فیلم‌نگار آموزش عملی

CCNA Security (210-260)

آموزش گام به گام از روی فیلم‌های آموزشی Keith Barker

شرکت CBT Nuggets

تألیف: مهندس مهران تاجبخش

انتشارات پندار پارس

سرشناسه : تاجبخش، مهران، ۱۳۴۷ -
عنوان و نام پدیدآور : فیلم‌نگار آموزش عملی (CCNA Security (210-260: آموزش گام به گام از روی فیلم‌های آموزشی Keith Barker .../ تالیف مهران تاجبخش.
مشخصات نشر : تهران : پندار پارس، ۱۳۹۵.
مشخصات ظاهری : ۴۴۴ص.: مصور، جدول. + دیسک فشرده.
شابک : با لوح فشرده978-600-8201-26-7 : ۳۳۰۰۰۰ریال
وضعیت فهرست نویسی : فیپا
عنوان دیگر : آموزش گام به گام از روی فیلم‌های آموزشی Keith Barker ...
موضوع : سیستم عامل اینترنتی سیسکو -- آزمون‌ها -- راهنمای مطالعه
موضوع : Cisco IOS -- Examinations -- Study guides
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی -- آزمون‌ها -- راهنمای مطالعه
موضوع : Computer networks -- Security measures -- Examinations -- Study guides
موضوع : مسیریاب‌ها (شبکه کامپیوتری) -- آزمون‌ها -- راهنمای مطالعه
موضوع : Routers (Computer networks) -- Examinations -- Study guides
موضوع : ارتباط بین شبکه ای -- آزمون‌ها -- راهنمای مطالعه
موضوع : Internetworking (Telecommunication) -- Examinations -- Study guides
رده بندی کنگره : ۱۳۹۵ ۹ف۲ت/TK۵۱۰۵/۵۹
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۴۵۵۵۰۲۵

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 (CCNA Security (210-260**

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 : ۹۷۸-۶۰۰-۸۲۰۱-۲۶-۷**

فهرست

پیش‌گفتار

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 داده است. 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 موسسه معتبر تحقیقاتی گارتنر، محصولات و خدمات شرکت سیسکو توانسته‌اند در شش حوزه مورد بررسی فناوری‌های شبکه، 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 بیشتر 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 دوره‌های آموزشی در زمینه فناوری‌های سخت‌افزاری و نرم‌افزاری شبکه، اقدام به تدوین و ارائه دوره‌های آموزشی تخصصی امینت در شبکه در سه حوزه 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.

کتاب حاضر با بهره‌گیری که یک شیوه ارائه محتوای آموزشی منحصر به فرد قصد دارد تا مفاهیم و موضوع‌های مورد نظر در دوره آموزشی CCNA Security (210-260) را بر طبق آخرین تغییرات آن پوشش دهد.

تجربه بیش از ۲۵ سال در زمینه مشاوره، آموزش و نصب و راه‌اندازی شبکه سبب شده است تا به این باور برسم که بهترین و کارآمدترین شیوه آموزش در زمینه‌های تخصصی و کاربردی، استفاده از روش‌های عملی و استفاده از مورد کاری‌های نمونه در بیان مفاهیم و دستورالعمل‌های موجود است.

با این هدف و دیدگاه و برای نخستین بار، اقدام به گردآوری این مجموعه با مشخصات و ویژگی‌های زیر نموده‌ام:

- استفاده از بهترین و با کیفیت‌ترین فیلم‌های آموزشی برای بیان عملی و کاربردی مفاهیم و مبانی تخصصی
- برگردان نکات و مباحث مطرح شده در فیلم آموزشی به زبان فارسی به همراه تصاویر منتخب از فیلم‌ها به گونه‌ای که خواننده بتواند به همراه مطلب کتاب، فیلم را هم دنبال نماید.
- انتخاب و تعیین ترتیب مناسب بر اساس محتوای فیلم‌های آموزشی بر اساس موضوع‌های مورد نظر در دوره CCNA Security (210-260)
- استفاده از ۳۷ فیلم آموزشی به مدت تقریبی بیش از ۳۲ ساعت.
- ارائه نسخه اصلی فیلم‌ها به همراه تصاویر منتخب مورد استفاده در کتاب با کیفیت خود در داخل یک لوح فشرده همراه با کتاب.

آشنایی بیشتر با آزمون بین المللی CCNA Security (210-260 IINS)

سرفصل و محتوای آموزشی و همچنین شرایط و قالب برگزاری آزمون بین‌المللی آن توسط شرکت سیسکو اعلام می‌گردد. این دوره آموزشی از نوامبر سال ۲۰۱۵ به جای دوره پیشین (CCNA Security 640-554) با کد جدید (CCNA Security – 210-260 IINS) توسط سیسکو ارائه شد. آزمون بین‌المللی این دوره آموزشی از ۶۰ تا ۷۰ سوال تشکیل شده است که مدت پاسخگویی به سوالات نیز ۹۰ دقیقه می‌باشد. این آزمون در سطح بین‌المللی توسط موسسه Pearson VUE برگزار می‌گردد.

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

- حوزه مبانی امنیت: ۱۲ درصد
- حوزه دسترسی امن: ۱۴ درصد
- حوزه شبکه‌های خصوصی مجازی (VPN): ۱۷ درصد
- حوزه سوئیچینگ و مسیریابی امن: ۱۸ درصد
- حوزه فناوری فایروال‌های سیسکو: ۱۸ درصد
- حوزه پیشگیری از نفوذ غیرمجاز: ۹ درصد
- حوزه امنیت محتوا و نقاط دسترسی: ۱۲ درصد

چه مطالبی را در این کتاب خواهید آموخت

در این کتاب، مبانی امنیت اطلاعات، مثلث امنیت و چگونگی ایجاد امنیت در تجهیزات و فناوری‌های مورد استفاده در شبکه را فرا خواهید گرفت. افزون بر آن با راه حل‌ها و محصولات نرم‌افزاری و سخت‌افزاری که به طور تخصصی توسط سیسکو برای ایجاد امنیت در شبکه ارائه شده است نیز آشنا خواهید شد و در آخر با فناوری‌های ایمن‌سازی و برقراری ارتباط امن از طریق نقاط انتهایی و استفاده کننده در شبکه آشنا می‌شوید. همانگونه در پیش‌گفتار اشاره شد، در این کتاب تلاش شده است تا برای هر یک از موضوعات آموزشی، از یک

یا چند فیلم آموزشی بر اساس مورد کاوی‌های نمونه (Case studies) و منطبق با نیاز واقعی و عملی، استفاده شود.

این کتاب برای چه کسانی است

با توجه به موضوعات و سرفصل‌های آموزشی در نظر گرفته شده در این دوره، مطالعه این کتاب و مشاهده فیلم‌های آموزشی همراه آن به همه متخصصان نصب و راه‌اندازی شبکه، به‌ویژه افرادی که در حوزه امنیت شبکه فعالیت می‌کنند و راهبران امنیت فناوری اطلاعات سازمان‌ها توصیه می‌شود.

درباره 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 چندین مدرک بین‌المللی 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.

در صورت نیاز به برقراری ارتباط با ایشان می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

مهران تاجبخش

زمستان ۹۵

تقدیم به مادرم

به خاطر زحمات بی دریغش

و پسرم

که مایه امید و انرژی من است

فصل ۱

مبانی امنیت – ۱۲%

درس-۱: مثلث امنیت

نام فیلم: CIA (۶:۳۰)

امنیت فضای مجازی موضوعی وسیع و گسترده می‌باشد و به همه راه‌کارها و تجهیزاتی که برای ایجاد امنیت در حوزه مورد نظر مربوط باشد، گفته می‌شود. در این درس سعی خواهیم کرد تا به بررسی پارامترهای اصلی برای ایجاد امنیت در شبکه بپردازیم. اصولی که در ایجاد امنیت شبکه و فضای مجازی مورد بررسی قرار خواهیم داد، با حروف اختصاری CIA نامگذاری شده‌اند.

فرض کنید در سازمانی که دارای منابع سخت‌افزاری و نرم‌افزاری و همچنین مرکز داده و اطلاعات و پرسنل است، می‌خواهیم امنیت را در فضای مجازی و شبکه‌ی آن ایجاد کنیم. البته همواره باید به این نکته توجه داشته باشیم که مهم‌ترین و ارزشمندترین منبع هر سازمان، پرسنل و نیروی انسانی آن است و در درجه بعدی اهمیت، منابع محرمانه سازمان که همان داده‌ها و اطلاعات محرمانه موجود در سازمان است، قرار دارند.

اکنون می‌خواهیم اصولی را مورد بررسی قرار دهیم که با استفاده از آنها می‌توانیم، منابع و داده‌های مهم سازمان را ایمن نگهداری کنیم.

یکی از مواردی که باعث می‌شود تا اطلاعات و داده‌های باارزش سازمان ایمن باقی بمانند، حفظ محرمانگی آنها[1] است. به عبارت خیلی ساده، حفظ محرمانگی یعنی کاربران دارای مجوز دسترسی بتوانند داده‌های مهم و حساس را مشاهده کنند و یا از آن استفاده کنند و دیگر کاربران که دارای مجوز دسترسی نیستند نتوانند به این داده‌ها دسترسی پیدا کنند. برای تحقق چنین هدفی، از فناوری رمزنگاری داده‌ها و اطلاعات استفاده می‌کنیم. اطلاعات و داده‌ها را به‌صورت رمزنگاری شده در حافظه‌های جانبی نگهداری می‌کنیم و یا در زمان انتقال آنها در شبکه، آنها را به‌صورت رمزنگاری شده منتقل می‌کنیم تا بدین ترتیب از دسترسی افراد غیرمجاز به آنها جلوگیری به عمل آوریم. با توجه به اینکه برای دسترسی به اطلاعات می‌بایست اطلاعات را رمزگشایی کرد و این کار با استفاده از کلید رمزگشایی آن انجام خواهد شد، پس تنها افراد دارای مجوز دسترسی می‌توانند این کلید را در اختیار داشته باشند.

یکی دیگر از روش‌های محافظت از داده‌ها و اطلاعات موجود در سازمان، حفظ مشمولیت و یا جامعیت[2] آنها است. به دیگر سخن، با استفاده از روش‌ها و مکانیزم‌هایی از تغییر داده‌ها توسط افراد غیر مجاز، جلوگیری به عمل می‌آوریم. این تغییر می‌تواند در زمان نگهداری داده‌ها در حافظه جانبی و در زمان انتقال آنها در شبکه به‌وجود آید.

---

[1] Confidentiality - محرمانگی

[2] Integrity – مشمولیت

و سرانجام عامل دیگری که در برقراری امنیت داده‌ها و اطلاعات سازمان نقش بسیار مهم و کارآمدی را ایفا می‌کند، حفظ دسترسی به آنها[1] است. زیرا در صورت حفظ محرمانگی و جامعیت داده‌ها و اطلاعات، اگر در مواردی بر اثر حملاتی هم‌چون اختلال در سرویس[2] امکان دسترسی و استفاده از منابع در دسترس را در مواقع موردنیاز نداشته باشیم،

این تمهیدات بی اثر بوده و باز هم امکان استفاده از منابع ارزشمند سازمان وجود نخواهد داشت.

بنابراین هدف از ایجاد امنیت در منابع سازمان، پیرامون سه محور گفته شده که با حروف اختصاری CIA آنها را نشان می‌دهیم، شکل می‌گیرد.

[1] Availability - دسترسی

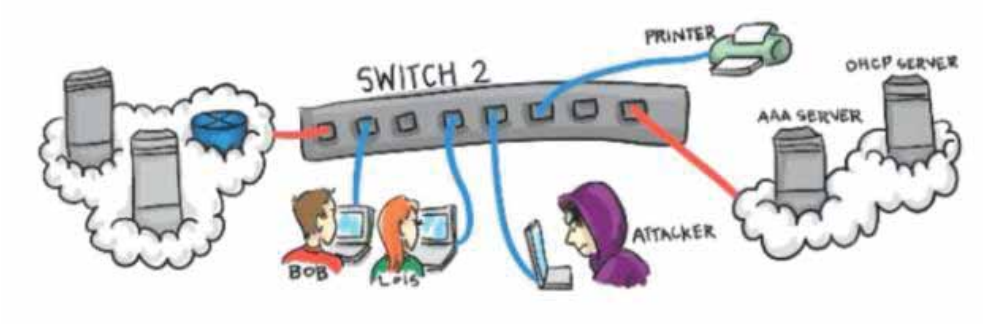
[2] DoS – Denial of Service Attack

درس-۲: مفاهیم امنیت گذرگاه

نام فیلم: Port Security Concepts (۱۴:۱۳)

فرض کنید در شبکه سازمانی که بخشی از آن در شکل زیر نشان داده شده، منابع سازمان و کاربران از طریق تجهیزات ارتباطی موجود در شبکه به یکدیگر متصل شده‌اند. در چنین شرایطی اگر هکری در شبکه وجود داشته باشد می‌تواند با شنود ترافیک شبکه، به اطلاعات مهم و محرمانه سازمان که در شبکه منتقل می‌گردند، دسترسی داشته باشد و به این ترتیب حفظ محرمانگی منابع سازمان، دچار اختلال خواهد گردید.

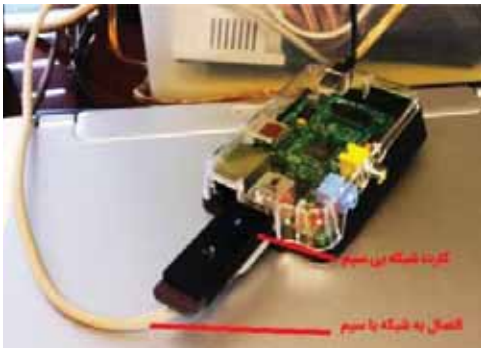
یکی از راه های رفع این مشکل در شبکه سازمان، استفاده از فناوری "امنیت گذرگاه‌ها [1]" می‌باشد.



در این بخش به شرح مبانی فناوری امنیت گذرگاه و همچنین نقش آن در ایجاد امنیت شبکه و جلوگیری از بروز حملات به شبکه و منابع مهم سازمان خواهیم پرداخت.

برای شروع فرض کنید که یک کارت هوشمند Rusbury PI شبیه به آنچه که در شکل زیر نشان داده شده است، در اختیار داریم و بر روی آن سیستم عامل کالی نصب شده است و یک کارت شبکه بی سیم نیز از طریق درگاه USB به آن متصل شده است. بر روی کارت هوشمند مزبور درگاه ارتباط شبکه باسیم نیز وجود دارد که از طریق آن کارت هوشمند موردنظر می‌تواند به سوئیچ شبکه موجود در سازمان متصل شود.

[1] Port Security



این کارت هوشمند به همراه سیستم عامل کالی موجود در آن، علی‌رغم ابعاد کوچک، خود می‌تواند امکانات لازم را برای هک و نفوذ به شبکه موردنظر را فراهم سازد. برای نفوذ به شبکه می‌توانیم از نرم‌افزارهای "apt-get" و "dsniff" و "macof" که در سیستم عامل کالی وجود دارند، استفاده کنیم.

ابتدا دستور "macof" را اجرا می‌کنیم که باعث خواهد شد تا هزاران بسته اطلاعاتی، حاوی مک آدرس‌های قلابی به سوئیچ ارسال شده و سوئیچ نیز سعی خواهد کرد که آنها را در جدول مدیریت ترافیک داخل خود، ثبت و نگهداری کند.

اینک فرض کنید که در جدول مورد نظر در سوئیچ[1]، تنها ظرفیت نگهداری ۵۰۰۰ هزار مک آدرس را داشته باشد و در این شرایط اگر به آن ۶۰۰۰ مک آدرس مختلف ارسال شود، اینکار باعث خواهد شد که حالت سرریزی در این جدول رخ دهد و به این ترتیب سوئیچ قادر نخواهد بود که فرق بین مک آدرس‌های واقعی و قلابی را تشخیص دهد. با توجه به پر شدن جدول بالا، ایستگاه‌های کاری که ازپیش با توجه به مک آدرس‌های خود می‌توانستند از طریق لایه ۲ در سوئیچ با یکدیگر ارتباط داشته باشند، در این شرایط یکدیگر را نخواهند شناخت و سوئیچ با دریافت بسته‌هایی که مک آدرس آنها را نتواند شناسایی کند، آنها را به همه‌ی گذرگاه‌های خود در شبکه مجازی موردنظر ارسال خواهد کرد (در این وضعیت سوئیچ همانند یک هاب کار می‌کند). اکنون در چنین شرایطی، سیستم عامل کالی موجود در شبکه مجازی مورد نظر می‌تواند با استفاده از نرم‌افزارهایی که در اختیار دارد به ترافیک دیگر ایستگاه‌های موجود در شبکه مجازی گوش دهد و از آنها نسخه‌برداری کند. این نوع حمله که به‌سادگی در شبکه‌های مجازی بر اساس سناریوی گفته شده بالا می‌تواند به اجرا درآید، به حمله‌ی "CAM Table Overflow" معروف است.

بهترین راه‌حل برای جلوگیری از بروز چنین حملاتی در شبکه مجازی، استفاده از فناوری امنیت گذرگاه است. در این فناوری می‌توانیم در هر گذرگاه سوئیچ، برای بیشینه مک آدرس‌های جدیدی که می‌تواند بپذیرد و آنها را در جدول "CAM Table" خود ذخیره کند،سقف مشخصی تعریف کنیم.

[1] CAM Table

برای نمونه، برای گذرگاه مورد نظر عدد ۵ را به‌عنوان بیشینه تعداد مک آدرس قابل پذیرش در نظر می‌گیریم و با رسیدن تعداد مک آدرس به بیش از اندازه تعریف شده در گذرگاه، سوئیچ می‌تواند واکنش‌هایی که از پیش برایش تعریف شده است را از خود نشان دهد.

عملیاتی که پس از بروز رخداد تشخیص مک آدرس‌های بیش از حد تعیین شده می‌تواند انجام شود، با حروف اختصاری "PRSS" نمایش داده می‌شوند.

"P" به طور مخفف برای "Protect" در نظر گرفته شده است. در این حالت برای حفاظت سوئیچ از وضعیت سرریزی در صورتیکه تعداد مک آدرس دریافتی از حدمجاز تجاوز کند، آنگاه از ورود مک آدرس‌های جدید به سوئیچ جلوگیری به‌عمل خواهد آمد که نتیجه آن عدم امکان برقراری ارتباط ایستگاه جدید از طریق سوئیچ به شبکه مجازی مورد نظر خواهد بود و این کار نیز بدون اعلان و یا ارسال پیام انجام می‌گردد. با توجه به این شیوه بازدارندگی معمولا این روش گزینه انتخاب درخوری نخواهد بود. چرا که معمولا برای جلوگیری از بروز اختلال در فعالیت‌های جاری سازمان نیاز به اطلاع‌رسانی و یا ثبت رخداد برای چنین شرایطی داریم.

"R" به طور مخفف برای "Restrict" در نظر گرفته شده است. این روش همانند روش "Protect" عمل می‌کند با این تفاوت که می‌توانیم آن را به‌گونه‌ای تنظیم کنیم که با بروز چنین رخدادی، با استفاده از پروتکل "SNMP" پیام درخور به کاربر ارسال شود و یا در فایل ثبت وقایع، رخداد موردنظر ثبت شود و یا با استفاده از شمارنده‌ای، تعداد دفعات بروز چنین رخدادی، ثبت و نشان داده شود. البته باید توجه داشته باشیم که در همه سوئیچ‌های سیسکو این عملیات پشتیبانی نمی‌شوند.

"s" به‌طور مخفف برای "Shutdown" استفاده می‌شود. این واکنش، به طور پیش فرض برای همه سوئیچ های سیسکو در هنگام بروز چنین رخدادی تعریف شده است. در این روش، با مشاهده مک آدرس بیش از تعداد مجاز، گذرگاه مورد نظر غیر فعال خواهد شد و البته در صورت تنظیم آن می‌توان با استفاده از پروتکل " SNMP" پیام مناسب به کاربر ارسال کرد و یا رخداد موردنظر را در فایل ثبت وقایع ثبت و یا با استفاده از شمارنده‌ای، تعداد دفعات بروز این وضعیت را ثبت کرد و نمایش داد.

سرانجام، حرف"S" آخر به طور مخفف برای "Shutdown VLAN" به‌کار برده شده است. در این حالت در صورت مشاهده مک آدرس بیش از تعداد در نظر گرفته شده در گذرگاه موردنظر، شبکه مجازی مربوط به آن گذرگاه غیر فعال خواهد شد.

همان‌گونه که گفته شد روش پیش فرض در بروز وضعیت دریافت تعداد مک آدرس غیر مجاز از طریق یک گذرگاه، غیر فعال‌سازی گذرگاه است (Shutdown) و تعداد مک آدرس مجاز که به‌صورت پیش فرض در سوئیچ‌های سیسکو و برای هر گذرگاه در نظر گرفته شده است، عدد یک می‌باشد.

امنیت گذرگاه در سوئیچ در سه وضعیت گوناگون می‌تواند مورد استفاده قرار گیرد:

- پویا (Dynamic)
- ایستا (Static)
- پیوسته (Sticky)

در وضعیت پویا (Dynamic)، عملیات حفاظت از گذرگاه سوئیچ در مقابل دریافت مک آدرس‌های مازاد بر تعداد مجاز به‌صورت پویا انجام می‌شود. به این معنی که به محض اتصال ایستگاه کاری جدید به سوئیچ، مک آدرس آن به سوئیچ ارسال می‌شود تا سوئیچ، آنرا در جدول "CAM Table" خود ذخیره کند و در این حالت عملیات کنترل و بازدارندگی برای پذیرش مک آدرس غیر مجاز به صورت پویا انجام خواهد شد.

در حالت ایستا (Static)، برای هر گذرگاه می‌بایست از پیش، مک آدرس مجاز مورد استفاده به‌صورت دستی در "Table CAM" سوئیچ تعریف شود که در صورت ورود مک آدرس جدید بیش از ظرفیت تعریف شده، رخداد دریافت مک آدرس بیش از حد مجاز بروز خواهد کرد.

در تعریف مک آدرس به‌صورت ایستا در سوئیچ سیسکو می‌بایست آدرس مربوط به هر گذرگاه در داخل حافظه "Running Config" ذخیره شود. برای اینکه این اطلاعات از میان نروند می‌بایست اطلاعات بالا در فایل "Startup Config " نیز کپی شوند که برای اینکار از فرمان‌های "w" و یا "wr mem" و یا " copy run startup"استفاده می‌کنیم.

و سرانجام سومین وضعیت برای حافظت گذرگاه به‌صورت پیوسته "Sticky" است. در این حالت به‌طور پویا مک آدرس‌های دریافتی از طریق گذرگاه در سوئیچ ذخیره می‌شوند و در عین حال به‌طور اتوماتیک در فایل "Running Config" هم ثبت می‌شوند و این کار باعث می‌شود تا در زمان، صرفه‌جویی شده و عملیات با سرعت بیشتری انجام شود.

در این وضعیت برای اینکه مک آدرس‌ها در سوئیچ ذخیره شوند می‌بایست در شروع کار یک بار همه ایستگاه‌های متصل به سوئیچ مورد نظر را روشن کرد تا همه با ارسال یک بسته اطلاعاتی، مک آدرس خود را به سوئیچ اعلام کنند و به این ترتیب مک آدرس‌ها افزون بر "CAM Table"، در فایل "Running Config" نیز ذخیره می‌شوند و برای اینکه در دفعه بعد راه اندازی سوئیچ، مک آدرس‌های تعریف شده وجود داشته باشند می‌بایست با استفاده از فرمان‌های بالا، محتویات فایل "Config Running" را در "Startup Config" ذخیره کنیم.

امنیت گذرگاه می‌تواند به‌صورت "Access" و یا "Trunk" تعریف شود و مورد استفاده قرار گیرد. انجام تعاریف در این بخش به‌صورت ایستا انجام می‌شوند و در مورد آنها تعریف پویا معنی ندارد؛ چون نمی‌توان وضعیت عملکرد را در حال کار تغییر داد و می‌بایست در هنگام تنظیم اولیه سوئیچ، آنرا تعریف کنیم.

در امنیت گذرگاه به صورت "Trunk" می‌توانید از تعداد مک آدرس بیشتری برای شبکه‌های مجازی متصل به سوئیچ استفاده کنید. در این حالت می‌توانید از واژه "VLAN" در تنظیم تعداد مک آدرس استفاده کنید و به این ترتیب می‌توانید تعداد مک آدرس را برای هر یک از شبکه‌های مجازی به‌طور مستقل تعیین کنید. همچنین می‌توانیم مدت زمانی که هر مک آدرس در داخل سوئیچ باقی می‌ماند را با استفاده از زمان‌های فعال ایستگاه و یا بازه‌های زمانی ثابت تعیین کنیم.

درس-۳: مفاهیم شبکه مجازی خصوصی

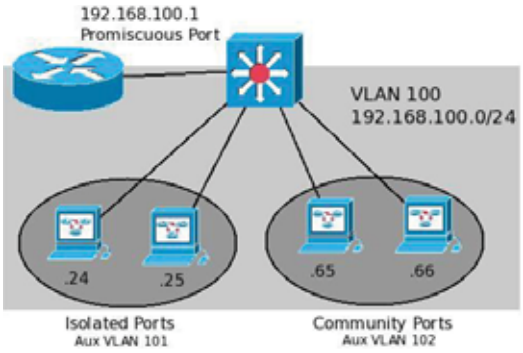
نام فیلم: PVLAN Concepts (۹:۵۱)

در این درس به مفاهیم مربوط به شبکه‌های محلی مجازی خصوصی (PVLAN)[1] خواهیم پرداخت. منظور از شبکه خصوصی مجازی، مجموعه‌ای از ایستگاه‌های کاری هستند که به‌طور مجزا شده از شبکه اصلی با یکدیگر در ارتباط هستند و تشکیل یک شبکه محلی خصوصی را داده‌اند و این شبکه می‌تواند به‌طور مستقل مدیریت و کنترل شود. نقطه مشترک این شبکه‌های خصوصی مجازی، وجود الگوی زیر شبکه مشترک میان آنهاست که همگی در عین اینکه از یکدیگر جدا و مستقل می‌باشند ولی از یک الگوی زیر شبکه مشترک استفاده می‌کنند.

در شکل زیر شمایی از یک شبکه‌ی خصوصی مجازی نشان داده شده است. همانگونه که مشاهده می‌کنید می‌توانیم شبکه‌های خصوصی مجازی را به دو نوع گوناگون تقسیم کنیم.

۱ – شبکه خصوصی مجازی اصلی (اولیه)

۲ – شبکه خصوصی مجازی فرعی (ثانویه)



در هر شبکه تنها یک شبکه خصوصی مجازی اولیه (اصلی) می‌توانیم داشته باشیم و در آن می‌توان به تعداد دلخواه شبکه خصوصی مجازی ثانویه (فرعی) تعریف کرد.

شبکه‌های خصوصی مجازی نیز می‌توانند به دو صورت در نظر گرفته شوند:

۱ –منفرد (Isolated)

۲ –گروهی (Community)

---

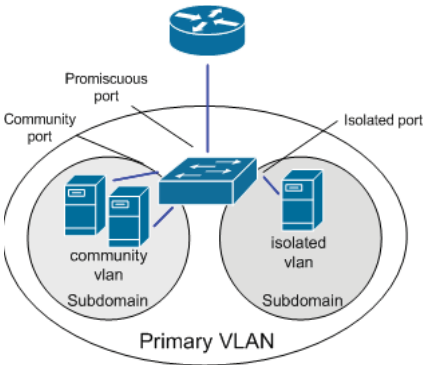
[1] Private VLAN

اگر بخواهیم گذرگاه‌های مورد استفاده در سوئیچ‌های شبکه‌های خصوصی مجازی را نیز مورد بررسی قرار دهیم، آنها نیز به سه گروه زیر تقسیم می‌شوند:

۱ – بی‌قاعده (Promiscuous)

۲ – منفرد (Isolated)

۳ – گروهی (Community)



همان‌گونه که از نام آنها نیز مشخص است، گذرگاه‌های منفرد و گروهی به ترتیب برای شبکه‌های خصوصی مجازی منفرد و گروهی استفاده می‌شوند، و گذرگاه بی‌قاعده[1] مربوط به سوئیچی است که ارتباط میان شبکه‌های مجازی خصوصی را با دنیای خارج برقرار می‌نماید.

[1] Promiscuous

درس-۴: پیاده‌سازی شبکه مجازی خصوصی

نام فیلم: PVLAN Implementation (۱۳:۳۶)

در این درس به‌طور عملی با تنظیم‌های سوئیچ برای آدرس‌دهی یک الگوی زیرشبکه در لایه ۳ برای ایجاد تعدادی زیرشبکه مجازی خصوصی آشنا خواهیم شد.

برای شروع همانند شکل زیر پنجره خط فرمان سوئیچ را باز می‌کنیم.

همانند شکل بالا برای انجام تنظیمات موردنیاز ابتدا سوئیچ را در وضعیت تنظیم قرار می‌دهیم که برای اینکار از فرمان "configure terminal" استفاده می‌کنیم و سپس بر اساس الگوی نمایش داده شده از شبکه مجازی اصلی با شماره ۱۰۰ در تصویر گوشه بالا و سمت راست شکل بالا، می‌خواهیم چهار شبکه مجازی خصوصی تعریف کنیم. برای اینکار به چهار گذرگاه سوئیچ احتیاج خواهیم داشت، پس گذرگاه‌های ۱۱ تا ۱۵ را در سوئیچ با استفاده از فرمان زیر انتخاب می‌کنیم:

```
default int range g0/11-15
```

مرحله بعدی نامرئی‌سازی پروتکل VTP[1] در سوئیچ موردنظر است. پیش از اینکه به آن بپردازیم ابتدا در مورد این پروتکل کمی توضیح می‌دهیم.

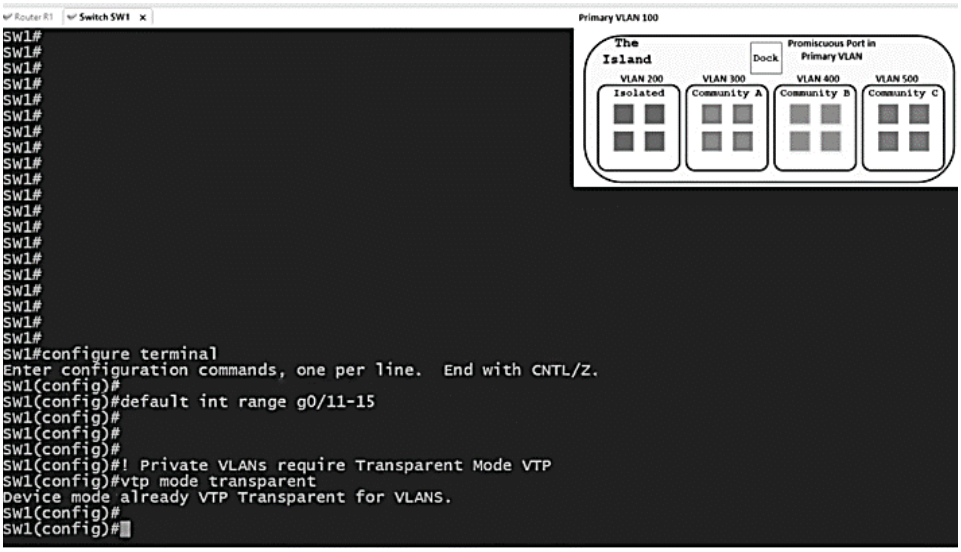
[1] VLAN Trunk Protocol

VTP پروتکلی است که در اغلب دستگاه‌های ارتباطی شبکه محصول سیسکو وجود دارد. با این پروتکل می‌توانیم از تنظیم مستقل هر یک از سوئیچ‌ها در یک شبکه مجازی جلوگیری کنیم. زیرا این پروتکل می‌تواند همه تنظیم‌های مربوط به شبکه مجازی موردنظر را در تمام سطح دامنه موردنظر گسترش دهد؛ به این ترتیب نیازی نخواهد بود که یک شبکه مجازی را چندین‌بار و در نقاط گوناگون دامنه موردنظر تعریف کنیم.

VTP دارای ویرایش‌های ۱، ۲ و ۳ است که از نسخه ۳ آنها تنها در سیستم عامل کاتالیست (CatOS) نسخه ۸/۱ به بعد می‌توان از آن استفاده کرد.

همانند شکل زیر، پیش از ایجاد شبکه‌های مجازی خصوصی موردنظر ابتدا این پروتکل را در وضعیت نامرئی قرار می‌دهیم. برای اینکار از فرمان زیر استفاده می‌کنیم:

```
vtp mode transparent
```



بر طبق دیاگرامی که از شبکه‌های مجازی موردنظر نشان داده شده است، در مجموع، چهار شبکه مجازی خصوصی خواهیم داشت که سه عدد از آنها با اسامی VLAN 300,400,500 از نوع گروهی (community) می‌باشند. برای تعریف آنها همانند شکل زیر از فرمان‌های زیر استفاده می‌کنیم:

```
vlan 500
private-vlan community
exit
```

فرمان‌های بالا را برای هر یک از شبکه‌های خصوصی مجازی تکرار می‌کنیم.

در ادامه می‌بایست یکی از شبکه‌های مجازی خصوصی را به عنوان منفرد (isolate) تعریف کنیم که برای اینکار از فرمان‌های زیر استفاده می‌کنیم:

```
vlan 200
private-vlan isolated
exit
```

مراحل انجام آن در شکل زیر نشان داده شده است.

و همچنین آخرین شبکه مجازی خصوصی را به عنوان شبکه مجازی خصوصی اصلی تعریف می‌کنیم. این شبکه در شکل با شماره 100 مشخص شده است و برای اینکار همانند شکل زیر از فرمان‌های ارائه شده استفاده می‌کنیم:

```
vlan 100
private-vlan primary
exit
```

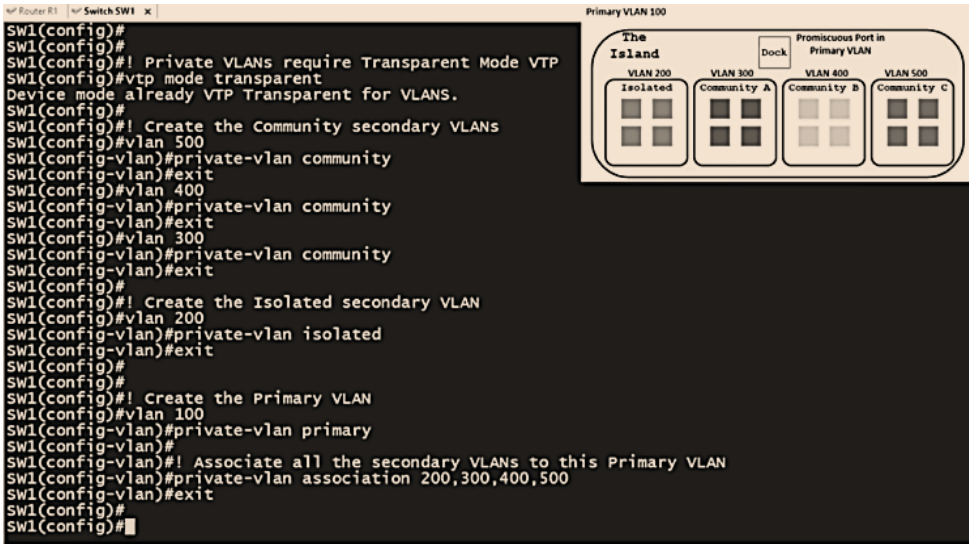
اکنون می‌بایست همه شبکه‌های خصوصی مجازی با شماره‌های 200,300,400,500 را به‌عنوان شبکه‌های فرعی در شبکه اصلی که با شماره 100 آنرا تعریف کردیم، قرار دهیم. برای این کار از فرمان زیر استفاده می‌کنیم:

```
private-vlan association 200,300,400,500
```

با توجه به اینکه شبکه مجازی خصوصی با شماره 100 به عنوان شبکه اصلی تعریف شده است پس در دستور بالا همه شبکه‌های دیگر به عنوان شبکه مجازی خصوصی فرعی در نظر گرفته خواهند شد.

اکنون نوبت به تعریف گذرگاه اصلی ارتباطی مشترک میان زیر شبکه‌های خصوصی مجازی یا همان Promiscuous port موردنظر می‌رسد. برای این کار از فرمان زیر استفاده می‌کنیم:

```
switchport mode private-vlan promicuous
```



با توجه به اینکه از میان گذرگاه‌های ۱۱ تا ۱۵ گذرگاه‌های ۱۲ تا ۱۵ برای زیر شبکه‌های خصوصی مجازی در نظر گرفته شده‌اند بنابراین برای این گذرگاه از شماره ۱۱ استفاده می‌کنیم.

پس از اینکه گذرگاه مشترک میان زیر شبکه‌های مجازی خصوصی تعریف شدند می‌بایست ارتباط آنرا با شبکه‌های خصوصی موجود تعیین کنیم. برای این کار از فرمان زیر همانند شکل استفاده می‌کنیم:

switchport private=vlan mapping 100 200,300,400,500

در مرحله بعد گذرگاه‌های شماره ۱۲ و ۱۳ را در شبکه مجازی خصوصی منفرد (isolated) برای اتصال ایستگاه‌های کاری تعریف کنیم. برای این کار از فرمان‌های زیر استفاده می‌کنیم:

int range gig 0/12-13
switchport mode private-vlan host
switchport private-vlan host-association 100 200

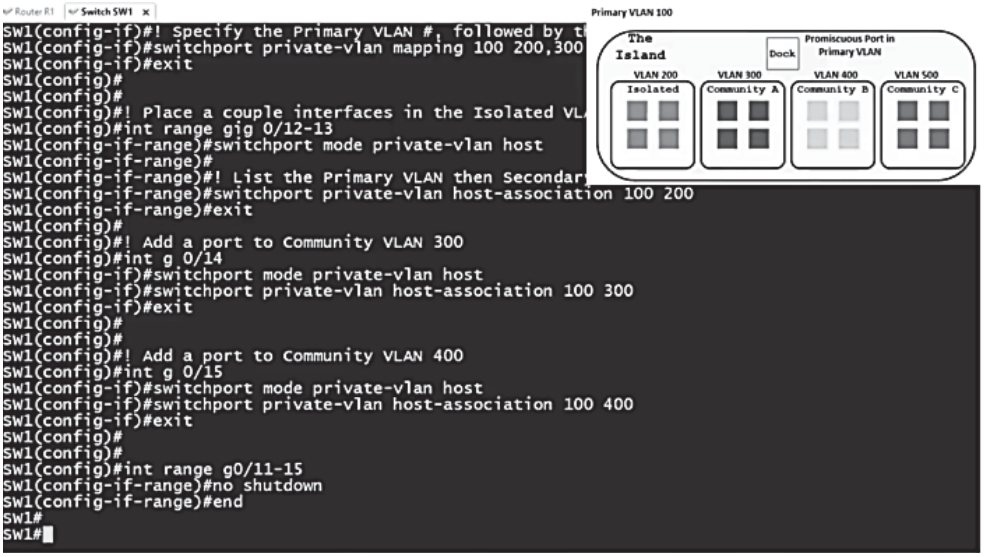
در فرمان آخر توجه داشته باشید که می‌بایست برای تعیین زیر شبکه‌های مجازی خصوصی ابتدا شماره شبکه اصلی (100) و سپس شماره شبکه مجازی خصوصی فرعی موردنظر (200) را بیاوریم.

برای اینکه گذرگاهی را در شبکه‌های مجازی خصوصی فرعی از نوع گروهی (community) تعریف کنیم، از همان دستورات گفته شده بالا استفاده خواهیم کرد و به جای واژه isolated از واژه community و به جای شماره شبکه موردنظر (100) از عدد شبکه گروهی موردنظر (300) استفاده خواهیم کرد. نتیجه فرمان‌های موردنظر به شکل زیر در خواهند آمد:.

و به همان ترتیب که گفته شده، گذرگاه شماره ۱۵ را برای شبکه مجازی خصوصی شماره ۵۰۰ که از نوع گروهی است تعریف می‌کنیم. در شکل زیر مراحل انجام این‌کار نشان داده شده است:

و پس از انجام تعریف‌های موردنظر در مورد درگاه‌های ارتباطی ۱۱ تا ۱۵ می‌بایست برای اینکه مطمئن شویم که همه آنها فعال و آماده به‌کار هستند، از فرمان زیر استفاده کنیم:

no shutdown



اکنون برای کنترل تنظیم‌ها و تعاریف انجام شده مراحل زیر را انجام می‌دهیم:

فهرست شبکه‌های مجازی خصوصی تعریف شده را مشاهده می‌کنیم.

مطابق با شکل بالا در بخش گذرگاه‌ها تنها گذرگاه شماره ۱۳ نشان داده شده است چون هنوز به گذرگاه‌های دیگر موجود در شبکه‌های خصوصی مجازی دستگاهی متصل نشده است و اگر به آنها دستگاهی متصل شود، همانند شکل زیر فهرست گذرگاه‌های نسبت داده شده به شبکه‌های خصوصی مجازی به‌طور کامل نشان داده خواهند شد.

اکنون برای اینکه تنظیمات جزئی‌تر مربوط به گذرگاه اصلی مشترک میان شبکه‌های خصوصی مجازی (Promiscuous port) را مشاهده کنیم، از فرمان زیر استفاده می‌کنیم:

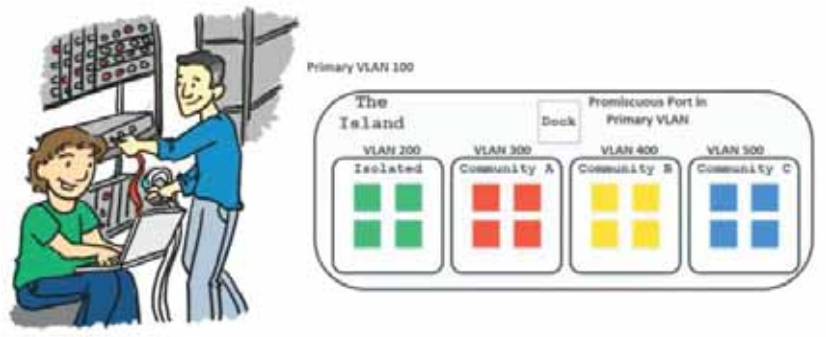
```
show int gig 0/11 switchport
```

نتیجه اجرای آن در شکل زیر نشان داده شده است:

```
100      200        isolated          Gi0/11, Gi0/12, Gi0/13
100      300        community         Gi0/11, Gi0/14
100      400        community         Gi0/11, Gi0/15
100      500        community         Gi0/11

SW1#show int gig 0/11 switchport
Name: Gi0/11
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 100 (VLAN0100) 200 (VLAN0200) 300 (VLAN0300) 400 (VLAN0400) 5
500)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan:
  100 (VLAN0100) 200 (VLAN0200) 300 (VLAN0300) 400 (VLAN0400) 500 (VLAN0500)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

یکی از کاربردهای مهم تعریف و استفاده از شبکه‌های مجازی خصوصی این است که در یک شبکه بزرگ در یک زیر دامنه مشترک که از یک الگوی شبکه مشترک استفاده می‌کنند، می‌توانیم امکان ارتباط مستقیم میان ایستگاه‌های کاری موجود در زیرشبکه‌های خصوصی مجازی را مسدود کنیم و به این ترتیب همانند شکل زیر اگر ایستگاهی از زیرشبکه مجازی نخست بخواهد با ایستگاهی در زیر شبکه مجازی چهارم ارتباط برقرار کند، چنین امکانی به او داده نخواهد شد و تنها این مسیر ارتباطی از طریق گذرگاه ارتباطی بی قاعده (Promicuous port)برای زیرشبکه‌های مجازی امکان‌پذیر خواهد بود. و برای مسدود کردن زیرشبکه مجازی از یکدیگر می‌توانیم به‌راحتی گذرگاه موردنظر را طوری تنظیم کنیم که بسته‌های خروجی از هر زیرشبکه مجازی امکان ورود به همان شبکه را نداشته باشند. با اینکار به‌طور کامل همه زیرشبکه‌های خصوصی مجازی را از یکدیگر جدا خواهیم کرد.



درس-۵: مبانی رمزنگاری

نام فیلم: Cryptography Essentials (۴۲:۰۱)

در این درس به مبانی و اصول ایمن‌تر کردن ترافیک شبکه می‌پردازیم. هنگامیکه ترافیک شبکه حاوی اطلاعات مهم و حساس باشد و نباید در اختیار افراد غیرمجاز قرار گیرد، از فناوری رمزنگاری برای انتقال آن استفاده می‌کنیم.

با استفاده از رمزنگاری می‌توانیم امنیت را در لایه داده شبکه (Data Plane) (انتقال ترافیک) و همچنین لایه کنترل (Control Plane) و لایه مدیریت (Management Plane) ارتقا دهیم.

در حوزه فناوری اطلاعات، مبحثی با نام امنیت اطلاعات (Information Security) یا "InfoSec" وجود دارد که به مباحث مربوط به ایمن سازی داده‌ها و اطلاعات می‌پردازد.

در این حوزه داده‌ها در دو بخش گوناگون مورد بررسی قرار می‌گیرند. یا در وضعیت سکون قرار دارند (در حافظه‌ای ذخیره شده‌اند و نگهداری می‌شوند) و یا در حال انتقال در شبکه می‌باشند.

داده‌ها در وضعیت سکون می‌توانند در دیسک سخت ایستگاه‌های کاری، حافظه‌های پنهان سرویس دهنده‌ها و دیسک‌های سخت موجود در سرویس دهنده‌ها و یا در حافظه‌ها و در انتظار فراخوانی قرار داشته باشند.

داده‌های در حرکت نیز بخشی از ترافیک در جریان شبکه است که میان ایستگاه‌ها و سوئیچ‌ها و مسیریاب‌ها درحال انتقال است.

با در نظر گرفتن فناوری ایمن‌سازی ساختار شبکه[1](NFP) که شرکت سیسکو از آن به‌عنوان فناوری‌های موردنیاز برای ایمن‌سازی هر آنچه که در شبکه قرار دارد، استفاده می‌کند، ساختار شبکه به سه سطح مدیریت، کنترل و داده تقسیم می‌شود. برای اینکه داده‌ها، در حال سکون و یا در حرکت ایمن باشند، می‌بایست برای آنها در هر یک از سه سطح موردنظر، ایمنی ایجاد کنیم.

برای یادآوری، وظیفه هر یک از لایه‌های بالا را به‌طور مختصر مرور می‌کنیم:

لایه مدیریت شامل همه فناوری‌های موردنیاز برای برقراری ارتباط با تجهیزات موجود در شبکه است و با استفاده از عملکرد تجهیزات شبکه تعیین می‌شوند. برای نمونه با استفاده از لایه مدیریت، چگونگی مسیریابی و نوع پروتکل مورد استفاده در مسیریاب را مشخص می‌نماییم. لایه کنترل شامل همه فناوری‌های مربوط به تعیین نحوه ارتباط و به‌روز رسانی جداول مسیریابی در مسیریاب‌ها است. لایه داده نیز شامل فناوری‌های مربوط به انتقال ترافیک در شبکه از یک نقطه به نقطه دیگر از طریق سوئیچ‌ها و مسیریاب‌ها است.

[1] Network Foundation Protection