CLOUDDADDY

Cloud Daddy Easy Instance Firewall 1.0

USER GUIDE

CLOUD DADDY, INC
WEB: HTTPS://WWW.CLOUDDADDY.COM
E-MAIL: INFO@CLOUDDADDY.COM

Contents

Introduction

Cloud Daddy Easy Instance Firewall (EIF) is a desktop security solution built specifically for Amazon Web Service (AWS). The solution simplifies AWS instance firewall configuration, working with security groups and provides tools for firewall logging.

Solution Architecture

EIF is a Windows-based desktop application that connects to your AWS infrastructure using AWS APIs to manage the overall security of instances. EIF provides an easy to use front-end interface for AWS firewall management.

Setup

The setup of EIF consists of the following stages:

1. EIF installation.
2. EIF configuration.

EIF installation

The first stage is typical for any Windows-based product installation. You only need to choose the 32 or 64-bit version to install.

EIF configuration

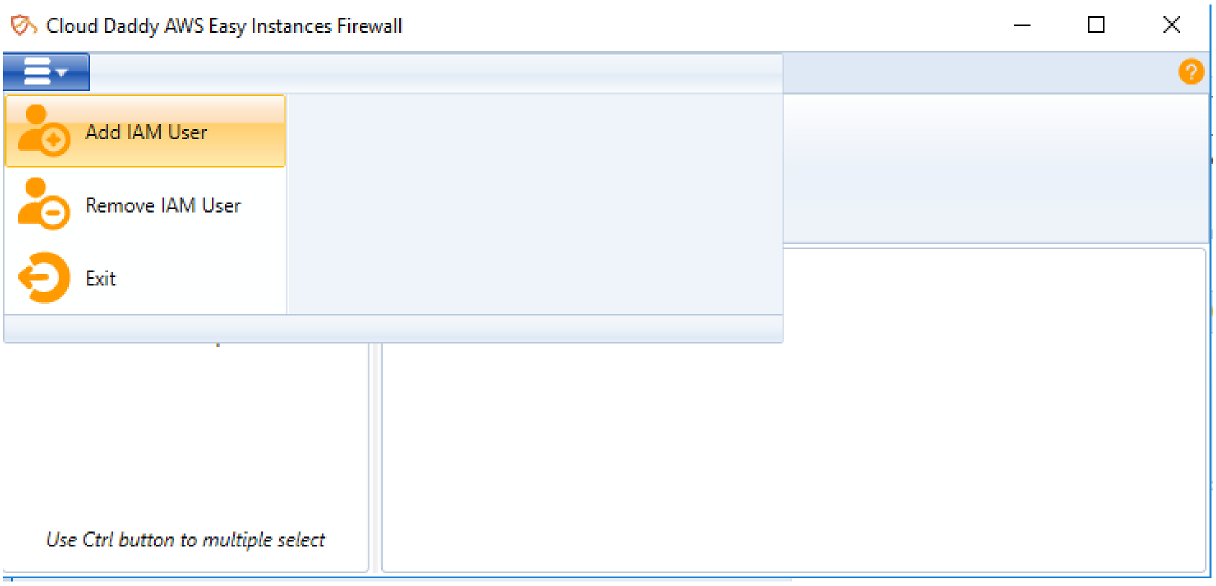
The first time you start the application, you will need to set the **Access Key ID**, **Secret Access Key** and new **Key Word.** All configurations will be stored within this account. As a security precaution, whenever you run the application later, you will need to submit the same information to attain access and restore the configurations.

You must add users in order to use the application’s functionality. To do this, click the **Add IAM User** button in the burger dropdown, visible in the upper left corner of the application window. Enter the **Access Key ID** and **Secret Access Key** of the IAM user and press the **OK** button.

Each IAM user has to have permissions in AWS:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSBackup",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:CreateTags",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteTags",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:ModifyInstanceAttribute",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeTags",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeFlowLogs",
                "ec2:CreateFlowLogs",
                "iam:GetUser",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListPolicies",
                "iam:AttachRolePolicy",
                "logs:CreateExportTask",
                "logs:DescribeExportTasks",
                "logs:CancelExportTask",
                "logs:DescribeLogGroups",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutBucketPolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:CreateSecret",
                "secretsmanager:DeleteSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "*"
        }
    ]
}
```

You can add several IAM users.


Cloud Daddy AWS Easy Instances Firewall
Add IAM User
Remove IAM User
Exit
Use Ctrl button to multiple select

It is also necessary to add any used AWS regions (the regions in which the protected infrastructure is located) for each user. To do this, highlight the IAM user in the tree displayed in the left window of the application and press the **Add Region** button and then select the necessary region in drop-down menu provided. You can add multiple regions.

Instance Firewall

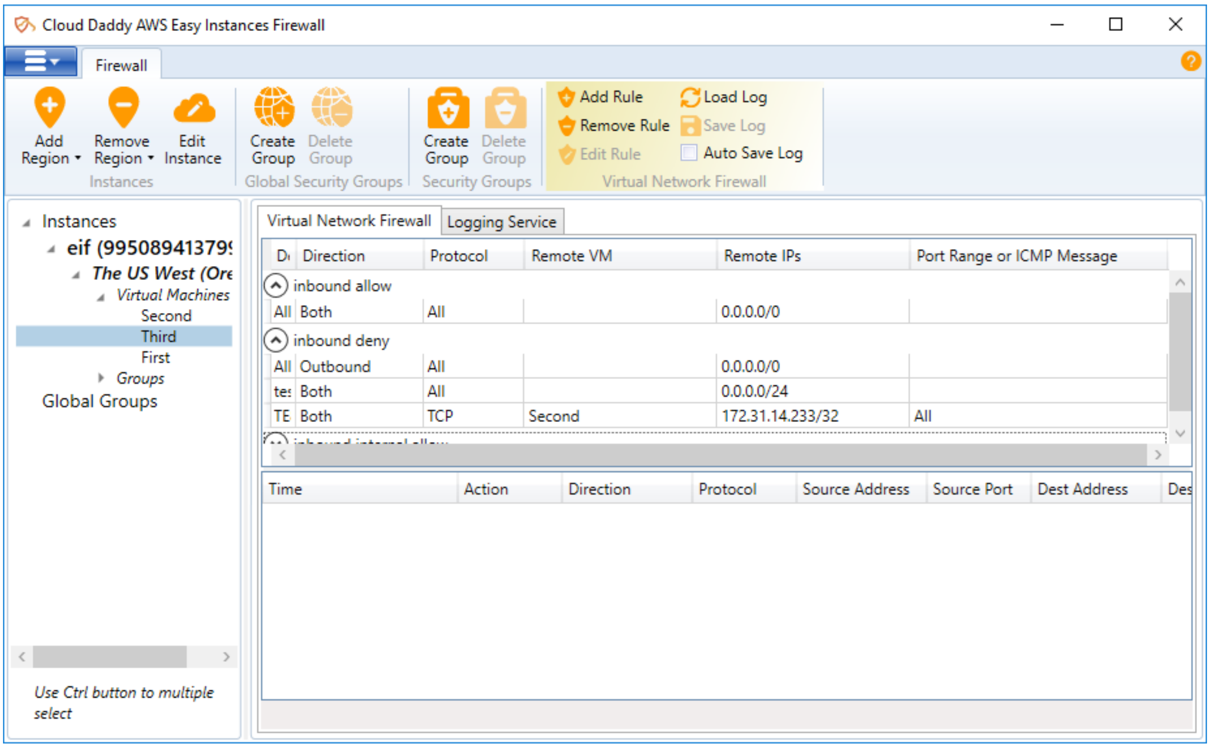
EIF provides an efficient way to manage firewall rules applied to all of your AWS instances. With EIF, you can also manage rules in all security groups.

