مقاله

« امنیت در شبکه های جدید IP/MPLS »

علی ثاقب موفق –فوق لیسانس فناوری اطلاعات

واژه MPLS مخفف Multi protocol label switching است که لغت سوئیچینگ آن مبین تعلق آن به خانواده شبکه های packet switching بوده و لغت multi protocol آن به معنی این است که می تواند با چندین پروتکل سازگاری داشته باشد.

پروتکل MPLS در مدل لایه ای OSI و بین لایه های ۲ و ۳ (Data link & physical layer) قرار می گیرد و از اینرو بعنوان پروتکل لایه 2.5 از آن یاد می شود. لغت label که مشخصه منحصر به فرد MPLS است ، نقش زیادی در ارسال داده ها دارد به طوریکه بخشی از مسیر یابی مربوطه به نقل و انتقال داده براساس label صورت می گیرد.

به هر حال MPLS دارای یک سری قابلیت های خاص خود است که عبارتند از:

- مهندسی ترافیک - TE (Traffic Engineering)
- مسیریابی مجدد سریع Fast re-route
- پشتیبانی از کیفیت سرویس (QOS) وامکان اولویت دهی به سرویس های شبکه (Quality Of Service)
- شبکه خصوصی مجازی VPN با قابلیت مقیاس پذیری . (Scalable VPN -Virtual Private Network)

در خصوص اهمیت موضوع مهندسی ترافیک در IP/MPLS می توان گفت به واسطه اینکه در مواقعی تغییر الگوهای ترافیکی مثل انتشار اخبار انتخابات روی سایت اینترنتی یا تجارت و خرید و فروش بر خط و یا رویدادهای ورزشی بزرگ ، ما ازدحام و ترافیک

سنگین را بر روی سایت های مربوطه و اینترنت خواهیم داشت لذا MPLS برای مقابله با این تغییرات سریع ترافیکی قابلیت های زیر را ارائه نموده است:

- استفاده بهتر از عرض باند موجود (بعنوان مثالً مسیردهی روی مسیرهایی که کوتاهترین مسیر نیستند)
- مسیردهی پیرامون گره ها و link های fail شده (انجام مسیردهی سریع اطراف گره های fail شده به سمت کاربر شبیه حالت SONET APS) (Automatic protection switching)
- ایجاد سرویس های جدید مثل سرویس های Leased line مجازی (کاربردهایی از VOIP و گارانتی نمودن عرض باند از نقطه به نقطه)
- برنامه ریزی برای ظرفیت خطوط (بهبود دسترس پذیری شبکه)
- هماهنگی و ترکیب موثرمهندسی ترافیک و VPN برای سرویس های انتها به انتها

همچنین استفاده از Label ها برای ایجاد یک IP VPN تواناییها و قابلیت های زیر را برای ما به ارمغان می آورد:

- امکان توزیع Label ها را به هر VPN توسط شبکه
- امکان پذیری QOS , Privacy بدون رمزگذاری .
- انجام مکانیزم (Labels) برای کیفیت سرویس و VPN ها

لذا برای محدودکردن ریسک ، ضروری است که پیکربندی پروتکل مسیریابی روی روترها به اندازه ممکن امن باشد که با شیوه های زیر امکان پذیر خواهد بود:

- با کمک ACL که اجازه دهد پروتکل مسیریابی تنها از روتر امکان پذیر باشد نه از هر جایی دیگر
- در صورت لزوم پیکربندی MP5 برای پروتکل مسیریابی ضروری است.
- در موارد لازم پیکربندی پارامترهایی از پروتکل مسیریابی ضروری است.

علاوه بر قابلیتهای فوق، MPLS دارای قابلیت های امنیتی ویژه نیز می باشد. همانگونه که می دانیم MPLS نسبت به پیشینیان خود از امنیت بالاتری برخوردار است که برخی از دلایل آن را می توان به پارامتر های امنیتی و شبکه ای ذیل نسبت داد:

- فضای آدرسی و جداسازی مسیریابی

- پنهان سازی ساختار هسته MPLS
- مقاوم در برابر حمله ها (Attacks)
- عدم امکان Label spoofing

حال به هر کدام از پارامترهای امنیتی فوق به تفکیک می پردازیم:

فضای آدرسی و جداسازی مسیریابی:

- فضای آدرسی بین VPN های مختلف ، کاملاً مستقل است.
- هر سیستم پایانی در یک VPN دارای یک آدرس منحصر به فرد است و همه مسیرها به این آدرس در واقع به همان سیستم پایانی اشاره می کند و این نکته از منظر مسیریابی مهم است.
- پاکت های ارسالی به میزبان a.b.c.d در یک VPN، به میزبان دیگر با همان آدرس در VPN دیگر، ارسال نخواهند شد و این موضوع به لحاظ امنیتی مهم و جوابگوی نیازهای ما است .
- MPLS اجازه می دهد که VPNهای مجزا از فضای آدرسی خصوصی یکسان استفاده نمایند. این کار با افزودن یک 64 بیت به هر مسیر IPV4 انجام می شود. ایجاد آدرس های VPN یکتا در هسته MPLS نیز منحصر به فرد است . این آدرس توسعه یافته همچنین آدرس VPN- IPV4 نامیده می شود. بنابراین مشتریان سرویس MPLS نیازی به تغییر آدرس دهی جاری در شبکه هایشان را ندارند.

جداسازی فضای آدرس:

- هر VPN باید قادر باشد که از همان فضای آدرس که بقیه VPNها استفاده می کنند بهره گیرد.
- هر VPN باید قادر باشد تا از فضای آدرسی مشابه هسته MPLS استفاده کند.

جداسازی مسیریابی و قواعد آن:

- مسیریابی بین هر دو VPN باید مستقل باشد.
- مسیریابی بین هر VPN و هسته باید مستقل باشد.

- هر VRF دارای یک RD باشد (RD یا Route Distinguisher یک ۶۴ بیتی است که به آدرس ip ۳۲ بیتی ، اضافه شده و آدرس VPN IPV4 را تشکیل می دهد، VRF یا Virtual Routing and Forwarding instant مسیریابی و ارسال مجازی است)

مقاوم در برابر حمله ها:

علیرغم خصوصیات امنیتی ذکر شده هسته MPLS به دو روش می تواند مورد حمله قرار می گیرد:

۱. با حمله مستقیم به روترهای ضعیف

۲. با حمله به مکانیزم های سیگنالینگ MPLS (عموماً در مسیریابی)

همچنین تهدیدهای امنیتی MPLS (داده ای و کنترلی) عبارتند از:

- حمله Replay
- DOS
- دستکاری غیرمجاز
- تحلیل الگوی ترافیک
- جعل هویت
- پروتکل های مسیریابی
- عدم پیکربندی امن

به طور کلی حمله به MPLS مشکل است مثلا عدم امکان Label spoofing که با توجه به این نکته است که در MPLS پاکت های شبکه براساس آدرس مقصد IP ارسال نمی شوند و براساس Label هایی است که توسط روترها تنظیم می شوند. همچنین می توان گفت MPLS در برابر حمله ها به اندازه کافی قوی است که این موضوع با توجه به اهمیت امنیت برای سرویس دهندگان اینترنتی مورد استقبال آنها نیز قرار می گیرد.(Internet Service Provider). بنابراین می بینیم که فراهم کنندگان سرویس اینترنت نیز از خصوصیات MPLS بی بهره نیستند به طوریکه مزایای Service provider ها از VPN های MPLS ی را می توان در موارد زیر خلاصه کرد:

- قابلیت میزبانی محتوی در داخل شبکه
- مستقل بودن انتقال
- امکان گروه بندی کاربران و سرویس های آنها به طور ساده
- کیفیت سرویس (QOS) در VPN ها
- سرویس اینترنتی (فایروال و IDS بایستی بین VPN ها و اینترنت قرار بگیرند)
- اجرای Ipsec تحت MPLS (اگر امنیت شبکه IP/MPLS ناکافی باشد)
- شبکه هسته به طور کامل از شبکه مشتری مخفی می شود.
- فعال سازی ویژگی های فایروال برای حمایت از شبکه MPLS

Ipsec & MPLS:

اگر یک یا چند نیاز زیر وجود داشته باشد ، باید Ipsec استفاده شود:

- رمزگذاری بخش ها یا همه ترافیک تحت هسته MPLS
- تغییر هویت نقاط انتهایی
- جامعیت ترافیک
- کشف Replay

گزینه های عمومی توپولوژی که با Ipsec در دسترس است شامل موارد ذیل است:

- نقطه به نقطه
- Hub and spoke
- Full mesh

نکات قابل توجه امنیتی در اجرای IP/MPLS در سازمانها و شرکت (نتیجه گیری):

۱. اطمینان از سازگاری و هماهنگی تجهیزات ارتباطی MPLS با تجهیزات مورد استفاده موجود (مثل سیسکو (edge) و هواوی و ...) و استفاده موازی از شبکه قدیم و جدید در بازه زمانی مشخص تا انتقال کامل سرویسها

۲. بهره گیری از سیستم Accounting کامل به طوریکه گزارشات حجمی و زمانی را داشته باشد.

۳. اطمینان از پشتیبانی سرویس های لازم Radius یا Tacact توسط IOS (گاهاً IOS های جدید ، سرویس های قدیمی را پشتیبانی نمی کنند.)

۴. نرم افزار محل آموزش کارکنان (معمولا کشور خارجی) با نرم افزارهای موجود در محیط اجراء واقعی، یکسان باشند.

۵. استفاده از Log Server

۶. اطمینان از اینکه IOS های تست شده روی تجهیزات ارتباطی با همان Version به کشور مقصد(ایران) می آیند.

۷. امکان Traffic Shapping کامل (حتی delay بین دو روتر مجاور را بدهد)

۸. امکان Traffic Monitoring کامل (performance را بدهد)

۹. اطمینان از اینکه تجهیزات ارتباطی خریداری شده همه سرویس های مورد نیاز ما را پشتیبانی نموده و مجبور به قراردادن Slot های اضافی آن به طور مکرر با تقبل هزینه های گزاف بعدی نباشیم.

۱۰. اخذ تمام ماجولهای I/O Manager و بکارگیری آن

۱۱. امکان Back up گیری کامل داشته باشد.

۱۲. باتوجه به اینکه تجهیزات Access عموماً در اختیار شعب (استانها) است. اطمینان از سازگاری تجهیزات استانها با Core وهمچنین شعبی (استانهایی) که از آلکاتل استفاده می کنند.

۱۳. اطمینان از سازگاری تجهیزات Tellaps با تجهیزات MPLS (مثلا هواوی یا ...)

۱۴. همکاری موثر همکاران با پرسنل پشتیبان و آموزش شرکت مربوطه با در نظرگرفتن ملاحظات امنیتی

و من ا... التوفیق