



**Forcepoint
FlexEdge
Secure
SD-
WAN**

5.10 and higher

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

Contents

1 How to receive logs from Forcepoint Sidewinder in SD-WAN Manager.....	4
Requirements.....	4
Configuration overview.....	5
Syslog packets and what they contain.....	5
Predefined elements for Sidewinder log reception.....	7
Import elements for Sidewinder log reception.....	8
Create a Host element to represent the Sidewinder firewall.....	8

Contents

- Requirements
- Configuration overview
- Syslog packets and what they contain
- Predefined elements for Sidewinder log reception
- Import elements for Sidewinder log reception
- Create a Host element to represent the Sidewinder firewall

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 screenshot shows a Wireshark capture of a Syslog message. The packet list pane shows a Syslog packet (No. 491) with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
412	142.806739	172.18.1.240	172.18.1.150	SNMP	1306	get-response 1.3.6.1.2.1.2.2.1.13.1 1.3.6.1.2.1.2.2.1.14.1 1.3.6.1.2.1.2.2.1.15.1 1...
438	150.180173	172.18.1.240	172.18.1.150	Syslog	486	LOCAL0.NOTICE: Dec 5 13:57:28 sidewinder auditd: date="2016-12-05 18:57:28 +0000",fac=f...
490	167.858303	172.18.1.240	172.18.1.150	Syslog	552	LOCAL0.NOTICE: Dec 5 13:57:46 sidewinder auditd: date="2016-12-05 18:57:46 +0000",fac=f...
491	168.073290	172.18.1.240	172.18.1.150	Syslog	535	LOCAL0.DEBUG: Dec 5 13:57:46 sidewinder auditd: date="2016-12-05 18:57:46 +0000",fac=f...
491	168.078032	172.18.1.240	172.18.1.150	Syslog	333	LOCAL0.DEBUG: Dec 5 13:57:46 sidewinder auditd: date="2016-12-05 18:57:46 +0000",fac=f...
491	168.078130	172.18.1.240	172.18.1.150	Syslog	855	LOCAL0.DEBUG: Dec 5 13:57:46 sidewinder auditd: date="2016-12-05 18:57:46 +0000",fac=f...
498	170.456065	172.18.1.240	172.18.1.150	Syslog	486	LOCAL0.NOTICE: Dec 5 13:57:48 sidewinder auditd: date="2016-12-05 18:57:48 +0000",fac=f...

The details pane for the selected Syslog packet (No. 491) shows the following structure:

- Frame 43809: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface 0
- Ethernet II, Src: Vmware_ed:e0:f7 (00:0c:29:ed:e0:f7), Dst: Vmware_91:76:18 (00:50:56:91:76:18)
- Internet Protocol Version 4, Src: 172.18.1.240, Dst: 172.18.1.150
- User Datagram Protocol, Src Port: 17698 (17698), Dst Port: 514 (514)
- [truncated] Syslog message: 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.v...

The raw packet bytes are shown at the bottom of the details pane, with the Syslog message content starting at offset 0x0000:

```

0000 00 50 56 91 76 18 00 0c 29 ed e0 f7 08 00 45 00 .PV.v... ).....E.
0010 01 d8 0c e0 00 00 40 11 10 8b ac 12 01 f0 ac 12 .....@. ....
0020 01 96 45 22 02 02 01 c4 99 8b 3c 31 33 33 3e 44 ..E"....<133>D
0030 65 63 20 20 35 20 31 33 3a 35 37 3a 32 38 20 73 ec 5 13 :57:28 s
0040 69 64 65 77 69 6e 64 65 72 20 61 75 64 69 74 64 idewinde r auditd
0050 3a 20 64 61 74 65 3d 22 32 30 31 36 2d 31 32 2d : date=" 2016-12-
0060 30 35 20 31 38 3a 35 37 3a 32 38 20 2b 30 30 30 05 18:57 :28 +000
0070 30 22 2c 66 61 63 3d 66 5f 6b 65 72 6e 65 6c 5f 0",fac=f _kernel_
0080 69 70 66 69 6c 74 65 72 2c 61 72 65 61 3d 61 5f ipfilter ,area=a
0090 67 65 6e 65 72 61 6c 5f 61 72 65 61 2c 74 79 70 general _area,typ
00a0 65 3d 74 5f 6e 65 74 74 72 61 66 66 69 63 2c 70 e=t_nettraff ic,p
00b0 72 69 3d 70 5f 6d 61 6a 6f 72 2c 68 6f 73 74 6e ri=p_maj or,hostn
00c0 61 6d 65 3d 73 69 64 65 77 69 6e 64 65 72 2e 6c ame=
00d0 65 70 61 67 65 73 2e 6c 6f 63 61 6c 2c 65 76 65 ,eve
00e0 6e 74 3d 22 73 65 73 73 69 6f 6e 20 62 65 67 69 nt="sess ion begi
00f0 6e 22 2c 61 70 70 6c 69 63 61 74 69 6f 6e 3d 61 n",appli cation=a
0100 6e 79 2c 6e 65 74 73 65 73 73 69 64 3d 36 39 37 ny,netse ssid=697
  
```

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.v.m.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.v.m.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**.

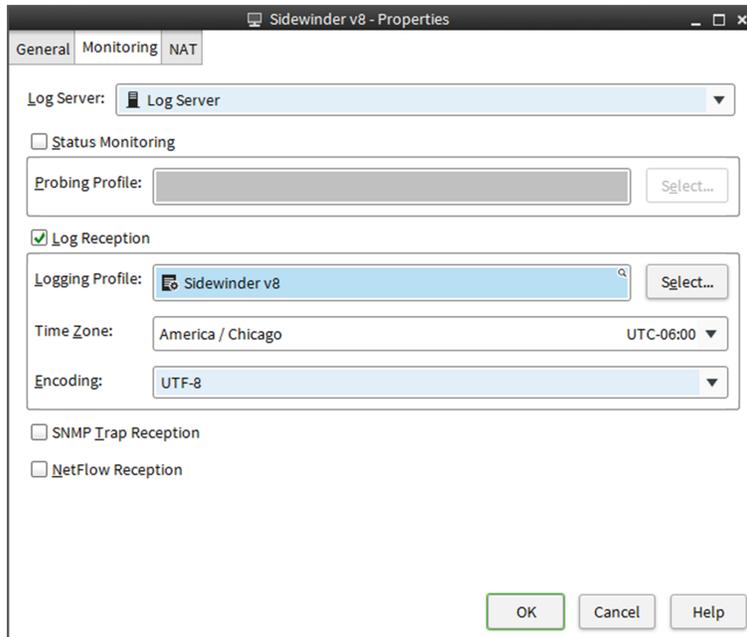
Create a Host element to represent the Sidewinder firewall

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

Logs ▶ ◻ ◀ ▶ | 📊 Statistics 🔍 Analyze ⚙️

Creation Time	Sever...	Sender	Situation	Action	Src Addr	Dst Addr	Service	NetworkApplication	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										
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										
2016-11-30 14:15:42		Sidewinder v8										
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	64882	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	High	Sidewinder v8	MFE_TCP_Netprobe	Discard	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	

