بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش سوم: امن‌سازی مسیریابی

مسیریابی یکی از مباحث مهم شبکه می‌باشد و حفظ امنیت آن از اهمیت بالایی برخوردار است. مسیریابی در معرض خطرها و حملات گوناگونی است، از تزریق به‌روز رسانی‌های غیر مجاز در جدول مسیریابی گرفته تا حملات DOS که مخصوصاً برای مختل کردن عملیات مسیریابی طراحی شده‌اند. اهداف این حملات می‌توانند روترها، نشست‌های فعال و یا اطلاعات مسیریابی باشند. البته پروتکل‌هایی مانند BGP ، IS-IS ، OSPF ، EIGRP و RIPv2 امکاناتی برای امن‌سازی بستر مسیریابی در اختیار می‌گذارند. در این گزارش به معرفی و نحوه استفاده از این امکانات پرداته شده است.

حملاتی که در مورد روترها بیشتر مرسوم می‌باشند عبارتند از:

- Password cracking
- Privilege escalation
- Buffer overflows
- Social engineering

با اعمال دستوراتی که در این فصل آورده شده‌اند، می‌توان تعدادی از این حملات را کاهش داد و یا حتی از آن‌ها جلوگیری کرد. همچنین بعضی از حملات، نشست‌های بین روترهای همسایه را هدف قرار می‌دهند. در تعدادی از پروتکل‌های مسیریابی، روترهای مجاور هم به عنوان همسایه یکدیگر محسوب می‌شوند. حال اگر حمله‌ای این ارتباط را قطع کند و با یکی از روترها مجدداً ارتباط برقرار نماید، می‌تواند به نتایج ناخوشایندی منجر گردد.

محدود کردن روترها

بسیاری از پروتکل‌های مسیریابی پویا دارای یک مکانیزم خودکار برای شناسایی روترهای همسایه خود می‌باشند. به طور پیش فرض این مکانیزم تمام روترهای مجاور را قابل اعتماد فرض می‌کند در صورتی که می‌تواند این‌گونه نباشد. IOS سیسکو با در اختیار قرار دادن امکاناتی که در زیر آورده شده است، می‌تواند به برقراری ارتباطات فقط با همسایه‌های مجاور و مورد اعتماد منجر شود:

- احراز اصالت همسایه‌ها
- تعیین مسیریابی نظیر

- اینترفیس‌های پسیو پیش‌فرض
- بررسی امنیت TTL در پروتکل BGP
- iACLs
- rACLs
- کنترل سطح سیاست‌ها
- کنترل سطح حفاظت

احراز اصالت همسایه‌ها

احراز اصالت همسایه‌ها در بسیاری از پروتکل‌های مسیریابی وجود دارد و بدین وسیله روتر از معتبر بودن اطلاعات مسیریابی دریافت شده از همسایه خود، اطمینان حاصل می‌کند. روش انجام کار به این صورت است که هر روتر یک کلید رمز برای تعیین اعتبار آپدیت‌های مسیریابی دریافت شده از طرف همسایه خود دارد. قبل از ارسال این آپدیت‌ها، هر روتر باید آن‌ها را با این کلید امضا کند. در روتر مقصد این آپدیت‌ها ابتدا اعتبارسنجی و در صورت معتبر بودن استفاده می‌شوند. احراز اصالت همسایه‌ها در پروتکل‌های BGP ، IS-IS ، OSPF ، RIPv2 و EIGRP وجود دارد.

بسیاری از پروتکل‌های مسیریابی از دو نوع احراز اصالت همسایه‌ها پشتیبانی می‌کنند. این دو نوع شامل احراز اصالت از طریق متن فاش و یا از طریق MD5 می‌باشند. احراز اصالت از طریق متن فاش به این صورت است که هر روتر هنگام ارسال آپدیت‌های مسیریابی یک کلید رمز را به صورت فاش در آن قرار می‌دهد. واضح است که در این حالت به علت فاش بودن کلید، امنیت قابل قبولی فراهم نمی‌شود. در روش دیگر هنگام ارسال آپدیت‌های مسیریابی ابتدا از آن‌ها MD5 hash گرفته می‌شود و پس از آن آپدیت به همراه این hash ارسال می‌شود. روتر دریافت‌کننده اطلاعات، همین روال را طی می‌کند و اگر مقدار هر دو hash با هم برابر بود، آپدیت را قبول می‌کند. این روش از امنیت بیشتری برخوردار است، چون کلید رمز هیچ‌گاه در طول شبکه ارسال نمی‌شود.

احراز اصالت همسایه‌ها باید در همه روترها اعمال شود، مخصوصاً در روترهای مرزی شبکه که پل ارتباطی با اینترنت یا دیگر شبکه‌ها می‌باشند. در بهترین حالت باید برای هر اینترفیس و یا به ازای هر همسایه یک کلید

رمز در نظر گرفته شود. البته ممکن است در شبکه‌های بزرگ این مسئله دردسرآفرین باشد. در نتیجه مدیر شبکه باید تعادل میان امنیت و عملیاتی بودن آن ایجاد کند.

