SBCE Безопасный доступ из публичной сети к корпоративному серверу SIP

Или как удалённому сотруднику быть на связи

AVAYA

Докладчик: Кирилл Прусов, RIM-NIHOL

Ташкент-2022

Nihol

Что такое SIP.

```
172.16.52.221:5061 —TLS→ 95.214.210.18:19125

SIP/2.0 200 OK
From: <sip:700@192.168.42.65>;tag=19258397-767b-4cd3-9b2d-7552e90aab37
To: <sip:700@192.168.42.65>;tag=cb1a3e7748dfd2cc
CSeq: 2 REGISTER
Call-ID: 619f51d2-8d98-4fd0-8fe4-05e1e0d19ef2
Contact: <sip:700@10.137.183.230:48873;transport=tls>;+av.sip.iptolerance
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: vnd.avaya.ipo
User-Agent: IP Office 11.1.2.2.0 build 20
Via: SIP/2.0/TLS 10.137.183.230:48873;branch=z9hG4bK0b8e4d9e-03bb-4caf-b0e7-34e8dec56e9d
Expires: 720
Date: Tue, 22 Nov 2022 10:10:51 GMT
Server: IP Office 11.1.2.2.0 build 20
Content-Type: application/vnd.avaya.ipo
Content-Length: 234

<ipo>
backup_ipoffice_server="ipo02.avaya.local:5061;transport=tls";
FAILBACK_POLICY="auto";
username="700";
username_twin="&0.700";
FullName="Anatoliy";
GUID="9adfd88013ad11e6a912000c29aa8d73";
onex_server="0.0.0.0";
</ipo>
```

- *SIP. Session Initiation Protocol, Протокол установления сеанса — протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи, включающего обмен мультимедийным содержимым (IP-телефония, видео и аудио-конференции, мгновенные сообщения)*
- *Этот протокол описывает, каким образом клиентское приложение (например, софт-фон) может запросить начало соединения у другого, возможно, физически удалённого клиента, находящегося в той же сети, используя его уникальное имя. Протокол определяет способ создания канала связи и согласования протоколов обмена информации между клиентами (например, протокол RTP используется для обмена голосовыми данными). Допускается добавление или удаление таких каналов в течение установленного сеанса, а также подключение и отключение дополнительных клиентов (то есть предусмотрена конференц-связь, когда допускается участие в обмене более двух сторон). SIP также определяет порядок завершения сеанса.*

Nihol

Разработчики протокола SIP

- Разработкой SIP занималась организация IETF MMUSIC Working Group. Протокол начал разрабатываться в 1996 году Хенингом Шулзри (Henning Schulzrinne, Колумбийский университет) и Марком Хэндли (Университетский колледж Лондона). В ноябре 2000 года SIP был утверждён как сигнальный протокол проекта 3GPP и основной протокол архитектуры IMS (модификация 3GPP TS 24.229). SIP — один из протоколов, активно использующихся для передачи речи через интернет (Voice over IP), наряду с H323.

Архитектура сети

- Протокол SIP имеет клиент-серверную архитектуру.

- Клиент выдаёт запросы, с указанием того, что он хочет получить от сервера. Сервер принимает и обрабатывает запросы, выдаёт ответы, содержащие уведомление об успешности выполнения запроса, уведомление об ошибке или информацию, запрошенную клиентом.

- Обслуживание вызова распределено между различными элементами сети SIP. Основным функциональным элементом, реализующим функции управления соединением, является абонентский терминал. Остальные элементы сети могут отвечать за маршрутизацию вызовов, а иногда служат для предоставления дополнительных сервисов

Сервер телефонии опасно публиковать в публичной сети

- SIP protocol всегда на прицеле у злоумышленников

- DoS/DDoS атака поможет нарушить не только работу удалённых сотрудников но и персонала на местах

- Компрометация голосовых данных может нанести большой ущерб бизнесу

TCP	5061	SIP
TCP	5222	XMPP
TCP	9443	WebRTC, REST, XMPP
TCP	7443	BOSH/XMPP
TCP	80	HTTP
TLS	443	HTTPS
UDP	3478	STUN
UDP	50000-55000	RTP relay
UDP	35000-40000	RTP media

Nihol

ASBCE?

Session Border Controller for Enterprise (SBCE) (Legacy)

by Avaya

"Deployment was easy but the updates were a bit complicated, depend of the version."

For general is a excellent product, it have a friendly platform for configuration and deployment, Avaya have a lot of information and documentation to bring solution. The mobile and sip trunk services ...

Cisco Unified Border Element (CUBE)

by Cisco

"cube experience"

we have just integrated Cube gateway into our systems.It is working high performance and its structure is very clear ..

Oracle Communications Session Border Controller

by Oracle

"Oracle SBCs - The gateway to our Business voip customers."

Oracle's Session border controllers are the gateway to our business VoIP customers. It's used on all our flagships products like IP flex reach, VDNA and AVOICS.

