Как перейти на NGFW от CheckPoint и ничего не упустить?

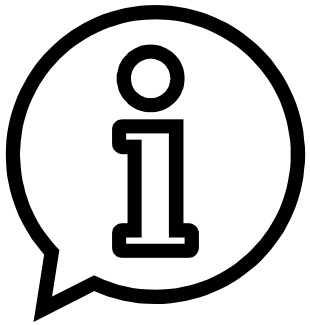
Андрей Черняков

CheckMates Live

Москва, 16 апреля 2019

X5 RETAIL GROUP

Agenda



- **Сегодня в программе**:
  - Переход на CheckPoint с другого вендора
  - Рекомендации по внедрению и эксплуатации
  - Обновление с R77.30/R80.10 на R80.20

- Как перейти на NGFW от CheckPoint и ничего не упустить?

Роль NGFW в жизни Компании

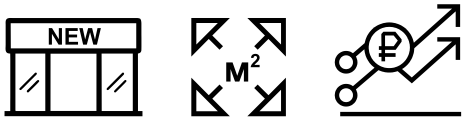
- Защита внешнего Интернет-периметра Компании
- Фильтрация трафика в сегмент DMZ
- Разграничение прав доступа внутренним пользователям и сервисам к сети Интернет
- Сегментация и защита периметров инновационных торговых объектов(SMB appliance’ы)
- Защита от угроз нулевого дня с помощью песочницы
- Анализ инцидентов ИБ через средства отчетности NGFW

В планах:

- Ограничение полосы доступа приложениям и сервисам, использующих Интернет каналы(blade QoS)
- Перенос фильтрации файлов(download/upload) на blade Content Awareness
- Тонкая настройка IPS(используя protection scope)

- Как перейти на NGFW от CheckPoint и ничего не упустить?

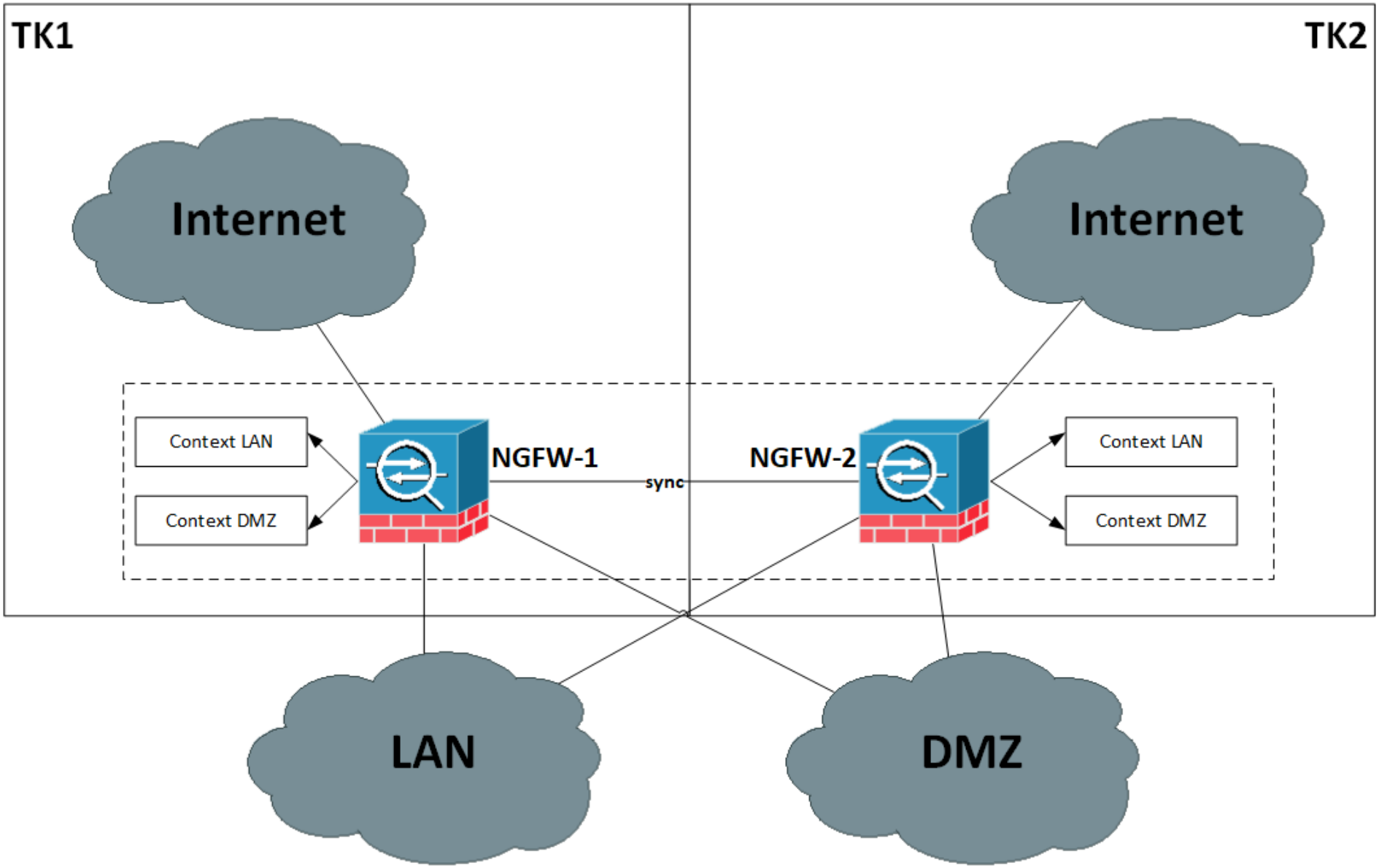
Причины перехода на CheckPoint



- Пропускной способности текущего решения NGFW переставало хватать
- Текущее решение NGFW было не способно обеспечить органический рост бизнеса на годы вперёд
- Текущий дизайн внедрения NGFW вызывал немало проблем
- Высокая критичность сервисов, работающих через сеть Интернет(онлайн кассы, ЕГАИС, Меркурий(ВетРФ)), требует надёжного, защищённого и стабильного соединения
- Был инициирован проект по модернизации корневой сети передачи данных Компании

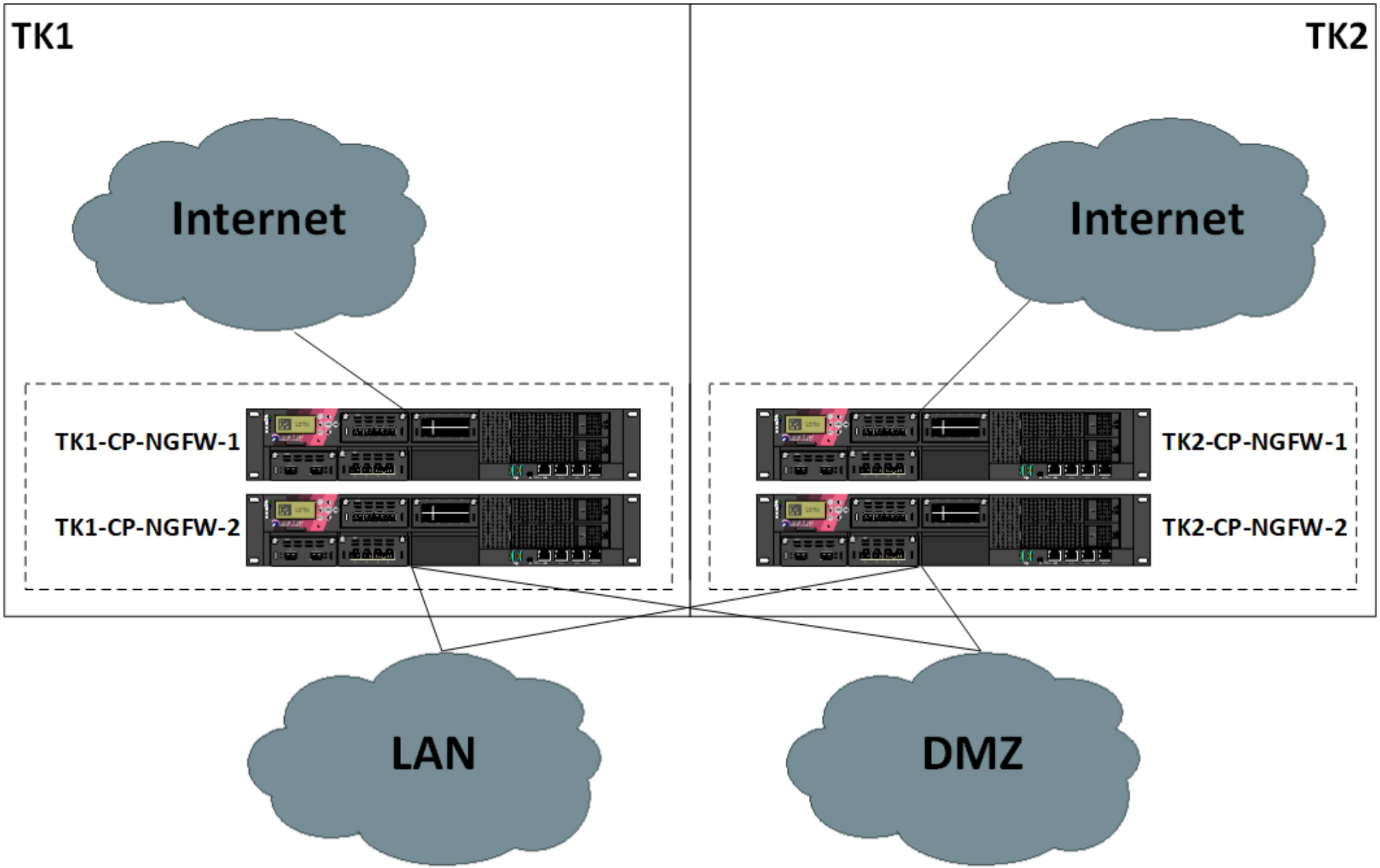
- Как перейти на NGFW от CheckPoint и ничего не упустить?

