أمثلة على تكوين جودة الخدمة على جهاز الأمان التكيفي (ASA) من Cisco

المحتويات

المقدمة

يشرح هذا المستند كيفية عمل جودة الخدمة (QoS) على جهاز الأمان القابل للتكيف (ASA) من Cisco، كما يقدم العديد من الأمثلة على كيفية تنفيذها لسيناريوهات مختلفة.

يمكنك تكوين جودة الخدمة على جهاز الأمان لتوفير تحديد المعدل على حركة مرور الشبكة المحددة، لكل من التدفقات الفردية وتدفقات نفق VPN، لضمان حصول جميع حركة المرور على نصيبها العادل من النطاق الترددي المحدود.

تم دمج الميزة مع معرف تصحيح الأخطاء من CSCsk06260 Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بإطار عمل السياسة النمطية (MPF).

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ASA أن يركض صيغة 9.2، غير أن صيغة مبكر يستطيع كنت استعملت أيضا.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

QoS هي ميزة شبكة تسمح لك بإعطاء الأولوية لأنواع معينة من حركة مرور الإنترنت. ومع ترقية مستخدمي الإنترنت لنقاط الوصول من أجهزة المودم إلى إتصالات النطاق الترددي العريض عالية السرعة مثل خط المشترك الرقمي (DSL) والكبل، فإن الاحتمالات تتزايد حتى يصبح بوسع مستخدم واحد في أي وقت أن يستوعب أغلب، إن لم يكن كل، النطاق الترددي المتاح، وبالتالي يتضور المستخدمين الآخرين جوعا. ومن أجل منع أي اتصال مستخدم واحد أو اتصال من موقع إلى موقع من إستهلاك أكثر من حصته العادلة من عرض النطاق الترددي، توفر QoS ميزة تنظيم النطاق الترددي الأقصى التي يمكن لأي مستخدم إستخدامها.

تشير QoS إلى قدرة الشبكة على توفير خدمة أفضل لحركة مرور الشبكة المختارة عبر التقنيات المختلفة للحصول على أفضل الخدمات الشاملة مع عرض نطاق ترددي محدود للتقنيات الأساسية.

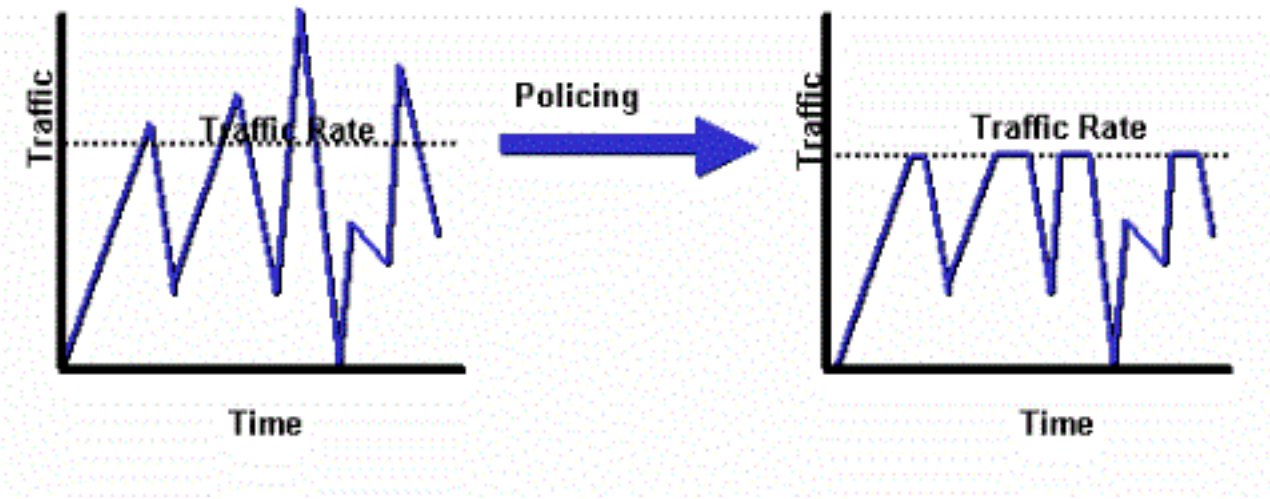
والهدف الرئيسي من جودة الخدمة في جهاز الأمان هو توفير تحديد المعدل لحركة مرور الشبكة المحددة لكل من تدفق البيانات الفردي أو تدفق نفق VPN لضمان حصول جميع حركة المرور على نصيبها العادل من النطاق الترددي المحدود. يمكن تعريف التدفق بعدد من الطرق. في جهاز الأمان، يمكن تطبيق جودة الخدمة على مجموعة من عناوين IP للمصدر والوجهة، ورقم منفذ المصدر والوجهة، ونوع الخدمة (ToS) بايت من رأس IP.

