Configuring BIG-IP Advanced Firewall Manager for Splunk

Configuration tasks for configuring BIG-IP AFM 11.3.0 for High Speed Logging to Splunk

Table of Contents

Configuring BIG-IP for High Speed Logging 2

Overview 2

Network Topology 2

Pre-requisites 3

Basic Network and Virtual Servers 3

Licensing and Provisioning 3

Configuring AFM Logging 4

Log Pool 4

Log Destinations 4

Log Publisher 5

Log Profile 6

Protocol Security Logging 8

DoS Protection Logging 8

Associate Profile to the Virtual Server 8

Create AFM Rules 10

Rule Lists 10

Individual Rules 10

Virtual Server Rules 12

Configuring Device Management Logging 13

Log Destinations 13

Log Publisher 14

Configuring Log filtering 15

Configuring the Splunk iRule 16

Add the iRuel to the BIG-IP 16

Apply   the iRule to the Virtual server 17

Splunk Web Access iRule 18

Configuring BIG-IP for High Speed Logging

Overview

The configuration for high speed logging to Splunk is covered in this document. The logging will include Security based logs, Network Management logs, and the Splunk provided iRule. The network connectivity for the logging from BIG-IP to the Splunk server(s) is via an F5 BIG-IP LTM Pool. The Splunk server is a member of this pool. The BIG-IP logging profile is defined to send log messages to the pool that in turns sends the message to the pool member(s).

Network Topology

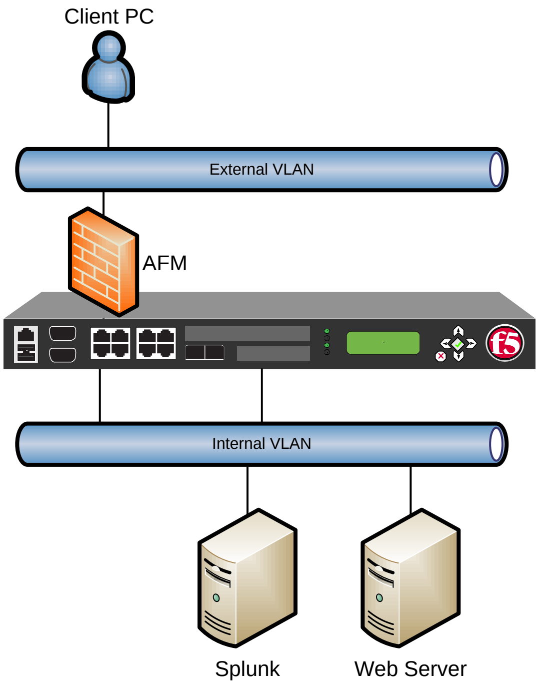


Figure 1: AFM Logging Network Topology

Pre-requisites

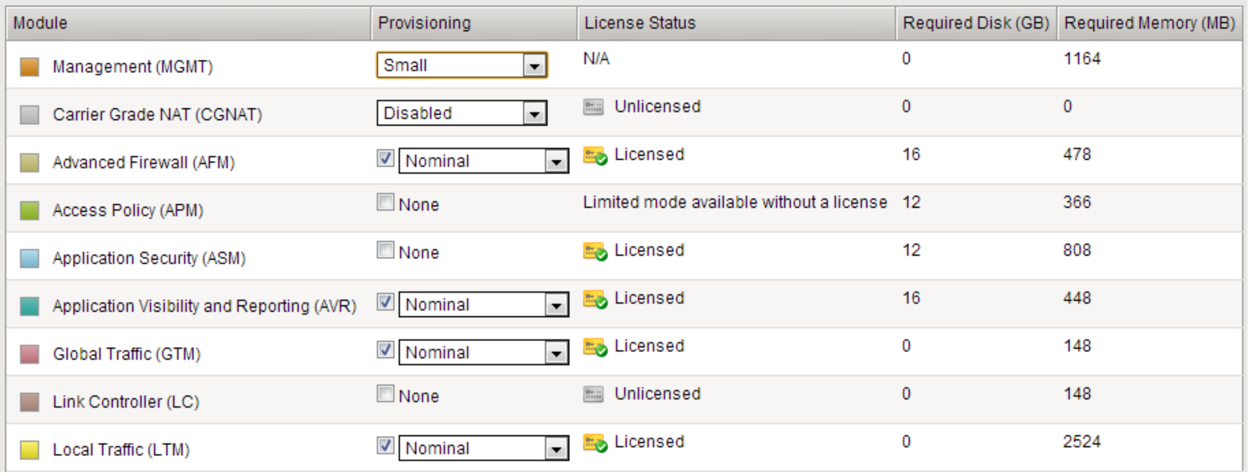
Basic Network and Virtual Servers

This guide assumes the BIG-IP has been configured for Network Management access. External servers are configured and network reachable.

Licensing and Provisioning

The BIG-IP needs to be operating the 11.3 BIG-IP release. The BIG-IP needs to be licensed for LTM and AFM. Verify it has a license by logging into the Management Interface and choose System → License

Provision the BIG-IP to enable LTM and AFM. Choose System → Resource Provisioning. **Enabl**e the provisioning check boxes next to the LTM and AFM and select **Nominal**. Optionally provision the other modules that your license permits.



Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1164
Carrier Grade NAT (CGNAT)	Disabled	Unlicensed	0	0
Advanced Firewall (AFM)	☑ Nominal	Licensed	16	478
Access Policy (APM)	□ None	Limited mode available without a license	12	366
Application Security (ASM)	□ None	Licensed	12	808
Application Visibility and Reporting (AVR)	☑ Nominal	Licensed	16	448
Global Traffic (GTM)	☑ Nominal	Licensed	0	148
Link Controller (LC)	□ None	Unlicensed	0	148
Local Traffic (LTM)	☑ Nominal	Licensed	0	2524

Figure 2: LTM and AFM Provisioning

Choose **Submit** to commit the changes.

Configuring AFM Logging

The Splunk pool needs to be created and the Splunk server added as a pool member.

Log Pool

The logs will be sent to an external log server. An LTM Pool is the destination for high speed logging. Create a pool and name it **Logging_Pool**. Select Local Traffic → Pools → Pool List and select **Create**. Enter the name and select a *TCP* or *UDP* **Health Monitor**. The logging server may support UDP or TCP or Both. For very large log messages that span multiple Ethernet packets requires TCP.

In the Resource section define the **Node Name** to be **Logging_Node**, enter the **IP** address to be the Splunk Server **10.10.10.1** and configure the **Service Port** to be **514**. Choose **Add**, and then **Finished**.

Note: The Service port number must be defined. It must match to one of the settings in Manager→Data Inputs on the Splunk Server.

Name	Logging_Pool		
Health Monitor	TCP or UDP		
Load Balancing Method	Round Robin		
Members	**Node Name**	**Address**	**Service Port**
	Logging_Node	10.10.10.1	514

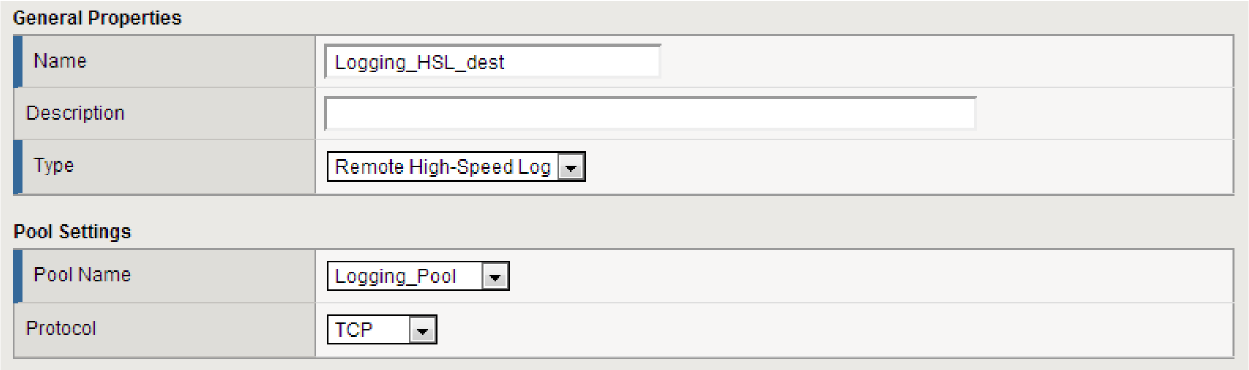
Log Destinations

At least, two log destinations need to be created. The first one will be the High Speed Logging Destination and the second one will be a Log Destination for log formatting purposes. The logs will be sent as formatted log sentences to the HSL destination.

High Speed Logging Log Destination

Select System → Logs → Configurations → Log Destinations and choose *Create*. Name the Log destination **Logging_HSL_dest,** type is **Remote High-Speed Log**, and select the pool name to be **Logging_Pool**. Select **Repeat** to create another log destination

Name	Logging_HSL_dest
Type	Remote High-Speed Log
Pool Name	Logging_Pool
Protocol	TCP



General Properties

Name	Logging_HSL_dest
Description	
Type	Remote High-Speed Log

Pool Settings

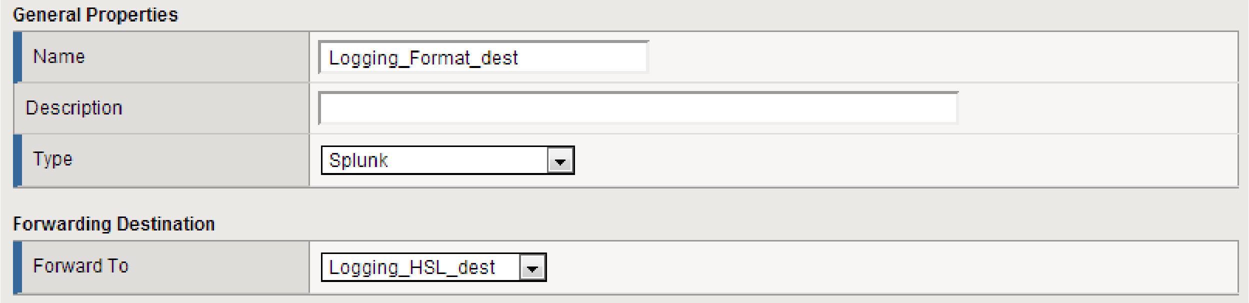
Pool Name	Logging_Pool
Protocol	TCP

Figure 5: HSL Logging Destination

Formatted Log Destination

This log destination will be used to format the log output. The formatted log events will be sent to the HSL Log Destination previously created. Name the log destination **Logging_Format_dest,** type is **Splunk**, and the **High Speed Log Destination** is **Logging_HSL_dest**. This builds a layering effect for formatting and dispatching the logs.

Name	Logging_Format_dest
Type	Splunk
Forward To	Logging_HSL_dest



General Properties

Name	Logging_Format_dest
Description	
Type	Splunk

Forwarding Destination

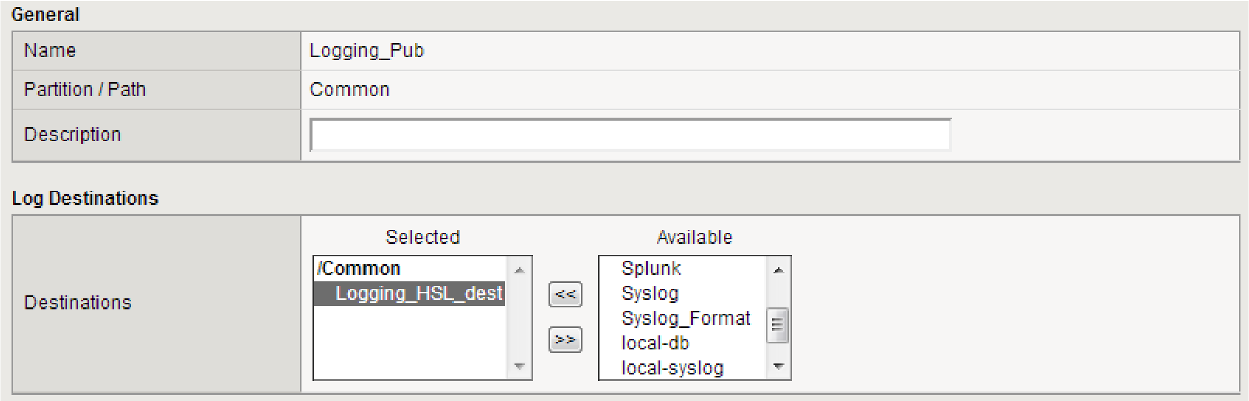
Forward To	Logging_HSL_dest

Figure 6: Syslog Formatting

Log Publisher

The log publisher is a way to associate individual or multiple log destinations to a security log profile. Select System → Logs → Configurations → Log Publishers and choose *Create*. Name this publisher **Logging_Pub** and select **Logging_Format_dest** and move it into the selected column. Select **Finished** when done.

