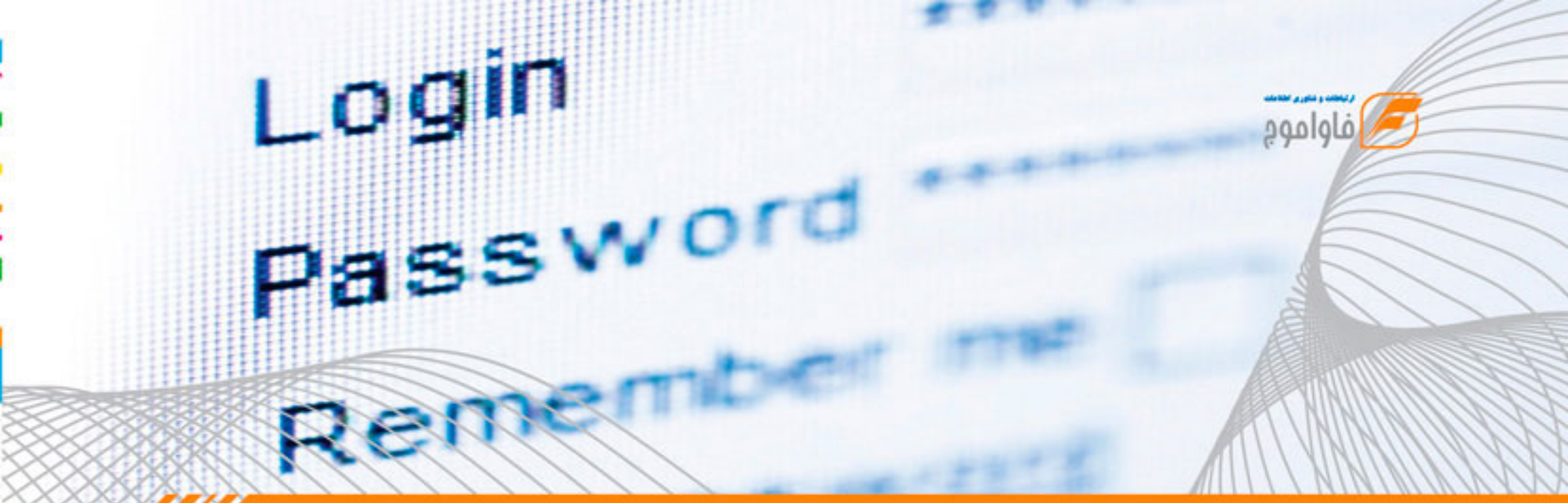
فاواموج
ارتباطات و فناوری اطلاعات

SCB
Shell Control Box Solution

BalaBit
IT Security

راه حل جامع
ممیزی مدیران شبکه



ممیزی مدیران شبکه

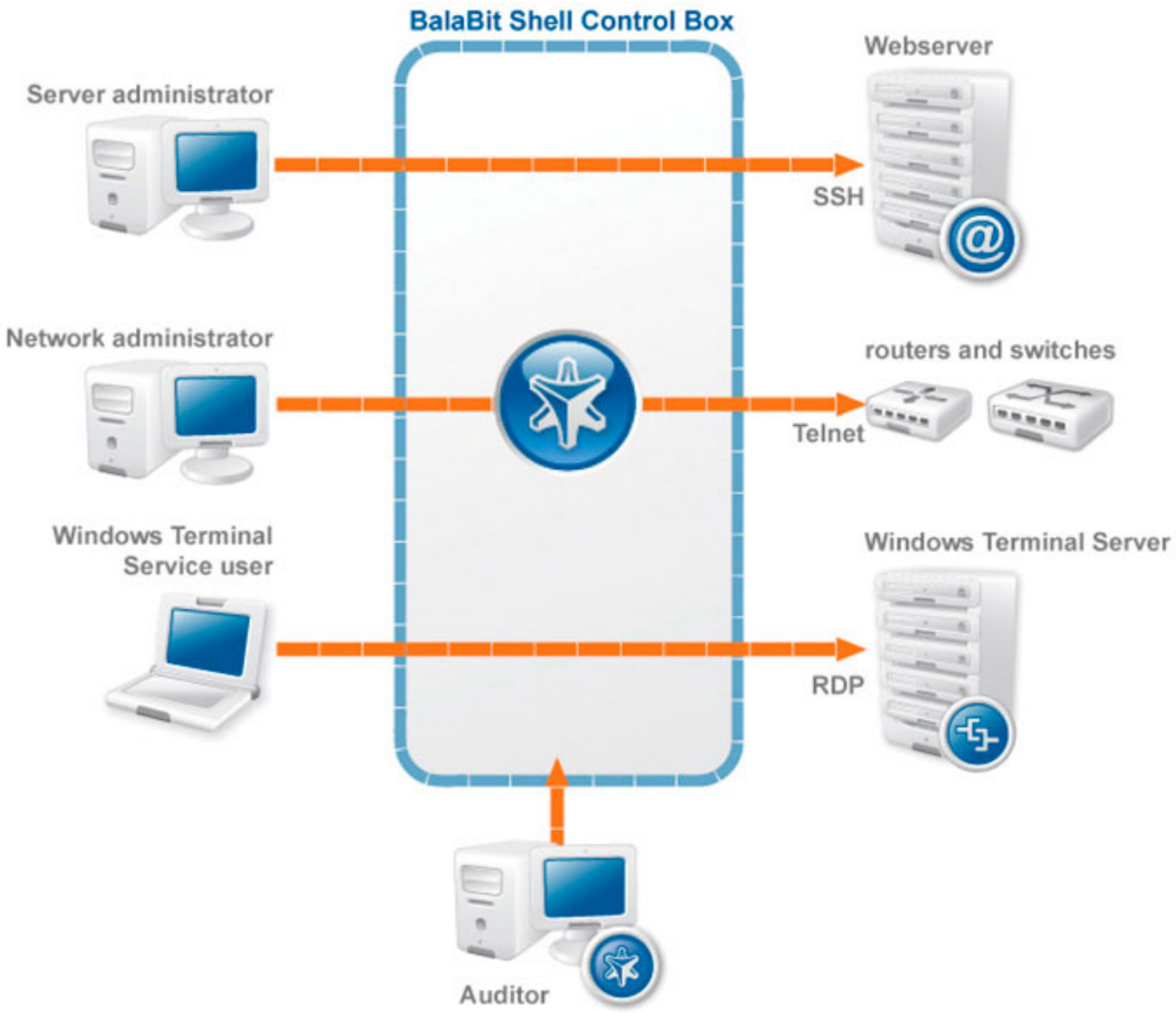
ممیزی کاربران خاص و خصوصا مدیران و راهبران شـبکه، موضوع مهم و پیچیده ای در فناوری اطلاعات اسـت. استاندارد ها و "به روش های" بسـیاری به این نیاز اشـاره می کنند اما ، کمتر محصولی را می توان یافت که این قابلیت را در خود داشته باشد. شـرکت Balabit محصولـی را تحت عنوان Shell control Box (SCB) به بـازار معرفی کرده که اختصاصاً به همین منظور طراحی و ساخته شده است.

