Directory Groups and description for each within an environment.
    - Active Directory Group Names used to secure the environment.

- Description (friendly name) of the AD Groups in the environment.

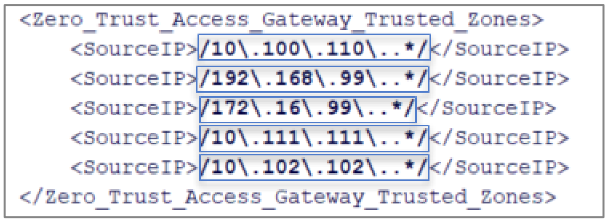
If using the ~~Steering~~ Group Use Case, the Edge Security Pack Single Sign On domain must be configured prior to running the ZTAG Policy Builder



```
<Zero_Trust_Access_Gateway_Policies>
    <Policy Group="Admin_Group" SourceIP="/10\.100\.110\..*/" Path="admin"></Policy>
    <Policy Group="Dev_Group" SourceIP="/192\.168\.10\..*/" Path="release"></Policy>
    <Policy Group="Sales_Group" SourceIP="/172\.16\.10\..*/" Path="opps"></Policy>
    <Policy Group="Admin_Group" SourceIP="/10\.100\.110\..*/" Path="release"></Policy>
    <Policy Group="Dev_Group" SourceIP="/172\.16\.10\..*/" Path="admin"></Policy>
</Zero_Trust_Access_Gateway_Policies>
```

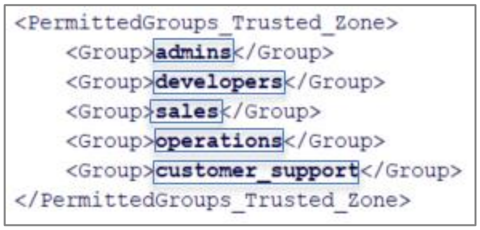
10. **SteeringGroup/SourceIP/Path Only** - The policy section is where the security settings are configured. Lines can be added or removed depending on the number of rules that should be applied in the policy.
    - Username to apply the security policy to.
    - The source IP Address as to where the traffic originates from using Regular Expression (RegEx)
    - The path of the application that the AD group should have access to.

Any Groups that are applied here **must** be identified in the Identify_Groups section for the SteeringGroup use case above



```
<Zero_Trust_Access_Gateway_Trusted_Zones>
    <SourceIP>/10\.100\.110\..*/</SourceIP>
    <SourceIP>/192\.168\.99\..*/</SourceIP>
    <SourceIP>/172\.16\.99\..*/</SourceIP>
    <SourceIP>/10\.111\.111\..*/</SourceIP>
    <SourceIP>/10\.102\.102\..*/</SourceIP>
</Zero_Trust_Access_Gateway_Trusted_Zones>
```

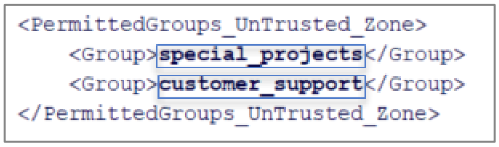
11. **Trusted/Un-Trusted Only** - The Trusted Zone section identifies the known networks in the environment. These are the networks where Multi Factor Authentication will not be required.
    - The Source IP will be the network address using Regular Expression (RegEx) that clients will be connecting from. Lines can be added or removed depending on the number of known networks in the environment.



```
<PermittedGroups_Trusted_Zone>
    <Group>admins</Group>
    <Group>developers</Group>
    <Group>sales</Group>
    <Group>operations</Group>
    <Group>customer_support</Group>
</PermittedGroups_Trusted_Zone>
```

12. **Trusted/Un-Trusted Only -** The Permitted Groups Trusted Zone section is where the Active Directory groups are defined. Members of these groups should be granted access to the application if they are connecting to the application from a network that is listed in the Trusted Zones section above. Lines can be added or removed depending on the number of groups that need access to the application.
    - Group – Active Directory group name

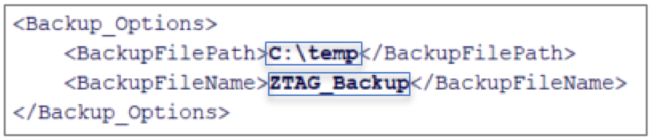
> If using the Trusted/ Un-Trusted Use Case, the Edge Security Pack Single Sign On domain for the trusted zone must be configured prior to running the ZTAG Policy Builder



```
<PermittedGroups_UnTrusted_Zone>
    <Group>special_projects</Group>
    <Group>customer_support</Group>
</PermittedGroups_UnTrusted_Zone>
```

