دليل أفضل الممارسات للتحقق من القفزة وعناصر التحكم في الوجهة الثابتة

المحتويات

المقدمة
التحقق من القفزة
تكوين ESA
إستخدام جدول التحكم في الوجهة
إضافة مجال جديد إلى جدول التحكم في الوجهة
نشر المصادقة المستندة إلى SMTP DNS للكيانات المسماة (DANE)
تكوين ESA

المقدمة

يمكن أن يؤدي تسليم البريد الإلكتروني بكميات كبيرة دون التحكم فيه إلى تجاوز مجالات المستلمين. يمنحك AsyncOS التحكم الكامل في تسليم الرسائل من خلال تحديد عدد الاتصالات التي ستفتحها خدمة "أمان البريد الإلكتروني" أو عدد الرسائل التي سيتم إرسالها إلى كل مجال وجهة.

في هذا المستند، سنغطي ما يلي:

1. إعداد التحقق من الارتداد لحماية مؤسستك من هجمات الارتداد
2. إستخدام جدول التحكم في الوجهة لممارسة سياسات حسن الجوار
3. نشر المصادقة المستندة إلى SMTP DNS للكيانات المسماة (DANE) لتوفير تسليم آمن للرسائل

التحقق من القفزة

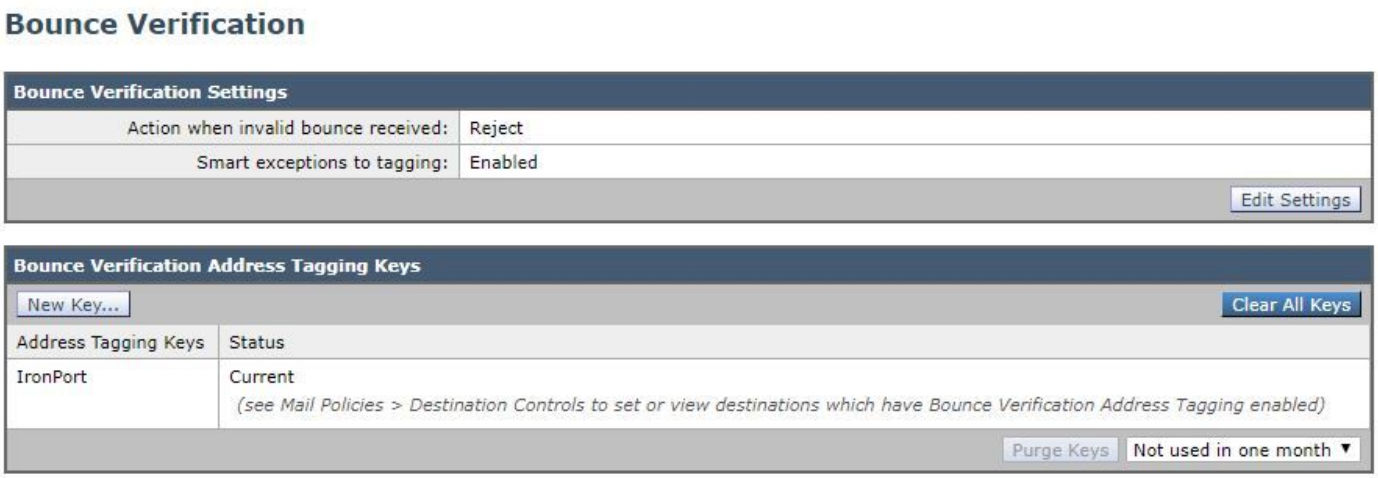
يعتبر تمكين التحقق من الارتداد طريقة جيدة جدا لمكافحة هجمات التشتت/الارتداد. المفهوم وراء التحقق من الارتداد بسيط. أولا، قم بوضع علامة على الرسائل التي تركت وكالة الفضاء الأوروبية. ابحث عن تلك العلامة على أي رسائل ترميز، إذا كانت العلامة موجودة، فهذا يعني أن هذه هي قفزة من رسالة نشأت في بيئتك. إذا كانت العلامة مفقودة، القفزة مخادعة ويمكن رفضها أو إسقاطها.