The EIF window contains a working tree display that includes:

- Virtual Machines (EC2 instances) which are divided into IAM USERS and regions
- Groups which are divided into IAM USERS and regions
- Global groups

Virtual Machines

To manage an instance's name, rules and view firewall logs, highlight the virtual machine name in the working tree contained in the left window of the application and the related information will display within the right window of the application.

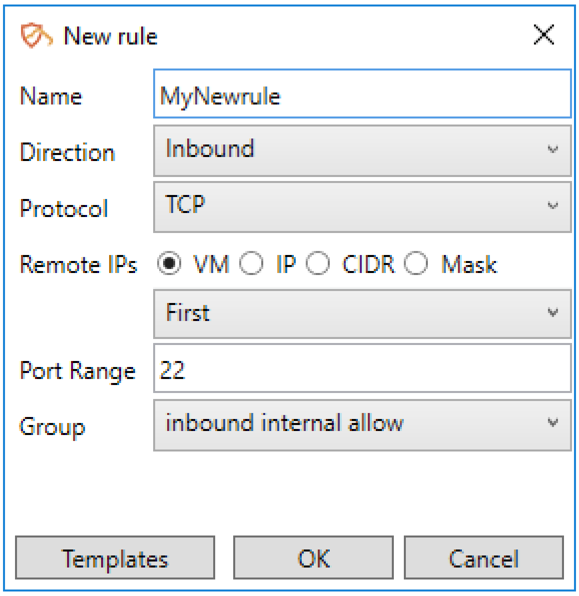


D	Direction	Protocol	Remote VM	Remote IPs	Port Range or ICMP Message
inbound allow					
All	Both	All		0.0.0.0/0	
inbound deny					
All	Outbound	All		0.0.0.0/0	
te:	Both	All		0.0.0.0/24	
TE	Both	TCP	Second	172.31.14.233/32	All

Time	Action	Direction	Protocol	Source Address	Source Port	Dest Address	Des

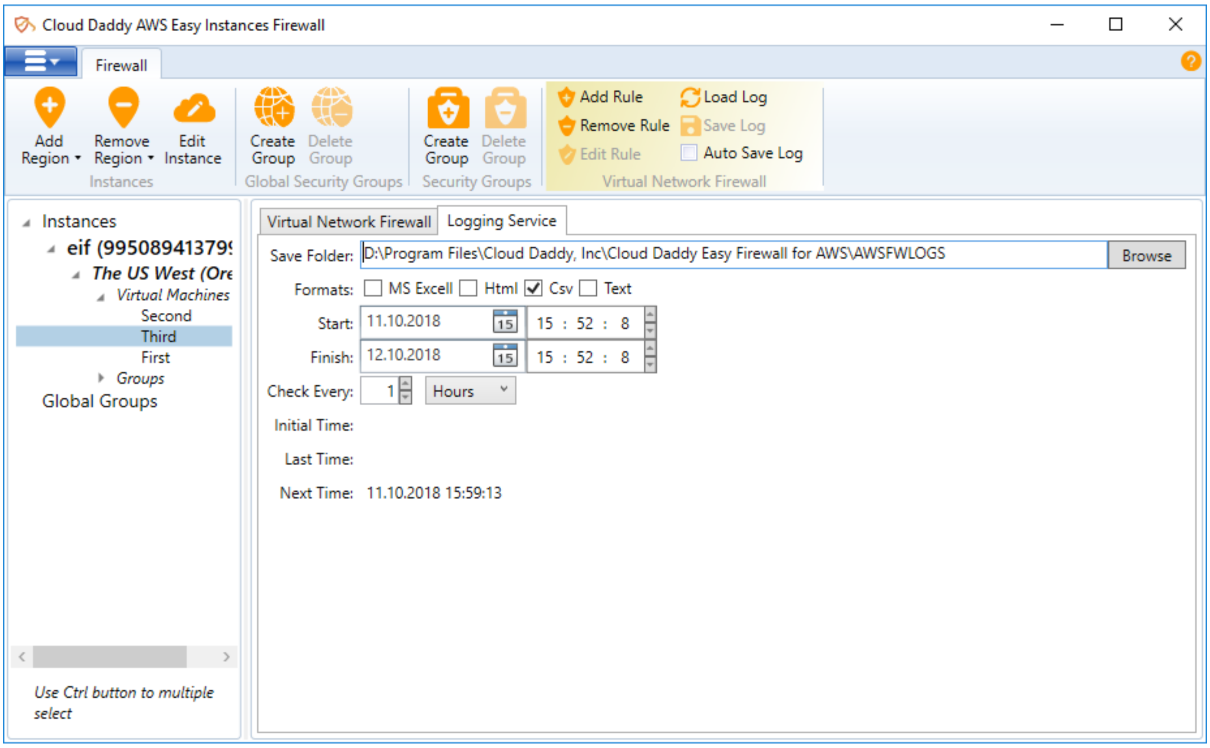
In the **Virtual Network Firewall** tab, you can see the list of groups and global groups with all firewall rules attached to them. You can add, remove or edit rules by clicking the appropriate buttons within Virtual Network Firewall panel of the top level menu. You can also load, save to file, or configure scheduled firewall logs within the **Logging Service** tab. You can change the instance name tag by clicking on the **Edit Instance** button.

To create a new rule, click **Add Rule** from the top level menu within the Virtual Network Firewall panel which will add the new rule to the existing firewall group, as shown below:



Name	MyNewrule
Direction	Inbound
Protocol	TCP
Remote IPs	● VM ○ IP ○ CIDR ○ Mask
	First
Port Range	22
Group	inbound internal allow

In the **Logging Service** tab, you can manage scheduled firewall logs to be saved at specific dates and in specific file formats.



Save Folder: D:\Program Files\Cloud Daddy, Inc\Cloud Daddy Easy Firewall for AWS\AWSFWLOGS

Formats: □ MS Excell □ Html ☑ Csv □ Text

Start: 11.10.2018 15 : 52 : 8

Finish: 12.10.2018 15 : 52 : 8

Check Every: 1 Hours

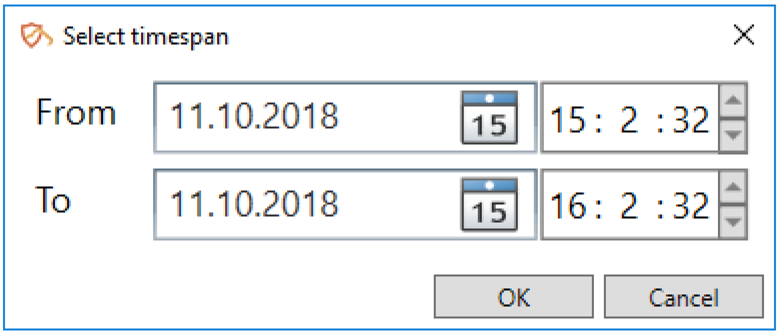
Initial Time:

Last Time:

Next Time: 11.10.2018 15:59:13

The automatic log saving feature is activated by clicking on the **Auto Save Log** check-box within the top level menu of the Virtual Network Firewall panel. Once enabled, you can set the schedule and file format desired for the firewall logs to be saved.

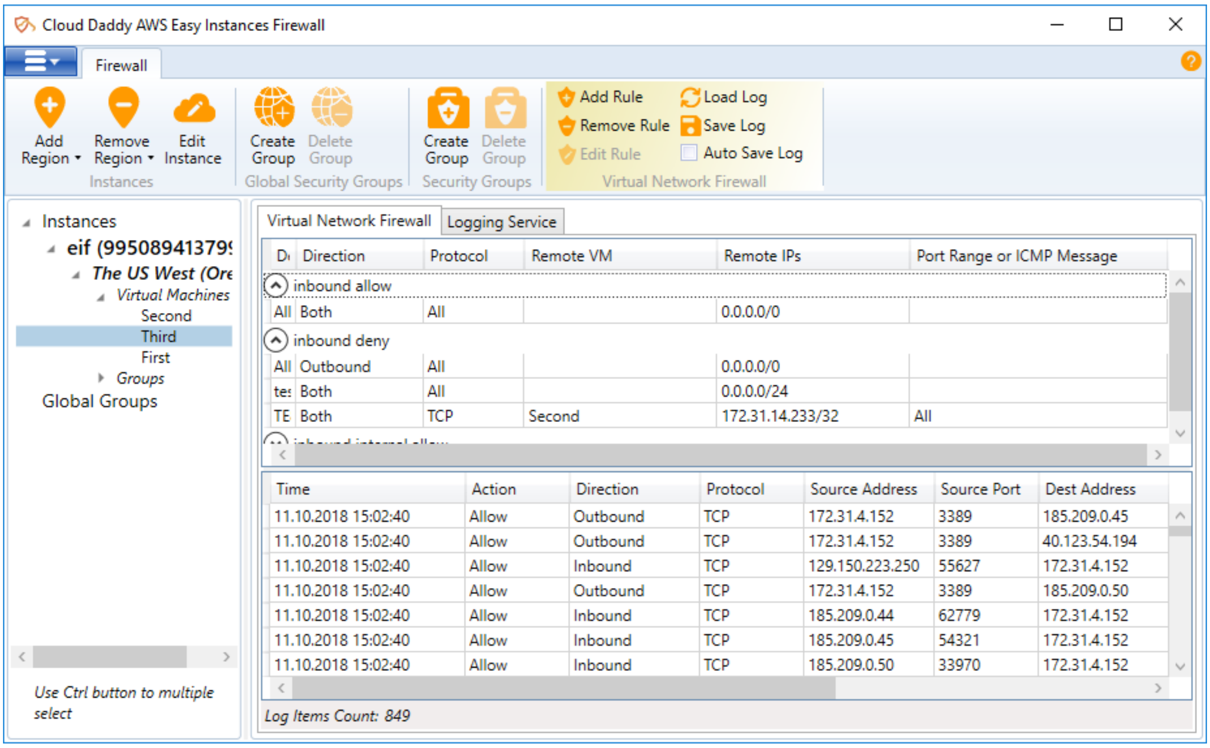
You can manually load a log by clicking on the **Load Log** button within the top level menu of the Virtual Network Firewall panel and setting the desired timeframe, as shown below.



From 11.10.2018 15: 2 :32

To 11.10.2018 16: 2 :32

Once the timespan is set, click on the **OK** button and the log will be retrieved as desired. Selecting the Virtual Network Firewall tab will display the loaded log.



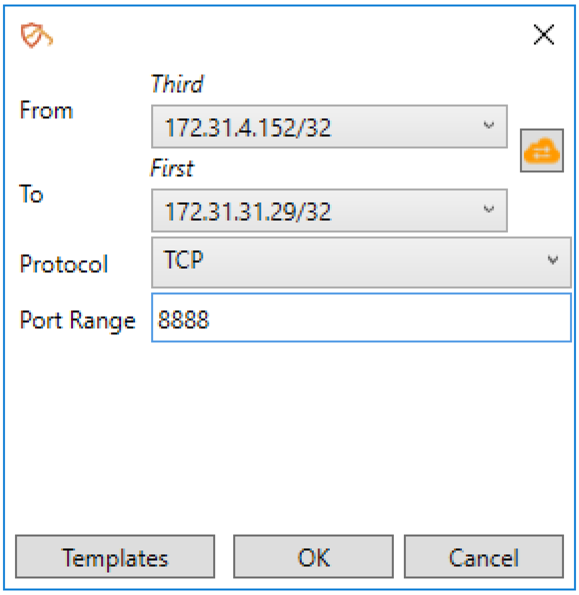
D	Direction	Protocol	Remote VM	Remote IPs	Port Range or ICMP Message
inbound allow					
All	Both	All		0.0.0.0/0	
inbound deny					
All	Outbound	All		0.0.0.0/0	
te:	Both	All		0.0.0.0/24	
TE	Both	TCP	Second	172.31.14.233/32	All

Time	Action	Direction	Protocol	Source Address	Source Port	Dest Address
11.10.2018 15:02:40	Allow	Outbound	TCP	172.31.4.152	3389	185.209.0.45
11.10.2018 15:02:40	Allow	Outbound	TCP	172.31.4.152	3389	40.123.54.194
11.10.2018 15:02:40	Allow	Inbound	TCP	129.150.223.250	55627	172.31.4.152
11.10.2018 15:02:40	Allow	Outbound	TCP	172.31.4.152	3389	185.209.0.50
11.10.2018 15:02:40	Allow	Inbound	TCP	185.209.0.44	62779	172.31.4.152
11.10.2018 15:02:40	Allow	Inbound	TCP	185.209.0.45	54321	172.31.4.152
11.10.2018 15:02:40	Allow	Inbound	TCP	185.209.0.50	33970	172.31.4.152

Log Items Count: 849

To save a retrieved log to file, press the **Save Log** button within the top level menu of the Virtual Network Firewall panel.

The application also provides the ability to create cross-instance (from – to) rules. To perform this operation, simply highlight two instances and click on the **Add Rule** button within the top level menu of the Virtual Network Firewall panel. Enter the required information and press the **OK** button. You can also flip the From-To machines by clicking on the yellow cloud button on the right side of the dialog window.



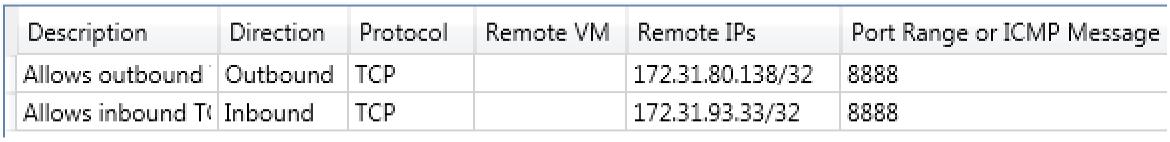
From: Third 172.31.4.152/32

To: First 172.31.31.29/32

Protocol: TCP

Port Range: 8888

The Outbound – Inbound rule pair will be created.



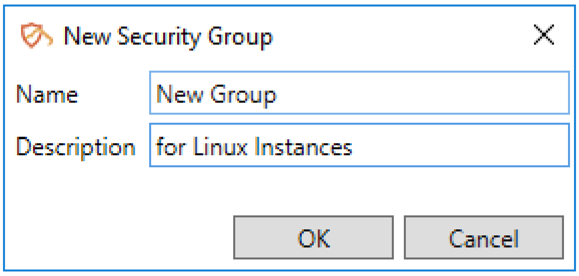
Description	Direction	Protocol	Remote VM	Remote IPs	Port Range or ICMP Message
Allows outbound	Outbound	TCP		172.31.80.138/32	8888
Allows inbound T	Inbound	TCP		172.31.93.33/32	8888

Groups

Firewall groups – which are ordinary AWS security groups that are associated with EC2 instances and provide security at the protocol and port access level, can be created by clicking on the Create Group button within the top level menu of the Security Groups panel.

EIF also includes rule templates that can be used to speed up the process of adding and customizing new firewall rules.

To create a firewall group for an EC2 instance, highlight the desired region (or any object within it) and click on the **Create Group** button within the top level menu of the Security Groups panel. A New Security Group creation form will appear.

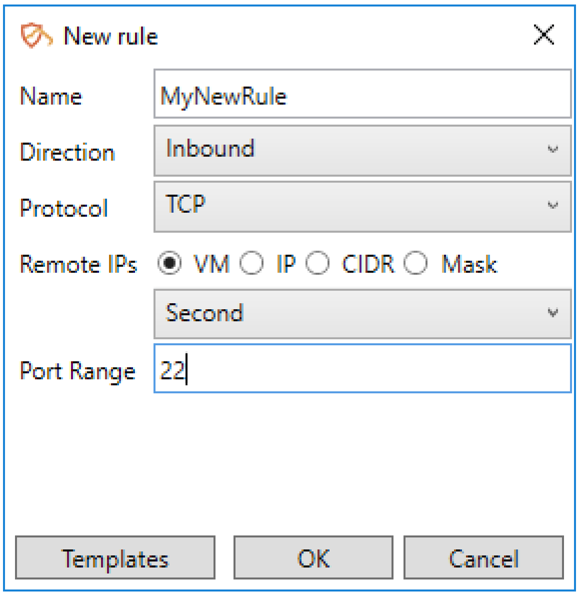


New Security Group

Name: New Group

Description: for Linux Instances

To add rules to a group, highlight the group desired and click on the **Add Rule** button.



New rule

Name: MyNewRule

Direction: Inbound

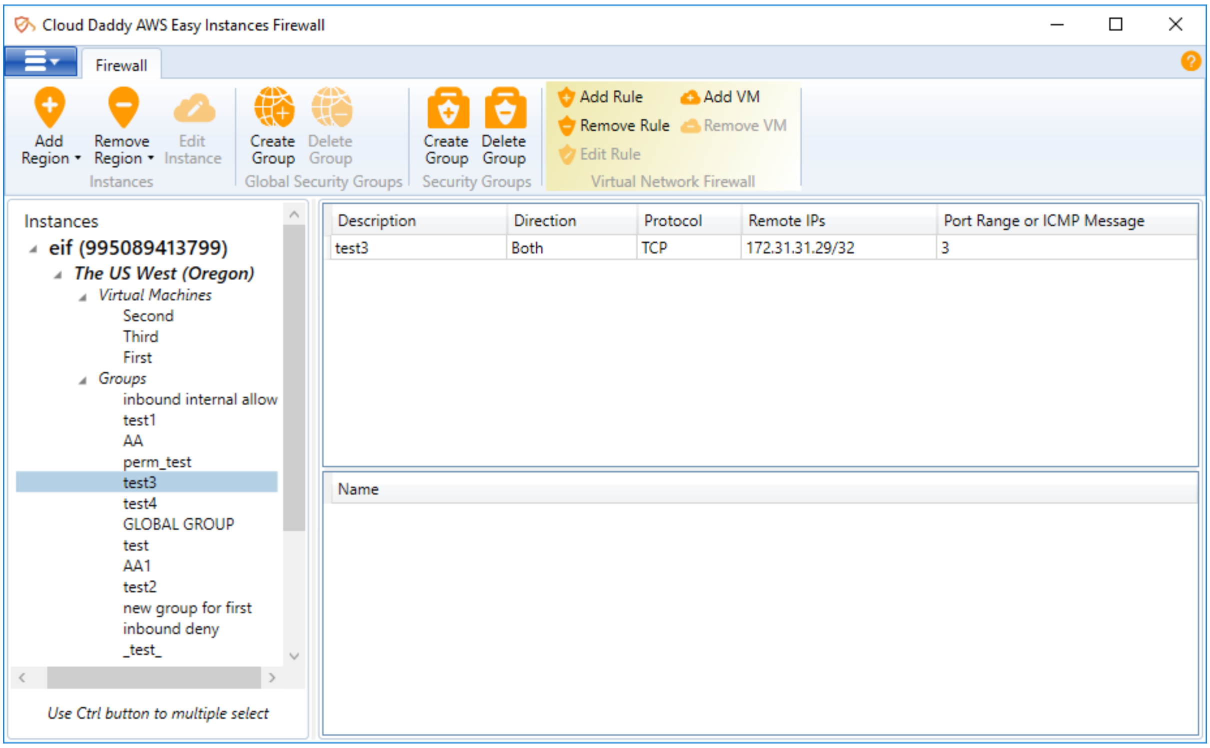
Protocol: TCP

Remote IPs: ● VM ○ IP ○ CIDR ○ Mask

Second

Port Range: 22

When done, the new rule will appear in the list of rules.



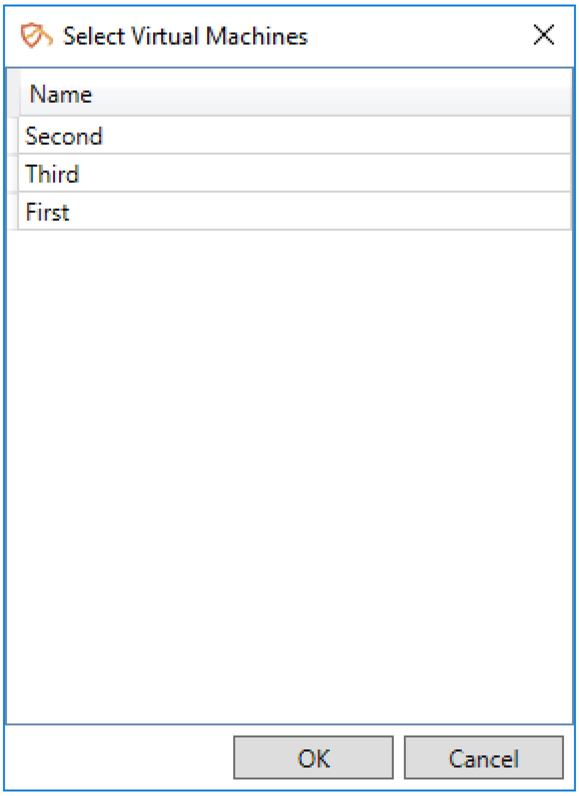
Instances
- eif (995089413799)
  - *The US West (Oregon)*
    - *Virtual Machines*
      - Second
      - Third
      - First
    - *Groups*
      - inbound internal allow
      - test1
      - AA
      - perm_test
      - test3
      - test4
      - GLOBAL GROUP
      - test
      - AA1
      - test2
      - new group for first
      - inbound deny
      - _test_

Description	Direction	Protocol	Remote IPs	Port Range or ICMP Message
test3	Both	TCP	172.31.31.29/32	3

Name

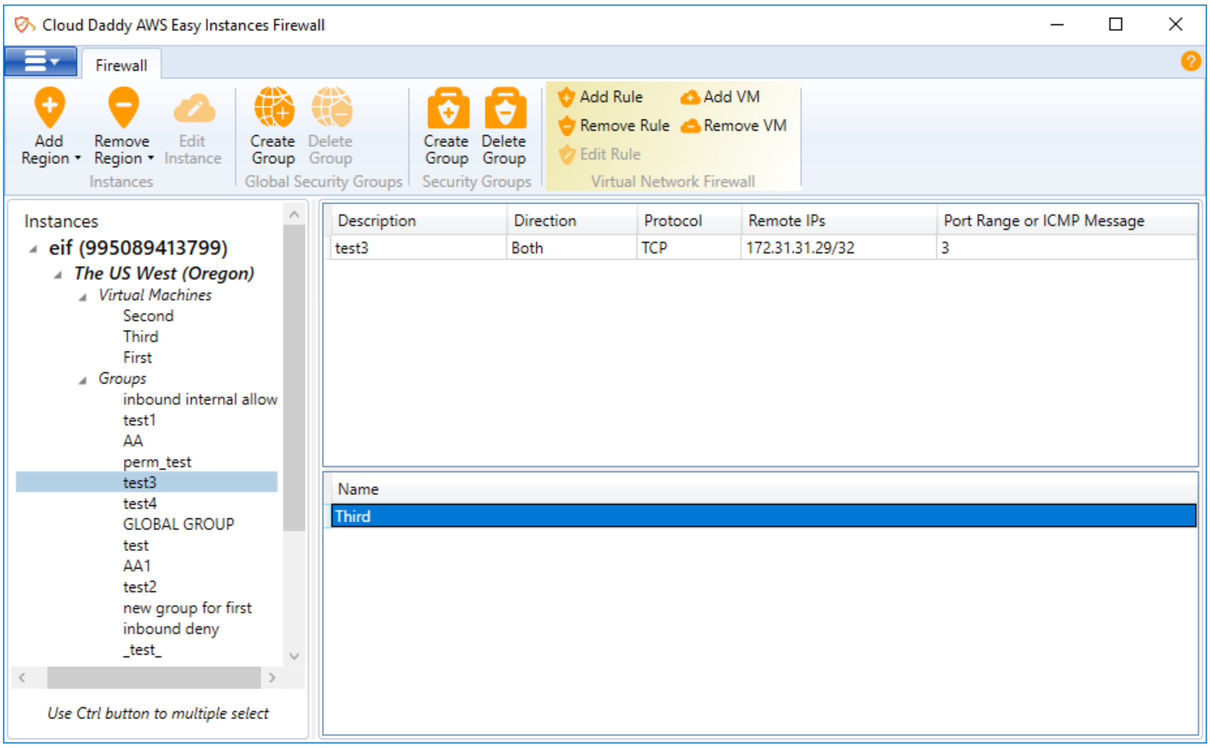
With EIF, you can also delete and edit existing rules. To do so, simply highlight a rule and click on either the **Remove Rule** or **Edit Rule** buttons.

To connect the group with an existing instance, highlight a rule and click on the **Add VM** button within the top level menu of the Virtual Network Firewall panel. A list of instances from the current account and the current region will display.



