بررسی امنیت فایروال وراهکارها

سمیه خدابنده لو

مقدمه ای بر فایروال

امروزه روش‌های بسیاری برای مقابله با ویروس‌ها و بدافزاری جاسوسی وجود دارد. استفاده از فایروال‌ها یکی از کاربردی‌ترین روش‌های مقابله با حملات سایبری است. ممکن است در مورد فایروال برای شبکه خانگی خود نیز چیزهایی شنیده باشید. این طور به نظر می رسد که یک شبکه خانگی کوچک با مسایل امنیتی مشابهی با شبکه های شرکت های بزرگ درگیر است. شما می توانید برای محافظت از شبکه خانگی خود و خانواده در مقابل وب سایت های مخرب یا نفوذ بالقوه هکرها از فایروال استفاده کنید.در واقع ، فایروال مانعی برای جلوگیری از نفوذ نیروهای مخرب به دارایی های مجازی شما است. به همین دلیل است که به آن فایروال (دیواره آتش) نام داده اند. کار آن شبیه به دیوار فیزیکی است که از گسترش آتش از یک منطقه به منطقه دیگر جلوگیری می کند. دیواره‌های آتش یکی از مؤثرترین و مهمترین روشهای پیاده سازی "مصونیت شبکه "هستند و قادرند تا حد زیادی از دسترسی غیر مجاز دنیای بیرون به منابع داخلی جلوگیری کنند.دیواره‌های آتش، مانند خندق‌های دور قلعه‌های دوران قرون وسطی عمل می‌کنند. دیواره آتش اغلب در نقطه‌ای که شبکه داخلی به شبکه خارجی متصل است قرار داده می‌شود . تمام ترافیکی که از سمت شبکه خارجی به شبکه داخلی وارد می‌شود و یا از شبکه داخلی به سمت شبکه خارجی، خارج می‌شود از دیواره آتش عبور می‌کند، به همین علت دیواره آتش فرصت و موقعیت مناسبی را داراست که تشخیص دهد آیا ترافیک عبوری مورد پذیرش هست یا خیر. اینکه چه ترافیکی مورد پذیرش هست به "سیاست

امنیتی(Security Policy) [1]شبکه باز می‌گردد. سیاستهای امنیتی تعیین می‌کنند که چه نوع ترافیکهایی مجوز ورود و یا خروج را دارا هستند .انواع پیچیده تر دیواره های آتش به صورت ترکیبی از چندین سیستم و راه حلهای Multi-computer[2]و Multi-router[3] پیاده سازی می‌شوند. شبکه های مختلف بسته به نیازهای امنیتی مختلف و هزینه ای که برای تأمین امنیت در نظر گرفته اند از دیواره‌های آتش مختلف و روشهای پیاده سازی مختلف آنها استفاده می‌کنند .

سپاس گذاری:

از استاد ارجمند جناب آقای صادقی استاد فرهیخته دوران تحصیل و استاد راهنمای این پروژه کمال تشکر و سپاسگزاری می کنیم و از خداوند برای ایشان بهترین ها را خواستاریم.

[1] سیاست امنیتی

[2] چند کامپیوتری

[3] چند روتری

تقدیم به:

همه کسانی که درسختی‌ها و دشواری‌های زندگی همواره یاوری دلسوز وفداکار و پشتیبانی محکم ومطمئن برایم بوده‌اند.

چکیده

فایروال وسیله ای است که کنترل دسترسی به شبکه رابنابرسیاستهای امنیتی شبکه تعریف میکند.وسیستم وشبکه راازنفوذ کاربران وهکرهای غیرمجاز برنامه های محافظت می کند. دیوار آتش یکی از مهمترین لایه‌های امنیتی شبکه‌های کامپیوتری است. مزیت استفاده ازفایروال اینست که شبکه وسیستمی امن داریم . دیواره‌های آتش یکی از مؤثرترین و مهمترین روشهای پیاده سازی "مصونیت شبکه "هستند و قادرند تا حد زیادی از دسترسی غیر مجاز دنیای بیرون به منابع داخلی جلوگیری کنند.

فهرست مطالب

عنوان **صفحه**

مقدمه ای بر فایروال.....أ

سپاس گذاری:.....ت

تقدیم به:.....ث

چکیده.....ث

فهرست مطالب.....I

فصل اول.....1

1-1مقدمه فصل یک: 2

1 -2 تاریخچه: 3

مبانی طراحی فایروال:.....5

1-4 تعریف فایروال.....6

1-5 مشخصه‌های مهم یک فایروال.....7

1-5-2 بازدید حجم بالایی از بسته‌های اطلاعات:.....7

1-5-3 سادگی پیکربندی:.....7

1-5-4 امنیت و افزونگی فایروال:.....8

امنیت سیستم عامل فایروال :.....8

دسترسی امن به فایروال جهت مقاصد مدیریتی :.....8

1-7 نتیجه گیری این فصل.....9

فصل دوم.....10

2-1 مقدمه فصل دوم:.....11

2-2 انواع دیواره‌های آتش از لحاظ عملکرد: 11

2-3 فایروالها راازلحاظ عملکرد.....14

2–3–3 فیلترهای Nosstateful packet : 14
2–3–4 فیلترهایِ Stateful Packet : 15
2–3–5 دیواره‌های آتش شخصی 15
2–4 انواع فایروالها: 16
2–4–1 مسیر کاربردی: 16
2–4–2 فیلتر کردن بسته 17
2–4–3 سیستمهای ترکیبی (Hybrid systems): 17
2-5-1 Packet Filtering Firewall 18
2-5-2 Stateful Packet Inspection 18
2-5-3 Circuit Level Gateway 18
2-5-3 Aplication Level Gateway 19
SMLI (Staeful Multi Level Inspection) 19
2–6 چه نوع فایروال هایی وجود دارد ؟ 20
2-6-1 فایروال ها سخت افزاری : 20
2-6-2 فایروال های نرم افزاری : 21
2-6-3 فایروال NAT ساده 21
تفاوت فایروال سخت افزاری ونرم افزاری 22
2-**7** مسیریابهای بیسیم 22
2-7-1 مزایا 22
2-7-2 معایب 22
2-**8** ضرورت توجه به امکانات سایر فایروال های نرم افزاری 23
2-9 نتیجه این فصل: 24
فصل سوم 25
3–1 مقدمه فصل سوم : 26
3–2توپولوژی فایروال 27
3–2–1 موقیت قرار گیری فایروال از لحاظ فیزیکی : 27

3-2-2 در نظر گرفتن نواحی امنیتی مختلف با قابلیت دسترسی های متفاوت :.....27
3-2-3 حفاظت لایه ای :.....27
3-4 چند نوع توپولوژی :.....27
3-4-1 درون فایروال (بین فایروال و شبکه) :.....28
3-4-2 میان دو فایروال :.....28
3-5-1 لایه اول دیوار آتش:.....28
آدرس مبدا.....28
شماره شناسایی یک دیتاگرام قطعه قطعه شده.....29
3-5-2 لایه دوم دیوار آتش:.....30
3-5-3 لایه سوم دیوار آتش:.....30
فیلترهای Stateful و هوشمند:.....31
دیوار آتش مبتنی بر پراکسی (Proxy Based Firewall):.....32
3-6 ضرورت استفاده از فایروال.....32
3-8-1 نشانی IP.....33
3-8-2 نام حوزه (Domain name):.....33
3-9 فایروال در برابر چه خطراتی از ما محافظت می کنند؟.....34
3-9-1 ویروس ها.....34
3-9-2 اشکالات برنامه ها و سیستم عامل ها:.....34
3-9-3 ماکرو ها.....34
3-9-4 بمب های ایمیل:.....34
بررسی نحوه عملکرد فایروال Firewallیا دیواره آتش.....34
تبدیل آدرس.....35
نقطه پایانی VPN.....35
3-13 VPN.....36

3-12-1 مزایا.....36
3-12-2 معایب.....36
3-14 شیوه کاری یک فایروال به این صورت است:.....36
3-15-1 باستیون هاست (Bastion host):.....37
3-15-2 روتور:.....37
3-15-3 لیست کنترل دسترسی (ACL) :.....37
3-15-4 منطقه بیطرف (DMZ):.....37
3-15-5 پراکسی (Proxy):.....38
3-16 مزایای استفاده از پراکسی:.....38
3-16-1 ذخیره‌سازی.....38
3-16-2 دیوار آتش (fire wall).....39
3-16-3 فیلتر کردن.....39
3-16-4 تصدیق هویت.....39
3-16-5 تغییر هویت.....39
3-16-6 ثبت کردن.....39
3-17 مزایای پراکسی سرور.....40
3-18 برخی از انواع پراکسی.....40
نواحی خطر.....41
ناحیه امنیتی با Zone :.....41
توپولوژی های قرارگیری فایروال در شبکه: 42
طراحی Single-Firewall.....43
طراحی Dual Firewall:.....43
یک سیستم تشخیص نفوذ.....44
ابزارهای لازم برای تست نفوذ و ارزیابی فایروال:.....46

مزایا.....46
فایروال وهکرها.....47
فایروال بر روی چه برنامه هائی تاثیر می گذارد ؟.....48
طراحی فایروال محیطی (Perimeter Firewall) 48
طراحی فایروال برای Data Center و محافظت از یک Data Center 48
تعاریف.....48
طراحی جزیی محیطی:.....49
دفاع در عمق.....49
فایروال داخلی.....49
فایروالهای خارجی.....50
دستاوردها.....50
ضرورت توجه به امکانات سایر فایروال های نرم افزاری.....51
حفاظت با سه حالت فایروال.....51
حفاظت Keylogger 52
حفاظت DNS-Spoofing 52
کنترل Autostart 52
حالت بانکداری آنلاین.....53
پوشش محافظ برنامه.....53
تشخیص فعالیت ویروسی.....53
آنتی ویروس:.....54
Anti-Spam:.....55
فیلترینگ:.....55
پیکربندی فایروال و انواع DMZ در حفاظت از شبکه.....55
نتیجه فصل سوم:.....57

فصل چهارم 59
4-1 مقدمه فصل چهارم 60
4-2 مزایا و معایب استفاده از فایروال 61
4-2-1 معایب 61
Access Restrictions 61
Back-Door Challenges: The Modem Threat 61
4-2-2 مزایای فایروال: 62
4-3 مزایای فایروال های سخت افزاری 63
4-3-1 معایب: 63
4-4 فایروال نرم افزاری – برنامه ویندوز فایروال 64
4-4-1 مزایا : 64
4-4-2 معایب 64
4-5 برتری فایروال سخت افزاری به فایروال نرم افزاری 65
4-6 برتری فایروال نرم افزاری به فایروال سخت افزاری 65
مزایا 66
معایب : 66
4-5-1 مزایا 66
4-5-2 معایب 66
4-6توانایی‌های دیواره‌های آتش : 67
4-7 ناتوانی‌های دیواره‌های آتش: 68
4-8 دفاع لایه ای 70
راهکارهای هدفمند کردن وبهبودی فایروال 71
استفاده از دیوارهای آتش (فایروال) مبتنی بر میزبان) 71
4-9-3 چند راهکار طبقه بندی شده برای بهبود فایروال: ..... **Error! Bookmark not defined.**
پیکر بندی مناسب وبهینه فایروال 72

نحوه ی انتخاب یک فایروال مناسب.....73
نصب dmz.....73
استفاده از proxy server.....73
استفاده از آنتی ویروس وآنتی اسپم ها در کنار بسته فایروال.....73
مقابله با روت کیت:.....73
اسکن ترافیک داخل وخارج رایانه.....73
استفاده از تکنیک هایی برای مخفی ماندن.....73
استفاده از فایروال های چند لایه.....73
اتخاذ روشهایی برای عملکرد سریع.....74
متوقف کردن.....74
استفاده از فایروالهای تودرتو.....74
استفاده از سیستم تشخیص نفوذبه همراه فایروال.....74
افزودن لایه های مختلف به آنتی ویروس.....74
استفاده ازسیستم عامل های جداگانه.....74
بکارگیری هانی پات.....74
رمزنگاری:.....74
10-4 نتیجه گیری.....75
فصل پنجم.....76
1-5 مقدمه فصل پنجم:.....77
2-5 HONEY POT.....78
1-2-5 نحوه کار HONEY POT.....78
2-2-5 مزیت های یک هانی پات.....78
3-2-5 معایب هانی پات.....79
UTM.....79
تاریخچه‌ای پیرامونUTM 80

1-3-5 مزایایUTM.....80
2-3-5 وظایف امنیتی.....81
4-3-5سرویس‌های امنیتی تشکیل دهندهUTM 81
UTM و Firewallتفاوت.....82
6-5 آنتی فیلتر چیست ؟.....82
9-5 نتیجه فصل پنجم:.....83
فصل ششم.....84
1-6 مقدمه فصل ششم.....85
2-6نتیجه گیری کل.....85
Abstract.....86
فهرست منابع:.....87

فصل اول

1-1)مقدمه فصل یک:

امروزه روش‌های بسیاری برای مقابله با ویروس‌ها و بدافزاری جاسوسی وجود دارد. استفاده از فایروال‌ها یکی از کاربردی‌ترین روش‌های مقابله با حملات سایبری است دیوار آتش یکی از مهمترین لایه‌های امنیتی شبکه‌های کامپیوتری است که وجود نداشتن آن موجب می‌شود هکرها و افراد خراب کار بدون وجود داشتن محدودیتی به شبکه وارد شده و کار خود را انجام دهند

2-1)تاریخچه:

اولین نسل از دیواره های آتش در حدود سال 1985 بوجود آمدند و " دیواره های آتش پالایشگر بسته " (Packet filter firewalls4)نام گرفتند. ایده اصلی آنها از امکانات نرم افزاری گرفته شده بود که متعلق به شرکت Cisco بود و تحت عنوان Internetworking Operation system (IOS[5]) شناخته می شد. اولین مقاله در ارتباط با فرآیند غربال کردن (Screening Process6) که توسط این نوع دیواره های آتش مورد استفاده قرار می گرفت در سال 1988 منتشر شد .در سال 1989 آزمایشگاه شرکت AT&T برای اولین بار نسل دوم دیواره‌های آتش که در آینده "دیواره‌های آتش سطح مدار 7(Circuit level firewalls) "لقب گرفتند را بوجود آوردند. در همان سال آنها همچنین اولین مدل عملی 8(Working Model) از نسل سوم دیواره‌های آتش یعنی "دیواره‌های آتش لایه کاربرد 9(Application layer firewalls) "پیاده‌سازی کردند اما نه هیچ مقاله‌ای در این ارتباط منتشر شد و نه محصولی بر اساس این مدل به بازار عرضه گشت .در اواخر سال 1989 و اوایل دهه 90 تحقیقات مختلف و پراکنده ای در سطح کشور آمریکا بر روی نسل سوم دیواره های آتش انجام شد و بالاخره نتایج این تحقیقات به صورت جداگانه درسال های 1990 و 1991 توسط Gene Spafford از دانشگاه Bill Cheswick,Purdue از لابراتوری Bell شرکت AT&T و Marcus Ranum انتشار یافتند. در سال 1991 تحقیقات Marcus Ranum بیشترین توجه را به خودش معطوف کرد و باعث بوجود آمدن Bastion host10 هایی که سرویس proxy ۱۱را اجرا می کردند شد. نتایج این تحقیقات به سرعت در اولین محصول تجاری شکل عینی یافت و به کار گرفته شد. این محصول که SEAL نام داشت توسط شرکت DEC عرضه شد .در اواخر سال1991، Bill Cheswick و Steve Bellovin تحقیقاتی را در ارتباط با پالایش کردن بسته ها به صورت پویا (Dynamic12) شروع کردند و بر این اساس محصولی داخلی را در لابراتوار Bell پیاده‌سازی کردند که البته هرگز به بیرون عرضه نشد. در سال 1992، Bob Barden و Annette DeSchon در مؤسسه USC's Information Sience Institute تحقیقاتی را بر روی نسل چهارم دیواره‌های آتش تحت عنوان "دیواره‌های آتش پالایشگر بسته پویا (Dynamic packet filter firewalls13) "برای سیستمی با نام Visas به طور جداگانه

---

[4] دیواره های آتش پالایشگر بسته

[5] Internetworking Operation system- سیستم عامل کار بر روی شبکه

[6] غربال کردن

[7] دیوار های آتش سطح مدار

[8] مدل عملی

[9] دیواره آتش لایه کاربردی

[10] میزبان ها

[11] نام سرویسی رایج در امور اینترنت و شبکه

[12] پویا

[13] دیواره‌های آتش پالایشگر بسته پویا

شروع کردند و در نهایت نرم افزارChech Point ، اولین محصول تجاری بر پایه معماری نسل چهارم دیواره های آتش، در سال 1994 به بازار عرضه شد .در سال 1996، Scott Wiegelطرحی را برای نسل پنجم دیوارههای آتش با عنوان Kernel Proxyارایه داد. دیواره آتش Cisco Centri که درسال 1997 پیاده سازی شد اولین محصول تجاری بر اساس معماری این نسل بود .در سال های اخیر نیاز به سیستم های امنیتی که پرسرعت و در عین حال قابل گسترش(Extensible)، قابل نگهداری (Maintainable)و انعطاف پذیر (Flexible)باشند باعث شده است شرکت های فعال در زمینه امنیت در تکاپوی یافتن راه حلهایی مناسب و کاربردی برای پاسخگویی به این نیازها باشند .

مبانی طراحی فایروال:

از آنجایی که معماری شبکه به صورت لایه لایه است و اینترنت هم از مدل TCP/IP[14] حمایت می کند، ما بیشتر توضیحاتمان را روی این مدل می آوریم. در مدل TCP/IP برای انتقال یک واحد اطلاعات از لایه چهارم بر روی شبکه، باید تمام لایه ها را گذراند و هر لایه برای انجام وظیفه خود تعدادی فیلد مشخص به ابتدای بسته اطلاعاتی اضافه کرده و آن را تحویل لایه زیرین می دهد. قسمت اعظم کار یک دیوار آتش تحلیل فیلدهای اضافه شده در هر لایه وسرایند بسته می باشد. در بسته ای که وارد دیوار آتش می شود به تعداد لایه ها سرایند مختلف وجود خواهد داشت. معمولا سرایند لایه اول (لایه فیزیکی یا network interface[15] از شبکه اینترنت) اهمیت چندانی نخواهد داشت. چرا که محتوای این فیلدها فقط روی کانال فیزیکی از شبکه محلی معنا دارند و در گذر از هر شبکه یا مسیریاب این فیلدها عوض خواهد شد. بیشترین اهمیت در سرایندی است که در لایه های دوم سوم و چهارم شبکه به یک واحد از اطلاعات اضافه خواهد شد:در لایه شبکه دیوار آتش فیلدهای بسته IP[16] را پردازش و تحلیل می کند.در لایه انتقال دیوار آتش فیلدهای بسته های TCP[17] یا UDP[18] را پردازش و تحلیل می کند.در لایه کاربرد دیوار آتش فیلدهای سرایند و همچنین محتوای خود داده ها را بررسی می کند. (مثلا سرایند و محتوی یکه نامه الکترونیکی یا یک صفحه وب می تواند مورد بررسی قرار گیرد.با توجه به لایه لایه بودن معماری شبکه لاجرم دیوار آتش نیز باید لایه لایه طراحی شود. (البته توجه به این نکته مهم است که این به این معنا نیست که همه Firewall ها همه این لایه ها و قابلیت ها را دارند، بلکه بسته به کاربرد در بعضی انواع Firewall فقط برخی لایه های آن پیاده سازی می شوداگر یک بسته در یکی از لایه های دیوار آتش شرایط عبور را احراز نکند همان جا حذف شده و به لایه های بالاتر ارجاع نمی شود بلکه این امکان وجود دارد که آن بسته جهت پیگیری های امنیتی نظیر ثبت و ردگیری به سیستمی جانبی تحویل داده شود.

---

[14] مخفف کلمه Transmission Control Protocol/Internet Protocolبه معنی پروتکل کنترل انتقال / پروتکل اینترنت

[15] رابط شبکه

[16] نشانی پروتکل اینترنت- به انگلیسی (Internet Protocol Address)یا به اختصار نشانی آی‌پی (IP Address):نشانی عددی است که به هریک از دستگاه ها و رایانه‌های متصل به شبکه رایانه اختصاص داده می‌شوند.

[17] به معنی پروتکل کنترل انتقال

[18] قرارداد بسته دادهٔ کاربر یا پروتکل بسته دادهٔ کاربر –به انگلیسی UDP :یا (User Datagram Protocol)یکی از اجزاء اصلی مجموعه پروتکل اینترنت، مجموعه‌ای از پروتکل‌های شبکه که در اینترنت مورد استفاده قرار می‌گیرند، می‌باشد .

4-1)تعریف فایروال

فایروال یک برنامه و یا دستگاه سخت افزاری است که با تمرکز بر روی شبکه و اتصال اینترنت ، تسهیلات لازم در جهت عدم دستیابی کاربران غیرمجاز به شبکه و یا کامپیوتر شما را ارائه می نماید. فایروال ها این اطمینان را ایجاد می نمایند که صرفا" پورت های ضروری برای کاربران و یا سایر برنامه های موجود در خارج از شبکه در دسترس و قابل استفاده می باشد .به منظور افزایش ایمنی ، سایر پورت ها غیرفعال می گردد تا امکان سوء استفاده از آنان توسط مهاجمان وجود نداشته باشد . در برخی موارد و با توجه به نیاز یک برنامه می توان موقتا" تعدادی از پورت ها را فعال و پس از اتمام کار مجددا" آنان را غیرفعال نمود . بخاطر داشته باشید که به موازات افزایش تعداد پورت های فعال ، امنیت کاهش پیدا می نماید . فایروال های نرم افزاری ، برنامه هائی هستند که پس از اجراء ، تمامی ترافیک به درون کامپیوتر را کنترل می نمایند(برخی از فایروال ها علاوه بر کنترل ترافیک ورودی ، ترافیک خروجی را نیز کنترل می نمایند). تعداد زیادی از اینگونه فایروال ها، صرفا" نظاره گر ترافیک بین شبکه داخلی و اینترنت بوده و ترافیک بین کامپیوترهای موجود در یک شبکه داخلی را کنترل نمی نمایند.در اصطلاح کامپیوتری واژه فایروال به سیستمی اطلاق می‌شود که شبکه خصوصی یا کامپیوتر شخصی شما را در مقابل نفوذ مهاجمین ، دسترسی‌های غیرمجاز ، ترافیک‌های مخرب و حملات هکری خارج از سیستم شما محافظت می‌کند . فایروال‌ها می‌توانند ترافیک ورودی به شبکه را کنترل و مدیریت کرده و با توجه به قوانینی که در آن‌ها تعریف می‌شود به شخص یا کاربر خاصی اجازه ورود و دسترسی به یک سیستم خاص را بدهند.یک فایروال از شبکه شما در برابر ترافیک ناخواسته و همچنین نفوذ دیگران به کامپیوتر شما حفاظت می کند. توابع اولیه یک فایروال به این صورت هستند که اجازه می دهند ترافیک خوب عبور کند و ترافیک بد را مسدود می کنند! مهمترین قسمت یک فایروال ویژگی کنترل دستیابی آن است که بین ترافیک خوب و بد تمایز قائل می شود.فایروال نرم افزار یا سخت افزاری است که در قسمت دروازه (Gateway[19]) قرار گرفته و منابع درون شبکه را از دسترسی غیر مجاز خارجی محافظت می کند . یک فایروال یا دیواره آتش همیشه در قسمت junction point[20]شبکه یعنی قسمتی که شبکه داخلی به شبکه های دیگر متصل می شود یا با اینترنت ارتباط برقرار می کند قرار می گیرد که به آن Edge [21]شبکه نیز گفته می شود ، و از شبکه داخلی در برابر نفوذ مهاجمان و ابزارهای مخرب حفاظت می کند .

