استاندارد ملی ایران
۱۱۲۱۰-۳
چاپ اول
۱۳۹۳

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

INSO
11210-3
1st. Edition

2014

فناوری اطلاعات - فنون امنیتی- امنیت شبکه فناوری اطلاعات- قسمت ۳: امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی

Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways

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 می‌شود 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، سازمان‌های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع 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 به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شوند 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 ملی استاندارد (ISO)[1] ،کمیسیون ملی الکتروتکنیک (IEC)[2] و سازمان ملی اندازه شناسی قانونی (OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. 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 می‌تواند با رعایت موازین پیش‌بینی شده در قانون، به‌منظور پشتیبانی 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 می‌تواند به‌منظور حفظ بازارهای ملی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تائید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تائید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه ملی 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 فناوری اطلاعات- قسمت ۳: امن‌سازی ارتباطات با استفاده از دروازه‌های امنیتی»

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیرکل اداره خدمات ارزش‌افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق‌لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق‌لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران داده آرای سپاهان
طی‌نیا، رضا (فوق‌لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فولادیان، مجید (فوق‌لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
مغانی، مهدی (فوق‌لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی

یوسف زاده، سمیرا پژوهش‌گر دانشگاه شهید بهشتی
(فوق‌لیسانس مهندسی کامپیوتر نرم‌افزار)

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات - فنون امنیتی - امنیت شبکه فناوری اطلاعات- قسمت ۳: امن‌سازی ارتباطات با استفاده از دروازه‌های امنیتی» که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و چهارمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۳ 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 پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که در تهیه این استاندارد استفاده شده است:

ISO/IEC 18028-3:2005،Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways

مقدمه

صنایع فناوری اطلاعات و ارتباطات راه دور به دنبال راه‌حل‌های امنیتی جامع و مقرون‌به‌صرفه هستند. توصیه می‌شود شبکه‌ی امن در برابر حملات مخرب و ناخواسته محافظت شود و الزامات کسب وکار را برای محرمانگی[1]، یکپارچگی[2]، دسترس‌پذیری[3]، عدم انکار[4]، پاسخگویی[5]، اصالت سنجی[6] و اطمینان‌پذیری[7] اطلاعات و خدمات، تأمین کند. همچنین امن‌سازی شبکه برای حفظ دقت در صدور صورت‌حساب یا استفاده از اطلاعات به شکل مناسب ضروری است.

قابلیت‌های امنیتی در محصولات امنیت کلی شبکه (شامل برنامه‌های کاربردی و خدمات) بسیار مهم است. بااین‌حال، هر چه محصولات بیش‌تری برای ارائه راه حل جامع ترکیب شوند، قابلیت همکاری یا عدم همکاری، موفقیت راه حل را تعریف خواهد نمود. امنیت نه تنها باید موضوع نگرانی هر محصول یا خدمات باشد، بلکه باید به شیوه‌ای توسعه یابد که درهم آمیختن قابلیت‌های امنیتی در راه‌حل‌های امنیتی انتها به انتهای کلی را ارتقاء دهد؛ بنابراین، هدف استاندارد ISO/IEC 18028 ارائه راهنمایی دقیق در مورد جنبه‌های امنیتی مدیریت، عملیات و استفاده از شبکه‌های فناوری اطلاعات و ارتباطات درونی آن‌ها است. آن دسته از افرادی که به طور کلی در درون سازمان مسئول امنیت فناوری اطلاعات و به طور خاص امنیت شبکه‌ی فناوری اطلاعات هستند، بهتر است قادر به انطباق اصول موجود در استاندارد ISO/IEC 18028 برای برآورده کردن الزامات خاص خود باشند. اهداف اصلی این استاندارد عبارت‌اند از:

- استاندارد ISO/IEC 18028-1، به‌منظور تعریف و توصیف مفاهیم مرتبط با آن است و راهنمایی مدیریت امنیت شبکه را ارائه می‌دهد- از جمله مواردی که باید مورد توجه واقع شود، نحوه شناسایی و تحلیل عوامل مربوط به ارتباطات برای استقرار الزامات امنیت شبکه، با معرفی حوزه‌های کنترلی ممکن و زمینه‌های فنی خاص است (که در قسمت‌های بعدی استاندارد ISO/IEC 18028 مطرح شده‌اند)؛
- استاندارد ISO/IEC 18028-2، به‌منظور تعریف معماری امنیتی استاندارد که چارچوبی منسجم برای حمایت از طرح‌ریزی، طراحی و پیاده‌سازی امنیت شبکه را توصیف می‌کند؛
- استاندارد ISO/IEC 18028-3، به‌منظور تعریف فنون تأمین جریان اطلاعات بین شبکه با استفاده از دروازه-های امنیتی؛
- استاندارد ISO/IEC 18028-4، به‌منظور تعریف فنون تأمین امنیت دسترسی از راه دور؛

1- Confidentiality
2- Integrity
3- Availability
4- Non-repudiation
5- Accountability
6- Authenticity
7- Reliability

- استاندارد ISO/IEC 18028-5، به‌منظور تعریف فنون تأمین امنیت ارتباطات بین شبکه‌ای است که با استفاده از شبکه‌های خصوصی مجازی[1] برقرار شده‌اند.

استاندارد ISO/IEC 18028-1 به هر کسی که درگیر مالکیت، به‌کار انداختن یا استفاده از یک شبکه است مربوط است. این کار شامل مدیران ارشد و دیگر مدیران غیر فنی یا کاربران است، علاوه بر مدیران و سرپرستانی که مسئولیت‌های خاص برای امنیت اطلاعات (IS)[2] و/یا امنیت شبکه، عملیات شبکه دارند، یا کسانی که مسئول برنامه‌های امنیتی سازمان و امنیت خط‌مشی توسعه هستند.

استاندارد ISO/IEC 18028-2 به تمام کارکنان که در طرح‌ریزی، طراحی و پیاده‌سازی جنبه‌های معماری امنیت شبکه (برای مثال مدیران شبکه، سرپرستان، مهندسان و مأموران فناوری اطلاعات امنیت شبکه) درگیر هستند، مربوط است.

استاندارد ISO/IEC 18028-3 به تمام کارکنان که در طرح‌ریزی با تهیه طرح تفصیلی، طراحی و پیاده‌سازی دروازه‌های امنیتی (برای مثال مدیران شبکه، سرپرستان، مهندسان و مأموران فناوری اطلاعات امنیت شبکه) درگیر هستند مربوط است.

استاندارد ISO/IEC 18028-4 به تمام کارکنان که در طرح‌ریزی با جزئیات بالا، طراحی و پیاده‌سازی امنیت دسترسی راه دور (برای مثال مدیران شبکه، سرپرستان، مهندسان و کارشناسان امنیت شبکه فناوری اطلاعات) درگیر هستند مربوط است.

استاندارد ISO/IEC 18028-5 به تمام کارکنان که در طرح‌ریزی با جزئیات بالا، طراحی و اجرای امنیت شبکه اختصاصی مجازی (برای مثال مدیران شبکه، سرپرستان، مهندسان و کارشناسان امنیت شبکه فناوری اطلاعات) درگیر هستند مربوط است.

1- VPN
2 -Informatin security

فناوری اطلاعات - فنون امنیتی – امنیت شبکه فناوری اطلاعات- قسمت ۳: امن‌سازی ارتباطات با استفاده از دروازه‌های امنیتی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی تعیین مرور کلی فنون مختلف دروازه‌های امنیتی، از مؤلفه‌ها و انواع مختلف معماری دروازه امنیتی است. همچنین دستورالعمل‌هایی را برای انتخاب و پیکربندی دروازه امنیتی تهیه می‌کند. اگرچه دیواره‌های آتش[1] شخصی از فنون مشابهی استفاده می‌کنند، از محدوده‌ی توجه این قسمت از ISO/IEC 18028 خارج هستند زیرا به‌عنوان دروازه‌ی امنیتی عمل نمی‌کنند. مخاطبانی که برای این قسمت از ISO/IEC 18028 در نظر گرفته شده‌اند کارکنان فنی و مدیریتی هستند، به‌عنوان مثال مدیران فناوری اطلاعات، سرپرستان سامانه، سرپرستان شبکه و کارکنان امنیتی فناوری اطلاعات. این استاندارد در کمک به کاربر برای انتخاب نوع مناسب معماری برای یک دروازه امنیتی راهنمایی ارائه می‌دهد که به بهترین وجه، مطابق با نیازمندی‌های امنیتی آنها 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 ملی ایران محسوب می‌شود.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای 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 تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 18028-4:2005, Information technology — Security techniques — IT network security — Part 4:Securing remote access

۳ اصطلاحات، تعاریف

در این استاندارد اصطلاحات و تعاریف مشخص‌شده در زیر به‌کار می‌رود:

۳-۱

هشدار[2]

«فوری» نشان می‌دهد که ممکن است یک سامانه‌ی اطلاعاتی و شبکه مورد حمله قرار گیرد، یا به دلیل حادثه، شکست یا خطای فردی در معرض خطر باشد.

1- Firewalls
2- Alert

۲-۳

مهاجم[1]

هر فرد که به‌عمد از آسیب‌پذیری‌های فنی و غیر فنی در کنترل‌های امنیتی سامانه‌های اطلاعاتی و شبکه‌ها به هدف سرقت یا در معرض خطر قرار دادن، بهره‌برداری کند، یا دسترس‌پذیری کاربران مجاز به سامانه‌های اطلاعاتی و منابع شبکه‌ها را به خطر بیندازد.

۳-۳

ممیزی[2]

تحقیق رسمی، بازرسی رسمی، یا درستی‌سنجی حقایق در برابر انتظارات، برای انطباق[3]

۴-۳

واقعه‌نگاری ممیزی[4]

جمع‌آوری اطلاعات و داده در مورد رخدادهای امنیتی اطلاعاتی به‌منظور بررسی و تحلیل و پایش مداوم.

۵-۳

منطقه غیرنظامی[5]

میزبان امنیتی یا شبکه کوچک (که با نام زیرشبکه گزینشی[6] یا یک شبکه محیط نیز شناخته می‌شود) که به‌عنوان «منطقه بی‌طرف» بین شبکه‌ها قرار داده شده است.

یادآوری: این کار منطقه‌ی میانگیر امنیتی[7] را شکل می‌دهد.

رجوع شود به امنیت میزبان.

۶-۳

پالایش[8]

با توجه به معیارهای مشخص فرآیند پذیرش یا رد جریان داده‌ها از درون شبکه.

1- Attacker
2- Audit
3- Compliance and Conformity
4- Audit logging
5- DMZ (Demilitarised Zone)
6- Screened sub-net
7- Security buffer zone
8- Filtering

۷-۳

دیواره‌آتش

نوعی مانع امنیتی که میان محیط‌های شبکه -متشکل از یک افزاره تخصیص‌یافته یا ترکیبی از مؤلفه‌ها و فنون مختلف- که از طریق آن تمام ترافیک رد و بدل شده از یک محیط شبکه به دیگری و بالعکس، در حال پیمایش است و تنها ترافیک مجاز، بر طبق خطمشی امنیت محلی تعریف‌شده، اجازه عبور دارد.

۸-۳

رخداد امنیت اطلاعات[1]

شامل وقایع امنیت اطلاعات منفرد یا مجموعه‌ای از وقایع امنیت اطلاعات ناخواسته یا غیرمنتظره می‌شود که دارای احتمال قابل‌توجه شکست عملیات کسب‌وکار و تهدید امنیت اطلاعات است.

یادآوری- به استاندارد ISO/IEC 18044 مراجعه شود.

۹-۳

مدیریت رخداد امنیت اطلاعات

فرآیند رسمی پاسخگویی و رسیدگی به وقایع امنیت اطلاعات و رخدادها.

یادآوری-به استاندارد ISO/IEC 18044 مراجعه شود.

۱۰-۳

نفوذ[2]

دسترسی غیرمجاز به شبکه یا سامانه متصل به شبکه، یعنی دسترسی‌های غیرمجاز عمدی یا تصادفی به یک سامانه‌ی اطلاعاتی که شامل فعالیت‌های بدخواه علیه یک سامانه‌ی اطلاعاتی، یا استفاده‌ی غیرمجاز از منابع در یک سامانه‌ی اطلاعاتی می‌شود.

