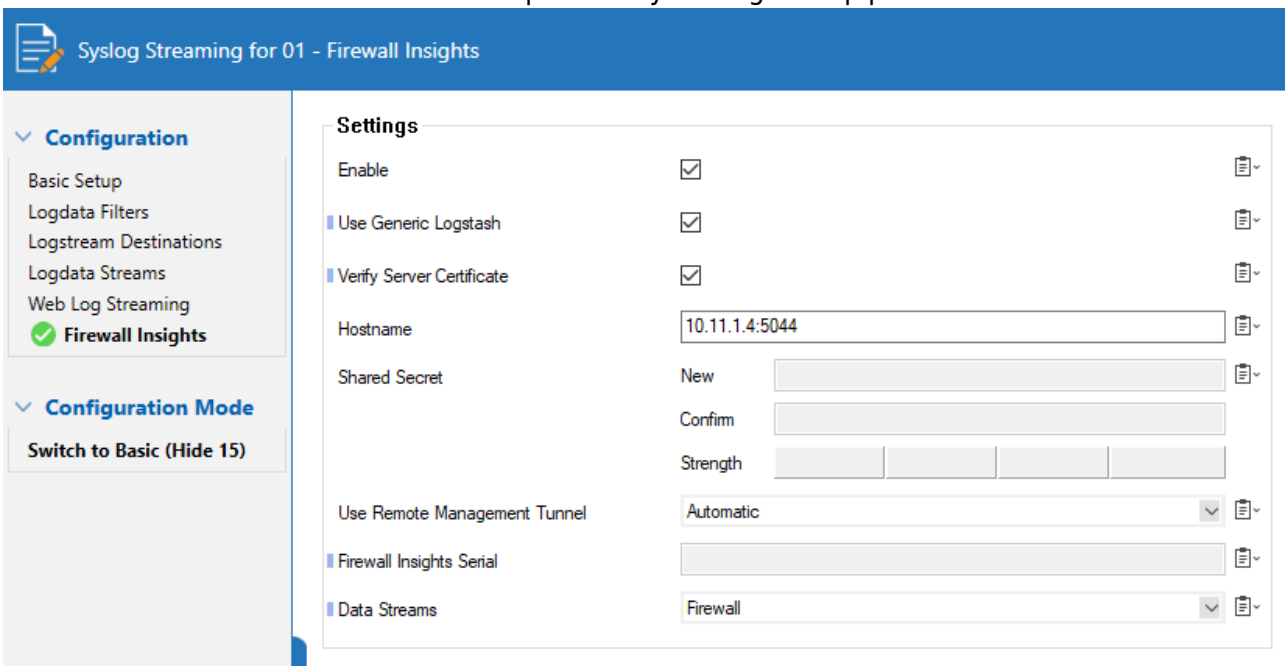
How to Enable Filebeat Stream to a Logstash Pipeline

https://campus.barracuda.com/doc/96025953/

The Barracuda CloudGen Firewall allows you to stream event logs from Firewall Insights to a Logstash server, which provides information on firewall activity, threat logs, and information related to network, version, and location of managed firewall units. To receive Filebeat data streams through the Logstash pipeline, enable debugging and syslog streaming, and configure the firewall to send data to a Logstash server. Streaming logs from Firewall Insights through the Logstash pipeline requires a Firewall Insights license.

Enable Stream to Logstash Pipeline

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the **Configuration** menu on the left, select **Firewall Insights**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced**.
4. Click **Lock**.
5. **Enable** the service and select **Use Generic Logstash**.
6. Enter the IP address or host name that points to your Logstash pipeline.



7. Click **Send Changes** and **Activate**.

Default Logstash Configuration File

To receive and forward all events through your Logstash pipeline, use the following

configuration. Make sure to use the PKSCS8 certificate key.

