به نام خدا

سند هدف امنیتی

APK Gate

شرکت فنی و مهندسی امن پردازان کویر

دی ماه ۱۴۰۰

نسخه ۱,۰

فهرست

۱ مقدمه

این بخش سند هدف امنیتی APKGate، شرکت امن‌پردازان کویر و قراردادها را معرفی می‌نماید. محصول APKGate که در این سند امنیتی ارائه شده؛ یک UTM بومی است که جهت تامین امنیت تجهیزات شبکه در مقابل تهدیدات و حملات در لبه شبکه قرار می‌گیرد.

۱.۱ مرجع سند هدف امنیتی و مرجع هدف ارزیابی

عنوان سند هدف امنیتی	سند هدف امنیتی APKGate
نسخه	۲.۱۲
تاریخ	۹۸/۰۷/۰۳
نویسندگان	کارشناسان تحقیق و توسعه گروه APKGate شرکت امن پردازان کویر

نام تولید کننده (شرکت)	امن پردازان کویر
نام هدف ارزیابی	APKGate ۳۳۰
نوع هدف ارزیابی	UTM
نسخه	۵.۸.۰

۲.۱ دید کلی هدف ارزیابی

APKGate یک سیستم مدیریت یکپارچه تهدیدات است که دارای امکانات و خصوصیت‌های زیر می‌باشد که در ادامه تشریح شده است.

- **Firewall و NAT**

فایروال محصول از نوع statefull می باشد. همچنین با استفاده از قسمت NAT می‌توان port forward، NAT ۱ to ۱ و SNAT را برای مدیریت ارتباطات تعریف کرد.

- **شناسایی و جلوگیری از حملات(IDS&IPS)**

این محصول با به‌روزرسانی مداوم Signature حملات در بستری کاملا امن، قادر به تشخیص طیف وسیعی از حملات در لایه های مختلف شبکه است. در این محصول قابلیت‌هایی نظیر مدیریت الگوی حملات، کار در وضعیت غیر محسوس و امکان تعریف الگوی جدید حملات در نظر گرفته شده است.

- **شبکه‌های خصوصی مجازی(VPN)**

سرویس VPN این محصول که علاوه بر پشتیبانی از VPNها بر روی پروتکل IPsec از پروتکل Open VPN نیز استفاده و با ایجاد بستری مستقل تبادل اطلاعات و داده‌ها را امن و از بروز حوادث جلوگیری می‌نماید.

- **مدیریت گزارش‌گیری (Logs&Report)**

یکی از بخش‌های مهم و کلیدی این محصول گزارش‌گیری و واقعه‌نگاری آن می‌باشد. ماژول مدیریت گزارش‌گیری و گزارش‌ساز این محصول امکان مشاهده رخداد Firewall، IPS، Visited Site و Accounting را میسر می‌سازد.

۱.۲.۱ نوع هدف ارزیابی

APKGate نوعی UTM است که شامل مجموعه ای از راهکارهای امنیتی مانند: دیوار آتش (Firewall) ، VPN Server، IDS و IPS می‌باشد.

۲.۲.۱ نرم افزار/سخت افزار/میان افزار غیر هدف ارزیابی ضروری

محصـــول APKGate به صـــورت Appliance جهت ارزیابی امنیتی ارســـال گردیده اســـت و تنها به یک مرورگر اینترنت جهت دسترسی به محیط مدیریتی گرافیکی محصول نیاز دارد.

Component	حداقل الزامات
APKGate	دستگاه APKGate
Web Console	Web Browser به روز شده

۳.۱ توصیف هدف ارزیابی

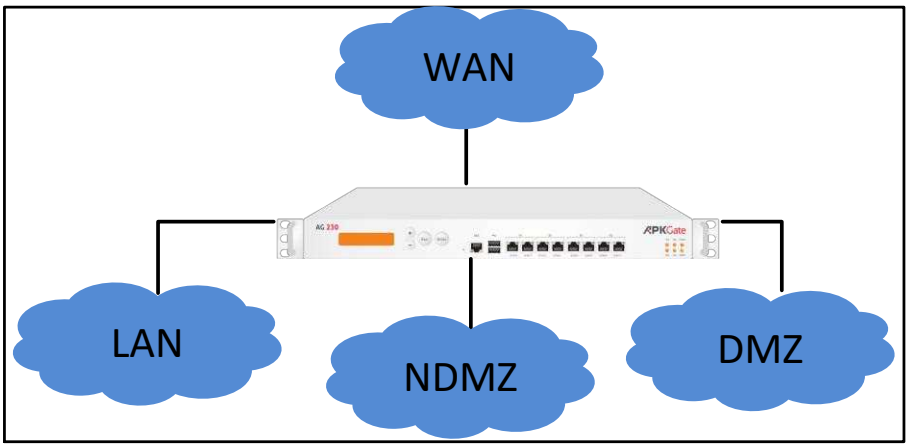
محصول APKGate شامل یک سیستم‌عامل و یک سخت‌افزار است که به صورت Appliance ارائه می‌گردد. در این محصول با قرار گرفتن ماژول‌ها (Firewall، VPN-GW، IDS و IPS) کنار یک دیگر امکان مدیریت یکپارچه تهدیدات در لبه (edge) شبکه فراهم است. به‌طوری که می‌توان نحوه دسترسی به منابع شبکه را بر اساس IP، Port و پروتکل مدیریت کرد و همچنین با استفاده از ماژول IDS/IPS امکان امن کردن شبکه در برابر طیف وسیعی از حملات و بد افزارها فراهم می‌شود. این دستگاه قادر است تا کلیه ترافیک‌های ورودی و خروجی شبکه را زیر نظر داشته، مدیریت کرده و گزارش بگیرد. لازم به ذکر است که این محصول در مدل‌های AG ۱۱۰، AG ۱۳۰، AG ۲۱۰، AG۲۲۰، AG ۳۱۰، AG ۳۳۰، AG ۴۱۰، AG ۴۳۰، AG ۵۱۰، AG ۵۳۰، AG ۶۱۰ و AG ۶۳۰ قابل ارائه می‌باشد.

۱.۳.۱ حوزه فیزیکی

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر هدف ارزیابی	شماره مدل یا نسخه
APKGate	مدل ۳۳۰ نسخه ۵.۸.۰

دستگاه APKGate دارای پورت‌های USB (اتصال صفحه کلید) و VGA (اتصال مانیتور) برای مدیریت دستگاه به صورت Local می‌باشد. همچنین با استفاده از پروتکل HTTPS (برای دسترسی به محیط گرافیکی) به صورت امن از داخل و یا خارج از شبکه محلی (از راه دور) قابل مدیریت و پیکربندی است. همچنین با استفاده از پورت کنسول می‌توان به کنسول دستگاه دسترسی پیدا کرد.



نحوه قرارگیری دستگاه APKGate در شبکه

۲.۳.۱ حوزه منطقی

کارکردهای امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می‌شود که به صورت مشخص هر یک از کارکردها و شرح آن‌ها در این قسمت مطرح شده است.

کارکردها	توصیف
کنترل ومدیریت دسترسی	کنترل دسترسی با استفاده از firewall و مدیریت ارتباط به اینترنت با استفاده از NAT
ایجاد ارتباط امن	برقراری ارتباط امن به منظور تبادل اطلاعات در درون یا برون سازمان را فراهم می‌کند
حفاظت شبکه در برابر تهدیدات	جهت حفظ امنیت منابع سازمان در برابر طیف وسیعی از حملات و بدافزارها
ممیزی امنیت	هدف ارزیابی رویدادهای ممیزی متنوعی را تولید و به صورت محلی ذخیره می نماید.
حوزه رمزنگاری	هدف ارزیابی از انواع الگوریتم های رمزنگاری متقارن و نامتقارن پشتیبانی می کند.
مدیریت امنیت در محصول	فقط کاربران تعریف شده در محدوده های مجوزهای داده شده می‌توانند به امکانات مدیریتی دسترسی داشته باشند.

۲ ادعای انطباق

۱.۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO/IEC ۱۵۴۰۸ Information technology — Security techniques — Evaluation criteria for IT security, Common Criteria September ۲۰۱۲, Version ۳,۱, Revision ۴
انطباق با SFR ها (قسمت دوم از CC)	این سند هدف امنیتی منطبق بر قسمت دوم از استاندارد ارزیابی معیار مشترک است.
انطباق با SARها (قسمت سوم از CC)	این سند هدف امنیتی منطبق بر قسمت سوم از استاندارد ارزیابی معیار مشترک است.

۲.۲ انطباق با پروفایل حفاظتی

پروفایل حفاظتی سامانه مدیریت یکپارچه تهدیدات (UTM) – اسفند ۹۶ – نسخه ۲,۰

۳.۲ انطباق با سطح اطمینان امنیتی

EAL۱	این سند جهت تطابق هدف ارزیابی با EAL۱ ارائه گردیده است.

نوع انطباق: منطبق

۳ تعریف مسائل امنیتی

این بخش به منظور مشخص نمودن ماهیت مسائل امنیتی که هدف ارزیابی آن ها را برطرف نموده در نظر گرفته شده است و شامل موارد زیر است:

- هر گونه خط‌مشی سازمانی یا قوانینی که هدف ارزیابی مطابق با آن باشد.
- هر تهدید شناخته شده یا فرضی در قبال دارایی‌ها که در داخل هدف ارزیابی یا محیط عملیاتی به حفاظت خاصی نیاز دارند.
- هرگونه فرضیاتی در رابطه با معیارهای امنیتی محیط و/یا طریقه‌ای که برای استفاده هدف ارزیابی در نظر گرفته شده است.

۱.۳ خط‌مشی امنیتی سازمانی

این بخش از تعریف مسائل امنیتی، خط‌مشی‌های امنیتی سازمانی که توسط هدف ارزیابی یا محیط عملیاتی و یا هردو اجرا می‌گردند را مشخص می‌نماید.

خط‌مشی‌ها	توصیف
P.ACCACP	تمام کاربران مجاز هدف ارزیابی مسئول اقداماتشان باشند.
P.MANAGE	هدف ارزیابی توسط کاربران مجاز مدیریت گردد.
P. PROTCT	هدف ارزیابی از ورود غیرمجاز و اختلال در اجرای سرویس‌ها محافظت می‌نماید.
P.ACCESS_BANNER	هدف ارزیابی باید علامت اولیه‌ایی را نمایش دهد که توصیف کننده محدودیت‌های استفاده، توافقات قانونی یا هرگونه اطلاعات مناسب دیگری است که کاربران با دستیابی به هدف ارزیابی با آن‌ها موافقت می‌کنند.

۲.۳ تهدیدات

این بخش از تعریف مسائل امنیتی، تهدیداتی که توسط هدف ارزیابی یا محیط عملیاتی یا هردو مقابله می‌شوند را مشخص می‌نماید.

تهدید	توصیف
T.ACCIDENTAL_ADMIN_ERROR	سرپرست ممکن است ناخواسته هدف ارزیابی را به صورت نادرست نصب و پیکربندی کند و سبب ناکارآمد شدن ساز و کارهای امنیتی شود.
T.NETWORK_ACCESS	به یک یا چند شبکه، نقطه پایانی، یا سرویس دسترسی نامناسب یافتن مثلاً از طریق جستجوی فراگیر برای تخمین گذرواژه‌ها، یا انتقال کد اجرایی مخرب، اسکریپت، یا دستورات. اگر ابزارهای خارجی مخرب بتوانند با ابزارهای موجود در شبکه حفاظت شده، ارتباط برقرار کنند، آنگاه این ابزارها مستعد دسترسی غیرمجاز و افشاء اطلاعات هستند.
T.NETWORK_DOS	حمله به سرویس‌های شبکه از بیرون(DOS)
T.NETWORK_MISUSE	دسترسی به سرویس‌هایی که توسط یک شبکه حفاظت شده فراهم شده است، ممکن است بر خلاف خط‌مشی‌های محیط عملیاتی صورت گیرد. ابزارهایی که خارج از شبکه حفاظت شده قرار دارند ممکن است حین ارتباط با سرویس‌های عمومی مجاز، در صدد اجرای فعالیت‌های نامتعارف برآیند. برای مثال، دستکاری

	ابزارهای موجود در شبکه، تزریق کدهای SQL ، فیشینگ، اجبار به بازنشانی، فایل‌های فشرده مخرب، کدهای اجرایی مبدل، ابزارهای ارتقای سطح دسترسی و بات نت‌ها.
T.NETWORK_DISCLOSURE	اطلاعات حساس روی یک شبکه حفاظت شده ممکن است در اثر افشا/انتقال اطلاعات بر خلاف خط‌مشی‌ها فاش گردد، به عنوان مثال با ارسال شماره کارت اعتباری به صورت رمزنگاری نشده، اطلاعات حساس فاش شوند. هدف ارزیابی IPS قادر خواهد بود تا محتوای بسته‌ها را برای شناسایی رشته داده‌ها و الگوهای کاراکتری، بازرسی کند
T.TSF_FAILURE	شکست سازوکارهای امنیتی هدف ارزیابی، عملکرد امنیتی هدف ارزیابی را نیز به خطر می‌اندازد.
T.REPLAY_ATTACK	اگر موجودیت IT خارجی یا مخرب بتواند به شبکه دستیابی داشته باشد، ممکن است توانایی ربودن اطلاعات در حرکت در سراسر شبکه و فرستادن آن‌ها به مقصد مورد نظر را نیز داشته باشد.
T.DATA_INTEGRITY	بخش مخربی که سعی در تغییر داده فرستاده شده دارد سبب از بین رفتن صحت داده می‌شود.
T.UNDETECTED_ACTIONS	کاربران مخرب از راه دور یا موجودیتهای IT خارجی ممکن است اقدامی انجام دهند که امنیت هدف ارزیابی را به صورت مخرب تحت تاثیر قرار بدهند .این اقدام ممکن است تشخیص داده نشده، باقی بماند و بنابراین نمیتوان اثر این گونه اقدامات را به طور موثری کاهش داد.
T.UNAUTHORIZED_ACCESS	ممکن است کاربر دسترسی غیرمجازی به دادهها و کد اجرایی هدف ارزیابی پیدا کند .یک کاربر، پروسه مخرب یا موجودیت IT خارجی ممکن است خود را به عنوان یک موجودیت مجاز جا بزند تا بتواند به صورت غیرمجاز به داده‌ها یا منابع هدف ارزیابی دستیابی پیدا کند .یک کاربر، پروسه مخرب یا موجودیت IT خارجی ممکن است خودش را به عنوان هدف ارزیابی معرفی کند تا بتواند داده‌های شناسایی و احراز هویت را به دست آورد.
T.UNAUTHORIZED_UPDATE	بخش مخرب سعی میکند به کاربر به روز رسانی از محصول ارائه دهد که ویژگیهای امنیتی هدف ارزیابی را به خطر اندازد.
T.USER_DATA_REUSE	فرستنده ممکن است سهواً داده کاربری را به گیرندهای ارسال کند که مدنظر نبوده است.

۳.۳ فرضیات

جهت عملکرد بهتر هدف ارزیابی در ازمون، توصیه می‌شود تا مفروضات مذکور در جدول زیر رعایت گردد.

فرضیات	توصیف
A.NO_GENERAL_PURPOSE	فرض شده است که قابلیت محاسباتی همه منظوره (به طور مثال، کامپایلر یا برنامه‌های کاربردی) به غیر از سرویس‌های لازم برای عملیات، سرپرستی و پشتیبانی از هدف ارزیابی در دسترس هدف ارزیابی نمی‌باشد
A.CONNECTIONS	فرض می‌شود که هدف ارزیابی در لبه شبکه قرار گرفته است و به عنوان Default Gateway مورد استفاده است.
A. Physical security	هدف ارزیابی در یک محیط فیزیکی امن قرار دارد که تنها افراد مجاز دسترسی فیزیکی به آن دارند.
A. Trusted administrator	سرپرست مجاز هدف ارزیابی سوء نیت نداشته و آموزشهای مناسب برای کارکردهای مربوط به سرپرست هدف ارزیابی و وظایف محوله به وی را مطابق با دستورالعمل سرپرستی فراگرفته است.

٤ اهداف امنیتی

۱.٤ اهداف امنیتی برای هدف ارزیابی

این قسمت شامل مجموعه‌ای از اهداف است که هدف ارزیابی با انجام آن‌ها، بخشی از مسائل مطرح شده در بخش قبل را حل خواهد نمود.

۱.۱.٤ Firewall

هدف امنیتی	توصیف

O.ADDRESS_FILTERING	هدف ارزیابی توانایی فیلتر نمودن و گزارش‌گیری بسته‌های شبکه را براساس آدرس مبدا و مقصد فراهم خواهد نمود.
O.PORT_FILTERING	هدف ارزیابی توانایی فیلتر نمودن و گزارش‌گیری بسته‌های شبکه را براساس پورت‌های لایه انتقال مبدا و مقصد فراهم خواهد نمود.
O.STATEFUL_INSPECTION	اگر بسته شبکه به یک اتصال برقرار شده مجاز تعلق داشته باشد، پیش از اعمال مجموعه قوانین، هدف ارزیابی تصمیم گیری خواهد کرد.
O.RELATED_CONNECTION_FILTERING	برای پروتکل‌های خاص، هدف ارزیابی به صورت داینامیک اجازه جریان بسته شبکه را در واکنش به اتصال مجاز شده توسط مجموعه قوانین را خواهد داد.

۲.۱.٤ VPN Gateway

هدف امنیتی	توصیف
O.AUTHENTICATION	هدف ارزیابی توانایی احراز هویت کاربران را ارائه خواهد نمود تا اطمینان دهند که آن‌ها با موجودیت IT خارجی مجاز در ارتباط هستند.
O.CRYPTOGRAPHIC_FUNCTIONS	هدف ارزیابی توانایی رمزنگاری و رمزگشایی داده را ارائه خواهد نمود تا محرمانگی حفظ گردد و اجازه می‌دهد تا داده‌های عملکرد امنیتی هدف ارزیابی که خارج از هدف ارزیابی منتقل میگردند تغییر شکل یابند (رمز شوند) و آشکار گردند (رمزگشایی گردند).
O.FAIL_SECURE	هنگامی‌که خودآزمایی با شکست مواجه می‌گردد، هدف ارزیابی خاموش خواهد شد تا اطمینان حاصل شود که داده‌ها نمی‌توانند منتقل گردند.

۳.۱.٤ Network Equipment

هدف امنیتی	توصیف
O.PROTECTED_COMMUNICATIONS	هدف ارزیابی برای سرپرستان، دیگر بخشهای هدف ارزیابی توزیع شده و موجودیتهای IT مجاز کانالهای ارتباطی محافظت شدهای فراهم خواهد کرد.
O.DISPLAY_BANNER	هدف ارزیابی پیام مشورتی نمایش خواهد داد
O.TOE_ADMINISTRATION	هدف ارزیابی سازوکارهایی ارائه خواهد داد تا اطمینان دهد که تنها سرپرستان قادر به وارد شدن به سیستم و پیکربندی هدف ارزیابی هستند و برای سرپرستان وارد شده به سیستم محافظتی فراهم خواهد کرد
O.RESIDUAL_INFORMATION_CLEARING	هدف ارزیابی اطمینان خواهد داد هیچ یک از داده‌های یک منبع محافظت شده در زمان آزادسازی آن منبع، در دسترس قرار نخواهند گرفت
O.SESSION_LOCK	هدف ارزیابی سازوکارهایی ارائه خواهد داد که خطر سرقت نشست‌های بدون مراقبت را کاهش می‌دهد
O.TSF_SELF_TEST	هدف ارزیابی قابلیتی جهت آزمودن برخی از زیر مجموعه عملکردهای امنیتی خود ارائه خواهد داد تا از عملکرد مناسب آن‌ها اطمینان حاصل کند

٤.۱.٤ IDS

- **مانیتور کردن سیستم**

برای این که سـرپرست سیستم بتواند بر عملیات کارکرد IPS شرح داده شده « تجهیزات شبکه » نظارت کند، این هدف امنیتی، که در پروفایل حفاظتی است، به شرح زیر تکمیل می‌گردد.
برای این که بتوان نقض خط‌مشی‌ها در شبکه را تحلیل کرد و به آن‌ها واکنش نشان داد، IPS بتواند عناصر داده‌های ضروری ترافیک را در شبکه‌های مورد نظارت، جمع‌آوری و ذخیره می‌نماید.

(O.SYSTEM_MONITORING -> FAU_GEN.۱(۲), IPS_NTA_EXT.۱, IPS_IPB_EXT.۱, IPS_SBD_EXT.۱, IPS_ABD_EXT.۱)

- **تحلیل نقض خط‌مشی‌های ترافیکی شبکه**

فعالیت موجودیت‌هایی که روی شبکه‌های نظارت شده قرار دارند یا با آن‌ها در ارتباط هستند، به طور مؤثر مورد تجزیه و تحلیل قرار گیرد تا هرگونه نقض خط‌مشـی در اسـتفاده از شـبکه، شـناسـایی شود. هدف ارزیابی بتواند داده‌های جمع آوری شده از شبکه‌های مورد نظارت را به طور مؤثر تجزیه و تحلیل کند تا خطر افشـای ناخواسـته اطلاعات، دسـترسی غیرمجاز به سرویس‌ها و سوء استفاده از منابع شبکه، کاهش یابد.

(O.IPSANALYZE -> IPS_NTA_EXT.۱, IPS_IPB_EXT.۱, IPS_SBD_EXT.۱, IPS_ABD_EXT.۱

- **واکنش به نقض خط‌مشی‌های ترافیک شبکه**

هدف ارزیابی بتواند به صـورت بلادرنگ و طبق پیکربندی سـرپرسـت IPS ، واکنش مناسـب نشـان داده و جریان ترافیک مغایر با خط‌مشی‌های تعریف شده توسط سرپرست تشخیص را متوقف/ قطع کند.

(O.IPSREACT -> IPS_ABD_EXT.۱,۳, IPS_SBD_EXT.۱,۵)

- **سرپرستی هدف ارزیابی**

برای رفع مشـکلات موجود در ابزارهای مورد اعتماد سـرپرسـتی سـیسـتم IPS ، این هدف امنیتی که در پروفایل حفاظتی تجهیزات شبکه تشریح شد، به شرح زیر تکمیل می‌گردد.
اهداف ارزیابی انطباق پذیر، کارکرد مورد نیاز سرپرست برای تعیین خط‌مشی‌های IPS را فراهم می‌کند؛ خط‌مشی‌هایی که توسط هدف ارزیابی اجرا خواهند شد. مفروض است که حفاظت از کارکردهایی که در زیر نشان داده شده‌اند، در تطابق با الزامات پروفایل حفاظتی تجهیزات شبکه صورت می‌گیرد.

(O.TOE_ADMINISTRATION -> FMT_SMF.۱(۲))

۲.٤ اهداف امنیتی برای محیط عملیاتی

محیط عملیاتی هدف ارزیابی، با پیاده‌سـازی اقدامات فنی و رویه‌ای به هدف ارزیابی در ارائه عملکرد امنیتی آن کمک می‌نماید. این بخش شامل مجموعه‌ای از بیانیه‌ها است که اهدافی که محیط عملیاتی انجام دهد را توصیف می‌نماید

هدف امنیتی	توصیف
OE.CONNECTIONS	سرپرستان هدف ارزیابی اطمینان خواهند داد که هدف ارزیابی به صورتی نصب می‌گردد که اجازه خواهد داد خط مشی‌های هدف ارزیابی بر روی جریان ترافیک شبکه در میان شبکه‌های متصل شده، اجرا گردد.

OE.NO_GENERAL_PURPOSE	به غیر از سرویس‌های لازم برای عملیات، سرپرستی و پشتیبانی هدف ارزیابی، هیچ قابلیت محاسباتی همه منظوره (همانند کامپایلرها یا برنامه‌های کاربردی) که بر روی هدف ارزیابی در دسترس باشند، وجود ندارد.
OE.PHYSICAL	امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌های آن، توسط محیط ارائه می‌شود و در محیط فیزیکی امن تنها افراد مجاز قادرند به هدف ارزیابی دسترسی داشته باشند
OE.TRUSTED_ADMIN	سرپرستان هدف ارزیابی جهت دنبال کردن و به کاربردن مطمئن تمام راهنماهای سرپرستی، قابل اعتماد هستند.

۳.٤ مانیتور کردن سیستم

برای نظارت سرپرست سیستم بر عملیات کارکرد هدف ارزیابی، این هدف امنیتی، به شرح زیر تکمیل می‌گردد.

برای این که بتوان نقض خط‌مشی‌ها در شبکه را تحلیل کرد و به آن‌ها واکنش نشان داد، هدف ارزیابی باید بتواند عناصر داده‌های ضروری ترافیک را در شبکه‌های مورد نظارت، جمع‌آوری و ذخیره نماید.

(O.SYSTEM_MONITORING -> FAU_GEN.۱(۲), IPS_NTA_EXT.۱, IPS_IPB_EXT.۱, IPS_SBD_EXT.۱, IPS_ABD_EXT.۱)

٤.٤ تحلیل نقض خط‌مشی‌های ترافیکی شبکه

فعالیت موجودیت‌هایی که روی شبکه‌های نظارت شده قرار دارند یا با آن‌ها در ارتباط هستند، باید به طور مؤثر مورد تجزیه و تحلیل قرار گیرد تا هرگونه نقض خط‌مشی در استفاده از شبکه، شناسایی شود. هدف ارزیابی می‌تواند داده‌های جمع آوری شده از شبکه‌های مورد نظارت را به طور مؤثر تجزیه و تحلیل کند تا خطر افشای ناخواسته اطلاعات، دسترسی غیرمجاز به سرویس‌ها و سوء استفاده از منابع شبکه، کاهش یابد.

(O.IPSANALYZE -> IPS_NTA_EXT.۱, IPS_IPB_EXT.۱, IPS_SBD_EXT.۱, IPS_ABD_EXT.۱)

۵.٤ واکنش به نقض خط‌مشی‌های ترافیک شبکه

هدف ارزیابی می‌تواند به صورت بلادرنگ و طبق پیکربندی سرپرست هدف ارزیابی، واکنش مناسب نشان داده و جریان ترافیک مغایر با خط‌مشی‌های تعریف شده توسط سرپرست را متوقف/ قطع کند.

(O.IPSREACT -> IPS_ABD_EXT.۱,۳, IPS_SBD_EXT.۱,۵)

٦.٤ سرپرستی هدف ارزیابی

برای رفع مشکلات موجود در ابزارهای مورد اعتماد سرپرستی هدف ارزیابی، این هدف امنیتی به شرح زیر تکمیل می‌گردد.

اهداف ارزیابی انطباق‌پذیر، کارکرد مورد نیاز سرپرست برای تعیین خط‌مشی‌های هدف ارزیابی را فراهم می‌کند؛ خط‌مشی‌هایی که توسط هدف ارزیابی اجرا خواهند شد. مفروض است که حفاظت از کارکردهایی که در زیر نشان داده شده اند، در تطابق با الزامات پروفایل حفاظتی تجهیزات شبکه صورت می‌گیرد.

(O.TOE_ADMINISTRATION -> FMT_SMF.۱(۲))

۵ الزامات امنیتی

۱.۵ الزامات کارکرد امنیتی

با استفاده از الزامات مطرح شده در بخش دوم استاندارد ارزیابی امنیتی معیار مشترک، کارکرد امنیتی هدف ارزیابی توصیف می گردد. الزامات هر کلاس به صورت جداگانه در یک جدول آورده شده است.

در جدول زیر به طور خلاصه نام تمام کلاس‌ها، خانواده‌ها و الزامات مطرح شده در سند هدف امنیتی آورده شده است:

جدول ۵-۱ الزامات کارکرد امنیتی

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	تولید داده ممیزی ۱	FAU_GEN.۱,۱
۲	تولید داده ممیزی ۲	FAU_GEN.۱,۲
۳	تولید داده ممیزی ۳	FAU_GEN.۲,۱
۴	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.۱,۱
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.۱,۲
۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.۱,۳
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.۱,۱
۸	مدیریت کلید رمزنگاری ۲	FCS_CKM.۲,۱
۹	مدیریت کلید رمزنگاری ۴	FCS_CKM.۴,۱
۱۰	عملیات رمزنگاری ۱ (۱)	FCS_COP.۱,۱(۱)
۱۱	عملیات رمزنگاری ۱ (۲)	FCS_COP.۱,۱(۲)
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.۱,۱(۳)
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.۱,۱(۴)
۱۴	تولید بیت تصادفی ۱	FCS_RBG_EXT.۱,۱
۱۵	تولید بیت تصادفی ۲	FCS_RBG_EXT.۱,۲
۱۶	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.۱,۱
۱۷	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.۱,۲
۱۸	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.۱,۳
۱۹	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.۱,۴
۲۰	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.۱,۵
۲۱	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.۱,۶
۲۲	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.۱,۷
۲۳	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.۱,۸
۲۴	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.۱.۹
۲۵	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.۱.۱۰

شماره الزام	نام الزام	عنصر متناظر با الزام
۲۶	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.۱.۱۱
۲۷	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.۱.۱۲
۲۸	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.۱.۱۳
۲۹	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.۱.۱۴
۳۰	فیلترینگ حالتمند ۱	FFW_RUL_EXT.۱,۱
۳۱	فیلترینگ حالتمند ۲	FFW_RUL_EXT.۱,۲
۳۲	فیلترینگ حالتمند ۳	FFW_RUL_EXT.۱,۳
۳۳	فیلترینگ حالتمند ۴	FFW_RUL_EXT.۱,۴
۳۴	فیلترینگ حالتمند ۵	FFW_RUL_EXT.۱,۵
۳۵	فیلترینگ حالتمند ۶	FFW_RUL_EXT.۱,۶
۳۶	فیلترینگ حالتمند ۷	FFW_RUL_EXT.۱,۷
۳۷	فیلترینگ حالتمند ۸	FFW_RUL_EXT.۱,۸
۳۸	فیلترینگ حالتمند ۹	FFW_RUL_EXT.۱,۹
۳۹	فیلترینگ حالتمند ۱۰	FFW_RUL_EXT.۱,۱۰
۴۰	مدیریت احراز هویت ناموفق ۱	FIA_AFL.۱,۱
۴۱	مدیریت احراز هویت ناموفق ۲	FIA_AFL.۱,۲
۴۲	مدیریت رمز عبور ۱	FIA_PMG_EXT.۱,۱
۴۳	شناسایی و احراز هویت کاربر ۱	FIA_UIA_EXT.۱,۱
۴۴	شناسایی و احراز هویت کاربر ۲	FIA_UIA_EXT.۱,۲
۴۵	سازوکار احراز هویت بر اساس رمز عبور ۲	FIA_UAU_EXT.۲,۱
۴۶	احراز هویت کاربر ۱۰	FIA_UAU.۷,۱
۴۷	مدیریت کارکرد در محصول IPS۱	FMT_SMF.۱,۱
۴۸	مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن	FMT_MOF.۱,۱(۱)/TrustedUpdate
۴۹	مدیریت داده‌های محصول ۱	FMT_MTD.۱,۱
۵۰	کارکرد مدیریتی محصول ۱	FMT_SMF.۱,۱
۵۱	نقش‌های امنیتی ۳	FMT_SMR.۲,۱
۵۲	نقش‌های امنیتی ۴	FMT_SMR.۲,۲

شماره الزام	نام الزام	عنصر متناظر با الزام
۵۳	نقش‌های امنیتی ۵	FMT_SMR.۲,۳
۵۴	محافظت از داده‌های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.۱,۱
۵۵	حفاظت از گذرواژه سرپرست محصول ۱	FPT_APW_EXT.۱,۱
۵۶	حفاظت از گذرواژه سرپرست محصول ۲	FPT_APW_EXT.۱,۲
۵۷	خودآزمایی محصول ۱	FPT_TST_EXT.۱,۱
۵۸	به‌روزرسانی امن ۱	FPT_TUD_EXT.۱,۱
۵۹	به‌روزرسانی امن ۲	FPT_TUD_EXT.۱,۲
۶۰	به‌روزرسانی امن ۳	FPT_TUD_EXT.۱,۳
۶۱	مهرهای زمانی ۱	FPT_STM_EXT.۱,۱
۶۲	مهرهای زمانی ۲	FPT_STM_EXT.۱.۲
۶۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.۱,۱
۶۴	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.۳,۱
۶۵	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.۴,۱
۶۶	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.۱,۱
۶۷	کانال امن ۱	FTP_ITC.۱,۱
۶۸	کانال امن ۲	FTP_ITC.۱,۲
۶۹	کانال امن ۳	FTP_ITC.۱,۳
۷۰	مسیر امن ۱	FTP_TRP.۱,۱
۷۱	مسیر امن ۲	FTP_TRP.۱,۲
۷۲	مسیر امن ۳	FTP_TRP.۱,۳
۷۳	کارکرد IPS مبتنی بر رفتار غیرعادی ۱	IPS_ABD_EXT.۱,۱
۷۴	کارکرد IPS مبتنی بر رفتار غیرعادی ۲	IPS_ABD_EXT.۱,۲
۷۵	کارکرد IPS مبتنی بر رفتار غیرعادی ۳	IPS_ABD_EXT.۱,۳
۷۶	بلوکه کردن آدرس IP ۱	IPS_IPB_EXT.۱,۱
۷۷	بلوکه کردن آدرس IP ۲	IPS_IPB_EXT.۱,۲
۷۸	تحلیل ترافیک شبکه ۱	IPS_NTA_EXT.۱,۱
۷۹	تحلیل ترافیک شبکه ۲	IPS_NTA_EXT.۱,۲

شماره الزام	نام الزام	عنصر متناظر با الزام
۸۰	تحلیل ترافیک شبکه ۳	IPS_NTA_EXT.۱,۳
۸۱	کارکرد IPS مبتنی بر امضاء ۱	IPS_SBD_EXT.۱,۱
۸۲	کارکرد IPS مبتنی بر امضاء ۲	IPS_SBD_EXT.۱,۲
۸۳	کارکرد IPS مبتنی بر امضاء ۳	IPS_SBD_EXT.۱,۳
۸۴	کارکرد IPS مبتنی بر امضاء ۴	IPS_SBD_EXT.۱,۴
۸۵	کارکرد IPS مبتنی بر امضاء ۵	IPS_SBD_EXT.۱,۵
الزامات مربوط به پیوست دو		
۱۳۸	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.۱,۱
۱۳۹	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.۱,۲
۱۴۰	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.۱,۳
۱۴۱	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.۱,۱
۱۴۲	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.۱,۲
۱۴۳	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.۱,۳
۱۴۴	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.۱,۴
۱۴۵	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.۱,۵
۱۴۶	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.۱,۶
۱۴۷	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.۱,۷
۱۴۸	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.۱,۸
۱۴۹	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.۱,۹
۱۵۰	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.۱,۱
۱۵۱	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.۱,۲
۱۵۲	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.۱,۳
۱۵۳	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.۱,۴
۱۵۴	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.۱,۵
۱۵۵	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.۱,۶
۱۵۶	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.۱,۷

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۵۷	الزامات پروتکلSSH Server (۸)	FCS_SSHS_EXT.۱,۸
۱۵۸	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.۱,۱
۱۵۹	الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.۱,۲
۱۶۰	الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.۱,۳
۱۶۱	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.۱,۴
۱۶۷	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.۱,۱
۱۶۸	الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.۱,۲
۱۶۹	الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.۱,۳
۱۷۶	الزامات پروتکل X۵۰۹(۱)/ ابطال	FIA_X۵۰۹_EXT.۱,۱/Rev
۱۷۷	الزامات پروتکل X۵۰۹(۱)/ ابطال	FIA_X۵۰۹_EXT.۱,۲/Rev
۱۷۸	الزامات پروتکل X۵۰۹(۳)	FIA_X۵۰۹_EXT.۲,۱
۱۷۹	الزامات پروتکل X۵۰۹(۴)	FIA_X۵۰۹_EXT.۲,۲
۱۸۰	الزامات پروتکل X۵۰۹(۵)	FIA_X۵۰۹_EXT.۳,۱
۱۸۱	الزامات پروتکل X۵۰۹(۶)	FIA_X۵۰۹_EXT.۳,۲
۱۸۵	مدیریت کارکرد در محصول مورد ارزیابی /۱ به‌روزرسانی خودکار	FMT_MOF.۱,۱/AutoUpdate
۱۸۶	مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع	FMT_MOF.۱,۱/Functions

۱.۱.۵ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**
محصول مورد ارزیابی می تواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند: الف) آغاز و اتمام توابع ممیزی؛ ب) تمامی رویدادهای قابل ممیزی برای سطوح ممیزی. پ) تمام اقدامات مدیریتی شامل موارد زیر:	

شماره الزام	نام الزام
	• ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به‌حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز ثبت می شود) • تغییرات در داده‌های توابع امنیتی هدف ارزیابی مرتبط با تغییرات پیکربندی (علاوه بر اطلاعات حاکی از تغییرات رخ داده، باید تعیین شود که چه مواردی تغییر کرده‌اند) • تولید، واردکردن، تغییر یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز ثبت می شود. • تغییر گذرواژه (نام حساب کاربری مربوطه نیز باید ثبت شود) • شروع و پایان توابع IPS • همه رویدادهای متفاوت IPS • همه واکنش‌های متفاوت IPS • [آغاز و توقف سرویس‌ها، هیچ اقدام دیگر] د) تعداد رویدادهای مشابه که در واحد زمان مشخص روی داده است ه) تعداد اقدامات متقابل که در واحد زمان مشخص روی داده است. ت) دیگر رویدادهای ممیزی لیست در نکته کاربردی ۳.
۲	**تولید داده ممیزی ۲**
	محصول مورد ارزیابی در هر یک از سوابق ممیزی، دست‌کم اطلاعات زیر را ثبت می نماید: الف) تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت[۱] فعال و نتیجه رویداد (موفقیت یا شکست)؛ و ب) در مورد هر یک از انواع رویدادهای ممیزی و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در نکته کاربردی ۳ مشخص‌شده است. • با توجه به الزام «شناسایی و احرازهویت کاربر ۲» برای ثبت رکورد ممیزی علاوه بر اطلاعات بند الف این الزام باید آدرس IP منشأ احرازهویت را در رکورد ممیزی (به‌عنوان نمونه در قسمت توضیحات رکورد) ثبت نماید. • برای الزام « مدیریت احرازهویت ناموفق» اطلاعات ممیزی تلاش‌های ناموفق که از تعداد مجاز بیشتر بوده است، ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد. • برای الزام «سازوکار احرازهویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای مکانیزم تعیین هویت و احرازهویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.برای الزام «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی، دستی ثبت می‌شود. • برای الزام «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود. • برای الزامات «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود. • برای الزام «مهرهای زمانی[۲]» اطلاعات ممیزی مربوط به تغییرات صورت گرفته در زمان ثبت می‌شود. این اطلاعات باید شامل زمان‌های جدید و قدیم، منشأ تلاش (مانند آدرس IP) برای تغییر زمان موفق یا ناموفق باشد.

[۱] Subject

[۲] Time stamps

شماره الزام	نام الزام

- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها ۷» در صورت "خاتمه دادن" ، اطلاعات ممیزی مربوط به خاتمه دادن یک نشست محلی از طریق یک مکانیزم قفل‌کردن نشست ثبت می‌شود.
- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها ۵» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه‌دور از طریق یک مکانیزم قفل‌کردن نشست ثبت می‌شود.
- برای الزام « قفل‌کردن و خاتمه دادن به نشست‌ها ۶» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست تعاملی ثبت می‌شود.
- برای الزامات «کانال امن» اطلاعات ممیزی مربوط به آغاز کردن کانال امن / خاتمه دادن کانال امن / شکست توابع کانال امن ثبت می‌شود. این اطلاعات باید شامل شناسایی دلیل و هدف تلاش ناموفق برای ایجاد کانال امن باشد.
- برای الزامات «مسیر امن» اطلاعات ممیزی مربوط به آغاز کردن مسیر امن / خاتمه دادن مسیر امن / شکست توابع مسیر امن ثبت می‌شود.
- برای الزام «فایروال حالتمند» اطلاعات ممیزی برای اعمال قوانین پیکربندی‌شده با عملیات log ثبت می شود. این اطلاعات باید شامل آدرس‌های مبدأ و مقصد،پورت‌های مبدأ و مقصد، پروتکل لایه انتقال،واسط هدف ارزیابی می باشد.
- برای الزام «فایروال حالتمند» اطلاعات ممیزی برای وجود نشانه‌ای مبنی بر کنار گذاشته شدن[۱] بسته‌ها به دلیل زیاد بودن ترافیک شبکه ثبت می‌شود. این اطلاعات باید شامل واسط هدف ارزیابی که نمی‌تواند بسته‌ها را پردازش کند، شناسه قوانینی که موجب کنار گذاشته شدن بسته‌ها می‌شوند باشد.
- الزامات پروتکل IPSEC، شکست در ایجاد یک SA مربوط به پروتکل IPSEC، دلایل شکست

برای ماژول IPS لازم است هر یک از داده‌های ممیزی مطابق جدول زیر ثبت گردد.

نام الزام	رویدادهای ممیزی	اطلاعات اضافه رکوردهای ممیزی
مدیریت کارکرد محصول IPS ۱	تغییرات در المان‌های خط و مشی های IPS	شناسه‌ها یا نام المان‌های خط و مشی های IPS تغییر یافته(به عنوان نمونه کدام امضاء، مبنا، لیست–های سیاه و سفید تغییر داده شده است)
کارکرد IPS مبتنی بر رفتار غیر عادی	ترافیک بازرسی شده که با خط مشی IPS مبتنی بر رفتار غیرعادی انطباق دارد.	آدرس‌های IP مبدا و مقصد
		محتوای فیلدهای سرآیند که با خط ومشی های مشخص شده انطباق دارد.
		واسطی که از آن بسته دریافت شده است.

[۱] Drop

شماره الزام	نام الزام	
		جنبه های از خط و مشی های قوانین مبتنی بر ناهنجاری که رویداد تریگر شده است(به عنوان نمونه گذردهی،زمان روز،فرکانس و ...).
		واکنش محصول در مقابل رویداد(اجازه داده شده است، مسدود شده است، هشدار مسدود شدن به فایروال ارسال شده است)
بلوکه کردن آدرسIP ۱	انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا	آدرس‌های IP مبدأ و مقصد (و در صورت امکان، نشانه‌ای دال بر این که این آدرس‌های مبدأ و/یا مقصد منطبق با لیست هستند یا خیر)
		واسط محصول که بسته را دریافت کرده است.
		اقدامی که محصول در شبکه انجام می‌دهد (مانند اجازه دادن، مسدود کردن، ارسال دستورreset)
تحلیل ترافیک شبکه ۱	تغییر این که کدام خط‌مشی‌های پیشگیری از نفوذ روی واسط محصول فعال هستند.	شناسایی واسط محصول
	فعال کردن و غیر فعال کردن واسط محصول که خط‌مشی‌های پیشگیری از نفوذ روی آن اعمال شده‌اند.	خط‌مشی پیشگیری از نفوذ و مد واسط (در صورت امکان)
	تغییر این که کدام مُدها روی واسط محصول فعال هستند.	
کارکرد IPS مبتنی بر امضاء ۱	انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا	نام یا شناسه امضای انطباق‌داده‌شده
		آدرس‌های IP مبدأ و مقصد.
		محتوای فیلدهای سرآیند که باید با خط‌مشی انطباق داشته باشند.
		محصول که بسته را دریافت کرده است.
		اقدامی که محصول در شبکه انجام می‌دهد (مانند اجازه دادن، مسدود کردن، ارسال دستورreset)

شماره الزام	نام الزام
	رویداد ممیزی «الزامات پروتکل X۵۰۹» در صورتی رخ می‌دهد که توابع امنیتی هدف ارزیابی نتواند از موارد زیر اطمینان حاصل نماید و گواهی‌نامه‌ها را تأیید کند: • وجود افزونه basicConstraints و تأیید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است • تأیید امضای دیجیتال CA سلسله مراتبی مورد اعتماد • خواندن و دسترسی به CRL یا دسترسی به سرور OCSP اگر هر یک از این موارد وجود نداشته باشند، یک رویداد ممیزی با نتیجه شکست در سوابق ممیزی ثبت می شود.
۳	**تولید داده ممیزی ۳**
	در مورد آن دسته از رویدادهای ممیزی که حاصل اقدامات کاربران احرازهویت‌شده هستند، محصول مورد ارزیابی باید بتواند هر رویداد قابل ممیزی را با هویت کاربری که مسبب آن رویداد شده است، مرتبط سازد.
٤	**محل ذخیره‌سازی داده‌های ممیزی ۱**
	محصول باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال امن مطابق با الزام FTP_ITC.۱ باشد.
۵	**محل ذخیره‌سازی داده‌های ممیزی ۲**
	محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.
٦	**محل ذخیره‌سازی داده‌های ممیزی ۳**
	درصورتی‌که حافظه محلی محصول پرشده باشد و ظرفیتی برای ذخیره‌سازی داده‌های ممیزی نداشته باشد، محصول مورد ارزیابی باید [سوابق ممیزی گذشته را بر اساس این قوانین بازنویسی[۱] کند: [بازنویسی سوابق ممیزی گذشته در صورت اتمام حجم تعیین شده]]

۲.۱.۵ پشتیبانی رمزنگاری (FCS)

شماره الزام	نام الزام
۷	**مدیریت کلید رمزنگاری ۱**
	محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری، کلیدهای رمزنگاری نامتقارن را تولید کند: • الگوهای RSA با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB ۱۸۶-۴، استاندارد امضای دیجیتال (DSS)، پیوست B.۳؛

[۱] Overwrite

• الگوهای ECC با استفاده از «منحنی‌های NIST» » [انتخاب: P-۳۸۴, P-۵۲۱] بر اساس این الزامات: FIPS PUB ۱۸۶-۴، استاندارد امضای دیجیتال (DSS)، پیوست B.۴.	
مدیریت کلید رمزنگاری ۲	**۸**
محصول مورد ارزیابی استقرار کلید[۱] رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام می دهد: • الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: انتشار ویژه NIST ۸۰۰-۵۶B بازبینی ۱ ، « توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛ • الگوهای استقرار کلید منحنی بیضوی[۳] که این الزامات را رعایت کنند: انتشار ویژه NIST ۸۰۰-۵۶A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۴]؛ • الگوی استقرار کلید با استفاده از دیفی–هلمن گروه ۱۴ که این الزامات را رعایت کنند: RFC ۳۵۲۶، بخش۳؛	
مدیریت کلید رمزنگاری ٤	**۹**
محصول مورد ارزیابی کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: • برای کلیدهای متن–آشکار در ذخیره‌ساز فرار[۵]، نابودی باید از طریق یک [بازنویسی ساده شامل [الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی] انجام شود. • برای کلیدهای متن–آشکار در ذخیره‌ساز غیرفرار، نابودی باید از طریق فراخوان[۶] یک واسط مهیا شده توسط محصول مورد ارزیابی که [○ یک بخشی از توابع امنیتی محصول را برای نابودی انتزاع معرف کلید، می‌سازد] انجام شود.]	
عملیات رمزنگاری ۱ (۱)	**۱۰**
محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص [الگوریتم AES که در حالت [CBC، GCM] و در اندازه‌های کلید [۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] استفاده می‌شوند] و با توجه به [استاندارد AES که در ISO ۱۸۰۳۳-۳ تعریف‌شده است، [CBC که در ISO ۱۰۱۱۶ تعریف‌شده است، GCM که در ISO ۱۹۷۷۲ تعریف‌شده است]] انجام دهد.	
عملیات رمزنگاری ۱ (۲)	**۱۱**
محصول مورد ارزیابی باید سرویس‌ها امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [• الگوریتم امضای دیجیتال RSA و کلید رمزنگاری با اندازه‌های (ماژول‌ها) [۲۰۴۸ بیتی یا بزرگ‌تر]	

[۱] Key establishment

[۲] Integer factorization cryptography

[۳] Elliptic curve-based

[٤] Discrete logarithm cryptography

[٥] Volatile Storage

[٦] Invocation

[با رعایت موارد زیر:] • در مورد الگوهای RSA: FIPS PUB ۱۸۶-۴ «استاندارد امضای دیجیتال (DSS)»، بخش ۵,۵، با استفاده از الگوی امضای RSASSA-PSS نسخه ۲,۱ v۱ PKCS و/یا ۵_RSASSA-PKCS۱v۱؛ ISO/IEC ۹۷۹۶-۲، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳،	
۱۲	**عملیات رمزنگاری ۱ (۳)**
محصول مورد ارزیابی باید سرویس‌ها درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [SHA-۱، SHA-۲۵۶، SHA-۳۸۴، SHA-۵۱۲] و اندازه‌های خلاصه پیام [۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی که [ISO/IEC ۱۰۱۱۸-۳:۲۰۰۴] را رعایت کند، ارائه نماید.	
۱۳	**عملیات رمزنگاری ۱ (٤)**
محصول مورد ارزیابی باید احرازهویت پیام مبتنی بر کلید درهم‌سازی شده[۱] را بر اساس الگوریتم رمزنگاری خاص [HMAC-SHA-۱, HMAC-SHA-۲۵۶,HMAC-SHA-۳۸۴, HMAC-SHA-۵۱۲] و با استفاده از اندازه‌های کلید [۲۵۶ بیت و اندازه‌های خلاصه پیام [۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح‌شده در [بخش هفتم ISO/IEC ۹۷۹۷-۲:۲۰۱۱ با نام «الگوریتم MAC ۲»] انجام دهد.	
۱٤	**تولید بیت تصادفی ۱**
محصول مورد ارزیابی باید سرویس‌ها تولید بیت تصادفی را بر اساس ISO/IEC ۱۸۰۳۱:۲۰۱۱ و با استفاده از [Hash_DRBG، HMAC_DRBG، CTR_DRBG (AES)] ارائه دهد.	
۱۵	**تولید بیت تصادفی ۲**
RBG قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [[یک] منبع نویز مبتنی بر نرم‌افزار، [یک] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست کم [۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و CSPs که تولید می‌کند، مطابق با ISO/IEC ۱۸۰۳۱:۲۰۱۱، باشد.	

۳.۱.۵ الزامات پروتکل IPsec

شماره الزام	نام الزام
۱٦	**الزامات پروتکل IPSEC (۱)**

[۱] Keyed-hash message authentication

محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آن چه در RFC ۴۳۰۱ مشخص شده است، پیاده‌سازی کند.	
الزامات پروتکل IPSEC (۲)	**۱۷**
محصول مورد ارزیابی باید مقدار/قانون در پایگاه داده SPD، برای تمام موارد غیر منطبق داشته باشد و آن‌ها را طبق آن مقدار/قانون دور بریزد.	
الزامات پروتکل IPSEC (۳)	**۱۸**
محصول مورد ارزیابی باید [مد انتقال، مد تونل] را پیاده‌سازی کند.	
الزامات پروتکل IPSEC (٤)	**۱۹**
محصول مورد ارزیابی باید بر اساس آنچه در RFC ۴۳۰۳ گفته شده است فریمورک ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری [AES-CBC-۱۲۸ (تشریح شده در RFC ۳۶۰۲)، هیچ الگوریتم دیگری] به همراه یک HMAC مبتنی بر الگوریتم درهم‌سازی امن (SHA) [HMAC-SHA-۲۵۶، HMAC-SHA-۳۸۴، HMAC-SHA-۵۱۲، هیچ الگوریتم دیگری] و [AES-GCM-۱۲۸،AES-GCM-۱۹۲ و AES-GCM-۲۵۶ (تشریح شده در RFC ۴۱۰۶)، هیچ الگوریتم دیگری] پیاده‌سازی کند.	
الزامات پروتکل IPSEC (٥)	**۲۰**
محصول مورد ارزیابی باید یکی از این پروتکل‌ها را به کار گیرد: [• IKEv۱، با استفاده از مد اصلی[۱] برای انتقال در فاز اول، طبق آنچه که در RFC ۴۱۰۹, ۲۴۰۹, ۲۴۰۸, RFCs ۲۴۰۷، [RFC۴۳۰۴ برای اعداد متوالی بسط‌یافته] و [RFC ۴۸۶۸ برای توابع درهم‌ساز] بیان شده است. • IKEv۲، مطابق با آنچه که در RFC ۵۹۹۶ و [با پشتیبانی اجباری از پیمایش NAT چنان که در بخش ۲,۲۳ از RFC ۵۹۹۶ تشریح شده است] و [RFC ۴۸۶۸ برای توابع درهم‌ساز] تشریح شده است.].	
الزامات پروتکل IPSEC (٦)	**۲۱**
محصول مورد ارزیابی باید اطمینان حاصل کند که برای پی‌آیند (پایه‌بار)[۲] رمزگذاری‌شده در پروتکل [IKEv۱،IKEv۲]، از الگوریتم‌های رمزنگاری [AES-CBC-۱۲۸ (تشریح شده در RFC ۳۶۰۲)، AES-GCM-۱۲۸، AES-GCM-۱۹۲، AES-GCM-۲۵۶ (تشریح شده در RFC ۵۲۸۲)] استفاده می‌شود.	
الزامات پروتکل IPSEC (۷)	**۲۲**
محصول مورد ارزیابی باید اطمینان حاصل کند که [• سرپرست محصول می‌تواند طول عمر SA فاز اول IKEv۱ را بر اساس [○ مدت زمان که مقدار آن را می‌توان در بازه [۱ ۲۴] ساعت قرار داد؛] پیکربندی کند. • سرپرست محصول می‌تواند طول عمر IKEv۲ SA را بر اساس [	

[۱] Main Mode

[۲] Payload

○ مدت زمان که مقدار آن را می‌توان در بازه [۲۴ ۱] ساعت قرار داد؛] پیکربندی کند.	
۲۳	**الزامات پروتکل IPSEC (۸)**
محصول مورد ارزیابی باید اطمینان حاصل کند که [• سرپرست محصول می‌تواند طول عمر SA فاز دوم IKEv۱ را بر اساس [○ مدت زمان که مقدار آن را می‌توان در بازه [۸ ۱] ساعت قرار داد؛] پیکربندی کند. • سرپرست محصول می‌تواند طول عمر IKEv۲ Child SA را بر اساس [○ مدت زمان که مقدار آن را می‌توان در بازه [۸ ۱] ساعت قرار داد؛] پیکربندی کند.	
۲٤	**الزامات پروتکل IPSEC (۹)**
محصول باید مقدار x را که در تبادل کلید IKE DiffieHellman (x در $g^x \bmod p$) به کار می‌رود، با استفاده از تولیدکننده بیت تصادفی که در الزام «تولید بیت تصادفی ۱» مشخص شده است و دست‌کم طول آن [۲۵۶ بیت] تولید نماید.	
۲۵	**الزامات پروتکل IPSEC (۱۰)**
محصول باید نانس‌های مورداستفاده در تبادلات [IKEv۱، IKEv۲] را با طول [▪ [قدرت امنیتی مربوط به گروه Diffie-Hellman مذاکره‌شده]؛ ▪ حداقل ۱۲۸ بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی[۱] مذاکره‌شده (PRF)] تولید کند.	
۲٦	**الزامات پروتکل IPSEC (۱۱)**
محصول باید اطمینان حاصل نماید که پروتکل‌های IKE، همه گروه(های) DH [۱۴ (۲۰۴۸-bit MODP) و ۱۹ (۲۵۶-bit Random ECP)، ۲۰ (۳۸۴-bit Random ECP)، ۲۴ (۲۰۴۸-bit MODP به همراه ۲۵۶-bit POS)] را پشتیبانی می‌کنند.	
۲۷	**الزامات پروتکل IPSEC (۱۲)**
محصول باید به صورت پیش‌فرض بتواند اطمینان حاصل نماید که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [فاز ۱ IKEv۱، IKEv۲ IKE_SA] مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [فاز ۲ IKEv۱، IKEv۲ CHILD_SA] مذاکره شده است، باشد.	
۲۸	**الزامات پروتکل IPSEC (۱۳)**
محصول باید اطمینان حاصل نماید که همه پروتکل‌های IKE احرازهویت همتا را با استفاده از [RSA] که از گواهی‌های X.۵۰۹v۳ مطابق با RFC۴۹۴۵ و [کلیدهای پیش‌اشتراکی] استفاده می‌کند، انجام می‌دهند.	
۲۹	**الزامات پروتکل IPSEC (۱٤)**
محصول باید کانال امن را فقط در صورتی که شناساننده موجود در گواهی‌نامه دریافتی با شناساننده مرجع پیکربندی شده انطباق داشته باشد، برقرار نماید. شناساننده مرجع و ارائه شده از انواع زیر می‌باشند: [آدرس IP، نام متمایز شده (DN[۲])] و[نام متمایز شده کاربر، نام متمایز شده ASN.۱].	

[۱] Pseudorandom Function hash

[۲] Distinquished Name

٤.١.٥ کلاس دیواره آتش (FFW)

شماره الزام	نام الزام
۳۰	**فیلترینگ حالتمند ۱**
محصول، باید برروی بسته‌های شبکه‌ای که توسط محصول پردازش میشود، فیلترنمودن ترافیک را انجام دهد.	
۳۱	**فیلترینگ حالتمند ۲**

محصول، باید قوانین فیلترنمودن ترافیک را با استفاده از فیلدهای پروتکل شبکه زیر و واسطهای مجزا تعریف نماید:

- ICMPv۴
  - نوع
  - کد
- ICMPv۶
  - نوع
  - کد
- IPv۴
  - آدرس مبدا
  - آدرس مقصد
  - پروتکل لایه انتقال
- IPv۶
  - آدرس مبدا
  - آدرس مقصد
  - پروتکل لایه انتقال
  - [هیچ فیلد دیگری]
- TCP
  - پورت مبدا
  - پورت مقصد
- UDP

- پورت مبدا
- پورت مقصد
- و واسطه متمایز

۳۲	**فیلترینگ حالتمند ۳**

محصول، باید امکان انجام عملکردهای زیر را برای هر یک از قوانین فیلتر نمودن حالتمند شبکه فراهم آورد:

- اجازه داده (allow)
- کنار گذاشتن (drop)
- گزارش‌گیری (log)

۳۳	**فیلترینگ حالتمند ٤**

محصول، باید امکان اعمال هر یک از قوانین فیلتر نمودن حالتمند شبکه را بر روی هر یک از واسط های شبکه فراهم آورد.

۳٤	**فیلترینگ حالتمند ٥**

محصول باید:

الف) بسته‌های شبکه را بدون پردازش نمودن قوانین مربوط به فیلترنمودن حالتمند ترافیک قبول نماید، چنانچه آن بسته منطبق با نشستی شروع شده مجازی برای پروتکلهای TCP، UDP و [*ICMP، هیچ پروتکل دیگری*] و بر اساس صفات پروتکلهای شبکه ای زیر باشد:

- TCP: آدرس مبدا و مقصد، پورت‌های مبدا و مقصد، شماره توالی[۱]، پرچم‌ها
- UDP: آدرس مبدا و مقصد، پورت‌های مبدا و مقصد
- ICMP : آدرس مبدا و مقصد براساس نوع، کد

ب) جریان ترافیک موجود را از مجموعه جریان ترافیک ایجاد شده براساس مدت زمان غیرفعال بودن نشست حذف نماید.

۳۵	**فیلترینگ حالتمند ٦**

محصول، باید قوانین فیلترنمودن حالتمند شبکه زیر را به طور پیش‌فرض بر روی تمام ترافیک شبکه اعمال نماید:

۱- محصول باید بسته‌های اطلاعاتی که به صورت نامعتبر قطعه بندی شده اند را رد نماید و قادر به شمردن آنها می باشد.

۲- محصول باید بسته‌های IP قطعه بندی شده‌ای که نمی‌توانند به طور کامل مجدداً گردآوری شوند را رد نماید و قادر به [ثبت] نمودن آنها باشد.

۳- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا بسته اطلاعاتی شبکه، روی یک شبکه به صورت پخشی [۲] تعریف شده است.

[۱] Sequence number

[۲] Broadcast network

۴- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا بر روی شبکه چندپخشی[۱]تعریف شده است، محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا از بسته اطلاعاتی شبکه به صورت یک آدرس برگشتی [۲]تعریف شده باشد.

۵- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا و یا آدرس مقصد آن نامشخص باشد(به عنوان نمونه ۰،۰،۰،۰)و یا به صورت آدرس "رزرو شده برای استفاده در آینده" (به عنوان نمونه ۲۴۰،۰،۰،۰/۴) همان‌گونه که در RFC۵۷۳۵ برای IPv۴ مشخص شده، تعریف شده باشد.

۶- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا و مقصد بسته اطلاعاتی به صورت آدرس "نامشخص" یا آدرسی که"رزرو شده برای تعریف و استفاده در آینده" (به عنوان نمونه آدرس های تک پخشی که در بازه ۲۰۰۰::/۳: نیست) همان‌گونه که در RFC۳۵۱۳ برای IPv۶ مشخص شده، تعریف شده باشد.

۷- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه با گزینه های IP زیر را رد نماید و قادر به ثبت باشد:

- Loose source routing
- strict source routing
- record route specipied

۸- [*بدون هیچ قانون دیگر*]

۳۶	**فیلترینگ حالتمند ۷**

محصول، باید قادر به حذف و ثبت مطابق با قوانین زیر باشد:

۱- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدا آن با آدرس واسط شبکه‌ای که بسته‌های اطلاعاتی شبکه را دریافت نموده برابر باشد را کنار بگذارد و قادر به ثبت باشد.

۲- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدا و یا مقصد آن یک آدرس link-local است را کنار بگذارد و قادر به ثبت باشد.

۳- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدا آن متعلق به شبکه‌های مرتبط با واسط شبکه ای که آن بسته‌ها را دریافت کرده است، نباشد را کنارد بگذارد و قادر به ثبت باشد.

۳۷	**فیلترینگ حالتمند ۸**

محصول باید قادر باشد قوانین اجرایی فیلترنمودن حالتمند ترافیک را به ترتیب تعیین شده توسط سرپرست محصول، پردازش نماید.

۳۸	**فیلترینگ حالتمند ۹**

محصول باید مانع از عبور جریان بسته های شود که هیچ قانونی برای آن مشخص نشده است.

۳۹	**فیلترینگ حالتمند ۱۰**

محصول باید قادر باشد تعداد اتصالات نیمه باز TCP را مطابق با تعریف سرپرست سیستم محدود نماید. برای رویدادهای که مقدار آن به مقدار حد پیکربندی می رسد، اتصالات جدید باید حذف و رویداد حذف شده باید [ثبت] شود.

---

[۱] Multicast network

[۲] Loopback address

۵.۱.۵ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
٤٠	**مدیریت احراز هویت ناموفق ۱**
محصـول مورد ارزیابی باید وقتی که یک عدد مثبت قابل تنظیم توسط سرپرست در [بازه مقادیر صحیح مثبت کوچکتر از ۲۰]، از تلاش‌های ناموفق احرازهویت مرتبط با تلاش‌های سرپرستان برای احرازهویت راه‌دور اتفاق میافتد، را تشخیص دهد.	
٤١	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاش‌های ناموفق صـورت گرفته برای احرازهویت به حد تعیین شـده برسد، محصول مورد ارزیابی باید [سرپرست راه‌دور تخطی‌کننده را از احرازهویت موفق جلوگیری نماید تا وقتی که یک [اقدام برای مجوز دسـترسـی به آن آدرس تخطی کننده] توسـط یک سرپرست محلی صورت گیرد یا سرپرست راه‌دور تخطی‌کننده را از احرازهویت موفق جلوگیری نماید تا وقتی که یک دوره زمانی تعریف شده توسط سرپرست سپری شود.] انجام دهد.	
٤٢	**مدیریت رمز عبور ۱**
محصول مورد ارزیابی باید قابلیت‌های مدیریت گذرواژه زیر را برای کلمه‌ی عبور سرپرست اجرایی محصول فراهم آورد: الف) گذرواژه را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شـده در این بخش سـاخت: [“!”, “@”, “#”,“$”, “%”, “^”, “&”, “*”, “(“, “)”,”?”,”_”,”~”؛] ب) حداقل طول گذرواژه باید قابل پیکربندی به [۱] و [بدون محدودیت] باشد.	
٤٣	**شناسایی و احراز هویت کاربر ۱**
محصول مورد ارزیابی پیش از آن که از دیگر موجودیت‌های خارج از محصول بخواهد که فرایند تعیین و احرازهویت را انجام دهد، باید اجازه انجام فعالیت‌های زیر را بدهد: • نمایش بنر اخطار با توجه به الزام FTA_TAB.۱ • [هیچ اقدامی]	
٤٤	**شناسایی و احراز هویت کاربر ۲**
پیش از آن که محصول مورد ارزیابی امکان انجام اقدامات مدیریتی سیستم را فراهم آورد، باید هر مدیرسیستم را ملزم نماید که به صورت موفق شناسایی و احرازهویت گردد.	
٤٥	**سازوکار احراز هویت بر اساس رمزعبور ۲**
محصـــول مورد ارزیـابی باید یک مکانیزم محلی احرازهویت مبتنی بر گذرواژه و [هیچ مکانیزم دیگری] را برای احرازهویت کاربر محلی مدیر سیستم فراهم آورد.	
٤٦	**احراز هویت کاربر ۱۰**

هنگامی که فرایند احرازهویت بر روی کنسول محلی در حال جریان است، محصول مورد ارزیابی تنها باید بازخورد مبهم[۱] را در اختیار سرپرست محصول قرار دهد.

٦.١.٥ کلاس مدیریت امنیت

شماره الزام	نام الزام
٤٧	**مدیریت کارکرد در محصول IPS ۱**
محصول مورد ارزیابی باید قادر به انجام توابع مدیریتی زیر باشد: ۱) فعال‌سازی، غیرفعال‌سازی امضاهایی که در واسطهای حسگر به کار می‌روند، و تعیین رفتار کارکرد IPS ۲) تغییر و اصلاح این پارامترهایی که جمع‌آوری و تحلیل ترافیک شبکه را تعیین می‌کنند: الف) آدرس‌های IP مبدأ (آدرس میزبان و آدرس شبکه) ب)آدرس‌های IP مقصد (آدرس میزبان و آدرس شبکه) پ) پورت مبدأ (TCP و UDP) ت) پورت مقصد (TCP و UDP) ث) پروتکل (IPv۴ و IPv۶) ج) کد و نوع ICMP ۳) به‌روزرسانی (وارد کردن) امضاها ۴) ایجاد امضاهای خاص ۵) پیکربندی کشف رفتارهای غیرعادی ۶) فعال‌سازی و غیرفعال‌سازی اقدامات هنگامی که امضا یا رفتارهای غیرعادی مورد شناسایی قرار می‌گیرند. ۷) تغییر آستانه‌هایی که واکنش‌های IPS را هدف می‌گیرند. ۸) تغییر مدت زمان بلوکه کردن ترافیک ۹) تغییر لیست سیاه و لیست سفید (از آدرس‌های IP و بازه آدرس‌ها) ۱۰) پیکربندی لیست سیاه و لیست سفید برای نادیده گرفتن خطمشی‌های IPS مبتنی بر امضا	
٤٨	**مدیریت کارکرد در محصول ۱ (۱)/ به روزرسانی امن**
محصول مورد ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست‌های امنیتی محدود نماید.	
٤٩	**مدیریت داده های محصول ۱**

[۱] Obscured feedback

محصول مورد ارزیابی باید امکان «مدیریت» داده‌های توابع امنیتی محصول را به سرپرست‌های امنیتی محدود کند.	
۵۰	**کارکرد مدیریتی محصول ۱**
محصول مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد: • [اداره کردن محصول به‌صورت محلی و راه‌دور • پیکربندی بنر دسترسی • پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن • به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از [مقایسه درهم‌سازی] پیش از نصب شدن این به‌روزرسانی‌ها • پیکربندی پارامترهای شکست احرازهویت برای الزام FIA_AFL.۱ • [پیکربندی رفتار ممیزی • پیکربندی کارکرد رمزنگاری • پیکربندی طول عمر برای IPSec SAs • فعال‌سازی مجدد حساب سرپرست • تنظیم زمان برای مهرهای زمانی • پیکربندی شناساننده مرجع برای همتا • هیچ قابلیت دیگری]]	
۵۱	**نقش‌های امنیتی ۳**
محصول باید نقش‌های زیر را نگهداری کند. • سرپرست امنیتی	
۵۲	**نقش‌های امنیتی ٤**
محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.	
۵۳	**نقش‌های امنیتی ۵**
محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند: • نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را به صورت محلی اداره کند. • نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را از راه‌دور اداره کند.	

