POSITIVE TECHNOLOGIES

Обеспечение безопасности корпоративной сети с помощью MaxPatrol

Строев Евгений

эксперт по информационной безопасности Positive Technologies

О чём пойдёт речь

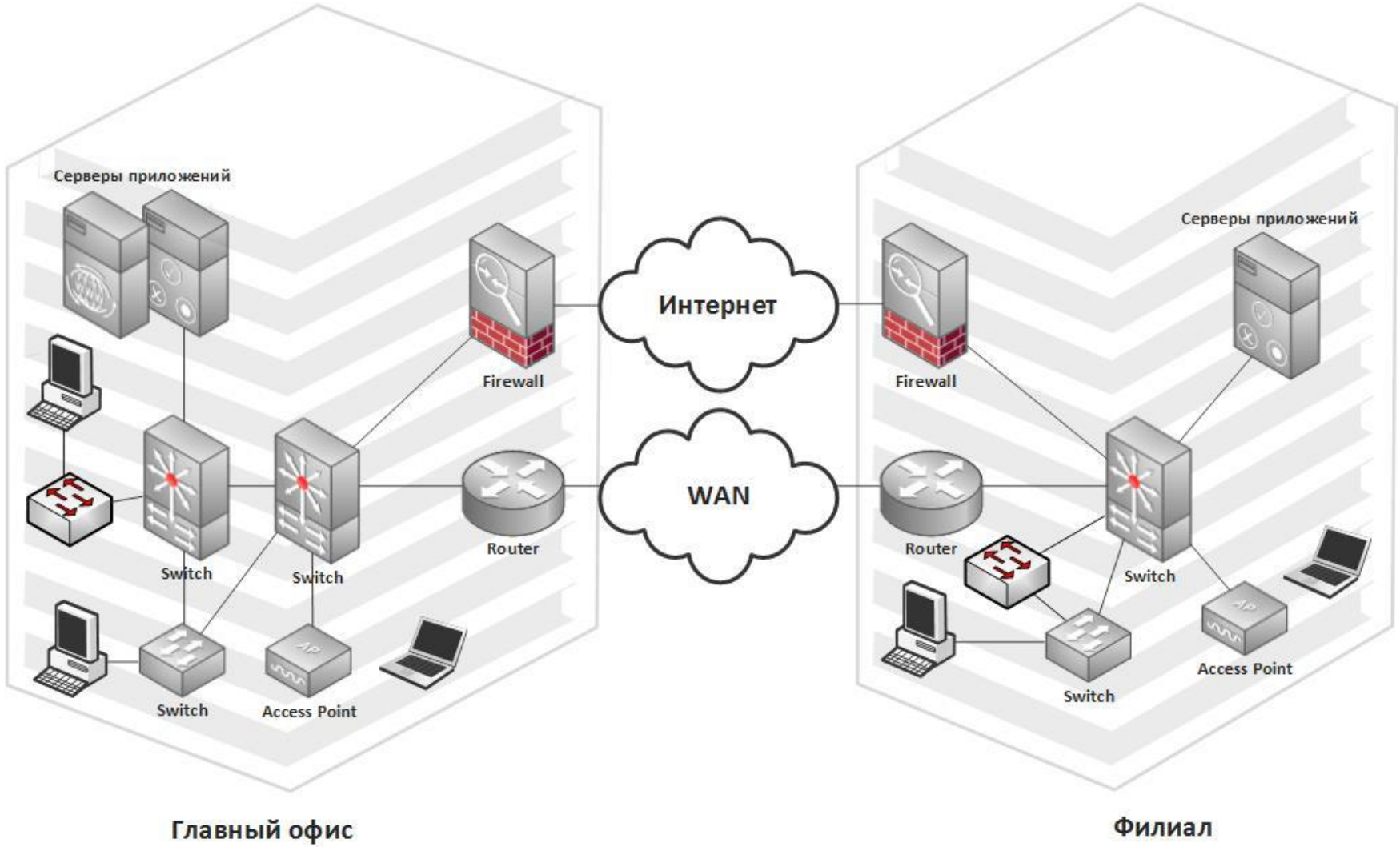
— Почему безопасность сетевой инфраструктуры так важна
— Какие сложности возникают при обеспечении безопасности
— Зачем нужна инвентаризация активов
— Что может показать аудит безопасности
— Что такое стандарт по безопасности для сетевых устройств

Особенности обеспечения безопасности сетевой инфраструктуры

Почему это важно?

— Компьютерные сети распространены повсеместно
— Зависимость от ресурсов сети чрезмерная
— Защита ресурсов начинается с защиты сети

Типичный пример сети



Сложности

— Разнообразие сетевого оборудования от различных производителей
  - Cisco
  - Juniper
  - Huawei
  - Alcatel
— Большой размер сети
— Динамичность сети
  - Новые устройства
  - Изменение конфигурации

Проблемы

Много единиц оборудования

Различные производители оборудования

Ошибки в администрировании

Бреши в безопасности

Решение есть!

— Инструкций по безопасной настройке достаточно
— Информация об уязвимостях публикуется
— Рекомендации по устранению уязвимостей доступны
— Стандартов по безопасности и рекомендаций тоже много

Решение есть?

- Информация об уязвимостях публикуется

TOTAL CVEs: 49264

NIST National Institute of Standards and Technology

- Рекомендации по устранению доступны

KNOWLEDGE BASE

Cisco Blogs

SECURITY INTELLIGENCE CENTER

- Инструкций по безопасной настройке достаточно

SANS

how to secure network

Результатов: примерно 595 000 000 (0,13 сек.)

- Стандартов по безопасности и рекомендаций тоже много

Что делать?

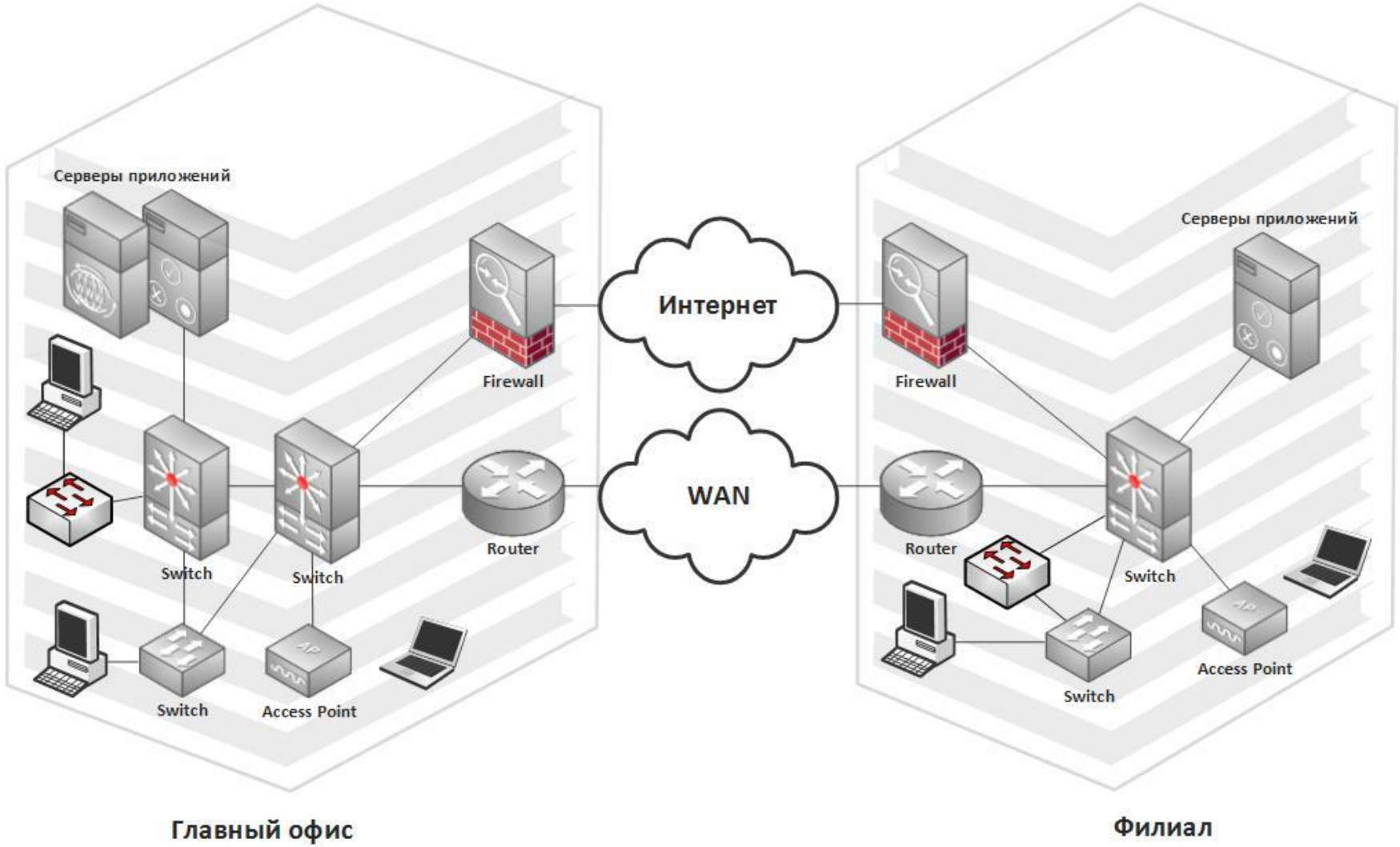
— Много различного оборудования
  - База знаний с самым лучшим и полезным

— Ошибки в администрировании
  - Автоматизация процесса аудита безопасности

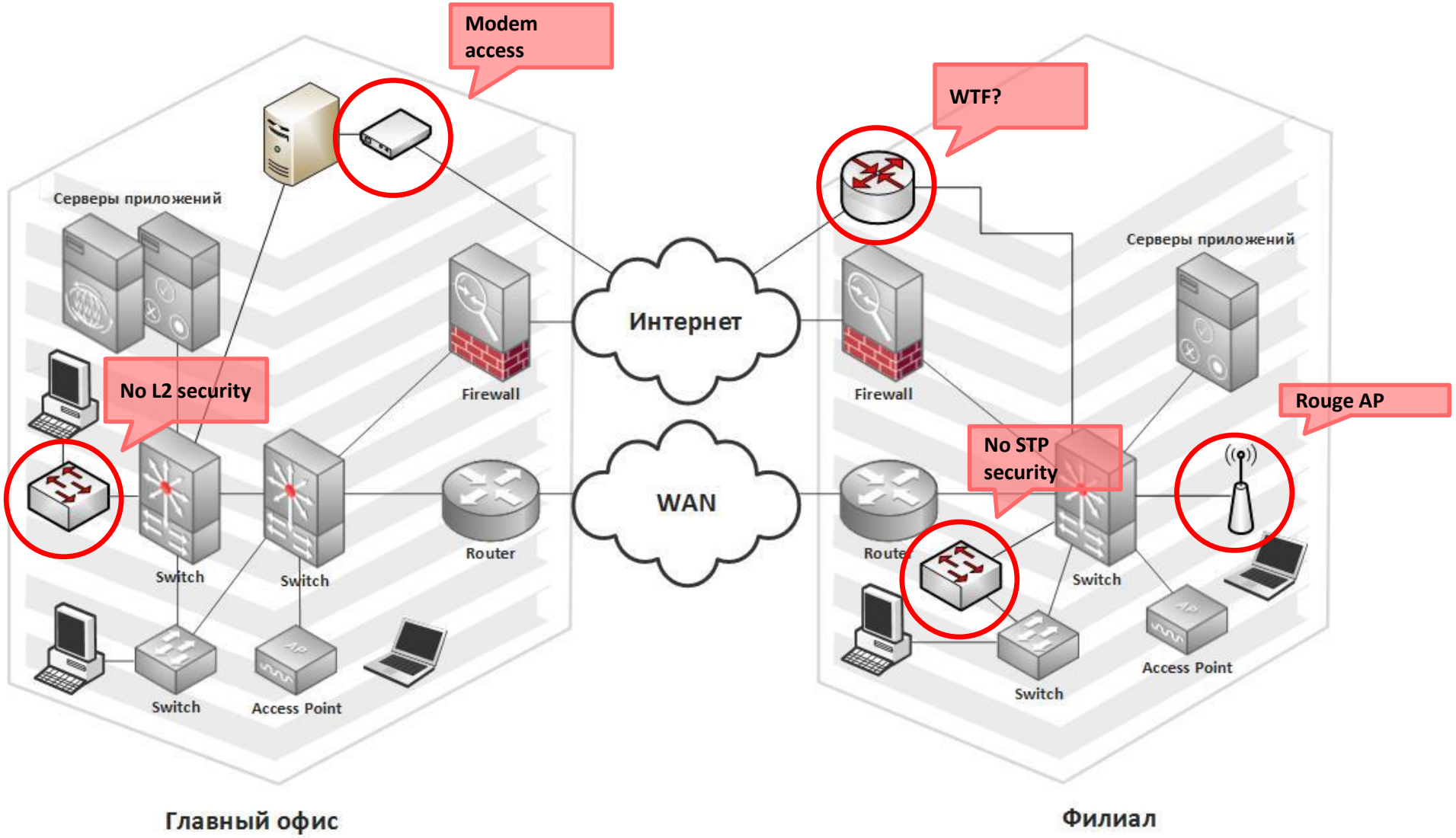
— Бреши в безопасности
  - Рекомендации аудита
  - Автоматизация процесса контроля соответствия стандартам по безопасности

Как это делается:
Инвентаризация активов

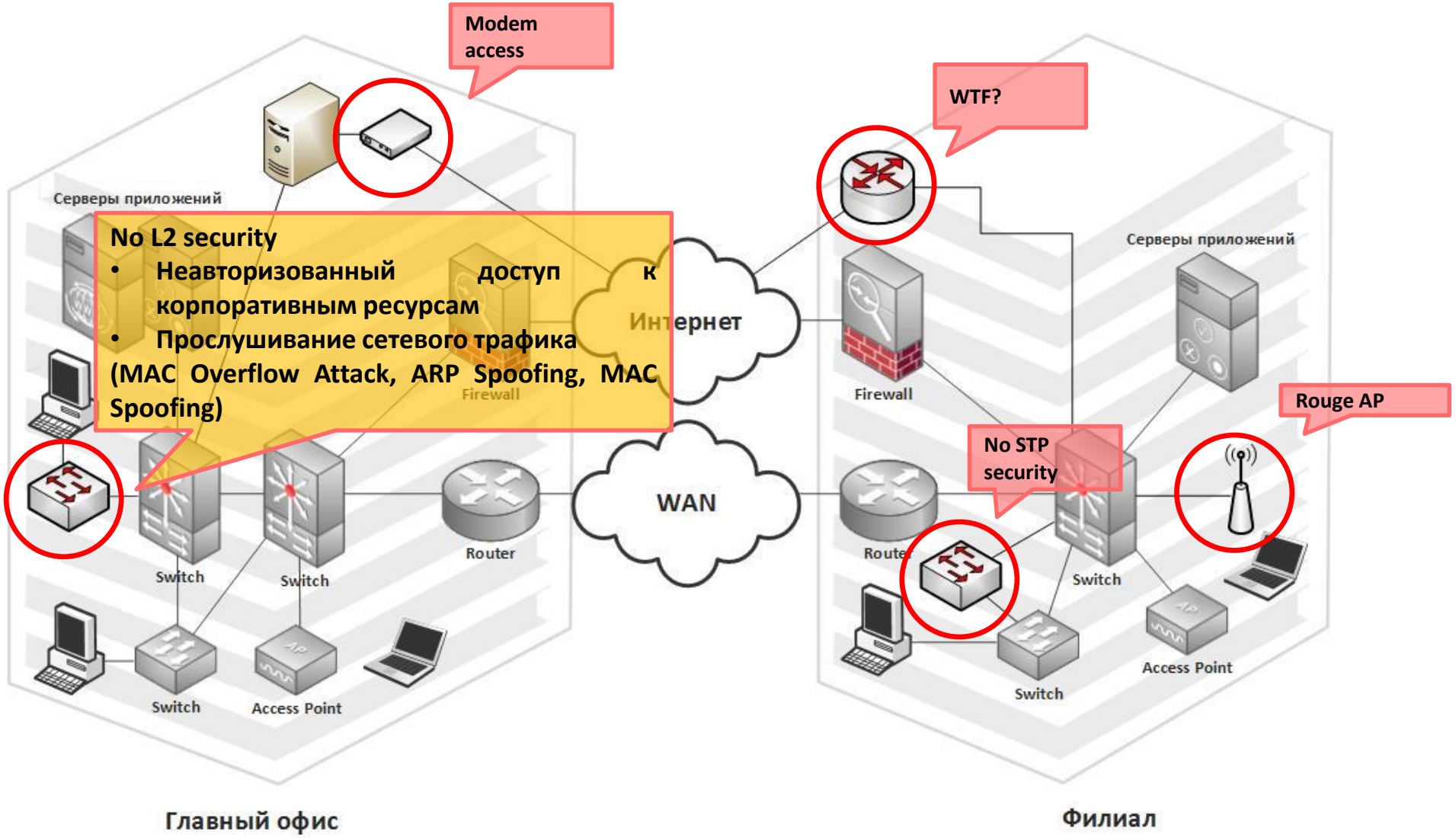
Инвентаризация активов



Результаты инвентаризации активов

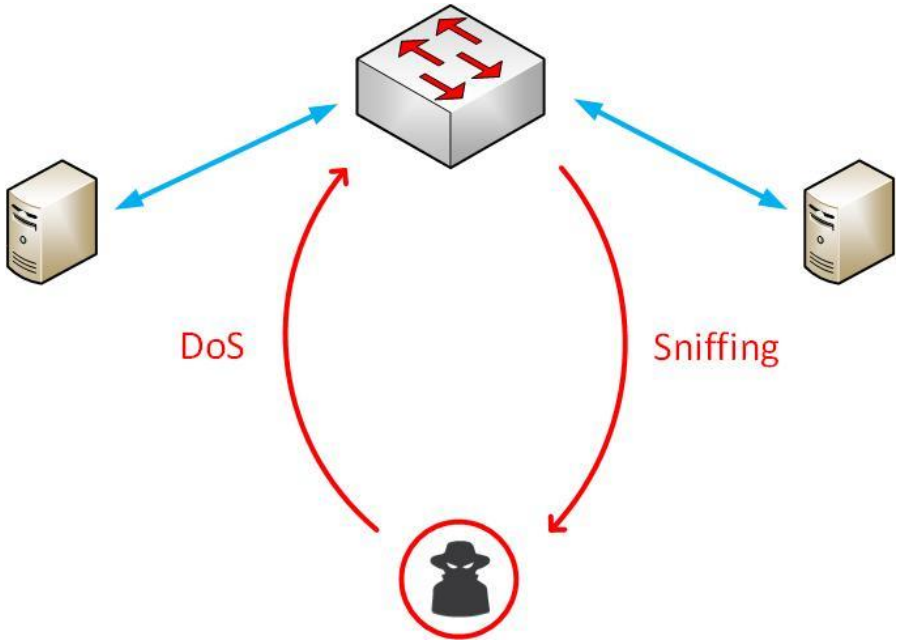


Результаты инвентаризации активов



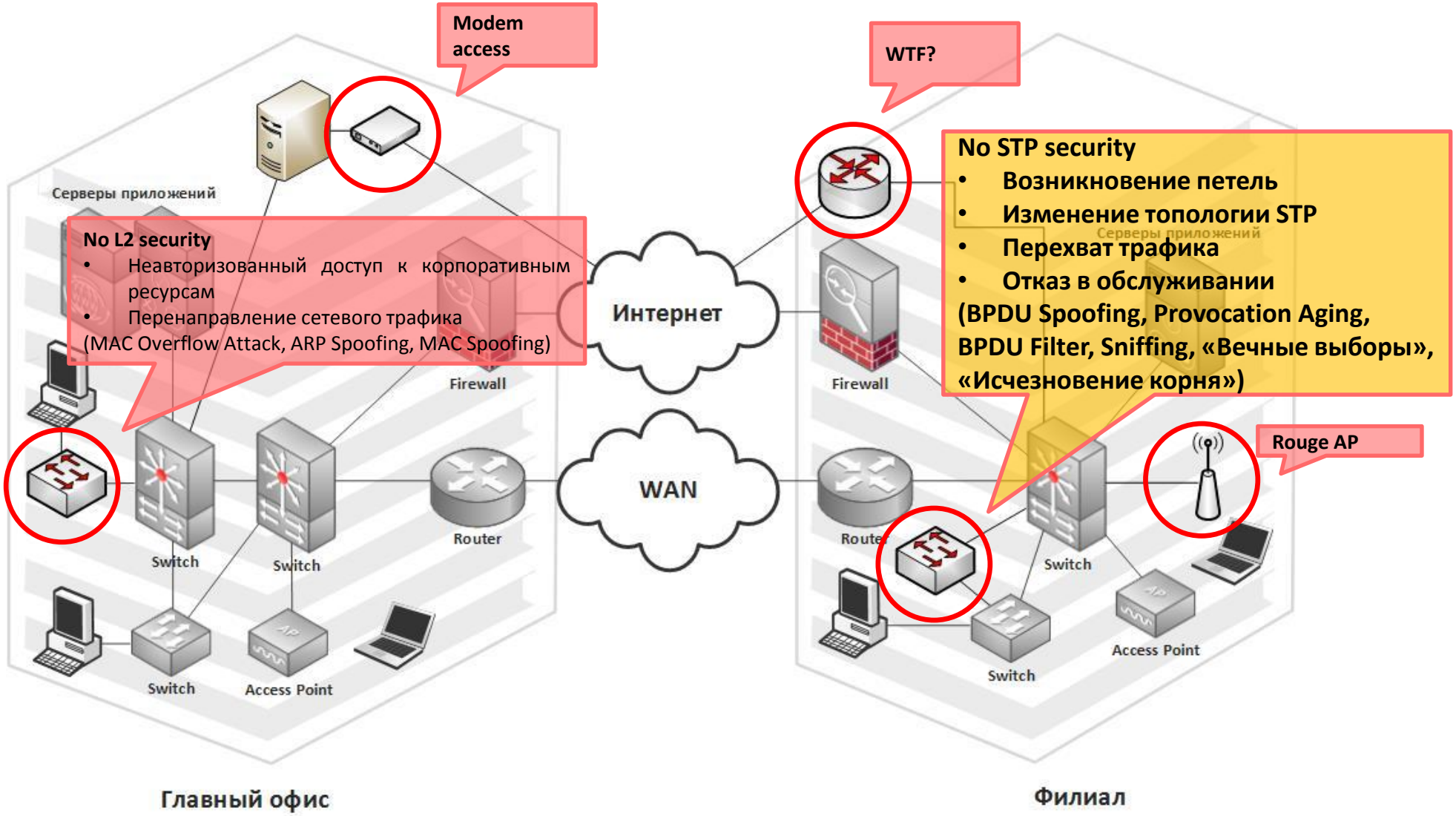
Эксплуатация

MAC Overflow



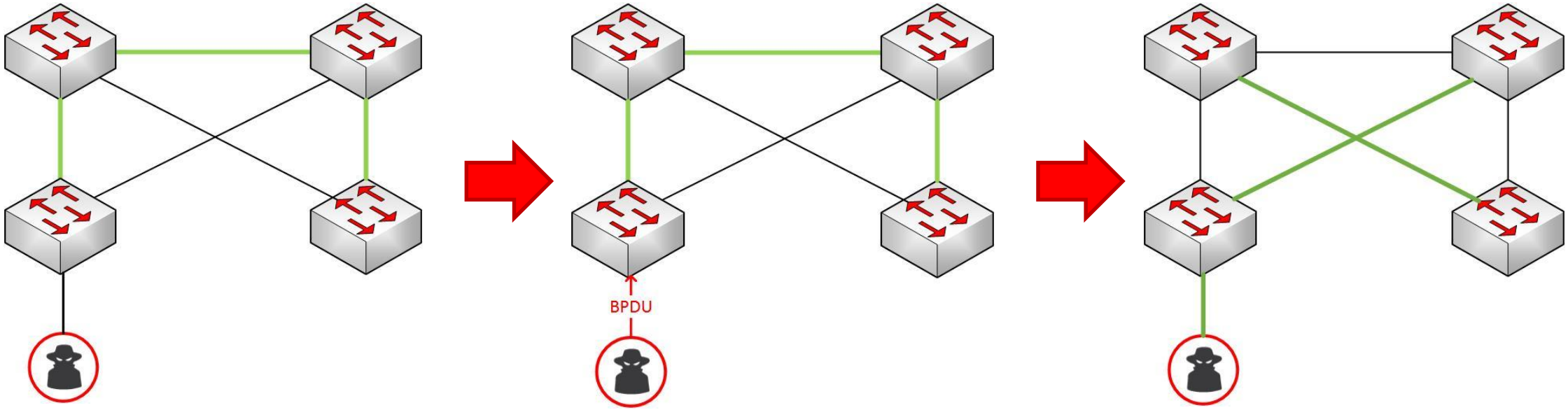

```
root@Kali:~# macof -d 192.168.197.2 -n 100000
24:cb:d7:5b:79:50 db:14:5a:74:a3:dd 0.0.0.0.945 > 192.168.197.2.13588: S 2075515
961:2075515961(0) win 512
5:9d:6d:39:be:f4 67:74:a6:2c:a5:51 0.0.0.0.21670 > 192.168.197.2.14225: S 164250
484:164250484(0) win 512
f9:38:1e:45:b3:2d 1c:ac:a:60:d8:4 0.0.0.0.40717 > 192.168.197.2.14800: S 4302105
56:430210556(0) win 512
59:fa:8a:20:26:92 50:95:6d:43:40:66 0.0.0.0.10551 > 192.168.197.2.28534: S 17016
87641:1701687641(0) win 512
81:35:a6:3d:da:cb bd:1c:3e:4a:de:3e 0.0.0.0.56250 > 192.168.197.2.24556: S 16253
63217:1625363217(0) win 512
e9:5d:a9:56:83:2b 8c:d0:1c:22:d3:8b 0.0.0.0.8284 > 192.168.197.2.38906: S 126634
4696:1266344696(0) win 512
4:70:3:47:43:68 55:2f:73:5f:a4:da 0.0.0.0.41198 > 192.168.197.2.45922: S 1821487
49:182148749(0) win 512
e3:eb:b6:70:de:d8 a1:15:37:5b:a6:6b 0.0.0.0.48306 > 192.168.197.2.21153: S 88656
0268:886560268(0) win 512
42:5:1a:29:d0:6a a6:c6:4c:c:c6:d3 0.0.0.0.65142 > 192.168.197.2.50799: S 1052961
908:1052961908(0) win 512
a5:2c:26:3a:32:43 ea:a9:99:2c:f4:5d 0.0.0.0.48839 > 192.168.197.2.27836: S 85649
8642:856498642(0) win 512
91:71:1a:1c:41:88 41:1b:16:10:bc:e7 0.0.0.0.1078 > 192.168.197.2.22677: S 145597
8937:1455978937(0) win 512
92:81:b5:13:24:23 97:bd:89:1d:48:74 0.0.0.0.17905 > 192.168.197.2.18236: S 12549
```

Результаты инвентаризации активов



Эксплуатация

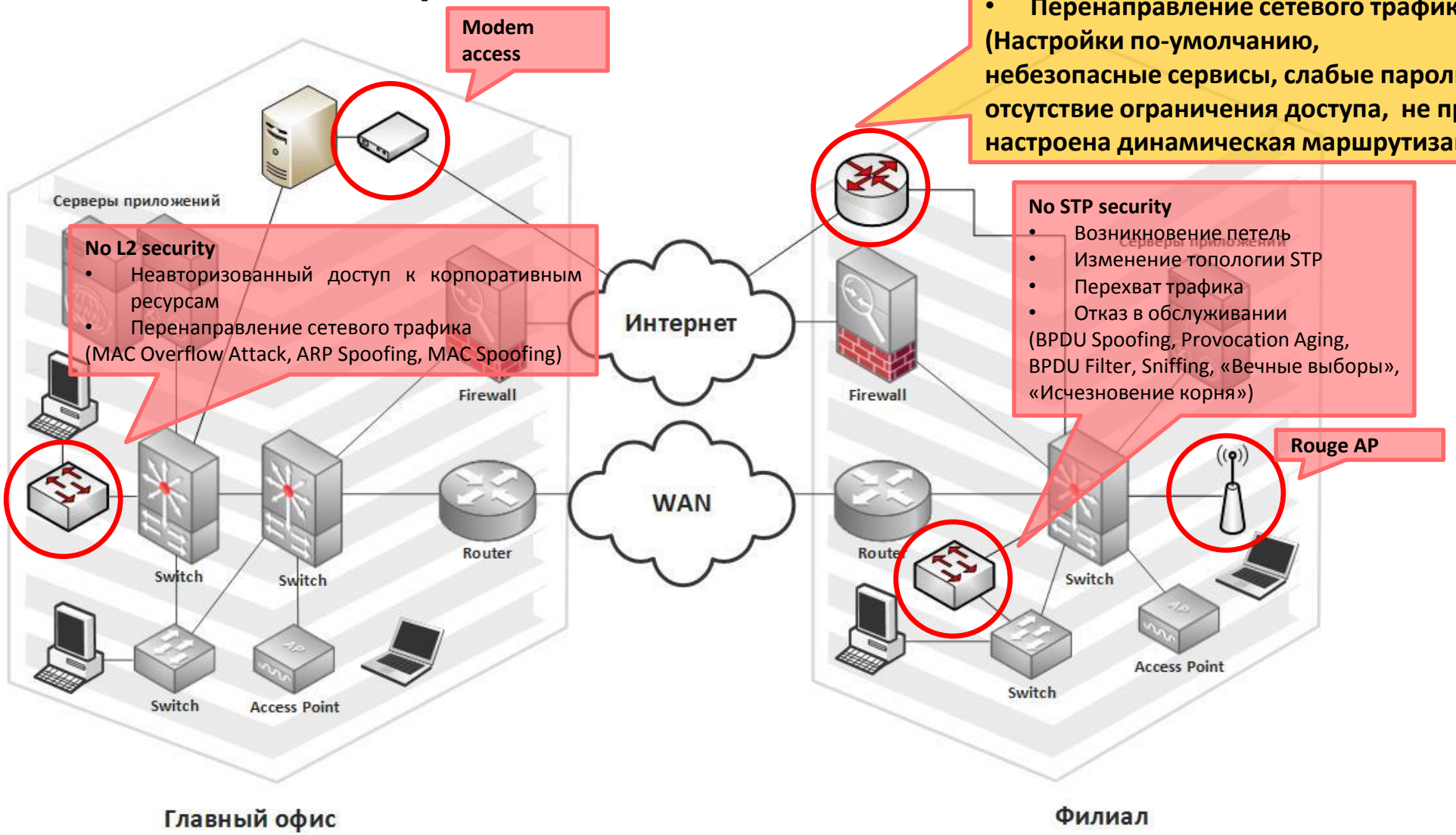
BPDU Spoofing



Результаты инвентаризации активов

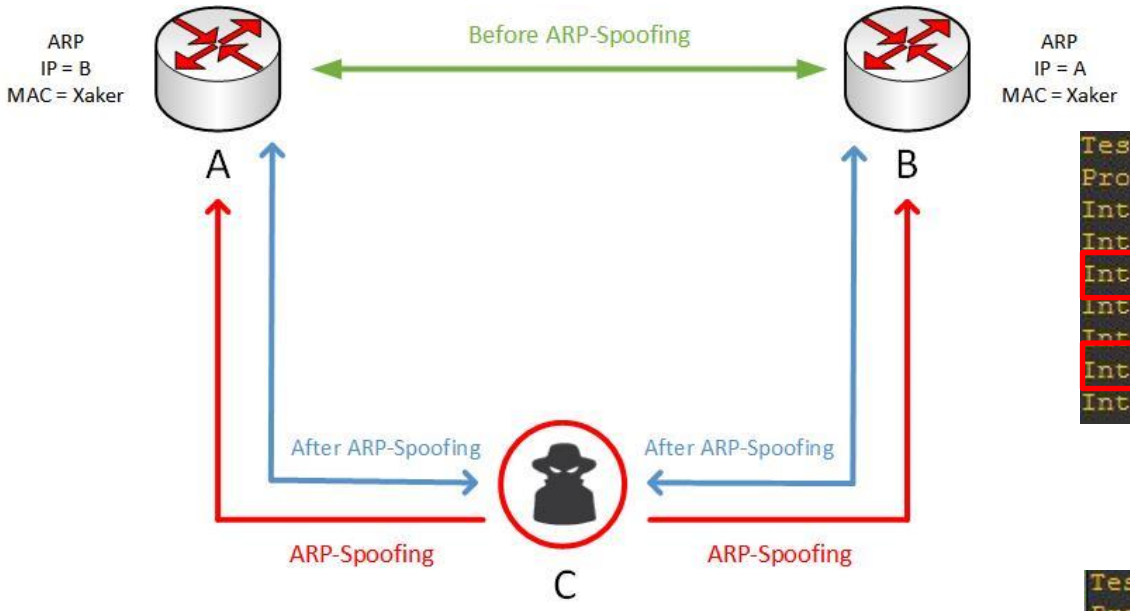
WTF?
- **Неавторизованный доступ к корпоративным ресурсам**
- **Перенаправление сетевого трафика**

(Настройки по-умолчанию, небезопасные сервисы, слабые пароли, отсутствие ограничения доступа, не правильно настроена динамическая маршрутизация)



Эксплуатация

ARP Spoofing




```
TestLab#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.0.1             75   ca01.1068.0008  ARPA   FastEthernet0/0
Internet  172.16.0.2              -   ca00.1068.0008  ARPA   FastEthernet0/0
Internet  192.168.197.1            0   0050.56c0.0008  ARPA   FastEthernet1/0
Internet  192.168.197.2            0   0050.56e2.65f1  ARPA   FastEthernet1/0
Internet  192.168.197.3            -   ca00.1068.001c  ARPA   FastEthernet1/0
Internet  192.168.197.128          2   000c.295a.e794  ARPA   FastEthernet1/0
Internet  192.168.197.254          0   0050.56f4.a172  ARPA   FastEthernet1/0
```

```
TestLab#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.0.1             91   ca01.1068.0008  ARPA   FastEthernet0/0
Internet  172.16.0.2              -   ca00.1068.0008  ARPA   FastEthernet0/0
Internet  192.168.197.1            0   000c.295a.e794  ARPA   FastEthernet1/0
Internet  192.168.197.2            0   0050.56e2.65f1  ARPA   FastEthernet1/0
Internet  192.168.197.3            -   ca00.1068.001c  ARPA   FastEthernet1/0
Internet  192.168.197.128          0   000c.295a.e794  ARPA   FastEthernet1/0
Internet  192.168.197.254         10   0050.56f4.a172  ARPA   FastEthernet1/0
```

Результаты инвентаризации активов

Modem Access
- **Неавторизованный доступ к корпоративным ресурсам**

(Отсутствие ограничения доступа)

WTF?
- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика

(Настройки по-умолчанию, небезопасные сервисы, слабые пароли, отсутствие ограничения доступа, не правильно настроена динамическая маршрутизация)

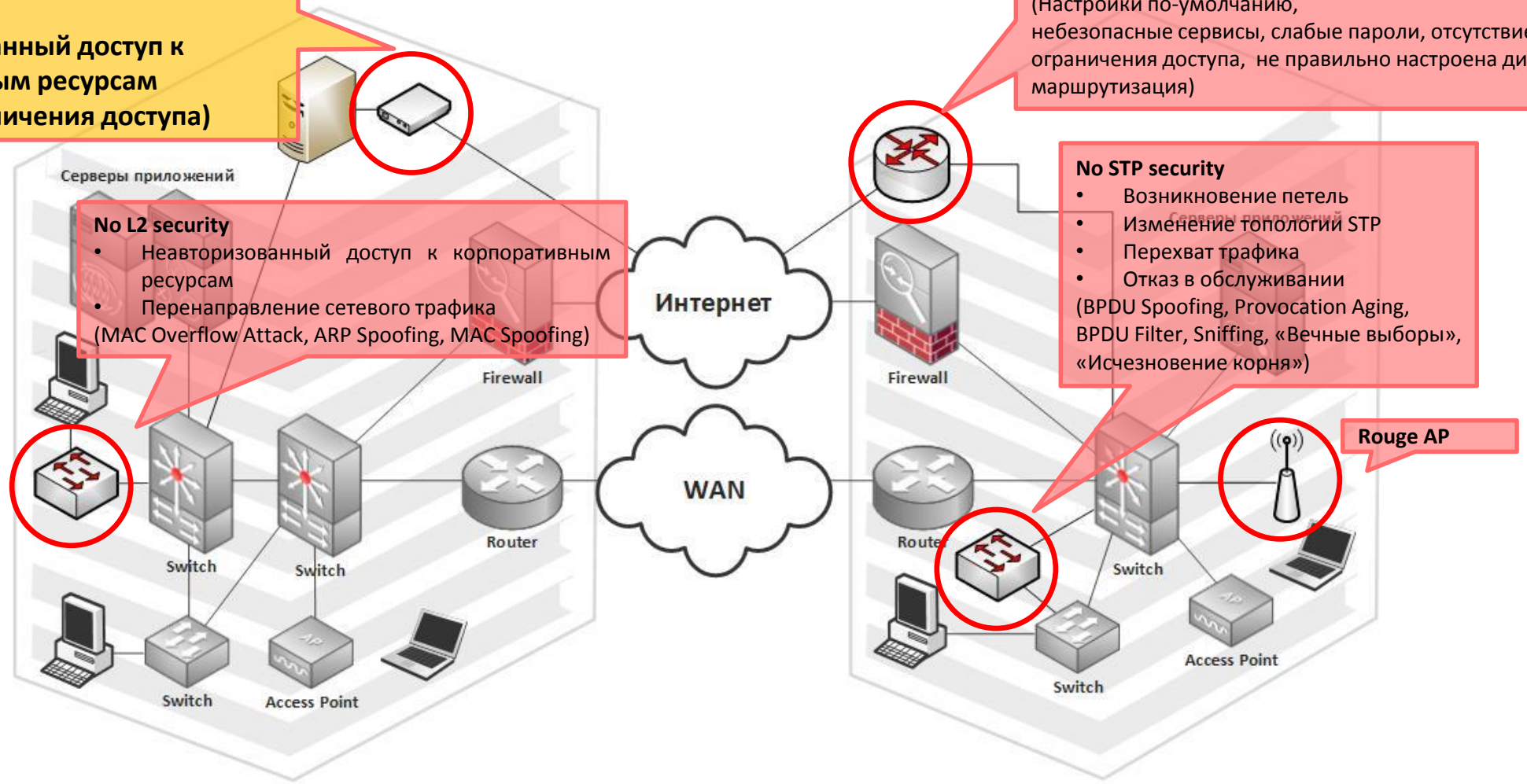
No L2 security
- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика

(MAC Overflow Attack, ARP Spoofing, MAC Spoofing)

No STP security
- Возникновение петель
- Изменение топологии STP
- Перехват трафика
- Отказ в обслуживании

(BPDU Spoofing, Provocation Aging, BPDU Filter, Sniffing, «Вечные выборы», «Исчезновение корня»)

Rouge AP



Результаты инвентаризации активов

Modem Access
- Неавторизованный доступ к корпоративным ресурсам

(Отсутствие ограничения доступа)

WTF?
- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика

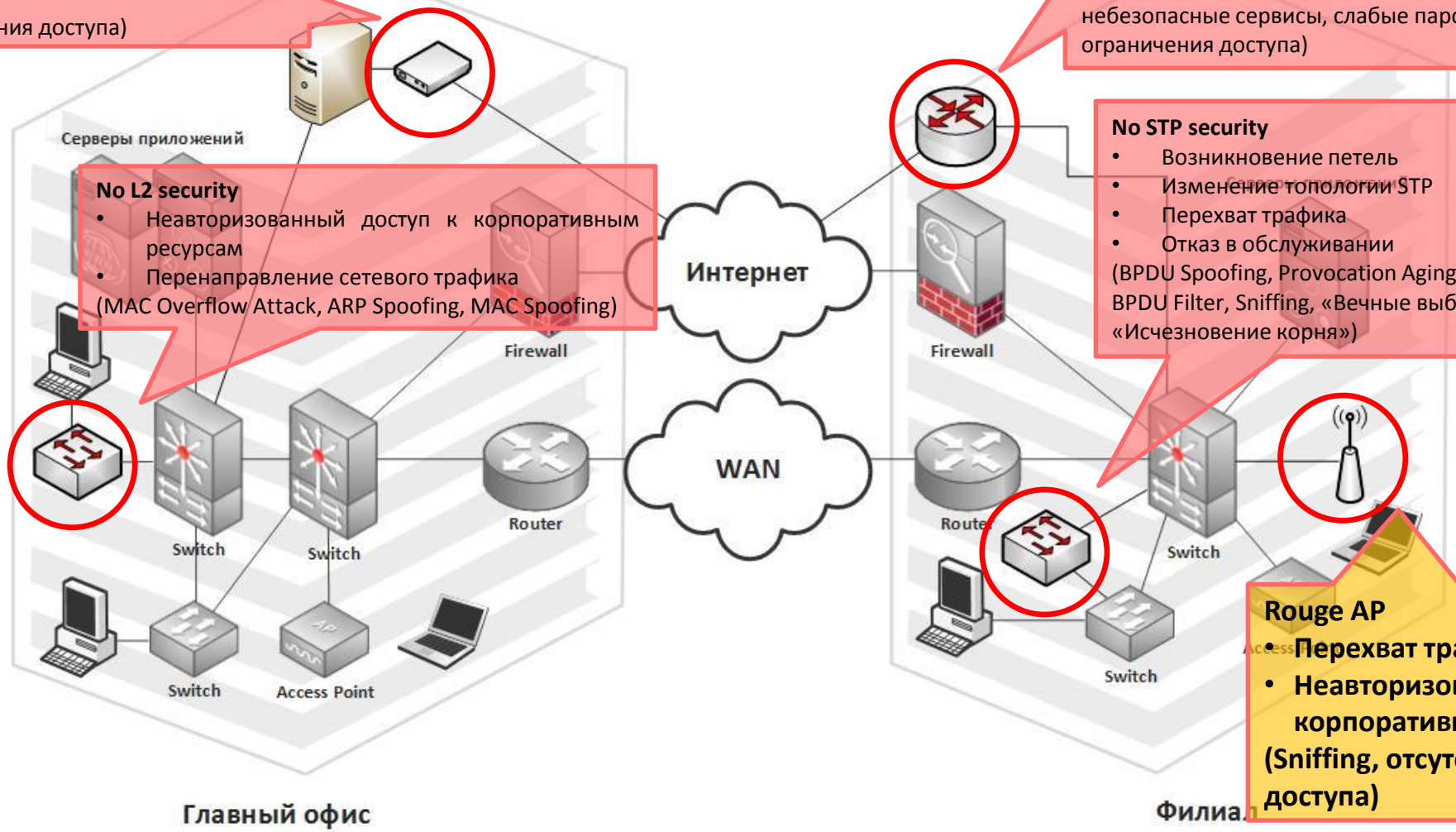
(Настройки по-умолчанию, небезопасные сервисы, слабые пароли, отсутствие ограничения доступа)

No L2 security
- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика

(MAC Overflow Attack, ARP Spoofing, MAC Spoofing)

No STP security
- Возникновение петель
- Изменение топологии STP
- Перехват трафика
- Отказ в обслуживании

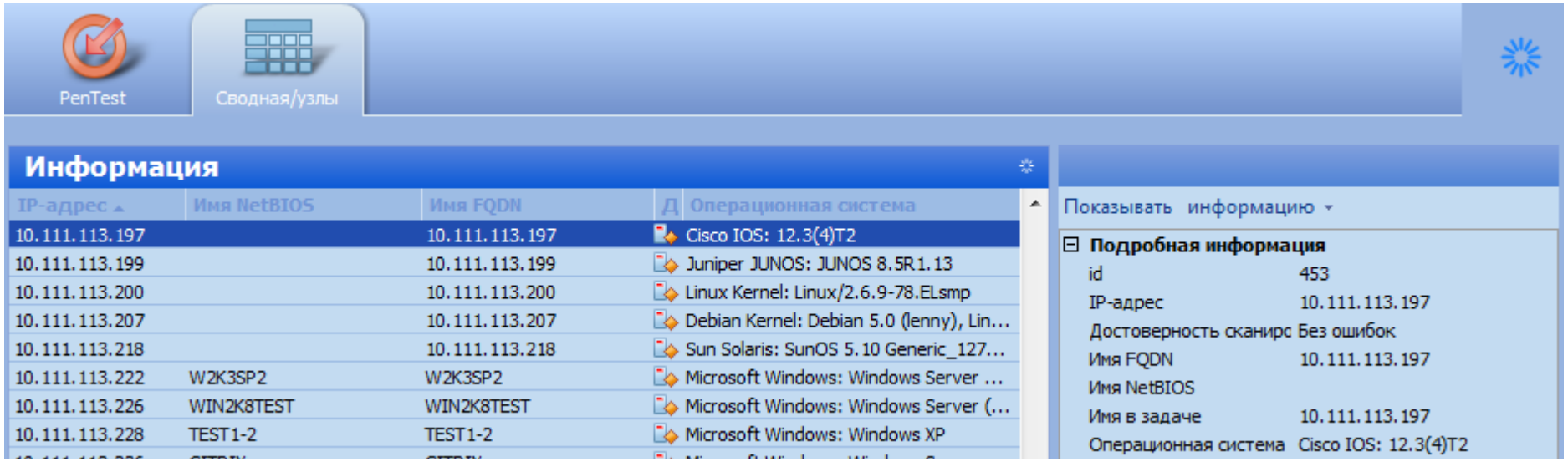
(BPDU Spoofing, Provocation Aging, BPDU Filter, Sniffing, «Вечные выборы», «Исчезновение корня»)



Rouge AP
- **Перехват трафика**
- **Неавторизованный доступ к корпоративным ресурсам**

(Sniffing, отсутствие ограничения доступа)

Результаты инвентаризация активов



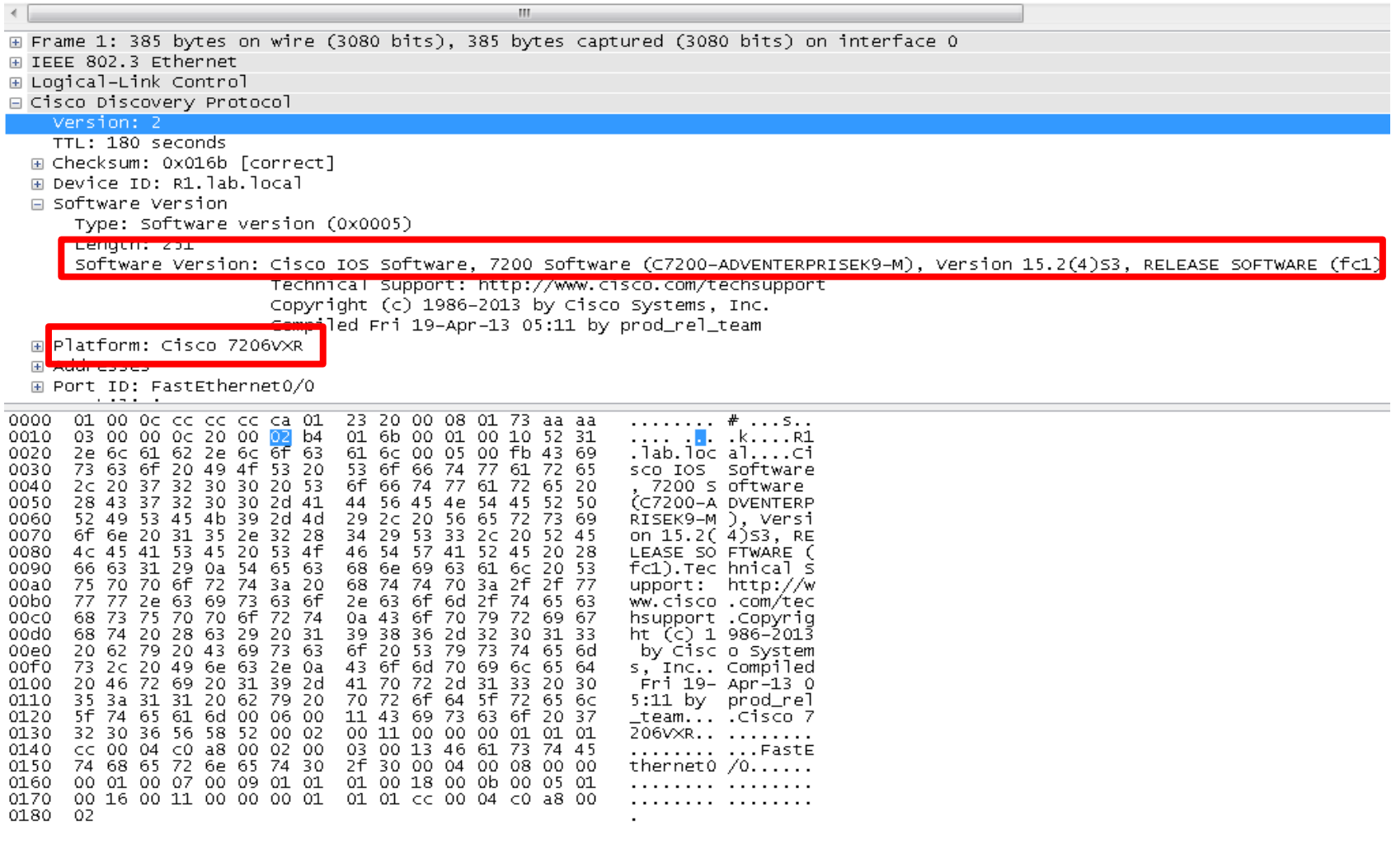
Как это делается:

Аудит безопасности

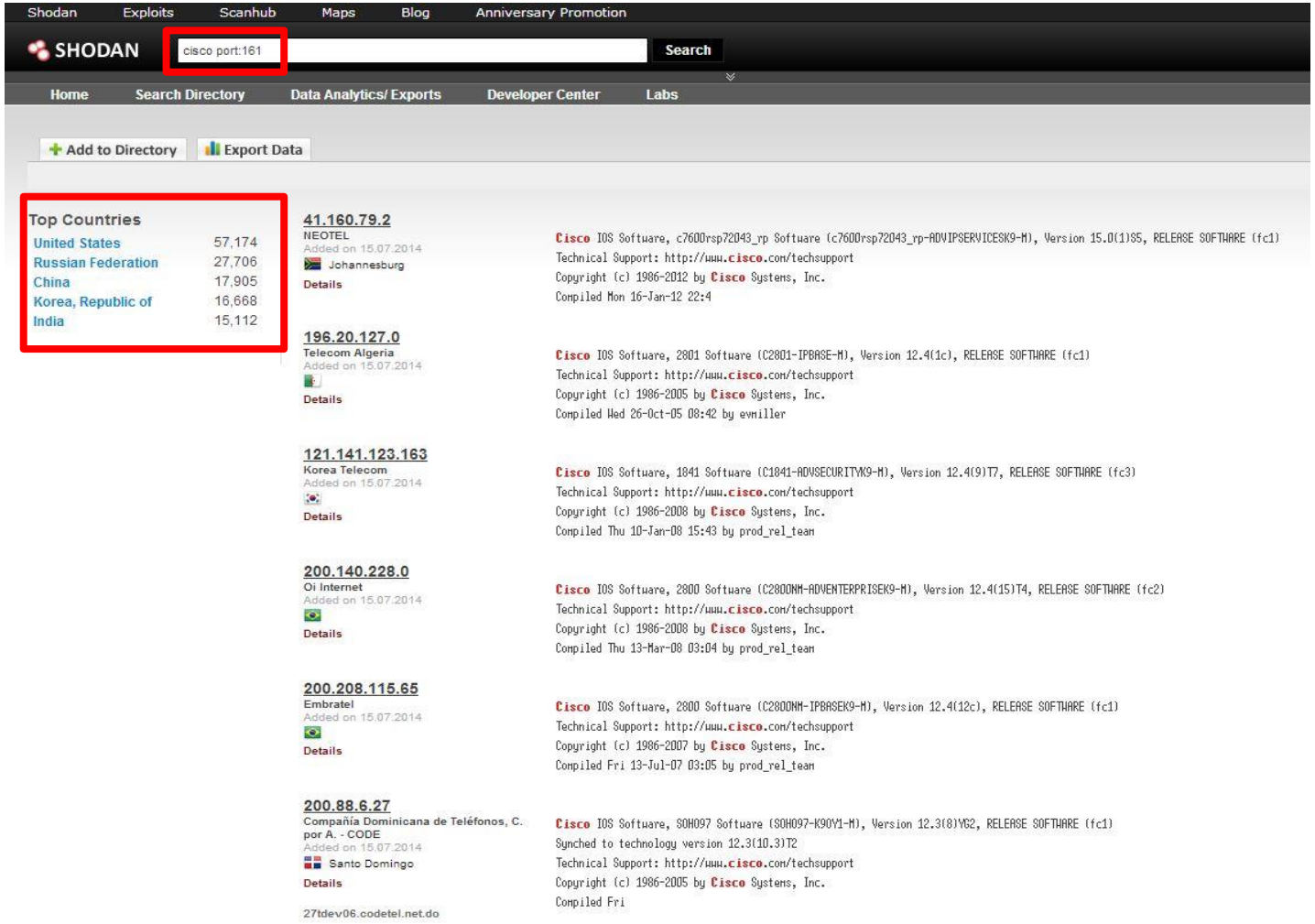
Основные причины брешей в безопасности

— Отсутствие или слабый контроль доступа к корпоративной инфраструктуре
  - Слабая парольная политика
  - Отсутствие ограничения доступа
— Небезопасные сервисы или сервисы с настройками по-умолчанию
  - CDP
  - HTTP
  - Finger
  - SNMP
— Ошибки в настройке оборудования
— Уязвимости в протоколах и ОС

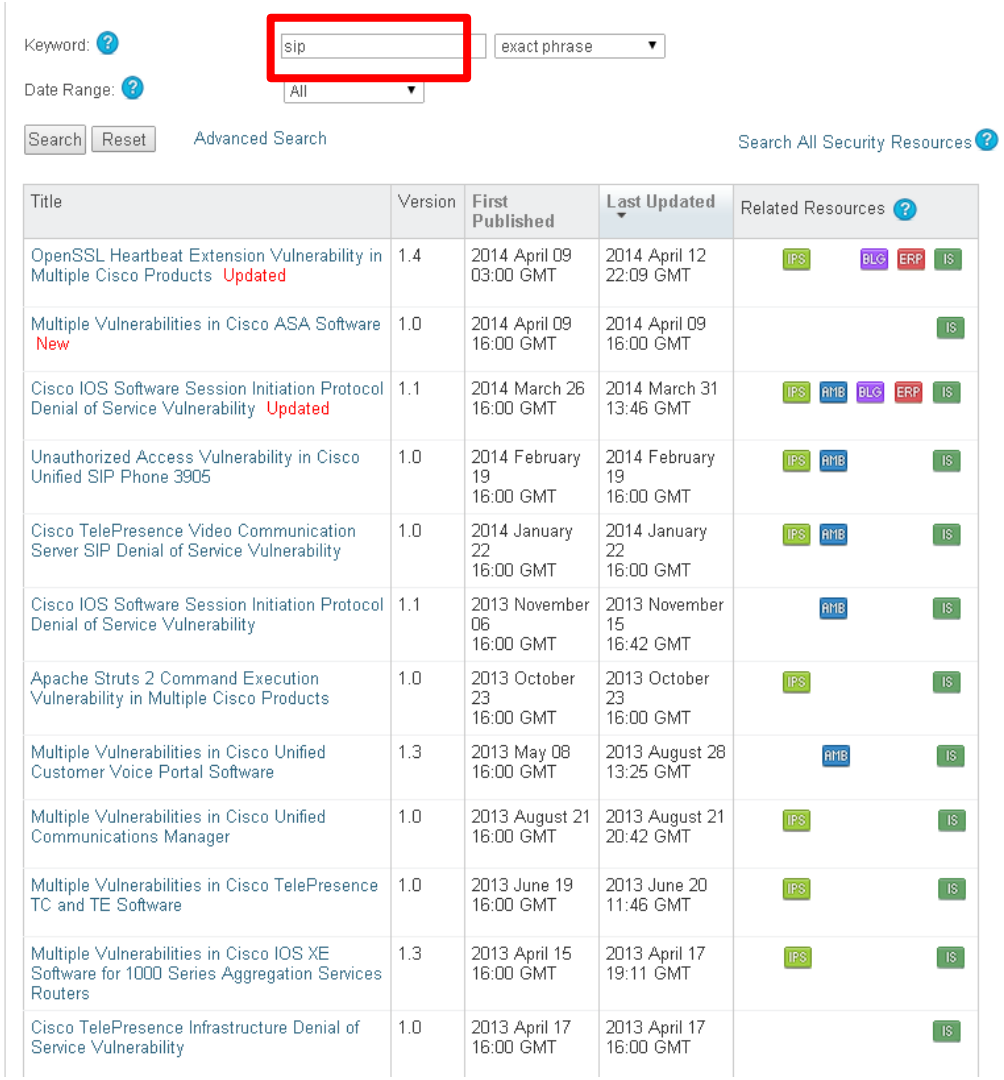
Небезопасные сервисы или сервисы с настройками по-умолчанию



