INSO-ISO-IEC

27033-4

1st. Edition

2015

Identical with
ISO/IEC 27033-4:
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران-ایزو- آی ای سی
۲۷۰۳۳-۴
چاپ اول
۱۳۹۳

فناوری اطلاعات- فنون امنیتی- امنیت شبکه
قسمت ۴: امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی

Information technology — Security techniques — Network security — Part 4: 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 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 ۴: امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی »

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل سازمان فناوری اطلاعات ایران
اعضاء : (اسامی به ترتیب حروف الفبا)	
بخشایش، سعید (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت فناوران توسعه امن ناجی
آریا، بهناز (دکتری مهندسی کامپیوتر)	قائم مقام مؤسسه کهکشان نور
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل‌پناه، ناصر (فوق لیسانس کامپیوتر)	کارشناس ارشد حوزه مخابرات
مغانی، مهدی (فوق لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکترای مهندسی کامپیوتر نرم‌افزار)	استادیار دانشگاه شهید بهشتی

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

یعقوبی رفیع، کمال‌الدین پژوهش‌گر دانشگاه شهید بهشتی
(فوق لیسانس فناوری اطلاعات معماری سازمانی)

فهرست مندرجات

عنوان **صفحه**

کتاب‌نامه

Error! Bookmark not defined.

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت ۴: امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و شصت و دومین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۳/۱۱/۲۹ 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 می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های 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 27033-4: 2014, Information Technology — Security Techniques — Network Security — Part 4: Securing Communications Between Networks Using Security Gateways

فناوری اطلاعات-فنون امنیتی- امنیت شبکه قسمت ۴: امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنما برای امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی (دیواره آتش[1]، دیواره آتش برنامه کاربردی، سامانه حفاظت در برابر نفوذ و غیره) مطابق با خط مشی امنیت اطلاعات مستند شده‌ی دروازه‌های امنیتی است که شامل موارد زیر است:

الف) شناسایی و تحلیل تهدیدات امنیتی شبکه مرتبط با دروازه‌های امنیتی

ب) تعیین الزامات امنیتی شبکه برای دروازه‌های امنیتی مبتنی بر تحلیل تهدید

پ) استفاده از فنون طراحی و پیاده‌سازی برای توجه به تهدیدات و جنبه‌های واپایشی[2] مرتبط با فرانامه[3]های کلی شبکه

ت) توجه به جنبه‌های مرتبط با پیاده‌سازی، بهره‌برداری، پایش و بازبینی واپایش‌های دروازه امنیتی شبکه

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 می‌شوند.

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 مرجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts

۳ اصطلاحات وتعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در ISO/IEC 27033-1، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

1- Firewall
2- Control
3- Scenario

۱-۳

میزبان تکیه‌گاه[1]

میزبانی خاص با سامانه عامل قوی‌شده که برای رهگیری بسته‌های ورودی یا خروجی شبکه استفاده می شود و به‌طور طبیعی هر عامل خارجی باید به آن اتصال پیدا کند تا بتواند به خدمت یا سامانه‌هایی که درون دیواره آتش سازمان قرارگرفته است دسترسی پیدا کند.

۲-۳

دیواره آتش مبتنی بر نرم‌افزار پایانگاهی[2]

نرم‌افزار کاربردی که روی یک ماشین اجرا می‌شود، و ترافیک شبکه ورودی و خروجی آن ماشین را حفاظت می‌کند تا براساس خط مشی امنیتی تعریف شده توسط کاربر انتهایی اجازه ارتباطات صادر یا رد شود.

۳-۳

سامانه عامل قوی‌شده[3]

سامانه عاملی که به‌صورت ویژه پیکربندی و طراحی شده تا موارد بالقوه حمله را کمینه نماید.

یادآوری- این سامانه عامل ممکن است یک سامانه عامل عمومی باشد، مانند Linux،که برای این محیط پیکربندی شده یا راه‌حل ساخته‌شده‌ی بومی باشد.

۴-۳

دروازه اینترنت[4]

نقطه ورودی برای دسترسی به اینترنت

۵-۳

بسته[5]

هستاری که از یک بستک[6] از بایت‌ها تشکیل شده است و شامل «سرآیند[7]»، «داده» و «پسایند[8]» اختیاری است که می‌تواند بین شبکه‌ها یا بر روی خطوط تلفن منتقل شود.

یادآوری- قالب یک بسته به پروتکل ایجاد آن بستگی دارد. استانداردها و پروتکل‌های گوناگون ارتباطات از بسته‌های خاص-منظوره برای نظارت و واپایش جلسات ارتباطات استفاده می‌کند. برای مثال، دراستاندارد X.25 از بسته‌های تشخیصی، بسته-های زدودن[9] و بازنشانی تماس، و نیز بسته‌های داده (یا) واحدی از داده که روی شبکه منتقل می‌شود، استفاده می‌شود.

1- Bastion host
2- End-point software-based firewall
3- Hardened operating system
4- Internet gateway
5- Imaging
6- Block
7- Header
8- Trailer
9- Clear

۶-۳
محیط شبکه[1]
زیرشبکه فیزیکی یا منطقی که خدمات خارجی سازمان را در برمی‌گیرد و آنرا در معرض شبکه عمومی قرار می‌دهد.

۷-۳
دفتر راه دور[2]
دفتر شعبه [3]
دفتری که از طریق شبکه‌های راه دور از بیرون به دفتر اصلی سازمان متصل شده است تا خدماتی (برای مثال، خدماتی چون فایل، چاپ و غیره) را که برای نگهداری روال‌های کسب‌وکار روزانه لازم هستند برای کاربران خود مهیا سازد.

۸-۳
خرابی تک نقطه[4]
نوعی خرابی که اگر قسمتی از یک سامانه خراب شود، کل سامانه کار نخواهد کرد.

۹-۳
دروازه پروتکل آغاز نشست (SIP)[5]
افزاره‌ی محیطی که بین شبکه VoIP داخلی و شبکه بیرونی هم‌چون شبکه تلفن عمومی قرار می‌گیرد.

یادآوری- اغلب یک مسیریاب برای انجام این نقش استفاده می‌شود. در جایی که VoIP برای شبکه‌های IP بیرونی استفاده می‌شود، اطمینان از این‌که دروازه‌ها حاوی سنجش‌های امنیتی کافی به‌ویژه تغییرات مبتنی بر قاعده پویا در امن‌سازی برقراری تمامی تماس‌ها باشند، اهمیت دارد.

۴ کوته‌نوشت‌ها

ACL	Access Control List	فهرست واپایش دسترسی
API	Application Programming Interface	واسط برنامه‌نویسی برنامه‌کاربردی
ASIC	Application Specific Integrated Circuit	مدار مجتمع کاربردهای خاص
BGP	Border Gateway Protocol	پروتکل دروازه مرزی
CPU	Central Processing Unit	واحد پردازش مرکزی
DDoS	Distributed Denial-of-Service	منع خدمت توزیع‌شده
DLL	Dynamic Link Library	کتابخانه پیوند پویا
DMZ	Demilitarized Zone	ناحیه غیرنظامی

1- Perimeter network
2- Remote office
3- Branch office
4 - Single point of failure
5 - Session Initiation Protocol

DNS	Domain Name Server	کارساز نام دامنه
DoS	Denial-of-Service	منع خدمت
FTP	File Transfer Protocol	پروتکل انتقال فایل
HTTP	Hypertext Transfer Protocol	پروتکل انتقال فرامتن
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	پروتکل انتقال فرامتن بر روی لایه دریچه امن
ICMP	Internet Control Message Protocol	پروتکل پیام واپایش اینترنت
IDS	Intrusion Detection System	سامانه تشخیص نفوذ
IP	Internet Protocol	پروتکل اینترنت
IPS	Intrusion Prevention System	سامانه جلوگیری از نفوذ
ISP	Internet Service Provider	فراهم‌کننده خدمت اینترنت
MIME	Multipurpose Internet Mail Extensions	گسترش‌های پست اینترنتی چند منظوره
NAT	Network Address Translation	ترجمه نشانی شبکه
NFS	Network File System	سامانه پرونده‌ی شبکه
NIS	Network Information System	سامانه اطلاعاتی شبکه
NNTP	Network News Transport Protocol	پروتکل انتقال اخبار شبکه
NTP	Network Time Protocol	پروتکل زمان شبکه
OS	Operating System	سامانه عامل
OSI	Open System Interconnection	اتصال متقابل سامانه های باز
OSPF	Open Shortest Path First	ابتدا کوتاه‌ترین مسیر باز
RIP	Routing Information Protocol	پروتکل اطلاعات مسیریابی
RPC	Remote Procedure Call	فراخوانی روال از راه دور
SIP	Session Initiation Protocol	پروتکل آغاز نشست
SMS	Short Message Service	خدمت پیام کوتاه
S/MIME	Secure/Multipurpose Internet Mail Extensions	گسترش‌های پست اینترنتی چند منظوره/امن
SMTP	Simple Mail Transfer Protocol	پروتکل انتقال پست ساده
SOAP	Simple Object Access Protocol	پروتکل دسترسی شیء ساده
SPA	Switched Port Analyzer	تحلیلگر درگاه سوداده
SPOF	Single Point Of Failure	خرابی تک نقطه
SQL	Structured Query Language	زبان پرسمان ساخت‌یافته

SSL	Secure Sockets Layer protocol	پروتکل لایه دریچه‌های امن
SYN	Synchronous	هم‌زمان
TCP	Transmission Control Protocol	پروتکل هدایت انتقال
TLS	Transport Layer Security	امنیت لایه‌ی ترابری
UDP	User Datagram Protocol	پروتکل بستک کاربر(پبک)
VLAN	Virtual Local Area Network	شبکه داخلی مجازی
VM	Virtual Machine	ماشین مجازی
VoIP	Voice over Internet Protocol	صدا در بستر پروتکل اینترنت
VPN	Virtual Private Network	شبکه خصوصی مجازی
WAIS	Wide-area Information Servers or Service	کارسازها یا خدمت اطلاعات ناحیه گسترده
WLAN	Wireless Local Area Network	شبکه داخلی بی‌سیم
XML	Extensible Markup Language	زبان نشانه‌گذاری قابل گسترش

۵ ساختار

ساختار این استاندارد ملی به صورت زیر است:

- مرورکلی بر دروازه امنیتی (به بند ۶ مراجعه شود)
- تهدیدات امنیتی مرتب با دروازه امنیتی (به بند ۷ مراجعه شود)
- الزامات امنیتی مبتنی بر تحلیل دروازه‌های امنیتی (به بند ۸ مراجعه شود)
- واپایش‌های امنیتی مرتبط با فرانامه‌های شبکه نوعی و نواحی فناوری شبکه استفاده کننده از دروازه امنیتی (به بند ۹ مراجعه شود)
- فنون طراحی متنوع برای دروازه‌های امنیتی (به بند ۱۰ مراجعه شود)
- راهنماهایی برای انتخاب محصول (به بند ۱۱ مراجعه شود)