Mediant

by AudioCodes

"Solid SIP endpoints and gateways"

solid devices with lots of customizations, need to have a good understading of SIP protocol before you deal with these devices

Sonus SBC 7000 Series

by Ribbon Communications

"Works as designed and has strong support"

Vendor is very responsive to issues and it's nice to have a dedicated support team (at the management level anyway)

Nihol

Тип	Общественный
Торгуется как	Нью -йоркская фондовая биржа : АВЬЯ Компонент Russell 2000
Промышленность	Технологии
Предшественник	Люсент Технологии
Основан	2000 ; 22 года назад
Главное управление	Дарем, Северная Каролина,Соединенные Штаты
Обслуживаемая площадь	Мировой
Ключевые люди	Алан Масарек (генеральный директор) Киран Дж. МакГрат (финансовый директор)
Товары	Цифровые коммуникационные продукты, услуги
Доход	▲ 2,97 миллиарда долларов США (2021 г.)
Операционный доход	▲ 180 миллионов долларов США (2021 г.)
Чистая прибыль	▲ −13 миллионов долларов США (2021 г.)
Всего активов	▼ 5,99 миллиарда долларов США (2021 г.)
Общий капитал	▲ 392 миллиона долларов США (2021 г.)

В 1995 году Lucent Technologies была выделена из AT&T , а затем Lucent выделила собственные подразделения в попытке реструктурировать свои борющиеся операции.

Затем в 2000 году Avaya была выделена из Lucent как отдельная компания (Lucent объединилась с Alcatel SA в 2006 году, став Alcatel-Lucent , которая, в свою очередь, была куплена Nokia в 2016 году). С 2000 по 2007 год она оставалась публичной компанией. В октябре 2007 года Avaya была приобретена двумя частными инвестиционными компаниями, TPG Capital и Silver Lake Partners , за 8,2 миллиарда долларов.

19 января 2017 года Avaya подала заявление о банкротстве в соответствии с главой 11

15 декабря 2017 года она снова стала публичной компанией, торгующейся под биржевым кодом AVYA на NYSE.

