فایرپاور سیسکو فایروال نسل جدید

فایروال های سخت افزاری که به آن ها فایروال های شبکه در تجهیزات شبکه نیز گفته می‌شود، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط DSL قرار خواهند گرفت. فایروال های سخت افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می‌نمایند. فایروال های سخت افزاری، دستگاه های سخت افزاری مجزائی می‌باشند که دارای سیستم عامل اختصاصی خود بوده بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می‌گردد.

تمام شبکه خود را در برابر تهدیدات به یک معماری امنیتی محافظت شده ، با کنترل های امنیتی در کلاس جهانی تبدیل کنید.

بیش از دو دهه ، این فایروال سنگ بنای استراتژی امنیت شبکه سازمان ها است.

فایر پاور بر اساس این تصور که ترافیک داخلی ، ترافیک خارجی و کاربران نیز ذاتاً قابل اعتماد نبودند ، بنابراین مرز اعتماد - یا محیطی - بین شبکه ها ایجاد شد.

این محیط شبکه به نقطه کنترل امنیتی منطقی برای حمایت از کل سازمان، شبکه ، داده ها ، کاربران و دستگاه ها تبدیل شد. همه ترافیک شبکه ، چه از مبدا دفتر مرکزی ، یک مرکز داده یا کارمند از راه دور ، از طریق این نقطه کنترل واحد عبور داده می‌شد.

بسیاری از برنامه های کاربردی مهم در تجارت از مراکز داده سیسکو و شبکه های ابری حرکت می‌کنند. شعب سیسکو اکنون به طور مستقیم به اینترنت وصل می‌شوند.

کاربران می‌توانند به منابع تجهیزات شخصی خود از همه جا دسترسی داشته باشند.

با این تحولات جدید نیاز است که به فایروال و امنیت شبکه با رویکردی جامع تر فکر کرد.

در سیسکو ، رهبری شبکه و فناوری امنیتی پیشرفته با هم جمع می‌شود تا معماری شبکه همیشه از امنیت بیشتری برخوردار شود

سیسکو روتر شما را به فایروال تبدیل می‌کند و نمی‌خواهد نوآوری را برای مشتریان متوقف شود زیرا (Next-Generation Firewall)Cisco NGFW امنیت شبکه ای است که برای شما طراحی شده است - از شرکتی که شبکه را ساخته است

توانایی ها

متوقف کردن تهدیدهای بیشتر

شامل بدافزارهای شناخته شده یا ناشناخته توسط ماژول حفاظت پیشرفته بدافزار سیسکو و سندباکسینگ(استراتژی مدیریت نرم افزار)

اولویت بندی تهدیدات:

با سیستم جلوگیری از نفوذ نسل جدید فایرپاور سیسکو دید برتر را به محیط کاری خود جلب کنید.(NGIPS)

رتبه بندی تهدیدات و شناسایی اطلاعات آسیب پذیر را الویت تیم خود قرار دهید.

زودتر تشخیص دهید ، سریعتر عمل کنید:

سیسکو تالوس پیشرو در صنعت تحقیقات اطلاعاتی تهدید

فایرپاور سیسکو فایروال نسل جدید

سیسکو تالوس سازمانی می‌باشد که نمونه کارهای NGFW سیسکو را ارائه می‌دهد

گروه اطلاعاتی تالوس سیسکو با پیدا کردن بدافزارهای جدید ، دامنه ها ، URL های مخرب همچنین ناشناس یا آسیب پذیری های کشف نشده و نوشتن قوانین به کاهش آنها کمک و از مشتریان دفاع می‌کند می‌کند.

این قوانین برای فراهم کردن امنیت پیشرفته در برابر تهدیدات پیچیده همچنین کمک به رعایت مقررات و الزامات در SNORT IPS of Cisco NGFW گنجانیده شده اند.

کنترل های امنیتی کلاس جهانی

وقت آن است که دوباره به فایروال فکر کنید. برای انجام این مهم، شما به رویکردی چابک و یکپارچه تر برای هماهنگی سیاست ها و اجرا به طور فزاینده بر روی شبکه های ناهمگن نیاز دارید

در سیسکو ، ساختن یک پلد فرم امنیتی که فقط با ارائه امنیت در کلاس جهانی کنترل می‌کند هرجایی که به آنها احتیاج دارید

مرکز مدیریت سیسکو فایر پاور

(Cisco FirePower Management Center)

مرکز مدیریت سیسکو FirePOWER بهره‌وری راهکارهای امنیتی مورد استفاده در شبکه را، از طریق مدیریت آسان، متمرکز و یکپارچه، ارتقا داده است.

