

EXPERIENCE AVAYA

Moscow

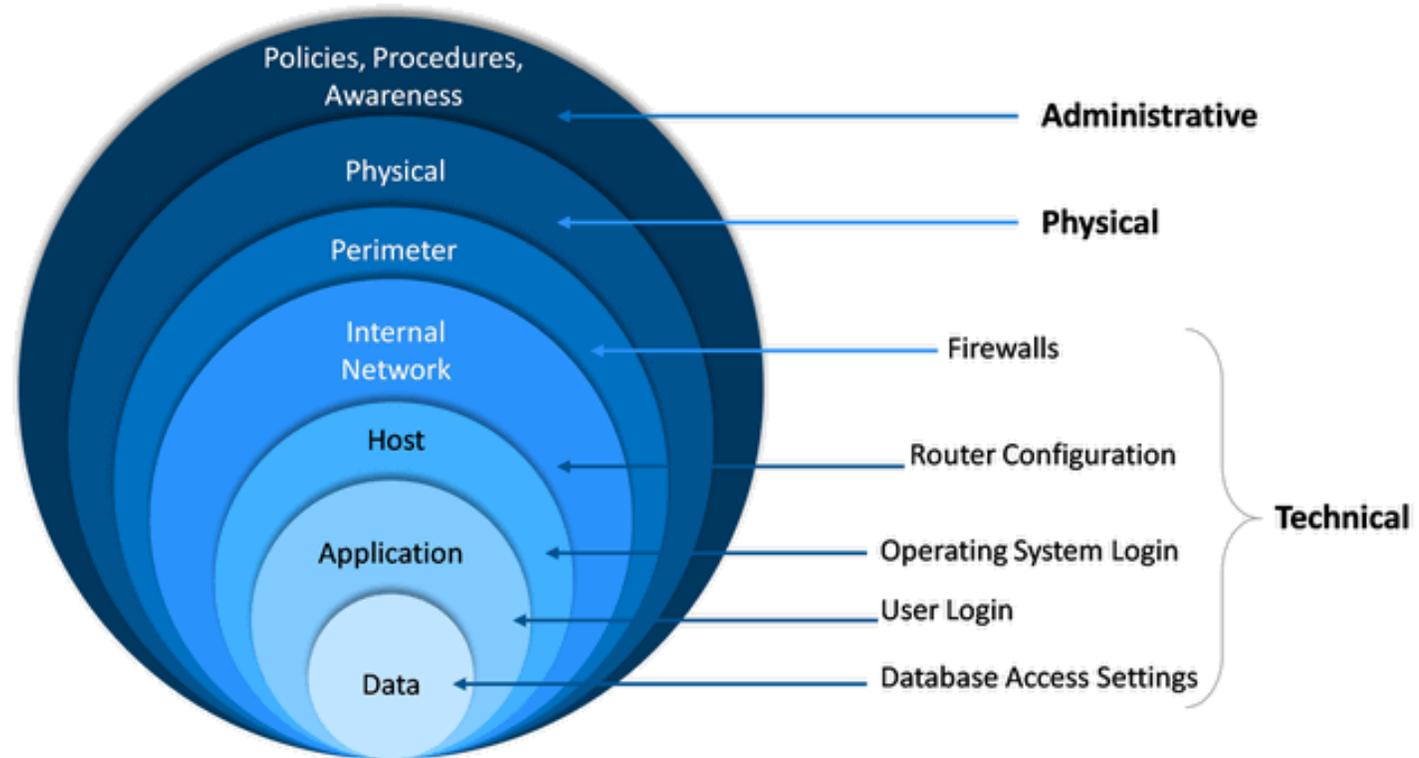


Безопасное цифровое рабочее пространство: коммуникации без границ

Александр Симернин