۶ مرور کلی

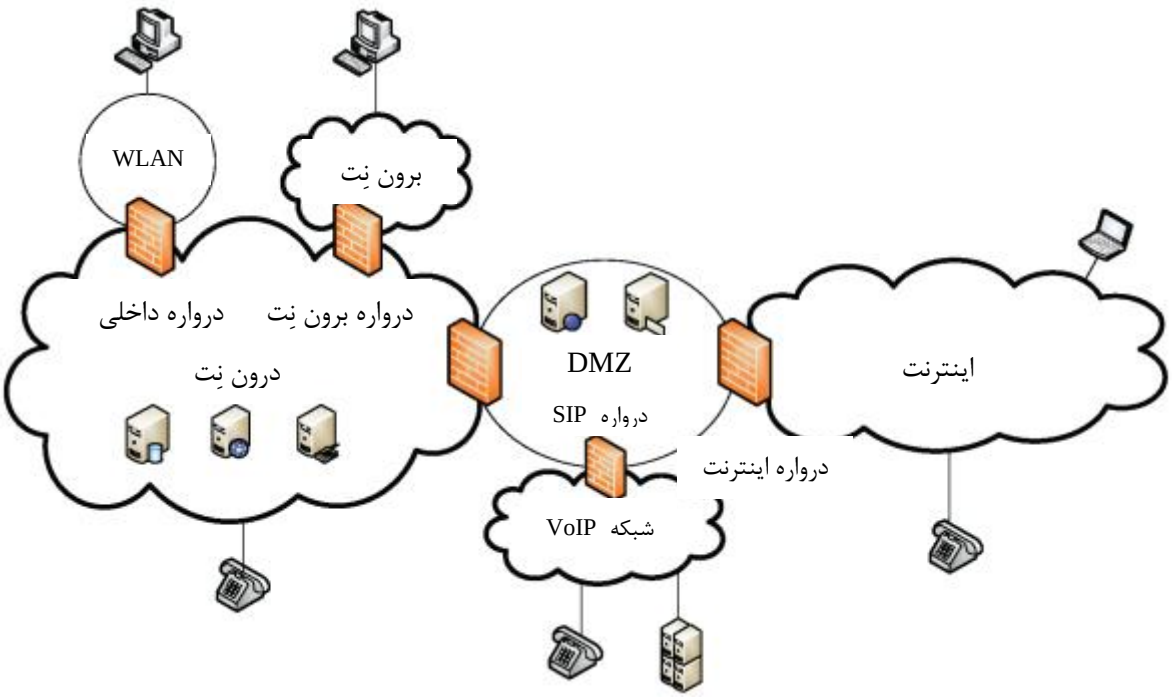
دروازه امنیتی در مرز بین دو یا چند بخش شبکه قرار می گیرد، به عنوان مثال، بین شبکه داخلی سازمان و یک شبکه عمومی، تا ترافیک روان را در سراسر مرز با توجه به خط مشی دسترسی خدمات دروازه امنیتی مستند برای آن مرز، پالایش کند.

یکی دیگر از استفاده‌های دروازه امنیتی جدا کردن بخش‌های شبکه در هنگام استفاده از خدماتی است که ممکن است دارای چندین مستاجر[1] باشند، به عنوان مثال در هنگام استفاده از خدمات ابری، دروازه امنیتی با اعمال خط مشی امنیتی سازمان، اطلاعات سازمان را حفاظت می‌کند.

1- Tenant

مثالی از محیط شبکه در شکل ۱ نشان داده شده است که در این مرور کلی فقط با اهداف روشن‌گری ارائه شده است. ناحیه DMZ، که از آن به عنوان محیط شبکه یاد می‌شود، زیرشبکه فیزیکی یا منطقی است که خدمات خارجی سازمان را در برمی‌گیرد و آن را در معرض شبکه عمومی (معمولا اینترنت) قرار می‌دهد. هدف از DMZ اضافه کردن یک لایه اضافی امنیتی به شبکه داخلی سازمان است. مهاجم خارجی به جای هر بخش دیگری از شبکه داخلی، تنها به خدمات موجود در DMZ دسترسی دارد. توصیه می‌شود همه اتصالات خارجی به خدمات در داخل DMZ خاتمه یابد و توصیه می‌شود سامانه‌های DMZ به سامانه‌های داخلی دسترسی کم داشته باشند و یا هیچ دسترسی نداشته باشند. طراحی یک شبکه به این صورت، مخاطره شبکه داخلی را از بین نمی‌برد، و فقط مشکل‌تر می‌کند.

هر نفوذگری که بتواند خدمتی را در داخل محیط شبکه، تخریب[1] سازد، ممکن است این فرصت را داشته باشد که آسیب‌پذیری دیگری که می تواند دسترسی به شبکه داخلی را امکان پذیر کند، شناسایی نماید. به همین دلیل، توصیه می‌شود شبکه داخلی، تا حد امکان امن شود.



شکل ۱- مثال محیط شبکه

اکثر سازمان‌ها ممکن است برای لایه‌های وب، برنامه کاربردی و دادگان و نیز برای مواجهه با برخی از الزامات انطباق/ مقرراتی، چندین «نواحی[2]» و یا مناطق DMZ داشته باشند.

2- Subvert
2- Zones

در حال حاضر راه‌حل‌های «ترکیبی» وجود دارد که چندین منطقه کارکردی را ترکیب می‌کند. بسیاری از دیواره های آتش پالایش بسته در حال حاضر برای خدمات معین پیشکارهایی[1] دارند و واپایش‌های بیشتری برای زمینه‌هایی مانند نقش، زمان روز، و غیره را شامل می‌شوند.

درون نِت[2] متعلق به سازمان توسط افراد مجاز سازمان مدیریت و نگهداری می‌شود. توصیه می‌شود هر سازمان به هر اندازه مهم، بخش‌های شبکه را جدا سازد تا دروازه‌های امنیتی داخلی جریان ترافیک را واپایش کند. ممکن است زیرساخت‌های جداگانه‌ای را بتوان برای مقاصد ویژه استفاده داخل درون نِت استفاده کرد. به عنوان نمونه، اگر یک WLAN به عنوان بخشی از درون نِت استفاده می‌شود، توصیه می‌شود که جدا شود و با توجه به این‌که خطرات اضافی با خود به همراه دارد، نیاز به اصالت سنجی بیشتری دارد. در دروازه امنیتی داخلی می‌توان برای محافظت از دارایی‌های سازمان در مقابل حملات از این تقسیم‌بندی استفاده کرد.

این سازمان با گسترش درون نِت به سمت شبکه‌ای از شبکه شریک تجاری از طریق به‌اصطلاح شبکه برون نِت[3]، به برقراری ارتباط و تبادل داده با طرف‌های سوم مورد اعتماد می‌پردازد. ازدروازه امنیتی برون نِت می‌توان برای مقابله با تهدیدات ناشی از این گسترش استفاده نمود. هنگام استفاده از خدماتی مانند رایانش ابری، دروازه امنیتی برای محدود کردن دسترسی و اعمال خط مشی امنیتی برای شبکه‌های منطقی سازمان استفاده می‌شود. کسب‌وکار سازمان مستلزم ارتباطات و تبادل داده با شرکای کسب‌وکار، مشتریان، و عموم مردم از طریق شبکه‌های عمومی (که اینترنت شایع ترین مثال آن می‌باشد) است. از آنجا که سطح اعتماد به شبکه عمومی به‌نسبت پایین است، دروازه‌های امنیتی، به‌اصطلاح دروازه‌های اینترنت، نیازمند توجه به خطرات ناشی از شبکه عمومی می‌باشد.

۷ تهدیدات امنیتی

برای آینده‌ی قابل پیش بینی، سازمان‌ها می‌توانند انتظار حملات پیچیده داشته باشند که به‌طور فزاینده سامانه‌های آن‌ها را هدف قرار خواهد داد. تلاش‌ها جهت دسترسی‌های غیر مجاز می تواند مخرب باشد، به عنوان مثال، منجر به حمله منع خدمت، سوء استفاده از منابع، یا دسترسی غیر مجاز به اطلاعات ارزشمند شود. توصیه می‌شود سازمان‌ها شبکه داخلی و یا دارایی‌های خود را از تهدیدهای مختلف، از جمله سوء استفاده عمدی از دارایی‌ها، پیکربندی اشتباه سامانه‌ها، گذر ترافیک غیرمجاز از حوزه های مختلف مورد اعتماد در درون سازمان یا تهدیدات دیگر از خدمات برنامه‌کاربردی اینترنتی محافظت نماید.

دروازه امنیتی باید سازمان را در مقابل نفوذ کاربران غیر مجاز که از شبکه‌های داخلی، اینترنت، یا شبکه‌های طرف سوم به شبکه دسترسی دارند، محافظت نماید. محتوای واپایش نشده ای که این سازمان را ترک می‌کند، ممکن است منجر به وقوع مسائل حقوقی و احتمال از دست رفتن مالکیت شود. علاوه بر این، چون سازمان‌های بیشتری برای رسیدن به الزامات سازمانی خود به اینترنت متصل می‌شوند، نیازمند واپایش

1- Proxies

2- Intranet

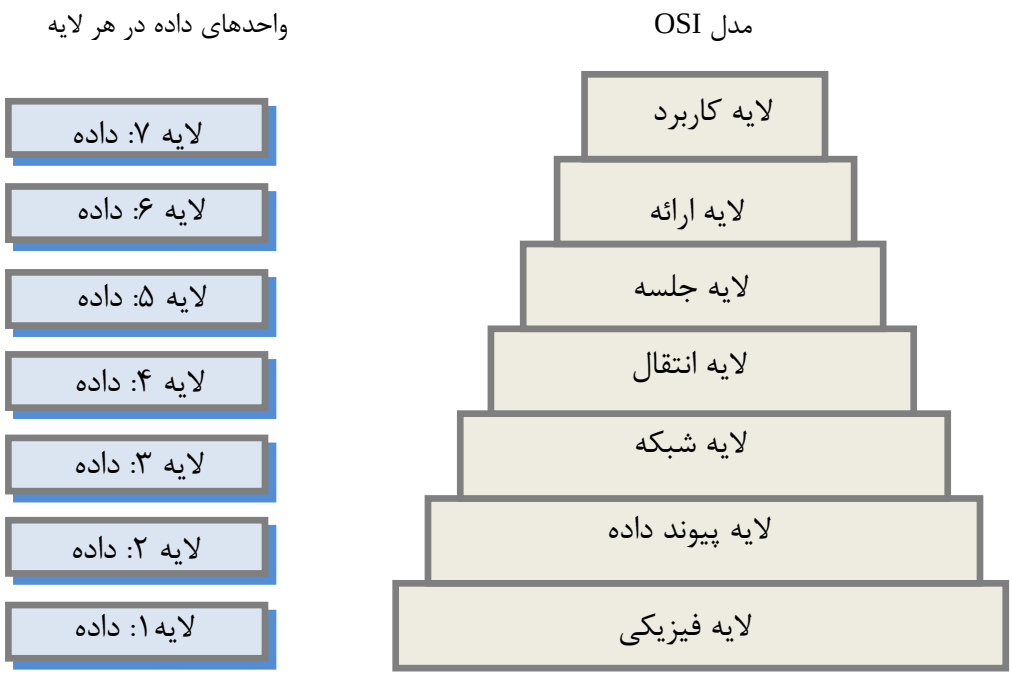
3- Extranet

دسترسی به وبگاه‌های نامناسب و ناخوشایند یا برنامه‌های کاربردی وب و خدمات می‌شوند. بدون واپایش، سازمان‌ها با تهدید از دست دادن بهره‌وری، قرار گرفتن در معرض مسئولیت و تخصیص نامناسب از پهنای باند در نتیجه‌ی وب گردی غیر مولد روبرو هستند. بنابراین تهدیدات امنیتی کلیدی که باید مورد توجه قرار گیرند که شامل مواردی در ارتباط با موارد زیر است:

- منع خدمت برای کاربران مجاز؛
- تغییرغیرمجاز داده‌ها؛
- افشای غیرمجاز داده‌ها؛
- پیکربندی دوباره غیرمجاز سامانه‌ها؛
- استفاده غیر مجاز از منابع و دارایی‌های سازمان؛
- تقاطع غیرمجاز[1] محتوا به عنوان مثال ویروس‌ها و بد افزارها؛
- ایجاد اختلال در مجازی‌سازی؛ و
- حمله منع خدمت و منع خدمت توزیع شده به دروازه امنیتی.

۸ الزامات امنیتی

واپایش دسترسی دروازه‌های امنیتی به شبکه (لایه ۲، ۳، و ۴ مدل OSI)، و یا به یک برنامه کاربردی (لایه های ۵ تا ۷ مدل OSI) در شکل ۲ نشان داده شده است.



شکل ۲- هفت لایه‌ی OSI

دروازه‌های امنیتی جهت برآوردن الزامات امنیتی زیر استفاده می‌شوند:

- ارائه بخش‌بندی منطقی شبکه؛

1 - Transversal

- محدود کردن و تحلیل ترافیکی که بین شبکه‌های منطقی عبور می‌کند؛
- واپایش دسترسی به و از شبکه سازمان، توسط بازرسی از اتصالات یا با عملکردهای پیشکار در برنامه‌های کاربردی انتخاب‌شده؛
- اعمال خط مشی امنیت شبکه سازمان‌ها؛
- واقعه نگاری[1] ترافیک برای ممیزی‌های بعدی؛
- پنهان کردن معماری شبکه داخلی، میزبان و برنامه کاربردی؛ یا
- فراهم کردن قابلیت برای تسهیل عملکردهای مدیریت شبکه، به‌عنوان مثال کاهش DoS یا DDoS.

جدول ۱ رابطه بین تهدیدات در بند ۷ و الزامات امنیتی در این بند را توضیح می‌دهد.

1- Log

جدول ۱- رابطه بین تهدیدات و الزامات

تهدیدات	الزامات						
	ارائه تقسیم بندی منطقی شبکه	محدود کردن و تحلیل ترافیکی که بین شبکه‌های منطقی عبور می‌کند	واپایش دسترسی به و از شبکه سازمان، توسط بازرسی از اتصالات یا با عملکردهای پیشکار در برنامه‌های کاربردی انتخاب شده	اجرای خط مشی امنیت شبکه سازمان‌ها	واقعه نگاری برای ممیزی‌ها ی بعدی	پنهان کردن شبکه داخلی، میزبان و معماری برنامه کاربردی	فراهم کردن قابلیت برای تسهیل کارکرد مدیریت شبکه
منع خدمت برای کاربران مجاز		x		x	x		x
تغییر غیرمجاز داده‌ها	x	x	x	x	x		x
افشای غیرمجاز داده‌ها	x	x	x	x	x		x
پیکربندی مجدد غیرمجاز سامانه‌ها			x	x	x	x	x
استفاده غیرمجاز از منابع و دارایی‌های سازمان	x	x	x	x	x	x	x
تغییر غیرمجاز محتوا به عنوان مثال ویروس ها و نرم افزارهای مخرب	x	x	x	x	x	x	x
تخلف مجازی‌سازی	x	x	x	x	x		x
منع خدمت و حمله منع خدمت توزیع شده در برابر دروازه امنیتی		x		x	x		x

۹ واپایش‌های امنیتی

۹-۱ مرور کلی

برای هر دروازه امنیتی، توصیه می‌شود سند خط مشی دسترسی (امنیت) به خدمت جداگانه توسعه داده شود و محتوا پیاده‌سازی شود تا اطمینان حاصل شود که تنها ترافیک مجاز، اجازه عبور دارد. توصیه می‌شود این سند شامل جزئیات مربوط به مجموعه دستوراتی که دروازه برای اداره و پیکربندی خود نیاز دارد، شود. این نیاز وجود دارد که از اعمال اجباری سلسله مراتب خط مشی نیز اطمینان حاصل شود: سازمانی با هر اندازه مهم، احتمالا خط مشی عمومی در کل سازمان دارد و ممکن است توسط یک خط مشی عمومی در برابر یک دسته کامل از افزاره‌های امنیتی تشدید شود، و ممکن است یک خط مشی خاص برای یک افزاره ویژه بیشتر تشدید شده باشد. بنابراین، به منظور اطمینان از این که تنها کاربران و ترافیک معتبر از طریق اتصالات ارتباطات دسترسی دارند، توصیه می‌شود خط مشی تعریف شود و محدودیت‌ها و قوانین اعمال‌شده به ترافیک عبوری به داخل و خارج از دروازه امنیتی و پارامترهایی برای مدیریت و پیکربندی آن را با جزئیات ثبت کند. در تمام دروازه‌های امنیتی، توصیه می‌شود استفاده‌ی مناسب، از شناسایی و اصالت سنجی دسترس‌پذیر، واپایش دسترسی منطقی و امکانات ممیزی ساخته شود. علاوه بر این، توصیه می‌شود دروازه‌های امنیتی به‌طور منظم از جهت نرم‌افزارها و/یا داده‌های غیر مجاز بررسی شوند، و اگر چنین مواردی یافت شد، توصیه می‌شود گزارش‌های رخداد مطابق با شمای مدیریت رخداد امنیت اطلاعات سازمان و/یا جامعه تولید شود(به استاندارد ملی ایران به شماره ۲۷۰۳۵: سال ۱۳۹۲ مراجعه شود). وصله[1]های امنیتی تغییراتی هستند که برای تصحیح ضعف بیان شده توسط یک آسیب‌پذیری به یک دروازه امنیتی اعمال می‌شود، و این کار به‌منظور جلوگیری از سوءاستفاده موفق و حذف و یا کاهش قابلیت یک تهدید در دروازه است. از این رو، توصیه می‌شود دروازه‌های امنیتی به‌طور منظم با آخرین وصله‌ها و نسخه‌ها به‌روز رسانی شوند تا اطمینان حاصل شود که در مقابل آخرین آسیب‌پذیری‌ها موثر هستند.

توصیه نمی‌شود دروازه امنیتی تا زمانی که پیکربندی الزامات خط مشی‌های حاکمیتی را برآورده نسازد، به شبکه سازمان متصل شود.

دیواره آتش یک مثال خوب از یک دروازه امنیتی است. به طور معمول توصیه می‌شود دیواره آتش‌ها به‌گونه‌ای باشند که سطح تضمین مناسب و متناسب با تهدیدات ارزیابی‌شده را به‌دست دهند، به همراه مجموعه قوانین استاندارد دیواره آتش که به‌طور ضمنی همه ترافیک بین شبکه‌ها را راه نمی‌دهد و همچنین قوانین صریح و روشن تنها برای برآوردن راه‌های ارتباطات مورد نیاز را اضافه نمایند.

خط مشی‌های حاکم بر یک دروازه امنیتی که برای محافظت از سامانه راه دور مورد استفاده قرار می‌گیرند، ممکن است هزینه و مهارت‌های تخصصی برای حمایت از افزاره سخت‌افزاری اختصاصی را تضمین نکند. در عوض، یک دیواره آتش مبتنی‌بر نرم‌افزار پایانگاهی، به اصطلاح دیواره آتش شخصی، می تواند جهت واپایش‌های جریان ترافیک بین رایانه راه دور و شبکه‌ای که به آن وصل شده است، مورد استفاده قرار گیرد. همانند هر دروازه امنیتی دیگر، سازمان باید مجاب شود که پیکربندی مجموعه قوانین در دیواره آتش مبتنی‌بر نرم‌

1- Patch

افزار پایانگاهی، الزامات خط مشی‌های حاکم را برآورده می‌سازد.
انواع مختلفی از دروازه‌های امنیتی وجود دارد، از جمله پالایش بسته، دیواره آتش پیشکار، بازرسی بسته حالت دار[1]، دیواره آتش پالایش محتوا و برنامه‌کاربردی. جزئیات مربوط به هر نوع از دروازه‌های امنیت در زیر بندهای بعدی شرح داده خواهد شد.
دروازه امنیتی ممکن است برای پیاده‌سازی کارکردهای مورد نیاز، یک فناوری مجازی‌سازی را به‌کار گیرد. توصیه می‌شود ماشین‌های مجازی(VM)[2]، به‌هنگام اشتراک گذاری ظرفیت‌های حافظه، CPU و ذخیره‌ساز به خوبی از یکدیگر جدا باشند.
توصیه می‌شود ابرناظر[3] که به آن مدیر ماشین مجازی نیز گفته می‌شود، حفاظت خود و VMهای میزبانی شده را تامین کند؛ به عنوان مثال با تغییر مکان پردازش ضدویروس و پادهرز[4] از VM به ابرناظر.
امنیت مجازی‌سازی از ابرناظر و VMهای آن محافظت می‌کند و ابرناظر را از حملات محافظت می‌کند و جداسازی VM را امکان‌پذیر می‌سازد. این کارکرد همچنین شامل محافظت از تصاویر VM، نمونه‌های به حالت تعلیق درآورده‌شده VM در ذخیره‌ساز و در مدت مهاجرت و نیز مدیریت چرخه حیات امنیت کلی VM می‌شود.

۹-۲ پالایش بی‌حالت بسته

پالایش بسته، هر بسته را جدا از هر بسته دیگر بررسی می‌کند. تصمیم بر اجازه یا منع پیشرفت آن بسته، به‌طور کامل مبتنی بر داده‌های درون همان بسته است. هیچ تلاشی برای ارتباط آن بسته با بسته‌های قبلی که ممکن است به پالایش بسته داده شده باشد وجود ندارد. بنابراین این تصمیم مبتنی بر چنین عواملی است:

- آدرس IP منبع و/یا مقصد
- پایه‌بار[5] که بسته حمل می‌کند (به عنوان مثال TCP، UDP، ICMP)
- درگاهی[6] منبع و/یا مقصد برای پایه‌بار TCP یا UDP
- زمان/تاریخ ورود/خروج بسته و
- کارت واسط شبکه ورود/خروج.

دروازه‌های پالایش بسته سریع هستند، اما اهمیت هر بسته در مدت کلی جریان ارتباط را پیگیری نمی‌کنند.

۹-۳ بازرسی حالت دار بسته[7]

بازرسی حالت دار بسته، از طریق ضبط رویدادهای کلیدی در چرخه حیات تبادل ارتباطات، گسترشی بر روش پالایش بی حالت بسته‌ها است، این امر به‌طور معمول با ردیابی حالات پروتکل‌های لایه انتقال انجام

1- Stateful
2- Virtual Machine
3- Hypervisor
4- Anti-spam
5- Payload
6- Port
7- Stateful

می‌شود. بر اساس فناوری پالایش بسته، روش بازرسی حالت دار بسته در برخی از محصولات دیواره آتش با اضافه کردن بازبینی‌های امنیتی بیشتر در تلاش برای شبیه‌سازی بازبینی‌های امن روی دیواره آتش پیشکار نرم‌افزار در نظر گرفته شده و پیاده‌سازی می‌شود. به جای این‌که به سادگی در آدرس هر یک از بسته‌های ورودی به‌صورت جداگانه جستجو کند، دیواره آتش بازرسی حالت دار بسته، بسته‌ها را در لایه شبکه تا زمانی که به اطلاعات کافی برای تعیین حالت اتصال تلاش در لایه‌های بالا دست یابد، رهگیری می‌کند.
به‌هنگام تصمیم‌گیری برای سرنوشت یک بسته، پالایش حالت دار بسته، بسته را در زمینه دیگر بسته‌هایی که تا کنون دیده است در نظر می‌گیرد. به‌عنوان مثال این امر اجازه می دهد تا پالایش، بین یک بسته که بخشی از ارتباط TCP برقرارشده است با یک بسته مشابه که خودش آمده است تمایز قایل شود. بنابراین پالایش حالت دار بسته می تواند تصمیم‌گیری‌های دقیق‌تر نسبت به پالایش بی‌حالت بسته داشته باشد. با این‌حال این موضوع برای رسیدن به همان میزان حجم‌گذر[1] بسته نیاز به منابع بیشتر (حافظه و قدرت پردازش) دارد.

