ارتباطات و فناوری اطلاعات

فاوا موج

FAVAMOUJ ICT Co.

CISCO ISE SOLUTION

راه حل دسترسی پاک به شبکه

Identity Services Engine

شرکت فاوا موج

فنـــاوری نوین . ارتبـــاط پـــایدار

ICT TOTAL SOLUTIONS

دسترسی پاک به شبکه با محصول منحصر بفرد ISE

با گسترش روز افزون تکنولوژی و در دسترس بودن تجهیزات هوشمند نرخ قابل توجهی از کارکنان و کارمندان سازمان ها خواهان دسترسی به منابع کاری از دستگاه های مختلف و از شبکه های خارج سازمان به شبکه سازمان و اینترنت می باشند که تهدیدات امنیتی بی شمار اهمیت، ایجاد امنیت دسترسی به این شبکه های در حال تکامل را نشان می دهند. همچنین با گسترش روز افزون این شبکه ها پیچیدگی مدیریت منابع و راه کار های امنیتی مختلف نیز افزایش می یابد. بنابراین راهکار متفاوتی برای مدیریت و امنیت شبکه های امروزی نیاز است.

راه کار ارایه شده برای پاسخ گویی به این نیاز ها ISE ، Cisco® Identity Services Engine می باشد.

● معرفی محصول

سیسکو تنها فراهم کننده یک سیاست واحد و هموار در طول کل سازمان است. و در این راستا محصول ISE را ارایه داده است.

Cisco® Identity Services Engine (ISE) برترین محصول در زمینه کنترل دسترسی کاربران به شبکه می باشد. ISE نسل پیشرفته NAC می باشد، که سیسکو از لحاظ معماری و مباحث وایرلس تغییر اساس در آن ایجاد کرده است. با استفاده از این سیستم شما ترکیبی از احراز هویت ، TrustSec Posture Control را یکجا خواهید داشت. جایگاه محصول ISE به عنوان هسته مرکزی راهکار BYOD سیسکو می باشد.

نوآوری های صورت گرفته در (ISE) شامل : zero-touch on-boarding و همگام سازی سیاست ها به صورت مرکزی توسط open API ها با راه حل های مدیریت دستگاه های متحرک (MDM) می باشد. (که شامل تنظیمات سیاست پاک سازی MDM یا سیاست دسترسی به شبکه مبتنی بر MDM posture می باشد.)

محصول ISE سیسکو تنها راه کاری است که هم اسکن مبتنی برنقطه پایانی و هم اسکن مبتنی بر شبکه را فراهم می کند. و این امکان را به سازمان می دهد که آزادی عملکرد تجاری متحرک را فراهم کند و درعین حال با سیاست های مرکزی تعیین کند که چه کسی ، از کجا ، در چه زمانی و چگونه به شبکه دسترسی داشته باشد. قابلیت سنسور دستگاه ها ، امکان شناسایی دقیق انواع مختلف دستگاه درون شبکه را توسط ISE ممکن می سازد و شامل رنج گسترده ای از انواع دستگاه ها می شود که این امکان را به سازمان ها می دهد که دید جامع و قابل توسعه و مقیاس پذیری را برروی شبکه داشته باشند. این محصول همچنین اسکن بلادرنگ نقطه های پایانی را بر اساس سیاست های تعریف شده به منظور بدست آوردن بینش عمیق و مرتبط ترفراهم می کند. این ویژگی های خودکار شده سبب بدست آوردن تجربه کاربری بهترو دستگاه های امن ترمی شود.

● مقدمه

امروزه با توجه به گسترش شبکه¬ها، افزایش کاربران فناوری اطلاعات و خدمات آن مانند اینترنت و بروز پدیده های همچون تجهیزات گوشی های هوشمند و تبلت ها، بیش از پیش نیاز به روال های امنیتی مشخص و کارامد حس می شود. به عنوان مثال، برخی کارمندان و یا میهمانان حاضردر شرکت ها، جهت دسترسی به اینترنت و یا سرویس های داخلی شرکت، قصد استفاده از تلفن همراه یا تبلت خود را دارند. (BYOD)

جهت امکان برقراری اینگونه دسترسی، می بایست کاربرو تجهیزمورد استفاده¬ی وی مطابق با سیاست های سازمانی عمل کرده تا باعث بروز مخاطرات امنیتی نگردد؛ در واقع مکانیزمی می بایست شکل گیرد تا مشخص شود چه شخصی، در چه زمانی، توسط چه تجهیزی، به چه مقصدی، چه میزان دسترسی داشته باشد. (who, how, what, when)

شرکت Cisco در راستای پاسخ گویی به این دغدغه های بیان شده، با معرفی محصول Cisco ISE گام در این راه برداشته است.

بدینوسیله، امکان پیاده سازی سیاست های سازمانی در هرنقطه از شبکه امکان پذیربوده و قابلیت مدیریت متمرکزو گزارش گیری کامل از وقایع تسهیل می گردد.

راه حل دسترسی پاک به شبکه (ISE)

در معماری این محصول، بوسیله ی پیاده سازی policy های dynamic و context-aware، زبان جدیدی از سیاست گذاری امنیتی شکل گرفته است. امنیت شبکه وابستگی خود را از زیرساخت فیزیکی از دست می دهد و امکان تأمین امنیت در طول شبکه مطابق با قوانین مشخص بوجود می آید و تا مرز شبکه با دنیای بدون مرز اینترنت پیش روی می کند. با استفده از این معماری، سیاست گذاری ها و اجراها مؤثرتر خواهد بود؛ همچنین با توجه به استفاده ی این معماری از آرایه ای وسیع از پارامترهای مختلف امنیتی، امکان پیاده سازی قوانین خاص براساس آنالیز وقایع مختلف در کنار هم بوجود می آید.

این معماری ، مدیران شبکه را قادر می سازد تا با احراز هویت کاربر، در هر نقطه از شبکه و توسط هر وسیله ای که کاربر از آن استفاده می کند، سیاست ها و قوانین سازمانی برای وی اعمال گردد.

این معماری، با استفاده از راه کار TrustSec، تضمین می نماید که کاربر براساس ،what ،what ،who ،when ،where و how احراز هویت و تفویض اختیار شده، و همچنین تجهیز مورد استفاده وی، مشخصات موردنظر سازمان (مانند بروز بودن سیستم عامل یا آنتی ویروس) را داشته باشد.

سپس بوسیله ی علامت گذاری ترافیک کاربر (tag)، در طول مسیر با عبور ترافیک از هر تجهیز شبکه، سیاست های خاص آن کاربر روی ترافیک وی اعمال می گردد.

در ابتدای امر، این محصول بعنوان profiler عمل می کند و با کنار هم قراردادن اطلاعات کاربر و عملکرد وی و سایر صفت های موجود مانند زمان، مکان و غیره، یک نمایه کامل و تفصیلی ایجاد می کند تا سیاست های مدنظر براساس آن ها اعمال گردد.

قدرت اعمال قوانین ISE نیز باعث شده تا با ورود کاربر در هر نقطه از شبکه، بلافاصله قوانین مشخص برای وی از همان Ingress port اعمال گردند.

همچنین این محصول، با بررسی رفتار و Signature های موجود، قادر به تشخیص نوع و عملکرد تجهیزت مورد استفاده ی کاربران بوده تا بهترین حالت تأمین امنیت را فراهم آورد.

در واقع می توان گفت این محصول تمام قابلیت های احراز هویت، تفویض اختیار، حسابرسی، Profiler ،Posture و مدیریت مهمان را بطور کامل پیاده سازی می کند.

عملکرد احراز هویت در این محصول از روش های WebAuth ،802.1X و MAC Authentication Bypass (MAB) بهره جویی می کند.

پس از عملکرد احراز هویت کاربر، عملکرد تفویض اختیار (Authorization) صورت می گیرد که از روش های VLAN، ACL و SGA (Security Group Access) استفاده می کند. ACL ها و تعیین VLAN بصورت پویا بلافاصله پس از ارتباط تجهیز کاربر با Ingress Port صورت می گیرد. همچنین ترافیک کاربر در Egress Port تجهیز ورودی، بوسیله ی SGA علامتگذاری می شود.

یکی دیگر از مهم ترین سرویس های این محصول، بحث بررسی Posture می باشد که همانطور که قبلاً بیان شد، با بررسی دقیق وضعیت سیستم کاربر، چه از لحاظ سخت افزاری و چه از لحاظ نرم افزاری، نسبت به حصول اطمینان از تطابق با مشخصات مدنظر سازمان عمل می کند. این سرویس دارای سیاست های از پیش تعریف شده برای بیش از ۳۵۰ نرم افزار مدیریتی و آنتی ویروس است؛ شایان ذکر است ادغام با Active Directory یکی از پایه ای ترین امکانات این سرویس می باشد.

زمینه های کاربرد و کاربران نوعی سیستم

محافظت از داده های سازمانی ، برنامه های کاربردی و سیستم ها برای هرشرکتی ضروری است و سازمان های فناوری اطلاعات می بایست چه از دیدگاه دستگاه ها و چه از دیدگاه دسترسی شبکه ، تجربه امنی را فراهم کنند. بنابراین وقتی شرکت ها استراتژی دسترسی از هر کجا و توسط هر دستگاهی را درون سازمان خود گسترش می دهند ، باید بدانند که چه کسی در شبکه است و از چه محلی به شبکه متصل شده است ، توسط چه دستگاهی به شبکه متصل شده است و وضعیت دستگاه مورد استفاده کاربر به چه صورت است.

بهترین پاسخ برای سازمانی هایی که دارای نیازمندی های زیر می باشند به کارگیری راه کار ISE سیسکو می باشد.

- اطمینان از سالم بودن و امن بودن دستگاه هایی که برای دسترسی به شبکه مورد استفاده قرار می گیرند . این دستگاه ها نباید شامل برنامه ها و بد افزارها یی باشند که بتواند شبکه سازمان و اطلاعات آن را مورد تهدید قرار دهند.
- اطمینان حاصل کردن از این امر که کاربران و دستگاه هایی که به صورت on-premise یا off-premise به شبکه دسترسی پیدا می کنند قابل شناسایی اند و اجازه اتصال به آن ها در شرایطی داده می شود که مجاز شناخته شده باشند و سیاست های شرکت را برآورده کنند.

راه حل دسترسی پاک به شبکه (ISE)

- عملکرد های امنیتی در سطح دستگاه همچون پاک سازی یا قفل کردن دستگاه از راه دور با کنترل دسترسی شبکه یکپارچه شده به منظور اطمینان از امکان انجام هر عملکردی بر روی دستگاه های غیرسازگار در هرزمانی.
- داشتن دید واضح برروی کاربران ، دستگاه ها و برنامه های کاربردی که در شبکه وجود دارد.

ویژگی ها و مزایای محصول

ISE مدیریت امنیتی منابع را با کنترل دید کاربران و دستگاه ها از شبکه و سطح دسترسی آنان انجام می دهد و امنیت منابع را فراهم می کند. اطمینان حاصل می کند تنها افراد درست از دستگاه های درست دسترسی مناسب را به سرویس های سازمان پیدا کنند.

برخلاف راه کار های امنیتی سنتی ، ISE پیاده سازی دسترسی مهمان (Guest) و احراز هویت ۸۰۲٫۱۱ X RADIUS را تسریع می بخشد .

مزایای ISE

از جمله مزایایی که میتوان در سازمان هایی با گستردگی و تنوع کاربران زیاد از آنها بهره برد به صورت زیر می باشد:

- کنترل دسترسی مرکزی و واحد با امنیت بالا
- بدست آوردن دید بهتر و شناسایی دستگاه های دقیق تر
- آسان سازی تجربه کاربر مهمان
- تسریع BYOD و تحرک سازمانی
- پیاده سازی تقسیم بندی های شبکه منطقی مبتنی برنقش ها و قوانین تجاری
- به اشتراک گذاری Contextual data با شرکت های شبکه ای و امنیتی دیگر

ویژگی های عملکردی

ویژگی های عملکردی کلیدی زیراین امکان را می دهد که شما تمامی دسترسی های شبکه خود را مدیریت کنید :

- **دسترسی شبکه مبتنی برهویت**

امکان مدیریت هویت مبتنی برروش های تایید شده و پیکربندی شده را میدهد و این روش ها براساس نوع سیاست سازمان قابلیت پیکربندی را دارند ، برفرض مثال تنها افرادی که عضو AD میباشند اجازه ورود به شبکه را دارند.

- **پشتیبانی از سناریو های پیاده سازی چندگانه**

می توانید ISE را در ساختارهای سازمانی با شبکه وایرلس ، سیمی و VPN پیاده سازی کرد ، همچنین می توان آن را به صورت توزیعی و یا standalone پیاده سازی کرد. برفرض مثال در سازمانی هم از دسترسی سیمی و هم به دلیل استفاده کارمندان از تجهیزات هوشمند مانند موبایل و تبلت ممکن است از سیستم وایرلس استفاده شود و همچنین پیمانکاران با استفاده از راه حل VPN به شبکه وصل شوند بنابراین برای کنترل تمامی این ارتباطات میتوان از حالتهای گوناگون ISE استفاده کرد و تمامی ترافیک ها را به صورت متمرکز بررسی نمود.

- **مجموعه هایی از سیاست های امنیتی**

اجازه میدهد مجموعه ای از سیاست های احراز هویت و تصدیق را پیاده سازی کرد برفرض مثال استفاده از گواهینامه امنیتی خاص برای کاربران عضو AD و حتی برای یک گروه خاص از اکتیو دایرکتوری و یا دسترسی به کاربرانی که تنها با وایربه شبکه وصل میشوند و گواهینامه خاصی نیز برروی تجهیزآنها نصب است .

- **پیاده سازی (Federal Information Processing Standard (FIPS**

به منظور معتبرشناسی مدل های رمزنگاری و ماژول های cryptographic به کار می رود و تمامی قوانین FIPS را که درایالات متحده به تصویب رسیده است را دراین حالت رعایت میکند و از گواهینامه ها نیزنگه داری میشود .

- **پشتیبانی از عملکرد Common Access Card Functions**

CAC یک دستگاه احراز هویت است که ISE امکان کارکردن با آن را نیزدارد.

Client Posture Assessment

اطمینان حاصل میکند که به روزترین تنظیمات امنیتی و نرم افزارهای امنیتی بر روی ماشین کلاینت موجود باشند و با بررسی Services ، DLL ، Registry ، به روز بودن آنتی ویروس به سالم نگه داشتن شبکه کمک شایانی میکند و کامپیوترهایی که برخلاف سیاست های ما باشند را به VLAN دیگری میفرستند تا پس از رفع مشکل دوباره وارد شبکه اصلی شوند و این اتفاق به صورت اتوماتیک می افتد به دلیل این که CoA به صورت داینامیک عمل میکند .

دسترسی به شبکه برای کاربران مهمان

این ویژگی امکان تعریف حساب های کاربری برای مهمانان با مجوز های دسترسی متناسب با آنها را ایجاد می کند. در سرویس ISE یکی از ویژگی های منحصربه فرد نسبت به سیستم های دیگر وجود راه حل Guest Portal میباشد که با استفاده از یک پورتال ساده کاربران مهمان را به شبکه های از پیش تعیین شده ، اجازه دسترسی میدهد . و کاربران مهمان با وارد کردن مشخصات خود و با تایید مدیر وارد شبکه میشوند و یا با نام های کاربری Local برای مدت محدود به منابع محدود دسترسی خواهند داشت .

پشتیبانی از دستگاه های شخصی

اجازه می دهد کارمندان از دستگاهی شخصی خود به شبکه وصل شوند و استفاده کنند بدون هیچ گونه دغدغه ای از لحاظ امنیتی. با توجه به این که ISE تجهیزات و پلت فرم های گوناگون را میشناسد میتواند براساس نوع و پلت فرم آنها تصمیم گیری کند و دسترسی آن را مشخص کند.

ترافیک بی سیم و VPN از طریق گره های Inline Posture

پس از آنکه کاربر توسط بی سیم و یا VPN به شبکه دسترسی پیدا کرد این وظیفه Inline Posture است که سیاست های امنیتی باقیمانده که توسط دستگاه های دیگر قابل اجرا نیست را اعمال کند . و کاربران در هر نقطه ای که باشند مورد بررسی قرار میگیرند.

نقاط پایانی پروفایل شده در شبکه

کمک میکند به شناسایی ، مکان یابی ، و تشخیص ظرفیت های تمام دستگاه های پایانی .

پشتیبانی از دستگاه های SAnet (Session Aware Networking)

Sanet یک چهارجوب پروتکل میدیریت session در سویچ هاست که سبب پایداری بیشتر و منعطف تر کردن دسترسی می شود.

CISCO IDENTITY SERVICES ENGINE (ISE)

- پشتیبانی از نصب برروی بسترهای سخت افزاری و مجازی چندگانه

هم به صورت از قبل نصب شده برروی SNS-۳۴۰۰ Series appliance وجود دارد و هم می توان آن را برروی سرور های مجازی نصب کرد.

مکانیزم احراز هویت

اساس پروتکل احراز هویت در ISE پروتکل ۸۰۲٫۱x می باشد ، که چهار چوبی برای آدرس دهی و فراهم آوردن کنترل دسترسی مبتنی برپورت با استفاده از احراز هویت می باشد. در درجه اول ۸۰۲٫۱x یک تعریف بسته بندی برای بسته های EAP برروی LAN (EAPOL) به عنوان یک پروتکل کلیدی می باشد. به بیان دیگرا۸۰۲٫۱x. یک پروتکل لایه دو به منظور انتقال پیغام های احراز هویت بین درخواست کننده (کامپیوتر با کاربر) و احراز هویت کننده (سوئیچ یا اکسس پوینت) می باشد.

تعریف دسترسی

تعریف دسترسی در ISE می تواند به صورت های مختلف صورت پذیرد که همگی آن ها برمبنای دسترسی Context-Based می باشد.

شکل زیرنشان دهنده مهم ترین پارامترهای درنظرگرفته شده به هنگام تعریف دسترسی در ISE می باشد.

Who? Known users (Employees, Sales, HR) Unknown users (Guests)	**What?** Device identity Device classification (profile) Device health (posture)	**How?** Wired Wireless VPN
Where? Geographic location Department SSID / Switchport	**When?** Date Time Start/Stop Access	**Other?** Custom attributes Device/User states Applications used

Identity Store تحت ساپورت در ISE

در زیر می توان لیستی از Identity Store های قابل استفاده در ISE را مشاهده کرد.

Identity Store	OS / Version
ISE	Internal Endpoints, Internal Users
RADIUS	RFC 2865-compliant RADIUS servers
Active Directory	Microsoft Windows Active Directory 2000 Microsoft Windows Active Directory 2003, 32-bit only Microsoft Windows Active Directory 2003 R2, 32-bit only Microsoft Windows Active Directory 2008, 32-bit and 64-bit Microsoft Windows Active Directory 2008 R2, 32-bit and 64-bit
LDAP Servers	SunONE LDAP Directory Server, Version 5.2 Linux LDAP Directory Server, Version 4.1 NAC Profiler, Version 2.1.8 or later
Token Servers	RSA ACE/Server 6.x Series RSA Authentication Manager 7.x Series RADIUS RFC 2865-compliant token servers SafeWord Server prompts

پروتکل EAP تحت ساپورت در ISE

Challenge-response-based	• EAP-MD5: uses MD5 based challenge-response for authentication • LEAP: username/password authentication • EAP-MSCHAPv2: username/password MSCHAPv2 challenge-response authentication
Certificate-based	• EAP-TLS: X.509 v3 PKI certificates and the TLS mechanism for authentication
Tunneling methods	• EAP-PEAP: encapsulates other EAP types in an encrypted tunnel • EAP-TTLS: encapsulates other EAP types in an encrypted tunnel • EAP-FAST: designed to not require client certificates
Other	• EAP-GTC: generic token and OTP authentication • GSS-API : Kerberos

Profiling

این قابلیت در ISE باعث می شود کلیه تجهیزات موجود در شبکه برحسب نوع و ماهیت آن ها طبقه بندی شوند که با توجه به این طبقه بندی می توان سیاست لازم را اتخاذ نمود.

نوع دستگاه (پروفایل) : براساس اینکه دستگاه در چه نوع گروهی (مثل : لپ تاپ ، موبایل و یا دستگاه های غیرکاربرو غیره) جای می گیرد بررسی می شود.

سیسکو ISE در این قابلیت خود با استفاده از منابع زیرنوع دستگاه را مشخص می نماید.

RADIUS	SNMP Queries/Traps	HTTP Span
Netflow v5/v9	DHCP Span/Helper/Proxy	DNS Lookup

Posture

این عملیات از جمله عملکرد های خاص و مهم سیستم ISE می باشد.

معمولا این عمل به صورت فعالانه با برآوردهای مبتنی برشبکه انجام می شود که یا توسط agent های موجود بردستگاه های درون شبکه و یا توسط پرتال وب مورد استفاده درخواست کننده انجام می پذیرد.

بدین صورت که agent قبلا برروی سیستم یا دستگاه نصب شده است و یا از طریق هدایت ترافیک کاربربه صفحه وبی به صورت اتوماتیک ویا با کسب اجازه از کاربربه صورت دستی نصب می شود تا عملیات Posture انجام شود.

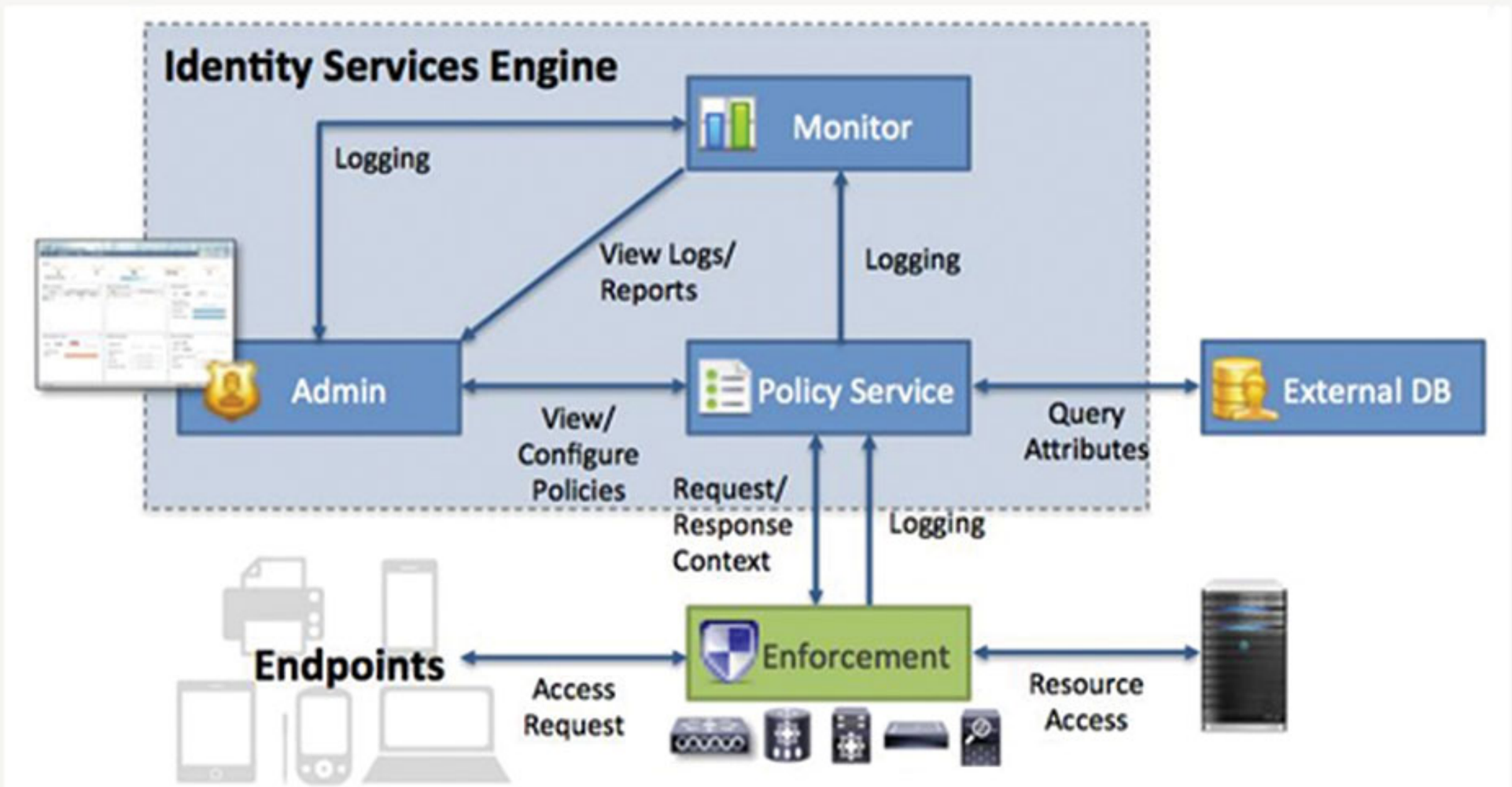
عملیات Posture مواردی از قبیل نصب بودن و به روز بودن آنتی ویروس ، رجیستری های سیستم عامل ، فایل های سیستمی ، به روز بودن سیستم عامل ، برنامه های نصب شده برروی سیستم و غیره را مورد بررسی قرار می دهد.

مانیتورینگ و عیب یابی در ISE

از جمله امکانات منحصربه فرد سرویس ISEکنسول مدیریتی آن است که ابزار مانیتورینگ و عیب یابی پیشرفته ای در اختیار مدیران شبکه قرار می دهد که متناسب با نیاز ها بسیار جامع و کامل است. از جمله کاربردی ترین موارد قابل ذکر در این کنسول می توان به موارد زیر اشاره کرد:

- مشاهده لاگ های احراز هویت به صورت در لحظه در یک جدول واحد که امکان customize کردن آن نیز وجود دارد و امکان جستجو پیشرفته در لاگ ها براساس حساب کاربری و آدرس و IP و بسیاری موارد دیگر را نیز داراست.
- ممیزی پیکربندی و تنظیمات دستگاه های شبکه.
- امکان تعریف ایجاد اخطار در صورت بروز شرایط خاص و مد نظر مدیر شبکه.
- امکانات گزارش گیری متنوع و کارآمد.

نحوه کار سیسکو ISE



شکل بالا نمایی نمونه از نمودار منطقی ISE را نمایش می دهد .

همانگونه که در این شکل نمایان است:

ارتباط از جانب نقطه پایانی آغاز می شود. (که میتواند لپ تاپ و تلفن ، هوشمند، تبلت ، دوربین امنیتی ، سیستم های ویدیو کنفرانس و هرچیز دیگری که نیازمند دسترسی شبکه هست باشد).

کلاینت می بایست از طریق یک دستگاه دسترسی به شبکه متصل شود (سویچ ، کنترل کننده lan وایرلس ، متمرکزکننده vpn و غیره) این جایی است که اجرای تمام سیاست های امنیتی (Policy Enforcement) اتفاق میافتد .

از ایستگاه پایانی تقاضای یک احراز هویت می شود. و این درخواست به گره سرویس سیاست های امنیتی فرستاده می شود.

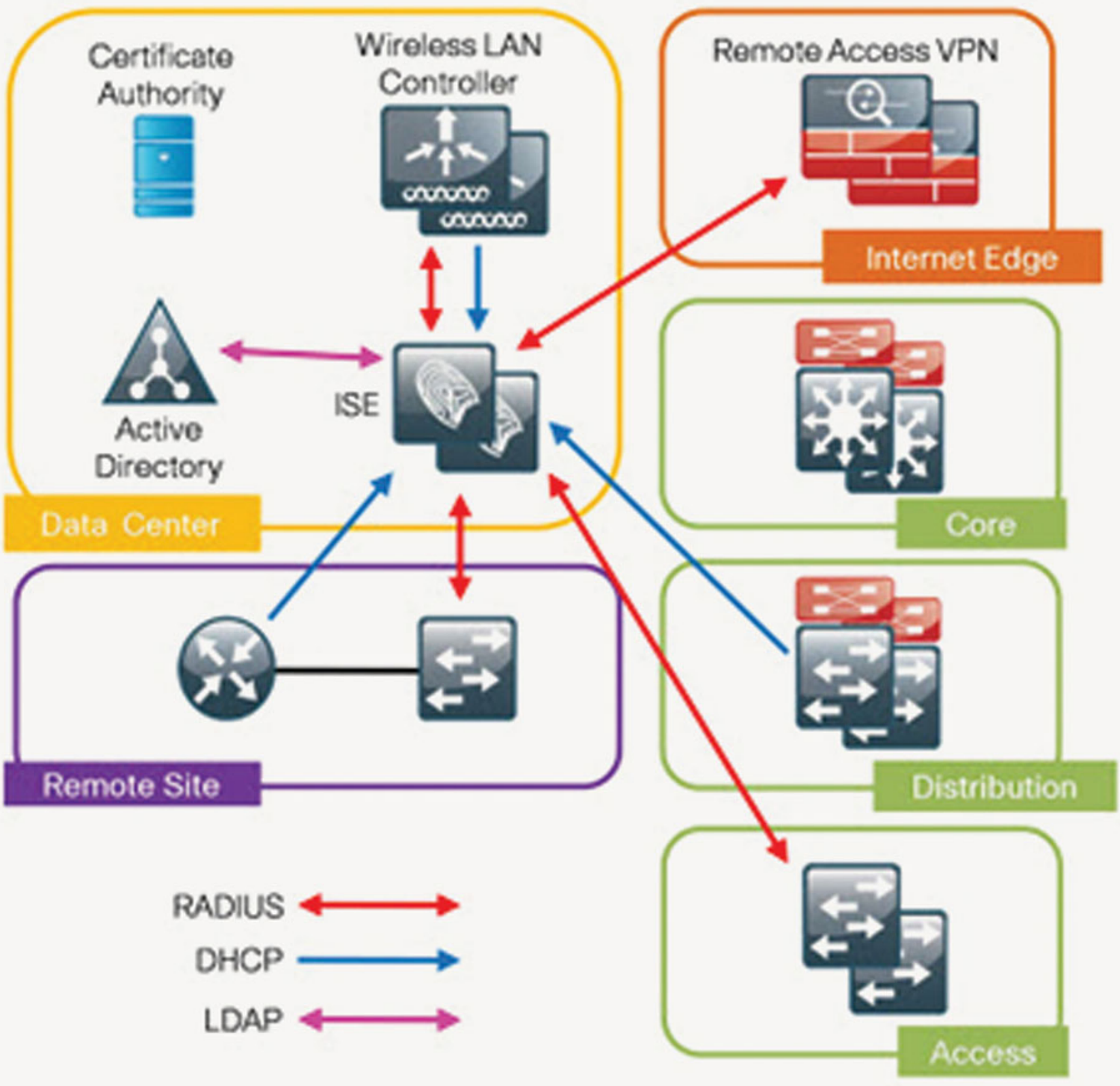
در این مرحله از قبل به گره سرویس سیاست های امنیتی توسط گره مدیریت پیکربندی داده شده است. گره سرویس سیاست های امنیتی مجوز دسترسی را پردازش می کند و ممکن است نیاز به پرسش و پاسخ از یک پایگاه داده خارجی همچون Active Directory ، LDAP و غیره باشد.

(در مورد سازمان ما ، با پرسش و پاسخ از AD و متناسب با گروه های تعریف شده در آن و عضویت کاربران در این گروه ها و سیاست های امنیتی از قبل تعریف شده بر روی آنها سطح دسترسی کاربران به منابع شبکه مشخص می شود) سپس مبتنی بر مجموعه پیکربندی گره سرویس سیاست های امنیتی یک تصمیم احراز هویتی اعمال می کند.

گره سرویس سیاست های امنیتی تصمیم را به دستگاه دسترسی شبکه می فرستد تا آن بتواند تصمیم را اجرا کند . عملیات معینی برای اجرا بر روی session به دستگاه دسترسی شبکه فرستاده می شود. عملیات زیادی متناسب با سیاست امنیتی در اینجا می تواند انجام شود ، اما فقط برخی ویژگی های عمومی شامل لیست های دسترسی پویا ، change of authorization و برچسب های گروه های امنیتی می باشد.

حال کلاینت می تواند به منابع خاص مشخص شده مبتنی برآنچه که گره سرویس سیاست های امنیتی به عنوان مجموعه قوانین فرستاده است دسترسی پیدا کند. و یا متناوبا کلاینت می تواند به صفحه ورود مهمان هدایت شود و یا کاملا از دسترسی اش به شبکه جلوگیری شود.

تمام این پیغام هایی که ارسال و دریافت شدند در گره مانیتورینگ ثبت می شوند و توسط گره مدیریت در یک فرمت سازمان دهی شده قابل مشاهده می باشند.
و به طور کلی فلوچارت عملکرد ISE به صورت زیر خواهد بود:



ارتباطات و فناوری اطلاعات
فاوا موج

CISCO IDENTITY SERVICES ENGINE (ISE)

دسترسی پاک به شبکه

با راه حل جامع:

CISCO Identity Services Engine

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

تلفن : ۸۹۳٤۱۰۰۰ دورنگار : ۸۹۳٤۱۰۰۱

پست الکترونیک : info@favamouj.com

وب سایت : www.FavaMouj.com