مرکز مدیریت سیسکوFirePOWER که پیش‌تر با نام FireSIGHT Management Centerشناخته می‌شد یک مرکز مدیریت عصبی به منظور انتخاب و کنترل محصولات امنیتی سیسکو موجود در سیستم عامل‌های مختلف است، این مرکز مدیریت کامل و یکپارچه‌ای بر فایروال‌ها، کنترل برنامه‌ها، پیشگیری از نفوذ، فیلترینگ URL و Cisco Advanced Malware Protection (AMP) ، را ارائه می‌دهد. مرکز مدیریت، نقطه مرکزی مدیریت رخدادها و سیاست‌گذاری‌های راهکارهای امنیتی ذیل است:

NGFW

سرویس ASA with FirePOWER

NGIPS

سیسکو FirePOWER دفاع در برابر تهدیدات برای ISR

AMP

مرکز مدیریت سیسکو FirePOWER اطلاعات کاملی در ارتباط با کاربران، نرم‌افزارها، ابزارها، تهدیدات و نقاط ضعف موجود در شبکه فراهم می‌کند؛ از این اطلاعات به منظور تحلیل آسیب‌پذیرهای شبکه استفاده می‌کند؛ سپس به ارائه توصیه‌های مناسب در ارتباط با سیاست‌های امنیتی مورد نیاز برای شبکه و رخدادهای امنیتی که نیاز به بررسی و تحلیل دارند، می‌پردازد.

مرکز مدیریت یک واسط گرافیکی ساده برای اعمال سیاست‌گذاری-ها به منظور کنترل دسترسی و محافظت در برابر حملات ارائه می-دهد، که با AMP و تکنولوژی sandboxing ادغام شده و ابزاری مناسب جهت شناسایی و ردیابی بدافزارها در سراسر شبکه را فراهم کرده است. مرکز مدیریت تمامی‌این قابلیت‌ها را در یک ابزار به صورت

یک‌پارچه ارائه می‌دهد که به راحتی امکان مدیریت فایروال جهت کنترل نرم‌افزارها به منظور بررسی و بازسازی شبکه در هنگام وجود بدافزارها، را فراهم می‌کند.

مدیریت در کلاس تجاری

مرکز مدیریت سیسکو Firepower اطلاعات بی‌درنگی در ارتباط با تغییرات منابع و عملیات شبکه ارائه می‌دهد، که پایه کاملی برای تصمیم‌گیری‌ها است، فراهم می‌کند (شکل شماره ۱). مرکز مدیریت علاوه بر ارائه اطلاعات گسترده در ارتباط با شبکه، جزئیات دقیقی از موارد ذیل گردآوری کرده است:

✓ **Trends and high-level statistics**

این اطلاعات مدیران شبکه را در تعیین وضعیت امنیتی در یک لحظه و همچنین نحوه تغییرات آن ، یاری می‌کند.

✓ **جزئیات رویدادها، سازگاری و اعمال قوانین**

درک کاملی نسبت به وقایعی که در حین یک رویداد امنیتی اتفاق می‌افتد، فراهم می‌کنند؛ که موجب ارتقا حفاظت امنیتی، پشتیبانی

از تلاش‌هایی به منظور رفع آسیب‌پذیری‌های و حمایت از اقدامات قانونی می‌شود.

Workflow data

به راحتی انتقال این داده‌ها به راهکارهای دیگر به منظور ارتقا مدیریت بحران امکان‌پذیر است.

قابلیت‌ها و مزایای آن‌ها

جدول شماره ۱ نحوه اعمال یک سیاست‌گذاری به چندین راهکار امنیتی را نشان می‌دهد.

