Forcepoint

Forcepoint FlexEdge Secure SD-WAN

5.10 and higher

How to receive logs from Forcepoint Sidewinder in SD-WAN Manager

[LANGUAGE NOT FOUND] A

Contents

Contents

Receiving logs from Forcepoint Sidewinder firewalls in Forcepoint FlexEdge Secure SD-WAN Manager allows you to view data from Sidewinder firewalls using the same log browsing tools as Forcepoint™ FlexEdge Secure SD-WAN engines.

Product name change

This release introduces change to product and component names. For more information about the change to product and component names, refer to the **About this Help** section in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Important

1) Some documentations, knowledge base articles, and other support information are still using the old product name.

2) There is no change in the Engine local user interface.

3) The IPS role has transitioned now from L2FW mode to L3FW mode.

Deprecated features

The following features are no longer supported:

- SSL VPN Portal.
- Web Portal User Interface is deprecated and is not available by default.

For more information on deprecated features, refer to the **About this release** section in the *FlexEdge Secure SD-WAN Manager 7.1.0 Release Notes*.

Requirements

You must use versions of the software that meet these requirements.

- SD-WAN Manager version 5.10 or higher.
- Sidewinder version 8.3.x

Configuration overview

Configuring the SMC to receive logs from Sidewinder as third-party data consists of these high-level steps.

1) Import the Logging Profile element that identifies the syslog fields to be parsed and other related elements.

2) Create a Host element that uses the Logging Profile to represent the Sidewinder firewall.

Syslog packets and what they contain

Understanding the syslog format enables you to more easily configure how Sidewinder logs are parsed.

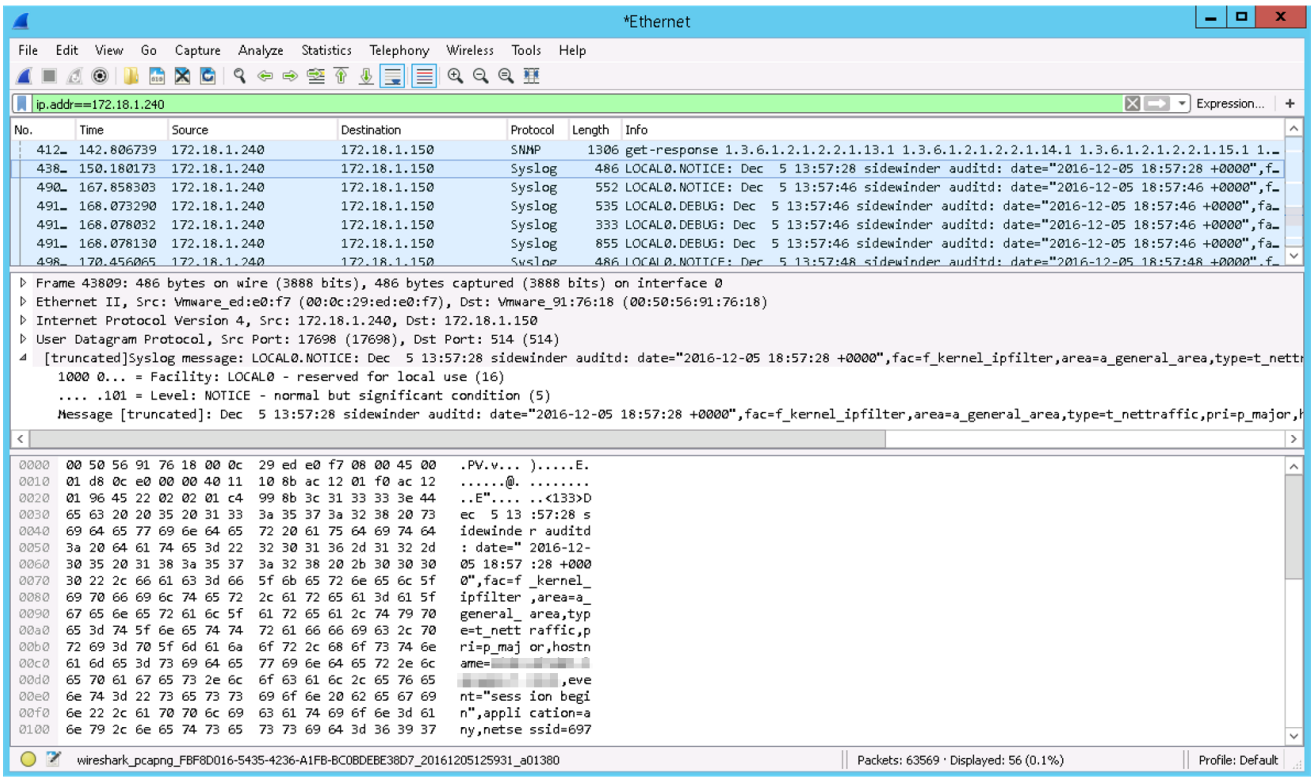
A syslog packet consists of three parts: <PRI>, HEADER, and MSG.

Parts of the syslog packet

Section	Description
<PRI>	Contains facility and priority information. The Log Server automatically extracts the Facility value from the <PRI> part and converts it to the Syslog Facility field in SMC logs. You do not define patterns for mapping this section in the Logging Profile.
HEADER	Contains a time stamp and the host name or IP address of a device. The Log Server automatically extracts the data in the HEADER part. You must define patterns for mapping this section in the Logging Profile.
MSG	Contains the text of the syslog message. In the Logging Profile, you define the mapping for parsing this part of the syslog packet.

This example shows a tcpdump view of a syslog record from a Sidewinder firewall:

Syslog record from a Sidewinder firewall



The example includes the <PRI>, HEADER, and MSG fields.

The syslog message is:

```
LOCAL0.NOTICE: Dec 5 13:57:28 sidewinder auditd: date="2016-12-05 18:57:28 +0000",
fac=f_kernel_ipfilter,area=a_general_area,type=t_nettraffic,pri=p_major,
hostname=test.vm.local,event="session begin",application=any,netsessid=6971f5845b898,
srcip=172.18.1.23,srcport=64189,srczone=internal,protocol=6,dstip=172.31.13.212,
dstport=443,dstzone=external,rule_name="any from protected to outbound",cache_hit=0,
start_time="2016-12-05 18:57:28 +0000"\n
```

In this syslog event, the value of the <PRI> field is `LOCAL0.NOTICE`.

The HEADER field is `Dec 5 13:57:28 sidewinder auditd:`

The MSG field is:

```
date="2016-12-05 18:57:28 +0000",fac=f_kernel_ipfilter,area=a_general_area,
type=t_nettraffic,pri=p_major,hostname=test.vm.local,event="session begin",
application=any,netsessid=6971f5845b898,srcip=172.18.1.23,srcport=64189,
srczone=internal,protocol=6,dstip=172.31.13.212, dstport=443,dstzone=external,
rule_name="any from protected to outbound",cache_hit=0,
start_time="2016-12-05 18:57:28 +0000"\n
```

Predefined elements for Sidewinder log reception

The .zip file contains several predefined elements for Sidewinder log reception.

A Logging Profile parses the data in a syslog message to the corresponding SMC log fields when the syslog entry is converted to an SMC log entry. The .zip file contains the **Sidewinder v8** Logging Profile element. The **Sidewinder v8** Logging Profile parses the following information from the header of the syslog packet:

- The date and time when the Sidewinder log was created
- The name of the Sidewinder firewall
- The auditing facility that generated the message

Field Resolvers convert values in incoming syslog fields to different values in SMC logs. The .zip file contains the following Field Resolver elements that are used in the Logging Profile:

- Sidewinder v8 Area Mappings
- Sidewinder v8 Event Mappings
- Sidewinder v8 Alert Type Mappings
- Sidewinder v8 URL Request Mappings
- Sidewinder v8 Facility Mappings
- Sidewinder v8 Type Mappings

Key-value pairs in the Logging Profile define how the Log Server parses each received syslog entry data. The **Sidewinder v8** Logging Profile contains the following key-value pairs:

Key-value pairs in the Sidewinder v8 Logging Profile

Key	Field
hostname	Sender address
srcip	Src Addr
srcport	Src Port
dstip	Dst Addr
sdtport	Destination port
bytes_written_to_client	Bytes Rcvd
bytes_written_to_server	Bytes Sent
application	Application Detail
app_categories	Resource
protocol	IP Protocol
area	Sidewinder v8 Area Mappings
event	Sidewinder v8 Event Mappings
alert_type	Sidewinder v8 Alert Type Mappings
request_command	Sidewinder v8 URL Request Mappings
fac	Sidewinder v8 Facility Mappings

Key	Field
type	Sidewinder v8 Type Mappings

Import elements for Sidewinder log reception

Import the .zip file that contains the predefined elements for Sidewinder log reception.

The .zip file is available in Knowledge Base article 12192.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) Save the .zip file in a location that is accessible from the computer where you use the Management Client.
2) In the Management Client, select **Menu** > **File** > **Import** > **Import Elements**.
3) Select the .zip file, then click **Import**.
4) When the import is finished, click **Close**.

