Руководство Cisco для укрепления межсетевого экрана Cisco ASA

Содержание

Введение

Этот документ содержит информацию, чтобы помочь вам защищать устройства Cisco ASA, который увеличивает общую безопасность вашей сети. Этот документ структурирован в 4 Разделах

Укрепление Панели управления - Это применяется к отнесенному Менеджменту/К всего ASA трафик коробки как SNMP, SSH и т.д.
Обеспечение config - Команды, посредством которых мы можем прекратить заполнять пароли и т.д. для рабочего config и т.д.
Регистрация и Контролирующий - Это применяется к любым параметрам настройки, отнесенным к входу ASA.
Сквозной трафик - Это применяется к трафику, который проходит ASA.

Покрытие характеристик безопасности в этом документе часто предоставляет достаточно подробности для вас для настройки функции. Однако в случаях, где это не делает, функция объяснена таким способом, которым можно оценить, требуется ли дополнительное внимание к функции. Где возможный и соответствующий, этот документ содержит рекомендации, что, если внедрено, справка защищает сеть.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Cisco ASA5500-X 9.4 (1) и позже.

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.

Родственные продукты

Эта конфигурация может также использоваться с Версией программного обеспечения 9 Устройства безопасности Cisco ASA 5500-X Series. x.

Условные обозначения

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

Безопасные операции

Операции защищенной сети являются существенной темой. Несмотря на то, что большая часть этого документа посвящена безопасной конфигурации устройства Cisco ASA, одни только конфигурации не делают абсолютно безопасный сеть. Рабочие процедуры в использовании в сети способствуют так же безопасности как конфигурация базовых устройств.

Эти темы содержат в рабочем состоянии рекомендации, которые вам рекомендуют внедрить. Эти темы выделяют определенные критические области функционирований сети и не являются всесторонними.

Cisco Security монитора информационные сообщения и ответы

Команда расследования инцидента, связанного с безопасностью продукта Cisco (PSIRT) создает и поддерживает публикации, обычно называемые Информационными сообщениями PSIRT, для связанных с безопасностью проблем в продуктах Cisco. Метод, используемый для связи менее серьезных проблем, является Cisco Security Ответ. Рекомендации по вопросам безопасности и ответы доступны в PSIRT.

Дополнительные сведения об этих механизмах связи доступны в Политике Уязвимости Cisco Security.

Для поддержания защищенной сети необходимо знать об информационных сообщениях Безопасности Cisco и ответах, которые были освобождены. Необходимо ознакомиться с уязвимостью перед угрозой, которую она может представить сети, может быть оценен. См. Медицинскую сортировку Риска для Объявлений Уязвимости безопасности для помощи этот процесс оценки.

Аутентификация, авторизация и учет рычагов

Платформа Аутентификации, авторизации и учета (AAA) жизненно важна для устройств

защищенной сети. Инфраструктура AAA предоставляет аутентификацию сеансов управления и может также ограничить пользователей определенными, определенными администраторами командами и регистрировать все команды, введенные всеми пользователями. Посмотрите раздел Аутентификации, авторизации и учета этого документа для получения дополнительной информации о том, как усилить AAA.

Централизуйте регистрационный набор и мониторинг

Для получения знания о существующем, появлении и исторических событиях, отнесенных к случаям нарушения безопасности, организация должна иметь унифицированную стратегию регистрации событий и корреляции. Эта стратегия должна усилить регистрацию от всех сетевых устройств и использование предварительно упакованные и настраиваемые возможности корреляции.

После того, как централизовано регистрация внедрена, необходимо разработать структурированный подход для регистрации анализа и отслеживания инцидента. На основе потребностей вашей организации этот подход может колебаться от простого прилежного анализа данных журнала к усовершенствованному основанному на правилах анализу.

Используйте защищенные протоколы, когда возможно

Много протоколов используются для переноса чувствительных данных управления сетью. Необходимо использовать защищенные протоколы, когда это возможно. Выбор защищенного протокола включает использование SSH вместо Telnet так, чтобы были зашифрованы и данные проверки подлинности и данные для управления. Кроме того, необходимо использовать безопасные протоколы передачи файлов при копировании данных о конфигурации. Примером является использование протокола SCP вместо FTP или TFTP.

Видимость трафика усиления с NetFlow

NetFlow позволяет вам контролировать трафики в сети. Первоначально предназначенный для экспортирования информации о потоке данных в приложения для управления сетью NetFlow может также использоваться для показа сведений о потоках на маршрутизаторе. Эта возможность позволяет вам видеть, какой трафик пересекает сеть в режиме реального времени. Независимо от того, экспортируются ли сведения о потоках в удаленный коллектор, вам рекомендуют настроить сетевые устройства для NetFlow так, чтобы это могло использоваться реактивным образом в случае необходимости.

Управление конфигурацией

Управление конфигурацией является процессом, которым изменения конфигурации предложены, рассмотрены, утверждены и развернуты. В контексте конфигурации устройства Cisco ASA два дополнительных аспекта управления конфигурацией важны: архивация конфигурации и безопасность.

Можно использовать архивные конфигурации для отката изменений, которые внесены в сетевые устройства. В контексте безопасности архивные конфигурации могут также использоваться для определения, какие изменения безопасности были сделаны и когда произошли эти изменения. В сочетании с данными журнала AAA эта информация может помочь в аудите безопасности сетевых устройств.

Конфигурация устройства Cisco ASA содержит много чувствительных подробных данных. Имена пользователей, пароли и содержание списков контроля доступа являются примерами этого типа информации. Репозиторий, который вы используете для архивации конфигураций устройства Cisco ASA должен быть защищен. Опасный доступ к этой информации может подорвать безопасность всей сети.

Панель управления

Панель управления состоит из функций, которые достигают целей управления сети. Это включает интерактивные сеансы управления, которые используют SSH, а также сбор статистики с SNMP или NetFlow. Когда вы рассматриваете безопасность сетевого устройства, важно, что защищена панель управления. Если случай нарушения безопасности в состоянии подорвать функции панели управления, для вас может быть невозможно восстановить или стабилизировать сеть.

Укрепление панели управления

Панель управления используется, чтобы обратиться, настроить, и управлять устройством, а также контролировать его операции и сеть, в которой она развернута. Панель управления является плоскостью, которая получает и передает трафик за использованием этих функций. Этот список протоколов используется панелью управления:

- Simple Network Management Protocol
- Протокол Secure Shell
- Протокол передачи файлов
- Trivial File Transfer Protocol
- Безопасный протокол копирования
- TACACS +
- RADIUS
- NetFlow
- Протокол NTP (Network Time Protocol, протокол сетевого времени)
- Системный журнал
- ICMP
- SMB

Примечание: Включение TELNET не рекомендуется, поскольку это - открытый текст.

Управление паролями

Пароли управляют доступом к ресурсам или устройствам. Это выполнено через определение пароль или тайна, которая используется для аутентификации запросов. Когда запрос получен для доступа к ресурсу или устройству, запросу бросают вызов для проверки пароля и идентичности, и доступ может быть предоставлен, запрещен или ограничен на основе результата. Как оптимальный метод безопасности, паролями нужно управлять с TACACS + или Сервер проверки подлинности RADIUS. Однако обратите внимание, что локально настроенный пароль для привилегированного адреса все еще необходим в случае сбоя TACACS + или Сервисы RADIUS. Устройство может также иметь другой подарок сведений о пароле в своей конфигурации, такой как ключ NTP, Строка имени и пароля SNMP или ключ Протокола маршрутизации.

ASA использует алгоритм представления сообщения в краткой форме 5 (MD5) для хеширования пароля. Этот алгоритм имел значительную общественную оценку и, как известно, не обратим. Однако алгоритм подвергается подборам пароля по словарю. В подборе пароля по словарю атакующий пробует каждое слово в словаре или другом списке паролей кандидата для обнаружения соответствия. Поэтому файлы конфигурации должны быть надежно сохранены и только разделены с доверяемыми частными лицами.

