بسمه تعالی

سامانه مدیریت و نظارت بر دسترسی راه دور

فیدار پم

شناسه سند ..... Fidar_PAM_Introduction_14041208_V5

نوع سند ..... پروپوزال

شماره نگارش ۰.۵

تاریخ نگارش 14041208

طبقه‌بندی سند ..... **عادی**

تهران، خیابان ولیعصر – فاطمی کوچه شهید حمید صدر پلاک ۶۲ طبقه ۳ واحد ۵

(۰۲۱) ۸۸۸۰۸۳۸۰

(۰۹۱۹) ۶۳۹۲۹۲۶

www.xnetx.ir

فهرست مطالب

۱ مقدمه

در سال‌های اخیر با رشد روزآفزون وابستگی سازمان‌های بزرگ به شبکه‌های رایانه‌ای، مخاطرات درون سازمانی نیز جایگاه ویژه ای را در فهرست نگرانی‌های امنیتی این سازمان‌ها به خود اختصاص داده است.

منابع سازمانی عمدتا به صورت دیجیتال و بر بستر شبکه‌های رایانه ای نگهداری می‌گردند تا دسترسی به آن‌ها در تمامی نقاط سازمان مهیا گردد، که این موضوع سبب می‌گردد تا تمامی این نقاط در دسترس مدیران و کاربران مجموعه قرار گیرد. مدیران و کاربران با سطح دسترسی ممتاز عمدتا دارای دسترسی‌های نا محدود به این منابع هستند که این مساله می‌تواند منجر به آسیب‌هایی مانند نشت اطلاعات، دسترسی غیر مجاز به منابع، تخریب و حذف اطلاعات حیاتی به صورت سهوی و یا با برنامه ریزی قبلی، گردد.

روش‌هایی که عموما به طور سنتی به منظور کنترل دسترسی افراد در سازمان‌ها به کار گرفته می‌شوند، معمولا یا با محدود کردن کامل دسترسی افراد و مدیران و یا حذف تمامی محدودیت‌ها صورت می‌پذیرد که در مورد اول، افراد به منظور انجام وظایف روزمره خود با مشکلات بسیاری مواجه می‌گردند که همین موضوع گاها سبب می‌شود تا فرهنگ سازمانی ناخودآگاه به سمت پیروی اجباری از بدعت‌های امنیتی سوق داده شوند که در دراز مدت آثار مخرب بسیاری را به جا خواهد گذاشت. در مورد دوم نیز، عدم وجود هرگونه نظارت و محدودیت دست کاربران و مدیران سازمان را برای سواستفاده‌های احتمالی کاملا باز می‌گذارد.

از سوی دیگر، ابزارهای نظارت و پیشگیری تا حد مشخصی توان تشخیص و جلوگیری از اعمال مخرب را دارا می‌باشند، و در صورتی که هیچ سازوکار حسابرسی بر اعمال مدیران و کاربران وجود نداشته باشد، امکان انجام و پیگیری اقدامات قانونی به منظور حبران خسارات وارده به هیچ عنوان میسر نخواهد بود، زیرا دلایل محکمه پسندی دال بر دخالت فرد یا افراد در بروز خسارت وارد شده وجود نخواهد داشت.

سامانه‌های مدیریت دسترسی‌های ممتاز یا به اختصار PAM پاسخ جامعی به به نیازهای فوق و همچنین سایر جنبه‌های مخاطرات درون سازمانی ارایه می‌دهند که در صورت پیاده سازی و اجرا موثر، تا حد بسیار زیادی خسارات ناشی از دسترسی‌های غیر مجاز را کاهش خواهد داد.

۲ سازمان‌های بزرگ و مخاطرات درون‌سازمانی

دسترسی امن و کنترل شده به زیرساخت‌های فناوری اطلاعات در راستای برقراری تعاملات درون یا برون‌سازمانی همواره یکی از دغدغه‌های اصلی سازمان‌های بزرگ بوده است. گوناگونی نرم‌افزارها و سیستم‌های عامل مورد استفاده و همچنین وابستگی تمامی بخش‌های سازمان به سامانه‌های نرم‌افزاری سبب شده است تا بستری مستعد برای اقدامات مخرب سهوی و برنامه‌ریزی شده شکل بگیرد. در این راستا، بازدارندگی، پیشگیری، تشخیص و حسابرسی ۴ اصل مهم و حیاتی در مدیریت درسترسی‌های محلی و راه‌دور می‌باشد.

نباید از نظر دور داشت که محدود ساختن میزان دسترسی کاربران به منابع سازمانی همواره با کاهش بهره وری آنها همراه خواهد بود و دستیابی به امنیت دسترسی از طریق کاهش چشم‌گیر اختیارات به تنهایی تضمین کننده امنیت منابع سازمانی نخواهد بود.

راه‌کاری که توسط این مجموعه ارائه شده است، با در نظر گرفتن مراحل مورد اشاره فوق، و با اعمال محدودیت‌های کنترل‌شده و لایه‌ای و همچنین پیاده‌سازی حسابرسی دقیق در لایه‌های مختلف امکان بروز مخاطرات و فعالیت‌های مخرب را تا حد بسیار زیادی کاهش می‌دهد.

در ادامه به بررسی هر چهار جنبه‌ی عملیاتی این سامانه خواهیم پرداخت.

۲-۱ بازدارندگی

استفاده از سازوکارهای استاندارد و پیش‌فرض برای دسترسی به زیرساخت‌ها و منابع شبکه، مانند Microsoft Remote Desktop Client برای پروتکل RDP و یا Putty برای پروتکل SSH همواره مورد استفاده مدیران و کارشناسان فنی بوده است، و این موضوع سبب شکل‌گیری یک حاشیه امنیت ذهنی برای

آنها شده است. تغییر الگوی دسترسی و فاصله گرفتن از ابزارهای مورد اشاره، این امنیت ذهنی کاذب را نزد استفاده کنندگان از بین خواهد برد.

این سامانه با استفاده از تکنولوژی های مبتنی بر وب، و با استفاده از مرورگرهای متداول امکان دسترسی کامل به منابع شبکه را در اختیار کاربران قرار خواهد داد. شایان ذکر است، تمامی امکانات موجود در Clientهای اصلی پروتکل‌های دسترسی همچنان در اختیار کاربران خواهد بود و استفاده از مرورگر موجب کاهش اختیارات و امکانات کاربران نخواهد گردید.

۲-۲ پیشگیری

کنترل اختیارات کاربران دارای نقش مهم و حیاتی در پیش‌گیری از حوادث سهوی و همچنین اقدامات مخرب می‌باشد. از همین رو، این سامانه با در اختیار نهادن مجموعه گسترده‌ای از متغیرها و نمایه‌های مختلف، انعطاف پذیری بالایی را در اختیار مدیران بالایی سازمان ها قرار میدهد تا ضمن ارائه اختیارات مورد نیاز، از اعطای اختیارات غیر ضروری و خطر آفرین نیز جلوگیری به عمل آورند. از جمله این‌ها میتوان به محدود ساختن دسترسی به کارگزارهای خاص، اعمال محدودیت در دستورات اجرایی توسط کاربر و همچنین عدم دسترسی به اطلاعات محرمانه شامل نام‌های کابری و رمزهای عبور اشاره کرد.

۲-۳ تشخیص

آگاهی به موقع از مخاطرات احتمالی در طول زمان دسترسی کاربران می‌تواند از بروز خسارات جبران ناپذیر پیش‌گیری نماید. این سامانه مدیران را قادر می‌سازد تا به طور زنده صفحه نمایش، اطلاعات مربوط به کیبورد، ماوس و نقل و انتقال اطلاعات را زیر نظر گرفته و در هر لحظه نسبت به قطع دسترسی کاربر اقدام نمایند.

۲-۴ حسابرسی

تمامی وقایع مربوط به اتصال و تعامل کاربر با شبکه به طور کامل ثبت و نگهداری می‌شوند تا امکان بازبینی کامل تعاملات کاربر با شبکه توسط مدیران شبکه فراهم گردد. اطلاعات ثبت شده شامل مواردی مانند صفحه نمایش کاربر، صفحه کلید، ماوس، کلیپ‌بورد و نقل و انتقال فایل می‌باشد. این اطلاعات به صورت بهینه شده ذخیره می‌گردند تا مانع از مشکلات مربوط به فضای ذخیره‌سازی در دراز مدت گردد.

۳ ویژگی‌های کلی سامانه

از مهمترین ویژگی‌های «سامانه مدیریت و نظارت بر دسترسی راه دور» می‌توان به موارد زیر اشاره کرد:

- پشتیبانی از پروتکل رایج دسترسی راه‌دور: RDP, SSH, VNC , TELNET,HTTP/S, DataBases(Oracle,Mysql,MSQL)
- واسط کاربری مبتنی بر فناوری‌های وب HTML5 و WebSocket
- بدون نیاز به نصب هرگونه Pluginیا افزودنی جانبی
- قابلیت نصب در حالت شفاف و غیر شفاف
- امکان دسترسی از طریق دستگاه‌های همراه مانند تلفن همراه یا تبلت
- امکان نصب سامانه در چندین نقطه مجزا و مدیریت دسترسی‌ها از طریق یک واسط کاربری
- نصب و راه‌اندازی بدون نیاز به اعمال تغییرات در زیرساخت شبکه
- مدیریت آسان و قدرتمند برای کاربران و مدیران سامانه
- ثبت دقیق وقایع در طول ارتباط کاربران با منابع شبکه
- جلوگیری از ورود دستورات در نشست ها
- قابلیت OCR تمام محتوا صفحه
- امکان جستجو در دستورات ارسال شده به سرور
- محدودسازی دسترسی راهبران ارشد سیستم
- احراز هویت دو مرحله ای
- ذخیره امن کلمات عبور
- قابلیت شفاف سازی (Transparent Mode)
- نظارت بر ارتباطات
  - SSH
  - VNC
  - Remote Desktop
  - Telnet
  - Database (Oracle,SQLServer,Mysql,Redis, Mongodb)
  - HTTP/S
- کنترل و بررسی نشست ها بصورت لحظه ای و زنده
- مدیریت کلید های SSH
- کنترل دسترسی پیشرفته کاربران به منابع سامانه

- کنترل دسترسی پیشرفته کاربران به سرورها
- تنظیمات پیشرفته جهت کنترل دسترسی کاربران به سامانه
- تنظیمات کنترلی مختلف از جمله
  - ارسال کننده ایمیل
  - ارسال کننده پیامک
  - پشتیبانی از SNMP
  - قابلیت افزایش دیسک ذخیره سازی
  - انتقال فایل بر بستر FTP
- قابلیت Bastion جهت محدودسازی gateway دسترسی به سرورها
  - منع دسترسی به SSH در نشست های برقرار شده
  - منع دسترسی به TELNET در نشست های برقرار شده
- گروه بندی مجازی
- قابلیت شخصی سازی داشبورد بصورت محدود
- مدیریت فرآیند کاری
- ارتقای سطح دسترسی و مدیریت نقش ها
- قابلیت ثبت سامانه های احراز هویت
  - Active Directory
  - LDAP
  - Radius
  - TACACS+
- ورود یکپارچه با استفاده از یک پسورد کاربر
- قابلیت جلوگیری از حملات Brute Force با اعمال تنظیمات Captcha
- اضافه کرد کاربران از Active Directory
  - به صورت دسته بندی شده بر اساس Orgnization Unit
- کنترل دسترسی توسط یک ادمین
- زمانبندی برای انقضا و اعتبار پسورد کاربران
- راهکار جداسازی اینترنت از شبکه داخلی
- قابلیت اشترک گذاری یک برنامه خاص برای کاربران در نشست
  - اشتراک گذاری برنامه های متفاوت برای هر کاربر
- قابلیت پشتیبان گیری از دیتابیس و اطلاعات کاربران
- مدیریت لاگ های سرور سامانه در برنامه وب
- پشتیبانی از سامانه های SIEM و لاگ مانیتورینگ

- مدیریت زمان فایل های آپلود شده سرور
- ایجاد دسترسی و مدیریت انتقال فایل بر روی نشست
  - قابلیت مشاهده و کنترل فایل منتقل شده توسط مدیر سیستم
  - لیست سیاه و سفید برای ئسوند فایل‌های قابل انتقال در نشست
  - محدود سازی در حجم فایل‌های انتقال داده شده در نشست
- اسکن فایل ها قبل از انتقال بر روی سیستم مبدا و مقصد توسط سامانه کاوش
- ایجاد چند نشست همزمان برای یک کاربر
- پشتیبانی از قابلیت رمز یکبار مصرف TOTP از طریق
  - ایمیل
  - پیامک
  - QR Code
  - Google Authenticator
- تخصیص دسترسی برای هر کاربر به طور اختصاصی
- گزارش ساز منعطف جهت Export کاربران و دسترسی های هر کاربر در قالب
  - فایل اکسل
- انطباق
  - گزارشگیری سفارشی
  - لاگ متنی
  - نمودار آمار اتصالات
- بازبینی کامل تعامل کاربر با منابع شبکه با اعمال زمان‌بندی دقیق:
  - صفحه نمایش
  - صفحه کلید
  - ماوس
  - کلیپبورد
  - انتقال دو طرفه فایل
- امکان Export تعامل کاربر به صورت ویدئو (صفحه نمایش) و فایل‌های متنی (کیبورد)
- ثبت کلیه رویدادهای سامانه مانند ورود، اتصال و قطع کاربران و ارسال آنها به سایر سامانه‌های ثبت متمرکز وقایع
- قابلیت HA به دو صورت داکر و سخت افزار مجزا

در ادامه به بررسی دقیق‌تر این ویژگی‌ها خواهیم پرداخت.

۳-۱ ویژگی‌های سامانه در بخش کاربران

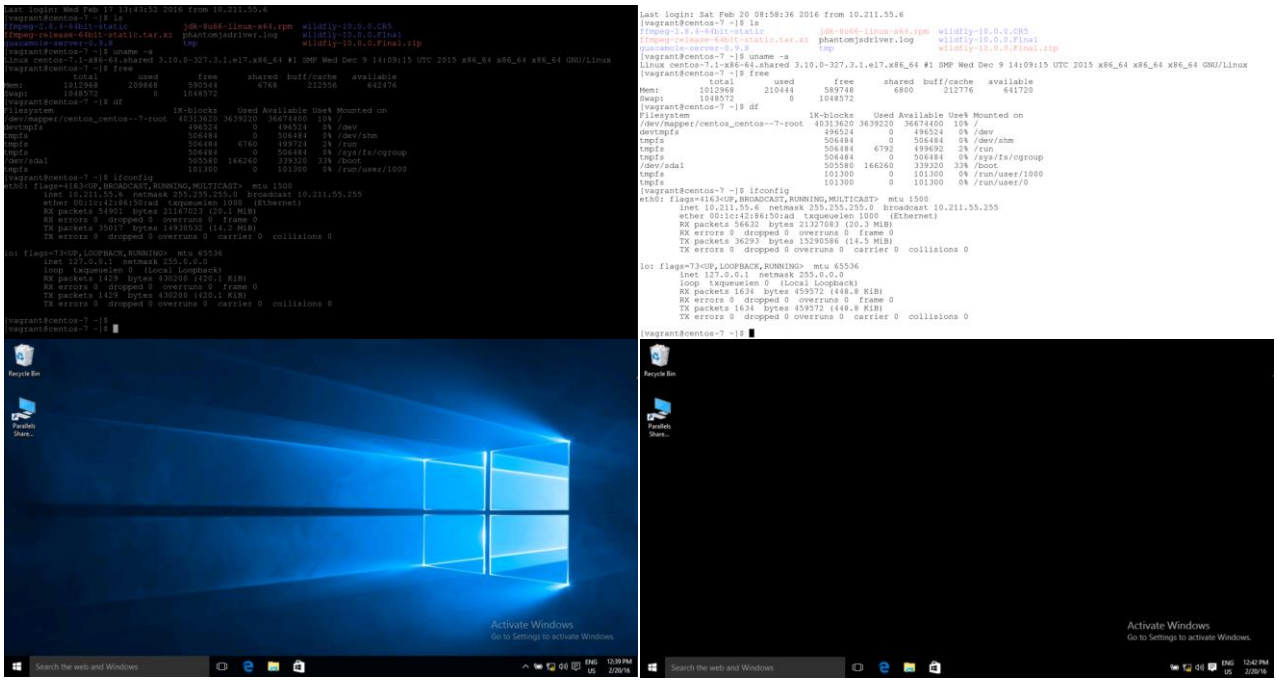
- ایجاد دسترسی برای کاربران به یک یا چند منبع شبکه
- کاربر در سامانه فیدارپم می تواند با قابلیت شفاف سازی Transpatern Mode از سامانه استفاده کند
- پشتیبانی از احراز هویت چندوجهی در صورت وجود زیرساخت فعلی
- محدود ساختن کاربران به دسترسی به منابع شبکه در روزها و ساعت‌های از پیش تعیین شده
- محدود ساختن تعداد اتصالات همزمان کاربر
- سیاست انتقال فایل بر اساس نوع فایل و حجم فایل
- محدود کردن کاربران به اجرای یک برنامه خاص (در دسترسی‌های از نوع RDP)
- امکان یا محدود سازی استفاده از کلیپبورد به منظور انتقال دو طرفه اطلاعات
- امکان یا محدود سازی نقل و انتقال دو طرفه فایل
- امکان اسکن فایل های منتقل شده بر روی نشست یا از روی نشست توسط سامانه کاوش
- امکان یا محدود ساختن استفاده از Audioدر اتصالات RDP
- قابلیت اتصال و استفاده از طریق دستگاه‌های Touch مانند تلفن همراه هوشمند یا تبلت
- ذخیره‌سازی امن اطلاعات حساس منابع شبکه به استفاده از AES 256

۳-۲ ویژگی‌های سامانه در بخش مدیران

- ایجاد کاربران «حسابرس» با اختیارات قابل تعریف:
- دسترسی به اطلاعات ثبت شده کاربران یا اتصالات خاص
- تخصیص میزان پیچیدگی پسورد برای کاربران
- امکان تخصیص نشست های شفاف به کاربر(Transpatrent Mode)
- نوع دسترسی مانند صفحه نمایش، اطلاعات کیبورد، کلیپبورد و یا انتقال فایل
- تعریف هشـــدارهای مدیریتی با نمایه‌های قابل تعریف جهت واکنش ســـریع به رویدادهای حاصـــل از تعامل کاربران با منابع شبکه
- مشاهده فهرست اتصالات در حال انجام و خاتمه پذیرفته به همراه جزییات اتصال
- مشاهده اتصالات در حال انجام به صورت زنده (شامل صفحه نمایش، صفحه کلید، کلیپبورد و انتقال فایل)
- دریافت کامل تعامل کاربر به صورت فایل ویدئو

- دریافت گزارش کامل از عملکرد کاربران از قبیل:
  - تعداد احراز هویت‌های انجام شده بر حسب زمان
  - مدت زمان نشست‌های اخیر
  - مدت زمان نشست‌های اخیر
  - مجموع اقدام ورود به سامانه
  - تعداد نشست‌های ایجاد شده بر حسب زمان
  - فایل‌های جابجا شده توسط کاربر
  - محدودیت ورودی نقض شده توسط کاربر
- قابلیت جستجو در ورودی‌های صفحه کلید به منظور یافتن دستورات یا ورودی‌های مخاطره آمیز
- قطع دسترسی کاربر به صورت لحظه‌ای
- ایجاد دسترسی به کاربر فقط به یک برنامه خاص در نشست
- مشاهده وضعیت سامانه به منظور بررسی بار و اطلاعات لحظه‌ای سامانه

۳-۳ ویژگی های انحصاری پروتکل ها



پروتکل RDP

- احرازهویت از طریق نام کاربری، گذرواژه و نام دامنه
- پشتیبانی از روش‌های رمزنگاری RDP Standard, TLS, NLA و Server Selected

- پذیرش Self-signed Certificate در صورت نبود CA مناسب در شبکه
- امکان مشخص کردن Client Name تا Endpoint نهایی بتواند در صورت نیاز تشخیص دهد که از چه نقطه ای بدان متصل شده‌اند.
- امکان اتصال به Console به جای Sessionهای مجزا
- امکان استفاده از پروتکل RDP در حالت شفاف یا Transparent
- امکان تعیین یک برنامه تا به محض اتصال کاربر برای وی اجرا شود
- امکان محدود کردن Session کاربر به یک برنامه خاص و همینطور یک Working Directory خاص (این ویژگی تنها در صورت فعال بودن RemoteApp در Endpoint قابل ارایه خواهد بود)
- امکان تعیین Color Depth از میان ۲۵۶ رنگ، ۱۶ بیت، ۲۴ بیت و ۳۲ بیت
- پشتیبانی از نقل و انتقال دوطرفه فایل
- امکان فعال یا غیر فعال کردن Theme، Wallpaper، Animationها
- پشتیبانی از Keyboard Layout لاتین و Unicode در سمت Endpoint

پروتکل SSH

- پشتیبانی از نام کاربری و گذرواژه برای احرازهویت
- پشتیبانی از PKI و Passphrase برای احراز هویت
- قابلیت برقراری نشست در مد شفاف
- قابلیت حذف اطلاعات رمز عبور استفاده شده در نشست
- امکان فعال سازی نقل و انتقال فایل از طریق SFTP

پروتکل TELNET

- امکان تشخیص Password Prompt توسط Regular Expression

پروتکل VNC

- پشتیبانی از احرازهویت توسط گذرواژه (Password)
- امکان تعیین Color Depth از میان ۲۵۶ رنگ، ۱۶ بیت، ۲۴ بیت
- قابلیت Red-Blue Swap برای رفع مشکل رنگ در برخی VNC Serverها
- قابلیت پشتیبانی از Local Cursor و Remote Cursor
- پشتیبانی از انواع VNC Repeaterها
- پشتیبانی از Clipboard فقط با ISO 8859-1

- سرورهای تایید شده با عملکرد بهینه: RealVNC & TigerVNC & x11vnc

۳-۴ تعیین محدودیت در دستورات ارسالی

این فیلتر کردن توسط Regular Expression انجام خواهد شد و در صورت شخیص، به صورت خودکار بر اساس تصمیم مدیر سامانه عمل خواهد شد، که می‌تواند ثبت در گزارش، ارسال اخطار به صورت پست الکترونیکی و یا قطع Session باشد.

- اعمال محدودیت در دستورات وارد شده توسط صفحه کلید
- اعمال محدودیت در دستورات وارد شده توسط Clipboard

۳-۵ مدیریت کاربران

- ایجاد تعداد نامحدود کاربران
- ایجاد محدودیت زمانی برای ورود و یا اعتبار حساب‌های کاربری
- مسدودسازی حساب کاربری به صورت دستی و یا پس از تعداد بالای تلاش برای ورود ناموفق به سامانه
- امکان مجبور کردن کاربر به تعویض رمز عبور
- غیرفعال سازی موقت حساب‌های کاربری توسط مدیر مافوق
- امکان تغییر اطلاعات کلی کاربر، توسط خود کاربر
- پشتیبانی از گروه‌های کاربری
  - این گروه‌ها در بر دارنده کاربران سامانه خواهند بود
  - اعمال همان محدودیت‌ها و سیاست‌هایی که برای کاربران نیز قابل اعمال هستند
  - افزودن و حذف گروه‌های کاربری به صورت دلخواه
- پشتیبانی از گروه‌های Connection
  - این گروه‌ها در بر دارنده Connectionهای سامانه خواهند بود
  - امکان اعمال همان محدودیت‌ها و سیاست‌هایی که برای هر Connection نیز قابل اعمال هستند
  - افزودن و حذف گروه‌های Connection به صورت دلخواه
- تولید گزارش‌های دقیق فعالیت کاربران سامانه در طول زمان
  - دسترسی کاربران به Endpointها

- رویدادهای امنیتی احتمالی
- فایل‌های منتقل شده
- ذخیره گزارش با File Formatهای متداول
- کاربر باید دارای مجوز گزارش‌گیری از سامانه باشد

- رسانه SMS به منظور ارسال هشدارها و پیام‌ها
- رسانه EMAIL به منظور ارسال هشدارها و پیام ها

۳-۶ پشتیبانی از نقش های پیش فرض

سامانه به صورت پیش فرض از ۴ نقش Root | Admin | Auditor | User پشتیبانی می‌نماید. هرکدام از این نقش‌ها دارای همه یا بخشی از مجوزهای موجود در Permission pool را دارا می‌باشند.

- Root بالاترین نقش سامانه می‌باشد که تمامی مجوزهای موجود را دارا می باشد و می تواند به همه اجزا و بخش‌های سامانه دسترسی کامل داشته باشد.
- Admin قادر خواهد بود تا کاربرانی با نقش‌های Auditor و User را ایجاد کند. Adminها فقط به کاربرانی که توسط خودشان ایجاد شده اند دسترسی خواهند داشت.
- Auditor قادر خواهد بود تا با مجوزهایی که به وی داده شده است Sessionهای ضبط شده را بررسی و ممیزی نماید. Auditor اجازه برقراری Connection را نخواهد داشت.
- User کاربران عادی سامانه هستند که در چارچوب محدودیت‌های تعیین شده به Connectionها دسترسی خواهند داشت.
- در سامانه همچنین امکان ایجاد نقش ها با دسترسی های متفاوت نیز وجود دارد.

۳-۷ اعمال محدودیت های دسترسی

محدودیت‌ها و سیاست‌های اعمال شده هم می‌توانند در سطح Connection مشخص شوند و هم در سطح پروفایل دسترسی کاربر به آن Connection. تضادهای احتمالی به نفع Connection درنظر گرفته می‌شوند، در غیر این صورت، تجمیع هردو مبنای تصمیم‌گیری خواهد بود.

۳-۸ امکان تعریف Access Profile

Connectionها در حقیقت فقط در بردارنده ی اطلاعات مربوط به نوع پرتکل و مشخصات Endpoint و محدودیت‌های دسترسی کلی به آن Connection می‌باشد. نگاشت یک Connection به یک کاربر از طریق Access

Profileها میسر می‌گردد. محدودیت‌های مشخص شده در Connectionها فقط در صورتی توسط Access Profileها نقض می‌شوند که مدیر سامانه هنگام ایجادConnection ، آن را مجاز اعلام کرده باشد. تعیین تاریخ انقضا، که پس از آن تاریخ دسترسی به طور خودکار لغو می‌گردد.

۳-۹ امکان فعال یا غیرفعال کردن اجازه دریافت و ارسال فایل

این قابلیت فقط در پروتکل‌هایی که تولنایی انتقال فایل را دارند، یعنی پرتکل‌های SSH و RDP میسر می‌باشد و این اجازه برای ارسال و دریافت فایل به صورت جداگانه مشخص می‌گردد. این محدودیت نیز، مانند سایر سیاست‌های محدودیتی هم در سطح Connection و هم در سطح پروفایل دسترسی کاربر قابل تعریف خواهد بود. همچنین نام Directory نگهداری موقت فایل‌ها قابل تعریف خواهد بود. فایل‌های منتقل داده شده در نشست کاربر توسط مدیر سامانه قابل مشاهده می‌باشد.

۳-۱۰ تعیین بازه های زمانی مجاز برای دسترسی به یک Connection

این قابلیت هم در سطح Connection و هم در سطح Access Profile قابل تعریف خواهد بود. در صورتی که این محدودیت هم در Connection و هم در Access Profile وجود داشته باشد، تجمیع بازه زمانی در نظر گرفته خواهد شد.

۳-۱۱ تعریف Persona های مختلف برای یک Connection

هر Persona نشانگر یک نام کاربری و مجوز دسترسی در Endpoint می باشد. یک Persona می‌تواند مربوط به یک حساب کاربری با دسترسی معمولی باشد و یک Persona دیگر مربوط به یک حساب با دسترسی‌های ممتاز بر روی همان Endpoint باشد.در زمان تعریف پروفایل دسترسی می‌توان مشخص کرد که از کدام Persona استفاده شود.

۳-۱۲ قابلیت OCR تمام محتوای صفحه

با توجه به اینکه در ارتباطات RDP قابلیت جستجو در برنامه‌های استفاده شده از اهمیت بالایی برخوردار می باشد، در تمامی پرتکل‌ها این قابلیت وجود دارد که از نشست برقرار شده تصاویری تهیه شده و مدیر سیستم می‌تواند این تصاویر را مشاهده نموده و علاوه بر این می‌تواند با استفاده از تکنولوژی OCR این عکس‌ها را با دقت بالا به متن تبدیل نموده و در متن تولید شده جستجو نماید.

۳-۱۳ ثبت دقیق تمام وقایع سامانه

- ورودهای موفق و ناموفق به سامانه
- برقراری اتصالات توسط کاربران
- مشاهده و ممیزی Sessionها توسط Auditorها
- دارای سطوح مختلف رخدادنگاری
- پشتیبانی از خروجی‌های Console و File و Syslog
- پشتیبانی از Logstash
- قابلیت محدود سازی و جست و جو بر روی Log ها

۳-۱۴ جداسازی اینترنت از شبکه داخلی

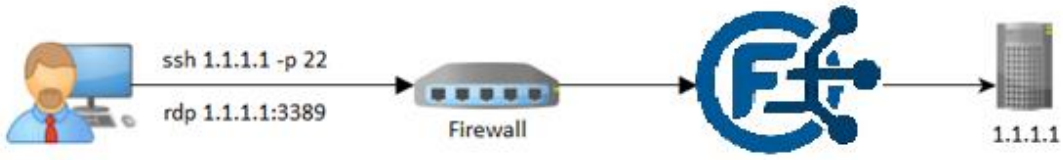
فیدارپم با توجه به سیاست‌های سازمان مبنی بر جداسازی اینترنت کاربران از شبکه داخلی، با استفاده از دو قابلیت RemoteApp و Bastion دسترسی کنترل شده کاربران به اینترنت را فراهم می‌نماید.

در این معماری کاربر بعد از ورود به سامانه فیدارپم می‌تواند به نشست Internet Access دسترسی داشته باشد و مدیر سامانه با اعطای مجوز دانلود و آپلود فایل بر عملکرد کاربر نظارت داشته باشد. در این نشست کاربر تنها به مرورگر دسترسی خواهد داشت. فایل‌های منتقل داده شده در نشست توسط مدیر سامانه قابل مشاهده می‌باشد.

در این بین تمامی فایل های منقل شده بر روی نشست یا از روی نشست علاوه بر آنکه توسط ادمین سامانه کنترل می شود قبل از انتقال بر روی نشست یا از روی نشست توسط سامانه آنتی ویروس تحت وب کاوش اسکن شده و در صورتی که فایل مخرب باشد اجازه انتقال و یا دانلود از روی نشست به کاربر داده نمی شود.

۳-۱۵ حالت شفاف (Transparent)

در حالت شفاف، کاربران با استفاده از آدرس IP سرور به سرور مقصد متصل می‌شوند و کاربران و پیمانکاران متوجه حضور پم نمی شوند. در این حالت کاربر اطلاعات سرور مقصد را مانند قبل وارد نموده و نشست توسط فیدارپم ضبط می‌شود.



۳-۱۶ ویژگی های انحصاری جلسات

- ضبط جلسات انجام شده توسط کاربران
  - محتویات صفحه نمایش کاربر
  - کلیدهای فشرده شده توسط کاربر
  - Metadata مربوط به فایل‌های منتقل شده (ارسال / دریافت)
- بازپخش جلسات ضبط شده توسط Auditorها
  - بازپخش دقیق Session کاربر
  - مشاهده Keystrokeهای وارد شده توسط کاربر در صورت دارا بودن مجوز
- امکان دریافت جلسه ضبط شده کاربر به صورت فایل ویدیو
  - Export با فرمت MP4
  - مشخصات و پارامترهای Encoding توسط سامانه
  - انجام فرایند به صورت On-Demand
  - حذف ویدیوها پس از دریافت و گذشت زمان مشخص
- مشاهده بلادرنگ جلسات در حال اجرا
  - مشاهده بلادرنگ Session در حال اجرا
  - خاتمه آنی Session توسط مدیر
- Tamper proof بودن اطلاعات مربوط به Sessionها
- قابلیت جستجو در واژگان و دستورات تایئ شده
- حضور همزکان کاربر در چنیدین جلسه مختلف
- پشتیبانی از تعداد کاربران نامحدود در نشست‌های مختلف و همزمان (Concurrent Connection)
- رمزنگاری کلیه ارتباطات سامانه با کاربران از طریق HTTPS رمزنگاری و محافظت خواهد شد.
- قابلیت جستجو بر روی تصاویر در پرتکل RDP
- قابلیت اعمال لیست‌های سیاه سفید از دستورات در جلسات SSH
- توقف خودکار جلسات بدون فعالیت

- قابلیت جستجو و کنترل برنامه‌های اجرا شده توسط کاربر در جلسات RDP
- حذف اطلاعات رمز عبور در نشست

۳-۱۷ احرازهویت

پیاده‌سازی احراز هویت توسط LDAP

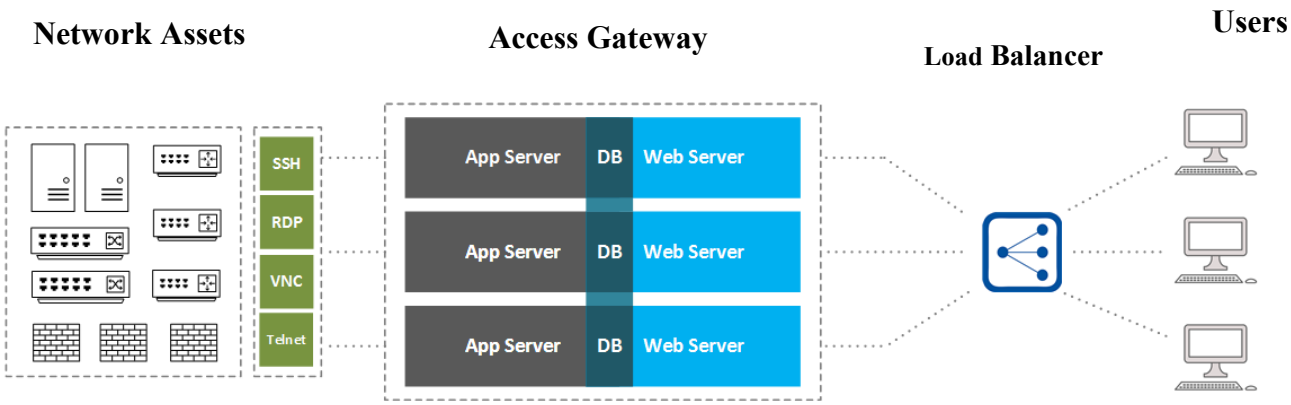
- پشتیبانی از پیاده‌سازی Microsoft Active Directory
- استفاده از LDAP Bind و Attribute search
- پشتیبانی از احرازهویت RADIUS
- پشتیبانی از Authentication Class خاص سامانه
- پشتیبانی از Retry و Timeout

پشتیبانی از احراز هویت +TACACS

پشتیبانی از احراز هویت DIAMETER

۴ معماری کلی سامانه

«سامانه مدیریت و نظارت بر دسترسی راه‌دور» با قرار گرفتن درمقابل منابع شبکه، مانع از هرگونه دسترسی مستقیم به منابع شبکه می‌گردد و مدیران شبکه می‌توانند به راحتی تمامی دسترسی‌های مستقیم را مسدود نمایند. با عنایت به این موضوع که این سامانه تنها نیازمند پورت HTTPS 443 می‌باشد، مدیریت دسترسی آن در لایه شبکه به راحتی انجام پذیر خواهد بود.



این سامانه می‌تواند هم به صورت تجهیز سخت‌افزاری و هم به صورت نرم‌افزاری در ساختار شبکه داخلی پیاده‌سازی گردد.

مولفه های معماری سامانه:

واسط دسترسی: این بخش عهده دار برقراری اتصال راه دور به نقاط انتهایی شبکه می‌باشد. تمامی پروتکل‌های تحت پشتیبانی سامانه در این بخش پیاده سازی شده‌اند و فرایند تبدیل داده‌ها از پروتکل مبدا به پروتکل انحصاری سامانه در این بخش انجام می‌پذیرد.

درگاه بصری مبتنی بر وب: این بخش یک واسط مبتنی بر HTML5 می‌باشد که وظیفه تبدیل پروتکل انحصاری سامانه به تصاویر قابل نمایش را به انجام می‌رساند. تمامی تعاملات سامانه ار طرف مدیریان و کاربران از طریق همین درگاه صورت می‌پذیرد. شایان ذکر است این درگاه در از طریق کانال‌های TCP با واسط دسترسی در ارتباط می‌باشد.

بانک اطلاعاتی: اطلاعات مربوط به کاربران، اتصالات، نشست‌های کاری و ... در این بخش از سامانه نگهداری می شوند. تنهای مولفه‌ای که با این بخش در ارتباط مستقیم است، درگاه بصری وب می‌باشد. شایان ذکر است، اطلاعاتی که از نظر امنیتی دارای اهمیت ویژه‌ای هستند، به صورت رمز شده در بانک اطلاعاتی ذخیره می‌گردند.

سرویس نگهداری فایل: این بخش از سامانه وظیفه نگهداری نشست‌های ضبط شده را دارا می‌باشد. دسترسی به این بخش از سامانه توسط واسط دسترسی و درگاه بصری انجام می‌پذیرد.

سرویس تایید یکپارچگی و تبدیل نشست‌ها به ویدیو: تبدیل نشست‌ها به فایل‌های ویدیو استاندارد و همچنین احراز عدم ایجاد دستکاری و تغییر در فایل‌های ضبط شده توسط این بخش انجام می‌گردد.

۵ عملکرد سامانه در مقیاس گسترده

با عنایت به معماری لایه‌ای و غیر متمرکز سامانه، امکان افزودن تجهیز به منظور افزایش بهره‌وری و پاسخ‌گویی به تعداد کاربران بالا فراهم می‌گردد. شایان ذکر است، از آنجاییکه نحوه تعاملات کاربران با منابع شبکه توسط پروتکل‌های قابل پشتیبانی متغیر می‌باشد، نمی‌توان تعداد دقیقی از کاربران همزمان به ازای هر یک تجهیز از سامانه ارائه نمود، لیکن شرایط هر محیط عملیاتی می‌تواند تابع عوامل گوناگونی مانند انواع پرتکل‌های مورد استفاده و یا رفتار کاربران باشد.

همچنین معماری HA سامانه به صورت شکل ذیل می‌باشد:

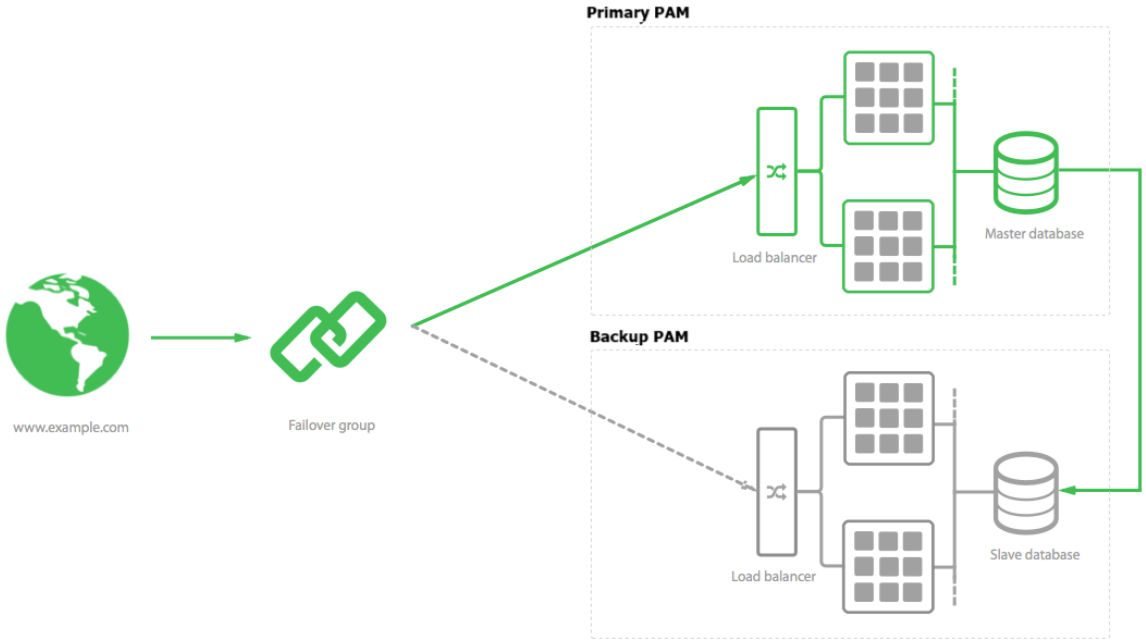


Figure ۱ معماری HA

سرویس Fidarnet Intelligent System بر پایه FID-PAM با پشتیبانی از اتصال مستقیم به Grafana برای مانیتورینگ و Auditing ، در مقایسه با CyberArk ، BeyondTrust و Wallix Bastion ، انعطاف‌پذیری بالاتری در سفارشی‌سازی داشبوردهای نظارتی دارد.

جدول مقایسه سرویس‌های PAM با تمرکز بر مانیتورینگ و اتصال به Grafana شرکت فیدارنت

ویژگی‌ها / سرویس‌ها	FID-PAM (Fidarnet Intelligent System)	Wallix Bastion	BeyondTrust	CyberArk
نوع محصول	تجاری، قابل سفارشی‌سازی	تجاری، اروپایی	تجاری، Enterprise	تجاری، Enterprise
پروتکل‌های پشتیبانی‌شده	SSH, RDP, SFTP, Telnet, Kubernetes, MySQL, Redis, RemoteApp	SSH, RDP, VNC, SQL, HTTPS	SSH, RDP, VNC, SQL, HTTPS, Telnet	SSH, RDP, HTTPS, SQL, Oracle, SAP
ضبط نشست‌ها (Session Recording)	دارد برای همه پروتکل‌ها	دارد با کنترل دقیق	دارد با فیلترهای امنیتی	دارد با تحلیل رفتاری
Keystroke Logging	دارد	دارد	دارد	دارد
Command Log و Process Monitor	دارد	دارد	دارد	دارد
Replay Activity Player	Web-Based	Web-Based	Web-Based	Web-Based
قابلیت OCR و Full-Text Search	OCR داخلی با جستجوی کامل	OCR داخلی با تشخیص پنجره‌ها	OCR وابسته به سرویس ثالث	OCR داخلی
نظارت نشست	دارد	دارد	دارد	دارد
پشتیبانی از Agent-less Access	دارد (SSH و RDP)	دارد	دارد	دارد

دارد، خودکار	دارد، Cloud-Scale	دارد با تنظیمات دقیق	دارد (تنظیم دستی)	پشتیبانی از Just-in-Time Access (JIT)
کامل و خودکار	کامل و خودکار	کامل و قابل تنظیم	دارد، با تنظیم دستی	ادغام با LDAP/AD/SIEM
AWS، Azure، GCP Container	AWS، Azure، GCP	AWS، Azure Docker	Docker، Kubernetes	پشتیبانی از Containerو Cloud
کامل، SDK	کامل، ادغام با DevOps	محدود، بیشتر برای مانیتورینگ	RESTful API، Webhook، Plugin	پشتیبانی از APIو توسعه‌پذیری
اتصال به Amazon Managed Grafana	ادغام با Entitleو داشبوردهای Grafana	مانیتورینگ داخلی، بدون اتصال مستقیم	اتصال مستقیم با داشبورد آماده (GitHub Repo)	مانیتورینگ و اتصال به Grafana
Vault پیشرفته با چرخه عمر رمزها	Password Safeبا سیاست‌های قوی	Vaultاختصاصی با کنترل دسترسی	Vault داخلی با رمزنگاری AES	مدیریت رمز عبور ممتاز(Vault)
MFA، SAML، RADIUS، Biometric SSO	MFA، Duo، RADIUS ،LDAP SSO	Wallix باMFA Authenticator، SSO دارد	MFA، TOTP ،LDAP SMS، SSO	پشتیبانی از MFAو SSO
کامل	کامل	Blacklist/White list، ACL، Time Policy	کامل	سیاست‌های کنترلی و محدودیت‌ها
کامل، انطباق باSIEM	کامل، زمان‌بندی شده، ارسال ایمیل	ارسال به Syslog ، SNMP، گزارش‌های دستی	کامل، ارسال به Syslog ، SNMP، CSV، BI	گزارش‌گیری و هشداردهی امنیتی

دارد	دارد	دارد	دارد	پشتیبانی از High Availabilityو Backup
دارد	دارد	دارد	دارد	مدیریت آبشاری و چند دامنه‌ای
دائمی یا سالانه، محدودیت نشست	سالانه، بدون محدودیت کاربر	دائمی، محدودیت در نشست و کاربر	سالانه، بدون محدودیت کاربر	لایسنس‌گذاری

۶ پشتیبانی و لایسنسینگ

پشتیبانی سامانه در سال اول به صورت رایگان می‌باشد و در سال دوم به بعد ۲۵ درصد قیمت پایه به همراه درصد تورم بر مبلغ این ۳۰ درصد اضافه خواهد شد. با توجه به نیاز مشتریان قابلیت‌های جدید در سامانه فیدار پم توسعه داده خواهد شد که به صورت فصلی وصله جدید از سامانه ارایه داده می‌شود. همچنین خدمات پس فروش به مدت ۱۰ سال می‌باشد.