ما هو إعداد "خلف جدار الحماية" في TMS ولماذا تستخدمه بدلا من "إمكانية الوصول إلى الإنترنت العامة"؟

المحتويات

المقدمة

تتعلق هذه المقالة بمجموعة إدارة نظام TelePresence من Cisco.

س. ما هو إعداد "خلف جدار الحماية" في TMS ولماذا تستخدمه بدلا من "يمكن الوصول إليه على الإنترنت العام"؟

أ. للعثور على هذا الإعداد:

1. انتقل إلى **Systems > Navigator** وحدد نقطة النهاية/النظام الذي تريد تكوينه.
2. انقر على علامة تبويب **التوصيل**.
3. يحتوي إعداد اتصال النظام على أربعة خيارات:لا يمكن الوصول إليهإمكانية الوصول على الشبكة المحلية (LAN)يمكن الوصول إليه على الإنترنت العامخلف جدار الحماية

عند تكوين نظام كقابل للوصول إليه على الإنترنت العامة، تتوقع TMS إمكانية الاتصال به دون حظره بواسطة جدران الحماية أو موجهات NAT.

يتيح خيار جدار الحماية الخلفي ل TMS العمل باستخدام الأجهزة المدعومة التي لا يمكنها الاتصال بها مباشرة، مثل تلك الموجودة خلف جدار حماية أو موجه nat كما هو شائع في مراكز HOME/SOHO.

لا تزال الأنظمة التي تم تكوينها خلف جدار الحماية ترسل ملاحظات إلى TMS حول النشاط مثل الأنظمة الأخرى، كما تقوم باستطلاع TMS لاستطلاع أي أوامر معلقة ليتم تنفيذها. ولهذا السبب، لا تسري التغييرات التي يتم إجراؤها على الأنظمة المعينة على "جدار الحماية الخلفي" على الفور، ولكن سيتم تطبيقها في المرة التالية التي يتصل فيها النظام ب TMS، وهي كل 15 دقيقة.

معلومات ذات صلة

- 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).