به نام خدا

پروفایل حفاظتی

مدیریت یکپارچه تهدیدات (UTM)

آبان ماه ۹۹

نسخه ۲,۱

پیشگفتار

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده نمودن الزامات ارائه‌شده‌اند، در محصول خود فراهم و به خریداران آن محصول نیز در انتخاب محصول خود کمک نمایند. مرکز مدیریت راهبردی افتا با همکاری مرکز تحقیقات صنایع انفورماتیک و سازمان فناوری اطلاعات ایران این سند را در راستای این هدف تهیه کرده است. این سند معرفی کننده‌ی الزامات کارکرد امنیتی برای سیستم مدیریت یکپارچه تهدیدات است تا تولیدکنندگان این محصول بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ کنند و همچنین سند هدف امنیتی آن را ارائه نمایند.

در بخش اول به معرفی سیستم مدیریت یکپارچه تهدیدات پرداخته‌شده است. سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدات، اجرای خط‌مشی‌ها و بکار بردن فرضیات مطرح می‌گردد. در بخش بعدی «الزامات کارکرد امنیتی» آورده شده؛ بر اساس استاندارد ارزیابی معیار مشترک این قسمت از چندین کلاس تشکیل‌شده است که هر یک از این کلاس‌ها حوزه‌ی خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای محصول UTM در این سند مطرح‌شده است، عبارت‌اند از:

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس IPSEC
- کلاس حفاظت از داده‌های کاربری
- کلاس دیواره آتش
- کلاس شناسایی و احراز هویت
- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی
- کلاس دسترسی به هدف ارزیابی
- کلاس کانال‌ها / مسیرهای مورد اعتماد
- کلاس IPS

هریک از این کلاس‌ها، از مجموعه‌ای از خانواده‌ها تشکیل یافته و هر خانواده از مجموعه‌ای عنصر و هر عنصر از مجموعه‌ای مؤلفه تشکیل یافته است. با استفاده از «الزامات کارکرد امنیتی» درواقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌گردد.

در بخش پایانی «الزامات تضمین امنیتی» که از ساختاری مشابه بخش قبلی برخوردار است مطرح گردیده است، این بخش الزامات لازم جهت ارزیابی محصول را عنوان می‌نماید.

تذکر: این فایل از لحاظ الزامات مورد به‌روزرسانی قرار گرفته است. برخی نکات کاربردی نیز در فایل اصلی تغییر کرده یا بروز شده‌اند که این تغییرات در این پروفایل انجام نشده است و در نسخه‌های بعدی ارائه خواهند شد.

فهرست

۱ شرح محصول UTM

سند حاضر، پروفایل حفاظتی برای ارزیابی محصولی است که به‌عنوان یک سیستم مدیریت یکپارچه تهدیدات (UTM) شناخته می‌شود. منظور از یک دستگاه UTM در این پروفایل حفاظتی، دستگاهی متشکل از سخت‌افزار و نرم‌افزار است که به شبکه متصل می‌شود و نرم‌افزار آن می‌تواند شامل مجموعه‌ای کامل و جامع از تمامی راهکارهای امن شامل دیوار آتش، ایجاد شبکه خصوصی مجازی (VPN)، ضدویروس، ضد هرزنامه، سیستم شناسایی و جلوگیری از نفوذ، فیلترینگ محتوی، مدیریت پهنای باند، مدیریت ضد جاسوس‌افزار و غیره باشد.

این پروفایل حفاظتی، مجموعه‌ای از حداقل الزامات امنیتی را ارائه می‌کند که یک دستگاه UTM که به صورت پایه‌ای شامل دیواره آتش، VPN و IPS است و باید به‌منظور کاهش تهدیدات، آن‌ها را رعایت نمایند. این مجموعه اولیه کارکردهای امنیتی، شامل مواردی ازجمله حفاظت از تمام مسیرهای مدیریتی راه دور، ارائه خدمات شناسایی و احراز هویت برای ورودهای محلی و راه دور، ممیزی رویدادهای امنیتی، تائید رمزنگاری امن تمام به‌روزرسانی‌ها و حفاظت در برابر حملات مرسوم به شبکه، الزامات اولیه کلاس فایروال، الزامات اولیه IPS است. هدف این است که تمام دستگاه‌های UTM که در حیطه شمول این پروفایل حفاظتی قرار می‌گیرند، به گونه مناسبی در شبکه «رفتار» کنند و آسیبی را به شبکه وارد نکنند. بدین منظور، انتظار می‌رود که دستگاه UTM از پروتکل‌های استانداردی مانند IPsec یا TLS یا SSH استفاده کند و بدین ترتیب از مسیرهای ارتباطی برقرارشده با موجودیت‌های خارجی محافظت نماید. همچنین لازم است که گواهی‌نامه‌های X.509 به‌منظور احراز هویت مورداستفاده قرار گیرند. این گواهی‌نامه‌ها گزینه‌ای برای امضای دیجیتال و امضای کد هستند.

۱-۱ موارد کاربرد محصول

مدیریت یکپارچه تهدیدات ((UTM معمولاً شامل بسته‌های امنیتی کامل برای محافظت از شبکه در مقابل تهدیداتی از جمله: ویروس‌ها، هرزنامه‌ها، بدافزارها، برنامه‌های کلاه‌برداری، حملات امنیتی، نفوذ هکرها و ... است. این بسته‌های امنیتی معمولاً شامل: فایروال، آنتی‌ویروس، آنتی‌اسپم، VPN، سیستم جلوگیری از نفوذ، فیلترینگ مبتنی بر متن، تعدیل بار، مدیریت پهنای باند، جلوگیری از افشای داده، کنترل کاربردی، متمرکز کردن و ... می‌باشند.

در این روش به جای استفاده و مدیریت چندین سیستم، می‌توان به طور مستقل تنها از یک UTM که تمام عملیات حفاظتی را در یک سیستم انجام می‌دهد، استفاده کرد.

علاوه بر آنکه پیاده‌سازی، مدیریت و به‌روزرسانی سیستم‌های مختلف امنیتی مشکل است، این پیاده‌سازی، مدیریت و به‌روزرسانی باعث افزایش پیچیدگی عملیات و هزینه‌های بالاسری نیز می‌شود. بدین ترتیب سازمان‌ها

امروزه از یک نگرش یکپارچه برای امنیت و بهره‌وری شبکه استفاده می‌کنند که تکنولوژی‌های قدیمی مجزا را ترکیب کرده و به صورت یکجا آن‌ها را مدیریت می‌کنند.

ابزار UTM با استفاده از یک دستگاه که در چندین لایه سخت‌افزاری و نرم‌افزاری گماشته شده‌اند، مدیریت استراتژی امنیت شرکت‌ها را ساده می‌کند، همچنین تنها با استفاده از یک کنسول متمرکز، تمام راهکارهای امنیتی، پیاده‌سازی و مدیریت می‌شوند.

UTM دارای تمام ویژگی‌های امنیتی همه‌منظوره، به جهت افزایش کارایی است که می‌تواند منجر به یکپارچه‌سازی و خروجی بهتری از یک مجموعه قطعات جداگانه شود.

در سازمان‌هایی با شبکه‌های راه دور یا اداراتی که با فاصله واقع شده‌اند، UTM ها امنیت متمرکز را برای کنترل کامل روی شبکه‌های توزیع شده سرتاسری خود فراهم می‌کنند.

۲ تعریف مسائل امنیتی

هر UTM باید نقش خود را به عنوان یک زیرساخت شبکه ایفا نماید. به منظور ایفای این نقش، دستگاه مذکور ارتباطاتی را از طریق شبکه با دیگر دستگاه‌های شبکه و سایر موجودیت‌های شبکه (موجودیتی که به عنوان یک دستگاه شبکه تعریف نشده است) برقرار می‌نماید. در عین حال، UTM باید مجموعه‌ای از حداقل کارکردهای امنیتی معمول که از همه دستگاه‌های شبکه انتظار می‌رود را ارائه نماید. مسئله امنیتی که یک UTM مطابق با پروفایل حاضر باید به آن بپردازد، حداقل کارکردهای امنیتی معمول برای مقابله با تهدیدات معمول پیش روی دستگاه‌های شبکه است. این تهدیدات در مقابل تهدیداتی قرار می‌گیرند که یک کارکرد خاص از یک نوع خاص از UTM را هدف قرار می‌دهند. مجموعه حداقل کارکردهای امنیتی معمول باید قابلیت‌های زیر را داشته باشند:

- برقراری ارتباط با دستگاه‌های مجاز و غیرمجاز شبکه
- توانایی انجام به‌روزرسانی‌های معتبر و امن
- توانایی ممیزی فعالیت‌های دستگاه‌ها
- توانایی ذخیره‌سازی و استفاده امن از داده‌ها و اطلاعات محرمانه راهبر و دستگاه
- توانایی انجام خودآزمایی در صورت از کار افتادن مؤلفه‌های کلیدی.

۲-۱ تهدیدات

در ادامه، تهدیدات پیش روی UTM بر اساس عملکرد این دستگاه‌ها دسته‌بندی شده‌اند.

۲-۱-۱ ارتباط با دستگاه‌های شبکه

یک UTM با سایر دستگاه‌های شبکه و موجودیت‌های شبکه ارتباط برقرار می‌کند. مقصد این ارتباط ممکن است از لحاظ منطقی یا جغرافیایی یک دستگاه راه دور به شمار آید و مسیر ارتباط ممکن است از سیستم‌های متعدد دیگری بگذرد. این احتمال وجود دارد که سیستم‌های میانی مورد اعتماد نباشند و ارتباط غیرمجازی را با UTM برقرار کنند یا ارتباطات مجاز را در معرض خطر قرار دهند. کارکرد امنیتی UTM باید این قابلیت را داشته باشد که از ترافیک حساس شبکه (مانند ترافیک راهبری، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست) محافظت نماید. ارتباطات برقرارشده با UTM را می‌توان به دو دسته تقسیم‌بندی کرد: ارتباطات مجاز و ارتباطات غیرمجاز. ارتباطات مجاز شامل ترافیکی است که بر اساس خط‌مشی UTM، اجازه جریان یافتن دارد. ارتباطات مجاز ترافیک حساس شبکه را شامل می‌شود که از آن جمله می‌توان به ترافیک راهبری UTM و ارتباطات آن با یک سرور ممیزی یا احراز هویت اشاره کرد. حفاظت از این ارتباطات نیازمند استفاده از یک کانال امن است. کارکرد امنیتی UTM باید به گونه‌ای باشد که اطمینان حاصل نماید تنها ارتباطات مجاز می‌توانند برقرار شوند. این کارکرد امنیتی باید کانال امنی را برای جریان یافتن ترافیک حساس شبکه فراهم آورد. تمامی ارتباطات دیگر، ارتباطات غیرمجاز به شمار می‌آیند. تهدید اصلی علیه ارتباطات UTM

که در این پروفایل حفاظتی به آن پرداخته می‌شود، یک موجودیت غیرمجاز خارجی است که تلاش می‌کند به ترافیک حساس شبکه دسترسی پیدا کند، آن را تغییر دهد یا به هر طریقی آن را افشا نماید. در صورتی که از الگوریتم‌های رمزنگاری نامناسبی استفاده شده باشد یا پروتکل‌های تونل‌زنی غیراستاندارد و اطلاعات محرمانه راهبری ضعیفی به کار گرفته شده باشند، یک عامل تهدید می‌تواند به صورت غیرمجاز به دستگاه دسترسی پیدا کند. استفاده از رمزنگاری ضعیف یا عدم استفاده از چنین الگوریتمی به طور کل، باعث می‌شود که عامل تهدید بتواند با کمترین تلاش، ترافیک را بخواند، دست‌کاری کند یا کنترل نماید. استفاده از پروتکل‌های تونل‌زنی غیراستاندارد نه‌تنها قابلیت هم‌کنش‌پذیری دستگاه را محدود می‌کند، بلکه ضمانت و اعتماد حاصل از استانداردسازی را نیز از دستگاه می‌گیرد.

