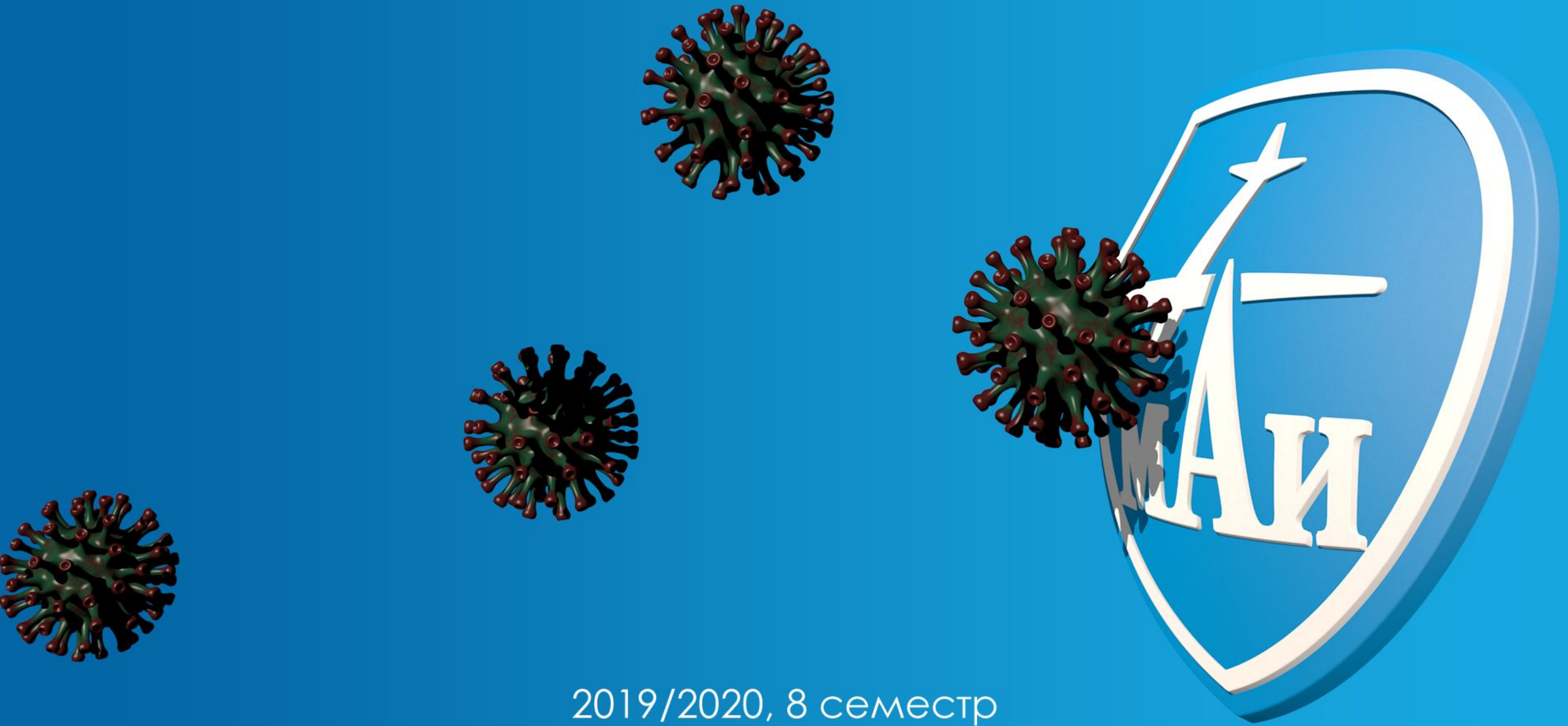
Вычислительные сети и Телекоммуникации

Безопасность компьютерных сетей



2019/2020, 8 семестр

Базовые принципы

- Информационная безопасность как вид управления рисками
- Уровень риска не может быть равен нулю
- Стоимость информации или ее утраты является критерием
- Доверие, его уровни и их (не)существование в XXI веке
- Необходимость учета человеческого фактора
- Безопасность сети как комплексная задача
- Модель Confidentiality-Integrity-Availability (CIA)
- «Бумажная» безопасность (политики, 152-ФЗ, …)

“There’s no device known to mankind that will prevent people from being idiots” Mark Rasch, CSC

Элементы модели безопасности

- Физическая безопасность
- Безопасность конечных систем
- Безопасность программного обеспечения
- Управление доступом пользователей
- Сетевая безопасность
- Управление и контроль

Виды сетевых атак

Пассивные:

- Прослушивание и сбор трафика
- Сканирование диапазонов IP
- Сканирование портов

Активные:

- Фишинг
- Переполнение буфера
- Атаки веб-приложений: XSS, CSRF, SQL-инъекции
- Подмена DNS
- Man-in-the-middle (MITM)
- Подмена IP, ARP, VLAN hopping
- Атаки на полосу
- Вирусные пандемии

Эволюция целей взлома

- Proof of Concept, развлечение (70е – середина 80х)
- DoS, повреждение файлов (середина 80х – конец 90х)
- Удаленное управление, создание ботнетов (2000 – н.в.)
- Рассылка спама и DDoS-атаки (2000 – н.в.)
- Вымогательство (2005 – н.в.)
- Шифрование файлов (2010 – н.в.)
- Майнинг (2015 – н.в.)
- Кибервоенные операции (2011 - ∞)
- Internet of Things (IoT) (2015 – н.в.)

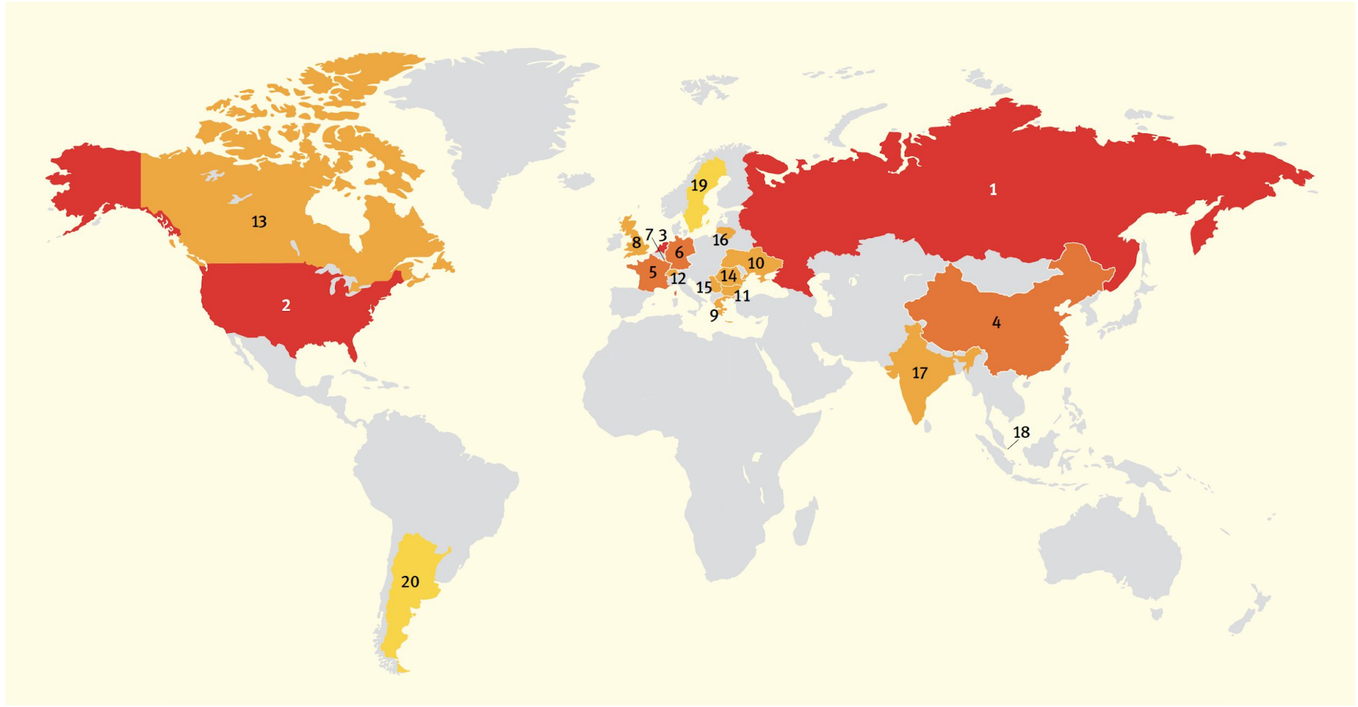
Количество компьютеров в ботнетах по странам

The 10 Worst Botnet Countries

As of 15 April 2020 the world's worst botnet infected countries are:

1	India	Number of Bots: 1542560
2	China	Number of Bots: 1490600
3	Iran (Islamic Republic of)	Number of Bots: 884772
4	Viet Nam	Number of Bots: 808327
5	Brazil	Number of Bots: 687762
6	Egypt	Number of Bots: 479783
7	Thailand	Number of Bots: 472978
8	Algeria	Number of Bots: 422771
9	United States of America	Number of Bots: 411854
10	Turkey	Number of Bots: 388823

Количество управляющих серверов ботнетов по странам



Rank	Botnet C&Cs	Country	% change
1	4,712	Russia	+143%
2	4,007	United States	+76%
3	1,441	Netherlands	+33%
4	770	China	+390%
5	691	France	+97%
6	585	Germany	+28%
7	423	Luxembourg	—
8	401	Great Britain	+31%
9	314	Greece	—
10	300	Ukraine	+13%
11	274	Bulgaria	+57%
12	256	Switzerland	+1,119%
13	245	Canada	+5%
14	243	Romania	+63%
15	157	Serbia	—
16	117	Lithuania	–34%
17	114	India	—
18	97	Singapore	–20%
19	96	Sweden	—
20	94	Argentina	—

Безопасность пользовательских систем

Описание опытной установки:

- Две виртуальные машины с Windows XP SP2 и Windows 7 SP1
- Обновления не установлены и отключены
- Firewall отключен
- Пользователь с простым паролем
- Включен протокол SMB/CIFS
- Публичные IP-адреса, на которых ранее никогда ничего не было
- Трафик контролируется системой обнаружения атак Snort3

Сколько времени они проживут и как будет выглядеть процесс их гибели?

Направления борьбы

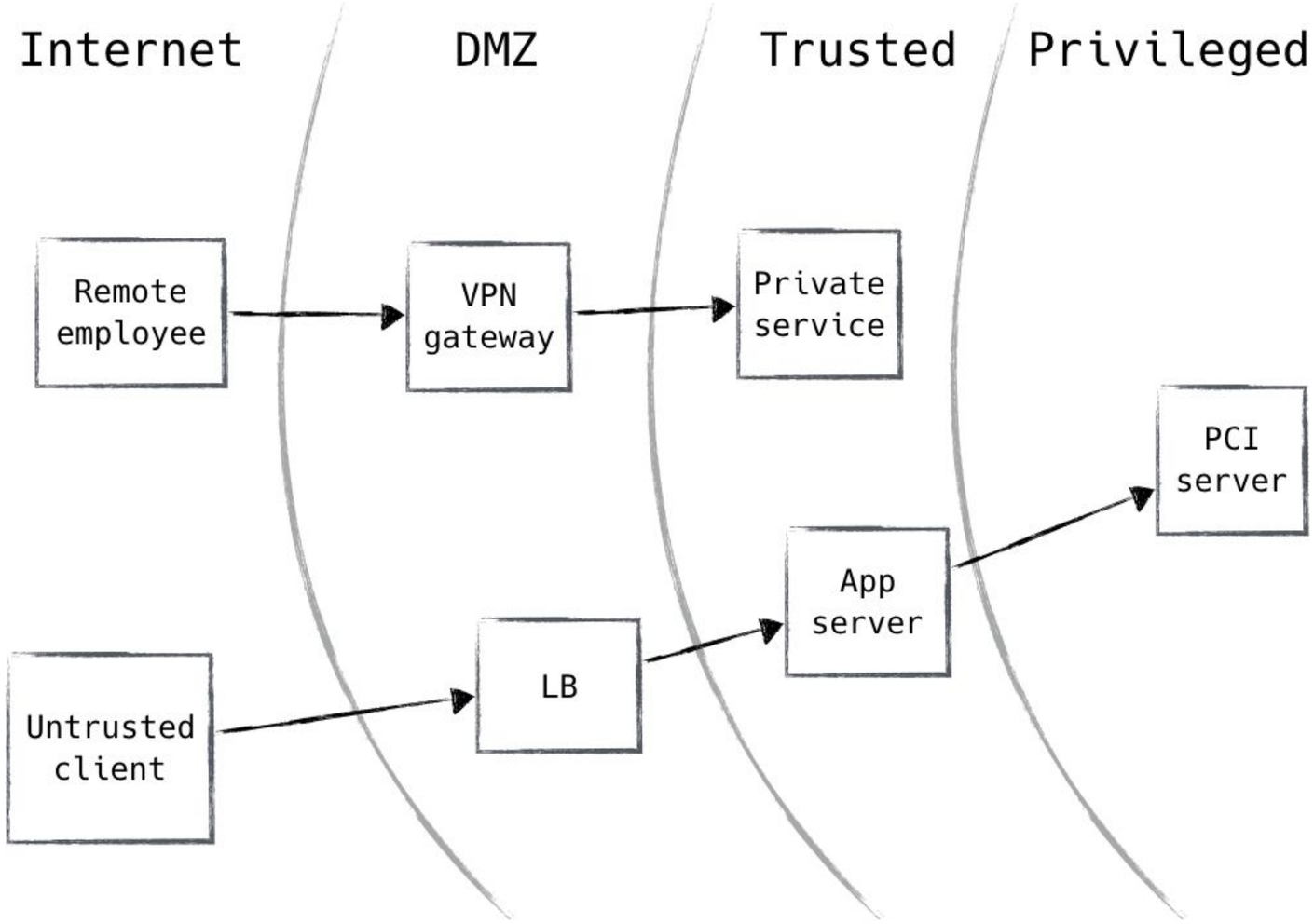
Со стороны конечных устройств:

- Обучение пользователей
- Физическая безопасность устройств и сети
- Внедрение ограничений на основе политик
- Автоматическая установка обновлений
- Антивирусная защита

Со стороны сети:

- Использование межсетевых экранов (Firewall)
- Использование систем обнаружения и предупреждения атак (NIDS, NIPS)
- Контроль и ограничение контента

Традиционная модель сетевой безопасности на основе зон доверия



Традиционная архитектура сетевой безопасности на основе зон доверия

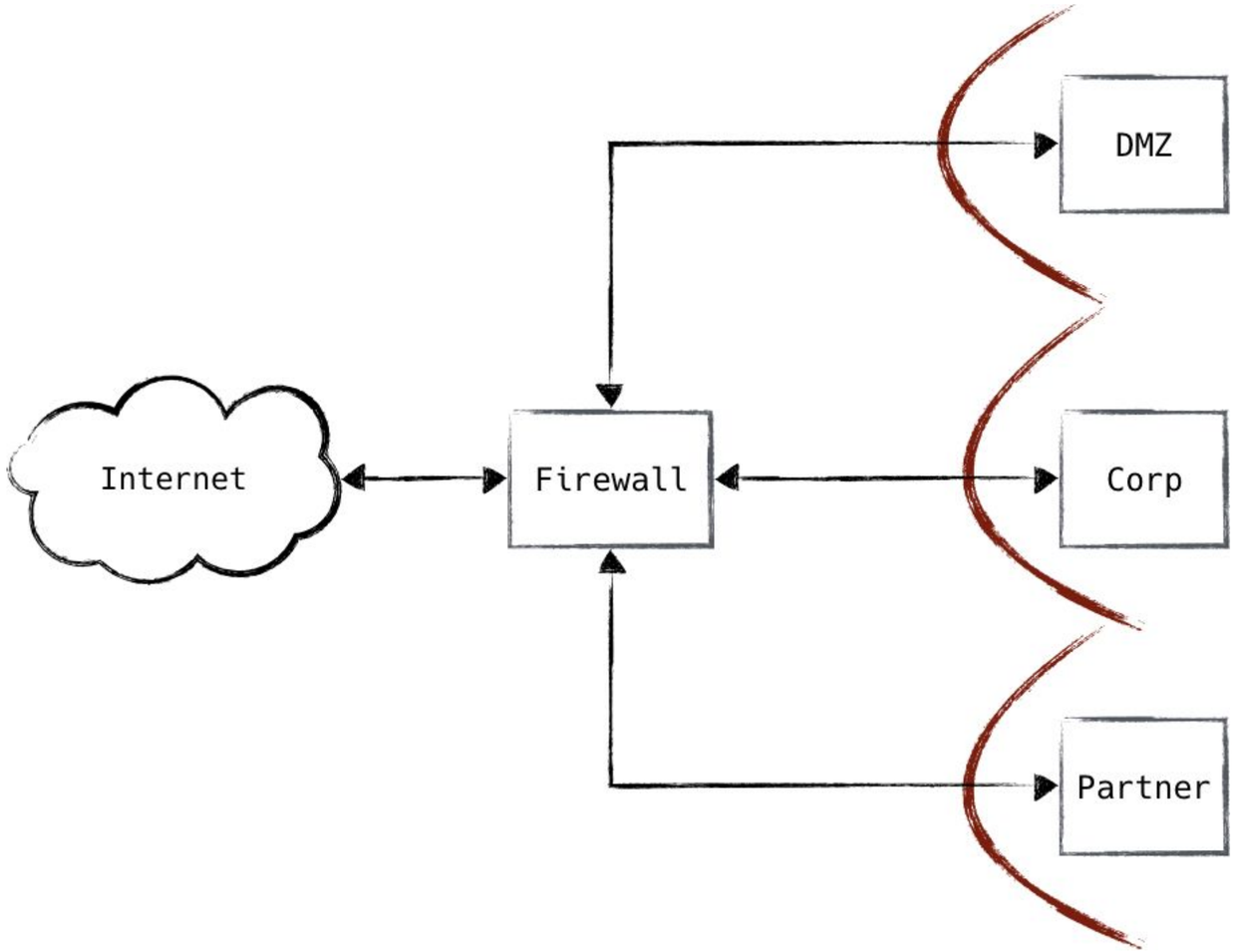
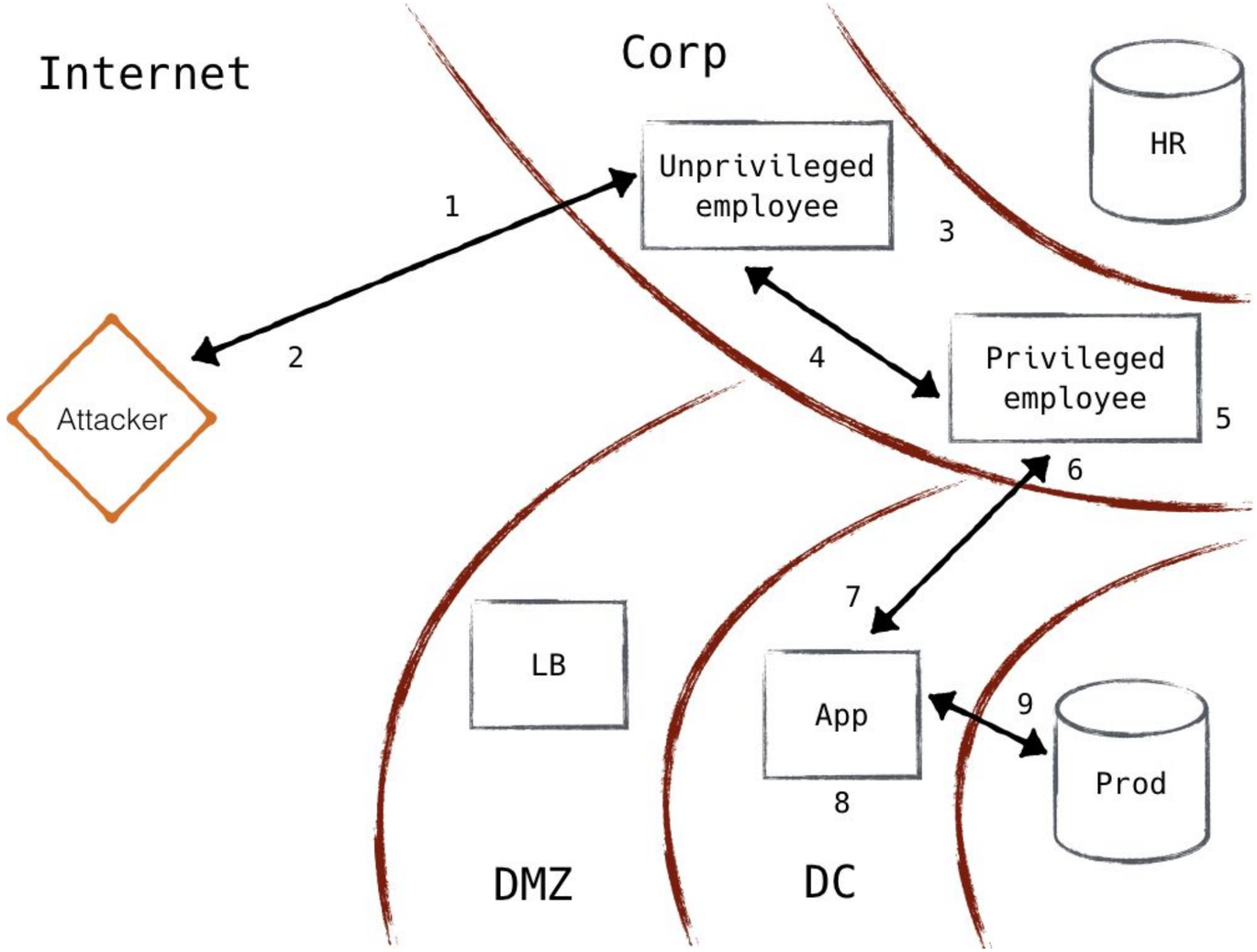


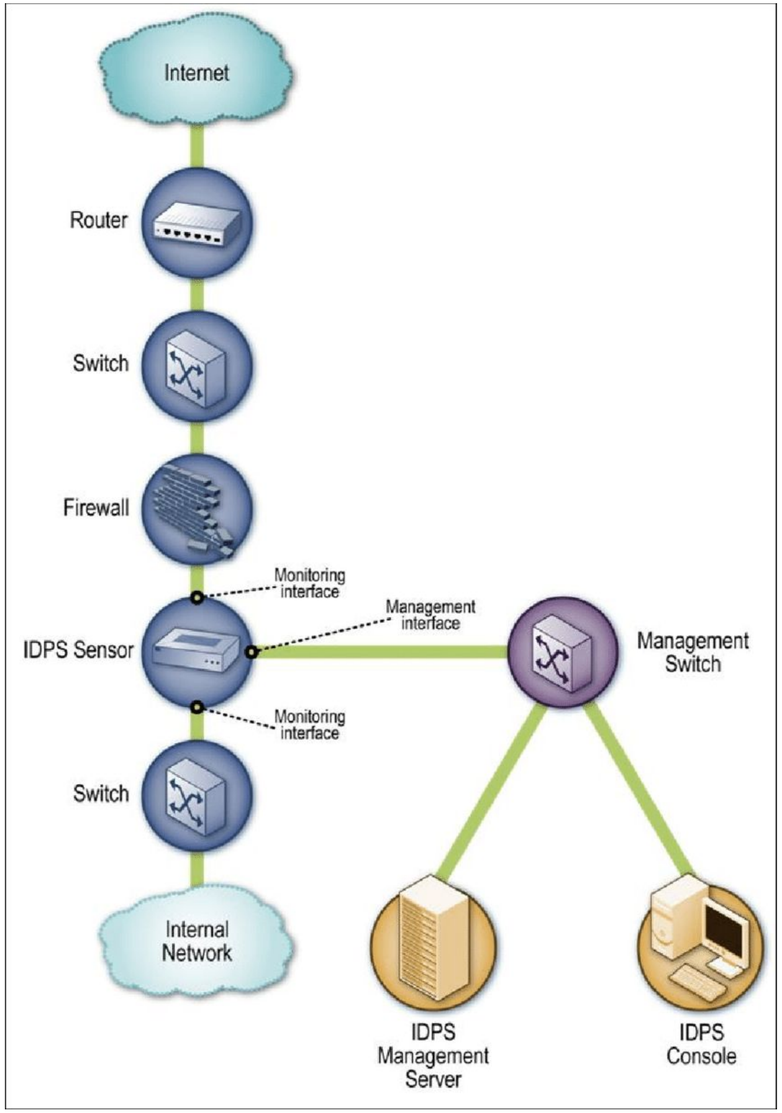
Схема взлома архитектуры сетевой безопасности на основе зон доверия



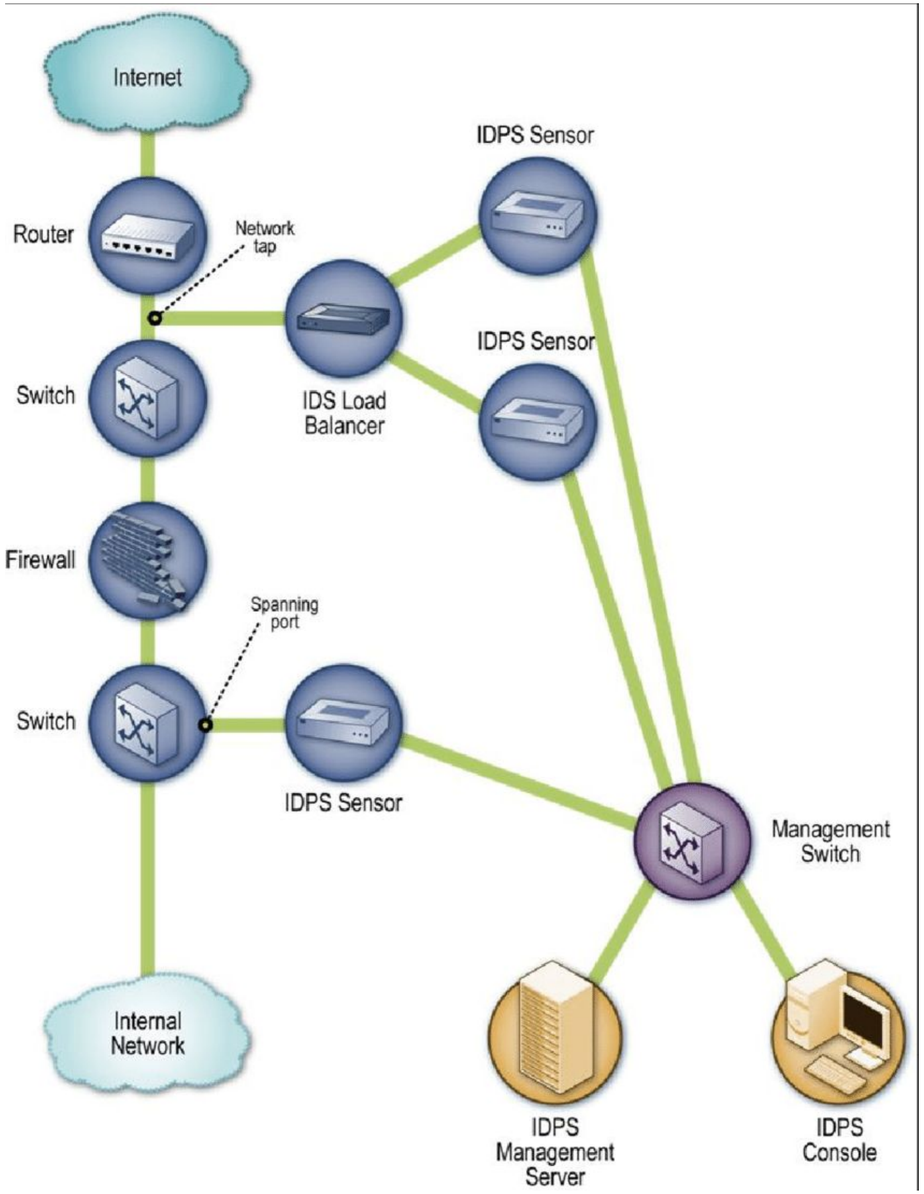
Недостатки традиционной архитектуры

- Трафик в пределах зоны не контролируется
- Доступ в соседнюю зону на основе IP-адресов и портов
- Плохо адаптируется к концепции BYD и мобильности
- Слабо применима в облачных системах и виртуализации
- Слабая поддержка L4-L7 инспекции
- Внедрение IDS представляет непростую задачу
- Не учитывает возможность атаки изнутри периметра

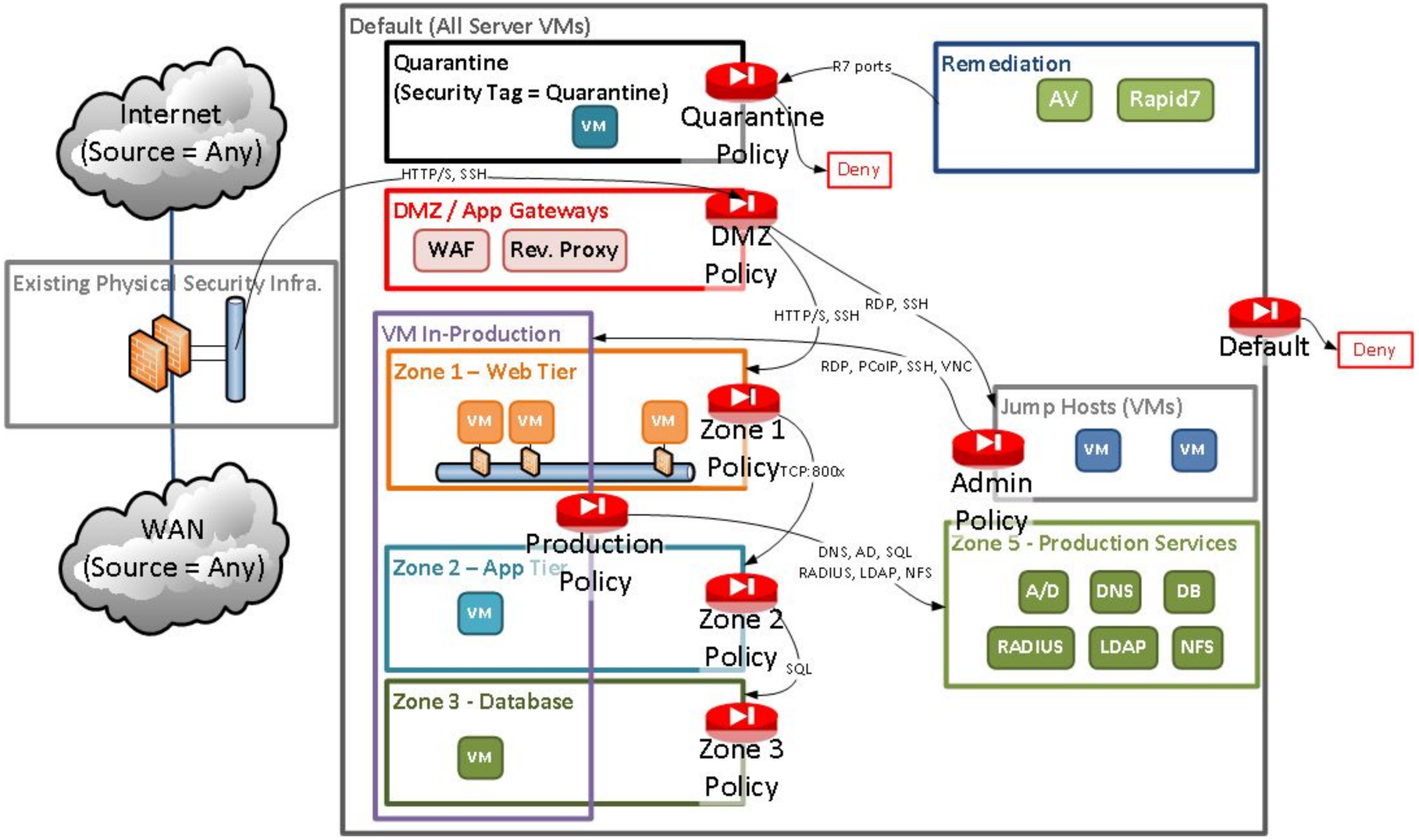
Системы обнаружения и предупреждения атак (NIDS, NIPS)



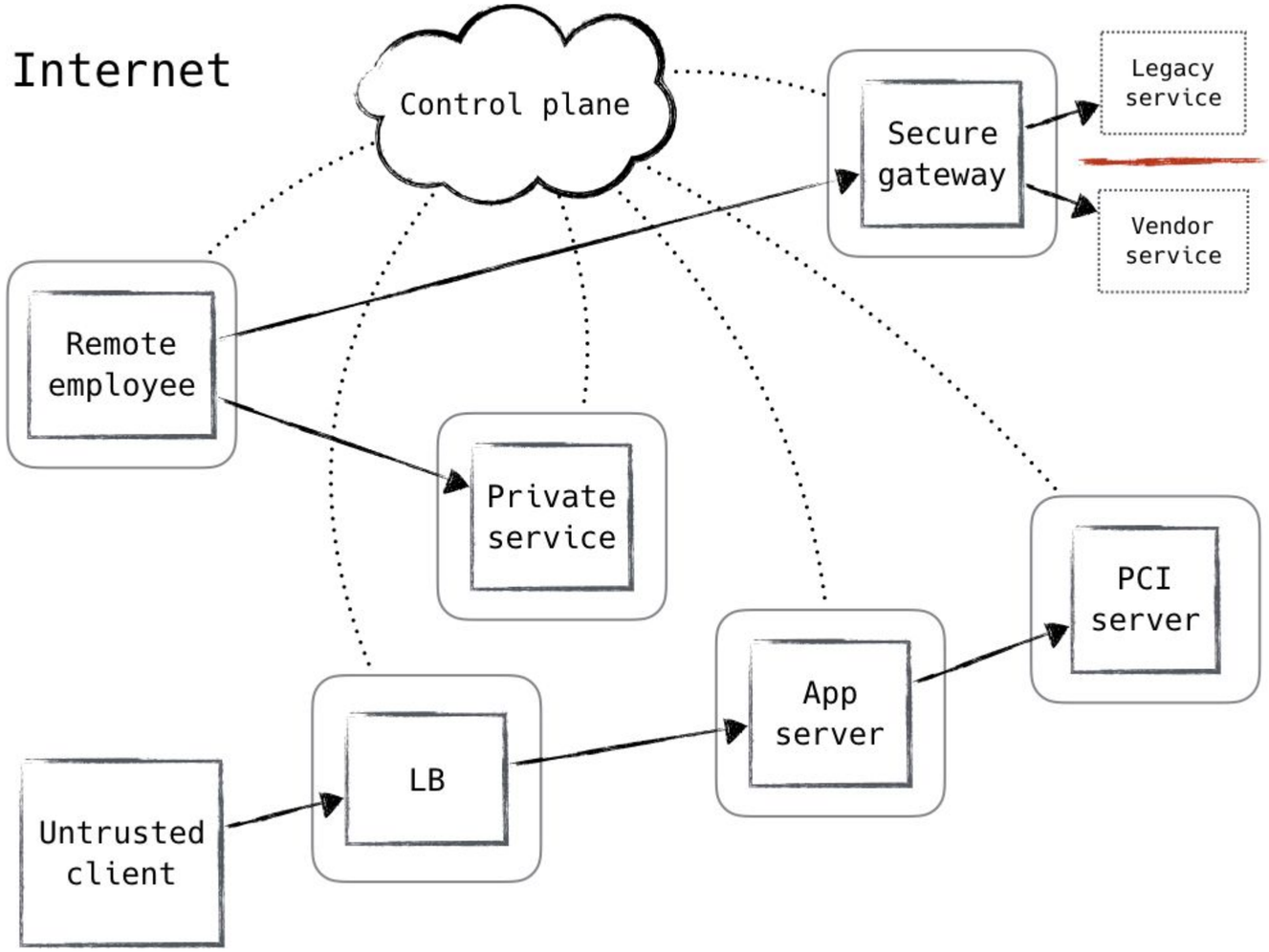
Системы обнаружения и предупреждения атак (NIDS, NIPS)



Архитектура сетевой безопасности с нулевым уровнем доверия



Архитектура сетевой безопасности с нулевым уровнем доверия



Достоинства и недостатки модели Zero Trust

- Хорошо подходит для облачных архитектур и SDN
- Доступ определяется политикой безопасности
- Весь трафик подлежит обязательной инспекции
- Хорошая поддержка уровней L4-L7
- Отсутствие единой точки отказа
- Необходимы значительные вычислительные мощности
- Для внедрения необходимо изменение архитектуры сети

Практические рекомендации

- Проверь свой (и не только) пароль - https://haveibeenpwned.com/
- Смени его на нормальный
- Включи и установи обновления, firewall и антивирус
- Делай резервные копии
- Выключи IPv6 :)
- Включи обратно (и не отключай) SELinux!
- Не доверяй данным, полученным из сети. Никогда!
- Любая сеть опасна. Wi-Fi опасен вдвойне. Открытый Wi-Fi – средоточие зла
- Bluetooth – изобретение диавола, выключи его
- Выключи JavaScript в браузере
- Выключи cookies
- Научись делать шапочку из фольги