باسمه تعالی

مستند مرجع طراحی امن شبکه

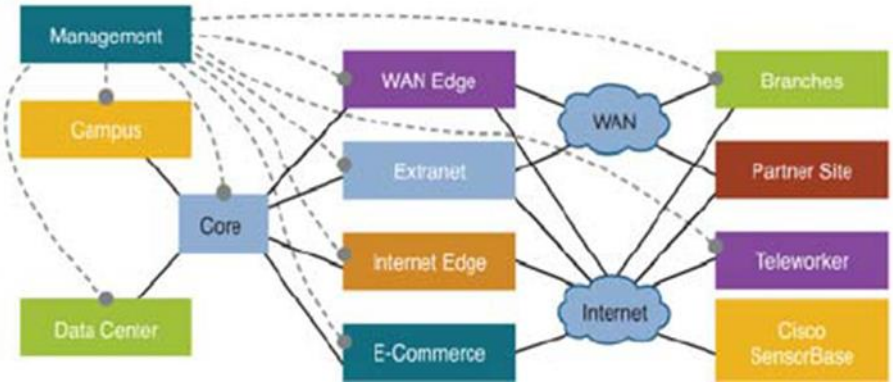
(فصل اول: نگاهی کلی به طراحی امن شبکه براساس مستند Cisco Safe)

مقدمه

انتشار و تکثیر گسترده شبکه‌های بات، افزایش حملات تکامل یافته شبکه، روند رو به رشد و هشداردهنده جرایم اینترنتی سازمان‌یافته، سرقت داده در فضای مجازی، تهدیدات متنوع و پیچیده سایبری به صورت مداوم امنیت شبکه‌های سازمانی و شبکه‌های حیاتی کشور را در معرض تهدید قرار می‌دهد. در این راستا طراحی و پیاده‌سازی امن شبکه یکی از ضرورت‌های اساسی در شبکه‌های سازمانی و شبکه‌های حساس کشور محسوب می‌گردد.

مستند مرجع طراحی امن توپولوژی شبکه به طراحی و پیاده‌سازی امنیت در شبکه‌های کوچک، متوسط و بزرگ می‌پردازد. این مستند بر اساس استاندارد cisco Safe ارائه شده است. در این مستند سعی شده تا با هدف ایجاد لایه‌های دفاعی متعدد و استفاده از استراتژی دفاع در عمق در بخش‌های گوناگون شبکه، دستورالعمل‌ها، الزامات و راه‌کارهای مناسب در حوزه طراحی امن شبکه ارائه گردد. این مستند، در چندین بخش ارائه می‌گردد:

- نگاهی کلی به طراحی safe
- امنیت پایه شبکه (چکیده‌ایی از الزامات امنیت پایه شبکه)
- طراحی امن در شبکه CORE
- طراحی امن در شبکه Campus
- طراحی امن در Internet Edge



Cisco Safe

تکامل و تغییر مداوم در چشم‌اندازها و روش‌های حفظ امنیت، تبدیل به چالشی دنباله‌دار برای سازمآن‌ها شده است. تکثیر سریع باتنت‌ها، پیچیدگی حملات شبکه، رشد زیاد جرم و جنایات سازمان‌یافته‌ی اینترنتی، دزدی اطلاعات و هویت، حملات خلاقانه‌ی داخلی، اَشکال جدیدِ تهدیدات موبایلی و ... مثال‌هایی از مخاطراتِ پیچیده و متنوعی هستند که چشم‌انداز امنیتیِ امروزه را شکل می‌دهند.

شبکه‌ها باید به صورتی امن طراحی و توسعه یابند تا محرمانگی[۱]، اصالت[۲] و دسترسی‌پذیری[۳] اطلاعات و منابع سیستمی در آن‌ها حفظ شده و عملکردهای کلیدی کسب و کار تضمین شود. ساختارِ Cisco SAFE دستورالعمل‌هایی برای توسعه و طراحی به منظور امن‌سازیِ تجهیزات شبکه فراهم می‌کند که هم در برابر حملاتِ شناخته‌شده و هم حملات جدید مقاوم است.

Cisco SAFE رویکرد دفاع در عمق[۴] دارد و چندین لایه‌ی حفاظتی را به صورت استراتژیک در شبکه جای می‌دهد. این ساختار از تکنولوژی‌ها و راه حل‌های جدید و همچنین طراحیِ ماژولار برای سرعت بخشیدن به توسعه استفاده می‌کند. این تکنولوژی از فریم‌ورکِ SCF[۵] استفاده می‌کند. SCF فریم‌ورکی رایج است که دو اصل اساسیِ امنیت یعنی شفافیت[۶] و کنترل[۷] را به حداکثر می‌رساند.

فریم‌ورکِ کنترلِ امنیتِ سیسکو (SCF)

SCF یک فریم‌ورکِ امنیتی با هدفِ در دسترس بودن شبکه و سرویس‌ها و همچنین دوام کسب و کار می‌باشد. تهدیدات امنیتی همواره در حال تحول بوده و SCF با استفاده از راه حل‌های جامع، مجموعه‌ای از تهدیدات

---

۱ Confidentiality

۲ Integrity

۳ Availability

۴ defense-in-depth

۵ Security Control Framework

۶ visibility

۷ control

کنونی و همچنین تهدیدات جدید را پوشش می‌دهد. این فریم‌ورک مجموعه‌ای از قابلیت‌ها و محصولات امنیتی را هدایت می‌کند که به‌وسیله‌ی آن‌ها، میزان مناسبی از شفافیت و کنترل در شبکه به‌دست خواهد آمد.
در SCF فرض شده که سیاست‌های امنیتیِ مناسبی در مقابل تهدیدات و ریسک‌ها به منظور تنظیم اهداف کسب و کار تعیین شده است. این سیاست‌ها و راهبردهای امنیتی، باید استفاده‌ی امن و قابل قبول از سرویس‌ها، تجهیزات و سیستم‌ها را فراهم کنند. همچنین سیاست‌های امنیتی باید فرایندها[۱] و رویه‌های[۲] مورد نیاز برای دست‌یابی به اهدافِ کسب و کار را هم تعیین کنند. مجموعه‌ای از فرایندها و رویه‌ها، عملیات امنیتی[۳] را مشخص مشخص می‌کنند. برای موفقیت یک کسب و کار ضروری است که سیاست‌ها، راهبردها و عملیات‌ها نه تنها سازمان را از رسیدن به اهدافش دور نکند، بلکه به آن سرعت بخشد.

موفقیت سیاست‌های امنیتی به طور عمده وابسته به آن است که تا چه میزان شفافیت و کنترل افزایش یافته باشد. در حالت کلی، امنیت به صورت تابعی از شفافیت و کنترل شناخته می‌شود. بدون دیده شدن، کنترلی انجام نمی‌شود و بدون کنترل، امنیتی وجود ندارد. بنابراین تمرکز اصلیِ SCF بر روی افزایش کنترل و شفافیت است.

SCF شش اقدام امنیتی تعریف می‌کند که سیاست‌های امنیتی را اجرا کرده و شفافیت و کنترل را افزایش می‌دهد. شفافیت به وسیله‌ی تشخیص[۴]، مانیتورینگ و همبسته‌سازی[۵] افزایش می‌یابد. کنترل نیز توسط مقاوم‌سازی[۶]، ایزوله‌سازی[۷] و تحمیل[۸] بهبود می‌یابد (جدول ۱).

---

۱ processes
۲ procedures
۳ Security operation
۴ identify
۵ correlate
۶ harden
۷ isolate
۸ enforce

جدول ۱ . شش اقدام امنیتی معرفی شده توسط Cisco Safe

کنترل			شفافیت		
مقاوم‌سازی، افزایشِ انعطاف‌پذیری، محدودسازیِ دسترسی و ایزوله‌سازیِ تجهیزات، کاربران، ترافیک، اپلیکیشن‌ها و پروتکل‌ها			شناسایی، مانیتور، جمع‌آوری، تشخیص و طبقه‌بندیِ کاربران، ترافیک، اپلیکیشن‌ها و پروتکل‌ها		
تحمیل	ایزوله‌سازی	مقاوم‌سازی	همبسته‌سازی	مانیتور	شناسایی
-تحمیلِ سیاست‌های امنیتی -انتقال رویدادهای امنیتی -پاسخ دادن به رویدادهای غیرعادی به شکل پویا	-ایزوله کردنِ مشترکین، سیستم‌ها و سرویس‌ها - محدود نگه داشتن و حفاظت	-مقاوم کردن تجهیزات، انتقالات، سرویس‌ها و برنامه‌ها -افزایشِ انعطاف‌پذیریِ زیرساخت، رفع اشکالات و تحمل خطا	- جمع‌آوری، همبسته‌سازی و آنالیز اتفاقات در سرتاسرِ سیستم -شناسایی، اعلام و گزارش اتفاقاتِ مهم و مرتبط	-مانیتور کردن عملکردها، رفتارها و اتفاقات و انطباق آن‌ها با سیاست‌ها -شناساییِ ترافیکِ غیرعادی	شناسایی، طبقه‌بندی و اختصاص دادنِ سطوحِ اعتماد به مشترکین، سرویس‌ها و ترافیک

در یک شرکت، قسمت‌های مختلفی در شبکه (PIN[۱]) وجود دارد مانند دیتاسنتر[۲]، پردیس[۳] و شاخه[۴]. طراحی‌های SAFE، از به کار بستنِ SCF برای هر PIN به دست آمده است. نتیجه‌ی آن، شناسایی تکنولوژی‌ها و بهترین کوشش‌ها برای دست‌یابی به شفافیت و کنترل در هر یک از شش فعالیت کلیدی می‌باشد. بدین طریق، طراحی‌های SAFE تکنولوژی‌ها و قابلیت‌های متنوعی را برای دست‌یابی به شفافیت در فعالیت‌های شبکه به کار

[۱] Places in network (PIN)

[۲] data center، گروه بزرگی از سرورها، زیرساخت‌های ارتباطی و امنیتی که برای ذخیره‌سازی، پردازش و توزیع مقادیرعظیمی از داده‌ها از راه دور مورد استفاده قرار می‌گیرند.

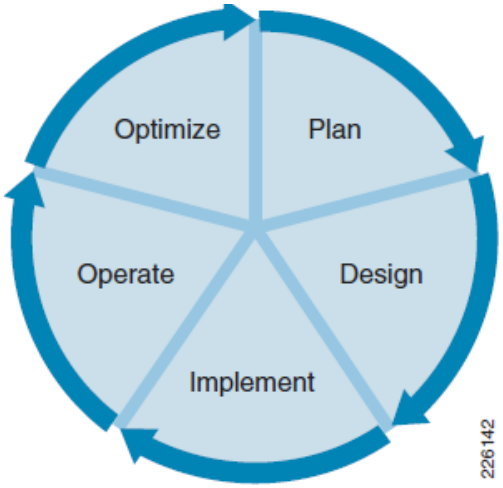
[۳] campus، یک شبکه‌ی رایانه‌ای که از اتصال چند شبکه‌ی محلی (LAN) که همه آنها محدود به یک ناحیه‌ی جغرافیایی هستند ساخته می‌شود، مانند محوطه یک دانشگاه، مجموعه‌ی صنعتی یا پایگاه نظامی که بزرگتر از LAN و کوچکتر ازMAN است.

[۴] branch

می‌گیرد. درنتیجه، عناصر زیرساخت شبکه مانند روترها و سوئیچ‌ها، به شکلی فراگیر و فعال و به عنوان نظارت‌کننده بر سیاست‌ها و عواملِ تحمیل‌کننده استفاده می‌شوند.

چرخه‌ی حیات

چرخه‌ی حیات در Cisco SAFE از ساختار شکل ۱ پیروی می‌کند.



شکل ۱. چرخه‌ی حیات Cisco SAFE

چرخه با برنامه‌ریزی[۱] آغاز می‌شود که باید شامل ارزیابی ریسک و تهدیدات، با هدفِ شناسایی خواسته‌ها و وضعیت فعلی امنیت باشد. همچنین به منظور آشکار شدنِ نقاط قوت و ضعفِ معماریِ فعلی، برنامه‌ریزی باید آنالیز شکاف[۲] را نیز شامل شود.

پس از برنامه‌ریزیِ اولیه، این چرخه با طراحی و انتخاب بسترها، قابلیت‌ها و بهترین تلاش‌های مورد نیاز به منظور از بین بردن شکاف و برطرف کردن نیازمندی‌های آینده ادامه می‌یابد. این نتایج به صورت موشکافانه طراحی شده تا نیازمندی‌های فنی و کسب و کار را برطرف کند.

مرحله‌ی پیاده‌سازی[۳] پس از طراحی انجام می‌گردد که شامل گسترش[۴] و تامین بسترها و قابلیت‌ها می‌باشد. گسترش معمولاً در فازهای مجزا اجرا می‌شود که نیازمند توالی در برنامه‌ها است.

---

[۱] planning

[۲] Gap analysis

[۳] implementation

[۴] deployment

زمانی که یک پیاده‌سازی جدید مستقر می‌شود، نیازمند نگهداری و گردانیدن است. این موضوع شامل مدیریت و مانیتورکردن زیرساخت‌ها و اطلاعات امنیتی به منظور مقابله با تهدیدها می‌باشد.

از آنجا که نیازمندی های امنیتی و کسب و کار پیوسته در حال تغییر هستند، ارزیابی‌های منظم باید انجام شده تا شکاف‌های ممکن شناسایی و برطرف شوند. اطلاعاتِ به دست آمده از عملیات‌های روزانه و ارزیابی‌های تک منظوره می‌تواند بدین منظور مورد استفاده قرار گیرد.

همانطور که در شکل ۱ نشان داده شده است، این فرایند به صورتِ تکرارشونده انجام می‌پذیرد.

ساختارِ SAFE

Cisco SAFE شامل الگوهای طراحی[۱] بر پایه‌ی CVDها[۲] و همینطور بهترین تلاش‌ها بوده و دستورالعمل‌های طراحی امن و قابل اطمینانِ زیرساخت شبکه را فراهم می‌کند. الگوهای طراحیِ Cisco SAFE با جای دادن استراتژیکِ محصولات و قابلیت‌های سیسکو در شبکه، دفاع در عمق را توسعه می‌دهند. در نهایت، چند لایه کنترل امنیتی تحت یک استراتژی و سیاست رایج در طول شبکه اعمال می‌شود.

همزمان، الگوهای طراحی، نیازمندی‌های ثابت و مشخصی را به PINهای مختلفی که در مجموعه موجود هستند اعمال می‌کند. همچنین، الگوهای طراحیِ Cisco SAFE به شکل یک زیربنا برای راه‌حل‌های امنیتیِ افقی و عمودی توسعه یافته است تا نیازمندی‌های صنایع مختلفی مانند مالی، سلامت و تولید را مرتفع کند. به علاوه، سرویس‌های امنیتیِ سیسکو به عنوان بخش‌هایی ذاتی در Cisco SAFE تعبیه شده‌اند.

اصولِ ساختار

الگوهای طراحیِ Cisco SAFE شامل اصول زیر است:

[۱] Design blueprint

[۲] cisco validated design

- دفاع در عمق: Cisco SAFE با دنبال کردنِ روشِ دفاع در عمق و همینطور اطمینان از محرمانگی[۱]، اصالت[۲] و دسترسی‌پذیریِ[۳] داده‌ها، برنامه‌ها، نقاط پایانی و همینطور خودِ شبکه، امنیت را در شبکه تعبیه کرده است. برای افزایش شفافیت و کنترل، مجموعه‌ای غنی از تکنولوژی و قابلیت‌های امنیتی در چندین لایه ولی تحت یک استراتژیِ واحد گسترش یافته است.

