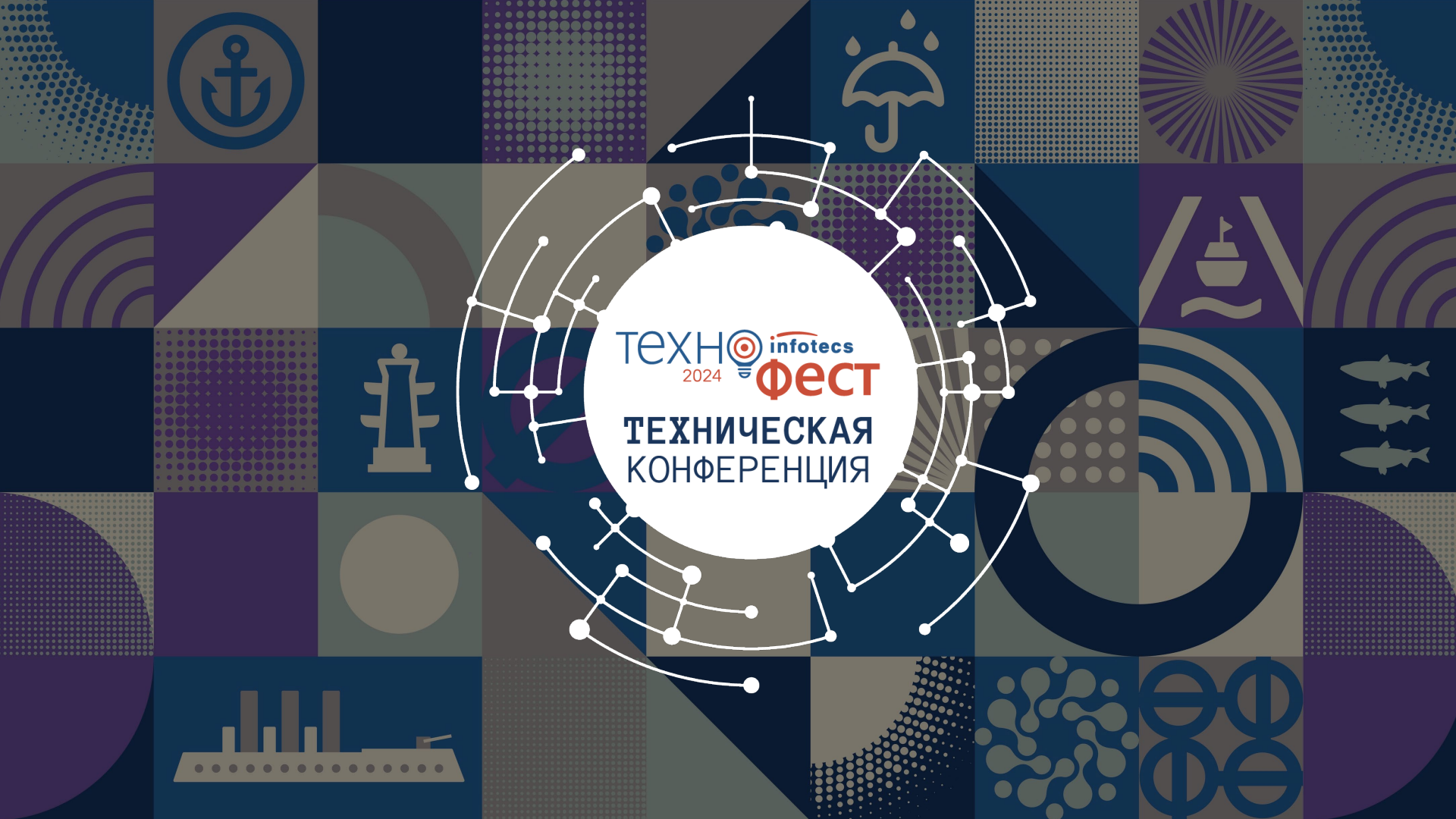
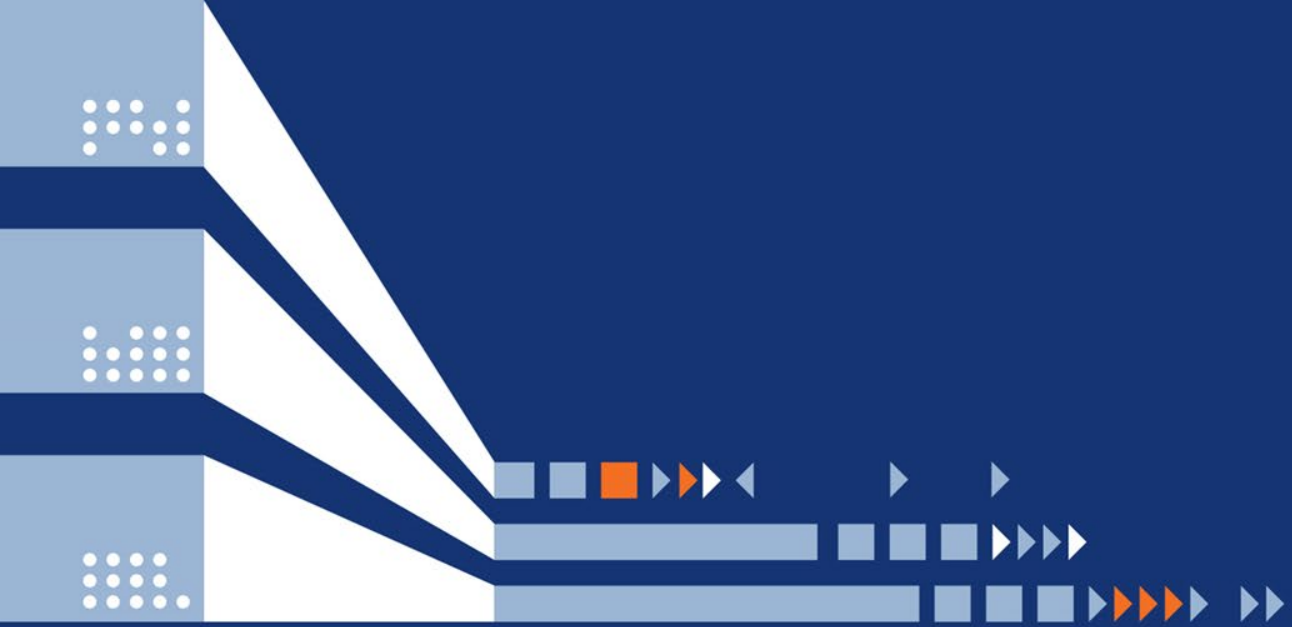

