Содержание

Введение

Маршрутизаторы Интегрированного сервиса Cisco (ISR) предлагают масштабируемую платформу адресным сведениям и требованиям голосовой сети для широкого диапазона приложений. Несмотря на то, что среда угрозы и частных и подключенных к Интернету сетей очень динамическое окружение, Cisco, которую IOS® Firewall предлагает проверке трафика потоком и Контролю приложения и Контролю (AIC) возможности определить и принудить положение защищенной сети, в то время как это включает бизнес-возможность и непрерывность.

Этот документ описывает дизайн и обсуждения конфигурации для аспектов межсетевой защиты определенной Cisco основанные на ISR данные и сценарии голосового приложения. Конфигурации для голосовых сервисов и межсетевого экрана предоставлены для каждого сценария приложения. Каждый сценарий описывает VoIP и конфигурации безопасности отдельно, придерживавшийся всей конфигурацией маршрутизатора. Ваша сеть возможно может потребовать другой конфигурации для сервисов, таких как QoS и VPN, для поддержания качества голосовой связи и конфиденциальности.

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Общие сведения межсетевого экрана IOS

Межсетевой экран Cisco IOS, как правило, развертывается в сценариях приложения, которые отличаются от моделей развертывания межсетевых экранов устройства. Типичные развертывания включают приложения Удаленного сотрудника, маленькие - или узлы филиала компании и розничные приложения, где желаемы низкое количество устройства, интеграция множественного обслуживания, и низшая производительность и глубина возможностей по обеспечению безопасности.

В то время как приложение контроля межсетевого экрана, наряду с другими интегрированными сервисами в продуктах ISR, может казаться привлекательным от стоимости и в рабочем состоянии перспективы, определенные факторы должны быть оценены, чтобы определить, является ли основанный на маршрутизаторе межсетевой экран соответствующим. Если недостаточно мощное основанное на Интегрированном маршрутизаторе решение развернуто, приложение каждой дополнительной характеристики подвергается памяти и затратам на обработку, и может, вероятно, способствовать уменьшенным скоростям производительности пересылки, увеличенная задержка передачи пакетов, и потеря функциональных возможностей в течение периодов пиковой нагрузки. Наблюдайте эти рекомендации, когда вы решите между маршрутизатором и устройством:

- Маршрутизаторы со множественными интегрированными активированными опциями подходят лучше всего для филиала компании или узлов удаленного пользователя, где меньше устройств предлагает лучшее решение.
- Высокая пропускная способность, высокоэффективные приложения, как правило, лучше обращаются с устройствами; Cisco ASA и Cisco, Унифицированный Сервер Call Manager должен быть применен для обработки NAT и приложения политики безопасности и обработки вызовов, в то время как маршрутизаторы обращаются к приложению политики QoS, завершению глобальной сети (WAN) и сквозным VPN-соединение требованиям подключения.

До введения версии программного обеспечения Cisco IOS 12.4 (20) T Классический Межсетевой экран и Zone-Based Policy межсетевой экран (ZFW) были неспособны к полностью возможностям поддержки, требуемым для Трафика VoIP и основанных на маршрутизаторе голосовых сервисов, которые потребовали, чтобы большие разрывы в иначе безопасной политике межсетевого экрана приняли голосовой трафик и предложили ограниченную поддержку развития протоколы сред и VoIP передача сигналов.

Разверните Zone-Based Policy межсетевой экран Cisco IOS

Если требования безопасности сети определены и описаны политикой безопасности, Zone-Based Policy межсетевой экран Cisco IOS, подобный другим межсетевым экранам, может только предложить безопасный межсетевой экран. Существует два фундаментальных подхода для поступления в политику безопасности: *доверчивая* перспектива, в противоположность *подозрительной* перспективе.

Доверчивая перспектива предполагает, что весь трафик защищен, за исключением того, что, который может быть специально определен как злонамеренный или нежелательный. Определенная политика проводится, который запрещает только нежелательный трафик. Это, как правило, выполняется посредством использования определенные записи контроля доступа или подпись - или основанные на поведении программные средства. Этот подход имеет тенденцию вмешиваться меньше в существующие приложения, но требует всестороннего знания среды угрозы и уязвимости и требует, чтобы постоянная бдительность обратилась к новым угрозам и использованию, как они появляются. Кроме того, сообщество пользователей должно играть значительную роль в обслуживании соответствующей безопасности. Среда, которая позволяет широкую свободу с небольшим контролем для жителей, предлагает существенную возможность для проблем, вызванных небрежными или злонамеренными частными лицами. Дополнительная проблема этого подхода состоит в том, что он полагается намного больше на программные средства эффективного управления и управление приложениями, которое предлагает достаточную гибкость и производительность, чтобы быть в состоянии контролировать и управлять подозрительными данными во всем сетевом трафике. В то время как технология в настоящее время доступна для размещения этого, в рабочем состоянии нагрузка часто превышает пределы большинства организаций.

Подозрительная перспектива предполагает, что весь сетевой трафик нежелателен, за исключением специально определенного *хорошего* трафика. Это - политика, которая применена, который запрещает весь трафик приложения, за исключением того, что, который явно разрешен. Кроме того, контроль приложения и контроль (AIC) могут быть внедрены, чтобы определить и запретить вредоносный трафик, который в частности обработан для использования *хороших* приложений, а также нежелательного трафика, который подменяет *хорошим* трафиком. Снова, управление приложениями налагает в рабочем состоянии и трудности производительности в сети, невзирая на то, что большая часть нежелательного трафика должна управляться фильтрами не сохраняющими состояние, такими как списки управления доступом (ACL) или Zone-Based Policy межсетевой экран (ZFW) политика, таким образом, существует существенно меньше трафика, который должен быть обработан AIC, системой предотвращения вторжений (IPS) или другими основанными на подписи средствами управления, такими как гибкое пакетное соответствие (FPM) или сетевое распознавание приложений (NBAR). Если только порты требуемого приложения (и динамический специфичный для сред трафик, являющийся результатом известных контрольных соединений или сеансов), в частности разрешены, единственный нежелательный трафик, который присутствует в сети, должен попасть в определенное, more-easily-recognized подмножество, которое уменьшает техническую и в рабочем состоянии нагрузку, наложенную для обеспечивания контроля над нежелательным трафиком.

Этот документ описывает конфигурации безопасности VoIP на основе *подозрительной* перспективы, поэтому только трафик, который допустим в сегментах голосовой сети, разрешен. Политика данных имеет тенденцию быть более разрешающей, как описано примечаниями в конфигурации каждого сценария приложения.

Все развертывания политики безопасности должны придерживаться цикла замкнутой петли обратной связи; развертывания безопасности, как правило, влияют на возможность и функциональность существующих приложений и должны быть отрегулированы, чтобы минимизировать или решить это влияние.

При необходимости в дополнительных общих сведениях для настройки Zone-Based Policy межсетевого экрана, рассмотрите Зональное Руководство по дизайну Межсетевого экрана и Руководство по приложениям.

Факторы для ZFW в средах VoIP

Зональное Руководство по дизайну Межсетевого экрана и Руководство по приложениям предлагают краткое обсуждение о безопасности маршрутизатора с использованием политики безопасности к и от *сам* зона маршрутизатора, а также альтернативные возможности, которые предоставлены через различные функции Сетевой защиты основы (NFP). Основанные на маршрутизаторе возможности VoIP размещены в *сам* зона маршрутизатора, таким образом, политика безопасности, которая защищает маршрутизатор, должна знать о требованиях для голосового трафика для размещения голосовой сигнализации и сред, инициируемых и предназначенный к Cisco Unified CallManager Express, Survivable Remote Site Telephony и ресурсам Голосового шлюза. До версии программного обеспечения Cisco IOS 12.4 (20) T, Классического Межсетевого экрана и Zone-Based Policy межсетевого экрана было неспособно полностью принять требования Трафика VoIP, таким образом, политика межсетевого экрана не была оптимизирована, чтобы полностью защитить ресурсы. Политика самозоне security, которая защищает основанные на маршрутизаторе ресурсы VoIP, полагается в большой степени на возможности, представленные в 12.4 (20) T.

Голосовые характеристики межсетевого экрана IOS

Программное обеспечение Cisco IOS версии 12.4(20)T представило несколько усовершенствований для включения совместно расположенного Зонального Межсетевого экрана и мощностей речевого сигнала. Три основных характеристики применяются непосредственно для обеспечения голосовых приложений:

- Усовершенствования SIP: шлюз уровня приложения и контроль приложения и контрольПоддержка версии SIP обновлений к SIPv2, как описано RFC 3261Расширяет поддержку сигнализации SIP для распознавания более широкого разнообразия диаграмм вызововПредставляет Контроль приложения SIP и Контроль (AIC) для применения гранулированных средств управления для адресации к определенным уязвимостям уровня приложения и использованиюРазворачивает самозональный контроль, чтобы быть в состоянии распознать вторичную сигнализацию и каналы сред тот результат locally-destined/-originated трафик SIP
- Поддержка Skinny локального трафика и CMESCCP обновлений поддерживает к версии 16 (ранее поддерживаемая версия 9)Представляет Контроль приложения SCCP и Контроль (AIC) для применения гранулированных средств управления для адресации к определенным уязвимостям уровня приложения и использованиюРазворачивает самозональный контроль, чтобы быть в состоянии распознать вторичную сигнализацию и каналы сред, которые следуют из locally-destined/-originated трафика SCCP
- Поддержка H.323 версий 3 и 4H.323 обновлений поддерживает к версиям 3 и 4 (ранее поддерживаемые версии 1 и 2)Представляет Контроль приложения H.323 и Контроль

(AIC) для применения гранулированных средств управления для адресации к определенным уязвимостям уровня приложения и использованию

Конфигурации безопасности маршрутизатора, описанные в этом документе, включают возможности, предлагаемые этими усовершенствованиями с пояснениями для описания действия, примененного политикой. Гиперссылки к документам отдельной функции доступны в Дополнительных сведениях