Обеспечение безопасности сети при предоставлении доступа третьим сторонам

Содержание

Введение

В течение этого запроса на обслуживание можно хотеть, чтобы Инженеры Cisco обратились сети организации. Предоставление такого доступа будет часто позволять вашему запросу на обслуживание быть решенным более быстро. В таких случаях, Cisco, и будет только, может обратиться к вашей сети с вашими разрешениями.

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.

Условные обозначения

Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Лучшие методы

Cisco рекомендует придерживаться этих рекомендаций, чтобы помочь вам защищать безопасность своей сети, когда вы предоставляете доступ к любому специалисту службы поддержки или человеку за пределами вашей компании или организации.

- Если возможно, используйте Cisco Unified MeetingPlace, чтобы поделиться информацией со специалистами службы поддержки. Cisco рекомендует использовать Cisco Unified MeetingPlace по этим причинам:Cisco Unified MeetingPlace использует Протокол SSL, который более безопасен, чем "Безопасная оболочка" (SSH) или Telnet в некоторых случаях.Cisco Unified MeetingPlace не требует, чтобы вы предоставили пароли любому за пределами вашей компании или организации.**Примечание:** Каждый раз, когда вы предоставляете доступ к сети людям за пределами вашей компании или организации, любые пароли, которые вы предоставляете, должны быть временными паролями, которые допустимы только, пока третья сторона требует доступа к вашей сети.Как правило, Cisco Unified MeetingPlace не требует, чтобы вы изменили свою политику межсетевого экрана, потому что большинство межсетевых экранов предприятия предоставляет исходящий доступ HTTPS.Cisco Unified MeetingPlace посещения для получения дополнительной информации.
- Если вы не можете использовать Cisco Unified MeetingPlace и если вы принимаете решение предоставить сторонний доступ через другое приложение, такое как SSH, гарантировать, что пароль является временным и доступным для одноразового использования только. Кроме того, необходимо сразу изменить или лишить законной силы пароль после того, как сторонний доступ больше не будет необходим. При использовании приложения кроме Cisco Unified MeetingPlace можно выполнить эти процедуры и рекомендации:Для создания временной учетной записи на маршрутизаторах Cisco IOS используйте эту команду:`Router(config)#`**`username tempaccount secret QWE!@#`** Для создания временной учетной записи на PIX/ASA используйте эту команду:`PIX(config)#`**`username tempaccount password QWE!@#`** Для удаления временной учетной записи используйте эту команду:`Router (config)#`**`no username tempaccount`** Случайным образом генерируйте временный пароль. Временный пароль не должен быть отнесен к запросу определенного сервиса или поставщику служб поддержки. Например, не используйте пароли, такие как *Cisco*, *cisco123* или *ciscotac*.Никогда не давайте свое собственное имя пользователя или пароль.Не используйте Telnet по Интернету. Это не безопасно.
- Если устройство Cisco, которое требует поддержки, расположено позади корпоративного межсетевого экрана, и изменение к политике межсетевого экрана требуется для специалиста службы поддержки к SSH в устройство Cisco, гарантируйте, что изменение политики является определенным для специалиста службы поддержки, назначенного на проблему. Никогда не делайте исключение политики открытым для всей сети или для более широкого диапазона хостов, чем необходимый.Для изменения политики межсетевого экрана на межсетевом экране Cisco IOS добавьте эти линии к списку доступа на вход под интернет-интерфейсом направления:`Router(config)#`**`ip access-list ext inbound`** `Router(config-ext-nacl)#`**`1 permit tcp host <`***`IP address for TAC engineer`***`> host <`***`Cisco device address`***`> eq 22`** **Примечание:** В данном примере `(config-ext-nacl) #` конфигурация отображен на двух линиях для сохранения пространства. Однако, когда вы добавляете эту команду к списку доступа на вход, конфигурация должна появиться на одной линии.Для изменения политики межсетевого экрана на межсетевом экране PIX/ASA Cisco добавьте эту линию к входящему access-group:`ASA(config)#`**`access-list inbound line 1 permit tcp host <`***`IP address for TAC engineer`***`> host <`***`Cisco device address`***`> eq 22`** **Примечание:** В данном примере `ASA (config) #` конфигурация отображен на двух линиях для сохранения пространства. Однако, когда вы добавляете эту команду к входящему access-group, конфигурация должна появиться на одной линии.Для предоставления доступа SSH на маршрутизаторах Cisco IOS добавьте эту линию к

access-class:`Router(config)#`**`access-list 2 permit host <`***`IP address for TAC engineer`***`>`
`Router(config)#`**`line vty 0 4`** `Router(config-line)#`**`access-class 2`** Для предоставления доступа SSH на PIX/ASA Cisco добавьте эту конфигурацию:`ASA(config)#`**`ssh <`***`IP address for TAC engineer`***`> 255.255.255.255 outside`**

Если имеют вопросы об или требуют, чтобы дополнительная помощь с информацией, описанной в этом документе, связалась с Центром технической поддержки Cisco (TAC).

Эта веб-страница для получений информации только и предоставлена на, "как" основание без любой гарантии или гарантии. Оптимальные методы выше не предназначены, чтобы быть всесторонними, но предложены дополнить текущие процедуры обеспечения безопасности клиентов. Эффективность любой практики безопасности зависит от определенной ситуации каждого клиента; и клиенты поощрены рассмотреть все соответствующие факторы при определении процедур обеспечения безопасности, самых соответствующих их сетям.

Дополнительные сведения

- Cisco Unified MeetingPlace
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Центр технической поддержки Cisco (TAC)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация