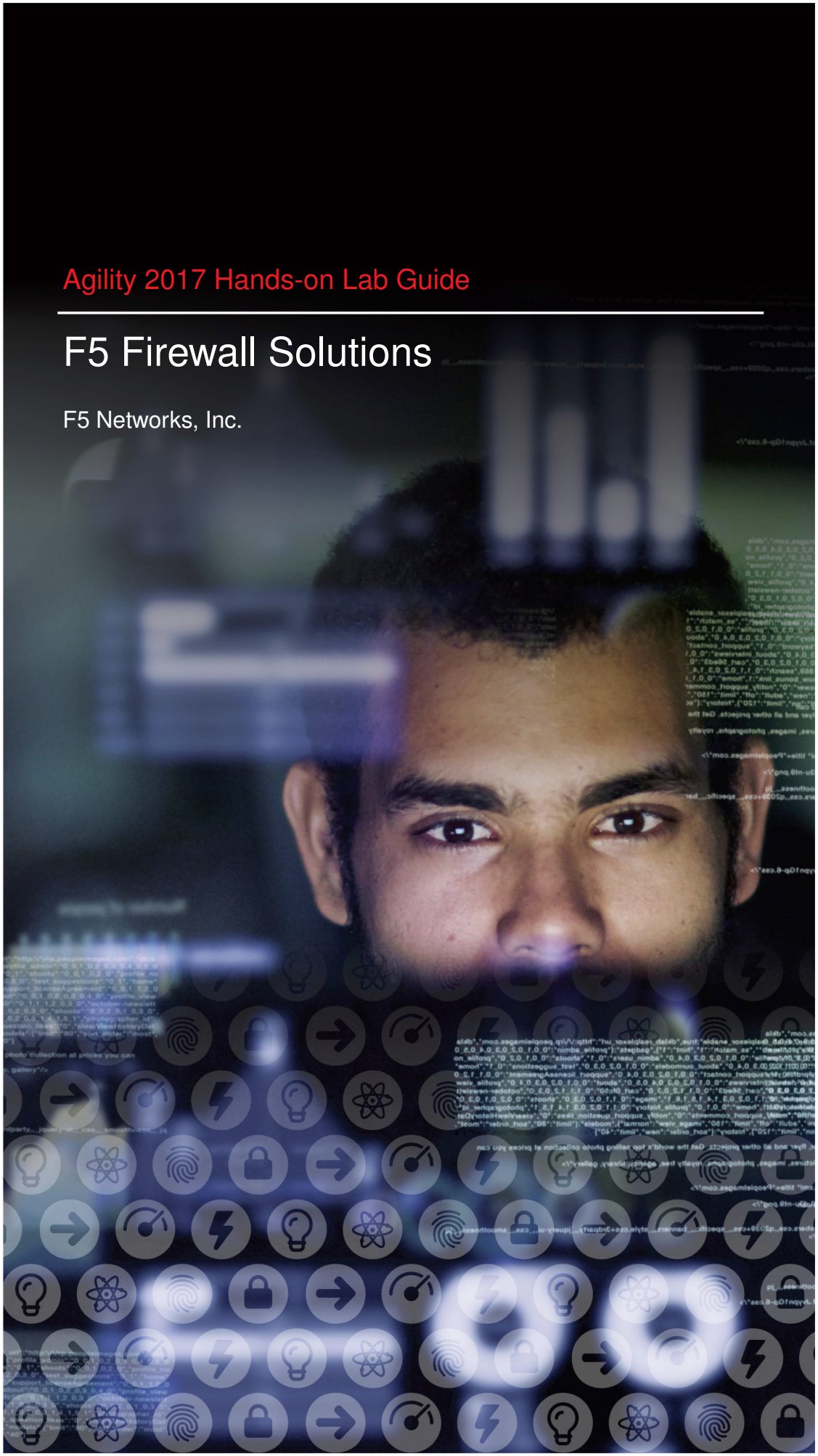


Agility 2017 Hands-on Lab Guide

F5 Firewall Solutions

F5 Networks, Inc.

Contents:

1

Class 1: Advanced Firewall Manager, the ENTERPRISE Firewall

1.1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

Note: All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

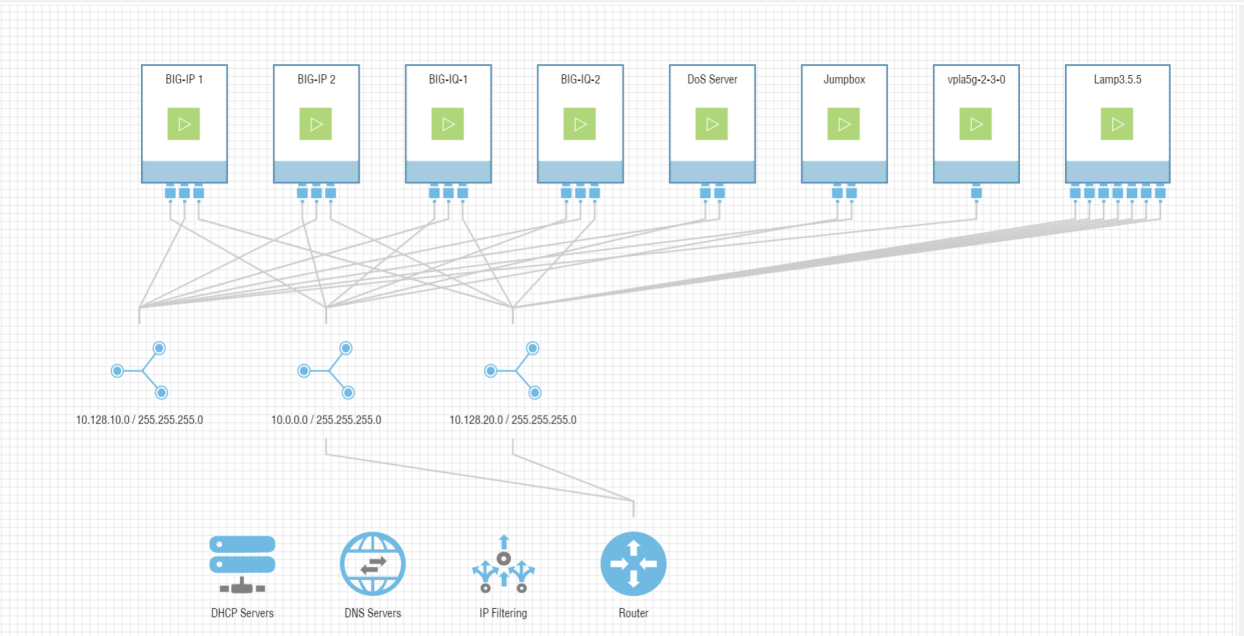
1.1.1 Lab Topology

The training lab is accessed over remote desktop connection.

Your administrator will provide login credentials and the URL.

Within each lab environment there are the following Virtual Machines:

- Windows 7 Jumpbox
- Two BIG-IP Virtual Editions (VE) – running TMOS 13.0
- Two BIG-IQ Virtual Editions (VE) – running TMOS 5.2
- LAMP Server (Web Servers)
- DoSServer
- SevOne PLA 2.3.0



Lab Components

Below are all the IP addresses that will be used during the labs. Please refer back to this page and use the IP addresses assigned to your site.

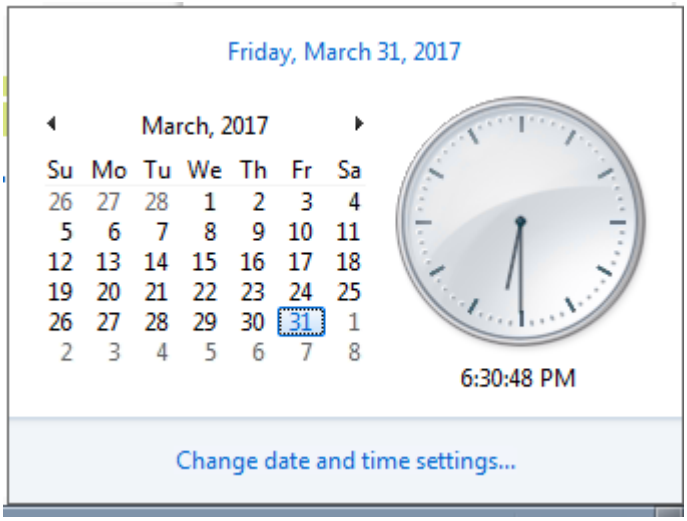
	IP Addresses
Lampserver	10.128.20.150, 10.128.20.160, 10.128.20.170

1.2 Module 1: Advanced Firewall Manager (AFM) Introduction

In this lab, you will create a pool of servers to be load balanced behind the BIG-IP. You will then experiment with AFM policies to permit and deny traffic and examine the AFM logging and reporting capabilities. In subsequent labs you will experiment with the DDoS mitigation features of AFM.

Caution: When you RDP into the Windows box, make sure the time on the windows client is correct for the current time in the Eastern Time Zone.

If the time needs to be corrected, click on the clock and choose “Change date and time settings. . . ”



If the time is not corrected please alert an instructor before proceeding.

1.2.1 Create a Pool and Virtual Server using REST API

About Representational State Transfer

Representational State Transfer (REST) describes an architectural style of web services where clients and servers exchange representations of resources. The REST model defines a resource as a source of information, and defines a representation as the data that describes the state of a resource. REST web services use the HTTP protocol to communicate between a client and a server, specifically by means of the POST, GET, PUT, and DELETE methods to create, read, update, and delete elements or collections. In general terms, REST queries resources for the configuration objects of a BIG-IP® system, and creates, deletes, or modifies the representations of those configuration objects. The iControl® REST implementation follows the REST model by:

- Using REST as a resource-based interface, and creating API methods based on nouns.
- Employing a stateless protocol and MIME data types, as well astaking advantage of the authentication mechanisms and caching built into the HTTP protocol.
- Supporting the JSON format for document encoding.
- Representing the hierarchy of resources and collections with a Uniform Resource Identifier (URI) structure.
- Returning HTTP response codes to indicate success or failure of an operation.
- Including links in resource references to accommodate discovery.

About URI format

The iControl® REST API enables the management of a BIG-IP® device by using web service requests. A principle of the REST architecture describes the identification of a resource by means of a Uniform Resource Identifier (URI). You can specify a URI with a web service request to create, read, update, or delete some component or module of a BIG-IP system configuration. In the context of REST architecture, the system configuration is the representation of a resource. A URI identifies the name of a web resource; in this case, the URI also represents the tree structure of modules and components in TMSH.

In iControl REST, the URI structure for all requests includes the string /mgmt/tm/ to identify the namespace for traffic management. Any identifiers that follow the endpoint are resource collections.

Tip: Use the default administrative account, admin, for requests to iControl REST. Once you are familiar with the API, you can create user accounts for iControl REST users with various permissions.

https://management-ip/mgmt/tm/module

The URI in the previous example designates all of the TMSH subordinate modules and components in the specified module. iControl REST refers to this entity as an organizing collection. An organizing collection contains links to other resources. The management-ip component of the URI is the fully qualified domain name (FQDN) or IP address of a BIG-IP device.

Important: iControl REST only supports secure access through HTTPS, so you must include credentials with each REST call. Use the same credentials you use for the BIG-IP device manager interface.

For example, use the following URI to access all the components and subordinate modules in the LTM module:

https://192.168.25.42/mgmt/tm/ltm

The URI in the following example designates all of the subordinate modules and components in the specified sub-module. iControl REST refers to this entity as a collection; a collection contains resources.

https://management-ip/mgmt/tm/module/sub-module

The URI in the following example designates the details of the specified component. The Traffic Management Shell (TMSH) Reference documents the hierarchy of modules and components, and identifies details of each component. iControl REST refers to this entity as a resource. A resource may contain links to sub-collections.

https://management-ip/mgmt/tm/module[/sub-module]/component

About reserved ASCII characters

To accommodate the BIG-IP® configuration objects that use characters, which are not part of the unreserved ASCII character set, use a percent sign (%) and two hexadecimal digits to represent them in a URI. The unreserved character set consists of: [A - Z] [a - z] [0 - 9] dash (-), underscore (_), period (.), and tilde (~).

You must encode any characters that are not part of the unreserved character set for inclusion in a URI scheme. For example, an IP address in a non-default route domain that contains a percent sign to indicate an address in a specific route domain, such as 192.168.25.90%3, should be encoded to replace the %character with %25.

About REST resource identifiers

A URI is the representation of a resource that consists of a protocol, an address, and a path structure to identify a resource and optional query parameters. Because the representation of folder and partition names in TMSH often includes a forward slash (/), URI encoding of folder and partition names must use a different character to represent a forward slash in iControl®

To accommodate the forward slash in a resource name, iControl REST maps the forward slash to a tilde (~) character. When a resource name includes a forward slash (/) in its name, substitute a tilde (~) for the forward slash in the path. For example, a resource name, such as /Common/plist1, should be modified to the format shown here:

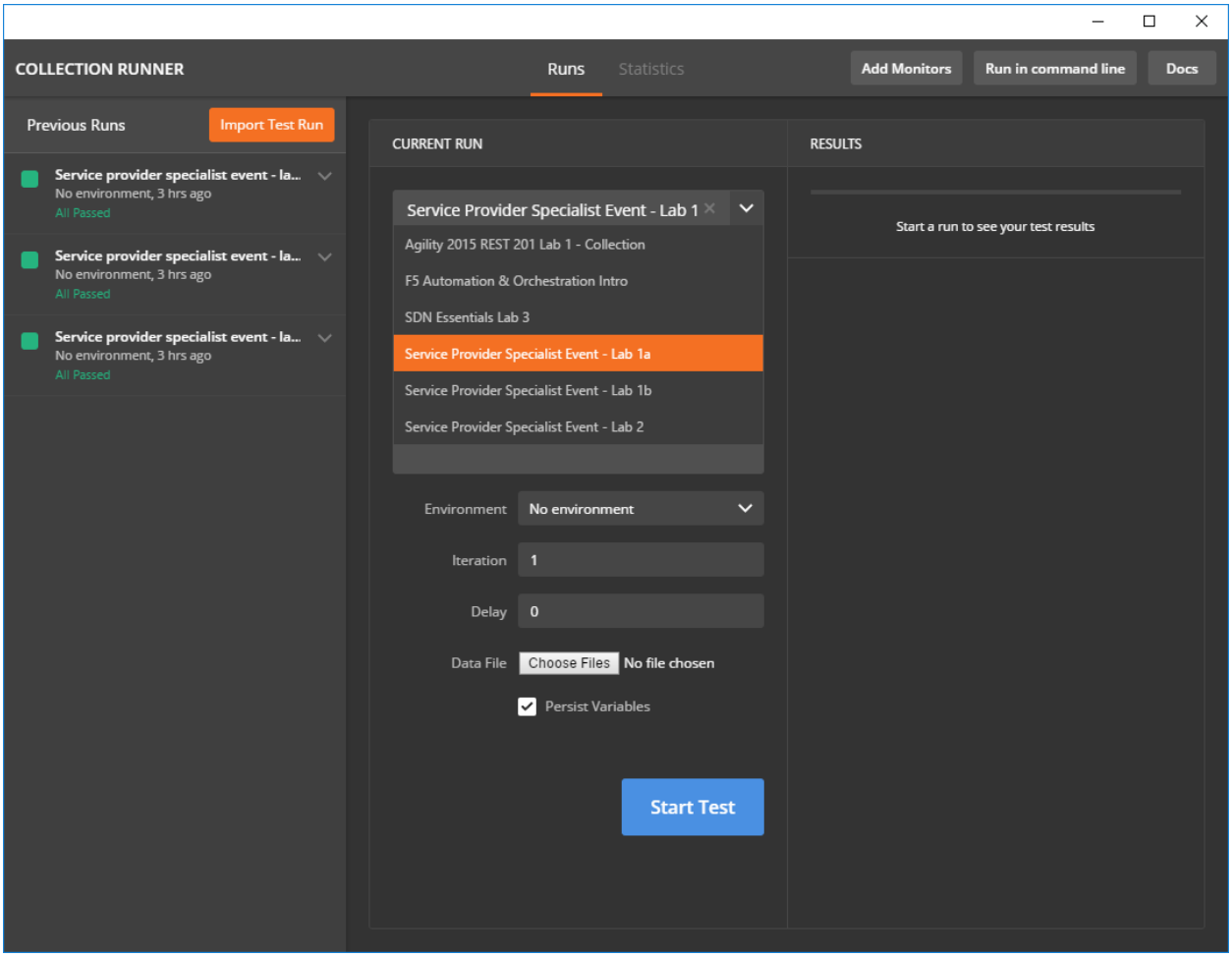
https://management-ip/mgmt/tm/security/firewall/port-list/~Common~plist1

About Postman – REST Client

Postman helps you be more efficient while working with APIs. Postman is a scratch-your-own-itch project. The need for it arose while one of the developers was creating an API for his project. After looking around for a number of tools, nothing felt just right. The primary features added initially were a history of sent requests and collections. You can find Postman here: www.getpostman.com

A PostMAN collection has been created to simplify building the pools and virtuals necessary for the remainder of this course. The collection is called “Service Provider Specialist Event – Lab 1a”. You can sequentially execute all twelve steps by pressing the send button after clicking on each call.

Alternatively, you can run all commands at once using the “Runner” feature. To use the Runner feature locate the Runner Icon at the top of POSTMan. Select the appropriate collection and click “Start Test” as exampled below:

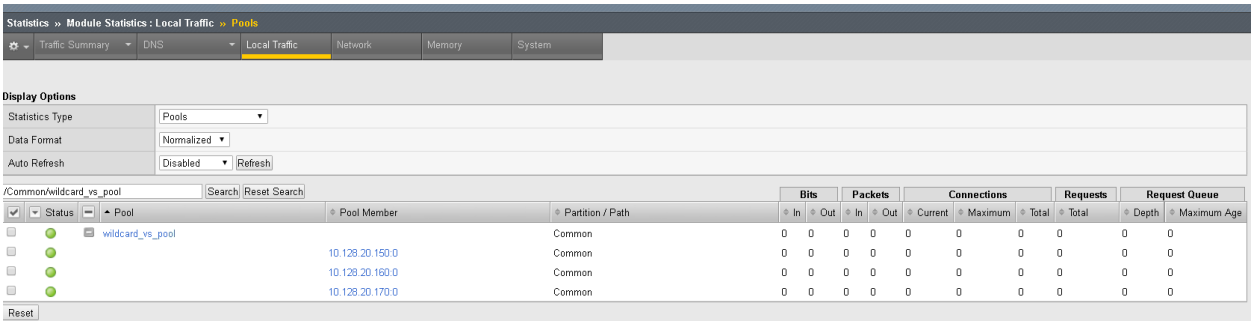


Once completed, all the necessary nodes, pools, and virtuals for the lab will have been created. As a general POSTMan rule, you should close the tabs you’ve opened when you are finished working with them (after each section). POSTMan has a known bug and will crash when there are too many tabs opened at once.

Now let’s test the virtual server to ensure it works. On your workstation open a browser and enter the address of your virtual servers that you just created (*http://10.128.10.223* and *http://10.128.10.224*). Refresh the browser screen several times (use “<ctrl>” F5 to ensure you are not displaying cached objects). Note the ***Server IP address*** should be alternating between the three destination servers in your pool (10.128.20.150, 10.128.20.160, 10.128.20.170). The BIG-IP is load balancing requests in a round-robin fashion.

Go to bigip1.agility.com (10.0.0.4) and view the statistics for the **wildcard_vs** virtual server and the **wild-**

card_vs_pool pool and its associated members. Go to **Statistics** > **Module Statistics** > **Local Traffic**. In the **Statistics Type** drop down item select **Pools**.



- You may also go to **Local Traffic > Pools > Statistics**
  - Did each pool member receive the same number of connections?
  - Did each pool member receive approximately the same number of bytes?

Try connecting directly to the IP addresses of the servers in the pool from your browser, and through the virtual server on the BIG-IP and take note of the Client IP Address on the web page as highlighted below:

- Why does the Source IP address change when going through BIG-IP?
  - What address is it changing to?
- Verify that you can connect through the wildcard virtual server using various ports:
  - Edit the URL in your browser to *http://10.128.10.223:8081*
  - Edit the URL in your browser to *https://10.128.10.223*
  - Edit the URL in your browser to *ftp://10.128.10.223*

Note: There is no need to login, a prompt will eventually be displayed.

  - Open Putty (SSH) and access 10.128.10.223

Note: you do not need to login, getting a prompt is sufficient for this test

---

  - All of these connections should be successful through the BIG-IP, and should be load balanced to the servers in the pool. Since the BIG-IP is configured for a wildcard port on the virtual server and pool, these connections are allowed through.

– Close the Web Browsers and Putty.

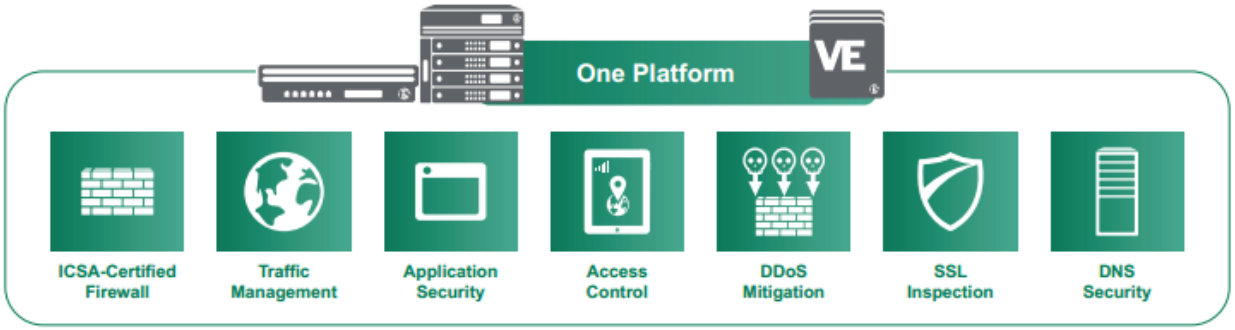
1.2.2 Advanced Firewall Manager (AFM)

Advanced Firewall Manager (AFM) is a new module that was added to TMOS in version 11.3. F5

BIG-IP Advanced Firewall Manager™ (AFM) is a high-performance ICSA certified, stateful, full-proxy

network firewall designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols—including HTTP/S, SMTP, DNS, SIP, and FTP.

By aligning firewall policies with the applications, they protect, BIG-IP AFM streamlines application deployment, security, and monitoring. With its scalability, security, and simplicity, BIG-IP AFM forms the core of the F5 application delivery firewall solution.



Some facts below about AFM, and its functionality:

- Advanced Firewall Manager (AFM) provides “Shallow” packet inspection while Application Security Manager (ASM) provides “Deep” packet inspection. By this we mean that AFM is concerned with source IP address and port, destination IP address and port, and protocol (this is also known as 5-tuple/quintuple filtering).
- AFM is used to allow/deny a connection before deep packet inspection ever takes place, think of it as the first line of firewall defense.
- AFM is many firewalls in one. You can apply L4 firewall rules to ALL addresses on the BIG-IP or you can specify BIG-IP configuration objects (route domains, virtual server, self-IP, and Management-IP).
- AFM runs in 2 modes: ***ADC mode*** and ***Firewall*** mode. ***ADC mode*** is called a “blacklist”, all traffic is allowed to BIG-IP except traffic that is explicitly DENIED (this is a negative security model). ***Firewall mode*** is called a “whitelist”, all traffic is denied to BIG-IP except traffic that is explicitly ALLOWED. The latter is typically used when the customer only wants to use us as a firewall or with LTM.
- We are enabling “SERVICE DEFENSE IN DEPTH” versus traditional “DEFENSE IN DEPTH”. This means, instead of using multiple shallow and deep packet inspection devices inline increasing infrastructure complexity and latency, we are offering these capabilities on a single platform.
- AFM is an ACL based firewall. In the old days, we used to firewall networks using simple packet filters. With a packet filter, if a packet doesn’t match the filter it is allowed (not good). With AFM, if a packet does not match criteria, the packet is dropped.
- AFM is a stateful packet inspection (SPI) firewall. This means that BIG-IP is aware of new packets coming to/from BIG-IP, existing packets, and rogue packets.
- AFM adds more than 80 L2-4 denial of service attack vector detections and mitigations. This may be combined with ASM to provide L4-7 protection.

- Application Delivery Firewall is the service defense in depth layering mentioned earlier. On top of a simple L4 network firewall, you may add access policy and controls from L4-7 with APM (Access Policy Manager), or add L7 deep packet inspection with ASM (web application firewall), You can add DNS DOS mitigation with LTM DNS Express and GTM + DNSSEC. These modules make up the entire application delivery firewall (ADF) solution.

1.2.3 Creating AFM Network Firewall Rules

Default Actions

The BIG-IP® Network Firewall provides policy-based access control to and from address and port pairs, inside and outside of your network. Using a combination of contexts, the network firewall can apply rules in many ways, including: at a global level, on a per-virtual server level, and even for the management port or a self IP address. Firewall rules can be combined in a firewall policy, which can contain multiple context and address pairs, and is applied directly to a virtual server.

By default, the Network Firewall is configured in ***ADC mode***, a default allow configuration, in which all traffic is allowed through the firewall, and any traffic you want to block must be explicitly specified.

The system is configured in this mode by default so all traffic on your system continues to pass after you provision the Advanced Firewall Manager. You should create appropriate firewall rules to allow necessary traffic to pass before you switch the Advanced Firewall Manager to Firewall mode. In ***Firewall mode***, a default deny configuration, all traffic is blocked through the firewall, and any traffic you want to allow through the firewall must be explicitly specified.

The BIG-IP® Network Firewall provides policy-based access control to and from address and port pairs, inside and outside of your network. By default, the network firewall is configured in ADC mode, which is a ***default allow*** configuration, in which all traffic is allowed to virtual servers and self IPs on the system, and any traffic you want to block must be explicitly specified. This applies only to the Virtual Server & Self IP level on the system.

Important: Even though the system is in a default allow configuration, if a packet matches no rule in any context on the firewall, a Global Drop rule drops the traffic.

1.2.4 Rule Hierarchy

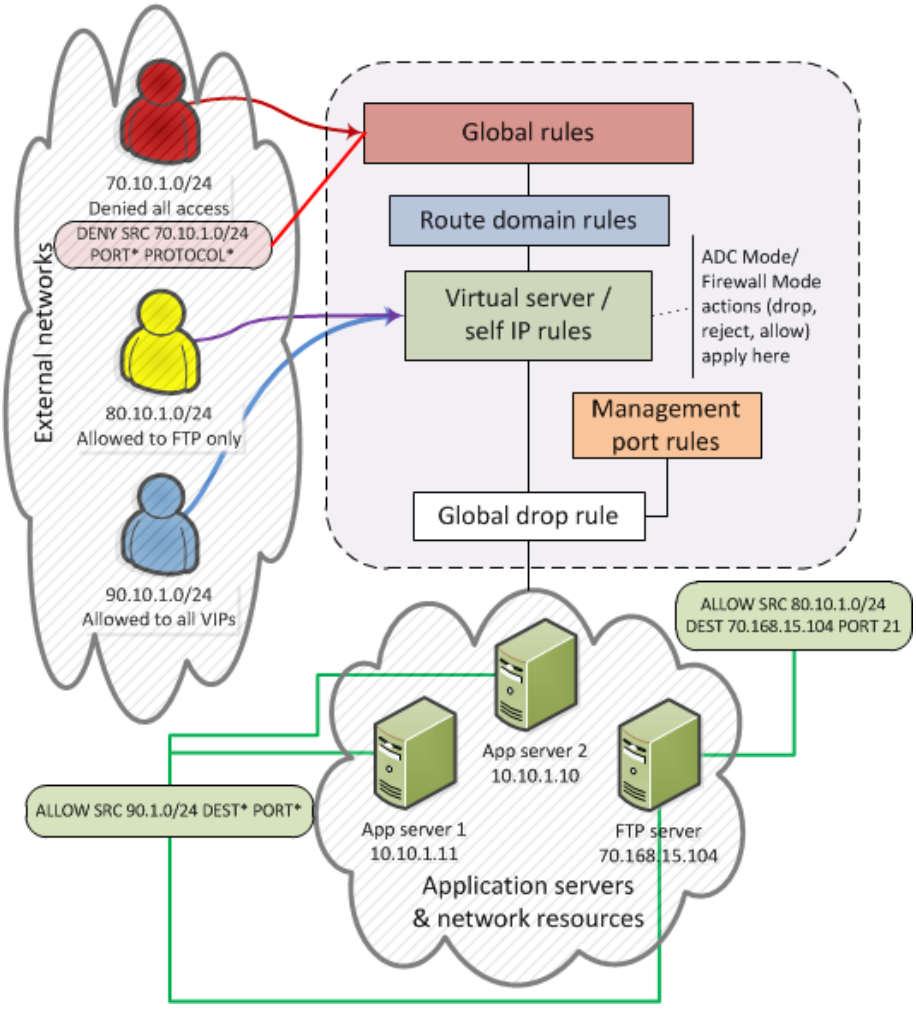
With the BIG-IP® Network Firewall, you use a context to configure the level of specificity of a firewall rule or policy. For example, you might make a global context rule to block ICMP ping messages, and you might make a virtual server context rule to allow only a specific network to access an application.

Context is processed in this order:

- Global
- Route domain
- Virtual server / self IP
- Management port*
- Global drop*

The firewall processes policies and rules in order, progressing from the global context, to the route domain context, and then to either the virtual server or self IP context. Management port rules are processed separately, and are not processed after previous rules. Rules can be viewed in one list, and viewed and reorganized separately within each context. You can enforce a firewall policy on any context except the management port. You can also stage a firewall policy in any context except management.

Important: You cannot configure or change the Global Drop context. The Global Drop context is the final context for traffic. Note that even though it is a global context, it is not processed first, like the main global context, but last. If a packet matches no rule in any previous context, the Global Drop rule drops the traffic.



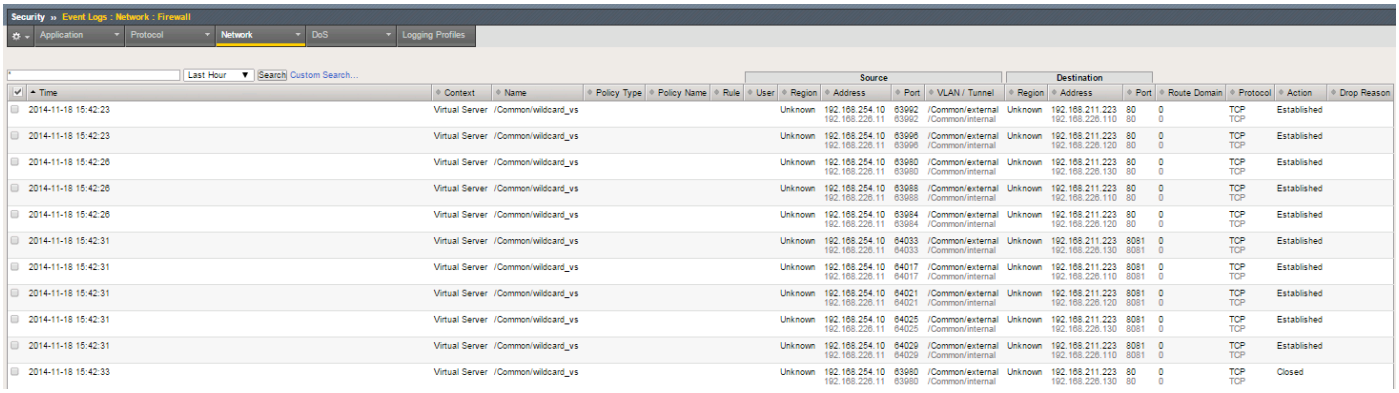
1.2.5 Create and View Log Entries

In this section, you will generate various types of traffic through the virtual server as you did previously, but now you will view the log entries using the network firewall log. Open the ***Security > Event Logs > Network > Firewall*** page on bigip01.agility.com (10.0.0.4). The log file is empty because no traffic has been sent to the virtual server since you enabled logging.

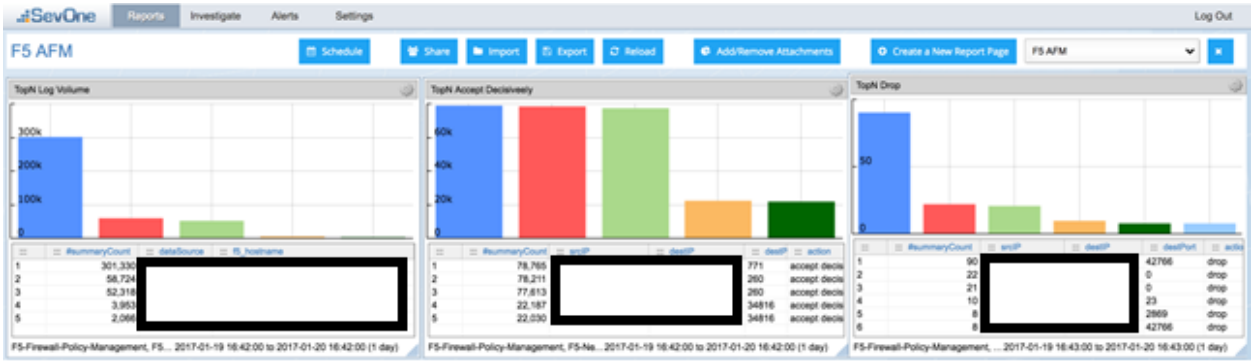
- Open a new Web browser and access your ***wildcard_vs*** *http://10.128.10.223*
- Edit the URL to *http://10.128.10.223:8081*
- Edit the URL to *https://10.128.10.223*
- Open either Chrome or Firefox and access *ftp://10.128.10.223*
- Open Putty and access 10.128.10.223, you do not need to log in.
- Close all Web browsers and Putty sessions.
- In the Configuration Utility, reload the Firewall log page.

– ***Security > Event Logs > Network > Firewall***

- Sort the list in descending order by the Time column.



Examine the Source Address and Destination Port values. Note how requests for all services were established and none were blocked. Although we will not configure external logging in this lab, you should be aware that the BIG-IP supports high speed external logging in various formats including ***SevOne***, ***Splunk*** and ***ArcSight***. Below are some examples of AFM Firewall and DoS logs being presented by SevOne:

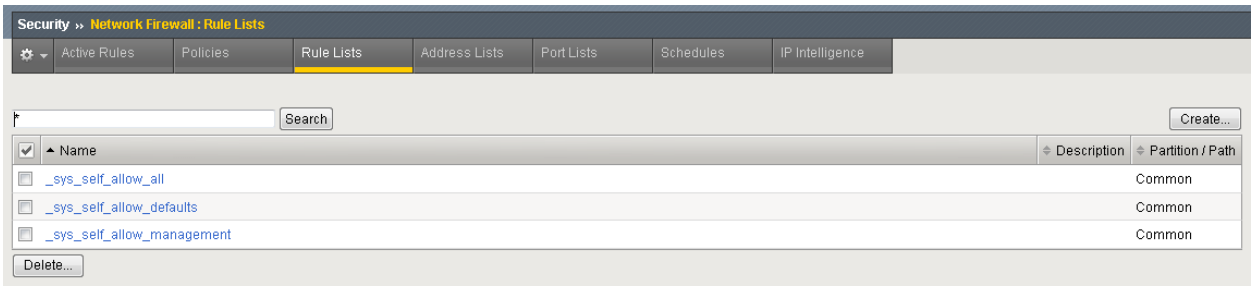


1.2.6 Create a Rule List

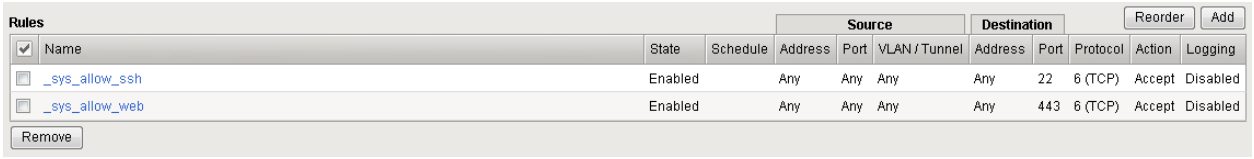
Rule lists are a way to group a set of individual rules together and apply them to the active rule base as a group. A typical use of a rule list would be for a set of applications that have common requirements for access protocols and ports. As an example, most web applications would require TCP port 80 for HTTP and TCP port 443 for SSL/TLS. You could create a Rule list with these protocols, and apply them to each of your virtual servers.

Let's examine some of the default rule lists that are included with AFM. Go to ***Security >Network Firewall > Rule Lists***. They are:

- _sys_self_allow_all
- _sys_self_allow_defaults
- _sys_self_allow_management

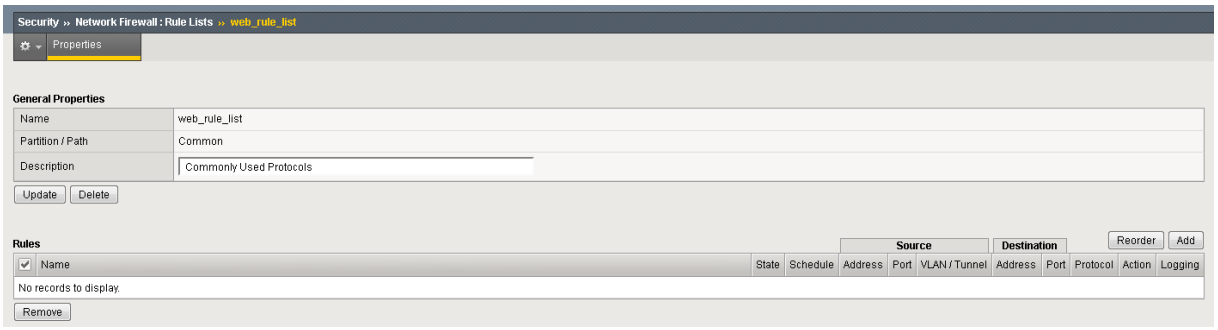


If you click on ***_sys_self_allow_management*** you'll see that it is made up of two different rules that will allow management traffic (port 22/SSH and port 443 HTTPS). Instead of applying multiple rules over and over across multiple virtual servers, you can put them in a rule list and then apply the rule list as an ACL.

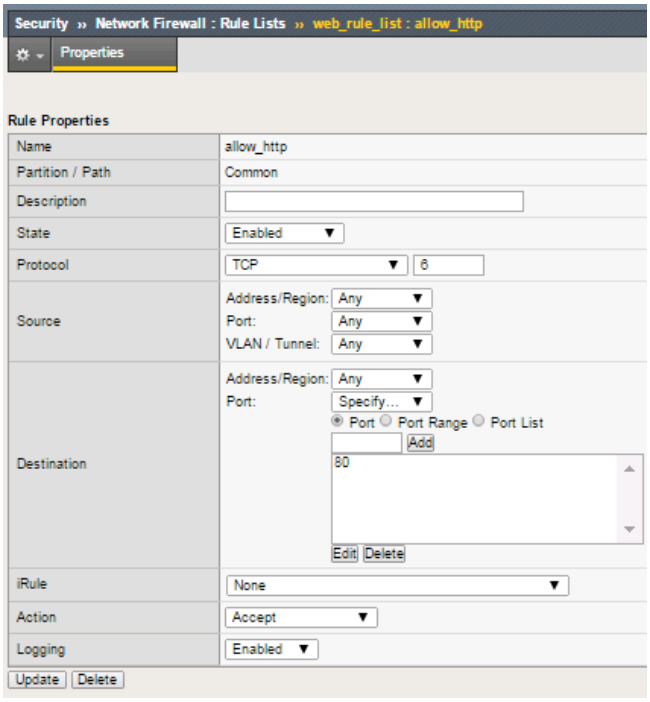


On bigip01.agility.com (10.0.0.4) create a rule list to allow Web traffic. A logical container must be created before the individual rules can be added. You will create a list with three rules, to allow port 80 (HTTP), allow port 443 (HTTPS) and reject traffic from a specific IP subnet. First you need to create a container for the rules by going to ***Security > Network Firewall > Rule Lists*** and select ***Create*.** For the ***Name*** enter ***web_rule_list***, provide an optional description and then click ***Finished*.**

Edit the ***web_rule_list*** by selecting it in the Rule Lists table, then click the ***Add*** button in the Rules section. Here you will add three rules into the list; the first is a rule to allow HTTP.



Name	allow_http
Protocol	TCP
Source	Leave at Default of ***Any***
Destination Address	Any
Destination Port	Specify Single Port ***80***, then click ***Add***
Action	Accept
Logging	Enabled



Select **Repeat** when done.

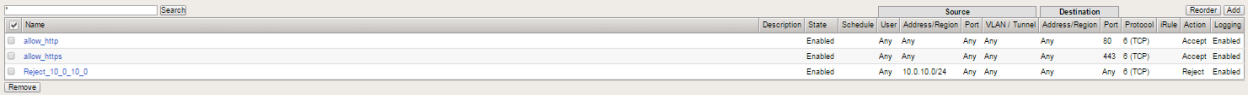
Create a rule to allow HTTPS.

Name	allow_https
Protocol	TCP
Source	Leave at Default of Any
Destination Address	Any
Destination Port	Specify Single Port 443, then click ***Add***
Action	Accept
Logging	Enabled

Select **Finished** when done. Create another rule by clicking ***Add*** to reject all access from the 10.0.10.0/24 network.

Name	reject_10_0_10_0
Protocol	Any
Source	Address 10.0.10.0/24, then click ***Add***
Destination Address	Any
Destination Port	Any
Action	Reject
Logging	Enabled

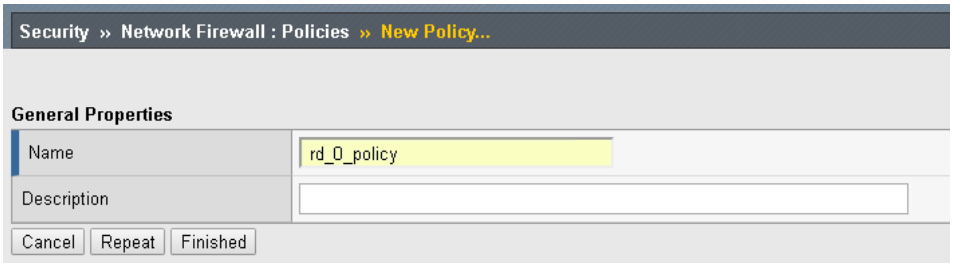
Select ***Finished*** when done. When you exit you'll notice the reject rule is after the ***allow_http*** and ***allow_https*** rules. This means that HTTP and HTTPS traffic from 10.0.10.0/24 will be accepted, while all other traffic from this subnet will be rejected based on the ordering of the rules as seen below:



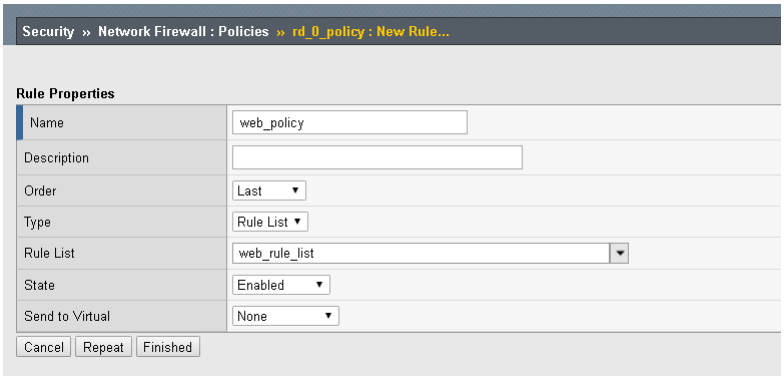
1.2.7 Create a Policy with a Rule List

Policies are a way to group a set of individual rules together and apply them to the active policy base as a group. A typical use of a policy list would be for a set of rule lists that have common requirements for access protocols and ports.

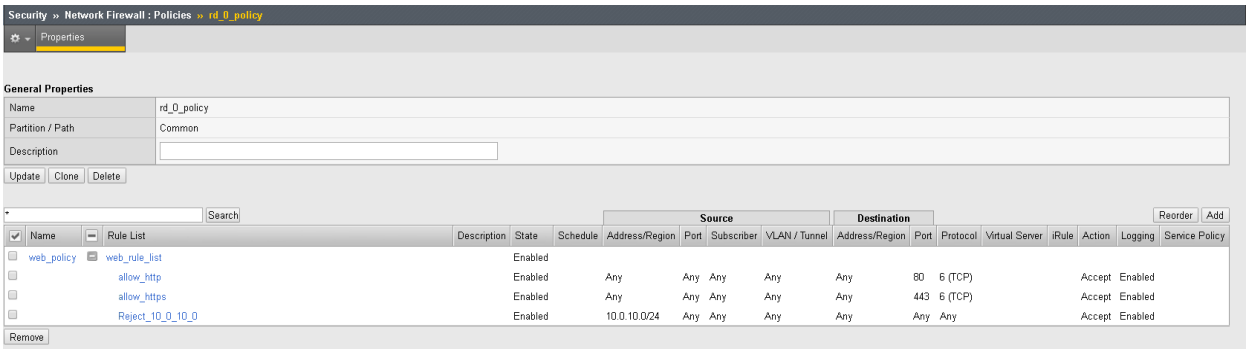
Create a policy list to allow the traffic you created in the rule list in the previous section. A logical container must be created before the individual rules can be added. First you need to create a container for the policy by going to ***Security > Network Firewall > Policies*** and select ***Create*.** For the ***Name*** enter ***rd_0_policy***, provide an optional description and then click ***Finished*.**



Edit the ***rd_0_policy*** by selecting it in the Policy Lists table, then click the ***Add*** button in the Rules section. Here you will add the rule list you created in the previous section. For the ***Name*** enter ***web_policy***, provide an optional description, for type select ***Rule List,*** select the Rule List "***web_rule_list***" and then click ***Finished*.**



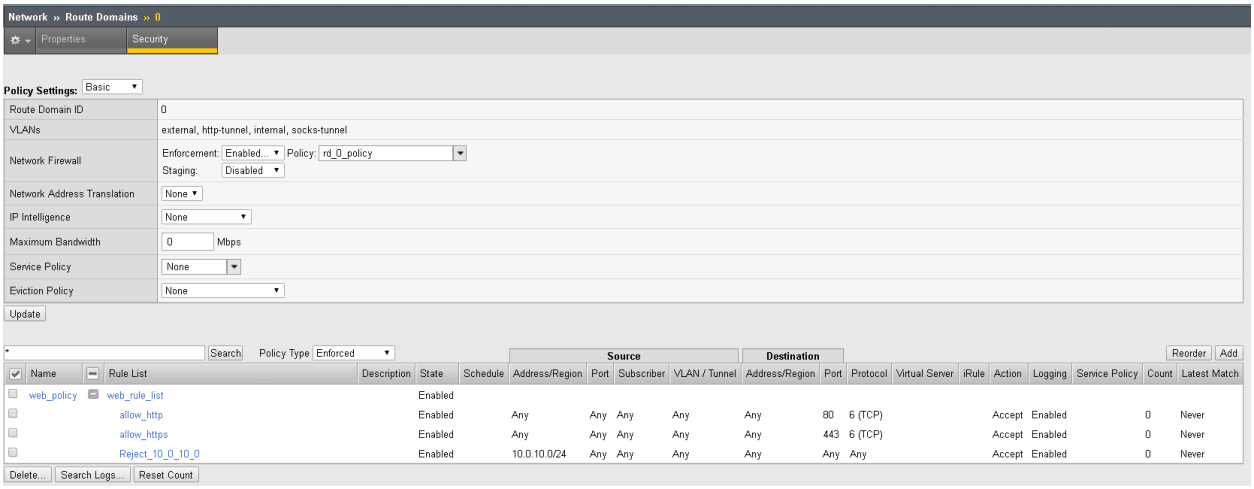
When finished your policy should look similar to the screenshot below.



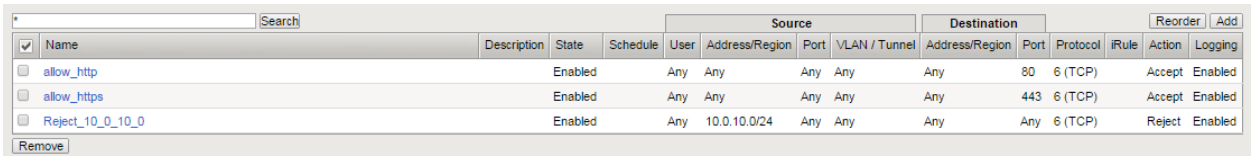
1.2.8 Add the Rule List to a Route Domain

In this section, you are going to attach the rule to a route domain using the ***Security*** selection in the top bar within the ***Route Domain*** GUI interface. Go to ***Network***, then click on ***Route Domains***, then select the hyperlink for route domain ***0***. Now click on the ***Security*** top bar selection, which is a new option that was added in version 11.3. From the Network Firewall Enforcement dropdown menu select enabled. Select the policy you just created “rd_0_policy” and click update.

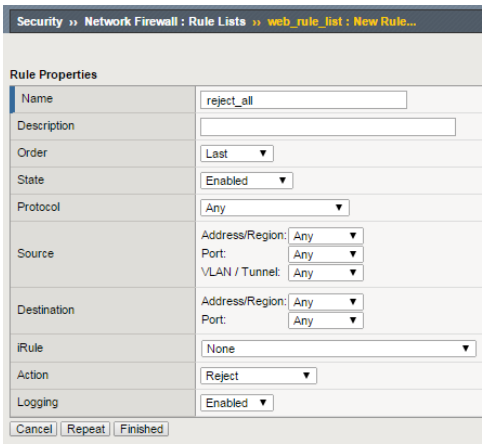
Review the rules that are now applied to this route domain.



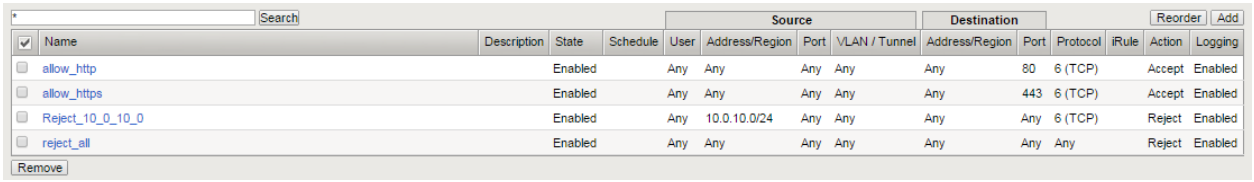
We will insert a reject clause into the existing rule list so that you can examine different types of log entries. Go to ***Security > Network Firewall > Rule Lists***. Select the ***web_rule_list*** you created earlier so that you may edit it, and then click the ***Add*** button.



For ***Name*** configure ***reject_all***, and leave all options default except set ***Action*** for ***Reject***, and set ***Logging*** to ***Enabled***, then click ***Finished***.

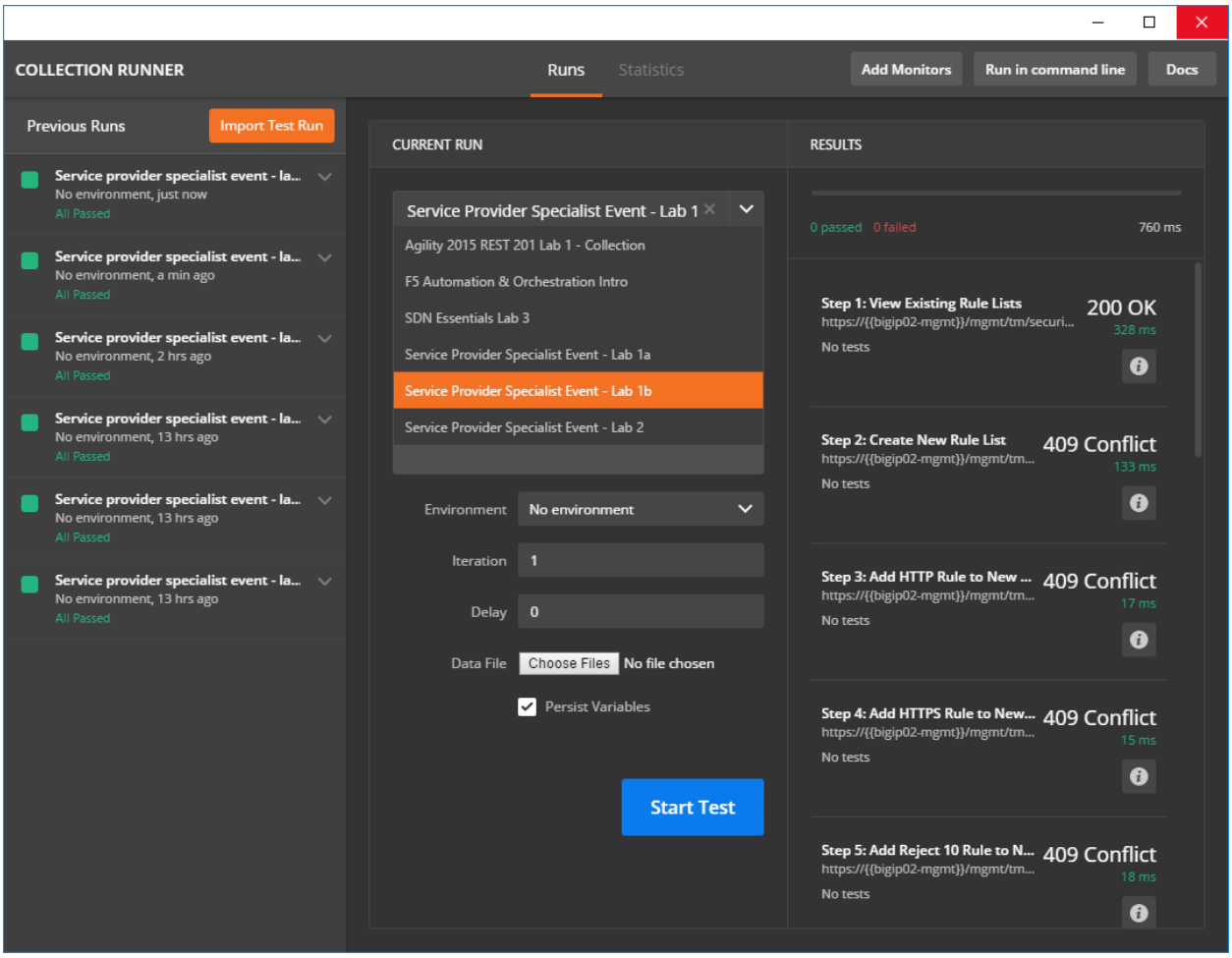


Your rule set should look similar to the screenshot below:



1.2.9 Creating Rules and Policy via REST API

The RESTful API is also capable of AFM modifications. To add the same rules and policy to bigip02.agility.com (10.0.0.5), simply follow the calls in the collection “Service Provider Specialist Event - Lab 1b”. These calls can be run individually in the sequence provided or using Runner as exampled below:



1.2.10 Test the New Firewall Rules

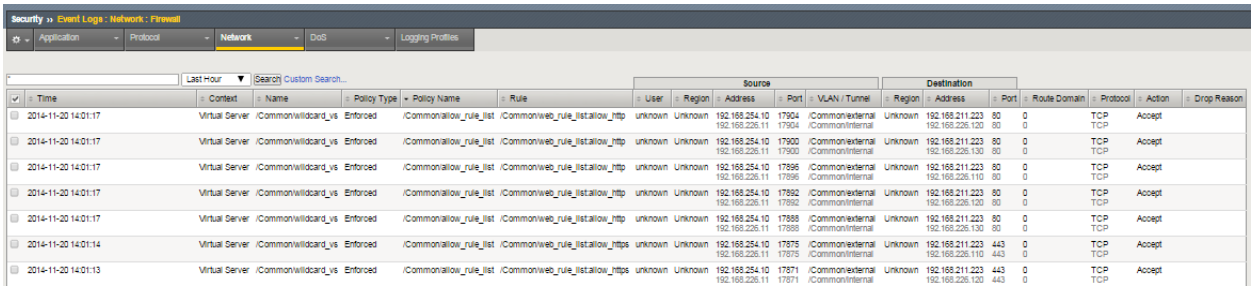
Once again you will generate traffic through the BIG-IP VE system using the ***wildcard_vs*** virtual server and then

view the AFM (firewall) logs.

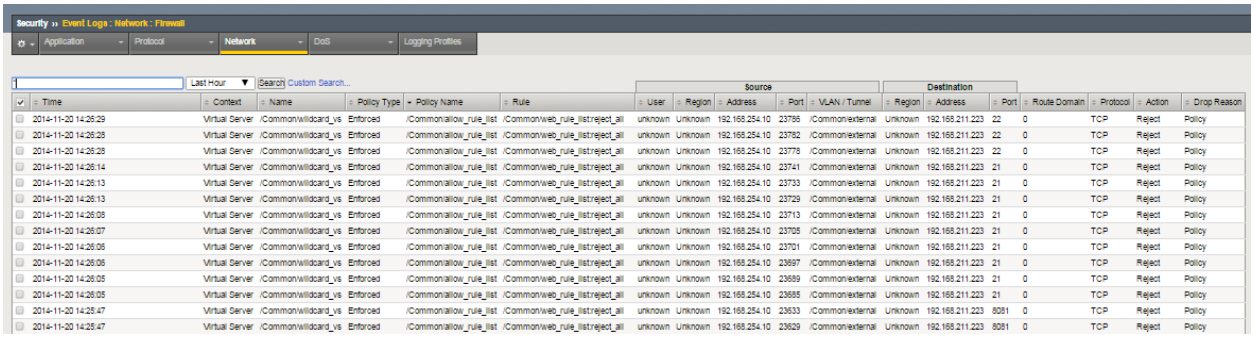
- Open a new Web browser and access *https://10.128.10.223*
- Edit the URL to *http://10.128.10.223*
- Edit the URL to *http://10.128.10.223:8081*
- Open either Chrome or Firefox and access *ftp://10.128.10.223*
- Open Putty and access 10.128.10.223

In the Configuration Utility, open the ***Security > Event Logs > Network > Firewall*** page.

Access for port 80 was granted to a host using the web_rule_list: ***allow_http*** rule and access for 443 was granted using the web_rule_list: ***allow_https rule***.

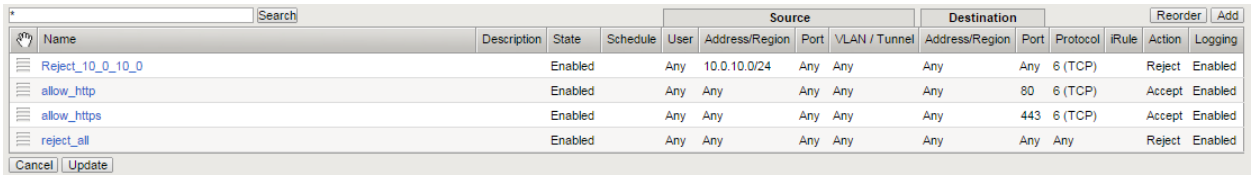


Requests for port 8081, 21, and 22 were all rejected due to the reject_all rule.



You may verify this, by going to ***Network > Route Domains***, then selecting the hyperlink for route domain 0, then select ***Security***. Note the ***Count*** field next to each rule as seen below. Also note how each rule will also provide a ***Latest Matched*** field so you will know the last time each rule was hit:

If you wanted to reject all traffic from the 10.0.10.0/24 network including HTTP & HTTPS, then open the ***Security > Network Firewall > Rules Lists*** page. Select ***web_rule_list*** and click the ***Reorder*** button. Use your mouse to move the ***reject_10_0_10_0*** rule above the ***allow_http rule***.



Click ***Update***.

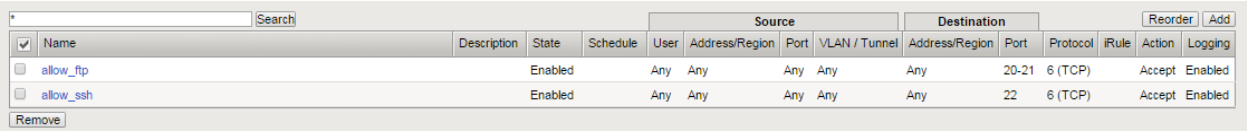
1.2.11 Creating a Rule List for Multiple Services

Rules and Rule Lists can also be created and attached to a context from the Active Rules section of the GUI. Go to the ***Security > Network Firewall > Rule Lists*** and create a ***Rule List*** called ***common_services_rule_list*** then click ***Finished***. Enter the rule list by clicking on its hyperlink, then in the ***Rules*** section click ***Add***, and add the following information:

Name	allow_ftp
Protocol	TCP
Destination: Port	Specify: Port Range: 20 to 21
Action	Accept
Logging	Enabled

Add another rule using the following information:

Name	allow_ssh
Protocol	TCP
Destination: Port	Specify: Single Port: 22 (be sure to delete the port range of 20-21)
Action	Accept
Logging	Enabled

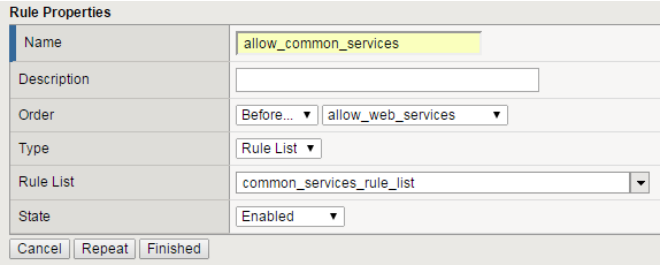


1.2.12 Add Another Rule List to the Policy

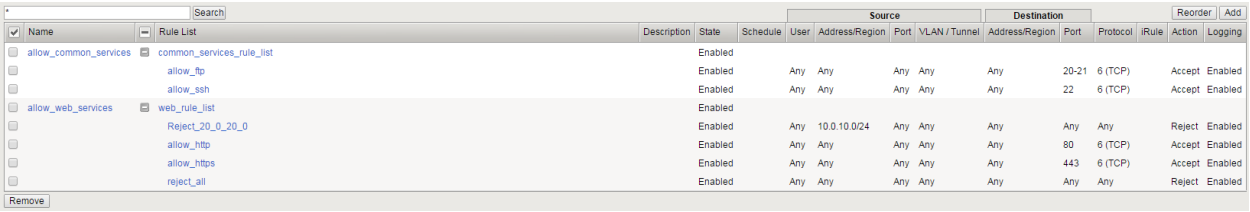
Use the ***Policies*** page to add the new firewall rule list to the ***rd_0_policy***. Open the ***Security > Network Firewall > Policies*** page. Click on the policy name to modify the policy.

The only current active rule list is for the web_policy. Click on ***Add*** to add the new rule list you just created.

Configure as seen below, for ***Name*** use ***allow_common_services***, for ***Order*** select ***Before*** ***web_policy***, and for ***Type*** select ***Rule List*** and select the rule ***common_services_rule_list***, then click ***Finished***.



You should see the policy similar to the one below:



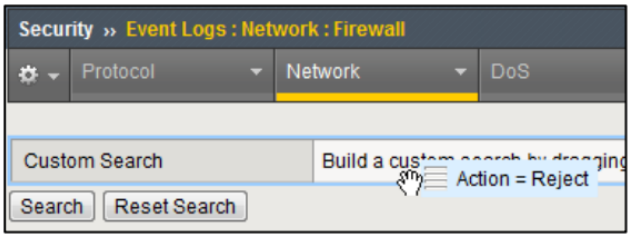
At this point all FTP and SSH traffic will be allowed, before BIG-IP AFM reaches the second rule list.

1.2.13 Test Access to the Wildcard Virtual Server

- Open a new Web browser and access *http://10.128.10.223:8081*
- Edit the URL to *https://10.128.10.223*
- Edit the URL to *http://10.128.10.223*
- Open either Chrome or Firefox and access *ftp://10.128.10.223*
- Open Putty and access 10.128.10.223
- Close all Web browsers and Putty sessions.

You should notice HTTP, HTTPS, FTP, and SSH traffic is now allowed through the firewall, while traffic destined to port 8081 is still rejected. If you do not see the 8081 request failing, you may need to refresh to avoid using the browser cache.

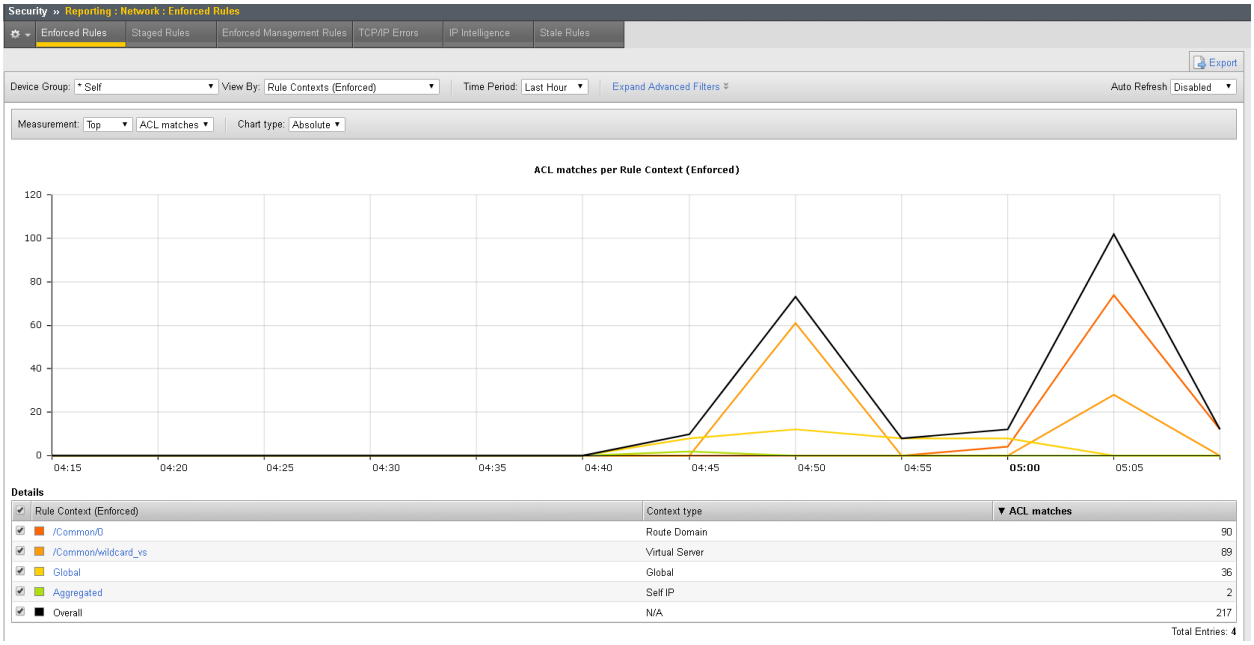
Next, you'll see how easy it is to search through the logs. In the Configuration Utility, open the ***Security > Event Logs > Network > Firewall*** page. Click ***Custom Search***. Select a ***Reject*** entry in the list (just the actual word "reject") and drag it to the custom search area.



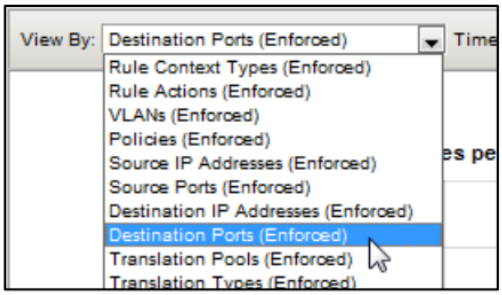
Click ***Search***. This will filter the logs so that it just displays all rejected entries.

1.2.14 View Firewall Reports

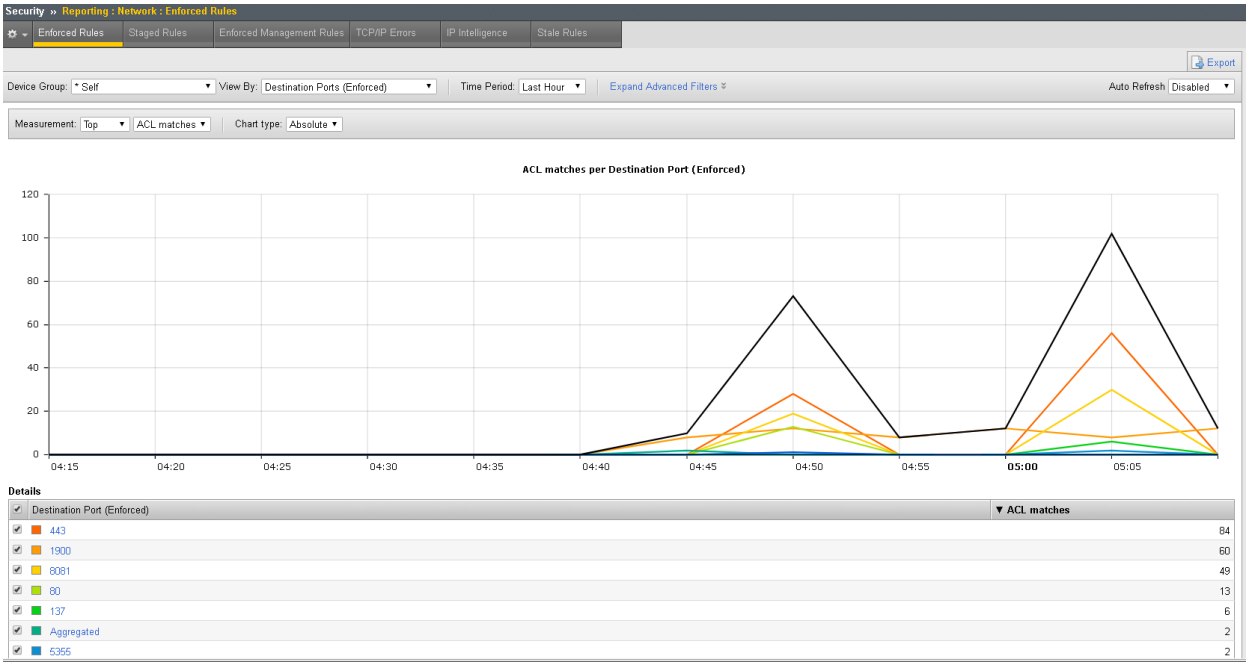
View several of the built-in network firewall reports and graphs on the BIG-IP system. On BIG-IP01 (10.0.0.4) open the ***Security >Reporting > Network > Enforced Rules*** page. The default report shows all the rule contexts that were matched in the past hour. The default view gives reports per Context, in the drop-down menu select ***Rules (Enforced)***.



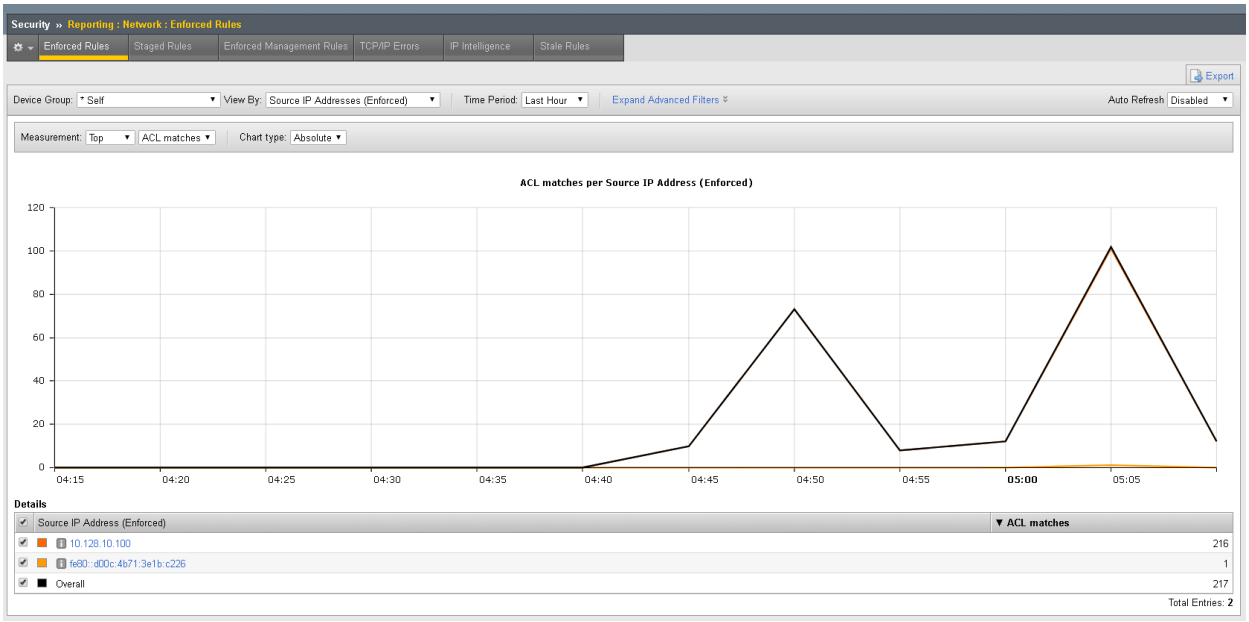
From the ***View By*** list, select ***Destination Ports (Enforced)***.



This redraws the graph to report more detail for all of the destination ports that matched an ACL.



From the ***View By*** list, select ***Source IP Addresses (Enforced)***. This shows how source IP addresses matched an ACL clause:

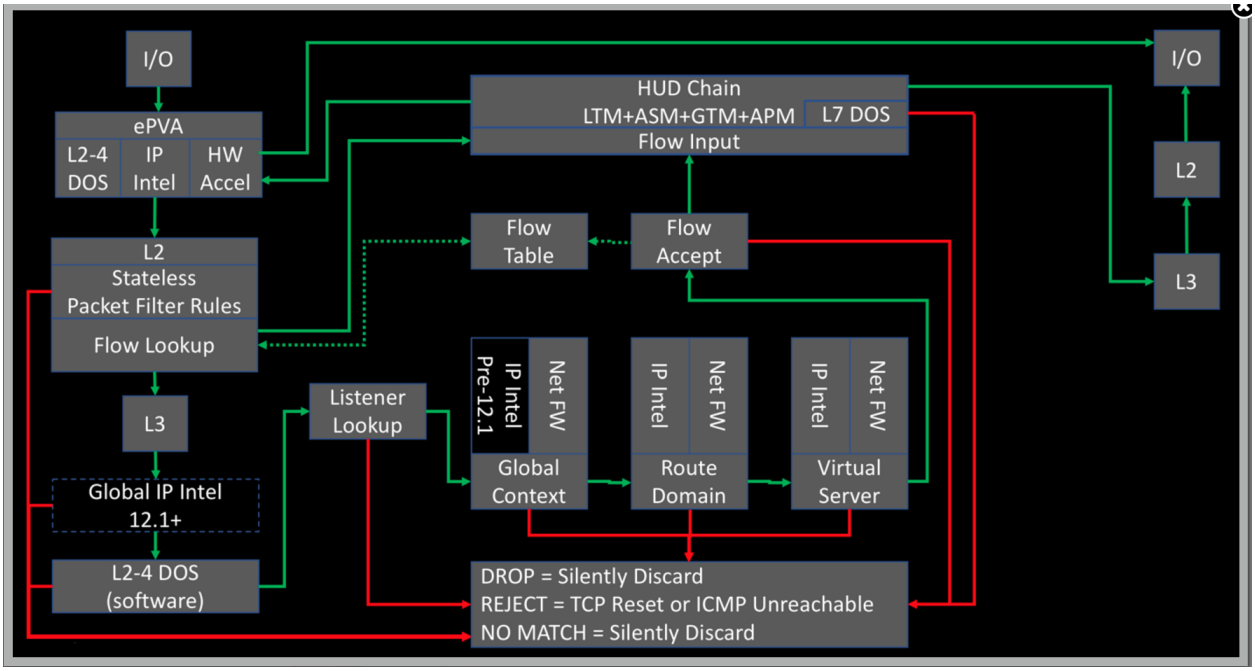


1.2.15 AFM Reference Material

- Network World Review of AFM: F5 data center firewall aces performance test
- AFM Product Details
- AFM Operations Guide

1.3 Module 2: AFM Packet Tester

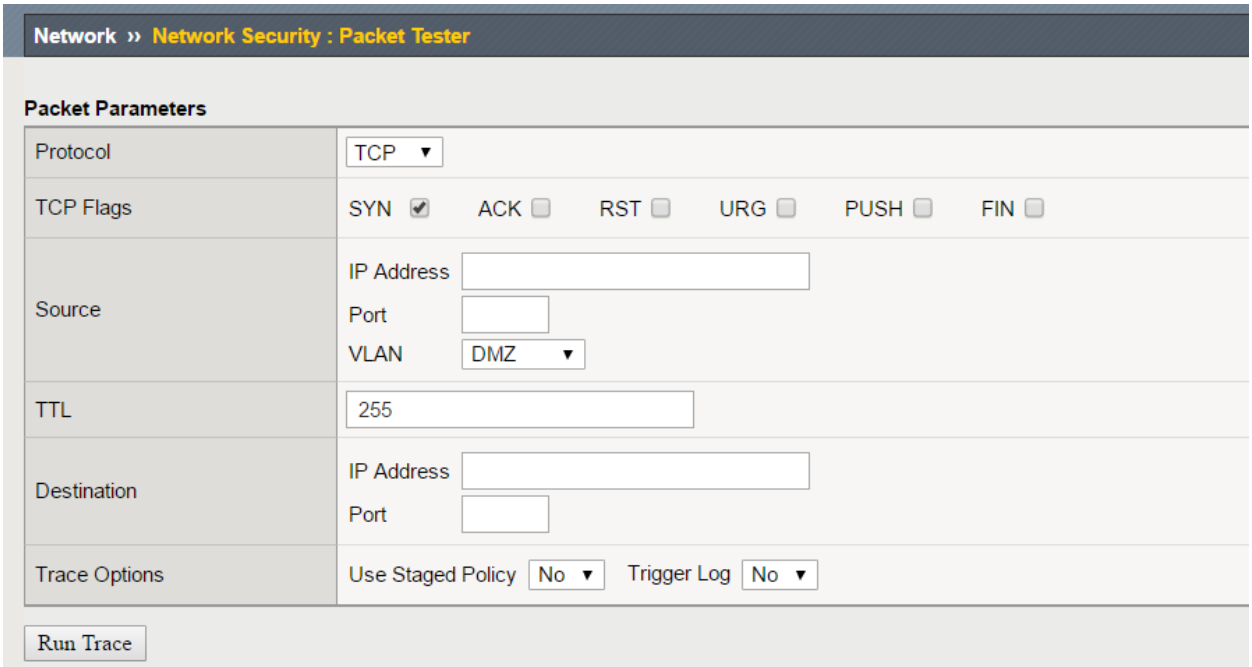
New in the v13 release of the BIG-IP Advanced Firewall Manager is the capability to insert a packet trace into the internal flow so you can analyze what component within the system is allowing or blocking packets based on your configuration of features and rule sets.



The packet tracing is inserted at L3 immediately prior to the Global IP intelligence. Because it is after the L2 section, this means that a) we cannot capture in tcpdump so we can't see them in flight and b) no physical layer details will matter as it relates to testing. That said, it's incredibly useful for what is and is not allowing your packets through. You can insert tcp, udp, sctp, and icmp packets, with a limited set of (appropriate to each protocol) attributes for each.

1.3.1 Create and View Packet Tracer Entries

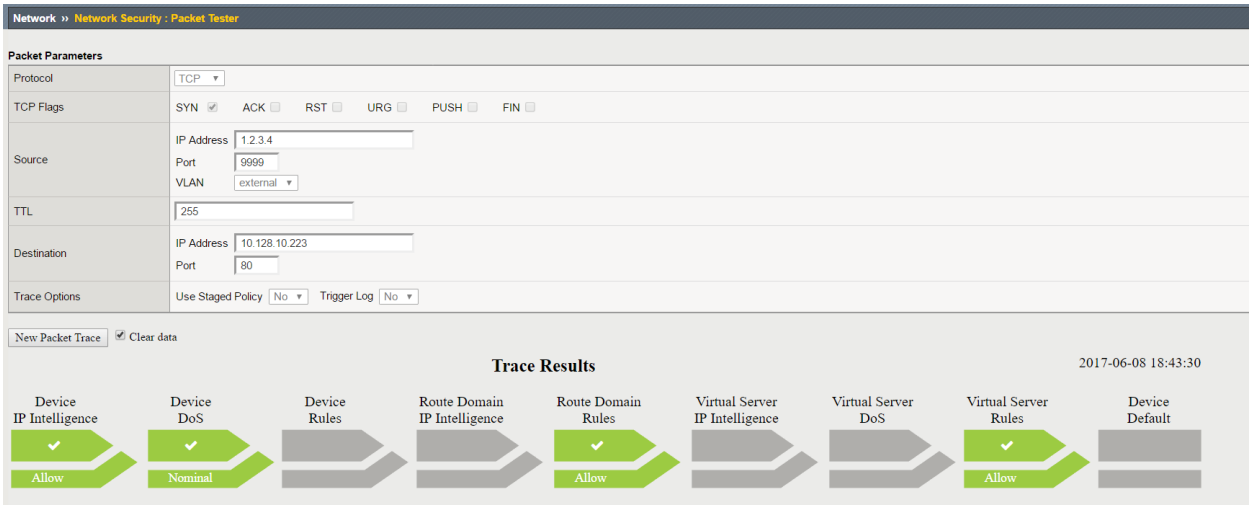
In this section, you will generate various types of traffic as you did previously, but now you will view the flow using the network packet tracer. Login to bigip01.agility.com (10.0.0.4), open the ***Network > Network Security > Packet Tester*** page.



Create a packet test with the following parameters.

Protocol	TCP
TCP Flags	SYN
Source	IP - 1.2.3.4 Port – 9999 Vlan – External
TTL	255
Destination	IP – 10.128.10.223 Port – 80
Trace Options	Use Staged Policy – no Trigger Log - no

Click Run Trace to view the response. Your output should resemble the allowed flow as shown below:

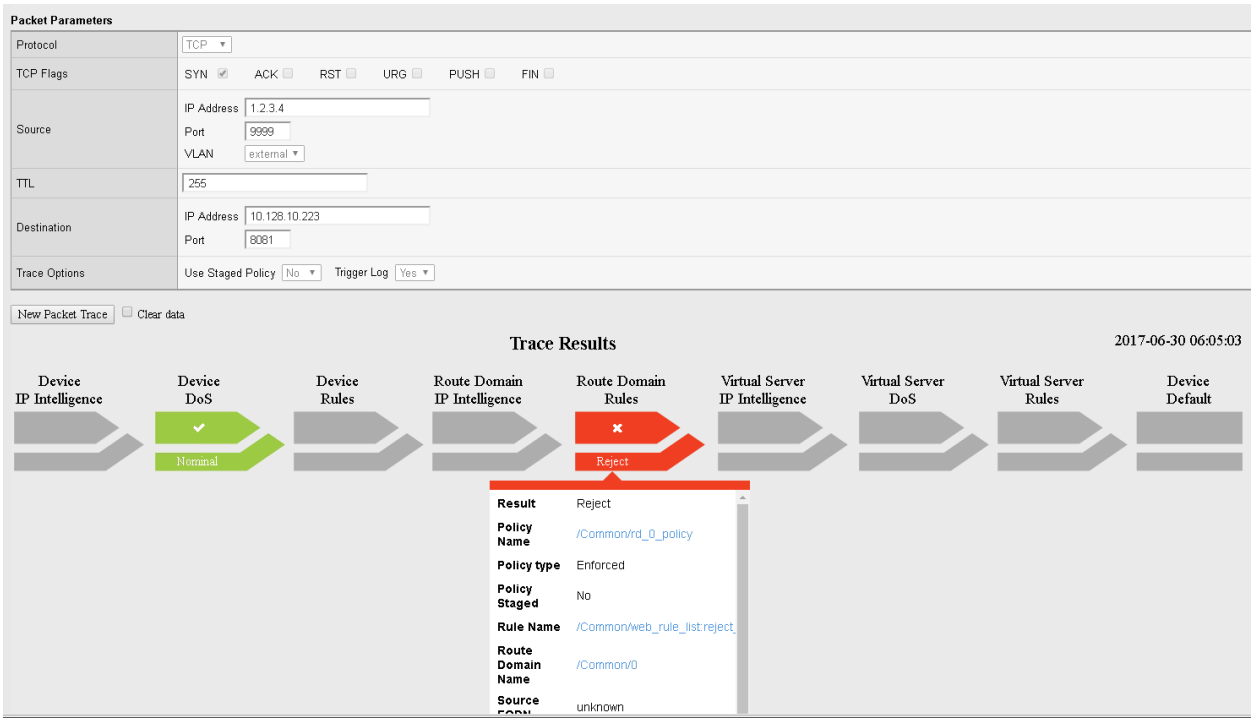


Click **New Packet Trace** (optionally do not clear the existing data).

Create a packet test with the following parameters.

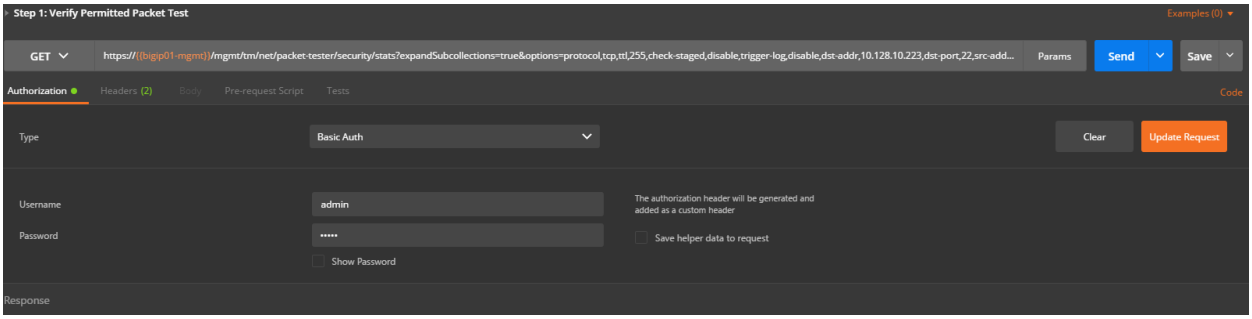
Protocol	TCP
TCP Flags	SYN
Source	IP - 1.2.3.4 Port – 9999 Vlan – External
TTL	255
Destination	IP – 10.128.10.223 Port - **8081**
Trace Options	Use Staged Policy – no Trigger Log - yes

Click Run Trace to view the response. Your output should resemble the allowed flow as shown below:



You can click on the /common/rd_0_policy hyperlink to examine the policy which is rejecting the request.

You can also perform the same tests using the API. To do, so launch POSTMan and use the collections for Lab 2. The first call will mirror what was sent in the accept. The second call will mirror what was sent in the rejected response. Example shown below:



If you examine the JSON output for the second request, the rejected request, you'll notice the following lines within the JSON output:

```
{

"acl_rtdom_policy_type": {
```

```
            "description": "Enforced"
},
"acl_rtdom_rule_name": {
            "description": "/Common/web_rule_list:reject_all"
}
```


This is the same rule which was show in the UI packet tester for the rule that is not permitting this request. If you search for the keys above in the permitted flow you'll notice the output is quite different.

These are possible values:


```
var aclActionType = {"0":"Drop","1":"Reject","2":"Allow","3":"Decisive Allow",
"4":"Default","5":"Prior Decisive","6":"Default Rule Allow","7":"Default
Rule Drop","8":"Default Rule Reject","9":"Allow (No Policy)", "10":"Allow
(No Match)","11":"Prior Drop","12":"Not Applicable","13":"Drop (Flow Miss)",
"14":"Prior Reject"}

var dosActionType = {"0":"Default","1":"Allow (No Anomaly)","2":"White
List","3":"Allow (Anomaly)","4":"Drop (Rate Limited)","5":"Drop (Attack)",
"6":"Prior White List","7":"Allow (No Policy)","8":"Prior Drop","9":"Drop
(Flow Miss)","10":"Not Applicable","11":"Prior Reject"}

var ipiActionType = {"0":"Default","1":"Allow","2":"Drop","3":"Allow (White
List)","4":"Allow (No Policy)", "5":"Allow (No Match)","6":"Prior Drop",
"7":"Drop (Flow Miss)","8":"Not Applicable","9":"Prior Reject"};
```


acl_device_is_default_rule = could be true or false.

1.4 Module 3: DDoS Protection with AFM

During this lab, you will configure the BIG-IP system to detect and report on various network level Denial of Service events. You will then run simulated attacks against the BIG-IP and verify the mitigation, reporting and logging of these attacks.

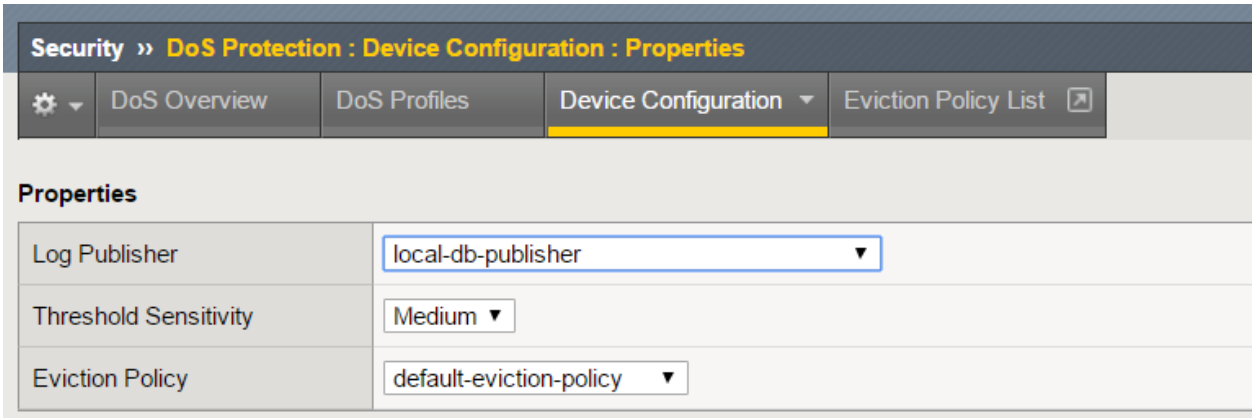
1.4.1 Create a Pool and Virtual Server using REST API

Use the POSTMan collection named "Service Provider Specialist Event - Lab 3a" to create the necessary pools and virtual servers for this exercise.

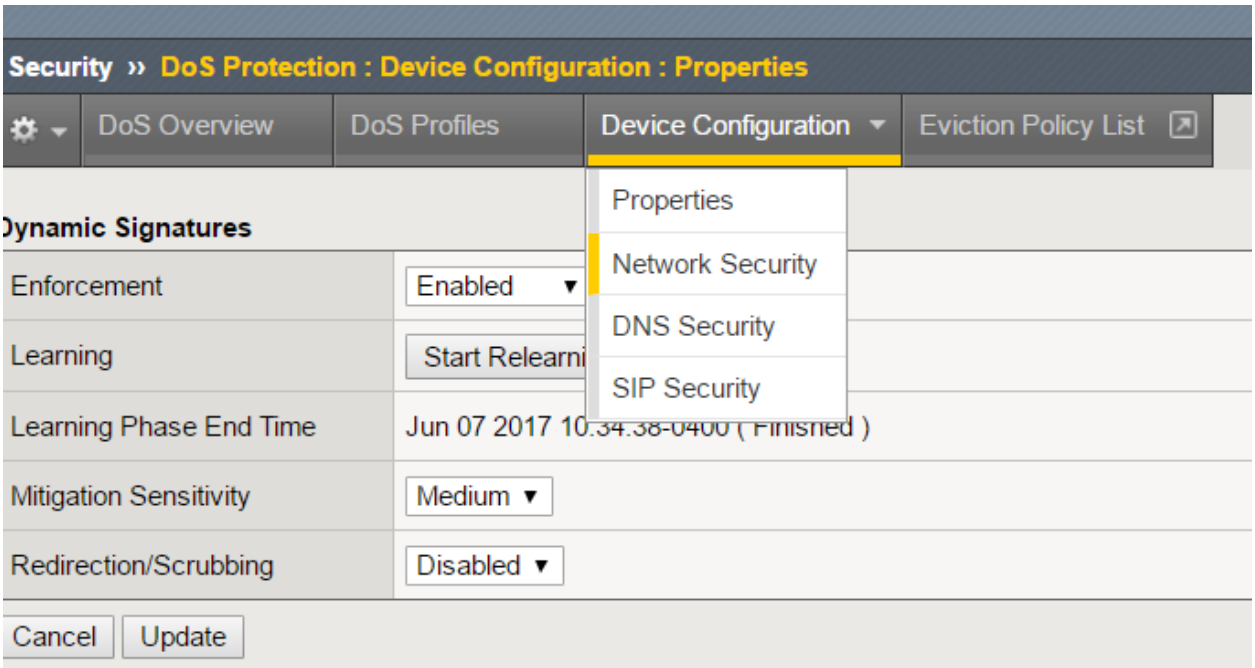
Verify connectivity to the new virtual server by opening a browser and connecting to *http://10.128.10.20*

1.4.2 Configuring DoS Protection

Since we are in a lab environment with no production traffic, we will need to lower some of the default values for DoS detection values so that attacks are seen in a timely manner. We are also going to verify the DoS events are logged locally. Log into bigip01.agility.com (10.0.0.4), access the ***Security > DoS Protection > Device*** ***Configuration*** → ***Properties*** page. From the ***Log Publisher*** list, verify ***local-db-publisher*** is selected.



- Select Network Security from the Device Configuration drop down at the top



- Select the + sign next to ***Bad-Header – Ipv4***
- Then select ***Bad IP TTL Value***.
- Specify the following threshold values and Click ***Update*** when finished:

Detection Threshold PPS	25
Detection Threshold Percent	100
Leak Limit/Rate Limit PPS	25

This is what set's F5's BIG-IP apart from other offerings. It monitors for DoS activity and when a DoS event is detected, it will not block all traffic from a IP address, as this could affect legitimate traffic such as that behind a proxy. Instead, the Big-IP will limit only the offending traffic allowing legitimate traffic to pass through. Below is some background on how the detection mechanism works:

Detection Threshold PPS: This is the number of packets per second (of this attack type) that the BIG-IP system uses to determine if an attack is occurring. When the number of packets per second goes above the threshold amount, the BIG-IP system logs and reports the attack, and then continues to check every

second, and marks the threshold as an attack if the threshold is exceeded. The default value is 10,000 packets per second, but we'll change the values to 25 packets per second for the purposes of this demo.

Detection Threshold Percent: This is the percentage increase value that specifies an attack is occurring. The BIG-IP system compares the current rate to an average rate from the last hour. For example, if the average rate for the last hour is 1000 packets per second, and you set the percentage increase threshold to 100, an attack is detected at 100 percent above the average, or 2000 packets per second. When the threshold is passed, an attack is logged and reported.

The BIG-IP system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped. The BIG-IP system continues to check every second until the incoming packet rate drops below the percentage increase threshold. Rate limiting continues until the rate drops below the specified limit again. The default value is 500 percent, but we'll change the values to 100 percent for the purposes of this demo. This is the lowest value allowed for this setting.

Rate/Leak Limit: This is the value, in packets per second that cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again. The default value is 10,000 packets per second, but we'll change the values to 25 packets per second.

We will set the thresholds for other DDoS events, but rather than go through the GUI for each one, we will set the thresholds for all of them at once using tmsh CLI commands. To do so go to the following URL to see the tmsh commands that will be used:

http://10.128.20.150/ddos-commands.txt

Optionally, you can use the POSTMan collection "Service Provider Specialist Event - Lab 3b" to modify the values on both devices.

Copy all the DDoS commands and then open up an SSH session (via Putty or similar program) to the management IP address of bigip01.agility.com (10.0.0.4). Login with the following credentials:

- User: root
- Password: 401elliottW!

Once you are connected paste in the tmsh commands from the web page into the SSH session to set the DoS thresholds. The following parameters will be set:

- **Bad Header – IPv4**
- Bad IP Version
- Header Length > L2 Length
- Header Length Too Short
- IP Error Checksum
- IP Length > L2 Length
- IP Source Address == Destination Address
- L2 length >> IP length
- No L4
- **Bad Headers - TCP**
- Bad TCP Checksum
- Bad TCP Flags (All Flags Set)
- FIN Only Set
- SYN & FIN Set

- TCP Header Length > L2 Length
- TCP Header Length Too Short (Length < 5)
- **Flood**
- ICMP Flood
- **Fragmentation**
- IP Fragment

Close the PuTTY session to disconnect from the BIG-IP.

1.4.3 Run an Attack Script against your Virtual Server

Open an SSH session to the Ubuntu server **10.128.10.250** using Putty or the command line. Login using the username **root** with the password **default**.

Once logged in, list the contents of the current directory using the ***ls*** command. You should see a filename similar to ***dos-attack-2xx-commands.txt*** file. This file contains various DoS attack commands that you will run from the Ubuntu machine you are currently logged into. It may be easiest to copy the file or its contents to your local desktop or open another SSH session so you will have easy access to the commands while you open a program on the Ubuntu server called ***Scapy*** to run the DDoS commands.

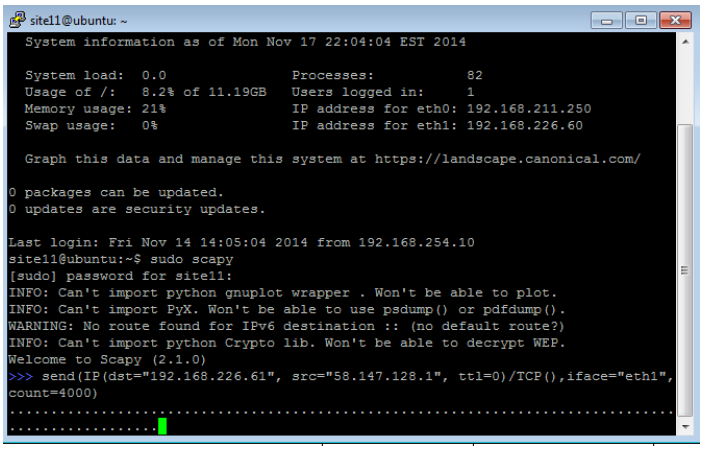
Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery (it can replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f, etc.). If you want to learn more about Scapy the link below is provided for reference:

http://www.secdev.org/projects/scapy/

We will be using Scapy to create specific attacks to launch at your Virtual Server. We'll then verify the logging and reporting as well as attack mitigation of the BIG-IP.

While logged into the Ubuntu server type the following command: ***scapy***

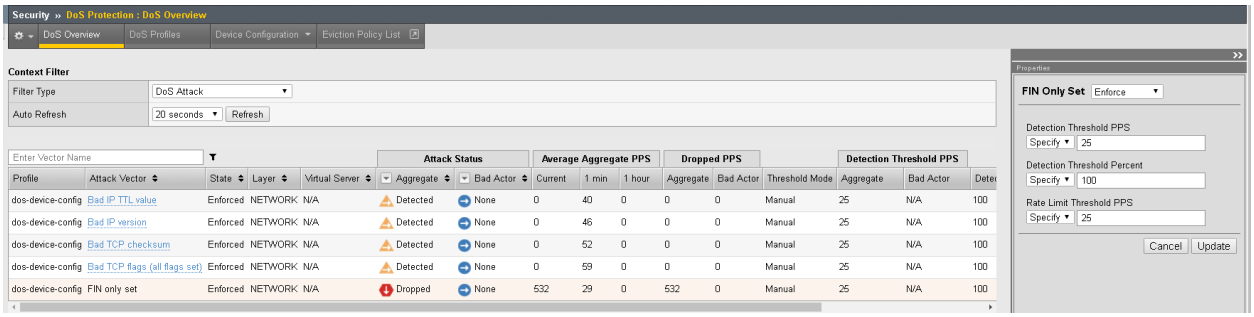
Copy the first attack command for ***Bad IP TTL value***, and then paste the command in the scapy terminal window and hit enter. You should see dots move across the screen indicating that the attack is being sent.



- This attack will launch 4000 packets that are configured to send IP requests with a TTL value of 0

1.4.4 View DoS Logging

Use the BIG-IP configuration utility to view the DoS logging. While the attacks are running, access **Security > DoS Protection > DoS Overview**.

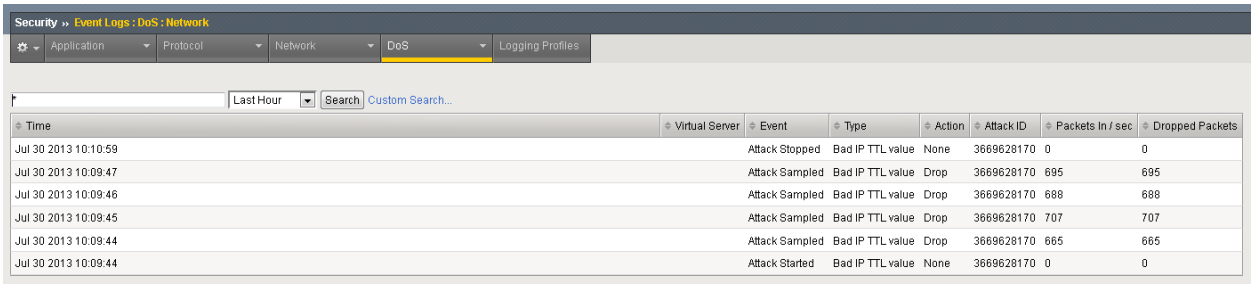


Note that the attack vector properties are available for modification to the right. This is useful during an attack if a value needs to be immediately modified.

In the configuration utility access, the ***Security > Event Logs > DoS > Network > Events*** page. If necessary, sort the list in descending order by the Time column.

Time	Virtual Server	Event	Type	Action	Attack ID	Packets In / sec	Dropped Packets
2014-11-14 18:10:49		Attack Stopped	Bad IP TTL value	None	3234340500	0	0
2014-11-14 18:09:42		Attack Sampled	Bad IP TTL value	Drop	3234340500	784	784
2014-11-14 18:09:41		Attack Sampled	Bad IP TTL value	Drop	3234340500	757	757
2014-11-14 18:09:40		Attack Sampled	Bad IP TTL value	Drop	3234340500	738	738
2014-11-14 18:09:39		Attack Sampled	Bad IP TTL value	Drop	3234340500	772	772
2014-11-14 18:09:39		Attack Started	Bad IP TTL value	None	3234340500	0	0

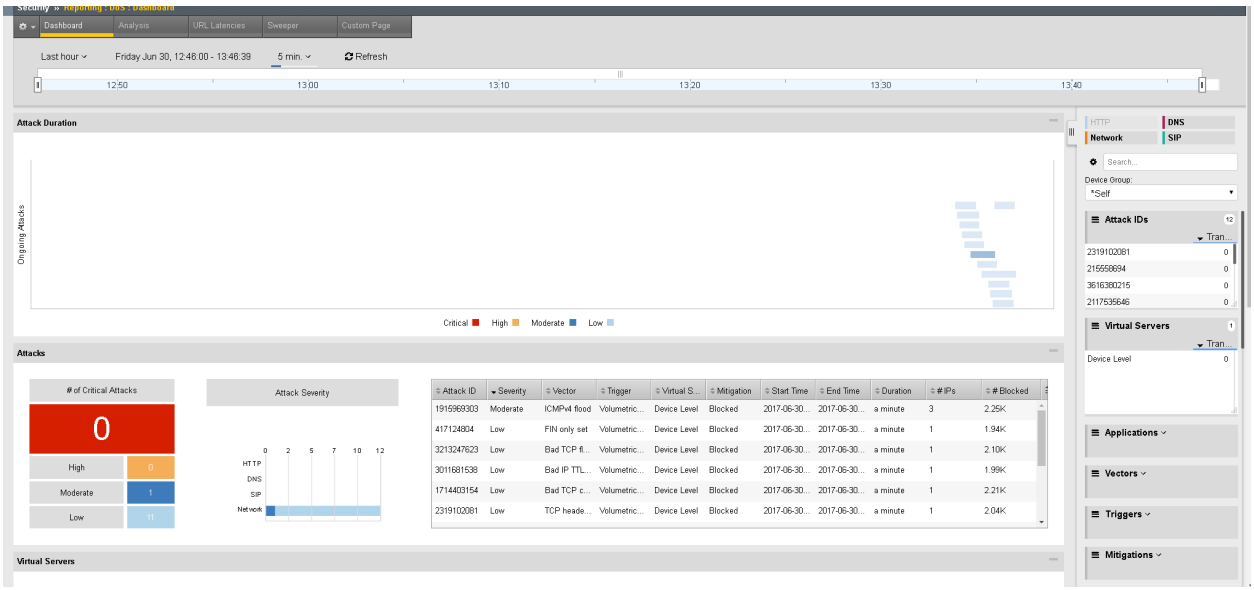
There should be an entry that was created when the BIG-IP identified the start of the DoS attack, and then one or more entries for dropped packets every second that the DoS attack continued. Eventually there will be an entry for when the BIG-IP determines that the DoS attack has stopped.



Note the ***Action*** and ***Dropped Packets*** column, this indicates that the BIG-IP not only detected the attack, but it also mitigated the attack by dropping the packets with the bad IP TTL value.

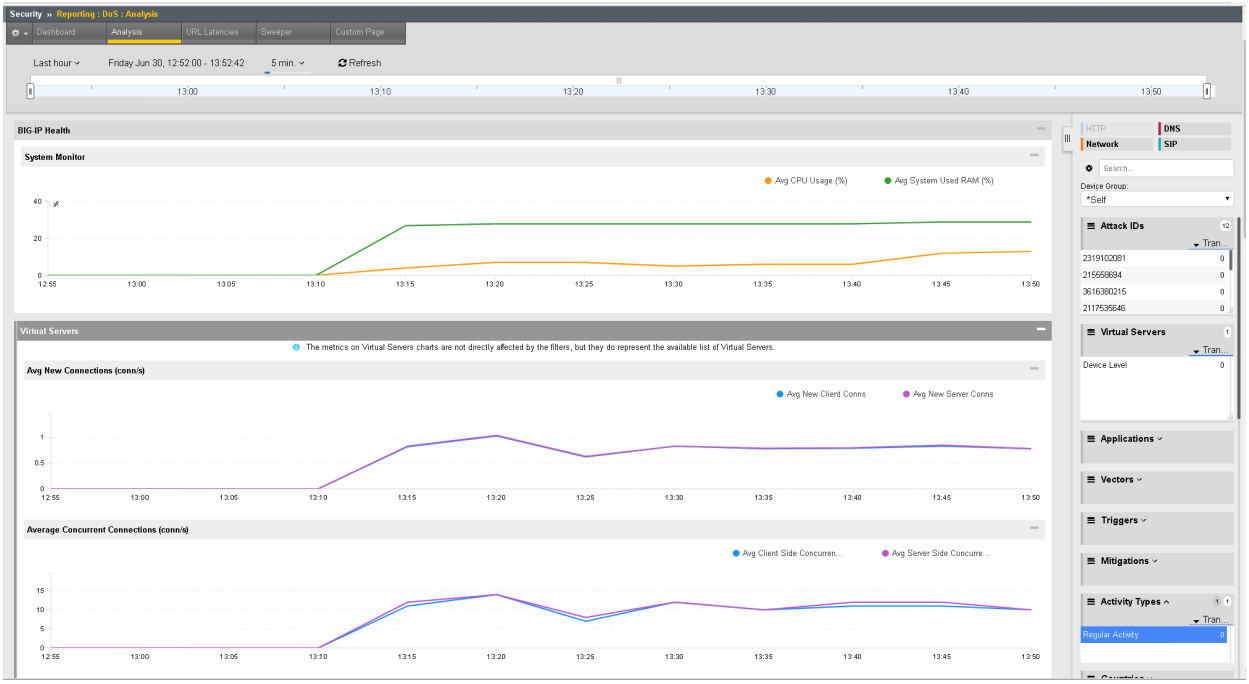
Repeat the same steps for all the network attacks in the file and be sure to verify the DoS logs and ensure each event has a start and a stop.

Once you are finished running and verifying all the attacks, we will then examine the network DoS reporting capabilities within the BIG-IP. In the configuration utility go to ***Security > Reporting > DoS > Dashboard (note it may take a few moments for the data to fully populate).*** You should see a screen similar to the one below.

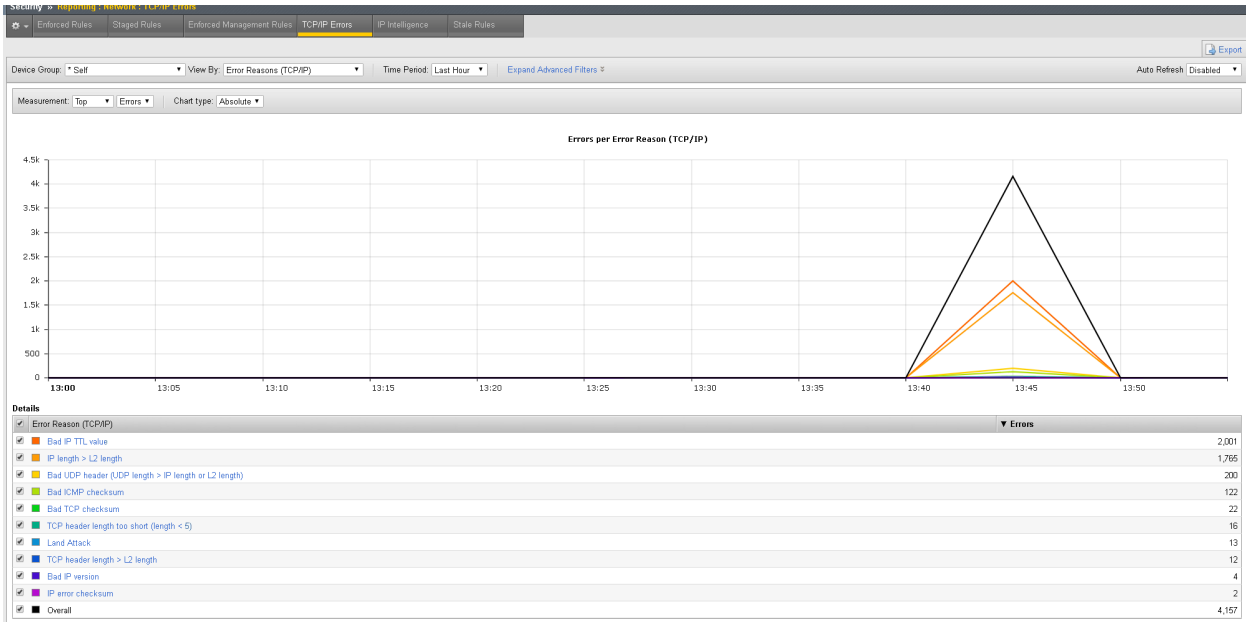


Note the real time CPU, RAM, and Throughput stats. When an attack has stopped the line will stop, so it's easy to see what attacks are still active. Feel free to explore the dashboard and the data represented.

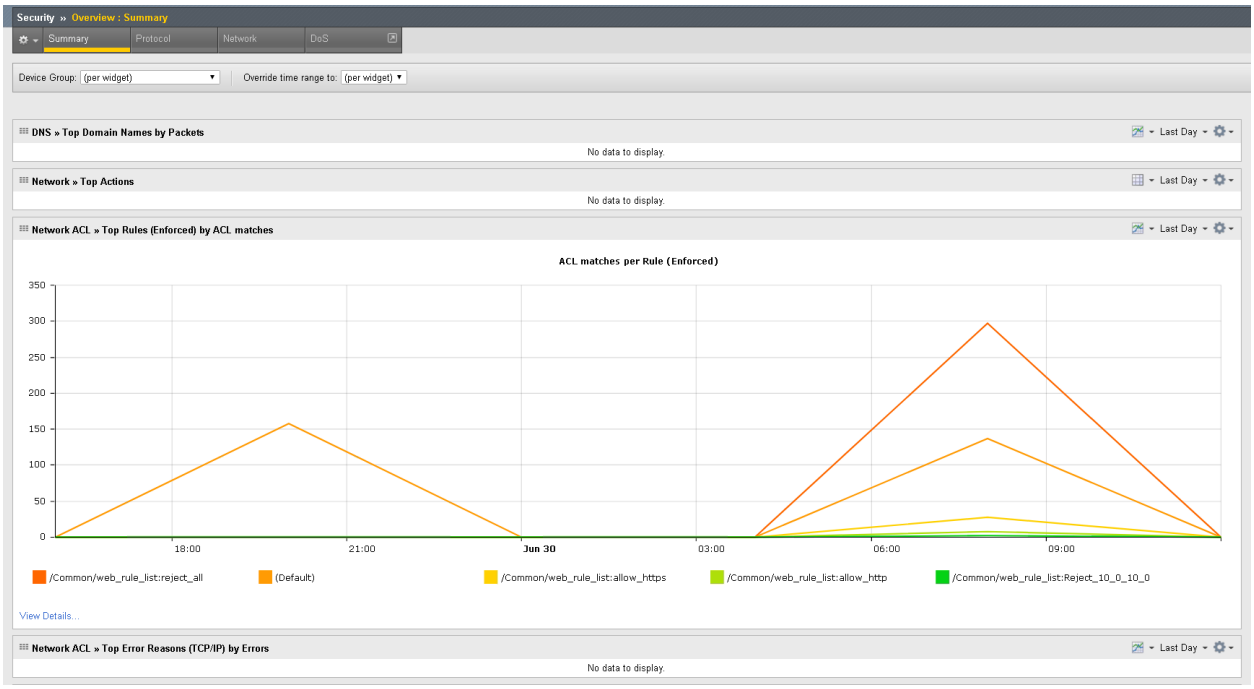
In the configuration utility go to ***Security > Reporting > DoS > Analysis (note it may take a few moments for the data to fully populate).*** You should see a screen similar to the one below.



In the configuration utility go to ***Security > Reporting > Network > TCP/IP Errors (note it may take a few moments for the data to fully populate).*** You should see a screen similar to the one below.



Examine the other options in the ***View By*** drop down menu. When you are finished examining the options go to ***Security > Overview > Summary*** screen. Try some of the various options in the top right of each chart. You can change between ***Details***, ***Line Chart***, ***Pie Chart*** and ***Bar Charts***. Also note how you can export this data to CSV or PDF format. Below are some examples of the summaries:



All of the reports are historical and provide aggregate stats based upon the selected time period (last day, month, year etc. . .). In version 11.6 real time DDoS monitoring was added so that an administrator can see what attacks are currently active, how serious they are, and how long they have been active. The real time DDoS attack reporting also provides visibility into the health of the BIG-IP by showing real time CPU, RAM, and Throughput consumption.

Paste in all of the DDoS attack commands into the Scapy window again. In the BIG-IP GUI go to ***Security > Reporting > DoS > Overview Summary***.

This concludes the AFM DDoS lab.

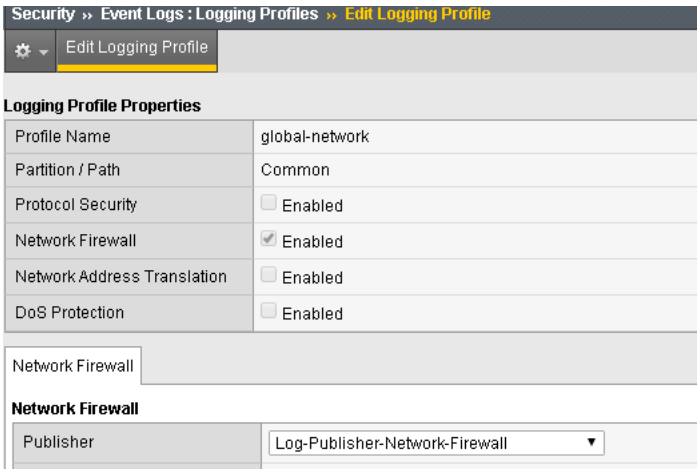
Before proceeding, please change the following logging settings for the remainder of the labs to work correctly:

Login to bigip01.agility.com (10.0.0.4).

Navigate to Security > Event Logs > Logging Profiles

Click on global-network

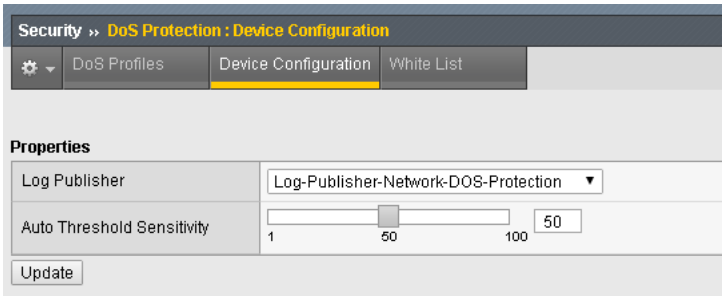
Modify the Network Firewall Publisher to ***Log-Publisher-Network-Firewall***



Click Update

Navigate to Security > DoS Protection > Device Configuration > Properties

Modify the Log Publisher to ***Log-Publisher-Network-DOS-Protection***



Click Commit Changes to System

1.4.5 Test Access to the Wildcard Virtual Server

- Open a new Web browser and access *http://10.128.10.223:8081* **(this is expected to fail due to policy)**
- Edit the URL to *https://10.128.10.223*
- Edit the URL to *http://10.128.10.223*
- Open either Chrome or Firefox and access *ftp://10.128.10.223*
- Open Putty and access 10.128.10.223
- Close all Web browsers and Putty sessions.

- Paste in all the DDoS attack commands into the Scapy window again

1.5 Module 4: Device Management

During this lab, you will configure the BIG-IP system to detect and report on various network level Denial of Service events. You will then run simulated attacks against the BIG-IP and verify the mitigation, reporting and logging of these attacks.

1.5.1 BIG-IQ Workflow Overview

Statistics Dashboards

This is the real first step managing data statistics using a DCD (data collection device) evolving toward a true analytics platform. In this guide, we will explore setting up and establishing connectivity using master key to each DCD (data collection device).

- Enabling statistics for each functional area as part of the discovery process. This will allow BIG-IQ to proxy statistics gathered and organized from each BIG-IP device leveraging F5 Analytics iApp service (*https://devcentral.f5.com/codeshare/f5-analytics-iapp*).
- Configuration and tuning of statistic collections post discovery allowing the user to focus on data specific to their needs.
- Viewing and interaction with statistics dashboard, such as filtering views, differing time spans, selection and drill down into dashboards for granular data trends and setting a refresh interval for collections.

SSL Certificate Management

BIG-IQ 5.2 has introduced the ability to manage SSL certificates. From creating self-signed certificates to creating a CSR (Certificate Signing Request) provided to a Certificate Authority when applying for a SSL Certificate. Some features we will cover in this lab:

- Importing SSL certificates, key information and PKCS12 “Personal Information Exchange Syntax Standard” bundles.
- When discovering a BIG-IP device, BIG-IQ will import the metadata from the certificates discovered. These certificates are unmanaged. BIG-IQ provides the ability to move or convert to a fully managed certificate by porting SSL certificate source and SSL key properties into BIG-IQ.
- Related to searching to display where SSL certificates are used.
- Renew an expired self-signed SSL certificate on BIG-IQ.
- Provide a reference for a SSL certificate / key pair to a Server SSL profile.

Global Search

BIG-IQ 5.2 has introduced platform wide search that will allow the user to globally search for any object or object contents and display related-to objects. Some features we will cover in this lab:

- Search for specific terms across all of BIG-IQ.
- Narrow the scope to the search to show “all of an object type”.
- Selection of an object to drill into an editable page.
- Search for specific CVE-####-#### in attack signatures documentation to find an ASM signature.

Partial Deployment/Partial Restore

BIG-IQ 5.2 has introduced the flexibility to deploy or restore selective changes made:

- Provides a user the ability to select only changes, out of many, he or she wants or is approved to deploy during the evaluation process.
- As well as the ability to rollback or restore selective changes out of multiple staged changes.

New Server SSL Profiles

- Client / Server SSL – Enables BIG-IP to initial secure connections to SSL servers using fully SSL-encapsulated protocol.
- HTTP – This profile will leverage the header contents to define the way to manage http traffic through BIG-IP.
- Universal / Cookie Persistence -
  - Universal persistence profile. To persist connections based on the string.
  - Cookie-based session persistence. Cookie persistence directs session requests to the same server based on HTTP cookies that the BIG-IP system stores in the client's browser.

Public Facing REST API References and HOWTO Guides

BIG-IQ 5.2 has introduced documentation that will assist the Engineer when automating central management tasks or providing integration with orchestration tools using a REST API using HTTPS. In this lab, we will explore a couple example API Calls and supporting reference and how-to documents.

- Device Management – trust, discover, enable statistics and import configuration.
- Add a policy (firewall) to an application – select an existing policy and reference to a virtual server.

Licensing Server

BIG-IQ 5.1 and 5.2 licensing support for four differing pool models. Using the base registration key and correct SKU, users can enable and activate BIG-IP virtual editions of types:

- Purchased Pools – are purchased once, and you assign them to a number of concurrent BIG-IP VE devices, as defined by the license. These licenses do not expire. Purchased license pools contain VEP in the name of the license.
- Volume Pools - are prepaid for a fixed number of concurrent devices, for a set period of time, but have a number of different license offerings available in the pool. Volume license pools contain VLS in the name of the license.
- Utility License Pools – provide the customer the ability to use licenses as they need them, and true up with F5 for their actual usage. VE licenses can be granted with usage billing at an hourly, daily, monthly, or yearly interval. Utility license pools contain MSP-LOADV in the name of the license.
- Registration Key Pools – A pool of single standalone BIG-IP virtual edition registration keys, allowing customers to import their existing keys and/or import new keys with just the options they require.

1.5.2 Dependencies

- The BIG-IP device must be located in your network.
- The BIG-IP device must be running a compatible software version.
- Enable basic authentication on BIG-IQ using set-basic-auth on in the shell.

BIG-IP Versions AskF5 SOL with this info:

https://support.f5.com/kb/en-us/solutions/public/14000/500/sol14592.html

---

Note: Ports 22 and 443 must be open to the BIG-IQ management address, or any alternative IP address used to add the BIG-IP device to the BIG-IQ inventory.

Description	Minimum BIG-IP version
Backup/Restore	11.5.0 HF7
Upgrade - legacy devices	10.2.0
Upgrade - managed devices	11.5.0 HF7
Licensing BIG-IP VE	11.5.0 HF7
Licensing – Web-Safe	12.0.0
ADC management	11.5.1 HF4
AFM	11.5.2
Access	12.1.0
ASM	11.5.3 HF1
DNS	12.0.0

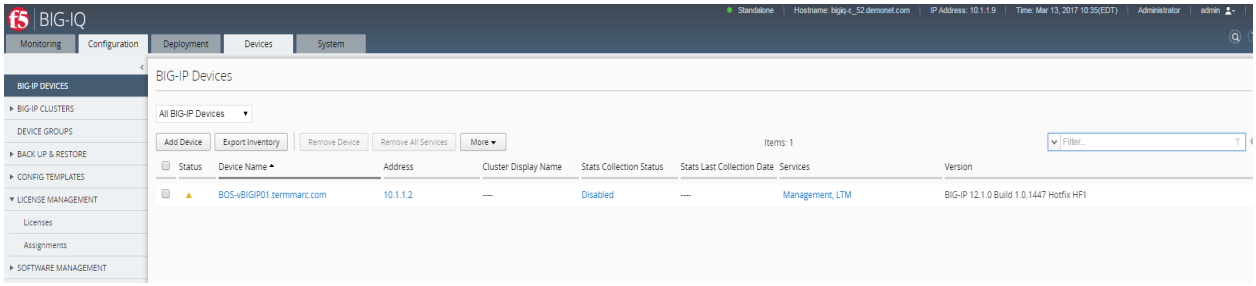
1.5.3 Changes to BIG-IQ User Interface

The user interface in the 5.2 release navigation has changed to a more UI tab based framework.

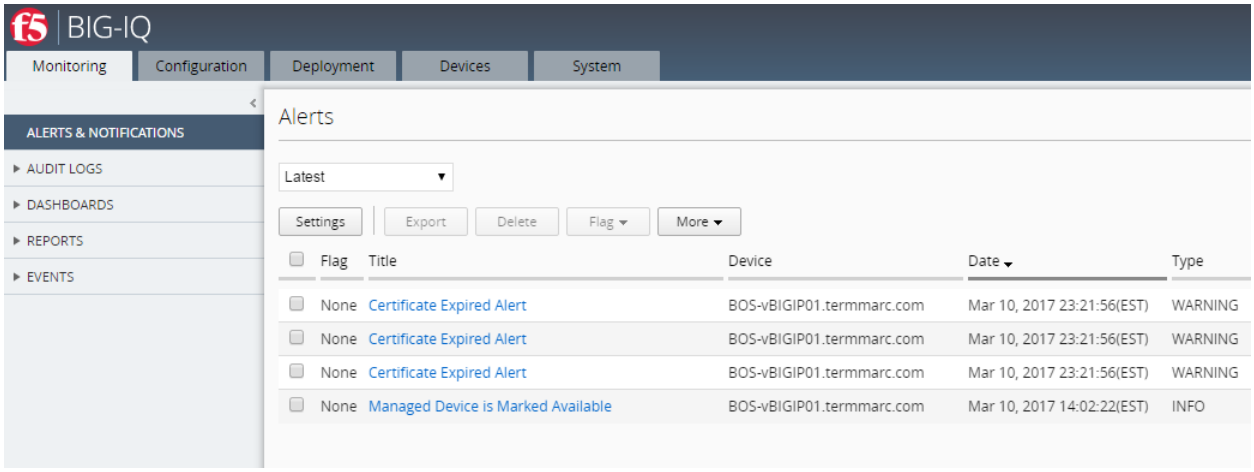
In this section, we will go through the main features of the user interface. Feel free to log into the BIG-IQ device to explore some of these features in the lab.

After you log into BIG-IQ, you will notice:

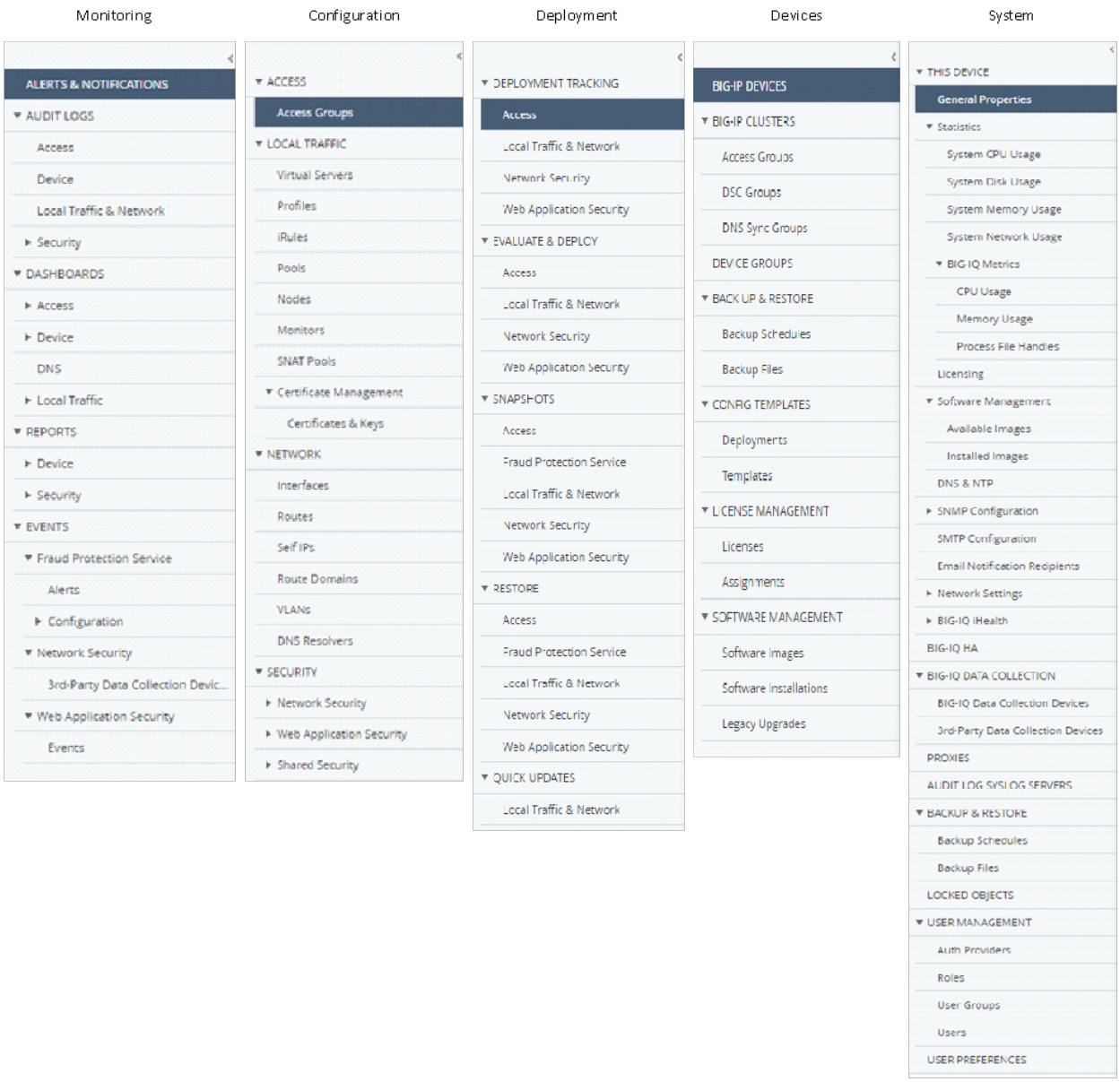
- A navigation tab model at the top of the screen to display each high level functional area.
- A tree based menu on the left-hand side of the screen to display low-level functional area for each tab.
- A large object browsing and editing area on the right-hand side of the screen.



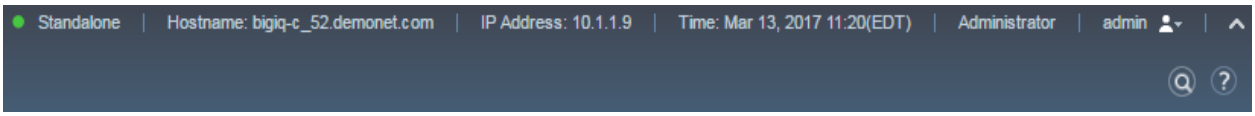
- Let us look a little deeper at the different options available in the bar at the top of the page.



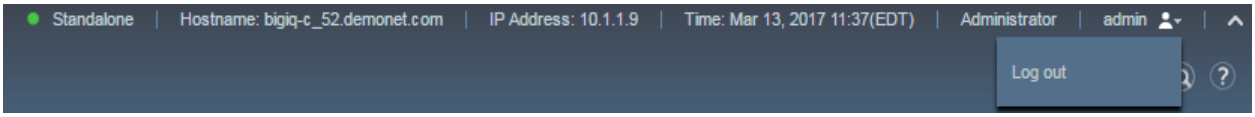
- At the top, each tab describes a high-level functional area for BIG-IQ central management:
- Monitoring –Visibility in dashboard format to monitor performance and isolate fault area.
- Configuration – Provides configuration editors for each module area.
- Deployment – Provides operational functions around deployment for each module area.
- Devices – Lifecycle management around discovery, licensing and software install / upgrade.
- System – Management and monitoring of BIG-IQ functionality.
- Overview of left hand navigation for each top-level functional area.



BIG-IQ 5.2 has introduced "**global search**" which was added to the BIG-IQ toolbar top here, and will be explored further in this lab.



Next to the username, there is an icon of a person. If you click on that icon, a menu appears to allow a user to logout of BIG-IQ.



1.5.4 BIG-IQ Statistics Dashboards

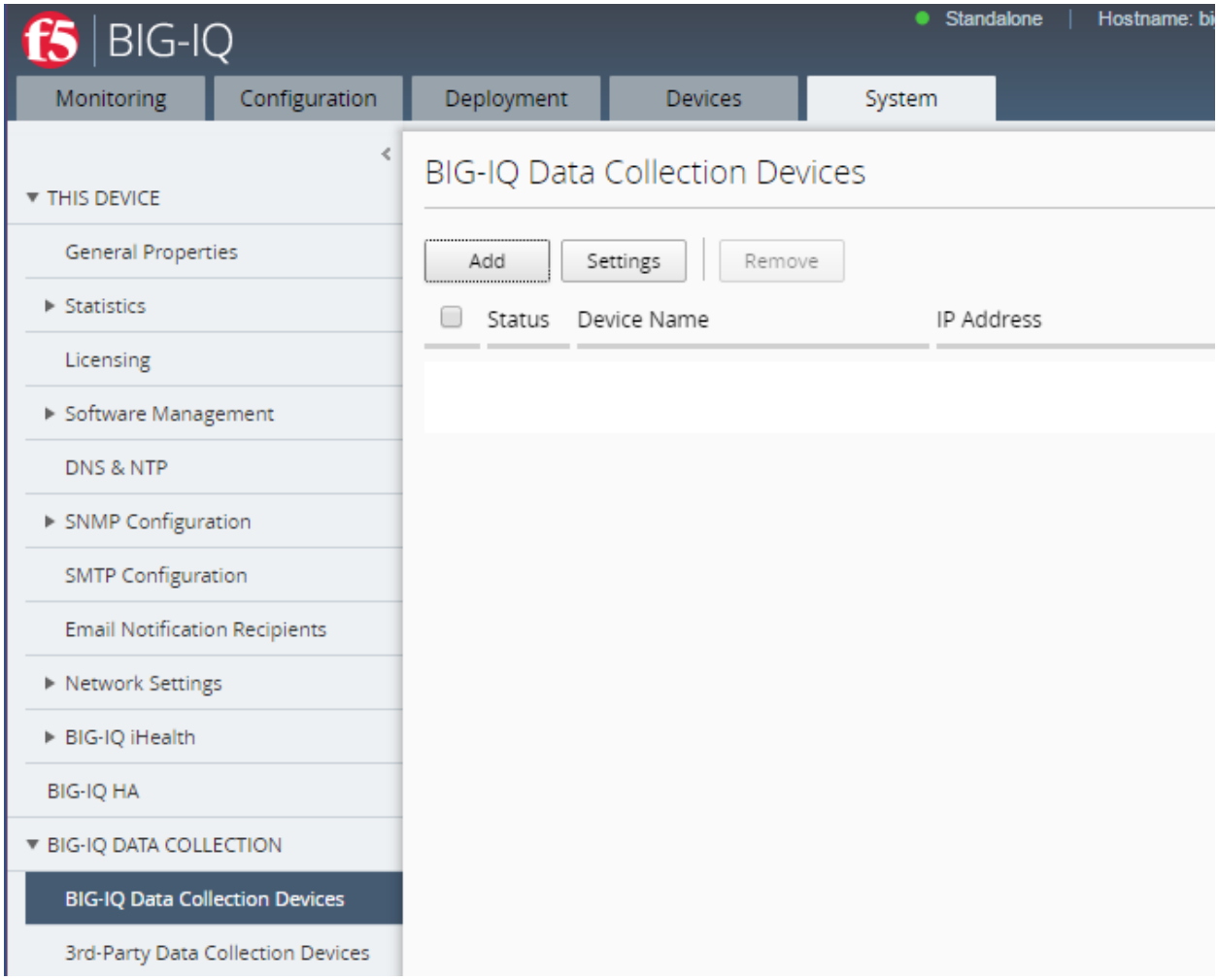
WORKFLOW 1: Setting up of BIG-IQ Data Collection Devices (DCD) and establishing connectivity to BIG-IQ console. (REQUIRED)

Objective

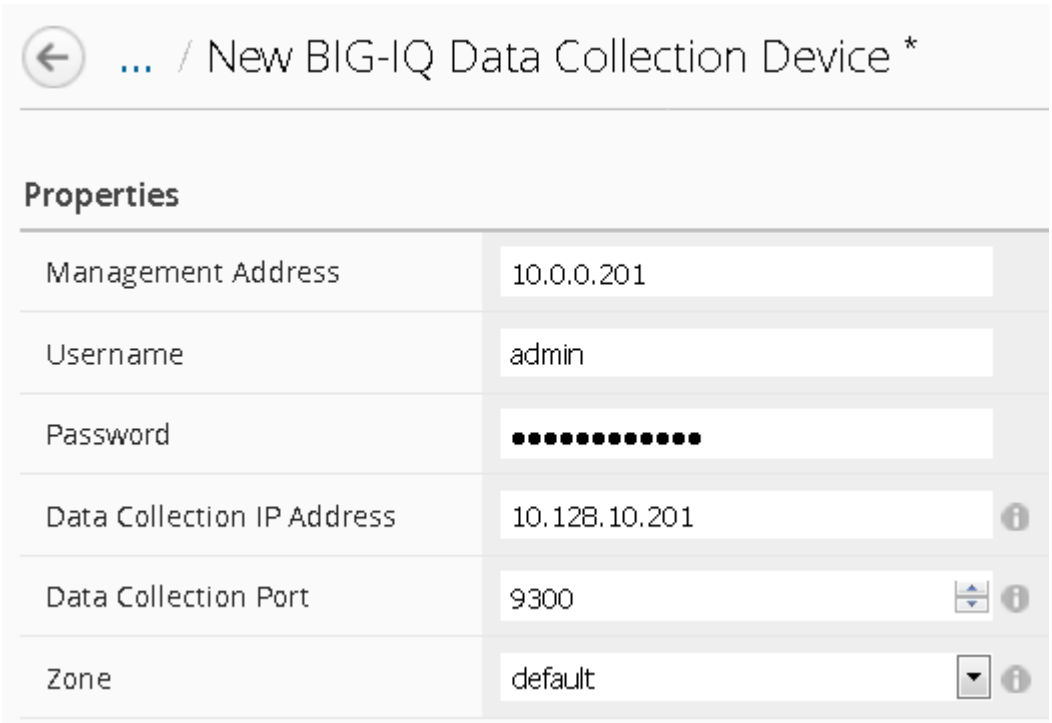
To introduce the user to a DCD, establish connectivity with BIG-IQ console node to begin data collection task. For the purposes of this lab the Data Collection Device has already been deployed and licensed with the appropriate license key (F5-BIQ-LOGNOD101010E-LIC).

Click Add to add a DCD to the BIG-IQ console node.

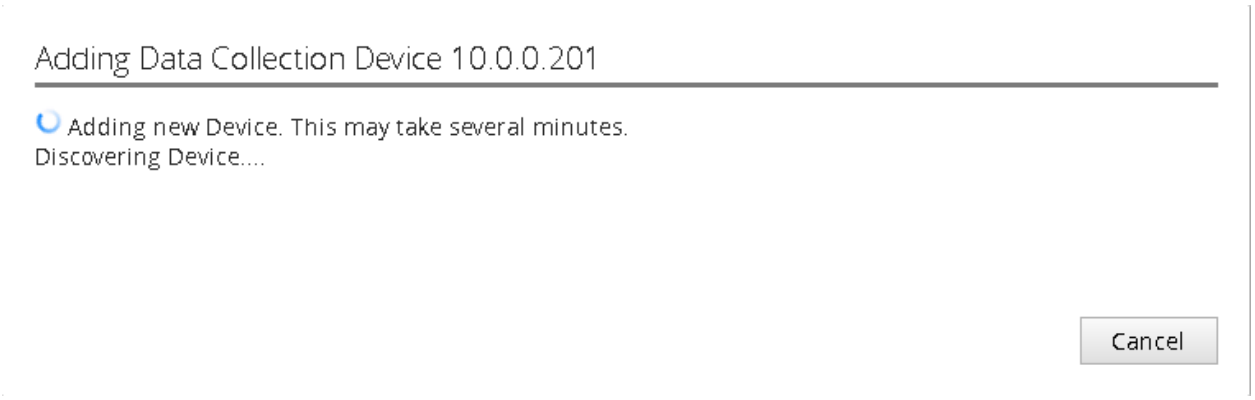
- Log in to the BIG-IQ Console Node (10.0.0.200 admin/401elliottW!)
- Under System→BIG-IQ DATA COLLECTION
- Select BIG-IQ Data Collection Devices
- Click the Add button



- Add the DCD Management IP Address (10.0.0.201), Username: admin, Password: 401elliottW! and the Data Collection IP Address (self-IP: 10.128.10.201). Data collection port default is 9300. Click the Add button in the lower right of the screen.



- Adding the DCD will take a minute or two:



- DCD item in UI displayed.
  - Status – State indicator. Green (UP) | Yellow (Unhealthy) | Red (Down)
  - Device name – Hostname of DCD (data collection device)
  - IP Address – IP Address of interface used for data collection.
  - Version – Software version of BIG-IQ DCD (data collection device)

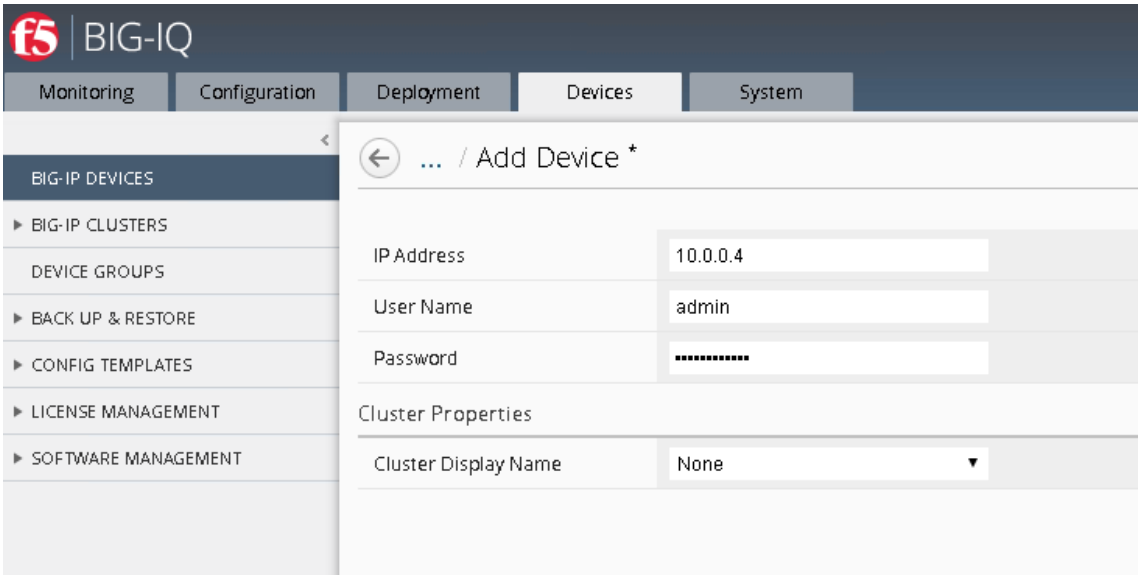
Add device to inventory after DCD has been added to see the user experience around statistics.

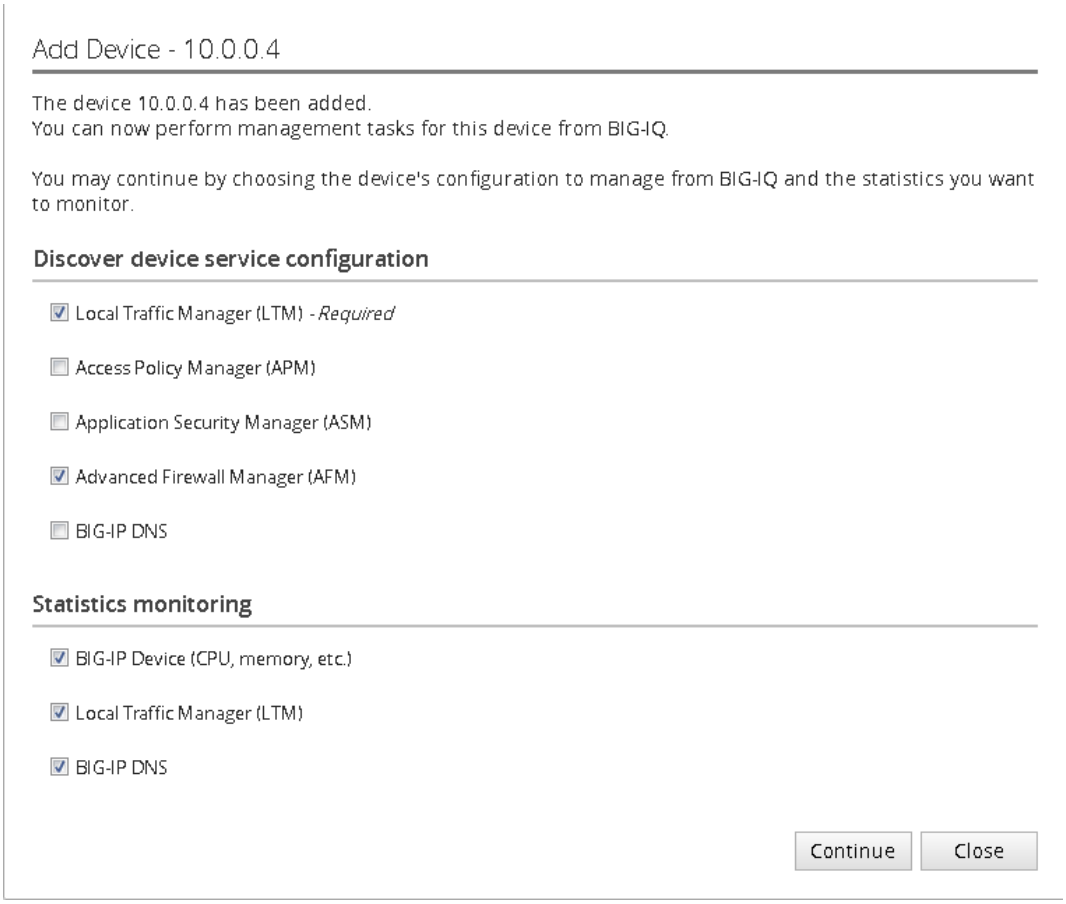
We will discover devices 10.0.0.4 using the UI and 10.0.0.5 using REST and enable statistic collection for these BIG-IP's.

Click Add to add a device to the BIG-IQ console.

- Log in to the BIG-IQ Console Node (10.0.0.200 admin/401elliottW!)
- Under Device→Add Device

-Complete the form for the device add using IP 10.0.0.4, username: admin, password: 401elliottW!

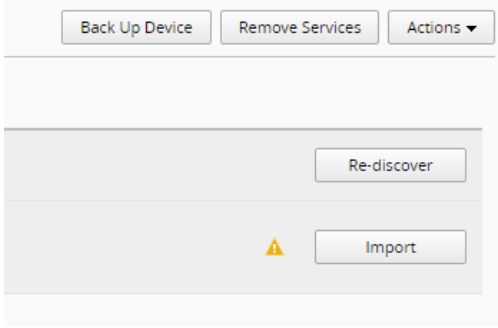




To discover 10.0.0.5, use the POSTMan collection labeled “Service Provider Specialist Event - Lab 4”. Please note you may have to manually import the ADC service due to a conflict. Conflict resolution is capable via the API however; outside of the scope of this lab. For additional details please reference the API documentation located here:

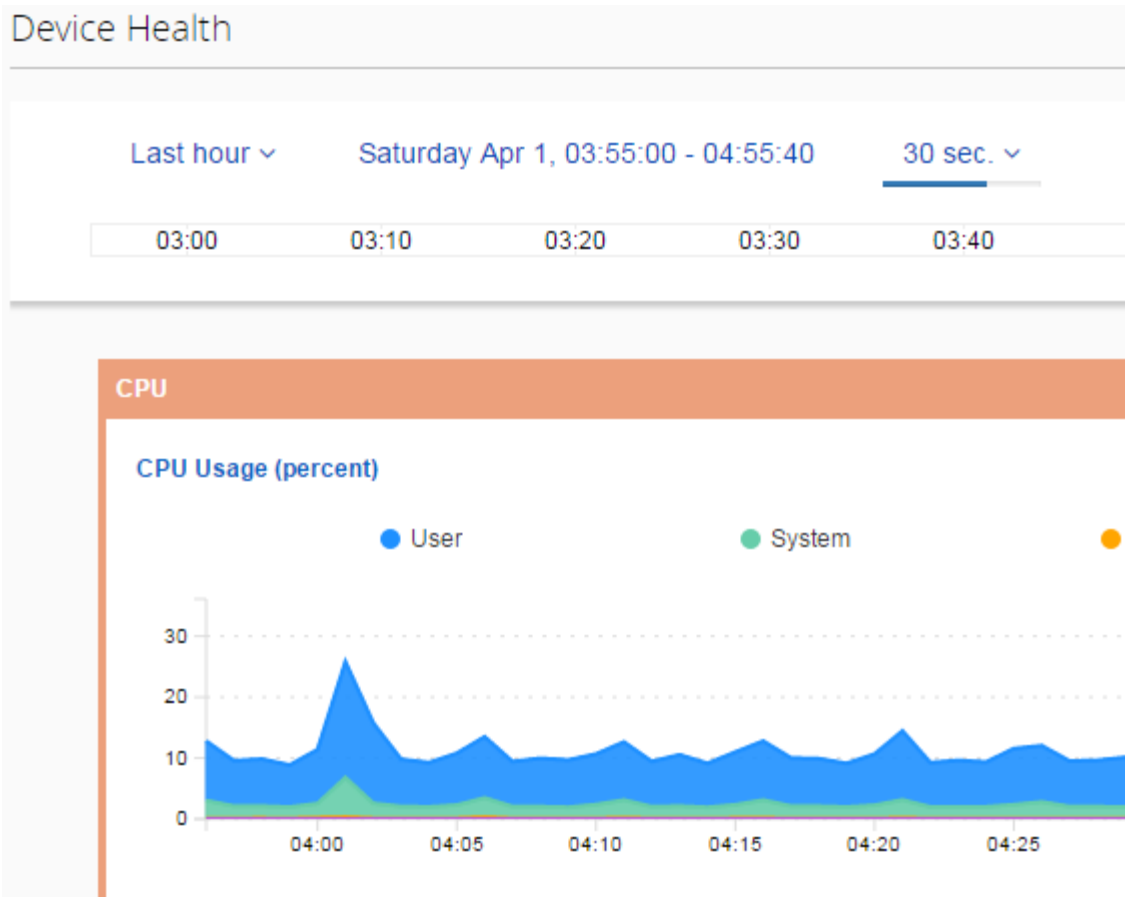
http://bigiq-cm-restapi-reference.readthedocs.io/en/latest/HowToGuides/Trust/Trust.html

- Complete the Import (current-configuration copy to working-configuration on BIG-IQ) for LTM and AFM for both BIG-IP’s. For any conflict resolution use BIG-IP as the source of truth



Navigate to the monitoring dashboards to validate that statistics are being collected and displayed for the BIG-IP devices.

- Navigate to Monitoring→Dashboards→ Device→ Health to verify that the graphs are populated.

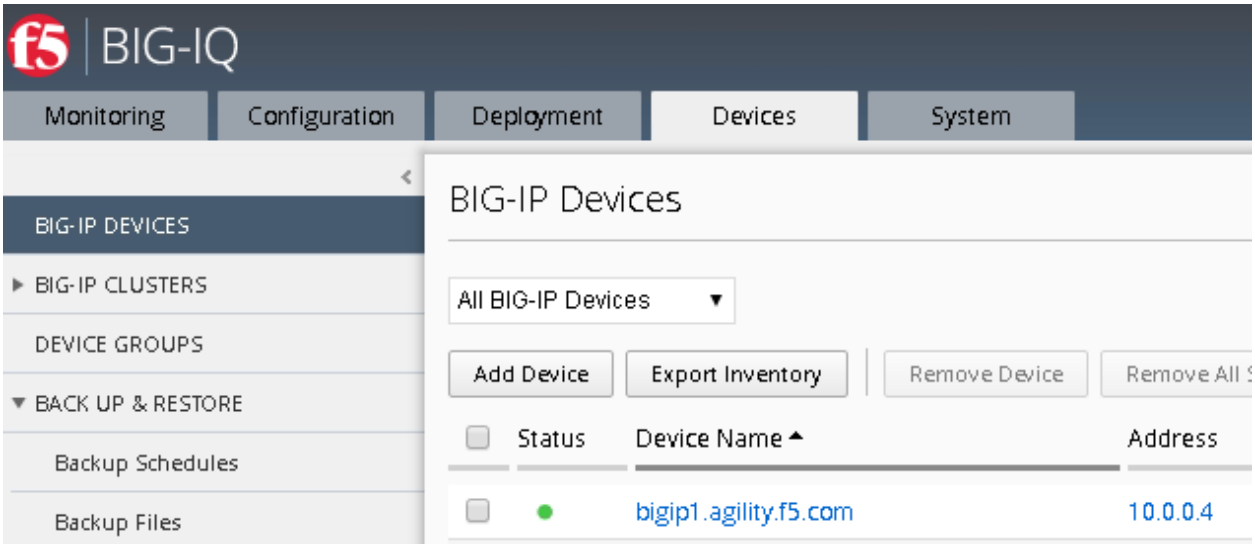


- If you don't see data, raise your hand to get some help.
- We are going to move on to other parts of the lab while we collect some stats and then we will circle back when we have more data to work with.

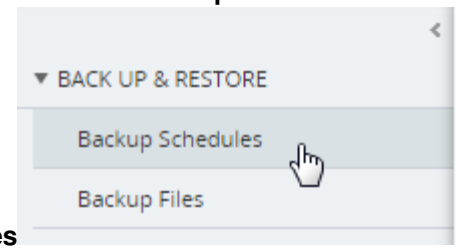
1.5.5 WORKFLOW 2: Creating a Backup Schedule

BIG-IQ is capable of centrally backing up and restoring all of the BIG-IP devices it manages. To create a simple backup schedule, follow the following steps.

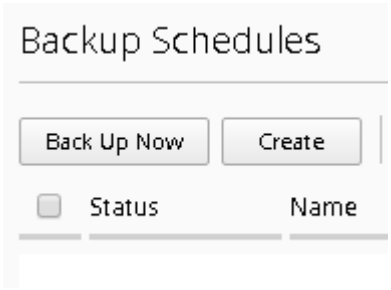
1. Click on the **Back Up & Restore** submenu in the Devices header.