قابلیت	مزایا
مدیریت یکپارچه توابع امنیتی چندگانه در طول چندین راهکار امنیتی	سهیل مدیریت متمرکز بخش‌های امنیتی سیسکو شامل: · NGFW ·سرویس سیسکو with ASA FirePOWER · NGIPS ·سیسکو FirePOWERدفاع در برابر تهدیدات برایISR · AMP
مدیریت یکپارچه سیاست‌گذاری بر عملکرد چندگانه امنیتی	پیکربندی دسترسی فایروال کنترل برنامه، پیشگیری از تهدیدات، فیلترینگ URL و تنظیمات حفاظت پیشرفته در مقابل بدافزارها از طریق تنظیم یک سیاست مدیریتی ساده، کاهش خطاها و ارتقا سازگاری امکان اعمال یک سیاست واحد به چندین راهکار امنیتی را فراهم کرده می‌کند.
مدیریت یکپارچه سیاست‌گذاری‌های کنترل دسترسی از طریق سرویس تشخیص هویت سیسکو	کنترل دسترسی مبتنی بر برچسب امنیتی ISE، نوع دستگاه، محل IP و مهار سریع تهدید صورت می‌گیرد، که در بهبود سازگاری، ارتقا زیرساخت امنیتی و تسهیل فرآیندهای ارائه سرویس نقش بسزایی دارد.
سیستم هوشمند دفاع در مقابل تهدیدات	راهکارهای گروه امنیتی تالوس در ارتباط با تهدیدات و سیستم بهنگام شناسایی نقاط ضعف شبکه و راهکارهای هوشمند مبتنی بر IP و) URL شامل قابلیت Cisco Umbrellaبه منظور شناسایی تهدیدات حتی خارج از محیط شبکه) به همراه اطلاعات به دست آمده از تهدیدات-third party و بسترهای هوشمند تهدیدات STIX/TAXIIادغام شده است.
پایش و کنترل نرم-افزارها	علاوه بر کاهش تهدیدات شبکه، قابلیت کنترل دقیق بیش از ۴۰۰۰ نرم‌افزار تجاری متن‌باز و یا مطابق استاندارد Open App ID، به منظور شناسایی و کنترل برنامه‌های سفارشی را دارد.
مدیریت مشترک و ارثبری سیاست-گذاری ها	قابلیت ایجاد ۵۰ دامین مدیریتی با داده‌ها، گزارش‌دهی و network mapping مجزا که از طریق کنترل دسترسی به اجرا در می-آید. مدیریت مستحکم و موثر از طریق اجرای ساختار سلسله مراتبی سیاست‌ها، که هر سطح سیاست‌گذاری‌های سطوح بالاتر را به ارث می‌برد.
گزارش‌ها و داشبورد مدیریتی	پایش شبکه از طریق داشبوردهای مدیریتی قابل تنظیم و گزارشات و فرم‌ها و الگوهای مختلف ارائه هشدارها و گزارش‌های جامع نمایش اطلاعات رخدادها به شکل جداول، گراف‌ها و نمودارهای مختلف به منظور تحلیل ساده‌تر آنها مانیتورینگ رفتار و کارایی شبکه برای شناسایی نقاط ضعف و حفظ سلامت آن
Secure boot	Secure bootراهکاری مناسب به منظور ارزیابی یک‌پارچگی نرم‌افزار سیسکو موجود در سخت‌افزار FMC در هنگام بوت

	سیستم است. چنانچه signature وجود نداشته باشد و یا نرم‌افزار معتبر نباشد، بارگذاری نخواهد شد) فقط در FMC 1000، FMC 2500و FMC 4500).

دید و بینش استثنایی

Exceptional Visibility and Insight

مرکز مدیریت سیسکو Firepower به صورت خودکار همه اطلاعات مرتبط با محیط شبکه را جمع‌آوری، تلفیق و نمایش می‌دهد. جدول شماره ۱ گستره contextual awareness مرکز مدیریت که تکنولوژی‌های قدیمی‌قادر به ارائه آن نبودند، را نشان می‌دهد. این دیدگاه بحرانی به شبکه در بخش سیاست‌گذاری‌های امنیتی شبکه استفاده شده و سطحی از امنیت که سایر راهکارها قادر به ارائه آن نبودند را ایجاد می‌کند.

جدول شماره۲: پایش کامل Stack

دسته بندی	مرکز مدیریت سیسکو Firepower	IPS	NGFW
تهدید ها	❋	❋	❋
کاربران	❋	❋	❋
نرم افزارهای تحت وب	❋	–	❋
پروتکلهای نرم افزارها	❋	–	❋
انتقال فایلها	❋	–	❋
بذافزارها	❋	–	–
سرورهای c&c	❋	–	–
نرم افزارهای کلاینت	❋	–	–
سرورهای شبکه	❋	–	–
سیستم عامل ها	❋	–	–
روتر ها و سویچ ها	❋	–	–
ابزارهای سیار	❋	–	–
پرینتر ها	❋	–	–
تلفن های voip	❋	–	–
ماشین های مجازی	❋	–	–
اطلاعات نقاط ضعف شبکه	❋	–	–

مدیریت قبل، بعد و در حین حمله

مرکز مدیریت سیسکو Firepower مدیریت یک‌پارچه‌ای در کلیه مراحل وقوع یک حمله ارائه می‌دهد:

قبل از حمله

با توجه به دید کاملی که نسبت به رخدادهای داخل شبکه فراهم کرده است به راحتی می‌توان نیازهای حفاظتی شبکه را شناسایی کرد.