۱۱-۳

تشخیص نفوذ[3]

به طور کلی فرآیند رسمی تشخیص نفوذ، با جمع‌آوری دانش در مورد الگوهای استفاده‌ی غیرطبیعی و همچنین پرسش‌های چه، چگونه و کدام در مورد بهره‌جویی[4] آسیب‌پذیری توصیف می‌شود تا مشخص شود چگونه و چه زمانی رخ داده است.

۱۲-۳

سامانه‌ی تشخیص نفوذ[5]

سامانه‌ی فنی است که تلاش‌های نفوذی را که رخ می‌دهد یا رخ داده است شناسایی می‌کند و احتمال دارد برای پاسخ به نفوذ در سامانه‌های فناوری اطلاعات و شبکه استفاده شود.

1- Information Security Incident
2- Intrusion
3- Intrusion Detection
4- Exploited
5- IDS

۱۳-۳
درگاه (۱)
نقطه پایانی به یک اتصال

۱۴-۳
درگاه (۲)
(پروتکل اینترنت) نقطه پایانی منطقی مجرای اتصال TCP[1](پروتکل کنترل ارسال) یا UDP[2](پروتکل داده‌های کاربر)

یادآوری- پروتکل‌های برنامه کاربردی که بر مبنای TCP یا UDP هستند و به طور معمول شماره درگاه‌های پیش‌فرض به آنها اختصاص داده شده است، به‌عنوان مثال درگاه ۸۰ برای پروتکل HTTP[3](پروتکل انتقال مبتنی ابرمتن).

۱۵-۳
حریم خصوصی[4]
حق هر فرد است که بدون دخالت مراجع قدرت، زندگی خصوصی خود و خانواده‌اش، خانه و مکاتبات وی محرمانه تلقی شود، به‌جز جایی که مطابق با قانون و ضرورت جامعه مردم‌سالار به نفع امنیت ملی، ایمنی عمومی یا رفاه اقتصادی کشور، برای جلوگیری از اغتشاش یا ارتکاب جرم، حفاظت از سلامت یا اخلاق، یا برای حفاظت از حقوق و آزادی‌های دیگران است.

۱۶-۳
دسترسی راه دور[5]
روند دسترسی به منابع شبکه از شبکه‌ی دیگر، یا دسترسی از یک افزاره پایانه که به طور دائم به شبکه متصل نیست.

۱۷-۳
مسیریاب[6]
افزاره شبکه که برای ایجاد و کنترل جریان داده‌ها بین شبکه‌های مختلف مورد استفاده قرار می‌گیرد و می‌تواند با انتخاب مسیر یا مسیرهایی بر اساس سازوکارهای پروتکل مسیریابی و الگوریتم‌ها بر روی پروتکل شبکه‌های مختلف مستقر شود.

یادآوری- اطلاعات مسیریابی در جدول مسیریابی نگهداری می‌شود.

۱۸-۳
بعد امنیتی[7]

1- Transmission Control Protocol
2- User Datagram Protocol
3- Hypertext Transfer Protocol
4- privacy
5- Remote Access
6- Router
7- Security Dimension

مجموعه‌ای از کنترل‌های امنیتی که برای رسیدگی به جنبه‌های خاصی از امنیت شبکه طراحی شده‌اند.

یادآوری- شرح مفصلی از ابعاد امنیتی در استاندارد ISO/IEC 18028-2 آورده شده است.

۳-۱۹

حوزه امنیتی[۱]

مجموعه‌ای از دارایی‌ها و منابع مربوط به یک خط مشی امنیتی مشترک.

۳-۲۰

دروازه‌ی امنیتی

نقطه اتصال بین شبکه‌ها، یا بین زیرگروه های درون شبکه، یا بین برنامه‌های کاربردی نرم‌افزار درون حوزه‌های مختلف امنیتی که با توجه به خط مشی امنیتی برای محافظت از شبکه در نظر گرفته شده‌اند.

یادآوری- دروازه امنیتی معنایی بیش از دیواره‌آتش دارد؛ این واژه شامل مسیریاب‌ها و سوده‌هایی[۲] است که قابلیت‌های کنترل دسترسی و رمزگذاری اختیاری را ارائه می‌دهند.

۳-۲۱

جعل[۳]

جعل هویت یک منبع یا کاربر مشروع

۳-۲۲

سوده[۴]

افزاره‌ای که اتصال بین افزاره‌های شبکه را با استفاده از سازوکارهای سوده داخلی فراهم می‌کند.

یادآوری ۱- سوده‌ها از دیگر افزاره‌های شبکه محلی با اتصال داخلی (مانند یک هاب) مجزا هستند زیرا فناوری مورد استفاده در سوده‌ها مبتنی بر اتصالات نقطه‌به‌نقطه است. این امر تضمین می‌کند که ترافیک شبکه تنها توسط افزاره‌های شبکه‌ای نشانی‌دهی شده دیده می‌شود و قادر می‌سازد چندین اتصال به طور همزمان وجود داشته باشند.

یادآوری ۲- فناوری سودهی را می‌توان در لایه ۲ یا لایه ۳ مدل مرجع OSI[۵] (ISO/IEC 7498-1) پیاده‌سازی کرد.

۳-۲۳

شبکه خصوصی مجازی

شبکه رایانه‌ای منطقی با استفاده‌ی محدود که از منابع سامانه شبکه‌ی فیزیکی ساخته شده است، به‌عنوان مثال با استفاده از رمزنگاری و/یا با تونل‌زنی[۶] پیوندهای شبکه مجازی در سراسر شبکه واقعی.

1- Security Domain
2 -Switch
3- Spoofing
4- Switch

۵- اتصالات داخلی سامانه‌ی باز

6- Tunneling

۴ کوته‌نوشت‌ها

API	Application Program Interface	واسط برنامه کاربردی
BGP	Border Gateway Protocol	پروتکل دروازه مرزی
DLL	Dynamic Link Library	کتابخانه پیوند پویا
ICMP	Internet Control Message Protocol	پروتکل کنترل پیام اینترنت
IDP	Intrusion Detection Prevention	پیشگیری و تشخیص نفوذ
NFS	Network File Transfer	انتقال پرونده شبکه
NIS	Network Information System	سامانه اطلاعات شبکه
NNTP	Network News Transfer Protocol	پروتکل انتقال خبر شبکه
NTP	Network Time Protocol	پروتکل زمانی شبکه
OSPF	Open Shortest Path First	باز کردن کوتاه‌ترین مسیر در ابتدا
RIP	Routing Information Protocol	پروتکل اطلاعات مسیریابی
RPC	Remote Procedure Call	فرآیند فراخوانی راه دور
SHTTP	Secure Hypertext Transfer Protocol	پروتکل انتقال ابرمتن امن
SOAP	Simple Object Access Protocol	پروتکل دسترسی شیء ساده
S/MIME	Secure Multipurpose Internet Mail Extensions protocol	پروتکل چند منظوره‌ی توسعه یافته رایانامه اینترنتی امن
SPAN	Switched Port Analyzer	تحلیلگر درگاه سودهی شده
TCP-SYN	Transmission Control Protocol, SYNchronisation	پروتکل کنترل انتقال، همزمانی
V.35	high-speed synchronous data exchange protocol	پروتکل تبادل داده همزمان با سرعت بالا
WAIS	Wide Area Information Service	خدمات اطلاعات ناحیه وسیع
X.11	graphical user interface protocol	پروتکل واسط کاربری نگاشتاری
XML	Extensible Mark-up Language	زبان نشانه‌گذاری قابل توسعه

۵ الزامات امنیتی

توصیه می‌شود مطابق با خط‌مشی امنیتی مستند، یک چیدمان دروازه امنیتی مناسب از سامانه‌های داخلی سازمان محافظت کند و به‌صورت امن جریان ترافیک در سراسر آن را کنترل و مدیریت کند. دروازه‌های امنیتی دسترسی به یک شبکه (مدل OSI، لایه ۲، ۳ و ۴)، یا برنامه‌ای کاربردی (مدل OSI لایه‌های ۵ تا ۷) را کنترل می‌کنند. مثال‌های زیر شامل دیواره‌آتش مورد استفاده برای محافظت است:

- محافظت شبکه‌ی داخلی سازمان از اینترنت،
- محافظت دو شبکه‌ی داخلی سازمان از یکدیگر،
- محافظت شبکه‌ی داخلی سازمان از شبکه‌ی خارجی سازمان.

دروازه‌های امنیتی برای تحقق الزامات امنیتی زیر استفاده می‌شوند:
- شبکه‌های منطقی مجزا،
- ارائه عملیات محدودکننده و تحلیلگرانه بر روی اطلاعاتی که بین شبکه‌های منطقی عبور می‌کنند،
- ارائه ابزار کنترل دسترسی به/از شبکه سازمان، به‌وسیله بازرسی اتصال‌ها یا با عملیات پیشکار[1] بر روی برنامه-های کاربردی انتخاب‌شده،
- ارائه نقطه ورودی کنترل‌شده و مدیریت‌شده به یک شبکه،
- اجرای خط‌مشی امنیتی سازمان در رابطه با اتصالات شبکه،
- ارائه نقطه‌ای برای واقعه‌نگاری،
- ارائه ترجمه نشانی شبکه برای پنهان کردن شبکه‌های داخلی،
- ارائه نگاشت درگاه (از جمله باز کردن پویای درگاه) و تشخیص حمله و حفاظت سطح برنامه‌ی کاربردی (شامل پالایش محتوا).

۶ فنون دروازه‌های امنیتی

روش‌های فنی مورد استفاده درون دروازه‌ی امنیتی که با پالایش ساده بسته آغاز شدند، تکامل می‌یابند و شامل رویکردهایی مانند پیشکار برنامه کاربردی و بازرسی وضعیت بسته می‌شوند. علاوه بر این، از آنجا که این فنون اغلب در ترکیب با دروازه امنیتی استفاده می‌شوند، ترجمه نشانی شبکه و همچنین پالایش محتوا در این فصل معرفی می‌شوند.

۶-۱ پالایش بسته

پالایش بسته به این معنا است که ترافیک شبکه با مقایسه اطلاعات موجود در سرآیند[2] هر بسته ورودی یا خروجی در برابر جدولی از قوانین کنترل دسترسی مسدود یا چشم‌پوشی شده است. افزاره پالایش به‌صورت جداگانه هنگام ورود هر بسته به سرآیند آن را نظاره و نشانی IP[3] و درگاه منبع و مقصد را با پایگاه قوانین

1- Proxy
2- Header
3- Internet Protocol

مقایسه می‌کند. اگر نشانی و اطلاعات درگاه مجاز باشد، بسته از طریق دیواره‌آتش به طور مستقیم به مقصد خود حرکت می‌کند. اگر یک بسته نتواند از این آزمون بگذرد، رها می‌شود.

ممکن است بسته‌های IP به‌صورت انتخابی بررسی شوند که آیا باید به جریان داده‌ها بین دو میزبان یا شبکه اجازه داده شود یا خیر. ضوابط حاکم بر تصمیم به اجازه یا رد این جریان داده‌ها می‌تواند شامل موارد زیر باشد:

- نشانی IP مبدأ؛
- نشانی IP مقصد؛
- پروتکل(به عنوان مثال TCP، UDP، ICMP)
- درگاه مبدأ؛
- درگاه مقصد؛
- جهت ارتباط (ورودی و خروجی).

دروازه‌های پالایش بسته سریع هستند زیرا در شبکه و لایه انتقال کار می‌کنند و تنها بررسی‌های گذرا را به اعتبار اتصال داده‌شده انجام می‌دهند.