۹-۴ دیواره آتش برنامه کاربردی

دیواره آتش برنامه کاربردی تبادل ارتباطات را در سطح پروتکل کاربرد، تجزیه و تحلیل می‌کند. به عنوان مثال، دیواره آتش برنامه کاربردی وب با قوانینی پیکربندی می‌شود که عملکردی صحیح از HTTP را نشان دهد. این تصمیم درباره این‌که آیا یک درخواست HTTP یا پاسخ HTTP اجازه داده شود، می‌تواند هم بر اساس حالت گفتگوی HTTP (برای مثال، آیا این پاسخ مناسبی برای درخواست قبلی مشاهده شده است؟) و یا برخی از الگوی خاص در داده‌ها (به عنوان مثال، آیا نویسه‌های حاضر حمله تزریق SQL را نشان می‌دهد) باشد.
اگر یک دیواره آتش برنامه کاربردی باید در ارتباط رمزشده مانند SSL/TLS عملکرد داشته باشد، آنگاه رمزگذاری انتها به انتها باید در دیواره آتش برنامه کاربردی شکسته شود به‌طوری که بتواند داده‌های برنامه کاربردی را در شرایط وضوح پالایش کند. در این شرایط، توصیه می‌شود دیواره آتش برنامه کاربردی از یک جفت کانال ارتباطی رمزگذاری پشت به پشت بین منبع و مقصد بهره‌برداری کند. اگر یکپارچگی چنین دیواره آتش برنامه کاربردی به خطر بیافتد، آن‌گاه عواقب ناگوار ناشی از اعتماد کاربران به حفاظت از رمزگذاری انتها به انتها، را به دنبال دارد.
دیواره آتش‌ها برخی از تهدیدات شرح داده‌شده در بند ۷ را پوشش[2] می‌دهند، به عنوان مثال، استفاده غیر مجاز از منابع و دارایی‌های یک سازمان، با محدود کردن دسترسی به برنامه کاربردی و یا سامانه رایانه‌ای به مجموعه ای محدود از وظایف قابل شناسایی درون خود پیشکار.
رویکرد دیواره آتش برنامه کاربردی واپایش امنیتی برتری را ارائه می‌دهد، به این دلیل که از طریق بررسی همه چیز در بالاترین لایه از پروتکل پشته[3]، آگاهی سطح برنامه کاربردی را فراهم می‌کند. دیواره آتش برنامه کاربردی را می‌توان در قسمتی از پیشکار برنامه کاربردی پیاده‌سازی کرد. این امر می‌تواند پاسخگویی و

1- Through put
2- Mask
3- Protocol Stack

کاهش ترافیک های تکراری را بهبود بخشد. خدمت پیشکار برنامه کاربردی دارای دید کامل در لایه کاربرد است و بر این اساس می‌تواند جزئیات واضحی از هر اقدام اتصال را ببیند و در نتیجه خط مشی‌های امنیتی را پیاده‌سازی کند. همچنین خدمات پیشکار برنامه کاربردی، قابلیت عملکرد پیشکار ساخته‌شده‌ای دارند که اتصال مشتری در دروازه برنامه کاربردی را پایان می‌دهد و اتصال جدیدی را به شبکه محافظت‌شده داخلی آغاز می‌کند. سازوکار پیشکار امنیت افزونه‌ای را ایجاد می‌کند، به دلیل آنکه سامانه های داخلی و خارجی را جدا می‌کند و بهره برداری از آسیب پذیری‌ها در سامانه های داخلی را برای مهاجمان در خارج سخت‌تر می-سازد. ارتباطات رمزگذاری‌شده‌ی انتها به انتها به‌طور مستقیم نمی تواند از دیواره آتش برنامه کاربردی عبور کند اما در عوض به عنوان دو جریان رمزگذاری‌شده‌ی پشت به پشت با پیام واضح در دیواره آتش برنامه کاربردی وجود دارد. این مساله سبب می‌شود دیواره آتش برنامه کاربردی به‌طور ویژه‌ای جذاب باشد چرا که به‌عنوان هدف حمله برای راه‌اندازی حمله فرد در میانه[1] بر علیه اتصالات رمزگذاری شده است، مورد توجه باشد.

در حال حاضر بسیاری از دیواره آتش‌ها همراه با قابلیت‌های شفاف پیشکار هر دو خدمت پیشکار سنتی را ارائه می‌کنند، که اغلب با عنوان «بازرسی عمیق بسته» و یا واپایش برنامه کاربردی به آن اشاره می‌شود. این دیواره آتش‌ها آگاه به برنامه کاربردی هستند و قادرند تنها عملکردهای خاص درون یک برنامه کاربردی اجازه دهند یا واپایش‌های اضافی را اعمال نمایند (به‌عنوان مثال، پویش فایل‌های درون یک برنامه کاربردی و یا مسدود کردن تماس‌های ویدئویی درون کارخواه‌های پیام‌رسانی فوری با استفاده از ضدویروس).

دروازه امنی که از پیشکار برنامه کاربردی استفاده می‌کند، قوی‌ترین امنیت را ارائه می‌کند اما تنها اشکالی که وجود دارد، تاثیر منفی روی عملکرد، به دلیل امنیت افزوده‌شده است. علاوه‌براین، زمان خدمات جدید را اغلب قبل ازاین‌که پیشکار برای این خدمت در دسترس باشد، طولانی می‌کند.

۹-۵ پالایش محتوا

دروازه‌های امنیتی با پیشکار در سطح برنامه کاربردی، اغلب پالایش محتوا را پیاده‌سازی می‌کنند. پالایش محتوا محافظتی کلیدی در برابر کدهای مخرب و یا نامناسب است. این می تواند به مقابله در برابر تهدیدها در هنگام بارگیری‌های برنامه کاربردی یا اجرا در مرورگر کمک نماید. این امر می تواند محدوده‌ای از اسب-های تروآ تا واپایش‌های ActiveX نامناسب را داشته باشد. از آن‌جایی‌که بسیاری از این کد های مخرب بر روی اینترنت از طریق پست الکترونیک یا ارتباطات مبتنی بر HTTP توزیع می‌شود(به عنوان مثال بارگیری-های از وبگاه یا وبگاه FTP)، توصیه می‌شود محافظت در نقطه واسط دروازه امنیتی به اینترنت شروع شود. بنابراین، یک پویگشر ویروس و یا به‌طور کلی، یک پویگشر محتوا به زیرشبکه غربال و یا منطقه غیرنظامی (DMZ) اضافه می‌شود. در بسیاری از نصب و راه‌اندازی‌ها، پویشگر محتوا به طور مستقیم از طریق واسط شبکه با دیواره آتش پیوند دارد، به طوری که خدماتی مانند ترافیک پست الکترونیک مبتنی بر SMTP و ارتباطات مبتنی بر HTTP به پویشگر پالایش محتوا مسیردهی می‌شوند.

فناوری غالب برای تحلیل محتوا به شرح زیر است:

1- Man-in-the-middle

- تحلیل پروتکل.
- پویش مبتنی بر امضا (جستجو برای الگوهای شناخته‌شده).
- تحلیل تحقیقی (تجزیه‌وتحلیل کد برای عملکردها و رفتار شناخته‌شده مرتبط با کدهای مخرب). و
- فناوری Sandbox (در اصل برنامه نظارت بر محتوا، که کد مشکوک را در «Sandbox » قرنطینه می‌کند).

از آنجایی که تفاوت بین پویش محتوا و تشخیص نفوذ ناچیز است، به خصوص در مورد تشخیص نفوذ مبتنی بر شبکه، سامانه تشخیص نفوذ (IDS) همچنین میتواند از طریق پیاده‌سازی یک عامل IDS برروی افزاره دیواره آتش با دیواره آتش ترکیب شود. به استاندارد ISO / IEC TR 15947 مراجعه شود.

یادآوری- انتخاب، استقرار و عملیات سامانه‌های تشخیص نفوذ و یا پیشگیری بر اساس موضوع استاندارد ISO / IEC 27039 را است.

فناوری پالایش محتوا نیز مقداری محدودیت دارد. اگر داده‌ها در لایه انتقال و یا کاربرد رمزگذاری شود (به عنوان مثال SSL/TLS و یا S/MIME)، غربالگری محتوا دیگر امکان‌پذیر نیست مگر این که داده‌های رمزگذاری شده، در دیواره آتش رمزگشایی و دوباره رمزگذاری شود. این امر می‌تواند تهدیدات امنیتی مانند حملات «فرد در میانه» را مطرح نماید.

ممکن است پیامدهای حقوقی در مورد پویش و پالایش محتوا وجود داشته باشد، به خصوص در جایی که در آن قوانین قوی حفاظت از داده‌ها اثر دارد. در چنین فرانامه‌ای، فقط پویش خودکار برای کدهای مخرب اجازه داده می‌شود، اما نه برای پویش محتوای خاص از یک پست الکترونیک، به این دلیل که این موضوع ممکن است تجاوز به حریم خصوصی فرستنده و گیرنده را به دنبال داشته باشد.

۹-۶ سامانه پیشگیری نفوذ و سامانه تشخیص نفوذ

نفوذ، دسترسی غیرمجاز به شبکه و یا یک سامانه متصل به شبکه است، یعنی دسترسی آگاهانه و یا تصادفی غیر مجاز به یک سامانه اطلاعاتی، فعالیت‌های مخرب بر علیه سامانه اطلاعاتی و یا استفاده غیرمجاز از منابع درون سامانه اطلاعاتی است. پیشگیری از نفوذ فرایند رسمی در پاسخ به جلوگیری از نفوذ به‌طور فعال است. سامانه پیشگیری از نفوذ یک نوع از سامانه‌های تشخیص نفوذ است که به‌طور خاص برای ارائه قابلیت پاسخ به‌صورت فعال طراحی شده است، در حالی که سامانه‌های تشخیص نفوذ به سادگی نفوذهای ممکن اقدام شده، یا در حال وقوع، یا رخ داده را تشخیص می‌دهند و در صورت امکان نفوذها را به سرپرستان[1] اطلاع می‌دهند.

۹-۷ مدیریت امنیت API

کارکرد مدیریت متمرکز، امکان مدیریت مناسب و کارآمد دروازه‌های امنیتی مستقر در شبکه سازمان را ایجاد می‌کند.

1- Administrators

توصیه می‌شود API مدیریت امنیت توسط دروازه امنیتی برای این مدیریت متمرکز از راه دور در سازمان فراهم شود. توصیه می‌شود این کارکرد مدیریت متمرکز به مدیریت از راه دور دروازه‌های امنیتی، از لحاظ بهره برداری و پیکربندی کمک کند.
توصیه می‌شود سرپرست امنیتی راه دور توسط دروازه امنیتی شناسایی و اصالت سنجی شود. توصیه می‌شود این API مدیریت از راه دور سرپرست شبکه‌ای را با ابزارهایی جهت سرپرستی، نظارت، و عیب یابی دروازه امنیتی فراهم کند.

۱۰ فنون طراحی

۱۰-۱ مولفه‌های دروازه امنیتی

۱۰-۱-۱ سوده‌ها[1]

سوده‌ها برای ایجاد امکان ارتباطات با سرعت بالا برای ارائه پهنای باند کامل شبکه به هر درگاه فیزیکی استفاده می‌شود. به‌طور کلی سوده‌ها افزاره‌های لایه ۲ هستند که به‌طور گسترده برای بخش‌بندی شبکه‌های داخلی استفاده می‌شود. علاوه‌براین، می‌توانند جداسازی زیرشبکه را هنگام اجرای فنون VLAN فراهم کنند. ترافیک بین سوده و گره‌های متصل به سوده می تواند از طریق استفاده از فهرست‌های واپایش دسترسی (ACL ها) واپایش شود. این‌را می توان به لایه های ۲، ۳ و ۴ مدل OSI اعمال کرد. کارکرد واپایش دسترسی ارائه‌شده توسط سوده باعث سودمندی آن‌ها برای گنجاندن مولفه‌های معماری دروازه امنیتی، به‌خصوص برای پیاده‌سازی و ساختار مربوط مناطق غیرنظامی هر زیرشبکه غربال‌شده می‌شود. توصیه نمی‌شود سوده مورد استفاده در محیط دروازه امنیتی با توجه به تهدیدهای مختلف به عنوان مثال حملات منع خدمت که می تواند سوده را در معرض سیل بسته‌های شبکه‌های متصل قرار دهد، به‌طور مستقیم به شبکه عمومی متصل شود.
ممکن است سوده‌های بار متعادل[2] که در لایه ۷ عمل می‌کنند وجود داشته باشد. این سوده‌ها برای فراهم نمودن دسترس‌پذیری به دیواره آتش‌ها و همچنین کارسازها استفاده می‌شود (هر چند به‌طورمعمول لایه ۷ برای دیواره آتش‌ها استفاده نمی‌شود).