[19] دروازه

[20] نقطه اتصال

[21] لبه

1-5)مشخصه‌های مهم فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

1-5-1)توانایی ثبت و اخطار :

ثبت وقایع یکی از مشخصه‌های بسیار مهم یک فایروال به شمار می‌رود و به مدیران شبکه این امکان را می‌دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می‌تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می‌تواند به راحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

2-5-1) بازدید حجم بالایی از بسته‌های اطلاعات:

یکی از تستهای یک فایروال، توانایی آن در بازدید حجم بالایی از بسته‌های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می‌تواند کنترل کند برای شبکه‌های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود. عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیت‌ها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می‌شوند. عامل محدودکننده دیگر می‌تواند کارتهای واسطی باشد که بر روی فایروال نصب می‌شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL [22]و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

3-5-1)سادگی پیکربندی:

سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامن گیر شبکه‌ها می‌شود به پیکربندی غلط فایروال بر می‌گردد؛ لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می‌کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزرای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

[22] (Uniform Resource Locator یا یوآرال):شخص‌کننده موقعیت مکانی و نحوهٔ واکشی یک منبع در اینترنت یا شبکه‌هایی مشابه اینترنت است.

4-5-1) امنیت و افزونگی فایروال:

امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال، تامین کننده امنیت فایروال و شبکه است:

الف- **امنیت سیستم عامل فایروال** :

اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می‌کند، نقاط ضعف امنیتی سیستم عامل، می‌تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- **دسترسی امن به فایروال جهت مقاصد مدیریتی** :

یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می‌تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

6-1)**آنچه فایروال سیستم از آن محافظت می نماید**:

1-ورودبه سیستم از راه دور

2-درهای مخفی برنامه کاربردی

3-دزدیدن ارتباط

4-اشکالات سیستم عامل

5-ردسرویس

6-بمب های ایمیل

7-ویروس ها

8-هرزنامه

9-تغییر دادن مسیر بمب ها

10-مسیریابی مبدا

11-ماکروها

7-1)نتیجه گیری این فصل

فایروال ها ، یکی از عناصر اساسی در نظام مهندسی امنیت اطلاعات می باشند که استفاده از آنان به یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات و کامپیوتر تبدیل شده است . بسیاری از افرادی که جدیدا" قدم در عرصه گسترده امنیت اطلاعات می گذارند ، دارای نگرانی و یا سوالات مفهومی خاصی در ارتباط با فایروال ها و جایگاه استفاده از آنان در جهت ایمن سازی شبکه های کامپیوتری می باشنددر هر حال یک دیواره آتش قادر است در جهت بالا رفتن سطح امنیتی شبکه اقدامات مفیدی را انجام دهد

فصل دوم

2-1)مقدمه فصل دوم:

فایروالها به دودسته سیستمی وشبکه ای تقسیم می شوند فایروالهای سیستمی عبارتنداز:

سخت افزاری ونرم افزاری

براساس عملکرد به 5نوع تقسیم می شوند ازجمله :سطح مدار.پروکسی سرور nosstateful [۲۳]و stateful[۲۴] و ...

هرکدام ازاین فایروالها مشخصه وکارکرد مخصوصی دارند وباید باآگاهی ازنوع کارکرد آن وشرایط مدنظرخود فایروال موردنیاز راانتخاب کرد.

2-2)انواع دیواره‌های آتش از لحاظ عملکرد:

دیواره‌های آتش پالایشگر بسته

دیواره‌های آتش سطح مدار

دیواره‌های آتش لایهٔ کاربرد

دیواره‌های آتش پالایشگر بسته پویا

دیواره‌های آتش Kernel Proxy[25]

دیواره‌های آتش مخفی

دیواره‌های آتش توزیع شده

دیواره‌های آتش شخصی

دیواره‌های آتش با توسعه‌پذیری بالا

---

[23] غیر قابل حالت دهی

[24] حالتمند

[25] هسته ای

دیواره‌های آتش نرم‌افزاری

دیواره‌های آتش اختصاصی

دیواره‌های آتش شخصی

2-3)فایروالها را ازلحاظ عملکرد به 5 گروه تقسیم می کنند.

2-3-1) **فایروالهای سطح مدار (Circuit-Level)**: این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

2-3-2) **فایروالهای پروکسی سرور**:

فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتواندابن فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

2-3-3)**فیلترهای Nosstateful packet** :

این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی

عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

2-3-4) فیلترهای[26] Stateful Packet :

این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای TCP. بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP [۲۷]و HTTP [۲۸]را تشخیص دهند و لذا می توانندعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.همچنین فیلتر های هوشمند باعث می شود بسته هایی که با ظاهر مجاز می خواهند درون شبکه راه پیـدا کننـد را از بسته های واقعی تمیز داده شوند. بزرگترین مشکل این فیلتر ها غبله بر تاخیر پردازش و حجم حافظـه مـورد نیاز می باشد، ولی در مجموع قابلیت اعتماد بسیار بالاتری دارند و ضریب امنیت شبکه را افـزایش خواهنـد داد؛ و بطور کل یک دیواره آتش یا فیلتر هوشمند پیشینه ترافیک خروجی را برای چند ثانیه آخر به خـاطر مـی سـپارد و بر اساس آن تصمیم می گیرد که آیا ورود یک بسته مجاز است یا خیر.؟

2-3-5)دیواره‌های آتش شخصی

(که به آنها desktop firewalls نیز گفته می‌شود (نرم‌افزارهایی هستند که برای محافظت از یک کامپیوتر تنها که به اینترنت متصل است مورد استفاده قرار می‌گیرند. این کامپیوتر ممکن است به طور دایمی از طریق خطوط(Cable modem)[29] , (DSL[30])و یا موقت از طریق ارتباطات Dial-up[31] به اینترنت متصل باشد. در مقایسه با برنامه های ضد ویروس دیواره های آتش در زمینه و در سطحی پایین تر اجرا می شوند. دیواره های آتش

---

[26] بسته های حالت مند

[27] The File Transfer Protocol – قرارداد (پروتکلی) است که در شبکه‌های رایانه‌ای برای جابه‌جایی پرونده از مبدا به مقصد مورد استفاده قرار می‌گیرد.

[28] The Hypertext Transfer Protocol (**HTTP**) – اصطلاحا به پروتکلی گفته می شود که برای ایجاد ارتباط، دریافت، و ارسال داده ها بین سرویس دهنده و سرویس گیرنده استفاده می شود .

[29] مودم های کابلی

[30] Digital Subscriber Line –خط دیجیتال مشترک (دی.اس.ال) یا (DSL) از دسته فناوری‌هایی است که انتقال مخابراتی اطلاعات دیتا را به وسیله سیم‌های ارتباطی در یک شبکه تلفنی محلی فراهم می‌آورد

[31] روش اتصال به اینترنت

شخصی با چک کردن جامعیت فایل های سیستم، پالایش ترافیک ورودی و خروجی، اخطار به کاربر در ارتباط با حملات در حال شکل‌گیری و .... سعی می‌کنند کامپیوتر مرتبط با اینترنت را مورد محافظت قرار دهند. در آیندهٔ نزدیک امن‌سازی سیستم‌ها با دیواره‌های آتش شخصی به یکی از استانداردهای کامپیوترهای خانگی تبدیل خواهد شد .دیواره‌های آتش شخصی مانند دیواره‌های آتش توزیع شده کار می‌کنند به جز چند مورد. در واقع قابلیت‌های دیواره‌های آتش توزیع شده بیشتر از دیواره‌های آتش شخصی است. دیواره‌های آتش شخصی برای محافظت از یک کامپیوتر تنها که به اینترنت متصل است استفاده می‌شود در حالی که دیواره‌های آتش توزیع شده برای محافظت از کامپیوترهای موجود در یک شبکهٔ بزرگ سازمانی طراحی شده‌اند.یک شرکت یا سازمان می تواند با خرید یک distributed firewall solution[29]، کارمندان دور، شبکه‌های محلی سازمان و شبکه‌های گسترده‌اش را مورد محافظت قرار دهد. مدیریت مرکزی، قابلیت, وارد شدن در یک نقطهٔ مرکزی و ریزسازی کنترل دسترسی (Access Control Granularity)ویژگی‌هایی هستند که در دیواره‌های آتش شخصی وجود ندارند. می‌توان گفت دیواره‌های آتش شخصی مستقل و مجزا هستند در حالی که دیواره‌های آتش توزیع شده با یک نقطهٔ مرکزی در ارتباطند و در صحبت با او قادرند اطلاعات سیاست‌های امنیتی را دریافت و اطلاعات ثبت شده و جمع‌آوری شده را ارسال کنند (به این علت به دیواره های آتش توزیع شده Firewall agent نیز گفته می شود).

2-4)انواع فایروالها:

سه نوع عمده فایروال وجود دارد که ما آنها را مورد بررسی قرار میدهیم:

1-4-2)مسیر کاربردی:

اولین فایروال ، مسیر کاربردی هستند که بعنوان پراکسی مسیری شناخته می شوند.آنها از باستین هاستهایی ساخته شده اند که برای عمل کردن به صورت پراکسی سرور یک نرم افزار خاص را اجرا می کند. این نرم افزار در لایه کاربردی دوست قدیمی ما مدل مرجع ISO/OSI [30]اجرا می شود. کلاینتهای پشت سر فایروال بایستی proxitized (به این معنا که بایستی دانست که چگونه از پراکسی استفاده کرد و آنها را پیکربندی نمود)شوند تا از خدمات اینترنتی استفاده کرد.معمولاً اینها دارای ویژگی امنیتی هستند ، زیرا آنها به همه اجازه عبور بدون اشکال را نمی دهند و نیاز به برنامه هایی دارند که برای عبور از ترافیک نوشته و اجرا شدند. آنها عموماً کندترین هستند زیرا برای داشتن یک درخواست سرویس نیاز به اجرای پروسه های زیادی دارند.

---

[29] دیواره های آتش توزیع شده

[30] OSIاز کلمات Open Systems Interconnect اقتباس و یک مدل مرجع در رابطه با نحوه ارسال پیام بین دو نقطه در یک شبکه مخابراتی و یا کامپیوتری است .

2-4-2)فیلتر کردن بسته

فیلتر کردن بسته تکنیکی است که بواسطه آن روتورها دارای ACL [31]های (لیستهای کنترل دسترسی) فعال می شوند. به طور پیش فرض ،یک روتور تمامی ترافیک به سمت خود را عبور می دهد و همه نوع کار را بدون هیچ محدودیتی انجام می دهد .استفاده از ACLها روشی برای اعمال سیاست امنیتی شما با توجه به نوع دسترسی که می خواهید جهان خارج به شبکه داخلی شما داشته باشد و غیره ، می باشد.استفاده از فیلتر کردن بسته بجای مدخل کاربردی دارای هزینه اضافی است زیرا ویژگی کنترل دسترسی در لایه پایینتر ISO/OSI اجرا می شود. (عموماً لایه انتقال یا لایه session[32]). با توجه به سربار کمتر و این واقعیت که فیلترینگ بوسیله روتورهایی انجام میشوند که به صورت کامپیوترهای خاص برای اجرای موارد مرتبط با شبکه بندی ،بهینه شده اند ،یک مسیر فیلترینگ بسته اغلب بسیار سریعتر از لایه کاربردی آن است.با توجه به آنکه ما بر روی یک لایه پایین ترکار میکنیم ،پشتیبانی از کاربردهای جدید یا به صورت خودکار انجام می شود یا یک موضوع ساده است که در آن بسته های خاص از مسیر عبور میکنند.در این روش مشکلاتی وجود دارد،بنابراین بخاطر بسپارید که TCP/IP به صورت مطلق است یعنی اینکه هیچ تعهدی برای آدرسهایی که ادعا می کنند به آن مرتبط هستند وجود ندارد.بنابراین ،به منظور محلی کردن ترافیک ما از لایه های فیلترهای بسته استفاده می کنیم. ما نمی توانیم تمام مسیرهای منتهی به هاست واقعی را داشته باشیم اما از طریق دو لایه از فیلترهای بسته می توانیم بین بسته ایی که از اینترنت می آید با بسته ایی که از شبکه داخلی ما می آید ،تفاوت قائل شد.ما می توانیم مشخص کنیم که بسته از کدام شبکه می آید اما نمی توانیم مشخصات بیشتری در مورد آن داشته باشیم.

2-4-3)سیستمهای ترکیبی (Hybrid systems):

در یک تلاش برای هماهنگ کردن مسیرهای لایه کاربردی با انعطاف پذیری و سرعت فیلترینگ بسته ، برخی از فروشندگان سیستمهایی را ایجاد کردند که از هر دو اصل استفاده می کنند.در چنین سیستمهایی ،اتصالات جدید باید در لایه کاربردی تایید وبه تصویب برسند. زمانی که این اتفاق افتاد ،بقیه اتصال به لایه session فرستاده می شود، که در آن برای فیلترهای بسته اتصال را کنترل می کنند تا مطمئن شوند که تنها بسته هایی که بخشی از یک محاوره در حال پیشرفت (که همچنین مجاز و مورد تایید هستند) عبور میکنند.سایر احتمالات شامل استفاده از هر دو پراکسی فیلترینگ بسته و لایه کاربردی است. مزیتهای این حالت شامل ،ارائه معیاری برای محافظت از ماشینهای شما در مقابل خدماتی که به اینترنت ارائه میکند (همانند یک سرور عمومی وب) و همچنین ارائه امنیت یک مسیر لایه کاربردی به شبکه داخلی است.

---

[31] Access control list - لیستهای کنترل دسترسی

[32] لایه نشست

بعلاوه ،با استفاده از این مدل ، یک مهاجم که قصد بدست آوردن خدمات روی شبکه داخلی را دارد ،از طریق روتور دسترسی ، هاست بوستین و روتور مسدود کننده با شکست مواجه می شود.

2-5)حال به سراغ انواع تکنولوژی **در فایروال** می رویم.این تکنولوژی ها به 4 دسته تقسیم می شوند:

Packet Filtering Firewall(1-5-2

این نوع فایروالها یکی از ساده ترین و معمولی ترین انواع فایروالها است که در سال 1985 عرضه شد . درواقع عنوان packet filtering بیان کننده همه چیز در رابطه با این دسته از فایرواهاست.داده های خام به عنوان frameیا packet وارد شبکه می شوند.در این مدل ،بسته ها براساس پروتکل،پورت یا آدرس مبدا و مقصد از کارت شبکه عبور می کنند یا در آن block می شوند.به عبارتی در این مدل،فایروال آدرس مبدا و مقصد هر بسته را چک میکند،در صورتی که آن آدرس با پروتکل،پورت و آدرس هایی که برایش غیر مجاز تعریف شده است منافاتی نداشته باشد بسته اجازه خروج یا ورود را دارد،اما اگر منافات داشت یا آنها را بی سروصدا دور می اندازد و یا به مبدایی که از آنجا می آیند پیغام خطایی جهت عدم ارسال بسته میفرستد.همانطور که پیداست این نسل از فایروالها تنها با لایه های اول OSI ،برای به دست آوردن IP ها سروکار دارند .

Stateful Packet Inspection(2-5-2

تکامل یافته ی packet filteringاست که در سال 1993 ارائه شد SPI.عملکردی مشابه با packet filtering دارد با این تفاوت که دارای حافظه ای است که کلیه ی ارتباطات داخلی و خارجی را ذخیره و نگهداری میکند .

Circuit Level Gateway(3-5-2

این دسته از فایروالها از دسته ی قبلی حرفه ای تر هستند.این نسل از فایروالها در سال 1989-1990 به میان آمدند.این دسته در لایه ی sessionمدل OSI کار می کنند و به عنوان واسط بین لایه کاربردی و لایه ی انتقال TCP/IPعمل می کنند و ترافیک شبکه را براساس آدرس و پورتها در لایه ی session فیلتر میکنند.زمانی که یک کامپیوتر تصمیم به برقراری ارتباط ایجاد session با کامپیوتری دیگر در خارج از شبکه میگیرد، gateway اطلاعات مربوط به این ارتباط را بررسی و چک میکند که این ارتباط بر اساس آدرس و شماره پورتش در شبکه مجاز است یا نه،سپس آن را به کامپیوتر مقصد میفرستد.تازمانی که gatewayارتباط را مجاز نشمارد،هیچ گونه دیتایی منتقل نمی شود.زمانی که دیتایی از gateway عبور میکند،کامپیوتر مقصد آدرس gateway را می بیند نه کامپیوتری که از آن دیتا ارسال شده است.این دسته از فایروالها از دسته ی قبلی دارای امنیت بیشتری هستند .

(3-5-2 **Aplication Level Gateway**:

دودسته ی قبلی فایروالها تنها هدرهای لایه های network و session را مورد بررسی قرار می دادند.در آنها امکان دیدن payload بسته ها وجود نداشت. هیچ کدام از فایروالها آنقدر قدرتمند نبودند که بتوانند محتویات بسته ها را مشاهده کنند.تا قبل ازاین نسل از فایروالها،ارتباطی مجاز بود که IP و پورت مجازی داشته باشد و sessionمجازی را نیز تشکیل دهد که این می توانست موجب بروز حملاتی به داخل شبکه شود.مثلا اگر در شبکه ای استفاده از telnet مجاز نبوده اما استفاده از HTTP مجاز بوده باشد،از نظر این فایروال ارتباط مجاز است اگر از پورت 80 استفاده شده باشد و غیرمجاز است اگر از پورت 23 استفاده شود.خوب اگراز telnet پورت 80 استفاده کنیم فایروال متوجه نخواهد شد چون محتویات داخل بسته ها را چک نمیکند و فقط شماره پورت ها رو بررسی می کند application level gateway[34].یا فایروالهای proxy،نرم افزارهای کاربردی هستند که دو حالت دارند proxy server و proxy client زمانی که یک کاربر در یک شبکه مطمئن می خواهد با یک کاربر دیگر در یک شیکه غیرمطمئن مانند اینترنت متصل شود،درخواست به صورت مستقیم به proxy serverارسال می شود.

[33] شبکه راه دور

[34] لایه کاربردی

[35] پراکسی سرویس دهنده

[36] پراکسی سرویس گیرنده

(Staeful Multi Level Inspection) SMLI

فایروالهای SMLIنسل چهارم از فایروالها هستند که در سال 1994 ارائه شدند.در این فایروالها از تکنولوژی بکار برده شده در سه نسل قبلی استفاده شده است.درواقع SMLI ها می توانند عمل filter packet یا فیلترکردن بسته ها را در لایه شبکه ، sessionو همچنین لایه کاربردی نیز انجام دهند.درواقع این فایروال با مانیتورینگ داده هایی که در حال رد و بدل در لایه کاربردی و یا پورتها هستندسطح امنیتی بالایی را برقرار می کند. ارتباطاتی که از طریق SMLIانجام می شود برای طرفین کاملا مشخص و شفاف بوده و جهت سازگاری به هیچ عنوان مشکل ساز نمی باشد.به جای استفاده از application level filtering یا نسل سوم تکنولوژی فایروالها، در فایروالهای دیگر، SMLI deviceاز الگوریتم هایی استفاده میکنند که منابع کمتری را برای بررسی بسته ها در لایه کاربردی لازم داشته باشند (استفاده از منابع زیاد در نسل سوم از فایروالها از معایب آن دسته بود).این دسته از فایروالها سطح بالایی از امنیت را برقرار میکنند و دارایی کارایی خوبی نیز هستند اما قیمت آنها نیز بالاست .تنظیم قوانین در این فایروالها کمی پیچیده است و اگر اینکار خوب صورت نپذیرد،فایروال قادر به برقراری امنیت نخواهد بود. یکی از مزایای آنها این است که زمانی که یک session کامل شد،هر پورتی که در آن sessionاستفاده می شده است ،بسته می شود SMLI.ها می توانند به صورت داینامیکی پورتها را برای هر sessionبسته یا باز کنند،که در نسل اول یا packet filtering بعد از هر session آن پورت درهمان وضعیت قبلی باقی می ماند . آخرین ورژن Checkpoint Firewall[37]-1 نمونه ای ازتکنولوژی SMLI فایروالهاست.

2-6)چه نوع فایروال هایی وجود دارد ؟

به طور کلی فایروال ها به دوصورت فایروال شبکه ای (Network firewall) وفایروال سیستمی (Host[38]) تقسیم می شوند که فایروال سیستمی می توان به فایروال خود ویندوز ویا فایروال هایی مانند , Comodo MCafee را نام برد .و اما فایروال های شبکه ای نیز دارای تقسیم بندی دیگری هستند که بیشتر با این نوع تقسیم بندی آشنا هستیم :فایروال ها به دو شکل سخت افزاری (خارجی) و نرم افزاری (داخلی) ارائه میشوند. با اینکه هر یک از مدل های فوق دارای مزایا و معایب خاص خود می باشند ، تصمیم در خصوص استفاده از یک فایروال به مراتب مهمتر از تصمیم در خصوص نوع فایروال است.

2-6-1)فایروال ها سخت افزاری :

این نوع از فایروال ها که به آنان فایروال های شبکه نیز گفته میشود، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط DSL قرار خواهند گرفت. تعداد زیادی از تولید کنندگان و برخی از مراکز ISP دستگاههایی با نام روتر را ارائه میدهند که دارای یک فایروال نیز میباشد. فایروال های سخت افزاری در مواردی نظیر حفاظت چندین

[37] بازسازی فایروال

[38] میزبان

کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می نمایند(امکان استفاده از آنان به منظور حفاظت یک دستگاه کامپیوتر نیز وجود خواهد داشت).در صورتی که شما صرفا دارای یک کامپیوتر پشت فایروال می باشید و یا این اطمینان را دارید که سایر کامپیوترهای موجود بر روی شبکه نسبت به نصب تمامی PATCHها [۳۹]، بهنگام بوده و عاری از ویروس ها و یا کرم های می باشد، ضرورتی به استفاده از یک سطح اضافه حفاظتی (یک نرم افزار فایروال) نخواهید داشت.فایروال های سخت افزاری، دستگاه های سخت افزاری مجزائی می باشند که دارای سیستم عامل اختصاصی خود می باشند.بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می گردد.

2-6-2)فایروال های نرم افزاری :

برخی از سیستم های عامل دارای یک فایروال تعبیه شده درون خود می باشند.در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می باشد، پیشنهاد می گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن سازی کامپیوتر و اطلاعات، ایجاد گردد

3-6-2)فایروال **NAT** [۴۰]ساده

فایروالهایی که برای broadband router [۴۱]ها ساخته شده اند و نرم افزارهایی مانند Microsoft ICS[42] فایروالهای بسیار ساده ای هستند. و این فایروالها شبکه را با جلوگیری از ارتباط مستقیم هر کامپیوتر با کامپیوترهای دیگر شبکه محافظت می کنند. این نوع فایروالها تقریباً هر نوع هکری را متوقف می کنند .هکرهای حرفه ای ممکن است بتوانند از این فایروالها عبور کنندااما تعداد چنین اشخاصی کم و احتمال آن ضعیف است

[39] افزونه یا وصله هایی برای تکامل

[40] Network Address Translation

[41] مسیر یاب پهن باند

[42] Internet Connection Sharing – ارتباط اشتراکی اینترنت

تفاوت فایروال سخت افزاری ونرم افزاری

فایروال های سخت افزاری معمولا بصورت زیر ساخت هایی هستند که توسط شرکت های تولید کننده بر روی بوردهای سخت افزاری نصب و راه اندازی شده اند و معمولا در قالب یک روتر در شبکه فعالیت می کنند، یک روتر نیز می تواند در یک شبکه به عنوان یک فایروال سخت افزاری فعالیت کند. یک فایروال سخت افزاری می تواند بصورت پیش فرض و بدون انجام هرگونه تنظیمات اولیه در حد مطلوبی از ورود داده ها و ترافیک ناخواسته به شبکه محافظت کرده و اطلاعات را ایمن نگه دارد. اینگونه فایروال ها معمولا در قالب فیلترینگ بسته یا Packet Filtering فعالیت می کنند و Header های مربوط به مبدا و مقصد (Source & Destination) بسته ها را به دقت بررسی کرده و در صورتیکه که محتویات بسته با قوانینی که در فایروال انجام شده است مغایرت داشته باشد بلافاصله از ورود آن به شبکه جلوگیری کرده و آنرا بلاک می کند. بسته اطلاعاتی در صورتیکه مغایرتی با قوانین موجود در فایروال نداشته باشد به مقصد مورد نظر هدایت خواهد شد. راحتی کار با فایروال های سخت افزاری این است که هر کاربر ساده ای ممکن است براحتی بتواند آنرا در شبکه قرار داده و از تنظیمات پیش فرض انجام شده در آن استفاده کند، تنها بعضی از تنظیمات پیشرفته امنیتی در اینگونه فایروال ها هستند که نیاز به داشتن دانش تخصصی فراوان برای انجام دادنشان دارند. اما این را در نظر داشته باشید که فایروال های سخت افزاری می بایست توسط یک کارشنان متخصص امنیت آزمایش شود تا از کارکرد آنها اطمینان حاصل گردد. فایروال های سخت افزاری بار ترافیکی و لود کاری کمتری برای شبکه ایجاد می کنند و طبیعتا سرعت و کارایی بهتری در شبکه دارند اما از نظر هزینه بیشتر از فایروال های نرم افزاری هزینه دارند .

7-2) مسیریابهای بی‌سیم :

اگر شما قصد دارید که یک شبکه بی‌سیم راه اندازی نمایید، به یک مسیریاب بی‌سیم نیاز خواهید داشت. این نوع مسیریاب نیز در بسیاری از مواقع دارای یک فایروال درونی است و علاوه بر ایجاد ارتباط بین کامپیوترهای شبکه شما، محافظت از آنها را نیز بر عهده می‌گیرد. مزایا و معایب این نوع فایروال به این شرح است:

1-7-2)مزایا:مسیریابهای بی‌سیم به شما اجازه می‌دهند که کامپیوترها، کامپیوترهای قابل حمل، PDA[43]ها، و پرینترها را بدون نیاز به کابل کشی به هم متصل کنید. مسیریابهای بی‌سیم برای متصل کردن کامپیوترهای نوت بوک به شبکه و به اینترنت بسیار مناسب هستند.

2-7-2)معایب

[43] personal digital assistant - دستیار دیجیتالی شخصی یا دستیار رقمی شخصی- یک دستگاه کوچک قابل حمل شخصی با سیستم‌عامل است. کاربرد اصلی این وسیله در موردی است که نیاز به مزایای رایانه عادی در محیط‌هایی است که به قابل حمل بودن آن نیاز می‌باشد.

ابزارهای بی‌سیم اطلاعات را با استفاده از سیگنالهای رادیویی منتشر می‌کنند که می‌توانند توسط فردی در خارج از شبکه شما خوانده شوند ممکن است نیاز به پرداخت هزینه اضافی برای برخی تجهیزات باشدتمامی مسیریابهای بی‌سیم مجهز به فایروال درونی نیستند.

8-2)ضرورت توجه به امکانات سایر فایروال های نرم افزاری

فایروال ویندوز ، امکانات حفاظتی لازم به منظور بلاک نمودن دستیابی غیرمجاز به سیستم شما را ارائه می نماید . در این رابطه دستیابی به سیستم از طریق کاربران و یا برنامه های موجود در خارج از شبکه محلی ، کنترل خواهد شد . برخی از فایروال های نرم افزاری یک لایه حفاظتی اضافه را نیز ارائه داده و امکان ارسال اطلاعات و یا داده توسط کامپیوتر شما به سایر کامپیوترهای موجود در شبکه توسط برنامه های غیر مجاز را نیز بلاک می نمایند (سازماندهی و مدیریت یک فایروال دوطرفه) . با استفاده از این نوع فایروال ها ، برنامه ها قادر به ارسال داده از کامپیوتر شما برای سایر کامپیوترها بدون اخذ مجوز نخواهند بود . در صورت نصب یک برنامه مخرب بر روی کامپیوتر شما) سهوا" و یا تعمدا") برنامه فوق می تواند در ادامه اطلاعات شخصی شما را برای سایر کامپیوترها ارسال و یا آنان را سرقت نماید . پس از نصب فایروال های دوطرفه ، علاوه بر تمرکز بر روی پورت های ورودی (Incoming)، پورت های خروجی (Outgoing) نیز کنترل خواهند شد .

انواع و اقسام فایروال وجود دارد که در طبقه بندی های مختلفی می توان آنها را قرار داد . اما بهترین طبقه بندی فایروال ها بر اساس لایه های OSI است که یک طبقه بندی هفت لایه دارد که در هر لایه شما می توانید یک نوع فایروال داشته باشید Packet Filter Firewall .ها یا فایروال های فیلترینگ بسته های اطلاعاتی همانطور که از نامش هم پیداست در لایه سوم از مدل OSI کار می کنند ، این نوع از فایروال ها بسته های اطلاعاتی ورودی و خروجی به شبکه را بر اساس قوانینی که برایشان تعریف شده است بررسی می کنند و در صورت نیاز اجازه عبور به بسته اطلاعاتی مربوطه را می دهند و یا اینکه آن را مسدود می کنند. فایروال ها را می توانید شما در لایه هفتم از مدل OSI نیز داشته باشید که در انجا به این نوع از فایروال ها Web Application Firewall[44] گفته می شود یعنی فایروالی که می تواند ترافیک های ورودی و خروجی به نرم افزارهای کاربردی تحت وب لایه هفتم را بررسی کند ، این نوع فایروال ها در مفهوم کلی در واقع حملاتی که بر روی نرم افزارهای تحت وب انجام می شود را بر اساس قوانینی که از قبل بر روی آنها تعریف شده است شناسایی و مسدود می کنند. توجه کنید که در شبکه های کامپیوتری سرویس هایی مثل NAT و _Proxyنیز می توانند به عنوان یک فایروال در مدار عمل کنند

[44] Web Application Firewall

9-2) نتیجه این فصل:

فایروالهادونوع سیستمی وشبکه ای هستند وبه لحاظ عملکرد به 5دسته تقسیم می شوند.وبراساس نوع وبسته به عملکردشان ونیاز هرشخص مورد استفاده قرارمی گیرند.

فصل سوم

3-1)**مقدمه فصل سوم** :

دراین فصل به طور کامل به تشریح عملکرد فایروال می پردازیم.

بعد از آشنایی با مفهوم فایروال و وظایف آن نوبت به آن می رسد که توپولوژی فایروال ها.انواع پیکربندی.چگونگی عملکرد.متناسب ساختن نحوه انتخاب .پروتکل ها نواحی خطر ابزارهای لازم برای تست نفوذوارزیابی سرورهایDMZ [45]و... .می پردازیم.

[45] demilitarized zone

3-2) توپولوژی فایروال

بعد از آشنایی با مفهوم فایروال و وظایف آن نوبت به آن می رسد که توپولوژی فایروال ها را بررسی کنیم. موقعیت یابی برای فایروال و تعیین محل برای آن ، از درجه اهمیت بسیار بالایی برخوردار می باشد. برای درک بیشتر اهمیت موضوع ، مثال هایی را بیان خواهیم کرد. قبل از هر چیز به نکات مهمی که در هنگام تعیین محل و موقعیت فایروال باید بدان توجه شود دقت نمایید:

3-2-1)موقعیت قرار گیری فایروال از لحاظ فیزیکی :

معمولا ، فایروال ها را در مرزهای ورودی و خروجی شبکه نصب می کنند تا فایروال هم به عنوان پوشش امنیتی مناسب برای حفاظت از شبکه داخلی باشد و هم شبکه داخلی را از شبکه عمومی(اینترنت) جداسازی کند.

3-2-2)در نظر گرفتن نواحی امنیتی مختلف با قابلیت دسترسی های متفاوت :

مدیران و مهندسین شبکه برحسب نیاز ، شبکه را به نواحی امنیتی متفاوت تقسیم می کنند بطوریکه هر ناحیه سطوح دسترسی خاصی به افراد می دهد و برای هر کدام از این سطوح فایروال هایی با قوانین وساستگذاری های خاصی نصب و تعریف می کنند.

3-2-3)حفاظت لایه ای :

در شبکه های بزرگی که از درجه امنیت بالایی برخوردار باشند ، معمولا داده ها از چندین فایروال عبور می کنند. بدین ترتیب لایه های امنیتی متفاوتی در موقعیت های مختلف در شبکه نصب می کنند. این ویژگی باعث می شود که در صورتی که یکی از فایروال ها دچار مشکل شود ویا اینکه یک فایروال نتوانست جلوی حمله را بگیرد، بقیه فایروال ها راه نفوذ را ببندند.

3-4)چند نوع توپولوژی :

خارج از فایروال (بین اینترنت وفایروال) : در این شیوه ، سرور مستقیما و بدون حفاظ و لایه امنیتی در معرض دید عموم قرار می گیرد. و بعد از آن یک فایروال نصب می شود. ممکن است که این شیوه طراحی برای وب سرور شما خطرناک باشد ، اما چنانچه هکرها با سوء استفاده از ضعف طراحی وب مستر بتوانند وب سرور را در کرده و به بخواهند به داخل شبکه نفوذ کنند به یک فایروال سفت و سخت مواجه خواهند شد.

3-4-1)درون فایروال (بین فایروال و شبکه) :

در این طراحی ، وب سرور تحت حمایت کامل امنیتی فایروال قرار دارد. در این شیوه باید طراح وب و مدیر شبکه پورت های مورد نیاز و ضروری را باز بگذارد و سایر پورت ها را ببندد. در این صورت چنانچه هکری توانست از حفاظت وب نفوذ کند ، احتمال دارد که به راحتی به سایر پورت ها و منابع شبکه هم دسترسی پیدا کند.

3-4-2)میان دو فایروال :

اگر وب سرور دارای منابع حساس و مهمی باشد ، وب مستر و مدیر شبکه ضرورت پیدا می کند که از این شیوه امنیتی استفاده نماید. که در واقع ترکیبی از دو حالت فوق می باشد. در این شیوه طراحی ، وب سرور تحت حمایت و کنترل کامل دو فایروال می باشد و جلوی نفوذ هر فرد سودجویی گرفته می شود..

3-5) سیاست امنیتی یک شبکه مجموعه ای متناهی از قواعد امنیتی است که بنابر ماهیتشان در یکی از لایه های دیوار آتش تعریف میشوند :

1- قواعد تعیین بسته های ممنوع (بسته های سیاه) در اولین لایه از دیوار آتش

2- قواعد بستن برخی از پورتها متعلق به سرویسهایی مثل Telnet یا FTP در لایه دوم

3- قواعد تحلیل header متن یک نامه الکترونیکی یا صفحه وب در لایه سوم

3-5-1)لایه اول دیوار آتش:

لایه اول دیوار آتش بر اساس تحلیل بسته IP و فیلدهای header[46]این بسته کار میکند و در این بسته فیلدهای زیر قابل نظارت و بررسی هستند :

1-آدرس مبدا :

برخی از ماشینهای داخل و یا خارج شبکه با آدرس IP خاص حق ارسال بسته نداشته باشند و بسته هایآنها به محض ورود به دیوار آتش حذف شود.

2- آدرس مقصد :

[46] یک فایل هدر یا سرایند (به انگلیسی: header) عموماً معرفی مستقیم کلاس‌ها، سابروتین‌ها، متغیرها و دیگر معین‌کننده‌ها را دربرمی گیرد.

برخی از ماشینهای داخل و یا خارج شبکه با آدرس IP خاص حق دریافت بسته نداشته باشند و بسته های آنها به محض ورود به دیوار آتش حذف شود. (آدرس های IP غیر مجاز توسط مسئول دیوار آتش تعریف میشود.)

شماره شناسایی یک دیتاگرام قطعه قطعه شده (Fragment Offset & Identifier) : بسته هایی که قطعه قطعه شده اند یا متعلق به یک دیتاگرام خاص هستند باید حذف شوند.

4- شماره پروتکل :

بسته هایی که متعلق به پروتکل خاصی در لایه بالاتر هستند میتوانند حذف شوند. یعنی بررسی اینکه بسته متعلق به چه پروتکلی است و آیا تحویل به آن پروتکل مجاز است یا خیر؟

5- زمان حیات بسته :

بسته هایی که بیش از تعداد مشخصی مسیریاب را طی کرده اند مشکوک هستند و باید حذف شوند.

6- بقیه فیلدها بنابر صلاحدید و قواعد امنیتی مسئول دیوار آتش قابل بررسی هستند.

مهمترین خصوصیت لایه اول از دیوار آتش آنست که در این لایه بسته ها بطور مجزا و مستقل از هم بررسی میشوند و هیچ نیازی به نگه داشتن بسته های قبلی یا بعدی یک بسته نیست. بهمین دلیل ساده ترین و سریع ترین تصمیم گیری در این لایه انجام میشود. امروزه برخی مسیریابها با امکان لایه اول دیوار آتش به بازار عرضه میشوند یعنی به غیر از مسیریابی وظیفه لایه اول یک دیوار آتش را هم انجام میدهند که به آنها مسیریابهای فیلترکننده بسته (Pocket Filtering Router) گفته میشود. بنابراین مسیریاب قبل از اقدام به مسیریابی بر اساس جدولی بسته های IP را غربال میکند و تنظیم این جدول بر اساس نظر مسئول شبکه و برخی قواعد امنیتی انجام میگیرد.

با توجه به سزیع بودن این لایه هرچه درصد قواعد امنیتی در این لایه دقیقتر و سخت گیرانه تر باشند حجم پردازش در لایه های بالاتر کمتر و در عین حال احتمال نفوذ پایین تر خواهد بود ولی در مجموع بخاطر تنوع میلیاردی آدرسهای IP نفوذ از این لایه با آدرسهای جعلی یا قرضی امکان پذیر خواهد بود و این ضعف در لایه های بالاتر باید جبران شود.

2-5-3)لایه دوم دیوار آتش:

در این لایه از فیلدهای header لایه انتقال برای تحلیل بسته استفاده میشود. عمومی ترین فیلدهای بسته های لایه انتقال جهت بازرسی در دیوار آتش عبارتند از :

شماره پورت پروسه مبدا و مقصد : با توجه به آنکه پورتهای استاندارد شناخته شده هستند ممکن است مسئول یک دیوار آتش بخواهد سرویس ftp فقط در محیط شبکه محلی امکان پذیر باشد و برای تمام ماشینهای خارجی این امکان وجود نداشته باشد. بنابراین دیوار آتش میتواند بسته های TCP با شماره پورت های 20 و 21 (مربوط به ftp) که قصد ورود و خروج از شبکه را دارند ، حذف کند. یکی دیگر از سرویسهای خطرناک که ممکن است مورد سو استفاده قرار گیرد Telnet است که میتوان به راحتی پورت 23 را مسدود کرد. یعنی بسته هایی که مقصدشان شماره پورت 23 است حذف شوند.

1- فیلد شماره ترتیب و فیلد Acknowledgment [47]: این دو فیلد نیز بنا بر قواعد تعریف شده توسط مسئول شبکه قابل استفاده هستند.

2- کدهای کنترلی (TCP code Bits) : دیوار آتش با بررسی این کدها ، به ماهیت آن بسته پی برده و سیاستهای لازم را بر روی آن اعمال میکند. بعنوان مثال یک دیوار آتش ممکن است بگونه ای تنظیم شود که تمام بسته هایی که از بیرون به شبکه وارد میشوند و دارای بیت SYN=1 هستند را حذف کند. بدین ترتیب هیچ ارتباط TCP از بیرون به درون شبکه برقرار نخواهد شد.

از مهمترین خصوصیات این لایه آنست که تمام تقاضا های برقراری ارتباط TCP بایستی از این لایه بگذرد و چون در ارتباط TCP ، تا مراحل " سه گانه اش" به اتمام نرسد انتقال داده امکان پذیر نیست لذا قبل از هر گونه مبادله داده دیوار آتش میتواند مانع برقراری هر ارتباط غیر مجاز شود. یعنی دیوار آتش میتواند تقاضاهای برقراری ارتباط TCP را قبل از ارائه به ماشین مقصد بررسی نموده و در صورت قابل اطمینان نبودن مانع از برقراری ارتباط گردد. دیوار آتش این لایه نیاز به جدولی از شماره پورتهای غیر مجاز دارد.

3-5-3)لایه سوم دیوار آتش:

در این لایه حفاظت بر اساس نوع سرویس و برنامه کاربردی انجام میشود. یعنی با در نظر گرفتن پروتکل در لایه چهارم به تحلیل داده ها میپردازد. تعداد header ها در این لایه بسته به نوع سرویس بسیار متنوع و فراوان است. بنابراین در لایه سوم دیوار آتش برای هر سرویس مجزا (مانند وب، پست الکترونیک و...) باید یک سلسله پردازش و قواعد امنیتی مجزا تعریف شود و به همین دلیل حجم و پیچیدگی پردازش ها در لایه سوم

[47] تصدیق

زیاد است. توصیه موکد آنست که تمام سرویسهای غیر ضروری و شماره پورتهایی که مورد استفاده نیستند در لایه دوم مسدود شوند تا کار در لایه سوم کمتر باشد.

فیلترهای Stateful و هوشمند:

دقت کنید که فیلترهای معمولی کارایی لازم را برای مقابله با حملات ندارند زیرا آنها بر اساس یک سری قواعد ساده بخشی از ترافیک بسته های ورودی به شبکه را حذف میکنند. امروزه بر علیه شبکه ها حملاتی بسیار تکنیکی و هوشمند طرح ریزی میشود بگونه ای که یک فیلتر ساده قابل اعتماد و موثر نخواهد بود. بدیهی است که یک فیلتر یا دیوار آتش قطعا بخشی از ترافیک بسته ها را به درون شبکه هدایت خواهد کرد . (زیرا در غیر اینصورت شبکه داخلی هیچ ارتباطی با دنیای خارج نخواهد داشت.) نفوذگر برای آنکه ترافیک داده های مخرب او حذف نشود تلاش میکند با تنظیم مقادیر خاص در فیلدهای بسته های TCP و IP آنها را با ظاهری کاملا مجاز از میان دیوار آتش یا فیلتر به درون شبکه بفرستد. به عنوان مثال فرض کنید فیلتری تمام بسته ها به غیر از شماره پورت 80 (وب) را حذف میکند. حال یک نفوذگر در فاصله هزاران کیلومتری میخواهد فعال بودن یک ماشین را از شبکه بیازماید. بدلیل وجود فیلتر او قادر نیست با ابزارهایی مانند Ping[۴۸]، Nmap[۴۹] و Cheops[۵۰] و ... از ماشینهای درون شبکه اطلاعاتی کسب کند. بنابراین برای غلبه بر این محدودیت یک بسته SYN-ACK (با شماره پورت 80) به سمت هدف میفرستد. یک دیوار آتش معمولی با بررسی Source Port[۵۱] به این بسته اجازه ورود به شبکه را میدهد زیرا ظاهر آن نشان میدهد که توسط یک سرویس دهنده وب تولید گشته است و حامل داده های وب میباشد.

بسته به درون شبکه داخلی راه یافته و و چون ماشین داخلی انتظار دریافت آنرا نداشته پس از دریافت یکی از پاسخ های RESET یا ICMP Port Unreliable[۵۲] را برمیگرداند. هدف نفوذگر بررسی فعال بودن چنین ماشینی بوده است و بدین ترتیب به هدف خود میرسد. فیلتر بسته (یا دیوار آتش) نتوانسته از این موضوع باخبر شود!

---

[48] ping یک ابزار شبکه‌ای است که برای آزمایش میزان دسترسی‌پذیری یک میزبان در شبکهٔ پروتکل اینترنت به کار می‌رود و می‌تواند زمان رفت و برگشت برای بسته‌های فرستاده‌شده از میزبان عامل تا یک رایانهٔ مقصد را محاسبه کند.

[49] انمپ (به انگلیسی: Nmap) (برگرفته از حروف اول Network Mapper) یک پویشگر امنیتی است که در ابتدا به دست گُردُن لیون (با اسم مستعار فیودور واسکوویچ) نوشته شده و برای کشف میزبان‌ها و خدمتگزاران در یک شبکه رایانه‌ای و در نتیجه ایجاد یک «نگاشت» از شبکه، استفاده می‌شود.

[50] Cheops یک ابزار برای نقشه برداری از شبکه می باشد که یک شبکه را آنالیز کرده و به صورت گرافیکی تمام کامپیوترها و روترها و ... را نشان می دهد.

[51] پورت منبع

[52] پروتکل کنترل پیام‌های اینترنتی (آی‌سی‌ام‌پی) یکی از پروتکل‌های اصلی بسته پروتکل‌های اینترنت می باشد. مورد اصلی استفاده از آن در سیستم عاملهای کامپیوترهای متصل به شبکه، برای ارسال پیام‌های خطا، برای مثال، سرویس مورد درخواست در دسترس نمی باشد و یا اینکه میزبان یا روتر غیرفعال، است.

برای مقابله با چنین عملیاتی دیوار آتش باید فقط به آن گروه از بسته های SYN-ACK اجازه ورود به شبکه را بدهد که در پاسخ به یک تقاضای SYN قبلی ارسال شده اند. همچنین باید بشرطی بسته های ICMP Echo Reply بدرون شبکه هدایت شود که حتما در پاسخ یک پیام ICMP Echo Request[53] باشد. یعنی دیوار آتش باید بتواند پیشینه (History) بسته های قبلی را حفظ کند تا در مواجهه با چنین بسته هایی درست تصمیم بگیرد. دیوار های آتشی که قادرند مشخصات ترافیک خروجی از شبکه را برای مدتی حفظ کنند و بر اساس پردازش آنها مجوز عبور صادر نمایند دیوار آتش هوشمند نامیده میشوند.