AS WAS



- Как перейти на NGFW от CheckPoint и ничего не упустить?

AS IS



- Как перейти на NGFW от CheckPoint и ничего не упустить?

Проблемы при переходе на CheckPoint

- 32-битный контекст для DMZ не выдержал дневную нагрузку на шлюзах R77.30(внедрение – конец 2017 года, R77.30). Решение – отказ от VSX, объединение политик LAN и DMZ.

- Пришлось вносить правки в политики(например, для правил с перенаправлением на captive portal)

- Проверка в излишнем количестве операционных систем приводила к перегрузке песочницы(очередь – десятки тысяч файлов, среднее время эмуляции – несколько часов). Применили рекомендованные настройки, это помогло сократить время эмуляции до 10 минут, очередь – не более 300 файлов

- Столкнулись с большим количеством RX-DROP(при проверке через netstat –ni). Решение - sk42181:

set interface *NAME_of_PHYSICAL_INTERFACE* rx-ringsize *NUMBER_OF_DESCRIPTORS*

Рекомендации по внедрению и эксплуатации

- Как перейти на NGFW от CheckPoint и ничего не упустить?

HTTPS Inspection 

✓ Оптимизируйте rulebase до нескольких правил, сгруппировав их по общим признакам(source IP, destination IP, user groups, site category)

No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificate
1	Bypass based on destination address	Any	No_HTTPS_Dst	TCP https TCP HTTP_and_HTTPS_proxy	Any	Bypass	Log	All	All	Outbound Certificate
2	Bypass based on source addresses	No_HTTPS_Src	Any	TCP https TCP HTTP_and_HTTPS_proxy	Any	Bypass	Log	All	All	Outbound Certificate
3	Users bypass	L-MSK-KLTN-Acc-Internet-for-VIP l-msk-kltn-acc-internet-for-bloomberg	Internet	TCP https TCP HTTP_and_HTTPS_proxy	Any	Bypass	Log	All	All	Outbound Certificate
4	Dont decrypt	Any	Any	TCP https TCP HTTP_and_HTTPS_proxy	Financial Services Health	Bypass	Log	All	All	Outbound Certificate
5	Predefined Rule	Any	Any	TCP https TCP HTTP_and_HTTPS_proxy	Any	Inspect	Log	All	All	Outbound Certificate

✓ Учитывайте, что без инспекции SSL трафика CheckPoint не может достоверно определить категорию сайта(например, youtube.com подписан сертификатом, где CN=*.google.com)

✓ В случае перехода с другого решения NGFW, импортируйте используемый сертификат для HTTPS инспекции на шлюзы CheckPoint

- Как перейти на NGFW от CheckPoint и ничего не упустить?

Captive Portal

- ✓ Заведите для captive portal доменное имя(прим.:https://captive.company.org/)
- ✓ Подпишите captive portal сертификатом(wildcard)
- ✓ Уберите весь “паразитный” трафик, который попадает под action:accept(display captive portal)
  - ❖ Отключив запросы в Интернет в приложениях, генерирующих этот трафик
  - ❖ Сделав подмену на DNS серверах для ’паразитных’ URL
  - ❖ Создав блокирующее этот трафик правило

  Яркий пример: detectportal.firefox.com
- ✓ Убедитесь, что доступ к captive portal настроен только с внутренних интерфейсов
- ✓ sk85040 - Web Portals become unresponsive on Security Gateway

В данном sk есть подробная информация как управлять ресурсами, выделяемыми на captive portal

Identity Collector vs AD Query

sk88520 - Best Practices - Identity Awareness Large Scale Deployment
>2 000 users = large scale deployment

AD Query:

- 800 events per second
- 30 000 ассоциаций user-IP на шлюз

Identity Collector:

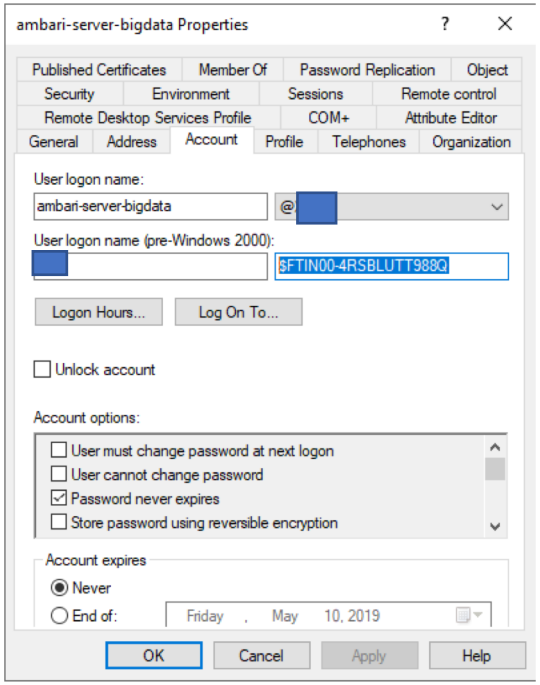
- 1900 events per second
- 200 000 ассоциаций user-IP на шлюз, 20 000 Identity Agent на шлюз
- До 35 домен контроллеров на один Identity Collector
- Поддерживается начиная с R77.30+Giraffe Hotfix(включён в Take308)/R80.10 и выше
- По нашей просьбе открыт RFE на новый функционал: оповещение о новых контроллерах домена

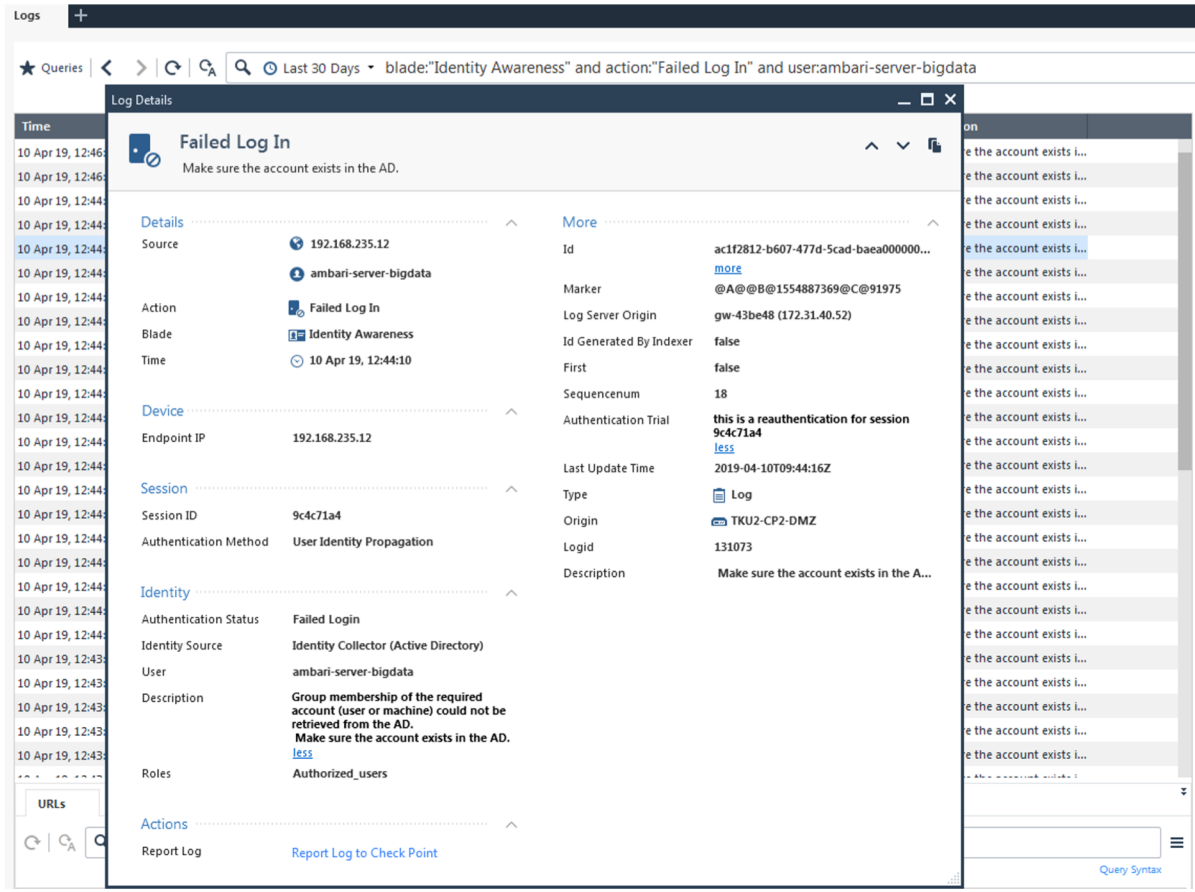
Используя Identity Collector’ы вы уменьшаете нагрузку как на шлюзы CheckPoint, так и на контроллеры домена.
В R77.30 в качества ключа для соединения между шлюзом и Identity Collector используется тот же ключ, что и для Terminal Servers

Identity Awareness and Hadoop

Система Hadoop генерирует учетные записи, используя спец. символы для User logon name

Шлюзы CheckPoint не могут получить информацию о членстве в группах таких пользователей

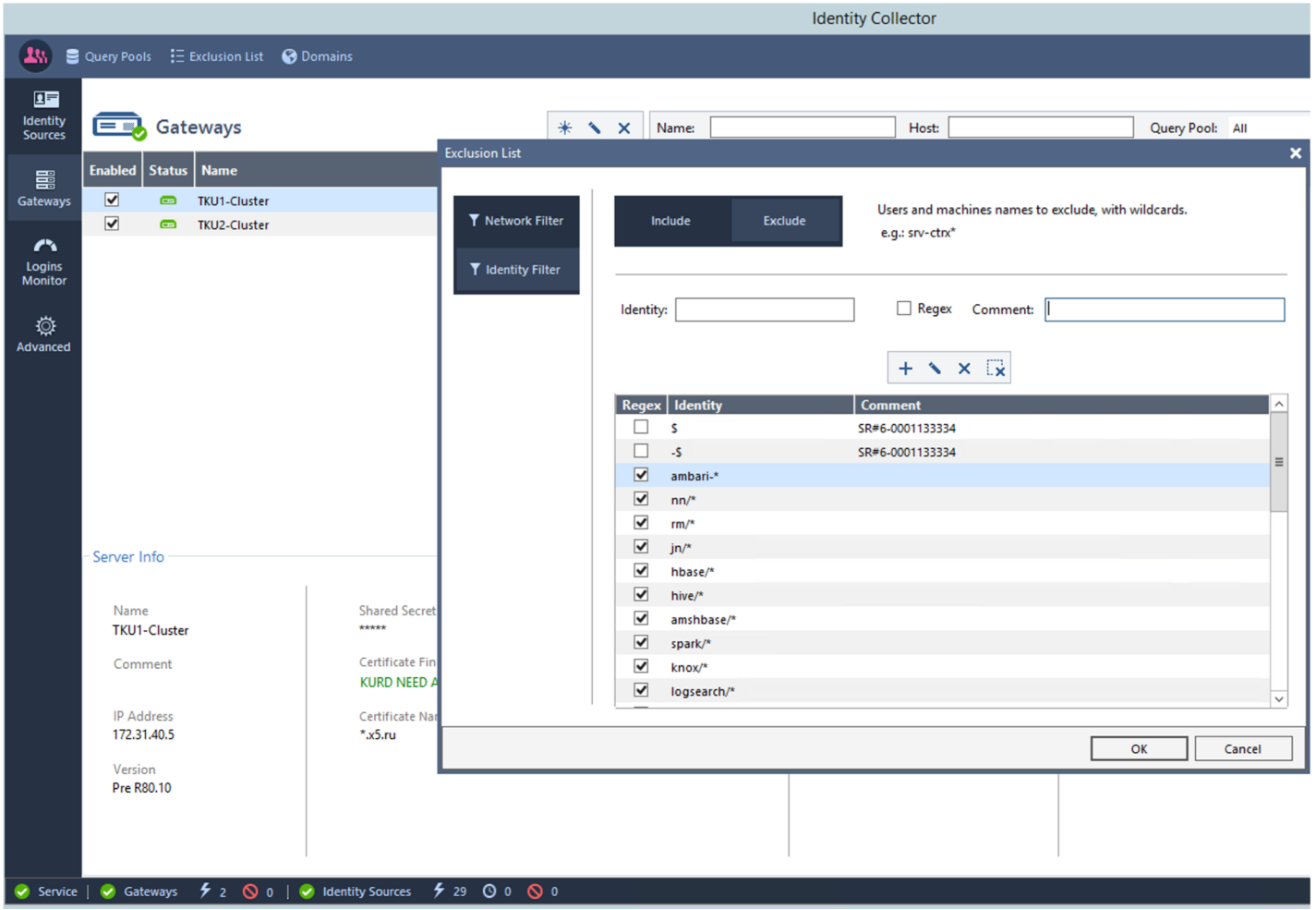




- Как перейти на NGFW от CheckPoint и ничего не упустить?

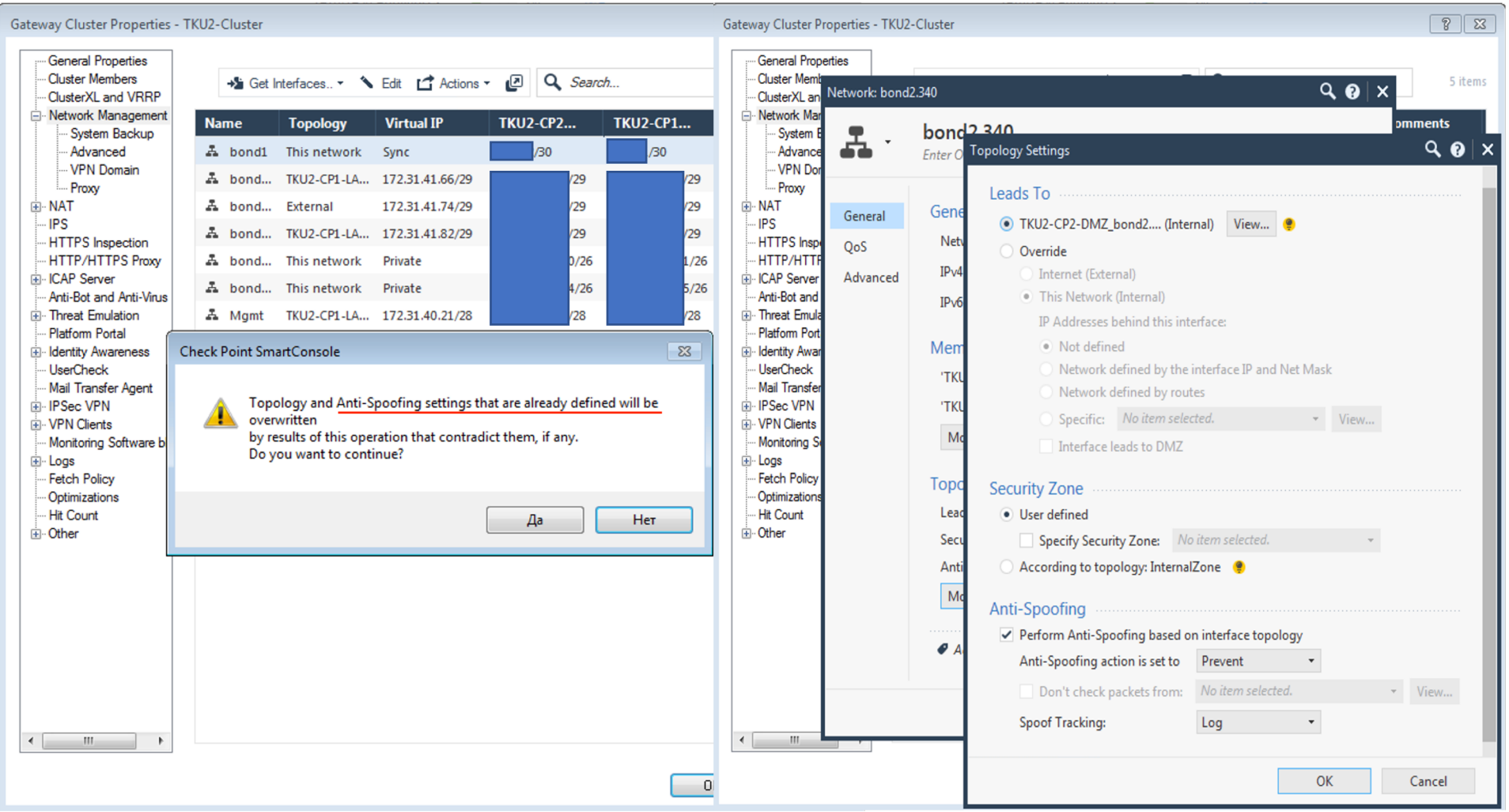
Identity Awareness and Hadoop - Solution

Исключите проблемные учетные записи и/или сервера на которых они работают на Identity Collector(ax).



- Как перейти на NGFW от CheckPoint и ничего не упустить?

Antispoofing включился/изменился ”сам”



- Как перейти на NGFW от CheckPoint и ничего не упустить?

LOM порт

LOM port – ваш главный помощник в критической ситуации и вы обязаны его настроить. Он поможет не только получить доступ в консоль, но и управлять питанием appliance’а.

Если вам надо изменить настройки IP/mask/GW:
sk92986 - How to check and set an IP address of a LOM card on a Check Point appliance

Если вам надо сбросить пароль для пользователя LOM интерфейса:
https://community.pivotal.io/s/article/How-to-work-on-IPMI-and-IPMITOOL

Обновление с R77.30/R80.10 на R80.20

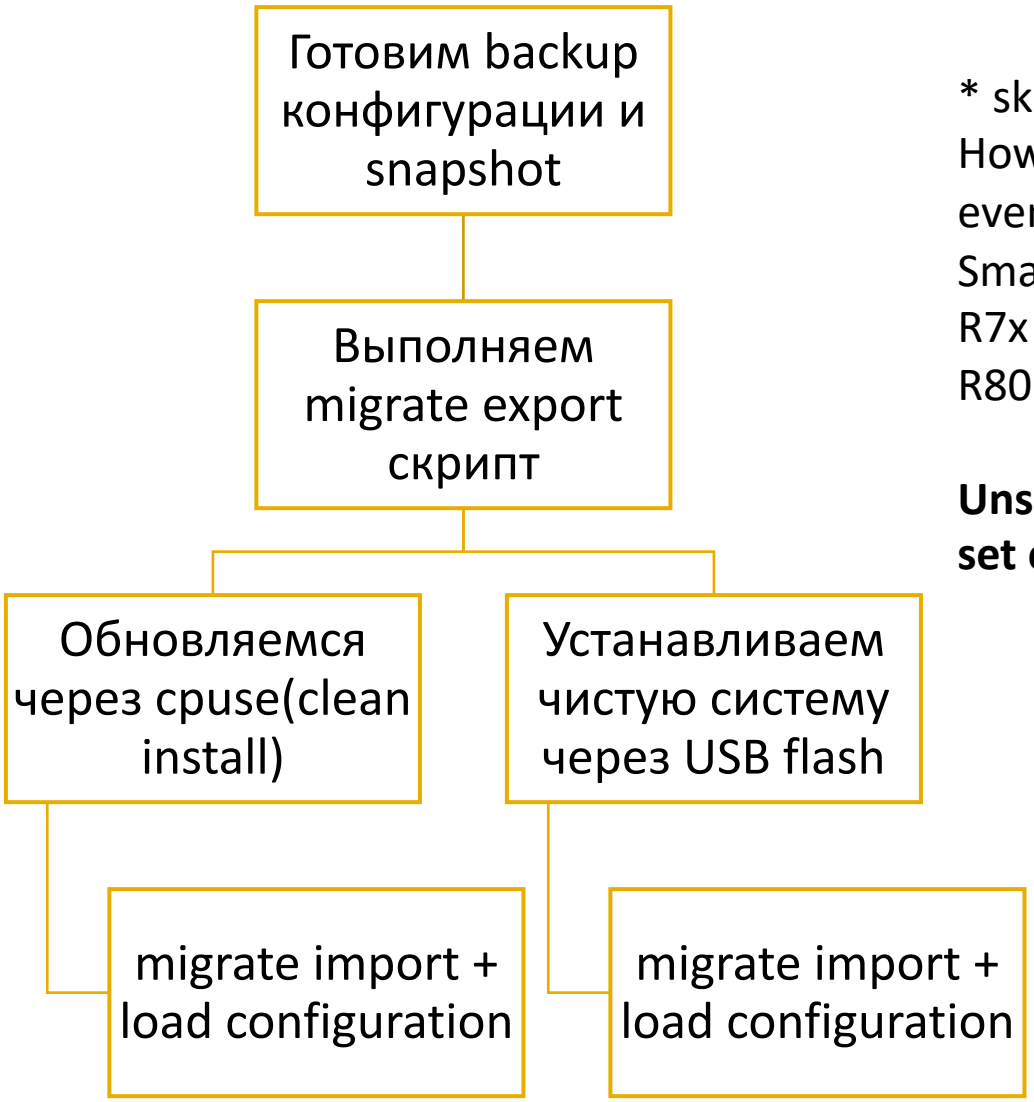
- Как перейти на NGFW от CheckPoint и ничего не упустить?

Почему мы обновляемся до R80.20?

1) Встроенный ICAP клиент
2) API для GaiaOS на шлюзах
3) Новый blade – Content Awareness
4) Полноценная поддержка dynamic objects
5) Полноценная поддержка domain objects
6) Полноценная поддержка time objects
7) Возможность более тонкой настройки IPS

- Как перейти на NGFW от CheckPoint и ничего не упустить?

