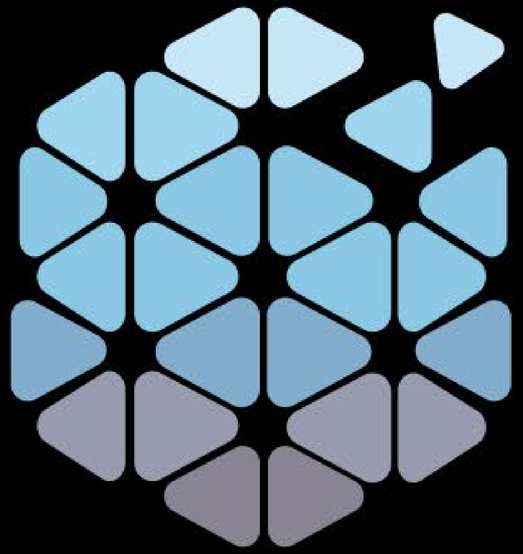


Сетевая Безопасность

[NGFW, WAF, NDR, VPN, ZTNA, Anti-DDOS, NAC, MFA]

09.12.2024

г. Москва, отель «Холидей Инн Сокольники»

Сетевая
Безопасность

Управление и организация сетевых доступов

Дмитрий Резников

Архитектор

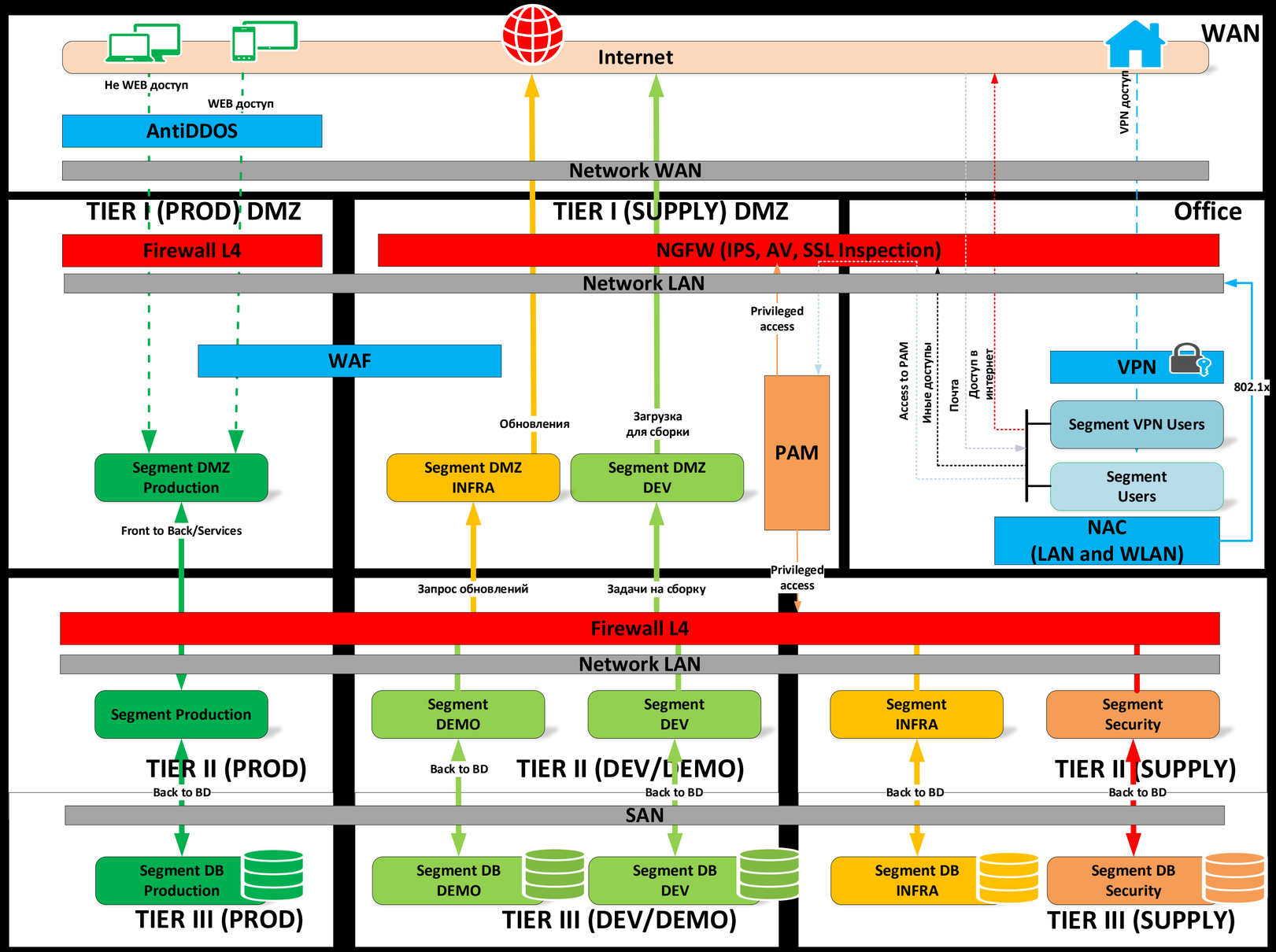
Сетевая
Безопасность

Взгляд на сеть глазами ИБ

Типовая архитектура сети
Сетевые устройства
Модули контроля в NGFW
Головная боль
Профилактика

Сетевая Безопасность

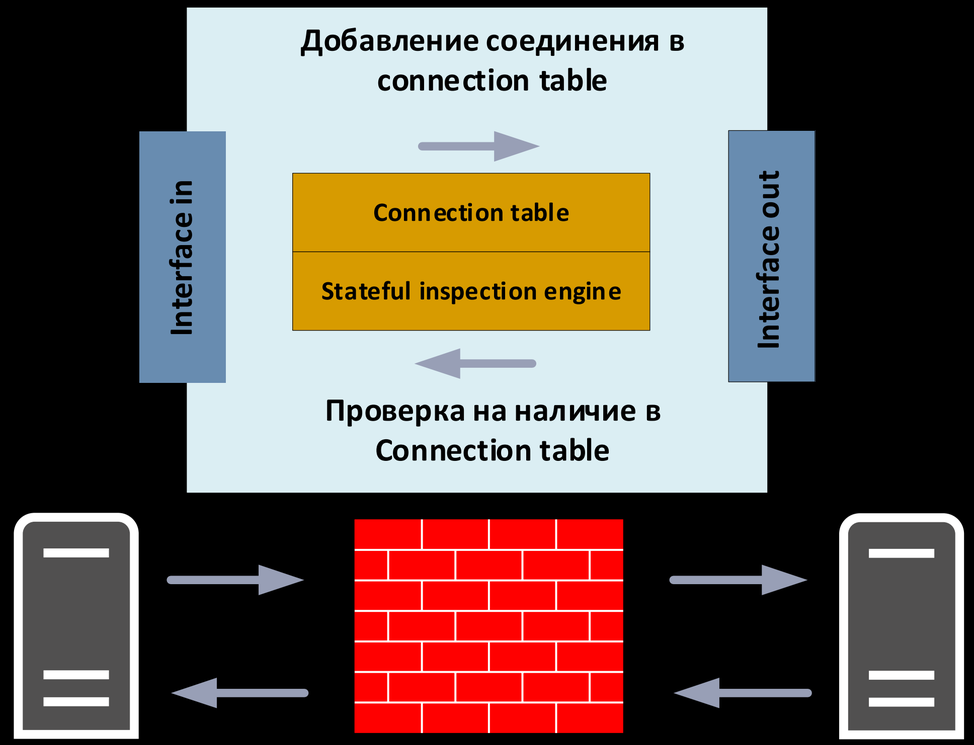
Типовая архитектура сети



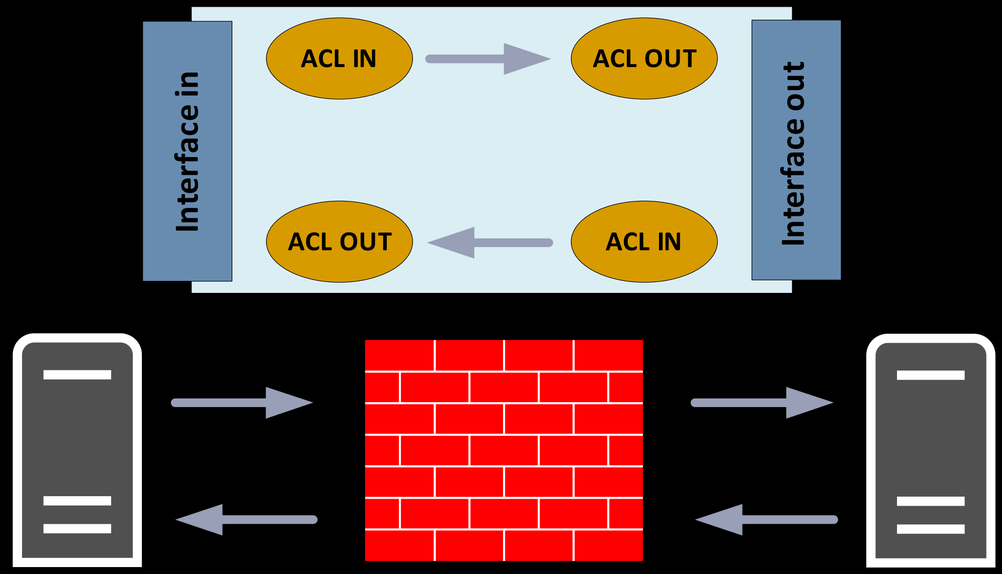
Сетевая Безопасность

Сетевые устройства

Stateful Inspection*:
Next Generation Firewalls (NGFW)
Firewalls
Host-Based Firewalls (HBF)



Stateless Inspection:**
Маршрутизаторы
L2/L3 коммутаторы



* - инспекция с контролем состояния сессий

** - инспекция без контроля состояния сессий

Модули контроля в NGFW

- **L4 Firewall**
  - ❑ Правила на основе IP адресов и контроль состояния сессий
- **Application Control**
  - ❑ Идентификация приложений
- **URL-filtering**
  - ❑ Правила фильтрации для http и https адресов
- **User Identity**
  - ❑ Идентификация пользователей и возможность применения в правилах групп пользователей

Сетевая Безопасность

Головная боль

- **Огромное количество правил**
  Невозможно провести аудит и составить полную картину
- **Отсутствие структуры**
  Инциденты доступности после применения политики
- **Деградация производительности**
  Долгое применение политик, как минимум
- **Отказ от URL фильтрации**
  Недоступность некоторых сайтов после включения SSL Inspection
- **Последнее правило разрешает весь трафик**
  Страшно включать блокирующее правило

Сетевая
Безопасность

Профилактика

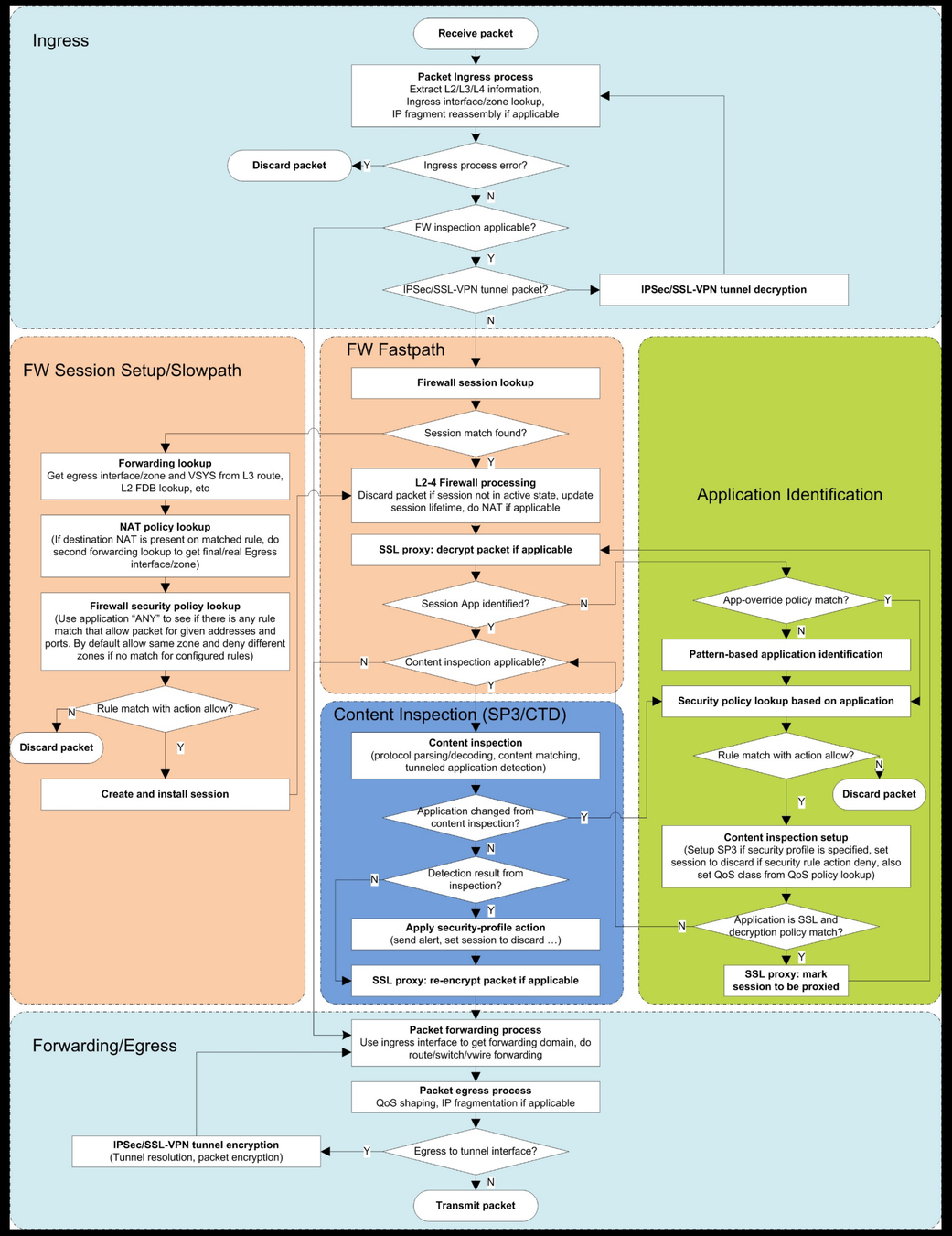
- Понимание пути трафика в NGFW
- Продуманная политика фильтрации
- Баланс производительности и безопасности
- Понимание инфраструктуры
- Использование инструкций и регламентов

Сетевая
Безопасность

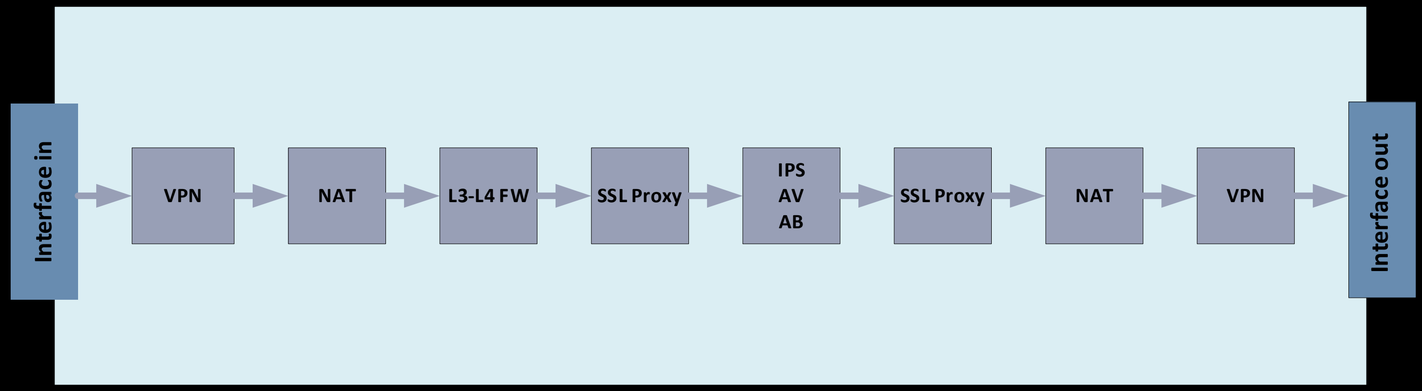
Трафик внутри NGFW

Traffic Flow
Packet Trace

Traffic flow



- Путь трафика внутри NGFW: fastpath и slowpath
- Работа всех функций: VPN, QoS, NAT и модулей
- У каждого вендора свои особенности



Сетевая Безопасность

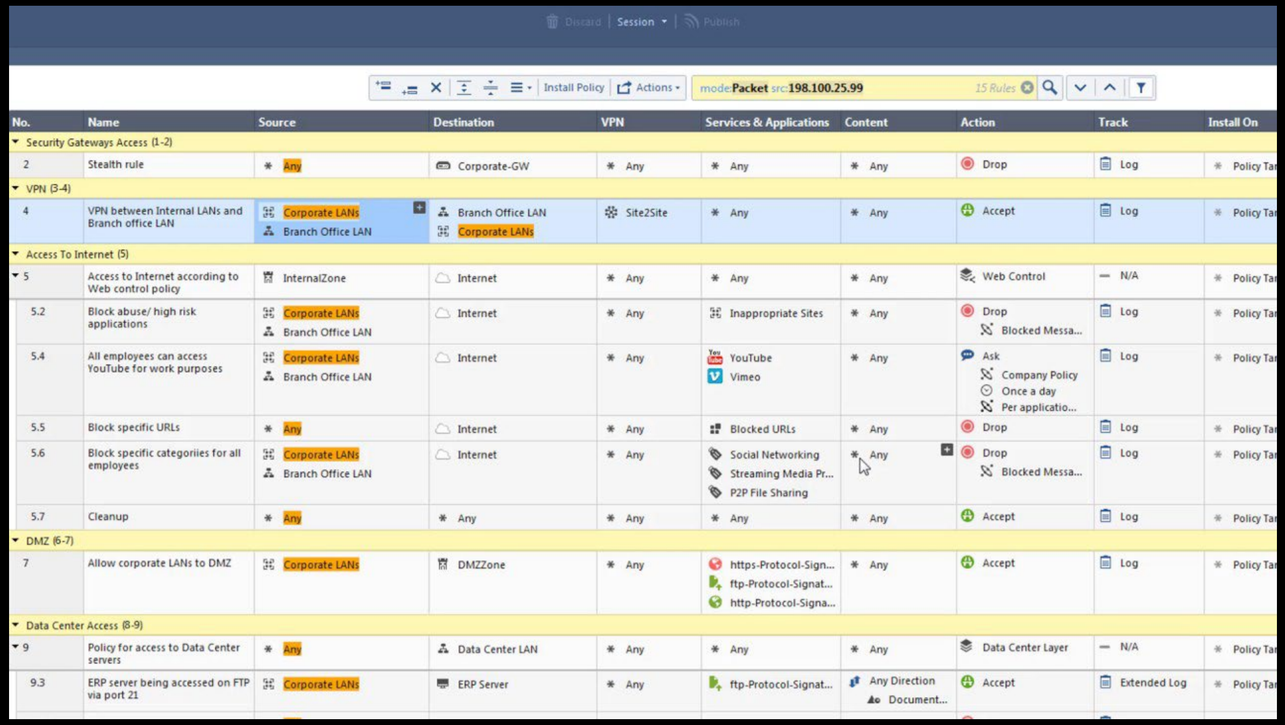
Packet Trace

Использование встроенных утилит

Packet-tracer

```
ASA# packet-tracer input inside udp 192.168.1.53 80 10.10.300.10 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   10.10.300.0     255.255.255.0   outside

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) after-auto source static OBJ-SUBNET-VLAN-USER OBJ-SUBNET-VLAN-USER destination
static GRP-NETWORK-DPC1 GRP-NETWORK-DPC1 no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.300.10/80 to 10.10.300.10/80

...
```

Packet Mode



Сетевая
Безопасность

Создание правил

Взгляд на одно правило
5 Tuples
IP / Subnets / Objects / GeoIP
Зоны безопасности
Группы пользователей
Комбинирование и объединение
Ports vs Applications
URL-filtering
Explicit allow, Implicit deny и Explicit deny
Уровни и секции
Комментарии в правилах

Сетевая Безопасность

Одно правило

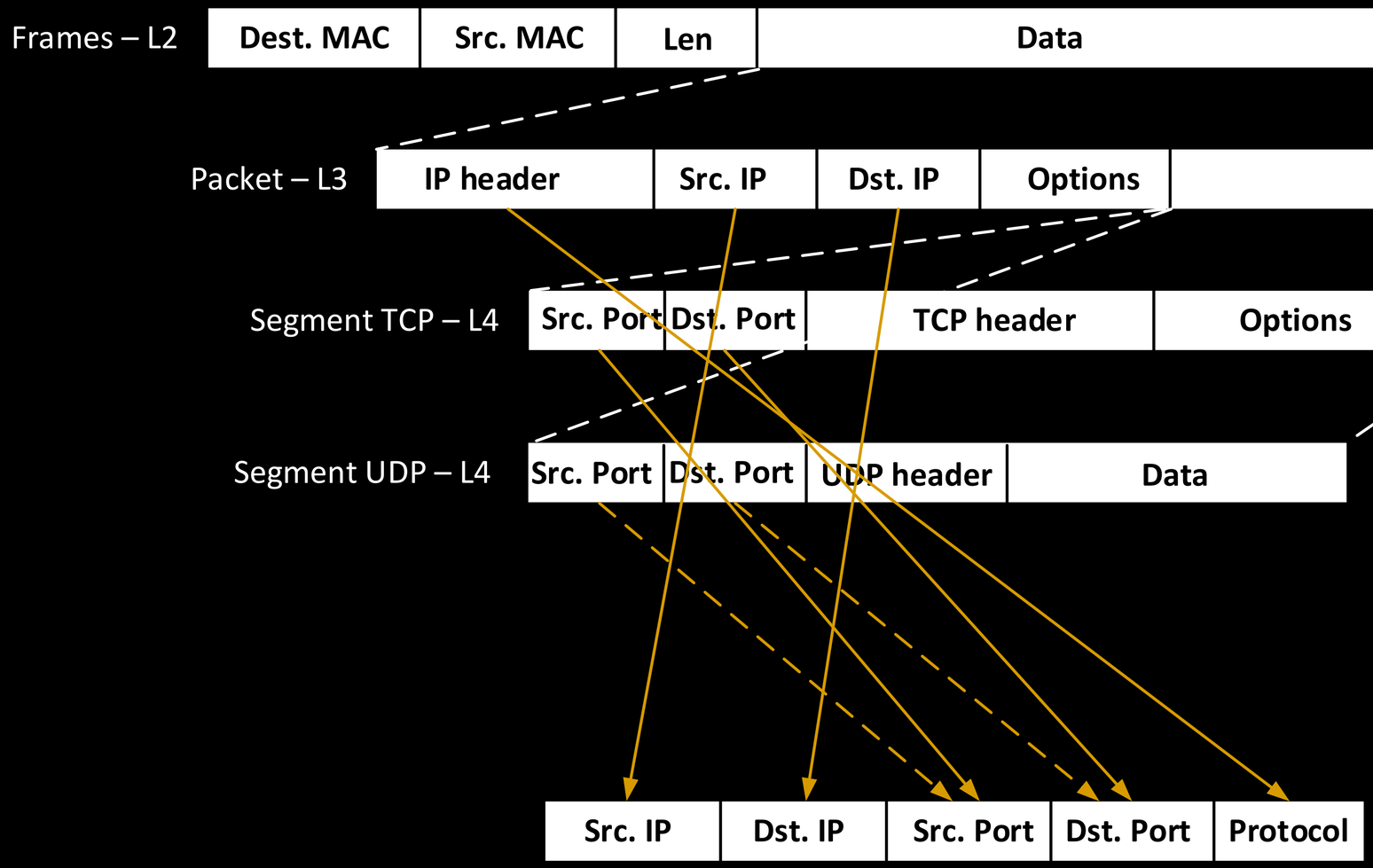
Откуда | Куда | Кто | Как

#	Название	Действие	Исходная зона	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис	Приложения
1	Block from China	Запретить	Untrusted	China	Любая	Любой	Любой	Любой	Любое
2	Block to botnets	Запретить	Trusted	Любой	Untrusted	Список бот-сете	Любой	Любой	Любое
3	Block from botnets	Запретить	Untrusted	Список бот-сете	Любая	Любой	Любой	Любой	Любое
4	Allow from DMZ to Untrusted	Разрешить	DMZ	Любой	Untrusted	Любой	Любой	Любой	Любое
5	Allow trusted to untrusted	Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое
6	VPN for remote access to Trusted and Untrust...	Разрешить	VPN for remote ...	Любой	Trusted Untrusted	Любой	Любой	Любой	Любое
7	VPN for Site-to-Site to Trusted and Untrusted	Разрешить	VPN for Site-to-...	Любой	Trusted Untrusted	Любой	Любой	Любой	Любое
	Блокировать все	Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое

Что делать

Сетевая Безопасность

5 Tuples



L4 фильтрация:

- IP-адрес источника
- IP-адрес назначения
- Порт источника
- Порт назначения
- Протокол

Сетевая Безопасность

IP, Subnets, Objects и GeoIP

- **IP и подсети используются как SRC и DST в правилах:**
  - **IP безопаснее Subnet, Subnet безопаснее Any**
  - **подсети хорошо применимы для правил массового (типового) доступа к сервисам**

Src. IP	Dst. IP	Src. Port	Dst. Port	Protocol
10.200.2.4 ... 10.200.2.253 10.200.4.4 ...	172.18.20.4 172.18.40.4	any	636 389	tcp

Src. IP	Dst. IP	Src. Port	Dst. Port	
10.200.2.0/24 10.200.4.0/24	172.18.20.4 172.18.40.4	any	636 389	tcp

- **IP и подсети можно заменить объектами:**
  - **возможность редактировать один объект, применяя изменения к десяткам правил**
  - **объекты могут состоять из других объектов**
  - **стоит сделать регламент по созданию и наименованию объектов**
  - **у NGFW есть ограничения на кол-во IP/подсетей/объектов добавленных в один объект**

objects	IP
srvs_int	10.200.2.0/24 10.200.4.0/24
srvs_dns	172.18.20.4 172.18.40.4

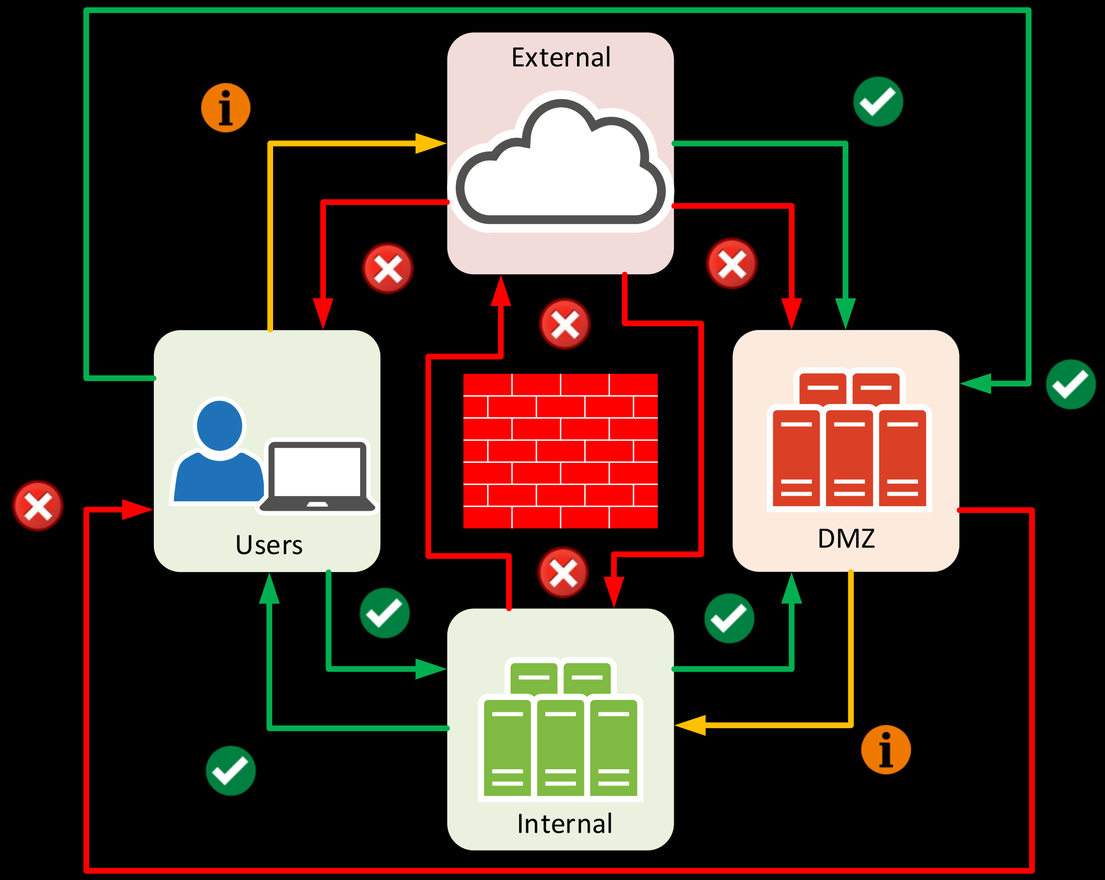
Src. IP	Dst. IP	Src. Port	Dst. Port	Protocol
10.200.2.0/24 10.200.4.0/24	172.18.20.4 172.18.40.4	any	636 389	tcp

Src. IP	Dst. IP	Src. Port	Dst. Port	
srvs_int	srvs_dns	any	636 389	tcp

- **GeoIP это объекты, включающие в себя прописанные производителем подсети**
  - **базы некоторых вендоров требуют корректировок**

Сетевая Безопасность

Зоны безопасности



- Логическое объединение интерфейсов и сетей за интерфейсом
- Межзоновые правила без использования IP, подсетей и объектов или в комбинации
- Использование явных правила запрета взаимодействия зон безопасности
- Позволяют бороться со спуфингом путем проверки соответствия IP подсети и зоны
- Позволяет визуально оценить безопасность правила
- Иногда настройка зон обязательна для вендора

Сетевая Безопасность

Зоны безопасности

Пример настроенных правил с зонами

Межсетевой экран

Добавить | Редактировать | Удалить | Переместить | Копировать | Включить | Отключить | Принудительно применить | Все | Обновить

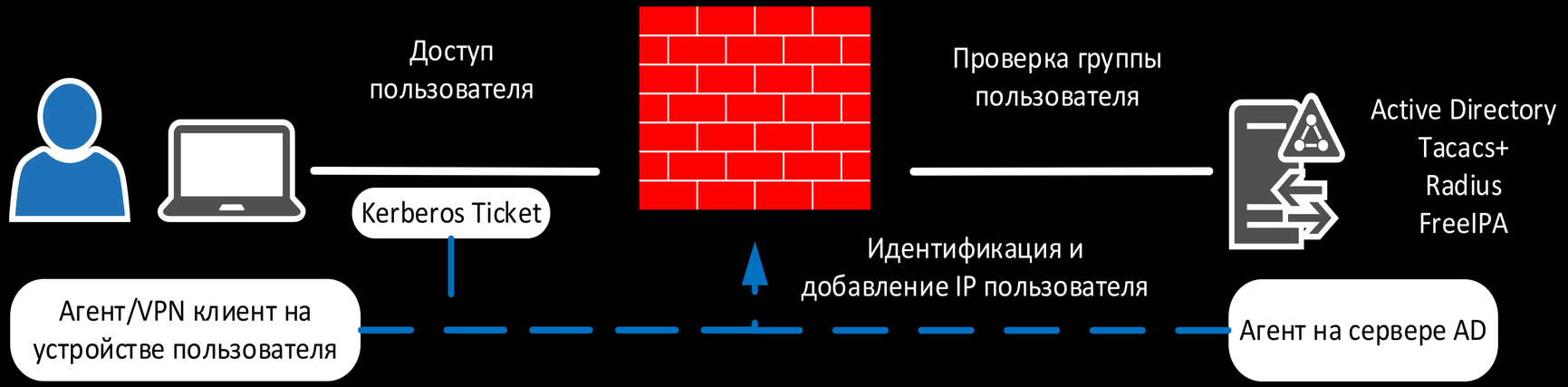
#	Название	Действие	Исходная зона	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис	Приложения	Время	Сценарий
1	Block from China	Запретить	Untrusted	China	Любая	Любой	Любой	Любой	Любое	Любое	—
2	Block to botnets	Запретить	Trusted	Любой	Untrusted	Список бот-сетей	Любой	Любой	Любое	Любое	—
3	Block from botnets	Запретить	Untrusted	Список бот-сетей	Любая	Любой	Любой	Любой	Любое	Любое	—
4	Allow from DMZ to Untrusted	Разрешить	DMZ	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—
5	Allow trusted to untrusted	Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—
6	VPN for remote access to Trusted and Untrust...	Разрешить	VPN for remote ...	Любой	Trusted Untrusted	Любой	Любой	Любой	Любое	Любое	—
7	VPN for Site-to-Site to Trusted and Untrusted	Разрешить	VPN for Site-to-...	Любой	Trusted Untrusted	Любой	Любой	Любой	Любое	Любое	—
	Блокировать все	Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action
Security Gateways Access (1-2)							
2	Stealth rule	Any	Corporate-GW	Any	Any	Any	Drop
VPN (3-4)							
4	VPN between Internal LANs and Branch office LAN	Corporate LANs Branch Office LAN	Branch Office LAN Corporate LANs	Site2Site	Any	Any	Accept
Access To Internet (5)							
5	Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Any	Web Control
5.2	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Any	Inappropriate Sites	Any	Drop Blocked Messa...
5.4	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	Any	YouTube Vimeo	Any	Ask Company Policy Once a day Per applicatio...
5.5	Block specific URLs	Any	Internet	Any	Blocked URLs	Any	Drop
5.6	Block specific categories for all employees	Corporate LANs Branch Office LAN	Internet	Any	Social Networking Streaming Media Pr... P2P File Sharing	Any	Drop Blocked Messa...
5.7	Cleanup	Any	Any	Any	Any	Any	Accept
DMZ (6-7)							
7	Allow corporate LANs to DMZ	Corporate LANs	DMZZone	Any	https-Protocol-Sign... ftp-Protocol-Signat... http-Protocol-Signa...	Any	Accept

Сетевая Безопасность

Группы пользователей

- **Позволяет использовать группы пользователей для открытия доступов:**
  - использование моделей RBAC/ABAC*
  - комбинация IP и групп в правилах позволяет предоставить разные доступы одному пользователю в разных офисах**
  - возможно использовать разные каталоги пользователей
  - разные источники для идентификации: Active Directory, Агент / VPN клиент, Kerberos, - веб-порталы и т.п.



- **Условия:**
  - наличие отдельного модуля/блейда
  - необходимость интеграции с каталогом пользователей
  - некоторым вендорам требуется отдельное ПО на пользовательских машинах

Сетевая Безопасность

Группы пользователей

Role-based access control (RBAC) – модель доступа на основание ролей

Подход: все бухгалтеры добавлены в группу «accountants»

Правило: всем пользователям с группой «accountants» разрешен доступ к «1С» и сайтам налоговой и банков

RBAC подходит для открытия базовых доступов для существующих ролей в компании

Attribute-based access control (ABAC) – модель доступа на основание атрибутов

Подход : все сотрудники, относящиеся к закупкам, добавлены в группа «finance»

Правило: всем пользователям с группой «finance» разрешен доступ к ERP, 1С, сайтам торгов

ABAC подходит для открытия «тонких» доступов в соответствие с потребностями

Примеры:

- мессенджеры и социальные сети

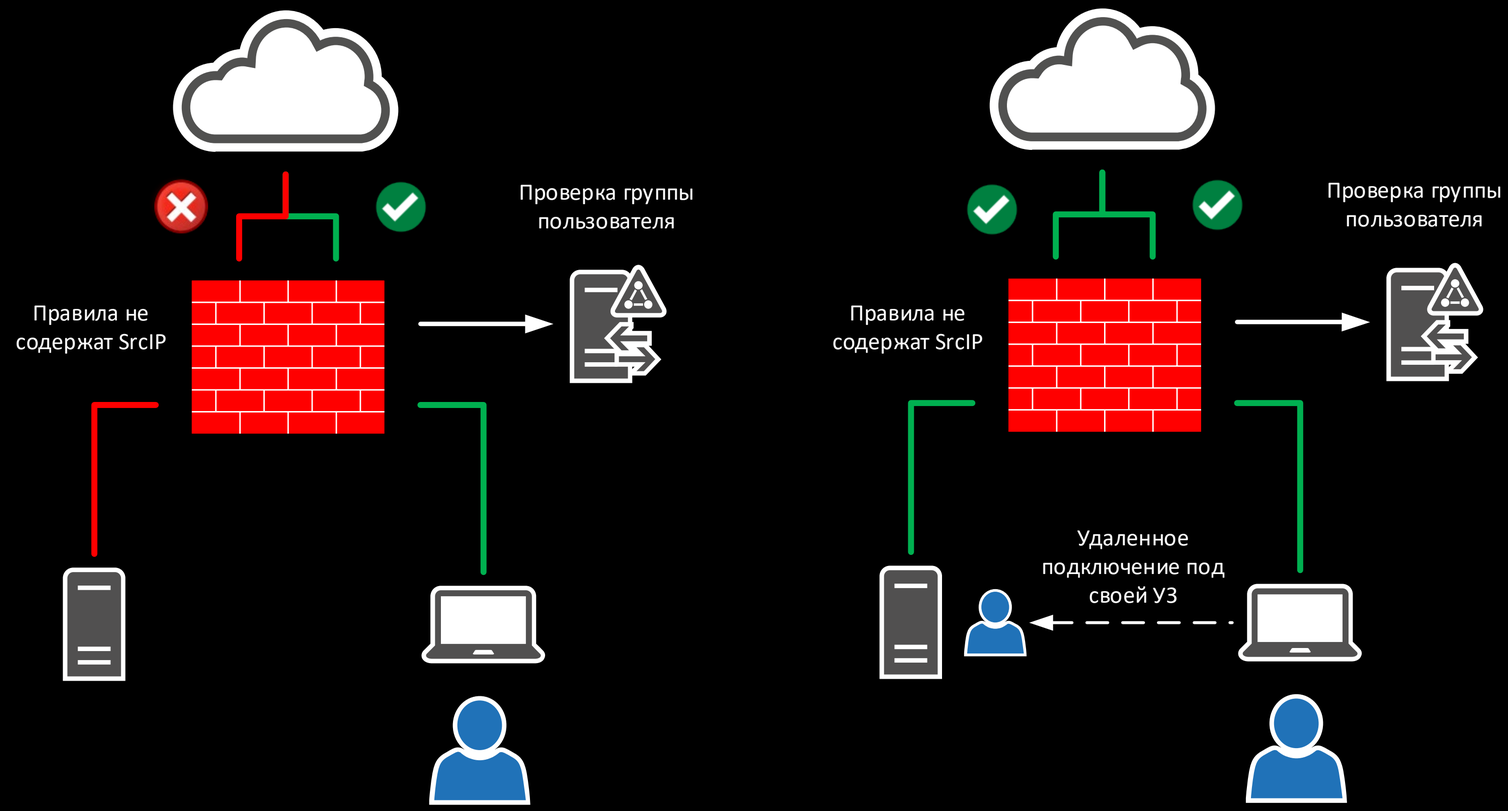
- администраторы разных групп оборудования

- VIP-сотрудники

Сетевая Безопасность

Группы пользователей

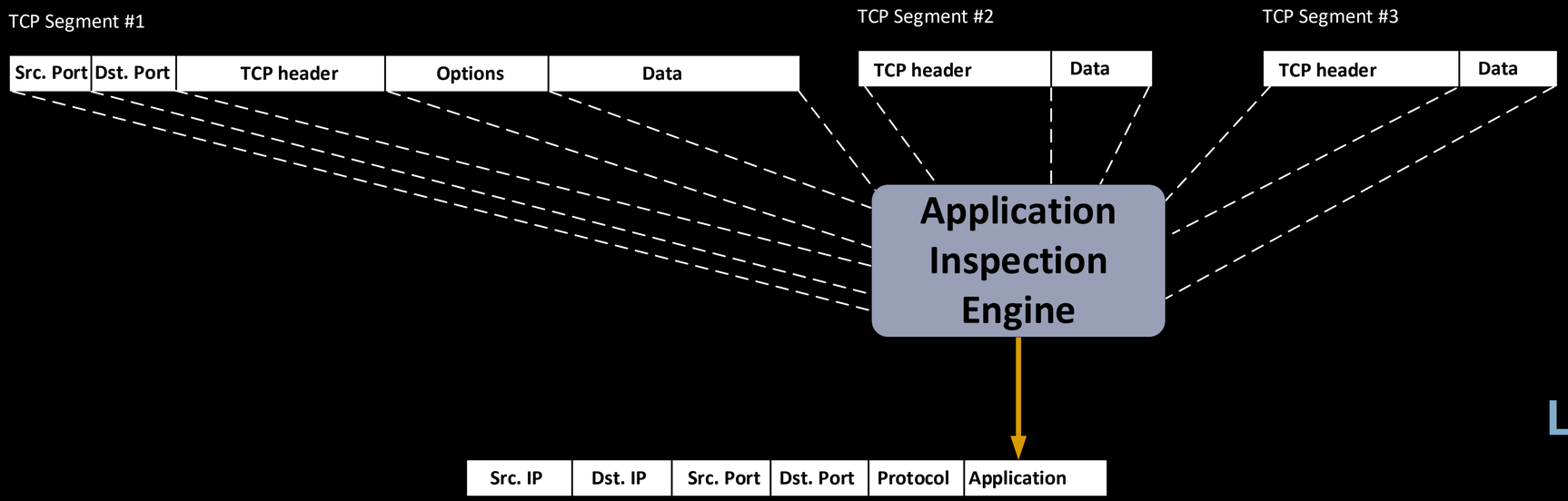
- ** Комбинирование групп пользователей и IP в SRC
  User-Case: правило доступа группе без использования SRC IP в правиле

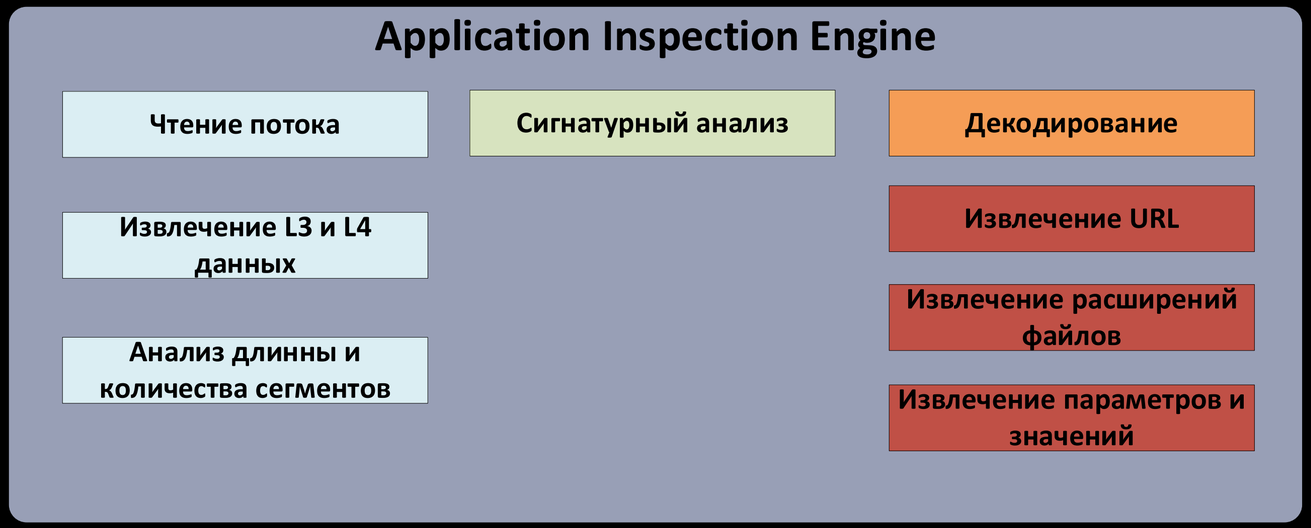


- Сервер «получает» доступ в интернет, если к нему подключился пользовать для которого создано правило доступа в интернет по группе
  Использовать SRC IP или Зоны в сочетание с группами AD

Сетевая Безопасность

Ports vs Applications





L7 фильтрация:

- Данные L3 и L4
- Сигнатурный анализ
- Размер сегментов
- Параметры и значения в поле дата
- URL
- Расширения файлов
- и многое другое

Сетевая Безопасность

Ports vs Applications

- **Использование приложений в правилах реализуется через отдельный модуль/блейд в NGFW**
- **Определение приложений по множеству параметров**
- **У каждого производителя своя база приложений**

Квалификатор L4 Firewall

RULE 1
- Если совпал Source IP, Source user, Destination IP, port, URL
- Действие

RULE 2
- Если совпал Source IP, Source user, Destination IP, port, URL
- Действие

RULE 3
- Если совпал Source IP, Source user, Destination IP, port, URL
- Действие

Квалификатор L7 Firewall

RULE 1
- Если совпал Source IP, Source user, Destination IP, port, приложение, URL
- Действие

RULE 2
- Если совпал Source IP, Source user, Destination IP, port, приложение, URL
- Действие

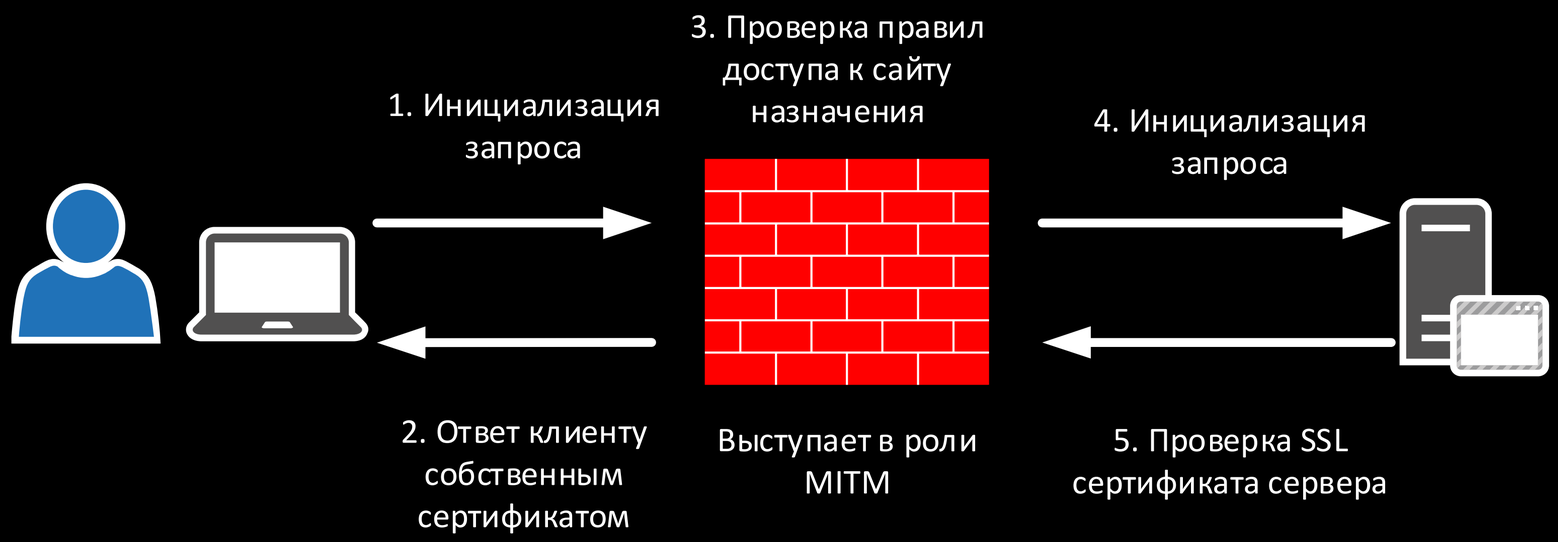
RULE 3
- Если совпал Source IP, Source user, Destination IP, port, приложение, URL
- Действие

- **Особенность Stateful Inspection: для ряда протоколов, таких как SIP, HTTP, FTP, SMB, RPC, требуется анализ трафика приложения**
  Пример: команда PORT в FTP и подмена IP в параметрах PORT для работы FTP за NAT

Сетевая Безопасность

URL-filtering

- Открытие или запрет доступ к определенным сайтам и приложениям, работающим по URL
- Категории сайтов и приложений: социальные сети, новости, банки, медицина и т.п.



- Условия:
  - использование SSL-Decrypt для HTTPS и соответствующие ограничения:
    - Certificate Pinnig
    - ГОСТ или работает через QUIC
    - сервер аутентифицирует клиента по токену/ключу
    - необходимо добавить данные приложения в исключения
  - не рекомендуется использовать regex, т.к. может привести к деградации производительности

Explicit allow, Implicit deny и Explicit deny

- Explicit allow – явное разрешение

- Implicit deny – не явный запрет
  Пример: deny IP any any в конце списка правил

- Explicit deny – явный запрет
  User-case №1: первым стоит запрещающее правило для IP, подсети или объектов, следующим идёт разрешающее правило для более «широкой» группы IP, подсети или объектов
  Пример:
  Правило №1: запрет доступа от зоны DMZ до зоны Internal
  Правило №2: разрешение доступа от объекта all_servers до syslog-сервера
- User-case №2: после ряда разрешающих правил до определенного объекта идет явное запрещающее правило до этого же объекта, далее идут разрешающие правила
- Пример:
  Правила №1-10: разрешающие правила до MGMT интерфейса NGFW для администраторов и служебных сервисов.
  Правило №11: запрещающее правило до MGMT интерфейса NGFW для всех

Сетевая Безопасность

Комбинирование и объединение

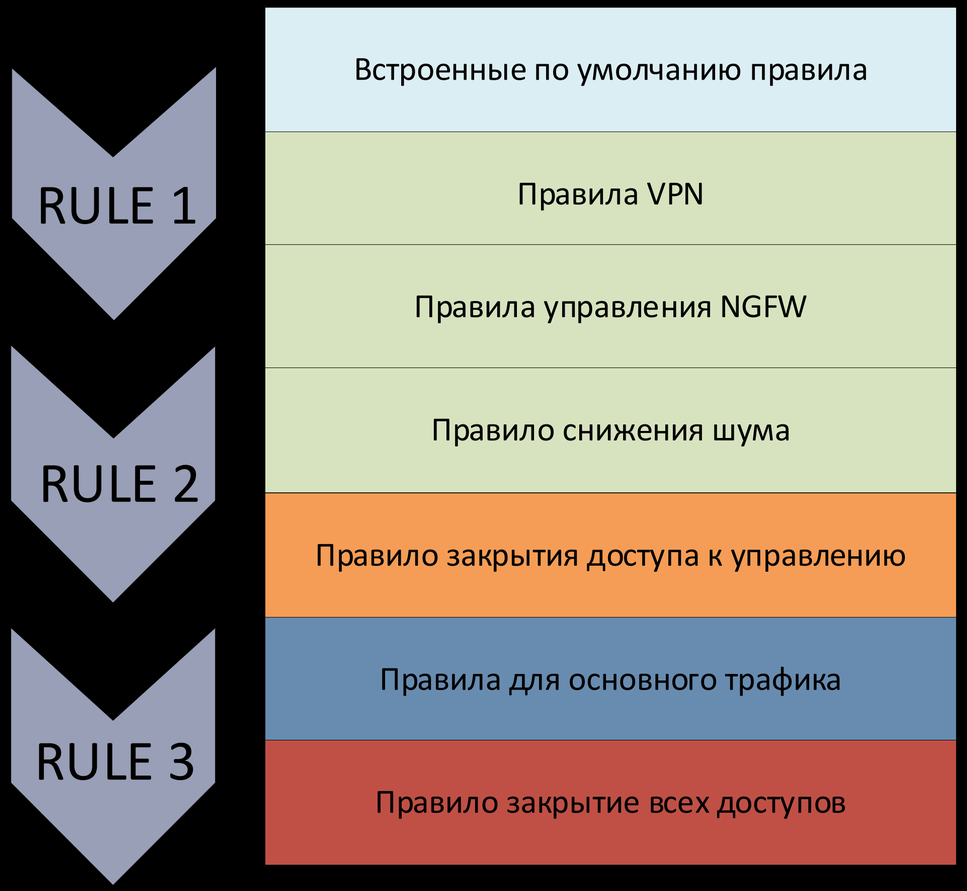
- **Комбинация параметров в правилах повышает уровень безопасности и снижает вероятность ошибок:**
  - IP и Zone для защита от спуфинга
- **- IP и/или Zone и User Group для разделения офиса и VPN, серверов и рабочих станций**

- **Объединение снижает нагрузку и отдаляет достижение лимита правил:**
  - DST по идентичной паре SRC и DST порты/приложения
- **- SRC по идентичной паре DST и DST порты/приложения**

- **Частые ошибки:**
  - при замене IP на подсеть не проверили полный список существующих серверов
  открыли избыточный доступ
- **- при объединение правил не заметили различий в парах:**
  открыли избыточный доступ или закрыли нужный
- **- пропустили Explicit Deny для «нижнего» правила**
  открыли избыточный доступ

Сетевая Безопасность

Уровни и секции



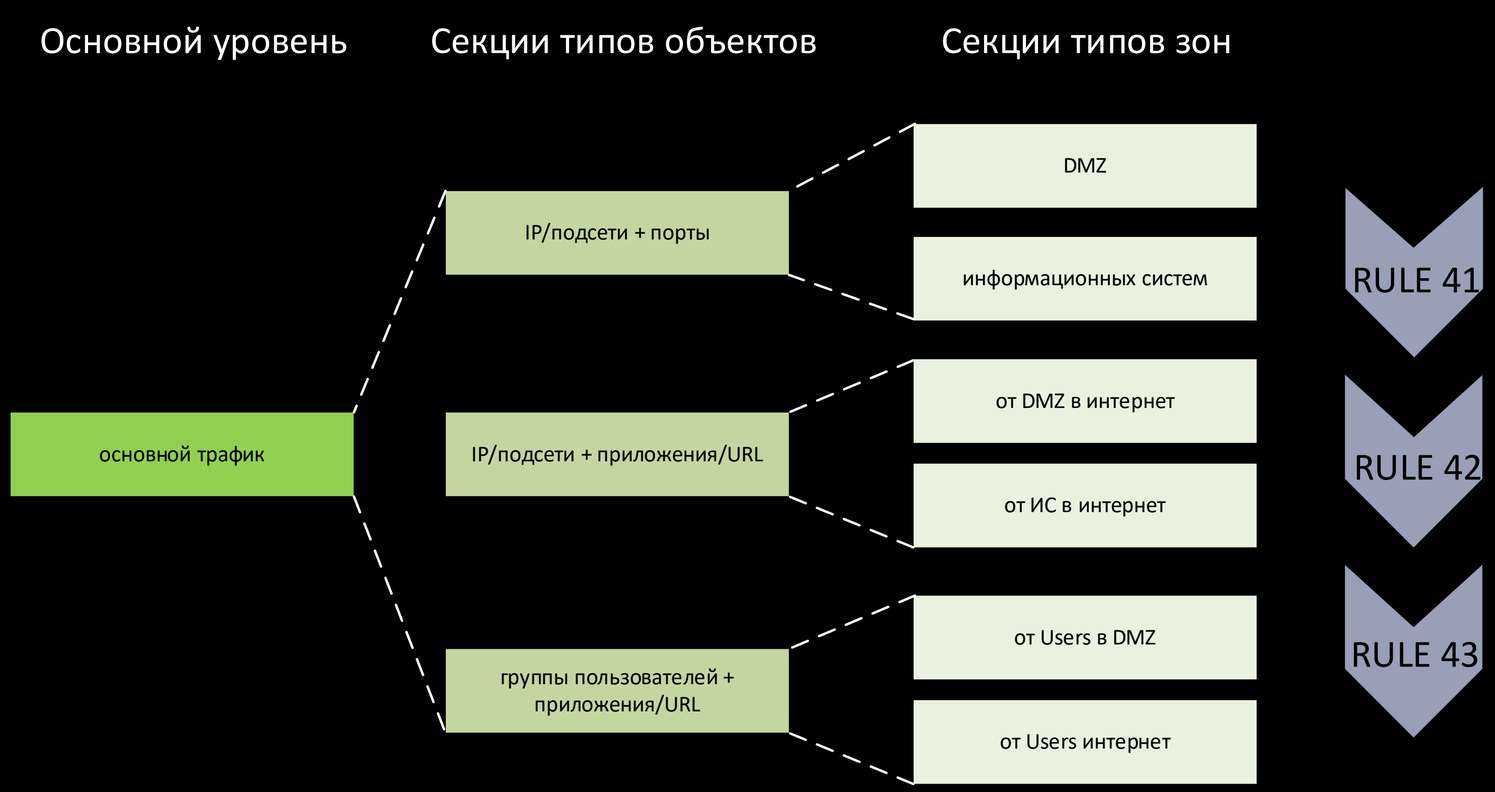
Порядок имеет значение:

1. **встроенные правила могут быть выключены**
2. **правила для работы VPN**
3. **правила для управления NGFW**
4. **правило снижение шума от «паразитного трафика»*:**
5. **правило закрытия доступа к MGMT NGFW**
6. **правила основного трафика пользователей и серверов**
7. **финальное правило запрета всего трафика**

***зависит от вендора и особенностей сети:**
udp-high-ports, domain-udp, bootp, NBT, QUIC
мультикаст трафик от роутеров

Сетевая Безопасность

Уровни и секции



Блок основных правил можно поделить на секции:

- **по сущностям, пример:**
  1. **MGMT оборудования**
  2. **серверы**
  3. **пользователи**
  4. **информационные системы и другие**

- **по функционалу, пример:**
  1. **IP/подсети + порты**
  2. **IP/подсети + APP/URL,**
  3. **группы пользователей + порты**
  4. **группы пользователей + APP/URL**

Лучше их комбинировать

Комментарии в правилах

- **Имеют ограничения на длину:**
  возможно в будущем вы смените NGFW и у нового вендора будут другие ограничения

- **Проблемы с кириллицей:**
  абракадабра при автоматической конвертации политик с одного NGFW на другой

- **Номера заявок в комментариях:**
  перестают работать на больших объемах тикетов: SD3441212, SD3451214, SD4152325…

- **Использование смысловых названий на латинице и условных обозначений:**

1. **«from_» / «to_» и комбинации**
2. **«is-*name*» для обозначения информационных систем, так же «srv», «users», «int», «ext»**
3. **«tmp_» для временных правил**
4. **номера тикетов в случаях, когда без этого нельзя**
5. **«exception» или аналог для исключений**

Сетевая
Безопасность

Влияние на производительность

Оптимизация правил
Логирование
Модули безопасности

Сетевая
Безопасность

Оптимизация правил

- **Объединение правил**
- **Использование рекомендованных вендором подходов**
- **Анализ счетчика срабатываний**
  - если у вас есть правила, по которым не было обращений в течение 3–6 месяцев, отключите их и переместите в назначенный вами раздел политики, чтобы их впоследствии можно было удалить
  - наиболее часто используемые правила стоит располагать на самом верху секции правил для основного трафика

Сетевая
Безопасность

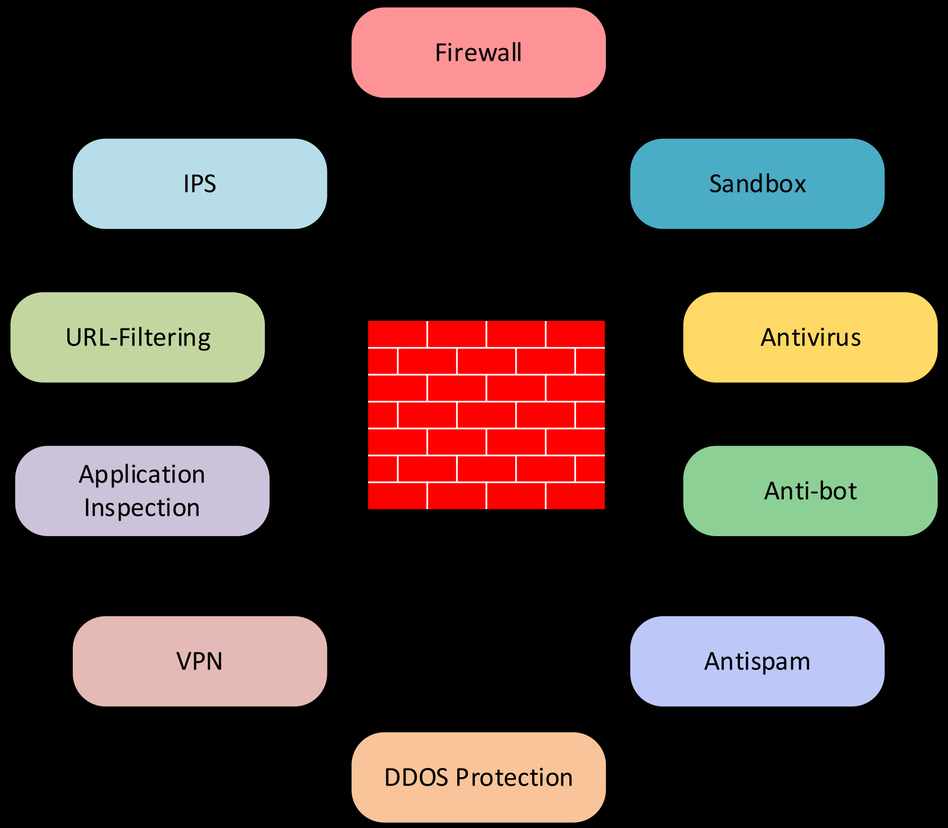
Логирование

- Отключение логирования на правиле снижения «шума»
- Включение логирование на всех правилах кроме правила снижения «шума»
- Включение ротации логов
- Включены уведомления о исчерпание дискового пространства для логов
- Включено авто-удаление старых логов при достижение порога исчерпания дисков

- Режим логирования troubleshooting снижает производительность
- Подразделения SOC просят отключить часть логов для снижения нагрузки на SIEM
  Не соглашайтесь!

Сетевая Безопасность

Модули безопасности



- **В NGFW существуют ряд модулей безопасности несвязанных напрямую с предоставлением доступа: IPS, Antivirus, Anti-bot, DLP, Sandbox**

- **Применение модулей безопасности зависит от архитектуры вашей инфраструктуры и политик безопасности**

Примеры:

1. ssl-offload выполняется на балансировщиках нагрузки, не имеет смысла анализировать трафик до снятия сертификатов SSL

- **2. правило открывает доступ только по шифрованным протоколам для взаимодействия с БД, AD, FTP**
- **3. DLP между серверами одной зоны**
- **4. Sandbox для корпоративной шары с встроенной интеграций с Sandbox**

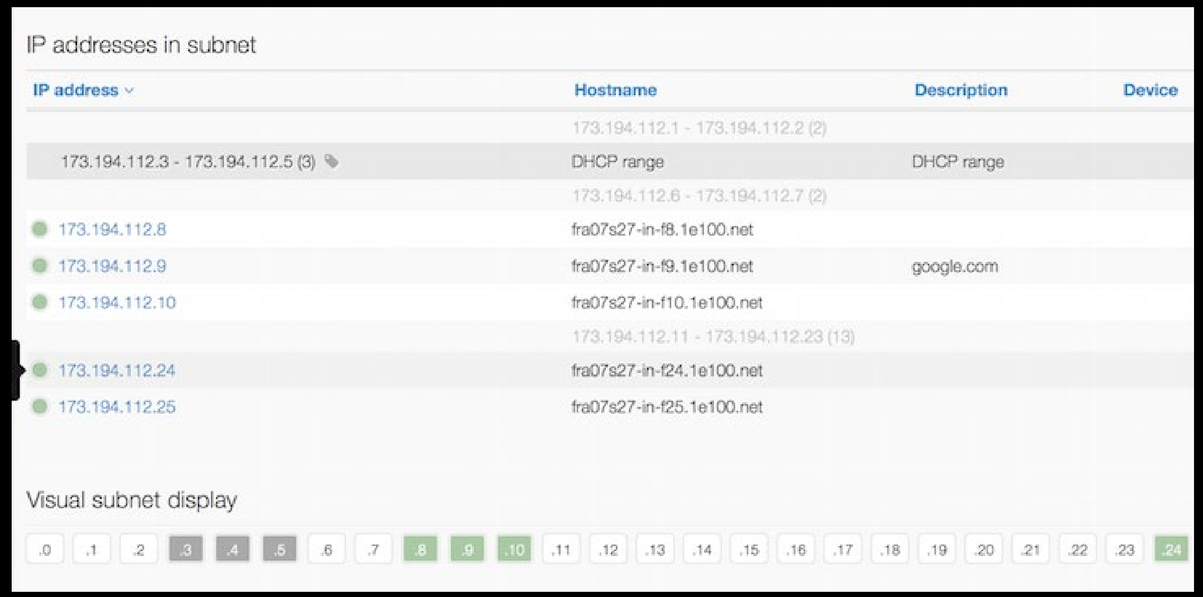
Сетевая
Безопасность

Инфраструктура как модель

Понимание активов
Связь с IT
Согласование доступов

Сетевая Безопасность

Понимание Активов

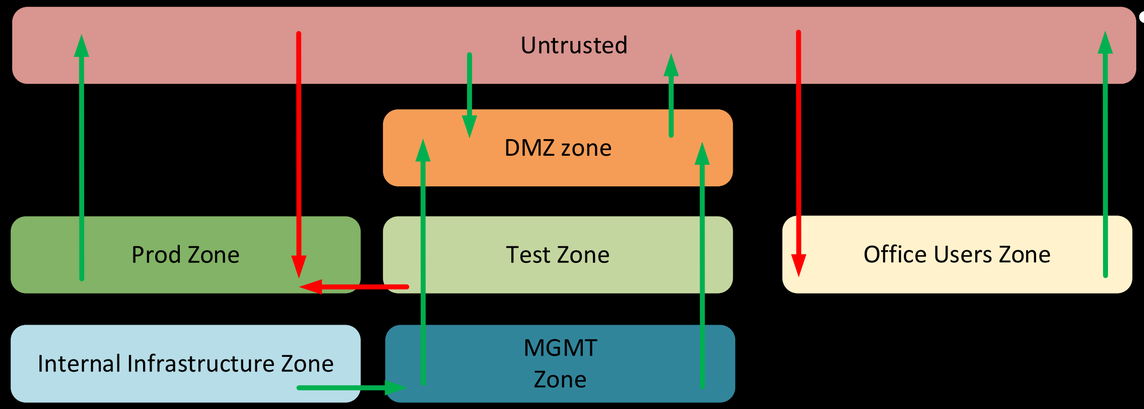


- **IPAM**
  Платформа для управления и аудита IP адресов в сети организации
  Можно добавить атрибуты зон безопасности и сред исполнения (prod, test, dev)

- **CMDB**
  Репозиторий, содержащий информацию об ИТ-инфраструктуре, используются ИТ-подразделениями
  Также можно добавить атрибуты или настроить интеграцию с IPAM

Связь с IT

Сетевая Безопасность



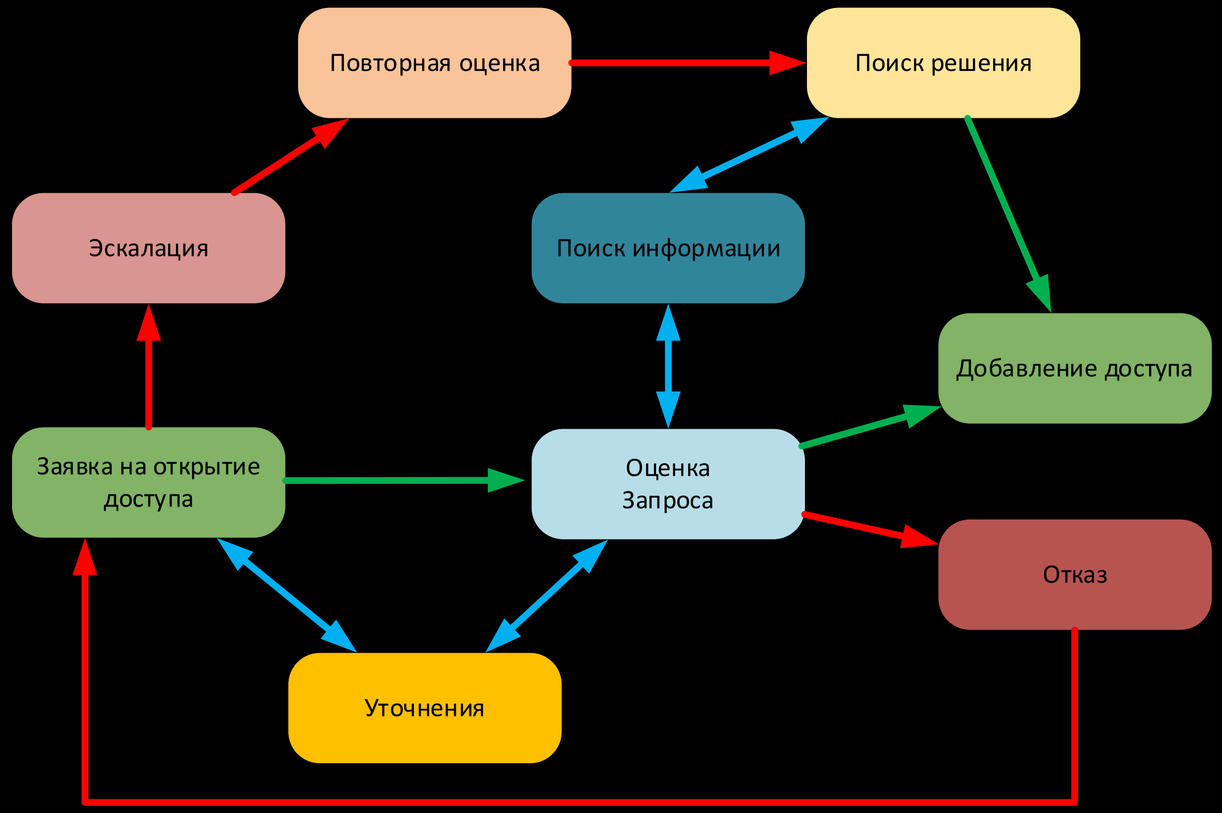
- **Wiki**
  - описание зон безопасности
  - правила взаимодействия между зонами
  - обновляемый список правил для базовых инфраструктурных сервисов
  - обновляемый список правил для базовых групп пользователей

Сервисы	IP
DNS	172.24.20.6 172.24.40.6
NTP	172.18.20.4 172.18.40.4
Exchange	10.215.20.1 10.215.20.2
AD	172.18.20.4 172.18.40.4 192.168.5.7 > 172.18.60.4
Logs	172.18.20.4 172.18.40.4

- **Отдельный процесс взаимодействия с администраторами инфрастуктурных сервисов и сетевыми инженерами:**
  - обновление списка подсетей для зон
  - обновление списка серверов базовых сервисов

Сетевая Безопасность

Согласование доступов



- **Согласование отдельных заявок**

- простота организации процесса
- про вас будут вспоминать каждый день

- экспертная оценка каждой заявки
- частые эскалации

Согласование доступов

Сетевая Безопасность

- **Согласование архитектуры**
- **Проверка заявок на соответствие целевой архитектуре**

- не требует от исполнителей заявок знаний ИБ
- ранее внесение исправлений за счет подхода shift-left

- умножаем на количество проектов
- сложность организации процесса
- не исключает случаев согласования отдельных доступов

Сетевая Безопасность

Согласование доступов

Удобная для всех форма подачи доступов

- Портал или Service Desk система
- ❑ выпадающие списки параметров:
  - тип доступа
  - контур (продуктивный, тестовый и т.п.)
  - информационная система
  - наличие согласования архитектуры
- ❑ автоматическая проверка значений на корректность ввода:
  - IP или Subnet
  - порты или сервисы
- ❑ автоматическая проверка прав на запрос точка контакта с пользователями:
  - схема карта зон
  - ссылка на Wiki
  - полезные IP адреса

- Письма
- Заполненная руками Excel таблица
- Мессенджеры

Сетевая
Безопасность

Собственная инструкция

- **Написанный с учетом:**
  - особенностей вашего NGFW
  - политик безопасности в т.ч. использования зон безопасности и модулей NGFW
  - особенностей инфраструктуры и типовых сервисов

- **Должна включать:**
  - регламент наименований и порядок создания объектов, правил и комментариев
  - иерархию правил
  - регламент проверки изменений
  - регламент «отката» изменений

- **Расширение знаний:**
  - знание Traffic flow и особенностей работы модулей и политик конкретного вендора и модели
  - результаты тестовых испытаний лабораторий
  - гайды от вендоров и профильных интеграторов

Сетевая
Безопасность

Итог

- Изучение документации и гайдов по лучшим практикам
- Создание инструкции по созданию и изменению правил на NGFW
- Осознанный подход к использованию дополнительных модулей
- Ведение актуальной схемы зон, их взаимодействия и передача информации в IT
- Получение от IT информации о типовых сервисах и изменениях в них
- Передача информации о правилах сетевых взаимодействий IT подразделениям
- Проработанный процесс согласования доступов

Сетевая
Безопасность

Благодарю за внимание!