Bring Your Own Device (BYOD)

۱- مقدمه:

امنیت دیتا، یکی از دغدغه‌های اصلی سازمانها بلاخص بانکها و موسسات مالی می‌باشد. تهدیدات سایبری میتوانند در بخشهای متفاوت از جمله درگاه‌های اینترنتی، وب سایت‌ها، پایگاه‌های داده،.... و یا حتی در رایانه‌های کاربران وجود داشته باشند. برای مقابله با چنین تهدیداتی و جلوگیری از وارد آمدن خسارات، لازم است راهکارهای مناسبی در نظر گرفته شود.

یکی از حوزه‌هائی که صحت کارکرد اجزاء مرتبط با آن اهمیت بسزایی در تامین امنیت دارد، تجهیزات مورد استفاده کاربران و نحوه ارتباطات آنها با شبکه می‌باشد. تَعدد و تنوع تجهیزات شخصی مورد استفاده کابران (از جمله PC, Smartphone, Tablet, Laptop,..) و همچنین تغییر سیاست سازمان‌ها درخصوص اعطاء مجوز استفاده از این تجهیزات جهت افزایش بهره‌وری و ایجاد مزایای رقابتی، بر پیچیدگی مباحث امنیتی این گونه ارتباطات افزوده و لزوم استفاده از سیستمی را که بتواند نیازها و مشکلات امنیتی این حوزه را پوشش دهد بیش از پیش نمایان می‌کند.

۲- چالشها

چالشهای اصلی که سازمان در برقراری امنیت ارتباطات کابران با شبکه با آنها روبرو است به شرح زیر است:

- تعدد راههای اتصال کابران به شبکه (باسیم، بی‌سیم و یا کاربران راه دور)
- تنوع تجهیزات مورد استفاده کاربران (از جمله PC, Smartphone, Tablet, Laptop,..)
- لزوم اعمال سطوح دسترسی مختلف برای هر کاربر، با توجه پُست و مسئولیت سازمانی وی و نوع تجهیزاتی که در هر لحظه استفاده می‌کند
- رعایت سیاست‌های امنیتی (سیاست‌های داخلی سازمان، سیاست‌های ملی، استانداردهای بین‌المللی)
- توجه به افزایش بهره‌وری کارکنان و رضایت سایر ذی‌نفعان و همچنین حریم خصوصی ایشان هنگام اعمال سیاست و کنترل‌های امنیتی

۳- نیازمندی‌ها:

برای پیاده سازی معماری BYOD لازم است ابتدا نیازمندی‌های سازمان مورد مطالعه قرار گرفته و پس از آن راه‌حل مناسب طراحی و پیاده سازی گردد. عموماً نیازمندی‌های به شرح زیر می‌باشند:

- امکان تمایز هویت کاربر از تجهیزات مورد استفاده، به منظور تعریف سطوح دسترسی مختلف مختص استفاده از هریک از تجهیزات از جمله رایانه، لپ تاپ، تلفن همراه و یا تَبلِت و ...
- وجود راهکاری جهت یکپارچه نمودن تنظیمات امنیتی برای کنترل دسترسی کاربران (معمولاً تنظیمات لازم برای کنترل دسترسی به صورت غیر متمرکز و از طریق اعمال پیکربندی خاص بر روی سرویسها و تجهیزات مختلف شبکه صورت می‌گیرد)
- ساده بودن نحوه استفاده از ساختار مورد بحث برای کاربران و سایر ذینفعان
- قابلیت یکپارچه سازی با زیر ساخت‌های امنیتی موجود در شبکه
- همخوانی با استانداردهای امنیتی و امکان تعریف انواع کنترل‌های مربوطه با در نظر گیری حریم خصوصی

اصولا به دلیل حالات بسیار متنوعی که ممکن است کابران سطوح مختلف سازمان به روشهای گوناگون و با تجهیزات مختلف به شبکه متصل گردند، مدیریت و امنیت صحیح این شبکه‌ها امری بسیار پیچیده است. لذا راهکار مورد نظر باید در عین سادگی، انواع تجهیزات (PC, Smartphone, Laptop, tablet..) و نرم‌افزارهای مربوطه (iOS, Android, Windows,...) را پوشش داده و بتواند در لایه‌های مختلف شبکه و در مراحل مختلف (قبل و بعد از اتصال) کنترل‌های امنیتی لازم را انجام دهد. به همین منظور راهکار BYOD، پارامتر ها و کنترل های امنیتی را در دو سطح مختلف شامل Infrastructure و Application اعمال می‌نماید.

← **سطح Infrastructure** : این مرحله قبل از اتصال کاربر به شبکه انجام می‌پذیرد و فرآیند اتصال وی (بسته به نوع تجهیزات مورد استفاده)، نحوه‌ی احراز هویت، کلاس‌بندی و جداسازی، بررسی وضعیت سیستم کاربر و در صورت لزوم قرنطینه نمودن تجهیزات ، از طریق VLAN، SGT، ACL و روشهای دیگر مدیریت و کنترل می‌گردد.

← **سطح Application** : در این مرحله تجهیز مورد استفاده کاربر (PC, Smartphone, Laptop, tablet..) به شبکه متصل شده و لازم است سازوکاری برای تفکیک Applicationهای مجاز از غیر مجاز و محدود ساختن دسترسی کاربر به موارد غیر مجاز ایجاد گردد. به علاوه دسترسی به فایلهای سازمانی بلاخص فایل‌های محرمانه می‌بایست مورد کنترل قرار گرفته و حتی در صورت جدا شدن دستگاه از شبکه، می‌بایست مکانیزمی جهت پاک سازی اطلاعات حیاتی از روی آنها به صورت خودکار وجود داشته باشد.

پلتفرم‌های متعددی برای مدیریت موارد فوق توسعه یافته‌اند. در بسیاری از سازمان‌ها به منظور مدیریت کارآمد و قابلیت‌های بیشتر، استفاده از چند پلتفرم بصورت هیبرید توصیه می‌گردد.

۴- راه‌حل پیشنهادی

از راهکارهای بسیار موثر، جامع و قابل اجرا برای رفع نیازها و مشکلات فوق، استفاده از ۲ فناوری CISCO ISE (جهت مدیریت زیرساخت شبکه) و AirWatch (مدیریت Applicationها) بصورت هیبرید می‌باشد، که بعنوان leader از سوی مراجع معتبر مانند Gartner و Forester معرفی شده‌اند.

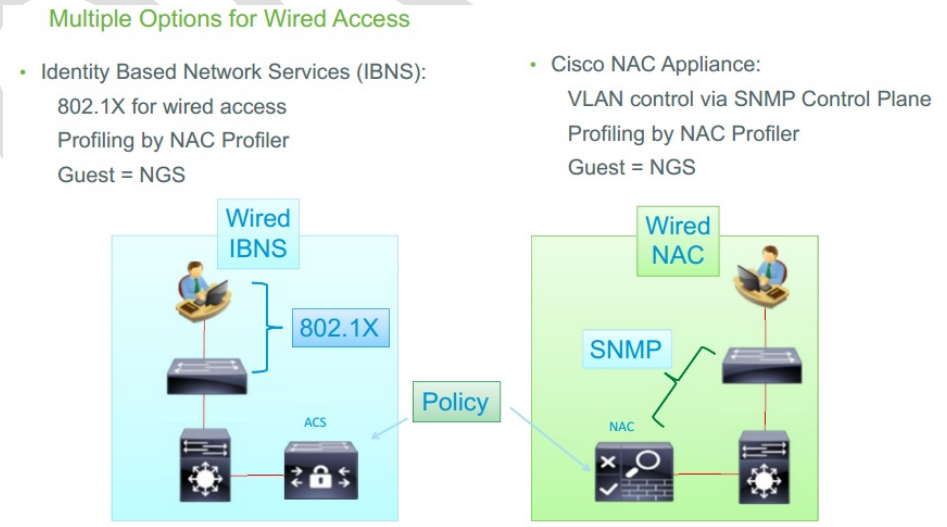
۵- معرفی Cisco ISE:

کمپانی سیسکو برای احراز هویت کاربران و اعطای سطح دسترسی‌های گوناگون بر اساس سیاستهای موجود (Authentication and Authorization) ، محصولی به نام **ACS** را معرفی نمود، که با استفاده از استاندارد Dot1x سیاست‌های مختلف را (از جمله اعطای دسترسی و عضویت در VLAN های از پیش تعیین شده و ...) اعمال میکند.

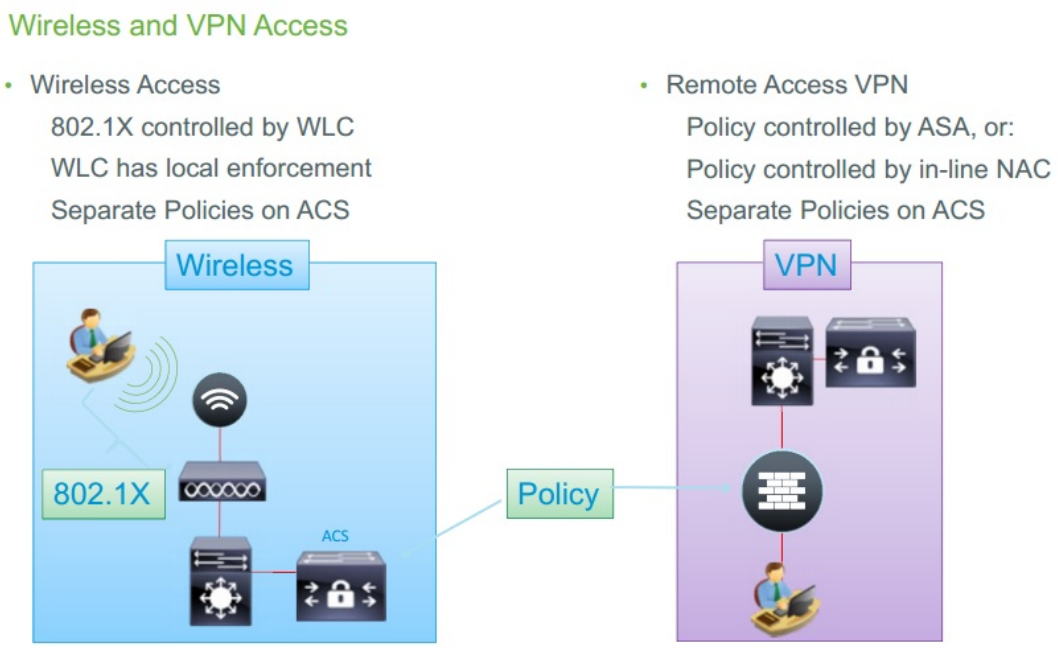
علاوه بر ACS ، کمپانی سیسکو محصول دیگری را با هدف تکمیل عملکرد استاندارد Dot1x تحت نام **NAC** ارائه نمود، که با استفاده از آن میتوان فاکتورهای دیگری (از جمله Update بودن سیستم‌عامل و آنتی ویروس، فعال بودن فایروال و...) را نیز علاوه بر نام کاربری جهت صدور اجازه اتصال یک سیستم به شبکه و اعطای دسترسی در نظر گرفت. ضمناً با استفاده از اطلاعات بدست آمده میتوان جهت ایزوله، مسدود کردن، برطرف سازی مشکلات سیستم‌های ناسالم، تسهیلات دسترسی برای تجهیزات احراز هویت نشده، فراهم نمودن دسترسی کاربران مهمان و موارد مشابه دیگر استفاده نمود.

در کنار مزایای فوق، این راهکارها به نوبه خود دارای مشکلاتی به شرح زیر می‌باشند:

- ✓ عدم یکپارچگی در سیاست‌های اعمالی
- ✓ روشهای متفاوت در اعمال سیاست‌ها

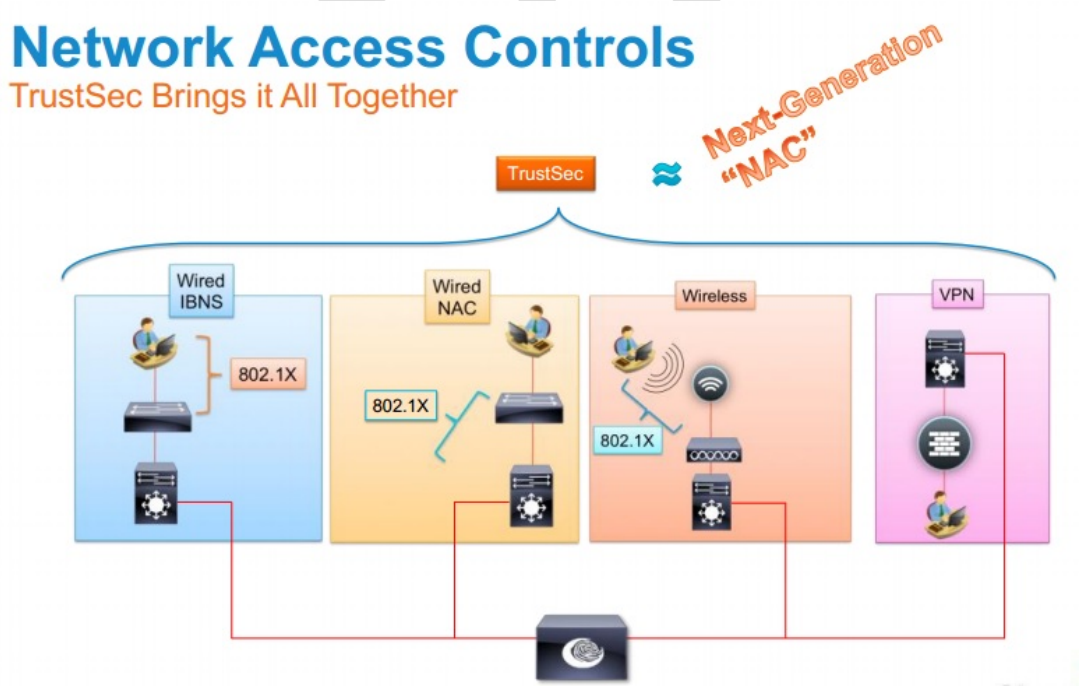


گزینه های مختلف برای دسترسی کابلی و عدم وجود ساختار یکپارچه



سیاست های متفاوت در تجهیزات مختلف برای دسترسی بی سیم و VPN

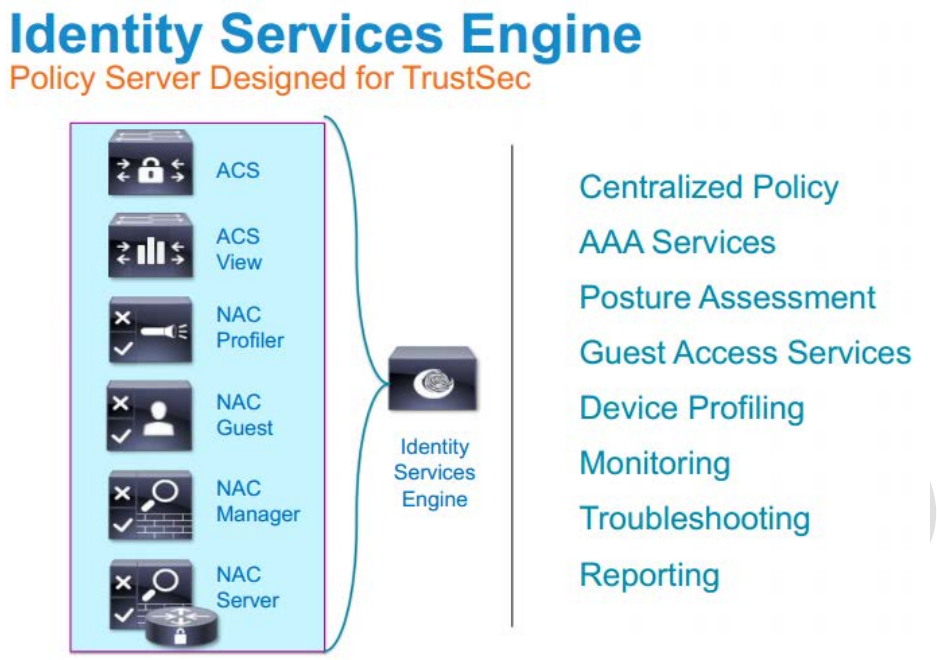
مشکلات فوق سبب گردید کمپانی سیسکو راه حل جامع‌تری را تحت عنوان **TrustSec** ارائه دهد، که از آن به عنوان **نسل بعدی NAC** نیز یاد میشود .



TrustSec بعنوان راهکار جامعی که همه مشکلات فوق را مرتفع می‌سازد

Cisco ISE پلتفرم مورد نظر برای پیاده سازی راه‌حل TrusSec می‌باشد، که بسیاری از امکانات NAC و ACS را دربر دارد. این محصول امکان یکپارچه شدن با پیشرفته‌ترین پلتفرم‌های MDM و SIEM را دارد و در واقع اکو سیستمی

را با هدف ارائه راهکار جامع BYOD بعلاوه راه‌حل جامع یکپارچه سازی و متمرکز سازی مدیریت سیاست‌های امنیتی ایجاد میکند.



ISE ترکیبی از ویژگی های ACS و NAC در قالب یک Policy Server متمرکز

۶- قابلیت‌های مهم پلتفرم Cisco ISE:

۶-۱-احراز هویت و تعیین سطح دسترسی از طریق پروتکل dot1x

Dot1x استاندارد IEEE برای کنترل سطح دسترسی بر مبنای پورت–(Port based Network Access Control PNAC) می‌باشد، که در پلتفرم ISE این قابلیت به صورت پیش فرض وجود داشته و نیازی به استفاده از نرم افزارهای جانبی همانند ACS برای احراز هویت تجهیزات باسیم (Wired) و بی‌سیم (Wireless) نمی‌باشد. به علت استفاده از پروتکل dot1x این پلتفرم قادر است تا دسترسی کابران را به شبکه از لایه‌های پایین و قبل از اتصال و گرفتن آدرس IP کنترل کند. کاربران تنها در صورتی که بطور کامل احراز هویت شده باشند، میتوانند به شبکه دسترسی پیدا کنند. در غیر اینصورت سیستم آنها یا قرنطینه شده، یا دسترسی‌شان محدود خواهد بود و یا کلاً اجازه دسترسی به شبکه را نخواهند داشت.

۶-۲- پشتیبانی از روش‌های جایگزین برای احراز هویت تجهیزاتی که dot1x را پشتیبانی نمی‌کنند.

یکی از چالش‌ها، تجهیزاتی (مانند موارد زیر) هستند که از استاندارد dot1x را پشتیبانی نمی‌کنند.

- ✓ رایانه‌هایی که سیستم عامل آنها این قابلیت را نداشته باشد

- ✓ تجهیزات هوشمند فاقد قابلیت مذکور مانند بعضی از موبایلها و تبلت‌ها
- ✓ پرینتر، اسکنر یا فکس که به شبکه متصل شوند
- ✓ و غیره

برای ارتباط تجهیزات فوق با شبکه، ISE دو روش زیر را در نظر گرفته است.

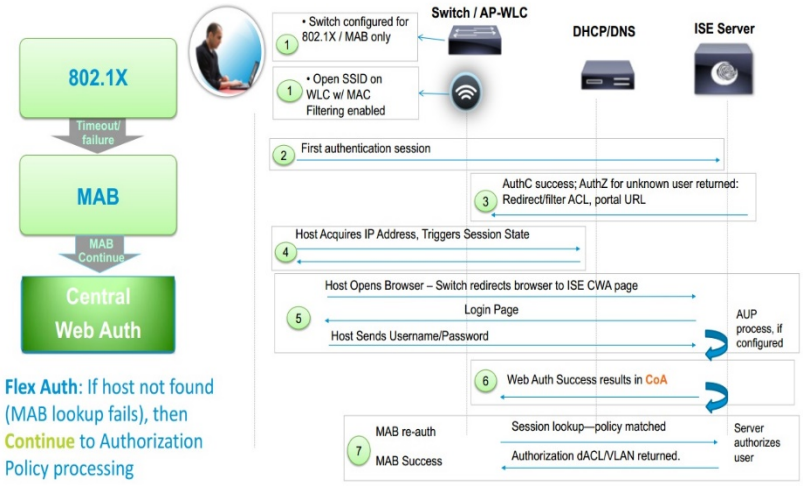
روش اول : MAB (MAC Authentication Bypass)

در این روش آدرس فیزیکی (MAC Address) تجهیزاتی از قبیل پرینتر ، فکس وغیره که به شبکه اتصال پیدا کردند، در دیتابیس ISE در گروهی که مرتبط با MAB می باشد، ذخیره می‌گردد و از این طریق در صورتی که دستگاه قادر به احراز هویت خود از طریق dot1x نباشد، در مرحله بعد ISE آدرس فیزیکی دستگاه را در لیست خود بررسی و در صورت وجود، آن را تایید نموده و امکان اتصال به شبکه را برای آن سیستم فراهم میکند.

لازم به ذکر است که برای انجام عمل فوق می‌بایست تنظیمات خاصی، هم بر روی دستگاه احراز هویت کننده یا Authenticator (همان سوئیچی که دستگاه از طریق آن به شبکه متصل شده است) و هم بر روی سرور ISE صورت بگیرد.

روش دوم : WEB Authentication

در این روش چنانچه احراز هویت سیستم نتواند از طریق dot1x و MAB انجام شود، سیستم برای اتصال به شبکه نیاز به وارد نمودن نام کاربری و رمز عبور خواهد داشت که برای این منظور به یک پرتال مرکزی جهت وارد نمودن اطلاعات فوق ارجاع میگردد. معمولا این عمل درصورتیکه ۲ روش دیگر با موفقیت صورت نگرفته باشد، انجام میشود



متدهای مختلف احراز هویت کاربران (Flex Auth)

۶-۳- امکان ایجاد دسترسی برای کاربر مهمان (Guest)

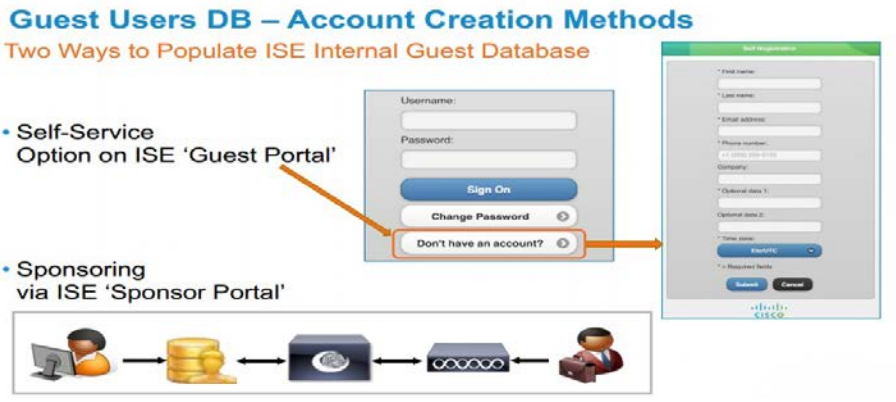
با استفاده از این قابلیت ISE ، کاربران مهمان پس از اتصال به شبکه باسیم یا بی‌سیم سازمان و پس از redirect شدن به پرتال مربوطه، می‌توانند برای خود اقدام به ایجاد نام کاربری و کلمه عبور نموده و پس از تایید احراز هویت به عنوان کاربر مهمان، بر اساس سیاست تعیین شده مختص مهمان، از سرویس‌های مورد نظر (که در اغلب موارد محدود به اینترنت است) استفاده نمایند.

ایجاد اکانت برای کاربران مهمان از ۲ طریق امکان پذیر است .

- **روش اول- از طریق گزینه Self-Service در پرتال مهمان (Guest portal)**
- **روش دوم- از طریق یک اکانت اسپانسر و پرتال اسپانسر (Sponsor portal)**

روش اول - کاربر میهمان از طریق یک پورت باز و یا یک شبکه وایرلس با SSID بدون رمز وارد شبکه شده سپس به پرتال میهمان (Guest portal) به صورت خودکار forward می‌گردد. در آنجا پس از وارد نمودن اطلاعات شخصی لازم، یک نام کاربری و رمز عبور موقت جهت دسترسی محدود و کنترل شده به شبکه دریافت میکند.

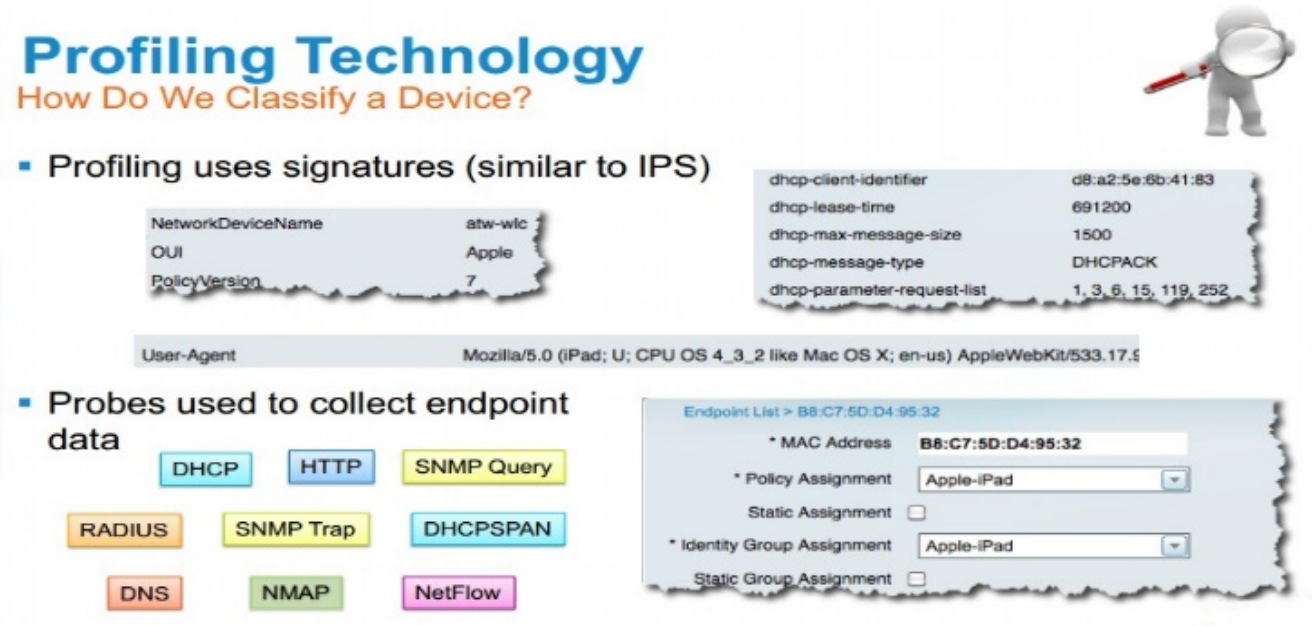
روش دوم - مختص مواردی است که سازمان با شرکت‌ها و پیمانکارانی در ارتباط می‌باشد که از شبکه سازمان با دسترسی بالاتر از اکانت میهمان استفاده می‌کنند و یا ممکن است سازمانی داخل خود چند شرکت همکار نیز داشته باشد که آنها داخل شبکه سازمان دارای سرویس ها و سرورهای خاص خود باشند. در اینگونه موارد نوع دیگری از اکانت به نام اسپانسر که میتواند برای عده‌ای خاص دسترسی‌هایی محدود ولی فراتر از حد یک کاربر میهمان تعریف کند وجود دارد. حدود این دسترسی توسط Admin شبکه تعریف و کنترل می‌گردد. مزیت این روش در این است که با ایجاد اکانت اسپانسر حجم کار متصدی اصلی شبکه کاهش یافته و در مواردی همچون مثال فوق وظیفه‌ی تولید اکانت کاربران شرکت های همکار بر عهده‌ی فردی از طرف همان شرکت خواهد بود نه متصدی اصلی شبکه.



دو روش موجود برای ایجاد حساب کاربری مهمان

۶-۴- قابلیت کلاس‌بندی و پروفایل نمودن تجهیزات موجود در شبکه و اعمال سیاست‌های مورد نظر بر روی آنها

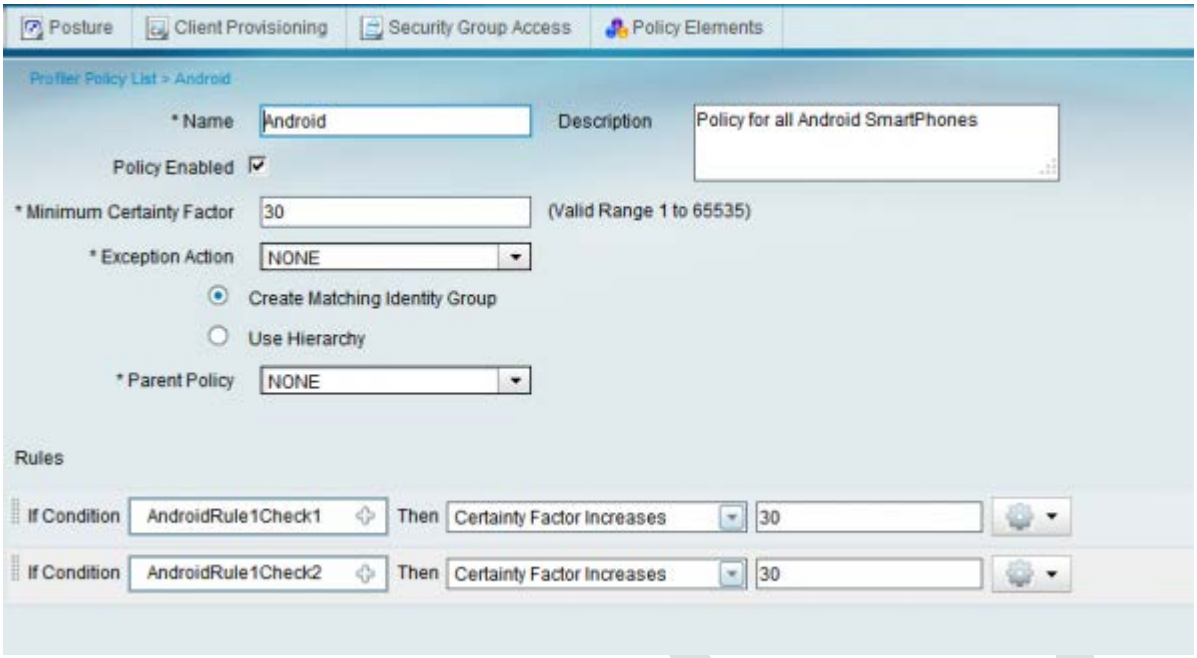
از قابلیت های کلیدی و کاربردی در ISE ، قابلیت دسته بندی تجهیزات می‌باشد که این مهم از طریق فعال سازی و تنظیم سنسورها و کاوشگرهایی (Probes) که در سیستم قرار داند، حاصل میشود.



تکنولوژی پروفایلینگ به کار رفته در ISE

هر کدام از این سنسورها ، سعی در جمع‌آوری ویژگی‌ها و صفات خاصی از تجهیزات (Endpoints) موجود در سازمان می‌کنند. اطلاعاتی که میتوانند از کاوشگرهای فوق کسب شود در قالب شرط های (conditions) مختلف به صورت مجزا و ترکیبی برای پروفایل کردن تجهیزات مورد استفاده قرار میگیرد.

برای مثال در شکل زیر یک نمونه سیاست پروفایلینگ برای سیستم های مبتنی بر سیستم عامل اندروید که بر روی پلتفرم ISE به صورت پیش فرض وجود دارد نشان داده شده.



همانگونه که در شکل فوق نیز مشخص شده برای اینکه ISE یک سیستم را به عنوان اندروید شناسایی کند دو شرط در نظر گرفته شده و به هر کدام از آنها امتیازی تحت عنوان فاکتور قطعیت (Certainty Factor) اختصاص داده شده.

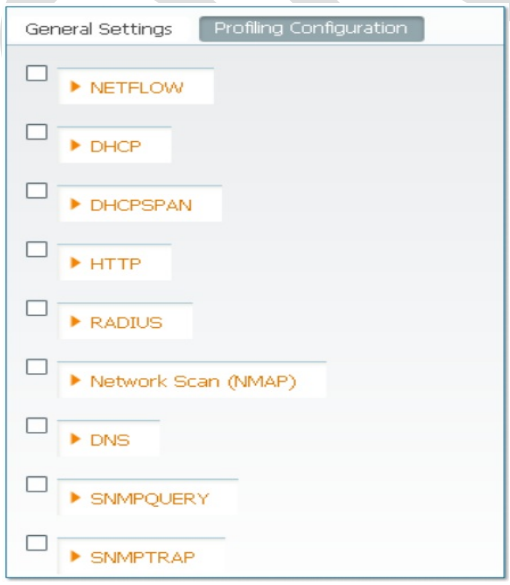
- **شرط اول:** در اطلاعات بدست آمده از User-Agent موجود در مرورگر کاربر به دنبال واژه ی "Android" میگردد (که این داده ها از کاوشگر HTTP بدست می آید)

- **شرط دوم:** در اطلاعات بدست آمده از DHCP Request کاربر در بخش host-name بدنبال واژه ی "android" میگردد. (این داده ها از کاوشگر DHCP بدست می آید)

چنانچه هر یک از این شروط برقرار باشند فاکتور قطعیت متناسب با مقدار در نظر گرفته برای آن شرط (که در این مورد برابر با ۳۰ میباشد) افزایش می یابد و برای اینکه یک endpoint توسط ISE به عنوان Android شناخته شود لازم است که حداقل فاکتور قطعیت (Minimum Certainty Factor)، طبق آنچه در سیاست پروفایلینگ فوق در نظر گرفته شده برابر ۳۰ باشد که به این معنی است که حداقل یکی از دو شرط بالا میبایست درست باشد.

لازم به ذکر است که سیاست های پروفایلینگ بر روی پلتفرم ISE به صورت پیش فرض وجود دارند و از طرف کمپانی سیسکو به صورت دوره ای آپدیت میگردند. همچنین برای سهولت شخصی سازی و افزایش انعطاف پذیری پلتفرم، این قابلیت نیز وجود دارد که بتوان سیاست های پروفایلینگ دلخواه را به آن اضافه یا کم نمود.

سنسورها و کاوشگرهایی که در ISE وجود دارند شامل موارد زیر می‌شوند:



- NETFLOW
- DHCP
- DHCPSPAN
- HTTP
- SNMP Query
- Radius
- DNS
- NMAP
- SNMP Trap

سنسورها و کاوشگرهای موجود بر روی سرور ISE

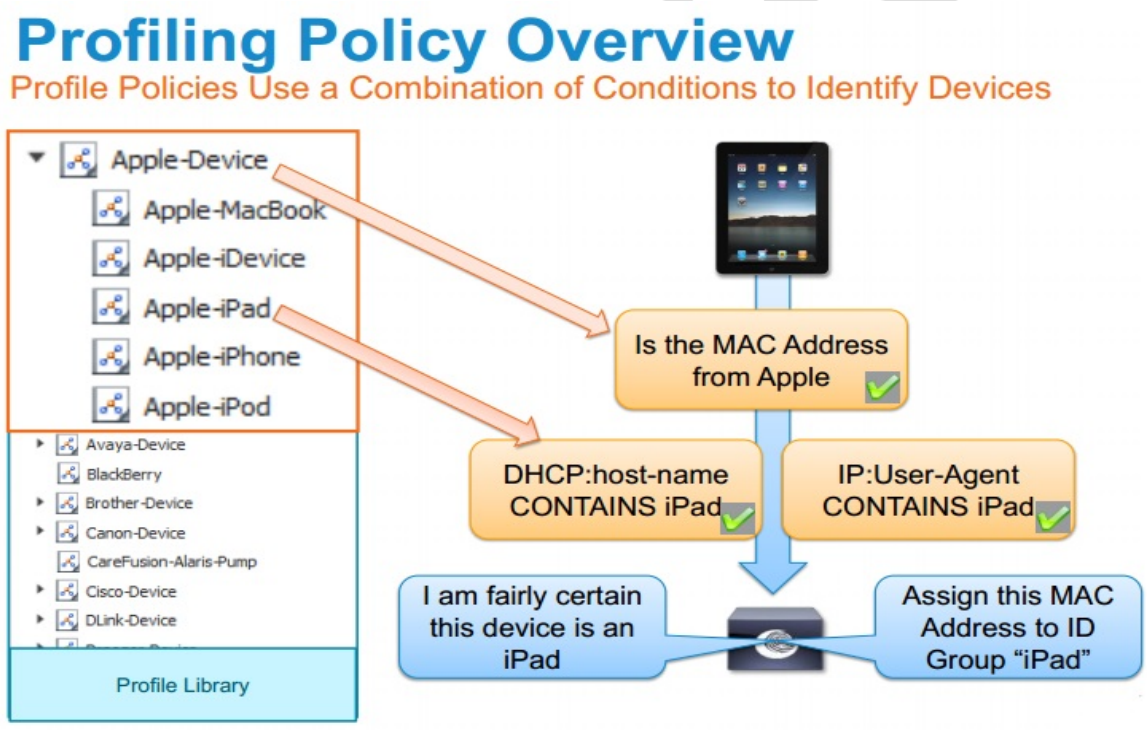
کاوشگرهای تعبیه شده بر روی سیستم ISE به دو طریق Active و Passive می‌توانند اطلاعات را از تجهیزات موجود در سطح شبکه، جمع آوری کنند.

- **Passive :**

در روش Passive یا Network-based اطلاعات به دست آمده از طریق کاوشگر هایی نظیر DNS,HTTP SNMP NETFLOW, در سطح شبکه، برای دسته بندی تجهیزات استفاده می‌گردد .

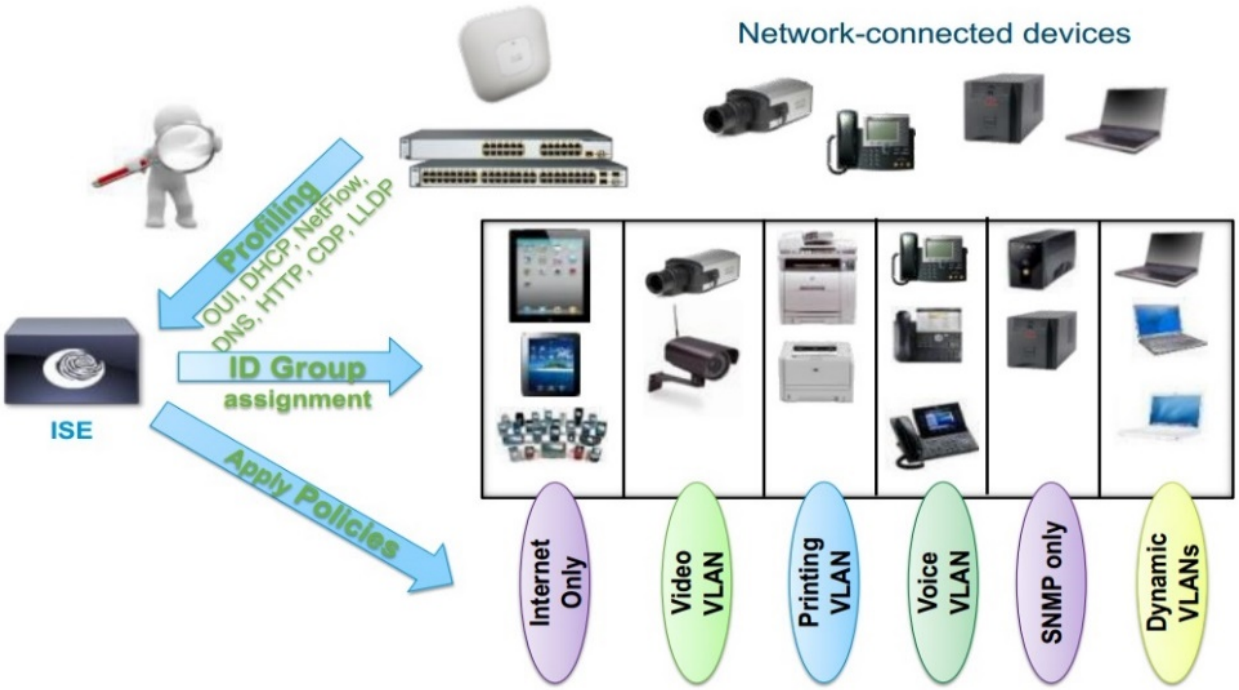
- **Active :**

در روش Active یا endpoint-based از کاوشگری همانند NMAP جهت اسکن و شناسایی هر چه دقیق تر تجهیزات استفاده میشود.



نحوه شناسایی و کلاس بندی یک iPad توسط ISE

پس از اینکه تجهیزات از طریق قابلیت پروفایلنگ، دسته بندی شدند بسته به نیازهای هر سازمان میتوان سیاست‌های مختلفی را بر روی پروفایل‌ها و دسته‌های مختلف تعریف نمود. برای مثال در شکل زیر تجهیزات گوناگون پس از دسته بندی، بسته به نوع آنها در VLAN های مجزا با دسترسی‌های متفاوت قرار گرفتند.



تجهیزات ابتدا دسته بندی و پروفایل میگردند سپس به هر پروفایل سیاست امنیتی خاصی اعمال میگردد

۶-۵- قابلیت یکپارچه‌سازی با Active directory و LDAP و پوشش کامل پروتکل‌های احراز هویت کاربران

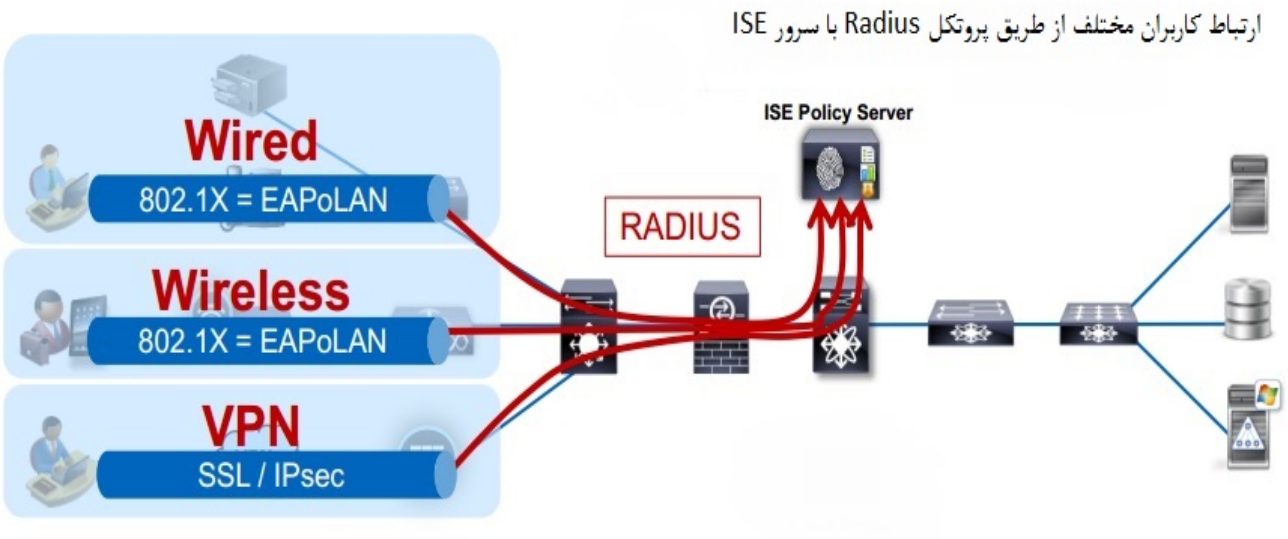
یکی دیگر از قابلیت‌های ISE امکان یکپارچگی با طیف وسیعی از سرویس‌های دایرکتوری همانند Microsoft Active Directory، LDAP و ... می‌باشد.

از آنجائیکه برای احراز هویت کاربران در سازمان‌های مختلف روش‌های متنوعی به کار گرفته می‌شود، قابلیت پشتیبانی از روش‌های گوناگون در فازهای طراحی و پیاده سازی (به دلیل اینکه چنین سرویس‌هایی از قبل راه اندازی شده‌اند)، بسیار مهم است. در نرم‌افزار ISE احراز هویت کاربران به روش‌های متنوعی میتواند صورت گیرد از جمله :

- Active Directory
- LDAP
- Certificate
- RADIUS
- RSA token
- ...

۶-۶- پشتیبانی کامل از روشهای مختلف دسترسی به شبکه

ISE هم قابلیت پشتیبانی از کاربران بی‌سیم (wireless) و هم کابلی (wired) را داشته و برای احراز کاربران راه دور مورد استفاده قرار می‌گیرد.



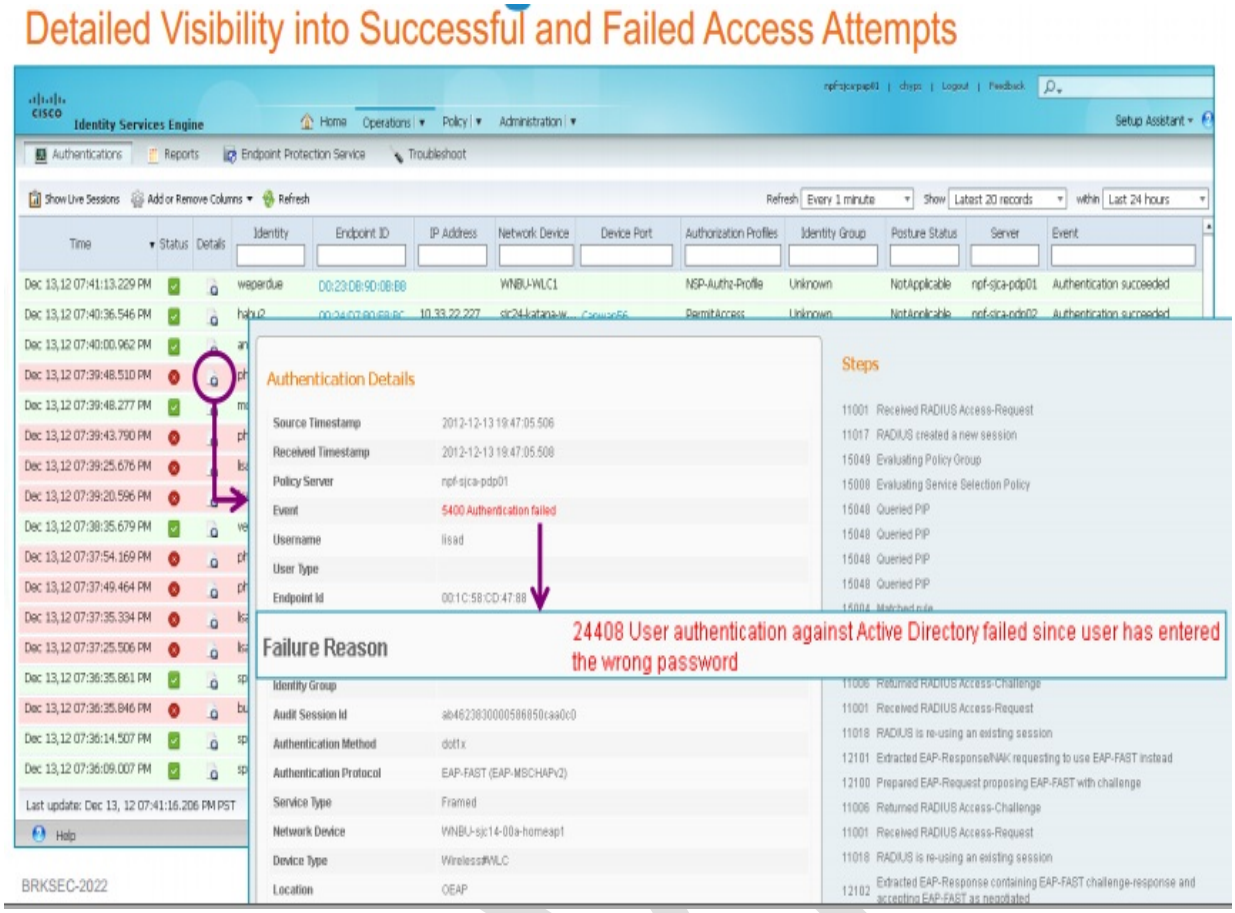
پشتیبانی از روش های مختلف اتصال به شبکه

۶-۷- امکان پیاده سازی در مدل‌ها و ساختارهای گوناگون در مقیاس‌های متفاوت SMB تا Enterprise

از ویژگی های یک راهکار امنیتی جامع، قابلیت توسعه پذیری (scalability) آن می‌باشد. نرم افزار ISE میتواند با تعداد کاربران متفاوت مورد استفاده قرار گیرد . این سیستم توانایی پشتیبانی تا ۲۵۰ هزار کاربر را دارد.

۶-۸- قابلیت مانیتورینگ و عیب یابی بسیار پیشرفته

ISE جزیی ترین اطلاعات مربوط به نحوه ارتباط کابران به شبکه، از جمله روش اتصال، محل اتصال و مشکلات پیش آمده در حین اتصال را با جزئیات کامل ثبت می‌نماید. این موضوع تصویر کاملی از ملاحظات ارتباطی شبکه ارائه نموده و در عیب یابی مشکلات بوجود آمده کمک بسزایی می‌نماید. به عنوان مثال در شکل زیر یک کاربر به علت اشتباه وارد نمودن رمز عبور، نتوانسته به شبکه اتصال پیدا کند.



نمایی از محیط مانیتورینگ و عیب یابی ISE

۶-۹- ارائه تصویر بسیار کامل و شفافی از وضعیت کاربران

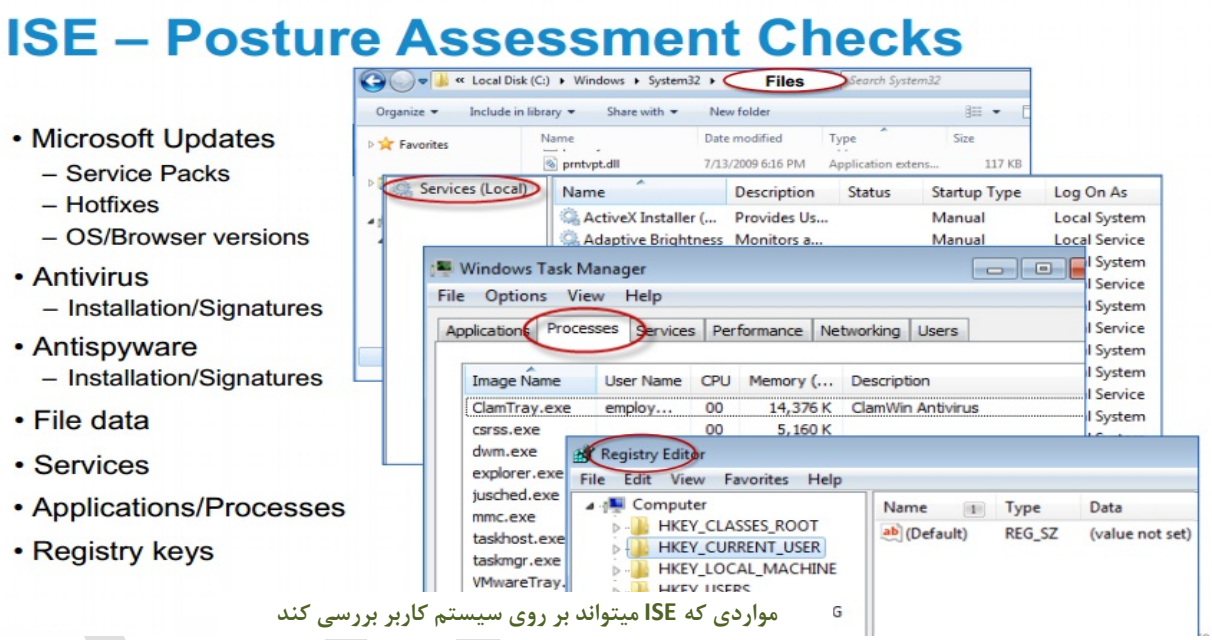
بدین شرح که چه کسی و از طریق چه دستگاهی به شبکه متصل شده؟ به چه قسمتهایی دسترسی داشته؟ از کجا، در چه زمان‌هایی و چگونه این دسترسی صورت گرفته؟

از کجا ؟	**چه زمانی ؟**	**موارد دیگر**
موقعیت جغرافیایی	تاریخ	وضعیت کاربر/سیستم
پورت سوییچ یا SSID	ساعت	اپلیکیشن های استفاده شده
	زمان شروع و پایان	....
چه کسی؟	**از چه طریقی ؟**	**چگونه ؟**
کاربر شناخته شده (کارمند،مدیر،کارمند بخش فروش ...)	نوع وسیله اتصال به شبکه	کابلی
کاربر ناشناخته (مهمان)	وضعیت سیستم در زمان اتصال به شبکه	بی سیم
	دسته بندی که سیستم در آن قرار گرفته	VPN

ارائه دید کامل از وضعیت کاربران در شبکه

۶-۱۰- امکان بررسی وضعیت سیستم کاربران قبل از اجازه دسترسی کاربر به شبکه و اعمال محدودیت در دسترسی آنها

با استفاده از این قابلیت قبل از اجازه دسترسی به شبکه، میتوان به بررسی وضعیت سیستم کاربران از جمله وضعیت رجیستری، آنتی ویروس و غیره، و اعمال محدودیت و قرنطینه سازی بر روی سیستم هایی که با سیاست های تعریف شده در این زمینه همخوانی نداشته باشند، پرداخت. در صورت لزوم میتوان دستگاههایی را که با موارد فوق همخوانی ندارند را به سرور یا سرویس مذبور ارجاع داد تا مشکل امنیتی سیستم برطرف گردد. برای مثال در مورد پتچها و یا آپدیت های امنیتی که بر روی سیستم قرنطینه شده وجود ندارند سیستم میتواند مادامیکه دستگاه مورد نظر را قرنطینه و ایزوله میکند در عین حال آنرا به سرور WSUS متصل کند تا آپدیت های لازم بر روی آن نصب شده و سپس پس از آنکه تهدید امنیتی حاصل از موارد فوق بر روی دستگاه برطرف گشت بتواند با دسترسی کامل به شبکه متصل گردد .



موارد‌ی که ISE میتواند بر روی سیستم کاربر بررسی کند

بررسی وضعیت سیستم کاربران از طریق NAC agent صورت میگیرد که به دو صورت موجود است.

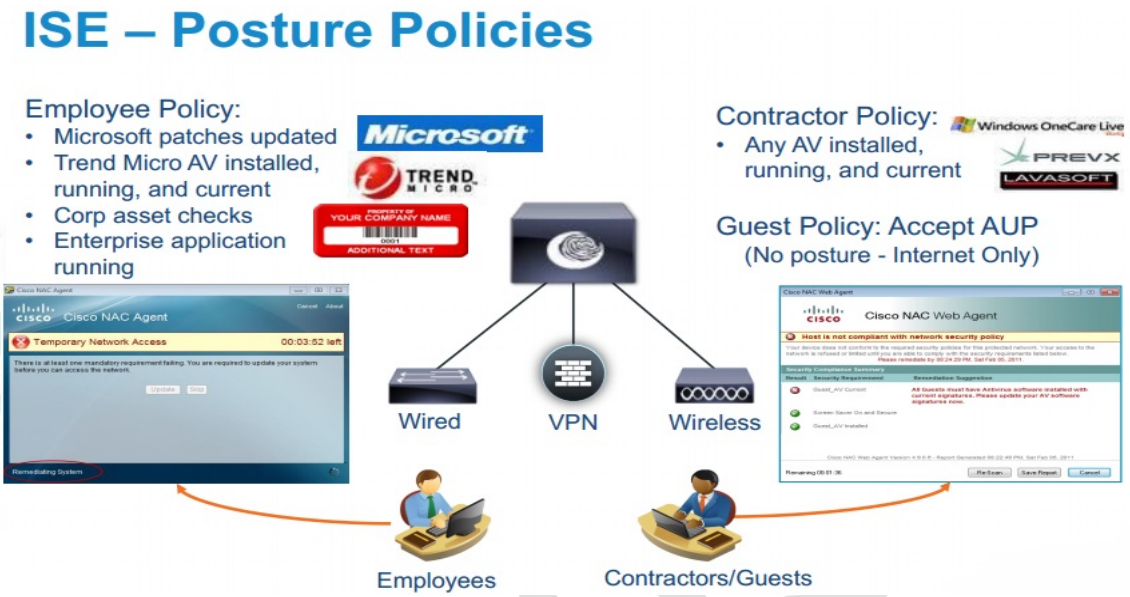
- **NAC Agent**
- **NAC Web Agent**

NAC Agent بر روی سیستم‌هایی که مدیریت متمرکز دامین بر آنها صورت می‌گیرد (managed devices) قابل اعمال هستند و به صورت یک نرم افزار بر روی سیستم‌های ذکر شده نصب میشود.

NAC Web Agent برای سیستم‌هایی که عضوی از دامین سازمان نبوده (Un-managed device)، همانند سیستم های کاربران مهمان، کاربران شرکت‌های طرف قرارداد، لپ‌تاپ‌های شخصی کاربران سازمان که

مدیریتی بر آنها صورت نمی‌گیرد و غیره مورد استفاده قرار می‌گیرد. این agent از طریق ActiveX و مرورگر، بر روی سیستم مد نظر به صورت موقت نصب می‌گردد.

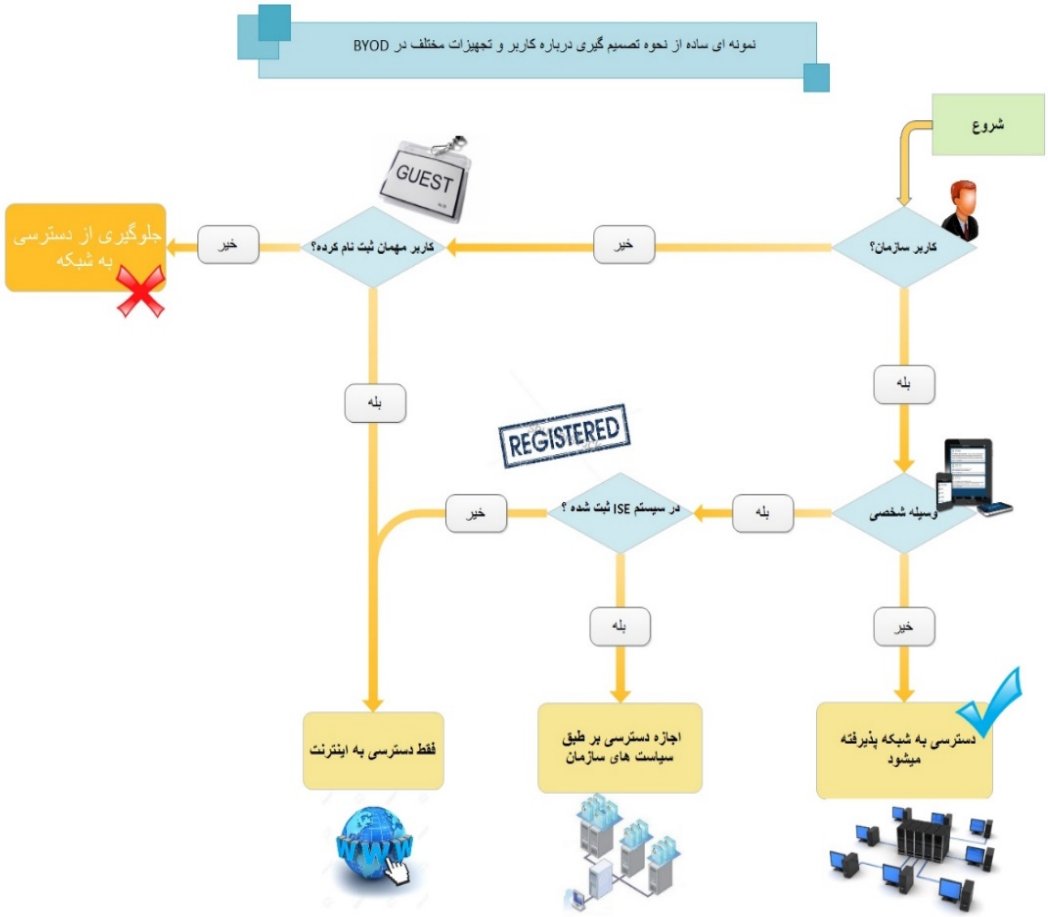
برای مثال در شکل زیر برای کاربر سازمان از NAC Agent و برای کاربر میهمان و یا اسپانسر از NAC web Agent استفاده شده است.



استفاده از **NAC Agent** و **NAC Web Agent** برای بررسی وضعیت سیستم های کاربران

۶-۱۱- انعطاف پذیری بالا و شروط بسیار متنوع و جامع برای تعریف سیاست‌های دسترسی به شبکه که این اجازه را به متصدی شبکه میدهد که بنا به نیازهای روز بتواند سطوح دسترسی مورد نظر را به راحتی تعریف و اعمال نماید.

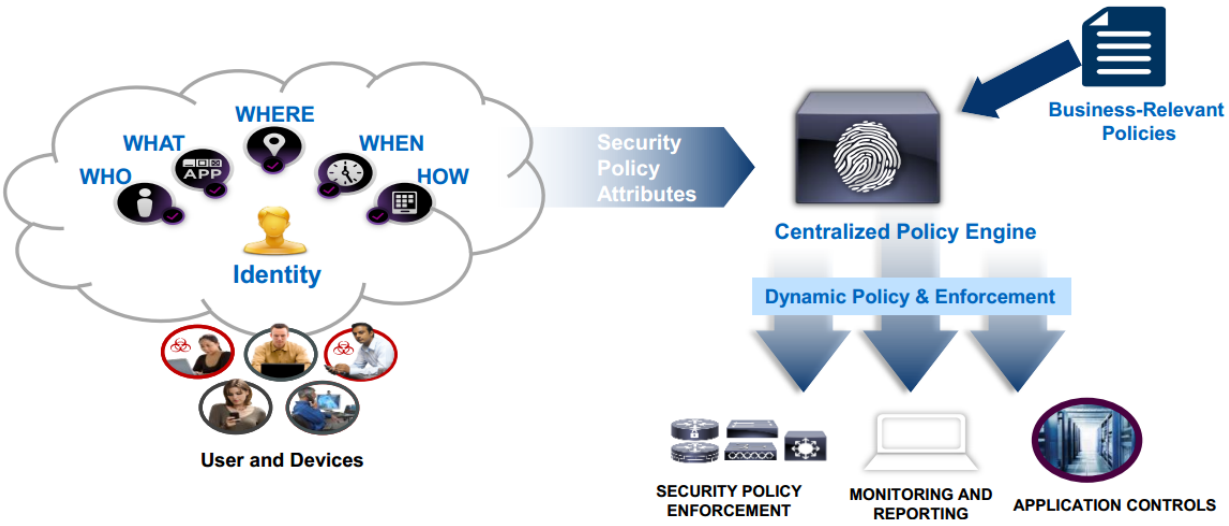
میتوان سطوح دسترسی متفاوتی را برای کاربران مختلف از جمله کاربران میهمان و پرسنل سازمان در نظر گرفت. برای مثال کاربر میهمان فقط دسترسی به سرویس های خاص و محدود و یا تنها اینترنت را داشته باشد و پرسنل سازمان دسترسی طبقه‌بندی شده به سرویسهای مربوطه و یا حتی محدودیت‌ها را در صورت لزوم با جزییات بیشتری اعمال نمود. برای مثال پرسنل سازمان تنها در صورتیکه با رایانه‌ی سازمان به شبکه اتصال پیدا کرد دسترسی کامل داشته باشد و اگر با همان نام کاربری ولی از طریق لپ‌تاپ ، تلفن همراه و یا تبلت شخصی به شبکه اتصال پیدا کرد دسترسی محدودتری برای آن کاربر اعمال گردد .



نمونه ای ساده از روال تصمیم گیری درباره کاربر و تجهیزات مختلف در **BYOD**

۱۲-۶- امکان متمرکز سازی محل تعریف سیاست های امنیتی و جلوگیری از هم گسیختگی آنها

هدف از ارائه نرم افزار ISE نه تنها راهکاری جهت پیاده سازی معماری BYOD بلکه ایجاد ساختاری جهت متمرکز سازی سیاست‌های امنیتی نیز می‌باشد. بدین معنی که در صورت استفاده از این راهکار سیاست های مورد نظر سازمان تا حد امکان متمرکز شده و بر روی سرور ISE تعریف می‌گردد و دستگاه های دیگر از جمله سوییچ‌ها، مسیریاب‌ها، تجهیزات وایرلس و فایروال نقش اعمال کننده‌ی سیاست های امنیتی را خواهند داشت که بر روی سرور ISE تعریف گردیده است. این قابلیت، مدیریت را برای متصدی شبکه تسهیل می‌نماید. بعلاوه تعریف سیاست‌های تازه در قیاس با قبل که نیاز به تعریف آن بر روی تک تک تجهیزات شبکه است، بسیار راحت تر صورت خواهد گرفت.



ISE به عنوان یک واحد تصمیم گیری متمرکز که سیاست های آن از طریق دیگر تجهیزات اعمال میگردد.

۶-۱۳- همخوانی ISE با برنامه های مهم همانند MDM و SIEM

نرم افزار ISE کمپانی سیسکو به تنهایی بسیاری از نیازهای سازمان را پوشش می‌دهد. برای مثال می‌توان به مواردی از قبیل پروفایلینگ، مانیتورینگ و عیب‌یابی بسیار پیشرفته، بررسی وضعیت سیستم‌ها و پوشش راه‌های مختلف اتصال به شبکه از جمله باسیم، بیسیم، VPN ، کاربران مهمان و غیره اشاره نمود.

اما برای هر چه جامع‌تر شدن این راهکار، کمپانی سیسکو اکو سیستمی را ایجاد نموده تا با یکپارچگی ISE با برترین محصولات SIEM و MDM طیف عظیمی از نیاز های امنیتی پوشش داده شود.

برای مثال می‌توان به مواردی از قبیل: بررسی روت یا جیلبریک بودن دستگاه، روشن نبودن اینترنت دیتا در زمان اتصال به شبکه سازمان و غیره اشاره نمود.

برای این منظور ISE از قابلیت‌های پلتفرم‌های MDM (Mobile Device Management) و یا نسل جدید این تکنولوژی ها تحت عنوان EMM (Enterprise Mobility Management) کمک می‌گیرد.

در مواردی ممکن است سازمان نیاز به جمع آوری لاگ‌های ISE و تحلیل آن در کنار دیگر لاگ‌های امنیتی داشته باشد (log correlation) و یا پس از تحلیل لاگ‌های تجهیزات مختلف و تشخیص یک رخداد امنیتی نیاز به اعمال محدودیت‌هایی در دسترسی کاربر یا تجهیزاتی باشد. اینگونه موارد عموما جزء وظایف حوزه‌ی SIEM محسوب میشود و اعمال محدودیت های ذکر شده بهتر است به صورت متمرکز و از طریق نرم افزارهای کنترل دسترسی (همانند ISE) صورت گیرد. بنابراین نیاز به وجود ارتباط کاملی بین ساختار SIEM و BYOD در یک مجموعه میباشد . برای پوشش این نیاز، نرم افزار ISE قابلیت یکپارچه شدن با برترین محصولات SIEM موجود در بازار را دارد.

خلاصه ای از محصولات **SIEM** و **MDM** که توسط **ISE** پشتیبانی میشوند

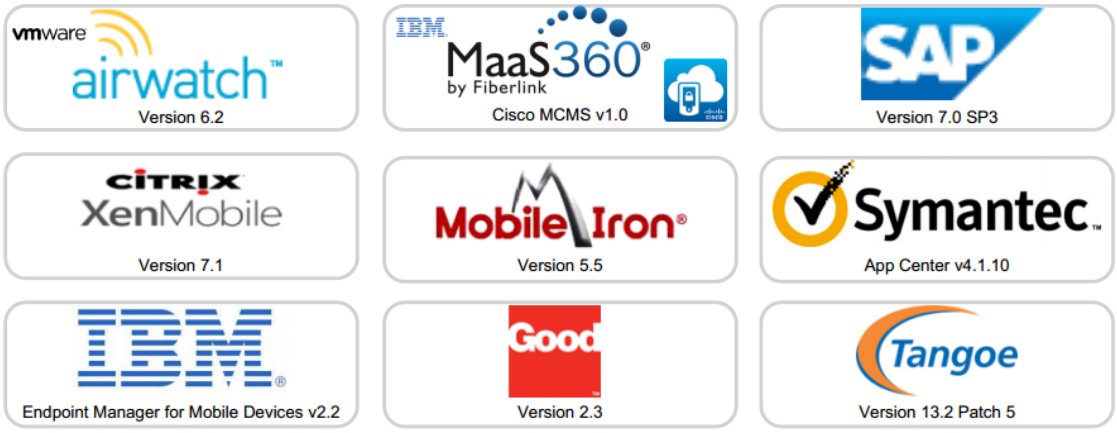
محصولات MDM پشتیبانی شده در ISE	محصولات SIEM پشتیبانی شده در ISE
AirWatch	Splunk
MobileIron	HP ArcSight
Citrix (XenMobile)	IBM
IBM(MaaS360)	LogRhythm
Symantec	Lancope
...	...

۷- معرفی AirWatch :

در مواردی که سیاست های امنیتی سازمانی ایجاب کند که شروطی همانند موارد زیر در سیاست های کنترل دسترسی برای کاربران موبایل مورد استفاده قرار گیرد، اکوسیستم ISE از نرم افزارهای مختلف MDM و EMM برای پوشش نیازهای فوق بهره می‌گیرد. این اکو سیستم از برترین پلتفرم‌های در این زمینه پشتیبانی می‌کند.

- وضعیت جیلبریک یا روت بودن تجهیزات موبایل
- مدل سخت افزار و نرم افزار به کار رفته بر روی این تجهیزات
- وضعیت خاموش یا روشن بودن اینترنت دیتا به هنگام اتصال به شبکه
- وضعیت برنامه‌های کاربردی نصب شده بر روی تجهیزات موبایل و محدودسازی دسترسی به آنها هنگام اتصال به شبکه
- محافظت از فایل های سازمان و پاک سازی اطلاعات سازمانی از روی تجهیز پس از جداسازی از شبکه بدون دستکاری داده های شخصی کاربران

خلاصه ای از بِرَند های MDM که توسط ISE پشتیبانی میشوند



یکی از نرم افزارهای MDM مورد پوشش این اکوسیستم، نرم افزار AirWatch محصول شرکت VMware میباشد که به گواه مراجع معتبر از جمله گارتنر، AirWatch یکی از شرکت های پیشرو در زمینه ارائه راهکار های MDM در سال ۲۰۱۴ محسوب میشود.

گزارش سال ۲۰۱۴ شرکت گارتنر در مورد برترین راهکارهای MDM

این محصول میتواند به هر یک از سه حالت زیر پیاده سازی شود :

- ✓ Cloud
- ✓ On-premise
- ✓ Appliance

این پلتفرم انواع سیستم عامل‌های موبایل را پشتیبانی میکند.

- Android
- Apple IOS
- BlackBerry
- Mac OS
- Windows

در ضمن این نرم‌افزار از تجهیزات مختلف از جمله انواع تلفن‌های هوشمند، رایانه‌های همراه، رایانه‌های Desktop و پرینترها و تجهیزات جانبی پشتیبانی میکند.

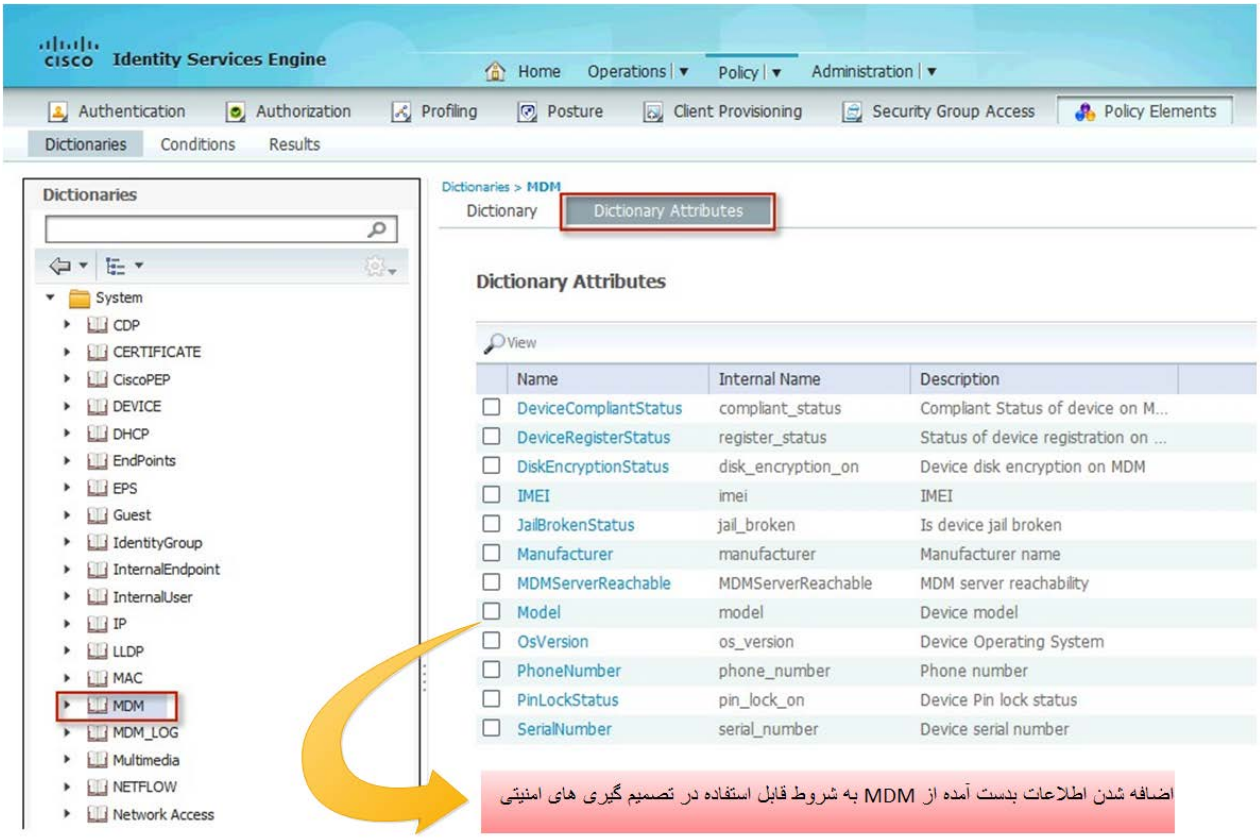
برخی از مزایای استفاده از این نرم افزار به شرح زیر می‌باشد:

- امکان کنترل دسترسی به برنامه‌های کاربردی، نصب برنامه‌های کاربردی مورد نیاز سازمان و اعمال محدودیت بر روی آنها
- ایمن سازی دسترسی به محتوا و داده های سازمانی از جمله فایل ها و داده های متصل به ایمیل ها
- محافظت از داده های حساس از طریق احراز حویت و رمزنگاری ، محدودسازی اشتراک فایل ها و همچنین اعمال محدودیت در نمایش فایل ها به صورت افلاین (offline viewing)
- یکپارچه سازی با زیر ساخت ایمیل سازمان و کنترل دسترسی تجهیزات به ایمیل های سازمانی و رمزنگاری داده های حساس از طریق AirWatch® Secure Email Gateway
- کنترل دسترسی به اینترنت از طریق دسته بندی سایت ها به Whitelist و Blacklist
- و غیره

۷-۱- مزایای پیاده سازی MDM به همراه Cisco ISE :

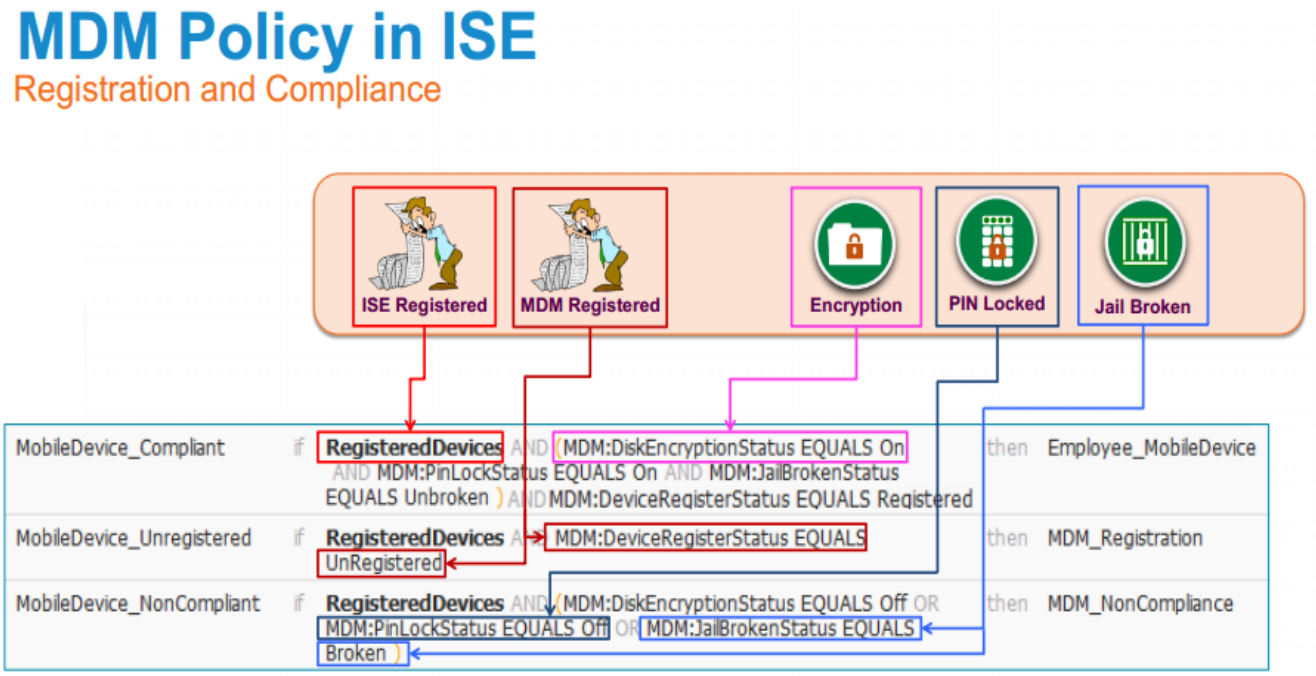
MDM عملکردی مشابه سیستم مدیریت پچ (Patch management) در رایانه ها را دارد (اپلیکیشن های لازم را بر روی تجهیزات موبایل نصب کرده، وضعیت کلی سیستم کاربر را با بیس لاین های امنیتی مطابقت میدهد و ...) . به طور کلی نرم افزارهای MDM تفاوتی بین کاربر و دیوایس در شبکه قائل نشده و مکانیزم های کنترل دسترسی در آنها محدود هستند. ولی در صورت یکپارچه سازی با ISE ، اطلاعات کسب شده از طریق MDM میتواند به عنوان پیش شرط هایی برای کنترل دسترسی کاربران به شبکه توسط ISE استفاده شده . به عنوان مثال اطلاعاتی همانند روت یا جیلبریک بودن دستگاه ، اپراتور تلفن همراه و یا اینکه حافظه

دستگاه رمزنگاری شده یا خیر ، میتوانند به عنوان پیش شرط هایی برای کنترل دسترسی به شبکه ، توسط ISE استفاده شوند.



یکپارچه سازی ISE و MDM و استفاده از داده های MDM برای اعمال محدودیت دسترسی در نرم افزار ISE

به طور کلی نرم افزار های MDM کنترل دسترسی را در لایه های بالاتر شبکه (لایه ۷) و در سطح اپلیکیشن انجام میدهند و ISE کنترل دسترسی را از لایه های پایینی شبکه انجام میدهد (از لایه ۳) . ترکیب و یکپاچه سازی این دو محصول باعث میشود کنترل کاملی در تمامی لایه ها بر روی تجهیزات متصل به شبکه وجود داشته باشد که نظیر آن در هیچ راهکار دیگری مشاهده نمی‌شود.



نمونه ای از سیاست های امنیتی تعریف شده در ISE که در آن از داده های MDM استفاده شده

۸- معرفی Splunk :

SOC (Security Operation Center) واحدی جهت کنترل و مدیریت رخدادهای امنیتی در سازمان میباشد. یکی از عناصر اصلی ساختار SOC ، پلتفرم SIEM میباشد که جهت جمع آوری لاگ های امنیتی و تحلیل آنالیز همبستگی آنها مورد استفاده قرار میگیرد. در اکوسیستم محصول ISE ، بزرگترین شرکت های تولید کننده‌ی محصولات SIEM نیز قرار دارند از جمله:

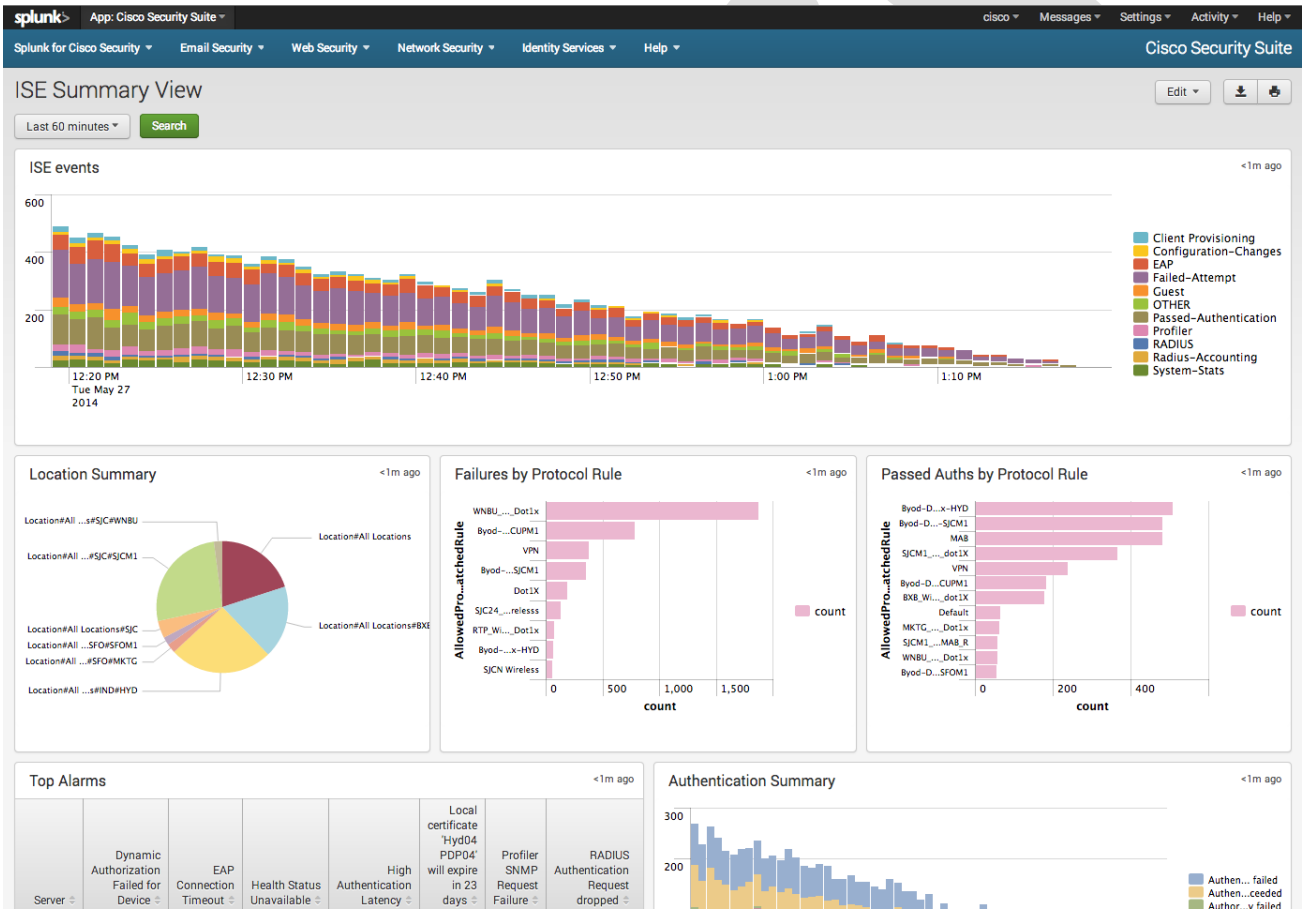
- Splunk
- HP ArcSight
- IBM QRadar
- Lancope
- LogRythm
- Symantec
- Tibco (LogLogic)

گزارش سال ۲۰۱۴ گارتنر در مورد برترین محصولات حوزه SIEM

Splunk از جمله محصولات پیشرو در این حوزه محسوب میشود که قابلیت های مهم زیر را داراست:

- جمع آوری و مدیریت حجم بسیار بزرگی از لاگ ها
- جستجو
- اعلام خطر
- انالیز هم بستگی بین لاگ‌ها (با حجم بسیار بالا) به صورت بلادرنگ
- و یک زبان Query با بیش از ۱۰۰ دستور که میتواند خروجی های گرافیکی و تصویری بسیار متنوعی ایجاد کند

شکل ۱- نمایی از کنسول ISE در نرم افزار Splunk

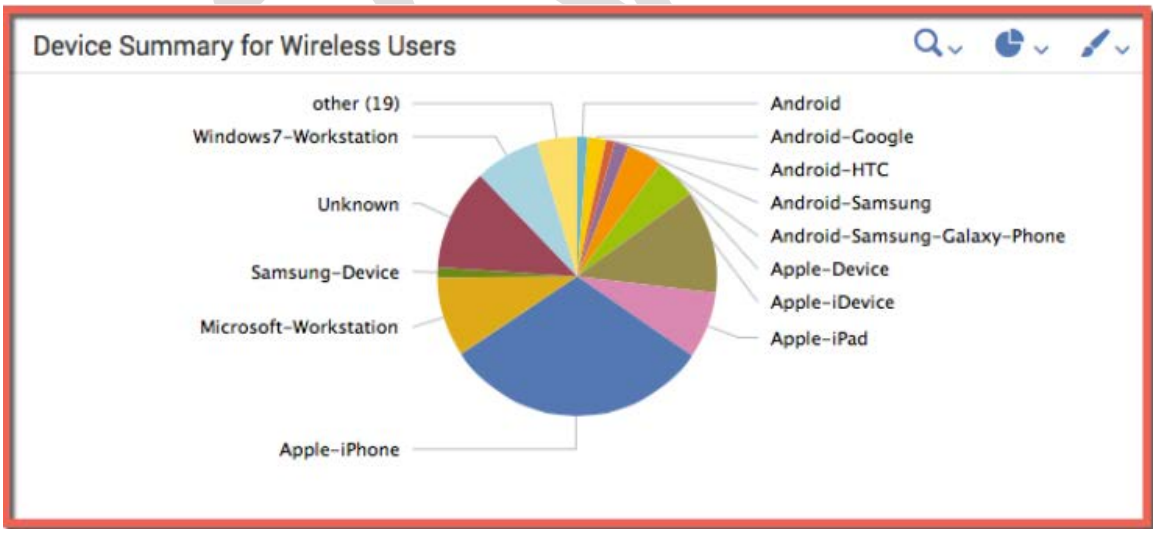


۸-۱- مزایای پیاده سازی Splunk (SIEM) به همراه Cisco ISE :

عموماً پلتفرم‌های SIEM ، اطلاعاتی از قبیل (مکان، زمان، نوع تجهیزات و کاربر متصل به شبکه) را به صورت یکپارچه ندارند و تنها آدرس IP ملاک تصمیم‌گیری آنها میباشد. در صورت یکپارچه سازی ISE با نرم افزار های SIEM ، اطلاعات فوق که تحت عنوان Contextual Data یا داده‌های متنی شناخته میشوند، میتوانند در پلتفرم SIEM دید کامل‌تری از شبکه را در اختیار متصدی امنیت شبکه قرار دهند. این داده های متنی همچنین میتوانند به عنوان شروطی در سیاست های امنیتی (Security policies) استفاده شوند .

برای مثال در پاسخ به یک رخداد امنیتی میتوان از داخل نرم افزار Splunk دسترسی را برای گروه یا فرد خاصی با در نظر گرفتن شروط زمان، مکان، نوع تجهیزات دسترسی به شبکه و غیره ، محدود نمود . این اعمال محدودیت سپس ازطریق نرم افزار ISE بر روی تجهیزاتی از قبیل سوییچ ، مسیریاب، فایروال ASA و یا Wireless Lan Controller ها اعمال میشود.

بعلاوه در مواردی که نیاز به گزارش‌های خاص و شخصی‌سازی شده‌ای باشد که در بخش گزارشات نرم افزار ISE موجود نباشد، این قابلیت در نرم افزار Splunk وجود دارد (که به دلیل وجود زبان جستجویی همانند زبان‌های برنامه نویسی ساده و دستورات متعدد) می‌توان گزارش‌های دلخواه مورد نظر را در بازه های زمانی مورد نظر ایجاد و حتی در قالب یک داشبورد شخصی در سیستم ذخیره کرد. به گونه‌ای که هنگام وارد شدن به داشبورد شخصی تنها گزارش‌هایی که مد نظر کاربر بوده نمایش داده شود. مزیت استفاده از این روش اینست که هیچ گونه محدودیتی در نوع گزارش ها وجود ندارد.

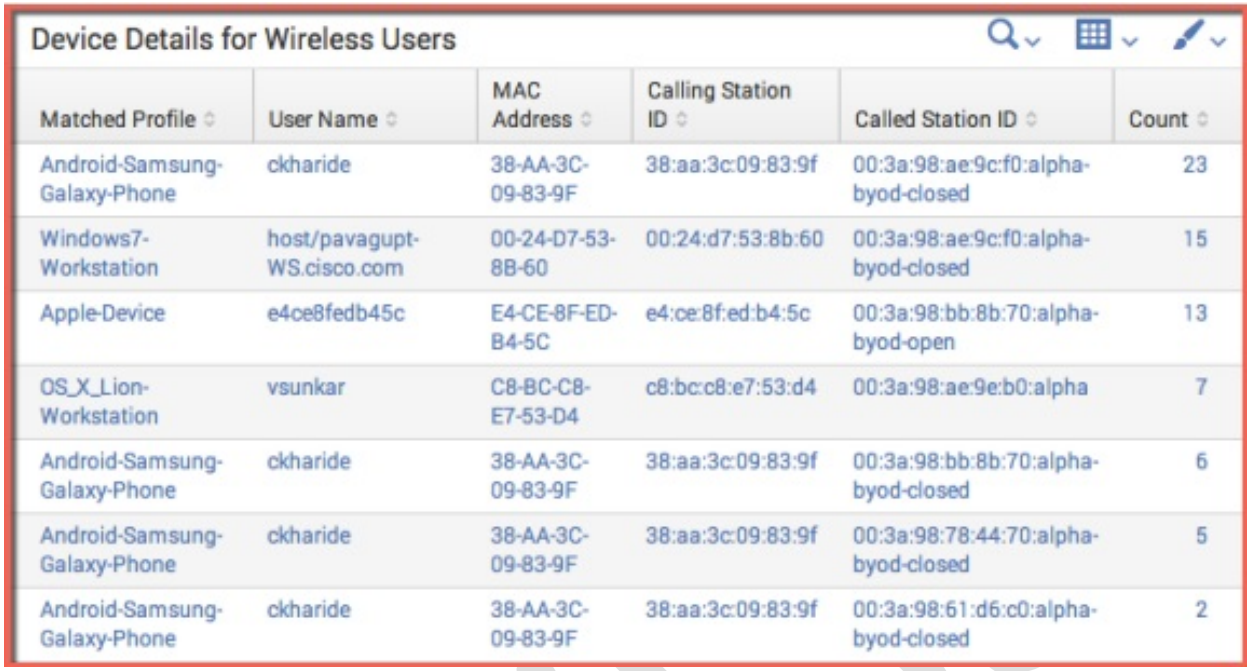


شکل ۲۳ – گزارش کاربران وایرلس متصل به شبکه بر اساس پروفایلینگ صورت گرفته در ISE

نمونه دستور استفاده شده در ISE جهت تولید نمودار پای شکل فوق به صورت زیر میباشد .

```
eventtype=cisco-ise NAS_Port_Type="Wireless - IEEE 802.11" | stats count by EndPointMatchedProfile | rename EndPointMatchedProfile AS "Endpoint Matched Profile"
```

جدول آماری جزییات تجهیزات کاربران وایرلس متصل به شبکه



Device Details for Wireless Users

Matched Profile	User Name	MAC Address	Calling Station ID	Called Station ID	Count
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:ae:9c:f0:alpha-byod-closed	23
Windows7-Workstation	host/pavagupt-WS.cisco.com	00-24-D7-53-8B-60	00:24:d7:53:8b:60	00:3a:98:ae:9c:f0:alpha-byod-closed	15
Apple-Device	e4ce8fedb45c	E4-CE-8F-ED-B4-5C	e4:ce:8f:ed:b4:5c	00:3a:98:bb:8b:70:alpha-byod-open	13
OS_X_Lion-Workstation	vsunkar	C8-BC-C8-E7-53-D4	c8:bc:c8:e7:53:d4	00:3a:98:ae:9e:b0:alpha	7
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:bb:8b:70:alpha-byod-closed	6
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:78:44:70:alpha-byod-closed	5
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:61:d6:c0:alpha-byod-closed	2

دستور استفاده شده در ISE جهت تولید گزارش فوق به صورت زیر میباشد .

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" | fillnull value="NULL"
Called_Station_ID | stats count by EndPointMatchedProfile UserName EndPointMACAddress Calling_Station_ID
Called_Station_ID | sort -count | `format_field_names`
```

۹- مزایای پیاده سازی راهکار BYOD سیسکو در قیاس با دیگر راهکارها :

- به علت اینکه زیرساخت شبکه های فعلی اکثراً بر پایه محصولات سیسکو می‌باشد، استفاده از این راهکار همخوانی بهتری با سایر محصولات زیر ساخت شبکه خواهد داشت.
- نرم افزار ISE کمپانی سیسکو از طریق تکنیک‌ها و روش‌های جدید این شرکت تحت نام pxGrid میتواند به اشتراک داده های متنی (contextual data) همچون هویت (identity)، موقعیت و ... با دیگر تجهیزات امنیتی بپردازد .این قابلیت در حال حاضر مختص ISE میباشد و راهکارهای مشابه در این زمینه این توانایی را ندارند.
- راهکارهای مختلفی که تا به حال در این زمینه ارائه شده‌اند هر کدام نقص‌هایی دارند، برای مثال عدم پوشش دستگاههایی که dot1x را پشتیبانی نمیکنند، نداشتن قابلیت پروفایلینگ و یا بررسی وضعیت سیستم کاربر و ... .

- در نرم افزار ISE قابلیت‌های مهم فوق بعلاوه بسیاری از امکانات دیگر به صورت یکجا و متمرکز موجود است که پیاده سازی و راهبری آن را برای متصدیان شبکه آسان میکند.

قابلیت‌های اشاره شده در این سند سبب گردیده که برای چندمین سال متوالی راهکار BYOD ارائه شده از طرف کمپانی سیسکو به عنوان برترین راهکار در این زمینه از سوی موسسات معتبری همچون گارتنر شناخته شود .

راهکار سیسکو به عنوان برترین راهکار در زمینه NAC و BYOD