Ошибки в настройке оборудования



Уязвимости в протоколах и ОС



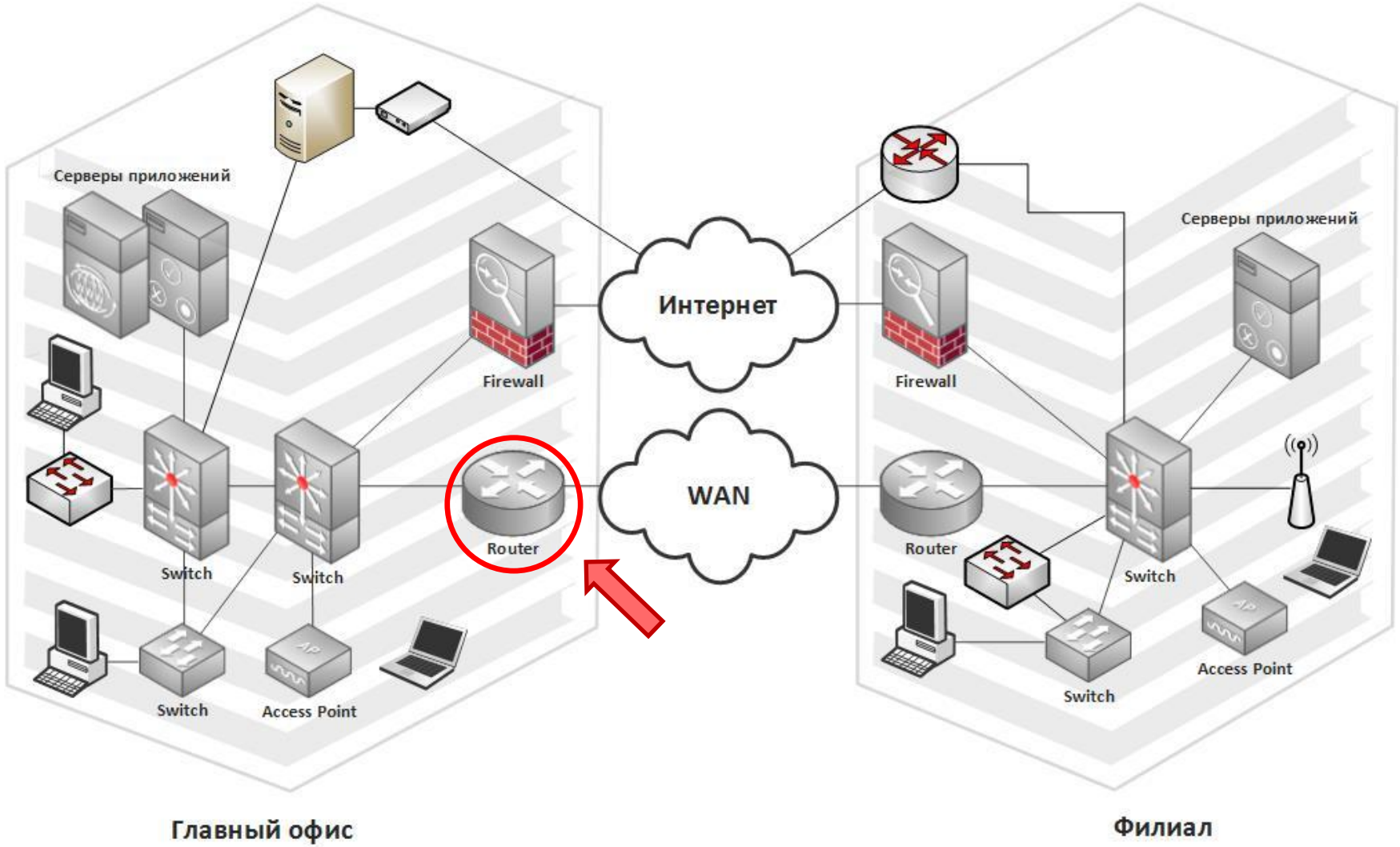
Keyword: sip exact phrase

Date Range: All

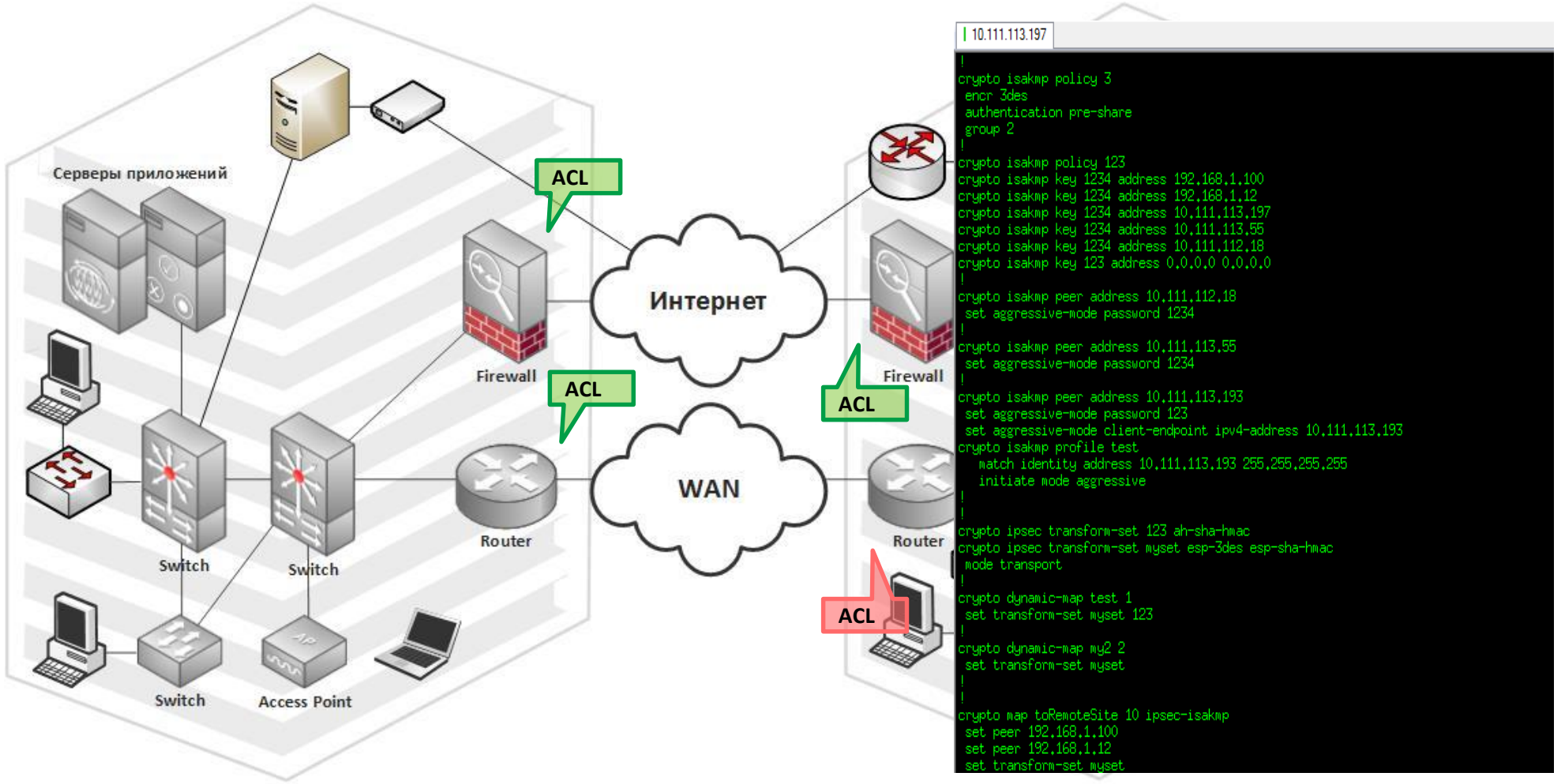
Search Reset Advanced Search Search All Security Resources

Title	Version	First Published	Last Updated	Related Resources
OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products Updated	1.4	2014 April 09 03:00 GMT	2014 April 12 22:09 GMT	IPS BLG ERP IS
Multiple Vulnerabilities in Cisco ASA Software New	1.0	2014 April 09 16:00 GMT	2014 April 09 16:00 GMT	IS
Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability Updated	1.1	2014 March 26 16:00 GMT	2014 March 31 13:46 GMT	IPS AMB BLG ERP IS
Unauthorized Access Vulnerability in Cisco Unified SIP Phone 3905	1.0	2014 February 19 16:00 GMT	2014 February 19 16:00 GMT	IPS AMB IS
Cisco TelePresence Video Communication Server SIP Denial of Service Vulnerability	1.0	2014 January 22 16:00 GMT	2014 January 22 16:00 GMT	IPS AMB IS
Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability	1.1	2013 November 06 16:00 GMT	2013 November 15 16:42 GMT	AMB IS
Apache Struts 2 Command Execution Vulnerability in Multiple Cisco Products	1.0	2013 October 23 16:00 GMT	2013 October 23 16:00 GMT	IPS IS
Multiple Vulnerabilities in Cisco Unified Customer Voice Portal Software	1.3	2013 May 08 16:00 GMT	2013 August 28 13:25 GMT	AMB IS
Multiple Vulnerabilities in Cisco Unified Communications Manager	1.0	2013 August 21 16:00 GMT	2013 August 21 20:42 GMT	IPS IS
Multiple Vulnerabilities in Cisco TelePresence TC and TE Software	1.0	2013 June 19 16:00 GMT	2013 June 20 11:46 GMT	IPS IS
Multiple Vulnerabilities in Cisco IOS XE Software for 1000 Series Aggregation Services Routers	1.3	2013 April 15 16:00 GMT	2013 April 17 19:11 GMT	IPS IS
Cisco TelePresence Infrastructure Denial of Service Vulnerability	1.0	2013 April 17 16:00 GMT	2013 April 17 16:00 GMT	IS

Как это делается вручную

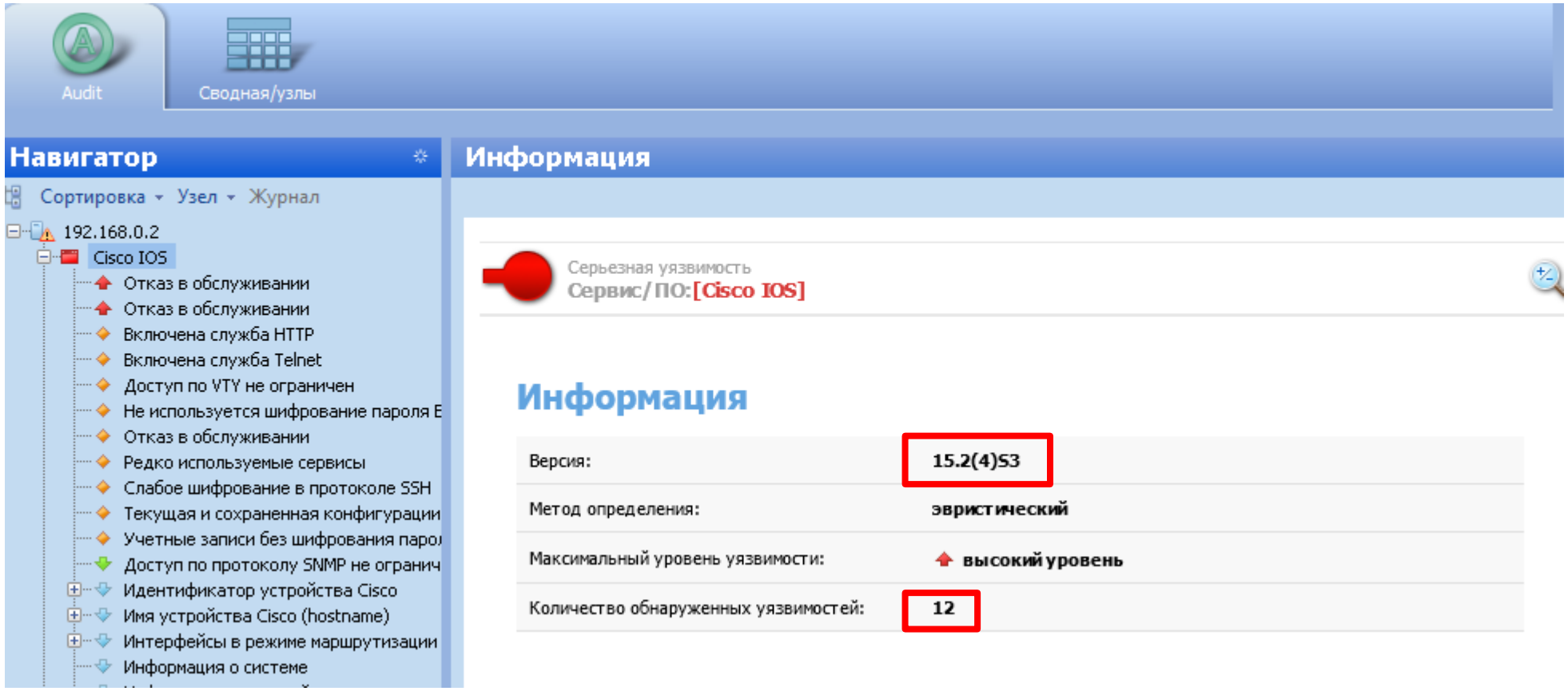


Ручной аудит

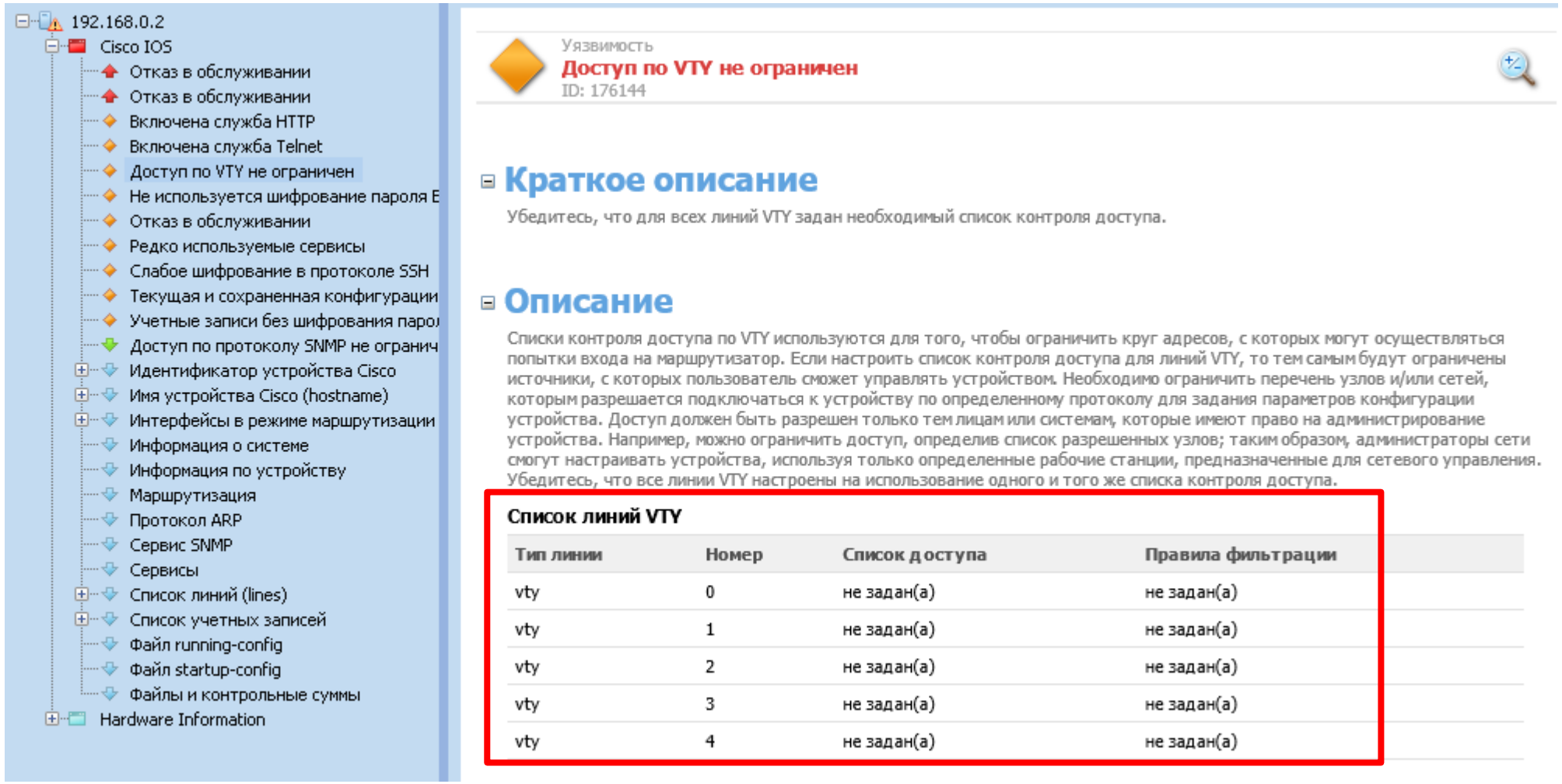



```
10.111.113.197
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 123
crypto isakmp key 1234 address 192.168.1.100
crypto isakmp key 1234 address 192.168.1.12
crypto isakmp key 1234 address 10.111.113.197
crypto isakmp key 1234 address 10.111.113.55
crypto isakmp key 1234 address 10.111.112.18
crypto isakmp key 123 address 0.0.0.0 0.0.0.0
!
crypto isakmp peer address 10.111.112.18
 set aggressive-mode password 1234
!
crypto isakmp peer address 10.111.113.55
 set aggressive-mode password 1234
!
crypto isakmp peer address 10.111.113.193
 set aggressive-mode password 123
 set aggressive-mode client-endpoint ipv4-address 10.111.113.193
crypto isakmp profile test
   match identity address 10.111.113.193 255.255.255.255
   initiate mode aggressive
!
!
crypto ipsec transform-set 123 ah-sha-hmac
crypto ipsec transform-set myset esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map test 1
 set transform-set myset 123
!
crypto dynamic-map my2 2
 set transform-set myset
!
!
crypto map toRemoteSite 10 ipsec-isakmp
 set peer 192.168.1.100
 set peer 192.168.1.12
 set transform-set myset
```

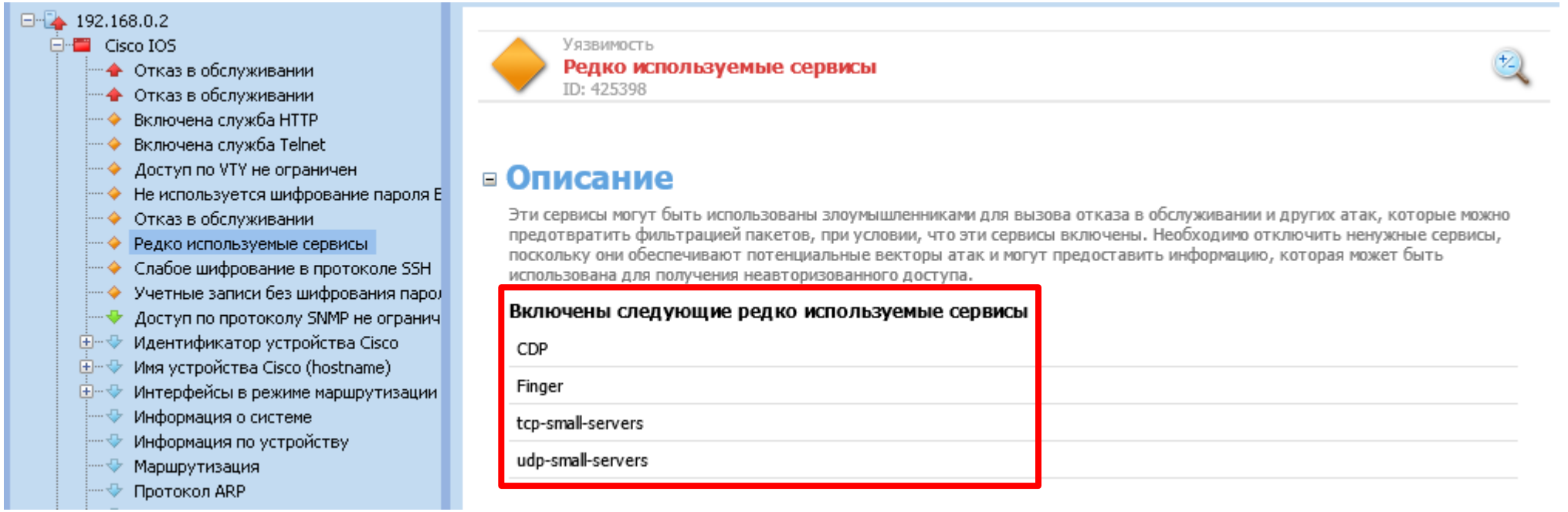
Автоматизация аудита безопасности



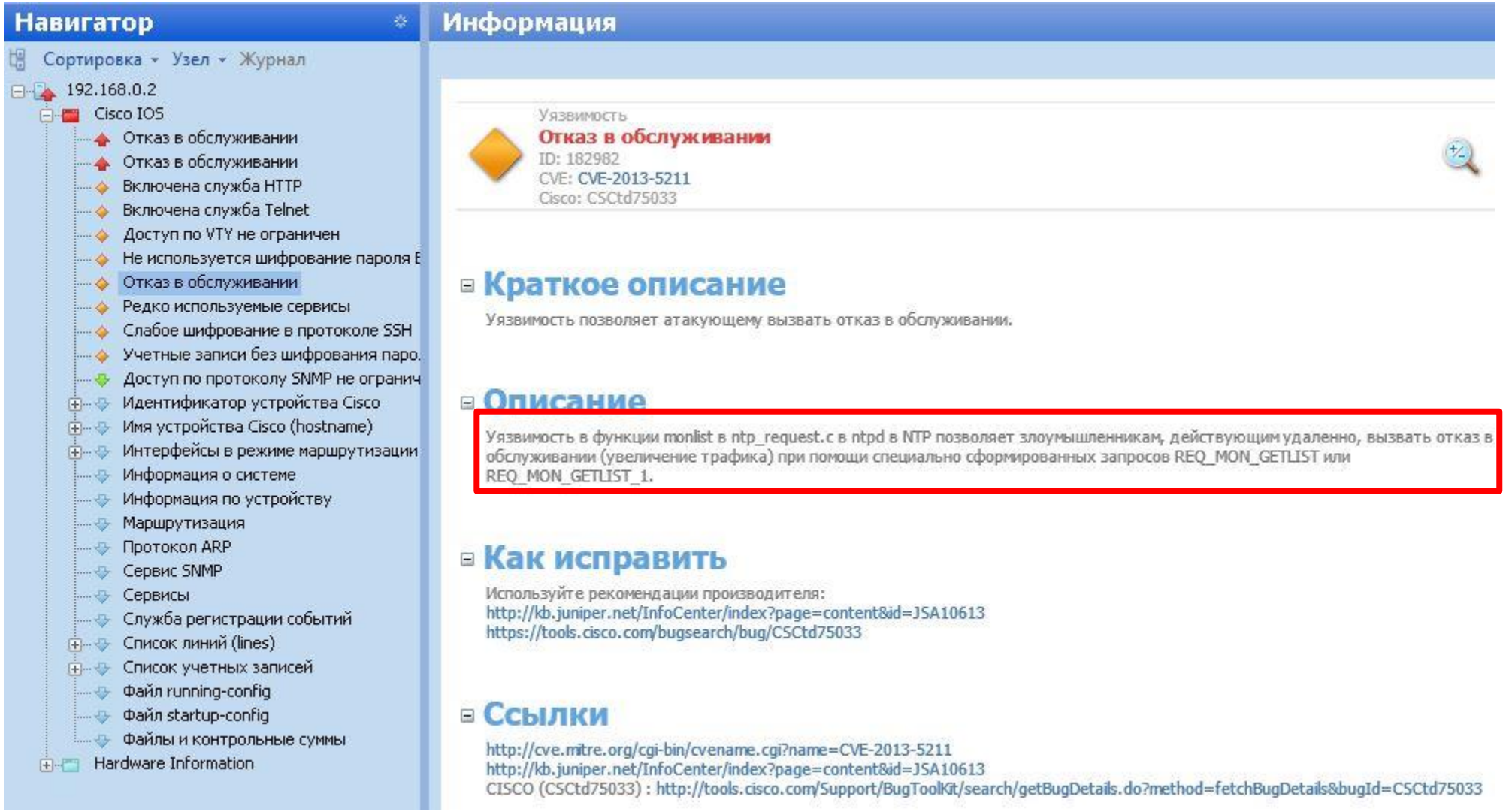
Результаты аудита безопасности



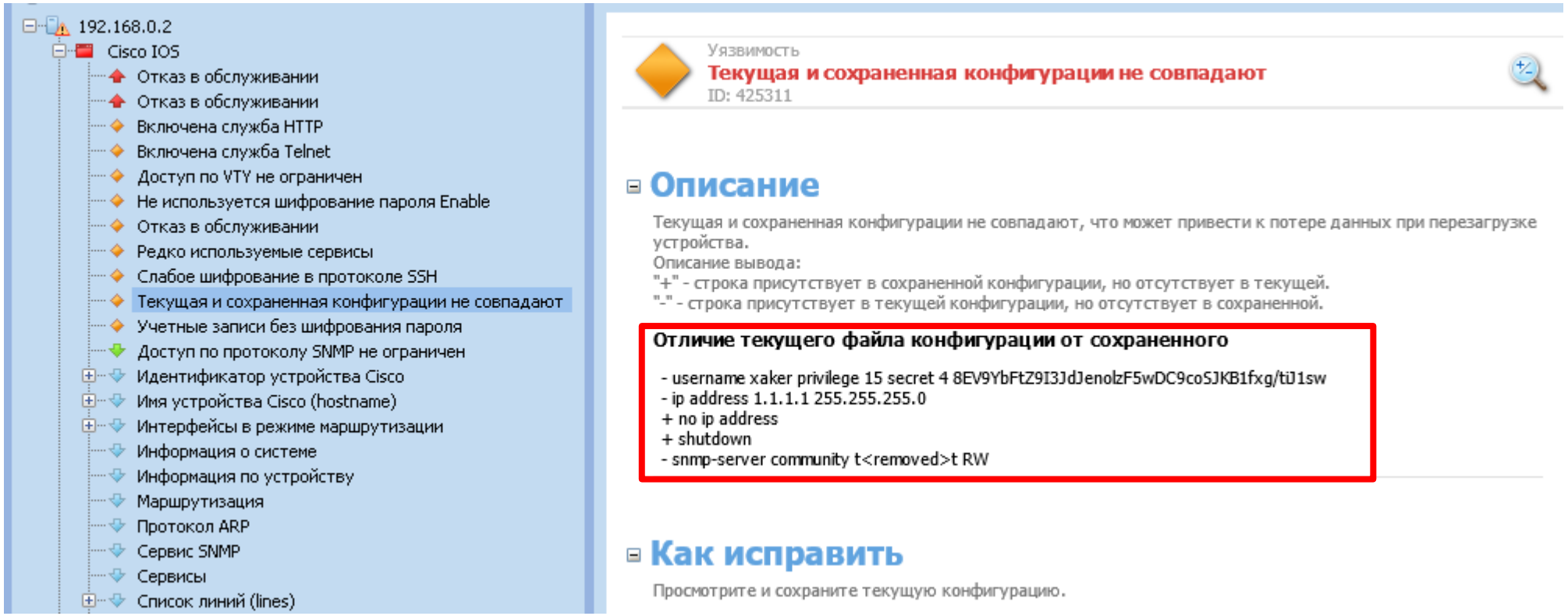
Результаты аудита безопасности



Результаты аудита безопасности



Результаты аудита безопасности



Как это делается:

Соответствие стандартам по безопасности

Требования и стандарты по безопасности

— Готовые стандарты

- Security Configuration Benchmark for Juniper JUNOS
- Security Configuration Benchmark for Cisco IOS
- Security Configuration Benchmark for Cisco Firewall Devices

— Собственные требования

- Версия программного обеспечения
- Парольная политика
- Сервисы аутентификации
- Правила фильтрации
- Регистрация событий

Security Configuration Benchmark for Cisco IOS

Группы проверок:

— Authentication, Authorization and Accounting (AAA)
— SNMP
— Global Services (CDP, DHCP, HTTP)
— Logging
— Neighbor Authentication (OSPF, EIGRP, RIP)

Проверка SNMP – Требование стандарта

Remediation:
Disable the default SNMP community string "private"

IOS:

```
hostname(config)#no snmp-server community {private}
```

Audit:
Perform the following to determine if the private community string is enabled:

IOS:

1. Ensure `private` does not show as a result

```
hostname# show snmp community
```

Настройки на устройстве

```
!
snmp-server community verystrongcommunity RO
snmp-server community private RW
!
```

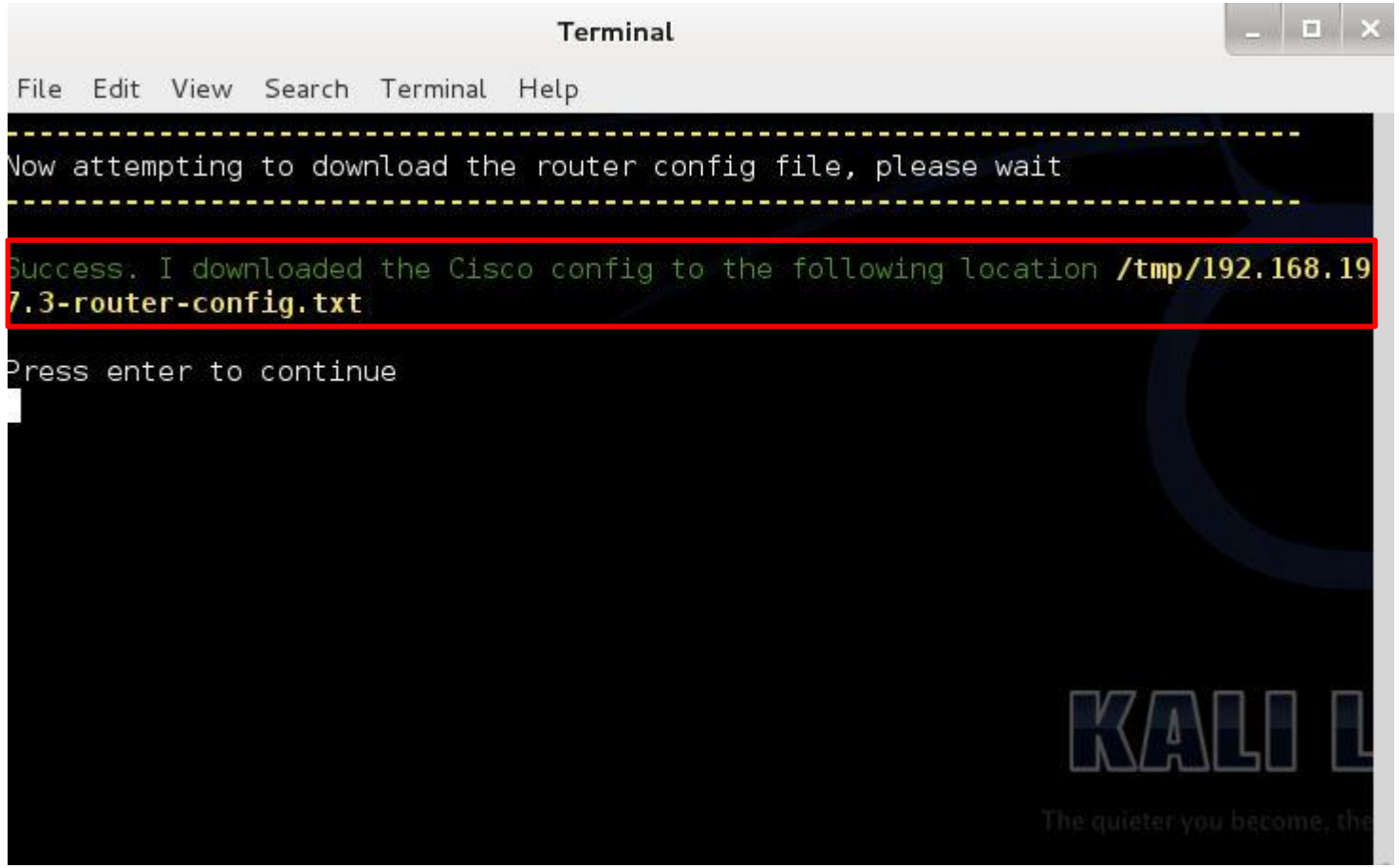
Угроза

```
root@Kali:~# snmpcheck -t 192.168.0.2
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 192.168.0.2
[*] Connected to 192.168.0.2
[*] Starting enumeration at 2014-05-12 12:16:09

[*] System information
-------------------------------------------------------------------------
----------------

Hostname               : TestLab.ptveb.com
Description            : Cisco IOS Software, 7200 Software (C7200-A
K9-M), Version 15.2(4)S3, RELEASE SOFTWARE (fc1)Technical Support: h
sco.com/techsupportCopyright (c) 1986-2013 by Cisco Systems, Inc.Com
-Apr-13 05:11 by prod_rel_team
Uptime system          : 0.00 seconds
Uptime SNMP daemon     : 1 hour, 01:03.94
Motd                   : -
```

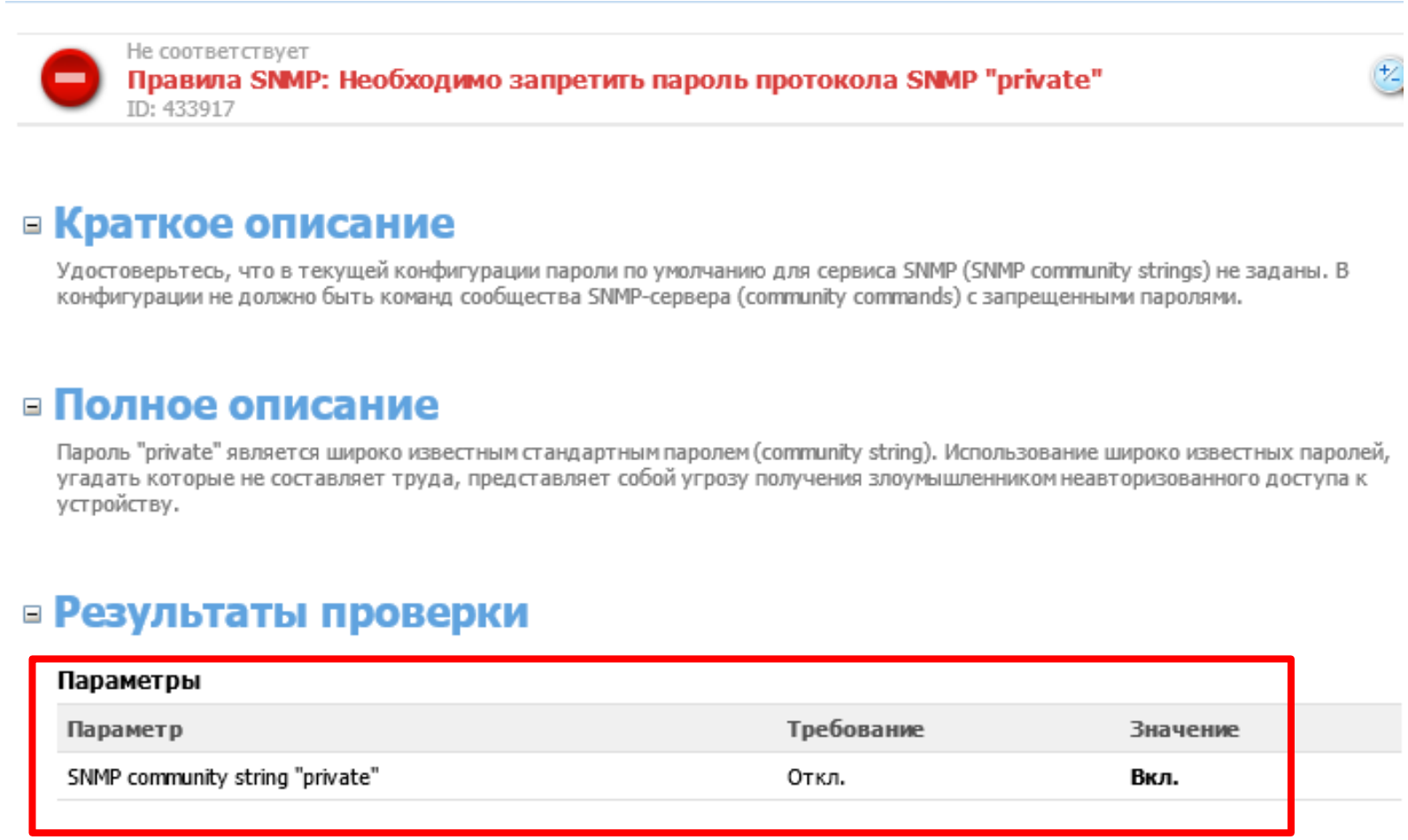
Угроза

```
Interface                : [ up ] FastEthernet1/0

       Interface Speed   : 100 Mbps
       IP Address        : 192.168.0.2
       Netmask           : 255.255.255.0
       MTU               : 1500

Interface                : [ up ] FastEthernet1/1

       Interface Speed   : 100 Mbps
       MTU               : 1500

Interface                : [ up ] Null0

       Interface Speed   : 4294.967295 Mbps
       MTU               : 1500


[*] Listening UDP ports
-----------------------------------------------------

  Local Address   Port

    192.168.0.2    123
    192.168.0.2    161
    192.168.0.2    162
```

Угроза


Terminal
File Edit View Search Terminal Help
Now attempting to download the router config file, please wait
Success. I downloaded the Cisco config to the following location /tmp/192.168.19
7.3-router-config.txt
Press enter to continue

Результат проверки



Не соответствует

Правила SNMP: Необходимо запретить пароль протокола SNMP "private"

ID: 433917

Краткое описание

Удостоверьтесь, что в текущей конфигурации пароли по умолчанию для сервиса SNMP (SNMP community strings) не заданы. В конфигурации не должно быть команд сообщества SNMP-сервера (community commands) с запрещенными паролями.

Полное описание

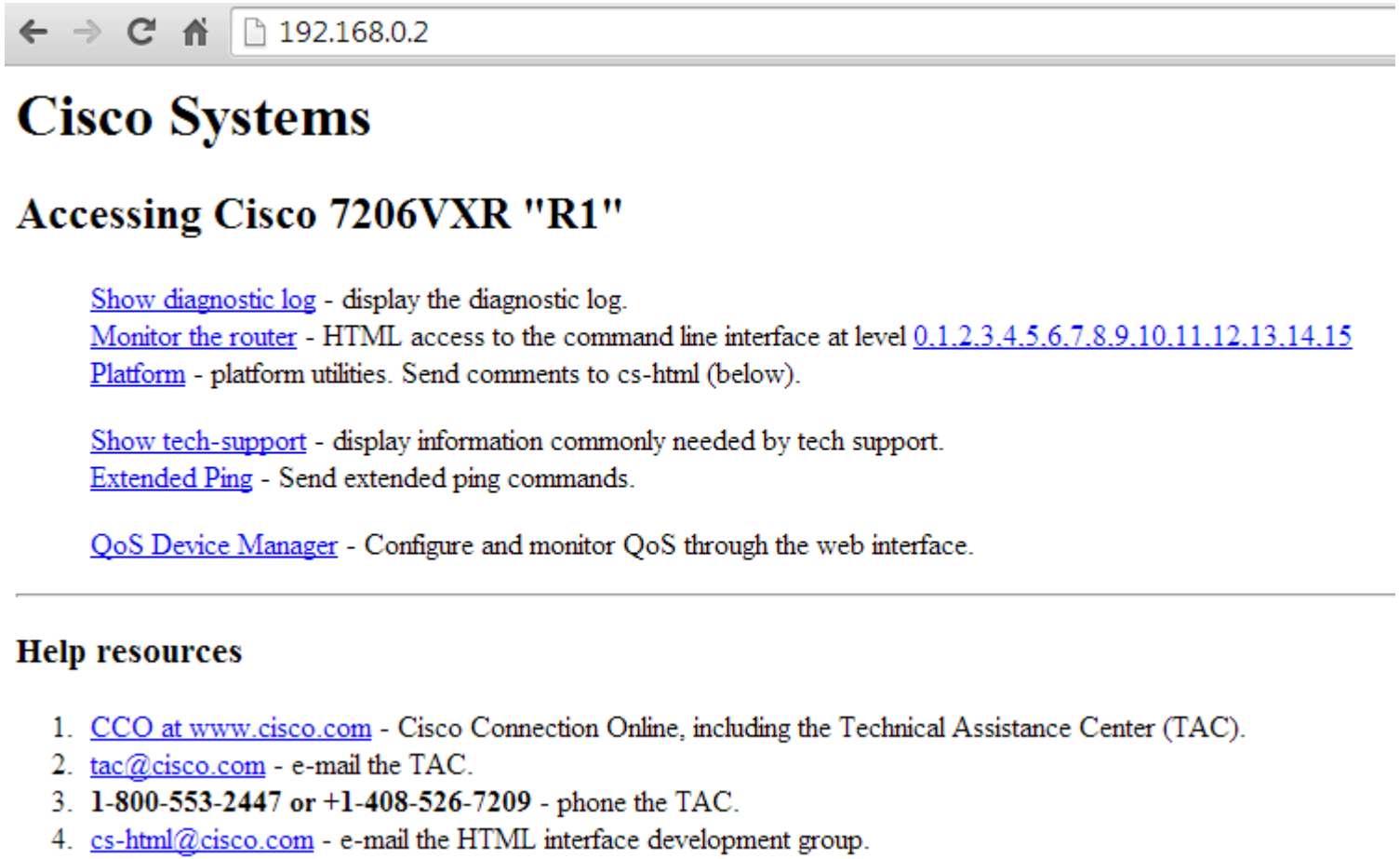
Пароль "private" является широко известным стандартным паролем (community string). Использование широко известных паролей, угадать которые не составляет труда, представляет собой угрозу получения злоумышленником неавторизованного доступа к устройству.

Результаты проверки

Параметры

Параметр	Требование	Значение
SNMP community string "private"	Откл.	**Вкл.**

Использование веб-интерфейса



Проверка HTTP – Требование стандарта

Remediation:
Disable the HTTP services.

IOS:

```
hostname(config)#no ip http server
hostname(config)#no ip http secure-server
```

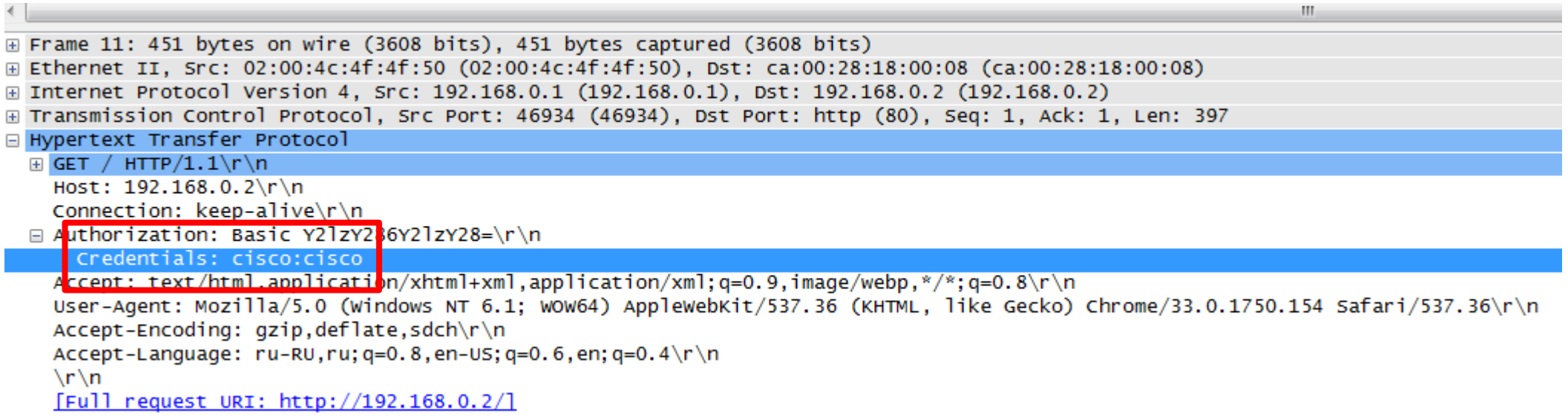
Audit:
Perform the following to determine if the HTTP services are enabled:

IOS:

1. Verify both "no ip http server" and "no ip http secure-server" results return

```
hostname#show run | incl http server
hostname#show run | incl http secure
```

Угроза


Frame 11: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits)
Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: ca:00:28:18:00:08 (ca:00:28:18:00:08)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
Transmission Control Protocol, Src Port: 46934 (46934), Dst Port: http (80), Seq: 1, Ack: 1, Len: 397
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: 192.168.0.2\r\n
Connection: keep-alive\r\n
Authorization: Basic Y2lzY2
6Y2lzY28=\r\n
Credentials: cisco:cisco
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36\r\n
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4\r\n
\r\n
[Full request URI: http://192.168.0.2/]

Результат проверки

Не соответствует

Правила глобальных сервисов: Необходимо отключить сервисы HTTP (включая ASDM)

ID: 433937

Краткое описание

Рекомендуется отключить сервисы HTTP.

Полное описание

Сервисы HTTP позволяют осуществлять удаленное управление маршрутизаторами. Однако если используется обычный HTTP, при аутентификации пароль передается в не зашифрованном виде. Это может привести к получению неавторизованного доступа к маршрутизатору и возможности неправомерного управления им. Рекомендуется отключить службы HTTP. Если необходим интерфейс веб-управления, обеспечьте использование функций HTTPS-сервера.

Результаты проверки

Параметры

Параметр	Требование	Значение
HTTP-сервер	Откл.	**Вкл.**
HTTPS-сервер	Откл.	**Вкл.**

Проверка OSPF – Требование стандарта

Remediation:
Configure the message Digest option for OSPF.

IOS:

```
hostname(config)#router ospf <ospf process-id>
hostname(config-router)#area <ospf_area-id> authentication message-
digest
```

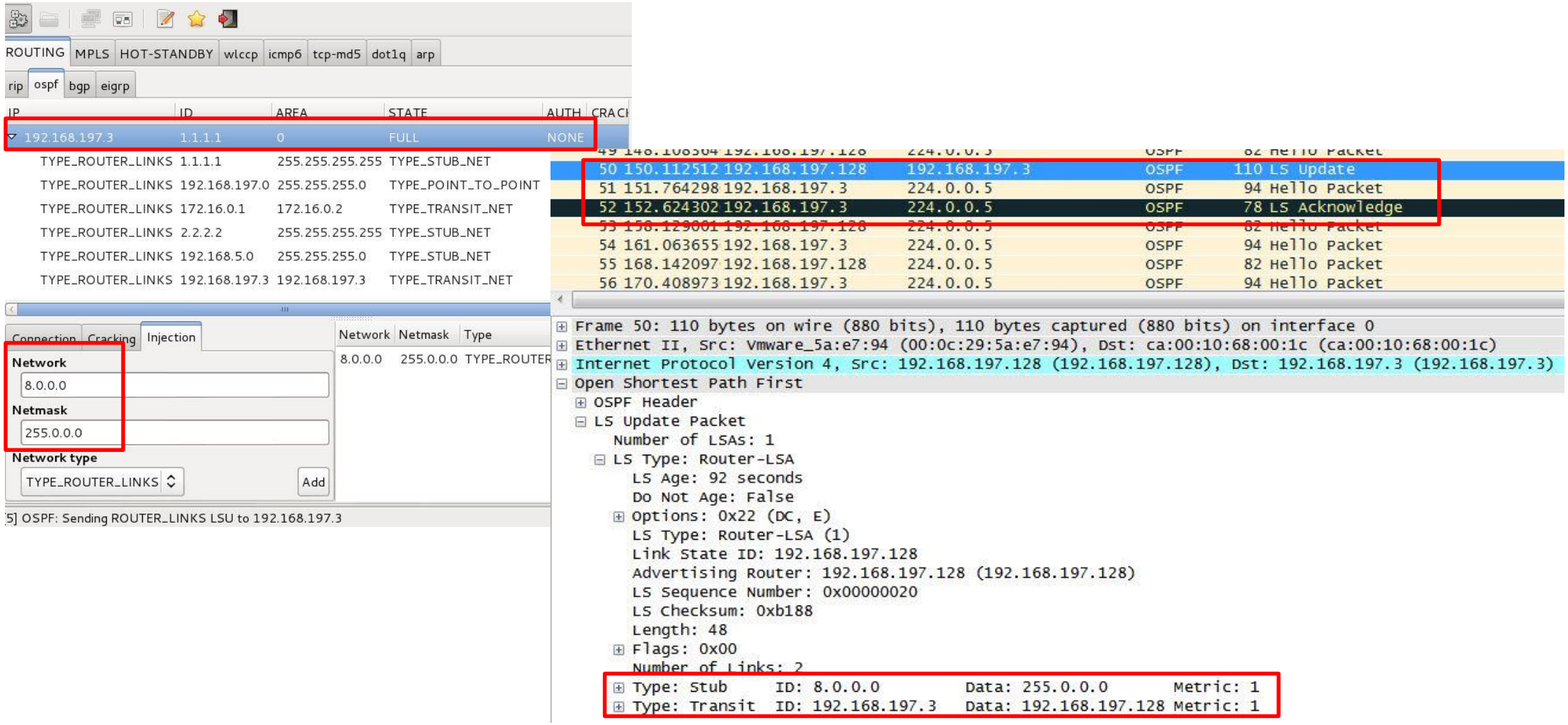
Audit:
Perform the following to determine if the OSPF authentication is enabled:

IOS:

1. Verify message digest for OSPF is defined

```
hostname#sh run | sec router ospf
```

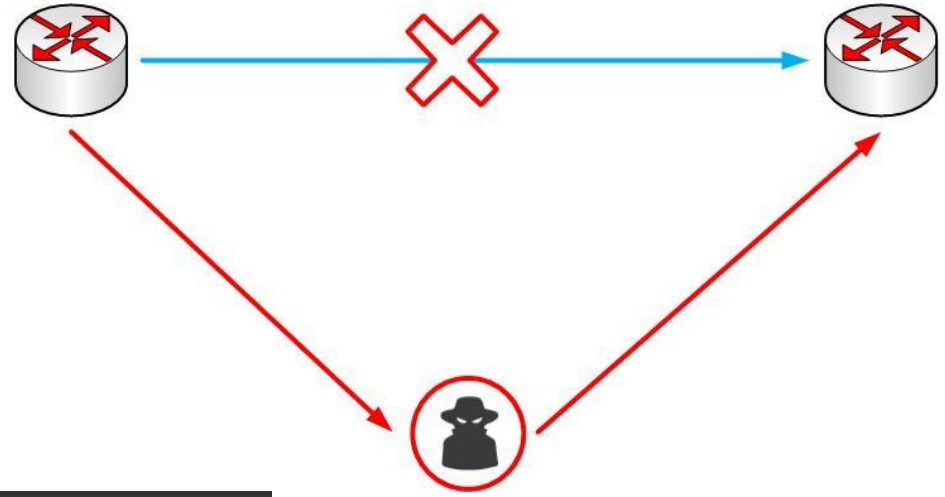
Угроза


ROUTING MPLS HOT-STANDBY wlccp icmp6 tcp-md5 dot1q arp
rip ospf bgp eigrp
IP ID AREA STATE AUTH
192.168.197.3 1.1.1.1 0 FULL NONE
TYPE_ROUTER_LINKS 1.1.1.1 255.255.255.255 TYPE_STUB_NET
TYPE_ROUTER_LINKS 192.168.197.0 255.255.255.0 TYPE_POINT_TO_POINT
TYPE_ROUTER_LINKS 172.16.0.1 172.16.0.2 TYPE_TRANSIT_NET
TYPE_ROUTER_LINKS 2.2.2.2 255.255.255.255 TYPE_STUB_NET
TYPE_ROUTER_LINKS 192.168.5.0 255.255.255.0 TYPE_STUB_NET
TYPE_ROUTER_LINKS 192.168.197.3 192.168.197.3 TYPE_TRANSIT_NET
Connection Cracking Injection
Network
8.0.0.0
Netmask
255.0.0.0
Network type
TYPE_ROUTER_LINKS
Add
Network Netmask Type
8.0.0.0 255.0.0.0 TYPE_ROUTER
5] OSPF: Sending ROUTER_LINKS LSU to 192.168.197.3
50 150.112512 192.168.197.128 192.168.197.3 OSPF 110 LS Update
51 151.764298 192.168.197.3 224.0.0.5 OSPF 94 Hello Packet
52 152.624302 192.168.197.3 224.0.0.5 OSPF 78 LS Acknowledge
54 161.063655 192.168.197.3 224.0.0.5 OSPF 94 Hello Packet
55 168.142097 192.168.197.128 224.0.0.5 OSPF 82 Hello Packet
56 170.408973 192.168.197.3 224.0.0.5 OSPF 94 Hello Packet
Frame 50: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: Vmware_5a:e7:94 (00:0c:29:5a:e7:94), Dst: ca:00:10:68:00:1c (ca:00:10:68:00:1c)
Internet Protocol Version 4, Src: 192.168.197.128 (192.168.197.128), Dst: 192.168.197.3 (192.168.197.3)
Open Shortest Path First
OSPF Header
LS Update Packet
Number of LSAs: 1
LS Type: Router-LSA
LS Age: 92 seconds
Do Not Age: False
Options: 0x22 (DC, E)
LS Type: Router-LSA (1)
Link State ID: 192.168.197.128
Advertising Router: 192.168.197.128 (192.168.197.128)
LS Sequence Number: 0x00000020
LS Checksum: 0xb188
Length: 48
Flags: 0x00
Number of Links: 2
Type: Stub ID: 8.0.0.0 Data: 255.0.0.0 Metric: 1
Type: Transit ID: 192.168.197.3 Data: 192.168.197.128 Metric: 1

Угроза

Before:

```
TestLab#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 172.16.0.1, 17:17:52, FastEthernet0/0
O     192.168.5.0/24 [110/2] via 172.16.0.1, 17:17:52, FastEthernet0/0
```



After:

```
TestLab#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 172.16.0.1, 1d01h, FastEthernet0/0
O     8.0.0.0/8 [110/2] via 192.168.197.128, 00:01:23, FastEthernet1/0
O     192.168.5.0/24 [110/2] via 172.16.0.1, 1d01h, FastEthernet0/0
```

Ooops!

Результат проверки

Не соответствует

Аутентификация протоколов маршрутизации: Необходимо настроить OSPF-аутентификацию, если используется протокол

ID: 433976

Краткое описание

Удостоверьтесь, что OSPF-аутентификация настроена там, где это возможно.

Полное описание

Маршрутизация OSPF (если она развернута) необходима для нормального функционирования сетевой инфраструктуры организации. Точная информация о маршруте необходима для того, чтобы маршрутизаторы точно направляли трафик по сети.
Злоумышленник, действуя от имени одного из соседских OSPF-узлов целевого маршрутизатора, может внедрить некорректную информацию в таблицу маршрутизации, что приведет к отказу в обслуживании или утечке конфиденциальных данных при проведении атаки типа "человек посередине".
На маршрутизаторах Cisco (а также маршрутизаторах других производителей, таких как Juniper или Brocade) возможна аутентификация протоколов маршрутизации при помощи MD5-дайджеста в сочетании с порядковым номером для защиты от атак связанных с повторной передачей пакетов.
Аутентификация настраивается индивидуально для каждой зоны.
Примечание: удостоверьтесь, что аутентификация протоколов маршрутизации настроена одинаково для всех маршрутизаторов в зоне OSPF; в противном случае обновления маршрута не будут выполнены.

Результаты проверки

Список Area, учавствующих в маршрутизации

ID	Номер Area	Процесс	Аутентификация
1	0	1	**не задан(а)**

Проверка сложности паролей – Требование стандарта

Remediation:
Create a local user with an encrypted, complex (not easily guessed) password.

IOS:

```
hostname(config)#username <LOCAL_USERNAME> secret <LOCAL_PASSWORD>
```

Audit:

Perform the following to determine if a user with an encrypted password is enabled:

1. If a result does not return a result, the feature is not enabled

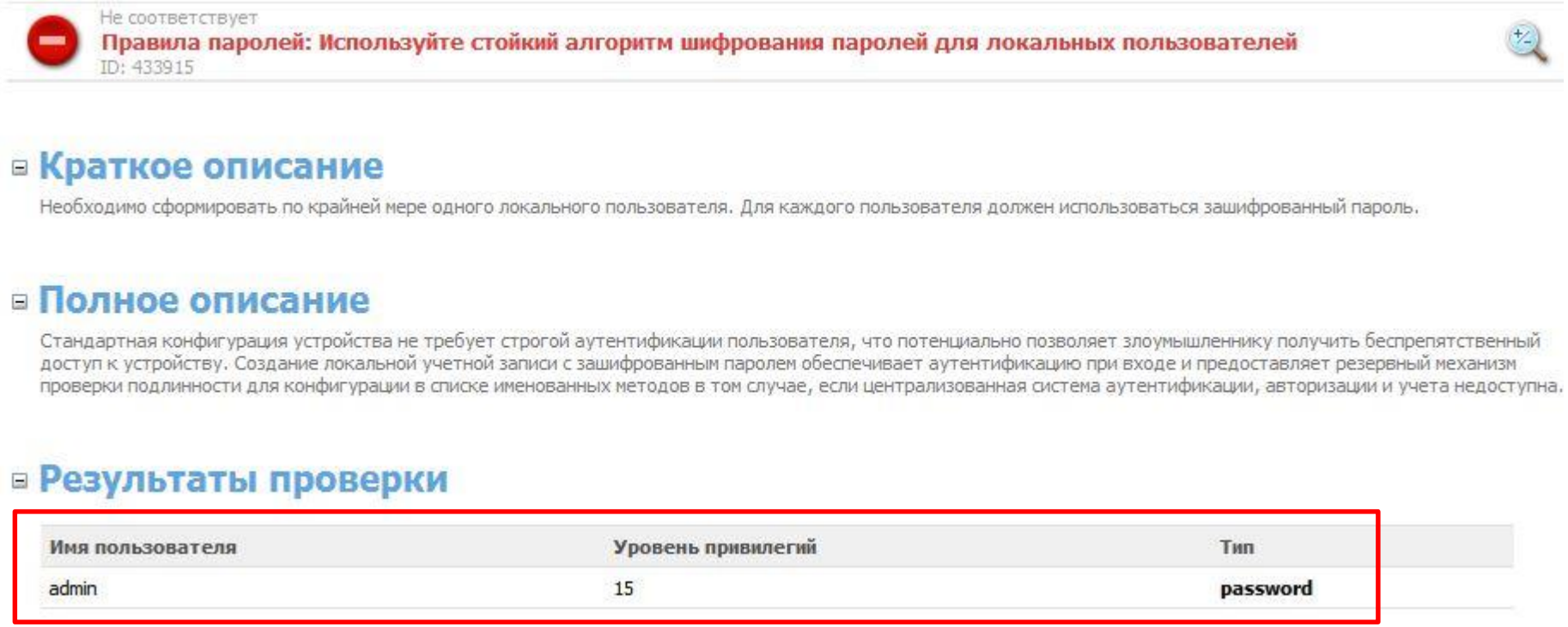
IOS:

```
hostname#show run | incl username
```

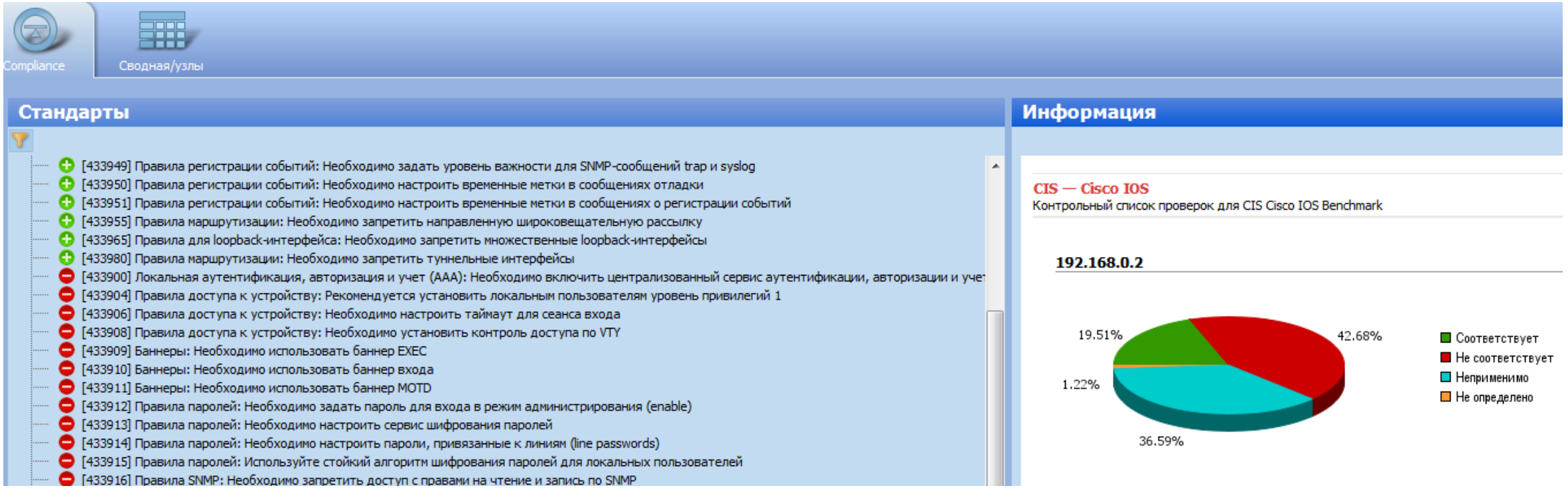
Угроза

```
TestLab#sh run | sec user
username admin privilege 15 password 7 0125261042535 54E71464A5A5C
```

Результат проверки



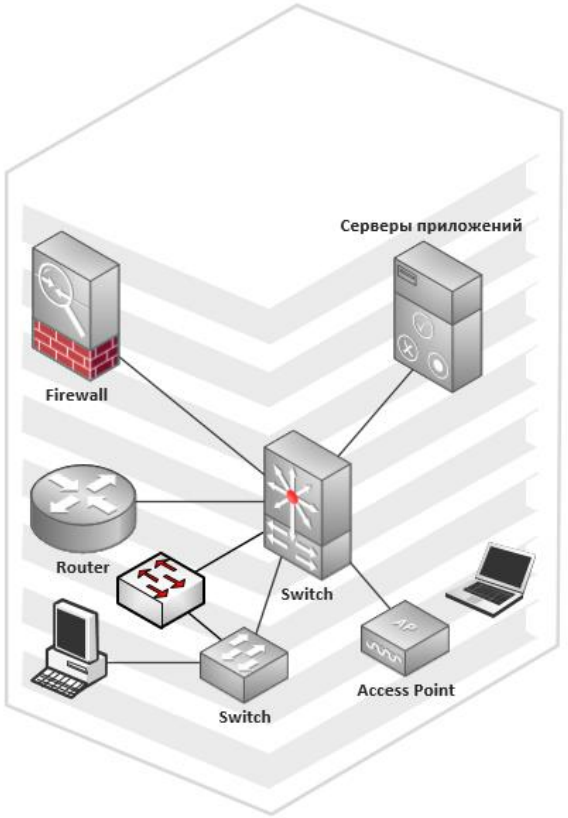
Результат сканирования



Что в итоге?

Что в итоге?

- ✔ Инвентаризация активов
- ✔ Аудит безопасности
- ✔ Соответствие политике ИБ



Филиал

Конец рассказа
Спасибо за внимание

Строев Евгений

Эксперт по информационной безопасности

Positive Technologies

estroev@ptsecurity.com

POSITIVE TECHNOLOGIES