بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش ششم: الزام رعایت سیاست‌های شبکه

اجرای سیاست‌های شبکه به حصول اطمینان از تطبیق ترافیک ورودی با سیاست‌های شبکه شامل محدوده آدرس IP و نوع ترافیک کمک می‌کند. بسته‌های غیر عادی وارد شده به شبکه باید در همان ابتدای ورود به شبکه دور ریخته شوند.

این بخش مراحل کلیدی برای اجرای سیاست‌های شبکه را نشان می‌دهد، که شامل موارد زیر است:

- فیلترینگ دسترسی مرزی
- محافظت از جعل آدرس IP

سیاست‌های شبکه از دید CSF

نتایج حاصل از اعمال روش CSF برای اجرای سیاست‌های شبکه در جدول ۱ ارائه شده است.

دید کلی:

جدول ۱: اجرای سیاست شبکه-دید کلی

مانیتور
• ورود ○ Syslog ○ SNMP

کنترل کامل:

جدول ۲: اجرای سیاست شبکه-کنترل کامل

اجرا	جداسازی
• فیلترینگ دسترسی لبه ✓ iACLs • محافظت از جعل IP ✓ uRPF ✓ حفاظت از IP مبدا ✓ اجرای DHCP/ARP	• ACL

فیلترینگ دسترسی مرزی

اساس امنیت شبکه در تامین امنیت زیرساخت خود آن شبکه می‌باشد. فیلترینگ دسترسی مرزی جهت اجرای سیاست تشخیص ترافیک مجاز ورودی به شبکه می‌باشد.

در IOS سیسکو، فیلترینگ دسترسی مرزی با استفاده از ACL های نوع extended به منظور کنترل ترافیک ورودی و خروجی انجام می‌شود. به این نوع ACL ها، ACL های حفاظت از زیرساخت (iACLs) می‌گویند.

محافظت از جعل آدرس IP

به منظور حفاظت از جعل آدرس IP ، ترافیک با آدرس IP مبدا نامعتبر دور ریخته می‌شود. بسته‌های با آدرس‌های IP مبدا جعلی یک ریسک امنیتی و بیانگر رخداد یک حمله می‌باشند.

جدول۳: محافظت از جعل IP

اقدامات متقابل ممکن	حملات مرتبط	نوع جعل
• ACLs • uRPf • حفاظت از IP مبدا • تخصیص آدرس IP از طریق DHCP به صورت امن	• ICMP unreachable • ISYN flood • SYN flood • DDoS • جعل آدرس آی‌پی‌های مجـاز و برقراری ارتباط از طریق آن	جعل IP

حفاظت از جعل آدرس IP مزایای کلیدی زیر را فراهم می‌کند:

- بهبود تجزیه و تحلیل داده‌های تله متری شبکه
- افزایش موفقیت ردیابی
- بهبود قابلیت ردیابی منبع رفتار مخرب
- کمک به افزایش کارایی iACLs

روش‌های زیر برای فیلترکردن ترافیک ورودی به شبکه در تجهیزات سیسکو استفاده می‌شود:

لیست‌های کنترل دسترسی (ACL)

ACL ها روش‌های سنتی برای فیلترکردن ترافیک با آدرس جعلی IP می‌باشند، با این حال، ACL پویا نیست و نیازمند پیکربندی دستی تغییرات می‌باشد. به همین دلیل توصیه می‌شود که ACL ها را تنها در یک محدوده به عنوان یک مکمل URPF استفاده کرد.

URPF

URPF یک روش پویا برای فعال کردن فیلترینگ ترافیک ورودی و دور ریختن بسته با آدرس IP مبدا نامعتبر می‌باشد. این روش طبیعت پویا دارد. علاوه بر این، URPF دارای کمترین تاثیر منفی بر عملکرد یک دستگاه می‌باشد و معمولاً به عنوان یک تکنولوژی مرزی جهت داشتن بیشترین تأثیر، به حداقل رساندن محدوده آدرس IP معتبر و مانع شدن از ورود بسته‌های غیر مجاز استفاده می‌شود.

حفاظت از IP مبدأ

این ویژگی در محیط‌هایی که از سوئیچ استفاده می‌شود به منظور جلوگیری از استفاده آدرس MAC جعلی و آدرس IP های مبدا جعلی به کار می‌رود. این ویژگی در سوئیچ‌های لایه ۲ استفاده می‌گردد.

تخصیص آدرس IP از طریق DHCP به صورت امن

این ویژگی، همان قابلیت‌هایی که "حفاظت از IP مبدأ" در لایه ۲ فراهم می‌کند را در لایه ۳ در دسترس قرار می‌دهد. از این ویژگی برای حالتی که از روتر به عنوان DHCP نیز استفاده می‌شود، می‌توان به منظور جلوگیری از ترافیک غیر مجاز با آدرس‌های IP و MAC جعلی بهره برد.

ارسال مسیر واحد برعکس (uRPF)

URPF یک روش پویا برای فعال کردن فیلترینگ ترافیک ورودی و دورریختن بسته‌های با آدرس‌های مبدا غیرمعتبر بر پایه جست‌وجوی مسیر برعکس می‌باشد.

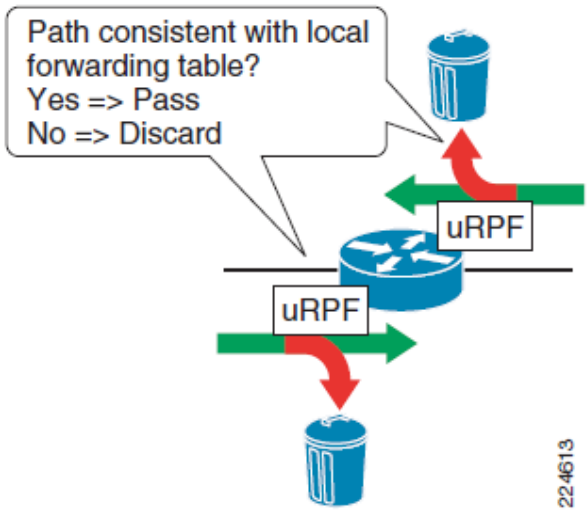
مزایای کلیدی آن:

- حداقل سربار عملیاتی
- مقیاس پذیری، روش اجرای به موقع
- دارای حداقل تاثیر بر روی عملکرد دستگاه

URPF یک جایگزین مناسب برای ACL ها می‌باشد و معمولاً به عنوان یک تکنولوژی مرزی استفاده می‌شود.

تابع کلیدی URPF این موضوع را بررسی می‌کند که آیا مسیر یک بسته ورودی با اطلاعات ارسالی بسته‌ها در تجهیز مطابقت دارد یا خیر؟ این امر با جست‌وجوی یک مسیر برعکس با استفاده از آدرس IP مبدا از یک بسته ورودی به منظور تعیین مسیر فعلی به دست می‌آید. اعتبار این مسیر مشخص می‌کند که uRPF بسته را عبور دهد یا دور بریزد.

اگر مسیر معتبر باشد، بسته عبور خواهد کرد و اگر مسیر معتبر نباشد، بسته دور انداخته می‌شود.



شکل ۱- uRPF

زمانی‌که uRPF بر روی یک اینترفیس فعال گردد، تمام بسته‌های IP در مسیر ورودی آن اینترفیس را بررسی می‌کند.

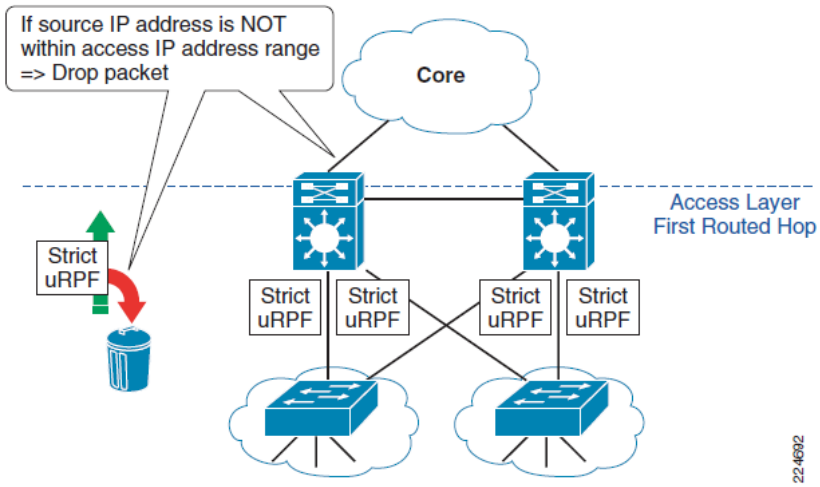
مکان‌های مرزی و اهداف خاص uRPF در هریک از این مکان‌ها، در جدول ۴ نشان داده شده است.

جدول ۴: اهداف و مکان‌های لبه کلیدی uRPF

اهداف خاص uRPF	مکان لبه شبکه
بسته های ورودی بر روی اولین تجهیز مسیریابی در مرز شبکه که آدرس IP مبدا در محدوده آدرس IP شبکه ندارند را دور می ریزد.	اولین لبه لایه دسترسی
بسته های ورودی بر روی اینترفیس داخلی که آدرس IP مبدا در محدوده آدرس IP شبکه داخلی ندارند را دور می ریزد. بسته های ورودی بر روی اینترفیس خارجی که آدرس IP مبدا در محدوده آدرس IP شبکه داخلی ندارند را دور می ریزد.	لبه اینترنت

اولین لبه لایه دسترسی

در این مکان، فیلترینگ ترافیک برای محافظت از جعل آدرس IP مبدا، در لایه ۲ و لایه ۳ شبکه به کار می‌رود.



شکل ۲- اولین لبه لایه دسترسی

اهداف کلیدی عبارتند از:

اولین تجهیز مسیریابی در مرز شبکه، بسته‌های ورودی که آدرس IP مبدا در محدوده آدرس IP شبکه ندارند را دور می ریزد.

رویکرد کلی، فعال کردن uRPF در همه اینترفیس‌های اولین تجهیزات مسیریابی در مرز شبکه است که با دستگاه‌های لایه ۲ در داخل شبکه ارتباط دارند.

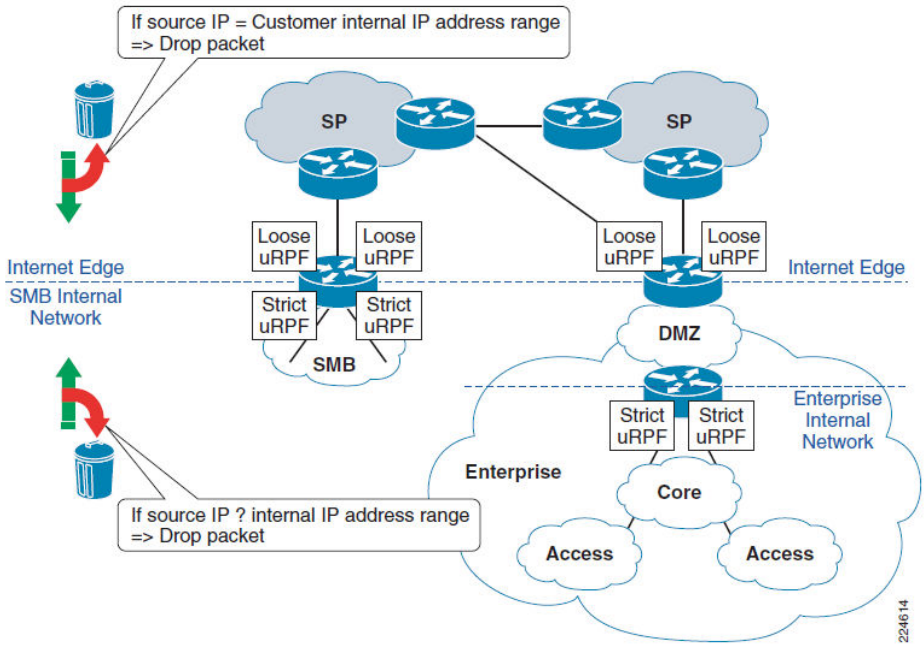
گسترش ملاحظات:

در برخی حالات، اجرای URPF می‌تواند ناممکن باشد و یا نیازمند طراحی بیشتری باشد. سناریوهای رایج، مستلزم ملاحظات بیشتری می‌باشند:

- توپولوژی‌های لایه دسترسی با دستگاه‌های لایه ۲ که برای افزونگی به هم متصلند، امکان ایجاد چندین مسیر به یک IP خاص را به وجود می‌آورند.
- سیستم‌های دوتایی که ارسال ترافیک به هر دو دروازه را ممکن می‌سازند.

لبه اینترنت:

در این مکان، فیلترینگ ترافیک برای محافظت از جعل آدرس IP بر روی SMB یا دستگاه‌های لبه اینترنت به کار می‌رود.



شکل ۳- لبه اینترنت

اهداف کلیدی عبارتند از:

- بسته‌های ورودی بر روی اینترفیس داخلی که آدرس IP مبدا در محدوده آدرس IP شبکه داخلی ندارند را دور می‌ریزد.
- بسته‌های ورودی بر روی اینترفیس خارجی که آدرس IP مبدا در محدوده آدرس IP شبکه داخلی ندارند را دور می‌ریزد.

ملاحظات گسترش

- اعمال URPF در حالت strict mode بر روی اینترفیس داخلی تجهیزات مرزی امکان پذیر است، اگر تمام مسیرها به مقصد یک آدرس داخلی دارای cost یکسان باشد.
- در شبکه‌های با یک ارتباط اینترنت خارجی، ممکن است که بتوان uRPF در حالت strict mode را به کار برد.

- اعمال URPF در حالت strict mode بر روی لبه خارجی اینترنت امکان پذیر نیست.
- حالت آزاد URPF تنها حفاظت از جعل آدرس IP مبدا را فراهم می‌کند.