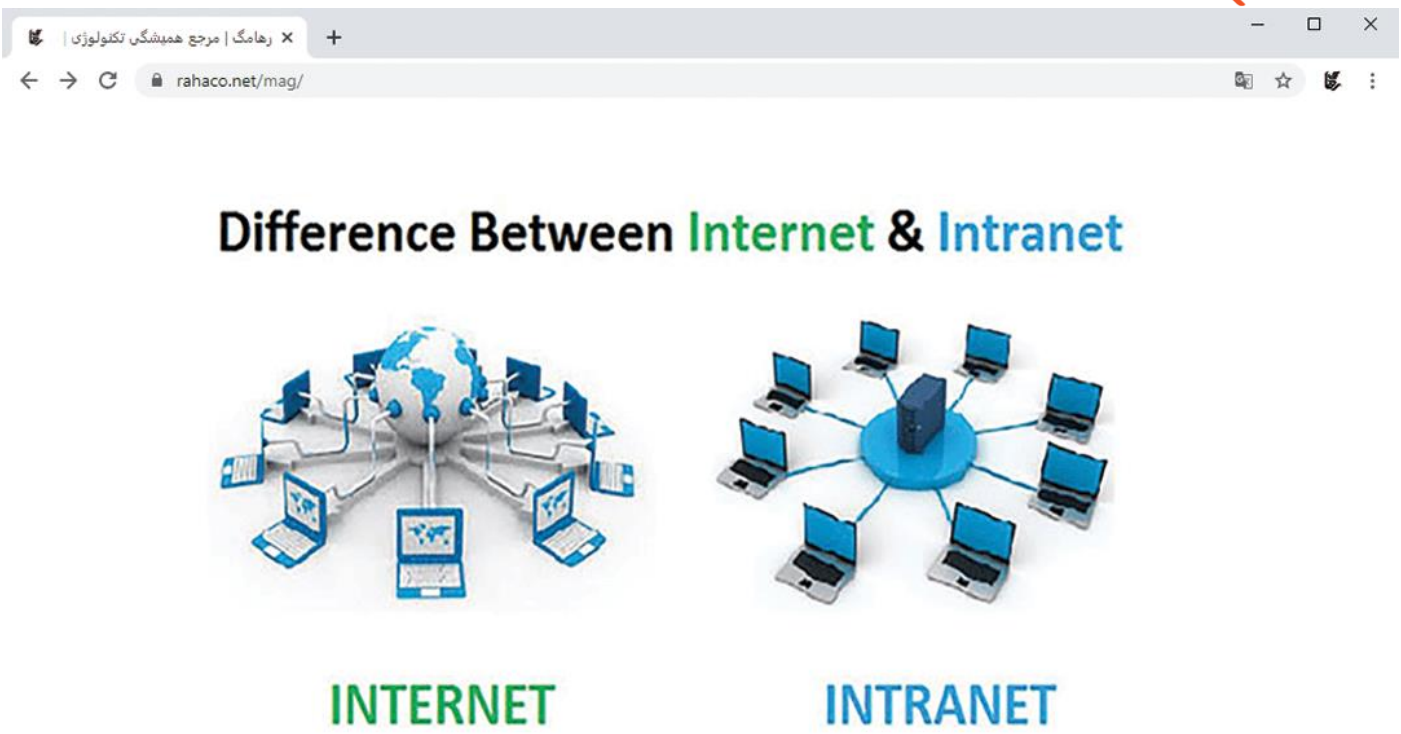
جداسازی اینترنت از اینترانت از طریق vlan چگونه انجام می شود؟

مجموعه شرکت‌های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

چرا جداسازی اینترنت از اینترانت از طریق vlan باید انجام شود؟

یکی از اصولی ترین مبانی امنیت اطلاعات محافظت از محیط سرویس دهی در فضای سایبر می باشد.

از همین رو یکی از مهم ترین دغدغه های سازمان ها، شرکت‌ها و مراکز دولتی در حال حاضر **جداسازی اینترنت از اینترانت از طریق vlan** سازمانی می باشد.

مسلما به واسطه این جداسازی به میزان قابل توجهی، از تهدیدات امنیتی کاسته شده و از وقوع مشکلات بسیاری جلوگیری به عمل خواهد آمد.

از سوی دیگر استفاده ازاینترنت به عنوان یک منبع اطلاعاتی وارتباطی بسیار ضروری بوده وغیرقابل چشم پوشی است.

بنابراین حفظ و پایداری شبکه های داخلی و امنیت آن از اهمیت بسیار بالایی برخوردار است.

چه راهکارهایی جداسازی اینترنت از اینترانت از طریق vlan وجود دارد؟

بهره وری و سازگار بودن شبکه و کاربر از اهداف رشد کسب و کار می باشد.

یکی از روش های بهبود و ارتقاء در شبکه **جداسازی اینترنت از اینترانت از طریق vlan** می باشد.

استفاده از این تکنولوژی باعث افزایش امنیت و کارآیی شبکه بدون استفاده از تجهیزات گرانقیمت شده است.

به منظور استفاده و اجرای VLAN در شبکه خود ، شما نیاز به یک سوئیچ لایه ۲ خواهید داشت. که قابلیت مدیریت را داشته باشد یعنی Manageable باشد.

باید توجه داشت که هر VLAN که بر روی سوئیچ ایجاد می شود ، به منزله یک شبکه جداگانه خواهد بود و این شبکه ها هیچگونه ارتباطی با یکدیگر نخواهند داشت.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

یکی از مهمترین ویژگی هایی که باعث استفاده از شبکهVLAN شده است ، Broadcastنشدن پیام ها در سراسر شبکه می باشد.

VLANها در شبکه و بر روی سوئیچ این اجازه را می دهند که شبکه هایی با آدرس های IP متعدد و زیر شبکه های متعدد وجود داشته ، بدون اینکه با یکدگیر در ارتباط باشند.

مزایای اصلی جداسازی اینترنت از اینترانت از طریق vlan چیست؟

- امنیت
- کاهش هزینه
- افزایش بازدهی و کارآیی
- کاهش و جلوگیری ازBroadcast
- سادگی اجرا و مدیریت آساندر این پروژه ۴ vlan داریم.
- ۱۰۱
- ۱۰۲
- ۱۰۳
- ۱۰۴

که هرکدام برای قسمت خاصی می باشد.

قسمت های این شرکت شامل server room, support , sales ,it می باشد که همه قسمت ها بجز قسمت salesدارای اینترنت هستند.

در قسمت sales دونفر که مدیر و معاون فروش هستند دارای اینترنت می باشند.

برای دسترسی دادن به ip ها در روتر مربوطه که از سمت دیگری به اینترنت وصل است باید acl بنویسیم.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

طرح اجرایی شرکت اجرای vlan بر روی سوییچ های سیسکو می باشد.اجرای این طرح بسیار کم هزینه بوده و مورد پسند مشتری قرار گرفته است.

که پس از بازدید و بررسی های اولیه و تعیین دسترسی ها اینکه هر کاربر دسترسی به اینترنت داشته باشد یا نه مورد بررسی قرار می گیرد.

و اینکه در کدام vlan باشد کار را آغاز می کند. در این میان، روی هر vlan لیست دسترسی یا همان acl مربوطه نوشته می شود.

Cisco Access Listبه چه معناست؟

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

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

از آنجا که بحث فایروال بسیار گسترده است و تنها به یک access list منتهی نمیشود به این نوع فایروال packet filterگفته میشود.

حتما خوانندگان عزیز سیسکو را شناخته و از کارایی آن خبر دارند.

از آنجا که ورودی اینترنت ۸۰ درصد شبکه هایی که ما با آنها کار می کنیم.

Ciscoهست میتوانیم با بکار گیری Access list در 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.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

بر روی هر سیستم عامل یا سخت افزاری تنها با آموختن Syntax آن میتوانید یک فایروال ایجاد کنید.

من در اینجا به توضیح قوائد آن در سیسکو می پردازم.

برای ایجاد access list شما نیاز به IOS های بالاتر از ورژن ۸.۳ دارید.

دو مرحله برای ایجاد یک access list داریم. اول میبایست ACL مربوطه را نوشته و دوم آن را به یک اینترفیس اعمال کنیم.

بدیهی است در صورت عدم اعمال ACL به یک اینترفیس ACL مذکور بلا استفاده می ماند.

پر کاربردترین ACL ها IP Access list است. زیرا اکثر ترافیکها بر روی پروتکل IP انتقال می یابد.

