QoS на примерах конфигурации Cisco ASA

Содержание

Введение

Этот документ объясняет, как Качество обслуживания (QoS) работает на устройство адаптивной защиты Cisco (ASA) и также предоставляет несколько примеров о том, как внедрить его для других сценариев.

Можно настроить QoS на устройстве безопасности для обеспечения ограничения скорости

на выбранном сетевом трафике, и для отдельных потоков и для потоков VPN-туннеля, чтобы гарантировать, что весь трафик получает свои справедливые доли ограниченной пропускной способности.

Функция была интегрирована с идентификатором ошибки Cisco CSCsk06260.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с Модульной политикой Framwork (MPF).

Используемые компоненты

Сведения в этом документе основываются на ASA, который выполняет Версию 9.2, но более ранние версии могут использоваться также.

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.

Общие сведения

QoS является функцией сети, которая позволяет вам уделять первостепенное значение определенным типам интернет-трафика. Поскольку интернет-пользователи обновляют свои точки доступа от модемов до высокоскоростных широкополосных соединений как Цифровая абонентская линия (DSL) и кабель, увеличения вероятности, которые в любое заданное время, одиночный пользователь мог бы быть в состоянии поглотить больше всего, если не все, доступной пропускной способности, таким образом исчерпав ресурсы другие пользователи. Чтобы предотвратить потребление одним пользователем или соединением типа узел-узел большей части полосы пропускания, QoS предоставляет функцию управления трафиком, регулирующую максимальную полосу пропускания, которую может использовать пользователь.

QoS обращается к возможности сети предоставлять лучшее обслуживание выбранного сетевого трафика с помощью различных технологий для улучшения обслуживания в целом посредством ограничения пропускной способности основных технологий.

Основной целью QoS в устройстве безопасности является обеспечение ограничения скорости выбранного сетевого трафика для отдельного потока или потока через VPN-туннель, чтобы гарантировать, что каждый тип трафика получает предназначенную для него ограниченную часть полосы пропускания. Поток можно определить несколькими способами. В устройстве безопасности QoS может применяться к комбинации IP-адресов отправителя и получателя, номеров портов отправителя и получателя и байтов типа обслуживания (ToS) заголовка IP.

Существует три вида QoS, которое можно внедрить на ASA: Применение политик, Формирование и Постановка в очередь с установлением приоритета.

Применение к трафику политик

С применением политик отброшен трафик по указанному пределу. Применение политик является способом гарантировать, что "no traffic" (нет трафика) превышает максимальное значение (в битах/секунда), что вы настраиваете, который гарантирует, что никакой трафик или класс не могут принять весь ресурс. Когда трафик превышает максимальное значение, ASA отбрасывает дополнительный трафик. Применение политик также устанавливает самый большой одиночный позволенный пакет трафика.

Эта схема иллюстрирует то, что делает мониторинг трафика; когда скорость трафика достигает скорости настраиваемого максимального значения, дополнительный трафик отброшен. Результат скорости вывода отображается в виде пилообразной линии с гребнями и впадинами.

Данный пример показывает, как отрегулировать пропускную способность к 1 Мбит/с для определенного пользователя в исходящем направлении:

```
ciscoasa(config)# access-list WEB-LIMIT permit ip host 192.168.10.1 any
ciscoasa(config)# class-map Class-Policy
ciscoasa(config-cmap)# match access-list WEB-LIMIT
ciscoasa(config-cmap)#exit

ciscoasa(config)# policy-map POLICY-WEB
ciscoasa(config-pmap)# class Class-Policy
ciscoasa(config-pmap-c)# police output 1000000 conform-action transmit exceed-
action drop
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit

ciscoasa(config)# service-policy POLICY-WEB interface outside
```

Формирование трафика

Формирование трафика используется для соответствия с устройством и скоростями связи, который управляет потерей пакета, переменной задержкой и насыщенностью ссылки, которая может вызвать дрожание и задержку. Формирование трафика на устройстве безопасности позволяет устройству ограничивать поток трафика. Этот механизм буферизует трафик по "ограничению скорости" и пытается передать трафик позже. Формирование не может быть настроено для определенных типов трафика. Имеющий форму трафик включает трафик, проходящий через устройство, а также трафик, который получен от устройства.

