ВИЗУАЛЬНЫЙ ГАЙД ДЛЯ НОВИЧКОВ

Один взломанный принтер не должен дать доступ ко всей базе данных.

FLAT NETWORK

Одна сеть. Без сегментации.

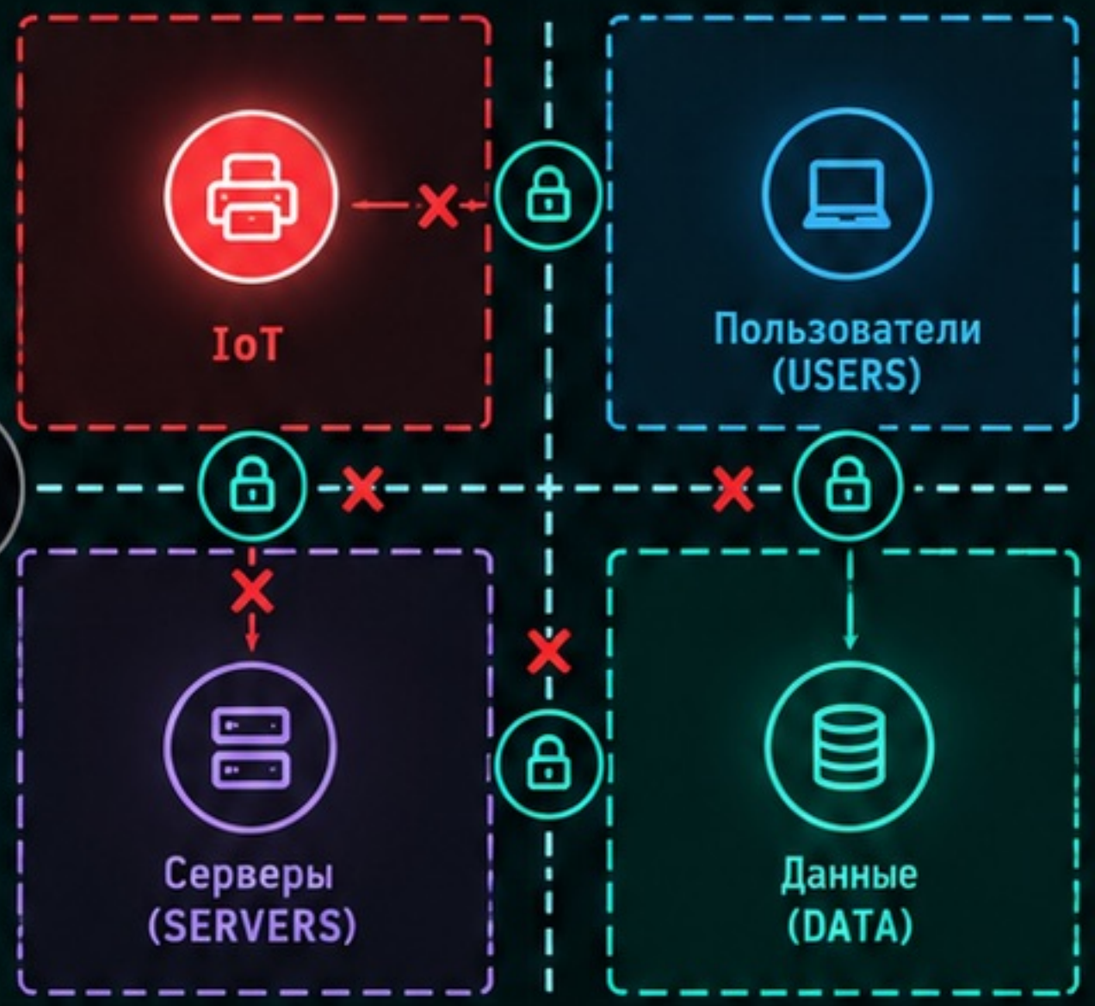


1 взлом → полный доступ ко всей сети

VS

SEGMENTED

Сеть разделена на зоны.



1 взлом → только одна зона

Сетевая сегментация простыми словами

@lioncoulbatyshchikov

Плоские сети — кошмар для безопасности.

В плоской сети каждое устройство может напрямую достичь любого другого устройства.

Удобно для IT. Идеально для атакующих.



1

скомпрометированное устройство

ВСЕ

устройства становятся доступными

0

внутренних барьеров (контролей)

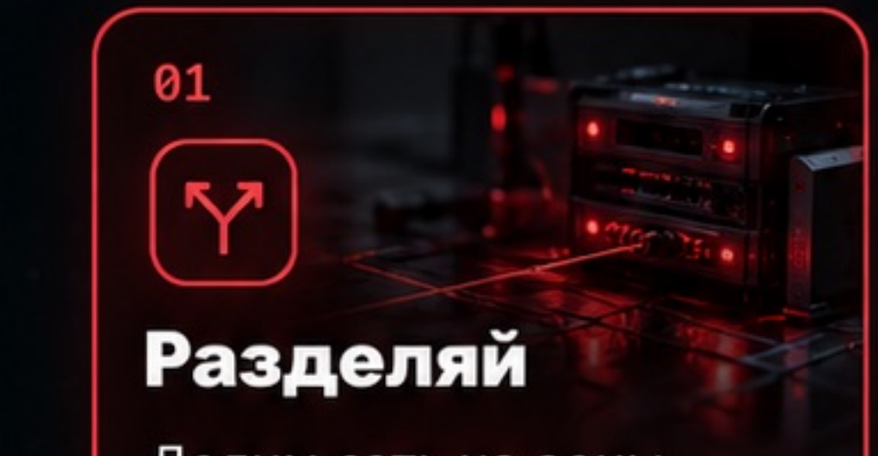
Большинство домашних и небольших офисных сетей по умолчанию **плоские:** один роутер, одна подсеть, никаких правил внутри.

Что такое сегментация?

Представьте сеть как корабль, разделённый на отдельные отсеки. Если один отсек затоплен, корабль **продолжает держаться на плаву.**



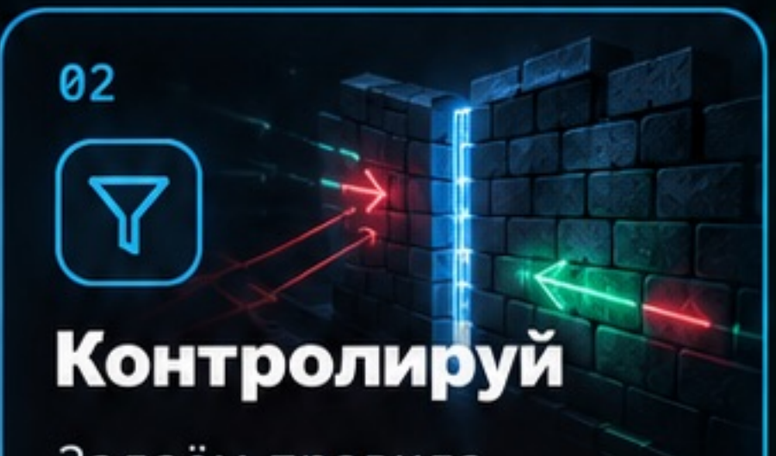
Сетевая сегментация — это разделение сети на более **маленькие, изолированные зоны** и точный контроль, какой трафик может между ними проходить.



01

Разделяй

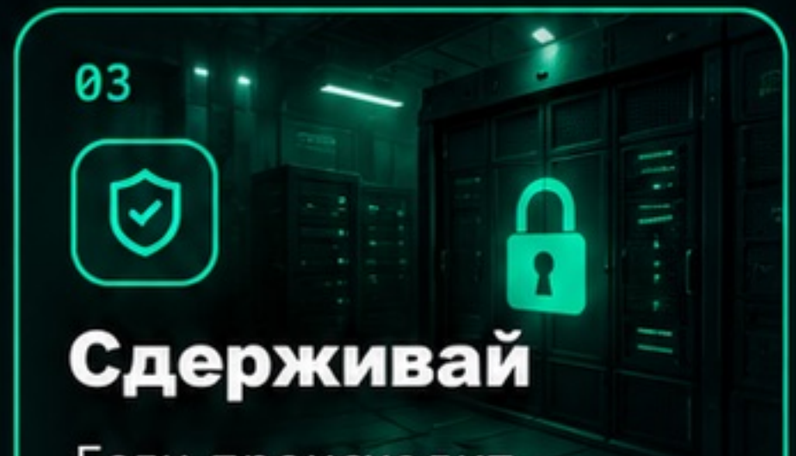
Делим сеть на зоны по уровню доверия (trust level).



02

Контролируй

Задаём правила на каждой границе между зонами (правила доступа).



03

Сдерживай

Если происходит взлом, он остаётся в одной зоне и не распространяется далее.

Почему это важно?

Сегментация не предотвращает первый взлом.
Она решает, **насколько далеко** сможет зайти атака.

SECURITY

Ограничивает последствия взлома

Если злоумышленник попал в одну зону, он остаётся только в ней, а не получает доступ ко всей сети.



DETECTION

Останавливает латеральное движение

Каждый переход между зонами проходит через контрольную точку (checkpoint), где его можно заблокировать и зафиксировать.



COMPLIANCE

Уменьшает область аудита

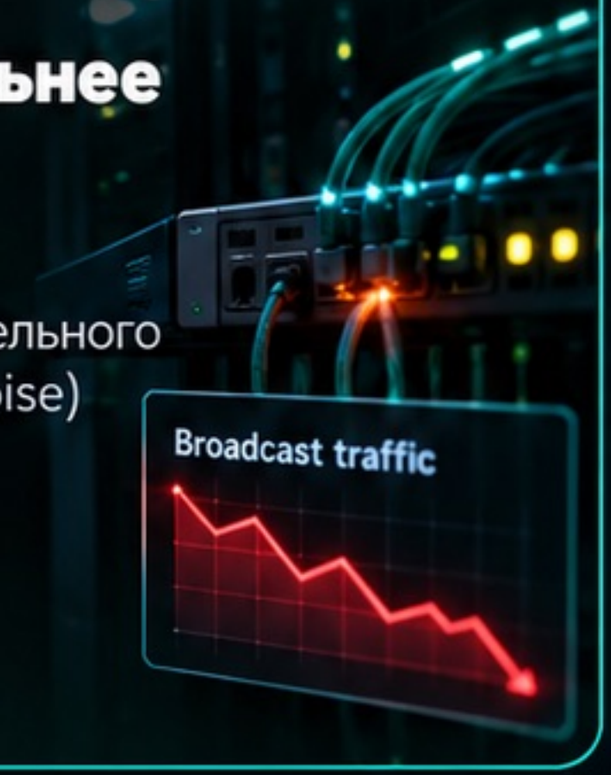
Можно изолировать платёжные системы, чувствительные данные и другие критичные разделы, чтобы аудит охватывал только несколько систем, а не всю компанию.



PERFORMANCE

Чище и стабильнее сеть

Меньшие зоны — меньше широковещательного трафика (broadcast noise) и проще поиск неисправностей в случае проблем.

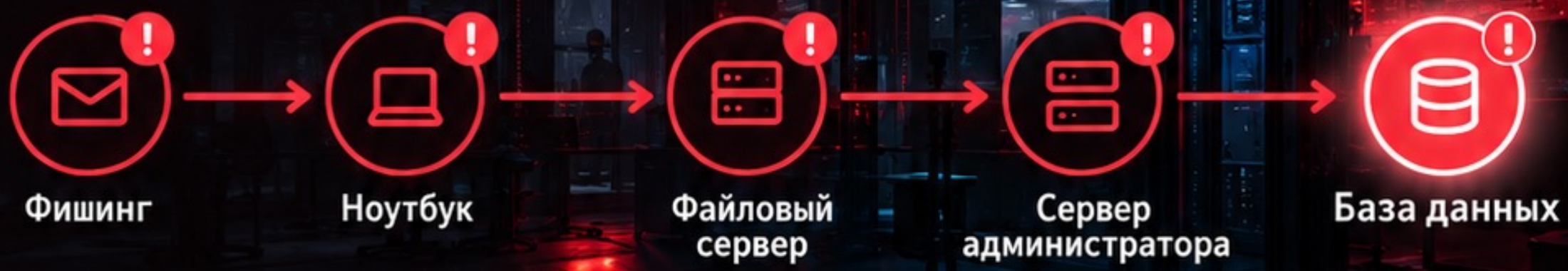


Сегментация не останавливает первый взлом.
Она определяет, **насколько серьёзными** будут его последствия.

Латеральное движение

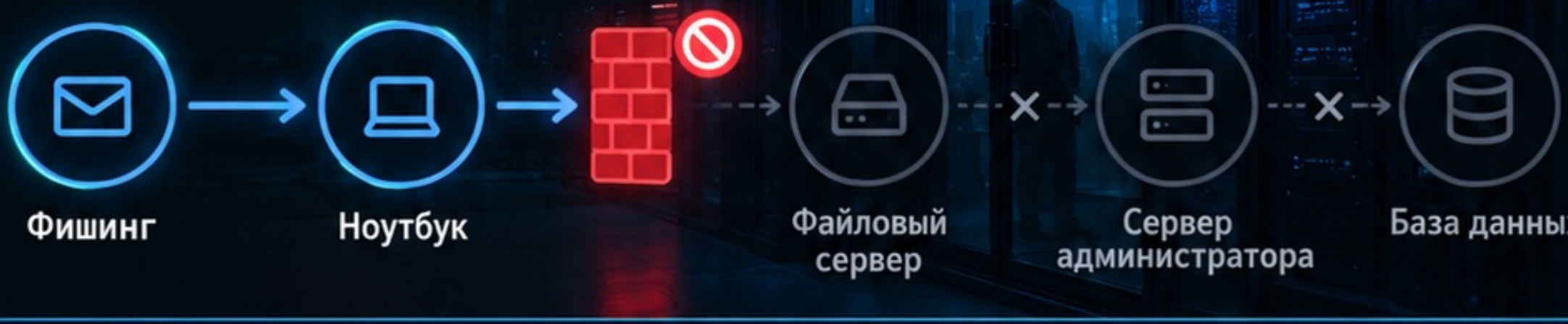
Латеральное движение — это переход с первого скомпрометированного устройства к **более ценным системам** внутри сети.

✕ БЕЗ СЕГМЕНТАЦИИ



4 перехода • ничего их не останавливает • данные украдены

✓ С СЕГМЕНТАЦИЕЙ



Заблокировано на границе зоны + зафиксировано в логах

Злоумышленники редко сразу попадают туда, где хранятся ценные данные. Они идут туда **постепенно**. Сегментация ставит **закрытые двери** на этом пути.

Основные термины

Эти понятия — основа сетевой сегментации.
Зная их, проще понимать архитектуру, настраивать защиту
и обсуждать решения с командой.

GROUP

Zone

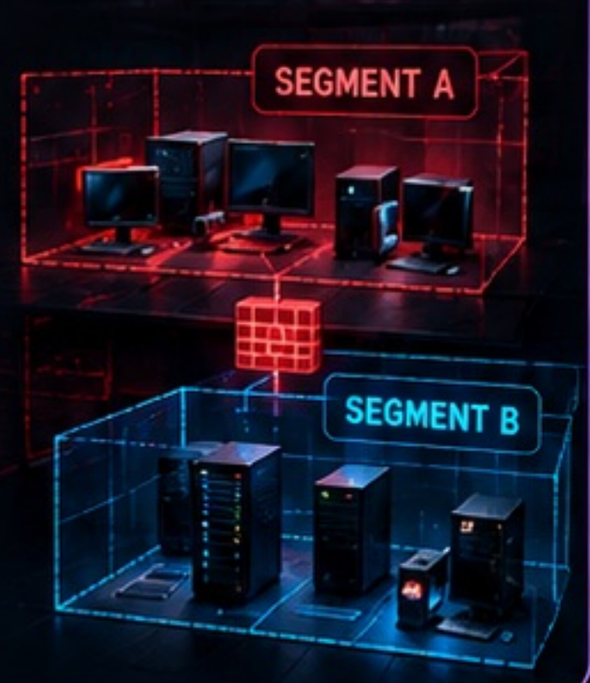
Группа систем, которые находятся в **одном контуре доверия** и имеют одинаковые требования к безопасности.



SLICE

Segment

Часть сети, которая **отделена от других сегментов** и имеет собственные правила доступа.



LAYER 3

Subnet

Диапазон **IP-адресов**. Классический способ разделить сеть на части на уровне **Layer 3**.

192.168.10.0/24
USERS

192.168.20.0/24
SERVERS

192.168.30.0/24
IoT

LAYER 2

VLAN

Виртуальная локальная сеть, которая делит **один физический коммутатор** на несколько независимых сегментов.



EDGE

Trust boundary

Граница между зонами с **разным уровнем доверия**. Через неё проходит и контролируется сетевой трафик.



GATE

Chokepoint

Единая контролируемая точка, через которую должен проходить весь межзонный трафик.



Лестница сегментации

Сегментация — это не один инструмент, а **набор методов** от грубого разделения к тонкому контролю.

1

Физическое разделение

AIR GAP

Отдельное оборудование. **Самый надёжный,** но дорогой вариант.



2

VLAN

LAYER 2

Логическое разделение на одном коммутаторе. Каждый VLAN — отдельный широковещательный домен.



3

Подсети (Subnets)

LAYER 3

Диапазоны IP-адресов. Разделяют сеть на части, между которыми действуют правила маршрутизации (routing).



4

Зоны межсетевого экрана

L3 – L7

Firewall зоны **проверяют каждое соединение** и применяют политики безопасности (policy).



5

Микросегментация

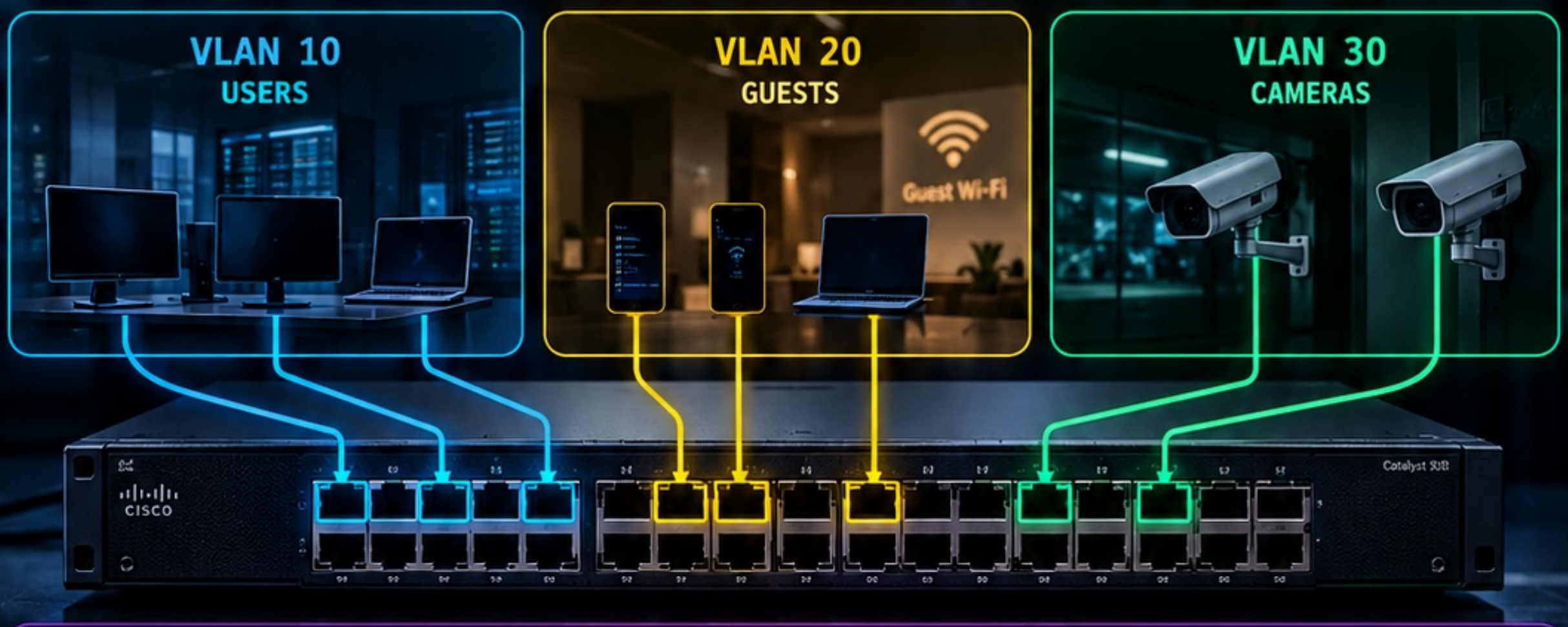
WORKLOAD

Политики на уровне отдельных приложений, сервисов и рабочих нагрузок (workload). Позволяет контролировать трафик **максимально точно.**



VLANs

На одном физическом коммутаторе можно создать **несколько изолированных сетей (VLAN)**, которые логически разделяют трафик.



Коммутатор определяет VLAN по 802.1Q tag





VLAN разделяет трафик, но это не firewall.

Если на маршрутизаторе между VLAN нет правил, они всё равно могут обмениваться трафиком.



Подсети и маршрутизация

Устройства в одной подсети (subnet) общаются напрямую.
Трафик между подсетями проходит через маршрутизатор,
где **применяются правила.**



Как устроен IP-адрес (IPv4)

IP-адрес = 32 бита

СЕТЬ · 24 бита

ХОСТЫ · 8 бит

/24	/25	/26	/27
256 адресов	128 адресов	64 адреса	32 адреса

Подсети (subnets) разделяют трафик, но сами по себе **не являются firewall.** Если на маршрутизаторе между подсетями нет правил, они всё равно могут обмениваться трафиком.

Правила firewall

Между зонами firewall проверяет каждое соединение по набору правил.

#	Источник (From)	Назначение (To)	Порт	Действие
1	**Пользователи** (Users)	**Web servers**	443 HTTPS	ALLOW
2	**Web servers**	**Database**	5432 PostgreSQL	ALLOW
3	**Администраторы** (Admins)	**Все серверы** (All servers)	22 SSH	ALLOW
4	**Гостевая Wi-Fi** (Guest Wi-Fi)	**Интернет** (Internet)	80, 443 HTTP, HTTPS	ALLOW
5	**Любой источник** (Any)	Любое назначение (Any)	Любой (Any)	DENY



Срабатывает первое совпадение

Правила читаются сверху вниз. Действует **первое совпадение**.



Запрет по умолчанию

Всё, что явно не разрешено, отбрасывается **(default deny)**. Всегда в конце.

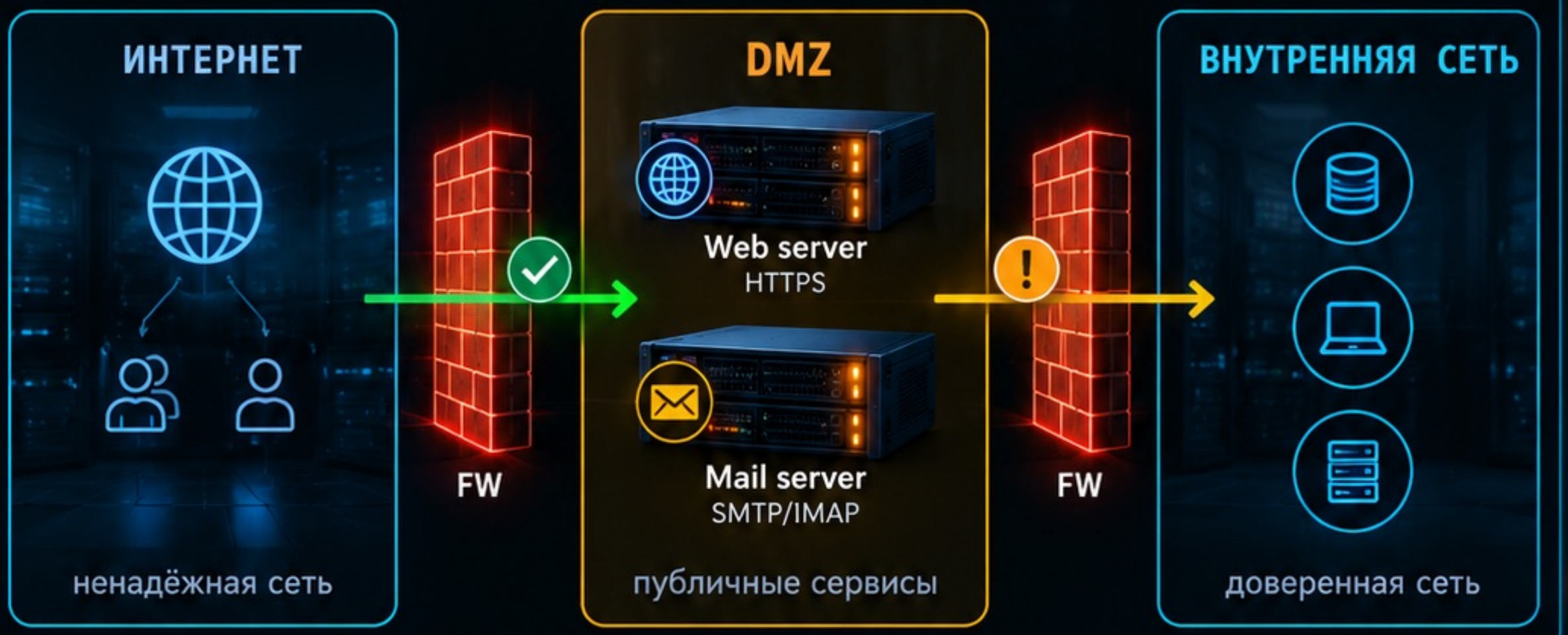


Принцип наименьших привилегий

Разрешайте **только необходимые** порты, протоколы и зоны.

DMZ

DMZ — это **буферная зона**, в которой размещаются публичные сервисы, доступные из интернета, например, **web** и **mail** серверы.



ИНТЕРНЕТ → DMZ

Разрешаем только нужные **публичные** порты, например, web (80/443) и mail (25/587).



DMZ → ВНУТРЕННЯЯ СЕТЬ

Только конкретные, необходимые соединения (по строгим правилам).



ИНТЕРНЕТ → ВНУТРЕННЯЯ СЕТЬ

Никогда. Прямой доступ из интернета во внутреннюю сеть запрещён.



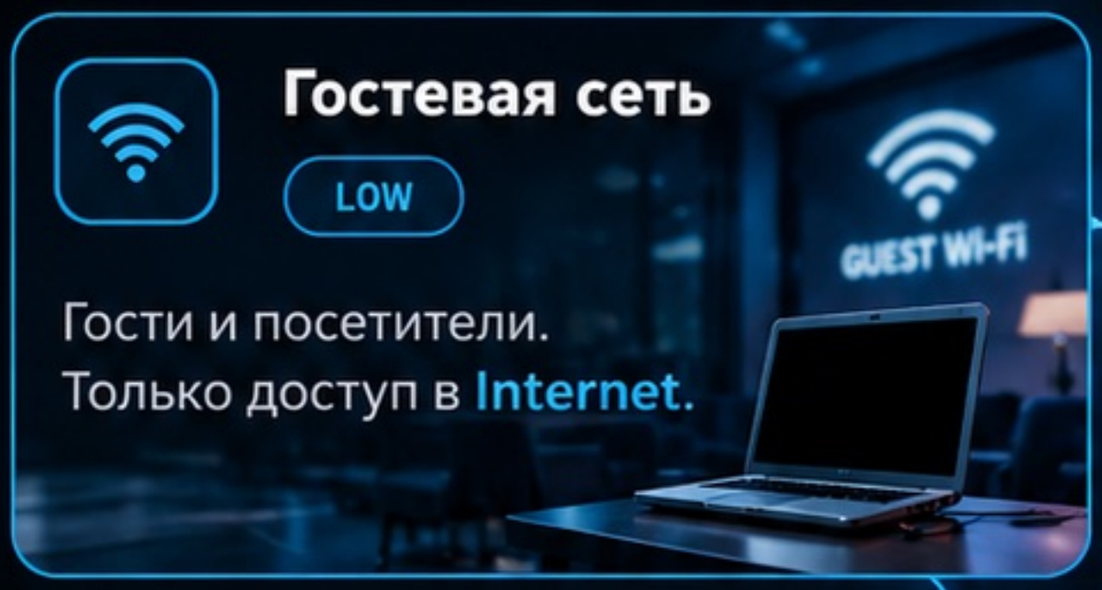
Пример зон сегментации

В большинстве организаций используются такие зоны.
Весь их трафик контролируется на **central firewall**.

Гостевая сеть

LOW

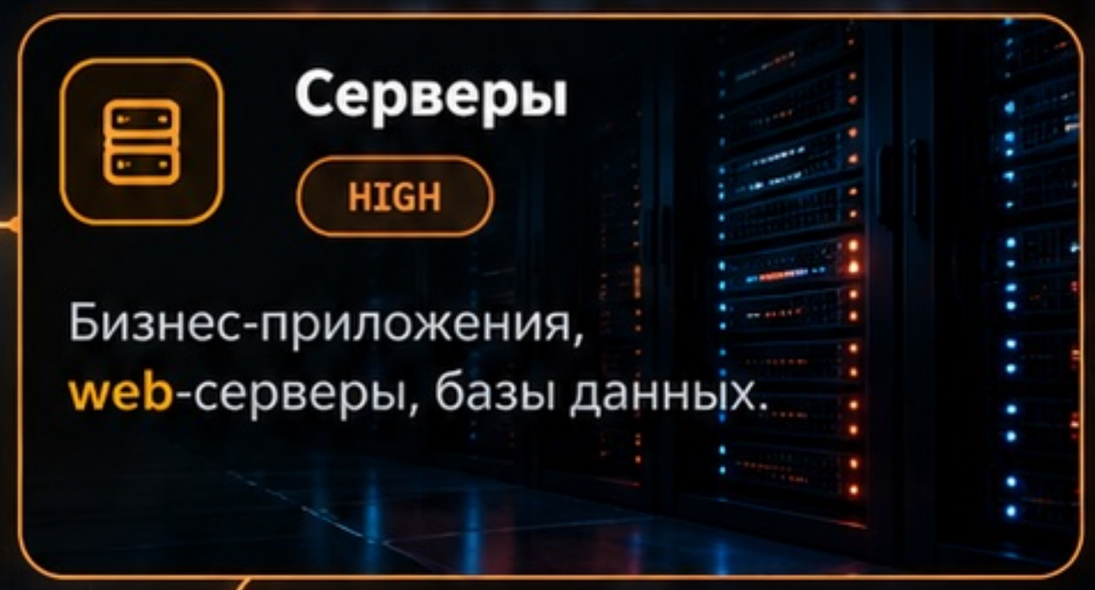
Гости и посетители.
Только доступ в **Internet**.



Серверы

HIGH

Бизнес-приложения,
web-серверы, базы данных.



IoT

LOW

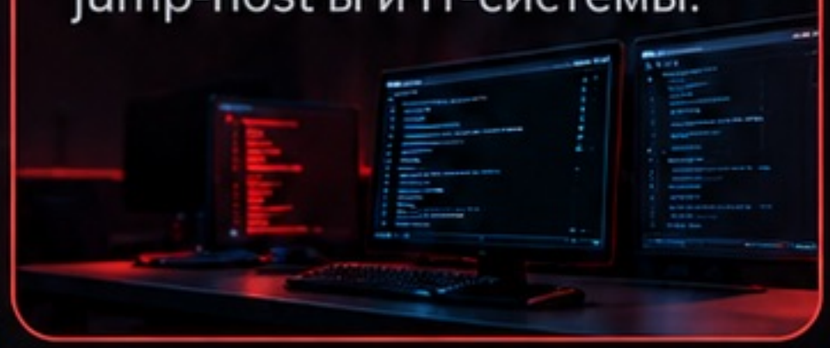
Камеры, принтеры,
датчики, умные ТВ
и другие устройства.



Управление

CRITICAL

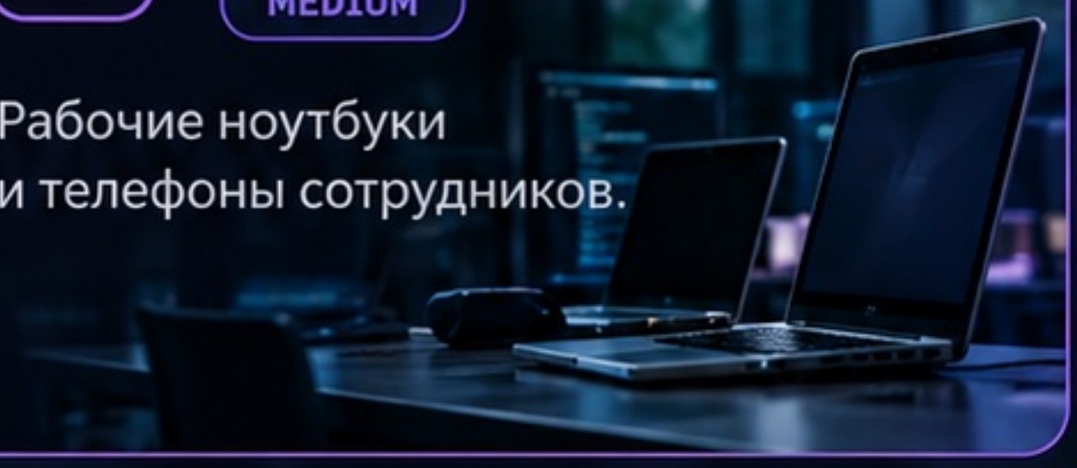
Панели администрирования,
jump-host'ы и IT-системы.



Пользователи

MEDIUM

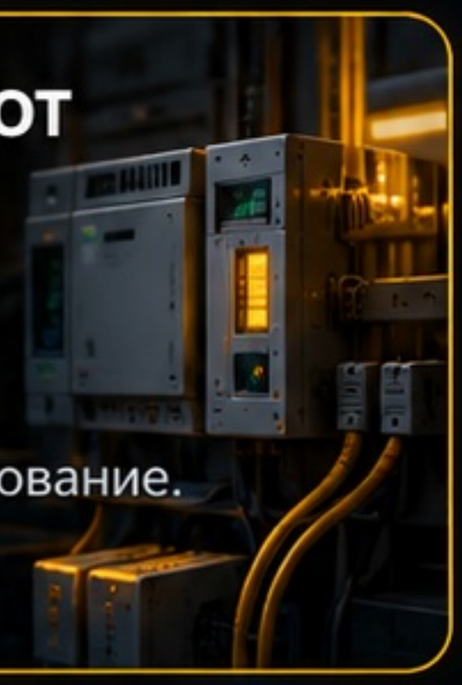
Рабочие ноутбуки
и телефоны сотрудников.



Платежи / OT

CRITICAL

Платежные системы,
данные карт и
промышленное оборудование.



Микросегментация

Вместо одной большой зоны каждый сервис и приложение получает свою собственную зону с **отдельными правилами.** Так мы ограничиваем перемещение злоумышленника.

NORTH–SOUTH

INTERNET ↔ DC

Трафик из интернета и обратно.

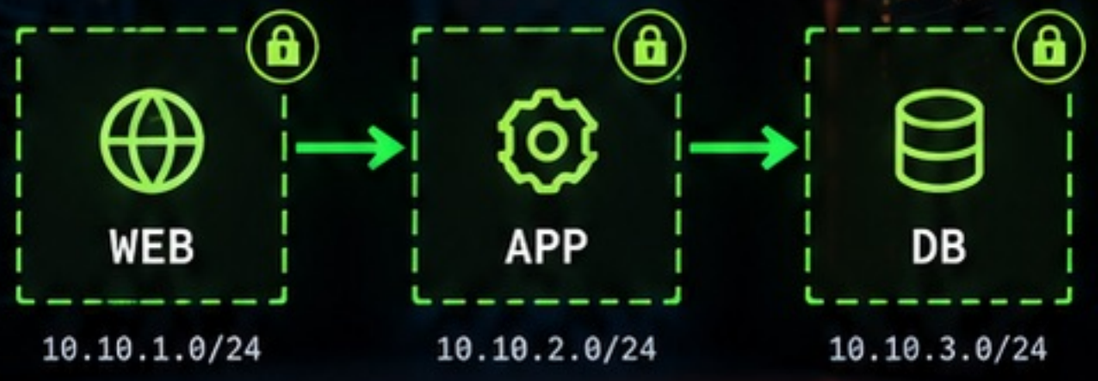


Perimeter firewall контролирует этот трафик.

EAST–WEST

ВНУТРИ DC

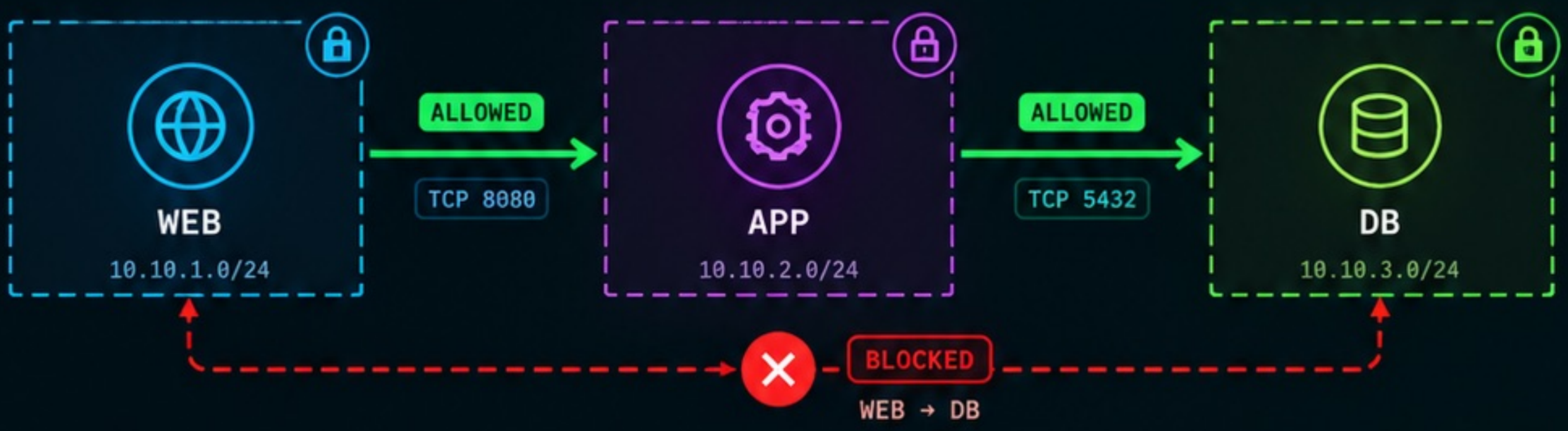
Трафик между сервисами внутри сети.



Большая часть трафика остаётся внутри этих зон.

КАЖДАЯ НАГРУЗКА — СВОЯ ЗОНА

MICROSEGMENTATION POLICY



Вместо одной общей «стены» для всей сети каждая нагрузка получает **свои правила**. Даже если злоумышленник скомпрометирует **web server**, он не сможет напрямую достучаться до **database**.

Сегментация + Zero Trust

Сегментация определяет, **где** находятся ресурсы.
Zero Trust проверяет, **кто вы, каждый раз.**

СТАРАЯ МОДЕЛЬ

Замок и ров

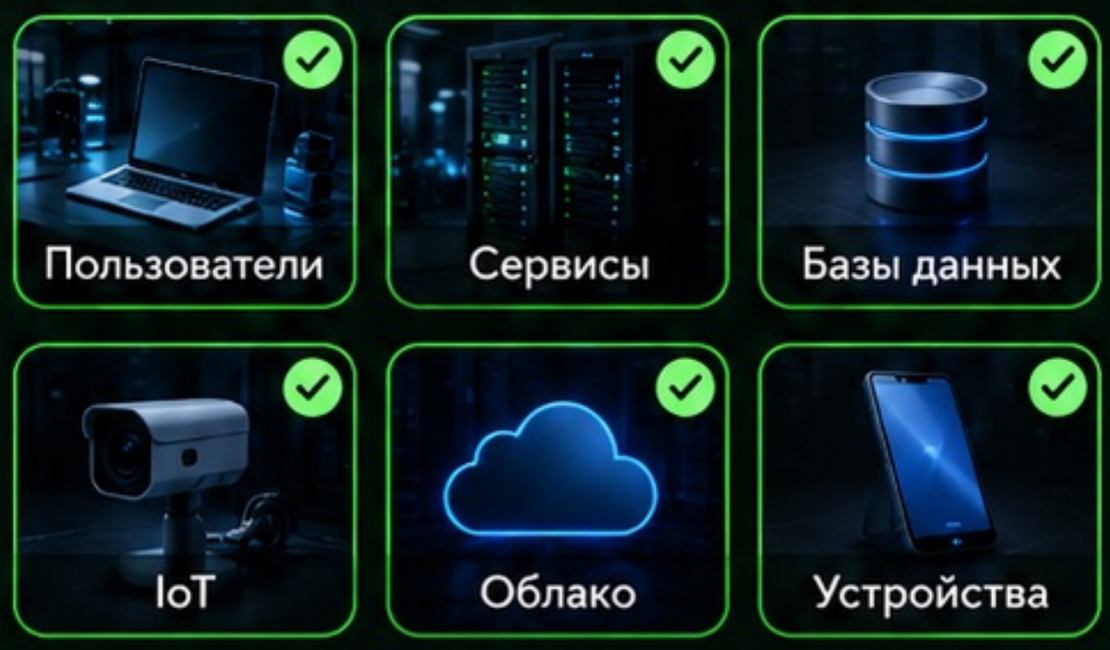
Всё внутри сети считается доверенным.



ZERO TRUST

Никому не доверять, всегда проверять

Каждый запрос проходит проверку: кто вы, в каком состоянии устройство и позволяет ли политика доступ.



КАЖДЫЙ ЗАПРОС ПРОХОДИТ ПРОВЕРКУ

Кто вы?
Идентификация и аутентификация

В порядке ли устройство?
Проверка состояния и соответствия

Разрешает ли политика?
Проверка правил доступа

Доступ к приложению
Только если все проверки пройдены

Сегментация отвечает на вопрос **где вы находитесь**.
Zero Trust — **кто вы, каждый раз**, при каждом обращении.

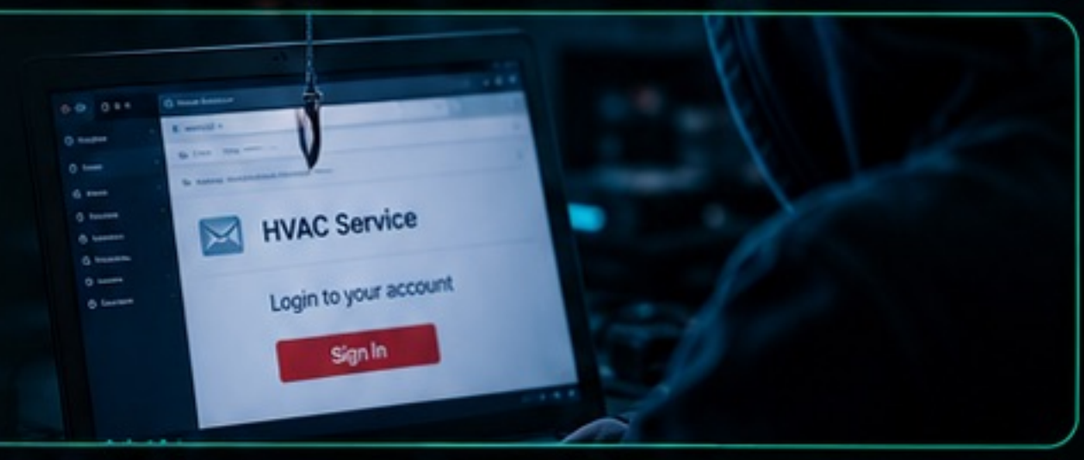
Реальная атака: шаг за шагом

Как злоумышленники через подрядчика HVAC добрались до платёжных систем крупной розничной сети.

ШАГ 1

Компрометация подрядчика

Злоумышленники получили учётные данные через **фишинг**, нацеленный на небольшого подрядчика **HVAC**.



ШАГ 2

Удалённый доступ

Используя учётные данные, они вошли через **VPN** подрядчика в сеть крупного ритейлера.



ШАГ 3

Горизонтальное перемещение

Злоумышленники перемещались по сети, так как доступ подрядчика **не был изолирован** от остальных систем.



ШАГ 4

Компрометация POS

На платёжные терминалы в магазинах было распространено **malware** для кражи данных карт.



ШАГ 5

Масштабная кража

Было похищено около **40 миллионов** платёжных карт, а также записи клиентов.



У подрядчика HVAC не было причин иметь доступ к платёжным системам.
Сегментация закрыла бы этот путь.

Как всё это внедрить

01

ШАГ 1

Проведите инвентаризацию

Вы не сможете защитить то, что не знаете. Составьте полный список всех устройств, систем и приложений.

IT Asset Inventory

Name	Type	IP Address	Status
WEB-01	Server	10.10.1.10	Online
APP-01	Server	10.10.2.15	Online
DB-01	Database	10.10.3.20	Online
POS-01	Terminal	10.10.4.30	Online
CAM-01	Camera	10.10.5.25	Online

02

ШАГ 2

Классифицируйте данные

Оцените важность: публичные, внутренние, конфиденциальные, критичные.



03

ШАГ 3

Определите зоны

Объедините системы с одинаковым уровнем доверия и требованиями к доступу.



04

ШАГ 4

Опишите потоки

Кто с кем должен взаимодействовать и по каким портам. Задокументируйте все необходимые подключения.

Web (10.10.1.0/24)	→	App (TCP 8080)
App (10.10.2.0/24)	→	DB (TCP 5432)
Users (10.10.10.0/24)	→	Internet (TCP 443)

05

ШАГ 5

Включите default deny

Сначала блокируйте всё, затем разрешайте только те потоки, которые описаны в вашей модели.

Firewall Policy

✓	Allow	Users → Web	TCP 443
✓	Allow	Web → App	TCP 8080
✓	Allow	App → DB	TCP 5432
⊗	Deny	Any → Any	Any

06

ШАГ 6

Мониторьте и проверяйте

Логируйте трафик на границах зон, регулярно проверяйте правила и проводите тесты.



Хорошая сегментация — это не разовый проект, а постоянный процесс.
Инвентаризация, контроль и тестирование должны быть регулярными.

Частые ошибки

Эти ошибки сводят на нет всю проделанную работу по сегментации и делают сеть уязвимой.

Слишком широкие правила

Одно ленивое правило any-to-any может полностью нивелировать все границы, которые вы построили.

Как исправить: используйте конкретные allow rules.



Доверие VLAN без правил

VLAN сами по себе не обеспечивают изоляцию — устройства из разных VLAN всё равно могут обмениваться трафиком.

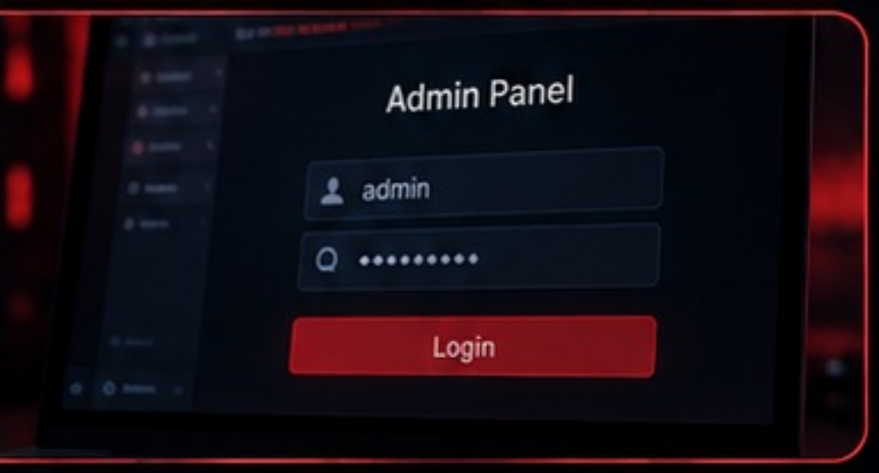
Как исправить: фильтруйте трафик между VLAN.



Открытые панели управления

Интерфейсы управления (например, веб-панели) доступны из пользовательских или гостевых сетей.

Как исправить: выделите отдельную management zone.



Незадокументированные правила

Никто не помнит, зачем создано правило, поэтому его боятся удалять, даже если оно больше не нужно.

Как исправить: указывайте владельца и причину для каждого rule.



#	SOURCE	DESTINATION	PORT	COMMENT
12	10.10.10.5	10.10.20.10	443	???
13	10.10.30.0/24	ANY	ANY	legacy?
14	ANY	10.10.40.5	3389	temp
15	10.10.20.0/24	10.10.30.0/24	ANY	???

Настроили и забыли

Сеть постоянно меняется: появляются новые сервисы, устройства и требования. Правила без регулярного обзора устаревают.

Как исправить: регулярно проверяйте правила по расписанию.



Тестируем сегментацию

Регулярно проверяйте, что правила реально работают и нет неожиданных путей между зонами.

segmentation-test

```
$ scan --from each-zone --to all
```

FROM		TO	PORT	STATUS	RESULT
guest	→	servers	22	BLOCKED	✓
guest	→	servers	443	BLOCKED	✓
users	→	web	443	OPEN	✓
users	→	db	5432	BLOCKED	✓
iot	→	mgmt	22	OPEN	✗ LEAK

Найден неожиданный путь. Исправьте правила до того, как это сделают атакующие.

01

Сканируйте из каждой зоны

Запустите порт-сканер из каждого сегмента. Должны быть доступны только **ожидаемые порты.**

```
$ nmap -Pn 10.20.30.0/24
PORT     STATE      SERVICE
22       filtered   ssh
80       open       http
443      closed     https
3306     filtered   mysql
```

02

Проводите регулярный pentest сегментации

Тестируйте, как реальные атакующие: пытайтесь обойти правила, использовать нестандартные пути и протоколы.



03

Анализируйте логи

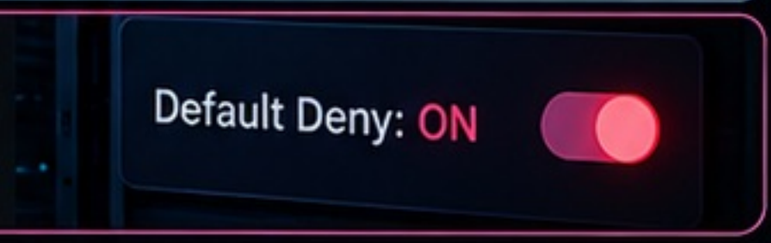
Проверяйте firewall и flow logs на попытки доступа, которые были заблокированы, и на **неожиданные пути.**

TIME	SRC	DST	ACTION	INFO
12:14:01	10.10.5.23	10.20.1.10	DENY	blocked by rule
12:14:03	10.10.5.23	10.20.1.10	DENY	blocked by rule
12:16:27	10.30.2.11	10.10.0.5	DENY	unexpected path
12:17:12	10.20.8.14	10.10.0.5	DENY	scan detected

Сегментация работает только тогда, когда вы регулярно её проверяете.
Проверяйте, тестируйте, анализируйте — и закрывайте найденные пути.

Шпаргалка по сегментации

Ключевые термины, их назначение и как они помогают строить безопасную архитектуру.

ТЕРМИН	ЗАЧЕМ НУЖЕН	ТИП	
Flat network	Все устройства в одной сети видят друг друга. Любая компрометация быстро распространяется.	ИЗБЕГАТЬ	
VLAN	Разделяет один коммутатор на изолированные группы устройств.	LAYER 2	
Subnet	Делит IP-адресное пространство на отдельные сегменты (subnets).	LAYER 3	192.168.10.0/24 Users 192.168.20.0/24 Servers 192.168.30.0/24 Mgmt
Firewall rule	Разрешает или блокирует трафик между зонами согласно политике.	POLICY	ALLOW Users → Web TCP 443 DENY Any → DB TCP 5432 ALLOW App → API TCP 8080
DMZ	Буферная зона для публично доступных серверов (например, web и почтовые серверы).	ZONE	
Microsegmentation	Правила применяются вокруг каждой рабочей нагрузки (workload), а не только на уровне сети.	WORKLOAD	
Zero Trust	Проверяет каждый запрос и каждое подключение, каждый раз.	IDENTITY	
Default deny	Блокирует всё по умолчанию. Разрешаются только явно описанные правила.	RULE	

Сегментируйте по принципу минимального доверия.
Запрещайте по умолчанию. Разрешайте только необходимые потоки. Тестируйте.

Было полезно?

Сохраните, чтобы не потерять, и поделитесь с тем, кто тоже изучает сетевую безопасность и сегментацию.

Сохранить
чтобы вернуться к этому материалу

Поделиться
с коллегой, которому будет полезно

Сохраните на потом

Поделитесь с коллегой

