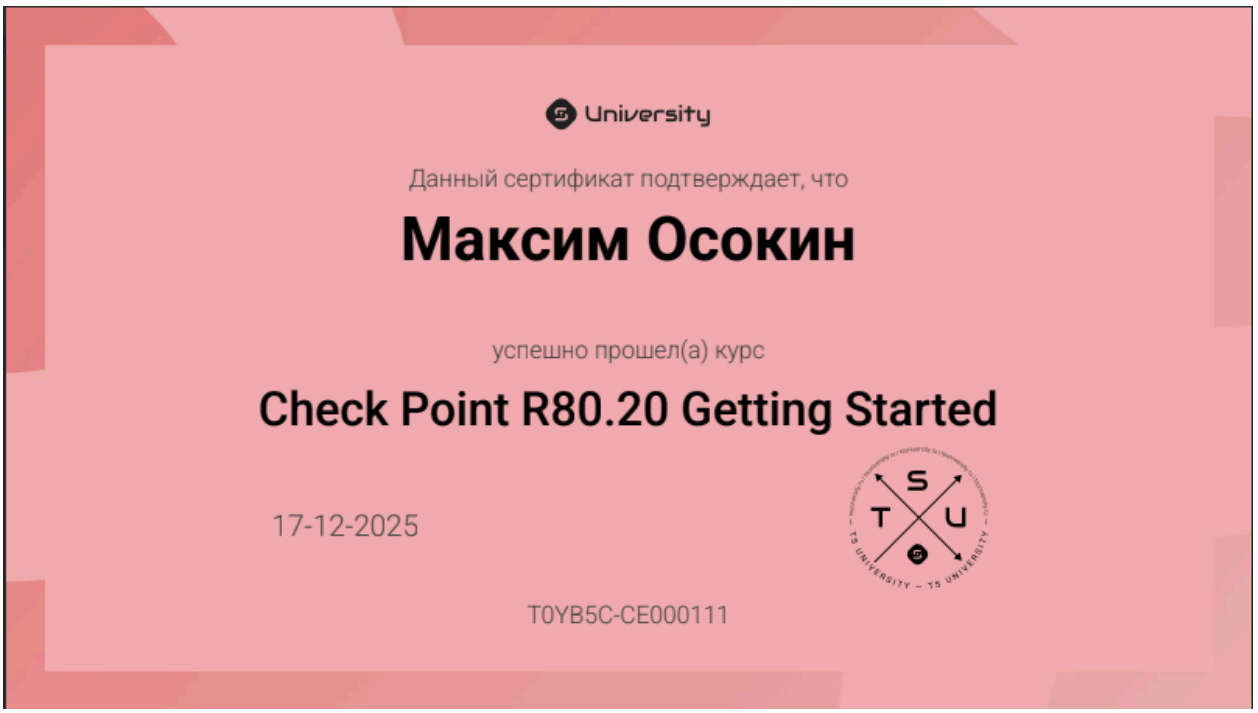
Изучив материалы курса от вендора Check Point, узнал как применять межсетевые экраны нового поколения на максимум, и как настраивать такие блейды, как Anti-Virus, IPS, Threat Emulation, Application Control, Content Awareness, Compliance, которые обладают лучшим в своем классе функционалом предотвращения угроз, удобны в развертывании и управлении. В процессе изучения курса, мной были составлены, далее представленные методика настройки и чек-лист для проверки выполненной настройки.

По итогам курса, выполнил практические задания, узнал о правилах настройки повышающих безопасность и познакомился с различием версий операционных систем безопасности от компании Check Point "Gaia". Обучаясь в университете выполнял базовые настройки сетевого оборудования (на кафедре были лабораторные работы по промышленному оборудованию), а также проводились работы с оборудованием Cisco. Успешно прошел тестирование и получил сертификат от вендора.



Методика настройки Check Point

Этап 1. Планирование и подготовка.

- ☐ Определить роли: Выделить серверы для Security Management Server и Security Gateway (физические или виртуальные).
- ☐ Спланировать сетевую схему: IP-адреса, зоны (LAN, DMZ, WAN), режим работы шлюза (роутер, bridge).
- ☐ Спланировать политики: Какие пользователи/сети что могут делать, какие угрозы блокировать в первую очередь.

Этап 2. Базовая установка и настройка.

- ☐ Установить ОС Gaia на оборудование(предустановленная версия урезан функционал) + обновить.
- ☐ Выполнить первичную настройку через Gaia Portal или `config_system` в CLI: задайте hostname, IP-адреса интерфейсов, маршруты по умолчанию, настройки DNS и NTP.
- ☐ Инициализировать Security Management Server и установить клиент SmartConsole.
- ☐ Создать объекты шлюзов в SmartConsole, установить с ними SIC-соединение.

Этап 3. Настройка базовых политик безопасности.

- ☐ Безопасность управления: Ограничить доступ к портам управления (TCP 22, 443, 18190) только с доверенных сетей.
- ☐ Базовая политика доступа (Access Control):
  - ☐ Создать правило, разрешающее необходимый служебный трафик (DNS, NTP, обновления) из внутренних сетей.
  - ☐ Добавить правило "Cleanup" в конце политики, которое запрещает и логирует весь остальной трафик.
- ☐ Настроить NAT (статические или маскарад) для выхода в интернет.

Этап 4. Включение и тонкая настройка защитных механизмов.

- ☐ HTTPS Inspection: Создать корневой CA, развернуть его на клиентах и включите инспекцию. Начать с пилотной группы пользователей.
- ☐ Контроль контента: В Access Control Policy включить блейды и создайте правила для блокировки опасных приложений (Application Control) и типов файлов (Content Awareness).
- ☐ Предотвращение угроз: Создать Threat Prevention Policy, активировать блейды (IPS, Anti-Virus, Anti-Bot) и настроить профили для разных сегментов сети.

Этап 5. Ввод в эксплуатацию и мониторинг

- ☐ Установить все политики на шлюзы.
- ☐ Протестировать доступность ключевых сервисов.
- ☐ Активировать мониторинг: Включить SmartEvent, настроить алерты, регулярно (минимум два раза в неделю) проверять логи на предмет аномалий и ложных срабатываний.
- ☐ Документировать все изменения и настройки.

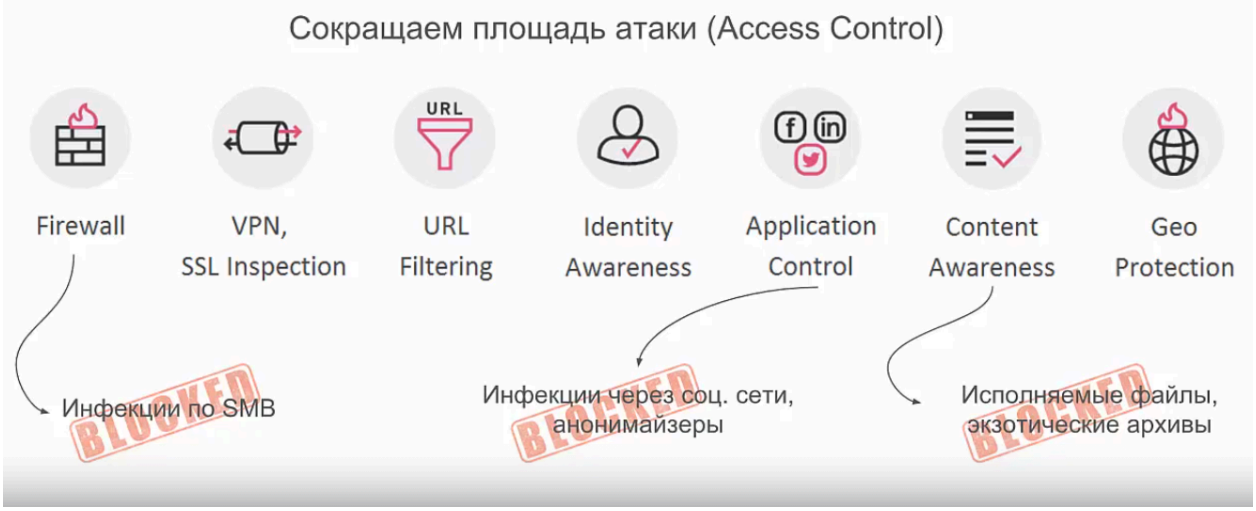


Рисунок 1. Сокращаем площадь атаки (Access Control)

Рисунок 2. Сокращаем площадь атаки (Threat Prevention)

Рекомендуется проверить надежность настроек практическим методом - полнофункциональным сканером уязвимостей (OPENVAS, RedCheck, HScan, XSpider (Positive Technologies), Nessus / Tenable, Burp Suite, OWASP ZAP, ScanOVAL, F-Secure Radar, Nikto, ..). Для предотвращения перегрузки сети, съем данных лучше проводить в часы минимальной нагрузки. В случае проверки приложений стоит дополнять автоматизированные тесты ручным пентестингом и/или инструментами из Kali Linux.