- ماژولار بودن و انعطاف‌پذیری: الگوهای طراحیِ Cisco SAFE، یک طراحی ماژولار را دنبال می‌کند که در آن همه‌ی مؤلفه‌ها به وسیله‌ی نقش‌های عملکردیِ خود توصیف می‌شوند. زیرساختِ کلیِ شبکه به ماژول‌های عملکردی تقسیم می‌شوند که هریک، یک PIN مجزا را نشان می‌دهد مانند پردیس و دیتاسنتر. سپس ماژول‌های عملکردی به لایه‌ها و بلوک‌های کوچکتر و قابل مدیریت‌تر تقسیم می‌شوند که هر کدام نقشی خاص را در شبکه بازی می‌کنند.

  طراحی‌های ماژولار، انعطاف‌پذیری را بالا برده که امکان پیاده‌سازیِ فازبندی شده‌ی ماژول‌ها را فراهم می‌کند و نیازهای کسب و کارِ سازمان را به بهترین نحو برطرف می‌کند. توصیفِ مؤلفه‌ها به وسیله‌ی نقش‌های عملکردیشان و نه بسترهای اشاره، موجب می‌شود امکان انتخاب بهترین بستر برای نقش‌های ثابت و جایگزین‌های نهایی آن‌ها همگام با پیشرفت تکنولوژی فراهم شود. همچنین ماژولار بودن طراحی، به پذیرش نقش‌ها و سرویس‌های جدید سرعت بخشیده و زندگی مفید تجهیزات موجود را افزایش داده و سرمایه‌گذاری‌های قبلی را بهبود می‌بخشد.

- دسترسی‌پذیری[۴] و بهبودپذیری[۵] سرویس‌ها: الگوهای طراحی Cisco SAFE چندین لایه افزونگی اضافه می‌کنند تا در برابر خرابی‌های تک‌نقطه‌ای مقاوم بوده و دسترسی‌پذیریِ تجهیزات شبکه را بیشینه کند. این موضوع شامل استفاده از رابط‌های[۶] افزونه، ماژول‌های پشتیبان، تجهیزاتِ آماده به کار و مسیرهای

---

[۱] confidentiality

[۲] integrity

[۳] availability

[۴] availability

[۵] resiliency

[۶] interface

افزونه در توپولوژی می‌شود. به علاوه، طراحی‌ها از مجموعه‌ی وسیعی از امکانات که شبکه را نسبت به حملات و خرابی‌های شبکه انعطاف‌پذیرتر کرده‌اند استفاده می‌کند.

- پیروی از مقررات: Cisco SAFE یک خط مبنای امنیتی را به عنوان جزئی ذاتی در زیرساخت شبکه توسعه داده است. خط مبنای امنیتی شامل مجموعه‌ای غنی از عملکردها و شیوه‌های امنیتی است که موجب تسهیلِ پیروی از مقررات می‌گردند.

- تلاش برای بهره‌وری عملیاتی: طراحیِ Cisco SAFE تسهیل مدیریت و عملیات در تمامی چرخه‌ی حیات آن را مد نظر قرار داده است. محصولات، قابلیت‌ها و توپولوژی‌ها با دقت انتخاب شده‌اند تا شفافیت و کنترل را در هر محافظ بیشینه کنند و در عین حال یک دید واحد از وضعیت کلی شبکه فراهم آورند. به منظور تسریعِ تأمین و همینطور کمک به عیب‌یابی و محدود کردنِ سریعِ مشکلات و کم کردن هزینه‌های عملیاتی، طراحی‌ها ساده فرض شده‌اند. مرکز اصلیِ کنترل و مدیریت، توسط ابزارها و رویه‌های مورد نیاز برای تایید عملیات و اثربخشیِ محافظت‌کننده‌ها فراهم شده است.

- پیاده‌سازی قابل بازرسی: Cisco SAFE مجموعه‌ای از ابزارها را برای اندازه‌گیری و بررسی عملیات‌های مرتبط با تدابیر حفاظتی در شبکه پیاده‌سازی می‌کند، نمایی از وضعیت فعلیِ شبکه فراهم می‌کند و به ارزیابیِ تطابق آن‌ها با سیاست‌ها، استانداردها و مقررات امنیتی کمک می‌کند.

- به اشتراک گذاری اطلاعات و همکاری: Cisco SAFE از به اشتراک گذاری اطلاعات و امکاناتِ تعاملی که در بسترها و محصولات سیسکو موجود است استفاده می‌کند. به منظور بیشینه کردنِ شفافیت، اطلاعات مربوط به ورود به سیستم و اطلاعاتِ رویدادهای تولید شده از تجهیزاتِ موجود در شبکه به‌طور مرکزی جمع‌آوری شده، هدایت گردیده و همبسته‌سازی می‌گردند. به منظور افزایش کنترل، پاسخ دادن و مقابله به شکل مرکزی و هماهنگ انجام می‌شود.

اصولِ SAFE

شبکه‌ها متشکل از انواع مختلفِ تجهیزات، سرویس‌ها و اطلاعات است که ممکن است محرمانگی، اصالت یا دسترسی‌پذیری در آن‌ها در معرض خطر قرار گیرد. امن‌سازی شبکه و سرویس‌های آن، نیازمند فهم کافی از این

دارایی‌ها و تهدیدات بالقوه‌ی آن‌ها می‌باشد. هدفِ این بخش، افزایش آگاهی در مورد عناصر مختلف شبکه است که ممکن است در معرض خطر قرار داشته باشند.

تجهیزات زیرساخت به عنوان هدف:

تجهیزاتِ شبکه فقط شامل روترها و سوئیچ‌ها نیست، بلکه انواعِ مختلفِ دستگاه‌های in-line همچون فایروال، سیستم‌های جلوگیری از نفوذ[۱]، متعادل‌کننده‌های بار[۲] و ابزارهای شتاب‌دهنده‌ی برنامه را نیز شامل می‌شود. همه‌ی این تجهیزاتِ زیرساختی ممکن است در معرض حمله قرار گیرند. این امر دسترسی‌پذیریِ شبکه را به‌طور مستقیم یا غیرمستقیم تحت تاثیر قرار می‌دهد. این حملات شاملِ دسترسی غیرمجاز، بالا بردن سطح دسترسی، منع سرویسِ توزیع شده (DDoS)، سرریز بافر، حملاتِ traffic flood و ... می‌شود.

به طور کلی ابزارهای زیرساخت شبکه، مکانیزم‌های دسترسیِ چندگانه‌ای از قبیلِ دسترسیِ کنسول و دسترسی از راه دور برپایه‌ی پروتکل‌هایی مثل Telnet، rlogin، HTTP، HTTPS و SSH را فراهم می‌کنند. مقاوم کردن این تجهیزات برای جلوگیری از دسترسیِ غیرمجاز ضروری است. بهترین تلاش‌ها عبارتند از استفاده از پروتکل‌های امن، غیرفعال کردنِ سرویس‌های استفاده نشده، محدود کردن دسترسی به پورت‌ها و پروتکل‌های ضروری و اِعمالِ Authentication، Authorization و Accounting (همان AAA).

از آنجا که تجهیزاتِ زیرساخت یکسان نیستند، به منظور امن کردن آن‌ها ضروری است ویژگی‌های منحصر به فردِ هر کدام درک شود. هدف اولیه‌ی روترها و سوئیچ‌ها فراهم کردن اتصال است؛ بنابراین پیکربندی‌های پیش فرض معمولاً اجازه‌ی انتقالِ بدون محدودیتِ ترافیک را می‌دهند. علاوه براین ممکن است بر روی تجهیزات، سرویس‌هایی به طور پیش فرض فعال بوده در حالیکه ممکن است برای یک محیط خاص نیاز نباشند. این موضوع می‌تواند منجر به ایجاد امکانی برای سوءاستفاده شود. لذا باید برای غیرفعال کردن سرویس‌های غیرضروری، گام های لازم برداشته شود.

---

[۱] Intrusion Prevention System (IPS)

[۲] Load Balancer

مسئولیت روتر به طور خاص، یادگیری و گسترشِ اطلاعات مسیریابی و در نهایت هدایت کردنِ بسته‌ها به مسیرهای مناسب است. حملات موفق در برابر روترها آن‌هایی هستند که قادرند با تسخیرِ خود روتر یا نشست‌های آن و یا جدول مسیریابی، بر روی حداقل یکی از کارکردهای اصلی آن تاثیر بگذارند یا آن‌ها را مختل کنند. به دلیل طبیعتِ لایه سومیِ آن‌ها، روترها می‌توانند از شبکه‌های دوردست نیز مورد حمله قرار گیرند. بهترین تلاش‌ها برای امن کردن روتر عبارتند از مقاوم‌سازی، فیلتر کردن بسته‌ها، محدود کردن عضویت در پروتکل مسیریابی و کنترلِ گسترشِ اطلاعات مسیریابی.

برخلاف روترها، ماموریت سوئیچ‌ها فراهم کردن اتصالِ LAN است. بنابراین آن‌ها بیشتر نسبت به حملات لایه‌ی دو آسیب‌پذیر هستند که منشأ آن معمولاً در داخل سازمان است. حملات رایج در محیط‌هایی که از سوئیچ استفاده می‌کنند عبارتند از broadcast storm، MAC flooding و همچنین حملاتی که برای محدود کردن پروتکل‌هایی نظیرِ APR[۱]، DHCP[۲] و STP[۳] طراحی شده‌اند.

بهترین تلاش‌ها برای امن کردنِ سوئیچ شامل مقاوم‌سازی، محدود کردن دامنه‌ی همه‌پخشی[۴]، امنیتِ SPT ، بازرسیِ ARP[۵]، Anti-spoofing، غیرفعال کردن پورت‌های بی‌استفاده و پیروی از توصیه‌های منتشر شده تحت عنوان بهترین تلاش‌ها است.

فایروال‌ها، متعادل‌کننده‌های بار و تجهیزاتِ in-line نیز به طورکلی در معرض دسترسی غیرمجاز قرار می‌گیرند و لذا مقاوم‌سازی آن‌ها ضروری است. مانند هر تجهیزِ زیرساختیِ دیگر، دستگاه‌های in-line منابع و قابلیت‌های محدودی دارند و در نتیجه به طور بالقوه در برابر حملات اتمام منابع[۶] هم آسیب‌پذیر هستند. این نوع از حملات با هدفِ مصرف کردن قدرت پردازش یا حافظه‌ی دستگاه‌ها طراحی شده‌اند و با مشغول کردن ظرفیت دستگاه به

---

[۱] Address Resolution Protocol

[۲] Dynamic Host Configuration Protocol

[۳] Spanning Tree Protocol

[۴] broadcast domain

[۵] ARP inspection

[۶] resource exhaustion

لحاظ تعدادِ ارتباط در ثانیه، ماکزیمم تعداد ارتباط‌ها یا تعداد بسته‌ها در ثانیه قابل انجام می‌باشند. همچنین ممکن است حمله‌کنندگان با استفاده از بسته‌های بدشکل یا دستکاریِ پروتکل‌ها، بتوانند روندِ پروتکل‌ها یا تجزیه‌ی بسته‌ها را هدف قرار دهند. بهترین تلاش‌های امنیتی، متناسب با طبیعتِ هر دستگاهِ in-line متفاوت است.

سرویس به عنوان هدف:

ارتباطات شبکه وابسته به مجموعه‌ای از سرویس‌ها از جمله DNS[۱]، NTP[۲] و DHCP است. قطع چنین سرویس‌هایی ممکن است باعث شود همه یا بخشی از اتصالات از دست برود و دستکاری آن‌ها می‌تواند منجر به ایجاد بستری برای دزدی اطلاعات، حمله‌ی DoS[۳]، سوءاستفاده از سرویس و فعالیت‌های مخرب دیگر شود. در نتیجه، حملات متنوع و متعددی دائماً سرویس‌های زیرساخت را هدف قرار داده‌اند.

DNS یک تناظر بین نام‌های دامنه و آدرس‌های IP برقرار می‌کند. از آنجا که اغلب سرویس‌ها در اینترنت و اینترانت‌ها به وسیله‌ی نام دامنه و نه آدرس IP مورد دسترسی قرار می‌گیرند، خرابیِ DNS به احتمال زیاد منجر به قطع ارتباطات می‌شود. حملات DNS ممکن است سرورهای نام و یا همچنین کلاینت‌ها (که اینجا با نام resolver نیز شناخته می‌شوند) را مورد هدف قرار دهد. بعضی از حملات رایج عبارتند از DNS amplification attack، DNS cache poisoning و domain name hijacking. حمله‌ی DNS amplification attack معمولاً به این صورت است که سرورِ نام را با پاسخ‌های ناخواسته غرق می‌کند (معمولاً در پاسخ به استعلام‌های مجعول بازگشتی). DNS cache poisoning بدین شکل است که حمله‌گر cache سرور را تغییر داده یا مدخلی به آن اضافه می‌کند تا بتواند به حملاتی همچون man-in-the-middle و یا فیشینگ دست بزند. domain name hijacking اشاره دارد به عمل غیرقانونیِ شخصی که کنترلِ سرورِ نام را از صاحب قانونی آن می‌رباید.

---

[۱] Domain Name System

[۲] Network Time Protocol

[۳] Denial of Service

بهترین تلاش‌ها برای برطرف کردنِ این حملات عبارتند از مدیریت وصله[۱]، مقاوم‌سازیِ سرورهای DNS، استفاده از فایروال برای کنترلِ استعلام‌های DNS و ترافیک‌های منطقه‌ای، پیاده‌سازیِ سیستم‌های پیشگیری از نفوذ به منظور شناسایی و بلاک کردن حملات مبتنی بر DNS و... .

NTP که برای هم‌زمان‌سازیِ سیستم‌های رایانه‌ای روی شبکه‌ی IP استفاده می‌شود، در اپلیکیشن‌هایی مانند احراز هویت کاربر[۲]، ثبت رویداد[۳] و برنامه‌ریزیِ پروسس‌ها[۴] و ... استفاده می‌شود که بر مبنای زمان کار می‌کنند. سرویسِ NTP توسط انواع مختلفی از حملات مانند rogue serverها که اطلاعات نامعتبرِ NTP را نشر می‌دهند و یا حملات DoS به سرورهای NTP تهدید می‌شود. بهترین تلاش‌ها برای امن کردنِ NTP عبارت است از NTP peer authentication، استفاده از لیست های کنترل دسترسی، مقاوم‌سازیِ تجهیزات و... .

DHCP پراستفاده‌ترین پروتکل به منظور پیکربندی پویای سیستم‌ها در یک شبکه‌ی IP می‌باشد. دو عدد از رایج‌ترین حملات DHCP عبارتند از اضافه کردن rogue DHCP server و DHCP starvation. حمله‌ی rogue DHCP server کاربران معتبر را به وسیله‌ی اطلاعاتِ نادرستِ پیکربندی به اشتباه انداخته و از دسترسیِ آن‌ها به شبکه جلوگیری می‌کند. همچنین از این حمله می‌توان برای انجام حملاتِ man-in-the-middle استفاده کرد که در آن IP مربوط به یک سیستمِ تسخیرشده به عنوان default gateway به کلاینت‌های معتبر شناسانده می‌شود. starvation DHCP نوع رایج دیگری از حملات است که در واقع اشغال کردنِ آدرس‌های IP موجود در DHCP server برای یک بازه‌ی زمانی بوده که با روشِ همه‌پخشیِ DHCP requestهای جعلی به دستِ یک یا چند سیستمِ تسخیرشده انجام می‌پذیرد. بهترین تلاش‌ها برای امن کردنِ DHCP عبارت است از مقاوم‌سازیِ سرور و همچنین استفاده از قابلیت‌های امنیتیِ موجود در سوئیچ‌ها مثل DHCP snooping، برقرای امنیت پورت‌ها و... .

نقاط پایانی به عنوان هدف:

---

[۱] Patch management

[۲] User authentication

[۳] Event logging

[۴] Process scheduling

نقطه‌ی پایانی، سیستمی است که به شبکه وصل شده و با موجودیت‌های دیگر در زیرساخت ارتباط برقرار می‌کند. سرورها، کامپیوترهای دسکتاپ، لپ‌تاپ‌ها، سیستم‌های ذخیره‌سازی شبکه، IP phoneها، تجهیزات موبایل با قابلیت اتصال به اینترنت و سیستم‌های ویدیوییِ برمبنای IP، همگی مثال‌هایی از نقاط پایانی هستند. به دلیل تفاوتِ بسیار زیادِ نقاط پایانی از لحاظِ بسترهای سخت‌افزاری، سیستم‌های عامل و اپلیکیشن‌ها، آن‌ها در معرضِ دشوارترین چالش‌های امنیتی قرار دارند. آپدیت‌ها، پچ‌ها و اصلاحیه‌ها برای مؤلفه‌های مختلفِ نقاط پایانی، از منابع متفاوت و در زمان‌های مختلف ارائه می‌شوند. این امر باعث می‌شود آپدیت نگه داشتنِ سیستم دشوارتر گردد. علاوه بر تنوع در نرم‌افزارها و بسترها، سیستم‌های قابل حمل مانند لپ‌تاپ‌ها و دستگاه‌های موبایل نیز معمولاً از hot-spotهای وای‌فای، هتل‌ها، خانه‌های کارمندان و سایر محیط‌ها که خارج از کنترل شرکت هستند استفاده می‌کنند. به دلیل چالش‌های امنیتیِ ذکر شده، نقاط پایانی آسیب‌پذیرترینِ دستگاه‌ها هستند و بیش از سایر تجهیزات در معرض تسخیر قرار دارند.

از آنجا که نرم‌افزارها و بسترها در نقاط پایانی متنوع هستند، خطرهای تهدیدکننده‌ی آن‌ها نیز گسترده و متنوع می‌باشند. بدافزارها، کرم‌ها، بات‌نِت‌ها و اسپم‌های ایمیلی، همگی مثال‌هایی از تهدیدات رایج برای نقاط پایانی هستند. بدافزارها نرم‌افزارهای مخربی هستند که به منظور دسترسی غیرمجاز و یا دزدی اطلاعاتِ قربانی طراحی می‌شوند. بدافزارها معمولاً به وسیله‌ی ایمیل‌های حاوی تروجان و یا با مرورِ وب‌سایت‌های آلوده انتشار می‌یابند. key-loggerها و همچنین جاسوس‌افزار مثال‌هایی از بدافزارها هستند که به منظور ضبط کردنِ رفتارِ کاربر و دزدیدن اطلاعاتِ شخصیِ وی مانند اطلاعاتِ کارت‌های اعتباری طراحی شده‌اند. کرم‌ها فرم دیگری از نرم‌افزارهای مخرب هستند که قادرند به صورت اتوماتیک در شبکه منتشر شوند. بات‌نت ها یکی از در حال رشدترین اَشکالِ نرم افزارهای مخرب هستند که می‌توانند با ایمیل‌های اسپم، حمله‌ی DoS در وب‌سرورها و سایر فعالیت‌های مخرب، تعداد زیادی از سیستم ها را در معرض خطر قرار دهند. ایمیل‌های اسپم در واقع ایمیل‌های ناخواسته‌ای هستند که اغلب شامل بدافزارها بوده و یا در جهت کلاهبرداریِ فیشینگ فعالیت می‌کنند.

امن‌سازیِ نقاط پایانی نیازمند توجه زیاد به هریک از مؤلفه‌ها در سیستم و همچنین آگاهی دادن به کاربرانِ آن‌ها می‌باشد. بهترین تلاش‌ها شامل به روز رسانیِ نقاط پایانی به وسیله‌ی آپدیت، پچ و اصلاحیه، مقاوم‌سازی کردن سیستم عامل و اپلیکیشن‌ها، توسعه‌ی نرم‌افزارهای امنیتی در نقاط پایانی، ایمن کردنِ ترافیکِ وب و ایمیل و همینطور آموزش دادنِ پیوسته‌ی کاربران درباره‌ی تهدیدات و روش‌های امنیتی می‌باشد.

شبکه‌ها به عنوان هدف:

تمامیِ قسمت‌های شبکه ممکن است در معرض حمله‌هایی مانند دزدیِ سرویس، سوء استفاده از سرویس، DoS، MITM و از دست رفتن اطلاعات قرار گیرند. دزدیِ سرویس به دسترسی غیرمجاز به سرویس‌ها و استفاده از منابع شبکه اشاره دارد (مثلاً استفاده از access point بی‌سیم به دست کاربری غیرمجاز). سوء استفاده از سرویسِ شبکه برای سازمان‌ها سالانه میلیون‌ها دلار خسارت در بر دارد و به معنیِ استفاده از منابع شبکه برای اهدافی غیر از اهداف تعیین شده می‌باشد (مثل استفاده‌ی شخصی کارمندان از منابع شبکه‌ی سازمان). همچنین شبکه‌ها در معرض حملاتِ DoS که به قصد مختل کردن سرویس‌های شبکه و حملاتِ MITM که به قصد دزدیِ اطلاعات شخصی انجام می‌پذیرند نیز قرار دارند.

حملات شبکه از جمله دشوارترین مسائلی است که با آن سروکار داریم، چرا که آن‌ها از برخی ویژگی‌های ذاتی شبکه به منظور حمله بهره می‌برند. حملات شبکه ممکن است در لایه‌ی دو یا لایه‌ی سه اتفاق بیافتد. حملات لایه‌ی دو اغلب از طبیعتِ خوش‌بینانه‌ی پروتکل‌های لایه‌ی دو مثل STP، ARP و CDP[1] استفاده می‌کنند. بعضی از حملات دیگرِ لایه‌ی دو نیز ویژگی‌های منحصر به فردِ برخی ابزارهای انتقال (همانند دسترسی بی‌سیم) را هدف قرار می‌دهند.

حملاتی که مبتنی بر لایه‌ی سه هستند، از پروتکلِ IP استفاده می‌کنند و ممکن است دستکاری‌هایی در پروتکل‌های مسیریابی انجام دهند. حملاتِ DDoS[2] و black-holing و انحرافِ ترافیک مثال‌هایی از این نوع حملات هستند. حمله‌ی DDoS ده‌ها یا هزاران ماشین را وادار می‌کند تا اطلاعاتی قلابی به آدرس IP هدف ارسال کنند. هدف چنین حملاتی نه لزوماً از کار انداختنِ یک هاستِ مشخص، بلکه مختل کردنِ پاسخگوییِ شبکه می‌باشد.

یکی از حملاتِ متداولِ دیگر در لایه‌ی سه، وارد کردن اطلاعات غلطِ مسیریابی به فرآیندِ مسیریابی است تا ترافیک را به سمت یک شبکه‌ی دیگر منحرف کنند. ترافیک ممکن است به سمتِ black-hole منحرف شود (که باعث می‌شود شبکه‌ی شنودکننده قابل دسترسی نباشد) و یا برای یک سیستم که به عنوان MITM عمل

[1] Cisco Discovery Protocol

[2] Distributed DoS

می‌کند ارسال شود. بهترین تلاش‌های امنیتی در برابر حملات لایه‌ی سه‌ی شبکه شامل مقاوم‌سازی تجهیزات، فیلترهای anti-spoofing، امن کردن پروتکل‌های مسیریابی، مسافت‌سنجیِ شبکه، فایروال‌ها و سیستم‌های جلوگیری از نفوذ می‌باشد.

اپلیکیشن‌ها به عنوان هدف:

اپلیکیشن‌ها به وسیله‌ی افراد متعدد نوشته شده‌اند لذا در معرض خطاهای زیادی قرار دارند. لازم است از آپدیت بودنِ دامنه‌های تجاری و عمومی با آخرین اصلاحیه‌های امنیتی اطمینان حاصل شود. اپلیکیشن‌های عمومی و همچنین سفارشی نیازمند بازبینیِ کد هستند تا خطرات امنیتیِ ناشی از برنامه‌نویسیِ ضعیف در آن‌ها بررسی شود. این بازبینی‌ها شامل بررسیِ اصولی بودنِ ورودی‌های کاربر، نحوه‌ی صدا زدنِ اپلیکیشنی دیگر یا سیستم عامل توسط یک اپلیکیشن، سطح دسترسی‌ای که اپلیکیشن در آن اجرا می‌شود، میزان اعتمادی که اپلیکیشن به سیستم‌های اطراف خود دارد و شیوه‌ای که اپلیکیشن به منظور انتقال اطلاعات در شبکه استفاده می‌کند می‌باشد.

برنامه‌نویسی ضعیف می‌تواند منجر به سرریز بافر، افزایشِ سطح دسترسی، حدس زدنِ اطلاعاتِ session، تزریقِ SQL و حملاتِ cross-site scripting شود. حملات سرریز بافر می‌تواند موجب ایجادِ exception در اپلیکیشن شده که بخش خاصی از حافظه را بازنویسی کرده و موجبِ DoS می‌شود و یا امکان اجرای یک فرمانِ غیرمجاز را فراهم می‌کند. افزایشِ سطح دسترسی معمولاً به خاطر ضعف در اعمال کنترل های مجوز[1] به وجود می‌آید. استفاده از اعتبار کاربرانِ قابلِ پیش‌بینی یا اطلاعاتِ شناساییِ session به ربوده شدنِ session و حملاتِ جعلِ هویت کمک می‌کند. تزریقِ SQL یک حمله‌ی رایج در محیط وب است و در مواقعی که ورودی کاربر به طور مناسب سلامت‌سنجی نمی‌گردد، امکان وقوع آن وجود دارد. این حمله با دستکاری داده‌های ورودی می‌تواند منجر به اجرای یک دستورِ SQL توسط حمله‌کننده شود. حمله‌ی cross-site scripting نوع دیگری از حمله است که شامل تزریق کدهای خرابکاری در وب‌سایت‌ها می‌شود و این کدها توسط سایر کاربرانی که سایت را مرور می‌کنند اجرا می‌شود. این نوع از حملات در وب‌سایت‌هایی امکان‌پذیر است که کاربران بتوانند محتواهایی را در وب‌سایت قرار دهند و این محتواها به شکل مناسبی اعتبارسنجی نشوند.

[1] Authorization control

محیط اپلیکیشن‌ها می‌تواند با استفاده از نرم‌افزارهای امنیتی در نقاط پایانی و همینطور مقاوم‌سازیِ سیستم‌عامل امن گردد. همچنین فایروال‌ها، سیستم‌های جلوگیری از نفوذ و دروازه‌های XML نیز می‌توانند برای برطرف کردنِ حملاتِ مبتنی بر اپلیکیشن مؤثر واقع گردند.

الگوهای طراحیِ SAFE[1]

طراحی‌های Cisco SAFE از قواعدِ تعیین‌شده‌ی این معماری پیروی می‌کند و با اصول امنیتی در SAFE سازگار است. با توجه به حملات پیچیده‌ی روز افزون، راه‌حل‌های امنیتیِ تک‌نقطه‌ای دیگر موثر نیستند. محیط‌های کنونی نیازمند میزان بالایی از شفافیت بوده که تنها با آگاهی و همکاریِ وسیع در کلِ زیرساخت به‌دست می‌آید. بدین منظور، الگوهای طراحیِ Cisco SAFE از فرم‌های مختلفِ مسافت‌سنجی در شبکه که در تجهیزات شبکه‌ی سیسکو، دستگاه‌های امنیتی و نقاط پایانی موجود است استفاده کرده تا به دیدی دقیق از فعالیت‌های شبکه دست پیدا کنند. رویدادها و وقایعِ ثبت‌شده توسط روترها، سوئیچ‌ها، فایروال‌ها، سیستم‌های جلوگیری از نفوذ و نرم‌افزارهای حفاظتی در نقاط پایانی، به عنوان بخشی از مانیتورینگ و آنالیز و همبسته‌سازیِ اتفاقات، جمع‌آوری و هدایت و همبسته‌سازی می‌شود.

SCF شش عمل امنیتی را تعریف کرده که موجب اعمال سیاست‌های امنیتی و بهبودِ شفافیت و کنترل می‌شود. شفافیت به وسیله‌ی عمل‌های تشخیص، مانیتور و همبسته‌سازی افزایش می‌یابد. با فراهم‌آوردنِ همکاری و هوشمندیِ امنیتی در ابعادِ کلِ زیرساخت، الگوهای طراحیِ Cisco SAFE می‌تواند به طور موثر موارد زیر را ارائه کند:

- افزایش شفافیت: هوشمندی در ابعاد کلِ شبکه، تصویر دقیقی از توپولوژی‌های شبکه، مسیرهای حمله و میزان آسیب فراهم می‌کند.
- شناسایی تهدیدها: جمع‌آوری، هدایت، همبسته‌سازی و ثبتِ اطلاعاتِ رویدادها به شناسایی وجود تهدیدات امنیتی، تسخیرها و نشت اطلاعات کمک می‌کند.
- تایید تسخیر: این ساختار با استفاده از توانایی دنبال کردنِ حملات در حین گذر از شبکه و همچنین با استفاده از شفافیت در نقاط پایانی، می‌تواند موفقیت یا شکستِ یک حمله را تایید کند.
- کم کردنِ false positiveها: شفافیت در سیستم و نقاط پایانی، به تشخیصِ آسیب‌پذیر بودنِ یک هدف در برابر حمله‌ای مشخص کمک می‌کند.

[1] SAFE design blueprint

- کم کردن حجم اطلاعات رویداد: همبسته‌سازی رویدادها به طور چشمگیری تعداد آن‌ها را کاهش داده، در زمانِ با ارزشِ اپراتورهای امنیت صرفه‌جویی کرده و به آن‌ها اجازه می‌دهد بر روی پردازش‌های مهم‌تر تمرکز کنند.
- تشخیص شدت یک حادثه: افزایش شفافیت در شبکه و نقاط پایانی به معماری اجازه می‌دهد تا به طور پویا درجه‌ی شدتِ یک حمله را براساس درجه‌ی آسیب‌پذیری هدف و شرایطِ حمله تعیین کند.
- کم کردنِ زمان پاسخ: وجود شفافیت نسبت به کلِ شبکه، امکان تخمین زدن مسیر حمله و همچنین مشخص کردن بهترین مکان‌ها برای خنثی‌سازی حمله را میسر می‌سازد.

Cisco SAFE از قابلیت‌های همکاری و هوشیاری در سطح کلِ زیرساخت استفاده می‌کند که به وسیله‌ی محصولات سیسکو به منظور کنترل و مقابله با حمله‌های شناخته‌شده و یا حمله‌های zero-day فراهم شده است. سیستم‌های حفاظت از نفوذ، فایروال‌ها، کنترل‌های ورود به شبکه، نرم‌افزارهای محافظت از نقاط پایانی و سیستم‌های آنالیز و مانیتورینگ، تحت الگوهای امنیتیِ Cisco SAFE با یکدیگر فعالیت کرده تا به صورت پویا حملات را شناسایی کرده و به آن‌ها پاسخ دهند. طراحی‌های انجام شده، به عنوان بخشی از کنترل و مهار تهدیدات، توانایی شناسایی منبع تهدیدات، تشخیصِ مسیر حمله، پیشنهاد دادن و حتی پاسخ دادن به صورت پویا را دارند. پاسخ‌های ممکن می‌تواند شامل ایزوله‌سازیِ سیستم‌های تسخیرشده، محدودسازیِ سرعت، فیلتر کردنِ بسته‌ها و... باشد.

کنترل، به وسیله‌ی روش‌هایی همچون مقاوم‌سازی، ایزوله‌سازی و تحمیل بهبود می‌یابد. در ادامه به تعدادی از اهداف الگوهای طراحیِ Cisco SAFE اشاره شده است:

- پاسخِ تطبیق‌پذیر به تهدیدات بلادرنگ[1]: تهدیداتِ منبع به طور پویا شناسایی شده و ممکن است به شکل بلادرنگ بلاک شوند.
- پوشش پایدارِ سیاست‌های تحمیل: عمل‌های مهار و رفع‌سازی ممکن است در مکان‌های مختلفِ شبکه برای دفاع در عمق اعمال شود.
- کمینه کردن تأثیر حمله: عملیات پاسخ‌دهی باید به صورت پویا و به محض اینکه حمله شناسایی شد اتفاق بیفتد تا موجب کمینه شدنِ آسیب گردد.

[1] Real-time

- مدیریت امنیت و سیاست‌های رایج: بسترِ مدیریت امنیت و سیاست‌های رایج، موجب آسان‌تر شدنِ مدیریت و کنترل گردیده و هزینه‌های عملیاتی را کاهش می‌دهد.

شبکه‌های سازمانی متشکل از روترها، سوئیچ‌ها و دستگاه‌های دیگرِ شبکه هستند که اجرای اپلیکیشن‌ها و سرویس‌ها را میسر می‌سازند. لذا امن‌سازیِ مناسبِ این تجهیزات برای عملیات‌های مربوط به کسب و کارهای دنباله‌دار ضروری است. زیرساختِ شبکه نه تنها به عنوانِ بستری برای حمله به سایر اهداف، بلکه بعضاً به عنوان هدف مستقیمِ فعالیت‌های مخرب نیز مورد هدف قرار می‌گیرند. به همین دلیل لازم است اقدامات مناسب برای اطمینان از امنیت، اطمینان‌پذیری[1] و دسترسی‌پذیریِ زیرساختِ شبکه انجام گردد. Cisco SAFE طراحی‌ای پیشنهادی به منظور بالابردن امنیت و همچنین بهترین تلاش‌هایی به منظور بهبود سطح کنترل و مدیریتِ زیرساختِ شبکه فراهم آورده است. این معماری، زیربنایی قوی فراهم کرده که تکنیک‌ها و متدهای پیشرفته‌تر نیز می‌توانند متعاقباً برپایه‌ی آن ساخته شوند.

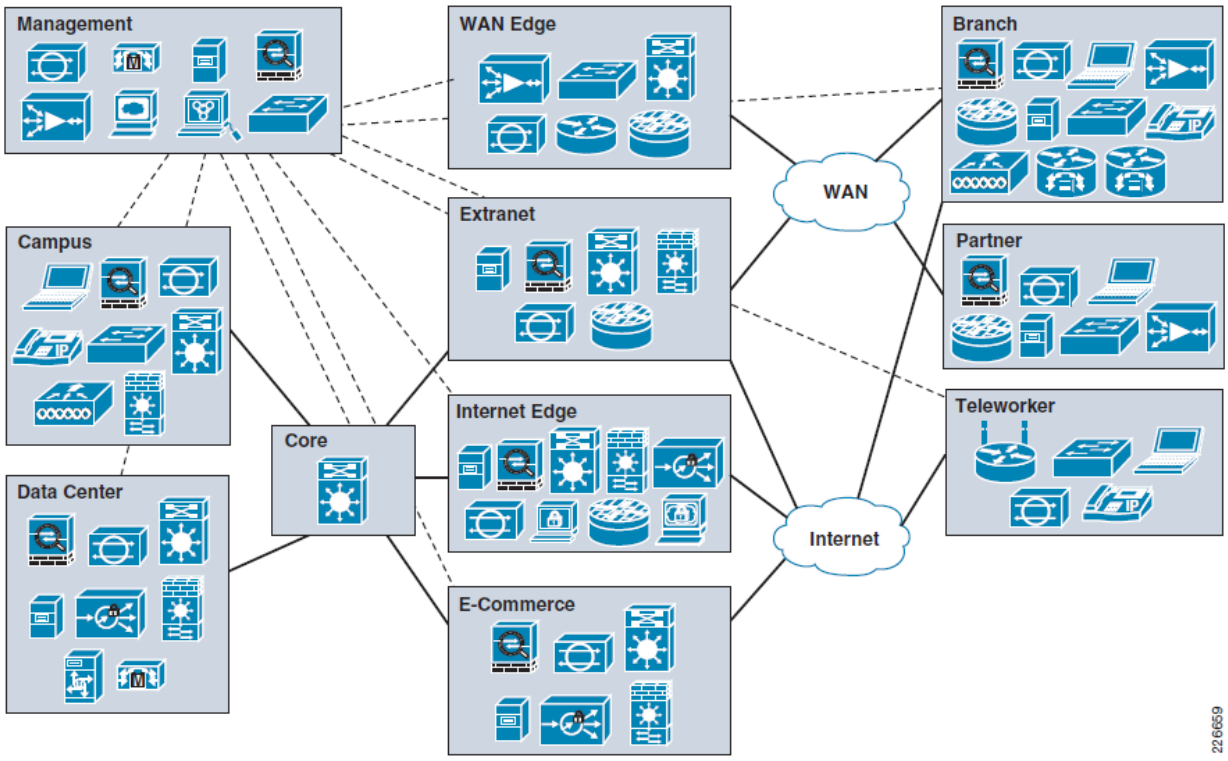
بهترین تلاش‌ها و پیشنهادات طراحی در زمینه‌های زیر ارائه شده‌اند:

- دسترسی به تجهیزات شبکه
- انعطاف‌پذیری و ابقاءپذیریِ تجهیزات
- زیرساخت مسیریابی
- زیرساخت سوئیچینگ
- اجرای سیاست‌های شبکه
- مسافت‌سنجی شبکه
- مدیریت شبکه

الگوهای طراحی، از یک طراحیِ ماژولار تبعیت می‌کنند که در آن زیرساختِ کلیِ شبکه به ماژول‌های عملکردی تقسیم شده‌اند که هریک، نشانگرِ یک PIN متمایز است. ماژول‌های عملکردی سپس به لایه‌ها و بلوک‌های عملکردیِ کوچک‌تر و مدیریت‌پذیرتری تقسیم می‌شوند که هر یک نقشی خاص را در شبکه ایفا می‌کنند. شکل ۲ الگوی طراحیِ Cisco SAFE را نشان می‌دهد.

[1] reliability

هر ماژول، با هدفِ فراهم‌سازیِ سرویس‌های در دسترس و منعطف، کمک به پیروی از مقررات، انعطاف‌پذیری در جای دادن سرویس‌های جدید، انطباق پذیری با زمان و همچنین تسهیل مدیریت طراحی شده است.



شکل ۲. الگوی طراحیِ Cisco SAFE

در این قسمت توصیف مختصری از ماژول‌های طراحی ارائه می‌گردد. هر ماژول در فصل‌های بعدی با جزئیات بیشتر شرح داده می‌شود.

هسته‌ی سازمان (Core)

هسته، بخشی از زیربنا بوده که ماژول های دیگر را به هم متصل می‌کند. هسته در واقع یک زیرساختِ پرسرعت بوده که هدف آن فراهم کردن یک انتقالِ قابل اطمینان و مقیاس‌پذیر[۱] در لایه‌ی دو و لایه‌ی سه می‌باشد. در

[۱] scalable

هسته معمولاً سوئیچ‌های فراوانی تعبیه شده که ارتباطات را به سمتِ پردیس‌ها، دیتاسنترها، لبه‌ی WAN و لبه‌ی اینترنت تجمیع می‌کند.

دیتاسنترِ اینترانت

Cisco SAFE شامل یک طراحیِ دیتاسنترِ اینترانت است که توانایی میزبانی از تعداد زیادی سیستم‌ها به منظور خدمت به اپلیکیشن‌ها و ذخیره‌سازیِ حجم قابل توجهی از داده را دارا می‌باشد. همچنین طراحی دیتاسنتر، زیرساخت‌های شبکه که از اپلیکیشن‌ها پشتیبانی می‌کنند را هم میزبانی می‌کند (همچون سوئیچ‌ها، روترها، متعادل‌کننده‌های بار و تجهیزاتِ تسریعِ اپلیکیشن). دیتاسنترِ اینترانت به منظور خدمت به کاربران و اپلیکیشن‌های داخلی طراحی شده و مستقیماً از اینترنت برای عموم قابل دسترس نیست.

در ادامه بعضی از ویژگی‌های کلیدیِ طراحیِ دیتاسنترِ اینترانت در Cisco SAFE آورده شده است:

- دسترسی‌پذیری و انعطاف‌پذیریِ سرویس‌ها
- جلوگیری از DoS، سوء استفاده از شبکه، نفوذ، نشت اطلاعات و کلاه برداری
- اطمینان از محرمانگی، صحت و دسترسی‌پذیریِ داده‌ها
- کنترلِ محتوا و بازرسی در سطح اپلیکیشن
- محافظت و دسته‌بندیِ[1] سرور و اپلیکیشن

پردیسِ سازمان (campus)

پردیسِ سازمان، دسترسی به شبکه را برای کاربران و تجهیزاتی که در یک محدوده‌ی جغرافیایی واحد قرار دارند فراهم می‌کند (این محدوده ممکن است چند طبقه از یک ساختمان یا چندین ساختمان در یک محدوده باشد). پردیس همچنین ممکن است سرویس‌های محلیِ داده، صدا و و ویدیویی را میزبانی کند. Cisco SAFE شامل یک طراحیِ پردیس است که به کاربرانِ خود اجازه می‌دهد تا به طور ایمن از طریق زیرساختِ پردیس به منابع اینترنت یا شرکت دسترسی داشته باشند.

[1] segmentation

از نقطه نظر امنیت، ویژگی‌های کلیدیِ طراحیِ پردیس در Cisco SAFE بدین شرح است:

- دسترسی‌پذیری و انعطاف‌پذیریِ سرویس‌ها
- جلوگیری از دسترسی غیرمجاز، سوء استفاده از شبکه، نفوذ، نشت اطلاعات و کلاه برداری
- اطمینان از محرمانگی، صحت و دسترسی‌پذیریِ داده‌ها
- اطمینان از دسته‌بندیِ کاربران
- تحمیلِ کنترلِ دسترسی
- حفاظت از نقاط پایانی

لبه‌ی اینترنتِ در سازمان (Internet Edge)

لبه‌ی اینترنت، زیرساختی است که اتصال به اینترنت را فراهم کرده و به عنوانِ دروازه‌ی سازمان به فضای مجازیِ خارج عمل می‌کند. این سرویس‌ها شامل سرویس‌های عمومیِ DMZ[1]، دسترسیِ سازمانی به اینترنت و دسترسیِ از راه دورِ VPN است. الگوی طراحیِ Cisco SAFE طراحی‌ای برای لبه‌ی اینترنت ارائه کرده که به کاربرانِ پردیس‌ها امکان دسترسیِ امن به ایمیل، پیام‌رسانِ فوری، وب‌گردی و سایر سرویس‌های رایج را فراهم می‌سازد. در ادامه تعدادی از ویژگی‌های کلیدیِ لبه‌ی اینترنت در Cisco SAFE آورده شده است:

- دسترسی‌پذیری و انعطاف‌پذیریِ سرویس‌ها
- جلوگیری از نفوذ، DoS، نشت اطلاعات و کلاه برداری
- اطمینان از محرمانگی، صحتِ داده و دسترسی‌پذیریِ کاربر
- حفاظت از سرور و اپلیکیشن
- دسته‌بندیِ سرور و اپلیکیشن
- اطمینان از دسته‌بندی کاربران
- کنترل محتوا و بازرسی

لبه‌ی WAN در سازمان

لبه‌ی WAN بخشی از زیرساختِ شبکه است که لینک‌های WAN که دفاتر دور از هم را به یکدیگر متصل کرده‌اند را به یک سایتِ مرکزی یا سایتِ هابِ منطقه‌ای متصل می‌کند. WAN می‌تواند متعلق به همان سازمان

[1] Demilitarized Zone

باشد یا توسط یک ارائه‌دهنده‌ی سرویس[1] فراهم شود، که البته روش دوم رایج‌تر است. هدف WAN این است که برای کاربرانی که در شاخه‌ها قرار دارند، سرویسی هم‌طراز با کاربرانِ پردیس که در سایت مرکزی هستند فراهم سازد. Cisco SAFE شامل یک طراحیِ لبه‌ی WAN است که به شاخه‌ها و دفاتر دوردست اجازه می‌دهد به شکلی امن تحتِ یک WAN خصوصی با یکدیگر مرتبط گردند. این طراحی همچنین چندین WAN cloud را برای اهداف افزونگی و تعادلِ بار پیاده‌سازی کرده است. به علاوه، می‌توان از یک ارتباط اینترنتی نیز به عنوان پشتیبانِ ثانویه استفاده نمود.

از نقطه نظر امنیت، در ادامه تعدادی از خصوصیات کلیدیِ طراحی لبه‌ی WAN در Cisco SAFE بیان شده است:

- دسترسی‌پذیری و انعطاف‌پذیریِ سرویس‌ها
- جلوگیری از DoS، سوء استفاده از شبکه، نفوذ، نشت اطلاعات و کلاه برداری
- فراهم کردن محرمانگی ، صحت و دسترسی‌پذیریِ داده‌های گذرکننده از WAN
- ارائه‌ی پشتیبانِ امنِ اینترنتی برای WAN
- اطمینان از محرمانگی، صحت و دسترسی‌پذیریِ داده‌ها
- اطمینان از دسته‌بندی کاربران

شاخه‌های سازمان

شاخه‌ها ارتباط کاربران و تجهیزاتِ دور از هم را میسر می‌کنند. آن‌ها معمولاً متشکل از یک یا چند LAN بوده و از طریقِ یک WAN خصوصی یا یک ارتباط اینترنتی به سایت‌های مرکزی متصل می‌شوند. شاخه‌ها همچنین ممکن است از سرویس‌های محلیِ داده، صوتی و ویدیویی نیز میزبانی کنند. Cisco SAFE شامل چندین طراحیِ شاخه است که به کاربران و تجهیزات اجازه می‌دهد به صورت امن به منابع موجود در شاخه دسترسی پیدا کنند. طراحیِ شاخه در Cisco SAFE، یک یا دو WAN cloud و همینطور یک ارتباط اینترنتیِ پشتیبان را در خود جای داده است. مطابق با سیاست‌های دسترسی در سازمان، امکان دسترسیِ مستقیم به اینترنت می‌تواند مجاز باشد و یا اینکه دسترسی به اینترنت فقط از طریق اتصال مرکزی در مراکز فرمان‌دهی یا دفاتر

[1] service provider

محلی اجازه داده شود. در حالت دوم، لینک اینترنت در شاخه احتمالاً تنها به عنوان پشتیبانِ WAN مورد استفاده قرار می‌گیرد.

خصوصیات کلیدیِ امنیتی در طراحیِ شاخه در Cisco SAFE در ادامه آمده است:

- دسترسی‌پذیری و انعطاف‌پذیریِ سرویس‌ها
- جلوگیری از دسترسی غیرمجاز، سوء استفاده از شبکه، نفوذ، نشت اطلاعات و کلاه برداری
- فراهم کردن محرمانگی، صحت و دسترسی‌پذیریِ داده‌های گذرکننده از WAN
- اطمینان از محرمانگی، صحت و دسترسی‌پذیریِ داده‌ها
- اطمینان از دسته‌بندی کاربران
- حفاظت از نقاط پایانی

مدیریت

این معماری، شامل یک مدیریتِ شبکه است که به منظور انتقال ترافیکِ مربوط به plane کنترل و مدیریت همچون NTP، SSH، SNMP، syslog و ... در نظر گرفته شده است. مدیریت شبکه، مدیریت‌های OOB[۱] و همینطور IB[۲] را در گستره‌ی تمامی بلوک‌های سازنده با یکدیگر ترکیب می‌کند. در مراکز فرمان‌دهی، یک شبکه‌ی مدیریتِ OOB می‌تواند به شکل مجموعه‌ای از سوئیچ‌ها و یا برمبنای VLAN بندی پیاده‌سازی گردد.

[۱] out-of-band

[۲] in-band