Техническое примечание на часто задаваемых вопросах для удаленного доступа на Cisco ESA/WSA/SMA

Содержание

Введение

Этот документ предоставляет ответы на часто задаваемые вопросы об использовании удаленного доступа технической поддержкой Cisco на устройствах Безопасности содержания Cisco. Это включает Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA) и Устройство менеджмента Cisco Security (SMA).

Предварительные условия

Используемые компоненты

Сведения в этом документе основываются на устройствах Безопасности содержания Cisco, выполняющих любую версию AsyncOS.

Что такое удаленный доступ?

Удаленный доступ является соединением Secure Shell (SSH), которое включено от устройства Безопасности содержания Cisco до безопасного хоста в Cisco. Только Помощь

Клиента Cisco может обратиться к устройству, как только включен удаленный сеанс. Удаленный доступ позволяет Поддержке Клиента Cisco анализировать устройство. Доступы к поддержке устройство через туннель SSH, который эта процедура создает между устройством и upgrades.ironport.com сервером.

Как работает удаленный доступ

Когда соединение удаленного доступа инициирует, устройство открывает безопасное, случайное, высокий исходный порт через SSH - подключение на устройстве к настроенному/выбранному порту из следующих серверов Безопасности содержания Cisco:

IP-адрес	Host name	Использовать
63.251.108.107	upgrades.ironport.com	Все устройства безопасности содержания
184.94.240.126	c . tunnels.ironport.com	используемый для устройств/ESA Серии C
184.94.240.126	x. tunnels.ironport.com	используемый для устройств/ESA Серии X
184.94.240.126	m.tunnels.ironport.com	используемый для устройств/SMA Серии M
184.94.240.126	s.tunnels.ironport.com	используемый для appliances/WSA Серии S

Следует отметить, что межсетевой экран клиента, возможно, должен быть настроен для разрешения исходящих соединений одному из вышеупомянутых перечисленных серверов. Если вашему межсетевому экрану включат контроль протокола SMTP, то туннель не установит. Порты, что Cisco примет соединения от устройства для удаленного доступа:

- 22
- 25 (По умолчанию)
- 53
- 80
- 443
- 4766

Соединение удаленного доступа сделано к имени хоста а не к жестко закодированному IP-адресу. Это действительно требует, чтобы Сервер доменных имен (DNS) был настроен на устройстве, для установления исходящего соединения.

На сети заказчика некоторые осведомленные о протоколе сетевые устройства могут заблокировать это соединение к несоответствию протокола/порта. Некоторый Транспортный протокол простой почты (SMTP) - осведомленные устройства могут также прервать соединение. В случаях, где существуют осведомленные о протоколе устройства или исходящие соединения, которые заблокированы, может требоваться использование порта кроме по умолчанию (25). Доступ к удаленному концу туннеля ограничен только Поддержкой Клиента Cisco. Убедитесь, что вы рассматриваете свой межсетевой экран/сеть для исходящих соединений при попытке установить или устранить неполадки соединений удаленного доступа для устройства.

> **Примечание:** Когда Специалист службы поддержки Клиента Cisco связан с устройством через удаленный доступ, системное приглашение на устройстве показывает *(СЕРВИС)*.

Как включить удаленный доступ

Примечание: Обязательно рассмотрите Руководство пользователя вашего устройства и версию AsyncOS для инструкций по "Включению Удаленного доступа для Персонала технической поддержки Cisco".

Примечание: Прикрепления, передаваемые по электронной почте attach@cisco.com, могут не быть безопасными в пути. Менеджер Случая поддержки является предпочтительной безопасной опцией Cisco для загружения информации к случаю. Узнать больше о безопасности и ограничениях по размеру других опций выгрузки файла: Выгрузки файла Клиента к Центру технической поддержки Cisco

Определите порт, который может быть достигнут из Интернета. По умолчанию является портом 25, который будет работать в большинстве сред, потому что система также требует общего доступа по тому порту для передачи сообщений электронной почты. Соединения по этому порту позволены в большинстве конфигураций межсетевого экрана.

CLI

Для установления соединения удаленного доступа через CLI, как пользователь Admin, выполните эти шаги:

1. Введите **techsupport** команду
2. Выберите **TUNNEL**
3. Примите решение Генерировать или *Ввести* случайную инициирующую строку
4. Задайте номер порта для соединения
5. Ответьте **"Y"** для включения сервисного доступа

Удаленный доступ wil быть включенным в это время. Устройство теперь работает для установления безопасного соединения с безопасным хостом оплота в Cisco. Предоставьте и серийный номер устройства и инициирующую строку, которая генерируется Инженеру TAC, поддерживающему ваш случай.

GUI

Для установления соединения удаленного доступа через GUI, как пользователь Admin, выполните эти шаги:

1. Перейдите, чтобы **Помочь и Поддержать> Удаленный доступ** (для ESA, SMA), **Поддержка и Справка> Удаленный доступ** (для WSA)
2. Нажмите **Enable**
3. Выберите метод для инициирующей строки
4. Гарантируйте, что вы проверяете *Инициировать соединение через* флажок *безопасного туннеля* и задаете номер порта для соединения
5. **Нажмите кнопку Submit (Отправить)**

Удаленный доступ wil быть включенным в это время. Устройство теперь работает для установления безопасного соединения с безопасным хостом оплота в Cisco. Предоставьте и серийный номер устройства и инициирующую строку, которая генерируется Инженеру TAC, поддерживающему ваш случай.

Как отключить удаленный доступ

CLI

1. Введите **techsupport** команду
2. Выберите **DISABLE**
3. Ответьте **"Y"**, когда предложено, "Вы уверены, что хотите отключить сервисный доступ?"

GUI

1. Перейдите, чтобы **Помочь и Поддержать> Удаленный доступ** (для ESA, SMA), **Поддержка и Справка> Удаленный доступ** (для WSA).
2. Нажмите **Disable**
3. Выходные данные GUI покажут "Успех — Удаленный доступ был отключен"

Как протестировать подключение удаленного доступа

Используйте данный пример для выполнения начального теста для подключения от устройства до Cisco:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

Подключение может быть протестировано на любой из упомянутых выше портов: 22, 25, 53, 80, 443, или 4766. Если подключение отказывает, вы, возможно, должны выполнить захват пакета для наблюдения, где связь прерывается от устройства/сети.

Почему удаленный доступ не работает на SMA?

Если SMA размещен в локальную сеть без прямого доступа к Интернету, удаленный доступ может не включить на SMA. Для этого экземпляра удаленный доступ может быть включен на ESA или WSA, и доступ SSH может быть включен на SMA. Это позволяет Поддержке Cisco сначала соединяться через удаленный доступ с ESA/WSA, и затем от ESA/WSA до SMA через SSH. Это потребует подключения между ESA/WSA и SMA на порту 22.

> **Примечание:** Обязательно рассмотрите Руководство пользователя вашего устройства и версию AsyncOS для инструкций по "Включению Удаленного доступа к Устройствам Без прямого Интернет-соединения".

CLI

Для установления соединения удаленного доступа через CLI, как пользователь Admin, выполните эти шаги:

1. Введите **techsupport** команду

2. Выберите **SSHACCESS**
3. Примите решение Генерировать или *Ввести* случайную инициирующую строку
4. Ответьте **"Y"** для включения сервисного доступа

Удаленный доступ wil быть включенным в это время. Выходные данные CLI покажут инициирующую строку. Предоставьте это Специалисту службы поддержки Клиента Cisco. Выходные данные CLI также покажут статус соединения и подробные данные удаленного доступа, включая серийный номер устройства. Предоставьте этот серийный номер Инженеру службы поддержки Клиента.

GUI

Для установления соединения удаленного доступа через GUI, как пользователь Admin, выполните эти шаги:

1. Перейдите, чтобы **Помочь и Поддержать> Удаленный доступ** (для ESA, SMA), **Поддержка и Справка> Удаленный доступ** (для WSA)
2. Нажмите **Enable**
3. Выберите метод для инициирующей строки
4. Не проверяйте *Инициировать соединение через* флажок *безопасного туннеля*
5. **Нажмите кнопку Submit (Отправить)**

Удаленный доступ wil быть включенным в это время. Выходные данные GUI покажут вам сообщение об успешном завершении и инициирующую строку устройства. Предоставьте это Специалисту службы поддержки Клиента Cisco. Выходные данные GUI также покажут статус соединения и подробные данные удаленного доступа, включая серийный номер устройства. Предоставьте этот серийный номер Инженеру службы поддержки Клиента.

Как отключить удаленный доступ, когда включено для SSHACCESS

Отключение удаленного доступа для SSHACCESS является теми же шагами как предусмотрено выше.

Устранение неисправностей

Если устройство не будет в состоянии к включенному удаленному доступу и подключению к upgrades.ironport.com через один из перечисленных портов, то необходимо будет выполнить захват пакета непосредственно от устройства для рассмотрения то, что заставляет исходящее соединение отказывать.

> **Примечание:** Обязательно рассмотрите Руководство пользователя вашего устройства и версию AsyncOS для инструкций по "Выполнению Захвата пакета".

Специалист службы поддержки Клиента Cisco может запросить предоставить .pcap файл, чтобы рассмотреть и помочь с устранением проблем.

Дополнительные сведения

- Часто задаваемые вопросы ESA: Что уровни административного доступа доступны на

ESA?

- Поддержка продуктов устройства безопасности электронной почты Cisco
- Веб-поддержка продукта безопасности Cisco
- Поддержка продуктов устройства менеджмента безопасности содержания Cisco
- Cisco Systems – техническая поддержка и документация