INSO-ISO-IEC

27033-5

1st. Edition
Identical with
ISO/IEC 27033-5:
2013
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ایران-ایزو-آی ای سی

۲۷۰۳۳-۵

چاپ اول

۱۳۹۲

فناوری اطلاعات – فنون امنیتی- امنیت شبکه – قسمت ۵: ارتباطات امن‌ساز سرتاسر شبکه‌ها با استفاده از شبکه‌های خصوصی مجازی(VPNs)

Information Technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization

2 - International Electrotechnical Commission

3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- فنون امنیتی- امنیت شبکه – قسمت ۵: ارتباطات امن‌ساز سرتاسر شبکه‌ها با استفاده از شبکه‌های خصوصی مجازی (VPNs) »

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤل سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
ده موبد، بیژن (فوق لیسانس مدیریت فناوری اطلاعات)	کارشناس گروه راهبری امنیت اطلاعات شرکت خدمات انفورماتیک
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران داده آرای سپاهان
سراج زاده، سید هادی (فوق لیسانس فناوری اطلاعات)	پژوهشگر دانشگاه شهید بهشتی
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
سوزنگر، علی (لیسانس مهندسی کامپیوتر)	رئیس هیأت مدیره شرکت اینفوامن
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات

ناظمی، اسلام
(دکترای مهندسی کامپیوتر)
استادیار دانشگاه شهید بهشتی

نصیری آسایش، حمید رضا
(فوق لیسانس مهندسی فناوری اطلاعات)
پژوهشگر دانشگاه شهید بهشتی

یوسف زاده، سمیرا
(فوق لیسانس مهندسی فناوری اطلاعات)
پژوهشگر دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی - امنیت شبکه – قسمت پنجم: ارتباطات امن‌ساز سرتاسر شبکه‌ها با استفاده از شبکه‌های خصوصی مجازی)» که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و بیست و سومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۲/۱۱/۲۸ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 27033-5: 2013, Information technology — Security techniques — Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

فناوری اطلاعات – فنون امنیتی – امنیت شبکه قسمت ۵: ارتباطات امن‌ساز سرتاسر شبکه‌ها با استفاده از شبکه‌های خصوصی مجازی(VPNs)[1]

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنماهایی برای انتخاب، پیاده‌سازی و پایش کنترل‌های فنی لازم در تامین امنیت شبکه با استفاده از ارتباطات شبکه‌های خصوصی مجازی جهت اتصال متقابل شبکه‌ها و اتصال کاربران دور به شبکه‌ها است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات - الزمات

۲-۲ استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – آیین کار مدیریت امنیت اطلاعات

۲-۳ استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۸۸، فناوری اطلاعات – فنون امنیتی – مدیریت مخاطرات امنیت اطلاعات

۲-۴ استاندارد ملی ایران شماره ۱-۱۴۸۶۶: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی – امنیت شبکه – قسمت ۱: مرور کلی و مفاهیم

1 - Virtual private networks

۳ اصطلاحات وتعاریف

در ایـــن اســـتاندارد اصـــطلاحات و تعـــاریف تعیـــین شـــده در مجموعـــه اســـتاندارد ISO/IEC 7498، ISO/IEC 27000[1]، ISO/IEC 27001[2]، ISO/IEC 27002[3]، ISO/IEC 27005[4] و ISO/IEC 27033[5] به کار می‌روند.

٤ کوته‌نوشت‌ها

در این استاندارد، علاوه بر کوته‌نوشت‌های تعیین شده در استاندارد ملی ایـران بـه شـماره ۱-۱۴۸۶۶: سـال ۱۳۹۱، کوته‌نوشت‌های زیر نیز به کار می‌رود:

AH	Authentication Header	سرایند اصالت‌سنجی
ESP	Encapsulating Security Payload	پایه‌بار امنیتی پوشینه‌دارسازی
IKE	Internet Key Exchange	تبادل کلید اینترنت
IPsec	Internet Protocol Security	امنیت پروتکل اینترنت
ISAKMP	Internet Security Association and Key Management Protocol	پروتکل پیمان امنیـت اینترنـت و مـدیریت کلیدها
L2F	Layer Two Forwarding (Protocol)	هدایت لایه دوم (پروتکل)
LDP	Label Distribution Protocol	پروتکل توزیع برچسب
MPPE	Microsoft Point-to-Point Encryption	رمزبندی نقطه به نقطه مایکروسافت
MPLS	Multi-protocol Label Switching	سودهی برچسب چند پروتکلی
NAS	Network Area Storage	ذخیره‌ساز ناحیه شبکه
OSI	Open Systems Interconnection	اتصال متقابل سامانه‌های باز
PPP	Point-to-Point Protocol	پروتکل نقطه به نقطه
PPTP	Point-to-Point Tunneling Protocol	پروتکل تونل‌سازی نقطه به نقطه
SSL	Secure Sockets Layer	لایه پریزهای امن
VPLS	Virtual Private LAN Service	خدمت شبکه محلی خصوصی مجازی
VPWS	Virtual Private Wire Service	خدمت سیم خصوصی مجازی
WAN	Wide Area Network	شبکه گسترده

۱ - استاندارد بین‌المللی ISO/IEC 27000 در سال ۱۳۹۱ با شماره ملی ۲۷۰۰۰ منتشر شده است.
۲ - استاندارد بین‌المللی ISO/IEC 27001 در سال ۱۳۸۷ با شماره ملی ۲۷۰۰۱ منتشر شده است.
۳ - استاندارد بین‌المللی ISO/IEC 27002 در سال ۱۳۸۷ با شماره ملی ۲۷۰۰۲ منتشر شده است.
٤ - استاندارد بین‌المللی ISO/IEC 27005 در سال ۱۳۸۸ با شماره ملی ۲۷۰۰۵ منتشر شده است.
٥ - استاندارد بین‌المللی ISO/IEC 27033 در سال ۱۳۹۱ با شماره ملی ۱٤۸٦٦-۱ منتشر شده است.

۵ ساختار مستند

ساختار این استاندارد شامل قسمت‌های زیر است:

- مرور کلی بر VPNها (به بند ۶ مراجعه شود)
- تهدیدهای امنیتی مرتبط با شبکه‌های خصوصی مجازی (به بند ۷ مراجعه شود)
- نیازهای امنیتی استنتاج شده از تحلیل تهدیدها برای VPN (به بند ۸ مراجعه شود)
- کنترل‌های امنیتی مرتبط با سناریوهای رایج شبکه و حوزه‌های فناوری شبکه که از VPN استفاده می‌کنند (به بند ۹ مراجعه شود)
- فنون طراحی متنوع VPN (به بند ۱۰ مراجعه شود).

