



Cisco Expo 2009

Безопасность
инфраструктуры
системы
унифицированных
коммуникаций
предприятия



Алексей Гомонюк
Системный инженер

agomonyu@cisco.com

О чем данная презентация?

Давайте рассмотрим:

- Наиболее типичные уязвимости инфраструктуры системы Унифицированных коммуникаций и методы их устранения,
- Методы и средства защиты от потенциальных атак на элементы инфраструктуры системы.

Какой уровень информационной безопасности считать достаточным для системы Унифицированных коммуникаций ?



Оглавление

1. Какой уровень безопасности необходим для системы унифицированных коммуникаций,
2. Состав системы унифицированных коммуникаций,
3. Наиболее распространенные уязвимости/атаки:
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Какой уровень безопасности у Вас сейчас?

Есть ли в Вашей сети критичные бизнес-приложения ?

1. Достаточно ли безопасна Ваша сеть сейчас?

Если нет, то что еще нужно сделать ?

2. Делает ли внедрение VoIP менее безопасной Вашу сеть?

3. Какие риски появляются в сети при внедрении системы унифицированных коммуникаций?

4. Будут ли работать внедряемые Вами элементы информационной безопасности совместно с VoIP и для системы унифицированных коммуникаций?

Установить уровень безопасности для VoIP

1. Определите что для Вас является важным, расставьте приоритеты,
От каких атак и уязвимостей вы собираетесь защищаться?
2. Как много безопасности Вам необходимо, где компромисс между безопасностью и удобством для пользователей?
3. Где Вы собираетесь внедрять систему унифицированных коммуникаций?
Центр обработки вызовов, корпоративная телефония, и т.д..
4. Как вы будете управлять системами информационной безопасности?
5. Определите бюджет для внедрения систем информационной безопасности.

Голос – это данные, но какие?

1. Определите приоритет голоса среди других Ваших бизнес-приложений,
2. Оцените насколько Ваша текущая политика безопасности подходит для системы унифицированных коммуникаций,
3. Я не могу вам сказать, сколько безопасности Вам необходимо. Я могу только помочь Вам определить что может быть приемлемо для Вас.



**Банковские приложения
Oracle и др. БД**

Дилинг

Голос?

Биллинг

АТМ-терминалы

Web приложения

E-Mail

Directory

Политика безопасности для системы унифицированных коммуникаций

1. Вам необходима отдельная политика безопасности для голоса/видео/IM данных в Вашей сети,
2. Классифицируйте приложения в своей сети,
Может быть что-то, по типу трафика, очень похоже на трафик системы унифицированных коммуникаций.
3. Если у Вас план мероприятий, на случай инцидентов по информационной безопасности?
Внесите туда раздел посвященный системе унифицированных коммуникаций.
4. Оцените риски и убедитесь, что руководство компании в курсе этой оценки.

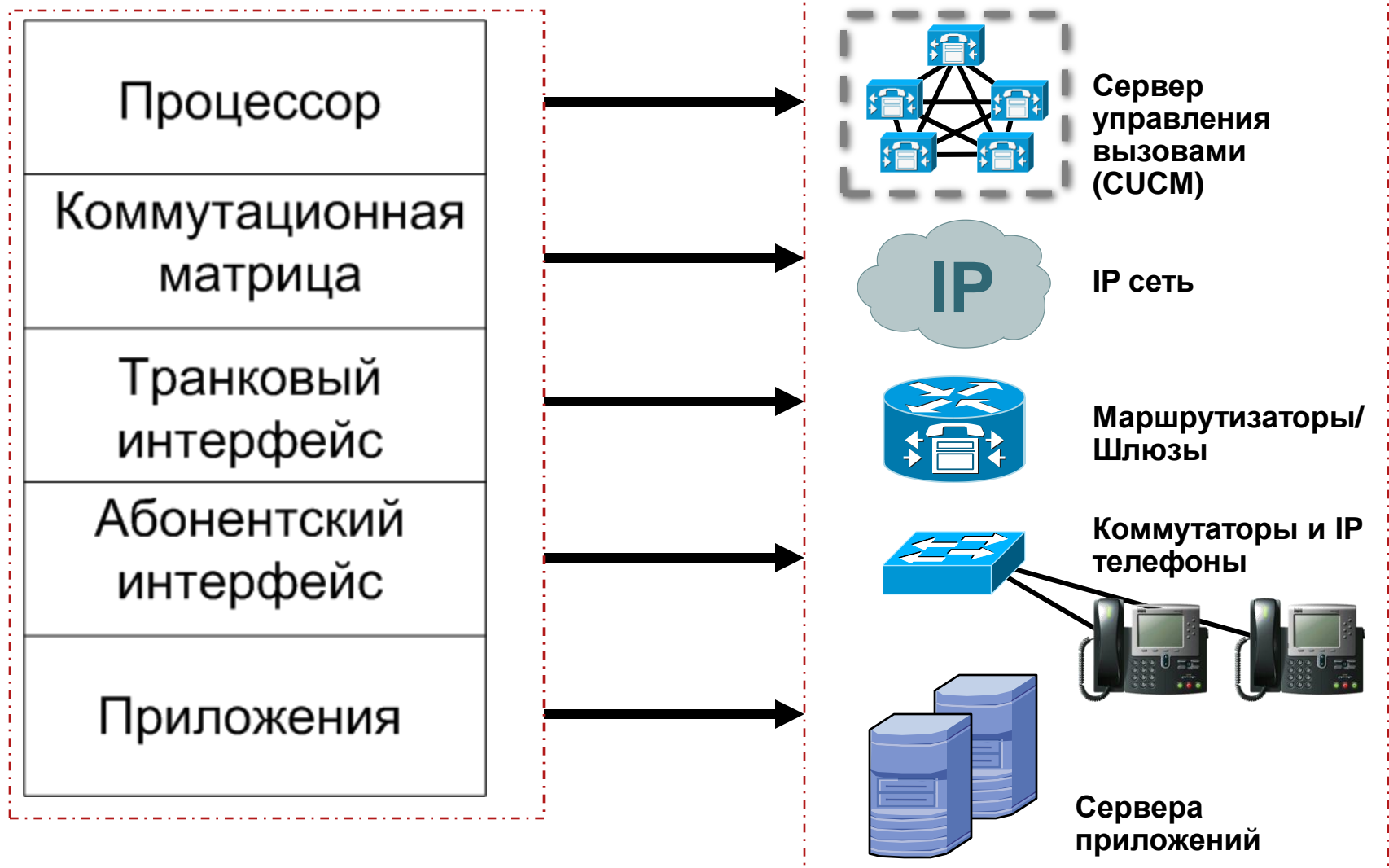
Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- Наиболее распространенные уязвимости/атаки:
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Как выглядит система унифицированных коммуникаций

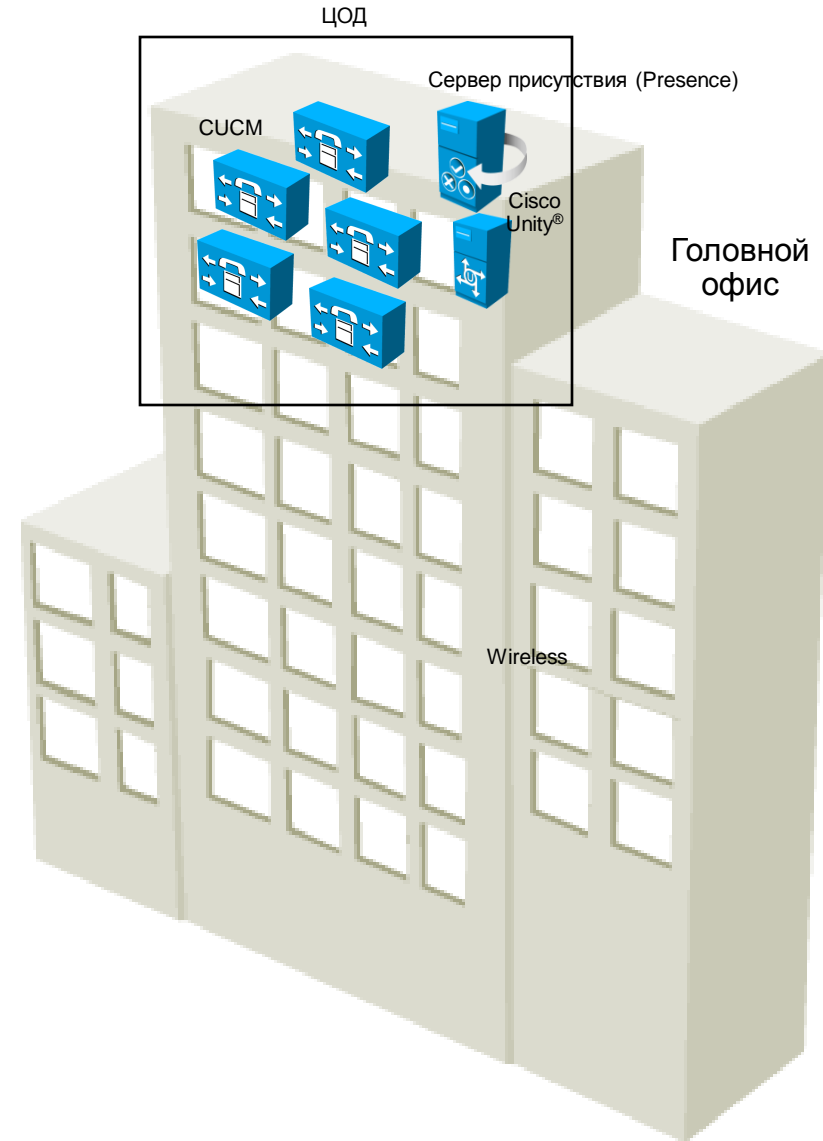
УАТС

UC система

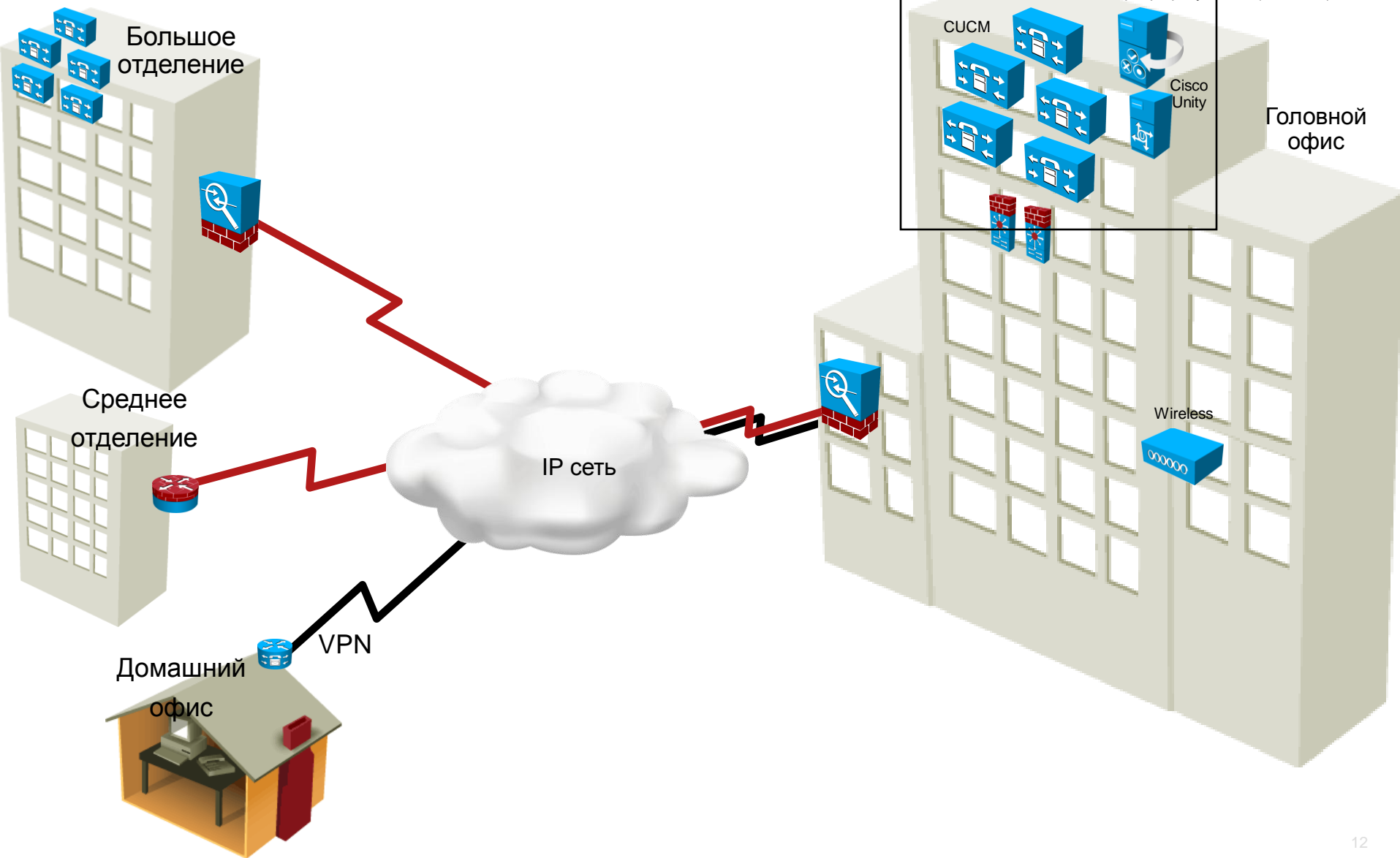


Типовая инфраструктура

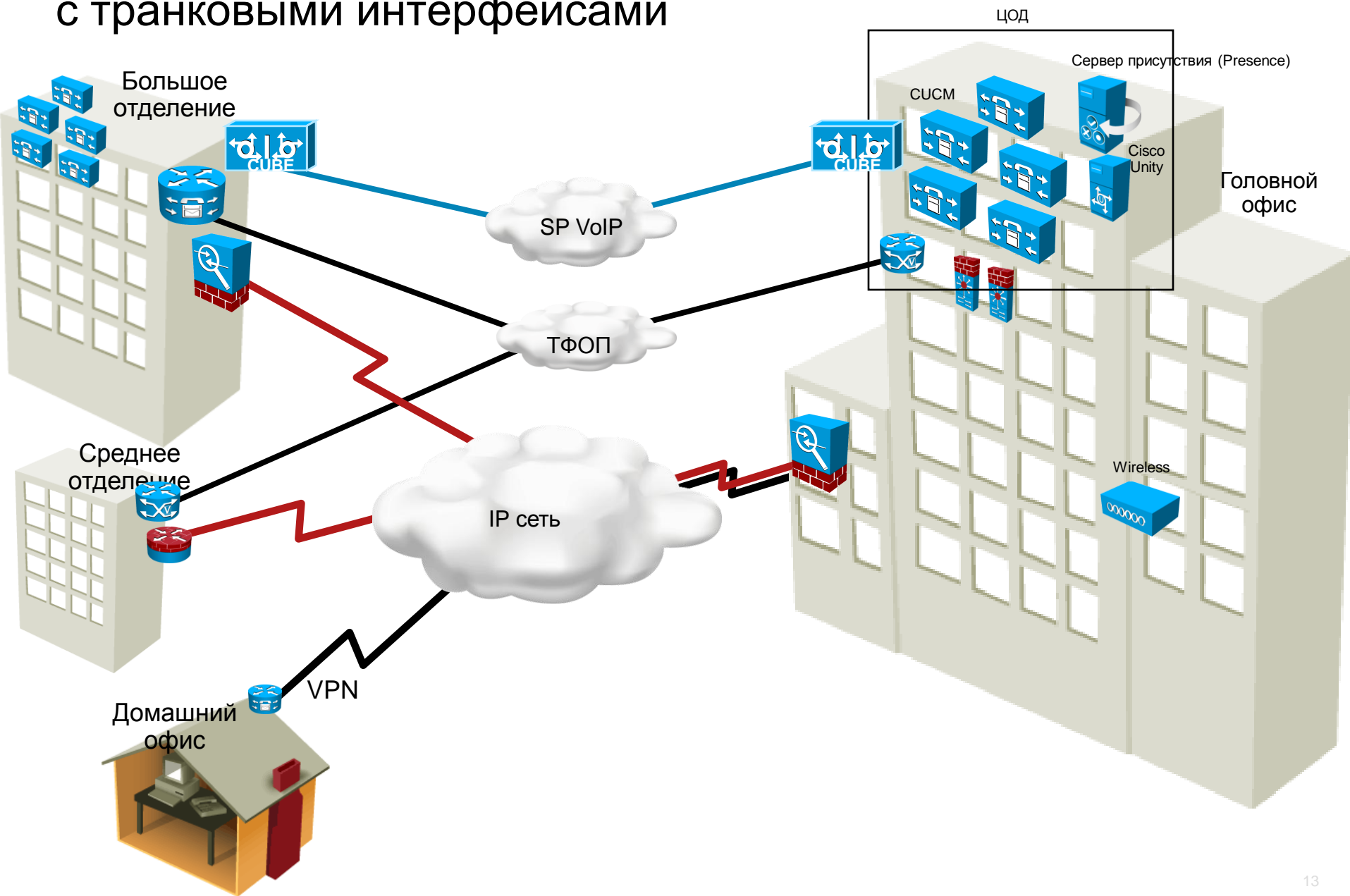
УС процессоры



Типовая инфраструктура С UC коммутационной матрицей



Типовая инфраструктура с транковыми интерфейсами

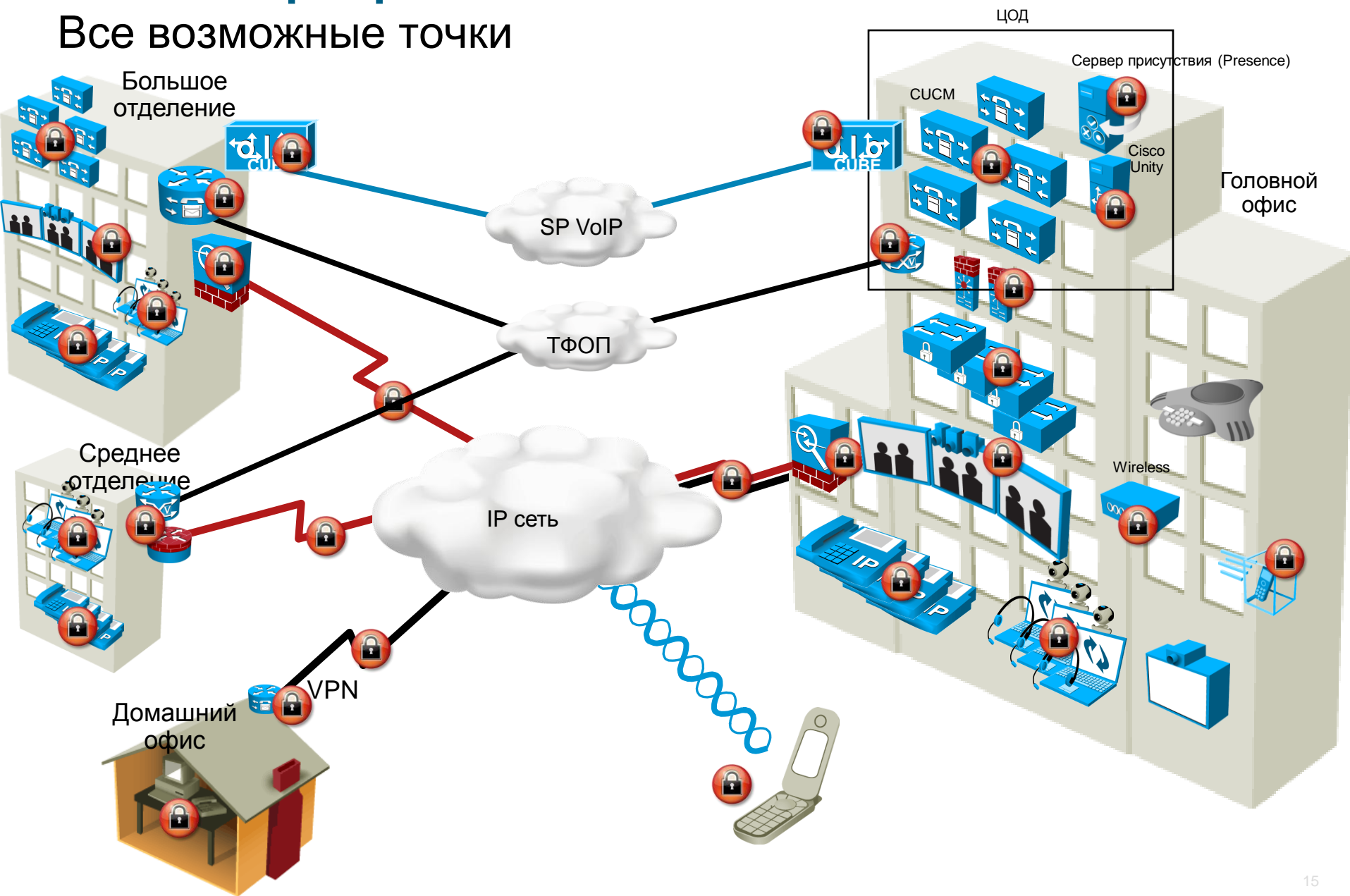


Типовая инфраструктура с абонентскими интерфейсами



Что защищать?

Все возможные точки



Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- **Наиболее распространенные уязвимости/атаки:**
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Источники атак

1. 50% атак внутренние,
2. 5% компаний заявляют что 80–100% атакующих их ресурсы находятся внутри периметра,
3. 23% компаний не могут сказать сколько атак они подверглись за прошедший год.

*CIS/FBI Computer Crime and Security Survey, 2008 (<http://www.gocsi.com/>)

Основные типы атак и атакуемые объекты

1. Несанкционированное прослушивание,
Прослушивание и запись данных без санкции.
2. Отказ в обслуживании (DoS) или распределенный отказ в обслуживании (DDoS),
3. Заимствование прав,
Попытка получить доступ к администрированию системы или информации под чужими правами.
4. Приложения UC,
Систем голосовой почты, сервера представлений и т.д.
5. Программные клиенты,
Все программные телефоны, клиенты IM.
6. Мошенничество.
Несанкционированные вызовы (междугородние, международные).

Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	X	X	X	X	X	X
Отказ в обслуживании	X	X	X	X	X	X
Заимствование прав	X	X	X	X	X	X
Безопасность ОС приложений	X	X	X	X	X	X
Программные клиенты	X	X	X	X	X	X
Мошенничество	X	X	X	X	X	X

E = легко реализовать; I = средняя степень сложности; C = сложная защита

Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- Наиболее распространенные уязвимости/атаки:
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Что такое несанкционированное прослушивание?

1. Несанкционированное прослушивание - это действие по прослушиванию частных разговоров,
2. Может быть осуществлено путем прослушивания телефонной линии (wiretapping), перехвата email и IM, перехвата трафика в сети и т.д.,
3. Существует термин для такой операции—unlawful interception.

Wikipedia: <http://en.wikipedia.org/wiki/Eavesdropping>

Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	E-C	E-I	E-I	NA	E-I	NA
Отказ в обслуживании	X	X	X	X	X	X
Заимствование прав	X	X	X	X	X	X
Безопасность ОС приложений	X	X	X	X	X	X
Программные клиенты	X	X	X	X	X	X
Мошенничество	X	X	X	X	X	X

E = легко реализовать; I = средняя степень сложности; C = сложная защита

Защита от прослушивания

Телефоны/CUCM: Настройки

1. Настройки доступа к телефону,
2. Предотвращают получение информации о сети для не IT-сотрудников,
3. Скрывают информацию об IP адресах, VLAN ID, и т.д.,
4. Включены по умолчанию.

Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="password"/>

Product Specific Configuration ?	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP **	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Защита от прослушивания

Телефоны/CUCM: доступ к Voice VLAN

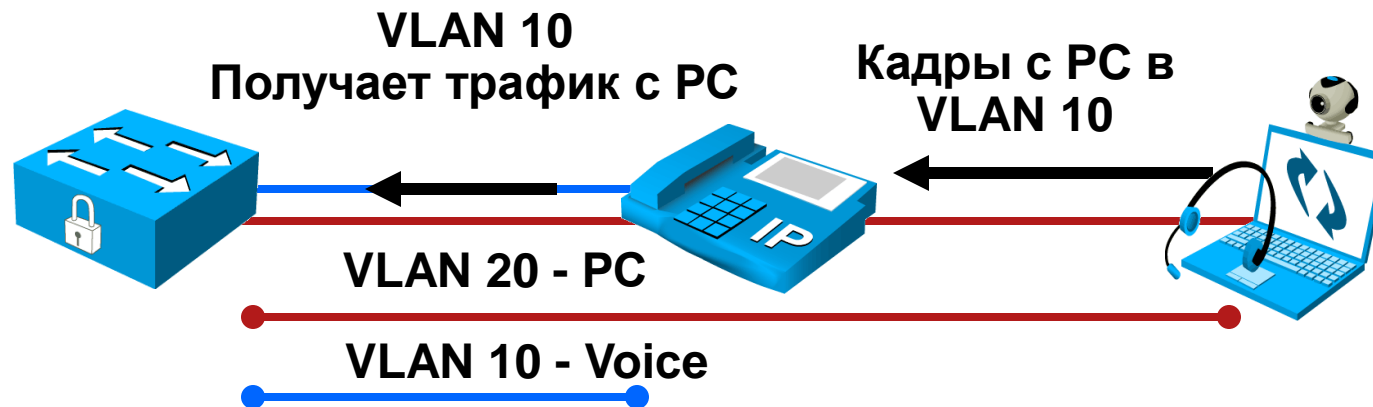
1. Телефон может контролировать трафик в Voice VLAN,
2. Предотвращает подключение PC к Voice VLAN, через порт телефона,
3. Выключены по умолчанию.

Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="password"/>

Product Specific Configuration	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Защита от прослушивания

Телефоны/CUCM: Доступ к Voice VLAN

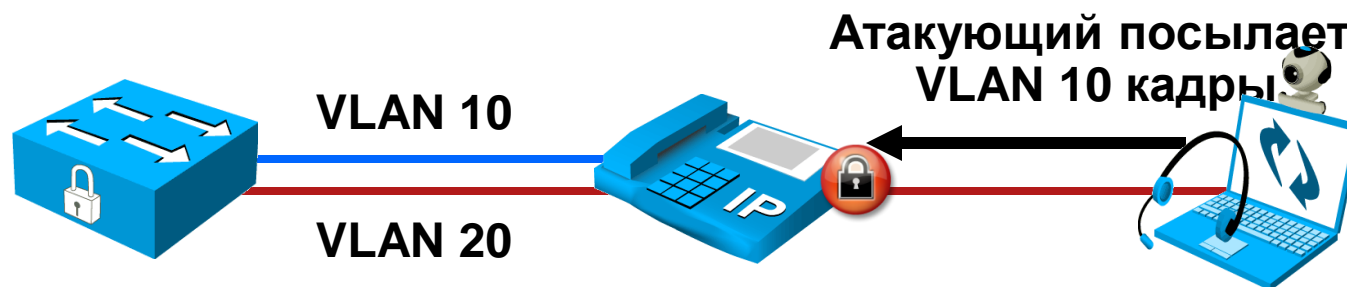


Получение доступа в Voice VLAN:

1. Атакующий посылает 802.1q (VLAN 10) кадры с PC на телефон,
2. Трафик с PC попадает в Voice VLAN (10), хотя PC находится в VLAN 20.

Защита от прослушивания

Телефоны/CUCM: Доступ в Voice VLAN



1. Предотвращение атаки на voice VLAN:

Включить (enable) PC voice VLAN access опцию,

Трафик с VLAN ID 10 со стороны PC будет остановлен на PC порту телефона.

2. Различная реализация функции для разных моделей телефонов:

7940, 7960, 7941G, 7961G, и 7971G блокируют voice VLAN, позволяя посылать PC кадры 802.1Q с любым другим номером VLAN,

7970, 7961, и 7941 блокируют все кадры 802.1Q,

7912 ничего не блокирует.

Защита от прослушивания

Телефоны/CUCM: MITM Prevention

1. Телефоны имеют возможность защиты от Man in the Middle (MITM) атак,
2. Защищаются данные только с телефона,
3. Включено по умолчанию.

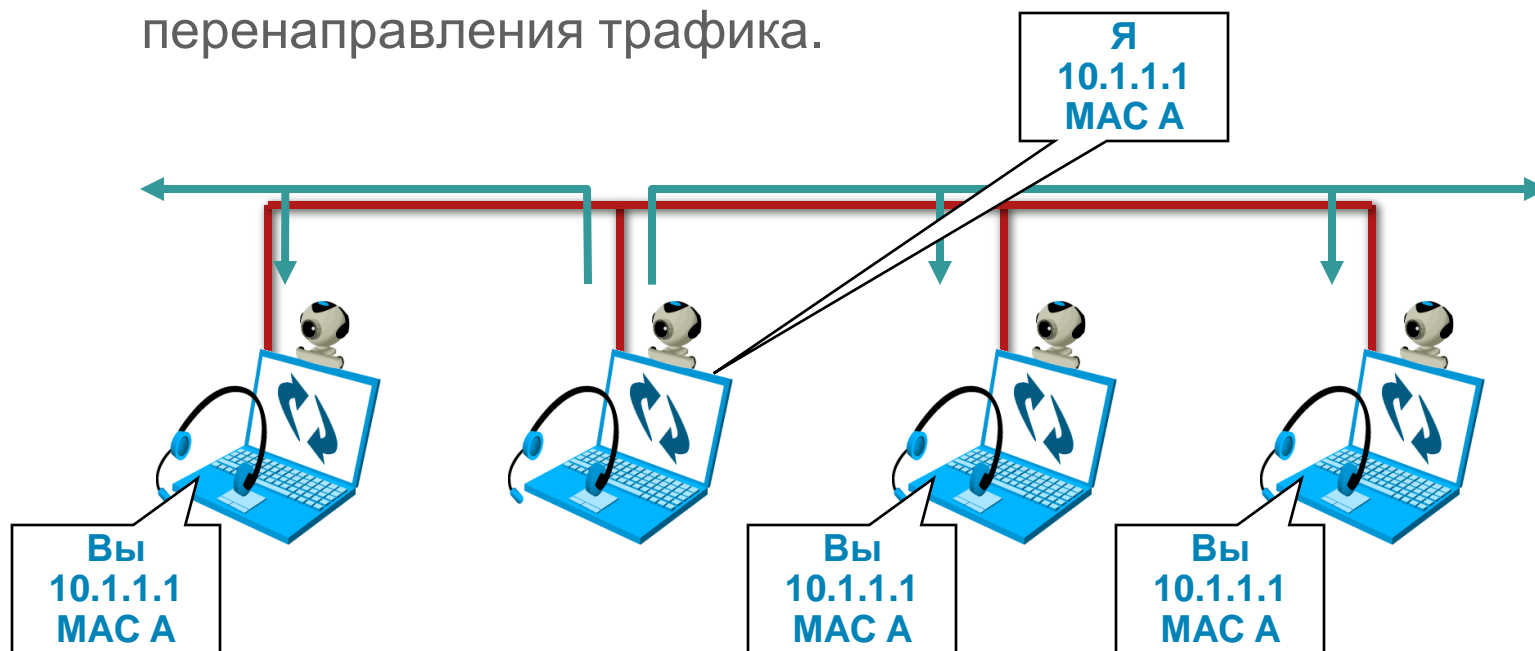
Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="password"/>

Product Specific Configuration	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Защита от прослушивания

ARP уязвимости

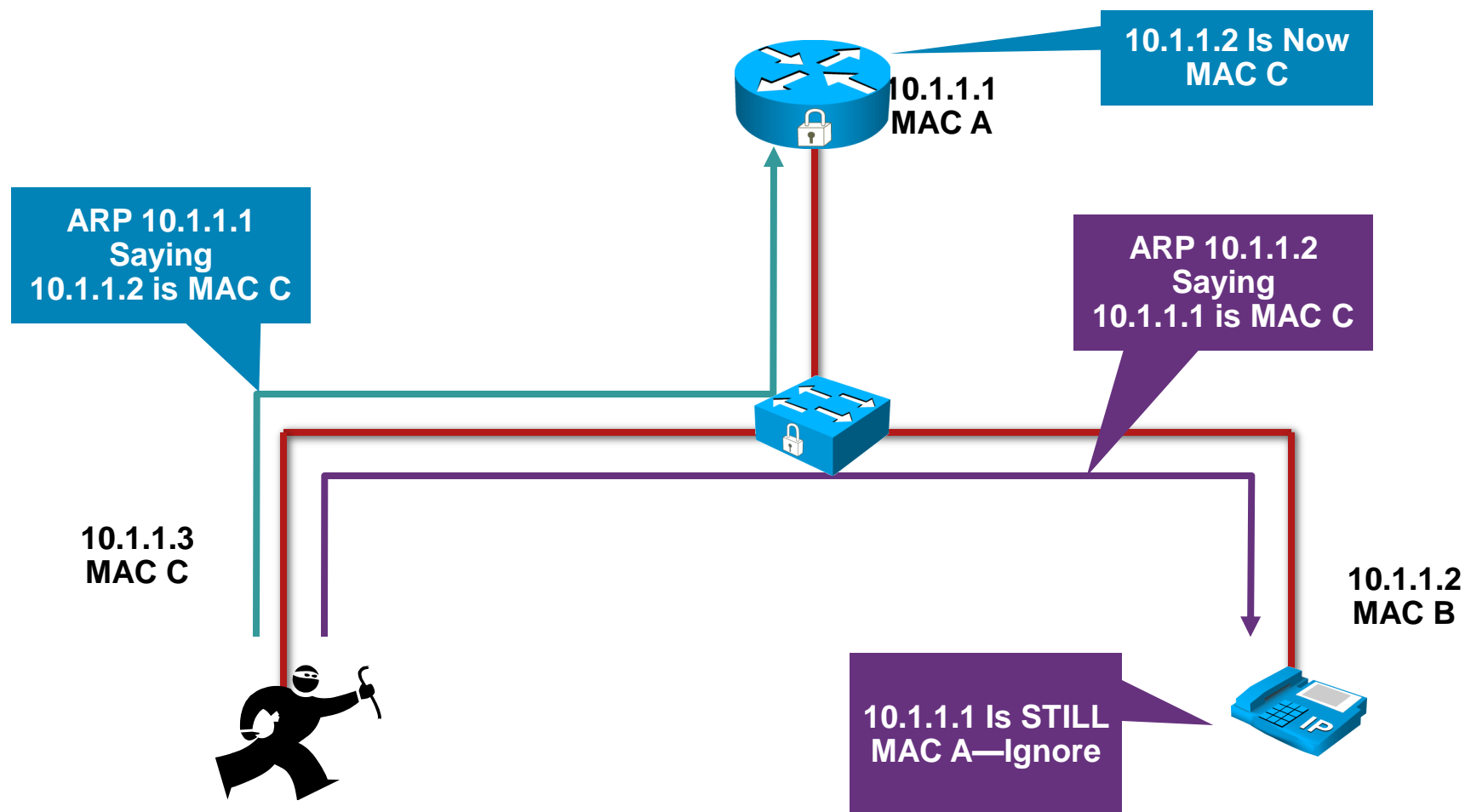
1. Согласно ARP RFC, клиенту разрешено посылать так называемые *unsolicited ARP* ответы. Этот механизм называется *gratuitous ARP*. Другие хосты из данной подсети сохраняют данную информацию в своих ARP таблицах,
2. Любой хост может заявить IP/MAC адрес, который ему нравится,
3. Атаки на ARP используют вышеописанный механизм для перенаправления трафика.



Защита от прослушивания

Телефоны/CUCM: MITM

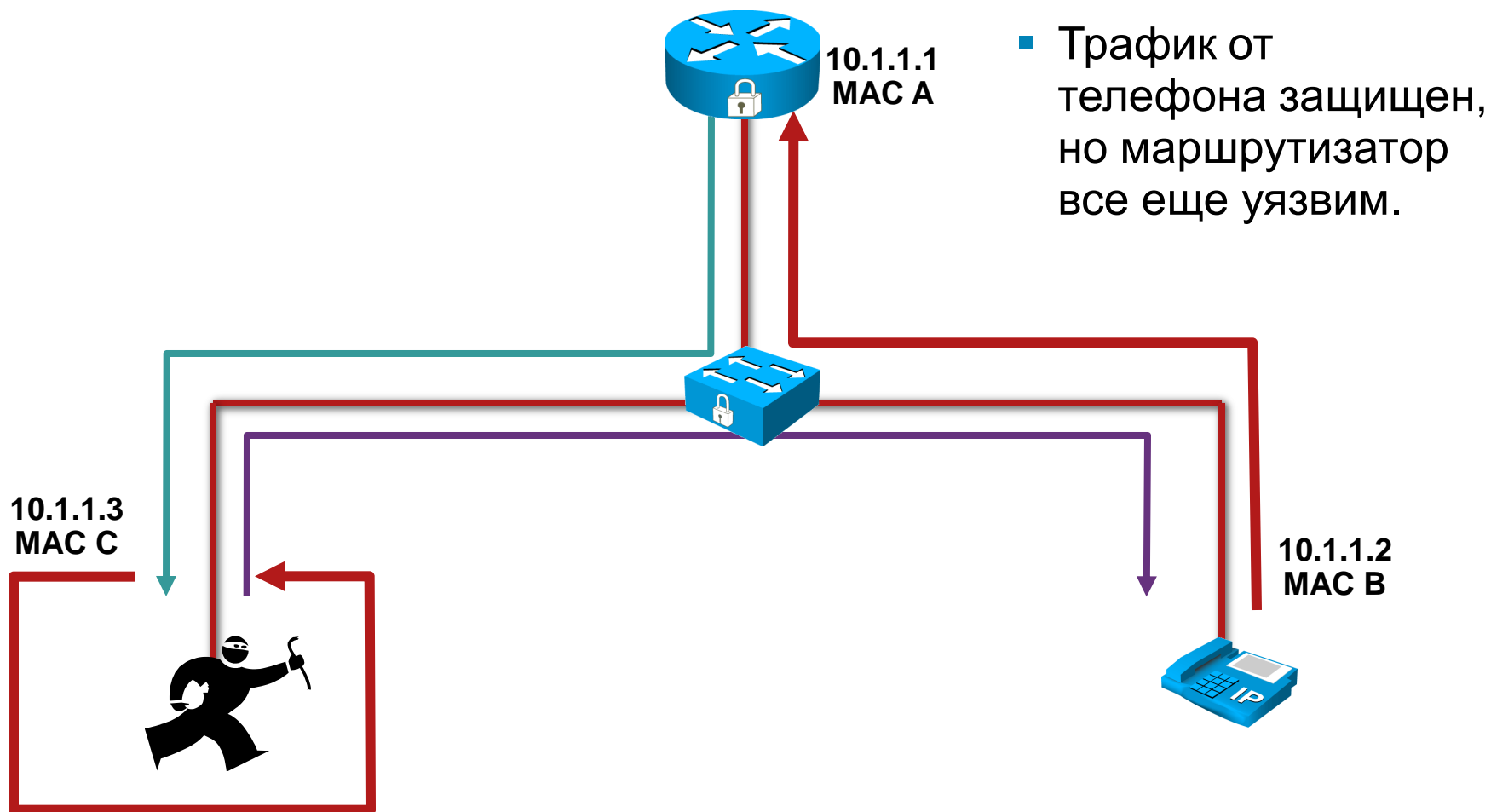
1. Атакующий «отравляет» MAC таблицу на маршрутизаторе.



Защита от прослушивания

Телефоны/CUCM: MITM

1. Трафик от маршрутизатора до атакующего—трафик от телефона до маршрутизатора.




- Трафик от телефона защищен, но маршрутизатор все еще уязвим.

Защита от прослушивания

Телефоны: доступ

1. Контроль web доступа к телефону с помощью ACLs:
Шлюз по умолчанию,
DHCP сервер,
DNS сервер,
TFTP сервер,
CUCM сервера,
Сервер директории,
И т.д.
2. Запретить web доступ к телефону.

		Network Configuration	
		Cisco Systems, Inc. IP Phone CP-7960 (SEP003094C25E70)	
<u>Device Information</u>	DHCP Server	10.27.15.1	
<u>Network Configuration</u>	BOOTP Server	No	
<u>Network Statistics</u>	MAC Address	003094C25E70	
<u>Ethernet</u>	Host Name	SEP003094C25E70	
<u>Port 1 (Network)</u>	Domain Name		
<u>Port 2 (Access)</u>	IP Address	10.27.15.27	
<u>Port 3 (Phone)</u>	Subnet Mask	255.255.255.0	
<u>Device Logs</u>	TFTP Server 1	10.27.11.12	
<u>Debug Display</u>	Default Router	10.27.15.1	
<u>Stack Statistics</u>	1		

Защита от прослушивания

Телефоны/CUCM: Загрузки

1. Подписанные ЭЦП файлы ОС телефонов,
Подписываются производителем для предотвращения загрузки неавторизованных версий ОС.
2. Подписанные ЭЦП файлы конфигурации,
Подписываются на CUCM и проверяются при загрузке на телефон.
3. TFTP используется для загрузки, в том числе и подписанных файлов.

Защита от прослушивания

Телефоны/CUCM: TLS/SRTP

1. Шифрование полностью предотвращает прослушивание разговора:

Новые ключи для каждого разговора,

X.509v3 цифровые сертификаты,

TLS:

RSA подписи,

HMAC-SHA1 аутентификация,

AES-128 CBC шифрование.

SRTP:

HMAC-SHA1 и AES-128.

2. Не предотвращает от перехвата трафика.

MITM атакующий может перехватить трафик но требуются усилия по расшифровке.

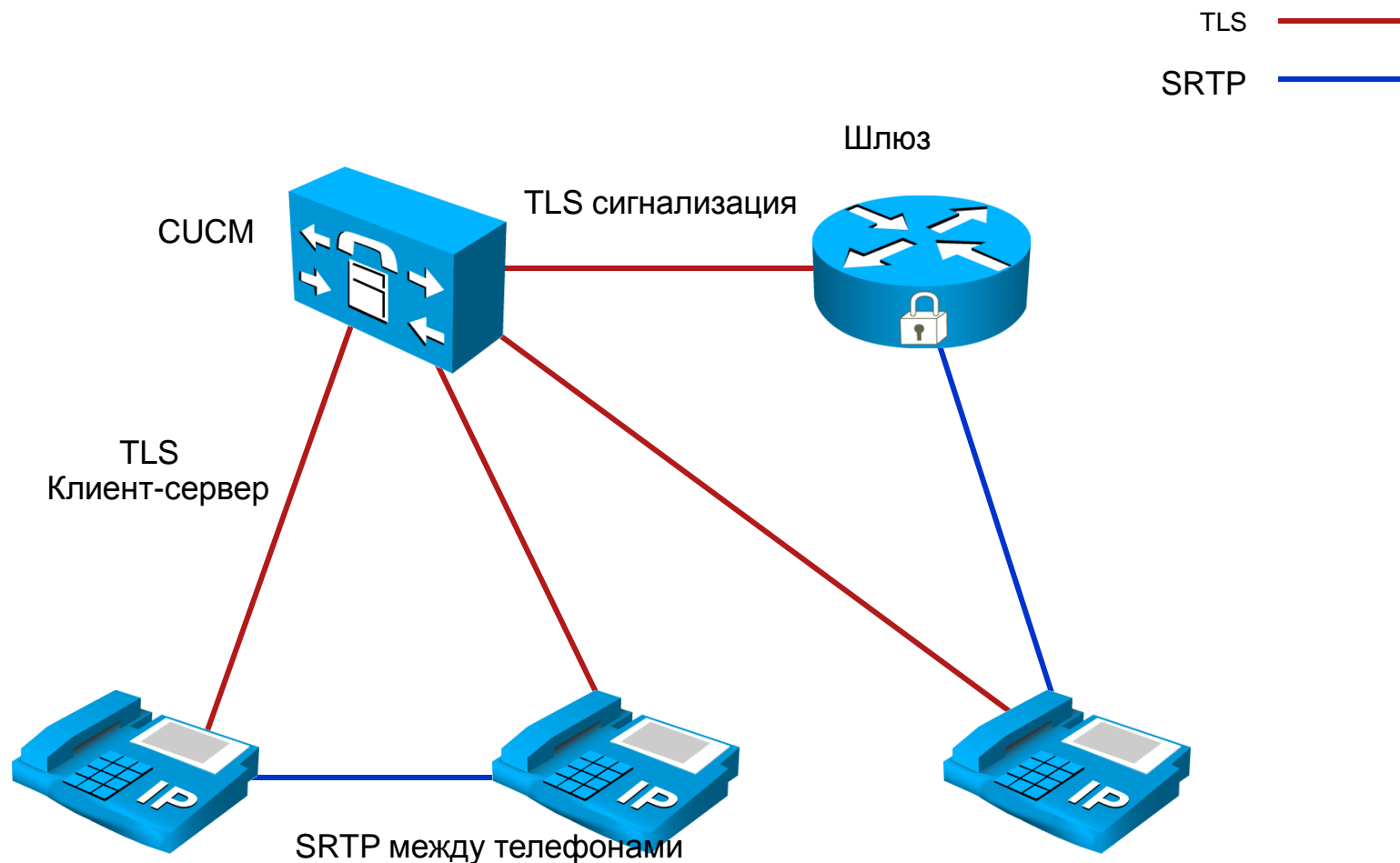
Защита от прослушивания

Телефоны/CUCM: TLS/SRTP

1. Не предотвращает перехват трафика,
MITM атакующий может перехватить трафик, но требуется
расшифровка.
2. Количество телефонов в кластере влияет на
масштабируемость.
Использовать средства для расчета масштабируемости
кластера при использовании TLS/SRTP.

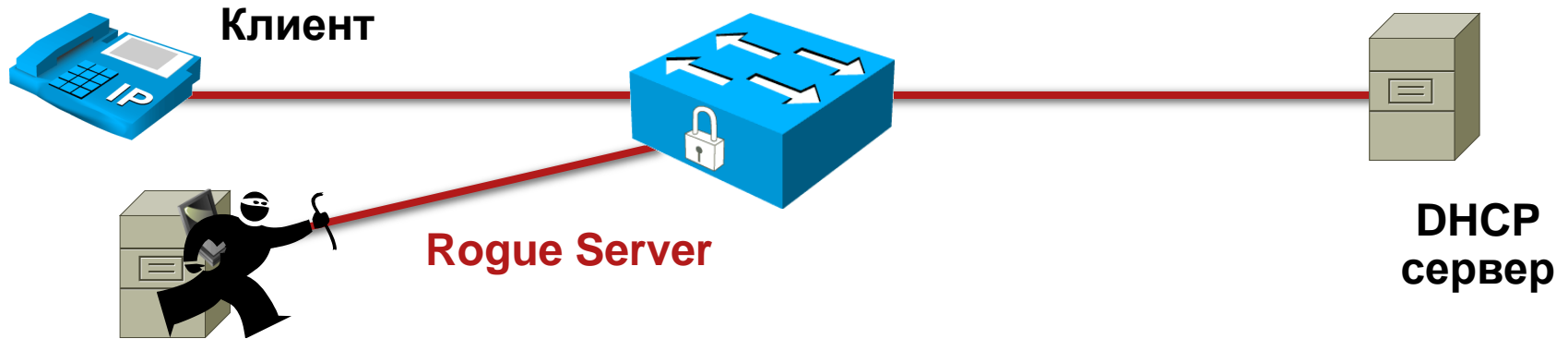
Защита от прослушивания

Телефоны/CUCM: TLS/SRTP



Защита от прослушивания

Коммутаторы: Несанкционированный (Rogue) DHCP Сервер



DHCP Discovery (Broadcast)



DHCP Offer (Unicast) **From Rogue Server**



DHCP Request (Broadcast)

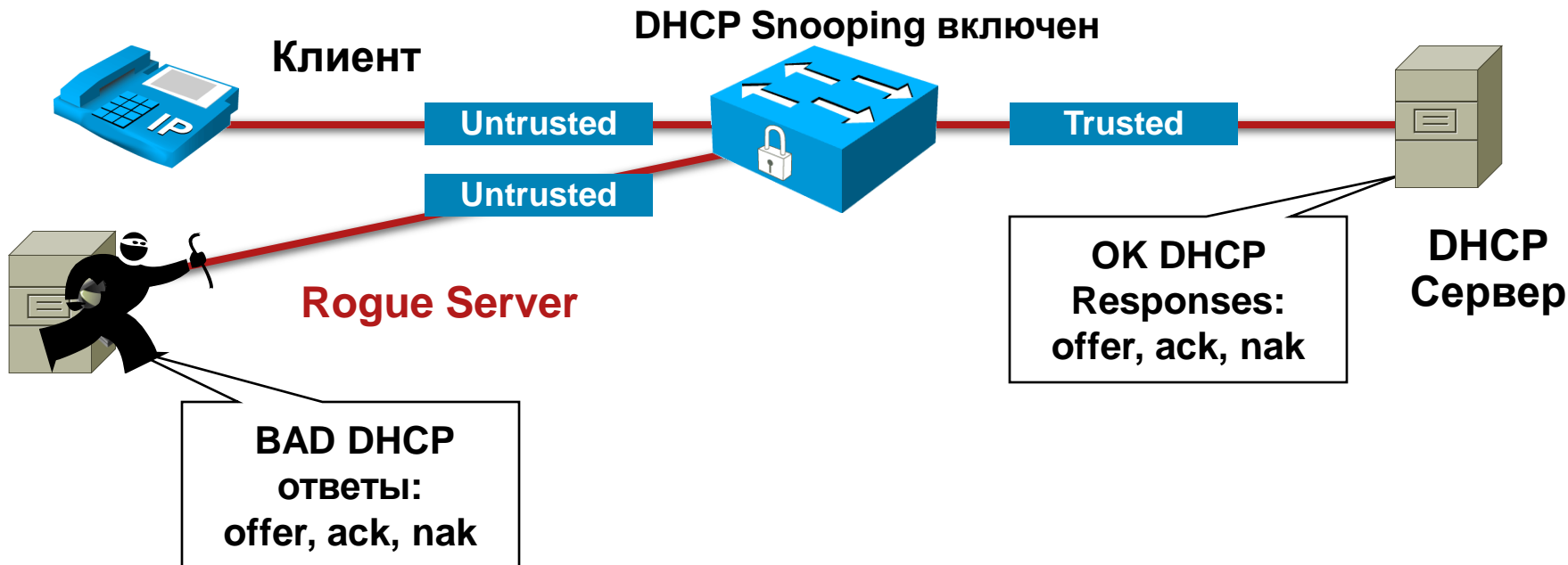


DHCP Ack (Unicast) **From Rogue Server**



Защита от прослушивания

Коммутаторы: DHCP Snooping



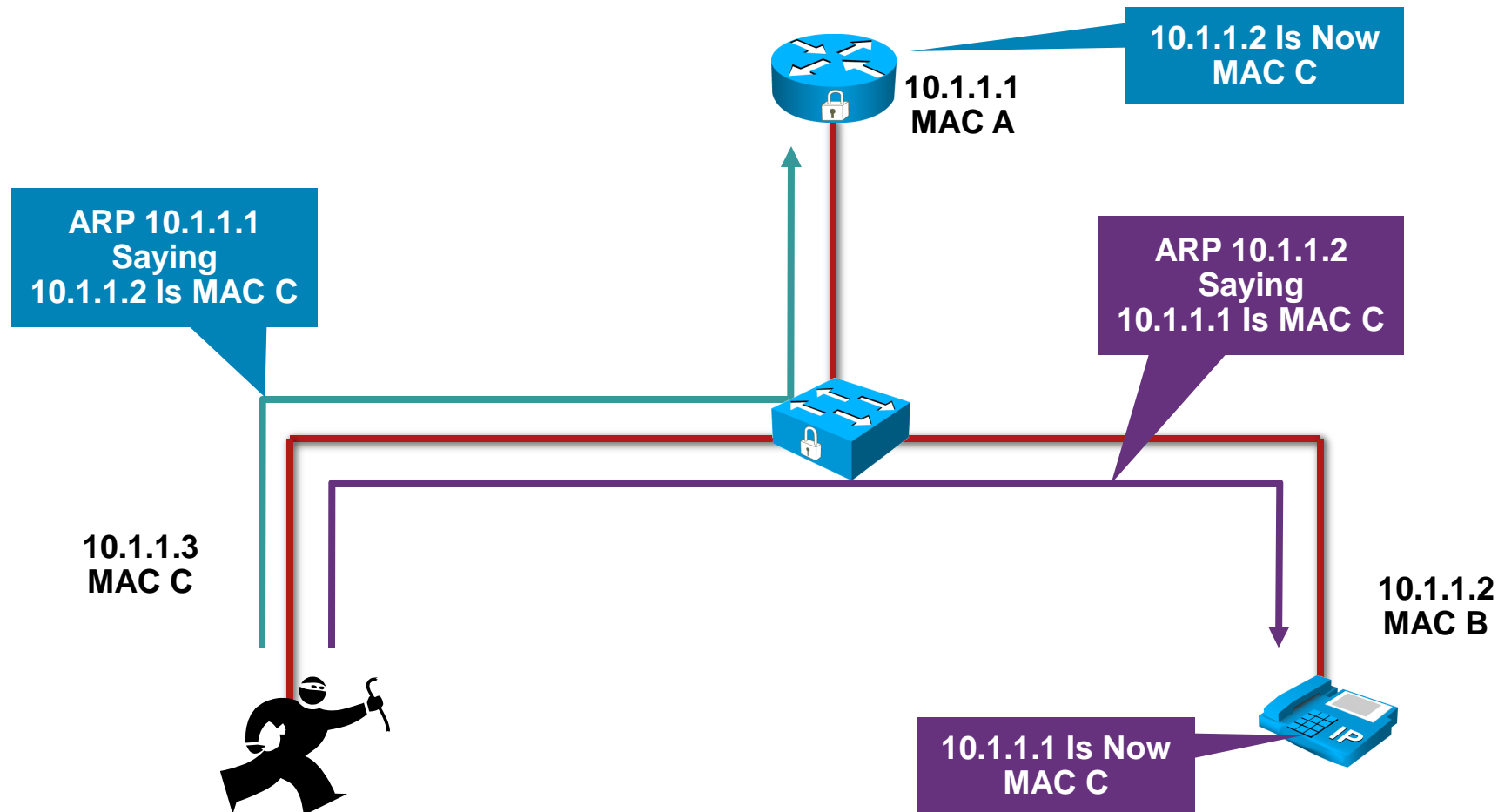
DHCP snooping защищает от того, что кто-то станет неавторизованным DHCP сервером.

Сервер не сможет маршрутизировать трафик на неправильный шлюз (адрес которого выдан неавторизованным DHCP сервером).

Защита от прослушивания

Коммутаторы: ARP атаки

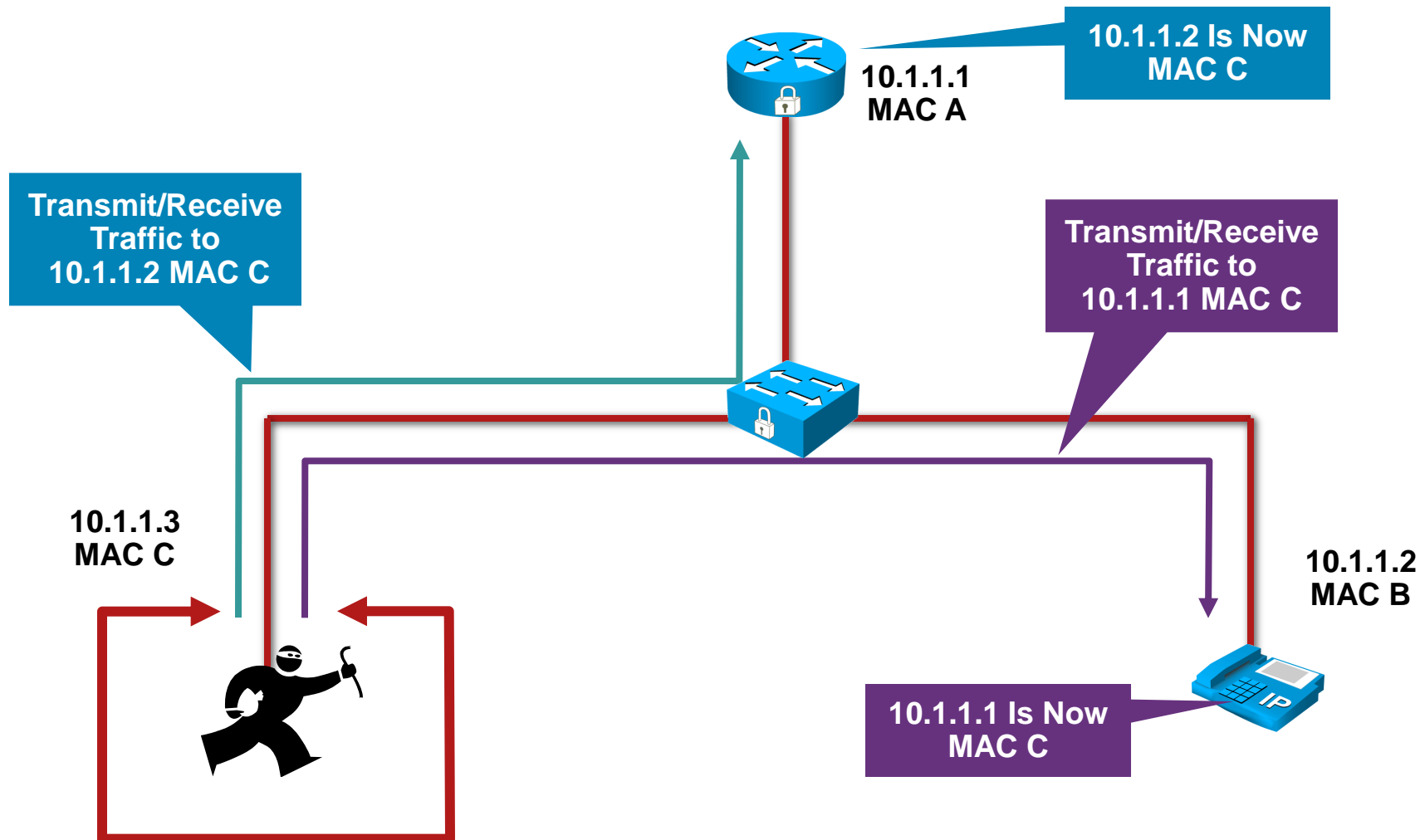
1. Атаки «отравляющие» ARP таблицы.



Защита от прослушивания

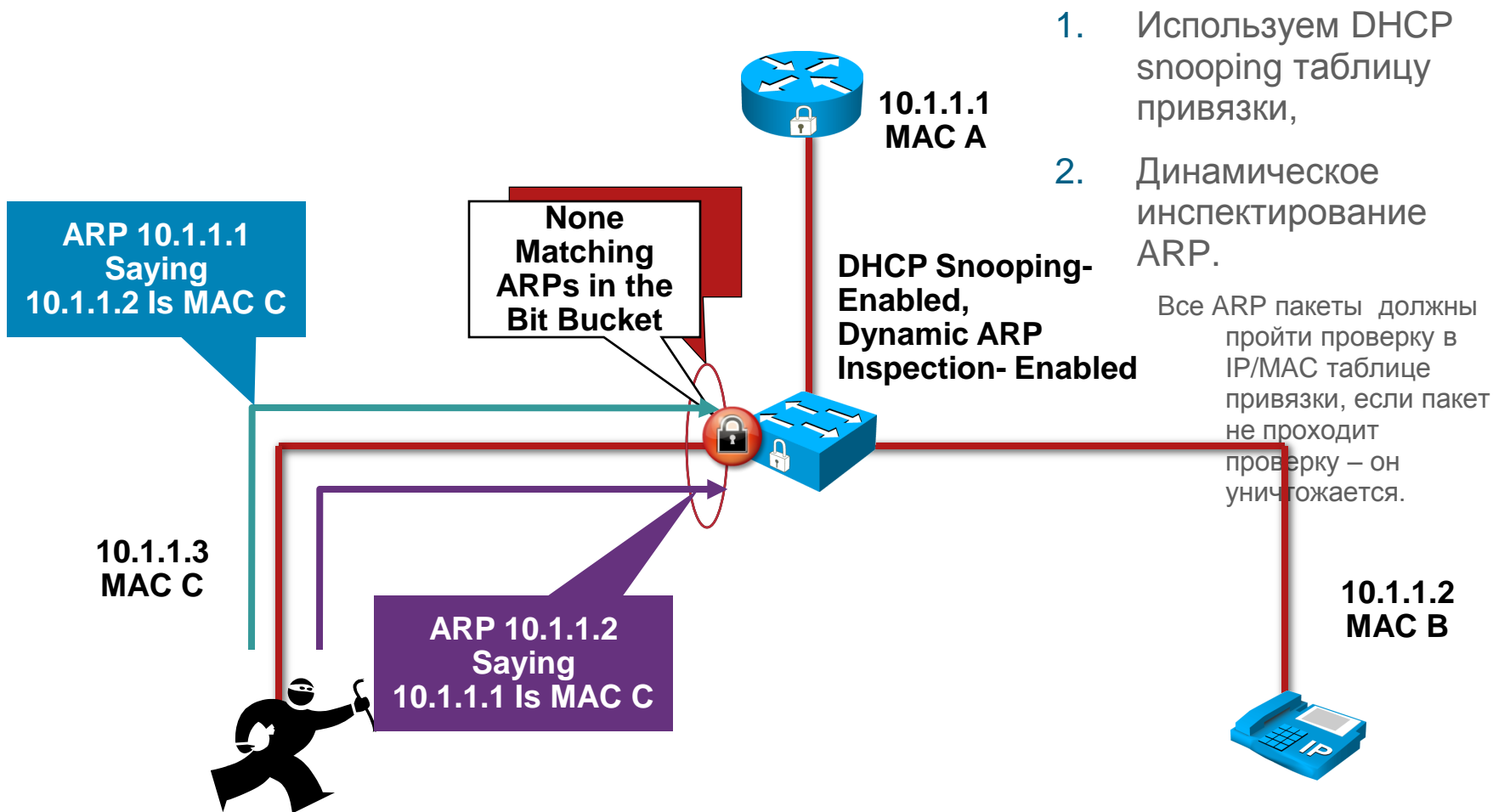
Коммутаторы: ARP атаки

1. Весь трафик идет через атакующего.



Защита от прослушивания

Коммутаторы: Динамическое инспектирование ARP



Маршрутизаторы

1. Наиболее распространенный способ прослушивания на 3 уровне – компрометация маршрутизатора,
2. Злоумышленник контролирующей маршрутизатор – контролирует трафик через него:
 - Использование сильных паролей,
 - Отдельный управляющий канал,
 - Доступ контролируется с помощью ACLs,
 - Защищать HSRP и протоколы маршрутизации,
 - Сервисы безопасности (Cisco ACS аутентификация/авторизация, SSH, и т. д.).

Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- Наиболее распространенные уязвимости/атаки:
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	E-C	E-I	E-I	NA	E-I	NA
Отказ в обслуживании	E	E-I	E-I	I-C	E	E
Заимствование прав	X	X	X	X	X	X
Безопасность ОС приложений	X	X	X	X	X	X
Программные клиенты	X	X	X	X	X	X
Мошенничество	X	X	X	X	X	X

E = легко реализовать; I = средняя степень сложности; C = сложная защита

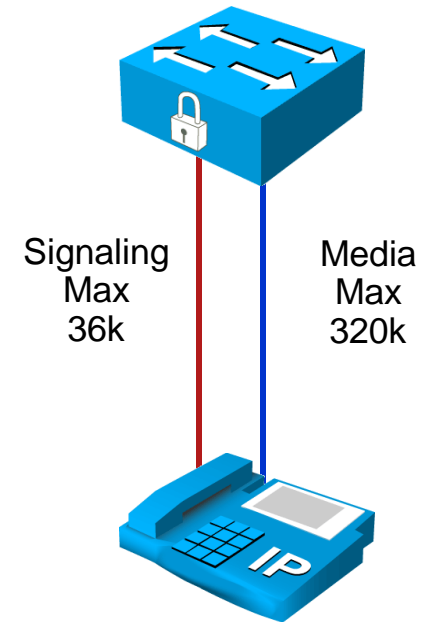
1. Телефоны проходят тестирование на различные виды сетевых атак,
2. Runts, shorts, giants, malformed пакеты, и т.д.,
3. Телефоны не могут принимать SIP пакеты Invite от незарегистрированных в CUCM кластере устройств.

DoS: Коммутаторы

1. Существует множество способов защиты от DoS атак на коммутаторах,
2. Только часть примеров приведено на последующих слайдах,
3. Основное средство, которое вы должны использовать и которое позволит Вам защититься от DoS атак в VoIP:
QoS – качество обслуживания.

1. Базовые QoS ограничения (Auto QoS):
Сигнализация 36к,
Данные 320к.
2. Защищают сервера и приложения от перегрузки,
3. В расширенных функциях QoS вы можете использовать “scavenger class” QoS.

Определяя лимит трафика для пользователя, который маркирован классом ниже чем best effort.



Защита от атак

DoS: Коммутаторы—Port Security (Dynamic)

1. Port security (dynamic) позволяет привязывать ограниченное количество MAC адресов к порту или VLAN,
2. Защищает коммутатор “MAC CAM Flooding Attack”,

```
macof -i eth1
```

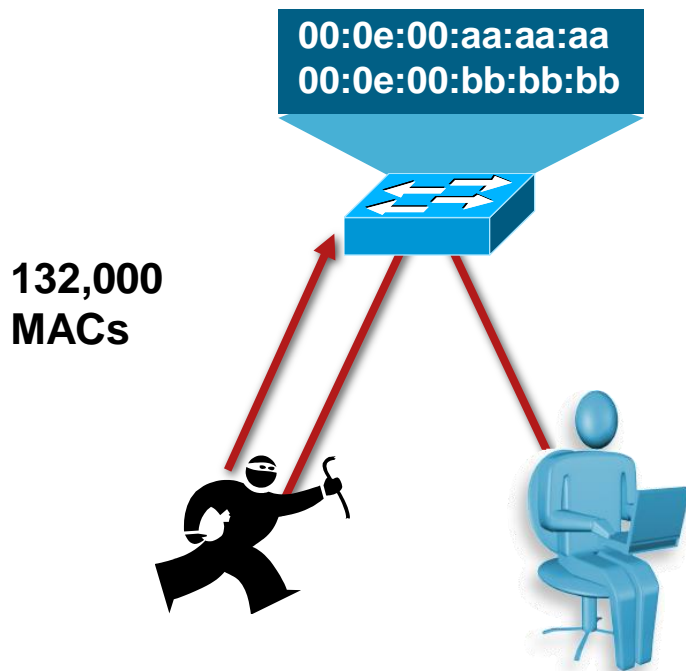
```
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

3. Утилита Macof посылает пакеты со случайными MAC и IP адресами источника,
4. Может генерировать до 8000 MACs в секунду,
5. Превращает Ваш VLAN на коммутаторе а хаб.

Защита от атак

DoS: Коммутаторы—Port Security (Dynamic)

1. Port security ограничивает количество MAC адресов на интерфейсе.



Решение:

- Ограничение количества MAC адресов, при атаке блокирует порт и коммутатор генерирует SNMP.

DoS: Коммутаторы—Voice VLAN

1. Не забывайте о логическом разделении Вашей сети,
2. Легче будет создавать ACLs если все Ваши VoIP устройства находятся внутри непрерывного диапазона IP-адресов,
3. Установите точку контроля на входе и выходе из Вашего сегмента VoIP сети,

Пример: Телефоны используют только UDP протокол для коммуникаций друг с другом, и может быть создан ACL запрещающий TCP трафик между аппаратными телефонами и программными телефонами.

Наиболее успешные атаки базируются на TCP протоколе.

DoS: Коммутаторы—BPDU Guard

1. Если вы построите сеть с loop-free топологией то и не потребуются использование STP,
2. Не запрещайте STP, искусственное или случайное создание «петли» - это еще один вид атаки,
3. Механизм BPDU Guard (Bridge Protocol Data Units)—помогает предотвратить образование петель,
4. Должен быть включен на всех пользовательских портах с помощью команды `port fast`.

DoS: Коммутаторы—Root Guard

1. Блокирует порты по которым приходят BPDU с информацией о новом корневом коммутаторе, что с точки зрения топологии быть не должно,
2. Конфигурируется индивидуально на портах, в зависимости от топологии,
3. Защищает от ошибок в конфигурации и от злоумышленников пытающихся сделать корневым неавторизованный коммутатор.

DoS: Маршрутизаторы

1. QoS,

Самое лучшее, что может быть сделано—система находящаяся под атакой и с загрузкой CPU 99% продолжает передавать высокоприоритетный трафик.

2. Устойчивая маршрутизация,

3. Оптимальное суммирование маршрутов,

4. Базовые ACLs.

Пример: Блокировать UDP порт 1985 от клиентов, так как клиенты не могут посылать HSRP сообщения маршрутизаторам.

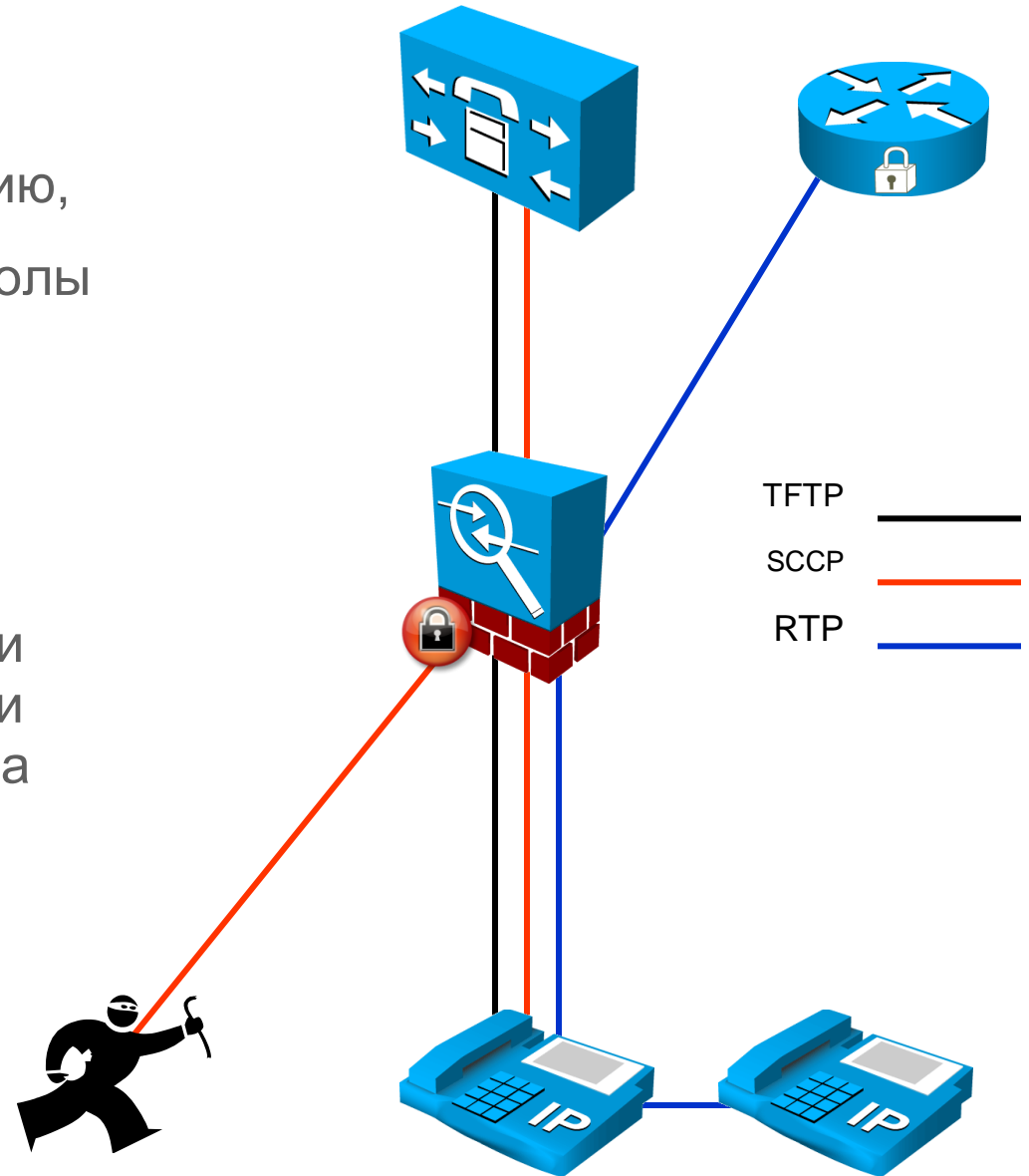
DoS: Межсетевые экраны (МСЭ)

1. Application Layer Gateways (шлюзы уровня приложений) для голосовых протоколов:
H.323, SIP, SCCP, MGCP, RTSP, RTP, RTCP.
2. Пакеты и сообщения проходящие через МСЭ проверяются на соответствие требованиям RFCs или Cisco спецификации,
3. Если сообщение или пакет не удовлетворяют требованиям, то они блокируются,
4. Ограничение по скорости (rate limit) для протоколов на МСЭ.

Защита от атак

DoS: МСЭ

1. Телефон регистрируется, получает OS, конфигурацию,
2. Все используемые протоколы инспектируются,
3. Если происходит что-то нестандартное, то пакет уничтожается,
4. На основании информации сигнализации динамически открываются RTP порты на время сессии.

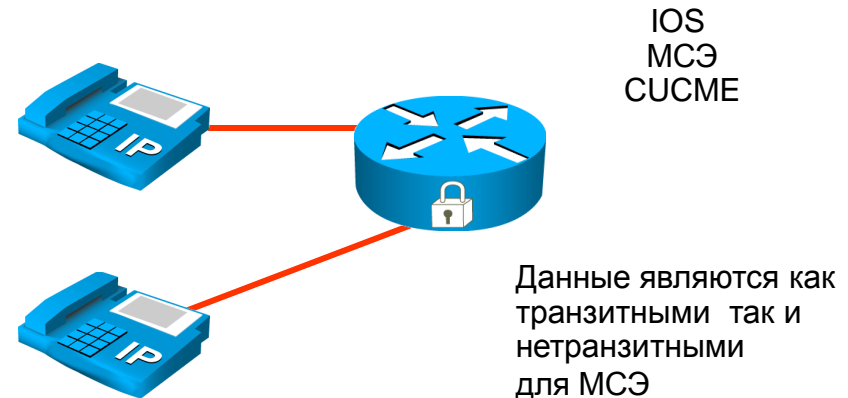
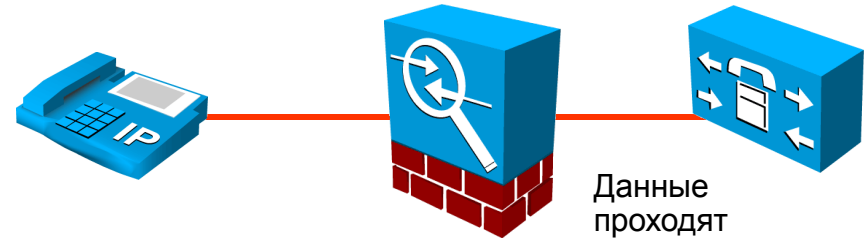


Защита от атак

DoS: МСЭ — Общая информация

1. МСЭ-ы защищают транзитные данные,
2. Новые релизы Cisco IOS МСЭ защищают как транзитные данные так и данные для Cisco Unified Communications Manager Express,
3. Есть возможность создавать зоны безопасности,
4. Есть функция доверенный МСЭ.

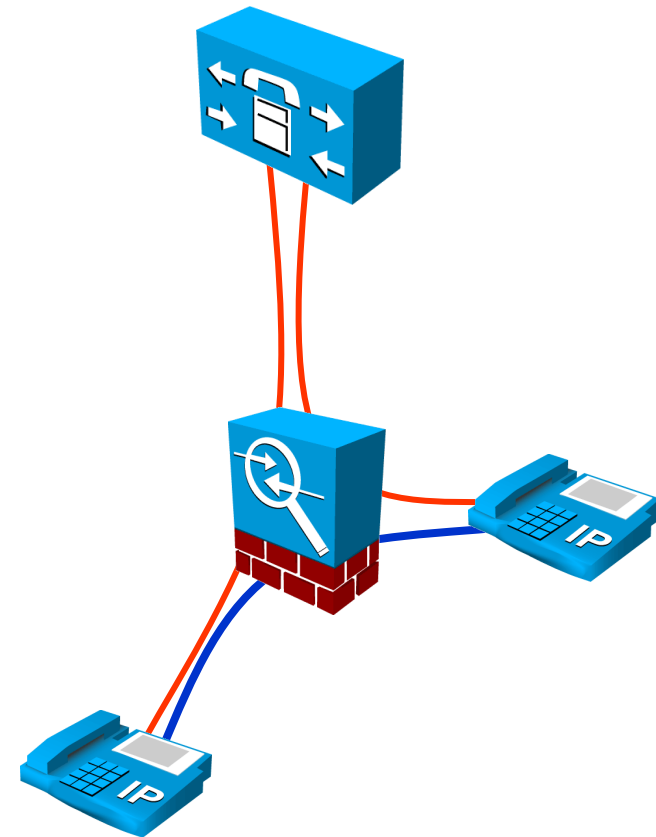
СМЕ сообщает МСЭ какой voice трафик разрешить через IOS МСЭ.



Защита от атак

DoS: МСЭ — Общие правила

1. Сигнализация должна быть известна,
Если МСЭ понимает сигнализацию, то RTP работает корректно.
2. Если Вы делаете обновление ПО голосовых приложений, то возможно следует делать обновление ПО МСЭ,
3. Постоянно отслеживайте изменения в VoIP сети,
4. Проверяйте на совместимость версии ПО.



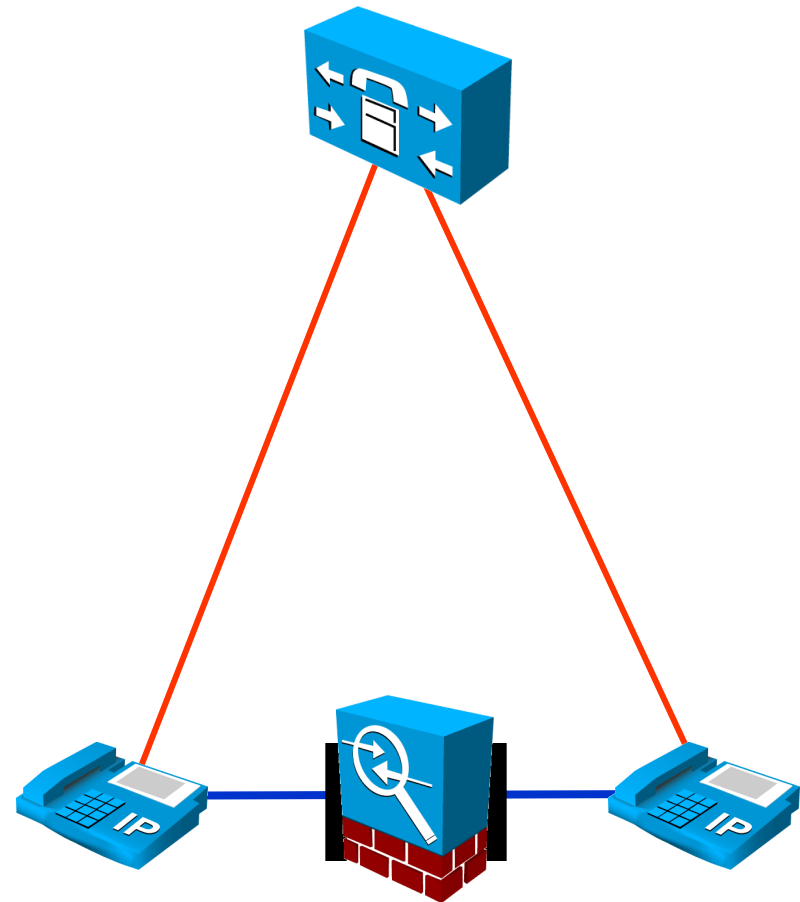
<http://www.cisco.com/go/firewalls/>

Сигнализация — (red line)
Голос и видео — (blue line)

Защита от атак

DoS: МСЭ — Общие правила

1. **Анализируйте место расположения МСЭ:**
МСЭ не видит сигнализации,
Голос не идет через МСЭ,
Вызовы не проходят.
2. VoIP дизайн может стать сложнее с использованием МСЭ,
3. В этом примере Вы должны статически описать диапазон UDP портов для RTP (используя ACL).



Сигнализация — (red line)
Голос и видео — (blue line)

Защита от атак

DoS: МСЭ — Общие правила

1. Учитывайте масштабируемость МСЭ,
2. Придерживайтесь правила 10% — 10% телефонов всегда делают вызов в любой момент времени,
3. Следите за загрузкой CPU, что бы он была менее 60% для всех типов трафика,
4. В ASA реализован QoS и соответственно вы можете его использовать на низкоскоростных линках.

Firewall	Кол-во телефонов
ASA 5510	До 200
ASA 5520	500-5,000
ASA 5540	5000-15,000
ASA 5550	15,000-30,000
ASA 5580	До 60,000

Защита от атак

DoS: MCЭ — TLS Proxy

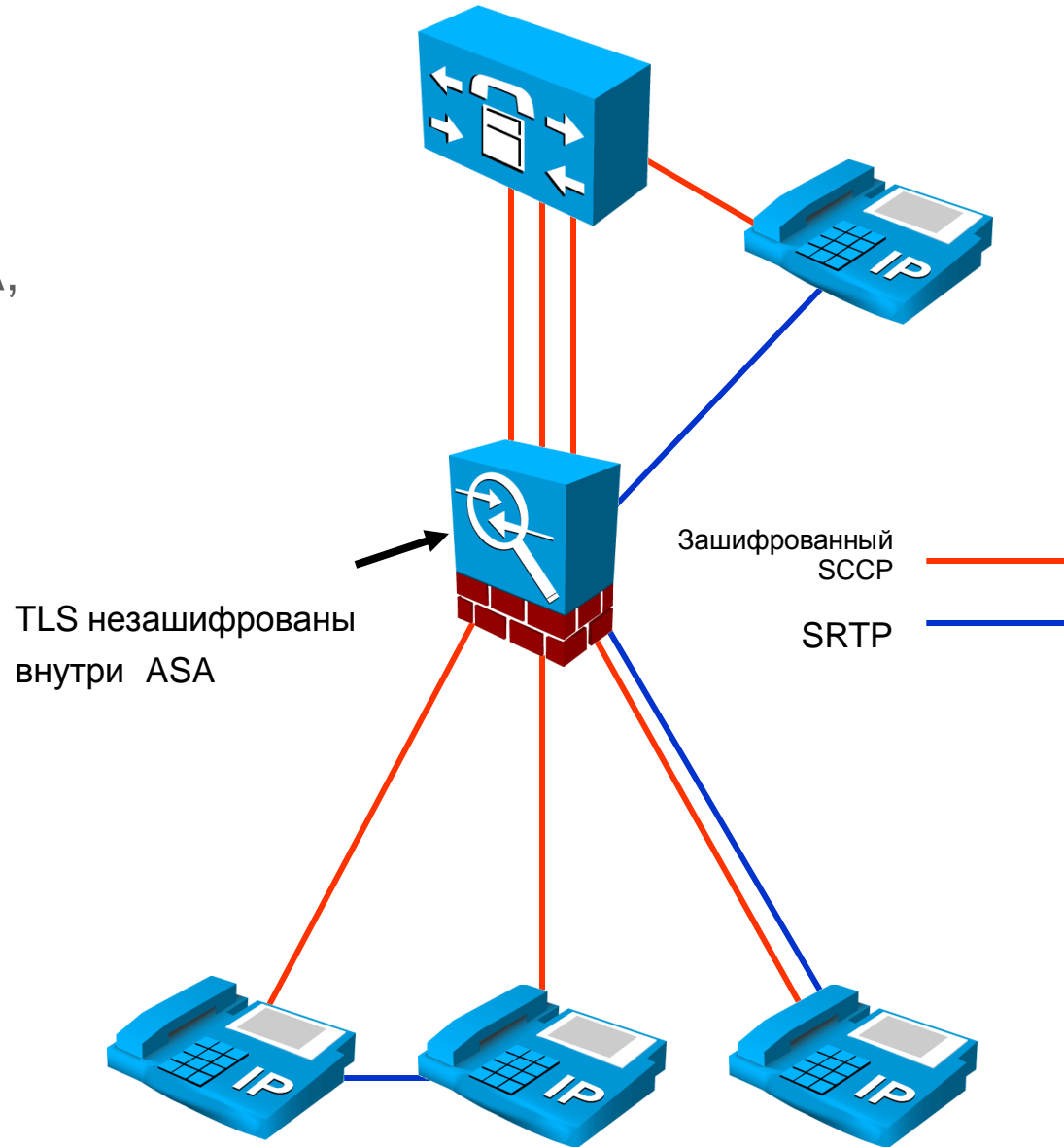
ASA MCЭ может инспектировать TLS сигнализацию

1. ASA присутствует в CTL листе, как доверенное устройство для телефонов и CUCM,
2. TLS сигнализация терминируется на ASA,
3. ASA расшифровывает TLS,
4. ASA инспектирует сигнализацию,
5. ASA зашифровывает TLS,
6. ASA открывает порты для SRTP,
7. ASA закрывает порты для SRTP, если видит в сигнализации завершение сессии.

Защита от атак

DoS: MCЭ — TLS Proxy

1. У каждого телефона своя TLS сессия с ASA,
2. Порты для SRTP открываются и закрываются по информации сигнализации,
3. SRTP не инспектируется,
4. SRTP может идти а может не идти через ASA.



Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- **Наиболее распространенные уязвимости/атаки:**
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - **Заимствование прав,**
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	E-C	E-I	E-I	NA	E-I	NA
Отказ в обслуживании	E	E-I	E-I	I-C	E	E
Заимствование прав	E/C	C	N/A	C	E	I
Безопасность UC приложений	X	X	X	X	X	X
Программные клиенты	X	X	X	X	X	X
Мошенничество	X	X	X	X	X	X

E = легко реализовать; I = средняя степень сложности; C = сложная защита

Защита от атак

Заимствование прав:

Механизмы которые уже рассматривались в предыдущих разделах:

1. Подписанные ЭЦП файла OS телефонов,
2. Подписанные ЭЦП конфигурационные файлы,
3. TLS/SRTP.

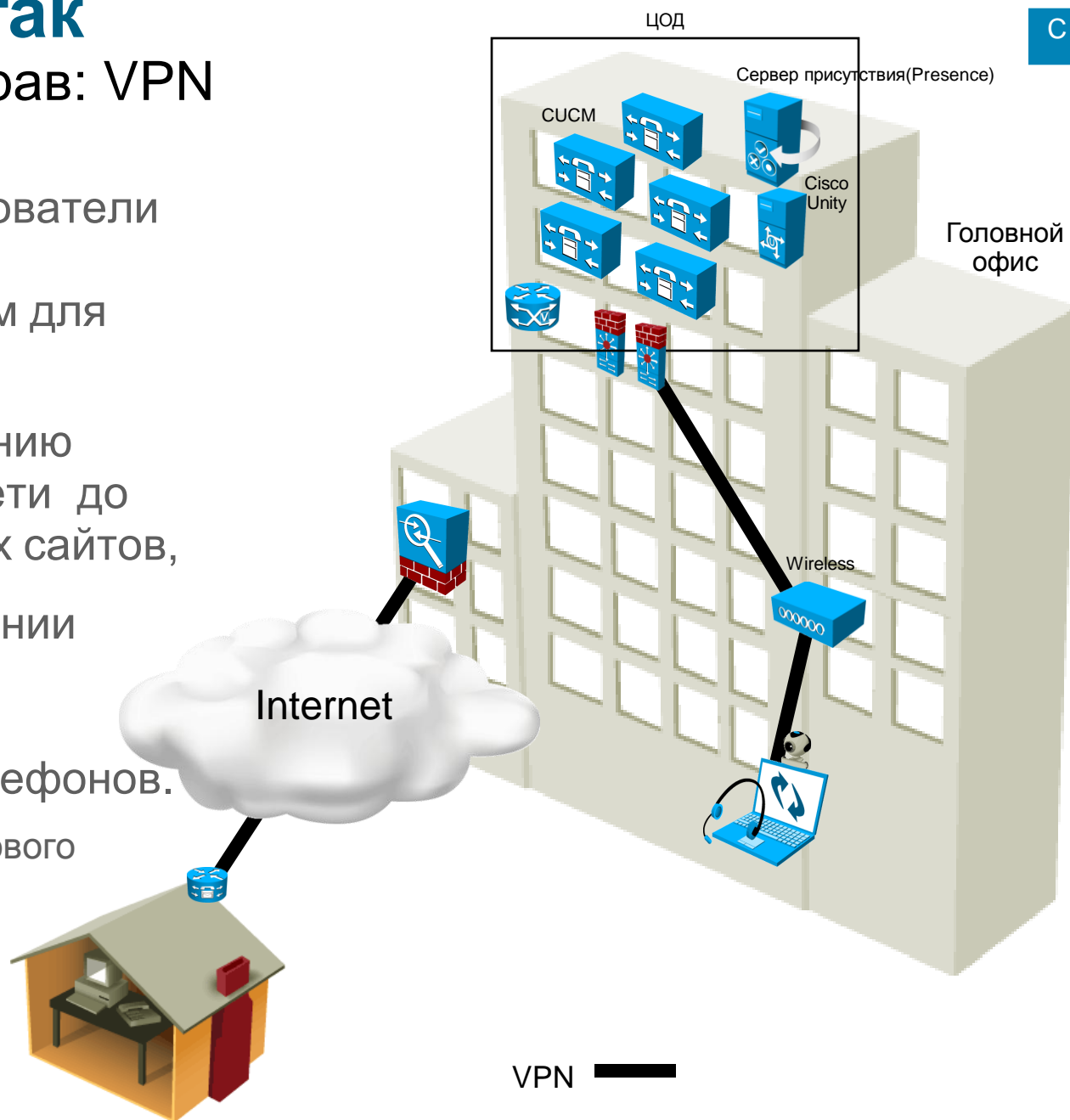
Использование VPN для удаленных телефонов (аппаратных и программных):

1. Для аппаратных телефонов Вам необходим маршрутизатор,
2. Для программных телефонов необходим VPN клиент на PC.

Защита от атак

Заимствование прав: VPN

1. Домашние пользователи обеспечены VPN соединением для всего трафика,
2. Ведет к расширению корпоративной сети до пользовательских сайтов,
3. Некоторые компании используют VPN для подключения программных телефонов.
Для контроля голосового трафика.



Защита от атак

Заимствование прав: Phone Proxy

1. ASA может быть использована как phone proxy для удаленных пользователей:

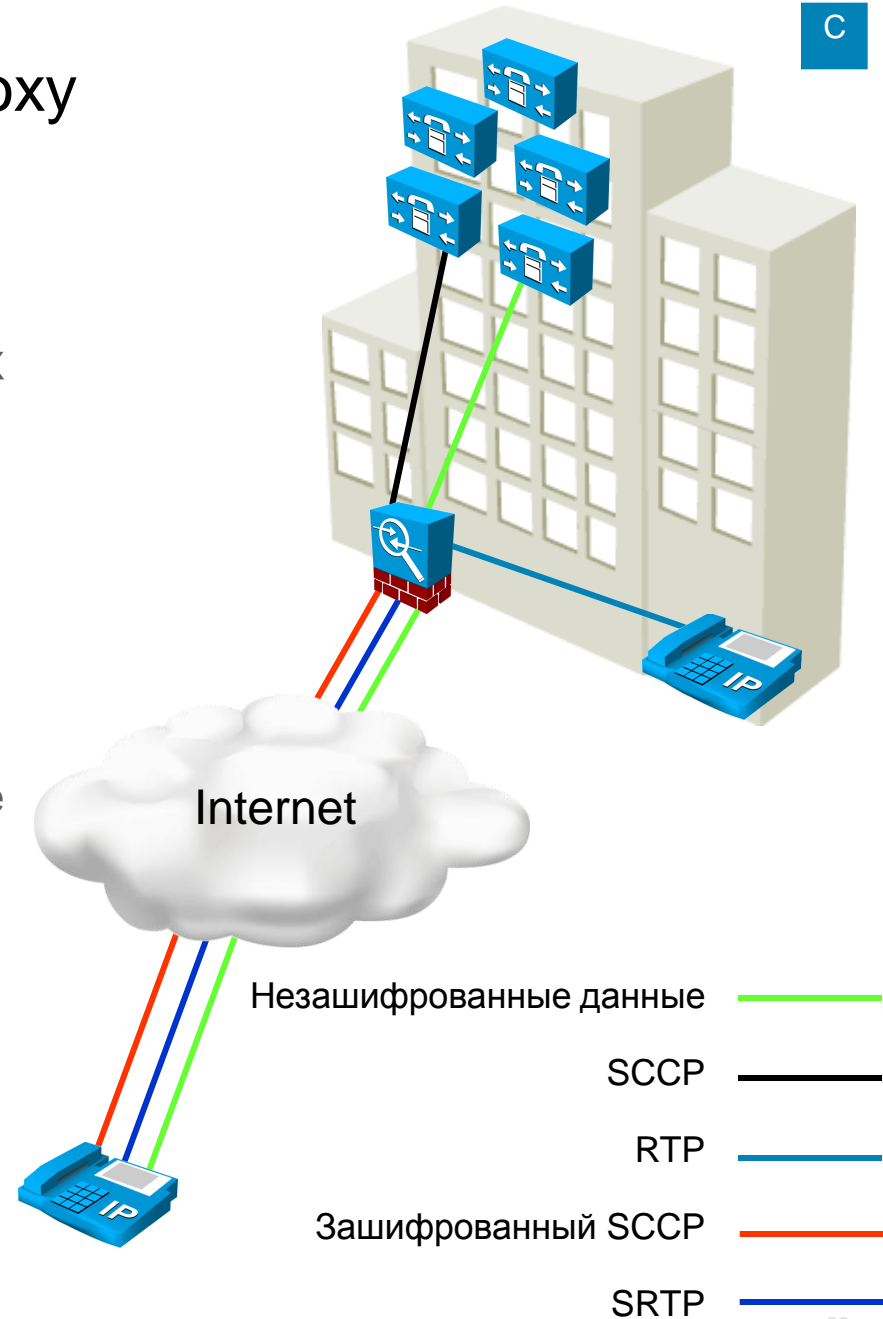
Зашифрованный трафик для TLS и SRTP от удаленных пользователей,

Все остальные сообщения от телефона незашифрованы,

Все сервисы запрещены, если они не зашифрованы—поиск по директории, услуги и т.д.,

Данные могут быть зашифрованы или нет внутри сети предприятия.

2. ASA 8.04.



Защита от атак

Заимствование прав: Cisco Security Agent (CSA)



CSA на программных телефонах:

1. Может быть использован для контроля рабочих станций,
2. Может быть сконфигурирован так, что бы запретить установку новых приложений или наложить ограничения на работу приложений,
3. Может контролировать QoS маркирование, используемое приложениями,
4. Также контролирует порты, используемые приложениями.

Заимствование прав: Сеть

1. 802.1x на аппаратных телефонах,

Вместо идентификации средствами приложений может быть использована сетевая идентификация,

Может быть использовано совместно с функцией мобильный профиль пользователя (extension mobility),

После успешной аутентификации телефон нормально работает в сети.

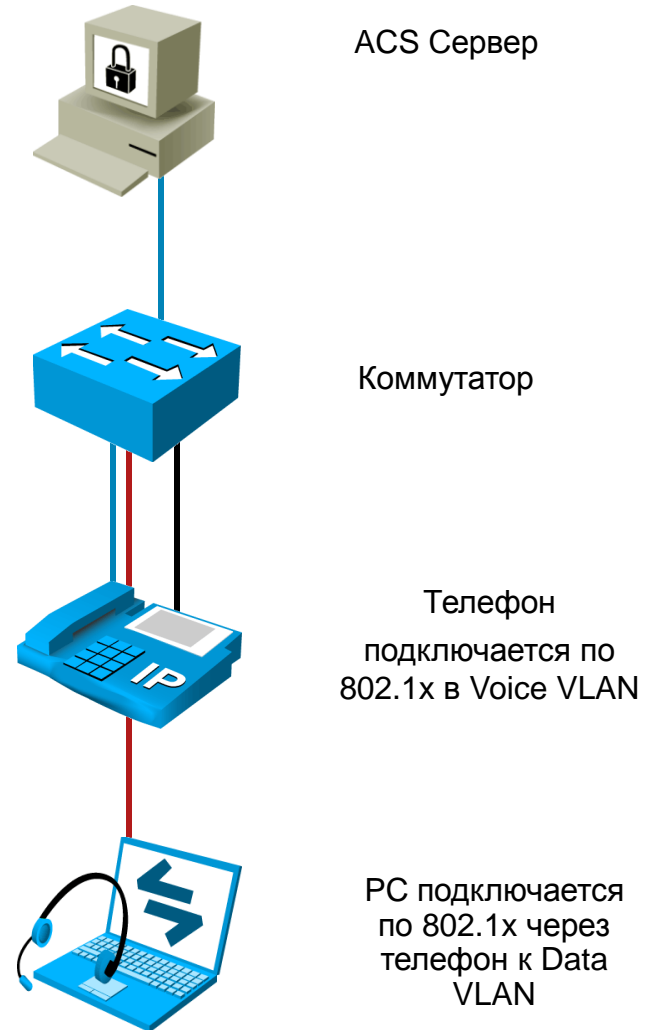
2. 802.1x на рабочих станциях.

Для аутентификации пользователей или рабочих станций в сети.

Защита от атак

Заимствование прав: Сеть

1. 802.1x протокол, который дает разрешение на подключение к сети,
2. Cisco предлагает EAP-TLS 802.1x:
На основе MIC (Manufactured Installed Cert)
или
LSC (Locally Significant Cert).
Используется метод информации с устройства против старого метода на основе информации пользователя.
3. Мульти-доменная аутентификация (MDA) с MAC-аутентификацией (MAB).
MDA аутентификация двух устройств и помещение устройств в соответствующие VLAN-ы.
MAB аутентифицирует по MAC адресам для устройств, где нет агента 802.1x (supplicant).



Идентификация средствами приложений:

1. Используем CUCM для идентификации телефонов—если телефона нет в базе CUCM, то он не может зарегистрироваться,
2. Существует возможность авторегистрации телефонов.

Следует запретить в целях безопасности!

Защита от атак

Заимствование прав: Приложения

1. Улучшение политики в 6.0 для паролей:

Длина,

Сложность,

Блокировка,

Время действия,

История,

и т.д..

2. Удовлетворяет большинству требований пользовательских политик безопасности.

Credential Policy Information	
Display Name*	<input type="text"/>
Failed Logon*	<input type="text" value="3"/>
Reset Failed Logon Attempts Every*	<input type="text" value="30"/>
Lockout Duration*	<input type="text" value="30"/>
Minimum Duration Between Credential Changes*	<input type="text" value="0"/>
Credential Expires After*	<input type="text" value="180"/>
Minimum Credential Length*	<input type="text" value="8"/>
Stored Number of Previous Credentials*	<input type="text" value="12"/>
Inactive Days Allowed*	<input type="text" value="0"/>
Expiry Warning Days*	<input type="text" value="0"/>
<input checked="" type="checkbox"/> Check for Trivial Passwords	

<input type="checkbox"/> No Limit for Failed Logons
<input type="checkbox"/> Administrator Must Unlock
<input type="checkbox"/> Never Expires

Credential Information	
<input type="checkbox"/> Locked by Administrator	
<input type="checkbox"/> User Cannot Change	
<input type="checkbox"/> User Must Change at Next Login	
<input checked="" type="checkbox"/> Does Not Expire	
<input type="checkbox"/> Reset Hack Count	
Authentication Rule*	Default Credential Policy
Time Last Changed	December 11, 2006 08:59:40 MST
Failed Logon Attempts	<input type="text" value="0"/>
Time of Last Failed Logon Attempt	<input type="text"/>
Time Locked by Administrator	<input type="text"/>
Time Locked Due to Failed Logon Attempts	<input type="text"/>

Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- Наиболее распространенные уязвимости/атаки:
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	E-C	E-I	E-I	NA	E-I	NA
Отказ в обслуживании	E	E-I	E-I	I-C	E	E
Заимствование прав	E/C	C	N/A	C	E	I
Безопасность UC приложений	N/A	N/A	N/A	N/A	E/I	E
Программные клиенты	N/A	N/A	N/A	E/I	E	N/A
Мошенничество	X	X	X	X	X	X

E = легко реализовать; I = средняя степень сложности; C = сложная защита

UC Приложения: CUCM/Сервера

1. CSA позволяет открыть только те порты и запустить только те процессы, которые необходимы для работы,
2. Основные функции CSA:

Процесс между сетевыми интерфейсом и kernel, просматривающий весь трафик,

Процесс между приложением и kernel для отслеживания корректности работы приложения,

Для управления CSA клиентами требуется CSA консоль управления.

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/product_data_sheet09186a00801f8e59.html

UC Приложения: CUCM/Сервер

1. CSA для Windows:

Управляемый для Windows,

Управляемая система позволяет импортировать новые политики <http://www.cisco.com/go/software> если это необходимо,

CSA не включен в инсталляцию Windows.

2. CSA для предустановленных систем:

Неуправляемый для предустановленных систем,

CSA устанавливается во время установки CUCM.

UC Приложения: CUCM/Сервера

1. МСЭ приложений встроен в Windows версию CUCM,
2. Предустановленная версия CUCM использует ippref как МСЭ приложений,
Разрешает только межкластерные коммуникации, включенные в IPTables МСЭ.
3. Windows версия CUCM может так же включать:
Поддерживаемые антивирусы, которые могут работать на системе.

Обзор CUCM МСЭ

1. Ограничивает IPv4 трафик к серверу и от сервера,
2. Можно создавать динамические правила,
3. Использует cluster node лист (список серверов кластера) управляемый процессом Cluster Manager внутри CUCM,
4. ipprefs новый сервис по обновлению правил.

7.X CUCM.

Правила по умолчанию для МСЭ

1. Весь localhost трафик разрешен,
2. Весь исходящий трафик разрешен,
3. Трафик всех установленных соединений разрешен (established),
4. Весь ICMP разрешен, но ограничен по полосе (rate-limited),
5. Все остальное запрещено.

Конфигурация МСЭ

1. Каждый сервис регистрирует используемые порты,
2. Типы портов:
 - Публичный порт—для внешних клиентов,
 - Частный порт—для клиентов внутри кластера,
 - Порт трансляции—публичный порт, транслируемый в частный порт.
3. Порты должны быть открыты (происходит когда запускается сервис).

Информация из пользовательского интерфейса (GUI)

The screenshot displays the Cisco Unified Operating System Administration web interface. At the top, the Cisco logo and the title "Cisco Unified Operating System Administration" are visible, along with the subtitle "For Cisco Unified Communications Solutions". The navigation bar includes "Navigation" with a dropdown menu set to "Cisco Unified OS Administration" and a "GO" button. Below this, there are links for "admin", "About", and "Logout". A secondary navigation bar contains "Show" and several dropdown menus: "Settings", "Security", "Software Upgrades", "Services", and "Help". A left-hand sidebar menu is open, listing "Cluster", "Hardware", "Network", "Software", "System", and "IP Preferences", with "IP Preferences" highlighted. The main content area features a large blue banner with the text "Cisco Unified Operating System Administration" and "Version: 7.0.0.39000-9002". To the right of the banner is a photograph of a server rack aisle. Below the banner, there is a small "IP Preferences" button. The footer contains the following text: "Copyright © 1999 - 2008 Cisco Systems, Inc. All rights reserved.", a disclaimer about cryptographic features, and a link to U.S. laws governing Cisco cryptographic products: <http://www.cisco.com/wwl/export/crypto/tool/starg.html>. It also provides an email address for further assistance: export@cisco.com.

Информация из пользовательского интерфейса (GUI)

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration Go

admin | About | Logout

Show Settings Security Software Upgrades Services Help

IP Preferences

Status

51 records found

IP Preferences (1 - 50 of 51) Rows per Page 50

Find IP Preferences where Application begins with Find Clear Filter

Select item or enter search text

Application	Protocol	Port Number	Type	Translated Port	Status	Description
sshd	tcp	22	Public		Enabled	sftp and ssh access
CiscoDRFMaster	tcp	4040	Public		Enabled	DRS Master Agent port
racoon	esp		Public		Enabled	ipsec traffic
racoon	udp	500	Public		Enabled	ipsec setup port
clm	udp	8500	Public		Enabled	cluster manager
clm	tcp	8500	Public		Enabled	cluster manager
syslogd	udp	514	Public		Disabled	syslog port
tomcat	tcp	8443	Translated	443	Enabled	secure web access
tomcat	tcp	8080	Translated	80	Enabled	web access
ntpd	udp	123	Public		Enabled	network time sync
soapmonitor	tcp	5007	Public		Enabled	soapmonitor port
dhcpd	udp	67	Public		Disabled	DHCP server port
cmoninit	tcp	1500	Private		Enabled	IDS port for DB clients
dblrpc	tcp	1515	Private		Enabled	DB replication port
dbmon	tcp	8001	Private		Enabled	DB change notification port
RisDC	tcp	2555	Private		Enabled	RISDC service port
RisDC	tcp	2556	Private		Enabled	RISDC service port
snmpdm	udp	161	Public		Enabled	SNMP
amc	tcp	1090	Private		Enabled	AMC RMI Object Port
amc	tcp	1099	Private		Enabled	AMC RMI Registry Port
ctlprovider	tcp	2444	Public		Enabled	ctlprovider
capf	tcp	3804	Public		Enabled	CAPF
ccm	tcp	8002	Public		Enabled	CCM SDL Link
ccm	tcp	1720	Public		Enabled	H225 SIGNAL
ccm	udp	1719	Public		Disabled	RAS SIGNAL
ccm	tcp	2000	Public		Enabled	SCCP-SIG
ccm	tcp	2001	Public		Enabled	TITAN CONVERT
ccm	tcp	2002	Public		Enabled	VEGA CONVERT
ccm	udp	2427	Public		Enabled	MCCP

Информация из пользовательского интерфейса (GUI)

1. Показывает список портов, которые были зарегистрированы, так же отображается тип порта и его статус (открыт/закрыт),
2. Дополнительно видно, какое приложение зарегистрировало порт,
3. На странице GUI есть возможности производить поиск по фильтру (открытые порты, номер порта и т.д.).

Защита от атак

Программные клиенты:

Механизмы безопасности для защиты от атак на программных клиентов, уже рассмотренные в предыдущих секциях:

1. 802.1x,
2. CSA,
3. VPN.

Программные клиенты: CSA

CSA на программных клиентах:

1. Может быть использован для контроля рабочих станций,
2. Может быть сконфигурирован так, что бы запретить установку новых приложений или наложить ограничения на работу приложений,
3. Может контролировать QoS маркирование, используемое приложениями,
4. Так же контролирует порты, используемые приложениями.

Программные клиенты: 802.1x

Клиент 802.1x:

1. Используется для идентификации пользователей и рабочих станций,
2. Динамически помещает рабочую станцию в соответствующий VLAN,
3. Аутентификация на основе VLAN позволяет контролировать доступ к системе UC.

Программные клиенты: VPN

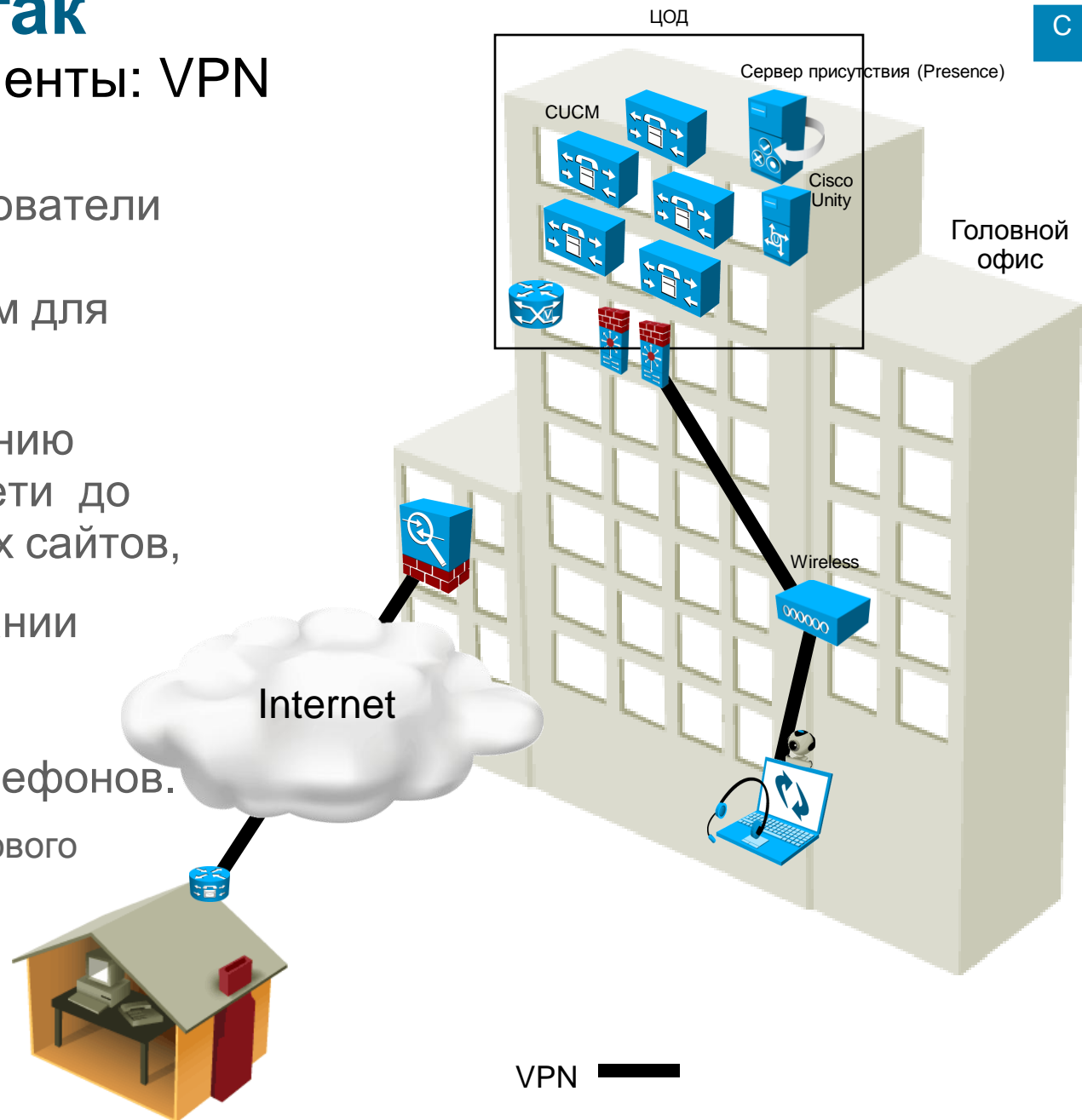
VPN для удаленных клиентов и для клиентов внутри периметра:

1. Позволяет удаленными пользователями использовать корпоративную телефонию,
2. Позволяет контролировать пользователей в корпоративной сети.

Защита от атак

Программные клиенты: VPN

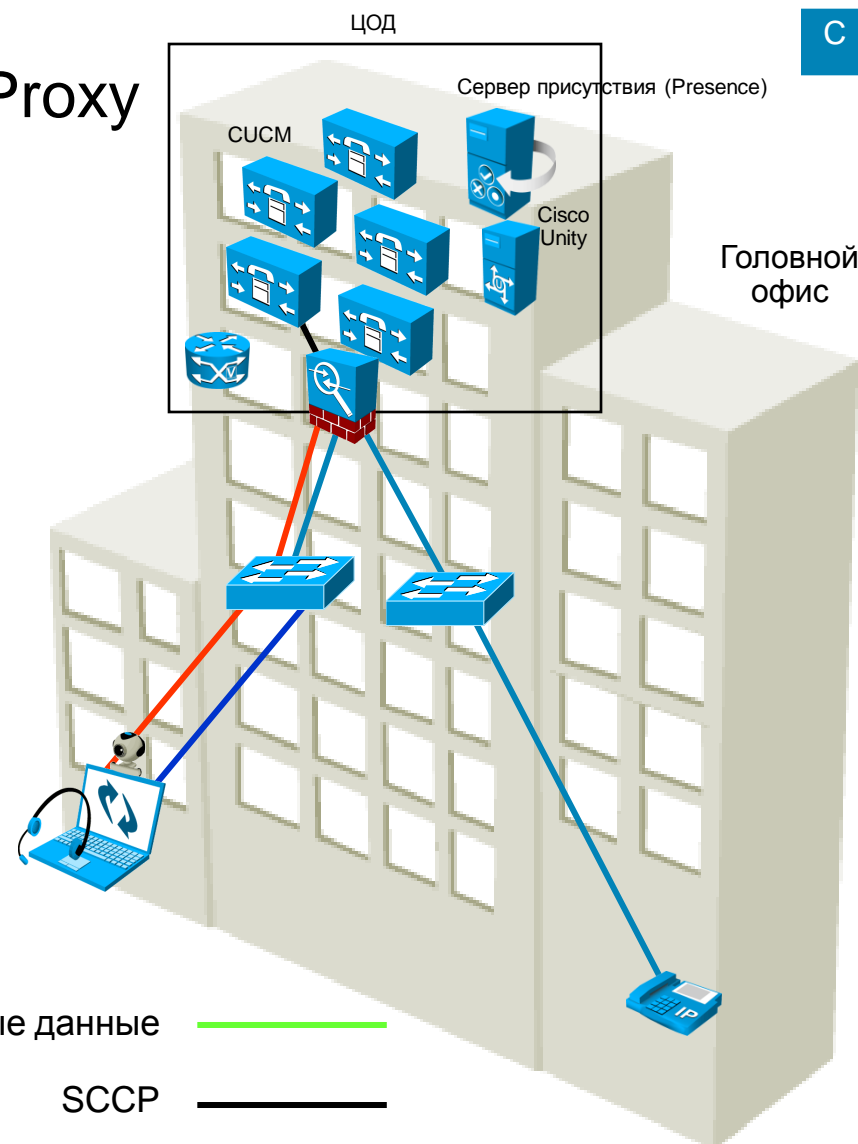
1. Домашние пользователи обеспечены VPN соединением для всего трафика,
 2. Ведет к расширению корпоративной сети до пользовательских сайтов,
 3. Некоторые компании используют VPN для подключения программных телефонов.
- Для контроля голосового трафика.



Защита от атак

Программные клиенты: Phone Proxy

1. Phone proxy может быть использован для контроля доступа в и из голосовых VLAN-ов,
2. Может быть рассмотрен как метод контролируемого внедрения программных телефонов,
3. Только в режиме аутентификации,
4. ASA 8.04.



Оглавление

- Какой уровень безопасности необходим для системы унифицированных коммуникаций,
- Состав системы унифицированных коммуникаций,
- Наиболее распространенные уязвимости/атаки:
 - Несанкционированное прослушивание,
 - Отказ в обслуживании (DoS и DDoS),
 - Заимствование прав,
 - Уязвимости приложений системы унифицированных коммуникаций,
 - Мошенничество.

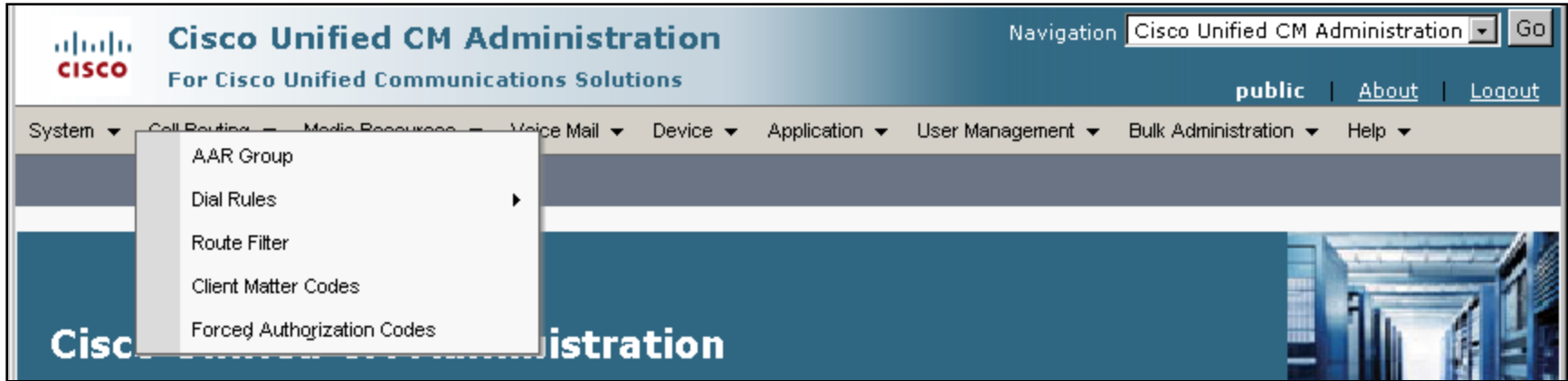
Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	E-C	E-I	E-I	NA	E-I	NA
Отказ в обслуживании	E	E-I	E-I	I-C	E	E
Заимствование прав	E/C	C	N/A	C	E	I
Безопасность UC приложений	N/A	N/A	N/A	N/A	E/I	E
Программные клиенты	N/A	N/A	N/A	E/I	E	N/A
Мошенничество	N/A	N/A	E	N/A	E	N/A

E = легко реализовать; I = средняя степень сложности; C = сложная защита

Защита от атак

Мошенничество: CUCM



1. Переадресация вызова, удаленная переадресация и переводы с транка на транк – функции, создающие возможности для мошенничества с телефонным трафиком,
2. Partitions и calling search spaces ограничивают доступ абонентам к услугам и другим абонентам,
3. Фильтры плана нумерации контролируют доступ к используемым телефонным номерам,
4. Ad hoc конференции принудительно завершаются если организатор вышел из конференции,
5. Forced authentication codes и client matter codes предотвращают неавторизованные звонки и обеспечивают информацию для биллинга и трекинга.

Мошенничество: Маршрутизаторы

Ограничить пользователям доступ к шлюзам:

1. Ограничить трафик от пользователей к маршрутизаторам только необходимым— RTP/UDP,
2. Нет причин давать пользователям посылать TSP трафик на шлюз.

Заключение

1. Сначала надо определить политику безопасности,
2. После определения политики безопасности идет выбор механизмов безопасности, которые будут использоваться,
3. Определяется место, где будут использоваться механизмы безопасности:
 - В сети,
 - В приложениях.
4. По возможности, перед внедрением, тестируйте механизмы безопасности,
 - Это позволит вам определить что необходимо подстроить в механизмах,
 - Даст опыт по поиску и устранению неисправностей.

Предотвращение атак

	Телефоны	Коммутаторы	Маршрутизаторы	Сеть	CUCM	Сервера
Прослушивание	E-C	E-I	E-I	NA	E-I	NA
Отказ в обслуживании	E	E-I	E-I	I-C	E	E
Заимствование прав	E/C	C	N/A	C	E	I
Безопасность UC приложений	N/A	N/A	N/A	N/A	E/I	E
Программные клиенты	N/A	N/A	N/A	E/I	E	N/A
Мошенничество	N/A	N/A	E	N/A	E	N/A

E = легко реализовать; I = средняя степень сложности; C = сложная защита

Вопросы и Ответы

security-request@cisco.com

Мы хотели бы узнать Ваше мнение

Пожалуйста,
заполните анкету





CISCO