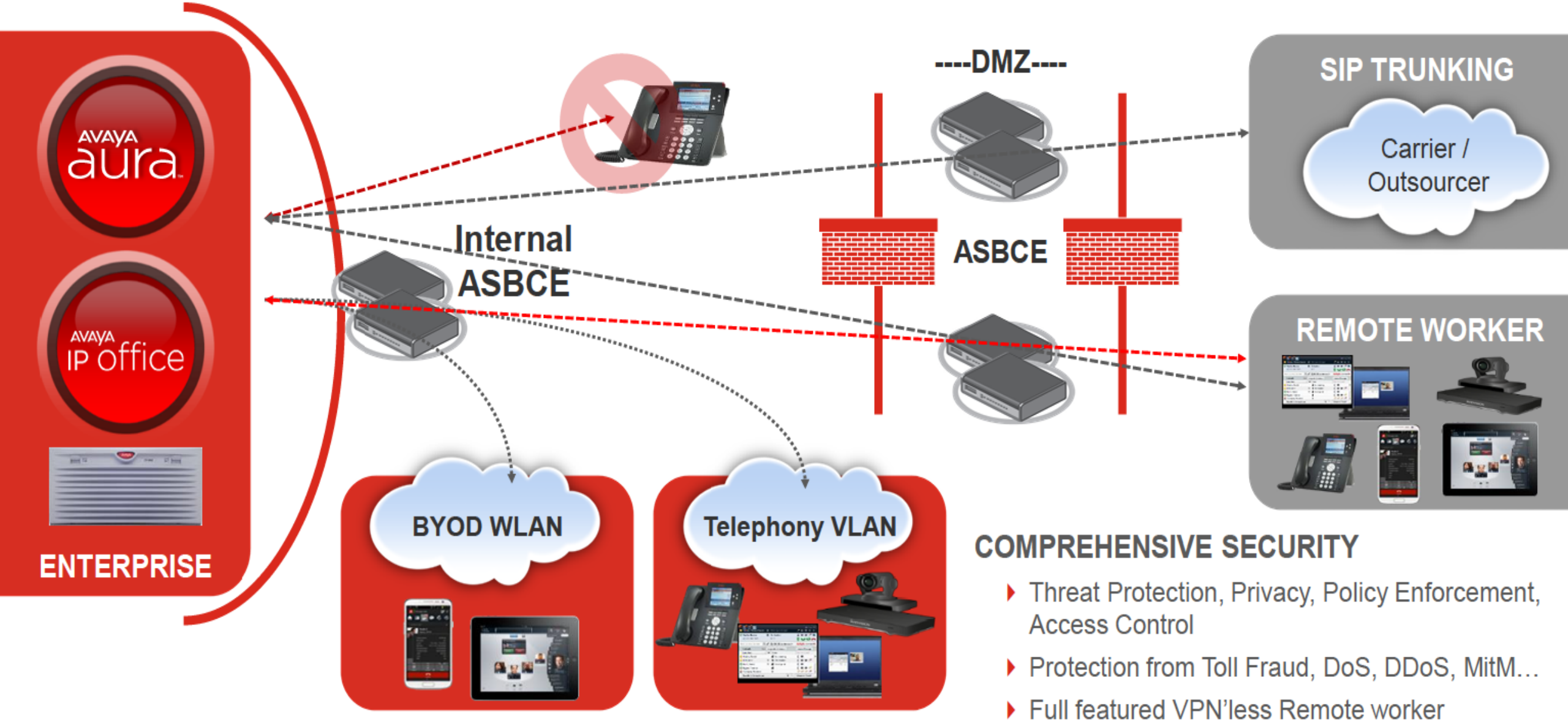
Nihol

CHALLENGERS
LEADERS
Cisco
Microsoft
NEC
Mitel
ALE
Huawei
Avaya
Unify
ShoreTel
Interactive Intelligence
NICHE PLAYERS
VISIONARIES

Nihol

AVAYA SBCE - LAYERED SECURITY APPROACH

Nihol



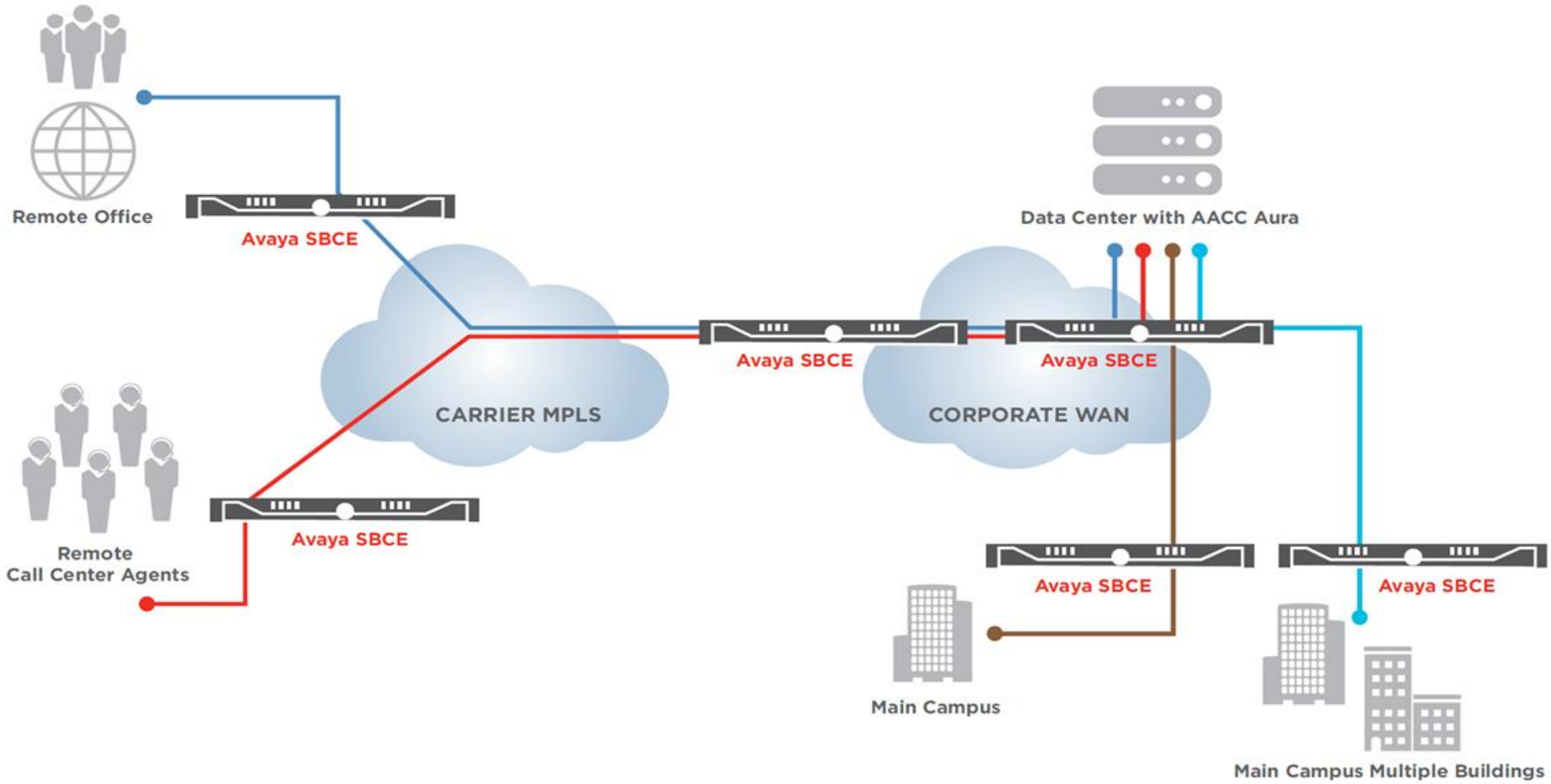
COMPREHENSIVE SECURITY

- Threat Protection, Privacy, Policy Enforcement, Access Control
- Protection from Toll Fraud, DoS, DDoS, MitM…
- Full featured VPN'less Remote worker
- Layer 7-deep packet inspection and signature based protection

