ارتباطات و فناوری اطلاعات

فاواموج

FAVAMOUJ ICT Co.

100%

Customer Satisfaction
Guaranteed

100%

پیوندی ماندگار از
تخصص + تعهد

شرکت فاواموج

فنـــاوری نوین . ارتبـــاط پـــایدار

ICT TOTAL SOLUTIONS

ارتباطات و فناوری اطلاعات

فاواموج

راه حل های برتر در تکنولوژی های به روز دنیای ارتباطات برای کسب وکار امروز و آینده

فاواموج شرکتی متمرکز بر خدمات مهندسی ارتباطات و بازرگانی حرفه ای است.

تیم متخصص و حرفه ای، ساختار و سازمان توانمند، بهره گیری از ابزار و امکانات مناسب، تمرکز بر تحقیق و توسعه کاربردی، توجه به نیاز مشتری و رضایت او، تلاش شبانه روزی و روحیه همکاری، همواره از ویژگی های فاواموج بوده است.

شبکه و ارتباطات، ارتباطات یکپارچه (UC)، مدیریت و امنیت ارتباطات، سرویس ها و نرم افزارهای ارتباطی، به عنوان محورهای اصلی فعالیت شرکت معرفی شده اند.

از مهمترین راه حل های شرکت می توان به راه حل ممیزی ادمین ها، مراکز تلفنی آی پی، راه حل وب کنفرانس و ارتباط یکپارچه، راه حل کشینگ برای سرویس دهنده های اینترنت، احراز هویت دو عاملی و راه حل جامع دیتاسنتر اشاره کرد.

فاواموج همواره تلاش نموده تا برای مشتریان دوست داشتنی خود، مشاوری صدیق و امین باشد و تمام توان خود را به منظور موفقیت آنهادر کسب و کار خویش، به کار برده و خواهد برد.

Business Area

دیدگاه و اهداف :

مدیریت شـــرکت با درک این واقعیت که فاواموج باید بتواند در سازمان مشتریان خود جایگاهی مؤثر کسب نماید ، چشم انداز شرکت را ترسیم نموده است .

ایجاد توانمندی روزآمد ، منعطف و منطبق با بازار هدف ، ارائه صادقانه تصویر این توانمندی و جلب اعتماد همه جانبه مشتری در تمام سطوح ، زمینه ساز حضور شرکت در سازمان مشتری خواهد بود .

شناختی که طی چندین سال تجربه از نیازهای مشتریان بدست آمده است مبنای تدوین اهداف شرکت فاواموج بوده است. مهمترین این اهداف به شرح زیر می باشند:

* **دستیابی به جایگاه برتر در ارائه خدمات مهندسی ارتباطات و شبکه ، بازرگانی و تأمین تجهیزات و اجرای پروژه های مربوطه**
* **کســـب توانائی ارائه راه حل های جامع و نوین ارتباطات و مشـــارکت در ارائه راه حل های جامع فناوری اطلاعات و ارتباطات**
* **ایجاد توانمندی تأمین تجهیزات و پشتیبانی شبکه و ارتباطات در سطح ملی**
* **فعالیت جدی به عنوان ارائه کننده برتر سرویس های مجازی و ارزش افزوده در بستر ارتباطات**

زمینه های فعالیت شرکت :

۱ - زیرساخت های ارتباطات و شبکه داده ها

۲ - امنیت و مدیریت جامع ارتباطات و شبکه داده ها

۳ - آی پی تلفنی ، مراکز تماس و ارتباط یکپارچه

٤ - زیرساخت های فیزیکی و فاوای مراکز دیتا

۵ - کشینگ اینترنت برای سرویس دهنده های بزرگ و اپراتورهای ارتباطی

۶ - سرویس ها و نرم افزارهای یکپارچه با شبکه

FAVAMOUJ ICT

ارتباطات و فناوری اطلاعات
فاواموج

ممیزی ادمین ها با Shell Control Box (SCB)

امروزه و با پیشرفت تکنولوژی و گسترش روز افزون IT در انجام کارها و با حجم وسیع سرورها و گسترش دیتاسنترها ، سرورها و تجهیزات کاربردی سازمان به ندرت به صورت محلی مدیریت می شوند. با توجه به اینکه اغلب سرورها از راه دور و توسط پروتکلهایی نظیر SSH (یونیکس) و RDP (ویندوز) مدیریت می شوند، عملیات ممیزی و پایش کمی دشوار خواهد شد.

به منظور ممیزی قابل اطمینان برای جمع آوری اطلاعات ممیزی باید نسبت به سرورها و کلاینت ها، به صورت Transparent و مستقل عمل کنیم، زیرا در غیراینصورت یک ادمین ماهر و یا یک هکر قوی می تواند به گونه ای عمل کند که هیچ اثری از کارهایی که انجام داده یا اتفاقات دیگر باقی نگذارد.

راه حل SCB (Shell control Box) شرکت فاواموج ، یک لایه مجازی ممیزی (Auditor layer) تعریف می کند. در این لایه در واقع دیده بانی فعالیت های ادمین های سیستم انجام می شود و هیچگونه حساسیتی در کار سازمان بوجود نخواهد آمد .

BalaBit IT Security
بالابیت

*SCB تجهیزی است که با پایش فعالیتها، دسترسی به سرورهای راه دور و کامپیوترهای مجازی یا تجهیزات شبکه را کنترل نموده و فعالیت کاربرانی که به این سیستم ها دسترسی دارند را به صورت تریل های شبه ویدئو ضبط می کند.

برای مثال اگر ادمین های سیستم در حال تغییر اطلاعات سرورهای بانک اطلاعاتی از طریق پروتکل SSH و یا انجام تراکنش از طریق Thin Client با استفاده از پروتکل VM Ware View باشند، SCB فعالیت آنها را ثبت می نماید.

ویژگی ها و کاربردها:

- نظارت برادمین ها و ضبط فعالیت های مدیریتی آنها برروی سرویس دهنده ها
- کنترل SSH (شامل X11 و ترافیک های هدایت شده در SSH) ، RDP 5 ، RDP 6 ، RDP 7، VM Ware View ، VNC ، Telnet ، TN 3270 Connection
- نظارت برارتباطات SCP ، SFTP و لیست کردن فایل ها و استخراج آنها
- جمع آوری اطلاعات قابل استفاده در مراجع قضایی
- دسترسی قابل اعتماد به سرورها و تریل های ممیزی
- کاملا جدا از سرورها و کاربران (Out-of-band)
- انطباق آسان با زیرساخت شبکه
- دسترسی به سرورهای حساس فقط با تائید مجوز دهندگان
- پشتیبانی از قابلیت دسترسی بالا (High Availability)

RCII

دارای گواهی سطح بلوغ امنیتی از
مرکز تحقیقات صنایع انفورماتیک

بدلیل گسترش روزافزون دسترسی های راه دور و گستردگی راه حل های Cloud و همچنین عدم توانایی مدیران در کنترل تمامی فعالیت های ادمین ها ، تمامی سازمان ها نیازمند راه حل جامع و کاملی می باشند تا بتوانند مخاطرات خود را از قبال دسترسی های گوناگون برطرف کنند. بدین منظور محصول Shell Control Box شرکت فاواموج اهمیتی ویژه یافته است.

