Обзор продукта Microsoft Forefront TMG 2010

Антон Миносьян
Ведущий инженер отдела системной интеграции
AMinosjan@polikom.ru

ПОЛИКОМ ПРО

Поставка ПО и оборудования
ИТ-инфраструктура
Бизнес-приложения
ЦОД, сети, инженерная инфраструктура

Линейка продуктов Microsoft Forefront

- Не только антивирусная защита
- Идентификация
  - Forefront Identity Manager (бывший ILM)
- Пограничная безопасность (Edge Security)
  - Forefront Threat Management Gateway 2010
  - Unified Access Gateway 2010 (предыдущая версия называлась IAG 2007)
- Безопасность серверов Microsoft (Suite)
  - Forefront Protection 2010 for Exchange Server
  - Forefront Online Protection for Exchange
  - Forefront Protection 2010 for SharePoint
  - Forefront Security for OCS
- Безопасность конечной точки (часть Suite)
  - Forefront Client Security, FEP 2010

Продукты Forefront для защиты периметра

- Продукты Forefront Edge Security and Access обеспечивают расширенную безопасность периметра сети, а также настраиваемые политики доступа к корпоративной IT-инфраструктуре
- ISA 2006 -> Forefront Threat Management Gateway 2010
  - Защита сети, интегрированная расширенная защита от Интернет-угроз
- IAG 2007 -> Forefront Unified Access Gateway 2010
  - Платформа для управления удаленным доступом в корпоративную сеть