معرفی محصول

SCB محصـول شرکت Balabit مجارستـان می باشـد. این شـرکت فعالیت خود را از سال ۱۹۹۶ در زمینه امنیـت شبکه آغاز کرده است.

برتـری این محصـول در مقایسـه با سـایر محصولات موجـود در بـازار ایـن اسـت که اولاً SCB محصـولی پـایه ای است، که تولیـد کننـدگان بسـیاری در تولیدات خود از آن اسـتفاده می کننـد و صرفاً رابط کاربـر (User Interface) سیسـتم را تغییـر می دهنـد، در ثـانی جزء معدود محصولاتی است که ممیـزی را به روش Out-of-band انجام می دهـد. این برتـری موجب می شـود تا امکان ممیزی تجهیزاتی نظیر سـوئیچ، روتر و کلیه تجهیزاتی که امکان نصب Agent روی آنها نیسـت هم فراهم شـود. این ممیزی به صورت کاملاً ترانسـپارنت و مخفی از دید کاربر خواهد بود. به این ترتیب کاربر دخالت دائمی را در کار خود احسـاس نمی کند و با آسـایش کامل به کار خود ادامه می دهد. در همین راسـتا شـرکت فاواموج نیز پس از نصب و بهـره بـرداری موفقیت آمیز این محصول در تعدادی از سـازمان ها و شـرکت های معتبر، موفق به دریافت نمایندگی شـرکت Balabit در ایران شد و در حال حاضر تنها نماینده این شرکت در ایران می باشد.

SCB
Shell Control Box Solution



مقدمه

سرورها 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 ترانسپارنت و مستقل عمل کنیم، زیرا در غیر این صورت یک ادمین ماهر 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 یک لایه مجازی ممیزی (Auditor layer) تعریف می کند. در این لایه درواقع دیده بانی فعالیت های ادمین های سیستم انجام می شود.

SCB تجهیزی جهت پایش فعالیتهاست که 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 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 ضبط می کند.

SCB
Shell Control Box Solution

محتوای تریل ممیزی ضبط شـــده، نشـــانه گذاری (اندیکس) شده تا امکان جســـتجوی وقایع و گزارشگری خودکار فراهم شود. این محصول بخصوص برای نظارت بر دسترسی کاربران ممتاز ساخته شده است. اینگونه نظارت مطابق بسیاری از استانداردها نظیر PCI-DSS تأکید شـــده یا در برخی موارد ضروری دانســـته شده است. SCB دستگاهی مستقل و کاملاً ترانسپارنت است که به هیچ عنوان وابستگی به کلاینت ها و سرورها ندارد. برای بکارگیری SCB در زیرساخت نیازی به ایجاد تغییر در برنامه های کاربردی سرورها و کلاینت ها نداریم. این سیستم به مرور با زیرساخت موجود، یکپارچه و همگام می شود. SCB کلیه ترافیک های ادمین (نظیر تغییرات پیکربندی، فرمانهای اجرا شـــده و غیره) را در تریل های ممیزی ثبت می کند. تمام داده ها در فایل ها رمز نگاری و امضا شـــده و با برچســـب زمانی که تغییر و دستکاری آنها غیرممکن اســـت ذخیره می شوند. در زمان بروز اشکال (پیکربنـــدی نادرســـت ســـرور، دســـتکاری بانـــک اطلاعاتـــی، قطعـــی یـــا خاموشـــی ناخواســـته) شـــرایط بـــروز خطـــا بـــه آســـانی در تریل های ممیزی قابل بازیابی اســـت، بنابرایـــن علت بروز خطا به راحتی قابل شناســـایی خواهد بود. تریل های ضبط شده ممیزی شبیه فیلم نمایش داده می شود و امکان تکرار تمام عملیات ادمین وجود خواهد داشت.

همه تریل های ممیزی روی سرور جداگانه نشانه گذاری (ایندکس) می شوند. این نشانه گذاری امکان حرکت سریع روی رویداد ضبط شـــده و جســـتجوی اتفاقات خاص (برای مثال، کلیک ماوس، فشردن صفحه کلید) و متن هایی که توسط ادمین مشاهده شـــده را فراهم می کند. امکان تهیه گزارشـــات و جستجوهای خودکار نیز وجود دارد. به منظور حفظ اطلاعات حساس موجود در این گونه ارتباطات امکان تفکیک و رمزنگاری جداگانه ترافیک در هر کدام از جهت ها (کلاینت به سرور و سرور به کلاینت) بـــا اســـتفاده از کلیدهای متفاوت وجود دارد. با این امکان اطلاعات حســـاس نظیر کلمات عبـــور فقط در صورت لزوم می توانند نشان داده شوند.

SCB امکان باز کردن رمز ترافیک و ارســـال ترافیک رمز نشـــده به یک سیستم تشخیص نفوذ (IDS) را دارد. این قابلیت امکان آنالیز و تحلیل ترافیک رمز نگاری شده را نیز فراهم می کند. با این شیوه، آنالیز ترافیکی که تا به حال برای IDS قابل دسترسی نبود به صورت بلادرنگ (Real-Time) ممکن خواهد شـــد.همچنین پروتکل های دیگری که از طریق SSH تونـــل می شـــوند می توانند بازرسی شوند. مثلاً لیست کلیه فایلهایی که در فضای رمز نگاری شده ارسال می شوند یا از طریقی دسترسی به آنها صورت می گیرد جهت بررسی می تواند به سیستم جلوگیری از نشت اطلاعات (DLP) گزارش شود.