ایجاد قانون‌گذاری‌های فایروال و کنترل عملکرد بیش از ۴۰۰۰ نرم-افزار تجاری و غیرتجاری مورد استفاده در محیط شبکه

در حین حمله

می‌توان سطوح پیشگیری از نفوذ، قوانین اعتبارسنجی URL و حفاظت پیشرفته در مقابل بدافزارها تعریف کرد.

اعمال سیاست‌گذاری‌هایی همچون: " در صورت ورود ترافیک از کشور مورد نظر از طریق نرم‌افزار خاصی و در صورت وجود فایل پیوست، چه سطحی از شناسایی نفوذ اعمال و تجزیه وتحلیل بدافزار صورت گرفته و در صورت لزوم فایل به Sandbox ارسال شود."

پس از وقوع حمله

ارائه گزارش گرافیکی از تمامی‌ابزارهایی که آلوده شده‌اند.

توانایی ایجاد قوانین موردنیاز برای جلوگیری از پیشرفت حمله

تجزیه و تحلیل دقیق بدافزار به منظور بازسازی و ایمن‌سازی مجدد شبکه

امنیت خودکار به منظور ایجاد قابلیت دفاع پویا

مرکز مدیریت سیسکو Firepower به صورت پیوسته تغییرات شبکه را رصد می‌کند، و به روش‌های ذیل موجب تسهیل فرآیندها و ارتقا امنیت می‌شود:

به صورت اتوماتیک ارتباط میان رخدادهای جدی امنیتی و نقاط ضعف شبکه را بررسی می‌کند، تا در صورت وجود احتمال حمله موفق هشدارهای لازم را ارائه دهد. به این ترتیب تیم‌های امنیتی می‌توانند بر روی موضوعاتی که اهمیت بیشتری دارند، تمرکز کنند.

به تجزیه و تحلیل آسیب پذیری های شبکه پرداخته و به صورت خودکار سیاست های امنیتی مناسب برای رفع آن ها را اعمال می‌کند. به این ترتیب امکان تطبیق راهکارهای حفاظت شبکه با شرایط در حال تغییر آن وجود دارد.

برقراری ارتباط میان رویدادهای خاص شبکه، endpoint، نفوذ و منابع اطلاعاتی شبکه، امکان ارائه هشدارهای لازم در صورت بروز هر گونه نشانه از حمله در یکی از میزبان‌ها، به وجود می‌آورد.

سیاست‌گذاری امنیت بر فایل‌ها نیز اعمال می‌شود، به صورت خودکار فایل‌ها به منظور شناسایی بدافزارهای شناخته شده تحلیل می‌شوند و در صورت وجود هر گونه فایل مشکوک، آن را به Sandboxبرای شناسایی نوع نرم‌افزار مخرب آن ارسال می‌کند

یکپارچه سازی آسان از طریق استفاده ازOpen APIs

مرکز مدیریت سیکو Firepower از طریق چهار واسط نرم‌افزار قدرت‌مند و کاربردی، با تکنولوژی‌های third-party می‌تواند ادغام شود APIs. نقاط دسترسی برای موارد زیر فراهم می‌کنند:

انتقال اطلاعات از مرکز مدیریت به سایر بسترها، مانند[1]SIEM

ارتقا اطلاعات موجود در پایگاه داده سیسکو Firepower از طریق داده‌هایthird-party ، چنین اطلاعاتی شامل اطلاعات مدیریت نقاط ضعف شبکه و یا اطلاعات سیستم‌های اجرایی از پویش‌گران فعال شبکه است.

آغاز روندهای کاری و بازسازی‌هایی که توسط قانون‌گذاری‌های کاربر تعریف شده است. به عنوان مثال شما ملزم به ادغام روند کار با NAC[2] به منظور قرنطینه یک endpoint آلوده و یا ایجاد یک رویه قانونی جدید هستید.

