
Эшелон
комплексная безопасность
infosecurity
RUSSIA

Эшелон
комплексная безопасность

infosecurity RUSSIA

Концепция построения безопасной сети нового поколения

Грибов Максим

Заместитель директора департамента проектов
«ЗАО «НПО Эшелон»

Содержание

Тенденции рынка

Мобильность

В ближайшие три года на рынке появятся 1,3 миллиарда новых мобильных устройств

Использование рабочего места

Границы размываются:
Клиент - Работник
Потребитель - Партнер
Физический - Виртуальный

Видео

Изменение стиля работы. По прогнозам объем видео-трафика к 2014 году превысит текущий объем IP-трафика в 4 раза и составит 767 эксабайт

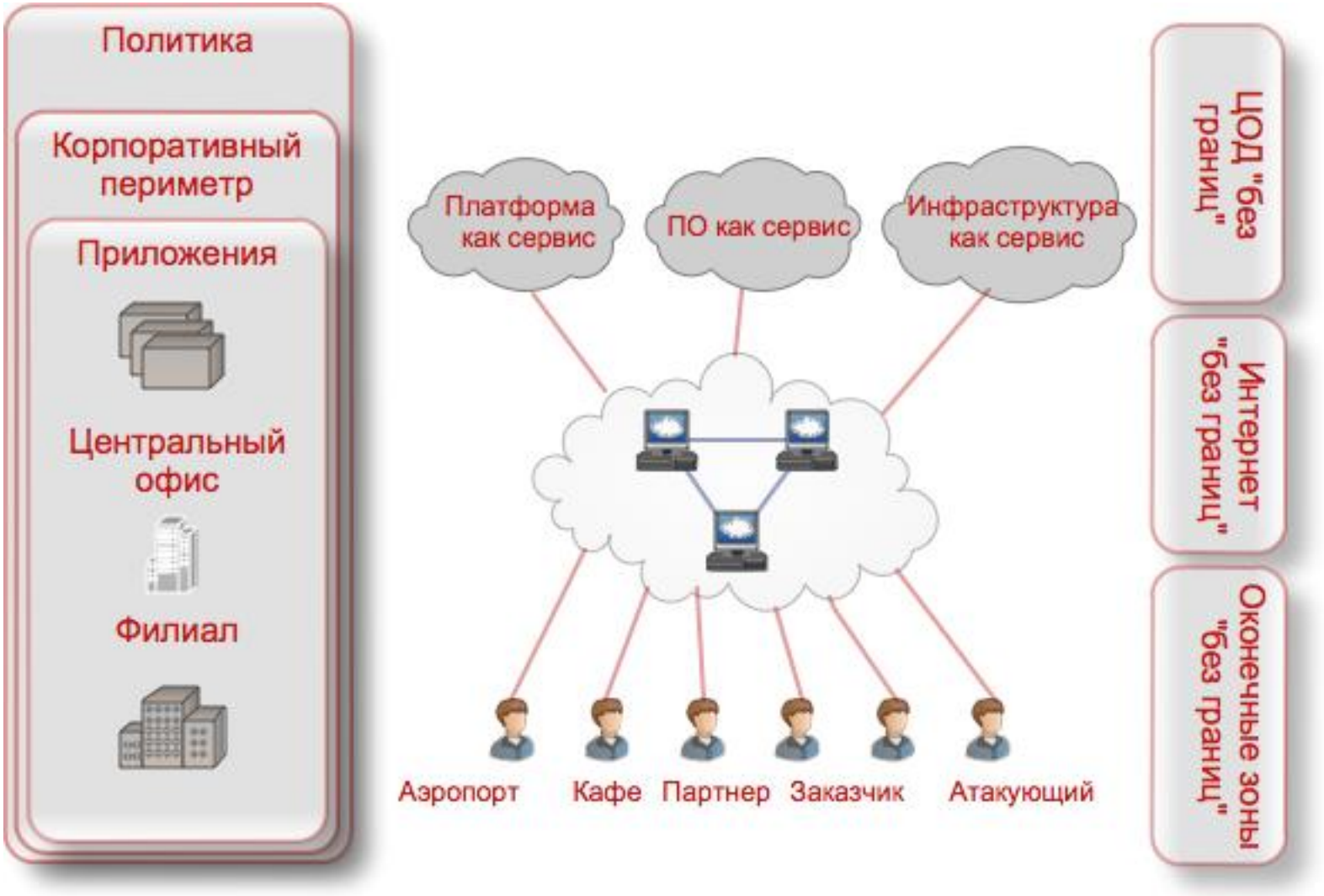
Основные предпосылки

1. Новые бизнес-модели
2. Новые задачи ИТ
3. Устранение границ объектов и снятие ограничений на используемые устройства
4. Обеспечение безопасного доступа из любой точки мира с любого устройства

«Сеть без границ» Cisco:
архитектура следующего поколения, изменяющая условия работы

«Сеть без границ» Cisco:
архитектура для обеспечения гибкой работы без границ

Архитектура системы безопасности «сети без границ»



Эшелон комплексная безопасность infosecurity RUSSIA

Создание зон подключения «без границ»

Контроль доступа к ресурсам

Контроль подключений

1. Разрашение/запрет доступа или карантин оконечных устройств в соответствии с их состоянием
2. Сегментация пользователей по доменам доверия локальной сети на основании идентификационной информации
3. Защита от кражи идентификационных данных на 2 уровне

Управление методом доступа

1. Поддержка систем обеспечения физической безопасности
2. Обнаружение точек беспроводного доступа злоумышленника, обеспечение надежной аутентификации и надежного шифрования в беспроводной сети
3.Управление подключениями к корпоративной сети по VPN удаленного доступа

Управление пользователями и приложениями

1. Обеспечение доступа к корпоративным ресурсам в соответствии с политиками
2. Обнаружение и контроль доли пропускной способности сети, используемой приложениями
3. Шифрование трафика управления, ведение журналов аудита в соответствии с нормативными требованиями

Работа в сети Интернет «без границ»

Отражение угроз на уровне филиала

Контроль периметра

1. Защита сети филиала и ее сегментация с помощью МСЭ
2. Глубокий анализ и управление трафиком, связанным с портом 80, обнаружение нарушений правил использования других протоколов
3. Защита доступа к приложениям, размещенным в распределенных сетевых сервисах

Предотвращение вторжений

1. Обнаружение и реакция на известные угрозы и совершенно новые угрозы
2. Корреляция угроз и динамическая реакция на угрозы
3. Снижение числа ложных срабатываний

Безопасность контента

1. Ограничение использования Интернет-ресурсов, фильтрация веб-сайтов в соответствии с их репутацией
2. Борьба с вредоносным программным обеспечением: вирусами, троянскими конями, и средствами проведения атак типа "фишинг"
3. Борьба со спамом

Создание ЦОД «без границ»

Защищенное подключение

Защищенная MPLS сеть

1.Поддержка масштабируемой ифраструктуры шифрования в MPLS сети
2. Выделенный уровень управления для поддержки аутсорсинга услуг
3. Доступ к закрытым распределенным сетевым сервисам в соответствии с политиками использования виртуальных ресурсов

VPN по Интернет

1. Масштабируемые и гибкие архитектуры
2. Защита сети и абонентских устройств от интернет-угроз
3. Автоматизация управления для поддержки самообслуживания удаленных объектов

Производительность приложений

1. Повышение производительности работы по глобальной сети
2. Повышение приоритета критически важного трафика для оптимизации производительности

Этапы развития «сети без границ»

Преимущества архитектуры

Для специалистов в сферах ИТ и безопасности:

- Упрощает распространение необходимых средств безопасности на системы современных сотрудников
- Увеличивает производительность, обеспечивая гибкость и свободу выбора для сотрудников
- Позволяет внедрять новые бизнес-модели, такие как модель «ПО как услуга» (SaaS), без ущерба для безопасности
- Помогает управлять рисками и обеспечивать соответствие нормативным требованиям

Для конечных пользователей:

- Предоставляет возможность выбора места и времени получения доступа к информации
- Позволяет выбирать используемые устройства для доступа к информации и выполнения работы
- Обеспечивает безопасность и постоянный доступ пользователей, позволяя им не беспокоится о подключении

Эшелон
комплексная безопасность

infosecurity RUSSIA

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте mail@npo-echelon.ru
или по телефону +7(495) 645-38-09


Эшелон
комплексная безопасность
infosecurity
RUSSIA