البته نگهداری مشخصات ترافیک خروجی شبکه (یا ورودی) در یک فیلتر Stateful همیشگی نیست بلکه فقط کافی است که ترافیک چند ثانیه آخر را به حافظه خود بسپارد! وجود فیلترهای Stateful باعث میشود بسته هایی که با ظاهر مجاز میخواهند درون شبکه راه پیدا کنند از بسته های واقعی تمیز داده شوند. بزرگترین مشکل این فیلتر ها غلبه بر تاخیر پردازش و حجم حافظه مورد نیاز میباشد.ولی در مجموع قابلیت اعتماد بسیار بالاتری دارند و ضریب امنیت شبکه را افزایش خواهند داد. اکثر فیلترهای مدرن از این تکنیک بهره گیری نموده اند. یک دیوار آتش یا فیلتر هوشمند و Stateful پیشینه ترافیک خروجی را برای چند ثانیه آخر به خاطر میسپارد و بر اساس آن تصمیم میگیرد که آیا ورود یک بسته مجاز است یا خیر.

دیوار آتش مبتنی بر پراکسی (Proxy Based Firewall):

فیلترها و دیوارهای آتش معمولی و Stateful فقط نقش ایست و بازرسی بسته ها را ایفا میکنند. هر گاه مجوز برقراری یک نشست صادر شد این نشست بین دو ماشین داخلی و خارجی بصورت مستقیم (انتها به انتها) برقرار خواهد شد . بدین معنا که بسته های ارسالی از طرفین پس از بررسی عینا تحویل آنها خواهد شد.

فیلترهای مبتنی بر پراکسی رفتاری کاملا نتفاوت دارند:وقتی ماشین مبدا تقاضای یک نشست (Session) مثل نشست FTP یا برقراری ارتباط TCP با سرویس دهنده وب را برای ماشین ارسال میکند فرایند زیر اتفاق میافتد:

پراکسی به نیابت از ماشین مبدا این نشست را برقرار میکند. یعنیطرف نشست دیوار آتش خواهد بود نه ماشین اصلی! سپس یک نشست مستقل بین دیوار آتش و ماشین مقصد برقرار میشود. پراکسی داده های مبدا را میگیرد ، سپس از طریق نشست دوم برای مقصد ارسال می نماید.

3-6)ضرورت استفاده از فایروال

[53] درخواست اکو

یک سیستم بدون وجود یک فایروال ، در مقابل مجموعه ای گسترده از برنامه های مخرب آسیپ پذیر است و در برخی موارد صرفا" پس از گذشت چندین دقیقه از اتصال به اینترنت ، آلوده خواهد شد . در صورتی که تدابیر و مراقبت لازم در خصوص حفاظت از سیستم انجام نگردد ، ممکن است کامپیوتر شما توسط برنامه هائی که به صورت تصادفی آدرس های اینترنت را پویش می نمایند ، شناسائی شده و با استفاده از پورت های فعال اقدام به تخریب و یا سوء استفاده از اطلاعات گردد .

3-7)عملکرد دیواره‌های آتش را می‌توان در سه جمله خلاصه کرد :

3-7-1) آنها افراد را موقع ورود در یک نقطه کاملاً کنترل شده محدود می‌سازد .

3-7-2)آنها از نزدیک شدن خرابکاران به منابع داخلی جلوگیری می‌کنند .

3-7-3) آنها افراد را موقع خروج در یک نقطه کاملاً کنترل شده محدود می‌سازند .

3-8)فایروال ها چگونه کار می کنند؟

با تنظیم هر کدام از موارد زیر به فایروال دیکته کنیدکه چطور عمل کند:

3-8-1)نشانی IP:

اگر هنگام اداره شبکه محلی خود متوجه شدید که رایانه ای از طریق اینترنت مرتبت به serverشبکه شما وصل میشود و بار ترافیکی زیادی ایجاد می کند،می توانید از فایروال خود بخواهید که به آن رایانه یا نشانی IP مشخص،اجازه ورودبه شبکه را ندهد.

3-8-2)نام حوزه (Domain name):

از آنجا که نشانی IPیک عدد 32بیتی و استفاده از آن راحت نیست،به همهserver ها در اینترنت علاوه بر نشانی IP یک نام حوزه اختصاص میدهند.شما می توانید فایروال را طوری تنظیم کنید که رایانه های شبکه محلی بتواند به سایت های خاصی (با نشانی حوزه خاص)دسترسی داشته باشند. یا اینکه به مشخص کردن نام حوزه در فایروالبه رایانه های شبکه تان اجازه بدهید که از آن سایت ها دیدن کنند.

3-8-3)پورت و پروتکل:فایروال می تواندا‌ز طریق شماره پورت های رایانه ها که برای ارتباط با یکدیگر به کار می برند،اطلاعاترد و بدل شده را کنترل کند،همچنین می توان کلمات واصطلاحات خاصی را در بانک اطلاعاتی فایروال مشخص کرد. در اینصورت هنگام وارد یا خارج شدن اطلاعات فایروال محتوای آنها را بررسی می کند و اگر با کلمات خاصی که برایش مشخص کرده ایم روبه رو شود،اجازه نمی دهد آن اطلاعات عبورکنند.

3-9)فایروال در برابر چه خطراتی از ما محافظت می کنند؟

3-9-1)ویروس ها

:از معمول ترین خطرات برای هر رایانه به حساب می آیند و معمولا برنامه های کوچکی هستند که خود را رویرایانه های دیگر کپی کرده و به این روش به سرعت در شبکه شما پخش می شوند.

3-9-2)اشکالات برنامه ها و سیستم عامل ها:

در بعضی برنامه ها امکان دسترسی به آن برنامه از راه دور(Backdoor) آن همبدون امنیت کافی فراهم شده است.به این ترتیب هکرها می توانند از آن استفاده کرده واز راه دور کنترل برنامه شمارا بدست بگیرند.

3-9-3)ماکرو ها

:اگر فایروال ورود وخروج اطلاعات را کنترل نکند.هکرها میتوانند با فرستادن قطعه برنامه ها(که ماکرو نام دارند)به رایانه ها،داده ها را پاک کنند یا تغییر دهند و کل شبکه را از کار بیندازند.

3-9-4)بمب های ایمیل:

در یک لحظه یک نامه صدها و هزاران بار برای یک سرویس دهنده نامه الکترونیکی فرستاده می شود وکاراو را مختل می کند تا جایی که این سیستم دیگر نمی تواند نامه ها را دریافت کند و از کار می افتد.

3-9-5)در بسیاری از مواردی که به سایت ها حمله می شود،هکرها برای وصل شدن بهserver ،سعی می کنند درخواست هایبی شماری برای سرور بفرستد به طوری که سرور نمی تواند سیستم درخواست دهنده را پیدا کند و گیج می شود،به این ترتیبوقتی تعداد این نوع در خواست ها زیاد باشد، serverکند میشود در نهایت از کار می افتد.هر فایروال با توجه به سطح امنیتیکه ایجاد می کند،می تواند در مقابل تعدادی از این خطرات از شبکه ما محافظت کند .

3-10)بررسی نحوه عملکرد فایروال Firewall یا دیواره آتش

بسته های TCP و IP قبل از ورود یا خروج به شبکه ابتدا وارد دیوار آتش میشوند و منتظر میمانند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند. پس از پردازش و تحلیل بسته سه حالت ممکن است اتفاق بیفتد:

1 – اجازه عبور بسته صادر میشود(Accept Mode)

2– بسته حذف میشود(Blocking Mode)

بسته حذف شده و پاسخ مناسب به مبدا آن بسته داده شود(Response Mode)

غیر از حذف بسته میتوان عملیاتی نظیر ثبت ، اخطار، ردگیری، جلوگیری از ادامه استفاده از شبکه و توبیخ هم در نظر گرفت.

به مجموعه قواعد دیوار آتش سیاستهای امنیتی نیز گفته میشود. همانطور که همه جا عملیات ایست و بازرسی وقتگیر و اعصاب خرد کن است دیوار آتش هم بعنوان یک گلوگاه میتواند منجر به بالا رفتن ترافیک ، تاخیر، ازدحام و نهایتا بن بست در شبکه شود. یعنی بسته ها آنقدر در پشت دیوار آتش معطل میمانند تا زمان طول عمرشان به اتمام رسیده و فرستنده مجبور میشود مجددا اقدام به ارسال آنها کند و این کار متناوبا تکرار میگردد .به همین دلیل دیوار آتش نیاز به طراحی صحیح و دقیق دارد تا کمترین تاخیر را در اطلاعات امن و صحیح ایجاد نماید. تاخیر در دیوار آتش اجتناب ناپذیر است و فقط باید به گونه ای باشد که بحران ایجاد نکند.از آنجایی که معماری شبکه به صورت لایه لایه است ، در مدل TCP/IP برای انتقال یک واحد اطلاعات از لایه چهارم بر روی شبکه باید تمام لایه ها را بگذراند، هر لایه برای انجام وظیفه خود تعدادی فیلد مشخص به ابتدای بسته اطلاعاتی اضافه کرده و آنرا تحویل لایه پایین تر میدهد. قسمت اعظم کار یک دیوار آتش تحلیل فیلدهای اضافه شده در هر لایه و header هر بسته میباشد.

11-3)فایروال سه عمل اصلی انجام می دهد:

۱- کنترل ترافیک

۲- تبدیل آدرس

۳- نقطه پایانی VPN

فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه اجازه عبور دارند .بعلاوه فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند .. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند.یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN عمل کند.این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.آنتی

ویروس شبکه – این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترها مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.

VPN(12-3

- یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند VPN .اساساً یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود.

3-12-1)مزایا

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند . بعضی از فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

3-12-2)معایب

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان IT تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

3-13)شیوه کاری یک فایروال به این صورت است:

کلیه ترافیکی که از ورودیهای خود که هر کدام به یک شبکه متصل هستند را دریافت کرده و آن را با معیارهای تعیین شده بر روی خود مقایسه می کند و بر اساس این معیارهای تصمیم گیری می کند.

فایروال بسته های را در بین شبکه ها رد و بدل و مسیریابی (route)می کند

می تواند هم ترافیک وردی (inbound) و هم ترافیک خروجی (outbound) را مدیریت و فیلتر کند .

این نرم افزار دسترسی عمومی از طریق شبکه های بیرونی را به منابع داخلی مانند اتوماسیون اداری یا مثل آنرا مدیریت می کند . تمامی درخواست های دسترسی به شبکه داخلی را log برداری کرده و در صورت مشاهده مورد مشکوک بصورت ارسال هشدار (alarm) مدیر سیستم را در جریان می گذارد.

3-14) *تعدادی* از واژه خاص مرتبط با فایروالها و شبکه بندی در این بخش مورد استفاده قرار می گیرند که آنها را معرفی می کنیم.

3-14-1)باستیون هاست (Bastion host):

یک کامپیوتر با هدف عمومی که برای کنترل دسترسی بین شبکه(خصوصی) داخلی (انترانت)و اینترنت (یا هر شبکه ناشناخته دیگر)مورد استفاده قرار می گیرد. عموماً اینها هاستهایی هستند که دارای سیستم عامل یونیکس بوده و برای کاهش عملیات آن به عملیاتی که فقط برای پشتیبانی از وظایف آن اصلاح شده است .بسیاری ار اهداف عمومی آن خاموش شده است و در بسیاری از موارد به طور کامل حذف شده اند تا امنیت ماشین ارتقا یابد.

3-14-2)روتور:

یک کامپیوتر با هدف خاص برای اتصال شبکه ها به یکدیگر. روتورها همچنین برخی عملیات خاص همانند مسیریابی،یا مدیریت ترافیک شبکه هایی که به آنها متصل هستند را به عهده دارند.

3-14-3)لیست کنترل دسترسی (ACL) :

بسیاری از روتورها در حال حاضر این توانایی را دارند به طور انتخابی برخی از وظایفشان را بر اساس اطلاعاتی در مورد اینکه یک بسته به کجا می رود ، انجام دهند.این اطلاعات شامل مواردی همانند : آدرس مبدا ، آدرس مقصد ، پورت سرویس مقصد ، و غیره است. این موارد می توانند به نوع خاصی از بسته ها که از یک شبکه خازج یا به آن وارد می شوند ، محدود گردد.

3-14-4)منطقه بیطرف (DMZ):

DMZ بخش مهمی از یک فایروال است: این منطقه شبکه ایی است که نه بخشی از شبکه مشترک شده می باشد و نه بخشی از شبکه مشترک نشده است. ولی شبکه ایی است که بخش مشترک نشده را به بخش مشترک شده ارتباط می دهد.اهمیت DMZ فوق العاده بزرگ است: هرکسی که از طریق اینترنت بخواهد به شبکه شما نفوذ کند ، بایستی برای موفقیت در این کار از چند لایه بگذرد.این لایه ها توسط DMZ و در بخشهای مختلف ایجاد شده اند.

3-14-5)پراکسی (Proxy):

پراکسی سرور برنامه واسطه‌ای بین کاربر داخلی شبکه و اینترنت است که قابلیت‌های فراوانی در راستای حفظ امنیت، نظارت مدیریتی، کنترل کاربران و سرویس‌های ذخیره‌سازی دارد. پراکسی سرور امکان ایجاد فیلترهایی خاص را برای امنیت بیشتر در شبکه فراهم می‌کند، قابلیت ذخیره‌سازی، سرعت دستیابی به اطلاعات را بالا می‌برد و با سیستم‌های تصدیق هویت و تغییر هویت، ضامن امنیت در شبکه داخلی سازمان است و نیز امکان ثبت گزارش کامل کارکردش را دارد. همچنین قابلیت مسدود کردن محتویات آسیب‌رسان و بررسی تبعیت از قوانین برقرار شده در شبکه را دارا می‌باشد. پراکسی سرور امکان استفاده از اکثر پروتکل‌های محلی را فراهم می‌آورد و امکان رمز کردن داده‌ها را نیز دارد .پراکسی‌ها انواع مختلفی دارند که هر یک کار خاصی را انجام می‌دهد، که از آن جمله می‌توان FTP ، HTTP، SMTPو DNS را نام برد .

در حقیقت پراکسی در خواست کلاینت(client) را به پراکسی سرور فرستاده، پراکسی سرور محتویات بسته را بررسی می‌کند و در صورت لزوم پردازش‌های مورد نظر را روی بسته دیتا انجام می‌دهد و بسته را می‌سنجد، در صورت عدم مغایرت با سیاست‌های امنیتی تنظیم شده برای شبکه به آن‌ها اجازه عبور از فایروال را می‌دهد و این درخواست روی شبکه ارسال می‌شود و جواب آن توسط پراکسی سرور از اینترنت دریافت و برای کلاینت ارسال می‌شود.

3-16)مزایای استفاده از پراکسی:

3-16-1)ذخیره‌سازی

با توجه به گران بودن هزینه استفاده از اینترنت (بسته به اندازه پهنای باند مصرفی) و محدودیت پهنای باند معمولاً اطلاعات مورد نظر در زمان کم و با سرعت مطلوب به دست نمی‌آید. برای کمک به رفع این مشکل، پراکسی سرور منابعی مانند فایل‌ها و صفحات وبی که مورد دسترسی قرار می‌گیرند در یک حافظهٔ جداگانه ذخیره می‌کند و تقاضای مجدد این منابع با محتویات کش پاسخ داده می‌شود، در نتیجه از یک سو زمان دستیابی کاهش می‌یابد و از سوی دیگر چون اطلاعات از اینترنت دریافت نمی‌شود باعث کاهش ترافیک شبکه می‌شود و پهنای باند محدود با اطلاعات تکراری اشغال نمی‌شود.

3-16-2)دیوار آتش (Firewall)

پراکسی سرور می‌تواند تقاضای کاربران را به فایروال بدهد که به انها اجازه ورود یا خروج به شبکه داخلی داده شود.

3-16-3)فیلتر کردن

پراکسی سرور می‌تواند تمام محتویات ترافیک وارد شونده یا خارج شونده از شبکه داخلی سازمان را باز بینی کند و طبق تنظیمات انجام شده هر چیزی که به معیارهای تعیین شده برای امنیت یا سیاست‌های آن سازمان، مغایرت دارد مسدود کند (مانند سیستم فیلترینگ مخابرات ایران)

3-16-4)تصدیق هویت

بیشتر منابع الکترونیکی سازمان‌ها برای حفظ امنیت محدود می‌شوند. این محدودیت می‌تواند با ایجاد کلمه رمز یا محدود کردن دامنه آی پی اعمال شود در اینصورت اگر کاربری از یک سرویس‌دهنده اینترنت دیگر، در جایی غیر از سازمان استفاده کند آی پی کامپیوتر کاربر غیر معتبر تشخیص داده می‌شود و نیز برای کاربرانی که در داخل سازمان باشند ولی به صورت فیزیکی به شبکه داخلی متصل نشده باشند پراکسی می‌تواند به کاربران دور اجازه عبور موقت دهد و یا به آنها به طور موقت یک آی پی سازمان تخصیص داده می‌شود (مانند استفاده از لپ تاپ شخصی در شبکه داخلی سازمانی مثل دانشگاه) تا بتوانند از منابع محدود شده استفاده کنند.

3-16-5)تغییرهویت

برای جلوگیری از برخی حمله‌های نفوذ گران و محافظت از شبکه داخلی سازمان سرور پراکسی قادر به تغییر هویت کلاینت‌های داخلی می‌باشد. بدین صورت که اگر منبع تقاضا شده در کش موجود نباشد، سرور پراکسی برای آن کاربر به عنوان کلاینت عمل می‌کند و از یکی از آدرس‌های آی پی خودش، برای ارسال تقاضا به سرور موجود در اینترنت استفاده می‌کند و سپس پاسخ به وسیله پراکسی سرور برای کاربر ارسال می‌شود. این پروسه تغییر آی پی باعث می‌شود تقاضا دهنده اولیه قابل ردیابی نباشد و معماری شبکه سازمان از دید بیرونی مخفی بماند.

3-16-6)ثبت کردن

پراکسی سرور امکان ثبت گزارش کامل کارکردش را دارد تا در هر زمان امکان پیگیری اعمال کاربران داخل سازمان را فراهم آورد. اینکه کلاینت در چه ساعت و و دقیقه‌ای چه درخواستی ارسال کرده و حجم اطلاعات مبادله شده، نوع اطلاعات و ... از این جمله‌اند.

3-17)مزایای پراکسی سرور

Application Getways که عموماً پراکسی نامیده می‌شود پیشرفته‌ترین روش استفاده شده برای کنترل ترافیک عبوری از فایروال‌ها هستند. مزیتهای فراوانی دارند که به تعدادی از آنها اشاره می‌کنیم:

پراکسی سرور علاوه بر هدرها محتویات داخل هر بسته را نیز کنترل می‌کند و هرچیزی که سیاست‌های امنیتی سازمان را نقض کند می‌تواند تغییر دهد یا دور بریزد.

کدهای آسیب‌رسان مثل فایل‌های اجرایی، اپلت‌های جاوا و اکتیوکس‌ها را مسدود می‌کند.

قابلیت ذخیره‌سازی توسط پراکسی سرور امکان استفادهٔ بهتر از پهنای باند و بالا بردن سرعت دریافت اطلاعات را می‌دهد.پراکسی همچنین امکان سنجیدن محتوای بسته برای بررسی مطابقت با استانداردهای پروتکل را داراست. به طور نمونه گاهی حملات نفوذ گران از طریق ارسال متاکارکترها برای فریب سیستم قربانی یا تحت تاثیر قرار دادن سیستم با دیتای بسیار زیاد است. پراکسی می‌تواند کاراکترهای غیرقانونی یا رشته‌های خیلی طولانی را مشخص و مسدود کند.با توجه به امکاناتی نظیر تصدیق و تغییر هویت و ... امنیت شبکه داخلی را تا حد زیادی تامین می‌کند.با ستفاده از پراکسی سرور می‌توان از اکثر پروتکل‌های موجود در شبکه‌های محلی در محدوده نرم‌افزارهای کاربردی در شبکه‌های LAN مرتبط با اینترنت استفاده کرد.این ویژگی به این معناست که هنگام پیاده‌سازی برنامه با یک سرویس یا پروتکل خاص محدودیتی نبوده و کدی در برنامه برای ایجاد هماهنگی نوشته نمی‌شود.با استفاده از پراکسی سرور همه کاربران شبکه نمی‌توانند از همه سایت‌ها استفاده کنند و چون مستقیماً به اینترنت وصل نیستند می‌توان طبق تنظیمات از ورود به برخی سایت‌ها و دامنه‌ها جلوگیری به عمل آورد.همچنین هر کسی از روی اینترنت نمی‌تواند به اطلاعات شبکه دسترسی داشته باشد.برای امنیت بیشتر نیز می‌توان با استفاده از SSL امکان رمز کردن داده‌ها را فراهم آورد .

3-18)برخی از انواع پراکسی

تا کنون به پراکسی بصورت یک کلاس عمومی تکنولوژی پرداختیم. در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد.

Proxy SMTP

HTTP Proxy

FTP Proxy

نواحی خطر

پیاده سازی یک فایروال بگونه ای که بتوان موازنه ای بین امنیّت و سرعت برقرار نمود، اساساً کار بسیار مشکلی است. یک فایروال همواره لازم است اجازهٔ کار با شبکهٔ داخلی و اینترنت را به شکل قابل قبول و کارآمد برقرار و در کنار آن امنیّت لازم برای این ارتباط را نیز فراهم نماید.

طرّاحان فایروال همیشه قسمتی از معماری سیستم خود را به ناحیهٔ خطر اختصاص می دهند.منظور از ناحیهٔ خطر جائیست که موازنهٔ میان سرعت و امنیّت در آنجا مورد توافق قرار گرفته و یک نفوذگر در صورت شناسائی چنین نقطه ای می تواند به راحتی به شبکه نفوذ نماید

موارد مهم و لازم برای نواحی خطر در هنگام پیاده سازی فایروال

عملکرد فایروال همیشه بر اساس موازنه ای بین امنیّت و سرعت دسترسی به اطّلاعات سنجیده می شود از این رو هر چه از سطح امنیّتی بالاتری در شبکه استفاده نماییم کاهش کارایی و عملکرد شبکه را فراهم نموده ایم.فیلترها می توانند در ارزیابی دسترسی به شبکه مناسب باشند ولی با طولانی کردن لیست فیلترینگ باعث می شویم زمان بیشتری برای ارزیابی بسته ها در فایروال صرف شود.سیستم هایی که برای سرویس های فیلترینگ استفاده می شوند لازم است بر اساس اینکه تا چه سطحی عمل فیلترینگ را بر روی بسته اجرا نمایند انتخاب شوند تا کارایی و سرعت شبکه در حدّ قابل قبول حفظ شود.رمزگذاری و رمزگشایی بسته ها تأخیری را به شبکه اعمال می نماید که می بایست در هنگام پیاده سازی فایروال در نظر گرفته شود.بلوکه نمودن تمام پورت های غیر ضروری متد مناسبی برای افزایش کارایی فایروال و کاهش ریسک و خطر نفوذ می باشد.

