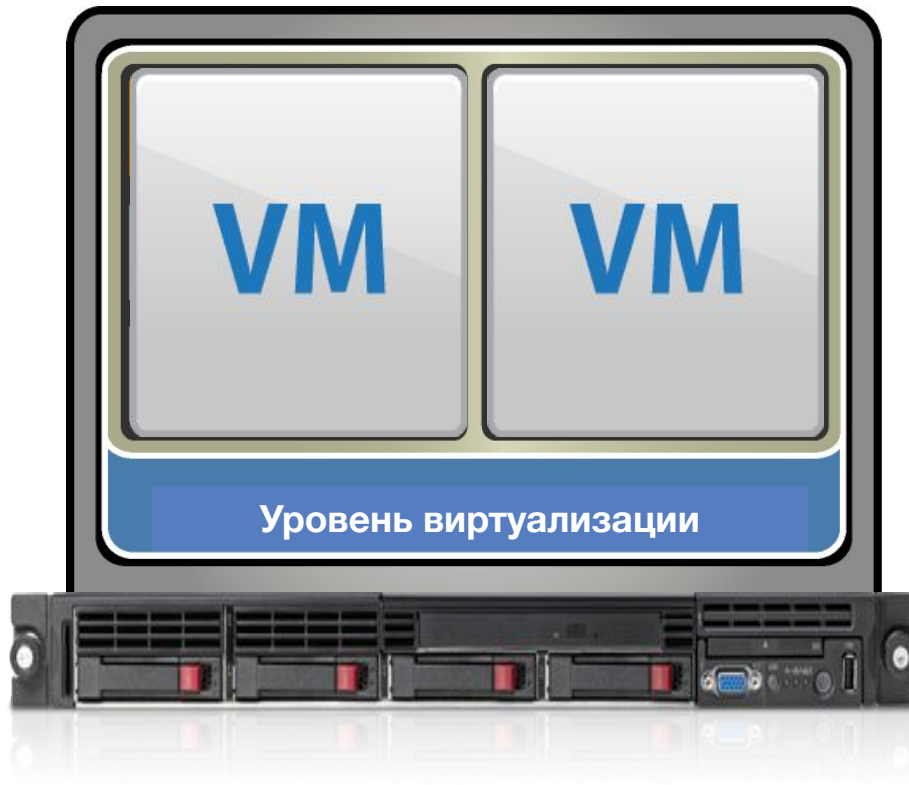




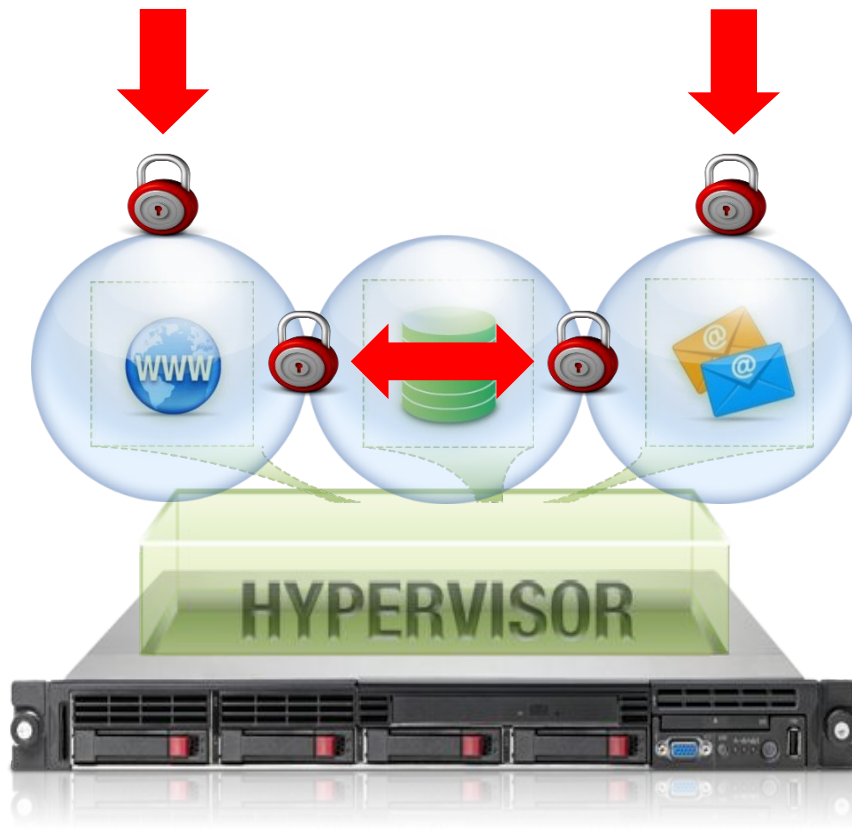
Security Gateway Virtual Edition (VE)

Сергей Голяк
RRC Россия | технический специалист
sgolyak@rrc.ru
Тел.: +7-495-956-1717 * 1129





- Виртуализация отделяет физические ресурсы от ОС и приложений
- Машины помещаются в файлы



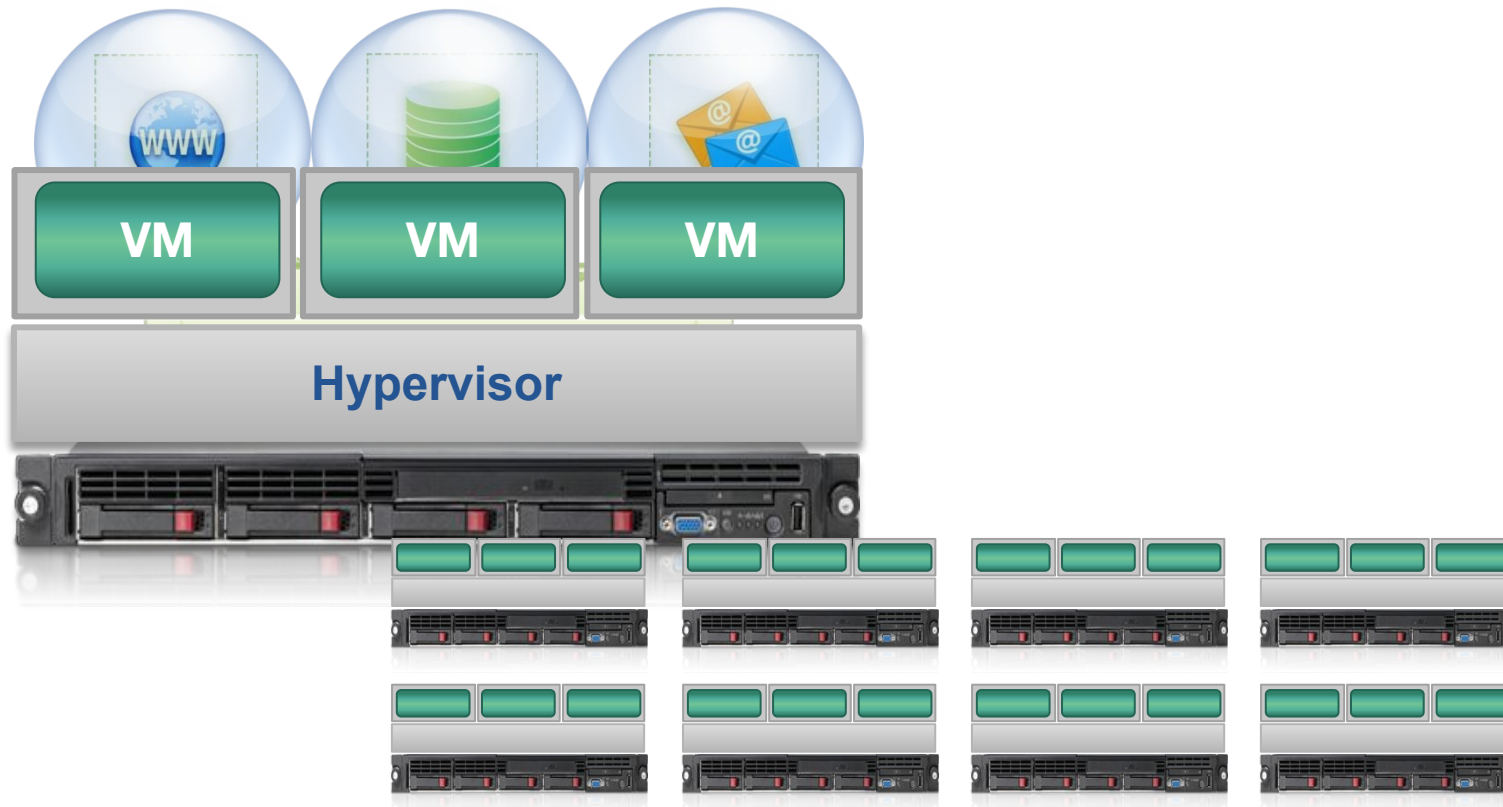
Вызовы безопасности в виртуализованных средах

