EXPERIENCE AVAYA

Moscow

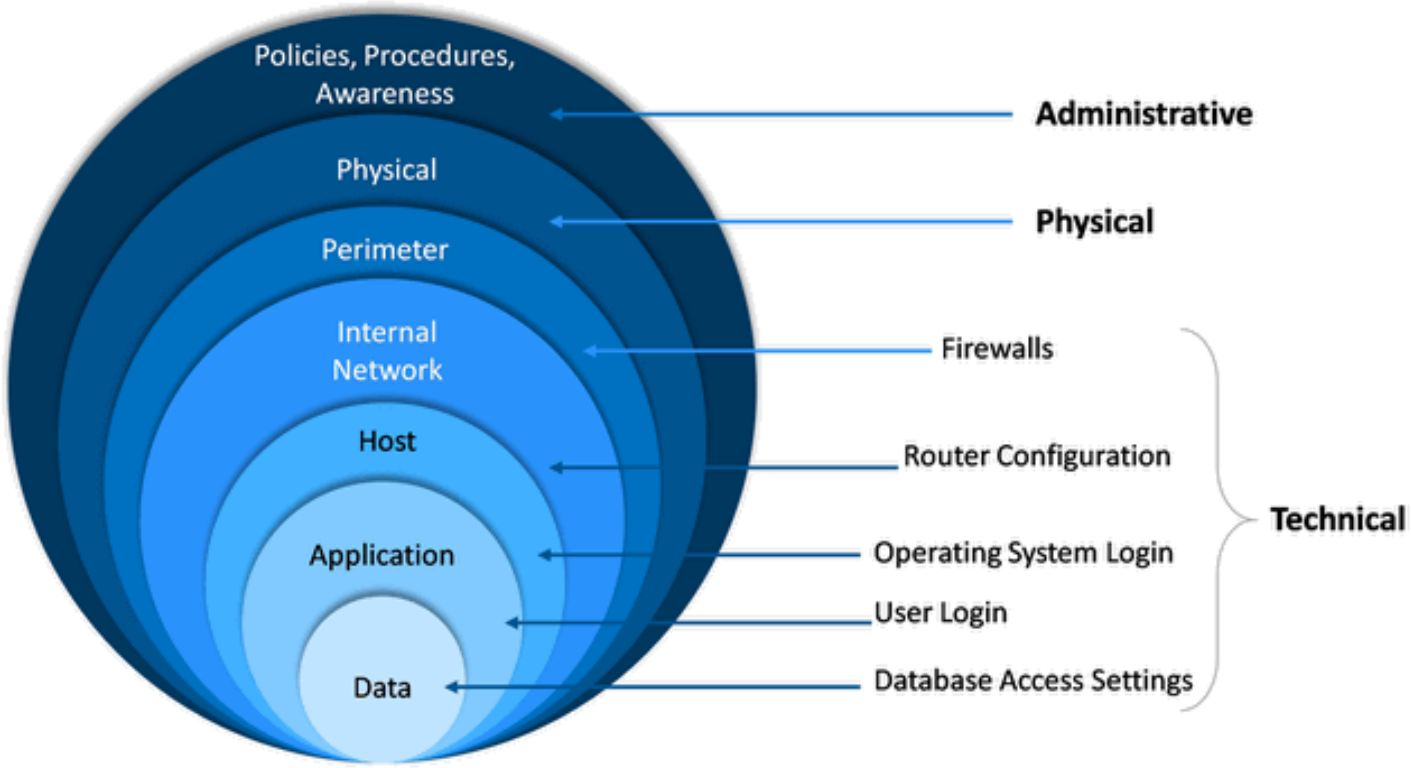
EXPERIENCE AVAYA
Moscow

Безопасное цифровое рабочее пространство: коммуникации без границ

Александр Симернин
технический консультант, Avaya

Defense in depth

- Классическая модель уровней информационной безопасности

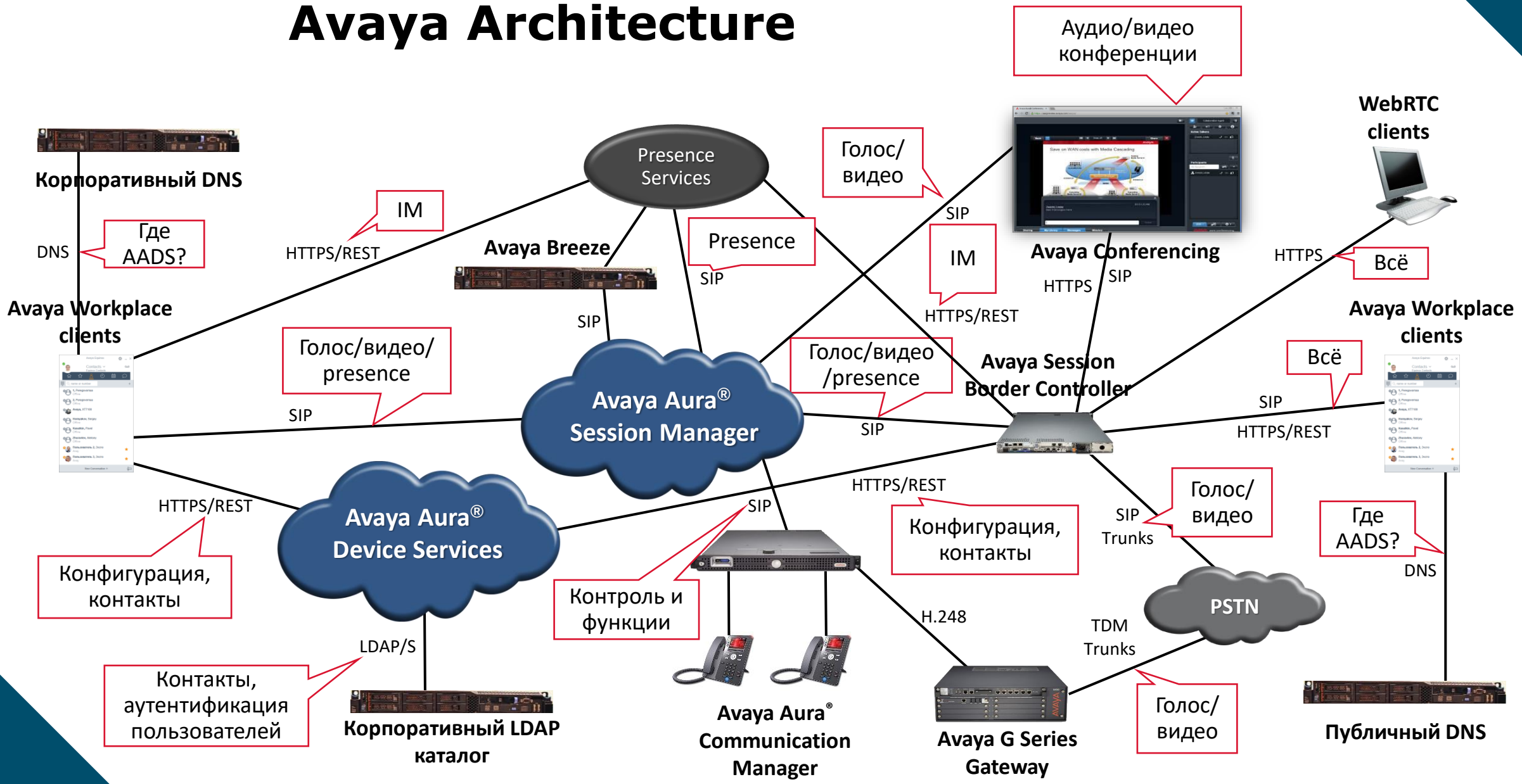


Data, Application & Host

- Защита на уровне данных обеспечивается вендором
- Защита на уровне приложений и узлов – частично обеспечивается на этапах инсталляции и эксплуатации продуктов:

  - Используйте надёжные пароли администраторов
  - Меняйте имена учётных записей администраторов по умолчанию
  - Никогда не допускайте использования слишком простых паролей пользователей (Corporate Domain и Communication Profile password)

Avaya Architecture



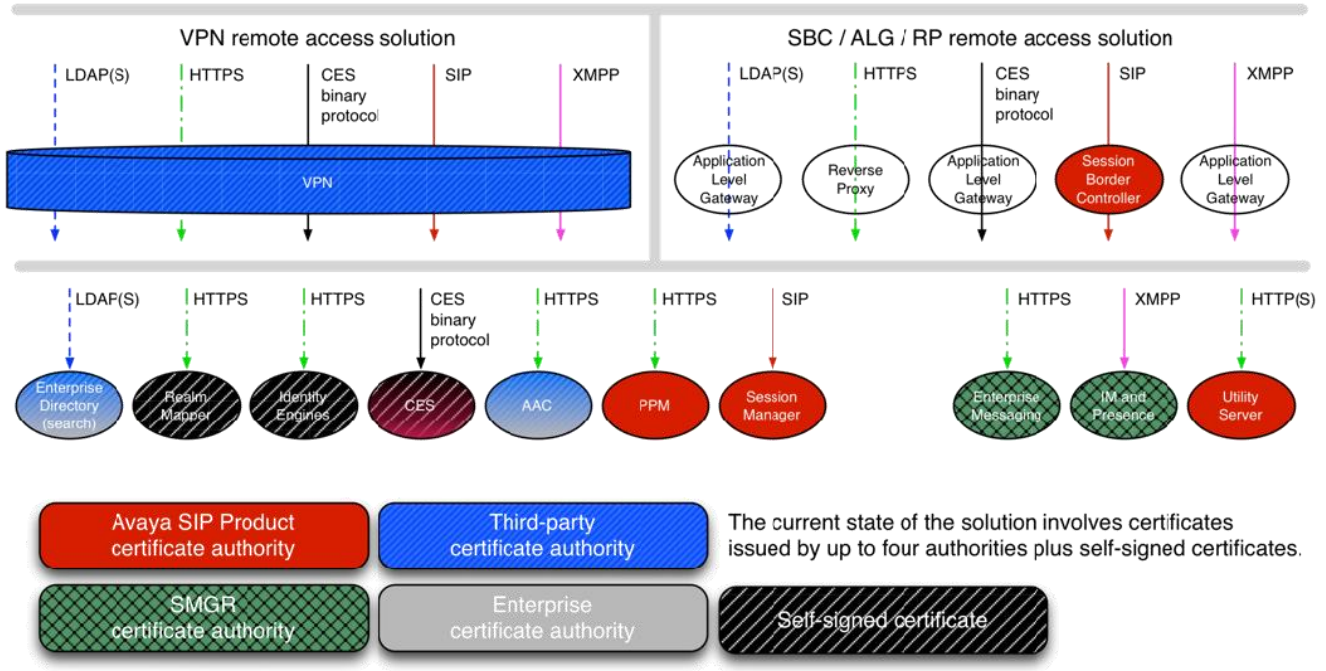
Internal Network