ТЕХНО
2024
infotecs
Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ



RiT
ЭКСПЕРТ
В ОБЛАСТИ
СИСТЕМНОЙ
ИНТЕГРАЦИИ

ОПЫТ ЭКСПЛУАТАЦИИ ПРОДУКТОВ ViPNet

Советы

Трюки

Фишки

Предостережения

ViPNet HW не смартфон, из коробки не работает!

Фундаментальные знания сети

Желание и время разбираться

Кривая архитектура сети

ПРОДЛЯЕМ ЖИЗНЬ HW50/100

Питание только через ИБП

Размер логов на интерфейсе

```
iplir config eth*

    [db]registerall= off          maxsize = 0 MBytes
```

УДАЛЕННЫЙ ПРОСМОТР ПАКЕТОВ


```
View results
 Date/time      | Dev  | Flags | Prot | Source IP      | Port | Destination IP | Port
 12/26 10:12:55 | eth0 | >-C-- | icmp | 192.168.1.10   |    0 | 192.168.0.2    |    0
 12/26 10:12:55 | eth0 | <-C-- | icmp | 192.168.0.2    |    0 | 192.168.1.10   |    0
 12/26 10:10:11 | eth1 | >-C-- | udp  | 192.168.2.1    | 2050 | 192.168.2.1    | 2050
 12/26 10:10:11 | eth0 | >-C-- | udp  | 192.168.0.2    | 2050 | 192.168.0.2    | 2050
 12/26 10:07:23 | eth0 | >-C-- | udp  | 192.168.0.1    | 2046 | 192.168.0.2    | 2046
 12/26 10:07:23 | eth0 | <-C-- | udp  | 192.168.0.2    | 2046 | 192.168.0.1    | 2046
 12/26 10:05:11 | eth1 | >-C-- | udp  | 192.168.2.1    | 2050 | 192.168.2.1    | 2050
 12/26 10:05:11 | eth0 | >-C-- | udp  | 192.168.0.2    | 2050 | 192.168.0.2    | 2050
 12/26 10:00:11 | eth1 | >-C-- | udp  | 192.168.2.1    | 2050 | 192.168.2.1    | 2050
 12/26 10:00:11 | eth0 | >-C-- | udp  | 192.168.0.2    | 2050 | 192.168.0.2    | 2050
 12/26 09:55:11 | eth1 | >-C-- | udp  | 192.168.2.1    | 2050 | 192.168.2.1    | 2050
 12/26 09:55:11 | eth0 | >-C-- | udp  | 192.168.0.2    | 2050 | 192.168.0.2    | 2050
 12/26 09:52:45 | eth1 | >D--T | udp  | 192.168.2.10   | 5353 | 224.0.0.251    | 5353
40 - Encrypted IP packet allowed

Interface : eth0                Packets Size : 345     Total In : 12695 b
Eth. proto: 800h                Packets Count: 1       Total Out: 26160 b

Esc - return to main window  Enter - view details  F2 - export to file
```