ناحیه امنیتی با Zone :

حتما در محیط اینترنت وشبکه با این واژه آشنا شده ایداما شاید تعریف دقیقی از آن نداشته باشید.در واقع ناحیه امنیتی یک اصلاح در شبکه می باشد و تعریف آن به این صورت می باشد که ناحیه و یک اصطلاح منطقی و یا مجازی که درواقع قسمتی از شبکه می باشد که از نظر امنیت و دسترسی با دیگر قسمت ها متفاوت می باشد در بعضی از فایروال ها مانند فایروال Juniper [54],Fortigate [55]کنترل دسترسی برروی ناحیه ها می باشد و اما

[54] نام یکی از شرکت های تولید کننده

[55] ام یکی از شرکت های تولید کننده

در بعضی دیگر مانند Cisco ASA[56] واژه ناحیه وجود ندارد و شما کنترل دسترسی را برروی ترافیک ورودی به اینترفیس ها اعمال می کنید. در واقع ناحیه به هرکدام از اینترفیس ها گفته میشود.

.با یک بررسی های انجام شده ناحیه ها از نظر امنیتی عبارتند از:

سرورها

کاربران

DMZ

WAN

اینترنت

توپولوژی های قرارگیری فایروال در شبکه:

قرارگیری فایروال در شبکه در واقع طراحی مجدد یک شبکه با رویکرد حفاظت در برابر حملات و کنترل دسترسی می باشد. اگرچه پیاده سازی هر فایروال برحسب نوع برند منحصربفرد می باشد اما کلیات طراحی و قرارگیری فایروال در همه یکسان میباشد. توپولوژی پیاده سازی فایروال در شبکه در پیاده سازی یک فایروال و یا دو فایروال متفاوت می باشد.

[56] ام یکی از شرکت های تولید کننده

طراحی Single-Firewall

در این طراحی به دو صورت:

قرارگیری فایروال در مرکز شبکه و عبور کلیه ترافیک ها از آن

قرار گیری در جلوی اینترنت و یا Internet Access[57] می باشد

در طراحی در مرکز شبکه جدا سازی ناحیه ها بستگی به منابعی که شما قرار است از آن حفاظت کنید می باشد . این ناحیه ها می تواند به صورت زیر باشد:

DMZ

Internal[58]

اینترنت

طراحی Dual Firewall:

شما ممکن است علاوه بر قرار گیری فایروال در برابر ورودی اینترنت خواستار برقراری امنیت دیتا سنتر خود در برابر شبکه داخلی خود نیز باشد . در این طراحی ما امنیت بالاتری را نسبت به مورد قبل می توانیم ایجاد نماییم و یکی از بهترین توپولوژی این توپولوژی می باشد پیشنهادی که از نظر امنیتی می توان به این توپولوژی اضافه نمود این است درصورت امکان از فایروال با دو برند متفاوت استفاده نمود تا در صورت آسیب پذیری در یک فایروال این آسیب پذیری به لایه دیگر که فایروال با برند دیگر قرار دارد آسیب نرساند.

در این توپولوژی دفاع از شبکه داخلی دو لایه می باشد و ناحیه ها به این صورت می باشد:

سرور ها

کاربران

DMZ

اینترنت

[57] دستیابی به اینترنت

[58] داخلی

موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن ، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از :

موقعیت و محل نصب از لحاظ توپولوژیکی : معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.

قابلیت دسترسی و نواحی امنیتی : اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند ، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی وتنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیه DMZ ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.

مسیریابی نامتقارن : بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.

فایروالهای لایه ای : در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرارگیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می دهد.معمولا بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند.

یک سیستم تشخیص نفوذ

عبارتست از ابزاری که منحصرا برای پایش دروازه‌های اطلاعاتی، فعالیتهای خصمانه و نفوذهای شناخته شده پیکربندی شده‌است. یک IDS یک ابزار تخصصی است که به خوبی قادر است تا ترافیک شبکه و یا فعالیتهای میزبانهای آنرا تجزیه و تحلیل کند. داده‌های تحلیل شده می‌تواند از آنالیز بسته‌های شبکه گرفته تا محتوای فایلهای Log متعلق به فایروال‌ها، روترها و سرویس‌دهنده‌ها و نیز فایلهای Log سیستم‌های محلی و داده‌های

جریان شبکه را شامل شود. بعلاوه، یک IDS [۵۹]معمولاً دارای یک پایگاه‌داده از الگوها و مشخصه‌های حملات شناخته شده است که می‌تواند این الگوها و مشخصه‌ها را با داده‌های ترافیک شبکه و رفتار شبکه برای یافتن موارد انطباق مقایسه کند. در مواجهه با موارد یافته شده ترافیک خطرناک، سیستم تشخیص نفوذ می‌تواند هشدارهایی را اعلام کرده و یا اقدامات خودکار مختلفی را همچون قطع جلسه ارتباطی یا لینک اینترنتی مبدأ حمله، مسدود کردن وی با به‌روز کردن قواعد فایروال و یا انجام دادن فعالیتهای بیشتر در جهت شناخت دقیق‌تر نفوذکننده و جمع آوری شواهد بیشتری در مورد فعالیتهای شرورانه انجام دهد. درصورتی که یک سیستم IDS توان پیشگیری ازنفوذ را نیز داشته باشند به عنوان IPS [۶۰]معرفی می‌شوند؛ که در این حالت معمولاً سیستم تشخیص نفوذ یا با فایروال در ارتباط بوده و بسته‌ها را از آن دریافت می‌کند و یا اینکه خود در لایه‌های پایینی هم سطح فایروال قرار داشته و فعالیت جلوگیری از نفوذ را نیز انجام می‌دهد.

[59] کلمه (IDS Intrusion Detection System) که به معنای سیستم شناسایی نفوذ است دارای پهنه وسیعی از دانش مربوط به پرتکل ها و محتوای داخلی بسته ها است.

[60] IPS (Intrusion Prevention System)-IPS برای جلوگیری از ورود بدون مجوز به شبکه یا سرویس دهنده طراحی شده است و بجای اعلام اخطار مبنی بر اینکه قسمتی از سیستم دچار مشکل شده از صدمه سیستم جلوگیری به عمل می آورد.

ابزارهای لازم برای تست نفوذ و ارزیابی فایروال:

Tracert/Traceroute[61]

Firewalking[62]

Hpinging

پویش پورت های مبدأ(مبتنی بر UDP)

(icmpenum)(ICMP Enumerating)

Nmaping(Network mapping)

Ws_Ping Pro Pack

مزایا

تکنولوژی های IDS و IPS و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدید ها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک ، بر پایه مقصد نهایی آن اجازه عبور می دهد. ابزار IPS و IDS تجزیه و تحلیل عمیق تری را بر عهده دارند و بنا براین سطح بالاتری از محافظت را ارائه می کنندبا این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد.سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند.انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدودی زیادی غیر عملی خواهد بود.بعلاوه شبکه ساختار پویایی دارد.ابزار جدید،ارتقاء دادن نرم افزار ها و وصله ها ، و افزودن و کاستن از کاربران ، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیر جدید پیمایش کنید.روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است.هکر ها بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه

[61] traceroute یک ابزار شبکه رایانه‌ای است که برای ردیابی مسیر حرکت بسته‌های شبکه ای در شبکه ای با پروتکل اینترنت (IP) مورد استفاده قرار می گیرد.-Tracerout : یکی از دستورات جهت اطلاع از میزان ارسال و دریافت در شبکه

[62] روشی برای حفاظت در مقابل ورود بسته های غیر قابل اطمینان

هستند .همچنانکه پدیده های اخیر چون Mydoom , Sobig,Sasser گواهی بر این مدعا هستند.برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند.

فایروال وهکرها

اینترنت مقادیر زیادی از اطلاعات قابل دسترس را در اختیار کامپیوترهای خانگی متوسط در زمینه های تجارت و یا اموزش فراهم اورده است . برای اکثر مردم دسترسی به این اطلاعات نه تنها یک امتیاز بلکه یک امر ضروری محسوب می گردد. ولی هنوز اتصال نت ورک خصوصی به اینترنت می تواند یک اشکار شدنی خطرناک و در معرض قرار داد ن اطلاعات محرمانه در برابر حملات الکترونیکی اشخاص مغرض از هر کجا ی دنیا باشد. کاربرانی که کامپیوترشان را به اینترنت متصل می کنند می بایست در برابر این خطرات هوشیار باشند و از اطلاعات و نقاط ضعف سیستم خود حفاظت کنند . فایروال ها می توانند هر دو نمونه کامپیوترهای شخصی و شبکه های شرکتی را در مقابل دشمنان نفوذی از طریق اینترنت محافظت نمایند بشرطی که کاربرد صحیح آن ها رعایت شود.هکرها در مرحله آماده سازی برای حمله، به جمع آوری اطلاعات در مورد سیستم شما میپردازند. یک روش معمول ،ارسال یک بسته در یک وضعیت غلط به منظوری خاص است. برای مثال، یک بسته با عنوان پاسخ (Reply) به سیستمی که تقاضایی نکرده، میفرستند. معمولا کامپیوتر دریافت کننده باید پیامی بفرستد و بگوید "I don't understand" به. این ترتیب، به هکر نشان میدهد که وجود دارد، و آمادگی برقراری ارتباط دارد. بعلاوه، قالب پاسخ میتواند سیستم عامل مورد استفاده را نیز مشخص کند، و برای یک هکر گامی به جلو باشد. یک فیلتر Stateful packet منطق یک ارتباط TCP/IP را میفهمد و میتواند یک "Reply" را که پاسخ به یک تقاضا نیست، مسدود کند ـــ آنچه که یک فیلتر packet ردگیری نمیکند و نمیتواند انجام دهد. فیلترهای Stateful packetمیتوانند در همان لحظه قواعدی را مبنی براینکه بسته مورد انتظار در یک ارتباط عادی چگونه باید بنظر رسد، برای پذیرش یا رد بسته بعدی تعیین کنند. فایده این کار امنیت محکمتر است. این امنیت محکمتر، به هرحال، تا حدی باعث کاستن از کارایی میشود . نگاهداری لیست قواعد ارتباط بصورت پویا برای هر ارتباط و فیلترکردن دیتای بیشتر، حجم پردازشی بیشتری به این نوع فیلتر اضافه می کند.

فایروال بر روی چه برنامه هائی تاثیر می گذارد ؟

فایروال ویندوز با هر برنامه ای که تصمیم به ارسال داده برای سایر کامپیوترهای موجود در شبکه داخلی و یا اینترنت را داشته باشد ، تعامل خواهد داشت . پس از نصب فایروال ، صرفا" پورت های مورد نیاز برنامه های متداول مبادله اطلاعات نظیر Email و استفاده از وب، فعال می گردند . در این راستا و به منظور حفاظت کاربران ، امکان استفاده از برخی برنامه ها بلاک می گردد . سرویس FTP رویس ارسال و یا دریافت فایل ، بازی های چند نفره ، تنظیم از راه دور Desktop و ویژگی های پیشرفته ای نظیر کنفرانس های ویدئویی و ارسال فایل از طریق برنامه های Instant Messaging (IM) ، از جمله برنامه هائی می باشند که فعالیت آنان توسط فایروال بلاک می گردد . در صورت ضرورت می توان پیکربندی فایروال را بگونه ای انجام داد که پورت های مورد نیاز یک برنامه فعال تا امکان مبادله اطلاعات برای برنامه متقاضی فراهم گردد .

طراحی فایروال محیطی(Perimeter Firewall)

طراحی فایروال برای Data Center و محافظت از یکData Center [۶۳]

1-تعاریف

طراحی محیط شبکه مطابق با مدل های روز به صورت زیر خواهد بود

-جدا سازی دامن های خطر با لایه های مختلف فایروال

-یک دامنه خطر در هر لایه در ساختار طراحی

-نواحی امنیتی در Outer-Tire برای دسترس بودن

-نواحی امنیتی در دامنه خطر Middle-Tire برای اجزایTire-2

-امنیت در دامنه خطر لایه داخلی (Tire Inner-)برای دسترسی داخلی به سرورها و برنامه های کاربردی و سرور پایگاه داده

- Out Of Band Management [۶۴]

- Out Of Band Back up [۶۵]

-جدا سازی فیزیکی دامنه های خطر

---

63 مرکز داده

64 خارج از مدیریت پهنا

65 خارج از باند پشتیبان گیری

-جدا سازی منطقی نواحی امنیتی

-زوج فایروالهای با ضریب اطمینان بالا

واژه های خارجی، میانی و داخلی جهت توصیف 3 لایه از فایروال می باشد. مدل لایه نرم افزار کاربردی به صورت:

Tier 1 Presentation

Tier 2 Application

Tier 3 Data

طراحی جزیی محیطی:

Tier 1از ساختار نرم افزار که توسط فایروال خارجی سرویس داده می شود.

Tier 2از ساختار نرم افزار که توسط فایروال میانی سرویس داده می شود.

Tier 3 از ساختار نرم افزار که توسط فایروال داخلی سرویس داده می شود.

در این طراحی، فایروالها تمام ترافیک ورودی وخروجی محیط شبکه را کنترل می کنند بنابراین افزونگی (Redundancy)کامل لایه های خارجی، داخلی و میانی فایروال میزان اطمینان و پایداری بالا را حتمی می سازد.

2-دفاع در عمقدر این طراحی، دو محصول فایروال متفاوت در نظر گرفته شده است. آسیب پذیرهایی که ممکن است در یک سیستم فایروال کشف شوند نمی توانند روی فایروال دیگر به اجرا در آمده و شبکه پیرامون مرکز دیتا (Data Center) را مورد تهاجم قرار دهند.جدا سازی فیزیکی نواحی خطر، داخل لایه (Tier) فایروال به کمک سوئیچ های لایه دو و رابط های فیزیکی فایروال حاصل می شود.نواحی چندگانه خطر می توانند برای هر لایه تعریف شوند. نواحی امنیتی داخل یک حوزه خطر جهت رسیدن به تفکیک بیشتر با استفاده از جداسازی منطقی توسط VLAN به کار می آیند. دو سوئیچ مجزا ممکن است در یک حوزه خطر برای اهداف افزونگی زیر ساخت به کار آیند. استفاده ا ز دو کارت شبکه نیز برای افزونگی ارتباط Host در این راستا قرار دارد. دیاگرام زیر طراحی شبکه در سطوح بالا را نشان می دهد.

3-فایروال داخلی

کنترل فایروال ها توسط فایروال داخلی انجام می شود. اگر هر کدام از فایروال های خارجی و یا میانی و یا سیستم های داخل DMZ مورد حمله قرار گرفته و کنترل آنها توسط هکرها بدست گرفته شود فایروال داخلی به عنوان محافظ آدرس های داخلی شبکه در برابر حملات انجام شده خواهد بود. فایروال Check Pointمی تواند بعنوان لایه سوم مورد استفاده قرار بگیرد. به عنوان مثال مجموع دستگاه Nokia IP 530 که در حالت فعال/غیر فعال تنظیم شده اند را می توان استفاده نمود.

4-فایروالهای میانی:

نقش فایروالهای لایه داخلی (Inter-tier) بوسیله فایروالهای میانی ایفا می شود. آنها برنامه های کاربردی را در معماری سه لایه ای فعال می کنند

فایروال NG[66]می تواند در یک پیکربندی HA (High Availability) برای این منظور استفاده شود.

5-فایروالهای خارجی

نقش مکانیزمهای تقویت امنیت بوسیله این فایروالها ایفا می شود. این فایروالها به اینترنت متصل می شوند. این فایروالها در یک زوجی از پیکربندی فعال-غیر فعال پیاده سازی شده که یکی از آنها به عنوان فایروال اولیه عالیت کرده و دیگری به عنوان فایروال Standby به منظور اطمینان بالا (High Availability) عمل می کند.نواحی امنیتی لایه 1 (Tier-1) نیز بوسیله فایروالهای خارجی کنترل می شوند. سرویس های برنامه های کاربردی مانندMail Relay ، DNS [67]و پروکسی های وب توسط فایروالهای خارجی کنترل می شوند. فایروالهای Ciscoمانند سری Cisco pix 535 می توانند برای لایه خارجی به کار آیند.

6-دستاوردها

طراحی محیطی (Perimeter design) دستاوردهای زیر را به همراه دارد:

-اطمینان و پایداری بالا از طریق افزونگی

-کارایی بالا

- OSPF[68](آگاهی شبکه)

-افزایش اطمینان و بازیابی(VRRP)

---

[66] نام یکی از محصولات فایروال

[67] The Domain Name System-سیستم نام دامنه

[68] Open Shortest Path First- کوتاهترین مسیر گسترش اول

-افزونگی (Failover) ارتباطات داخلی

-افزونگی (Failover) ارتباطات خارجی

-نواحی امنیتی و حوزه های خطر چند گانه درگاههای (VLAN)

-بازرسی بسته ها و فیلترینگ آنها به روش Statefull

-بازرسی محتوی بوسیله مکانیزم Check Point Application Intelligence [۶۹]

-سخت افزار مختص عملکرد فایروال

-دفاع در عمق- لایه های مختلف فایروال و محصولات متنوع

-ترجمه و تفسیر آدرس بین شبکه ها

-قابلیت IDS در ساختار موجود

ضرورت توجه به امکانات سایر فایروال های نرم افزاری

فایروال ویندوز ، امکانات حفاظتی لازم به منظور بلاک نمودن دستیابی غیرمجاز به سیستم شما را ارائه می نماید . در این رابطه دستیابی به سیستم از طریق کاربران و یا برنامه های موجود در خارج از شبکه محلی ، کنترل خواهد شد . برخی از فایروال های نرم افزاری یک لایه حفاظتی اضافه را نیز ارائه داده و امکان ارسال اطلاعات و یا داده توسط کامپیوتر شما به سایر کامپیوترهای موجود در شبکه توسط برنامه های غیر مجاز را نیز بلاک می نمایند (سازماندهی و مدیریت یک فایروال دوطرفه) . با استفاده از این نوع فایروال ها ، برنامه ها قادر به ارسال داده از کامپیوتر شما برای سایر کامپیوترها بدون اخذ مجوز نخواهند بود . در صورت نصب یک برنامه مخرب بر روی کامپیوتر شما) سهوا" و یا تعمدا") برنامه فوق می تواند در ادامه اطلاعات شخصی شما را برای سایر کامپیوترها ارسال و یا آنان را سرقت نماید . پس از نصب فایروال های دوطرفه ، علاوه بر تمرکز بر روی پورت های ورودی (Incoming)، پورت های خروجی (Outgoing) نیز کنترل خواهند شد .

حفاظت با سه حالت فایروال

[69] بازرسی کاربرد اطلاعات

Online Armorبرای نخستین بار بعد از نصب در حالت استاندارد اجرا می شود که استفاده از آن برای هر کاربری آسان است. پیچیدگی فنی وجود ندارد.

یک لیست سفید از برنامه هایی که Online Armor تضمین می کند امن هستند، آماده می شود. به عبارت دیگر فایروال به طور خودکار آن ها را در لیست مجاز ها (لیست سفید) قرار می دهد. در حالت پیشرفته گزینه های بیشتری برای کاربر های حرفه ای وجود دارد. برای نمونه: ممکن است ایجاد محدودیت دسترسی به چند شبکه انتخاب شده، برای جلوگیری از بارگذاری محتوای ناخواسته وب سایت هایی از کشور های خاص که برای انتشار نرم افزار های مخرب شناخته شده هستند. حالت سوم حالت بانکی است که مخفف بانکداری آنلاین مطمئن می باشد.

حفاظت Keylogger

Keyloggers نوعی از مخرب ها هستند که به صورت پنهان فعالیت می کنند .کلید های تایپ شده معمولا برای یک هکر فرستاده می شوند. برای نمونه در هنگام ورود به سیستم پی پال، یا وارد کردن مشخصات در پرداخت از طریق سایت های بانکی Online Armor در هر لحظه حاضر است و تمامی برنامه هایی را که به طور مشکوک اقدام به ذخیره کردن عملکرد صفحه کلید می کنند را گزارش می دهد .یک لیست سفید وجود دارد که می توانید برنامه هایی را که از امن بودن آن ها اطمینان دارید در آن وارد کنید تا با هشدار برنامه مواجه نشوید.

حفاظت DNS-Spoofing

یک روش پنهانی ارسال کاربر ها به صفحات جعلی بانکداری آنلاین است که DNS-Poisoningنامیده می شود. آنلاین آرمور از این روش به خوبی جلوگیری می کند.

کنترل Autostart

بسیاری از برنامه ها به طور خودکار هنگام شروع به کار ویندوز اجرا می شوند. آیا این مطلوب است یا خیر . Online Armorتمامی این برنامه ها را لیست کرده و وضعیت امنیتی آن ها را مشخص می کند)مطمئن، غیر مطمئن، ناشناخته). کاربر می تواند خودش تصمیم گیری کند که آیا آن برنامه ها برای اجرا شدن بعدی مجاز

باشند یا خیر. Online Armorلیست سفیدی شامل تمامی برنامه های ایمنی که کاربر می تواند به آن ها اطمینان کند ارایه می دهد.

حالت بانکداری آنلاین

انجام پرداخت های بانکی از طریق اینترنت بسیار راحت به نظر می رسد اما می تواند خطرناک باشد. به همین دلیل Online Armor قابلیت های ویژه و منحصر به فردی برای حالت بانکداری آنلاین ارایه می دهد. در این حالت کامپیوتر تنها می تواند به صفحات بانکداری آنلاین مجاز دسترسی داشته باشد و صفحات خانگی سایت های دیگر از جمله صفحات فیشینگ قابل دسترس نمی باشد. با استفاده از Online Armor شما می توانید با خیال راحت اقدام به پرداخت های اینترنت کنید

پوشش محافظ برنامه

از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شفاف است و با درجه بالایی با سیستم یکپارچه می شود .یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور پیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.

تشخیص فعالیت ویروسی

در حالی که برنامه ضدویروس در تشخیص ویروس ها مهارت دارد، این نرم افزار برای تشخیص فعالیت ویروسی طراحی نشده است. در این شرایط بکارگیری یک برنامه تشخیص نفوذ یا IDS شبکه برای تشخیص این نوع فعالیت بسیار مناسب است .

پروتکل های رایج که شما می توانید فیلترهای فایروال را بر آن اساس تنظیم کنید عبارتند از:

الف) IP :پروتکل اینترنت) – سیستم اصلی انتقال اطلاعات بر روی اینترنت.

ب) TCP :پروتکل کنترل انتقال اطلاعات) – برای خرد کردن و بازسازی اطلاعاتی که بر روی اینترنت جا به جا می شود به کار می رود.

ج) HTTP:پروتکل انتقال ابر متن – (Hyper Text Transfer)– برای صفحات وب استفاده می شود.

د) FTP :پروتکل انتقال فایل – برای دانلود و آپلود فایل استفاده می شود.

