Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Dell SonicWALL Firewall Syslog

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Dell SonicWALL Firewall Syslog

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
01/17/2017	Added mappings and additional data to support AppFlow Reporting and SonicOS v6.2. Updated mappings for Device Custom Strings 1, 2, and 3.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	Updated Device Vendor and Device Product.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
05/15/2012	Updated installation procedure.
03/30/2012	Added OS version supported.
03/30/2011	Added version supported.
02/11/2010	Added support for FIPS Suite B and CEF File transport.

SmartConnector for Dell SonicWALL Firewall Syslog

This guide provides information for installing the SmartConnector for Dell SonicWALL Firewall Syslog and configuring a SonicWALL Firewall device to send syslog events. Sonic OS 5.8 and 6.2 are supported.

Product Overview

SonicWALL's family of Internet security appliances provide the first line of defense against Internet security threats. Designed to increase security by reducing complexity, SonicWALL Internet security appliances eliminate the cost and complexity of installing and managing separate devices and software packages for comprehensive security.

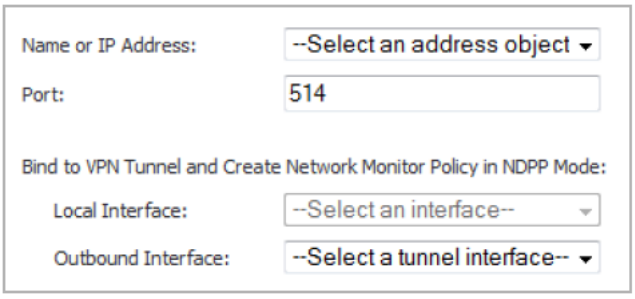
Configuration

Configuring the SonicWALL Device for SonicOS 6.2

In addition to displaying event messages in the GUI, the Dell SonicWALL security appliance can send the same messages to an external, user-configured Syslog server for viewing. The Syslog message format can be selected in Syslog Settings and the destination Syslog Servers can be specified in the table of Syslog Servers. See the Administration Guide for SonicOS 6.2 for details

Configure the SonicWALL device to send syslog events as follows:

1. Login to the SonicWALL management interface with the **admin** account.
2. Go to **Log > Syslog**.
3. In the Syslog Servers section, click **Add**.



4. Select the syslog server name or IP address from the **Name or IP Address** drop-down menu. Messages from the firewall are then sent to the servers.
5. If your syslog server does not use default port 514, type another port number in the **Port Number** field.
6. Click **OK**.
7. Click **Accept** to save all Syslog Server settings.

Configuring the SonicWALL Device for SonicOS 5.8

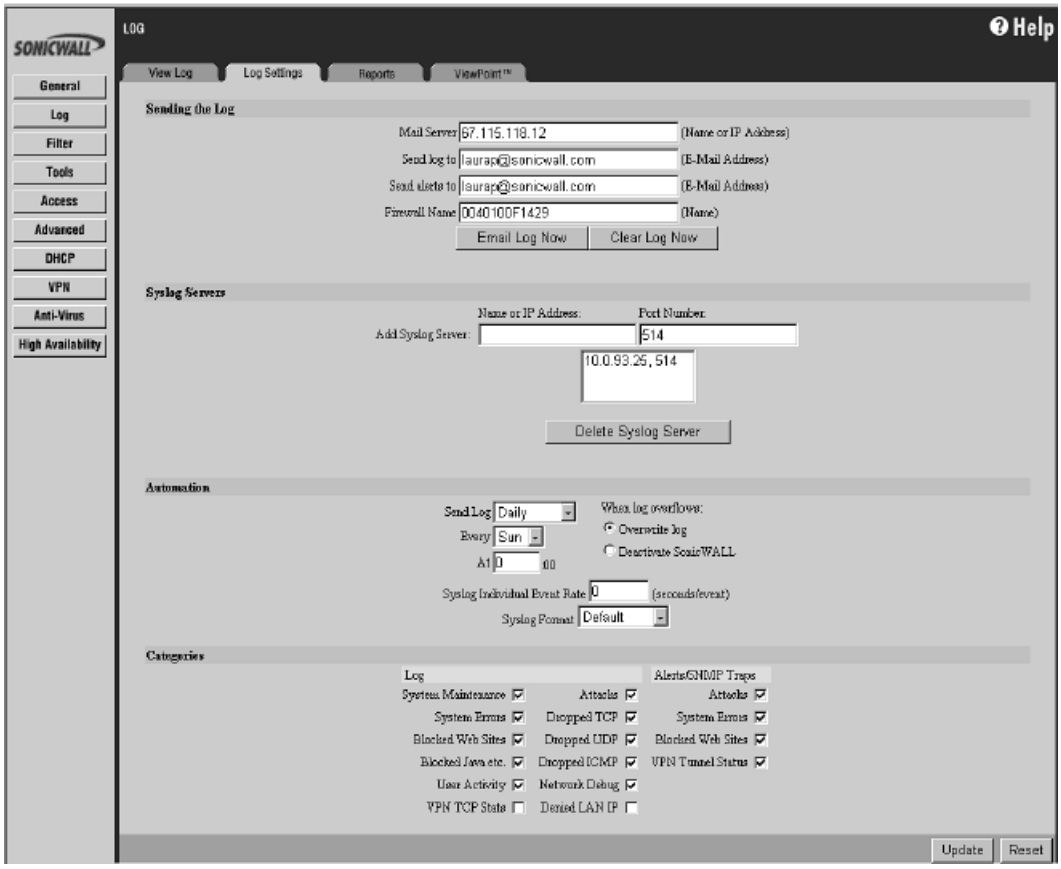
The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL Syslog support requires an external server running a syslog daemon on UDP Port 514.

Configure the SonicWALL device to send syslog events as follows:

1 Login to the SonicWALL management interface with the **admin** account.

2 Click **Log** on the left side of the browser window; then click the **Log Settings** tab.

3 In the Syslog Servers section, enter the syslog server name or IP address in the **Add Syslog Server** field. Messages from the SomnicWALL device are then sent to the servers. Up to three Syslog Server IP addresses can be added.



4 In the Automation section, select how often the log is to be sent and what to do upon overflow.

Set the **Syslog Individual Event Rate** as appropriate. This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Individual Event Rate** field, they are not written to Syslog as unique events. Instead the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The Syslog Individual Event Rate default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.

You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select Webtrends, however, you must have WebTrends software installed on your system.

5 Click on **Update** to save your settings.

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

Syslog Daemon
Syslog Pipe
Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.

Messages longer than 1024 bytes may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file (`rsyslog.conf`) can be added to write the events to either a ***file*** or a system ***pipe*** and the ArcSight SmartConnector can be configured to read the events from it. **In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon.**

The **Syslog Pipe** SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The **Syslog File** SmartConnector is similar to the Pipe SmartConnector; however, this SmartConnector monitors events written to a syslog file (such as `messages.log`) rather than to a system pipe.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the **/etc/rsyslog.conf** file, which contains specific details about which events to write to files, write to pipes, or send to another host. First, create a pipe or a file; then modify the **/etc/rsyslog.conf** file to send events to it.

For syslog pipe:

1. Create a pipe by executing the following command:

   ```
   mkfifo /var/tmp/syspipe
   ```

2. Add the following line to your **/etc/rsyslog.conf** file:

   ```
   *.debug  /var/tmp/syspipe
   ```

   or

   ```
   *.debug  |/var/tmp/syspipe
   ```

   depending on your operating system.

3. After you have modified the file, restart the syslog daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.

   On RedHat Linux, you would execute:

   ```
   service syslog restart
   ```

   On Solaris, you would execute:

   ```
   kill -HUP `cat /var/run/syslog.pid´
   ```

   This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

Syslog Daemon
Syslog Pipe
Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

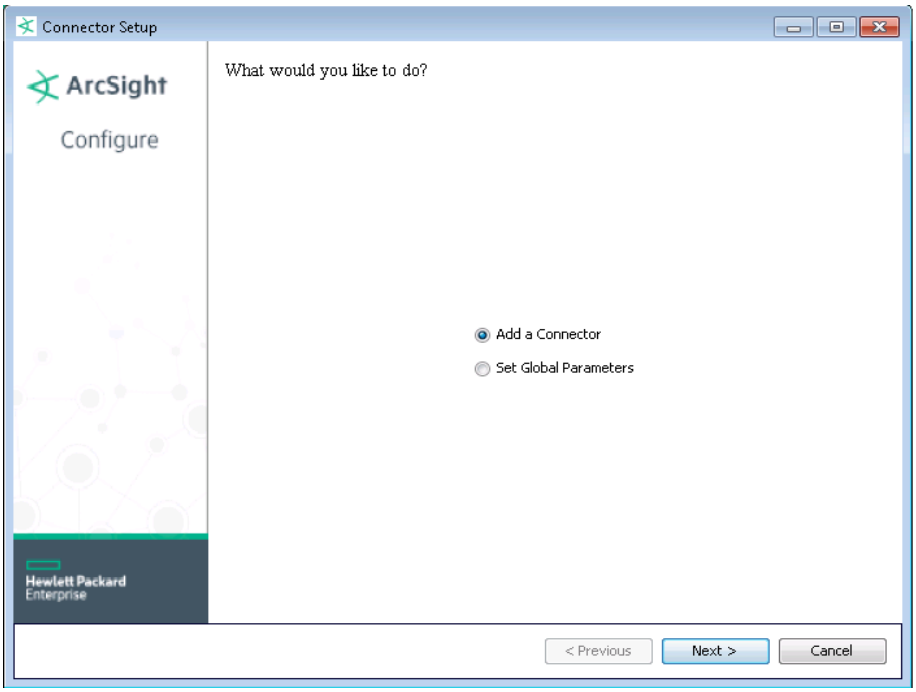
1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.

