

# Inbound Autoscaling with Transit Gateway

*Runbook*

**Matt McLimans**  
Public Cloud Consultant Engineer

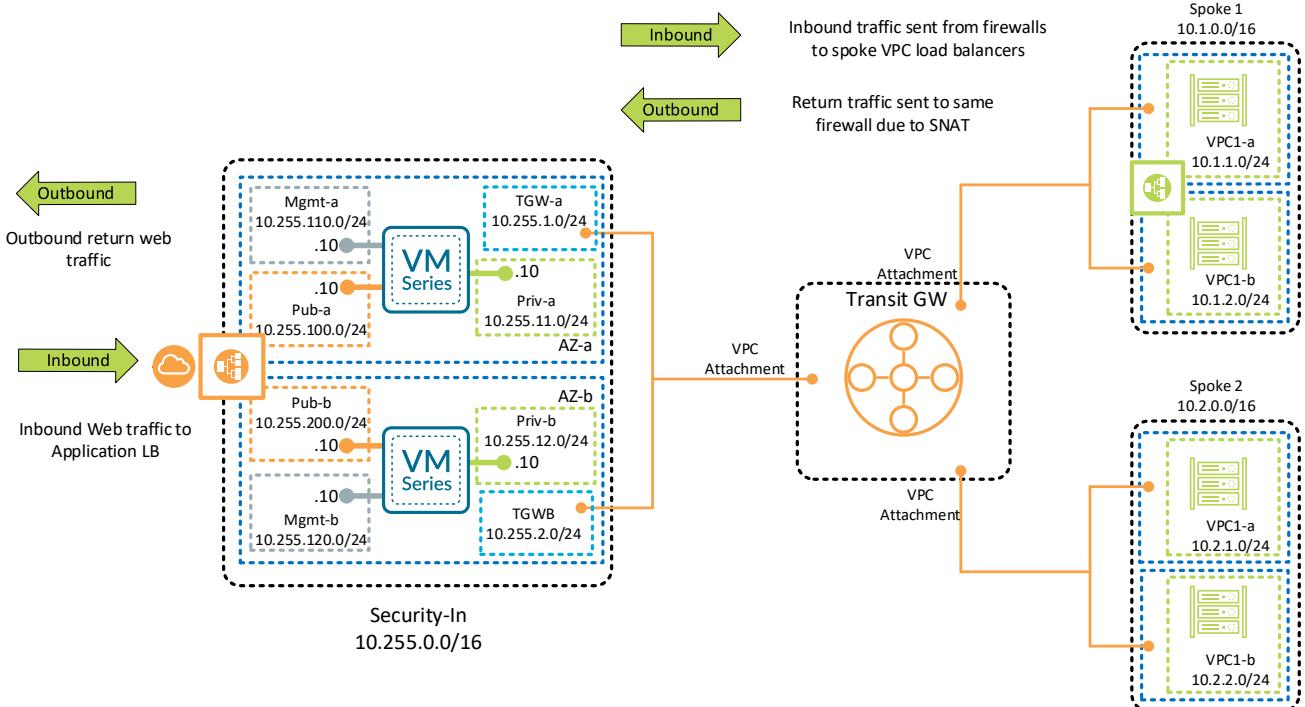


# SUPPORT POLICY

This is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself. Unless explicitly tagged, all projects or work posted in our GitHub repository (at <https://github.com/PaloAltoNetworks>) or sites other than our official Downloads page on <https://support.paloaltonetworks.com> are provided under the best effort policy.

# DEPLOYMENT OVERVIEW

- The build creates VM-Series firewalls that can secure inbound traffic flows to Spoke VPCs connected to a TGW.
- VM-Series can horizontal scale based on performance demand.
- Spoke VPCs are deployed to automatically connect to TGW.
- Lambda automatically creates a NAT policy when an NLB is created within a Spoke VPC.



# BUILD STEPS

## 1. Prepare Environment

1. Create S3 Bucket for VM-Series bootstrap & Lambda packages
2. Create Transit Gateway
3. Create 2 empty TGW Route Tables