ASBCE – READY FOR CLOUD DEPLOYMENTS

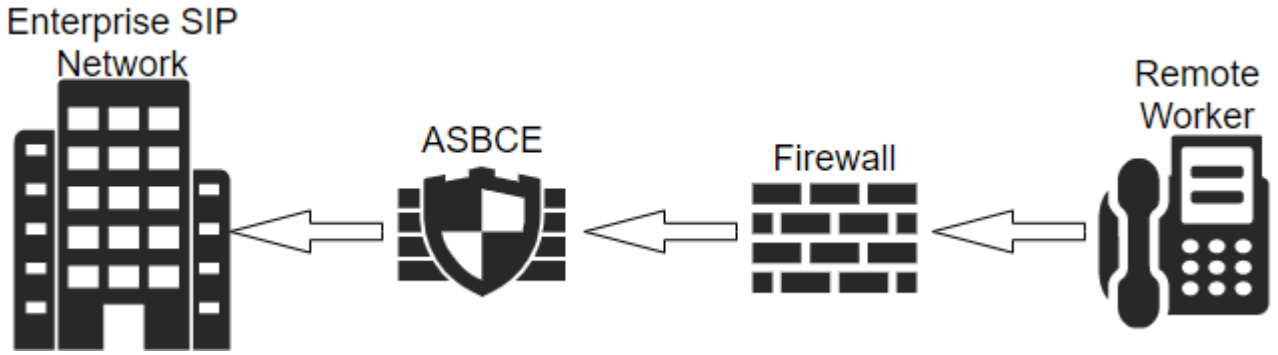
Nihol

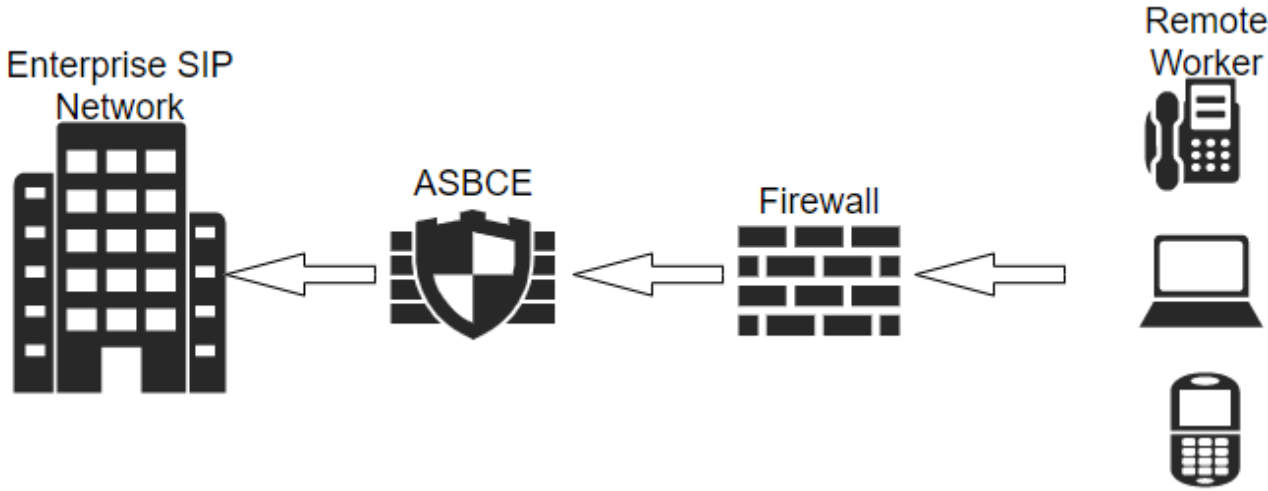
Large Enterprise, Multi-site, Remote Worker



Доступность сервисов AVAYA через SBCE

- ASBCE позволяет безопасно организовать подключение к SIP-телефонии, обеспечивая сокрытие внутренней топологии и защиту сети от возможных атак на уровне протоколов высокого уровня
- ASBCE обеспечивает возможность подключения к внутренним ресурсам организации пользователей из сети Intranet, обеспечивая как работу стандартных и проприетарных функций так и возможность максимально обезопасить внутреннюю инфраструктуру от потенциальных угроз





UNIFIED COMMUNICATIONS
Unified Messaging
Mobility
Audio/VIdeo Conferencing
Presence
Call Recording
Instant Messaging
Desktop Sharing
Hosted Fax
Nihol