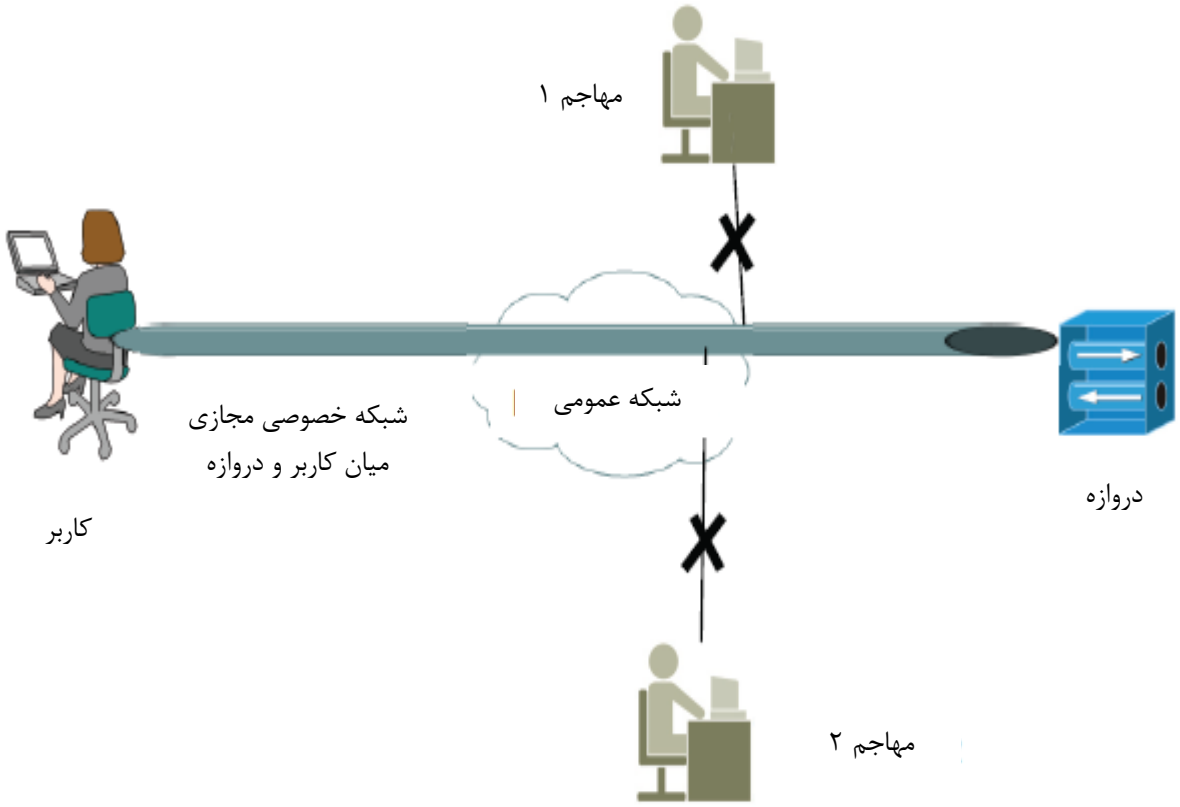
۶ مرور کلی

۶-۱ مقدمه

شبکه‌های خصوصی مجازی به عنوان وسیله‌ای برای اتصال متقابل شبکه‌ها و روشی جهت اتصال کاربران دور به شبکه‌ها رشد سریعی داشته است.

تعاریف متعددی برای شبکه‌های خصوصی مجازی وجود دارد. در ساده‌ترین شکل، شبکه‌های خصوصی مجازی سازوکاری برای برقراری یک یا چندین کانال داده امن بر روی یک شبکه یا اتصال نقطه به نقطه فراهم می‌کنند. آن‌ها به استفاده انحصاری گروه کاربری محدودی اختصاص داده می‌شوند و می‌توانند بر حسب نیاز به صورت پویا استقرار یابند یا حذف شوند. شبکه میزبان می‌تواند خصوصی یا عمومی باشد.

مثالی از یک VPN که در آن یک کانال داده امن کاربر نهایی را به یک دروازه سرتاسر شبکه عمومی متصل می‌سازد و کانال داده امن که دو دروازه را در سطح یک شبکه عمومی به هم متصل می‌سازد، در شکل ۱ نمایش داده شده است.



شکل ۱- مثال نشان‌دهنده یک VPN

دسترسی راه دور از طریق VPN بر روی یک اتصال نقطه به نقطه معمول پیاده‌سازی می‌شود. اتصال نقطه به نقطه معمول بین کاربر محلی و مکان دور ابتدا دایر می‌شود. برخی شبکه‌های خصوصی مجازی به عنوان خدمت مدیریت شده ارائه می‌شوند که در آن اتصال، مدیریت و آدرس‌دهی امن و قابل اعتماد، معادل مشخصات یک شبکه خصوصی، بر روی زیرساختی مشترک فراهم می‌شود. در نتیجه ممکن است لازم باشد کنترل‌های امنیتی اضافی جهت تقویت VPN در نظر گرفته شوند، همان گونه که در این استاندارد نشان داده می‌شود.

داده و کد در حال گذر در یک VPN باید به سازمانی که از VPN استفاده می‌کند، محدود باشد و از سایر کاربران شبکه اصلی جدا نگه داشته شود. امکان دسترسی داده و کد متعلق به سایر کاربران به کانال VPN توصیه نمی‌شود. هنگام ارزیابی میزان کنترل‌های امنیتی اضافی مورد نیاز توصیه می‌شود سطح اطمینان به محرمانگی و سایر جنبه‌های امنیتی سازمان صاحب یا ارائه کننده VPN در نظر گرفته شود.

۲-۶ انواع شبکه‌های خصوصی مجازی

همان طور که در بالا اشاره شد، روش‌های متنوعی جهت تعریف VPN وجود دارد.

از لحاظ معماری، شبکه‌های خصوصی مجازی به دو دسته تقسیم می‌شوند:

- اتصال نقطه به نقطه (به عنوان مثال، افزاره کـارخواهی کـه از راه دور از طریـق دروازه سـایت بـه شـبکه سازمان دسترسی پیدا می کد، یا دروازه یک سایت که به دروازه سایتی دیگر متصل می‌شود)

- اتصال نقطه به ابر (به عنوان مثال اتصالی که با استفاده از فناوری MPLS پیاده‌سازی شده است).

از دیدگاه مدل مرجع پایه OSI، سه نوع VPN وجود دارد:

- شبکه‌های خصوصی مجازی لایه ۲ تسهیلات شبکه داخلی شبیه‌سازی شده را ارائه می‌کنند، که در آن از اتصال‌های VPN، در حال اجرا بر روی یک شبکه میزبان (به عنوان مثال شبکه یک فراهم کننده) برای متصل کردن سایت‌های یک سازمان یا فراهم آوردن اتصال راه دور به یک سازمان استفاده می‌کنند. امکانات قابل ارائه رایج در این حوزه شامل VPWS، که یک «اتصال فقط سیمی[1]» شبکه‌سازی شده را فراهم می‌کند، یا VPLS، که یک خدمت شبکه داخلی شبیه‌سازی شده کامل‌تری را فراهم می‌کند، می‌شوند.

- شبکه‌های خصوصی مجازی لایه سه تسهیلات شبکه گسترده شبیه‌سازی شده را فراهم می‌کنند، که در این حالت نیز از شبکه‌های خصوصی مجازی در حال اجرا بر روی زیرساخت شبکه استفاده می‌شود. این امکانات سایت‌هایی با اتصال «لایه شبکه OSI» شبیه‌سازی شده، فراهم می‌کنند. جاذبه اصلی در اینجا قابلیت استفاده از شماهای آدرس‌دهی IP خصوصی بر روی یک زیرساخت عمومی است، رویه‌ای که در یک ارتباط IP عمومی «معمولی» اجازه داده نمی‌شد. در حالیکه آدرس‌های خصوصی می‌توانند از طریق ترجمه آدرس شبکه (NAT)[2] در شبکه‌های عمومی استفاده شوند، این موضوع می‌تواند استقرار و استفاده از IPsec در VPN را پیچیده کند، هر چند راه‌هایی برای دور زدن این مسئله وجود دارند.

- شبکه‌های خصوصی مجازی لایه‌های بالایی برای امن‌سازی تراکنش‌ها میان شبکه‌های عمومی استفاده می‌شوند. این شبکه‌های خصوصی مجازی معمولا یک کانال امن میان برنامه‌های کاربردی در حال ارتباط برقرار می‌کنند، و از این رو محرمانگی و یکپارچگی داده‌ها در حین تراکنش را تضمین می‌کنند. این نوع VPN ممکن است با نام VPN لایه ۴ نیز شناخته شود زیرا اتصال VPN به طور معمول بر روی TCP که یک پروتکل لایه ۴ است برقرار می‌شود.

۷ تهدیدهای امنیتی

در آینده قابل پیش‌بینی، سازمان‌ها می‌توانند انتظار انجام حملات پیچیده‌ای علیه سـامانه‌هـای خـود داشـته باشند. تلاش‌ها برای دسترسی غیرمجاز می‌تواند از روی بدخواهی باشند، به عنوان مثـال سـبب حملـه انکـار خدمات (DOS)[3] شوند، جهت سوءاستفاده از منابع، یا دسترسی به اطلاعات با ارزش باشد.

به طور کلی، تهدیدها علیه یک VPN می‌تواند در قالب نفوذها یا DOS باشد.

1 - Wires only connection
2 - Network address translation
3 - Denial of service

نفوذها هنگامی رخ می‌دهند که یک عامل بیرونی یا مجرم بدخواه کنترل بخشی از شبکه شما را به دست می‌گیرد؛ این می‌تواند یک رایانه یا افزاره شبکه دیگری (از جمله افزاره‌های سیار) باشد.

نفوذها ممکن است از هر مکانی که به شبکه دسترسی دارد رخ دهد. این حملات می‌تواند از شبکه‌های خصوصی مجازی دیگر، اینترنت یا خود هسته ارائه کننده خدمات نشات بگیرند. حفاظت در برابر این نوع حملات از قابلیت پالایش تردد ناخواسته از منابع ناخواسته در نقاط ورودی شبکه ممکن می‌شود. یک مثال رایج نفوذ دسترسی غیرمجاز به تونل امن توسط یک هستار غیرمجاز است.

این موضوع می‌تواند در برخی مدل‌های طراحی VPN که فاقد استقرار مرکزی هستند دشوار باشد زیرا تمامی سایت‌ها بدون کنترل تردد به یکدیگر متصل می‌شوند.

حملات DOS نوع دیگری تهدید علیه یک VPN هستند. حملات DOS و نفوذها هر دو می‌توانند از یک VPN دیگر، اینترنت یا هسته ارائه کننده خدمات صورت گیرند. تفاوت اصلی میان این دو نوع حمله این است که برای حملات DOS مهاجم نیاز دارد به برخی از تجهیزات شما دسترسی پیدا کند یا کنترل آن را به دست گیرد.

حملات DOS علیه افزاره‌های ارائه کننده خدمات نیز می‌تواند سبب انکار خدمات به قسمت‌هایی از VPN شما شوند. با وجود اینکه محافظت از شبکه خود در برابر حملات DOS ممکن است در برخی اوقات دشوار باشد، محافظت اصلی در برابر آن‌ها به طراحی شبکه مناسب VPN بر می‌گردد.

مسائل امنیتی شبکه‌های خصوصی مجازی شامل موارد زیر می‌شوند:

- تفکیک فضای آدرس و مسیریابی بین شبکه‌های خصوصی مجازی که بر روی شبکه برچسب سوداده[1] حمل می‌شوند
- تضمین اینکه ساختار داخلی هسته شبکه برچسب سوداده برای شبکه‌های بیرونی قابل رویت نیست (به عنوان مثال محدود کردن اطلاعات در دسترس یک مهاجم بالقوه)
- ایجاد مقاومت در برابر حملات انکار خدمات
- ایجاد مقاومت در برابر حملات دسترسی غیرمجاز
- محافظت در برابر جعل برچسب (با وجود اینکه ممکن است بتوان از بیرون برچسب‌های اشتباهی را وارد شبکه برچسب سوداده کرد، به دلیل تفکیک آدرس، بسته جعلی تنها به VPN که بسته از آنجا نشات گرفته آسیب می‌رساند).

1 - Label switched network

۸ الزامات امنیتی

۸-۱ مرور کلی

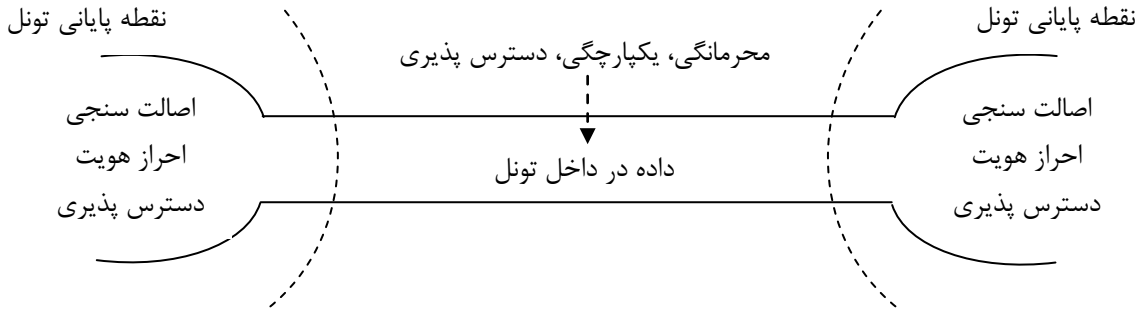
هدف امنیتی اصلی یک VPN محافظت از دسترسی غیرمجاز است. در نتیجه شبکه‌های خصوصی مجازی می‌توانند برای برآورده ساختن اهداف امنیتی گسترده‌تری به کار گرفته شوند:

- حفاظت از اطلاعات در شبکه‌ها، در سامانه‌های متصل به شبکه‌ها و خدمات استفاده شده توسط آن‌ها
- محافظت از زیرساخت پشتیبان شبکه
- محافظت از سامانه‌های مدیریت شبکه

جهت دستیابی به اهداف عنوان شده در بند فوق، شبکه‌های خصوصی مجازی باید به نحوی پیاده‌سازی شوند که موارد زیر تضمین شود:

- محرمانگی داده‌ها در انتقال بین نقاط پایانی شبکه‌های خصوصی مجازی
- یکپارچگی داده‌ها در انتقال بین نقاط پایانی شبکه‌های خصوصی مجازی
- اصالت‌سنجی کاربران و سرپرست‌های VPN
- مجوز کاربران و سرپرست‌های VPN
- دسترس پذیری نقاط پایانی VPN و زیرساخت شبکه

این به نوبه خود نشان می‌دهد که تونل‌های اصلی به کار رفته برای ساخت VPN باید به نحوی پیاده‌سازی شوند که اهداف امنیتی برآورده شوند. این اهداف به طور خلاصه در شکل ۲ نشان داده شده‌اند.