## 2. Launch VM-Series CFT

- vmseries\_asg\_tgw.template

## 3. Launch the testapp.template

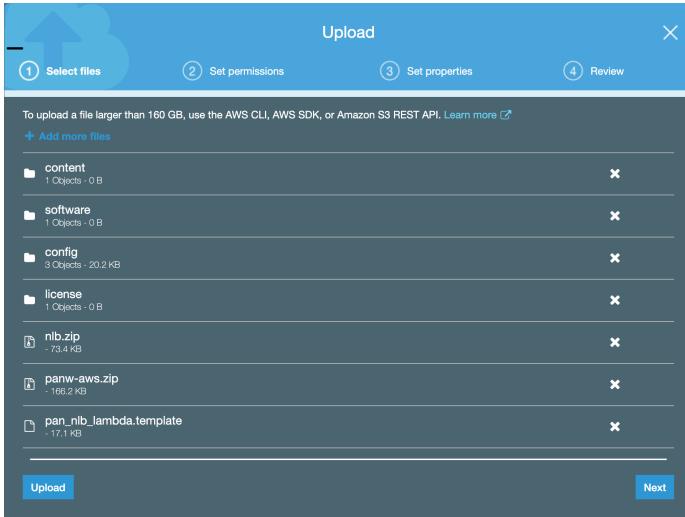
- app\_asg\_tgw.template



Prepare Environment

# STEP 1. CREATE AN S3 BUCKET

1. Create an S3 bucket in your deployment region.
2. Drag-n-drop all files & folders in /bootstrap\_files to the bucket.



Note: The nlb.zip and pan\_nlb\_lambda.template can be omitted if you are not using the application template.

Your S3 bucket should look like this before continuing

The screenshot shows the AWS S3 'mcilmans-vmseries-tgw-asg' bucket overview. The navigation bar has tabs for Overview, Properties, Permissions, and Management (which is selected). A search bar at the top says 'Type a prefix and press Enter to search. Press ESC to clear.' Below are buttons for Upload, Create folder, Download, and Actions. The location is listed as US West (Oregon). The main table lists the uploaded files:

Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
nlb.zip	Aug 9, 2019 10:19:35 AM GMT-0400	73.4 KB	Standard
pan_nlb_lambda.template	Aug 9, 2019 10:19:33 AM GMT-0400	17.1 KB	Standard
panw-aws.zip	Aug 9, 2019 10:19:36 AM GMT-0400	166.2 KB	Standard

Note: If you are using BYOL for the VM-Series, paste your auth codes inside the /license/authcodes file. The authcodes must be registered to your PANW support account prior to deployment.



## STEP 2. CREATE TRANSIT GATEWAY

1. Go to **VPC → Transit Gateways → Create Transit Gateway**
2. **Uncheck Default Route Table Association and Default Route Table Propagation.**

The screenshot shows the AWS VPC console. In the left sidebar, under the 'Transit Gateways' section, 'Transit Gateways' is highlighted. The main area displays a message: 'You do not have any Transit Gateways in this region'. Below this, a button labeled 'Create Transit Gateway' is visible. At the top, there is a navigation bar with tabs like 'Services', 'Resource Groups', and 'Actions', along with a search bar and user information.

The screenshot shows the 'Create Transit Gateway' dialog box. It includes fields for 'Name tag' (tgw) and 'Description' (Demo Transit Gateway). The 'Configure the Transit Gateway' section contains several settings:

- Amazon side ASN: 64512
- DNS support:  enable
- VPN ECMP support:  enable
- Default route table association:  enable
- Default route table propagation:  enable

A red box highlights the 'Default route table association' and 'Default route table propagation' checkboxes. At the bottom, a red arrow points to the 'Create Transit Gateway' button, which is also highlighted with a red box. A note at the bottom left indicates '\* Required'.



# STEP 3. CREATE TRANSIT GATEWAY ROUTE TABLES

1. Go to **VPC → Transit Gateway Route Tables**
2. Create two Route Tables (1 for spoke attachments, 1 for security attachment)

Create Transit Gateway Route Table

A route table controls how traffic flows for all associated attachments.

Name tag: security-rtb

Transit Gateway ID\*: tgw-00276cd598dce470b

\* Required

Create Transit Gateway Route Table

Create Transit Gateway Route Table

A route table controls how traffic flows for all associated attachments.

Name tag: spoke-rtb

Transit Gateway ID\*: tgw-00276cd598dce470b

\* Required

Create Transit Gateway Route Table

Record your TGW ID & TGW Route Table IDs

Transit Gateways

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

Traffic Mirroring

Create Transit Gateway Route Table Actions

Filter by tags and attributes or search by keyword

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default as
	tgw-rtb-0224a3170b6a56bf4	tgw-00276cd598dce470b	available	Yes
security-rtb	tgw-rtb-012d21816100a6fa8	tgw-00276cd598dce470b	available	No
spoke-rtb	tgw-rtb-0a007e7f79998b5c6	tgw-00276cd598dce470b	available	No



# LAUNCH VM-SERIES TEMPLATE

# LAUNCH THE VM-SERIES AUTOSCALING CFT

1. Go to **CloudFormation → Create Stack**
2. Select **Upload a template file**
3. Upload the **vmseries\_asg\_tgw.template**

**Create stack**

**Prerequisite - Prepare template**

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready    Use a sample template    Create template in Designer

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL    Upload a template file

Upload a template file  
 `vmseries_asg_tgw.template`  
JSON or YAML formatted file

S3 URL: `https://s3-us-west-2.amazonaws.com/cf-templates-l3397x2426v3-us-west-2/2019221bYM-vmseries_asg_tgw.template`



# VPC Parameters

## Stack name

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Enter name for Stack.

## VPC Parameters

VPC Name

Name of the VM-Series VPC

Availability Zones (max 2)

Select two availability zones for VPC's subnetworks

us-west-2a X

us-west-2b X

Select 2 Availability Zones.

ALB Name:

Name of the external Application Load Balancer



# VM-Series Parameters

## VM-Series Parameters

### VM-Series AMI

AMI List: <https://www.paloaltonetworks.com/documentation/global/compatibility-matrix/vm-series-firewalls/aws-cft-amazon-machine-images-ami-list>

### Key Pair

EC2 Key Pair

### Security Group Source Prefix

Source address to restrict access to the VM-Series (enter a valid CIDR range in the format of x.x.x.x/x)

### Bootstrap Bucket

Name of the S3 bucket to bootstrap the VM-Series

Enter the VM-Series AMI to match the license SKU, PAN-OS

Version, and AWS Region

\* screenshot shows: bundle1, 8.1, us-west-2

Enter the S3 Bucket name from step 1



# Lambda Parameters

## Lambda Parameters

### Lambda Bucket

Name of the S3 Bucket that contains Lambda scripts and CFTs

### API Key - Firewall

API key of VM-Series user. Default: pandemo/demopassword

### API Key - Panorama

API key associated with Panorama user

### API Key - Delicense

API key to delicense: <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/virtualization-features/vm-series-license-deactivation-api-key>

### Enable Debugging

Enter the S3 Bucket name from step 1.

If you are using the default bootstrap.xml, leave the default key. Do not use default bootstrap.xml for any real environments.



# Transit Gateway Parameters

## Transit Gateway Parameters

Transit Gateway ID:

Transit Gateway resource ID (i.e. tgw-xxxxxx)

tgw-00276cd598dce470b

## Transit Gateway Route Table - TO ASSOCIATE

Transit Gateway Route Table to associate with the VM-Series VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-012d21816100a6fa8

## Transit Gateway Route Table - TO PROPAGATE

Transit Gateway route table resource ID to propagate the VM-Series VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-0a007e7f79998b5c6

Filter by tags and attributes or search by keyword			
<input type="checkbox"/>	Name	Transit Gateway route table ID	Transit Gateway ID
<input type="checkbox"/>	tgw-rtb-0224a3170b6a56bf4	tgw-00276cd598dce470b	
<input type="checkbox"/>	security-rtb	tgw-rtb-012d21816100a6fa8	tgw-00276cd598dce470b
<input type="checkbox"/>	spoke-rtb	tgw-rtb-0a007e7f79998b5c6	tgw-00276cd598dce470b

Paste TGW ID from Step 2

Paste Security TGW-RTB ID. This will be associated with the VM-Series VPC.

Paste the Spoke TGW-RTB. The VM-Series VPC will propagate its route to it.



# Post Completion Check

CloudFormation > Stacks: security-in

**Stacks (1)**

Active

View nested

security-in  
2019-08-09 10:53:17 UTC-0400  
CREATE\_COMPLETE

**Outputs (11)**

Key	Value
BootstrapS3Bucket	arn:aws:s3:::mclimans-vmseries-tgw-asg
ELBDNSName	vmseries-alb-737962544.us-west-2.elb.amazonaws.com
ELBName	vmseries-alb
KeyName	mrm-westus2-key
LambdaCodeFile	panw-aws.zip
LambdaS3Bucket	arn:aws:s3:::mclimans-vmseries-tgw-asg
NATGateway1	52.25.33.100
NATGateway2	54.68.50.32
NetworkLoadBalancerQueue	<a href="https://sns.us-west-2.amazonaws.com/704043199546/security-in-NetworkLoadBalancerQueue-P9OJCA85GQMP">https://sns.us-west-2.amazonaws.com/704043199546/security-in-NetworkLoadBalancerQueue-P9OJCA85GQMP</a>
SSHLlocation	0.0.0.0/0
ScalingParameter	DataPlaneCPUUtilizationPct