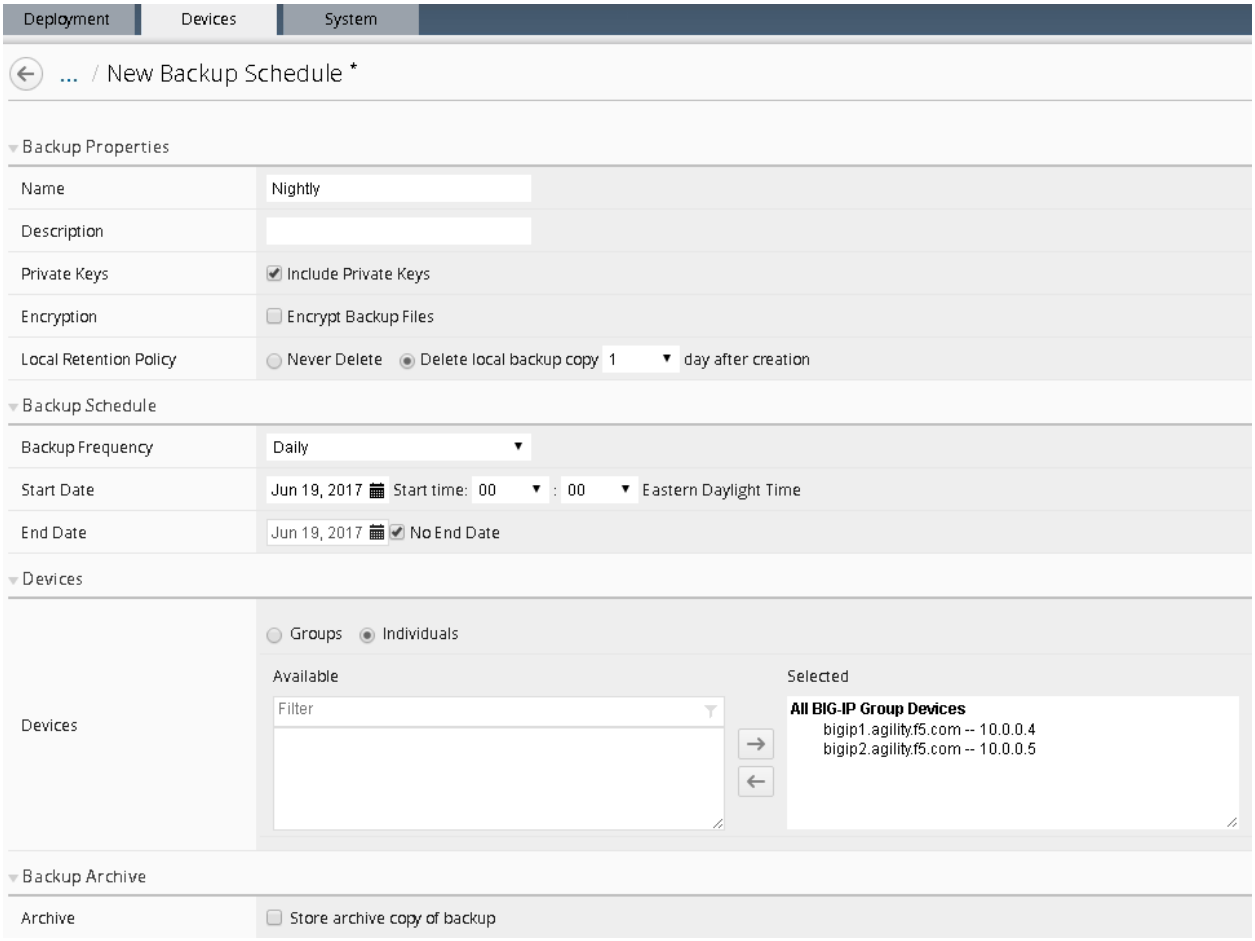
2. Expand the **Back Up and Restore** menu item found on the left and click on **Backup Schedules**



3. Click the **Create** button



4. Fill out the Backup Schedule using the following settings:
   - **Name:** Nightly
   - **Local Retention Policy:** Delete local backup copy 1 day after creation
   - **Backup Frequency:** Daily
   - **Start Time:** 00:00 Eastern Daylight Time
   - **Devices: Groups:** All BIG-IP Devices
   - Your screen should look similar to the one below.

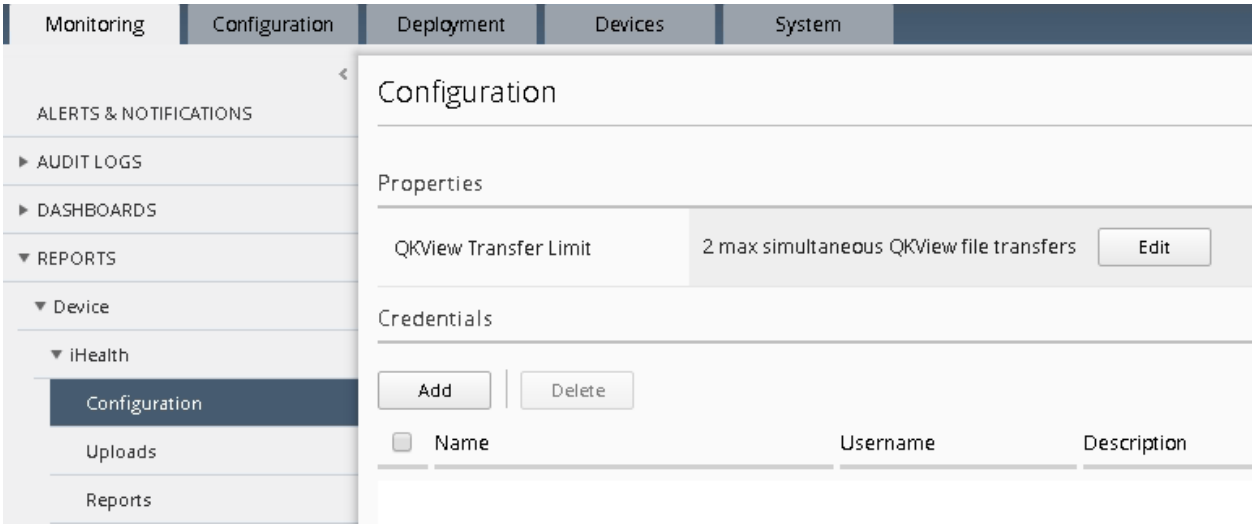


5. Click **Save** to save the scheduled backup job.
6. Optionally feel free to select the newly created schedule and select “Back Up Now” to immediately backup the devices.
   (a) When completed the backups will be listed under the Backup Files section

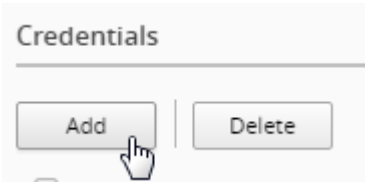
1.5.6 WORKFLOW 3: Uploading QKViews to iHealth for a support case

BIG-IQ can now push QKViews from managed devices to ihealth.f5.com and provide a link to the report of heuristic hits based on the QKView. These QKView uploads can be performed ad-hoc or as part of a F5 support case. If a support case is specified in the upload job, the QKView(s) will automatically be associated/linked to the support case. In addition to the link to the report, the QKView data is accessible at ihealth.f5.com to take advantage of other iHealth features like the upgrade advisor.

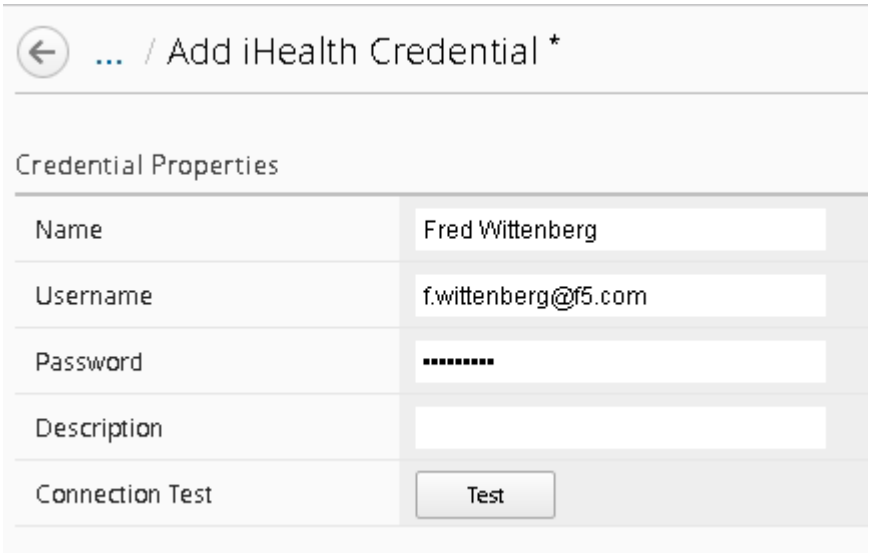
1. Navigate to **Monitoring** → **Reports** → **Device** → **iHealth** → **Configuration**



2. Add Credentials to be used for the QKView upload and report retrieval. Click the Add button under Credentials.

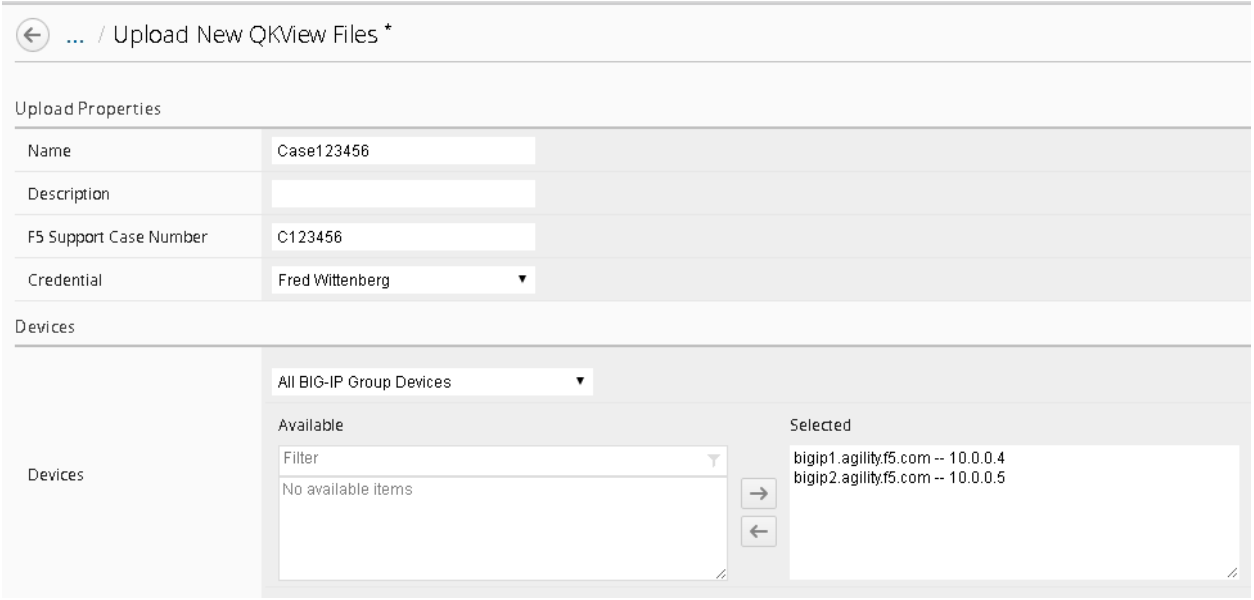


3. Fill in the credentials that you used to access https://ihealth.f5.com:
   - Name: Give the credentials a name to be referenced in BIG-IQ
   - Username: <Username you use to access iHealth.f5.com>
   - Password: <Password you use to access iHealth.f5.com>

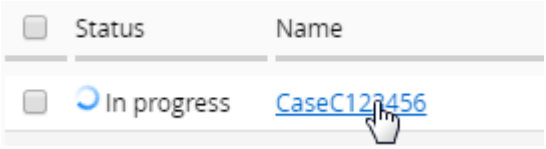


4. Click the Test button to validate that your credentials work.
5. Click the Save & Close button in the lower right.
6. Click the Uploads button in the BIG-IP iHealth menu.

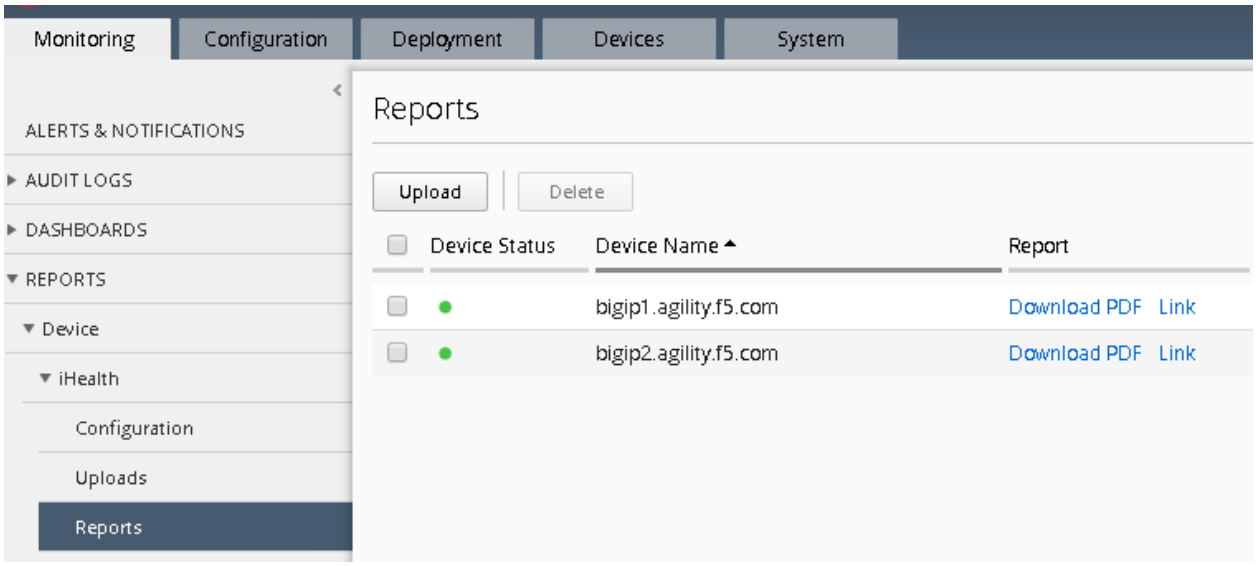
7. Click the Upload button to select which devices we need to upload QKViews from Case123456
8. Fill in the fields to upload the QKViews to iHealth.
    - Name: CaseC123456
    - F5 Support Case Number: C123456
    - Credentials: <Select the credentials you just stored in step 5>
    - Devices: Move all devices from Available to Selected



9. Click the Upload button in the lower right.
10. Click on the name of your upload job to get more details



11. Observe the progress of the QKView creation, retrieval, upload, processing, and reporting. This operation can take some time, so you may want to move on to the next exercise and come back.
12. Once a job reaches the Finished status, click on the Reports menu to review the report.
13. Click on the Download PDF link to view each of the reports.



14. Open a browser window/tab to https://ihealth.f5.com
15. Log in with the same credentials that you saved in step 5.
16. Observe the full QKViews that are available in iHealth for further use with items like the Upgrade Advisor.

1.5.7 BIG-IQ Global Search and Related to Search

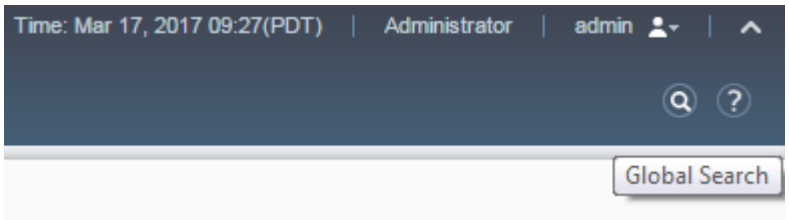
WORKFLOW 1: BIG-IQ Global Search and Related to Search (REQUIRED)

Objective

To introduce the user to BIG-IQ global search which will provide a product wide index to all configuration objects and supporting properties.

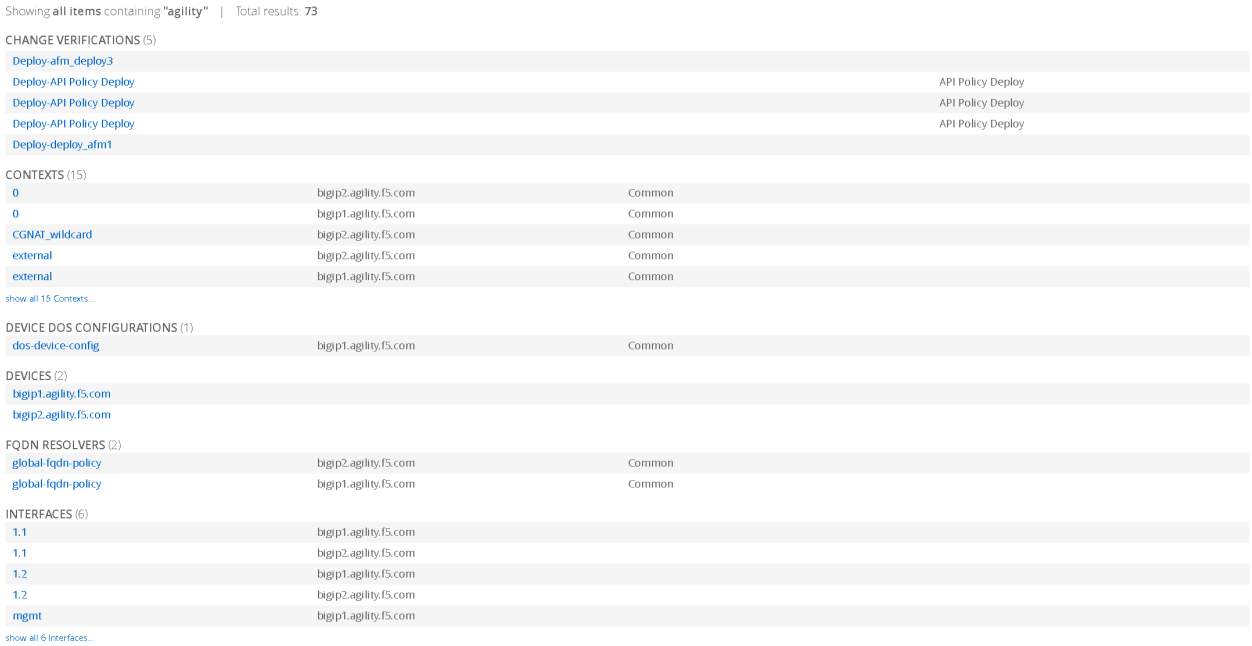
Global Search

- Select the Global Search Icon in the upper right corner of the top panel.

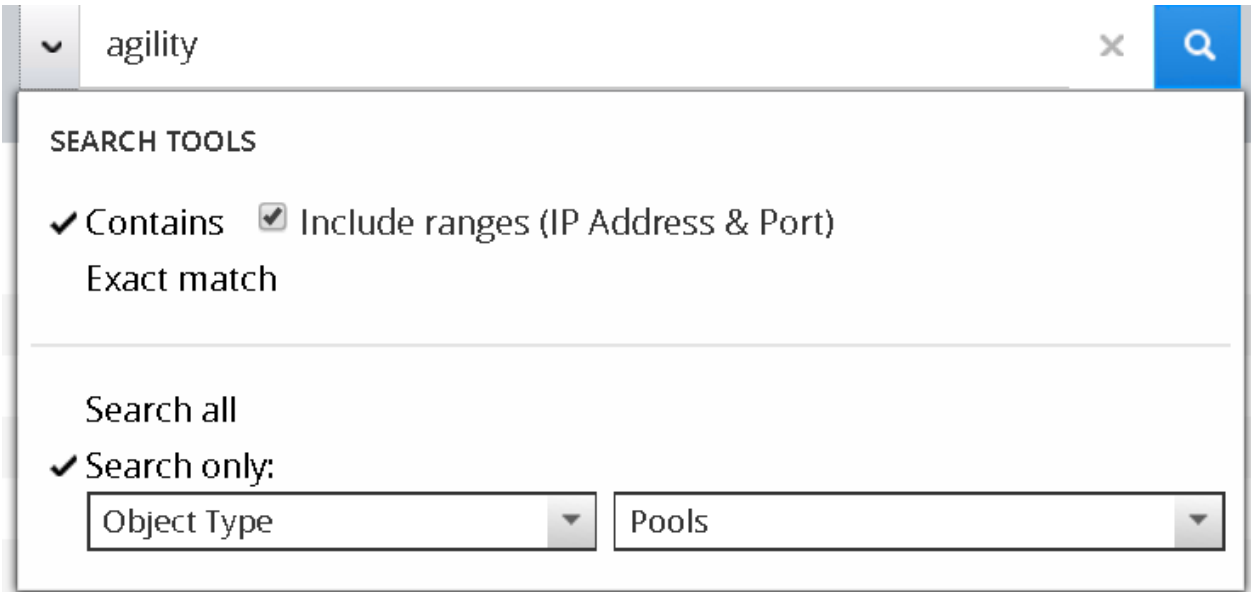


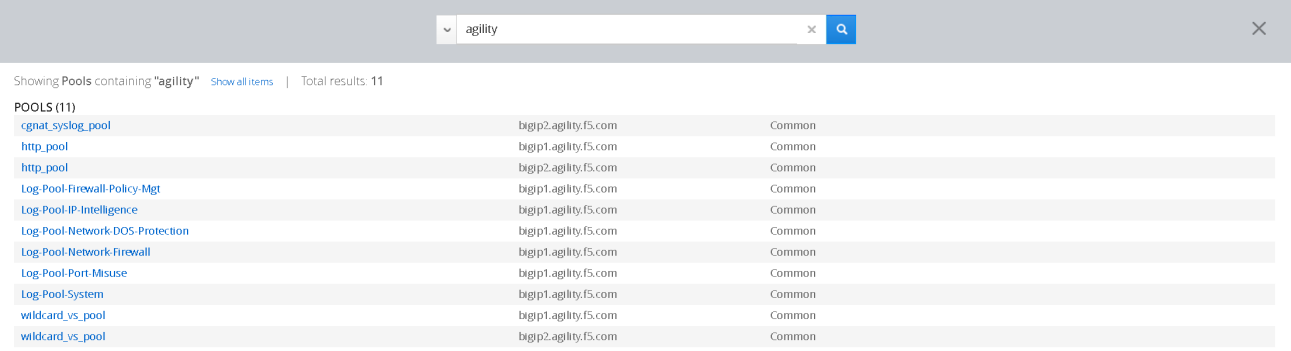
- Enter search terminology.

- Produces results.
- Select to the object to preview by drilling into editor page.

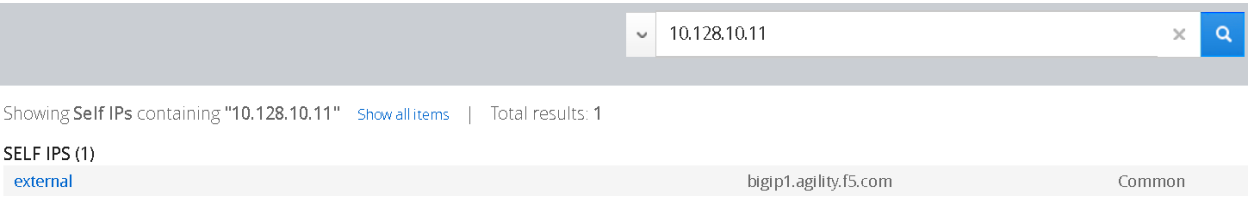


- Narrowing the search results
- Click the down arrow next to the search term and observe that you have various options to scope your search
- Update your search to only return pool members that match the search term and refresh your results





Note: This can be especially useful if you are running a traceroute and want to narrow down the results to the IP and/or hostname of the firewall in the traceroute. Try searching for the IP 10.128.10.11 with a filter of Object Type and SelfIP (hit you can start typing what you're looking for). Your results should look similar the following:



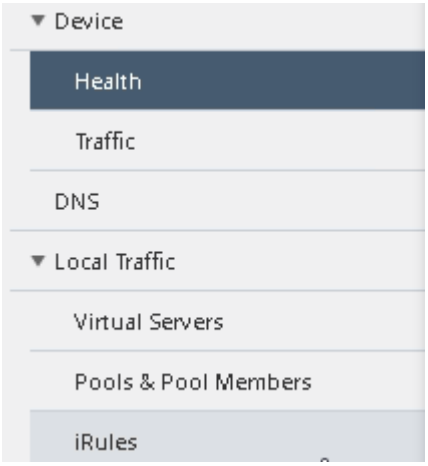
1.5.8 BIG-IQ Statistics Dashboards (Continued)

Note: Now that some time has passed, we should have more statistics to review and interact with.

WORKFLOW 1: Reviewing the data in the dashboards

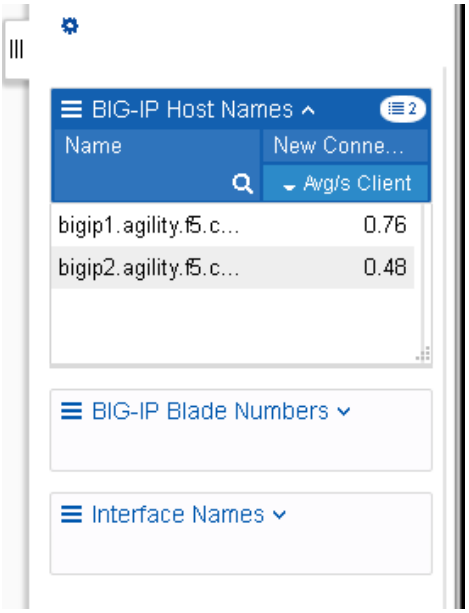
Navigate to Monitoring→Dashboards→Local Traffic

- Click through all the stats dashboards and see the metrics that are gathered

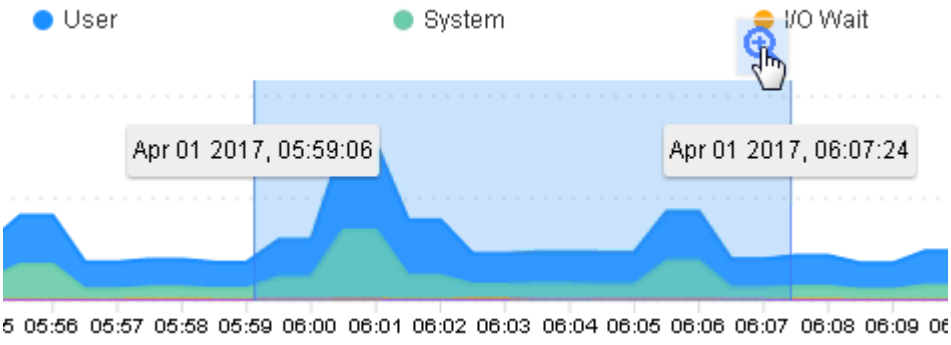


WORKFLOW 2: Interacting with the data in the dashboards

- You can narrow the scope of what is graphed by selecting an object or objects from the selection panels on the right. For example, if you only want to see data from BIG-IP01, you can click on it to filter the data.

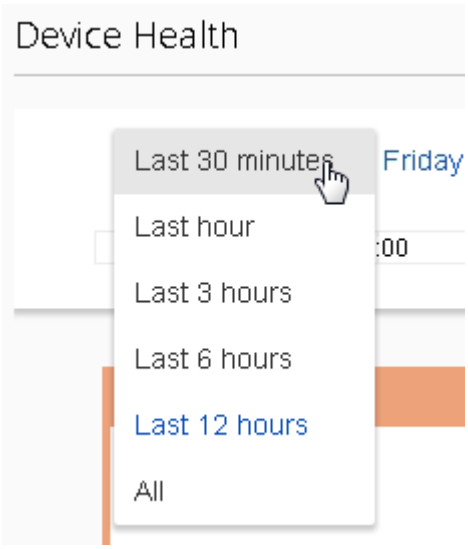


- You can create complex filters by making additional selections in other panels
- You can zoom in on a time, by selecting a section of a graph or moving the slider at the top of the page

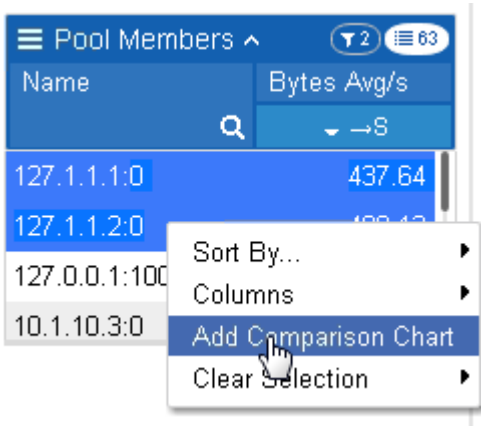


or

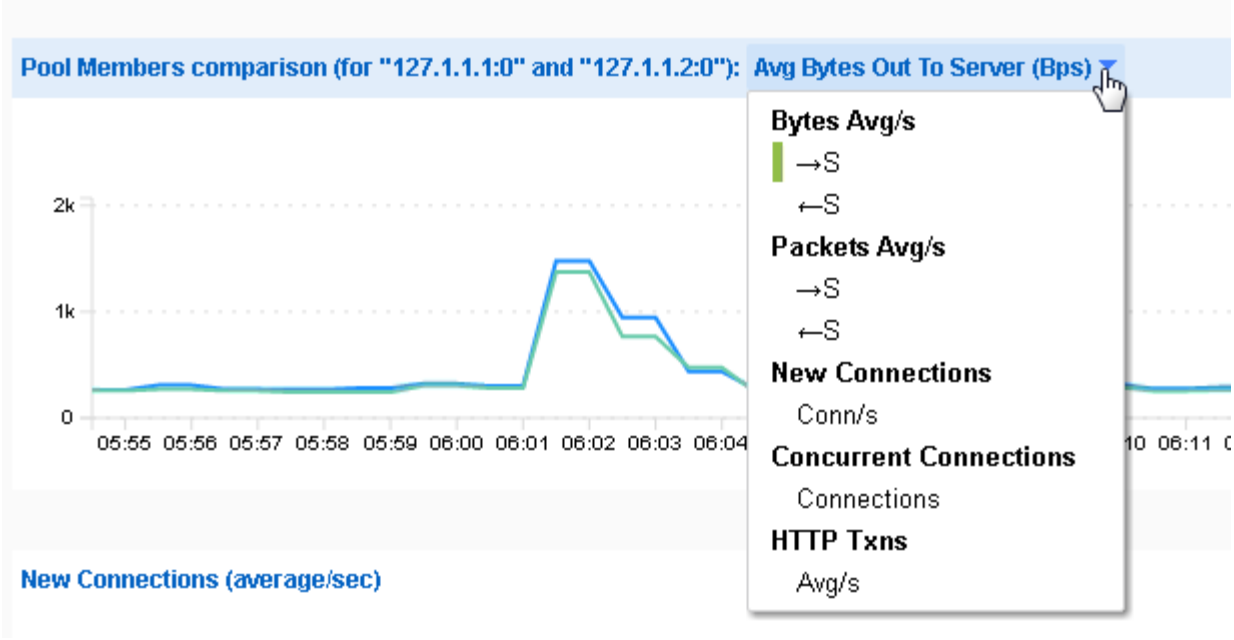
- All the graphs update to the selected time.
- You can change how far in the data you want to look back by using the selection in the upper left (note you may need to let some time elapse before this option becomes available)



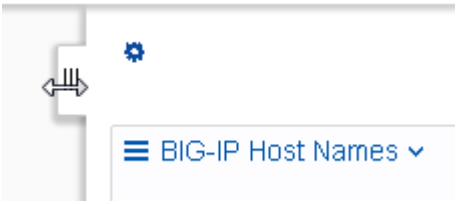
- Creating a comparison chart
- You can select multiple objects of the same type and create a comparison chart. Select the objects in the right-hand selector, right click, and select Add Comparison Chart

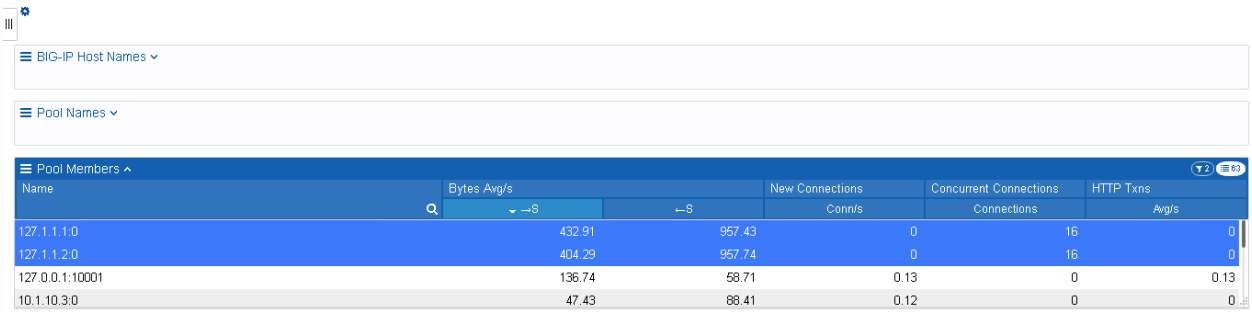


- The chart will appear at the top of the page. You can choose what metric you want to see in the chart

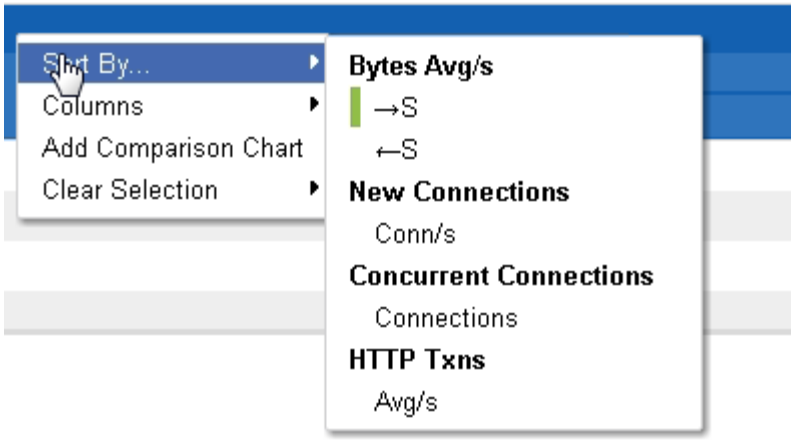


- Viewing the data in tabular form
- You can open the selector panel on the right to view and interact with the data in tabular form. Double click the tab at the top of the selector panel to open up the tabular view.



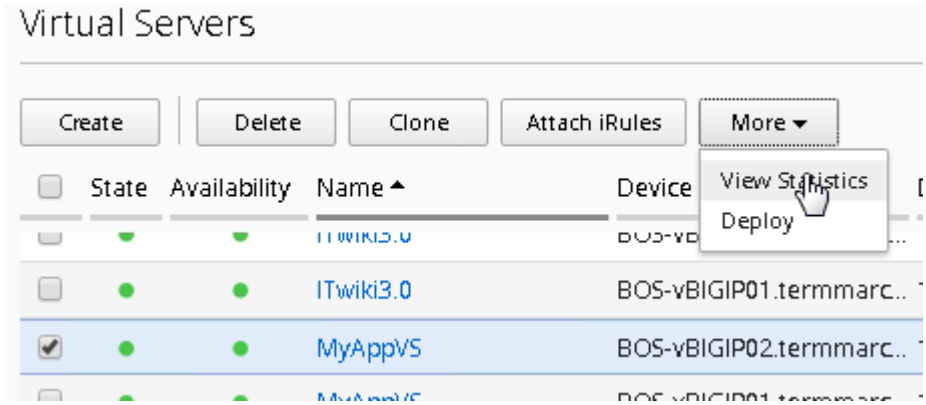


- Now you can view the averages, sort the columns, and add and remove columns from the view, by right clicking on the table



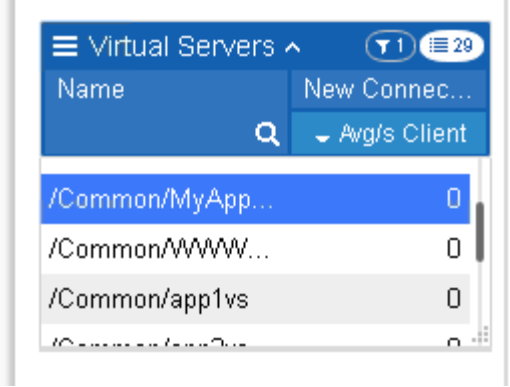
WORKFLOW 3: Getting to the statistics from the configuration/property pages for an object

- If you know that you only want to see stats for an object, you can launch the stats page from the configuration table or properties page.
- Navigate to Configuration→Local Traffic → Virtual Servers
- Select the object you want to see stats for, click the more button, and click view statistics



Or open the properties page of a virtual server and click the view statistics button in the upper right

- The launched stats page will be filtered to the object or objects you selected.



1.5.9 BIG-IQ REST API Documentation

References (DevCentral How-to and supporting references):

https://devcentral.f5.com/wiki/BIGIQ.HomePage.ashx

1.6 Module 5: Network Security (AFM) Management Workflows

1.6.1 Managing AFM from BIG-IQ

WORKFLOW 1: Managing AFM from BIG-IQ

In this lab, you will create all the components of a firewall policy. Port lists and address lists are the building blocks of firewall policies. They can be nested inside of each other to make address and port management easier, or policies can be created without using the lists at all. In this example, you'll use the lists to see how they work. Once created, you will deploy the configuration to two BIG-IP units.

Objective

- Create a simple firewall policy and dependent objects (address and port list)
- Deploy new firewall configuration to BIG-IP

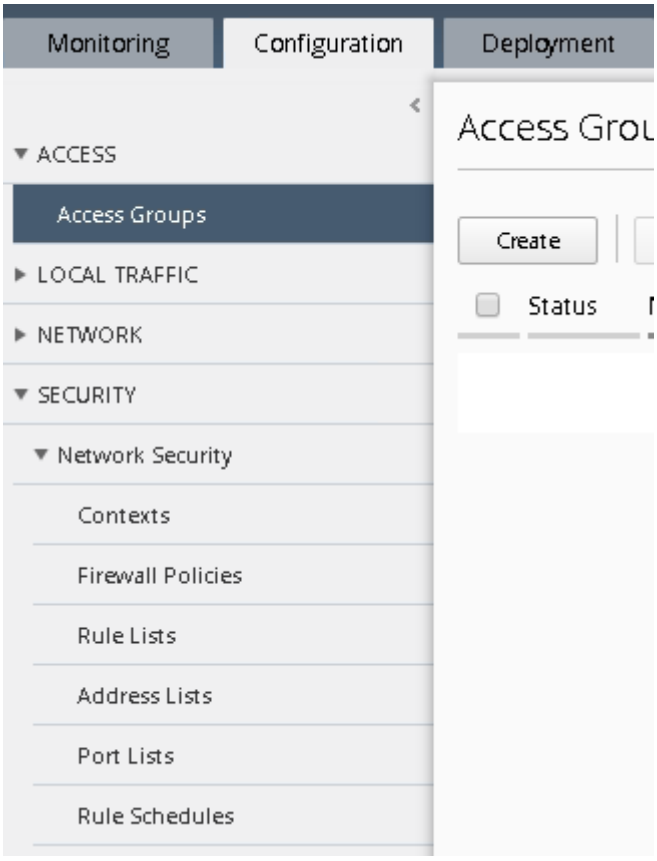
Lab Requirements

- Web UI access to BIG-IQ

Task 1 – Create Port List

On **BIGIQ1**: (*https://10.0.0.200)*

Navigate to the **Configuration** tab from the top menu of **BIG-IQ** then to **Security** → **Network Security**.



Click **Port Lists** from the left side navigation menu.

Click the **Create** button.

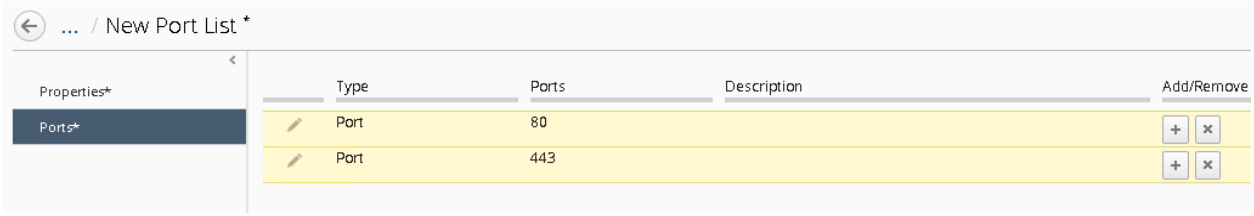
On the **Properties** tab, type in **HTTP_HTTPS** for **Name.**

Click the **Ports** tab.

Create the port list with the below information.

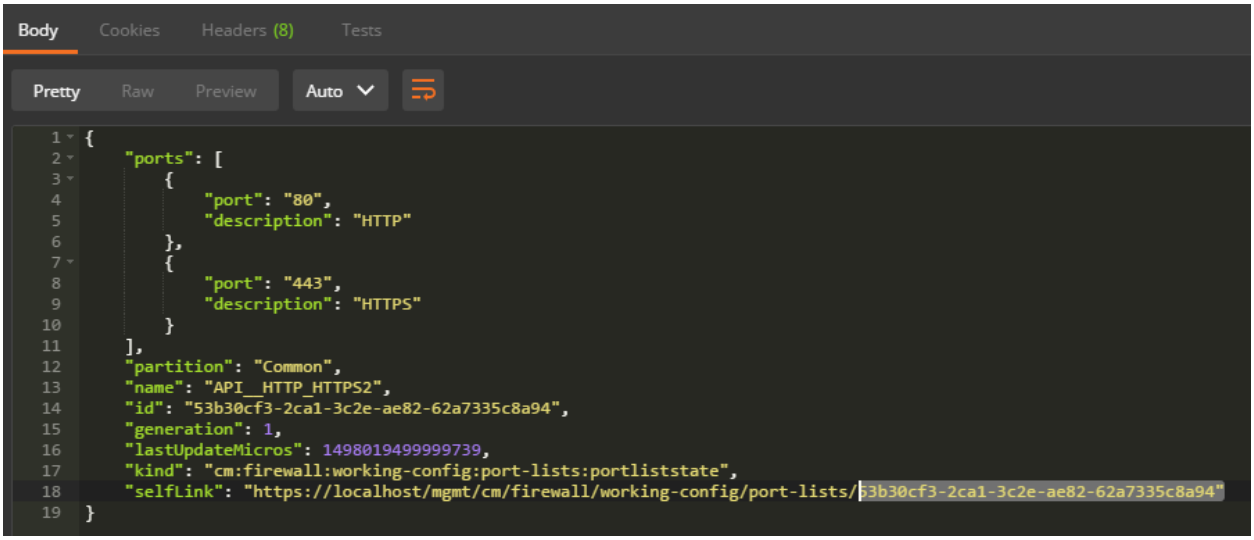
Type	Ports	Description
Port	80	HTTP
Port	443	HTTPS

Click on the **+** to add additional ports



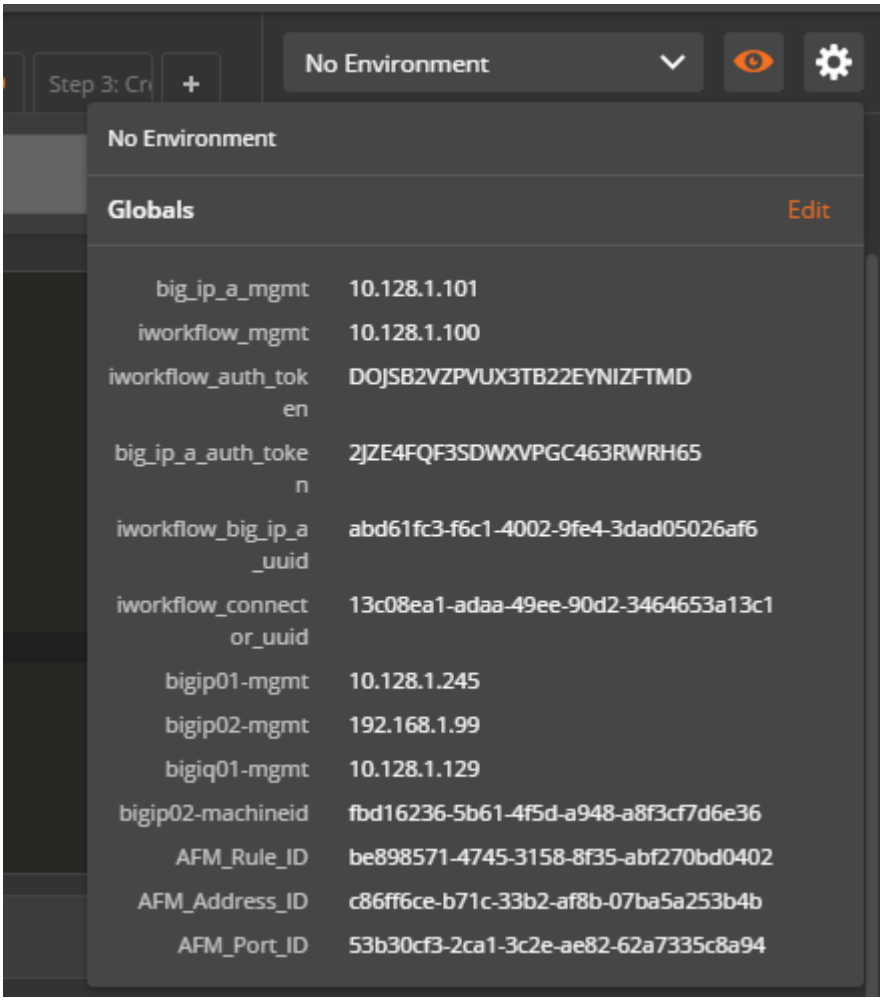
Click **Save & Close** when finished.

To create a port list via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 1 – Create New Port List. It is important to note the value returned within the self-link as shown below:



This value will be assigned to the environment variable AFM_Port_ID.

To modify the environment variables, click on the “eye” icon located in the top right section of POSTMan and select edit. The screen shot following shows an example of this screen:



Task 2 – Create Address List

Click on the **Address Lists** from the left navigation menu

Click the **Create** button

In Properties, type in **Trusted_Clients** for Name

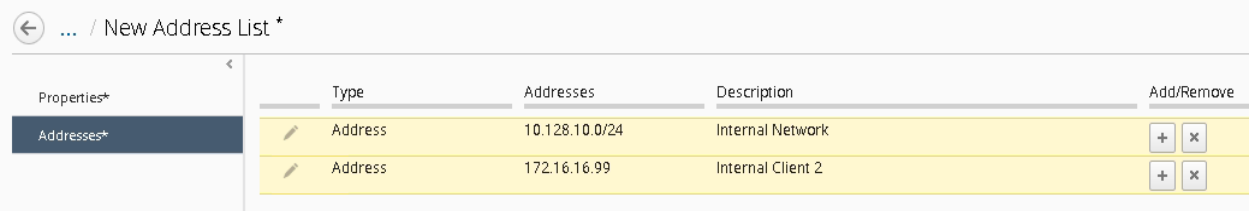
The ability to Pin address to a device is also new in 5.2. This feature allows objects to remain on a device even if they are orphaned and/or not currently in use in a policy on the “pinned” device.

Click the **Addresses** tab

Create a new address list with the below information

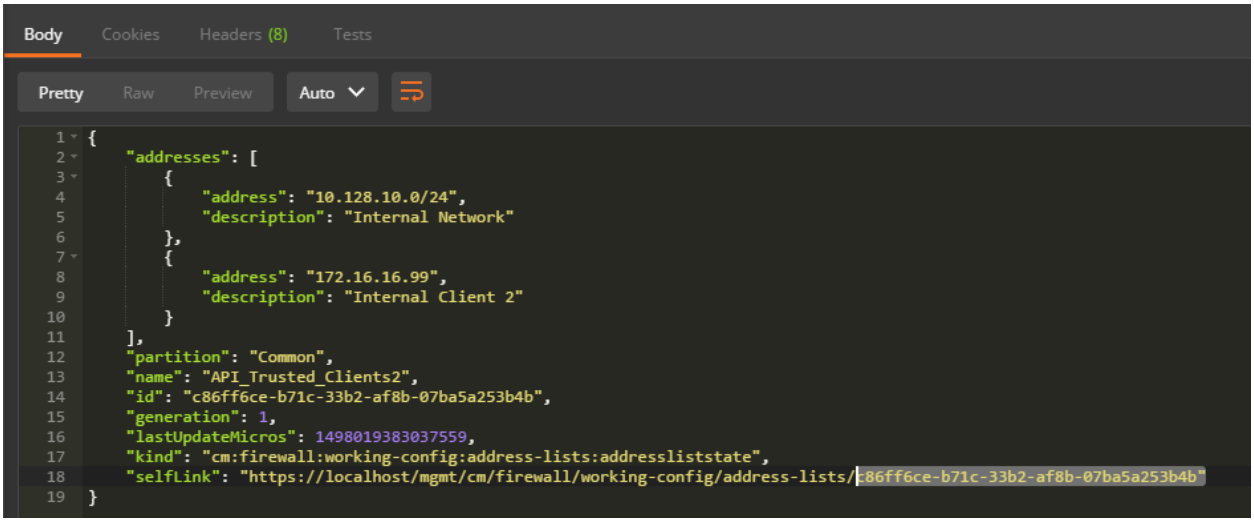
Type	Addresses	Description
Address	10.128.10.0/24	Internal Network
Address	172.16.16.99	Internal Client 2

Click on the **+** to add additional addresses



Click **Save and Close** when finished.

To create an address list via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 2 – Create New Address List. It is important to note the value returned within the self-link as shown below:



This value will be assigned to the environment variable AFM_Address_ID.

Task 3 – Create Rule List

Click on the **Rule Lists** from the left navigation menu.

Click the **Create** button.

On the Properties tab, type in **Rule_List_Allow_Trusted** for Name.

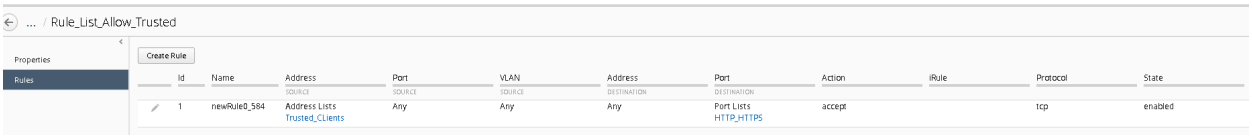
Click the **Rules** tab.

Click **Create Rule** button.

Click on the pencil (edit rule) of the newly created rule listed with **Id** of **1.**

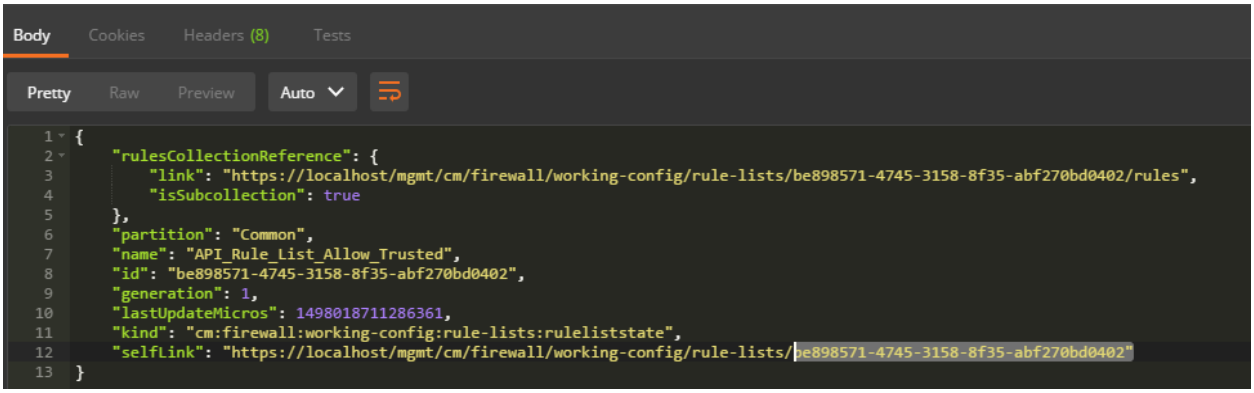
Create a new rule with the below information.

Name		Rule_Allow_Trusted
**Source Address **	**Address List**	Trusted_Clients
Source Port	**Port **	Any
Source VLAN		Any
Destination Address	**Address**	Any
Destination Port	**Port List**	HTTP_HTTPS
Action	**Accept**	Accept
Protocol	**TCP**	TCP
State		enabled
Log		checked



Click **Save & Close** when finished.

To create a rule list via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 3 – Create New Rule. It is important to note the value returned within the self-link as shown below:



This value will be assigned to the environment variable AFM_Rule_ID.

To create a rule within the rule list via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 4 – Create New Rule List.

Task 4 – Create Firewall Policy

Click on **Firewall Policies** from the left navigation menu.

Click the **Create** button.

On the Properties tab, type in **Policy_Forward** for Name.

On Pin Policy to Device(s), move bigip1.agility.f5.com to Selected.

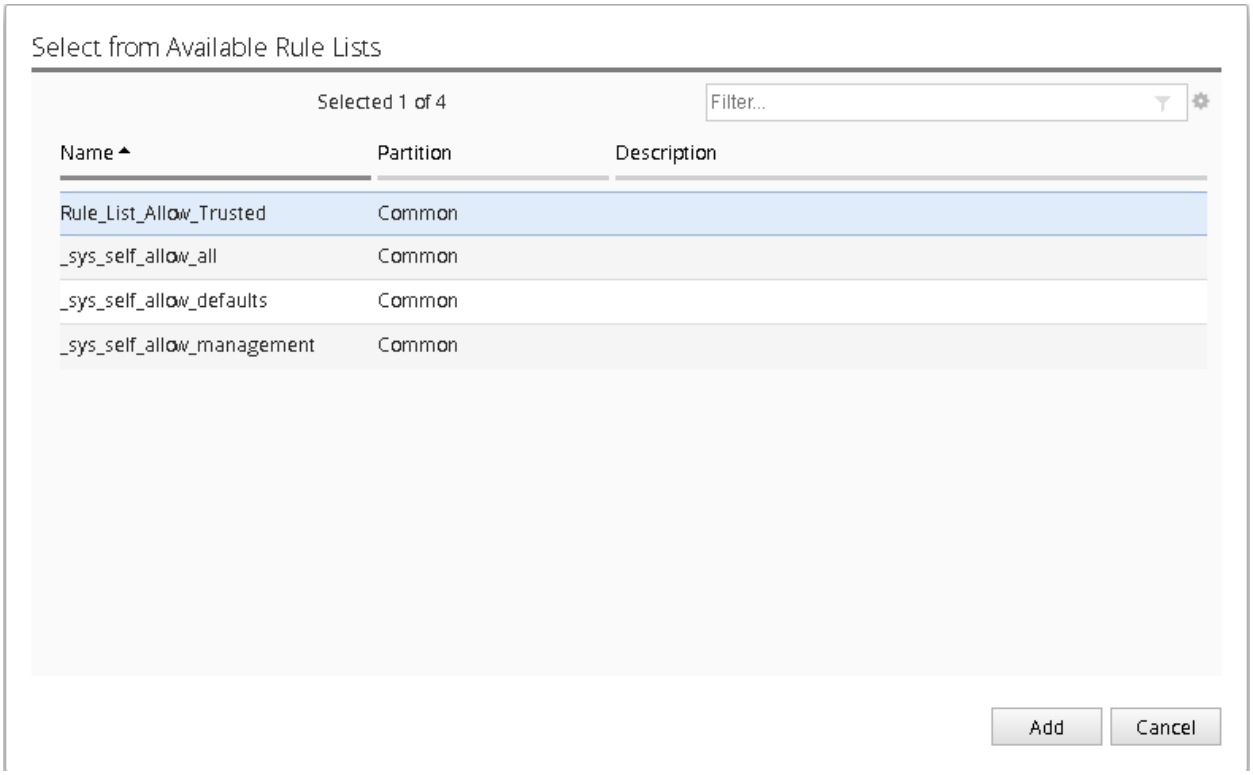
Click the Rules tab.

Click the **Add Rule List** button.

Select the checkbox for **Rule_Allowed_Trusted.**

Click **Add** button.

You will see the new policy listed as shown below.



Click on drop down arrow to verify our rule within the rule list is there.

Click **Create Rule** button

Click on the pencil (edit rule) of the newly created rule listed with **Id** of **2.**

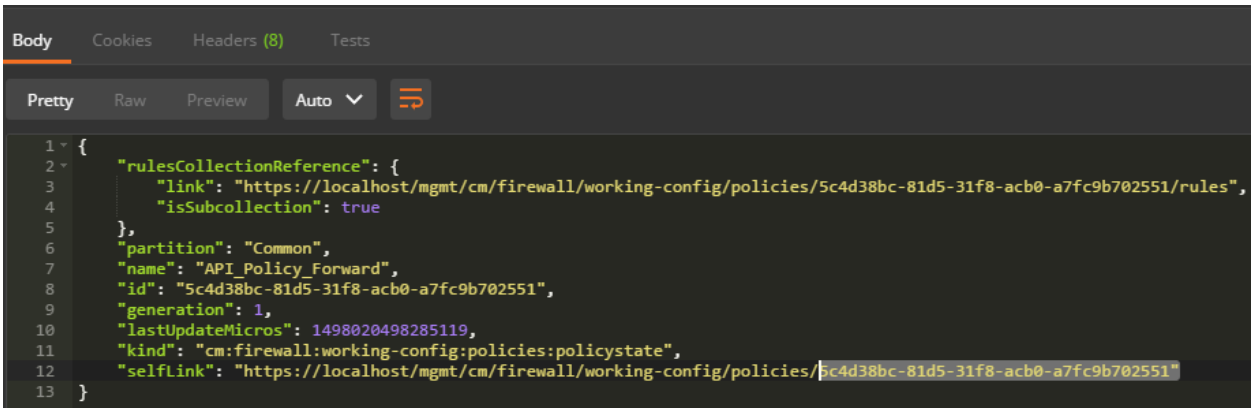
Create a new rule with the below information.

Name		Rule_Drop_Everything_Else
**Source Address **	**Address**	Any
Source Port	**Port **	Any
Source VLAN		Any
Destination Address	**Address List**	Any
Destination Port	**Port List**	Any
Action		*drop*
Protocol		*any*
State		*enabled*
Log		*checked*

Click the **Save and Close** button at the top.

You should see the policy with the new rule as shown below.

To create a policy via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 5 – Create New Policy. It is important to note the value returned within the self-link as shown below:



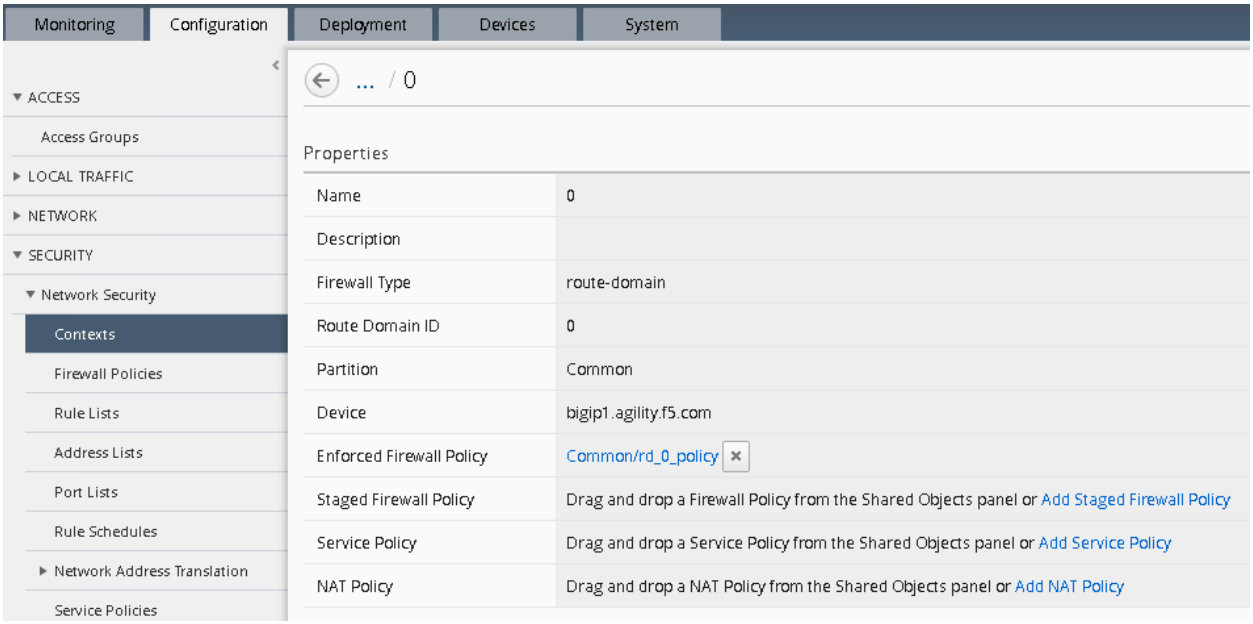
This value will be assigned to the environment variable AFM_Policy_ID.

To reference a rule within the policy via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 6 – Create New Rule Reference.

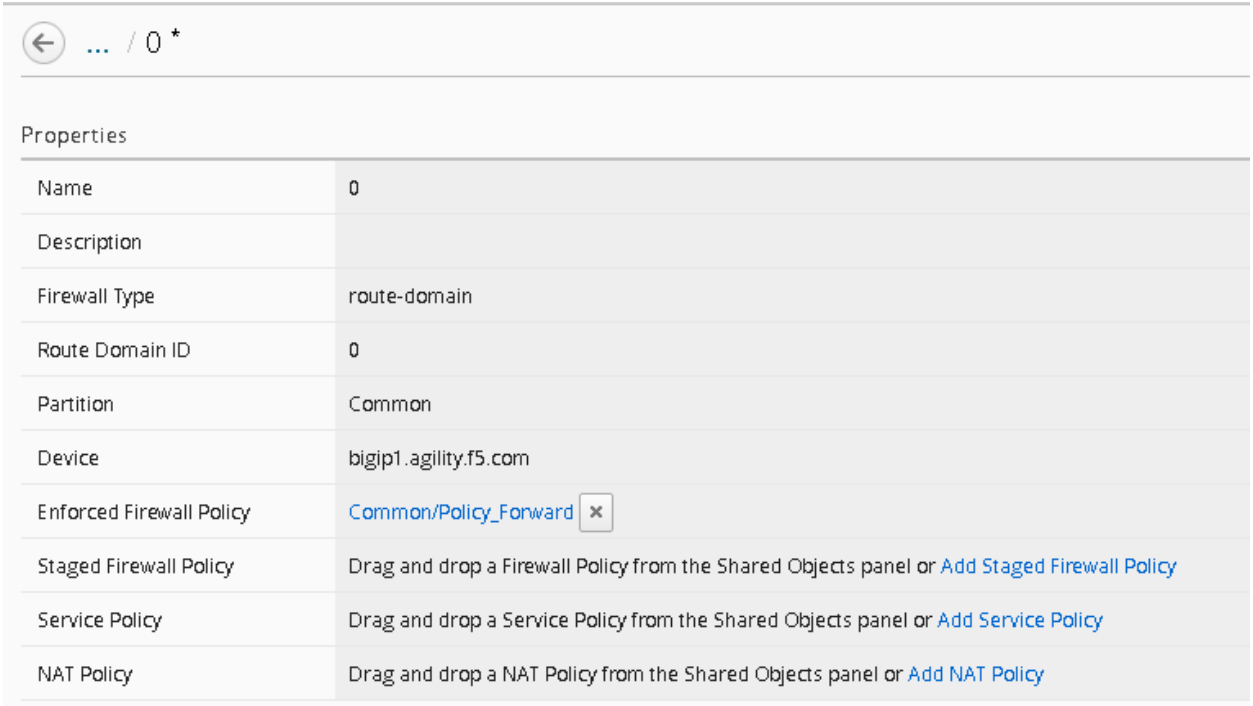
To create a drop rule within the policy via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 7 – Create Drop Rule in Policy. *Task 5 – Assign the Firewall Policy to a Context.*

In this task, you will take the policy you created above and apply it to a route domain on a BIG-IP. Typically, the route domain you apply firewall policies to has a wildcard virtual server that you forward all traffic through (as opposed to a standard single port virtual server that only allows specific traffic). This type of configuration is like the more classic firewall deployment.

In the left navigation menu, click **contexts**, then chose 0 for device bigip1.agility.f5.com



From the **Shared Objects** panel at the bottom of the screen, *grab* the **Policy_Forward** and *drag* it to the **Enforced Firewall Policy** shaded area. The policy should then appear in the **Enforced Firewall Policy** section. Alternatively, delete the existing policy (Common/rd_0_policy) by clicking the x, then select **Add Enforce Firewall Policy** and select **Policy_Forward** and click **Add.**



Click the **Save & Close** button.

At this point, the policy is assigned to the route domain in the BIG-IQ configuration, but the configuration has **not** been deployed/pushed to the BIG-IP units yet.

To assign a policy via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 8: Get bigip02 Contexts. This call will list all the firewall contexts using a filter for just route-

domains. You will need to copy the “id” assigned to bigip02 route-domain as exampled by the following:


```
        "partition": "Common",
        "deviceReference": {
            "id": "2ac67010-2d1e-44f1-9f72-fd8b21117339",
            "name": "bigip2.agility.f5.com",
            "kind": "shared:resolver:device-groups:restdeviceresolverdevicestate",
            "machineId": "2ac67010-2d1e-44f1-9f72-fd8b21117339",
            "link": "https://localhost/mgmt/shared/resolver/device-groups/cm-firewall-allFirewallDevices/devices/2ac67010-2d1e-44f1-9f72-fd8b21117339"
        },
        "name": "0",
        "id": "a739fb41-c928-3b2c-b3e1-88bf31b4cba5",
        "generation": 1,
        "lastUpdateMicros": 1499425468272853,
        "kind": "cm:firewall:working-config:firewalls:firewallstate",
        "selfLink": "https://localhost/mgmt/cm/firewall/working-config/firewalls/a739fb41-c928-3b2c-b3e1-88bf31b4cba5"
    }
],
```


This value will be assigned to the environment variable bigip02-rd0id.

To assign the policy to RD0 via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 9: Apply Policy to RD0.

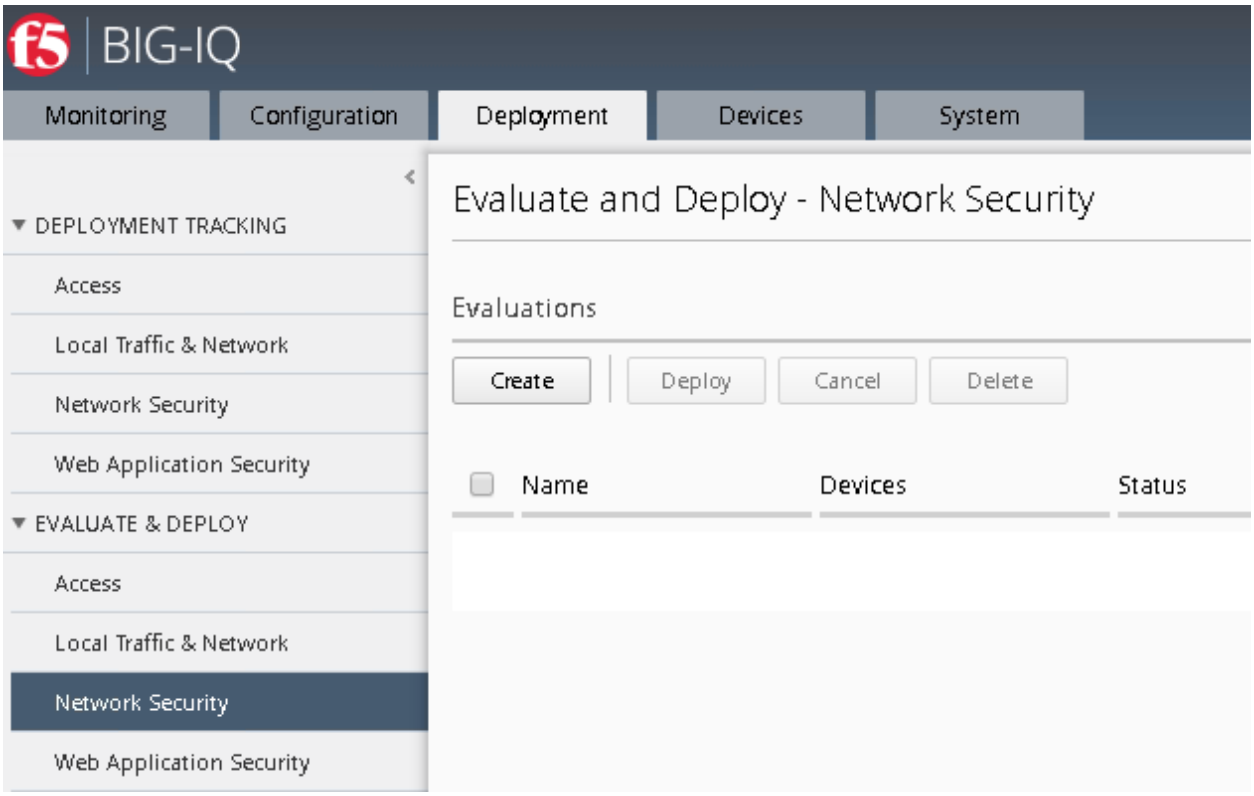
Task 6 – Deploy the Firewall Policy and related configuration objects

Now that the desired firewall configuration has been created on the BIG-IQ, you need to deploy it to the BIG-IP. In this task, you create the deployment, verify it, and deploy it.

From the top navigation bar, click on **Deployments**.

Click on the **EVALUATE & DEPLOY** section on the left to expand it.

Click on **Network Security** in the expansion.



Click on the top Create button under Evaluations

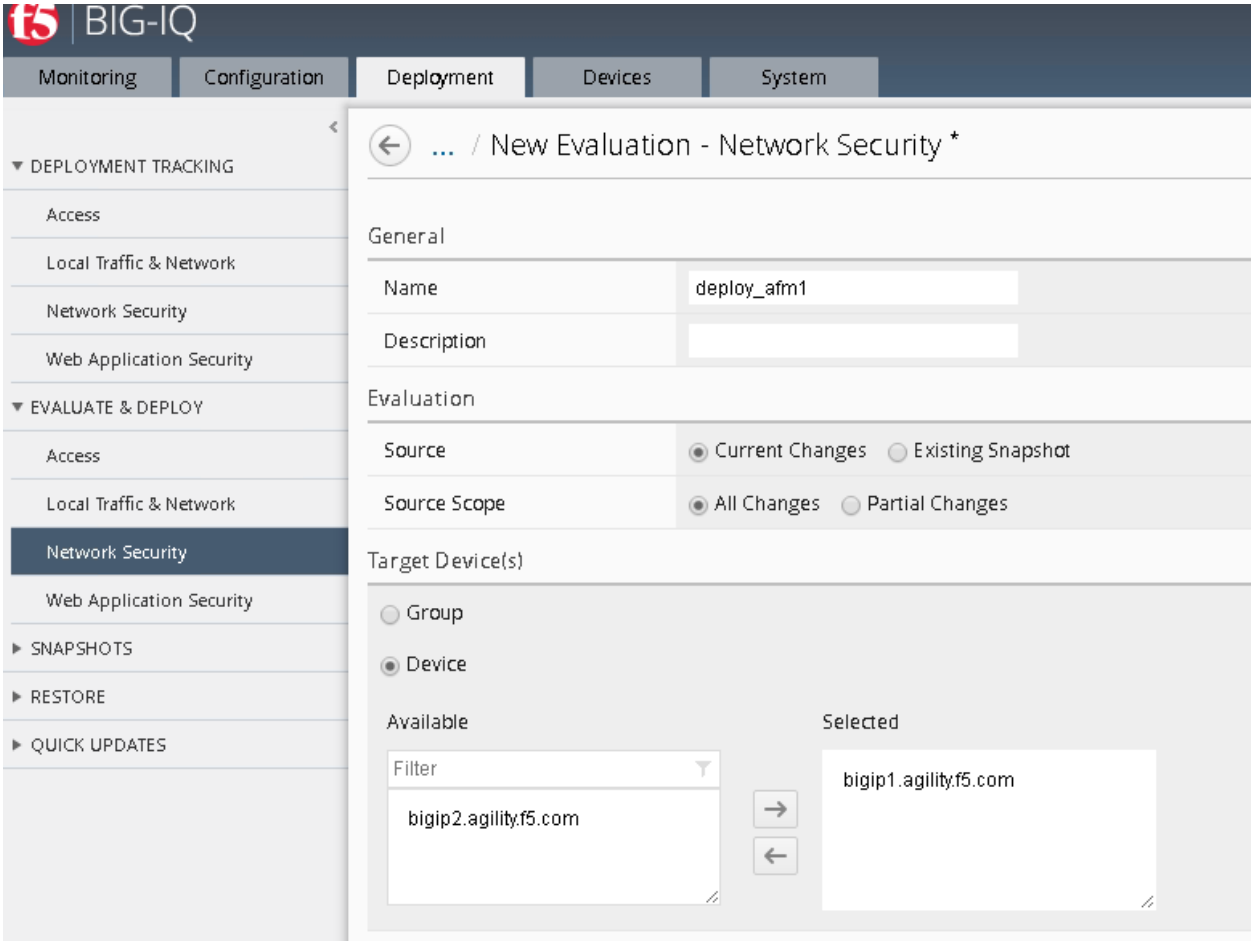
Give your evaluation a name (ex: **deploy_afm1**).

Evaluation **Source** should be **Current Changes** (default).

Source Scope should be **All Changes** (default)

Target Device(s) should be **Device**.

Select bigip1.agility.f5.com from the list of Available devices and move it to Selected.



Click the **Create** button at the bottom right of the page.

You should be redirected to the main **Evaluate and Deploy** page.

- This will start the evaluation process in which BIG-IQ compares its working configuration to the configuration active on each BIG-IP. This can take a few moments to complete.

The **Status** section should be dynamically updating. . . (What states do you see?)

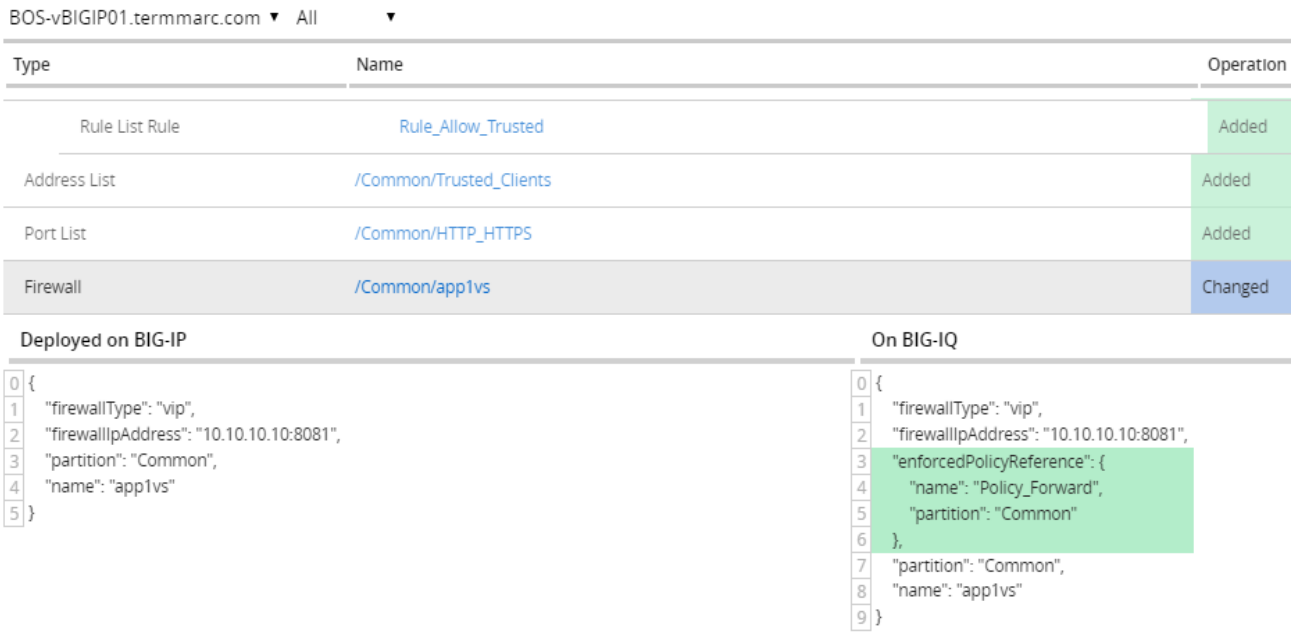
Once the status shows **Evaluation Complete** you can view the evaluation results.

- Before selecting to deploy, feel free to select the differences indicated to see the proposed deployment changes. This is your check before making changes on a BIG-IP.

Click the number listed under **Differences – Firewall**.

Scroll through the list of changes to be deployed.

Click on a few to review in more detail.



What differences do you see from the **Deployed on BIG-IP** section and on **BIG-IQ**?

Click **Cancel**.

Deploy your changes by checking the box next to your evaluation **deploy_afm1**.

With the box checked, click the **Deploy** button.

Your evaluation should move to the **Deployments** section.

After deploying, the status should change to **Deployment Complete**.

- This will take a moment to complete. Once completed, log in to the BIG-IP and verify that the changes have been deployed to the AFM configuration.

To deploy the changes via the API, follow the POSTMan Collection “Service Provider Specialist Event - Lab 5”, using Step 10: Deploy Policy to bigip02. This call will deploy only the changes made to bigip02

Congratulations, you just deployed your first AFM policy via BIG-IQ!

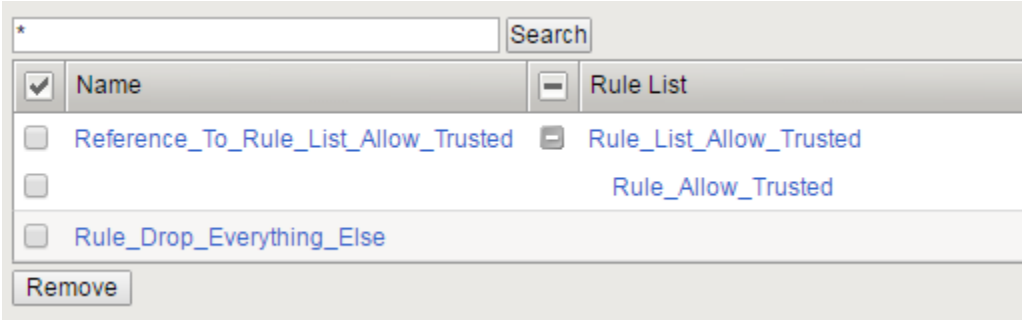
Review the configuration deployed to the BIG-IP units.

On **BIGIP1**: (*https://10.0.04)*

Navigate to Security > Network Firewall > Policies.

Click on Policy_Forward.

Are the two rules you created in BIG-IQ listed for this newly deployed firewall policy?



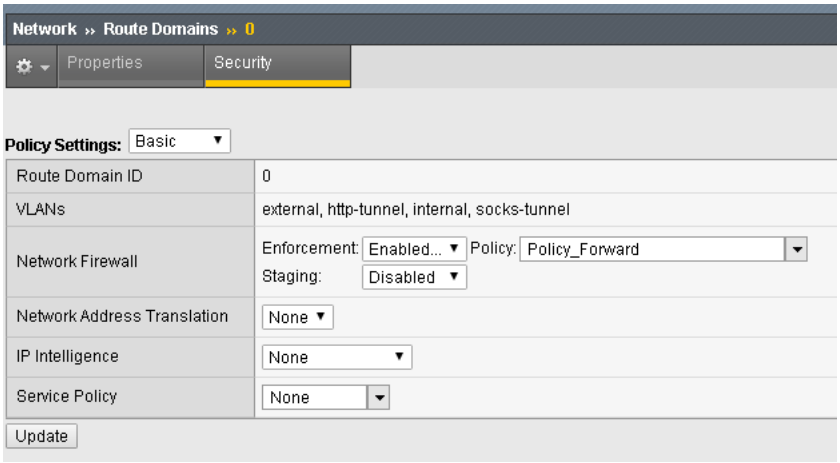
Navigate to Network > Route Domains

Click on route domain 0.

Click on the **Security** tab, click on **Policies** in the drop down.

What policy is deployed to this route domain?

Are the correct firewall rules applied to this route domain from the policy you associated to it?



Test Access to the Wildcard Virtual Server

- Open a new Web browser and access *http://10.128.10.223:8081* (this is expected to fail as are some others)
- Edit the URL to *https://10.128.10.223*
- Edit the URL to *http://10.128.10.223*
- Open either Chrome or Firefox and access *ftp://10.128.10.223*
- Open Putty and access 10.128.10.223
- Close all Web browsers and Putty sessions.

1.6.2 Service Policies and Timer Policies from BIG-IQ

WORKFLOW 2: Service Policies and Timer Policies from BIG-IQ

In this lab, you'll be creating a timer policy in a service policy and associating the service policy to a firewall rule. This allows you to control the idle connection time before a connection is removed from the state table. This control within AFM is a new feature in BIG-IP version 12.0+

Objective:

- Create a Timer Policy
- Create a Service Policy
- Associate Service Policy to a firewall rule
- Deploy to both BIG-IP units

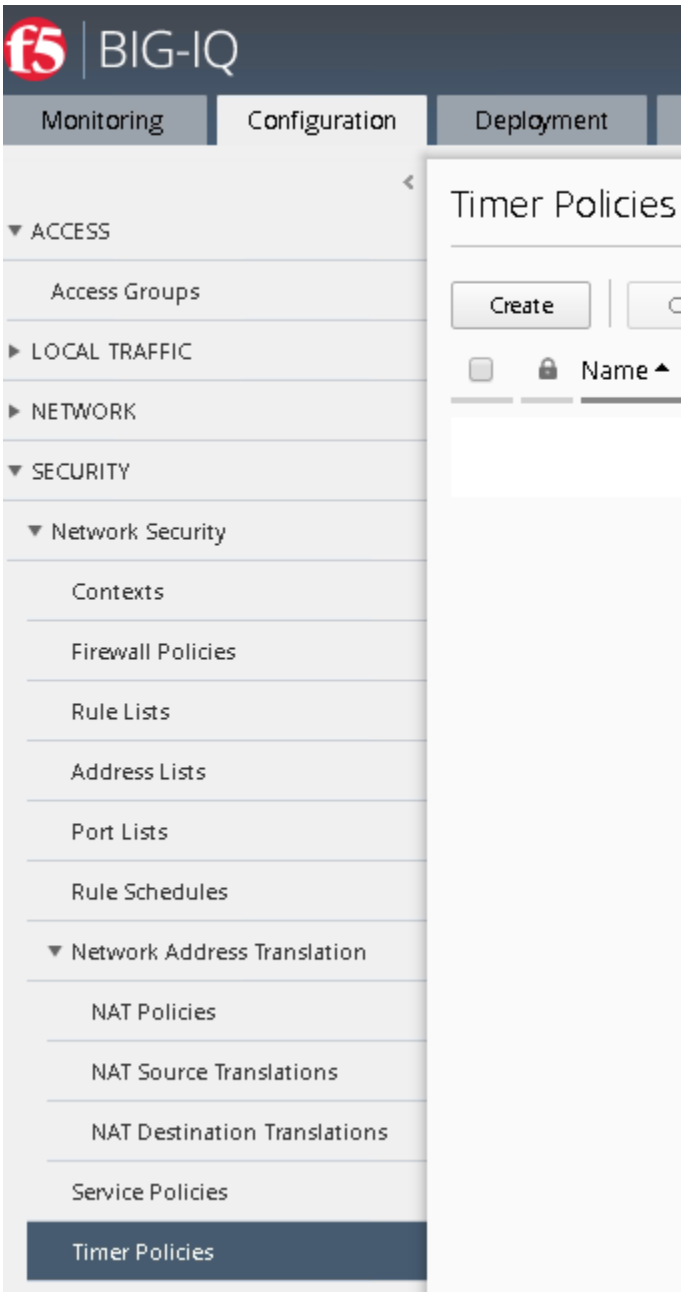
Lab Requirements:

- Web UI access to BIG-IQ

Task 1 – Create a Timer Policy

On **BIGIQ1**: (*https://10.0.0.200)*

Navigate to Configuration→ Security → Network Security → Timer Policies.



In the left navigation, click on **Timer Policies**.

Click **Create**.

In **Name** field, type *timer_tcp_60_min*.

Click **Rules** tab.

Click **Create Rule** button.

Click the pencil next to the new rule to modify it.

Create the new rule with the below information.

Name	**timer_rule_tcp_60_min**	
**Protocol **	**tcp**	
Destination Ports	**Port Range**	**1 – 65535**
Idle Timeouts	**Specify. . .**	**3600**
Description	**Allow TCP connections to idle for 60 minutes**	

Click the **Save and Close** button at the bottom.

Task 2 – Create a Service Policy

In the left navigation, click on **Service Policies**.

Click **Create** button.

In the **Name** field, fill in **policy_timer**.

On the Timer Policy drop down, select /**commom**/**timer_tcp_60_min**.

On Pin Policy to Device(s), move **bigip1.agility.f5.com**.

Click the **Save and Close** button at the bottom right.

Task 3 – Associate Service Policy to Firewall Rule

In the left navigation, click on **Rule Lists**.

Select Rule List named **Rule_List_Allow_Trusted**.

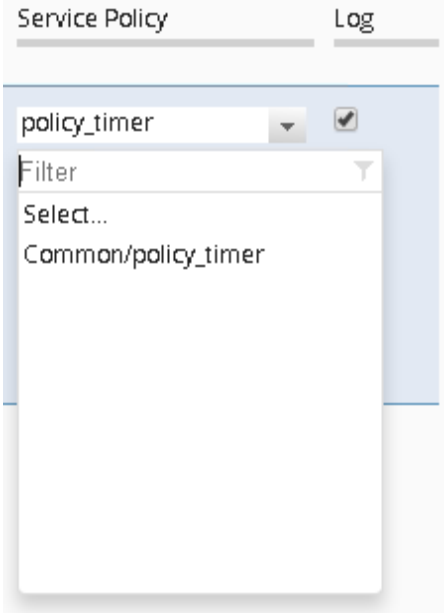
Click on rule 1 named **Rule_Allow_Trusted** to enter rule modification mode.

Scroll to the far right.

Under Service Policy field, type in **policy_timer**.

Click **Save** button at the bottom.

Validate **policy_timer** is listed under **Service Policy** on the rule.



Click **Save & close** button at the top.

Task 4 – Deploy the Service Policy and related configuration objects

Now that the desired timer and service policy configuration has been created on the BIG-IQ, you need to deploy it to the BIG-IP units. In this task, you create the deployment, verify it, and deploy it.

From the top navigation bar, click on **Deployment**.

Click on the **EVALUATE & DEPLOY** section on the left to expand it.

Click on **Network Security** in the expansion.

Click on the top Create button under Evaluation

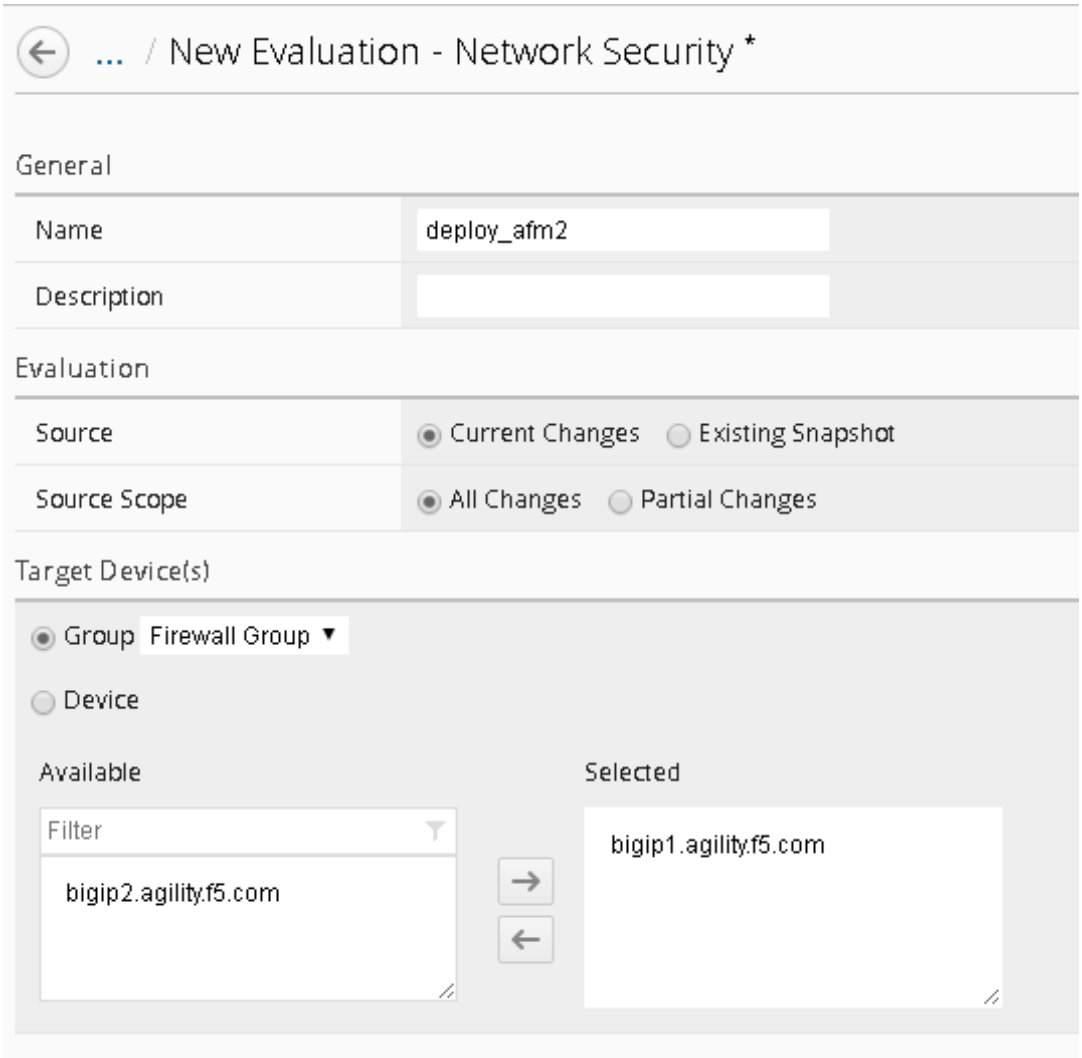
Give your evaluation a name (ex: **deploy_afm2**).

Evaluation **Source** should be **Current Changes** (default).

Source Scope should be **All Changes**

Evaluation **Target** should be **Device**.

Select bigip1.agility.f5.com from the list of Available devices and move it to Selected.



Click the **Create** button at the bottom right of the page.

You should be redirected to the main **Evaluate and Deploy** page.

- This will start the evaluation process in which BIG-IQ compares its working configuration to the configuration active on each BIG-IP. This can take a few moments to complete.
- The **Status** section should be dynamically updating. . . (What states do you see?)

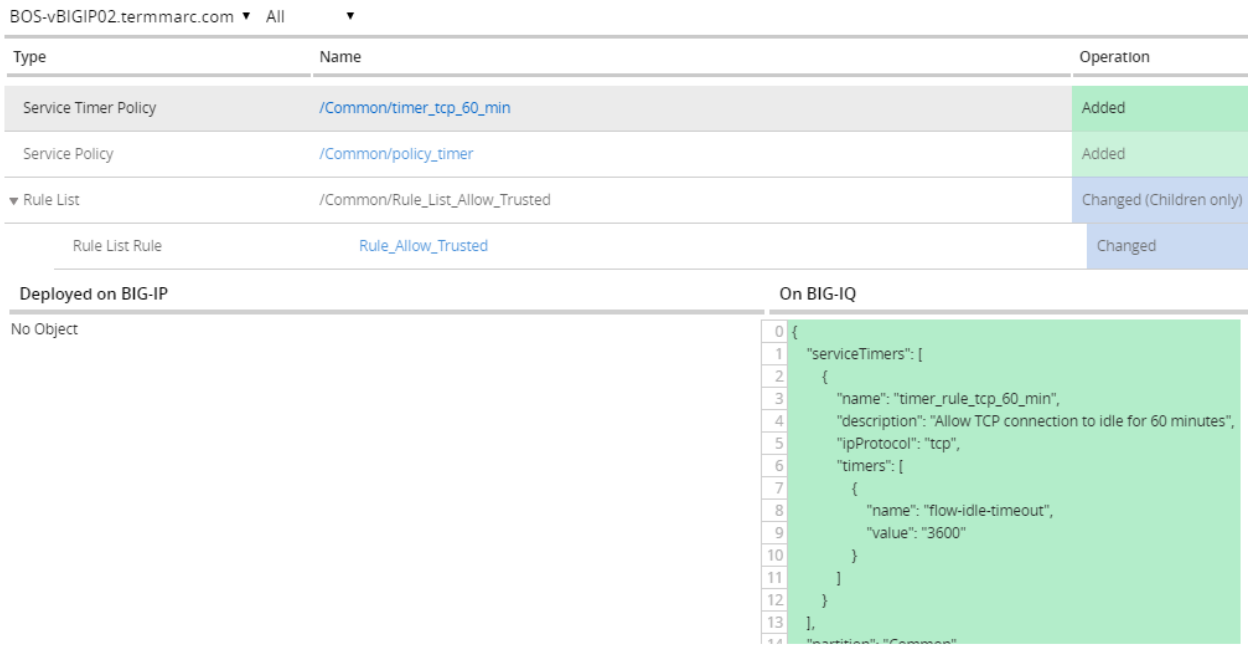
Once the status shows **Evaluation Complete** you can view the evaluation results.

Before selecting to deploy, feel free to select the differences indicated to see the proposed deployment changes. This is your check before actually making changes on a BIG-IP.

Click the number listed under **Differences – Firewall**.

- Scroll through the list of changes to be deployed.

Click on a few to review in more detail.



What differences do you see from the **Deployed on BIG-IP** section and on **BIG-IQ**?

Click **Cancel**.

Deploy your changes by checking the box next to your evaluation **deploy_afm2**.

With the box checked, click the **Deploy** button.

- Your evaluation should move to the **Deployments** section.
- After deploying, the status should change to **Deployment Complete**.
- This will take a moment to complete. Once completed, log in to the BIG-IP and verify that the changes have been deployed to the AFM configuration.

Congratulations, you just deployed your second AFM policy via BIG-IQ!

1.6.3 Locate orphaned and stale firewall rules

WORKFLOW 3: Locate orphaned and stale firewall rules

In this lab, you will be creating a report that will show you firewall rules that do not have any network traffic matching them. You could then consider this firewall rule stale and potentially orphaned if it is no longer needed in your environment.

Objective:

- Locate firewall rules that are orphaned (unused)

Lab Requirements:

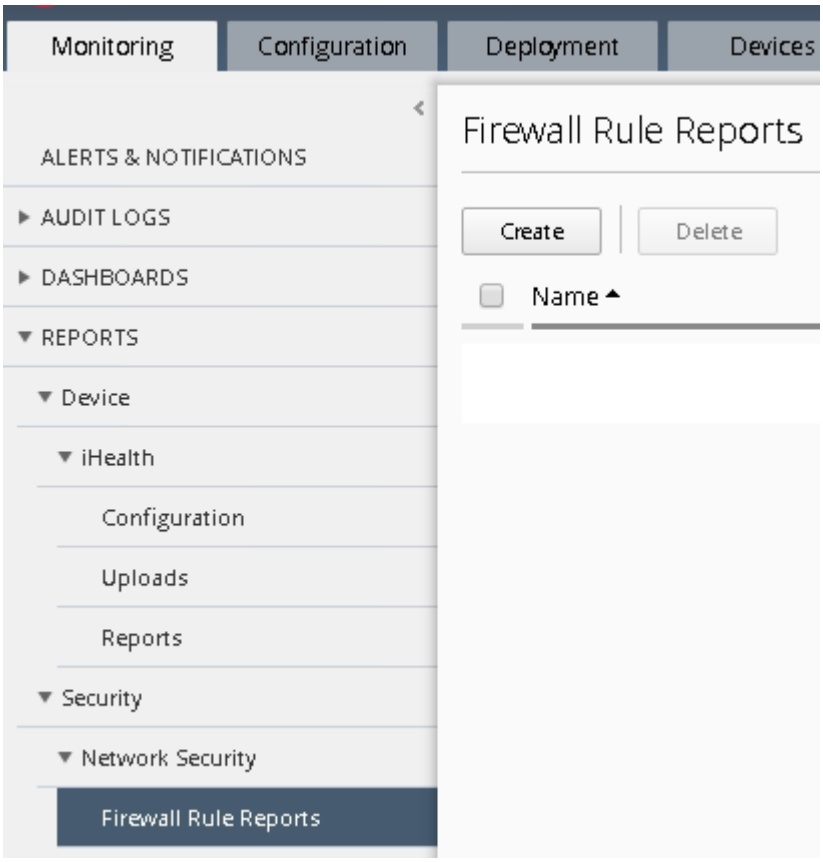
- Web UI access to BIG-IQ

Task 1 – Review Network Firewall Security Reports

On **BIGIQ1**: (*https://10.0.0.200)*

Navigate to **Monitoring** from the top tabs of **BIG-IQ**.

In the left navigation, click on Reports→Security→Network Security→Firewall Rule Reports.



Click **Create**.

For **Name**, type in **test_report**.

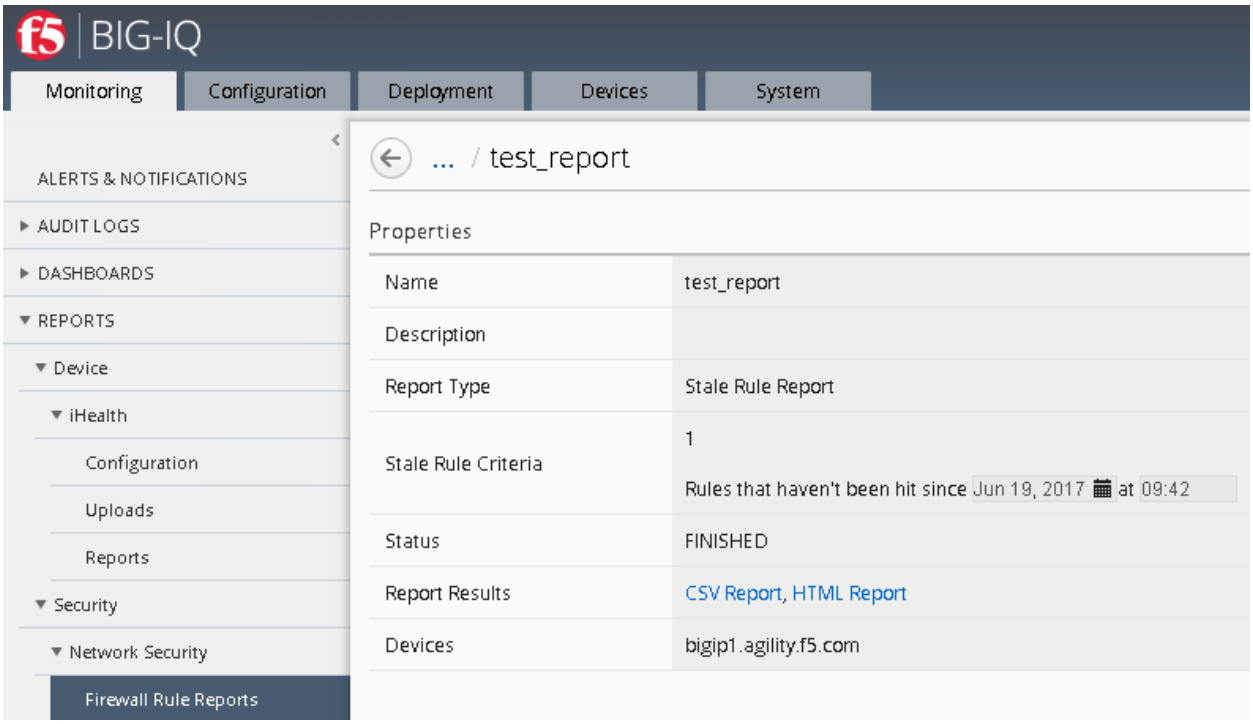
On the **Report Type** dropdown, select **Stale Rule Report**.

On **Stale Rule Criteria**, select Rules with count less than **1** and use today's date

On Available Devices, move bigip1.agility.f5.com to the right Selected box.

Click Save & Close.

Click on the report name **test_report**.



Down below to the right of **Report Results**, click on **HTML Report**.

- There might be a browser pop up block warning in the upper right corner of your browser.
- Allow the pop up. You may have to click on **HTML Report** again.

You should now see a report of rules that do not have **Hit Counts**.

You can also export CSV for further processing of data by selecting **CSV Report.**

1.7 Module 6: External Logging Devices (SevOne)

BIG-IQ Central Management Version - 5.1 has introduced the ability to integrate with SevOne's Performance Logging Appliance (PLA) for high speed logging and reporting.

With SevOne, you can move beyond traditional log search, into real-time troubleshooting of log data at scale. That's because it extracts terabytes of log data daily and correlates it to performance events, thereby eliminating the need for search in your process. It also increases application performance visibility by providing single-click drill-down from related data — SNMP metrics to NetFlow records to syslog files, for example

- Automatically correlate real-time performance metrics with log data.
- Improve visibility of the root cause of performance degradation.
- Receive proactive alerts of customer and end-user behavioral trends.
- Decrease time-to-troubleshoot with integrated metrics, flow and logs.
- Eliminate timely error code analysis with fully configurable value-based lookups.
- Get targeted and intelligent anomaly detection using multiple log metrics across many devices in real-time.
- Leverage multi-variable alerting of log data to identify issues and trends.

- Gain a greater understanding of how configuration changes impact application performance.

1.7.1 Add External Logging Device

WORKFLOW 1 : Add an External Logging Device and Configure Single Sign On

In this lab, you'll be creating a connection to an external logging device (PLA) and configuring single sign on for monitoring

Objective

- Create an external logging device
- Create a login token for SSO

Lab Requirements

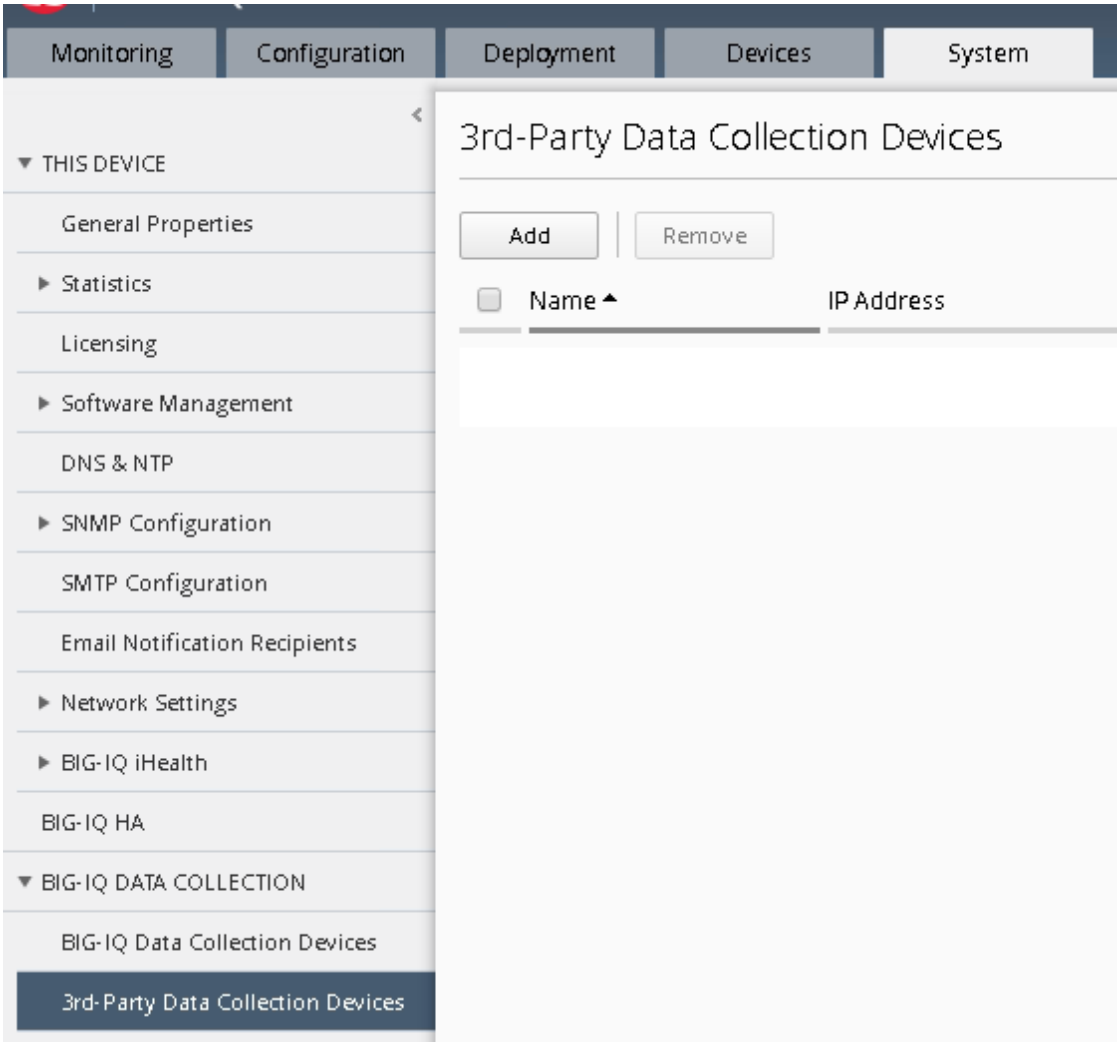
- Web UI access to BIG-IQ

Task 1 – Create an external logging device

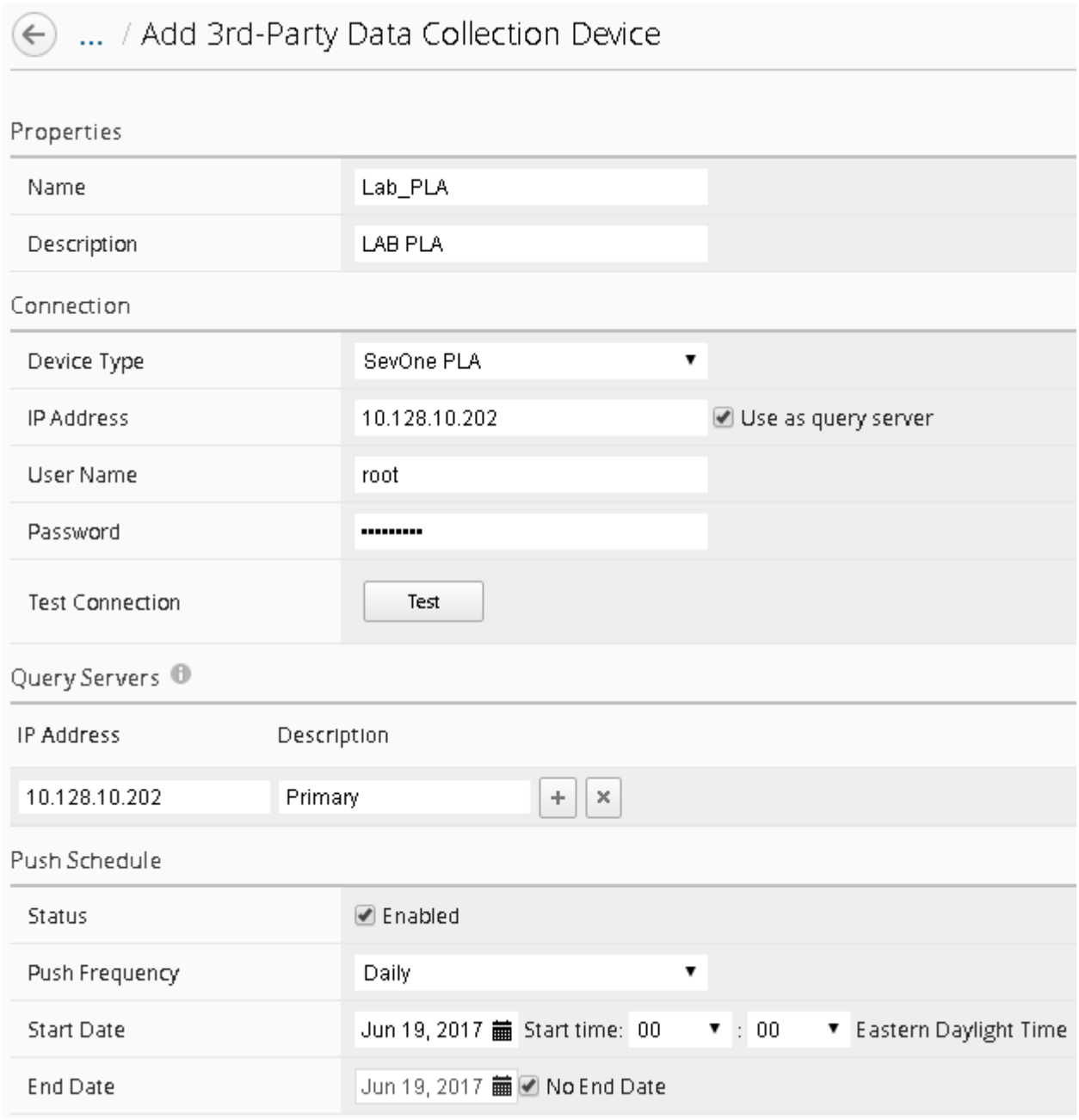
Log into BIG-IQ at *https://10.0.0.200*

Navigate to **System** from the top tabs of **BIG-IQ**.

In the left navigation, click on **BIG-IQ Data Collection** → **3:sup:'rd' Party Data Collection Devices**



Click Add to add a new 3rd Party Data Collection Device

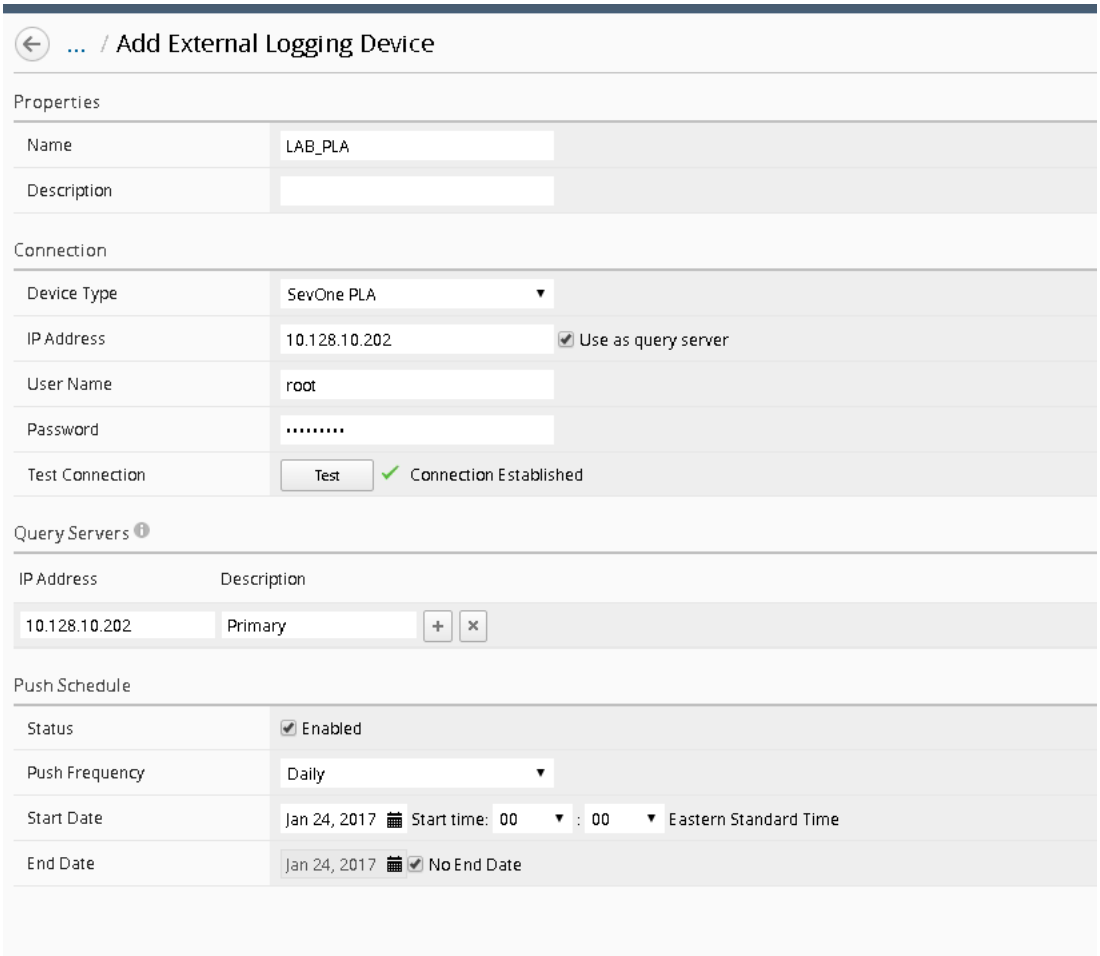


Complete the page with the following table:

Name	**Lab_PLA**	
**Description **	**LAB PLA**	
Device Type	**SevOne PLA**	
IP Address	**10.128.10.202**	Check Use as Query Server
User Name	**root**	
Password	**dRum&5853**	
Push Schedule		
Status	**Enabled Checked**	
Push Frequency	**Daily**	
Start/End Date	**Set to beginning of tomorrow's date (00:00)**	

When completed click the “Test” button on the “Test Connection”

Test will come back successful if settings are all correct as shown below

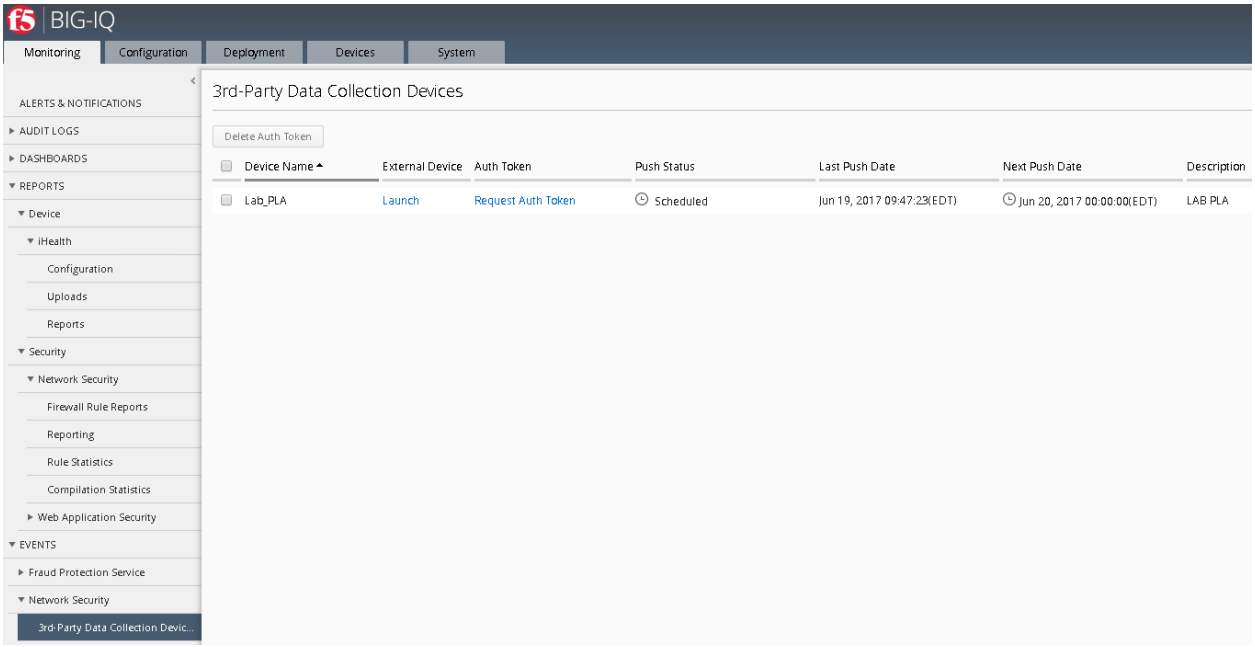


Click Add to complete the addition of an external logging device.

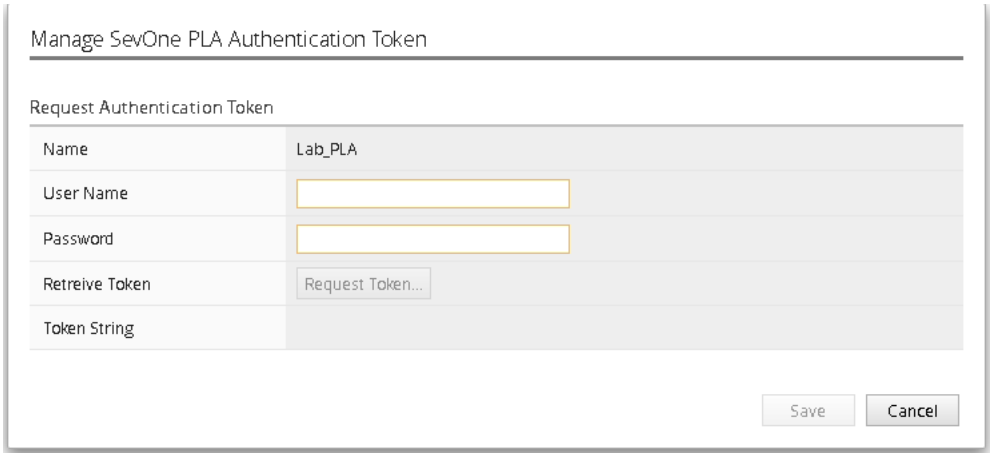
Task 2 – Configure Single Sign On

Navigate to **Monitoring** from the top tabs of **BIG-IQ**.