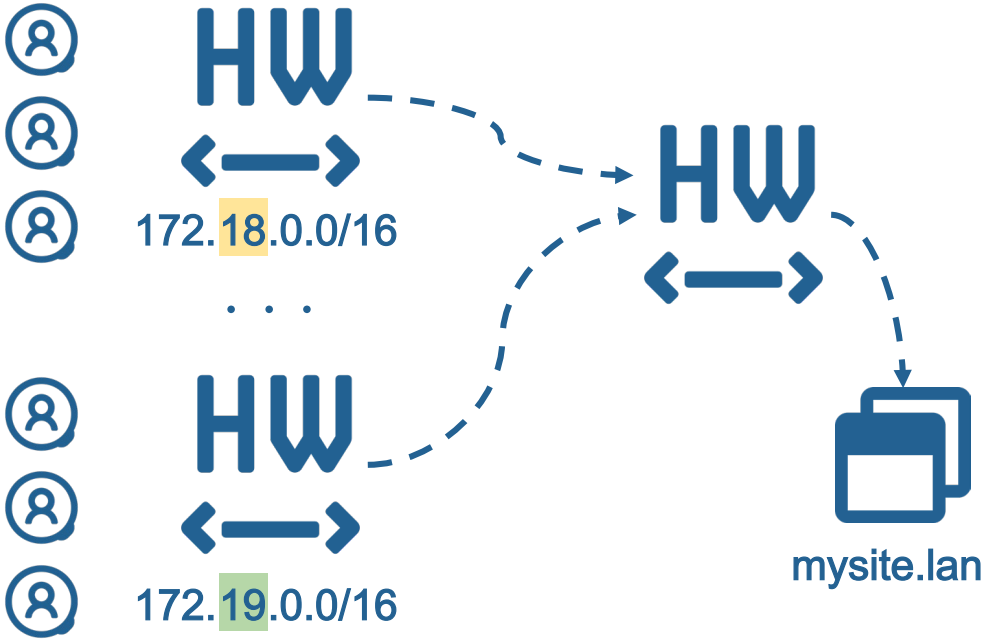
```
View results
 Date/time      | Dev  | Flags | Prot | Source IP      | Port | Destination IP | Port
 05/26 11:29:05 | eth0 | >D--- | tcp  | 10.1.15.17     | 50758| 10.1.15.10     | 179
 05/26 11:28:41 | eth0 | >D--- | tcp  | 10.1.15.17     | 63288| 10.1.15.10     | 179
 05/26 11:28:17 | eth0 | >D--- | tcp  | 10.1.15.17     | 57883| 10.1.15.10     | 179
 05/26 11:27:53 | eth0 | >D--- | tcp  | 10.1.15.17     | 51134| 10.1.15.10     | 179
 05/26 11:27:23 | eth0 | >D--- | tcp  | 10.1.15.17     | 51248| 10.1.15.10     | 179
 05/26 11:26:55 | eth0 | >D--- | tcp  | 10.1.15.17     | 50293| 10.1.15.10     | 179
 05/26 11:26:29 | eth0 | >D--- | tcp  | 10.1.15.17     | 51761| 10.1.15.10     | 179
 05/26 11:26:01 | eth0 | >D--- | tcp  | 10.1.15.17     | 62505| 10.1.15.10     | 179
 05/26 11:25:34 | eth0 | >D--- | tcp  | 10.1.15.17     | 49796| 10.1.15.10     | 179
 05/26 11:25:05 | eth0 | >D--- | tcp  | 10.1.15.17     | 53601| 10.1.15.10     | 179
 05/26 11:24:41 | eth0 | >D--- | tcp  | 10.1.15.17     | 64897| 10.1.15.10     | 179
 05/26 11:24:13 | eth0 | >D--- | tcp  | 10.1.15.17     | 59758| 10.1.15.10     | 179
 05/26 11:23:47 | eth0 | >D--- | tcp  | 10.1.15.17     | 52439| 10.1.15.10     | 179
22 - Non-encrypted IP Packet from network node

Interface : eth0                Packets Size : 116 B   Total In : 74530 B
Eth. proto: 800h                Packets Count: 2       Total Out: N/A

Source Node: (12AC000A) 1CGW01
Destin Node: (12AC000A) 1CGW01
Esc - return to main window  Enter - view details  F2 - export to file
```

```
vipnet dbview tcp 2047
```

УНИКАЛЬНАЯ АДРЕСАЦИЯ У КАЖДОГО HW



HW1 : iplir.conf

```
...

[virtualip]
startvirtualip= 172.18.0.1
maxvirtualip= 172.18.127.254
starttunnelvirtualip= 11.0.0.1
```

HW2 : iplir.conf

```
...

[virtualip]
startvirtualip= 172.19.0.1
maxvirtualip= 172.19.127.254
starttunnelvirtualip= 12.0.0.1
```

ПОЧЕМУ 10?

/opt/vipnet/user/iplir.conf

```
[id]
id= 0x********
name= CM HW<NAME> VPN-69
ip= 10.57.3.4, 10.80.3.80
ip= 172.16.185.50, 10.81.3.80
ip= 172.28.11.73, 10.82.3.80
ip= 172.28.111.1, 10.83.3.80
ip= 172.28.114.1, 10.84.3.80
ip= 172.28.114.9, 10.85.3.80
ip= 172.28.114.17, 10.86.3.80
ip= 172.28.114.25, 10.87.3.80
ip= 172.28.114.41, 10.88.3.80
ip= 172.28.134.1, 10.89.3.80
accessip= 10.57.3.4
tunnel= 172.28.11.74-172.28.11.74
```