технический консультант, Avaya

Defense in depth

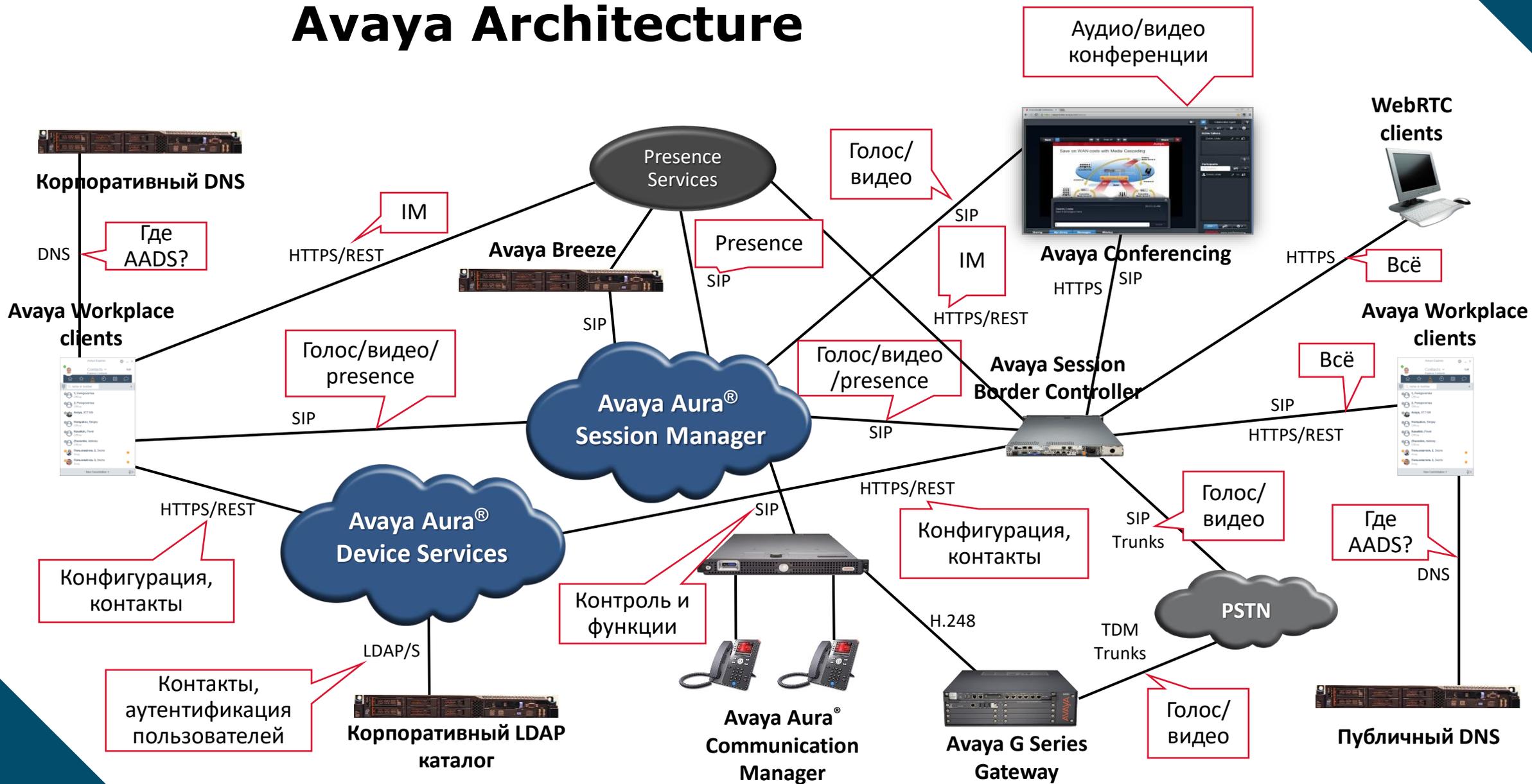
- Классическая модель уровней информационной безопасности



