

# Аудит безопасности Security CheckUP Rxx.xx

## Для чего нужен аудит безопасности Security CheckUP?

По результатам аудита безопасности Security CheckUP вы поймете:

- 1) Насколько эффективны существующие средства защиты;
- 2) Какие угрозы информационной безопасности актуальны для вашей сети;
- 3) Какие приложения используют и какие сайты посещают ваши сотрудники;
- 4) На что тратится полоса пропускания канала связи в Интернет.

Самое главное, отчет по результатам Security CheckUP даст рекомендации по устранению существующих уязвимостей.

## Содержание документа:

[Как проходит Security Checkup ?](#)

[Требования к ресурсам](#)

[Образ ПО R81.10](#)

[1 Как развернуть образы в ESXI](#)

[2 Как развернуть образы в Hyper-V](#)

[3 Настройка виртуальной машины](#)

[4 Установка SmartConsole](#)

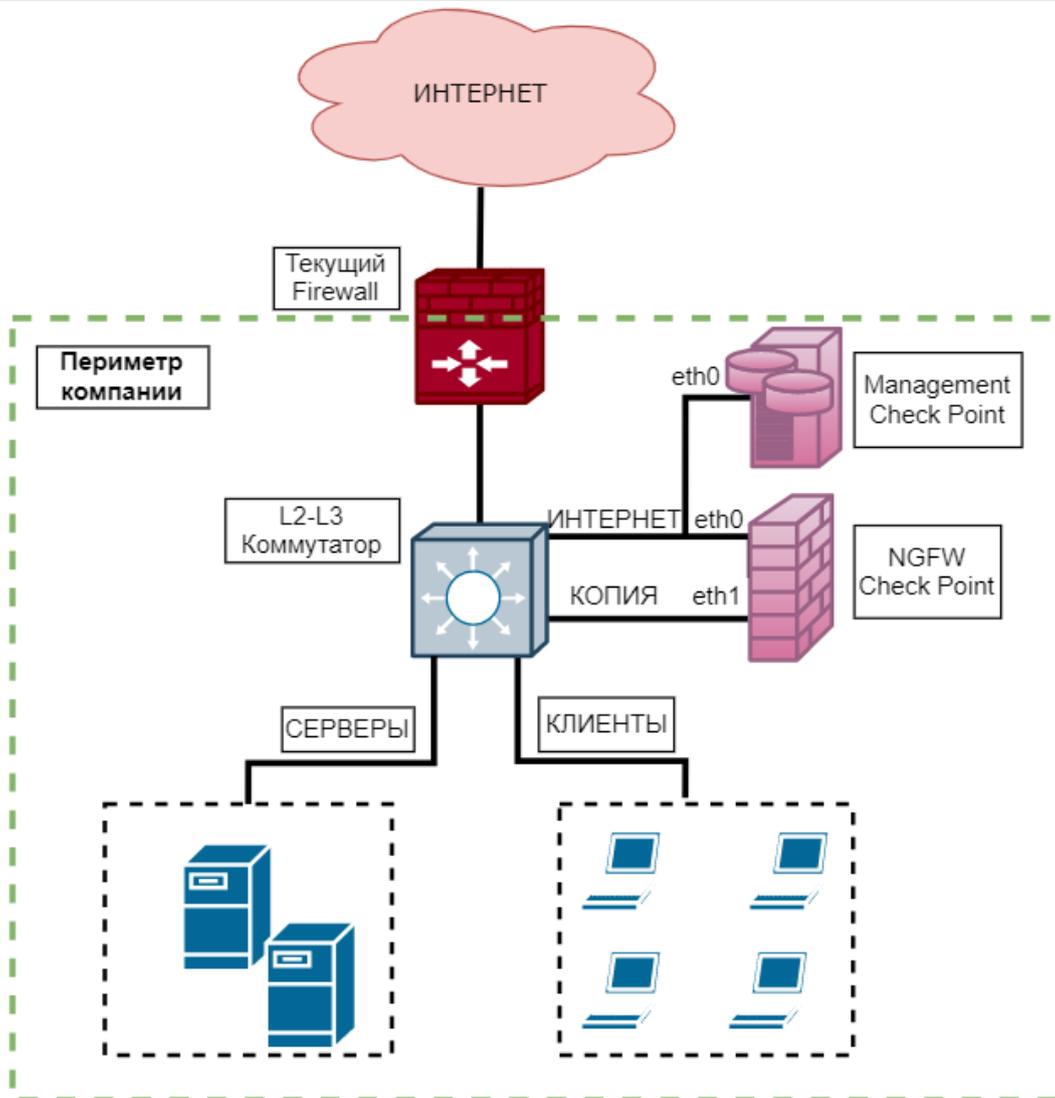
[5 Подключение шлюза к серверу управления](#)

[6 Самостоятельная настройка Security CheckUP](#)

[7 Как составить отчет?](#)

[8 Как получить отчет на русском языке?](#)

## Как проходит Security CheckUP?



В течение двух недель шлюз безопасности Check Point (SG) будет анализировать трафик в вашей сети. Security CheckUP выполняется на копии трафика, чтобы исключить влияние шлюза безопасности на сеть. Для этого на пограничном коммутаторе настраивается зеркалирование Интернет трафика в сторону SG. Система управления (SMS) хранит и обрабатывает логи SG, коррелирует события безопасности, составляет отчеты.

В данном документе SG и SMS - программные комплексы (ПК) версия ПО **R81.10**, виртуальные машины. Используется гипервизор VMware ESXi. Функциональность ПК аналогична функциональности ПАК.

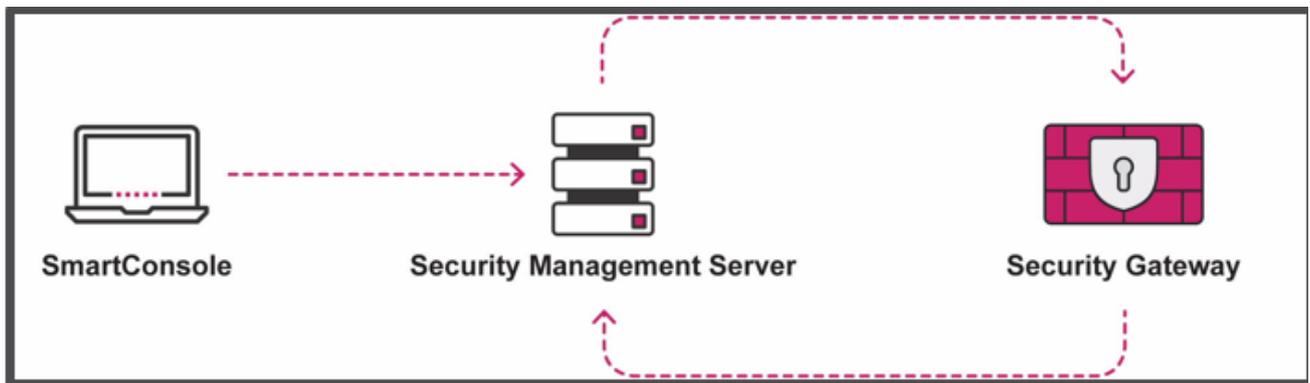
На виртуальной машине SG используется два порта: eth1 для приема зеркалированного трафика, eth0 для настройки и управления. На виртуальной машине SMS используется один порт eth0 для связи и управления шлюзом SG и для выхода в Интернет.

## Требования к ресурсам виртуальных машин

VM	CPU	RAM	HDD	Network
Security Gateway (SG)	4 Cores	4 GB	200 GB	eth0 – управление, доступ в Интернет eth1 – SPAN
Security Management Server (SMS)	4 Cores	не менее 10 GB	не менее 400 GB	eth0 – управление, доступ в Интернет

## Образ ПО R81.10

Для SG и SMS образ единый, доступ для скачивания по [ссылке](#).



# 1 Как развернуть образ на VMWare ESXi

## Создание виртуальной машины

При создании новой виртуальной машины обратите внимание на следующие пункты:

- 1) **Совместимость.** По умолчанию используйте совместимость с версией **ESXi 5.5 and Later**. Выберите другие настройки совместимости, если нужна поддержка определенной версии VMWare Workstation или VMWare Player:

New Virtual Machine

✓ 1 Select a creation type	Select compatibility
✓ 2 Select a name and folder	Select compatibility for this virtual machine depending on the hosts in your environment
✓ 3 Select a compute resource	The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.
✓ 4 Select storage	
✓ 5 Select compatibility	Compatible with: <input type="text" value="ESXi 5.5 and later"/> ⓘ
6 Select a guest OS	This virtual machine uses hardware version 10, which is compatible with ESXi 5.5 and later. Some virtual machine hardware features are unavailable with this option.
7 Customize hardware	
8 Ready to complete	

- 2) **Гостевая операционная система.** В качестве гостевой операционной системы выберите **Linux Red Hat Enterprise Linux 7 (64-bit)**:

New Virtual Machine

✓ 1 Select a creation type	Select a guest OS
✓ 2 Select a name and folder	Choose the guest OS that will be installed on the virtual machine
✓ 3 Select a compute resource	Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.
✓ 4 Select storage	
✓ 5 Select compatibility	
✓ 6 Select a guest OS	Guest OS Family: <input type="text" value="Linux"/>
7 Customize hardware	Guest OS Version: <input type="text" value="Red Hat Enterprise Linux 7 (64-bit)"/>
8 Ready to complete	

Compatibility: ESXi 5.5 and later (VM version 10)

- 3) **Тип HDD.** Disk Provisioning установите в **Thin Provision** или **Thick** (в зависимости от вашей политики использования ресурсов):

New Virtual Machine

1 Select a creation type	Memory Hot Plug	<input type="checkbox"/> Enable
2 Select a name and folder	New Hard disk *	
3 Select a compute resource	400	GB
4 Select storage	Maximum Size	4.25 TB
5 Select compatibility	VM storage policy	
6 Select a guest OS	Location	Store with the virtual machine
7 Customize hardware	Disk Provisioning	Thin Provision
8 Ready to complete	Sharing	Unspecified
	Shares	Normal 1000
	Limit - IOPs	Unlimited

4) **SCSI контроллер.** Тип контроллера установите в **LSI Logic Parallel** или **LSI Logic SAS**:

New Virtual Machine

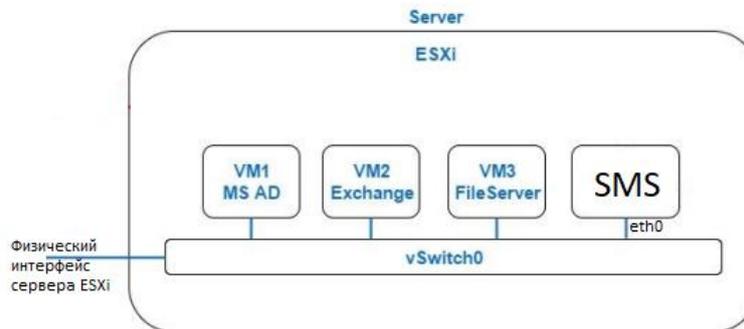
1 Select a creation type	Disk Mode	Dependent
2 Select a name and folder	Virtual Device Node	New SCSI controller
3 Select a compute resource		SCSI(0:0) New Hard disk
4 Select storage	New SCSI controller *	
5 Select compatibility	Change Type	LSI Logic Parallel
6 Select a guest OS	SCSI Bus Sharing	None
7 Customize hardware	New Network *	Test Virtual Server: <input checked="" type="checkbox"/> Connect...
8 Ready to complete	New CD/DVD Drive *	Client Device <input type="checkbox"/> Connect...
	Video card *	Specify custom settings
	VMCI device	

5) **Сетевой адаптер.** Тип сетевого адаптера установите в **VMXNET 3**. Убедитесь, что установлен чекбокс **Connect At Power On**:

New Virtual Machine

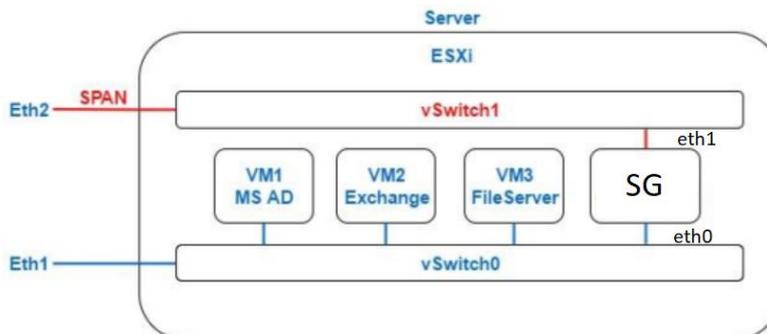
1 Select a creation type	SCSI Bus Sharing	None
2 Select a name and folder	New Network *	
3 Select a compute resource	Status	<input checked="" type="checkbox"/> Connect At Power On
4 Select storage	Adapter Type	VMXNET 3
5 Select compatibility	DirectPath I/O	<input checked="" type="checkbox"/> Enable
6 Select a guest OS	Shares	Normal 50
7 Customize hardware	Reservation	0 Mbit/s
8 Ready to complete	Limit	Unlimited Mbit/s
	MAC Address	Automatic
	New CD/DVD Drive *	Client Device <input type="checkbox"/> Connect...

## Настройка vSwitch для SMS



Интерфейс eth0 устройства SMS определяется в существующий виртуальный коммутатор (в нашем случае это vSwitch0). Подключение служит для управления и для выхода SMS в Интернет для скачивания обновлений.

## Настройка vSwitch для SG



Интерфейс eth0 устройства SG определяется в существующий виртуальный коммутатор (в нашем случае это vSwitch0). Подключение служит для управления.

Для интерфейса eth1 устройства SG создайте новый виртуальный коммутатор vSwitch1, который будет привязан к свободному Ethernet адаптеру сервера ESXi (на рисунке Eth2). На интерфейс Eth2 сервера ESXi направлен зеркалированный трафик.

**При создании vSwitch1 в свойствах виртуального коммутатора разрешите Promiscuous mode для поддержки зеркалированного трафика.**

## 2 Как развернуть образ на Microsoft Hyper-V

### Создание виртуальной машины

При создании виртуальной машины выберите тип виртуальной машины версии 1.

### Настройка vSwitch для SG

По умолчанию Hyper-V позволяет настраивать зеркалирование трафика между виртуальными машинами, которые находятся на одном и том же сервере. При этом, нельзя настроить зеркалирование трафика реального внешнего интерфейса сервера на виртуальный интерфейс:

1. **Создайте vSwitch.** Для vSwitch задайте имя (например vSwitch\_Span), в поле Connection Type выберите **External Network** и добавьте опцию **Allow management operating system to share this network adapter option**. Также укажите физический порт сервера, на который будет направлен зеркалированный трафик;
2. **Добавьте vSwitch в виртуальную машину.** В расширенных настройках адаптера (Advanced Features) в секции Port Mirroring настройте Mirroring mode, указав в поле **Destination**;
3. **Включите Microsoft NIDS.** Откройте Virtual Switch Manager для vSwitch\_Span, перейдите в Extensions. Включите Microsoft NIDS;
4. **Включите Mirroring на внешнем интерфейсе.** Выполните команды:

```
$ExtPortFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName «Ethernet Switch Port Security Settings»
$ExtPortFeature.SettingData.MonitorMode=2
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName vSwitch_Span -VMSwitchExtensionFeature $ExtPortFeature
```

### Команды для Microsoft Windows Server 2012 R2:

```
$ExtPortFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName 'Ethernet Switch Port Security Settings'
$ExtPortFeature.SettingData.MonitorMode=2
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName
<имя_виртуального_коммутатора> -VMSwitchExtensionFeature $ExtPortFeature
```

Статус настройки можно проверить с помощью команды:

```
Get-VMSwitchExtensionPortFeature -FeatureName «Ethernet Switch Port Security Settings» -SwitchName vSwitch_Span -ExternalPort | select -ExpandProperty SettingData
```

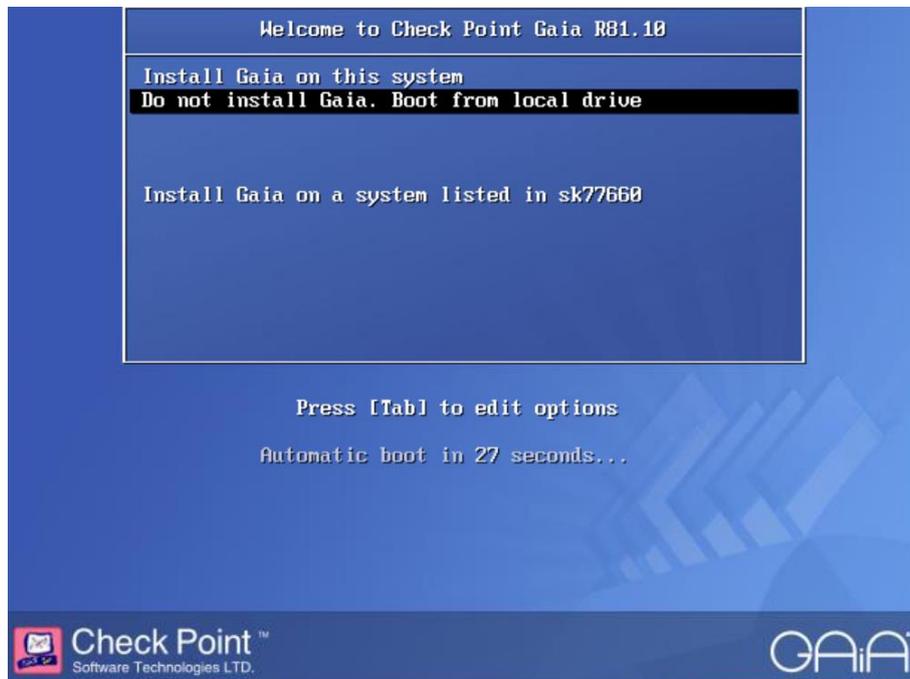
Вывести статус:

```
Get-VMSwitchExtensionPortFeature -FeatureName 'Ethernet Switch Port Security Settings' -SwitchName <имя_виртуального_коммутатора> -ExternalPort | select -ExpandProperty SettingData
```

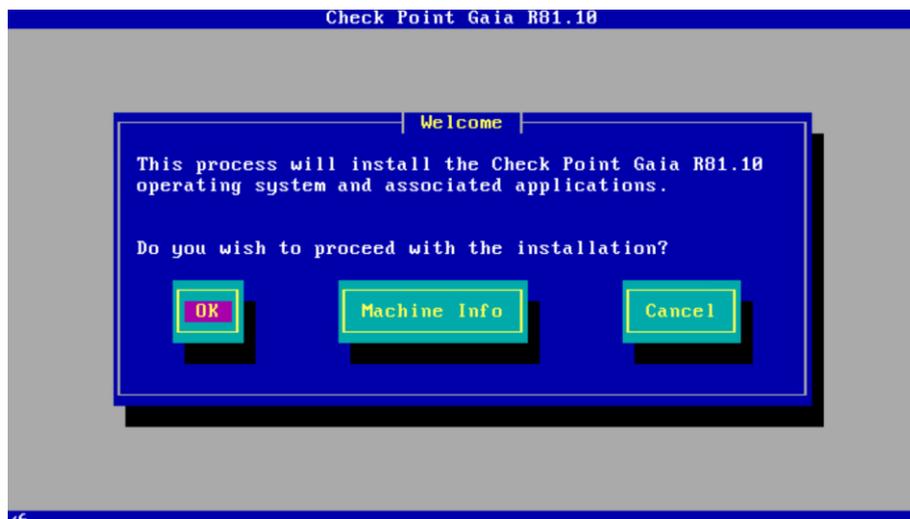
### 3 Настройка виртуальной машины

#### Установка операционной системы

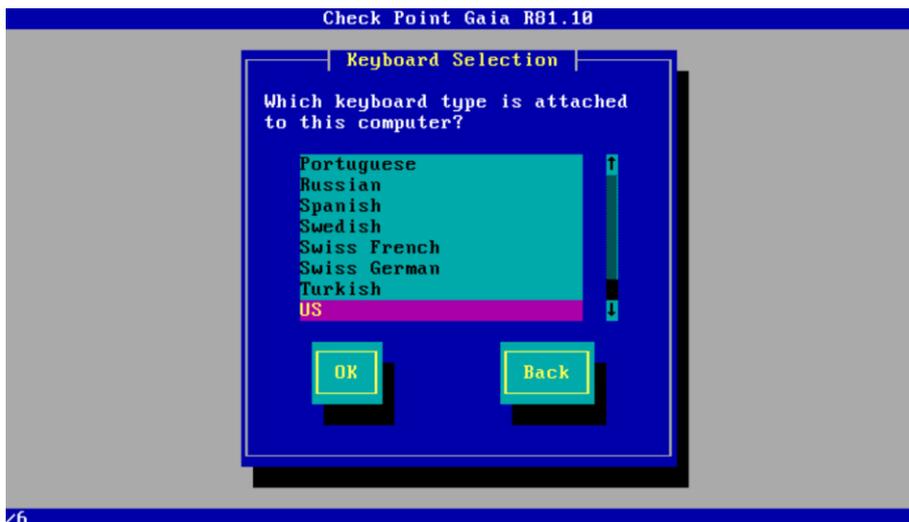
1. Запустите виртуальную машину. Выберите **Install Gaia on this system**:



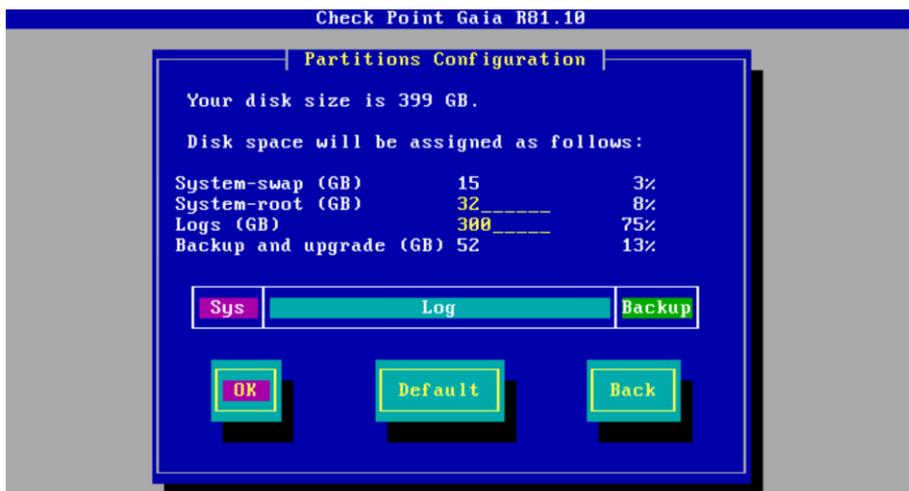
2. В окне Welcome нажмите **OK**:



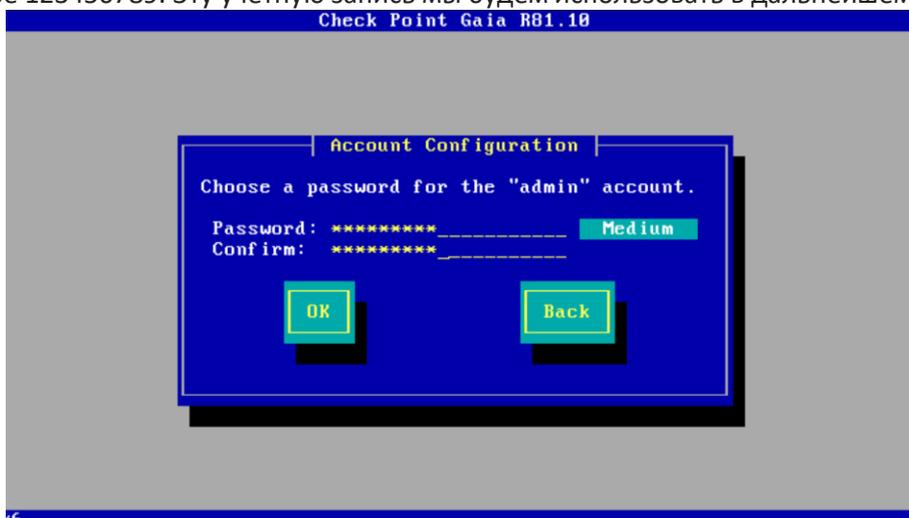
3. В окне Keyboard selection выберите **US** и нажмите **OK**:



4. В окне Partitions Configuration задайте разметку жесткого диска. Для **System-root** выделите не менее **30GB**, большую часть памяти выделите для Logs, для Security CheckUP бекапы не нужны, поэтому Backup & Upgrade не требует большого количества памяти:

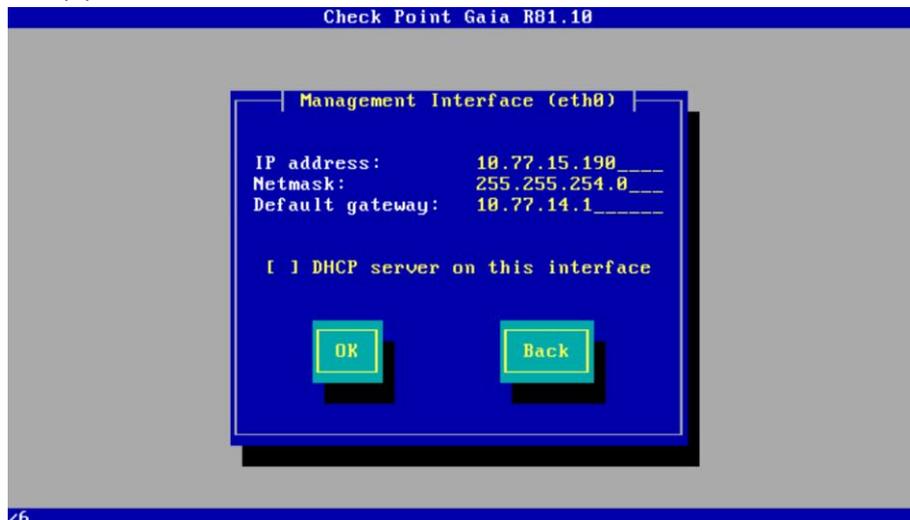


5. В окне Account configuration задайте пароль для внутреннего суперпользователя **admin**, в примере 123456789. Эту учетную запись мы будем использовать в дальнейшем. Нажмите **OK**:

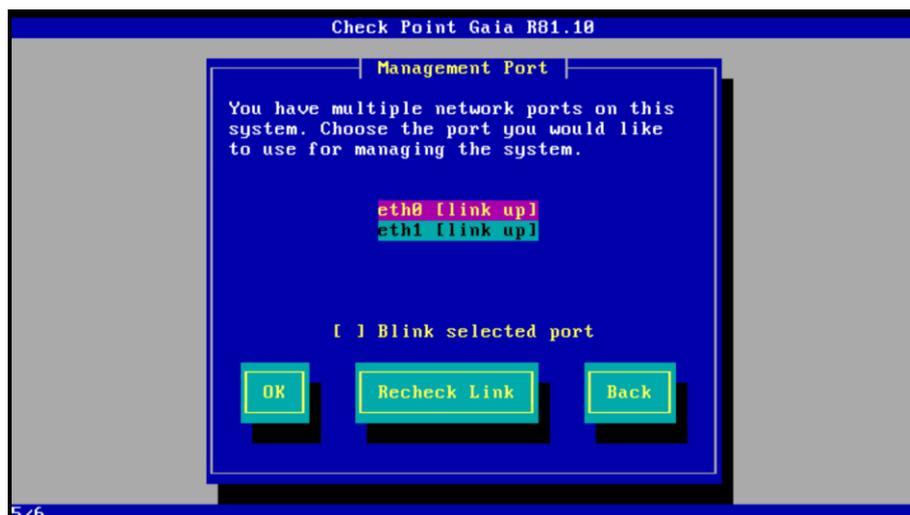


6. Настройте **интерфейс управления**:

- a. Для устройства **SMS**, задайте **IP адрес, маску сети** и шлюз по умолчанию на eth0 интерфейсе:



- b. для устройства **SG**, выберите интерфейс управления eth0, нажмите **OK**:

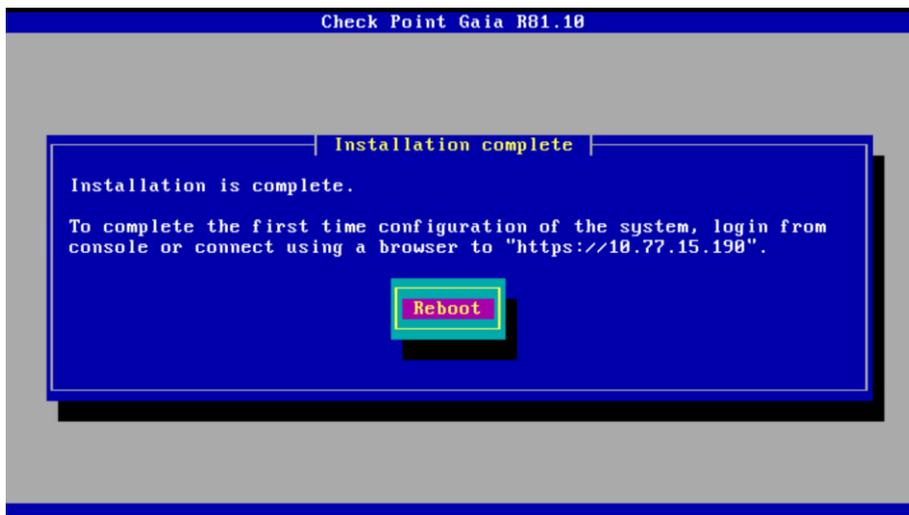


задайте **IP адрес, маску сети** и шлюз по умолчанию на eth0 интерфейсе, в примере IP адрес 10.77.15.191/23, default gw 10.77.14.1;

7. В окне Confirmation нажмите **OK**:



8. Дождитесь завершения установки и перезагрузите виртуальную машину:

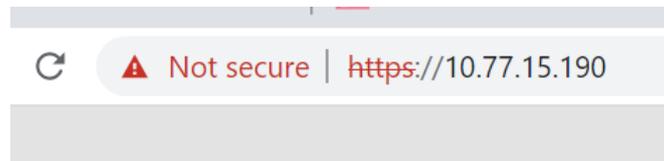


9. Дождитесь приглашения ввести логин и пароль. На этом этапе нужно выполнить **First Time Configuration Wizard**:

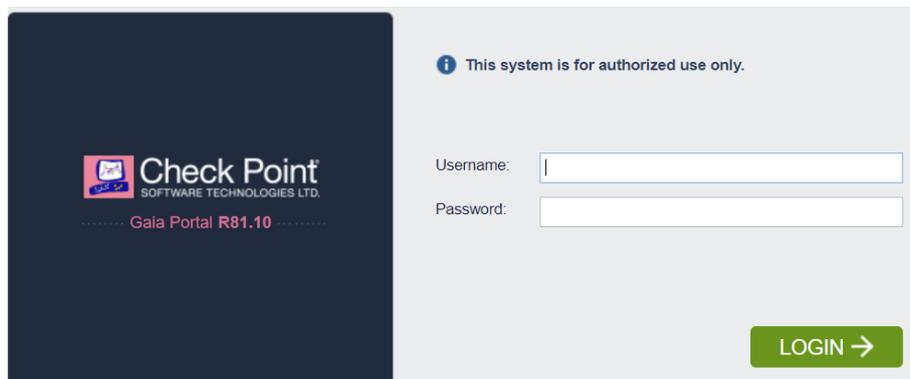


### First time configuration wizard

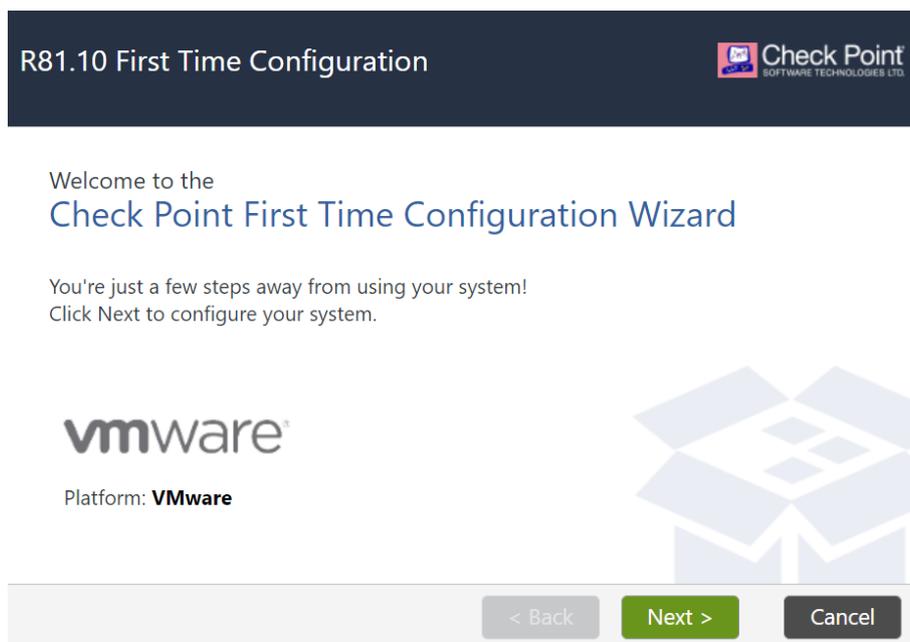
1. С помощью Web браузера (рекомендован Google Chrome, Edge и т.п.) подключитесь к Web интерфейсу управления ОС Gaia. Web Интерфейс доступен по **IP адресу интерфейса управления (прописать HTTPS)**:



2. Войдите в систему под учетной записью суперпользователя **admin** (в примере используется пароль 123456789):

A screenshot of the Check Point Gaia Portal R81.10 login page. On the left is a dark blue sidebar with the Check Point logo and "Gaia Portal R81.10". On the right, there is a light gray login form. At the top of the form is an information icon and the text "This system is for authorized use only." Below this are two input fields: "Username:" and "Password:". At the bottom right of the form is a green "LOGIN" button with a right-pointing arrow.

3. Нажмите **Next>**:

A screenshot of the "R81.10 First Time Configuration" wizard. The title bar at the top says "R81.10 First Time Configuration" and includes the Check Point logo. The main content area has a dark blue header with the text "Welcome to the Check Point First Time Configuration Wizard". Below this, it says "You're just a few steps away from using your system! Click Next to configure your system." The VMware logo is displayed on the left, with "Platform: VMware" underneath. On the right, there is a large, light blue graphic of an open box. At the bottom, there is a navigation bar with three buttons: "< Back" (disabled), "Next >" (active), and "Cancel" (disabled).

4. В окне Deployment options установите Continue with R81.10 configuration. Нажмите **Next>**:

## Deployment Options

**Setup** \_\_\_\_\_

Continue with R81.10 configuration

**Installation** \_\_\_\_\_

Install from Check Point cloud

Install from USB device

**Recovery** \_\_\_\_\_

Import existing snapshot ?

< Back
Next >
Cancel

5. В окне Management Connection при необходимости измените настройки интерфейса управления:

## Management Connection

Interface: eth0

Configure IPv4: Manually ▼

IPv4 address: 10 . 77 . 15 . 190

Subnet mask: 255 . 255 . 254 . 0

Default Gateway: 10 . 77 . 14 . 1

Configure IPv6: Off ▼

IPv6 Address:

Mask Length:

Default Gateway:

< Back
Next >
Cancel

6. В окне Device Information задайте **host name, domain name, адреса DNS серверов**. В примере задан Host Name для устройства SMS. Для SG задайте другой Host Name, в примере DM-SG1:

## Device Information



Host Name:

Domain Name:

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

### Proxy Settings

Use a Proxy server

Address:

Port:

< Back   Next >   Cancel

7. В окне Date and time settings установите правильное время, либо настройте адреса NTP серверов:

## Date and Time Settings



Set time manually:

Date:

Time:  :

Time Zone:

Use Network Time Protocol (NTP):

Primary NTP server:  Version:

Secondary NTP server:  Version:

Time Zone:

< Back   Next >   Cancel

8. В окне Installation Type выберите **Security Gateway and/or Security Management**:

## Installation Type



Security Gateway and/or Security Management  
 Multi-Domain Server

< Back   Next >   Cancel

## 9. В окне Products:

- а. Для SMS установите чекбокс в
- Security Management**
- :

## Products



**Products**

Security Gateway  
 Security Management

**Clustering**

Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

Automatically download and install Blade Contracts, new software, and other important data (highly recommended)  
For more information click [here](#)

< Back   Next >   Cancel

В окне Security Management Administrator настройки оставьте без изменений:

Security Management Administrator 

Use Gaia administrator: admin

Define a new administrator

Administrator Name:

New Password:

Confirm Password:

< Back

Next >

Cancel

В окне Security Management GUI Clients оставьте настройки без изменений:

Security Management GUI Clients 

GUI clients can log into the Security Management from:

Any IP Address

This machine

IP address:

Network

IP Address:

Subnet:

Range of IPv4 addresses:

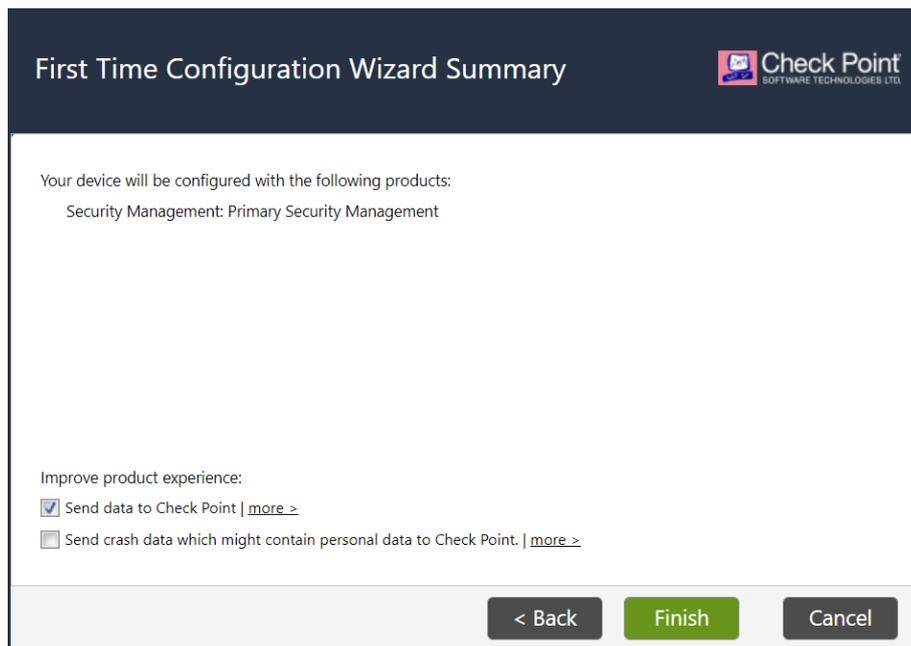
-

< Back

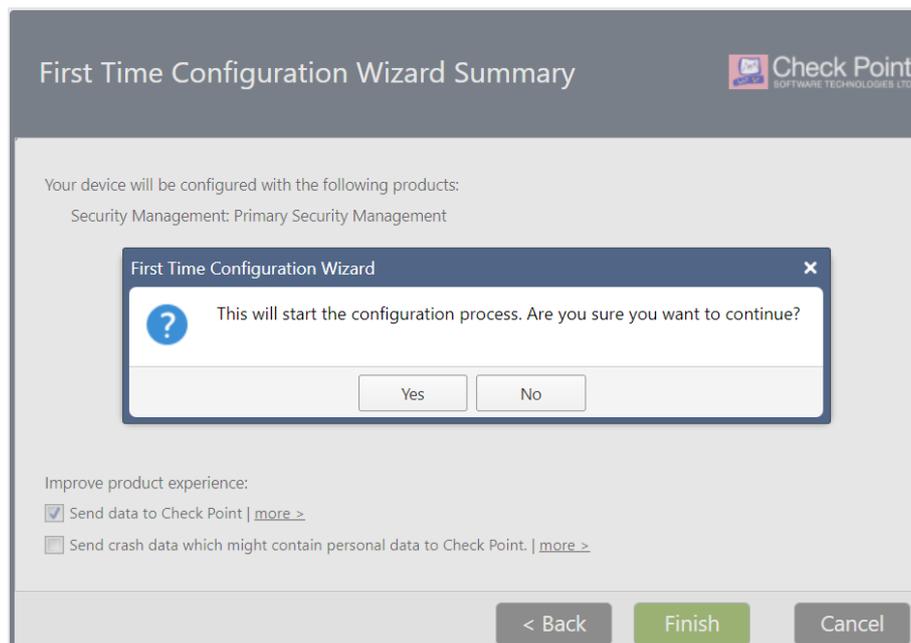
Next >

Cancel

В окне First time configuration wizard summary нажмите **Finish**:



Далее в окне подтверждения нажмите **Yes**:



b. Для SG установите чекбокс в **Security Gateway**:

## Products



Products

Security Gateway  
 Security Management

Clustering

Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

Automatically download and install Blade Contracts, new software, and other important data (highly recommended)  
[For more information click here](#)

< Back   Next >   Cancel

В окне Dynamically Assigned IP установите No. Нажмите Next>:

## Dynamically Assigned IP

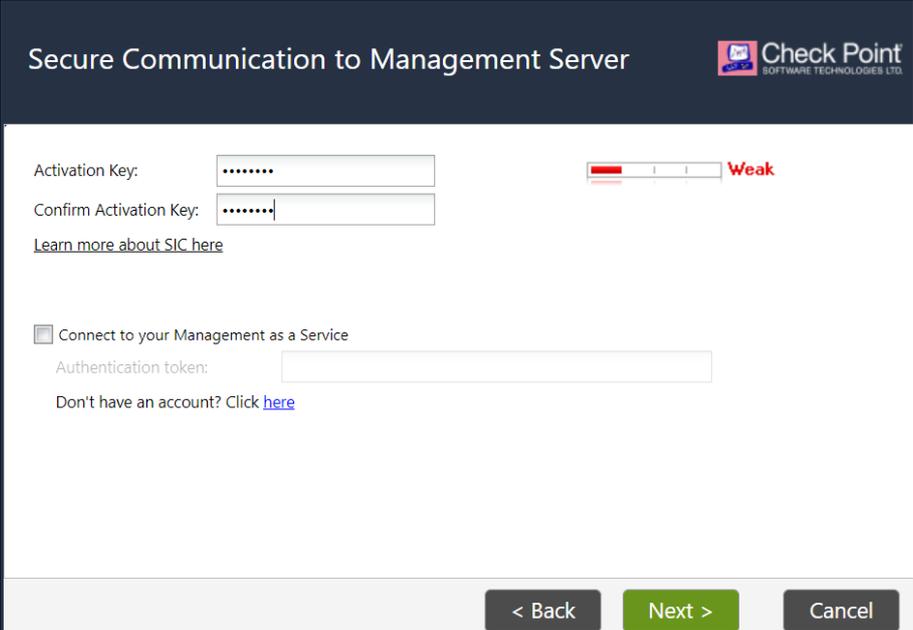


Does this gateway have a dynamically assigned IP address (DAIP gateway)?

Yes  
 No

< Back   Next >   Cancel

В окне Secure Communication to Management Server задайте пароль для первичного защищенного **SIC туннеля** до SMS, в примере 12345678:



Secure Communication to Management Server

Check Point  
SOFTWARE TECHNOLOGIES LTD.

Activation Key: [.....] Weak

Confirm Activation Key: [.....]

[Learn more about SIC here](#)

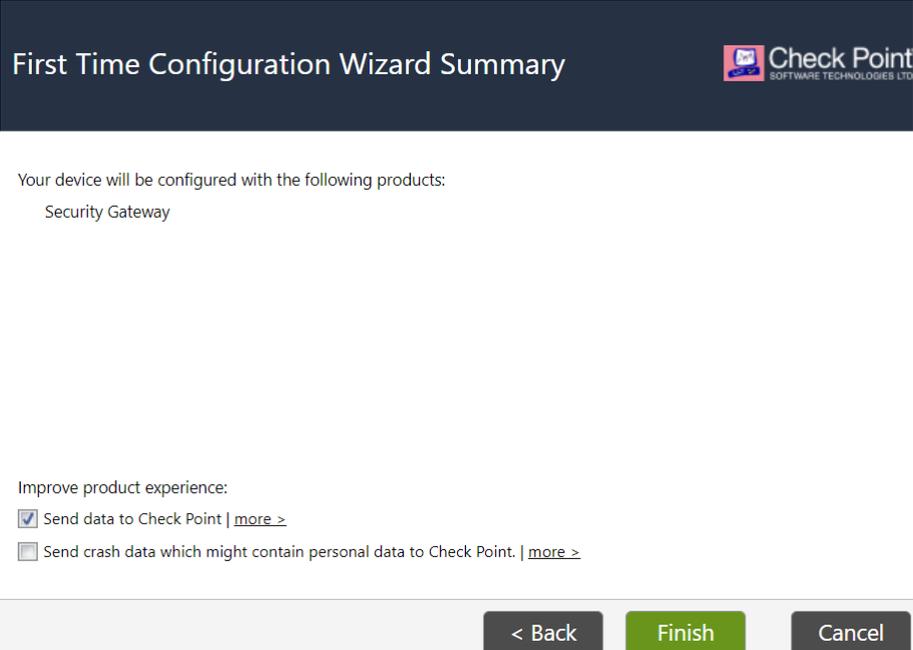
Connect to your Management as a Service

Authentication token: [ ]

Don't have an account? Click [here](#)

< Back Next > Cancel

В окне First Time Configuration Wizard Summary нажмите **Finish**:



First Time Configuration Wizard Summary

Check Point  
SOFTWARE TECHNOLOGIES LTD.

Your device will be configured with the following products:  
Security Gateway

Improve product experience:

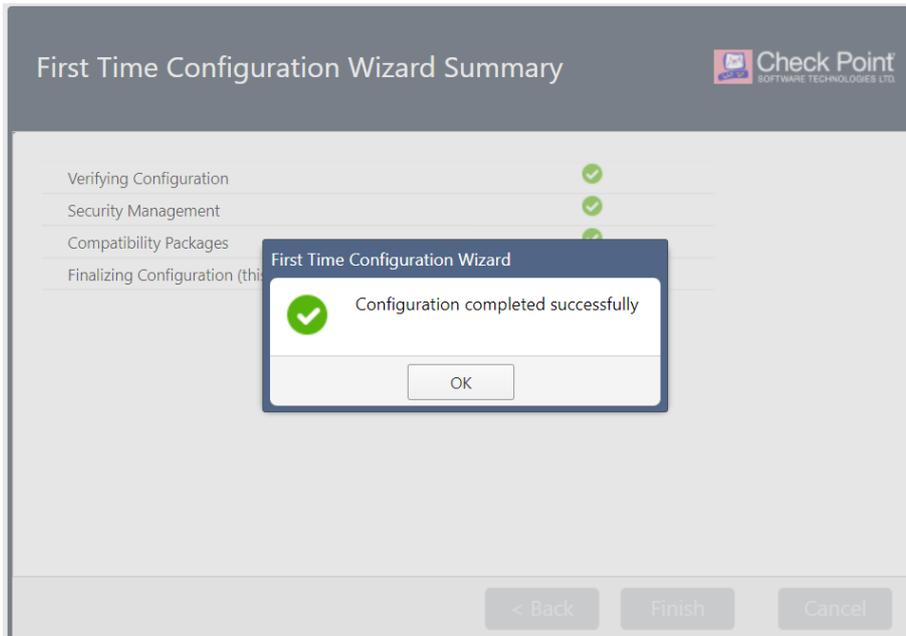
Send data to Check Point | [more >](#)

Send crash data which might contain personal data to Check Point. | [more >](#)

< Back Finish Cancel

Далее в окне подтверждения нажмите **Yes**.

10. Дождитесь завершения установки и нажмите ОК. Далее откроется Web интерфейс управления ОС Gaia:



## 4 Установка SmartConsole

Дальнейшая настройка и управление SG выполняется с помощью утилиты SmartConsole.

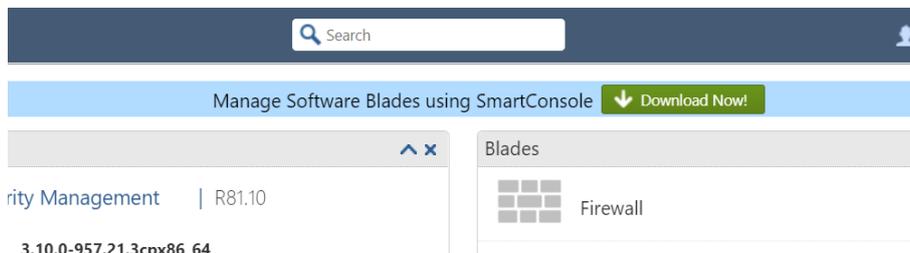
- Загрузить последнюю SmartConsole можно по [ссылке](#) дистрибутива:



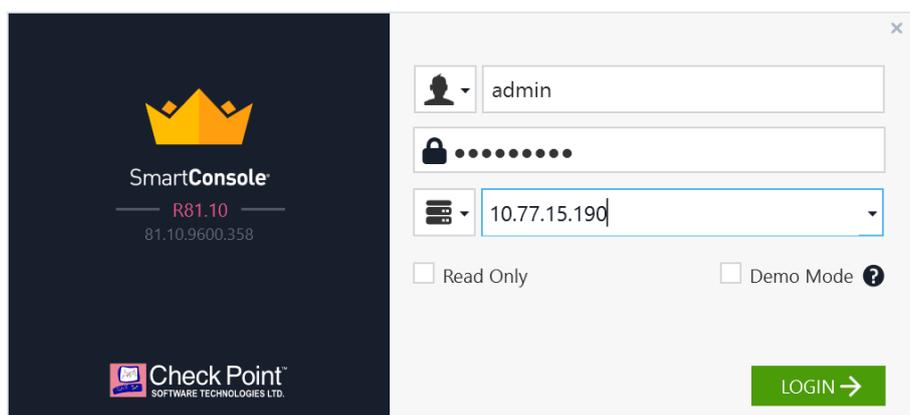
For Web SmartConsole, see [sk170314](#)

- Либо загрузить из установленного SMS (может потребоваться обновление).

1. Подключитесь к WEB интерфейсу SMS с помощью WEB браузера. Скачайте и установите SmartConsole на компьютер администратора:

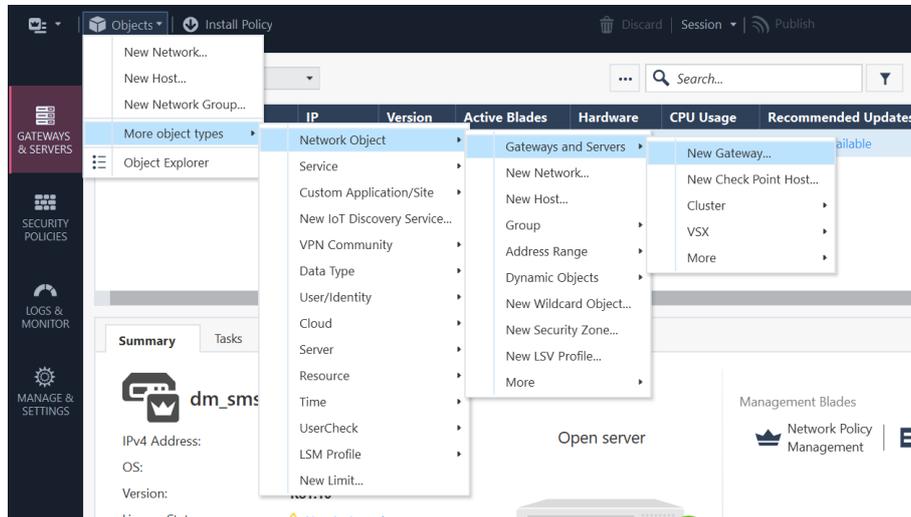


2. После установки залогиньтесь в SmartConsole с учетной записью суперпользователя **admin** (в примере пароль 123456789) устройства SMS, подключение по IP адресу SMS:

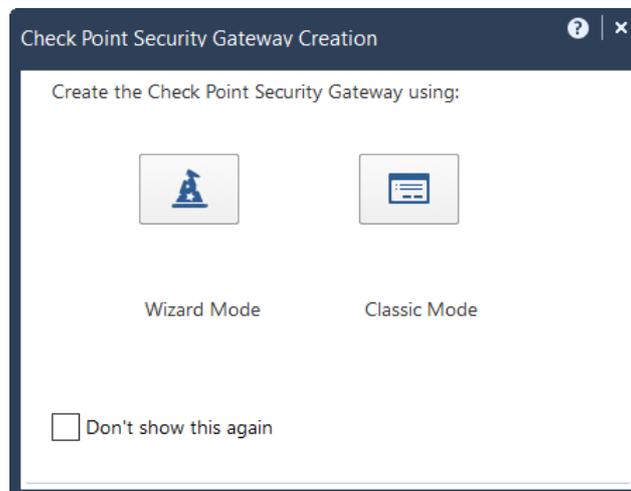


## 5 Подключение SG к SMS

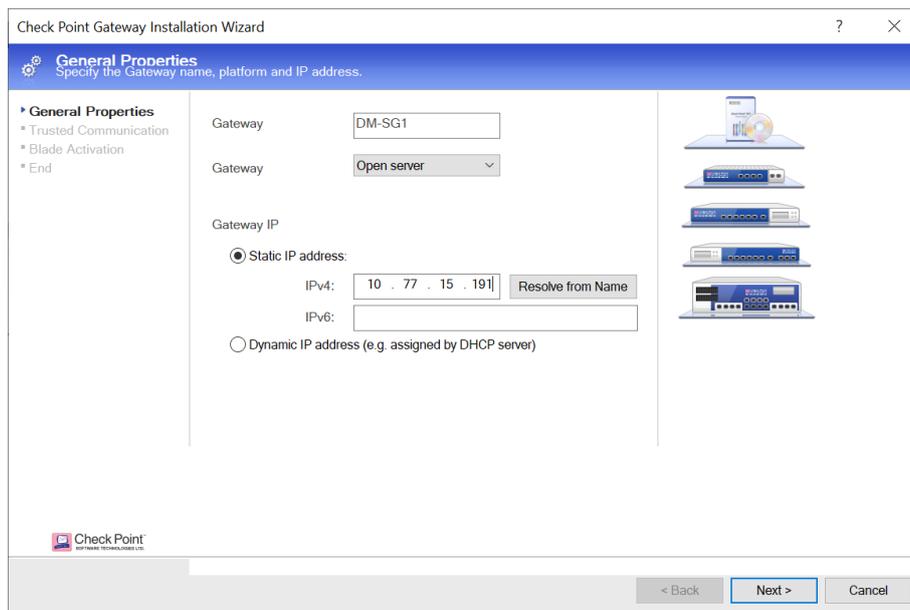
1. Подключитесь к SMS с помощью SmartConsole. Для того, чтобы подключить SG к SMS выполните **Objects - Network Object - Gateways and Servers - New Gateway...**:



2. В окне Check Point Security Gateway Creation выберите **Wizard Mode**:

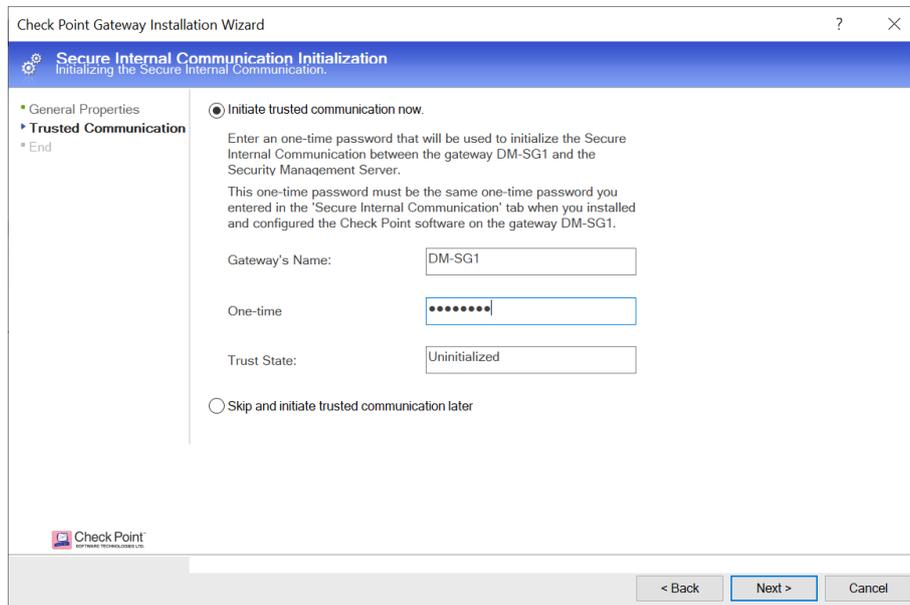


3. В окне General Properties задайте **Host name** устройства SG, который был задан в процессе First time configuration wizard (см. [п.6](#)), в выпадающем меню выберите **Open Server** и задайте IP адрес устройства SG (интерфейс управления eth0). Нажмите **Next>**:

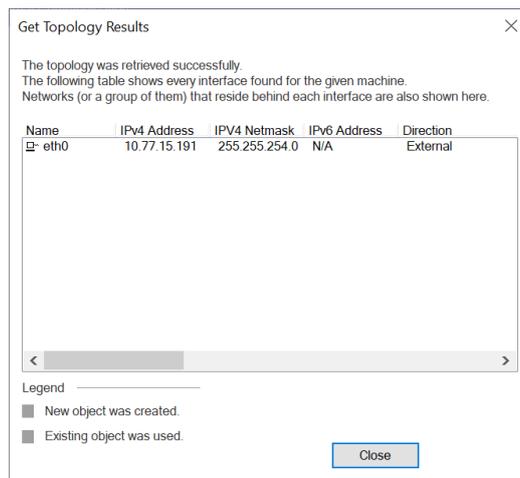


4. В окне Trusted Communication в поле One-time задайте пароль для установления защищенного SIC туннеля между SMS и SG, который был задан в процессе First time configuration wizard (см. [п.9b](#)). Нажмите **Next>**:

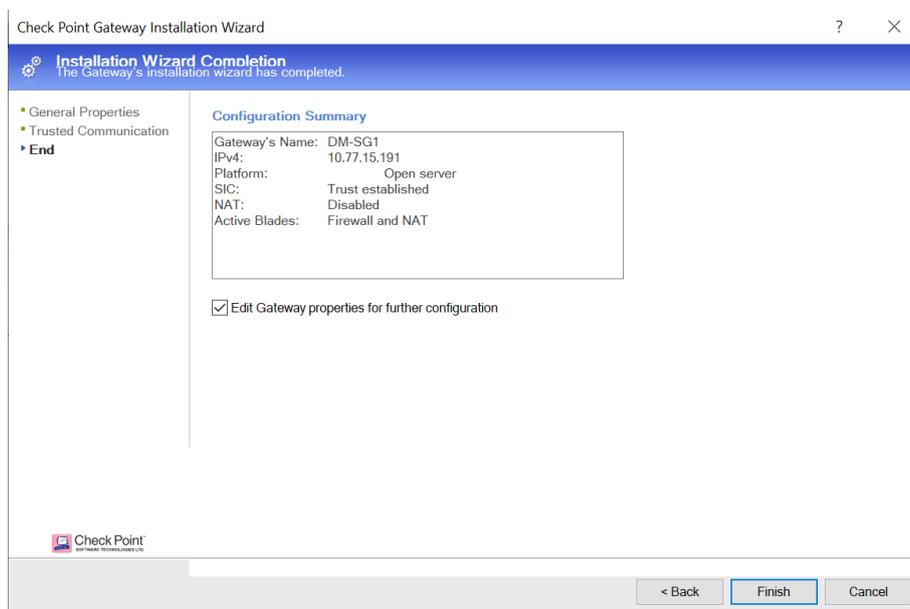
5.



6. В окне Get topology Results нажмите **Close**:



7. В окне End нажмите **Finish**:



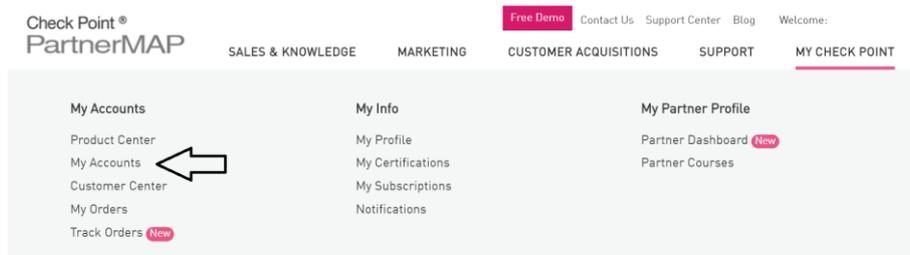
8. В окне Check Point Gateway нажмите **Cancel**.

Рекомендуем для дальнейшей настройки устройств SMS, SG подключить инженера интегратора или инженера Check Point.

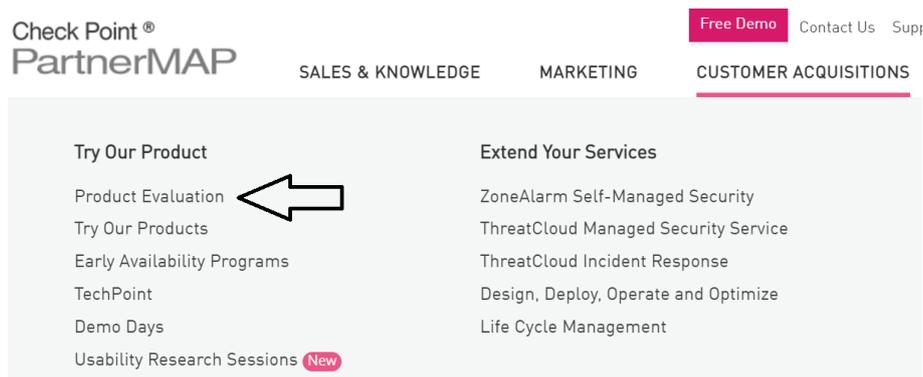
## 6 Самостоятельная настройка Security CheckUP

### Выпуск демо лицензий

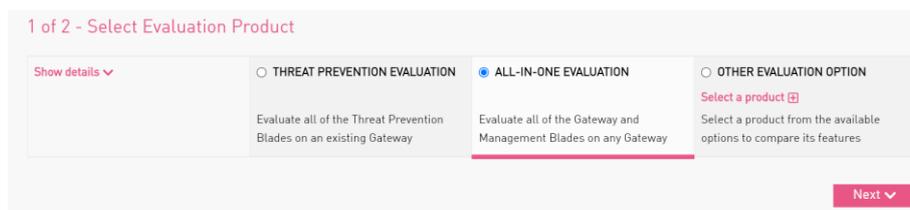
1. На портале <https://usercenter.checkpoint.com/usercenter/portal> (нужна короткая регистрация) перейдите **My Check Point - My accounts**. Убедитесь, что для вашей учетной записи создан аккаунт в User Center, если нет - создайте новый:



2. Далее перейдите **Customer Acquisitions - Product Evaluation**:



3. Далее выберите **All-in-one evaluation** и нажмите **Next>**:



4. Заполните поля **Provide Evaluation Info**. В поле IP address укажите **правильный IP адрес SMS**. Нажмите **Get Evaluation**:

5. Нажмите **Get license file**, чтобы скачать файл лицензии (CPlicenseFile.lic):

## NOTE:

- This is an evaluation license valid for 30 days.
- This certificate key is valid for 1 licenses.

[Back to Product Evaluation](#)[Get License File](#)

6. Перейдите **My Check Point - Product Center - Details**. И скачайте файл контрактов - **Get contracts** (ServiceContract.xml):

Product Center

Selected Accounts | Products | Blades | Services | Accessories | **Evaluations** | Support | Training

▲ Summary Export Evaluate Blades Product Evaluation

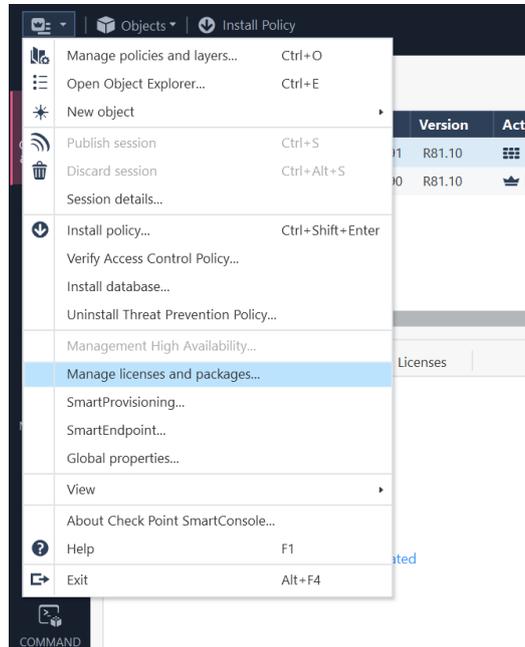
Issue Date ▲	Total	Not Licensed Yet	Valid	Expired
Last 1-6 Months	2	1	1	0
Last 7-12 Months	0	0	0	0
Previous Periods	0	0	0	0
<b>Total</b>	<b>2</b>	<b>1</b>	<b>1</b>	<b>0</b>

▲ Details License Move Edit Info Export License Instructions **Get Contracts**

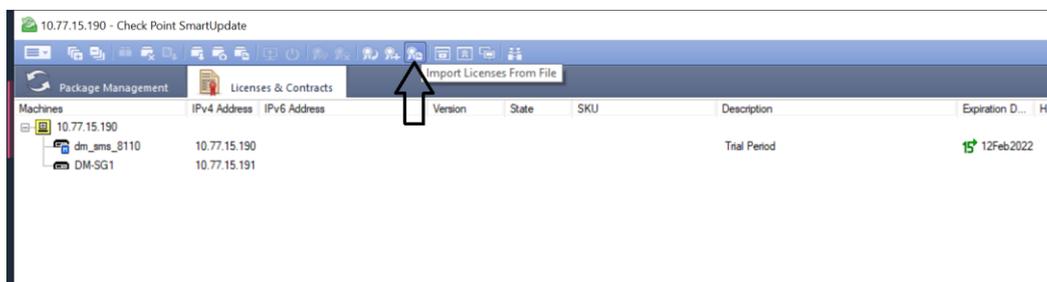


## Установка демо лицензий

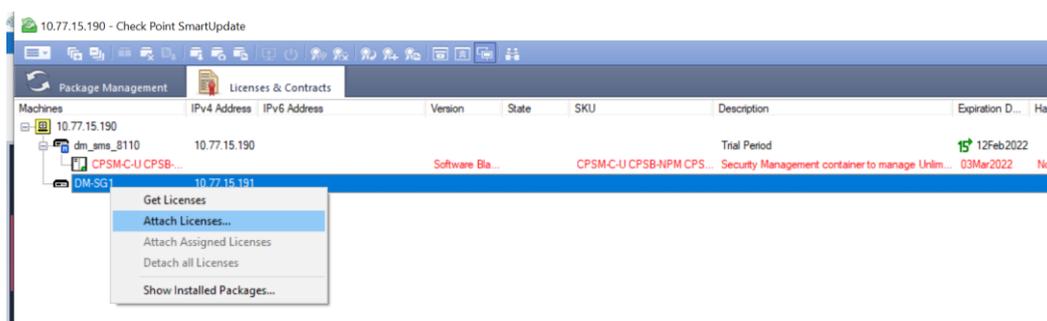
1. Для установки лицензий в главном окне SmartConsole выберите **Menu - Manage licenses and packages...** Откроется окно Check Point SmartUpdate:



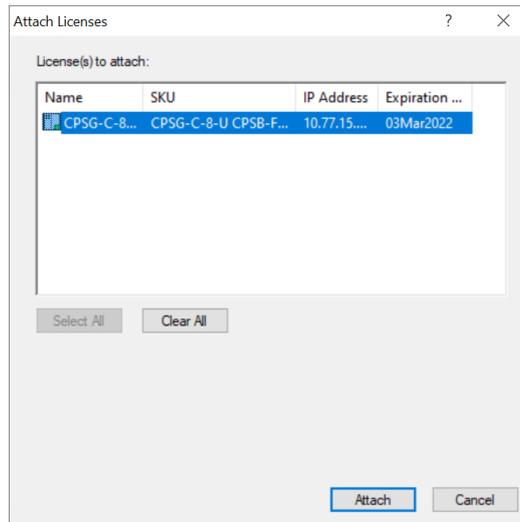
2. Перейдите во вкладку **Licenses and Contracts** и нажмите кнопку **Import Licenses From File**. Выберите скачанный файл **CPLicenseFile.lic** и нажмите **Open**. Обратите внимание, что лицензия CPSM (Security Management) устанавливается автоматически:



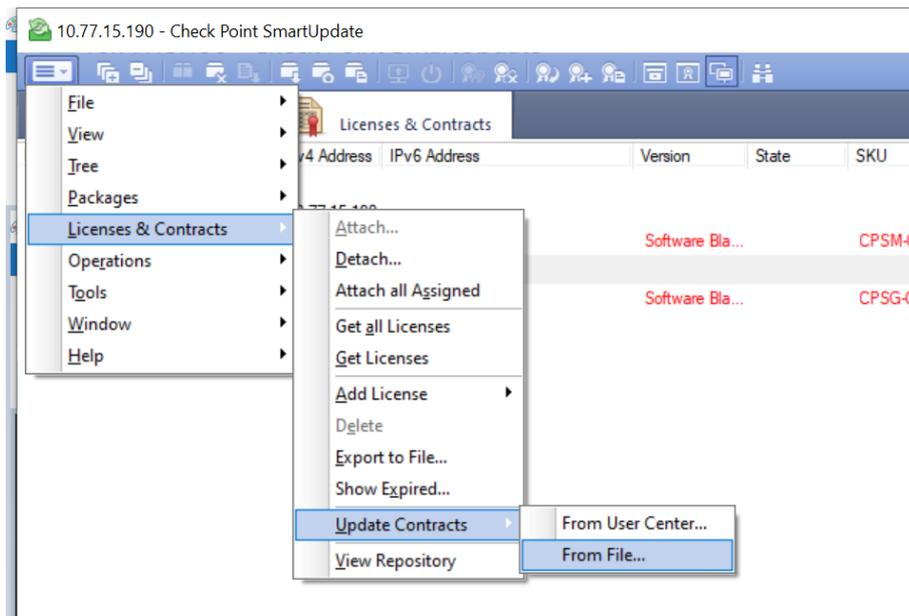
3. Установите лицензию CPSG на шлюз безопасности. Для этого нажмите правой кнопкой на шлюз безопасности и выберите **Attach Licenses...**:



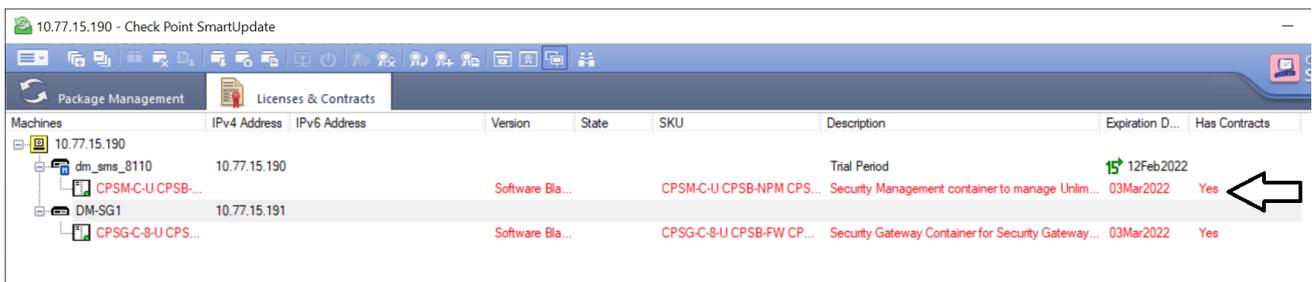
4. В окне Attach Licenses выберите лицензию CPSG и нажмите **Attach**:



- Далее обновите контракты. Для этого в окне Check Point SmartUpdate выберите **Menu - Licenses & Contracts - Update Contracts - From file...** Выберите скачанный файл **ServiceContract.xml** и нажмите **Open**:

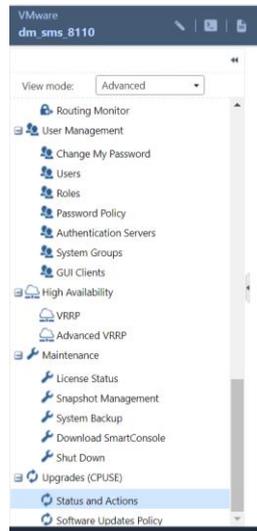


- Убедитесь, что контракты обновились:

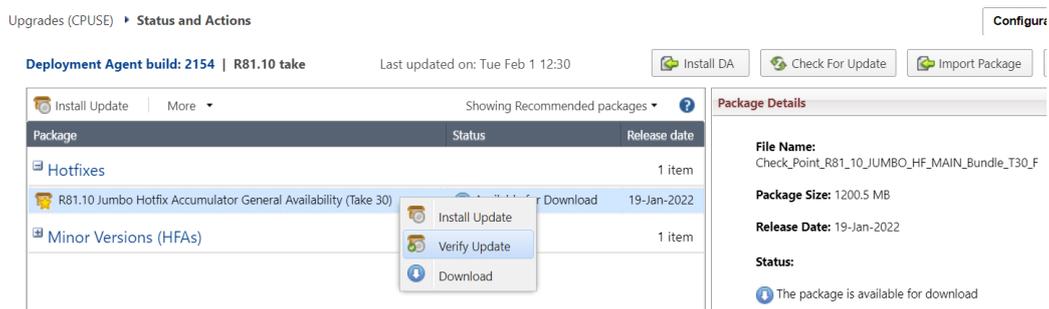


## Установка обновлений на SMS

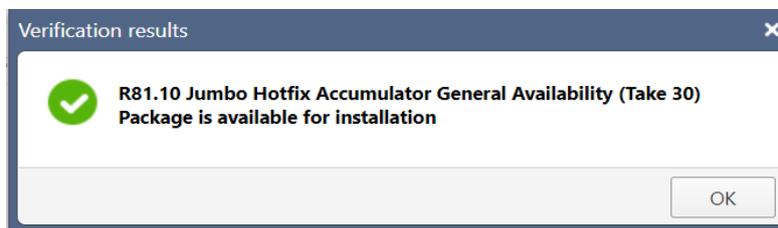
1. С помощью WEB браузера подключитесь к WEB Интерфейсу управление ОС GAIA;
2. Перейдите в меню **Upgrades (CPUSE) - Status and Actions**:



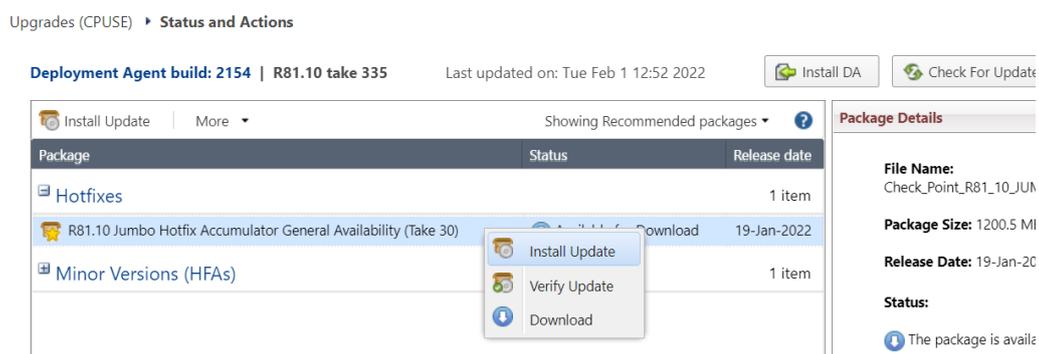
3. Проверьте наличие обновлений Hotfixes. Если обновление доступно, то нажмите на него правой кнопкой и выберите **Verify Update**:



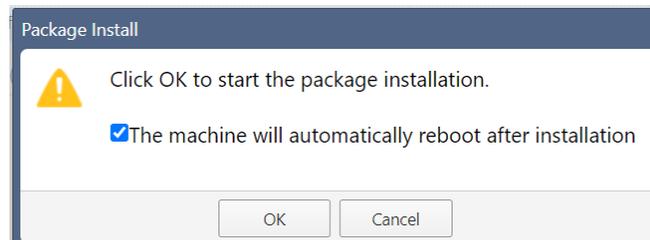
4. В окне Verification results нажмите **OK**:



5. Затем выполните **Install Update**:



6. После установки обновления SMS перезагрузится автоматически. Нажмите **OK**:

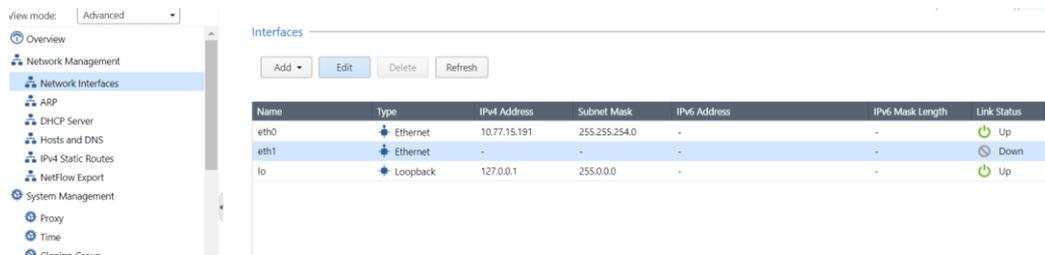


### ***Установка обновлений на SG***

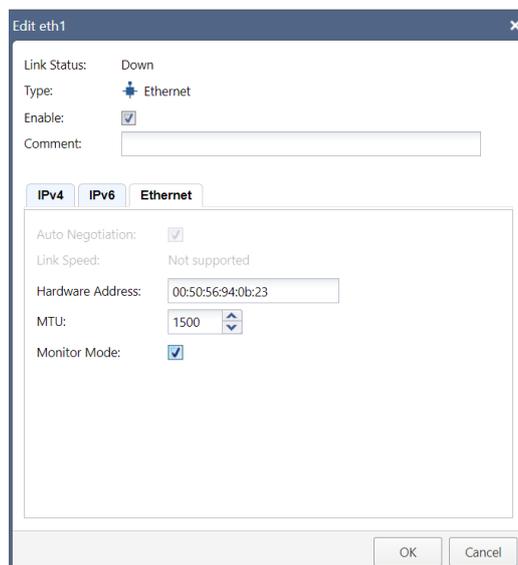
Выполняется аналогично установке обновлений на SMS.

## Настройка топологии

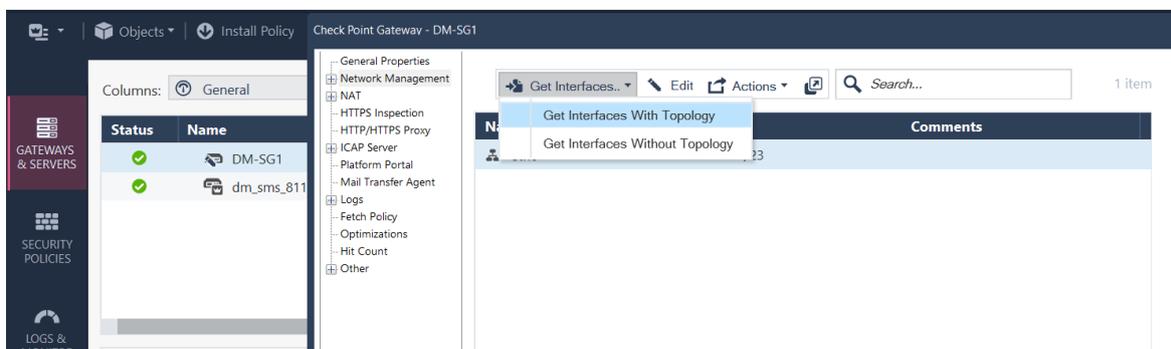
1. Подключитесь к WEB интерфейсу ОС GAIA устройства SG (в примере <https://10.77.15.191>);
2. Перейдите во вкладку **Network Management - Network Interfaces**. Выберите интерфейс eth1 и нажмите **Edit**:



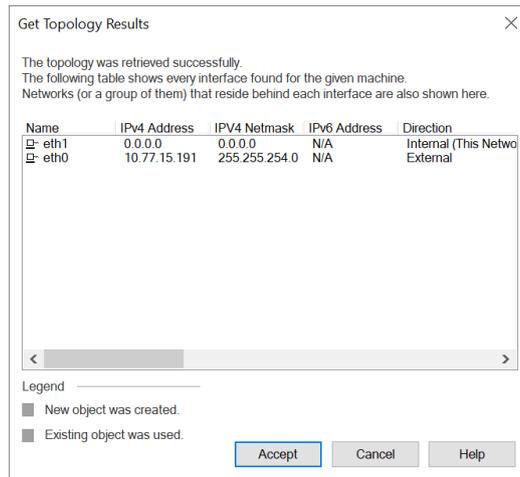
3. Установите чекбокс **Enable**, перейдите во вкладку Ethernet и установите чекбокс **Monitor Mode**. Нажмите **OK**:



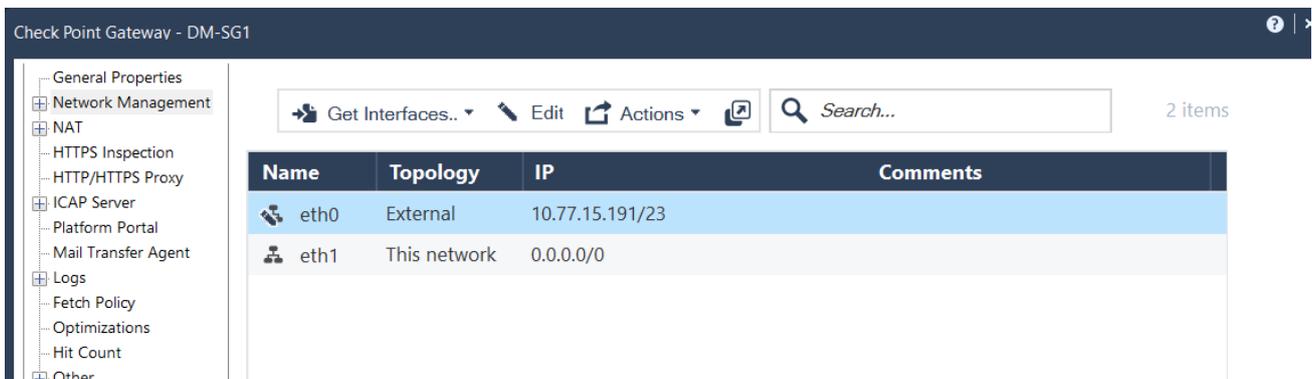
4. В SmartConsole перейдите во вкладку **Gateways and Servers**. Дважды нажмите на шлюз безопасности. Затем выберите **Network Management - Get Interfaces - Get interfaces With Topology**:



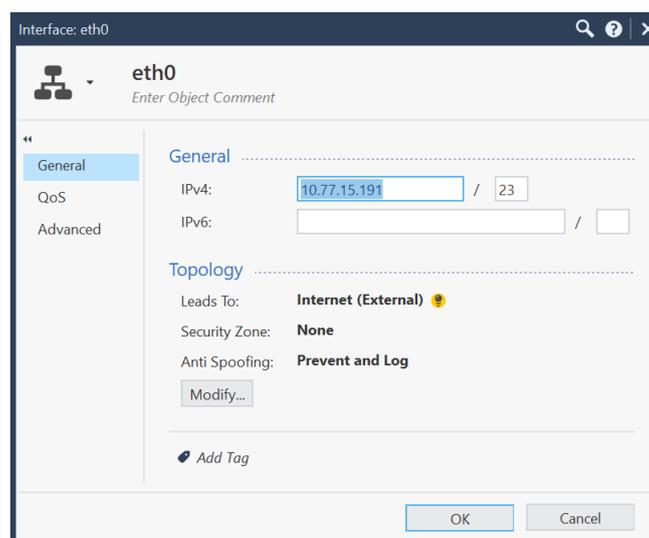
5. В окне Get Topology Results нажмите **Accept**:



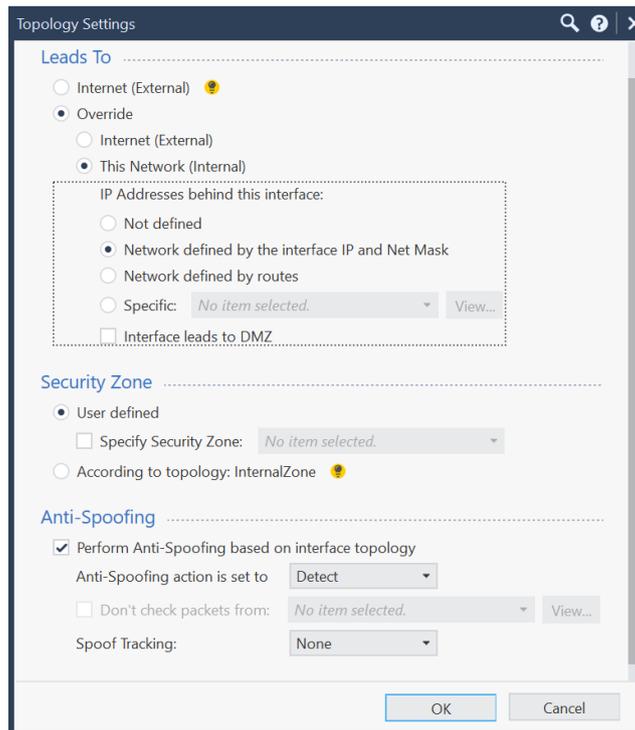
6. Интерфейс управления eth0 определите, как **Internal** интерфейс, настройки антиспуфинга переключите в **Detect**, отключите логирование. Для этого дважды нажмите на интерфейс eth0:



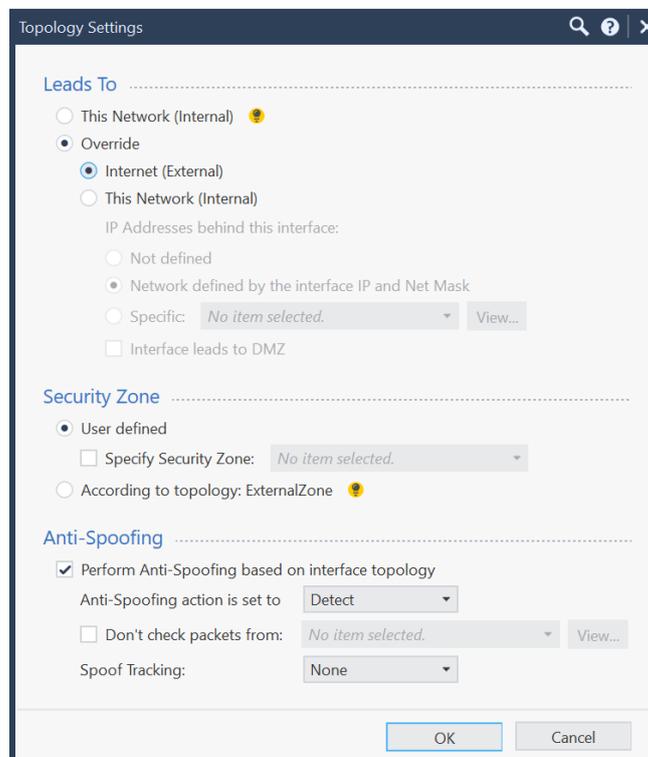
7. В поле Topology нажмите **Modify**:



8. Приведите настройки к следующему виду, дважды нажмите **OK**:

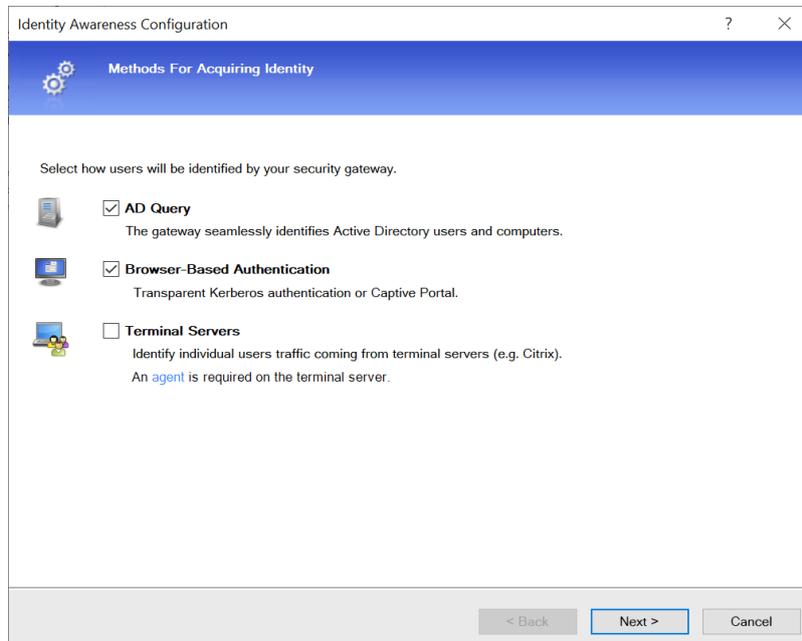


9. Интерфейс eth1 определите, как **External**, антиспуфинг установите в **Detect**, отключите логирование. Дважды нажмите **OK**:

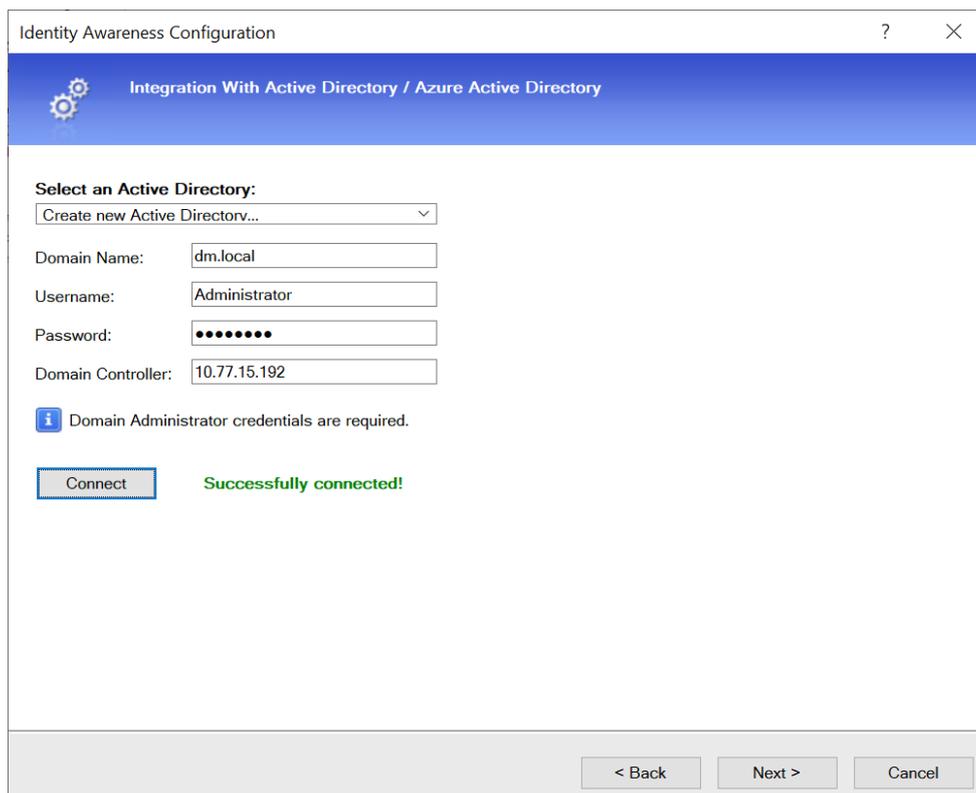


## Активация блейдов

1. Перейдите в меню General Properties. Во вкладке Network Security активируйте блейды Application Control, URL filtering, Content Awareness и Identity Awareness. Identity Awareness потребует дополнительной настройки:

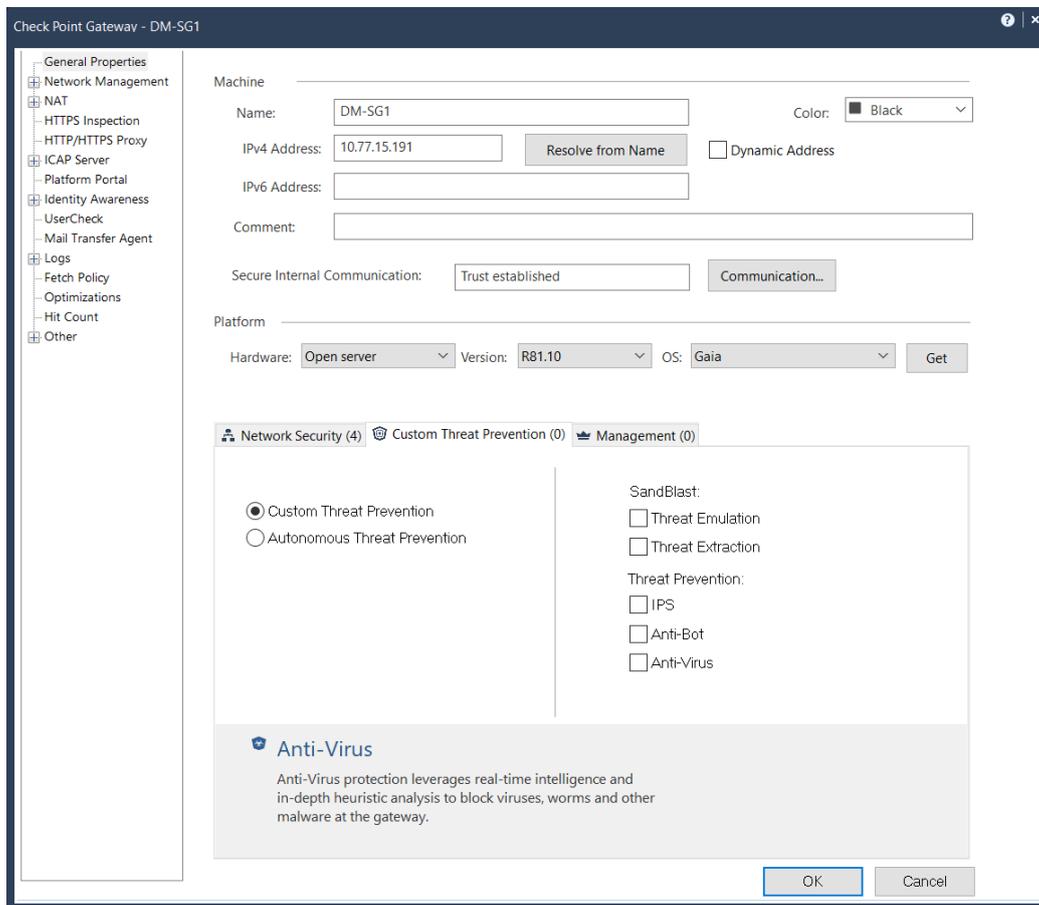


2. Нужно указать учетную запись Администратора сервера AD. Если корпоративная политика безопасности не допускает использование учетной записи администратора, то нужно создать пользователя с необходимыми правами доступа: [sk43874](#) и [sk93938](#):

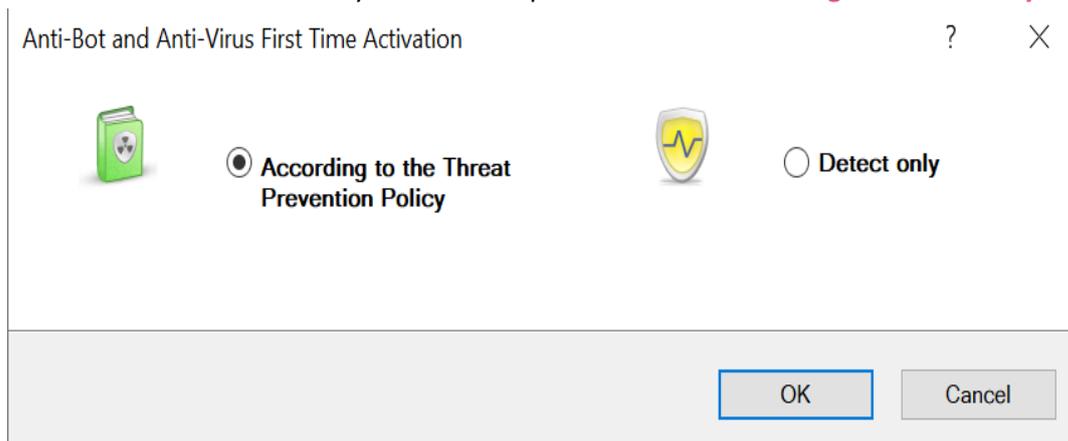


3. Завершите настройку блейда Identity Awareness;

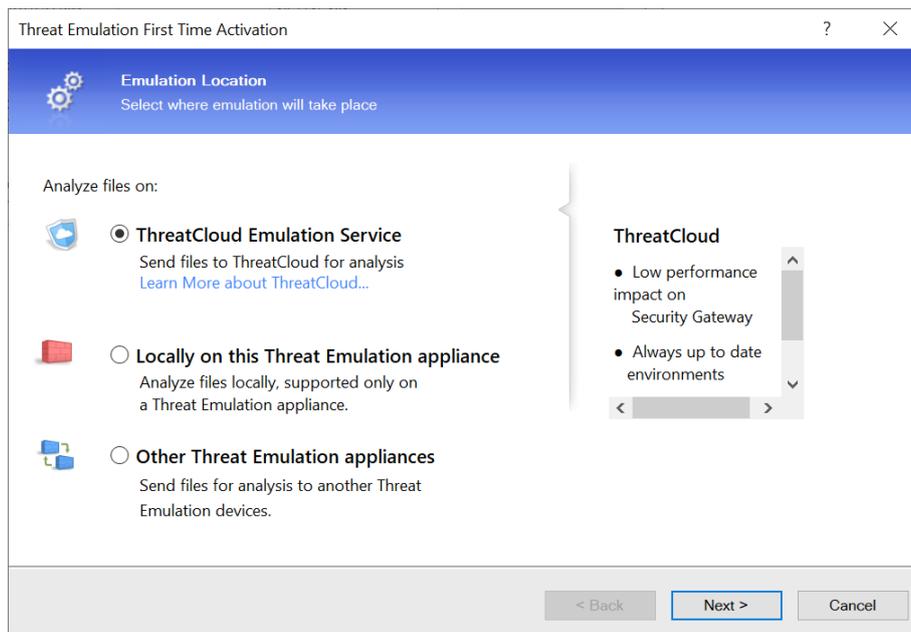
- Перейдите во вкладку Custom Threat Prevention и активируйте блейды IPS, Anti-bot, Anti-Virus:



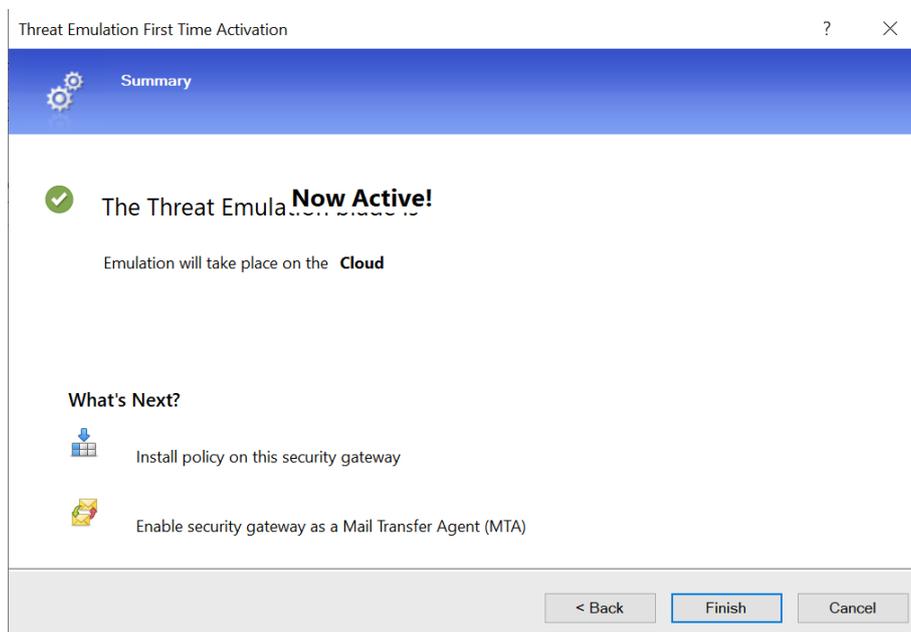
- В окнах First time activation установите переключатель в **According to the TP Policy**:



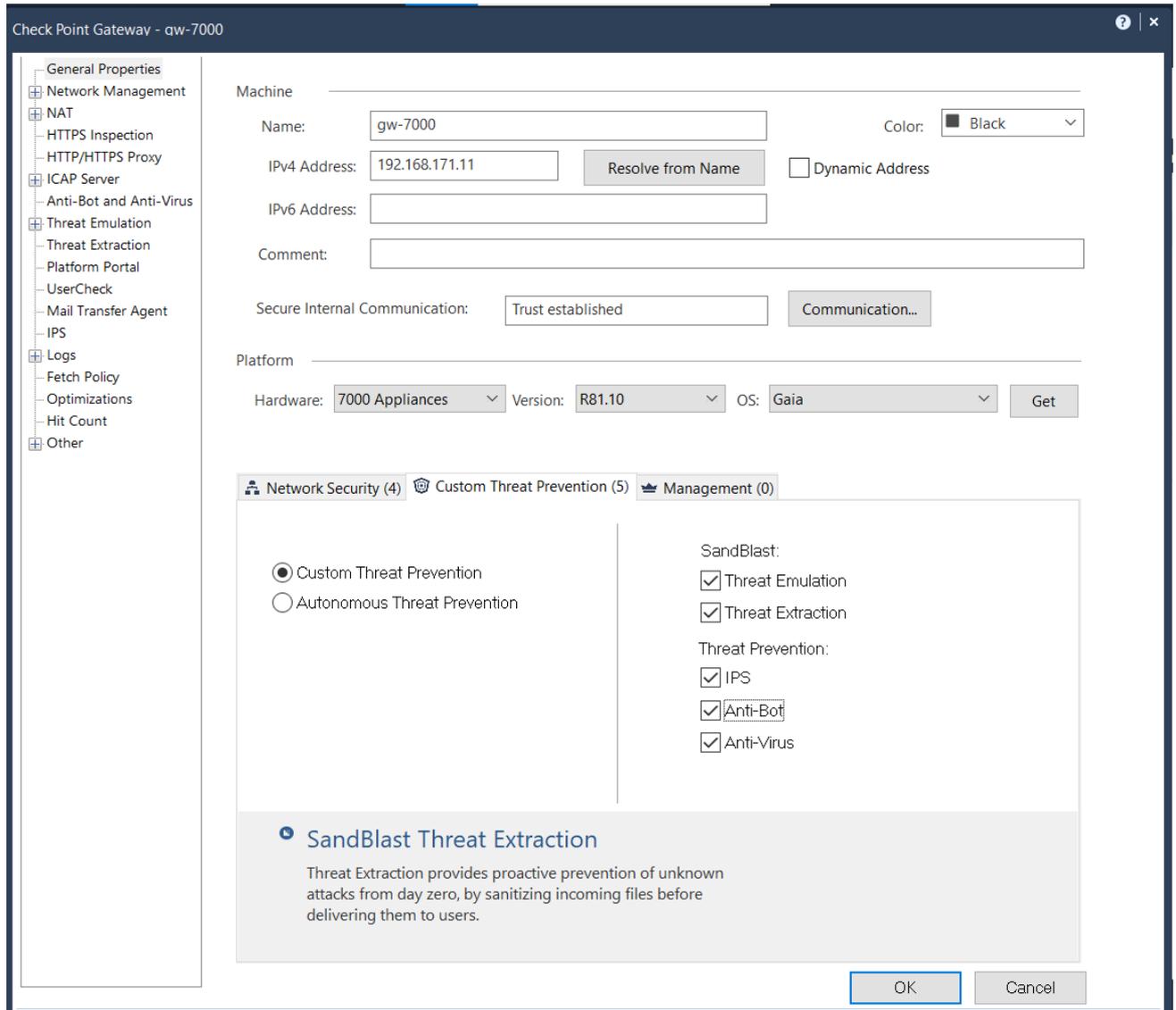
- Активируйте блейд Threat Emulation:



7. Завершите настройку блейда Threat Emulation. Нажмите **Finish**:



8. После настройки блейдов в окне свойств шлюза нажмите **OK**:



9. Дважды нажмите на устройство SMS. Активируйте блейды **SmartEvent Server** и **SmartEvent Correlation Unit**. Эти блейды отвечают за корреляцию событий безопасности и составление отчетов. Нажмите **OK**:

Check Point Host - dm\_sms\_8110

General Properties  
 Network Management  
 NAT  
 Logs  
 Other

Machine

Name:  Color:

IPv4 Address:

IPv6 Address:

Comment:

Secure Internal Communication:

Platform

Hardware:  Version:  OS:

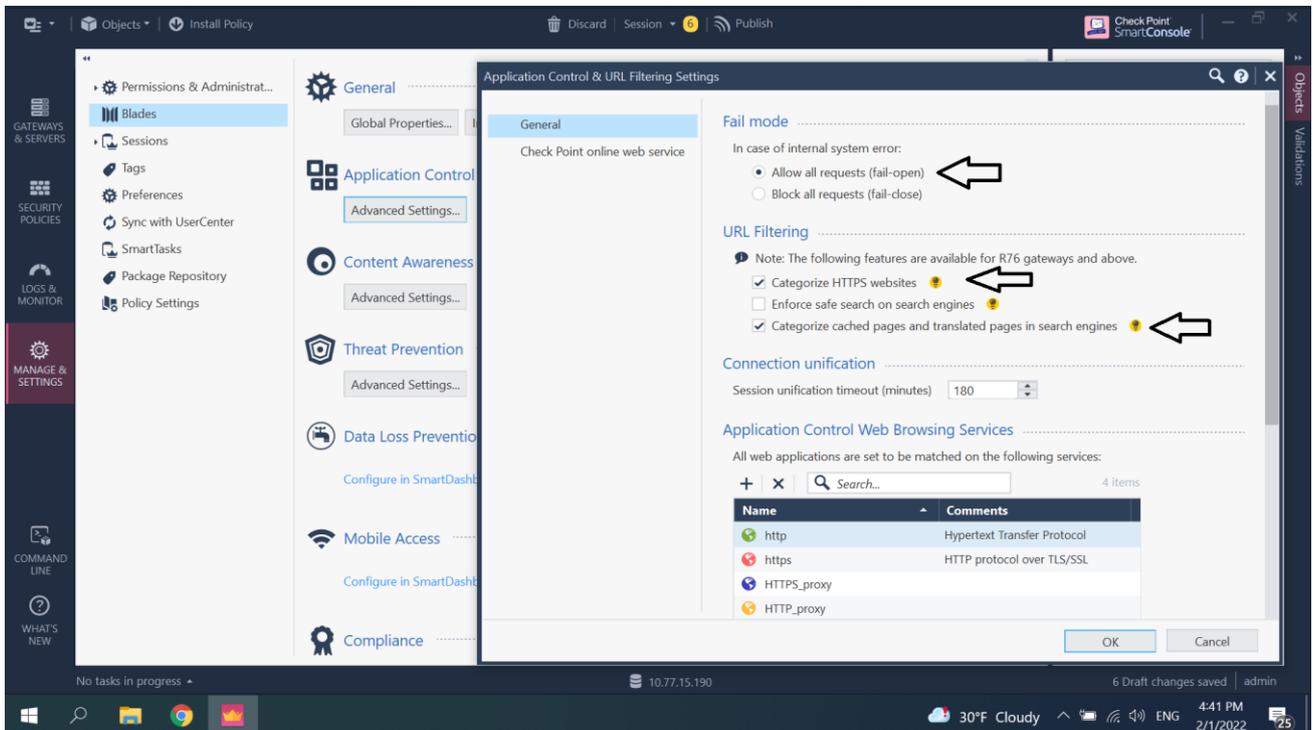
Management (5)

<input checked="" type="checkbox"/> Network Policy Management	<input type="checkbox"/> Workflow	<b>SmartEvent</b> <input checked="" type="checkbox"/> SmartEvent Server <input checked="" type="checkbox"/> SmartEvent Correlation Unit
<input type="checkbox"/> Secondary Server	<input type="checkbox"/> User Directory	
<input type="checkbox"/> Endpoint Policy Management	<input checked="" type="checkbox"/> Provisioning	
<input checked="" type="checkbox"/> Logging & Status	<input type="checkbox"/> Compliance	
<input type="checkbox"/> Identity Logging		

**Event Correlation**  
 Centralized, real-time, security event correlation and management for Check Point and 3rd party devices.

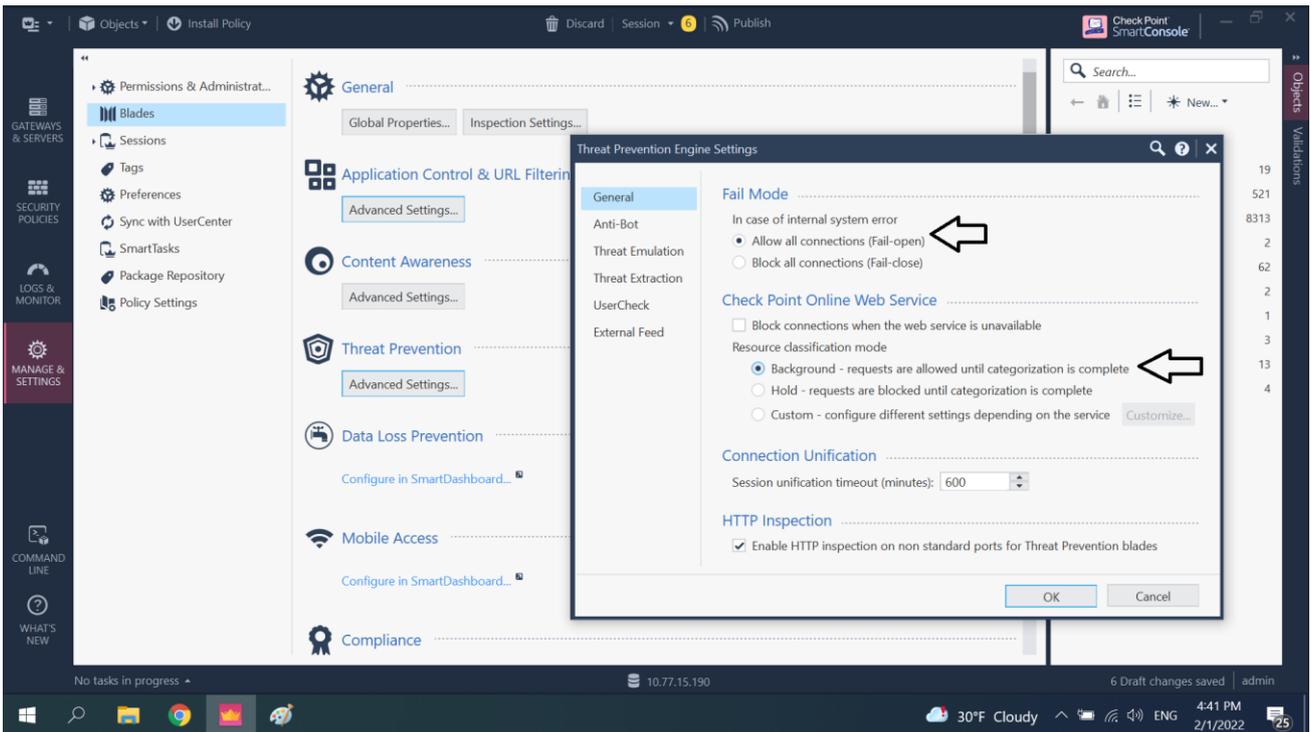
## Настройка блейда Application Control

Настройте блейд Application Control для Security CheckUP. Для этого перейдите **Manage & Settings - Blades - Application control. Advanced Settings...** В окне Application Control & URL filtering settings установите переключатель в положение **Allow all requests (fail-open)**, установите чекбоксы **Categorize HTTPS websites**, **Categorized cached pages and translated pages in search engines**. Нажмите **OK**:



## Настройка блейдов Threat Prevention

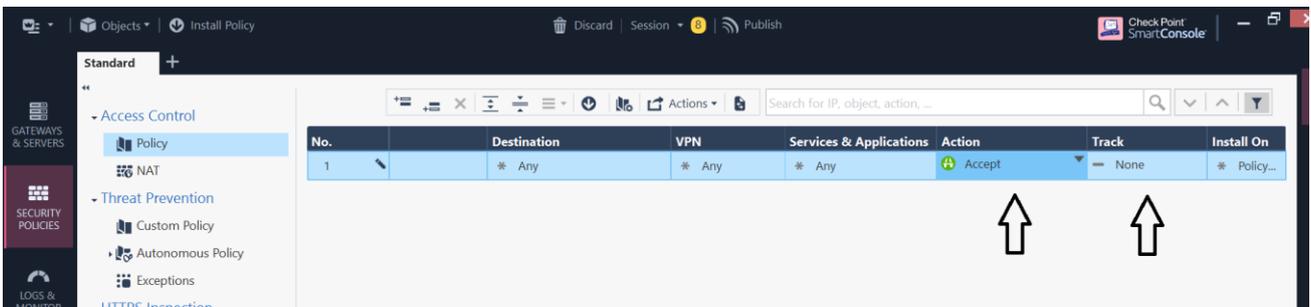
Для настройки блейдов Threat Prevention перейдите **Manage & Settings - Blades - Threat Prevention. Advanced Settings...** В окне Threat Prevention Engine Settings установите переключатели в положения **Allow all connections (fail-open)** и **Background - requests are allowed until categorization is complete**. Нажмите **OK**:



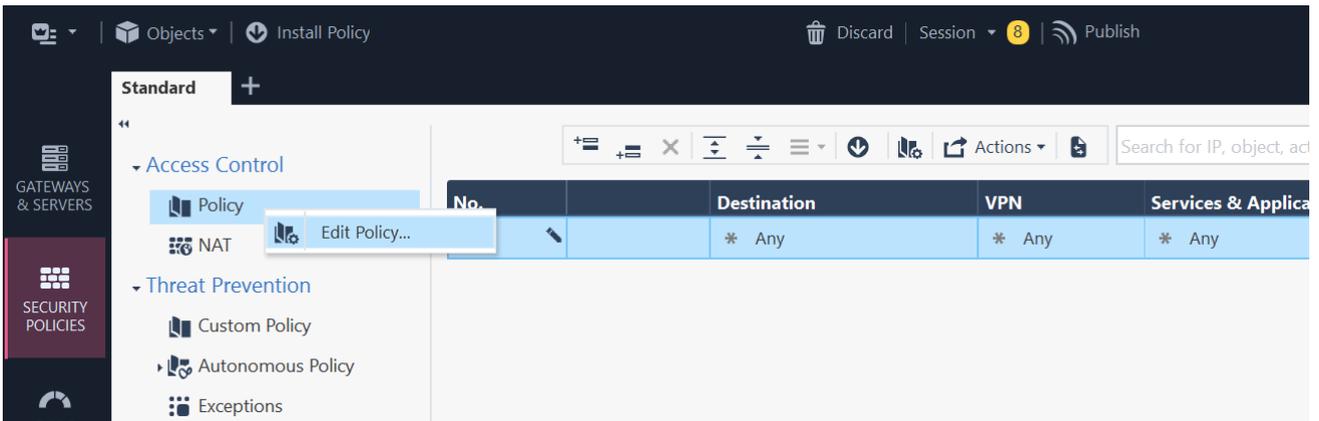
### Настройка политики Access Control

Для настройки политики Access Control перейдите в меню Security Policies.

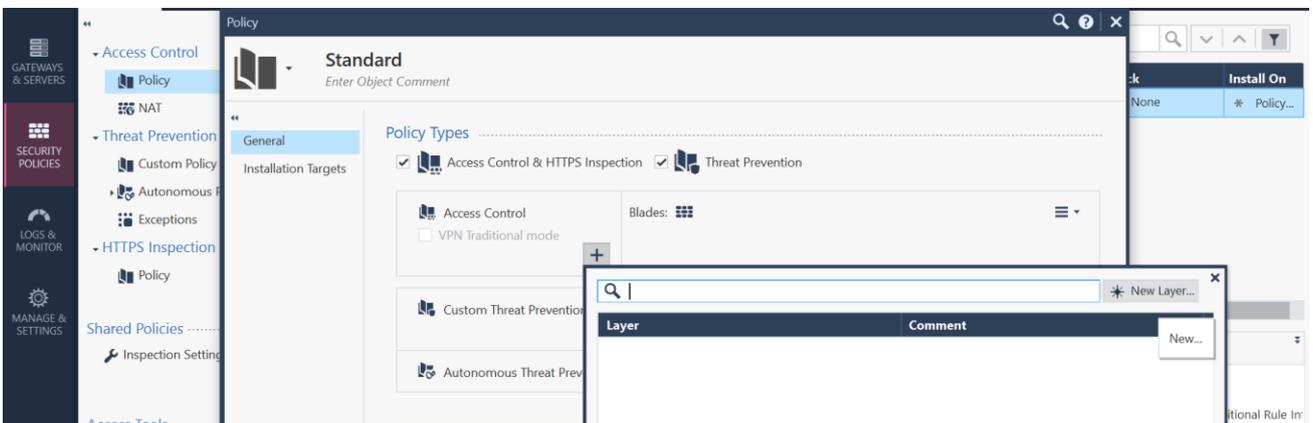
1. Измените CleanUP rule. В поле **Action** установите значение **Accept**, убедитесь, что в поле **Track** отключено логирование - **None**:



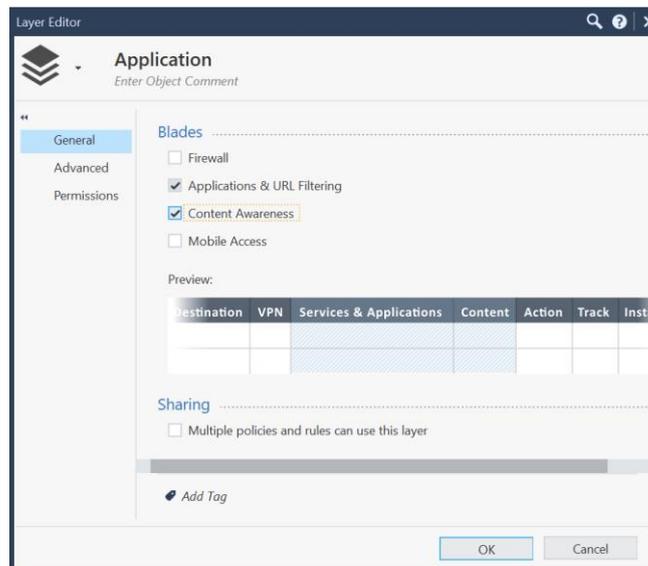
2. Создайте второй уровень политики для Application Control, для этого правой кнопкой мыши нажмите на Policy и выберите **Edit Policy**:



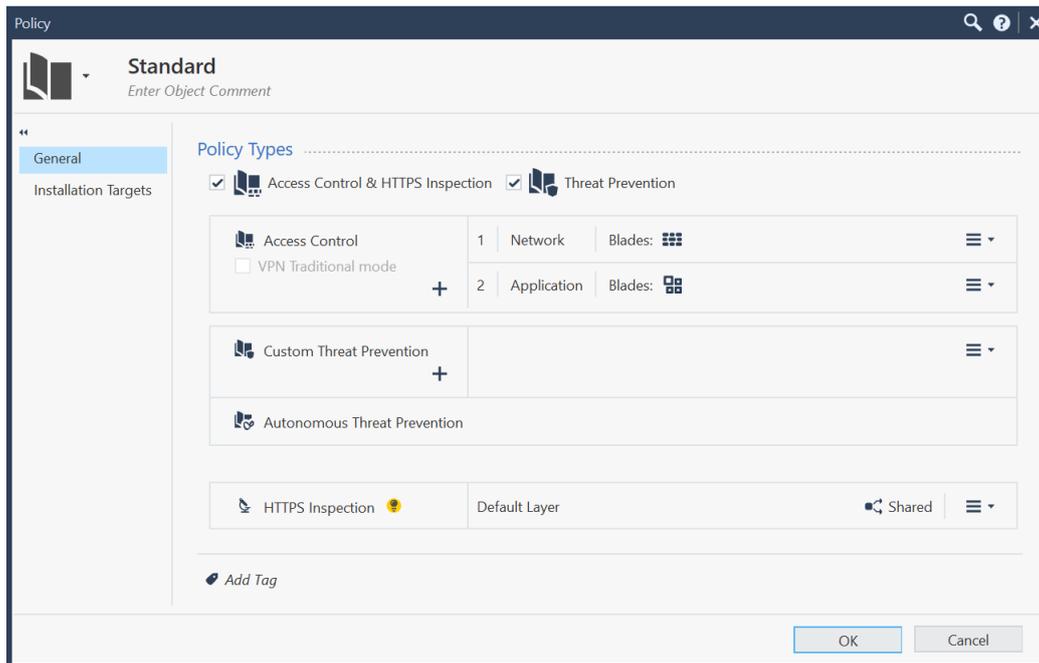
3. В окне Policy в поле **Access Control** нажмите **“+” - New Layer - New...**:



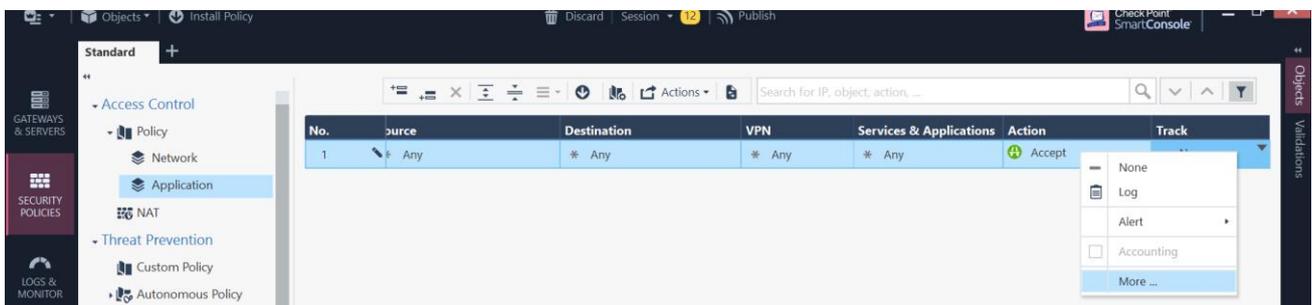
4. В окне Layer Editor задайте имя, например, **Application**. Установите чекбоксы **Application Control & URL Filtering** и **Content Awareness**:



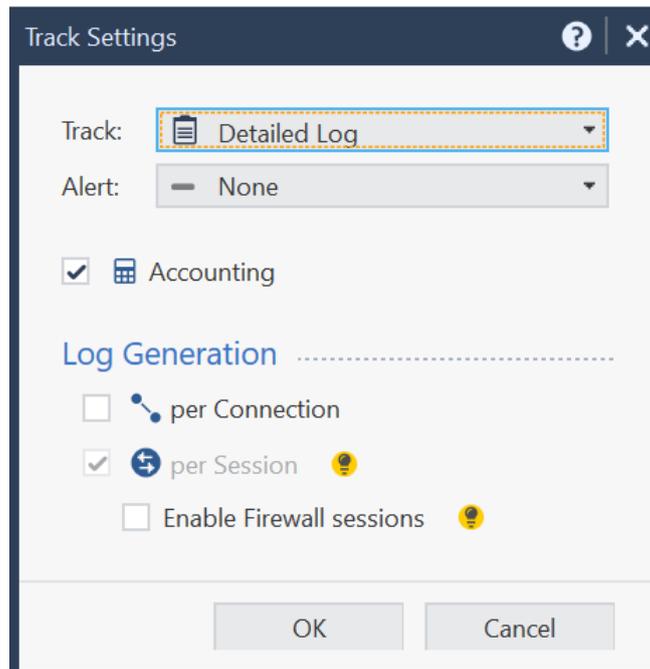
5. В окне Policy нажмите **ОК**:



- Измените CleanUP rule для уровня Application. Убедитесь, что в поле **Action** установлен **Accept**, в поле **Track** установлен **Detailed log**. Для установки Detailed log левой кнопкой мыши нажмите на None в поле Track, выберите **More ...**:

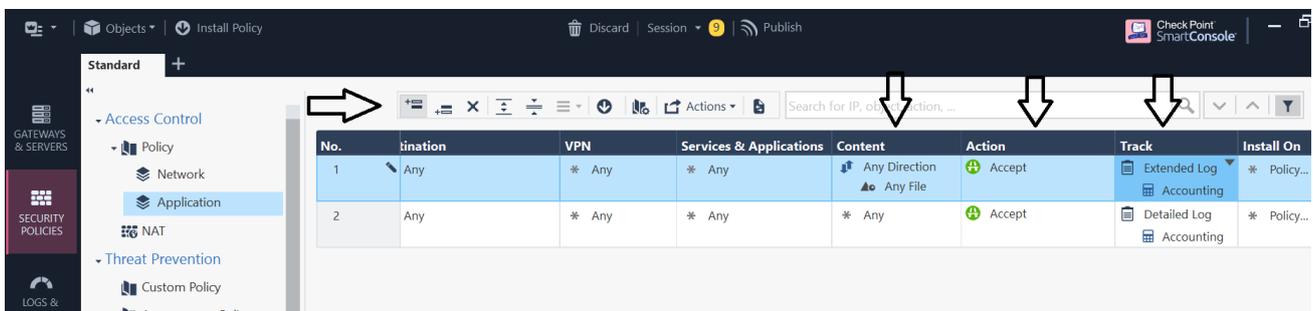


- В окне Track settings в поле Track выберите Detailed log, убедитесь, что установлен чекбокс **Accounting**. Нажмите **OK**:

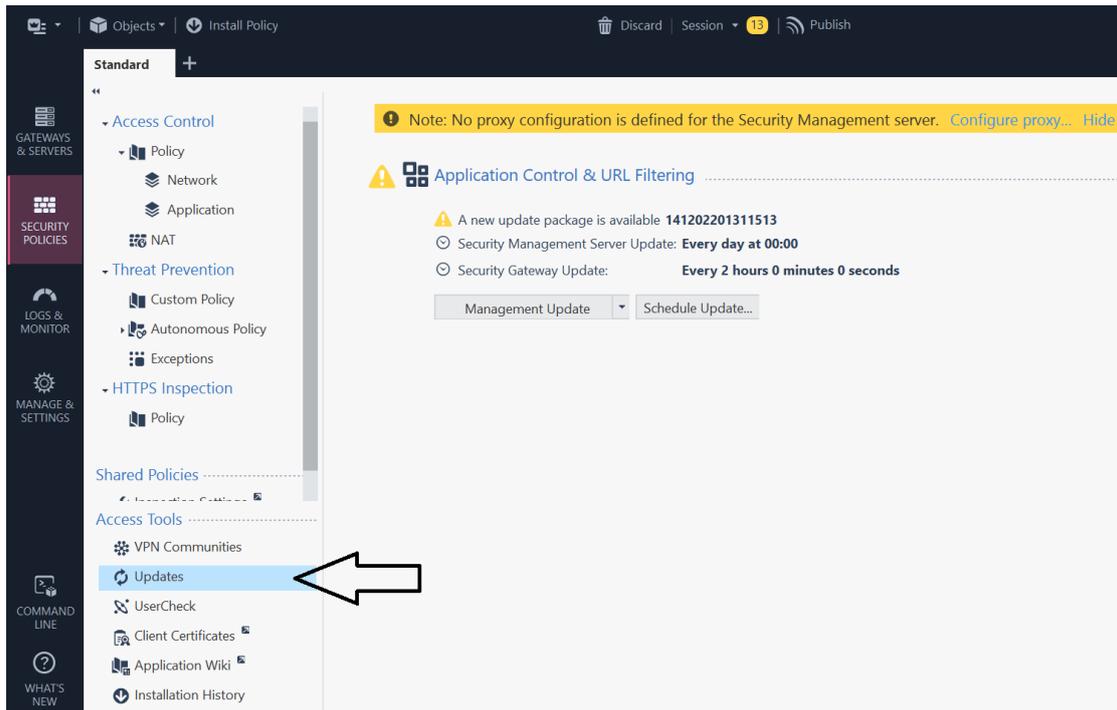


8. Добавьте правило для Content Awareness. Нажмите **Add rule above**. Убедитесь, что в полях установлены следующие значения:

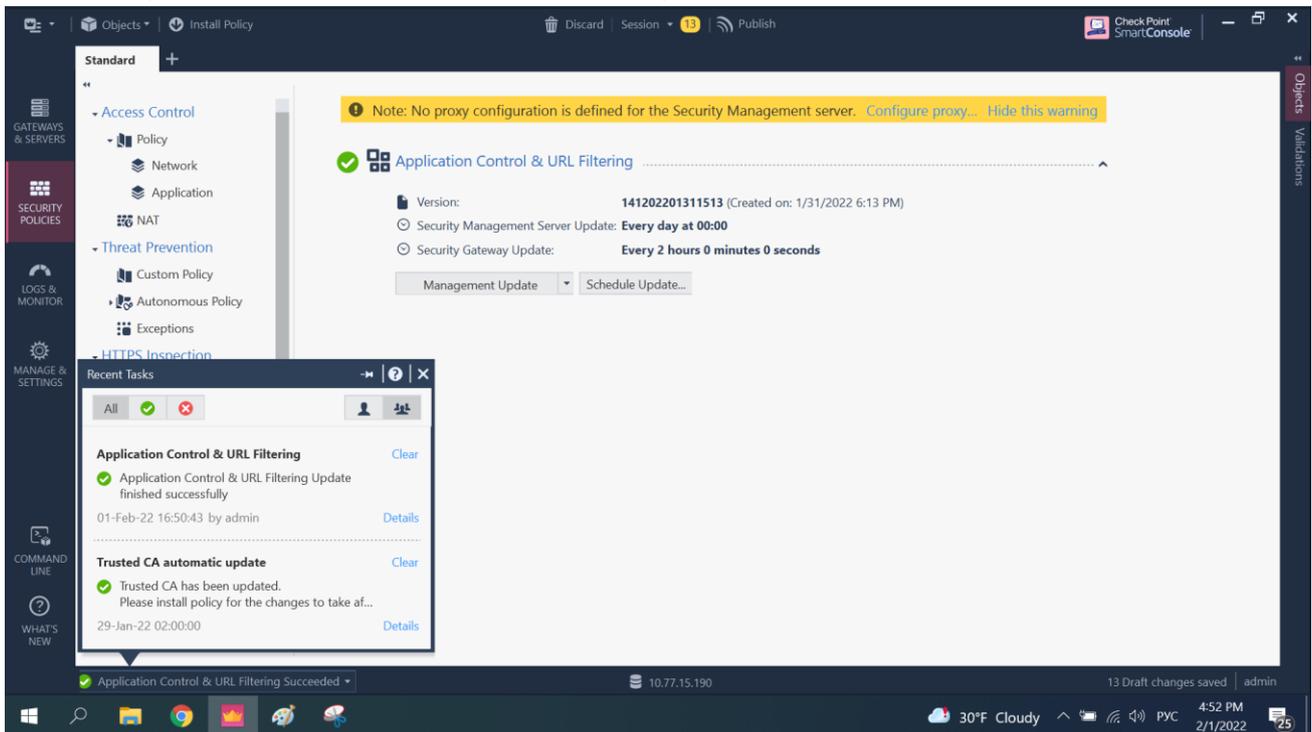
**Source - Any, Destination - Any, Services & Applications - Any, Content - Any file|Any direction, Action Accept, Track - Extended log + Accounting:**



9. Обновите базы бейда Application Control, для этого в разделе **Access Tools** выберите **Updates**:



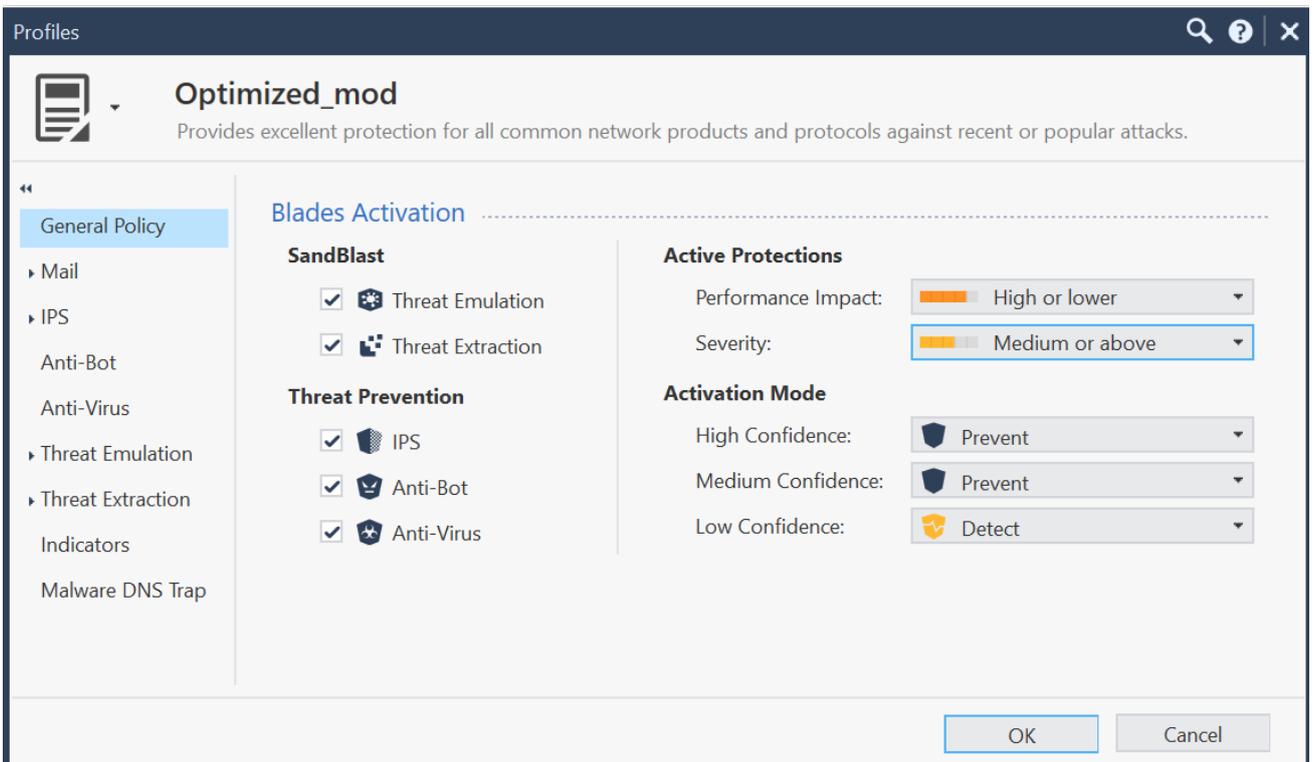
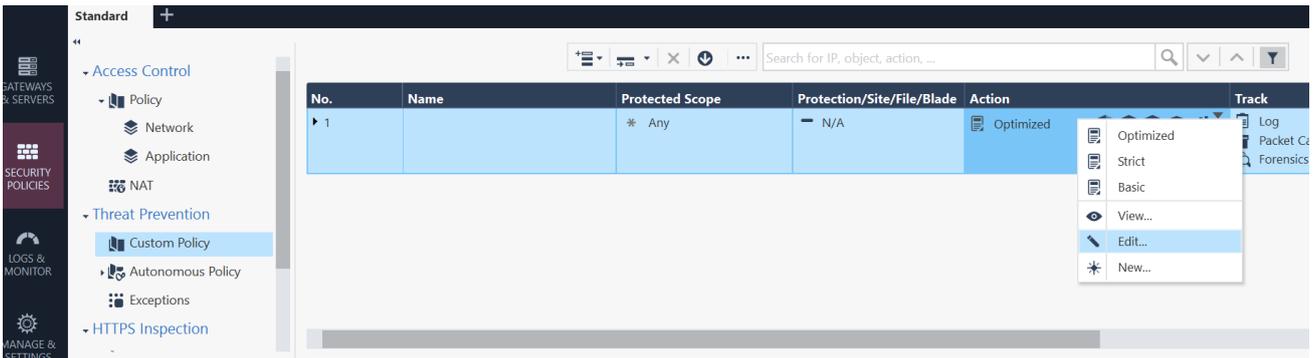
10. Запустите обновление баз и дождитесь завершения обновления:



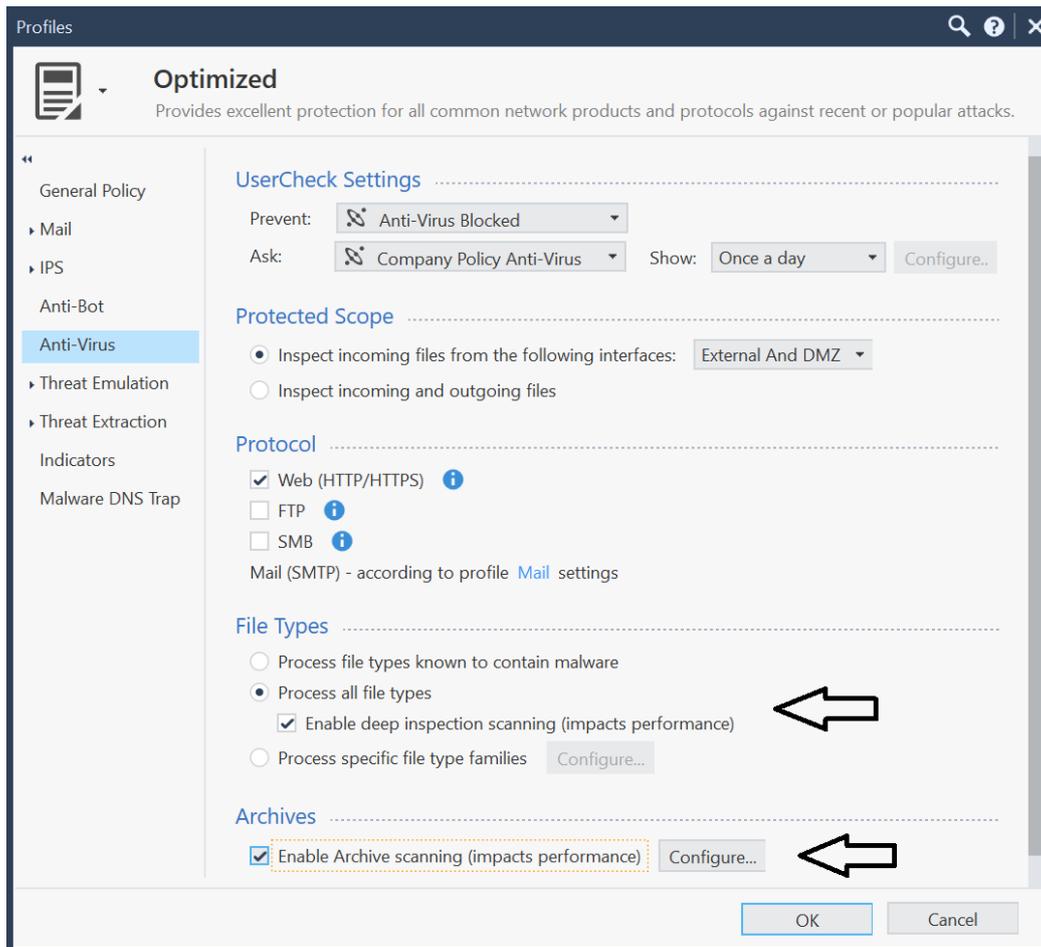
### Настройка политики Threat Prevention

Перейдите **Security Policies - Threat Prevention - Custom Policy**. По умолчанию установлена политика Optimized.

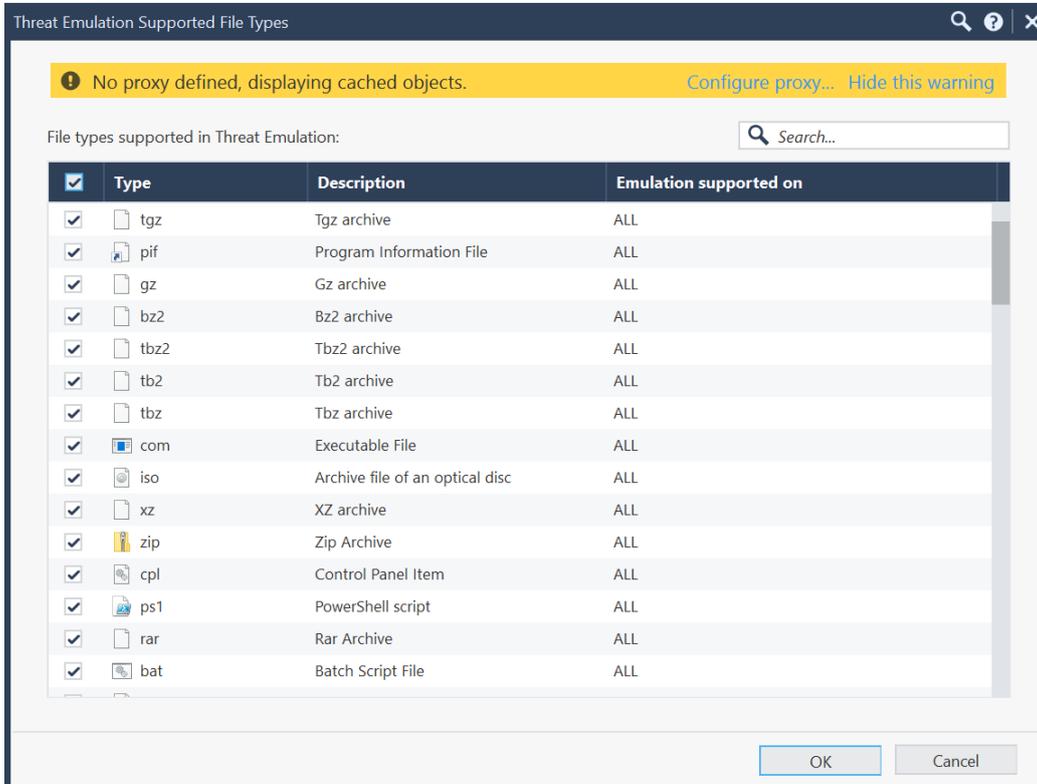
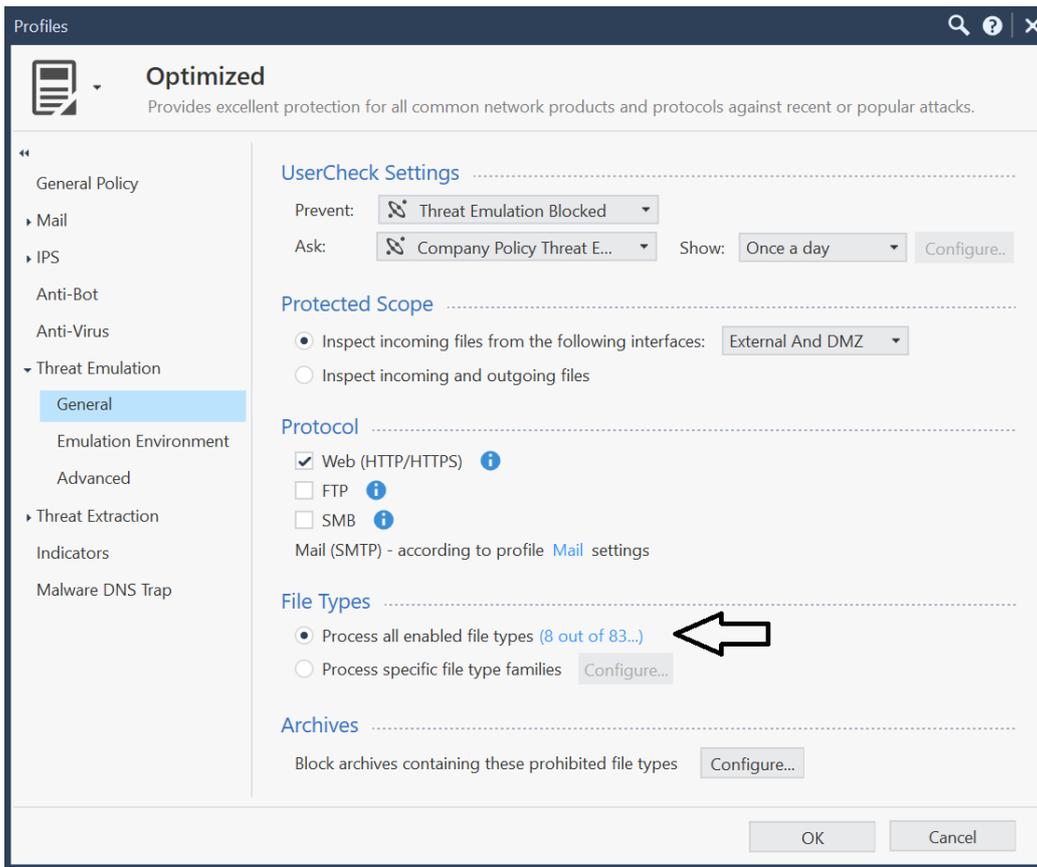
1. Измените настройки политики, для этого нажмите правой кнопкой мыши и выберите **Edit...**:



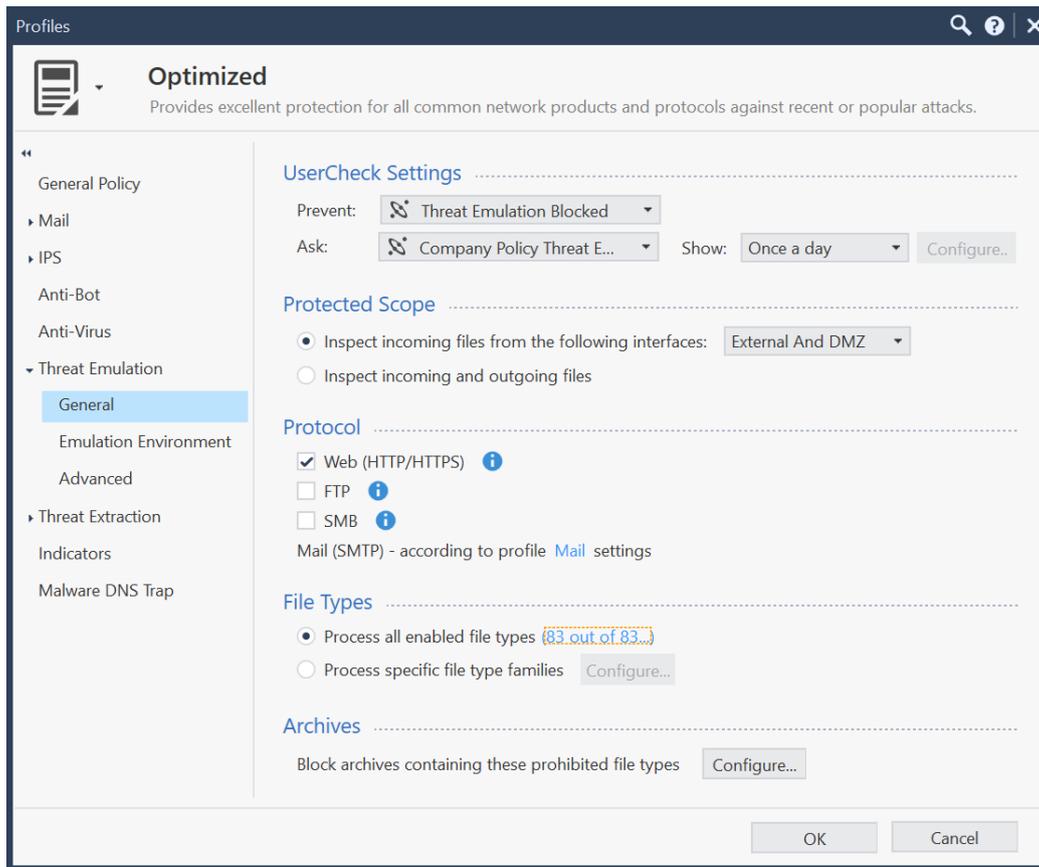
- Перейдите во вкладку Anti-Virus, в поле File Types установите переключатель в положение **Process all file types**, установите чекбокс **Enable drop inspection scanning**. Убедитесь, что установлен чекбокс **Enable Archive Scanning**:



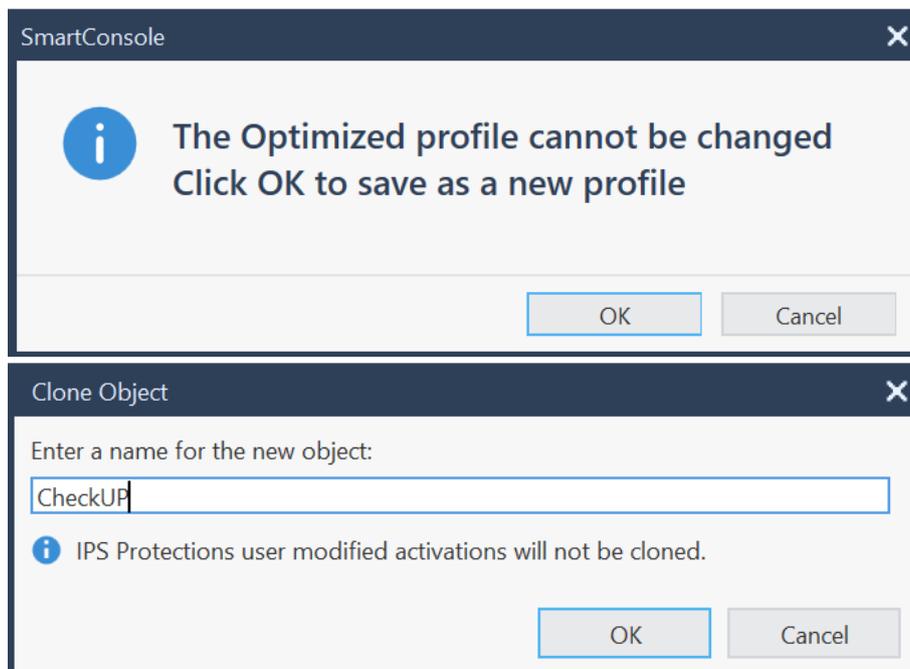
3. Перейдите во вкладку **Threat Emulation - General**. Включите эмуляцию для всех известных типов файлов:



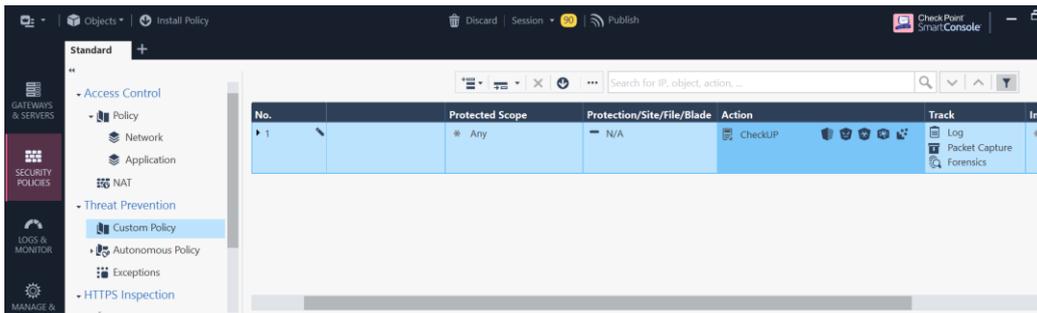
4. В окне Profiles нажмите **OK**:



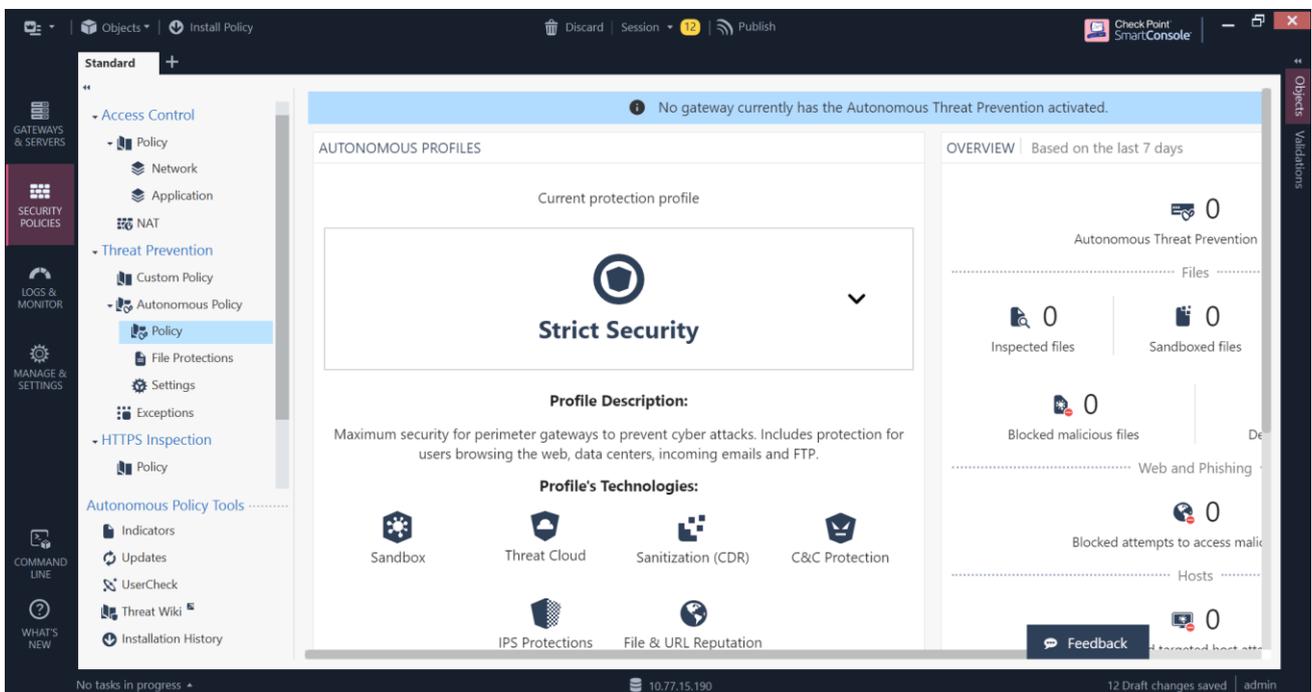
5. Сохраните измененную политику под другим именем, например, **CheckUP**:



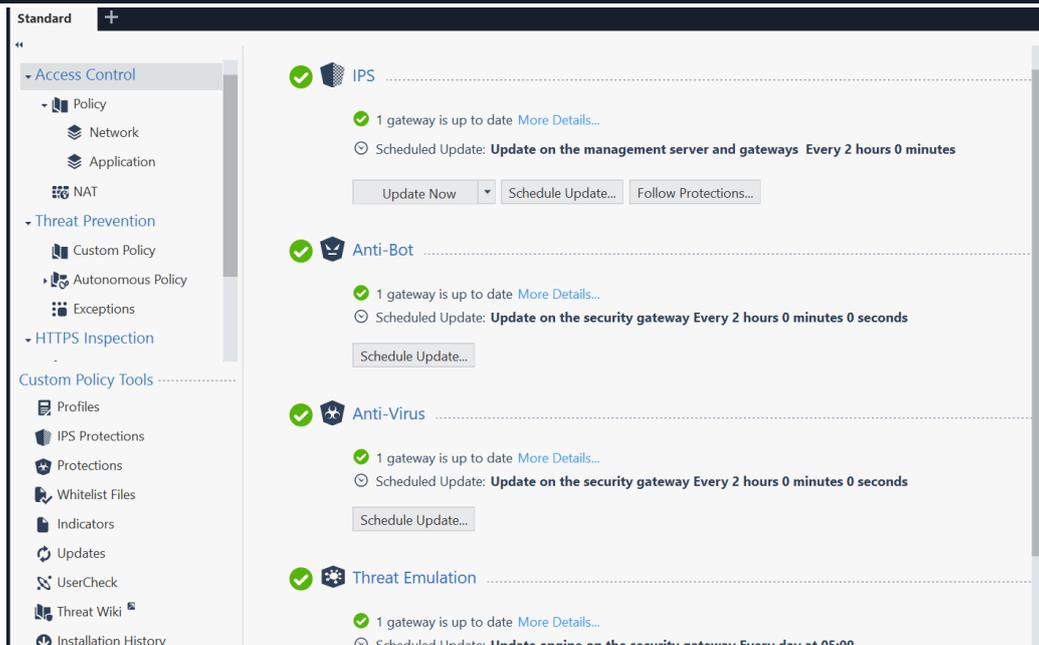
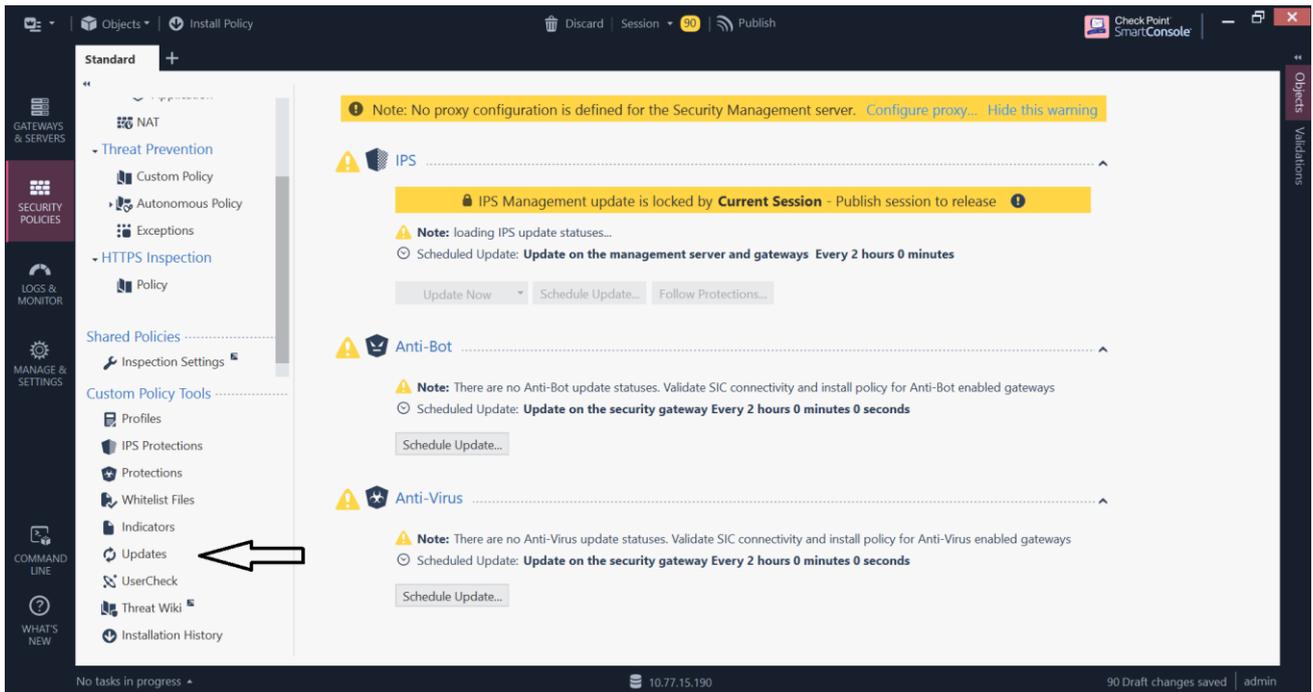
6. Замените политику Optimized на политику CheckUP:



7. **Опционально\***, вместо Custom Policy можно использовать **Autonomous policy** в режиме Strict. Для этого выберите Threat Prevention - Autonomous policy - Policy. В выпадающем меню выберите режим Strict:

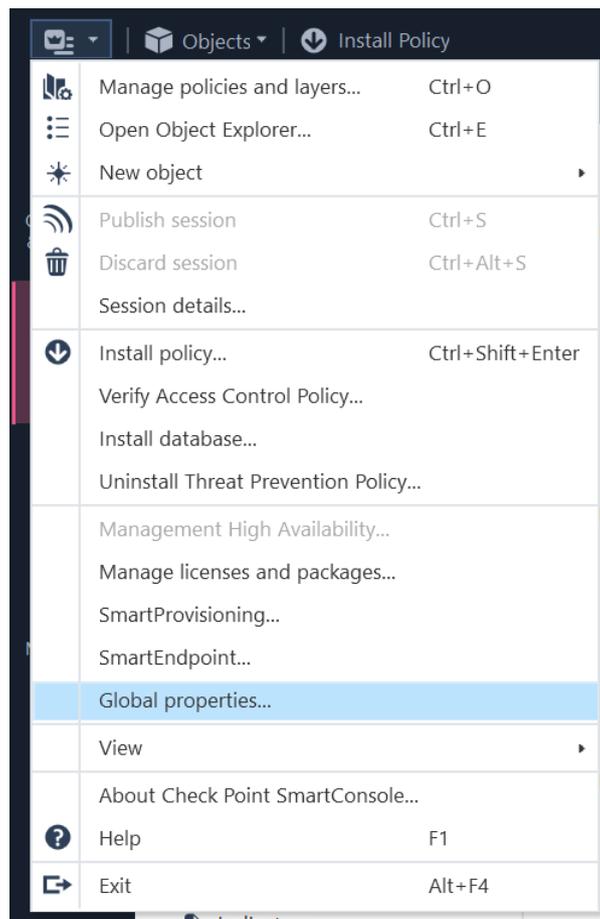


8. Перейдите в раздел **Custom Policy Tools - Update**. И обновите базы блейдов IPS, Anti-bot, Anti-Virus и Threat Emulation:

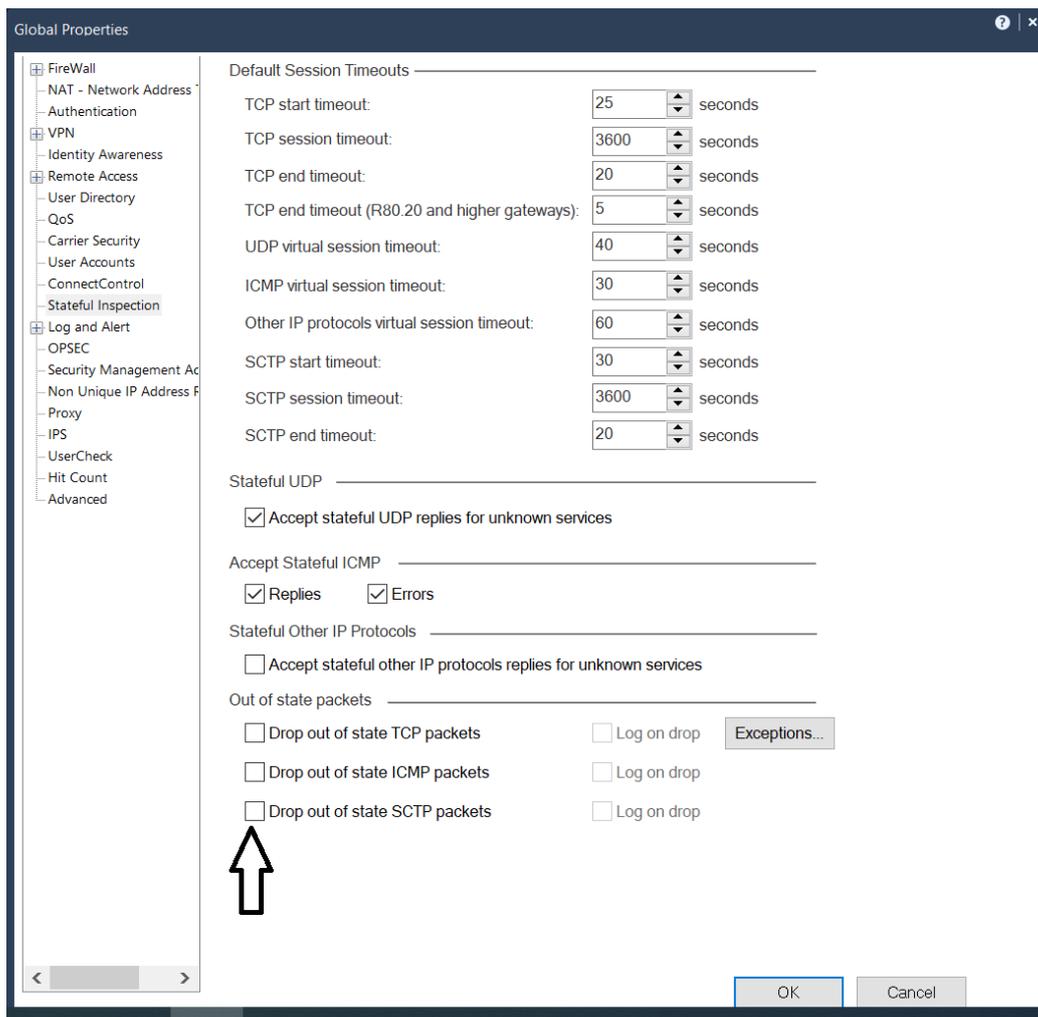


## Настройка параметра Stateful Inspection

1. Перейдите в **Menu - Global Properties**:

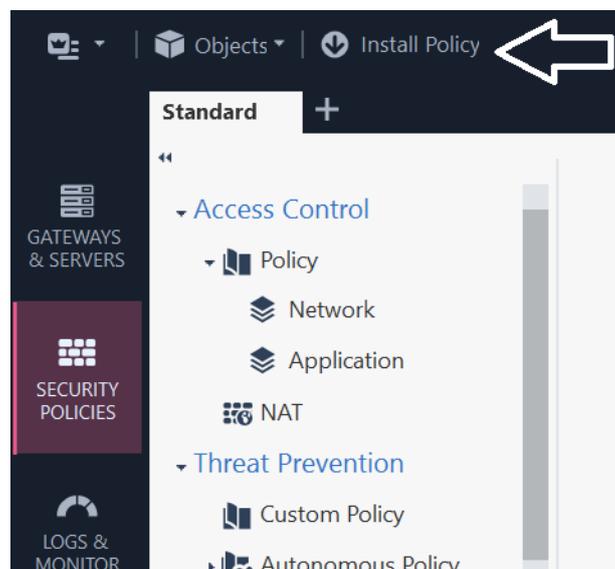


2. Перейдите в раздел **Stateful inspection** и снимите чекбоксы для **Drop out of state TCP packets**, **Drop out of ICMP packets** и **Drop out of SCTP packets**. Нажмите **OK**:

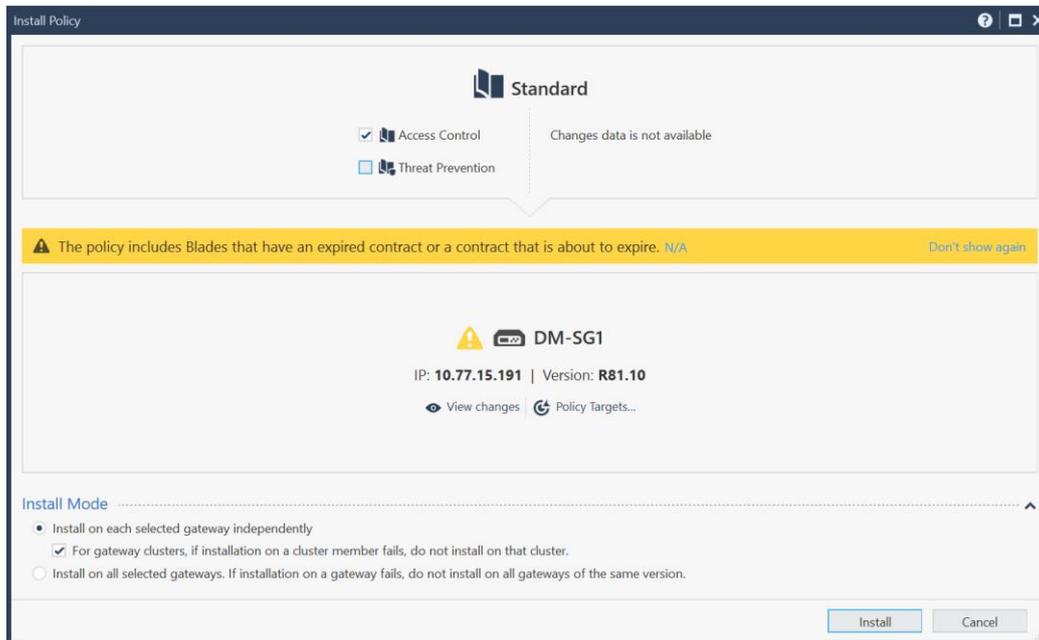


## Установка политик Access Control u Threat prevention

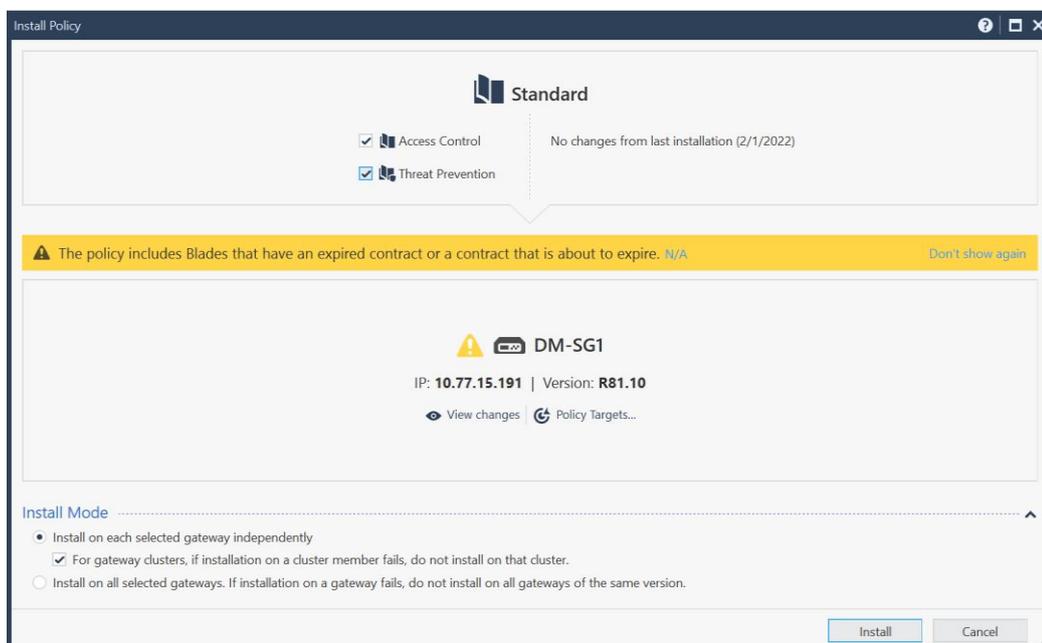
1. Нажмите **Install Policy - Publish & Install**:



2. В окне Install Policy **снимите чекбокс Threat Prevention** и нажмите **Install**. Дождитесь окончания установки политики:



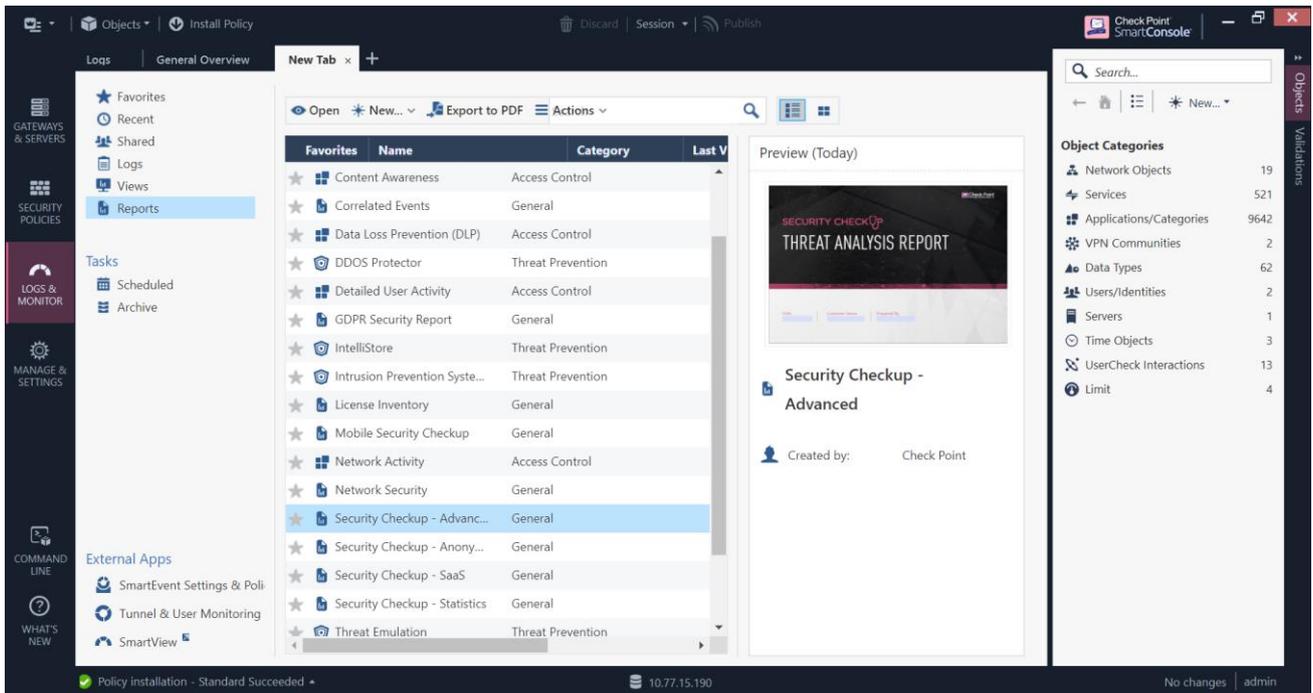
3. Установите политику Threat Prevention. Для этого нажмите **Install Policy**, убедитесь, что **установлен чекбокс Threat Prevention**, нажмите **Install**. Дождитесь окончания установки:



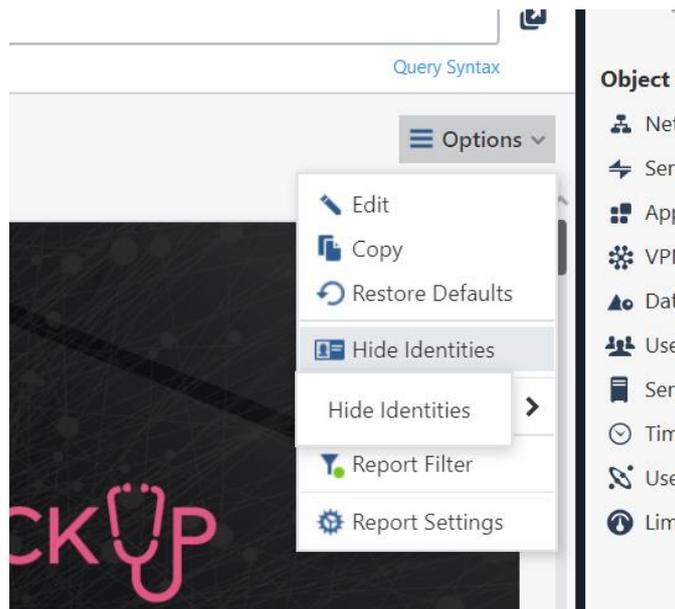
## 7 Как составить отчет

После двух недель работы оборудования, составляется отчет Security CheckUP. Для этого:

1. Перейдите во вкладку **Logs & Monitor**. Создайте новую вкладку **New tab - Reports - Security CheckUP advanced**:



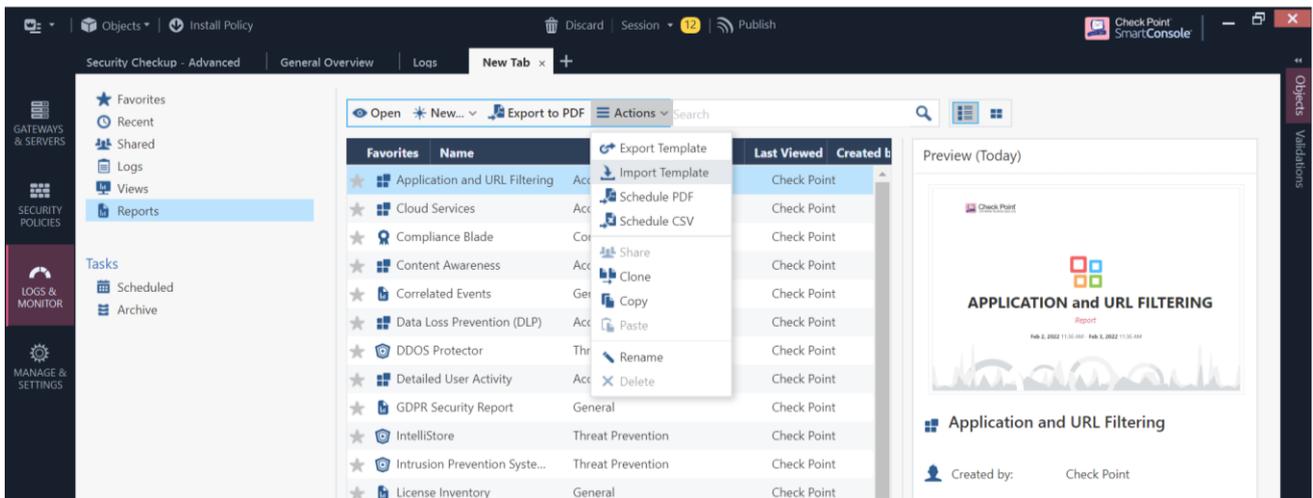
2. При необходимости отчет можно обезличить, для этого выберите **Options - Hide Identities**:



Ознакомьтесь с [примером отчета](#).

## 8 Как получить отчет на русском языке

1. Загрузите [шаблон отчета](#) на русском языке;
2. Распакуйте скачанный архив;
3. В SmartConsole перейдите **Logs & Monitor - New Tab - Reports - Actions - Import**. Укажите путь до скачанного шаблона .cpr:



4. Теперь в списке шаблонов доступен отчет на русском языке:

