Cyberoam

Cyberoam Unified Treatment Management systems (UTM)

Sale & Technical Support **:** Info@IRITClub.com

UTM (مدیریت یکپارچه تهدیدات)

تهدیدات بیرونی همچون کلاهبرداریها و سرقت های اینترنتی و جاسوس افزارها، ویروسها و غیره هدفشان دستیابی به اطلاعات محرمانه شخصی یا مربوط به شرکت یا تغییر نوع دستگاه برای حملات بیشتر می‌باشد. به علاوه اینکه کاربران داخلی امنیت شرکت را از روی نادانی یا از روی عمد به خطر می‌اندازد و امنیت شرکت را در مقابل یک حمله بزرگ قرار می‌دهند.

راهکارهای امنیتی مجزا، در مواجهه با انواع مختلف تهدیدات واکنش سریع و مناسبی را ارائه نمی‌دهند. یک راهکار مدیریت یکپارچه تهدیدات (UTM) محافظت جامعی را برای شرکتها فراهم می‌کند با این ویژگی که امنیت چند گانه مستحکمی را در یک دستگاه به کار گرفته است.یک دستگاه UTM، مدیریت استراتژیک امنیتی شرکتها را بسیار آسان کرده و بدلیل وجود مدیریت واحد روی یک دستگاه، پشتیبانی یک منبع و همچنین نیاز به یک راه‌اندازی و نگهداری، بسیار مقرون به صرفه است. کنسول مرکزی آن باعث می شود که بتوان امنیت شبکه را در نقاط دیگر ارزیابی کرد.

کنترلها و قابلیت نمایش بر اساس شناسه کاربری بخش حساس امنیت شبکه است. بوسیله داده‌های ترکیب‌شده از شبکه و شناسه‌ها،شرکتها قادر خواهند بود تا رفتار کاربران یا گروههای خاصی را که می توانند دلالت بر استفاده نادرست، ورود غیرمجاز یا حملات عمدی از داخل یا بیرون شرکت باشند شناسایی کنند. تعریف سیاستهای امنیتی وکاربری براساس هویت و شناسه می تواند روی بخشهای مختلفی از شبکه اعمال شود.

مدیریت یکپارچه تهدیدات Cyberoam

Cyberoam اولین تولید کننده راهکاری امنیت شبکه UTM براساس شناسه کاربری برای شرکتهای کوچک، متوسط و بزرگ است.تجهیزات UTM Cyberoam شامل دیوارآتش، شبکه خصوصی مجازی VPN، مدیریت پهنای باند، سیستم مدیریت ارتباطات همزمان چند گانه و جلوگیری از مسدود شدن دروازه (Gateway)، سیستم گزارش‌گیری روی یک دستگاه واحد می‌باشد. سایبروم در جهت بروز رسانی سیستمهای ضد ویروس، ضد جاسوس افزار، ضد هرزنامه، سیستم جلوگیری از نفوذ و سیستم پالایش و فیلترینگ برنامه ها و وب، لایسنسهای اشتراکی بصورت سالیانه ارائه می کند.

Cyberoam به منظور نیل به بیشترین حفاظت لحظه‌ای جامع، تمامی راهکارهای امنیتی همچون دیوارآتش، ضدجاسوسی،ضدویروس دروازه، ضدهرزنامه دروازه، سیستم جلوگیری از ورودغیر مجاز و پالایش محتوی را در یک دستگاه گرد آورده است که مقرون به صرفه بوده ومدیریت آسانی برای شرکتها فراهم می کند. تجهیزات VPN – دیوارآتش Cyberoam تونلهای رمزشده مطمئنی را برای برقرار کردن ارتباط از راه دور کاربران متحرک با شبکه مرکزی شرکت فراهم می‌کند.

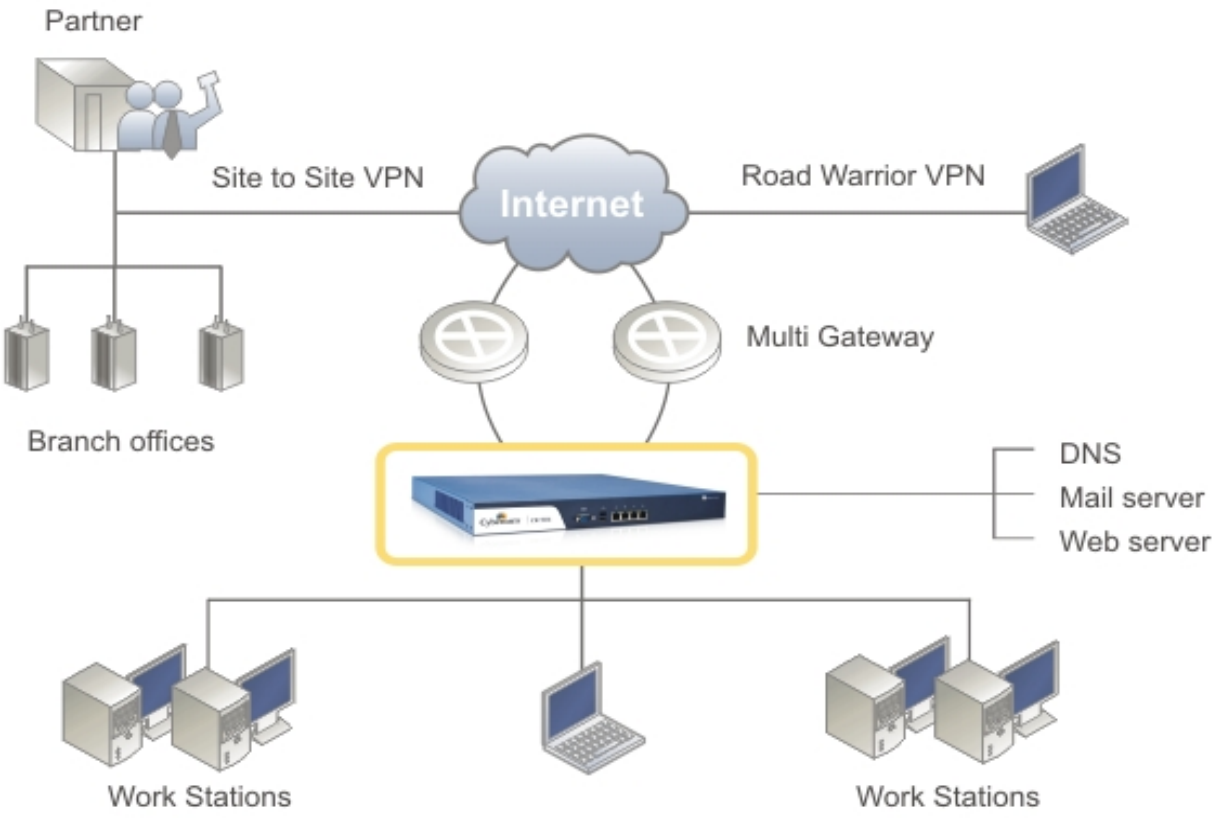
سری های CR Cyberoam

امنیت
دیواره آتش
شبکه خصوصی مجازی VPN
ضد ویروس،ضد جاسوس افزار و ضد هرزنامه دروازه
سیستم جلوگیری از ورود غیرمجاز (IPS)
محافظت در برابر جاسوسها، دزدیدن اطلاعات شخصی، کلاهبرداریها و سرقت های اینترنتی

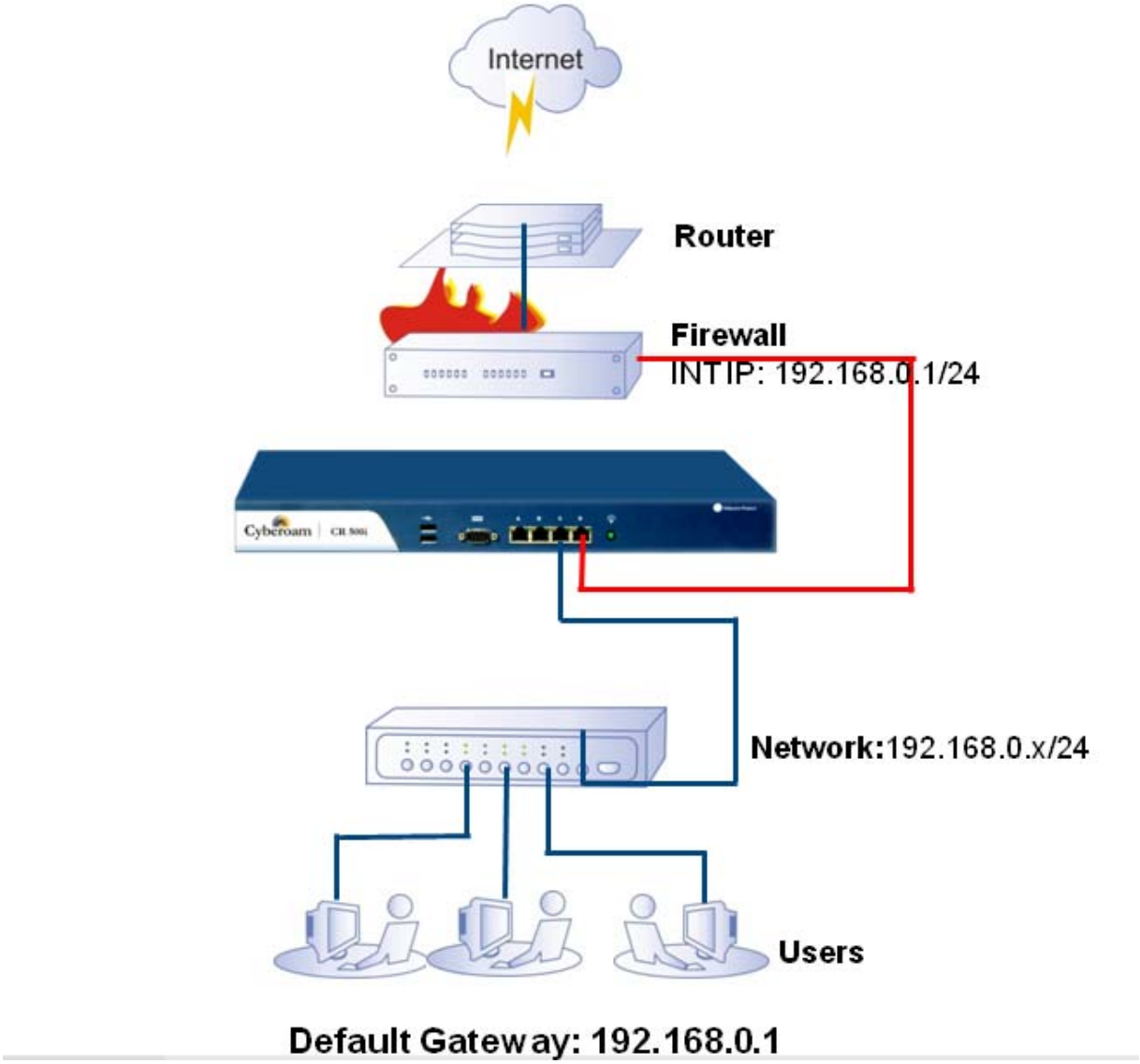
بهره وری
مدیریت پهنای باند.
تقسیم بار ارتباطهای چندگانه و جلوگیری از مسدود شدن دروازه

حالت های نصب در شبکه

- **Cyberoam in Gateway Mode**



- **Cyberoam in Bridge Mode**



تکنولوژی اعطای حق امنیتی بر اساس شناسه کاربری

Cyberoam تنها UTM براساس شناسه کاربری است که ترکیبی از شناسه کاربر و امنیت یکپارچه را ارائه کرده‌است.این دستگاهها نه تنها شرکتها را قادر می‌سازد خط‌مشی برای کار تعریف کنند بلکه گزارش کاملی از کاربر و فعالیتهای وی می‌دهد. به طور مثال قابلیت دیدن اینکه " چه کسی چه کار کرده‌است" به شرکتها اجازه می‌دهد که هر کجا که افراد روی دستگاههای مشترک کار می‌کنند امنیت کامل و جامع را تامین کرده و کاربران را حتی در محیط‌های Wi-Fi و محیط‌های پویای DHCP شناسایی و کنترل کنند.

در Cyberoam شناسه کاربر شناسایی شده و توسط همه قابلیتهای آن کنترل می شود که این خود حد بی نظیری از انعطاف پذیری و قابلیت رؤیت در شبکه را می‌رساند.

راهکارهای امنیتی در سطح پیشرفته

میزان آمادگی و قابلیت واکنش سریع Cyberoam، زمان بالابودن و دسترسی بدون وقفه به منابع شبکه را به حداکثر رسانده است. این دستگاههای امنیتی، مسیریابی پویا را ارائه داده که زمان بالا آمدن سریع، توان خروجی بالای شبکه با کمترین تأخیر و پیکربندی آسان و امکان توسعه سریع شبکه را به همراه دارد. قابلیتVLAN در

Cyberoam شرکتهای بزرگ را قادر می‌سازد تا متناسب با محیط کاری، خط‌مشی‌های مورد نیاز را، در سراسر شبکه از یک مکان واحد یا دفتر مرکزی تعریف کنند

مدیریت متمرکز و گزارش‌گیری براساس شناسه کاربری

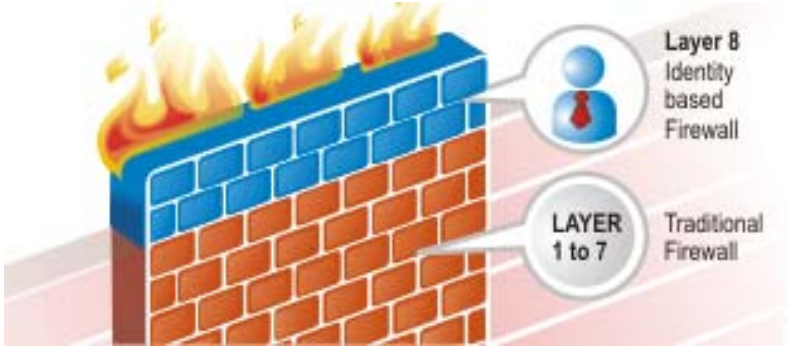
به وسیله کنسول مرکزی Cyberoam، با اعمال کنترل کامل روی شبکه‌هایی توزیع شده در هر نقطه، امنیت متمرکز فراهم می گردد. شرکتها بدون نیاز به منابع فنی در محلهای شرکت، از حفاظت بی‌وقفه و لحظه‌ای در برابر حملات شبکه‌ای ترکیبی و گوناگون در دفاتر شعب خود برخوردار هستند.

Cyberoam محدوده وسیعی از گزارشهای بر اساس شناسه کاربری شامل: مرور کاملی از اطلاعات مربوط به فعالیت کاربر و وقوع حمله، اطمینان از انجام‌شدن تنظیمات و ردیابی‌های دورهای کوتاه را ارائه می‌دهد. شرکتها میتوانند با سرعت تهدیدات امنیتی روی شبکه را خلاصه‌بندی کرده و خط‌مشی‌های دقیق برای پیشگیری و رسیدن به سطح قابل قبولی از بهره‌وری ایجاد کنند.

تجهیزات سخت‌افزاری دیواره آتش

دیواره آتش Cyberoam تنها فایروال UTM ی است که شناسه کاربران را به قواعد دیواره آتش وارد کرده بدین ترتیب نیاز صرف به استفاده از آدرس IP را به عنوان مؤلفه‌ای میانی در شناسایی و کنترل کاربران حذف نموده‌است. دیواره آتش سخت‌افزاری Cyberoam قابلیت بررسی هوشمند بسته‌های اطلاعاتی و داده‌ها را داشته و کنترل دسترسی،تشخیص هویت کاربر و محافظت در سطح برنامه‌ها و شبکه را برای مدیر شبکه فراهم می‌کند.

دیواره آتش تأیید شده توسط موسسه ICSA به همراه VPN، ضد جاسوس افزار، ضد ویروس دروازه، ضد هرزنامه دروازه، سیستم جلوگیری از ورود غیر مجاز، پالایش محتوا، مدیریت پهنای باند و ارتباط‌های چندگانه قابل استفاده است که امنیتی جامع برای شرکتهای کوچک متوسط و بزرگ که دارای دفاتر راه‌دور و شعبه هستند فراهم می‌آورد.



ویژگیهای کلـیدی :

- دیواره آتش با قابلیت بررسی هوشمند بسته‌های اطلاعاتی(Stateful Inspection Firewall)
- مدیریت متمرکز برای قابلیتهای امنیتی چندگانه
- وارد کردن شناسه کاربری در معیارهای سنجش
- امنیت محدوده چندگانه
- کنترل نرم افزارهای ارتباط مستقیم و نقطه به نقطه(P2P)
- تائیدیه از مؤسسهICSA

تکنولوژی اعطای حق امنیتی بر اساس شناسه کاربری

از آنجایی که دیوارهای آتش ابزارهایی برای مقایسه سیاستهای دسترسی با اطلاعات ارتباطی است، Cyberoam دیواره آتشی را ارائه کرده که شناسه‌کاربری را در دیگر قوانین مقایسه از جمله مبداء، محدوده مقصد و آدرس IP، به سیاستهای شرکت اضافه می‌کند. با این دیواره آتش دسترسی یک کاربر بر اساس محیط کاری خاص نیز کنترل می‌شود.

این دستگاه همچنین با کنترل روی ترافیک برنامه های P2P و IM اجازه دسترسی به برنامه‌های خاص به مقصد مورد نظر را می دهد ولی از اشتراک فایلها و ردوبدل شدن آنها جلوگیری می کند. به علاوه Cyberoam کنترل زمانبدی شده دسترسی را برای شرکتها به ارمغان می‌آورد.در حالت داشتن چندGateway، شرکتها می توانند قوانین دیواره آتش را برای مسیریابی کاربر و ترافیک برنامه‌ها روی یک دروازه خاص تعریف کنند.

امنیت در حد گسترده

- Cyberoam با به حداقل رساندن امکان بروز مشکل ارتباط، قابلیت دسترسی بالایی ارتباطی مستمر را فراهم می‌کند. Cyberoam نیاز به امنیت در سطح گسترده را از طریق مسیریابی پویا ایجاد می‌کند که این خود باعث بالا آمدن سریع شبکه، توان خروجی بیشتر شبکه با مدت زمان تأخیر کمتر و پیکربندی ساده‌تر می‌شود.
- Cyberoam – امکان پشتیبانی از VLAN را دارد که خود توانایی گسترده ای در ساختن پروفایل گروههای کاری در سراسر شبکه شرکت ایجاد می‌کند.
- امکان میزبانی مجازی Cyberoam، امکان ایجاد سرورهای میزبان را در داخل LAN و DMZ برای شرکتها فراهم می‌کند. این توانایی، استفاده مفید و مؤثر از آدرسهای IP اینترنت را برای سرویسهای میزبانی بهمراه دارد.
- دیوارآتش CyberoamUTM بازرسی هوشمند و مفیدی را جهت حفاظت جامع در برابر حملات DoS و حملات

کلاهبرداری IPال(Spoofing IP)پیشنهاد می‌دهد.

- Cyberoam اطلاعات کاملی در رابطه با ترافیک شرکت از طریق گزارشهای دیواره آتش تهیه می‌کند.

Multicast برای بروز کردن موجودی‌ها

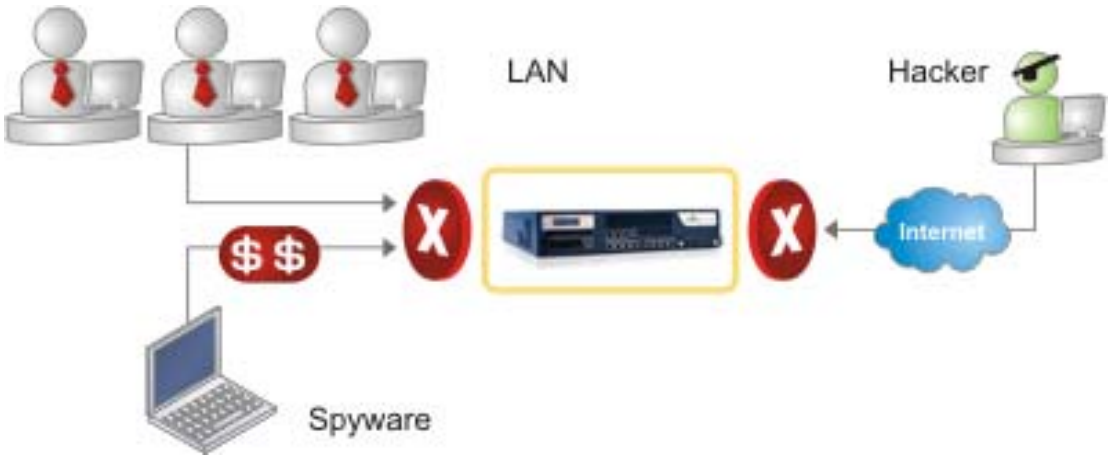
دیواره آتش Cyberoam با قابلیت پشتیبانی از Multicast، شرکتها و مؤسسات مالی را قادر می‌سازد تا اطلاعات کالاها و سهام خود را که از طریق این روش دریافت کنند. همچنین بدلیل اشغال پهنای باند توسط برنامه‌هایی که حاوی فایلهای صوتی- تصویری هستند، قابلیت Cyberoam Multicast، با محدود کردن پهنای باند، کارایی شبکه را افزایش داده و هزینه های سازمانی را کاهش می دهد.

دیوارآتش سخت افزاری Cyberoam با پشتیبانی از پروتکل IPSec VPN، امنیتی سطح بالا برای مکانهای توزیع شده مهیا می‌کند.

جلوگیری از ورود غیرمجاز و نفوذ

مهاجمان به طور فزاینده‌ای به سمت حملات داخلی و بیرونی روی‌آورده‌اند. بعضی اوقات این حملات تمرکز زیادی دارند به منظور اینکه کلید اصلی دسترسی به منابع شبکه را بدست آورند. در خیلی از حملات احتمال اینکه در محدوده راداری ضدویروس و ضدMalware بسیارکم است به همین دلیل باعث شده تا شرکتها به سمت استفاده از موتورهای پیشرفته IPS برای محافظت لحظه‌ای حرکت کنند.

راهکار IPS Cyberoam در زمینه مسدودکردن تلاشهای ورود غیرمجاز، محافظت در برابر Malware، تروجان، حملات DoS، انتقال عمدی رمز، فعالیت Backdoorها و حملات ترکیبی حفاظت و امنیت قدرتمندی را ارائه کرده‌است. ارائه جامع‌ترین حفاظت لحظه‌ای برای شرکتها با ترکیبی از فایروال، ضدجاسوسی، ضدویروس Gateway، ضدهرزنامه و پالایش محتوا یک سرویس اشتراکی است.



ویژگیهای کلیدی

- سیاستهای انتخابی و چندگانه IPS
  IPS policies
- سیاستهای بر اساس شناسه کاربر
- به روز رسانی شدن در هر لحظه و بصورت خودکار
- گزارش‌گیری از ورود غیرمجاز براساس شناسه کاربری

حفاظت یکپارچه

IPS یا سیستم جلوگیری از نفوذ Cyberoam، پروتکلهای متعددی از جمله IM,P2P,IMAP,POP3,SMTP,FTP,HTTP را پشتیبانی می‌کند و به طور خودکار ترافیک‌های مشکوک را کشف کرده و مسدود یا دور می‌اندازد. IPS محافظت لایه شبکه و کاربردی را با بیش از ۴۵۰۰ امضای تعریف‌شده که می‌تواند به طور خودکار به روز شود ارائه می‌دهد.

گزارش‌گیری و سیاستگذاری سیستم IPS براساس شناسه کاربری

سایبروم UTM در ایجاد سیاستهای متعدد IPS منحصر بفرد است و شرکتها را قادر می‌سازد تا بجای ایجاد سیاستهای مبهم، به طور مشخصی سیاستها را متناسب با هر کاربر یا گروه تعریف کنند. به عبارتی، شرکتها می‌توانند با وضع سیاستهای چندگانه و براساس شناسه کاربر، دسترسی کاربران را به برنامه‌هایی همچون IM و P2P، محدود کنند.

سیستم جلوگیری از ورود غیرمجاز Cyberoam هشدارهای براساس شناسه کاربری را ارائه می‌دهد و گزارش‌گیری کاملی بر اساس نام کاربری روی هر دو ترافیک ورودی و خروجی انجام می‌دهد. شرکتها با بدست‌آوردن نمایی از برنامه‌ها به همراه نام‌کاربریِ مبداء، مقصد، محدوده کاربرد می توانند تا کاربران متخلف را در پائین ترین سطح دسترسی به اطلاعات نگه دارند. به علاوه داشبورد Cyberoam دید وسیعی از وضعیت حملات را نمایش داده و گزارشهای جمع آوری شده توسط IPS یا سیستم جلوگیری از نفوذ Cyberoam، آمار بیشترین هشدارها، مهاجمان و قربانیان به همراه نامهای کاربران و نمونه‌ای از حملات شدید و ملایم ارائه می‌کند.

محافظت بی وقفه

سیستم جلوگیری از تفوذ Cyberoam با پشتیبانی از امضاهای منتخب این امکان را به شرکتها میدهد تا امضاهایشان را برای محافظت مداوم تعریف کنند و جلوی حملات سازمان‌یافته به سمت شرکت را بگیرند. بانک امضاهای

IPS شامل امضاهای پروکسی HTTP می‌باشد که جلوی نقاب‌گذاری کاربرها را در قالب کاربر ناشناس می‌گیرد.

امنیت متمرکز

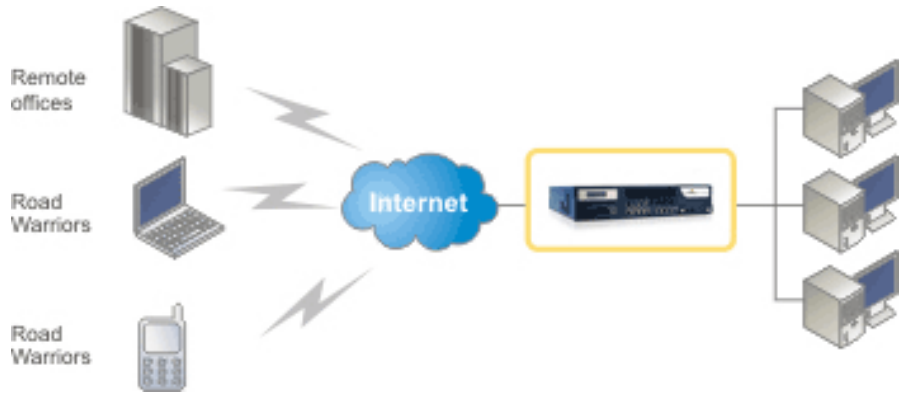
شرکتها می‌توانند از طریق کنسول مرکزی Cyberoam امضاهای دلخواه را برای دفاتر شعب خود بسازند. سیاستهای IPS می‌توانند در کل شبکه سراسری شرکت اعمال شده و شرکتها از محافظت مداوم دفاتر شعب خود در برابر حملات شبکه‌ای مرکب حتی بدون حضور منابع فنی، برخوردار شوند.

