باسمه تعالی

مستند مرجع طراحی امن شبکه

(فصل سوم: شبکه Core)

مقدمه

Core بخشی از زیرساخت شبکه است که سایر ماژول‌ها را به یکدیگر مرتبط می‌کند. این ماژول یک زیرساخت پرسرعت را با هدف فراهم کردن انتقالات مقیاس پذیر و قابل اعتماد در لایه‌ی دو و لایه‌ی ۳ فراهم ساخته و ترافیک را با حداکثر سرعت ممکن از یک ماژول شبکه به ماژول دیگر مانند campus، data center، WAN edge و لبه اینترنت، مسیریابی و یا سوئیچ می‌کند.

هیچ‌گاه از شبکه Core انتظار فراهم‌سازی سرویس برای کاربران نهایی نمی‌رود بلکه در واقع ماژول‌های دیگر شبکه را قادر می‌سازد تا این سرویس‌ها را فراهم نمایند. مقصد اصلی ترافیک‌های ip هیچگاه زیرساخت شبکه core نیست و فقط ترافیک‌های مدیریتی و کنترلی که به وسیله عناصر دیگر شبکه یا station های مدیریتی در همان دامنه مدیریتی تولید شده‌اند به سوی زیرساخت core روانه می‌شوند.

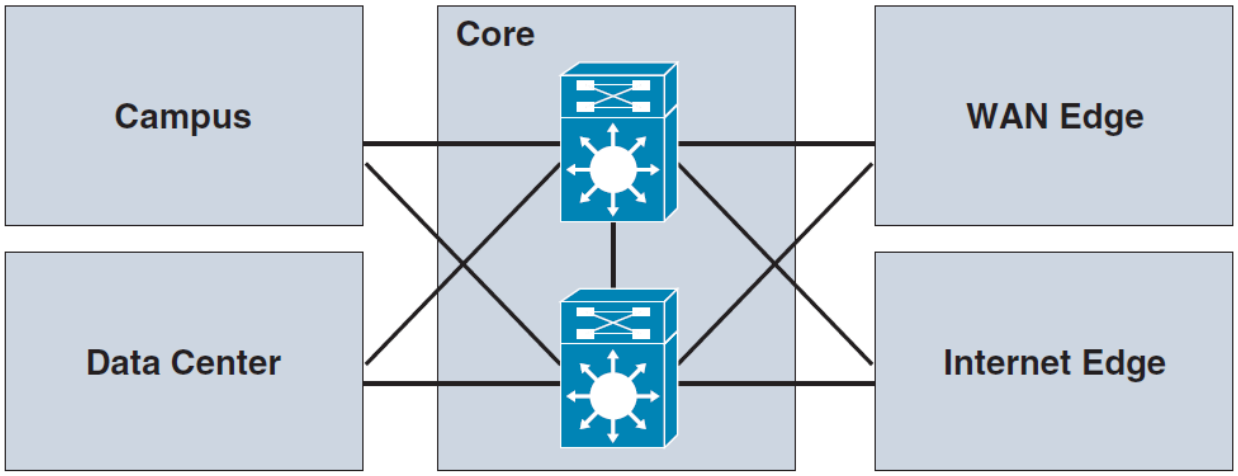
تهدیدات کلیدی در core

در ادامه، تعدادی از تهدیداتی که ممکن است شبکه core یک سازمان را تحت تاثیر قرار دهد آمده است:

- قطع سرویس: حملات DOS و DDOS در زیرساخت
- دسترسی غیرمجاز: نفوذ، کاربران غیرمجاز، ارتقاء سطح دسترسی، دسترسی غیرمجاز به تجهیزاتی که دسترسی به آن ها محدود شده است و حملات مربوط به پروتکل‌های مسیریابی
- تغییر و افشای اطلاعات: شنود بسته‌ها و حملات Man-In-The-Middle به اطلاعاتی که در حال انتقال است.

طراحی core سازمان

ماژول core در معماری safe با ماژول core در معماری‌های دیگر شبکه تقریباً مشابه است. دستورالعمل‌های استاندارد توسعه با ساختار لایه‌ایی core، distribution و access در این ماژول نیز صادق است. این طراحی با سوئیچ‌های افزونه که connection ها را از جاهای مختلف شبکه مانند campus، data center، WAN edge و internet edge تجمیع می‌کند، توسعه می‌یابد (شکل ۱).



شکل ۱. enterprise core topology

دستورالعمل‌های طراحی برای core

نکته کلیدی در این بخش آن است که وقتی سخن از امنیت در ماژول های core می‌شود، منظور محافظت کردن از خود core است نه اعمال سیاست‌هایی برای مقابله با تهدیداتی که از طریق core انتقال می‌یابند. چنین تهدیداتی بایستی در edge شبکه یا campus و یا سایر ماژول‌های شبکه فیلتر شوند. از سوی دیگر سیاست‌های امنیتی edge شبکه اگر به درستی طراحی و اجرا گردد، مخاطرات امنیتی core را به شدت کاهش می‌دهد. اگرچه خطاهای انسانی، پیکربندی اشتباه، مدیریت تغییرات و گاهی موارد استثناء این الزام را ایجاد می‌نماید که بر اساس قواعد دفاع در عمق، مکانیزم‌های امنیتی برای core در نظر گرفته شود. حتی در صورتی که به صورت سهوی سیاست‌های امنیتی در edge دور زده شود، سیاست‌های امنیتی در core به ما در برطرف ساختن تهدیدات core یاری‌رسان خواهد بود.

امن‌سازی موثر در core نیازمند اجرای اقدامات امنیتی گوناگون در یک رویکرد لایه‌ای و تحت یک استراتژی خاص است. این اقدامات شامل امن‌سازی در edge و سایر ماژول‌های شبکه که به core متصل هستند و نیز امن‌سازی خود سوئیچ‌های core است. سوئیچ‌های core با پیروی از قواعد امنیت پایه زیرساخت[۱] که در فصل دوم توضیح داده شد امن می‌شوند. این امر شامل محدود ساختن و کنترل‌دسترسی به تجهیزات مدیریتی،

[۱] Infrastructure baseline security principles

امن‌سازی زیرساخت مسیریابی و حفاظت از سطوح مدیریت و کنترل (management plane و control plane) است. برای جزئیات بیشتر به فصل دوم مراجعه کنید.

تعدادی از best practice های امنیت پایه که برای محافظت از زیرساخت شبکه core مورد استفاده قرار می‌گیرد در ادامه لیست شده است:

- دسترسی به تجهیزات زیرساخت: توسعه اینترفیس‌های مدیریتی اختصاصی به شبکه مدیریت out-of-band (OOB)، محدودکردن پورت‌های دسترسی و communicator های مجاز و متدهای مجاز دسترسی، وجود بنرهای اطلاع رسانی حقوقی، احراز هویت و بررسی مجوز دسترسی و سیستم حسابرسی با استفاده از سیستم‌های AAA، ثبت وقایع و ردگیری و حسابرسی برای همه دسترسی‌ها و نیز حفاظت از اطلاعات حساس محلی در برابر دیده شدن و کپی شدن (مانند پسوردهای محلی).
- زیرساخت مسیریابی: احراز هویت همسایگان مسیریابی، فیلترکردن مسیر، فعال‌سازی default passive interface ها و ثبت کردن تغییرات همسایه.
- انعطاف‌پذیری و پایداری تجهیزات: غیرفعال کردن سرویس‌های غیرضروری، فیلتر کردن و محدودکردن سرعت ترافیک control-plane و ایجاد افزونگی
- Network telemetry : فعال‌سازی NTP بر روی تجهیزات به منظور همگام‌سازی زمان با ساعت همان شبکه، نگهداری آمار ترافیک اینترفیس‌ها و تجهیزات، نگهداری اطلاعات وضعیت سیستم (حافظه، CPU و process ها)

مقابله با تهدیدات در core

جدول زیر تهدیدات شبکه core و راه‌کارهای مقابله را نشان می‌دهد.

	DOS	DDOS	دسترسی غیرمجاز	نفوذ	حملات پروتکل مسیریابی	Botnets	visibility	control
افزونگی	✓	✓				✓	✓	✓
غیرفعال‌کردن سرویس‌های غیرضرور	✓	✓	✓	✓			✓	✓
سیاست پسورد قوی			✓	✓				✓
AAA			✓	✓			✓	✓
SSH			✓	✓				✓
احراز هویت SNMP			✓	✓			✓	✓
ACL	✓	✓	✓	✓			✓	✓
احراز هویت مسیریاب‌های همسایه	✓		✓		✓			✓
CoPP	✓	✓	✓	✓	✓	✓		✓
NetFlow, Syslog							✓	