Oakley و Red ISAKMP تامولعم

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات فنية
حول ISAKMP
حول أوكلي
حول IPSec
برامج ISAKMP
تنفيذ أنظمة Cisco
تنفيذ وزارة الدفاع الأمريكية
معلومات ذات صلة

المقدمة

يوفر هذا المستند معلومات حول بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) وبروتوكول تحديد مفتاح Oakley. تعد هذه البروتوكولات منافس رئيسي لإدارة مفتاح الإنترنت التي يتم النظر فيها من قبل مجموعة العمل IPSec التابعة لفرقة عمل هندسة الإنترنت (IETF).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات فنية

حول ISAKMP

يوفر ISAKMP إطار عمل لإدارة مفتاح الإنترنت ويوفر دعم البروتوكول المحدد للتفاوض على سمات الأمان. لا يقوم هذا الخيار وحده بإنشاء مفاتيح جلسات العمل. ومع ذلك، يمكن إستخدامه مع العديد من بروتوكولات الإنشاء الرئيسية للجلسة، مثل Oakley، لتوفير حل كامل لإدارة مفاتيح الإنترنت. تتوفر مواصفات ISAKMP أيضا في PostScript.

حول أوكلي

يستخدم بروتوكول Oakley تقنية Diffie-Hellman المختلطة لإنشاء مفاتيح الجلسة على مضيفات وموجهات الإنترنت. يوفر أوكلي خاصية الأمان الهامة لسرية التقدم الكامل (PFS) ويقوم على تقنيات التشفير التي نجت من التدقيق العام الكبير. يمكن إستخدام Oakley بنفسها، إذا لم تكن هناك حاجة إلى تفاوض السمة، أو يمكن إستخدام Oakley بالاشتراك مع ISAKMP. وعندما يستخدم ISAKMP مع أوكلي، لا يمكن توفير الضمان الأساسي.

تم دمج بروتوكولي ISAKMP و Oakley في بروتوكول هجين. يستخدم حل ISAKMP مع Oakley إطار ISAKMP لدعم مجموعة فرعية من أوضاع تبادل المفاتيح في Oakley. يوفر بروتوكول تبادل المفاتيح الجديد PFS الاختياري، تفاوض سمة اقتران الأمان الكامل، وأساليب المصادقة التي توفر كلا من الرفض وعدم الإنكار. يمكن إستخدام عمليات تنفيذ هذا البروتوكول لإنشاء شبكات VPN والسماح أيضا للمستخدمين من المواقع البعيدة (الذين قد يكون لديهم عنوان IP مخصص ديناميكيا) بالوصول إلى شبكة آمنة.

حول IPSec

ويقوم فريق العمل IPSec التابع لفرقة العمل بتطوير معايير لآليات الأمان من طبقة IP لكل من بروتوكولي IPv4 و IPv6. كما تقوم المجموعة بتطوير بروتوكولات إدارة رئيسية عامة لاستخدامها على الإنترنت. للحصول على مزيد من المعلومات، ارجع إلى نظرة عامة على أمان IP وتشفيره.

برامج ISAKMP

تنفيذ أنظمة Cisco

يتوفر برنامج Isakmp Daemon الخاص بالأنظمة من Cisco مجانا لأي إستخدام تجاري أو غير تجاري للمساعدة في تطوير ISAKMP كحل قياسي لإدارة مفاتيح الإنترنت.

يتوفر برنامج Cisco ISAKMP داخل الولايات المتحدة وكندا من خلال نموذج تنزيل عبر الويب من معهد ماساتشوستس للتقنية (MIT). بسبب قوانين مراقبة الصادرات في الولايات المتحدة، لا تستطيع Cisco توزيع هذا البرنامج خارج الولايات المتحدة وكندا.

يستخدم برنامج Cisco ISAKMP الأساسي واجهة برنامج إدارة مفتاح (API) PF_KEY للتسجيل مع نواة نظام التشغيل (التي قامت بتنفيذ واجهة برمجة التطبيقات هذه) والبنية الأساسية لإدارة المفاتيح المحيطة. يتم إدراج اقترانات الأمان التي تم التفاوض عليها بواسطة برنامج ISAKMP Daemon في المحرك الرئيسي ل Kernel. وتكون بعد ذلك متوفرة للاستخدام بواسطة آليات أمان IPSec القياسية للنظام (رأس المصادقة [AH] وحمولة الأمان المضمنة [ESP]).

ويتضمن توزيع برامج IPv6+IPSec في مختبر البحوث البحرية الأمريكي (NRL) القابل للتوزيع بحرية للأنظمة المشتقة من BSD-4.4 (بما في ذلك شركة [Berkeley Software Design، Inc. BSDI] و NetBSD) تنفيذ بروتوكولات IPv6 و IPSec لبروتوكول IPv6 و IPSec لبروتوكول IPv4 وواجهة PF_KEY. ويتوفر برنامج NRL في الولايات المتحدة وكندا من خلال نموذج تنزيل على الويب من MIT. وخارج الولايات المتحدة وكندا، تتوفر برامج NRL من خلال FTP من ftp://ftp.ripe.net/ipv6/nrl .

يستند برنامج Cisco إلى ISAKMP الإصدار 5 ويستخدم مميزات من بروتوكول تحديد مفتاح Oakley الإصدار 1.

وقد وضعت في الموقع isakmp-oakley@cisco.com قائمة بريدية للمشاكل، وإصلاح الأخطاء، والتغييرات المتعلقة بالإبلاغ، والمناقشة العامة بشأن ISAKMP و Oakley. للانضمام إلى هذه القائمة، قم بإرسال طلب بريد إلكتروني يتضمن نص رسالة **اشتراك isakmp-oakley** إلى: majordomo@cisco.com.

تنفيذ وزارة الدفاع الأمريكية

وقد جعل مكتب بحوث أمن المعلومات التابع لوزارة الدفاع الأمريكية تنفيذ النموذج الأولي ل ISAKMP متاحا مجانا للتوزيع داخل الولايات المتحدة. تتوفر واجهة مستندة إلى الويب لتنزيل البرنامج. لا يتضمن هذا التطبيق أي إمكانيات تبادل مفاتيح جلسة العمل، ولكنه يتضمن ميزات ISAKMP الكاملة.

معلومات ذات صلة

- صفحة دعم IPSec
- الدعم الفني - 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).