Эта схема иллюстрирует то, что делает формирование трафика; это сохраняет избыточные пакеты в очереди и затем планирует избыток для более поздней передачи по инкрементам времени. Результатом процесса формирования трафика является более ровная выходная скорость передачи пакетов.

> **Примечание:** Формирование трафика только поддерживается на Версиях ASA 5505, 5510, 5520, 5540, и 5550. Многоядерные модели (такой как 5500-X) не поддерживают формирование.

С формированием трафика трафик, который превышает определенный предел, помещен в очередь (буферизованный) и передаваемый во время следующего интервала.

Если устройство восходящего потока данных налагает bottlneck на сетевой трафик, формирование трафика на межсетевом экране является самым полезным. Хороший пример был бы ASA, который имеет интерфейсы на 100 Мбит с восходящим подключением к Интернету через кабельный модем или T1, который завершается на маршрутизаторе. Формирование трафика позволяет пользователю настраивать максимальную исходящую пропускную способность на интерфейсе (внешний интерфейс, например); когда ссылка менее насыщается, межсетевой экран передает трафик из того интерфейса до указанных пропусканий способность, и затем пытается буферизовать избыточный трафик для передачи позже.

Формирование применено ко всему совокупному трафику это выходы заданный интерфейс; вы не можете принять решение только сформировать определенные трафики.

> **Примечание:** Формирование сделано после шифрования и не обеспечивает приоритизацию на внутреннем пакете или основании туннельной группы для VPN.

Данный пример настраивает межсетевой экран для формирования всего исходящего трафика на внешнем интерфейсе к 2 Мбит/с:

```
ciscoasa(config-pmap)#policy-map qos_outside_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape average 2000000
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit

ciscoasa(config-pmap-c)# service-policy qos_outside_policy interface outside
```

Постановка в очередь с установлением приоритета

С постановкой в очередь с установлением приоритета вы в состоянии разместить определенный класс трафика в Очередь с низкой задержкой (LLQ), которая обработана перед стандартной очередью.

> **Примечание:** При расположении по приоритетам трафика под политикой формирования вы не можете использовать подробные данные внутреннего пакета. Межсетевой экран может только выполнить LLQ, в отличие от маршрутизаторов, которые могут предоставить более сложную организацию очереди и механизмы QoS (Взвешенная организация очередей (WFQ), Взвешенная организация очереди на основе классов (CBWFQ), и так далее).

Иерархическая политика QoS предоставляет механизм для пользователей для определения политики QoS иерархической формой. Например, если пользователи хотят сформировать трафик на интерфейсе и кроме того в имеющем форму интерфейсном трафике, предоставить приоритет организация очереди для Трафика VoIP, то пользователи могут задать политику формирования трафика наверху и политику постановки в очередь с установлением приоритета под политикой формы. Иерархическая поддержка политики QoS ограничена в области. Единственная позволенная опция:

- Формирование трафика в верхнем уровне
- Постановка в очередь с установлением приоритета на следующем уровне

  Примечание: При расположении по приоритетам трафика под политикой формирования вы не можете использовать подробные данные внутреннего пакета. Межсетевой экран может только выполнить LLQ, в отличие от маршрутизаторов, которые могут предоставить более сложную организацию очереди и механизмы QoS (WFQ, CBWFQ, и так далее).

Данный пример использует иерархическую политику QoS для формирования всего исходящего трафика на внешнем интерфейсе к 2 Мбит/с как пример формирования, но это также указывает, что Голосовые пакеты со значением точки кода дифференцированных услуг (DSCP) "ef", а также трафик Secure Shell (SSH), должны получить приоритет.

Создайте очередь с приоритетами на интерфейсе, на котором вы хотите активировать опцию:

```
ciscoasa(config)#priority-queue outsideciscoasa(config-priority-queue)#queue-limit
2048ciscoasa(config-priority-queue)#tx-ring-limit 256
```

Класс к ef match DSCP:

```
   ciscoasa(config)# class-map Voice
ciscoasa(config-cmap)# match dscp ef
ciscoasa(config-cmap)# exit
```

Класс к трафику SSH TCP/22 match port:

```
   ciscoasa(config)# class-map SSH
ciscoasa(config-cmap)# match port tcp eq 22
ciscoasa(config-cmap)# exit
```

Карта политик для применения приоритизации Голоса и трафика SSH:

```
   ciscoasa(config)# policy-map p1_priority
ciscoasa(config-pmap)# class Voice
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class SSH
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

Карта политик для применения формирования ко всему трафику и присоединению расположила по приоритетам трафик SSH и Голос:

```
   ciscoasa(config)# policy-map p1_shape
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape average 2000000
ciscoasa(config-pmap-c)# service-policy p1_priority
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

Наконец подключите политику формирования к интерфейсу, на котором можно сформировать и расположить по приоритетам исходящий трафик:

```
   ciscoasa(config)# service-policy p1_shape interface outside
```

QoS для трафика через VPN-туннель

QoS с IPSec VPN

Согласно битам RFC 2401 Типа обслуживания (ToS) в исходном заголовке IP скопированы к IP - заголовку зашифрованного пакета так, чтобы политики QoS могли быть принуждены после шифрования. Это позволяет битам DSCP/еифференцированных услуг (DiffServ) использоваться для приоритета где угодно в политике QoS.

Применение политик на Туннеле IPSec

Применение политик может также быть сделано для определенных VPN-туннелей. Для выбора туннельной группы, на которой можно определить политику, вы используете команду **<tunnel> туннельной группы соответствия** в своем class-map и команду **адреса назначения (DA) match flow ip**.

```
 class-map tgroup_out
match tunnel-group ipsec-tun
match flow ip destination-address
policy-map qos
class tgroup_out
police output 1000000
```

Контроль соблюдения правил для входящих соединений не работает в это время при использовании **команды tunnel-group соответствия**; посмотрите идентификатор ошибки Cisco CSCth48255 для получения дополнительной информации. При попытке сделать контроль соблюдения правил для входящих соединений с адресом назначения (DA) match flow ip, вы получаете эту ошибку:

```
   police input 10000000
ERROR: Input policing cannot be done on a flow destination basis
```

Контроль соблюдения правил для входящих соединений, кажется, не работает в это время при использовании **туннельной группы соответствия** (идентификатор ошибки Cisco CSCth48255). Если бы контроль соблюдения правил для входящих соединений работает, необходимо было бы использовать class-map без **адреса адреса назначения (DA) match flow ip**.

```
  class-map tgroup_in
match tunnel-group ipsec-tun
policy-map qos
class tgroup_in
police input 1000000
```

При попытке определить политику выходных данных на class-map, который не имеет **адреса назначения (DA) ip соответствия**, вы получаете:

```
   police output 10000000
ERROR: tunnel-group can only be policed on a flow basis
```

Также возможно выполнить QoS на внутренних сведениях о потоках с использованием Списков контроля доступа (ACL), DSCP, и так далее. Из-за ранее упомянутого дефекта, ACL являются способом быть в состоянии сделать контроль соблюдения правил для входящих соединений прямо сейчас.

> **Примечание:** Максимум 64 policy-map может быть настроен на всех типах платформы. Используйте другие карты классов в policy-map для сегментации трафика.

QoS с VPN уровня защищенных сокетов (SSL)

До Версии ASA 9.2 ASA не сохранил биты ToS.

Туннелирование VPN SSL не поддерживается с этой функциональностью. Посмотрите идентификатор ошибки Cisco CSCsl73211 для получения дополнительной информации.

```
   ciscoasa(config)# tunnel-group a1 type webvpn
ciscoasa(config)# tunnel-group a1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# class-map c1
ciscoasa(config-cmap)# match tunnel-group a1
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# policy-map p1
ciscoasa(config-pmap)# class c1
ciscoasa(config-pmap-c)# police output 100000
ERROR: tunnel with WEBVPN attributes doesn't support police!

ciscoasa(config-pmap-c)# no tunnel-group a1 webvpn-attributes
ciscoasa(config)# policy-map p1
ciscoasa(config-pmap)# class c1
ciscoasa(config-pmap-c)# police output 100000
ciscoasa(config-pmap-c)#
```

> **Примечание:** Когда пользователи с телефонным vpn используют клиента AnyConnect и Протокол защиты транспортного уровня для дейтаграмм (DTLS) для шифрования их телефона, установление приоритетов не работает, потому что AnyConnect не сохраняет флаг DSCP в инкапсуляции DTLS. См. запрос на расширение CSCtq43909 для подробных данных.

Обсуждение QoS

Вот некоторые вопросы для рассмотрения о QoS.

- Это применено через Модульную систему политик (MPF) строгой или иерархической формой: Применение политик, Формирование, LLQ.

  Может только влиять на трафик, который уже передают от сетевой интерфейсной платы (NIC) до DP (Путь данных)Бесполезный для борьбы с переполнениями (они происходят слишком рано), пока не применено на смежное устройство

- Применение политик применено на ввод после того, как пакет будет разрешен и на выходные данные перед NIC.

  Прямо после перезаписи Уровня 2 (L2) адрес на выходных данных

- Это формирует исходящую пропускную способность для всего трафика на интерфейсе.

  Полезный с ограниченной соединительной пропускной способностью (такой (GE) as1Gigabit Ethernet ссылка на модем 10 МБ)Не поддерживаемый на

высокоэффективных моделях ASA558x

- Постановка в очередь с установлением приоритета могла бы исчерпать ресурсы наилучший уровень трафика.

  Не поддерживаемый на 10GE взаимодействует на ASA5580 или подчиненных интерфейс VLANИнтерфейсный размер кольца может быть далее настроен для оптимальной производительности

Примеры конфигураций

Пример конфигурации трафика QoS для VoIP на VPN-туннелях

Схема сети

В настоящем документе используется следующая схема сети:

> **Примечание:** Убедитесь, что IP-телефоны и хосты находятся в разных сегментах (подсетях). Это рекомендуется для хорошей организации сети.

Эти конфигурации используются в данном документе:

- Конфигурация QoS на основе DSCP
- QoS на основе DSCP с конфигурацией VPN
- Конфигурация QoS на основе ACL
- QoS на основе ACL с конфигурацией VPN

Конфигурация QoS на основе DSCP

```
!--- Create a class map named Voice.

ciscoasa(config)#class-map Voice


!--- Specifies the packet that matches criteria that
!--- identifies voice packets that have a DSCP value of "ef".


ciscoasa(config-cmap)#match dscp ef


!--- Create a class map named Data.


ciscoasa(config)#class-map Data
```

```
!--- Specifies the packet that matches data traffic to be passed through
!--- IPsec tunnel.


ciscoasa(config-cmap)#match tunnel-group 10.1.2.1
ciscoasa(config-cmap)#match flow ip destination-address


!--- Create a policy to be applied to a set
!--- of voice traffic.


ciscoasa(config-cmap)#policy-map Voicepolicy


!--- Specify the class name created in order to apply
!--- the action to it.


ciscoasa(config-pmap)#class Voice


!--- Strict scheduling priority for the class Voice.

ciscoasa(config-pmap-c)#priority

PIX(config-pmap-c)#class Data


!--- Apply policing to the data traffic.


ciscoasa(config-pmap-c)#police output 200000 37500



!--- Apply the policy defined to the outside interface.


ciscoasa(config-pmap-c)#service-policy Voicepolicy interface outside
ciscoasa(config)#priority-queue outside
ciscoasa(config-priority-queue)#queue-limit 2048
ciscoasa(config-priority-queue)#tx-ring-limit 256
```

> **Примечание:** DSCP-значение "ef" обращается к ускоренной пересылке, которая совпадает с трафиком VOIP RTP.