Filter by tags and attributes or search by keyword

1 to 3 of 3

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association	Default propagation
tgw-rb-0224a3170b6a56bf4	tgw-00276cd598dce470b	available	Yes	Yes	Yes
<b>security-rtb</b>	<b>tgw-rb-012d21816100a6fa8</b>	<b>tgw-00276cd598dce470b</b>	<b>available</b>	<b>No</b>	<b>No</b>
spoke-rtb	tgw-rb-0a007e7f79998b5c6	tgw-00276cd598dce470b	available	No	No

**Transit Gateway Route Table: tgw-rb-012d21816100a6fa8**

Details Associations Propagations Routes Tags

Create association Delete association

Filter by attributes or search by keyword

1 to 1 of 1

Attachment ID	Resource type	Resource ID	State
tgw-attach-0ca4e42a92bea9ee3	VPC	vpc-0669ec71f1ad20b0a	associated

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association	Default propagation
tgw-rb-0224a3170b6a56bf4	tgw-00276cd598dce470b	available	Yes	Yes	Yes
security-rtb	tgw-rb-012d21816100a6fa8	tgw-00276cd598dce470b	available	No	No
<b>spoke-rtb</b>	<b>tgw-rb-0a007e7f79998b5c6</b>	<b>tgw-00276cd598dce470b</b>	<b>available</b>	<b>No</b>	<b>No</b>

**Transit Gateway Route Table: tgw-rb-0a007e7f79998b5c6**

Details Associations Propagations Routes Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

1 to 1 of 1

CIDR	Attachment	Resource type	Route type	Route state
10.255.0.0/16	tgw-attach-0ca4e42a92bea9ee3   vpc-0669ec71f1ad20b0a	VPC	propagated	active



# LAUNCH APPLICATION TEMPLATE

# LAUNCH THE APPLICATION CFT

1. Go to **CloudFormation → Create Stack**
2. Select **Upload a template file**
3. Upload the **app\_tgw\_template.template**

**Create stack**

**Prerequisite - Prepare template**

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready    Use a sample template    Create template in Designer

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL    Upload a template file

Upload a template file  
 app\_asg\_tgw.template  
JSON or YAML formatted file

S3 URL: [https://s3-us-west-2.amazonaws.com/cf-templates-l3397x2426v3-us-wes-t-2/2019221iyR-app\\_asg\\_tgw.template](https://s3-us-west-2.amazonaws.com/cf-templates-l3397x2426v3-us-wes-t-2/2019221iyR-app_asg_tgw.template)  



# VPC Parameters

## Stack name

Stack name

spoke1

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Enter name for Stack.

## VPC Parameters

### VPC Prefix

Spoke VPC Prefix

10.1.0.0/16

### Subnet Availability Zones

Select two availability zones for Spoke VPC's subnetworks

us-west-2a 

us-west-2b 

Select 2 Availability Zones.

### Subnet Prefixes

In a comma separated list, enter the spoke VPC's subnetworks prefixes

10.1.1.0/24, 10.1.2.0/24



# Application Parameters

## Application Parameters

### NLB Name

The name of the internal NLB for the application instances

### Application Instance Type

Application Instance Size

### Key Pair

EC2 Key Pair

### Security Group Source Prefix

Source address to restrict access to the application instances (enter a valid CIDR range in the format of x.x.x.x/x)

Name for NLB. The name cannot conflict with an existing NLB.

Select existing EC2 Key Pair.



# Lambda Parameters

## Lambda Parameters

### Lambda Bucket

Name of the S3 Bucket that contains Lambda scripts and CFTs

mclimans-vmseries-tgw-asg

### VM-Series SQS URL

Enter the URL of the Queue (SQS) to send NLB updates

<https://sq.s.us-west-2.amazonaws.com/704043199546/security-in-NetworkLoadBalancerQueue-P9OJCA85GC>

### DynamoDB Table

Enter the name of the DynamoDB table

nlb\_db\_tbl

## security-in

Stack info | Events | Resources | **Outputs** | Parameters | Template | Change

### Outputs (11)

Search outputs

Key	Value
BootstrapS3Bucket	arn:aws:s3:::mclimans-vmseries-tgw-asg
ELBDNSName	vmseries-alb-737962544.us-west-2.elb.amazonaws.com
ELBName	vmseries-alb
KeyName	mrm-westus2-key
LambdaCodeFile	panw-aws.zip
LambdaS3Bucket	arn:aws:s3:::mclimans-vmseries-tgw-asg
NATGateway1	52.25.33.100
NATGateway2	54.68.50.32
NetworkLoadBalancerQueue	<a href="https://sq.s.us-west-2.amazonaws.com/704043199546/security-in-NetworkLoadBalancerQueue-P9OJCA85GQMP">https://sq.s.us-west-2.amazonaws.com/704043199546/security-in-NetworkLoadBalancerQueue-P9OJCA85GQMP</a>
SSHLocation	0.0.0.0/0
ScalingParameter	DataPlaneCPUUtilizationPct



# Transit Gateway Parameters

## Transit Gateway Parameters

### Transit Gateway ID

Transit Gateway resource ID (i.e. tgw-xxxxxx)

tgw-00276cd598dce470b

### Transit Gateway Route Table - SPOKE

Transit Gateway Route Table to associate with the spoke VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-0a007e7f79998b5c6

### Transit Gateway Route Table - SECURITY

Transit Gateway route table resource ID to propagate the spoke VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-012d21816100a6fa8

Filter by tags and attributes or search by keyword			
<input type="checkbox"/>	Name	Transit Gateway route table ID	Transit Gateway ID
<input type="checkbox"/>	tgw-rtb-0224a3170b6a56bf4	tgw-00276cd598dce470b	
<input type="checkbox"/>	security-rtb	tgw-rtb-012d21816100a6fa8	tgw-00276cd598dce470b
<input type="checkbox"/>	spoke-rtb	tgw-rtb-0a007e7f79998b5c6	tgw-00276cd598dce470b

Paste TGW ID from Step 2

Paste the Spoke TGW-RTB. The Spoke VPC will be associated with it.

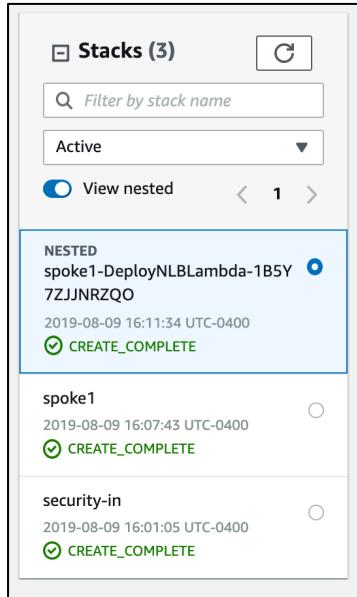
Paste Security TGW-RTB ID. The Spoke VPC will propagate its route to it.



# Test Deployment

# TEST DEPLOYMENT

Once deployment is complete, copy the DNS record of the public ELB and place it in a web-browser.



← → ⌛ vmseries-alb-737962544.us-west-2.elb.amazonaws.com

**SOURCE & DESTINATION ADDRESSES**  
INTERVAL: 0.00026297569274902  
SOURCE IP: 68.0.234.87  
LOCAL IP: ip-10-1-2-195  
VM NAME: ip-10-1-2-195

**HEADER INFORMATION**  
HTTP\_X\_FORWARDED\_FOR: 68.0.234.87  
HTTP\_X\_FORWARDED\_PROTO: http  
HTTP\_X\_FORWARDED\_PORT: 80  
HTTP\_HOST: vmseries-alb-1281801741.us-west-2.elb.amazonaws.com  
HTTP\_X\_AMZN\_TRACE\_ID: Root=1-5d4dd782-1198bd7cf4b302b0a7c235fc  
HTTP\_CACHE\_CONTROL: max-age=0  
HTTP\_UPGRADE\_INSECURE\_REQUESTS: 1  
HTTP\_USER\_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36  
HTTP\_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3  
HTTP\_ACCEPT\_ENCODING: gzip, deflate  
HTTP\_ACCEPT\_LANGUAGE: en-US,en;q=0.9

**Web-App-2**

← → ⌛ vmseries-alb-737962544.us-west-2.elb.amazonaws.com

**SOURCE & DESTINATION ADDRESSES**  
INTERVAL: 0.00023698806762695  
SOURCE IP: 68.0.234.87  
LOCAL IP: ip-10-1-1-62  
VM NAME: ip-10-1-1-62

**HEADER INFORMATION**  
HTTP\_X\_FORWARDED\_FOR: 68.0.234.87  
HTTP\_X\_FORWARDED\_PROTO: http  
HTTP\_X\_FORWARDED\_PORT: 80  
HTTP\_HOST: vmseries-alb-1281801741.us-west-2.elb.amazonaws.com  
HTTP\_X\_AMZN\_TRACE\_ID: Root=1-5d4dd803-3171870cc237431cd045dd8c  
HTTP\_CACHE\_CONTROL: max-age=0  
HTTP\_UPGRADE\_INSECURE\_REQUESTS: 1  
HTTP\_USER\_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36  
HTTP\_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3  
HTTP\_ACCEPT\_ENCODING: gzip, deflate  
HTTP\_ACCEPT\_LANGUAGE: en-US,en;q=0.9

**Web-App-1**