

Обзор продукта Microsoft Forefront TMG 2010

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

ПОЛИКОМ ПРФ

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)
 - Enhanced 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 отдельно
- Движок EMPE (Enhanced Malware Protection Engine)
 - Тот же, что в FCS, Windows Defender, One Care
 - “Многодвигковости” антивируса в TMG **НЕТ**

Антивирус в Forefront TMG 2010

The image shows two overlapping dialog boxes from the Microsoft Forefront TMG 2010 configuration interface. The background window is titled "Malware Inspection [ISA4ALL]" and has tabs for "Content Delivery", "Storage", and "Destination Exceptions". The "Malware inspection options:" section contains several checked checkboxes: "Attempt to clean infected files", "Block suspicious files", "Block encrypted files", "Block files if scanning time exceeds" (with a value of 300), "Block files if archive depth level exceeds" (with a value of 20), "Block files larger than (MB):" (with a value of 1000), and "Block archive files if unpacked content exceeds" (with a value of 4095). The foreground window is titled "Forefront TMG (ISA4ALL) Properties" and has tabs for "General", "Assign Roles", "Customer Feedback", and "Telemetry Reporting Service". The "General" tab is active, showing a Microsoft privacy notice about telemetry reporting. It offers three participation levels: "Basic" (selected), "Advanced", and "None". A link to "Read our Privacy Statement" is provided at the bottom. Both windows have "OK", "Cancel", and "Apply" buttons.

Malware Inspection [ISA4ALL]

Content Delivery | Storage | Destination Exceptions

General | Destination Exceptions | Storage

Malware inspection options:

- Attempt to clean infected files
- Block files with low and medium severity (always blocked)
- Block suspicious files
- Block corrupted files
- Block files that cannot be scanned
- Block encrypted files
- Block files if scanning time exceeds:
- Block files if archive depth level exceeds:
- Block files larger than (MB):
- Block archive files if unpacked content exceeds:

Forefront TMG (ISA4ALL) Properties

General | Assign Roles | Customer Feedback | Telemetry Reporting Service

If you choose to participate in Microsoft telemetry reporting, information regarding malware and other attacks on your network is sent to Microsoft. This information helps Microsoft improve Forefront TMG's ability to identify attack patterns and mitigate threats. In some cases, personal information may be inadvertently sent, but Microsoft will not use the information to identify or contact you.

Select your level of participation:

- Basic
Basic information about potential threats including their type and origin, as well as the response taken, is sent to Microsoft.
- Advanced**
In addition to basic information, information about potential threats in greater detail, including traffic samples and full URL strings is sent to Microsoft. This additional information provides Microsoft with more help in analyzing and mitigating threats.
- None. No information is sent to Microsoft.

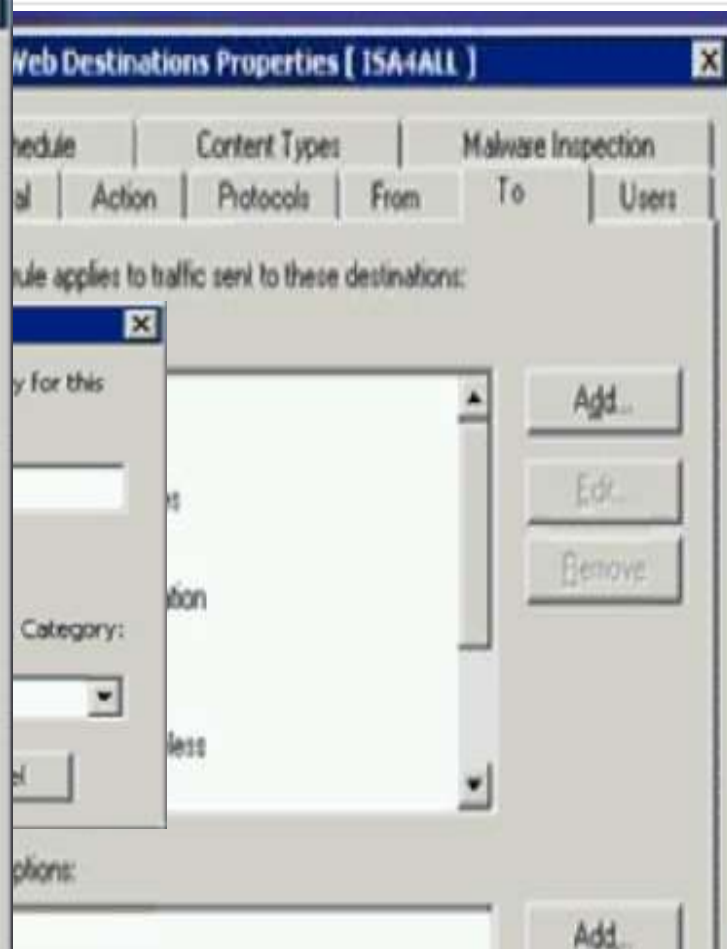
[Read our Privacy Statement](#)

OK Cancel Apply

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 8eб, 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

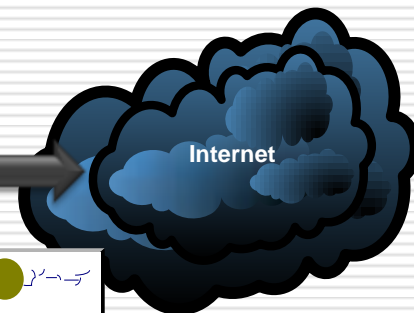
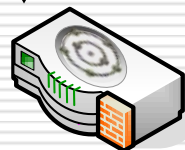
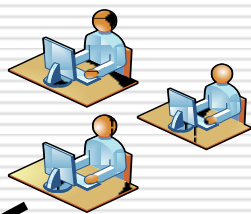
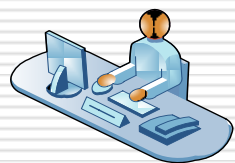
URL-филтрация Forefront TMG 2010



Проверка зашифрованного трафика

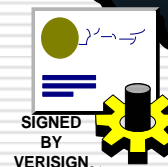
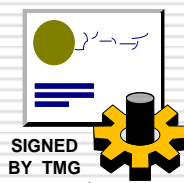
Распространение сертификата прокси-сервера (GPO, Export/Import)

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



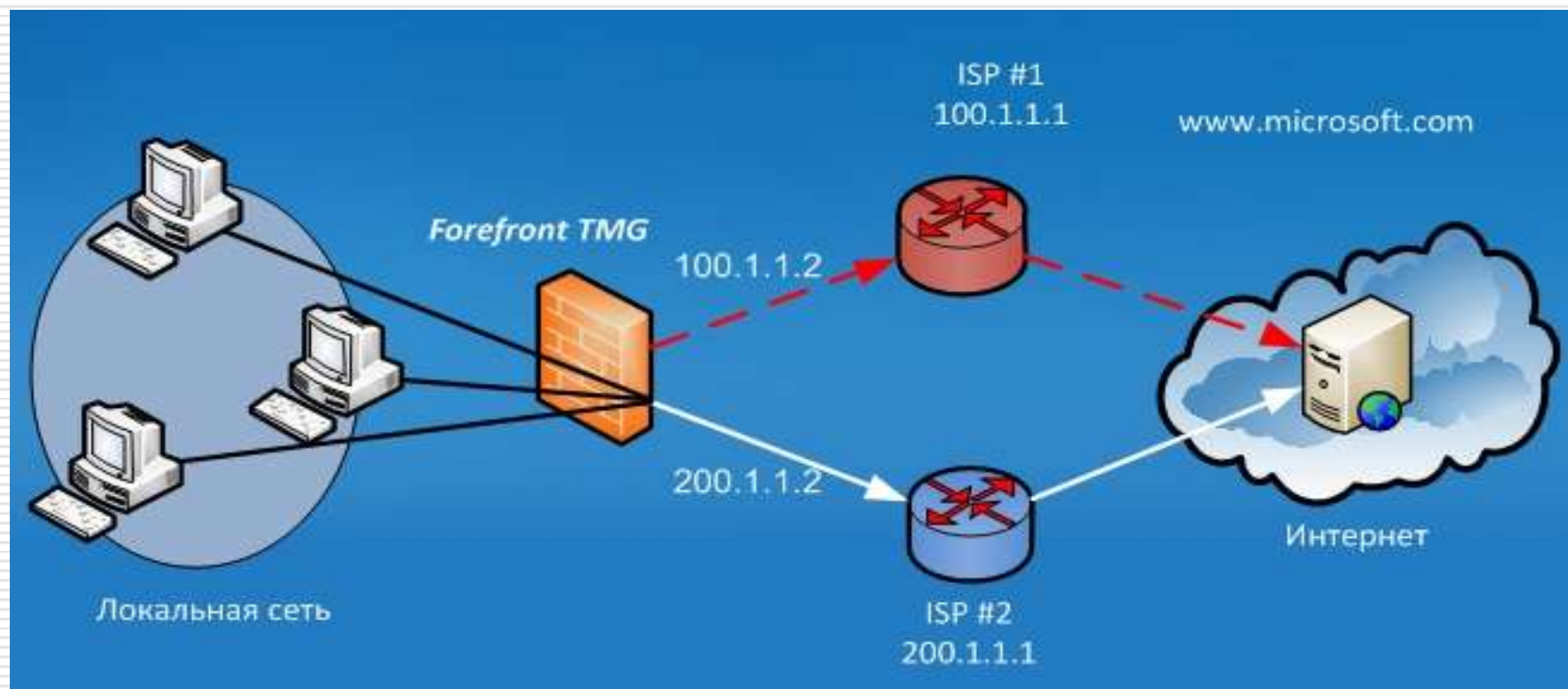
Оповещение клиентов об инспектировании HTTPS-соединений (via Firewall Client)

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

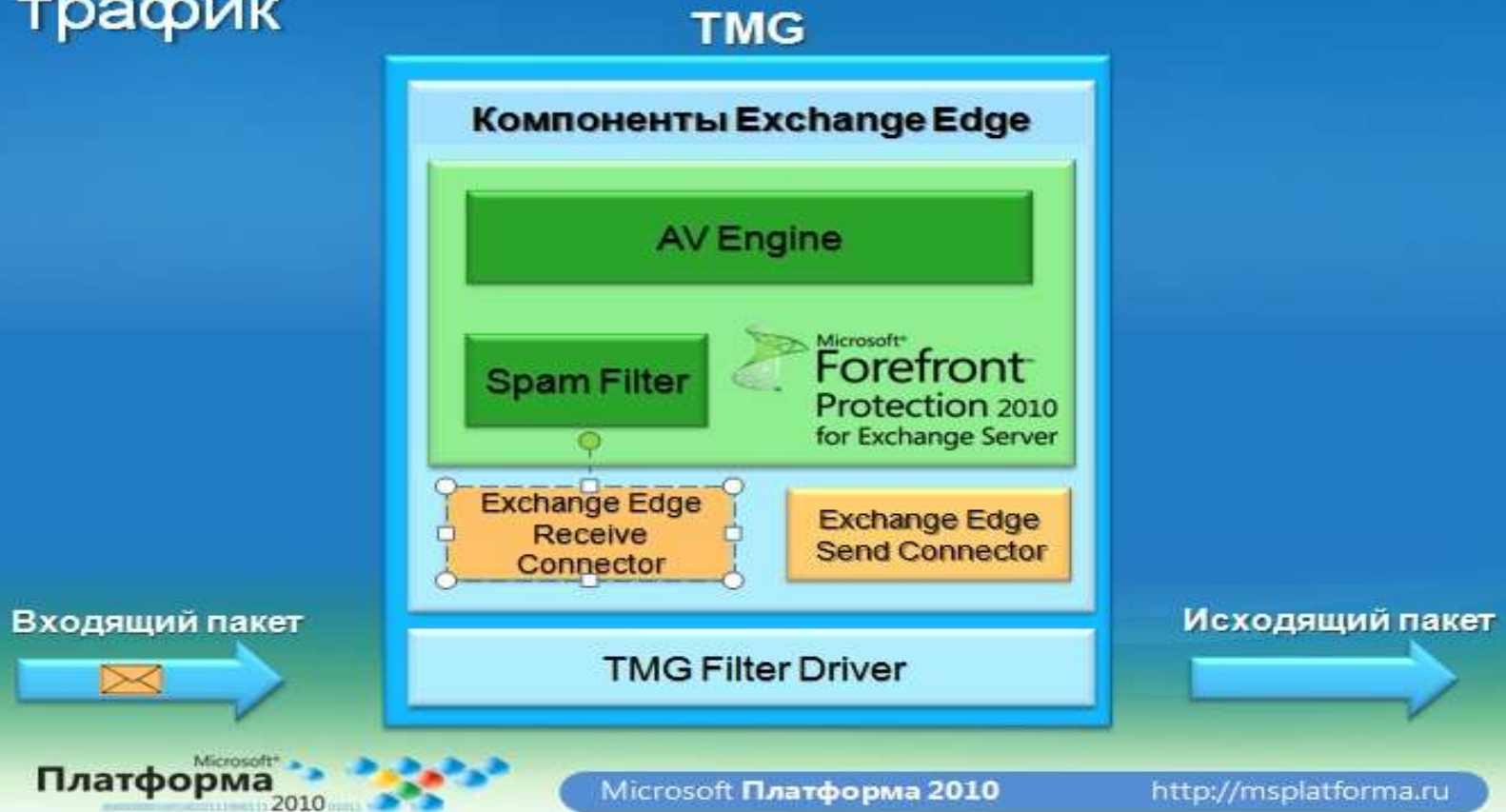
Любой SMTP-сервера (не Exchange)

- 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

Как Forefront TMG сканирует почтовый трафик



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