General Brochure

واحد طرح و ساخت دیتاسنتر:

بخش دیتاسنتر فاواموج در سال ۱۳۸۵ فعالیت خود را با تکیه بر پرسنل متخصص و باتجربه و همچنین گردآوری دانش روز دنیا در این حوزه آغاز نموده و هدف اصلی شرکت فاواموج در این بخش، تلاش در جهت ارتقاء سطح آشنائی بیشتر کارفرمایان با استانداردها و روش‌های بهینه پیاده‌سازی دیتاسنترها و هدف‌گذاری در خصوص معرفی دیتاسنتر به عنوان یک صنعت و تلاش در تبیین و ارائه راهکارهای حفظ و سلامت انرژی دردیتاسنترها.

شـــرکت فاواموج در راستای رسیدن به اهداف تعریف شده فوق علاوه بر مطالعات و جمع آوری اطلاعات جامع در این صفت، در سال ۲۰۱۰ اقدام به اعزام پرسنل شرکت در کلاس‌های طراحی و کارشناسی پیاده‌سازی دیتاسنتر با شرکت epi نموده است و علاوه بر ارتقاء سطح دانش پرسنل شرکت اقدام به ایجاد کنسرسیوم با شرکت‌های مرتبط با این حوزه نموده است که در زیر نام برده شده است:

* واحد مهندسی دیتاسنتر
* واحد معماری و ساختمان دیتاسنتر
* واحد برق با همکاری شرکت برق پاسارگاد و شرکت نوین آریاپترونیر
* واحد سرمایش با همکاری شرکت نیکان صنعت سردسان و شرکت تهویه نیا
* واحد ایمنی ، اعلان و اطفاء حریق با همکاری شرکت آرون
* واحد سیستم‌های امنیتی و نظارت تصویری با همکاری شرکت وگا
* واحد شیلد الکترومغناطیس با همکاری شرکت فاتحین صنعت شریف

فعالیت های بخش دیتاسنتر فاواموج :

خدمات مهندسی زیرساخت و دیتاسنتر:

- انجام مطالعات امکان‌سنجی ، توجیهی فنی و اقتصادی دیتاسنترها و تعیین مکان
- مشاوره، طراحی مقدماتی، طراحی جزئیات ، تهیه مشخصات فنی و ارزیابی فنی و مالی پروژه
- مدیریت پروژه، برنامه‌ریزی و کنترل پروژه های دیتاسنتر
- انجام خدمات ممیزی بر طراحی (Design Assessment and Validation)
- بررسی و ارائه گزارش ممیزی (Audit) در بخش‌های (پیاده‌سازی و بهینه‌سازی سایت‌های در حال کار)
- ارائه روش پشتیبانی از دیتاسنتر بر اساس استاندارد TIA-۹۴۲
- همکاری در اخذ گواهینامه Tier از مراجع ذیصلاح (epi)
- نظارت و مهندسی کارگاهی در مرحله ساخت دیتاسنتر

ساخت و اجرای زیرساخت و دیتاسنتر:

- اجرای پروژه‌های زیرساخت فیزیکی مراکزداده
- اجرای دیتاسنترها و اتاق سرورهای کانتینری
- تغییر کاربری ، مقاوم سازی و اجرای اتاق سرور
- تولید و ساخت سیستم سرمایش با تجهیزات استاندارد (Chiller ، IN Row و CRAC)
- تولید و ساخت تابلوهای برق بر اساس مشخصات مورد نیاز دیتاسنتر

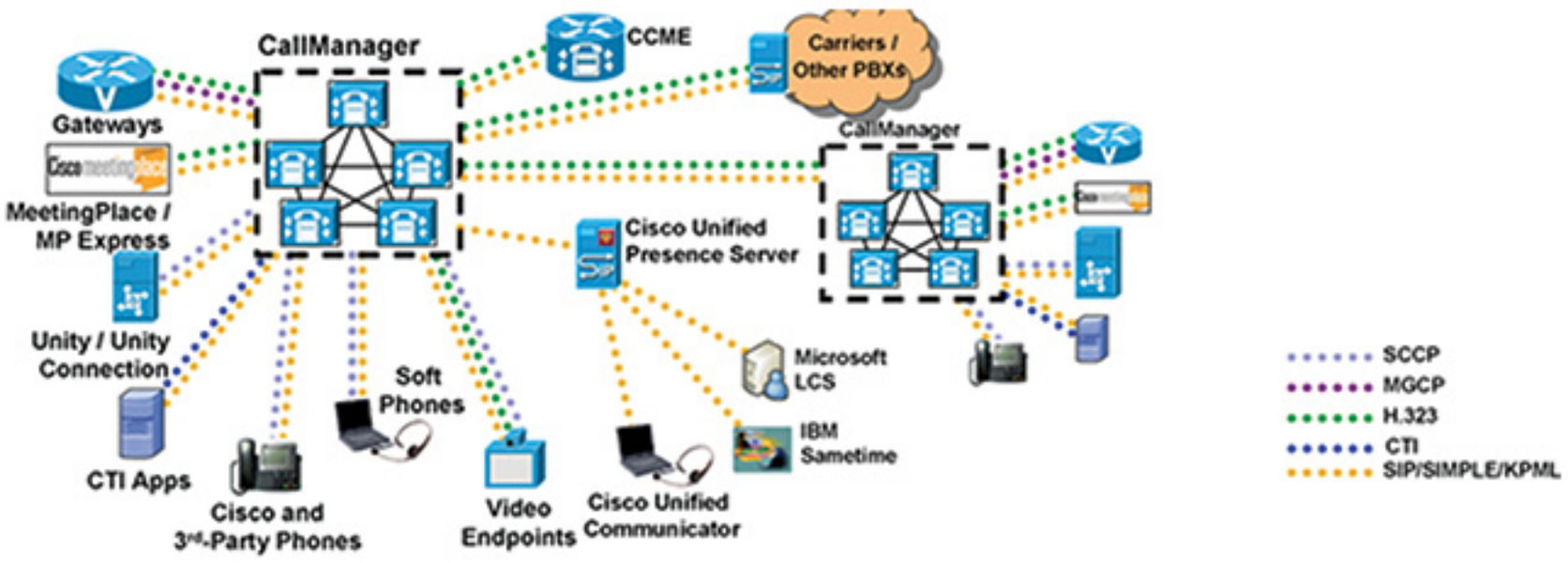
گواهی نامه های اخذ شده در بخش دیتاسنتر فاواموج :

BICSI Member | CDCP (Certified Data Centre Professional) | CDCS (Certified Data Centre Specialist)

CISCO IP-Telephony

امروزه با گسترش روز افزون کسب و کار در زمینه هاي مختلف و پراکندگي هاي جغرافياي سازمان ها، ارتباطات نقش عمده اي را در توسعه کسب وکار و ميزان بازدهي هرسازمان برعهده دارد. با توجه به توسعه واسطهاي ارتباطي اعم از: تلفن، مکاتبات (E-Mail و فکس) و اطلاعات که عموما درقالبهاي اسناد و داده ها و اطلاعات درون نرم افزار هاي مختلف مبادله ميشوند، تعداد اين واسط ها هر روز در حال افزايش است.

شرکت فاواموج دارای تجربه چندین ساله در پیاده سازی راه حل های Ip_telephony با استفاده از Cisco call manager و ادغام آن با سایر محصولات سیسکو جهت ارائه سرویس های ارزش افزوده می باشد.



*معرفی محصول Cisco call manager:

Cisco call manager محصول اصلی مجموعه IPTشرکت سیسکو میباشد ، این نرم افزار نقش اصلی مدیریت و کنترل تماس ها را به عهده دارد.

بسیاری از سازمان ها و موسسات نیاز به ابزاری به منظور مدیریت و گزارش گیری از تماس ها ،کم کردن هزینه تماس ، امکان استفاده از سرویس های ارزش افزوده در خارج از سایت خود ، مدیریت ارتباط با مشتری و دیگر امور مربوطه دارند ، Cisco Call manager همراه با سایر محصولات سیسکو اعم از Unity Connection و Cisco Media sense ، Cisco webex ، Cisco Contact Center و...ابزارهایی بدین منظور می باشند.

VoIP (Voice over IP) فناوري ارسال صدا بر روی بستر شبکه داده با استفاده از پروتکل IP است. مزاياي استفاده از چنين روشي کمابيش بر همگان روشن است. راه‌حل‌هاي تلفني مبني بر IP (IP Telephony Solution) حاصل مستقيم اين فناوري است. سيسکو بعنوان شرکت پيشرو، راه حل جامع(CUCS) Cisco Unified Communication System را ارائه نموده است.

از ویژگی سرور کنترل تماس سیسکومیتوان به موارد زیر اشاره کرد:

- امکان برقراری ارتباط VoIP بین شعب یک سازمان و هرسازمان دیگرتحت پروتکلهای استاندارد و از طریق بسترهای شبکه موجود نظیر Fiber،MAN، WAN، Wireless، MPLS، VSAT،باعث کاهش هزینه مکالمات و بازگشت سرمایه می گردد.
- امکان توسعه راه حل جهت برقراری ارتباطات Voice Over IP برروی بستراینترنت و کاهش هزینه های مکالمات بین شهری و بین المللی وجود دارد.
- برقراری ارتباط با شبکه مخابرات(PSTN) از طریق خطوط آنالوگ(FXO) و خطوط E1 PRI با قابلیت DID (Direct Invard Dialing) ، با استفاده از روترها و Access server های سیسکو باظرفیت دلخواه امکانپذیر است.
- وجود Redundancy در سیستم مرکزی مدیریت تماس ها (Call Manager)، بسترشبکه و Voice Gateway ها ، در دسترس بودن(Availability) و قابلیت اطمینان(Reliability) راه حل IP-Telephony را بسیار بالا می برد.

- امکان یکپارچگی VoIP با قابلیتهای سوئیچها و روترهای Cisco نظیر RSVP Agent ،AutoQoS و ... به صورت هوشمندانه کیفیت سرویستهای Voice را بر بستر IP فراهم می کند.
- امکان Real Time Monitoring Tool مانیتورینگ بهنگام سرویس IP-Telephony و اطمینان از صحت و کارایی مطلوب سیستم را فراهم می کند.
- ارائه صفحه وب اختصاصی برای هر کاربر جهت شخصی سازی تلفن و دفترچه تلفن شخصی
- امکان ارائه سرویس AAA برای تماسهای کاربران با استفاده از Radius Server و فعال کردن پروتکل Radius بر روی Voice Gateway وجود دارد.
- یکپارچگی با Microsoft Exchange جهت پشتیبانی Fax-over-IP تحت پروتکل T.38 امکانپذیر است.
- امکان استفاده از کلاینتهای متعدد ممکن می باشد نظیر:
  - IP-Phone های Cisco و غیر Cisco (sccp,SIP)
  - Soft Phone توسط Cisco IP Communicator
  - Web Conferencing، Voice mail ، Voice ، Video ، Instant messaging به صورت
  - یکپارچه بر روی PC توسط Jabber windows و قابلیت ارئه روی Smart phone ها
  - گوشی های موبایل توسط Cisco jabber بر روی سیستم عامل های ios و اندروید
  - گوشی های WLAN ، IP Phone تحت استانداردهای 802.11a /b /g
  - گوشی های Dual-mode نوکیا سری E به صورت عنوان WLAN IP Phone تحت استانداردهای 802.11a /b /g
  - Cisco Unified Video Advantage جهت برقراری کنفرانس تصویربرداری P2P به صورت یکپارچه با IPTelePhony.

سیسکو

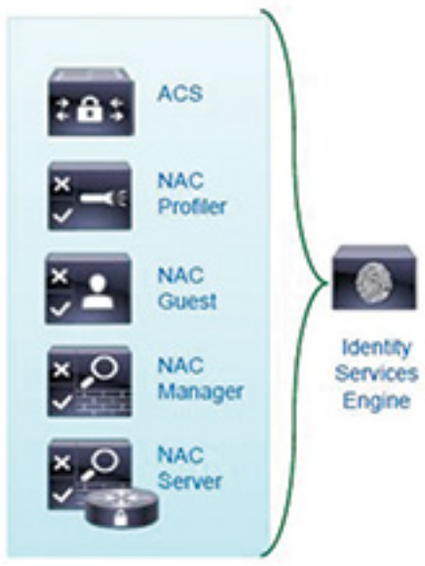
مرکز تلفن سیسکو
(Cisco IP-PBX)

سرویس ها و امکانات متنوع دیگری نیز توسط این محصول ارائه شده است ومطالب عنوان شده تنها بخشی از امکانات سرویس IPT شرکت سیسکو می باشد. علاوه برآن امکان استفاده از تمام سرویس های فوق حتی د رخارج از سایت و با امنیت بالا (جهت جلوگیری از شنود و نفوذ پذیری به داده های صدا) در خارج از سایت نیز با استفاده از راه حل های سیسکو امکان پذیر می باشد که برای شرکت هایی که گستره جغرافیایی خدمات آن روز به روز درحال افزایش می باشد کاربردی است.

راه حل ISE (Identity Service Engine)

با توجه به معرفی مفهوم (Bring Your own Device) و اهمیت ایجاد امنیت در شبکه های کامپیوتری شرکت ها و سازمانها، شرکت سیسکو درصدد آن برآمده است که محصولی را به صورت یکپارچه و ترکیبی از محصولاتی که تا کنون به بازار عرضه کرده است همانند (NAC ،ACS) تولید و به بازار معرفی نمایند.

بر این اساس محصول (Identity Service Engine) ISE در سال 2012 به بازار معرفی شد که علاوه بر ویژگی های محصولات قبلی یک سری ویژگی های جدید هم به آن اضافه شده است. عملکرد اصلی این سیستم بر پایه پروتکل استاندارد Radius می باشد که با استفاده از احراز هویت کاربران و تعیین سطح دسترسی آنها امکان اعمال سیاست های مختلف را برای انواع کاربران در بسترهای گوناگون (VPN-Wired-Wireless) فراهم می سازد.



کارکرد اصلی محصول ISE:

امروزه در سازمان های مختلف، کاربران تجهیزات شخصی خود را وارد شبکه می نمایند لذا باید سیستمی وجود داشته باشد که از دسترسی کامل آنها به تمامی بخش های شبکه جلوگیری نماید و در صورتیکه به دسترسی بیشتر هم نیاز باشد بتوان آن را مدیریت و کنترل نمود. از طرف دیگر تجهیزات مختص به شرکت و سازمان نیز باید از لحاظ امنیتی کنترل و مدیریت شوند زیرا به دلیل استفاده آن توسط کاربران و کارمندان سازمان می تواند بستر مناسبی برای ورود ویروس ها و تهدیدهای امنیتی به شبکه باشد. سیستم ISE این امکان را فراهم می سازد که تمامی موارد امنیتی بررسی و ارزیابی شوند و در صورت نبود تهدید و خطری برای شبکه دسترسی در سطوح مختلف فراهم شود.

ویژگی ها:

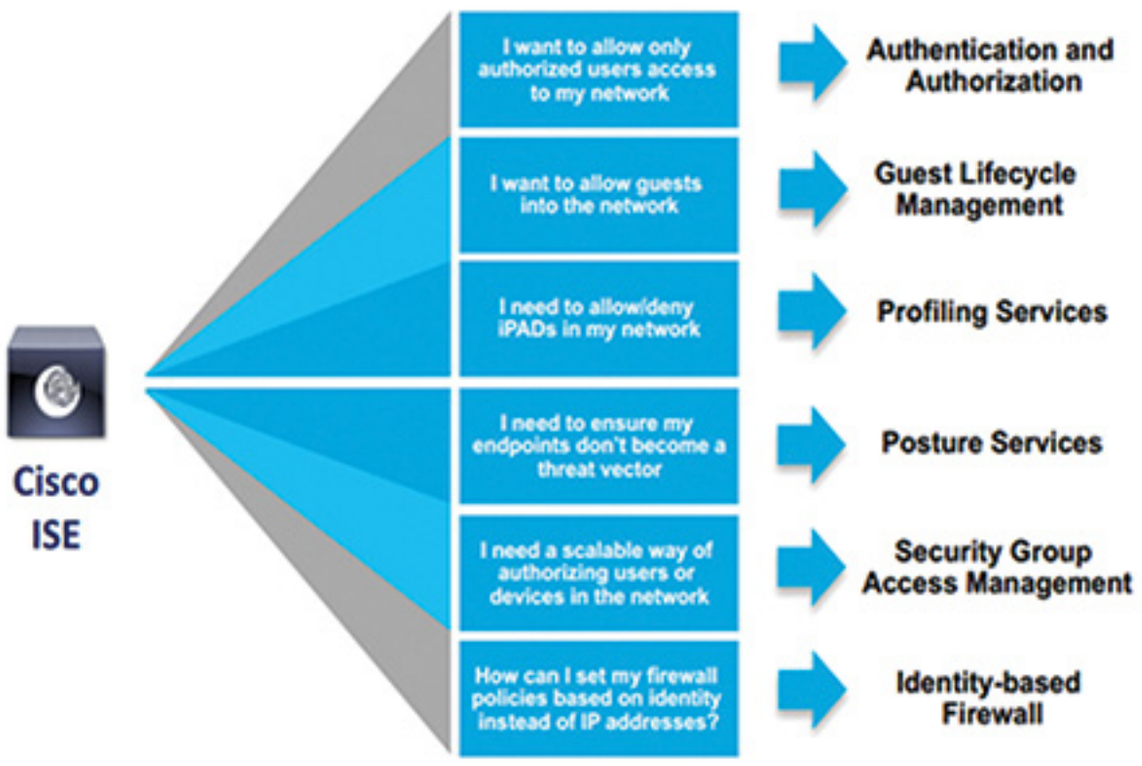
ویژگی هایی که سیستم ISE در اختیار ما قرار می دهد براساس تفکیک به موارد به شرح ذیل می باشد:

- AAA Protocol: استفاده از استاندارد RADIUS ، جهت بهره مندی از Authentication ،Authorization ،Accounting
- Authentication Protocols: پشتیبانی از یک سری پروتکل های مشهور احراز هویت TLS ،EAP ،MS-CHAP ،PAP- و ...
- Policy Model: پشتیبانی از مدل سیاست گذاری قانونمند و ویژه برای ایجاد سیاست های کنترل دسترسی
- Access Control: ایجاد یک سری مکانیزم های کنترل دسترسی، شامل لیست های کنترل دسترسی قابل دانلود (dACL)، انتصاب Vlan، تغییر مسیر URL ، SGA tagging leveraging (مخصوص دستگاه های تحت شبکه سیسکو).
- Profiling: وجود الگو های از پیش تعریف شده یا ایجاد شده توسط راهبران شبکه برای دستگاه های مختلف جهت تشخیص و طبقه بندی محصولات مختلف موجود در بازار
- Guest lifecycle management: فعال سازی مدیریت کلی زمان دسترسی کاربران خارجی و مهمان، که بوسیله آن کاربران مهمان زمان مشخصی برای دسترسی به شبکه خواهند داشت. راهبران شبکه می توانند براساس نیاز سازمان آن را سازماندهی نمایند.
- Posture: بررسی وضعیت تمامی کاربران متصل به شبکه. این فعالیت از طریق یک عامل Client-Base یا یک عامل تحت وب انجام می شود تا صحت تأییدیه یک دستگاه را بررسی نماید. امکان توانایی ایجاد سیاست های قدرتمند که شامل بررسی بسته های به روز رسانی، رجیستری ها و نرم افزار ها
- Endpoint protection service: مجوز اعمال سریع اقدام های خاص مانند (Quarantine ،Un-Quarantine ،or Shutdown)، در مواقع بحرانی و حساس بلادرنگ که در کاهش خطر و افزایش امنیت نقش موثری خواهد داشت.
- Centralized management: مدیریت متمرکز برای راهبری سیستم از طریق یک کنسول تحت وب

- Monitoring and Troubleshooting: وجود کنسول تحت وب برای مدیریت سیستم و گزارش گیری بلادرنگ از سیستم های فعال در شبکه.
- Platform Options: این سیستم برروی سه نوع دستگاه فیزیکی با ظرفیتهای مختلف و سیستم مجازی ارائه می شود.
- Endpoint Protection Service: سرویسی است که برای مانیتورینگ و کنترل تجهیزات نقطه پایانی راه اندازی می شود. با استفاده از این سرویس می توان تجهیزات را، مانیتور کرد و مجوز دهی به آنها را بدون تغییر کلی در حالتی که به شبکه متصل هستند تغییر داد.
- Common access Card Support: یک امضای تشخیص با تراشه الکترونیکی است که شامل یک سری گواهینامه X.509 می باشد و برای تعیین هویت اپراتور به کار می رود. بدین صورت که ابتدا یک کارت به رایانه متصل شده و گواهینامه ها از کارت وارد محیط ویندوز می شود و سپس اجازه دسترسی به محیط وب ISE صادر خواهد شد.
- Internationalization and Localization: امکان تغییر زبان کل سیستم وجود دارد تا برای راهبران امکان درک مفاهیم و مدیریت بهتر فراهم شود.
- IOS sensor for profiling: در انواع شبکه ها ، برای جمع آوری اطلاعات گوناگون از تجهیزات شبکه از پروتکل های DHCP , LLDP , CDP استفاده می شود . این قابلیت در ISE وجود دارد که با استفاده از پروتکل های ذکرشده به جمع آوری اطلاعات از تجهیزات شبکه بپردازد و برای آنها براساس نوع و مدل آنها پروفایل ایجاد کند . بنابراین با استفاده از پروفایل های تهیه شده می توان به راحتی سیاست های گوناگون را برروی آنها اجرا کرد .
- NMAP Probe: نرم افزار NMAP (network Mapper) با سیستم ISE یکپارچه سازی شده است، با استفاده از این قابلیت پروفایل سازی در ISE افزایش می یابد. و علاوه برآن قابلیت شناسایی تجهیزات امکان پذیربوده و می توان پروفایل های مختلفی به خصوص برای انواع موبایل ها ایجاد کرد.
- OCSP Support: با استفاده از این قابلیت می توان با سرورهای بررسی وضعیت گواهینامه های آنلاین موجود برروی اینترنت در ارتباط بود تا از این طریق از معتبربودن X.509 digital certificates ها آگاه شد.
- External Authentication for Administrator Users: قابلیت ایجاد احراز هویت خارجی با استفاده از سیستمهایی مانند LDAP, RSA OTP که به دو طریق زیرمی باشد ، وجود دارد:

1- External authentication + External authorization

2- rnal authentication + Internal authorization



ضرورت به کارگیری ISE:

با توجه به اهمیت ایجاد امنیت ، مدیریت آن و بررسی تمامی ارتباطات و اتصالات داخا یک سازمان نیاز به این سیستم از اهمیت بالایی برخوردار می باشد. ویژگیهای معرفی شده توسط این سیستم این امکان را برای ما ایجاد می کند که بردسترسی تمامی کاربران، تجهیزات و مهمان ها یک سازمان مدیریت و کنترل کامل داشته باشیم و در صورتیکه تهدید یا مشکلی در شبکه ایجاد شد بتوانیم آن را تشخیص و ردیابی نمائیم و یا در کوتاه ترین زمان ممکن از آن جلوگیری کنیم.

راه حل جامع SSL-VPN

انتقال داده از طریق اینترنت نیازمند امنیت می باشد. شبکه‌ی خصوصی مجازی VPN (Virtual Private Network) راهکاری است که می‌توان با استفاده از آن ارتباط یک کاربر با یک شبکه خصوصی را در بستر یک شبکه‌ی عمومی به‌صورت امن فراهم کرد. این ویژگی همچنین در بستر شبکه داخلی و برای برقراری ارتباط امن با سرورها و تجهیزات مهم سازمان نیز مورداستفاده قرار می گیرد.

با استفاده از تکنولوژیهای VPN امروز سازمانها میتوانند به طور موثر به هر کسی مجوزهای لازم را بدهند تا بتوانند از هر جایی و در هر زمانی برای پیشبرد کارها و پشتیبانی های مورد نیاز به منابع سازمان دسترسی پیدا کنند.

VPN ها به دلایل زیر به عنوان یک راه حل منطقی برای دسترسی از راه دور انتخاب میشوند:

- ارائه امکان برقراری ارتباطات امن با مجوزهای دسترسی مناسب برای کاربران خاص، از جمله کارمندان سازمان، پیمانکاران، و یا شرکا
- افزایش بهره وری با گسترش شبکه شرکتها به خارج از سازمان
- کاهش هزینه های ارتباطات و افزایش انعطاف پذیری

برای این منظور علاوه برامنیت بسترعبور اطلاعات با استفاده از تونلهای رمزشده، مدیران سازمان باید از اعمال مجوزهای مشخص به هر فرد و امنیت احراز هویت افراد در دسترسی به اطلاعات سازمان نیزاطمینان کافی داشته باشند تا هرکس نتواند با نام کسی از خانه یا هرجای دیگر به اطلاعات سازمان دسترسی پیدا کرده و سازمان را مورد حمله و آسیب قرار دهد.
این دسترسی به سرورها و اطلاعات حساس در سازمان نیازمند یک راهکار بینقص و غیرقابل نفوذ است در این خصوص استفاده از 2FA یا احراز هویت چند عاملی یک لایه امنیتی اضافی برای دسترسی از راه دور فراهم می آورد تا از دسترسی کاربران غیرمجاز به دارایی های شبکه جلوگیری به عمل آورد.

با استفاده از احراز هویت چند عاملی و تکنولوژی OTP میتوان امنیت ورود کاربر به سیستم را تامین نمود و این اطمینان را فراهم آورد که فقط کاربران مجاز امکان دسترسی به سیستم را داشته باشند.