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

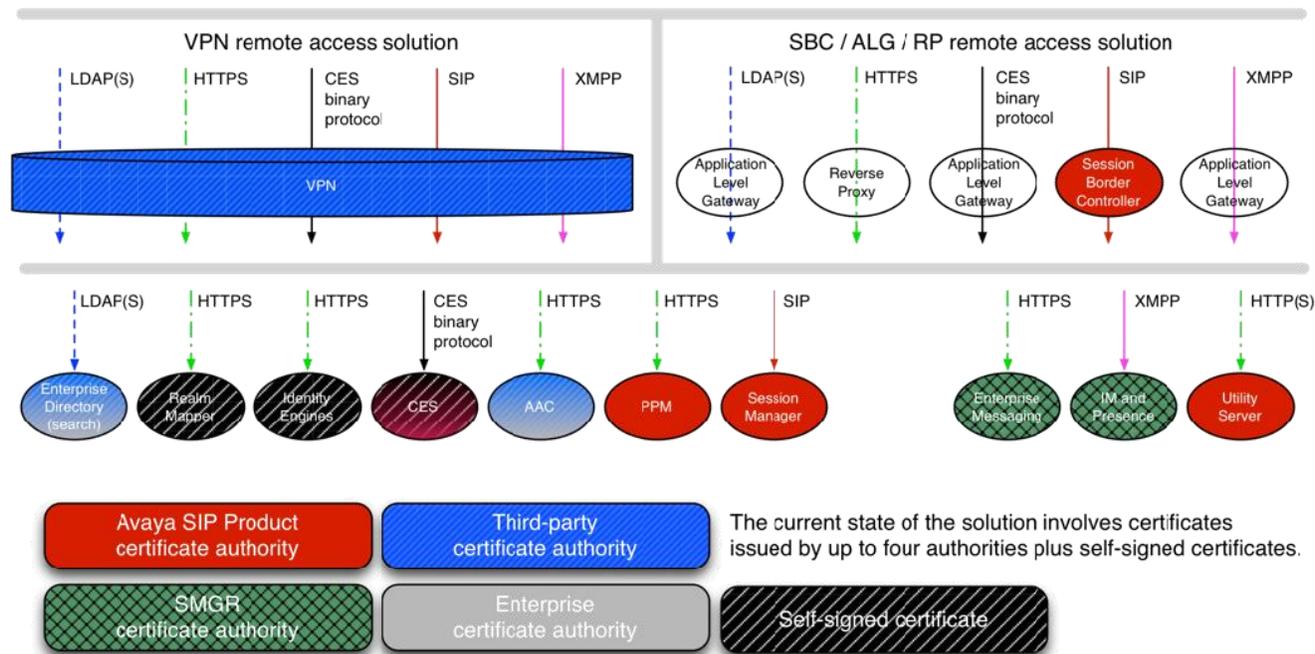


Internal Network

- 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

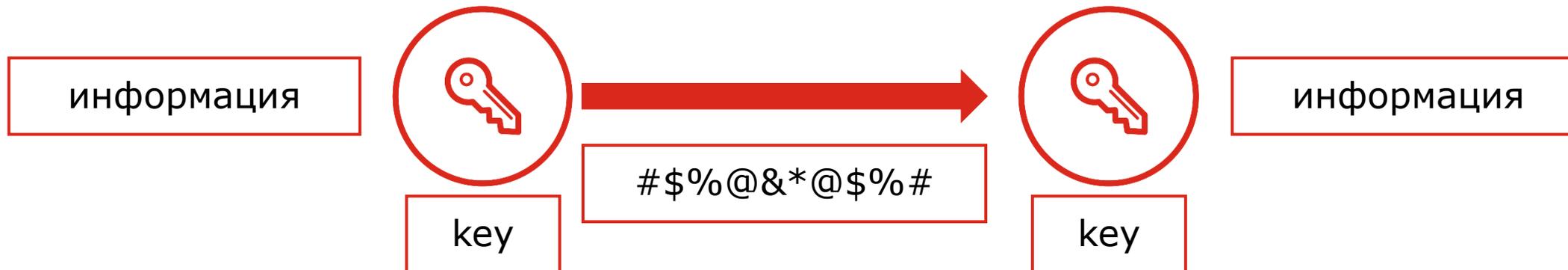
Сервисы, использующие сертификаты

- 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

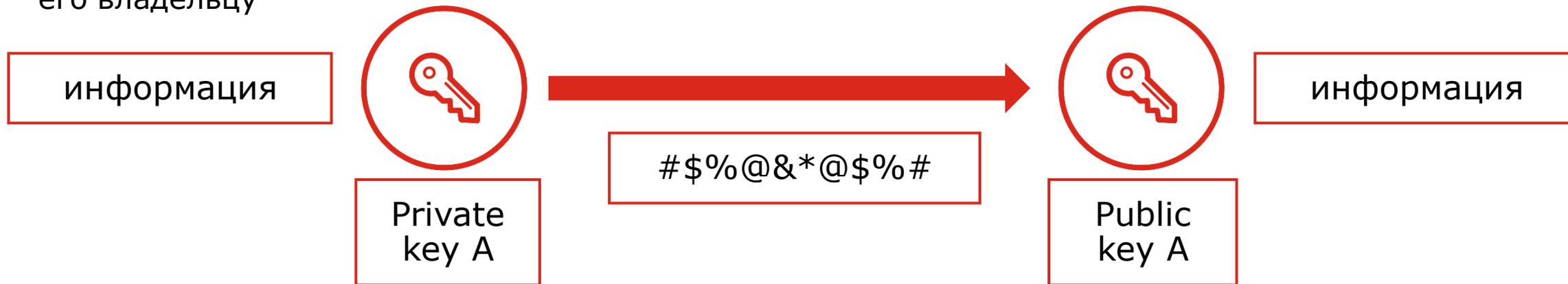


- Асимметричный полагается на два разных, но связанных друг с другом ключа: публичный и приватный (public key & private key)



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