Включите сервис HTTP

Для использования ASDM необходимо включить сервер HTTPS и позволить Подключения HTTPS ASA. Устройство безопасности позволяет максимум 5 параллельных экземпляров ASDM на контекст, при наличии, максимум с 32 экземпляров ASDM между всеми контекстами. Для настройки ASDM обращаются к использованию:

```
http server enable <port>
```

Позвольте только IP, которые необходимы в списке ACL. Предоставление широкого доступа является неправильной практикой.

```
http 0.0.0.0 0.0.0.0 <interface>
```

Настройте управление доступом ASDM:

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Начиная с выпуска ПО ASA 9.1 (2), 8.4 (4.1), ASA теперь поддерживает следующий эфемерный Диффи-Хеллман (DHE) наборы шифров SSL.

DHE-AES128-SHA1
DHE-AES256-SHA1

Эти наборы шифров заданы в **RFC 3268**, Расширенный стандарт шифрования (AES) Ciphersuites для Transport Layer Security (TLS).

Когда поддерживается клиентом, DHE является предпочтительным шифром, потому что это предоставляет Непосредственный контроль секретности (Perfect Forward Secrecy). Посмотрите следующие ограничения:

DHE не поддерживается на соединениях SSL 3.0, поэтому удостоверьтесь, что также включили TLS 1.0 для SSL - сервера.

```
// Set server version ASA(config)# ssl server-version tlsv1 sslv3
// Set client version ASA(config) # ssl client-version any
```

Некоторые широка используемые приложение не поддерживают DHE, поэтому включают, по крайней мере, еще один метод шифрования SSL, чтобы гарантировать, что может использоваться набор шифров, характерный и для клиента SSL и для сервера. Некоторые клиенты могут не поддержать DHE, включая AnyConnect 2.5 и 3.0, Cisco Secure Desktop и Internet Explorer 9.0.

ASA включил ниже шифров в заказе как ниже по умолчанию.

```
ASA(config)#ssl encryption rc4-sha1 dhe-aes128-sha1 dhe-aes256-sha1 aes128-sha1 aes256-sha1
3des-sha1
```

версия сервера ssl любой (по умолчанию)

ASA по умолчанию использует Временный Подписанный сертификат, который изменяется на каждой перезагрузке. При поиске одиночного сертификата можно перейти по ссылке ниже для генерации Постоянного Подписанного сертификата.

Теперь ASA поддерживает версию TLS 1.2 startig от версии программного обеспечения 9.3.1for безопасная передача сообщения для ASDM, Безклиентого SSVPN и VPN AnyConnect. Следующие команды были представлены или модифицированные команды: **версия клиентской части ssl**, **ssl версия сервера**, **ssl шифр**, **ssl точка доверия**, **ssl dh группа**, **show ssl**, **шифр show ssl**, **покажите vpn-sessiondb**

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

Включите SSH

ASA позволяет SSH - подключения ASA для целей управления. ASA позволяет максимум 5 параллельных SSH - подключений на контекст, при наличии, максимум с 100 соединений, разделенных между всеми контекстами.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

Тип пары согласованных ключей по умолчанию является общим ключом. Размер модуля по умолчанию 1024. Сумма пространства NVRAM для хранения пар ключей варьируется в зависимости от платформы ASA. Можно достигнуть предела при генерации больше чем 30 пар ключей. 4096-разрядные ключи RSA только поддерживаются на ASA5580, 5585, или более поздние платформы.

Удалить пары ключей обозначенного типа (rsa или dsa)

```
crypto key zeroize { rsa | dsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

Настройте SSH для доступа удаленного устройства:

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Для ограничения версии SSH, принятого ASA, используйте команду version ssh в режиме глобальной конфигурации. Ограничить ASA, чтобы только использовать версию 2 может быть Доном wusing ниже команды.

```
ASA(config)#ssh version 2
```

Для обмена ключами с помощью или Группы Diffie-Hellman (DH) 1 или DH Group 14 методов обмена ключами используйте команду обмена ключами ssh в режиме глобальной конфигурации. при начале от 9.1 (2) ASA поддерживает dh-group14-sha1 для SSH