با استفاده از SSLVPN امکان اتصال به‌تمامی سرورها با استفاده از مکانیسم‌های احراز هویتی قوی وجود دارد و نیزاین امکان وجود دارد تا فقط ترافیک سرورها وارد تونل کاربران شود و مابقی ترافیک کاربراز قبیل ترافیک اینترنت وارد تونل نخواهد شد. در این راه حل می‌توان هم از نرم‌افزار کلاینتی استفاده کرد هم از طریق وب به VPN وصل شد. هرنرم‌افزار کلاینتی که برای دسترسی به برنامه‌ها از طریق SSLVPN موردنیاز باشد می¬تواند در صورت لزوم به‌صورت داینامیک دانلود شود و در نتیجه نیاز به پشتیبانی را به حداقل برساند.

راهکار احراز هویت چند عاملی که به صورت یکپارچه با SSLVP برای احراز هویت کاربران VPN مورد استفاده قرار میگیرد از حداقل دو فاکتور برای احراز هویت استفاده میکند. این فاکتورها می تواند شامل اطلاعاتی باشد که کاربر می‌داند مثل پسورد یا PIN به‌عنوان فاکتور اول و چیزی باشد که کاربر دارد مثل Token و کدی که روی Token به صورت تصادفی تولید می‌شود.

- از ویژگی‌ها و کارآیی های راه حل SSLVPN به صورت یکپارچه با MFA می‌توان به موارد زیر اشاره کرد :
- ارتباط آسان از دسکتاپهای غیر سازمانی
- عدم نیاز به پشتیبانی و نگهداری نرم‌افزار دسکتاپ
- قابلیت داینامیک بودن و به روز رسانی اتوماتیک نرم افزار دسکتاپ
- امکان ایجاد پورتال های وب سفارشی کاربر برای هر کاربر خاص برحسب نام کاربری login شده
- کاهش هزینه‌های عملیاتی دسترسی از راه دور با VPN
- گسترش دسترسی به شبکه برای کلیه کاربران مانند کارمندان، پیمانکاران و شرکای تجاری
- تأیید هویت کاربر از راه دور از طریق یک سرور دسترسی از راه دور
- تأیید هویت کانکشن های VPN یا فایروال از اینترنت به شبکه داخلی
- تأیید هویت تمام دسترسی ها به شبکه های بی‌سیم و شبکه‌های سیمی شرکت‌ها که می‌توان به تمام کاربران یا بخشی از یک گروه یا یک سطح دسترسی مشخص اعمال کرد
- حفاظت از اطلاعات حساس برروی شبکه‌های اینترانت و اکسترانت، با محدود کردن دسترسی به صفحات وب، آدرس ها و دایرکتوری ها
- محدود کردن دسترسی به نرم افزارهای مهم، فایل های حساس و یا منابع دیگر
- جلوگیری از دست‌کاری تنظیمات مدیریتی شبکه

ازجمله کاربردهای رایج VPN می‌توان به دورکاری کارمندان، ایمن‌سازی ارتباط داخلی و ارتباط امن با مراکز داده، احراز هویت و تعیین دسترسی کاربران به اطلاعات و تعیین ضوابط جهت دسترسی اشاره کرد.

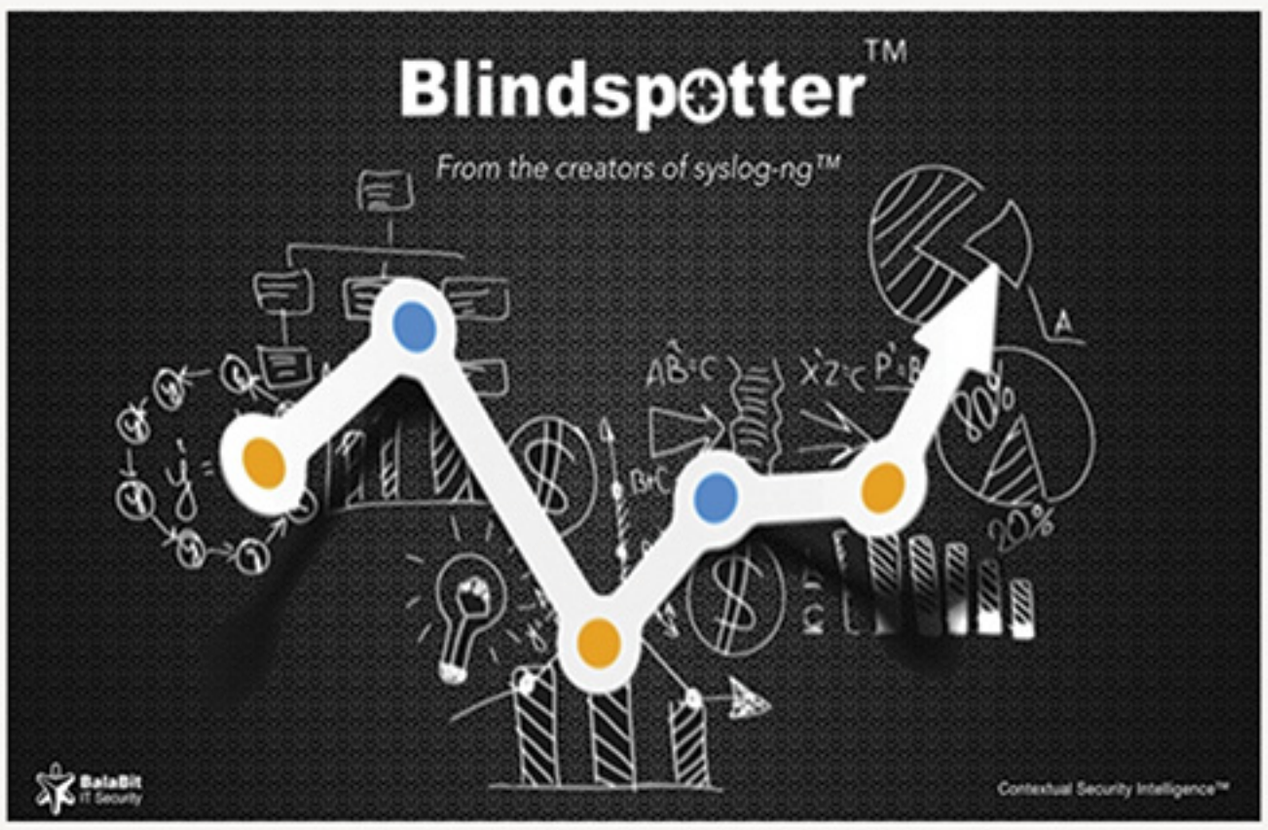
PN های مبتنی بر SSL به صورت یکپارچه با راه حل احراز هویت چند عاملی ، دسترسی از راه دور را با استفاده از یک مرورگر وب و رمزگذاری SSL، تقریباً از هر مکان دارای اینترنت فعال فراهم می‌آورند. این روش به هیچ نرم‌افزار سرویس گیرنده خاص از پیش نصب شده برروی سیستم نیازی ندارد؛ این امر باعث می‌شود راه‌حل SSLVPN قادر باشد از "هرکجا" از دسکتاپهای قابل مدیریت شرکت و یا دسکتاپ های غیرقابل مدیریت مثل دستگاههای شخصی کارمندان، پیمانکاران یا شرکای تجاری ارتباط برقرار کند. با استفاده از این راه‌حل تنها ترافیک افرادی که مجوز دسترسی به سرورها را دارند وارد شبکه می شوند . دسترسی به شبکه در هرزمان و از هرجا به کارمندان این انعطاف‌پذیری را می دهد تا بتوانند در هرزمان و هرمکانی وظایف شغلی خود را پیگیری کنند و پشتیبانی‌های لازم را انجام دهند.