تجهیزات دیوارآتش VPN

شرکتها در هر اندازه‌ای که باشند، به داشتن ارتباطی امن و سریع بین شعبه‌ها و دفاتر راه‌دورو دفتر مرکزی خود نیازمندند. برای کاربران متحرک و کاربران خانگی، دسترسی امن به منابع شرکت مثل Email ها، شبکه‌داخلی، اسناد و برنامه‌ها و از همه بیشتر کارایی بالا، ضروری است.

تجهیزات VPN Cyberoam با ایجاد تونلهای رمزشده شبکه و امن، شرکتها را، برای دسترسی کارمندان متحرکشان در هر کجای جهان قابل دسترس می‌سازند. تجهیزاتVPN راهکار بسیار مقرون به صرفه‌ای هستند که کارایی بالایی با مصرف پهنای باند کم، ارائه می‌دهند. تجهیزات دیوارآتش Cyberoam VPN به دلیل کارایی و آسانی بی‌نظیر و امنیت دسترسی به منابع شرکتی، گزینه مناسبی برای شعبه‌ها، کاربران خانگی، و کاربران متحرک است که نیاز به یک اتصال مطمئن به شبکه مرکزی دارند.

VPN Cyberoam که توسط کنسرسیوم VPNC تأیید شده‌است، قابلیت سازگاری با اکثر پروتکل های IPSecVPN موجود در بازار را دارد. این دستگاه از پروتکل های اتصالی IPSec,L2TP,PPTP پشتیبانی کرده و می‌تواند ارتباطهای شبکه به شبکه و کاربر به کاربر را ایجاد کند.



ویژگیهای کلیدی

- پشتیبانی ازIPSec,L2TP,PPTP
- تأییدیهVPNC .
- خروج از خطایVPN
- اتصالات شبکه به شبکه و کاربر به کاربر

Cyberoam VPN بر اساسIPSec

VPN بر اساس IPSec شرکت Cyberoam با پشتیبانی کامل از IPSec, IKE شبکه‌ای با تشخیص هویت و رمز نگاری قوی از طریق DES,3DES,AES ایجاد می‌کند.

تجهیزات Cyberoam VPN فایل تنظیمات سرویس گیرنده IPSecVPN را به طور خودکار ایجاد می‌کند که باعث می‌شود نیاز به دانش فنی جهت انجام تنظیمات برطرف شود.

خروج از بن‌بست VPN

تجهیزات Cyberoam VPN با ایجاد خروج از بن‌بست خودکار اتصالات VPN روی اتصالات IPSec,L2TP امکان ارتباط VPN مداوم و مستمر را در میان دروازهای ISP های مختلف فراهم می‌کند. دفاتر شعب و کاربران متحرک با استفاده از ارتباطات کاربر به کاربر و شبکه به شبکه می‌توانند یک ارتباط VPN ثانوی برای وقتی که ارتباطات WAN آنها قطع می‌شود برقرار کنند تا بتوانند کار بی‌وقفه و پویایی را انجام دهند.

مدیر پهنای باند

استفاده مداوم اینترنت و انسداد پهنای باند به واسطه دانلودهای کاربران داخلی، در اکثر اوقات، شرکتها را با کمبود پهنای باند برای برنامه‌های حساس کاری مواجه می‌کند. مدیریت پهنای باند بر اساس شناسه‌کاربری Cyberoam، استفاده از پهنای باند را بهینه ساخته و با کنترل پهنای باند روی گلوگاه‌ها، مانع از بین‌رفتن پهنای باند و مسدود شدن آن می‌شود. به شرکتها توصیه می‌شود تا با ممانعت از برنامه های غیرحساس که باعث افت کارایی شبکه می‌شوند، کنترل امنیت پهنای باند را نیز به دست گیرند.

مدیریت پهنای باند Cyberoam با ترکیب توزیع بار روی ارتباط‌های چندگانه و جلوگیری از بروز بن‌بست Gateway، راهکاری برای یک فعالیت جامع بدون وقفه و با پهنای باند بهینه شده ارائه می‌دهد.

مدیریت پهنای باند براساس شناسه کاربری

با استفاده از مدیریت پهنای باند Cyberoam، شرکتها میتوانند اولویتهایی براساس کاربر، گروه وبرنامه هابا اختصاص پهنای باند دقیق و برمبنای زمان و کاربرد آن در روز تعریف کنند. ماژول پالایش محتوای اینترنت Cyberoam، مدیریت بهینه پهنای باند را، بوسیله جلوگیری از دانلودهای صوتی- تصویری، بازی،تبلیغات وغیره که خطوط را بیهوده اشغال می کنند، تکمیل می‌کند. این کار به فعالیتها و برنامه‌های حساس به پهنای باند مانند: CPM,VOIP و غیره، اطمینان می دهد که پهنای باند تضمین شده را بدست بیاورند.شرکتها می‌توانند، با تنظیم سیاستهای ویژه جهت اختصاص پهنای باند بر اساس نیاز کاربران، کارایی شبکه خود را اصلاح کنند.

ویژگیهای کلیدی

- اختصاص پهنای باند بر اساس برنامه و شناسه کاربری
- پهنای باند قابل افزایش
- اختصاص پهنای باند زمان بندی شده.

الویت بندی پهنای باند

تجهیزات دیواره آتش Cyberoam گذشته از اینکه قادر به تعریف خط‌مشی‌های پهنای باند برای اختصاص پهنای باند به ترافیک‌های کاری با اهمیت‌تر هستند، به شرکتها این توانایی را می‌دهند که دسترسی بی وقفه را برای کاربرها و برنامه های حساس فراهم آورند. علاوه بر این آنها را کنترل پهنای باند را روی ترافیک‌های غیرضروری و برنامه‌های رسانه‌ای که پهنای باند زیادی مصرف می‌کند را حفظ کند.

پهنای باند قابل افزایش و اختصاصی

شرکتها می‌توانند بوسیله مشخص‌کردن حداقل و حداکثر پهنای‌باند، سیاستهایی را برای اختصاص پهنای باند تضمینی به کاربران ایجاد کنند. پهنای‌باند اختصاصی این اطمینان را می‌دهد که کاربران حساس، سطح یکسانی از پهنای باند را در زمانهای اوج ترافیک دریافت کنند. پهنای‌باند اختصاصی و قابل افزایش، به کاربران این اجازه را می دهد تا در صورت امکان و اطمینان از بهینه بودن منابع شبکه، پهنای باند بیشتر دریافت کنند

اختصاص پهنای باند بر اساس زمان

شرکتها می‌توانند بوسیله مدیریت پهنای‌باند Cyberoam،رپهنای باند را بر اساس نیازهای هر کاربر تنظیم و زمان‌بندی کنند. پهنای‌باند را میتوان برای یک کاربر در طی زمان خاصی از روز وقتی که دسترسی بدونّ وقفه لازم است فراهم کرد. با این کار شرکتها می‌توانند نقاط اوج پهنای باندکاری را در طول روز کمتر کنند. این کار نیاز به خرید پهنای‌باند را به خاطر اوج بیش از حد در کار محدود کرده و باعث کنترل هزینه‌های عملیاتی می شود.

جلوگیری از انسداد و ازکار افتادن GATEWAY و توزیع بار ارتباط‌های چند گانه (MULTI LINK)

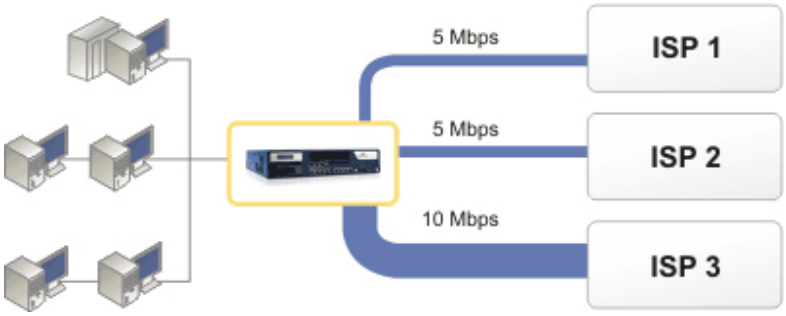
وجود یک ارتباط صرف به یک ISP، می‌تواند برنامه های حساس شرکتها را، که در برابر از مشکلات ارتباطی آسیب‌پذیر می باشند از کار انداخته و باعث صدمه کاری شدید شود. تحمل خرابی در برابر لینکهای ISP، برای تداوم کار و سودآوری بیشتر شرکتها،امری مهم و ضروریست. سیستم مدیریت کننده ارتباطهای چند گانه Cyberoam، شرکتها را قادر می سازد تا با ارائه مدیریت جامع ترافیک جهت بهینه سازی ارتباطات، ترافیک روی ارتباطهای متعدد WAN را کنترل کنند. این موضوع باعث برقراری اتصال با بالاترین سرعت ممکن و صرفه جویی در سرمایه و استفاده بهینه از منابع را به ارمغان می‌آورد.

یک‌دستگاه دیواره آتش UTM سایبروم، لینک‌های WAN متعدد را بخوبی مدیریت می‌کند که در مقایسه با استفاده از چندین دستگاه برای مدیریت چند WAN، هزینه کمتری دارد. به طور کلی، Cyberoam امنیت متمرکز و جامع را در قالب یک دستگاه ارائه می‌کند که مقرون به صرفه نیز می باشد.

ویژگیهای کلیدی

- تنظیمات خودکار در زمان بروز نقص فنی ارتباطی
- توزیع بار بصورت وزنی بر اساس الگوریتمRound Robin
- سیاست مسیریابی برای کاربر و برنامه

- نمایش وضعیت Gateway در داشبورد.



توزیع بار ترافیکی

سیستم مدیریت ارتباط‌های چندگانه و همزمان Cyberoam، ترافیک اینترنت را در شرکتها بوسیله توزیع بار شبکه روی چندین ارتباط مجزای ISP و توزیع بار بصورت وزنی بر اساس الگوریتم Round Robin برای برنامه‌ها و کاربرها کنترل می‌کند.

شرکتها می‌توانند ترافیک برنامه های ضروری را روی لینکهای با سرعت بالا قرار دهند و سطح بالایی از قابلیت دسترس بودن را برای خدمات و برنامه ها را فراهم کنند. همچنین با دادن بارهای سنگین به لینکهای پر سرعت، می توان در زمانهای افت پهنای‌باند، با استفاده بهینه از ارتباطهای کم هزینه، به نتایج مطلوب دست یافت.

جلوگیری از انسداد و ازکار افتادن Gateway

مدیر ارتباط چند گانه Cyberoam، ارتباطهای در دسترس و قابل استفاده و متصل به WAN را زیر نظر گرفته و ترافیک را از یک ارتباط مشکل دار به یک ارتباط در حال کار و قابل اطمینان انتقال می‌دهد. این سرویس دردسترس بودن همیشگی برنامه‌های مهم و حساسی همچون CRM, VOIP را تضمین کرده و در نتیجه، افزایش بهره‌وری و کاهش هزینه‌های نگهداری را به دنبال دارد.

هشدارها و گزارش‌دهی ها

Cyberoam مدیران شرکت را از قطع‌شدن ارتباط دروازه بوسیله پیغامهای هشدار Email و از طریق داشبورد آگاه می‌سازد، در نتیجه اشکال زدایی سریع را ساده می‌کند. گزارش‌گیری Cyberoam گزارش‌گیری زمانی و در لحظه را ارائه داده و این امکان را به مدیران می‌دهد تا کارایی و ظرفیت ارتباط را ارزیابی کنند- به طور مثال گزارش‌گیری جامع این امکان را به مدیران می‌دهد تا درباره خرید پهنای‌باند تصمیم‌گیری کنند.

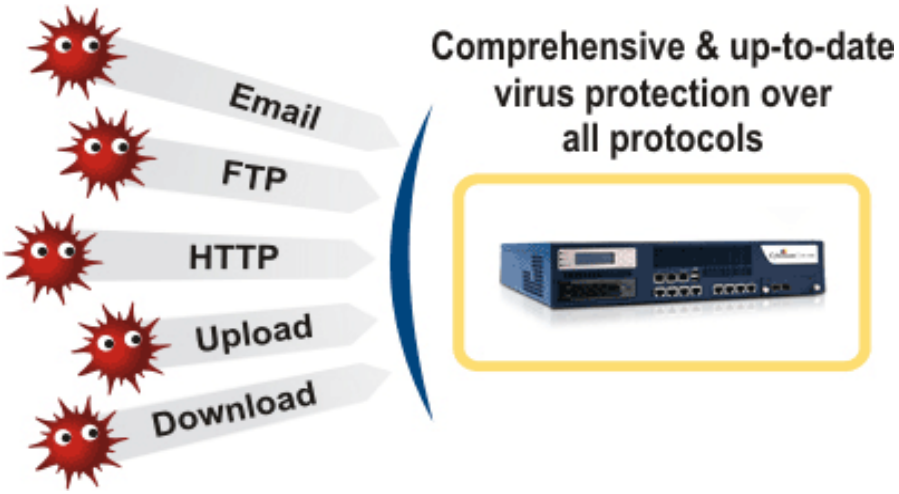
ضدجاسوس افزار و ضدویروس GATEWAY

راهکار ضدجاسوس افزار و ضدویروس Gateway سایبروم، که دارای تأییدیه از موسسه Check Mark است پویش ترافیک Web , Email در محل دروازه برای انسداد ورود تهدیدات آگاهانه و عمدی به شبکه است.

این روش حفاظت بلادرنگ در مقابل انواع کدهای مخرب و جاسوس افزارها از قبیل: ویروسها، کرمها، ابزارهای جاسوسی، backdoor ها،اسب های تروا، keylogger ها وغیره را فراهم می‌کند. تجهیزات VPN دیوارآتش Cyberoam،جهت ارائه راهکار امن‌تر، ترافیک ورودی و خروجی HTTP,FTP, SMTP,POP3,IMAP تجسس می‌کند. با پرداخت هزینه اشتراک لایسنس ضدجاسوس افزار و ضدویروس Cyberoam، از لزوم تهیه اشتراک مجزا برای تک تک کاربران بی نیاز شده و به کمک ماژولهای فیلترینگ محتوا و سیستم جلوگیری از ورود غیرمجاز(IPS)، محافظت پیشگیرانه را برای دفاتر راه‌دور و مرکزی شرکتها ایجاد می‌گردد.آنتی ویروس Cyberoam هر نیم ساعت به روز شده و محافظت آن بر اساس لیست سیاه ولیست سفید و محافظت پویا براساس شناسه کاربر می‌باشد.

ویژگیهای کلیدی

- بازرسی ترافیک پروتکل های .HTTP,FTP,SMTP,POP3,IMAP
- فضای قرنطینه فایل های آلوده در درون دستگاه
- سیاستهای بازرسی بر اساس شناسه کاربر
- گزارشهای ویروس‌های HTTP بر اساس شناسه کاربر



تکنولوژی انحصاری امنیتی بر اساس شناسه کاربر

تجهیزات VPN دیواراتش و ضدویروس دروازه Cyberoam این امکان را فراهم می‌کنند که ایا این کاربرخود مهاجم است یا قربانی؟ شرکتها،بوسیله شناسایی و کنترل کاربر روی ویروسای HTTP که از طریق صفحات وب منتقل می شوند، قادر خواهند بود اعمال پیشگیرانه را با ضدویروس Gateway جهت امنیت بیشتر فراهم‌کنند. ضدجاسوس افزار و ضدویروس Cyberoam به شرکتها اجازه می‌دهند سیاستهای بازرسی متفاوتی را تنظیم کنند تا بتوان بازرسی بهینه شده‌ای را بر اساس نیازهای کاری کاربران فراهم آورند.

امنیت Email

شرکتها میتوانند تعریف کنند که فایلهای ضمیمه قابل اجرا، فایلهای صوتی و تصویری و غیره برای یک کاربرخاص مسدود شود. به علاوه Cyberoam با مسدودکردن فایلهای ضمیمه ای که با کلمه رمز محافظت شده اند، سطح امنیتی و قدرتمندی را برای Email های شرکت فراهم می کند.

قرنطینه‌کردن ویروسها در خود

تجهیزات امنیتی دروازه Cyberoam یک فضای داخلی قرنطینه برای کاربران ایجاد می‌کند تا بتوانند Email های قرنطینه‌شده شان را در فضایی امن بررسی کنند. این ویژگی به همراه قابلیت تهیه پشتیبان از نامه هایی که از قبل دارای گیرنده مشخص هستند، از گم‌شدن نامه های مهم ممانعت کرده و حجم کاری مدیر شبکه را در جستجوی نامه های مخرب کاهش می دهد.

امنیت متمرکزشده

بوسیله کنسول مرکزی Cyberoam شرکتها می‌توانند محافظت بی وقفه‌ای را در دفاتر شعب در مقابل حملات شبکه‌ای حتی با وجود نبودن امکانات فنی تجربه کنند. این کنسول IPS را قادر می‌سازد تا امضاهای انتخابی و سیاست به روز شدن خودکار را از یک مکان متمرکز به سراسر شبکه اعمال کند که این عمل باعث افزایش امنیت دفاتر راه‌دور و شعب به علاوه کاهش پیچیدگی عملیاتی می‌شود.

