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.

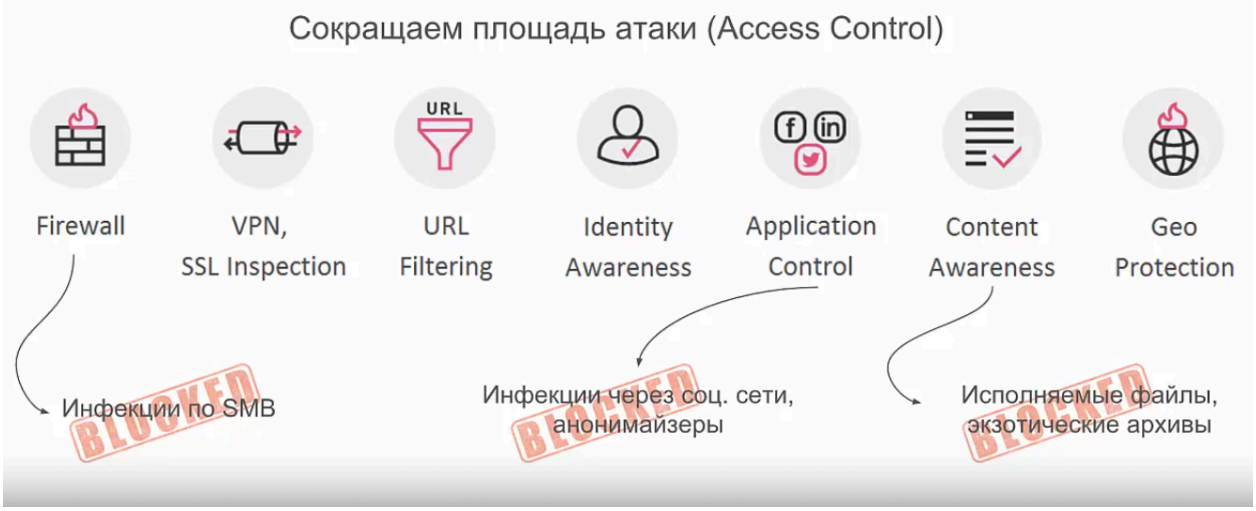

Рисунок 1. Сокращаем площадь атаки (Access Control)

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.