۲-۱-۲ دسترسی راهبری غیرمجاز

ممکن است عامل تهدید تلاش کند تا با استفاده از ابزارهای بدخواهانه، به UTM دسترسی راهبری پیدا کند. به عنوان مثال، عامل تهدید خود را به عنوان راهبر به دستگاه معرفی می‌کند، به عنوان دستگاه به راهبر معرفی می‌نماید، نشست راهبری را بازپخش می‌کند (به طور کامل یا بخش‌هایی خاص از آن)، یا حملات کسی در میانه را ترتیب می‌دهد تا به نشست‌های راهبری یا نشست‌های بین دستگاه‌های شبکه دسترسی پیدا کند. بدین ترتیب، عامل تهدید قادر خواهد بود تا اقدامات بدخواهانه‌ای را انجام دهد و کارکرد امنیتی دستگاه و شبکه را به خطر اندازد.

۲-۱-۳ رمزنگاری ضعیف

ممکن است عامل تهدید از ضعیف بودن الگوریتم رمزنگاری بهره‌برداری کند یا حملات رمزنگاری گسترده را علیه حافظه اصلی ترتیب دهد. انتخاب نادرست الگوریتم رمزنگاری، مُدها یا اندازه کلیدها به مهاجمان اجازه می‌دهد تا به الگوریتم رمزنگاری حمله کنند یا با ترتیب دادن حملات جستجوی فراگیر علیه حافظ اصلی، با کمترین تلاش موفق به خواندن، دست‌کاری یا کنترل ترافیک شوند.

۲-۱-۴ کانال‌های ارتباطی غیرقابل اعتماد

ممکن است عامل تهدید آن دسته از دستگاه‌های شبکه را هدف قرار دهد که از پروتکل‌های تونل‌زنی استاندارد برای حفاظت از ترافیک حساس شبکه خود استفاده نمی‌کنند. مهاجمان می‌توانند با بهره‌گیری از پروتکل‌های با طراحی نامناسب یا فرایندهای ضعیف مدیریت کلید، حملات مردی در میان، حملات بازپخش یا حملات دیگری از این دست را ترتیب دهند. حملات موفق باعث از دست رفتن محرمانگی و یکپارچگی ترافیک حساس شبکه می‌شوند و حتی می‌توانند UTM را به خطر اندازند.

۲-۱-۵ نقاط پایانی با احراز هویت ضعیف

ممکن است عامل تهدید به پروتکل‌های امنی حمله کند که برای احراز هویت در دستگاه‌های انتهایی از روش‌های ضعیفی استفاده می‌کنند (مثلاً گذرواژه‌های اشتراکی که قابل حدس هستند یا به صورت متن ساده ارسال شده‌اند). عواقب این فرایند، مشابه وقتی است که از پروتکل‌های با طراحی ضعیف استفاده شده باشد. مهاجم می‌تواند خود را به جای راهبر به دستگاه دیگری معرفی کند یا خود را در جریان شبکه قرار دهد و حملات مردی در میان را طراحی نماید. در نتیجه، ممکن است مهاجم به ترافیک حساس شبکه دسترسی پیدا کند، محرمانگی و یکپارچگی آن را به خطر اندازد و حتی UTM را در معرض خطر قرار دهد.

۲-۱-۶ به‌روزرسانی‌های معتبر

برای حصول اطمینان از صحت کارکرد امنیتی UTM، لازم است که نرم‌افزار و ثابت‌افزار آن به‌روزرسانی شوند. منبع و محتوای به‌روزرسانی‌ها را باید با استفاده از روش‌های رمزنگاری تائید کرد؛ در غیر این صورت، یک منبع غیر معتبر می‌تواند به‌روزرسانی خود را به کار گیرد و کارکرد امنیتی UTM را دور بزند. نسخه‌های به‌روز نشده نرم‌افزارها و ثابت‌افزارها می‌توانند UTM را در معرض خطر عوامل تهدیدی قرار دهند که در پی سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده آن‌ها هستند. به‌روزرسانی‌های تائید نشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تائید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روز شده را در معرض خطر عوامل تهدیدی قرار می‌دهند که به دنبال بهره‌گیری از نرم‌افزار یا ثابت‌افزار برای رسیدن به مقاصد خویش هستند.

۲-۱-۷ به‌روزرسانی‌های مخرب

ممکن است عامل تهدید یک به‌روزرسانی معیوب و دستکاری‌شده را برای نرم‌افزار یا ثابت‌افزار UTM ارائه کند و کارکرد امنیتی دستگاه را در معرض خطر قرار دهد. به‌روزرسانی‌های تائید نشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تائید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روز شده را در معرض خطر دست‌کاری غیرمجاز قرار می‌دهد.

۲-۱-۸ فعالیت‌های ممیزی شده

راهبران می‌توانند با ممیزی فعالیت‌های UTM، وضعیت دستگاه را به خوبی پایش نمایند. این فرایند امکان بررسی، گزارش‌دهی در خصوص کارکردهای امنیتی، بازسازی رویدادها و تحلیل مشکل امنیتی را برای راهبر فراهم می‌آورد. پردازش‌هایی که در پاسخ به فعالیت‌های دستگاه انجام می‌شوند، نشانه‌هایی از به خطر افتادن یا از کار افتادن کارکردهای امنیتی را ارائه می‌کنند. در صورتی که فعالیت‌هایی انجام شده و بر کارکرد امنیتی تأثیر گذاشته باشند اما نشانه‌ای دال بر انجام شدن آن‌ها تولید و پایش نشده باشد، ممکن است که این فعالیت‌ها بدون آگاهی راهبر صورت گرفته باشند. علاوه بر این، در صورتی که سوابق تولید و نگهداری نشده باشند، امکان بازسازی شبکه و درک شدت و میزان آسیب‌های وارده تحت تأثیر قرار خواهد گرفت. داده‌های ممیزی ثبت‌شده

در خصوص تغییر و حذف غیرمجاز، باید به دقت محافظت شوند. داده‌های مذکور ممکن است در درون محصول یا در هنگام انتقال به حافظه‌های خارجی مورد حمله قرار گیرند. توجه داشته باشید که بر اساس این پروفایل حفاظتی مشارکتی، UTM باید داده‌های ممیزی را تولید کند و قابلیت ارسال آن‌ها به یک موجودیت شبکه مورد اعتماد را داشته باشد.

۲-۱-۹ فعالیت ردیابی‌نشده

ممکن است عامل تهدید تلاش کند تا بدون اطلاع راهبر، به کارکرد امنیتی UTM دسترسی پیدا کند، آن را تغییر دهد و/یا دست‌کاری نماید. بدین ترتیب، ممکن است مهاجم راهی برای حمله UTM پیدا کند و راهبر نیز آگاه نشود که دستگاه در معرض خطر قرار گرفته است.

۲-۱-۱۰ داده‌ها و اطلاعات محرمانه دستگاه و راهبر

UTM دربردارنده داده‌ها و اطلاعات محرمانه‌ای است که باید به طور امن ذخیره‌سازی شوند و امکان دسترسی به آن‌ها تنها برای موجودیت‌های مجاز وجود داشته باشد. به عنوان مثال، می‌توان به اطلاعات محرمانه احراز هویت و پیکربندی نرم‌افزار و ثابت‌افزار و اطلاعات محرمانه راهبری اشاره کرد. کلیدهای راهبر و دستگاه، اطلاعات کلید و اطلاعات محرمانه احراز هویت را باید در برابر دست‌کاری و افشای غیرمجاز محافظت نمود. علاوه بر این، کارکرد امنیتی دستگاه باید کاربران را ملزم کند تا اطلاعات محرمانه احراز هویت پیش‌فرض را تغییر دهند (مثلاً راهبران ملزم باشند که اطلاعات محرمانه ورود پیش‌فرض را عوض کنند). عدم ذخیره‌سازی امن و مدیریت نامناسب داده‌ها و اطلاعات محرمانه (مانند رمزگذاری نکردن اطلاعات محرمانه درون فایل‌های پیکربندی یا دسترسی به کلیدهای نشست کانال امن) به مهاجم امکان می‌دهد تا به UTM دسترسی پیدا کند و حتی امنیت شبکه را از طریق دست‌کاری ظاهراً مجاز پیکربندی یا ترتیب دادن حملات کسی در میانه در معرض خطر قرار دهد. این حملات به موجودیت غیرمجاز امکان می‌دهند تا با استفاده از اطلاعات محرمانه راهبر امنیتی، به کارکردهای راهبری دست پیدا کند و آن‌ها را اجرا نماید و همچنین به عنوان یک دستگاه پایانی مجاز، تمامی ترافیک را دریافت نماید. بدین ترتیب، شناسایی حملات امنیتی و بازسازی شبکه دشوار خواهد شد و حتی دسترسی غیرمجاز مهاجم به داده‌های دستگاه و راهبر ادامه خواهد یافت.

۲-۱-۱۱ به خطر افتادن کارکرد امنیتی

ممکن است عامل تهدید داده‌های دستگاه و اطلاعات محرمانه را به خطر اندازد و بدین ترتیب، دسترسی غیرمجاز و مستمری به UTM و داده‌های آن پیدا کند. منظور از به خطر انداختن اطلاعات محرمانه، مواردی از این قبیل است: جایگزین کردن اطلاعات محرمانه فعلی حساب‌های کاربری با اطلاعات محرمانه مهاجم، دست‌کاری اطلاعات محرمانه حساب‌های کاربری یا دست یافتن به اطلاعات محرمانه دستگاه و راهبر و استفاده از آن‌ها توسط مهاجم.

۲-۱-۱۲ هک شدن گذرواژه

ممکن است عامل تهدید از ضعیف بودن گذرواژه‌های راهبری بهره‌گیری کند و از سطح دسترسی ویژه‌ای به دستگاه برخوردار گردد. دسترسی ویژه به دستگاه، مهاجم را قادر می‌سازد تا به ترافیک شبکه نیز دسترسی پیدا کند و حتی از روابط مبتنی بر اعتماد دستگاه با سایر دستگاه‌های شبکه سوءاستفاده نماید.

۲-۱-۱۳ از کار افتادن کارکردهای امنیتی دستگاه

سازوکارهای UTM معمولاً از مراجع اعتماد[۱] آغاز می‌شوند و تا سازوکارهای بسیار پیچیده‌تر ادامه می‌یابند. از کار افتادن این سازوکارها باعث به خطر افتادن کارکرد امنیتی دستگاه می‌شود. UTM برای حصول اطمینان از صحت کارکرد امنیتی خود می‌تواند خودآزمایی‌هایی را در هنگام راه‌اندازی اولیه و همچنین در حین عملیات انجام دهد.

۲-۱-۱۴ از کار افتادن کارکرد امنیتی

ممکن است یکی از مؤلفه‌های UTM در هنگام راه‌اندازی اولیه یا در حین عملیات از کار بیفتد و این امر سبب از کار افتادن کارکرد امنیتی دستگاه شود. بدین ترتیب، دستگاه در معرض حملات مختلف قرار خواهد گرفت.

۲-۲ فرضیات

در این بخش به فروض مربوط به شناسایی تهدیدات و الزامات امنیتی دستگاه‌های شبکه می‌پردازیم. انتظار نمی‌رود که UTM در هیچ‌یک از این موارد ضمانتی ارائه کند و در نتیجه، الزاماتی برای کاهش خسارات ناشی از مخاطرات نیز در نظر گرفته نشده‌اند.

۲-۲-۱ حفاظت فیزیکی

چنین فرض می‌شود که UTM در محیط عملیاتی خود به صورت فیزیکی محافظت شده و در معرض حملات فیزیکی و خسارت‌های ناشی از آن‌ها قرار ندارد. چنین فرض می‌شود که این محافظت برای تأمین امنیت دستگاه و داده‌های آن کافی است. در نتیجه، این پروفایل حفاظتی مشارکتی شامل هیچ الزامی در زمینه حفاظت فیزیکی و ابزارهای لازم برای کاستن از خسارات ناشی از حملات فیزیکی نیست. این پروفایل از محصولات انتظار ندارد که از دسترسی فیزیکی به دستگاه (که به موجودیت‌های غیرمجاز امکان می‌دهد تا داده‌ها را استخراج کنند، سایر کنترل‌ها را دور بزنند یا به هر طریق دیگری دستگاه را دست‌کاری کنند) جلوگیری به عمل آورند.

---

[۱] Roots of trust

۲-۲-۲ کارکرد محدود

چنین فرض می‌شود که دستگاه کارکردهای شبکه را به عنوان کارکرد اصلی خود ارائه می‌کند و خدمات و کارکردهایی که در دسته رایانش همه‌منظوره قرار می‌گیرند را ارائه نمی‌نماید. به عنوان مثال، دستگاه نباید پلتفرم رایانشی را برای کاربردهای همه‌منظوره (کاربردهای غیر مرتبط با کارکرد شبکه) ارائه کند.

۲-۲-۳ عدم محافظت از ترافیک

یک UTM عمومی یا استاندارد، هیچ ضمانتی در خصوص حفاظت از داده‌هایی که از آن می‌گذرند ارائه نمی‌کند. UTM باید از داده‌هایی حفاظت کند که از آن نشأت گرفته یا به آن ارسال شده‌اند. این داده‌ها، داده‌های ممیزی و راهبری را در برمی‌گیرند. ترافیکی که صرفاً از UTM می‌گذرد و مقصد آن دستگاه شبکه دیگری است، در این پروفایل حفاظتی پوشش داده نشده است. چنین فرض می‌شود که این حفاظت برای انواع خاصی از دستگاه‌های شبکه (مانند فایروال)، در پروفایل‌های حفاظتی مشارکتی پوشش داده شود.

۲-۲-۴ راهبر مورد اعتماد

چنین فرض می‌شود که راهبران امنیتی UTM مورد اعتماد هستند و در راستای منافع امنیتی سازمان فعالیت می‌کنند. آن‌ها آموزش مناسب دیده‌اند، از خط‌مشی‌ها پیروی می‌کنند و اسناد راهنما را رعایت می‌نمایند. چنین فرض می‌شود که راهبران امنیتی از اطلاعات محرمانه حساب کاربری و گذرواژه‌هایی با قدرت امنیتی و آنتروپی مناسب استفاده می‌کنند و در هنگام راهبری دستگاه، اهداف بدخواهانه‌ای در سر ندارند. از UTM انتظار نمی‌رود که در صورت انجام اقدامات بدخواهانه توسط راهبر امنیتی، در مقابل اقدامات وی از خود محافظتی به عمل آورد.

۲-۲-۵ به‌روزرسانی منظم

چنین فرض می‌شود که در صورت منتشر شدن به‌روزرسانی‌های جدید در پاسخ به آسیب‌پذیری‌های شناخته‌شده، راهبر نرم‌افزار و ثابت‌افزار UTM را به صورت منظم به‌روزرسانی می‌کند.

۲-۲-۶ امنیت اطلاعات محرمانه راهبر

اطلاعات محرمانه راهبر (کلید خصوصی) که برای دسترسی به UTM استفاده می‌شوند، توسط پلتفرمی که روی آن قرار دارند محافظت می‌گردند.

۲-۳ خط‌مشی امنیتی سازمان

خط‌مشی امنیتی سازمان مجموعه‌ای است از قوانین، اقدامات و رویه‌های سازمان برای برآورده ساختن نیازهای امنیتی آن. یک خط‌مشی امنیتی در بخش زیر ارائه شده است.

۲-۳-۱ بنر دسترسی

محصول باید یک بنر اولیه را نمایش دهد که محدودیت‌های کاربرد، موافقت‌نامه‌های قانونی و هرگونه اطلاعات مقتضی دیگر (که کاربران با دسترسی به محصول با آن‌ها موافقت کرده‌اند) را به نمایش می‌گذارد.

۳ اهداف امنیتی

۳-۱ اهداف امنیتی مربوط به محیط عملیاتی

بخش‌های زیر، اهداف امنیتی مربوط به محیط عملیاتی را تشریح می‌کنند.

۳-۱-۱ امنیت فیزیکی

امنیت فیزیکی، متناسب باارزش محصول مورد ارزیابی و داده‌هایی که در آن قرار دارند، توسط محیط ارائه می‌شود.

۳-۱-۲ عدم کارکرد عمومی

در محصول مورد ارزیابی، هیچ قابلیت محاسباتی عمومی (مانند کامپایلرها یا برنامه‌های کاربردی کاربری) به‌جز خدمات لازم برای کارکرد، مدیریت سیستم و پشتیبانی از محصول مورد ارزیابی وجود ندارد.

۳-۱-۳ محافظت از ترافیک

محصول مورد ارزیابی از ترافیکی که از آن عبور می‌کند، محافظت نمی‌نماید. فرض بر این است که حفاظت از این ترافیک توسط سایر ابزارهای امنیتی و تضمینی موجود در محیط عملیاتی صورت می‌گیرد.

۳-۱-۴ راهبر مورد اعتماد

راهبران محصول مورد ارزیابی امن هستند و فرض بر این است که تمام موارد ذکرشده در اسناد راهنما را به‌طور صحیح انجام می‌دهند.

۳-۱-۵ به‌روزرسانی

نرم‌افزارها و میان‌افزارهای محصول مورد ارزیابی به‌طور منظم توسط سرپرست محصول به‌روز می‌شوند تا بتوانند خود را با به‌روزرسانی‌های محصولات همگام سازند و آسیب‌پذیری‌های شناخته‌شده را برطرف نمایند.

۳-۱-۶ امنیت حساب کاربری راهبر

اطلاعات حساب کاربری سرپرست محصول (کلید خصوصی) مورداستفاده برای دسترسی به محصول، باید در هر پلتفرمی که قرار دارند حفاظت‌شده باشند.

۴ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول آمده‌اند. الزامات تشریح شده در این بخش الزامی هستند و تمامی محصولات باید آن‌ها را رعایت نمایند. بر اساس انتخاب‌هایی که در این الزامات صورت می‌گیرند، لازم خواهد بود که برخی الزامات مورداشاره در پیوست دو نیز رعایت شوند. برخی الزامات اختیاری نیز ممکن است از پیوست یک برگزیده شوند. موارد ذکرشده در قالب فعالیت‌های ارزیابی، بیان می‌کنند که توسعه‌دهندگان محصول مورد ارزیابی باید چه مواردی را رعایت کنند.

به‌طورکلی، الزامات کارکرد امنیتی مورد اشاره در پیوست دو که در هدف امنیتی به‌عنوان موارد ضروری به آن‌ها اشاره‌شده است، در اثر انتخاب‌های صورت گرفته در سایر الزامات کارکرد امنیتی تعیین و تکمیل می‌شوند. به‌عنوان‌مثال، در هر یک از الزامات «کانال امن» و «مسیر امن» باید پروتکل‌هایی را برای انواع کانال‌های امن تشریح شده در الزامات کارکرد امنیتی انتخاب کرد. انتخاب این پروتکل‌ها تعیین می‌کند که کدام‌یک از الزامات کارکرد امنیتی مورداشاره، در هدف امنیتی نیز لازم هستند. درصورتی‌که الزامات کارکرد امنیتی تشریح شده در پیوست یک توسط محصول مورد ارزیابی فراهم‌شده باشند، می‌توان آن‌ها را در هدف امنیتی گنجاند؛ اما این الزامات برای این‌که محصول مورد ارزیابی مطابق با این پروفایل حفاظتی باشد ضروری نیستند.

جدول ۱. لیست الزامات

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	تولید داده ممیزی ۱	FAU_GEN.1.1
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	تولید داده ممیزی ۳	FAU_GEN.2.1
۴	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.1.1
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2
۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.1.3
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۸	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۹	نابودی کلید رمزنگاری ۴	FCS_CKM.4.1
۱۰	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1/DataEncryption
۱۱	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1/SigGen

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1/Hash
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1/KeyedHash
۱۴	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۱۵	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۱۶	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۱۷	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۱۸	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۱۹	شناسایی و احراز هویت کاربر ۱	FIA_UIA_EXT.1.1
۲۰	شناسایی و احراز هویت کاربر ۲	FIA_UIA_EXT.1.2
۲۱	سازوکار احراز هویت بر اساس رمز عبور ۲	FIA_UAU_EXT.2.1
۲۲	احراز هویت کاربر ۱۰	FIA_UAU.7.1
۲۳	مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی دستی	FMT_MOF.1.1(1)/ManualUpdate
۲۴	مدیریت داده‌های محصول ۱	FMT_MTD.1.1/CoreData
۲۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۲۶	نقش‌های امنیتی ۳	FMT_SMR.2.1
۲۷	نقش‌های امنیتی ۴	FMT_SMR.2.2
۲۸	نقش‌های امنیتی ۵	FMT_SMR.2.3
۲۹	مدیریت کارکرد در محصول IPS۱	FMT_SMF.1.1/IPS
۳۰	محافظت از داده‌های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1
۳۱	حفاظت از کلمه عبور مدیر سیستم ۱	FPT_APW_EXT.1.1
۳۲	حفاظت از کلمه عبور مدیر سیستم ۲	FPT_APW_EXT.1.2
۳۳	خودآزمایی محصول۱	FPT_TST_EXT.1.1
۳۴	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۳۵	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۳۶	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۳۷	مهرهای زمانی معتبر ۱	FPT_STM_EXT.1.1
۳۸	مهرهای زمانی معتبر ۲	FPT_STM_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۳۹	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۴۰	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۴۱	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۴۲	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
۴۳	کانال امن ۱	FTP_ITC.1.1
۴۴	کانال امن ۲	FTP_ITC.1.2
۴۵	کانال امن ۳	FTP_ITC.1.3
۴۶	مسیر امن ۱/ مدیر	FTP_TRP.1.1/Admin
۴۷	مسیر امن ۲/ مدیر	FTP_TRP.1.2/Admin
۴۸	مسیر امن ۳/ مدیر	FTP_TRP.1.3/Admin
۴۹	فیلترینگ حالتمند ۱	FFW_RUL_EXT.1.1
۵۰	فیلترینگ حالتمند ۲	FFW_RUL_EXT.1.2
۵۱	فیلترینگ حالتمند ۳	FFW_RUL_EXT.1.3
۵۲	فیلترینگ حالتمند ۴	FFW_RUL_EXT.1.4
۵۳	فیلترینگ حالتمند ۵	FFW_RUL_EXT.1.5
۵۴	فیلترینگ حالتمند ۶	FFW_RUL_EXT.1.6
۵۵	فیلترینگ حالتمند ۷	FFW_RUL_EXT.1.7
۵۶	فیلترینگ حالتمند ۸	FFW_RUL_EXT.1.8
۵۷	فیلترینگ حالتمند ۹	FFW_RUL_EXT.1.9
۵۸	فیلترینگ حالتمند ۱۰	FFW_RUL_EXT.1.10
۵۹	کارکرد IPS مبتنی بر رفتار غیرعادی ۱	IPS_ABD_EXT.1.1
۶۰	کارکرد IPS مبتنی بر رفتار غیرعادی ۲	IPS_ABD_EXT.1.2
۶۱	کارکرد IPS مبتنی بر رفتار غیرعادی ۳	IPS_ABD_EXT.1.3
۶۲	بلوکه کردن آدرس IP ۱	IPS_IPB_EXT.1.1
۶۳	بلوکه کردن آدرس IP ۲	IPS_IPB_EXT.1.2
۶۴	تحلیل ترافیک شبکه ۱	IPS_NTA_EXT.1.1
۶۵	تحلیل ترافیک شبکه ۲	IPS_NTA_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۶۶	تحلیل ترافیک شبکه ۳	IPS_NTA_EXT.1.3
۶۷	کارکرد IPS مبتنی بر امضاء ۱	IPS_SBD_EXT.1.1
۶۸	کارکرد IPS مبتنی بر امضاء ۲	IPS_SBD_EXT.1.2
۶۹	کارکرد IPS مبتنی بر امضاء ۳	IPS_SBD_EXT.1.3
۷۰	کارکرد IPS مبتنی بر امضاء ۴	IPS_SBD_EXT.1.4
۷۱	کارکرد IPS مبتنی بر امضاء ۵	IPS_SBD_EXT.1.5
الزامات مربوط به پیوست یک		
۷۲	ذخیره‌سازی رویدادهای ممیزی **محافظت شده** ۱	FAU_STG.1.1
۷۳	ذخیره‌سازی رویدادهای ممیزی **محافظت شده** ۲	FAU_STG.1.2
۷۴	شمارش داده‌های ممیزی از دست رفته	FAU_STG_EXT.2.1/LocSpace
۷۵	نمایش هشدار برای فضای ذخیره‌سازی محلی	FAU_STG.3.1/LocSpace
۷۶	تائید گواهینامه X509 (۱)	FIA_X509_EXT.1.1/ITT
۷۷	تائید گواهینامه X509 (۲)	FIA_X509_EXT.1.2/ITT
۷۸	حفاظت از انتقال داخلی داده‌های اساسی محصول	FPT_ITT.1.1
۷۹	مسیر امن Join /۱	FTP_TRP.1.1/Join
۸۰	مسیر امن Join /۲	FTP_TRP.1.2/Join
۸۱	مسیر امن Join /۳	FTP_TRP.1.3/Join
۸۲	مدیریت رفتار توابع امنیتی/خدمات	FMT_MOF.1.1/Services
۸۳	مدیریت داده‌های محصول ۱	FMT_MTD.1.1/CryptoKeys
۸۴	حفاظت از انتقال داخلی داده‌های اساسی محصول	FPT_ITT.1.1
۸۵	مسیر امن Join/۱	FTP_TRP.1.1/Join
۸۶	مسیر امن Join/۲	FTP_TRP.1.2/Join
۸۷	مسیر امن Join/۳	FTP_TRP.1.3/Join
۸۸	حفظ وضعیت امن در زمان شکست ۱/ فضای ذخیره‌سازی ممیزی محلی	FPT_FLS.1.1/LocSpace
۸۹	تعریف کانال ثبت مؤلفه ۱	FCO_CPC_EXT.1.1
۹۰	تعریف کانال ثبت مؤلفه ۲	FCO_CPC_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۹۱	تعریف کانال ثبت مؤلفه ۳	FCO_CPC_EXT.1.3
۹۲	فیلترینگ حالتمند پروتکل‌های پویا	FFW_RUL_EXT.2.1
الزامات مربوط به پیوست دوم		
۹۳	محل ذخیره‌سازی داده‌های ممیزی IPS/۱	FAU_STG_EXT.1.1
۹۴	محل ذخیره‌سازی داده‌های ممیزی IPS/۲	FAU_STG_EXT.1.2
۹۵	محل ذخیره‌سازی داده‌های ممیزی IPS/۷	FAU_STG_EXT.4.1
۹۶	مدیریت رفتار توابع امنیتی IPS ۱	FMT_MOF.1.1
۹۷	مدیریت داده‌های محصول IPS ۱	FMT_MTD.1.1
۹۸	حفظ وضعیت امن در زمان شکست IPS/۱	FPT_FLS.1.1
۹۹	انتقال داده‌های امنیتی در داخل محصول ۱	FPT_ITT.1.1
۱۰۰	تخصیص منابع IPS/۱	FRU_RSA.1.1
۱۰۱	نرمال‌سازی ترافیک ۱	IPS_SBD_EXT.2.1
۱۰۲	نرمال‌سازی ترافیک ۲	IPS_SBD_EXT.2.2
۱۰۳	نرمال‌سازی ترافیک ۳	IPS_SBD_EXT.2.3
الزامات مربوط به پیوست سوم		
۱۰۴	تولید داده ممیزی ۱	FAU_GEN_EXT.1.1
۱۰۵	محل ذخیره‌سازی داده‌های ممیزی حفاظت شده	FAU_STG_EXT.3.1
۱۰۶	محل ذخیره‌سازی داده ممیزی ۴	FAU_STG_EXT.4.1
۱۰۷	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
۱۰۸	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2
۱۰۹	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3
۱۱۰	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
۱۱۱	الزامات پروتکل DTLS Client / احراز هویت (۱)	FCS_DTLSC_EXT.2.1
۱۱۲	الزامات پروتکل DTLS Client / احراز هویت (۲)	FCS_DTLSC_EXT.2.2
۱۱۳	الزامات پروتکل DTLS Client / احراز هویت (۳)	FCS_DTLSC_EXT.2.3
۱۱۴	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1
۱۱۵	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۱۶	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
۱۱۷	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
۱۱۸	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
۱۱۹	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
۱۲۰	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
۱۲۱	الزامات پروتکل DTLS Server / احراز هویت متقابل (۱)	FCS_DTLSS_EXT.2.1
۱۲۲	الزامات پروتکل DTLS Server / احراز هویت متقابل (۲)	FCS_DTLSS_EXT.2.2
۱۲۳	الزامات پروتکل DTLS Server / احراز هویت متقابل (۳)	FCS_DTLSS_EXT.2.3
۱۲۴	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۱۲۵	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۱۲۶	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۱۲۷	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۱۲۸	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۱۲۹	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۱۳۰	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۱۳۱	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۱۳۲	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۱۳۳	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۱۳۴	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۱۳۵	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۱۳۶	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۱۳۷	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۱۳۸	الزامات پروتکل NTP (۱)	FCS_NTP_EXT.1.1
۱۳۹	الزامات پروتکل NTP (۲)	FCS_NTP_EXT.1.2
۱۴۰	الزامات پروتکل NTP (۳)	FCS_NTP_EXT.1.3
۱۴۱	الزامات پروتکل NTP (۴)	FCS_NTP_EXT.1.4
۱۴۲	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۱۴۳	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۴۴	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۱۴۵	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۱۴۶	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۱۴۷	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۱۴۸	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۱۴۹	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۱۵۰	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۱۵۱	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۱۵۲	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۱۵۳	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۱۵۴	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۱۵۵	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۱۵۶	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3
۱۵۷	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۱۵۸	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۱۵۹	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۱۶۰	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۱۶۱	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8
۱۶۲	الزامات پروتکل TLS Client ۱	FCS_TLSC_EXT.1.1
۱۶۳	الزامات پروتکل TLS Client ۲	FCS_TLSC_EXT.1.2
۱۶۴	الزامات پروتکل TLS Client ۳	FCS_TLSC_EXT.1.3
۱۶۵	الزامات پروتکل TLS Client ۴	FCS_TLSC_EXT.1.4
۱۶۶	الزامات پروتکل TLS Client/ احراز هویت ۱	FCS_TLSC_EXT.2.1
۱۶۷	الزامات پروتکل TLS Server ۱	FCS_TLSS_EXT.1.1
۱۶۸	الزامات پروتکل TLS Server ۲	FCS_TLSS_EXT.1.2
۱۶۹	الزامات پروتکل TLS Server ۳	FCS_TLSS_EXT.1.3
۱۷۰	الزامات پروتکل TLS Server ۴	FCS_TLSS_EXT.1.4

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۷۱	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۷۲	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۲	FCS_TLSS_EXT.2.2
۱۷۳	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۳	FCS_TLSS_EXT.2.3
۱۷۴	اعتبارسنجی گواهینامه X509 (۱)	FIA_X509_EXT.1.1/Rev
۱۷۵	اعتبارسنجی گواهینامه X509 (۲)	FIA_X509_EXT.1.2/Rev
۱۷۶	احراز هویت گواهینامه X509 (۱)	FIA_X509_EXT.2.1
۱۷۷	احراز هویت گواهینامه X509 (۲)	FIA_X509_EXT.2.2
۱۷۸	درخواست‌های گواهینامه X509 (۱)	FIA_X509_EXT.3.1
۱۷۹	درخواست‌های گواهینامه X509 (۲)	FIA_X509_EXT.3.2
۱۸۰	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۸۱	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۸۲	الزامات به‌روزرسانی امن ۶	FPT_TUD_EXT.2.3
۱۸۳	الزامات به‌روزرسانی امن ۷	FPT_TUD_EXT.2.4
۱۸۴	مدیریت رفتار توابع امنیتی/ به‌روزرسانی خودکار ۱	FMT_MOF.1.1/AutoUpdate
۱۸۵	مدیریت رفتار توابع امنیتی/ به‌روزرسانی خودکار ۲	FMT_MOF.1.1/Functions
۱۸۶	مدیریت رفتار توابع امنیتی/خدمات ۱	FMT_MOF.1.1/Services
۱۸۷	مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱	FMT_MTD.1.1/CryptoKeys

۱-۴ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات عمدی و غیرعمدی موجود در زمینه پیکربندی و/یا کارکرد سیستم را در اختیاردارند، محصول باید این قابلیت را داشته باشد که داده‌های ممیزی موردنیاز برای تشخیص چنین فعالیت‌هایی را تولید نماید. ممیزی فعالیت‌های مدیریت سیستم سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سیستم، می‌توان برای طراحی اقدامات اصلاحی از آن‌ها استفاده کرد. ممیزی رویدادهای گزینش‌شده نشان می‌دهد که آیا بخش‌هایی مهم محصول مورد ارزیابی در معرض شکست قرار دارند یا خیر (مثلاً این‌که فرایند رمزنگاری اجرا نشود) و همچنین به شناسایی فعالیت‌های غیرمعمول (مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم) یک مورد مشکوک، کمک می‌کند. در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به‌اندازه‌ای زیاد شود که محصول مورد ارزیابی یا راهبران مسئول بازبینی این اطلاعات را دچار سردرگمی‌کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت مورد اعتماد خارجی ارسال کند. این اطلاعات باید دارای مهرهای زمانی قابل‌اعتماد باشند، این امر سبب می‌شود که بتوان اطلاعات را پس از ارسال به دستگاه‌های خارجی مرتب کرد. از دست رفتن ارتباط با سرور ممیزی می‌تواند مشکل‌ساز شود. هر چند که راه‌های مختلفی برای کاهش این تهدید وجود دارد، اما این پروفایل حفاظتی هیچ اقدام خاصی را الزام نمی‌کند. مناسب بودن محصول مورد ارزیابی در یک محیط خاص، متأثر از میزان حفاظت از اطلاعات ممیزی با این اقدامات و توانایی محصول مورد ارزیابی برای انجام کارکردهای خود در اثر انجام اقدامات مذکور است.

از محصول مورد ارزیابی دستگاه‌های شبکه انتظار نمی‌رود که تمام داده‌های ممیزی را ذخیره کند. هرچند که لازم است داده‌ها به‌صورت محلی در زمان تولید ذخیره شوند و در صورت تجاوز از ظرفیت ذخیره‌سازی، اقدامات مقتضی صورت گیرند، محصول مورد ارزیابی همچنین باید بتواند یک لینک امن را با یک سرور ممیزی خارجی ایجاد کند تا بتوان داده‌های ممیزی خارجی را ذخیره کرد.