در مثال زیر یک نمونه از پیکربندی احراز اصالت روتر همسایه با استفاده از پروتکل مسیریابی OSPF آورده شده است:

```
OSPF MD5 authentication
interface Ethernet1
ip address 10.139.20.1 255.255.255.0
ip ospf message-digest-key 10 md5 oursharedsecret
router ospf 20
network 10.139.20.0 0.0.0.255 area 0
```

به عنوان مثالی دیگر، در پروتکل EIGRP می‌توان برای هر اینترفیس یا زیر-اینترفیس[1] عملیات احراز اصالت را انجام داد. البته بایستی توجه کردد که هنگامی که احراز اصالت بر حسب EIGRP MD5 بر روی یک اینترفیس فعال شود، این روتر تا وقتی که روتر مجاورش نیز از همین احراز اصالت استفاده نکند، آپدیت‌های مسیریابی از آن روتر را پردازش نمی‌کند:

```
EIGRP authentication
interface Ethernet 1
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 mychain
!
router eigrp 10
network 10.0.0.0
!
key chain mychain
key 1
key-string oursharedsecret
!
```

همین پیکربندی هنگامی که از پروتکل RIPv2 استفاده شده است، در زیر نمایش داده شده است:

```
interface ethernet 0
```

[1] sub-interface

```
ip rip authentication key-chain mychain
ip rip authentication mode md5
!
router rip
network 10.0.0.0
version 2
!
key chain mychain
key 1
key-string oursharedsecret
!
```

در مثال زیر نیز نمونه پیکربندی با استفاده از پروتکل BGP آورده شده است:

```
router bgp 10
no synchronization
bgp log-neighbor-changes
network 64.104.0.0
neighbor 198.133.219.10 remote-as 10
neighbor 198.133.219.10 password 7 05080F1C22431F5B4A
```

تعیین مسیریابی متناظر

مکانیزم شناسایی روترهای همسایه با این پیش فرض عمل می‌کند که تمامی روترهای مجاور قابل اعتماد هستند، درصورتی که در عمل این چنین نیست. این مشکل می‌تواند با غیرفعال کردن این مکانیزم‌ها به‌وسیله ایجاد یک لیست ثابت از روترهای همسایه مجاز، با آدرس IP های شناخته شده صورت بگیرد. در این صورت آپدیت‌های رسیده از روترهایی که آدرس آن‌ها در این لیست نمی‌باشند، drop می‌شوند. با این کار از ورود روترهای غیرمجاز جلوگیری می‌گردد.

هنگامی که احراز اصالت همسایه‌ها عملی می‌شود، انتشار آپدیت‌های مسیریابی درحالت multicast متوقف شده و از این به بعد به صورت unicast توزیع می‌شوند. این تغییر به سخت‌تر شدن شنود و قطع ارتباط بین دو روتر منجر می‌شود. البته به دلیل اینکه همسایه‌های مجاور با استفاده از لیست ثابتی از آدرس IP ها شناخته می‌شوند، همچنان حمله IP address spoofing کارساز می‌باشد. این حمله با اعمال مکانیزم احراز اصالت روترهای همسایه قابل جلوگیری می‌باشد، در نتیجه تا هنگامی که حمله کننده کلید رمز یک روتر را نداشته باشد، نمی‌تواند کاری از پیش ببرد.

همانطور که در مثال زیر نشان داده شده است، برای پروتکل EIGRP می‌توان با استفاده از دستور neighbor ، روتر مجاور را به صورت استاتیک به لیست روترهای مجاز اضافه کرد.

```
router eigrp 100
network 10.0.0.0
neighbor 10.139.20.1 FastEthernet0/0
```

دقت شود که در پروتکل OSPF حتی با تعریف یک لیست استاتیک از روترهای مجاز، باز هم دیگر روترهای مجاور موجود می‌توانند به عنوان همسایه با روتر ارتباط برقرار کنند و این تکنیک برای پروتکل OSPF اثری ندارد.

اینترفیس پسیو پیش فرض

در شبکه‌ها بزرگ ممکن است بعضی روترها دارای اینترفیس‌های زیادی باشند. یک راه حل برای تسهیل پیکربندی روتر، فعال کردن پروتکل مسیریابی مورد نظر بر روی تمام اینترفیس‌های روتر می‌باشد. اگرچه این راه به تسریع پیکربندی کمک می‌کند ولی از نظر امنیتی قابل قبول نیست. برای اینکه پروتکل مسیریابی را بتوان بر روی بعضی اینترفیس‌های روتر غیرفعال کرد، از دستور passive-interface استفاده می‌شود. بدین منظور بهتر است در ابتدا با استفاده از دستور passive-interface default تمامی اینترفیس‌ها را در حالت پسیو قرار داده که در این صورت هیچ پروتکل مسیریابی بر روی آن‌ها فعال نمی‌باشد و پس از آن بر روی هر کدام از اینترفیس‌ها که مورد نیاز باشند، بایستی پروتکل مسیریابی را فعال کرد.

نکته قابل توجه این است که تأثیر دستور passive-interface کاملاً به پروتکل مورد استفاده بستگی دارد. در پروتکل‌های RIP و IGRP اعمال این دستور باعث می‌شود که عملیات ارسال آپدیت‌های مسیریابی بر روی اینترفیس‌های انتخاب شده متوقف شود، اما روتر همچنان می‌تواند روی این اینترفیس‌ها آپدیت دریافت کند. در پروتکل EIGRP و OSPF اعمال این دستور باعث جلوگیری از ایجاد نشست بر روی آن اینترفیس می-شود. این عمل نه تنها باعث توقف ارسال آپدیت‌ها می‌شود بلکه آپدیت‌ها دریافتی را نیز drop می‌کند.

