



شبکه‌های خصوصی مجازی

VPNs

مؤلفان:

داریوش زاهدمنش

مهران طریحی

ناشر: کتاب پهنجی، کاتبی، و دانشگاهی، تهران



سرشناسه	زاهدمنش، داریوش، ۱۳۶۱
عنوان و نام پدیدآور	شبکه‌های خصوصی مجازی (رهیافتی تئوری و عملی) / داریوش زاهدمنش، مهران طریحی.
مشخصات نشر	تهران: نص، ۱۳۸۹.
مشخصات ظاهری	ص: ۲۴۸؛ مصور، جدول، نمودار + یک لوح فشرده.
شابک	۷۰۰۰۰ ریال یا CD
	ISBN: 978-964-410-226-4
وضعیت فهرست نویسی	فیب.
موضوع	اکسترنات (شبکه‌های کامپیوتری)
شناسه افزوده	طریحی، مهران، ۱۳۶۰
رده‌بندی کنگره	۱۳۸۸ ز ۲ الف ۷۵/۸۷۵ TK ۵۱۰۵
رده‌بندی دیویی	۰۰۵۸
شماره کتابخانه ملی	۱۹۰۱۰۰۹



موسسه علمی فرهنگی

شبکه‌های خصوصی مجازی (رهیافتی تئوری و عملی)

داریوش زاهدمنش - مهران طریحی

چاپ اول: زمستان ۸۹

تیراژ: ۲۵۰۰

ناشر: «نص»

طراحی، چاپ، صحافی: موسسه علمی فرهنگی «نص» قیمت با CD: ۷۰۰۰ تومان

دفتر: تهران، میدان انقلاب، خ منیری جارید، بن بست مبین، شماره ۶ **فروشگاه ۱:** تهران - ضلع جنوب شرقی میدان انقلاب، شماره ۳۰۰۰۷۳

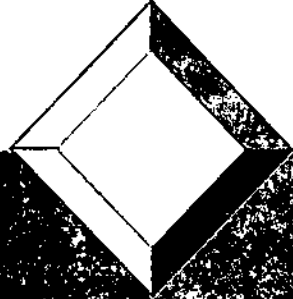
تلفن: ۶۶۴۰۵۳۷۲ - ۶۶۲۱۱۳۸۵ - ۶۶۴۶۵۶۷۲ - ۶۶۸۵۴۰۸۳ - ۶۶۹۵۷۶۹۰ فاکس: ۶۶۹۵۷۶۹۰

ص.ب. ۱۳۱۲۵-۸۶۳ ایمیل: info@nasspub.com **فروشگاه ۲:** بزد - فلکه اطلسی - بلوار دانشگاه - نرسیده به مجتمع خورشید

وب سایت: www.nass.ir

تلفن: ۰۲۵۱-۸۲۵۷۱۰۵ کتابفروشی بزرگ نص

شابک: ۹۷۸-۹۶۴-۲۱۰-۲۲۶-۴ ISBN: 978-964-410-226-4



پیشگفتار

حمد و سپاس خداوند متعال را که به ما توفیق گام برداشتن در راه علم و حقیقت را عنایت فرمود. سه سال پیش، هنگامی که کار بر روی شبکه‌های خصوصی مجازی را آغاز نمودیم، هرگز تصور نمی‌کردیم قدم به دریایی بیکران از علوم و فنون مختلف گذاشته باشیم. دانش شبکه، سیستم عامل، امنیت و برنامه‌نویسی، همه و همه دست در دست هم داده‌اند تا یکی از مهمترین پایه‌ها و رتوس امنیت شبکه را تشکیل دهند. در حین انجام کار، کمبود منابع و مثال‌های کاربردی همواره سدی بزرگ بر سر راه پیشرفت سریع‌مان بود. کتاب‌ها و منابع زیادی را مطالعه کردیم اما به جرأت می‌توان گفت دسترسی به نمونه‌های کاربردی این کتاب در هیچ کتاب داخلی و یا حتی خارجی به طور یکپارچه و دسته‌بندی شده در اختیار مشتاقان قرار نداشت. حتی کتاب‌های مرجعی مثل OpenVPN و Openswan نیز که یک بسته خاص را تشریح کرده بودند، از نقطه نظر عملی کاستی‌های بسیاری داشتند. در طول این مدت با تلاش مضاعف، بیشتر آنچه را که به دنبال آن بودیم، بدست آوردیم. کار عملی در این زمینه باعث شد تا تجارب بسیاری کسب کنیم، و با مشکلات و مسائل مربوط بصورت ملموس دست و پنجه نرم کنیم. سپس بر آن شدیم تا هر آنچه را که آموخته‌ایم با دیگر علاقمندان این زمینه به اشتراک بگذاریم، و در نتیجه ایده پیدایش این کتاب شکل گرفت. در آن موقع هرگز گمان نمی‌کردیم که نگارش این کتاب تا به این اندازه سخت باشد، و بیش از یک سال برای به ثمر رسیدن آن زمان سپری شود.

شبکه خصوصی مجازی (VPN) به همراه دیواره آتش (Firewall) و سیستم‌های تشخیص نفوذ (IDS) جزء سرویس‌های امنیتی غیر قابل اغماضی هستند که هر نهاد و سازمانی که به دنبال حفظ منابع اطلاعاتی خود است، باید جایگاه آنها را در شبکه خود محفوظ بدارد. اما از آنجائیکه محرمانگی داده‌ها نقش پر رنگ‌تری دارد، لذا اهمیت وجود VPN بیش از پیش آشکار می‌گردد. اگر چه پیاده‌سازی VPN

در لایه‌های مختلف شبکه قابل انجام است، ولی با مقایسه مزایا و معایب آنها می‌توان به این نتیجه رسید که بهترین پیاده‌سازی‌ها، IPSec و VPN‌های مبتنی بر SSL/TLS می‌باشند. در واقع تمرکز مطالب این کتاب نیز بیشتر بر روی مباحث مربوط به این دو پیاده‌سازی خواهد بود.

این کتاب مناسب چه کسانی است؟

این کتاب برای افرادی که می‌خواهند با شبکه‌های خصوصی مجازی آشنا شده و در این زمینه فعالیت عملی کنند، بسیار مفید است. همچنین کسانی که با توجه به قیمت بالای دستگاه‌های امنیت شبکه به دنبال راه کارهای متن باز و رایگان هستند، این کتاب راهگشای سیاست‌های امنیتی‌شان خواهد بود. در این کتاب فرض شده است که خواننده با مفاهیم شبکه و همچنین کاربری سیستم عامل لینوکس آشنا است.

ساختار فصول کتاب

این کتاب شامل هشت فصل و چهار ضمیمه است. فصل اول مقدمه‌ای بر مفاهیم کلی شبکه خصوصی مجازی، اصول اولیه رمزنگاری و امنیت اطلاعات است. علاوه بر مطالب فوق، با گواهینامه‌ها و امضای دیجیتال نیز آشنا می‌شوید. مطالب این فصل به عنوان پایه‌ای برای فصول بعدی در نظر گرفته شده است.

فصل کوتاه دوم، نگاشت بین تکنولوژی‌های مختلف شبکه‌های خصوصی مجازی و مدل هفت لایه‌ای مرجع OSI را بیان می‌کند. در این فصل تکنولوژی‌های شبکه خصوصی مجازی در هر لایه به اختصار بررسی شده‌اند.

فصول سوم و چهارم پیرامون پروتکل IPSec می‌باشند. فصل سوم شامل مفاهیم و توضیحات تئوری بوده و در فصل چهارم یک پیاده‌سازی متن باز از آن به نام Openswan، توضیح داده شده است. سعی بر آن بوده که مطالب مربوط به نصب و راه‌اندازی به صورت یک رهافت گام به گام باشد. همچنین مثال‌های کاربردی مختلفی در انتهای فصل چهارم در نظر گرفته شده که می‌تواند راهنمای مناسبی برای انجام پیکربندی سناریوهای واقعی باشد.

فصول پنجم و ششم نیز ساختار دو فصل قبلی را دارند، بدین صورت که فصل پنجم اصول مقدماتی پروتکل SSL/TLS را تشریح کرده و در ادامه، فصل ششم یک پیاده‌سازی متن باز از شبکه خصوصی مجازی مبتنی بر این پروتکل، به نام OpenVPN، را آموزش می‌دهد. در انتهای فصل ششم نیز چند سناریوی امنیتی مختلف ارائه شده است.

فصل هفتم به معرفی User Mode Linux (UML) که تکنیک اجرای همزمان چند سیستم عامل لینوکس بر روی یک میزبان لینوکس است، می‌پردازد. در این فصل پس از توضیح UML و آشنایی با ویژگی‌های مختلف آن، چگونگی نصب و راه‌اندازی Openswan بر روی یک UML تشریح شده است. در انتها نیز، بر روی یک کامپیوتر میزبان، یک ارتباط VPN بین دو UML برقرار کرده‌ایم.

فصل هشتم تجربه‌ای جالب از راه‌اندازی IPSec VPN در مسیراب‌های سیسکو است. در این فصل

با معرفی ابزار نمونه‌سازی مسیرب‌های سیکو (GNS3 Emulator)، نحوه راه‌اندازی اینگونه مسیرب‌ها را بدون نیاز به خرید تجهیزات گران قیمت سیکو، به خوانندگان آموزش خواهیم داد. ضمیمه الف مثالی از راه‌اندازی و پیکربندی PPTP بر روی لینوکس است. ضمیمه ب مرجعی از دستورات پر کاربرد سیستم عامل لینوکس است. بسیاری از این دستورات در مثال‌های این کتاب استفاده شده است. دستورات پر کاربرد خط فرمان سیکو نیز در ضمیمه ج قرار دارد، همچنین فهرستی از RFC‌های مربوط به پروتکل IPSec در ضمیمه د ارائه شده است. به همراه این کتاب یک لوح فشرده عرضه می‌شود، که شامل برنامه‌ها و فایل‌های مربوط به فصول عملی کتاب است. علاوه بر این، کلیه کتاب‌های الکترونیکی مورد استفاده ما و آنهایی که به عنوان مرجع در انتهای کتاب ذکر شده‌اند، در این لوح فشرده قرار دارند تا خوانندگان کتاب به آنها نیز دسترسی داشته باشند.

سخن پایانی

امید است این اثر ناچیز گامی کوچک در ارتقاء سطح دانش جامعه علمی کشور برداشته و مورد رضایت صاحب‌نظران قرار گیرد. در پایان لازم می‌دانیم از آقایان محمد نژادپور (دوست و همکار عزیزی که همواره راهنمای ما بوده است)، پاول ووترز (Paul Wouters)، نویسنده کتاب Openswan و یکی از توسعه‌دهندگان آن که پاسخگوی سؤالات متعدد ما بود، مدیریت محترم انتشارات نص، جناب آقای زارع، و کلیه عزیزانی که ما را در تهیه این کتاب یاری نمودند، کمال تشکر و قدردانی را داشته باشیم. همانند هر اثر دیگری، این کتاب نیز عاری از نقص نخواهد بود. از تمامی خوانندگان، دانشجویان، اساتید و همکاران محترم خواهشمند است که نقطه نظرات و پیشنهادات خود را از طریق پست الکترونیکی زیر با ما در میان گذاشته، و ما را از راهنمایی‌های خود بی‌بهره نسازند.

Dariush Zahedmanesh: zahedmanesh@gmail.com
Mehran Toreihi: mtoreihi@gmail.com

داریوش زاهدمنش - مهرا ن طریحی

مهر ۱۳۸۸

فهرست مطالب

۱۱	فصل ۱ « مقدمه‌ای بر VPN و رمزنگاری
۱۲	۱-۱ VPN چیست؟
۱۶	۲-۱ اصول رمزنگاری و امنیت
۱۷	۱-۲-۱ الگوریتم‌های رمزنگاری با کلید متقارن (Symmetric-Key)
۱۸	۲-۲-۱ الگوریتم‌های کلید عمومی (Public Key)
۱۹	۳-۲-۱ الگوریتم‌های خلاصه پیام (Message Digest) یا درهم‌سازی
۲۱	۳-۱ امضای دیجیتال (Digital Signature)
۲۱	۱-۳-۱ امضای دیجیتال با کلید متقارن
۲۱	۲-۳-۱ امضای دیجیتال با کلید عمومی
۲۳	۴-۱ مدیریت کلیدهای عمومی
۲۳	۵-۱ گواهینامه (Certificate)
۲۷	۶-۱ ایجاد کلید مشترک: مبادله کلید به روش دیفی - هلمن
۲۹	فصل ۲ « تکنولوژی‌های VPN
۳۱	۱-۲ VPN در لایه‌های مختلف مدل OSI
۳۲	۱-۱-۲ لایه ۱ - فیزیکی
۳۲	۲-۱-۲ لایه ۲ - پیوند داده
۳۴	۳-۱-۲ لایه ۳ - شبکه
۳۴	۴-۱-۲ لایه ۴ - انتقال
۳۵	۵-۱-۲ لایه ۷ - کاربرد
۳۷	فصل ۳ « IPSec
۳۸	۱-۳ پروتکل IPSec
۴۲	۲-۳ پروتکل AH

۴۳	پروتکل AH در حالت انتقال	۱-۲-۳
۴۴	پروتکل AH در حالت تونل	۲-۲-۳
۴۴	پروتکل ESP	۳-۳
۴۵	پروتکل ESP در حالت انتقال	۱-۳-۳
۴۶	پروتکل ESP در حالت تونل	۲-۳-۳
۴۷	مجمع امنیتی	۴-۳
۴۸	پروتکل تبادل کلید در اینترنت (IKE) Internet Key Exchange	۵-۳
۵۱	احراز هویت با استفاده از کلید مخفی مشترک	۱-۵-۳
۵۳	احراز هویت با استفاده از امضاء	۲-۵-۳
۵۴	احراز هویت با استفاده از رمزنگاری کلید عمومی	۳-۵-۳
۵۵	احراز هویت با استفاده از رمزنگاری کلید عمومی بهینه شده	۴-۵-۳
۵۷	NAT T (NAT Traversal)	۶-۳
۶۱	بررسی فایل Log مربوط به Openswan	۷-۳

فصل ۴ « Openswan

۶۸	تاریخچه	۱-۴
۶۸	ساخت و نصب Openswan	۲-۴
۶۸	انتخاب یک توزیع لینوکس	۱-۲-۴
۶۹	انتخاب یک پشته IPSec	۲-۲-۴
۶۹	انتخاب برنامه بخش کاربر	۳-۲-۴
۷۰	انتخاب نصب از طریق کد برنامه یا بسته های آماده	۴-۲-۴
۷۰	آغاز عملیات ساخت و نصب	۵-۲-۴
۷۵	پیکربندی Openswan	۳-۴
۷۶	پیکربندی از طریق کنسول	۱-۳-۴
۷۹	پیکربندی از طریق واسط گرافیکی وب	۲-۳-۴
۸۳	مثال های کاربردی	۴-۴
۸۳	سناریوی شبکه به شبکه	۱-۴-۴
۸۷	سناریوی شبکه به شبکه با NAT	۲-۴-۴
۸۹	احراز هویت با استفاده از گواهی نامه دیجیتال X.509	۳-۴-۴
۹۵	ارتباط از راه دور توسط پروتکل های L2TP/IPSec	۴-۴-۴
۱۰۵	GRE بر روی IPSec	۵-۴-۴

فصل ۵ « مقدمه ای بر SSL و امنیت وب

۱۱۷	تاریخچه SSL	۱-۵
-----	-------------	-----

۱۱۸	۲-۵	رویکردهای امنیت شبکه
۱۲۱	۳-۵	محدودیت‌های پروتکل
۱۲۱	۴-۵	اهداف و ساختار SSL
۱۲۷	۱-۴-۵	از سرگیری یک نشست SSL
۱۲۷	۲-۴-۵	الگوریتم‌های مورد پشتیبانی در پروتکل SSL
۱۲۸	۵-۵	حملات تأثیرگذار بر SSL

فصل ۶ « OpenVPN ۱۳۱

۱۳۳	۱-۶	مزایا
۱۳۴	۲-۶	تاریخچه
۱۳۴	۱-۲-۶	OpenVPN نسخه ۱
۱۳۵	۲-۲-۶	OpenVPN نسخه ۲
۱۳۵	۳-۶	شبکه با OpenVPN
۱۳۷	۱-۳-۶	OpenVPN و ابزارهای آتش (فایروال)
۱۳۸	۲-۳-۶	پیکربندی OpenVPN
۱۳۸	۳-۳-۶	مشکلات OpenVPN
۱۳۹	۴-۶	مقایسه OpenVPN با VPN‌های مبتنی بر IPSec
۱۴۰	۵-۶	منابع و مستندات
۱۴۰	۶-۶	نصب OpenVPN
۱۴۱	۱-۶-۶	نصب OpenVPN تحت ویندوز
۱۴۲	۲-۶-۶	بررسی نرم‌افزار نصب شده
۱۴۵	۳-۶-۶	نصب OpenVPN تحت لینوکس
۱۴۹	۷-۶	راه‌اندازی اولین تونل OpenVPN
۱۵۴	۱-۷-۶	برقراری ارتباط VPN بین ویندوز و لینوکس
۱۵۵	۸-۶	راه‌اندازی OpenVPN با گواهینامه X.509
۱۵۶	۱-۸-۶	تولید گواهینامه با easy-rsa در ویندوز
۱۶۲	۹-۶	مثال‌های کاربردی OpenVPN
۱۶۳	۱-۹-۶	امن سازی شبکه بی‌سیم با OpenVPN
۱۷۱	۲-۹-۶	Road Warrior
۱۷۴	۳-۹-۶	حالت شبکه به شبکه

فصل ۷ « User Mode Linux ۱۷۷

۱۷۹	۱-۷	مزایای استفاده از UML
۱۸۰	۲-۷	نگاهی اجمالی به UML

۱۸۳.....	۳-۷ ابزارهای کمکی UML
۱۸۵.....	۴-۷ راه‌اندازی شبکه در UML
۱۸۸.....	۵-۷ راه‌اندازی دومین UML
۱۸۸.....	۱-۵-۷ فایل‌های COW
۱۸۹.....	۶-۷ پیکربندی شبکه برای چندین UML
۱۹۰.....	۷-۷ راه‌اندازی Openswan بر روی UML
۱۹۱.....	۱-۷-۷ آماده‌سازی هسته
۱۹۲.....	۲-۷-۷ آماده‌سازی سیستم فایل ریشه
۱۹۴.....	۳-۷-۷ راه‌اندازی UML‌های Left و Right
۱۹۵.....	۴-۷-۷ پیکربندی IPsec برای UML‌های Left و Right

فصل ۸ « راه‌اندازی IPsec در سیسکو » ۱۹۷.....

۱۹۸.....	۱-۸ GNS3
۱۹۸.....	۱-۱-۸ نصب و پیکربندی
۲۰۸.....	۲-۱-۸ محیط برنامه GNS3
۲۰۹.....	۳-۱-۸ راه‌اندازی اولیه GNS3
۲۱۰.....	۲-۸ راه‌اندازی IPsec در مسیرهای سیسکو
۲۱۱.....	۱-۲-۸ پیکربندی ابتدایی مسیرها
۲۱۲.....	۲-۲-۸ پیکربندی ISAKMP
۲۱۳.....	۳-۲-۸ پیکربندی IPsec

پیوسته الف « PPTP » ۲۱۹.....

۲۱۹.....	مقدمه
۲۱۹.....	نصب و پیکربندی
۲۲۹.....	ب « مرجع دستورات پر کاربرد سیسکو
۲۳۱.....	ج « راهنمای دستورات پر کاربرد سیستم عامل لینوکس
۲۳۷.....	د « جدول RFC‌های مرتبط با پروتکل IPsec
۲۴۱.....	مراجع
۲۴۲.....	فهرست سایت‌های مرتبط
۲۴۳.....	کوتاه نوشت‌ها
۲۴۵.....	واژه نامه