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**
توابع امنیتی هدف ارزیابی باید بتواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند: الف) آغاز و اتمام توابع ممیزی؛ ب) تمام اقدامات مدیریتی شامل موارد زیر: • ورود و خروج مدیریتی (درصورتی‌که مدیران نیاز به‌حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)	

- تغییرات امنیتی در پیکربندی (علاوه بر اطلاعات حاکی از تغییرات رخداده، باید ثبت 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 باید ثبت شود)
- تغییر کلمه عبور (نام حساب کاربری مربوطه نیز باید ثبت شود)
- شروع و پایان توابع IPS
- تمام رویدادهای قابل ممیزی IPS برای سطح مشخص‌نشده‌ای از ممیزی
- همه رویدادهای متفاوت IPS
- همه واکنش‌های متفاوت IPS
- تعداد رویدادهای مشابه که در واحد زمان مشخص روی داده است
- تعداد اقدامات مشابهی که در واحد زمان مشخص روی داده است.
- انتخاب: [هیچ اقدام دیگر، اختصاص: [لیست سایر کاربردهای ویژه]]؛

ت) انتخاب: [اختصاص لیست رویدادهای قابل ممیزی تعریف شده در ستون دوم جدول زیر.

نام خانواده	رویدادهای قابل ممیزی	موارد اضافی‌تر
FAU_GEN.1	هیچ	
FAU_GEN.2	هیچ	
FAU_STG_EXT.1	هیچ	
FCS_CKM.1	هیچ	
FCS_CKM_EXT.4	هیچ	
FCS_COP.1(1)	هیچ	
FCS_COP.1(2)	هیچ	
FCS_COP.1(3)	هیچ	
FCS_COP.1(4)	هیچ	
FCS_RBG_EXT.1	هیچ	
FDP_RIP.2	هیچ	
FIA_PMG_EXT.1	هیچ	
FIA_UIA_EXT.1	همه مواردی که از سازوکار شناسایی و احراز هویت استفاده می‌کنند.	ارائه کردن شناسه کاربری، مبدأ تلاش (به طور مثال IP address)
FIA_UAU_EXT.2	همه مواردی که از سازوکارهای احراز هویت استفاده می‌کنند.	مبدأ تلاش (به طور مثال IPaddress)

FIA_UAU.7	هیچ	
FIA_X509_EXT.1	تلاش ناموفق برای اعتبار سنجی یک گواهینامه	دلیل ناموفق بودن و شکست خوردن
FIA_X509_EXT.2	هیچ	
FIA_X509_EXT.3	هیچ	
FMT_MOF.1(1)/ TrustedUpdate	هرگونه تلاش برای شروع یک به‌روزرسانی دستی	هیچ
FMT_MTD.1	هیچ	
FMT_SMF.1	هیچ	
FMT_SMR.2	هیچ	
FPT_SKP_EXT.1	هیچ	
FPT_APW_EXT.1	هیچ	
FPT_TST_EXT.1	هیچ	
FPT_TUD_EXT.1	شروع به‌روزرسانی؛ نتیجه تلاش به‌روزرسانی (موفقیت یا شکست)	هیچ اطلاعات اضافه دیگری
FPT_STM.1	تغییرات زمانی	مقادیر جدید و قدیم برای زمان مبدأ تلاش (به طور مثال IP address)
FPT_TST_EXT.1	هیچ	
FTA_SSL_EXT.1	هرگونه تلاش در باز کردن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
FTA_SSL.3	پایان دادن به نشست راه دور توسط سازوکارهای قفل نمودن نشست	بدون هیچ اطلاعات اضافه
FTA_SSL.4	پایان دادن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
FTA_TAB.1	هیچ	
FTP_ITC.1	راه‌اندازی یک کانال امن پایان کانال امن شکست در عملکرد کانال امن	شناسایی راه‌انداز و مقصد تلاشی که در برقراری یک کانال امن، با شکست مواجه شده است.
FTP_TRP.1	راه‌اندازی یک کانال امن پایان کانال امن شکست در عملکرد مسیر امن	شناسایی، شناسه کاربری ادعا شده

نکته کاربردی:

در صورتی که لیست «اقدامات مدیریتی» ناقص به نظر می‌رسد، باید از «اختصاص» درون «انتخاب» برای لیست اقدامات مدیریتی ممیزی شده اضافی استفاده کرد. نویسنده سند هدف امنیتی، جدول رویدادهای ممیزی متناظر را با اختصاص متناظر برای سند هدف امنیتی جایگزین می‌کند. همچنین ممکن است شامل قسمت‌های مربوط به نکته کاربردی ۳ و جدول ۳، برای SFR های انتخابی یا اختیاری درون سند هدف امنیتی باشد.

برای هدف‌های ارزیابی توزیع شده، هر مؤلفه باید یک رکورد ممیزی برای هر یک از SFR هایی که آن را پیاده‌سازی کرده است تولید کند. اگر در زمان triggered یک رویداد ممیزی، بیش از یک کامپوننت هدف ارزیابی درگیر باشد، باید رویداد روی هر کامپوننت ممیزی شود. (مثال: در طول تلاش برای برقراری کانال ارتباطات امن بین دو مؤلفه، رد ارتباط توسط یک مؤلفه باید منجر به رویداد ممیزی تولید شده توسط هر دو مؤلفه شود.) این موارد محدود به خطاها نیستند بلکه شامل رویدادهایی درباره اقدامات موفقی مانند ایجاد/قطع موفق یک کانال ارتباطی امن بین مؤلفه‌های هدف ارزیابی نیز هستند.

نکته کاربردی:

نویسنده سند هدف امنیتی می‌تواند سایر رویدادهای قابل ممیزی را به طور مستقیم در جدول قرار دهد. آن‌ها (رویدادهای قابل ممیزی) محدود به لیست ارائه شده نیستند.

TSS باید تعیین کند که چه اطلاعاتی برای شناسایی کلیدهای مرتبط به وظایف مدیریتی تولید، واردکردن، تغییر یا پاک کردن کلیدهای رمزنگاری، ثبت شده‌اند.

مطابق FAU_GEN.1.1 اصطلاح «سرویس‌ها» به ارتباطات صورت‌گرفته از طریق کانال امن و مسیر امن، در خودآزمایی‌های درخواست شده، به‌روزرسانی امن و نشست‌های مدیریتی سیستم اشاره دارد. (که در مسیر قابل اعتماد وجود داشته باشد) (مانند netconf). اگر سند هدف امنیتی شامل شاخص انتخابی SFR FMT_MOF.1/Services باشد، لازم است گزینه "آغاز و اتمام سرویس‌ها" از انتخاب‌های موجود در FAU_GEN.1.1 انتخاب شود.

نکته کاربردی مربوط به IPS

نویسنده سند هدف امنیتی برای لیست رویدادهای ممیزی در سند هدف امنیتی تنها به موارد ذکر شده در این الزام محدود نمی‌گردد و باید «جدول رویدادها» ذکر شده در الزام ۲ را با اطلاعات اضافه‌تر به‌روزرسانی کند. نویسنده EP باید از FAU_GEN.1 که بر اساس pp برای توابع ممیزی استاندارد تعریف شده است (داده غیر IPS)، استفاده کند.

رویدادهای غیرمشابه آن دسته از رویدادهای هستند که بغیر از زمان از نظر سایر ویژگی‌های دیگر نیز متفاوت هستند.

رویدادهای مشابه آن دسته از رویدادهای را شامل می‌شود که در یک بازه زمانی روی و دارای ویژگی مشابه هستند ولی تنها زمان آن‌ها متفاوت است. برای مثال، مورد انتظار نیست که محصول پیام ممیزی منحصربفردی برای هر رویداد از همان نوع که در مدت زمان معقولی رخ می‌دهد، تولید کند. (توابع امنیتی هدف ارزیابی فقط نیاز دارد یک پیام ممیزی برای یک رویداد که X دفعه در طول Y ثانیه رخ می‌دهد، تولید کند.)

۲	تولید داده ممیزی ۲

توابع امنیتی هدف ارزیابی باید در هر یک از سوابق ممیزی، دست‌کم اطلاعات زیر را ثبت 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 مؤلفه‌های کارکردی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات ستون سوم در جدول زیر مشخص‌شده است.

نام خانواده	رویدادهای قابل ممیزی	موارد اضافی‌تر
FAU_GEN.1	هیچ	
FAU_GEN.2	هیچ	
FAU_STG_EXT.1	هیچ	
FCS_CKM.1	هیچ	
FCS_CKM_EXT.4	هیچ	
FCS_COP.1(1)	هیچ	
FCS_COP.1(2)	هیچ	
FCS_COP.1(3)	هیچ	
FCS_COP.1(4)	هیچ	
FCS_RBG_EXT.1	هیچ	
FDP_RIP.2	هیچ	
FIA_PMG_EXT.1	هیچ	
FIA_UIA_EXT.1	همه مواردی که از سازوکار شناسایی و احراز هویت استفاده می‌کنند.	ارائه کردن شناسه کاربری، مبدأ تلاش (به طور مثال IP address)
FIA_UAU_EXT.2	همه مواردی که از سازوکارهای احراز هویت استفاده می‌کنند.	مبدأ تلاش (به طور مثال IPaddress)
FIA_UAU.7	هیچ	
FIA_X509_EXT.1	تلاش ناموفق برای اعتبار سنجی یک گواهینامه	دلیل ناموفق بودن و شکست خوردن
FIA_X509_EXT.2	هیچ	
FIA_X509_EXT.3	هیچ	
FMT_MOF.1(1)/ TrustedUpdate	هرگونه تلاش برای شروع یک به‌روزرسانی دستی	هیچ
FMT_MTD.1	هیچ	

[۱] Subject

FMT_SMF.1	هیچ	
FMT_SMR.2	هیچ	
FPT_SKP_EXT.1	هیچ	
FPT_APW_EXT.1	هیچ	
FPT_TST_EXT.1	هیچ	
FPT_TUD_EXT.1	شروع به‌روزرسانی؛ نتیجه تلاش به‌روزرسانی (موفقیت یا شکست)	هیچ اطلاعات اضافه دیگری
FPT_STM.1	تغییرات زمانی	مقادیر جدید و قدیم برای زمان مبدأ تلاش (به طور مثال IP address)
FPT_TST_EXT.1	هیچ	
FTA_SSL_EXT.1	هرگونه تلاش در باز کردن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
FTA_SSL.3	پایان دادن به نشست راه دور توسط سازوکارهای قفل نمودن نشست	بدون هیچ اطلاعات اضافه
FTA_SSL.4	پایان دادن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
FTA_TAB.1	هیچ	
FTP_ITC.1	راه‌اندازی یک کانال امن پایان کانال امن شکست در عملکرد کانال امن	شناسایی راه‌انداز و مقصد تلاشی که در برقراری یک کانال امن، با شکست مواجه شده است.
FTP_TRP.1	راه‌اندازی یک کانال امن پایان کانال امن شکست در عملکرد مسیر امن	شناسایی، شناسه کاربری ادعا شده

در مورد هر یک از انواع رویدادهای ممیزی IPS و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات مشخص‌شده در جدول زیر:

نام الزام	رویدادهای ممیزی	اطلاعات اضافه رکوردهای ممیزی
مدیریت کارکرد در محصول IPS ۱(الزام شماره ۵۴)	تغییرات در المان‌های خط و مشی‌های IPS	شناسه‌ها یا نام المان‌های خط و مشی‌های IPS تغییر یافته (به عنوان نمونه کدام امضاء، مبنا، لیست‌های سیاه و سفید تغییر داده شده است)
کارکرد IPS مبتنی بر رفتار غیرعادی (الزامات شماره	ترافیک بازرسی شده که با خط‌مشی IPS مبتنی بر رفتار غیرعادی انطباق	آدرس‌های IP مبدأ و مقصد
		محتوای فیلدهای سرآیند که با خط‌مشی‌های