على سبيل المثال، بريد من: joe@example.com يصبح بريد من: prvs=joe=123ABCDEFG@example.com. السلسلة 123 في المثال هي القفزة علامة التحقق من الصحة التي تتم إضافتها إلى مرسل المظروف عند إرسالها بواسطة جهاز ESA لديك. إذا الرسالة ترتد، سيتضمن عنوان مستلم المظروف في الرسالة المرصوصة علامة التحقق من الارتداد، والتي تمكن الإيسا من معرفة أنها مشروعة رسالة.

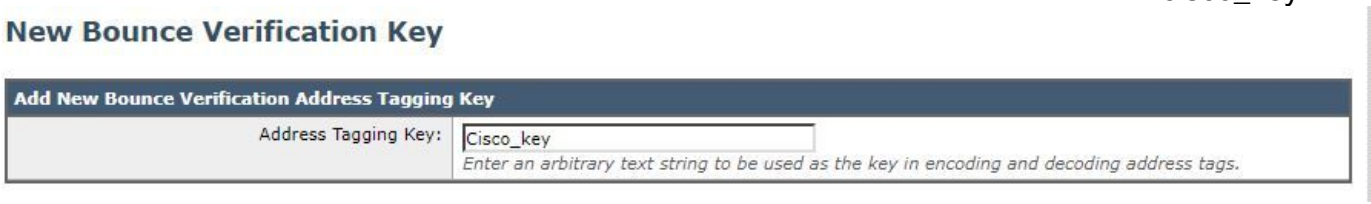
يمكنك تمكين أو تعطيل علامات التحقق من الارتداد على مستوى النظام كافتراضي. يمكنك ذلك قم أيضا بتمكين أو تعطيل تمييز التحقق من الارتداد للمجالات المحددة. في معظم لعمليات النشر، يتم تمكينها بشكل افتراضي لجميع المجالات.

تكوين ESA

- انتقل إلى **سياسات البريد > التحقق من الارتداد** وانقر **مفتاح جديد**



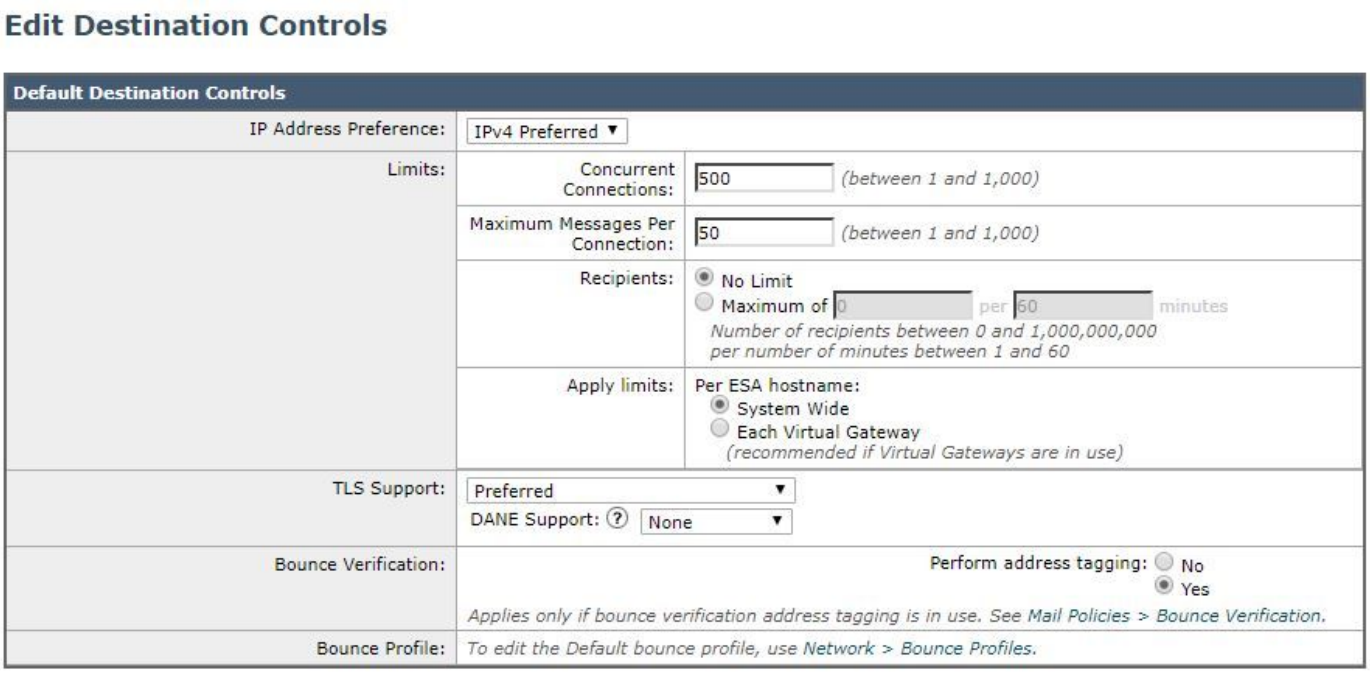
- قم بإدخال أي نص عشوائي ليتم إستخدامه كمفتاح في تشفير وفك علامات التمييز للعنوان. على سبيل المثال، "cisco_key".



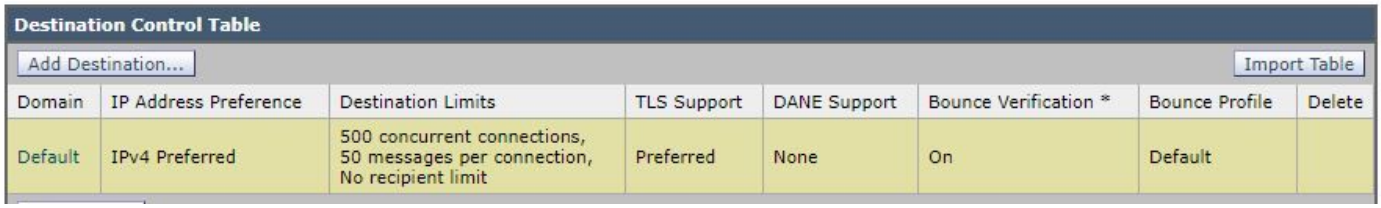
- انقر فوق **إرسال** والتحقق من صحة المفتاح الجديد لتمييز العنوان

الآن، دعونا نمكن التحقق من الارتداد للمجال "الافتراضي" الخاص بنا:

- انتقل إلى **سياسات البريد > عناصر التحكم في الوجهة** وانقر على **الافتراضي**.
- تكوين **التحقق من الارتداد: تنفيذ تمييز العنوان: نعم**



- انقر فوق **إرسال** وإجراء **تغييرات.** لاحظ أن التحقق من الارتداد قيد التشغيل الآن للمجال الافتراضي.



إستخدام جدول التحكم في الوجهة

يمكن أن يؤدي تسليم البريد الإلكتروني غير المتحكم به إلى تجاوز مجالات المستلمين. تعطيك الإيسا كامل التحكم تسليم الرسالة من خلال تحديد عدد الاتصالات التي سيفتحها الجهاز أو عدد الرسائل التي سيقوم الجهاز بإرسالها إلى كل مجال وجهة. يوفر جدول عناصر تحكم الوجهة إعدادات لمعدلات الاتصال والرسائل عندما يكون ESA التسليم إلى وجهات بعيدة. كما يوفر إعدادات لمحاولة أو فرض إستخدام TLS إلى هذه الوجهات. يتم تكوين ESA بتكوين افتراضي لجدول التحكم في الوجهة.

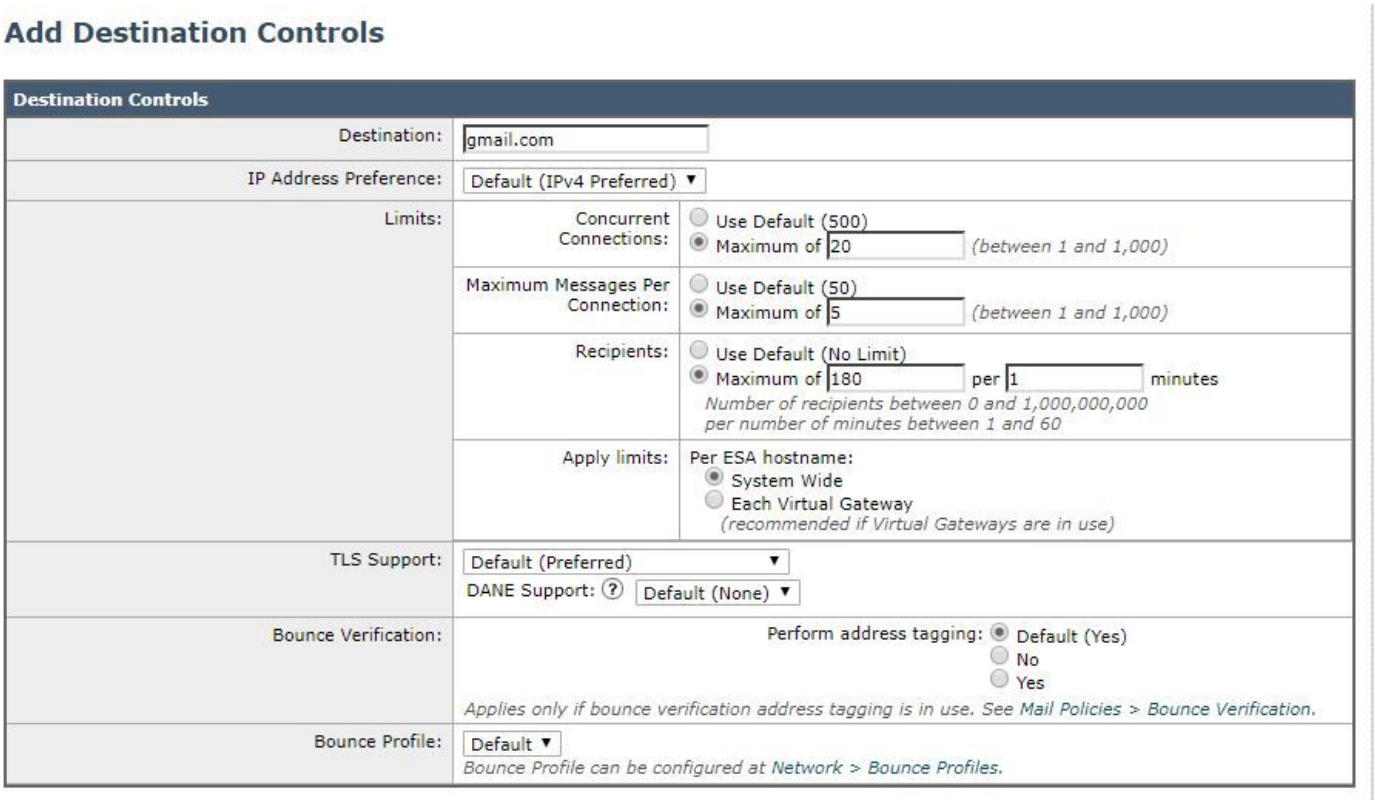
ما سنغطيه في هذا المستند هو كيف يمكننا إدارة التحكم وتكوينه على الوجهات التي يكون فيها الإعداد الافتراضي غير مناسب. على سبيل المثال، لدى Google مجموعة من قواعد الاستلام التي يجب على مستخدمي Gmail اتباعها أو أنهم يجازفون بإرسال رمز إستجابة SMTP 4XX ورسالة تقول أنك ترسلها بسرعة كبيرة أو أن علبة بريد المستلم قد تجاوزت حد التخزين. سنضيف مجال Gmail إلى جدول التحكم الوجهة الذي يحدد مقدار الرسالة المرسلة إلى مستلم Gmail أدناه.