- Защита на уровне внутренней сети осуществляется на нескольких подуровнях:

  - Всегда выносите интерфейсы управления компонентами инфраструктуры в отдельные сети, либо VLAN, куда имеют доступ только уполномоченные администраторы (OOBM)
  - Ограничивайте доступ к компонентам инфраструктуры из пользовательских сегментов, чтобы разрешить только подключение к разрешённым сервисам
  - Используйте HIDS/NIDS для мониторинга инцидентов безопасности

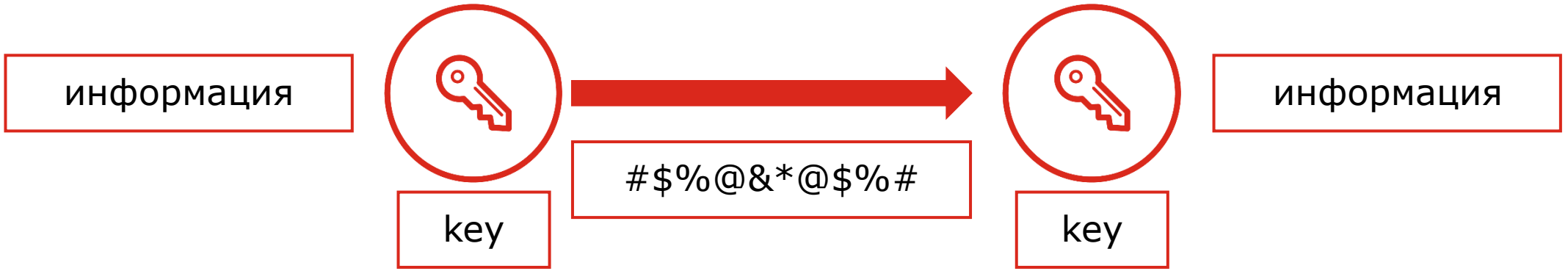
Сервисы, использующие сертификаты

- Практически все службы работают по защищённым каналам
- Шифрование обеспечивается протоколом TLS (Transport Layer Security)
- Большая часть внутренних механизмов скрыта, однако там, где речь идёт об интерфейсах управления (HTTPS), или подключении пользователей (SIPS/HTTPS), потребуется дополнительно уделить внимание настройке сервисов и клиентов для корректной и безопасной работы

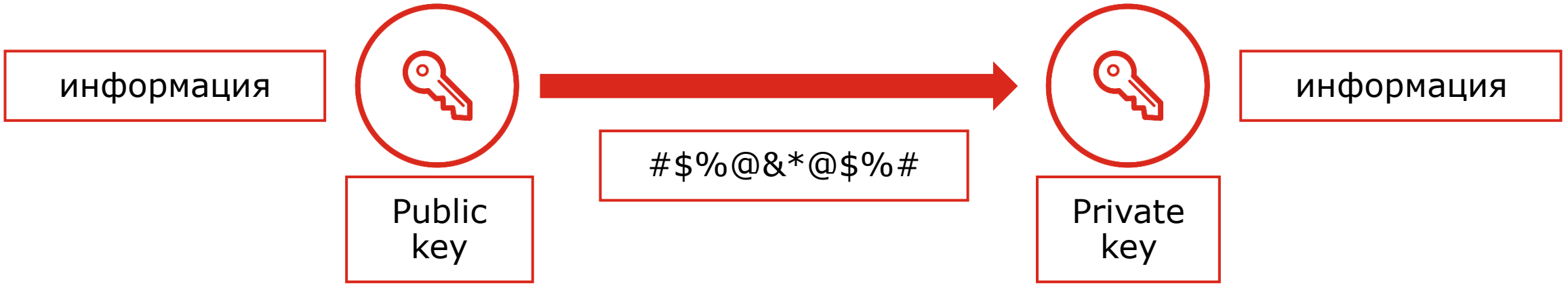


Симметричное и асимметричное шифрование

- Симметричный алгоритм использует один и тот же ключ (key) для шифрации и дешифрации данных

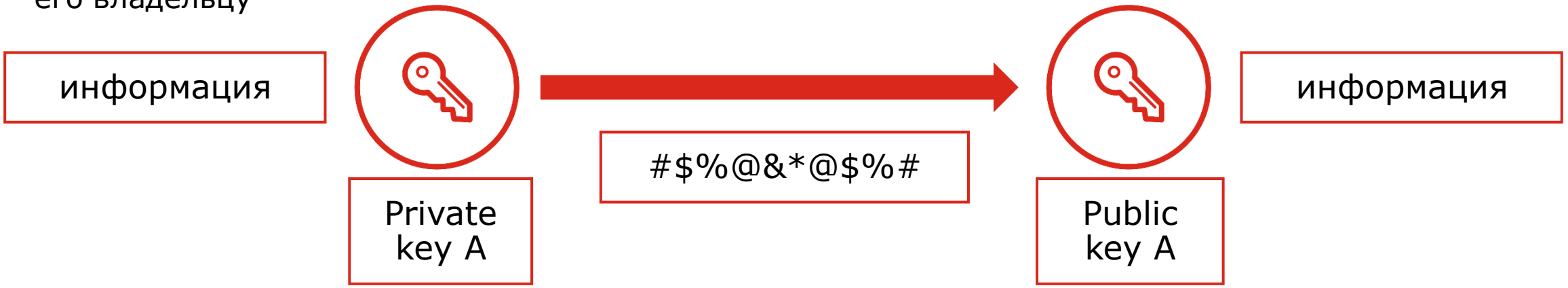


- Асимметричный полагается на два разных, но связанных друг с другом ключа: публичный и приватный (public key & private key)

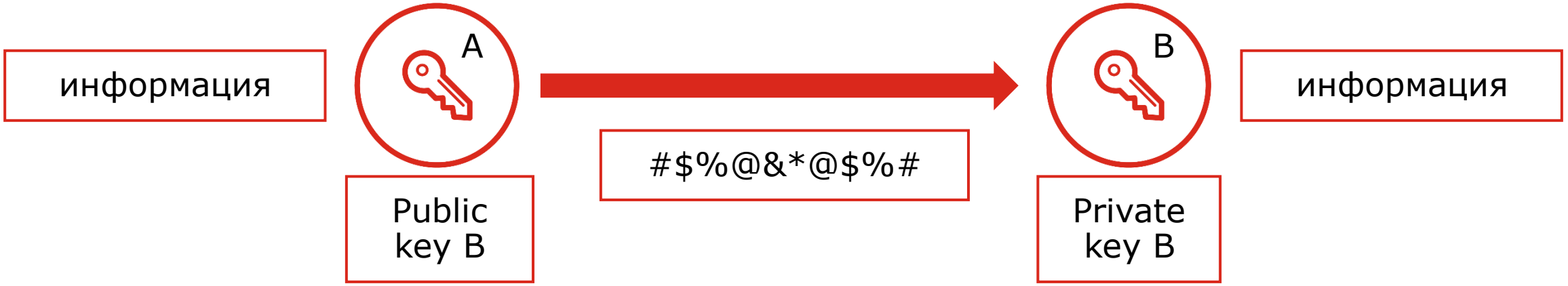


Цели использования ключей: аутентификация и шифрование

- Для аутентификации используется приватный ключ, так как он «привязан» к его владельцу



- Для шифрования сессии обычно используется публичный ключ удалённой стороны (B)



Identity certificates и Trusted CA certificates

- Identity Certificate и Trusted Certificate – термины, которые используются для определения ролей сертификатов

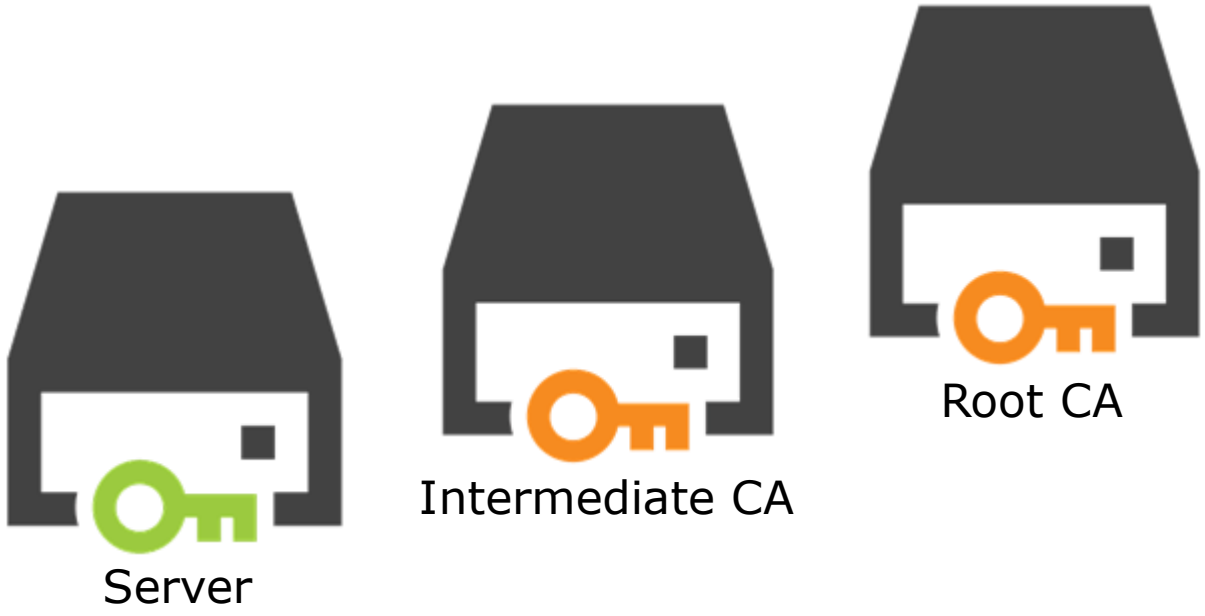
Identity Certificate – это цифровой сертификат, использующийся для определения идентичности приложения, сервиса, или устройства

Identity Certificate передаётся удалённой стороне в процессе установки TLS соединения для идентификации предъявителя

Trusted Root CA Certificate используется для проверки аутентичности сертификата, полученного от удалённой стороны в процессе установки TLS соединения

Intermediate Certification Authority

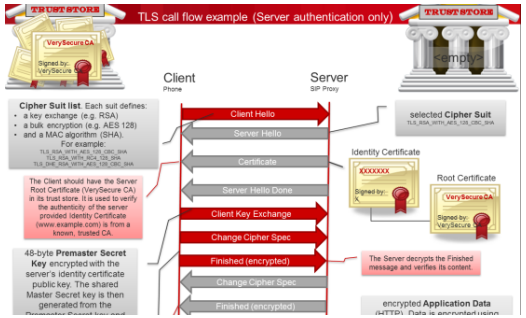
- Часто для того, чтобы уберечь корневой CA от любого рода компрометации (а это немедленно сделает всё, что он когда-либо выдавал, недостоверным), от его имени выписывают сертификат промежуточному центру, а сам корневой CA выключают
- Промежуточный CA имеет право выдавать персональные, а иногда и другие промежуточные сертификаты
- Для валидации таких персональных сертификатов серверы и клиенты обычно проверяют всю цепочку доверия (chain of trust)



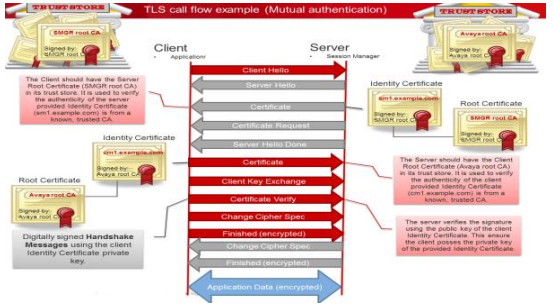
Защита трафика с использованием transport layer security (TLS)

- Все управляющие соединения между клиентами и серверами Avaya должны быть защищены с помощью протокола Transport Layer Security (TLS)
  - Все серверы и сервисы получают Identity Certificates, подписанные выбранным Центром Сертификации (CA)
    Когда клиент (например, телефон) подключается к серверу, тот предоставляет свой Identity certificate для проверки
  - Клиент проверяет, действительно ли Identity certificate был выдал Центром сертификации, которому клиент доверяет
  - Если проверка успешна, устанавливается защищенное соединение. Это Server Authentication (One-way TLS)
  - Серверы устраивают друг другу перекрёстную проверку
    Это Mutual Authentication (Two-way TLS)

Server Authentication



Mutual Authentication



Perimeter

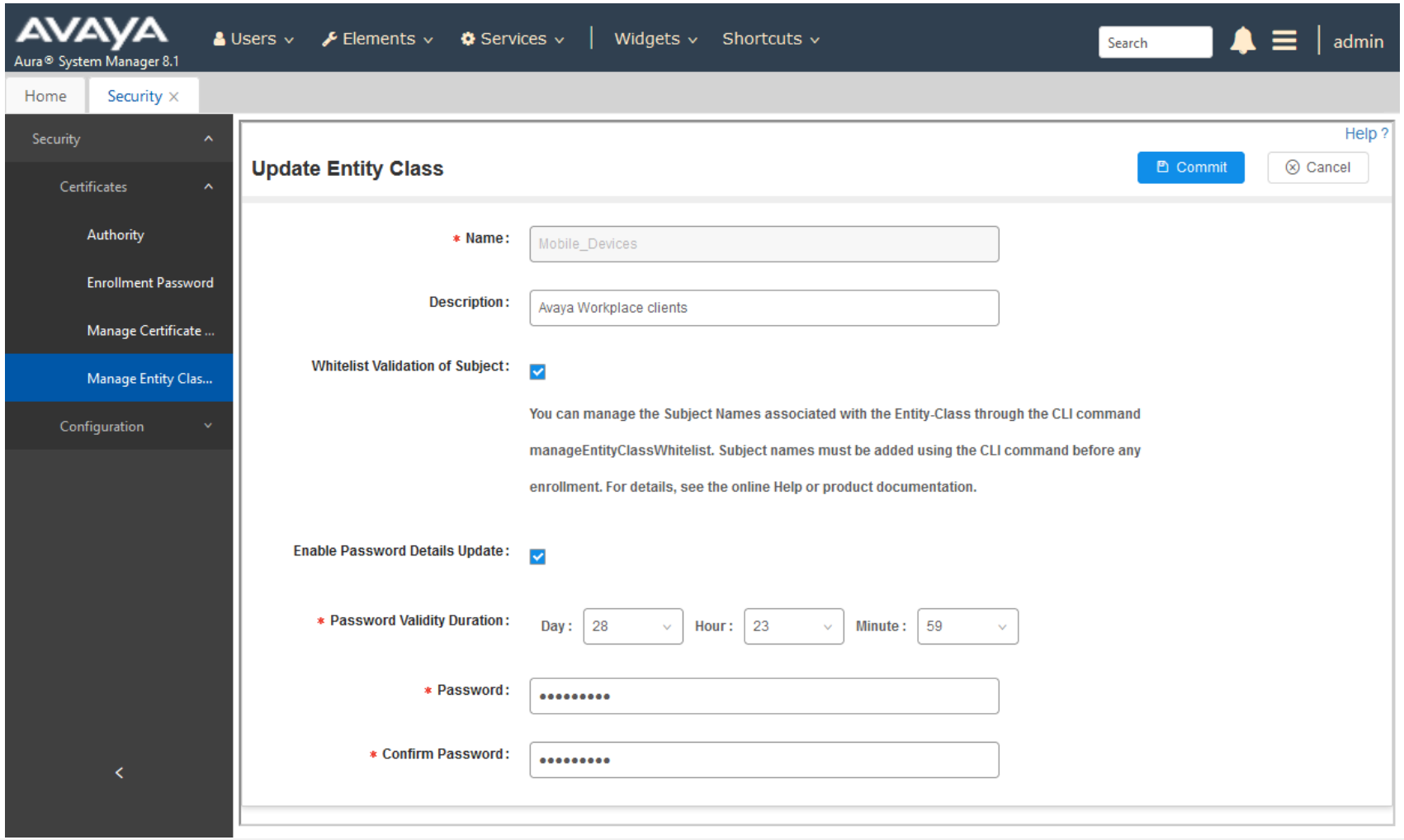
- Защита на уровне периметра корпоративной сети также осуществляется на нескольких подуровнях:

  - Используйте рекомендованные схемы подключения ASBCE с обязательным использованием Firewall
  - Используйте двустороннюю проверку сертификатов, чтобы не допустить самого факта несанкционированных подключений
  - Используйте NIDS/IPS для мониторинга инцидентов безопасности и оперативного реагирования на них

«Граница на замке»

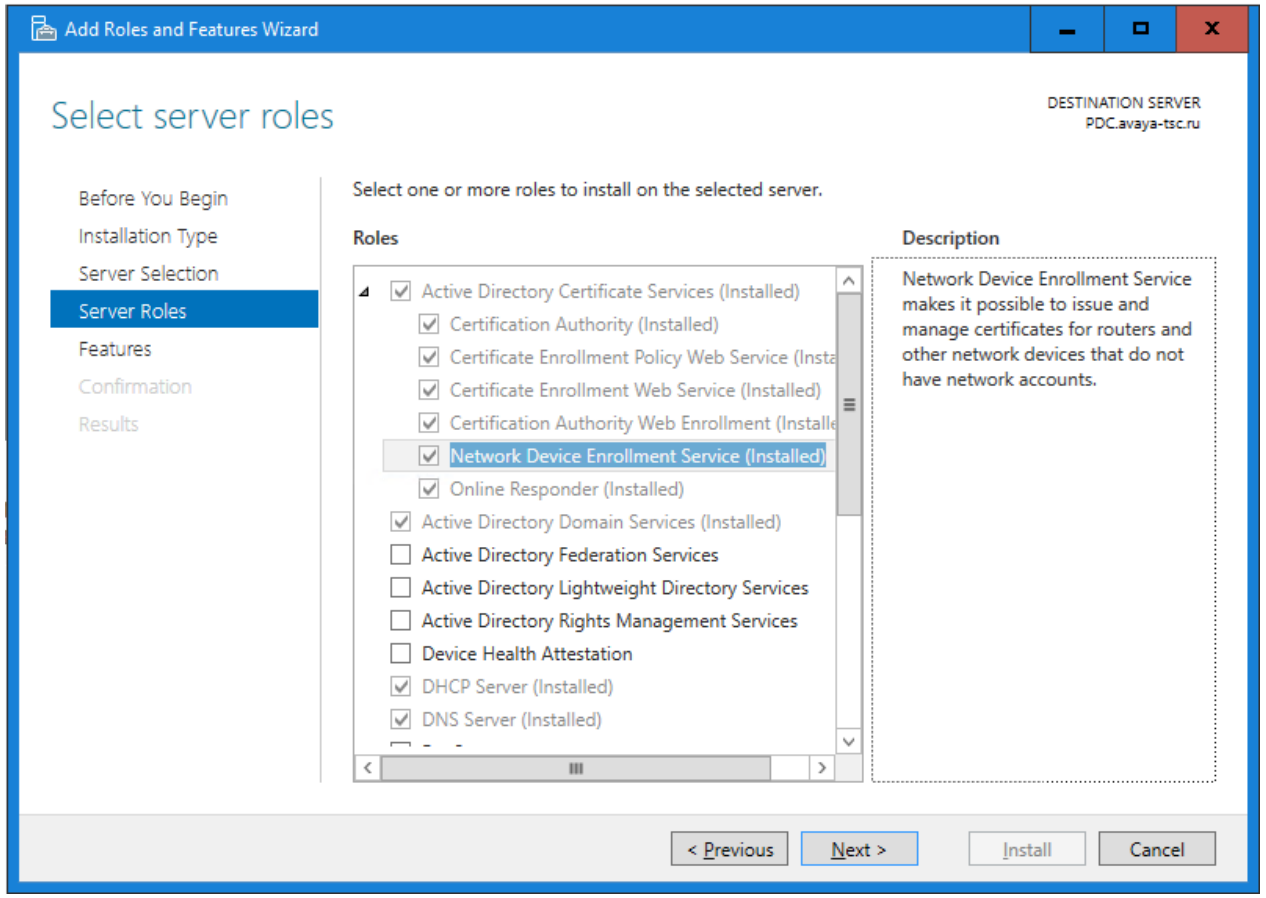
Mutual Authentication и SCEP

- SMGR умеет быть SCEP сервером для клиентов
- Пароль должен быть минимум 32 символа
- Срок действия пароля ограничен
- Для обновления сертификата пароль не нужен