```
ASA(config)#ssh key-exchange dh-group14-sha1
```

Настройте таймаут для сеансов регистрации

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

Управление паролями

Пароли управляют доступом к ресурсам или устройствам. Это выполнено через определение пароль или тайна, которая используется для аутентификации запросов. Когда запрос получен для доступа к ресурсу или устройству, запросу бросают вызов для проверки пароля и идентичности, и доступ может быть предоставлен, запрещен или ограничен на основе результата. Как оптимальный метод безопасности, паролями нужно управлять с TACACS + или Сервер проверки подлинности RADIUS. Однако обратите внимание, что локально настроенный пароль для привилегированного адреса все еще необходим в случае сбоя TACACS + или Сервисы RADIUS. Устройство может также иметь другой подарок сведений о пароле в своей конфигурации, такой как ключ NTP, Строка имени и пароля SNMP или ключ Протокола маршрутизации.

Настройте локального пользователя и зашифрованный пароль

```
username <local_username> password <local_password> encrypted
```

Настройте Enable Password

```
enable password <enable_password> encrypted
```

Настройте аутентификацию AAA (проверка подлинности, авторизация и учет) для режима включения

```
ASA(config)#aaa authentication enable console LOCAL
```

Аутентификация, авторизация и учет

Платформа Аутентификации, авторизации и учета (AAA) важна для обеспечения интерактивного доступа к сетевым устройствам. Инфраструктура AAA предоставляет высоконастраиваемую среду, которая может быть адаптирована на основе потребностей сети.

Аутентификация TACACS+

TACACS + является протоколом аутентификации, который ASA может использовать для аутентификации пользовательских интерфейсов управления против удаленного AAA-сервера. Эти пользовательские интерфейсы управления могут обратиться к устройству ASA через SSH, HTTPS, telnet или HTTP.

TACACS + аутентификация, или более широко аутентификация AAA (проверка подлинности, авторизация и учет), предоставляет способность использовать учетные записи отдельного пользователя на каждого администратора сети. Когда вы не зависите от одиночного совместно используемого пароля, безопасность сети улучшена, и ваша отслеживаемость усилена.

RADIUS является протоколом, подобным в цели к TACACS +; однако, это только шифрует пароль, передаваемый по сети. Напротив, TACACS + шифрует все Содержимое tcp, которое включает обоих имя пользователя и пароль. Когда TACACS + поддерживается AAA-сервером, поэтому TACACS + должен использоваться в предпочтении к RADIUS. См. TACACS + и Сравнение RADIUS для более подробного сравнения этих двух протоколов.

TACACS + аутентификация может быть включен на устройстве Cisco ASA с конфигурацией, подобной данному примеру:

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

Подписание образа ASA и проверка

Начало с образов ASA версии программного обеспечения 9.3.1 теперь подписано с помощью цифровой подписи. Цифровая подпись проверена после того, как ASA загружен.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done! Embedded Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e Computed Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e CCO Hash SHA-512:
1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
c99f49f70354715441385e0b96e4bd3e861d18fb30433d52e12b15b501fa790f36d0ea0 Signature Verified
ASA(config)# verify /signature running Requesting verify signature of the running image...
Starting image verification Hash Computation: 100% Done! Computed Hash SHA2:
2fbb0f62b5fbc61b081acfca76bddbb2 26ce7a5fb4b424e5e21636c6c8a7d665
1e688834203dfb7ffa6eaefc7fdf9d3d 1d0a063a20539baba72c2526ca37771c Get key records from key
storage: PrimaryASA, key_store_type: 6 Embedded Hash SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
26ce7a5fb4b424e5e21636c6c8a7d665 1e688834203dfb7ffa6eaefc7fdf9d3d
1d0a063a20539baba72c2526ca37771c Returned. rc: 0, status: 1 The digital signature of the running
image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
Signer Information
Common Name : abraxas
Organization Unit : ASAv
Organization Name : CiscoSystems
Certificate Serial Number : 550DBBD5
Hash Algorithm : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version : A
```

Настройте зону времени синхронизации

```
clock timezone GMT <hours offset>
```

Настройте NTP

Протокол NTP не является особенно опасным сервисом, но любой ненужный сервис может представлять вектор атаки. Если NTP используется, важно явно настроить доверяемый источник времени и использовать правильную проверку подлинности. Точное и надежное время требуется в целях системного журнала, такой как во время судебных расследований потенциальных атак, а также для успешной возможности VPN - подключения когда в зависимости от сертификатов для аутентификации Фазы 1.

