PSC2009
24rd International Power System Conference
09-F-DTC-0135
بیست و چهارمین
کنفرانس بین‌المللی برق

مسایل امنیتی در خصوص استفاده از شبکه‌های MPLS VPN در مخابرات صنعت برق کشور

مهدیه علی بخشی – صوفیا آهنج
کارشناس مخابرات – کارشناس ارشد الکترونیک
پژوهشگاه نیرو – گروه پژوهشی مخابرات
تهران, ایران

واژه‌های کلیدی: MPLS VPN، امنیت شبکه، DoS، نفوذ، IPSec

چکیده

امروزه بیشتر سرویس‌های جدید مورد نیاز در صنعت برق برمبنای IP بوده و یا درحال تبدیل به IP می‌باشد. مساله مهم در برقراری این سرویس‌ها، جداسازی آن‌ها بصورت امن است. مناسب‌ترین تکنولوژی برای برآوردن این نیاز، MPLS می‌باشد. تکنولوژی MPLS از دستاوردهای مهمی است که در سال‌های اخیر بسیار مورد توجه قرار گرفته و به یکی از استانداردهای مهم IP تبدل شده است. هرچند که هنوز این تکنولوژی در شبکه مخابرات صنعت برق مورد استفاده قرار نگرفته ولی به‌دلیل محدود بودن امکانات تجهیزات برای جداسازی فیزیکی سرویس‌ها، این طرح به عنوان بهترین راه‌حل برای جداسازی سرویس‌ها در لایه ۲/۵ شبکه مطرح می‌باشد. لذا به لحاظ امکان استفاده از آن در شبکه مخابرات صنعت برق (بصورت اختصاصی و یا بصورت اجاره‌ای شرکت مخابرات)، شناسایی تهدیدات و روش‌های افزایش امنیت MPLS دارای اهمیت بسزایی بوده و در این مقاله مورد بررسی قرار می‌گیرد.

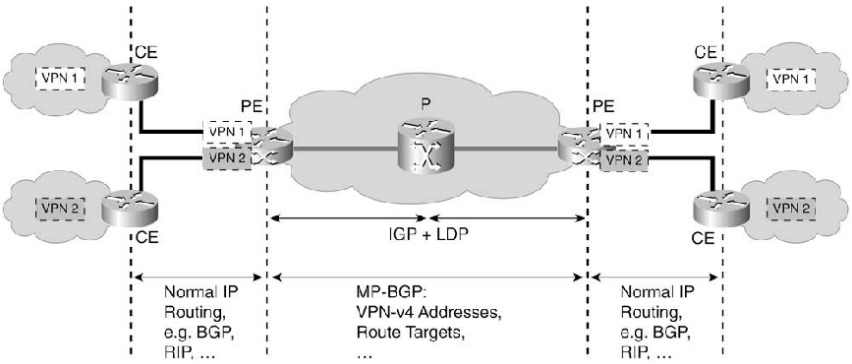
در این مقاله ابتدا مقدمه‌ای در خصوص MPLS ذکر شده و سپس به بررسی کلی شبکه‌های MPLS VPN و آنالیز امنیت آن پرداخته می‌شود. در نهایت مواردی که باید در تامین امنیت شبکه MPLS مدنظر قرار گیرد تا هکرها نتوانند از بیرون و یا درون شبکه به آن حمله کنند بیان می‌شود.

۱– مقدمه

با احداث شبکه مخابرات نوری در صنعت برق و ظرفیت بالای این شبکه، بحث استفاده از سرویس‌های مختلف جهت کنترل و مدیریت شبکه و کاربردهای اداری از طریق آن مطرح شده است. اگرچه امروزه سرویس‌های مورد استفاده در صنعت برق برمبنای IP نمی‌باشند ولی استفاده از این سرویس‌ها در آینده صنعت برق گریزناپذیر است. از جمله این سرویس‌ها می‌توان به سرویس‌های بازار برق، VoIP، ویدیو کنفرانس، DTS مبتنی بر IP و اینترانت (اتوماسیون‌های اداری) اشاره کرد. همچنین در صورت افزایش تعداد مراکز

دیسپاچینگ در سطح کشور به صورت توزیع شده، امکان نیاز به استفاده از نرم‌افزارهای دیسپاچینگ مبتنی بر IP نیز وجود خواهد داشت. همچنین علیرغم آنکه در حال حاضر اتصال به اینترنت برای شبکه مخابرات اختصاصی صنعت برق در نظر گرفته نشده است اما به‌دلیل ظرفیت بالای مخابرات نوری، این سرویس می‌تواند یکی دیگر از نیازهای آینده شبکه مخابرات صنعت برق باشد.

یکی از راه‌های جداسازی سرویس‌های مبتنی بر IP، استفاده از پورت‌های LAN مجزا در تجهیزات انتقال مخابرات نوری (جداسازی در لایه فیزیکی) می‌باشد. این روش اگرچه جداسازی کاملی را ایجاد می‌نماید اما با محدویت‌هایی مواجه است که مهمترین آنها محدود بودن تعداد پورت‌های LAN در هر سیستم مخابراتی می‌باشد.



شکل ۱- نمونه‌ای از ارتباطات اختصاصی از طریق VPN

راه‌حل دیگر برای جداسازی سرویس‌ها، استفاده از یک شبکه یکسان و ایجاد شبکه‌های اختصاصی مجازی (VPN[1]) برای هر سرویس می‌باشد. در واقع با استفاده از یک پورت LAN و با کمک تکنولوژی VPN می‌توان جداسازی سرویس‌های مختلف را انجام داد. شکل ۱ نمونه‌ای از این ارتباطات را نشان می‌دهد. در واقع این نودها به جای استفاده از خطوط اختصاصی، از VC[2] یا مدارات مجازی برای داشتن ارتباط اختصاصی استفاده می‌نمایند.

ارتباطات VPN به دو طریق مورد استفاده قرار می‌گیرند. مدل اول بصورت دسترسی کاربر از راه دور است. سازمان‌هائی که از مدل فوق استفاده می‌نمایند، به‌دنبال ایجاد تسهیلات لازم برای ارتباط پرسنل از راه دور به شبکه سازمان می‌باشند. مدل دیگر استفاده بصورت سایت به سایت است. در این مدل یک سازمان با توجه به سیاست‌های موجود، قادر به اتصال چندین سایت از طریق یک هسته مرکزی می‌باشد. در شبکه مخابرات صنعت برق، احتمال بکارگیری هر دو روش با استفاده از خطوط اجاره‌ای شرکت مخابرات یا در آینده در شبکه اختصاصی وجود دارد.

برای ایجاد شبکه‌های VPN، فناوری‌های مختلفی از جمله ATM و Frame Relay در لایه ۲ و MPLS در لایه ۲/۵ وجود دارد. بهترین و جدیدترین روش برای پیاده‌سازی VPN، استفاده از فناوری MPLS بدلیل پیاده‌سازی ساده‌تر، قیمت مناسب‌تر، قابلیت پشتیبانی از پروتکل‌های مختلف و همچنین کیفیت‌سرویس بالاتر می‌باشد.

۲- مروری بر MPLS

MPLS بر پایه پروتکل چندگانه استوار است. بدین معنی که این تکنولوژی بر روی هر ساختار و معماری قابل پیاده‌سازی و اجرا می‌باشد و از این نظر دارای محدودیتی نیست. در این مبحث پیاده‌سازی بر روی IP مد نظر می‌باشد.

[1] Virtual Private Network
[2] Virtual Circuit

بطور کلی مزایای استفاده از MPLS شامل مهندسی ترافیک، کیفیت سرویس‌دهی، مقیاس پذیری[1]، ایجاد VPN و همچنین پشتیبانی از پروتکل‌های چندگانه است.

در شبکه‌های سنتی بر مبنای IP، برای انتقال بسته‌های داده در هر روتر، سربار بسته‌ها جداگانه باز و آنالیز شده و سپس الگوریتم مسیریابی در هر روتر اجرا و مسیر مناسب انتخاب می‌شود. این عمل برای هر بسته بطور مستقل و برروی هر روتر انجام می‌گیرد. با اندکی دقت مشخص می‌شود که با روند رشد ترافیک، عملیات پردازشی بسیار افزایش یافته و کیفیت سرویس بسیار کاهش می‌یابد. درحالیکه در شبکه MPLS به جای استفاده از آدرس IP برای مسیریابی، از برچسب[2] استفاده می‌شود. بدین صورت که بر روی سربار هر بسته ورودی به شبکه MPLS یک برچسب بیست بایتی قرار می‌گیرد. هر گونه عملیات پردازشی مورد نیاز بر روی این بسته با توجه به برچسب آن انجام می‌شود و دیگر بر روی آدرس IP آن، عملیات خاصی صورت نمی‌گیرد.

روتری که عملیات برچسب‌زنی به بسته‌ها را انجام می‌دهد، LER[3] یا روتر PE[4] نامیده می‌شود و به روترهای خارج از شبکه MPLS که روتر CE[5] نامیده می‌شود، متصل می‌شود. روترهای درون شبکه MPLS که روترهای PE را به‌یکدیگر متصل می‌کنند، LSR[6] یا روتر P[7] نامیده می‌شوند. عملیات مسیریابی در درون شبکه MPLS با استفاده از پروتکل‌های مسیریابی MP-BGP[8] و IGP[9] انجام می‌شود که مسیر بهینه برای عبور بسته‌ها که LSP[10] نامیده می‌شود را تعیین می‌کند (مطابق شکل ۱).

یکی از عناصر کلیدی تکنولوژی MPLS VPN، جدول مسیریابی بسته داده است که VRF[11] نامیده می‌شود. در واقع هر روتر P در شبکه MPLS یک جدول مسیریابی VRF دارد (مطابق شکل ۲) که در ستون اول آن برچسب بسته‌های ورودی، در ستون دوم، آدرس IP بسته‌های ورودی، در ستون دیگر شماره واسط خروجی و در ستون آخر برچسب خروجی مشخص شده است. قابل ذکر است که هر VPN بر روی PE متصل به آن دارای یک جدول VRF می‌باشد. در یک PE، کنترل مبادله مسیرهای خاص هر VPN، توسط RT[12] انجام می‌شود. RT مسیرهای ورودی و خروجی به هسته MPLS و VRF مربوطه را تعیین می‌کند [۱،۲،۳].

۳- بررسی تهدیدات MPLS VPN

بطور کلی تهدیدات شبکه MPLS از نظر VPN و هسته MPLS قابل بررسی می‌باشد.

تهدیدات VPN بطور کلی شامل دو دسته است [۴،۵]:

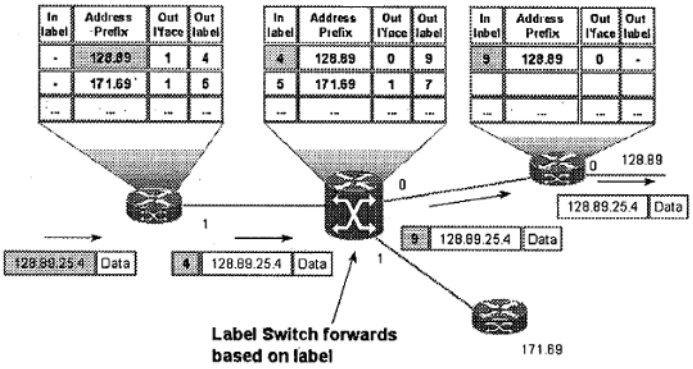
- نفوذ از طریق VPNهای دیگر، هسته و...
- انکار سرویس (DoS[13]) از طریق VPNهای دیگر، هسته و...

شکل ۳ پتانسیل‌های نفوذ به VPN و شکل ۴ نقاط مورد نظر در حمله DoS را نشان می‌دهد. تفاوت کلیدی بین نفوذ و حمله DoS این است که نفوذ، اجازه دسترسی کامل به داده‌ی داخلی را می‌دهد در حالی که DoS از دسترسی همه کاربران جلوگیری می‌کند. در عمل، هر قسمت از شبکه که به اشتراک گذاشته شده، ممکن است تحت تأثیر حمله DoS قرار گیرد.

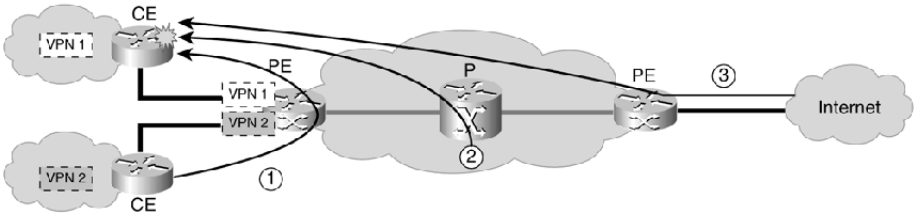
معماری‌های مختلفی برای ایجاد هسته MPLS وجود دارد. امن‌ترین آن‌ها، هسته MPLS بصورت یک سیستم مستقل (AS[14]) است که در این معماری، هسته بصورت یکپارچه تحت کنترل قرار می‌گیرد که به آن هسته یکپارچه می‌گویند. تهدیدات علیه هسته یکپارچه عبارتند از [۴]:

- نفوذ از VPNهای متصل به هسته یا از طریق اینترنت
- انکار سرویس (DoS) توسط VPNهای متصل به هسته یا از طریق اینترنت
- تهدیدات داخلی شامل خطای اپراتور و یا پیکربندی نادرست که می‌تواند مشکلات امنیتی را به وجود آورد.

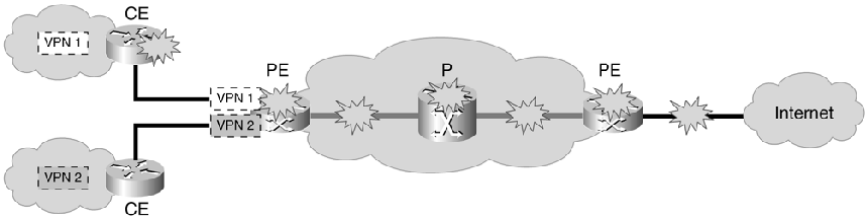
[1] Scalability
[2] Label
[3] Label Edge Router
[4] Provider Edge Router
[5] Customer Edge
[6] Label Switching Router
[7] Provider Router
[8] Multi-Protocol Border Gateway Protocol
[9] Interior Gateway Protocol
[10] Line Switching Path
[11] VPN Routing Forwarding Table
[12] Roue Target
[13] Denial of Service
[14] Autonomous System



شکل ۲- جداول مسیر یابی در LSRها



شکل ۳- جهت‌های نفوذ به یک VPN



شکل ۴- نقاط مورد حمله DoS در VPN

۴- بررسی امنیت معماری MPLS

داشتن سرویس‌های اختصاصی و امن به اندازه مدارات اختصاصی، یکی از نیازهای اصلی کاربران VPN می‌باشد. نیازهای امنیتی VPN بطور خلاصه عبارتند از [۴،۵،۶]:

- جداسازی VPN (شامل آدرس و ترافیک VPN)
- مقاوم‌سازی در مقابل حملات
- مخفی‌سازی ساختار هسته
- حفاظت در مقابل جعل IP[1]

جهت برآورده ساختن نیازهای فوق در شبکه MPLS، استاندارد RFC 2547bis با نام "BGP/MPLS VPNs" توسط IETF[2] تدوین شده است که در ادامه به بررسی چگونگی تامین هر یک از این نیازها درصورت بکارگیری این استاندارد پرداخته می‌شود.

[1] Spoofing
[2] Internet Engineering Task Force

۴-۱- جداسازی VPN (آدرس و ترافیک)

یکی از مهمترین نیازهای VPN، جداسازی ترافیک آن از ترافیک دیگر VPNها و ترافیک هسته است. به عبارت دیگر ترافیک یک VPN نباید در دیگر VPNها دیده شود. نیاز دیگر هر VPN، توانایی استفاده از فضای آدرس‌دهی IP بطور کامل، بدون اثر بر روی دیگر VPNها می‌باشد. همچنین تهیه‌کننده‌های سرویس MPLS نیاز دارند که هسته از VPNها جدا باقی بماند و فضای آدرس آن با VPNها تضادی نداشته باشد. به عبارت دیگر یک VPN باید بطور کامل از دیگر VPNها یا هسته MPLS از لحاظ ترافیک و آدرس جدا باشد.

در RFC 2547bis برای تمایز بین آدرس‌های VPNهای مختلف، از استاندارد آدرس‌دهی IPv4 یا IPv6 استفاده نمی‌شود و در عوض از استاندارد خانواده آدرس VPN-IPv4 و VPN-IPv6 استفاده می‌شود. بطور مثال آدرس

VPN-IPv4 شامل هشت بایت مشخص‌کننده مسیر(RD[1]) به‌اضافه چهار بایت IP می‌باشد. در واقع با استفاده از هشت بایت RD، اجازه آدرس دهی کامل IPv4 به همه VPNها داده می‌شود.

در معماری MPLS VPN، تنها روترهای PE باید مسیرهای VPN را بشناسند. از آنجایی‌که فقط روترهای PE از VPN-IPv4 برای آدرس دهی VPNها استفاده می‌کنند لذا فضای آدرس VPNهای مختلف کاملا مجزا از یکدیگر می‌باشد. علاوه بر آن بدلیل آنکه روترهای درون هسته MPLS بطور داخلی از IPv4 استفاده می‌کنند که از خانواده آدرس متفاوتی از خانواده آدرس VPN-IPv4 است، آدرس هسته نیز مستقل از آدرس‌های VPNهاست. این امر باعث جداسازی کامل آدرس بین VPNها و همچنین بین VPNها و هسته می‌شود.

جداسازی ترافیک در واقع به مفهوم جداسازی ترافیک کنترل و داده هسته و داده VPN است. بدین معنی که ترافیک هسته با ترافیک VPNمخلوط نشده و بسته‌های یک VPN به دیگر VPNها ارسال نشود و دیگر VPNها نتوانند داده‌ای به داخل VPN مورد نظر وارد نمایند. در خصوص تهیه کننده سرویس، این تعریف متفاوت است زیرا ترافیک VPNها همواره در هسته شبکه MPLS انتقال داده می‌شوند. البته ترافیک سطح دیتا در هنگام عبور از هسته شبکه در یک LSP کپسوله می‌شود و از یک PE به یک PE دیگر منتقل می‌گردد لذا هسته، هرگز ترافیک VPN را به علت کپسوله‌شدن نمی‌بیند. در واقع جداسازی ترافیک بین VPNهای مختلف با کپسوله کردن بسته دریافتی بر اساس سربار VPN مربوطه انجام می‌شود.

بطور خلاصه می‌توان گفت به دلایل زیر ترافیک هر VPN از دیگر VPNها و هسته مجزا می‌باشد:

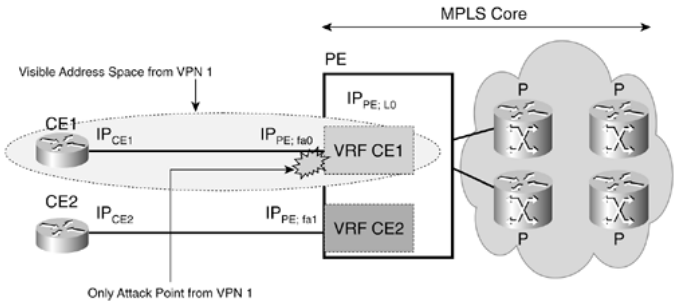
- واسطهای یک PE یا به یک VRF و یا به هسته تعلق دارند.
- مدار اتصالی (خطوط CE-PE) به طور منطقی به یک VPN متعلق است و VPNهای دیگر به آن دسترسی ندارند.
- در هر PE، اطلاعات آدرس هر VPN بصورت VPN-IPv4 نگهداری می‌شود که هر VPN را با استفاده از RD، مجزا و یکتا می‌سازد. آدرس VPN-IPv4 فقط در روترهای PE نگهداری می‌شوند.
- ترافیک VPN در هسته از طریق مسیرها و تونل‌های خاص VPN ارسال می‌شود. ارسال از طریق نشانه‌گذاری هر بسته با برچسب ویژه هر VPN صورت می‌گیرد.
- روترهای P اطلاعاتی از VPN ندارند، بنابراین نمی‌توانند در جداسازی VPNها دخالتی داشته باشند.
- از دید تهیه‌کننده‌های سرویس MPLS نیز هسته از VPNها مجزا می‌باشد زیرا آدرس‌های روترهای P و PE، IPv4 است و VPNها منحصراً از VPN-IPv4 استفاده می‌نمایند لذا VPNها به روترهای P و PE نمی‌توانند دسترسی داشته باشند.

۴-۲- مقاومت هسته در برابر حمله

از آنجاکه همه VPNها از یکدیگر و از هسته مجزا هستند، این مساله باعث محدود شدن نقاط حمله می‌شود. شکل ۵ نقطه اتصال VPN به هسته را که همان روتر PE یا به عبارتی واسط CE-PE است نشان می‌دهد. نقاط حمله توسط یک VPN، منحصر به این واسط است و یک VPN نمی‌تواند دیگر واسطها را در PE و هیچکدام از روترهای هسته ببیند. اما در MPLS VPN اگر یک حمله‌کننده بتواند یک PE را کنترل کند، امنیت همه VPNهای هسته چه مستقیماً به آن PE متصل باشد یا متصل نباشد، به خطر می‌افتد. بنابراین امن بودن PEها یک پارامتر مهم برای تهیه‌کنندگان سرویس و همچنین برای کاربران VPN است و بنابراین تنها باید از واسط PE مربوط به آن VPN حفاظت کرد [۴].

همچنین با توجه به آن‌که یک روتر CE حتی اگر بوسیله تهیه کننده سرویس مدیریت شود بدلیل ماهیت آن همیشه نامطمئن است بنابراین تنها نقطه حمله در یک محیط MPLS VPN می‌باشد.

[1] Route Distinguisher



شکل ۵- فضای آدرس قابل دید از VPN

در عمل یک PE می‌تواند با ترافیک انتقالی (ترافیکی که مقصد آن PE نیست) و یا ترافیک دریافتی (ترافیکی که مقصد آن PE است) مورد حمله واقع شود. ترافیک انتقالی معمولاً دارای مشکلات کمتری است زیرا روترها طوری طراحی شده‌اند که این ترافیک را سریعاً منتقل نمایند لذا یک روتر باید پتانسیل برقراری ترافیک انتقالی را بطور مناسب دارا باشد که این مساله باید در طراحی شبکه درنظر گرفته شود. هرچند شکل‌های خاصی از بسته‌ها وجود دارند که نمی‌توانند در سخت‌افزار روتر براحتی عبور کنند لذا سبب اضافه بار در روتر می‌شوند بنابراین جریان این بسته‌ها می‌تواند منجر به حمله DoS در روترها شود. بسته‌هایی با IP انتخابی[1] یک مثال از این گونه بسته‌ها هستند. یک بسته با IP انتخابی، یک سربار IP با طول متغیر دارد و بنابراین در ASIC[2]های موجود در روتر قابل شناسایی نیست که به این معنی است که بسته‌هایی با IP انتخابی، باید در نرم افزار سوئیچ شود. این عمل سبب کاهش کارایی یک روتر می‌شود.

در خصوص حمله به هسته، ترافیک دریافتی و یا به‌عبارت دیگر ترافیک‌هایی با مقصد PE، دارای اهمیت بیشتری هستند زیرا اثر مستقیمی بر روی PE دارند. دو شکل از حملات که توسط ترافیک دریافتی امکانپذیر است عبارتند از:

DoS- این عمل بطور مثال می‌تواند از طریق فرستادن تعداد زیادی از فایل‌های به‌روزرسانی مسیریابی به روتر انجام شود، که همه حافظه موجود در PE را درگیر نماید.

نفوذ- در این روش حمله کننده با استفاده از کانال غیر مجاز سعی در تغییر پیکربندی PE دارد. برای مثال حملات حدس زدن کلمه عبور پورت‌های telnet، SSH یا نوشتن بر روی پورت SNMP[3] روتر از این دسته حملات می‌باشند. البته این پتانسیل حمله می‌تواند با پیکربندی مناسب بر اساس استاندارد به‌درستی کنترل شود. اما در عمل مشکلات عملکردی مانند پیکربندی نادرست یا ضعف کلمه عبور و نیز مشکلات پیاده‌سازی (در جائیکه ممکن است آسیب‌پذیری‌های امنیتی در سیستم عملکردی وجود داشته باشد) می‌تواند رخ دهد.

۴-۳- مخفی‌سازی هسته

VPNهای لایه دو قدیمی مانند ATM و Frame Relay دارای معماری هستند که کاربر VPN نمی‌تواند ساختار هسته را مشاهده نماید. به این دلیل که کاربرVPN در لایه سه و هسته شبکه‌های فوق در لایه دو شبکه عمل می‌کنند. شبکه‌های MPLS VPN نیز اغلب ساختار معماری هسته را مخفی می‌سازند. در واقع تنها آدرس‌های روتر PE در معرض دید کاربر بوده و روترهای P کاملاً مخفی هستند. این امر به علت جداسازی ذاتی آدرس در هسته MPLS می‌باشد بطوریکه حتی اگر آدرس روتر P بدست آورده شود، از آنجا که این آدرس با فضای آدرس‌دهی کاربر VPN متفاوت است بنابراین غیرقابل دسترسی است. تنها استثنا آدرس‌های روتر PE است که این آدرس‌ها نیز متعلق به VPN است نه به هسته. البته در صورت اتصال چندین VPN به یک PE، اگرچه یک فضای آدرس‌دهی کامل می‌تواند بدون

[1] IP Options
[2] Application Specific Integrated Circuit
[3] Simple Network Management Protocol

تداخل برای هر VPN تخصیص داده شود ولی همیشه باید در نظر گرفت که آدرس‌های PE در معرض دید هر VPN هستند و این موضوع یکی از تهدیدات اصلی امنیت شبکه است.

برای مخفی نگه داشتن کامل روترهای PE از جانب کاربر VPN، راه‌حل‌هایی وجود دارد. استفاده از مسیریابی استاتیک بین CE-PE و نیز اعمال کنترل دسترسی از طریق ACL[1] از آن جمله می‌باشد [۴].

۴-۴- حفاظت در برابر جعل

امروزه جعل IP یکی از وقایعی است که همه روزه در حملات مختلف اتفاق می‌افتد. از آنجائی که MPLS تکنولوژی لایه دو و نیم است کاربران شبکه MPLS همواره نگران وقوع جعل در سطح IP و نیز در سطح برچسپ می‌باشند که در ادامه به بررسی آن‌ها پرداخته می‌شود [۴].

۴-۴-۱- امنیت در برابر جعل آدرس IP

هر VPN بصورت تئوری می‌تواند از فضای آدرس‌دهی کامل از 0.0.0.0 تا 255.255.255.255 استفاده کند. یک سایت VPN ممکن است آدرس‌های IP را جعل نماید اما جعل آدرس IP تنها در همان VPN باقی می‌ماند. از آنجا که هر VPN در هسته توسط آدرس RD مشخص شده و RD در PE تعیین می‌شود، درنتیجه جعل IP در خود VPN باقی مانده و به VPNهای دیگر اثر نمی‌گذارد بنابراین جعل IP در VPN نمی‌تواند بر تفکیک VPN اثر بگذارد.

۴-۴-۲- امنیت در برابر جعل برچسپ

درون هسته MPLS، بسته‌های VPNهای مختلف به‌وسیله برچسپ VPN (با استفاده از RD) از هم جدا می‌شوند. یک کاربر ناراضی ممکن است سعی کند بسته‌های جعلی را با جعل برچسپ مربوط به VPNهای دیگر تولید کند و سعی برای فرستادن بسته نماید. اما از آنجا که روتر PE، بسته‌های برچسپ‌دار را از CEها دریافت نمی‌کند لذا بسته‌های جعلی به آسانی به وسیله روتر PE حذف می‌شوند. البته این مساله فقط برای معماری استاندارد MPLS با هسته یکپارچه صادق است زیرا دیگر معماری‌های MPLS که دارای هسته یکپارچه نیستند، اجازه می‌دهند که بسته‌های برچسپ دار به روتر PE فرستاده شوند. در این معماری‌ها درصورتیکه یک بسته با برچسپ جعلی شده وارد هسته شود ممکن است واقعا به یک VPN دیگر برسد.

۴-۵- موضوعات امنیتی که MPLS آنها را پوشش نمی‌دهد

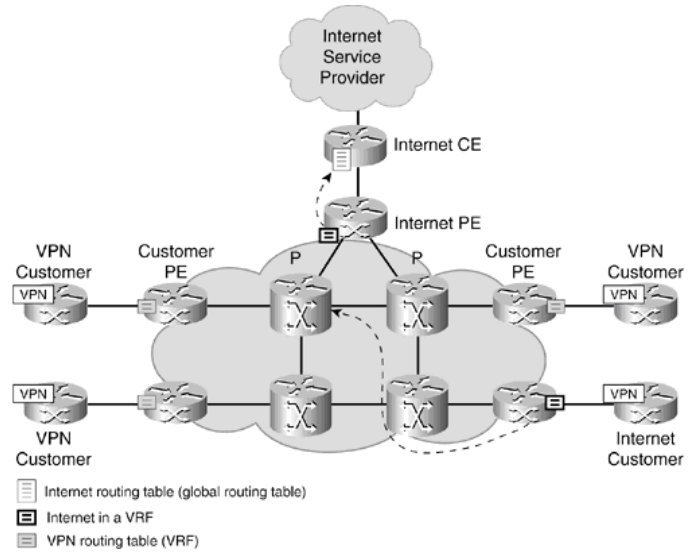
در بحث امنیت MPLS، موضوعاتی وجود دارد که MPLS در خصوص آن‌ها اقدامی انجام نداده و نمی‌تواند آنها را کنترل نماید. لیست زیر بیان کننده این موضوعات است:

- حفاظت در مقابل پیکربندی نادرست یا اشتباه‌های عملکردی - بطور مثال اگر روتر PE بطور صحیح پیکربندی شود، دارای امنیت می‌باشد اما اگر اپراتور در پیکربندی PE اشتباه کند، امنیت شبکه به خطر می‌افتد.
- محرمانگی، تمامیت داده VPN و تصدیق صحت - هیچ ضمانتی در خصوص عدم شنود و خرابی بسته در حین انتقال در هسته MPLS وجود ندارد و MPLS هیچ‌کدام از سرویس‌های محرمانگی، تمامیت داده و تصدیق صحت را ایجاد نمی‌نماید.
- امنیت شبکه مشتری - حملات در داخل VPNها مرتبط به شبکه MPLS نبوده و لذا امنیت آن در نظر گرفته نشده است.

در مجموع درصورت پیاده‌سازی شبکه MPLS براساس استاندارد RFC 2547bis، این شبکه‌ها به دلایل زیر می‌توانند بطور امن عمل نمایند:

- VPNها کاملاً جدا هستند (آدرس و ترافیک).
- هسته به آسانی مورد حمله واقع نمی‌شود.
- جعل آدرس و برچسپ VPN غیرممکن است.
- هسته برای کاربران VPN غیرقابل مشاهده می‌باشد.

[1] Access Control List



شکل ۶- اتصال به اینترنت از طریق نگهداری مسیرها در VRF

۵- نکات مطرح در طراحی امن شبکه MPLS

از آنجاکه دسترسی به اینترنت یکی از نیازهای مرسوم در شبکه‌ها می‌باشد در این بخش به شرح چگونگی برقراری این دسترسی به صورت امن پرداخته می‌شود. همچنین علیرغم توضیحات ذکر شده در خصوص امنیت ذاتی MPLS درصورت پیکربندی صحیح، همواره احتمال پیکربندی نادرست یا اشتباه اپراتورهای تعمیر و نگهداری وجود دارد لذا برای جلوگیری از وقوع تهدید نفوذ، استفاده از فایروال‌ها توصیه می‌شود و راهکارهایی نیز برای مقابله با DoS در شبکه مطرح می‌باشد. در ادامه به معرفی این راهکارها پرداخته می‌شود.

۵-۱- دسترسی امن به اینترنت

راه امن ایجاد اینترنت، نگهداری مسیرهای اینترنت در جدول VRF است. در این مدل، ترافیک اینترنت مشابه یک VPN در شبکه MPLS برقرار می‌شود (شکل ۶). در این مدل، اتصال به ISP[1] مستقیما از طریق جدول VRF و از طریق روتر PE برقرار می‌شود و مشتری‌هایی که نیاز به اینترنت دارند به VPN اینترنت متصل می‌شوند.

از آنجائیکه اینترنت در حقیقت یک VPN در هسته است، لذا همه ویژگی‌های بیان شده در خصوص MPLS VPN در آن صادق می‌باشد و تفاوت آن با سایر VPNها در این است که VPN مشتری نبوده و بخشی از سرویس می‌باشد.

البته بسته‌های داده هنوز به عنوان یک پتانسیل حمله از اینترنت مطرح می‌باشند و احتمال حمله DoS وجود دارد که ممکن است برروی PE و درنتیجه بر روی VPNهای متصل به آن اثر بگذارد. راه‌حل این مشکل در بخش طراحی شبکه مقاوم در برابر DoS مطرح خواهد شد.

۵-۲- فایروال

اگرچه VPNها در شبکه MPLS بطور ذاتی از یکدیگر مجزا می‌باشند اما این جداسازی کافی نبوده و اقدامات امنیتی دیگری نیز مورد نیاز است. فایروال‌ها یک راه‌حل برای جلوگیری از این مشکلات می‌باشند. برای انتخاب بهترین توپولوژی برای قرار دادن فایروال، باید مراحل زیر درنظر گرفته شود:

۱- داشتن یک نقشه از تمام شبکه که شامل سایت‌های VPN و مناطق اکسترانت (قسمت مشترکی از شبکه که همه VPNها به آن دسترسی دارند) و اینترنت است. البته مفهوم کلیدی در تهیه این نقشه دسترس‌پذیری است، یعنی چه کسی می‌تواند به چه چیزی دسترسی یابد.

[1] Internet Service Provider

۲- تقسیم کل شبکه به "مناطق اعتماد" یا به عبارتی تقسیم شبکه بر اساس سیاست‌های امنیتی. بطور مثال اینترنت، اکسترانت، هر VPN و هسته MPLS مناطق جدایی از هم باشند.

فایروال‌ها برای همه مرزهای مناطق تعیین شده موردنیاز می‌باشند. بر طبق این روش حتی بین هسته MPLS و VPNها نیز فایروال مورد نیاز می‌باشد. البته هسته MPLS معمولاً از طرف مشتری‌های VPN مورد اعتماد است و آن‌ها هیچ راهی جز اعتماد به هسته ندارند. اگر نتوان به هسته اعتماد کرد، در این صورت فایروال‌ها نیز نقش اندکی در این رابطه خواهند داشت. بنابراین فایروال‌ها تنها در نقاط بین اینترنت - هسته و اکسترانت - هسته مورد نیاز می‌باشند. اما از دید هسته، مشتری VPN غیرقابل اعتماد است لذا باید هسته در برابر هر VPNحفاظت شود. برای حفاظت هسته در مقابل کاربران VPN، هسته از فایروال استفاده نمی‌کند بلکه از دیگر اقدامات امنیتی مانند زیرساخت‌های ACL، تامین امنیت روتر به علاوه امنیت پروتکل مسیریابی (از طریق پیکربندی روترها به منظور استفاده از قابلیت تصدیق صحت MD-5) استفاده می‌نماید.

فایروال بین VPNها و اینترنت و اکسترانت می‌تواند به طرق مختلف ایجاد شود. فایروال می‌تواند در سایت VPN قرار داده شود که در این صورت تحت کنترل کاربران VPN می‌باشد. از طرف دیگر یک فایروال مرکزی می‌تواند برای شیلد کردن VPNها در مقابل مناطق اعتماد خارجی استفاده شود(فایروال مجازی). شکل ۷ این مسئله را نشان می‌دهد. در این روش فایروال‌های مجازی، VRF هر VPN را که نیاز به اتصال به اینترنت/اکسترانت دارد در خود نگه می‌دارد. در واقع در این روش، فایروال‌های مجازی، جداسازی مشتری‌ها را مانند PE بر اساس VRF انجام می‌دهند. بنابراین در این روش هر VPN می‌تواند فضای آدرس IP خود را بطور کامل استفاده نماید و هر VPN، فایروال مجازی را بصورت فایروال اختصاصی خود درنظر می‌گیرد.

در صورتی که VPNها با سطوح مختلف امنیتی بخواهند که به اینترنت/اکسترانت متصل شوند، فایروال باید بین این سایت‌ها مانند شکل۸ قرار داده شود. در این مثال فایروال، درون هر VPNای که از آن حفاظت می‌کند قرار گرفته‌است و هر خط بین فایروال و روتر PE به یک VPN تعلق دارد.

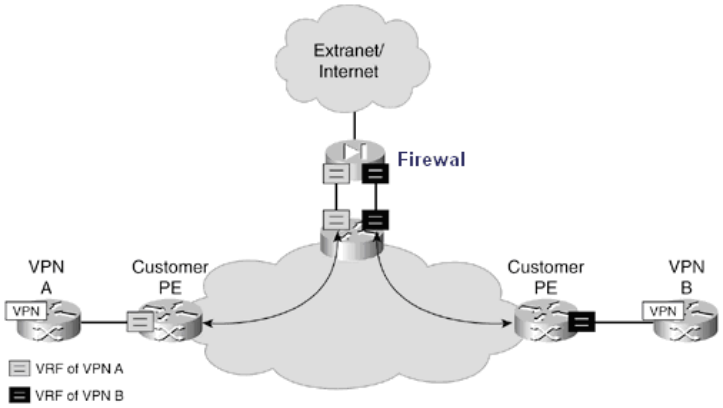
بطور کلی اصولاً فایروال‌ها برای جلوگیری از نفوذ استفاده می‌شوند و در مقابل تهدید DoS موثر نیستند. برای مثال اگر خطوط دسترسی بین فایروال و PE اضافه بار داشته باشد، (مطابق شکل ۷) فایروال در برابر اضافه بار کمکی نمی‌کند و حتی درصورتی‌که روتر PE اضافه بار داشته باشد، ممکن است بر VPNهای دیگر متصل به آن (فایروال مجازی) اثر بگذارد [۴،۵،۶].

۵-۳- طراحی شبکه مقاوم در برابر DoS

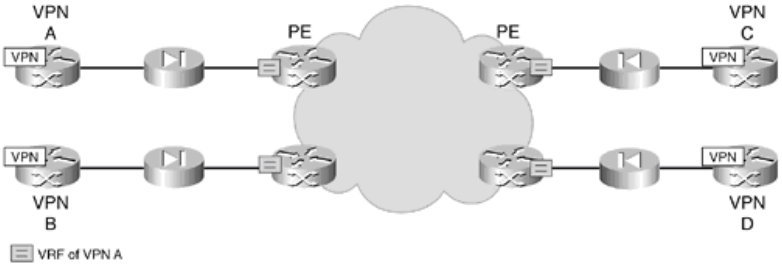
حملات DoS با تاثیرگذاری بر روی منابع خاص اشتراکی از جمله پهنای باند، CPU و حافظه ایجاد می‌شود. بنابراین برای حفاظت در برابر حملات DoS، شبکه باید طوری طراحی شود که هیچ کدام از منابع آن نتوانند توسط مهاجم اضافه بار پیدا کنند. بطور کلی راه‌حل‌هایی را که می‌توان جهت مقاومت در برابر حملات DoS در هر شبکه (نه تنها در شبکه MPLS) ارائه نمود عبارتند از [۴]:

- استفاده از تجهیزات مناسب؛ هر وسیله در شبکه باید قادر به پردازش حداکثر بار وارد شونده به آن باشد. روترهای لبه شبکه نیز باید توانایی پشتیبانی از حداکثر سرعت خط را داشته باشند.
- طراحی پهنای باند مناسب؛ خطوط شبکه باید قادر به برقراری ترافیک رگباری[1] باشند. این عمل به دو طریق قابل انجام است. یکی در نظر گرفتن منابع اضافه بصورتیکه خطوط حتی در بدترین حالت طوری طراحی شوند که دچار اضافه بار نشوند و دوم طراحی شبکه به‌نحوی‌که کیفیت سرویس آنها پایین نیاید. یعنی نه تنها ترافیک اضافی در نظر گرفته شود بلکه ترافیک به دو نوع کم اهمیت و پر اهمیت تقسیم شود.

[1] Burst



شکل ۷- فایروال بین VPN و اینترنت/اکسترانت



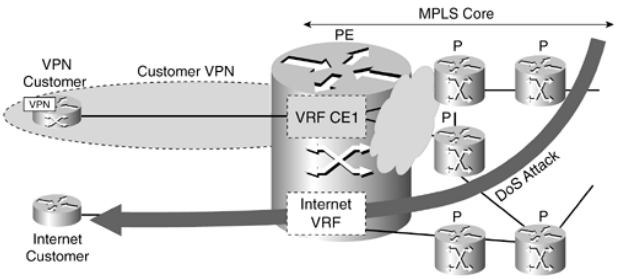
شکل ۸- فایروال بین VPNها با سیاست‌های امنیتی مختلف

- در نظر گرفتن سرویس‌ها بیش از اندازه مورد نیاز؛ بطور مثال سرویس‌های وب باید طوری طراحی شوند که بدترین حالت در نظر گرفته شود.
- راه‌حل‌های ضد DoS؛ هر شبکه‌ای باید با تجهیزاتی برای جلوگیری از حمله DoS مجهز شود که بتواند حملات DoS را آنالیز و تشخیص و این حملات را کاهش دهد. سیستم Cisco Guard نمونه‌ای از این‌گونه تجهیزات می‌باشد.

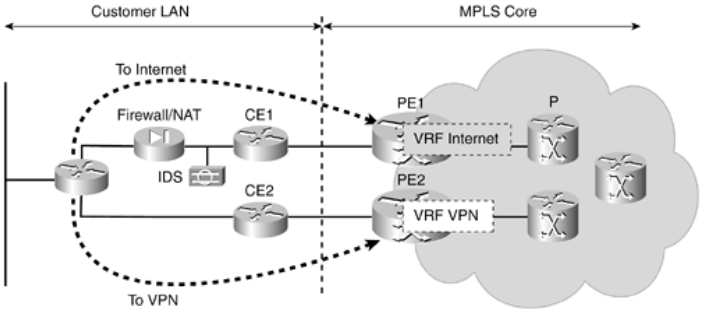
در شبکه‌های MPLS، وجود روتر لبه مقاوم در برابر DoS از اهمیت ویژه‌ای برخوردار است. این امر خصوصاً در مواقعی که روتر PE به چندین VPN سرویس‌دهی کند اهمیت بیشتری دارد (شکل ۹). مطابق این شکل حمله DoS می‌تواند از طریق یکی از VPNها انجام شود. حملات DoS معمولاً از طریق اینترنت انجام می‌شوند ولی این حملات می‌توانند توسط دیگر VPNها نیز انجام شوند. اغلب روترهای PE موجود در صنعت، از منابع مشترک (CPU، پهنای باند و حافظه) برای VRFهای مختلف استفاده می‌کنند که این موضوع به معنی آن است که حمله DoS درصورت استفاده از یک PE مشترک برای چند VPN می‌تواند بر روی همه VPNهای متصل به PE اثر بگذارد. جهت حل این مشکل برخی شرکت‌ها راه‌حل‌هایی را ارائه کرده‌اند. بطور مثال شرکت CISCO روتری به نام IOS-XR تولید نموده که حفاظت موثری را در مقابل حافظه و CPU برای VRFهای مختلف در برابر حملات DoS ایجاد می‌نماید. در این روتر تنها VPN تحت حمله مستقیم، تحت تاثیر قرار می‌گیرد و VPNهای دیگر در PE از کار نمی‌افتند.

به‌دلیل آنکه اکثر روترهای موجود، حفاظت CPU و حافظه در مقابل حمله DoS ندارند، مشکل PE اشتراکی باید با استفاده از طراحی‌های مختلف برطرف گردد. بهترین راه‌حل به این منظور استفاده از PE مجزا برای هر VPN می‌باشد.

همچنین درصورتیکه VPN خواستار اتصال به اینترنت باشد، از آنجاکه احتمال حمله DoS از اینترنت بیشتر از حمله DoS از طریق VPN است، پیشنهاد می‌شود که این دو سطح امنیتی نیز کاملاً مجزا از هم طراحی شوند.



شکل ۹- PE روتر اشتراکی بین چنین VPN تحت حمله DoS



شکل ۱۰- جداسازی روتر PE اینترنت و VPN

شکل ۱۰ ایده این کار را نشان می‌دهد. در این روش بجای یک روتر PE، دو روتر قرار داده می‌شود که یکی تنها اتصال VPN و دیگری اتصال به اینترنت را برقرار می‌کند. به این طریق اگر حمله از اینترنت صورت گیرد تنها روتر PE مربوط به VPN اینترنت مورد حمله واقع می‌شود. همچنین در این روش می‌توان برای افزایش امنیت از یک فایروال به‌علاوه سیستم‌های امنیتی دیگر مانند سیستم تشخیص نفوذ (IDS)[1] نیز استفاده نمود. این روش مقاومت بالایی را در مقابل حملات DoS ایجاد می‌نماید و در حقیقت تنها قسمت اینترنت در معرض حمله DoS است و مسیریابی باید طوری ایجاد شود که ترافیک اینترنت هرگز از روتر PE مربوط به VPN نگذرد. در حقیقت برای جلوگیری از حملات مستقیم، روتر PE مربوط به VPN نباید از طریق اینترنت در دسترس باشد و اگر از طریق هسته، روتر PE مربوط به VPN مخفی نباشند باید حتماً ساختار ACL برای جلوگیری از دسترسی به این روترها به‌کارگرفته شود.

۶- تکمیل ویژگی‌های امنیتی MPLS با استفاده از IPSec

MPLS از برخی لحاظ (بطور مثال محرمانگی) دارای ضعف است. برای جبران این ضعف‌ها، تکنولوژی MPLS VPN می‌تواند نتایج کار خود را روی IPSec اضافه کند و از مزایای هر دو تکنولوژی استفاده شود. مزیت اصلی IPSecها در امنیت شبکه می‌باشد. این VPNها، داده انتقالی را رمز نموده و تصدیق هویت و تمامیت را برقرار می‌نمایند. IPSec یک تکنولوژی است که سرویس‌های امنیتی شامل قابلیت اعتماد از طریق رمزنگاری یا محرمانگی، تصدیق صحت دو طرفه، تمامیت و جلوگیری ازتکرار[2] (با استفاده از دنباله اعداد تصدیق‌شده برای اطمینان از تازه شدن پیام) را در شبکه IP ایجاد می‌نماید. یکی از نتایج IPSec آن است که امنیت را در لایه ۳ (لایه شبکه) و فقط بر اساس IP ایجاد می‌کند. به این طریق سرویس‌های امنیتی را غیر وابسته به روش‌های انتقال لایه زیرین مانند پروتکل‌ها و برنامه‌های

[1] Intrusion Detection System

[2] Anti-Replay

کاربردی قرار می‌دهد. در محیط MPLS VPN، IPSec می‌تواند به نقاط مختلفی اعمال شود که عبارتند از:

۱- CE-CE IPSec

اگر IPSec بین CEها بکار رود، کل مسیر بین آنها حفاظت می‌شود. این روش وقتی پیشنهاد می‌شود که رمزگذاری مورد نیاز باشد یا تهیه کننده سرویس، مورد اعتماد نباشد. در این صورت این روش یک راه حل پیشنهادی برای امن کردن VPNها است. لازم به ذکر است که این روش لزوما از حمله DoS و تهدیدات درون VPN حفاظت نمی‌نماید.

۲- PE-PE IPSec

روش PE-PE IPSec در مقایسه با روش قبلی، از انجام تغییر در تنظیمات IPSec توسط کاربران VPN جلوگیری می‌کند. این روش به آسانی از استراق سمع هسته جلوگیری می‌نماید. البته این روش همه نیازهای امنیتی را نمی‌پوشاند و ارتباط CE-PE در این روش امن نیست. در این مدل تونل IPSec جایگزین LSP در هسته MPLS می‌شود.

۳- IPSec در دسترسی از راه دور

در شبکه‌های امروزی، نیاز برای دسترسی از راه دور به شبکهMPLS از طریق VPN وجود دارد. جهت برقراری امنیت، تونل IPSec می‌تواند از کاربر راه دور به روتر PE مرتبط ایجاد شود. بنابراین روتر PE علاوه بر روتر MPLS، ترمینال دسترسی راه دور هم هست. در واقع در این روش IPSec باعث امن شدن انتقال داده از طریق یک محیط نا امن مانند اینترنت می‌شود.

۷- نتیجه‌گیری

به منظور جداسازی سرویس‌های IP در شبکه صنعت برق، می‌توان از پروتکل MPLS جهت ایجاد VPN استفاده نمود. این پروتکل با توجه به اساس طراحی و ماهیت آن، امن محسوب می‌شود. علاوه بر آن با رعایت موارد امنیتی به‌شرح زیر می‌توان امنیت آن را جهت تامین نیازهای صنعت برق تضمین نمود:

- پیکربندی صحیح تجهیزات شبکه بر اساس استاندارد
- استفاده از لیست کنترل دسترسی (ACL) و فیلتر کردن
- استفاده از پروتکل‌های مسیریابی استاتیک
- استفاده از قابلیت MD-5 برای برقراری امنیت در پروتکل‌های مسیریابی
- استفاده از یک روتر PE برای هر VPN
- استفاده از هسته یکپارچه بر اساس استاندارد برای جلوگیری از جعل IP و برچسب.
- استفاده از جدول VRF و فایروال برای اتصال به اینترنت
- اقدامات لازم برای جلوگیری از حمله DoS
- استفاده از IPSec بر روی MPLS

مراجع:

[۱]. غفاری علی، فاطمه سواران، "شبکه های خصوصی مجازی (VPN)"، هشتمین کنفرانس دانشجویی مهندسی برق،۱۳۸۴

[۲]. Jim Guichard, Ivan Pepelnjak, Jeff Apcar, "MPLS and VPN Architectures, Volume II", June 06, 2003

[۳]. علی رستمی، "مروری بر پروتکل MPLS VPN"، ۱۳۸۳

[۴]. Michael H. Behringer, Monique J. Morrow, "MPLS VPN Security", June 08, 2005,

[۵]. محمد مهدی خدایاری، پیام گوران، "رهیافتی بر امنیت در شبکه‌های VPN مبتنی بر MPLS بر روی بستر IP"، چهارمین همایش ملی دانشجویی انجمن کامپیوتر ایران

[۶]. Cisco Systems, Inc., "Security of the MPLS Architecture", www.cisco.com