آموزش ترفندهای ویندوز در کلیپ‌های کوتاه

دانشگاه مدیریت و فناوری امیرکبیر

موضوع : سخت افزارهای دیتا سنتر

شهره لیثی بهرمانی

بهار ۱۳۹۳

چکیده

در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها درMIT ، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار گردید. امنیت اطلاعات باید در سه بخش مبدا ، مسیر انتقال پیام و مقصد مورد بررسی قرار بگیرد. دستیابی به اطلاعات با روش های مطمئن و با سرعت و امنیت بالا یکی از رموز موفقیت هر سازمان و موسسه است.

برای راه اندازی یک اتاق سرور و ارتباط آن با خارج از محیط و امنیت آن مستلزم استفاده از سخت افزار های شبکه هستیم .

کامپیوتر ،سوییچ ، روتر ، سرور ، فایروال و کابل های شبکه اجزای اصلی سخت افزار یک شبکه کامپیوتری را تشکیل می دهند.

هر کدام از این سخت افزار ها بسته به نوع شرکت سازنده و پروتکل ها ، امنیت منحصر به فردی دارند در این پایان نامه سعی شده است که این سخت افزار ها را با هم مقایسه کنیم و نقاط ضعف و قوت آنها را از نظر امنیتی توضیح دهیم.

هرسازمان و موسسه ای یک روز ناگزیر است که مکانی بنام دیتا سنتر برای خود ایجاد ، دیتا سنتر ها مهمترین بخش در یک موسسه یا سازمان هستند که تجهیزات شبکه را در خود جای میدهند وباید تحت امنیت زیادی باشند . برای طراحی و امنیت دیتا سنترها باید به موضوعات زیر توجه کرد : ابعاد ساختمان و محل قرار گیری دیتا سنتر و تعمیر و تغییرات عمرانی ، تامین برق و استفاده از upsها ، سامانه اطفاء حریق ، سامانه های امنیتی مانند : دوربین های مدار بسته و حسگر حضور فیزیکی، دیوار پوش ، کف کاذب ، سقف کاذب ، کانالهای تهویه و ... که در این پایان نامه به صورت مفصل بحث می شوند.

وقتی صحبت از امنیت شبکه می شود جنبه های مختلفی را شامل می شود که یکی از مهمترین این مو ضوع ها جنبه ی سخت افزاری امنیت است وجلوگیری از نفوظ هکر ها به سخت افزار یکی از دغدغه های ، طراحان و مدیران شبکه می باشد وسعی بر این است که بالاترین سطح امنیت را به کار ببرند. هدف از این پروژه بررسی و مقایسه روش های تامین امنیت شبکه های کامپیوتری با تکیه بر امنیت سخت افزاری است ، که تا حد امکان موجب بالارفتن امنیت در شبکه های lan , man , wan از لحاظ سخت افزاری می شود.

فهرست مطالب

عنوان **صفحه**

فصل اول : معرفی دیتا سنتر و استاندارد آن

فصل دوم : ایجاد دیتا سنتر و امنیت فیزیکی آن

فصل سوم : تجهیزات شبکه و بررسی آن ها

منابع

فهرست اشکال

عنوان **صفحه**

پیشگفتار

فراهم نمودن امنیت یکی از اساسی ترین ملزومات مخابره داده می باشد و ، با گسترش روز افزون شبکه ها جایگاه ویژه ای پیدا کرده است .امنیت در قالب کارکردهایی چون : محرمانگی ، جامعیت پیام، احراز اصالت ، انکار ناپذیری ودر دسترس بودن تعریف می شود.

امنیت شبکه به طور کلی برای فراهم کردن امکان حفاظت از مرزهای یک سازمان در برابر نفوذگران (مانند هکرها) به کار می رود.

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

هر رویدادی از ابتدا در سطح فیزیکی آن آغاز می شود. به علاوه زمانی که به امنیت فناوری اطلاعات مربوط شود.

با توجه به رشد فناوری اطلاعات در کشور ، ما شاهد گسترش و بزرگ شدن هر روزه اتاق های سرور ور افزایش تعداد سرورها و سرویس های مستقر در آن هستیم و گاهی این گسترش به حدی میرسد که دیگر یک فضای معمولی جوابگوی نیازهای سرورها نمی باشد .در این بین سرمایش، تهویه، امنیت، نگهداری و دیگر عوامل جانبی اتاق های سرور نیز باید به تناسب گستردگی آن اتاق سرور تامین گردد. هرسازمان و موسسه یک روز مجبور به راه اندازی مکانی بنام اتاق سرور است ، اگرچه شرکت ها و پیمانکاران زیادی هستند که تمام مراحل اجراء یک اتاق سرور را انجام داده و همه چیز را حاضر و آماده تحویل می دهند ولی داشتن کمی اطلاعات در خصوص راه اندازی اتاق سرور برای هر فرد دست اندرکاری لازم است. تعداد کمی از مدیران سیستم های رایانه متوجه اهمیت برنامه ریزی قبلی برای راه اندازی یک اتاق سرور هستند ، غافل از اینکه داشتن برنامه ریزی برای آینده حجم زیادی از وقت ، پول و مشکلات آینده شما را کاهش خواهد داد.

امنیت و کنترل دسترسی به دیتاسنتر از مواد مهم و دغدغه های همیشگی مدیران دیتاسنترهاست چرا که اولین سد دفاعی در برابر خطر، دفاع فیزیکی است و اولین مرحله دفاع فیزیکی صدور، قطع و یا کنترل تردد در مناطق حفاظتی است.

آماده سازی اتاق سرور جهت ارتباطات شبکه ای سرورها با ایستگاه های مختلف شبکه از جمله کارهای پایه ای در اتاق سرور می باشد. درواقع کلیه کارها و هزینه هایی که در اتاق سرور انجام می شود هدفش استفاده منطقی و مطمئن از تجهیزات اتاق سرور می باشد.

فصل اول
معرفی دیتا سنتر و استاندارد آن

مقدمه

دیتاسنتر(یا مرکز داده) اصلی ترین بخش یک شبکه در مراکز امروزی می باشد. نیاز به مدیریت متمرکز منابع، کاهش هزینه های نگهداری، مقابله موثر با تهدیدات امنیتی و حصول اطمینان از عملکرد صحیح و بلادرنگ ، طراحی یک دیتاسنتر مناسب با ویژگی های مورد نیاز را اجتناب ناپذیر نموده است.

در کل به حاصل تجمیع و مدیریت متمرکز سرورها، شبکه ها و تأسیسات کنترل و نگهداری یک مرکز بزرگ داده وسرویس دهی رایانه ها، دیتاسنتر می گویند.

قبل از هر چیز در راه اندازی یک دیتا سنتر باید طرحی را پیاده سازی کنیم که احتیاجاتمان را پوشش دهد ، در حال حاضر چه چیزی احتیاج داریم و در آینده چه چیزی نیاز خواهیم داشت .

ممکن است در حال حاضر ، همه تجهیزات شما بر فرض مثال درفضایی به مساحت ۸×۱۰ جای بگیرد ، اما در پنج سال آینده چقدر فضا نیاز خواهید داشت ؟ اگرچه اطلاع از اینکه چقدر فضا در آینده نیاز خواهید داشت امکان پذیر و تاثیر گذار در بودجه می باشد ، اما برنامه ریزی قبلی برای این مساله امکانات بیشتری را در این خصوص در اختیار شما قرار میدهد.

هنگامی تحقیقات شما در مورد میزان فضای مورد نیاز به نتیجه رسید ، زمان آن فرا میرسد که مافوق های خود رامتقاعد کنید که برآوردهای شما صحیح و عملی است.

استانداردهای جهانی TIA ۹۴۲, ISO ۲۷۰۰۰ از جمله استانداردهایی است که ما در طراحی و پیاده سازی مراکز داده از آنها بهره می بریم.

یک دیتاسنتر استاندارد از نظر ANSI/TIA از بخشهای متعددی چون Entrance Room, Storage Room, Telecomm Room و ... تشکیل می گردد که اتاق سرور(Server Room/Computer Room) مهمترین آنهاست. با توجه به محدودیت منابع، هزینه و اطلاعات در شرکت ها، سازمان ها و موسسات متوسط و کوچک، راه اندازی یک اتاق سرور استاندارد در اینگونه مراکز کافی می باشد.

معرفی دیتاسنتر و استانداردآن

اتاق سرور[۱] مرکزی است که از مجموع خدمات و تکنولوژی هایی درست می شود که نتیجه آنها ارائه خدمات الکترونیکی می باشد .هسته دیتاسنتر را سرورها، سوئیچ ها و روترها تشکیل می دهند که خدمات الکترونیکی بر روی بستر آنها ارائه می گردد اما برای نگهداری و حفاظت و کارکرد صحیح این سامانه ها از تکنولوژی ها و تاسیسات دیگری نیز در دیتاسنتر استفاده می شود که

[۱] Server room

اهمیت آنها برای حیات دیتاسنتر و اطلاعات الکترونیکی ، کمتـر از سـرورها و سـوئیچ هـا نیـست . سامانه هایی مانند سامانه های تولید، پشتیبانی وانتقال و توزیع برق که بایـد بـر اسـاس تکنولـوژی های دیتاسنتری تهیه گردند، سامانه های سرمایشی و دفع گرد و غبار و سامانه های امنیتی ماننـد اطفاء حریق و کنترل تردد و ... همه و همه سامانه ها و تکنولوژی هایی هستند که حیات مناسب و پایداری اطلاعات و دیتاسنتر راتأمین و تضمین می کنند.

با توجه به اینکه هر کدام از این سامانه ها و تاسیسات که دیتاسنتر را تشکیل مـی دهنـد دارای حساسیت محیطی، ضریب امنیت مکانی وکارشناسان پشتیبان متفاوتی هستند لازم است کـه هـر گروه از آن ها در محیط های متفاوت با شرایط متفاوتی نگهداری شوند . به همین دلیل فضای کلی دیتاسنتر را به فضاها و بخش های گوناگونی تقسیم می کنند که به آنها اصطلاحاً مناطق[1] دیتاسنتر می گویند.در این رابطه در ادامه نیز بخش های گوناگونی کـه طبـق اسـتانداردها بـرای دیتاسـنتر طراحی و پیشبینی می کنند را شرح داده و تجهیزاتی که در آنها نصب می شود را مورد بررسی قرار می دهیم.

استاندارد TIA ۹۴۲ استانداردی برای طراحی و تجهیز دیتا سنتر:

استانداردی است که توسط TIA در سال ۲۰۰۵ برای تعیین راهکارهای عملی بـرای طراحـی و ساختDatacenter ها

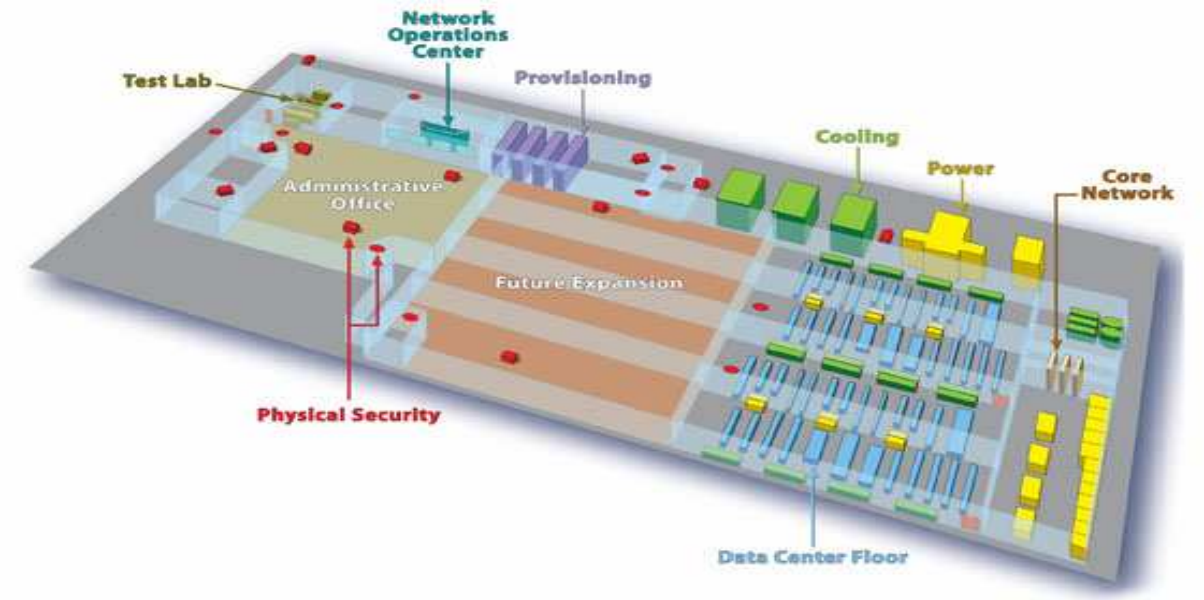
مخصوصا با توجه به سیستم های کابل کشی و طراحی شبکه ایجاد شده است. این استاندارد، در دستورالعمل های خود هر دو نوع رسانه فیبر نوری و کابل های مسی را مـد نظـر قـرار داده اسـت. همچنین مرجع تعیین کننده برای نیازمندی های خاص نواحی خصوصی و عمـومی datacenter در مورد برنامه های کاربردی و دستورالعمل های اجرایی می باشد.

اهداف استاندارد۹۴۲-TIA

هدف مهم این استاندارد، تهیه نیازمندی ها و راهنمایی های لازم برای طراحی و نـصب Data Center و یا اتاق کامپیوتر می باشد. این استاندارد مد نظر طراحانی اسـت کـه احتیـاج بـه فهـم گسترده در مورد طراحیData Center شامل طرح ریزی ساختمان، سیستم های کابل کـشی و طراحی شبکه دارند.

شکل زیر نمای کلی یک دیتا سنتر با استفاده از استا ندارد TIA-۹۴۲ را نشان میدهد:

[1] zone



شکل (۱ – ۱) نمای کلی یک دیتا سنتر

استاندارد TIA-۹۴۲ چهار ناحیه اصلی را در Data Center بررسی می کند که عبارتند از:

۱. اتاق تجهیزات[۱]
۲. اتاق تاسیسات[۲]
۳. اتاق سرور و شبکه[۳]
۴. اتاق مانیتورینگ[۴]

نکاتی که قبل ازراه اندازی یک اتاق سروربابد بدانیم

هنگامی تحقیقات شما در مورد میزان فضای مورد نیاز به نتیجه رسید ، زمان آن فرا می رسد که همه را متقاعد کنید که برآوردهای شما صحیح و عملی است:

۱: شماباید به مافوق های خود نشان دهید که در حال حاضر چندنفر پرسنل و چه مقدر تجهیزات باید درآن فضا جای داده شود.

۲ : باید به آن ها بگویید که طبق برآوردهای شما،شرایط در ۵ یا ۱۰ سال آینده چگونه خواهد بود. اعلام کنید که توسعه در آینده چه میزان هزینه خواهد داشت ،ده سال دیگر هزینه تاسیسات و

[۱] Equipment room
[۲] Facilities room
[۳] Server and Network room
[۴] Monitoring room

تجهیزات قطعا افزایش خواهد داشت . به آنها یادآوری کنید که اگر مجبور شوید تجهیزاتی را به هر مکان دیگری منتقل کنید مجبور خواهید شد کابل کشی نیز انجام دهید. نکته کلیدی که باید روشن کنید این است که با انجام این عملیات در حال حاضر شما در بودجه موسسه صرفه جویی خواهید نمود .اگر بتوانید این اطلاعات را به همراه نمودار و یا سایر اطلاعات دیگر نمایش دهید قطعا موفق خواهید شد.

۳ : مکان مناسبی پیدا کنید: یکی از مهم ترین مراحل طراحی یک اتاق سرور پیدا کردن محل مناسب است .

شما با انتخاب یک محل مرکزی در ساختمان می توانید از بسیاری از مشکلات جلوگیری کنید. مثلا بهترین مکان در یک ساختمان ۳ طبقه ، طبقه اول و در کنار دفتر مدیریت است ، به این دلیل که قاعدتا شما با مدیران بیش از هر فرد دیگری در تماس و ارتباط هستید.بخاطر داشته باشید که هرقدر سریعتر به نیازهای مشتریانتان پاسخ بدهید ، شناخته تر خواهید شد! با استفاده از یک مکان مرکزی ، وقت کمتری را در رفت و آمد برای ارائه سرویس تلف خواهید نمود . همچنین اگر در یک مکان مرکزی قرار بگیرید ، صرفه جویی زیادی در هزینه های کابل کشی انجام خواهید داد .شما کابل های کوتاهتری استفاده خواهید نمود ، نیاز به نگهداری کمتری خواهید داشت ، به سخت افزارهای کمتری (ازقبیل روتر) نیاز خواهید داشت و نگران نقشه کشی های کمتری خواهید بود. در اتاق سرور محدودیت ایجاد کنید :

برخی از مدیران سیستم ترجیح میدهند که اتاق سرور را جدا[۱] کنند تا کسی به کامپیوترها دسترسی نداشته باشد. به دلایلی کارمندان علاقه دارند که در اتاق سرور جمع شوند ، بعضی مواقع کارمندان احساس راحتی بیشتری می کنند اگر بتوانند مشکلات را شخصا با شما درمیان بگذارند ، بعضی مواقع آنها فقط برای یک گپ کوتاه به آنجا می آیند. بهترین راه برای این مساله محدودنمودن دسترسی به اتاق سرور برای کارمندان ، بجز کارمندان بخش IT میباشد. می توانید دسترسی به اتاق کامپیوترها را بوسیله سیستم های دسترسی با کارت و یا دستگاه های رمزی[۲] محدود کنید.در عین حال می توانید تماس خود با سایرین را بوسیله راه اندازی یک سیستم ایمیل حفظ کنید.به این ترتیب سایرین میتوانند مشکلات خودرا به شما از طریق ایمیل اعلام کنند.

کنترل محیط اتاق سرور:

اتاق که در آن تجهیزات کامپیوتری خودرا نگهداری می کنید باید الکتریسته ساکن، اختلالات مغناطیسی و نویزهای برقی حاصل از ترانسفورماتور و چراغ های فلورسنت باشد. شما باید یک پد استاتیک در نزدیکی در ورودی اتاق قرار دهید. کارمندان باید یادبگیرند که چگونه از این پد

[۱] Isolated
[۲] Cryptographic devices

استفاده کنند. . به دلایل روشن ، اتاق را باید تهویه مطبوع داشته باشد ، و آن را باید تمیز و عاری از گرد و غبار نگهداری نمود. درجه حرارت را کمتر از ۲۲ درجه سانتی گراد ثابت کنید و اگر تجهیزات زیادی نصب کرده اید ، شایدلازم باشد که درجه حرارت را پایینتر هم بیاورید.

تجهیزات کامپیوتری آنطور که عموما تصور می شود به خاک و غبار حساس نیستند ولی احتیاط از پشیمانی بهتر است .

معمولا استفاده از فیلتر در سیستم های تهویه ، خاک و غبار را از فضا خارج خواهد نمود.

امنیت فیزیکی

انوع کنترل امنیت فیزیکی[1] که هر سازمانی می بایست آن را اتخاذ کند :

محصور نگاه داشتن اتاق سرور

حتی قبل از راه اندازی سرورها، در حقیقت قبل از روشن ساختن آن ها برای اولین بار می بایست از تجهیزات امنیتی جهت محفوظ نگاه داشتن آن ها استفاده کرد. بهترین قفل ها تا زمانی که استفاده نشوند خوب نیستند، در نتیجه نیازمند راه هایی هستیم که در هر زمانی که اتاق اشغال نشده باشد، درها قفل شده و همچنین نشان دهد که چه کسی کلید و یا کد کلید را دارد. اتاق سرور قلب شبکه فیزیکی ماست و کسی با دسترسی فیزیکی به سرورها، سوئیچ ها، روترها، کابل ها و سایر دستگاه ها در آن اتاق، می تواند خسارات شدیدی به بار آورد.

راه اندازی سیستم پایش و تجسس

بستن اتاق سرور یک گام نخست خوب محسوب می شود، اما باید توجه داشت که یک نفر می تواند آن را بشکند یا شخصی که دسترسی مجاز دارد می تواند از این دسترسی سوء استفاده کند. ما به روشی نیاز داریم که بدانیم چه کسی، چه زمانی، به داخل اتاق وارد و از آن خارج شده است. دفتر ثبت برای ثبت ورود و خروج، ابتدایی ترین روش جهت انجام این امر است، اما موانع زیادی در بر دارد. یک فرد از روی تمایل بدخواهانه می تواند با خوش شانسی از آن عبور کند. کارت ورود و یا اسکن های بیومتریک برای باز کردن در مورد نیاز خواهد بود و سندی مبنی بر شناسایی هر فرد وارد شونده به اتاق می بایست ایجاد شود؛ همچنین نصب یک دوربین پایش می تواند کارهای زیرکانه افراد را خنثی (پیدا کند) و تصویر مشخصی از افراد هنگام ورود و یا ترک از محل با درج زمان آن به ما ارائه کند که می تواند سیستم دفتر ثبت الکترونیکی ما را تکمیل کند. این دوربین ها می توانند به صورت مستمر فعال بوده یا از تکنولوژی تشخیص حرکت و ثبت حرکت هر فرد

[1] Physical Security

برخوردار باشند و حتی میتوانند برای ارسال e-mail یا یک هشدار تلفن همراه ما را از حرکتی زمانی که نباید اتفاق میافتاد آگاه سازد.

مطمئن شویم که آسیب پذیرترین وسایل و تجهیزات ما در آن اتاق سرور است

باید توجه داشت که این فقط سرورها نیستند که باید در موردشان نگران باشیم، یک هکر می تواند یک لپ تاپ را به یک سوییچ وصل کرده و از طریق یک نرم افزار ساده به اطلاعات شبکه دسترسی پیدا کند. اطمینان حاصل کنیم که در حد امکان تمامی وسایل در اتاق ایمن مذکور بوده یا چنانچه نیاز دارند در مکانی دیگر باشند، در مکانی ایمن و بسته، در هر کجای ساختمان قرار داشته باشند.

از سرورهای دارای قفسه های مستحکم استفاده کنیم

این سرورها نه تنها فضای کمتری را اشغال میکنند، بلکه به راحتی ایمن می شوند، قفسه های آن میتوانند چندین سرور را تحمل کرده و بر روی سطح زمین محکم قرار گیرند. تهیه یک پکیج کامل از ابزار امنیتی اغلب غیر ممکن است اما میتوان با استفاده از آنها در حد امکان دزدی را به حداقل رساند.

از ایستگاه های کاری غافل نشویم

هکرها از هر کامپیوتر غیر ایمنی که به شبکه متصل باشد، به منظور حذف یا دسترسی اطلاعاتی از آن که برای کسب و کار ما مهم است استفاده میکنند. ایستگاه های کاری شامل میز اشغال نشده یا دفاتر خالی (ترک خدمت فرد به علت تعطیلات) و یا مکان هایی که برای افراد خارج از سازمان قابل دسترسی هستند از قبیل جلوی میز پذیرش گر منحصرا آسیب پذیرند. کاهش یا حذف کامپیوترهایی که مورد استفاده قرار نمیگیرند، یا بستن درهای دفاتر خالی شامل آنهایی که موقتا خالی میباشند در حالی که مجهز به کامپیوترهایی اغلب خارج از دید سایر کارمندان میباشد امری مؤثر در کاهش آسیب پذیری است و می توان ورود به آن ها را با تجهیز آن ها به کارت های هوشمند، دشوار ساخت.

دور نگاه داشتن متجاوزین از کسب موقعیت

هم در خصوص سرورها و هم ایستگاه های کاری می بایست از سارقانی که می توانند مکان را باز کرده و سخت افزارهار را به سرقت ببرند ایمن سازی های مورد نیاز انجام شود. بسیار آسانتر است که با یک سخت افزار در جیبتان از محل خارج شوید تا یک تجهیز بزرگ که نیازمند تأییدیه های

مختلف است. بسیاری از کامپیوترهای با قفل های کیس جهت جلوگیری از باز کردن کیس بـدون داشتن کلید آن میباشند. شما می توانید جعبه ابزار قفل را از منابع مختلف با هزینه های پائین در محصولات امنیت ابتکاری تهیه کنید.

از پرتابل ها محافظت کنیم

لپ تاپ ها و کامپیوترهای قابل حمل حالت خاصی از ریسک های امنیت فیزیکی محسوب مـی شوند. یک سارق میتواند به راحتی کل کامپیوتر را به سرقت ببرد؛ که شامل داده های ذخیره شده روی دیسک و همچنین پسوردهای ورود به شبکه ای که ممکن است ذخیره کـرده باشـیم، باشـد. چنانچه یک کارمند از لپ تاپ روی میزش استفاده میکند، میبایست هنگـام تـرک محـل آن را بـا خودش حمل کند یا آنها را با یک بست موقت یا قفل کابلی و یا قرار دادن در کشوی قفل دار ایمن سازد. بکارگیری هشدارهای حسگر حرکت نیز اغلب برای اخطار به حرکت درآمدن پرتابل ها ایـده ی مناسبی میتواند باشد.

بستن و محفوظ نگاه داشتن نسخه پشتیبان

بستن داده های مهم، یک عامل ضروری در بازگشت از فجایای رخ داده است، اما فراموش نکنیم که اطلاعاتی که در دیسک ها پشتیبان گیری شده اند می توانند ربـوده شـده و توسـط فـردی در خارج از سازمان مورد استفاده قـرار بگیرنـد. بـسیاری از راهبـران فنـاوری اطلاعـات نـسخه هـای پشتیبان[1] را در مقابل سرورها در اتاق سرور حفظ می کنند، در حالی که آنها میبایست این نـسخه ها را حداقل در کشوی دارای قفل نگهداری کننـد. ایـده آل آن اسـت کـه دسـته هـایی از نـسخه پشتیبان در خارج از محل، جایی که ایمن بودن آن جا را تضمین می کنید، نگهداری شود. نباید از اینکه بسیاری از کارکنان، نسخه پشتیبان را بر روی دیسک فلاپی، CD، USBیا دیسک های هارد اکسترنال نگهداری می کنند به راحتی گذشت؛ اگر چنین روشی اجازه داده شده یـا بـدان تـشویق شده است، باید از اینکه تمام سیاست های مورد نیاز جهت ایمن سازی نـسخه پـشتیبان در تمـام مدت اعمال میشود، اطمینان حاصل کنیم.

از کار انداختن درایوها

چنانچه شما نمی خواهید کارمندان شرکت، اطلاعات شرکت را روی یک رسانه قابل حذف کپی کنند، باید درایوهای فلاپی یا پرت های USBو سایر وسایل ارتباط با یک وسیله خارجی را حـذف

[1] Backups

یا غیر فعال کنید. قطع ارتباط کابل ها برای مدتی موجب نگرانی کارمندان نخواهد شد. برخی از سازمان ها خیلی فراتر از پر کردن پرت ها با چسب یا سایر مواد محافظ موقتی جهت جلوگیری از استفاده می روند، با استفاده از نرم افزارهایی جهت غیر فعال کردن آن ها.

از پرینترها محافظت کنیم

شما نباید در خصوص پرینترها به ریسک امنیتی فکر کنید، اما بسیاری از پرینترهای امروزی محتویات اسناد را در بردهای حافظه خودشان ذخیره میکنند؛ اگر یک هکر پرینتر را بدزدد یا به حافظه آن دسترسی پیدا کند، او قادر خواهد بود که از پرینت های اخیر اسناد را کپی برداری کند. در نتیجه پرینترها نیز مشابه با سرورها و ایستگاه های کاری که اطلاعات مهم را ذخیره می کنند می بایست در جایی امن قرار گیرند. اغلب پرینت هایی مشاهده می شود که در کنار پرینتر رها شده و یا در سطل آشغال انداخته شده اند و دارای اطلاعات مهمی از سازمان می باشند که قابل برداشت و بازخوانی هستند. بهترین حالت، پیاده سازی سیاستی است که پرسنل سازمان اسنادی که مورد نیاز نمی باشند را پاره کنند، حتی آن هایی را که اطلاعات به خصوص در آن ها درج نشده است.

جمع بندی

به یاد خواهیم داشت که امنیت شبکه از سطح فیزیکی آن آغاز می شود و تمامی دیوارهای آتش در جهان، متجاوز را متوقف نخواهند کرد، شخصی که توانایی این را دارد که به شبکه شما و کامپیوترهای شما دسترسی فیزیکی پیدا کند، می تواند موجب خسارت های جبران ناپذیر شود ، بنابراین از قفل کردن ها و ایمن سازی های فیزیکی پرهیز نکنیم .

فصل دوم
ایجاد دیتا سنتر و امنیت فیزیکی آن

مقدمه

شاید برای مخاطب سوال این باشد که دیتا سنتر چیست . در این فصل سعی شده است که مخاطب دیتا سنتر و راه های امنیت آن را فرا گیرد.

قلب یک شبکه بزرگ را دیتا سنتر گویند ، که اجزای آن را سوییچ ها ،روترها، فایروال ها ،کابل کشی ها و اجزای مهم سخت افزاری شبکه تشکیل می دهند .

سوال دیگری که ممکن است برای شما پیش آید این است که دیتا سنتر چه فایده ای دارد .

حذف ترافیک بی مورد و کاهش ارزبری : ده ها سرویس پیشتاز مبتنی بر وب مانند سرویس های وبلاگ نویسی،اتاق های گفتگو ، انجمن های تبادل نظر ، بانک های اطلاعاتی سازمان ها و ادارات و نهادهای دولتی و خصوصی و بانک ها و ده ها وب سرویس پیشتاز دیگر ایرانی بعلت نبود دیتاسنتر و هاستینگ ایرانی در سرورهای خارجی و اکثر آمریکایی ، هاست شده اند که موجب پیدایش ترافیک داخلی و بی موردی در دروازه نقاط تماس بین المللی شده است. بیش از ۸۰درصد بازدیدکنندگان و کاربران وب سایت ها و وب سرویس های ایرانی و (فارسی) مقیم داخل کشور هستند و با نصب و راه اندازی و هاست کردن این سایت ها در داخل کشور می توان به مقدار قابل توجهی از ترافیک لوپ شده تقاضاهای بازدید و استفاده از این سایت ها کاست و به این ترتیب ترافیک و دروازه نقطه تماس بین الملل کشور را برای دیگر درخواست ها خالی کرد. ضمن اینکه با کاهش ترافیک خروجی از نقاط تماس بین الملل ارز بری کمتری صورت خواهد گرفت .

بالا رفتن ضریب ایمنی : با راه اندازی دیتاسنترهای ایمن داخلی بانک ها ، نهادها و موسسات دولتی که نیاز به امنیت بالایی در ارتباطات خود دارند می توانند با استفاده از سرورهای داخلی و قابلیت سفارشی کردن سیستم های حفاظتی سرورها با اطمینان بیشتری اقدام به نگهداری ، تبادل و ارائه سرویس در بستر ICT بکنند.

کاهش هزینه ها و جلوگیری از ارزبری : با استفاده از دیتا سنتر داخلی جز کاهش هزینه ها و جلوگیری از ارزبری بی مورد در هزینه های نقاط تماس بین الملل به سبب ارائه هاستیگ داخلی دیگر نیازی به خرید هاست از شرکتهای خارجی و خروج ارز از کشور نخواهد بود. اضافه بر اینکه در صورت مدیریت درست این مراکز و استفاده از دانش و نیروی ارزان متخصصان داخلی و کاهش هزینه های نگهداری می توان به رقابتی شدن قیمت های هاست های داخلی با خارجی اندیشید. بازار هاستیگ در کشورهای درحال توسعه بازار بکر و پراستعدادی است که در صورت هدایت و مدیریت درست میتواند سود کلانی را نصیب صاحبان مراکز داده بکند.

توسعه فناوری اطلاعات :راه اندازی و استفاده از دیتا سنتر داخلی موجب افزایش توان و تخصص نیروهای داخلی، جلوگیری از فرار مغزها و استفاده از توانشان در داخل کشور و توسعه IT از جهت توسعه زیر ساخت های آن می شود .

تحقق دولت الکترونیک : بعد از زیرساخت های مخابراتی اولین و مهمترین چیزی که برای راه اندازی و ارائه خدمات دولت الکترونیک به مردم مورد نیاز است مراکز داده و سرورهای استانی و ASPهاست .

راه اندازی هاستینگ ملی : حتما شما هم جریان مسدود شدن سرور وبسایت خبرگزاری دانشجویان ایران (ایسنا) توسط شرکت آمریکایی The Planet و یا توقیف صد ها دامنه[1] اینترنتی متعلق به ایرانی ها توسط شرکت های آمریکایی ای مثل RegisterFlye, Enom و Register.comرا به یاد می آورید که با استناد به قوانین تحریم ایالات متحده انجام شده بود. با راه اندازی دیتا سنتر ایرانی و مهاجرت سایت های ایرانی به این سرورها دیگر اخبار ناراحت کننده ای از این دست منتشر نخواهد شد.

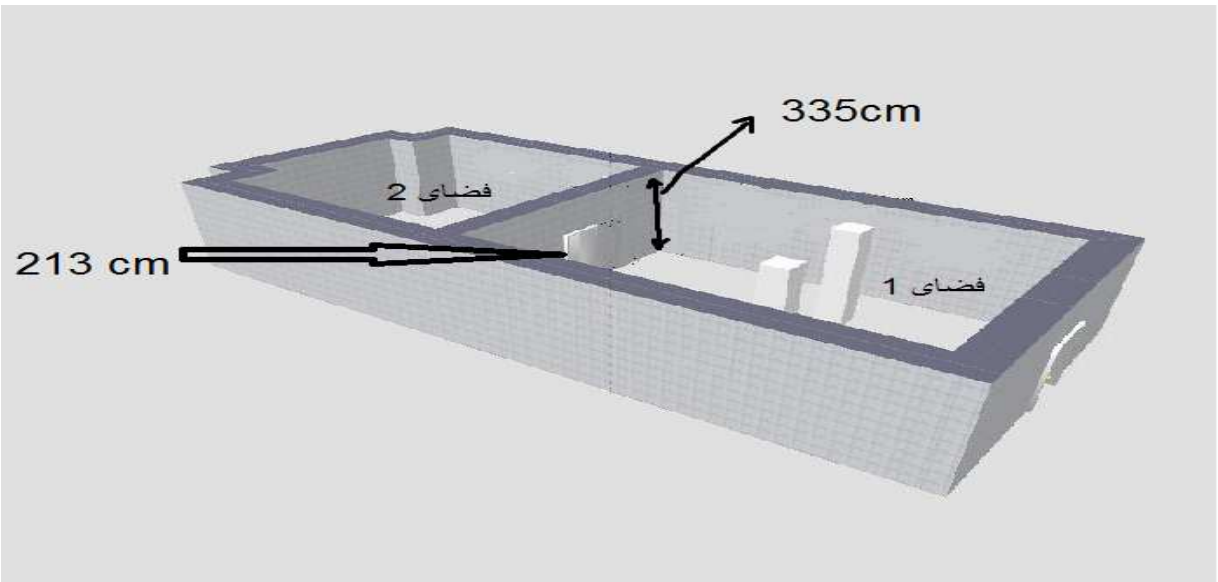
ایجاد دیتا سنتر

وضعیت موجود و ابعاد ساختمان

اولین گام در طراحی یک دیتا سنتر وضعیت ساختمان و ابعاد موجود می باشد . باید فضای پیش بینی شده به صورتی باشد که نزدیکترین فضا به استانداردهای لازم تعیین شود. در این مرحله باید نقشه و ابعاد ساختمان مورد بررسی قرار گیرد.

نمای سه بعدی و اندازه ها و ارتفاعات فضای موجود دیتاسنتر نیز در شکل زیر آورده شده است :

[1] Domain



شکل (۲- ۱) نمای سه بعدی فضای موجود دیتاسنتر

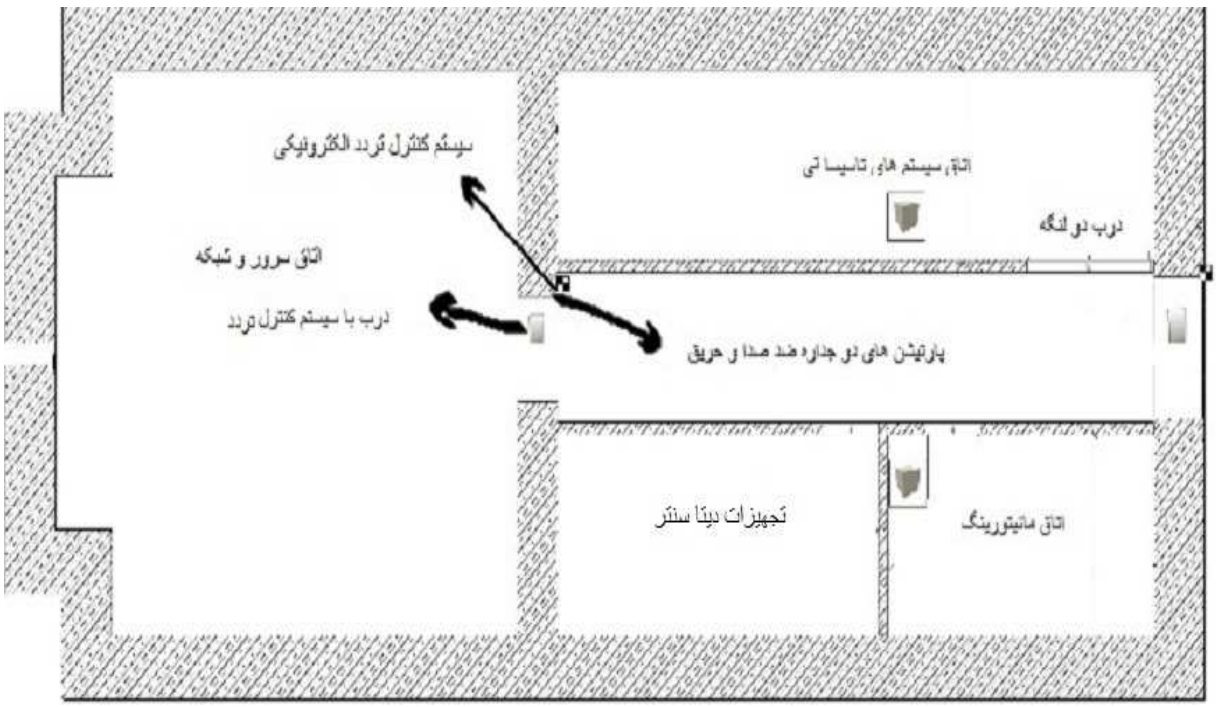
سقف از جنس بتون و همراه با با تیغه های بتونی موازی که در عرض کشیده شده اند وبه ارتفاع ۳۵ سانتی متر دراز سقف بیرون کشیده شده اند . ارتفاع دیوارها از زمین تا سقف (با حساب تیغه ها) ۳۳۵ سانتی متر است.

در وسط ، دو فضای شماره ۱ و ۲ را از هم جدا شده است . ارتفاع در ۲۱۳ سانتی متر تعیین شده است. فاصله تیغه ها از هم حدود ۱۰۵ سانتی متر است . باید به این نکته توجه داشت که در سقف هر فضا چند تیغه به کار رفته است.

در یک اتاق سرور استاندارد به علت مسائل امنیتی و گرد و خاک نباید پنجره وجود داشته باشد و اگر هم وجود داشته باشد باید آن را پوشاند.

وضعیت و نقشه ساختمانی

یک نقشه به نام نقشه هدف باید طراحی شود که هدف انجام دیتا سنتر را شرح می دهد ، که چیدمان نهایی تجهیزات و فضا های عملیاتی دیتا سنتر را تعیین می نماید. باید سعی شود با تکیه بر استانداردها و ساده ترین روش و کمترین مخارج به هدف نهایی که برپایی دیتاسنتر است رسید.



شکل (۲ – ۲) نقشه ساختمانی دیتا سنتر

همان طور که در نقشه مشاهده می کنید فضای ۲ به اتاق سرور و شبکه اختصاص داده شده که تلفیقی از دو منطقه سرور و شبکه است . فضای شماره ۱ نیز به سه منطقه تبدیل شده است که یک بخش آن اتاق سیستم های تاسیساتی و در بخش دیگر دو منطقه اتاق مانیتورینگ و مدیریت و تجهیزات دیتاسنتر درست شده است.

برای فضاها از پارتیشن[۱] دو جداره با ۱۰ سانتی متر ضخامت و عایق پشم سنگ، به صورتی که پارتیشن ها کاملاً ضد صدا و ضد حریق و ضدالکتریسیته باشند استفاده شده است .

پارتیشن ها تا سقف کشیده شده و در محل اتصال به دیوارها، سقف و درب ها نیز عایق می شوند، طراح باید جنس پیشنهادی خود را با قیمت متراژ واحد و کل مشخص نماید.

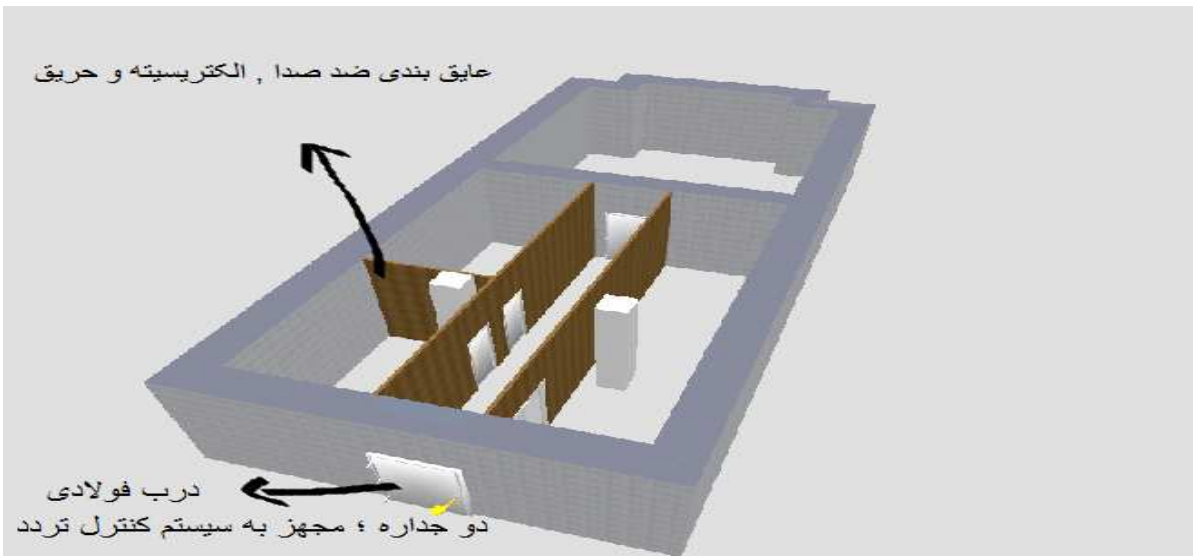
برای اتاق تاسیسات از درب دولنگه استفاده می شود که مقاومت لازم را نیز داشته باشد و به مرور زمان دچار خرابی نشود.

درب مذکور نیز باید دوجداره و با شرایط پارتیشن ها و در محل های اتصال خود عایق شده باشد . برای اتاق های مانیتورینگ وتجهیزات نیز باید درب هایی تک لنگه که آنها نیز باید شرایط پارتیشن ها را داشته و در محل اتصالات خود عایق شده باشند و در داخل درب ها استحکام لازم داده شود.

[۱] Partition

درب اصلی ورودی از نوع فولادی و دارای گارد مستحکم در دیوار باشد و بعـلاوه دارای سیـستم دربازکن الکترونیکی در داخل خود درباشد که بتواند توسط سیستمهای کنترل تردد الکترونیکی باز و بسته شود و در عین حال از استحکام لازم نیز برخوردار باشد و و در محل اتصالات خود در برابـر صدا، آتش و رطوبت عایق باشد.

درب ورودی اتاق سرورها و شبکه نیز باید شرایط درب اصلی را داشـته باشـد. بـرای نـصب درب های ورودی اصلی و اتاق سرورها نیز باید چهارچوب مستحکم در دیوارها نصب گردد.



شکل (۲ – ۳) وضعیت ساختمانی دیتا سنتر

به یاد داشته باشید پنجره های موجود باید به طور کلی با مصالح عمرانی، مسدود گردد تا هـیچ گونه راه نفوذی برای افراد، تبادل حرارتی، گردوخاک ورطوبت به داخل مناطق مذکور وجود نداشته باشد. پنجره ها معمولا در ساختمان ها عوامل ناخواسته هستند.

ایجاد کانال جهت تردد برق، شبکه و کانال های هوای بین مناطق

با توجه به اینکه برای عبور کانال های هوا و برق از اتاق تاسیسات به محیط اتاق سرور و شـبکه، همچنین برای کشیدن کابل های شبکه بین اتاق های سرور و مانیتورینگ و تجهیزات و همچنـین عبور کابل های مخابراتی و شبکه از محیط خارج دیتاسنتر به داخل آن نیاز به کانال می باشد، باید

عملیات عمرانی حفر [1] و تنظیم آنها به صورتی انجام شود که موجب ترکیب هوای بین مناطق شود اما توجه کنید که این کار باعث ورود گرد و خاک به محیط دیتاسنتر و بالاخص اتاق سرور نشود.

نصب دیوار کوب های ضد حریق و ضد الکتریسیته

با توجه به اینکه محیط دیتاسنتر محیطی الکتریکی است و احتمال انباشت الکتریسیته ساکن [2] بر روی سطوحی که امکان بارداری الکتریکی [3] را دارند وجود دارد باید دیوارهای کل محیط با روکش های مناسب ضد حریق و ضد الکتریسیته و ضد گرد و خاک پوشیده گردد تا از بروز خطراتی که از این محل متوجه دیتاسنتر می شود جلوگیری گردد.

معرفی بخش های ساختمان دیتاسنتر

همانگونه که قبلاً نیز اشاره گردید، ساختمان دیتاسنتر را به بخش هایی که به آن ها مناطق عملیاتی دیتاسنتر گفته می شود تقسیم می کنیم، در هر منطقه از آن ها شرایط محیطی مورد نیاز تاسیسات آن منطقه ایجاد می شود وتاسیسات خاص آن محیط در آن نصب می گردد و در نتیجه هر گروه کارشناسی تنها در محیط مربوط به خود تردد دارد و کارهای جاری نیز با هم درگیر نمی شوند .در ادامه به معرفی بخشهای دیتاسنتر و تاسیسات آنها میپردازیم:

اتاق سرور و شبکه

در این پایان نامه سعی بر این شده که اتاق سرور و شبکه برای یکپارچگی بیشتر با هم ترکیب شوند . اتاق سرور فضایی است که در آن سرورهای دیتاسنتر در داخل رک های مستقر شده در آن نصب می شوند وبیشتر خدمات دیتاسنتر به هدف ایجاد پایداری در این مرکز است، برای اینکه امنیت و شرایط مجزا و بهتری برای تاسیسات این اتاق در نظر گرفته شود در دیتاسنترها اتاقی مجزا و با امکانات و حساسیت بیشتر را برای این منظور درنظر می گیرند. قلب ارتباطات دیتاسنتر روترها، سوئیچها و دیوارههای آتشی است که در این اتاق مستقر میشوند، این اتاق باکابل های شبکه و فیبرهای نوری [4] بین بیرون و داخل دیتاسنتر ارتباط اطلاعاتی برقرار میکند، کنترل ها و اجازه ورود وخروج اطلاعات از اتاق سرور در این نقطه انجام میشود .

[1] Drilling
[2] Static
[3] Electrically charged
[4] Optical fibers

اتاق سیستم های تاسیساتی

گرچه همان گونه که گفته شد اتاق سرور و شبکه منطقه مرکزی دیتاسنتر هست اما این تجهیزات به سامانه هایی برای مراقبت و ایجاد شرایط مناسب نیاز دارند که به آنها تاسیسات جانبی دیتاسنتر می گویند، این اتاق را اتاق خدمات[۱] یا تاسیسات می گویند. درصد اهمیت سامانه های مستقر در این اتاق بسیار بالاست مانند سامانه برق دیتاسنتر که خود از اهمیت صد در صد برخوردار است، سامانه های مستقر در اتاق تاسیسات موارد زیر هستند:

- سامانه برق
- سامانه سرمایش و تهویه
- سامانه اطفاء حریق و کنترل محیطی[۲]

در این اتاق سامانه های اصلی برق، سرمایش و اطفاء حریق[۳] نصب و نگهداری می شوند که برای عملکرد بهتر قلب دیتاسنترالزامی هستند.

اتاق تجهیزات

با توجه به اینکه تجهیزات اتاق سرور و شبکه نیاز به تعمیر پیدا می کنند و تعمیر آنها گاهی اوقات زمان برخواهد بود بنابراین انجام عملیات مذکور در محل اتاق سرور و شبکه مناسب نیست و گاهی نیز برای آماده سازی تجهیزاتی که باید در این اتاق ها نصب شود نیاز به فضایی برای مهیا سازی می باشد که این عملیات ها در این اتاق انجام میشود، در این اتاق باید قفسه هایی قفل دار مناسب برای تجهیزات و کارت های کوچک تعبیه گردد و همچنین یک دستگاه رایانه و میز کار کامپیوتر که بتوان در صورت نیاز به مهیا سازی تجهیزات از آن استفاده نمود .گردش هوای مناسب و سامانه سرمایش نیز باید برای این محل در نظر گرفته شود.

اتاق مانیتورینگ

این اتاق را اصطلاحا Management Room یعنی اتاق نگهداری و مدیریت و یا Monitoring roomیعنی اتاق نظارت نیز گویند . با توجه به گستردگی و حوزه عمل دیتاسنتر این اتاق دارای بزرگی و گستردگی متفاوتی خواهد بود، در این اتاق عملکرد سرورها و تجهیزات جانبی اتاق سرور تحت نظارت و کنترل رایانه ای قرار میگیرد، در این مکان باید یک میز اداری مجهز به رایانه

[۱] Service room
[۲] Environmental Control
[۳] Fire control

جهت مدیر دیتاسنتر و به تعداد مورد نیاز نیز میز ورایانه های مناسب مانیتورینگ برای کارشناسان در نظر گرفته شود، بعلاوه باید در این محل به تعداد مورد نیاز نیز کابل شبکه جهت ارتباط با دیتاسنتر در نظر گرفته شود .بعلاوه این اتاق با توجه به بزرگی، نیاز به سامانه های متناسب سرمایشی/گرمایشی دارد.

تاسیسات دیتاسنتر

تاسیسات دیتاسنتر نقش مهمی در حفاظت و پایداری اطلاعات دارند اگر چه آنها جزو هسته دیتاسنتر نیستند اماخدماتی را به سرورها و شبکه ارائه می دهند که موجب تضمین حیات دیتاسنتر می شود، لذا باید توجهات لازم را به آنها داشت وبرای آنها اهمیت بسیاری قایل شد .با اینکه این تاسیسات در نگاه اول بسیار ساده و عادی می آیند ولی با توجه به ساختار دیتاسنتر نیاز به تکنولوژی های خاصی در راه اندازی آن ها می باشد و استانداردهایی فراتر از استانداردهای اماکن عمومی را باید رعایت کنند که در زیر به آنها اشاره بیشتری میشود :

لدر سقفی

برای انتقال کابل های برق در این اتاق باید لدر های لازم برای آن در سقف نصب گردد، این لدرها بایداستانداردهای لدرهای سقفی[1] به شرح زیر را داشته باشند:

- لدرها باید در سقف و دیوارها بصورت محکم نصب شوند.
- لدرها باید سبک باشند.
- لدرها باید در برابر حرارت و آتش سوزی مقاوم باشند و مشتعل نگردند.
- در محل خمش ها باید از زا نوهای خمش مناسب استفاده گردد.
- کابل ها باید دسته بندی و مرتب گردند و کابل های برق سیستم های تاسیساتی با کابل های تغذیه رک ها باید مجزا باشند.

سامانه سرمایش

بخش مهم دیگر در تاسیسات دیتاسنتر سامانه ی سرمایشی و تهویه می باشد، مرکزیت این سامانه در اتاق تاسیسات دیتاسنتر قرار دارد و کانال های هوای سرد از این مرکز به سمت اتاق سرور و شبکه کشیده می شود تا هوای خنک و تصفیه شده را به اتاق سرورها برساند . باید سیستم سرمایشی ویژگی های زیر را پوشش دهد :

[1] Ldrhay ceiling

- توان سرمایشی[1] سیستم مذکور باید متناسب با رک ها و گستردگی دیتاسنتر باشد . باید توان حرارتی سرورها و افزایش تعداد رک ها در آینده پیش بینی شود.
- سیستم دمش هوای HVAC باید قدرت رساندن سرمایش به تمامی رک های موجود در دیتاسنتر را داشته باشد.
- توان دمشی منتشر شده در رک های موجود باید یکنواخت باشد و سیستم هدایت دمش (هدایت کانال های هوا به جلوی رک) در داخل رک طوری جایگذاری شود که هوای خنک به تمامی سرورهای موجود در طبقات رک برسد.
- کانال های سیستم سرمایش باید ضدصدا و عایق باشد و به صورتی تنظیم و طراحی گردند که موجب هدررفت و یا مقاومت در برابر جریان هوای خنک نشوند.
- با توجه به اینکه در دیتاسنتر تجهیزاتی قرار دارد که در زمان گرم شدن از خود گازهای خطرناک یونی[2] آزاد می کنند، سیستم سرمایشی باید هوا را نیز تصفیه کند.
- تجهیزاتی از سیستم سرمایش که در این فضا قرار می گیرند باید کم صدا باشند و در صورت نیاز آن ها را جداگانه عایق صوتی نمود.
- برای اتاق های مانیتورینگ و تجهیزات و تاسیسات باتوجه به اینکه محل سکونت طولانی کارشناسان خواهد بود باید از اسپلیترهای سرمایش/گرمایشی اداری استفاه گردد. این اسپلیترها باید با توان بالایی داشته باشند ودارای فیلتر تصفیه هوا باشند. که موارد یونی هوای مسموم دیتاسنتر را نیز کنترل نمایند و دارای فیلتر هوای ضد قارچ و باکتری، تولید کننده هوای سالم و مطبوع باشد، بعلاوه دارای سیستم ضد یخزدگی باشد.
- تمامی سیستمهای سرمایشی چه اداری و چه HVAC باید توانایی کار بدون نقص و وقفه در بازه دمایی۱۰ درجه سانتیگراد تا ۶۰ درجه سانتیگراد بالای صفر را داشته باشند.
- سامانه ی مذکور باید ضد یخ زدگی بوده و هوای خروجی آن باید بدون نم و رطوبت باشد.

سامانه سرمایش و تهویه یکی از تضمین های سلامتی سرورها و شبکه می باشند که عمر و سلامت دیگرتجهیزات را نیز تضمین میکنند، سامانه سرمایشی در دیتاسنتر از چند بخش تشکیل شده است که باید هر کدام استانداردی را مختص خود داشته باشد و در صورت نیاز بتوان کانال های سرمایش را برای هر منطقه اتاق سرور تنظیم نمود، چون توان سرمایشی که در هر منطقه مورد نیاز است با دیگر مناطق متفاوت است لذا این سیستم باید بتواند به فراخور مناطق تحت پوشش خود قابلیت تنظیم متفاوت را داشته باشد.

در زیر به مناطق سرمایشی دیتاسنتر توجه بیشتری میکنیم:

---

[1] cooling power
[2] Ionic

- اتاق های سرور و شبکه : در اتاق سرور ما نیـاز بـه سـرمایش مناسـب آن داریـم و دمـای سرورها باید همیشه در سطح بین ۲۰ تا ۲۵ درجه سانتی گراد نگه داشته شود تا به آن ها صـدمه وارد نشود ولی در این اتاق ها به سیستم گرمایش نیازی نداریم.
- اتاق تاسیسات : در این اتاق به جای سرمایش مطلق بیشتر نیاز به تهویه مناسب و گردش هوا داریم گرچه دمای این سیستم ها نیز باید در حد ۲۵ تا ۳۰ درجه باشند و در دمـای بـالاتر بـه تجهیزات صدمه وارد میشود.
- اتاق های مانیتورینگ و تجهیزات : این اتاق ها که بیشتر محل حضور و توقف کارشناسـان اسـت نیـاز بـه سـرمایش و تهویـه هـوای اداری دارد و عـلاوه بـر سـرمایش نیـاز بـه سـامانه سرمایشی/گرمایشی دارد وتهویه نیز در این مناطق بسیار مهم است، بعلاوه کنتـرل گـرد و غبارهـا بالاخص گرد و غبارهای یونی حاصل از فعالیت دستگاه های برقی و الکترونیکـی نیـز بـرای حفـظ سلامتی کارشناسان ضروری میباشد.

سامانه برق

با توجه به اینکه سیستمهای برق و تغذیه دیتاسنتر بصورت ساختار یافته طراحی می شوند باید مسیرها وساختار انتقال آن نیز متناسب و جوابگوی نیازهای دیتاسنتر باشد .کابل های برق در این اتاق برای دو مقصد کشیده می شوند، یکی برای سیستم روشنایی و دیگری برای رکهای سروری و شبکه ای.

همانگونه که میدانید برق، مهمترین مساله در راه اندازی و پایداری تاسیسات رایانه ای میباشـد . برق دیتاسنتر در محل های زیر کاربرد دارد :

۱. برق سرورها و رک ها
۲. برق سیستم روشنایی و تغذیه دیواری
۳. برق سیستم سرمایشی
۴. برق سیستم های امنیتی و هشدار و اطفاء حریق

برق دیتاسنتر باید از دو سیستم متفاوت دریافت شود که در صورت بروز مشکل در هـر کـدام از آنها بتوان بار را به پست دیگر منتقل نمود.