پشتیبانی از تحلیل و گزارش‌های third-party از طریق فعال کردن امکان جستجوی آن‌ها در دیتابیس مرکز مدیریت

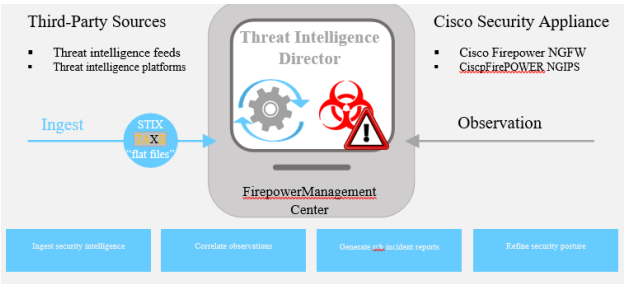
APIsهمچنین برای ادغام با تعدادی از محصولات امنیتی و workflowسیسکو استفاده می‌شود. که شامل sandboxing از طریق AMP Threat Grid ، سرویس شناسایی سیسکو به منظور تعیین وضعیت دیتا و تقسیم بندی شبکه و Cisco Umbrella .

Threat Intelligence Director

Threat Intelligence Director عملیات هوشمند دفاع در مقابل تهدیدات را از طریق تجهیزات امنیتی سیسکو ذیل انجام می‌دهد:

Cisco Firepower NGFW
Cisco Firepower NGIPS

شکل شماره ۱- Threat Intelligence Director Integrates Third-Party Security Intelligence :



جدول شماره ۳ نسخه‌هایی از محصولات سیسکو FirePOWER که مرکز مدیریت قابلیت کنترل آن، به همراه بستر سخت‌افزاری مرتبط را نشان می‌دهد.

جدول شماره ۳: نسخه های Firepower پشتیبانی شده و سیستم عامل های آنها

Management Platform	Software Revision Level	Hardware Platform
Cisco Firepower Management Center	Cisco Firepower Threat Defense 6.x (NGFW)	ASA 5500-X (except ASA 5585-X) Cisco 2100 Series (min FMC 6.2.1) Cisco Firepower 4100 Series Cisco Firepower 9300
	FirePOWER Services 6.x	ASA 5500-X
	Cisco Firepower NGIPS 6.x	Cisco Firepower 7000 Cisco Firepower 8000
	FirePOWER Threat Defense for ISR 6.x (Cisco Firepower Services)	۴۰۰۰ Series ISR ISR G2
	FirePOWER Services 5.4.x	ASA 5500-X
	Cisco Firepower NGIPS 5.4.x	Cisco Firepower 7000 Cisco Firepower 8000

سازگاری Hypervisor

ابزار مجازی مرکز مدیریت سیسکو Firepower از Hypervisor جدول شماره ۵ پشتیبانی می‌کند.

جدول شماره ۵ Hypervisor :قابل اجرا در ابزارهای مجازی

Hypervisor	Version and Details	VirtualCisco Firepower Management Center Version
VMware vSphere	۶،۰:, ۵،۵, ۵،۱ ● ESXi Server ● vCenter Server (optional) ● vSphere Web Client, vSphere Client, or OVF Tool for Windows or Linux	۶،۰, ۵،۴
KVM	Ubuntu 14.04 LTS Red Hat Enterprise Linux (RHEL) Version 7.1	۶،۱
Amazon Web Services	AWS Instance Types: c3.xlarge and c3.2xlarge	۶،۱, ۶،۰،۱

مدل های مختلف سیسکو فایرپاور FirePOWER

تجهیزات سیسکو Firepower سری ۱۰۰۰

سری Cisco Firepower 1000 یک خانواده متشکل از چهار پلتفرم امنیتی فایروال نسل بعدی (NGFW) متمرکز بر تهدید است که از طریق دفاع برتر برابر تهدید، انعطاف پذیری تجاری را ارائه میدهد. هنگامی‌که توابع تهدید پیشرفته فعال هستند، عملکرد پایدار استثنایی را ارائه می‌دهد. محدوده توان عملیاتی سری ۱۰۰۰ از مواردی مانند دفاتر کاری کوچک ، دفتر خانه ، دفتر شعبه راه دور تا لبه اینترنت استفاده می‌کند. سیستم عامل های سری ۱۰۰۰ نرم افزار Cisco Firepower Threat Defense (FTD) و Cisco Adaptive Security Appliance (ASA) را اجرا می‌کنند.