شکل ۲- نگاشت الزامات امنیتی عمومی شبکه‌های خصوصی مجازی بر تونل اصلی

هر یک از این الزامات در زیر به تفصیل بررسی می‌شوند.

در بند ۹ نیز در مورد انواع کنترل‌های امنیتی به کار گرفته شده جهت پیاده‌سازی شبکه‌های خصوصی مجازی امن بحث می‌شود.

۸-۲ محرمانگی

محرمانگی داده و کد در زمان انتقال در تونل نباید به خطر بیافتد. استفاده از فناوری‌های تونل ممکن است بر این دلالت داشته باشد که داده و کد در زمان انتقال برای سایر کاربران شبکه قابل رویت نیستند. با این حال، این بدان معنا نیست که تردد، محرمانه نگه داشته می‌شود. به طور خاص، داده و کد در حال جریان در تونل‌ها در برابر بازرسی به وسیله رهگیرها و تحلیل‌گرهای داده حفاظت نمی‌شوند. در نتیجه حفاظت از محرمانگی داده و کد در حین انتقال در تونل‌ها به طور اساسی به احتمال وقوع چنین بازرسی‌هایی بستگی دارد. این به نوبه خود عاملی از میزان اعتماد موجود در شبکه‌های اصلی پشتیبان شبکه‌های خصوصی مجازی است، که بسته به مالک شبکه انتقال متفاوت خواهد بود. اگر شبکه انتقال در یک دامنه مورد اعتماد واقع نشده باشد (برای اطلاعات بیشتر در مورد دامنه‌های اعتماد به استاندارد ملی ایران شماره ۱-۱۴۸۶۶: سال ۱۳۹۱ مراجعه شود) یا اگر داده و کدی که باید منتقل شوند حساس حساب شوند، ممکن است لازم باشد کنترل‌های امنیتی اضافی جهت حفاظت بیشتر محرمانگی به کار گرفته شوند. در چنین مواردی، توصیه می‌شود سازوکارهای تونل به کار گرفته شده از رمزبندی حمایت کنند، یا مواردی که قرار است ارسال شوند قبل از مخابره بر روی VPN به صورت برون‌خط رمزنگاشتی شوند. توصیه می‌شود امنیت نقاط پایانی تونل نیز فراموش نشود.

۸-۳ یکپارچگی

یکپارچگی داده و کد هنگام انتقال در تونل نباید به خطر بیافتد. توصیه می‌شود سازوکارهای به کار رفته جهت پیاده‌سازی تونل VPN با استفاده از فنونی مانند کدهای درستی‌سنجی پیام، کدهای اصالت‌سنجی پیام و سازوکارهای ضد بازپخش از بررسی یکپارچگی داده و کد هنگام انتقال حمایت کنند. اگر پیاده‌سازی تونل چنین محافظتی را فراهم نکند یا اگر داده و کدی که قرار است مخابره شود به نسبت حساس باشند، آن گاه توصیه می‌شود کنترل‌های حفظ یکپارچگی در سامانه‌های پایانی پیاده‌سازی شوند، به گونه‌ای که محافظت یکپارچگی به صورت انتها به انتها[1] فراهم شود.

۸-٤ اصالت‌سنجی

توصیه می‌شود اصالت‌سنجی اطلاعات در حال عبور از شبکه‌های IP عمومی میان طرفین متناظر شرکت کننده در یک VPN فراهم شود. توصیه می‌شود فرایند استقرار و اجرای تونل توسط کنترل‌های اصالت‌سنجی حمایت شود به نحوی که هر یک از پایانه‌های تونل مطمئن باشد با شریک درستی در نقطه پایانی، که ممکن است یک سامانه دسترس دور باشد، در حال ارتباط است و این که داده‌های دریافت شده از منبع مجاز صحیحی نشات گرفته‌اند.

1 - End-to-end

۸-۵ مجوز

توصیه می‌شود فرایند استقرار و اجرای تونل به وسیله کنترل‌های مجوزدهی حمایت شود و شامل فهرست‌های کنترل دسترسی (ACL)[1] باشد. این امر تضمین می‌کند که هر یک از پایانه‌های تونل با یک نقطه پایانی شریک مُجاز، که می‌تواند یک سامانه دسترس دور باشد، در حال ارتباط است و اینکه داده و کد دریافت شده از منبعی مجاز نشات گرفته‌اند.

۸-۶ دسترس پذیری

دسترس پذیری تونل‌ها، و در نتیجه VPN، تابعی از دسترس پذیری زیرساخت پشتیبان شبکه و سامانه‌های نقطه پایانی است، اما توصیه می‌شود هرگاه که امکان پذیر باشد، کنترل‌های امنیتی برای مقابله با حملات انکار خدمات که مختص سازوکارهای تونل هستند، به کارگرفته شوند.

توصیه می‌شود برای توافق‌نامه سطح خدمات خاص، تونل‌سازی متفاوت و انعطاف‌پذیر به عنوان راه‌های جایگزین بررسی شوند.

۸-۷ امنیت نقطه پایانی تونل

توصیه می‌شود الزامات امنیتی برای نقاط پایانی VPN نیز در نظر گرفته شوند. به طور معمول، توصیه می‌شود هر نقطه پایانی VPN تضمین کند که تنها تردد شبکه کنترل شده بین شبکه میزبان و VPN برقرار شود. این معمولا بر غیرفعال سازی مسیریابی، و حداقل استفاده از فناوری پالایش بسته[2] یا دیواره آتش دلالت دارد. برای اطلاعات بیشتر به بند ۱۰-۴-۲ (امنیت نقطه پایانی) و ۱۰-۴-۳ (امنیت پایان‌دهی)[3] مراجعه شود.

۹ کنترل‌های امنیتی

۹-۱ جنبه‌های امنیتی

با وجود اینکه تونل‌ها از کاربران معمول شبکه پنهان هستند، اما نامرئی نیستند و در نتیجه به طور ذاتی امن نیستند. فرایند افراز مقدماتی (به مدارهای مجازی یا مسیرهای برچسب سوداده[4]) یا پوشینه‌دارسازی به کار رفته جهت ساخت یک تونل از ممیزی‌های مصمم توسط مهاجمان به وسیله تحلیل‌گرها یا رهگیرهای[5] شبکه محافظت نشده است. اگر تونل با استفاده از رمزبندی پیاده‌سازی نشده باشد، آنگاه مهاجم قادر خواهد بود به تردد دست یابد، و حتی اگر رمزبندی به کار گرفته شود، وجود تونل و نقاط پایانی آن باز هم پنهان نخواهد ماند.

علاوه بر این، ممکن است نقاط پایانی تونل نیز الزاما از دسترسی غیرمجاز منطقی یا فیزیکی محافظت شده نباشند. از این رو به منظور دستیابی به پیاده‌سازی امن VPN لازم است که با توجه به سیاست امنیتی

1 - Access control list
2 - Packet filter
3 - Termination security
4 - Label-switched paths
5 - Interceptor

سازمان و سطوح پذیرش مخاطره کنترل‌های امنیتی را در تونل‌ها اعمال کرد. این به سیاست امنیتی سازمان بر می‌گردد که چنین آسیب‌پذیری‌هایی قابل قبول هستند یا نه.

یادآوری- اگر داده رمزبندی شود، حضور جریان داده می‌تواند حتی به همان میزان خود داده که در حال مکاتبه است، مهم باشد. به عنوان مثال اگر نقاط پایانی VPN قابل تشخیص باشند محل کاربر نیز قابل تشخیص خواهد بود. این تهدیدی برای حریم خصوصی فرد محسوب می‌شود و در مورد مراجع قانونی یا نظامی ممکن است ماموریت آن‌ها را به خطر بیاندازد.

۹-۲ مدارهای مجازی

کنترل‌های امنیتی که کانال‌های امن اصلی را برقرار می‌کند ممکن است از مدارهای مجازی در تجهیزات مخابراتی گسترده مرسوم، مانند خطوط اجاره‌ای، با استفاده از فناوری‌هایی مانند رله‌ی قاب[1] یا ATM استفاده کنند. در این فناوری‌ها، شبکه‌های اصلی نیز ذاتا امن هستند تا حدی که متصدیان مخابرات تفکیک میان تجهیزات خط اجاره‌ای برای مشترکان خصوصی و تدارک خدمات دسترسی به اینترنت عمومی را حفظ می‌کند. فناوری به کار رفته در مدارهای مجازی به طور ذاتی میزانی از محرمانگی تونل اما نه امنیت کامل را اعطا می‌کند. یک VPN که بر روی چنین مدارهای مجازی سنتی ساخته شده باشد نسبتا غیر قابل نفوذ پنداشته می‌شود، زیرا نفوذها و حملات امنیتی به طور معمول نیاز دارند از درون هسته شبکه ارائه کننده نشات بگیرند.

۱۰ فنون طراحی

۱۰-۱ مرور کلی

شبکه‌های خصوصی مجازی از منابع سامانه یک شبکه فیزیکی ساخته می‌شوند، به عنوان مثال با استفاده از رمزبندی یا تونل کردن پیوندهای شبکه مجازی سرتاسر شبکه واقعی.

شبکه‌های خصوصی مجازی می‌توانند به طور کامل درون یک شبکه خصوصی تحت کنترل سازمان، در میان شبکه‌ها در یک دامنه عمومی، یا میان ترکیبی از دو حالت فوق پیاده‌سازی شوند. در حالی که ساخت شبکه-های خصوصی مجازی بر روی شبکه‌های گسترده خصوصی موجود امکان‌پذیر است، دسترسی عمومی به اینترنت با قیمت به نسبت پایین سبب شده است در بسیاری از کاربردها این سامانه شبکه عمومی یک وسیله مقرون به صرفه برای پشتیبانی شبکه‌های خصوصی مجازی گسترده و شبکه‌های خصوصی مجازی دسترسی دور به نظر برسد.

در مقابل، کانال‌ها می‌توانند با به کار گرفتن کانال‌های امنی دایر شوند که با استفاده از تونل‌های در حال جریان بر روی شبکه‌های ارائه دهنده خدمات اینترنت ساخته شده‌اند. در این حالت، اینترنت عمومی در عمل سامانه انتقال اصلی است. این بر میزان عدم قطعیت بیشتری برای محرمانگی VPN دلالت دارد. تونل یک مسیر داده بین افزاره‌های شبکه شده است، که در سطح زیرساخت یک شبکه موجود استقرار یافته است. این تونل‌ها برای عملیات شبکه معمول شفاف هستند و در اکثر اهداف کاربردی می‌توانند مانند ارتباطات شبکه

1 - Frame relay

معمول استفاده شوند. آن‌ها می‌توانند به راحتی بر طبق نیاز فعال و غیرفعال شوند بدون اینکه تغییری در زیرساخت فیزیکی شبکه اصلی ایجاد شود. از این رو، یک VPN که با تونل‌ها ایجاد شده است بیش از شبکه مبتنی بر پیوندهای فیزیکی انعطاف‌پذیر است.

تونل‌ها می‌توانند با استفاده از موارد زیر ایجاد شوند:

- مدارهای مجازی
- سودهی برچسب
- پوشینه‌دارسازی پروتکل[1]

تونل‌هایی که با استفاده از مدارهای مجازی ایجاد شده‌اند به طور معمول در تاسیسات شبکه گسترده مرسوم به صورت خطوط اجاره شده با استفاده از فناوری‌های سودهی[2] (به عنوان مثال رله‌ی قاب یا ATM) استقرار می‌یابند. این فناوری‌ها تضمین می‌کنند که جریان‌های داده میان تونل‌ها از هم جدا هستند.

سودهی برچسب روش دیگری برای ایجاد تونل‌ها است. به تمامی بسته‌های داده در حال جریان در یک تونل یک برچسب شناسایی اختصاص داده می‌شود. این برچسب تضمین می‌کند که بسته‌هایی با برچسب متفاوت از مسیر مشخص شده در شبکه بیرون نگه داشته می‌شوند.

با وجود اینکه فنون به کار گرفته شده برای تونل‌سازی تفکیک مناسب داده در حال جریان میان تونل‌ها و شبکه‌های اصلی را تضمین می‌کنند، آن‌ها الزامات محرمانگی عمومی را برآورده نمی‌سازند. اگر محرمانگی مورد نیاز باشد، برای تامین سطح امنیت خواسته شده لازم است از فناوری‌های رمزنگاشتی استفاده شود.

تونل‌های VPN می‌توانند در لایه‌های مختلف مدل OSI ایجاد شوند. مدارهای مجازی تونل‌ها را در لایه ۲ ایجاد می‌کنند. فنون سودهی برچسب امکان ایجاد تونل‌ها در لایه‌های ۲ و ۳ را فراهم می‌کنند. پوشینه-دارسازی پروتکل می‌تواند در تمامی لایه‌ها به جز لایه فیزیکی استفاده شود (اکثر پیاده‌سازی‌های آن بر روی لایه‌های ۳ به بالا است). رمزبندی می‌تواند جهت فراهم کردن یک سطح امنیتی بیشتر برای تونل‌های مبتنی بر مدارهای مجازی، پوشینه‌دارسازی پروتکل و سودهی برچسب استفاده شود.

تونل‌ها همچنین می‌توانند با استفاده از فن پوشینه‌دارسازی پروتکل ایجاد شوند که به موجب آن واحد داده یک پروتکل در پروتکل دیگری پوشینه‌دار و حمل می‌شود. برای مثال، یک بسته IP با استفاده از روش تونل پروتکل IPsec ESP پوشینه‌دار می‌شود. یک سرایند IP اضافی در بسته تعبیه شده و سپس بر روی یک شبکه IP ارسال می‌شود.

1 - Protocol encapsulation
2 - Switching technologies

۱۰-۲ جنبه‌های تنظیم مقررات و قانون‌گذاری

توصیه می‌شود الزامات امنیتی مقرراتی و قانونی مرتبط به اتصالات شبکه و استفاده از VPN تعریف شده توسط ارگان‌های تنظیم مقررات و قانون‌گذاری (از جمله نهادهای دولتی) در کشورهایی که VPN قرار است استفاده شود در نظر گرفته شوند.

اینها شامل مقررات و قانون‌های مرتبط با موارد زیر می‌شود:

- محافظت حریم خصوصی/داده
- استفاده از فناوری رمزنگاشتی
- مدیریت/حاکمیت مخاطره عملیاتی

۱۰-۳ جنبه‌های مدیریت VPN

هنگام بررسی استفاده از شبکه‌های خصوصی مجازی توصیه می‌شود تمامی افرادی که مسئولیت‌هایی در ارتباط با VPN دارند در خصوص الزامات کسب و کار و مزایای آن توجیه باشند. علاوه بر این، آن‌ها و همه کاربران دیگر VPN باید از تهدیدهای امنیتی مرتبط با چنین اتصالی و نواحی کنترلی وابسته به آن آگاه باشند. الزامات کسب و کار و مزایای آن به احتمال زیاد بر بسیاری از تصمیمات گرفته شده و اقدامات انجام شده در فرایند بررسی اتصالات VPN، شناسایی نواحی کنترل احتمالی، و در نهایت انتخاب، طراحی، پیاده-سازی و نگهداری کنترل‌های امنیتی تاثیر گذار خواهند بود. از این رو، لازم است الزامات و مزایای کسب و کار در تمامی فرایند انتخاب در نظر گرفته شوند.

۱۰-٤ جنبه‌های معماری VPN

۱۰-٤-۱ مرور کلی

در انتخاب VPN توصیه می‌شود جنبه‌های معماری زیر لحاظ شوند:

- امنیت نقطه پایانی
- امنیت پایان‌دهی اتصال
- محافظت در برابر نرم‌افزارهای مخرب
- اصالت‌سنجی
- سامانه شناسایی و جلوگیری نفوذ
- دروازه‌های امنیتی (شامل دیوارهای آتش)
- طراحی شبکه
- اتصال‌های دیگر
- تونل‌سازی مجزا
- رویدادنگاری ممیزی‌ها و پایش شبکه
- مدیریت آسیب‌پذیری فنی
- رمزبندی مسیر شبکه عمومی

هر یک از این موارد در زیر به طور خلاصه بحث شده می‌شوند.

۱۰-٤-۲ امنیت نقطه پایانی

وظیفه VPN فراهم کردن کانال ارتباط امن در گستره رسانه‌های شبکه است. هنگامی که VPN مستقر می‌شود پایش بر محتوای جریان داده غیرممکن است. اگر هر یک از نقاط پایانی به خطر بیافتد، این مسئله می‌تواند به نشست‌ها در سطح VPN گسترش پیدا کند. امنیت نقطه پایانی نه تنها به خود افزاره‌ها مرتبط می‌شود، بلکه برنامه‌های کاربردی روی این افزاره‌ها و جنبه‌های فرایندی/فیزیکی مربوط به استفاده از آن‌ها را نیز در بر می‌گیرد.

به منظور اجرای آسان کنترل امنیت نقطه پایانی توصیه می‌شود تعداد نقاط پایانی انبوه[1] به حداقل رسانده شود.

برخی افزاره‌های کاربری نقطه پایانی (مانند تجهیزات پردازشی موبایل/دورکاری) که برای دسترسی از دور استفاده می‌شوند ممکن است تحت مدیریت کنترل مشابه VPN نباشند. این افزاره‌ها ممکن است به شبکه-های متفاوتی وصل باشند، به عنوان مثال برای دسترسی به اینترنت و شبکه خصوصی سازمان در زمان‌های متفاوت. این شبکه‌ها ممکن است تهدیدات اضافی را مطرح کنند و توصیه می‌شود جهت تضمین استفاده از کنترل‌های امنیتی مناسب ملاحظاتی در نظر گرفته شود. توصیه می‌شود هنگام بررسی امنیت افزاره‌های نقطه پایانی این‌چنینی کنترل‌های امنیتی مطابق استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ لحاظ شوند، از جمله مواد مرتبط به موارد زیر:

- امنیت تجهیزات
- محافظت در برابر کد مخرب و سیار
- اطلاع، آموزش و تعلیم افرادی که از این افزاره‌ها استفاده می‌کنند در خصوص امنیت اطلاعات
- مدیریت آسیب‌پذیری فنی افزاره‌ها و فناوری VPN مرتبط

توصیه می‌شود سایر کنترل‌ها مانند پالایش بسته یا دیوار آتش نیز لحاظ شوند.

۱۰-٤-۳ امنیت پایان‌دهی

یکی از عوامل کلیدی تاثیرگذار بر امنیت یک VPN نحوه پایان‌دهی آن در هر پایانه است. اگر پایان‌دهی به طور مستقیم در هسته نقطه پایانی صورت می‌گیرد (به عنوان مثال، در ناحیه امن یک شبکه)، امنیت مستقیما به امنیت شریک راه دور وابسته است. اگر نقطه پایان‌دهی در ناحیه ناامن باشد، این احتمال وجود دارد که ارتباطات به آسانی جعل شوند.

روش استاندارد برای پایان‌دهی VPN استقرار نقاط پایانی اختصاصی VPN در شبکه‌های پیرامونی است که قابلیت پردازش بیشتر اطلاعات از VPN را ممکن می‌سازد (به عنوان مثال، در تصمیم‌گیری در خصوص اعطا

1 - Aggregating endpoints

دسترسی به برنامه‌های کاربردی/سامانه‌ها در ناحیه امن). به طور بالقوه، پایان‌دهی در ناحیه میانی کنترل بیشتر بر VPN و کاربران آن را ممکن می‌سازد.

یادآوری – ناحیه میانی با عنوان شبکه‌های پیرامونی یا منطقه حائل (DMZ)[1] در استاندارد ISO/IEC 27033-4 بحث می‌شود.

در هر حالت، توصیه می‌شود نقطه پایانی VPN قبل از دادن دسترسی اعتبار هستار (به عنوان مثال کاربر یا افزاره) را بررسی کند. این کار اضافه بر اصالت‌سنجی انجام شده بین نقاط پایانی برای برقراری پیوند VPN است. برای مثال، این موضوع برای کاربران به طور معمول شامل یک شناسه کاربری و اسم‌رمز می‌شود و ممکن است مستلزم استفاده از نوعی اصالت‌سنجی اضافه باشد، به عنوان مثال فناوری نمود افزار[2]، کارت یا زیست‌سنجشی (که به اصطلاح «اصالت‌سنجی قوی» نامیده می‌شود).

۱۰-٤-٤ محافظت در برابر نرم‌افزارهای مخرب

هنگامی که سامانه‌های اطلاعاتی فاقد نرم‌افزارهای مخرب نشان داده شوند، تنها راه ورود چنین کدی از طریق داده‌هایی است که توسط گیرنده اجرا می‌شوند (مانند کد). بسیاری از برنامه‌ها، کدجاسازی شده[3] در داده که جزئی به نظر می‌رسند را می‌پذیرند. نقاط پایانی VPN نقاط کنترل مناسبی برای پیاده‌سازی محافظت در برابر نرم‌افزارهای مخرب فراهم می‌سازند تا ارسال چنین کدهایی را کنترل کنند.

اطلاعات بیشتر در مورد محافظت در برابر کد مخرب، شامل ویروس‌ها، کرم‌ها و تروآها، در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ شرح داده شده است.