۲-۶ بازرسی وضعیت بسته

بر اساس فناوری پالایش بسته، رویکرد بازرسی وضعیت بسته بررسی‌های امنیتی بیشتری را در یک تلاش می‌افزاید تا بررسی امن دیواره‌آتش پیشکار برنامه کاربردی را شبیه‌سازی کند. به‌جای اینکه به سادگی به نشانی هر یک از بسته‌های دریافتی به‌صورت جداگانه نظاره کند، دیواره‌آتش با بازرسی و بازبینی وضعیت بسته، از ورود بسته‌ها به لایه شبکه جلوگیری می‌کند تا زمانی که به‌اندازه کافی اطلاعات برای برخی تصمیم‌ها در مورد وضعیت اقدام به اتصال در لایه‌های بالایی داشته باشد. این بسته‌ها سپس در یک پودمان[1] اختصاصی بازرسی داخل هسته سامانه عامل بازرسی می‌شوند. اطلاعات مربوط به وضعیت مورد نیاز برای تصمیم‌گیری‌های امنیتی در این پودمان بازرسی مورد بررسی قرار می‌گیرند، سپس در جدول‌های وضعیت پویا برای ارزیابی اقدام‌های اتصال بعدی نگهداری می‌شوند. بسته‌هایی که تائید می‌شوند به دیواره‌آتش فرستاده می‌شوند و اجازه ارتباط مستقیم بین سامانه‌های داخلی و خارجی را می‌گیرند.

ازآنجاکه اکثر بازرسی‌ها در هسته رخ می‌دهد، دیواره‌آتش بازرسی وضعیت بسته اغلب سریع‌تر از دیواره‌های آتش پیشکار برنامه کاربردی هستند. اگر چه رویکرد بازرسی وضعیت بسته به میزان قابل‌توجهی امنیت دیواره‌های آتش پالایش ساده بسته را افزایش می‌دهد، اما در بازرسی‌های امنیتی که نیازمند جمع‌آوری بسته‌های اطلاعاتی به واحدهای بزرگ‌تر مانند نشانی‌ها یا پرونده‌ها هستند، شکست می‌خورد. علاوه بر آن باید تصمیم‌گیری‌های امنیتی را بدون اطلاع لایه کاربرد پروتکل پشته به همان صورت که پیشکار برنامه کاربردی رسیدگی می‌کند انجام داد.

---

1 - Module

پالایش بسته با بازرسی وضعیت باز هم به کاربران خارجی اجازه دسترسی مستقیم به برنامه‌های کاربردی کسب‌وکار و سامانه‌ها را می‌دهد که شاید دارای سامانه‌های عامل با پیکربندی ضعیف و آسیب‌پذیری‌های امنیتی شناخته‌شده‌ای هستند. پیشکار برنامه کاربردی این آسیب‌پذیری‌های مشابه را پنهان می‌کند، این پنهان‌سازی با محدود کردن دسترسی به یک برنامه کاربردی یا یک سامانه‌ی رایانه‌ای به یک مجموعه‌ی متناهی از وظایف شناسایی‌شده درون پیشکار انجام می‌شود.

۶-۳ پیشکار برنامه کاربردی

رویکرد پیشکار برنامه کاربردی پیشنهاد کنترل امنیت برتر می‌دهد زیرا آگاهی سطح برنامه کاربردی اتصالات اقدام شده را با بررسی همه‌چیز در بالاترین لایه در پشته پروتکل فراهم می‌کند. ازآنجاکه خدمات پیشکار برنامه کاربردی دارای دید کامل در لایه کاربردی است، به‌راحتی می‌تواند جزئیات ریز هر اقدام به اتصال واقعی را ببیند و بر طبق آن خط مشی‌های امنیتی را پیاده‌سازی کند. همچنین خدمات پیشکار برنامه کاربردی شامل عملیات توکار پیشکار می‌شود - خاتمه اتصال مشتری در دروازه برنامه کاربردی و شروع یک اتصال جدید به شبکه حفاظت‌شده داخلی. سازوکار پیشکار امنیت افزوده ایجاد می‌کند، زیرا سامانه‌های خارجی و داخلی را جدا و بهره‌جویی از آسیب‌پذیری در سامانه‌های داخلی را برای رخنه‌گرهای[1] خارجی مشکل‌تر می‌کند.

دروازه‌های امنی که از پیشکار برنامه کاربردی استفاده می‌کنند قوی‌ترین امنیت را ارائه می‌دهند، تنها نقطه‌ضعف آن‌ها این است که امنیت افزوده می‌تواند بر عملکرد تأثیر منفی داشته باشد. علاوه بر این، اغلب برای خدمات جدید مدت زمانی طول می‌کشد تا پیشکار این خدمت در دسترس قرار گیرد.

۶-۴ ترجمه نشانی شبکه[2]

یکی از ویژگی‌هایی که فناوری ترجمه نشانی شبکه (NAT) فراهم می‌کند، این است که «پنهان‌سازی»[3] طرح‌واره‌ی آدرس‌دهی شبکه را در پس محیط دیواره‌آتش فعال می‌کند. با ترجمه نشانی شبکه، نشانی IP یک سامانه در شبکه داخلی به نشانی IP نظیر به نظیر خارجی آن که قابل مسیریابی است، نگاشت می‌شود. همچنین ممکن است بسیاری از سامانه‌های پشت یک دیواره‌آتش نشانی IP خارجی را به اشتراک گذاشته باشند. منابع پشت دیواره‌آتش هنوز هم با ارسال ارتباط‌های درون‌مرزی بر روی شماره درگاه خاص در دسترس کاربران خارجی هستند. ترجمه نشانی شبکه بر روی اکثر افزاره‌های شبکه (سودهنده‌ها، مسیریاب‌ها و همچنین میزبان مستحکم[4] یا دیواره‌آتش) قابل‌اجرا است.

۶-۵ تحلیل و پالایش محتوا

دروازه‌های امنیتی با برنامه کاربردی سطح پیشکار اغلب تحلیل و پالایش محتوا را نیز اجرا می‌کنند. پالایش محتوا شامل محافظت در برابر کدهای بدخواه (مانند ویروس‌ها، کرم‌ها و اسب‌های تروآ) و همچنین کد

1- Hackers
2- NAT (Network Address Translation)
3- Hiding
4- Bastion

تغییرپذیر (مانند Java، JavaScript، ActiveX، یا هر کد اجرایی دیگر) است که ممکن است باعث آسیب به شبکه‌ها، برنامه‌های کاربردی و داده شود. ازآنجاکه بیشتر کدهای بدخواه بر روی اینترنت از طریق رایانامه یا ارتباطات بر مبنای پروتکل مبتنی بر ابرمتن توزیع می‌شوند (به‌عنوان مثال بارگیری از یک وب‌گاه یا یک وب‌گاه پروتکل انتقال پرونده[1])، حفاظت باید در نقطه‌ای که دروازه امنیتی واسط اینترنت است شروع شود.
بنابراین یک پویشگر[2] ویروس یا به طور کلی، یک پایشگر محتوا به زیر شبکه گزینش‌شده یا منطقه‌ی غیرنظامی(DMZ) اضافه شده است. در بسیاری از تأسیسات[3]، پایشگر محتوا به طور مستقیم به دیواره‌آتش با یک واسط شبکه پیوند یافته است به‌طوری که ترافیک رایانامه مبتنی بر پروتکل انتقال رایانامه ساده[4] و ارتباطات بر مبنای پروتکل انتقال مبتنی بر ابرمتن به پویشگر پالایشگر محتوا هدایت می‌شوند. فناوری‌های غالب برای تحلیل محتوا به شرح زیر عبارت‌اند از:

- پیمایش مبتنی بر امضاء (جستجو برای الگوهای شناخته‌شده)؛
- تحلیل تحقیقاتی (تحلیل کد برای عملیات و رفتار شناخته‌شده که با کدهای بدخواه در ارتباط است)
- فناوری جعبه شنی[5] (در اصل یک برنامه پایش[6] محتوا که کد مظنون را در یک «جعبه شنی» قرنطینه می‌کند).

ازآنجاکه تفاوت بین پیمایش محتوا و تشخیص نفوذ کم است، به‌خصوص در مورد تشخیص نفوذ مبتنی بر شبکه، سامانه‌های تشخیص نفوذ (IDS) می‌توانند با دیواره‌آتش هم ترکیب شوند. این ترکیب با اجرای یک عامل IDS بر روی افزاره‌ی دیواره‌آتش انجام می‌شود. به استاندارد ISO/IEC TR 15947:2002 مراجعه شود.

یادآوری- انتخاب، استقرار و عملیات سامانه‌های تشخیص نفوذ موضوع استاندارد ملی آینده (ISO/IEC 18043) را تشکیل می‌دهد.

فناوری پالایش محتوا نیز دارای برخی محدودیت‌ها است. اگر داده‌ها در لایه انتقال یا کاربردی (به‌عنوان مثال، SSL/TLS و یا S/MIME) رمزگذاری شود، گزینش محتوا دیگر مقدور نیست مگر این‌که داده‌های رمزگذاری شده در دیواره‌آتش رمزگشایی و دوباره رمزگذاری شوند. این مسئله می‌تواند تهدیدهای امنیتی مانند حملات «فردی در میان[7]» را مطرح کند.
پیامدهای قانونی در مورد پیمایش و پالایش محتوا موجود است، به‌ویژه جایی که در آن قانون قوی حفاظت از داده‌ها مورد نیاز است. در چنین فرانامه‌ای[8]، تنها پیمایش خودکار برای کدهای بدخواه مجاز است، اما پیمایش

1- File Transfer Protocol (FTP)
2- Scanner
3- Installations
4- Simple Mail Transport Protocol (SMTP)
5 Sandbox
6- Monitor
7- Man In the Middle
8- Scenario

محتوای خاص یک رایانامه مجاز نیست زیرا این امر حریم خصوصی فرستنده و گیرنده را تحت تأثیر قرار می‌دهد.

۷ مؤلفه‌های دروازه امنیتی

این بخش یک مرور کلی از چهار دسته‌ی مجزای دروازه‌های امنیتی به‌وسیله مؤلفه، به‌عنوان مثال، سودهنده‌ها، مسیریاب و دیواره آتش را فراهم می‌کند.

۷-۱ سودهنده‌ها

سودهنده‌ها برای اجازه دادن ارتباطات با سرعت بالا که پهنای باند کامل شبکه را به هر یک از درگاه‌های فیزیکی ارائه می‌دهند استفاده می‌شوند. به طور کلی سودهنده‌ها افزاره‌ی لایه ۲ هستند که به طور گسترده برای بخش‌بندی شبکه‌های محلی استفاده می‌شوند. علاوه بر این، می‌توانند جداسازی زیر شبکه را زمانی که روش‌های VLAN پیاده‌سازی می‌شود ارائه کنند. از طریق استفاده از فهرست‌های کنترل دسترسی (ACLها)ی اعمال‌شده به لایه‌های مختلف مدل OSI، لایه‌های ۲، ۳ و ۴، ترافیک بین سودهنده و گره‌های متصل به آن سودهنده قابل کنترل هستند. قابلیت کنترل دسترسی ارائه‌شده به‌وسیله سودهنده باعث می‌شود آنها برای ورود به‌عنوان مؤلفه‌های معماری دروازه امنیتی مفید واقع شوند، به‌خصوص برای پیاده‌سازی و ساختاربندی هر زیرشبکه گزینشی مربوط به منطقه‌های بی‌طرف.

به دلیل تهدیدهای مختلف، اتصال سودهنده‌های مورد استفاده در محیط دروازه‌ی امنیتی به طور مستقیم به شبکه‌ی عمومی توصیه نمی‌شود، به‌عنوان مثال، حملاتی مانند منع خدمت[1] که ممکن است سبب شود سودهنده‌ی در معرض، در این حالت سیلی از بسته‌ها را به شبکه‌های متصل جاری کند.

۷-۲ مسیریاب‌ها

مسیریاب‌ها به طور معمول برای اتصال شبکه‌های مختلف با پشتیبانی پروتکل‌های مختلف شبکه و بهینه‌سازی ترافیک شبکه و مسیرهای برقراری ارتباط میان میزبان‌ها طراحی شده‌اند. علاوه بر این، مسیریاب‌ها را می‌توان به‌عنوان مؤلفه‌هایی برای دروازه امنیتی استفاده کرد، چون قادر به پالایش بسته‌های داده‌ی ارتباط داده‌ی مربوطه بر اساس فنون پالایش بسته هستند. مسیریابی که از این بررسی اطلاعات بسته برای کنترل ترافیک شبکه بهره‌گیری می‌کند اغلب به‌عنوان یک مسیریاب گزینشی[2] (به ۸-۱-۱ مراجعه شود) نامیده می‌شود. مسیریاب‌ها معمولاً در لایه ۳ مدل OSI، لایه شبکه که در آن تنها امکان کنترل اطلاعات سطح پایین بسته‌های داده وجود دارد کار می‌کنند تا آنجا که هیچ بررسی روی داده‌های کاربر صورت نمی‌گیرد. مسیریاب‌ها می‌توانند پالایش بسته و ترجمه نشانی شبکه را انجام دهند.

1- DOS
2- Screening Router

۷-۳ دروازه در سطح برنامه کاربردی

دروازه در سطح برنامه کاربردی، افزاره یا مجموعه‌ای از افزاره‌های مبتنی بر سخت‌افزار و نرم‌افزار است. دروازه-های در سطح برنامه کاربردی به طور خاص برای محدود کردن دسترسی بین دو شبکه مجزا طراحی شده‌اند. در ابتدا دو روش برای اجرای دروازه در سطح برنامه کاربردی استفاده می‌شود:

- بازرسی و بازبینی وضعیت بسته؛
- پیشکار برنامه کاربردی.

ترکیب و تغییرات (به‌عنوان مثال، دیواره‌های آتش در سطح مدار) مختلفی از این فنون ممکن است استفاده شوند. بعلاوه، NAT را می‌توان توسط دروازه سطح برنامه کاربردی به اجرا درآورد.

۷-۴ لوازم امنیتی

افزاره‌های شبکه (مسیریاب، سودهنده ، مودم و غیره) که با سامانه عامل قوی‌شده مجهز و همه به اهداف امنیتی اختصاص داده شده‌اند، لوازم امنیتی نامیده می‌شوند. این افزاره‌ها می‌توانند پایه‌ای برای نرم‌افزار امنیتی (دیواره-آتش، IDS/IDP، حفاظت ضد ویروس و غیره) باشند. لوازم امنیتی بر روی طیف گسترده‌ای از بستر برای برآورده کردن نیازهای امنیتی متنوع ارائه شده‌اند، این طیف از کوچک‌ترین مکان‌های راه دور تا شبکه‌های شرکت‌های بزرگ و مراکز داده را شامل می‌شود. لوازمی که برای حفاظت از مکان‌های راه دور یا یک رایانه اختصاص داده شده‌اند لوازم دیواره‌آتش اختصاصی نامیده می‌شوند اگر چه ممکن است شامل کارهای امنیتی دیگر، به عنوان مثال حفاظت ضد ویروس، باشند.

تمامی فنون ذکرشده در بند ۶ را می‌توان با استفاده از لوازم امنیتی اجرا کرد.

۸ معماری دروازه امنیتی

برای محافظت کافی یک شبکه داخلی از در معرض قرار گرفتن حملات شبکه‌های خارجی، مانند اینترنت، توصیه می‌شود معماری موثری برای دروازه‌ی امنیتی انتخاب شود. دو رویکرد مختلف می‌تواند در ایجاد دروازه-های امنیتی در نظر گرفته شود، رویکرد ساخت‌یافته و رویکرد مرحله‌ای. رویکرد ساخت‌یافته بر اساس اصول طراحی شبکه و گزینه‌های امنیتی معین‌شده به‌وسیله پروتکل اینترنت تعیین شده است. رویکرد مرحله‌ای مربوط به حوزه‌های امنیتی و تدابیر حفاظتی است که در محدوده‌ی پیرامون حوزه مطابق با نیازمندی‌های امنیتی خط‌مشی امنیتی سازمان تعریف می‌شوند و به اجرا درمی‌آیند. هر دو روش در زیر مورد بحث قرار گرفته-اند.

۸-۱ رویکرد ساخت‌یافته

رویکرد ساخت‌یافته را می‌توان به‌وسیله چهار معماری مختلف اجرا کرد که ممکن است از نیازمندی‌های مختلف و خاص امنیتی یک شرکت مشتق شده باشد. این معماری‌ها عبارت‌اند از:

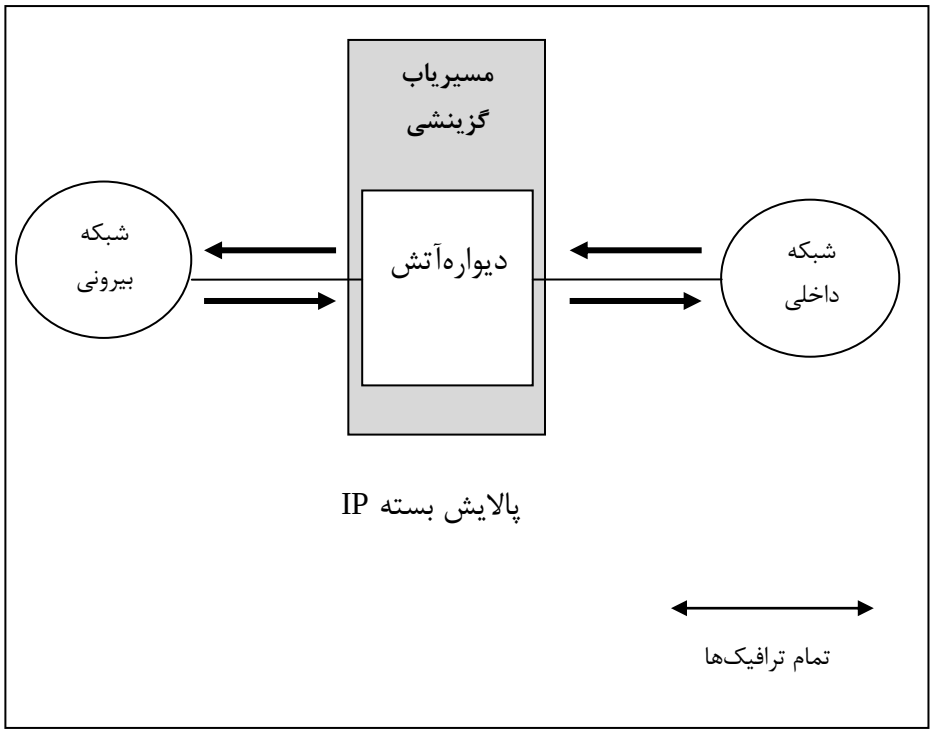
دیواره آتش پالایش بسته؛

دروازه شبکه دوتایی همزاد[1] (متعلق به دو شبکه مختلف)؛
میزبان گزینش شده؛
زیر شبکه گزینش‌شده.
حفاظت باید شامل تدابیر حفاظتی در برابر کدهای بدخواه، ویروس‌ها، قفل‌شکن‌ها، حملات منع خدمت و دیگر فعالیت‌های غیر مجاز باشد.

۸-۱-۱ معماری دیواره آتش پالایش بسته

ابتدایی‌ترین نوع معماری دیواره آتش پالایه‌ی بسته نامیده می‌شود. دیوارهای آتش پالایه‌ی بسته اساساً افزاره-های مسیریابی هستند که شامل قابلیت کنترل دسترسی برای آدرس‌های سامانه و نشست‌های ارتباط می‌شوند و اغلب به‌عنوان مسیریاب گزینشی نامیده می‌شود. در ساده‌ترین شکل خود، پالایه‌های بسته در لایه ۳ مدل OSI کار می‌کنند.
قابلیت کنترل دسترسی به یک دیواره آتش پالایش بسته با مجموعه‌ای از دستورات جمعی به‌عنوان یک مجموعه دستور اداره می‌شود. این دستورات کنترل دسترسی به شبکه را ارائه می‌دهند و می‌توانند به‌عنوان مثال، مبتنی بر نشانی مبدأ بسته، نشانی مقصد بسته، نوع ترافیک، برخی از ویژگی‌های جلسه‌ی ارتباطی لایه ۴ مانند درگاه مبدأ و مقصد باشد و همچنین (گاهی) اطلاعات مربوط به اینکه بسته‌ی اطلاعاتی از کدام واسط مسیریاب و مقصد بسته کدام واسط مسیریاب است.
دیواره آتش پالایش بسته دو نقطه قوت اصلی دارد: سرعت و انعطاف‌پذیری. ازآنجاکه پالایه‌ی بسته‌ها معمولاً داده‌های بالای لایه ۳ مدل OSI را بررسی نمی‌کنند، می‌توانند بسیار سریع عمل کنند. سادگی اجازه می‌دهد دیواره آتش پالایش بسته به‌عنوان یک مسیریاب خارجی در مقابل میزبان گزینشی یا زیر شبکه‌ی گزینشی مستقر شود. دلیل این قرار دادن، توانایی آنها در پیشگیری حمله منع خدمت و سایر حملات مرتبط است.
مسیریاب‌های گزینشی نمی‌توانند از حملاتی که از آسیب‌پذیری‌های خاص برنامه کاربردی یا عملیات استفاده می‌کنند جلوگیری کنند چون اطلاعات لایه بالاتر (لایه ۵ و ۷) را بررسی نمی‌کنند. ازآنجاکه اطلاعات در دسترسِ دیواره‌آتش محدود است، کارکرد واقعه‌نگاری در دیواره‌های‌آتش پالایش بسته نیز محدود شده است. با توجه به تعداد زیاد متغیرهای مورد استفاده در تصمیم‌گیری‌های کنترل دسترسی، آمادگی نقض امنیت ناشی از پیکربندی‌های نامناسب را دارند.

1- Dual-homed



شکل۱- مسیریاب دیواره آتش/گزینش پالایش بسته

۸-۱-۲ معماری دروازه شبکه دوتایی همزاد

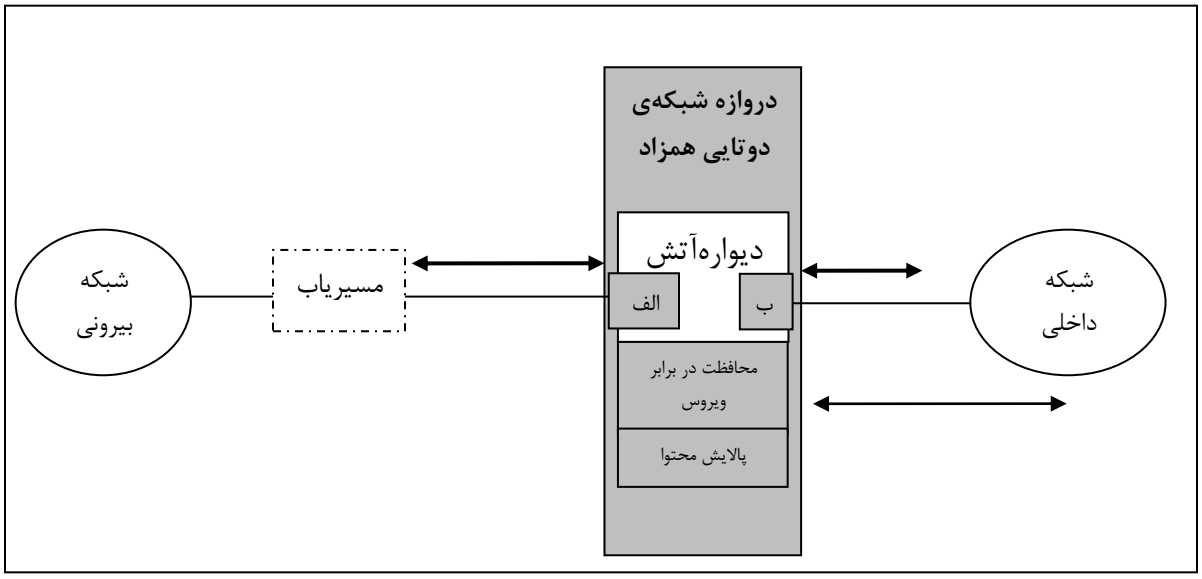
دروازه شبکه دوتایی همزاد شامل یک سامانه‌ی میزبان با دو واسط شبکه الف و ب و با قابلیت انتقال IP غیرفعال شده‌ی میزبان است؛ بنابراین، بسته‌های IP از یک شبکه (مثلاً اینترنت) به طور مستقیم به شبکه‌ی دیگر (به‌عنوان مثال، شبکه‌ی داخلی) مسیریابی نمی‌شوند. سامانه‌های شبکه داخلی می‌توانند با میزبان شبکه دوتایی همزاد ارتباط برقرار کنند و سامانه‌های بیرون دیواره‌آتش در شبکه‌های خارجی می‌توانند با میزبان دوتایی همزاد ارتباط برقرار کنند، اما این سامانه‌ها نمی‌توانند به طور مستقیم با یکدیگر ارتباط برقرار کنند.

اگر میزبان مجهز به چندین کارت شبکه باشد انواع گوناگونی از این تنظیمات موجود است، به‌عنوان مثال، به اینترنت برای اتصال‌های جداگانه به ارائه‌دهندگان خدمات اینترنت، یا به شبکه داخلی به کارسازهای مختلف از قبیل کارسازهای پست الکترونیک یا کارسازهای ورود به سامانه.

در این حالت به آن یک دروازه چندتایی همزاد[1] گفته می‌شود.

به‌صورت اختیاری، می‌توان مسیریاب را در مسیر اتصال به شبکه‌های خارجی قرارداد تا با پالایش بسته‌های شبکه حفاظت مضاعف ارائه کند. دروازه‌ی شبکه دوتایی همزاد تمامی ترافیک‌های مستقیم IP بین شبکه‌های خارجی و وب‌گاه را مسدود می‌کند. خدمات و دسترسی به‌واسطه‌ی خدمات پیشکار در سطح برنامه کاربردی در دیواره‌آتش ارائه شده است.

1- Multi-homed



شکل۲- دروازه شبکه دوتایی همزاد

دروازه شبکه دوتایی همزاد نشان‌دهنده‌ی نوع شایسته‌تری از دروازه‌های امنیتی است به دلیل آنکه نشانی‌های IP داخلی را از سامانه شبکه‌های خارجی پنهان می‌کند و قابلیت واقعه‌نگاری را ارائه می‌دهد که می‌تواند در رابطه با سامانه‌های تشخیص نفوذ (IDS) برای شناسایی فعالیت‌های مزاحم محتمل مورد استفاده قرار گیرد. انعطاف-پذیری محدود - تنها این خدمات را می‌توان برای خدمات پیشکار موجود قبول کرد - که نقطه‌ضعفی برای برخی از وب‌گاه‌ها باشد. مسیریاب اضافی درصورتی‌که در این مورد ارتباطی جنبی و قابل‌اعتماد به دروازه‌ی امنیتی محقق شود، توان حل مشکل را دارد. امنیت سامانه‌ی میزبان برای دیواره آتش برای حفاظت کلی بسیار تعیین کننده است زیرا اگر دیواره‌آتش به خطر بیفتد شخصی مزاحم[1] می‌تواند به سامانه‌های داخلی دسترسی یابد.

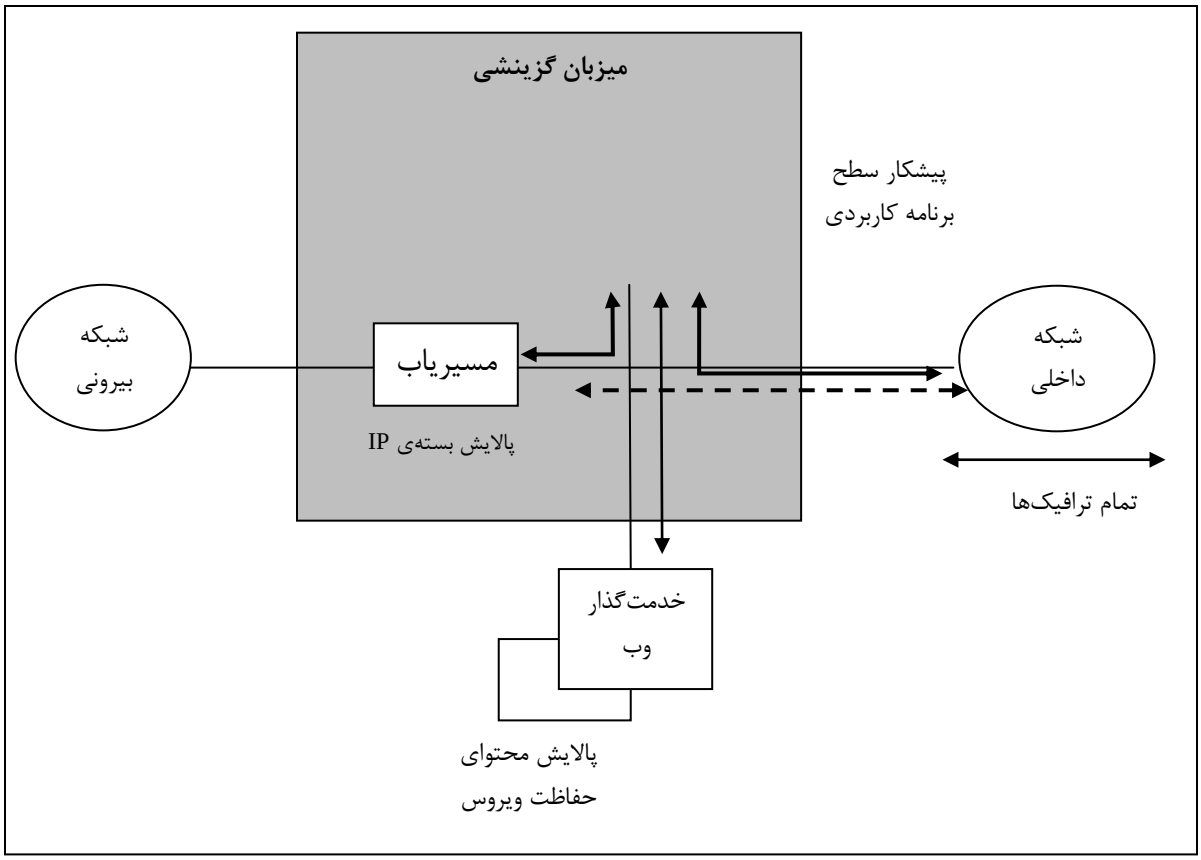
۸-۱-۳ معماری میزبان گزینشی

معماری میزبان گزینش‌شده‌ی مسیریاب پالایش بسته را با میزبان مستحکم با استفاده از پیشکار برنامه کاربردی ترکیب می‌کند. میزبان مستحکم در سمت حفاظت‌شده زیر شبکه مسیریاب جای گرفته است. در این معماری، امنیت اصلی به‌وسیله مسیریاب پالایش بسته ارائه شده است، به‌عنوان مثال، جلوگیری مردم از دور زدن کارسازهای پیشکار برای استقرار اتصال مستقیم به شبکه داخلی.

پالایش بسته بر روی مسیریاب گزینش به شیوه‌ای تنظیم شده است که میزبان مستحکم تنها سامانه‌ای است که میزبان شبکه‌های خارجی می‌توانند به آن متصل شوند. چنین میزبان مستحکمی به‌عنوان دیواره آتش سطح برنامه کاربردی شامل خدمات پیشکاری است که خدمات را با توجه به خط مشی وب‌گاه تصویب یا مسدود می-کند. مسیریاب پروتکل‌های ذاتاً خطرناک را از دستیابی به مکان سامانه‌ها یا دیواره آتش پالایش می‌کند.

1- Intruder

ترافیک برنامه کاربردی از شبکه‌های خارجی به میزبان مستحکم مسیریابی می‌شود، دیگر ترافیک‌ها از مکان‌های خارجی پذیرفته نمی‌شود. مسیریاب هر ترافیک برنامه کاربردی از شبکه‌های داخلی را نپذیرفته، مگر اینکه از سوی میزبان مستحکم آمده باشد.



شکل۳- میزبان گزینشی

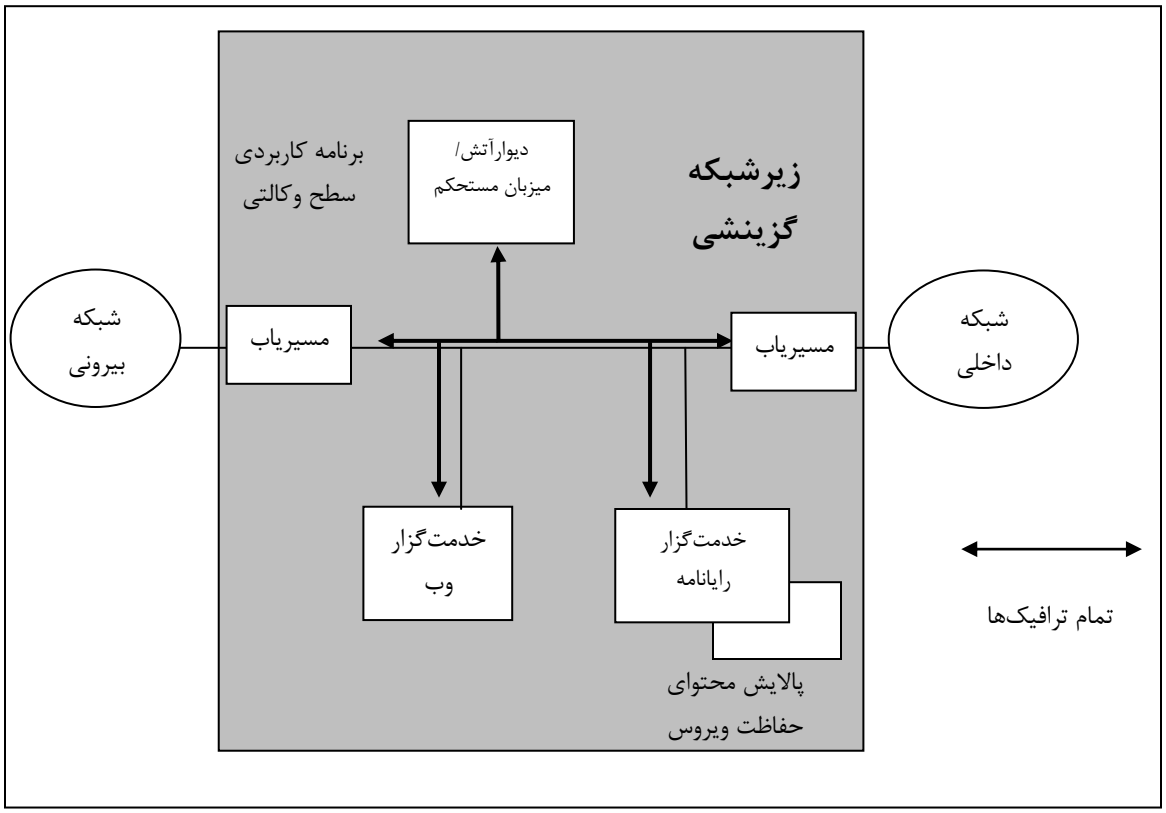
این معماری انعطاف‌پذیرتر است زیرا میزبان مستحکم تنها به یک واسط شبکه نیاز دارد و به یک زیرشبکه جداگانه بین میزبان مستحکم و مسیریاب نیاز ندارد. بعلاوه، مسیریاب می‌تواند خدمات مورد اعتماد «در اطراف» میزبان مستحکم را به طور مستقیم به سامانه‌های داخلی منتقل کند.

به طور کلی این انعطاف‌پذیری را می‌توان با امنیت پایین‌تر فرض نمود به دلیل اینکه نقض خط‌مشی امنیتی مستقر به‌مراتب آسان‌تر تفسیر شده است. نقطه‌ضعف عمده این است که اگر یک مهاجم موفق به شکستن میزبان مستحکم شود، هیچ مانعی در راستای امنیت شبکه بین میزبان مستحکم و شبکه داخلی باقی نمی‌ماند. مسیریاب همچنین یک نقطه‌ی شکست را ارائه می‌دهد؛ اگر مسیریاب در معرض خطر قرار گیرد، کل شبکه نیز در دسترس مهاجم قرار می‌گیرد. نقطه‌ضعف دیگر این است که باید دو سامانه داشته باشیم که با دقت پیکربندی شوند. قوانین پالایش بسته مسیریاب می‌تواند بسیار پیچیده و نگهداری آنها دشوار شود.

۸-۱-۴ معماری زیرشبکه گزینشی

معماری زیرشبکه گزینشی نوعی از دروازه‌ی شبکه‌ی دوتایی همزاد و معماری میزبان گزینشی است. با افزودن یک شبکه مرزی که شبکه داخلی را از شبکه‌های خارجی مانند اینترنت جدا می‌کند، یک لایه اضافی از حفاظت به معماری میزبان گزینشی می‌افزاید. دو مسیریاب برای ایجاد یک شبکه‌ی داخلی گزینشی استفاده می‌شوند. این زیر شبکه که گاهی اوقات به‌عنوان منطقه‌ی غیرنظامی (DMZ) یا یک شبکه مرزی شناخته می‌شود، جایگاه میزبان مستحکم یا دیواره آتش سطح برنامه کاربردی است، بااین‌حال، می‌تواند همچنین جایگاه کارساز (های) وب، کارساز (های) رایانامه یا کارساز (های) خدمت نام دامنه و دیگر سامانه‌ها که به دسترسی کنترل‌شده نیاز دارند باشد. مسیریاب خارجی دسترسی شبکه‌های خارجی به سامانه‌های خاص بر روی زیرشبکه گزینشی (به‌عنوان مثال، مسیریابی ترافیک رایانامه از وب‌گاه‌های اینترنتی به کارسازهای رایانامه) را محدود می‌کند و تمام ترافیک‌های دیگر به شبکه‌های خارجی را که از سامانه‌هایی که نباید ارتباط را آغاز می‌کردند مسدود می‌کند (به‌عنوان مثال، نصب سامانه‌ی پرونده شبکه[1] به سامانه‌های خارجی). مسیریاب داخلی با توجه به قوانین موجود ترافیک را به و از سامانه‌ها بر روی زیر شبکه گزینشی عبور می‌دهد (به‌عنوان مثال، مسیریابی ترافیک رایانامه از محل سامانه‌ها به خدمت‌گزارهای رایانامه و بالعکس).

1- Network File System



شکل۴- زیر شبکه گزینشی

بسیار مهم است که با داشتن دروازه‌ی شبکه‌ی دوتایی همزاد و همچنین اغلب دروازه چندتایی همزاد کـه هـیچ سامانه داخلی به طور مستقیم از شبکه‌های خارجی و بـالعکس قابـل‌دسـترس نیسـت. بـا معمـاری زیـر شـبکه گزینشی، هیچ ضرورت مطلقی برای پیاده‌سازی میزبان مستحکم متناظر دروازه سطح برنامه کاربردی بـه‌عنـوان یک سامانه شبکه دوتایی همزاد وجود ندارد.

معماری زیرشبکه گزینشی ممکن است برای مکان‌هایی با مقدار ترافیک زیاد یا مکان‌هایی که نیازمند ترافیک با سرعت بسیار بالا هستند مناسب‌تر باشد.

۸-۲ رویکرد مرحله‌ای

یک مرحله حفاظت شامل ابعاد مختلف امنیتی از دامنه امنیتی است که الزامات امنیتی را پوشش می‌دهد. برای مثال، اعلان رمز عبور از یک سامانه‌ی عامل یک مرحله حفاظت برای کنترل دسترسی است. اگر کاربران خارجی به‌درستی در مرحله حفاظت با شناسه و رمز عبور معتبر احراز هویت شده باشـند، مـی‌تواننـد بـه حـوزه امنیـت دسترسی داشته باشند.

اگر سازوکار احراز هویت به‌اندازه کافی برای پاسخگویی به الزامـات احـراز هویـت دسترسـی قـوی باشـد، بـرای حفاظت دامنه از دسترسی‌های غیرمجـاز قابلیـت اجـرا دارد. الزامـات مراحـل حفاظـت را مـی‌تـوان بـر حسـب

محرمانگی، یکپارچگی، دسترس‌پذیری، پاسخ‌گویی، اصالت‌سنجی و اطمینان‌پذیری داده‌های حساس و خدمات موجود در حوزه امنیت بیان نمود. یک مرحله حفاظت می‌تواند از کنترل‌های امنیتی همچون موارد زیر تشکیل شود:

الف- احراز هویت،

ب- پالایش بسته،

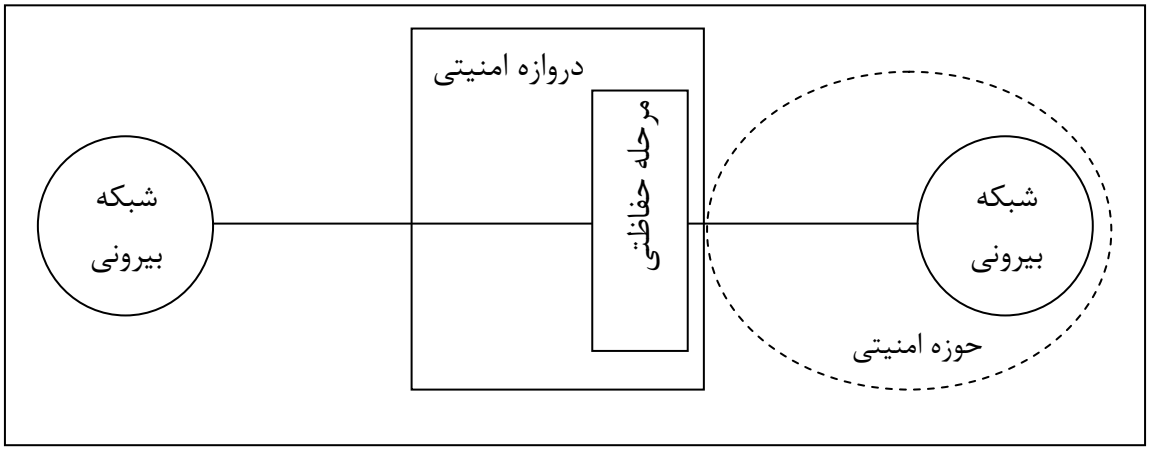
پ- تشخیص نفوذ،

ت- واقعه‌نگاری.

مراحل حفاظت را می‌توان به طور جداگانه در افزاره‌های مختلف پیاده‌سازی، یا در صورت امکان در یک یا چند افزاره گروه‌بندی کرد. در این نقطه است که رویکردهای ساخت‌یافته و مرحله‌ای با هم به اشتراک می‌رسند، به‌عنوان مثال درصورتی‌که تمام مراحل را بتوان در یک افزاره جای داد، پالایش بسته یا معماری دروازه شبکه دوتایی همزاد را می‌توان ساخت. این رویکرد، کنترل‌های امنیتی چندلایه در عمق[1] را از طریق اجرای بسیاری از مراحل حفاظت جایگذاری‌شده که مورد نیاز هستند و ارائه کنترل‌های امنیتی کافی برای ایفای الزامات امنیتی حوزه‌های امنیتی حفاظت‌شده ایجاد می‌کند.

۸-۲-۱ معماری دروازه‌ی امنیتی تک مرحله‌ای و چندمرحله‌ای[2]

معماری تک مرحله‌ای ساده‌ترین رویکرد مرحله‌ای است. اگر تنها دستیابی به یک الزام امنیتی هدف باشد می‌توان آن را اعمال نمود به‌عنوان مثال احراز هویت کاربر پیش از دسترسی به حوزه. به طور معمول عملیات مسیریاب تنها یک وظیفه‌ی امنیتی احراز هویت کاربر را اجرایی می‌کند.

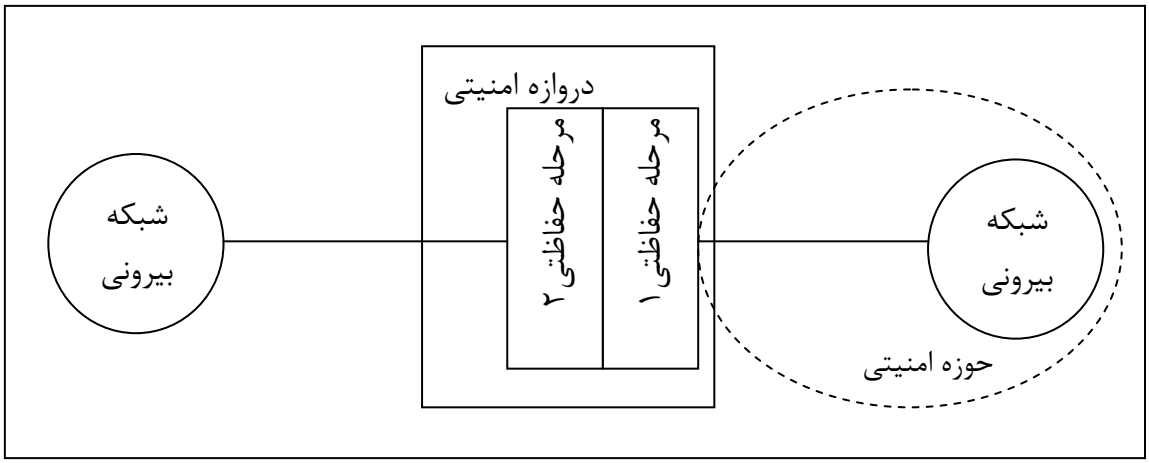


شکل۵- دروازه امنیتی تک مرحله‌ای

معمولاً حوزه امنیتی باید الزامات امنیتی بیشتری را برآورده کند و دروازه امنیتی پیچیده‌تر می‌شود، به‌عنوان مثال مجموعه‌ی مشخصی از پروتکل‌ها مجاز شمرده می‌شود و احراز هویت پیش از دسترسی به دامنه انجام

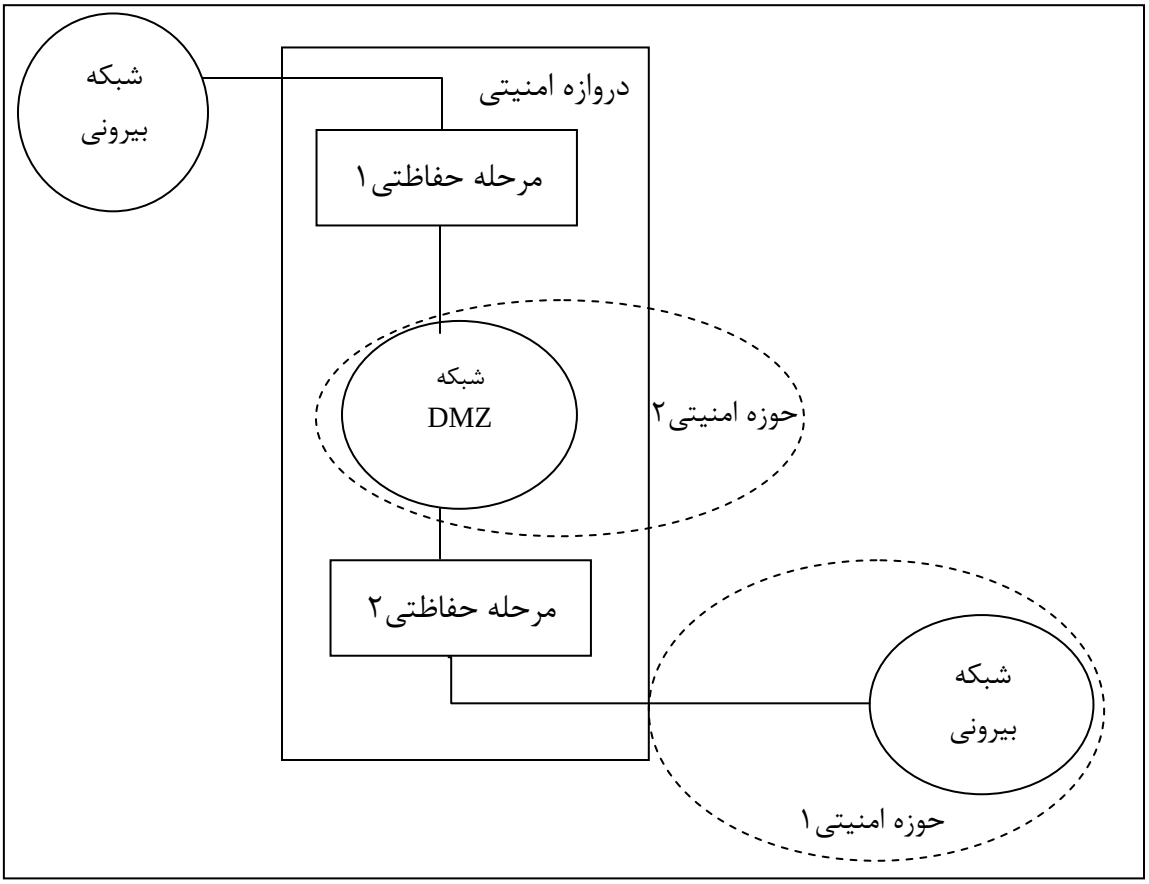
1- Defence in Depth
2- Multi-Staged

خواهد شد. در آن صورت دو مرحله امنیتی مورد نیاز است - مرحله پالایش بسته و مرحله احراز هویت. هر دو با یک مسیریاب پالایش بسته و احراز هویت قابل‌اجرا هستند.



شکل۶- دروازه امنیتی چندمرحله‌ای

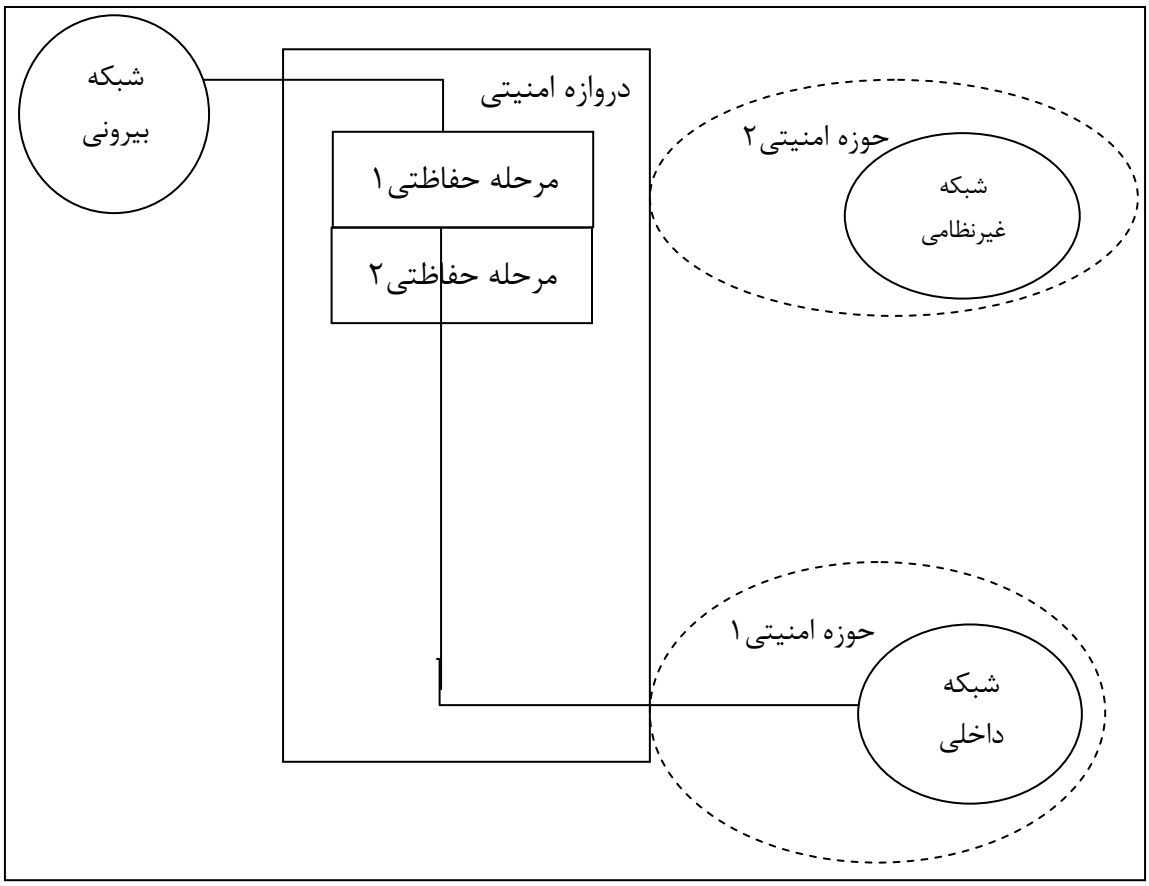
بیشتر سازمان‌ها بیش از یک حوزه امنیتی در شبکه خود دارند. درصورتی که در سازمان حوزه‌ی دیگری با الزامات امنیتی مشابه وجود داشته باشد ممکن است دروازه امنیتی هر دو حوزه را به طور هم‌زمان محافظت کند. در این مورد می‌توان منطقه‌ی غیرنظامی (DMZ) یا شبکه مرزی را ایجاد کرد. اگر خط‌مشی امنیتی حوزه‌ی اول به ترافیک اجازه عبور از حوزه دوم را دهد، DMZ شبیه به DMZ در معماری زیر شبکه گزینشی می‌شود (به شکل ۷ توجه کنید).



شکل۷- DMZ در دروازه امنیتی چندمرحله‌ای

اگر خط‌مشی امنیتی دامنه اول به ترافیک خود اجازه عبور از دامنه‌ی دیگر را ندهد و مرحله‌ی خارجی توان ارائه‌ی ارتباط مستقل به دامنه‌ی دوم را داشته باشد، در نتیجه DMZ، منطقه‌ی غیرنظامی خدمت پایه[1] خوانده می‌شود (به شکل ۸ توجه شود).

1- Service leg DMZ



شکل۸- خدمت غیرنظامی پایه در دروازه امنیتی چندمرحله‌ای

۹ راهنمایی برای انتخاب و پیکربندی

برای اطمینان از اینکه الزامات همان طور که در بند ۵ مشخص شده برآورده می‌شوند یک رویکرد ساخت‌یافته برای انتخاب و پیکربندی دروازه امنیتی لازم است. این بند برخی راهنمایی‌ها را برای این فرآیند، به‌ویژه در زمینه‌ی موارد زیر ارائه می‌دهد:

- انتخاب معماری دروازه امنیتی و مؤلفه‌ی مناسب
- انتخاب بستر[1] سخت‌افزار و نرم‌افزار
- پیکربندی[2]
- ویژگی‌ها و تنظیمات امنیتی
- سرپرستی[3]
- واقعه‌نگاری

1- Platform
2- Configuration
3- Administration

- مستندسازی[1]
- ممیزی
- آموزش/ دانش و مهارت

توصیه می‌شود به‌عنوان یک راهنمایی کلی چهار اصل زیر دنبال شوند:
الف- توجه به همه تهدیدات احتمالی که به‌خصوص شامل تهدیدهای داخلی است
ب- توجه به عامل انسانی، به‌عنوان مثال، در حوزه مدیریت و دانش و مهارت
پ- ساده‌گیری تا جایی که ممکن است، اگر چه الزامات امنیتی بالاتر به طور معمول حاکی از معماری‌های پیچیده‌تر است؛
ت- استفاده از مؤلفه‌ها یا افزاره‌ها در عملکرد و پیکربندی اختصاصی آنها

۹-۱ انتخاب معماری دروازه امنیتی و مؤلفه‌های مناسب

بر اساس الزامات مورد نیاز کسب‌وکار و امنیت برای دروازه امنیتی (به بند ۵ به‌عنوان مرجع مراجعه شود) توصیه می‌شود معماری دروازه امنیتی مناسب انتخاب و اقتباس شود (برای مرور بر معماری‌های احتمالی دروازه امنیتی به بند ۸ توجه شود).

یادآوری- مدیریت امنیت شبکه موضوع استاندارد ملی آتی (ISO/IEC 18028-1) را شکل خواهد داد.

هنگامی که یک معماری تعریف شد، لزوماً هر یک از مؤلفه‌های آن باید تعیین و قابلیت‌های آن نیز ارزیابی شود، برای مرور کلی مؤلفه‌های ممکن به بند ۸ مراجعه شود و برای شرح مفصلی از توابع ارائه‌شده، به بند ۷ مراجعه شود. بندهای زیر راهنمایی‌های بیشتری در مورد انتخاب مؤلفه‌های درست با معماری مناسب ارائه می‌دهند.

۹-۲ بستر سخت‌افزار و نرم‌افزار

هنگام انتخاب بستری سخت‌افزاری، کارایی، اطمینان‌پذیری و کاربست‌پذیری باید به‌صورت ویژه در نظر گرفته شود، به‌عنوان مثال اگر بستر تنها واسط اترنت داشته باشد و به استاندارد frame relay روی V.35 مورد نیاز باشد، در این صورت این بستر غیرقابل استفاده است. سپس سامانه‌ی عامل افزاره‌ی سخت‌افزاری باید مورد توجه واقع شود. توصیه می‌شود برای اهداف امنیتی سامانه‌ی عامل را با کاهش سطح آسیب‌پذیری‌ها امن[2] سازند. همچنین توصیه می‌شود در برابر آسیب‌پذیری‌های شناخته‌شده نیز مورد بازرسی قرار گیرد. بسترهای نرم‌افزاری نیز نیازمند درستی‌سنجی بر طبق عملکرد و اطمینان‌پذیری هستند، به‌عنوان مثال مسیریاب BaseT۱۰ واسط اترنت نمی‌تواند بازده گیگا بیت را ارائه دهد.

1- Documentation
2- hardened operating system

۹-۳ پیکربندی

توصیه می‌شود تنظیمات زیر برای افزاره‌های شبکه امنیت دروازه در طول فرایند پیکربندی در نظر گرفته شود:

- شبکه‌ی سودهی شده برای معماری زیرشبکه گزینشی مربوطه در منطقه‌ی بی‌طرف؛
- مسیریابی ایستا بین مسیریاب (ها) و دروازه امنیتی؛
- منبع اطلاعات مسیریابی نباید پذیرفته شود؛
- فقط نرم‌افزار/برنامه‌ها بر روی دروازه امنیتی که کاملاً برای عملیات لازم است («بستر امن شده»)، باید نصب شود.
- تعریف قوانین در مورد پالایش بسته با این امکان که آنچه که به‌صراحت مجاز نیست ممنوع تعریف شود؛
- اطمینان از اینکه درگاه‌ها به طور پیش‌فرض فعال نیستند؛
- اطمینان از اینکه درگاه‌های SPAN فعال نیستند مگر اینکه استفاده از سامانه‌های تشخیص نفوذ مورد نیاز باشد؛
- اطمینان از اینکه رمزهای عبور بر روی واسط‌های افزاره اجرا می‌شوند؛
- رد پیام پروتکل اطلاعات مسیریابی «مسیریابی مبدأ سست[1]»؛
- قابلیت ترجمه نشانی شبکه به شکل مناسب؛
- عملکرد شفاف دروازه امنیتی؛
- کنترل دسترسی بر روی دروازه امنیتی (شناسایی، احراز هویت)؛
- در مورد ازکارافتادن دروازه‌های امنیتی تنها وظایف اجرایی هنوز هم ممکن هستند؛
- سخت شدن بستر نرم‌افزاری در مورد سامانه عامل.

۹-۴ ویژگی‌ها و تنظیمات امنیتی

یک برنامه کاربردی پیشکار در حالت کمینه باید قادر باشد:

- پشتیبانی از خدمات اصلی اینترنت (HTTP، FTP، شبکه راه دور، ۲SMTP، ۳NNTP) ؛
- پشتیبانی از سایر خدمات اینترنت؛
- پشتیبانی از پیشکارهای عمومی (برای پروتکل‌ها یا خدمات جدید)؛
- پیشکار HTTP نیز باید قادر باشد به رسیدگی درست به SHTTP ؛
- رد اخطار پیام BGP (به‌عنوان مثال، توسط پیشکار عام)؛
- پشتیبانی از پروتکل‌های مسیریابی پویا؛
- پشتیبانی از خدمات وب (به‌عنوان مثال، SOAP / XML)؛

1- Loose-source-routing
2- Simple Mail Transport Protocol
3- Network News Transfer Protocol

- پشتیبانی از پیشکار برای برنامه‌های کاربردی سازمانی بسته‌بندی‌شده یا دیگر برنامه‌های کاربردی کسب-وکار؛
- امکان اجازه، انکار یا حذف اتصالات یا بسته.

یک افزاره‌ی پالایش بسته باید حداقل قادر به:

- پشتیبانی از خدمات NFS، NIS، RPC، RIP، OSPF، خدمات نام دامنه، WAIS با حفاظت کافی از طریق پالایش پویای بسته‌ها؛
- پشتیبانی از پالایش بسته بر اساس:
  - نشانی مبدأ و مقصد IP؛
  - درگاه مبدأ و مقصد (TCP، UDP)؛
  - جهت ارتباط (ورودی و خروجی).
- حفظ قوانین پالایش به‌ذات سازگار؛
- پالایش جداگانه بسته‌های اطلاعاتی برای هر واسط شبکه؛
- پشتیبانی از بسته‌های چندپخشی[1] درصورتی‌که خوشه‌بندی افزاره مورد نیاز باشد؛
- حفظ نظم قوانین پالایش به‌وسیله‌ی دروازه امنیتی؛
- تشخیص حملات منع خدمات (به‌عنوان مثال، جاری شدن سیل TCP-SYN)؛
- پیشگیری از حدس زدن شماره دنباله TCP؛
- محدود کردن طول قطعات بسته‌های اطلاعاتی IP و تعریف حداقل ورنهاد[2] قطعه؛
- هم‌گذاری[3] دوباره بسته‌های IP؛
- پالایش پیام‌های ICMP «مقصد غیرقابل دسترسی» و «تغییر مسیر»؛
- مقاومت در برابر حملات مرگ عملکرد زمان ارسال پیام در شبکه[4] (یک نوع حمله منع خدمات)؛
- جلوگیری از جعل IP، یعنی نشانی IP داخلی درصورتی‌که از اینترنت آمده باشد قابل‌قبول نیست؛
- استفاده دوتایی از دستورات FTP با حقوق دسترسی خاص؛
- فراهم کردن امکان ذخیره اطلاعات مقوله، به‌عنوان مثال بررسی شماره درگاه تخصیص داده‌شده به‌صورت پویا؛
- پالایش دیگر اشیاء شبکه (حوزه‌ها، گروه‌ها، اشیاء VPN و غیره)؛
- جلوگیری از ربودن[5] جلسه.

توصیه می‌شود دیگر ویژگی‌ها یا تنظیمات متفرقه بررسی شوند، به‌عنوان مثال:

- هشدار در مورد نفوذ بر اساس اطلاعات واقعه‌نگاری (حسگرهای تشخیص نفوذ البته اگر نصب شده باشد).

1- Multicast
2- Offset
3- Assembling
4- Ping-of-death
5- Hijacking

- لازم به ذکر است برنامه‌های کاربردی که از سازوکار ارتباطات SOAP استفاده می‌کنند می‌توانند ناآشکارا از طریق بازرسی وضعیت و دیواره‌های آتش پیشکار نرم‌افزار عبور کنند. این فرصتی را به وجود می‌آورد تا پیشکار نرم‌افزار و دیگر خط‌مشی‌های دیواره آتش دور زده شوند. باید به شرایطی که در آن برنامه‌های کاربردی مبتنی بر SOAP نیازمند ارتباط‌هایی هستند که از طریق دروازه‌های امنیتی عبور می‌کند توجه ویژه داشت. به‌عنوان مثال، برخی از برنامه‌های کاربردی مبتنی بر SOAP را می‌توان با اجرای پالاینده محتوای XML خاص برنامه‌کاربردی محافظت نمود (در دیواره آتش XML که اجازه می‌دهد تا پالاینده‌های XML مناسب برنامه‌ریزی شوند) و/یا با اجرای خط‌مشی‌ای که اجازه می‌دهد برنامه‌های کاربردی مبتنی بر SOAP از طریق دروازه‌ی امنیتی ارتباط برقرار کنند البته درصورتی‌که توسط یک VPN پایان به پایان[1] محافظت شود.

۹-۵ سرپرست

فرآیند مدیریت یکی از حساس‌ترین وظایف در نگهداری سطح مناسبی از امنیت است.
بایستی ملاحظات لازم به طور عمده به ویژگی‌های دروازه امنیتی زیر داده شود:

- شناسایی و احراز هویت سرپرست‌های دروازه امنیتی؛
- راه‌های قابل‌اطمینان ارتباطی برای انجام وظایف سرپرستی (به‌عنوان مثال، پیشانه[2]، ارتباط رمزگذاری شده، شبکه‌ی جداشده)؛
- مدیریت از راه دور فقط با احراز هویت و رمزگذاری قوی.
- امکان سرپرستی متمرکز در مورد استقرار دروازه امنیتی چندگانه؛
- آزمایش یکپارچگی برنامه‌های مورد استفاده و پرونده‌های دروازه امنیتی؛
- توصیه می‌شود هشدار ورود به سامانه از دروازه‌ی امنیتی به میزبان خارجی ارسال شود؛
- هشدار سرپرست به‌وسیله‌ی هر کانال امن مناسب، به‌عنوان مثال رایانامه؛
- تلاش‌های ضعیف سرپرست.

۹-۶ واقعه‌نگاری

زمانی که ردیابی جریان داده‌ها مورد نیاز است فرآیند واقعه‌نگاری بسیار مهم است، به‌عنوان مثال برای بازیابی حادثه، تحقیقات قانونی و غیره:

- قابلیت واقعه‌نگاری (شناسایی کاربر، نشانی مبدأ و مقصد IP، شماره درگاه، زمان، تاریخ). در اینجا نکته این است که هر چه اطلاعات بیشتری ذخیره شود رسیدگی به حادثه بهتر می‌شود؛
- قابلیت هم‌زمان‌سازی با کارساز NTP برای تاریخ و زمان دقیق؛
- حفاظت از پرونده‌های ورود به سامانه در برابر تغییرات بدخواه.

1- End to End
2- Console

۹-۷ مستندات

برای مدیریت مؤثر دروازه امنیتی ضروری است که مستندات شبکه بر روی وب‌گاه حفظ شوند. حداقل، توصیه می‌شود موارد زیر تهیه شوند:

- مستندات در فرم الکترونیکی (با نمودارهای گرافیکی)؛
- مستندات فرآیندهای مربوط به دروازه امنیتی (فرآیند تصویب، فرآیند بررسی)؛
- مستندات راهنمایی دسترسی (خدمات و برنامه‌های کاربردی که برای دسترسی مجاز هستند)؛
- مستندات قوانین پالایش و پیشکار اعمال‌شده؛
- مستندات طرح‌ریزی تداوم/بازیابی حادثه کسب‌وکار در مورد محیط دروازه امنیتی.

توصیه می‌شود مستندات به‌صورت دوره‌ای بررسی شود.

۹-۸ ممیزی

دروازه‌ی امنیتی باید همزمان با حفظ مفاهیم اساسی امنیت اطلاعات مانند محرمانگی، یکپارچگی، دسترس-پذیری، احراز هویت، پاسخگویی و عدم انکار، از تسهیلات ممیزی به‌منظور درستی‌سنجی پرونده (های) ثبت وقایع پشتیبانی کند.

۹-۹ آموزش و دانش و مهارت[1]

- توصیه می‌شود دروازه امنیتی با مستندات و مواد پشتیبانی کافی برای نصب و پیاده‌سازی تأمین شود در نتیجه از حفاظت کافی شبکه‌ها و سامانه‌ها اطمینان حاصل می‌شود؛
- توسعه اصول آموزشی برای کارکنان درگیر در عملیات و نگهداری.
- توصیه می‌شود، کارکنان درگیر در عملیات و نگهداری دروازه‌های امنیتی، برای اطمینان از نگهداری و حفظ سطح مناسب دانش و شایستگی به‌صورت دوره‌ای آموزش ببینند.

۹-۱۰ متفرقه[2]

توصیه می‌شود سامانه‌های دیگر و افزاره‌هایی که می‌توانند بر سطح کلی امنیت تأثیر بگذارند مورد بررسی قرار گیرند، به‌عنوان مثال:

- توصیه می‌شود هر ارتباط دسترسی از راه دور[3] به وسیله‌ی دروازه امنیتی محافظت شود. برای اطلاعات بیشتر به استاندارد ISO/IEC 18028-4 مراجعه شود؛
- بررسی ضد ویروس؛
- پالایش کد اجرایی مانند Java، JavaScript، MIME، ActiveX؛ حتی اگر در انتقال داده، پروتکل انتقال داده گنجانده شده باشد؛
- استفاده از دروازه‌های امنیتی در زمینه‌ی شبکه‌های خصوصی مجازی (VPN)؛

1- Training and education
2- Miscellaneous
3- Remote Access

یادآوری- تأمین امنیت ارتباطات با استفاده از شبکه‌های خصوصی مجازی موضوع استاندارد ملی آینده‌ی (ISO/IEC 18028-5) را تشکیل می‌دهد.

- یکپارچگی محتوای محصولات امنیتی طرف سوم:

معماری‌های دروازه امنیتی اغلب راه‌حل‌های امنیت محتوا را در بر می‌گیرند که شامل پویش و بررسی پرونده‌ها یا ترافیک اینترنت (به‌عنوان مثال، SMTP، FTP، HTTP) برای ویروس یا کد بدخواه است. از سوی دیگر، رویکردهایی با کارسازهای دروازه‌ی جداشده وجود دارد که ترافیک اینترنت یا خدمات خاص اینترنت را برای ویروس‌ها یا کد بدخواه که از طریق کارسازها حرکت می‌کنند پویش می‌کند و از ورود کدهای خطرناک به شبکه داخلی پیشگیری می‌کند. از سوی دیگر راه‌حل‌هایی با یکپارچگی نزدیک‌تر قابلیت‌های بازرسی محتوا از طریق DLL یا API در محصول دیواره آتش وجود دارد.

اغلب بررسی یا گزینش URLها نیز در رویکردهای امنیتی محتوا گنجانده شده است.

- یکپارچه‌سازی سامانه‌های تشخیص نفوذ (IDS).

در زمینه دروازه‌های امنیتی، سامانه‌های تشخیص نفوذ در منطقه‌ی بی‌طرف واقع شده‌اند. سامانه‌های دیواره‌آتش و همچنین کارسازهای برنامه کاربردی مهم متعلق به چنین سامانه‌هایی هستند که به وسیله‌ی حسگر سامانه‌ی تشخیص نفوذ کنترل می‌شوند.

اطلاعات تکمیلی در استاندارد ISO/IEC TR 15947:2002 قابل دستیابی است.

یادآوری- انتخاب، استقرار و عملیات سامانه‌های تشخیص نفوذ موضوع استاندارد ملی شماره ۱۸۰۴۳ ایران، سال ۱۳۸۸ را تشکیل می‌دهد.

کتاب‌نامه

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall, Bonn 1997

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Firewall Studie II, Bonn 2001

[3] Chapman, D. Brent, Zwicky, Elizabeth D.: Building Internet Firewalls, Cambridge 2000 (O'Reilly)

[4] Cheswick, William R. Bellovin, Steven M.: Firewall and Internet Security. Repelling the Wily Hacker. Reading, a.o. 1994 (Addison-Wesley)

[5] Ellermann, Uwe: Firewalls. Isolations- und Auditttechniken zum Schutz von lokalen Computer-Netzen. Berlin 1994 (DFN-Bericht Nr. 76)

[6] Siyan, Karanjit; Hare, Chris: Internet Firewalls and Network Security. Indianapolis 1995 (New Riders Publishing)

[7] Wack, John; Cutler, Ken; Pole, Jamie: Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology, 2001 (National Institute of Standard and Technology (NIST) Special Publication 800-41)

[8] ISO/IEC TR 15947:2002, Information technology — Security techniques — IT intrusion detection framework

[۹] استاندارد ملی ایران شماره ۱۷۷۹۹: سال ۱۳۸۹، فناوری اطلاعات - فنون امنیتی - آیین کار مدیریت امنیت اطلاعات

[10] ISO/IEC 18028-2, Information technology — Security techniques — IT network security — Part 2:
Network security architecture 1)

[۱۱] استاندارد ملی ایران شماره ۱۸۰۴۴: سال ۱۳۸۹، فناوری اطلاعات -فنون امنیتی- مدیریت رویداد امنیت اطلاعات

[۱۲] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات -فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات - الزامات