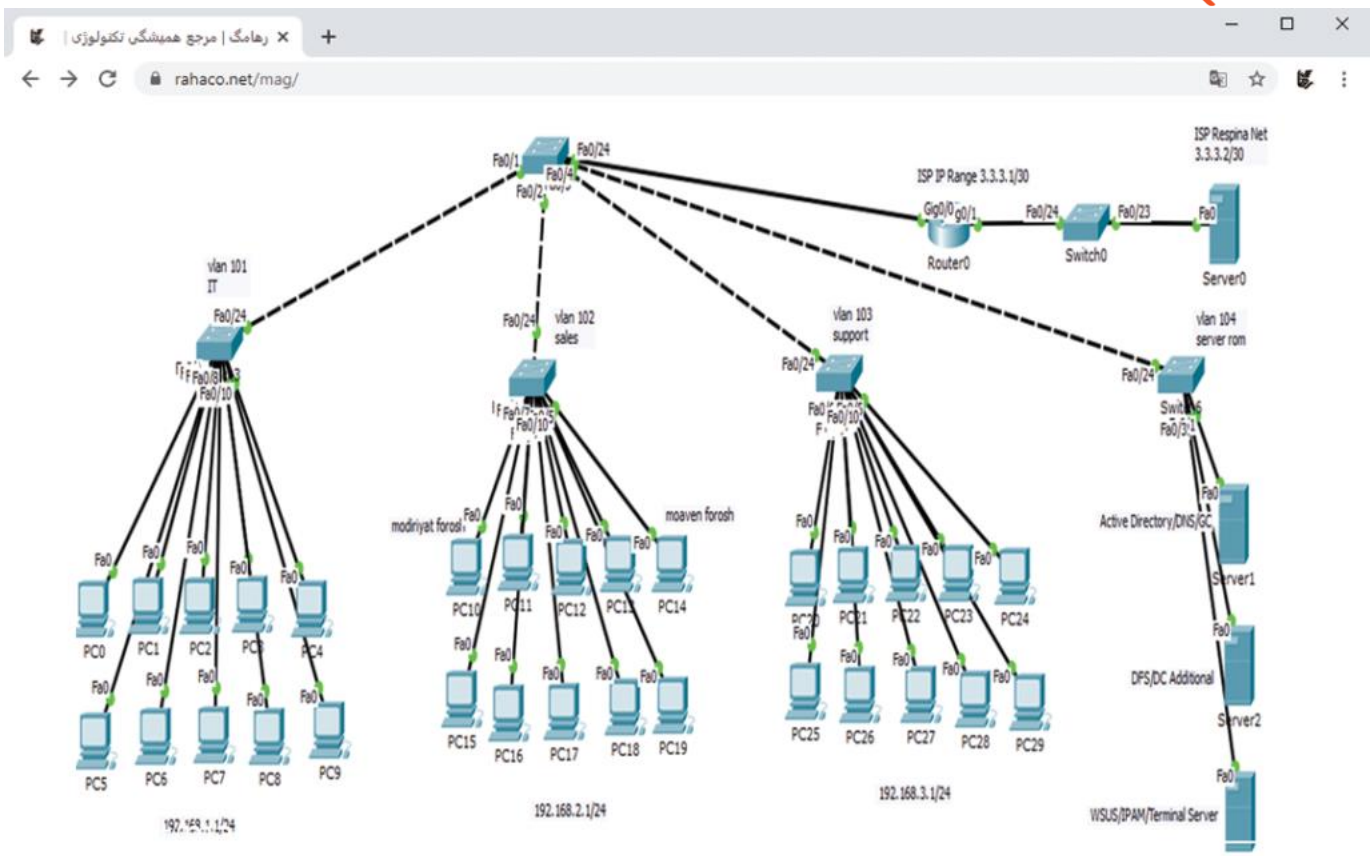
خود IP access list دو نوع است Standard :و Extended Standard تنها بر اساس SOURCE IP address می تواند کنترل کند.

Extendedبر حسب SOURCE and DESTINATION IP address و SOURCE and DESTINATION Port می تواند محدودیت ایجاد کند.

معمولا برای نام گذاری access list ها از اعداد استفاده میشود. که از شماره ۱ تا ۹۹ برای Standard و ۱۰۰ تا ۱۹۹ برای Extended استفاده میشود.

البته اعداد ۱۳۰۰ تا ۱۹۹۹ برای Standard و ۲۰۰۰ تا ۲۶۹۹ برای Extended رزرو شده اند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net



- port 0/1 access-list
- Router(config)#access-list 1 permit 192.168.1.2
- Router(config-if)#ip access-group 1 out
- SW1(config)#vlan access-map NOT-TO-SERVER 10
- SW1(config-access-map)#match ip address 100
- SW1(config-access-map)#action drop
- SW1(config-access-map)#vlan access-map NOT-TO-SERVER 20
- SW1(config-access-map)#action forward

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

حرف آخر!

پس از کشف ویروس Flame، جداسازی اینترنت از اینترانت از طریق vlan سازمانها بصورت نسخه ای واحد و در قالب بخشنامه به عنوان تنها راه حل ممکن برای جلوگیری از حملات نفوذگران به بسیاری از سازمانها و صنایع ابلاغ گردید.

آنه فرانک «من به بدبختی‌ها و چیزهای بد فکر نمی‌کنم؛ تنها چیزی که به یاد می‌آورم زیبایی‌هایی است که باقی می‌مانند».

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net