۷.۱.۵ کلاس حفاظت از محصول

شماره الزام	نام الزام
٥٤	**محافظت از داده‌های محصول (کلیدهای متقارن) ۱**

توابع امنیتی هدف ارزیابی از خواندن تمام کلیدهایی که از پیش به اشتراک گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد. (به غیر از خود سیستم هیچ کاربری اجازه دسترسی به آن ها را نداشته باشد و کلیدها به صورت درهم سازی رمزشده و ذخیره می شوند.)	
۵۵	**حفاظت از کلمه عبور سرپرست محصول ۱**
توابع امنیتی هدف ارزیابی نباید کلمه های عبور را به شکل متن ساده ذخیره کند.(کلمه های عبور به صورت درهم سازی ذخیره می شوند.)	
۵۶	**حفاظت از کلمه عبور سرپرست محصول ۲**
توابع امنیتی هدف ارزیابی از خوانده شدن کلمه‌های عبوری که به‌صورت متن ساده[1] هستند، جلوگیری کند.	

۱.۷.۱.۵ تست محصول مورد ارزیابی

شماره الزام	نام الزام
۵۷	**خودآزمایی محصول ۱**
محصول مورد ارزیابی باید مجموعه‌ای از این خودآزمایی‌ها را [در مرحله راه‌اندازی اولیه (روشن شدن دستگاه)] برای نشان دادن کارکرد صحیح محصول مورد ارزیابی انجام دهد: [بررسی صحت چکسام کد در راه اندازی، بررسی وضعیت سرویس ها و فایروال در هنگام اجرا به طور خودکار و به درخواست کاربر، بررسی وضعیت دیسک سخت به درخواست کاربر].	

۲.۷.۱.۵ به‌روزرسانی امن

شماره الزام	نام الزام
۵۸	**به روز رسانی امن ۱**
محصول مورد ارزیابی باید این امکان را به سرپرستان امنیتی محصول بدهد که به نسخه فعلی نرم‌افزار/میان‌افزار محصول و [هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول] دسترسی داشته باشد.	
۵۹	**به روز رسانی امن ۲**
محصول مورد ارزیابی باید این امکان را برای سرپرستان امنیتی محصول فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار محصول مورد ارزیابی را به صورت دستی انجام دهد و [از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند].	

[1] Plaintext

٦٠	**به روز رسانی امن ۳**
محصـول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [درهم‌ساز منتشرشده]، ابزاری را برای احرازهویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.	
٦١	**مهرهای زمانی ۱**
محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان[۱] برای استفاده خودش، را داشته باشد.	
٦٢	**مهرهای زمانی ۲**
محصول باید [به سرپرست امنیتی اجازه دهد که زمان را تنظیم نماید، زمان را با منابع خارجی زمان همگام سازد].	

۸.۱.۵ دسترسی به محصول

شماره الزام	نام الزام
٦٣	**قفل‌کردن و خاتمه دادن به نشست ها ۷**
در مورد نشـسـت‌های تعاملی محلی[۲]، محصول مورد ارزیابی باید پس از اتمام زمان غیر فعال بودن که توسط سرپرست محصول تعیین شده است، [نشست را خاتمه دهد].	
٦٤	**قفل‌کردن و خاتمه دادن به نشست ها ۵**
در مورد نشـسـت‌های تعاملی راه‌دور[۳]، درصـورتی که نشـست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود.	
٦٥	**قفل‌کردن و خاتمه دادن به نشست ها ٦**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
٦٦	**پیغام های هشدار در رابطه با استفاده محصول ۱**
قبل از ایجاد یک نشست کاربری سرپرست اجرایی[۴]، محصول مورد ارزیابی باید توصیه‌های مشخص شده توسط سرپرست امنیتی و همچنین تاییدیه استفاده از محصول مورد ارزیابی را نشان دهد.	

[۱] Reliable time stamps

[۲] Local interactive sessions

[۳] Remote

[۴] Administrative user

۹.۱.۵ کلاس کانال‌ها/مسیرهای مورد اعتماد

شماره الزام	نام الزام
٦٧	**کانال امن ۱**
محصـول، باید مسـیر ارتباطی امنی را با اسـتفاده از پروتکل [IPsec, TLS] میان خود و دیگر موجودیت‌های IT معتبر همچون سـرور ممیزی، [سـرور احرازهویت، [سرور NTP]، هیچ قابلیت‌های دیگری] که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
٦٨	**کانال امن ۲**
محصـول مورد ارزیابی باید اجازه داشـته باشـد یا به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
٦٩	**کانال امن ۳**
محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [NTP ، SYSlog-ng، Radius] راه‌اندازی نماید.	
۷۰	**مسیر امن ۱**
محصـول، باید با اسـتفاده از پروتکل [SSH, HTTPS] مسیر ارتباطی امنی را میان خود و سرپرست‌های راه‌دور مجاز که به طور منطقی از مسـیرهای ارتباطی دیگر متمایز است را فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات در داده کانال را تشخیص دهد.	
۷۱	**مسیر امن ۲**
محصول مورد ارزیابی باید به سرپرست‌های راه‌دور محصول اجازه دهد که ارتباطات را از طریق کانال امن آغاز کند.	
۷۲	**مسیر امن ۳**
محصـول مورد ارزیابی باید استفاده از کانال امن را برای احرازهویت اولیه سرپرست محصول و تمام فعالیت‌های راه‌دور سرپرستی الزامی کند	

۱۰.۱.۵ کلاس IPS: جلوگیری از نفوذ

شماره الزام	نام الزام
۷۳	**کارکرد IPS مبتنی بر رفتار غیرعادی ۱**
محصول باید از تعریف مبنا (مورد انتظار و تأییدشده) پشتیبانی کند و شامل مشخصات زیر باشد: [	

- تناوب
- آستانه‌ها
- و هیچ روش دیگر]

و فیلدهای پروتکل شبکه زیر:

تمامی سرآیند بسته و عناصر داده‌ها که در الزام « کارکرد IPS مبتنی بر امضاء» تعریف شده‌اند؛

- IPv۴: نسخه، طول سرآیند، طول بسته، پرچم IP، ID، آفست تکه ، زمان فعالیت (TTL)، پروتکل، سرآیند چک‌سام، آدرس مبدأ، آدرس مقصد، گزینه‌های IP.
- IPv۶: نسخه ، برچسب جریان، طول محتوا، سرآیند بعدی، محدودیت گام، آدرس مبدأ، آدرس مقصد، سرآیند مسیریاب، گزینه‌های آدرس مبدأ.
- ICMP: نوع، کد، چک‌سام سرآیند،ID، شماره توالی
- ICMPv۶: نوع، کد، و چک‌سام سرآیند
- TCP: پورت مبدأ، پورت مقصد، عدد توالی، عدد تصدیق، آفست، رزرو، پرچم‌های TCP، پنجره، چک‌سام، نشانگر اضطراری، و گزینه‌های TCP
- UDP: پورت مبدأ، پورت مقصد، طول، و چک‌سام UDP

۷٤	**کارکرد IPS مبتنی بر رفتار غیرعادی ۲**

محصول باید از تعریف فعالیت غیرعادی از طریق: [پیکربندی دستی توسط سرپرست] پشتیبانی نماید.

۷۵	**کارکرد IPS مبتنی بر رفتار غیرعادی ۳**

محصول باید به عملیات‌های زیر اجازه دهد که با خط‌مشی‌های مبتنی بر رفتارهای غیرعادی ترکیب شوند.

- در هر حالتی، برای هر واسط حسگری: [
  - اجازه به جریان ترافیک
  - ارسال یک پیام غیرقابل دسترسی ICMP [میزبان]]
- در حالت درون خطی:
  - اجازه به جریان ترافیک
  - بلوکه کردن/ قطع جریان ترافیک

و [بدون هیچ اقدام دیگر]

۷٦	**بلوکه کردن آدرس IP ۱**

محصول باید از پیکربندی و پیاده‌سازی لیست سیاه و لیست سفید از آدرس‌های IP [آدرس مبدأ، آدرس مقصد] پشتیبانی نماید.

۷۷	**بلوکه کردن آدرس IP ۲**

محصول باید به سرپرست IPS و [هیچ نقش دیگر [الزام: نقش‌های دیگر]] اجازه دهد که عناصر خط‌مشی IPS را پیکربندی نماید (قوانین لیست سیاه، قوانین لیست سفید، آدرس‌های IP).

۷۸	تحلیل ترافیک شبکه ۱

محصول باید ترافیک شبکه مبتنی بر IP را که به واسطهای سنسور محصول جریان دارد، مورد تجزیه و تحلیل قرار دهد و نقض خط‌مشی‌هایی که توسط سرپرست تعریف شده را شناسایی نماید.

۷۹	تحلیل ترافیک شبکه ۲

محصول باید پروتکل‌های ترافیک شبکه زیر را پردازش کند (بتواند بازرسی کند):

- پروتکل اینترنت (IPv۴)، RFC ۷۹۱
- پروتکل اینترنت نسخه ۶ (IPv۶)، RFC ۲۴۶۰
- پروتکل پیام کنترل اینترنت نسخه ۴ (ICMPv۴)، RFC ۷۹۲
- پروتکل پیام کنترل اینترنت نسخه ۶ (ICMPv۶)، RFC ۲۴۶۳
- پروتکل کنترل انتقال (TCP)، RFC ۷۹۳
- پروتکل داده‌های کاربر (UDP)، RFC ۷۶۸

۸۰	تحلیل ترافیک شبکه ۳

محصول باید برای واسطهای حسگر پیکربندی شده در حالت‌های بی‌قاعده[۱] و درون خط امضاهایی را تخصیص دهد و از طراحی یک یا چند واسط به عنوان مدیریت ارتباطات بین محصول و موجودیت‌های خارجی پشتیبانی کند بدون این‌که به طور همزمان واسطهای حسگر باشند.

- حالت بی‌قاعده (فقط شنود): [اترنت ، فیبر] ،
- حالت درون‌خط (داده‌های عبوری): [اترنت ، فیبر] ،
- حالت مدیریت: [اترنت ، فیبر] ،
- [و هیچ نوع دیگری از انواع واسط] .

۸۱	کارکرد IPS مبتنی بر امضاء ۱

محصول باید از بازرسی محتوای سرآیند بسته‌ها پشتیبانی نماید و بتواند حداقل سرآیند فیلدهای زیر را بازرسی نماید:

- IPv۴: نسخه، طول سرآیند، طول بسته، پرچم IP، ID، آفست تکه ، زمان فعالیت (TTL) ، پروتکل، سرآیند چک‌سام، آدرس مبدأ، آدرس مقصد، گزینه‌های IP، و]هیچ فیلد دیگری [.
- IPv۶: نسخه، طول محتوا، سرآیند بعدی، محدودیت گام، آدرس مبدأ، آدرس مقصد، سرآیند مسیریاب، و] هیچ فیلد دیگری .[
- ICMP: نوع، کد، چک‌سام سرآیند،ID ، شماره توالی
- ICMPv۶: نوع، کد، و چک‌سام سرآیند
- TCP: پورت مبدأ، پورت مقصد، عدد توالی، عدد تصدیق، آفست، رزرو، پرچم‌های TCP، پنجره، چک‌سام، نشانگر اضطراری، و گزینه‌های TCP

[۱] Promiscuous

- UDP: پورت مبدأ، پورت مقصد، طول، و چک‌سام

۸۲	کارکرد IPS مبتنی بر امضاء ۲

محصـول باید از بازرسی محتوای سرآیند بسته‌های پشتیبانی کند و قادر باشد حداقل فیلدهای سرآیند زیر را بازرسی کند تا فرایند تطابق الگوهای مبتنی بر رشته‌های داده را اجرا کند:

- داده‌های ICMPv۴: کاراکترهایی بیشتر از ۴ بیت اول از سرآیند ICMP
- داده‌های ICMPv۶: کاراکترهایی بیشتر از ۴ بیت اول از سرآیند ICMP
- داده‌های TCP (کاراکترهایی بیشتر از ۲۰ بیت سرآیند TCP)، با پشتیبانی برای شناسایی:
  - دستورات FTP (انتقال فایل): help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, type.
  - دستورات و محتوای HTTP (وب): دستوراتی شامل GET و POST، و رشته‌های تعیین‌شده توسط سرپرست مطابق با URL/URI ها، و محتوای صفحه وب.
  - وضعیت SMTP (ایمیل): شروع وضعیت، وضعیت دستورات SMTP، وضعیت سرآیند mail، وضعیت بدنه mail، وضعیت قطع فرایند.
- داده UDP: کاراکترهایی بیشتر از هشت بیت اول سرآیند UDP
  - وضعیت DNS (سیستم نام دامنه)
  - وضعیت SNMP (پروتکل مدیریت شبکه)

علاوه بر این، توابع امنیتی محصـول باید از بازترکیب اسـتریم پشتیبانی کند و قادر به شناسایی محتوای مخرب باشد، حتی اگر در چند بسته‌ی مختلف تقسیم شده باشد.

۸۳	کارکرد IPS مبتنی بر امضاء ۳

محصـول باید قادر به کشـف امضـاهای مبتنی بر سـرآیند (با اسـتفاده از فیلدهای مشخص شده در IPS_SBD_EXT.۱،۱) در واسطهای حسگر IPS باشد.