Forefront TMG 2010

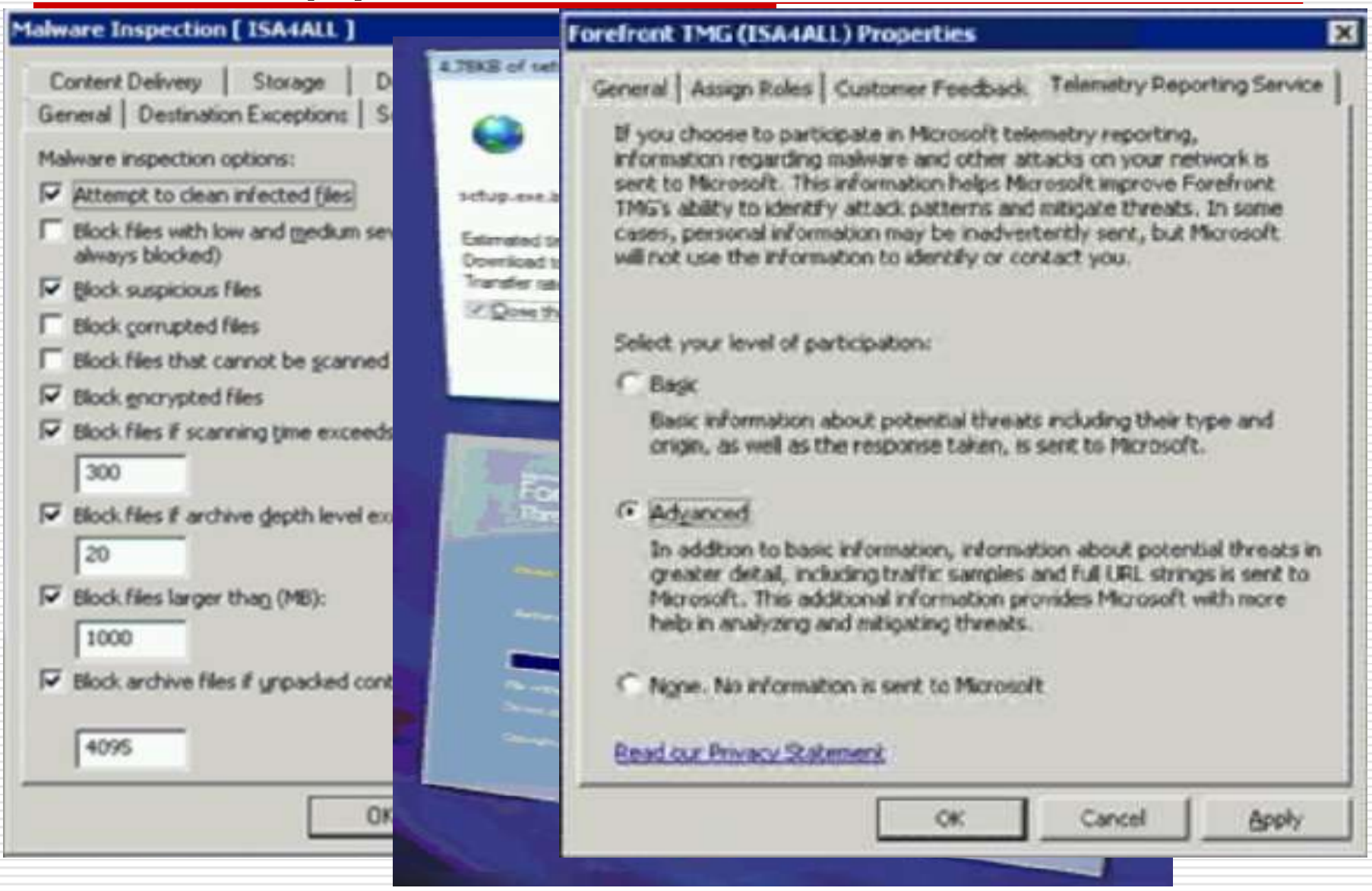
Безопасный доступ к Интернет

Инспектирование трафика на уровне приложений	• Контроль пользовательских приложений • Управление доступом к внешним ресурсам
Защита от вредоносного кода	• Встроенный модуль Web Anti-Malware • Динамические обновления движка и баз
Категоризация веб-ресурсов	• Контроль доступа на основе категорий URL Filtering
Проверка зашифрованного трафика	• Контроль SSL-трафика с помощью HTTPS Inspection
Поддержка работы с двумя интернет-каналами	• Отказоустойчивый доступ в Интернет - ISP Link Redundancy

Защита от вредоносного ПО в Forefront TMG 2010

- Два модуля защиты Web Protection Services (WPS)
  - Enchanced Malware Protection (EMP) – антивирус
  - URL Filtering (URLF) – фильтрация URL
- Лицензируется по подписке на обновления отдельно от основной лицензии TMG
  - Trial 120 дней, после этого перестает обновляться
- Модули работают независимо друг от друга и могут включаться/выключаться раздельно
- Движок EMPE (Enchanced Malware Protection Engine)
  - Тот же, что в FCS, Windows Defender, One Care
  - “Многодвижковости” антивируса в TMG НЕТ

