به نام خدا

سند هدف امنیتی
[سامانه امن سازی و مدیریت شبکه سبلان -نسخه۳.۷]

[شرکت ایده پژوهان اسپادانا]

[۰۵-۱۴۰۳]

[۳.۷]

فهرست

[شرکت ایده پژوهان اسپادانا]

۱ معرفی

[این بخش سند هدف امنیتی بیانگر مشخصات کلی محصول می‌باشد. در این قسمت باید دیدکلی از محصول ارزیابی شده ارائه گردد.]

۱،۱ مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه امن سازی و مدیریت شبکه سبلان
نسخه	۱.۰
تاریخ	۰۵/۱۴۰۳
نویسندگان	سارا اختری

نام شرکت	ایده پژوهان اسپادانا
نام محصول	سامانه امن سازی و مدیریت شبکه سبلان
نوع محصول	امن سازی و مدیریت شبکه های کامپیوتری
نسخه‌ی محصول	۳.۷

حداقل نیازمندی نرم‌افزاری/سخت‌افزاری/میان‌افزاری محصول

در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

سخت‌افزار/نرم-افزار/میان‌افزار	حداقل الزامات
سخت افزار	با توجه به لایسنس مورد تقاضا(بسته به میزان ترافیک عبوری) متغیر است. به طور کلی، نیاز محصول به RAN و حافظه کم و به دلیل رمزنگاری نیاز به cpu متوسط یا بالا دارد. برای نمونه در حالت شبکه به شبکه، و سوییچ حداقل به cpu(Core i3)، RAM(4GB) و SSD(64 GB).
نرم افزار	محصول در پکیج نرم افزاری قابل اجرا روی سیستم عامل Centos بدون پیشنیاز است. در صورت نیاز سایر سیستمهای عامل نیز قابل پشتیبانی هستند.

۲ ادعای انطباق

در این قسمت باید انطباق سند هدف ارزیابی با موارد مطرح شده در جداول زیر مشخص شود، برای اطلاعات بیشتر جهت تکمیل این قسمت به بخش ۱.۲ از سند «راهنمای نوشتن سند هدف امنیتی» مراجعه شود.

۱،۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO 15408 V3.1 R4
نام پروفایل حفاظتی	
سطح تضمین امنیتی	EAL1

۲،۲ شرح محصول

[در این قسمت محصول و کارکرد امنیتی آن به همراه کامپوننت‌های اصلی در حدود ۲ تا ۳ پاراگراف شرح داده می‌شود.]

سامانه سبلان، سامانه ای است که به منظور مدیریت شبکه، کاربران و تامین امنیت آنان تهیه شده است. این سامانه دارای خواصی است که آنرا برای مدیریت شبکه هایی با تعداد دفاتر زیاد که ممکن است با یکدیگر نیز ارتباط داشته باشند مناسب نموده است. این سامانه (غیر از سخت افزار) کاملا بومی بوده و برای ایران که موقعیت ویژه سیاسی و ایدئولوژیک دارد حائز اهمیت فراوان است. طراحی این سامانه کاملا ایرانی بوده و تقلیدی از پیاده سازی های دیگر نیست و غیر از الگوریتم های رمز استاندارد از هیچ سورس متن بازی استفاده نکرده است. سامانه سبلان ترافیک کاربران احراز هویت شده را گروه بندی نموده و سیاست های امنیتی هر گروه را به صورت جداگانه اعمال می‌کند. ترافیک احراز هویت نشده در گروهی با نام پیش فرض قرار دارد. بدین ترتیب قانون نویسی برای سامانه بر اساس گروه های مجزای کاربری به سادگی امکان پذیر است.

سامانه سبلان برای اجرای ماموریت های محوله دارای اجزایی است که این اجزاء به شرح زیر است:

- سرور اصلی (Sabalan Server): هسته اصلی سامانه که در لبه شبکه قرار می گیرید و شامل واحدهای پردازشی تفاوت از قبیل تونلینگ، روتینگ، فایروالینگ، شکلدهی ترافیک، ترجمه آدرس و ... است. سرور سبلان در مامورتها و سناریوهای متنوع قابل استفاده است. این ماموریتها شامل برقراری ارتباطات بین شبکه های محلی در سطح لایه ۳ شبکه، ارتباطات کاربران با شبکه داخلی و در کاملترین سناریو برقراری ارتباط امن در سطح لایه ۲ شبکه بین شبکه های توزیع شده(سوییچ امن توزیع شده)، است.
- نرم افزار های مدیریت سامانه(e_manager و e_token_manager و e_net_manager و e_keybank_manager) این نرم افزار های جهت مدیریت سامانه و اعمال پیکربندی طراحی شده اند.

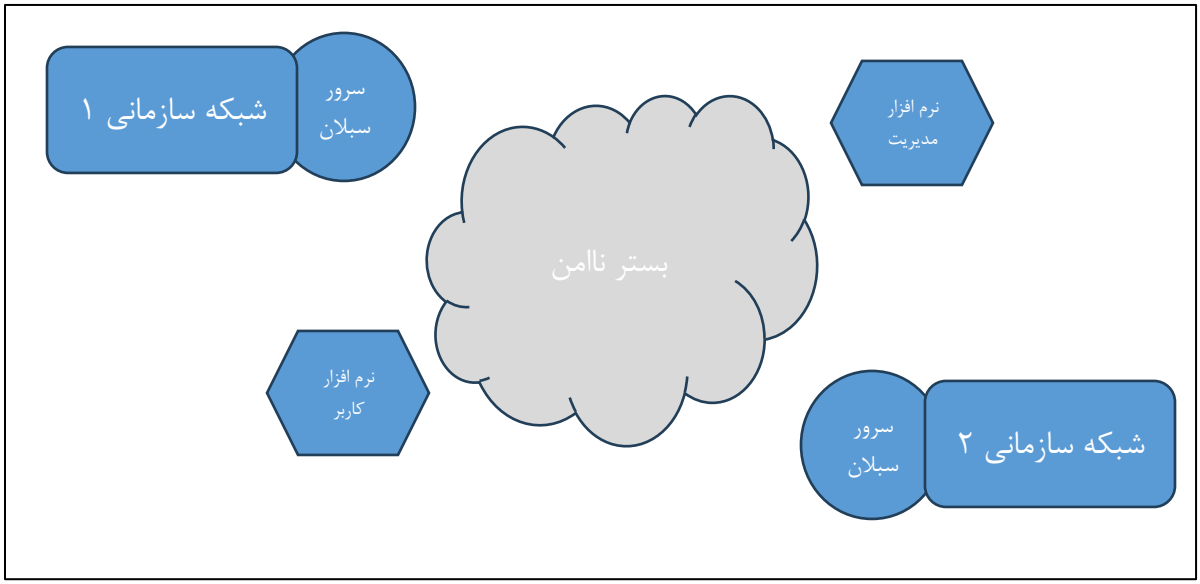
- نرم افزار های کاربر (e_client و e_phone و e_rclient و e_gclient) این نرم افزار ها جهت برقرار ارتباط کاربر با سامانه و هدایت ترافیک طراحی شده اند و در مامورتهای متفاوت مورد استفاده قرار می گیرند.

۱,۲,۲ حوزه فیزیکی

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده در جدول زیر مشخص گردیده است:

عناصر محصول	شماره مدل یا نسخه
سخت افزار	این محصول مستقل از سخت افزار است و روی هر نوع سخت افزار با حداقل نیازمندی ذکر شده قابل بهره برداری است.

در این بخش قرار گیری محصول در محیط عملیاتی و پیکربندی آن در قالب تصویر آورده شود. لازم است محصول و محیط عملیاتی به تفکیک در تصویر مشخص گردند. (به دلیل تنوع توپولوژی و سناریوهای ارتباطی، تنها یک سناریو به عنوان نمونه تشریح شده است. در این تصویر دو شبکه سازمانی که مجزا در نظر گرفته شده است که سرور های سبلان در لبه آنها قرار دارند. این سرورها ترافیک عبوری و دسترسی به شبکه های سازمانی شامل ارتباط بین دو شبکه مجزا و ارتباط کاربران خارجی با شبکه های داخلی را کنترل می کنند. به منظور مدیریت سرورها نرم افزار های مدیریتی مورد استفاده قرار میگیرند که پیکربندی و سیاستگذاریها با استفاده از آنها تعریف می شوند. موجودیتها و کاربرانی که قصد ارتباط با شبکه های سازمانی را دارند باید با استفاده از تونلینگ امن در سامانه سبلان احراز هویت شوند و سپس ترافیک آنها بر اساس پالیسی هدایت می شوند.)



شکل ۱: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

۲,۲,۲ حوزه منطقی

[شرکت ایده پژوهان اسپادانا]

[کارکردهای امنیتی محصول تحت عنوان حوزه منطقی شناخته می‌شود که باید به صورت مشخص هریک از کارکردها و شرح آنها در این قسمت مطرح شود.]

کارکردها	توصیف
تونلینگ و رمزنگاری	*کاربران و موجودیتهای سامانه با استفاده از پروتکل های بومی در سامانه احراز هویت می شوند و ترافیک آنها بر اساس سیاستهای ارتباطی هدایت می شوند.*
فایروالینگ	*ترافیک عبوری از سرور بر اساس سیاستهای فایروالینگ تعریف شده هدایت می شود.*
ترجمه آدرس	*در صورت نیاز برای برقراری ارتباط یا با هدف امن سازی شبکه داخلیترجمه آدرس مبدا و مقصد ترافیک(Source Nat- Destination NAT- IP/Port NAT) انجام می شود.*
شکل دهی ترافیک	*جهت مدیریت پهنای باند و ایجاد محدودیت برای کاربران با استفاده از واحد traffic shaping، پهنای باند بین کاربران و گروههای کاربری تسهیم می گردد.*

۳ مسائل امنیتی

[این فصل تنها کافیست از سند پروفایل حفاظتی کپی گردد.]

۱,۳ تهدیدات

تهدیدات	توضیحات

۲,۳ خط‌مشی امنیتی

خط مشی ها	توضیحات

۳/۳ فرضیات

فرضیات	توضیحات

٤ اهداف امنیتی

[این فصل تنها کافیست از سند پروفایل حفاظتی کپی گردد.]

۱،٤ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات

۲،٤ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توضیحات

٥ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید داده ممیزی ۱**	FAU_GEN.1.1
۲		
۳		
٤		

شماره الزام	نام الزام	تطابق الزام با استاندارد
٥		
٦		
٧		
٨		
الزامات مربوط به پیوست اول		
٩		
١٠		
١١		
١٢		
١٣		
١٤		

۱٫۵ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**
۲	.....

۲٫۵ کلاس .....

شماره الزام	نام الزام
۳	
٤	

[شرکت ایده پژوهان اسپادانا]

شماره الزام	نام الزام

۳/۵ کلاس .....

شماره الزام	نام الزام

٤,٥ کلاس .....

شماره الزام	نام الزام

٥,٥ کلاس .....

شماره الزام	نام الزام

۶٫۵ کلاس .....

شماره الزام	نام الزام

۷٫۵ کلاس ....

شماره الزام	نام الزام

۸٫۵ کلاس .....

شماره الزام	نام الزام
۱۱	

٦ الزامات تضمین امنیت

[این بخش از سند پروفایل حفاظتی کپی گردد.]

۷ خلاصه مشخصات محصول

[در این بخش به ازای هریک از کلاس‌های کارکردی در فصل پنجم، خلاصه‌ای از عملکرد امنیتی در آن کلاس بیان گردد.]