در مثال زیر، ابتدا تمام اینترفیس‌ها در حالت پسیو قرار داده شده‌اند، در حالی که فقط اینترفیس سریال صفر فعال می‌باشد. این بدین معنی است که این روتر تنها از طریق اینترفیس سریال صفرمی‌تواند با یک روتر دیگر ارتباط همسایگی تشکیل دهد.

```
router ospf 100
passive-interface default
no passive-interface Serial0
network 10.139.5.0 0.0.0.255 area 0
network 10.139.20.0 0.0.0.255 area 4
```

در مثال همان سناریو دنبال شده است، با این تفاوت که از پروتکل EIGRP استفاده شده است:

```
router eigrp 10
passive-interface default
no passive-interface Serial0
network 10.0.0.0
```

در مثال زیر، همان سناریو با استفاده از پروتکل RIP تکرار شده است:

```
router rip
passive-interface default
no passive-interface Serial0
network 10.0.0.0
version 2
```

بررسی امنیت TTL برای BGP

بررسی امنیت TTL یک ویژگی امنیتی برای محافظت از زوج روترهای BGP در برابر حمله multi-hop می-باشد. این ویژگی بر اساس مکانیزم امنیتی TTL طراحی شده است و در حال حاضر برای پروتکل BGP قابل استفاده می‌باشد، همچنین کار بر روی آن برای فعال کردن این ویژگی برای پروتکل‌های دیگر مثل EIGRP وOSPF در حال انجام است.

بررسی امنیت TTL به پیکربندی‌هایی که در آن‌ها حداقل مقدار TTL قابل قبول برای بسته در نظر گرفته شده است، اجازه تبادل بین زوج روترهای همسایه BGP را می‌دهد. زمانی که این ویژگی فعال باشد، هر زوج روتر که به عنوان همسایه BGP همدیگر می‌باشند، تمامی اطلاعات خود را با TTL برابر ۲۵۵ بین همدیگر رد و بدل می‌کنند. علاوه بر این، روترها زمانی یک نشست به منظور تشکیل همسایگی بین هم ایجاد می‌کنند که اگر یک روتر این درخواست را بدهد، حتماً باید روتر دیگر در جواب این بسته، یک بسته با مقدار TTL برابر

یا بزرگتر از مقدار TTL بسته اول بازگرداند. تمام بسته‌هایی که مقدار TTL آن‌ها کمتر از یک مقدار از پیش تعین شده باشند، drop می‌شوند.

بررسی امنیتی TTL از حمله DOS مبتنی بر مسیریابی و ارتباط با همسایه‌های غیر مجاز جلوگیری می‌کند. ولی این مکانیزم نمی‌تواند صحت و احراز اصالت بین روترهای همسایه BGP رافراهم کند.

در تجهیزات سیسکو این مکانیزم با استفاده از دستور neighbor ttl-security فعال می‌شود:

```
Router(config)# router bgp as-number
Router(config-router)# neighbor ip-address ttl-security hops hop-count
```

iACLs[2]

iACL ها در واقع ACL های نوع extended هستند که به منظور محافظت از زیرساخت مسیریابی و سوئیچینگ از طریق عبور ترافیک تنها دستگاه‌های مجاز، استفاده می‌شوند. این ACL معمولاً در روترهای مرزی و جایی که ترافیک خارجی به شبکه وارد می‌شود، اعمال می‌شوند.

فیلتر کردن مسیر

فیلترکردن مسیر یکی دیگر از روش‌هایی است که برای امن‌سازی زیرساخت مسیریابی استفاده می‌شود. بیشتر پروتکل‌های مسیریابی از این روش به منظور جلوگیری از تبلیغ یک مسیر در شبکه، پشتیبانی می‌کنند.

فیلترکردن مسیریابی به دو بخش تقسیم می‌شود: فیلترکردن اطلاعات مسیریابی که بین زوج روترهای همسایه تبادل می‌شود و فیلترکردن اطلاعات مسیریابی که بین پروسس‌های مختلف مسیریابی در یک روتر در حال تبادل هستند.

[2] Infrastructure protection access control list

IOS سیسکو برای کنترل اطلاعات مسیریابی منتشر شده در طول شبکه ویژگی‌های زیر را در اختیار می‌گذارد :

- Route Maps
- Prefix List
- Distribute Lists
- Peer Prefix Filtering
- Maximum Prefix Filtering
- EIGRP Stub Routing
- Route Redistribution Filtering

Route Maps

همانند ACL ها، از route map برای دسته‌بندی بسته‌ها، سیاست‌های مسیریابی، ترجمه آدرس‌ها و فیلترکردن مسیرها استفاده می‌شود. این روش نیز همانند ACL ها می‌تواند با تعریف لیستی با قوانین مشخص بر روی ترافیک شبکه محدودیت ایجاد کند. ولی بر خلاف ACL که تنها از دو عمل permit و deny پشتیبانی می‌کند، route map این قابلیت را دارد که بتوان از طریق آن بسیاری از پارامترهای بسته‌ها و یا مسیرها را تغییر داد و دوباره پیکربندی کرد. این روش انعطاف‌پذیری بهتری برای تعیین policy ها در اختیار قرار می‌دهد.

route map شامل چندین ورودی شامل تنظیمات مختلف می‌باشد. هر ورودی route map از یک لیست حاوی عبارات match و set تشکیل شده است. عبارت match زمانی عمل می‌کند که یک مسیر با یکی از این ورودی‌ها منطبق باشد. عبارت set که حاوی دستوراتی به منظور فیلترکردن ترافیک می‌باشد، زمانی عمل می‌کند که شرایط تعریف شده در عبارت match برآورده شوند. همانند ACL ها، ورودی‌های route map نیز تا زمانی که یک تطبیق اتفاق بیافتد، پردازش می‌شوند.

در مثال زیر یک پیکربندی نمونه route map با دو ورودی برای کنترل توزیع مجدد مسیرها از پروتکل OSPF به EIGRP نشان داده شده است.

```
route-map ospf-to-eigrp deny 10
match route-type external type-2
route-map ospf-to-eigrp permit 20
set metric 40000 1000 255 1 1500
!
router eigrp 1
```

```
redistribute ospf 1 route-map ospf-to-eigrp
default-metric 20000 2000 255 1 1500
```

Prefix List

ip prefix-list یک لیست از prefix های مورد استفاده در پروتکل BGP برای کنترل انتشار آپدیت‌های داخلی و خارجی بین زوج روترهای همسایه می‌باشد. مشابه ACL ، هر عبارت در prefix list شامل آدرس‌ها IP و subnet mask معادل آن می‌باشد که به یک دستور permit یا deny وابسته شده‌اند. این آدرس IP ها می-تواند یک آدرس classful ، یا آدرس یک شبکه و یا یک سیستم باشد. مشابه ACL ، ip prefix-list نیز به ترتیب اجرا می‌شود تا یک تطبیق رخ دهد. در این روش می‌توان بر حسب prefix های مختلف، محدودیت-های گوناگونی به منظور کنترل ترافیک شبکه اعمال کرد.

در مثال زیر یک ip prefix-list با نام CuxtomerA برای ترافیک‌های خروجی به سمت یک روتر نشان داده شده است:

```
ip prefix-list CustomerA permit 64.104.0.0/16
ip prefix-list CustomerA deny 0.0.0.0/0 le 32
!
router bgp 10
network 64.104.0.0
neighbor 198.133.219.10 prefix-list CustomerA out
```

در مثال زیر یک prefix list برای اینکه تنها شبکه 64.104.0.0 به همسایه‌های BGP روتر تبلیغ شود، نشان داده شده است:

```
ip prefix-list AllCustomers permit 64.104.0.0/16
ip prefix-list AllCustomers deny 0.0.0.0/0 le 32
!
router bgp 10
distribute-list prefix AllCustomers out
```

Distribute List

در یک روتر هنگامی که پردازش مربوط به مسیریابی در حال انجام است، از distribute-list بدین منظور استفاده می‌شود که کدامیک از مسیرها بر اساس قوانین مشخص شده در یک ACL نوع استاندارد پذیرفته و

یا اطلاع‌رسانی شوند. distribute-list در دو جهت عمل می‌کند: distribute-list-out آپدیت‌های مسیریابی خارجی و distribute-list in آپدیت‌هایی که به روتر می‌رسند را فیلتر می‌کند.

در پروتکل BGP ، distribute-list ها را می‌توان هم به همراه ACL های نوع استاندارد و هم نوع extended و یا prefix-list به‌کار برد. علاوه بر این، در پروتکل BGP می‌توان distribute-list ها را به ازای هر روتر همسایه و با استفاده از دستور neighbor distribute-list تعیین کرد.

در مثال زیر نحوه استفاده از distribute-list در پروتکل EIGRP به منظور کنترل آپدیت‌های رسیده از تمام روترهای همسایه نشان داده شده است:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 10.0.0.0
router eigrp 100
network 10.0.0.0
distribute-list 1 in
```

در مثال زیر نحوه استفاده از distribute-list به منظور کنترل توزیع دوباره مسیرها برای پروتکل OSPF نشان داده شده است:

```
router ospf 100
redistribute rip subnet
distribute-list 11 out rip
access-list 11 permit 10.139.0.0 0.0.255.255
```

Peer Prefix Filtering

Prefix filtering روشی برای جلوگیری از ورود و یا انتشار اطلاعات مسیریابی غیرمعتبر از طریق روترهای همسایه می‌باشد. این روش همچنین می‌تواند به کاهش میزان استفاده از منابع سخت‌افزاری مورد نیاز برای تولید و پردازش آپدیت‌های مسیریابی کمک کند.

Prefix filtering بر روی روترهای مرزی شبکه پیکربندی می‌شود و در حالتی که تنظیمات آن‌ها هم برای دریافت و هم توزیع مسیرها انجام شده باشد، نتیجه بهتری خواهد داشت. در هر دو حالت، انجام عملیات

فیلترکردن ترافیک شبکه می‌تواند بر اساس جلوگیری از آپدیت‌های مسیریابی ناخواسته و یا از طریق مجاز شمردن شبکه‌های مورد نظر صورت گیرد.

IGP Prefix Filtering

در پروتکل‌های مسیریابی درونی شبکه‌ها مثل EIGRP ، IGRP ، RIP و OSPF ، تبادل اطلاعات بین روترهای همسایه می‌تواند از طریق distribute-list ها کنترل شود. distribute-list ها دوجهته می‌باشند، بنابراین برای هر پردازش مسیریابی، باید دو distribute-list تعریف شود، یکی برای آپدیت‌های مسریابی وارد شده و دیگری برای آپدیت‌های مسیریابی توزیع شده. محدودیت‌های مورد نیاز برای مسدود کردن یا مجاز شمردن یک مسیر خاص بر اساس یک ACL نوع استاندارد تعیین می‌شود.

برای فیلتر کردن آپدیت‌های مسیریابی که به روتر وارد می‌شوند از دستور زیر استفاده می‌شود:

```
Router(config-router)# distribute-list [[access-list-number | name] | [route-map map-tag]] in [interface-type | interface-number]
```

که در آن:

- access list number or name

  تعداد نام‌های ACL های استاندارد که تعیین کننده شبکه‌های مجاز برای دریافت اطلاعات می‌باشند.

- Map tag

نام route map که تعیین می‌کندکدام شبکه‌ها می‌توانند در جدول مسیریابی ثبت شوند و کدامیک باید فیلتر شوند. این ویژگی تنها توسط پروتکل OSPF پشتیبانی می‌شود.

- in

اعمال ACL به آپدیت‌های مسیریابی ورودی

- Interface type and number

نوع و شماره اینترفیسی که ACL مورد نظر برای آپدیت‌های مسیریابی ورودی باید روی آن اعمال شوند.

برای یک پردازش مسیریابی نمونه، می‌توان برای هر اینترفیس یک distribute-list برای ترافیک ورودی و برای یک اینترفیس خاص تعیین کرد و یک distributed-list نیز به صورت کلی تعریف شود:

```
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 2 permit 10.122.139.0 0.0.0.255
router rip
distribute-list 2 in ethernet 0
distribute-list 1 in
```

در مثال بالا، روتر ابتدا بررسی می‌کند که از کدام اینترفیس‌ها آپدیت وارد شده است. اگر اینترفیس Ethernet 0 بود، ACL شماره ۲ قبل از قرار دان این آپدیت‌ها در جدول مسیریابی، روی آن اعمال می‌شود. اگر طبق این بررسی، شبکه مورد نظر اجازه اضافه شدن نداشته باشد، بررسی بیشتری بر روی این شبکه صورت نمی‌گیرد. به هر حال، اگر distributed-list 2 به این شبکه اجازه دهد، بعد از آن distributed-list 1 نیز که به صورت کلی تعریف شده است، بررسی می‌شود. اگر هر دو distributed-list به شبکه اجازه دهند و آن را مجاز بدانند، این شبکه در جدول مسیریابی قرار داده می‌شود.

آپدیت‌های مسیریابی خارج شده از روتر با استفاده از دستور distributed-list out می‌توانند فیلتر شوند:

```
distribute-list {access-list-number | access-list-name} out [interface-name | routing-process | as-number]
```

که در آن:

- access list number or name

  این لیست تعیین می‌کند که کدامیک از شبکه‌ها باید در آپدیت‌های مسیریابی ارسال شود.

- Interface name

نوع و شماره اینترفیسی که ACL مورد نظر برای آپدیت‌های مسیریابی خروجی باید روی آن اعمال شوند.

Routing process and autonomous system number

این قسمت تعیین کننده شماره پردازش مسیریابی و شماره AS برای مسیرهایی که مجدداً توزیع شده‌اند، می-باشد.

در مثال زیر، روتر فقط مسیرهایی که مربوط به شبکه 10.122.139.0 می‌باشد را از طریق Ethernet 0 به بیرون ارسال می‌کند و هر آپدیت دیگری در مورد شبکه 10.0.0.0 (شامل 10.122.139.0) را روی بقیه اینترفیس‌ها ارسال می‌کند:

```
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 2 permit 10.122.139.0 0.0.0.255
router rip
distribute-list 2 out ethernet 0
distribute-list 1 out
```

BGP Prefix Filtering

همانند پروتکل‌های مسیریابی داخلی، می‌توان از distribute-list در پروتکل BGP برای فیلترکردن اطلاعات مسیریابی تبادل شده بین زوج روترهای همسایه استفاده کرد. distribute-list ها یک جهته می‌باشند، بنابراین برای یک پردازش مسیریابی خاص دو distribute-list می‌تواند تعیین شود، یکی برای آپدیت‌های مسیریابی ورودی و دیگری برای آپدیت‌های مسیریابی خارج شده از روتر.

بر خلاف پروتکل‌های مسیریابی داخلی، علاوه بر ACL های نوع استاندارد، distribute-list ها در پروتکل BGP از ACL های نوع extended و prefix-list ها هم پشتیبانی می‌کنند.

برای فیلتر کردن آپدیت‌های مسیریابی ورودی از دستور زیر استفاده می‌شود:

```
distribute-list {acl-number | prefix list-name} in
```

که در آن:

- access list number
  لیست آدرس IP هایی که تعیین کننده شبکه‌های مجاز برای دریافت آپدیت‌های مسیریابی می‌باشند.
- Prefix list-name

این لیست تعیین می‌کند که کدامیک از شبکه‌ها، بر حسب prefix هایی که از قبل تعیین شده‌اند مجاز به دریافت آپدیت‌های مسیریابی می‌باشند.

در مثال زیر، یک prefix-list و distribute-list برای پیکربندی عملیات مسیریابی در پروتکل BGP و به منظور دریافت ترافیک فقط از دو شبکه 198.133.219 و 64.104.0.0 نشان داده شده است.

```
ip prefix-list RED deny 0.0.0.0/0 le 32
ip prefix-1ist RED permit 64.104.0.0/16
ip prefix-list RED permit 198.133.219.0/24
router bgp 10
network 64.104.0.0
distribute-list prefix RED in
```

آپدیت‌های مسیریابی خارجی می‌توانند با استفاده از دستور زیر و برای پروتکل‌های مسیریابی خارجی فیلتر شوند.

distribute-list {acl-number | prefix list-name} out [protocol process-number | connected | static]

که در آن:

- access list number

  لیست آدرس IP هایی که تعیین کننده شبکه‌های مجاز برای دریافت آپدیت‌های مسیریابی می‌باشند.

- prefix list-name

این لیست تعیین می‌کند که کدامیک از شبکه‌ها، بر حسب prefix هایی که از قبل تعیین شده‌اند، مجاز به دریافت آپدیت‌های مسیریابی می‌باشند.

- Protocol process-number

این شماره برای عملیات توزیع مجدد مسیرها به کار می‌رود و تعیین کننده نوع پروتکل مسیریابی برای اعمال روی لیست توزیع می‌باشد. پروتکل‌های BGP ، EIGRP ، OSPF و RIP می‌توانند برای اعمال روی این لیست استفاده شوند. این ویژگی در همه پروتکل‌ها به غیر از RIP وجود دارد. شماره پردازش می‌تواند از ۱ تا ۶۵۵۳۵ مقدار بگیرد.

- Connected

  شبکه‌ها و همسایه‌هایی که یک روتر از طریق مسیرهای متصل شده به آن شناسایی کرده است.

- Static

شبکه‌ها و همسایه‌هایی که یک روتر از طریق مسیرهای استاتیک شناسایی کرده است.

در مثال زیر، یک prefix-list و یک distribute-list به منظور پیکربندی مسیریابی در پروتکل BGP و برای اینکه تنها شبکه 192.133.219.0 تبلیغ شود، تعریف شده است:

```
ip prefix-list BLUE deny 0.0.0.0/0 le 32
 ip prefix-list BLUE permit 192.133.219.0/24
router bgp 10
distribute-list prefix BLUE out
```

می‌توان آپدیت‌های مسیریابی در پروتکل BGP را بر اساس روترهای همسایه کنترل کرد. چهار مکانیزم برای انجام این کار در دسترس می‌باشد:

- AS-path filters
- Neighbor distribute-list
- Neighbor prefix-list
- Neighbor route-map

روش اول در این گزارش پوشش داده نمی‌شود. در ادامه به معرفی سه روش دیگر پرداخته خواهد شد:

دستور neighbor-distribute-list این امکان را می‌دهد که برای هر روتر همسایه بتوان آپدیت‌های مسیریابی ورودی و خروجی را کنترل کرد. محدودیت‌های مورد نظر برای فیلتر کردن ترافیک می‌تواند بر اساس ACL نوع استاندارد و یا extended و یا prefix-list تعیین شوند. البته هنگامی که از آدرس IP های classless استفاده می‌شود، ACL نوع استاندارد نمی‌تواند کمک چندانی به منظور فیلترکردن ترافیک شبکه کند. در اینجا هم به دلیل یک جهته بودن distribute-list به ازای هر روتر همسایه، تنها می‌توان از دو distribute-list استفاده کرد. همچنین می‌توان distribute-list ها را به یک روتر همسایه و یا به گروهی از روترها اعمال کرد.

```
neighbor {ip-address | peer-group-name} distribute-list {access-list-number | expanded-list-number | access-list-name| prefix-list-name} {in | out}
```

که در آن:

- ip address

آدرس IP روتر همسایه

- peer-group-name

نام گروه روترهایی که در پروتکل BGP به عنوان همسایه هم شناخته می‌شوند.

- access list number or name

نام ACL های نوع استاندارد و نام و شماره ACL های نوع extended که تعیین‌کننده شبکه‌های مجاز برای دریافت اطلاعات مسیریابی می‌باشند.

- prefix list name

نام یک لیست مربوط به پروتکل BGP می‌باشد.

- in

با این دستور ACL به ترافیک‌های مسیریابی ورودی برای یک همسایه اعمال می‌شود.

- Out

با این دستور ACL به ترافیک‌های مسیریابی خروجی برای یک همسایه اعمال می‌شود.

در مثال زیر یک پیکربندی نمونه مشاهده می‌شود که ACL شماره ۳۹ را به آپدیت‌های مسیریابی ورودی از روتر همسایه 198.133.219.0 اعمال می‌کند. این ACL اجازه می‌دهد که شبکه 64.104.0.0 تبلیغ شود:

```
access-list 39 permit 64.104.0.0 0.0.255.255
 router bgp 10
network 64.104.0.0
neighbor 198.133.219.10 distribute-list 39 in
```

دستور neighbor prefix-list این امکان را می‌دهد که برای هر روتر همسایه بتوان آپدیت‌های مسیریابی ورودی و خروجی را بر حسب طول prefix آن کنترل کرد:

```
neighbor {ip-address | peer-group-name} prefix-list prefix-list-name {in | out}
```

در مثال زیر نمونه‌ای از پیکربندی با استفاده از این دستور نشان داده شده است. در اینجا پیکربندی به گونه-ای است که تنها به آدرس‌های منطبق با prefix مورد نظر یعنی 64.104.0.0./16 اجازه عبور داده می‌شود:

```
router bgp 101
neighbor 198.133.219.6 remote-as 10
neighbor 198.133.219.6 prefix-list customer in
!
ip prefix-list customer permit 64.104.0.0/16
ip prefix-list customer deny 0.0.0.0/0 le 32
```

برای کنترل آپدیت‌های مسیریابی برای هر همسایه از طریق دستور neighbor route-map نیز می‌توان استفاده کرد. route-map را می‌توان در هر دو جهت ترافیک ورودی و خروجی اعمال کرد. یکی برای آپدیت‌های

ورودی به روتر و دیگری برای آپدیت‌های خارج شده از روتر. همچنین می‌توان route-map را به یک روتر همسایه خاص و یا به گروهی از روترها اعمال نمود:

neighbor {ip-address | peer-group-name } route-map map-name {in | out}

که در آن:

- ip address

آدرس IP روتر همسایه

- peer-group-name

نام یک گروه BGP با پروتکل استفاده شده یکسان و یا یک گروه BGP که در آن از چند پروتکل مختلف استفاده شده است.

- map-name

نام یک route-map می‌باشد که تعیین می‌کند کدام شبکه‌ها برای دریافت آپدیت‌های مسیریابی مجاز هستند.

- In

اعمال route-map به مسیرهای ورودی

- Out

اعمال route-map به مسیرهای خروجی

در مثال زیر، دستور route-map localonly فقط به مسیرهایی که به صورت محلی تولید شده‌اند اجازه می‌دهد که به روتر همسایه با آدرس 192.133.219.10 اطلاع داده شود. این کار از ترانزیت ترافیک اینترنت از طریق یک AS جلوگیری می‌کند:

```
ip as-path access-list 10 permit ^$
 route-map localonly permit 10
 match as-path 10
 !
 router bgp 10
network 64.104.0.0
 neighbor 198.133.219.10 remote-as 100
neighbor 198.133.219.10 route-map localonly out
```

Maximum Prefix Filtering

در بعضی از پروتکل‌های مسیریابی می‌توان یک مقدار به عنوان حداکثر تعداد مسیرهایی که از یک روتر همسایه دریافت می‌شود، تعیین کرد. اگر این ویژگی در روتر فعال شده باشد و تعداد مسیرهایی که روتر از همسایه خود دریافت کرده است، به حداکثر تعداد خود رسیده باشد، روتر ارتباط خود با همسایه‌اش را قطع می‌کند، تمام مسیرهایی که از این روتر همسایه دریافت کرده بود را پاک می‌کند و تا یک مدت زمان مشخص به این روتر پاسخ نمی‌دهد. بعد از اتمام این مدت زمان، ارتباط بین آن‌ها همانند قبل شروع می‌شود. پیکربندی این تکنیک در روترها به خصوص روترهای مرزی توصیه می‌شود.

در پروتکل‌های BGP و EIGRP این مقدار با استفاده از دستور neighbor maximum-prefix تعیین می‌شود. پروتکل OSPF دارای یک ویژگی مشابه است که تعداد آپدیت‌های مسیریابی حالت لینک را که توسط دیگر روترها تولید شده است، محدود می‌کند. در OSPF این ویژگی با استفاده از دستور max-lsa پیکربندی می‌شود.

در حالی که اکثر پروتکل‌ها به صورت پیش‌فرض در صورت تجاوز از این محدودیت ارتباط خود را با همسایه‌اش قطع می‌کند، اکیداً توصیه می‌شود که در ابتدا این پیکربندی را به گونه‌ای تغییر داد که در صورت برآورده شدن این شرط، تنها یک هشدار نمایش داده شود. در این حالت ارتباط با روتر همسایه ادامه پیدا می‌کند و فقط یک هشدار نمایش داده شده و گزارش آن ثبت می‌شود.

در مثال زیر و برای پروتکل EIGRP مقدار این محدودیت برابر ۱۰۰۰ و آستانه هشداردهی نیز رسیدن به ۸۰ درصد این مقدار تعیین شده است. زمانی که تعداد مسیرها از حداکثر مقدار مشخص شده تجاوز کند، ارتباط روتر با همسایه‌اش قطع و اقدام‌های گفته شده در بالا انجام می‌شود. مدت زمانی که روتر با همسایه‌اش ارتباط برقرار نمی‌کند، در پروتکل EIGRP به طور پیش‌فرض برابر ۵ دقیقه در نظر گرفته شده است.

```
Router(config)# router eigrp 100
Router(config-router)# neighbor 10.0.0.1 maximum-prefix 1000 80
```

EIGRP Stub Routing

پروتکل EIGRP از پیکربندی روترهای stub پشتیبانی می‌کند. پیکربندی stub به کنترل انتشار اطلاعات مسیریابی کمک می‌کند، همچنین از توزیع اطلاعات غلط و یا دستکاری شده نیز جلوگیری می‌کند. روترهای

stub می‌توانند به منظور انتشار مسیرهایی که به صورت استاتیک، متصل و یا مسیرهای خلاصه تعریف شده-اند، پیکربندی شود.

توجه شود که اگرچه پروتکل OSPF نیز از مکانیزم روترهای stub پشتیبانی می‌کند، ولی پیاده‌سازی آن با همین مکانیزم در پروتکلEIGRP متفاوت است. پیکربندی یک ناحیه[3] از پروتکل OSPF نمی‌تواند از ورود مسیرهای نامعتبری که توسط یک روتر متصل به همان ناحیه وارد شده است، جلوگیری کند.

در زیر مثالی از نحوه پیکربندی مسیریابی stub برای پروتکل EIGRP نشان داده شده است:

```
router eigrp 100
 network 10.0.0.0
 eigrp stub connected static
```

فیلتر کردن مسیرهای دوباره توزیع شده

در شبکه‌هایی که توزیع مجدد مسیرها نیاز می‌باشد، باید مسیرهایی که نیاز به انتشار آن‌ها وجود دارد، به منظور محدود کردن حداکثر تعداد مسیرهایی که از یک ناحیه دیگر منتشر شده است، کنترل شود. مسیرهای غیرمعتبر که ممکن است به صورت سهوی و یا از روی عمد به‌وجود آمده باشد، می‌تواند از طریق توزیع مجدد مسیرها در طول شبکه انتشار یابد و بتواند سیاست‌های امنیتی یک ناحیه را دور بزند.

این مکانیزم با استفاده از دستور redistribute پیکربندی می‌شود. فیلترها می‌تواند با استفاده از یک route-map و یا از طریق distribute list انجام شود. در مثال زیر، این دستور به همراه تعدادی از ویژگی‌های آن مشاهده می‌شود:

```
redistribute protocol [process-id][as-number][route-map map-tag]
```

که در آن:

[3] area

- protocol

پروتکل اولیه مسیرهایی که باید مجدداً توزیع شوند. این پروتکل می‌تواند یکی از موارد زیر باشد:

bgp , connected, eigrp m isisi, mobile, ospf, static , rip

- Process ID

این ویژگی در پروتکل‌های bgp و eigrp ، شماره AS[4] می‌باشد که یک عدد ۱۶ بیتی است.

- AS_number

شماره AS برای مسیری که باید مجدداً منتشر شود.

- Route-map and map-tag:

به منظور اجازه دادن به یک مسیر با پروتکل مسیریابی اولیه و تغییر آن به مسیریابی فعلی، route map باید به طور کامل بررسی شود. اگر این عمل مجاز نبود، تمام مسیرها مجدداً منتشر می‌شوند.

وقتی که از دستور redistribute استفاده می‌شود، route-map به عنوان فیلتر ورودی عمل می‌کند و فقط وارد شدن مسیرها از پروتکل اولیه به پروتکل فعلی را کنترل می‌کند. برای اینکه بتوان توزیع مجدد آپدیت‌های مسیریابی مربوط به مسیرهایی که باید دوباره منتشر شوند را در هر دو جهت کنترل کرد، باید برای هر پردازش مسیریابی یک route-map تعریف نمود و یا اینکه با استفاده از دستور distribure-list out یک فیلتر خروجی برای پروتکل مسیریابی فعلی ایجاد کرد.

مثال زیر نحوه استفاده از دستور route-map به همراه دستور redistribute را نشان می‌دهد. در این مثال، مسیرها بین پروتکل EIGRP و RIP مجدداً توزیع شده‌اند. دستور route map rip-to-eigrp از وارد شدن شبکه 10.0.0.0/8 به EIGRP جلوگیری می‌کند. به همین ترتیب، دستور route map eigrp-to-rip از وارد شدن شبکه 20.0.0.0/8 به RIP جلوگیری می‌کند:

```
route-map rip-to-eigrp deny 10
 match ip address 1
 route-map rip-to-eigrp permit 20
!
 route-map eigrp-to-rip deny 10
```

[4] Autonomous system

```
 match ip address 2
 route-map eigrp-to-rip permit 20
!
 router eigrp 100
 network 10.0.0.0
redistribute rip route-map rip-to-eigrp
                                                                    !
 router rip
 network 20.0.0.0
redistribute eigrp 1
route-map eigrp-to-rip
 !
access-list 1
 permit 10.0.0.0 0.255.255.255
access-list 2
 permit 20.0.0.0 0.255.255.255
```

توزیع مجدد مسیرها می‌تواند با استفاده از دستور distribute list نیز فیلتر شود. آپدیت‌های مسیریابی را می-توان به طور همزمان در هر دو جهت به وسیله دستورهای distribute-list in و distribute-list out در یک پردازش مسیریابی فیلتر کرد. دستور distribute-list in عمل وارد کردن یک مسیر از تمامی منابع موجود به پردازش مسیریابی فعلی را کنترل می‌کند در حالی که دستور distribute-list out عمل خارج شدن یک مسیر از پردازش مسیریابی فعلی را فیلتر می‌کند.

مثال زیر یک سناریوی توزیع مجدد مسیرها را نشان می‌دهد (در حالی که بر خلاف مثال قبل، در این حالت از distribute-list استفاده شده است). در این مثال، پروتکل EIGRP به همراه یک distribute-list برای جلوگیری از توزیع مجدد شبکه 10.0.0.0/8 به RIP پیکربندی شده است. به همین ترتیب، RIP نیز به همراه یک distribute-list برای مانع شدن از تبلیغ شبکه 20.0.0.0/8 به EIGRP پیکربندی شده است:

```
router eigrp 100
 network 10.0.0.0
 redistribute rip distribute-list 10 out rip
 !
 router rip
 network 20.0.0.0
 redistribute eigrp 1 distribute-list 20 out eigrp 1
!
 access-list 10 deny 10.0.0.0 0.255.255.255
```

```
access-list 10 permit 0.0.0.0 255.255.255.255
access-list 20 deny 20.0.0.0 0.255.255.255
access-list 20 permit 0.0.0.0 255.255.255.255
```

یک روش دیگر، محدود کردن تعداد prefix هایی هستند که قرار است درون یک پردازش مسیریابی مجدداً توزیع شوند. در پروتکل OSPF و EIGRP حداکثر تعداد prefix ها را می‌توان با دستور redistribute maximum-prefix تعیین کرد. اگر این تعداد حداکثر تنظیم شده باشد و تعداد مسیرهایی که مجدداً توزیع شده‌اند به این مقدار حداکثر برسد، از این مرحله به بعد دیگر هیچ مسیری مجدداً توزیع نخواهد شد (مگر اینکه روتر به گونه‌ای پیکربندی شده باشد که فقط یک هشدار نمایش داده شود).

در مثال زیر که برای پروتکل OSPF تنظیم شده است، حداکثر تعداد prefix هایی که می‌توانند مجدداً به پروسس OSPF شماره ۱ توزیع شوند، برابر ۱۲۰۰ در نظر گرفته شده است. اگر تعداد این prefix ها به ۸۰ درصد این مقدار برسد، یک هشدار نمایش داده خواهد شد. همچنین اگر تعداد prefix ها به این آستانه برسد، یک هشدار دیگر ثبت خواهد شد و دیگر مسیری مجدداً توزیع نمی‌شود:

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 1200 80
```

گزارش‌گیری

تغییر وضعیت تجهیزات همسایه یکی از مواردی است که می‌توان از آن گزارش گرفت. این گزارش‌ها می‌تواند به حل مشکلات کمک کند. در بسیاری از پروتکل‌های مسیریابی، گزارش‌گیری از تغییر وضعیت به‌طور پیش‌فرض فعال است. زمانی که این ویژگی فعال شده باشد، هر زمان که یک نشست در روتر down ، up ویا reset می‌شود، روتر یک گزارش ثبت می‌کند. اگر syslog فعال شده باشد این گزارش به syslog server ارسال می‌شود، در غیر این صورت در بافر داخلی روتر نگه‌داری می‌شود.

برای اینکه ثبت گزارش را برای پروتکل BGP فعال شود، باید از دستور bgp log-neighbor-changes استفاده کرد. برای پروتکل EIGRP به منظور فعال‌سازی این مکانیزم باید از دستور eigrp log-neighbor-changes و برای پروتکل OSPF از دستور log-adjacency-changes استفاده کرد.

در مثال زیر نحوه پیکربندی این مکانیزم برای پروتکل BGP نشان داده شده است:

```
Router(config)# router bgp 10
Router(config-router)# bgp log-neighbor-changes
```