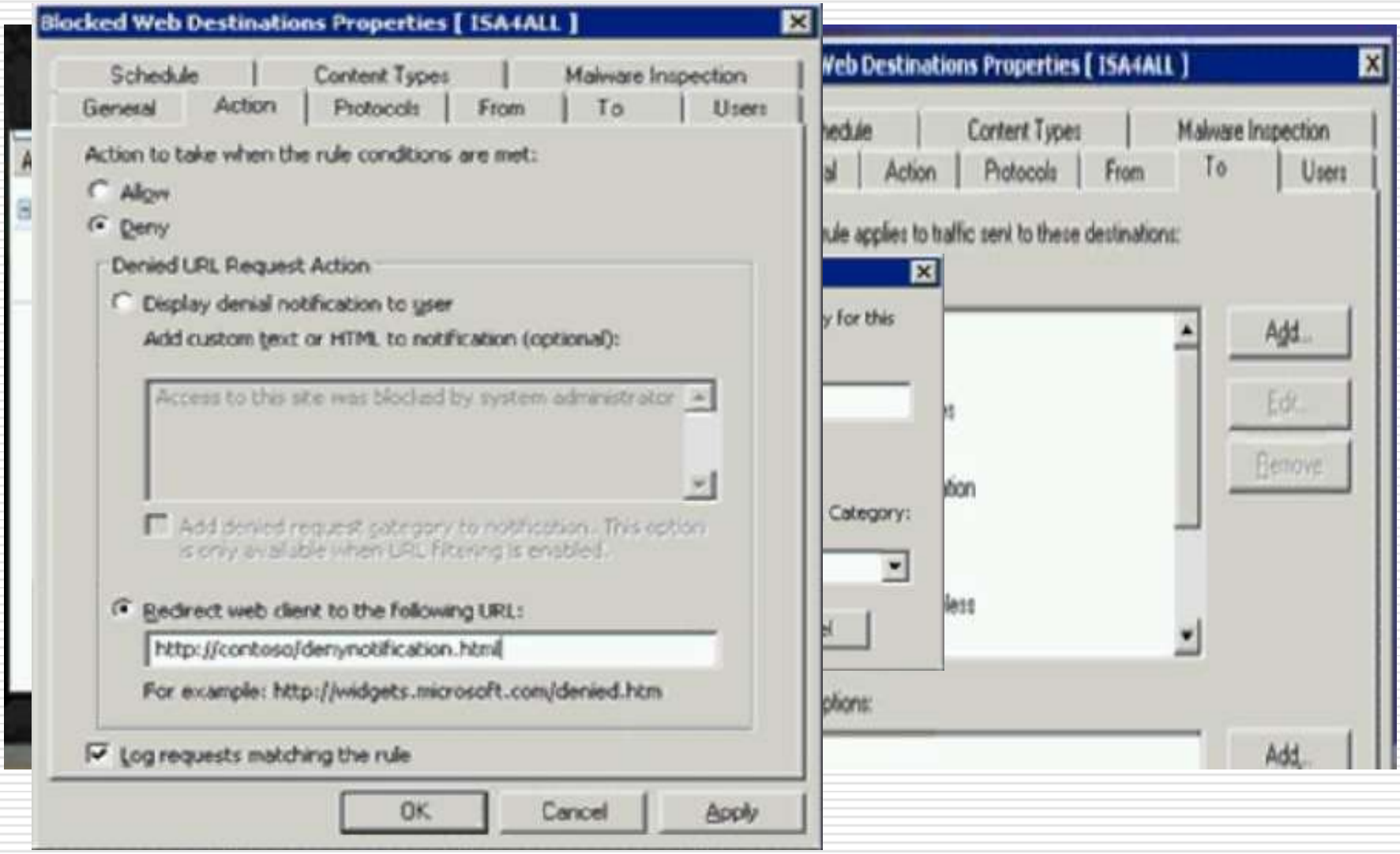
Антивирус в Forefront TMG 2010



URL-фильтрация Forefront TMG 2010

- Категории реализованы как объекты TMG и могут использоваться в правилах
- Для вычисления категории используются репутационные данные
  - БД URL на стороне TMG не существует
  - Microsoft Reputation Service “в облаке”
  - Опосредованно используются БД сторонних вендоров - Marshal 8e6, BrightCloud, iFilter и др.
  - Результаты репутационных запросов кэшируются на TMG с TTL, в результате до 96% запросов обрабатываются локально (без запроса в “облако”)
- Категории URL можно переопределять как локально, так и отправлять запрос в MRS