10

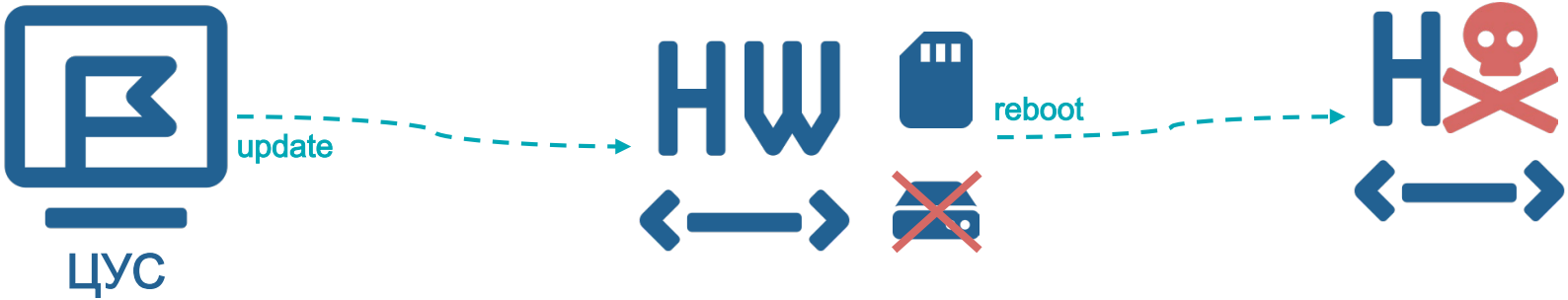
```
[adapter]
name= eth2
allowtraffic= on
type= external
```

/etc/config

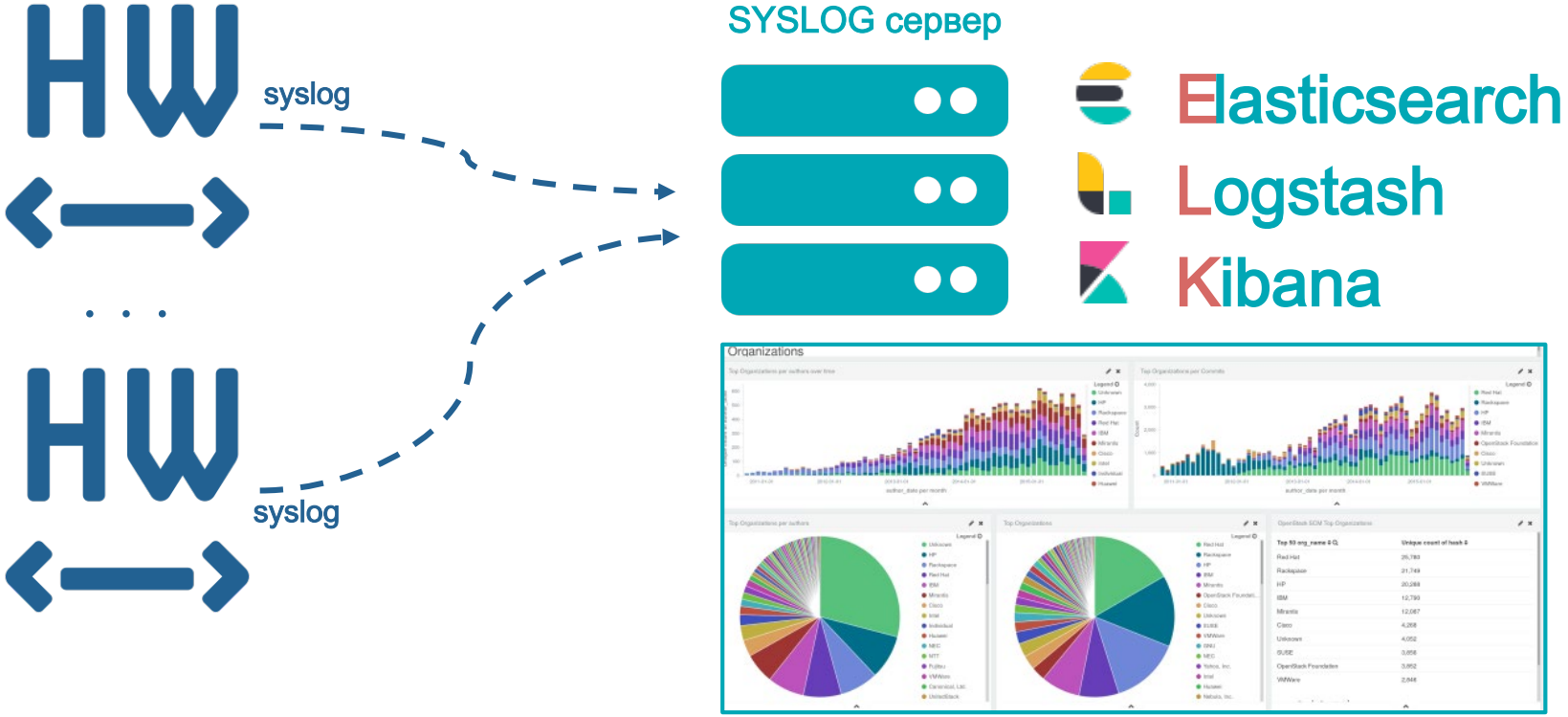
```
ETH3.2014_UP          1
ETH3.2014_VLAN 2014
ETH3.2014_PARENT eth3
ETH3.2014_IP 172.29.14.1 172.29.14.33
172.29.14.49 172.29.14.81 172.29.14.89
ETH3.2014_MASK 255.255.255.240
255.255.255.240 255.255.255.240
255.255.255.248 255.255.255.248
ETH3.2014_BROADCAST 172.29.14.15
172.29.14.47 172.29.14.63 172.29.14.87
172.29.14.95
ETH3.2014_SPEED auto
ETH3.2014_CLASS access
```

```
limit for device eth* is exceeded
```

