بررسی و پیکربندی Access Listها در سیسکو_قسمت اول (نسخه PDF)

در این مقـاله به طور جـامع در خصوص **Access List**هـا، قوانین موجود در تعریف ACLها، انواع Wildcard Maskمی پردازیم. در مقالات بعـدی در خصوص پیکربندی انواع ACLها و سـناریوهای مختلف پیکربندی ACL صـحبت خـواهیم کرد. به طور پیش فرض بعـد از اینکه روترها شـروع به کار می کننـد، تمامی پیامها قادر به عبور از یک اینترفیس به اینترفیس های دیگر خواهند بود. اما شـرایطی پیش خواهد آمد که شـما برای مقاصد مختلف، چه مباحث امنیتی شـبکه و چه سیاسـتهای کلی که در پیش گرفته شده اند، نیاز به اعمال محدودیت در انتقال ترافیک شبکه خواهیم داشت. سیسکو ما را قادر می سازد که در شرایط گفته شده، عبور ترافیک شبکه از یک اینترفیس به اینترفیس هـای دیگر را کنترل کنیم. **ACL**ها یکی از خصوصـیات قدرتمند IOS می باشـند که سیسـکو در کنار IP، پروتکـل هـای دیگری را نیز مانند IPX، Apple Talk، XNS، DECnet برای استفاده از ACL پشتیبانی می کند.

Access List یا همان ACL در حقیقت روشـی برای فیلتر کردن ترافیک خروجی و ورودی بر روی اینترفیس های روتر می باشد، به صورت پیش فرض همه ترافیک قابلیت ورود و خروج از همه اینترفیس های روتر را خواهنـد داشت که شـما با اسـتفاده از توانمنـدی ACLها می توانیـد ورود و خروج ترافیک را براساس قوانین و پروتکل های خاص فیلتر نمائیـد. شـما می توانید به وسـیله ACLها تعیین کنیـد که چه ترافیکی با چه مشـخصاتی از اینترفیس روتر اجازه ورود یا خروج را داشته باشد. از ACLها در دستوراتی مانند NAT و برخی دستورات دیگر اسـتفاده می شود. شما برای استفاده از ACLها بایـد آنها را تعریف نمایید و در مرحله بعد ACLها را به اینترفیسی که قصد کنترل ترافیک آن را خواهید داشت نسبت دهید که همه ترافیک ها با قوانین موجود در ACL بررسی شوند که براساس این قوانین به ترافیک اجازه ورود یا خروج داده می شود.

آشنایی با ACL در سیسکو

علاوه بر اینکه ACLها در فیلتر کردن ترافیک های انتقالی در شـبکه مورد اسـتفاده قرار می گیرند، برای مقاصد مختلف نیز می توان از آنها بهره برد. برای نمونه چند کاربرد عمده آنها عبارتند از:

- محدود کردن دسترسی از طریق VTY TELNET
- فیلتر کردن اطلاعات routing
- اولویت بندی ترافیک مربوط به WAN
- تغییر پارامتر Administrative distance
- برقراری تماس های تلفنی (DDR (Dial-Demand Routing

ACLها در **global configuration mode** ایجـاد شـده و سـپس آنهـا را بایـد فعال نمود. برای کنترل ترافیک انتقالی از راه اینترفیس ها، ACLهـا را بایـد روی اینترفیس موردنظر فعال نماییم. در هنگام فعال نمودن ACLهای ایجاد شـده بایـد نوع ترافیکی را که تحت تاثیر قرار خواهد گرفت را مشخص نماییم. ترافیک عبوری را میتوان در دو گروه عمده قرار داد:

- ترافیک ورودی یا **Inbound**
- ترافیک خروجی یا **Outbound**

در ترافیک ورودی روتر اطلاعات رسیده را ابتدا با ACLهای تعیین شده در روی اینترفیس مربوطه مقایسه کرده و سپس اقدام به ارسال آنها به مقصـد خود می کنـد. اما در ترافیک خروجی یا outbound، روتر اطلاعات رسـیده را ابتـدا به مقاصد خود اراسل کرده و سـپس اقدام به مقایسه آنها با ACL مربوطه می نماید. یکی از محدودیت هایی که اسـتفاده از ACL داراست این است که نمی توان ترافیکی که خود روتر آنها را ایجاد کرده به وسـیله ACLها فیلتر نمود. برای مثال اگر از دسـتورات ping و یا traceroute در روی روتر اسـتفاده کرده و یا اقدام به برقراری ارتباط telnet از روتر خود به سـمت دستگاههای دیگر نماییم، نمی توان این ترافیک ها را به وسیله ACLها فیلترگذاری کرد. اما اگر روتر دیگری اقدام به ping کردن و یا برقراری ارتباط telnet با روتر ما نماید و یا از طریق روتر ما، دستگاه دیگری را هدف قرار دهد، می توان از ACL بهره برد.

قوانین موجود در تعریف ACLها

هر ACL باید با یک شـماره یا یک نام منحصـر بفرد شـناسایی شود.شما قادر خواهید فقط یک ACL را به یک اینترفیس assign کنید.یک ACL بر اساس شـرایط و قوانین خاص ترافیک را فیلتر می کنـد که برخی از این پارامترها که ACL بر اساس آنها می تواند اقدام به بررسی ترافیک نماید، به شرح زیر می باشد:

- براساس Source IP Address یا آدرس فرستنده
- براساس Destination IP Address یا آدرس مقصد یا گیرنده
- براساس شماره پورت خاص
- براساس پروتکل های UDP و TCP
- براساس یکسری از پروتکلهای شبکه مانند IGMP، EIGRP، OSPF، ICMP و ...

همانطور که اشاره شد، یک ACL لیستی از دسـتورات می باشد که با یک شـماره یا نام شـناسایی می شود و این دستورات از بالا به پایین مورد بررسی قرار می گیرند، **پس به این نکته توجه داشته باشید که ترتیب نوشتن دستورات داخل ACL بسیار مهم است** و در پایان هر ACL یک Deny All وجود دارد که این عبارت Deny All را شما مشاهده نمی کنید ولی توسط خود IOS اضافه خواهد شد. پس در صورتی که ترافیک شـما با هیـچ کدام از قوانین داخل ACL مطابقت نداشـته باشد آن ترافیک Deny خواهـد شد. یعنی اجازه عبور از آن اینترفیس را نخواهـد داشت. وقتی ترافیک قصد عبور از اینترفیسـی را که یک ACL به آن نسـبت داده شده است دارد، باید آن ترافیک با دستورات داخل ACL مطـابقت شود و خـط به خط دسـتورات ACL بررسـی می شونـد و در صورتی که، اطلاعـات بـا یکی از خطوط ACL مطابقت داشـته باشد، آن قانون اعمال خواهد شد و خطوط بعد از آن قانون دیگر بررسی نخواهند شد و در صورتی که هیچکدام از قوانین داخل ACL با ترافیک مطابقتی نداشـته باشند، پیام از بین خواهد رفت.از این روست که ترتیب مشخص نمودن قانون های موجود در یک ACL بسیار مهم است.

برای مثال اگر دو قانون برای دسترسـی به یک دسـتگاه، که یکی اجازه عبور را داده و یکی نـداده در جدول موجود باشـند، قانونی را که در اول نوشته شده باشد اجرا شده و از دیگری صرف نظر خواهد شد.برای همین هم در هنگام نوشتن قانون ها موارد اختصاصی تر را باید در اول نوشـته و موارد عمومی تر را در آخر لیست قرار دهیم. برای درک بهتر، مثـالی را مطرح میکنیم.فرض کنیـد که یک ACL دارای دو عدد قانون یا به اصطلاح statement در لیست خود می باشد. به ترتیب زیر:

۱. اجازه دسترسی از شبکه ۱۷۲.۱۶.۰.۰/۱۶
۲. محدودیت دسترسی از دستگاه ۱۷۲.۱۶.۱.۱

بـا یادآوری این نکته که لیست ACL از بالاـ به پـایین پردازش می شود، فرض می کنیم که روتر یـک پیام را با آدرس فرسـتنده ۱۷۲.۱۶.۱.۱ دریـافت کرده است. روتر این آدرس را بـا اولین مورد موجود در لیست مقـایسه می کنـد: آیا پیام رسـیده از طرف شـبکه *۱۷۲.۱۶.۰.۰/۱۶ می باشـد؟ جواب مثبت است و بنابراین اجازه عبور به ترافیک رسـیده داده نخواهـد شـد. اما به دلیل اینکه مورد اول با پیام رسـیده مطابقت داشت، مورد دوم هیـچ وقت پردازش نخواهـد شد. در این مثال همه ترافیک هایی که مربوط به شـبکه ۷۲.۱۶.۰.۰/۱۶* می باشند، اجازه عبور خواهند یافت، حتی آدرس ۱۷۲.۱۶.۱.۱/۱۶.

بیایید که ترتیب نوشتن دو قانون بالا را تغییر دهیم. بدین صورت:

۱. محدودیت دسترسی از دستگاه ۱۷۲.۱۶.۱.۱
۲. اجازه دسترسی از شبکه ۱۷۲.۱۶.۰.۰/۱۶

اگر دستگاه ۱۷۲.۱۶.۱.۱ ترافیکی را به روتر بفرستد، روتر اولین مورد موجود در لیست ACL را با مشخصات پیام مقایسه کرده و از آنجایی که در همان اولین قدم تطابق موردنظر حاصل شد، روتر قانون اول را در مورد پیام رسیده صرفنظر از اینکه چه نوع ترافیکی باشد از بین خواهد رفت.اگر دسـتگاه دیگری مثل ۱۷۲.۱۶.۱.۲ اقـدام به ارسال ترافیک برای روتر نمایـد، روتر مشـخصات پیام را با اولین مورد موجود در لیسـت ACL مقایسه کرده و به دلیل نیافتن مطابقت مورد نظر، مورد دوم پردازش خواهد شد که تطابق وجود داشـته و اجازه دسترسی به ترافیک فوق داده می شود. از همین روست که گفته می شود ترتیب نوشـتن هریک از موارد لیست ACL بسیار مهم بوده و انتقال ترافیک شبکه را تحت تاثیر قرار خواهد داد.در تعریف ACLها به جای استفاده از Subnet Mask از **Wildcard Mask** استفاده می شود که بیان کننده تعداد بیت ها از آدرس می باشد که باید در ACL مورد بررسی قرار بگیرند و به عبارت دیگر مشخص کننده قسمتی از آدرس IP Address می باشد که باید در ACL مورد بررسی قرار بگیرد.Wildcard Mask دقیقا برعکس Subnet Mask می باشد به جای bitهای ۱ در subnet mask ما از بیت

های صفر در wildcard mask و به جای بیت های صـفر در subnet mask از بیت هـای یک در wildcard mask استفاده می کنیم.برای مثال فرض کنید که ماسک ۲۵۵.۲۵۵.۰.۰ را در اختیار داریم. اگر این ماسک را در مبنای ۲ بنویسیم خواهیم داشت:

```
255.255.0.0 = 11111111.11111111.00000000.00000000
```

سرانجام اگر این subnet mask را تبدیل به wildcard mask نماییم، نتیجه به صورت زیر خواهد بود:

```
00000000.00000000.11111111.11111111
```

که در این صورت تبدیل این آدرس به حالت دسیمال یا مبنای ۱۰ آدرس ۰.۰.۲۵۵.۲۵۵ به دست خواهد آمد. در این مثال wildcard mask به روتر می گوید که فقط ۱۶ بیت از اول آدرس IP پیا رسیده باید با ۱۶ بیت از آدرس مشخص شده در هریک از قانون های ACL یکسان باشد تا آن قانون روی پیام رسـیده اجرا گردد. در غیر اینصورت، روتر به بررسـی قانون های بعـدی خواهد پرداخت.دو نوع مخصوص از wildcard mask وجود دارد:

```
0.0.0.0
255.255.255.255
```

ماسک اولی به روتر می گویـد که تمامی ۳۲ بیت آدرس پیام رسـیده باید با آدرس مشخص شده در لیست ACL برابر باشد تا اینکه قانون موردنظر روی آن اجرا شود. برای همین هم اگر wildcard mask برابر با ۰.۰.۰.۰ باشد، به نام host mask نامیده می شود.

یـک مثـال ساده میزنیم: اگر قانون موجود در ACL را به صورت مقابل داشـته باشیم: ۱۹۲.۱۶۸.۱.۱ ۰.۰.۰.۰ بـه این معنی است که روتر دقیقا بدنبال آدرس ۱۹۲.۱۶۸.۱.۱ در بین پیامهای رسـیده می گردد که اگر هیـچ مشابهی پیـدا نشود، روتر موارد بعـدی موجود در لیست ACL را بررسـی می نماید.بعـد از اینکه لیست ACL را به صـورت ۱۹۲.۱۶۸.۱.۱ ۰.۰.۰.۰ تنظیم نمـودیم، روتر به طور اتوماتیـک آن را به حـالت **host** ۱۹۲.۱۶۸.۱.۱ در خواهد آورد.

ماسک دوم (۲۵۵.۲۵۵.۲۵۵.۲۵۵) به روتر می فهمانـد که همه آدرسـهایی که وارد روتر می شوند قابل پذیرش بوده و قانون مزبور روی همه پیام های ورودی اجرا خواهنـد شد. معمولا این نوع را به صورت آدرس IP برابر با ۰.۰.۰.۰ و Wildcard Mask برابر با ۲۵۵.۲۵۵.۲۵۵.۲۵۵ در داخل ACL مشخص می کنیم: ۲۵۵.۲۵۵.۲۵۵.۲۵۵ ۰.۰.۰.۰ که روتر آن را به صورت ۰.۰.۰.۰ any در خواهد آورد. آدرس IP نوشته شده در این فرمول اهمیت چندانی نداشـته و می توان هر آدرسـی را بدلخواه وارد نمود. مثلا میتوان نوشت: ۲۵۵.۲۵۵.۲۵۵.۲۵۵ ۱۹۲.۱۶۸.۱.۱۴۵ که در این حالت نیز روتر صـرف نظر از آدرسـی که مشخص شده است، به علت ماسک داده شده، همه آدرس ها را قبول خواهد کرد. برای اینکه بهتر بتوانید با Wildcard Mask آشـنا شویـد، چند مثال را در این باره مطرح می کنیم. **جدول زیر برخی از آدرس های IP و Wildcard Mask را نشان می دهد.**

Access Listها دو نوع به شرح زیر می باشند:

Standard Access List

Extended Access List

که در مقاله بعدی به شرح این دو ACL می پردازیم.

نویسنده: عاطفه حسین زاده

منبع: جزیره سیسکو وب سایت توسینسو

مطلب اصلی