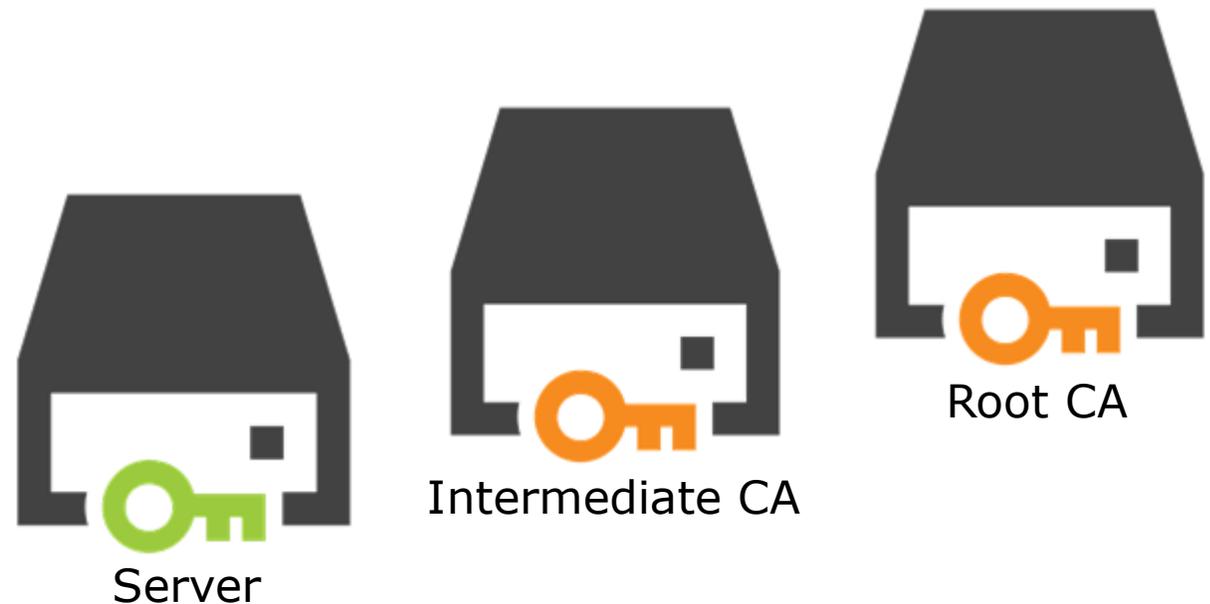
Server



Root CA

Intermediate Certification Authority

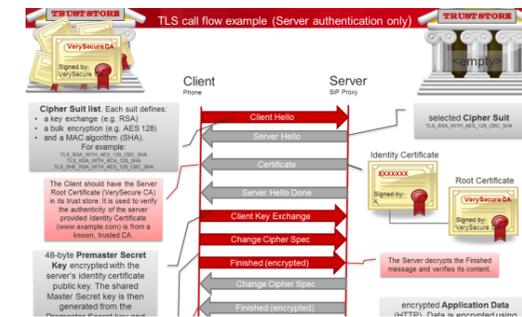
- Часто для того, чтобы уберечь корневой СА от любого рода компрометации (а это немедленно сделает всё, что он когда-либо выдавал, недостоверным), от его имени выписывают сертификат промежуточному центру, а сам корневой СА выключают
- Промежуточный СА имеет право выдавать персональные, а иногда и другие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



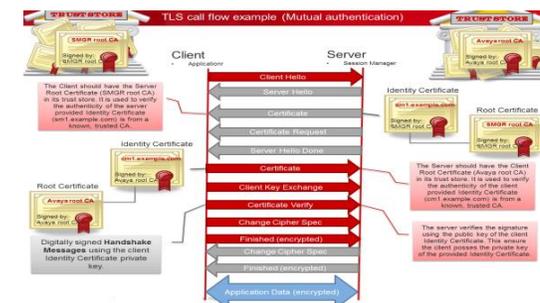
Защита трафика с использованием transport layer security (TLS)

- 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 выдан 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

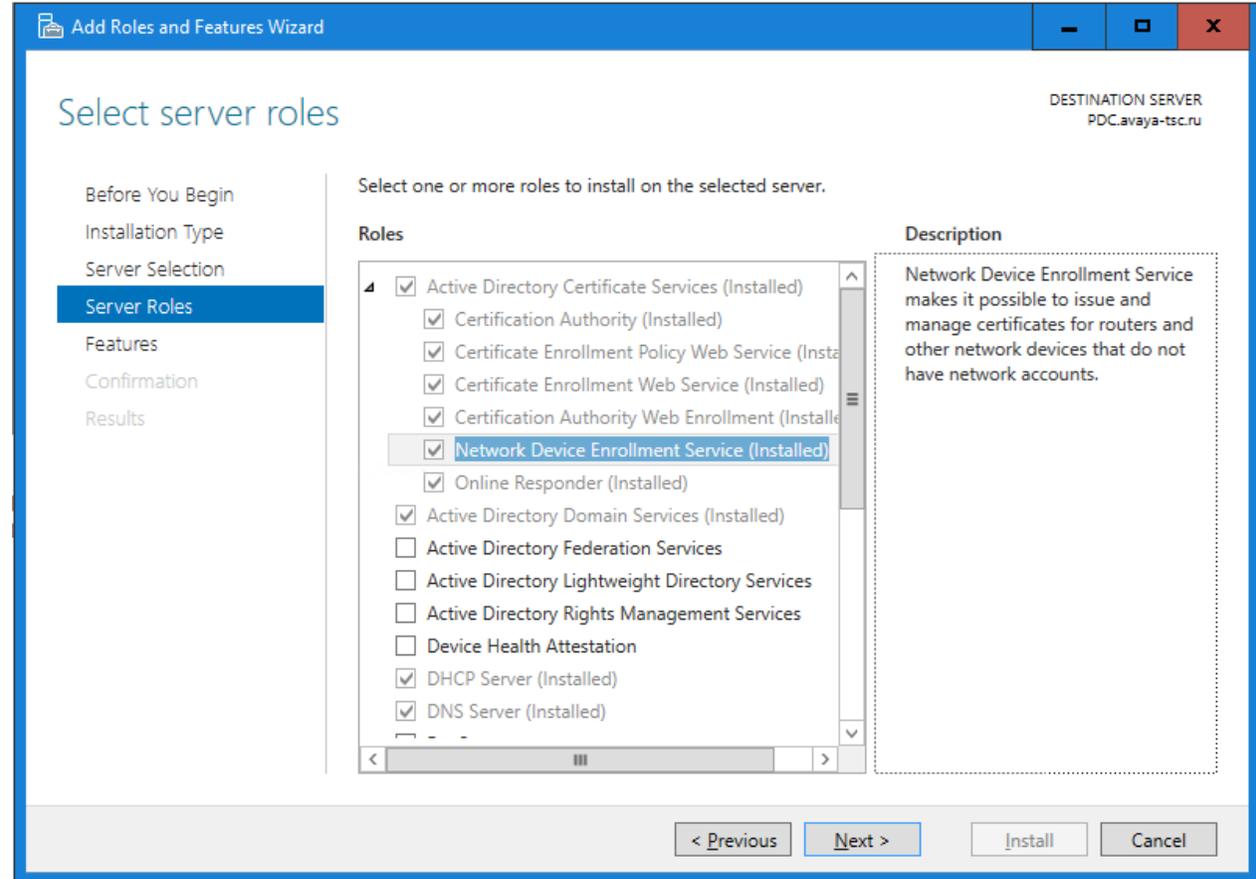
The screenshot shows the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and menu items for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The left sidebar shows a navigation menu with 'Security' selected, and sub-items like 'Certificates', 'Authority', 'Enrollment Password', 'Manage Certificate ...', 'Manage Entity Clas...', and 'Configuration'. The main content area is titled 'Update Entity Class' and contains the following fields and options:

- Name:** Mobile_Devices
- Description:** Avaya Workplace clients
- Whitelist Validation of Subject:** . Below this is a text block: "You can manage the Subject Names associated with the Entity-Class through the CLI command `manageEntityClassWhitelist`. Subject names must be added using the CLI command before any enrollment. For details, see the online Help or product documentation."
- Enable Password Details Update:**
- Password Validity Duration:** Day: 28, Hour: 23, Minute: 59
- Password:** [Redacted]
- Confirm Password:** [Redacted]

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

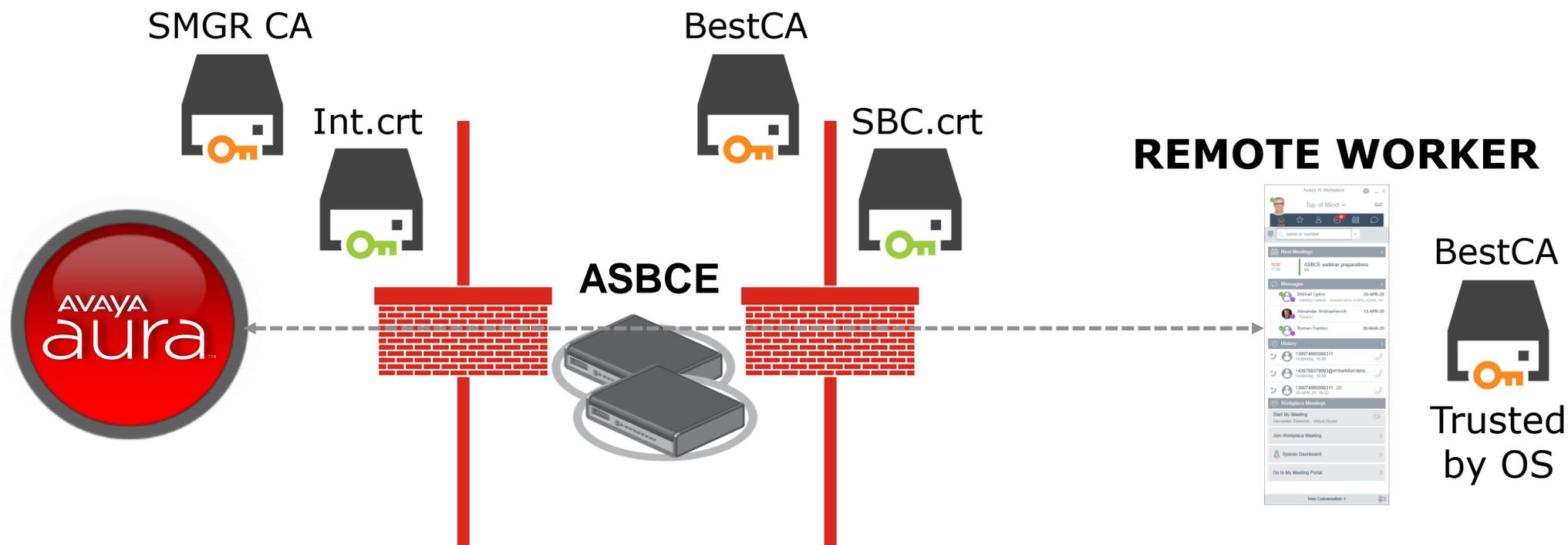
А какие ещё варианты?