Варианты установки ASBCE

Nihol

PLATFORM CAPACITIES

Nihol

	Appliance Model	Non-Encrypted Sessions	Encrypted Sessions	Remote Worker Users (Sessions)	SIPREC with SIP trunking replicated Sessions	Scopia Video Sessions	Internal AAMS Transcoding Sessions	External AAMS Transcoding Sessions	Reverse Proxy
High Range	Avaya Converged Platform 100 series server with profile 5	30,000	10,000	20000 (10,000)	10,000	800	1000	5000	500 HTTP Requests /sec. 50 TLS connections /sec 2000 concurrent webSockets
	Avaya Converged Platform 100 series server with profile 3	14,000	8,000	20,000 (8,000)	6,000	800	1,000	2500	Same as above
Mid-range	Dell R330	6,000	2,000	5,000 (2,000)	3,000	200	300	1,250	Same as above
	Virtual Appliance VMW	5,000	3,000	6,000 (3,000)	2,500	200	100	1,250	Same as above
	Nutanix AHV on Nutanix Appliance	5,000	3,000	6,000 (3,000)	2,500	200	100	1,250	
Low Range	Virtual Appliance KVM	1500	500	500	N/A	N/A	100	1,250	Same as above
	Portwell CAD0230	600	500	500 (500)	N/A	N/A	N/A	N/A	Same as above

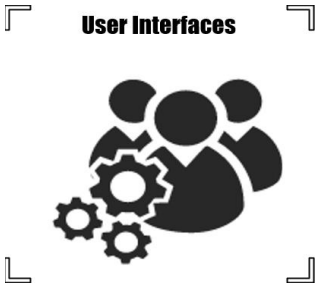
Минимальные требования

Resource	Variant		
	SBC	Small SBC	EMS
vCPU core	4 dedicated cores	2 dedicated cores	3 floating cores
vCPU reservation	8800 MHz to 9600 MHz	8800 MHz to 9600 MHz	6600 MHz to 7200 MHz
Minimum CPU speed based on Xeon x5670 or equivalent processor	2.2 GHz	2.2 GHz	2.2 GHz
Memory reservation	8 GB	4 GB	8 GB
Storage reservation	Automatically provisioned to minimum required storage — thin provisioned 160 GB — thick provisioned (Recommended)	Automatically provisioned to minimum required storage — thin provisioned 160 GB — thick provisioned (Recommended)	Automatically provisioned to minimum required storage — thin provisioned 160 GB — thick provisioned (Recommended)
Network Interfaces	6 Virtual Interfaces	4 Virtual Interfaces	2 Virtual Interfaces

Nihol

Архитектура

- EMS – управляющий компонент. Он не хранит на себе конфигурационных данных, а только информацию о текущих соединениях.

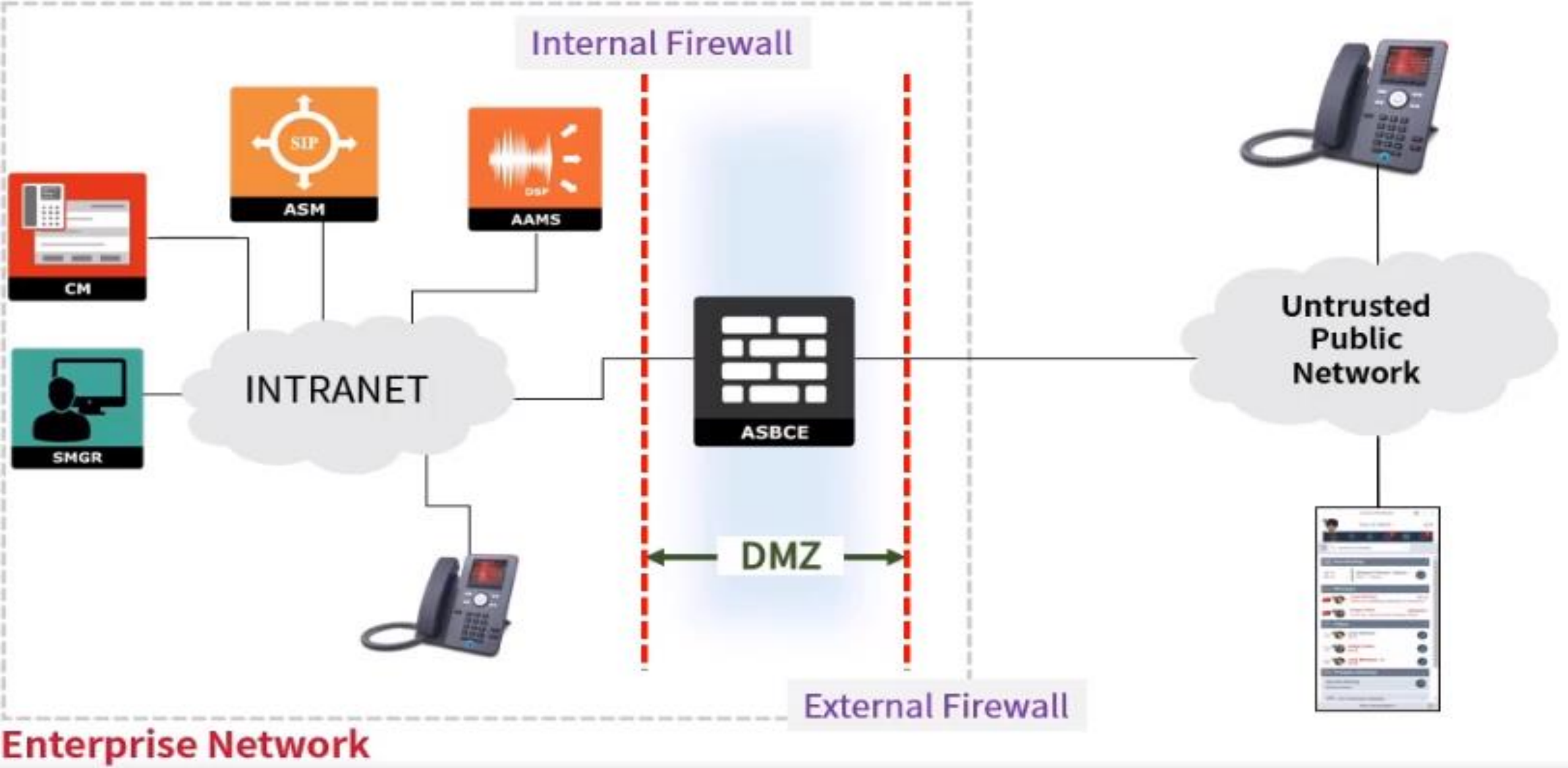


- SBC – предоставляющий сервисы компонент. Может работать при временном отсутствии EMS

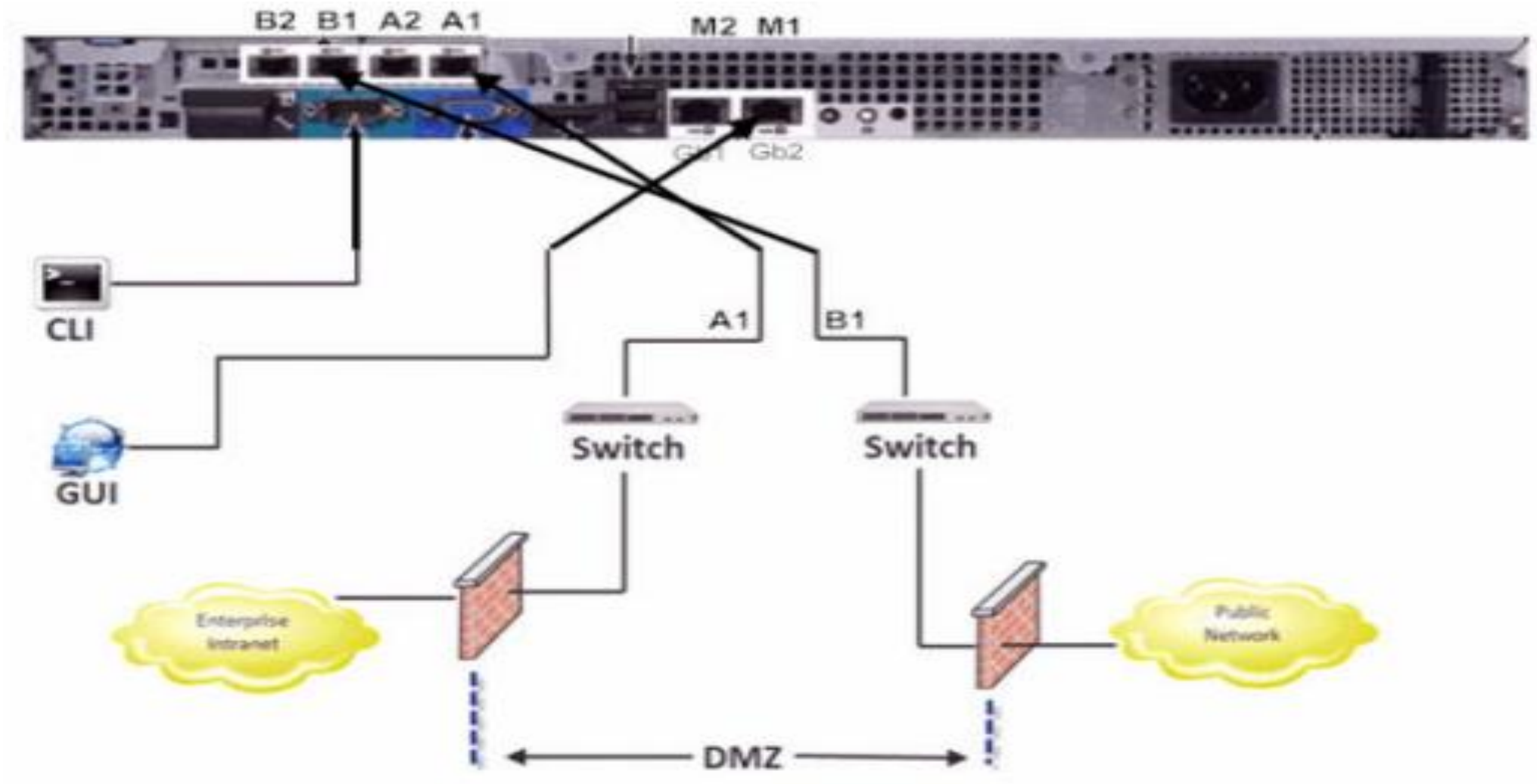
- Можно дублировать как EMS, так и SBC. При этом может быть до 12 HA пар SBC под управлением одной HA пары EMS.

Варианты применения

Nihol



Варианты применения



Nihol

Функции

- SIP Trunking – возможность работы с операторами SIP телефонии и сторонними системами
- Remote Worker – подключение клиентов из публичных сетей без VPN
- TLS шифрование управляющих соединений
- TURN/STUN обеспечение возможности прохождения RTP через все уровни NAT
- HTTP Reverse Proxy – подключение к внутренним ресурсам по протоколам HTTP/HTTPS для удалённых клиентов
- Video Services подключение удалённых аппаратных видеотерминалов XT и CU серии с поддержкой протоколов BFCP и FECC
- SigMa встроенный скриптовый язык для манипуляции заголовками и расширениями (например, SDP) SIP сообщений
- Topology Hiding сокрытие внутренней топологии для всех внешних подключений

Nihol

Еще немного функций

- Presence Services обеспечивает функционирования Presence для удалённых клиентов с корректным переопределением адресов сервисов в служебном обмене
- SIPREC подключение систем записи к ASBCE
- Transcoding – перекодирование RTP на лету с помощью как встроенных средств, так и подключаемого внешнего Media Server
- Transrating – изменение размера пакетов RTP на лету для адаптации к сетевым условиям
- Call Preservation возможность сохранить сессию при выходе из строя одного из внутренних Session Manager
- Dynamic licensing – динамическое распределение лицензий между несколькими SBC в зависимости от их состояния
- LDAP-based-SSO возможность перенаправить аутентификацию администраторов на внешние ресурсы по протоколу LDAP

Nihol

Лицензирование: Standard Services

- EMS: Element Management System, craft interface HA (Active-Active)
- Advanced UC Security: Toll Fraund, Call Walking
- Deep Packet Inspection (SIP and Media)
- DoS/DDoS (flood, resource hang/open transaction, crash/fuzz)
- ACL/White/Black listing
- SIP Normalization – ITSP integration
- Call admission control
- DTMF manipulation
- Network Address Traversal (NAT)
- RFC 5853 Compliant
- VLAN Routing
- Media Anchor Release
- Multi Tenancy (EMS Management included)
- Load Balancing
- Multiple interface Support
- Multiple subnet support
- IPv6 dual stack support
- ENUM Routing support

Nihol

Лицензирование: Advanced Services

- Remote Worker validate and securely support remote/mobile users for Avaya Aura UC services
- VPN-less Support both near and far end NAT
- Support Avaya hard and soft clients per solutions tested compatibility matrix
- SIP One-x Agent Support
- Encryption Services SIP TLS sRTP
- Signaling only encryption
- Media Forking to recording devices, SIPREC
- UCID generation
- Support for STUN/TURN – WebRTC support
- Reverse Proxy

Nihol

Описание лицензионного функционала

Nihol

VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_PREM_SESSION	Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_PREM_HA_SESSION	Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBCE elements managed.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted.
VALUE_SBCE_ENCRYPTION_1	Specifies that both media and signaling can be encrypted for Avaya SBCE. This license is required when using any advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBCE. The quantity of this license must match the quantity of standard licensing in the system being managed.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies Avaya SBCE encryption only for signaling.
VALUE_SBCE_NG911	Specifies the number of AMR-WB codec licenses.
VALUE_SBCE_NG911_HA	Specifies the number of AMR-WB codec HA licenses.

CCaaS — это contact center as a service, он же контакт-центр как услуга. Это облачный софт, который можно использовать для входящих и исходящих вызовов; своего рода контакт-центр в интернете, а не на локальном сервере в офисе. Его задача — маршрутизация контактов и отслеживание взаимодействия с клиентами; а цель — дать бизнесу технологии для работы без значительных инвестиций или затрат на обслуживание.

UCaaS

Модель UCaaS и ее компоненты

Унифицированные коммуникации (UC) — это сложное сочетание различных способов коммуникации, которые современный бизнес использует для работы. К компонентам UC мо отнести:

- аудио- и видеоконференции (в том числе, через веб-конференции);
- телефонию;
- чаты, SMS и MMS;
- совместное использование файлов и экрана;
- электронную и голосовую почту;
- управление контактами и вызовами;
- распознавание речи;
- инструменты для совместной работы.

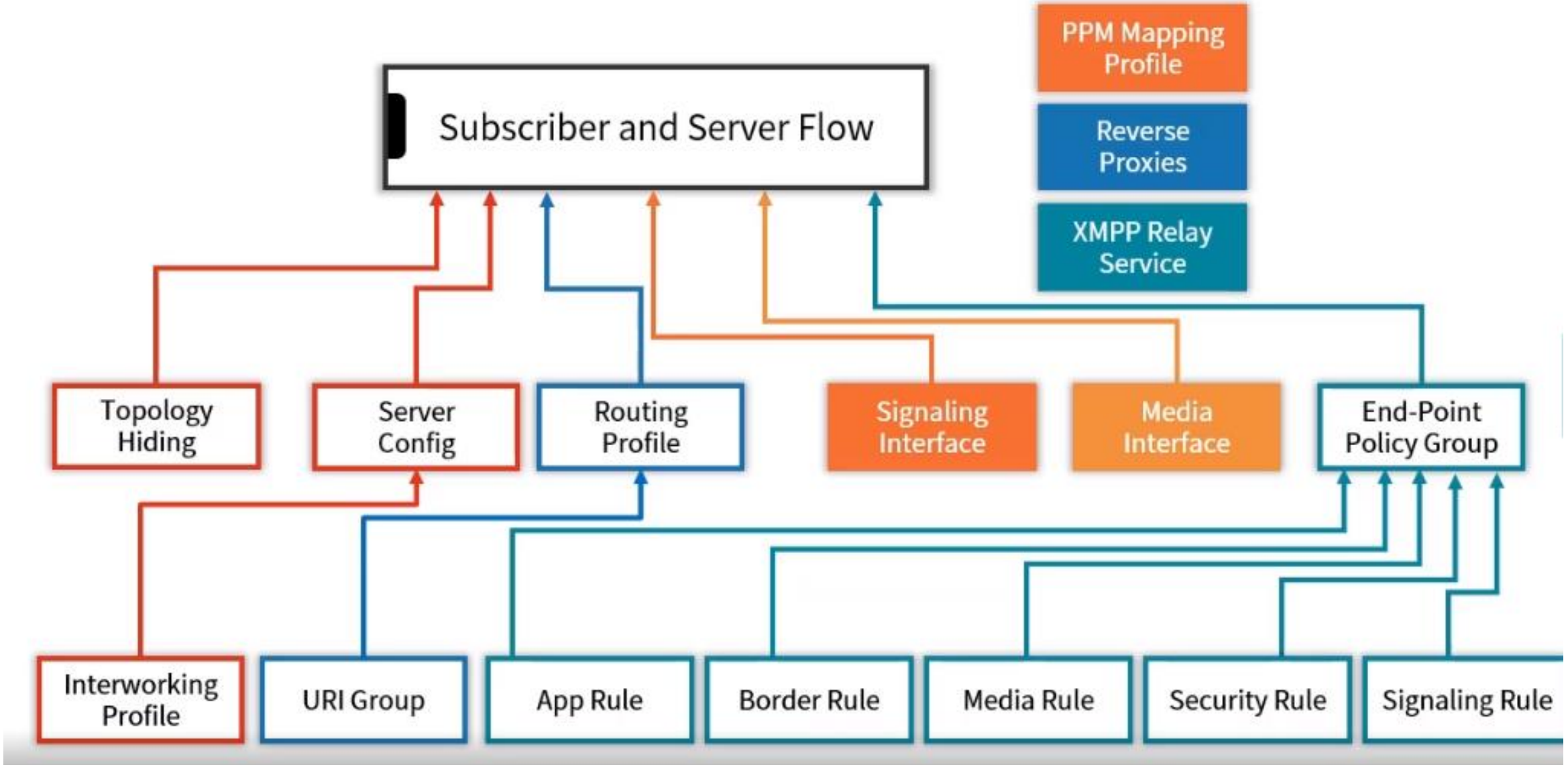
Nihol

Сколько и каких лицензий нужно?

- Использование лицензий инкрементальное
- Например 3 remote worker с TLS шифрованием и все 3 записываются с использованием SIPREC Потребуется 3 стандартных лицензии и 3 advanced.
- Система с 20 SIP trunks без шифрования, 10 из которых пишутся и 2 Remote Worker потребуют суммарно 22 standard и 12 advanced лицензий
- 500 SIP trunks 1000 Remote users потребуют 1500 standard и 1000 advanced лицензий
- Есть лицензии для второго сервера SBC Standard HA, Advanced HA

Nihol

Принцип конфигурации



Nihol

Nihol

Спасибо за внимание!

Узбекистан, г. Ташкент, 100187, ул. Интизор, 26,
Группа компаний NIHOL

(998-71) 208-58-44, 208-58-45, 208-58-48, 266-58-46,

266-58-47

info@nihol.uz