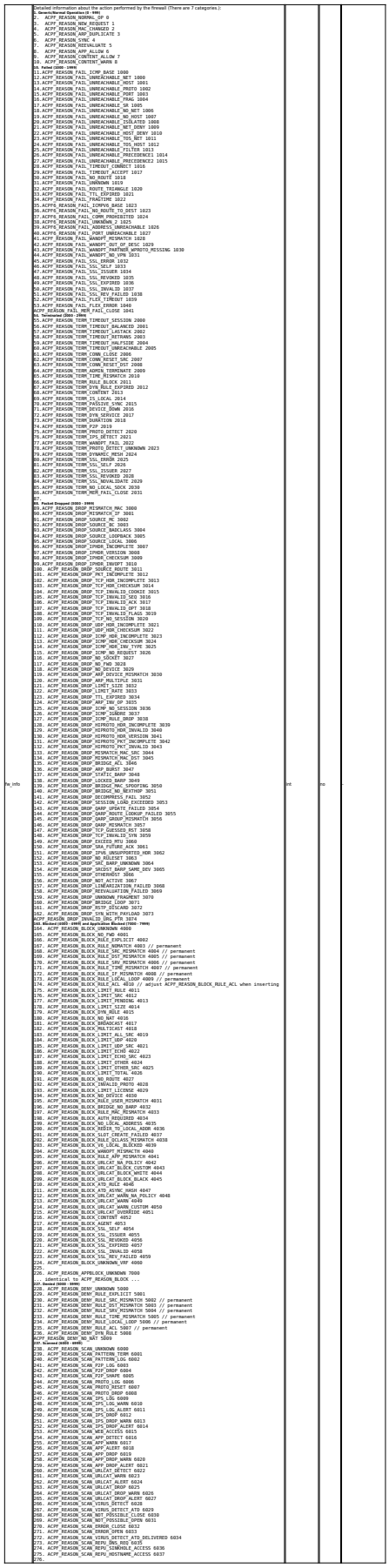
```
File beat Conifg: /log/logstash-cgf.conf
<code>
input {
  beats {
    port => 5044
    ssl => true
    ssl_certificate => "/etc/ssl/cert.pem"
    ssl_key => "/etc/ssl/key.pkcs8"
  }
}
filter {
  json {
    source => "message"
    target => "message"
  }
}
output {
  stdout { codec => rubydebug }
}
</code>
```

Firewall Activity Messages

(for Firewall Insights, type = ngfw-act)

JSON Fields

Field Name	Description	Datatype	Optional	Null Value
timestamp	Time stamp in seconds since epoch	int	no	
version	Message format version. Currently 1.	int	no	
action	Firewall Action: * "App": application has been detected (see apps field) * "AppBlock": application has been blocked (see apps field) * "Inter": intermediate report, which is sent every 60s * "End": session has been terminated	string	no	
duration	Duration of the session in milliseconds	int	no	
src_iface	source interface name (e.g. "eth0")	string	yes	key is not in JSON
src_ip	source IP	string	no	
src_port	source port or session identifier for protocols without ports (e.g., ICMP)	int	yes	key is not in JSON
src_mac	source mac address	string	yes	"00:00:00:00:00:00"
dst_iface	destination interface name	string	yes	key is not in JSON
dst_ip	destination IP	string	no	
dst_port	destination port or session identifier for protocols without ports (e.g. ICMP)	int	yes	key is not in JSON
dst_mac	destination mac address	string	yes	"00:00:00:00:00:00"
fw_rule	Firewall rule name	string	yes	key is not in JSON
app_rule	application rule name (e.g. "<App>:ALL-APPS")	string	yes	key is not in JSON



src_ip_nat	source IP after NAT	string	yes	'0.0.0.0'
dst_ip_nat	destination IP after NAT	string	yes	'0.0.0.0'
fwd_bytes	number of bytes sent in the session's forward direction	int	yes	key is not in JSON
rev_bytes	number of bytes sent in the session's reverse direction	int	yes	key is not in JSON
fwd_packets	number of packets sent in the session's forward direction	int	yes	key is not in JSON
rev_packets	number of packets sent in the session's reverse direction	int	yes	key is not in JSON
user	username	string	yes	key is not in JSON
tunnel	tunnel name	string	yes	key is not in JSON
ip_proto	numeric IP protocol id (see https://www.iana.org/assignments/protocol-numbers/)	int	no	
protos	detected application protocols, from most specific to least specific (e.g., ["HTTPS direct", "HTTPS", "All HTTP protocols"]	array of strings	yes	key is not in JSON
contents	detected content types, from most specific to least specific (e.g., ["HTML", "Web Files"]	array of strings	yes	key is not in JSON
host	FUTURE FIELD			
referrer	FUTURE FIELD			
url_cat	FUTURE FIELD			
spam	FUTURE FIELD			

Example


```
{
    "version": 1,
    "timestamp": 1606230141,
    "action": "End",
    "duration": 8436,
    "src_iface": "eth0",
    "src_ip": "10.17.35.171",
    "src_port": 40532,
    "src_mac": "00:0c:29:9a:0a:78",
    "dst_iface": "eth0",
    "dst_ip": "193.99.144.85",
    "dst_port": 443,
    "dst_mac": "00:0c:29:00:d6:00",
    "fw_rule": "BOX-LAN-2-INTERNET",
    "app_rule": "<App>:ALL-APPS",
    "fw_info": 2007,
    "src_ip_nat": "10.17.35.175",
    "dst_ip_nat": "193.99.144.85",
    "fwd_bytes": 7450,
    "rev_bytes": 561503,
    "fwd_packets": 129,
    "rev_packets": 439,
    "ip_proto": 6,
    "protos": [
        "HTTPS direct",
        "HTTPS",
        "All HTTP protocols"
    ],
    "apps": [
        "Web browsing"
    ]
}
```


Logstash Log


```
{
    "@timestamp" => 2021-12-27T10:55:16.660Z,
          "beat" => {
         "version" => "6.2.4",
        "hostname" => "cgf-scout-int",
```

```
          "name" => "cgf-scout-int"
    },
          "tags" => [
        [0] "beats_input_codec_plain_applied"
    ],
       "product" => "ngfw",
    "input_type" => "log",
          "type" => "ngfw-act",
    "prospector" => {
        "type" => "udp"
    },
          "sn" => "4f94abdf7a8c465fa2cd76f680ecafd1",
       "message" => {
          "rev_bytes" => 748,
           "fw_rule" => "Internet",
          "ip_proto" => 6,
          "contents" => [
           [0] "HTML",
           [1] "Web Files"
        ],
           "src_mac" => "fc:bd:67:a5:f0:0f",
            "src_ip" => "10.11.1.4",
         "dst_port" => 80,
          "fwd_bytes" => 421,
          "dst_iface" => "dhcp",
           "src_port" => 40252,
            "dst_mac" => "00:22:48:2d:11:74",
               "apps" => [
           [0] "Web browsing"
        ],
          "src_iface" => "dhcp",
           "duration" => 9261,
            "version" => 1,
             "action" => "End",
             "dst_ip" => "89.238.73.97",
          "app_rule" => "<App>:BlockMacros",
             "protos" => [
           [0] "HTTP direct",
           [1] "HTTP",
           [2] "All HTTP protocols"
        ],
           "fw_info" => 0,
        "dst_ip_nat" => "89.238.73.97",
        "src_ip_nat" => "10.11.0.4",
       "fwd_packets" => 5,
         "timestamp" => 1640602516,
```

```
        "rev_packets" => 5
    },
      "@version" => "1"
}
```

Web Messages

(type = ngfw-wf)

JSON Fields

Field Name	Description	Datatype	Optional	Null Value
timestamp	Unix time stamp indicating when the request passed through the firewall	int	no	-
version	Message format version. Currently 1.	int	no	-
traffic_type	Always "0"	int	no	-
action	Numeric ID of the action that was performed by the firewall: "0" for allowed and "1" for blocked	int	no	-
source_ip	The source IP address of the request	string	no	-
source_port	The source port of the request	int	no	-
destination_ip	The destination IP address of the request	string	no	-
destination_port	The destination port of the request	int	no	-
method	The method of the request (e.g., "GET", "POST", "PUT", "CONNECT")	string	yes	key is not in JSON
status_code	The HTTP status code of the response	int	yes	"0"
user_agent	The User-Agent header request header field	string	yes	key is not in JSON
content_type	The Content-Type response header field	string	yes	key is not in JSON
name	The full URI of the request	string	yes	key is not in JSON
size	The Content-Length response header field	int	yes	"0"
domain	The "Referer" request header field or The host part of the request URI	string	yes	key is not in JSON
category	Numeric ID of the detected url category (1 - 96). Please treat any other value, or an empty array as "unknown"	int	yes	key is not in JSON

user	The username of the user performing the request or The source IP address of the request	string	no	-
user_type	1 if "user" is a username 0 if "user" is an IP address	int	no	-
fw_rule	The firewall rule that has been applied to the request	string	yes	key is not in JSON
app_rule	The application rule that has been applied to the request	string	yes	key is not in JSON

Examples


```
{
    "timestamp": 1526383397000,
    "traffic_type": 0,
    "action": 0,
    "source_ip": "192.168.42.124",
    "source_port": "50646",
    "destination_ip": "193.99.144.85",
    "destination_port": "443",
    "method": "GET",
    "status_code": "0",
    "user_agent": "wget/1.19.2 (linux-gnu)",
    "content_type": "text/html; charset=UTF-8",
    "name": "https://www.heise.de/",
    "size": 59558,
    "domain": "www.heise.de",
    "category": [
        "79"
    ],
    "user": "192.168.42.124",
    "user_type": 0,
    "fw_rule": "LAN-2-INTERNET",
    "app_rule": "<App>:<pass-no-match>"
}
{
    "timestamp": 1526377804000,
    "traffic_type": 0,
    "action": 0,
    "source_ip": "192.168.42.105",
    "source_port": "50159",
    "destination_ip": "216.58.207.67",
    "destination_port": "443",
    "method": "GET",
```

```
    "status_code": "0",
    "user_agent": "mozilla/5.0 (windows nt 6.1) applewebkit/537.36 (khtml,
like gecko) chrome/66.0.3359.139 safari/537.36",
    "content_type": "",
    "name":
"https://clientservices.googleapis.com/chrome-variations/seed?osname=win&chan
nel=stable&milestone=66",
    "size": 0,
    "domain": "clientservices.googleapis.com",
    "category": [
    ],
    "user": "192.168.42.105",
    "user_type": 0,
    "fw_rule": "LAN-2-INTERNET",
    "app_rule": "<App>:<pass-no-match>"
}
```

Logstash Log

```
{
    "@timestamp" => 2021-12-27T10:55:38.870Z,
          "beat" => {
         "version" => "6.2.4",
        "hostname" => "cgf-scout-int",
            "name" => "cgf-scout-int"
    },
          "tags" => [
        [0] "beats_input_codec_plain_applied"
    ],
       "product" => "ngfw",
    "input_type" => "log",
          "type" => "ngfw-wf",
    "prospector" => {
        "type" => "udp"
    },
            "sn" => "4f94abdf7a8c465fa2cd76f680ecafd1",
       "message" => {
            "traffic_type" => 0,
          "destination_ip" => "18.67.76.12",
                    "user" => "10.11.1.4",
                 "fw_rule" => "Internet",
        "destination_port" => "443",
            "content_type" => "text/html; charset=UTF-8",
             "status_code" => "0",
                 "version" => 1,
                  "action" => 0,
```

```
                    "name" => "https://www.barracuda.com/",
                  "method" => "GET",
                    "size" => 0,
                "category" => [
            [0] "82"
        ],
               "user_type" => 0,
                "app_rule" => "<App>:BlockMacros",
                  "domain" => "www.barracuda.com",
               "source_ip" => "10.11.1.4",
             "source_port" => "45796",
              "user_agent" => "mozilla/5.0 (macintosh; u; intel mac os x;
en)",
              "timestamp" => 1640602538000
    },
      "@version" => "1"
}
```

Threat Log

(type = ngfw-threat)

Filebeat Configuration

JSON Fields

Field Name	Description	Datatype	Optional	Null Value
date	Date	int	no	-
time	Time	int	no	-
version	Message format version. Currently 1.	int	no	-
severity	part of syslog header (e.g.: Warning)	string	no	-
timezone	part of syslog header	int	no	-
component	Future use. Currently „firewall“	string	no	-
operation	The operation that has been performed by the firewall (“Allow” “Block”)	string	no	-
type	Type of threat ("Virus", "ATD", " IPS", "Reputation")	string	no	-
trans_proto	Transport protocol of the session that caused the threat hit ("TCP", "UDP", ...)	string	no	-
src_ip	Source IP of the session	string	no	-
dst_ip	Destination IP of the session	string	no	-

port	Port of the session	int	no	-
app_target	Detected application target. E.g., URL or file name (e.g.: 86.exe)	string	yes	key is not in JSON
description	Description of the threat (e.g.: “ID: 1059898 EXPLOIT Generic HTML Threat -21”)	string	yes	key is not in JSON
user	Username of the user that caused the threat hit; only present if known by the fw engine	string	yes	key is not in JSON
threat_severity	A number representing the severity of the threat ["0" (Informational),"1" (Low),"2" (Medium),"3" (High)]	int	no	-
ips_category	The category of an IPS hit; only present for IPS hits (e.g.: "Web Attack")	string	yes	key is not in JSON

Examples


```
{
    "app_target": "eicar.exe",
    "component": "firewall",
    "date": "2018 05 15",
    "description": "Eicar-Test-Signature",
    "dst_ip": "10.0.6.96",
    "operation": "Block",
    "port": "443",
    "severity": "Warning",
    "src_ip": "10.17.35.169",
    "threat_severity": "3",
    "time": "15:42:27",
    "timestamp": "2018-05-15T15:42:27+00:00",
    "timezone": "+00:00",
    "trans_proto": "TCP",
    "type": "Virus",
    "user": "user42"
}
{
    "app_target": "boese.pdf",
    "component": "firewall",
    "date": "2018 05 15",
    "description": "ad43f5fc1d679c8d766824abb41b2b28b364c3c8;.pdf",
    "dst_ip": "103.248.176.78",
    "operation": "Block",
    "port": "80",
    "severity": "Warning",
    "src_ip": "10.17.35.169",
    "threat_severity": "3",
    "time": "15:42:32",
```

```
    "timestamp": "2018-05-15T15:42:32+00:00",
    "timezone": "+00:00",
    "trans_proto": "TCP",
    "type": "ATD",
    "user": "user42"
}
{
    "component": "firewall",
    "date": "2018 05 15",
    "description": "ID: 1054837 WEB Remote File Inclusion /etc/passwd",
    "dst_ip": "81.19.145.78",
    "ips_category": "Web Attack",
    "operation": "Block",
    "port": "80",
    "severity": "Warning",
    "src_ip": "10.17.35.169",
    "threat_severity": "3",
    "time": "15:46:06",
    "timestamp": "2018-05-15T15:46:06+00:00",
    "timezone": "+00:00",
    "trans_proto": "TCP",
    "type": "IPS",
    "user": "user45"
}
```


Logstash Log


```
{
          "beat" => {
         "version" => "6.2.4",
        "hostname" => "cgf-scout-int",
            "name" => "cgf-scout-int"
    },
       "product" => "ngfw",
        "source" => "/var/phion/logs/box_Firewall_threat.log",
          "type" => "ngfw-threat",
        "offset" => 110126,
    "prospector" => {
        "type" => "log"
    },
      "@version" => "1",
    "@timestamp" => 2021-12-27T10:55:16.390Z,
          "tags" => [
        [0] "beats_input_codec_plain_applied"
    ],
    "input_type" => "log",
```

```
            "sn" => "4f94abdf7a8c465fa2cd76f680ecafd1",
       "message" => {
             "operation" => "Allow",
          "ips_category" => "Virus/Worm",
                  "time" => "10:55:07",
              "timezone" => "+00:00",
                  "port" => "443",
                "src_ip" => "10.11.1.4",
                "dst_ip" => "89.238.73.97",
            "app_target" => "www.eicar.org",
            "trans_proto" => "TCP",
                  "type" => "IPS",
               "version" => 1,
              "severity" => "Warning",
             "component" => "firewall",
           "description" => "ID: 1051723 VIRUS Eicar test string",
                  "date" => "2021 12 27",
        "threat_severity" => "3",
             "timestamp" => "2021-12-27T10:55:07+00:00"
    }
}
```

Version File

JSON Fields

Field Name	Description	Optional	Null Value
version	Message format version. Currently 1.	no	-
ip_addr	Management IP of the box	no	-
model	Hardware/Cloud model of the box	no	-
firmware	Firmware version	no	-
hostname	The host name	no	-
serial	The serial of the box	no	-
domain	Domain name	yes	key is not in JSON
box	Name of the box	no	-
cluster	Name of the cluster that the box is assigned to. Optional, only present on boxes that are managed by a CC.	yes	key is not in JSON

range	Name (a numeric id) of the range that the box is assigned to. Optional, only present on boxes that are managed by a CC.	yes	key is not in JSON
box_description	A textual description of the box. Optional.	yes	key is not in JSON
cluster_description	A textual description of the cluster. Optional.	yes	key is not in JSON
range_description	A textual description of the range. Optional.	yes	key is not in JSON
brs_type	Always "version"	no	-
brs_index	Always "version"	no	-
brs_version	Unix time stamp of the last update	no	-
geo_latitude	Geo IP latitude. Optional. Double value.	yes	key is not in JSON
geo_longitude	Geo IP longitude. Optional. Double value.	yes	key is not in JSON
geo_country	"Located in Country" setting from box properties. Optional.	yes	key is not in JSON
geo_location	"Appliance Location" setting from box properties. Optional.	yes	key is not in JSON
geo_timezone	"Appliance Timezone" setting from box properties. Optional.	yes	key is not in JSON
geo_position	"GPS Coordinates" setting from box properties. Optional.	yes	key is not in JSON
tended_box_descriptor	"Custom Box Descriptors" settings from box properties. Optional. Array of objects containing a "label" and "value". Available with version 8.0.6 or higher, 8.2.2 or higher, or 8.3.1 or higher for CC-managed box.	yes	key is not in JSON

Examples

```
{
    "ip_addr": "10.17.68.110",
    "model": "vf1000",
    "firmware": "GWAY-7.2.1-115.nightbuild",
    "domain": "test.example.com",
    "hostname": "box71",
    "serial": "904646",
    "box": "box71",
    "box_description": "bobobo",
    "brs_type": "version",
    "brs_index": "version",
    "brs_version": 1526386796
```

```
}
{
    "ip_addr": "10.17.35.173",
    "model": "vf1000",
    "firmware": "GWAY-7.2.1-123.nightbuild",
    "hostname": "managed01",
    "serial": "976524",
    "box": "managed01",
    "cluster": "clstr",
    "range": "42",
    "box_description": "qwerty",
    "cluster_description": "bab",
    "range_description": "aba",
    "brs_type": "version",
    "brs_index": "version",
    "brs_version": 1526358967
}
{
    "ip_addr": "10.17.35.168",
    "model": "vf1000",
    "firmware": "GWAY-7.2.1-127.nightbuild",
    "domain": "BRStest.local",
    "hostname": "BRStest2",
    "serial": "985753",
    "box": "BRStest2",
    "cluster": "BRS",
    "range": "20",
    "cluster_description": "BRS test boxes",
    "range_description": "real 17.33er boxes",
    "brs_type": "version",
    "brs_index": "version",
    "brs_version": 1526359051
}
}
```

Figures

1. fwins_log.png