۷۴ تا ۷۶)	دارد.	مشخص شده انطباق دارد.
		واسطی که از آن بسته دریافت شده است.
		جنبه‌هایی از خط‌مشی‌های 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 آدرس IP۱(الزامات شماره ۷۷ و ۷۸)	انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا	آدرس‌های IP مبدأ و مقصد (و در صورت امکان، نشانه‌ای دال بر این‌که 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 شبکه۱ (الزام شماره ۷۹)	تغییر این‌که کدام خط‌مشی‌های پیشگیری از نفوذ روی واسط محصول فعال هستند. فعال کردن و غیرفعال کردن واسط محصول که خط‌مشی‌های پیشگیری از نفوذ روی آن اعمال شده‌اند. تغییر این‌که کدام مُدها روی واسط محصول فعال هستند.	شناسایی واسط محصول
		خط‌مشی پیشگیری از نفوذ و مد واسط (در صورت امکان)
کارکرد IPS مبتنی بر امضاء۱ (الزام شماره ۸۲)	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)
نرمال‌سازی ترافیک ۱ (اختیاری-الزام شماره ۱۱۲)	بازرسی بسته‌های کپسوله‌شده	شناسایی روش کپسوله‌سازی
نرمال‌سازی ترافیک ۲ (اختیاری-الزام شماره ۱۱۳)	شکست در سر هم کردن مجدد بسته‌های چندتکه‌ای[۱]	آدرس‌های IP مبدأ و مقصد
		واسط محصول که تکه‌ها[۲] را دریافت کرده است.
نرمال‌سازی ترافیک ۳ (اختیاری-الزام شماره ۱۱۴)	نرمال‌سازی ترافیک توسط محصول	آدرس‌های IP مبدأ و مقصد بسته‌های کنار گذاشته‌شده[۳]
		واسط محصول که بسته‌ها را دریافت کرده است

نکته کاربردی:

رویدادهای ممیزی اضافی دیگر بر اساس الزامات اختیاری و انتخابی برگرفته‌شده از پیوست‌های یک و دو به محصول مورد ارزیابی اعمال می‌شود؛ بنابراین، نویسنده هدف امنیتی باید رویدادهای اضافی مشخص‌شده مربوطه در جدول‌های ۲ و ۳ را اضافه نماید.

۳	**تولید داده ممیزی ۳**

در مورد آن دسته از رویدادهای ممیزی که حاصل اقدامات کاربران احرازهویت‌شده هستند، توابع امنیتی هدف ارزیابی باید بتواند هر رویداد قابل ممیزی را با هویت کاربری که مسبب آن رویداد شده است، مرتبط سازد.

نکته کاربردی:

زمانی که یک رویداد ممیزی توسط مؤلفه دیگری triggered شده باشد، مؤلفه‌ای که رویدادها را ثبت می‌کند باید رویداد را با آن شناسه آغازگر مؤلفه که باعث رویداد شده است، مرتبط کند. (فقط برای اهداف ارزیابی توزیع شده اعمال می‌شود.)

۴	**محل ذخیره‌سازی داده‌های ممیزی ۱**

توابع امنیتی هدف ارزیابی باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال مورد اعتماد مطابق با FTP_ITC.1 باشد.

---

[۱] Fragmented packets
[۲] Fragments
[۳] Discarded packets

نکته کاربردی:

برای انتخاب گزینه انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به‌جز سرور محصول مورد ارزیابی متکی است. در این مورد ذخیره‌سازی، توسط محیط عملیاتی صورت می‌گیرد.

تا زمانی که سرور ممیزی خارجی بخشی از هدف ارزیابی نباشد، به جز قابلیت‌های انتقال داده ممیزی FTP_ITC.1، هیچ الزامی برای آن وجود ندارد. هیچ الزامی برای قالب یا اساس پروتکل داده‌های ممیزی که منتقل می‌شوند وجود ندارد. هدف ارزیابی باید قادر به پیکربندی برای انتقال داده‌های ممیزی به موجودیت IT خارجی بدون مداخله مدیر باشد. انتقال دستی نیازمندی‌ها را برآورده نخواهد کرد. انتقال می‌تواند در زمان واقعی یا به صورت دوره‌ای انجام شود. اگر انتقال در زمان واقعی انجام نشود، TSS شرح می‌دهد که باید چه رویدادی برای انتقال ایجاد شود و چه محدوده‌ای از فرکانس‌های هدف ارزیابی برای ایجاد انتقال داده‌های ممیزی به سرور ممیزی پشتیبانی می‌شود. همچنین TSS فرکانس‌های قابل‌قبولی برای انتقال پیشنهاد می‌دهد.

برای هدف‌های ارزیابی توزیع‌شده، هر مؤلفه باید به طور مناسبی قادر به استخراج داده ممیزی از طریق کانال محافظت شده خارجی (FTP_ITC.1) یا بین مؤلفه‌ای (FPT_ITT.1 یا FTP_ITC.1) باشد. حداقل یک مؤلفه از هدف ارزیابی باید قادر به استخراج سوابق ممیزی از طریق FTP_ITC.1 باشد تا تمامی سوابق ممیزی هدف ارزیابی را بتوان برای موجودیت IT خارجی استخراج کرد.

۵	**محل ذخیره‌سازی داده‌های ممیزی ۲**

محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.

[انتخاب:

- هدف ارزیابی شامل تنها یک جزء مستقل است که داده‌های ممیزی را به‌صورت محلی ذخیره می‌کند.
- هدف ارزیابی باید یک هدف ارزیابی توزیع شده باشد که داده‌های ممیزی را روی اجزاء هدف ارزیابی زیر ذخیره می‌کند: [اختصاص: شناسایی اجزاء هدف ارزیابی
- هدف ارزیابی یک هدف ارزیابی توزیع شده با ذخیره داده‌های ممیزی است که به صورت خارجی برای اجزای هدف ارزیابی زیر ارائه شده است. [اختصاص: لیستی از مؤلفه‌های هدف ارزیابی که داده‌های ممیزی را به‌صورت محلی ذخیره نمی‌کنند و سایر اجزای هدف ارزیابی که داده‌های ممیزی تولید شده خود را به آن‌ها منتقل می‌کنند].

نکته کاربردی:

If the TOE is a standalone TOE (i.e. not a distributed TOE) the option 'The TOE shall consist of a single standalone component that stores audit data locally' shall be selected. If the TOE is a distributed TOE the option 'The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components]' shall be selected and the TOE components which store audit data locally shall be listed in the assignment. Since all TOEs are required to provide functions to store audit data locally this option needs to be selected for all distributed TOEs. In addition, FAU_GEN_EXT.1 and FAU_STG_EXT.3 shall be claimed in the ST. If the distributed TOE consists only of

components which are storing audit data locally, it is sufficient to select only the option 'The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components]' and add FAU_GEN_EXT.1 and FAU_STG_EXT.3.
If the TOE is a distributed TOE and some TOE components are not storing audit data locally, the option 'The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data]' shall be selected in addition to the option 'The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components]'. In that case FAU_STG_EXT.4 shall be claimed in the ST in addition to FAU_GEN_EXT.1 and FAU_STG_EXT.3. For the option 'The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data]' the TOE components that to not store audit data locally shall be mapped to the TOE components to which they transmit their generated audit data.
For distributed TOEs this SFR can be fulfilled either by every TOE component storing its own security audit data locally or by one or more TOE components storing audit data locally and other TOE components which are not storing audit information locally sending security audit data to other TOE components for local storage. For the transfer of security audit data between TOE components a protected channel according to FTP_ITC.1 or FPT_ITT.1 shall be used. The TSS shall describe which TOE components store security audit data locally and which TOE components do not store security audit data locally. For the latter, the TSS shall describe at which other TOE component the audit data is stored locally.

۶	**محل ذخیره‌سازی داده‌های ممیزی ۳**

درصورتی‌که فضای حافظه محلی داده ممیزی پرشده باشد، محصول مورد ارزیابی باید [انتخاب: داده‌های ممیزی جدید را کنار بگذارد، سوابق ممیزی گذشته را بر اساس این قوانین بازنویسی[۱] کند: [اختصاص: قوانین بازنویسی سوابق ممیزی گذشته]، [اختصاص: اقدامات دیگر]].

نکته کاربردی:

درصورتی‌که فضای حافظه محلی پرشده باشد، سرور خارجی ثبت رویدادها[۲] می‌تواند به‌عنوان فضای ذخیره‌سازی جایگزین مورداستفاده قرار گیرد. «اقدامات دیگر» (که در بخش «اختصاص» ذکرشده است)، می‌تواند مواردی ازجمله «ارسال داده‌های ممیزی جدید به یک موجودیت IT خارجی» را شامل شود.

[۱] Overwrite
[۲] External log server

برای اهداف ارزیابی توزیع شده، ذخیره محلی داده ممیزی تولید شده برای هر مؤلفه الزامی نیست ولی لازم است هدف ارزیابی کلی بتواند داده‌های ممیزی را به صورت محلی ذخیره کند. برای اطمینان از حفاظت سوابق ممیزی در موارد خطای ارتباط شبکه، هر مؤلفه باید حداقل بتواند اطلاعات ممیزی محلی را به طور موقت بافر کند. (برای جزئیات بیشتر به بخش ۶,۳,۳ مراجعه کنید). بافر محلی اطلاعات ممیزی لزوماً شامل حافظه غیر فرار نیست و اطلاعات ممیزی را می‌توان در حافظه فرار ذخیره نمود. هرچند، مفهوم ذخیره‌سازی محلی اطلاعات ممیزی در FAU_STG_EXT.1.3 نیازمند ذخیره‌سازی در حافظه غیر فرار است. رفتار هر مؤلفه‌ای که ذخیره‌سازی اطلاعات ممیزی را انجام می‌دهد، در زمانی که حافظه محلی در آستانه پر شدن باشد باید شرح داده شود. لازم است برای تمامی مؤلفه‌هایی که اطلاعات ممیزی را به جای ذخیره‌سازی محلی در خود، بافر می‌کنند شرح داده شود که در صورت رسیدن فضای بافر به آستانه پر شدن چه اتفاقی می‌افتد.

۲-۴ پشتیبانی رمزنگاری (FCS)

در این بخش، الزامات رمزنگاری مربوط به سایر ویژگی‌های امنیتی محصول مورد ارزیابی تعریف می‌شوند. این الزامات شامل تولید کلید و تولید بیت تصادفی، روش‌های استقرار کلید[۱]، نابودی کلید و انواع مختلف عملیات رمزنگاری برای رمزگذاری و رمزگشایی AES، تائید امضا، تولید درهم‌ساز و تولید درهم‌ساز کلید گذاری شده[۲] هستند. این الزامات کارکرد امنیتی، از پیاده‌سازی الزامات مبتنی بر انتخاب و پروتکل لیست شده در پیوست دو پشتیبانی می‌کنند.

شماره الزام	نام الزام	
۷	**مدیریت کلید رمزنگاری ۱**	**FCS_CKM.1.1**

محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری مشخص‌شده، کلیدهای رمزنگاری نامتقارن را تولید کند: [انتخاب:

- الگوهای RSA با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.3؛
- الگوهای ECC با استفاده از «منحنی‌های NIST» [انتخاب: P-256, P-384, P-521] بر اساس این الزامات: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.4.
- الگوهای FFC با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.1.

رویه‌های FFC از Diffie-Hellman گروه ۱۴ استفاده می‌کند که موارد زیر را برآورده می‌کند: (RFC 3526، بخش ۳)

نکته کاربردی:

نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورد استفاده برای استقرار کلید و احراز هویت دستگاه‌ها را انتخاب می‌کند. درصورتی‌که برای استقرار کلید از تولید کلید استفاده شود، الگوی در «مدیریت کلید رمزنگاری ۲» و پروتکل‌های رمزنگاری انتخاب‌شده باید مطابق با انتخاب باشند. درصورتی‌که برای احراز هویت دستگاه‌ها از تولید کلید استفاده شود، به غیر از *ssh-rsa*، *ecdsa-sha2-nistp256*، *ecdsasha2-nistp384* و *ecdsa-sha2-nistp521*، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی‌نامه X.509v3 باشد.

اگر محصول مورد ارزیابی به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند و برای پشتیبانی از احراز هویت دوطرفه پیکربندی نشده باشد، نیازی نیست که هدف ارزیابی، تولید کلید را پیاده‌سازی نماید.

---

[۱] Key establishment

[۲] Keyed hash generation

شماره الزام	نام الزام	
در اهداف ارزیابی توزیع‌شده، اگر کامپوننت هدف ارزیابی به عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند، نیازی نیست که هدف ارزیابی تولید کلید را پیاده‌سازی نماید.		
۸	**مدیریت کلید رمزنگاری ۲**	**FCS_CKM.2.1**

محصول مورد ارزیابی باید استقرار کلید[۱] رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام دهد: [انتخاب:

- الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: شماره ویژه NIST 800-56B، مرور 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: شماره ویژه NIST 800-56A، مرور۲ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۴]؛
- الگوهای استقرار کلید میدانی[۵] که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، مرور ۲ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته».
- الگوی استقرار کلید با استفاده از گروه ۱۴ Diffie-Hellman مطابق RFC 3526 بخش ۳.

نکته کاربردی:

این عنصر در واقع نسخه اصلاح شده الزام «مدیریت کلید رمزنگاری۲[۶]» در استاندارد ISO 15408 است که به‌جای توزیع کلید، به استقرار کلید می‌پردازد.

نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورداستفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. برای گروه ۱۴ *Diffie-Hellman*، نویسنده هدف امنیتی باید به جای استفاده از انتخاب استقرار کلید میدانی محدود، از SFR به طور متناظر انتخاب کند.

الگوهای استقرار کلید مبتنی بر RSA در بخش ۹ از نسخه ۱ NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های نسخه ۱ SP 800-56B است. اگر محصول مورد ارزیابی در الگوی استقرار کلید RSA به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، تولید کلید RSA را اجرا نماید.

منحنی‌های بیضوی مورداستفاده در الگوهای استقرار کلید، با منحنی‌های مشخص‌شده در الزام شماره‌ی ۷ «مدیریت کلید رمزنگاری ۱» ارتباط دارند.

---

[۱] Key establishment
[۲] Integer factorization cryptography
[۳] Elliptic curve-based
[۴] Discrete logarithm cryptography
[۵] Finite filed-based
[۶] FCS_CKM.2

شماره الزام	نام الزام	
پارامترهای دامنه مورداستفاده در الگوهای استقرار کلید میدانی، توسط تولید کلید مورداشاره در «مدیریت کلید رمزنگاری ۱» مشخص‌شده‌اند.		
۹	نابودی کلید رمزنگاری ۴	FCS_CKM.4.1

توابع امنیتی مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: [اختصاص:

- در مورد کلیدهای با متن ساده در ذخیره‌سازی فرار[۱]، نابودی باید از طریق [انتخاب: یک بازنویسی ساده و مستقیم شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، مقدار جدیدی از کلید، [اختصاص: مقداری ایستا یا پویا که شامل هیچ CSP نباشد.]] از بین بردن ارجاع مستقیم به کلید پس از درخواست جمع‌آوری مقادیر باقی مانده] انجام شود
- در مورد کلیدهای با متن ساده در ذخیره‌سازی غیر فرار، نابودی باید از طریق فراخوانی یک رابط ارائه شده توسط بخشی از توابع امنیتی هدف امنیتی که [انتخاب:
  - به طور منطقی محل ذخیره‌سازی کلید را تعیین کرده و [انتخاب: تنها، [اختصاص: تعداد انجام]-بار] بازنویسی شامل [انتخاب: یک الگوی شبه تصادفی با استفاده از RBG توابع امنیتی هدف ارزیابی، صفرها، یک‌ها، مقدار جدیدی از کلید، [اختصاص: یک مقدار استاتیک یا پویا که شامل هیچ CSP نباشد]] انجام دهد.
  - آموزش بخشی از توابع امنیتی هدف ارزیابی برای تخریب انتزاعی که نشان‌دهنده کلید است.

  ] باشد.

نکته کاربردی:

در بخش‌هایی از انتخاب‌ها که کلیدهای تخریب شده توسط "بخشی از TSF" شناسایی شده‌اند؛ TSS بخش مربوطه و رابط درگیر را تشخیص می‌دهد. رابطی که در این الزام مورد ارجاع قرار می‌گیرد، می‌تواند اشکال مختلفی برای اهداف ارزیابی داشته باشد که بیشتر مانند رابط برنامه‌نویسی برنامه کاربردی برای هسته سیستم‌عامل است. ممکن است سطوح مختلفی از abstraction مشاهده شود. برای مثال، در یک پیاده‌سازی داده شده، برنامه ممکن است به جزئیات فایل سیستم دسترسی داشته باشد و ممکن است بتواند به‌به طور منطقی محل حافظه خاصی را آدرس‌دهی نماید. در پیاده‌سازی دیگری، برنامه ممکن است مدیریت ساده‌ای روی منبعی داشته باشد و فقط بتواند از بخش دیگری از توابع امنیتی هدف ارزیابی مانند مترجم[۲] یا سیستم‌عامل درخواست حذف منبع کند.

در صورتی که برای کلیدهای مختلف و/یا وضعیت‌های تخریب مختلف، از روش‌های مختلف تخریب کلید استفاده شود،

[۱] Volatile memory

[۲] interpreter

شماره الزام	نام الزام	
وضعیت‌های متفاوت و کلیدها/روش‌های اعمال آن‌ها در TSS شرح داده می‌شود؛ و ممکن است سند هدف امنیتی برای کمک به وضوح بیشتر از تکرارهای مجزایی از SFR ها استفاده کند. TSS تمامی کلیدهای مرتبط مورد استفاده در پیاده‌سازی SFR ها، از جمله مواردی که کلیدها در فرم غیر متنی ذخیره می‌شوند را شرح می‌دهد. در مورد ذخیره‌سازی غیر متنی، روش رمزنگاری و کلید مرتبط-کلید رمزنگاری در TSS شناسایی می‌شوند. برخی انتخاب‌ها اجازه اختصاص "مقداری که شامل هیچ CSP نیست" می‌دهند. به این معنی است که هدف ارزیابی از برخی داده‌های مشخصی استفاده می‌کند که توسط RBG برای برآورده کردن نیازمندی‌های FCS_RBG_EXT در نظر گرفته نشده است و هیچ‌کدام از مقادیر خاص ذکر شده در گزینه‌های دیگر انتخاب نیست. عبارت "شامل هیچ CSP" برای اطمینان از انتخاب با دقت داده‌ها است و از منبعی عمومی که ممکن است شامل داده‌های حاضر یا قبلی که خود نیازمند حفظ محرمانگی هستند، گرفته نشده است. برای اجتناب از تردید: "کلیدهای رمزنگاری" در این SFR شامل کلیدهای نشست است. تخریب کلید بر روی مؤلفه‌های عمومی جفت کلید نامتقارن اعمال نمی‌شود.		
۱۰	**عملیات رمزنگاری ۱ (۱)**	FCS_COP.1.1/DataEncryption
توابع امنیتی مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص AES که در حالت [انتخاب: CBC، CTR، GCM] استفاده می‌شوند و در اندازه‌های کلید رمزنگاری [اختصاص: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] و با توجه به استاندارد AES که در ISO 18033-3 تعریف شده است، [انتخاب: CBC همان‌طور که در ISO 10116 مشخص‌شده است، CTR مشخص شده در ISO 10116، GCM همان‌طور که در ISO 19772 مشخص‌شده است]. انجام دهد. **نکته کاربردی:** در مورد نخستین انتخاب عملیات رمزنگاری ۱(۱)/رمزنگاری داده، نویسنده هدف امنیتی باید حالت یا حالت‌های کارکردی AES را انتخاب کند. در مورد دومین انتخاب، نویسنده هدف امنیتی باید اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[1] در الزامات کانال امن هستند.		
۱۱	**عملیات رمزنگاری ۱ (۲)**	FCS_COP.1.1/SigGen

[1] Cipher suite

شماره الزام	نام الزام

توابع امنیتی مورد ارزیابی باید خدمات امضای رمزنگاری (تولید و تائید) را بر اساس الگوریتم‌های رمزنگاری خاص ارائه کند: [انتخاب:

- الگوریتم امضای دیجیتال RSA و اندازه کلیدهای رمزنگاری (ماژول‌ها) [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر]
- الگوریتم امضای دیجیتال منحنی بیضوی و اندازه کلیدهای رمزنگاری [اختصاص: ۲۵۶ بیتی یا بزرگ‌تر]

]

با رعایت موارد زیر:

[انتخاب:

- در مورد الگوهای RSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵,۵، با استفاده از الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA_PKCS1v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳،
- در مورد الگوهای ECDSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، با اجرای منحنی‌های NIST [انتخاب: P-384، P-256، P-521، هیچ منحنی دیگر]؛ ISO/IEC 14888-3، بخش ۶,۴

]

نکته کاربردی:

نویسنده هدف امنیتی باید الگوریتم پیاده‌سازی شده برای اجرای امضای دیجیتال را انتخاب کند. نویسنده هدف امنیتی باید انتخاب‌ها/اختصاص‌های مناسبی به منظور مشخص نمودن پارامترهایی که برای الگوریتم پیاده‌سازی می‌شوند، ایجاد کند. نویسنده هدف امنیتی باید اطمینان حاصل نماید که اختصاص‌ها و انتخاب‌های این SFR شامل تمامی مقادیر پارامترهای ضروری برای مجموعه رمزهای منتخب در سند هدف امنیتی برای پروتکل SFR ها است. (پیوست B.2.1 را ببینید)

نویسنده سند هدف امنیتی انطباق انتخاب‌ها با سایر الزامات SFR، مخصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی می‌شود بررسی می‌کند.

۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1/Hash

توابع امنیتی مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1, SHA-256, SHA-384, SHA-512] و اندازه پیام هشدار [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت با رعایت استاندارد ISO/IEC 10118-3:2004. ارائه نماید

نکته کاربردی:

به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند،

شماره الزام	نام الزام	
پیاده‌سازی کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از پیاده‌سازی‌های SHA-1 را بر اساس SP 800-131A فراهم می‌کند. در نسخه بعدی این پروفایل حفاظتی، SHA-256 حداقل نیازمندی برای تمامی اهداف امنیتی خواهد بود. انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای الزام شماره ۱۰ «عملیات رمزنگاری ۱(۱)» و الزام شماره ۱۱ «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی).		
۱۳	**عملیات رمزنگاری ۱ (۴)**	FCS_COP.1.1/KeyedHash
محصول مورد ارزیابی باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده[1] را بر اساس الگوریتم رمزنگاری خاص [انتخاب:HMAC-SHA-1, HMAC-SHA-256,HMAC-SHA-384, HMAC-SHA-512] و اندازه کلید رمزنگاری [اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)] و اندازه خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح‌شده در [اختصاص: بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم MAC ۲»] انجام دهد. **نکته کاربردی:** اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که L2<=k<=L1.		
۱۴	**تولید بیت تصادفی ۱**	FCS_RBG_EXT.1.1
محصول مورد ارزیابی باید تمامی خدمات تولید بیت تصادفی قطعی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG(هر)، HMAC_DRBG (هر)، CTR_DRBG (AES)] ارائه دهد.		
۱۵	**تولید بیت تصادفی ۲**	FCS_RBG_EXT.1.2

[1] Keyed-hash message authentication

شماره الزام	نام الزام

RBG قطعی باید دست‌کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم‌افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت‌افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست‌کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و درهم‌سازهای تولیدشده مورد اشاره در ISO/IEC 18031:2011 از کلیدها و CSP هایی که تولید خواهد کرد، باشد.

