с•терра

Ваш ориентир в мире безопасности

Диагностика и Траблшутинг С-Терра VPN

Мартышев Андрей
Инженер технического консалтинга
тел.: +7 (499) 940-90-01 доб. 235
e-mail: amartyshev @s-terra.ru

Этапы траблшутинга

Обнаружение

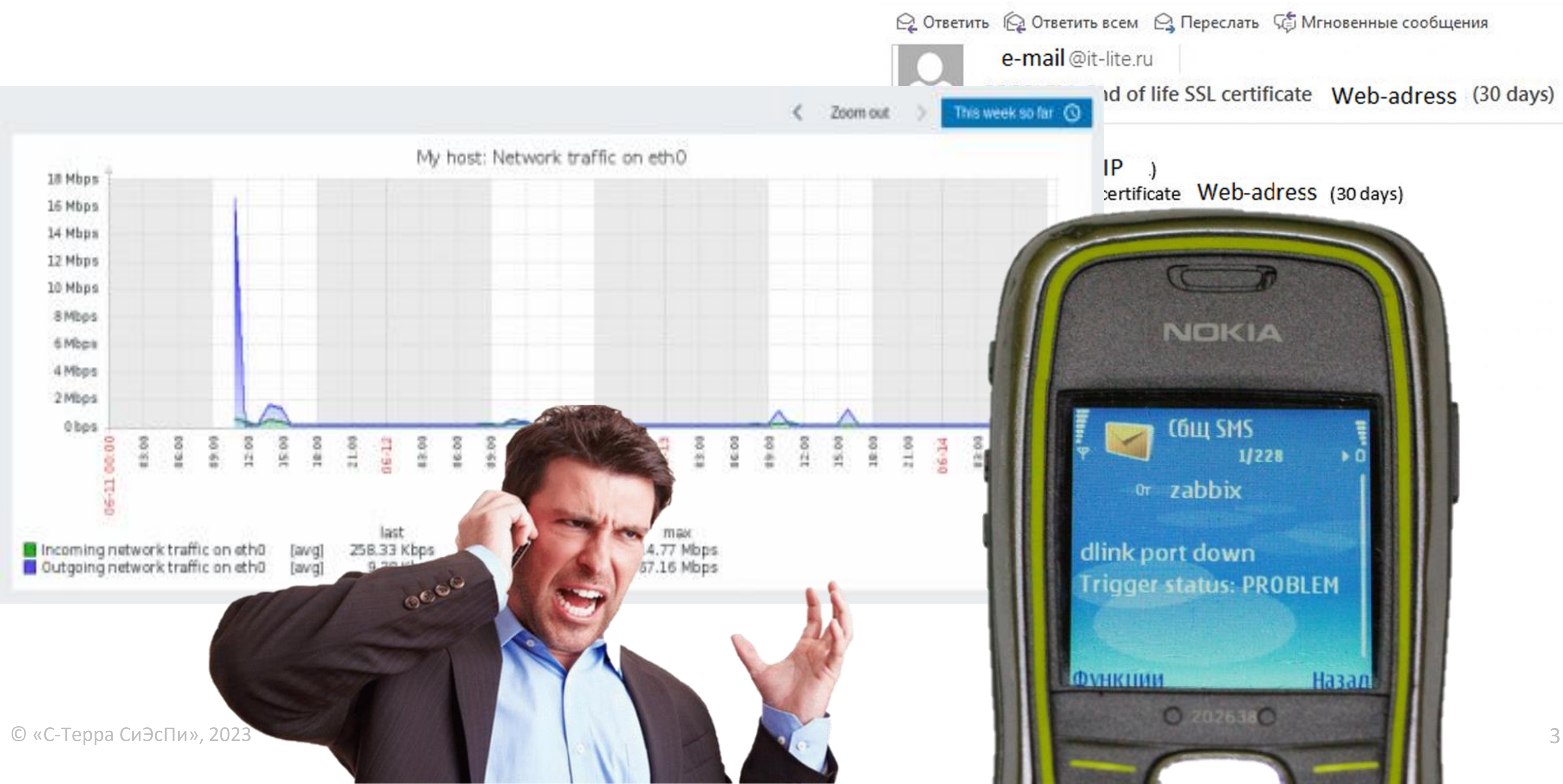
Диагностирование

Исправление

Проверка

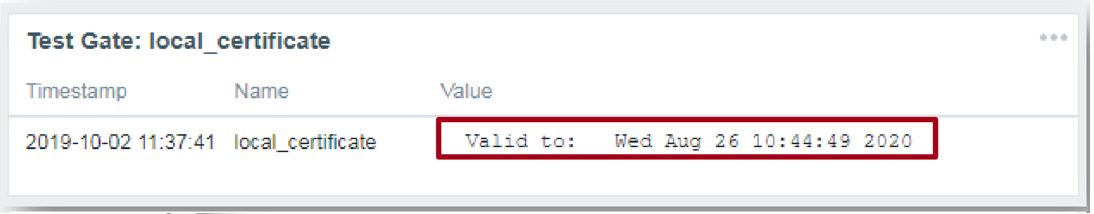
Обнаружение

Способы обнаружения



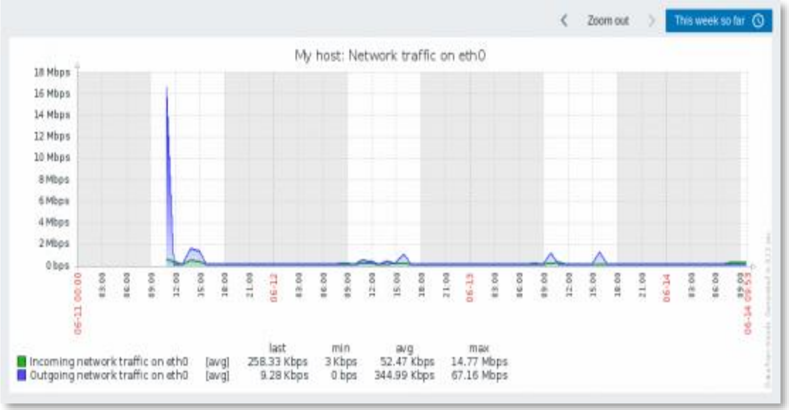
Обнаружение

Мониторинг по **SNMP**



Timestamp	Name	Value
2019-10-02 11:37:41	local_certificate	Valid to: Wed Aug 26 10:44:49 2020

ZABBIX



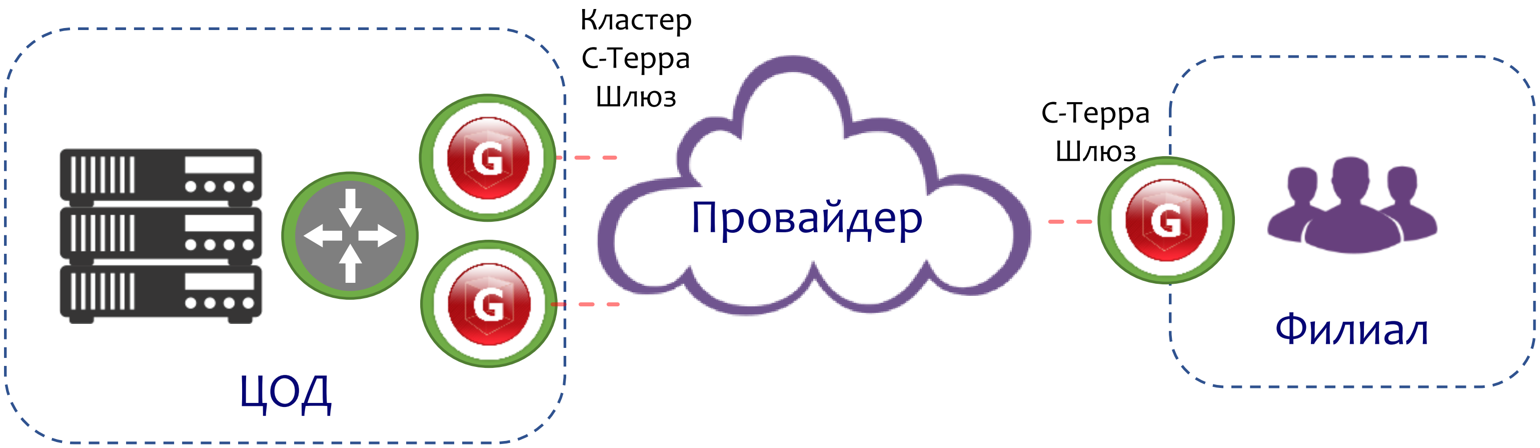
S-Terra UPWeb

https://www.youtube.com/watch?v=Gtf_JcaB0xo

http://doc.s-terra.ru/rh_output/4.3/Scenarios/output/mergedProjects/1main/ver_4_3_instr_01_monitoring.pdf

Обнаружение

Сужаем круг поиска

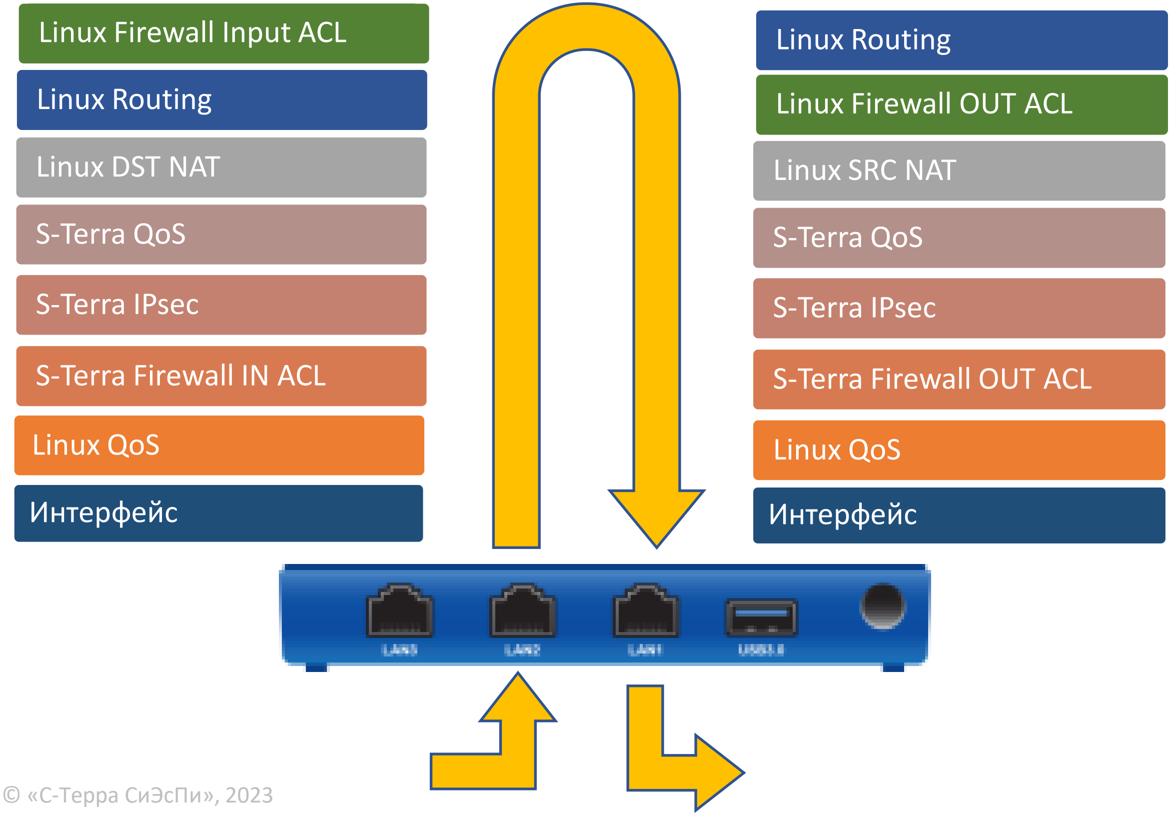


Диагностирование

Пример топологии

Диагностирование

Порядок обработки трафика




```
root@Hub:~# ip route
```

```
root@Hub:~# iptables –L
root@Hub:~# iptables –L –t nat
```

```
root@Hub:~#
            sa_mgr show
            klogview –l –f 0xffffff
            cat /var/log/cspvpngate.log
            csconf_mgr show
Hub# show running-config
```

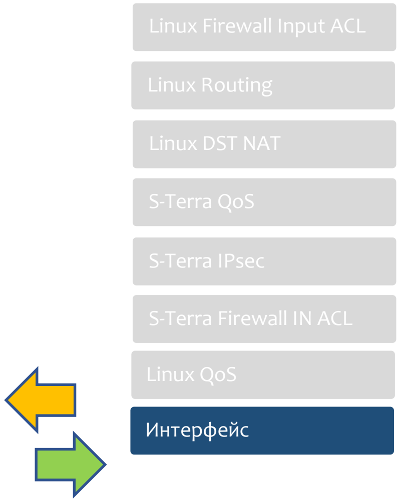
```
root@Hub:~# tc qdisc show
```

```
root@Hub:~# tcpdump –i eth0 -vvv
```

Проверяем трафик на интерфейсах

Spoke - PuTTY

```
root@Spoke:~# tcpdump -i eth1 -t host 172.16.1.100 and 172.16.2.100
…
IP 172.16.2.100 > 172.16.1.100: ICMP echo request, id 1079, seq 432, length 64

IP 172.16.1.100 > 172.16.2.100: ICMP echo reply, id 1079, seq 432, length 64

root@Spoke:~# tcpdump -i eth0 host 1.1.1.1 and 1.1.1.2
…
13:23:49.874280 IP 1.1.1.2 > 1.1.1.1: ESP(spi=0x6f167643,seq=0x144), length 108

13:23:49.874570 IP 1.1.1.1 > 1.1.1.2: ESP(spi=0xdeea801f,seq=0x144), length 108
```



Нет целевого трафика

Spoke - PuTTY

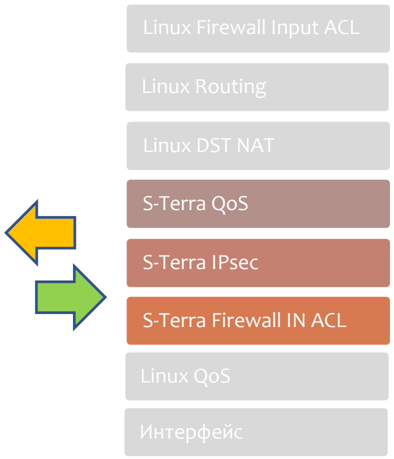
```
root@Spoke:~# tcpdump -i eth1 host 172.16.1.100 and 172.16.2.100
...
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

- Linux Firewall Input ACL
- Linux Routing
- Linux DST NAT
- S-Terra QoS
- S-Terra IPsec
- S-Terra Firewall IN ACL
- Linux QoS
- **Интерфейс**

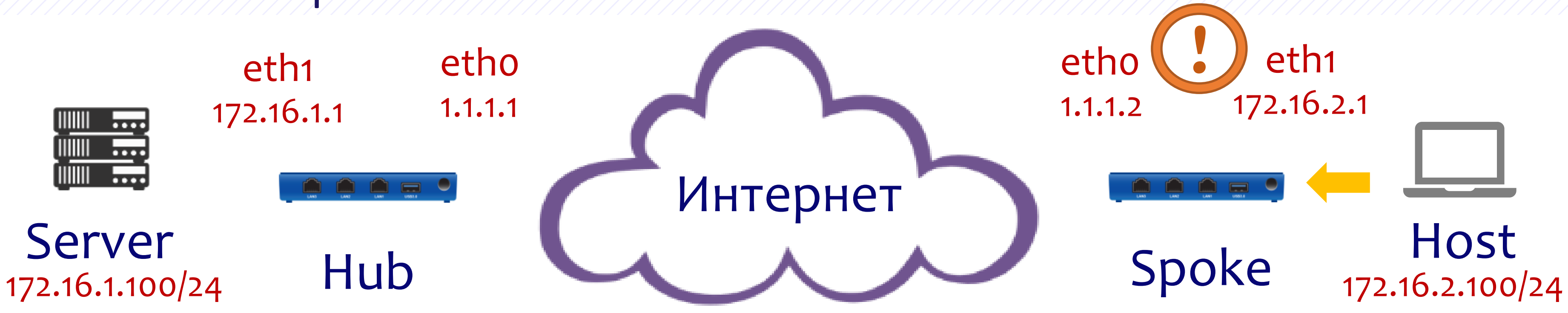
Проверяем работу драйвера

Spoke - PuTTY

```
root@Spoke:~# klogview -l -f 0xffffff | grep 172.16.1.100
filtration result for out packet 172.16.2.100->172.16.1.100, proto 1, len 84,
if eth0: chain 6 "IPsecPolicy:CMAP", filter 5,
event id IPsec:Protect:CMAP:1:HUB_ENCR, status PASS

encapsulating with SA 21: 172.16.2.100->172.16.1.100, proto 1, len 84, if eth0

filtration result for in packet 172.16.1.100->172.16.2.100, proto 1, len 84,
 if eth0: chain 6 "IPsecPolicy:CMAP", filter 5,
event id IPsec:Protect:CMAP:1:HUB_ENCR, status PASS

passed in packet 172.16.1.100->172.16.2.100, proto 1, len 84, if eth0: decapsulated
```



Ошибка настройки Firewall



Spoke - PuTTY

```
root@Spoke:~# tcpdump -i eth1 host 172.16.1.100 and 172.16.2.100
...
02:59:33 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,...
02:59:34 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,...

root@Spoke:~# klogview -l -f 0xffffff | grep '172.16.2.100->172.16.1.100'
filtration result for in packet 172.16.2.100->172.16.1.100, proto 1, len 84,
if eth1: chain 7 "FilterChain:FW_IN", filter 7, event id FW_IN, status DROP
dropped in packet 172.16.2.100->172.16.1.100, proto 1, len 84, if eth1:
firewall
```

Spoke - PuTTY

```
root@Spoke:~# csconf_mgr show
ip access-list extended FW_IN
 deny   ip 172.16.2.0 0.0.0.255 any
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 ip access-group FW_IN in
!
```

- Linux Firewall Input ACL
- Linux Routing
- Linux DST NAT
- S-Terra QoS
- S-Terra IPsec
- S-Terra Firewall IN ACL
- Linux QoS
- Интерфейс

Не применена криптокарта

Spoke - PuTTY

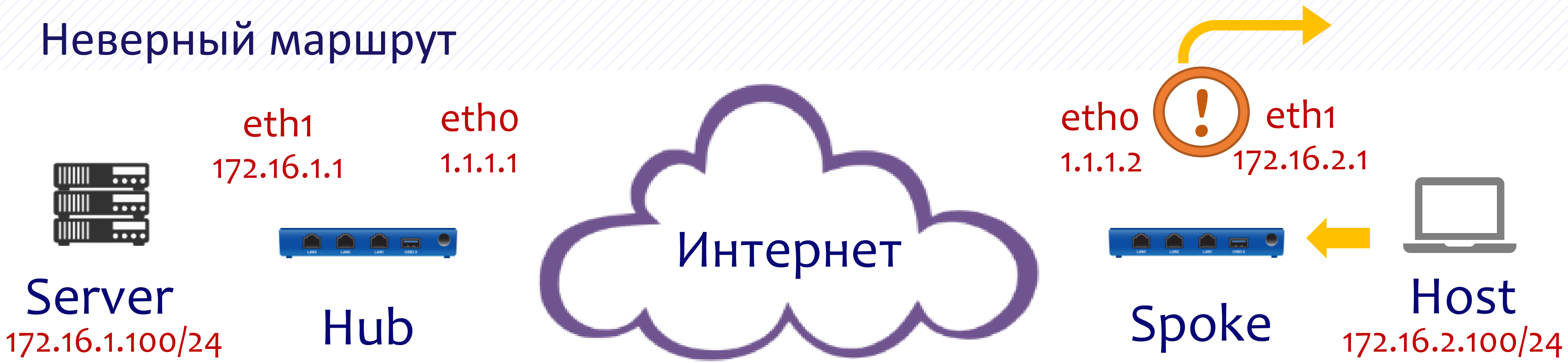
```
root@Spoke:~# tcpdump -i eth1 host 172.16.1.100 and 172.16.2.100
…
02:59:33 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,…
02:59:34 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,…

root@Spoke:~# klogview -l -f 0xffffff | grep '172.16.2.100->172.16.1.100’
…

root@Spoke:~# klogview -l -f 0xffffff
…
```

Spoke - PuTTY

```
root@Spoke:~# csconf_mgr show
crypto map CMAP 1 ipsec-isakmp
 match address HUB_ENCR
 set transform-set GOST
 set peer 1.1.1.1
!

interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 crypto map CMAP
!
```

- Linux Routing
- Linux Firewall Output ACL
- Linux SRC NAT
- S-Terra QoS
- **S-Terra IPsec**
- S-Terra Firewall OUT ACL
- Linux QoS
- Интерфейс

Неверный маршрут

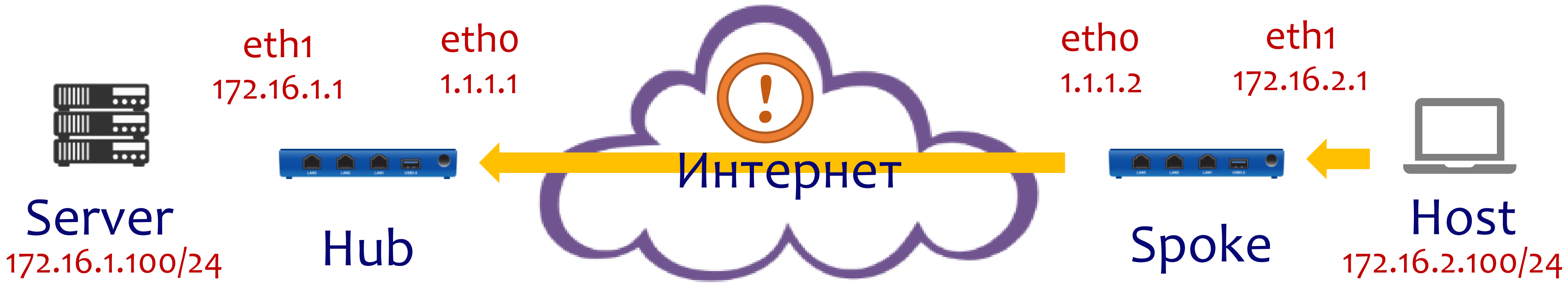


Spoke - PuTTY

```
root@Spoke:~# tcpdump -i eth1 host 172.16.1.100 and 172.16.2.100
02:59:33 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,...
02:59:34 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,...

root@Spoke:~# klogview -l -f 0xffffff | grep '172.16.2.100->172.16.1.100'
...
root@Spoke:~# ip route get 172.16.1.100
RTNETLINK answers: Network is unreachable

root@Spoke:~# ip route get 172.16.1.100
172.16.1.100 via 192.168.1.111 dev eth2 src 192.168.1.32
```

- Linux Firewall Input ACL
- **Linux Routing**
- Linux DST NAT
- S-Terra QoS
- S-Terra IPsec
- S-Terra Firewall IN ACL
- Linux QoS
- Интерфейс

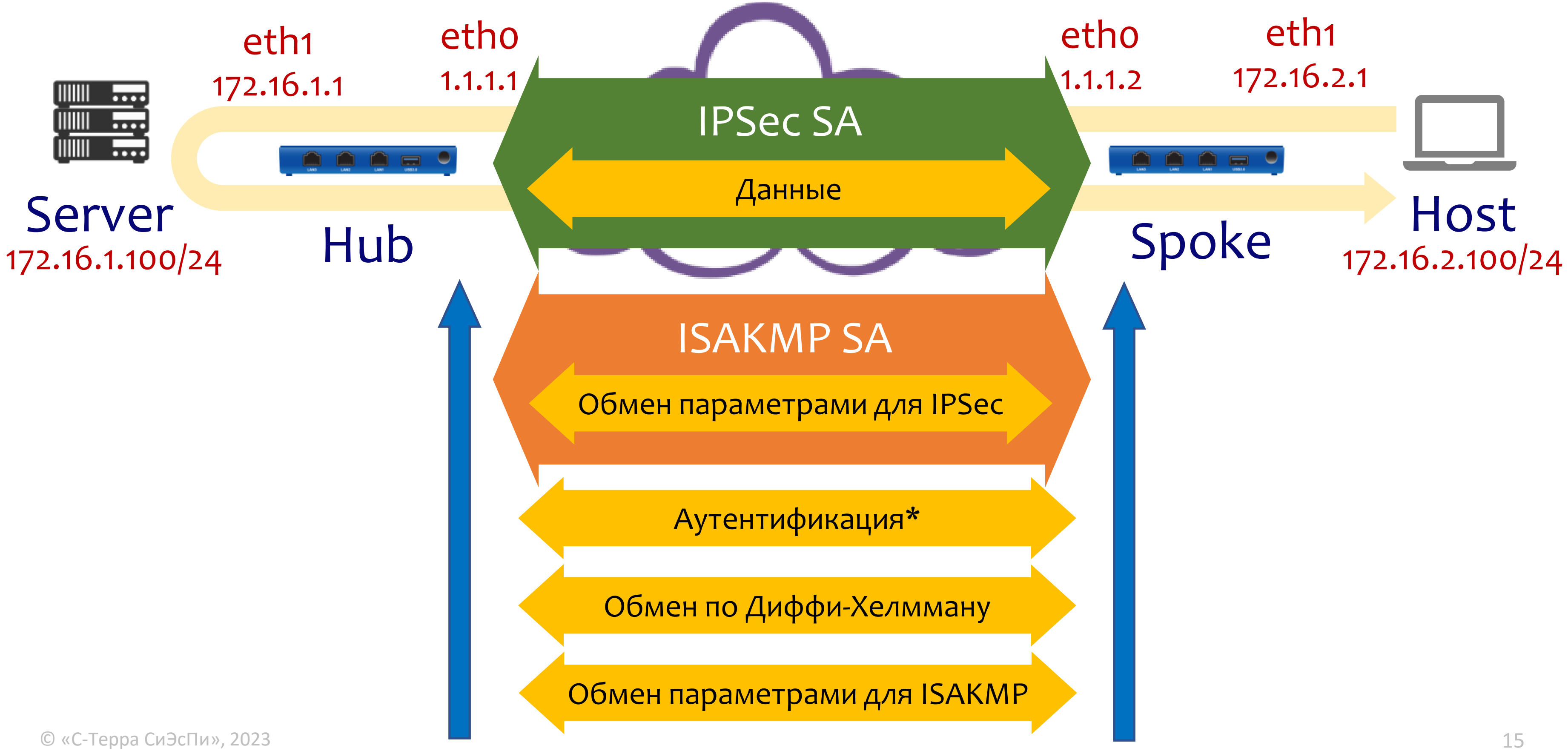
Не строится защищенное соединение



Spoke - PuTTY

```
root@Spoke:~# klogview -l -f 0xffffff | grep '172.16.2.100->172.16.1.100'

filtration result for out packet 172.16.2.100->172.16.1.100,… event id IPsec:Protect:CMAP:1:HUB_ENCR, status PASS
dropped out packet 172.16.2.100->172.16.1.100, proto 1, len 84, if eth0: filter 3: reached limit of 8 packets waiting for SA

root@Spoke:~# csconf_mgr show
crypto map CMAP 1 ipsec-isakmp
set peer 1.1.1.1

root@Spoke:~# sa_mgr show | grep 1.1.1.1
1 1 (1.1.1.2,500)-(1.1.1.1,500) incompleted 332 0
```

Построение защищенного соединения



Шлюз попал в blacklist

Spoke - PuTTY

```
root@Spoke:~# cat /var/log/cspvpngate.log |  grep 1.1.1.1
<4:0> Start IKE session, Request: IPSec connection request #4, type Main, peer 1.1.1.1, …
root@Spoke:~# cat /var/log/cspvpngate.log |  grep '<4:0>'
<4:0> Start IKE session, Request: IPSec connection request #4, type Main, peer 1.1.1.1, …
<4:0> Sending ISAKMP proposals: …
<4:0> IKE session stopped at [Main Mode, Initiator, Packet 1], Reason: Session timeout
```

Hub - PuTTY

```
root@Hub:~# cat /var/log/cspvpngate.log |  grep 1.1.1.2
Nov 30 04:38:30 localhost  vpnsvc: 1000000f [ISAKMP] Access denied for peer 1.1.1.2. 9 IKE-packet(s) dropped
root@Hub:~# service vpngate restart
```

Несоответствие конфигураций ISAKMP

Spoke - PuTTY

```
<4:0> Start IKE session, Request: IPSec connection request #4, type Main, peer 1.1.1.1, …
<4:0> Sending ISAKMP proposals: …
<4:1> Received unprotected notification [NO-PROPOSAL-CHOSEN] for <4:0>: Ignore
```

Hub - PuTTY

```
<1:0> Checking Transform #1 for Rule "IKERule:CMAP:1", Proposal #1, Protocol ISAKMP, Transform #1: group description not match
<1:0> IKE session stopped at [Main Mode, Responder, Packets 1,2][Compare policy], Reason: NO-PROPOSAL-CHOSEN
```

Hub - PuTTY

```
root@Hub:~# csconf_mgr
…
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
…
```

Spoke - PuTTY

```
root@Spoke:~# csconf_mgr
…
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko
!
…
```

Истек срок действия сертификата

Spoke - PuTTY

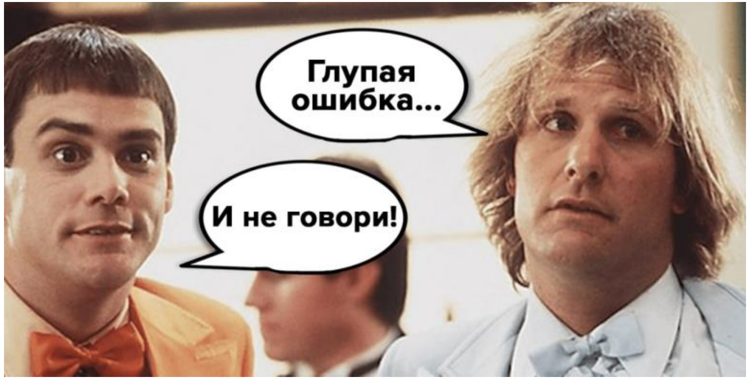
```
<4:0> Send identity "CN=GW2", peer 1.1.1.1
<4:1> Start IKE session, Request: Inbound ISAKMP packet, type Informational, peer 1.1.1.1, sessionId A965E3B44474D369.F8EBA8B5
<4:1> Received notification [CERTIFICATE-UNAVAILABLE] for <4:0>: Cancel session
<4:0> IKE session stopped at [Main Mode, Initiator, Packets 4,5, Signature], Reason: Authentication failed
```

Hub - PuTTY

```
<5:0> Receive identity "CN=GW2", peer 1.1.1.2
<5:0> Searching peer certificate failed. Reason: EXPIRED. Subject: CN=GW2 Issuer: C=RU,O=S-Terra,CN=autosterraCA SN:
1A0000000F37DD37133A7B23D000000000000F, peer 1.1.1.2, id "CN=GW2"
<5:0> IKE session stopped at [Main Mode, Responder, Packets 5,6, Signature][Choose Rule][Choose Rule for Partner's identity], Reason: No rule chosen
```

Hub - PuTTY

```
root@Hub:~# cert_mgr check
3 State: Inactive CN=GW2
        Certificate is expired.
        Valid from: Sat Nov 25 18:32:50 2019
        Valid to:   Fri Nov 25 18:42:50 2020

root@Hub:~# date
Sat Dec  1 12:22:19 MSK 2020
```



Отсутствует CRL при его включенной проверке

Spoke - PuTTY

```
<4:0> Searching local certificate failed. Reason: NOT VERIFIED. Subject: CN=GW2 Issuer: C=RU,O=S-Terra,CN=autosterraCA SN: 1A0000000F37DD37133A7B23D000000000000F, peer 1.1.1.1
<4:0> IKE session stopped at [Main Mode, Initiator, Packets 4,5, Signature][Form ID][Get Local Certificate]
```

Hub - PuTTY

```
<5:0> IKE session stopped at [Main Mode, Responder, Packets 3,4, Signature], Reason: Session timeout
```

Spoke - PuTTY

```
root@Spoke:~# cert_mgr check
1 State: Inactive CN=GW2
        Certificate can not be verified.

root@Spoke:~# csconf_mgr show
...
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
```

Несоответствие конфигураций IPSEC

Spoke - PuTTY

```
<3:404> Received notification [NO-PROPOSAL-CHOSEN] for <3:403>: Cancel session
<3:403> IKE session stopped at [Quick Mode, Initiator, Packet 1], Reason: No proposal chosen
```

Hub - PuTTY

```
<3:19> Receive traffic request: (172.16.2.0/255.255.254.0,,)->(172.16.1.0/255.255.255.0,,)
<3:19> IKE session stopped at [Quick Mode, Responder, Packets 1,2][Check incom IDs], Reason: Invalid traffic request
```

Hub - PuTTY

```
root@Hub:~# csconf_mgr
...
crypto ipsec transform-set GOST esp-gost28147-4m-imit
!
ip access-list extended SPOKE_ENCR
 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
crypto map CMAP 1 ipsec-isakmp
 match address SPOKE_ENCR
 set transform-set GOST
 set peer 1.1.1.2
```

Spoke - PuTTY

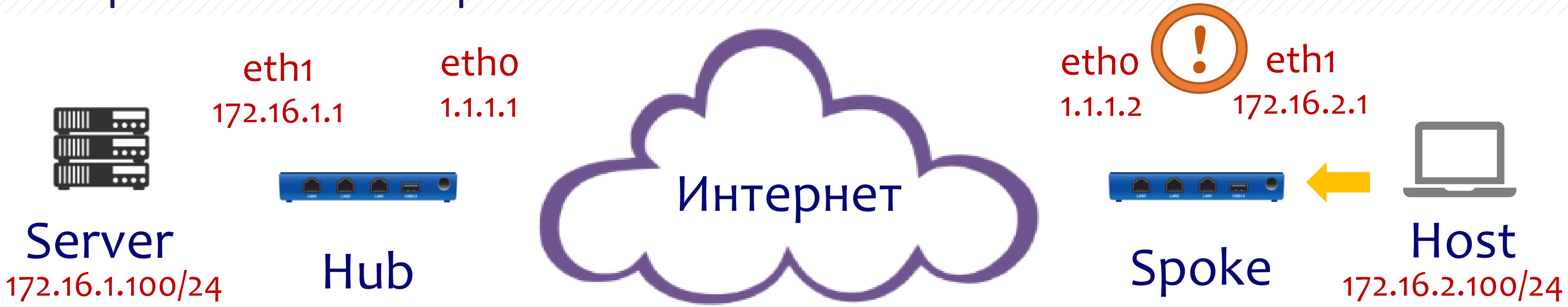
```
root@Spoke:~# csconf_mgr
...
crypto ipsec transform-set GOST esp-gost28147-4m-imit
!
ip access-list extended HUB_ENCR
 permit ip 172.16.2.0 0.0.1.255 172.16.1.0 0.0.0.255
!
crypto map CMAP 1 ipsec-isakmp
 match address HUB_ENCR
 set transform-set GOST
 set peer 1.1.1.1
```

Проверяем состояние туннеля

Spoke - PuTTY

```
root@Spoke:~# watch sa_mgr show
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 4 (1.1.1.2,500)-(1.1.1.1,500) active 1832 1776

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 2 (172.16.2.0-172.16.2.255,*)-(172.16.1.0-172.16.1.255,*) * ESP tunn 2024 2024
```

Не работает VPN-сервис



Spoke - PuTTY

```
root@Spoke:~# tcpdump -i eth1 host 172.16.1.100 and 172.16.2.100
02:59:33 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,...
02:59:34 IP 172.16.2.100 > 172.16.1.100: ICMP echo request,...

root@Spoke:~# klogview -l -f 0xffffff | grep '172.16.2.100->172.16.1.100'
passed in packet 172.16.2.100->172.16.1.100, proto 1, len 84, if eth1: driver default policy

root@Spoke:~# csconf_mgr show
ERROR: Could not establish connection with daemon.

root@Spoke:~# service vpngate start
```

- Linux Firewall Input ACL
- Linux Routing
- Linux SRC NAT
- S-Terra QoS
- **S-Terra IPsec**
- S-Terra Firewall IN ACL
- Linux QoS
- Интерфейс

Деградация сервиса

Неисправность оборудования

Версия 4.3

Spoke - PuTTY

```
root@Spoke:~# ip -s link
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN mode DEFAULT group default qlen 1000
    link/ether 00:50:56:2d:a7:4a brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    911322     3441     0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    401664     2912     0       0       0       0
...
```

Версия 4.2

Spoke - PuTTY

```
root@Spoke:~# ifconfig
...
eth0      Link encap:Ethernet  HWaddr 00:50:56:2d:a7:4a
          inet addr:1.1.1.2  Bcast:1.1.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2400
```

Деградация сервиса

Предельная нагрузка

Spoke - PuTTY

```
root@Spoke:~# top
top - 03:07:04 up  2:53,  1 user,  load average: 0.00, 0.00, 0.00
Tasks:  78 total,   1 running,  77 sleeping,   0 stopped,   0 zombie
%Cpu(s):  99.7 us,  0.0 sy,  0.0 ni, 0.03 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1010964 total,   777424 free,    95920 used,   1

root@Hub:~# watch kstat_show
ipsec in pkt:           2762
ipsec in oct:           353536
ipsec in drop:          0
ipsec no_sa:            0
ipsec replay drops:     0
ipsec auth fails:       0
ipsec decrypt fails:    0
ipsec out pkt:          2762
ipsec out oct:          353536
ipsec out drop:         0
frag ok:                0
frag fail:              0
link send:              0
link send err:          0
link recv:              0
rx errors:              0
tx errors:              0
route errors:           0
skb allocation errors:  0
send queue overflows:   0
high priority packets dropped:                5261
low priority packets dropped:                 0
high priority packets passed while overloaded:  0
```

Новые инструменты в версии 4.3

Скрипт сбора диагностической информации:

/opt/VPNagent/bin/get_info.bash

Дополнительные команды в CLI:

show ip interface [brief]

show vrrp [statistics]

show serial-number

show access-lists [interface]

с•терра®

Ваш ориентир в мире безопасности

Технический консалтинг:
Демо. Пилоты. Обучение.

presale@s-terra.ru

Москва, Зеленоград, ул. Конструктора Лукина, д.14, стр.12
+7 (499) 940 9061
www.s-terra.ru