برق سامانه های سرورها و تجهیزات شبکه که حساس ترین برق از نظر اختلالات برقی می باشد باید از طریق UPS های مناسب تهیه گردد تا موجب صدمه دیدن تجهیزات نگردد .علاوه بـر ایـن کابل ها باید توان کششی جریان تا دو برابر محاسبه شده را داشته باشند. برق لازم برای رک ها باید با کابل های مناسب، با دو فاز مجزا و به صورت مشخص از تابلوی برق مستقل به رک هـا کـشیده

شده و برای هر فاز رک فیوز مستقل تعبیه گـردد. آمپـراژ مـورد نیـاز بـرای سـرورها و سـوئیچ هـا ۸۰آمپر با در نظر گرفتن توسعه ها می باشد و برای ups ها نیز باید دو دسـتگاه UPS بـه صـورت Online و هر کدام با توان ۴۰KVA تهیه گردد بعلاوه این سامانه بایـد مـشکلات زیـر را از بـرق تغذیه رک ها حذف نماید :

- اعوجاج برق[۱]
- حالت گذرا در هنگام سوئیچ[۲]
- تغییرات فرکانسی[۳]
- نویز القایی به خط[۴]
- قطع برق[۵]
- افزایش لحظه ای ولتاژ[۶]
- کاهش لحظه ای ولتاژ[۷]
- کاهش ولتاژ[۸]
- افزایش ولتاژ[۹]

برق اتاق سرور باید بسیار استاندارد باشد و جهت اطمینان باید حد اقل از دو پست برقی متفاوت گرفته شده باشد، سامانه برقی اتاق سرور از ژنراتور UPS یا برق اضطراری و باطری ها و ثابت کننده ها تشکیل شده است .برق دیتاسنتر باید ۹فاکتور ناخواسته و مخرب برق را رفع نماید تا تجهیزات حساس دیتاسنتر بتوانند در سلامتی کامل و با بالاترین کارایی خود عمل نمایند.

برق دیتاسنتر باید پنج گروه مصرف کننده زیر را پوشش دهد :

برق مورد نیاز سرورها

این برق باید بصورت کاملا ایزوله از دیگر سامانه ها و مناسب تهیه شود و برای هر سرور دو کابل برق کشیده شود که از دو UPS خارج شده باشد تا در صورت از مدار خارج شدن هر کدام از UPS ها دیگری بتواند به کار خود ادامه دهد.

---

۱ Harmonic Distortion
۲ Switching Transient
۳ Frequency Variations
۴ PowerLine Noice
۵ Power Failure
۶ Power Surge
۷ Power Sag
۸ Low Power
۹ High Voltage

برق مورد نیاز سوئیچ ها و روترها

چون معمولاً این تجهیزات امکان توان اضافی[۳۶] را ندارند باید افزونگی ، به جای تجهیزات، بر روی مولد برق در نظر گرفته شود تا پایداری بیشتری تامین گردد .ضمناً این تجهیزات به شدت در برابر نویز و نوسان برق حساس اند و ممکن است از کار بیافتند.

برق سامانه های سرمایشی و تهویه دیتاسنتر

با توجه به توان مصرفی بالای سیستم های سرمایشی، باید برق آنها مستقل از تاسیسات داخلی دیتاسنتر و از پشت استابلایزر گرفته شود و جریان مصرفی این دستگاه باید مشخص گردد تا در زمان راه اندازی تابلوی برق در آن دیده شود .بعلاوه نباید قطعی مکرر برق موجب عملکرد نادرست سیستم سرمایشی دیتاسنتر و صدمه دیدن تجهیزات مرکزی گردد،.

با توجه به اینکه این سامانه ها معمولاً از موتور استفاده میکنند، برق این سیستم ها باید از برق شبکه و سرورها مجزا باشد و عمدتاً نیاز به توان بالایی در این زمینه می باشد و مهمترین مساله در برق آنها، قطع نشدن برق است.

برق سامانه های روشنایی و پریزها

برای این سامانه ها نیز باید برق مشخص و مجزایی تهیه گردد و UPS آنها باید از سیستم برق رک ها مجزا باشد و نباید از ups رک ها گرفته شود . تابلوی برق سیستم های روشنایی باید دارای فیوز-کلید مستقل برای هر واحد روشنایی محیط باشد که باید در طرح روشنایی پیشنهادی محاسبه و اعلام گردد.

برق سامانه های روشنایی دیتاسنتر نیز باید از دیگر سامانه ها مجزا باشد تا تاثیر مخرب بر روی برق سرورها و سوئیچ ها نگذارد، بعلاوه برق اضطراری باید این مناطق را نیز پوشش دهد اما نیاز ۱۰۰در صد به قطع نشدن برق این تجهیزات نیست و اگر با فاصله زمانی چند ثانیه نیزبه مدار برگردند حالتی مناسب می باشد، بعلاوه این سامانه ها میتوانند به حسگرهای حضورفیزیکی متصل شوند تا در صورت حضور فردی در اتاق روشن شوند و در صورت خروج کارشناسان از محل دیتاسنتر بصورت خودکار سامانه های روشنایی را خاموش کنند تا در مصرف برق صرفه جویی شود.

برق سامانه های امنیت و کنترل تردد

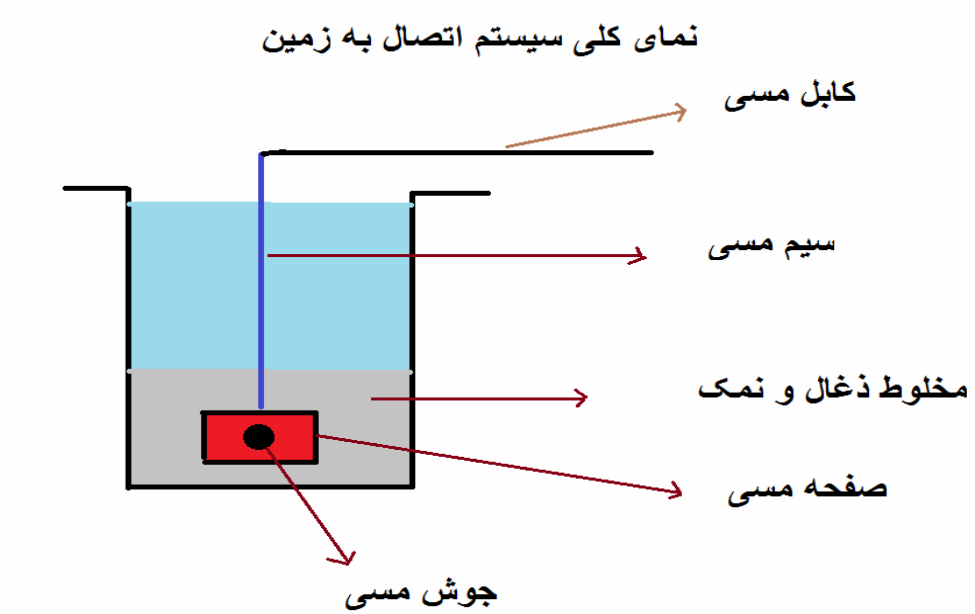
سیستم های امنیتی نیز با توجه به مسوولیت مهم خود نیاز به برق مستقل و با پایداری بیشتری دارند .رنگ کابل های این تاسیسات نیز باید مشخص و مجزا باشد که نیاز به یک دستگاه UPS

مختص خود دارد و باید پایداری برق آن بالا باشد و مدت زمان بیشتری قطعی برق را پشتیبانی نماید.

برق مورد نیاز سامانه هایی مانند دوربین مدار بسته، درب های الکترونیکی، کنترل تردد واطفاء حریق نیز باید بصورت مستقل تعبیه شوند و ضریب امنیت بالایی داشته باشند و بایدصورت بروز مشکل اساسی در سیستم برق دیتاسنتر نیز بتوان آن ها را فعال نگه داشت، لذا باید ازرله های کنترل برق و چند پست موازی استفاده نمود.

چاه ارت یا زمین شبکه برق

همانگونه که می دانید از مهمترین فاکتورهای دیتاسنتر وجود چاه ارت[۱] مناسب جهت زمین نمودن و ایجاد پایه ی استاندارد در جلوگیری از نوسانات و القائات[۲] برق است، اهمیت وجود این مساله با اهمیت راه اندازی برق دیتاسنتر برابر است و می تواند از صدمه دیدن تجهیزات جلوگیری کند.



شکل (۲ – ۴) چاه ارت یا زمین شبکه برق

[۱] Well Earth
[۲] Fluctuations and coercion

جهت جلوگیری از بارهای اضافی و مخرب روی سیستم برقی ، سیستم زمین یا Earth باید برقرار شود دراین سیستم ، نول واقعی شده و به چاه ارت توسط کابل مسی مرتبط می شود. شرایط ایجاد چاه ارت استاندارد در زیر آمده است :

حفر چاه تا رسیدن به خاک نم دار بایستی انجام شود . پودر ذغال و نمک (کلرید سدیم) به نسبت یک به دو (هرکیلو ذغال دو کیلو نمک) به مقدار ۴۰ کیلوگرم در چاه ریخته شود (این مواد با مقاومت خاک نسبت عکس دارند وکم یا زیاد کردن این مواد مقاومت خاک را زیاد و یا کم می کند)

صفحه ای مسی بصورت تیغه ای(عمودی) روی نمک و ذغال قرار میگیرد.

سیم مسی توسط پیچ و مهره مخصوص از **جنس مس** جهت جلوگیری از پوسیدگی و زنگ زدگی به صفحه مسی متصل می شود .

لوله پولیکا کنار هر چاه نصب می گردد . لازم به توجه است سوراخ های متعددی در بدنه لوله ها ایجاد شده تا اطراف لوله و چاه را مرطوب گرداند. در پایان چاه با خاک رس و نرم پر می شود. مقاومت چاه با استفاده از دستگاه ارت سنج باید زیر ۲ اهم باشد .

نتیجه : اگر صاعقه به ساختمان بزند از طریق این میله به زمین منتقل می‌شود اگر سیم لخت شده و به بدنه دستگاه ها وصل شود قبل از اینکه برای انسان خطری ایجاد کند به زمین منتقل می‌شود و خلاصه با ایجاد سیستم زمینی کردن خطر برق گرفتگی از بین می‌رود ضمنا در دو شاخه‌های جدید و پریزها جدید به جز سیم نول و فاز یک سیم دیگر وجود دارد و آن همین سیم ارت است.

در اثر برخورد صائقه به ساختمانی که سیستم ارتینگ ندارد معمولا کامپیوتر تاسیسات ساختمان و غیره آسیب می‌بینند در بهترین حالت استفاده از چاه ارت است پس توصیه می‌کنیم با توجه به هزینه نسبتا کم ساختمان را به این سیستم مجهز کنید.

کنترل محیطی و اطفاء حریق

با توجه به اینکه سیستم هایی که در دیتاسنتر قرار دارند با جریان برق کار می کنند، احتمال جرقه وآتش سوزی به صورت بیشتری وجود دارد، لذا وجود سامانه کنترل محیطی اهمیت بیشتری پیدا می کند .سامانه کنترل محیطی و اطفاء حریق این دیتاسنتر باید بتواند موارد زیر را تامین نماید :

- سامانه کنترل محیطی باید وضعیت های حریق(دود)، دما، رطوبت، ولتاژ هر فـاز بـرق رک ها، بار روی هر فاز ورودی برق رک، آمپراژ[1] هر کدام از فازهای برق رک ها، روشن یا خاموش بودن واحدهای روشنایی باز یا بسته بودن هر کدام از درب های دیتاسنتر را مانیتور کند.
- سامانه کنترل محیطی باید از موارد مانیتور شده گـزارش هـایی را تهیـه و در یـک رایانـه بصورت آنی ذخیره کند

و در صورت نیاز بتوان سابقه آنها را ذخیره نمود .گرچه گزارشگیری و ذخیره وضعیت موجود در روی رایانه ها برای مراجعات بعدی، اهمیت بسیاری دارد اما این سامانه باید بتواند وضعیت موجـود کنونی را بصورت زنده در مناطق مانیتورینـگ گونـاگون اعـلام نمایـد تـا در صـورت عـدم حـضور کارشناسان مربوطه در یک منطقه، اعلام خطر ناموفق نباشد، برای حسگرهای دما باید مانیتورهای لازم به صورت نمایشگر دما و چراغ و آژیر وضعیت غیرطبیعی را بتوان در مناطق گوناگون مانند اتاق تاسیسات، اتاق مانیتورینگ، دفتر مرکزی و هر نقطه ای که کشیک شیفت مستقر میگردد قرار داد، برای حسگر دود نیز باید آژیر و چراغ خطر در مناطق مذکور تعبیـه گـردد، همچنـین حـسگرهای حساس به آتش نیز باید توسط چراغ و آژیر بتوانند خطر را به افراد ذیربط اطلاع دهند .

- سامانه کنترل محیطی باید دارای سیستم های هشدار زنده جهت دود ، حرارت بیش از حد و آتش سوزی

به صورت آژیر و لامپ باشد و بتوان در صورت نیاز این اخطارها را در خارج از محیط نیز مشاهده نمود.

- سامانه باید دارای سیستم هشدار بر اساس SMS و پیغام و تماس تلفنی نیز باشد و ایـن امور قابل تنظیم باشند .
- باید بتوان سنسورها و هشدارهای سامانه کنترل محیطی را از طریق پا نل مدیریتی تحـت شبکه فعال یا تنظیم نمود.
- سنسورهای حرارتی برای هر رک باید سه عدد باشد و مکان آنهـا در پـایین(ورودی هـوای سرد)، وسط و بالای رک (محل خروج هوای گرم) باشد.
- تقسیم فضای هشدار و عملیات ضد حریق اتوماتیک باید به شکلی باشد که تمامی علاوه بر فضای دیتاسنتر سرورها و سوئیچ ها را نیز پوشش دهد.

[1] Amps

سامانه اطفاء حریق

آتش سوزی یکی از مسائلی است که احتمال وقوع آن در سامانه های برقی بسیار زیاد است، وقوع آتش سوزی

می تواند یک دیتاسنتر و اطلاعات آن را به طور کلی از بین ببرد، پس حفاظت از دیتاسنتر در برابر آتش سوزی از مسائل بسیار مهم دیتاسنتر است.

روش اطفاء حریق

اطفاء حریق در دیتاسنترها مانند اطفاء حریق در یک انبار یا اتاق معمولی نیست لذا از روش های معمولی نمی توان استفاده نمود و باید نازل های مواد اطفاء حریق با شدت مناسب و تنها به محل های منطقه کنترلی خود تابش داشته باشند، برای این مهم باید تنظیم دقیقی در منطقه بندی و انتحاب تجهیزات انجام شود، و بالاخص برای سرورها باید مراقب حساسیت تجهیزات به موارد رسانا نیز بود، بهتر است که سیستم اطفاء حریق دارای مخزن مرکزی باشد تا شارژ و بازبینی عامل اطفاء به سهولت ممکن باشد.

سامانه های امنیتی

گرچه در بحث امنیت دیتاسنتر، سامانه های کنترل محیطی و اطفاء حریق نیز از گروه تجهیزات امنیتی

محسوب می شوند اما برای راحتی در بررسی و پیاده سازی، آنها را در دو گروه جداگانه بررسی نموده ایم، در مبحث

سیستم های متمرکز امنیت دیتاسنتر، آنها را در دو مقوله بررسی ونیازسنجی می کنیم، ابتدا دوربین های مداربسته، دوم درب های الکترونیکی و کنترل تردد.

موارد زیر در مورد سیستم های متمرکز امنیت مورد نیاز می باشد:

- آرشیو فیلم های دوربین های مدار بسته باید حداقل برای مدت دوماه نگهداری شوند.
- دوربین ها باید فضای دیتاسنتر بالاخص اتاق سرور و شبکه را پوشش دهند .
- محل نصب دستگاه DVR ذخیره ساز در اتاق مانیتورینگ باید باشد.
- دوربین ها باید امکان مشاهده و مدیریت مرکزی و تحت شبکه و در عین حال امنیت بالایی داشته باشند.
- درب های اصلی دیتاسنتر و درب ورودی فضای سرور و شبکه باید از نوع گارد دار محکم فلزی با شاسی جاسازی شده در دیواره باشند.

- درب های اصلی دیتاسنتر و درب ورودی فضای سرور و شبکه باید دارای سیستم احراز هویت[1] تردد با ضرب انگشت یا کارت و رمز باشند.
- درب های اصلی دیتاسنتر و درب ورودی فضای سرور و شبکه باید از طریق قفل الکترونیکی باز و بسته شوند و برای زمان ضروری نیز دارای قفل و کلید مکانیکی باشند
- سیستم تردد اتاق سرور باید امکان گزارش گیری زنده و آرشیو ترددها را به صورت مستقل داشته باشد .درب های اتاق های دیگر دیتاسنتر نیز باید قابلیت گزارش دهی وضعیت باز و بسته بودن داشته باشند که در سامانه کنترل محیطی ذکر گردید.
- نرم فزارهای کاربردی این سامانه باید دارای امکان تهیه کاربر و تعیین سطوح دسترسی داشته باشند.
- عملکرد و گزارشات این سامانه باید قابل تنظیم بوده و از طریق شبکه به صورت امن قابل دسترسی و تغییر و تنظیم باشند.

سامانه های امنیتی دیتاسنتر نیز باید احتیاجات را برآورده نمایند در زیر به سامانه های امنیت فیزیکی دیتاسنتر اشاره می نماییم :

کنترل مجوز تردد درب ها

سامانه های کنترل تردد تجهیزاتی هستند که در ورودی و درب های دیتاسنتر متصل میگردند و چند نوع هستند گروهی توسط نشانه های حیاتی انسانی مانند چشم،ضرب انگشت یا تشخیص چهره عمل می کنند و گروه دوم با کارت های شناسایی مغناطیسی یا تماسی کار می کنند، پیشرفته ترین نوع سامانه های کنترل تردد ترکیبی از نوع نشانه های حیات انسانی و مغناطیسی هستند که علاوه بر باز و بسته کردن درب های تردد با مشخصه های انسانی، حضور افراد در هر کدام از مناطق دیتاسنتر را نیز به کمک کارت های مغناطیسی تشخیص می دهند که البته هزینه بیشتری به نسبت نمونه هایی که تنها کنترل تردد را انجام می دهند دارند.

دوربین مداربسته

برای ثبت فعالیت ها و چهره اشخاصی که در مناطق گوناگون دیتاسنتر حرکت و فعالیت می کنند ازسامانه های ثبت تصویری یعنی دوربین مدار بسته استفاده میشود. بدین صورت که این دوربین ها وقایع تصویری محیط دیتاسنتر را برای مدت مشخصی در حافظه خود یا یک سرور مشخص ثبت و نگهداری می کنند، تا در صورت نیاز مورد بازبینی قرار گیرند .البته این سامانه ها

[1] Authentication

نیز تنوع بسیاری دارند به عنوان مثال نمونه هایی از آنها فقط زمانی کـه Pattern منطقـه هـای اولیه آنها دچار تغییر می شود اقدام به ثبت فیلم می کنند .

دوربین تحت شبکه (Camera IP)

Network Camera دوربین تحت شبکه

Multiplexer مالتی پلکسر

DVR

شکل (۲ – ۵) دوربین و dvr و مالتی پلکسر تحت شبکه

استفاده از دوربین های تحت شبکه به علت بالا رفتن قابلیت های آن ها نسبت به گذشته روز به روز درحال افزایش است.

رزولیشن یا تفکیک پذیری

متفاوت از دوربین های آنالوگ که رزولیشن آن ها با تی وی لاین (TVL) مشخص مـی شـد ، تعداد خطوط افقی موجود در تصویر در دوربین ها ی تحت شبکه رزولیشن به پیکسن عنـوان مـی شود.

استفاده از دوربین های ۲ و ۳ مگاپیکسلی به صورت دوربین های شبکه به سرعت رایـج شـده و این دوربین ها

می توانند تصاویری به مراتب بهتر از دوربین های آنالوگ ارائه دهند. امروزه حتی دوربـین هـای شبکه با روزلیشن ۱۶ و ۲۰ مگاپیکسل نیز وجود دارد. این دوربین ها می توانند تصاویر را بـا تمـام جزئیاتشان نمایش دهند. دوربین های تحت شبکه عملکرد مناسبی در نور کم دارند .

عملکرد در شبکه

یکی از نگرانی های مهم مسئولان شبکه در مورد استفاده از دوربین های تحت شبکه تاثیر آن ها بر روی شبکه و کاهش سرعت آن است .چراکه به ویژه در دوربین رزولیشن بالا حجم زیادی از اطلاعات مربوط به دوربین باید در هر لحظه در شبکه جابه جا شود و با توجه به پهنای باند محدود شبکه این می تواند موجب ایجاد اختلال در شبکه نیز شود.

با این حال شبکه های گیگابایتی امروزی می توانند به راحتی نصب این دوربین ها را پشتیبانی کنند و در صورت ایجاد اختلال باید ظرفیت شبکه را افزایش داد .روش دیگر برای جلوگیری از ایجاد اختلال در شبکه استفاده از کابل های داده و عدم نصب مستقیم دوربین ها به شبکه است به طوری که تصاویر دارای شبکه خاص خود در سیستم باشند.

بیشتر دوربین های شبکه دارای قابلیت Power over Ethernet هستند ، به این معنا که می توانید دوربین را با همان کابل شبکه تغذیه کنید و این نیاز به یک کابل اضافه را جهت تغذیه دوربین از بین می برد.

در مقایسه با دوربین های آنالوگ که به یک کابل جداگانه برای تغذیه نیاز داشتند این قابلیت موجب صرفه جویی در زمان وهزینه کابل کشی خواهد شد.

داده ها بر روی کابل cat۵ دارای محدودیت مسافت تا ۱۰۰ متر هستند . با این حال تقویت کننده هایی وجود دارند که به راحتی این مسافت به ۲۰۰ متر افزایش می دهند . و با استفاده از تجهیزات پیچیده تر می توان این مسافت را تا ۵۰۰ متر نیز افزایش داد.

توجه داشته باشید که در هنگام نصب دوربین مدار بسته باید به تعداد دوربین های نصب شده توجه داشته باشید و امکان افزایش تعداد دوربین ها در آینده را نیز بدهید ، DVR را طوری انتخاب کنید که تعداد ورودی های آن از تعداد دوربین های نصب شده بیشتر باشد.

حسگر حضور فیزیکی

این سیستم ها جهت هشدار حضور شخص در ساعات غیر اداری به کار می روند و می توانند با سامانه های دوربین مدار بسته و کنترل روشنایی ترکیب شوند و در صرفه جویی مصرف برق کمک کنند . بدین صورت که اگر سیستم متوجه حضور فیزیکی مانند حرکت، منبع حرارتی و یا صدای غیر طبیعی شود ، هشدارها را فعال میکند.

اتاق سرور و شبکه

مرکز و قلب اطلاعاتی دیتاسنتر اتاق سرور است . همان گونه که از نام آن پیداست اتاقی است که مخصوص نصب سرورها تعیین شده است.

قلب ارتباطات دیتاسنتر اتاق شبکه است . همان گونه که از نام آن پیداست اتاقی است که مخصوص نصب سوئیچ ها و روترهای شبکه تعیین شده است، در این اتاق باید موارد زیر موجود باشند :

- سامانه کف کاذب برای رد کردن سینی و کابل های شبکه و کانال های ورودی دمش هوای سرد به زیر رک ها
- سقف کاذب برای نصب سیستم های روشنایی، رد کردن کابل های برق و سنسورهای محیطی و کانال های خروج هوای گرم از اتاق سرور
- سینی کابل در زیر کف کاذب برای تردد کابل ها و تقسیم آن ها
- لدر بالای سقف کاذب برای تردد کابل ها
- نصب رک های مناسب جهت سرور با استانداردهای دیتاسنتری
- درب های ضد حریق و سرقت و با قابلیت کنترل دیجیتال و ثبت تردد در سرورهای مرکزی
- سرمایش متمرکز که به صورت سرمایش در اتاق و سرمایش در رک ها طراحی میگردد
- روشنایی اتاق سرور نیز باید با توجه به محیط و متناسب، طراحی گردد و در میان راهروهای رک ها تعبیه گردد
- اطفاء حریق و کنترل شرایط محیطی که باید مناطقی را به تعداد رک ها در نظر گرفته و آنها را مانیتور نموده و وضعیت رطوبت حرارت و آتش در آن مناطق کنترل نماید و گزارشات را بصورت متمرکز در یک سرور ذخیره نماید.

دیوار پوش

سرتاسر دیوارهای اتاق شبکه و سرورها باید با دیوارپوش مناسب پوشیده گردد. دیوارپوش استاندارد دیتا سنتر باید این موارد را تضمین کنند : عدم انتقال گرمایی بین دیوار و هوای اتاق ، مقاومت در برابر آتش سوزی و عدم احتراق ، ضد گرد و خاک ، ضد الکتریسیته ساکن ، رنگ آن باید روشن باشد تا موجب هدر رفت نور محیطی نگردد ، ضد خش باشد.

کف کاذب

با توجه به این مساله که برخی از بخش های سامانه ها و تاسیسات اتاق سرور باید در زیر رک ها رد و یا نصب گردد، برای نصب رک های شبکه و سروری در اتاق باید کف کاذب[1] نصب و راه اندازی گردد. کف کاذب باید ۴۰ سانتیمتر از کف اصلی ارتفاع داشته باشد بدین صورت که تفاوت ارتفاع سطح بالا و سطح زیرین ۴۰ سانتیمتر باشد.

با توجه به اینکه کف برای انتقال کابل های شبکه در نظر گرفته شده است، در زیر کف کاذب باید از سینی کابل استفاده گردد.

شکل (۲ - ۶) کف های کاذب

کف کاذب باید این موارد را پوشش دهد :

ابعاد هر پوشش کف باید ۴۰*۴۰ یا ۶۰*۶۰ باشد ، جنس پوشش کف کاذب باید سبک بوده و به راحتی قابل برداشت و باز نصب باشد، ضد حریق باشد و در برابر حرارت و یا شعله مستقیم مشتعل یا دچار تغییر حالت نگردد، ضد الکتریسیته ساکن باشد، عایق در تبادل حرارتی، برق و گرد

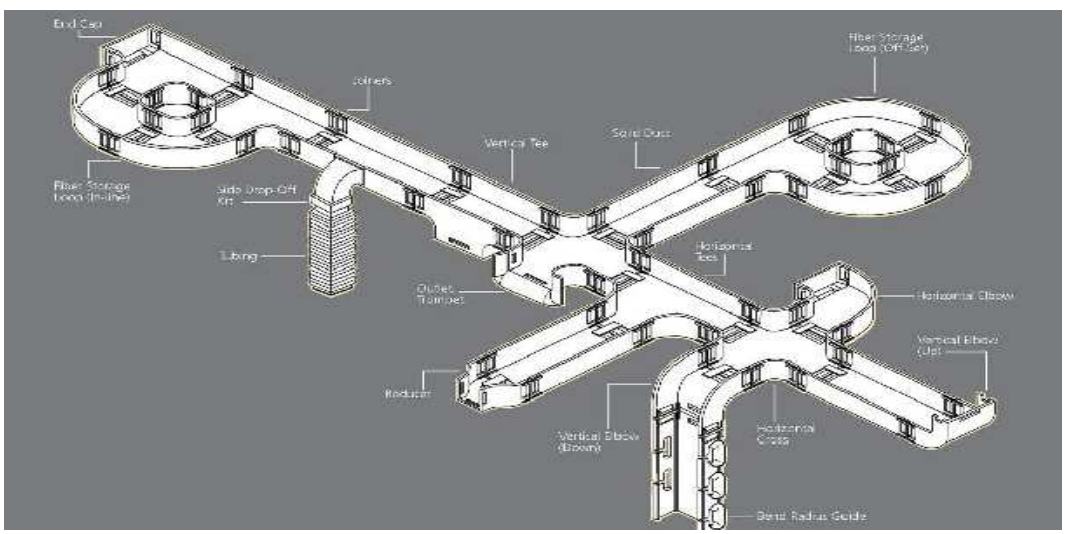
[1] False-faced

و خاک باشد، ضد خش باشد ، دارای توان مقاومتی مناسب در برابر فشار باشد و تحت فشار دچـار تغییر شکل نشود.

سینی انتقال کابل در زیر کف کاذب

در زیر کف کاذب برای انتقال کابل ها و فیبرهای نوری احتمالی از سینی کابل استاندارد استفاده میگردد، که سینی کابل مذکور باید دارای محل اتصال و بست برای اتصال کابل ها به بدنـه خـود و امکان قرار دادن اسپلیتر سینی وتقسیم فضای آن به چند فضای کنار هم بدون اختلاط کابل ها بـا یکدیگر برای مدیریت گروه های کابلی داشته باشد وپهنای آن حدود ۲۵ تا ۳۰ سانتیمتر باشد و در محل اتصال سینی کابل های رک های سروری به هر کدام از رک های شبکه باید پهنای سینی بـه حدود ۳۰ تا ۴۰ سانتیمتر برسد تا مدیریت کابل ها در آن راحت باشد، حداقل ارتفاع سینی نیز نیز باید۱۰ سانتیمتر باشد، بعلاوه سینی مذکور باید از جنس نسوز، ضد الکتریسیته ساکن و بایـد بـا گراند الکتریکی باشد و با اتصالات محکم به کف اتاق متصل گردد.

شکل زیر نمونه سینی که برای که برای فیبر کاربرد دارد را نشان می دهد :



شکل (۲ – ۷) سینی انتقال کابل

لدرهای سقفی

برای انتقال کابل های برق رک ها و تاسیسات روشنایی باید در سقف لدرهایی نصب گردد و این کابل ها از روی آن منتقل گردند، این لدرها دورادور سقف اتاق را پوشش داده و امکان انتقال کابل را راحتتر مینماید.

شکل (۲ – ۸) لدر سقفی

این لدرها باید موارد زیر را پوشش دهند :

- لدرها باید در سقف و دیوارها بصورت محکم نصب شوند.
- لدرها باید سبک باشند.
- لدرها باید در برابر حرارت مقاوم باشند.
- برای انتقال کابل ها به رک باید دارای ستون DownFall تا سقف رک باشند.
- در محل خمش ها باید از زانوهای خمش استفاده گردد
- در محل DownFall کابل ها از لدر باید از ایزولاتور استفاده گردد تا موجب ورود گرد و خاک احتمالی سقف به فضای دیتاسنتر و یا هدر رفت دمایی نشود.

رک های شبکه ای

اتاق سرور و شبکه محل قرار گرفتن رک های شبکه می باشد در این رک ها سوئیچ ها ، روترها و دیواره های آتش شبکه قرار می گیرد .با توجه به وظایف مذکور، این رک ها باید موارد زیر را پوشش دهند :

- امکان نصب انواع تجهیزات استاندارد رک
- دارای فن روف مجزا از بدنه در سقف برای جلوگیری از ورود گرد و غبار به سیستم و فن و امکان هدایت هوای دمیده شد از زیر رک به درون رک و جلوی سرورها و تجهیزات و خروج هوای گرم از پشت سرورها و تجهیزات
- رنگ بدنه ضد الکتریسیته ساکن و حریق باشد

- مجهز به سیستم ارت بدنه مناسب
- دارای فضای ورودی کابل زیاد از زیر رک و بالای رک
- دارای قاب متحرک برای فن جهت سهولت تعویض از بیرون بدون جابجایی تجهیزات
- مجهز به فیلتر قابل تعویض در کف جهت تصفیه هوا و افزایش عمر تجهیزات
- دارای فیلتر مناسب جهت پوشش ورودی -خروجی کابل های رک در برابر گردوخاک و هدررفت جریان هوا
- با توجه به دمش هوای خنک به درون رک ها، باید رک ها عایق حرارتی باشند و هوای خنک موجود در رک با هوای گرم بیرون تبادل نشود
- درب با قفل دیجیتال رمزدار
- اولین رک که به رک Rack-Net-۱ معروف است رک ورودی کابل های بیرونی و مخابراتی است ، که باید در آن دو سینی فیبر رکمونت مناسب وجود داشته باشد، کابل های شبکه از نودهای دیواری اتاق های مانیتورینگ، تاسیسات و تجهیزات نیز باید در یک پچ پانل در همین رک نصب گردند و دقیقاً شماره گذاری گردند
- در رک دوم که به Rack-Net-۲ موسوم است و برای ورود کابل های شبکه رک های سروری پیشبینی شده است.
- داشتن Splitter فضا بین خروجی هوا و کابل جهت جلوگیری از حرارات دیدن کابل ها و هدایت کننده دمنده جهت هدایت هوای گرم به سمت کانال های مکنده سقفی
- در هر رک حداقل باید ۲ پاور ۱۲ تایی وجود داشته باشد و از ۲ ups مجزا برق خود را تغذیه کنند
- سقف رک ها دارای حد اقل ۸ فن و کف رک جهت انتقال باد بصورت باز باشد، امکان انتقال کابل به تعداد از زیر و بالای رک ها وجود داشته باشد
- مهار کابل ها و فیبرها به بدنه رک ، توسط بست های قفل دار پلاستیکی باشد و با هلدرهای مناسب کابل ، انتقال کابل ها در درون رک صورت پذیرد.
- از اتیکت های چاپی چسبی باید در هر دو سر کابل ها استفاده گردد

رک های سروری

با توجه به ماموریت نگهداری از سرورها توسط دیتاسنتر لازم است رک مناسب جهت این ماموریت تهیه گردد که مشخصات ان تقریبا با رک های شبکه ای تفاوتی ندارد و معمولا از نظر اندازه ها با هم متفاوتند.

کابل های شبکه

می دانید که بحث شبکه در داخل دیتاسنتر و بالاخص بین سرورها و سوئیچ هـای هـسته Core بحثی مجزا از شبکه Access و با حساسیت بالایی میباشد .لذا بایـد برنـد تمـامی PatchPanel و کابل ها از یک نوع استفاده گردد و قابلیت انتقال بدون نویز را داشــته باشــند . ارتبــاط هــای بــین سرورها و سوئیچ ها باید ویژگی های زیر را داشته باشند :

- بین رک شماره ۱ تا سرورها کابل کشی STP-Cat۶ صورت پذیرد و کابل ها از سینی کف کاذب رد شوند.
- کابل های کشیده شده به اندازهای پیش بینی شوند که امکان مانور داشته و در صورت نیاز به جابجایی پچ پانل، بتوان آن را جابجا نمود.
- برای ورود کابل های شبکه رک های سروری در هر رک سروری پچ پانـل هـای مجـزا بـا تعداد پورت های بالا نصب شود و نگه دارنده و قلاب کابل مناسب باید در نظر گرفته شود.
- کابل ها باید در روی سینی بصورت مناسب دسته بندی شوند و با بست در فواصل مناسب بسته شوند تا برای عیب یابی در آینده مشکل نداشته باشد.
- رنگ بندی کابل ها برای هر رک باید متفاوت باشد تا در مسیر نیز به خـوبی از هـم قابـل تشخیص باشند
- در دوسر کابل های شبکه باید علامت گذاری شود که معرف رک، پچ پانل و شماره نود آن کابل باشد

جنس رک

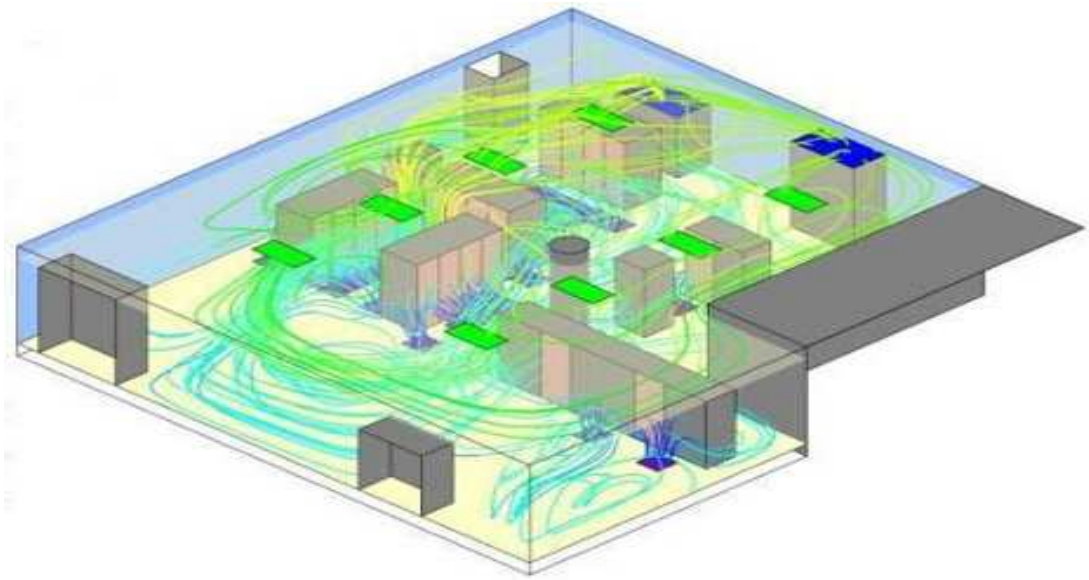
رک ها باید از جنس فولاد مرغوب باشند و چهارچوب آنها نیز در برابر فشار مقاوم باشد و به سبب بار دچارانحراف نگردد، درب های اطراف رک به استثنای درب جلو و عقب بایـد فلـزی باشـد، درب های جلو و عقب نیز باید ازجنس شفاف ضد حریق و آنتی الکترواستاتیک باشند .در محـل اتـصال درب ها به بدنه نیز از واشرهای عایق استفاده شود تا انتقال دما و گرد و خاک بین فضاهای بیرون و داخل رک وجود نداشته باشد .جنس درب ها شیشه ای باید از تلق شفاف و نشکن باشد که در برابر آتش و تغییر دما مقاوم باشد و عایق حرارتی نیز باشد.

ساختار شبکه و کابل کشی ها

کابل و فیبرهای شبکه در دیتاسنترها مانند سلسله اعصابی هستند که بدنه و بازوهای عملیاتی را به یکدیگر و به هسته فرماندهی دیتاسنتر متصل میکنند لذا باید این سیستم عصبی در هـر بخـش

بسته به کارایی و عملیاتی که به عهده دارد ویژگی های خاص خود را داشته باشد و به سلامتی کار کند.

شکل زیر نمای سه بعدی از کابل کشی دیتاسنتر را نشان می دهد :



شکل (۲ – ۹) نمای سه بعدی از کابل کشی دیتاسنتر

برای این منظور باید موارد زیر را مدنظر داشت:

- کابل کشی در اتاق سرور و شبکه کابل های برق باید از کابل های شبکه مجزا کشیده شوند و بر هم پوشانی نداشته باشند تا موجب کندی سرعت ارتباط شیکه نشوند.
- شکستگی در کابل ها و فیبرها نباید بیشتر از حد مجاز باشد، همانطور که می دانید شکست و خمش در کابل ها و فیبرها نباید ازاستانداردها بیشتر شود چون شکستگی بیش از حد موجب کندی سرعت انتقال در کابل ها می شود .
- در زیر کف کاذب باید سینی کابل وجود داشته باشد و به دو بخش تقسیم شود که یکی جهت رد کردن فیبرها و یکی برای ردکردن کابل های شبکه مسی باشد، بعلاوه کابل ها تا حد ممکن نباید بصورت ضربدری از روی هم رد شوند.
- دوسر کابل ها به صورت رمزی نامگذاری شود، طوری که نام قرار داده شده بر روی هر سر کابل نشان دهنده رک و گره طرف مقابل آن باشد، اما نباید نامگذاری به شکلی باشد که برای همگان درک آن ساده باشد و یا از نام های طولانی استفاده شود وبرای اتصال نام ها به کابل باید از برچسب های استاندارد دو سر کابل استفاده گردد.

- رنگ بندی کابل ها در دیتاسنتر باید به شکلی باشد که نشان دهنده عملیاتی که آن کابل به عهده دارد باشد .مثلاً رنگ زرد برای ارتباط بین رک های شبکه تا سرور ها استفاده شود و رنگ قرمز برای ارتباط بین شبکه بیرونی و سوئیچ ها یا روترها استفاده شود و از رنگ سبز برای ارتباط داخلی بین سوئیچ های شبکه دیتاسنتر استفاده شود و از کابل آبی برای ارتباط با سامانه های تاسیساتی و امنیتی استفاده نمایند و کابل های خاکستری برای اتصال بین اتاق های مانیتورینگ وتجهیزات با دیتاسنتر استفاده گردد.
- رک های ورودی کابل و فیبر به دیتاسنتر از رک های داخلی و تجهیزات شبکه مجزا گردد تا مدیریت آن ها راحتر باشد.
- حتماً برای فیبرها از سینی فیبر، استفاده گردد.

شکل زیر نمایی از دیتا سنتر اختصاصی وب سایت فیس بوک را نشان می دهد :

شکل (۲ – ۱۰) دیتا سنتر اختصاصی وب سایت فیس بوک

جمع بندی

در این فصل سعی شد که مخاطب دیتا سنتر یا اتاق سرور را شناخته و مسائل امنیتی را در راه اندازی یک دیتاسنتر به کار گیرد زیرا اولین واصلی ترین قسمت امنیت شبکه ، بخش فیزیکی آن است .

فصل سوم
تجهیزات شبکه و بررسی آن ها

مقدمه

در فصل های قبل با دیتا سنتر و راه های امنیت فیزیکی آن آشنا شدید. همانطور که گفته شد دیتا سنتر محل اصلی نگهداری تجهیزات شبکه است . دیتا سنتر را سخت افزار های مهمی مانند سوییچ ، روتر ، فایروال و ... تشکیل می دهند که برای راه اندازی یک شبکه بزرگ وامنیت آن به این سخت افزارها نیازمندیم.

شرکت های متفاوتی در جهان تجهیزات شبکه را تولید می کنند که هر کدام پروتکل ها و سیستم عامل و همچنین امنیت مربوط به خود را مد نظر قرار می دهند.

پروتکل به قوانینی گفته می شود که هر شرکت نسبت به این قوانین محصولات خود را ارائه می دهد.

در این فصل سعی شده است تجهیزات شبکه وشرکت های سازنده آن ها را توضیح ودر مورد امنیت آن ها بحث شود.

ابتدا شرکت معتبر سیسکو را که در زمینه تجهیزات شبکه فعالیت می کند را مورد بررسی قرار می دهیم و بعد تجهیزاتش را از جنبه های مختلف مورد بررسی قرار می دهیم .

در این فصل بیشتر در مورد تجهیزات سیسکو بحث می کنیم زیرا بیشترین درصد استفاده را میان برندهای مختلف در زمینه شبکه دارد.

تجهیزات شبکه و شرکت های سازنده

سوییچ

Switch برای اتصال دستگاهای مختلف از قبیل رایانه , مسیریاب , چاپگرهای تحت شبکه , دوربین های مدار بسته و .... در شبکه های کابلی مورد استفاده واقع می شود.

در وجه ظاهری switch همانند جعبه ایست متشکل از چندین درگاه اترنت[۱] که از این لحاظ شبیه Hub می باشد, با وجود آنکه هر دو این ها وظیفه برقراری ارتباط بین دستگاه های مختلف را بر عهده دارند , تفاوت از آنجا آغاز می شود که Hub بسته های ارسالی از طرف یک دستگاه را به همه ی درگاه های خود ارسال می کند و کلیه دستگاه های دیگر علاوه بر دستگاه مقصد این بسته ها را دریافت می کنند در حالیکه در Switch ارتباطی مستقیم بین درگاه دستگاه مبدا با درگاه دستگاه مقصد برقرار شده و بسته ها مستقیما فقط برای آن ارسال می شود. در Switch های معمولی که به سوییچ لایه۲ [۲]معروفند این پردازش تا لایه دوم مدل OSI پیش می رود و نتیجه

[۱] Ethernet
[۲] Layer switch۲

این پردازش جدولی است که در Switch با خواندن آدرس سخت افزاری (MAC) فرستنده بسته و ثبت درگاه ورودی تشکیل می شود. برای استفاده در شبکه های lan چون شبکه گستردگی بالایی ندارد ، معمولا از سوییچ های لایه ۲ استفاده می کنند .

پرکاربردترین Switch در بین لایه های مختلف بجز لایه دوم می توان به Switch layer۳ اشاره کرد که در بسیاری از موارد جایگزین مناسبی برای روتر می باشند.

از Switch می توان در یک شبکه خانگی کوچک تا در شبکه های بزرگ با Backbone [۱]های چند گیگابایتی استفاده کرد.

سوئیچ ها از لحاظ ساختار داخلی درست مثل یک کیس کامپیوتری کامل می ماند.این دستگاه ها همانند کیس دارای سخت افزارهایی چون RAM, CPU,FLASH(Hard) است .و از لحاظ نرم افزار نیز دارای سیستم عامل است که سیستم عامل آن معروف به IOS می باشد.

سوییچ ها پروتکل های زیادی را پشتیبانی می کنند که در این فصل سعی شده پروتکل هایی را توضیح دهیم که از نظر امنیتی مورد استفاده قرار می گیرند.

شکل (۳ – ۱) نمایی از سوییچ

بعضی از خصوصیات سوییچ ها

- می توان با دادن IP از هرجای شبکه به آنها وصل شد Telnet
- می توان ترافیک شبکه را به بهترین نحو کنترل کرد
- می توان به افراد خاصی اجازه دسترسی داد
- می توان پورت هایی را که لازم نداریم خاموش کنیم وامنیت را بالاتر ببریم
- تعریف وپیاده سازی NAT [۲]
- پیاده سازی پارامترهای امنیتی

[۱] ستون فقرات

[۲] Network Address Translation

- تشخیص نوع کابل استفاده شده از لحاظ هم بندی CRoss Over یا معمولی
- تعریف Vlanهای متعدد و تقسیم بندی شبکه به Lan های مجازی زیاد
- سرعت بالا ، اطمینان ،معتبربودن شرکت تولیدکننده ، وامکانات بالا

نباید از امنیت فیزیکی سوییچ ها غافل شد زیرا با دسترسی به این دستگاه می توان به شبکه نفوذ کرد و سیستم ها را از کار انداخت.

روتر

اگر روتر را بخواهیم از نظر لغوی معنا کنیم می توانیم به آن مسیر یاب بگوییم. روتر ها یا مسیر یاب ها تجهیزات فیزیکی هستند که چندین شبکه بی سیم یا کابلی را به یکدیگر متصل می کنند. و این همان تجهیزی است که در اینترنت مشخص می کند بسته های اطلاعاتی از کدام مسیر به مقصد برسند و در نهایت رسیدن آن به مقصد را کنترل می کند از نظر فنی یک روتر یک گذرگاه لایه ۳ است یعنی روتر های کابلی یا بی سیم شبکه ها را مانند یک گذرگاه به یکدیگر متصل می نمایند و این لایه همان لایه در مدل معروف شبکه یا مدل OSIاست.

روتر یک نوع کامپیوتر خاص است که دارای عناصر مشابه یک کامپیوتر استاندارد شخصی نظیر پردازنده ، حافظه ، خطوط داده و اینترفیس های مختلف ورودی و خروجی است. روترها به منظور انجام عملیات بسیار خاص که عموما" نمی توان آنان را توسط کامپیوترهای شخصی انجام داد ، طراحی شده اند . مثلا" با استفاده از روتر می توان دو شبکه را به یکدیگر متصل تا در ادامه امکان مبادله اطلاعات بین آنان فراهم گردد . روتر ، همچنین بهترین مسیر ارسال داده از یک شبکه به شبکه ای دیگر را تعیین می نماید. مهمترین استفاده روتر در شبکه های wan است.

شکل زیر نمایی از روتر ۲۸۱۱ شرکت سیسکو را نشان می دهد :

شکل (۳ – ۲) نمایی از روتر

ویژ گی های عمومی روتر ها

تمام روتر ها کامپیوتر های موجود در شبکه را به یکدیگر و نیز به اتصال اینترنتی وصل می کنند . صرف نظر از این وظیفه ی عمومی روترها ویژگی های دیگری نیز دارنـد :دیـواره ی آتـش تعبیـه شده: چنین ویژگی به شما اجازه می دهد کـه در شـبکه تـان تنهـا از یـک آدرس Ipبـرای اتـصال اینترنتی استفاده نمایید .بزرگترین مزیت امنیتی روش فوق این است که کاربران می توانند منـابع شبکه شان را به اشتراک بگذارند بی آنکه سایر کامپیوتر هـا ی موجـود دراینترنـت از حـضور آنهـا مطلع شوند . البته سایرین می توانند به آدرس Ip روتر دسترسی داشته باشـند ولـی بـرای یـافتن آدرس Ip تک تک کامپیوتر ها باید وقت بسیاری را صرف نمایند.اتصال بی سـیم : یکـی از مزایـای دیگر روتر ها امکان برقراری اتصالات بی سیم می باشد.

زمانی که روتر داده ای را از طریق یک شبکه و یا اینترنت دریافت مـی نمایـد ، پـس از بررسـی آدرس مبداء و مقصد ، داده دریافتی را برای هر یک از شبکه ها و یا اینترنت ارسال می نماید .

روتینگ (Routing) یکی از مهمترین ویژگی های مورد نیاز در یک شبکه به منظور ارتباط بـا سایر شبکه ها است. در صورتی که امکان روتینگ پروتکل ها وجود نداشته باشد ، کامپیوترها قـادر به مبادله داده نخواهند بود.

از روتینگ به منظور دریافت یک بسته اطلاعاتی (packet) از یک دستگاه و ارسال آن از طریق شبکه برای دستگاهی دیگر و بر روی شبکه ای متفاوت ، استفاده می گردد . در صورتی کـه شـبکه شما دارای روتر نباشد ، امکان روتینگ داده بین شبکه شما و سایر شبکه ها وجود نخواهد داشت . یک روتر به منظور مسیریابی یک بسته اطلاعاتی ، می بایست آگاهی لازم در خصوص اطلاعات زیر را داشته باشد:

- روترهای مجاور که با استفاده از آنان امکان اخذ اطلاعات لازم در خصوص شبکه های از راه دور، فراهم می گردد.
- مسیرهای موجود به تمامی شبکه های از راه دور
- بهترین مسیر به هر یک از شبکه های از راه دور
- نحوه نگهداری و بررسی اطلاعات روتینگ

پروتکل های روتینگ به منظور استفاده در روترها ، ایجاد شده اند . پروتکل هـای فـوق ، بـدین منظور طراحی شده اند که امکان مبادله اطلاعات جداول روتینـگ بـین روترهـا را فـراهم نمایـد . تاکنون پروتکل های متفاوتی به منظور استفاده در شبکه هائی با ابعاد گوناگون ، طراحـی و پیـاده سازی شده است.

دراین فصل پروتکل هایی را که در بحث امنیت کاربرد دارند را مورد بررسی قرار می دهیم.

فایر وال

اگر از اینترنت استفاده می‌کنید، و بخصوص اگر در یک شرکت بزرگ کار می‌کنید که در حین کار به اینترنت متصل هستید حتما نام فایروال را شنیده اید. شما می‌توانید با استفاده از فایروال از شبکه خود در مقابل وب سایت های خرابکار و هکرها محافظت نمایید. یک فایروال در حقیقت حصاری است که نیروهای خرابکار را از شما دور نگه می‌دارد. به همین دلیل به آن فایروال (دیوار آتش) گفته می‌شود. کار این حصار شبیه یک دیوار آتش فیزیکی است که از گسترش آتش از از یک ناحیه به ناحیه دیگر جلوگیری می‌کند.

کارهایی که یک فایروال انجام می دهد:

یک فایروال یک برنامه یا یک وسیله سخت افزاری است که اطلاعاتی را که از طریق اینترنت به شبکه یا کامپیوتر شما وارد و یا از آن خارج می‌شود، بررسی و درصورت نیاز فیلتر می‌کند. یک فایروال یک وسیله سخت افزاری است که اطلاعاتی را که از طریق اینترنت به شبکه یا کامپیوتر شما وارد و یا از آن خارج می‌شود، بررسی و درصورت نیاز فیلتر می‌کند. اگر بسته ای که در حال ورود به شبکه شماست بعنوان بسته فیلتری برچسب بخورد، دیگر اجازه ورود به شبکه شما را نخواهد داشت. فرض کنید که شما در شرکتی با چند صد کارمند کار می‌کنید. این شرکت چند صد کامپیوتر دارد که از طریق کارت شبکه به هم متصل هستنند. همچنین این شرکت از یک یا چند اتصال به اینترنت استفاده می کند. بدون استفاده از فایروال تمامی این کامپیوترها از طریق اینترنت برای هرکسی قابل دسترسی هستند. هر فردی خارج از شبکه شما که می‌داند چه کاری باید انجام دهد، می‌تواند با این کامپیوترها اتصال FTP[1] ، telnetو غیره برقرار کند. اگر یکی از کارمندان اشتباهی مرتکب شده و یک حفره امنیتی را باز بگذارد، هکرها می‌توانند به سیستم او وارد شده و از حفره امنیتی موجود سوء استفاده نمایند. اما در مقابل با استفاده از یک فایروال، اتفاق کاملا متفاوتی رخ می دهد. شرکت در سر راه هر اتصالی به اینترنت یک فایروال قرار می-دهد. فایروال می‌تواند قوانین امنیتی را پیاده کند. برای مثال یکی از قوانین امنیتی یک شرکت می‌تواند این باشد: از میان ۵۰۰ کامپیوتر شرکت، فقط یکی حق دارد ترافیک FTP را دریافت نماید. یک شرکت می‌تواند چنین قوانینی را برای سرورهای FTP ، سرورهای وب، سرورهای Telnetو مانند آن اختصاص داده و تعریف نماید. بعلاوه یک شرکت می‌تواند در مورد نحوه اتصال کارمندان به وب سایت ها و اینکه آیا فایل ها مجوز خروج از شبکه شرکت را دارند یا خیر، کنترل های لازم را اعمال نماید. یک فایروال کنترل مناسبی بر روی نحوه استفاده کارمندان از شبکه ایجاد

[1] file transfer protocol

می‌کند. فایروال ها با استفاده از حداقل یکی از روش های زیر، ترافیک ورودی و خروجی شبکه را کنترل می‌کنند:

فیلتر کردن بسته ها

بسته های داده بر اساس مجموعه ای از فیلترها تحلیل می‌شوند. بسته هایی که مجوز داشته باشند وارد شده و بقیه رد می‌شوند.

سرویس

اطلاعات دریافتی از اینترنت ابتدا توسط فایروال دریافت شده و سپس به سیستم درخواست کننده ارسال می‌شوند و برعکس.

تفتیش[۱]

روشی جدید که محتویات هر بسته را بررسی نمی‌کند و به جای آن، بخش های کلیدی مشخصی از بسته ها را با یک پایگاه داده مطمئن مقایسه می‌نماید. اطلاعاتی که از درون فایروال به بیرون می‌روند، از لحاظ برخی ویژگی ها بررسی و کنترل شده و اطلاعات ورودی با این ویژگی ها مقایسه می‌گردند. اگر تطابق معنا داری بین این دو دسته وجود داشته باشد، آنگاه اطلاعات اجازه ورود را خواهند داشت و در غیر اینصورت رد می‌شوند.

فایروال های سخت افزاری

این نوع فایروال ها که به آن فایروال شبکه نیز گفته می‌شود، بین کامپیوتر (یا شبکه) شما و کابل یا خط DSL[۲] قرار می گیرند. تعداد زیادی از تولید کنندگان و برخی از مراکز ISP[۳] ، مسیریاب هایی ارائه می دهند که دارای یک فایروال نیز می‌باشند. فایروال های سخت افزاری معمولا در مواردی که قصد حفاظت از چندین کامپیوتر را داشته باشید مفید بوده و یک سطح حفاظتی مناسب را ارائه می‌نمایند (بدیهی است که امکان استفاده از این فایروال ها به منظور حفاظت از یک دستگاه کامپیوتر نیز وجود دارد). در صورتی که شما صرفا یک کامپیوتر پشت فایروال قرار داده اید و یا این اطمینان را دارید که سایر کامپیوتر های موجود بر روی شبکه، از لحاظ نصب تمامی اصلاحیه ها به روز بوده و عاری از هرگونه بدافزاری می‌باشند، نیازی به استفاده از یک نرم افزار فایروال نخواهید داشت. فایروال های سخت افزاری، دستگاه های سخت افزاری مجزائی هستند که دارای سیستم عامل اختصاصی خود می‌باشند و استفاده از آنها باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می گردد.

---

[۱] Inspection
[۲] Digital Subscriber Line
[۳] Internet service provider

شرکت های ارائه دهنده تجهیزات شبکه

اسم «سیسکو» مخفف سانفرانسیسکو است. زوجی که در بخش کامپیوتر دانشگاه استنفورد کار می کردند، Cisco را در سال ۱۹۸۴ تأسیس کردند.

این شرکت محصولات مربوط به شبکه و ارتباطات را طراحی می کند و محصولات خود را با سه نام تجاری: سیسکو، لینک سیس(linksys) و ساینتیفیک آتلانتا (scientific atlanta) به فروش می رساند. شرکت سیسکو در سال ۲۰۰۳ موفق به دریافت جایزه ریاست جمهوری "ران براون" برای کیفیت عالی در روابط کارمندان و جامعه گردید. با وجود این که سیسکو نخستین شرکتی نبوده که مسیریاب طراحی و تولید می کند، اما اولین شرکتی بود که یک مسیریاب چند پروتکل موفق تولید کرده که اجازه ارتباط میان پروتکل های گوناگون شبکه را می دهد از زمانی که پروتکل اینترنتip به یک استاندارد تبدیل شد، اهمیت مسیریاب های چند پروتکل کاهش یافت. امروزه بزرگترین مسیریاب های سیسکو برای هدایت بسته های ip و فریم هایmpls طراحی شده اند. در ۱۹۹۰ ، شرکت به سهامی عام تبدیل شد و سهام آن در بازار بورسnasdaq عرضه گردید. زمان انفجار اینترنت در ۱۹۹۹، سیسکو شرکت سرنت (cerent) واقع در کالیفرنیا را به قیمت ۷ میلیارد دلار خرید. این شرکت گرانترین خرید سیسکو در آن زمان بود (تنها خرید گرانتر مربوط به ساینتیفیک آتلانتا است). در اواخر مارس۲۰۰۰، سیسکو با ارزش مالی بالغ بر ۵۰۰ میلیارد دلار ارزشمندترین شرکت جهان به شمار می آمد و در سال ۲۰۰۷، با ارزشی بالغ بر ۱۶۵میلیارد دلار همچنان یکی از ارزشمندترین شرکت ها بوده است.سیسکو با خرید شرکت های دیگر، توسعه داخلی و همکاری با دیگر شرکت ها، به بازار بسیاری از دیگر قطعات شبکه (مانند سوییچینگ اترنت (ethernet)، دسترسی از راه دور، مسیریاب های شعبه ای، شبکه خودپرداز بانک ها (atm)، امنیت، دیواره آتش، تلفن اینترنتی و ...) دست یافته است. در سال ۲۰۰۳، سیسکو شرکت خوشنام لینک سیس، تولیدکننده سخت افزار شبکه های کامپیوتری را خرید و آن را به برترین تولیدکننده قطعات مربوط به کاربران عادی تبدیل کرد. سیسکو و برگزاری دوره های شبکه ای شرکت سیسکو مدارک گوناگونی را در سطوح و شاخه های متفاوتی ارایه می کند. هر کدام از مدارک سیسکو، حوزه خاصی از مفاهیم شبکه ای را پوشش می دهد. سیسکو برای معرفی بهتر سطوح مدارک خود، هرم هایی را ترسیم کرده است که در راس هر یک از آنها، بالاترین مدرک و در قاعده هرم، مدرک ورودی شرکت بیان شده است. سیسکو و مدارک آن بر پایه استانداردهای عالی و بین المللی بنا نهاده شده و بنابراین اخذ هر یک از مدارک سیسکو، چه برای متخصصان و مدیران شبکه و چه برای شرکت ها و سازمان هایی که قصد استخدام افراد متخصص را دارند، ارزشمند است. سیسکو به منظور تعلیم افراد برای طراحی و نگهداری شبکه های کامپیوتری در ۱۵۰ کشور جهان مراکز

آموزشی بر پا کرده است. مدارک شرکت سیسکو در سه سطح به دانـشجویان عرضـه مـی گـردد و گذراندن هر سطح پیش نیاز تحصیل در سطوح بالاتر سطح است.

مقایسه سیسکو با برندهای مختلف

شرکت های متعددی در ساخت و راه اندازی تجهیزات شبکه فعالیت می کنند مانند :
(cisco,foundry,hp,۳com,dellو...)

برای مقایسه دو محصول تجاری مورد نظر، می بایست شاخص های ارزیابی مشخص شوند.در زیر شاخص هایی که برای مقایسه دو برند در درجه اول اهمیت قرار دارند آورده شده است:

- مستندات فنی (راهنمای استفاده، تعمیر و نگهداری)
- سیستم عامل تجهیزات(... ,IOS, Firmware)
- تعداد شرکت های پشتیبانی کننده تجهیزات در کشور
- تعداد متخصصین تجهیزات حاضر در کشور
- مراکز آموزش ارائه دهنده آموزش های تجهیزات
- مراکز تعمیر سخت افزاری تجهیزات
- فرایند پیکربندی، به روز رسانی و نگهداری تجهیزات
- ابزارهای مدیریت تجهیرات
- یکپارچگی با شبکه WAN[۱]
- ویژگی های امنیتی
- هزینه

تحلیل برخی از شاخص های بالا

مستندات فنی (راهنمای استفاده، تعمیر و نگهداری)

در مقایسه ای که بین ابزار و مستنداتی که توسط دو شـرکت Cisco و Foundry در رابطـه بـا محصولات تولیدی خود ارائه داده اند ، Ciscoبالاترین رتبه را کسب کرده اسـت ، بطوریکـه بـرای تمام تجهیزات خود اعم از سوئیچ های رده بالا تا تولیدات ماجول ها و کابل ها نیز مـستندات فنـی همراه با فرمت pdf ارائه داده است.همچنین لینکی برای استفاده کاربران در سایت خـود قـرار داده است که افراد می توانند تجهیز خود را در آنجا انتخاب و ماجول ها و نرم افزارهای مورد نیاز خود را انتخاب نمایند، در صورتیکه ماجول و یا نرم افزاری را اشتباه انتخاب نماینـد، ایـن ابـزار بـه کـاربر

[۱] Wide Area Network

اشتباه صورت گرفته را اعلام می نماید و طریقه صحیح پیکربندی و طراحی را اعلام می کند. همچنین اگر کاربر خواهان انتخاب نرم افزار با مشخصات خاصی باشد، ابزاری در این رابطه وجود دارد که به شما امکان انتخاب نرم افزار را بر اساس ویژگی مورد نظر می دهد. از دیگر ابزارهای سیسکو unit license calculator جهت انتخاب لایسنس نرم افزار IP Phone ، Power Calculatorبرای انتخاب میزان پاور روی سوئیچ ، ابزارهای طراحی شبکه و غیره می باشد.چنین امکاناتی در Foundry موجود نمی باشد.

شرکت های پشتیبانی کننده تجهیزات در کشور

در کشور ایران ارائه و پشتیبانی محصولات سیسکو به صورت گسترده توسط حداقل ده شرکت قدرتمند انجام می‌شود در مقابل کمتر از سه شرکت به صورت حرفه‌ای و تخصصی روی محصولات فاندری فعالیت می‌نمایند. لذا امکان جایگزینی شرکت خدمات دهنده و نیز رقابت میان شرکت‌های ارائه دهنده تجهیزات سیسکو به مراتب بیشتر است. بدیهی است که همواره رقابت موجب ارتقای سطح ارائه خدمات به مصرف کننده نهایی خواهد شد.

همچنین به دلیل اینکه این تجهیزات می بایستی از خارج از کشور تامین گردند و جهت وارد نمودن این تجهیزات و استفاده از آن ها به دلیل تحریم بودن ایران معمولاً مشکلات زیادی وجود دارد، لذا هر چقدر که تعداد تامین کنندگان داخلی این تجهیزات بیشتر باشند، امکان خرید و استفاده از آن ها آسانتر می شود.

متخصصین در کشور

در حال حاضر در کشور ایران تعداد متخصیص و کارشناسان سیسکو بسیار بیشتر از فاندری می باشند این مساله به دلایل زیر می باشد:

۱. شرکت سیسکو تنوع دوره آموزشی بیشتری دارد. دوره های آموزشی در گرایش های Swithing/Routing، IP Telephony، Security، نرم افزارهای مدیریت و غیره که در هر گرایش از سطح کارشناسی تا حرفه ای دوره برگزار می نماید، در ایران تمامی این دوره ها به دلیل در دسترس بودن کتاب و مرجع آن ها برگزار می گردد.

۲. به دلیل اینکه تعداد شبکه هایی که با تجهیزات سیسکو راه اندازی شده اند و همچنین تعداد شرکت هایی که محصولات سیسکو را ارائه می دهند، نسبت به فاندری بیشتر می باشند لذا افراد بیشتری در این زمینه مشغول به کار می شوند.

مراکز تعمیر سخت افزاری تجهیزات

مراکز متعددی در ایران وجود دارند که در زمینه تعمیرات سخت افزاری تجهیزات Cisco فعال می باشند. این مراکز اشکالات اولیه‌ای همچون تعمیر منبع تغذیه،تعویض برخی IC های روی برد تجهیزات و نیز تعمیر و تعویض دیگر قطعات را انجام می‌دهند. با اتکا به این مراکز می‌توان ضریب در دسترس بودن شبکه را افزایش داد. هنوز مراکز تعمیر اختصاصی برای تجهیزات Foundry وجود ندارد که در نتیجه در صورت خراب شدن برخی قطعات یا کل تجهیزات باید برای تعمیر می بایستی به خارج از کشور ارسال گردند که این مساله مستلزم صرف هزینه و زمان می باشد.

فرآیند پیکربندی، به روز رسانی و نگهداری تجهیزات

پیکربندی و نگهدای تجهیزات Foundry و Cisco تقریبا یکسان است. شکل دستورات، روال‌ها و فرآیندها و مفاهیم تقریبا مشابه است. نسخه IOS را می‌توان از دستگاهی به دستگاه دیگر به آسانی کپی کرد و شکل دستورات بسیار کوتاه، ساده و برای کاربر قابل فهم است.

ویژگی های امنیتی

ویژگی های امنیتی تجهیزات شبکه را از دو زاویه می‌توان بررسی نمود. از جنبه پشتیبانی از فرامین نرم‌افزاری صدور اجازه دسترسی (ACL) و نیز مسدود نمودن امکاناتی که بالقوه ممکن است توسط نفوذگران مورد سوء استفاده قرارگیرند هر دو تولید کننده جایگاه مشابهی در این زمینه دارند. همچنین تجهیزات به لحاظ حملات سخت افزاری مانند حمله differential power آزمایش، بررسی و تائید شده‌اند. اما از زاویه ارائه ماژول های امنیتی یکپارچه با سوئیچ ها، سیسکو تنوع قابل ملاحظه‌ای دارد. ماژول NAM که برای تحلیل و آنالیز ترافیک شبکه به کار می‌رود ماژول های IDS و Firewall که روی سوئیچ های رده ۶۵۰۰ نصب می‌شوند و نیز رده‌های مختلف IOSبا ویژگیهای DES۳، SSHو . . . از جمله این امکانات به شمار می‌رود.

شاخص هایی که ذکر شد تقریبا کامل هستند. پس اگر بتوان به آن ها به درستی وزن دهی و امتیاز دهی کرد و نتیجه را روی نمودار برد، می تواند به تصمیم گیری کمک قابل توجهی کند. به این کار می گویند.

فرایند تحلیل، بررسی و انتخاب راهکار (Solution Analysis)

در مورد هزینه، می بایست امروز سخت افزارهای متناظر از هر دو برند را انتخاب کنید و استعلام قیمت بگیرید. اتفاقا این روش از ساده ترین روش ها است.

در مورد IOS های Foundry (یا بهتر است بگوییم Brocade)، آن زمانی که شرکت Foundry وجود داشت، IOS هایش به راحتی پیدا نمی شد. حتی نمایندگی رسمی اش در دبی که از قضا تحت مدیریت یک فرد ایرانی بود نیز به سادگی به این IOS ها دسترسی نداشت.

پس از فروخته شدن Foundry به Brocade تغییر چندانی در سیاست انتشار دانش شرکت به وجود نیامده است. در نتیجه از نظر دانش عمومی سطح بسیار پایین تری نسبت به Cisco دیده می شود.یکی دیگر از موضوعات این است که فاندری روتر تولید نمی کند.

باید توجه داشت که به هیچ عنوان تجهیزات شبکه در دسترس نباشند که این موضوع باعث می شود صدمه شدیدی به شبکه وارد و شبکه ما مختل شود .

پروتکل ها قوانینی هستند که یک شرکت سیستم عامل خود را بنا بر این موضوع برنامه ریزی می کنند و میتواند نقطه ضعف و یا قوت یک شبکه باشند .

ابتدا برخی از پروتکل هایی که نقطه ضعف سیسکو می باشند را در زیر توضیح می دهیم :

این پروتکل ها هم نقطه مثبت و هم منفی دارند که نقطه منفی آ ن ها توسط هکرها استفاده می شود .

پروتکل cdp

این پروتکل اختصاصی Device های سیسکواست که اطلاعات مربوط به دستگاه هایی که به طور مستقیم به Device مورد نظر ما وصل است را ، نشان میدهد.

یک پروتکل شبکه لایه دو (Data Link) مخصوص سیسکو می باشد که این پروتکل جهت به اشتراک گذاری اطلاعات دستگاه های سیسکو (همانند نسخه سیستم عامل و آدرس IP) که بصورت مستقیم به یکدیگر متصل هستند توسط شرکت سیسکو توسعه یافته است . و این پروتکل در تجهیزات ساخته شده زیر توسط شرکت سیسکو اجرا می شود

- Routerها
- Bridgeها
- Access serverها
- Switchها

کارشناسان این پروتکل را یکی از ضعف های سیسکو می دانند. این پروتکل به پروتکل فضول نیز معروف هست . پیامهای CDP از طریق یک دستگاه سیسکو همسایه دریافت می شود و بصورت پیش فرض به هیچ دستگاه دیگری ارسال نمی شود .این به این معنی است که CDP فقط از دستگاه های سیسکو که به صورت مستقیم متصل می باشد عبور می کند.

پیغام CDP شامل اطلاعات زیر می باشد :

نام دستگاه (که با دستور hostname تنظیم شده است)

نسخه نرم افزار IOS

امکانات سخت افزار (routing/switching)

پلت فرم سخت افزار

آدرس IP دستگاه

اینترفیس که پیام CDP را ایجاد کرده است

CDP به صورت پیش فرض در روترهای سیسکو فعال می باشد .اگر شما ترجیح می دهید که این قابلیت را غیر فعال کنید می توانید از دستور no cdp run برای غیر فعال کردن آن و مجدد برای فعال کردن CDP می بایستی از دستور cdp runدر وضعیت global configuration استفاده نمایید

با این دستور می توانید دستورات را ببینید :

show cdp neighborsاطلاعات زیر را نمایش می دهد.

نوع دستگاه پیدا شده

نام دستگاه

تعداد و نوع پورت ها یا اینترفیس local

تعداد ثانیه ای که CDP advertisement برای پورت قابل معتبر است

شماره محصول دستگاه

شناسه پورت

هکر اول به دنبال بدست آوردن map network یک شبکه است ،که با این پروتکل می تواند این کار را کند.

هکر پروتکل را روی اینترفیس مورد نظر پیاده سازی کرده و اطلاعات مورد نظر را بدست می آورد.

بازیابی رمز عبور

دسترسی به روتر در صورت فراموش شدن کلمه ی رمز در صورتی که رمز را فراموش کرده اید ودیگر امکان دسترسی وجود ندارد می توانید از ریکاوری استفاده کنید .این پروسه اگر شبکه در دسترس فیزیکی افراد غیر مجاز باشد بسیار خطر ناک است . با استفاده از کابل کنسول می توان به روتر نفوظ کرد حتی اگر پسورد داشته باشد . یک هکربعد از دسترسی فیزیکی مراحل زیر را برای نفوظ انجام می دهد :

اول : کابل کنسول را به کامیوتر وصل کرده تا ارتباط با دستگاه بر قرار شود .

دوم : فشار دادن کلید break در ۶۰ ثانیه boot اولیه روتر

سوم : reload کردن روتر

چهارم : ورود به مد privileged mode روتر

پنجم : تغیر پسورد

دستورات زیر را باید پیاده سازی کنیم :

بعد از زدن کلید break و ورود به مد remmon

Remmon>confreg ۰x۲۱۰۲

دستور بالا روتر را به تنظیمات کارخانه برمی گرداند و بعد باید reset را تایپ کنیم .

اما اگر بخواهیم که بعد از پاک کردن دستورات و خاموش و روشن کردن روتر تنظیمات به حالت اول بر نگردند باید دستور زیر را تایپ کنیم :

Router(config)#configuration-register ۰x۲۱۴۲

این دستورات زمانی به کار میروند که امنیت فیزیکی نقض شده باشند و مختص سیستم عامل ios هستند.

پروتکل هایی که از لحاظ امنیتی کاربرد دارند

Port security

بسیار اتفاق می افتد که اینترفیس هایی در شبکه ما وجود دارند و مورد استفاده نیستند . محدود کردن اینترفیس های سوییچ به سخت افزارهای متفاوت یکی از مهمترین جنبه های امنیت فیزیکی است که ما باید در شبکه خود اتخاذ کنیم.

بنابراین با port security میخواهیم محدودیت سازی کنیم روی یک پورت Switch کدام Mac Address ها اجازه دارند وصل شوند و همچنین از این طریق میتوانیم مشخص کنیم چه تعداد Pc میتواند به پورت switch دسترسی داشته باشند.

مثلا اگر ۸ پورت داریم و ۵ تا کامپیوتر ۳ پورت آن خالی است و هر کسیمی تواند به این پورت ها دسترسی پیدا کند .اما ما میتوانیم با دستوراتی که به سوییچ میدهیم دسترسی به این پورت ها را محدود و امنیت را بالا ببریم. در این دستور فقط افراد مشخص از سوییچ استفاده می کنند.

این را باید اضافه کنیم که بر روی سوییچ ها دو نوع Port داریم:

ACCESS : پورت های بین Switch و User انتهایی

TRUNK : پورت های بین سوییچ ها

نکته مهم این می باشد که port security فقط Access Port ها پیاده سازی می شود.برای راه اندازی پورت سکوریتی باید دستورات زیر را بدهیم :

برای راه اندازی Port Security بر روی پورت مورد نظر،سوییچ را با دستور زیر به حالت Accessمیبریم:

۰/۱ switch (config)#interface fastethernet

switch(config-if)#switchport mode access

فعال کردن Port Security روی پورت مورد نظر:

switch(config-if)#switchport port-security

معرفی کردن Mac Address های مجاز:

یک کلاس درس را تصور کنید که دارای یک switch می باشد و همچنین تعداد client ها نیز،۱۰ عدد می باشد.

میخواهیم فقط کامپیوترهای کلاس یه سوییچ وصل شوند و نمیخواهیم کسی از بیرون به شبکه ی ما دسترسی داشته باشند.

فرض کنید به ترتیب پورت های ۱ تا ۱۰ به کامپیوترهای کلاس وصل میباشد.بنابراین باید وارد هرکدام از پورت ها شویم و Mac Address کامپیوتر متصل شده به آن پورت را،به صورت دستی تعریف کنیم در Port Security.

Switch(config-if)#switch port security macaddress H.H.H (e۲۳f.۲۳e۲.ef۲e)

.

.

.

در حال حاضر کلیه ی کامپیوترهای کلاس مجازند و کامپیوتر متخلف نداریم.غیر از این Mac addها هر کسی به سوییچ وصل بشه تخلف رخ داده!

تعداد ماکزیمم Mac Address هایی که می تواند بر روی یک پورت Learn شود از طریق دستور زیر می باشد.

switch(config-if)#switchport port-security maximum ۲

از آنجایی که Confige کردن کلیه ی Port ها،کار مشکل و وقت گیری میباشد،یک Rangeاز interfaceها را انتخاب میکنیم و Confige مربوطه را به کلیه Interfaceها اعمال می کنیم.

switch(config)#interface range fastethernet ۰/۱-۸

Violation

وقتی بـر روی یکـی از پـورت هـا تخلفـی صـورت بگیرد،بـه صـورت default،پـورت مـورد نظـر Shutdown می گردد.از طریق Violation می توانیم یکی از item های زیـر را انتخـاب کنـیم و Defult قرار دهیم.

Shutdown	Disable port(yes)	Discard packets(yes)	Send Log(yes)
Restrict	Disable port(No)	Discard packets(yes)	Send Log(yes)
Protect	Disable port(No)	Discard packets(yes)	Send Log(No)

switch(config-if)#switchport port-security violation {restrict|protect|shutdown}

اگر فرد غیر مجازی به سوییچ وصل شود اینترفیس این دسـتورات را فعـال میکنـد. کـه از نظـر امنیت فیزیکی خیلی اهمیت دارد.

گذاشتن پسورد ورود بر روی تجهیزات

مهمترین گام در راه اندازی یک شبکه گذاشتن پسورد بر روی تجهیزات است کـه از ورود افـراد غیر مجاز به سیستم جلوگیری می کند . همانطور که می دانید برای افزایش امنیت نیاز بـه تاییـد هویت می باشد. در این قسمت انواع پسورد و محل استفاده از هر یک از آن ها را مورد بررسی قرار می دهیم.

پنج نوع Password را می توان بر روی تجهیزات شبکه set کرد:

۱.Enable Password

۲.Secret password

۳.AUX Password

۴.Telnet Password

۵.Console Password

Enable Password : برای برقراری امنیت هنگام ورود به privileged mode استفاده میشود. هنگامی که درuser mode فرمان enable را وارد می کنید و میخواهید وارد privileged mode شوید این password پرسیده می شود.

Router (config)#Enable password cisco

Secret Password : همانند enable password میباشد. با این تفاوت که پسورد به صورت کد شده در فایل Running-config و startup-config ذخیره می شود و به صورت clear-text نمایش داده نمی شود.

Router (config)#Enable secret test

توجه داشته باشید هنگامی که secret password را تنظیم می کنید، تا زمان فعال بودن secret password، enable passwordبه صورت غیر فعال در می آید و میبایست هنگام ورود به Priviledeg Mode پسورد مربوط به Secret Password را وارد کنید.

Telnet Password : یکی از راههای دسترسی به روتر Virtual Terminal یا همان Telnet می باشد. بنابراین در صورتیکه به یک روتر Telnet می کنید، می بایست بعد از بررسی و صحت Authentiction ارتباط برقرار شود.

برای تنظیم کردن telnet password وارد global mode شده و فرمان زیر را وارد میکنید :

Router (config) # line vty ۰۴

به ازای هر ارتباط Telnet یک Session برقرار میشود بنابراین به اندازه تعداد Lineهایی که IOS ساپورت می کند می توانید Telnet Session برقرار کنید.

برای دیدن تعداد Line هایی که IOS ساپورت میکند کافی است از Help کمک بگیرید.

فرمان بعدی login می باشد. در واقع با این فرمان می گویید که در صورت telnet شدن به این device، پسورد پرسیده شود.

Router (config-line)#login

مرحله آخر تعریف پسورد می باشد:

Router (config-line)#password new

توجه داشته باشید telnet password قبل از وارد شدنuser به user mode پرسیده میشود.

AUX Password

همانطور که می دانید یکی دیگر از راه های برقراری ارتباط remote ، روش استفاده از پورت AUX می باشد. در این روش روتر را از طریق یک مودم به خط dial-up متصل شده است و

دسترسی به صورت remote به آن امکان پذیر می باشد. AUX password پسوردی است که قبل از وارد شدن به user mode پرسیده می شود.

Router (config) # line aux ۰

بقیه ی مراحل بالا را باید انجام دهیم .فقط تنها تفاوت در خط اول دستور است.

Console password

تنها راه ارتباط با روتر که بدون تنظیم می باشد استفاده از console port است. بنابراین بعد از انجام تنظیمات می توانید روتر را در یک جای ثابت قرار داده و از این به بعد آن را از طریق telnet یا Browser کردن تنظیم کنید.

اما توجه داشته باشید که نداشتن پسورد و محدودیت دسترسی افراد برای admin دردسر ساز می شود Console Password ، پسوردی است که قبل از وارد شدن به User Mode پرسیده میشود و به صورت زیر تنظیم می شود.

Router (config) # line console

بقیه ی مراحل بالا را باید انجام دهیم .فقط تنها تفاوت در خط اول دستور است.

Vlan

تعریف وی لن : LAN در واقع یک Broadcast Domain است، ایجاد Virtual LAN نیز یعنی تفکیک یک Broadcast Domain به دو یا چند Broadcast Domain جدا از هم!

VLAN، یکی از فن آوری های پیشرفته در شبکه های کامپیوتری است که اخیرا" با توجه به ویژگی های منحصربفرد خود توانسته است در کانون توجه طراحان و پیاده کنندگان شبکه های کامپیوتری قرار بگیرد .

طراحی و پیاده سازی یک شبکه کامپیوتری کار ساده ای نمی باشد و شبکه های VLAN نیز از این قاعده مستثنی نخواهند بود ، چراکه در این نوع شبکه ها مجموعه ای متنوع از پروتکل ها به منظور نگهداری و مدیریت شبکه بکار گرفته می شود.

در این مطلب قصد داریم به نحوه پیکربندی یک شبکه VLAN اشاره نمائیم .در ابتدا لازم است به طرح های فیزیکی متفاوت VLAN و مفاهیم اولیه آن اشاره ای داشته باشیم تا از این رهگذر با مزایا و دستاوردهای این نوع شبکه ها بیشتر آشنا شویم.

بخاطر داشته باشید که برای طراحی و پیاده سازی شبکه های کامپیوتری که هر یک دارای منابع و ملزومات مختص به خود می باشند ، فنآوری های متفاوتی در دسترس می باشد و مهم این است که بتوان با بررسی کارشناسی بهترین گزینه در این رابطه را استفاده نمود.

طراحی اولینVLAN

در اکثر پیکربندی های VLAN ، محوریت بر اساس گروه بندی دپارتمان ها صرفنظر از محل استقرار فیزیکی آنان در یک شبکه می باشد. بدین ترتیب مدیریت دپارتمان ها متمرکز و امکان دستیابی به منابع مهم و حیاتی شبکه محدود و صرفا" در اختیار کاربران مجاز قرار خواهد گرفت.

مدل پیشنهادی را بدون در نظر گرفتن VLAN و با لحاظ نمودن VLAN بررسی می نمائیم.

وضعیت موجود سازمان فرضی

سازمان فرضی دارای چهل دستگاه ایستگاه کاری و پنج سرویس دهنده است.

در سازمان فرضی دپارتمان های متفاوتی با وظایف تعریف شده ، وجود دارد : دپارتمان مدیریت ، دپارتمان حسابداری ، دپارتمان فنآوری اطلاعات

دپارتمان های اشاره شده در سه طبقه فیزیکی توزیع و پرسنل آنان ممکن است در طبقات مختلف مشغول به کار باشند .

اول : عدم استفاده ازVLAN

دپارتمان فناوری اطلاعات به عنوان مجری طراحی و پیاده سازی شبکه به این نتیجه رسیده است که بدلیل رعایت مسائل امنیتی مناسب تر است که شبکه را پارتیشن نموده و آن را به چندین بخش تقسیم نماید . هر دپارتمان در یک Broadcast domain قرار گرفته و با استفاده از لیست های دستیابی که بین محدوده های هر یک از شبکه ها قرار می گیرد، این اطمینان حاصل می گردد که دستیابی به هر یک از شبکه ها با توجه به سیاست های دستیابی تعریف شده،میسرمی گردد.

ویژگی های سناریوی اول:

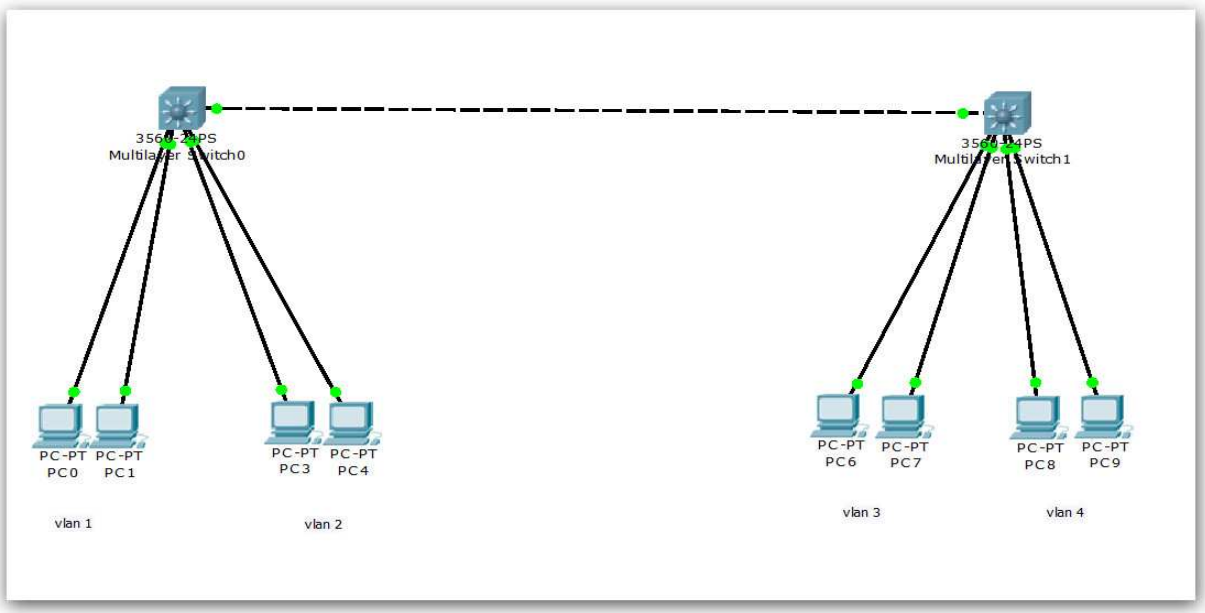
- به هر دپارتمان یک شبکه خاص نسبت داده شده است.
- در هر طبقه از یک سوئیچ اختصاصی برای هر یک از شبکه های موجود ، استفاده شده است.
- مهمترین دستاورد مدل فوق ، افزایش امنیت شبکه است چراکه شبکه های فیزیکی عملا" از یکدیگر جدا شده اند.
- سوئیچ های موجود در هر طبقه از طریق ستون فقرات شبکه با یکدیگر گروه بندی و به روتر اصلی شبکه متصل شده اند.

- روتر مسئولیت پیچیده کنترل دستیابی و روتینگ بین شبکه ها و سرویس دهنده ها را بـا استفاده از لیست های دستیابی بر عهده خواهد داشت.

مدیریت شبکه بدلیل عدم وجود یک نقطه متمرکز دارای چالش های مختص به خود می باشد.

دوم : استفاده ازVLAN

در این مدل ، طراحی شبکه با در نظر گرفتن فناوری VLAN به صورت زیر ارائه شده است:



شکل (۳ - ۳) شبکه vlan

ویژگی های سناریوی دوم

- در هر طبقه از یک سوئیچ استفاده شده است که مستقیما" به ستون فقرات شبکه متـصل می گردد.
- سوئیچ های استفاده شده در این سناریو دارای ویژگی VLAN بوده و بگونه ای پیکربندی می گردند که سه شبکه فیزیکی و منطقی جداگانه را حمایت نمایند.
- در مقابل روتر در سناریوی قبل از یک سوئیچ لایه سوم ، استفاده شده است . سوئیچ های فوق بسیار هوشنمند بوده و نسبت به ترافیک لایه سوم (لایه IP) آگاهی لازم را دارند.
- با استفاده از یک سوئیچ ، می توان لیست های دستیابی را به منظور محدودیت دسـتیابی بین شبکه ها تعریف نمود . دقیقا" مشابه عملیاتی که با استفاده از روتر در سناریوی قبلی انجام می

گردد (روتینگ بسته های اطلاعاتی از یک شبکه منطقی به شبکه منطقی دیگـر) . سـوئیچ هـای لایه سوم ، ترکیبی از یک سوئیچ قدرتمند و یک روتر از قبل تعبیه شده می باشند.

مقرون به صرفه بودن ، تسهیل در امر توسعه شبکه ، انعطاف پذیری و مدیریت متمرکز از جملـه مهمترین ویژگی های سناریوی فوق می باشد.

دستورات پیکربندی وی لن بر روی سوییچ به صورت زیر است:

```
Router>
Router> Enable
```

در اینجا کلمه عبور را وارد می کنیم و به مد تنظیمات می رویم.

```
Router# config terminal
Router (config)#
Router(cinfug)#vlan ۱
Router(config-vlan)#name marketing
Router(config-vlan)#exit
Router(config)#
Router(config)#vlan ۲
Router(config-vlan)name Human Resource
Router(config-vlan)#exit
```

تاکنون vlan های ۱ و ۲ را ساختیم. حالا نوبت این است که به هر یک از آن ها پورت های مورد نظرم را مرتبط کنیم. برای این کار باید به Interface رفته و دستورات زیر را وارد کنم:

```
Router(config)# interface fastethernet ۰/۲
Router(config-if)#switchport mode access
۱Router(config-if)#switchport access vlan
Router(config-if)#exit
Router(config)#interface fastethernet ۰/۳
Router(config-if)#switch mode access
۲Router(config-if)#switchport access vlan
Router(config-if)#exit
```

بعد از این دستورات clint ها از هم جدا و در وی لن های مختلف قرار گرفته اند کـه مـی تـوان سطح دسترسی و فیلترینگ آنها را مشخص نمود. این پروتکل از نظر امنیتی بسیار کار آمد است.

Access list

در ترجمه لغوی به معنای لیست دسترسی سیسکو می باشد که زیاد هم از معنای واقعـی خـود دور نیست.

همانطور که از اسم آن بر می آید به وسیله این ابزار می توانیم بر روی سخت افزارهای سیسکو فایروال ایجاد کنیم.

از آنجا که بحث فایروال بسیار گسترده است و تنها به یک access listمنتهی نمیشود به این نوع فایروال packet filter گفته می شود.

از آنجا که ورودی اینترنت ۸۰ درصد شبکه هایی که ما با آنها کار می کنیم Ciscoهست میتوانیم با بکار گیری Access listدر آنها امنیت زیادی را برای خود به ارمغان بیاوریم. نا گفته نماند که مهمترین گزینه در Packet filter ها کانفیگ خوب آنهاست نه Brand یا مدل دستگاه. شما اگر با اصول Packet Filtering آشنایی داشته باشید بر روی هر سیستم عامل یا سخت افزاری تنها با آموختن علم آن می توانید یک فایروال ایجاد کنید.

یک ACL در ios سیسکو برای مدیریت کردن ترافیک شبکه مورد استفاده قرار می گیرد . زمانی که شما ترافیک یک شبکه رو مشخص می کنید می توانید آن را به روش های گوناگونی مدیریت کنید برای مثال شما می توانید به آن اجازه ، رد ،محدود یا آز آن برای محدود کردن به روز شدن مسیر یابی (Routing Update) استفاده نمایید. از Access list می توان در بحث فیلترینگ و سطح دسترسی استفاده کرد .

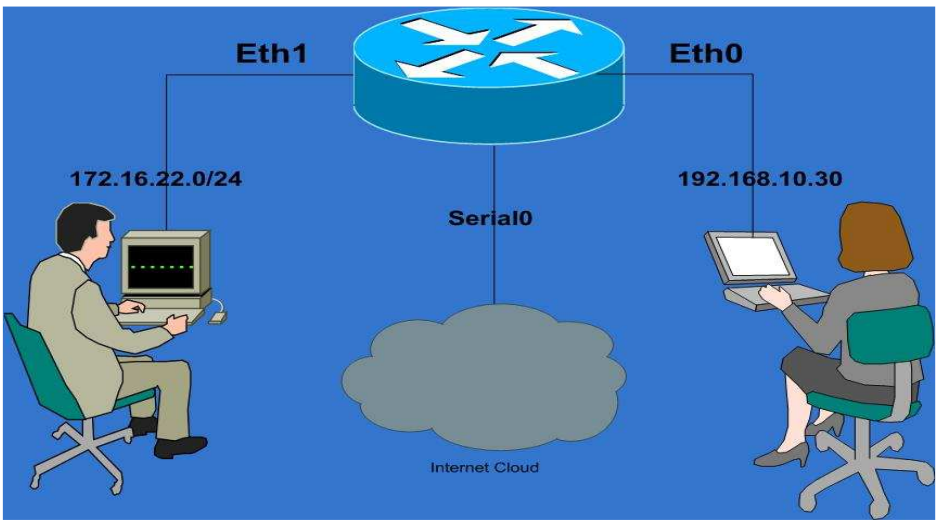
Access-Listمی تواند یکی از دو نوع زیر باشد:

۱. استاندارد(Standard)
۲. توسعه یافته (Extended)

شماره گذاری ACL ها بین رنج اعداد زیر میبایستی باشد ۱تا ۹۹ و ۱۳۰۰ تا ۱۹۹۹ برای ACL IPهای استاندارد ۱۰۰تا ۲۹۹ و ۲۰۰۰ تا ۲۶۹۹۹ برای ACL IP های توسعه یافته یک ACL استاندارد فقط می تواند ترافیک را بر اساس IP مبداء (Source Ip) تعیین کند این در حالی است که یک ACL توسعه یافته (Extended Access-list) می تواند ترافیک را بر اساس مبداء و مقصد و همچنین با شماره های پورت مبداء و مقصد تعیین کند .

قابل ذکر است که با یک Standard ACL فقط ترافیک IP را می توانیم تعیین کنیم حال آنکه با یک Extended ACL می توانیم ترافیک های TCP, UDP, ICMP, IP, AHP, EIGRP, IGRP, ESP, IGMP, OSPF,و PIM را مشخص کنیم.

با توجه به شکل زیر می خواهیم کاربر ۱۹۲,۱۶۸,۱۰,۳۰ به شبکه ۱۷۲,۱۶,۲۲,۰ دسترسی نداشته باشد :



شکل (۳ – ۴) دسترسی به وسیله acl

Access-List ها به تنهایی قادر به انجام کاری نیستند و تنها بعنوان یک لیست ، گروهی را بـا سیاست های دسترسی تعریف شده در خود جای داده است .

برای هر interface می توانیم دو ACL را پیوست کنیم:

in bound

ورود Packet را به دستگاه inbound گویند

out boubd

خروج packet را از دستگاه out bound گویند

با استفاده از قالب دستوری زیر ، بایستی قانون و سیاست نوشته شده خود را در قالب یک گروه ، به درگاه خاصی اختصاص دهیم :

R۱(config)#access-lis access-id action(permit or deny) source-address wild card mask

بطور مثال می خواهیم سناریوی زیر را در روتر ۱ اجرا کنیم :

۱۹۲,۱۶۸,۲۰,۲ Ip را Permit می دهیم و ۱۹۲,۱۶۸,۲۰,۳ ip را deny می کنیم :

R۱(config)#access-list ۱۰ permit ۱۹۲,۱۶۸,۲۰,۲ ۰,۰,۰,۲۵۵

R۱(config)#access-list ۱۰ deny ۱۹۲,۱۶۸,۲۰,۳ ۰,۰,۰,۲۵۵

R۱(config)#int s۰
R۱(config-if)#ip access-group ۱۰ in

توجه داشته باشید in همان inbound می باشد

حال سناریوی زیر را برای ۲ Router اجرا می کنیم به تمامی سیستم های روتر permit ۱ می دهیم و تمامی سیستم های روتر ۳ را deny می کنیم .

R۲(config)#access-list ۱۱ permit ۱۹۲,۱۶۸,۱۰,۰ ۰,۰,۰,۲۵۵
R۲(config)#int s۰
R۲(config-if)#ip access-group ۱۱ in
R۲(config)#access-list ۱۲ deny ۱۹۲,۱۶۸,۳۰,۰ ۰,۰,۰,۲۵۵
R۱(config)#int s۱
R۱(config-if)#ip access-group ۱۲ in

Extended ACL

در extended Acl می توانیم به آدرس source و به آدرس مقصد و سرویس ها رجوع کنیم

Ectended ACL ID

range از ۱۹۹-۱۰۰ می باشد که برای Extended استفاده می شود .

R۱(config)#access-lis access-id action(permit or deny) protocol source-address wild-card-mask Destination-address Destination-wild-card parameters port-number

اگر شبکه ای امنیت فیزیکی اش به خطر بیفتد بسیار خطر ناک است و می توان به راحتی به آن نفوذ کرد به همین ترتیب باید به امنیت فیزیکی بسیار توجه داشت.ولی با استناد به دستورات بـالا می توان شبکه را در برابر برخی حملات محافظت کرد تا صدمه کمتری به شبکه وارد شود .

منابع

منابع

کتاب ccna نوشته دکتر مسعود حسینقلی

کتاب آزمایشگاه شبکه های کامپیوتری نوشته مهندس حمید ریاضی

Website: http://www.irparsi.com
http://www.cisco.com
http://www.tejaratnama.ir
http://www.library.sharif.ir
http://www. http://digitallib.aut.ac.ir