Защита от внешних угроз

Анализ трафика между
виртуальными машинами

Автоматическая защита
новых виртуальных машин

Вызовы безопасности в виртуализованных средах





**Вызовы безопасности
в виртуализованных средах
(ЦОД/Облако)**

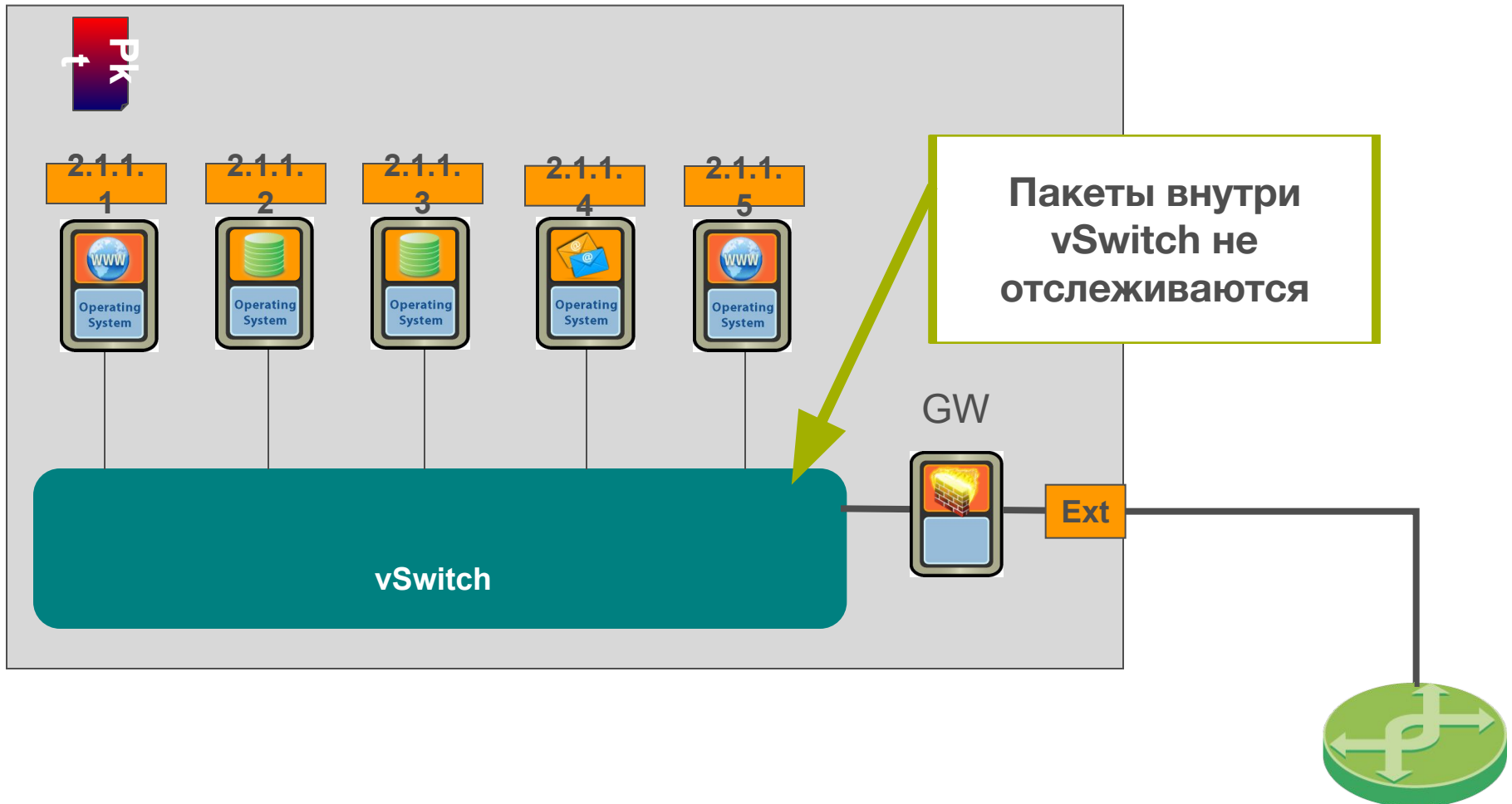
**Обеспечить защиту в
динамических средах**

**Поддерживать безотказную
работу во время миграции**



Внедрения до интеграции с VMsafe

Шлюз не в курсе трафика внутри vSwitch



Представляем Check Point Security Gateway Virtual Edition (VE)



Check Point предлагает легко встраиваемую защиту для публичных и частных облаков

От
\$2,000

Check Point
Security Gateway
Virtual Edition



Software
Blades

NEW!

Лучший шлюз защиты виртуализации с архитектурой Software Blade

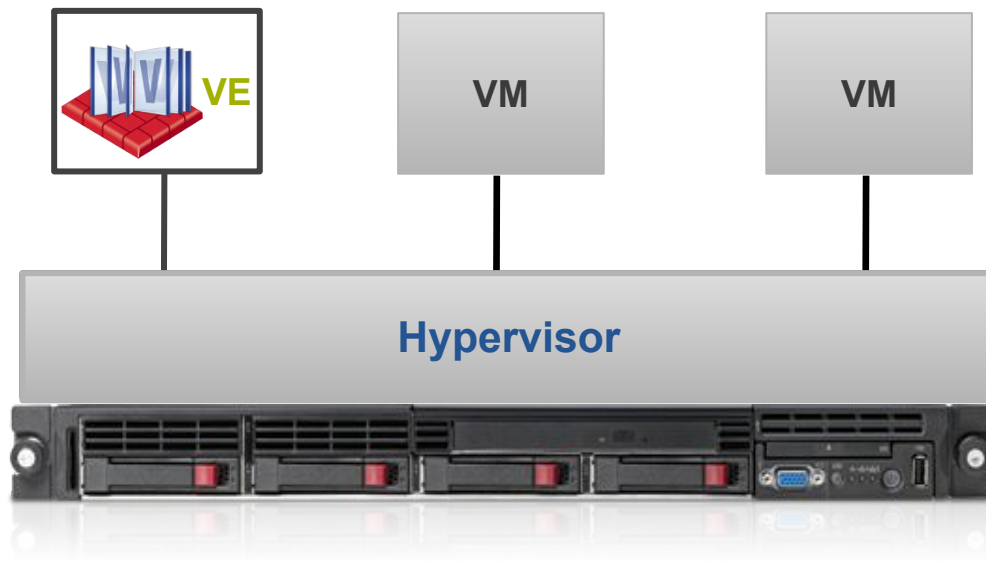
NEW!