۱۰-۱-۲ مسیریاب‌ها

مسیریاب‌ها به‌طور معمول برای اتصال شبکه‌های مختلف با پشتیبانی از پروتکل‌های مختلف شبکه و همچنین برای بهینه‌سازی ترافیک شبکه و مسیرهای بین میزبان‌های دارای ارتباط طراحی می‌شوند. علاوه براین، مسیریاب‌ها می‌توانند به‌عنوان مولفه‌هایی برای دروازه امنیتی استفاده شوند، زیرا قادر به پالایش داده‌های مربوط به بسته‌های داده ارتباطی مبتنی بر فنون پالایش بسته هستند. مسیریابی که از این بازبینی اطلاعات بسته، برای واپایش ترافیک شبکه بهره می‌گیرد، اغلب به عنوان مسیریاب غربالگری نامیده می‌شود. مسیریاب‌ها به‌طور معمول در لایه ۳ مدل OSI (لایه شبکه) کار می‌کنند. در این سطح تنها اطلاعات سطح

1- Switches
2- Load-balanced

بسته، مانند درگاه‌های منبع و مقصد، می‌تواند مورد تجزیه‌وتحلیل قرار گیرد. مسیریاب‌ها می توانند NAT و پالایش بسته‌ها را انجام دهد.

ممکن است سوده‌های متعادل-بار که در لایه ۷ عمل می‌کنند وجود داشته باشند. این سوده‌ها برای فراهم نمودن دسترس‌پذیری به دیواره آتش‌ها و همچنین کارسازها استفاده می‌شوند (هر چند به‌طور معمول لایه ۷ برای دیواره آتش‌ها استفاده نمی‌شود).

۱۰-۱-۳ دروازه سطح کاربرد

دروازه سطح کاربرد، افزاره یا مجموعه‌ای از افزاره های مبتنی بر سخت‌افزار و نرم‌افزار می باشد. دروازه‌های سطح کاربرد به‌طور خاص برای محدود کردن دسترسی بین دو شبکه مجزا طراحی می‌شوند. به‌طور ابتدایی دو فن برای پیاده‌سازی دروازه‌های سطح کاربرد استفاده می‌شود:

- بازرسی حالت دار بسته.
- پیشکار برنامه کاربردی.

ترکیب‌ها و حالت‌های مختلفی (به عنوان مثال دیواره آتش‌های در سطح مدار) از این فنون نیز ممکن است مورد استفاده قرار گیرد. علاوه بر این، NAT می تواند با دروازه‌های در سطح کاربرد انجام شود. دروازه سطح کاربرد، برنامه‌های کاربردی و پروتکل‌هایی را که توسط برنامه کاربردی استفاده می‌شود درک می‌کند تا قادر به تعیین پاسخ‌های مشروع درخواست باشد. به‌عنوان مثال در هنگام استفاده از برنامه‌های کاربردی مانند VoIP،دروازه سطح کاربرد نیاز به درک پروتکل شروع نشست (SIP) دارد تا امکان اطلاعات مناسب بین اتصالات را ایجاد کند.

هنگام به‌خدمت گرفتن فناوری VoIP برای فراهم نمودن خدمات تلفن، توصیه می‌شود شبکه سازمان در برابر حملات به SIP، با استفاده از یک دیواره آتش که به آن SIP-آگاه گفته می‌شود و یک نمونه معمولی دروازه سطح کاربرد است، حفاظت شود.

۱۰-۱-۴ لوازم امنیت

افزاره‌های شبکه (مسیریاب‌ها، سوده‌ها، مودم‌ها و غیره) که مجهز به سامانه عامل سخت هستند، و همگی برای اهداف امنیتی اختصاص داده شده‌اند، لوازم امنیتی نامیده می‌شود. این افزاره‌ها می‌توانند پایه‌ای برای نرم‌افزار امنیتی (دیواره آتش، IDS / IPS، حفاظت ضد ویروس و غیره) باشد. لوازم امنیتی بر روی طیف گسترده‌ای از بسترها ارائه می‌شود تا نیازهای امنیتی مختلف، از کوچکترین موقعیت‌های راه دور گرفته تا شبکه‌های شرکت‌های بزرگ و مراکز داده را تامین نماید. وسیله‌ی اختصاص داده شده به یک ماشین که وسیله دیواره آتش شخصی نامیده می‌شود، نرم‌افزار کاربردی در حال اجرا روی آن ماشین بوده تا ترافیک به داخل و خارج از ماشین را محافظت نماید. وسیله‌ی اختصاص داده شده برای حفاظت از یک موقعیت راه دور، لوازم امنیتی شاخه/خانه و یا دفتر راه دور و دفتر شعبه نامیده می شوند. لوازم امنیتی دفتر راه دور و دفتر شعبه به طور کلی ترافیک به داخل و خارج از دفتر راه دور/شعبه یا دفتر خانه را محافظت می‌کند. تمام فنون ذکرشده در بند ۹ را می توان با استفاده از لوازم امنیتی پیاده‌سازی نمود.

۱۰-۱-۵ کارکرد نظارت

کارکرد نظارت/ممیزی متمرکز، امکان ممیزی و/یا نظارت مناسب و کارآمد دروازه‌های امنیتی مستقر در شبکه سازمان را ایجاد می‌کند. توصیه می‌شود ارتباط بین کارکرد نظارت/ممیزی و دروازه امنیتی که برای تبادل اطلاعات لازم برای کارکرد مناسب ممیزی و نظارت مورد استفاده قرار می‌گیرد، امن شود.

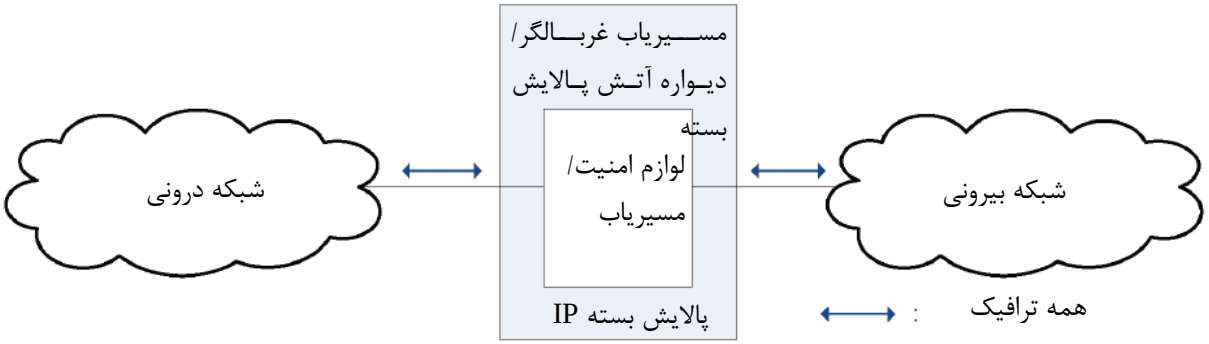
علاوه براین، توصیه می‌شود هر یک از دروازه‌های امنیتی، واسطی برای برقراری ارتباط با کارکرد نظارت/ممیزی متمرکز فراهم نماید. این کارکرد نظارت/ممیزی متمرکز ممکن است در به‌دست آوردن هر گونه وضعیت غیر طبیعی در دروازه‌های امنیتی و/یا کوشش‌ها و اقداماتی که می تواند نقض امنیتی دروازه و/یا سامانه‌های داخلی به دنبال داشته باشد و همچنین در پیگیری حسابرسی کاربر در مورد اقدامات انجام شده، و ثبت موارد نقض خط مشی امنیتی کمک نماید.

نظارت جامع در مورد عملیات دروازه امنیتی و مسیرهای ممیزی، توسط این کارکرد نظارت/ممیزی متمرکز تسهیل می‌شود. علاوه‌براین، ممکن است داشبورد توصیفی، کارآمد و همیشه در دسترس برای تصمیم‌گیری مدیریت ارائه دهد.

۱۰-۲ استقرار واپایش‌های دروازه امنیتی

۱۰-۲-۱ معماری دیواره آتش پالایش بسته

دو نوع دیواره آتش پالایش بسته وجود دارد: حالت دار یا بی‌حالت. دیواره آتش بسته بی‌حالت برای حذف بسته‌های ناقص، بسته‌های رسیده از منبع «اشتباه» و یا هدایت‌شده به سمت مقصد «اشتباه» مناسب است. منبع و یا مقصد ممکن است با استفاده از جهت جریان توسط دیواره آتش، آدرس شبکه بسته، و یا درگاه محتوای لایه انتقال بسته مشخص شود. هر بسته جدا از تمام بسته‌های دیگر در نظر گرفته می‌شود. دیواره آتش پالایش بسته اتصال انتها به انتها را نمی‌شکند. پایه‌ای‌ترین نوع معماری دیواره آتش، پالایش بسته نامیده می‌شود که در شکل ۳ نشان داده شده است. دیواره آتش‌های پالایش بسته دراساس افزاره مسیریابی هستند که شامل کارکرد واپایش دسترسی برای آدرس‌های سامانه‌ها و جلسات ارتباطات است. اغلب به عنوان مسیریاب‌های غربالگری اشاره می‌شوند. در پایه‌ای‌ترین شکل خود، پالایش بسته در لایه ۳ از مدل OSI کار می‌کند.



شکل ۳- دیواره آتش پالایش بسته/ مسیریاب غربالگر

کارکرد واپایش دسترسی در دیواره آتش پالایش بسته توسط مجموعه‌ای از دستورات که در مجموع به‌عنوان یک مجموعه قانون خوانده می‌شوند، اداره می‌شود. مجموعه‌های قانون به‌طور معمول به‌عنوان فهرست‌های واپایش دسترسی (ACL ها) نامیده می‌شوند. این مجموعه‌ها امکان واپایش دسترسی به شبکه را فراهم می‌آورند و به عنوان مثال می توانند، براساس آدرس منبع بسته، آدرس مقصد یک بسته، نوع ترافیک، برخی از ویژگی‌های لایه ۴ ارتباطات، مانند درگاه منبع و مقصد، و همچنین اطلاعات مربوط به واسط مسیریابی که بسته از آن آمده و از واسط مسیریابی که بسته به آن مقصد می‌رود، باشند.

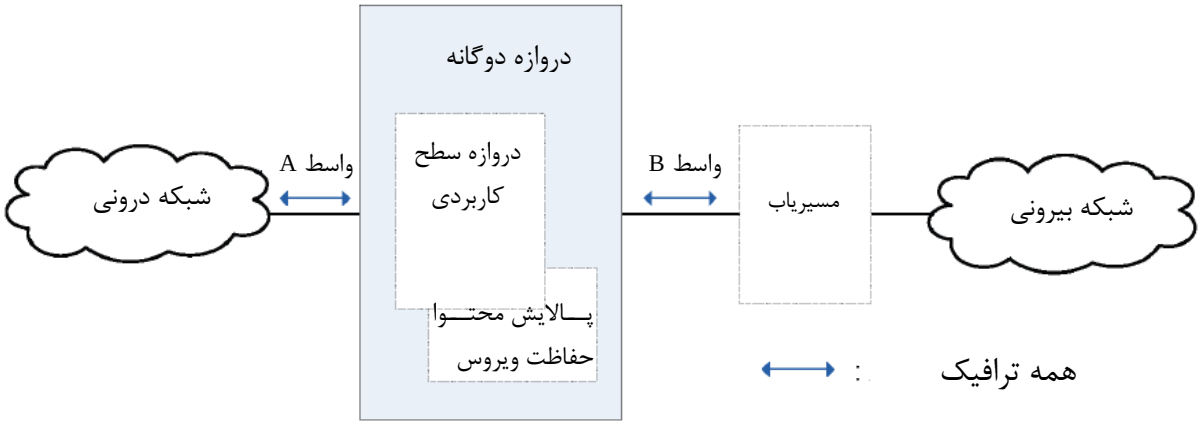
دیواره آتش‌های پالایش بسته دو نقطه قوت اصلی دارند: سرعت و انعطاف‌پذیری. از آن‌جا که پالایش بسته به‌طور معمول داده‌های بالای لایه ۴ از مدل OSI را بررسی نمی‌کند، می تواند با سرعت کار کند. این سادگی این امکان را می دهد تا دیواره آتش‌های پالایش بسته به‌عنوان یک مسیریاب خارجی در جلوی میزبان یا زیرشبکه غربال‌شده مستقر شوند. دلیل قابلیت قرارگیری آن‌ها، جلوگیری آن‌ها از منع خدمت و نیز حملات این چنینی می باشد. مسیریاب‌های غربال‌گری نمی توانند از حملاتی که از کارکردها و آسیب‌پذیری‌های خاص برنامه کاربردی استفاده می‌کنند، جلوگیری نمایند، زیرا این مسیریاب‌ها داده‌های لایه بالاتر را بررسی نمی‌کنند (لایه ۵ - ۷). نتیجه اطلاعات محدود در دسترس دیواره آتش، کارکرد واقعه‌نگاری محدود در دیواره آتش‌های پالایش بسته است. با توجه به تعداد زیاد متغیرهای مورد استفاده در تصمیمات واپایش دسترسی، این متغیرها مستعد بروز نقض امنیتی ناشی از پیکربندی‌های نامناسب هستند.

۲-۲-۱۰ معماری دروازه دوگانه

دروازه دوگانه یک پیشکار برنامه کاربردی/دروازه برنامه کاربردی است که اتصال انتها به انتها را می شکند. دروازه دوگانه در شکل ۴ نشان داده شده است که شامل یک سامانه میزبان با دو واسط شبکه A و B، و با قابلیت ارسال IP میزبان غیر فعال است. بنابراین، بسته‌های IP به‌طور مستقیم از یک شبکه (مثلا اینترنت) به شبکه دیگر منتقل نمی‌شود (به عنوان مثال شبکه داخلی). سامانه‌های شبکه داخلی می توانند با میزبان دوگانه ارتباط برقرار کنند، و سامانه های خارج از دیواره آتش در شبکه‌های خارجی می‌توانند با میزبان دوگانه ارتباط برقرار کنند، اما این سامانه‌ها نمی توانند به‌طور مستقیم با یکدیگر ارتباط برقرار نمایند.

اگر میزبان مجهز به چند کارت شبکه باشد، پیکربندی‌های مختلفی وجود خواهد داشت، به عنوان مثال به اینترنت برای اتصال به شبکه‌های جداگانه از ارائه‌دهندگان خدمات اینترنت، و یا به شبکه داخلی به کارسازهای مختلف مانند کارسازهای پست الکترونیک و یا کارساز واقعه‌نگاری. در این مورد، به عنوان یک دروازه چندگانه نامیده می‌شود.

در صورت تمایل، مسیریابی را که به عنوان یک پالایش بسته عمل می‌کند می توان در اتصال به شبکه های خارجی قرار داد تا محافظت بیشتری توسط پالایش بسته‌های شبکه فراهم نماید. دروازه دوگانه همه ترافیک IP مستقیم بین شبکه‌های خارجی و وبگاه محافظت‌شده را مسدود می‌سازد. خدمت و دسترسی، توسط خدمات پیشکار در سطح کاربرد در دیواره آتش فراهم می‌شود.



شکل ۴- دروازه دوگانه

دروازه دوگانه نوعی از دروازه‌های امنیتی دارای شرایط بیشتر را نشان می‌دهد، به دلیل آن‌که این نوع دروازه، آدرس IP داخلی را از سامانه‌های شبکه های خارجی پنهان می‌سازد. و قابلیت واقعه‌نگاری را فراهم می‌کند. این قابلیت می‌تواند به همراه سامانه تشخیص نفوذ (IDS) برای شناسایی فعالیت‌های احتمالی مهاجم استفاده شود. انعطاف پذیری محدود - تنها خدماتی را می تواند عبور دهد که برای آن‌ها خدمات پیشکار وجود داشته باشد- می تواند یک نقطه ضعف برای برخی از وبگاه‌ها باشد.

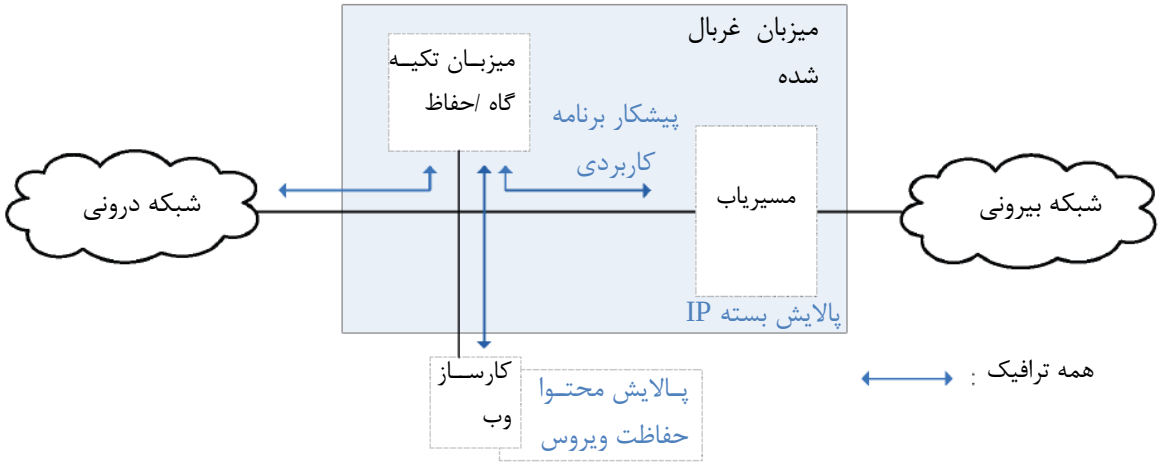
اگر ارتباط قابل اعتمادی را بتوان به عنوان میان‌بر در دروازه امنیتی مستقر نمود، در این‌صورت مسیریاب اضافی می تواند این مشکل را حل کند. امنیت سامانه میزبان مورد استفاده برای دیواره آتش برای حفاظت کلی بسیار مهم است چرا که اگر دیواره آتش به خطر بیافتد مهاجم می تواند دسترسی به سامانه‌های داخلی را به‌دست آورد.

۳-۲-۱۰ معماری میزبان غربال شده

معماری میزبان غربال‌شده در شکل ۵ نشان داده شده است، که ترکیبی از یک مسیریاب پالایش بسته با یک میزبان تکیه‌گاه است که از پیشکار برنامه کاربردی استفاده می‌کند. میزبان تکیه‌گاه در سمت زیرشبکه محافظت‌شده از مسیریاب قرار می گیرد. در این معماری، امنیت اولیه توسط مسیریاب پالایش بسته، فراهم می‌شود، به‌عنوان مثال برای جلوگیری از دور زدن کارسازهای پیشکار برای برقراری ارتباط مستقیم به شبکه داخلی.

پالایش بسته در مسیریاب غربالگری به گونه‌ای تنظیم شده که میزبان تکیه‌گاه تنها سامانه‌ای است که میزبان‌هایی از شبکه های خارجی می توانند با آن اتصال برقرار کنند. چنین میزبان تکیه‌گاهی، به عنوان یک دیواره آتش در سطح کاربرد، شامل خدمات پیشکاری است که عبوردهی و یا مسدود کردن را با توجه به خط مشی وبگاه انجام می‌دهد. مسیریاب به‌طور ذاتی پروتکل‌های خطرناک را از رسیدن به دیواره آتش و سامانه-های وبگاه پالایش می‌کند.

ترافیک برنامه کاربردی از شبکه‌های خارجی به میزبان تکیه‌گاه مسیریابی می‌شود. تمام ترافیک‌های دیگر از وبگاه‌های خارجی رد می‌شود. مسیریاب ترافیک نشات گرفته از هر برنامه کاربردی از شبکه‌های داخلی را رد می‌کند مگر این‌که از سوی میزبان تکیه‌گاه آمده باشد.



شکل ۵- میزبان غربال شده

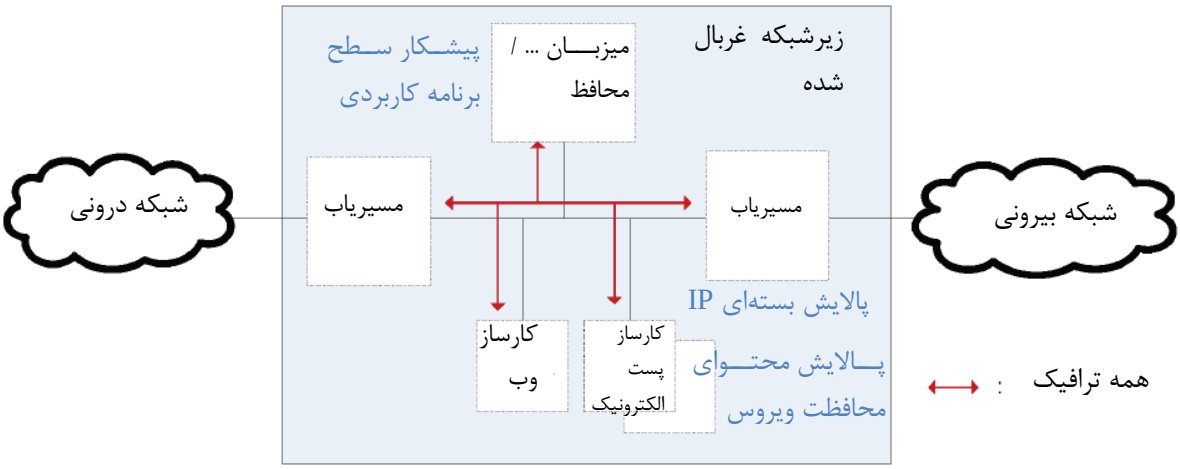
معماری میزبان غربال شده ترکیبی از یک مسیریاب پالایش بسته با یک میزبان تکیه‌گاه است که از پیشکارهای برنامه کاربردی استفاده می‌کند. میزبان تکیه‌گاه است که در سمت زیرشبکه محافظت‌شده از مسیریاب قرار می گیرد.

در این معماری، امنیت اولیه توسط مسیریاب پالایش بسته، فراهم می‌شود، به عنوان مثال برای جلوگیری از دور زدن کارساز های پیشکار برای برقراری ارتباط مستقیم به شبکه داخلی.

پالایش بسته در مسیریاب غربالگری به گونه‌ای تنظیم شده که میزبان تکیه‌گاه تنها سامانه‌ای است که میزبان‌های از شبکه های خارجی می توانند با آن ارتباط باز کند. چنین میزبان تکیه‌گاهی، به عنوان یک دیواره آتش در سطح کاربرد، شامل خدمات پیشکاری است که عبوردهی و یا مسدود کردن را با توجه به خط مشی وبگاه انجام می‌دهد. مسیریاب به‌طور ذاتی پروتکل‌های خطرناک را از رسیدن به دیواره آتش و سامانه‌های وبگاه پالایش می‌کند.

ترافیک برنامه کاربردی از شبکه های خارجی به میزبان تکیه‌گاه مسیریابی می‌شود. تمام ترافیک‌های دیگر از وبگاه‌های خارجی رد می‌شود. مسیریاب ترافیک نشات گرفته از هر برنامه کاربردی از شبکه های داخلی را رد می‌کند مگر این‌که از سوی میزبان تکیه‌گاه آمده باشد.

۴-۲-۱۰ معماری زیرشبکه غربال



شکل ۶- زیرشبکه غربال شده

معماری زیرشبکه غربال‌شده، که در شکل ۶ نشان داده شده است، یک گونه از معماری‌های دروازه دوگانه است و میزبان غربال‌شده است. این معماری با افزودن یک محیط شبکه با هدف جدا شدن بیشتر شبکه داخلی از شبکه‌های خارجی مانند اینترنت، یک لایه اضافی از حفاظت را به معماری میزبان غربال‌شده اضافه می‌کند.