تجهیزات سیسکو Firepower سری ۹۳۰۰

Cisco Firepower 9300 یک مقیاس قابل توسعه است (فراتر از ۱ Tbpsدر صورت خوشه ای)، پلت فرم ماژولار و درجه یک برای شرکت های ارائه دهنده اینترنت ، مراکز محاسباتی با عملکرد بالا ، مراکز داده بزرگ ، پردیس ها ، محیط های تجاری با فرکانس بالا

فایرپاور سیسکو فایروال نسل جدید

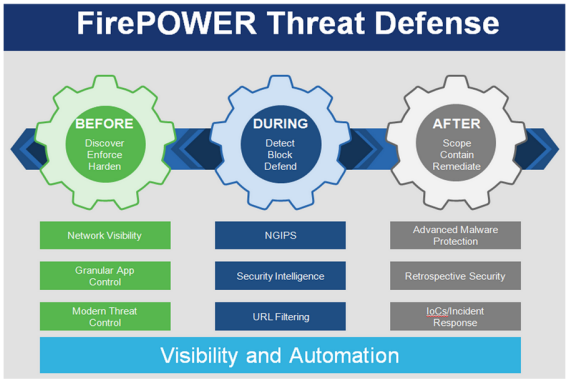
و سایر محیط هایی که نیازمند تأخیر کم (بارگیری کمتر از ۵ میکرو ثانیه) و توان استثنایی هستند. Cisco Firepower 9300 از flow-offloading، تنظیم به صورت برنامه ریزی شده و مدیریت سرویس های امنیتی با RESTful API پشتیبانی می‌کند .همچنین در تنظیمات سازگار با استانداردهای ساخت تجهیزات شبکه (NEBS) فعال است. سیستم عامل های سری ۹۳۰۰ می‌توانند Firewall Cisco C Adaptive Security Appliance Security (ASA) یا Cisco Firepower Threat Defense (FTD)را اجرا کنند.

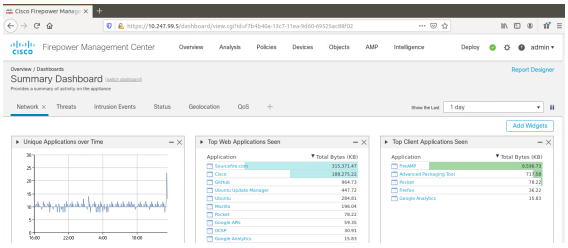
تجهیزات سیسکو Firepower سری ۲۱۰۰

سری Cisco Firepower 2100 یک خانواده متشکل از چهار پلتفرم امنیتی NGFW متمرکز بر تهدید است که از طریق دفاع برتر در برابر تهدید ، انعطاف پذیری تجاری را به ارمغان می‌آورد .هنگامی‌که توابع تهدید پیشرفته فعال هستند ، عملکرد پایدار استثنایی را ارائه می‌دهد .این پلتفرم ها به طور منحصر به فردی از معماری پردازنده چند هسته ای دوگانه ابتکاری استفاده می‌کنند که به طور همزمان فایروال، رمزنگاری و بازرسی تهدیدها را بهینه می‌کند. محدوده توان فایروال این سری از موارد از لبه اینترنت گرفته تا مرکز داده استفاده می‌کند. تطابق استانداردهای ساخت تجهیزات شبکه - (NEBS) توسط پلت فرم سری ۲۱۰۰ Cisco Firepower پشتیبانی می‌شود. سیستم عامل های سری ۲۱۰۰ می‌توانند Firewall Cisco ASA یا Cisco Firepower Threat Defense (FTD) را اجرا کنند.

تجهیزات سیسکو Firepower سری ۴۱۰۰

سری Cisco Firepower 4100 یک خانواده متشکل از هفت پلتفرم امنیتی NGFW متمرکز بر تهدید است .دامنه توان آنها موارد استفاده از مرکز داده و لبه اینترنت را نشان می‌دهد .آنها دفاع تهدید برتر ، با سرعت بیشتر ، با ردپای کوچکتر را ارائه می‌دهند Cisco . Firepower 4100 Series از قابلیت flow-offloading، تنظیم برنامه و مدیریت سرویس های امنیتی با RESTful API پشتیبانی می‌کند .رعایت استانداردهای ساخت تجهیزات شبکه (NEBS) توسط پلت فرم Cisco Firepower 4120 پشتیبانی می‌شود .سیستم عامل های سری ۴۱۰۰ می‌توانند نرم افزار Cisco ASA Firewall یا Cisco Firepower Threat Defense (FTD) را اجرا کنند.





درباه سیسکو: سیسکو از تولید کنندگان مطرح تجهیزات شبکه و امنیت در سطح جهانی است. سیسکو فایرپاور به عنوان فایروال نسل بعد، می‌تواند شبکه را در مقابل انواع تهدیدات محافظت کند.

رایان سامانه آرکا- نماینده رسمی‌سیسکو در ایران

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir www.arka.ir