Защищает виртуальные машины

Унифицированное управление физическими и виртуальными шлюзами



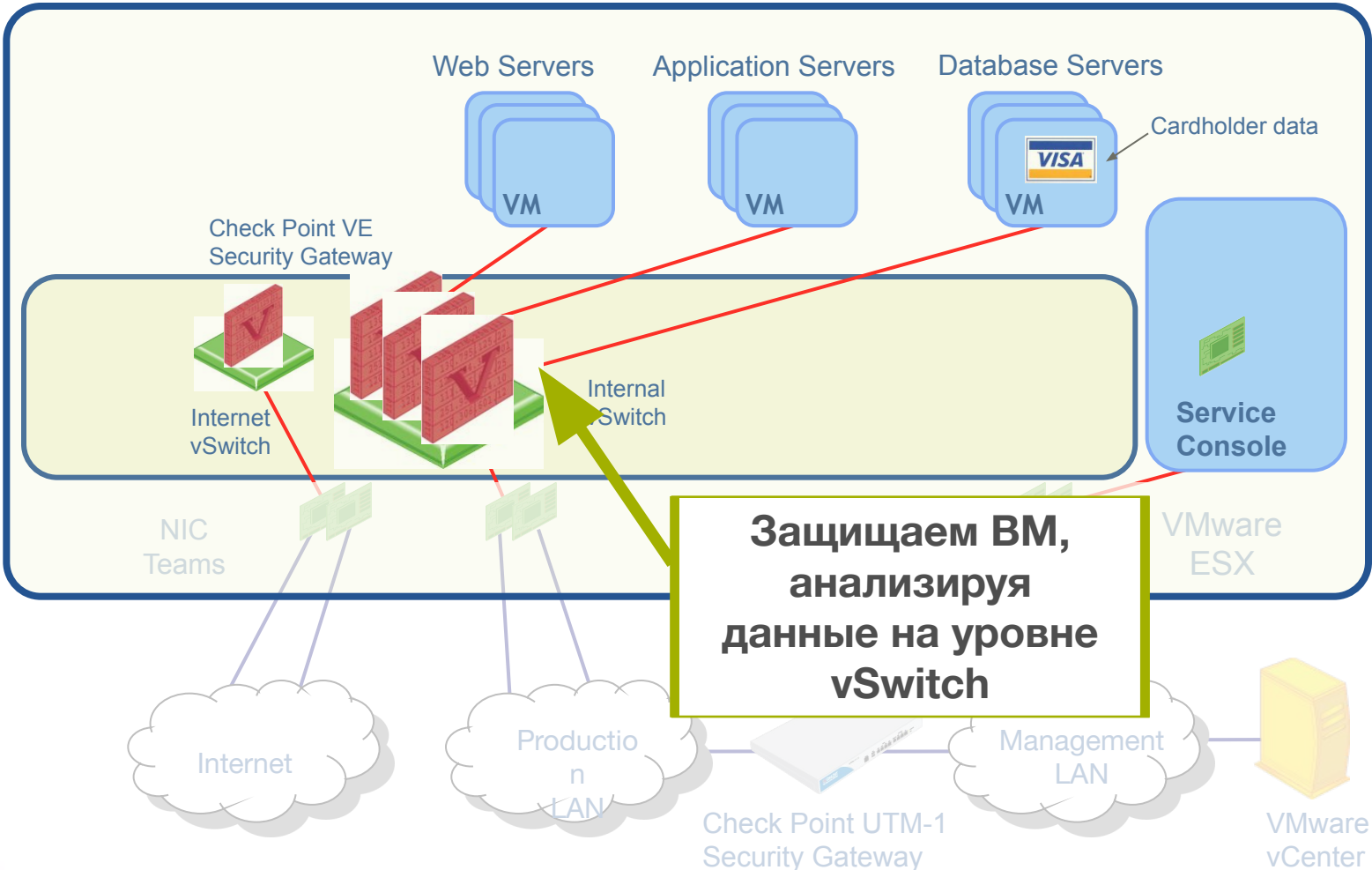
Анализ трафика между VM обеспечивает их защиту



- ▶ Защита встроена в Hypervisor
- ▶ Интеграция с технологией VMsafe
- ▶ Аудит изменений конфигурации сервера виртуализации

Security Gateway VE и VMsafe

Полная интеграция и поддержка технологий VMware - VMotion, Storage VMotion, HA и др.



Возможности Virtual Edition

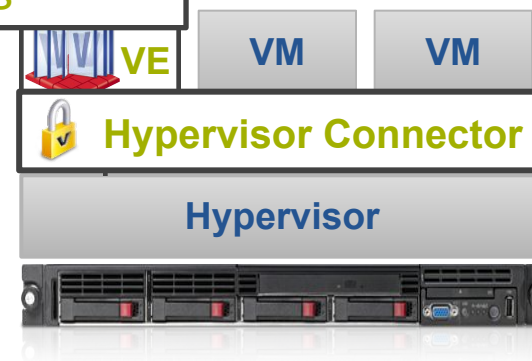
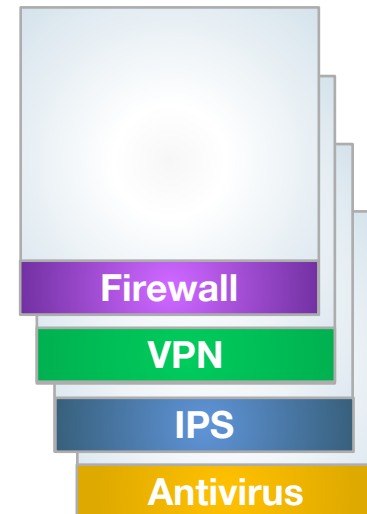
Лучшая защита

- ▶ Включает МСЭ, IPS, VPN и все остальные Software Blade.
- ▶ Гибкая, расширяемая защита

Check Point Security Gateway Virtual Edition (VE)



Software
Blades



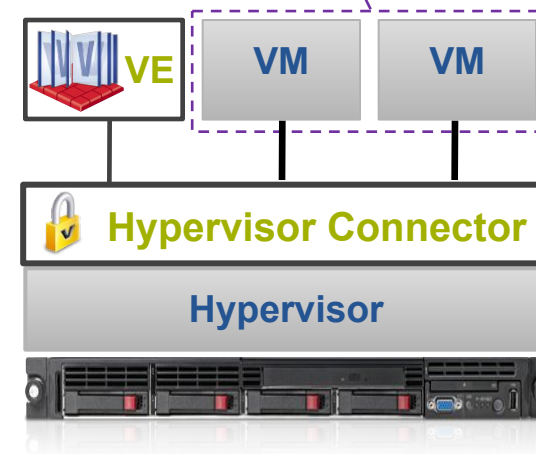
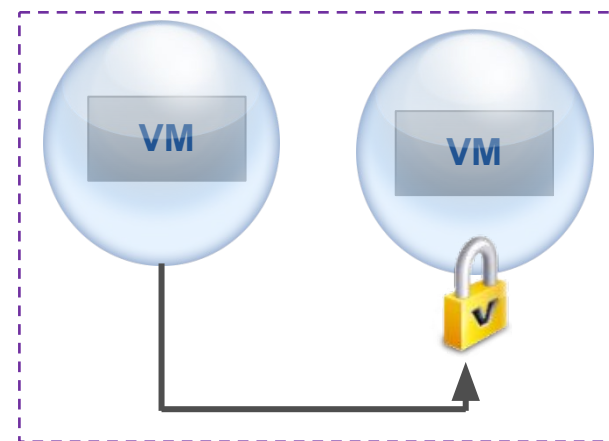
Возможности Virtual Edition

Лучшая защита

- ▶ Включает МСЭ, IPS, VPN и все остальные Software Blade.
- ▶ Гибкая, расширяемая защита

Защита VM

- ▶ Встроенная, без изменений топологии
- ▶ Автоматически защищает новые VM
- ▶ Непрерывная работа при миграции VM



Проверка трафика между VM

Возможности Virtual Edition

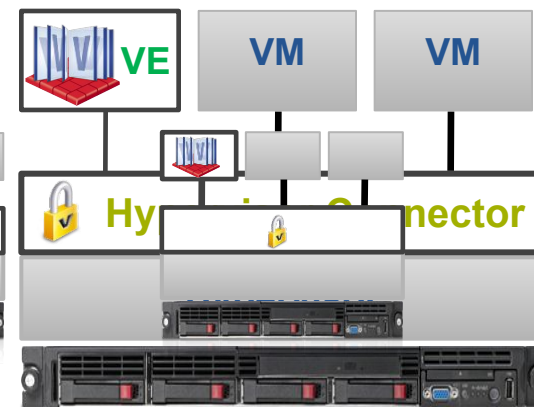
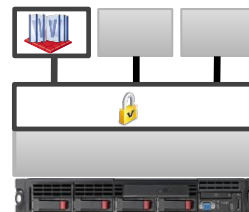
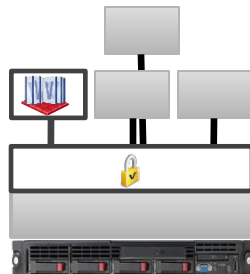
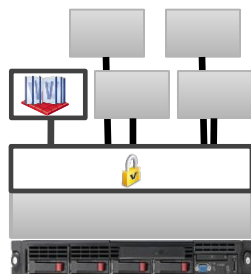
Лучшая защита

- ▶ Включает МСЭ, IPS, VPN и все остальные Software Blade.
- ▶ Гибкая, расширяемая защита

Защита VM

- ▶ Встроенная, без изменений топологии
- ▶ Автоматически защищает новые VM
- ▶ Непрерывная работа при миграции VM

Защита динамических сред



Возможности Virtual Edition

Лучшая защита

- ▶ Включает МСЭ, IPS, VPN и все остальные Software Blade.
- ▶ Гибкая, расширяемая защита

Защита VM

- ▶ Встроенная, без изменений топологии
- ▶ Автоматически защищает новые VM
- ▶ Непрерывная работа при миграции VM

- ▶ Общее управление физическими и виртуальными МСЭ
- ▶ Блейды управления работают на виртуальной машине



Возможности Virtual Edition

Лучшая защита

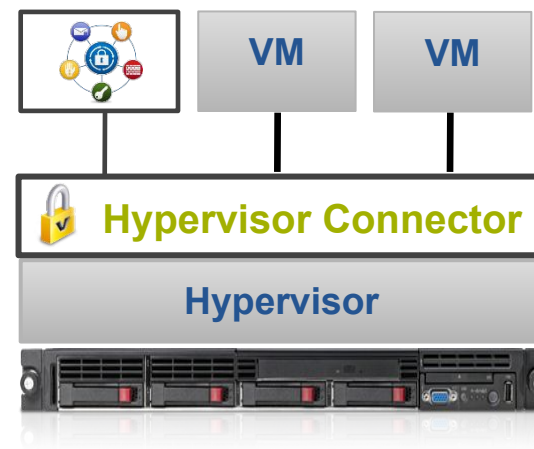
- ▶ Включает МСЭ, IPS, VPN и все остальные Software Blade.
- ▶ Гибкая, расширяемая защита

Защита VM

- ▶ Встроенная, без изменений топологии
- ▶ Автоматически защищает новые VM
- ▶ Непрерывная работа при миграции VM

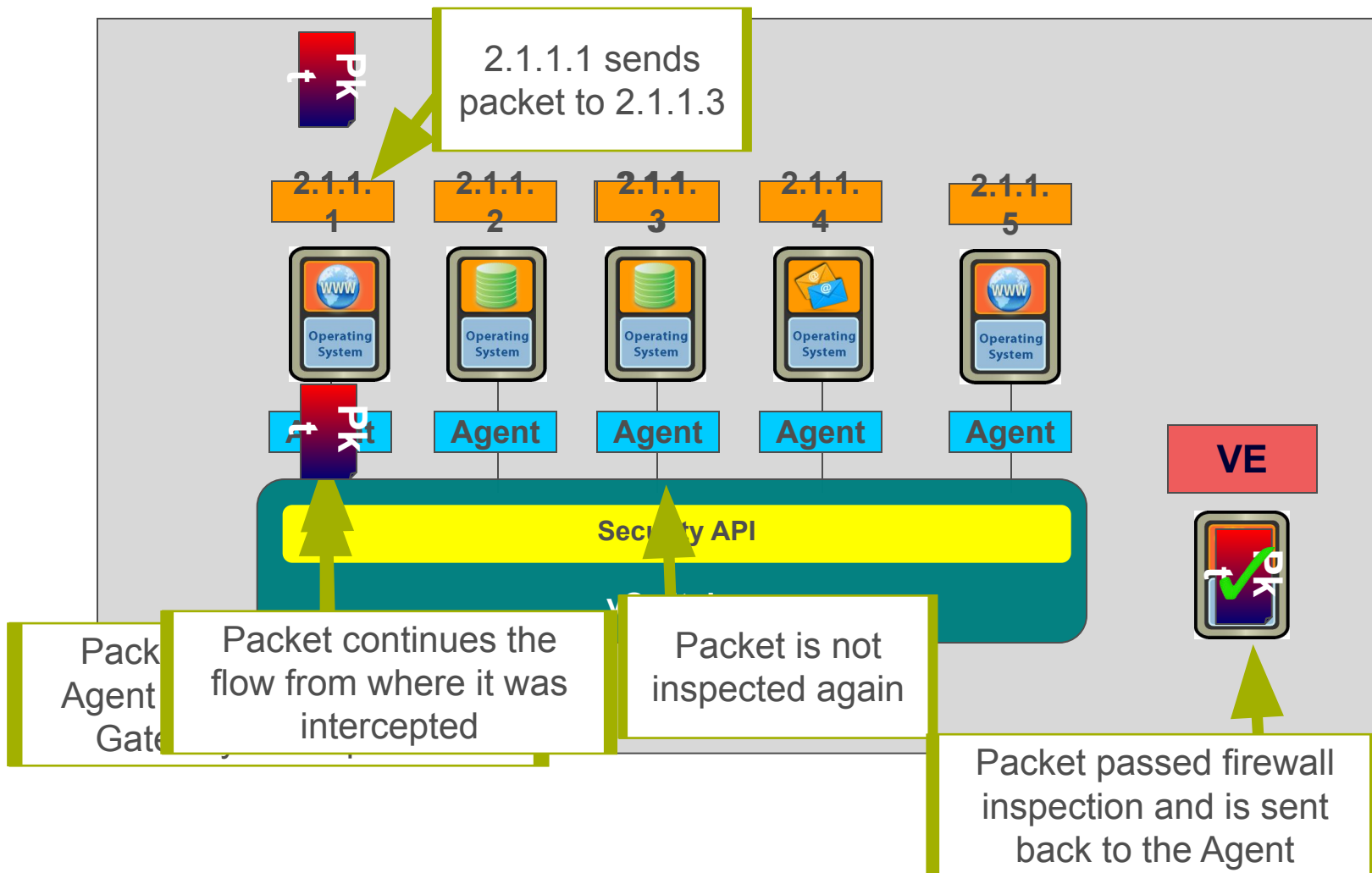
- ▶ Общее управление физическими и виртуальными устройствами
- ▶ Блейды управления работают на виртуальной машине

Виртуализация систем управления

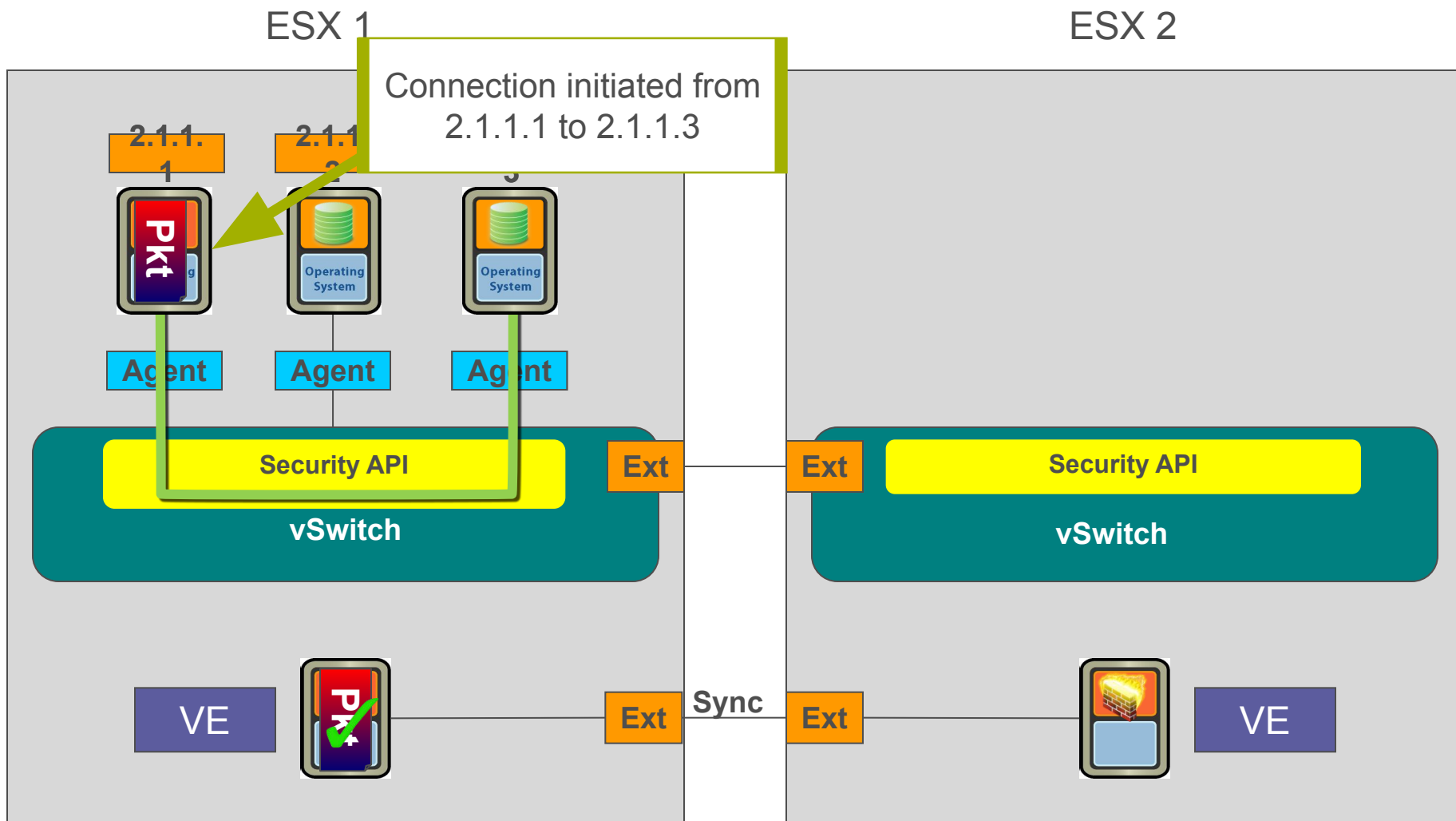


Защищенный поток пакетов на уровне 2

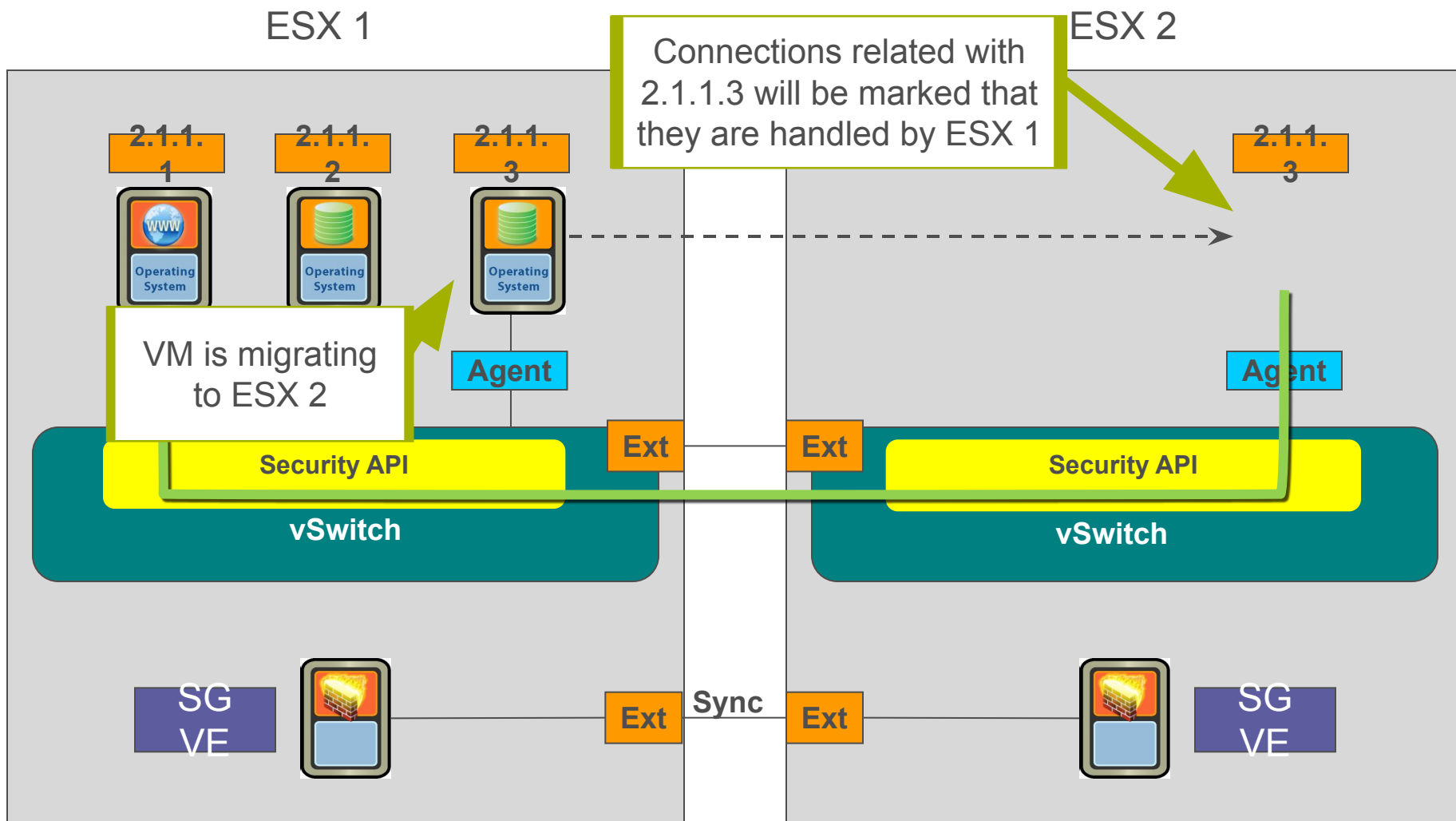
ESX Server



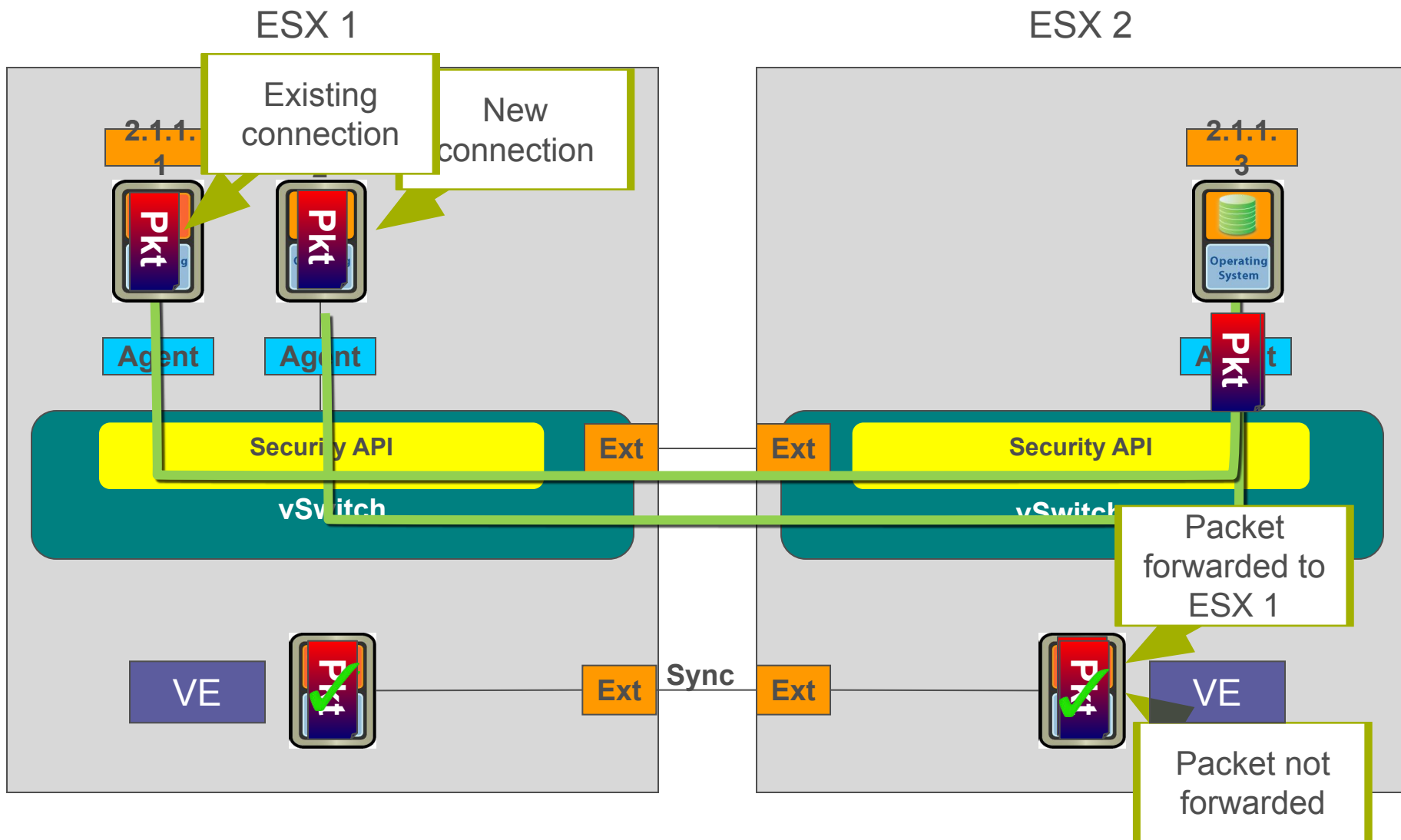
Защита уровня 2 в динамических средах



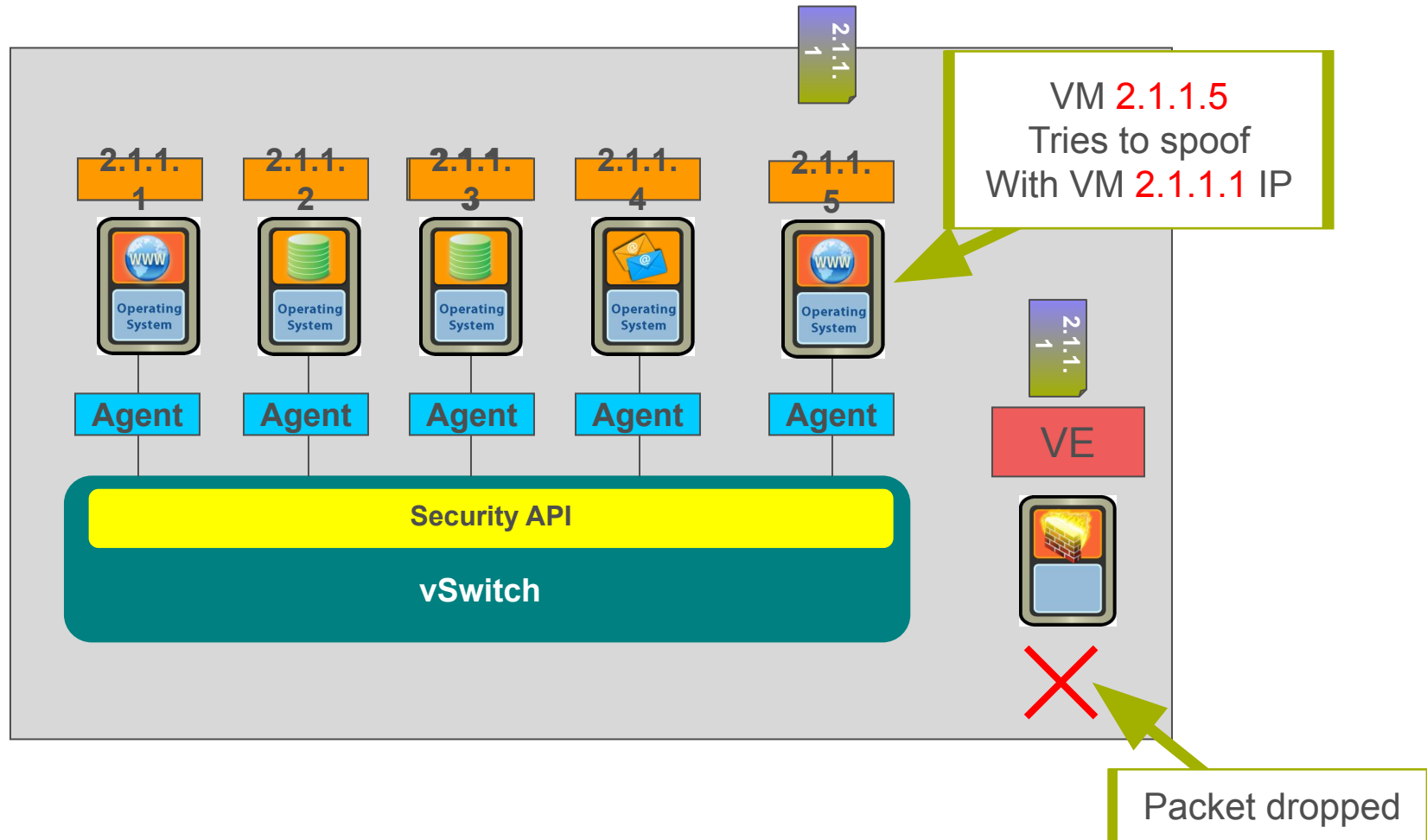
Защита уровня 2 в динамических средах



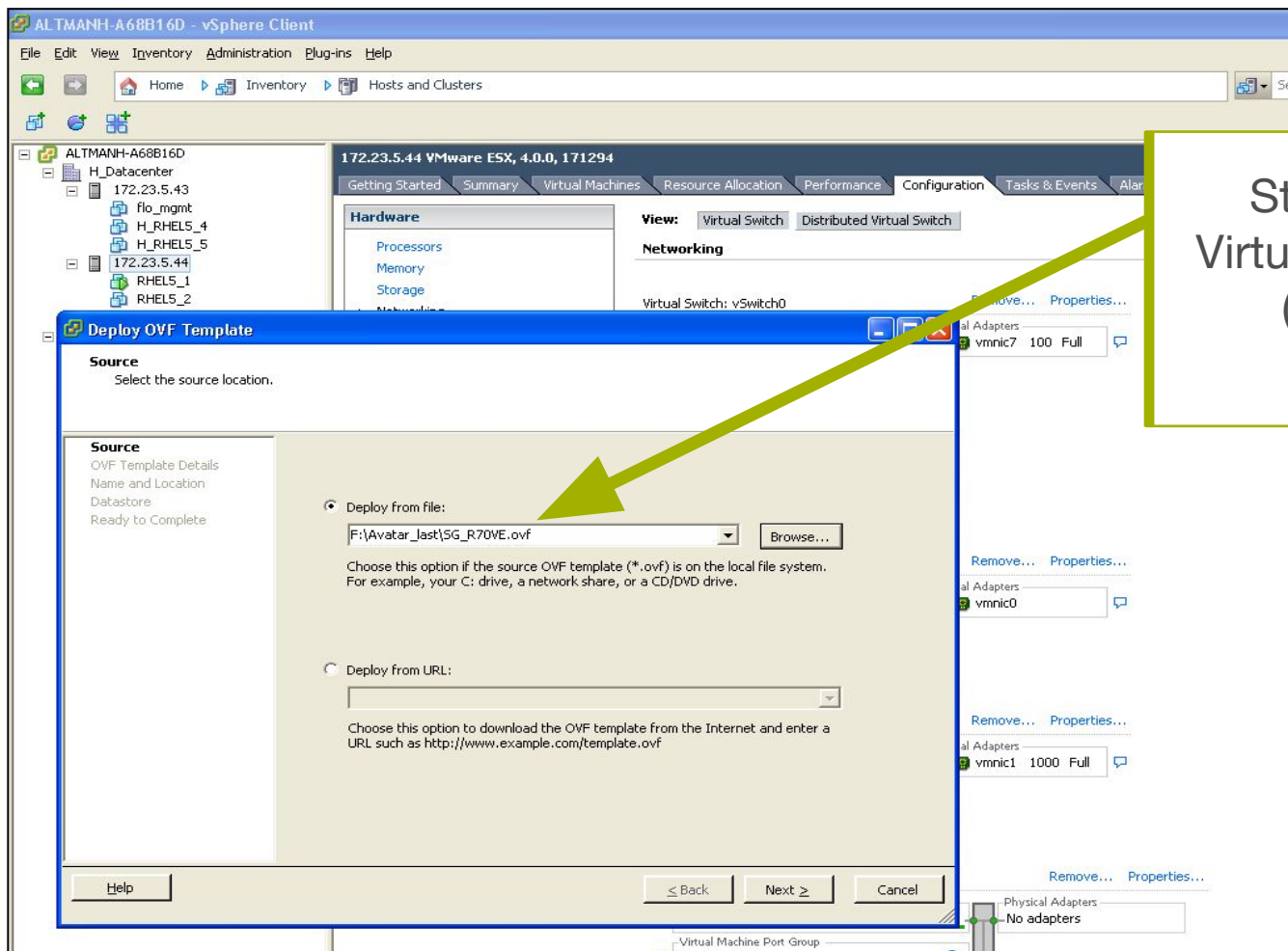
Защита уровня 2 в динамических средах



Демонстрация Anti-spoofing

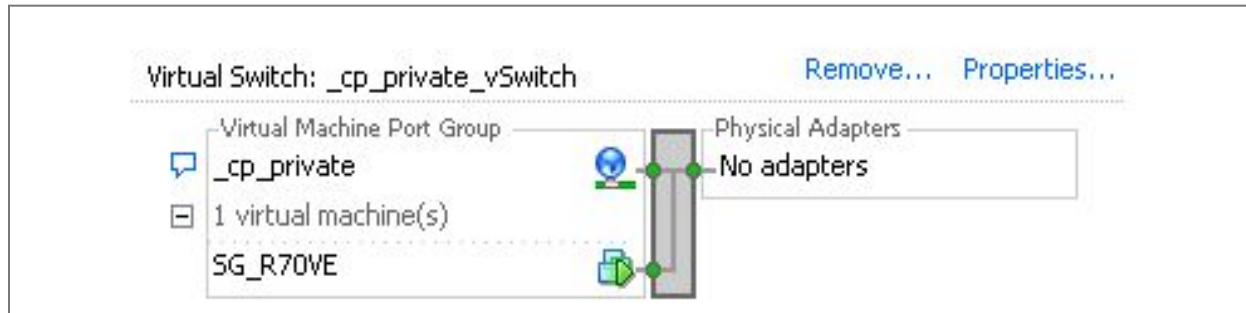


Защитите виртуальную среду, установив подготовленную VM



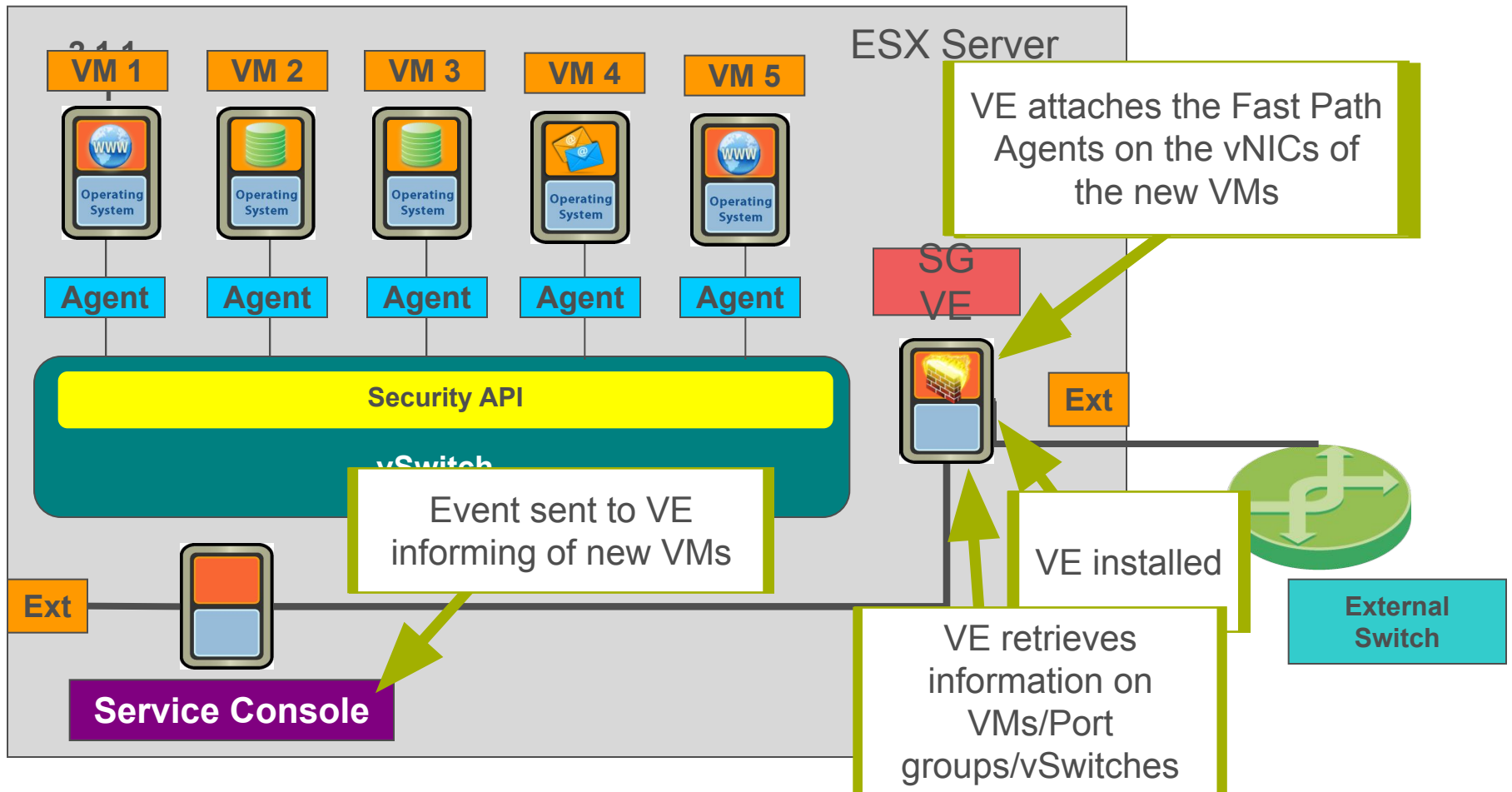
Standard Open
Virtualization Format
(OVF) virtual
appliance

Автоматически – Не требуется изменений сетевых настроек



- ▶ Защита всех виртуальных машин на сервере ESX
- ▶ Ко всем виртуальным сетевым картам подключается fast path agent
- ▶ Создается новый vSwitch с именем `_cp_private_vswitch`
- ▶ Создается новая группа портов с именем `_cp_private`
- ▶ Security Gateway VE подключается к группе портов `cp_private`

Встроенная защита для динамических сред

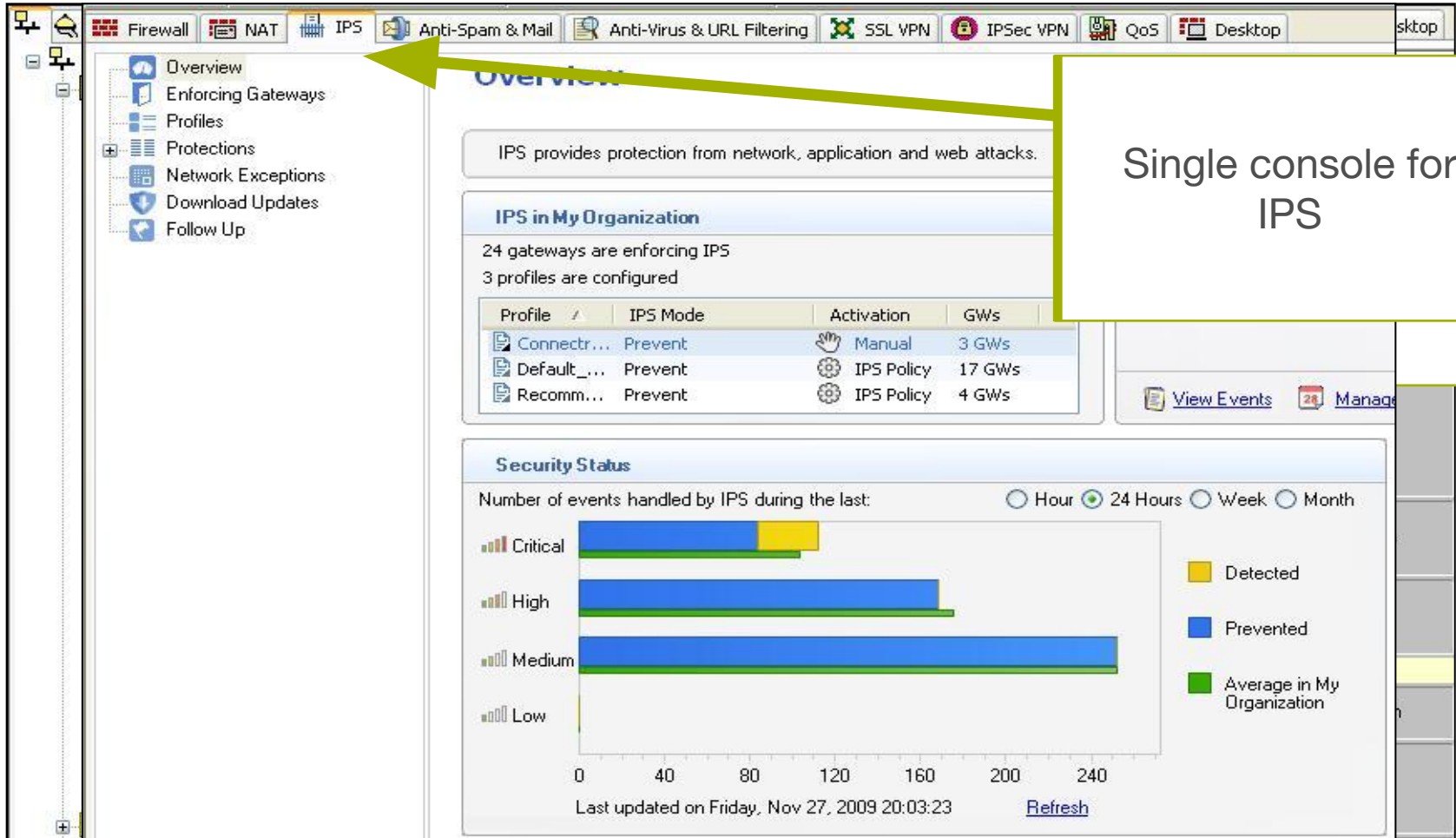


Опции настройки Fast Path Agent



- ▶ **Bypass:** Пакеты проходят без проверки
- ▶ **Secure:** Пакеты отправляются на шлюз VE
- ▶ **Block:** Пакеты сбрасываются
- ▶ **Monitor-only:** Анализ и генерация событий по пакетам, без их блокировки

Унифицированное управление физическими и виртуальными средами



IPS provides protection from network, application and web attacks.

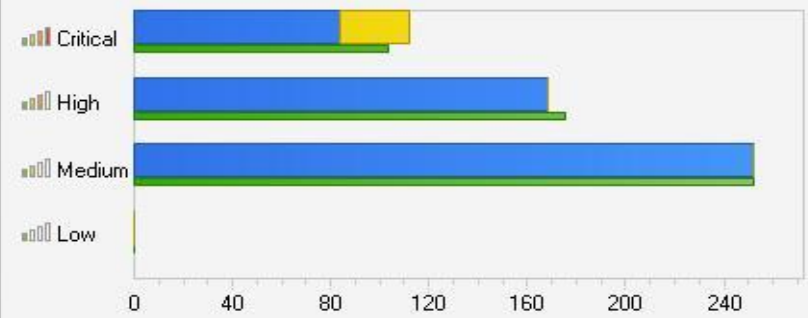
IPS in My Organization

24 gateways are enforcing IPS
3 profiles are configured

Profile	IPS Mode	Activation	GWs
Connectr...	Prevent	Manual	3 GWs
Default_...	Prevent	IPS Policy	17 GWs
Recomm...	Prevent	IPS Policy	4 GWs

Security Status

Number of events handled by IPS during the last: Hour 24 Hours Week Month



Legend:
■ Detected (yellow)
■ Prevented (blue)
■ Average in My Organization (green)

Last updated on Friday, Nov 27, 2009 20:03:23 [Refresh](#)

Внедрение событий ESX в Check Point

Фиксация и аудит событий виртуализации

Record Details

Previous Next Copy

VPN-1 Power/UTM

Product	VPN-1 Power/UTM
Date	24Nov2009
Time	19:31:28
Number	348011
Type	Log
Origin	Avatar

Source	...
Destination	...
Service	...
Protocol	...
Interface	...
Source Port	...

Policy Name	...
Policy Date	...
Policy Management	...

Action	...
Rule	...
Current Rule Number	...
Rule Name	...
User	...

Information

Event received from ESX: Message on RHEL5_2 on Inter in ha-datacenter: Do not forget to install the VMware Tools package inside this virtual machine; wait until your guest operating system finishes booting, then choose VM > Install VMware Tools and follow the instructions.










Abort Close

ESX logs integrated into Check Point management



Secure Gateway Virtual Edition – Containers

 The following products are based on the Software Blades architecture

Security Gateway VE Container	Specifications	Container Price
SGVE4801   	For Security Gateway VE on a Virtual System with up to 48 cores	\$6,000
SGVE1601   	For Security Gateway VE on a Virtual System with up to 16 cores	\$3,000
SGVE801   	For Security Gateway VE on a Virtual System with up to 8 cores	\$2,000

- The Firewall blade is included in the Security Gateway container price
- Additional software blades can added separately
- Gateways are licensed based on number of available physical cores.





Спасибо!

Сергей Голяк
RRC Россия | технический специалист
sgolyak@rrc.ru
Тел.: +7-495-956-1717 * 1129