Name	Logging_Pub
Destinations	Logging_Format_dest
	local-db (optional)
	local-syslog (optional)



General

Name	Logging_Pub
Partition / Path	Common
Description	

Log Destinations

	Selected	Available
Destinations	/Common Logging_HSL_dest	Splunk Syslog Syslog_Format local-db local-syslog

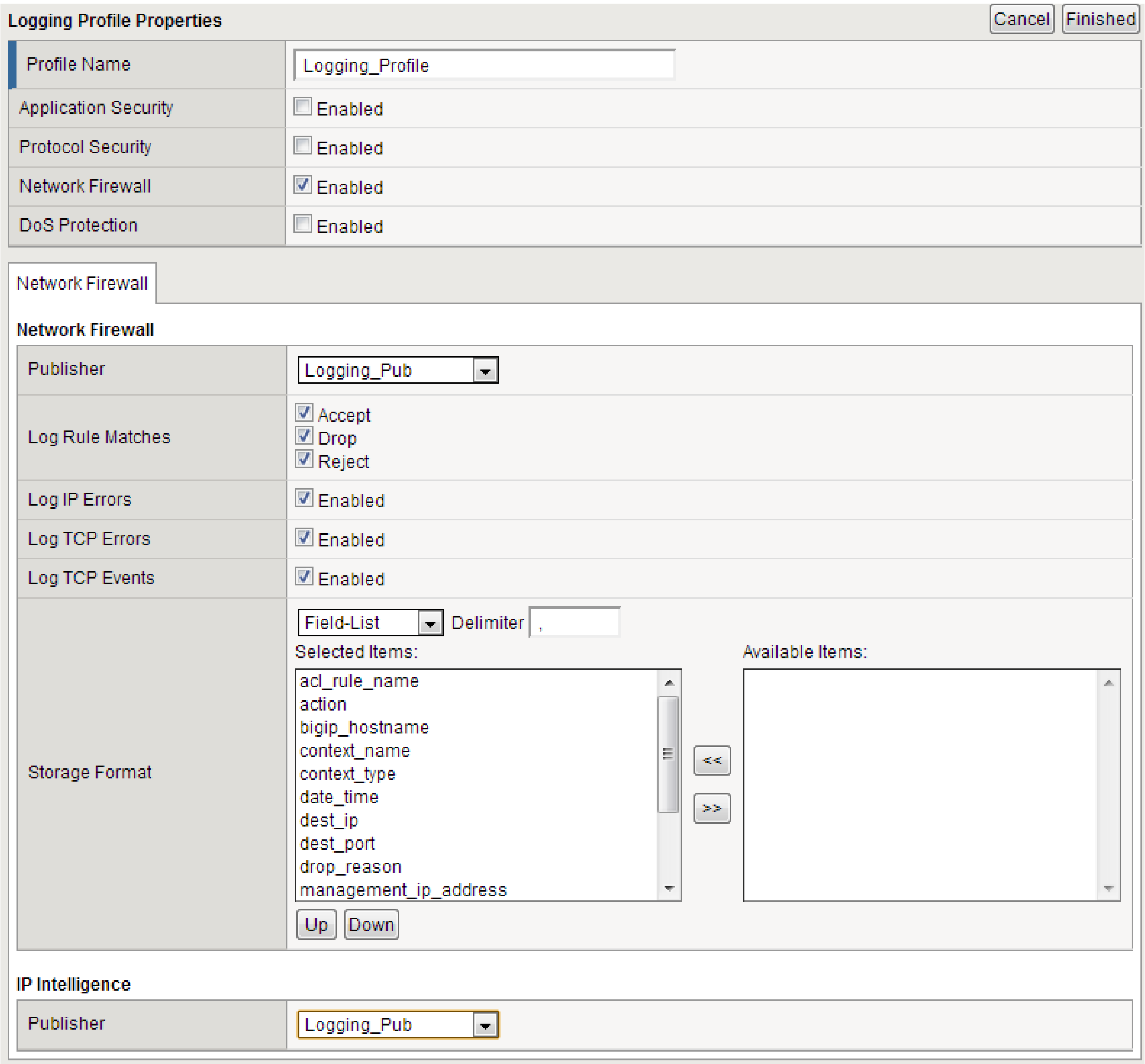
Figure 7: Logging Publisher

This step created a log publisher that will send Splunk formatted events to the Splunk server.

Log Profile

The Log Profile is the association between security log producers (AFM) with the log destinations. It also configures which type of events to be produced. Create a new Logging Profile by **selecting** *create* from Security → Event Logs → Logging Profiles. Specify the **Name** to be **Logging_Profile,** Enable **Network Firewall**, select the publisher **Logging_Pub**, all the log variants, select **field-list** and move all the available items to the selected column. Choose **Finished** when complete.

Note: in figure 8 the BIG-IP was provisioned for ASM, AFM, and PSM.



Logging Profile Properties

Profile Name	Logging_Profile
Application Security	□ Enabled
Protocol Security	□ Enabled
Network Firewall	☑ Enabled
DoS Protection	□ Enabled

Network Firewall

Network Firewall

Publisher	Logging_Pub
Log Rule Matches	☑ Accept ☑ Drop ☑ Reject
Log IP Errors	☑ Enabled
Log TCP Errors	☑ Enabled
Log TCP Events	☑ Enabled
Storage Format	Field-List Delimiter , Selected Items: acl_rule_name action bigip_hostname context_name context_type date_time dest_ip dest_port drop_reason management_ip_address Available Items:

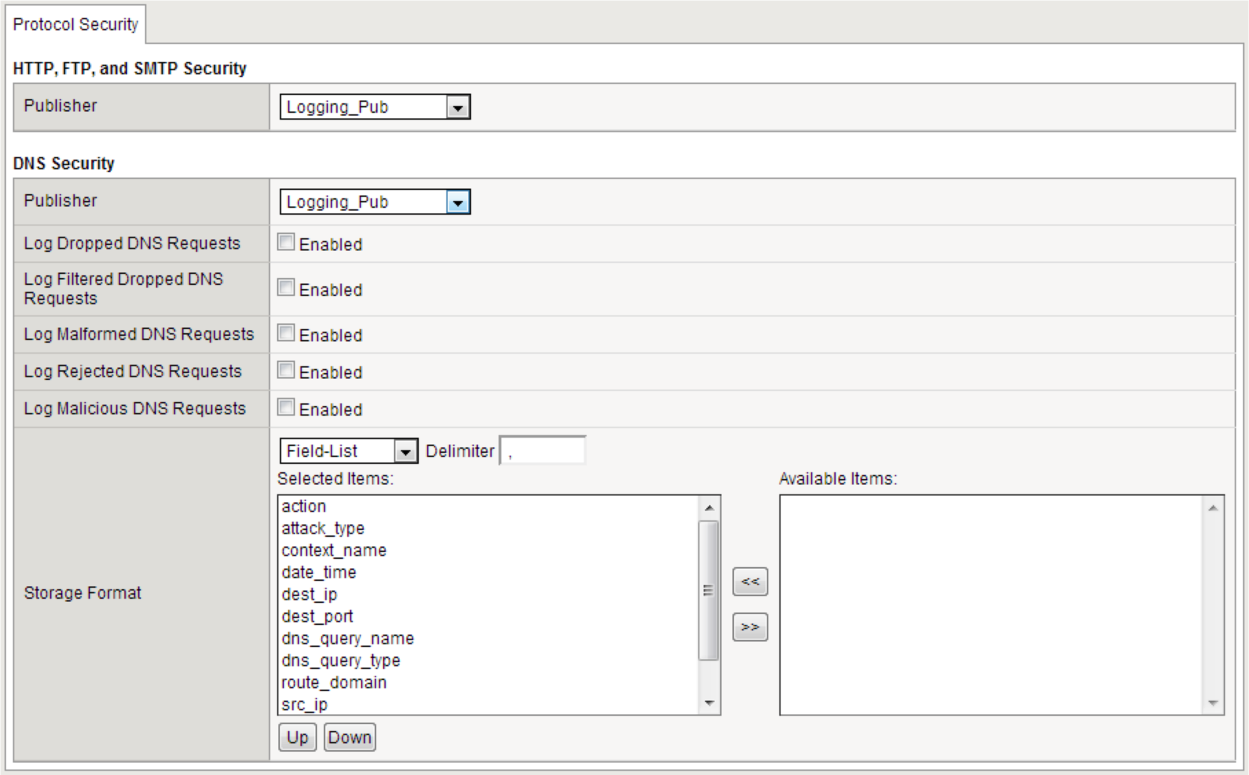
IP Intelligence

Publisher	Logging_Pub

Figure 8: Logging Profile: Network Firewall

Protocol Security Logging

Optionally you can choose to enable logging for Protocol Security.



Protocol Security

HTTP, FTP, and SMTP Security

Publisher	Logging_Pub

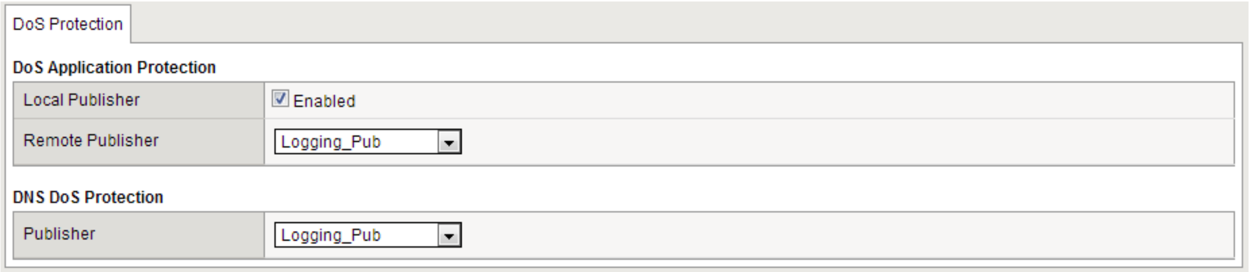
DNS Security

Publisher	Logging_Pub
Log Dropped DNS Requests	□ Enabled
Log Filtered Dropped DNS Requests	□ Enabled
Log Malformed DNS Requests	□ Enabled
Log Rejected DNS Requests	□ Enabled
Log Malicious DNS Requests	□ Enabled
Storage Format	Field-List, Delimiter , Selected Items: action, attack_type, context_name, date_time, dest_ip, dest_port, dns_query_name, dns_query_type, route_domain, src_ip Available Items:

Figure 10: Protocol Security Logging

DoS Protection Logging

Optionally you can choose to enable logging for DoS Protection Security.



DoS Protection

DoS Application Protection

Local Publisher	☑ Enabled
Remote Publisher	Logging_Pub

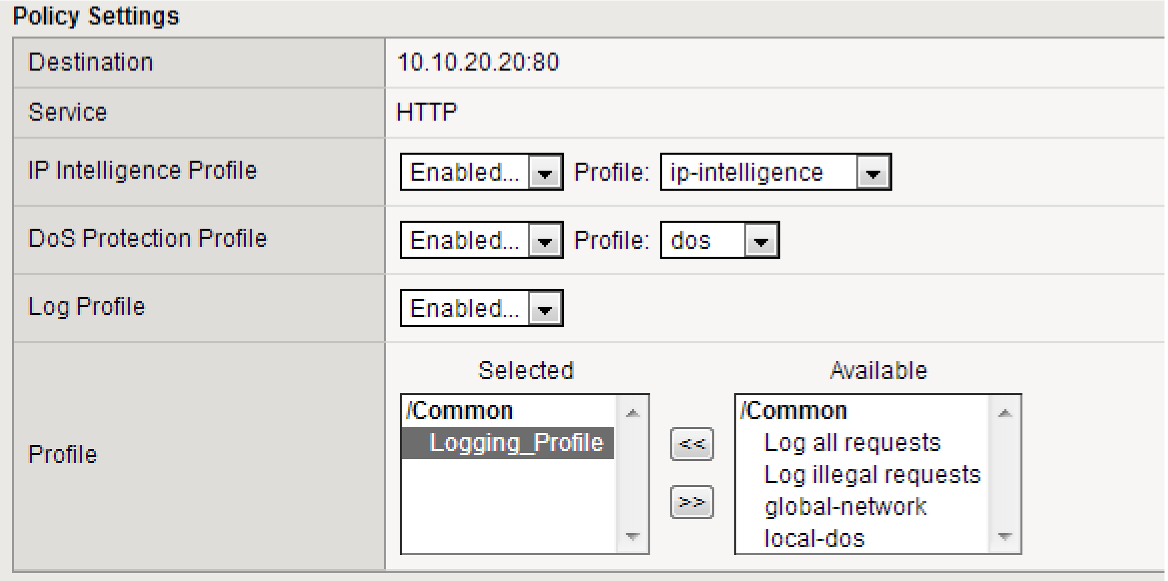
DNS DoS Protection

Publisher	Logging_Pub

Figure 11: DoS Protection logging

Associate Profile to the Virtual Server

The Security log profile is associated to Virtual Servers with in the Security Policy tab. Select Local Traffic → Virtual Servers. Select the virtual server to enable security logging on. Select the **Security** tab and choose **Policies**. Enable the Log Profile and move **Logging_Profile** to the selected column. Select **Update** when finished. The IP Intelligence Profile and DoS Protection Profile are enabled with the default profiles selected. Enabling these profiles will include the log messages associated to these features to be sent to the **Logging_Profile** and in turn to the log destinations via the log publisher.



Policy Settings

Destination	10.10.20.20:80
Service	HTTP
IP Intelligence Profile	Enabled... Profile: ip-intelligence
DoS Protection Profile	Enabled... Profile: dos
Log Profile	Enabled...
Profile	Selected: /Common Logging_Profile Available: /Common Log all requests Log illegal requests global-network local-dos

Figure12: Virtual Server: Security Policy Settings

Notice the lower portion of this page is the Rule section.

Create AFM Rules

Rule Lists

Rule lists are a way to group a set of like rule together and apply them to the active rule base as a group. Lists are made up of individual rules.

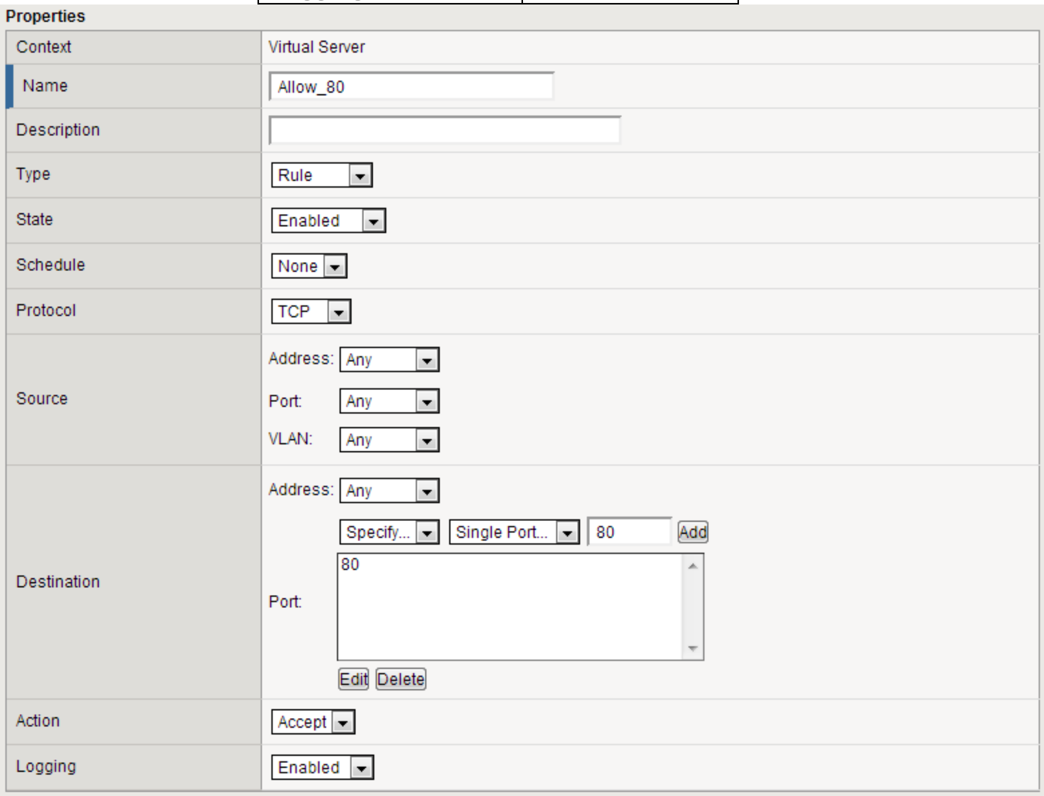
Individual Rules

Security → Network Firewall → Rules Lists Chose create specify the name to be **Web_List** hit Finished when complete. Edit the **Web_List** rule list by selecting it again. This is where individual rules can be added to the list.

Allow TCP port 80 and reject all

The first rule is to allow tcp port 80 with logging. Specify the name to be **Allow_80,** protocol **TCP**, specify port to be **80**, and logging **Enabled**.

Name	Allow_80
Type	Rule
Protocol	TCP
Destination Port	Specify Single Port 80
Action	Accept
Logging	Enabled



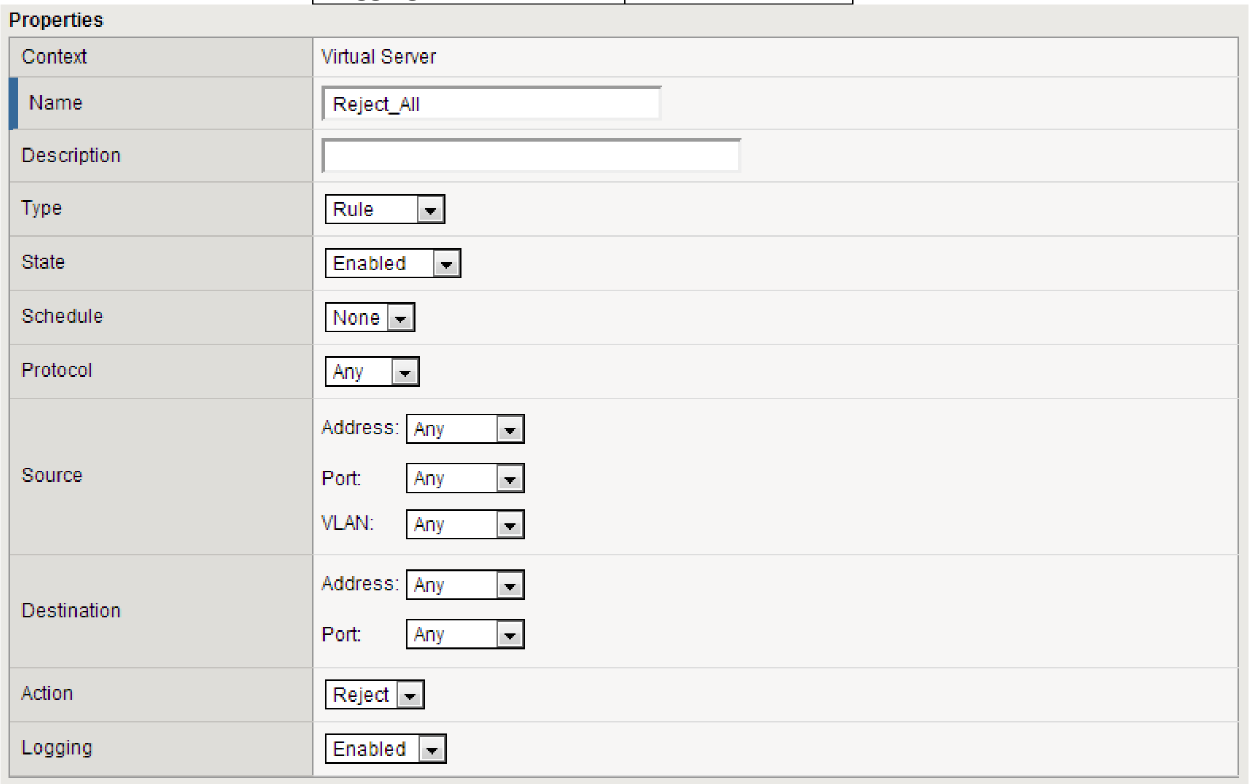
Properties

Context	Virtual Server
Name	Allow_80
Description	
Type	Rule
State	Enabled
Schedule	None
Protocol	TCP
Source	Address: Any Port: Any VLAN: Any
Destination	Address: Any Specify... Single Port... 80 Add Port: 80 Edit Delete
Action	Accept
Logging	Enabled

Figure 13: Simple Allow rule with logging

Select **Repeat** to create another rule. This next rule will logically go below the previous rule and it will be a Reject all rule. This will reject all traffic that has made it through previously listed rules. It will also log the event.

Name	Reject_All
Type	Rule
Protocol	Any
Destination Port	Any
Action	Reject
Logging	Enabled



Properties

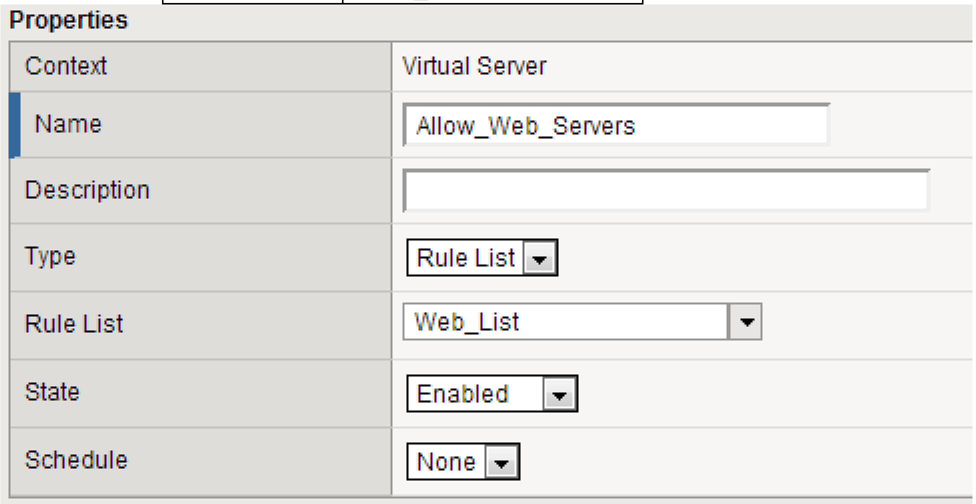
Context	Virtual Server
Name	Reject_All
Description	
Type	Rule
State	Enabled
Schedule	None
Protocol	Any
Source	Address: Any Port: Any VLAN: Any
Destination	Address: Any Port: Any
Action	Reject
Logging	Enabled

Figure 14: Reject All rule

Virtual Server Rules

Select Local Traffic → Virtual Servers. Then select the virtual server to apply the rule list to. Within the Virtual Server Security→ Policies section select **Add** to create a new rule entry. Name the rule entry **Allow_Web_Servers** and a type of **Rule_List** and select the rule list **Web_List**.

Name	Allow_Web_Servers
Type	Rule List
Rule List	Web_List

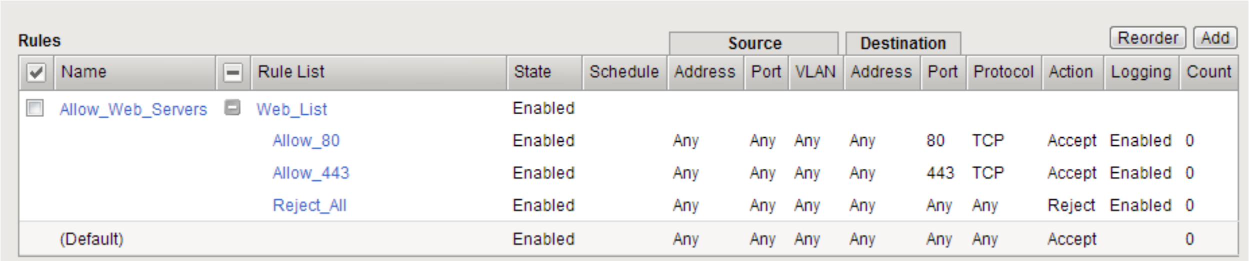


Properties

Context	Virtual Server
Name	Allow_Web_Servers
Description	
Type	Rule List
Rule List	Web_List
State	Enabled
Schedule	None

Figure 16: Virtual Server Rule

Select Finish when done. The rule listing should look as follows:



Rules

						Source			Destination					
☑	Name	⊟	Rule List	State	Schedule	Address	Port	VLAN	Address	Port	Protocol	Action	Logging	Count
□	Allow_Web_Servers	⊟	Web_List	Enabled										
			Allow_80	Enabled		Any	Any	Any	Any	80	TCP	Accept	Enabled	0
			Allow_443	Enabled		Any	Any	Any	Any	443	TCP	Accept	Enabled	0
			Reject_All	Enabled		Any	Any	Any	Any	Any	Any	Reject	Enabled	0
	(Default)			Enabled		Any	Any	Any	Any	Any	Any	Accept		0

Figure 17: http_vs Web List rule assignment

Repeat these steps for each of the Virtual Servers to be enabled for logging.

Configuring Device Management Logging

This section will explain how to configure the BIG-IP to send its device management logging information to Splunk. This will facilitate the LTM Pool reporting. The log data sent for Pool reporting is sent via standard syslog formatted log data. A log Destination, Publisher, and Filter are required.

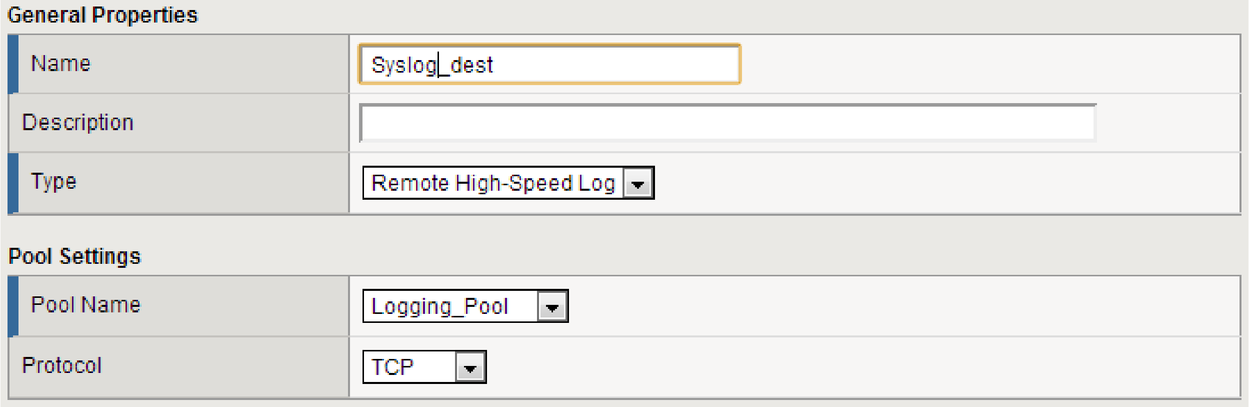
Log Destinations

At least, two log destinations need to be created. The first one will be the High Speed Logging Destination and the second one will be a Log Destination for log formatting purposes. The logs will be sent as formatted log sentences to the HSL destination.

High Speed Logging Log Destination

Select System → Logs → Configurations → Log Destinations and choose *Create*. Name the Log destination **Syslog_dest,** type is **Remote High-Speed Log**, and select the pool name to be **Logging_Pool**. Select **Repeat** to create another log destination

