HOWTO – Integrate Amazon VPC Flows

Contents

Change Control

Date (DD-MMM-YYYY)	Change Summary
01-MAR-2019	First Release by Dusan Tomic.

Document Owner: International FortiSIEM CSE Team

AWS VPC Flow Overview

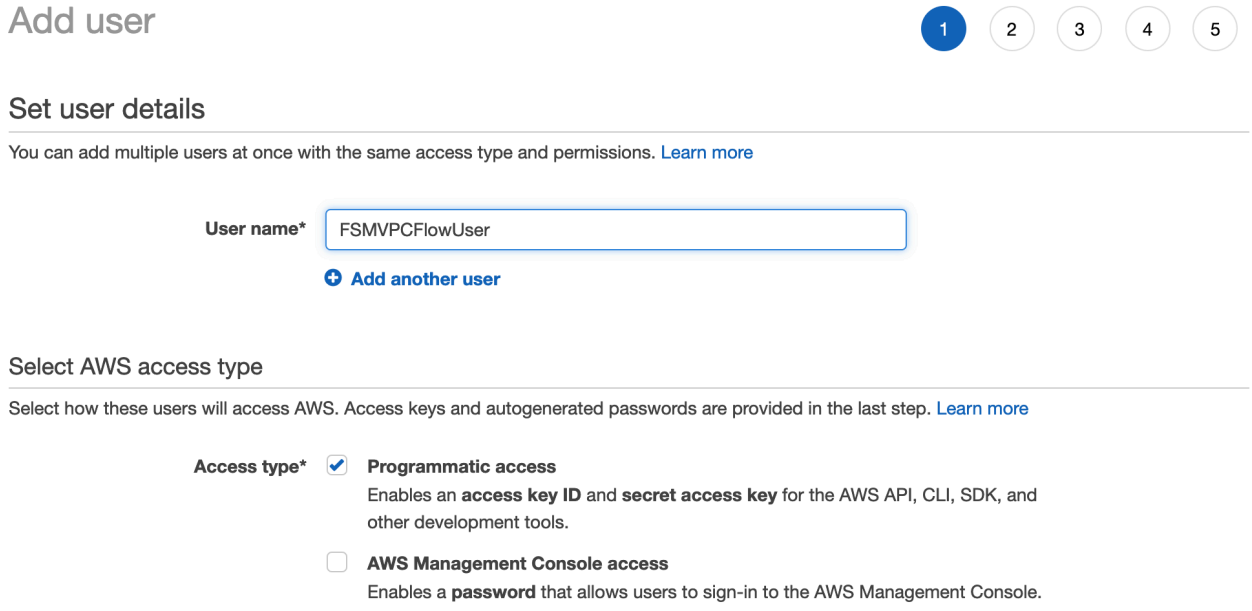
FortiSIEM can process amazon flow logs, the process is somewhat complicated and will be explained below.

We need a role that can access flows, a user attached to that role, a log group and to set the several interfaces we want to retrieve flows from to actually publish them to CloudWatch (publishing to S3 is another option we won't go over in this HOWTO).

Amazon frequently changes their services so an up to date user guide to flows can be found at https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Create a User attached to the ReadOnlyAccess policy

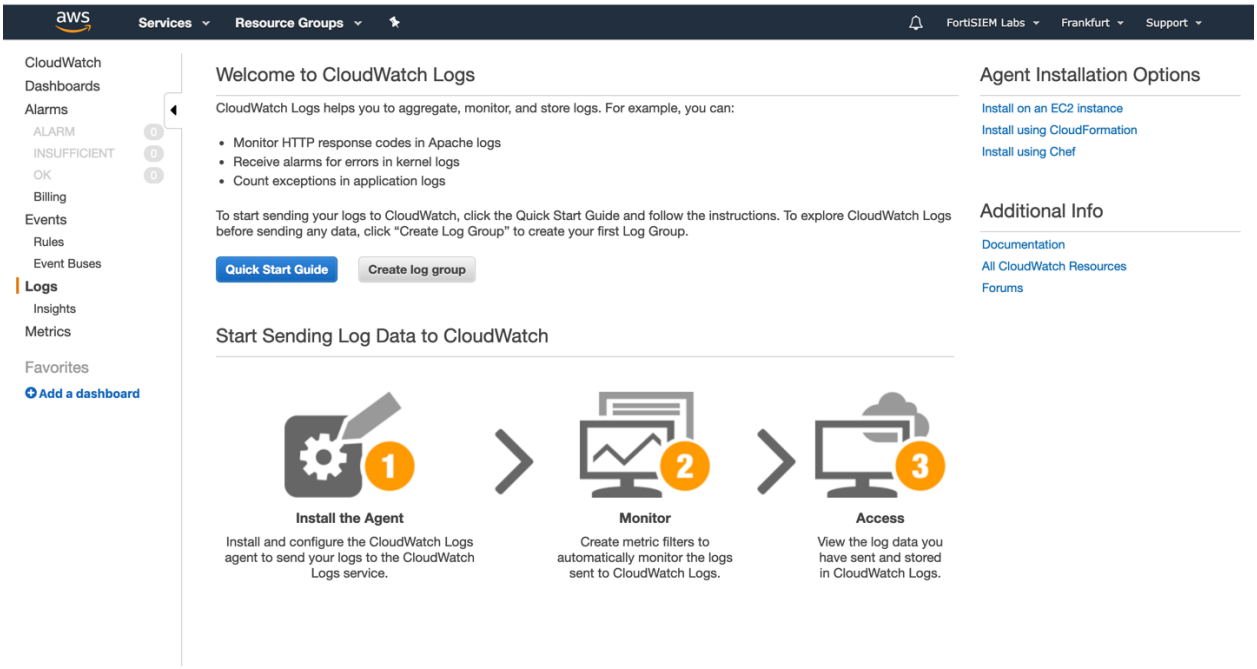
1. In your AWS Console, go to IAM > Users > Add User
2. Define your user name and select Programmatic access as the Access Type



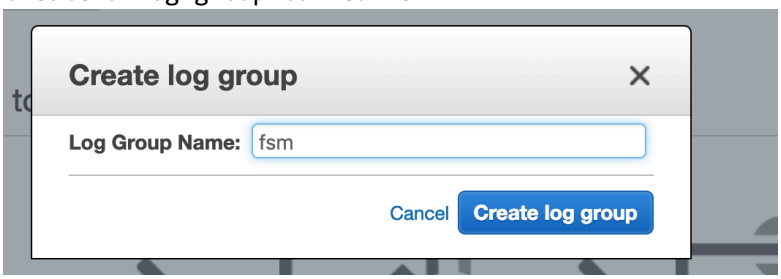
3. Click on Next: Permissions
4. Add user to the ReadOnlyAccess policy.
5. Save your Access key ID and the Secret access key, you will need this to populate credentials in FortiSIEM.

Create a Log group

1. Go to Services > CloudWatch > Lets get Started (if its there) > Logs and Click **Create log group**

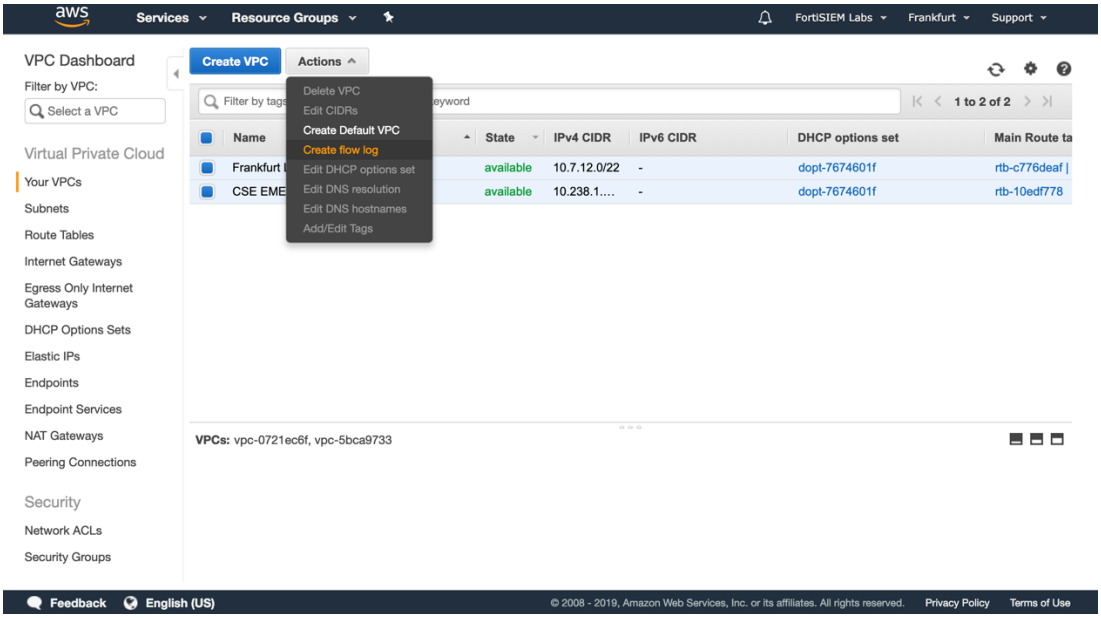


2. Create a log group called fsm

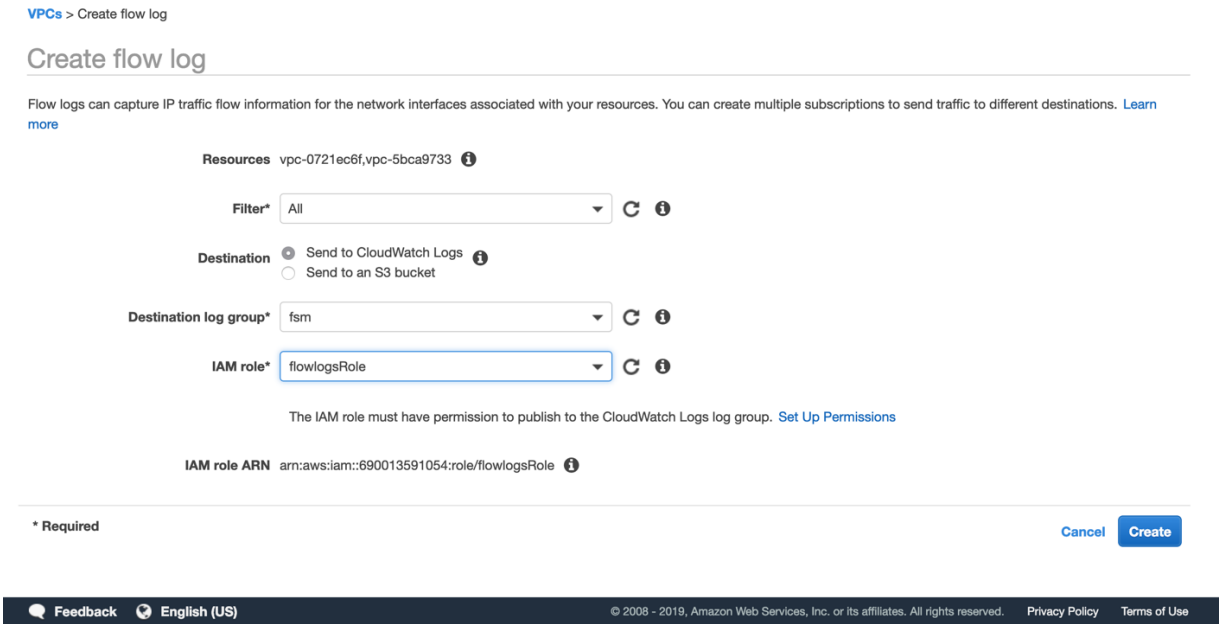


Create log streams for the VPC you want to obtain flows from

1. Go to Services > VPC > Your VPCs
2. Select the VPC or VPCs you want to enable flows for
3. Click on Actions > Create flow log



4. In the Filter, select Accept, Reject or All (depending what you want from your flows)
5. Set Destination to Send to CloudWatch logs
6. Set the Destination log group to the log group you created in the previous step
7. Set the IAM role to a role that has permissions to access flows.
   https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html#flow-logs-iam

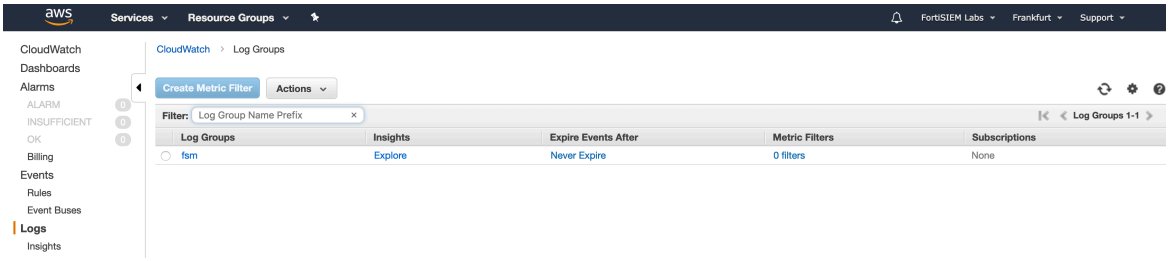


Select the interfaces that you want to generate flows

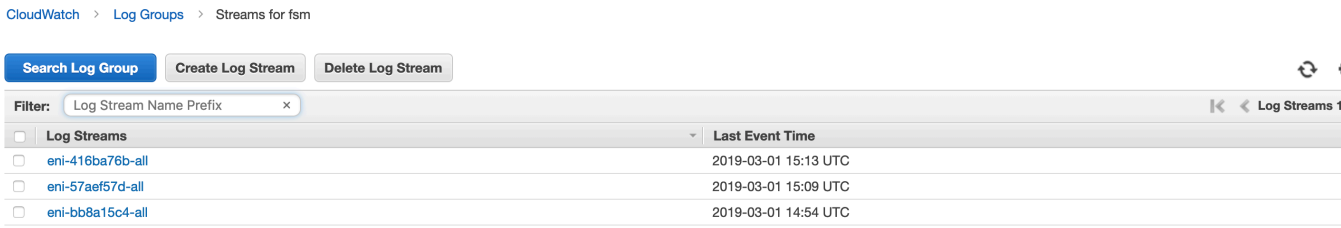
1. Go to Services > EC2 > Network Interfaces
2. Select each interface you want to generate flows and click Actions > Create flow log
3. Repeat Steps 4-7 above

View the log streams you created

1. Go to Services > CloudWatch > Logs
2. Click on fsm (or another group you used)



3. You will see all the streams (interfaces) that are generating flows

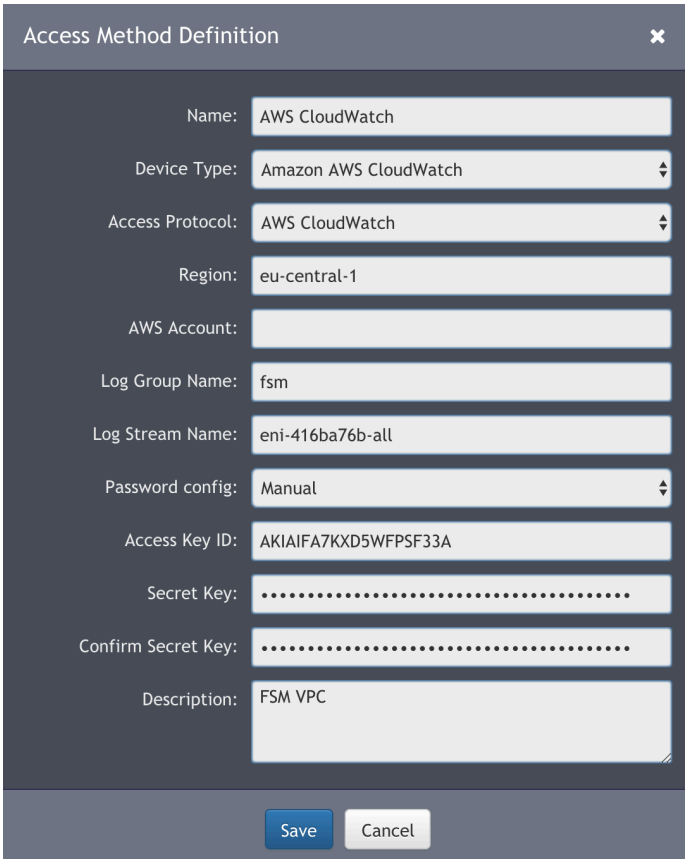


4. Write the names of these Log Streams somewhere, you will need them when creating the CloudWatch credential. Each interface generates a separate stream, so we will need as many credentials as there are log streams

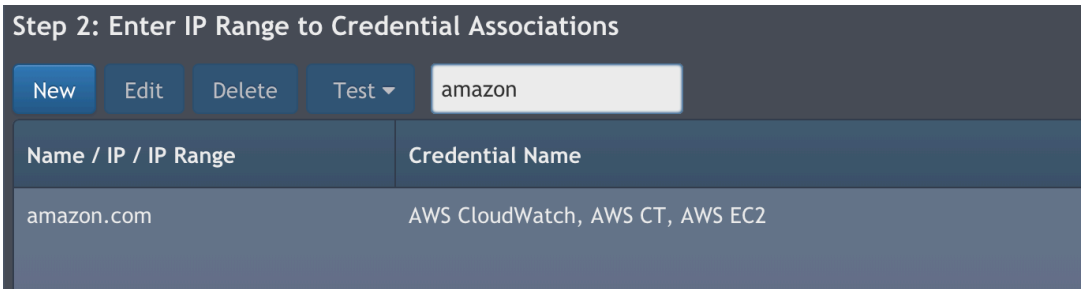
Create credential(s) in FortiSIEM for AWS CloudWatch

You will need your User/IAM Access Key ID, user/IAM Secret Key, region, log group name, log stream name(s)

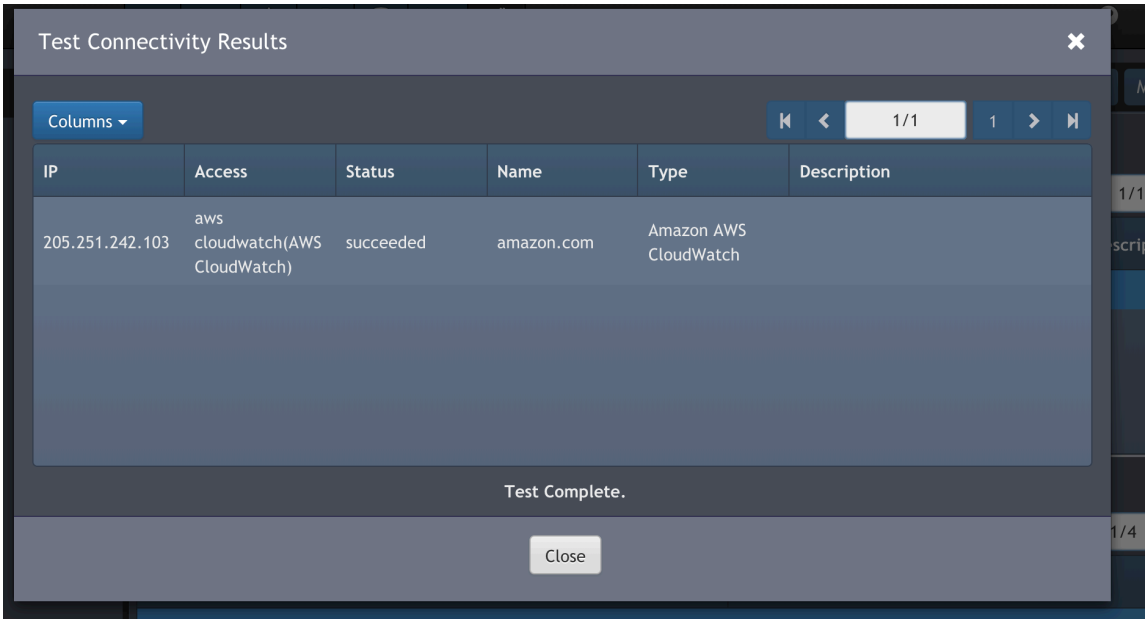
1. Populate the credential in FortiSIEM:



2. Associate the credential to amazon.com

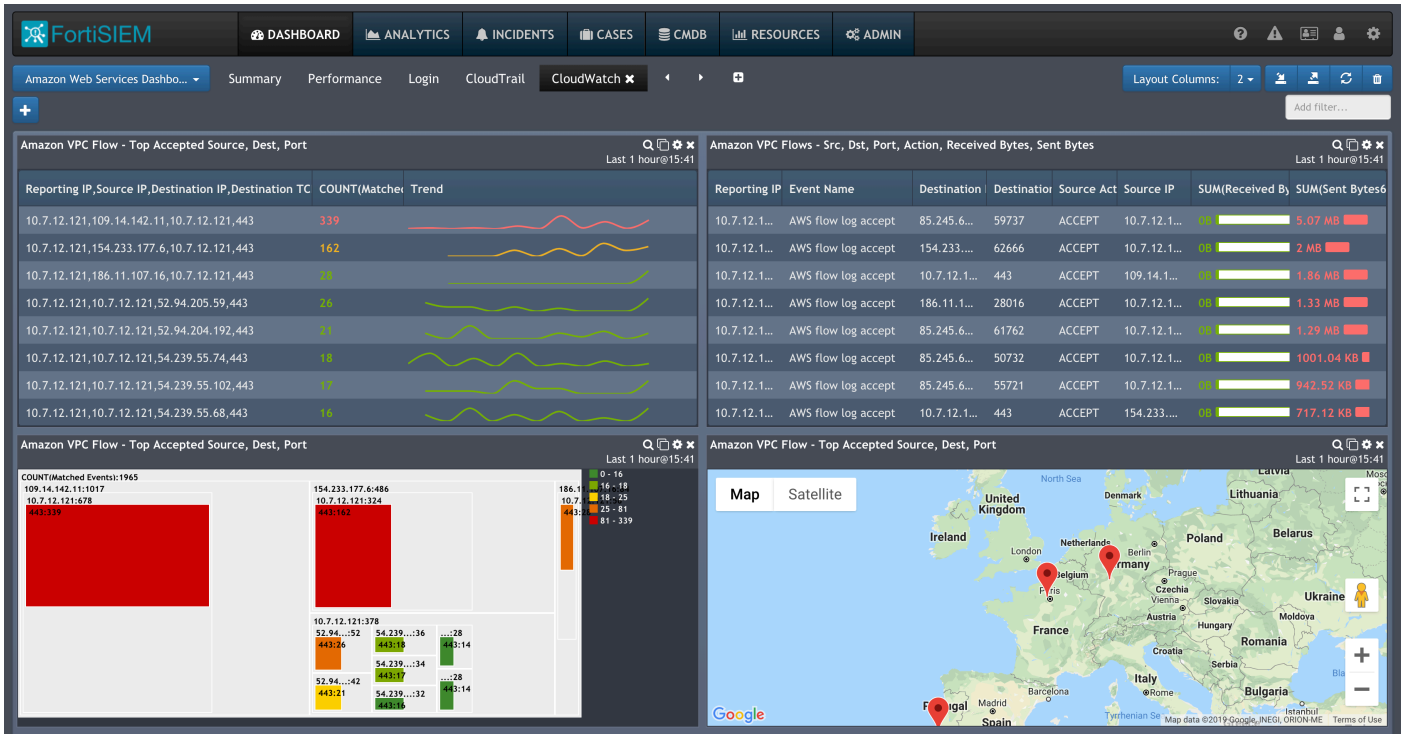


3. Test the Credential. This will create a job that will start pulling flows, we don't Discover any devices when we add CloudWatch or CloudTrail credentials.



Extra Goodies!

In version 5.1.2 (latest as of this writing), we don't have any Reports out of the box that leverage VPC flows. Below you can find two new reports that will allow you to create a dashboard such as the one below to visualize the traffic from your VPC.



The Reports

You can save each of the XML structures below into an .xml file and import them in Resources > Reports > Import in your FortiSIEM HTML5 GUI.

Amazon VPC Flow – Top Accepted Source, Dest, Port

<?xml version="1.0" encoding="UTF-8"?><Reports><Report baseline="" rsSync=""><Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name><Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description><CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope><SelectClause>
<AttrList>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause><PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause><userRoles>
<roles custId="1">1681500</roles>
</userRoles><SyncOrgs/><ReportInterval>
<Low>1551454378</Low>
<High>1551454977</High>
</ReportInterval></Report></Reports>

Amazon VPC Flows – Src, Dst, Port, Action, Received Bytes, Sent Bytes

<?xml version="1.0" encoding="UTF-8"?><Reports><Report baseline="" rsSync=""><Name>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes</Name><Description>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes - 01:13:33 PM Feb 27 2019</Description><CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope><SelectClause>
<AttrList>reptDevIpAddr,eventType,eventName,destIpAddr,destIpPort,srcAction,srcIpAddr,SUM(recvBytes64),SUM(sentBytes64)</AttrList>
</SelectClause><PatternClause>
<SubPattern id="194817050" name="">
<SingleEvtConstr>(eventType CONTAIN "AWS_VPC_FLOW") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,eventType,destIpAddr,destIpPort,srcAction,srcIpAddr</GroupByAttr>
</SubPattern>
</PatternClause><userRoles>
<roles custId="1">1681500</roles>
</userRoles><SyncOrgs/><ReportInterval>
<Low>1551454665</Low>
<High>1551455264</High>
</ReportInterval></Report></Reports>

The Dashboard

Once you have imported the reports, you copy/paste the following XML structure to a dashboard.xml file and import it into a Dashboard:

<?xml version="1.0" encoding="UTF-8"
standalone="no"?><DashboardConfigs><group><name>CloudWatch</name><description/><type>Widget</type><d
ashboard><columns>2</columns></dashboard><Widgets><widget pos="0">
<name>Amazon VPC Flow - Top Accepted Source, Dest, Port</name>
<description/>
<horizontalCell>0</horizontalCell>
<verticalCell>0</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings/>
<dataParam>twIndex:4;dtIndex:0;barType:overlaid;numResults:10;timeInterval:0;bizSvcId:0;</dataParam>
<dataProviderType>Report</dataProviderType>
<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551274433305">
<Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name>
<Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget><widget pos="1">
<name>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes</name>
<description/>
<horizontalCell>2</horizontalCell>
<verticalCell>2</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings>1,SUM(Received Bytes64):1:0|0|0.33|0.67|1:0,SUM(Sent
Bytes64):1:0|26890|368955.67|711021.33|1053087:0,0</displaySettings>
<dataParam>twIndex:4;dtIndex:4;numResults:50;timeInterval:300000;bizSvcId:0;</dataParam>
<dataProviderType>Report</dataProviderType>

<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551273213669">
<Name>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes</Name>
<Description>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes - 01:13:33 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,eventType,eventName,destIpAddr,destIpPort,srcAction,srcIpAddr,SUM(recvBytes64),SUM(sentBytes64)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817050" name="">
<SingleEvtConstr>(eventType CONTAIN "AWS_VPC_FLOW") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,eventType,destIpAddr,destIpPort,srcAction,srcIpAddr</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget><widget pos="2">
<name>Amazon VPC Flow - Top Accepted Source, Dest, Port</name>
<description/>
<horizontalCell>4</horizontalCell>
<verticalCell>6</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings/>
<dataParam>twIndex:4;dtIndex:7;numResults:10;timeInterval:300000;bizSvcId:0;chartSet:2,3,4,0</dataParam>
<dataProviderType>Report</dataProviderType>
<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551274433305">
<Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name>
<Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>

<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget><widget pos="3">
<name>Amazon VPC Flow - Top Accepted Source, Dest, Port</name>
<description/>
<horizontalCell>4</horizontalCell>
<verticalCell>6</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings/>
<dataParam>twIndex:4;dtIndex:9;numResults:50;timeInterval:300000;bizSvcId:0;</dataParam>
<dataProviderType>Report</dataProviderType>
<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551274433305">
<Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name>
<Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget></Widgets></group></DashboardConfigs>