- حملات IP
  - هم‌پوشانی تکه‌های IP (حمله Teardrop، حمله Bonk و یا حمله Boink)
  - یکسان بودن آدرس IP مبداء با آدرس IP مقصد
- حملات ICMP
  - ترافیک تکه‌ای ICMP (برای مثال حمله Nuke)
  - ترافیک حجیم ICMP (حمله Ping of Death)
- حملات TCP
  - TCP NULL flags
  - TCP SYN+FIN flags
  - TCP FIN only flags
  - TCP SYN+RST flags
- حملات UDP

○ حمله UDP Bomb ○ حمله UDP Chargen DoS	
کارکرد IPS مبتنی بر امضاء ٤	**٨٤**
توابع امنیتی محصـول می تواند تمامی امضاهای کشف الگوی ترافیکی زیر را شناسایی کند و این امضاها را در واسط حسگر IPS به کار گیرد: • سیل‌آسا به میزبان (حمله DoS) o سیل‌آسا ICMP (حمله Smurf، سیل آسا ping) o سیل‌آسا TCP (مثل سیل آسا SYN) • سیل‌آسا به شبکه (حمله DoS) • اسکن پورت و پروتکل ○ اسکن پروتکل IP ○ اسکن پورت TCP ○ اسکن پورت UDP ○ اسکن ICMP	
کارکرد IPS مبتنی بر امضاء ٥	**٨٥**
توابع امنیتی هدف ارزیابی به عملیات زیر اجازه می‌دهد تا با خط‌مشی‌های IPS مبتنی بر امضا، ترکیب شوند: • در هر حالتی، برای هر واسط حسگر: ○ اجازه به جریان ترافیک ○ ارسال پیام غیرقابل دسترسی ICMP میزبان تنها برای پروتکل TCP و UDP • حالت بر خط ○ اجازه به جریان ترافیک ○ بلوکه کردن/ قطع جریان ترافیک ○ بدون هیچ اقدام دیگری	

۱۱.۱.۵ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۱۳۸	**الزامات پروتکل HTTPS (۱)**
محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC ۲۸۱۸ اجرا کنند.	
۱۳۹	**الزامات پروتکل HTTPS (۲)**
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۱٤۰	**الزامات پروتکل HTTPS (۳)**
درصورتی‌که گواهی‌نامه همتا ارائه شده باشد و نامعتبر باشد، محصول مورد ارزیابی باید [اتصال را برقرار نکند یا برای برقراری اتصال درخواست مجوز کند].	

۱۲.۱.۵ الزامات پروتکل SSH Client

شماره الزام	نام الزام
۱٤۱	**الزامات پروتکل SSH Client (۱)**
محصول باید پروتکل SSH را مطابق با RFC های [۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۴۷، ۵۶۵۶، ۶۶۶۸، هیچ RFC دیگری] پیاده‌سازی کند.	
۱٤۲	**الزامات پروتکل SSH Client (۲)**
محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه در RFC ۴۲۵۲ توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [احراز هویت مبتنی بر گذرواژه، هیچ روش دیگری].	
۱٤۳	**الزامات پروتکل SSH Client (۳)**
همان‌طور که در RFC ۴۲۵۳ توضیح داده‌شده است، محصول باید اطمینان حاصل کند که بسته‌های دارای بایت‌های بیشتر از [۳۲۷۶۸ بایت] در یک ارتباطات انتقال SSH، کنار گذاشته شوند.	
۱٤٤	**الزامات پروتکل SSH Client (٤)**
محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [AES۱۲۸-CBC، AES-۲۵۶-CBC، AES۱۲۸-CTR، AES۲۵۶-CTR] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
۱٤٥	**الزامات پروتکل SSH Client (٥)**
محصول باید اطمینان حاصل کند که پیاده‌سازی پروتکل انتقال SSH، از [ssh-rsa, ecdsa-sha۲-nistp۲۵۶] و [ecdsa-sha۲-nistp۳۸۴، ecdsa-sha۲-nistp۵۲۱، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد کند.	
۱٤٦	**الزامات پروتکل SSH Client (٦)**

محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH، از [hmac-sha۱، hmac-sha۱-۹۶، hmac-sha۲-۲۵۶، hmac-sha۲-۵۱۲] و [هیچ الگوریتم MAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
الزامات پروتکل SSH Client (۷)	**۱۴۷**
محصول باید اطمینان حاصل کند که [diffie-hellman-group۱۴-sha۱، ecdh-sha۲-nistp۲۵۶] و [ecdh-sha۲-nistp۳۸۴، ecdh-sha۲-nistp۵۲۱، هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
الزامات پروتکل SSH Client (۸)	**۱۴۸**
محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه؛ طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد.	
الزامات پروتکل SSH Client (۹)	**۱۴۹**
محصول باید اطمینان حاصل کند که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن یا [هیچ روش دیگری] (تشریح شده در RFC ۴۲۵۱ بخش ۴,۱) همراه می‌کند، استفاده می‌کند.	

۱۳.۱.۵

۱۴.۱.۵ الزامات پروتکل SSH Server

شماره الزام	نام الزام
۱۵۰	**الزامات پروتکل SSH Server (۱)**
محصول باید پروتکل SSH را مطابق با RFC های [۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۴۷، ۵۶۵۶، ۶۶۶۸، هیچ RFC دیگری] پیاده‌سازی کند.	
۱۵۱	**الزامات پروتکل SSH Server (۲)**
محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC ۴۲۵۲ توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر گذرواژه.	
۱۵۲	**الزامات پروتکل SSH Server (۳)**
همان‌طور که در RFC ۴۲۵۳ توضیح داده‌شده است، محصول باید اطمینان حاصل کند که بسته‌های دارای بایت‌های بیشتر از [۳۲۷۶۸ بایت] در یک ارتباطات انتقال SSH، کنار گذاشته شوند.	
۱۵۳	**الزامات پروتکل SSH Server (٤)**
محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [AES۱۲۸-CBC، AES-۲۵۶-CBC، AES۱۲۸-CTR، AES۲۵۶-CTR] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	

۱۵٤	**الزامات پروتکل SSH Server (۵)**
محصـــول باید اطمینان حاصـــل کند که پیاده‌ســـازی پروتکل انتقال SSH، از [ssh-rsa, RSA-SHA۲-۲۵۶, RSA-SHA۲-۵۱۲] و [هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم(های) کلید عمومی خود اسـتفاده کند و همه الگوریتم‌های دیگر را رد کند.	
۱۵۵	**الزامات پروتکل SSH Server (٦)**
محصـول باید اطمینان حاصـل کند که در پیاده‌سـازی پروتکل انتقال SSH، از [hmac-sha۱، hmac-sha۱-۹۶، hmac-sha۲-۲۵۶، hmac-sha۲-۵۱۲] و [هیچ الگوریتم MAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
۱۵٦	**الزامات پروتکل SSH Server (۷)**
محصول باید اطمینان حاصل کند که [diffie-hellman-group۱۴-sha۱، ecdh-sha۲-nistp۲۵۶] و [ecdh-sha۲-nistp۳۸۴، ecdh-sha۲-nistp۵۲۱، هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۱۵۷	**الزامات پروتکل SSH Server (۸)**
محصـول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشـسـت یکسانی برای حد آستانه؛ طول نشست بیشتر از یک سـاعت نباشـد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد.	

۱۵.۱.۵ الزامات پروتکل TLS Client/ احراز هویت

شماره الزام	نام الزام
۱۵۸	**الزامات پروتکل TLS Client (۱)**
توابع امنیتی هدف ارزیابی [TLS ۱،۲ (RFC ۵۲۴۶) ، TLS ۱،۱ (RFC ۴۳۴۶)] با پشـتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: ○ TLS_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲۶۸ • مجموعه‌های رمز اختیاری: ○ TLS_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۳۲۶۸ ○ TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHAمطابق با RFC ۳۲۶۸	

○ TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۳۲۶۸	
○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۴۴۹۲	
○ TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۴۴۹۲	
○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۴۴۹۲	
○ TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۴۴۹۲	
○ TLS_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶ مطابق با RFC ۵۲۴۶	
○ TLS_RSA_WITH_AES_۲۵۶_CBC_ SHA۲۵۶ مطابق با RFC ۵۲۴۶	
○ TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_ SHA۲۵۶ مطابق با RFC ۵۲۴۶	
○ TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_ SHA۲۵۶ مطابق با RFC ۵۲۴۶	
○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
○ TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA۳۸۴ مطابق با RFC ۵۲۸۹	
○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
○ TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹	
○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
○ TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹	
۱۵۹	**الزامات پروتکل TLS Client (۲)**
محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC ۶۱۲۵، تائید کند.	
۱۶۰	**الزامات پروتکل TLS Client (۳)**
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [ارتباط را برقرار نسازد] .	
۱۶۱	**الزامات پروتکل TLS Client (٤)**
محصول باید [انتخاب ، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp۲۵۶r۱, secp۳۸۴r۱, secp۵۲۱r۱]]و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.	

شماره الزام	نام الزام

۱۶.۱.۵ الزامات پروتکل TLS Server

شماره الزام	نام الزام
۱۶۷	**الزامات پروتکل TLS Server (۱)**
محصول باید [(RFC ۵۲۴۶) TLS ۱،۲، (RFC ۴۳۴۶) TLS ۱.۱] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:	

• مجموعه‌های رمز اجباری: • TLS_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲۶۸ • مجموعه‌های رمز اختیاری: o TLS_RSA_WITH_AES_۲۵۶_CBC_SHAمطابق با RFC ۳۲۶۸ o TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHAمطابق با RFC ۳۲۶۸ o TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHAمطابق با RFC ۳۲۶۸ o TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHAمطابق با RFC ۴۴۹۲ o TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHAمطابق با RFC ۴۴۹۲ o TLS_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶مطابق با RFC ۵۲۴۶ o TLS_RSA_WITH_AES_۲۵۶_CBC_ SHA۲۵۶مطابق با RFC ۵۲۴۶ o TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶مطابق با RFC ۵۲۸۹ o TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹ o TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴مطابق با RFC ۵۲۸۹	
۱۶۸	**الزامات پروتکل TLS Server (۲)**
محصول باید برای کلاینت‌های دارای درخواست SSL ۲،۰، SSL ۳،۰، TLS ۱،۰ [هیچ موردی]، ارتباطات را ایجاد نکند.	
۱۶۹	**الزامات پروتکل TLS Server (۳)**
محصـول باید [اسـتقرار کلید مبتنی بر RSA را با اندازه کلید [۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] اجرا کند؛ پارامترهای EC–دیفی‌هلمن را بـه همراه منحنی‌هـای NIST[ ]secp۳۸۴r۱ و هیچ منحنی دیگری، تولیـد کند؛ پارامترهای دیفی‌هلمن را با اندازه [۳۰۷۲ بیت] تولید کند].	

۱۷.۱.۵ الزامات شناسایی و احراز هویت

شماره الزام	نام الزام
۱۷۶	**الزامات پروتکل X۵۰۹ (۱)/ ابطال**
محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند: • تائید گواهی‌نامه RFC ۵۲۸۰ و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل کند که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است	

• محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC ۵۲۸۰ بخش ۶،۳ لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC ۵۷۵۹ بخش ۵، هیچ روش فسخ] تائید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند: ○ گواهی‌نامه‌های مورداستفاده برای تائید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (id-kp ۳ با OID ۱،۳،۶،۱،۵،۵،۷،۳،۳) را در فیلد extendedKeyUsage خود داشته باشند ○ گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف «Server Authentication» (id-kp۱ با OID ۱،۳،۶،۱،۵،۵،۷،۳،۱) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف «Client Authentication» (id-kp۱ با OID ۱،۳،۶،۱،۵،۵،۷،۳،۲) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp۹ با OID ۱،۳،۶،۱،۵،۵،۷،۳،۹) را در فیلد extendedKeyUsage خود داشته باشند.	
۱۷۷	**الزامات پروتکل X۵۰۹ (۲)/ ابطال**
محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.	
۱۷۸	**الزامات پروتکل X۵۰۹ (۳)**
محصول مورد ارزیابی باید جهت پشتیبانی احراز هویت برای [IPsec, TLS, HTTPS,SSH] و [هیچ کاربرد دیگر] از گواهی‌نامه‌های X.۵۰۹v۳ تعریف‌شده در RFC ۵۲۸۰ استفاده کند.	
۱۷۹	**الزامات پروتکل X۵۰۹ (٤)**
زمانی که محصول مورد ارزیابی نمی‌تواند اتصال مورد نیاز برای تائید اعتبار یک گواهی‌نامه را برقرار کند، باید [به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند یا گواهی‌نامه را نپذیرد].	
۱۸۰	**الزامات پروتکل X۵۰۹ (۵)**
محصول مورد ارزیابی باید مطابق با آنچه در RFC ۲۹۸۶ تشریح شده است، یک Certificate Request Message تولید کند و بتواند اطلاعات؛ کلید عمومی و [Common Name، Organization ، Organization Unit ،Country] را در درخواست فراهم کند.	
۱۸۱	**الزامات پروتکل X۵۰۹ (٦)**
محصول مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.	

۱۸،۱۵ الزامات به‌روزرسانی امن

شماره الزام	نام الزام

۱۸۵	**مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار**
محصول باید قابلیت [فعال کردن و غیرفعال کردن] توابع [به‌روزرسانی خودکار] را به سرپرست امنیتی محصول محدود کند.	
۱۸٦	**مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع**
محصول باید قابلیت [تعیین رفتار[۱]] مربوط به توابع [مخابره داده ممیزی به موجودیت IT خارجی] را به سرپرست امنیتی محصول محدود کند.	

[۱] Determine the behaviour

٦ الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL۱ آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام الزام	توضیحات
Development	**ADV_FSP.۱**	مشخصات کارکرد ابتدایی
Guidance Documents	**AGD_OPE.۱**	راهنمای کاربری
	AGD_PRE.۱	راهنمای آماده‌سازی
Tests	**ATE_IND.۱**	آزمون مستقل- منطبق
Vulnerability Assessment	**AVA_VAN.۱**	تحلیل آسیب‌پذیری
Life cycle Support	**ALC_CMC.۱**	برچسب گذاری هدف ارزیابی
	ALC_CMS.۱	پوشش پیکربندی هدف ارزیابی

۱.٦ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نمی‌باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

۱.۱.٦ مشخصات کارکردی

مشخصات کارکردی، واسطهای کارکرد امنیتی محصول را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسطها نمی‌باشد. فعالیت‌های این خانواده باید بر روی شناخت واسطهای معرفی شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.۱,۱D)** **شرح مولفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.۱,۲D)** **شرح مولفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
	نکته کاربردی ٦٠: مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.۱,۱C)** **شرح مولفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [۱] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.۱,۲C)** **شرح مولفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.۱,۳C)** **شرح مولفه:**

[۱]-SFR-enforcing TSFI

[۲]-SFR-supporting TSFI

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	مشخصات کارکردی باید برای دسته‌بندی ضمنی واسطهای غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.۱,٤C)** **شرح مولفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطهای کارکرد امنیتی در سند مشخصات کارکردی باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.۱,۲E)** **شرح مولفه:** ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «تست» و «آسیب‌پذیری» ارائه شده است.

۲.٦ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

دستورالعمل نصب موفقیت‌آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر

دستورالعمل‌هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو می‌باشد.

۱.۲.٦ راهنمای کاربردی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.۱,۱D)** **شرح مولفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.۱,۱C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.۱,۲C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.۱,۳C)**

مولفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	شرح مولفه: سـند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسـط‌های دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.۱,٤C)** **شرح مولفه:** سـند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسـترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.۱,٥C)** **شرح مولفه:** سـند راهنمای کاربردی باید تمام مدهای عملیاتی محصـول (مدهایی شـامل شـکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.۱,٦C)** **شرح مولفه:** سـند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسـط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.۱,۷C)** **شرح مولفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مولفه‌های محتوایی را برآورده می‌نماید.

۲.۲.٦ راهنمای آماده‌سازی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.۱,۱D)** **شرح مولفه:** توسعه دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.۱,۱C)** **شرح مولفه:** مستندات آماده‌سازی بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مولفه: (AGD_PRE.۱,۲C)** **شرح مولفه:**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مولفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مولفه: (AGD_PRE.۱,۲E)** **شرح مولفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به صورت امن برای عمل نمودن آماده شود.

۳.٦ کلاس تست

تست محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آنها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. تست بخش‌های کارکردی سیستم از طریق خانواده ATE_IND، و تست بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL۱) تست براساس کارکردی که برای محصول در نظر گرفته شده و واسطهایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج تست و تحلیل آسیب‌پذیری باید در گزارش تست لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۱.۳.٦ تست مستقل

«تست مستقل» برای تائید کارکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای مدیر» ارائه شده، صورت می‌گیرند. هدف اصلی تست اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. ارزیاب باید در سند «گزارش تست»، طرح تست و نتایج آن را مستند نماید.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.۱,۱D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.۱,۱C)** **شرح مولفه:** محصول باید مناسب آزمودن باشد.

مولفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: تست مستقل ۱ **شماره مولفه: (ATE_IND.۱,۲E)** **شرح مولفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

٤.٦ کلاس آسیب‌پذیری

١.٤.٦ تحلیل آسیب‌پذیری

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.۱,۱D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارئه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.۱,۱C)** **شرح مولفه:** محصول باید مناسب آزمودن باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مولفه: (AVA_VAN.۱,۲E)** **شرح مولفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مولفه: (AVA_VAN.۱,۳E)**

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	شرح مولفه: ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۵.۶ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL۱) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان(EAL۱) تنها به این اطلاعات نیاز است.

۱.۵.۶ قابلیت‌های پیکربندی

این مولفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (بدین معنی که جدا ار برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.۱,۱D)** **شرح مولفه:** توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.۱,۱C)** **شرح مولفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۲.۵.۶ حوزه پیکربندی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.۱,۱D)** **شرح مولفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.۱,۱C)** **شرح مولفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مولفه: (ALC_CMS.۱,۱C)** **شرح مولفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.۱,۱E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۷ شرح خلاصه‌ای از هدف ارزیابی

هدف این قسمت ارائه دادن شرحی از چگونه فراهم نمودن تمام الزامات کارکرد امنیتی توسط هدف ارزیابی برای مصرف کنندگان می‌باشد.

توابع امنیتی که به وسیله هدف ارزیابی پیاده سازی شده است به شرح زیر است:

- ممیزی امنیت
- شناسایی و احزارهویت
- مدیریت امنیت
- سیستم جلوگیری از نفوذ
- دیوارآتش
- کانال‌ها و مسیرهای مورد اعتماد

۱.۷ ممیزی امنیت

رویدادهای امنیتی به معنی گزارش‌ها و تغییر وضعیت‌ها در سیستم می‌باشد. هدف ارزیابی از رویدادهای ممیزی زیر پشتیبانی می‌کند:
کلی: ورود به سیستم کاربر، خروج از سیستم کاربر

- احرازهویت ناموفق کاربران
- داشبورد: گزارش‌گیری‌ها و لیست‌های آماری
- مدیریت کاربر: تغییر و به روز رسانی و تنظیم مجدد دادههای احرازهویت، ایجاد و به روز رسانی و حذف کاربران.
- مدیریت دارایی‌ها: ایجاد، به روز رسانی و حذف دارایی‌ها؛ مشاهده، جستجو، ایجاد، به روز رسانی و حذف گروه‌های دارایی‌ها و یا وارد نمودن دارایی‌ها.
- پیکربندی: ایجاد، به روز رسانی و حذف گروه‌های شبکه (دسته‌بندی‌های IP)؛ ذخیره و بازیابی تنظیمات سیستم؛ ایجاد، به روز رسانی و حذف دسته‌بندی‌های IP؛ مشاهده و ذخیره تنظیمات شبکه؛
- اکتشاف دارایی‌ها: ایجاد اطلاعات دارایی‌ها؛ به روز رسانی پیکربندی اکتشاف دارایی‌ها به صورت ایستا؛ راه‌اندازی و متوقف نمودن اسکن اکتشاف دارایی‌ها به صورت ایستا

- رویداد بلادرنگ: ایجاد، تغییر دادن، کپی نمودن و حذف قوانین؛ ایجاد، تغییر، فعال‌سازی، غیرفعال نمودن و کپی نمودن قوانین همبستگی؛ ایجاد، تغییر دادن و حذف لیست IPها؛ ایجاد، تغییر دادن و حذف جزئیات پورت‌ها؛
- گزارش‌دهی: ایجاد، تغییر و حذف گزارشات اتوماتیک، دانلود و حذف گزارشات تولید شده، دانلود خلاصه گزارش‌گیری‌ها، ویرایش فیلتر گزارش براساس محدوده‌ی مدت تعیین شده؛ IP تجهیزات و طبقه‌بندی آن‌ها.

۲.۷ شناسایی و احراز هویت

- کنسول واسط کاربری را برای پیکربندی هدف ارزیابی برای مدیریت هدف ارزیابی توسط کاربران فراهم می‌کند. علاوه بر دسترسی از طریق کنسول، هدف ارزیابی با استفاده از مرورگر وب نیز قابل پشتیبانی می‌باشد. هدف ارزیابی شناسایی و احرازهویت را از طریق یک مکانیزم احرازهویت متمرکز شده فراهم می‌کند.
- اپراتورها با دسترسی مدیریتی باید با استفاده از نام کاربری و رمز عبور احرازهویت نمایند.

۳.۷ مدیریت امنیت

تنها سرپرست می‌تواند دسترسی‌های کاربر و خصیصه‌های حساب کاربری را مدیریت کند.

سرپرست می‌تواند:

- حساب کاربری ایجاد کند.
- حساب کاربری موجود را تغییر دهد.
- مجوز دسترسی جدید تعریف کند.
- مجوز دسترسی موجود را ویرایش کند.
- پیکربندی کلیه ماژول‌های دستگاه را مدیریت کند.

٤.۷ سیستم جلوگیری از نفوذ

سیستم تشخیص تهدیدات و جلوگیری از نفوذ قادر به انجام اقدامات زیر می‌باشد:

۱. نظارت بر بسته‌های عبوری محصور شده از طریق GRE، IP-in-IP، PPTP، MPLS و ...
۲. نرمال‌سازی به منظور باز ترکیب بسته‌های تکه تکه شده
۳. نرمال‌سازی TCP جریان‌های ترافیک از طریق هدف ارزیابی در حالتی که هدف ارزیابی در مد درون خط مستقر شده داشته باشد
۴. بازرسی محتوای سرآیند بسته‌ها و سرآیند فیلدهای: IPv۴، IPv۶، ICMP، ICMPv۶، TCP و UDP
۵. کشف امضاهای مبتنی بر سرآیند در واسطهای حسگر IPS: حملات IP، حملات ICMP، حملات TCP، حملات UDP(UDP Bom و UDP Chargen DoS)
۶. شناسایی تمامی امضاهای کشف الگوی ترافیکی و به‌کارگیری آن‌ها در IPS:

- حمله DoS
- حمله Smurf ، سیل آسا ping
- اسکن پورت و پروتکل

۷. ترکیب خط‌مشی‌های IPS مبتنی بر امضا، و عملیات‌های زیر:

- در هر حالتی، برای هر واسط حسگر:
  - اجازه به جریان ترافیک
  - ارسال بازنشانی TCP به آدرس مبدأ ترافیک متخلف
  - ارسال بازنشانی TCP به آدرس مقصد ترافیک متخلف
  - ارسال پیام غیرقابل دسترسی ICMP میزبان، مقصد، پورت
- حالت بر خط
  - اجازه به جریان ترافیک
  - بلوکه کردن/ قطع جریان ترافیک

لازم به ذکر است با توجه به عدم دسترسی کاربر به مکان ذخیره‌سازی لاگ‌ها امکان تغییر لاگ‌ها توسط کاربر وجود ندارد و در نتیجه الزام شماره FAU_STG.۱,۲ و FAU_STG.۱,۱ کاربردی ندارد.

۵.۷ دیوارآتش

دیوارآتش امکانات زیر را ارائه می‌دهد:

- فیلترنمودن حالتمند ترافیک بسته‌های شبکه‌ای که توسط هدف ارزیابی پردازش می‌شود

پردازش پروتکل‌های ترافیک شبکه زیر:

Internet Control Message Protocol version ۴ (ICMPv۴)

Internet Control Message Protocol version ۶ (ICMPv۶)

Internet Protocol (IPv۴)

Internet Protocol version ۶ (IPv۶)

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

و بررسی فیلد سرآیند بسته‌های شبکه که در RFCهای زیر تعریف شده‌اند:

RFC ۷۹۲ (ICMPv۴)

RFC ۴۴۴۳ (ICMPv۶)

RFC ۷۹۱ (IPv۴)

RFC ۲۴۶۰ (IPv۶)

RFC ۷۹۳ (TCP)

RFC ۷۶۸ (UDP)

- قوانین فیلترنمودن حالتمند ترافیک را بر روی واسطهای مختلف و با استفاده از فیلدهای پروتکل شبکه ICMPv۴، ICMPv۶، IPv۴، IPv۶، TCP و UDP تعریف می‌نماید
- امکان اجازه دادن، جلوگیری کردن و گزارش‌گیری را برای هر یک از قوانین فیلتر نمودن حالتمند شبکه ارائه می‌دهد.
- هر یک از قوانین فیلتر نمودن حالتمند شبکه بر روی هر یک از واسطهای شبکه اعمال نمود.

٦.٧ کانال‌ها و مسیرهای مورد اعتماد

یک مسیر امن، ارائه دهنده قابلیتی برای کاربران است تا فعالیتشان را از طریق یک تعامل مستقیم و مطمئن با توابع امنیتی هدف ارزیابی، انجام دهند. مسیر امن اغلب برای اقدامات کاربر همچون شناسایی و احراز هویت اولیه مطلوب است، اما ممکن است در زمآن‌های دیگری در طول بازه زمانی یک نشست کاربری نیز مفید باشد و تبادلات مسیر امن ممکن است توسط کاربر یا توابع امنیتی هدف ارزیابی آغاز گردد. پاسخ امن از طریق مسیر امن تضمین می‌کند که از تغییرات توسط برنامه ناامن یا افشا شدن برای یک برنامه ناامن محافظت می‌نماید. هدف ارزیابی از پروتکل IPsec (SSH، TLS/HTTPS) و openvpn (openssl) جهت ایجاد یک کانال ارتباطی امن بین خود و تمام موجودیت‌های IT مجاز ایجاد می‌نماید به طوری‌که این کانال بصورت منطقی از دیگر کانال‌های ارتباطی مجزا بوده و نقطه پایانی ارتباط را به طور قطعی شناسایی می‌نماید و از داده کانال در برابر افشا و تشخیص تغییرات داده کانال محافظت می‌نماید.

نکته فنی: با توجه به تحقیقات و یافته‌های علمی به دلایل زیر استفاده از Anomaly Detection به روش آماری توصیه نمی‌شود.

۱. برای استفاده از Anomaly Detection نیاز است که در یک بازه زمانی ترافیک نرمال ثبت شود (دوره Learning) تا با استفاده از آن یک Profile ایجاد شود که از آن به عنوان شاخص برای تفکیک ترافیک عادی و ترافیک دارای Anomaly استفاده شود. نقطه ضعف این روش آن است که در صورتی که در ترافیک نرمال، Anomaly وجود داشته باشد حاصل تولید یک Profile دارای ترافیک Anomaly می‌شود که استفاده از این Profile به معنای بازکردن راه ورود به سیستم می‌باشد.
۲. False Positive زیاد Anomaly Detection دلیل دیگر عدم استفاده از آن است. در صورتی که در حالت درون خط مورد استفاده قرار گیرد باعث اختلال در روند عادی شبکه می‌گردد.

به علت مشکلات مذکور شرکت‌های بزرگ مانند snort نیز دیگر Anomaly Detection را از سبد محصولات خود خارج کرده و آن را پشتیبانی نمی‌کنند.