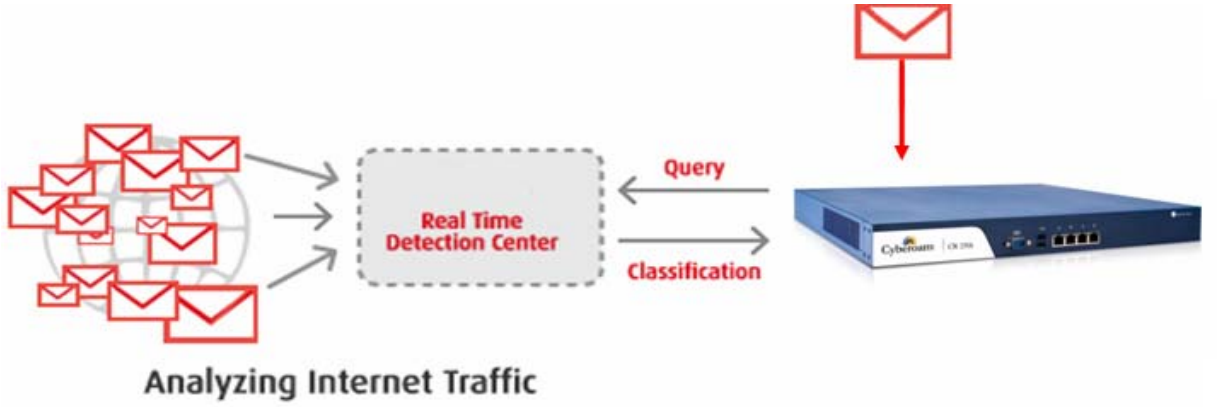
سیستم ضد هرزنامه در سطح GATEWAY

نویسندگان هرزنامه و کدهای مخرب با کمک همدیگر، از Email برای ارسال ویروس استفاده می‌کنند. امروزه Email ها در ۲۳ درصد از تمام شرکتها، محل سرایت Malware هستند. نویسندگان هرزنامه ازتکنیکهای بالایی همچون Zombie botnet ها برای غلبه‌کردن بر تکنولوژی‌های مسدودکننده هرزنامه ها در دزدیدن اطلاعات محرمانه مالی، دارویی و غیره استفاده می‌کنند. بعضی حمله ها به اندازه ای با هدف انجام می‌شود که توسط ضدویروسها و ضدهرزنامه‌های معمولی قابل شناسایی نیستند. شرکتها نیاز به یک مقابله بی وقفه‌ای دارند که نه تنها محافظت بر اساس امضاهای تجاری بلکه با تجزیه و تحلیل سریع محتوا، مبداء و نمونه‌های منتشرشده حفاظت مؤثری را در برابر Malware و هرزنامه ایجاد کنند.

محافظت جامع در برابر هرزنامه

تجهیزات ضدهرزنامه Cyberoam که توسط موسسه معتبر Check Mark موفق به کسب گواهینامه سطح ۵ شده

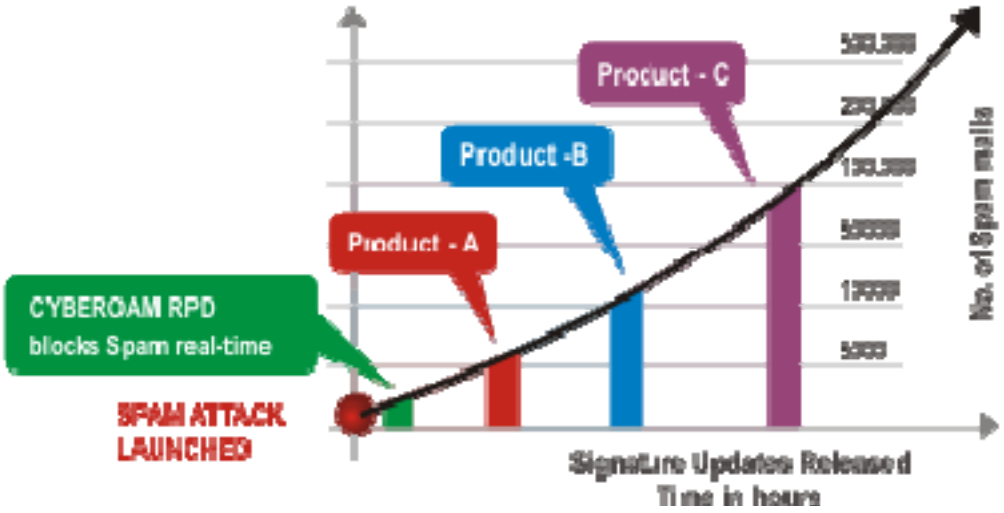
است، یک راهکار قدرتمند پالایش هرزنامه است که می‌تواند میلیونها پیغام را در ثانیه بازرسی کند. با خرید و فعال سازی سرویس اشتراک سیستم ضدهرزنامه، می‌توان به منظور نیل به بالاترین سطح مبارزه با Malware ها، این قابلیت را در کنار تجهیزات پالایش محتوا، سیستم جلوگیری از نفوذ، سیستم ضدجاسوس افزار و ضدویروس Cyberoam، بکارگرفت. ضدهرزنامه Cyberoam نامه‌های ورودی و خروجی را روی پروتکلهای IMAP,SMTP,POP3 بازرسی می‌کند و با پیداکردن خودکار علامتها، هرزنامه‌ها را قرنطینه و مسدود می‌کند. روش ضدهرزنامه ارائه انباری از هرزنامه‌های قرنطینه شده‌است برای در امان ماندن نامه‌های حساس کاری از تخریب شدن است.



پالایش هرزنامه Cyberoam با پشتیبانی ازلیست سفید و سیاه، ویروسها، تروجانها، برنامه‌های جاسوسی، Phishing وتبلیغات مضر راکنترل می‌کند. این کار شرکتها را در برابر فایلهای ضمیمه و عکسهای هرزنامه‌ای مصون نگه می‌دارد. به عبارت دیگر راه‌حل ضدهرزنامه کارایی و کاهش هزینه های پهنای‌باند و ذخیره‌سازی را بهتر می‌کند.

ویژگیهای کلیدی

- بازرسی ترافیک IMAP,POP3,SMTP
- ناحیه قرنطینه هرزنامه
- پالایش تصاویر با تکنولوژی کشف الگوی برگشتی
- نادیده گرفتن محتوا
- نمای محدودی از روبرو شدن



محافظت بی وقفه

در مقایسه با محافظت بر اساس اثر، روش ضدهرزنامه Cyberoam هرزنامه‌های جدید را در ابتدای شروع فعالیتشان با تکنولوژی کشف الگوی برگشتی (RPD) که هرزنامه را از طریق نمونه‌های منتشرشده‌شان تشخیص می‌دهد شناسایی می‌کند. به علاوه RPD با بیرون کشیدن و تحلیل نمونه‌هایی از نامه‌های مربوط، فوران‌های Email ها را برای حمله های بزرگ و کوچک شناسایی می‌کند. نتیجه این است که شرکتها با تجهیزات ضدهرزنامه Cyberoam محافظت در برابر تهدیدات با قالبها و زبانهای مختلف را بدون هیچ نگرانی دریافت خواهندکرد. تکنولوژی جستجوی پیشرفته RPD دیددقیقی از روبرو شدن را برای شرکتها فراهم می‌کند.

شرکتها همچنین می‌توانند با درست‌کردن امضاهای معینی بوسیله سیستم جلوگیری از ورود غیرمجاز (IPS) سایبروم محافظت لحظه‌ای از شبکه‌شان را در برابر حملات داخلی فراهم کنند.

تکنولوژی انحصاری امنیتی بر اساس شناسه کاربر

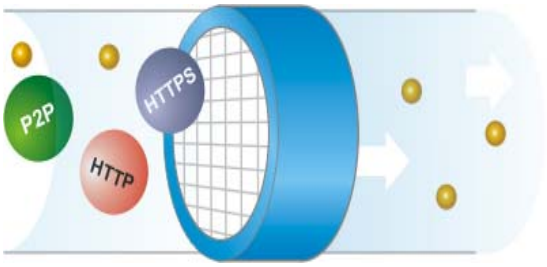
تجهیزات ضدهرزنامه Cyberoamامکان تعریف سیاستهای شدید و ملایم را بر اساس نیازها و محیط‌های کاری کاربر ایجاد می‌کند. پالایش هرزنامه Cyberoam با ارائه کنترلهای قدم به قدم روی مدیریت نامه ها، حجم و موضوع نامه‌ها و غیره انعطاف‌پذیری و امنیت کاری بالایی را فراهم می‌آورد. پالایش جامع هرزنامه Cyberoam با گرفتن گزارش اکثر هرزنامه‌های دریافتی هر شخص، بیشترین فرستنده ها و گیرنده‌های هرزنامه، دید کاملی از ترافیک Email های شرکتها می‌دهند.

گزارش‌گیری و سیاستهای بر اساس شناسه Cyberoam باعث برآورده شدن نیازهای شرکتها می‌شود.

پالایش محتوا

شرکتها به دلیل ورود ویروسها، Malwareها کرمها،تروجانها، ابزارهای جاسوسی و غیره، بدلیل سیاستهای غلط و یا

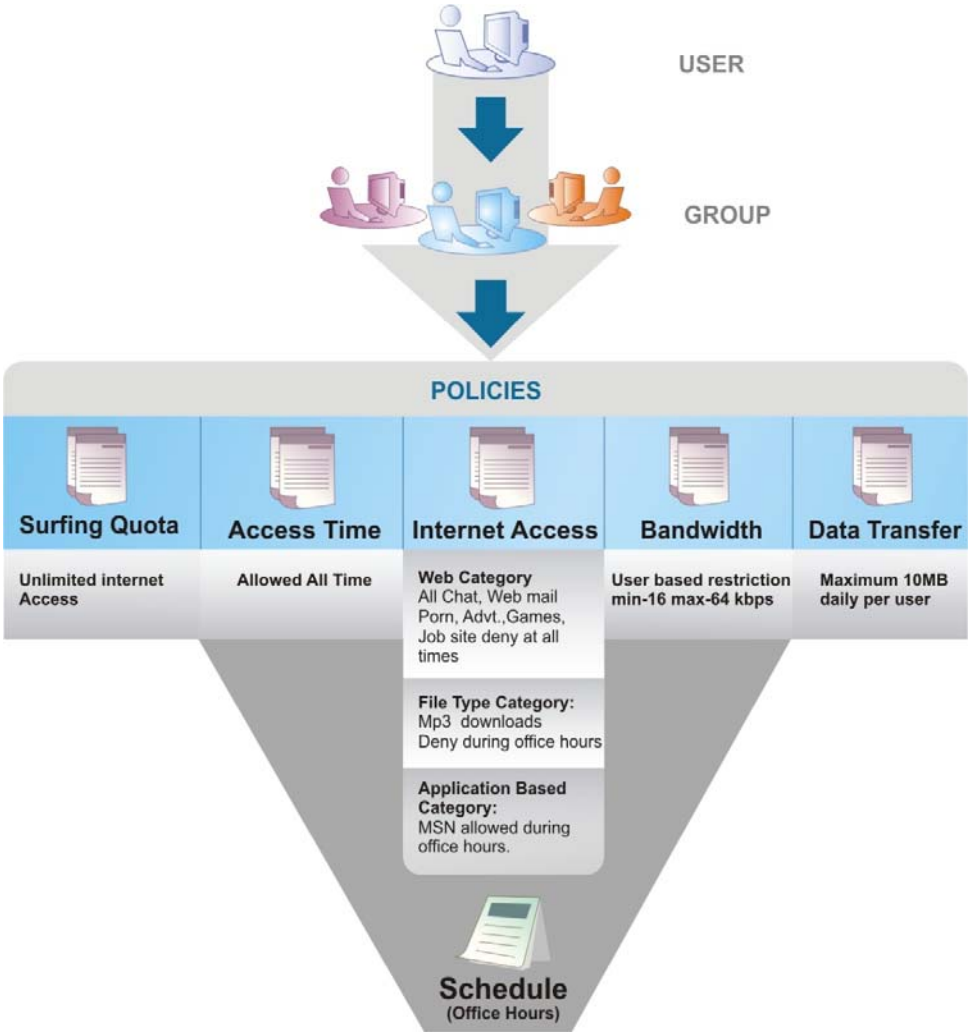
نقص در سیستم امنیتی با حجم زیاد ضرر مالی مواجهند. کلاهبرداریها، سرقت ها و جاسوسی های اینترنتی منجر به فاش شدن کلمات رمز، هویت و از دست‌رفتن اطلاعات محرمانه می‌گردند. مرور و سرکشی بی‌ملاحظه وب سایت ها در اینترنت توسط کاربران داخلی به غیر از کاهش کارایی، شرکت را متحمل آسیب‌های جبران‌ناپذیری می‌کند. استفاده نامحدود از برنامه‌های اشتراک فایل مثل: P2P,IM و دانلودهای صوتی و تصویری سبب خطر نفوذ یا از بین رفتن داده‌ها و همچنین هدر رفتن پهنای‌باند و در نتیجه محدود شدن منابع شرکت می‌شود.



آیا مرور کردن صفحات Web امنیت شبکه را تحت‌تاثیر قرار می‌دهد؟

- آیا کاربران شما به سایتهایی که مملو از کدهای مخرب هستند دسترسی دارند ؟
- یا اینکه برنامه‌های IM,P2P از طریق سرور پروکسی مسدود شده‌اند ؟
- آیا دستگاه شما بخشی از botnet می‌باشد ؟
- آیا پهنای‌باند بوسیله دانلودهای ویدئویی و Mp3اشغال می‌شود؟
- آیا می‌دانید که چه کسی چه چیزی را مرور می‌کند ؟

سیستم پالایش محتوا و برنامه Cyberoam توسط موسسه Check Mark موفق به کسب گواهینامه برترین خدمات شده است. به علاوه اینکه Cyberoam با تجهیزات امنیتی Gateway مثل: دیواره آتش با قابلیت بررسی هوشمند بسته‌های اطلاعاتی و کنترل بر اساس شناسه کاربری، ضدجاسوس افزار و ضد ویروس Gateway، ضد هرزنامه Gateway، سیستم جلوگیری از تفوذ IPS , VPNیا شبکه خصوصی مجازی، محافظت یکپارچه‌ای در برابر کلاهبرداریها، سرقت ها، جاسوسی های اینترنتی، سایتهای حاوی کدهای مخرب و بسیاری دیگر را در کنار سیستم پالایش محتوا و برنامه های خود فراهم می آورد. راهکار پالایش محتوای اینترنت Cyberoam نقش مهمی در اطمینان موسسات آموزشی از رعایت قوانین استانداردی مثل CIPA دارد.



محافظت جامع

پالایش Cyberoam بوسیله بانک اطلاعاتی یکپارچه خود، شامل میلیونها سایت که به بیش از ۸۲ نوع مختلف طبقه‌بندی شده‌اند دسترسی به اینترنت را کنترل می‌کند. WebCat که همان موتور طبقه‌بندی خودکار Web سایبروم است، یکی از بهترین و جامع‌ترین بانکهای اطلاعاتی URL یا آدرس اینترنتی را برای محافظت در برابر تهدیدات ترکیبی دارد. شرکتها می‌توانند با راهکار پالایش Webو برنامه Cyberoam، طبقه‌بندی‌های دلخواه خود را برای گروههای مشخصی از شرکت، جهت پوشش امنیتی دلخواهشان ایجاد کنند.در مقایسه با محصولات دیگر که بانک اطلاعات سایتهای موجود روی سرور می باشد، در سری‌های CR بانک اطلاعاتی Cyberoam، روی خود دستگاه موجود بوده و با کمترین تأخیر، وابستگی به بستر شبکه و خواندن اطلاعات از منبعی دیگر را حذف کرده‌است

پالایش لایه کاربردی (بالاترین لایه مدل OSI) سایبروم به شرکتها این اجازه را می‌دهد تا برنامه‌های کاربردی IM,P2P مثل: Yahoo, Skype, MSN غیره را کنترل کند. انتقال فایل بوسیله این برنامه ها را می‌توان بوسیله سیستم جلوگیری از تفوذ IPS Cyberoam مسدودکرد. شرکتها می‌توانند با ساختن پیامهای دلخواه برای سایتهای

مسدودشده، کاربران را جهت تمرین امنیت، آموزش دهند.

گزارش‌گیری و دسترسی براساس شناسه کاربربا دانستن اینکه " چه کسی چه کار می‌کند"

سیستم پالایش محتوای Cyberoam را می‌توان به گونه‌ای تنظیم کرد تا سیاست دسترسی بر اساس گروه، واحد سازمانی، سلسله مراتب اداری و یا حتی کاربر خاصی ایجادشود. این ویژگی به شرکتها این امکان را می‌دهد تا سیاستهای مختلفی را بر اساس محیط کاری بخشهای مالی، بازاریابی، روابط عمومی و یا براساس نیاز علمی دانشجویان، کارمندان و مدیران مؤسسات آموزشی تعریف کنند.

این کار ثابت می‌کند که Cyberoam امنیت را برای همه افراد فراهم می‌کند.با این روش دسترسی به صفحاتWeb را می‌توان برای یک کاربر خاص از یک گروه در طی دوره‌های خاصی از روز یا هفته و یا ایجاد دسترسی موقت کنترل کرد.

داشبورد Cyberoam دید وسیعی از دسترسی به صفحات Web به همراه گزارش‌گیری سطح کاربر و همچنین‌گزارشهای کاملی از انتقال داده‌ها، برنامه‌های استفاده‌شده، سایتهای دیده شده، موتورهای جستجوی به کارگرفته شده و غیره را ارائه می‌دهد این باعث می‌شود تا شرکتها مرور کردنهای بی‌حاصل و دانلودهای گیرنده پهنای‌باند را که ممکن است شرکت را در برابر کمبود منابع و بدهی قرار دهد کنترل کنند.

تطابق با استاندارد بین المللی CIPA – برای محافظت دانش‌آموزان و دانشجویان

سیستم پالایش قدرتمند Web سایبروم به مدارس و آزمایشگاهها این امکان را می‌دهد تا سیاست ایمنی اینترنت را که استفاده نامناسب از اینترنت را بر اساس قوانین فدرال CIPA پالایش می‌کند به اجرا درآورند. بانک اطلاعاتی جامع صفحات وب و سیاستهای بسیار دقیق بر اساس شناسه کاربری Cyberoam، دانش‌آموزان را از دسترسی به محتواها،Email ها و اتاقهای گفتگوی نامناسب بوسیله پالایش و مسدودکردن دسترسی آنها محافظت می‌کند.

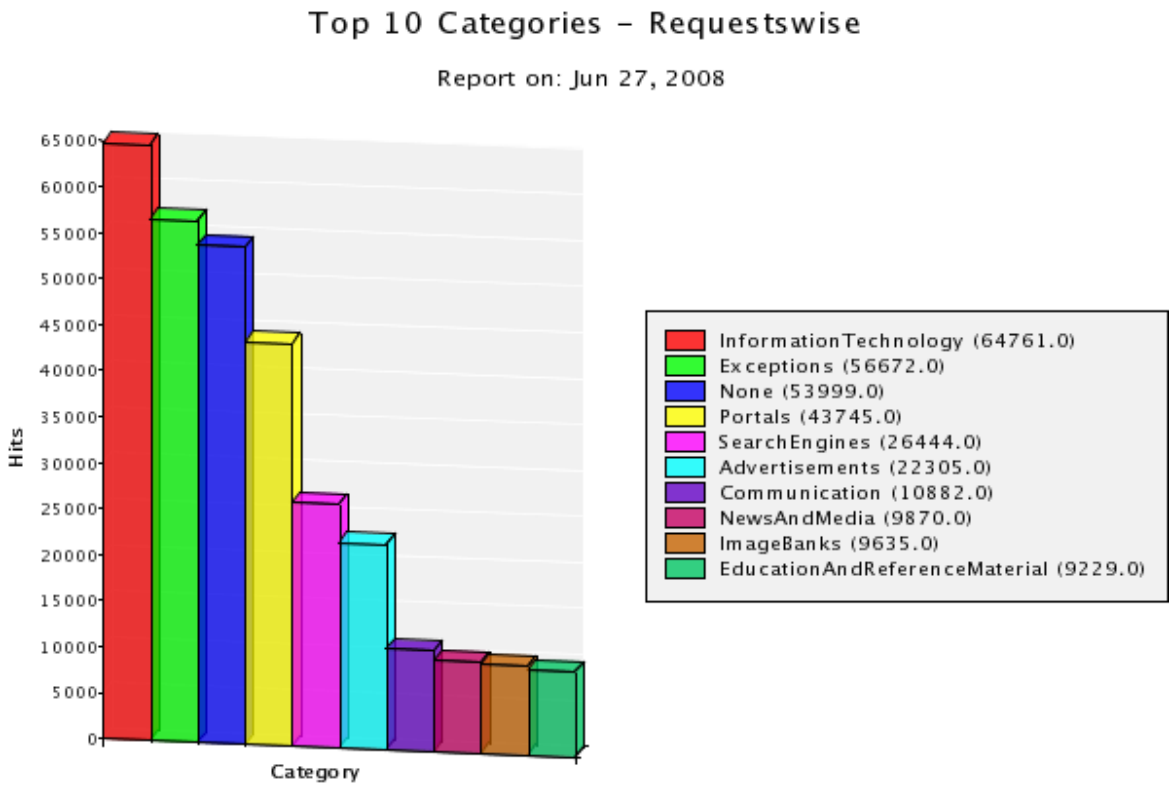
سیستم پالایش محتوای اینترنت Cyberoam نمونه‌های از پیش تعریف شده CIPA که شامل طبقه‌بندی‌های سایت‌های بزرگسالان، سایت های غیر اخلاقی، قماربازی‌ها، خشونت، سایت های غیر کاری، امنیت کامپیوتر و غیره می‌باشد را در خود دارد و مدارس و آزمایشگاهها را قادر می‌سازد تا سیاستهای CIPA را فوراً پیاده‌سازی کنند.

گزارشهای هوشمند

شرکتها نیاز به دید کاملی از نحوه استفاده شبکه و ایجاد امنیت اطلاعاتی برای محافظت بی‌وقفه در برابر تهدیدات ترکیبی دارند. آنچه مهم است، گزارش‌گیری از فعالیت یک‌کاربر خاص، به منظور حصول اطمینان از امنیت آن کاربر در برابر تهدیدات داخلی و خارجی است.

به علاوه راهکارهای امنیتی بدون گزارش‌گیری از فعالیت شبکه، ناقص هستند بنابراین، Cyberoam گزارش‌گیری

براساس شناسه یک کاربر خاص را روی تجهیزات سری CRخود پیشنهاد می‌کند که نیاز به انجام هزینه جداگانه برای راهکارهای گزارش‌گیری را برطرف می‌کند.



وقتی شرکتها تجهیزات CR Cyberoam را به خدمت می‌گیرند، به طور خودکار گزارش‌گیری منحصر بفردی روی این تجهیزات خواهند داشت و تجهیزات امنیتی شبکه Cyberoam، گزارشها را به شکل تحلیلی و مختصر و آماده تفسیر ارائه می‌کند. بدین ترتیب شرکتها قادر خواهند بود تا به سرعت تهدیدات امنیتی روی شبکه را جمع‌بندی کنند و سیاستهای درست و کاملی در جهت اقدامات امنیتی تعریف کنند.

ویژگیهای کلیدی

- داشبورد قابل تنظیم به صورت دلخواه
- نمایش هر گونه تخلف از سیاستهای سازمانی و نفوذ به شبکه
- گزارش‌گیری بر اساس شناسه کاربری-" چه کسی چه کار می‌کند"
- میزان گرایش به استفاده از صفحاتWeb
- گزارش‌گیری از ویروسها و ورودهای غیرمجاز

داشبورد Cyberoam

داشبورد Cyberoam خلاصه‌ای از تمایلات جاری شرکت از قبیل میزان استفاده از سیستمها و پهنای‌باند، ساعات کاری مؤثر، هشدارهای مربوط به ورود غیرمجاز و غیره را همه در یک صفحه بهینه شده ارائه می دهد. این داشبورد با دادن امکان تشخیص نمونه ها و موارد استفاده تهدیدات و همینطور نقاط ضعف و قوت بهره‌وری شرکت، آنها را قادر می‌سازد تا استراتژی امنیتی خود را طراحی و تنظیم کنند. داشبورد Cyberoam با دادن دید و تحلیل سریع از موارد کاربرد اینترنت توسط کارمندان شرکت، آنها را در کنترل داده‌ها و برنامه‌هایی که کارمندان در طی ساعات کاریشان استفاده می کنند یاری می کند.

رعایت قوانین با توانایی گزارش‌گیری بر اساس شناسه کاربری

گزارش‌گیری بر اساس شناسه کاربری نقش مهمی را در نیاز به ردیابی و رعایت‌کردن مقررات بازی می‌کند. با معیار قراردادن شناسه کاربری برای اجازه ورود به شبکه Cyberoam محدوده‌ای از گزارشهای بر اساس شناسه کاربری شامل : مرور کاملی از اطلاعات بدست‌آمده در رابطه با فعالیت کاربر ووقوع تهدیدات جهت اطمینان از رعایت مقررات و ردیابی دوره‌ای ارائه می‌دهد. با ارائه گزارشها بر اساس شناسه درباره دسترسی به اینترنت و برنامه‌ها بوسیله نام کاربری، Cyberoam شرکتها را قادر می‌سازد تا روی فعالیت‌های مورد نظر کاربران حتی در محیطهای DHCP، بی‌سیم واشتراک محیط‌کاری همچون مرکزبهداشت، مؤسسات آموزشی، فروشگاههای زنجیره‌ای، مراکز تلفن و غیره تمرکز کنند.

این ویژگی به شرکتها کمک می‌کند تا نمونه‌ای از تغییرات در نحوه‌کارکردن کاربر شناسایی کنند و بتوانند سیاستهای تنظیم دسترسی کاربر را جهت افزایش سطح امنیت و بهره‌وری تعریف کنند.

برنامه و شبکه

سیستم جستجوی ترافیک Cyberoam با ارائه اطلاعاتی درباره جریان ترافیک جاری شبکه، مدیران را از کاربرد نادرست و احتمال وقوع حمله آگاه می‌سازد.شرکتها می‌توانند روی مقدار استفاده از برنامه‌های اشتراک فایلی همچون IM,P2P که براساس نقل‌و انتقال داده‌های کاربر ایجاد شده‌اند کنترل داشته‌باشند.آنها همچنین می‌توانند با جداکردن سیستمهای ایجاد کننده تهدید، کنترل عمل دستگاهها و کاربرانی که اشغال‌کننده پهنای‌باند هستند گرفته و پهنای‌باند لازم را به کاربران و برنامه‌هایی که دارای حساسیت هستند اختصاص دهند.