فیلم‌نگار آموزش عملی

CCNP Security (300-206)

آموزش گام به گام از روی فیلم‌های آموزشی Keith Barker

شرکت CBT Nuggets

تألیف: مهندس مهران تاجبخش

انتشارات پندار پارس

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

www.pendarepars.com **info@pendarepars.com**

نام کتاب	:	**فیلم‌نگار آموزش عملی CCNP Security (300-206)**
ناشر	:	**انتشارات پندار پارس**
تألیف	:	**مهران تاجبخش**
چاپ نخست	:	**بهمن ماه ۹۵**
شمارگان	:	**۵۰۰ نسخه**
طرح جلد	:	**رامین شکرالهی**
چاپ، صحافی	:	**روز**
قیمت	:	**۳۳۰۰۰ تومان به همراه DVD**

شابک : ۹۷۸-۶۰۰-۸۲۰۱-۲۷-٤

فهرست

پیش گفتار

در طی سالیان گذشته تا به امروز همواره محصولات شرکت سیسکو در زمینه تجهیزات ساختاری شبکه (Routers / Switches) در صدر فروش قرار داشته و همواره بالاترین سهم بازار را به خود اختصاص داده‌اند.

کیفیت و قابلیت‌های موجود در تجهیزات سخت‌افزاری و نرم‌افزارهای مورد استفاده در این تجهیزات باعث شده است که از بالاترین سطح کارآیی، اطمینان‌پذیری و کیفیت برخوردار باشند. آن‌چنانکه طبق آخرین گزارش منتشر شده توسط مؤسسه معتبر تحقیقاتی گارتنر در شش حوزه مورد بررسی فناوری‌های شبکه، محصولات و خدمات شرکت سیسکو توانسته‌اند رتبه نخست را در سال ۲۰۱۶ به خود اختصاص دهند. این موارد عبارتند از :

- Unified Communications
- Corporate Telephony
- Video Conferencing
- Web Conferencing
- Customer Care
- Communications for Midsize Enterprises

امروزه در اغلب شبکه‌های حساس و مهم از لحاظ کیفیت و کارآیی و همچنین امنیت و اطمینان‌پذیری استفاده از تجهیزات و فناوری‌های ارائه شده در حوزه شبکه، شرکت سیسکو در اولویت انتخاب قرار دارند. بدون تردید بخشی از این کارآیی و قابلیت‌ها به فناوری‌های سخت‌افزاری و نرم‌افزاری در حوزه امنیت مربوط می‌باشند.

با توجه به اهمیت این موضوع، شرکت سیسکو به موازات توسعه فناوری‌های جدید در زمینه‌های سخت‌افزاری و نرم‌افزاری شبکه، اقدام به تدوین و ارائه دوره‌های آموزشی تخصصی امینت در شبکه در سه حوزه‌ی ساختار و تجهیزات و نقاط استفاده (CCNA Security) و ارتباط بین شبکه‌ای و شبکه‌های خصوصی مجازی و امنیت سیستم‌های همراه و مدیریت و برخورد با تهدیدها (CCNP Security) و سرانجام، امنیت در معماری و ساختار شبکه متوسط و بزرگ (CCIE Security) نموده است.

با توجه به اهمیتی که موضوع پیاده‌سازی امنیت در ساختارهای مختلف شبکه، به‌ویژه شبکه‌های بی‌سیم و همراه و همچنین ارتباط از راه دور و ارتباط بین شبکه‌ها و کنترل و مقابله با تهدیدها دارد، شرکت سیسکو دوره‌های بین‌المللی خود را که در یک گروه با عنوان CCNP Security ارائه می‌داد، در اواخر سال ۲۰۱۴ با توجه به گسترش فناوری‌ها و نیازهای روز افزون به آشنایی تخصصی‌تر و جزئی‌تر در موضوعات ذکر شده بالا، اقدام به به‌روز رسانی دوره‌های بین‌المللی خود در این حوزه کرد و هم اینک دوره بین‌المللی CCNP Security از چهار بخش به شرح زیر تشکیل شده است:

- 300-208 SISAS – Implementing Cisco Secure Access Solutions

(فناوری سیسکو برای دسترسی امن)

- 300-206 SENSS – Implementin Cisco Edge Netwrok Security Solutions

(فناوری های سیسکو برای ایجاد ارتباط امن بین شبکه با ایمن‌سازی تجهیزات مورد استفاده در این بخش، از جمله سوئیچ‌ها، مسیریاب‌ها، فایروال‌ها و ...)

- 300-209 SIMOS – Implementing Cisco Secure Mobility Solutions

(فناوری‌های سیسکو برای ایمن‌سازی شبکه‌های همراه و ارتباط‌های بی‌سیم)

- 300-210 SITCS – Implementing Cisco Threat Control Solutions

(فناوری‌های سیسکو برای کنترل و مقابله با تهدیدها، اعم از بدافزارها، ساختاری و منطقی و کاربران)

این کتاب مربوط به دوره آموزشی (SENSS) 300-206 شرکت سیسکو است که بر اساس فیلم‌های آموزشی ارائه شده توسط آقای کیت بارکر از شرکت CBT Nuggets تألیف و تدوین شده است. گفتنی است که این کتاب پس از (CCNA Security (IINS 210-260، دومین تجربه تألیف محتوای آموزشی به صورت فیلم نگار است.

با توجه به اینکه این نوع ارائه محتوای آموزشی در قالب کتاب برای نخستین بار انجام شده است، قطعا جا دارد تا در مجموعه‌های آینده بهبود یافته و نقاط ضعف آن تا حد امکان برطرف شود.

این کتاب در یک فاصله زمانی حدود یک ماه از کتاب نخست در این مجموعه (CCNA Security) ارائه می‌شود، میزان استقبال و همچنین نظرات ارسال شده در این فاصله زمانی کوتاه، من را بر آن داشت تا برای ارائه مجموعه‌هایی از این دست (فیلم نگار)، در موضوعات تخصصی دیگر همچون مجازی‌سازی Vmware و همچنین پیاده‌سازی و ایمن‌سازی فضاهای پردازش ابری و مراکز داده، برنامه‌ریزی‌های لازم را انجام دهم که امیدوارم در آینده نزدیک، اخبار مربوط به آنها را به آگاهی‌تان برسانم.

در نگارش این کتاب از ۲۹ فیلم آموزشی به مدت زمان بیش از ۱۶ ساعت استفاده شده است. برای استفاده بهینه‌تر و کارآمدتر از کتاب، آن را به همراه یک لوح فشرده حاوی تصاویر موجود در کتاب با کیفیت خوب و فیلم‌های آموزشی اصلی به تفکیک فصل‌های کتاب عرضه کرده‌ایم.

با آزمون بین المللی (300-206 SENSS) CCNP Security بیشتر آشنا شویم

سرفصل و محتوای آموزشی و همچنین شرایط و قالب برگزاری آزمون بین‌المللی آن توسط شرکت سیسکو اعلام می‌گردد. این دوره آموزشی از دسامبر سال ۲۰۱۴ با کد جدید (CCNP Security – 300-206 SENSS) ارائه شد. آزمون بین‌المللی این دوره آموزشی از ۶۵ تا ۷۵ سؤال تشکیل شده است که مدت پاسخگویی به سوالات نیز ۹۰ دقیقه است. این آزمون در سطح بین‌المللی توسط موسسه Pearson VUE برگزار می‌شود.

محتوای موضوعی آزمون بین المللی IINS 210-260 (CCNA Security)

- مقابله با تهدید: ۲۵ درصد
- ابزارهای مدیریت سیسکو در خط فرمان و رابط کاربری گرافیکی: ۲۵ درصد
- مدیریت سرویس‌ها در تجهیزات سیسکو: ۱۲ درصد

- ابزارهای کنترل و نظارت و اشکال‌یابی و تهیه گزارش : ۱۰ درصد
- معماری‌های مقابله با تهدید: ۱۶ درصد
- اجزا و نکات مربوط به امنیت: ۱۲ درصد

چه مطالبی را در این کتاب خواهید آموخت

موضوعات ارائه شده در این کتاب بر محور امن‌سازی تجهیزات ارتباطی بین شبکه‌ها و دسترسی امن آنها با یکدیگر متمرکز شده است. در بخش نخست این کتاب با معماری و عملکرد انتقال ترافیک در لایه دوم و سوم شبکه و تهدیدهای موجود، و نیز روش‌های شناسایی و مقابله با آنها آشنا خواهید شد و در ادامه با ابزارهای مدیریتی در خط فرمان و همچنین دارای رابط کاربری گرافیکی برای کنترل و نظارت و همچنین پیکربندی امنیت تجهیزات سیسکو آشنا می‌شوید و در بخش دیگری از این کتاب با سرویس‌های رمزنگار و کنترل و تأیید هویت در تجهیزات سیسکو برای برقراری ارتباط راه دور امن به منظور مدیریت و راهبری آنها آشنا خواهید شد و در ادامه با ابزارهایی که برای نظارت و کنترل و شناسایی اشکال‌ها و تهیه گزارش از عملکردهای تجهیزات ارتباطی در شبکه وجود دارند، آشنا می‌شوید و سرانجام با ساختارهای مقابله با تهدید همچون ایجاد لایه میانی و استفاده از فایروال‌های پشتیبان و مقابله با خرابی و فایروال‌های نامرئی و ... آشنا می‌شوید.

این کتاب برای چه کسانی است

موضوعات مورد بحث در این کتاب، به طور مشخص به ایمن‌سازی لایه‌های ارتباطی بین شبکه‌ای و تجهیزات مورد استفاده در آن می‌پردازد. بنابراین راهبران شبکه سازمان‌ها و مراکز داده می‌توانند از مطالب و فناوری‌هایی که در این فیلم نگار به آنها پرداخته شده است به منظور پیکربندی و مدیریت تجهیزات ارتباطی شبکه‌های مورد استفاده خود همچون سوئیچ‌ها و مسیریاب‌ها و فایروال‌ها و همچنین سرورهای پروکسی و ابزارهای تشخیص و جلوگیری از نفوذ غیرمجاز (IDS/IPS) استفاده کنند.

در باره نویسنده

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت داشته و دارای مدارک بین‌المللی فراوانی در حوزه شبکه، امنیت شبکه و تست نفوذ است که عبارتند از:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW security Professional, ISO27001 Lead Auditor.

برای برقراری ارتباط با نویسنده می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

تقدیم به مادرم

به خاطر زحمات به دریغش

و پسرم

که مایه امید و انرژی من است

فصل ۱

مقابله با تهدیدها – ۲۵%

درس ۱: کنترل لایه داده IPv4 با استفاده از فهرست کنترل دسترسی

نام فیلم: Controlling the IPv4 Data-plane with ACL (۲۲:۲۵)

در این درس با چگونگی استفاده از فهرست‌های کنترل دسترسی بر اساس آدرس‌های IPv4 برای کنترل جریان داده‌ها در مسیریاب‌ها آشنا خواهیم شد. با استفاده از این فناوری (همانند یک فیلتر عمل می‌کند) می‌توانیم ترافیک ورودی و خروجی مسیریاب را کنترل کنیم و به این ترتیب امنیت مسیریاب را ارتقا دهیم.

در فهرست کنترل دسترسی، دستورالعمل‌هایی برای مسیریاب در نظر گرفته می‌شود که بر اساس آن مسیریاب تصمیم می‌گیرد که به ترافیک اجازه عبور بدهد و یا اینکه آنرا در مسیریاب مسدود کند.

فهرست‌های کنترل دسترسی می‌توانند به تعداد و با اسامی دلخواه در مسیریاب‌ها تعریف شوند. سپس بر حسب نیاز می‌توانیم فهرست دسترسی فعال را انتخاب کنیم.

چنانچه فهرست کنترل دسترسی را تعریف نکرده باشیم و یا اینکه به فهرست دسترسی مشخصی اشاره نکرده باشیم، برای مسیریاب همانند این است که فهرست کنترل دسترسی وجود ندارد، بنابراین به همه ترافیک امکان عبور می‌دهد.

در مواردی که فهرست دسترسی تعریف شده است و همچنین آنرا نیز انتخاب کرده باشیم، آنگاه مسیریاب بر اساس مندرجات فهرست با اولویت از بالا به پایین نسبت به عبور ترافیک تصمیم‌گیری می‌نماید.

اگر مسیریاب تا پایان فهرست را بررسی کرد و در مورد ترافیک موردنظر، تعریفی در فهرست مشاهده نکرد، آنگاه مسیریاب ترافیک موردنظر را مسدود می‌نماید.

نکته: اگر فهرست وجود نداشته باشد، ترافیک مسدود نمی‌شود. چنانچه فهرست وجود داشته باشد ولی در مورد ترافیک موردنظر در آن تعریفی انجام نشده باشد، آنگاه مسدود خواهد شد.

نکته: اشتباه رایجی که اغلب مرتکب می‌شوند این‌است که فراموش می‌کنند در پایان فهرست، مجوز موردنیاز برای ترافیک‌هایی که اجازه عبور دارند را تعریف کنند. به همین دلیل مسیریاب از عبور ترافیک‌های مجاز جلوگیری می‌کند و در خیلی از موارد مشاهده می‌کنیم که در بخش‌هایی از شبکه بدون اینکه انتظار داشته باشیم از عبور ترافیک موردنیاز جلوگیری شده است.

فهرست‌های کنترل دسترسی دو نوع است. نوع نخست فهرست کنترل دسترسی استاندارد نام دارد و برای تعیین آیین‌نامه‌های کنترل ترافیک در لایه سوم استفاده می‌شود. نوع دوم فهرست کنترل دسترسی توسعه یافته (Extended ACL) است که برای تعریف آیین‌نامه کنترل دسترسی لایه سوم و چهارم از آن استفاده می‌شود (L3/L4 ACL).

همان‌گونه که در شکل زیر مشاهده می‌کنید، نامگذاری فهرست کنترل دسترسی با اعداد انجام می‌شود. اگر بخواهیم فهرستی به عنوان فهرست دسترسی استاندارد و یا توسعه یافته در نظر گرفته شود، باید از محدوده‌های عددی مشخصی برای آنها استفاده کنیم.

```
R1(config)#access-list ?
  <1-99>             IP standard access list
  <100-199>          IP extended access list
  <1000-1099>        IPX SAP access list
  <1100-1199>        Extended 48-bit MAC address access list
  <1200-1299>        IPX summary address access list
  <1300-1999>        IP standard access list (expanded range)
  <200-299>          Protocol type-code access list
  <2000-2699>        IP extended access list (expanded range)
  <2700-2799>        MPLS access list
  <300-399>          DECnet access list
  <600-699>          Appletalk access list
  <700-799>          48-bit MAC address access list
  <800-899>          IPX standard access list
  <900-999>          IPX extended access list
  compiled           Enable IP access-list compilation
  dynamic-extended   Extend the dynamic ACL absolute timer
  rate-limit         Simple rate-limit specific access list
R1(config)#
```

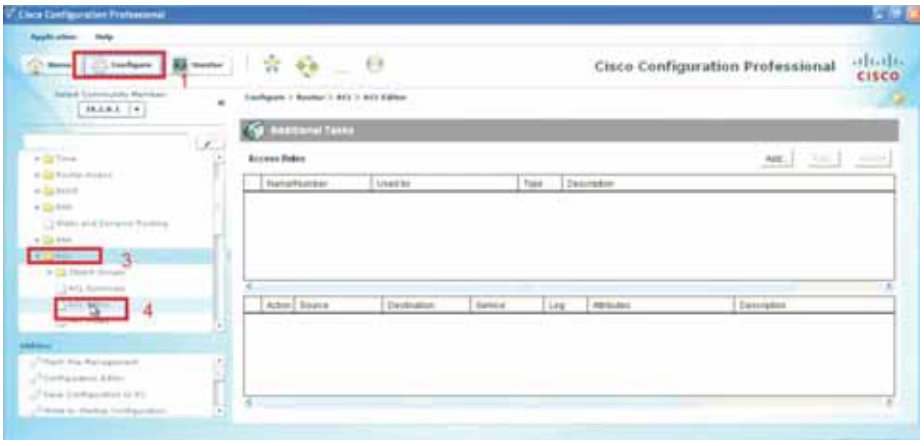
هرچند نیازی نیست که این اعداد به خاطر سپرده شوند زیرا محتوای فهرست‌های کنترل دسترسی دارای اهمیت و اولویت می‌باشند و عملکرد فهرست را مشخص می‌کنند، در ضمن اگر فهرست‌های کنترل دسترسی با استفاده از حروف نامگذاری شوند، دیگر نیازی به استفاده از اعداد ذکر شده مطابق با شکل بالا نخواهد بود.