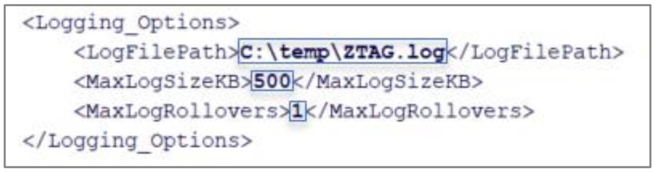
13. **Trusted/Un-Trusted Only -** The Permitted Groups Un-Trusted Zone section is where the Active Directory groups are defined. Members of these groups should be granted access to the application if they are connecting to the application from a network that is NOT listed in the Trusted Zone section above. If the same group should have access regardless of network they are connected to, the group names should be listed in both sections. Lines can be added or removed depending on the number of groups that need access to the application.
    - Group – Active Directory group name

> If using the Trusted/ Un-Trusted Use Case, the Edge Security Pack Single Sign On domain for the un-trusted zone must be configured prior to running the ZTAG Policy Builder.



```
<Backup_Options>
    <BackupFilePath>C:\temp</BackupFilePath>
    <BackupFileName>ZTAG_Backup</BackupFileName>
</Backup_Options>
```

14. Optional - During each run of the Zero Trust Policy Builder, the option to take a backup before any changes are applied is presented. These options are used to define the name and where the backup should be stored. A date and time stamp will also be included in the backup file name.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Backup file name – Used to identify the backup being taken



```
<Logging_Options>
    <LogFilePath>C:\temp\ZTAG.log</LogFilePath>
    <MaxLogSizeKB>500</MaxLogSizeKB>
    <MaxLogRollovers>1</MaxLogRollovers>
</Logging_Options>
```

15. Logging is generated for each run of the Zero Trust Policy Builder. These settings will provide the location for the log files and how much of the disk can be utilized to store files.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Max Log Size – The maximum size of each of the log files.

    Max Log Rollovers – The maximum number of log file rollovers to allow. Setting of 2 rollover files and 500KB maximum size will allow for 1000KB of storage to be used on the system running the Zero Trust Policy Builder.

Run the Zero Trust Policy Builder script

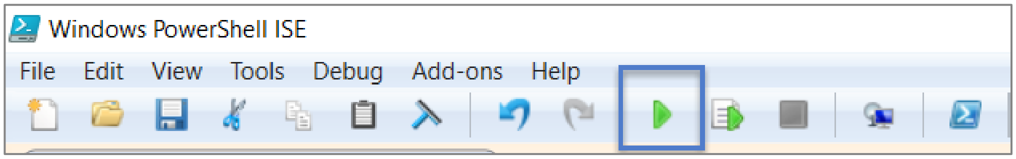
There are two approaches for running the Zero Trust Policy Builder PowerShell script. The PowerShell console and the PowerShell Integrated Scripting Environment (ISE). The interaction with the Zero Trust Policy Builder will be different between these two approaches but the results will be identical. This document will focus on using PowerShell ISE since it provides more user-friendly prompts than the PowerShell Console.

The Zero Trust Policy Builder is a fixed script that should not be modified under any circumstances.

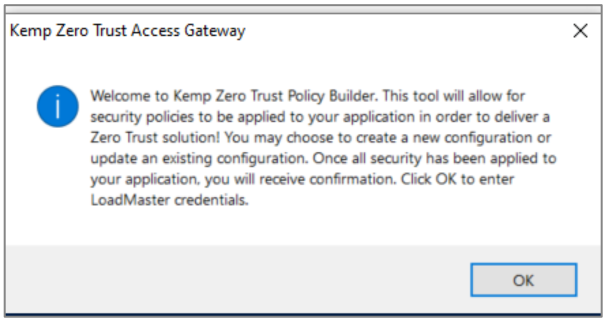
Although some interaction that is presented are common across the different use cases, there are some unique for each.

Deploy a new workload

1. Open the ZTAG-Policy-Builder.ps1 script using PowerShell ISE.

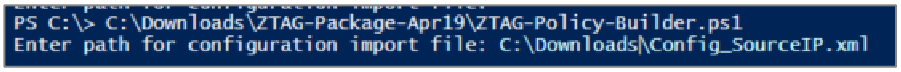


2. Click the Green Arrow to run the ZTAG Policy Builder script.


Kemp Zero Trust Access Gateway

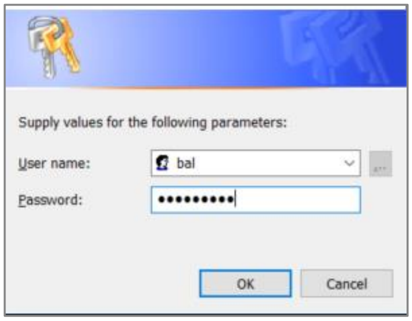
Welcome to Kemp Zero Trust Policy Builder. This tool will allow for security policies to be applied to your application in order to deliver a Zero Trust solution! You may choose to create a new configuration or update an existing configuration. Once all security has been applied to your application, you will receive confirmation. Click OK to enter LoadMaster credentials.

3. Click OK on the Welcome Message.



```
PS C:\> C:\Downloads\ZTAG-Package-Apr19\ZTAG-Policy-Builder.ps1
Enter path for configuration import file: C:\Downloads\Config_SourceIP.xml
```

4. Enter the path to the configuration file that should be used and **Enter**

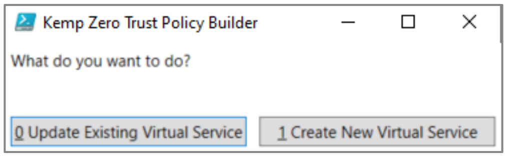


Supply values for the following parameters:

User name: bal

Password: ••••••••••

5. Enter the credentials to authenticate to the LoadMaster or ECS Connection Manager.

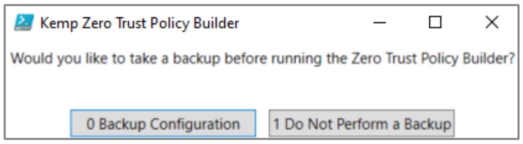


Kemp Zero Trust Policy Builder

What do you want to do?

0 Update Existing Virtual Service
1 Create New Virtual Service

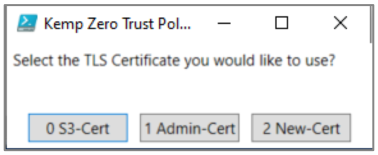
6. Select **Create New Virtual Service**



Kemp Zero Trust Policy Builder

Would you like to take a backup before running the Zero Trust Policy Builder?

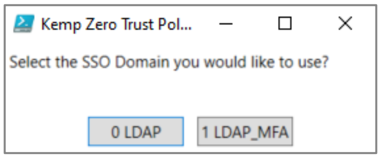
7. Choose whether to perform a backup prior to making any updates on the LoadMaster/ ECS Connection Manager.



Kemp Zero Trust Pol...

Select the TLS Certificate you would like to use?

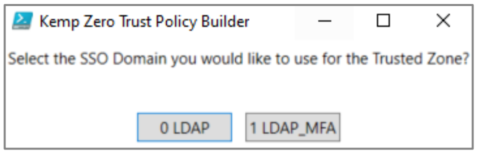
8. If enable TLS was set to "Y" in the configuration file and no parameters were provided to add a new certificate, a prompt to select an existing certificate is provided.



Kemp Zero Trust Pol...

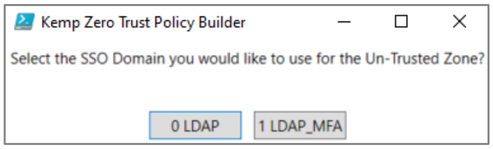
Select the SSO Domain you would like to use?

9. **(Steering Group Use Case Only)** – A prompt is presented to select an existing SSO domain to use to pre-authenticate users.



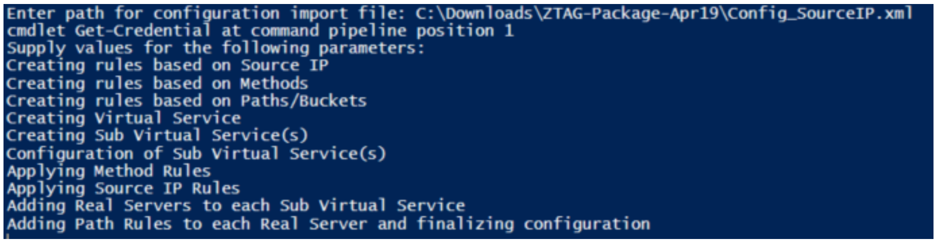
Select the SSO Domain you would like to use for the Trusted Zone?

