positive technologies

РУКОВОДСТВО ПО ПЕРЕДАЧЕ СЕТЕВОГО ТРАФИКА В PT NAD

ОТВЕТИТ НА ВОПРОСЫ

КАКИЕ

сегменты сети могут быть в инфраструктуре предприятия?

из них следует анализировать в первую очередь?

точки захвата трафика существуют и как устроена схема зеркалирования?

Определение сегментов сети в инфраструктуре

Разделение сети на сегменты и разграничение доступа к ним удлиняют путь хакера к целевым активам

Рекомендуем делить сеть на следующие логические сегменты:

- **Серверный сегмент**
  (может быть иерархическим, со своим ядром и уровнем доступа, или состоять из нескольких равнозначных коммутаторов)
- **Демилитаризованная зона**
  (ДМЗ)
- **Глобальная компьютерная сеть** –
  WAN (включая пограничные маршрутизаторы для доступа к интернету)
- **Сегмент удаленного доступа**
  (remote access VPN, site-to-site VPN)
- **Пользовательский сегмент**
  (состоит из ядра, уровня распределения и уровня доступа, а также Wi-Fi-сети для сотрудников)

В зависимости от размера сети одни сегменты могут входить в другие. Например, устройства для терминирования удаленного доступа могут быть в сегменте WAN.

Приоритизация сегментов для анализа трафика

В первую очередь рекомендуем анализировать сетевой трафик серверного сегмента, ДМЗ, входящий и исходящий интернет-трафик. Такой выбор неслучаен: по оценке Positive Technologies [1], атакующие чаще всего проникают в сеть через ДМЗ, а серверный сегмент используют для реализации недопустимых событий.

Ниже приведены приоритетные сегменты сети и те активности, которые PT NAD обнаруживает при зеркалировании трафика с них.

Сегменты первого приоритета

Серверный сегмент

(включая контроллеры домена и целевые системы)

- Эксплойты (например, Zerologon)
- Атака DCSync
- Разведка в домене (BloodHound, AdFind)
- Перебор учетных записей или паролей
- Атака Kerberoasting
- Активность злоумышленников и ВПО (по DNS-запросам)
- DNS-туннели
- Повышение привилегий и перемещение внутри периметра (по протоколам SSH, RDP, VNC, SMB, DCE, RPC)
- Атаки Relay (NTLM Relay, PetitPotam и прочие)
- Атаки на целевые серверы

Сегмент ДМЗ

- Эксплуатация уязвимостей на периметре (включая 0-day)
- Закрепление на периметре (реверс-шелл, фреймворки для постэксплуатации)
- Перебор паролей (брутфорс)
- Другие активности, связанные с закреплением и перемещением злоумышленников внутри периметра

Исходящий интернет-трафик

- Активность вредоносного ПО
- Активность хакерских инструментов (в том числе тоннели)
- Агенты фреймворков постэксплуатации
- Эксфильтрация данных (выгрузка злоумышленником данных на внешние ресурсы)

Сегменты второго приоритета

VPN

- Вся активность злоумышленников, их исходящий и локальный трафик.

Пользовательский сегмент

- Перемещение между хостами пользователей
- Атаки на некоторые целевые системы (АРМ бухгалтеров и первых лиц компании)

Wi-Fi

- Вся активность злоумышленников, их исходящий и локальный трафик

Таблица показывает, какие атаки останутся незамеченными, если не контролировать потоки данных из того или иного сегмента сети.

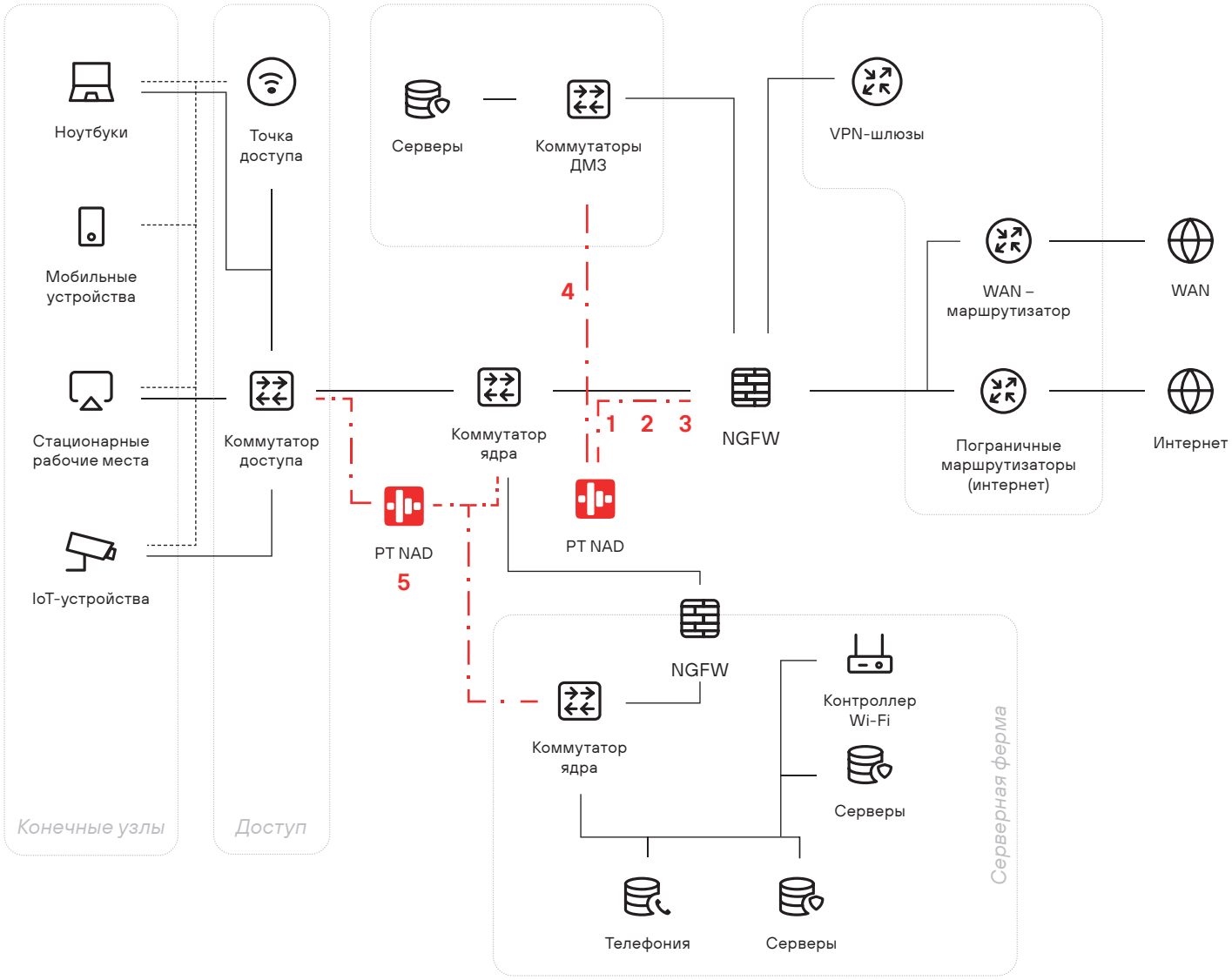
Полезные ссылки

Как обнаружить 10 популярных техник пентестеров [1]

Телеграм-чат о PT NAD

Дополнительные материалы о PT NAD

Схема зеркалирования трафика
на периметре и внутри сети



- Точки захвата копии трафика
- **1** Захват расшифрованного трафика VPN-шлюза
- **2** WAN - трафик
- **3** Трафик с пограничных маршрутизаторов (интернет)
- **4** Трафик ДМЗ
- **5** Трафик пользовательского сегмента и ЦОД

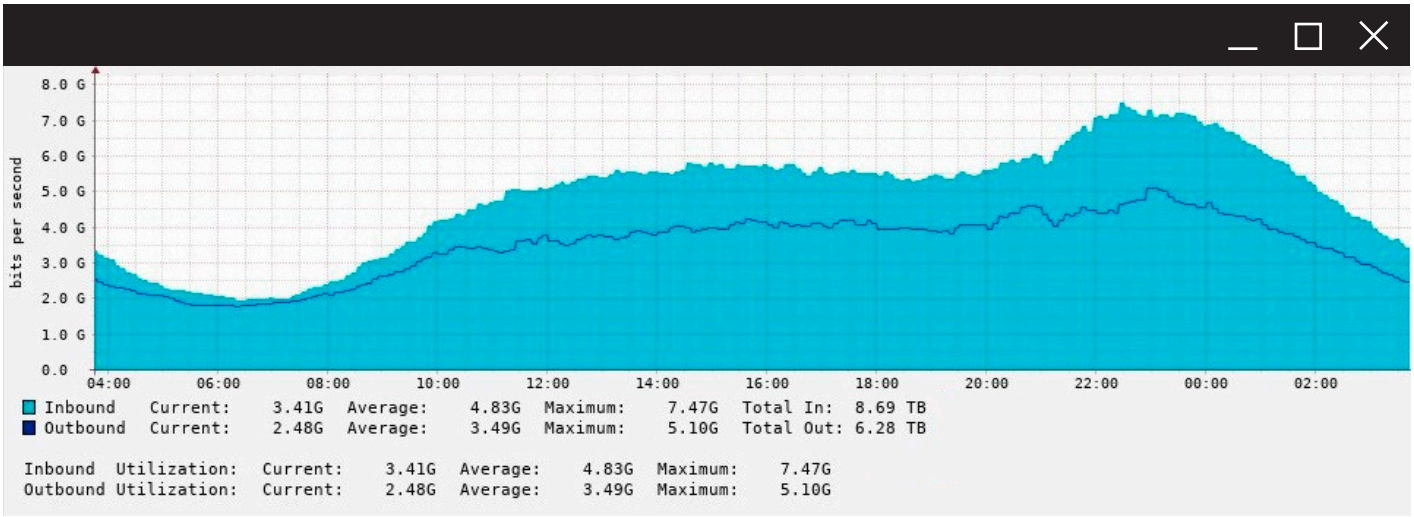
- Трафик можно захватывать с помощью SPAN или TAP-устройств с брокерами. Для захвата трафика со скоростью 10 Гбит/с рекомендуем использовать сетевые брокеры и несколько инсталляций PT NAD (например, для внешнего и внутреннего трафика, как изображено на схеме)
- Захватывайте трафик до трансляции сетевых адресов (NAT), чтобы видеть исходные IP-адреса
- Если трафик расшифровывается на одном из устройств (например, VPN-концентраторе или NGFW), зеркалировать нужно уже расшифрованные данные

Как оценить объем трафика в вашей сети

После того, как вы определили сетевые сегменты, которые хотели бы анализировать и перечень сетевых портов коммутатора, через которые передается трафик этих сегментов, необходимо оценить объем сетевого трафика. Это необходимо для расчета правильной конфигурации сервера. Оценить объем трафика на интерфейсе на коммутаторах Cisco можно при помощи команды show int:

```
ptdemo-switch1# show int Ethernet1/25| inc 'bits/sec'
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 4827831456 bits/sec, 6034756
  packets/sec
```

За последние 30 секунд средний трафик составил порядка 4,8 Гбит/с, но одно это число нельзя использовать для объективной оценки среднего объема трафика и величины дневных пиков. Для более точной оценки необходимо регулярно замерять число переданных байт через интерфейс на протяжении недели из-за существования дневной периодичности и локальных всплесков трафика, например, из-за бекапирования. Такой мониторинг удобно сделать при помощи систем Zabbix или Cacti, которые будут регулярно собирать статистику с одного или нескольких интерфейсов по SNMP.



Пример графика объемов зеркалированного трафика от системы мониторинга за день. Система показала, что пиковые дневные значения доходят до 12.6 Гбит/с

Пример настройки зеркалирования трафика

Зеркалирование сетевого трафика для анализа осуществляется двумя основными способами: SPAN и TAP. TAP больше подходит для работы на больших скоростях, но требует физического вмешательства в сеть (врезки TAP-устройств) и наличия специального сетевого брокера. Впрочем, сетевой брокер способен гибко фильтровать сетевые пакеты и легко вырезать ненужный трафик из анализа, например от систем резервного копирования или видеопотока систем ВКС. Зеркалирование при помощи SPAN может управляться ACL группами (пример), [2] если позволяет сетевое оборудование. Пример команды настройки зеркалирования Vlan или интерфейсов Eth1/10-12 на интерфейс Eth1/25 при помощи SPAN на примере Cisco Nexus 5548UP:

```
monitor session 1
  source vlan 101
  destination interface Ethernet1/25
  no shut
```

```
monitor session 1
  source interface Ethernet1/10 both
  source interface Ethernet1/11 both
  source interface Ethernet1/12 both
  destination interface Ethernet1/25
  no shut
```

После этих настроек весь трафик указанных сетевых портов или VLAN будет дублироваться в порт коммутатора Eth1/25. Проанализировать объем трафика можно как на каждом интерфейсе индивидуально, так и на зеркалированном интерфейсе Eth1/25 после его настройки.

[2]