- 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

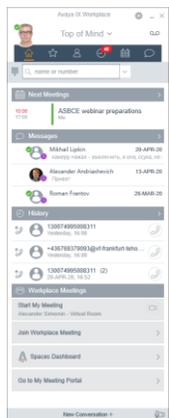


- Маленький «трюк» с DNS и клиенты внутри уверены, что работают напрямую с Aura

BestCA



Trusted by OS



INTERNAL USERS

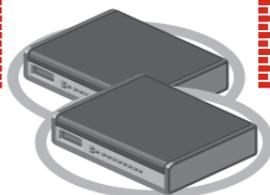
IntC.crt



BestCA



ASBCE



BestCA



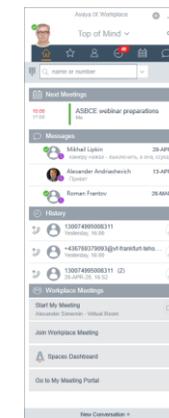
SBC.crt



BestCA



Trusted by OS



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.

Firewall: vabce

Service Name	Drop Threshold (connections initiated per second)	
CES	10	Edit
DNS	10	Edit
HTTP	10	Edit
HTTPS	10	Edit
LDAP	10	Edit
SCEP	10	Edit
SIP	10	Edit
XMPP	10	Edit

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.
- **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.

DoS / DDoS

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	---
Afternoon (1200 - 1759)	Call	INVITE	120	5	Alert Only	---
Evening (1800 - 2359)	Call	INVITE	120	2	Alert Only	---
Night (0000 - 0559)	Call	INVITE	120	1	Block	3600

SIP Servers: SessionManager

Server Profiles	General	Authentication	Heartbeat	Registration	Ping	Advanced	DoS Whitelist	DoS Protection
AAWG	Template Settings							
SessionManager	Traffic Type		Trunk Traffic and Remote Users					
EQ_Mgmt	Max Concurrent Sessions		100					
	Number of Remote Users		100					
	<input type="button" value="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	<input type="button" value="Edit"/>		
Registrations	REGISTER	220	44	11	Alert Only	<input type="button" value="Edit"/>		
Calls	INVITE	16	3	2	Alert Only	<input type="button" value="Edit"/>		
Presence Updates	PUBLISH	220	44	11	Alert Only	<input type="button" value="Edit"/>		
Subscriptions	SUBSCRIBE	880	176	88	Alert Only	<input type="button" value="Edit"/>		
Misc	OPTIONS	220	44	11	Alert Only	<input type="button" value="Edit"/>		

Incidents

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

The screenshot displays the Avaya Incident Viewer interface. At the top, there is a navigation bar with tabs for 'Device: vasbce', 'Alarms', 'Incidents' (highlighted), 'Status', 'Logs', 'Diagnostics', and 'Users'. Below this is a sidebar menu with options like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The main content area is titled 'Incident Viewer' and shows a table of incidents. A dropdown menu is open over the 'Category' column, listing various incident types such as 'Authentication', 'Black White List', 'DoS', 'High Availability', 'Media Anomaly Detection Policy', 'Protocol Discrepancy', 'RSA Authentication Scrubbing', 'Spam', 'TLS Certificate', 'DNS', 'Licensing', 'TURN/STUN', 'CES Proxy', 'Accounting', and 'WebUA'. The table lists incidents with columns for ID, Device, Date, Type, and Cause. The AVAYA logo is visible in the top right corner of the interface.

ID	Device	Date	Type	Cause	
793798237594946	vasbce		Registration Denied	No Subscriber Flow Matched	
793792024862800	vasbce		Message Detected	Scrubber Anomaly	
793791952665664	vasbce		TLS Handshake Failed	error:1412E0E2:SSL routines:ssl_parse_clienthello_tlsex:clienthello_tlsexerror:1408A0E3:SSL routines:ssl3_get_client_hello:pa	
793791952665607	vasbce		TLS Handshake Failed	SBCE configured with MANDATORY SNI, TLS handshake rejected due to no SNI request in handshake	
793791952654569	vasbce		TLS Handshake Failed	error:1412E0E2:SSL routines:ssl_parse_clienthello_tlsex:clienthello_tlsexerror:1408A0E3:SSL routines:ssl3_get_client_hello:pa	
793791952654504	vasbce	Apr 22, 2020, 10:31:45 PM	TLS Certificate	TLS Handshake Failed	SBCE configured with MANDATORY SNI, TLS handshake rejected due to no SNI request in handshake
793791936604473	vasbce	Apr 22, 2020, 10:31:13 PM	TLS Certificate	TLS Handshake Failed	error:1412E0E2:SSL routines:ssl_parse_clienthello_tlsex:clienthello_tlsexerror:1408A0E3:SSL routines:ssl3_get_client_hello:pa
793791936604398	vasbce	Apr 22, 2020, 10:31:13 PM	TLS Certificate	TLS Handshake Failed	SBCE configured with MANDATORY SNI, TLS handshake rejected due to no SNI request in handshake