ه) UDP :پروتکل دادهای کاربر – برای اطلاعاتی استفاده می شود که نیاز به پاسخ ندارد ، مانند پخش فایل های صوتی و ویدئویی.

و) ICMP :پروتکل کنترل پیام اینترنت – توسط یک روتر (router) به منظور مبادله اطلاعات با روترهای دیگر استفاده می شود.

ز) SMTP :پروتکل انتقال ساده ایمیل – مورد استفاده برای ارسال اطلاعات متنی (ایمیل)

ح) SNMP :پروتکل مدیریت شبکه ساده – برای جمع آوری اطلاعات سیستم از یک کامپیوتر از راه دور (remote computer).

ط) Telnet :شبکه راه دور – برای انجام و اعمال دستورات بر روی یک کامپیوتر از راه دور.

آیا باز نمودن پورت های فایروال خطرناک است ؟

با باز نمودن هر پورت ، کامپیوتر شما در معرض تهدیدات بیشتری قرار خواهد گرفت . علیرغم باز نمودن برخی پورت ها به منظور بازی و یا اجرای یک کنفرانس ویدئویی ، فایروال ویندوز همچنان از سیستم شما در مقابل اغلب حملات محافظت می نماید. پس از معرفی یک برنامه به فایروال ویندوز ، صرفا" در زمان اجرای این برنامه پورت های مورد نیاز فعال و پس از اتمام کار ، مجددا" پورت های استفاده شده غیرفعال می گردند . در صورتی که به صورت دستی اقدام به باز نمودن پورت هائی خاص شده باشد، پورت های فوق همواره باز شده باقی خواهند ماند . به منظور حفظ بهترین شرایط حفاظتی و امنیـتی ، می توان پس از استفاده از پورت و یا پورت هائی که با توجه به ضرورت های موجود فعال شده اند ، آنان را مجددا" غیرفعال نمود استفاده از checkbox موجود در مجاورت برنامه در لیست Exception [۷۰]

آنتی ویروس:

ویروس‌ها برنامه‌هایی هستند که به شکل پنهانی، موقع اجرا شدن برنامه آلوده خود را به برنامه‌های اجرایی نظیر فایل‌های COM و EXE می‌چسبانند و معمولاً بدون اینکه تاثیری در کار اصلی برنامه آلوده بگذارند، منتظر زمان فعالیت نهایی یا برقراری شرط خاصی می‌شوند. حال این فعالیت می‌تواند بزرگ‌تر کردن فایلهای مختلف DATAباشد، یا آلوده کردن فایلهای اجرایی و یا از بین بردن اطلاعاتPARTITION TABLE [۷۱]، معدوم کردن اطلاعا ت با ارزش یا از کار انداختن فایل‌های اجرایی و ... باشد. ولی در هر حال یک چیز در اکثر ویروس‌ها مشترک می‌باشد و آن انتقال ویروس از فایل‌های آلوده به فایل‌های سالم است. نرم‌افزارهای آنتی

[70] استثنا

[71] جدول پارتیشن

ویروس تمام فایل‌ها را به طور خودکار بررسی کرده و فایل‌هایی که دارای گونه‌های شناخته شده ویروس‌ها هستند را شناسایی و عکس‌العمل مناسب انجام می‌دهند.

Anti-Spam:

اسپم در کامپیوتر به ایمیل‌هایی گفته می‌شود که به طور ناخواسته برای ما فرستاده می‌شوند و جنبه تبلیغاتی دارند. راه‌های مختلفی برای مقابله با اسپم‌ها در جاهای مختلف آمده و حتی یاهو هم یک آنتی اسپم را برای کاربرانش پیشنهاد کرده است.

فیلترینگ:

فیلتر ابزاری است که به منظور تصفیه اتصالات وب استفاده می‌شود. در کشورهای مختلف دنیا فیلترینگ به دو روش انجام می‌شود: فیلتر کردن نشانی‌های اینترنتی براساس یک لیست سیاه (در یک پایگاه داده)، و فیلتر کردن براساس محتوای هر صفحه اینترنتی. روش دوم در دنیا به فیلتر محتوا (content filter) معروف است که برای پهنای باند خیلی بالا قابل انجام نیست.

پیکربندی فایروال و انواع DMZ در حفاظت از شبکه

مجتمع کردن دستگاه های اطراف شبکه به منظور محافظت از شبکه خصوصی مؤلفه مهمی برای طراحی امنیت محیط پیرامون است. انتخاب دستگاه ها بستگی به فاکتورهای متعددی برای هر کمپانی دارد، اما دستگاه های ضروری و لازم که باید لحاظ گردند به منظور صورت گرفتن این امنیت، روتر و فایروال هستند. روتر به عنوان اولین خط دفاعی عمل می کند و فایروال به عنوان ناظر ترافیک عمل می کند و فقط به ترافیک های مجاز شبکه اجازه می دهد. یک IDS یا IPSباید حتماً در محیط پیرامون شبکه لحاظ گردند تا از شبکه خصوصی در مقابل فعالیت های مخرب محافظت کنند .

به طور کلی در معماری شبکه سازمان سه ناحیه وجود دارد :

Border Network[۷۲]یا : Internet شبکه ای است که مستقیماً با اینترنت در تماس است.

[72] مرز شبکه

Perimeter Network:[۷۳]شبکه ای که کاربران ورودی را به سرورهای وب یا دیگر سرویس ها متصل می کند و معمولاً DMZ یا Edge Network[74] نامیده می شود Internal Network[75].یا : Private Network[76] شبکه داخلی سازمان است که سرورها را به یکدیگر و به کاربران داخلی متصل می کند .

[73] محیط شبکه

[74] لبه شبکه

[75] شبکه داخلی

[76] شبکه خصوصی

یک شبکه ساده که هیچ سرویس اینترنتی برای مشتریان فراهم نکرده است محافظت کردن آن ساده تر خواهد بود. روتر و فایروال اینترنت را از شبکه خصوصی جدا می کند، IDSیا IPS همه ترافیک ها را مانیتور می کند و VPNدستیابی از راه دور را فراهم می کند. هر کدام برای دفاع در عمق محیط پیرامون لازم هستند .پیکربندی رولهای فایروال برای اینچنین شبکه ای آسان است. فایروال دو دسته رول دارد که رول ingress [۷۷]و رول egress[۷۸]نامیده میشوند که به ترتیب مشخص میکند که ترافیک شبکه اجازه ورود و ترک را دارد. آن بخش از ترافیک شبکه که برای رسیدن به آدرس IP اختصاصی تلاش میکند باید به وسیله رولهایingress ، با استفاده از فیلترینگ استاتیک توسط روتر یا فایروال بلوکه شود. یک استثناء وجود دارد و آن زمانی است که یک ارتباط از راه دور از طریق سازمان، مجوز اتصال به شبکه خصوصی را دارد. ارتباطات از راه دور باید از یک ارتباط ایمن همچون VPN برای اتصال استفاده کنند VPN.باید با فایروال مجتمع گردد یا توسط یک appliance جداگانه پشت فایروال قرار گیرد .هنگامی که سرویس های وب و پست الکترونیک در شبکه خصوصی ارائه دهنده سرویس به اینترنت هستند به طراحی پیچیده تری برای محیط پیرامون شبکه نیاز می باشد به منظور فراهم کردن محیطی امن. سرورهای وب و پست الکترونیک نسبت به حمله آسیب پذیری بیشتری دارند به خاطر پیکربندی های پیچیده و متدلوژی های برنامه نویسی نامناسب که طرح امنیت را از ابتدا با مشکل مواجه می کند. این سرورها لازم است در فضایی از شبکه خصوصی قرار گیرند، اما ایزوله باشند. این جداسازی توسط DMZمحقق می شود. یکی از روش های پیاده سازی DMZ استفاده از دو دستگاه فایروال است و در فضای بین دو فایروال DMZ subnet [۷۹]قرار می گیرد .هزینه اضافی و نگهداری این طراحی می تواند فقط برای شبکه هایی با پهنای باند مناسب توجیه گردد. نوعاً DMZ با استفاده از سه ارتباط روی فایروالی که برای اینترنت، DMZو شبکه خصوصی استفاده شده است، پیاده سازی می شود. به خاطر اینکه شبکه خصوصی و شبکه DMZبه صورت فیزیکی با هم ارتباط ندارند یک IDSیا IPS باید در جلوی فایروال قرار گیرد تا تمامی ترافیک شبکه را ضبط کند .یک عیب برای طراحی یک DMZ زمانی است که داده ذخیره شده در شبکه خصوصی قابل دسترسی توسط هیچ سروری که در ناحیه DMZ قرار دارند نمی باشد. چنانچه داده ذخیره شده لازم باشد که در دسترس سروری در ناحیه DMZ قرار گیرد دو سناریو وجود دارد. سناریوی اول ارتباط دستی به سرور وب به منظور اپلود کردن داده است. سناریو دوم استفاده از دو ناحیه DMZ جداگانه است که اطلاعات عمومی را از اطلاعات خصوصی جدا میکند که به ترتیب DMZ[80] Anonymous و DMZ[81] Authenticated نامیده میشود

[77] ورود

[78] خروج

[79] زیرشبکه ای

[80] بی نام

[81] تصدیق شده

3-19 نتیجه فصل سوم

باتوجه به مسائل بیان شده به این نتیجه می رسیم که درواقع

می‌توان گفت یک دیواره آتش :

-یک جداساز است .

-یک محدودساز(Restrictor) است .

-یک آنالیزکننده(Analyzer) است.

یک دیواره آتش ممکن است :

-مسیریابی با چند لیست کنترل دسترسی باشد .

-نرم افزاری که روی یک PC یا یک سیستم Unix اجرا می شود، باشد .

-یک جعبه سخت افزاری اختصاصی باشد .

انواع پیچیده تر دیواره های آتش به صورت ترکیبی از چندین سیستم و راه حلهای Multi-computer و Multi-router پیاده سازی می‌شوند. شبکه های مختلف بسته به نیازهای امنیتی مختلف و هزینه ای که برای تأمین امنیت در نظر گرفته اند از دیواره‌های آتش مختلف و روشهای پیاده سازی مختلف آنها استفاده می‌کنند

فصل چهارم

1-4)مقدمه فصل چهارم

استفاده ازفایروالها مزایایی همچون: کنترل ترافیک،تبدیل آدرس،نقطه پایانیvpn،امنیت در شبکه،جلوگیری از ایجاد ترافیک،کاهش ریسک سروربا فیلتر کردن آن ومعایبی چون: محدودیت در دسترسی به اینترنت،ناامنی در مقابل هکرها درback doorدارد.راهکارهایی برای بهبودی ان نظیر: اسکن ترافیک داخل وخارج رایانه و..... وجود دارد.

2-4)مزایا و معایب استفاده از فایروال

1-2-4)معایب

بسته ها و نرم افزار های ویروسی نوسط فایروال سخت افزاری تشخیص داده نمی شوند.

برای فایروال های سخت افزاری مسئله هزینه و کابل کشی برای فایروال نرم افزاری مسئله زمان بر بودن و کمبود حافظه مطرح است.

فایروال نمی تواند ویروسهایی که در میزبان کپی شده را تشخیص و در نتیجه در کل شبکه پخش می شود.

فایروال های نرم افزاری سرعت را پایین می آورند.

Firewall ها دارای مزایای بسیاری می باشند با این وجود دارای معایب نیز هستند . بعضی از Firewall در مقابل محدود کردن کاربران و درهای پشتی (Back door) که محل حمله هکرها ست که امنیت ندارند.

Access Restrictions[۸۲]

Firewallهابرای ایجاد امنیت ، بعضی از سرویسها مانند Telnet , Ftp , Xwindow را از کار می اندازند و این تنها محدود به فایروالها نمی شود . بلکه در سطح سایت نیز می شود این کار را انجام داد.

Back-Door Challenges: The Modem Threat[۸۳]

تا حال مشخص شد که امنیت درهای پشتی کمپانی به وسیله Firewall تا مین نمی شود بنابراین اگر شما هیچ محدودیتی در دسترسی به مودم نداشته باشد این در بازی برای هکرها ست.

SLIP [84], و ppp [۸۵]راههای ورودی می باشند و سئوال پیش می آید که اگر این سرویسها وجود داشته باشند.محدودیت در دسترسی به اینترنت،بعضی از فایروالها در مقابل محدود کردن کاربران وback door که محل حمله هکرهاست امنیت ندارند.

---

[82] محدودیت های دسترسی

[83] چالش تروجان : تهدید مودم

[84] خط سریال پروتکل اینترنت

[85] Point-to-Point Protocol-پروتکل نقطه به نقطه

برای ایجاد امنیت بعضی از سرویس ها مانندxwindow،ftp،telnet،را از کار می اندازند.فایروالهای سخت افزاری هزینه زیادی نیاز دارند.جاگیر هستندوبه کابل کشی نیاز دارند.نصب وupgrade آن دشوار است.با مودم های dial upکار نمی کنند.فایروال نرم افزاری برای هر کامپیوتر موجود در شبکه نیاز به نصب جداگانه دارندوبسیار زمان بر است.گاهی un install کردن آن بسیار دشوار است.گاهی در پاسخگویی سیستم که بحرانی وحیاتی است مناسب نیستند.اشغال کردن فضای memoryوcpu .فایروال ها باعث کاهش توان مصرف ریزپردازنده می شوند.اسبهای تراوا می توانند به سادگی وبا استفاده از همان مکانیسم مورد استفاده فایروال در سطح پایین تری از آن قرار گرفته وبه فعالیت بپردازند

2-2-4)مزایای فایروال:

1.ایجاد یک دریچه متمرکز بر روی شبکه که از ورود کاربران غیر مجاز جلوگیری می کند

2.فایروال برای کامپیوتر ها، حفاظتی را جهت جلوگیری از ایجاد ترافیک و اخطار به کاربران ایجاد می کند اما در صورتی که کاربر به این پیغام های توجهی نکند ان کار فایده ندارد.

3.فضای منطقی برای گسترش آدرس های NAT ایجاد می کند .این آدرس ها به کم کردن فضای آدرس کمک می کند.

کنترل ترافیک.تبدیل آدرس .نقطه پایانیvpn وامنیت درشبکه.جلوگیری از ایجادترافیک کاهش ریسک سرور با فیلتر کردن ومعایب آن:محدودیت در دسترسی به اینترنت ناامنی درمقابل هکرهادر back doorکاهش سرعت دراینترنت در استفاده از فایروال نرم افزاری.باعث کاهش مصرف توان ریزپردازنده می شود. روش های هدفمندی فایروال:تخصیص آدرسهای منحصربه فرددرهرip استفاده از نام های دامنه .بهره گیری از پروتکل های سرویس دهنده وسرویس گیرنده. استفاده از پورت های شماره گذاری شده.استفاده از کلمات وعبارات خاص در متن مخصوص فایروالها.مشخص کردن سطوح امنیت .دقت به بستر اجرایی موردنظر.در فایروالهای مبتنی برمیزبان غربال سازی هنگام نیاز وافزودن ضابطه ممانعت به tcpwrapperمشخص کردن فایروال موردنیازوپیاده سازی آن مکانیسم های پشت فایروال امنیت را بالا می برند.یکی از مزایای Firewall ها استفاده آنها برای اینکه بتوانیم با Log کردن دسترسی به سایت آمار دسترسیهای به سایت خود را مشخص کنیم.

فایروالها امنیت را درشبکه برقرار می کنند.ریسک server های شبکه را با فیلتر کردن کاهش می دهند.از دسترسی مستقیم به سرور جلوگیری می کند.پیاده سازی فایروال ها بسیار اسان است چون یک نرم افزار خاص هستند.با استفاده از فایروال می توانیم با logکردن دسترسی به سایت آمار دسترسی ها به سایت خود رامشخص کنیم.فایروال ها حفاظت لازم را در مقابل مهاجمان خارجی را ایجادویک لایه یا پوسته پیرامون کامپیوتر ویا یک شبکه را در مقابل کدهای مخرب ویا ترافیک غیرضروری اینترنت را ارایه می نمایند.فایروال ها امکان بلاک نمودن داده ها رااز مکانی خاص فراهم می کند.تبدیل آدرس،نقطه پایانیvpn ،فایروال ها تحت کلیه ویندوزها قابل اجرا هستند.دسترسی فایروال به بسته کامل تمام بسته هایی که برای عبور از شبکه ناگزیربه تکه تکه شدن هستند. فرد راموقع ورودبه سیستم در یک نقطه کاملا کنترل شده محدود می سازد.از نزدیک شدن خرابکاران به منابع داخلی جلوگیری می کند.فرد را هنگام خروج در یک نقطه کاملا کنترل شده محدود می سازد.فایروال ها علاوه بر این که امنیت واقعی را برقرار می کنندیک نقش اساسی را در مدیریت امنیت پوشش می دهند

3-4)مزایای فایروال های سخت افزاری

-تحت کلیه ویندوزها به صورت یکسان قابل استفاده است

کل شبکه رامحافظت می کنند.این نوع فایروالها از سیستم عامل ونرم افزارهای سیستم عمل می کنندودارای سیستم عامل جدایی هستند

-دیواره آتش به بسته‌های کامل دسترسی خواهد داشت .یعنی بسته‌هایی که برای عبور از شبکه ناگزیر به تکه‌های متعددی شکسته شده‌اند به صورت سر هم شده به دیواره آتش خواهند رسید و لذا دیواره آتش مجبور به انجام عمل سر هم کردن بسته‌ها نیست .

حفاظت بیشتر و کلی تری نسبت به فایروال های نرم افزاری دارند.

کل شبکه را محافظت می کنند.

تا زمانی که در سیستم اجرا نشده اند هیچ تاثیری بر روی عملکرد سیستم ندارند.

این نوع فایروال ها به صورت مستقل از سیستم عامل و نرم افزار های سیستم عمل می کند و دارای سیستم عامل جدایی هستند.

4-3-1)معایب:

– نصب و پاک‌سازی چنین دیواره آتشی به سادگی امکان پذیر نیست و عدم دقت کافی به این مساله ممکن است نیاز به نصب مجدد ویندوز داشته باشد .

اسبهای تراوا می‌توانند به سادگی و با استفاده از همان مکانیزم مورد استفاده دیواره آتش در سطحی پائین‌تر از آن قرار گرفته و به فعالیت بپردازند.

هزینه بیشتری نسبت به فایروال های نرم افزاری دارند، حتی با وجود اینکه به نظر خرید یک فایروال سخت افزاری کم هزینه تر از خرید چند فایروال نرم افزاری در یک شبکه بزرگ است.

جاگیری و کابل کشی پیچیده دارد.

فایروال های سخت افزاری ، با مودم های Dial Up کار نمی کنند.

نصب و Upgrade[86] کردن آن دشوار است.

4-4)فایروال نرم افزاری – برنامه ویندوز فایروال

4-4-1)مزایا :

به سخت افزار اضافه ای نیاز نمی باشد .

به کابل کشی اضافه ای نیاز نخواهد بود .

گزینه ای مناسب برای یک کامپیوتر

.فایروالهای نرم افزاری به راحتی upgrade می شوندوبه طورجداگانه قابل نصب هستندونیاز به بسته یا دستور خاصی ندارند.سرعت وامنیت فایروالهای نرم افزاری بیشتر است وغالبا بدون مداخله هستند.فایروالهای نرم افزاری هزینه کمی دارند نیاز به کابل کشی ندارندوبا مودم های dial upکار می کنند

4-4-2)معایب

برای تهیه یک فایروال نرم افزاری می بایست هزینه ای اضافه پرداخت گردد.

استفاده از فایروال های نرم افزاری مستلزم نصب و پیکربندی خاصی می باشد .

برای هر کامپیوتر موجود در شبکه، نیاز به نصب جداگانه ای دارد در نتیجه زمان بر است.

گاهی Uninstall[87] کردن مامل آن دشوار است.

---

[86] بروز رسانی

[87] لغو نصب- حذف کردن

در زمانی که زمان پاسخگویی سیستم بحرانی و مهم است، مناسب نیستند.

اشغال کردن فضای CPU و Memory

برای هر کامپیوتر می بایست یک نسخه جداگانه نصب گردد

اما عیب این فایروال این است به دلیل ماهیت نرم افزاری بودن، فقط کامپیوتری را محافظت خواهد نمود که بر روی آن نصب شده باشد و هیچ اختلالی در فایل‌های فایروال وجود نداشته باشد به همین دلیل برای یک شبکه که از چندین کامپیوتر تشکیل شده باشد، استفاده از فایروال سخت افزاری در کنار فایروال نرم افزاری پیشنهاد می‌شود.برخلاف فایروال نرم افزاری، فایروال سخت افزاری می‌تواند بیش از یک کامپیوتر موجود در شبکه را محافظت کند چون هیچ وابستگی‌ای به کامپیوترهای شبکه نداشته و به تعداد پورت‌های آن می‌تواند کامپیوترهای شبکه را به وسیله یک فایروال سخت افزاری محافظت نمود

5-4)برتری فایروال سخت افزاری به فایروال نرم افزاری

سرعت:فایروال های سخت افزاری برای پاسخگویی سریعتر طراحی شده اند و از اینرو در کنترل بار ترافیکی شبکه و جایی که زمان پاسخگویی اهمیت دارد استفاده می شوند

امنیت:فایروال های سخت افزاری به دلیل داشتن سیستم عامل جدا کمتر از فایروال های نرم افزاری در معرض توجه نفوذگران قرار می گیرند از طرفی دارای کنترل کننده های بسیار قوی است.

بدون مداخله: این فایروال به دلیل جدا بودن از نود های شبکه مدیریت بهتر و آسان تری دارد و تاثیری بر کند یا تند کردن بقیه قسمت ها ندارد. به راحتی و جدا از سیستم می تواند خاموش یا دوباره نصب شود بدون هیچ تذاخلی در شبکه

6-4)برتری فایروال نرم افزاری به فایروال سخت افزاری

هزینه : هزینه کمتری نسبت به فایروال های سخت افزاری دارد

جاگیر نیست و هیچ گونه کابل کشی ندارد

با مودم های دایال اپ نیز کار می کند

نصب و راه اندازی ان نیاز به دانش خاصی ندارد

از مهمترین مزایای این گونه فایروال‌ها به نصب آسان آن (مثل یک برنامه ساده) و امکان پیکربندی و ایجاد Rule[88]های متنوع مورد نیاز اشاره کرد برای مثال می‌توان یک برنامه خاص را مجاز کرد و از اتصال یک برنامه دیگر به شبکه یا اینترنت جلوگیری کرد. همچنین کار با این فایروال‌ها بسیار ساده بوده و حتی کاربران مبتدی نیز می‌توانند با خیال راحت از آن‌ها استفاده کنند درحالی که نوع سخت افزاری فایروال‌ها نیاز به پیکربندی‌های دقیق تر دارند.

مزایا

معمولا" دارای حداقل چهار پورت برای اتصال سایر کامپیوترها می باشند .

امکان حفاظت چندین کامپیوتر را ارائه می نمایند .

معایب :

کابل کشی اضافه

5-4)روترهای بدون کابل : در صورتی که دارای یک شبکه بدون کابل می باشید و یا تصمیم به استفاده از چنین شبکه هائی را دارید ، به یک روتر بدون کابل نیاز خواهید داشت .روترهای بدون کابل اندکی به همراه یک فایروال تعبیه شده ارائه می شوند، بنابراین در چنین مواردی لازم است یک فایروال جداگانه تهیه گردد.

1-5-4)مزایا

با استفاده از روترهای بدون کابل می توان کامپیوترهای شخصی ، کامپیوترهای laptop ، دستگاه های PDA و چاپگرها را بدون استفاده از کابل به یکدیگر متصل نمود .

روترهای بدون کابل گزینه ای مناسب برای اتصال کامپیوترهای laptop به اینترنت و یا شبکه می باشند .

2-5-4)معایب

دستگاه های بدون کابل ، اطلاعات را با استفاده از امواج رادیوئی که می تواند توسط افرادی خارج از محل کار و یا منزل (با دارا بودن تجهیزات مناسب) استفاده گردد ، ارسال می نمایند .

برای استفاده از روترهای بدون کابل می بایست بر روی هر یک از دستگاه های مورد نظر یک آداپتور بدون کابل نصب گردد . بنابراین شما ملزم به پرداخت هزینه ای اضافه خواهید بود .

[8888] قوانین

تمامی روترهای بدون کابل به همراه یک فایروال تعبیه شده ارائه نمی گردند . در چنین مواردی می بایست یک فایروال جداگانه تهیه گردد .

اتصال به اینترنت برای کاربرانی که دارای دانش لازم به منظور ایمن سازی کامپیوتر نمی باشند ، همواره امری خطرناک است . با استفاده از فایروال ها می توان یک سطح مناسب امنیتی به منظور کاهش تهدیدات را ایجاد نمود . استفاده ایمن از اینترنت مستلزم عملیات متفاوتی است . نصب فایروال ، صرفا" یکی از اقدامات اولیه در این زمینه است. بهنگام سازی نرم افزارهائی که دارای نقشی اساسی بر روی یک کامپیوتر می باشند (نظیر سیستم عامل و مرورگر های وب) ، استفاده و بهنگام نگهداشتن یک نرم افزار آنتی ویروس از دیگر اقدامات ضروری در این رابطه می باشد

6-4)توانایی‌های دیواره‌های آتش :

یک دیواره آتش می‌تواند اجرای تصمیمات امنیتی را در یک نقطه متمرکزکند:، دیواره آتش یک نقطه محدود کننده بین دو شبکه است. تمام ترافیک به داخل و از خارج باید از این نقطه باریک عبورکند و راه دیگری برای عبور ترافیک وجود ندارد. بدین ترتیب دیواره آتش قابلیت اعمال کنترل شدیدی را دارا خواهد بود و می‌تواند با اعمال ابزار مختلف تأمین‌کننده امنیت در این نقطه سطح قابل قبولی از امنیت را تضمین کند. در واقع چون همه چیز در یک کانال ارتباطی قابل کنترل است می‌توان تصمیمات مختلفی را در ارتباط با امنیت شبکه گرفت و به اجرا در آوردن آنها را در یک نقطه متمرکز ساخت .یک دیواره آتش می‌تواند سیاست امنیتی شبکه را به اجرا در آورد: می‌دانیم سرویسهای مختلفی در شبکه‌ها وجود دارند و با گسترش اینترنت تنوع و تعداد آنها بسیار افزایش یافته است. اغلب این سرویسها ناامن هستند و هنگام استفاده و ارایه آنها باید دقت کرد. سیاست امنیتی شبکه‌های مختلف تعیین می‌کند که چه سرویسهایی در شبکه ارایه می‌شود و چه افرادی مجازند از این سرویسها استفاده کنند. دیواره‌های آتش قادرند با پاسبانی و کنترل سرویسهای مختلف تنها به سرویسهای مجاز تعریف شده در سیاست امنیتی اجازه عبور دهند و بدین ترتیب سیاست امنیتی شبکه را به اجرا درآورند. سیاستهای امنیتی نهایتاً به تعدادی قوانین اجرایی تبدیل می‌شوند که دیواره‌های آتش قادر خواهند بود تعداد زیادی از آنها را اجرا کنند. دیواره‌های آتش ممکن است سرویسهای خطرناک و ناامن و را با اعمال محدویت تنها در شبکه داخلی اجازه دهند .سیاستهای امنیتی مختلفی قابل اتخاذ هستند. مدیران یک شبکه ممکن است تنها به یک سیستم داخلی اجازه دهند. با دنیای بیرون در ارتباط باشد، در این صورت دیواره آتش تنها ترافیک متعلق به آن سیستم را از خود عبور خواهد داد .ذکر این نکته ضروری است که پیاده‌سازیهای مختلف از دیواره‌های آتش تواناییهای متفاوت در به اجرا در آوردن سیاستهای امنیتی دارند و بنابراین با استفاده از برخی از دیواره‌های آتش ممکن است نتوان برخی از سیاستها را به اجرا در آورد .یک دیواره آتش می‌تواند فعالیتهای

مهم را ثبت کند: به این علت که تمام ترافیک از دیواره آتش عبور می‌کند، دیواره آتش یک مکان مناسب برای ثبت مجموعه‌های مختلف از فعالیتهاست. به عنوان تنها نقطه دسترسی، دیواره آتش می‌تواند ثبت کند که چه اتفاقاتی بین شبکه محافظت شده و شبکه بیرونی رخ می‌دهند. با دسته بندی این اطلاعات می‌توان به نتایج خوبی در ارتباط با استفاده از شبکه، تهاجم‌های در حال شکل‌گیری، مزاحمان و متخلفان داخلی و خارجی و.... دست یافت .یک دیواره آتش قادر است سطوح مختلفی از امنیت را برای بخشهای مختلف پیاده‌سازی کند: از دیواره‌های آتش گاهی برای جدا نگه داشتن یک بخش از بخشهای دیگر استفاده می‌شود. این حالت زمانی اتفاق می‌افتد که یک بخش از شبکه بیشتر از بخشهای دیگرحساس باشد و نیازمند امنیت بیشتری باشد. بدین ترتیب با استفاده از دیواره‌های آتش می‌توان بخشهای مختلف با سطوح امنیتی مختلف را ایجاد نمود. این مسأله باعث می‌شود بروز مشکلات امنیتی نتواند تمام سرتاسر شبکه را تحت تأثیر قرار دهد و برخی بخشهای مهمتر و حساس‌تر مصون بمانند. دیواره‌های آتش در مجموع قادرند شبکه را در برابر تهدیدات مختلف تا حد زیادی مورد محافظت قرار دهند، اما آنها راه حل امنیتی کامل و بدون عیبی نیستند. برخی از خطرات و مشکلات از کنترل دیواره آتش خارج هستند و برای مقابله با آنها باید از روشهایی مانند ایجاد مکانیزم‌های قوی امنیت فیزیکی، " مصونیت میزبان" و آموزش کاربران و مدیران و... استفاده کرد .

7-4)ناتوانی‌های دیواره‌های آتش :

یک دیواره آتش نمی‌تواند شبکه و منابع آن را از خرابکاران داخلی محافظت‌کند: دیواره آتش ممکن است بتواند از اینکه اطلاعات مفید سازمان از طریق خط ارتباطی شبکه به بیرون انتقال یابند جلوگیری کند اما هنگامی که این اطلاعات از خط ارتباطی عبور نمی‌کنند نمی‌تواند هیچ‌کاری انجام دهد .کاربری ممکن است با استفاده از یک دیسک، Floppy، CDو یا تعدادی ورقه که آنها را در کیفش قرار می‌دهد اطلاعات حساس سازمان را به بیرون انتقال دهد .در مقابله با این نوع کاربران (که ممکن است اطلاعات داخل را عمداً و یا سهواً از روی غفلت افشا کنند)، دیواره‌های آتش ناتوان هستند و هیچ‌کاری از دستشان ساخته نیست. برخی از افراد داخلی سطوح دسترسی بالایی را در شبکه دارا هستند و مجازند به منابع مختلف در شبکه دسترسی داشته باشند، این افراد قادر خواهند بود سخت افزارها را خراب کنند، نرم افزارها و برنامه‌های مختلف را دچار مشکل‌کنند، به طور ماهرانه‌ای برنامه‌ها را تغییردهند، سطوح دسترسی‌ها را دستکاری کنند و.... واقعیت این است که دیواره‌های آتش در مقابله با این مشکلات کاری نمی‌توانند انجام دهند .یک دیواره آتش نمی‌تواند از بروز تمام مشکلات امنیتی جلوگیری‌کند: دیواره آتش برای مقابله با خطرات شناخته شده طراحی شده است. مدیران شبکه با شناختی که از حملات و خطرات مختلف دارند و با تصویب تعدادی قوانین و اجرای آنها توسط دیواره آتش سعی می‌کنند از بروز آنها جلوگیری کنند، اما واقعیت این است که روز به روز حملات و مشکلات امنیتی جدیدی به وجود می‌آیند و دیواره آتش نمی‌تواند به طور خودکار با این خطرات مقابله کند. دیواره آتش نیز مانند تجهیزات دیگر توسط مدیر سیستم پیکربندی می‌شود و پیرو دستوراتی است که مدیر می‌دهد. یک پیکربندی خوب تا حدودی

قادر خواهد بود از خطرات جدید نیز جلوگیری‌کند. در این پیکربندی هیچ ترافیکی عبور داده نمی‌شود غیر از ترافیک مربوط به تعداد بسیار اندکی سرویس مطمین. خرابکاران به طور مرتب راههای جدیدی برای نفوذ و خرابکاری پیدا می‌کنند. آنها یا از سرویسهای مطمین شناخته شده سوء استفاده می‌کنند ویا مشکلاتی که تا کنون برای کسی رخ نداده (و بنابراین هیچ کس راجع به آنها چیزی نمی‌داند و به همین دلیل در هیچ دیواره آتشی در نظر گرفته نشده) را به کار می‌بندند. یک دیواره آتش را نمی‌توان یک بار پیکربندی کرد و انتظار داشت برای همیشه شبکه را از هر خطری مورد محافظت قرار دهد .یک دیواره آتش معمولاً نمی‌تواند از ورود ویروسها جلوگیری کند: اغلب دیواره‌های آتش بخشهای مربوط به آدرس مبدأ و آدرس مقصد و شماره پورت مبدأ ومقصد شبکه‌های ورودی را مورد بازرسی قرار می‌دهند و به جزییات داده توجهی ندارند. پیاده‌سازی بخش تشخیص ویروس و بررسی کامل داده بسته‌ها در دیواره‌های آتش زیاد عملی وکارا نیست. انواع بسیار زیادی از ویروسها وجود دارند و روشهای زیادی برای آنکه ویروس خودش را در داخل داده مخفی‌کند وجود دارد. تشخیص ویروس (Virus Detection) در یک بسته تصادفی از داده‌ای که از دیواره آتش عبور می‌کند بسیار مشکل است. برای تشخیص ویروس در بسته‌ها نیازمندیهای زیر وجود دارد :

تشخیص این مطلب که بخش داده بسته بخشی از یک برنامه است .

مشخص کردن این‌که یک برنامه مجاز چگونه است و چه ویژگیهایی دارد .

تشخیص این که تفاوتی بین این برنامه و مدل برنامه‌های بدون مشکل و مجاز وجود دارد و بنابراین برنامه یک ویروس است .اغلب دیواره‌های آتش ماشینهایی از انواع مختلف و با فرمتهای اجرایی مختلف را مورد محافظت قرار می‌دهند .یک برنامه ممکن است یک برنامه کامپایل شده قابل اجرا و یا یک script باشد .علاوه بر این، بسیاری از برنامه‌ها قبل از اینکه انتقال یابند به شکل یک Packageدر می‌آیند و به خوبی فشرده سازی می‌شوند. این مسایل باعث می‌شود پیچیدگی مسأله تشخیص ویروسها بالاتر رود و پیاده‌سازی آن مشکل باشد. با این همه باز هم نمی‌توان تمامی منابع دیگر انتقال ویروسها را کنترل کرد .بسیاری از برنامه‌ها ممکن است از طریق مودمهای اشخاصی که به اینترنت متصلند و از دیواره آتش رد نمی شوند download شوند و یا با یک floppyاز محل سکونت به شبکه داخلی سازمان انتقال یابند و ... روش عملی تر مقابله با ویروسها استفاده از نرم افزارهای host-base virus protection[89] است. آموزش کاربران و آگاه کردن آنها از خطرات ویروسها نیز می تواند مؤثر باشددر نتیجه بهترین پیشنهاد استفاده همزمان از هر دونوع دیوار آتش است. شبکه های متعلق به سازمانها یا موسسات تجاری در دو بخش سازماندهی و پیکربندی میشوند:

[89] میزبان پایگاه-آنتی ویروس

-بخش عمومی شبکه شامل سرویس دهنده وب ، پست الکترونیکی و FTP که به عموم کاربران اینترنت سرویس میدهد. این بخش اصطلاحا DMZ (بخش غیر محرمانه غیر نظامی!) نام دارد.

-بخش خصوصی یا محرمانه که صرفا با هدف سرویس دهی به اعضای آن سازمانیا موسسه پیاده سازی شده است.بخش عمومی شبکه توسط یک فیلتر (معمولی یا هوشنمد) حفاظت میشود تا از کارایی سرویس دهنده آن کاسته نشود. شبکه داخلی در پشت یک دیوار آتش مبتنی بر پراکسی پنهان میشود تا ضمن غیر قابل نفوذ بودن با اینترنت در ارتباط باشد. در چنین ساختاری یک نفوذگر خارجی برای برقراری ارتباط بایک ماشین داخلی دو مانع عمده بر سر راه دارد: فیلتر و دیوار آتش مبتنی بر پراکسی. حال حتی اگر بتواند با مکانیزم های متداول از سد فیلتر بگذرد پشت دیوار آتش متوقف خواهد شد

8-4)دفاع لایه ای

. بهترین محصولات مربوط به ایمن سازی اطلاعات دارای نقاط ضعف ذاتی ، مربوط به خود می باشند.بنابراین همواره زمان لازم در اختیار مهاجمان اطلاعاتی برای نفوذ در سیستم های اطلاعاتی وجود خواهد داشت.بدین ترتیب لازم است قبل از سوءاستفاده اطلاعاتی متجاوزان، اقدامات مناسبی صورت پذیرد .یکی از روش های موثرپیشگیری در این خصوص ، استفاده از دفاع لایه ای در مکان های بین مهاجمان و اهداف مورد نظر آنان ،می باشد . هریک از مکانیزم های انتخابی ، می بایست قادر به ایجاد موانع لازم در ارتباط با مهاجمان اطلاعاتی (حفاظت)وتشخیص بموقع حملات باشد . بدین ترتیب امکان تشخیص مهاجمان اطلاعاتی افزایش و از طرف دیگر شانس آنها بمنظور نفوذ در سیستم و کسب موفقیت، کاهش خواهد یافت

استفاده از فایروال های تودرتو : هر فایروال در کنار خوداز یک سیستم تشخیص مزاحمین ، نیز استفاده می نماید(در محدوده های داخلی و خارجی شبکه ، نمونه ای از رویکرد دفاع لایه ای است . فایروال های داخلی ممکن است امکانات بیشتری را در رابطه با فیلتر سازی داده ها و کنترل دستیابی به منابع موجود ارائه نمایند.تعیین میزان اقتدار امنیتی هر یک از عناصر موجود در ایمن سازی اطلاعات(چه چیزی حفاظت شده و نحوه برخورد با تهاجم اطلاعاتی در محلی که از عنصر مربوطه استفاده شده ، به چه صورت است ؟(.پس از سنجش میزان اقتدار امنیتی هر یک از عناصر مربوطه ، می توان از آنان در جایگاهی که دارای حداکثر کارآئی باشند ، استفاده کرد . مثلا" می بایست از مکانیزم های امنیتی مقتدر در محدوده های مرزی شبکه استفاده گردد .استفاده از مدیریت کلید مقتدر و زیر ساخت کلید عمومی، که قادر به حمایت از تمام تکنولوژی های مرتبط با ایمن سازی اطلاعات بوده و دارای مقاومت مطلوب در مقابل یک تهاجم اطلاعاتی باشد.

راهکارهای هدفمند کردن وبهبودی فایروال

استفاده از دیوارهای آتش (فایروال) مبتنی بر میزبان

به نظر می‌رسد به فایروال های سخت افزاری که درون شبکه نصب می شوند، توجه بسیاری می‌شود. بسیاری آنها را مدافعانی با قدرت های جادویی می دانند. اما امروزه در عمل بیشتر دیوارهای آتش امنیت به مراتب کمتری کمتر از آن چیزی است که باید باشد. به عبارت دیگر، در ظاهر دیواره آتش بخش بزرگی از امنیت است. اما از آن نقشی که قرار است در امنیت شبکه شما بازی کند، سهم بسیار کمتری را بر عهده دارد. یکی از دلایل این موضوع این است که بیشتر حملات شدید اغلب از داخل شبکه حادث می‌شود، بنابراین وظیفه دیوار آتش در جلوگیری از کاربران بیرونی برای دسترسی به منابع داخلی شبکه بازده کمی دارد.در مقابل، «دیوار آتش مبتنی بر سیستم میزبان» قادر به حفاظت کامپیوتر از تمام حملات داخلی و خارجی می‌باشد. علاوه بر این، دیوارهای آتش مبتنی بر میزبانِ حرفه ای می توانند به شکلی پیکربندی شوند تا امکان ارتباطات ورودی را تنها برای سرویس‌های مشخصی فراهم نمایند.

این دیوارهای آتش مبتنی بر میزبان مانند (Windows Firewall with Advanced Security[90])حتی می توانند کاربران یا ماشین‌ها را ملزم به تایید هویت در لایه شبکه نماید، به طوری که اگر کاربری معتبر شناخته نشود یا اختیارات لازم را نداشته باشد، هرگز به نزدیکی لایه اپلیکیشن نرسد – لایه اپلیکیشن، لایه‌ایی است که اغلب رخنه‌های امنیتی در آنجا بوده و داده‌های شما تماما در آنجا قرار دارد

2-9-4)استقرار فایروال بین روتر داخلی و خارجی :یک سطح امنیتی اضافه اندک به منظور حفاظت در مقابل حملات در هر سمت را ارائه می نماید . این کار میزان ترافیکی را که فایروال می بایست بررسی نماید بطرز محسوسی کاهش داده و متعاقب آن کارآئی فایروال افزایش خواهد یافت چون ایجاد امنیت از سازمانی به سازمان دیگر متفاوت است والبته این بستگی به چیزی دارد که آنها می خواهند توسعه دهند.در این صورت باید بستر اجرایی موردنظر راپیدا کنیم.سطوح امنیت را مشخص کنیم.به جای محدود کردن serverیک serverرابا تمام دسترسی های ممکن به اینترنت وصل کنیم.وسرور دیگر را پشت فایروال به عنوان back upازسرور قبلی داشته باشیم.که با هک شدن یا خرابی سرور اولی ما می توانیم آن را بازیابی کنیم.در فایروال های مبتنی برمیزبان غربال سازی هنگام نیاز وافزودن ضابطه ممانعت بهtcp wrapper[91].مشخص کردن فایروال موردنیاز.

---

[90] فایروال ویندوز با امنیت پیشرفته

[91] پوشش

3-9-4) چند راهکار طبقه بندی شده برای بهبود فایروال

1-آدرس های ip :به هر دستگاه در اینترنت یک آدرس منحصر به فردبه نام آدرسipاختصاص داده می شودکه32بیتی هستندومعمولابه صورت4بایت به شکل اعداددهدهی نقطه دار بیان می شوندومی توانند تمام ترافیک از یابه آن آدرسipرامسدودنمایند.

2-نام های دامنه:چون یادآوری اعدادآدرسip سخت است وگاهی نیاز به تغییردارند،تمام سرورها در اینترنت دارای نام های قابل خواندن توسط بشر به نام نام های دامنه(domain names)هستند.

3-پروتکل ها(protocol):پروتکل روش از پیش تعیین شده است وکسی(browser) که می خواهد از سرویسی استفاده کند توسط آن با آن صحبت می کند.پروتکل ها غالبا متن هستندوبه سادگی توصیف می کنند که سرویس دهنده وسرویس گیرنده مکالماتشان را چگونه خواهند داشت.انواع پروتکل عبارتند از:(ip-snmp[92]-smtp[93]-ftp-udp-icmp[94]-http-tcp)

4-پورت ها(port):هر دستگاه سرور،سرویس هایش رادر اینترنت با استفاده از پورت های شماره گذاری شده،یک پورت برای هرسرویس که درسرور موجود است،فراهم می سازد.

5-کلمات وعبارات خاص:این می تواند هرچیزی باشد.فایروال هر بسته از اطلاعات را برای جستجوی دقیق متنی که فیلتر شده جستجو می کند.

6-پیکر بندی مناسب وبهینه فایروال

محصولات فایروال تجاری(هم سخت افزاری و هم نرم افزاری) دارای امکانات متعددی بمنظور پیکربندی بهینه می باشند.با توجه به تنوع بسیار زیاد فایروال ، می بایست به منظور پیکربندی بهینه آنان به مستندات ارائه شده،مراجعه تا مشخص گردد که آیا تنظیمات پیش فرض فایروال نیاز شما را تامین می نماید یا خیر ؟ پس از پیکربندی یک فایروال یک سطح امنیتی و حفاظتی مناسب در خصوص ایمن سازی اطلاعات انجام شده است.لازم است به این موضوع مهم اشاره گردد که پس از پیکربندی یک فایروال نمی بایست بر این باور باشیم که سیستم ما همواره ایمن خواهد بود.فایروال یک سطح مطلوب حفاظتی را ارائه می نماید ولی هرگز عدم تهاجم به سیستم شما را تضمین ایمنی می تواند یک سطح مطلوب حفاظتی را برای شما و شبکه شما بدنبال داشته باشد.

---

[92] -Simple Network Management Protocol پروتکل مدیریت شبکه ساده

[93] Simple Mail Transfer Protocol -پروتکل انتقال ساده پست الکترونیکی

[94] The Internet Control Message Protocol-پروتکل کنترل پیام‌های اینترنتی

7-نحوه ی انتخاب یک فایروال مناسب

8-نصب dmz:ناحیه ای است که بیرون فایروال قرار داردوبین اتصال به اینترنت وفایروال قرار میگیرد وامکان دسترسی غیر مجاز را کم می کند.

9-استفاده از proxy server:برای دسترسی به صفحات وب به وسیله کامپیوترهای دیگر استفاده می شود.ووقتی تقاضای یک صفحه وب را می کنیم آن صفحه توسط سرور پروکسی دریافت شده وبه کامپیوتر متقاضی ارسال می شود.که باعث عملکرد موثرتر در دسترسی ما به اینترنت می شوند.

10-استفاده از آنتی ویروس وآنتی اسپم ها در کنار بسته فایروال

11-مقابله با روت کیت:استفاده از نرم افزارهای امنیتی قدرتمند که که بتواند به صورت دائم فایل های مهم سیستمی را رصد کند، می توانیم با خیال آسوده تری به کار ادامه دهیم در واقع این برنامه ها، فعالیت های لایه‌ی سیستم عامل را با لایه های پایین تر مقایسه می کنند و در صورتی که متوجه تغییرات مشکوک شوند، با دقت بیشتری آن ها را بررسی خواهند کرد تا علت آنها مشخص شده و روتکیت را به دام بیاندازند. یکی ا ز اولین روشها برای ریشه یابی روت کیتها بوت کردن سیستم به یک سیستم عامل پاک از طریق یک س ی دی، گرفتن یک فهرست دیرکتوری از همهٔ فایلهای روی سیستم، و سپس مقایسه آن با یک فهرست مشابه تولید شده از داخل سیستم عامل مورد ریشه یابی است . اگر دو فهرست مختلف باشند، فایل های حذف شده از فهرست سیستم عامل مورد ریشه یابی، شک برانگیز است. اجرای این کار به طور دستی بسیار دشوار است. در نتیجه، برنامه هایی برای خودکارسازی این عملیات ساخته شده است . مشهورترین آنها برنامه ((Rootkit Revealer)) است.

12-اسکن ترافیک داخل وخارج رایانه

13-استفاده از تکنیک hauri برای انتی ویروس های عرضه شده به همراه فایروال برای تشخیص ویروس وهرزه نامه ها : در این تکنیک ویروس ها شناسایی و REPAIR [95]می شوند و آنتی ویروس را به 3 قسمت برای ماکرو، اسکریپت و ویندوز تقسیم می کند.همچنین INBOX را نیز جستجو و هرز نامه ها را از بین می برد.

14-استفاده از تکنیک هایی برای مخفی ماندن کاربر از دید کاربران شبکه اینترنت

15-استفاده از فایروال های چند لایه که اگرلایه اول ناتوان ماند وتشخیصی نداد لایه های بعدی بتوانند جلوگیری کرده ومحافظت کنند

[95] تعمیر

16-اتخاذ روشهایی برای عملکرد سریع وبه موقع سیاست های امنیتی فایروال

17-متوقف کردن هر کسی در بیرون از متصل شدن به کامپیوتر در شبکه خصوصی

18-استفاده از فایروال هایی که هنگام نفوذ سودجویان اخطار دهد وipشخص نفوذکننده را نشان دهد.

19-استفاده از فایروالهای تودرتو

20-استفاده از سیستم تشخیص نفوذبه همراه فایروال

21-افزودن لایه های مختلف به آنتی ویروس

22-استفاده ازسیستم عامل های جداگانه که باعث مخفی ماندن کاربرازدید کاربران شبکه اینترنت می شود

23-بکارگیری هانی پات

24-رمزنگاری:بهم ریختگی اطلاعات طوری که برای افراد غیرمجاز قابل فهم نباشد

10-4)نتیجه گیری این فصل:

مزایا ومعایب فایروال بیان شدوچندین راهکار برای ان بیان شد استفاده از این راهکارها تجربه استفاده ایمن از شبکه اینترنت را بدون ورود غیرمجاز کاربران سودجو وبرنامه های مخرب فراهم می سازد. یکی از مهم ترین مواردی که در بهبود فایروال ها به آن اشاره کردیم استفاده از آنتی ویروس وآنتی اسپم به همراه فایرول است که امنیت را تضمین می کند.واز ورود برنامه ها ی مخرب وکاربران غیرمجاز جلوگیری کرده وبا دادن هشدار مارا آگاه می سازد.

فصل پنجم

1-5)مقدمه فصل پنجم:

دراین فصل به معرفی ونحوه عملکرد هانی پات وuml [96]می پردازیم

هانی پات یک منبع سیستم اطلاعاتی می باشد که بر روی خود اطلاعات کاذب و غیر واقعی دارد

UTM عبارتست از سیستم مدیریت یکپارچه تهدیدات، شامل مجموعه ای کامل و جامع از تمامی راهکارها

هردوی این منابع به نوعی می توان چایگزین یا کمکی برای امنیت بیشتر فایروال دانست

[96] Unified Modeling Language- زبان مدل سازی یکپارچه

HONEY POT(2-5

هانی پات یک منبع سیستم اطلاعاتی می باشد که بر روی خود اطلاعات کاذب و غیر واقعی دارد و با استفاده از ارزش و اطلاعات کاذب خود سعی می کند فعالیت های غیر مجاز و غیرقانونی بر روی شبکه را کشف و جمع آوری کند.به زبان ساده هانی پات یک سیستم یا سیستم های کامپیوتری متصل به شبکه و یا اینترنت است که دارای اطلاعات کاذب بر روی خود می باشد . از عمد در شبکه قرار می گیرد تا به عنوان یه تله عمل کرده و مورد تهاجم یک هکر یا نفوذگر قرار بگیرد.با استفاده از این اطلاعات آنها را فریب داده و اطلاعاتی از نحوه ورود آنها به شبکه و اهدافی که در شبکه دنبال می کنند. هانی پات ها به دو دلیل استفاده می شوند: اول اینکه نقاط ضعف سیستم را بشناسیم، دلیل دوم جمع آوری اطلاعات لازم برای تعقیب و ردگیری نفوذگران است.

1-2-5)نحوه کار HONEY POT

هانی پات مشابه یک سیستم قربانی در برابر نفوذ ظاهر می شوند و مانند یک چنین سیستمی بایستی رفتار کنند اما در عین حال بدون آگاه نمودن نفوذگر با انواع روش های کنترلی و ثبت و ظبط داده خود او را تحت نظر دارند.این اطلاعات ثبت شده و بعدا جهت آنالیز می توانند مورد استفاده قرار گیرند و از آنها برای یادگیری روش های ناشناخته حملات و نفوذها بهره برد. فرق آن با سایر سیستم ها و فناوری های امنیتی مشابه در عملکرد سریعتر و بهینه آن است.قرار نیست تا دوباره سناریو های فایروال و سیستم های تشخیص نفوذ متدوال را تکرار کنیم. همگی این روش ها به دلیل حجم داده تولیدی بالا و غیر صحیح ناکارآمد به حساب می آیند.هانی پات مانند یک سیستم تدافعی عمل نمی کنند یعنی منتظر پیش قدم شدن نفوذگر در شروع حمله نمی ماند. بلکه سعی در جمع آوری اطلاعات در مورد سبک ها و فنون آنها دارد.هانی پات مانند فایروال تنها به شناسایی حملات شناخته شده محدود نیست ئ این ویژگی یک هانی پات است که روش های نفوذ جدید را کشف می کند.

2-2-5)مزیت های یک هانی پات

هانی پات اطلاعات کمی را جمع آوری می کند و در واقع به جای اینکه مانند خیلی از ابزار های امنیتی 1 گیگ داده را در روز LOG کند به مقادیر بسیار کمتر از 1 مگابایت و به جای 10000 اخطار روزانه به 10 تا بسنده می کند.در واقع هانی پات تنها فعالیت های مشکوک را ضبط می کند،بنابراین با جمع آوری داده ها در اندازه کمتر پارازیت را کاهش داده ولی در عوض ارزش آن داده بالاست.

2. هانی پات ها طوری طراحی می گردند که می توانند هر چیزی را شامل ابزار ها و تاکتیک های جدید که نفوذگر به کار می برد و هرگز قبلا دیده نشده اند به دام بیندازد

3. هانی پات ها برای فعالیت به حداقل منابع نیازمندند، یعنی با یک کامپیوتر Pentium پایین و حد اقل Ram 128 قادرند با شبکه کلاس B با OC-12 به خوبی کار کنند.

4. بر خلاف بسیاری از تکنولوژی مانندIDS [۹۷]، هانی پات ها به خوبی با محیط رمزنگاری شده یا هانی پات ها به خوبی با محیط های رمز نگاری شده با IPV6 [۹۸]کار می کنند.

5. هانی پات ها از لحاظ مفهومی بسیار ساده هستنددر آنها از الگوریتم های پیچیده و نگهداری جداول حالت و یا آپدیت Signatures [۹۹]خبری نیست . هرچه تکنولوژی ساده تر و آسانتر باشد کمتر دچار خطا خواهد شد.

3-2-5)معایب هانی پات

دید محدود : هانی پات ها تنها می توانند تحرکاتی را دنبال و شناسایی کنند که مستقیما با خودشان درگیر گردند.به عبارتی قادر نیستند حملات به سایر سیستم ها را گیر بیندازند تا زمانی که نفوذگر با خود هانی پات وارد رویارویی نشود

ریسک:هر تکنولوژی امنیتی با ریسک همراه است.در مورد فایروال چون ممکن است به داخل آنها رخنه شود رمزنگاری ممکن است شکسته شود.حسگرها IDS در شناسایی حمله ای ممکن است Fail شود، هانی پات ها هم از این قاعده مستثنا نیستند.علاوه بر اینکه این خطر هم وجود دارد که حتی به عنوان ابزاری توسط نفوذگر جهت خرابی به کار گرفته بشود.البته انواع هانی پات ها درجات ریسک پذیری متفاوتی دارند.

3-5) (Unified Threat management) UTMچیست؟

UTM عبارتست از سیستم مدیریت یکپارچه تهدیدات، شامل مجموعه ای کامل و جامع از تمامی راهکارهای امنیتی

برقراری دیوار آتش – Identity Based Firewall:

ایجاد شبکه خصوصی مجازی – Virtual Private NetworkVPN

---

[97] سامانه‌های تشخیص نفوذ (Intrusion Detection System) وظیفهٔ شناسایی و تشخیص هر گونه استفادهٔ غیرمجاز به سیستم، سوء استفاده و یا آسیب رسانی توسط هر دو دستهٔ کاربران داخلی و خارجی را بر عهده دارند.

[98] پروتکل اینترنت نسخه ٦ (به انگلیسی: Internet Protocol version 6) یا به اختصار IPv6

[99] امضا

ضدویروس – Anti-Virus

ضدهرزنامه – Anti-Spam

شناسایی و جلوگیری از نفوذگران – Intrusion Detection and Prevention

فیلترینگ محتوی – Content Filtering

مدیریت پهنای باند – Bandwidth management

ضد جاسوس افزار، ضد برنامه‌های کلاهبرداریAnti-Spyware/Anti-Phishing/AntiPharming

تاریخچه‌ای پیرامون UTM

اولین ویرایش‌های سیستم مدیریت یکپارچه تهدیدات با نامUTM ، از اوایل سال 2003 ایجاد شده است. با توجه به بررسی‌های انجام گرفته اولین محصول UTM توسط شرکت ServGate به بازار ارائه شده است. از آن زمان تاکنون شرکتهای بسیاری وارد این عرصه شده‌اند که بعضا محصول خود را به صورت نرم افزاری و بعضا همراه با سخت افزار ارائه می‌نمایند.

راهکار استفاده از UTM در مواجهه با حملات روز افزون علیه سیستم‌های اطلاعاتی سازمان‌ها از طریق هک، ویروس‌ها، کرم امنیتی (ترکیبی از حملات و تحدیدهای خارجی و داخلی) ضروری به نظر می‌رسد. به علاوه تکنیک‌هایی که کاربران سازمان‌ها را به عنوان لینک‌های ارتباطی ضعیف مورد هدف قرار می‌دهند، عواقبی فراتر از حد تصور در پی دارند. در حال حاضر امنیت داده‌ها و دسترسی غیر مجاز کارمندان به عمده‌ترین نگرانی شرکت‌ها تبدیل شده‌است. به این دلیل هدف‌های مخرب و از دست رفتن اطلاعات منجر به ضررهای زیاد مالی برای شرکت‌ها شده‌است. اصولا این دستگاه‌های از فناوری ASIC[100] سخت افزاری استفاده می‌کنند تا بالاترین performanceرا داشته باشند.

1-3-5)مزایای UTM

امکان مدیریت واحد و مجتمع جهت: – فیلترینگ براساس محتوی – کنترل ویروس‌ها و هرزنامه‌ها – دیوار آتشین و ایجاد شبکه‌های خصوصی مجازی – امکان نصب آسان در شبکه – بهره گیری از سیستم‌های دفاعی جهت واکنش سریع و بلادرنگ به هرگونه تهدید شبکه ای – مقرون به صرفه بودن از لحاظ اقتصادی و کم

[100] مدارهای مجتمع با کاربرد خاص (به انگلیسی : Application-specific integrated circuit) (به اختصار ASIC یا ایسیک) مدارهای مجتمعی هستند که به منظور انجام عملیات خاص، طراحی و بهینه سازی شده‌اند

بودن هزینه‌های نصب و نگهداری سیستم – بالا بردن بهره وری شبکه – امکان کنترل متمرکز – ایجاد محیط امن و سالم در شبکه – توانایی بالا در گزارش گیری و ارائه گزارشات متنوع به مدیر شبکه

2-3-5)وظایف امنیتی

دیواره آتش، جلوگیری از نفوذ، ضد ویروس، ضد هرز نامه، شبکه اختصاصی مجازی، فیلترینگ محتوا، گزارش گیری و ... بازار سیستم مدیریت یکپارچه تهدیدات در سراسر جهان به ارزش حدود ۱,۲ میلیارد دلار در سال ۲۰۰۷ رسید و پیش بینی می‌شود تا سال ۲۰۱۱ نرخ رشد سالانه ۳۵ تا ٤٠ درصدی داشته باشد. واژه سیستم مدیریت یکپارچه در اصل توسط شرکت IDC که شرکت پژوهش بازار است ابداع شد. مزایای امنیت یکپارچه در این نهفته شده‌است که در حقیقت بجای اجرای سیستم‌های متعدد که به صورت جداگانه هر کدام سرویس‌های مختلفی را ارائه دهند (آنتی ویروس، فیلترینگ محتوا، جلوگیری از نفوذ و توابع فیلتر کردن هرزنامه) یک دستگاه تمامی این سرویس‌ها را به صورت یکپارچه ارائه دهد. سازمان‌ها با استفاده از دستگاه‌های UTMدارای انعطاف پذیری بیشتری هستند. از مزیت‌های اصلی UTM می‌توان به سادگی، نصب و استفاده کارآمد و توانایی به روز رسانی تمامی توابع امنیتی اشاره کرد.

4-3-5)سرویس‌های امنیتی تشکیل دهنده UTM

از آنجایی که یک محصول UTM تعداد زیادی سرویس امنیتی را در درون خود بکارگیری می‌کند، لذا حجم زیادی از توان پردازنده و حافظه را به خود اختصاص می‌دهد، و شرکت‌های معتبر تولید کنندهUTM ، از سخت‌افزارهای قوی و بکارگیری تکنیک‌های مختلف سخت‌افزاری و نرم‌افزاری در جهت افزایش Performanceسیستم‌های خود استفاده می‌کنند Performance Acceleration .به منظور افزایش کارایی یک سامانه UTM اجرا می‌شود، به این منظور معمولاً فعالیت بخش‌هایی از سیستم که نیاز به حجم پردازنده بالایی دارد را به سخت‌افزار واگذار می‌کنند؛ به طور مثال بجای استفاده از VPN و یا IPS نرم‌افزاری از نمونه‌های معادل آن که به صورت سخت‌افزاری تولید شده‌اند، استفاده می‌شود. به این ترتیب هر سرویس امنیتی به صورت یک کارت سخت‌افزاری طراحی و در سامانه UTM مورد استفاده قرار گرفته و کارایی را فوق‌العاده افزایش می‌دهد.

تفاوت UTM و Firewall

فایروال Firewall در ساده ترین حالت ممکن وسیله ای است که می تواند تعیین کند که ترافیک از یک پورت یا IP به سایر پورت ها و یا IP ها یا ترکیبی از ایندو که سوکت Socket نامیده می شود باز باشد یا بسته باشد . بعضی از اینگونه فایروال ها می توانند با دارا بودن قابلیت Statefull Inspection کمی ترافیک مربوط به پروتکل TCP را مانیتور کنند ولی معمولا هیچ فایروالی توانایی واکاوی و جستجو در داخل بسته ها را ندارد . صرفا همان عملیات بلاک کردن را انجام می دهد . اما UTM که مخفف کلمه Unified Threat Management یا سیستم یکپارچه مدیریت تهدیدات هست با نگاهی عمیقتر به مسئله مانیتور کردن داخل بسته ها یا همان Packet ها نگاه کرده است و توانایی ویژه ای در مانیتور کردن Packet ها بویژه در لایه های 5 و 6 و 7 از مدل OSI دارد

6-5)آنتی فیلتر چیست ؟

آنتی فیلتر هایی که به صورت معمول برای رد شدن از فایروال ها استفاده می شوند مبتنی بر سرور های PROXY می باشند . در این حالت که بیشتر برای دریافت HTTP استفاده می شود درخواست کننده آدرس خود را به سرور PROXY می فرستد سرور صفحه را لود کرده و سپس به صورت رمزنگاری شده به درخواست کننده می فرستد.یک فایروال که به طور مثال برای بستن واژه (ترور) پیکر بندی شده است دیگر قادر به یافتن چنین واژه ای در صفحه وبی که در خواست شده نمی باشد.سایت های مختلفی اقدام به ارائه نمودن چنین سرویسی به افراد می نمایند که هر کدام بنا به علل مختلفی چون تبلیغات اقدام به اختصاص FREE PROXY برای افراد می کنند.

9-5)نتیجه فصل پنجم:

کاروعملکرد هانی پات وUMLبسیارشبیه به فایروال بوده وعملا کمک شایانی به فناوری فایروال می کنند

ودرصورت مشکل یافتن فایروال می توان ازآنها بعنوان جایگزینی مناسب استفاده کرد ودرگاهی موارد می توان آنها را درکنارفایروال قرارداد وکارایی فایروال را نیز بهبود بخشید.

فصل ششم

1-6)مقدمه فصل ششم

این فصل درواقع فصل پایانی ونتیجه گیری ازکل مباحثی است که تاکنون مطرح شده دراین فصل نتیجه گیری خلاصه ای ازتمام مطالب چکیده به انگلیسی ومنابع وجود دارد .

دراین پایان نامه تلاش کردم تا به طور کامل فایروال انواعش مزایا معایب رابررسی کرده راهکارهایی برای بهبودیش معرفی کنم ونرم افزارهای کمکی وجایگزینی احتمالی را بررسی کنم وامیدوارم مفید واقع شود.

2-6)نتیجه گیری کل

درحالت کلی فایروال سخت افزاریانرم افزاری برای حفاظت شبکه های کامپیوتری وسیستم ها از دسترس افرادغیرمجاز وخرابکاریا انواع حملات وویروس ها می باشد . مزایا ومعایب فایروال بیان شدوچندین راهکار برای ان بیان شد استفاده از این راهکارها تجربه استفاده ایمن از شبکه اینترنت را بدون ورود غیرمجاز کاربران سودجو وبرنامه های مخرب فراهم می سازد. یکی از مهم ترین مواردی که در بهبود فایروال ها به آن اشاره کردیم استفاده از آنتی ویروس وآنتی اسپم به همراه فایرول است که امنیت را تضمین می کند.واز ورود برنامه ها ی مخرب وکاربران غیرمجاز جلوگیری کرده وبا دادن هشدار مارا آگاه می شود.قبل از نصب فایروال سیستم خود را اسکن کرده تا بتوانیم از آن در مقابل ویروس ها محافظت کنیم.ادرس وشماره ipسیستم خود را بدانیم وآن را به لیست میزبان های قابل اعتماددر فایروال خود اضافه کنیم.با حدس وگمان عمل نکنیم.بعد از نصب فایروال آن را کاملا آزمایش کنیم ودر صورت وجود نقص نسبت به بهبود آن واستفاده از یکی از روشهای ذکر شده اقدام نماییم تا به طور ایمن از شبکه اینترنت استفاده کنیم.امروزه از اینترنت در ابعاد گسترده و با اهدافی مختلف استفاده بعمل می آید . یکی از نکات قابل توجه اینترنت ، تنوع استفاده کنندگان آن در رده های سنی مختلف و مشاغل گوناگون است. در سالیان اخیر و به موازات رشد چشمگیر استفاده از اینترنت خصوصا" توسط کاربران خانگی ، مشاهده شده است به محض شیوع یک ویروس و یا کرم جدید ، اغلب قربانیان را کاربرانی تشکیل می دهند که فاقد مهارت های لازم در جهت استفاده ایمن از اینترنت بوده و دارای یک سطح حفاظتی مناسب نمی باشند . کاربران اینترنت همواره در تیررس مهاجمان بوده و همیشه امکان بروز حملات وجود خواهد داشت .برای استفاده ایمن از اینترنت ، می بایست اقدامات متعددی را انجام داد . قطعا" استفاده از فایروال یکی از اقدامات اولیه و در عین حال بسیار مهم در این زمینه است .استفاده از اینترنت بدون بکارگیری یک فایروال ، نظیر بازنگهداشتن درب ورودی یک ساختمان است که هر لحظه ممکن است افراد غیرمجاز از فرصت ایجاد شده برای ورود به ساختمان استفاده نمایند . با نصب و استفاده از یک فایروال ، ضریب مقاومت و ایمنی کاربران در مقابل انواع حملات افزایش خواهد یافت.

3-6)Abstract

Firewall is a network security Rabnabrsyasthay define network access control network Myknd.vsystm Raaznfvz Vhkrhay unauthorized users protect programs. A firewall is one of the security layers of computer networks. Azfayrval advantage is that we have a secure network system. One of the most effective and important way to implement fire walls "safety net" and are capable of a lot of internal resources to prevent unauthorized access to the outside world. However, a firewall is able to raise the level of network security to do useful work.

فهرست منابع:

الف) **مقالات**: حسن نشاطی (firewall) در98صفحه دانلودکرده از سایت (alirezaweb.com)مقاله ابزارهای امنیتی (علی جودکی ،اذر87 زیرنظراستادافشه) قره گوزی.علیرضا.1389.بررسی نقش دیواره آتش درامنیت شبکه های کامپیوتری.کنفرانس ملی امنیت اطلاعات وارتباطات.اهواز.جهاددانشگاهی خوزستان

ب) **پایان‌نامه‌ها**:رضا قنبرزاده(بهار1390،فایروال،زیرنظر مهندس عقیقی ،مرکز آموزش علمی –کاربردی قوچان،گروهit) سعیدایرانشاهی (بهار 20/1/1393مرکز اموزش علمی کاربردی داده پردازی ایران با عنوان امنیت شبکه)

ج) **منابع الکترونیکی**: سایت (www.prozhe.com) در تاریخ 9/1/1393ودانلود مقاله فایروال .سایت (www.alirezaweb.com)سایت (www.srco.ir)گرفته شده از منبع مایکروسافت .سایت (www.amozesh-c.blogfa.com)در تاریخ 91/3/3 این مقاله فایروال چیست را منتشر کرده تاریخ مراجعه 1392/12/17برگرفته از سایتwww.ircert.com

http://www.us-cert.gov/وhttp://howstuffworks.com– نویسنده : محمد نصیری انجمن تخصصی فناوری اطلاعات ایرانmeta-guard : www.MakeUseOf.com..

انجمن پی سی ورلد

security.itpro.ir

د)**کتابها**:Fundamental firewall 2011

Network security architectures

میوالد. اریک. امنیت شبکه های کامپیوتری. ترجمه سید احمد صفایی.چاپ اول تهران:نشر دانش پرور

مهندسی اینترنت تالیف عباسعلی رضایی انتشارات پیام نور