

Интеграция пароля гостевого пользователя ISE с CM шлюз на основе постфикса и примера конфигурации Kannel

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Преимущества CM шлюз](#)

[Диаграмма сети и поток трафика](#)

[Конфигурации](#)

[ISE](#)

[Постфикс](#)

[Maildrop с Mailfilter](#)

[Kannel](#)

[Проверка](#)

[ISE](#)

[Постфикс](#)

[Maildrop](#)

[Mailfilter](#)

[Kannel](#)

[Гостевой телефон](#)

[Устранение неполадок](#)

[ISE](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как интегрировать решения с открытым исходным кодом (Постфикс, Maildrop, Kannel) с платформой Cisco Identity Services Engine (ISE) для отправки сообщения Службы коротких сообщений (SMS) пользователям с гостевыми учетными записями.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco ISE и гостевой доступ
- Linux и сценарии Shell

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 1.2 Cisco ISE или позже
- Постфиксная версия 2.10
- Версия 2.6.0 Maildrop
- Версия 1.5.0 Kannel

Примечание: Доводим до вашего сведения, что Постфикс, Maildrop и Kannel являются решениями с открытым исходным кодом, и Cisco не поддерживает эти продукты. Этот пример конфигурации просто представляет, как ISE может быть интегрирован с другими продуктами для отправки комплексного решения.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

ISE позволяет, что вы для создания гостя объясняете доступ временной сети, как правило, для гостей, посетителей, подрядчиков, консультантов и клиентов. Такие учетные записи созданы пользователями спонсора через Портал Спонсора. При создании учетной записи возможно передать динамично генерируемый пароль для доступа с СМ непосредственно к мобильному телефону гостя.

Cisco ISE в состоянии передать эти учетные данные по электронной почте с Протоколом SMTP к шлюзу Mail2SMS. Этот шлюз ответственен за доставку СМ.

Настройка

Преимущества СМ шлюз

На рынке существуют множественные решения для шлюза Mail2SMS. Они могут обычно получать данные с использованием других протоколов, таких как SMTP, Одноранговое короткое сообщение (SMPP), FTP, HTTP (Простой протокол доступа к объектам (SOAP),

веб-сервисы), и передавать SMS-сообщение к определенному мобильному телефону.

Могло бы быть лучше создать ваш собственный шлюз СМ. Это обеспечивает:

- Большая гибкость
- Способность создать составные правила о маршрутизации (контролируемый по времени, на основе политики, основанный на содержании)
- Интеграция с локальными базами данных (например, другая политика маршрутизации для других Групп Active Directory)
- Потенциально понизьте эксплуатационные расходы (никакая потребность заплатить за внешний сервис)
- Возможность использовать это решение также для предупреждений состояния, генерируемых ISE и передаваемых как электронные почты

Могло бы стоить иметь смешанные развертывания - персональный шлюз СМ, который также интегрирован с внешним сервисом.

Диаграмма сети и поток трафика

Вот поток:

1. Пользователь спонсора создает гостевую учетную запись с уведомлением SMS-сообщением и предоставляет номер мобильного телефона для пользователя. ISE посылает электронное письмо настроенному серверу SMTP. Адрес источника (От) принадлежит до определенного пользователя спонсора, тогда как адрес назначения (DA) (К) настроен глобально на ISE (в данном примере, `sms@test-cisco.com`). Все подробные данные о недавно созданном пользователе, такие как имя пользователя и пароль, в теле той электронной почты.
2. Электронная почта поступает в Постфиксный сервер, который настроен с maildrop как локальный курьер. Непосредственно перед доставкой пользователю СМ maildir каталог, maildrop ищет mailfilter в главном каталоге для пользователя. mailfilter сценарий анализирует электронную почту, и если все необходимые данные найдены, это использует `wget` для передачи HTTP-запроса GET к Kannel smsbox. То, что HTTP-запросы GET содержат текстовое сообщение наряду с именем пользователя и паролем и номер мобильного телефона пользователя. Kannel smsbox является фронтэндом Kannel, который используется для принятия всех запросов от пользователей для передачи СМ (для передачи его к Kannel bearerbox).
3. Kannel smsbox отправляет тот запрос к Kannel bearerbox, который несет ответственность передать СМ.
4. Могли бы быть множественные правила и Центры передачи коротких сообщений (SMSCs), настроенный на bearerbox. Данный пример использует внешний сервер SMPP. Конфигурация для локально подключенного мобильного телефона легка и представлена позже.

Каждый модуль этого решения (Постфикс, Kannel smsbox и Kannel bearerbox) может быть установлен на отдельном сервере. Для простоты в данном примере это настроено на том

же сервере.

Конфигурации

ISE

Выполните эти шаги для настройки ISE.

1. Настройте пользователя портала спонсора. В данном примере используется конфигурация ISE по умолчанию, и пользователь размещен в группу **SponsorAllAccount**:

Электронная почта для пользователя спонсора может быть настроена позже от Портала Спонсора.

2. Чтобы быть в состоянии передать уведомления SMS-сообщением, отредактируйте привилегии по умолчанию для группы **SponsorAllAccount**:

По умолчанию привилегия **СМ Передачи** отключена.

3. Настройте сервер SMTP и удостоверьтесь, что параметры настройки DNS корректны.

Все уведомления электронной почты передаются хосту **smtp.test-cisco.com**. ISE не пытается проверить записи MX DNS для настроенных доменов (этот сервер SMTP рассматривается как реле).

4. Настройте электронное письмо, которое послано как уведомление SMS-сообщением.

5. Настройте целевой адрес электронной почты, который является единственной установкой, которую не оставляют как по умолчанию. Все уведомления передаются через сервер SMTP, настроенный ранее с набором поля **To** как **sms@test-cisco.com**.

Примечание: Возможно настроить ISE для передачи предупреждений об аварийном состоянии через электронную почту. Это может также быть интегрировано с предложенным решением для передачи предупреждений как СМ к мобильным телефонам. Cisco советует использовать отдельную учетную запись на Постфиксном сервере для этого (например, **alert@test-cisco.com**).

Постфикс

Постфикс является сервером SMTP, который получает электронные письма от ISE. Конфигурация по умолчанию используется за исключением нескольких незначительных изменений. Выполните эти шаги для настройки его.

1. Настройте Постфикс, чтобы быть локальным назначением для домена **тестового cisco.com**. Важно также настроить локального курьера: maildrop. Вот необходимые изменения в main.cf:

```
myhostname = smtp.test-cisco.com
mydomain = test-cisco.com
mydestination = $myhostname, $mydomain, localhost
local_transport = maildrop
```

2. Следующий шаг должен активировать maildrop в master.cf. Измените корректную линию в master.cf:

```
maildrop unix -      n      n      -      -      pipe
 flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${user}
```

Поскольку это - простое развертывание без действительных доменов, **{пользователь}**, параметр используется вместо по умолчанию **{получатель}** параметр.

3. Настройте СМ локальной учетной записи, который используется для получения электронных писем:

```
neptun ~ # useradd sms
neptun ~ # passwd sms
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
neptun ~ # chown -R sms:sms /home/sms/
```

Прямо сейчас все электронные почты должны быть правильно отправлены пользователю СМ. maildir структура создана автоматически, когда она сначала получает электронное письмо.

Maildrop с Mailfilter

Непосредственно перед доставкой maildrop ищет **.mailfilter** в главном каталоге для пользователя. Если тот файл найден, сценарий выполняется. Привилегии для файла должны быть ограничены пользователем только:

```
neptun sms # touch /home/sms/.mailfilter
neptun sms # chmod go-rwx /home/sms/.mailfilter
```

Вот содержание файла:

```
# Mailfilter script for parsing ISE SMS messages
# Author: Michal Garcarz at cisco.com
# Date: 1 Dec 2013
```

```

#DEFAULT="$HOME/.maildir/"
DATE=`date`
SHELL="/bin/bash"

# Our log file
logfile "/home/sms/maildrop.log"

# Our verbosity in the log file
VERBOSE="5"

log "-----SMS MAILFILTER LOG-----"
log "Email received at: $DATE"

if (/^Subject:. *Guest.*Text.*Notification.*/)
{
    log "Email processed by script sending SMS via Kannel"

    USERNAME=""
    PASSWORD=""
    TO=""
    if (/^text:Username:(.*)/:b)
    {
        log "Username exists $MATCH1"
        USERNAME=$MATCH1
    }
    if (/^text:Password:(.*)/:b)
    {
        log "Password exists $MATCH1"
        PASSWORD=$MATCH1
    }
    if (/^to:(.*)/:b)
    {
        log "Mobile phone exists $MATCH1"
        TO=$MATCH1
    }

    if ($USERNAME ne "" && $PASSWORD ne "" && $TO ne "")
    {
        log "Sending via HTTP to kannel username=$USERNAME password=$PASSWORD to=$TO"
        DATA="ISE Guest portal Username: $USERNAME Password: $PASSWORD"

        #also curl can be used instead of wget
        xfilter "wget -O/dev/null \"http://192.168.112.100:13013/cgi-bin/sendsms?username=
tester&password=foobar&to=$TO&text=$DATA\" >> /tmp/maildrop-kannel.log 2>>
/tmp/maildrop-kannel.log"
    }

    #deliver to maildir (not used since xfilter returns !=0)
    to $DEFAULT/
}

```

Сценарий:

- Проверки, если предмет совпадает с тем, что настроено на ISE
- Читает имя пользователя и пароль в поля для почтового тела (шаблон по умолчанию от ISE используется),
- Если все поля существуют, вызывает внешнюю программу: **wget** для передачи GET HTTP к Kannel smsbox со всеми параметрами. Заметьте, что определенные учетные данные используются в URL (username=tester&password=foobar). Это учетные данные

настройки пользователя в Kannel с привилегиями передать СМ.
Здесь существует два файла журнала:

- **/home/sms/maildrop.log** - регистрирует от выполнения сценария
- **/tmp/maildrop-kannel.log** - регистрирует от выполнения wget

Kannel

И smsbox и bearerbox могут быть настроены от отдельного файла. Эта конфигурация использует внешний сервер SMPP для доставки. Легко найти множественное обслуживание в сети при поиске **smpp** фразы **поставщика услуг см**. Конфигурация проста, потому что нет никакой потребности получить и направить SMS-сообщения. Это решение только для передачи и использует одного поставщика SMPP.

Вот выборка от **/etc/kannel/kannel.conf**:

```
#bearerbox
group = core
admin-port = 13000
admin-password = bar
smsbox-port = 13001
log-level = 0
log-file = "/var/log/kannel/kannel.log"
access-log = "/var/log/kannel/access.log"

# SMSC SMPP
group = smsc
smsc = smpp
host = ****.com
port = 1775
smsc-username = 41jt7wi3
smsc-password = *****
system-type =
address-range =

# SMSBOX SETUP
group = smsbox
bearerbox-host = localhost
sendsms-port = 13013
sendsms-chars = "0123456789 +-"
global-sender = 12345
log-file = "/var/log/kannel/smsbox.log"
log-level = 0
access-log = "/var/log/kannel/access.log"
white-list =
black-list =
reply-couldnotfetch =
reply-couldnotrepresent =
reply-requestfailed =
reply-emptymessage =

# SEND-SMS USERS, this credentials has been used in wget script
group = sendsms-user
username = tester
password = foobar
user-deny-ip = "*. *.*.*"
user-allow-ip = "192.168.*.*"

# SMS SERVICE Default
```

```
# there should be default always (this is for receiving SMS messages - not used)
group = sms-service
keyword = default
text = "No service specified"
```

Возможно подключить мобильный телефон через USB и настроить GSM SMSC:

```
group = smsc
smc = at #type = GSM
smc-id = usb0-modem
my-number = 1234
modemtype = auto #types: wavcom, siemens, siemens-tc35, falcom,
nokiaphone, ericsson
device = /dev/ttyUSB0 #phone device seen on server
```

По большинству телефонов это также требуется, чтобы активировать функциональные возможности модема; например, в Версии 2.2 Android и позже, это включено в Параметрах настройки/Ограничивать и Портативном ограничивающем Хот-споте/USB.

Не забудьте выполнять и bearerbox и smsbox. Например:

```
neptun ~ # /etc/init.d/kannel-bearerbox start
* Starting kannel bearerbox ... [ ok ]
neptun ~ # /etc/init.d/kannel-smsbox start
* Starting kannel smsbox ... [ ok ]

neptun ~ # netstat -atcpn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:13013 0.0.0.0:* LISTEN 24170/smsbox
tcp 0 0 0.0.0.0:13000 0.0.0.0:* LISTEN 24151/bearerbox
tcp 0 0 0.0.0.0:13001 0.0.0.0:* LISTEN 24151/bearerbox
```

Bearerbox должен иметь по крайней мере один SMSC, настроенный для начала.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

ISE

Порт по умолчанию для Портала Спонсора используется (8443). Спонсор входит <https://ise.test-cisco.com:8443/sponsorportal/>.

Удостоверьтесь, что спонсору назначили адрес электронной почты в **Моих Параметрах настройки**:

Создайте гостевую учетную запись с уведомлением SMS-сообщением:

Вы получаете подтверждение, что была успешно создана гостевая учетная запись:

ISE должен послать электронное письмо настроенному серверу SMTP.

Постфикс

Сервер SMTP получает сообщение и использует maildrop для отправки его локальной учетной записи (**sms@test-cisco.com**). Вот выборка от `/var/log/messages`:

```
Nov 30 22:39:47 neptun postfix/smtpd[18460]: connect from unknown[192.168.112.1]
Nov 30 22:39:47 neptun postfix/smtpd[18460]: 2B36030B32: client=unknown
[192.168.112.1]
Nov 30 22:39:47 neptun postfix/cleanup[18463]: 2B36030B32: message-id=
<563762958.941385847586377.JavaMail.root@ise2>
Nov 30 22:39:47 neptun postfix/qmgr[32658]: 2B36030B32: from=<sponsor@test-cisco.com>,
size=689, nrcpt=1 (queue active)
Nov 30 22:39:47 neptun postfix/pipe[18464]: 2B36030B32: to=<sms@test-cisco.com>,
relay=maildrop, delay=0.18, delays=0.14/0/0/0.04, dsn=2.0.0, status=sent (delivered
via maildrop service)
```

Maildrop

Перед отправкой электронного письма CM maildir каталог выполняет `/home/sms/.mailfilter`, который выполняет определенное действие.

Вот выборка от `/home/sms/maildrop.log`:

```
-----SMS MAILFILTER LOG-----
Email received at: Sat Nov 30 22:39:47 CET 2013
Email processed by script sending SMS via Kannel
Username exists jsmith02
Password exists t6ub79_6r
Mobile phone exists 4850xxxxxxx
Sending via HTTP to kannel username= jsmith02 password= t6ub79_6r to=4850xxxxxxx
```

Mailfilter

mailfilter сценарий считывает все данные и выполняет **xfilter**, который вызывает **wget** для передачи всех параметров к Kannel.

Вот выборка от `/tmp/maildrop-kannel.log`:

```
--2013-11-30 22:39:47-- http://192.168.112.100:13013/cgi-bin/sendsms?username=
tester&password=foobar&to=4850xxxxxxx&text=ISE%20Guest%20portal%20Username:
%20%20jsmith02%20Password:%20%20t6ub79_6r
Connecting to 192.168.112.100:13013... connected.
HTTP request sent, awaiting response... 202 Accepted
Length: 24 [text/html]
Saving to: `/dev/null'
```

OK

100% 1.14M=0s

```
2013-11-30 22:39:47 (1.14 MB/s) - `/dev/null' saved [24/24]
```

HTTP-запрос GET принят.

Kannel

Kannel smsbox сообщает, что получил запрос HTTP от **wget**, и он отправил тот запрос к beargerbox для отправки CM.

Вот выборка от/var/log/kannel/smsbox.log:

```
2013-11-30 22:39:47 [18184] [5] INFO: smsbox: Got HTTP request </cgi-bin/sendsms>
from <192.168.112.100>
2013-11-30 22:39:47 [18184] [5] INFO: sendsms used by <tester>
2013-11-30 22:39:47 [18184] [5] INFO: sendsms sender:<tester:12345>
(192.168.112.100) to:<4850xxxxxx> msg:<ISE Guest portal Username:
jsmith02 Password: t6ub79_6r>
2013-11-30 22:39:47 [18184] [5] DEBUG: Stored UUID fd508632-9408-49e1-9eda-
3ce8d4b939d4
2013-11-30 22:39:47 [18184] [5] DEBUG: message length 57, sending 1 messages
2013-11-30 22:39:47 [18184] [5] DEBUG: Status: 202 Answer: <Sent.>
2013-11-30 22:39:47 [18184] [5] DEBUG: Delayed reply - wait for bearerbox
2013-11-30 22:39:47 [18184] [0] DEBUG: Got ACK (0) of fd508632-9408-49e1-9eda-
3ce8d4b939d4
```

Kannel bearerbox соединяется с удаленным сервером SMPP и передает сообщение успешно.

Вот выборка от/var/log/kannel/kannel.log:

```
2013-11-30 22:39:47 [18165] [8] DEBUG: boxc_receiver: sms received
2013-11-30 22:39:47 [18165] [8] DEBUG: send_msg: sending msg to box: <127.0.0.1>
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP[SMPP:*****.com:1775/0:4ljt7wi3:]:
throughput (0.00,0.00)
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP[SMPP:*****.com:1775/0:4ljt7wi3:]:
Sending PDU:
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP PDU 0x2056bf0 dump:
2013-11-30 22:39:47 [18165] [6] DEBUG: type_name: submit_sm
2013-11-30 22:39:47 [18165] [6] DEBUG: command_id: 4 = 0x00000004
2013-11-30 22:39:47 [18165] [6] DEBUG: command_status: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: sequence_number: 5 = 0x00000005
2013-11-30 22:39:47 [18165] [6] DEBUG: service_type: NULL
2013-11-30 22:39:47 [18165] [6] DEBUG: source_addr_ton: 2 = 0x00000002
2013-11-30 22:39:47 [18165] [6] DEBUG: source_addr_npi: 1 = 0x00000001
2013-11-30 22:39:47 [18165] [6] DEBUG: source_addr: "12345"
2013-11-30 22:39:47 [18165] [6] DEBUG: dest_addr_ton: 2 = 0x00000002
2013-11-30 22:39:47 [18165] [6] DEBUG: dest_addr_npi: 1 = 0x00000001
2013-11-30 22:39:47 [18165] [6] DEBUG: destination_addr: "4850xxxxxx"
2013-11-30 22:39:47 [18165] [6] DEBUG: esm_class: 3 = 0x00000003
2013-11-30 22:39:47 [18165] [6] DEBUG: protocol_id: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: priority_flag: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: schedule_delivery_time: NULL
2013-11-30 22:39:47 [18165] [6] DEBUG: validity_period: NULL
2013-11-30 22:39:47 [18165] [6] DEBUG: registered_delivery: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: replace_if_present_flag: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: data_coding: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: sm_default_msg_id: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: sm_length: 57 = 0x00000039
2013-11-30 22:39:47 [18165] [6] DEBUG: short_message:
2013-11-30 22:39:47 [18165] [6] DEBUG: Octet string at 0x205ec70:
2013-11-30 22:39:47 [18165] [6] DEBUG: len: 57
2013-11-30 22:39:47 [18165] [6] DEBUG: size: 58
2013-11-30 22:39:47 [18165] [6] DEBUG: immutable: 0
2013-11-30 22:39:47 [18165] [6] DEBUG: data&colon; 49 53 45 20 47 75 65 73
74 20 70 6f 72 74 61 6c ISE Guest portal
2013-11-30 22:39:47 [18165] [6] DEBUG: data&colon; 20 55 73 65 72 6e 61 6d
65 3a 20 20 6a 73 6d 69 Username: jsmi
2013-11-30 22:39:47 [18165] [6] DEBUG: data&colon; 74 68 30 32 20 50 61 73
73 77 6f 72 64 3a 20 20 th02 Password:
2013-11-30 22:39:47 [18165] [6] DEBUG: data&colon; 74 36 75 62 37 39 11 36
72 t6ub79.6r
2013-11-30 22:39:47 [18165] [6] DEBUG: Octet string dump ends.
```

```
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP PDU dump ends.
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP[SMPP:*****.com:1775/0:4ljt7wi3]:
throughput (1.00,0.00)
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP[SMPP:*****.com:1775/0:4ljt7wi3]:
throughput (1.00,0.00)
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP[SMPP:*****.com:1775/0:4ljt7wi3]:
Got PDU:
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP PDU 0x2056bf0 dump:
2013-11-30 22:39:47 [18165] [6] DEBUG: type_name: submit_sm_resp
2013-11-30 22:39:47 [18165] [6] DEBUG: command_id: 2147483652 = 0x80000004
2013-11-30 22:39:47 [18165] [6] DEBUG: command_status: 0 = 0x00000000
2013-11-30 22:39:47 [18165] [6] DEBUG: sequence_number: 5 = 0x00000005
2013-11-30 22:39:47 [18165] [6] DEBUG: message_id: "4128473611307259"
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP PDU dump ends.
2013-11-30 22:39:47 [18165] [6] DEBUG: SMPP[SMPP:*****.com:1775/0:4ljt7wi3]:
throughput (1.00,0.00)
```

Заметьте, что адрес источника установлен как **12345**. Эта установка не имеет значения. Внешние перезаписи сервера SMPP то значение. Возможно купить дополнительный сервис, чтобы быть представленным по-другому.

Гостевой телефон

Гость получает CM:

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

ISE

Вы могли бы встретиться с этой ошибкой при создании гостевой учетной записи: Неспособный передать текстовое сообщение следующим гостям: xxxx. Необходимо добавить адрес электронной почты к странице настроек. Если вы получаете то сообщение об ошибках, проверяете адрес электронной почты спонсора.

Дополнительные сведения

- [Платформа Cisco Identity Services Engine - пользовательское руководство 1.2](#)
- [Документация Kannel](#)
- [Постфиксная документация](#)
- [Cisco Systems – техническая поддержка и документация](#)