فهرست‌های کنترل دسترسی استاندارد و توسعه یافته در چه مواردی مورد استفاده قرار می‌گیرند؟

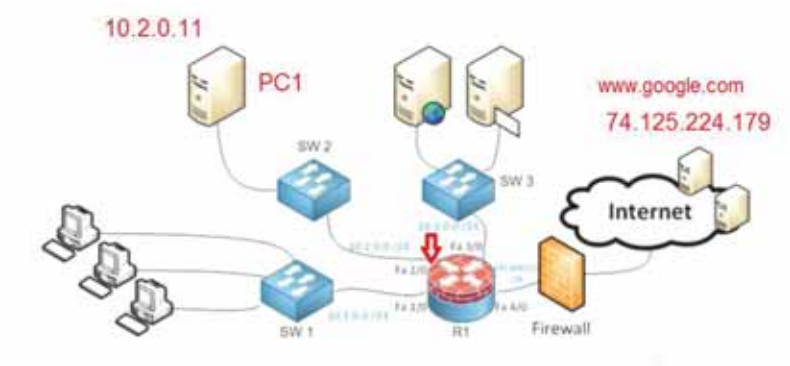
نمونه‌ای را به شرح زیر مطرح می‌کنیم:

فرض کنید ترافیک ایستگاهی که در شبکه داخلی قرار دارد را می‌خواهیم به‌گونه‌ای تنظیم کنیم که از طریق درگاه شماره ۸۰ به سرویس‌دهنده وب گوگل مرتبط نشود. در این مورد خاص اگر بخواهیم بر اساس ترافیک مبدأ، فهرست کنترل دسترسی را تعریف کنیم، آنگاه باید از فهرست استاندارد استفاده کنیم و اگر بخواهیم از مشخصات مقصد استفاده کنیم، آنگاه فهرست توسعه یافته، گزینه درخور خواهد بود.

در نرم‌افزار "CCP" امکانات گوناگونی برای تعریف و مدیریت فهرست‌های کنترل دسترسی در نظر گرفته شده است که در زیر به آنها خواهیم پرداخت.

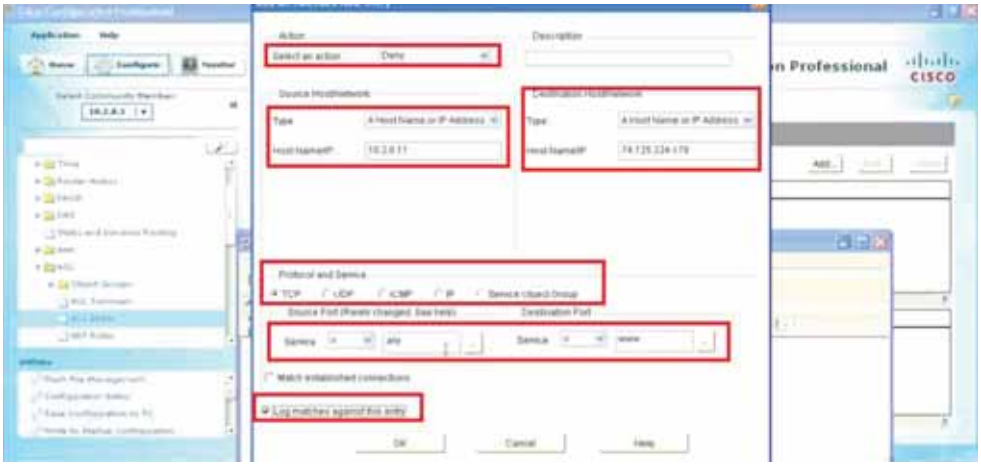


برای ورود به بخش تعریف و مدیریت فهرست‌های کنترل دسترسی (ACL Editor)، نخست از بالای صفحه گزینه "Configure" را انتخاب می‌کنیم(۱) و سپس از منوی سمت چپ صفحه گزینه "Router" و پس از آن گزینه "ACL" را انتخاب می‌کنیم(۲). در پایان بر روی گزینه "ACL Editor" کلیک می‌کنیم(۳). با توجه به توپولوژی شبکه زیر می‌خواهیم از برقراری ارتباط ایستگاه کاری (PC1) به سرویس‌دهنده وب گوگل در اینترنت جلوگیری کنیم.



برای ایجاد فهرست کنترل دسترسی جدید، بر روی کلید "Add" کلیک می‌کنیم.

فهرست کنترل دسترسی را از نوع توسعه یافته انتخاب می‌کنیم و سپس برای درج شرایط موردنظر در این فهرست از "Add" استفاده می‌کنیم:



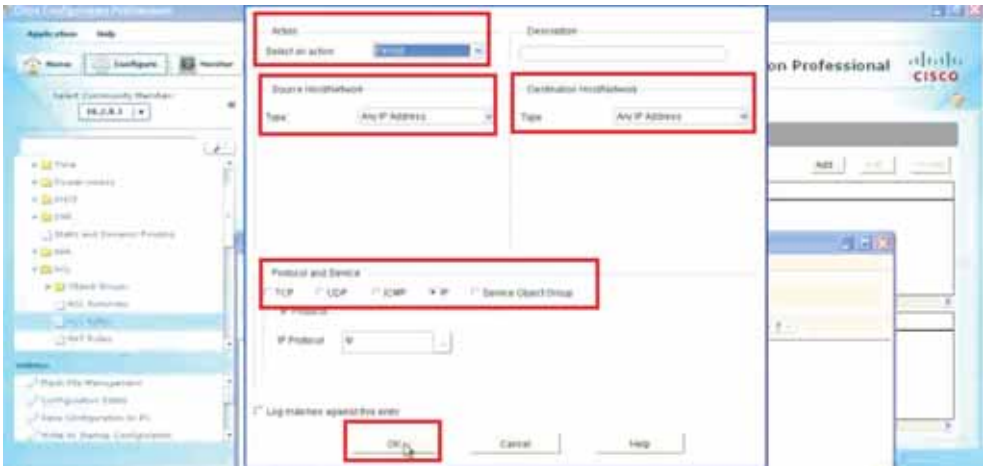
با توجه به شرایط موردنظر (ایستگاه با آدرس مشخص امکان ارتباط از طریق گذرگاه 80 با سرویس‌دهنده گوگل را نداشته باشد) در صفحه بالا اطلاعات موردنیاز را بر اساس آنچه که در توپولوژی شبکه نشان داده شده است، درج می‌کنیم و در پایان برای ثبت آن‌ها از کلید "Ok" استفاده می‌کنیم.

تا به اینجا آیین‌نامه مربوط به کنترل ترافیک موردنظر بر جسب مبدا و مقصد و نوع گذرگاه را مشخص کردیم. در مرحله آخر نوبت به تعیین گذرگاه ارتباطی در مسیریاب می‌رسد:

در این مورد و با توجه به توپولوژی شبکه موردنظر، گذرگاه "Fa2/0"" باید انتخاب شود.

توجه: اگر برای ترافیک دیگر در مسیریاب، آیین‌نامه‌ای تعریف نکنیم، به‌طور پیش‌فرض مسیریاب جلوی عبور ترافیک را می‌گیرد.

برای اینکه امکان عبور هر نوع ترافیک دیگری را از مسیریاب و گذرگاه آن فراهم سازیم، همانند شکل زیر آیین‌نامه جدیدی را ثبت می‌کنیم.



پس از اینکه آیین‌نامه‌های مربوط به فهرست کنترل دسترسی را ثبت کردیم، با استفاده از کلید "Deliver" آنها را به مسیریاب ارسال می‌نماییم.

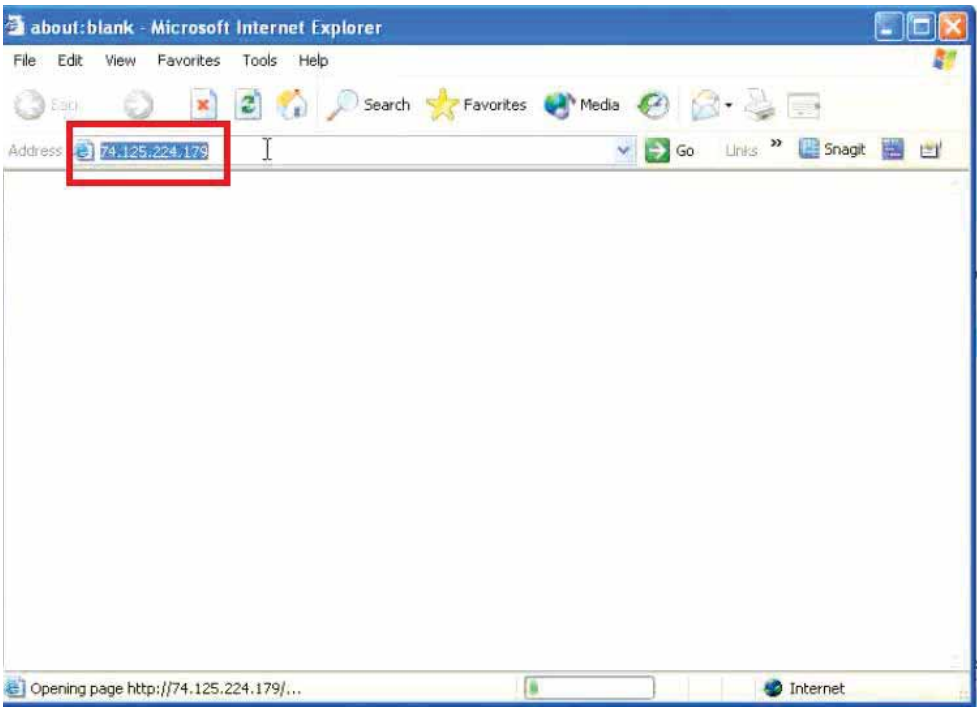
تنظیم‌های انجام شده در فهرست کنترل دسترسی را در خط فرمان مسیریاب مشاهده می‌کنیم:

```
R1#show access-lists
Extended IP access list No-Google-for-You
    10 deny tcp host 10.2.0.11 host 74.125.224.179 eq www log
    20 permit ip any any (68 matches)
R1#
```