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: vaspce

Learned Information

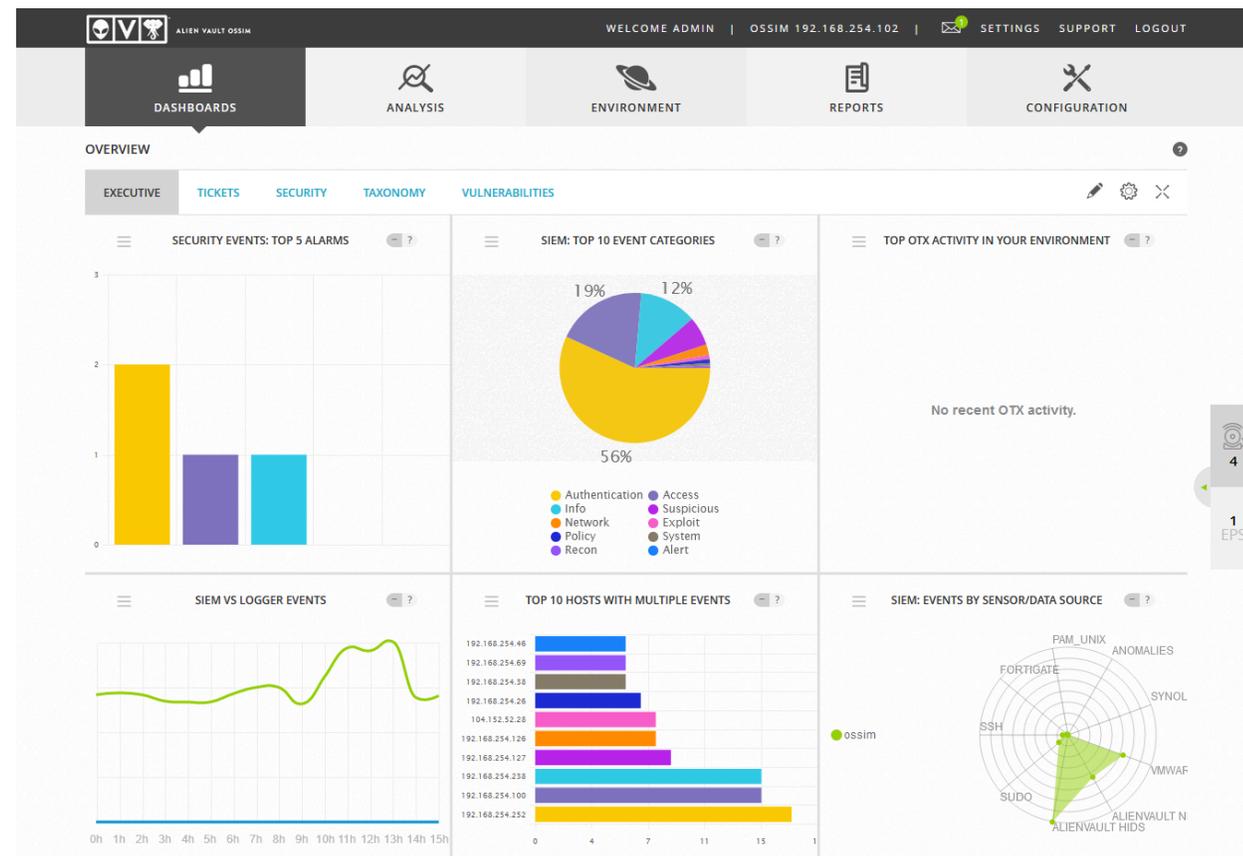
SIP Server: SessionManager

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