Remote agent

() (PC-), ( ) . , .

: **4.0.1236 (-).**

libpcap, tcpdump Wireshark. :

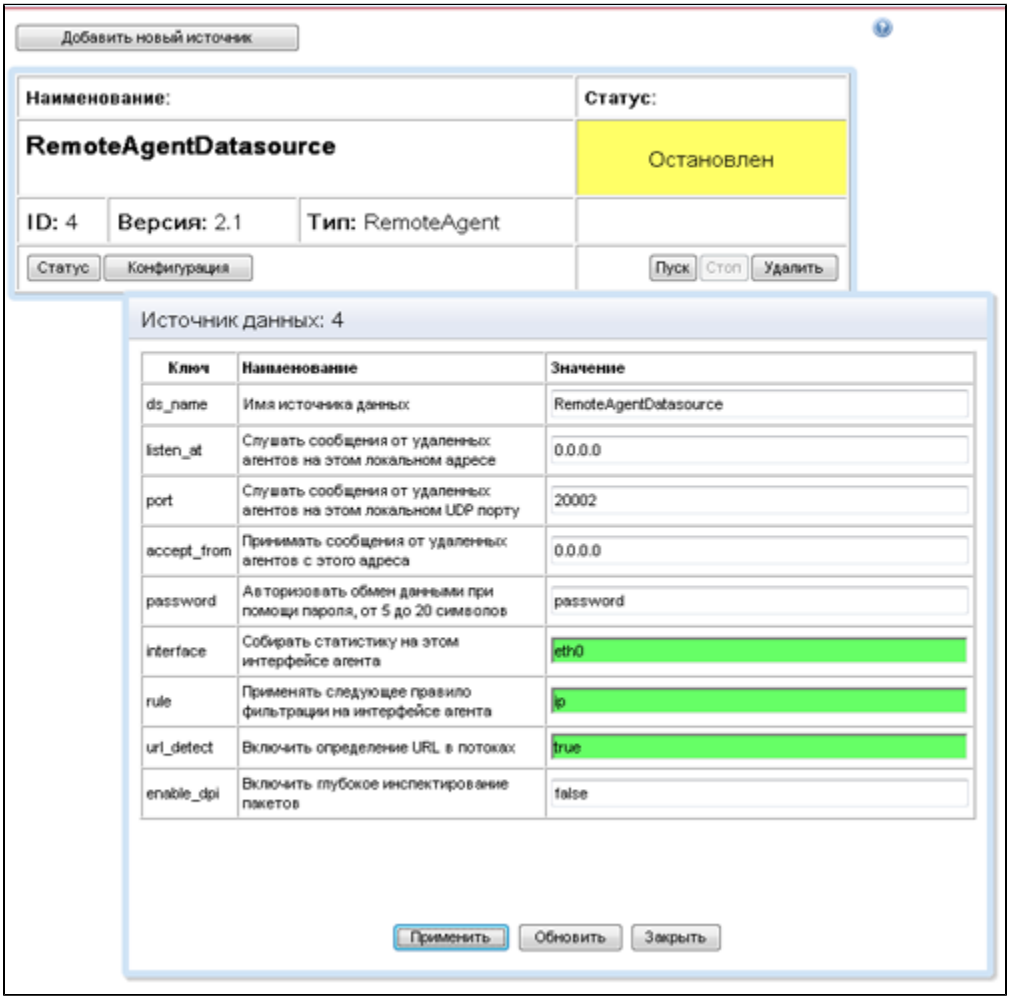
- (FreeBSD) jnetpcap
- ( )
- **(FreeBSD pf ipfw, Linux ipset)**

: ipfw pcap?

: ipfw kernel space user space , -. , , (- ,). , RemoteAgentDataSource libcap, pf, ipfw.

" " , ( ), Linux FreeBSD (32- , 64-). , , , . - , UDP, : 20002.

(jserver) (data source) **RemoteAgentDatasource**.



:

ds_name	
listen_at	IP-, . 0.0.0.0 - .
port	UDP-, . 20002.
accept_from	IP- (), . (0.0.0.0)
password	, "password". .
interface	, . , . " 0".

rule	, . , . " ".
url_detect	URL ( ) .
enable_dpi	- ()

" " - UNIX-. , jserver/agent.

:

```
demo:~#n4agent_pcap -c 127.0.0.1:20002 -p /var/run/n4agent.pid -d -q
```

:

-q	,
-p *pidfile*	,
-d	( )
-c *conn_str*	(RemoteAgentDatasource), UDP- (localhost: 20002)
-r *rule*	(man tcpdump). ( )
-i *ifname*	, PCAP ( )
-e *filename*	shell-, IP- **pf/ipfw/ipset**
-h	. , .
-b *bufsize*	PCAP (1 256) - .
-t *timeout*	, . (300). - .
-s *pwd*	(: password)

.

RemoteAgentDatasource. . , "" , .

- FreeBSD Linux, jserver/agent. http://www.netams.com/files/netams4/agents/ . (Windows), - (Linux FreeBSD).

n4agent -USR1, - (/var/log/messages /var/log/daemon.log) (,).

-e ( ) : , -.

: (FreeBSD 8.0), :

datasource @@ failed to open pcap interface: BIOCSRTIMEOUT: Invalid argument

? ?

: - (FreeBSD 8.2) c ( ) . . :

- : [http://www.netams.com/files/netams4/agents/n4agent-src.tar.gz] .
- gmake libevent
- src/ , [n4agent_pcap] .

- IP-. access-, -. , , . - (pf/ipfw/iptables). :

- ()
- , , IP- , . , ( ).

: -?

: -. , . . . , .

: , , ?

: . , , .