هناك ثلاثة أنواع من جودة الخدمة التي يمكنك تنفيذها على ASA: وضع السياسات وتشكيل قوائم الانتظار وتفضيلها.

وضع سياسات حركة المرور

مع تنظيم الحركة، يتم إسقاط حركة المرور عبر حد محدد. السياسة هي طريقة لضمان عدم تجاوز أي حركة مرور للحد الأقصى للمعدل (في وحدات بت/ثانية) الذي تقوم بتكوينه، والذي يضمن عدم إمكانية حدوث تدفق حركة مرور واحد أو فئة واحدة على المورد بالكامل. عندما تتجاوز حركة المرور الحد الأقصى للسرعة، يقوم ASA بإسقاط حركة المرور الزائدة. كما يحدد عمل الشرطة أكبر دفعة واحدة من المرور المسموح بها.

يوضح هذا المخطط ما تقوم به تنظيم حركة المرور؛ عند وصول معدل حركة المرور إلى الحد الأقصى الذي تم تكوينه، يتم إسقاط حركة المرور الزائدة. والنتيجة هي معدل إخراج يظهر على هيئة سن منشار مع ظهور النشقات والإعاقات.



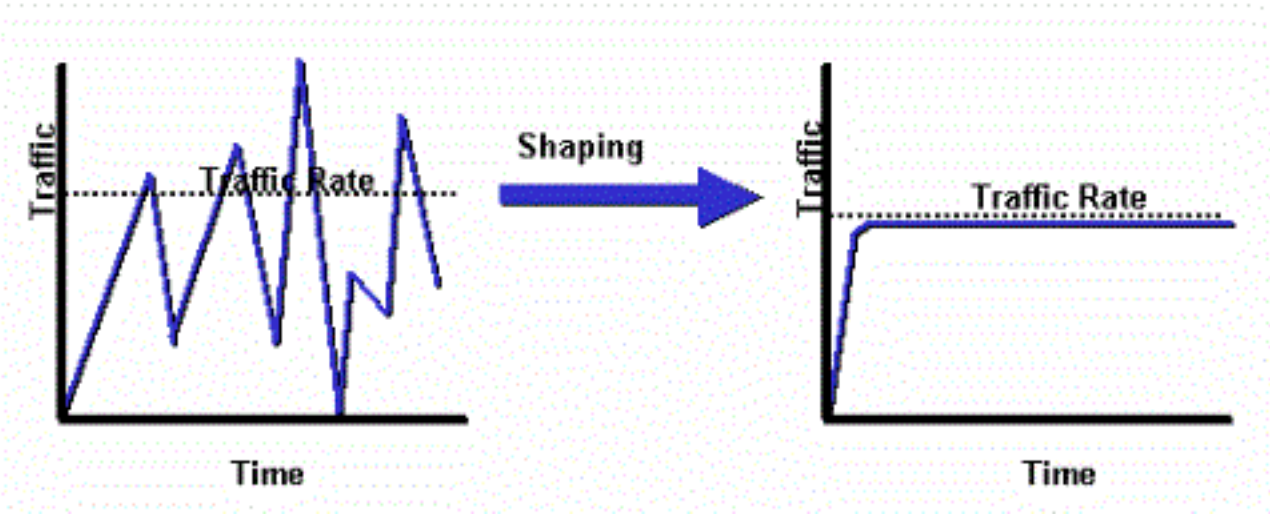
يوضح هذا المثال كيفية كبح النطاق الترددي إلى 1 ميجابت في الثانية لمستخدم معين في الإتجاه الصادر:

```
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
```

تنظيم حركة البيانات

يتم إستخدام تنظيم حركة البيانات لمطابقة سرعات الجهاز والربط، والتي تتحكم في فقدان الحزمة وتأخير المتغيرات وتشبع الارتباط، مما قد يتسبب في الرجفان والتأخير. يسمح تنظيم حركة البيانات على جهاز الأمان للجهاز بالحد من تدفق حركة مرور البيانات. تقوم هذه الآلية بتخزين حركة المرور فوق "حد السرعة" وتحاول إرسال حركة المرور لاحقا. لا يمكن تكوين التكوين لأنواع معينة من حركة المرور. تتضمن حركة المرور ذات الشكل حركة المرور التي تمر عبر الجهاز، وكذلك حركة المرور التي يتم الحصول عليها من الجهاز.

يوضح هذا المخطط ما يقوم به تنظيم حركة المرور؛ حيث يحتفظ بالحزم الزائدة في قائمة انتظار ثم يقوم بجدولة الزيادة للإرسال اللاحق عبر زيادات الوقت. نتيجة تنظيم حركة المرور هي معدل إخراج الحزمة المتجانس.



ملاحظة: يتم دعم تنظيم حركة مرور البيانات فقط على إصدارات ASA 5505 و 5510 و 5520 و 5540 و 5550. لا تدعم نماذج البث المتعدد (مثل X-5500) التشكيل.

مع تنظيم حركة البيانات، يتم وضع حركة المرور التي تتجاوز حدا معينا في قائمة الانتظار (المخزن مؤقتا) وإرسالها أثناء الجداول الزمنية التالية.

يكون تنظيم حركة مرور البيانات على جدار الحماية أكثر فائدة إذا كان جهاز تدفق البيانات من الخادم يفرض عنق زجاجة على حركة مرور الشبكة. قد يكون أحد الأمثلة الجيدة ASA الذي يحتوي على واجهات 100 ميجابت، مع اتصال الخادم بالإنترنت عبر مودم كبل أو T1 الذي ينتهي على موجه. يسمح تنظيم حركة المرور للمستخدم بتكوين الحد الأقصى للمعالجة الصادرة على واجهة (الواجهة الخارجية على سبيل المثال)؛ يرسل جدار الحماية حركة مرور البيانات من تلك الواجهة إلى النطاق الترددي المحدد، ثم يحاول تخزين حركة مرور البيانات الزائدة مؤقتا للإرسال لاحقا عندما يكون الارتباط أقل تشبعا.

يتم تطبيق التشكيل على كل حركة مرور التجميع التي تشغل الواجهة المحددة؛ لا يمكنك إختيار تشكيل تدفقات حركة مرور معينة فقط.

ملاحظة: يتم التشكيل بعد التشفير ولا يسمح بترتيب الأولويات على أساس الحزمة الداخلية أو مجموعة الأنفاق لشبكة VPN.

يقوم هذا المثال بتكوين جدار الحماية لتشكيل حركة مرور البيانات الصادرة على الواجهة الخارجية إلى 2 ميجابت في الثانية:

```
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
```

قائمة الانتظار ذات الأولوية

مع قائمة الانتظار ذات الأولوية، يمكنك وضع فئة معينة من حركة المرور في قائمة انتظار تقليل التأخير (LLQ)، والتي تتم معالجتها قبل قائمة الانتظار القياسية.

ملاحظة: إذا قمت بأولوية حركة المرور ضمن نهج التشكيل، لا يمكنك إستخدام تفاصيل الحزمة الداخلية. يمكن لجدار الحماية تنفيذ LLQ فقط، بخلاف الموجهات التي يمكنها توفير آليات أكثر تطورا لقوائم الانتظار وجودة الخدمة (قوائم الانتظار العادلة والمقدرة (WFQ)، قوائم الانتظار العادلة والمقدرة المعتمدة على الفئة (CBWFQ)، وما إلى ذلك).

يوفر نهج جودة الخدمة الهرمي آلية للمستخدمين لتحديد سياسة جودة الخدمة بطريقة هرمية. على سبيل المثال، إذا كان المستخدمون يرغبون في تشكيل حركة مرور البيانات على واجهة، وعلاوة على ذلك داخل حركة مرور الواجهة التي تم تكوينها، فقم بتوفير قوائم الانتظار ذات الأولوية لحركة مرور بيانات VoIP، ثم يمكن للمستخدمين تحديد سياسة تنظيم حركة مرور البيانات في الجزء العلوي ونهج قائمة الانتظار ذات الأولوية تحت نهج الشكل. دعم سياسة جودة الخدمة الهرمية محدود النطاق. الخيار الوحيد المسموح به هو:

- تنظيم حركة البيانات على المستوى الأعلى
- قائمة الانتظار ذات الأولوية في المستوى التالي

ملاحظة: إذا قمت بأولوية حركة المرور ضمن نهج التشكيل، لا يمكنك إستخدام تفاصيل الحزمة الداخلية. يمكن لجدار الحماية تنفيذ LLQ فقط، بخلاف الموجهات التي يمكن أن توفر آليات أكثر تطورا لقوائم الانتظار وجودة الخدمة (WFQ و CBWFQ وما إلى ذلك).

يستخدم هذا المثال سياسة جودة الخدمة الهرمية من أجل تشكيل جميع حركة المرور الصادرة على الواجهة الخارجية إلى 2 ميجابت في الثانية مثل مثال التكوين، ولكنه يحدد أيضا أن الحزم الصوتية ذات قيمة "ef" لنقطة كود الخدمات المميزة (DSCP)، بالإضافة إلى حركة مرور طبقة الأمان (SSH)، يجب أن تتلقى الأولوية.

قم بإنشاء قائمة الانتظار ذات الأولوية على الواجهة التي تريد تمكين الميزة عليها:

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

فئة تطابق DSCP EF:

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

فئة لمطابقة حركة مرور المنفذ SSH TCP/22:

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

خريطة سياسة لتطبيق ترتيب أولويات حركة مرور البيانات عبر الصوت و 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
```

خريطة نهج لتطبيق التشكيل على جميع حركة المرور وإرفاق حركة مرور الصوت و SSH ذات الأولوية:

```
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
```

أخيرا، قم بإرفاق سياسة التكوين بالقارن الذي يتم عليه تكوين حركة المرور الصادرة وترتيبها حسب الأولوية:

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

جودة الخدمة لحركة المرور عبر نفق VPN

جودة الخدمة مع VPN IPsec

طبقا لنوع الخدمة (ToS) RFC 2401، يتم نسخ وحدات بت في رأس IP الأصلي إلى رأس IP الخاص بالحزمة المشفرة حتي يمكن فرض سياسات جودة الخدمة بعد التشفير. وهذا يسمح باستخدام وحدات بت DSCP/DiffServ للأولوية في أي مكان في سياسة جودة الخدمة.

وضع السياسات على نفق IPsec

كما يمكن إجراء عمليات الشرطة لأنفاق الشبكات الخاصة الظاهرية (VPN). لتحديد مجموعة نفق يتم التحكم فيها، يمكنك إستخدام الأمر **match tunnel-group <tunnel>** في class-map لديك وأمر **match flow ip destination address**.

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

لا يعمل تنظيم الإدخال في هذا الوقت عندما تستخدم الأمر **match tunnel-group**؛ راجع معرف تصحيح الأخطاء CSCth48255 من Cisco للحصول على مزيد من المعلومات. إذا حاولت إجراء تنظيم الإدخال باستخدام عنوان وجهة IP لتدفق المطابقة، فأنت تتلقى هذا الخطأ:

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

لا يبدو أن تنظيم الإدخال يعمل في هذا الوقت عندما تستخدم **match tunnel-group** (معرف تصحيح الأخطاء من Cisco CSCth48255). إذا عمل تنظيم الإدخال، فستحتاج إلى إستخدام خريطة الفئة دون **عنوان عنوان وجهة IP** الخاص **بتدفق المطابقة**.

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

إذا حاولت تنظيم الإخراج على خريطة فئة لا تحتوي على **عنوان وجهة IP المطابق**، فأنت تستلم:

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

كما يمكن تنفيذ جودة الخدمة على معلومات التدفق الداخلي باستخدام قوائم التحكم في الوصول (ACLs) و DSCP

وما إلى ذلك. نظرا للخطأ المشار إليه سابقا، تعد قوائم التحكم في الوصول (ACL) الطريقة التي يمكن بها إجراء تنظيم الإدخال في الوقت الحالي.

ملاحظة: يمكن تكوين 64 خريطة سياسة كحد أقصى على جميع أنواع الأنظمة الأساسية. أستخدم مخططات فئة مختلفة ضمن خرائط السياسة لتقسيم حركة المرور.

جودة الخدمة باستخدام طبقة مآخذ التوصيل الآمنة (SSL) VPN

حتى الإصدار 9.2 من ASA، لم يحتفظ ASA بوحدات بت ToS.

لا يتم دعم اتصال SSL VPN النفقي باستخدام هذه الوظيفة. راجع معرف تصحيح الأخطاء من Cisco CSCsl73211 للحصول على مزيد من المعلومات.

```
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
```

ملاحظة: عندما يستخدم المستخدمون الذين لديهم شبكة Phone-VPN أمان طبقة نقل AnyConnect DTLS)) لتشفير هواتفهم، لا يعمل ترتيب الأولويات لأن AnyConnect لا يحتفظ بعلامة DSCP في تضمين DTLS. راجع طلب التحسين CSCtq43909 للحصول على تفاصيل.

اعتبارات جودة الخدمة

فيما يلي بعض النقاط التي يتعين أخذها بعين الاعتبار حول جودة الخدمة.

- ويتم تطبيقه من خلال إطار السياسات النمطية (MPF) بأسلوب صارم أو هرمي: وضع السياسات، وتشكيل الأشكال، ورسم الخرائط.

  يستطيع فقط أثرت حركة المرور التي تم تمريرها بالفعل من بطاقة واجهة الشبكة (NIC) إلى DP (مسار البيانات)لا فائدة من مكافحة التجاوزات (تحدث مبكرا جدا) ما لم تطبق على جهاز مجاور

- يتم تطبيق التنظيم على الإدخال بعد السماح للحزمة وعلى الإخراج قبل بطاقة واجهة الشبكة (NIC).

  مباشرة بعد أن تقوم بإعادة كتابة عنوان طبقة 2 (L2) على المخرج

  - إنه يشكل عرض النطاق الترددي الصادر لجميع حركة المرور على الواجهة.

مفيد مع عرض نطاق ترددي محدود للوصلات (مثل إرتباط إيثرنت 1 جيجابت بمودم 10 ميجابت)لا يتم دعمها في طرز ASA558X عالية الأداء

- قد تؤدي قائمة الانتظار ذات الأولوية إلى تجويع حركة مرور أفضل الجهود.

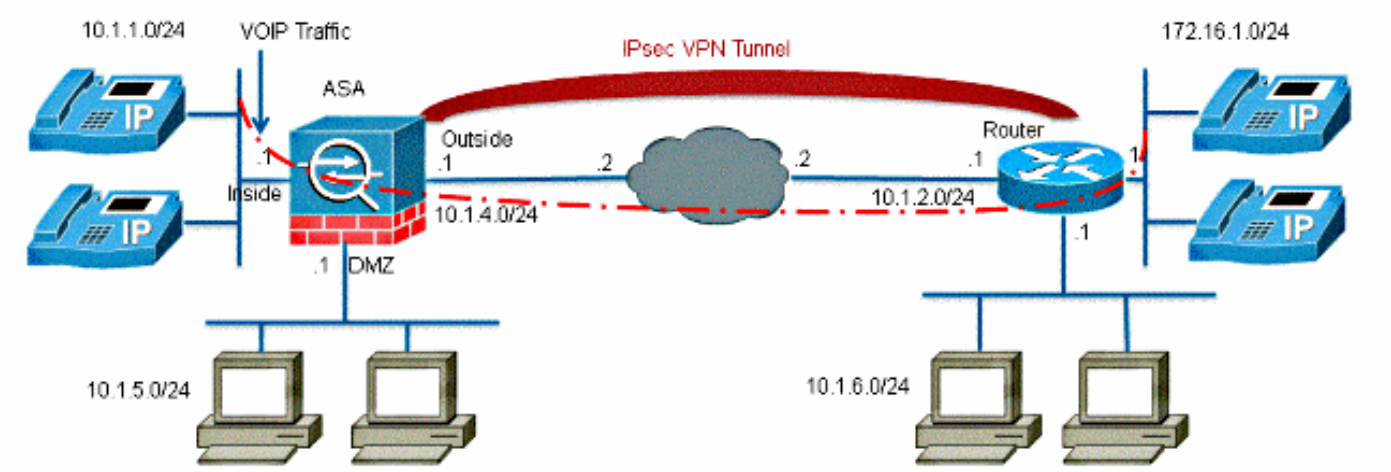
لا يساند على 10GE قارن على ASA5580 أو VLAN subinterfacesيمكن ضبط حجم حلقة الواجهة بشكل إضافي للحصول على الأداء الأمثل

أمثلة التكوين

مثال تكوين جودة الخدمة لحركة مرور VoIP على أنفاق VPN

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: تأكد من وضع هواتف IP والأجهزة المضيفة في مقاطع مختلفة (الشبكات الفرعية). يوصى بذلك لتصميم شبكة جيد.

يستخدم هذا المستند التكوينات التالية:

- تكوين جودة الخدمة استنادا إلى DSCP
- جودة الخدمة استنادا إلى DSCP مع تكوين VPN
- تكوين جودة الخدمة استنادا إلى قائمة التحكم في الوصول (ACL)
- جودة الخدمة استنادا إلى قائمة التحكم في الوصول (ACL) مع تكوين VPN

تكوين جودة الخدمة استنادا إلى 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
```

ملاحظة: تشير قيمة DSCP الخاصة ب "ef" إلى إعادة التوجيه السريع التي تطابق حركة مرور VoIP-RTP.

جودة الخدمة استنادا إلى DSCP مع تكوين 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 :
```

تكوين جودة الخدمة استنادا إلى قائمة التحكم في الوصول (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
                                                        eq h323 255.255.255.0

                                        .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
                                                         eq sip 255.255.255.0

                                    .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
                                                        eq 2000 255.255.255.0

                                                   .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
                                                        eq h323 255.255.255.0

                                                    .Permits outbound SIP calls ---!

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

                                                  .Permits outbound SCCP calls ---!

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

     .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
```

جودة الخدمة استنادا إلى قائمة التحكم في الوصول (ACL) مع تكوين 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
                                                    eq h323 255.255.255.0
              access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
                                                     eq sip 255.255.255.0
              access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
                                                    eq 2000 255.255.255.0


                                     .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
                                                    eq h323 255.255.255.0
              access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
                                                     eq sip 255.255.255.0
              access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
                                                    eq 2000 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
                                             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 :
```

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

شرطة إظهار سياسة الخدمة

لعرض إحصائيات جودة الخدمة لتنظيم حركة المرور، أستخدم الأمر **show service-policy** مع الكلمة الأساسية **police**:

```
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
```

إظهار أولوية سياسة الخدمة

لعرض إحصائيات سياسات الخدمة التي تنفذ الأمر **priority** ، أستخدم الأمر **show service-policy** مع الكلمة الأساسية **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
```

إظهار شكل نهج الخدمة

```
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)
```

إظهار إحصائيات قائمة الانتظار ذات الأولوية

لعرض إحصائيات قائمة الانتظار ذات الأولوية لواجهة، أستخدم الأمر **show priority-queue statistics** في وضع EXEC ذي الامتيازات. تظهر النتائج إحصائيات كل من قائمة انتظار أفضل جهد (BE) وقائمة انتظار LLQ. يوضح هذا

المثال إستخدام الأمر **show priority-queue statistics** للواجهة المسماة خارج، وإخراج الأمر.

```
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
```

وفي هذا التقرير الإحصائي، يكون معنى البنود كما يلي:

- يشير "الحزم التي تم إسقاطها" إلى العدد الإجمالي للحزم التي تم إسقاطها في قائمة الانتظار هذه.
- يشير "إرسال الحزم" إلى العدد الإجمالي للحزم التي تم إرسالها في قائمة الانتظار هذه.
- يشير "وضع الحزم في قائمة الانتظار" إلى العدد الإجمالي للحزم التي تم وضعها في قائمة الانتظار هذه.
- يشير "طول Q الحالي" إلى العمق الحالي لقائمة الانتظار هذه.
- يشير "Max Q Length" إلى الحد الأقصى للعمق الذي حدث على الإطلاق في قائمة الانتظار هذه.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات إضافية

فيما يلي بعض الأخطاء المقدمة من ميزة تنظيم حركة المرور:

معرف تصحيح الأخطاء من Cisco CSCsq08550	يتسبب تنظيم حركة المرور باس قوائم الانتظار ذات الأولوية في حركة مرور البيانات على ASA
معرف تصحيح الأخطاء من Cisco CSCsx07862	يتسبب تنظيم حركة البيانات باس قوائم الانتظار ذات الأولوية في الحزم وإسقاطها
معرف تصحيح الأخطاء من Cisco CSCsq07395	تؤدي إضافة تشكيل نهج الخدم الفشل في حالة تحرير مخطط السياسة

أسئلة شائعة

يقدم هذا القسم إجابة على أحد أكثر الأسئلة شيوعا فيما يتعلق بالمعلومات الموضحة في هذا المستند.

هل يتم الاحتفاظ بعلامات جودة الخدمة عند إجتياز نفق VPN؟

نعم. يتم الاحتفاظ بعلامات جودة الخدمة في النفق أثناء عبورها لشبكات الموفر إذا لم يقم الموفر بتجريدها أثناء النقل.

تلميح: راجع قسم حفظ DSCP و DiffServ من *دليل تكوين واجهة سطر الأوامر (CLI) رقم 2: جدار حماية Cisco ASA Series، الإصدار 9.2* للحصول على مزيد من التفاصيل.

معلومات ذات صلة

- دليل تكوين واجهة سطر الأوامر لجدار الحماية Cisco ASA Series، جودة الخدمة
- تطبيق سياسات جودة الخدمة
- فهم الميزات غير المدعومة في SSL VPN بدون عملاء
- تكوين جودة الخدمة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).