QoS на основе DSCP с конфигурацией VPN

```
ciscoasa#show running-config
: Saved
:
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0
nameif inside
```

```
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet1
nameif outside
security-level 0
ip address 10.1.4.1 255.255.255.0
!

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- This crypto ACL-permit identifies the
!--- matching traffic flows to be protected via encryption.


access-list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access-list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.1.4.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Configuration for IPsec policies.

crypto ipsec ikev1 transform-set myset esp-3des esp-sha-hmac
crypto map mymap 10 match address 110

!--- Sets the IP address of the remote end.

crypto map mymap 10 set peer 10.1.2.1

!--- Configures IPsec to use the transform-set
!--- "myset" defined earlier in this configuration.

crypto map mymap 10 set ikev1 transform-set myset
crypto map mymap interface outside

!--- Configuration for IKE policies

crypto ikev1 policy 10

!--- Enables the IKE policy configuration (config-isakmp)
!--- command mode, where you can specify the parameters that
!--- are used during an IKE negotiation.


authentication pre-share
encryption 3des
```

```
hash sha
group 2
lifetime 86400

!--- Use this command in order to create and manage the database of
!--- connection-specific records like group name
!--- as 10.1.2.1, IPsec type as L2L, and password as
!--- pre-shared key for IPsec tunnels.

tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes

!--- Specifies the preshared key "cisco123" which should
!--- be identical at both peers.


ikev1 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
queue-limit 2048
tx-ring-limit 256
!
class-map Voice
match dscp ef
class-map Data
match tunnel-group 10.1.2.1
match flow ip destination-address
class-map inspection_default
match default-inspection-traffic

!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
policy-map Voicepolicy
class Voice
priority
class Data
police output 200000 37500
!
service-policy global_policy global
service-policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
```

```
: end
```

Конфигурация QoS на основе ACL

```
!--- Permits inbound H.323 calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq h323

!--- Permits inbound Session Internet Protocol (SIP) calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq sip

!--- Permits inbound Skinny Call Control Protocol (SCCP) calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq 2000

!--- Permits outbound H.323 calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq h323

!--- Permits outbound SIP calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq sip

!--- Permits outbound SCCP calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq 2000

!--- Apply the ACL 100 for the inbound traffic of the outside interface.

ciscoasa(config)#access-group 100 in interface outside


!--- Create a class map named Voice-IN.

ciscoasa(config)#class-map Voice-IN

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 100.

ciscoasa(config-cmap)#match access-list 100


!--- Create a class map named Voice-OUT.

ciscoasa(config-cmap)#class-map Voice-OUT

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 105.
```

```
ciscoasa(config-cmap)#match access-list 105


!--- Create a policy to be applied to a set
!--- of Voice traffic.

ciscoasa(config-cmap)#policy-map Voicepolicy

!--- Specify the class name created in order to apply
!--- the action to it.

ciscoasa(config-pmap)#class Voice-IN
ciscoasa(config-pmap)#class Voice-OUT

!--- Strict scheduling priority for the class Voice.

ciscoasa(config-pmap-c)#priority
ciscoasa(config-pmap-c)#end
ciscoasa#configure terminal
ciscoasa(config)#priority-queue outside


!--- Apply the policy defined to the outside interface.

ciscoasa(config)#service-policy Voicepolicy interface outside
ciscoasa(config)#end
```

QoS на основе ACL с Конфигурацией VPN

```
ciscoasa#show running-config
: Saved
:
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet1
nameif outside
security-level 0
ip address 10.1.4.1 255.255.255.0
!
interface GigabitEthernet2
nameif DMZ1
security-level 95
ip address 10.1.5.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- This crypto ACL-permit identifies the
!--- matching traffic flows to be protected via encryption.


access-list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

```
access-list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0


!--- Permits inbound H.323, SIP and SCCP calls.

access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq h323
access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq sip
access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq 2000


!--- Permit outbound H.323, SIP and SCCP calls.

access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq h323
access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq sip
access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq 2000
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 100 in interface outside

route outside 0.0.0.0 0.0.0.0 10.1.4.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec ikev1 transform-set myset esp-3des esp-sha-hmac
crypto map mymap 10 match address 110
crypto map mymap 10 set peer 10.1.2.1
crypto map mymap 10 set ikev1 transform-set myset
crypto map mymap interface outside
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes
ikev1 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
!
class-map Voice-OUT
match access-list 105
class-map Voice-IN
match access-list 100
!
```

```
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp

!--- Inspection enabled for H.323, H.225 and H.323 RAS protocols.

inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp

!--- Inspection enabled for Skinny protocol.

inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp

!--- Inspection enabled for SIP.

inspect sip
inspect xdmcp
policy-map Voicepolicy
class Voice-IN
class Voice-OUT
priority
!
service-policy global_policy global
service-policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

> **Примечание:** Используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты) для получения дополнительных сведений команды, используемые в этом разделе.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

политика show service-policy

Для просмотра QoS statistics для мониторинга трафика используйте **команду show service-policy** с ключевым словом **политики**:

```
ciscoasa(config)# show ser
ciscoasa(config)# show service-policy police
Interface outside:
Service-policy: POLICY-WEB
Class-map: Class-Policy
Output police Interface outside:
cir 1000000 bps, bc 31250 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: drop
conformed 0 bps, exceed 0 bps
```

приоритет show service-policy

Для просмотра статистики для политики обслуживания, которая внедряет **приоритетную** команду, использует **команду show service-policy** с **ключевым словом priority**:

```
ciscoasa# show service-policy priority
Global policy:
Service-policy: qos_outside_policy
Interface outside:
Service-policy: qos_class_policy
Class-map: voice-traffic
Priority:
Interface outside: aggregate drop 0, aggregate transmit 9383
```

форма show service-policy

```
ciscoasa(config)# show service-policy shape
Interface outside:
Service-policy: qos_outside_policy
Class-map: class-default
shape (average) cir 2000000, bc 16000, be 16000
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

show priority-queue statistics

Чтобы отобразить статистику приоритетной очереди на интерфейсе, введите команду show priority-queue statistics в привилегированном режиме EXEC. Результаты показывают статистику и для наилучшим образом очередь (be) и для LLQ. Данный пример показывает использование **команды show priority-queue statistics** для интерфейса, названного снаружи, и выходные данные команды.

```
ciscoasa# show priority-queue statistics outside

Priority-Queue Statistics interface outside

Queue Type = BE
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length = 0

Queue Type = LLQ
```

```
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length = 0
ciscoasa#
```

В этом статистическом отчете значение элементов строки следующие:

- "Пакеты, Отброшенные", обозначают общее количество пакетов, которые были отброшены в этой очереди.
- "Пакетная Передача" обозначает общее количество пакетов, которые были переданы в этой очереди.
- "Пакеты, Ставившие в очередь", обозначают общее количество пакетов, которые были помещены в очередь в этой очереди.
- "Текущая Длина Q" обозначает текущую глубину этой очереди.
- "Длина Max Q" обозначает максимальную глубину, которая когда-либо происходила в этой очереди.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Устранение неполадок

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

Дополнительные сведения

Вот некоторые дефекты, представленные средством управления трафиком:

Идентификатор ошибки Cisco CSCsq08550	Формирование трафика с постановкой в очередь с установлением приоритета вызывает сбой трафика на ASA
Идентификатор ошибки Cisco CSCsx07862	Формирование трафика с постановкой в очередь с установлением приоритета вызывает задержку пакета и отбрасывания
Идентификатор ошибки Cisco CSCsq07395	Если policy-map был отредактирован, добавление стратегии обслужива формирования отказывает

Часто задаваемые вопросы

Этот раздел предоставляет ответ на один из большинства часто задаваемых вопросов в отношении информации, которая описана в этом документе.

Когда VPN-туннель пересечен, маркировки QoS сохранены?

Да. Маркировки QoS сохранены в туннеле, поскольку они пересекают поставщиков сетевых услуг, если поставщик не разделяет их в пути.

Совет: См. DSCP и раздел Сохранения дифференцированных услуг (DiffServ) *Книги 2 CLI: Руководство Конфигурации интерфейса командой строки Межсетевого экрана Серии Cisco ASA, 9.2* для получения дополнительной информации.

Дополнительные сведения

- Руководство конфигурации интерфейса командой строки Межсетевого экрана Серии Cisco ASA, Качество обслуживания
- Применение политик QoS
- Понимание функций, не поддерживаемых в VPN SSL без клиента
- Настройке функции QoS
- Cisco Systems – техническая поддержка и документация