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.