Parameter	Setting
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Syslog Daemon, File, or Pipe** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Syslog Daemon Parameters	*Network port*	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
Syslog File Parameters	*File Absolute Path Name*	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux). A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation. For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example: `filename'yyyy-MM-dd'.log;`

		For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: `filename'%d,1,99,true'.log;` Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.
	Reading Events Real Time or Batch	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
	Action Upon Reaching EOF	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
	File Extension If Rename Action	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Dell SonicWALL Firewall Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High when Device Severity = 6, 7; High when Device Severity = 4, 5; Medium when Device Severity = 3, 2; Low when Device Severity = 0, 1
Bytes In	rcvd or bytesRX
Bytes Out	sent or bytesTX
Destination Address	dadress or dst
Destination Host Name	dstname
Destination MAC Address	dstMac
Destination NT Domain	dstZone
Destination Port	dport or dst
Destination Service Name	proto
Destination Translated Address	natDst
Destination User ID	rcptTo
Destination User Name	usr
Detect Time	DetectTime
Device Action	fw_action, af_action
Device Address	WanIP
Device Custom IPv6 Address 2	natSrcV6 (Source IPv6 NAT Address)

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	dstV6 or natDstV6 (Destination IPv6 Address or Destination IPv6 NAT Address)
Device Custom Number 1	n (Event Count)
Device Custom Number 2	icmpCode (ICMP Code)
Device Custom Number 3	cdur (Connection Duration)
Device Custom String 1	rule (Rule)
Device Custom String 2	result (Result)
Device Custom String 3	vpnpolicy (Source VPN Policy)
Device Custom String 4	appName (Application Name)
Device Custom String 5	sess (Session Type)
Device Custom String 6	dur (Session Duration)
Device Event Category	One of (ipscat, spycat, gcat, f)
Device Event Class ID	m or sid
Device External ID	bid
Device Mac Address	mac
Device Outbound Interface	ai
Device Product	'SonicWALL Firewall'
Device Severity	pri, ipspri, or syprpi
Device Vendor	'Dell'
Event Name	msg
File ID	appid
File Name	arg
File Path	arg
File Type	appcat
Message	Submessage
Name	msg
Old File ID	af_polid
Old File Name	af_policy
Old File Type	af_type
Request Method	op
Request URL	arg
Source Address	saddress or src
Source Host Name	src
Source MAC Address	srcMac
Source NT Domain	srcZone
Source Port	sport or src
Source Service Name	af_service
Source Translated Address	natSrc
Source User Name	mailFrom
Transport Protocol	proto

Additional Data Mappings

Additional_Information=note	Application_Applied_Syslog=app
Application_Policy_Object_Name=af_object	Blocking_Code_Description=category
Broadcast_Packets_Received=bcastRX	Broadcast_Packets_Sent=bcastTX
Code=code	Configuration_Change_Webpage=change
Connections_In_Use=conns	Content_Object=contentObject
CPU_Utilization=cpuUtil	Destination_Interface=dst
Destination_VPN_Policy_Name=vpnpolicyDst	Device_Management_Port=pt
Firewall_Devices_With_Limited_Nodes=lic	Firewall_LAN_Zone_IP=fwlan
GMS_Message_Interval=i	HA_And_Dialup_Connection_State=dyn
ICMP_Type_Code=type	Interface_Statistics_Report=if
Message_Category=c	Number_Of_Packet_Sent=spkt
Packet_Receive=rpkt	RAM_Utilization=ramUtil
returncode=result	Rule_Category_ID=catid
SonicPoint_Radio=radio	SonicPoint_Station=station
Standby_SA_In_Use=usesstandbysa	Time_Since_Last_Change=unsynched
Unicast_Packets_Received=ucastRx	Unicast_Packets_Sent=ucastTx
URL_Of_Network_Packet_Capture_System=npcs	Well_Formed_Packets_Received=goodRxBytes
Well_Formed_Packets_Sent=goodTxBytes	