Name	Syslog_dest
Type	Remote High-Speed Log
Pool Name	Logging_Pool
Protocol	TCP



General Properties

Name	Syslog_dest
Description	
Type	Remote High-Speed Log

Pool Settings

Pool Name	Logging_Pool
Protocol	TCP

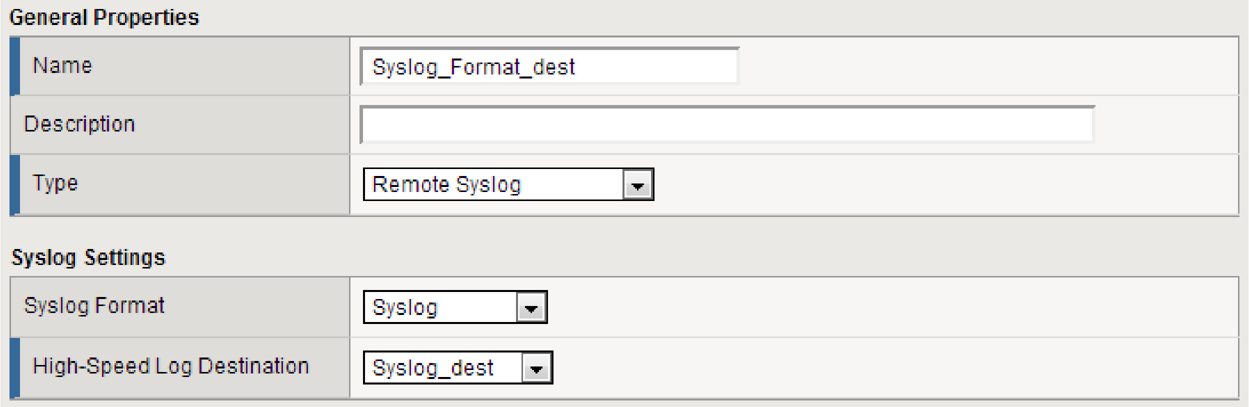
Figure 18: HSL Logging Destination

Note: The protocol value must match to one of the settings in Manager→Data Inputs on the Splunk Server. TCP is preferred as it will not truncate large log messages.

Formatted Log Destination

This log destination will be used to format the log output. The formatted log events will be sent to the HSL Log Destination previously created. Name the log destination **Syslog_Format_dest,** type is **Syslog**, and the **High Speed Log Destination** is **Syslog_dest**. This builds a layering effect for formatting and dispatching the logs.

Name	Logging_Format_dest
Type	Remote Syslog
Syslog Format	Syslog
High-Speed Log Destination	Syslog_dest



General Properties

Name	Syslog_Format_dest
Description	
Type	Remote Syslog

Syslog Settings

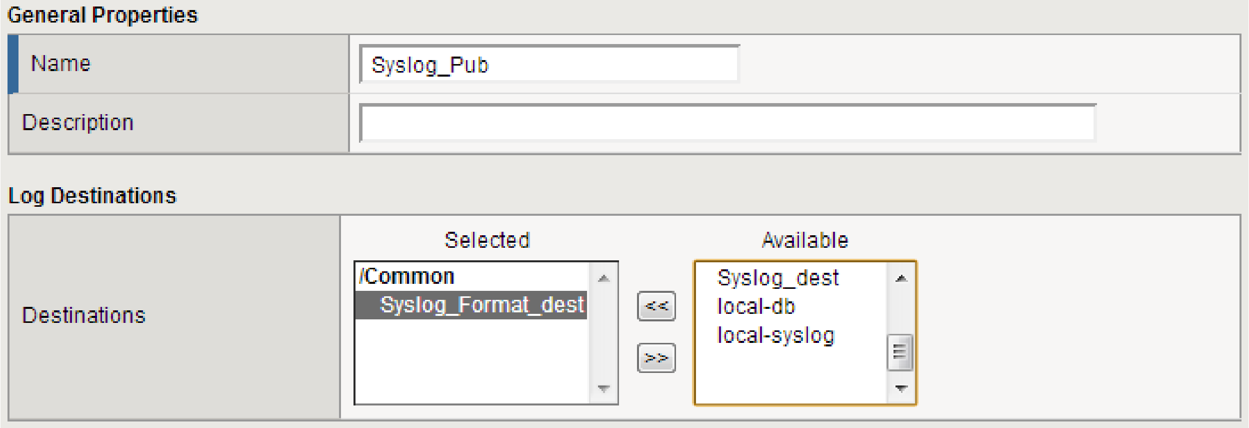
Syslog Format	Syslog
High-Speed Log Destination	Syslog_dest

Figure 19: Syslog Formatting

Log Publisher

The log publisher is a way to associate individual or multiple log destinations to a security log profile. Select System → Logs → Configurations → Log Publishers and choose *Create*. Name this publisher **Syslog_Pub** and select **Syslog_Format_dest** and move it into the selected column. Select **Finished** when done.

Name	Syslog_Pub
Destination	Syslog_Format_dest



General Properties

Name	Syslog_Pub
Description	

Log Destinations

Destinations

Selected:
/Common
Syslog_Format_dest

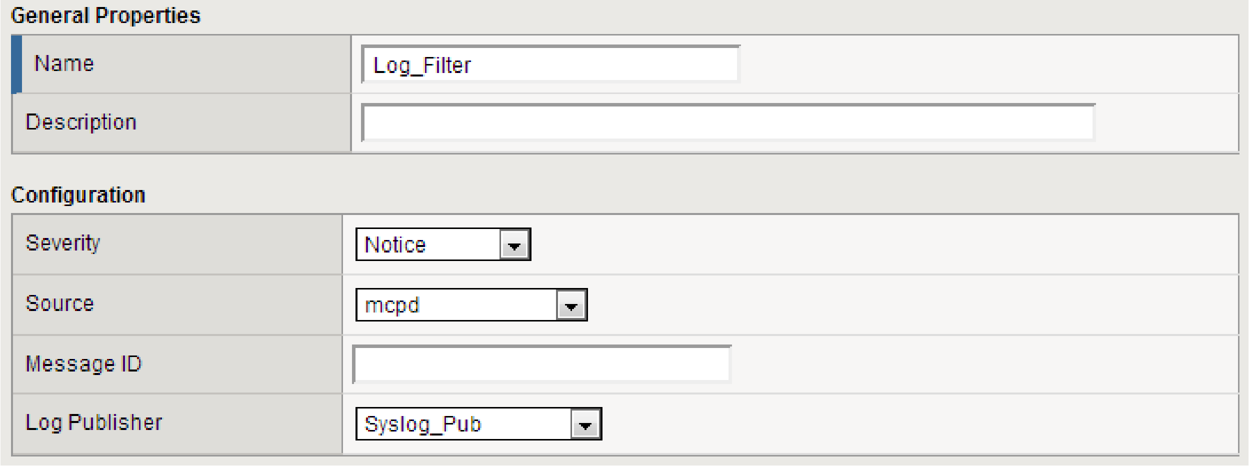
Available:
Syslog_dest
local-db
local-syslog

Figure 20: Logging Publisher

This step created a log publisher that will send Syslog formatted events to a Splunk server.

Configuring Log filtering

If more logging information is required from the BIG-IP the Log Filtering configuration can be defined to send more verbose logging information. Configure Log Filtering by selecting System → Logs → Configuration → Log Filters. Select the Create button. Enter a descriptive name **Log_Filter**, Select the severity level to be **Notice**, specify the Source to be **mcpd**, and the Logging publisher is **Syslog_Pub**.



General Properties

Name	Log_Filter
Description	

Configuration

Severity	Notice
Source	mcpd
Message ID	
Log Publisher	Syslog_Pub

Figure 21: Log Filter Configuration.

Configuring the Splunk iRule

This section will explain how to configure the Splunk provided iRule to monitor the Virtual Server in more detail. The irule is provided with the Splunk Application for F5 Networks and it is named irule.txt. The iRule needs to be added to the BIG-IP and applied to the Virtual servers that need to be monitored.

Add the iRule to the BIG-IP

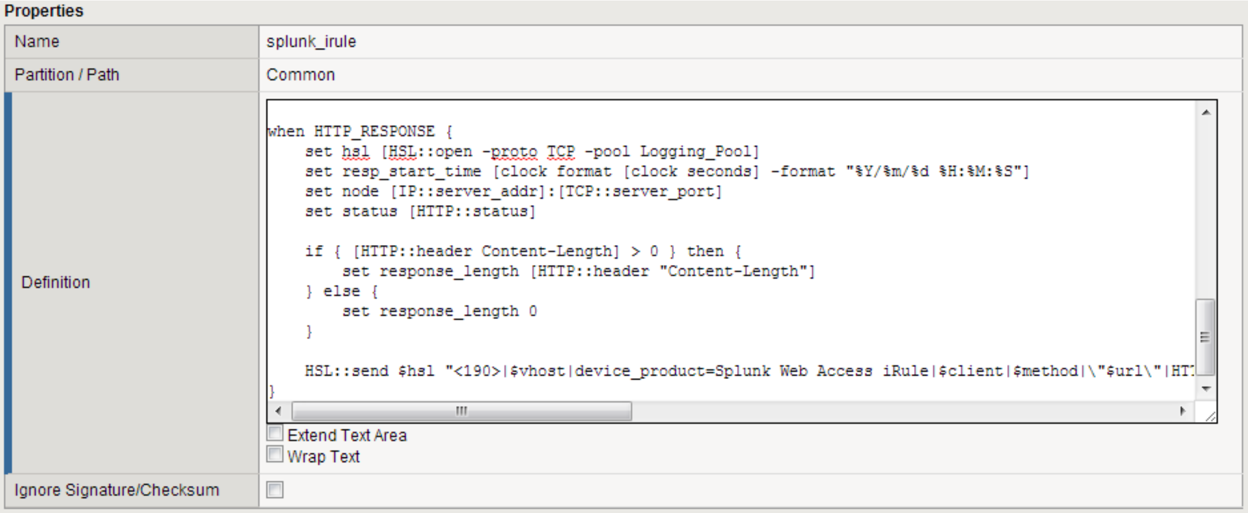
Select Local traffic → iRules and select the **Create** button. Specify a name for the iRule and paste the contents of Splunk_Web_Access_iRule.txt into the definition section. Edit the iRule and change the reference to in the line:

```
set hsl [HSL::open -proto TCP -pool pool_syslog]
```

Change **pool_syslog** to be the **Logging_Pool** from the previous section or the name of the pool containing the Splunk server.

Note: The logging protocol can be either TCP or UDP. But, it must match to the Data Input definitions in Manager → Data Inputs on the Splunk server.

Click **Finished** when complete.



Properties

Name	splunk_irule
Partition / Path	Common
Definition	see code below □ Extend Text Area □ Wrap Text
Ignore Signature/Checksum	□

```
when HTTP_RESPONSE {
    set hsl [HSL::open -proto TCP -pool Logging_Pool]
    set resp_start_time [clock format [clock seconds] -format "%Y/%m/%d %H:%M:%S"]
    set node [IP::server_addr]:[TCP::server_port]
    set status [HTTP::status]

    if { [HTTP::header Content-Length] > 0 } then {
        set response_length [HTTP::header "Content-Length"]
    } else {
        set response_length 0
    }

    HSL::send $hsl "<190>|$vhost|device_product=Splunk Web Access iRule|$client|$method|\"$url\"|HT
}
```

Figure 22: Defining the iRule definition

Apply the iRule to the Virtual server

The iRule needs to be applied to the Virtual Server. The Virtual server needs to have an HTTP Profile defined on it in order for the iRule to gather the required data.

1. Select the Virtual Server by choosing it from the list in Local Traffic → Virtual servers → Virtual Server List.
2. Within the Resources tab select **Manage** from within the iRule section.
3. Select the **splunk_irule** and move it over to the enabled column. Click **Finished** when complete.

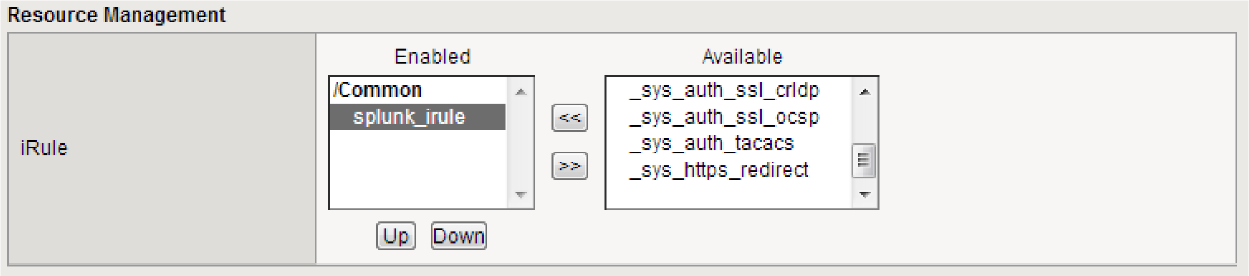


Figure 23: iRule selection

Splunk Web Access iRule

```
when CLIENT_ACCEPTED {
    set client [IP::client_addr]
}

when HTTP_REQUEST {
    set vhost [HTTP::host]:[TCP::local_port]
    set url [HTTP::uri]
    set method [HTTP::method]
    set http_version [HTTP::version]
    set user_agent [HTTP::header "User-Agent"]
    set tcp_start_time [clock clicks -milliseconds]
    set req_start_time [clock format [clock seconds] -format "%Y/%m/%d %H:%M:%S"]
    set req_elapsed_time 0
    set virtual_server [LB::server]

    if { [HTTP::header Content-Length] > 0 } then {
        set req_length [HTTP::header "Content-Length"]
        HTTP::collect $req_length
    } else {
        set req_length 4000000
    }

    if { [HTTP::header "Referer"] ne "" } then {
        set referer [HTTP::header "Referer"]
    } else {
        set referer -
    }
}

when HTTP_REQUEST_DATA {
    set req_elapsed_time [expr {[clock clicks -milliseconds] - $tcp_start_time}]
    HTTP::release
}

when HTTP_RESPONSE {
    set hsl [HSL::open -proto TCP -pool Splunk-5]

    set resp_start_time [clock format [clock seconds] -format "%Y/%m/%d %H:%M:%S"]

    set node [IP::server_addr]:[TCP::server_port]

    set status [HTTP::status]


    if { [HTTP::header Content-Length] > 0 } then {

        set response_length [HTTP::header "Content-Length"]

    } else {

        set response_length 0

    }


    HSL::send $hsl "<190>|$vhost|device_product=Splunk Web Access
iRule|$client|$method|\"$url\"|HTTP/$http_version|$user_agent|\"$referer\"|$req_start_time|$req_l
ength|$req_elapsed_time|$node|$status|$resp_start_time|$response_length|$virtual_server\r\n"

}
```

Splunk-Web-Access-iRule.txt