فاواموج
ارتباطات و فناوری اطلاعات
FAVAMOUJ ICT

تشخیص تهدید های پیشرفته و مستمر با Blindspotter

امروزه با توسعه روز افزون سازمان ها و اهمیت اطلاعات سازمانی ، مدیریت و کنترل فعالیت های کاربران سازمان به منظور حفظ امنیت اطلاعات سازمانی از اهمیت بسیاری برخوردار است. با توجه به ماهیت فعالیت کاربران سازمانی و نیاز به پویایی کاربران جهت شکوفایی بیشتر، امروزه ایجاد محدودیت برای کاربران کارآمد نمی باشد.

بدین منظور شرکت فاواموج با معرفی محصول Blindspotter این امکان را برای سازمان ها فراهم می کند که بدون ایجاد محدودیت برای کاربرانشان برروی عملکرد آن ها نظارت و مدیریت داشته باشند.

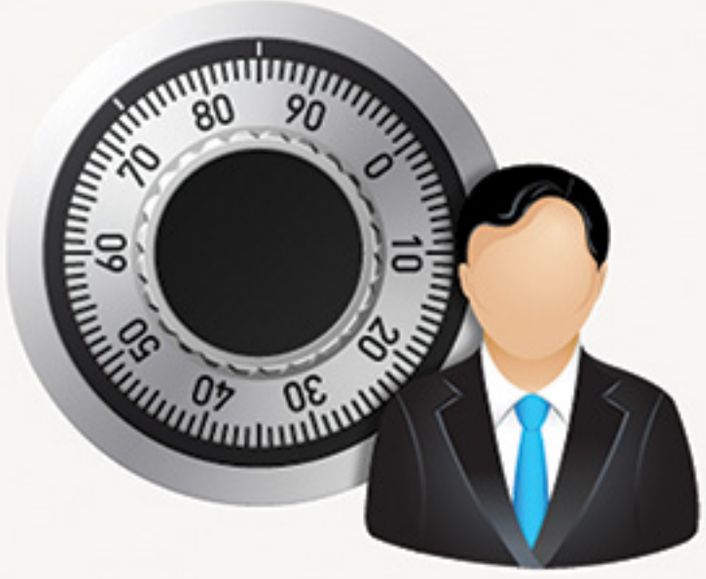


عملکرد Blindspotter بدین صورت است که به عنوان یک ابزار مانیتورینگ به صورت بلادرنگ پروفایلی از رفتار کاربران تشکیل می دهد و تشخیص ریسک برای سازمان از طریق تخطی کاربر از پروفایلش صورت می پذیرد. اطلاعات مفهمومی گوناگونی را به علاوه log های ثبت شده توسط الگوریتم های منحصر به فردی مورد پردازش قرار می دهد و خروجی های متنوعی از تولید اخطار تا دخالت اتوماتیک در عملکرد کاربر را ایجاد می کند.

این محصول برای جلوگیری از حملات APT و شناسایی مجرمان اطلاعاتی درون سازمانی بسیار کارآمد است.

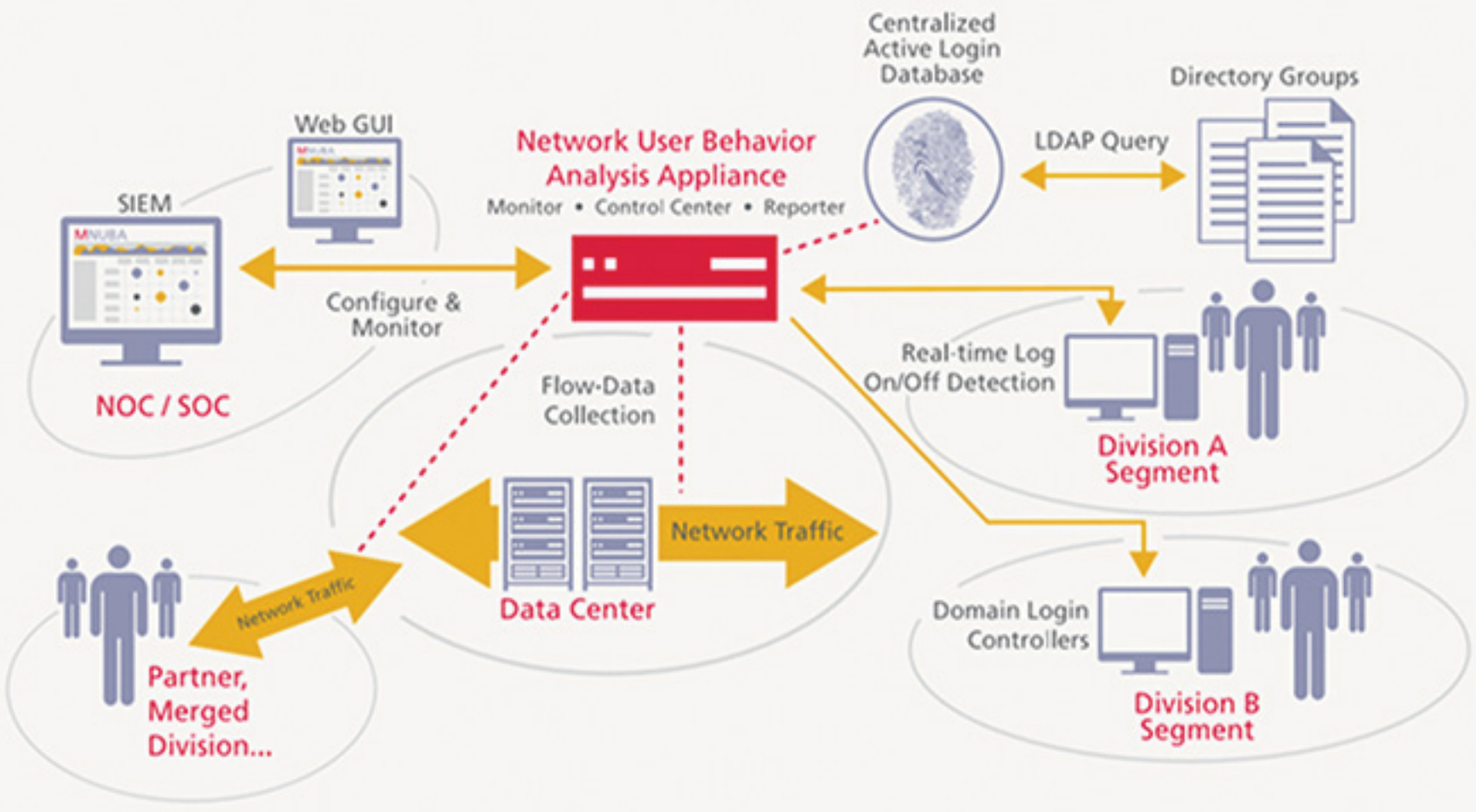
ویژگی ها و کاربردها:

- تشخیص تهدید های پیشرفته و مستمر (APT)
- کاهش پیغام های log بیهوده
- کاهش پیچیدگی های کنترل های امنیتی
- بهینه سازی هشدارهای اطلاعات امنیتی و مدیریت رخداد ها (SIEM)
- امنیت IT متمرکز بر کاربر
- پیدا کردن راحت تر ناهنجاری ها
- کاهش بار کاری تیم امنیت IT
- نظارت بیشتر و کنترل کمتر منجر به بار کاری کمتر برای کاربران می شود



General Brochure

از آنجا که شرکت فاواموج همواره پیشرو در فناوری های روز بوده است به منظور پاسخ گویی به نیاز های سازمان ها در زمینه امنیت اطلاعات سازمان و عدم افشای آن در مقابل حملات خارجی و تهدید های درون سازمانی ابزار Blindspotter را پیشنهاد می دهد که در عین عدم ایجاد محدودیت برای کاربران با عملکردی بی رقیب امنیت اطلاعات سازمان را با توجه به رفتار کاربران به صورت بلادرنگ فراهم می کند.



BalaBit
IT Security
بالابیت

ارتباطات و فناوری اطلاعات

فاواموج

احراز هویت چند عاملی:

با استفاده از تکنولوژیهای VPN امروز سازمانها میتوانند به طور موثر به هر کسی مجوزهای لازم را بدهند تا بتوانند از هر جایی و در هر زمانی برای پیشبرد کارها و پشتیبانی های مورد نیاز به منابع سازمان دسترسی پیدا کنند. برای این منظور علاوه بر امنیت بســـتر عبور اطلاعات با استفاده از تونلهای رمز شده، مدیران سازمان باید از اعمال مجوزهای مشخص به هر فرد و امنیت احراز هویت افراد در دسترسی به اطلاعات سازمان نیز اطمینان کافی داشته باشند تا هر کس نتواند با نام کسی از خانه یا هرجای دیگر به اطلاعات سازمان دسترسی پیدا کرده و سازمان را مورد حمله و آسیب قرار دهد.

این دسترسی به سرورها و اطلاعات حساس در سازمان نیازمند یک راهکار بی نقص و غیر قابل نفوذ است در این خصوص استفاده از 2FA یا احراز هویت چند عاملی یک لایه امنیتی اضافی برای دسترسی از راه دور فراهم می آورد تا از دسترسی کاربران غیر مجاز به دارایی های شبکه جلوگیری به عمل آورد.

با اســـتفاده از احراز هویت چند عاملی و تکنولوژی OTP میتوان امنیت ورود کاربر به سیستم را تامین نمود و این اطمینان را فراهم آورد که فقط کاربران مجاز امکان دسترسی به سیستم را داشته باشند.

2FA Solution

راهکار احراز هویت چند عاملی که به صورت یکپارچه با SSLVP برای احراز هویت کاربران VPN مورد استفاده قرار میگیرد از حداقل دو فاکتور برای احراز هویت استفاده میکند. این فاکتورها می¬تواند شامل اطلاعاتی باشد که کاربر می‌داند مثل پسورد یا PIN به‌عنوان فاکتور اول و چیزی باشد که کاربر دارد مثل Token و کدی که روی Token به صورت تصادفی تولید می‌شود.

از ویژگی‌ها و کارآیی های راه حل SSLVPN به صورت یکپارچه با MFA می‌توان به موارد زیر اشاره کرد :

- ارتباط آسان از دسکتاپهای غیرسازمانی
- عدم نیاز به پشتیبانی و نگهداری نرم‌افزار دسکتاپ
- قابلیت داینامیک بودن و به روز رسانی اتوماتیک نرم افزار دسکتاپ
- امکان ایجاد پورتال های وب سفارشی کاربر برای هر کاربر خاص برحسب نام کاربری login شده
- کاهش هزینه‌های عملیاتی دسترسی از راه دور با VPN
- گسترش دسترسی به شبکه برای کلیه کاربران مانند کارمندان، پیمانکاران و شرکای تجاری
- تأیید هویت کاربر از راه دور از طریق یک سرور دسترسی از راه دور
- تأیید هویت کانکشن های VPN یا فایروال از اینترنت به شبکه داخلی
- تأیید هویت تمام دسترسی ها به شبکه های بی‌سیم و شبکه‌های سیمی شرکت‌ها که می¬توان به تمام کاربران یا بخشی از یک گروه یا یک سطح دسترسی مشخص اعمال کرد
- حفاظت از اطلاعات حساس برروی شبکه‌های اینترانت و اکسترانت، با محدود کردن دسترسی به صفحات وب، آدرس ها و دایرکتوری ها
- محدود کردن دسترسی به نرم افزارهای مهم، فایل های حساس و یا منابع دیگر
- جلوگیری از دست‌کاری تنظیمات مدیریتی شبکه

با توجه به مشکلات و خطرات استفاده از Ssl/Vpn به تنهایی (خطراتی همچون فاش شدن کلمه عبور کاربر) و در معرض ریسک قرار گرفتن سازمان به منظور بالا بردن امنیت VPN راه کار استفاده از 2FA یا احراز هویت چند عاملی برای بالا بردن امنیت ارتباط VPN معرفی می شود تا از خطرات آن جلوگیری کند.

تهران ـ میدان هفت تیر ـ خیابان قائم مقام فراهانی ـ کوچه الوند ـ پلاک ۹ ـ ساختمان فاواموج

تلفن : ۸۹۳۴۱۰۰۰ دورنگار : ۸۹۳۴۱۰۰۱

پست الکترونیک : info@favamouj.com

وب سایت : www.FavaMouj.com