Шифрование хоста коммутатора MACsec с AnyConnect Cisco и примером конфигурации ISE

ID документа: 117277

Обновлено : Янв 31, 2014

Внесено Михалом Гаркарзом и Романом Мачуликом, специалистами службы технической поддержки Cisco.

Родственные продукты

- Безопасность
- 802.1x
- Cisco Identity Services Engine

Содержание

Соответствующие дискуссии сообщества технической поддержки Cisco

Введение

Этот документ содержит пример настройки шифрования системы безопасности контроля доступа к среде (MACsec) между соискателем 802.1x (Cisco AnyConnect Mobile Security) и средством аутентификации (коммутатором). Механизмы сервисов идентификации Cisco (ISE) используются в качестве средства аутентификации и сервера политик.

MACsec стандартизируется в 802.1AE и поддерживается на коммутаторах Cisco 3750X, 3560X и 4500 SUP7E. 802.1AE определяет шифрование каналов связи по проводным сетям, которые используют внеполосные ключи. Эти ключи шифрования согласовываются с протоколом согласования ключей MACsec (MKA), который используется после успешной аутентификации 802.1x. Протокол MKA стандартизирован в IEEE 802.1X 2010.

Пакет шифруется только на канале связи между ПК и коммутатором (одноточечное шифрование). Пакет, принимаемый коммутатором, дешифруется и передается по дешифрованным восходящим каналам связи. Для шифрования передаваемых данных между коммутаторами рекомендуется межкоммутаторное шифрование. Для этого шифрования используется протокол контекста безопасности (SAP) для согласования и регенерации ключей. SAP является предварительно стандартным протоколом согласования ключей, разработанным компанией Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации 802.1x
- Базовые знания о конфигурации интерфейса командой строки коммутаторов Catalyst
- Навыки работы с конфигурацией ISE

Используемые компоненты

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

- Операционные системы Microsoft Windows 7 и Microsoft Windows XP
- Программное обеспечение Cisco 3750X версии 15.0 или более поздней версии
- Программное обеспечение ISE Cisco версии 1.1.4 или более поздней версии
- Cisco AnyConnect Mobile Security с Network Access Manager (NAM) версии 3.1 или более поздней версии

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.

Настройка

Диаграмма сети и поток трафика

Шаг 1. Соискатель (NAM AnyConnect) открывает сеанс 802.1x. Коммутатор является средством аутентификации, а ISE является сервером аутентификации. Расширяемый протокол аутентификации по LAN (EAPOL) используется в качестве механизма передачи данных для EAP между соискателем и коммутатором. RADIUS используется в качестве протокола передачи данных для EAP между коммутатором и ISE. Обход MAC-аутентификации (MAB) не может использоваться, так как ключи EAPOL должны возвращаться из ISE и использоваться для сеанса согласования ключей MACsec (MKA).

Шаг 2. После того как сеанс 802.1x завершается, коммутатор инициирует сеанс MKA с EAPOL в качестве протокола передачи данных. Если соискатель настроен правильно, ключи для симметричного 128-разрядного (режим Галуа/счетчика) шифрования соответствуют требованиям.

Шаг 3. Все последующие пакеты между соискателем и коммутатором шифруются (инкапсуляция 802.1AE).

Конфигурации

ISE

Конфигурация ISE использует типичный сценарий 802.1x с исключением для профиля авторизации, который может включать в себя политики шифрования.

Выберите Administration> Network Resources> Network Devices для добавления коммутатора как сетевого устройства. Введите общий ключ RADIUS (общий секретный ключ).

Может использоваться правило аутентификации по умолчанию (для пользователей, определенных локально на ISE).

Выберите Administration>> Users Identity Management для определения пользователя "cisco" на локальном уровне.

Профиль авторизации может включать в себя политики шифрования. **Как показано в данном примере, выберите Policy> Results> Authorization Profiles, чтобы увидеть, что ISE возвращает на коммутатор данные о том, что шифрование канала связи является обязательным.** Кроме того, было указано число VLAN (10).

Выберите Policy> Authorization для использования профиля авторизации в правиле авторизации. Данный пример возвращает настроенный профиль для пользователя "cisco". При успешности 802.1x ISE возвращаетRadius - Accept на коммутатор с Cisco AVPair linksec-policy=must-secure. Этот атрибут вынуждает коммутатор инициировать сеанс MKA. Если

этот сеанс заканчивается неудачей, авторизация 802.1x на коммутаторе также заканчивается неудачей.