- **Часовой пояс NTP** - при настройке NTP, часовой пояс должен быть настроен так, чтобы могли быть точно коррелированы метки времени. Обычно существует два подхода для настройки часового пояса для устройств в сети с глобальным присутствием. Один метод должен настроить все сетевые устройства с Согласованным текущим временем (UTC) (ранее Время по Гринвичу (GMT)). Другой подход должен настроить сетевые устройства с местным часовым поясом.

```
ntp server ip_address [ key key_id ] [ source interface_name ] [ prefer ]
```

- **Аутентификация NTP** - при настройке Аутентификации NTP она предоставляет обеспечение, что сообщениями NTP обмениваются между доверяемым Ntp peer. Включите аутентификацию с помощью команды ntp authenticate, устанавливает доверяемый ключевой ID для этого сервера. При включении аутентификации ASA только связывается с сервером NTP, если это использует корректный доверяемый ключ в пакетах. Для включения аутентификации с сервером NTP используйте команду ntp authenticate в режиме глобальной конфигурации.

```
ASA(config)#ntp authenticate
```

Сервис Сервера DHCP (Не будучи используемым)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

Примечание: ASA не поддерживает CDP.

Access-list уровня управления

Правила управления доступом для трафика управления к коробке (определенный такими командами как http, ssh или telnet) имеют более высокий приоритет, чем список доступа, примененный с опцией уровня управления. Поэтому такому разрешенному трафику управления позволят войти даже если явно запрещенный списком доступа к коробке.

```
access-list <name> in interface <Interface_name> control-plane
```

От ASA

Вот протоколы, которые могут использоваться для копирования файлов к ASA.

Удалить текст:

- Ftp
- HTTP
- Tftp

- SMB

Безопасный:

- HTTPS
- SCP (Безопасный Клиент Копии) запускающийся от 9.1 (5), ASA поддерживает клиента SCP для передачи файлов и от сервера SCP.

Для Сквозного трафика

Рандомизация порядкового номера TCP

Каждый TCP - подключение имеет два ISN: один генерируется клиентом, другой - сервером. ASA рандомизирует ISN SYN TCP, проходящего и во входящем и в исходящих направлениях.

Рандомизация ISN защищенного хоста препятствует тому, чтобы атакующий предсказал следующий ISN для нового соединения и потенциально угнал новый сеанс.

Назначение случайного значения для ISN TCP может быть отключено. Пример:

- Если используется другой встроенный межсетевой экран, который назначает ISN в случайном порядке, то нет необходимости двум межсетевым экранам выполнять эту операцию, несмотря на то, что это не влияет на изменения объема трафика.
- При использовании мультипереход eBGP через ASA, и узлы eBGP используют MD5. Рандомизация ломает контрольную сумму MD5.
- Если мы используем устройство WAAS, которое требует, чтобы ASA не рандомизировал порядковые номера соединений.

Декремент TTL

По умолчанию, не постепенно уменьшает TTL в IP - заголовке, из-за которого ASA не обнаруживается как транзитный участок при выполнении Traceroute.

dnsguard

Принуждает один DNS - ответ на запрос. Это Может быть включено с помощью команды в режиме глобальной конфигурации.

```
ASA(config)#dns-guard
```

Настройте проверки фрагментации Fragment Chain

Чтобы предоставить дополнительное управление фрагментации пакета и улучшить совместимость с NFS, используйте команду фрагмента в режиме глобальной конфигурации.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

Настройте контроль протокола

Инспекционные механизмы требуются для сервисов, которые встраивают информацию о IP-адресации в пакет данных пользователя или что открытые дополнительные каналы на динамично назначенных портах. Эти протоколы требуют, чтобы ASA сделал глубокую проверку пакетов вместо того, чтобы передать пакет через быстрый маршрут. В результате инспекционные механизмы могут влиять на суммарную пропускную способность. Обратитесь Руководство Config ASA 9.4 для подробных сведений на Контроле Протокола уровня приложений.

С помощью контроль на ASA можно включить ниже команды

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

ASA по умолчанию имеет **"global_policy"**, включенный глобально.

Настройте одноадресную пересылку по обратному пути

```
ip verify reverse-path interface <interface_name>
```

Когда трафик отброшен из-за Проверки переадресации по обратному пути, ниже счетчика "покажите отбрасывание гадюки" на инкрементах ASA.

```
ASA(config)# show asp drop

Frame drop:
 Invalid TCP Length (invalid-tcp-hdr-length)                21
  Reverse-path verify failed (rpf-violated)                  90

// Check Reverse path statistics

ASA(config)# sh ip verify statistics
 interface inside: 11 unicast rpf drops
interface outside: 79 unicast rpf drops
```

Обнаружение угрозы

Обнаружение угрозы предоставляет администраторам межсетевого экрана необходимые программные средства, чтобы определить, понять, и остановить атаки, прежде чем они достигнут инфраструктуры внутренней сети. В заказе для этого функция полагается на многие другие триггеры и статистику, которая описана более подробно в этих разделах.

Обратитесь Функциональность Обнаружения Угрозы ASA и Конфигурацию для подробного пояснения на Обнаружении Угрозы на ASA.

Фильтр ботнета

Фильтр трафика BotNet контролирует запросы Сервера доменных имен (DNS) и ответы между клиентами Internal DN и внешними серверами DNS. Когда DNS - ответ обработан, домен, привязанный к ответу, проверен против базы данных известных злонамеренных доменов. Если существует соответствие, дальнейший трафик к подарку IP-адреса в DNS - ответе заблокирован.

Вредоносное ПО является вредоносным программным обеспечением, которое установлено на хосте незнания. Вредоносное ПО, которое делает попытку активности сети, такой как передача закрытых данных (пароли, номера кредитной карты, нажатия клавиш или составляющие собственность данные) может быть обнаружено Фильтром трафика Ботнета, когда вредоносное ПО запускает соединение с известным плохим IP-адресом. Поступление проверок Фильтра трафика Ботнета и исходящие соединения против базы динамических данных известных плохих доменных имен и IP-адресов (*черный список*), и затем регистрируют или блокируют любую подозрительную операцию.

Можно также добавить базу динамических данных Cisco с помещенными в черный список адресами выбора путем добавления их к статическому черному списку; если база динамических данных включает помещенные в черный список адреса, что вы думаете, не должен быть помещен в черный список, можно вручную ввести их в статический *белый список*. Адреса в белом списке все еще генерируют сообщения системного журнала, но потому что вы только предназначаетесь для сообщений системного журнала черного списка, они являются информационными. Обратитесь Настройку Фильтр трафика Ботнета для получения дальнейшей информации.

Добавления кэша ARP для несвязанных подсетей

ASA по умолчанию не отвечает на ARP для IP-адресов ненапрямую подключенной подсети. Если у вас есть IP NAT на ASA, который не принадлежит IP той же подсети интерфейса ASA, мы должны будем включить "arp, несвязанного с разрешением" на ASA с Proxy-arp для преобразованного посредством NAT IP.

```
arp permit-nonconnected
```

Всегда рекомендуется иметь корректную маршрутизацию на входящих и исходящих устройствах для NAT для работы, не выполняя вышеупомянутую команду.

Регистрация и мониторинг

Настройке функции SNMP

Этот раздел выделяет несколько методов, которые могут использоваться для обеспечения развертываний SNMP в устройствах ASA. Важно, что SNMP должным образом защищен для защиты конфиденциальности, целостности и доступности и сетевых данных и сетевых устройств, через которые передают транзитом эти данные. SNMP предоставляет вам полную информацию на состоянии сетевых устройств. Эта информация должна быть защищена от злонамеренных пользователей, которые хотят усилить эти данные для выполнения атак на сеть.

Строки имени и пароля SNMP

Строки имени и пароля являются паролями, которые применены к устройству ASA для ограничения доступа, и только для чтения и доступ для чтения-записи, к данным SNMP на устройстве. Эти строки имени и пароля, как со всеми паролями, должны быть тщательно выбраны, чтобы гарантировать, что они не тривиальны. Строки имени и пароля должны быть изменены через определенные промежутки времени и в соответствии с политикой сетевой безопасности. Например, когда администратор сети изменяет роли или покидает

компанию, строки должны быть изменены.

