Tomorrow Starts Here

ارسال پیام خصوصی ()

() () ()

مشاهده پروفایل (http://itpro.ir/profiles/jeffar)

امتیازات این مطلب

۱- jeffar
((http://itpro.ir/profiles/jeffar

۴۶۰ امتیاز

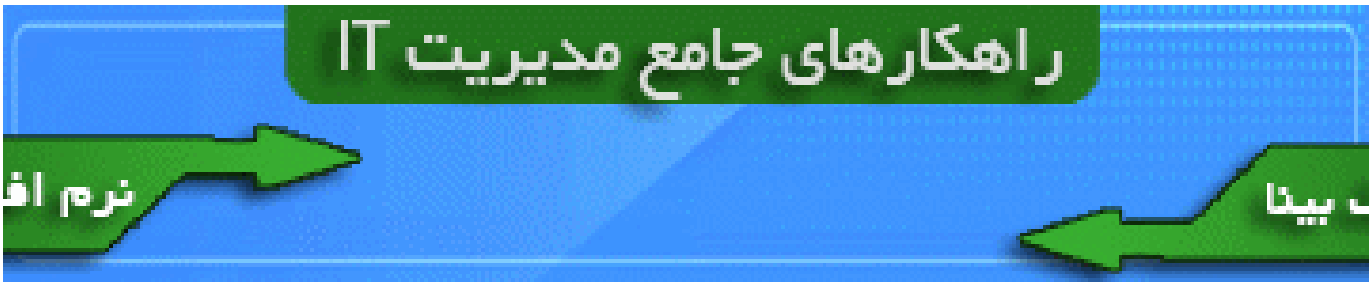
مشاهده پروفایل (http://itpro.ir/profiles/jeffar)

مقاله: Transparent Firewall یا فایروال لایه دو چیست؟ و عملکرد آن چگونه است ! ()

زمان ارسال: ۱۷ ماه قبل جزیره شبکه و زیرساخت ()

پسندها (۱۱ نفر) ۵۵۹ بازدید

-آ آ +آ () () () ()



(/http://www.danapardaz.net/site)

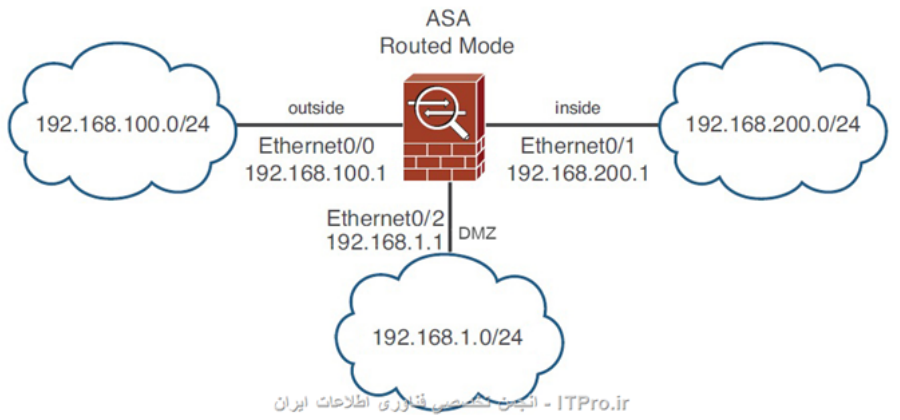
فایروال یک سیستم امنیتی برای شبکه است که به دو صورت سخت افزاری و نرم افزاری موجود است و وظیفه آن کنترل ترافیک ورودی و خروجی براساس سیاست ها و نقش هایی که برای آن تعریف می شود است. فایروال شرکت تحت نام Adaptive Security Applince یا ASA تولید می شود البته ASA علاوه بر فایروال امکانات مانند VPN ، IPS ، AntiVirus ((http://itpro.ir/gotorel/technichaltext/۲۰۴ و ... را برای ما فراهم می کند. ASA در دو Mode یا حالت Transparent و Routed کار می کند.

در این مقاله می خواهیم مفاهیم ، نحوی عملکرد و ویژگی های Transparent Mode را بررسی کنیم اما در ابتدا به صورت مختصر Routed Mode را بررسی می کنیم.

Routed Mode :

به صورت پیش فرض فایروال ASA در لایه سوم عمل می کند و بر پایه Packet و IP Address عمل می کند و کلیه عملیات بازرسی و انتقال ترافیک ، براساس پارامترهای لایه سوم انجام می گیرد هرچند که ASA می تواند در لایه های بالاتر نیز کنترل را انجام دهد. ASA با در نظر گرفتن IP Address برای اینترفیس ها ، خود را به عنوان یک روتر یا Gateway در شبکه ای که به آن متصل است معرفی کند. به این حالت Routed Mode گفته می شود.استفاده از این حالت نیاز به تغییرات در سیستم آدرس دهی IP دارد.

در این حالت هر اینترفیس ASA باید به یک Subnet متصل و یک IP از آن Subnet به آن اینترفیس اختصاص داده شود در تصویر زیر حالت Routed Mode را می بینید که اینترفیس ۰ به نام outside به شبکه ۱۹۲.۱۶۸.۱۰۰.۰۲۴ ، *اینترفیس ۱ به نام inside به شبکه* ۱۹۲.۱۶۸.۲۰۰.۰۲۴ و اینترفیس ۲ به نام DMZ به شبکه ۱۹۲.۱۶۸.۱.۱/۲۴ متصل است.



Transparent Mode :

حالت دیگری که ASA می تواند در آن عمل کند Transparent است. در این حالت ASA همانند یک دستگاه لایه دو فعالیت می کند و مانند یک روتر یا Gateway در شبکه دیده نمی شود این حالت استفاده فایروال را قایروال لایه دو یا فایروال مخفی نیز می نامند. چون در این حالت اینترفیس های فایروال IP نمی گیرند در نتیجه قابل شناسایی نیستند و تنها از یک IP آدرس برای ترافیک Management مربوط به خود دستگاه استفاده می شود.

نصب و راه اندازی فایروال در حالت Transparent در شبکه به سادگی انجام می پذیرد و شبکه ما را به دو قسمت inside و outside تقسیم می کند بودن اینکه نیاز به تغییر در سیستم آدرس دهی شبکه وجود داشته باشد در شکل زیر نحوی استقرار فایروال در حالت Transparent را نشان می دهد.

در حالت Transparent هر دو اینترفیس inside و outside به یک subnet متصل می شود. به این حالت bump in the wire گفته می شود چون در این حالت ASA شبکه را جدا نمی کند و بخشی از شبکه می شود و ترافیک شبکه مورد بازرسی قرار می دهد و نسبت به سیاست های و نقش های در نظر گرفته شده برای فایروال ، در مورد ترافیک های عبوری تصمیم می گیرد. به این همین دلیل نصب و راه اندازی Transparent mode ساده و آسان است.

با اینکه حالت Transparent در لایه دو عمل می کند ترافیک لایه سه تا زمانی که شما به آن اجازه عبور ندهید (با یک ACL) این ترافیک نمی تواند عبور کند. و تنها ترافیکی که بدون ACL اجازه عبور دارد ترافیک مربوط به ARP است. ترافیک ARP را با ARP Inspection می توان کنترل کرد.

- نکته : در حالت Transparent ترافیک CDP اجازه عبور ندارد.

به طور مثال شما می توانید با استفاده از یک ACL ترافیک (http://itpro.ir/gotorel/technichaltext/۳۱۰۲۴) Routing Protocol هایی مانند EIGRP ، (http://itpro.ir/gotorel/technichaltext/۱۴۶۱۶) OSPF (http://itpro.ir/gotorel/technichaltext/۱۷۸۸۵)) و ... را از Transparent Firewall عبور دهید

ASA در حالت transparent را می توان همانند یک سوئیچ در نظر گرفت که فریم ها را از یک اینترفیس به اینترفیس دیگر منتقل می کند اینکار براساس MAC آدرس فریم انجام می شود. ASA آدرس MAC مبدا و پورتی که روی آن این فریم را دریافت کرده را نگه داری می کند و از این طریق متوجه می شود که برای رسیدن به این MAC آدرس از چه اینترفیس می تواند استفاده کند. با استفاده از این اطلاعات ASA یک جدول تشکیل می دهد و این اطلاعات را در آن نگه داری می کند و با استفاده از این جدول اقدام به ارسال فریم های می کند.

زمانی که یک فریم که MAC مقصد را در جدول خود ندارد چه واکنشی نشان می دهد؟

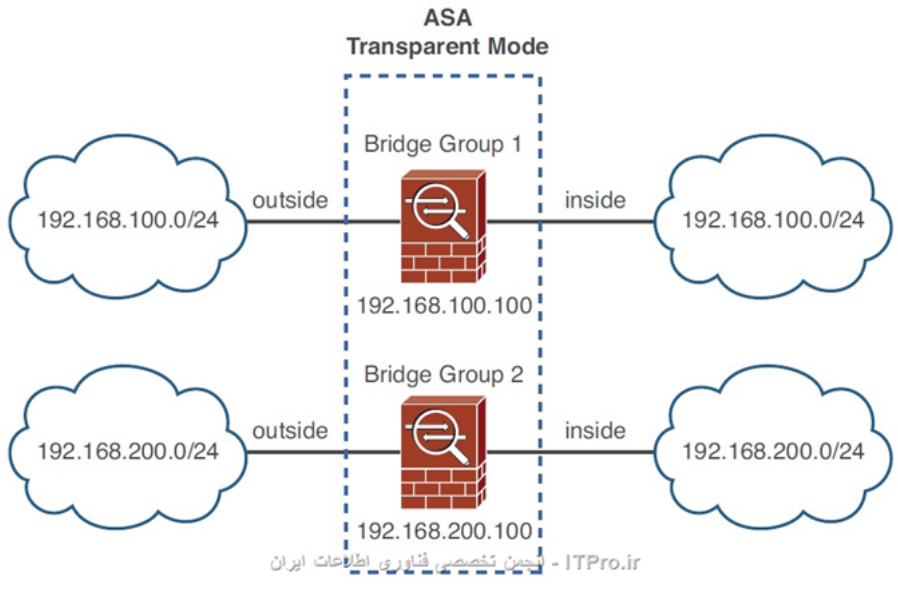
سوئیچ زمانی که MAC مقصد فریم را در جدول Cam خود پیدا نکند این فریم را روی تمام اینترفیس هایش غیر از اینترفیسی که این فریم را روی آن دریافت کرده ارسال می کند به این امید که مقصد به یکی از پورت هایش متصل باشد.

اما ASA همانند سوئیچ اینکار را به سادگی انجام نمی دهد چون به دلیل سیاست های امنیتی امکان ارسال بسته ها محدود شده است. در عوض ASA به منظور پیدا کردن مقصد به یکی از روش های زیر وارد عمل می شود:

- ARP request : زمانی که آدرس IP مقصد در شبکه Local (همان subnet) قرار دارد در نتیجه به ASA از طریق یک شبکه متصل است و ASA اقدام به ارسال یک ARP request می کند و در صورتی که مقصد به آن پاسخ دهد از روی این پاسخ محل استقرار مقصد را متوجه می شود.
- Ping request : زمانی که آدرس IP مقصد در یک شبکه دیگر قرار دارد ASA اقدام به ارسال echo request به مقصد مورد نظر می کند. زمانی که پاسخ توسط روتر یا مقصد پاسخ داده شد. ASA از روی پاسخ دریافتی می فهمد MAC بعدی (next-hop) که از طریق آن به مقصد می رسد چیست و چگونه می تواند به آن برسد.

ASA که نسخه ۸.۴(۱) یا بالاتر را اجرا کند این امکان را دارد که اینترفیس های خود را عضو یک یا چند گروه (bridge group) منطقی کند. هر bridge group به عنوان یک Transparent firewall کاملا مستقل عمل کند. ترافیکی که از یک bridge group عبور می کند نمی تواند وارد bridge group دیگر شود در صورت نیاز به ایجاد ارتباط بین این گروه ها باید از یک روتر خارجی استفاده شود. در

فایروال های ASA تا هشت bridge group می توان ایجاد کرد که به هر گروه می توان ۲ تا ۴ اینترفیس داشته باشد. حداقل هر گروه باید دو اینترفیس داشته باشد که معمولا به نام های inside و outside شناخته می شوند. تصویر زیر نشان دهنده دو bridge group است که به صورت کاملا مجزا از یکدیگر عمل می کنند.



با استفاده از این قابلیت این امکان فراهم می شود که چندین فایروال مستقل داشته باشیم.

نسخه های قبل ۸.۴(۱) تنها از یک bridge group پشتیبانی می کنند و از دو اینترفیس برای آنها می توان استفاده کرد که می توان نام های inside و outside را برای آنها در نظر گرفت و اجازه استفاده از اینترفیس سوم را نخواهیم داشت مگر به عنوان پورت Management از آن استفاده کنیم که تنها ترافیک مربوط به خود دستگاه از آن عبور داده شود.

زمانی که ASA چند Security Context دارد برای هر Context می تواند یک یا چند bridge group داشته باشیم. به هر Context می توان اینترفیسی را اختصاص داد که مربوط به Contextهای دیگر نباشد به عبارت دیگر اینترفیس ها نمی توانند بین Context ها مشترک باشند.

اینترفیس های فایروال در حالت Transparent باید همه به یک شبکه (subnet) متصل باشند هر چند که بسته های IP بودن محدودیت های لایه دو همچنان بازرسی می شوند. از یک Extended ACL برای بررسی و ارزیابی Policiesهای ، ترافیک استفاده می شود و موتور بازرسی و بررسی ASA می تواند فعالیت های ترافیک را در هر لایه ای مورد بررسی قرار دهد.

- نکته : از نسخه (۲)۸.۰ می توان از NAT در transparent firewall استفاده کرد.
- نکته : فایروال در حالت Routed عمل بازرسی و انتقال ترافیک را فقط براساس بسته های IP انجام می دهد اما در حالت transparent این محدود وجود ندارد چون در لایه دوم عمل می کند و می تواند ترافیک های غیر IP را نیز مدیریت کند. ترافیک های غیر IP را می توان به وسیله یک ACL کنترل کرد.

انتخاب Firewall Mode :

قبل از اینکه یکی از دو حالت Routed یا Transparent را برای شبکه خود انتخاب کنیم باید از نقاط ضعف و قوت این دو حالت آگاهی داشته باشیم. در اینجا به صورت خلاصه این ویژگی ها را نام می بریم:

Transparent Firewall Mode :

- زمانی استفاده می شود که بخواهیم ترافیک غیر IP را از آن عبور دهیم.
- نیاز به تغییرات در سیستم آدرس دهی در شبکه ندارد.
- به ازای هر bridge group می توان از ۲ تا ۴ اینترفیس استفاده کرد.
- از همه ویژگی ها و امکانات ASA نمی توان استفاده کرد مانند QoS ، Dynamic Routing و ...

Routed Firewall Mode :

- زمانی استفاده می شود که فقط بسته های IP را بخواهیم بازرسی کنیم.
- تغییرات در سیستم آدرس دهی شبکه مورد نیاز است.
- همه اینترفیس ها قابل استفاده هستند.
- از تمام امکانات ASA می توان استفاده کرد.

مواردی که در هنگام پیاده سازی حالت Transparent باید در نظر گرفته شود:

- در نظر گرفتن یک IP برای مدیریت فایروال (در صورتی که از چند Context استفاده می شود برای هر Context یک IP در نظر گرفته شود(. بر خلاف حالت Routed که برای هر اینترفیس آن یک IP در نظر گرفته می شود در حالت Transparent فقط یک IP برای خود دستگاه در نظر گرفته می شود و از آن برای ارسال و دریافت ترافیک که مربوط به خود دستگاه است استفاده می شود مانند ترافیک های ۳۱۰۵۳ (http://itpro.ir/gotorel/technichaltext/) AAA) یا Syslog و ... از این قبیل می باشد. IP در نظر گرفته شده باید در همان Subnet باشد که فایروال به آن متصل است.
- در حالت Transparent تنها از دو اینترفیس آن استفاده می شود که تحت نام inside و outside در نظر گرفته می شود. همچنین امکان استفاده از اینترفیس management وجود دارد ولی باقی اینترفیس ها را نمی توان استفاده کرد.
- IP Management دستگاه را به عنوان Default Gateway دستگاه های شبکه در نظر نگیرید. روش صحیح این است که Default Gateway در سمت دیگر فایروال قرار گیرد تا ترافیک دستگاه های شبکه از آن رد شود.
- در صورت داشتن چند Context برای هر Context باید اینترفیس های مجزا در نظر گرفت و نمی توان یک اینترفیس را برای چند Context استفاده کرد.