إضافة مجال جديد إلى جدول التحكم في الوجهة

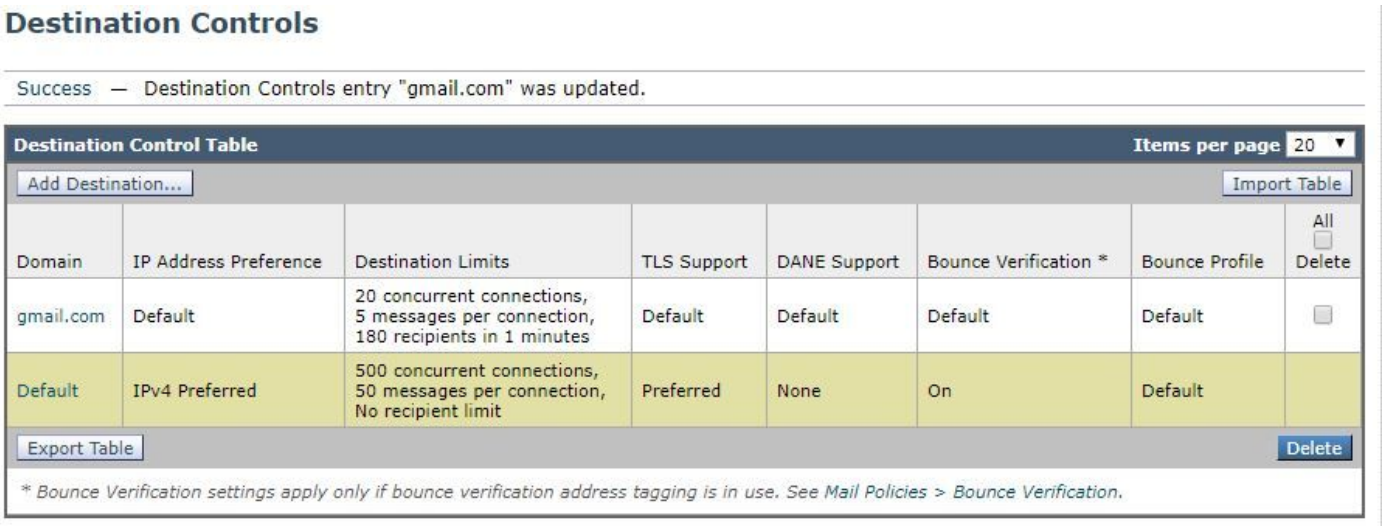
كما ذكرنا سابقا، فإن غوغل تضع قيودا على المرسلين الذين يرسلون إلى جي ميل. يمكن التحقق من حدود الاستلام من خلال النظر إلى قيود مرسل Gmail المنشورة هنا - https://support.google.com/a/answer/1366776?hl=en

لنقم بإعداد مجال الوجهة ل Gmail كمثال على السياسات المجاورة الجيدة.

- انتقل إلى **سياسات البريد > عناصر التحكم في الوجهة** وانقر على **إضافة وجهة** وقم بإنشاء ملف تعريف جديد باستخدام المعلمات التالية: **الوجهة: gmail.comتفضيل عنوان IP: IPv4 المفضلالاتصالات المتزامنة: بحد أقصى 20الحد الأقصى للرسائل لكل اتصال: 5المستلمين: الحد الأقصى 180 لكل دقيقةالتحقق من الارتداد: تنفيذ تمييز العنوان: الافتراضي (نعم)**



• انقر فوق **إرسال** وإجراء **تغييرات.** هذا ما يبدو عليه جدول التحكم في الوجهة بعد إضافة المجال.
لاحظ تغييرات "حدود الوجهة" و "التحقق من الارتداد" في الصورة أدناه:



نشر المصادقة المستندة إلى SMTP DNS للكيانات المسماة (DANE)

تقوم المصادقة المستندة إلى SMTP DNS لبروتوكول الكيانات المسماة (DANE) بالتحقق من صحة شهادات X.509 الخاصة بك باستخدام أسماء DNS باستخدام ملحق أمان نظام اسم المجال (DNSSEC) المكون على خادم DNS وسجل موارد DNS، المعروف أيضا باسم سجل TLSA.

تتم إضافة سجل TLSA في الشهادة التي تحتوي على تفاصيل حول المرجع المصدق (CA) أو شهادة الكيان النهائي أو رابط الثقة المستخدم لاسم DNS الموضح في RFC 6698. توفر ملحقات أمان نظام اسم المجال (DNSSEC) أمانا إضافيا على DNS من خلال معالجة نقاط الضعف في أمان DNS. يضمن DNSSEC الذي يستخدم مفاتيح التشفير والتواقيع الرقمية أن بيانات البحث صحيحة ويتصل بالخوادم الشرعية.

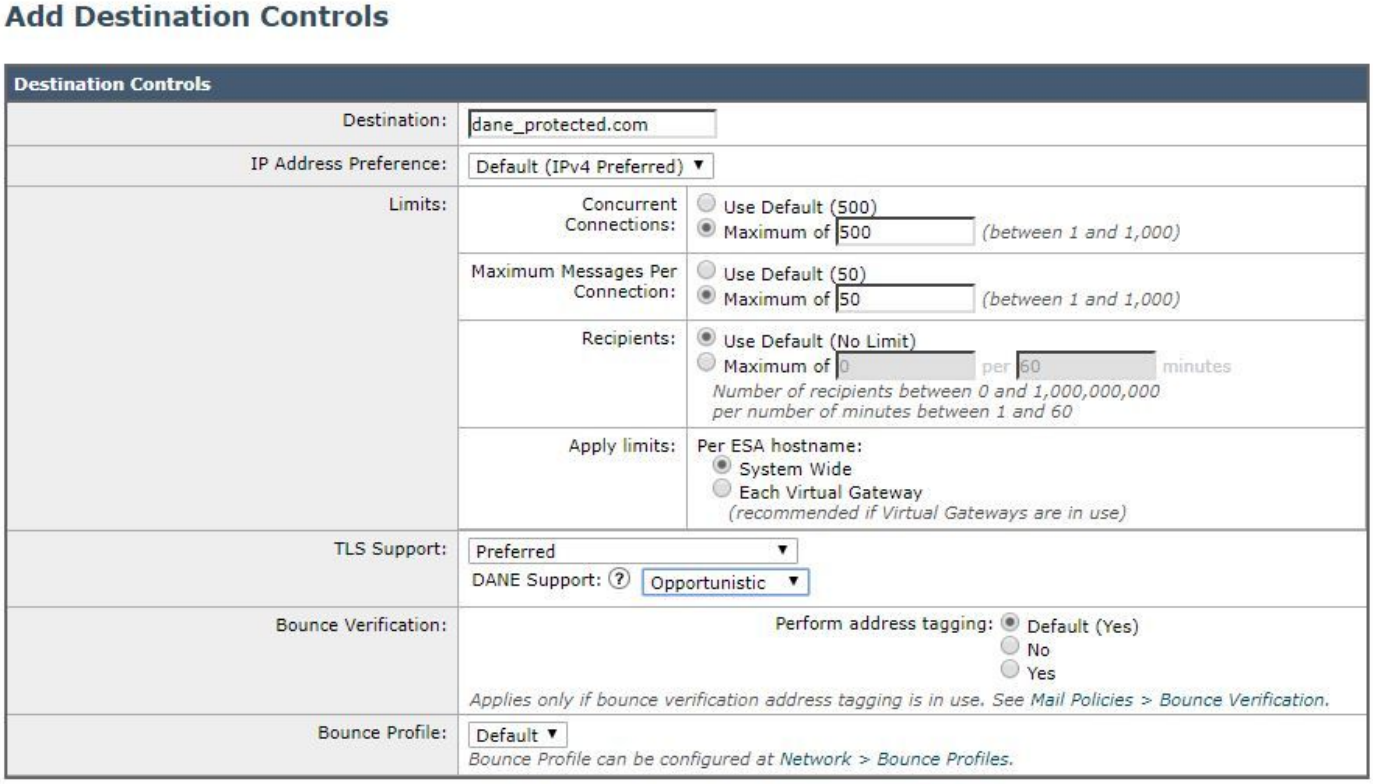
فيما يلي فوائد إستخدام SMTP DANE لاتصالات TLS الصادرة:

- يوفر التسليم الآمن للرسائل من خلال منع هجمات الرجوع إلى الوضع السابق (MITM) والتنصت وهجمات تسميم ذاكرة التخزين المؤقت ل DNS.
- يوفر أصالة شهادات TLS ومعلومات DNS، عند التأمين بواسطة DNSSEC.

تكوين ESA

قبل البدء في إعداد DANE على ESA، الرجاء التأكد من أن مرسل المغلف وسجل مورد TLSA تم التحقق من DNSSEC وأن مجال التلقي محمي DANE. يمكنك القيام بذلك على ESA باستخدام أمر **daneverify** CLI.

- انتقل إلى **سياسات البريد > عناصر التحكم في الوجهة** وانقر على **إضافة وجهة** وقم بإنشاء ملف تعريف جديد باستخدام المعلمات التالية: **الوجهة:** dane_protected.com**دعم TLS:** مفضل**دعم DANE:** انتهازي



- انقر فوق **إرسال** وإجراء **تغييرات**.

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).