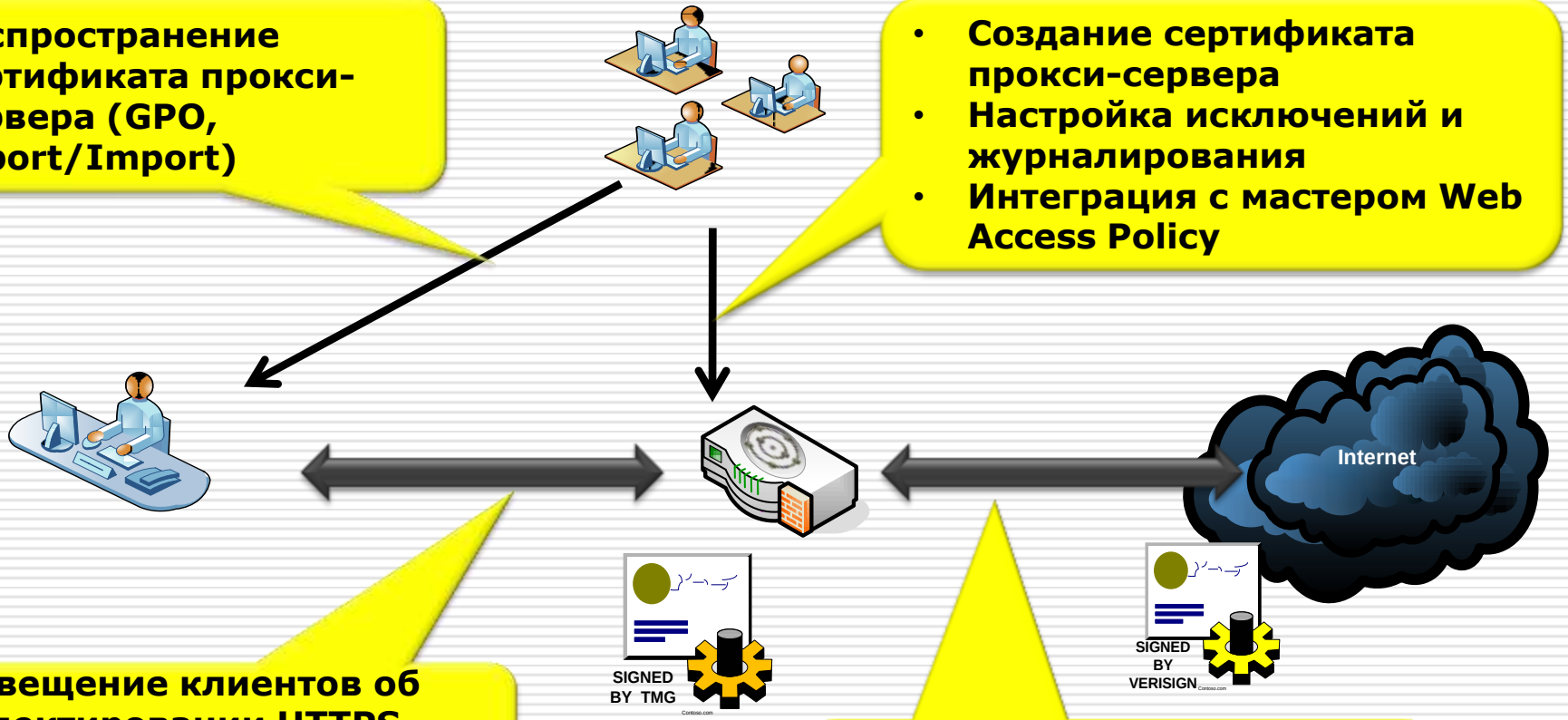
URL-фильтрация Forefront TMG 2010



Проверка зашифрованного трафика

Распространение сертификата прокси-сервера (GPO, Export/Import)

- **Создание сертификата прокси-сервера**
- **Настройка исключений и журналирования**
- **Интеграция с мастером Web Access Policy**

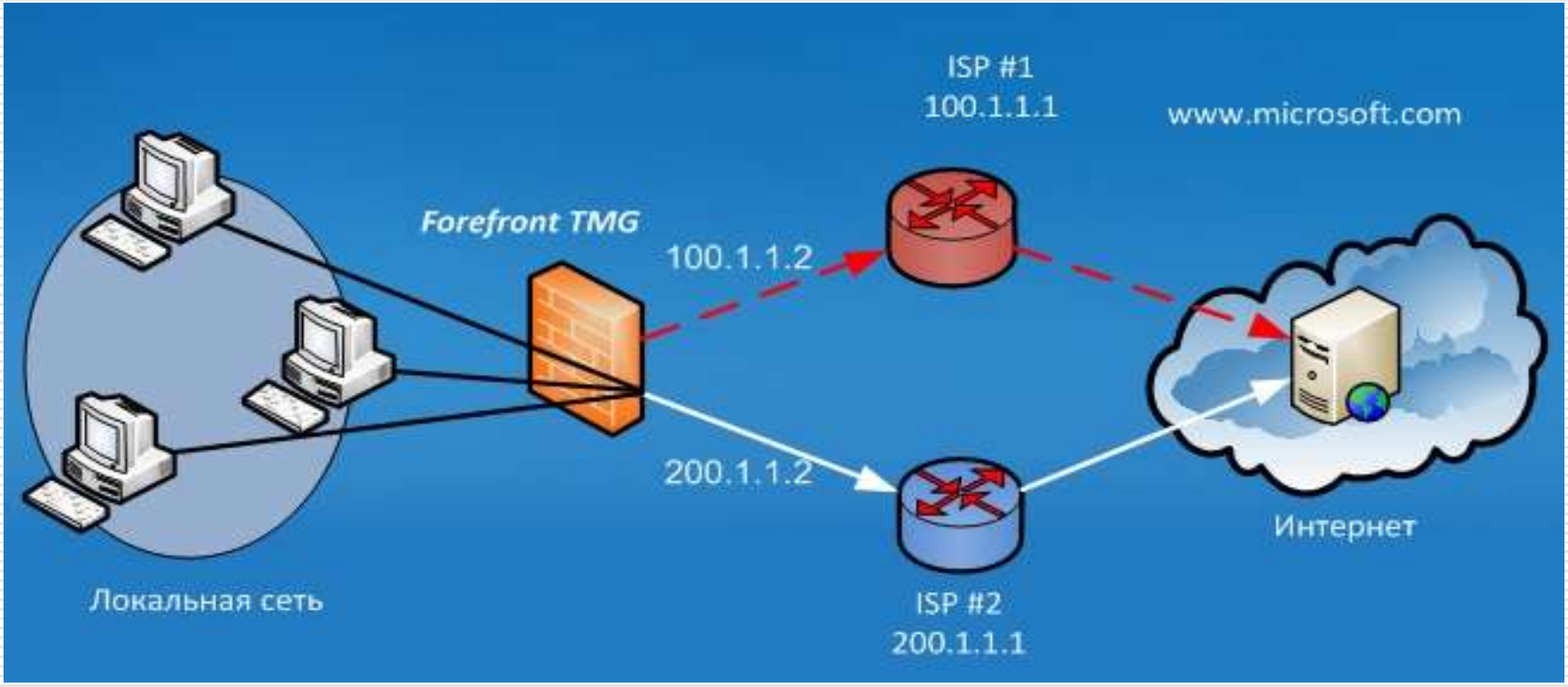


Оповещение клиентов об инспектировании HTTPS-соединений (via Firewall Client)

Проверка сертификата веб-сервера: срок действия, доверие, отзыв

Отказоустойчивый доступ к Интернет

- Два режима работы
  - Failover Mode (горячее резервирование)
  - Load Balancing Mode (балансировка нагрузки)



Защита периметра сети

Система предотвращения сетевых вторжений	• Network Inspection System (NIS)
Защита почтового трафика	• E-Mail Policy (EMP)
Расширенные возможности маршрутизации	• Enhanced NAT (ENAT)
Контроль трафика IP-телефонии	• SIP, VoIP

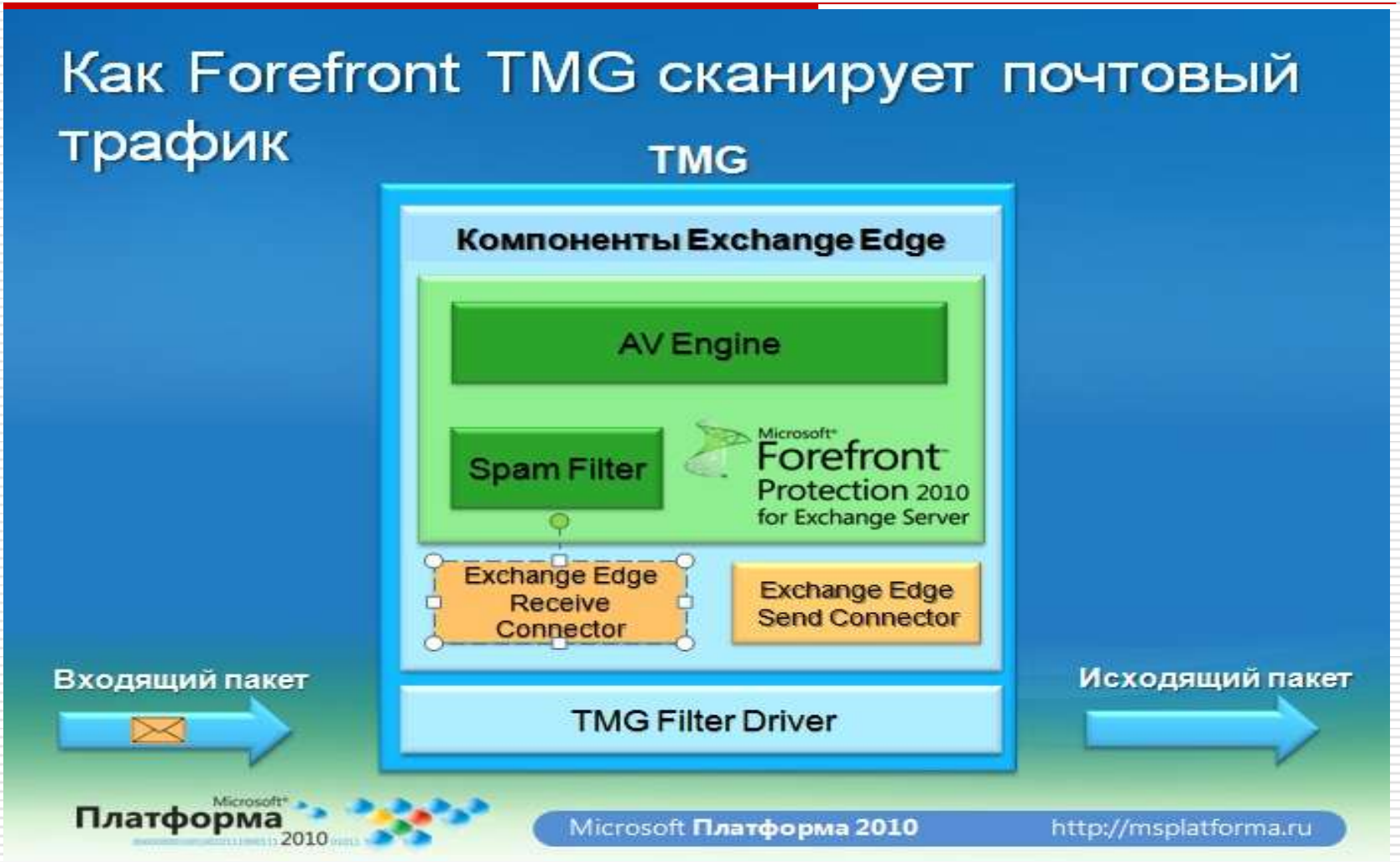
- Обнаруживает и предотвращает сетевые атаки, использующие определенные **уязвимости**
- Закрывает окно с момента обнаружения уязвимости до установки заплатки, возможно управление применением конкретной сигнатуры

Защита почтового трафика

SMTP Relay	• Безопасный SMTP-ретранслятор • Управление из консоли TMG
Интеграция с ролью Exchange Edge Transport Server	• Маршрутизация сообщений согласно правилам Exchange • Edge Subscription, EdgeSync
Интеграция с Forefront Security for Exchange	• Антивирус/антиспам/антифишинг
Любой SMTP-сервера (не Exchange)	• Теоретически (на практике используется редко)

- Роль ET обычно размещается вне производственного домена
- Если нужна авторизация в домене, использовать LDAP, а не Windows Integrated аутентификацию

TMG 2010. Интеграция с Exchange и FPE



Удаленный доступ

Публикация приложений	• Exchange Server (OWA, Outlook Anywhere, ActiveSync, EWS) • Sharepoint (WSS, MOSS), Dynamic CRM
VPN-сервер	• PPTP • L2TP/IPSec
SSL VPN	• SSTP
Построение сетей VPN	• Site-to-Site VPN (PPTP, L2TP, IPSec)

Контактная информация

195197, Санкт-Петербург,
Полюстровский пр., дом 59, литер Э
тел. 812 325-8400 факс : 812 320-5686

127018, Москва, Сущевский Вал ул., 16,
строение 3, офис 12
тел. 495 660-3291 факс : 495 660-3293

Антон Миносьян

aminosjan@polikom.ru