Настройте ESA для организации обновлений

Содержание

Введение

Этот документ описывает процесс для Бета клиентов и предварительно настроенные устройства , используемые для тестирования, которое должно быть настроено, чтобы использовать и вытянуть обновления от серверов обновления организации для Cisco Email Security Appliance (ESA) и устройство управления безопасностью (SMA). Следует иметь в виду, серверы организации не должны использоваться типичными производственными клиентами для производственного ESA или SMA.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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

Примечание: Клиенты должны быть только использованием URL сервера обновления организации, если они получили доступ к предварительной инициализации через Cisco для Бета использования только. Если вам не будут просить действующую лицензию Бета использование, то ваше устройство не получит обновления от серверов обновления организации. Эти инструкции должны только использоваться для Бета клиентов или администраторами, которые участвуют в Бета-тестах.

Для получения обновлений организации:

GUI

1. Выберите **Обновления> Services Security Services> Редактируют, Обновляют Настройки...**
2. Подтвердите , что все сервисы настроены для использования Серверов Обновления Cisco IronPort.

CLI

1. Введите команду **updateconfig**.
2. Введите скрытую подкоманду **dynamichost**.
3. Введите одну из этих команд: Для аппаратного ESA/SMA: **stage-update-manifests.ironport.com:443**Для действительного ESA/SMA: **stage-stg-updates.ironport.com:443**
4. Нажмите Enter , пока вы не будете возвращены к основному полю приглашения.
5. Введите **Передачу** для сохранения всех изменений.

Проверка

Проверка может быть замечена в *updater_logs* со связью, успешно выполняющейся для соответствующего URL этапа. От CLI на устройстве введите **этап grep updater_logs**:

```
9.9.5-033.local (SERVICE)>  grep stage updater_logs

Wed Mar 16 18:16:17 2016 Info: internal_cert beginning download of remote file "http://stage-
updates.ironport.com/internal_cert/1.0.0/internal_ca.pem/default/100101"
Wed Mar 16 18:16:17 2016 Info: content_scanner beginning download of remote file "http://stage-
updates.ironport.com/content_scanner/1.1/content_scanner/default/1132001"
Wed Mar 16 18:16:17 2016 Info: enrollment_client beginning download of remote file
"http://stage-updates.ironport.com/enrollment_client/1.0/enrollment_client/default/102057"
Wed Mar 16 18:16:18 2016 Info: support_request beginning download of remote file "http://stage-
updates.ironport.com/support_request/1.0/support_request/default/100002"
Wed Mar 16 18:16:18 2016 Info: timezones beginning download of remote file "http://stage-
updates.ironport.com/timezones/2.0/zoneinfo/default/2015100"
Wed Mar 16 18:26:19 2016 Info: repeng beginning download of remote file "http://stage-
updates.ironport.com/repeng/1.2/repeng_tools/default/1392120079"
```

Если существуют какие-либо неожиданные ошибки связи, войдите**, роют <URL этапа>** для проверки Сервера доменных имен (DNS).

```
9.9.5-033.local (SERVICE)>  dig stage-updates.ironport.com


; <<>> DiG 9.8.4-P2 <<>> stage-updates.ironport.com A
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52577
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;stage-updates.ironport.com. IN A

;; ANSWER SECTION:
stage-updates.ironport.com. 275 IN A 208.90.58.21

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 22 14:31:10 2016
;; MSG SIZE rcvd: 60
```

Чтобы проверить, что устройство в состоянии к telnet по порту 80, введите **telnet <URL этапа> 80** команд.

```
9.9.5-033.local (SERVICE)>  telnet stage-updates.ironport.com 80

Trying 208.90.58.21...
Connected to origin-stage-updates.ironport.com.
Escape character is '^]'.
```

Revert

Для возвращения назад к стандартным производственным серверам обновления, выполните эти шаги:

1. Введите команду **updateconfig**.
2. Введите скрытую подкоманду **dynamichost**.
3. Введите одну из этих команд: Для аппаратного ESA/SMA: **обновление-manifests.ironport.com:443**Для действительного ESA/SMA: **обновление-manifests.sco. cisco . com:443**
4. Нажмите Enter , пока вы не будете возвращены к основному полю приглашения.
5. Выполните **Передачу** для сохранения всех изменений.

Примечание: Совместимости оборудования (C1x0, C3x0, C6x0 и X10x0) должны ONLY использовать динамические URL хоста *stage-update-manifests.ironport.com:443* или *обновления-manifests.ironport.com:443*. Если существует конфигурация кластера и с ESA и с VESA, **updateconfig** должен быть настроен на уровне машины и подтвердить , что **dynamichost** тогда установлен соответственно.

Фильтрация URL-адресов

Если Фильтрация URL-адресов настроена и в использовании на устройстве, когда-то устройство было перенаправлено для использования URL этапа для обновлений, устройство должно будет также быть настроено для использования сервера организации для Фильтрации URL-адресов:

1. Обратитесь к устройству через CLI
2. Введите команду **websecurityadvancedconfig**.
   Шаг через конфигурацию и изменение значение для *имени хоста сервиса безопасности опции Enter the Web* к: **v2.beta.sds. cisco . com**

3. Измените значение для опции Enter пороговое значение для ожидающих запросов к:**5.** (По умолчанию равняется 50.)
4. Примите настройки по умолчанию для всех других опций.
5. Нажмите Enter , пока вы не будете возвращены к основному полю приглашения.
6. Введите **Передачу** для сохранения всех изменений.

Веб-отслеживание взаимодействия

Если веб-Отслеживание Взаимодействия настроено и в использовании на устройстве, когда-то устройство было перенаправлено для использования URL этапа для обновлений, устройство должно будет также быть настроено для использования сервера Агрегатора организации:

1. Обратитесь к устройству через CLI
2. Введите команду **aggregatorconfig**.
3. Используйте Команду редактирования и введите это значение: **stage.aggregator.sco. cisco . com**
4. Нажмите Enter , пока вы не будете возвращены к основному полю приглашения.
5. Выполните **Передачу** для сохранения всех изменений.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- VESA Не В состоянии Загрузить и Применить Обновления для Защиты от спама или Антивируса
- Cisco Systems – техническая поддержка и документация