10. **(Trusted/UnTrusted Zone Use Case Only)** – Select the SSO domain to use for known networks within the environment.



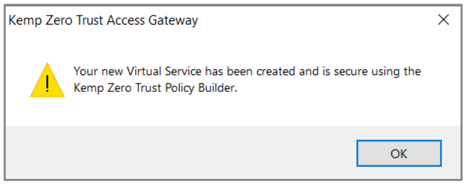
Select the SSO Domain you would like to use for the Un-Trusted Zone?

11. **(Trusted/UnTrusted Zone Use Case Only)** – Select the SSO domain to use for all other networks that do not exist in the environment.



```
Enter path for configuration import file: C:\Downloads\ZTAG-Package-Apr19\Config_SourceIP.xml
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Creating rules based on Source IP
Creating rules based on Methods
Creating rules based on Paths/Buckets
Creating Virtual Service
Creating Sub Virtual Service(s)
Configuration of Sub Virtual Service(s)
Applying Method Rules
Applying Source IP Rules
Adding Real Servers to each Sub Virtual Service
Adding Path Rules to each Real Server and finalizing configuration
```

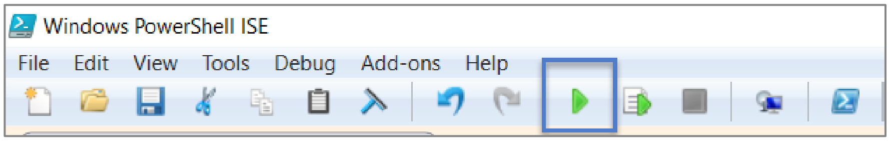
12. The script steps will be presented as the configuration takes place.



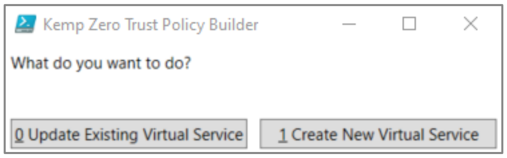
Your new Virtual Service has been created and is secure using the Kemp Zero Trust Policy Builder.

13. A confirmation that the script ran successfully will be presented at completion.

Update an existing workload

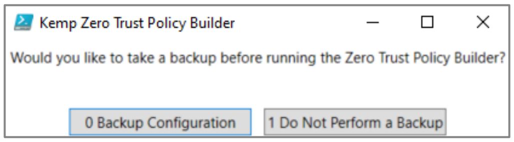


1. Run the script and accept the welcome message


Kemp Zero Trust Policy Builder
0 Update Existing Virtual Service
1 Create New Virtual Service

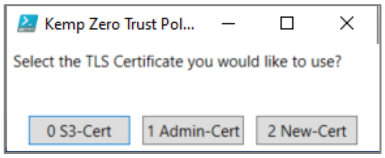
What do you want to do?

2. Select **Update Existing Virtual Service**



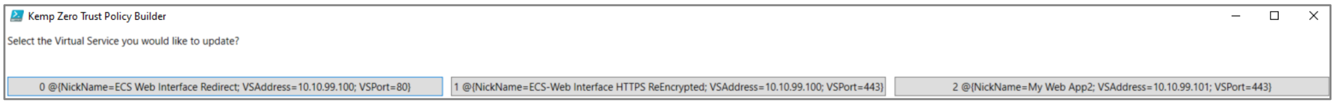
Would you like to take a backup before running the Zero Trust Policy Builder?

3. Choose whether to perform a backup prior to making any updates on the LoadMaster/ ECS Connection Manager.



Select the TLS Certificate you would like to use?

4. If enable TLS was set to “Y” in the configuration file and no parameters were provided to add a new certificate, a prompt to select an existing certificate is provided.


Kemp Zero Trust Policy Builder
0 @{NickName=ECS Web Interface Redirect; VSAddress=10.10.99.100; VSPort=80}
1 @{NickName=ECS-Web Interface HTTPS ReEncrypted; VSAddress=10.10.99.100; VSPort=443}
2 @{NickName=My Web App2; VSAddress=10.10.99.101; VSPort=443}

Select the Virtual Service you would like to update?

5. Select the Virtual Service you would like updated.
6. The remaining prompts will be identical to the steps outlined above.