زمینه های کاربرد و کاربران نوعی سیستم

انطباق با سیاستهای امنیتی

الزام برای انطباق های امنیتی، روز به روز در زمینه های مختلف اهمیت بیشتری پیدا می کند. قوانین، مقررات و استانداردهای صنعتی، سطوح هوشیاری و مراقبت های امنیتی و حفاظت و حراست از اطلاعات مشتریان را افزایش می دهند. در این شرایط شرکتها باید کنترل پذیری و قابلیت بازرسی و ممیزی فرآیندها بویژه مدیریت سرورها و دسترسی های راه دور را افزایش دهند. مقرراتی نظیر SOX[1]، PCI-DSS[2]، HIPAA[3] و باسل II در خصوص حفاظت اطلاعات شخصی، اطلاعات کارت اعتباری یا سایر اطلاعات، دستورالعمل هایی را ارائه می دهند. این اطلاعات معمولاً در یک بانک اطلاعاتی در یک سرور مرکزی ذخیره شده اند و از طریق برنامه های کاربردی اختصاصی نظیر برنامه های حسابداری یا مالی در دسترس قرار خواهند گرفت. این برنامه ها معمولاً وقایع و گزارشات را در انطباق با سیاست های امنیتی ثبت می کنند. اما این برنامه ها صرفاً مراقب دسترسی های مجاز به بانک های اطلاعاتی هستند. سرورهایی که بانک اطلاعاتی را ذخیره می کنند به منظور نگهداری در دسترس ادمین ها هستند. ادمین ها با داشتن دسترسی سطح بالا به سرور، امکان دستکاری بانک اطلاعاتی را نیز دارند و همچنین می توانند اینگونه عملیات را از ثبّات ها حذف کنند.

SCB می تواند فعالیت های ادمین ها را ممیزی کند و با توجه به اینکه SCB مستقل از هر دو (ادمین و سرورهای تحت مدیریت) است راه حل یگانه ای را برای تکمیل لاگ ها و گزارشات برنامه های دیگر دارد.

سازمانهایی که از پیمانکارهای فاوا استفاده می کنند

بسیاری از سازمان ها برای نگهداری و راه اندازی سرورها و سرویس های فاوا از شرکت های دیگر به عنوان پیمانکار استفاده می کنند. این بدان معناست که سازمان مجبور است به کارکنان چندین شرکت بیرونی اعتماد کند و تمام اطلاعات خود را در دسترس آنها قرار دهد. اطلاعاتی نظیر ایمیل های خصوصی و تجاری، اطلاعات مشتریان و موارد بسیار دیگر. علاوه بر اطلاعات،

1. SOX : Sarbanes – Oxley Act
2. PCI-DSS : Payment Card Industry – Data Security Standard
3. HIPAA : Health Insurance Partibility And Accountability

بسیاری از سرویس های حساس تجاری نظیر فروش مجازی نیز در دسترس ادمین های ناشناس قرار خواهد داشت. واضح است که در این شـرایط وجود یک دسـتگاه مسـتقل برای ثبت عملیات ادمین ها ضرورتی انکار ناپذیر اسـت. SCB این وظیفه را بر عهده خواهد گرفت. این سیسـتم جزئیات مشـکلات سـرورها را ثبت و پیدا کردن افراد مسئول را تسهیل می کند. به کمک شیوه اعتبار سنجی چهار چشمی، SCB کنترل بلادرنگ را برای دسترسی به سرورها و عملکرد ادمین ها فراهم می کند.

☑ سازمانهایی که امکان مدیریت از راه دور به مشتریان می دهند

در سـوی دیگر برونسـپاری، شرکتهایی که خدمات میزبانی وب و سرور را ارائه می کنند نیز می توانند به همان میزان از SCB بهره ببرند. SCB این امکان را به آنها می دهد که ادمین ها را ممیزی و نظارت کنند و موثر بودن کارکرد آنها را ارزیابی کنند. تریل های ضبط شده در خصوص معضلات سرورهایی که از راه دور مدیریت می شوند به عنوان مدرک قابل استفاده خواهند بود. SCB در بهبود کنترل "توافقنامه سـطح خدمات" (SLA) موثر خواهد بود. با این سیسـتم، کیفیت خدمات می تواند با مرور تریل های ممیزی و گزارشات دسترسی ارزیابی شود.

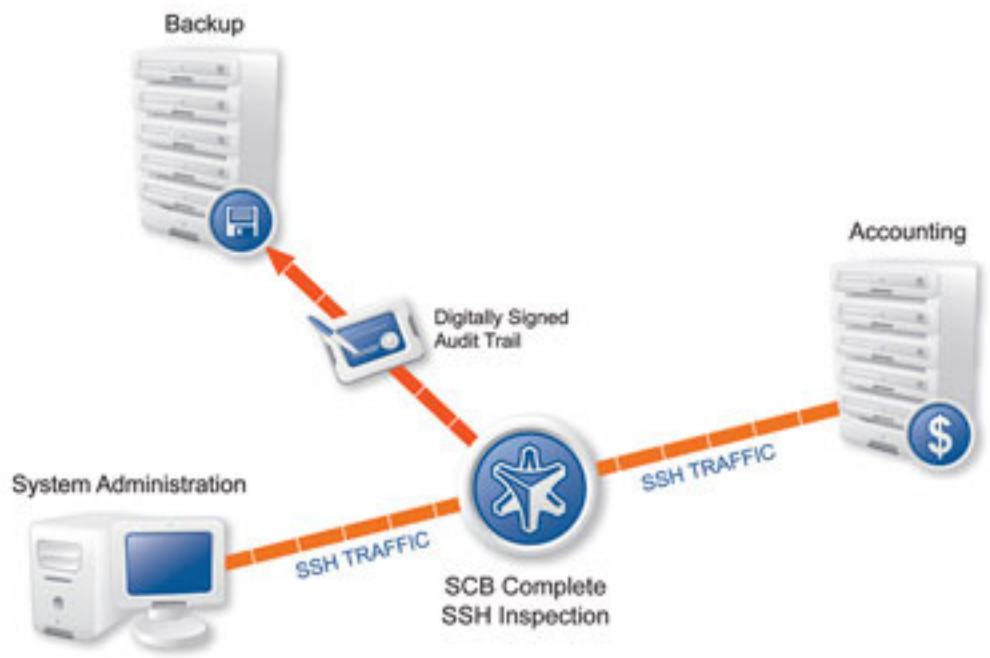
☑ سازمانهای دارای زیر ساخت Thin Client

SCB می تواند پروتکل هایی که در راه حل های عمومی Thin client اسـتفاده می شـوند (نظیر RDP، VMware View) را ممیزی کند. ممیزی با اسـتفاده از شـیوه ای مستقل از برنامه کاربردی، برای ضبط و پایش فعالیت هرکدام از کلاینت ها انجام می شود.

☑ مانیتورینگ بلادرنگ انتقال فایل ها و دسترسی به آنها

SCB مـی توانـد محتوای کانالهای خاصی را به یک DLP (Data leakage prevention) ارسـال دارد. این راه حل ترکیبی به منظور شناسایی، رهگیری و هشدار در خصوص دسترسی (Data at rest) و انتقال (Data in motion) دیتای حساس به کار می رود. با این شیوه سیاست DLP در سازمان می تواند به پروتکلهای رمز گذاری شده نظیر SSH و SFTP تعمیم یابد.

☑ سازمان هایی که نیاز به کنترل SSH دارند



در بسیاری از سازمان ها ارتباطات خروجی SSH ضروری است. ارتباطات SSH بدون کنترل، مخاطراتی در بردارد زیرا به صورت مجازی دیگر پروتکل ها می تواند از طریق تونل SSH برقرار شود. SCB می تواند نوع ترافیکی که از طریق ارتباط SSH برقرار می شوند را کنترل کند و انواع مختلف ترافیک نظیر ارتباطات ترمینالی، انتقال فایل به شیوه Agent forwarding ، SFTP، Port- and x11 Forwarding را به صورت جداگانه فعال نماید. همچنین به کمک SCB امکان استخراج فایل های منتقل شده توسط پروتکل های SFTP و SCP برای تحلیل آتی وجود دارد.

☑ سازمان هایی که از Jump Host ها استفاده می کنند

بسیاری از سازمان ها یا سرویس های راه دور از Jump Host ها استفاده می کنند. SCB می تواند به منظور اعتبار سنجی و ممیزی کلیه دسترسی های به Jump Host ها استفاده شود. از آنجایی که SCB از شیوه های اعتبار سنجی بسیار قوی (نظیر اعتبار سنجی بر پایه X.509) و اعتبار سنجی بوسیله دایرکتوری ها (به عنوان مثال Active Directory و یا دیتابیس های دیگر LDAP) بهره می گیرد، قادر است مدیریت کلمه عبور و کلید هاست ها را به میزان زیادی ساده کند.

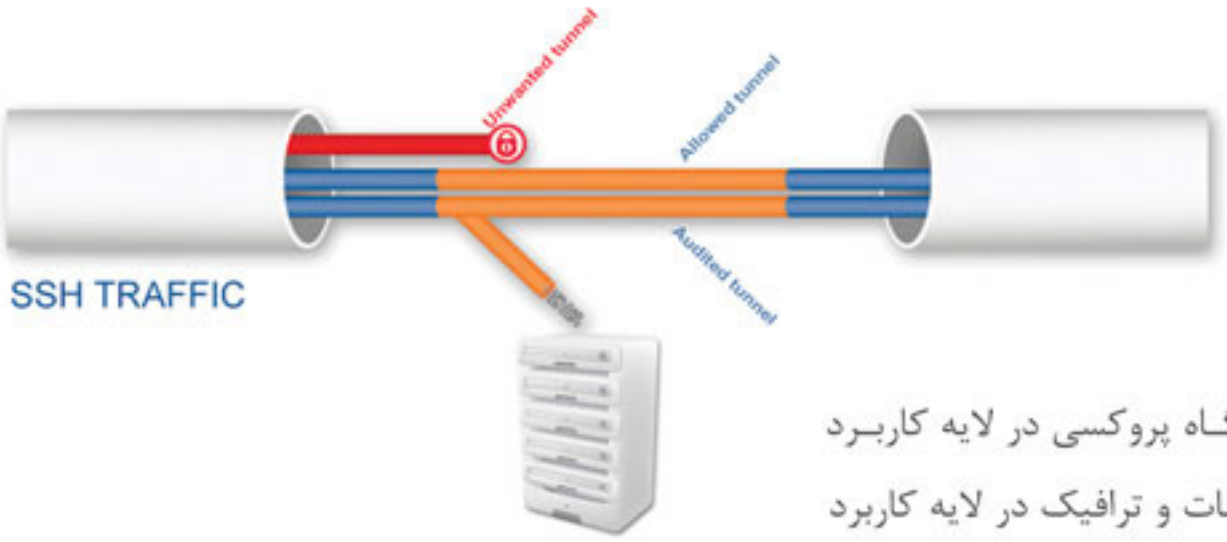
این امکان خصوصاً زمانی مفید است که یک سازمان مجبور باشد به تعداد زیادی هاست راه دور دسترسی یابد یا تعداد زیادی Jump Host داشته باشد.

ویژگی ها و مزایای محصول

- نظارت بر ادمین ها و ضبط عملیات مدیریت آنها بر روی سرویس دهنده ها.
- کنترل SSH (شامل X11 Forwarding) ، Telnet ، VNC ، VM Ware View ، RDP7 ، RDP6 ، RDP5 و ارتباطات TN 3270
- نظارت بر ارتباطات SCP ، SFTP و لیست کردن عملیات بروی فایلها و استخراج فایل های ارسال شده
- جمع آوری اطلاعات و مدارک قابل استناد در مراجع قضایی
- کنترل دقیق دسترسی به سرورها و تریل های ممیزی
- عملکردمستقل از سرورها و کاربران (Out-of-band)
- انطباق آسان با زیرساخت شبکه در مد های مختلف Bastion ، Bridge ، Router
- امکان محدود کردن دسترسی به سیستم های راه دور و دیتاها فقط با تائید مجوز دهندگان(4-eyes authorization)
- پشتیبانی از قابلیت دسترسی بالا (High Availability)
- مدیریت آسان از طریق مرورگر وب
- پشتیبان گیری و آرشیو به صورت خودکار

ویژگی ها و مزایای مرتبط با کسب و کار

- انطباق با مقررات و سیاست های امنیتی و ابزاری قوی برای ایجاد انطباق در سازمان
- ایجاد اطمینان در دسترسی های راه دور و انتقال دیتا
- کنترل آسان تر و بهتر SLA
- کنترل پیشگیرانه، فنی و روانی برای جلوگیری از دسترسی های ناخواسته و مخرب
- گزارش جزئیات دسترسی ها
- صرفه جویی در عیب یابی و رفع عیب و مسائل حقوقی و قضائی فاوا



بازرسی پروتکل

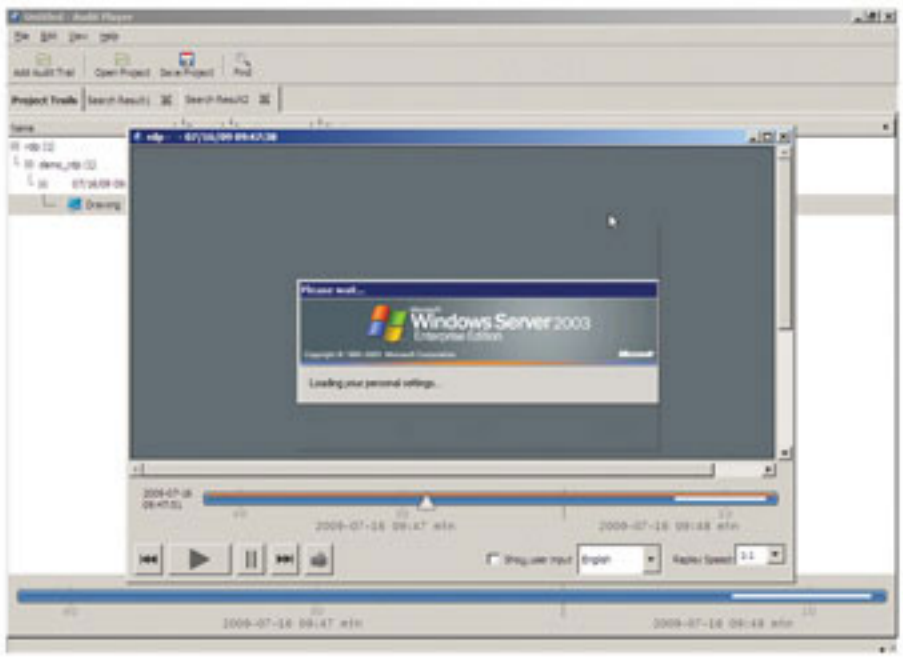
SCB به عنـوان درگـاه پروکسی در لایه کاربـرد عمل می کند. ارتباطات و ترافیک در لایه کاربرد (لایه ۷ مدل OSI) بازرسی می شوند و از برقراری ترافیک ناقض مقررات و پروتکل ها جلوگیری می شود. این سیستم به عنوان محافظ قوی در برابر حملات عمل می کند. این اشراف و نظارت سطح بالا بر ترافیک، قابلیت کنترل ویژگی های مختلف پروتکل ها را ایجاد می کند. ویژگی هایی نظیر شیوه های اعتبار سنجی و رمز نگاری که در ارتباطات SSH استفاده می شوند یا کانال های مجاز در ترافیک RDP از این دست هستند.

پروتکل های تحت پوشش SCB

- پروتکل SSH(v.2) که برای سرورهای بر پایه یونیکس و تجهیـزات شبکه به کار می‌رود.
- پروتکل RDP(v.7) که برای دسترسی به سیستم عامل های ویندوز از قبیل ویندوز سرور2008 و ویندوز7 استفاده می شـود.
- پروتکل (X11) که زیر مجموعه پروتکل SSH می باشـد و جهت دسترسـی راه دور به صورت گرافیکی به سیستم های شبه یونیکس به کار می رود.
- پروتـکل Telnet برای دسترسـی به تجهیزات شـبکه از قبیل روتر، سـوئیچ به کار می رود و پروتـکل TN3270 که برای دستگاه های یونیکس و Main Frames قدیمی استفاده می شود.
- سیستم به اشتراک گذاری دسکتاپ VNC که عموماً در دسترسی راه دور گرافیکی در محیط های چند پلتفرمی استفاده می گردد.
- پروتکل VMWare-view که برای دسترسـی به Virtual Desktop اسـتفاده می شود. (در حال حاضر ارتباط مستقیم تنها با استفاده از پروتکل RDP انجام پذیر است)
- پروتکل ICA برای ارتباطات Thin Client های مبتنی بر Citrix .
- RDP Gateway موجود بر روی کلاینت سرویس ترمینال مایکروسافت.

SCB
Shell Control Box Solution

بازرسی ترافیک ها و ممیزی با SCB



SCB تمام دسترسی ها و ارتباطات را در تریل های ممیزی قابل جستجو ذخیره می کند. این اقدام یافتن اطلاعات مرتبط در پیگیری های حقوقی و موارد دیگر را تسهیل می کند. تریل های ممیزی می تواند به صورت آنلاین مرور شود یا اینکه فعالیت ادمین ها، بی درنگ نظارت و کنترل شود. کلیه تریل هایی که در SCB و سرور آرشیو، ذخیره می شود، توسط اینترفیس وبی SCB در دسترس قرار دارد. برنامه Audit Player قطعات ضبط شده فعالیت را شبیه فیلم پخش می کند. تمام فعالیت های ادمین ها دقیقاً همانگونه که در مانیتورشان ظاهر می شود، دیده می شوند. تریل های ممیزی توسط سرور جداگانه ای نشانه گذاری می شوند تا بعد ها در GUI وبی SCB قابل جستجو باشند. عقب و جلوی سریع روی فیلم و جستجوی وقایع (کلیک ماوس و یا زدن کلید خاص)و مرور متونی که توسط ادمین دیده شده از ویژگی های Audit Player است. در ضمن جستجوی تعداد زیادی از تریل ها برای یافتن واقعه یا اطلاعات خاص نیز ممکن است. SCB می تواند به طور خودکار در تریل های جدید به جستجو ادامه داده و گزارشات لازم را تولید کند. علاوه بر ضبط تریل های ممیزی پروتکل های بازرسی شده، امکان ضبط پروتکل های درونی (نظیر پروتکل های تونل شده در SSH و Port Forwarding) و فایل هایی که ارسال یا دریافت می شوند نیز وجود دارد.

فایل های ضبط شده از ارتباطات SCP و SFTP برای تحلیل بیشتر می توانند استخراج شوند. ضمناً امکان تبدیل ترافیک ممیزی شده به فرمت PCap برای آنالیز توسط ابزارهای خارجی نیز وجود دارد. به منظور جلوگیری از دستکاری و با هدف تأمین اطلاعات قابل اطمینان برای ممیز، کلیه تریل های ممیزی برچسب گذاری زمانی و رمزنگاری شده و سپس امضاء می شود. تریل ها فشرده سازی می شوند و مهمتر اینکه ارتباطات معطل، فضا اشغال نمی کنند.

حصول ممیزی قابل اطمینان

ممیزی معمولاً مبتنی بر ثبت وقایع توسط خود سروری است که ممیزی می شود. این مدل اساساً ناقص است چرا که با این روش ثبت وقایع تعاملی (تعامل سرور با عناصر دیگر) معمولاً خیلی دقیق و با جزئیات کافی نیست و راهی برای حصول اطمینان از اینکه گزارشات وقایعی که توسط سرور ذخیره شده یا فرستاده شده توسط ادمین یا هکر، دستکاری نشده باشد، وجود ندارد. اما SCB دستگاه مستقلی است که ترانسپارنت عمل می کند و اطلاعات ممیزی را از ارتباط کلاینت و سرور استخراج می کند.

این طرز عملکرد سبب جلوگیری از اصلاح اطلاعات ممیزی شده، توسط هر شخص دیگری می شود. حتی ادمین SCB نیز نمی تواند تریل های ممیزی را دستکاری کند. SCB همچنین Change Log هایی از تمام اصلاحات روی پیکربندی خودش با جزئیات کامل تولید می کند.

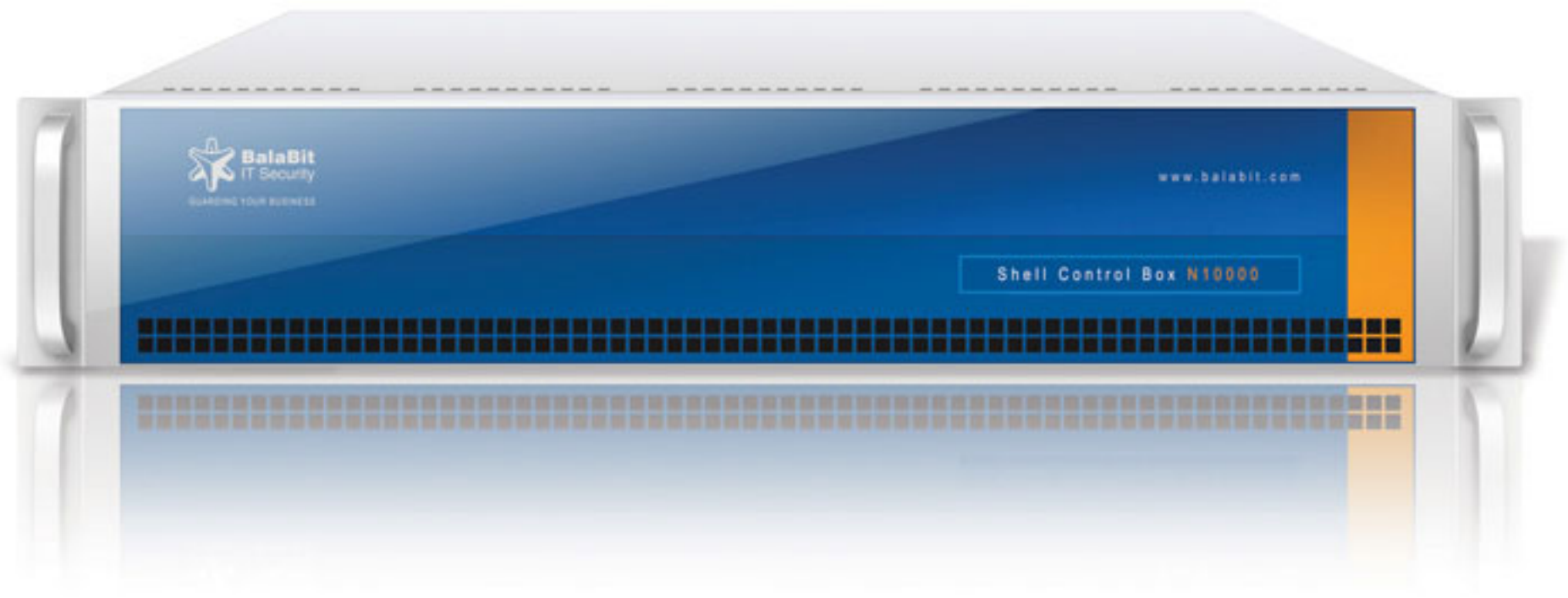
کنترل دقیق دسترسی (چه کسی، چه زمانی، چگونه و از کجا می تواند به چه سروری دسترسی پیدا کند)

SCB به شـما اجازه تعریف ارتباطات را می دهد، به عنوان مثال دسترسـی به یک سرور فقط از آدرس IP کلاینت های لیست شـده امکان پذیر اسـت. این محدودیت می تواند با اسـتفاده از پارامترهای دیگر ارتباط تشـدید شـود. مثلاً می توان به اعمال محدودیت زمانی برای دسترسی به سرور، نام های کاربری خاص و شیوه اعتبار سنجی استفاده شده در SSH یا کانال های مجاز در ارتباطات SSH و RDP اشاره نمود. کنترل اعتبار سنجی به این معناست که SCB می تواند استفاده از شیوه اعتبار سنجی قدرتمند (کلید عمومی) را اجباری نماید و همچنین کلید عمومی کاربران را تأیید کند. همچنین SCB می تواند اعتبار کاربران را در یک دایرکتوری خارجی بسنجد این اعتبار سنجی کاملاً مستقل از اعتبار سنجی کاربر در سرور راه دور است.

پارامترهای زیر می توانندتوسط SCB کنترل شوند:

- آدرس آی پی کلاینت هایی که اجازه دسترسی به سرور دارند.
- گروهی از ادمین ها که مجاز به دسترسی سرور هستند (براساس نام های کاربری- لیست سیاه و سفید - یا گروه های LDAP) و از احراز هویت SSH یا RDP6 در لایه شبکه استفاده می کنند.
- علاوه بر احراز هویت که روی سرور اجرا می شود. ممکن است به احراز هویت Out band ثانویه روی اینترفیس وب SCB نیاز باشد مجوز کاربری نیز می تواند برپایه همین احراز هویت باشد.
- شیوه احراز هویت (نظیر کلمه عبور، کلید عمومی، گواهی) که برای دسترسی به سرور با استفاده از SSH لازم است.
- زمان محدود دسترسی به سرور (برای مثال: طی ساعات کاری)
- نوع کانال SSH یا RDP برای دسترسی به سرور (مثلاً: ترمینال SSH یا Port forward، اشتراک فایل RDP و نظایر آنها).

قواعد بالا می تواند در هر دو سطح ارتباط و کانال اعمال شود، با این شیوه، دسترسی به یک کانال خاص می تواند به گروه کوچکتری از ادمین ها محدود شود و فقط آنهایی که ضروری هستند می توانند دسترسی داشته باشند.



صدور مجوز بر اساس اصل چهار چشمی

به منظور جلوگیری از پیکربندی اشتباه و دیگر خطاهای انسانی، SCB از اصل نظارت چهارچشـــمی یا دو نفره پشتیبانی می کند. در این روش یک نفر مجوز دهنده وجود دارد که به ادمین اجازه دسترســـی به سرور را خواهــد داد. مجوز دهنده امکان پایش فعالیت های ادمین به صورت بـــی درنگ را خواهد داشـــت به گونه ای کـــه دو نفر یک صفحه واحد را می بیند. اصل چهارچشـــمی برای ممیز نیز قابل اســـتفاده است. SCB می توانـــد چندین کلید را برای رمزنگاری تریل های ممیزی اســـتفاده کند. در این شرایط برای نمایش تریل ها چندین کلید گشایش رمز لازم است. بنابر این یک ممیز به تنهایی امکان دسترسی به اطلاعات سیستم شما را نخواهد داشت.

SCB
Shell Control Box Solution

تأیید هویت و اصالت سرورها

SCB قابلیت کنترل و تأیید کلیدهای SSH Host و گواهی شناسایی سرورها را به صورت پایه ای و درونـی دارد. ایـن موضـوع از حمـلات man in the middle و سایـر دستکاری هـا در سیستـم جلوگیری می کنـد.

ماندگاری داده های برای چند سال

ارتباط ترمینال SSH و Telnet که حجم عمده کاری ادمین سیستم را به خود اختصاص می دهند و بیشتر از بقیه انواع ترافیک برای ممیزی مورد توجه هســتند، حجم زیادی از فضای هارد دیســک را اشغال نمی کنند. (حدود1MB به ازای هرساعت بسته به شـرایط) بنابــر این SCB نزدیک ۵۰۰.۰۰۰ ســاعت از فعالیت های مدیـریت و ادمین را می توانـد در خـود ذخیـره کنـد. به این معنی که اگر شرکتی ۵۰ نفر ادمین داشته باشـد که به صورت ۲۴*۷ فعالیت میکنـد SCB می تواند کل ترافیک SSH و Telnet را برای مدت بیشــتر از یک ســـال با فرمت قابل جستجو، نمایش و تکـرار که به آسانی در دسترس قرار می گیـرد، در خود نگه دارد.

این زمان بدون در نظر گرفتن اطلاعات آرشیو شده روی سرور پشتیبان راه دور است که به راحتی از طریق SCB در دسترس است. ارتباطات RDP فضای قابل توجه تری را اشغال می کنند (معمولاً کمتر از 1MB در دقیقه) به این معنی که SCB هفته ها کار با این پروتکل را می تواند در خود ذخیره نماید.

یکپارچه سازی SCB در شبکه

این سیستم برای یکپارچگی با زیر ساخت شبکه مد های پیاده سازی مختلفی را پشتیبانی می کند که عبارتند از:

Bastion mode ، Router mode ، Bridge mode .

برای یکسو شدن با محیط دیواره آتش، SCB از NAT های مبتنی بر آدرس مبدا و مقصد پشتیبانی می کند (SNAT ، DNAT).

Bridge mode

در این حالت SCB همانند یک سوئیچ لایه ۲ شبکه عمل می کند به گونه ای که اینترفیس های سمت کلاینت و سرور در یک Subnet قرار دارند.

Router mode

در حالت روتر، SCB به عنوان یک روتر لایه ۳ شبکه عمل میکند به گونه ای که اینترفیس های سمت کلاینت و سرور در دو Subnet مختلف قرار می گیرند.

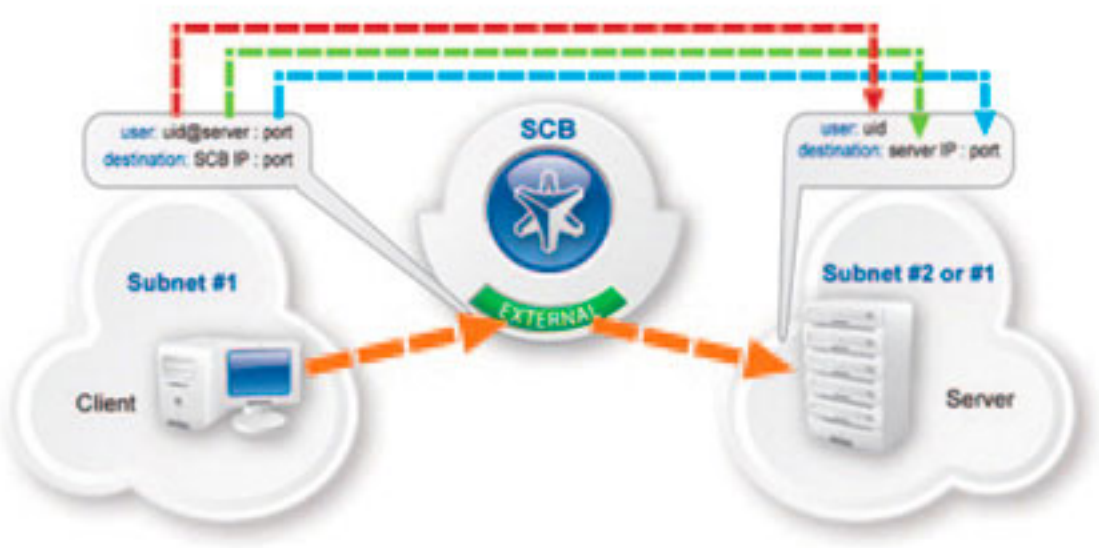
Bastion mode

در این حالت هر سرور به صورت یک پورت مجزا بر روی آدرس آی پی SCB تعریف می گردد. در نتیجه فایروال شبکه باید به گونه ای پیکربندی شود تا این اطمینان حاصل شود که تنها ارتباطاتی که از SCB نشأت گرفته اند، بتوانند به سرور دسترسی پیدا کنند.

به گونه ای که ادمین ها تنها SCB را می بینند و SCB ارتباط فوق را به ارتباط با سرور واقعی تبدیل می کند.

عملکرد غیرشفاف (مرئی)

SCB می تواند به صورت غیرشفاف عمل کند و آدرس سرور مورد نظر را با بررسی پکت های پروتکل که قصد اتصال به آن سرور را دارد استخراج کند. عملکرد غیرشفاف به طور کلی در حالت Bastion مورد استفاده قرار می گیرد.



یکپارچگی با دایرکتوری کاربر

SCB می تواند به یک بانک اطلاعاتی LDAP راه دور (نظیر اکتیودایرکتوری مایکروسافت) جهت احراز هویت گروه کاربرانی که به سرورهای محافظت شده دسترسی دارند، متصل شود. قوانین و محدودیت ها را می توان بر اساس هویت گروهی کاربران تعیین کرد.

هنگامی که از کلید عمومی برای احراز هویت در پروتکل SSH استفاده می شود، SCB می تواند کاربران را با استفاده از کلید یا مجوز x.509 که در بانک LDAP ذخیره کرده است، احراز هویت کند.

ادمین ها و ناظرانی که از طریق وب به SCB دسترسی دارند را نیز می توان با استفاده از دیتابیس LDAP احراز هویت کرد.

احراز هویت از طریق RADIUS (برای مثال استفاده، از SecurID) هم برای دسترسی به وب مدیریت SCB و هم برای احراز هویت ارتباطات ممیزی شده SSH ، ساپورت می شود.

مدیریت SCB

SCB دارای یک رابط گرافیکی دقیق و بی عیب می باشد.

وظایف و اختیارات ادمین های SCB قابل تعریف شدن براساس یک سری از دسترسی هاست.

- مدیریت SCB به عنوان یک هاست
- مدیریت ارتباطات به سمت سرورها.
- دیدن تریل های ممیزی شده و گزارشات و .....

دسترسی به اینترفیس وبی SCB می تواند به شبکه فیزیکی مستقل که مخصوص ترافیک مدیریت است، محدود شود. این اینترفیس مدیریتی همچنین برای پشتیبان گیری، لاگ کردن به سرور راه دور و سایر ترافیک های مدیریتی می تواند استفاده شود.

کاربرانی که به رابط گرافیکی SCB دسترسی دارند را می توان از طریق یک بانک LDAP یا RADIUS احراز هویت کرد.

تمام تغییرات پیکربندی به طور خودکار ثبت می شوند.

SCB این امکان را دارد که ادمین ها را وادار کند که اگر تغییری در پیکر بندی SCB ایجاد کردند دلیل آن را نیز ذکر کنند.

SCB از تغییرات پیکربندی دستگاه گزارش تهیه می کند. در جزئیات و توضیحات تغییرات اعمال شده می توان جستجو کرد و می توان آنها را از طریق وب مشاهده کرد. (ساده سازی ممیزی)

SCB
Shell Control Box Solution

پشتیبانی از سطوح دسترسی بالا (High Availability)

SCB از سطح دسترسی بالا پشتیبانی می کند. بدین صورت که دو سخت افزار (Master & Slave) که دارای پیکربندی یکسان می باشند به طور همزمان کار می کنند. دو سخت افزار دارای فایلهای زیر سیستمی یکسانی می باشند. Master تمامی داده ها را در سریعترین زمان ممکن که داده ها دریافت می شوند با Slave به اشتراک می گذارد. تمامی تغییرات پیکربندی و ترافیک های ضبط شده بلافاصله با Slave هماهنگ سازی می شود. اگر Master در عملکرد خود دچار مشکل شود Slave بلافاصله فعال می شود. بنابراین سرورهای محافظت شده به طور مداوم قابل دسترسی می باشند.

پشتیبان گیری به صورت خودکار

تریل های ممیزی ضبط شده، تغییرات پیکربندی SCB و باقی داده ها را می توان از ۳ روش زیر به یک سرور راه دور فرستاد.

- NFS (Network File System Protocol)
- Rsync over SSH
- Server Message Block protocol (SMB/CIFS)

آرشیو داده ها به صورت خودکار

تریل های ممیزی ضبط شده به صورت خودکار بر روی یک سرور راه دور آرشیو می شوند. داده ها برروی سرور راه دور قابل دسترسی و قابل جستجو باقی می مانند. چندین ترابایت از تریل های ممیزی از طریق رابط گرافیکی SCB قابل دسترسی است. SCB از سرورهای راه دور به عنوان یک درایو شبکه ای با استفاده از NFS یا SMB/CIFS استفاده می کند.

BalaBit IT Security

BY FavaMouj

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 کاربـردی، توجه به نیاز مشتری و رضـایت او، تلاش شبانه روزی و روحیه همکاری همـواره از ویـژگی هـای فاواموج بـوده اسـت.

شبکه و ارتباطات، ارتباط یکپارچه (UC)، مدیریت و امنیت ارتباطات، سرویس ها و نرم افزارهای ارتباطی به عنوان محورهای اصلی فعالیت شرکت معرفی شـده اند. از مهمترین راه حل هـای شرکت می توان به راه حـل مراکز تلفنی آی پـی، راه حل وب کنفرانس و ارتبـاط یکپارچه، راه حل کشینگ برای سرویس دهنده های اینترنت، احراز هویت دو عاملی و جدیدترین و شاید جذاب ترین آنها یعنی ممیـزی ادمین هـا، اشـاره کرد.

فاواموج همواره تلاش نموده تـا برای مشتـریان دوست داشتنی خـود، مشاوری صدیق و امین باشـد و تمام تـوان خـود را به منظور موفقیت آنها در کسب و کار خویش، به کار برده و خواهد برد.

فاواموج

ارتباطات و فناوری اطلاعات

تهران، خیابان قائم مقام فراهانی، پایین تر از مطهری، کوچه الونـد، شماره ۹

تلفن: (خط ویژه) ۱۰۰۰ ۳٤ ۸۹ دورنگار: ۱۰۰۱ ۳٤ ۸۹

www.favamouj.com