Обновление SmartManagement/SmartEvent*



* sk110173
How to migrate the events database from SmartEvent server R7x to SmartEvent R80 and above server

Unsupported command: set edition 64-bit

Зачем ставить GaiaOS с USB flash?

1) Файловая система будет переформатирована из ext3 в xfs

```
[Expert@MSK-RCOD-CPMgmtServer:0]# df -T
Filesystem                     Type   1K-blocks       Used Available Use% Mounted on
/dev/mapper/vg_splat-lv_current xfs    209612800   48151484 161461316  23% /
/dev/sda1                      ext3       297485      54952    227173  20% /boot
tmpfs                          tmpfs    66034456          4  66034452   1% /dev/shm
/dev/mapper/vg_splat-lv_log    xfs    3070500000 2543092384 527407616  83% /var/log
[Expert@MSK-RCOD-CPMgmtServer:0]#
```

2) Структура разделов(partition table) станет GPT

```
[Expert@MSK-RCOD-CPMgmtServer:0]# parted -l
Model: LSI MR9240-4i (scsi)
Disk /dev/sda: 1979GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
 1      17.4kB  315MB   315MB   ext3               boot
 2      315MB   1979GB  1979GB                     lvm


Model: LSI MR9240-4i (scsi)
Disk /dev/sdb: 1979GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system     Name  Flags
 1      17.4kB  135GB   135GB   linux-swap(v1)        boot
 2      135GB   1979GB  1844GB                        lvm
```

- Как перейти на NGFW от CheckPoint и ничего не упустить?

Какую USB flash выбрать? /ISOmorphic Tool

sk92423 - Errors when machine boots from a USB device formatted by ISOmorphic Tool
Solution: Make sure that USB key that you use is a USB 2.0 and that USB does not identify itself as fixed disk.

sk83200 - Installation of Gaia R75.45 - R77.30 on IPSO-based IP Series appliances from USB storage device

(2) Supported USB storage devices

The following USB storage devices have been tested and worked:

- *HP USB sticks (8G and 16G tested OK)*
- *Kingston Data Traveler G2 1.00 4GB*
- *Silicon Power 15GB and 16GB*
- *Imation 4GB*
- *PNY 8GB*
- *Sandisk Cruzer 4GB*
- *Gigamon "China" 4GB*
- *Lexar JumpDrive USB Flash Drive 4GB*

The following USB storage devices have been tested and the following issues were found:

USB storage device	Issue	Next Step
Sandisk Cruzer 8G	Installation script exits, and unit ends up in the Gaia Boot manager.	Refer to Workaround B below.
Sandisk 32G	Does not work; installation script interprets this USB device as a fixed HDD, and formats it with Gaia file system.	Refer to Workaround C below.
PNY 4G	Installation script exits, and unit ends up in the Gaia Boot manager.	Refer to Workaround B below.
Kingston DataTraveler G2 16GB	Works on all IP Series appliances, except IP290.	On IP290 appliance only, refer to Workaround A below.
A-DATA C906 4GB	Does not work.	None.
Emtec Micro USB Flash Drive 8GB	Does not work.	None.

Important Note: Use USB storage devices, which have only one partition. If a USB storage device was previously used for a third-party application, or is partially encrypted, Check Point ISOmorphic tool will not be able to remove the extraneous partitions, and the installation will fail.

- Как перейти на NGFW от CheckPoint и ничего не упустить?

Обновление кластера шлюзов(R77.30->R80.20)

В случае, если вы всё же решили обновлять шлюз через CPUSE – убедитесь что у вас есть статический маршрут к вашему ПК через mgmt интерфейс

Unsupported command: set edition 64-bit

После перехода на R80.20 

SmartManagement и SmartEvent(с R80.10 до R80.20):

- Проверить работу сторонних систем, использующих протокол OPSEC

Hint 1: Сделайте backup файла конфигурации OPSEC:$FWDIR/conf/fwopsec.conf
Hint 2: вместо OPSEC LEA можно перейти на использование LogExporter, который есть в составе R80.20

Шлюзы CheckPoint(с R77.30 до R80.20):

- Перенастроить шлюзы в Identity Collector
- Проверить, определяются ли пользователи в подгруппах AD

(sk148092 - Users are not matched to access roles with nested LDAP groups or LDAP groups with filter)

- Изменится формат logging (станет per connection)

Песочница обновляется самой последней. Перед обновлением песочницы переключаем эмуляцию файлов в облако, проводим upgrade и возвращаем эмуляцию обратно в песочницу.

Спасибо за внимание!

andrey.chernyakov@x5.ru

@oldflint