Включите доступ для чтения SNMP:

```
snmp-server host <interface_name> <remote_ip_address>
```

Включите trap-сообщения SNMP

```
snmp-server enable traps all
```

Системный журнал Настройки

Рекомендуется передать регистрационную информацию к удаленному серверу системного журнала. Это позволяет коррелировать и аудит сети и события связанное с безопасностью через сетевые устройства эффективнее. Обратите внимание на то, что сообщения системного журнала переданы ненадежно UDP и в открытом тексте. Поэтому любые меры защиты, которые сеть предоставляет трафику управления (например, шифрование или внеполосный доступ) должны быть расширены для включения трафика системного журнала. Журналы могут быть cofnigured, который будет передаваться следующему назначению от ASA:

- ASDM
- Буфер
- Флэш
- Электронная почта
- FTP-сервер
- Сервер SNMP как trap-сообщения
- Сервер системных журналов

Настройте уровень важности входа через консоль

```
logging console critical
```

TCP базировался, системный журнал также доступен. Все системные журналы могут быть переданы серверу системного журнала в простом тексте или в зашифрованном в случае TCP.

Простой текст

главный компьютер регистрации interface_name syslog_ip [tcp / порт

!--- который будет шифроваться

главный компьютер регистрации *interface_name syslog_ip* **[tcp /** *порт* **| [безопасный]**

Если TCP - подключение не может быть установлен с сервером системных журналов, все новые соединения будут запрещены. Можно изменить это поведение по умолчанию путем ввода "команды**" разрешения-hostdown на регистрацию**.

Настройте метки времени в сообщениях журнала

Конфигурация меток времени регистрации помогает вам коррелировать события через сетевые устройства. Важно внедрить корректную и последовательную конфигурацию метки времени регистрации, чтобы гарантировать, что вы в состоянии сопоставить данные регистрации.

```
logging timestamp
```

Для Дополнительных сведений, отнесенных к системному журналу, обратитесь Пример Конфигурации системного журнала ASA.

Netflow Настройки

Время от времени можно должны быть быстро определить и сетевой трафик обратной трассировки, особенно во время реагирования на инциденты или плохой производительности сети. NetFlow может предоставить видимость в весь трафик в сети. Кроме того, NetFlow может быть внедрен с коллекторами, которые могут предоставить долгосрочное отклонение и автоматизированный анализ.

Cisco ASA поддерживает сервисы Версии 9 NetFlow. ASA и реализации ASASM NSEL предоставляют метод отслеживания IP flow с отслеживанием состояния, который экспортирует только те записи, которые указывают на важные события в потоке. В отслеживании потока с отслеживанием состояния отслеженные потоки проходят серию изменений состояния. События NSEL используются для экспортирования данных о статусе потока и инициированы событием, которое вызвало изменение состояния.

Обратитесь Руководство по внедрению NetFlow Cisco ASA для получения дополнительной информации Netflow на ASA:

Обеспечение config

Проверка образа на ASA

При начале от 9.1 (2) и 8.4 (4.1), была добавлена Поддержка проверки целостности образа SHA 512. Для проверки контрольной суммы файла используйте команду verify в привилегированном режиме EXEC.

Вычисляет и отображает значение MD5 для указанного образа программного обеспечения. Сравните это значение со значением, доступным на Cisco.com для этого образа.

```
verify [ /md5 path ] [ md5-value ]
```

Пароли в config

Все пароли и Ключи или зашифрованы или запутаны. "Show running config" не показывает фактические пароли.

Такая резервная копия не может использоваться для резервной копии/восстановления на ASA. Резервная копия, которая взята в целях восстановления whould быть выполненной с помощью команды "больше system:running-config".The пароли config ASA, может быть зашифрована с помощью основной фразы - пропуска. Обратитесь Шифрование пароля для получения дальнейшей информации.

Восстановление сервисного пароля

Отключение этого отключит механизм восстановления пароля и отключит доступ к ROMMON. Единственные средства восстановления с потерянного или забытых паролей

будут для ROMMON для стирания всех файловых систем включая файлы конфигурации и образы. Необходимо сделать резервную копию конфигурации и иметь механизм для восстановления образов из командной строки ROMMON.

Устранение неполадок

Нет никакого раздела устранения проблем для этого документа.