یادآوری – توصیه می‌شود برای امنیت نقاط پایانی برای «کدهای فشار[4]» تدارک دیده شود، به خصوص هنگامیکه اطلاعات حساس ممکن است درگیر باشند. توصیه می‌شود کد فشار باز هم امکان دسترسی را جهت محافظت از کاربر نهایی به خطر افتاده فراهم کند؛ با این حال، می‌تواند رویدادنگاری و ردیابی اضافی را فعال کند و مدیریت مربوطه را در خصوص وضعیت مطلع سازد.

۱۰-٤-۵ اصالت‌سنجی

اصالت‌سنجی یکی از مراحل کلیدی در استقرار VPN است. حتما توصیه می‌شود که هر پایانه هویت خود را برای شریک نشست مورد نظرش احراز کند (به عبارت دیگر، اصالت‌سنجی متقابل لازم است). این امر می‌تواند به چندین روش انجام شود:

- کلیدهای مشترک از پیش تعیین شده، که می‌تواند راحتی را به همراه داشته باشد زیر بعد از به اشتراک‌گذاری، هیچ‌گونه مدیریت دیگری نیاز نیست. با این وجود، این روش اگر به خطر افتاده باشد می‌تواند مورد سوء استفاده قرار گیرد (به عنوان مثال حملات فرد در میانه).

- گواهی‌ها، که انعطاف‌پذیری و مقیاس‌پذیری بیشتری را فراهم می‌آورند، به خصوص اگر با پشتیبانی PKI برای ساده سازی مدیریت، فسخ و صدور مجدد کلیدها به کار گرفته شوند. اطلاعات بیشتر در مورد

1 - Demilitarized zone
2 - Token
3 - Embedded code
4 - Duress code

اصالت‌سنجی و استفاده از خدمات مبتنی بر رمزنگاشتی برای اصالت‌سنجی در ISO/IEC 11770-1 و استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ شرح داده شده است.

۱۰-٤-٦ سامانه‌های شناسایی و جلوگیری از نفوذ

توصیه می‌شود نیاز به فناوری سامانه‌های شناسایی و جلوگیری از نفوذ (IPDS)[1] در نظر گرفته شود. یک IPDS می‌تواند جهت شناسایی نفوذهای احتمالی در دو طرف VPN پیاده‌سازی شود. سپس هشدارهای سامانه شناسایی نفوذ (IDS)[2] توسط هر گونه سازوکار مناسب اعلام شده، و علاوه بر این به عنوان بخشی از دنباله ممیزی ثبت (و مدیریت) شود. باید اشاره کرد که برخی دیوارهای آتش شخصی حتی این قابلیت را دارند که به عنوان یک سامانه پیشگیری از نفوذ (IPS)[3] ساده عمل کنند و دسترسی برنامه‌های کاربردی غیرمجاز به شبکه را ممنوع سازند.
اطلاعات بیشتر در مورد IDS در ISO/IEC 27039 ارائه شده است.

۱۰-٤-۷ دروازه‌های امنیتی

توصیه می‌شود به انتخاب فناوری دروازه امنیتی مناسب (شامل دیوار آتش) جهت پشتیبانی از توسعه VPN به دقت توجه شود.
اطلاعات در مورد دروازه‌های امنیتی (شامل دیوارهای آتش) در ISO/IEC 27033-4 ارائه شده است.

۱۰-٤-۸ طراحی شبکه

توصیه می‌شود در طراحی شبکه برای هر یک از دو سمت VPN از اهداف امنیت پایان‌دهی اتصال، که در بالا بحث شد پشتیبانی شود. به طور خاص، توصیه می‌شود VPN به طور معمول در یک دیوار آتش بیرونی (به عنوان مثال در پیرامون شبکه) یا در درون DMZ خودش خاتمه یابد.

۱۰-٤-۹ اتصال‌های دیگر

توصیه می‌شود به هر گونه اتصال اضافی از یک نقطه پایانی VPN توجه شود. اگر اتصال‌های اضافی در هر یک از نقاط پایانی VPN وجود داشته باشند، احتمال دارد که یک خطر امنیتی شروع شده از آن کانال به سامانه‌های محلی و از طریق VPN به سامانه‌های دور حمله کند. این احتمال می‌تواند با طراحی صحیح شبکه و استفاده از دیوارهای آتش کاهش یابد. با این وجود، موثرترین کنترل این است که هیچ‌گونه اتصال غیرضروری وجود نداشته باشد. این ملاحظه در هنگام وجود مودم‌ها در سامانه‌های دور/خانگی اهمیت ویژه‌ای دارد.
توصیه می‌شود به اتصال میان شبکه‌های سازمان و سازمان‌های طرف سوم که خدماتی مانند پشتیبانی و عیب‌یابی فراهم می‌کنند، توجه ویژه‌ای شود. توصیه می‌شود کنترل‌های امنیتی برای محیط ارائه کننده

1 - Intrusion prevention and detection system
2 - Intrusion detection system
3 - Intrusion prevention system

خدمات به عنوان بخشی از توافقات پروتکلی استقرار یابد. توصیه می‌شود چنین کنترل‌هایی یک محیط منطقی و فیزیکی مجزا از سایر عملیات ارائه کننده خدمات و محیط‌های مشتری را تضمین کنند.

۱۰-٤-۱۰ تونل‌سازی مجزا

توصیه می‌شود هر جا عملی است از تونل‌سازی مجزا پرهیز شود. تونل‌سازی مجزا به قابلیت یک اتصال منفرد (معمولا اینترنت) در پشتیبانی از VPN و یک اتصال دیگر (VPN یا سایر اتصالات) اشاره می‌کند. در این وضعیت، این خطر وجود دارد که امنیت شبکه راه دور توسط حملاتی که از طریق تونل دیگر صورت می‌گیرند به خطر بیافتد؛ مشابه یک رایانه شخصی با دو کارت شبکه که مسیریابی میان دو شبکه را انجام می‌دهند. به طور کلی، می‌توان از طریق «حاکم کردن» محصولات VPN بر اتصال شبکه از تونل‌سازی مجزا دوری کرد.

۱۰-٤-۱۱ رویدادنگاری ممیزی و پایش شبکه

توصیه می‌شود راه حل VPN انتخاب شده مشابه تمامی فناوری‌های امنیتی دیگر رویدادنگاری ممیزی مناسب را برای تحلیل اقدامات انجام شده در نقاط پایانی نگه دارد. همانند سایر رویدادنگاری‌های ممیزی تولید شده توسط شبکه، توصیه می‌شود رویدادنگاری‌های ثبت شده جهت پیدا کردن نشانه‌هایی از رویداد-های امنیتی بررسی شوند.

توصیه می‌شود برای محافظت از خود رویدادنگاری‌های ممیزی اقداماتی تضمینی، متناسب با تهدیدهای ارزیابی شده و در جهت مقابله با تحریف و سوءاستفاده، صورت پذیرد. در حالتی که رویدادنگاری‌های ممیزی قرار باشد در پیگردهای قانونی استفاده شوند یکپارچگی آن‌ها باید فراتر از شک معقول قابل اثبات باشد.

۱۰-٤-۱۲ مدیریت آسیب‌پذیری فنی

محیط‌های شبکه، همانند سایر سامانه‌های پیچیده، عاری از خطا نیستند. آسیب‌پذیری‌های فنی در مولفه-های پر کاربرد در شبکه‌ها، مانند شبکه‌های خصوصی مجازی، وجود دارند و برای آن‌ها منتشر می‌شوند. سوء استفاده از این آسیب‌پذیری‌های فنی می‌تواند تاثیر شدیدی بر امنیت VPN داشته باشد، که اغلب در حوزه-های دسترس پذیری و محرمانگی مشاهده می‌شود. از این رو توصیه می‌شود مدیریت آسیب‌پذیری فنی در تمامی افزاره‌های VPN وجود داشته باشد.

۱۰-٤-۱۳ رمزبندی مسیر شبکه عمومی

مسیریابی بر روی یک تونل ایستا از میان یک شبکه طرف سوم/غیر قابل اطمینان، VPN را در خطر تحلیل شبکه قرار می‌دهد. همانطور که در بند ۹-۱ اشاره شد، حتی اگر رمزبندی داده نیز به کار گرفته شود، وجود تونل و نقاط پایانی آن باز هم پنهان نخواهد بود.

در معماری‌های VPN که پنهان‌سازی[1] نقطه پایانی یک الزام است، کنترل‌هایی جهت پوشاندن مکان مبدا و مقصد کاربران VPN مورد نیاز هستند. پیاده‌سازی این کنترل‌ها به خودی خود چالش انگیز است زیرا اپراتور VPN بر شبکه طرف سوم/غیر قابل اطمینان کنترل ندارد. فناوری‌های خاصی وجود دارند که پنهان‌سازی IP مبدا و مقصد در درون شبکه طرف سوم را فراهم می‌سازند، به عنوان مثال پیشکارهای مجازی[2] و پروژه مسیریاب آنیون[3]. لازم است پیش از به کار گیری چنین ابزاری مستلزمات قانونی اجرای آن‌ها با ارائه کننده شبکه طرف سوم بحث و تایید شود.

۱۰-۵ ملاحظات فنی VPN

۱۰-۵-۱ پیش‌زمینه

دستیابی به پیاده‌سازی امن VPN نیازمند توجه نظام‌مند به عناصر شناسایی شده در اهداف است. به طور خاص، توصیه می‌شود جنبه‌های پیاده‌سازی زیر در نظر گرفته شوند:

- انتخاب پروتکل حامل
- سخت‌افزار در مقابل نرم‌افزار
- مدیریت افزاره VPN
- پایش امنیت VPN.

هر یک از این جنبه‌ها در زیر بحث شده است.

۱۰-۵-۲ مدیریت افزاره VPN

توصیه می‌شود افزاره‌های VPN به درستی مدیریت شوند. مدیریت افزاره VPN واژه عمومی به کار گرفته شده برای فرایند مورد نیاز جهت راه‌اندازی و پایش بر افزاره‌های VPN است. راه‌اندازی افزاره VPN شامل پیکربندی آن با تنظیمات شبکه و دسترسی درگاه/برنامه کاربردی مورد نیاز، نصب گواهی‌ها (به عنوان مثال برای شبکه‌های خصوصی مجازی لایه‌های بالایی)، و پایش شبکه مداوم بر افزاره VPN، همانند هر گونه افزاره شبکه دیگر، می‌شود. توصیه می‌شود استقرار VPN با استفاده از رسانه‌های قابل‌حمل مانند لوح‌های فشرده، دیسک‌ها و غیره با ایجاد رویدادنگاری‌های تحویل و دریافت و با اعمال محدودیت‌ها بر استفاده مجدد از رسانه‌ها مانند تاریخ یا زمان انقضا یا محدودیت بر تعداد دفعاتی که یک برنامه می‌تواند اجرا شود، کنترل شود.

1 - Obfuscation
2 - Virtual proxy
3 - The Onion Router Project

۱۰-۵-۳ پایش امنیت VPN

شبکه‌های خصوصی مجازی اگر به دقت مدیریت و کنترل نشوند می‌توانند چالش‌های خاصی را برای مدیریت امنیت شبکه مطرح کنند، به خصوص هنگامیکه به عنوان کانال‌های دسترسی از دور بـه داخـل شـبکه‌هـای سازمانی به کار گرفته می‌شود. توصیه می‌شود به خود تونل، نقاط پایانی آن، و همچنین داده و کـد در حـال جریان درون تونل توجه شود تا مانع از این شود که یک مسیر امن به درون شبکه به عنوان تسـهیلات بـرای مهاجمان فراهم شود.

به منظور اینکه کنترل‌های امنیتی شبکه تاثیرگذار باقی بمانند، حیاتی است که پایش اصولی بر پیاده‌سازی-های امنیتی، شامل شبکه‌های خصوصی مجازی، اجرا شود و مدیران یا سرپرست‌های شبکه قادر به کشـف و واکنش به حوادث امنیت اطلاعات واقعی یا مظنون باشند.

علاوه بر این، توصیه می‌شود یک یا چندین مورد از اقدامات زیر نیز پیاده‌سازی شود:

- سامانه‌های شناسایی نفوذ
- هشدارهای امنیتی/رخداد
- رویدادنگاری امنیتی/ممیزی
- بازرسی‌های روزانه
- کاربران تعلیم دیده جهت شناسایی و گزارش حوادث امنیت اطلاعات

درک این مسئله که امنیت شبکه یک مفهوم پویا است نیز از اهمیت بالایی برخوردار است. از این رو ضرورت دارد که کارمندان امنیتی با پیشرفت‌ها در زمینه امنیـت بـه روز نگـه داشـته شـوند و VPN و فنـاوری‌هـای پشتیبان آن با جدیدترین وصله‌ها و اصلاحیه‌های امنیتی ارائه شده توسط فروشندگان کار کنند.

۱۱ راهنماهایی برای انتخاب محصول

۱۱-۱ انتخاب پروتکل حامل

توصیه می‌شود یک پروتکل حامل امن مناسب بر اساس معیارهای زیر انتخاب شود:

- الزام کسب و کار
- تعامل‌پذیری (استاندارد بین‌المللی رسمی یا استاندارد بومی)
- درک بازار
- ضعف‌های شناخته شده

- توانمندی.

۲-۱۱ تجهیزات VPN

توصیه می‌شود استفاده از تجهیزات VPN در نظر گرفته شود. در حالیکه در شبکه‌های خصوصی مجازی مقیاس کوچک (به عنوان مثال کاربر منفرد به سامانه‌های مرکزی) پیاده‌سازی کارکردهای VPN با راه‌حل‌های نرم‌افزاری کافی است، در بسیاری از مواقع استفاده از تجهیزاتی که کارکردهای VPN را فراهم می‌کنند می‌تواند مزایای قابل توجهی به همراه داشته باشد، به عنوان مثال از لحاظ مدیریت ساده شده و عمل بر روی یک بستر از لحاظ امنیتی تقویت شده. همچنین ممکن است نوعی بستر اصالت‌سنجی مورد نیاز باشد (به عنوان مثال راهنما[1]، PKI یا RADIUS) که، برای مثال، تنها به کاربران مجاز امکان اتصال به مکان مرکزی را می‌دهد.

1 - Directory

کتاب‌نامه

[1] ISO/IEC 11770-1, Information technology — Security techniques — Key management — Part1: Framework.

[2] ISO/IEC 27039, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)

[3] ISO/IEC 27033-2, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

[4] ISO/IEC 27033-3, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[5] ISO/IEC 27033-4, Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways