



POSITIVE TECHNOLOGIES

Обеспечение безопасности корпоративной сети с помощью MaxPatrol

Строев Евгений

эксперт по информационной безопасности Positive Technologies

О чём пойдёт речь

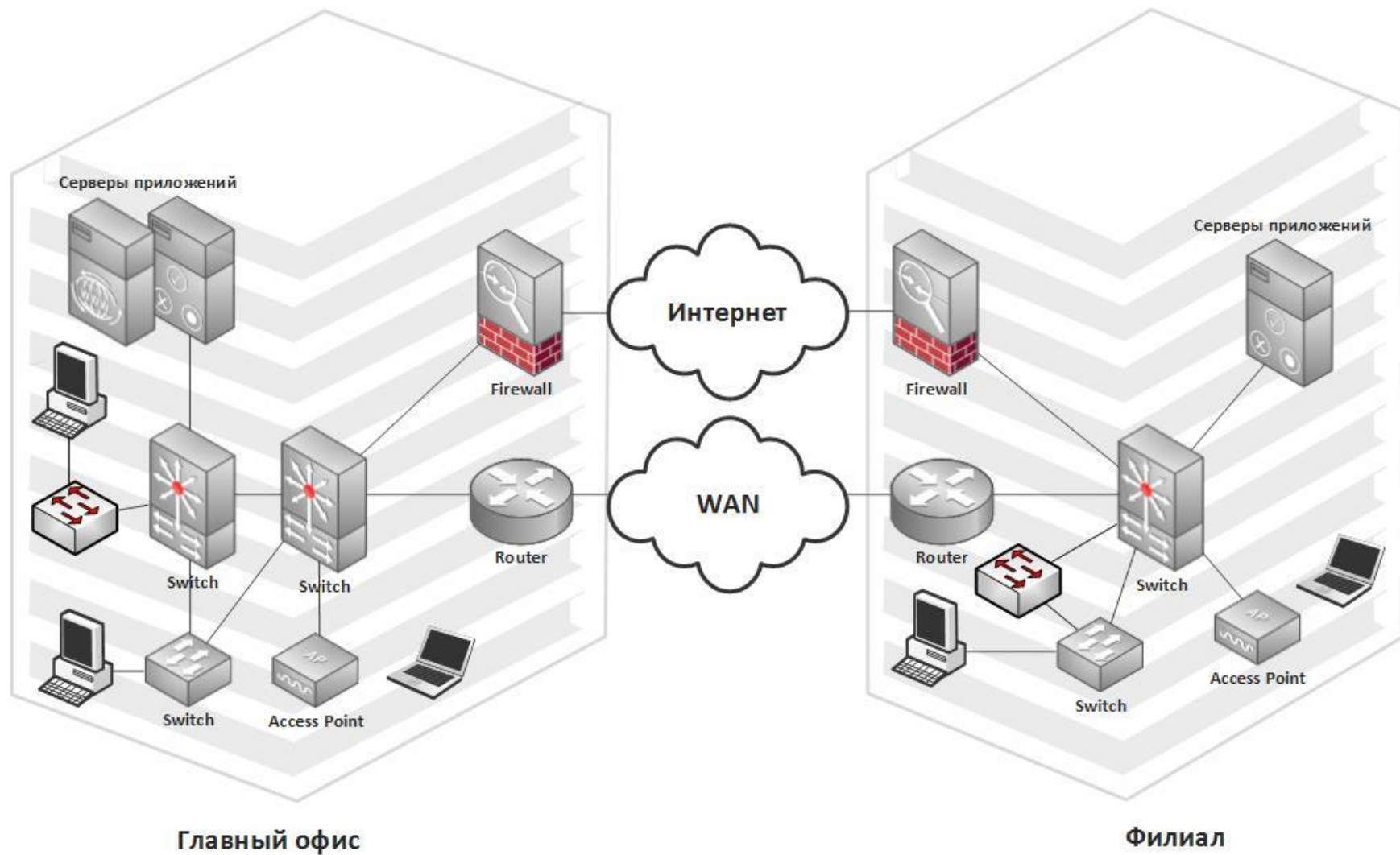
- Почему безопасность сетевой инфраструктуры так важна
- Какие сложности возникают при обеспечении безопасности
- Зачем нужна инвентаризация активов
- Что может показать аудит безопасности
- Что такое стандарт по безопасности для сетевых устройств

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



- Рекомендации по устранению доступны

KNOWLEDGE BASE

Cisco Blogs

SECURITY INTELLIGENCE CENTER

- Инструкций по безопасной настройке достаточно



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

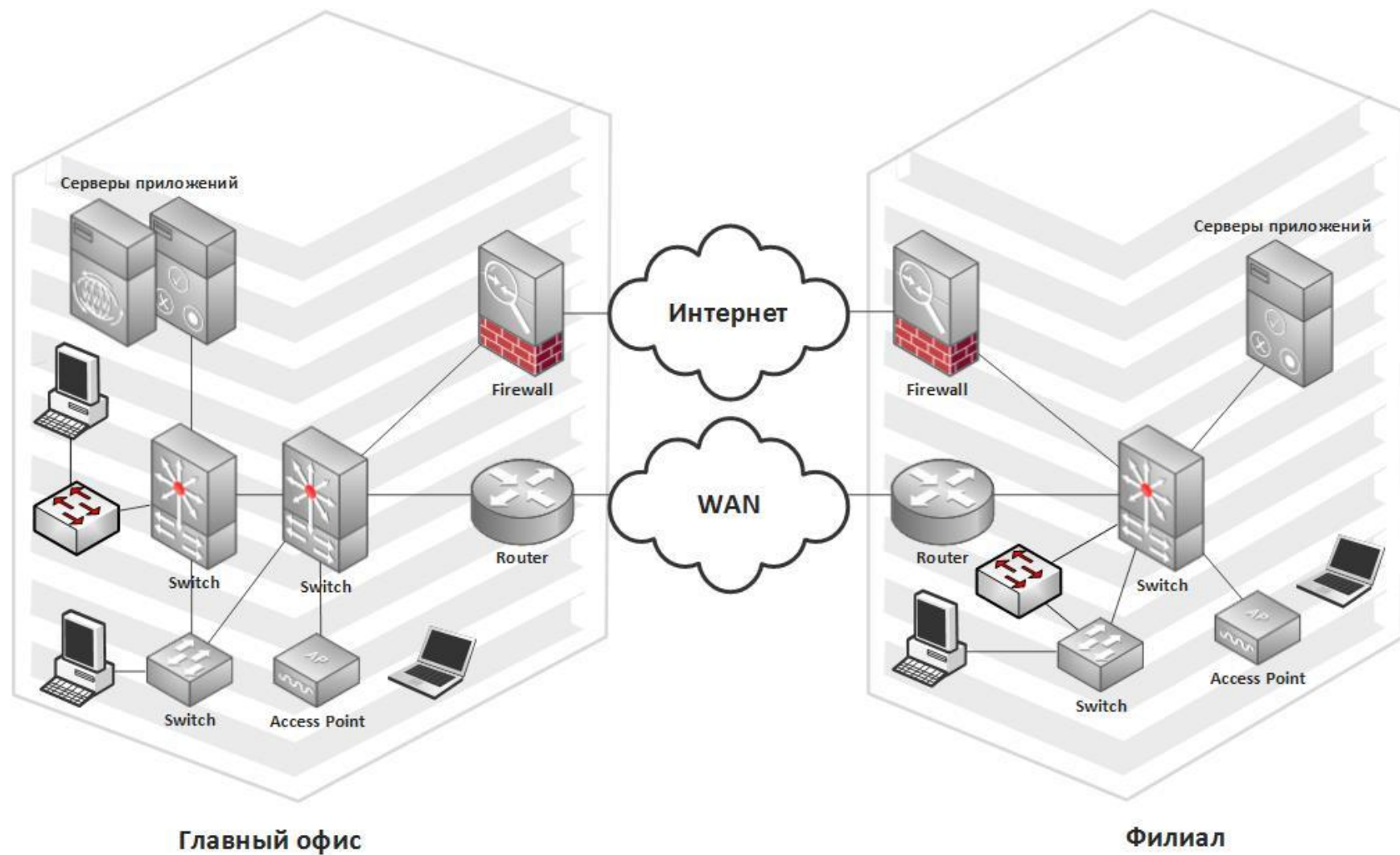
— Бреши в безопасности

- Рекомендации аудита
- Автоматизация процесса контроля соответствия стандартам по безопасности

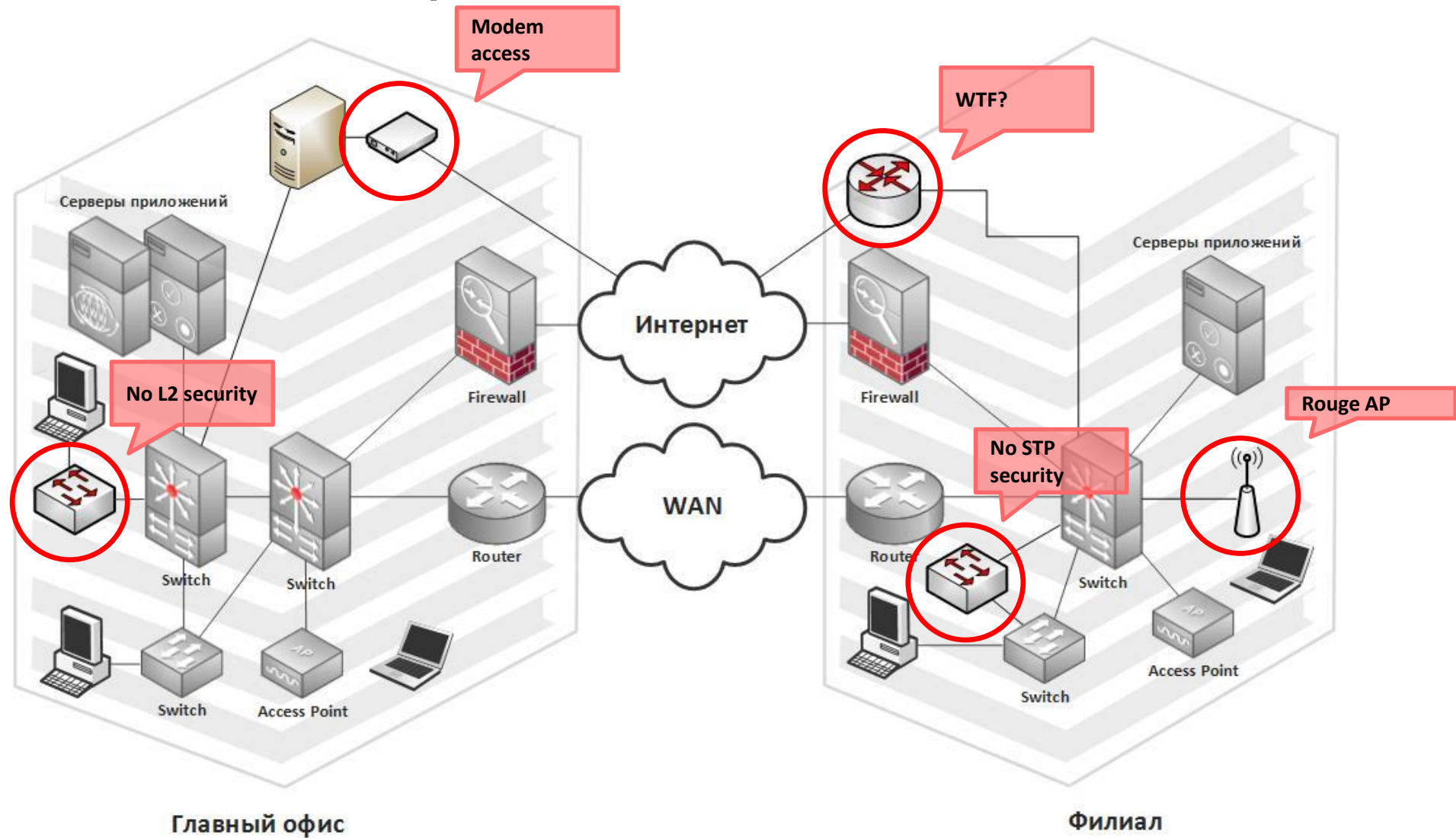
Как это делается:

Инвентаризация активов

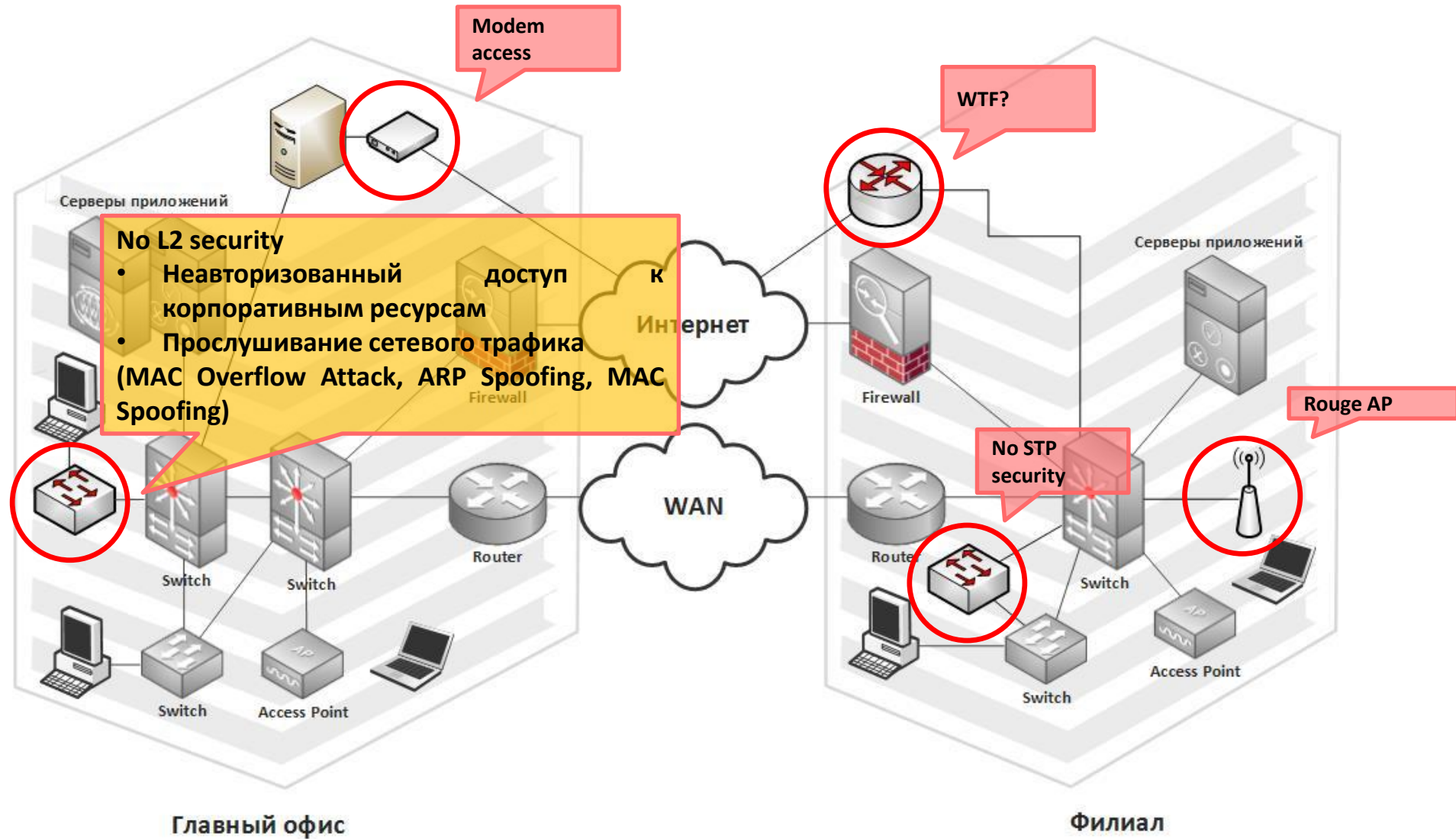
Инвентаризация активов



Результаты инвентаризации активов

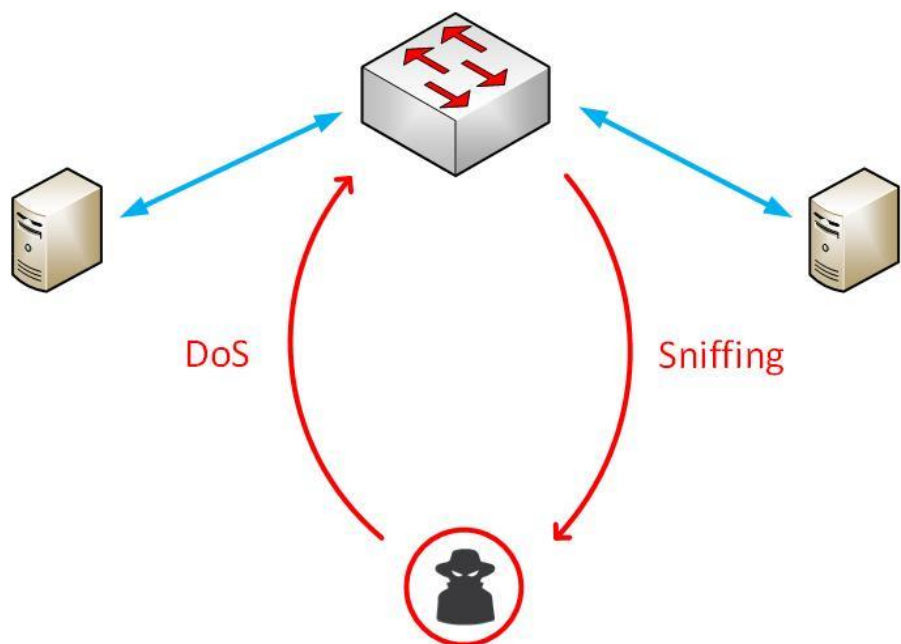


Результаты инвентаризации активов



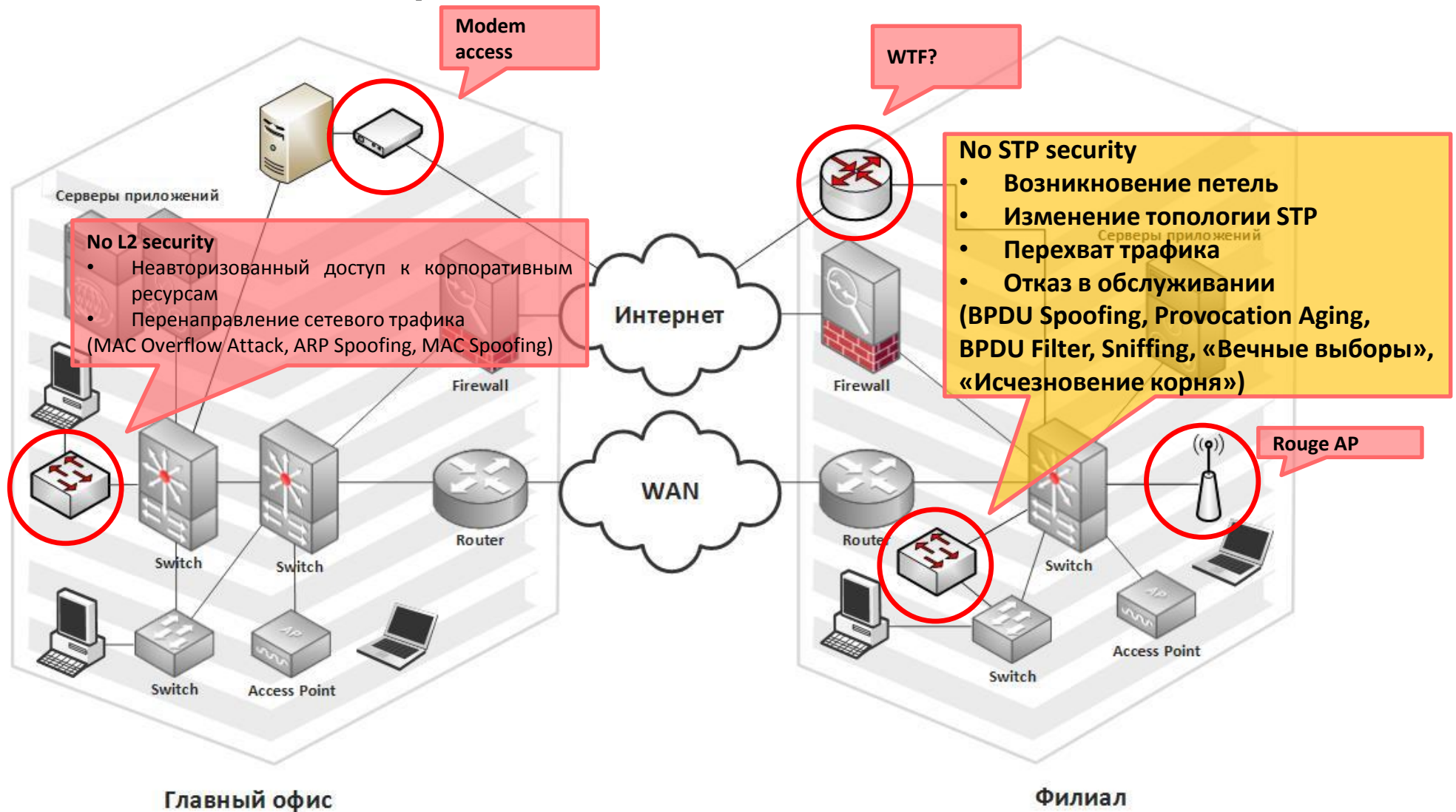
Эксплуатация

MAC Overflow

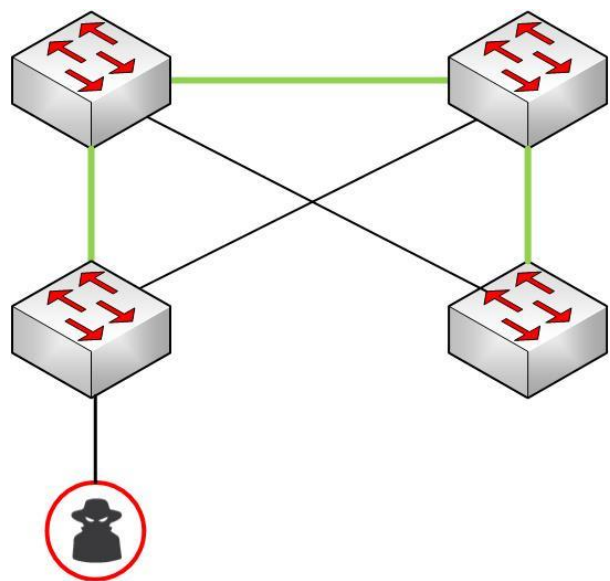


```
root@Kali:~# macof -d 192.168.197.2 -n 100000
24:cb:d7:5b:79:50 db:14:5a:74:a3:dd 0.0.0.0.945 > 192.168.197.2.13588: S 2075515
961:2075515961(0) win 512
5:9d:6d:39:be:f4 67:74:a6:2c:a5:51 0.0.0.0.21670 > 192.168.197.2.14225: S 164250
484:164250484(0) win 512
f9:38:1e:45:b3:2d 1c:ac:a6:0:d8:4 0.0.0.0.40717 > 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
```

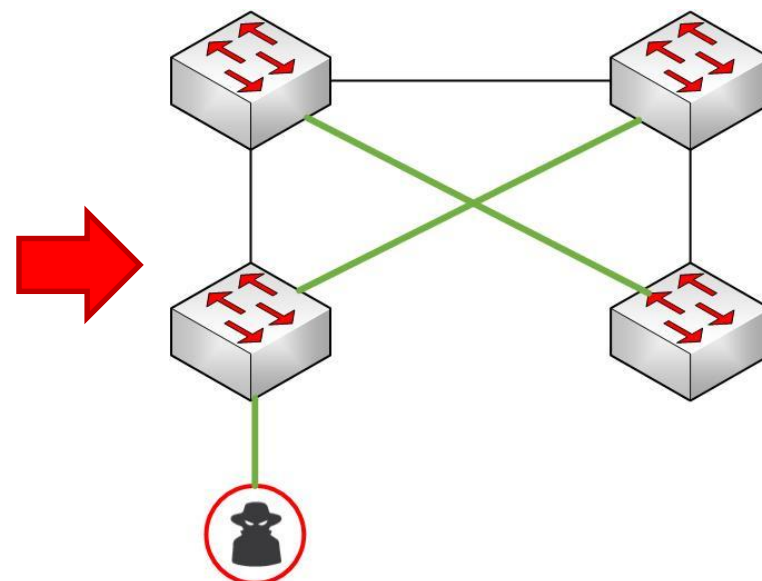
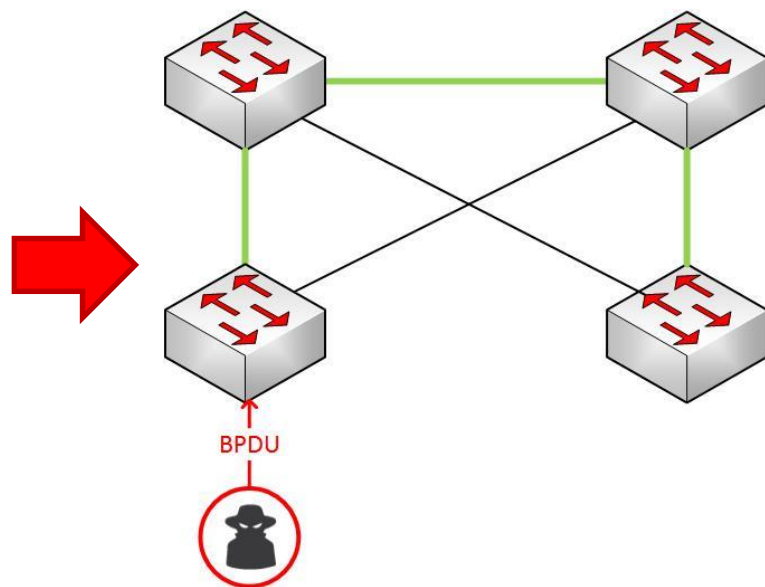

Результаты инвентаризации активов



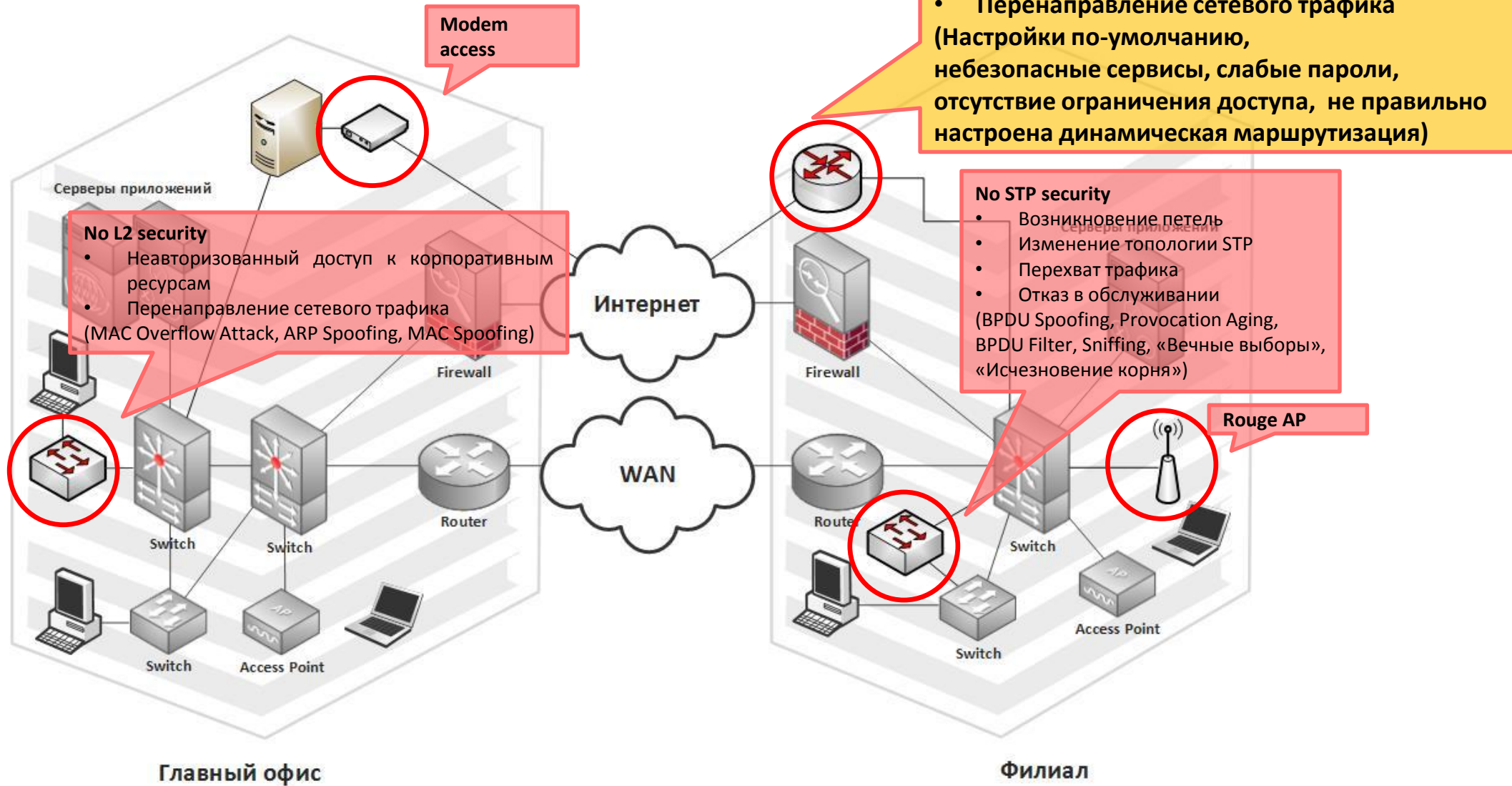
Эксплуатация



BPDUs Spoofing

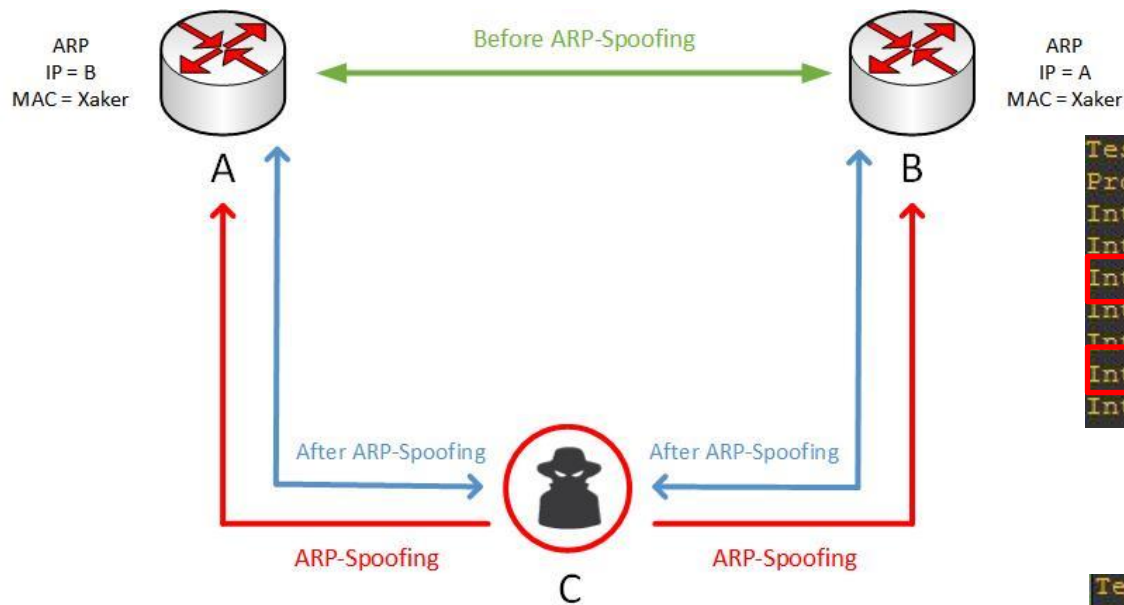


Результаты инвентаризации активов



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
```

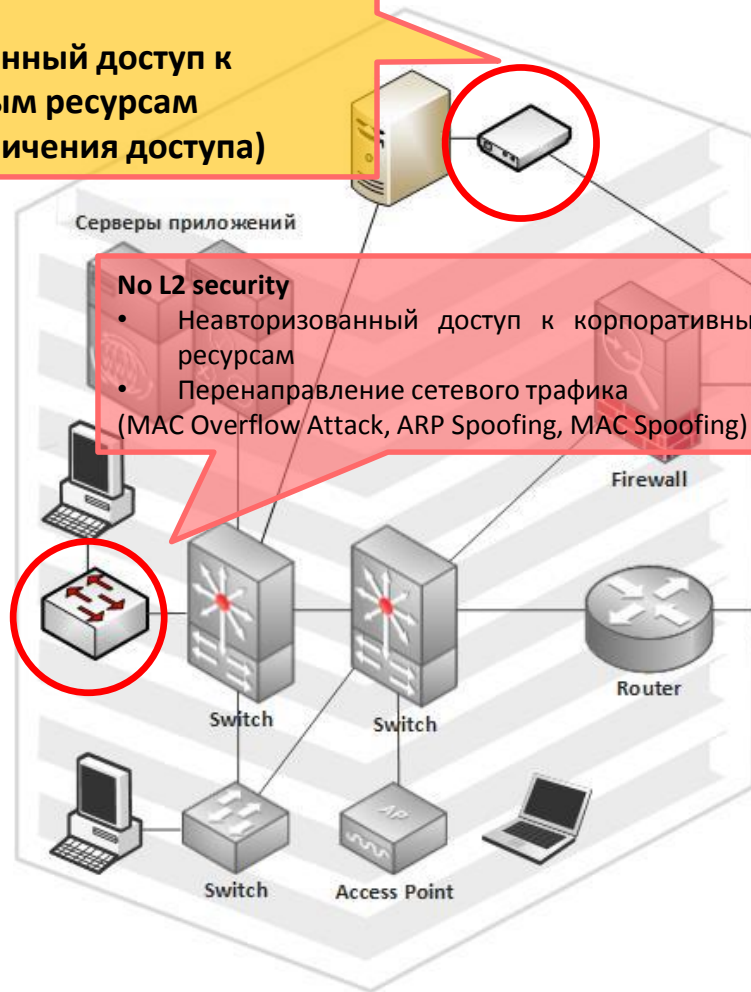


```
TestLab#sh arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 172.16.0.1      91        ca01.1068.0008 ARPA   FastEthernet0/0
Internet 172.16.0.2      -         ca00.1068.0008 ARPA   FastEthernet0/0
Internet 192.168.197.1   0         000c.295a.e794 ARPA   FastEthernet1/0
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)



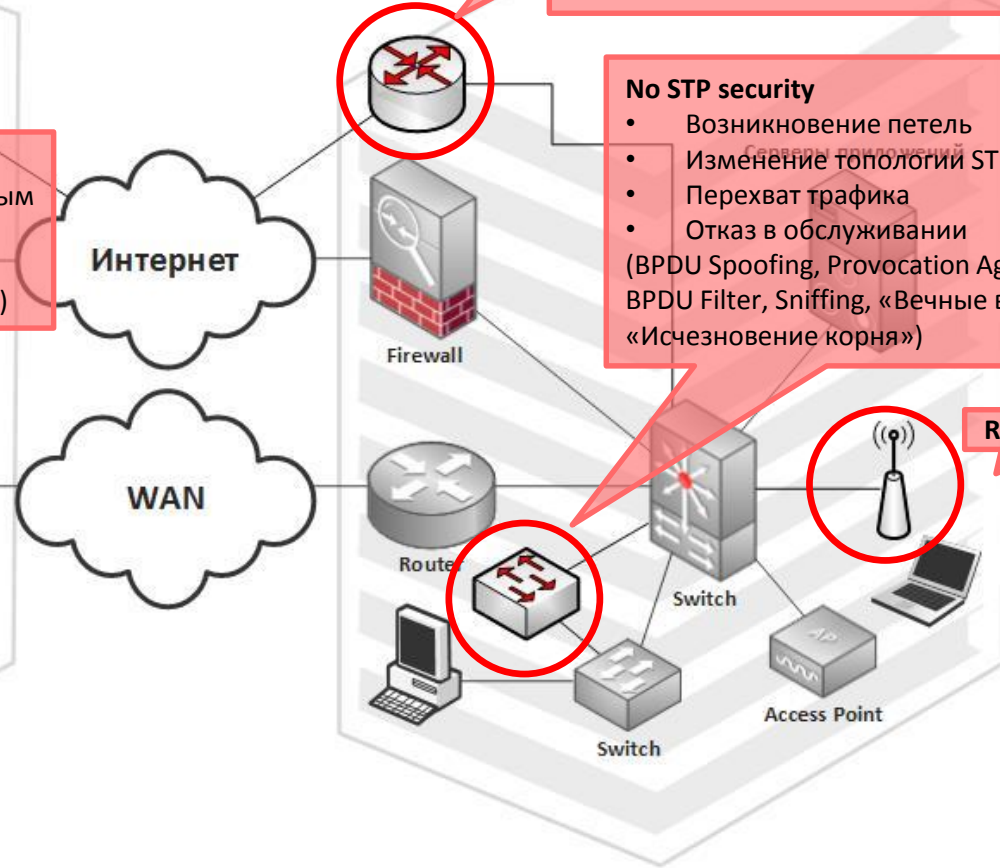
No L2 security

- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика (MAC Overflow Attack, ARP Spoofing, MAC Spoofing)

Главный офис

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 STP security

- Возникновение петель
- Изменение топологии STP
- Перехват трафика
- Отказ в обслуживании (BPDU Spoofing, Provacation Aging, BPDU Filter, Sniffing, «Вечные выборы», «Исчезновение корня»)

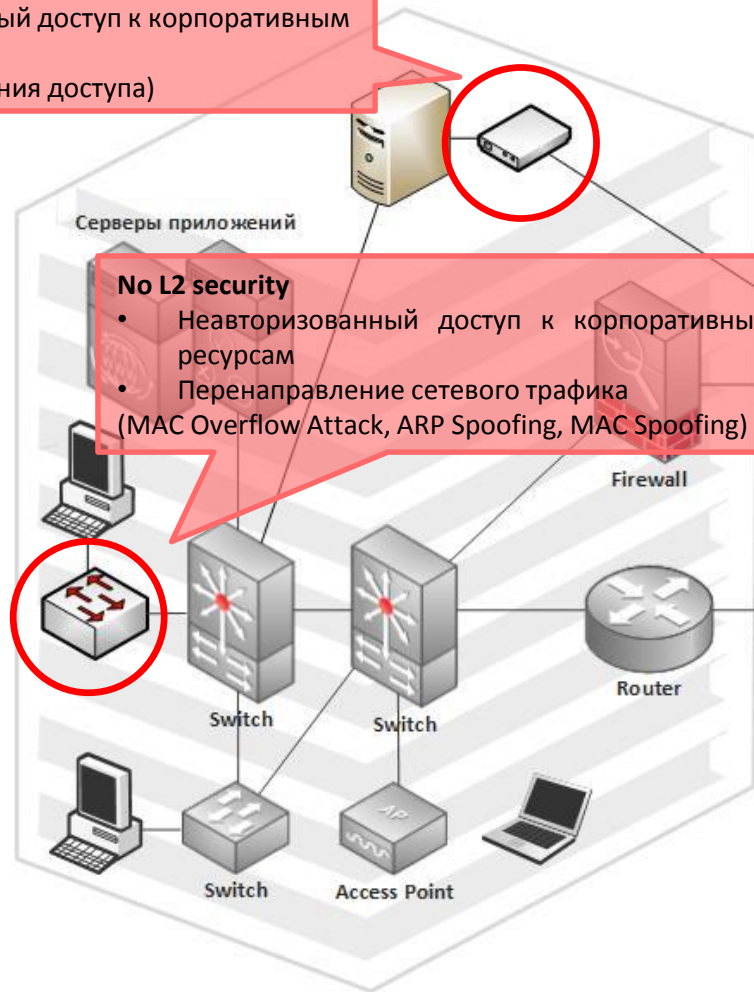
Rouge AP

Филиал

Результаты инвентаризации активов

Modem Access

- Неавторизованный доступ к корпоративным ресурсам
(Отсутствие ограничения доступа)



No L2 security

- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика
(MAC Overflow Attack, ARP Spoofing, MAC Spoofing)

Главный офис

WTF?

- Неавторизованный доступ к корпоративным ресурсам
- Перенаправление сетевого трафика
(Настройки по-умолчанию, небезопасные сервисы, слабые пароли, отсутствие ограничения доступа)



No STP security

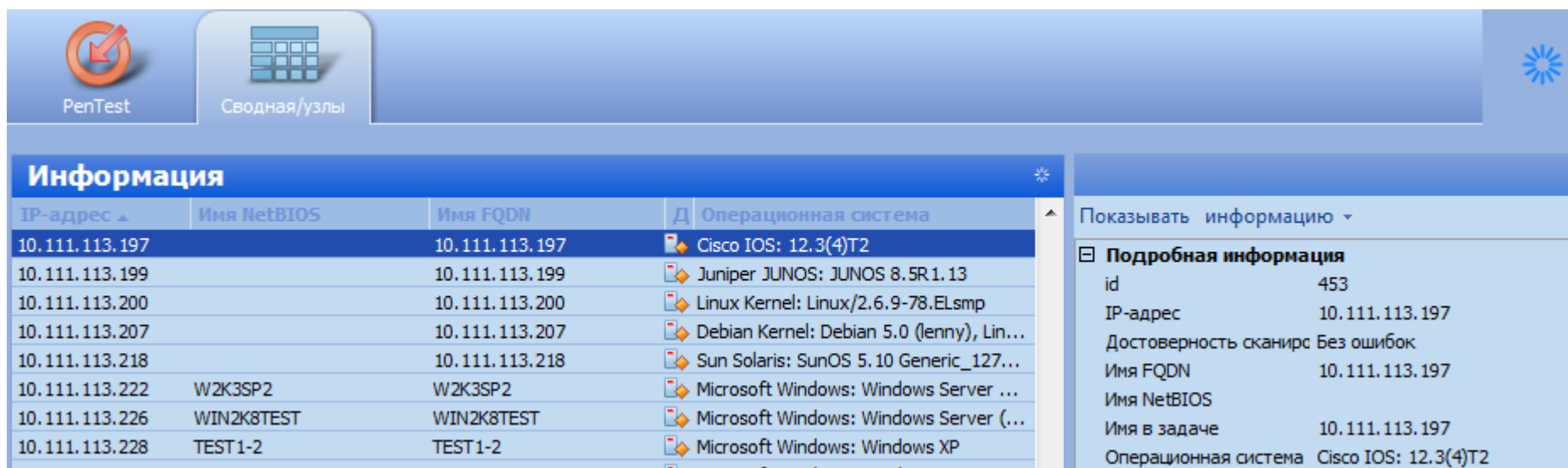
- Возникновение петель
- Изменение топологии STP
- Перехват трафика
- Отказ в обслуживании
(BPDU Spoofing, Provocation Aging, BPDU Filter, Sniffing, «Вечные выборы», «Исчезновение корня»)

Филиа.

Rogue AP

- Перехват трафика
- Неавторизованный доступ к корпоративным ресурсам
(Sniffing, отсутствие ограничения доступа)

Результаты инвентаризация активов



The screenshot shows a software interface for asset inventory. At the top, there are two tabs: 'PenTest' (with a red arrow icon) and 'Сводная/узлы' (with a grid icon). A sun icon is in the top right corner. Below the tabs is a table titled 'Информация' with columns: 'IP-адрес', 'Имя NetBIOS', 'Имя FQDN', and 'Операционная система'. The table lists several IP addresses and their corresponding OS types. To the right of the table is a panel titled 'Показывать информацию' with a dropdown arrow. It contains a section 'Подробная информация' with key-value pairs for the selected IP (10.111.113.197): id (453), IP-адрес (10.111.113.197), Достоверность сканирования (Без ошибок), Имя FQDN (10.111.113.197), Имя NetBIOS, Имя в задаче (10.111.113.197), and Операционная система (Cisco IOS: 12.3(4)T2).

IP-адрес	Имя NetBIOS	Имя FQDN	Операционная система
10.111.113.197		10.111.113.197	Cisco IOS: 12.3(4)T2
10.111.113.199		10.111.113.199	Juniper JUNOS: JUNOS 8.5R1.13
10.111.113.200		10.111.113.200	Linux Kernel: Linux/2.6.9-78.ELsmp
10.111.113.207		10.111.113.207	Debian Kernel: Debian 5.0 (lenny), Lin...
10.111.113.218		10.111.113.218	Sun Solaris: SunOS 5.10 Generic_127...
10.111.113.222	W2K3SP2	W2K3SP2	Microsoft Windows: Windows Server ...
10.111.113.226	WIN2K8TEST	WIN2K8TEST	Microsoft Windows: Windows Server (...)
10.111.113.228	TEST1-2	TEST1-2	Microsoft Windows: Windows XP

Показывать информацию ▾

Подробная информация

id	453
IP-адрес	10.111.113.197
Достоверность сканирования	Без ошибок
Имя FQDN	10.111.113.197
Имя NetBIOS	
Имя в задаче	10.111.113.197
Операционная система	Cisco IOS: 12.3(4)T2

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

```
Frame 1: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface 0
IEEE 802.3 Ethernet
Logical-Link Control
Cisco Discovery Protocol
  Version: 2
  TTL: 180 seconds
  Checksum: 0x016b [correct]
  Device ID: R1.lab.local
  Software Version
    Type: Software version (0x0005)
    Length: 231
    Software Version: Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), version 15.2(4)S3, RELEASE SOFTWARE (fc1)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2013 by Cisco Systems, Inc.
    Compiled Fri 19-Apr-13 05:11 by prod_rel_team
  Platform: Cisco 7206VXR
  Addresses
  Port ID: FastEthernet0/0
0000  01 00 0c cc cc cc ca 01 23 20 00 08 01 73 aa aa ..... # ...s..
0010  03 00 00 0c 20 00 02 b4 01 6b 00 01 00 10 52 31 .... .k....R1
0020  2e 6c 61 62 2e 6c 6f 63 61 6c 00 05 00 fb 43 69 .lab.local...Ci
0030  73 63 6f 20 49 4f 53 20 53 6f 66 74 77 61 72 65 sco IOS software
0040  2c 20 37 32 30 30 20 53 6f 66 74 77 61 72 65 20 , 7200 s
0050  28 43 37 32 30 30 2d 41 44 56 45 4e 54 45 52 50 (C7200-A
0060  52 49 53 45 4b 39 2d 4d 29 2c 20 56 65 72 73 69 RISEK9-M), Versi
0070  6f 6e 20 31 35 2e 32 28 34 29 53 33 2c 20 52 45 on 15.2(
0080  4c 45 41 53 45 20 53 4f 46 54 57 41 52 45 20 28 LEASE SO
0090  66 63 31 29 0a 54 65 63 68 6e 69 63 61 6c 20 53 fc1).Tec
00a0  75 70 70 6f 72 74 3a 20 68 74 74 70 3a 2f 2f 77 upport: http://w
00b0  77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 74 65 63 ww.cisco
00c0  68 73 75 70 70 6f 72 74 0a 43 6f 70 79 72 69 67 hsupport.Copyrig
00d0  68 74 20 28 63 29 20 31 39 38 36 2d 32 30 31 33 ht (c) 1
00e0  20 62 79 20 43 69 73 63 6f 20 53 79 73 74 65 6d by Cisc
00f0  73 2c 20 49 6e 63 2e 0a 43 6f 6d 70 69 6c 65 64 s, Inc..
0100  20 46 72 69 20 31 39 2d 41 70 72 2d 31 33 20 30 Fri 19-
0110  35 3a 31 31 20 62 79 20 70 72 6f 64 5f 72 65 6c 5:11 by
0120  5f 74 65 61 6d 00 06 00 11 43 69 73 63 6f 20 37 _team...
0130  32 30 36 56 58 52 00 02 00 11 00 00 00 01 01 01 206VXR..
0140  cc 00 04 c0 a8 00 02 00 03 00 13 46 61 73 74 45 .....
0150  74 68 65 72 6e 65 74 30 2f 30 00 04 00 08 00 00 ...FastE
0160  00 01 00 07 00 09 01 01 01 00 18 00 0b 00 05 01 thernet0
0170  00 16 00 11 00 00 00 01 01 01 cc 00 04 c0 a8 00 /0.....
0180  02 .....
```

Ошибки в настройке оборудования

SHODAN Search: cisco port:181

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory Export Data

Top Countries

United States	57,174
Russian Federation	27,706
China	17,905
Korea, Republic of	16,668
India	15,112

41.160.79.2
NEOTEL
Added on 15.07.2014
Johannesburg
Details
Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 15.0(1)S5, RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 16-Jan-12 22:4

196.20.127.0
Telecom Algeria
Added on 15.07.2014
Details
Cisco IOS Software, 2801 Software (C2801-IPBASE-M), Version 12.4(1c), RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 26-Oct-05 08:42 by emviller

121.141.123.163
Korea Telecom
Added on 15.07.2014
Details
Cisco IOS Software, 1841 Software (C1841-ADVSECURITYK9-M), Version 12.4(9)T7, RELEASE SOFTWARE (fc3)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jan-08 15:43 by prod_rel_team

200.140.228.0
Oi Internet
Added on 15.07.2014
Details
Cisco IOS Software, 2800 Software (C2800MM-ADVENTERPRISEK9-M), Version 12.4(15)T4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 13-Mar-08 03:04 by prod_rel_team

200.208.115.65
Embratele
Added on 15.07.2014
Details
Cisco IOS Software, 2800 Software (C2800MM-IPBASEK9-M), Version 12.4(12c), RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 13-Jul-07 03:05 by prod_rel_team

200.88.6.27
Compañía Dominicana de Teléfonos, C.
por A. - CODE
Added on 15.07.2014
Santo Domingo
Details
27tdev06.codetel.net.do
Cisco IOS Software, 80H097 Software (80H097-K90Y1-M), Version 12.3(8)Y62, RELEASE SOFTWARE (fc1)
Synched to technology version 12.3(10.3)T2
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri

Уязвимости в протоколах и ОС

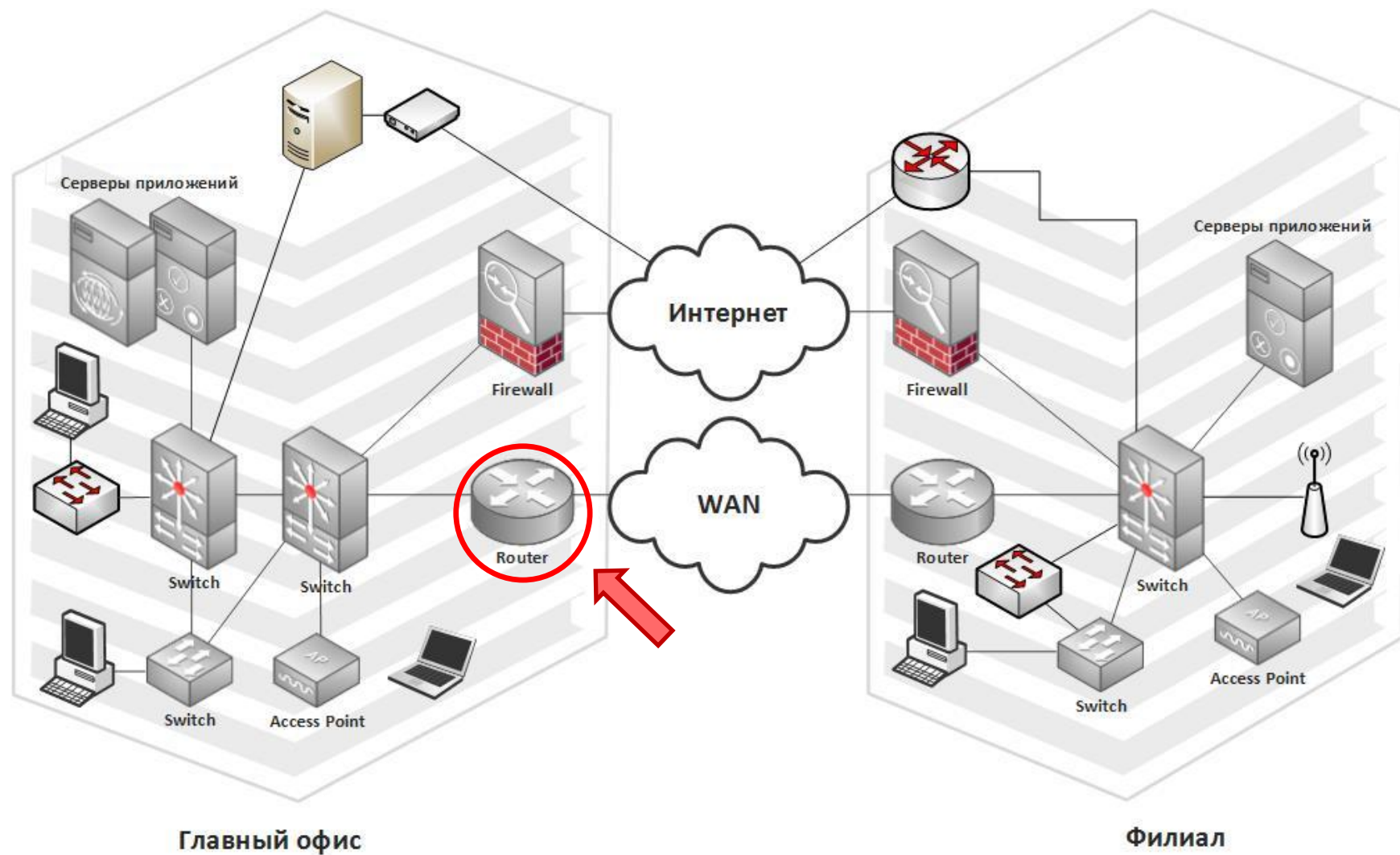
Keyword: exact phrase

Date Range:

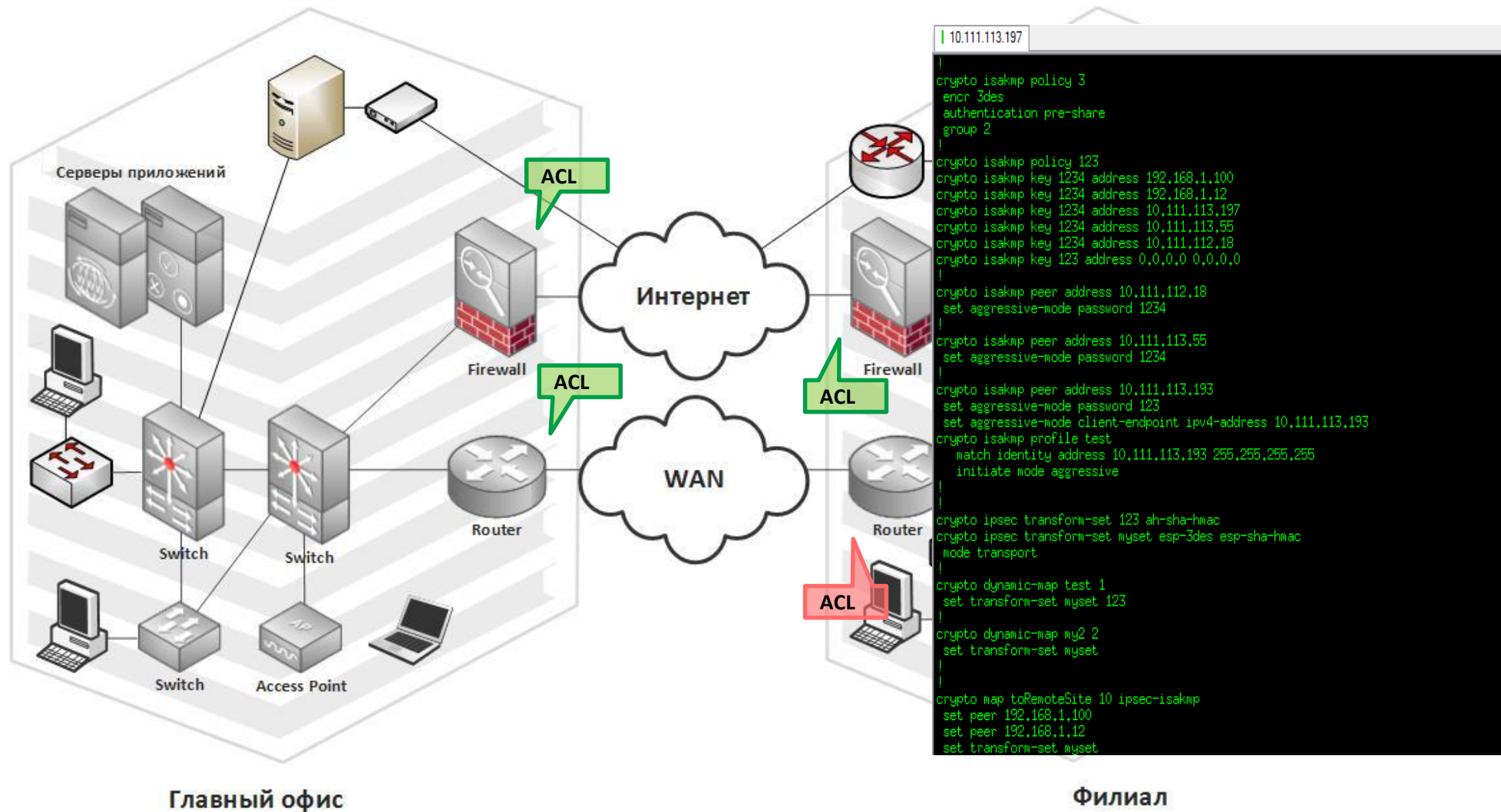
[Advanced Search](#) [Search All Security Resources](#)

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 RMB 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 RMB 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 RMB 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	RMB 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	RMB 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



Автоматизация аудита безопасности

The screenshot displays a web-based security audit interface. At the top, there are two tabs: 'Audit' (active) and 'Сводная/узлы'. Below the tabs is a navigation pane on the left titled 'Навигатор' and a main content area on the right titled 'Информация'.

In the 'Навигатор' pane, the tree structure shows the following items:

- 192.168.0.2
 - Cisco IOS
 - Отказ в обслуживании (Warning icon)
 - Отказ в обслуживании (Warning icon)
 - Включена служба HTTP (Warning icon)
 - Включена служба Telnet (Warning icon)
 - Доступ по VTU не ограничен (Warning icon)
 - Не используется шифрование пароля E (Warning icon)
 - Отказ в обслуживании (Warning icon)
 - Редко используемые сервисы (Warning icon)
 - Слабое шифрование в протоколе SSH (Warning icon)
 - Текущая и сохраненная конфигурации (Warning icon)
 - Учетные записи без шифрования пароля (Warning icon)
 - Доступ по протоколу SNMP не ограничен (Warning icon)
 - Идентификатор устройства Cisco (Info icon)
 - Имя устройства Cisco (hostname) (Info icon)
 - Интерфейсы в режиме маршрутизации (Info icon)
 - Информация о системе (Info icon)

The 'Информация' pane displays a vulnerability report for 'Cisco IOS' with a severity level of 'Серьезная уязвимость' (Critical). The report includes the following details:

Информация	
Версия:	15.2(4)S3
Метод определения:	эвристический
Максимальный уровень уязвимости:	↑ высокий уровень
Количество обнаруженных уязвимостей:	12

Результаты аудита безопасности

192.168.0.2

- Cisco IOS
 - Отказ в обслуживании
 - Отказ в обслуживании
 - Включена служба HTTP
 - Включена служба Telnet
 - Доступ по VTU не ограничен**
 - Не используется шифрование пароля E
 - Отказ в обслуживании
 - Редко используемые сервисы
 - Слабое шифрование в протоколе SSH
 - Текущая и сохраненная конфигурации
 - Учетные записи без шифрования паро
 - Доступ по протоколу SNMP не огранич
 - Идентификатор устройства Cisco
 - Имя устройства Cisco (hostname)
 - Интерфейсы в режиме маршрутизации
 - Информация о системе
 - Информация по устройству
 - Маршрутизация
 - Протокол ARP
 - Сервис SNMP
 - Сервисы
 - Список линий (lines)
 - Список учетных записей
 - Файл running-config
 - Файл startup-config
 - Файлы и контрольные суммы
- Hardware Information

Уязвимость
Доступ по VTU не ограничен
ID: 176144

Краткое описание
Убедитесь, что для всех линий VTU задан необходимый список контроля доступа.

Описание
Списки контроля доступа по VTU используются для того, чтобы ограничить круг адресов, с которых могут осуществляться попытки входа на маршрутизатор. Если настроить список контроля доступа для линий VTU, то тем самым будут ограничены источники, с которых пользователь сможет управлять устройством. Необходимо ограничить перечень узлов и/или сетей, которым разрешается подключаться к устройству по определенному протоколу для задания параметров конфигурации устройства. Доступ должен быть разрешен только тем лицам или системам, которые имеют право на администрирование устройства. Например, можно ограничить доступ, определив список разрешенных узлов; таким образом, администраторы сети смогут настраивать устройства, используя только определенные рабочие станции, предназначенные для сетевого управления. Убедитесь, что все линии VTU настроены на использование одного и того же списка контроля доступа.

Тип линии	Номер	Список доступа	Правила фильтрации
vty	0	не задан(а)	не задан(а)
vty	1	не задан(а)	не задан(а)
vty	2	не задан(а)	не задан(а)
vty	3	не задан(а)	не задан(а)
vty	4	не задан(а)	не задан(а)

Результаты аудита безопасности

192.168.0.2

- Cisco IOS
 - Отказ в обслуживании
 - Отказ в обслуживании
 - Включена служба HTTP
 - Включена служба Telnet
 - Доступ по VTU не ограничен
 - Не используется шифрование пароля E
 - Отказ в обслуживании
 - Редко используемые сервисы
 - Слабое шифрование в протоколе SSH
 - Учетные записи без шифрования паро
 - Доступ по протоколу SNMP не огранич
 - Идентификатор устройства Cisco
 - Имя устройства Cisco (hostname)
 - Интерфейсы в режиме маршрутизации
 - Информация о системе
 - Информация по устройству
 - Маршрутизация
 - Протокол ARP

Уязвимость
Редко используемые сервисы
ID: 425398

Описание

Эти сервисы могут быть использованы злоумышленниками для вызова отказа в обслуживании и других атак, которые можно предотвратить фильтрацией пакетов, при условии, что эти сервисы включены. Необходимо отключить ненужные сервисы, поскольку они обеспечивают потенциальные векторы атак и могут предоставить информацию, которая может быть использована для получения неавторизованного доступа.

Включены следующие редко используемые сервисы

- CDP
- Finger
- tcp-small-servers
- udp-small-servers

Результаты аудита безопасности

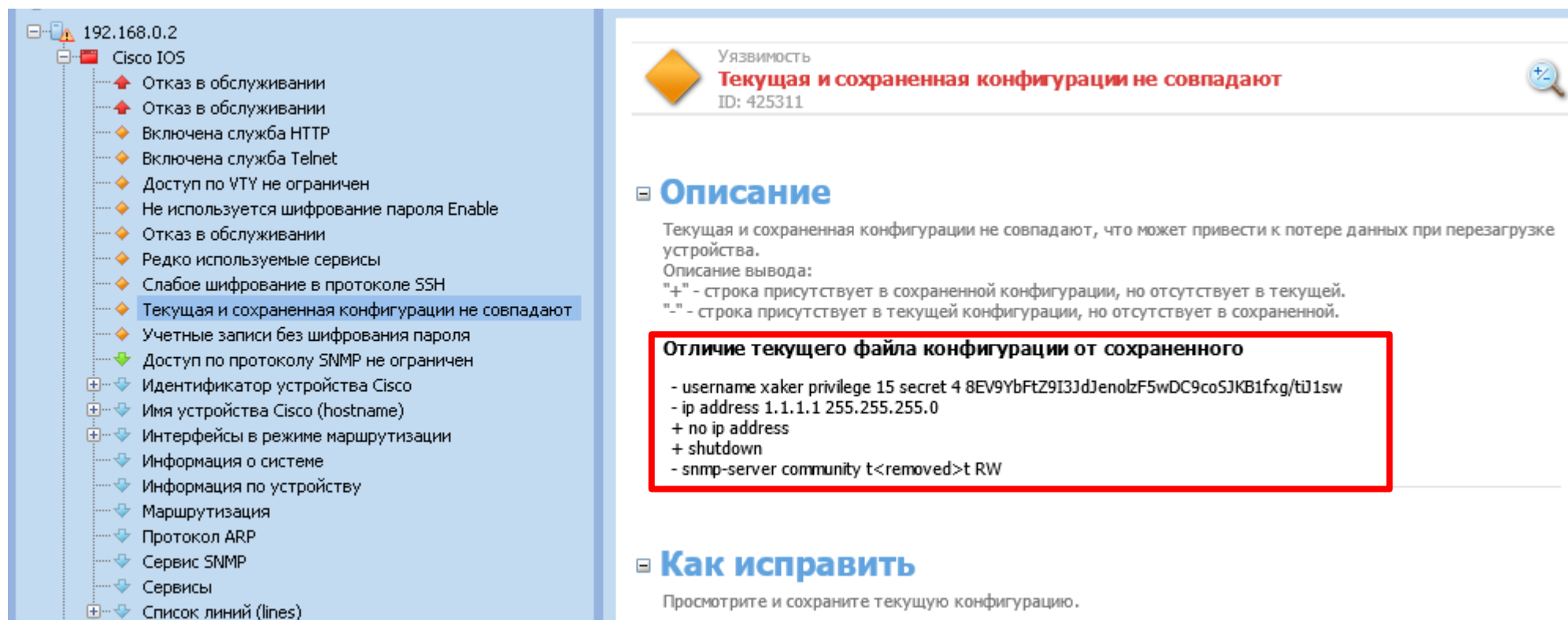
The screenshot displays a security audit tool interface with two main panels: "Навигатор" (Navigator) on the left and "Информация" (Information) on the right.

Навигатор (Navigator): Shows a tree view of the audit results for IP 192.168.0.2. Under "Cisco IOS", several items are listed, with "Отказ в обслуживании" (Service Denial) highlighted in blue.

Информация (Information): Displays details for the selected vulnerability:

- Уязвимость (Vulnerability):** **Отказ в обслуживании** (Service Denial)
ID: 182982
CVE: CVE-2013-5211
Cisco: CSCtd75033
- Краткое описание (Brief description):** Уязвимость позволяет атакующему вызвать отказ в обслуживании.
- Описание (Description):** Уязвимость в функции monlist в ntp_request.c в ntpd в NTP позволяет злоумышленникам, действующим удаленно, вызвать отказ в обслуживании (увеличение трафика) при помощи специально сформированных запросов REQ_MON_GETLIST или REQ_MON_GETLIST_1.
- Как исправить (How to fix):** Используйте рекомендации производителя:
<http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10613>
<https://tools.cisco.com/bugsearch/bug/CSCtd75033>
- Ссылки (Links):**
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211>
<http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10613>
CISCO (CSCtd75033) : <http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtd75033>

Результаты аудита безопасности



192.168.0.2
Cisco IOS

- Отказ в обслуживании
- Отказ в обслуживании
- Включена служба HTTP
- Включена служба Telnet
- Доступ по VTU не ограничен
- Не используется шифрование пароля Enable
- Отказ в обслуживании
- Редко используемые сервисы
- Слабое шифрование в протоколе SSH
- Текущая и сохраненная конфигурации не совпадают**
- Учетные записи без шифрования пароля
- Доступ по протоколу SNMP не ограничен
- Идентификатор устройства Cisco
- Имя устройства Cisco (hostname)
- Интерфейсы в режиме маршрутизации
- Информация о системе
- Информация по устройству
- Маршрутизация
- Протокол ARP
- Сервис SNMP
- Сервисы
- Список линий (lines)

Уязвимость
Текущая и сохраненная конфигурации не совпадают
ID: 425311

Описание

Текущая и сохраненная конфигурации не совпадают, что может привести к потере данных при перезагрузке устройства.
Описание вывода:
"+" - строка присутствует в сохраненной конфигурации, но отсутствует в текущей.
"- " - строка присутствует в текущей конфигурации, но отсутствует в сохраненной.

Отличие текущего файла конфигурации от сохраненного

```
- username xaker privilege 15 secret 4 8EV9YbFtZ9I3JdJenolzF5wDC9co5JKB1fxg/ti1sw  
- ip address 1.1.1.1 255.255.255.0  
+ no ip address  
+ shutdown  
- snmp-server community t<removed>t RW
```

Как исправить

Просмотрите и сохраните текущую конфигурацию.

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

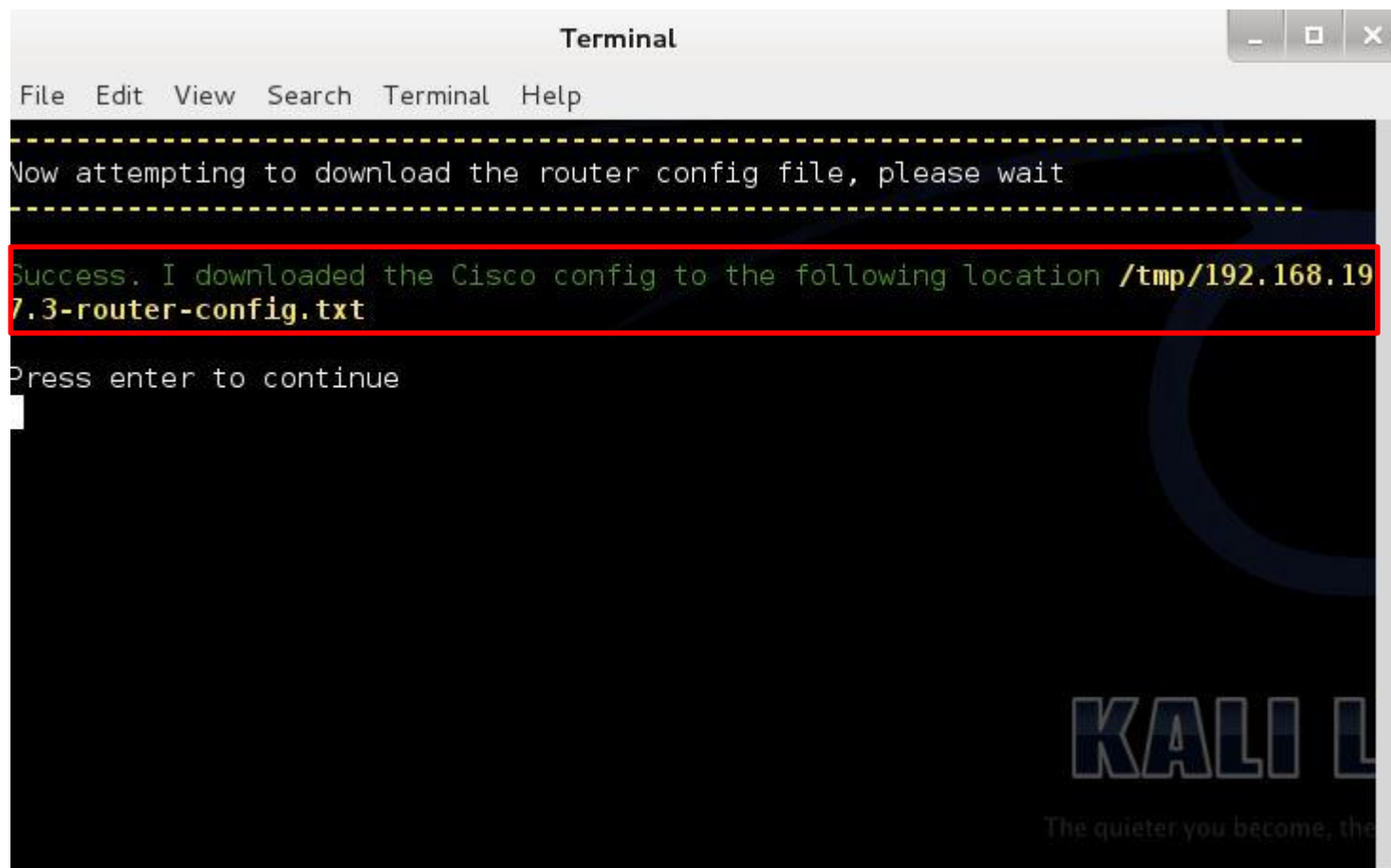
```
Interface           : [ up ] FastEthernet1/0
    Interface Speed  : 100 Mbps
    IP Address       : 192.168.0.2
    Netmask          : 255.255.255.0
    MTU              : 1500

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



A terminal window titled "Terminal" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows a message: "Now attempting to download the router config file, please wait" followed by a dashed line. Below this, a line of text is highlighted with a red box: "Success: I downloaded the Cisco config to the following location /tmp/192.168.197.3-router-config.txt". The terminal then prompts "Press enter to continue". The background of the terminal is dark with a "KALI" logo and the text "The quieter you become, the" visible at the bottom right.

```
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/192.168.197.3-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



Cisco Systems

Accessing Cisco 7206VXR "R1"

[Show diagnostic log](#) - display the diagnostic log.

[Monitor the router](#) - HTML access to the command line interface at level [0.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15](#)

[Platform](#) - platform utilities. Send comments to cs-html (below).

[Show tech-support](#) - display information commonly needed by tech support.

[Extended Ping](#) - Send extended ping commands.

[QoS Device Manager](#) - Configure and monitor QoS through the web interface.

Help resources

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447** or **+1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Проверка HTTP – Требование стандарта

Remediation:

Disable the HTTP services.

IOS:

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

Audit:

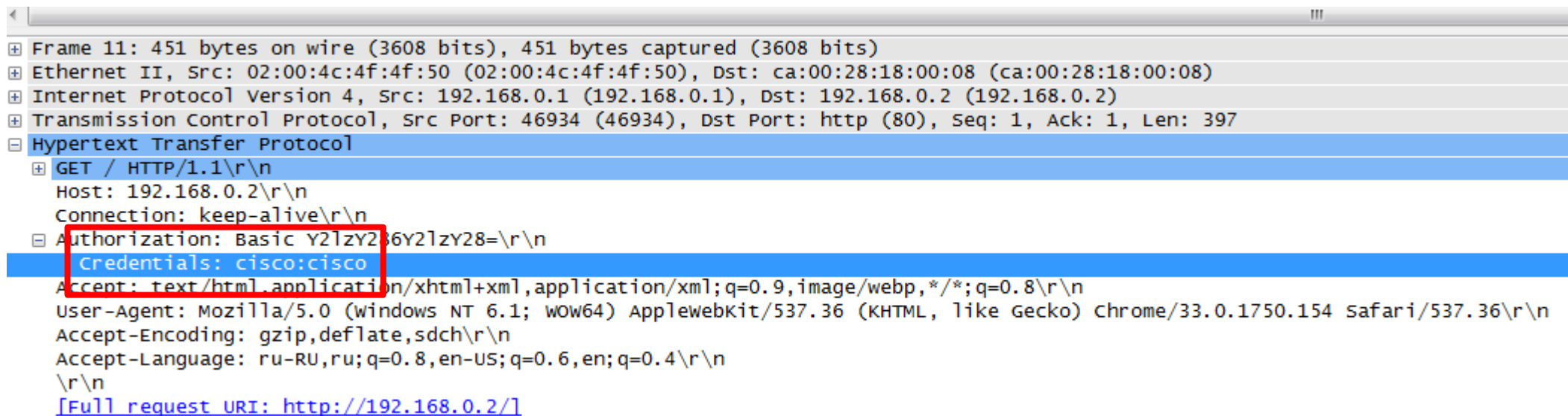
Perform the following to determine if the HTTP services are enabled:

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\nHost: 192.168.0.2\r\nConnection: keep-alive\r\nAuthorization: Basic Y2lzy286Y2lzy28=\r\n**Credentials: cisco:cisco**
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36\r\nAccept-Encoding: gzip,deflate,sdch\r\nAccept-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

IP	ID	AREA	STATE	AUTH	CRACI
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		

49	148.106304	192.168.197.128	224.0.0.5	OSPF	82 Hello Packet
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
53	158.123001	192.168.197.128	224.0.0.5	OSPF	82 Hello Packet
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

Connection Cracking Injection

Network	Netmask	Type
8.0.0.0	255.0.0.0	TYPE_ROUTER_LINKS

Network type: TYPE_ROUTER_LINKS

5] OSPF: Sending ROUTER_LINKS LSU to 192.168.197.3

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

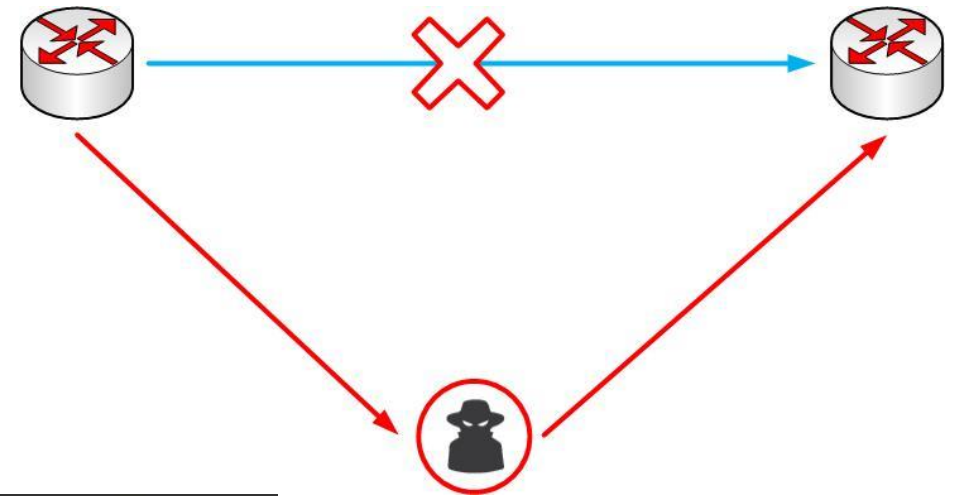
Угроза

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, участвующих 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 012526104253554E71464A5A5C
```



Результат проверки



Не соответствует

Правила паролей: Используйте стойкий алгоритм шифрования паролей для локальных пользователей

ID: 433915



Краткое описание

Необходимо сформировать по крайней мере одного локального пользователя. Для каждого пользователя должен использоваться зашифрованный пароль.

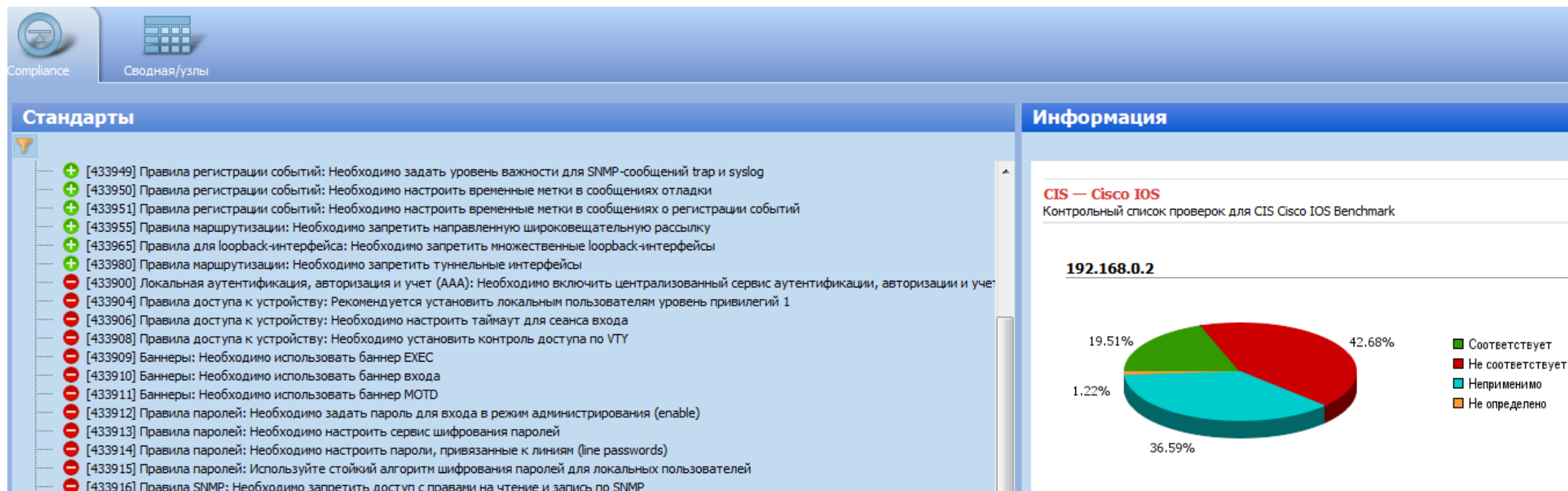
Полное описание

Стандартная конфигурация устройства не требует строгой аутентификации пользователя, что потенциально позволяет злоумышленнику получить беспрепятственный доступ к устройству. Создание локальной учетной записи с зашифрованным паролем обеспечивает аутентификацию при входе и предоставляет резервный механизм проверки подлинности для конфигурации в списке именованных методов в том случае, если централизованная система аутентификации, авторизации и учета недоступна.

Результаты проверки

Имя пользователя	Уровень привилегий	Тип
admin	15	password

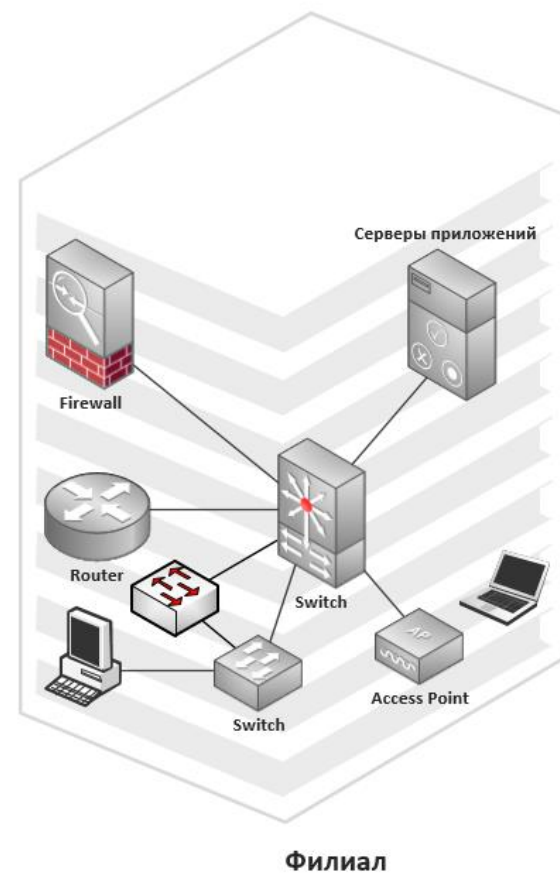
Результат сканирования



Что в итоге?

Что в итоге?

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



Конец рассказа

Спасибо за внимание

Строев Евгений

Эксперт по информационной безопасности

Positive Technologies

estroev@ptsecurity.com



POSITIVE TECHNOLOGIES