Create a Host element to represent the Sidewinder firewall

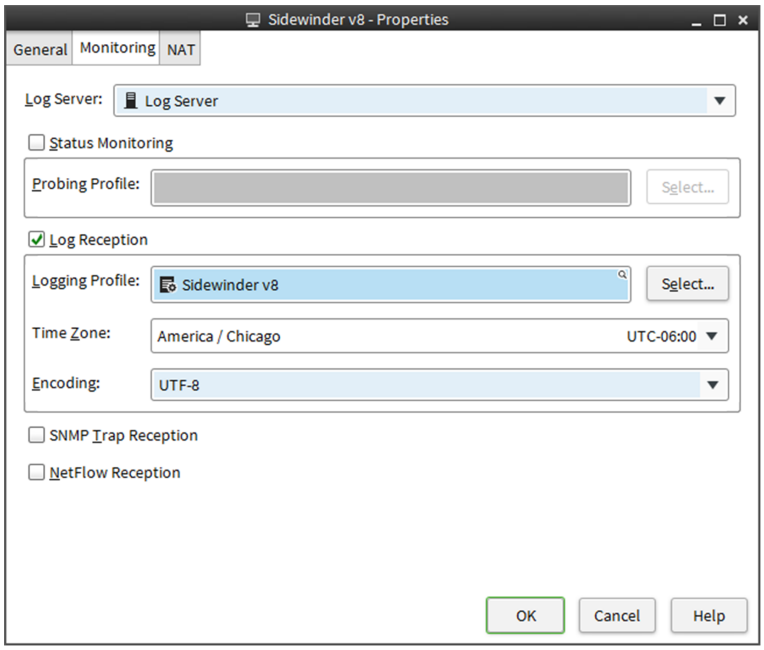
The Host element represents the Sidewinder firewall that sends syslog data to the SMC and specifies the Logging Profile that is used for the Sidewinder logs.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) Select **Configuration**, then browse to **Network Elements**.
2) Right-click **Hosts**, then select **New Host**.
3) In the **Name** field, enter a unique name.

4) In the **IPv4 Address** field, enter the IPv4 address of the Sidewinder firewall.



5) On the **Monitoring** tab, select the Log Server that receives the syslog data from the **Log Server** drop-down list.

6) To enable log reception, select **Log Reception**.

7) Select the Logging Profile for the Host element.
   a) Next to the **Logging Profile** field, click **Select**.

   b) Select the **Sidewinder v8** Logging Profile element, then click **Select**.

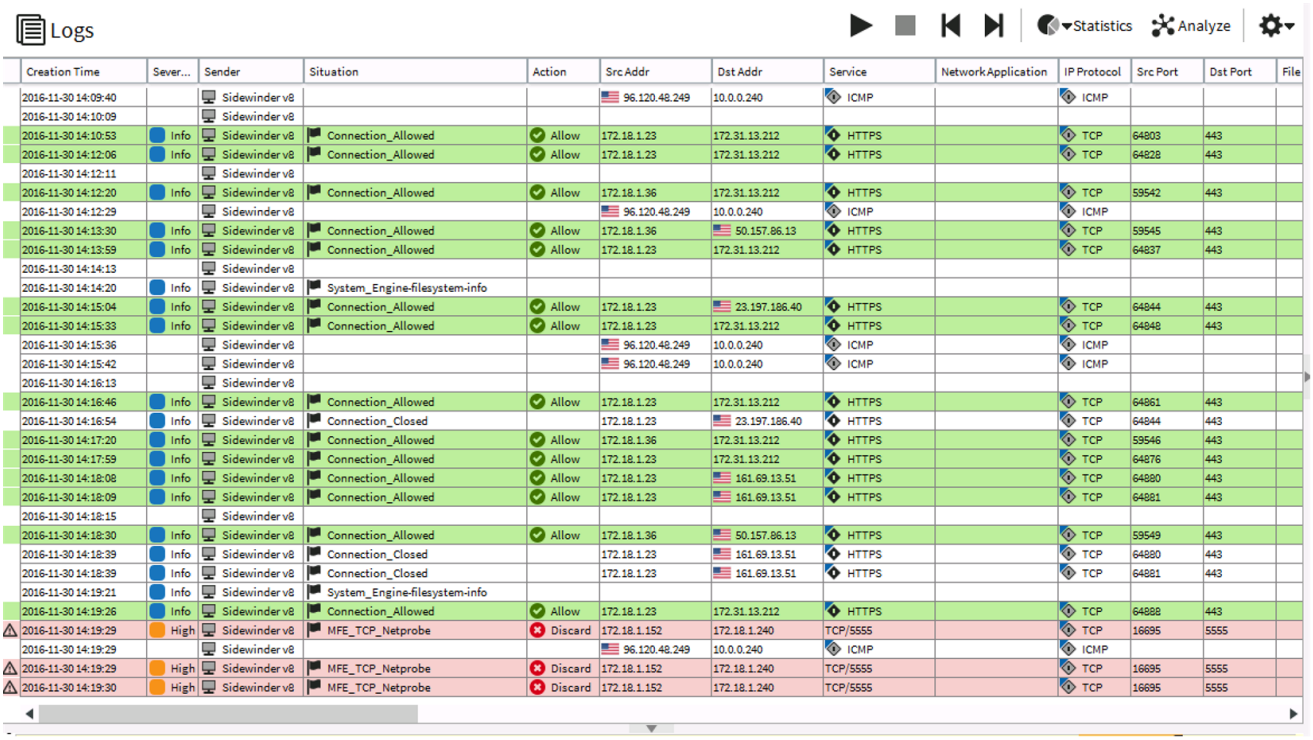
8) From the **Time Zone** drop-down list, select the time zone in which the Sidewinder firewall is located.