Коммутатор

Типичные параметры порта 802.1x включают в себя (показана верхняя часть):

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius

aaa group server radius ISE
 server name ISE

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order dot1x
 authentication port-control auto
 dot1x pae authenticator

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 timeout 5
 retransmit 2
key cisco
```

Локальная политика MKA создана и применена к интерфейсу. Кроме того, в интерфейсе включено шифрование MACsec.

```
mka policy mka-policy
 replay-protection window-size 5000

interface GigabitEthernet1/0/2
 macsec
 mka policy mka-policy
```

Локальная политика MKA позволяет настраивать детализированные параметры, которые не могут быть получены из ISE. Локальная политика MKA является дополнительной.

AnyConnect NAM

Профиль для соискателя 802.1x может быть настроен вручную или получен через Cisco ASA. Следующие действия составляют настройку вручную.

Для управления профилями NAM:

Добавьте новый профиль 802.1x с MACsec. Для 802.1x используется защищенный расширяемый протокол аутентификации (PEAP) (для настроенного пользователя "cisco" на ISE):

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Приложение AnyConnect NAM, настроенное на PEAP EAP, требует корректных учетных данных.

Сеанс на коммутаторе должен проходить аутентификацию и авторизацию. Состоянием системы безопасности должно быть "Secured":

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface: GigabitEthernet1/0/2
         MAC Address: 0050.5699.36ce
          IP Address: 192.168.1.201
           User-Name: cisco
              Status: Authz Success
              Domain: DATA
     Security Policy: Must Secure
     Security Status: Secured
      Oper host mode: single-host
    Oper control dir: both
       Authorized By: Authentication Server
         Vlan Policy: 10
     Session timeout: N/A
        Idle timeout: N/A
   Common Session ID: C0A8000100000D56FD55B3BF
     Acct Session ID: 0x00011CB4
              Handle: 0x97000D57

Runnable methods list:
      Method  State
      dot1x   Authc Success
```

Статистические данные MACsec на коммутаторе содержат подробные параметры настройки локальной политики, идентификаторы безопасных каналов (SCI) для принимаемого/отправляемого трафика, а также статистические данные порта и ошибки.

```
bsns-3750-5#show macsec interface g1/0/2
 MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
 Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0  Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
```

```
 SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0  Previous AN: -
  SC Statistics
   Notvalid pkts 0     Invalid pkts 0
   Valid pkts 76        Late pkts 0
   Uncheck pkts 0      Delay pkts 0
 Port Statistics
  Ingress untag pkts 0       Ingress notag pkts 2441
  Ingress badtag pkts 0       Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0        Unused pkts 0
  Notusing pkts 0             Decrypt bytes 176153
  Ingress miss pkts 2437
```

В AnyConnect статистические данные указывают на использование шифрования и пакетную статистику.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Отладка для рабочего сценария

Включите отладку на коммутаторе (некоторые выходные данные были пропущены для поонятности).

```
bsns-3750-5#show macsec interface g1/0/2
 MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
 Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0  Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
 SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0  Previous AN: -
  SC Statistics
   Notvalid pkts 0     Invalid pkts 0
   Valid pkts 76        Late pkts 0
   Uncheck pkts 0      Delay pkts 0
 Port Statistics
  Ingress untag pkts 0       Ingress notag pkts 2441
  Ingress badtag pkts 0       Ingress unknownSCI pkts 0
```

```
  Ingress noSCI pkts 0        Unused pkts 0
  Notusing pkts 0             Decrypt bytes 176153
  Ingress miss pkts 2437
```

После открытия сеанса 802.1x выполняется обмен множественными пакетами EAP по EAPOL. Последний успешный ответ от ISE (успешный результат EAP), перенесенный в Radius-Acccept, также включает в себя несколько атрибутов RADIUS.

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS: EAP-Key-Name       [102] 67 *
RADIUS: Vendor, Cisco      [26] 34
RADIUS:  Cisco AVpair      [1]  28 "linksec-policy=must-secure"
RADIUS: Vendor, Microsoft  [26] 58
RADIUS:  MS-MPPE-Send-Key  [16] 52 *
RADIUS: Vendor, Microsoft  [26] 58
RADIUS:  MS-MPPE-Recv-Key  [17] 52 *
```

Имя ключа EAP используется для сеанса MKA. Политика безопасности канала связи вынуждает коммутатор использовать MACsec (при неудачной авторизации, если операция не завершена). Эти атрибуты могут быть также проверены по захваченным пакетам.

Аутентификация успешна.

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Коммутатор применяет атрибуты (они включают в себя дополнительное число VLAN), которое также было передано).

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

Затем коммутатор открывает сеанс MKA, когда отправляет и принимает пакеты EAPOL.

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

После 4-х обменов пакетами создаются идентификаторы безопасности вместе с контекстом безопасности приема (RX).

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```

Сеанс завершается, и добавляется контекст безопасности передача (TX).

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
HULC-MACsec: Process install TxSA request66B4EEC for interface GigabitEthernet1/0/
```

Политика "must-secure" соответствует требованиям, и авторизация успешна.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
```

```
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Каждые 2 секунды выполняется обмен пакетами приветствия по MKA для проверки наличия участников в сети.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Отладка для сценария отказа

Если соискатель не настроен на MKA и ISE запрашивает шифрование после успешной аутентификации 802.1x:

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

Коммутатор пытается инициировать сеанс MKA, когда отправляет 5 пакетов EAPOL.

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

В конце концов время ожидания истекает и авторизация заканчивается неудачей.

```
 %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) MKA Session was stopped by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

Сеанс 802.1x сообщает как об успешной аутентификации, так и неудачной попытке авторизации.

```
bsns-3750-5#show authentication sessions int g1/0/2
           Interface: GigabitEthernet1/0/2
         MAC Address: 0050.5699.36ce
          IP Address: 192.168.1.201
           User-Name: cisco
              Status: Authz Failed
              Domain: DATA
     Security Policy: Must Secure
     Security Status: Unsecure
      Oper host mode: single-host
    Oper control dir: both
     Session timeout: N/A
        Idle timeout: N/A
   Common Session ID: C0A8000100000D55FD4D7529
     Acct Session ID: 0x00011CA0
              Handle: 0xA4000D56
```

```
Runnable methods list:
      Method  State
      dot1x   Authc Success
```

Трафик данных будет заблокирован.

Захваты пакетов

Когда трафик перехватывается на узле соискателя, отправляются и принимаются 4 эхо-запроса/ответа по протоколу ICMP, и:

- 4 зашифрованных эхо-запроса ICMP отправляются на коммутатор (88e5 зарезервирован для 802.1AE)
- Принимаются 4 дешифрованных эхо-ответа ICMP

Это происходит из-за того, что AnyConnect использует Windows API (до libpcap при отправке пакетов и до libpcap при приеме пакетов):

> **Примечание:** Возможность анализировать трафик MKA или 802.1AE на коммутаторе с помощью такого функционала, как анализатор коммутируемых портов (SPAN) или встроенная функция захвата пакетов (EPC), не поддерживается.

MACsec и режимы 802.1x

Не все режимы 802.1x поддерживаются для MACsec.

Руководство по Cisco TrustSec 3.0: Введение в MACsec и NDAC сообщает следую информацию:

- **Режим одиночного хоста: MACsec полностью поддерживается в режиме одиночного хоста.** В этом режиме только одиночный MAC или IP-адрес может пройти аутентификацию и быть защищенным с помощью MACsec. Если на порту обнаруживается другой MAC-адрес после того, как оконечная точка прошла аутентификацию, на порту фиксируется нарушение безопасности.
- **Режим мультидоменной аутентификации (MDA):** В этом режиме одна оконечная точка может находиться в домене данных, а другая оконечная точка может находиться в речевом домене. **MACsec полностью поддерживается в режиме MDA.** Если обе оконечных точки поддерживают MACsec, то каждый будет защищен своим собственным независимым сеансом MACsec. Если только одна оконечная точка поддерживает MACsec, эта оконечная точка может быть защищена, в то время как другая оконечная точка передает трафик без шифрования.
- **Режим мультиаутентификации:** В этом режиме виртуально неограниченное количество оконечных точек может пройти аутентификацию на порту одного коммутатора. **MACsec не поддерживается в этом режиме.**
- **Режим с множеством хостов: В то время как использование MACsec в этом режиме технически возможно, но не рекомендуется.** В режиме с множеством хостов первая оконечная точка на порту проходит аутентификацию, а затем любые дополнительные оконечные точки будут разрешены в сети с проходом через первую авторизацию.

MACsec будет работать с первым подключенным узлом, но не с какой-либо другой оконечной точкой? трафик на самом деле пройдет проверку, так как не является зашифрованным.

Дополнительные сведения

- Руководство по конфигурации Cisco TrustSec для 3750
- Руководство по конфигурации Cisco TrustSec для ASA 9.1
- Основанные на идентификации сетевые сервисы: Безопасность MAC
- Облако TrustSec с 802.1x MACsec на Catalyst — пример конфигурации коммутатора серии 3750X
- ASA и коммутатор Catalyst серии 3750X — пример конфигурации TrustSec и руководство по устранению неполадок
- Развертывание Cisco TrustSec и RoadMap
- Cisco Systems – техническая поддержка и документация

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

Обновлено : Янв 31, 2014
ID документа: 117277