Name
Second
Third
First

Select the instance and press the **OK** button. The virtual machine will appear within the list of Instances.



Instances

- eif (995089413799)
  - *The US West (Oregon)*
    - *Virtual Machines*
      - Second
      - Third
      - First
    - *Groups*
      - inbound internal allow
      - test1
      - AA
      - perm_test
      - test3
      - test4
      - GLOBAL GROUP
      - test
      - AA1
      - test2
      - new group for first
      - inbound deny
      - _test_

Use Ctrl button to multiple select

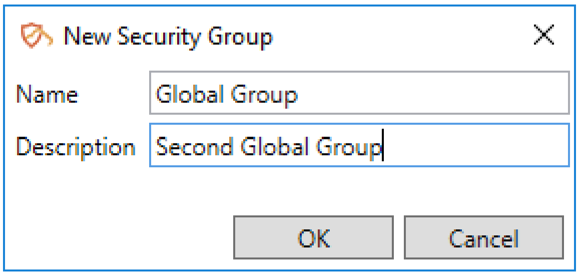
Description	Direction	Protocol	Remote IPs	Port Range or ICMP Message
test3	Both	TCP	172.31.31.29/32	3

Name
Third

Global Groups

Global groups – which are special EIF objects can be treated as AWS security group templates. They store firewall rules and can be associated with EC2 instances from any account or region through the EIF user interface. When an instance is associated with a global security group it means that EIF creates AWS security groups identical to the global group in the same region and AWS account where the instance is located.

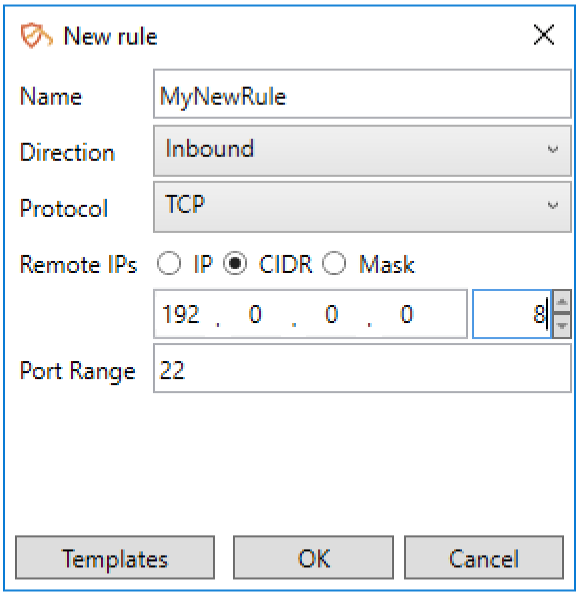
To create a global group, click on the **Create Group** button within the top level menu of the Global Security Groups panel. A new global group creation form will appear.



Name: Global Group

Description: Second Global Group

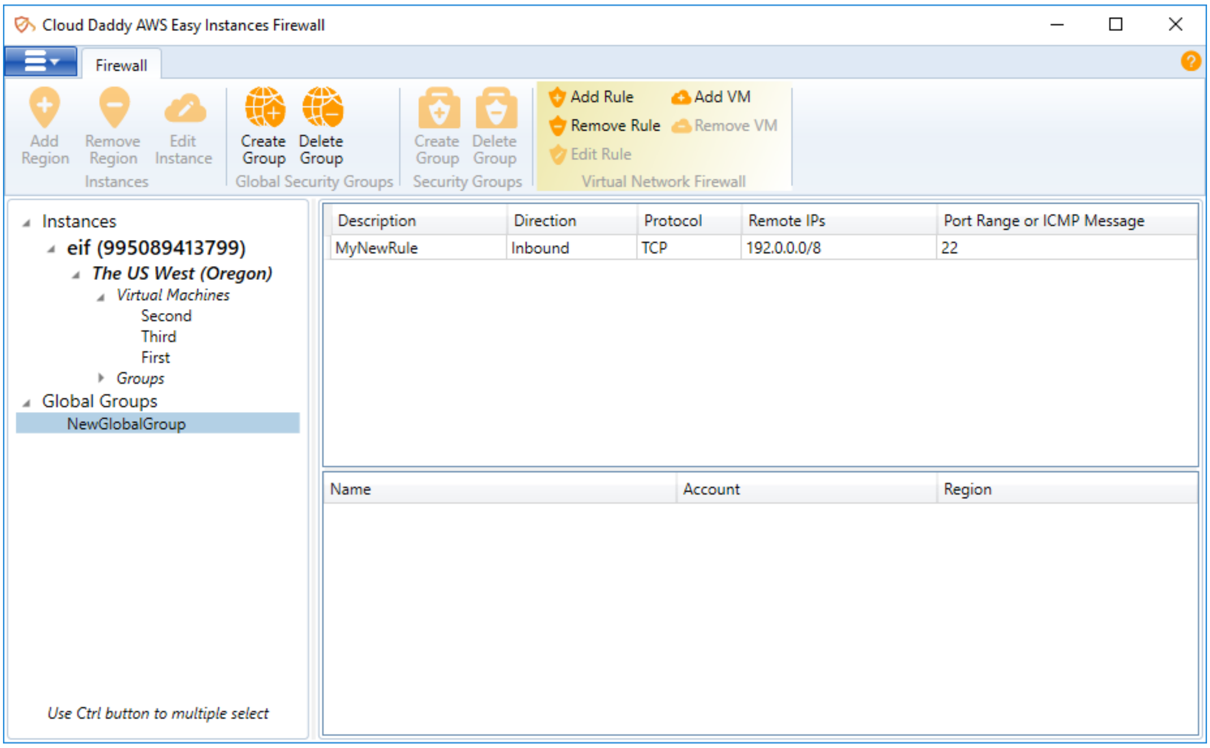
To create a global group with rules, highlight the global group and press the **Add Rule** button.



New rule

Name	MyNewRule
Direction	Inbound
Protocol	TCP
Remote IPs	○ IP ● CIDR ○ Mask
	192 . 0 . 0 . 0 / 8
Port Range	22

When done, the new rule will appear in the list of rules.



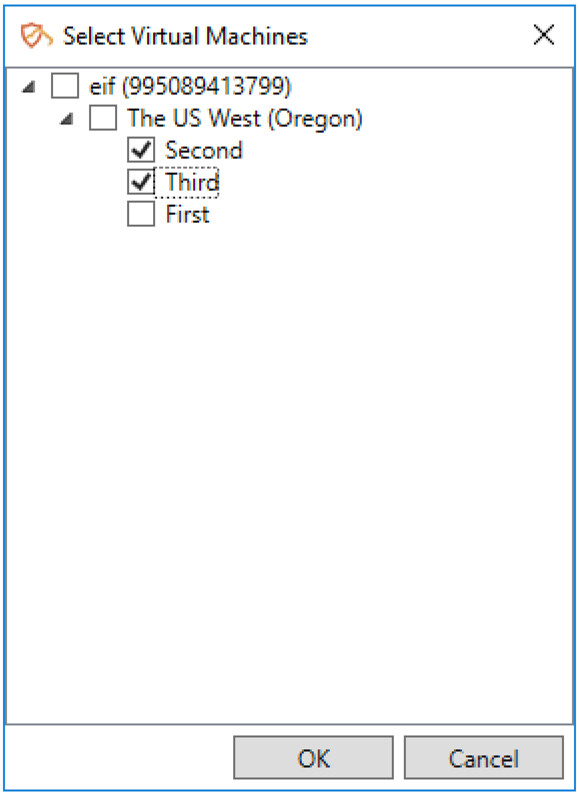
Cloud Daddy AWS Easy Instances Firewall

Description	Direction	Protocol	Remote IPs	Port Range or ICMP Message
MyNewRule	Inbound	TCP	192.0.0.0/8	22

Name	Account	Region

With EIF, you can also delete and edit existing rules. To do so, simply highlight a rule and click on either the **Remove Rule** or **Edit Rule** buttons.

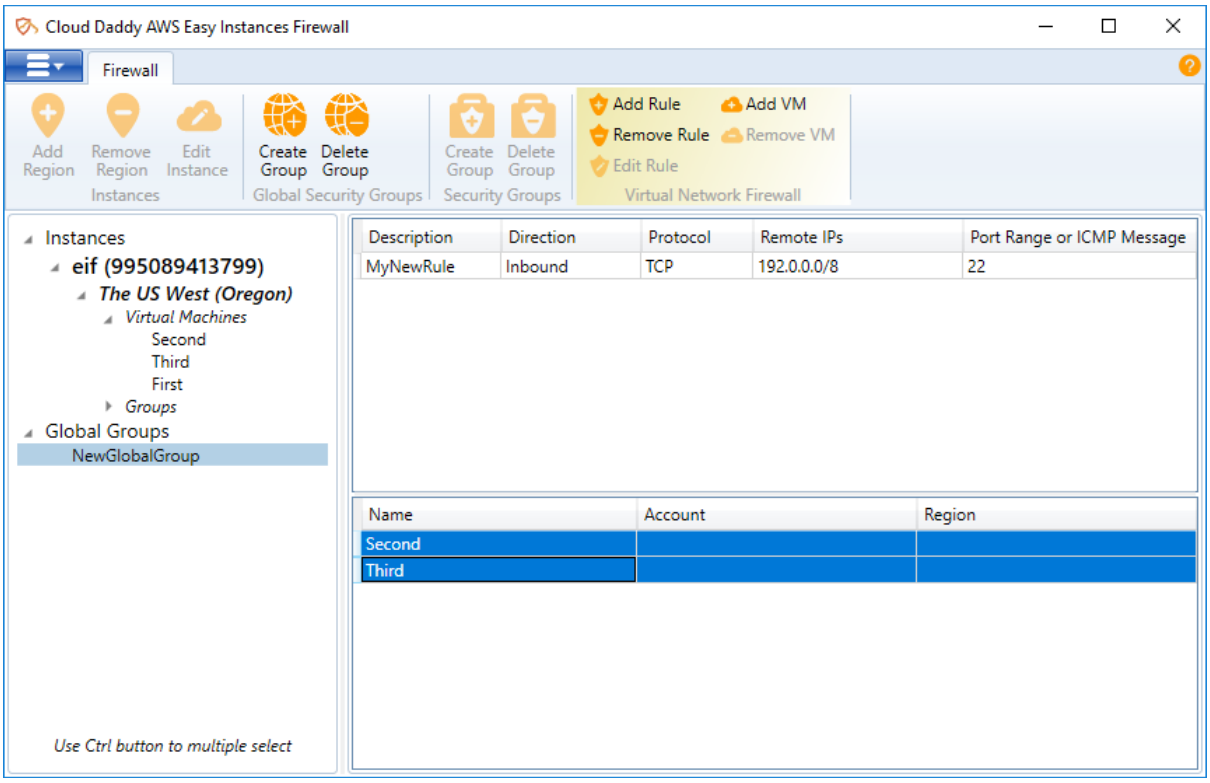
To connect the global group with an existing instance, highlight a rule and click on the **Add VM** button within the top level menu of the Virtual Network Firewall panel. A list of instances from all added accounts and all added regions will appear.



Select Virtual Machines

- □ eif (995089413799)
  - □ The US West (Oregon)
    - ☑ Second
    - ☑ Third
    - □ First

Select the instances and press the **OK** button. The virtual machines will appear in the list of Instances.



- Instances
  - eif (995089413799)
    - The US West (Oregon)
      - Virtual Machines
        - Second
        - Third
        - First
      - Groups
- Global Groups
  - NewGlobalGroup

Description	Direction	Protocol	Remote IPs	Port Range or ICMP Message
MyNewRule	Inbound	TCP	192.0.0.0/8	22

Name	Account	Region
Second		
Third		

Use Ctrl button to multiple select

We hope that you enjoy using Cloud Daddy Easy Instance Firewall.

You can reach us by email at info@clouddaddy.com or by phone at 1-866-403-8577 (Toll-Free from USA and Canada), 1-609-935-4192. For technical support, please visit our support page at https://www.clouddaddy.com/requestsupport.html or via email at support@clouddaddy.com.