9) Click **OK**.

Result

You can now view logs from the Sidewinder firewall in the **Logs** view of the Management Client.

Sidewinder logs in the Logs view of the Management Client



Creation Time	Sever...	Sender	Situation	Action	Src Addr	Dst Addr	Service	Network Application	IP Protocol	Src Port	Dst Port	File
2016-11-30 14:09:40		Sidewinder v8			96.120.48.249	10.0.0.240	ICMP		ICMP			
2016-11-30 14:10:09		Sidewinder v8										
2016-11-30 14:10:53	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64803	443	
2016-11-30 14:12:06	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64828	443	
2016-11-30 14:12:11		Sidewinder v8										
2016-11-30 14:12:20	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.36	172.31.13.212	HTTPS		TCP	59542	443	
2016-11-30 14:12:29		Sidewinder v8			96.120.48.249	10.0.0.240	ICMP		ICMP			
2016-11-30 14:13:30	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.36	50.157.86.13	HTTPS		TCP	59545	443	
2016-11-30 14:13:59	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64837	443	
2016-11-30 14:14:13		Sidewinder v8										
2016-11-30 14:14:20	Info	Sidewinder v8	System_Engine-filesystem-info									
2016-11-30 14:15:04	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	23.197.186.40	HTTPS		TCP	64844	443	
2016-11-30 14:15:33	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64848	443	
2016-11-30 14:15:36		Sidewinder v8			96.120.48.249	10.0.0.240	ICMP		ICMP			
2016-11-30 14:15:42		Sidewinder v8			96.120.48.249	10.0.0.240	ICMP		ICMP			
2016-11-30 14:16:13		Sidewinder v8										
2016-11-30 14:16:46	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64861	443	
2016-11-30 14:16:54	Info	Sidewinder v8	Connection_Closed		172.18.1.23	23.197.186.40	HTTPS		TCP	64844	443	
2016-11-30 14:17:20	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.36	172.31.13.212	HTTPS		TCP	59546	443	
2016-11-30 14:17:59	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64876	443	
2016-11-30 14:18:08	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	161.69.13.51	HTTPS		TCP	64880	443	
2016-11-30 14:18:09	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	161.69.13.51	HTTPS		TCP	64881	443	
2016-11-30 14:18:15		Sidewinder v8										
2016-11-30 14:18:30	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.36	50.157.86.13	HTTPS		TCP	59549	443	
2016-11-30 14:18:39	Info	Sidewinder v8	Connection_Closed		172.18.1.23	161.69.13.51	HTTPS		TCP	64880	443	
2016-11-30 14:18:39	Info	Sidewinder v8	Connection_Closed		172.18.1.23	161.69.13.51	HTTPS		TCP	64881	443	
2016-11-30 14:19:21	Info	Sidewinder v8	System_Engine-filesystem-info									
2016-11-30 14:19:26	Info	Sidewinder v8	Connection_Allowed	Allow	172.18.1.23	172.31.13.212	HTTPS		TCP	64888	443	
2016-11-30 14:19:29	High	Sidewinder v8	MFE_TCP_Netprobe	Discard	172.18.1.152	172.18.1.240	TCP/5555		TCP	16695	5555	
2016-11-30 14:19:29		Sidewinder v8			96.120.48.249	10.0.0.240	ICMP		ICMP			
2016-11-30 14:19:29	High	Sidewinder v8	MFE_TCP_Netprobe	Discard	172.18.1.152	172.18.1.240	TCP/5555		TCP	16695	5555	
2016-11-30 14:19:30	High	Sidewinder v8	MFE_TCP_Netprobe	Discard	172.18.1.152	172.18.1.240	TCP/5555		TCP	16695	5555	

Published 18 January 2024