On the left navigation, click on **Events→Network Security→3:sup:‘rd‘ Party Data Collection Devices**.

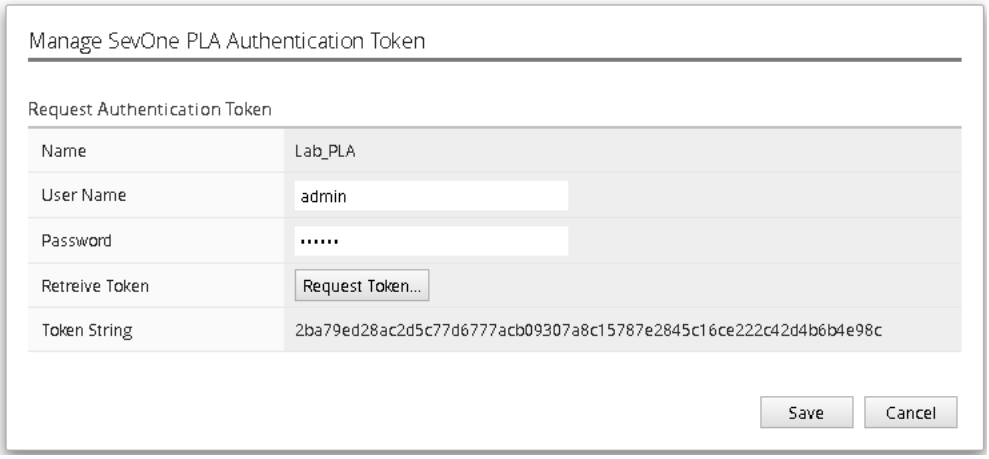


Click on “Request Auth Token”. This will bring up the SevOne PLA Authentication Token screen



Fill in ***admin*** for username and ***SevOne*** for the password and click “Request Token”

If the values are correct, a token will be returned



Click “Save” to save the configuration changes.

You can now click on the “Launch” link to log into the PLA without having to supply a username and password.

Additional Resources:

https://support.f5.com/kb/en-us/products/big-iq-centralized-mgmt/manuals/product/bigiq-central-mgmt-security-5-2-0/10.html#guid-8dbb4024-a82e-4173-83b0-72e0365207e4

1.7.2 Login to Your PLA

To login to your PLA open up a browser on your laptop and use the Management IP address (**10.128.10.202**) or use the Single Sign on in BIG-IQ.

i.e. https://10.128.10.202

The login information for your PLA is ***admin/SevOne***

1.7.3 Familiarize yourself with PLA Settings page

WORKFLOW 1: Familiarize yourself with PLA Settings page

In this lab, you’ll be reviewing the Settings page within PLA.

The Settings page can be accessed by logging into your PLA and clicking on the settings at the top of the page

Each of the sections is briefly detailed below:

Personal Preferences – Changes personal information, date display format and your background.

User Management – Create, enable, and disable users as well as their access levels.

Data Inputs – Create, monitor and stop/start data input listeners.

Cluster Management – View cluster statistics and storage information.

Container Management – View and create new containers and their respective data.

Active Queries – View and control actively running query processes.

Processing Jobs – View and control processing tasks in the job queue

Application Keys – Manage application key files.

Tuples Management – Manage Tuple Tag lists

Alert Configuration – Define alerting rules applied to incoming data

Data Retention – Configure data retention options and view average usage.

Licensing – Manage the license associated with the PLA

Software Update – Check for software updates.

1.7.4 Creating and Viewing Alerts

WORKFLOW 2: Creating and Viewing Alerts

In this lab, you'll be creating a new alert and reviewing the alert

Navigate to ***Settings*** > ***Alert Configuration***

Click "***Add New Rule***"

Select Content text matching or context tag analytics based on the rule you are trying to create. For example, to create a new rule that will alert when a new IP is ingested into the system (E.G. for a new DDoS alerting mechanism) you would enter the following:

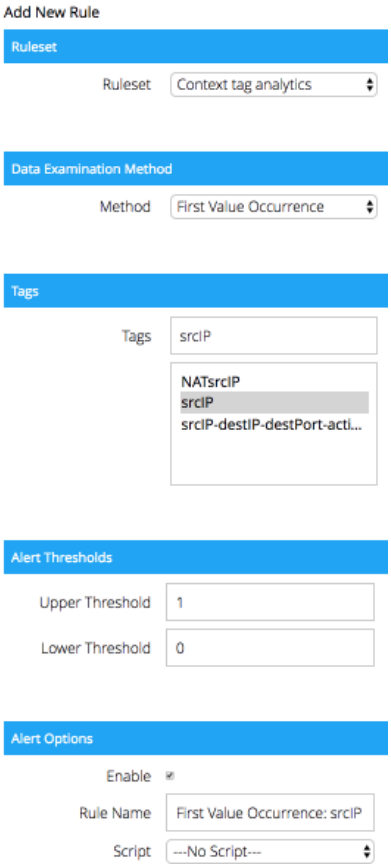
Ruleset – Context Tag Analytics

Data Examination Method – First Value Occurrence (FVO is unique to the PLA)

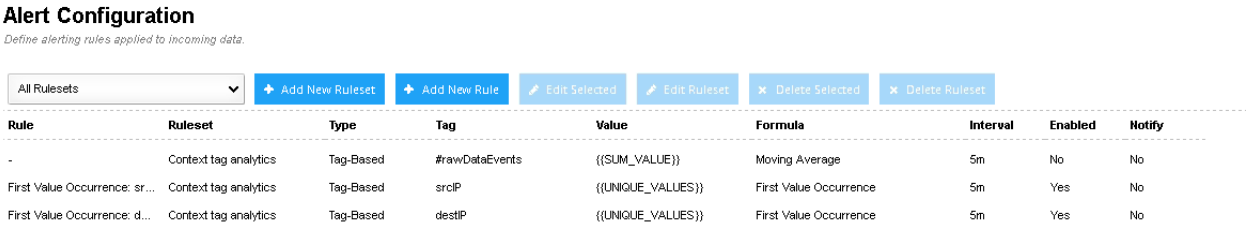
Tags – SrcIP

Alert Thresholds – Upper 1 Lower 0

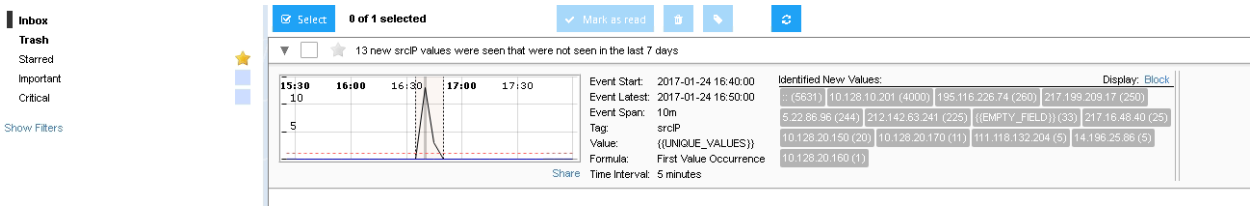
Alert Options – Enable (email or trap) or if left to –No Script—Alerts will appear on the Alerts Page



When finished click +**Add** and you will see a summary of the current alerts



If no external alerting mechanism is configured you can view current alerts on the ***Alerts*** tab as shown:



Now whenever a new Source or Destination IP is processed by the PLA an alert will be created.

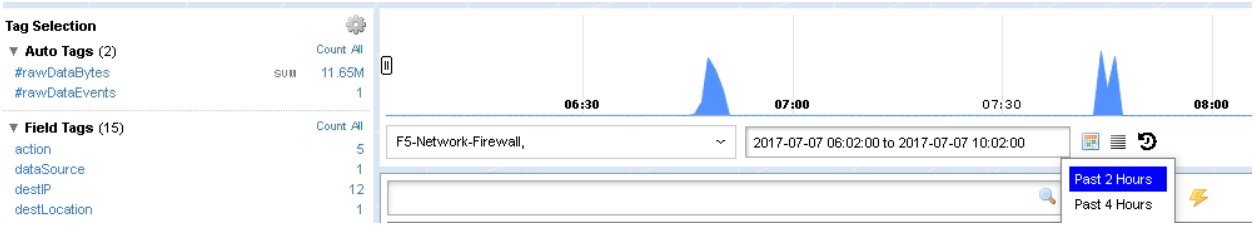
1.7.5 Viewing event logs and creating a tuple

WORKFLOW 3: Viewing event logs and creating a tuple

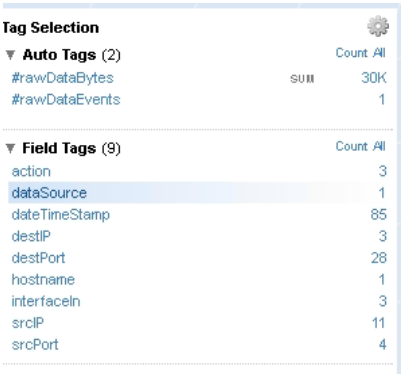
In this lab, you'll become familiar with the Investigate section, this is where the raw logs can be viewed along with tuples created.

Navigate to the ***Investigate*** tab at the top of the page.

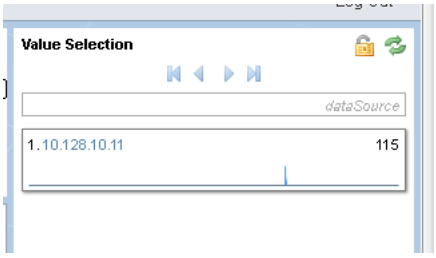
Verify you're looking at the most recent data by selecting the past 2 hours from the hamburger next to the date near the top of the screen as shown below



Select a field tag to view the data within the tag:



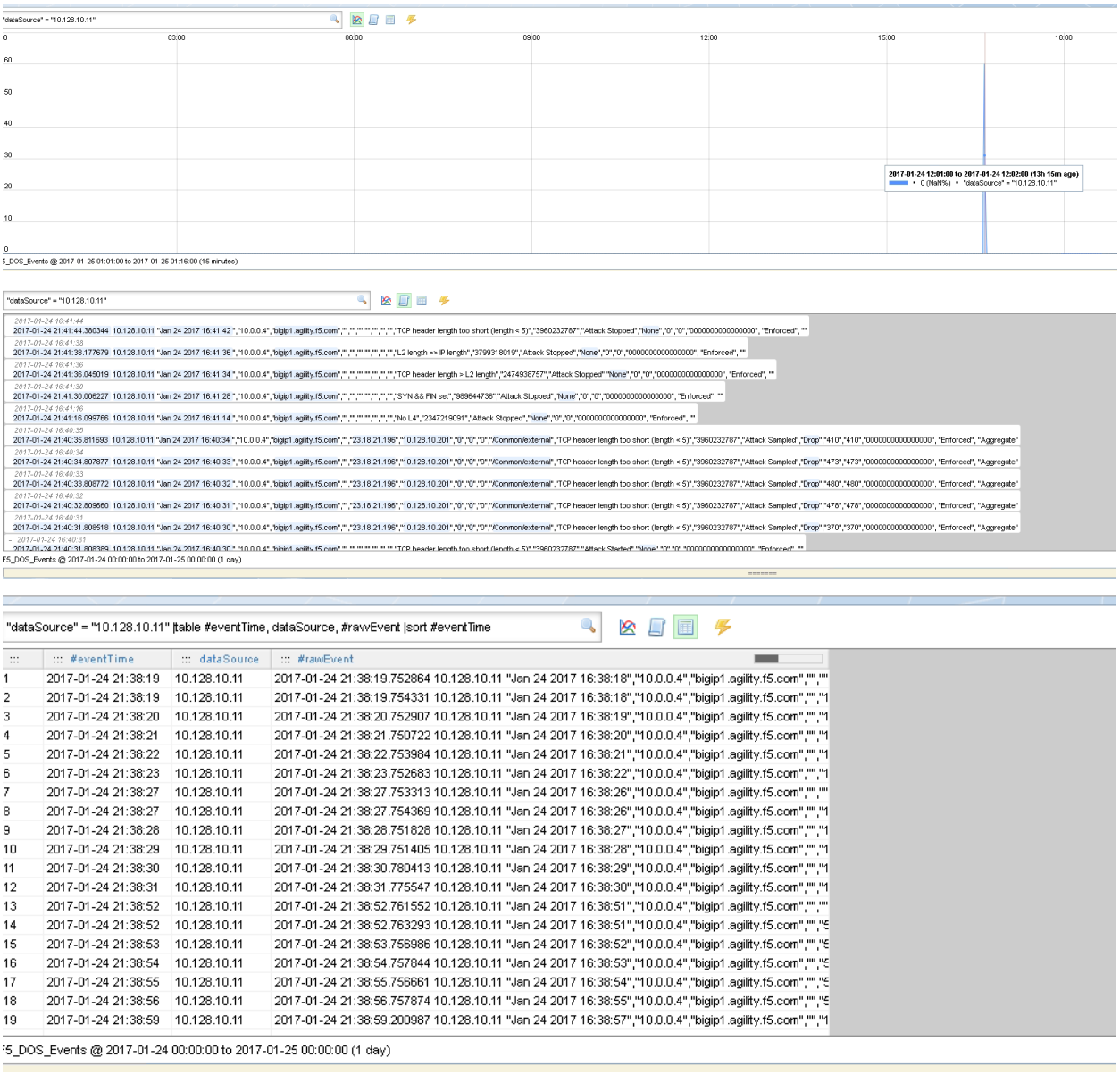
The far right will display the values within the selected tag:



This is useful if you are looking for data from a specific device for troubleshooting.

Click on the value and data will load from that selected field in the viewing pane:

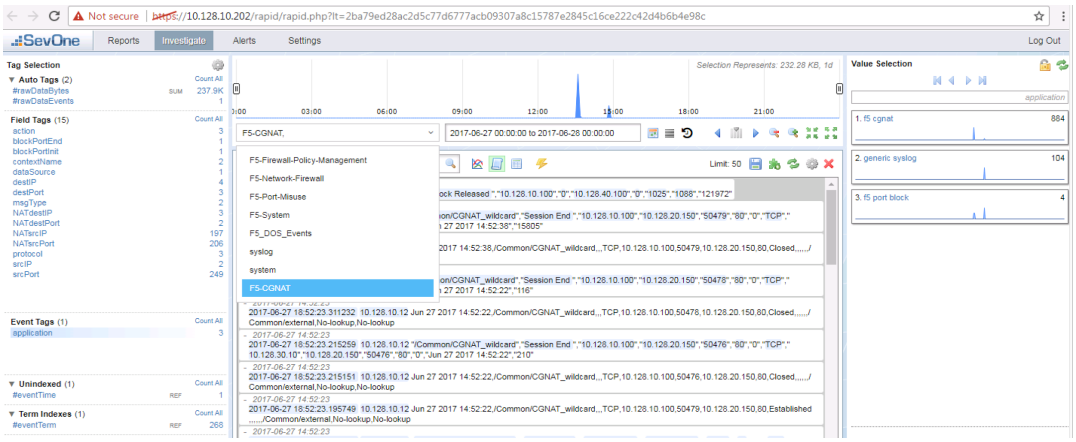
Different representations of the data can be selected by toggling through the graph, textual and grid-style as shown below



To view the logs from Lab one

Click on “Investigate”

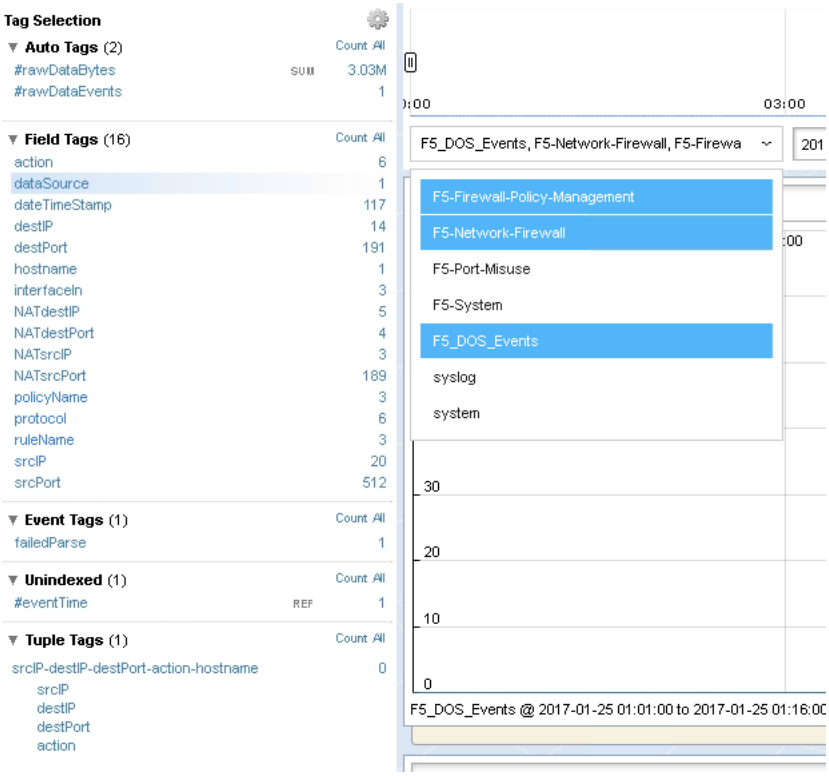
From the Central Menu select the F5-Network-Firewall container as shown in the following image:



From left Menu under ***Event Tag*** click on ***application.***

From the Right Menu click review the logs in the central part of the screen.

To select different containers or compound key searches select the desired keys from the drop down to represent the data you are investigating:

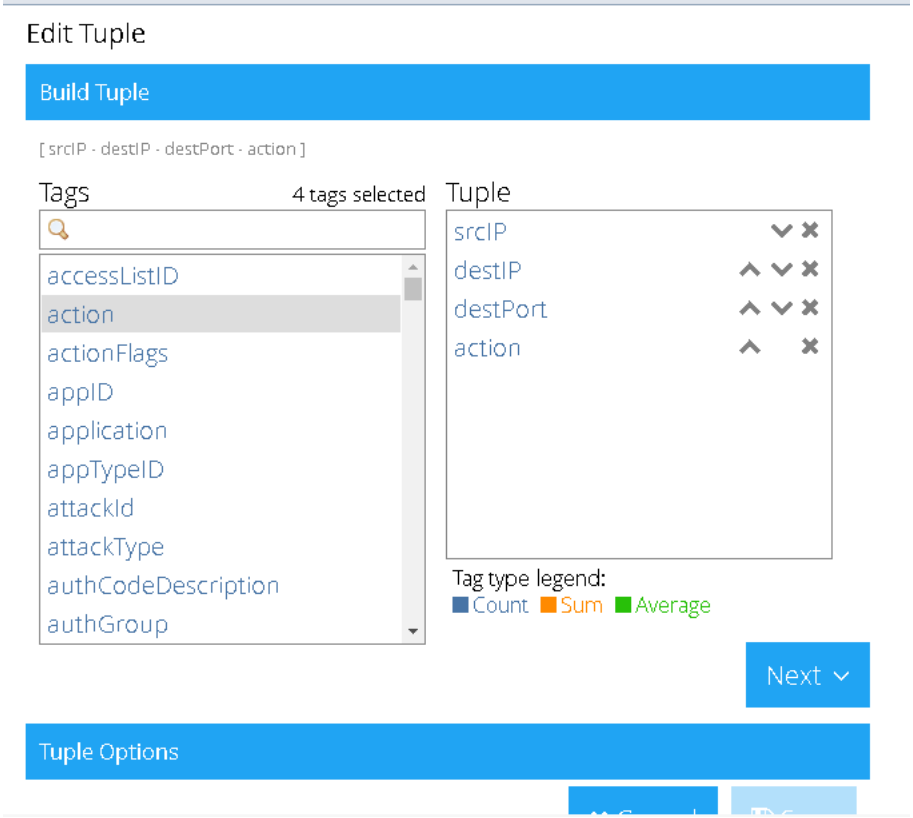


As more data is selected more tags become available for further analysis.

Tuples allow for quick views of multiple tags – for example if you wanted to always view just the srcIP, destIP, destPort, action and hostname you could build a quick tuple for this data representation.

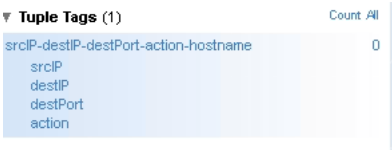
To create a new Tuple, navigate to Setting > Tuples Management

Click Add to create a new tuple and select the desired tags along with the time interval.



When finished click save.

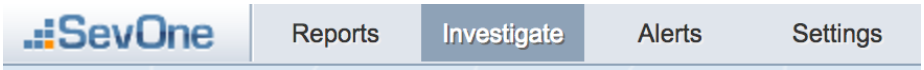
Tuples can be viewed from the ***Investigate*** page under tuple tags (note tuples take 5 minutes to refresh their defined data):

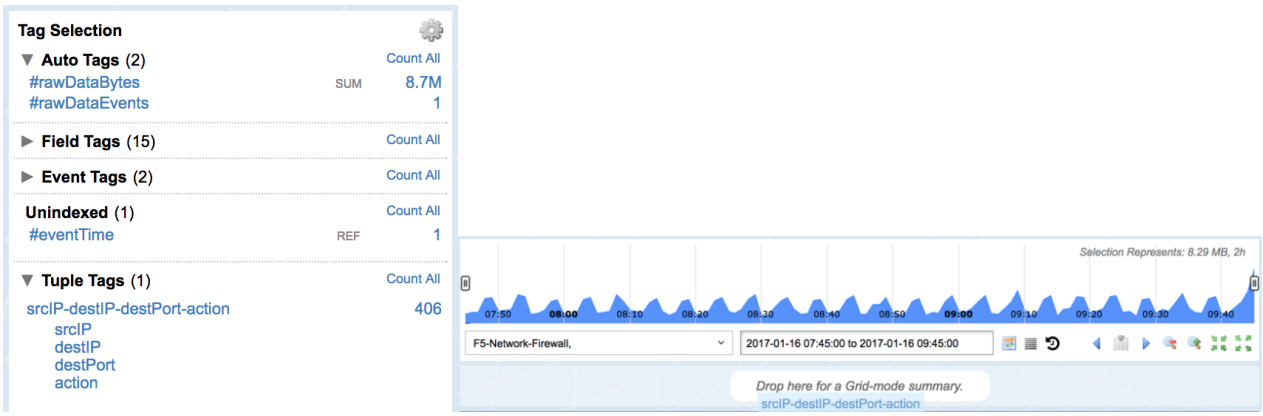


1.7.6 Creating Reports

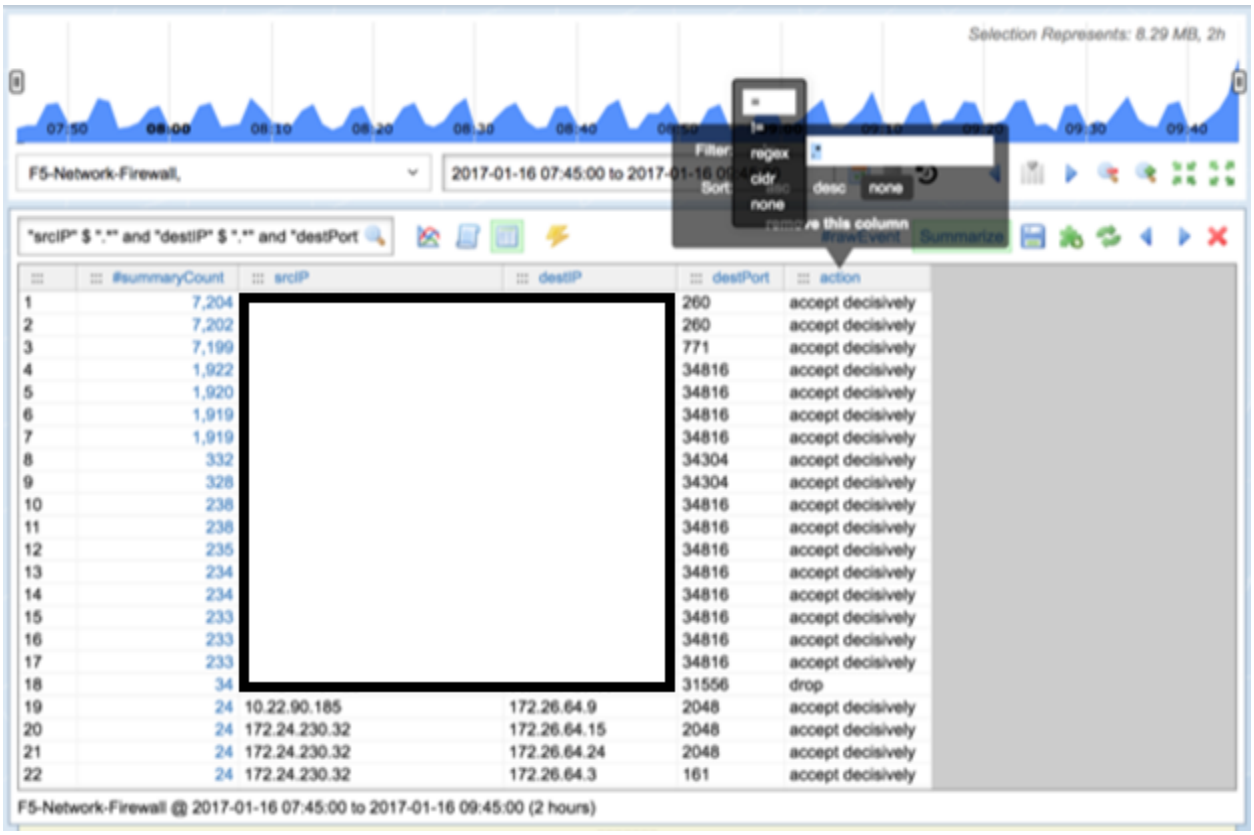
WORKFLOW 4: Creating Reports

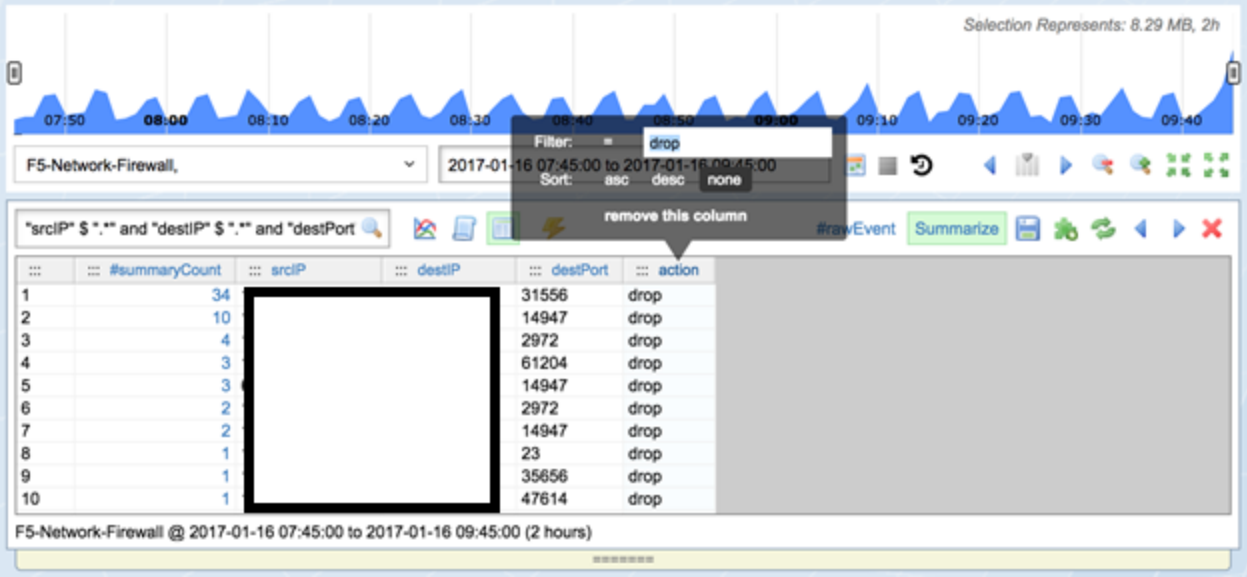
Navigate to Investigate Page & Select Past Two Hours



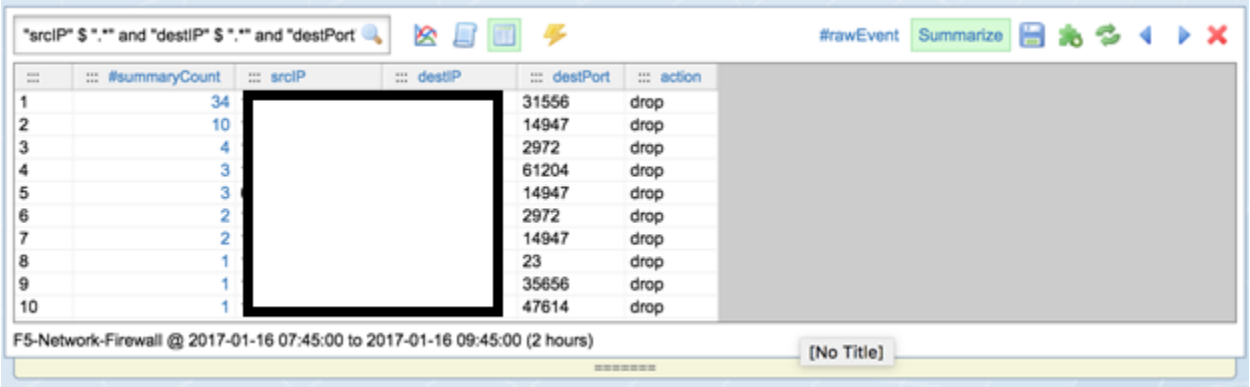


Right click ‘action’ column header to filter column, click on host & drag filter to select = (type in drop)



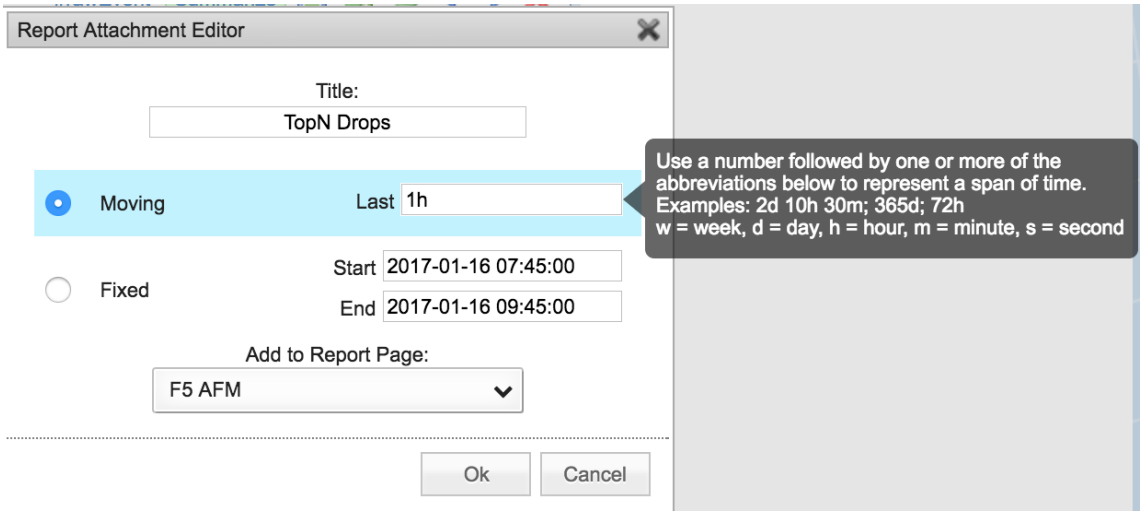


Click the “Puzzle” piece icon to open Report Attachment Editor



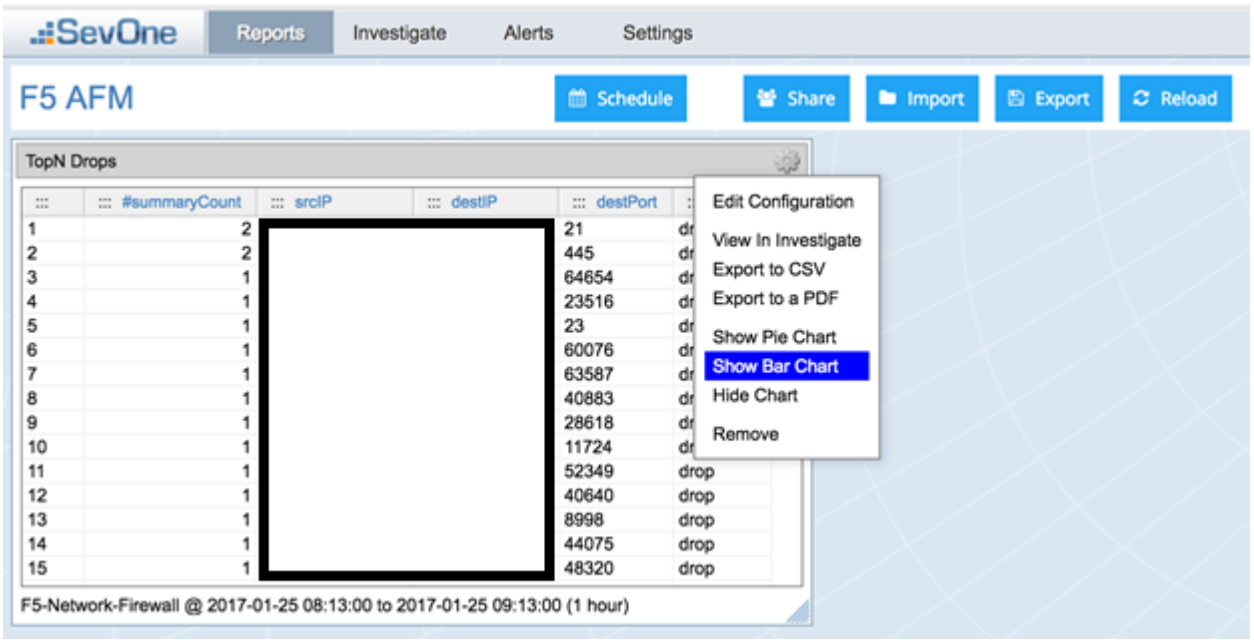
Enter Parameters:

- Title
- Moving time frame
- Report Page

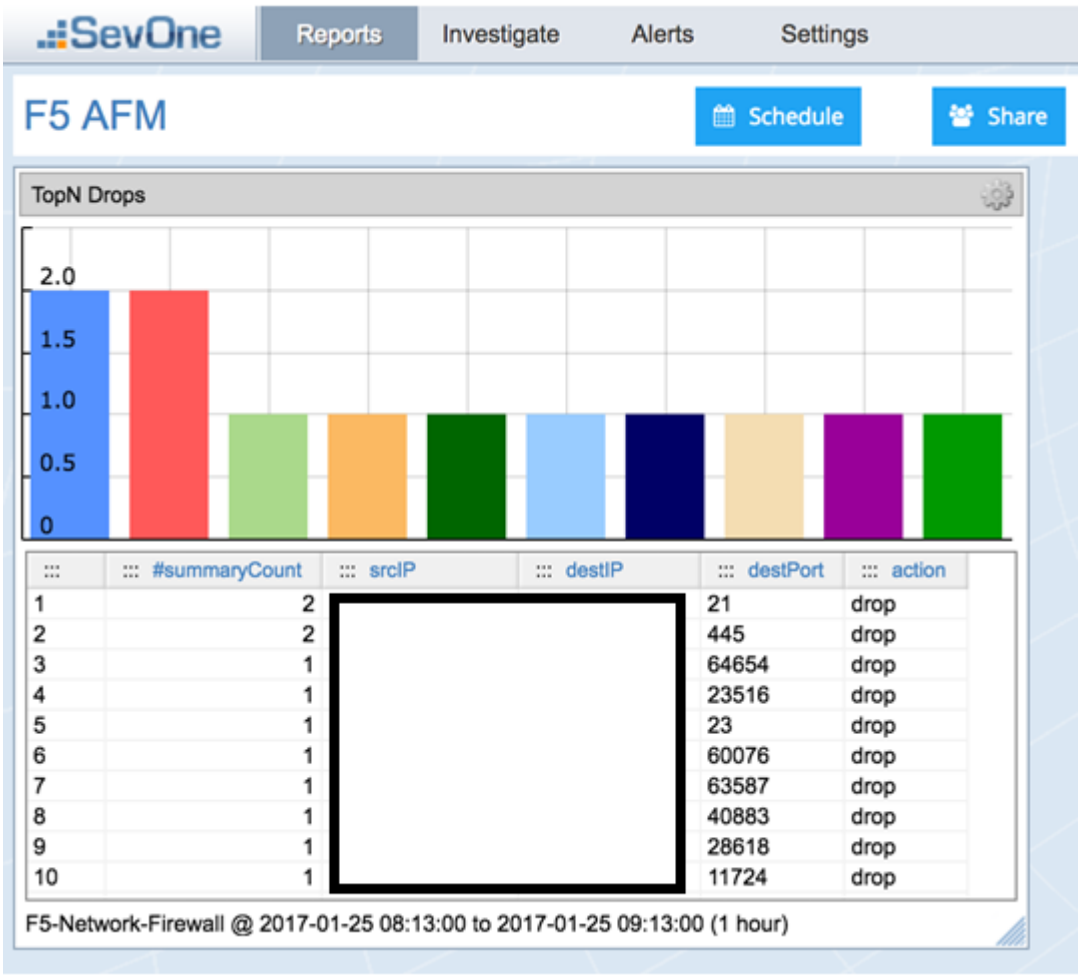


Navigate to Reports Page

Click on “Gear” icon and select Show Bar Chart



The appropriate chart selected will be displayed


SevOne
Reports
Investigate
Alerts
Settings
F5 AFM
Schedule
Share
TopN Drops
2.0
1.5
1.0
0.5
0
#summaryCount
srcIP
destIP
destPort
action
1 2 21 drop
2 2 445 drop
3 1 64654 drop
4 1 23516 drop
5 1 23 drop
6 1 60076 drop
7 1 63587 drop
8 1 40883 drop
9 1 28618 drop
10 1 11724 drop
F5-Network-Firewall @ 2017-01-25 08:13:00 to 2017-01-25 09:13:00 (1 hour)

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com