Сканирование рекомендуется проводить перед настройкой (Этап 1 планирования). Это поможет оценить исходное состояние сети, выявить небезопасные сервисы и активы, чтобы правильно спроектировать политики доступа.

После настройки (Этап 5). Сканирование позволяет верифицировать эффективность правил настройки Check Point. Например, проверить, что блокировка Geo-Policy работает, уязвимые порты закрыты, и т.д.

Чек-лист для проверки выполненной настройки.

Область настройки	Контрольный пункт	Где проверить / настроить	Комментарий и важность
1. Первичные и управление	Установлены последние обновления (и сигнатуры угроз) и сигнатуры угроз.	CPUSE (Gaia Portal или CLI), SmartConsole	Критично для безопасности и стабильности. Рекомендуется сначала проверять совместимость.
	Настроена синхронизация времени (NTP) на всех устройствах.	Gaia Portal (System Management > Date and Time)	Предотвращает рассинхронизацию кластера и проблемы с логированием.
	Роли серверов (Management, Gateway) и SIC-соединения настроены корректно.	SmartConsole (Gateways & Servers)	Основа для централизованного управления.
	Для кластера: выбран режим (Active/Standby), настроены sync-интерфейсы, разрешен multicast/broadcast трафик.	Gaia CLI (cphaprob -a if), настройки виртуальных коммутаторов	Корректная работа кластера высокой доступности.
2. Контроль трафика и контента	Включена HTTPS Inspection (SSL/TLS) для исходящего и, при необходимости, входящего трафика.	Свойства шлюза > HTTPS Inspection	Без этой функции NGFW слеп к большей части угроз. Ключевой приоритет.
	Корпоративный CA-сертификат для HTTPS Inspection создан/импортирован и развернут на доверенных клиентах.	Свойства шлюза > HTTPS Inspection, групповые политики (GPO)	Избегает постоянных предупреждений в браузерах пользователей.
	Настроены правила обхода (Bypass) HTTPS Inspection для критичных приложений (напр., мобильные банки).	SmartConsole > HTTPS Inspection Policy	Не все приложения работают с подменой сертификата.
	Включены и настроены блейды Application Control и URL Filtering для блокировки опасных категорий (анонимайзеры, ботнеты, фишинг и т.д.).	Access Control Policy > правила	Уменьшает "площадь атаки", блокируя угрозы до глубокой проверки.
	Включен и настроен блейд Content Awareness для блокировки загрузки нежелательных типов файлов (.exe, .scr, архивы).	Access Control Policy > столбец "Content & Data" в правилах	Превентивная защита, снижает нагрузку на антивирус.
3. Предотвращение угроз (Threat Prevention)	Профиль IPS изменен с "Optimized" на "Strict" или настроен вручную.	Threat Prevention Policy	Профиль по умолчанию часто недостаточно строгий.
	IPS и Anti-Bot вынесены в отдельные слои (Inline Layers).	Access Control Policy > меню "Layer"	Позволяет создавать более гибкие и эффективные правила.
	Для разных сегментов сети (пользователи/серверы) используются разные профили Threat Prevention.	Threat Prevention Policy	Защита адаптируется под специфику трафика, оптимизируется нагрузка.
	Включен режим Hold для Anti-Virus и Threat Emulation вместо Background.	Свойства блейда Anti-Virus / Threat Prevention	Файл задерживается до получения результата проверки, а не пропускается.
	Антивирус настроен на глубокую проверку (Deep Inspection) и сканирование архивов.	Свойства блейда Anti-Virus	Повышает вероятность обнаружения сложных угроз.
	Включен и настроен Threat Emulation (песочница) хотя бы в режиме Detect.	Threat Prevention Policy	Защита от атак нулевого дня и целевого вредоносного ПО.
4. Мониторинг, логирование и обслуживание	Настроена Geo-политика для блокировки трафика из/в нежелательные регионы.	Access Control Policy с объектами "Country"	Снижает нагрузку и риск атак из "опасных" юрисдикций.
	Включены и проверены блейды управления и логирования (Logging & Status, SmartEvent).	SmartConsole > Manage & Settings > Blades	Без логов невозможен анализ инцидентов.
	Регулярно анализируются логи на предмет ложных срабатываний (False Positive) и пропущенных угроз (False Negative).	Logs & Monitor, SmartEvent	Пример фильтра для поиска пропущенных угроз: action:Detect AND severity:(High OR Critical).
	Используется встроенный Compliance Blade для автоматической проверки лучших практик.	Вкладка "Compliance" в SmartConsole	Автоматизирует проверку многих пунктов этого чек-листа.