دو سطر در فهرست کنترل دسترسی مسیریاب تعریف شده است که با شماره های ۱۰ و ۲۰ مشخص شده‌اند.

با توجه به اینکه آیین‌نامه‌های تعریف شده در فهرست کنترل دسترسی دارای اولویت (از بالا به پایین) است، بنابراین می‌توانیم با شماره‌ای که برای آیین‌نامه جدید در نظر می‌گیریم، اولویت آنرا در فهرست موردنظر مشخص کنیم.

اکنون مرورگر وب را در ایستگاه کاری (PC1) باز می‌کنیم و آدرس سرویس‌دهنده وب گوگل (74.125.224.179) را در نوار آدرس آن وارد می‌نماییم:



واضح است که نباید صفحه‌ای باز شود. چون طبق آیین‌نامه تعریف شده، در فهرست کنترل دسترسی از ارسال ترافیک در مسیریاب جلوگیری کرده‌ایم.

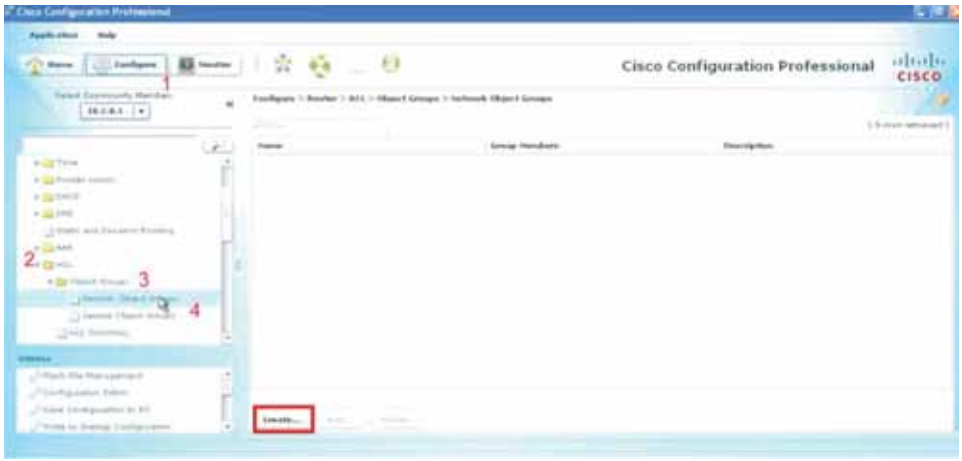
نتیجه ارسال این ترافیک از مسیریاب را در خط فرمان مشاهده می‌کنیم:

```
R1#
%SEC-6-IPACCESSLOGP: list No-Google-for-You denied tcp 10.2.0.11(1461) -> 74.125.224.179(80), 1 p
acket
R1#show access-lists
Extended IP access list No-Google-for-You
    10 deny tcp host 10.2.0.11 host 74.125.224.179 eq www log (3 matches)
    20 permit ip any any (1019 matches)
R1#
```

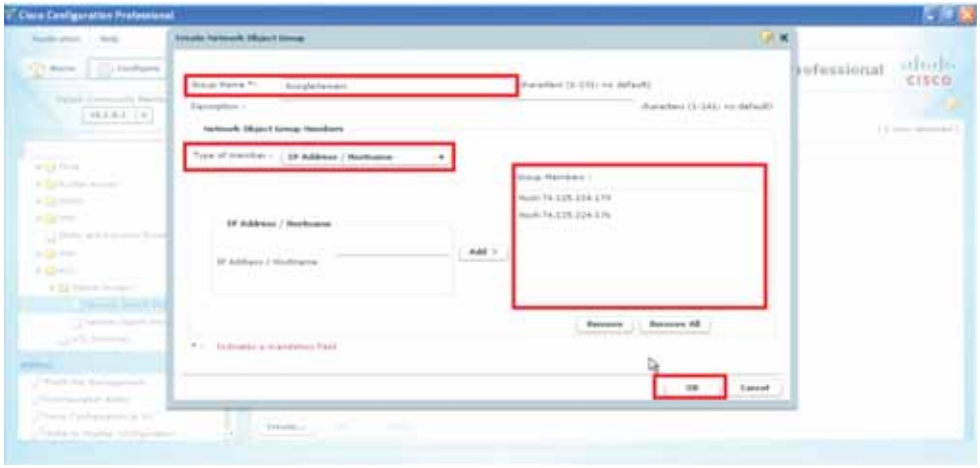
با توجه به مسدود شدن ترافیک موردنظر، پیام هشدار در خط فرمان مسیریاب نمایش داده شده است و در فهرست کنترل دسترسی سه مورد بسته اطلاعاتی مربوط به سطر نخست مشاهده می‌کنیم که مسدود شده‌اند.

همان‌گونه که در شکل زیر مشاهده می‌کنید، سرویس‌دهنده گوگل از یک IP آدرس مشخص استفاده نمی‌کند و اگر بخواهیم در فهرست کنترل دسترسی آنها را به صورت یک‌جا تعریف کنیم، باید از فناوری با نام "Object Group" استفاده نماییم. با استفاده از این روش می‌توانیم گروهی از منابع را با یک نام، مشخص کنیم و سپس آن‌ها را با استفاده از نام موردنظر بکار بریم.

برای تعریف گروهی آدرس‌های سرویس‌دهنده گوگل، نخست بخش مربوط به آنرا انتخاب می‌کنیم.



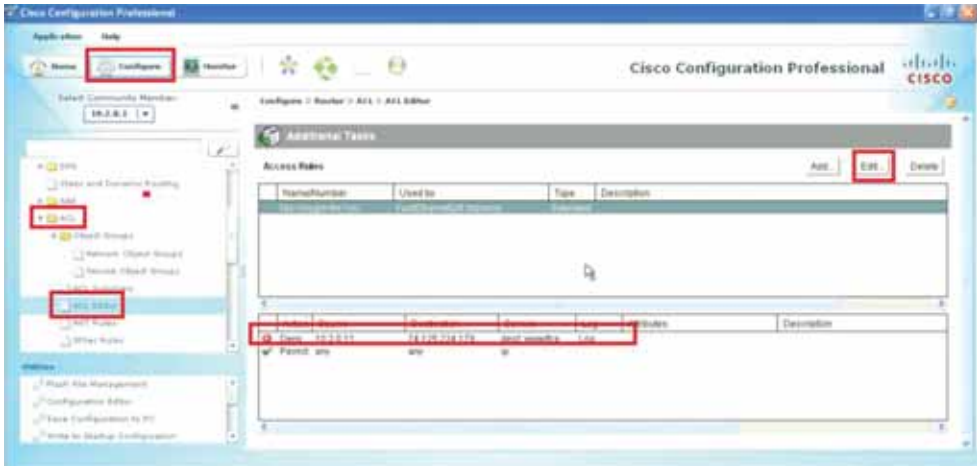
سپس برای ایجاد گروه جدید بر روی گزینه "Create" کلیک می‌کنیم.



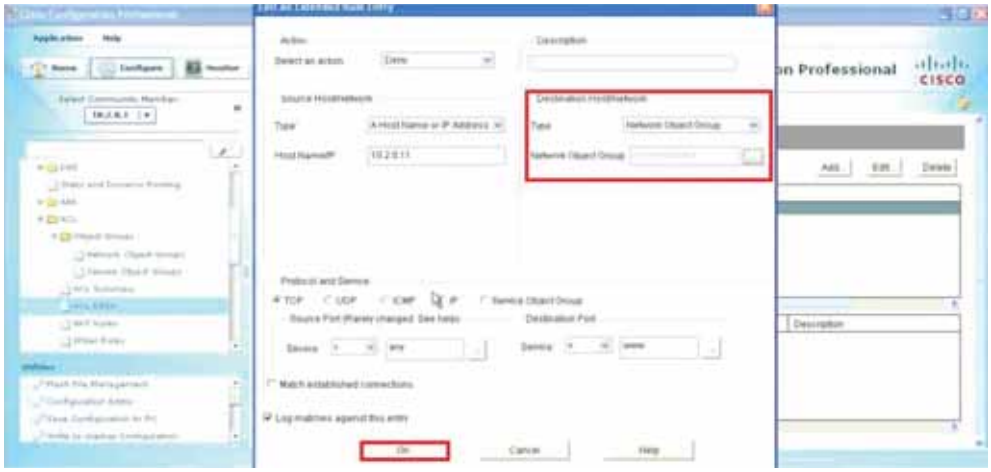
برای گروه موردنظر نام دلخواه انتخاب می‌کنیم و سپس آدرس‌های موردنظر برای درج در گروه را وارد می‌کنیم و در پایان برای ثبت بر روی کلید "Ok" کلیک می‌کنیم.

سپس با استفاده از کلید "Deliver" تنظیم‌های انجام شده را به مسیریاب ارسال می‌کنیم.

با توجه به گروه تعریف شده، در آیین‌نامه موجود در فهرست کنترل دسترسی تغییراتی را ایجاد می‌کنیم. بخش ویرایش فهرست‌های کنترل دسترسی را باز می‌کنیم.

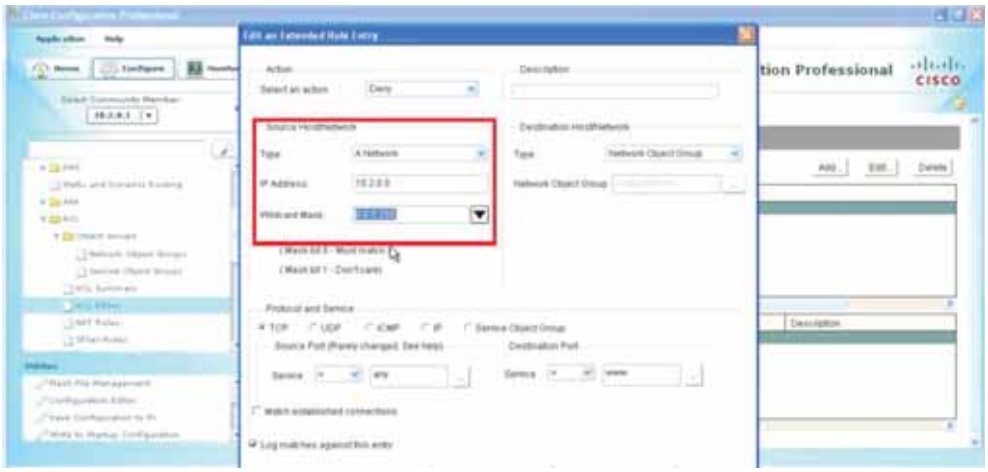


برای ویرایش نخست نام فهرست کنترل دسترسی را انتخاب می‌کنیم و سپس آیین‌نامه موردنظر را مشخص و بر روی کلید "Edit" کلیک می‌کنیم. (همانند شکل بالا)



مقصد ترافیک موردنظر در آیین‌نامه انتخاب شده را تغییر می‌دهیم و سپس با استفاده از کلید "Ok" تغییرات ایجاد شده را ثبت می‌کنیم.

اگر بخواهیم فهرست کنترل دسترسی، ترافیک یک زیرشبکه را کنترل کند، باید از آدرس‌های فراگیر (Wildcard) استفاده کنیم.



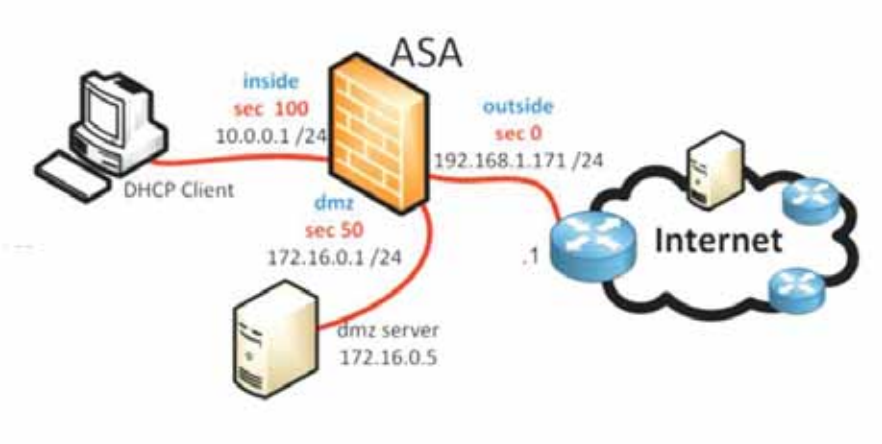
برای تعیین آدرس زیر شبکه از الگوی فراگیر (Wildcard Mask) استفاده می‌کنیم. بخشی از آدرس که باید ثابت باشد را با صفر مشخص می‌کنیم و بخشی دیگر که می‌تواند تغییر کند را با عدد "255" مشخص می‌کنیم. به این ترتیب الگوی موردنظر برای زیرشبکه در توپولوژی شبکه بالا، عبارت "0.0.0.255" است.

پس از اینکه تغییرات موردنظر ثبت شد با استفاده از کلید "Deliver" فهرست کنترل دسترسی تغییر یافته را به مسیریاب ارسال می‌نماییم.

درس۲: پیاده‌سازی فناوری PAT/ NAT

نام فیلم: NAT and PAT (۱:۱۱:۲۳)

در فایروال‌های ASA که از نرم‌افزار ویرایش 8.3 و بالاتر استفاده می‌کنند، جدول تعریف NAT[۱] از سه بخش جداگانه تشکیل شده است. در این درس با فناوری NAT در این نوع فایروال‌ها آشنا می‌شویم و نحوه تنظیم و استفاده از آنرا فرا خواهیم گرفت.



در دروس پیشین به طور مختصر با تنظیم و استفاده از فناوری NAT در فایروال‌های ASA، برای برقراری ارتباط میان شبکه‌های داخل (inside) و شبکه‌های خارج (outside) آشنا شدیم.

نسل جدید فایروال‌های ASA (مانند Cisco 5520) قابلیت پشتیبانی از درگاه ارتباطی با شبکه میانی (DMZ) را دارند. استفاده از شبکه میانی می‌تواند سطح امنیت را در شبکه ارتقا دهد. در این درس با تمرکز بر تعریف ناحیه میانی و استفاده از آن در فایروال ASA، نحوه به کارگیری فایروال را در شبکه مورد بررسی قرار خواهیم داد.

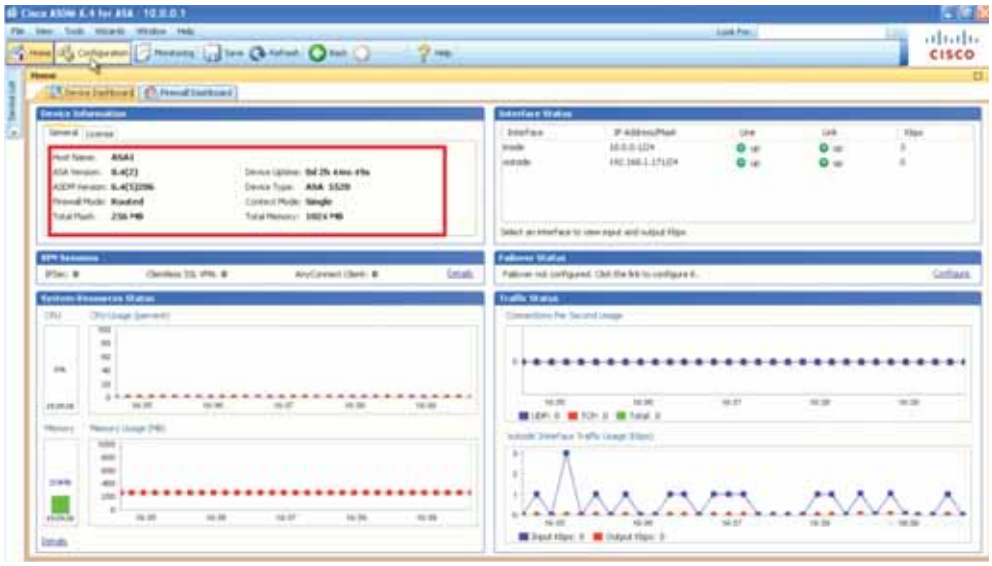
امکان استفاده از ناحیه میانی در فایروال‌هایی که از نسخه‌های قدیمی‌تر (ویرایش 8.2 و پیش از آن) استفاده می‌کردند نیز وجود داشت، اما استفاده از آن دارای ضعف‌های امنیتی بود که شبکه را آسیب‌پذیر می‌نمود.

برای آشنایی با نقاط ضعف موجود در نسل پیش فایروال ASA نخست این نوع فایروال را مورد استفاده قرار می‌دهیم و سپس به بررسی نسل جدید فایروال‌های ASA و امکانات و قابلیت‌های آن می‌پردازیم.

---

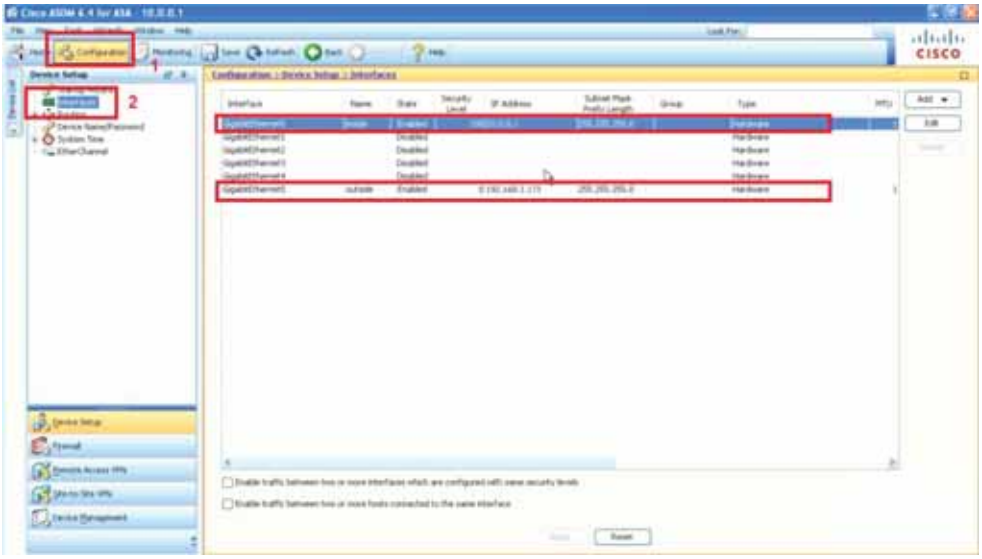
[۱] Network Address Translation

برای شروع همانند شکل زیر نرم‌افزار ASDM را که رابط کاربری گرافیکی برای دسترسی به فایروال ASA به منظور تنظیم و مدیریت آن در اختیار قرار می‌دهد را اجرا می‌کنیم. فایروالی که ASDM آنرا شناسایی کرده و به آن متصل شده است، از نرم‌افزار ویرایش 8.4 استفاده می‌کند. پس فایروال موجود، از نسل جدید فناوری‌های مورد استفاده در فایروال‌های ASA سیسکو پشتیبانی می‌کند.

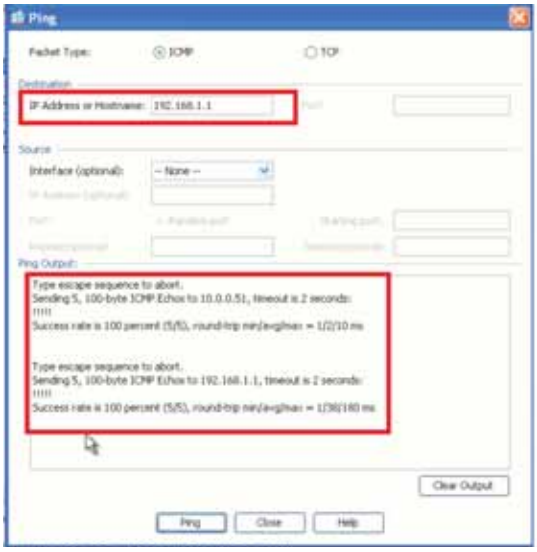


با توجه به مطالبی که در درس پیش برای تنظیم و راه‌اندازی فایروال‌های ASA ارائه شد، برای اینکه تنظیم فایروال را در شبکه به‌طور صحیح انجام دهیم، نخست از نوار ابزار بالای صفحه گزینه "Configuration" را انتخاب می‌کنیم (۱) و سپس در منوی سمت چپ صفحه گزینه "Interfaces" را انتخاب می‌کنیم(۲).

در فایروال موردنظر دو درگاه با اسامی "nside"و "outside" تعریف شده‌اند و برای هر یک سطح امنیتی و همچنین آدرسی برای دسترسی به آن در نظر گرفته شده است. برای کنترل عملکرد رابط‌های شبکه فایروال با استفاده از فرمان "Ping" ترافیک ورودی و یا خروجی از این درگاه‌ها را مورد آزمایش قرار می‌دهیم.



از نوار ابزار بالای صفحه گزینه "Ping" را انتخاب و سپس در پنجره آن آدرس درگاه شبکه را وارد می‌کنیم.



اگر درگاه‌های رابط شبکه به درستی تنظیم شده باشند آنگاه دستور "Ping" انتقال ترافیک از آنها را نشان خواهد داد.

آدرس‌های درگاه‌های رابط در فایروال ASA را به طور ثابت انتخاب کردیم، به‌عبارت دیگر برای تخصیص آدرس آنها از پروتکل DHCP استفاده نشده است. به‌همین دلیل آدرس مسیر پیش‌فرض برای ترافیک با مقصد

نامعلوم نیز می‌بایست به‌طور دستی تعیین شود و تنظیم خودکار آن توسط سرویس‌دهنده DHCP انجام نمی‌شود.

هرچند فایروال وظیفه مسیریابی را به عهده ندارد ولی با توجه به جایگاهی که در شبکه دارد، می‌بایست این کار را انجام دهد. به‌همین دلیل می‌بایست همانند یک مسیریاب تنظیم شود.

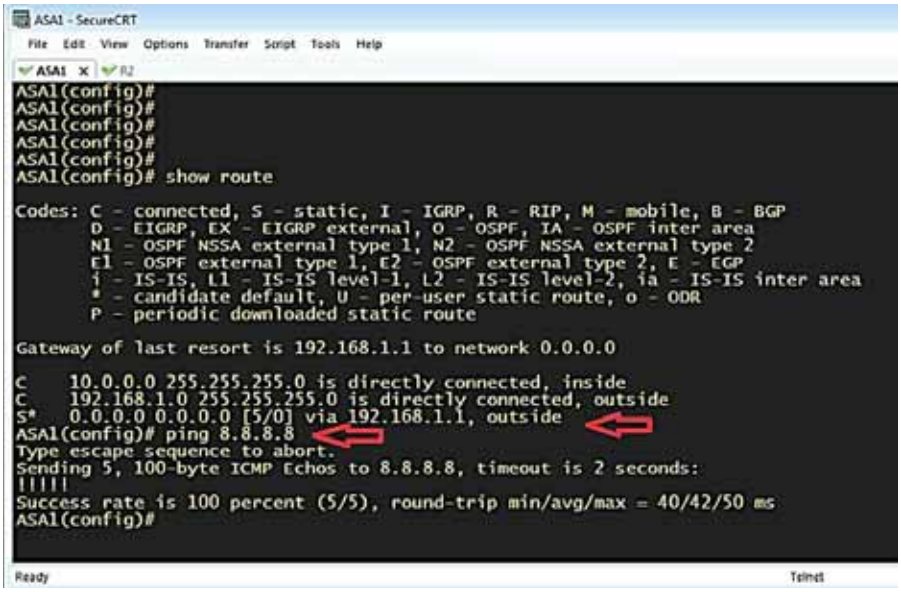
برای اینکه مسیرهای پیش‌فرض را در فایروال مشاهده کنیم، در بخش تنظیمات فایروال (۱) از منوی سمت چپ صفحه گزینه "Routing" را انتخاب می‌کنیم(۲) و سپس گزینه "Static Routes" را انتخاب می‌نماییم(۳).

آدرس مسیر پیش‌فرض در فایروال تعیین شده است. برای اینکه با نحوه تعریف آن آشنا شویم با استفاده از کلید Delete در سمت راست این بخش سطر مشخص شده را حذف می‌کنیم و سپس با استفاده از کلید "Add" مسیر پیش‌فرض موردنظر را همانند شکل زیر در فایروال تعریف می‌کنیم.

طبق تعریف بالا هر ترافیکی که از هر نقطه شبکه داخلی وارد فایروال شود و آدرس مقصد آن در فایروال تعریف نشده باشد به مسیر پیش‌فرض (192.168.1.1) از طریق درگاه خروجی (outside) ارسال خواهد شد. بخش متریک (Metric) نیز برای پروتکل‌هایی نظیر OSPF که بر اساس کوتاه‌ترین مسیر کار می‌کنند در نظر گرفته شده است. به‌طور پیش‌فرض مقدار آن عدد یک است که می‌توان آنرا تغییر داد و در این نمونه برای آن مقدار ۵ را در نظر می‌گیریم.

پس از تعریف مسیر پیش‌فرض، بر روی کلید "OK" کلیک می‌کنیم تا آن را ثبت کنیم و به صفحه مسیرهای ثابت (Static Route) باز گردیم. در این صفحه بر روی کلید "Apply" کلیک می‌کنیم تا جزئیات مسیر تعریف شده در پنجره‌ای نشان داده شود. پس از مرور آن با کلیک بر روی کلید Send آنرا به فایروال ارسال می‌کنیم.

برای کنترل، همانند شکل زیر در خط فرمان فایروال ASA، تنظیم‌های مسیرهای تعریف شده در آنرا مشاهده می‌کنیم:

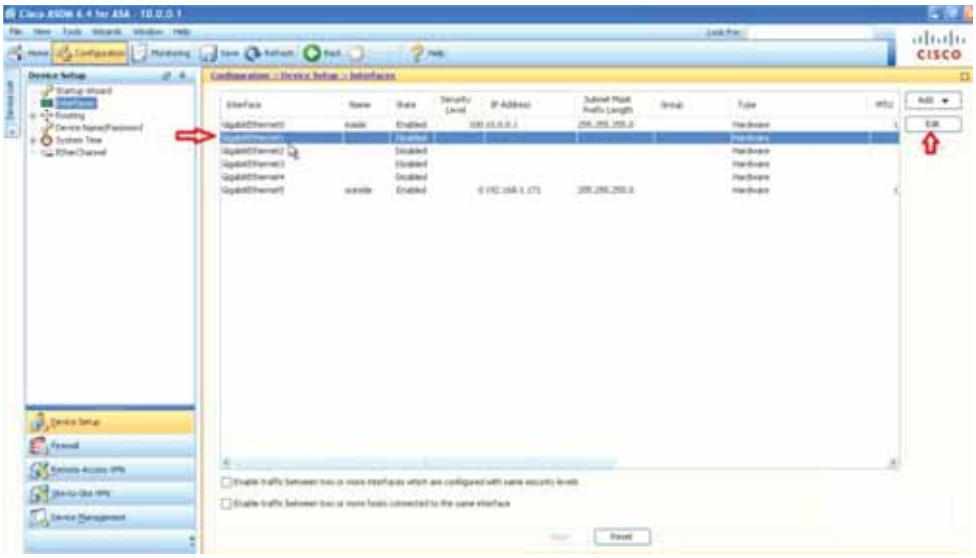


مسیر پیش‌فرض به درستی تنظیم شده است و برای آزمایش آن از دستور "Ping" در خط فرمان استفاده می‌کنیم. آدرسی را در شبکه اینترنت در نظر می‌گیریم (آدرس سرویس‌دهنده DNS گوگل).

و اگر بخواهیم مسیر پیش‌فرض را برای پروتکل TCP مورد آزمایش قرار دهیم، از فرمان "Ping" به شکل زیر استفاده می‌کنیم:

```
ASA1(config)#
ASA1(config)# ping tcp 192.168.1.1 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 192.168.1.1 port 80
from 192.168.1.171, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASA1(config)#
```

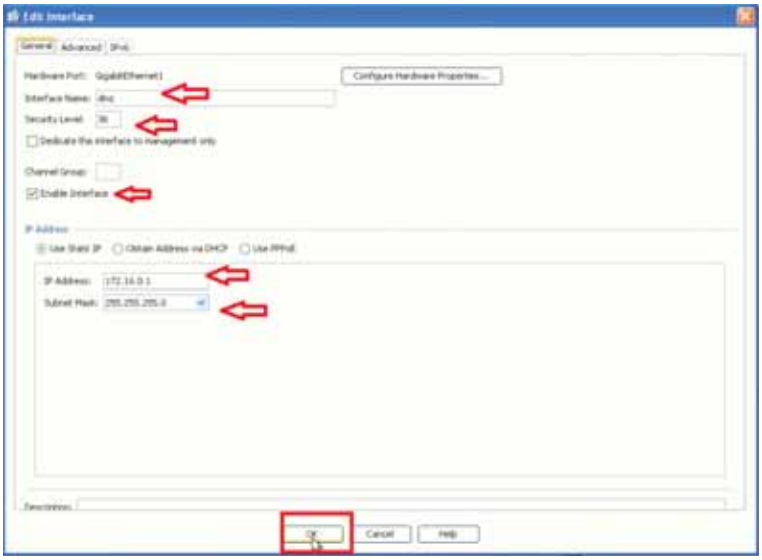
اکنون رابط سوم شبکه را برای اتصال به شبکه میانی (DMZ) تعریف می‌کنیم. نخست درگاه شبکه "GigaEthernet1" را انتخاب می‌کنیم و سپس بر روی کلید "Edit" در سمت راست صفحه کلیک می‌کنیم.



در صفحه تنظیم گذرگاه شبکه، فیلدهای موجود را بر اساس اطلاعات موجود در توپولوژی شبکه، همانند شکل زیر وارد می‌کنیم:

نوع آدرس‌دهی "IPv6" را غیرفعال می‌کنیم و در بخش تنظیم‌های پیشرفته "Advanecd" مک آدرس گذرگاه را تعیین می‌کنیم. وجود مک آدرس برای اشکال‌یابی و رفع اشکال در فایروال‌های ASA اهمیت زیادی دارد.

پس از انجام تنظیمات بالا بر روی کلید "OK" کلیک می‌کنیم تا تنظیم‌های انجام شده ثبت شوند.



نکته: همان‌گونه که در درس پیش نیز اشاره شد، سطح امنیتی یک عدد است که با توجه به مقیاسی که برای آن در نظر می‌گیریم میزان امنیت را مشخص می‌کند. عدد بزرگتر به معنی سطح امنیت بالاتر و عدد کوچکتر به معنی سطح امنیت پایین‌تر است. برای نمونه چون می‌خواهیم سطح امنیت شبکه میانی از بخش داخلی کمتر و از بخش خارجی بیشتر باشد بنابراین هر عددی میان صفر (سطح امنیت شبکه خارجی) تا صد (سطح امنیت شبکه داخلی) را می‌توانیم برای آن در نظر بگیریم (در این نمونه عدد ۳۶ را در نظر گرفته‌ایم).

پس از انجام تنظیم‌ها بر روی کلید "Apply" کلیک می‌کنیم. پنجره‌ای بر روی صفحه نمایش باز می‌شود و در آن جزئیات تنظیم‌ها به همراه فرمان‌های مربوط به آنها نمایش داده می‌شود. آنرا مرور می‌کنیم و سپس بر روی کلید Send کلیک می‌کنیم تا به فایروال ارسال شوند.

برای کنترل تنظیم‌های انجام شده، در خط فرمان فایروال دستور "Ping" را به همراه آدرس درگاه شبکه میانی اجرا می‌کنیم.

```
ASA1(config)#
ASA1(config)# ping 172.16.0.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA1(config)#
```

اکنون به چگونگی استفاده از فناوری NAT در فایروال‌های ASA با نرم‌افزار ویرایش 8.2 و پیش از آن می‌پردازیم. با توجه به اینکه این نوع فایروال همچنان در شبکه‌های گوناگون و سازمان‌ها استفاده می‌شود، بنابراین علی‌رغم نقاط ضعفی که دارد باید با نحوه تنظیم و استفاده از آن آشنا شوید. با توجه به ویژگی‌های بسیار زیاد و مثبتی که در فایروال‌های نسل جدید (دارای نرم‌افزار ویرایش 8.3 به بعد) به‌وجود آمده است، توصیه می‌کنیم که در صورت نیاز به تهیه فایروال جدید، از نسل جدید آن استفاده کنید.

در فایروال‌های ASA ویرایش 8.2 و پیش از آن فناوری NAT به دو شکل مشاهده می‌شود.

۱- وقتی که فناوری NAT فعال باشد
۲- وقتی که فناوری NAT غیرفعال باشد.

در حالت نخست نحوه تعریف و استفاده از این فناوری همانند دستورالعمل‌های شرطی در زبان‌های برنامه‌نویسی انجام می‌شود.

به نمونه زیر توجه کنید:

```
nat (inside) 1 10.0.0.0 255.255.255.0      1
global (outside) 1 192.168.1.51-192.168.1.100
global (outside) 1 192.168.1.101
global (dmz) 1 interface

access-list NONAT permit ip (source net to dest net)
nat (inside) 0 access-list NONAT

static (dmz,outside) 192.168.1.175 172.16.0.5
static (dmz,inside) 172.16.0.5 172.16.0.5
```

اگر ترافیک ورودی از طریق درگاهی که "inside" نام دارد به فایروال وارد شده باشد و مربوط به گروهی با شماره ۱ باشد، و مقصد آن شبکه‌ای با الگوی "10.0.0.*" باشد(۱)، یعنی شرط برقرار است و آیین‌نامه NAT تعریف شده برای آن اجرا خواهد شد.

در ادامه از عبارت "global" برای تنظیم فناوری NAT استفاده می‌کنیم. در سطر دوم مشخص کرده‌ایم که ترافیکی که در شرط سطر نخست صدق می‌کند باید به درگاهی که "outside" نام دارد، ارسال شود. در این بخش محدوده‌ای از آدرس‌هایی را که ترافیک موردنظر می‌تواند به آنها منتقل شود مشخص کرده‌ایم. (192.168.1.51- 192.168.1.100) (۲)

در صورت دلخواه می‌توانیم آدرس مقصد پیش‌فرض برای ترافیک ارسالی را مشخص کنیم. برای نمونه در سطر سوم، همه‌ی بسته‌ها پس از برقرار بودن شرط، به آدرس "192.168.1.101" ارسال خواهند شد.(۳)

این روش استفاده از فناوری "NAT" در فایروال را اصطلاحا "Dynamic NAT" می‌نامند.

می‌توانیم از عبارت "dmz" در تعریف آیین‌نامه‌های مورد استفاده در فناوری NAT نیز استفاده کنیم. در این حالت ترافیک دریافتی به‌طور خودکار به درگاهی که به این منظور اختصاص یافته است ارسال خواهد شد(۴). در این نمونه می‌توانیم آدرس سرویس‌دهنده در منطقه میانی را (172.16.0.5) قرار دهیم(۵). در بخش میانی (dmz) معمولا سرویس‌دهنده وب با امکان استفاده از پروتکل DHCP قرار داده می‌شود تا افزون‌بر تخصیص آدرس‌های موردنیاز برای شبکه داخلی، به عنوان رابط میان شبکه داخلی و شبکه خارجی در نظر گرفته شود تا به این ترتیب امنیت شبکه داخلی ارتقا یابد.

```
nat (inside) 1 10.0.0.0 255.255.255.0      1
global (outside) 1 192.168.1.51-192.168.1.100   2
global (outside) 1 192.168.1.101
global (dmz) 1 interface    4          3

access-list NONAT permit ip (source net to dest net)
nat (inside) 0 access-list NONAT

static (dmz,outside) 192.168.1.175 172.16.0.5
static (dmz,inside) 172.16.0.5 172.16.0.5
```

نکته: اگرچه از فناوری NAT در فایروال استفاده شود و ترافیک دریافتی با آیین‌نامه تعریف شده در آن مطابقت نداشته باشد، آنگاه از عبور ترافیک در فایروال جلوگیری به‌عمل خواهد آمد.

در حالت دوم می‌توان فناوری NAT را برای ترافیک موردنظر غیر فعال نمود. در چنین شرایطی فایروال به محض دریافت ترافیک مشخص شده، آنرا به مسیر پیش‌فرض و از پیش تعیین شده ارسال خواهد نمود و هیچ تغییری در آدرس مقصد بسته موردنظر ایجاد نمی‌کند. به دیگر سخن، بسته به آدرس مقصدی که توسط فرستنده مشخص شده است، ارسال خواهد شد.

یکی از موارد کاربرد این نوع تنظیم در فناوری NAT زمانی است که بخواهیم میان دو ایستگاه و یا سرور از پروتکل‌های رمزنگار نظیر "IPSec" و شبکه مجازی خصوصی (VPN) استفاده کنیم. در این حالت چون تونلی برای انتقال ترافیک رمزنگاری شده ایجاد می‌شود نمی‌توان در میان راه و در داخل تونل از فناوری NAT برای تبدیل و یا تغییر آدرس‌ها استفاده کرد و به همین دلیل می‌بایست برای این نوع ترافیک، فناوری NAT را غیرفعال کنیم.

در نمونه زیر نحوه غیر فعال کردن فناوری NAT برای ترافیکی که میان دو نقطه مشخص که آدرس آنها را مشخص می‌کنیم، نشان داده شده است (۱). در فرمان زیر(۲) عدد صفر به معنی عدم استفاده از فناوری NAT در مورد ترافیکی است که با نام NONAT نامگذاری شده است.

```
nat (inside) 1 10.0.0.0 255.255.255.0
global (outside) 1 192.168.1.51-192.168.1.100
global (outside) 1 192.168.1.101
global (dmz) 1 interface

access-list NONAT permit ip (source net to dest net) 1
nat (inside) 0 access-list NONAT   2

static (dmz,outside) 192.168.1.175 172.16.0.5
static (dmz,inside) 172.16.0.5 172.16.0.5
```

اکنون به روش سوم تعریف و استفاده از فناری "NAT" در فایروال می‌پردازیم که به آن "Static NAT" نیز می‌گویند. در این شیوه از عبارت "Static" در تعریف آیین‌نامه‌های "NAT" استفاده می‌کنیم.

```
nat (inside) 1 10.0.0.0 255.255.255.0
global (outside) 1 192.168.1.51-192.168.1.100
global (outside) 1 192.168.1.101
global (dmz) 1 interface

access-list NONAT permit ip (source net to dest net)
nat (inside) 0 access-list NONAT

static (dmz,outside) 192.168.1.175 172.16.0.5     1
static (dmz,inside) 172.16.0.5 172.16.0.5 2
```

در سطر نخست مشخص نموده‌ایم که اگر ترافیک موردنظر میان دو نقطه "dmz" و "outside" قرار داشته باشد، آنگاه آدرس گیرنده آن "172.16.0.5" به آدرس "192.168.1.175" تبدیل شود(۱). همان‌گونه که در دستور موردنظر مشخص شده است نخست می‌بایست آدرس عمومی که با آن تبدیل می‌شود را مشخص نماییم و سپس آدرس واقعی را که در شبکه استفاده شده است مشخص کنیم.

در سطر دوم ترافیک‌های میان شبکه داخلی "inside" و شبکه میانی "dmz" موردنظر است، با توجه به اینکه نیازی به تغییر آدرس نمی‌باشد پس از فناوری "Identity NAT" استفاده می‌کنیم. یعنی آدرس اصلی و آدرس جدید هر دو یکسان در نظر گرفته می‌شوند(۲). هرچند، این شیوه تعریف و استفاده از فناوری "NAT" مربوط به نسل قدیم فایروال‌های سیسکو است و در نسل جدید فایروال‌های سیسکو از فناوری "Object NAT" استفاده می‌شود. در این فناوری تعریف آیین‌نامه‌ها و استفاده و کاربرد آنها ساده‌تر می‌باشد.

یکی از ویژگی‌های بارز به‌وجود آمده در فایروال‌های نسل جدید سیسکو امکان تعریف و استفاده از فهرست‌های کنترل دسترسی (ACL) است که با استفاده از سطوح امنیتی گوناگونی که در بخش‌های گوناگون شبکه در نظر می‌گیریم، می‌توانیم مجوزهای گوناگونی را برای ترافیک‌های هر بخش تعریف کنیم.

در فایروال‌های نسل جدید سیسکو از مفهوم "Object" برای پیاده‌سازی و استفاده از فناوری "NAT" استفاده می‌شود. یک "Object" در واقع نامی است که به بخش‌های مورد استفاده در فناوری "NAT" اعم از ایستگاه‌های کاری، رابط‌های شبکه و زیرشبکه‌ها و پروتکل‌ها و سرویس‌ها و سرویس‌دهنده‌ها و غیره داده می‌شود.

برای بررسی فناوری "NAT" در فایروال‌های نسل جدید، از توپولوژی شبکه‌ای که در زیر مشاهده می‌کنید استفاده خواهیم کرد: