



مهندسی

پیکربندی امن تجهیزات سایت‌های کامپیوتری

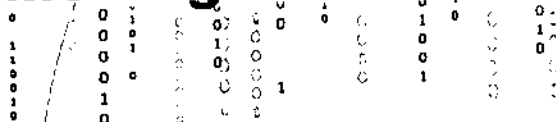
تألیف و تدوین:

دکتر ناصر مدیری

مهندس مرتضی سالاری اخگر



Mehregane Ghalam



سرشناسه

مدیری، ناصر، ۱۳۴۱ -

عنوان و نام پدیدآور

مهندسی پیکربندی امن تجهیزات سایت‌های کامپیوتری / تألیف و تدوین ناصر مدیری، مرتضی سالاری.

مشخصات نشر

تهران: مهرگان قلم، ۱۳۹۰.

مشخصات ظاهری

۳۲۴ ص: مصور، جدول.

شابک

978-600-6236-09-4

وضعیت فهرست نویسی

فیا

موضوع

شبکه‌های کامپیوتری - اقدامات تضمینی

موضوع

شبکه‌های کامپیوتری - اطمینان‌پذیری

موضوع

شبکه‌های کامپیوتری - مدیریت

شناسه افزوده

سالاری اخگر، مرتضی، ۱۳۶۳ -

رده بندی کنگره

TK۵۱۰۵۹۱۳۹-۵۹۷۷/م۴

رده بندی دیویی

۸۱۰۰۵

شماره کتابشناسی ملی

۲۴۸۲۴۵۸



مهندسی پیکربندی امن تجهیزات سایت‌های کامپیوتری

انتشارات مهرگان قلم

مولف: دکتر ناصر مدیری - مهندس مرتضی سالاری

ناشر: مهرگان قلم

طراحی و صفحه آرایی: مهندس سید حسین حسینی

چاپ اول: ۱۳۹۰

چاپ و صحافی: سپهر نوین

تیراژ: ۱۰۰۰ نسخه

قیمت: ۸۵۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۰۹-۴

کلیه حقوق این اثر متعلق به انتشارات مهرگان قلم می‌باشد.

تهران، خیابان انقلاب، خیابان دانشگاه، کوچه تقدیری - پلاک ۲۲، واحد ۴

تلفن بخش: ۶۶۹۵۸۵۵۸ - ۶۶۹۶۰۷۶۳ - ۰۹۱۲۱۵۲۴۴۲۵

پیشگفتار

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکت های دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است.

امنیت اطلاعات در محیط های مجازی همواره بعنوان یکی از زیرساخت ها و الزامات اساسی در کاربری توسعه ای و فراگیر از فناوری اطلاعات و ارتباطات مورد تاکید قرار گرفته است. اطمینان از ایمن بودن سرمایه های اطلاعاتی و تجهیزات زیر ساختی کشور گذشته از ابعاد گسترده امنیت ملی، کلید قفل فرصت های بی شمار تجاری و غیرتجاری جدید اینترنتی است. آنچه مسلم است چالش امنیتی رودرروی کشور عدم دسترسی به فناوری و یا عدم وجود محصولات امنیتی نیست، بلکه سیاست گذاری، فرهنگ سازی، بهره وری مناسب از منابع موجود و نیز سازگاری آن ها به گونه ای است، که نیاز منحصر به فرد شبکه و فضای دیجیتالی کشور را تأمین کند. نکته مهم حاصل از تجارب کشورهای پیشرو حاکی است که امنیت اطلاعات مسأله ای فرابخشی است و نیاز به همکاری های گسترده، هم در سطح ملی و هم در سطح بین المللی، در این زمینه دارد. تعیین نقش ها، وظایف و مسئولیت ها از نکات مهمی است که در این همکاری ها باید تعریف شوند.

این کتاب که در هفت فصل تدوین شده است، سعی دارد تا مسائل و پروتکل های مهم امنیتی را در برگیرد تا به وسیله آن بتوان امنیت سازمانی و اطلاعاتی محکمی طراحی کرد. یکی از مهمترین ابزارهای شبکه روترها می باشند که بدون آن ها شبکه های کامپیوتری بی معنی خواهد بود، بیشتر هدف مهاجمان این وسیله خواهد بود و به طور طبیعی باید پروتکل و تدابیر امنیتی زیادی برای آن در نظر گرفت. از این رو این کتاب در فصل اول به معرفی روترها خواهد پرداخت که حتی خواننده مبتدی نیز پس مطالعه این فصل به خوبی با این سخت افزار مهم و حیاتی آشنا خواهد شد.

این کتاب در هفت فصل سازماندهی شده است که هر فصل به قرار زیر می باشد:

فصل اول:

به معرفی روتر و جایگاه آن در شبکه های کامپیوتری پرداخته است، در این فصل بیشتر ماهیت سخت افزاری روتر بررسی شده است.

فصل دوم:

درباره کانفیگ و تنظیمات نرم افزاری روتر صحبت می‌کند. و این که روترها در هر شبکه خاص به چه صورت باید تنظیم شوند.

فصل سوم:

این فصل امنیت تجهیزات سخت افزاری شبکه را توصیف می‌کند، این ابزارهای شبکه از نظر امنیت فیزیکی و منطقی چه شرایطی باید داشته باشند.

فصل چهارم:

این فصل درباره اهمیت امنیت داده در سازمان‌ها صحبت می‌کند، این که چه راهکارهای در برابر حملات مهاجمان باید داشته باشیم به طور کامل تشریح شده است.

فصل پنجم:

با توجه به این آدرس‌های شبکه (IP) از اهمیت بالایی برخوردار می‌باشد این فصل درباره یک پروتکل مهم به نام NAT صحبت می‌کند، NAT وظیفه ترجمه آدرس‌های IP را دارد.

فصل ششم:

این فصل مهمترین قسمت این کتاب می‌باشد که به توصیف پروتکل حیاتی AAA پرداخته است، این پروتکل نقش بالایی در امنیت شبکه‌ها دارد که چندین فیلد امنیتی را پوشش می‌دهد.

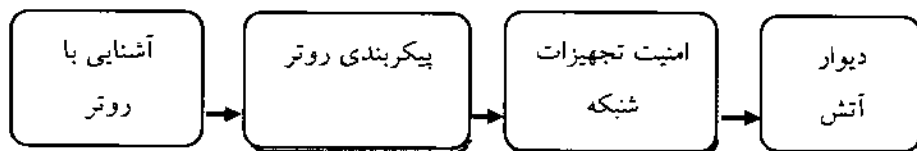
فصل هفتم:

این فصل درباره یک ابزار کارآمد دفاعی و امنیتی به نام دیواره آتش بحث می‌کند، عملکرد و تمام مدل‌های دیواره آتش در این فصل به طور مفصل توصیف شده است.

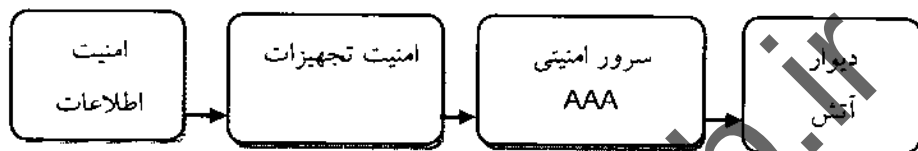
این کتاب با رویکردی خلاقانه در جهت توضیح و آموزش مسائل ذکر شده سعی دارد گامی در جهت پیشبرد علم امنیت شبکه بردارد، و امید است که به لطف خدای مهربان مورد توجه شما علم دوستان عزیز قرار گیرد.

راهنمایی جهت مطالعه کتاب:

برای آشنایی با امنیت روتر، فصل‌ها را مطابق با نمودار ۱ دنبال نمایید.



جهت درک مفاهیم مربوط به امنیت اطلاعات با فصل‌ها را مطابق با نمودار ۲، مورد مطالعه قرار دهید.



جهت یادگیری و شناسایی امنیت تجهیزات شبکه و یادگیری پیکربندی امن شبکه، فصل‌ها را به ترتیب نمودار ۳، مطالعه نمایید.



در پایان از تمام دوستانی که ما را در به ثمر رسیدن این کتاب یاری فرمودند کمال سپاس و تشکر را داریم و بی صبرانه منتظر نظرات، انتقادات و پیشنهادات شما عزیزان هستیم تا در آینده بتوانیم گامی محکمتر در جهت علم برداریم.

دکتر ناصر مدیری-مهندس مرتضی سالاری اخگر

پست الکترونیکی انعکاس نظرات

Info@27000.Ir

Www.27000.Ir



۲۳	۱. آشنایی با روتر
۲۴	۱.۱. خلاصه فصل
	۱.۲. مقدمه ۲۴
۲۵	۱.۳. آشنایی اولیه با روتر
۲۵	۱.۴. انواع روترها
۲۶	۱.۴.۱. روترهای سخت افزاری
۲۶	۱.۴.۲. روترهای نرم افزاری
۲۷	۱.۴.۳. روتر به منظور اتصال دو شبکه
۲۷	۱.۴.۴. روتر در یک شبکه LAN
۲۸	۱.۴.۵. روتر به منظور اتصال دو دفتر کار
۲۹	۱.۵. ویژگی‌های یک روتر
۲۹	۱.۶. عناصر داخلی روتر
۲۹	۱.۶.۱. پردازنده
۲۹	۱.۶.۲. حافظه اصلی
۳۰	۱.۶.۳. حافظه فلش
۳۰	۱.۶.۴. حافظه NVRAM
۳۰	۱.۶.۵. گذرگاه‌ها
۳۱	۱.۶.۶. حافظه ROM
۳۱	۱.۶.۷. منبع تغذیه
۳۱	۱.۷. آشنایی با اینترفیس‌های روتر
۳۳	۱.۷.۱. انواع اینترفیس‌های روتر
۳۴	۱.۸. انواع کابل در شبکه‌های کامپیوتری

۳۴	۱.۸.۱ کابل های چهار زوجی
۳۵	۱.۸.۲ مشخصه های کابل UTP
۳۶	۱.۸.۳ کابل کواکسیال
۳۷	۱.۸.۴ فیبر نوری
۳۷	۱.۹ پیکربندی روتر با پورت های مدیریت
۳۷	۱.۹.۱ نحوه اتصال به پورت کنسول روتر
۳۹	۱.۱۰ راه اندازی اولیه روتر
۴۱	۱.۱۱ چراغ های Leds
۴۱	۱.۱۲ راه اندازی سیستم و نمایش پیام ها
۴۱	۱.۱۲.۱ نمایش پیام عدم پیکربندی
۴۲	۱.۱۳ سری ها و مدل های مسیر یاب های سیکو
۴۲	۱.۱۳.۱ معرفی روتر ۵۳۰۰ سیکو
۴۵	۱.۱۳.۲ مدل Cisco36XX
۴۵	۱.۱۳.۳ مدل Cisco5350
۴۶	۱.۱۳.۴ مدل Cisco1750
۴۶	۱.۱۳.۵ مدل Ciscovg200
۴۸	۱.۱۴ نتیجه گیری
۴۸	۱.۱۵ پرسش و تحقیق
۴۹	۱.۱۶ منابع و مراجع
۵۲	۲ پیکربندی روتر های سیکو
۵۲	۲.۱ خلاصه بخش
	۲.۲ مقدمه ۵۲
۵۳	۲.۳ پیکربندی اولیه روتر
۵۴	۲.۳.۱ اجرای برنامه Hyperterminal
۵۴	۲.۳.۲ انتخاب یک نام برای Hyperterminal Session
۵۴	۲.۳.۳ انتخاب ایترفیس ارتباطی کامپیوتر
۵۵	۲.۳.۴ مشخص نمودن خصایص ایترفیس ارتباطی
۵۶	۲.۴ اتصال به روتر
۵۶	۲.۴.۱ پورت Console
۵۷	۲.۴.۲ پورت Auxiliary

۵۷	۲.۴.۳. پورت Telnet
۵۷	۲.۴.۴. پروتکل TFTP
۵۷	۲.۴.۵. مرورگر وب
۵۸	۲.۵. حالات متفاوت رابط کاربر روتر
۵۸	۲.۶. انواع مدهای دسترسی
۵۸	۲.۶.۱. مد کاربر
۵۸	۲.۶.۲. Router >
۵۸	۲.۶.۳. دستور HELP
۵۹	۲.۶.۴. Router> ?
۵۹	۲.۶.۵. مد دسترسی
۵۹	۲.۶.۶. Router > Enable
۶۰	۲.۶.۷. Router#
۶۰	۲.۶.۸. Router # Exit
۶۰	۲.۶.۹. مد پیکربندی
۶۰	۲.۶.۱۰. Router# Configure Terminal
۶۱	۲.۶.۱۱. پیکربندی نام برای روتر
۶۱	۲.۷. ذخیره کردن تنظیمات
۶۱	۲.۸. پیکربندی رمز عبور روتر
۶۲	۲.۸.۱. پسورد دسترسی
۶۲	۲.۸.۲. پسورد امنیتی
۶۲	۲.۸.۳. پسورد Telnet
۶۳	۲.۸.۴. پسورد پورت Console
۶۳	۲.۸.۵. پسورد پورت AUX
۶۴	۲.۹. ویژگیهای یک شبکه WAN
۶۴	۲.۹.۱. اتصال ایترفیس های WAN
۶۵	۲.۹.۲. استفاده از ایترفیس WAN
۶۵	۲.۱۰. اتصال روتر به شبکه LAN
۶۶	۲.۱۱. تنظیمات ایترفیس Serial
۶۷	۲.۱۲. تنظیمات Ethernet و Fast Ethernet
۶۷	۲.۱۳. فعال و غیرفعال کردن یک ایترفیس
۶۸	۲.۱۴. معرفی IP Address

۶۸	۲.۱۴.۱. آدرس دهی به اینترفیس روتر
۶۹	۲.۱۵. متداولترین دستورات Show
۷۰	۲.۱۶. مسیریابی
۷۱	۲.۱۶.۱. مسیریابی چیست؟
۷۲	۲.۱۶.۲. معرفی Static Routing و Dynamic Routing
۷۳	۲.۱۷. پروتکل های مسیریابی
۷۴	۲.۱۷.۱. مسیریابی بردار خطی
۷۴	۲.۱۷.۲. مسیریابی شناخت کلی
۷۵	۲.۱۷.۳. مسیریابی ترکیبی
۷۵	۲.۱۸. پروتکل RIP
۷۷	۲.۱۸.۱. راه اندازی پروتکل RIP
۷۷	۲.۱۸.۲. پیکربندی RIP بر روی روتر Router1
۷۸	۲.۱۸.۳. پیکربندی RIP بر روی روتر Router2
۷۸	۲.۱۸.۴. پیکربندی RIP بر روی روتر Router3
۷۸	۲.۱۸.۵. مشاهده جدول Routing Table
۷۹	۲.۱۸.۶. متریک
۸۰	۲.۱۹. پروتکل مسیریابی IGRP
۸۱	۲.۱۹.۱. پیکربندی IGRP
۸۲	۲.۱۹.۲. پیکربندی IGRP در یک مثال
۸۲	۲.۱۹.۳. پیکربندی IGRP بر روی Router 1
۸۲	۲.۱۹.۴. پیکربندی IGRP بر روی Router 2
۸۲	۲.۱۹.۵. پیکربندی IGRP بر روی Router 3
۸۲	۲.۲۰. پروتکل HDLC
۸۳	۲.۲۰.۱. پیکربندی پروتکل HDLC
۸۴	۲.۲۱. پروتکل PPP
۸۵	۲.۲۲. اجزای پروتکل لایه ای
۸۵	۲.۲۳. برقراری یک PPP Session
۸۷	۲.۲۴. تنظیم PPP روی لینک نقطه به نقطه
۸۷	۲.۲۴.۱. پیکربندی پروتکل PPP
۸۷	۲.۲۴.۲. تنظیم Authentication در پروتکل PPP
۸۸	۲.۲۴.۳. مشخص کردن یک نام برای روتر

۸۸	۲.۲۴.۴. مشخص کردن Username و Password
۸۸	۲.۲۴.۵. تنظیمات مربوط به روتر Hamadan
۸۹	۲.۲۴.۶. تنظیمات مربوط به روتر Tehran
۸۹	۲.۲۵. نتیجه گیری
۸۹	۲.۲۶. منابع و مراجع
۹۲	۳. امنیت تجهیزات شبکه
۹۲	۳.۱. خلاصه بخش
	۳.۲. مقدمه ۹۲
۹۳	۳.۳. تدوین سیاست
۹۴	۳.۴. استانداردها و روالهای امنیتی
۹۴	۳.۵. ساختار سیاست امنیتی
۹۴	۳.۶. امنیت تجهیزات شبکه
۹۵	۳.۷. امنیت فیزیکی
۹۶	۳.۷.۱. افزودنی در محل استقرار شبکه
۹۶	۳.۷.۲. تویولوژی شبکه
۹۷	۳.۷.۳. محل های امن برای تجهیزات
۹۷	۳.۷.۴. انتخاب لایه کانال ارتباطی امن
۹۸	۳.۷.۵. منابع تغذیه
۹۹	۳.۷.۶. عوامل محیط
۹۹	۳.۸. امنیت منطقی
۹۹	۳.۸.۱. امنیت مسیریابها
۱۰۰	۳.۸.۲. مدیریت پیکربندی
۱۰۰	۳.۸.۳. کنترل دسترسی به تجهیزات
۱۰۱	۳.۸.۴. امن سازی دسترسی
۱۰۱	۳.۸.۵. مدیریت رمزهای عبور
۱۰۱	۳.۹. ملزومات و مشکلات امنیتی ارائه دهندگان خدمات
۱۰۲	۳.۹.۱. قابلیت های امنیتی
۱۰۲	۳.۹.۲. مشکلات اعمال ملزومات امنیتی
۱۰۲	۳.۱۰. امنیت روترها از طریق پیکربندی
۱۰۵	۳.۱۰.۱. ساخت یک سیاست امنیتی برای یک روتر

۳.۱۰.۲	ایجاد ارتباط بین شبکه محلی و شبکه خارجی	۱۰۷
۳.۱۰.۳	تغییرات در سیاست های شبکه مادر یا شبکه محلی	۱۰۷
۳.۱۰.۴	چک لیست سیاست های کلی برای یک روتر	۱۰۷
۳.۱۰.۵	امنیت فیزیکی	۱۰۸
۳.۱۰.۶	امنیت پیکربندی ساکن	۱۰۹
۳.۱۰.۷	امنیت برای پیکربندی های داینامیک	۱۱۰
۳.۱۰.۸	امنیت در سرویس های شبکه	۱۱۱
۳.۱۰.۹	توپولوژی شبکه	۱۱۱
۳.۱۱	اقدامات عملی امن کردن روتر	۱۱۳
۳.۱۱.۱	امنیت سخت افزاری یا فیزیکی	۱۱۴
۳.۱۲	نسخه های نرم افزاری روترها	۱۱۸
۳.۱۳	پیکربندی روتر و فرمان IOS	۱۲۰
۳.۱۴	نتیجه گیری	۱۲۰
۳.۱۵	پرسش و تحقیق	۱۲۱
۳.۱۶	منابع و مراجع	۱۲۲
۴	امنیت اطلاعات	۱۲۴
۴.۱	خلاصه بخش	۱۲۴
۴.۲	مقدمه ۱۲۴	
۴.۳	اهمیت امنیت اطلاعات و کامپیوترها	۱۲۵
۴.۴	امنیت اطلاعات چیست ؟	۱۲۵
۴.۵	سیستم مدیریت امنیت اطلاعات	۱۲۶
۴.۶	چرا به امنیت اطلاعات نیاز داریم ؟	۱۲۸
۴.۷	آسیب پذیری سیستم اطلاعاتی و جرایم کامپیوتری	۱۲۸
۴.۸	لایه های شبکه های نوین	۱۲۹
۴.۸.۱	شبکه بیرونی	۱۳۰
۴.۸.۲	شبکه داخلی	۱۳۰
۴.۸.۳	فاکتور انسانی	۱۳۱
۴.۹	شرایط امنیتی شبکه بیرونی	۱۳۲
۴.۹.۱	Router های مرزی	۱۳۲
۴.۹.۲	فایروال	۱۳۲

۱۳۲	۴.۹.۳. سنسور IDS
۱۳۳	۴.۹.۴. سرور VPN
۱۳۳	۴.۹.۵. روتر و سوئیچ
۱۳۴	۴.۱۰. شرایط امنیت شبکه داخلی
۱۳۴	۴.۱۱. نرم افزارهای مهاجمان
۱۳۴	۴.۱۱.۱. ویروس‌ها
۱۳۵	۴.۱۱.۲. برنامه‌های اسب تروا
۱۳۵	۴.۱۱.۳. ویرانگران
۱۳۶	۴.۱۱.۴. ره‌گیری داده
۱۳۶	۴.۱۱.۵. کلاهبرداری
۱۳۶	۴.۱۱.۶. نامه‌های الکترونیکی ناخواسته
۱۳۷	۴.۱۲. شرایط امنیت فاکتور انسانی
۱۳۷	۴.۱۲.۱. آموزش کاربران
۱۳۸	۴.۱۲.۲. ساختار عملیات
۱۳۸	۴.۱۲.۳. سیاست‌های قابل اجرا
۱۳۸	۴.۱۳. سیاست امنیتی
۱۳۹	۴.۱۳.۱. بخشهای سند سیاست امنیت اطلاعات
۱۳۹	۴.۱۳.۲. نیاز به امنیت اطلاعات و محدودهی آن
۱۴۰	۴.۱۳.۳. هدف امنیت اطلاعات
۱۴۰	۴.۱۳.۴. تعریف امنیت اطلاعات
۱۴۰	۴.۱۳.۵. تعهد مدیریت در امنیت اطلاعات
۱۴۰	۴.۱۳.۶. تأییدیه سیاست امنیت اطلاعات
۱۴۰	۴.۱۳.۷. هدف سیاست امنیت اطلاعات
۱۴۱	۴.۱۳.۸. اصول امنیت اطلاعات
۱۴۱	۴.۱۳.۹. نقشها و مسئولیتها
۱۴۱	۴.۱۳.۱۰. اقدامات انطباقی
۱۴۲	۴.۱۳.۱۱. بازیینی و کنترل
۱۴۲	۴.۱۳.۱۲. اعلامیه کاربر و تأیید آن
۱۴۲	۴.۱۳.۱۳. ارجاعات
۱۴۲	۴.۱۳.۱۴. عناصر عمومی
۱۴۳	۴.۱۴. پیاده سازی سیاست امنیتی

۱۴۴	۴.۱۴.۱ سیستم های عامل و برنامه های کاربردی
۱۴۵	۴.۱۴.۲ آتشی ویروس
۱۴۵	۴.۱۴.۳ مقاوم سازی Host
۱۴۵	۴.۱۴.۴ رمزهای عبور
۱۴۶	۴.۱۴.۵ استاندارد سازی
۱۴۶	۴.۱۴.۶ بازبینی امنیت شبکه
۱۴۶	۴.۱۴.۷ روتر و سوئیچ
۱۴۶	۴.۱۴.۸ فایروال
۱۴۷	۴.۱۴.۹ فایروال شخصی
۱۴۷	۴.۱۵ پروتکل SNMP
۱۴۸	۴.۱۶ حملات
۱۴۸	۴.۱۶.۱ حملات شناسایی
۱۴۸	۴.۱۶.۲ حملات دستیابی
۱۴۹	۴.۱۶.۳ حملات از کار انداختن سرویس ها
۱۴۹	۴.۱۷ انواع دفاع در شبکه
۱۵۰	۴.۱۷.۱ جلوگیری از IP Spoofing
۱۵۰	۴.۱۷.۲ پیشگیری از Dos
۱۵۱	۴.۱۷.۳ متوقف کردن IP Spoofing خارج شونده
۱۵۱	۴.۱۷.۴ استفاده از Anti Spoofing بر روی Gateway
۱۵۲	۴.۱۷.۵ جلوگیری از حمله Smurf
۱۵۳	۴.۱۷.۶ جلوگیری از طوفان TCP SYN
۱۵۳	۴.۱۷.۷ جلوگیری از حمله LAND Attack
۱۵۳	۴.۱۷.۸ غیر فعال کردن ARP Proxy
۱۵۴	۴.۱۷.۹ جلوگیری از حمله ARP
۱۵۴	۴.۱۷.۱۰ جلوگیری از استفاده ICMP
۱۵۵	۴.۱۷.۱۱ محدود کردن Broadcast
۱۵۵	۴.۱۷.۱۲ جلوگیری از Fragmentation
۱۵۶	۴.۱۷.۱۳ Fragmentation چگونه کار می کند
۱۵۶	۴.۱۷.۱۴ مثال Fragmentation
۱۵۶	۴.۱۸ اجرای سیاست امنیت اطلاعات
۱۵۷	۴.۱۸.۱ برنامه آگاه سازی امنیتی

۱۵۷	۴.۱۸.۲ هدف از برنامه
۱۵۸	۴.۱۸.۳ شناخت مخاطبان
۱۵۸	۴.۱۸.۴ سنجش سطح دانش امنیتی کارکنان
۱۵۸	۴.۱۸.۵ تشویق کارکنان به رعایت نکات ایمنی
۱۵۹	۴.۱۸.۶ انتخاب شیوه آموزش
۱۵۹	۴.۱۸.۷ کاغذ اخبار امنیت اطلاعات
۱۶۰	۴.۱۸.۸ وب سایت امنیت اطلاعات
۱۶۰	۴.۱۸.۹ تکنیک "ما به کمک شما نیازمندیم"
۱۶۰	۴.۱۸.۱۰ جدال‌های آموزشی
۱۶۰	۴.۱۸.۱۱ مدیریت تهدیدات امنیتی
۱۶۱	۴.۱۹ ارزیابی سیاست امنیتی
۱۶۱	۴.۱۹.۱ محصول VPC
۱۶۱	۴.۱۹.۲ محصول Intel Integrated Security Software
۱۶۲	۴.۲۰ عوامل موفقیت برنامه امنیت اطلاعات
۱۶۳	۴.۲۱ نتیجه گیری
۱۶۴	۴.۲۲ پرمش و تحقیق
۱۶۴	۴.۲۳ منابع و مراجع
۱۶۶	۵ پروتکل NAT و VPN
۱۶۶	۵.۱ خلاصه بخش
	۵.۲ مقدمه ۱۶۶
۱۶۷	۵.۳ قابلیت‌های NAT
۱۶۹	۵.۴ مفاهیم اولیه NAT و انواع آن
۱۷۱	۵.۵ انواع NAT
۱۷۱	۵.۵.۱ Static NAT
۱۷۲	۵.۵.۲ Dynamic NAT
۱۷۲	۵.۵.۳ Dynamic NAT With Overload
۱۷۳	۵.۵.۴ Overlapping
۱۷۴	۵.۶ جدول NAT
۱۷۴	۵.۷ نحوه ترجمه آدرس مبدا در NAT
۱۷۵	۵.۸ نحوه پیکربندی Static NAT

۱۷۵	۵.۸.۱ فعال کردن Static NAT
۱۷۵	۵.۸.۲ تعیین Inside Interface
۱۷۵	۵.۸.۳ تعیین Outside Interface
۱۷۶	۵.۸.۴ مثال Static NAT
۱۷۶	۵.۹ نحوه پیکربندی Dynamic NAT
۱۷۷	۵.۹.۱ لیست آدرس های Valid
۱۷۷	۵.۹.۲ فعال کردن Dynamic NAT
۱۷۸	۵.۹.۳ تعیین Inside Interface
۱۷۸	۵.۹.۴ تعیین Outside Interface
۱۷۸	۵.۹.۵ مثال Dynamic NAT
۱۷۹	۵.۱۰ Nat داینامیک با سر بار
۱۸۰	۵.۱۰.۱ Dynamic NAT With Overload پیکربندی
۱۸۰	۵.۱۰.۲ فعال کردن Dynamic NAT With Overload
۱۸۰	۵.۱۰.۳ تعیین Inside Interface
۱۸۱	۵.۱۰.۴ تعیین Outside Interface
۱۸۱	۵.۱۰.۵ مثال Dynamic NAT With Overload
۱۸۲	۵.۱۱ عملکرد روتر در Dynamic NAT With Overload
۱۸۲	۵.۱۲ پاک کردن رکورد در NAT Table
۱۸۳	۵.۱۳ نمایش اطلاعات مربوط به NAT
۱۸۳	۵.۱۴ عدم رکورد در NAT Table
	۵.۱۵ امنیت ۱۸۳
۱۸۴	۵.۱۶ پیاده سازی NAT در ویندوز سرور ۲۰۰۳
۱۸۵	۵.۱۶.۱ تنظیم NAT
۱۸۶	۵.۱۷ شبکه مجازی VPN
۱۸۹	۵.۱۸ معایب و مزایا
۱۹۰	۵.۱۹ تونل کشی
۱۹۲	۵.۱۹.۱ هویت شناسی
۱۹۲	۵.۱۹.۲ فایروال
۱۹۳	۵.۱۹.۳ رمزنگاری
۱۹۵	۵.۲۰ معماری VPN شبکه‌ی محلی به شبکه‌ی محلی
۱۹۶	۵.۲۰.۱ شبکه‌ی محلی به شبکه‌ی محلی مبتنی بر اینترنت

۱۹۶	۵.۲۰.۲ شبکه‌ی محلی به شبکه‌ی محلی مبتنی بر اکسترانت
۱۹۶	۵.۲۰.۳ میزبان به شبکه‌ی محلی
۱۹۷	۵.۲۰.۴ میزبان به میزبان
۱۹۸	۵.۲۰.۵ تکنولوژی‌های VPN
۱۹۹	۵.۲۱ قراردادهای پیاده‌سازی VPN
۱۹۹	۵.۲۱.۱ رده‌ی بسته‌گرا
۱۹۹	۵.۲۱.۲ رده‌ی کاربردگرا
۲۰۰	۵.۲۱.۳ SSH قراردادهای
۲۰۰	۵.۲۱.۴ SOCKS قرار داد
۲۰۱	۵.۲۲ نتیجه‌گیری
۲۰۱	۵.۲۳ پرسش و تحقیق
۲۰۲	۵.۲۴ منابع و مراجع
۲۰۴	۶. سرور امنیتی AAA
۲۰۴	۶.۱ خلاصه بخش
	۶.۲ مقدمه ۲۰۴
۲۰۵	۶.۳ تایید، شما چه کسی هستید؟
۲۰۶	۶.۳.۱ فعال نمودن Authentication
۲۰۶	۶.۴ مجوز، مجاز به انجام چه کاری هستید؟
۲۰۸	۶.۴.۱ فعال نمودن Authorization
۲۰۸	۶.۵ حسابداری: چه کارهایی را انجام داده‌اید؟
۲۰۸	۶.۵.۱ فعال نمودن Accounting
۲۰۹	۶.۶ مزایای استفاده از AAA
۲۰۹	۶.۷ مفهوم دسترسی
۲۱۰	۶.۸ روش‌های Authentication
۲۱۰	۶.۸.۱ پروتکل PAP
۲۱۰	۶.۸.۲ پروتکل CHAP
۲۱۱	۶.۸.۳ پروتکل MSCHAP
۲۱۱	۶.۸.۴ پروتکل EAP
۲۱۱	۶.۹ استانداردهای AAA سرور
۲۱۱	۶.۹.۱ استاندارد RADIUS

۲۱۴	۶.۹.۲ استاندارد TACACS
۲۱۴	۶.۱۰ نحوه عملکرد مدل AAA
۲۱۵	۶.۱۱ عملکرد پروتکل های TACACS و RADIUS
۲۱۶	۶.۱۲ تصدیق کاربر
۲۱۶	۶.۱۳ مجوز دسترسی
۲۱۷	۶.۱۴ فرآیند تصدیق کاربری AAA
۲۱۸	۶.۱۵ فرآیند اعطای مجوز AAA
۲۱۸	۶.۱۵.۱ مجوز دسترسی TACACS
۲۱۹	۶.۱۵.۲ اخذ مجوز دسترسی توسط پروتکل RADIUS
۲۱۹	۶.۱۶ فرآیند حسابداری AAA
۲۲۰	۶.۱۷ مقایسه TACACS و RADIUS
۲۲۱	۶.۱۸ صفات RADIUS
۲۲۲	۶.۱۹ کلید رمزگذاری
۲۲۲	۶.۲۰ گروه ها و توارث بین آنها
۲۲۳	۶.۲۱ بانک اطلاعاتی کاربران
۲۲۳	۶.۲۱.۱ بانک های اطلاعاتی با ساختار سلسله مراتبی
۲۲۴	۶.۲۲ کنترل دستی اضافه
۲۲۴	۶.۲۳ امکانات اضافی هنگام حالات مشکوک
۲۲۵	۶.۲۴ امکانات اضافی برای حساب کاربران
۲۲۵	۶.۲۴.۱ پیکر بندی AAA برای قطع ارتباط کاربر
۲۲۶	۶.۲۵ قطع ارتباط کاربر
۲۲۶	۶.۲۶ سرویس دهنده کمکی
۲۲۶	۶.۲۷ سیستم پشتیبان
۲۲۷	۶.۲۸ پیکر بندی AAA بر روی روتر
۲۲۸	۶.۲۸.۱ هویت سنجی AAA با استفاده از TACACS و RADIUS
۲۲۹	۶.۲۸.۲ پیکر بندی TACAS +
۲۳۱	۶.۲۹ نتیجه گیری
۲۳۱	۶.۳۰ پرمش و تحقیق
۲۳۲	۶.۳۱ منابع و مراجع
۲۳۴	۷ دیوار آتش

۲۳۴	۷.۱ خلاصه بخش
۲۳۴	۷.۲ مقدمه
۲۳۵	۷.۳ بخشهای شبکه به لحاظ امنیتی
۲۳۵	۷.۳.۱ تجهیزات غیر فعال
۲۳۵	۷.۳.۲ تجهیزات فعال
۲۳۶	۷.۴ قسمتهای شبکه به لحاظ حفاظت امنیتی
۲۳۶	۷.۵ نحوه تقسیم بندی شبکه و مفهوم Firewall
۲۳۷	۷.۵.۱ تعریف Firewalls
۲۳۸	۷.۵.۲ تاریخچه ی Firewalls
۲۳۹	۷.۵.۳ محل قرار گرفتن دیوار آتش
۲۳۹	۷.۶ دسته بندی فایر وال
۲۳۹	۷.۶.۱ فایروال سخت افزاری
۲۴۰	۷.۶.۲ فایروال نرم افزاری
۲۴۰	۷.۶.۳ مزایا و معایب فایروال نرم افزاری
۲۴۱	۷.۶.۴ ترکیب سخت افزار و نرم افزار فایروال
۲۴۱	۷.۶.۵ فایروال NAT ساده
۲۴۲	۷.۶.۶ فایروالهای با ویژگی Stateful Packet Inspection
۲۴۲	۷.۷ انواع Firewall ها از نظر عملکرد
۲۴۲	۷.۷.۱ دیواره‌های آتشین فیلترینگ بسته ای
۲۴۲	۷.۷.۲ دیواره آتش فیلترینگ بسته مبتنی بر حالت
۲۴۲	۷.۷.۳ دیواره‌های آتشین پراکسی
۲۴۵	۷.۸ مبانی طراحی دیوار آتش
۲۴۷	۷.۸.۱ لایه اول دیوار آتش
۲۴۸	۷.۸.۲ لایه دوم دیوار آتش
۲۴۹	۷.۸.۳ لایه سوم دیوار آتش
۲۴۹	۷.۹ اجزای جانبی یک دیوار آتش
۲۵۰	۷.۹.۱ واسط محاوره‌ای و ساده ورودی / خروجی
۲۵۰	۷.۹.۲ فایروال NAT
۲۵۱	۷.۹.۳ فیلترینگ پورت‌ها
۲۵۲	۷.۹.۴ ناحیه غیرنظامی
۲۵۳	۷.۹.۵ فورواردینگ پورت‌ها

۲۵۵	۷.۱۰. توپولوژی های فایروال
۲۵۵	۷.۱۰.۱. Dual-Homed فایروال
۲۵۶	۷.۱۰.۲. Two-Legged فایروال
۲۵۸	۷.۱۰.۳. Three-Legged فایروال
۲۵۹	۷.۱۱. فایروال و نحوه کنترل ترافیک
۲۵۹	۷.۱۱.۱. فیلتر نمودن بسته های اطلاعاتی
۲۵۹	۷.۱۱.۲. Proxy سرویس
۲۵۹	۷.۱۲. مشخصه های مهم یک فایروال قوی
۲۶۰	۷.۱۳. امنیت فایروال
۲۶۱	۷.۱۳.۱. امنیت سیستم عامل فایروال
۲۶۱	۷.۱۳.۲. دسترسی امن به فایروال جهت مقاصد مدیریتی
۲۶۱	۷.۱۴. معایب عمومی Firewall ها
۲۶۲	۷.۱۵. پراکسی سرور
۲۶۲	۷.۱۵.۱. عملکردهای پراکسی سرور
۲۶۴	۷.۱۶. نتیجه گیری
۲۶۵	۷.۱۷. پرسش و تحقیق
۲۶۵	۷.۱۸. منابع و مراجع
۲۶۸	ضمیمه اول
۲۶۸	۸. استاندارد سیستم مدیریت امنیت اطلاعات
	۸.۱. مقدمه ۲۶۸
۲۶۸	۸.۲. سیاست ها و دستورالعمل های امنیتی
۲۶۸	۸.۳. تکنولوژی و محصولات امنیتی
۲۶۹	۸.۴. عوامل اجرایی
۲۶۹	۸.۵. خانواده استانداردهای ISO27000
۲۶۹	۸.۵.۱. موارد مطروحه در این استاندارد ها
۲۷۰	۸.۶. معرفی خانواده استاندارد های ISO27000
۲۷۱	۸.۷. استاندارد BS 7799
۲۷۲	۸.۸. استاندارد BS 7799
۲۷۳	۸.۹. استاندارد ISO/IEC 27006

۲۷۳		ISO/IEC 27005	۸.۱۰ استاندارد
۲۷۳		ISO/IEC 27011	۸.۱۱ استاندارد
۲۷۴		ISO/IEC 27004	۸.۱۲ استاندارد
۲۷۴		ISO/IEC 27003	۸.۱۳ استاندارد
۲۷۴		ISO/IEC 27007	۸.۱۴ استاندارد
۲۷۵		ISO 27001	۸.۱۵ استاندارد
۲۷۷		ISO/IEC 27001:2005	۸.۱۶ استاندارد
۲۷۷		۲۷۰۰۱	۸.۱۷ تاریخچه استاندارد
۲۷۸		۲۷۰۰۱	۸.۱۷.۱ بندهای استاندارد
۲۸۰		۹. ضمیمه دوم: منابع اینترنتی	
۲۸۱		۱۰. ضمیمه سوم: واژگان و عبارات (فارسی به انگلیسی)	
۳۰۲		۱۱. ضمیمه چهارم: واژگان و عبارات (انگلیسی به فارسی)	
۳۱۸		۱۲. ضمیمه پنجم: فهرست علائم اختصاری	