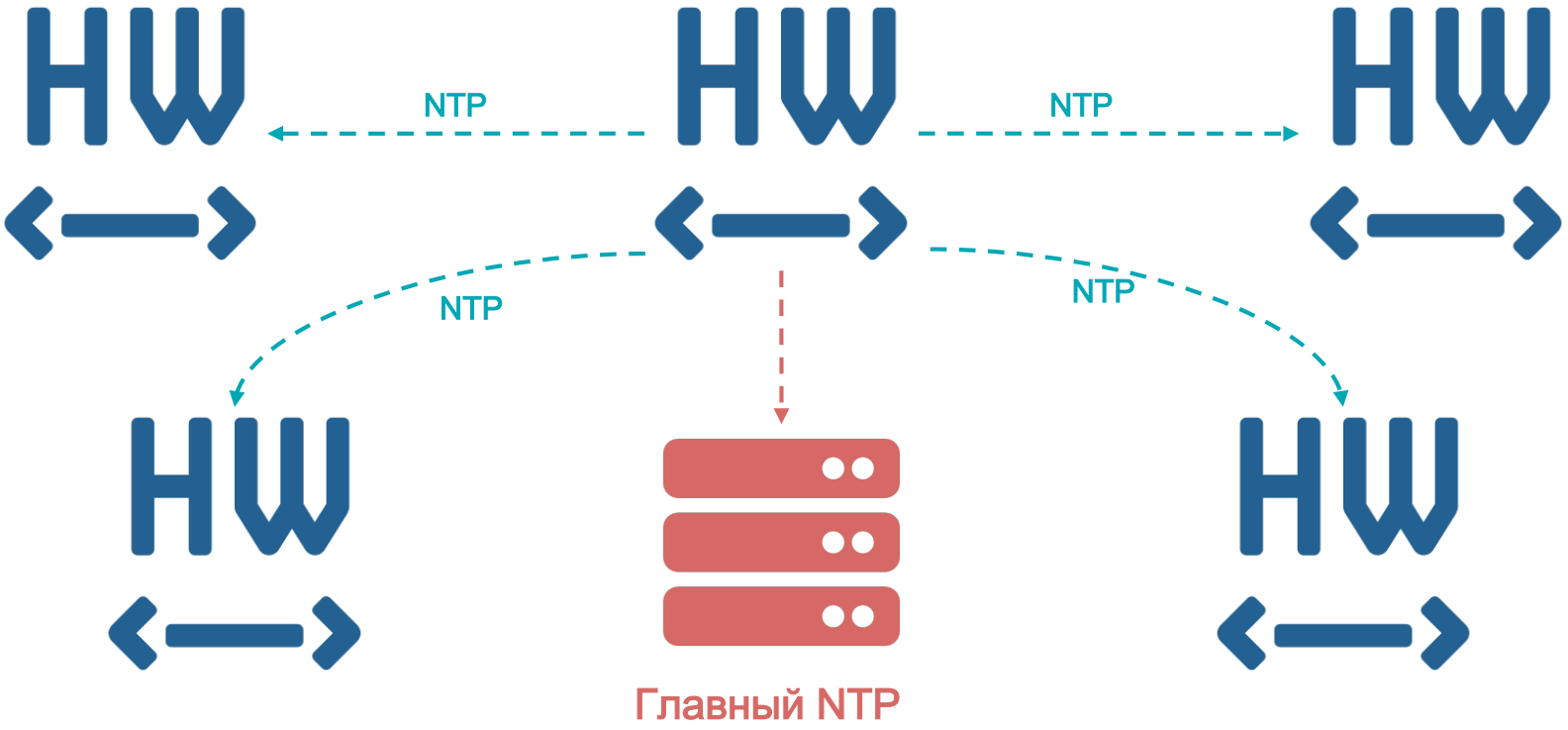
МОНИТОРИНГ ПАРКА HW



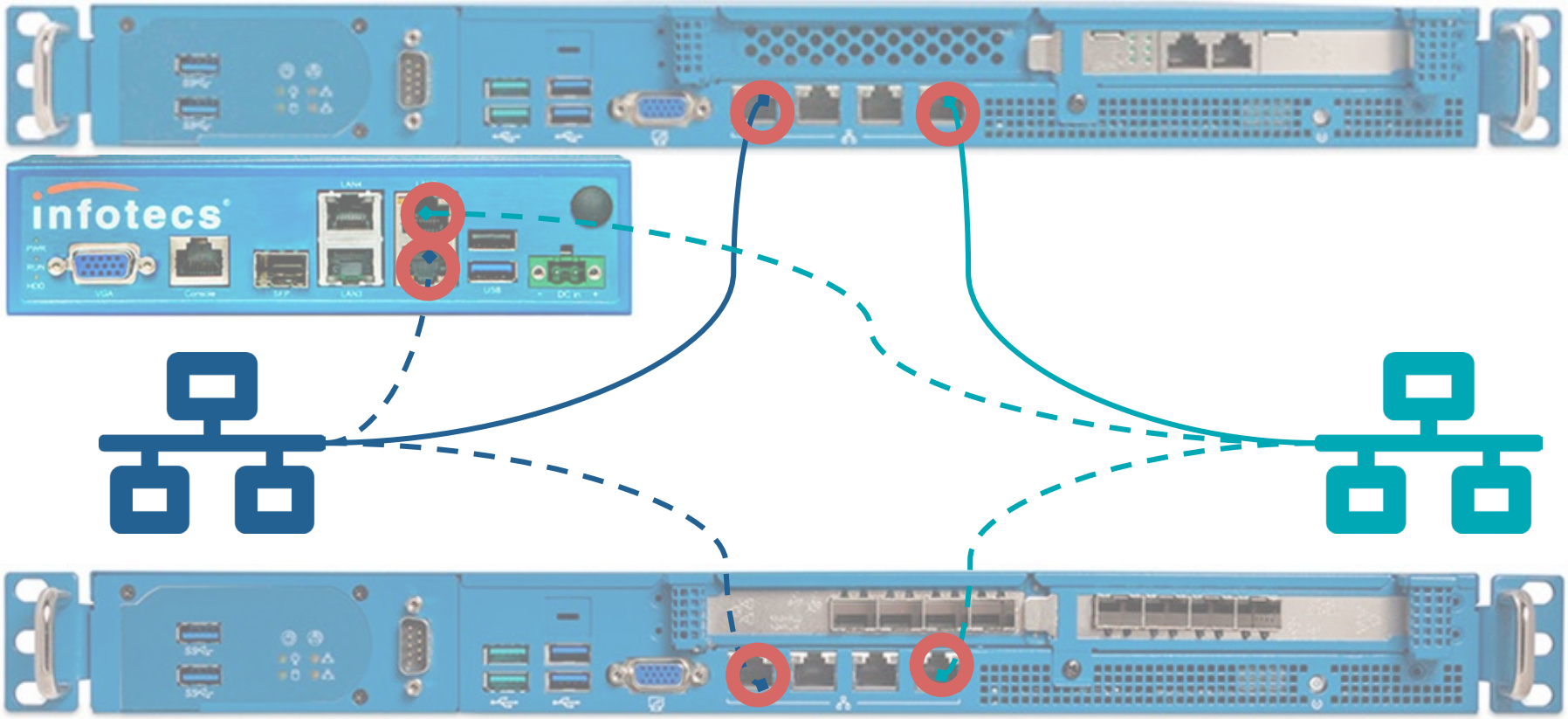
РАБОТА С ЛОГАМИ



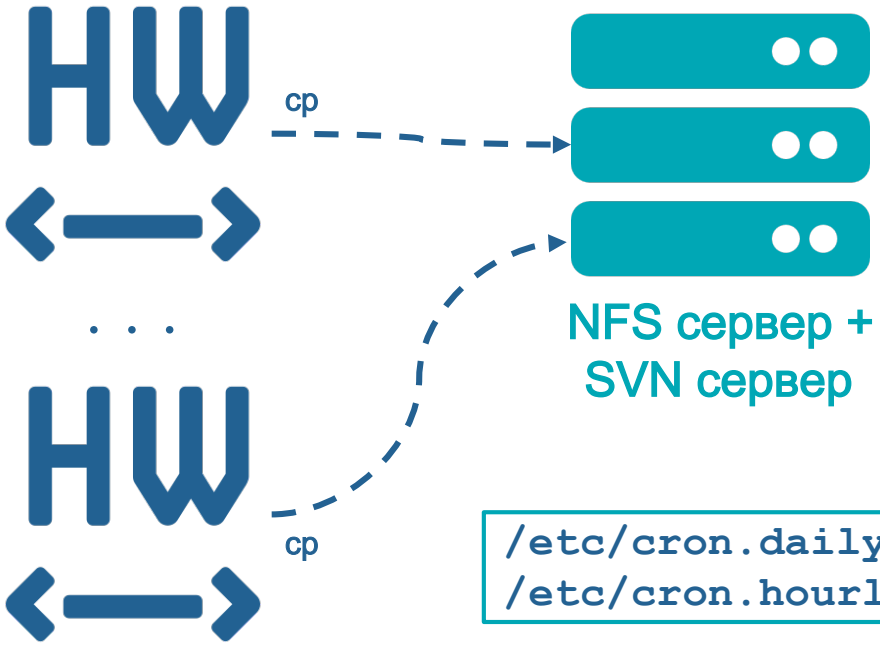
HW, СКОЛЬКО ВРЕМЕНИ?



ЗАМЕНИТЬ ЗА ТРИ СЕКУНДЫ



РЕЗЕРВНАЯ КОПИЯ КОНФИГУРАЦИЙ

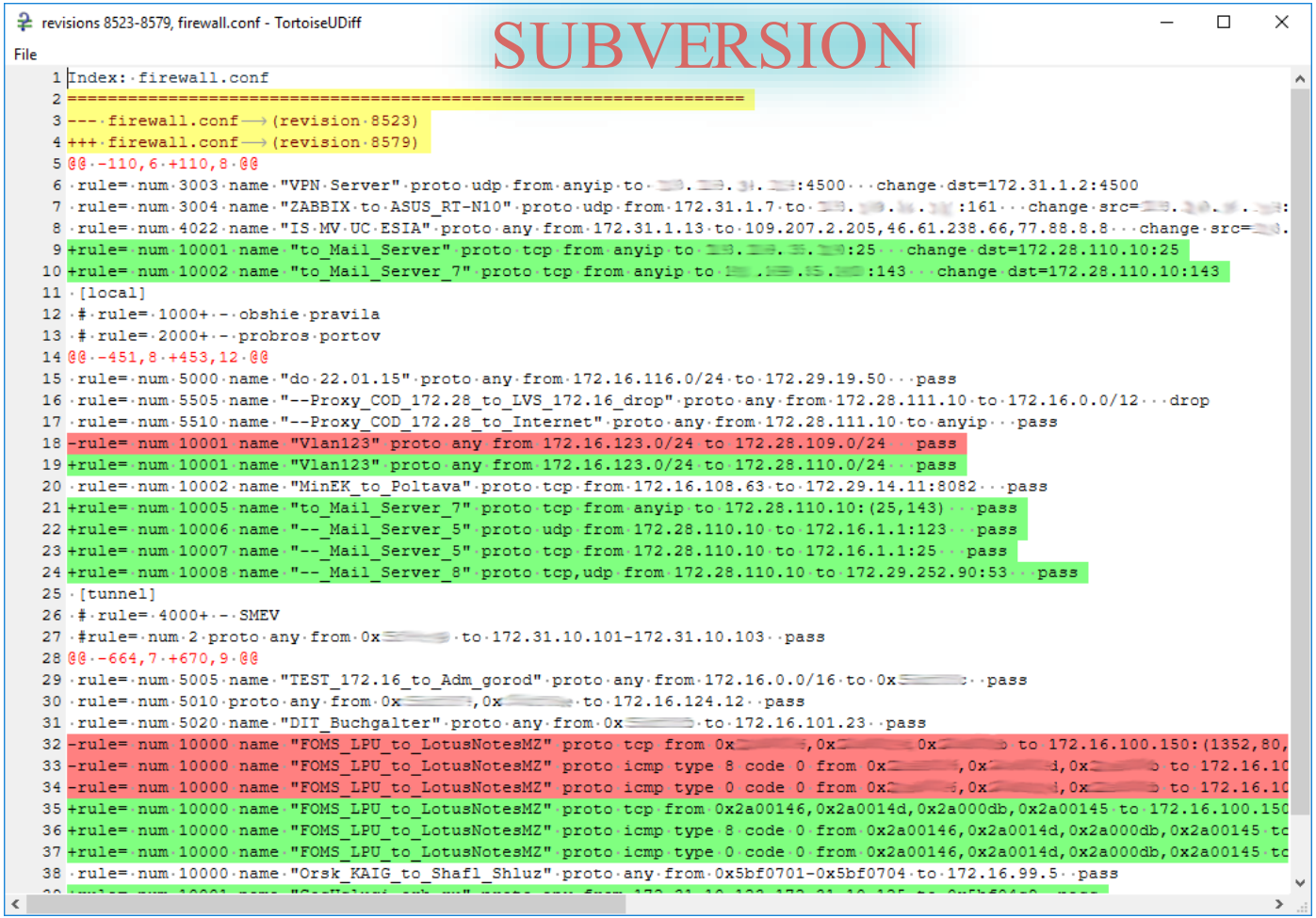


/opt/vipnet/user/iplir.conf
/opt/vipnet/user/user.xml – все правила firewall
/opt/vipnet/user/objects.xml – группы протоколов, узлов, ip
/etc/routing – таблица маршрутизации
/etc/config – список интерфейсов с их настройками

/etc/cron.daily/
/etc/cron.hourly/

```
scp /opt/vipnet/user/iplir.conf hw2000_1@host_ip:
```

SUBVERSION



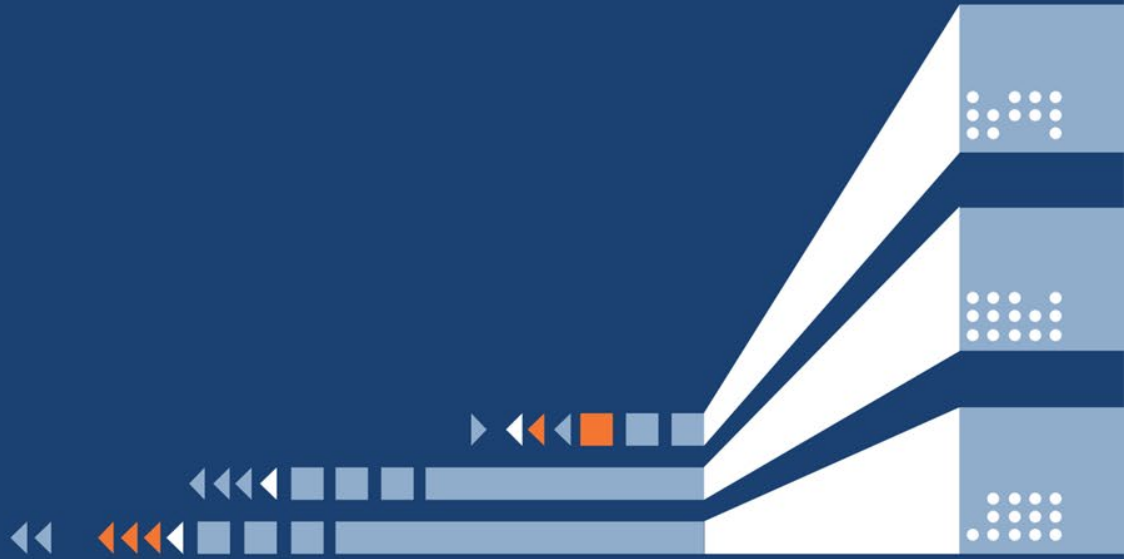
revisions 8523-8579, firewall.conf - TortoiseUDiff

File

```
Index: firewall.conf
===================================================================
--- firewall.conf ⟶ (revision 8523)
+++ firewall.conf ⟶ (revision 8579)
@@ -110,6 +110,8 @@
 rule= num 3003 name "VPN Server" proto udp from anyip to [redacted]:4500 ··· change dst=172.31.1.2:4500
 rule= num 3004 name "ZABBIX to ASUS_RT-N10" proto udp from 172.31.1.7 to [redacted]:161 ··· change src=[redacted]
 rule= num 4022 name "IS MV UC ESIA" proto any from 172.31.1.13 to 109.207.2.205,46.61.238.66,77.88.8.8 ··· change src=[redacted]
+rule= num 10001 name "to_Mail_Server" proto tcp from anyip to [redacted]:25 ··· change dst=172.28.110.10:25
+rule= num 10002 name "to_Mail_Server_7" proto tcp from anyip to [redacted]:143 ··· change dst=172.28.110.10:143
 [local]
 # rule= 1000+ - obshie pravila
 # rule= 2000+ - probros portov
@@ -451,8 +453,12 @@
 rule= num 5000 name "do 22.01.15" proto any from 172.16.116.0/24 to 172.29.19.50 ··· pass
 rule= num 5505 name "--Proxy_COD_172.28_to_LVS_172.16_drop" proto any from 172.28.111.10 to 172.16.0.0/12 ··· drop
 rule= num 5510 name "--Proxy_COD_172.28_to_Internet" proto any from 172.28.111.10 to anyip ··· pass
-rule= num 10001 name "Vlan123" proto any from 172.16.123.0/24 to 172.28.109.0/24 ··· pass
+rule= num 10001 name "Vlan123" proto any from 172.16.123.0/24 to 172.28.110.0/24 ··· pass
 rule= num 10002 name "MinEK_to_Poltava" proto tcp from 172.16.108.63 to 172.29.14.11:8082 ··· pass
+rule= num 10005 name "to_Mail_Server_7" proto tcp from anyip to 172.28.110.10:(25,143) ··· pass
+rule= num 10006 name "--_Mail_Server_5" proto udp from 172.28.110.10 to 172.16.1.1:123 ··· pass
+rule= num 10007 name "--_Mail_Server_5" proto tcp from 172.28.110.10 to 172.16.1.1:25 ··· pass
+rule= num 10008 name "--_Mail_Server_8" proto tcp,udp from 172.28.110.10 to 172.29.252.90:53 ··· pass
 [tunnel]
 # rule= 4000+ - SMEV
 #rule= num 2 proto any from 0x[redacted] to 172.31.10.101-172.31.10.103 ·· pass
@@ -664,7 +670,9 @@
 rule= num 5005 name "TEST_172.16_to_Adm_gorod" proto any from 172.16.0.0/16 to 0x[redacted] ·· pass
 rule= num 5010 proto any from 0x[redacted],0x[redacted] to 172.16.124.12 ·· pass
 rule= num 5020 name "DIT_Buchgalter" proto any from 0x[redacted] to 172.16.101.23 ·· pass
-rule= num 10000 name "FOMS_LPU_to_LotusNotesMZ" proto tcp from 0x[redacted],0x[redacted],0x[redacted] to 172.16.100.150:(1352,80,
-rule= num 10000 name "FOMS_LPU_to_LotusNotesMZ" proto icmp type 8 code 0 from 0x[redacted],0x[redacted],0x[redacted] to 172.16.10
-rule= num 10000 name "FOMS_LPU_to_LotusNotesMZ" proto icmp type 0 code 0 from 0x[redacted],0x[redacted],0x[redacted] to 172.16.10
+rule= num 10000 name "FOMS_LPU_to_LotusNotesMZ" proto tcp from 0x2a00146,0x2a0014d,0x2a000db,0x2a00145 to 172.16.100.150
+rule= num 10000 name "FOMS_LPU_to_LotusNotesMZ" proto icmp type 8 code 0 from 0x2a00146,0x2a0014d,0x2a000db,0x2a00145 to
+rule= num 10000 name "FOMS_LPU_to_LotusNotesMZ" proto icmp type 0 code 0 from 0x2a00146,0x2a0014d,0x2a000db,0x2a00145 to
 rule= num 10000 name "Orsk_KAIG_to_Shafl_Shluz" proto any from 0x5bf0701-0x5bf0704 to 172.16.99.5 ·· pass
```

- Туннелируемое адресное пространство межсетевого взаимодействия может перекрыть ваше
- Регуляторы ничего не знаю про номер сети ViPNet, они оперируют экземплярами СКЗИ

RiT ЭКСПЕРТ В ОБЛАСТИ СИСТЕМНОЙ ИНТЕГРАЦИИ



Михаил Шляпников

197375, г.Санкт-Петербург,
Ул. Смолячкова, д.19, офис 608

+7(812) 703-14-66 (7029)

m.shlyapnikov@ritservice.ru

ritservice.ru