دو مسیریاب برای ایجاد زیرشبکه درونی و غربال‌شده استفاده می‌شود. این زیرشبکه، که گاهی اوقات به عنوان منطقه غیرنظامی (DMZ) و یا یک محیط شبکه شناخته می‌شود، میزبان تکیه‌گاه و یا دیواره آتش سطح کاربرد را در خود جای می‌دهد، با این حال، می تواند کارساز وب (ها)، کارساز پست الکترونیک (ها) و یا کارساز DNS (ها) و سامانه‌های دیگر را که نیاز به دسترسی واپایش‌شده به دقت دارند در خود جای دهد. مسیریاب خارجی دسترسی از شبکه‌های خارجی به سامانه‌های خاص در زیرشبکه غربال‌شده را محدود می‌سازد (به عنوان مثال مسیریابی ترافیک پست الکترونیک از وبگاه‌های اینترنتی به کارساز پست الکترونیک)، و تمام ترافیک‌های دیگر را به شبکه های خارجی از سوی سامانه‌ها نشات گرفته که توصیه نمی‌شود اتصالات منشا باشند را مسدود می‌سازد (به عنوان مثال قرار دادن‌های NFS به سامانه های خارجی). مسیریاب داخلی ترافیک را به و از سامانه روی زیرشبکه غربال‌شده با توجه به قوانین موجود عبور می‌دهد (به عنوان مثال مسیریابی ترافیک پست الکترونیک از سامانه‌های وبگاه به کارساز پست الکترونیک و بالعکس).

در مورد دروازه‌های دوگانه و همچنین اغلب با دروازه‌های چندگانه، مهم است که هیچ سامانه داخلی به‌طور مستقیم از طرف شبکه‌های خارجی و بالعکس قابل دسترسی نباشد. با معماری زیرشبکه غربال‌شده، به‌طور مطلق هیچ ضرورتی برای پیاده‌سازی میزبان تکیه‌گاه مربوطه در دروازه سطح کاربرد به عنوان یک سامانه دوگانه وجود ندارد.

معماری زیرشبکه غربال‌شده ممکن است برای وبگاه های با مقدار زیاد ترافیک یا وبگاه‌هایی که نیاز به ترافیک با سرعت بسیار بالا دارند، مناسب تر باشد.

۱۱ راهنمایی برای انتخاب محصول

۱۱-۱ مرور کلی

فرض بر این است که اگر سازمانی به اینترنت متصل است، بنابراین شبکه‌های خود را اکنون توسط نوعی از دیواره آتش پالایش بسته‌ها محافظت کرده است. اگر این گونه نیست، بنابراین نیاز به قرار دادن و پیکربندی یک دیواره آتش محیط با توجه به خط مشی امنیتی توسط یک سازمان به‌عنوان نهایت اضطرار وجود دارد.

فرض بر این است که میزبان‌ها در همان زیرشبکه سطوح مشابهی از اعتماد را دارند. به عنوان مثال فرض بر این است که کارسازهای به بیرون‌رو[1] در سازمان (وب، پست الکترونیک، DNS و غیره) بر روی زیرشبکه جدای خود، و متمایز از زیرشبکه‌ی میزبان‌های داخلی سازمان هستند. اگر میزبان‌های دارای تفاوت معنی‌دار در سطح اعتماد، در زیرشبکه‌ی مشابهی سهیم باشند، نیاز است برای مشخص شدن مرز بین حوزه‌های اعتماد مختلف، طراحی شبکه تغییر نماید. در این مرزها است که لوازم دروازه‌های امنیت شبکه قرار داده خواهد شد.

برای اطمینان از این‌که الزامات همانطور که در بند ۸ ذکر شده به انجام برسد، یک رویکرد ساختار یافته برای انتخاب و پیکربندی دروازه‌های امنیتی ضروری است. این بند برخی راهنمایی برای این فرایند ارائه می‌دهد، به ویژه در زمینه های:

- انتخاب یک معماری امنیتی دروازه و مولفه‌های مناسب.
- انتخاب بستر سخت‌افزار و نرم‌افزار؛
- پیکربندی.
- ویژگی‌ها و تنظیمات امنیتی.
- سرپرستی؛
- واقعه‌نگاری.
- ممیزی. و
- آموزش/پرورش.

به عنوان یک راهنمای کلی، توصیه می‌شود اصول زیر به‌کار برده شود:

- توجه به تمام تهدیدهای ممکن، که به خصوص شامل تهدیدات داخلی است.
- توجه به عامل انسانی، به عنوان مثال در زمینه سرپرستی و آموزش
- تا حدامکان ساده گرفته شود، هرچند الزامات امنیتی بالاتر به‌طور معمول مستلزم معماری پیچیده‌تری هستند. و
- مولفه‌ها یا افزاره‌ها را در کارکرد و پیکربندی تعیین شده استفاده کنید.

۱۱-۲ انتخاب معماری دروازه امنیتی و مولفه‌های مناسب

توصیه می‌شود بر اساس الزامات کسب و کار و امنیت برای دروازه امنیتی (برای اطلاعات بیشتر به بند ۸ مراجعه شود)، معماری دروازه امنیتی مناسب انتخاب شود و سازگار شود (برای یک نمای کلی از معماری‌های دروازه امنیتی ممکن به بند ۱۰-۲ مراجعه شود).

1- Outward-facing servers

هنگامی که یک معماری تعریف شده است، هر جزء از این معماری باید بیشتر مشخص شده و نیاز است که کارکرد آن‌ها ارزیابی شود، اشاره به ۱۰-۲ برای یک مرور کلی از مولفه‌های ممکن و به ۱۰-۱ برای شرح مفصلی از کارکرد ارائه شده است. در عمل چند لایه از دروازه‌ها اغلب استفاده می‌شود.
زیر بندی که در ادامه می‌آید برخی راهنمایی های بیشتر در انتخاب مولفه‌های مناسب با معماری مناسب را ارائه می‌کند.

۱۱-۳ بستر نرم‌افزاری و سخت‌افزاری

هنگام انتخاب یک بستر سخت‌افزاری، توصیه می‌شود عملکرد، کارایی، قابلیت اطمینان و کاربست‌پذیری به طور ویژه در نظر گرفته شود، به عنوان مثال اگر بستر تنها واسط اترنت دارد، اما رله قاب[1] روی V.35 مورد نیاز است، پس این بستر غیر قابل استفاده است. در مورد بعدی سامانه عامل افزاره سخت‌افزاری باید دیده شود. توصیه می‌شود برای مقاصد امنیتی، سامانه عامل سخت‌شده استفاده شود. همچنین توصیه می‌شود آن را در برابر آسیب پذیری های شناخته شده وارسی کنید. بستر نرم‌افزاری نیز نیاز است با توجه به عملکرد و قابلیت اطمینان درستی‌آزمایی شود، به عنوان مثال یک مسیریاب با واسط اترنت 10BaseT نمی تواند حجم-گذر گیگابیتی فراهم کند.

۱۱-۴ پیکربندی

توصیه می‌شود تنظیمات پیشنهادی زیر برای افزاره‌های شبکه دروازه امنیتی در طول مدت فرایند پیکربندی در نظر گرفته شود:
- شبکه سودهی برای معماری زیرشبکه غربال‌شده مربوط به منطقه غیرنظامی.
- مسیریابی ایستا بین مسیریاب (ها) و دروازه امنیتی.
- توصیه نمی‌شود منبع اطلاعات مسیر یابی پذیرفته شود.
- توصیه می‌شود فقط نرم‌افزار/برنامه‌ها که برای بهره برداری(«قوی‌سازی بستر») کاملا ضروری می باشد، بر روی دروازه امنیتی نصب شود.
- حصول اطمینان از فعال نبودن درگاه‌ها به‌طور پیش فرض.
- حصول اطمینان از فعال نبودن تحلیل‌گر درگاه سودهی (SPA) مگر در مواردی که استفاده از سامانه‌های تشخیص نفوذ مورد نیاز باشد.
- حصول اطمینان از پیاده‌سازی کلمه‌های عبور در واسط‌های افزاره.
- رد کردن پیام پروتکل اطلاعات مسیریابی (RIP) «مسیریابی نادقیق منبع»؛
- قابلیت ترجمه مناسب آدرس شبکه.
- عملیات شفاف دروازه امنیتی.
- واپایش دسترسی در دروازه امنیتی (شناسایی، تصدیق هویت).
- در صورت از کار افتادن دروازه‌های امنیت تنها وظایف سرپرستی ممکن باشد.
- اطمینان از «واقعه‌نگاری» از تمام رویدادهای سرپرستی و تمام ترافیک.

1- Frame relay

- سخت‌سازی بستر در رابطه با سامانه عامل.

۵-۱۱ تنظیمات و ویژگی‌های امنیتی

به عنوان کمینه، توصیه می‌شود دیواره آتش برنامه کاربردی موارد زیر را فراهم نماید:

- پشتیبانی از خدمات اصلی اینترنت (HTTP، FTP، Telnet، SMTP، NNTP).
- پشتیبانی از خدمات بیشتر اینترنت.
- پشتیبانی از پیشکارهای عمومی (برای پروتکل‌های و یا خدمات جدید).
- توصیه می‌شود پیشکار HTTP قادر به ساماندهی HTTPS به درستی باشد؛
- رد کردن پیام اطلاع رسانی پروتکل دروازه مرزی (BGP) (به عنوان مثال توسط پیشکار عمومی).
- پشتیبانی از پروتکل‌های مسیریابی پویا.
- پشتیبانی از خدمات وب (به عنوان مثال SOAP / XML).
- پشتیبانی از پیشکارها برای برنامه های سازمانی بسته بندی‌شده و یا دیگر برنامه های کاربردی کسب و کار؛
- پشتیبانی از شناسایی برنامه‌های در حال اجرا در جریان پروتکل(برنامه‌های کاربردی بهره‌وری اداری، ویدئوی جاسازی شده، پیام های فوری و غیره)؛
- پشتیبانی از پالایش ترافیک ورودی برای نرم‌افزارهای مخرب و غیره، در صورت اتصال به VPN.
- امکان اجازه، انکار، و یا حذف اتصالات و یا بسته‌ها.

به عنوان کمینه، توصیه می‌شود افزاره پالایش بسته باید قادر به موارد زیر باشد:

- پالایش بسته بر اساس (بسته).
- آدرس IP منبع و مقصد.
- درگاه منبع و مقصد (برای TCP، UDP).
- جهت اتصال (ورودی، خروجی).

به عنوان کمینه، توصیه می‌شود هر دو افزاره پالایش بسته و پالایش بسته حالت دار باید قادر به موارد زیر باشد:

- حفظ قوانین پالایش به‌طور ذاتی سازگار.
- پالایش بسته‌ها به‌طور جداگانه برای هر واسط شبکه.
- پشتیبانی از بسته‌های چندپخشی اگر خوشه‌بندی افزاره مورد نیاز است.
- حفظ نظم قوانین پالایش توسط دروازه امنیتی.
- محدود کردن طول قطعات بسته‌های IP و تعریف کمینه نمایه بستک.
- پالایش پیام های ICMP «مقصد غیر قابل دسترسی» و «تغییر مسیر»؛
- جلوگیری از جعل هویت آدرس‌های IP داخلی در صورتی‌که از اینترنت (با توجه به جعل هویت IP) آمده است.

علاوه براین، به عنوان کمینه، توصیه می‌شود افزاره پالایش حالت دار باید قادر به انجام دادن موارد زیر باشد:

- پشتیبانی از خدمات NFS، NIS، RPC، RIP، OSPF، DNS، WAIS با حفاظت کافی از طریق پالایش-های پویای بسته.
- شناسایی برخی حملات خاص منع خدمت مانند جاری شدن سیل TCP-SYN.
- جلوگیری از حدس زدن شماره ترتیب TCP.
- مقاومت در برابر حملات ping-of-death (نوعی از حملات منع خدمت).
- استفاده پیوسته از دستورات FTP با حقوق دسترسی خاص؛
- فعال کردن ذخیره‌سازی اطلاعات زمینه، به‌عنوان مثال برای وارسی شماره‌های درگاه تخصیص یافته به صورت پویا.
- پالایش اشیاء دیگر شبکه (دامنه‌ها، گروه‌ها، اشیاء VPN، و غیره)؛
- جلوگیری از حملات خاص ربودن نشست.

توصیه می‌شود دیگر ویژگی‌های متفرقه و یا تنظیمات بازبینی شود، به عنوان مثال:
- ایجاد هشدار هنگام شناسایی نفوذ، یا بر اساس واقعه‌نگاری و یا حسگر تشخیص نفوذ.
- لازم به ذکر است که برنامه‌های کاربردی که از سازوکار ارتباطات SOAP استفاده می‌کنند، می‌توانند غیر قابل تشخیص از طریق بازرسی و دیواره آتش‌های پیشکار حالت دار برنامه کاربردی عبور کنند. این امر فرصتی برای هدف پیش‌دستی نسبت به پیشکار برنامه کاربردی و دیگر خط مشی‌های دیواره آتش فراهم می‌کند. نیاز توجه ویژه به شرایطی که در آن برنامه‌های کاربردی مبتنی بر SOAP نیاز به ارتباط های عبور داده شده از دروازه امنیتی دارند، وجود دارد: به عنوان مثال، برخی از برنامه‌های کاربردی مبتنی بر SOAP را می‌توان با پیاده‌سازی پالایش‌های محتوای XML خاص برنامه‌های کاربردی محافظت کرد (در دیواره آتش XML است که امکان برنامه‌ریزی پالایش مناسب XML ایجاد می‌شود) و/یا با اعمال یک خط مشی که برقراری از طریق یک دروازه امنیتی را تنها زمانی اجازه می‌دهد که برنامه های مبتنی بر SOAP توسط یک VPN انتها به انتها محافظت شود.

۱۱-۶ قابلیت سرپرستی

فرایند سرپرستی یکی از حساس‌ترین وظایف در نگهداری یک سطح کافی از امنیت است. توصیه می‌شود به-طور عمده به ویژگی‌های امنیتی دروازه که در زیر بیان می‌شود توجه شود:
- شناسایی و اصالت سنجی سرپرستان دروازه امنیتی.
- راه قابل اطمینان ارتباطات برای وظایف سرپرستی (مانند کنسول، ارتباط رمز شده، شبکه جداشده).
- سرپرستی از راه دور تنها با اصالت سنجی و رمزگذاری قوی.
- امکان سرپرستی متمرکز در موارد استقرار دروازه‌های امنیتی متعدد.
- آزمون جامعیت برنامه‌ها و پوشه‌های استفاده شده توسط دروازه امنیتی.
- توصیه می‌شود واقعه نگاری‌های مربوط به هشدار دروازه امنیتی قادر به ارسال به میزبان خارجی باشد.
- هشدار به سرپرست از هر کانال مناسب امن، به‌عنوان مثال پست الکترونیک، SMS.

- اجازه دسترسی دانه‌درشت، به عنوان مثال توصیه می‌شود حساب‌های «admin» و «read-only» وجود داشته باشد تا امکان انجام ممیزی خط مشی‌ها و واپایش‌ها از حساب read-only ایجاد شود.
- تلاش‌های پایین سرپرستی.

۱۱-۷ قابلیت واقعه‌نگاری

فرآیند واقعه‌نگاری، زمانی‌که ردیابی جریان‌های داده مورد نیاز است بسیار مهم است، به‌عنوان مثال برای بازیابی فاجعه، تحقیقات قانونی و غیره:
- قابلیت برای واقعه‌نگاری (شناسایی کاربر، آدرس IP منبع و مقصد، شماره درگاه، زمان، تاریخ). نکته‌ای که در این‌جا وجود دارد این است که هر چه اطلاعات بیشتری ذخیره می‌شود، رخداد بهتر سامان‌دهی می‌شود.
- قابلیت برای همگام‌سازی با کارساز NTP برای تاریخ و زمان دقیق؛
- حفاظت از پوشه‌های واقعه‌نگاری در برابر تغییرات مخرب و دسترسی های غیرمجاز.

۱۱-۸ قابلیت ممیزی

توصیه می‌شود دروازه امنیتی در حالی که مفاهیم اساسی امنیت اطلاعات مانند محرمانگی، جامعیت، دسترس‌پذیری، اصالت سنجی، حسابرسی و عدم انکار را حفظ می‌کند، از تسهیلات ممیزی به‌منظور درستی‌آزمایی پرونده(ها) واقعه‌نگاری پشتیبانی کند.

۱۱-۹ آموزش و پرورش

توصیه می‌شود به‌طور عمده به آموزش و پرورش ویژگی‌های دروازه‌های امنیت که در زیر بیان شده توجه شود:
- توصیه می‌شود دروازه‌های امنیتی با مستندات و مواد پشتیبانی کافی برای نصب و راه‌اندازی و پیاده‌سازی همراه باشند، تا از حفاظت کافی شبکه‌ها و سامانه‌ها اطمینان حاصل شود.
- توسعه مواد آموزشی برای کارکنان درگیر در بهره‌برداری و نگهداری.
- توصیه می‌شود کارکنان درگیر در بهره‌برداری و نگهداری از دروازه امنیتی به صورت دوره‌ای آموزش داده شوند تا اطمینان حاصل شود که کارکنان در سطح کافی از دانش و مهارت نگهداری می‌شوند.

۱۱-۱۰ انواع پیاده‌سازی

به‌طور کلی دو نوع پیاده‌سازی دیواره آتش وجود دارد: «سخت‌افزاری» و «نرم‌افزاری». این دو نوع نیز می تواند به انواع مختلفی شکسته شوند. سخت‌افزار به‌طورعمده به راه‌حل‌های لوازمی اشاره دارد و، در حال حاضر رایج‌ترین افزاره‌های دروازه هستند. راه حل‌های سخت‌افزاری را می توان به زیر نوع سخت افزار مبتنی بر CPU (به عنوان مثال I386 / X64) با سامانه عامل سخت‌شده، و افزاره هایی ساخته شده با هدف که اغلب شامل تراشه‌های "ASIC" برای انجام وظایف خاص مانند دیواره آتش سرعت بالا یا شتاب VPN، تقسیم‌بندی نمود. همچنین برخی از آن‌ها وجود دارد که دیواره آتش‌های سخت افزاری ساخته شده درون واسط شبکه هستند که کمتر مورد استفاده قرار می‌گیرد.

چند دیواره آتش سخت‌افزاری وجود دارند که گزینه‌ای برای ایجاد «دیواره آتش‌های مجازی» دارند کـه اگـر چه بخشی از همان تجهیزات فیزیکی هستند، اما به‌صورت منطقی جدا از هـم هسـتند و واسـطهـای خـود، مجموعه قوانین و جداول مسیریابی مرتبط با خود را دارند.
دیواره آتش نرم‌افزاری می تواند بیشتر نرم‌افزار سنتی باشد که در بالای یک سامانه عامل سخت‌شده، دیـواره آتش‌های «شخصی» برای سامانه‌های کاربر نهایی، یا تصاویر مجـازی کـه مـی‌توانـد در محـیط‌هـای کارسـاز مجازی استفاده شود، نصب می‌شود.
برخی از دیواره آتش نرم‌افزاری همچنین در لایه ابرناظر قرار می‌گیرد تا واپایش جریان ترافیک را از سـامانه-های مجازی انجام دهد.

۱۱-۱۱ دسترس‌پذیری بالا و حالت بهره‌برداری

اکثر سازمان در حال حاضر از برخی انواع فناوری دسترس‌پذیری بالا یا خوشه‌بندی برای افـزایش دسـترس-پذیری استفاده می‌نمایند. این موضوع به‌طور معمول با استفاده از فناوری فروشنده و نیـز بـا سـوده‌هـای بـار متعادل به دست می‌آید. توصیه می‌شود خرابی تک نقطه (SPOF) در دروازه امنیتی که می‌توانـد دسـترس-پذیری را تحت تاثیر قرار دهد در نظر گرفته شود.

۱۱-۱۲ ملاحظات دیگر

توصیه می‌شود سایر افزاره‌ها و سامانه‌ها که می‌تواند روی سطوح کلی امنیت تاثیر بگذارد بـازبینی شـود، بـه عنوان مثال:
- توصیه می‌شود هر گونه اتصالات دسترسی از راه دور توسط دروازه امنیتی امن شود؛
- وارسی ضد ویروس.
- پالایش کد اجرایی مانند جـاوا، جـاوا اسـکریپت، MIME، ActiveX. حتـی اگـر در انتقـال داده‌هـا FTP گنجانیده شده است.
- استفاده از دروازه‌های امنیتی در زمینه شبکه‌های خصوصی مجازی (VPN).

یادآوری- امن‌سازی ارتباطات با استفاده از شبکه‌های خصوصی مجازی، موضوع اسـتاندارد ISO / IEC 27033-5 را تشـکیل می‌دهد.

- یکپارچه‌سازی محتوای محصولات امنیتی طرف سوم:
معماری‌های دروازه امنیتی اغلب راه‌حل‌های امنیت محتوا شامل پویش و وارسی پوشه‌ها و یا ترافیک اینترنت (به عنوان مثال SMTP، FTP، HTTP) برای ویـروس یـا کـد مخـرب را یکپارچـه مـی‌سـازند. از یـک سـو، رویکردهایی با کارسازهای دروازه جدا وجود دارد که ترافیک اینترنـت و یـا خـدمات ویـژه اینترنـت را بـرای ویروس یا کد مخرب گذر کرده از طریق کارسازها، پویش و از ورود کد خطرناک به شبکه داخلی جلـوگیری می‌کند. از سوی دیگر، راه‌حل‌هایی با یکپارچه‌سازی نزدیک‌تر قابلیت هـای بازرسـی محتـوا توسـط کتابخانـه پیوند پویا (DLL) و یا واسط برنامه‌نویسی کاربردی (API) با محصـول دیـواره آتـش وجـود دارد. همچنـین وارسی یا غربالگری URLها اغلب در رویکردهای امنیت محتوا گنجانده شده است.
- یکپارچه‌سازی سامانه تشخیص نفوذ (IDS).

در زمینه دروازه‌های امنیتی، سامانه های تشخیص نفوذ در منطقه غیرنظامی واقع می‌شوند. سامانه‌های دیواره آتش مانند کارسازهای برنامه کاربردی مهم متعلق به این چنین سامانه ها هستند که توسط یک حسگر سامانه تشخیص نفوذ واپایش می‌شود. برای اطلاعات بیشتر به استاندارد ISO/ IEC TR 15947: 2002 مراجعه شود.

کتاب‌نامه

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

[۲] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات –فنون امنیتی– سامانه‌های مدیریت امنیت اطلاعات– الزامات

[۳] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات –فنون امنیتی– سامانه‌های مدیریت امنیت اطلاعات– آیین کار مدیریت امنیت اطلاعات

[۴] استاندارد ملی ایران شماره ۲۷۰۳۳-۳: سال ۱۳۹۳، فناوری اطلاعات -فنون امنیتی-امنیت شبکه قسمت ۳ -فرانامه های شبکه بندی مرجع -تهدیدها -فنون طراحی و مسائل کنترلی

[5] Recommendation ITU-T X.25:1996, Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit

[6] IEEE 802.3: *Defines the MAC layer for bus networks that use CSMA/CD*

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

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

[9] Chapman D.B., & Zwicky E.D. Building Internet Firewalls. O'Reilly, Cambridge, 2000

[10] Cheswick W .R. & B ellovin S.M. Firewall and Internet Security: Repelling the Wily Hacker. Addison-Wesley, Reading, 1994

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

[12] Siyan K., & Hare C. Internet Firewalls and Network Security. New Riders Publishing, Indianapolis, 1995

[13] Wack J ., C utler K ., P ole J. 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)