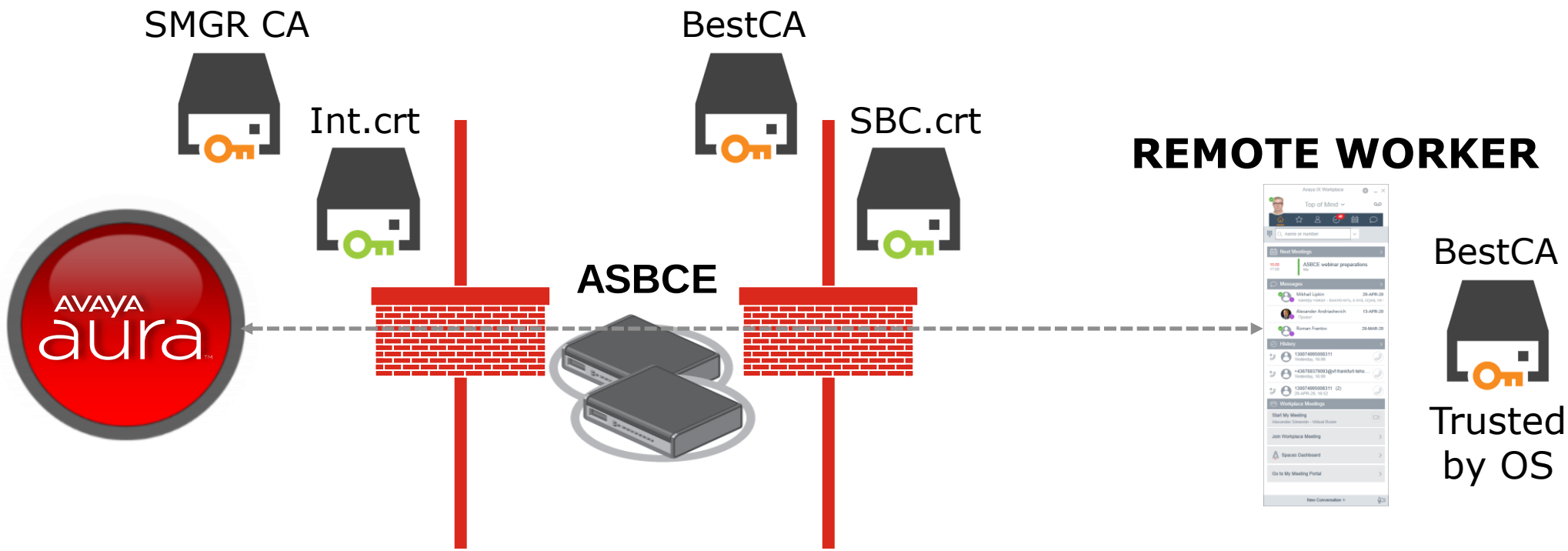
А какие ещё варианты?

- В MS AD CS есть компонент NDES
- Он также выполняет роль SCEP сервера
- Начальная настройка NDES подробно описана во множестве статей на Microsoft TechNet и сторонних ресурсах



Варианты для подключения клиентов

- Можно получить публичный сертификат от известного и доверенного коммерческого CA и установить его на ASBCE
- Удобный вариант, если настройка клиента производится сразу «снаружи», таким CA устройства доверяют сразу на уровне OS



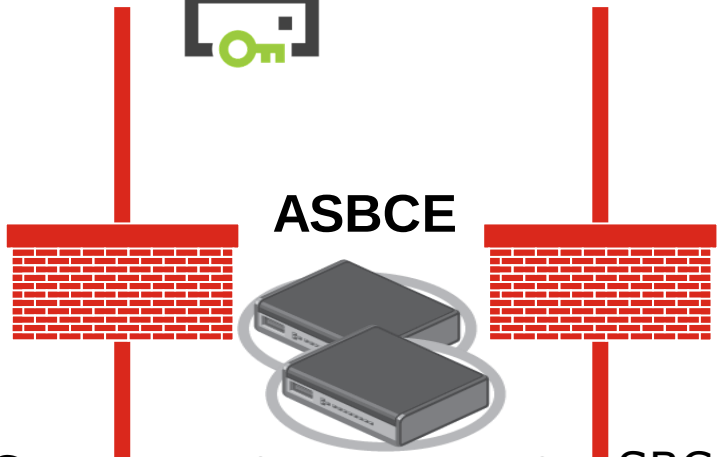
Ещё варианты для подключения клиентов

Deskphones

SMGR CA

IntA.crt

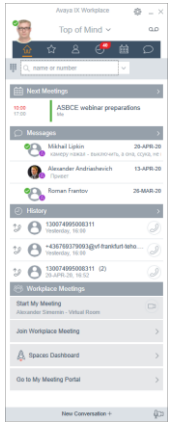
- Маленький «трюк» с DNS и клиенты внутри уверены, что работают напрямую с Aura



ASBCE

BestCA

Trusted by OS

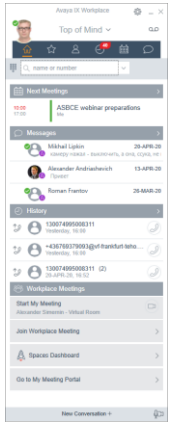


IntC.crt

BestCA

BestCA

SBC.crt



BestCA

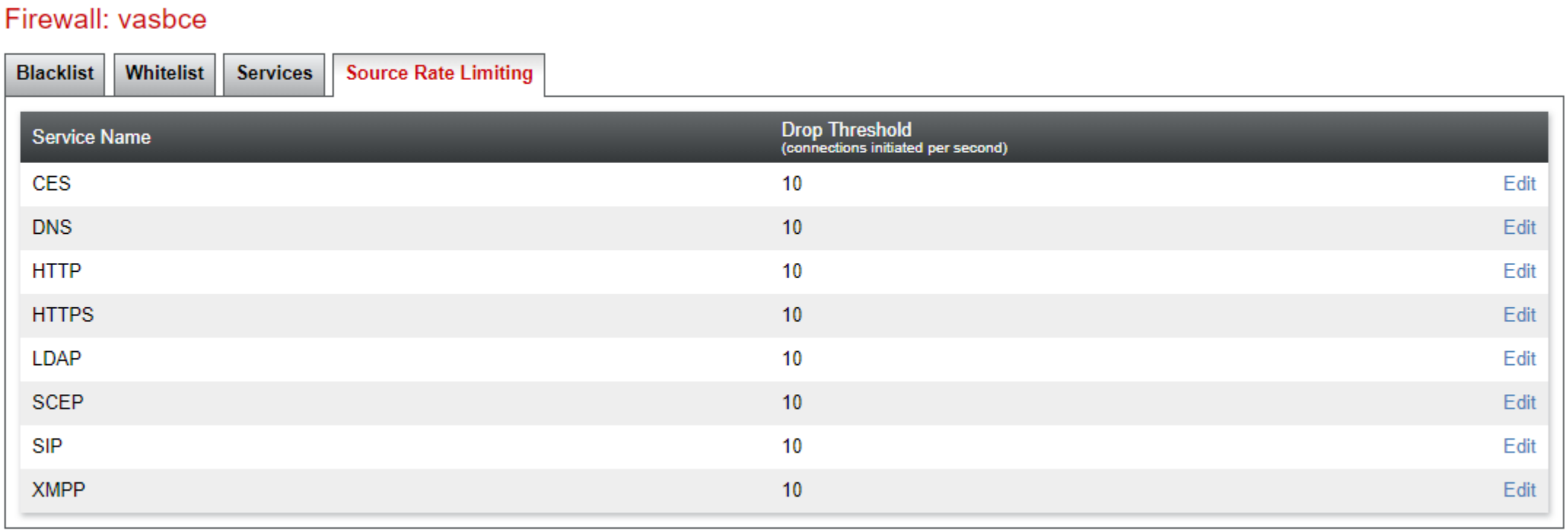
Trusted by OS

INTERNAL USERS

REMOTE WORKER

Защита периметра на уровне ASBCE

- Настраиваемые правила Firewall. Можно настраивать правила для блокировки, разрешения отдельных адресов и подсетей, а также лимиты для количества подключений в секунду для ASBCE.



Настройки защиты от DoS атак

Настройки защиты от DoS атак распределены по нескольким уровням:

- **System DoS/DDoS**: контроль сигнализации для устройств SBC, контроль частоты совершения вызовов для предотвращения попадания атак на SIP серверы, находящиеся за ASBCE.

DoS / DDoS

Single Source DoS | Phone DoS/DDoS | Stealth DoS/DDoS | Call Walking | Whitelist

Timeslot	SIP Service	SIP Method	Average Inter-Call Duration Threshold (in seconds)	Consecutive Average Inter-Call Duration Threshold Violations	Action	Block Duration (in seconds)	
Morning (0600 - 1159)	Call	INVITE	120	5	Alert Only	---	Edit
Afternoon (1200 - 1759)	Call	INVITE	120	5	Alert Only	---	Edit
Evening (1800 - 2359)	Call	INVITE	120	2	Alert Only	---	Edit
Night (0000 - 0559)	Call	INVITE	120	1	Block	3600	Edit

- **Domain DoS**: настройки, применяемые для Flow посредством Security Rules, включаемых в Endpoint Policy Groups). Пороговые значения вычисляются автоматически в зависимости от заданного количества одновременных транковых сессий и Remote Users.

SIP Servers: SessionManager

Add | Rename | Clone | Delete

Server Profiles: AAWG, SessionManager, EQ_Mgmt

General | Authentication | Heartbeat | Registration | Ping | Advanced | DoS Whitelist | DoS Protection

Template Settings

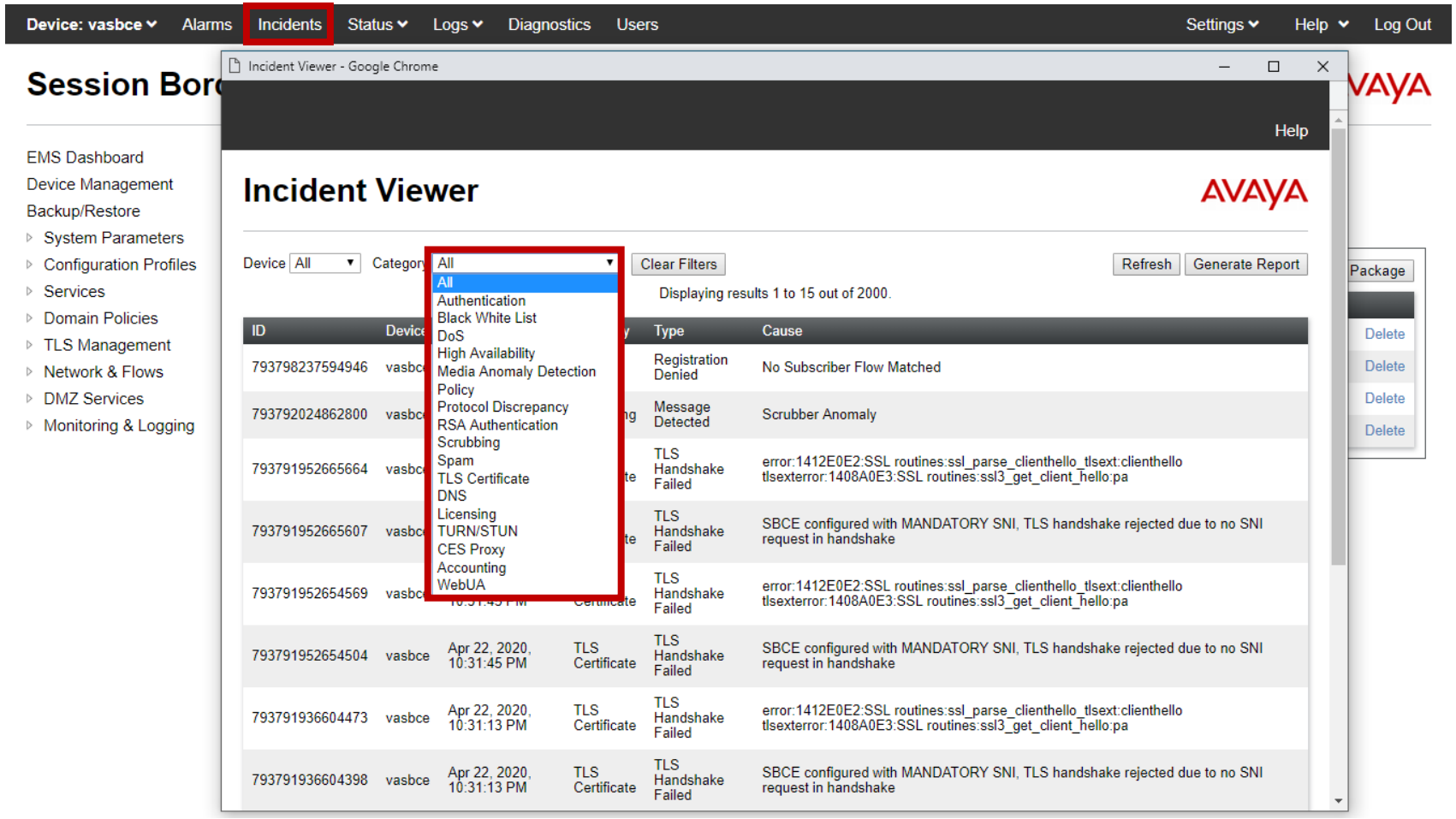
Traffic Type	Trunk Traffic and Remote Users
Max Concurrent Sessions	100
Number of Remote Users	100

Recalculate Values

SIP Service	SIP Method	Initiated Threshold (per 10 seconds)	Pending Threshold	Failed Threshold (per 10 seconds)	Action	
TOTAL	ALL	1712	171	171	Alert Only	Edit
Registrations	REGISTER	220	44	11	Alert Only	Edit
Calls	INVITE	16	3	2	Alert Only	Edit
Presence Updates	PUBLISH	220	44	11	Alert Only	Edit
Subscriptions	SUBSCRIBE	880	176	88	Alert Only	Edit
Misc	OPTIONS	220	44	11	Alert Only	Edit

Incidents

- На основании данных об инцидентах нужно принимать решения об изменении настроек безопасности.



DoS Learning

- ASBCE постоянно собирает статистику работы механизмов защиты от DoS/DDoS атак. Просмотреть все собранные данные в виде таблиц, отсортированным по SIP серверам можно в разделе Monitoring & Logging -> DoS Learning

DoS Learning: vasbce

Learned Information

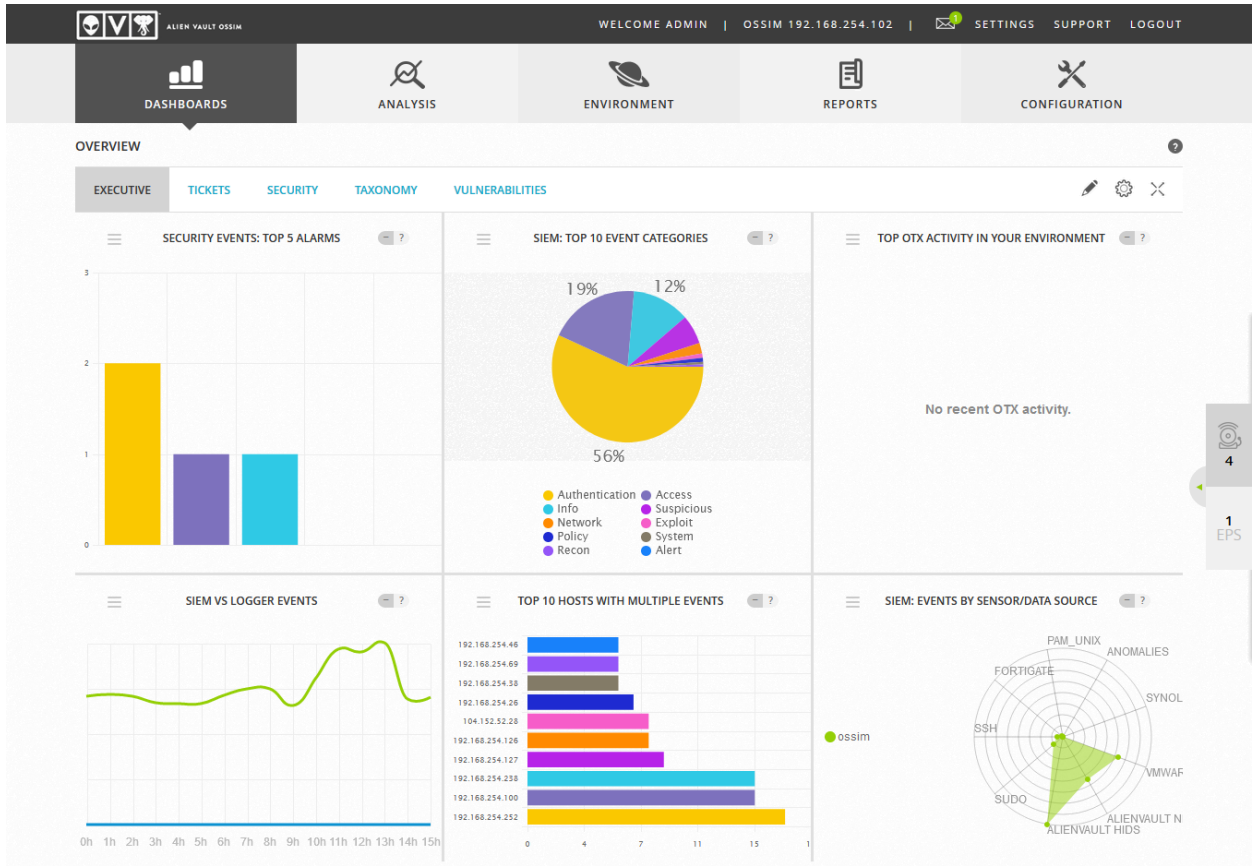
SIP Server: SessionManager

SIP Service	SIP Method	Initiated Count (per 10 seconds)	Pending Count	Failed Count (per 10 seconds)
TOTAL	ALL	0.061	0.000	0.005
Subscriptions	SUBSCRIBE	0.035	0.000	0.000
Presence Updates	PUBLISH	0.009	0.000	0.000
Calls	INVITE	0.008	0.000	0.004
Registrations	REGISTER	0.005	0.000	0.000
Misc	OPTIONS	0.004	0.000	0.000

- На основании этих данных также можно принимать решения о настройке пороговых значений и действий при их превышении.

Мониторинг с помощью IDS/SIEM

- Существует масса продуктов, как коммерческих, так и open-source
- Многие из них предлагают гибридный функционал: IDP/IPS/Vulnerability scanners/ SIEM
- Их инсталляция и настройка может занять внушительное время, однако в результате прозрачность процессов, проходящих в сети сильно повышается



Administrative

- Вероятно, самый сложный для реализации уровень защиты:

  - Внедряйте парольные политики не только на техническом уровне, но и на документальном
  - Разрабатывайте и внедряйте политики допустимого использования корпоративных ресурсов
  - Проводите обучение сотрудников с целью повышения их осведомлённости в области информационной безопасности
  - Используйте системы MDM для контроля личных устройств (BYOD)

EXPERIENCE AVAYA
Moscow

Thank you!

Александр Симернин
alexsimernin@avaya.com