



Configuration examples for the D-Link NetDefend Firewall series



Setting up logging and reporting



This configuration example is based on the following setup:



Step 1. Log into the firewall. The default access to LAN is via <u>https://192.168.10.1</u>. Default username is "admin" and password is "admin". Set your firewall's WAN settings as per Internet provider requirements.

Step 2. Enable logging for the desired IP rules. For monitoring outgoing traffic it is important to enable logging in the main NAT rule: Go to Policies > Main IP Rules > lan_to_wan > edit the "allow_standard" rule. Select "Enable logging".

Select if logging should be enabled and what severity to use.	General	Log Settings	NAT	SAT	Multiplex SAT	SLB SAT	SLB Monitor
Log with severity: Name Default Debug Info Notice Warning Error Critical Alert	Select if loggin	g should be enable ging	d and wha	t severity t	o use.		
Default Debug Info Notice Warning Error Critical Alert	Log with severity:	Info Name	Y				
Notice Warning Error Critical Alert		Debug					
Error Critical Alert		Notice					
Alert		Error					
		Alert					



Step 3. Go to Objects > Address Book. Add new IP4 address entry – specify your Syslog/Reporting server IP. Go to System > Device > Log and Event Receivers. Add a new Syslog Receiver which points to your server IP address. Click on Severity Filter tab. Specify the event that you want to be logged.

Facility:

Port:

local0

514

	Status Device	System Advanced Setti	Objects	Networ	k Policies	
Device Date and Time DNS Remote Management	Log ar	nd Event F	Receivers	re to receive lo	g and event informat	
Log and Event Receivers ▼ Monitoring Hardware Monitoring Settings	Syslog F SMTP EV SNMP2c	Receiver vent Receiver Event Receiver	A Sys	log Receive	eceiver	eive log
▼ Users Local User Databases	,			eneral	Severity Fil	ter
			Nam Rout	e: iing Table: ddress:	SysLog	y y

Syslog Receiver					
A Syslog receiver	A Syslog receiver is used to receive log events from the system				
General	Severity Filter	Message Exceptions			
Log Severity	Sel	ected			
(7) Debug + Include	(0 (1 (2 (3) (4 (5) (6)) Emergency) Alert) Critical) Error) Warning) Notice) Info			

Step 4. Download Splunk Enterprise from <u>www.splunk.com</u>. After installing Splunk add your firewall as new "Data input".



Select data input type as UDP on port 514.

splunk> Apps ~	Messages ~	Settings \sim Activity \sim Help \sim
Data inputs		
Туре	Inputs	Actions
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	1	Add new
Files & directories Upload a file, index a local file, or monitor an entire directory	5	Add new
Source UDP port * 514 Source name ove <i>If set, overrides the</i> Source type Set sourcetype field Set sourcetype * From list Select source typ syslog	rride • default source value for your UDP en d for all events from this source. e from list *	try (host:port).

Splunk server will start collecting logs from your firewall and continuously analyse them, identifying "Interesting Fields" like destination IP, source IP, firewall action, type of application or web site being opened.

splunk>	App: Se	arch & Repo	orting ~		Administrator \sim Messages \sim Settings \sim Activity \sim Help \sim		
Search F	Pivot	Reports	Alerts	Dashboards	Search & Reporting		
Q New	Q New Search Save As ~ Close						
host="192	. 168 . 21	.1"			Date time range ~ Q		
✓ 20,322 ever	nts (10/10	0/14 7:00:00	.000 AM t	0 10/10/14 11:00:00.0	00 AM) Job ∨ II 🔳 → 🛓 👼 📍 Smart Mode ∨		
Events (20,32	2)	Statistics	\ v	sualization			
Format Timel	ine 🗸	– Zoom O	ut +Z	oom to Selection X	Deselect 1 minute per column		
				the transfer	a set of the the		
			litere manit	. II. an Addubili	addina addina tha ann an ann ann ann an ann an ann an an		
				List 🗸 🛛 Format 🗸	20 Per Page → < < Prev 1 2 3 4 5 6 7 8 9 … Next >		
< Hide Fields		:≡ All Fiel	lds	<i>i</i> Time	Event		
Selected Field	Selected Fields			> 10/10/14 11:09:41.000 AM	Oct 10 10:09:41 192.168.21.1 [2014-10-10 11:11:00] FW: RULE: prio=3 id=06000051 rev=1 event=ruleset_drop_packet action=drop rule=Default_Access_Rule recvif=lan srcip=192.16 8.0.148 destip=239.255.255.100 ipproto=IGMP ipdatalen=72 type=V1_MEMBER_REPORT maxresp =0 groupaddr=239.255.255.100		
a application	17				action = drop destip = 239.255.255.100 host = 192.168.21.1 srcip = 192.168.0.148		
a destip 100 # destport 8 a host 1	a destip 100+ > 10/10/14 Oct 10 10:09:19 192.168.21.1 [2014-10-10 11:10:38] FW: RULE: prio=3 id=06000051 re # destport 81 11:09:19.000 AM event=ruleset_drop_packet action=drop rule=Default_Rule recvif=wan srcip=184.28.21 a host 1 0 destip=192.168.20.88 ipproto=TCP ipdatalen=20 srcport=80 destport=9085 ack=1 fin				Oct 10 10:09:19 192.168.21.1 [2014-10-10 11:10:38] FW: RULE: prio=3 id=06000051 rev=1 event=ruleset_drop_packet action=drop rule=Default_Rule recvif=wan srcip=184.28.21.11 0 destip=192.168.20.88 ipproto=TCP ipdatalen=20 srcport=80 destport=9085 ack=1 fin=1		
a srcip 39					action = drop destip = 192.168.20.88 destport = 9085 host = 192.168.21.1 srcip = 184.28.21.110		
Interesting Field	elds			> 10/10/14 11:09:18.000 AM	Oct 10 10:09:18 192.168.21.1 [2014-10-10 11:10:37] FW: RULE: prio=3 id=06000051 rev=1 event=ruleset_drop_packet action=drop rule=Default_Rule recvif=wan srcip=184.28.21.11 0 destip=192.168.20.88 ipproto=TCP ipdatalen=20 srcport=80 destport=9085 ack=1 fin=1		
a conndestif	1				action = drop destip = 192.168.20.88 destport = 9085 host = 192.168.21.1 srcip = 184.28.21.110		
a conndestip # conndestpo	a conndestip 100+ # conndestport 91			> 10/10/14 11:09:18.000 AM	Oct 10 10:09:18 192.168.21.1 [2014-10-10 11:10:37] FW: RULE: prio=3 id=06000051 rev=1 event=ruleset_drop_packet action=drop rule=Default_Rule recvif=wan srcip=184.28.21.11		
	_						



For each of the fields you can check the number of hits, top 10 values, etc.

Events (30,021) Statistics	Visualization					
Format Timeline ~ - Zoom Out	application			×		
	17 Values, 3.504% of events Selected			Yes No		
< Hide Fields i≡ All Fields	Reports Top values Events with this field	Top values by time	Rare values			
Salected Fields	Top 10 Values	Count	%			
a action 15	http	489	46.483%			
a application 17	steam	175	16.635%			
a destip 100+	tcp	74	7.034%			
# destport 94	aooale	73	6.939%	· · · · · · · · ·		
a host 1	vaboo groups	64	6.084%			
a srcip 54	dae	46	4 2729/			
Interesting Fields	ans	40	4.373%	. <u>.</u>		
a conn 2	yahoo	28	2.662%			
a conndestif 1	youtube	28	2.662%	<u> </u>		
a conndestip 100+	akamai	18	1.711%			
# conndestport 100	gstatic	16	1.521%			
a connipproto 2	connipproto 2					
a connewdestip 100+	$\sigma = \sigma = \sigma = \sigma = 102.162.21.1$					
# commewdestport 100	> 10/10/14	Oct 10 10:04:01 102 152.100.21.				

By clicking on each value you can then drill down to top source IPs, destination IPs and so on. E.g. top 10 clients on LAN for application "YouTube" (if you have Application Control license activated):

Events (20,322)	Statistics	srcip			\times
Format Timeline 🗸	- Zoom Out	39 Values, 29.648% of ev	vents	Selecte	d Yes No
		Reports Top values Events with this field	Top values by time	Rare value	5
< Hide Fields	:≡ All Fields	Top 10 Values	Count	%	
		192.168.21.122	1,647	27.336%	
Selected Fields	Selected Fields	192.168.21.117	1,298	21.544%	
a action 15		192.168.20.88	344	5.71%	1
a destip 100+		192.168.21.111	320	5.311%	
# destport 81		192.168.21.103	305	5.062%	I
a host 1		0.0.0.0	215	3.568%	I
a srcip 39		192.168.21.114	207	3.436%	
Interesting Fields a conn 2 a conndestif 1 a conndestip 100+		202.126.168.253	196	3.253%	
		192.168.21.116	189	3.137%	
		192.168.0.249	154	2.556%	



If your firewall has Web Content Filtering license you will be able to see web browsing categories:

Events (30,402) Statistics	categories		\times
Format Timeline → Zoom Out	12 Values, 1.23% of events	Selected Yes No	
	Reports Top values Top values by time Events with this field		Rare values
< Hide Fields ∷≣ All Fields	Top 10 Values	Count	%
	Business oriented	206	55.08%
Selected Fields	Search sites	60	16.043%
a application 29	Shopping	30	8.021%
a categories 12	Advertising	26	6.952%
a destip 100+	Drugs/Alcohol	17	4.545%
# destport 100+	Chatrooms	14	3.743%
a srcip 54	Chatrooms, Computing/IT	10	2.674%
a url 100+	Entertainment, Chatrooms	3	0.802%
	Computing/IT	3	0.802%

The URLs are also logged:

Events (30,402) Statistics	url	\boxtimes			
Format Timeline 🗸 🦳 — Zoom Out	>100 Values, 1.233% of events	Selected Yes No			
	Reports Top values Top values by time Events with this field	Rare values			
< Hide Fields ∷≣ All Fields	Top 10 Values				
	http://www.milandirect.com.au/catalog/product/view/id/12296%3Fgclid%3D*				
Selected Fields	www.milandirect.com.au/orderpopup/index/show/				
a action 19	platform.twitter.com/widgets/tweet_button.2df3b13213b70e6d91180bf64c17db20.en.html				
a application 29	www.jimbeam.com.au/sites/default/files/heroes/Mila and Fred_0.jpg				
a categories 12	www.shoppingsquare.com.au/images/products/58478	B_thumb.jpg			
a destip 100+	http%3A%2F%2Fwww.thespiritsbusiness.com%2F2014%2F10%2Fjim-beam-moves-into-cinnamon-flavoured				
a host 1	www.google-analytics.com/ga.js				
a srcip 54	www.jimbeam.com.au/				
a url 100+	www.milandirect.com.au/media/catalog/product/cach -size-3-white-base.jpg	ne/2/thumbnail/68x/9df78eab33525d08d6e5fb8d271			
Interesting Fields a conn 2	www.milandirect.com.au/newsletter/subscriber/check				

Splunk allows you to create customizable dashboards and reports. You can view your firewall activity live or analyse the data logged earlier. The free version of Slunk has limitation on the size of the logs you can keep (500MB), old data is purged automatically.