نکته کاربردی:

در مورد نخستین عبارت انتخاب در «تولید بیت تصادفی ۲»، هدف امنیتی باید حداقل به یکی از انواع منابع نویز اشاره کند. اگر محصول مورد ارزیابی شامل چندین منابع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی برای هر یک از انواع منابع پر می‌کند (مثلاً دو منبع نویز مبتنی بر نرم‌افزار و یک منبع نویز مبتنی بر سخت‌افزار). مستندات و آزمون‌های مورداشاره در فعالیت‌های ارزیابی برای این عنصر، باید تکرار شود تا تمام منابع مورد اشاره در هدف امنیتی را پوشش می‌دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها، به نوبه خود، به عناصر اولیه رمزنگاری اساسی (توابع درهم‌ساز و رمزها) بستگی دارد. نویسنده هدف امنیتی، تابع مورداستفاده را انتخاب خواهد کرد و شامل عناصر اولیه رمزنگاری اساسی خاص مورد استفاده در الزام است با اینکه هریک از توابع درهم‌ساز تعیین‌شده (SHA-1,, SHA-256, SHA-384, SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، تنها اجازه پیاده‌سازی‌های مبتنی بر AES در CTR_DRBG وجود دارد.

اگر اندازه کلید برای پیاده‌سازی AES متفاوت از اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تنظیم یا تکرار «عملیات رمزنگاری» باشد تا اندازه کلید مختلف در آن لحاظ گردد. برای انتخاب در «تولید بیت تصادفی ۲»، نویسنده هدف امنیتی حداقل تعداد بیت‌های آنتروپی تزریق‌شده به RBG را تعیین می‌کند؛ که باید برابر با یا بیشتر از قدرت امنیتی هر کلید تولید شده توسط هدف ارزیابی باشد.

۳-۴ کلاس شناسایی و احراز هویت

محصول، یک مکانیسم ورود مبتنی بر کلمه عبور را به عنوان ابزاری امن در اختیار راهبران قرار می‌دهد تا بتوانند با استفاده از آن با محصول مورد ارزیابی ارتباط برقرار کنند. سرپرست محصول باید یک کلمه عبور قدرتمند را تهیه کند و مکانیسمی را برای تغییر منظم آن در نظر گیرد. برای جلوگیری از حملاتی که در آن‌ها فرد مهاجم تایپ شدن کلمه عبور را می‌بیند، کلمه عبور را باید در هنگام ورود به حالت محو و ناخوانا درآورد. قفل‌کردن و خاتمه دادن نشست را نیز می‌توان برای جلوگیری از ورود غیرمجاز به حساب کاربری مورداستفاده قرار داد. کلمه‌های عبور باید به شکل محو و ناخوانا ذخیره شوند، به گونه‌ای که هیچ واسطی برای خواندن آن به شکل متن ساده وجود نداشته باشد.

شماره الزام	نام الزام	
۱۶	**مدیریت احراز هویت ناموفق ۱**	FIA_AFL.1.1
توابع امنیتی هدف ارزیابی، باید هنگامی که یک عدد صحیح مثبت قابل تنظیم توسط سرپرست در [اختصاص: بازه عددی قابل‌قبول] از تلاش‌های ناموفق احراز هویت مربوط به تلاش سرپرست برای احراز هویت راه دور رخ داد، مشخص نمایند		
۱۷	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
زمانی که تعداد تعیین شده از تلاش‌های احراز هویت ناموفق صورت گرفت، توابع امنیتی هدف ارزیابی باید انتخاب: [○ احراز هویت موفق سرپرست راه دور متخلف را تا [اختصاص: اقدام] توسط سرپرست محلی انجام شود، محدود کند. ○ احراز هویت موفق سرپرست راه دور متخلف را تا اتمام زمان تعیین شده توسط مدیر، محدود کند.] **نکته کاربردی:** این الزام برای تعداد مشخصی از تلاش‌های احراز هویت ناموفق پیوسته اعمال می‌شود و برای مدیر در کنسول محلی تا زمانی که حساسیتی برای قفل کردن حساب مدیر به این شکل نباشد؛ اعمال نمی‌شود. این مورد می‌تواند (برای مثال) با نیاز به حساب جداگانه برای مدیران محلی یا وجود مکانیسم احراز هویت پیاده‌سازی شده‌ای که تلاش ورود محلی و راه دور را تشخیص می‌دهد مورد توجه قرار گیرد. "اقدام" که توسط مدیر محلی انجام می‌شود، به طور خاص پیاده‌سازی شده و در راهنما مدیر تعریف می‌شود. (برای مثال؛ تنظیم مجدد تحریم، تنظیم مجدد رمز عبور). نویسنده سند هدف امنیتی با توجه به نحوه پیاده‌سازی و مدیریت هدف ارزیابی، یکی از گزینه‌ها را برای مدیریت شکست احراز هویت انتخاب می‌کند. در TSS شرح داده شده است که هدف ارزیابی چگونه تضمین کند که شکست احراز هویت توسط مدیران راه دور، نمی‌توانند منجر به حالتی شوند که هیچ دسترسی مدیریتی چه به طور دائم و چه به طور موقت وجود نداشته باشد. (برای مثال: با ارائه ورود محلی که مسدود نباشد.) دستورالعمل عملیاتی توصیف و شناسایی اهمیت هر اقدامی که برای اطمینان از حفظ دائمی دسترسی مدیر مورد نیاز است را ارائه می‌دهد، حتی اگر مدیر راه دور در نتیجه FIA_AFL.1 به دلیل مسدود شدن حساب‌ها، به طور دائمی یا موقت در دسترس نباشد.		
۱۸	**مدیریت رمز عبور ۱**	FIA_PMG_EXT.1.1
توابع امنیتی مورد ارزیابی باید قابلیت‌های مدیریت کلمه عبور زیر را برای کلمه عبور سرپرست محصول فراهم آورد: الف) کلمه عبور را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: [انتخاب: "(", ")", "*", "&", "^", "%", "$", "#", "@", "!"، [اختصاص: سایر کاراکترها]]؛ ب) حداقل طول کلمه عبور باید بین [اختصاص: حداقل تعداد کاراکترهای پشتیبانی شده توسط هدف ارزیابی] و [اختصاص: تعداد کاراکترهای بزرگ‌تر یا مساوی ۱۵]قابل پیکربندی باشد.		

نکته کاربردی:

نویسنده هدف امنیتی کاراکترهای ویژه که توسط هدف ارزیابی پشتیبانی می‌شوند را تعیین می‌کند. وی می‌تواند با استفاده از عبارت اختصاص، کاراکترهای ویژه دیگری را به لیست اختیاری بیفزاید. منظور از «کلمه‌های عبور سرپرستی»، کلمه‌های عبوری هستند که توسط مدیران سیستم در کنسول محلی مورد استفاده قرار می‌گیرند. این کلمه‌های عبور روی پروتکل‌هایی استفاده می‌شوند که از آن‌ها پشتیبانی کنند. به عنوان مثال، می‌توان از SSH و HTTPS نام برد. این کلمه‌های عبور گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی مورداستفاده قرار می‌گیرند که از دیگر الزامات کارکرد امنیتی در هدف امنیتی پشتیبانی می‌کنند.

اختصاص دوم باید با حداقل طول بزرگ‌ترین کلمه عبور توسط مدیر امنیتی پیکربندی شود.

۱۹	**شناسایی و احراز هویت کاربر ۱**	FIA_UIA_EXT.1.1

توابع امنیتی مورد ارزیابی پیش از آن که از دیگر موجودیت‌های خارج از محصول بخواهد که فرایند تعیین و احراز هویت را انجام دهد، باید اجازه انجام فعالیت‌های زیر را بدهد:

- نمایش بنر هشدار مطابق با FTA_TAB.1
- [انتخاب: هیچ اقدامات دیگری، تولید خودکار کلیدهای رمزنگاری [اختصاص: لیست خدمات، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های غیر از هدف ارزیابی]]

۲۰	**شناسایی و احراز هویت کاربر ۲**	FIA_UIA_EXT.1.2

پیش از آن که توابع امنیتی مورد ارزیابی امکان انجام هر اقدامات میانی دیگری از طرف کاربر مدیریتی سیستم را فراهم آورد، باید مدیر سیستم را با موفقیت شناسایی و احراز هویت نماید.

نکته کاربردی:

این الزام برای کاربران خدماتی که به طور مستقیم توسط محصول مورد ارزیابی در دسترس قرار می‌گیرند (چه مدیران سیستم و چه موجودیت‌های IT خارجی) اعمال می‌شود و در مورد خدماتی که از طریق ارتباطات محصول مورد ارزیابی در دسترس قرار می‌گیرند، اعمال نمی‌شود. از آنجا که موجودیت‌های خارجی پیش از تعیین و احراز هویت تنها باید به چند خدمت محدود (و یا هیچ خدمتی) دسترسی داشته باشند، این خدمات باید در عبارت اختصاص ذکر شوند. در غیر این صورت، باید «هیچ اقدام دیگر» را انتخاب کرد.

اگر از تولید خودکار کلیدهای رمزنگاری بدون تائید سرپرست پشتیبانی شود، گزینه "تولید خودکار کلیدهای رمزنگاری" باید انتخاب شود.

احراز هویت ممکن است مبتنی بر کلمه عبور باشد و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از کلمه‌های عبور پشتیبانی می‌کند (مانند SSH)، یا اینکه بر اساس گواهی‌نامه انجام شود (مانند SSH و TLS). در مورد ارتباط با موجودیت‌های IT خارجی (مانند یک سرور ممیزی) این ارتباطات باید بر اساس الزام‌های «کانال امن» انجام شوند که پروتکل‌ها تعیین و احراز هویت را انجام می‌دهند. این امر بدین معنی است که نیازی نیست (ارتباطاتی از قبیل ایجاد ارتباط IPsec با سرور احراز هویت)، در عبارت اختصاص ذکر شوند، زیرا ایجاد ارتباط "counts" به معنی آغاز فرایند تعیین و احراز هویت است.

مطابق نکته کاربردی ۲۴، برای اهداف امنیتی توزیع شده، حداقل یک مؤلفه باید از احراز هویت مدیران امنیتی مطابق FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی کند. ولی تمامی مؤلفه‌های هدف ارزیابی ضروری نیست. در صورتی که تمامی مؤلفه‌های هدف ارزیابی از این روش احراز هویت مدیران امنیتی پشتیبانی نکنند، TSS باید نحوه شناسایی و احراز هویت مدیران امنیتی را شرح دهد.		
۲۱	**سازوکار احراز هویت بر اساس رمز عبور ۲**	FIA_UAU_EXT.2.1
توابع امنیتی مورد ارزیابی باید یک مکانیسم احراز هویت مبتنی بر کلمه عبور محلی، [انتخاب: [اختصاص: سایر مکانیسم‌های احراز هویت]، هیچ مکانیسم احراز هویتی] را برای احراز هویت کاربر مدیر محلی فراهم آورد. **نکته کاربردی:** عبارت اختصاص باید تمام مکانیسم‌های احراز هویت پشتیبانی شده محلی اضافی را شناسایی کند. مکانیسم‌های احراز هویت محلی از طریق کنسول محلی تعریف می‌شوند. نشست‌های مدیریتی از راه دور (و مکانیسم‌های احراز هویت مربوط به آن‌ها) در «*FTP_TRP.1/Admin*» مشخص شده‌اند. مطابق نکته کاربردی ۲۴، برای اهداف امنیتی توزیع شده، حداقل یک مؤلفه باید از احراز هویت مدیران امنیتی مطابق FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی کند. ولی تمامی مؤلفه‌های هدف ارزیابی ضروری نیست. در صورتی که تمامی مؤلفه‌های هدف ارزیابی از این روش احراز هویت مدیران امنیتی پشتیبانی نکنند، TSS باید نحوه شناسایی و احراز هویت مدیران امنیتی را شرح دهد.		
۲۲	**احراز هویت کاربر ۱۰**	FIA_UAU.7.1
هنگامی که فرایند احراز هویت در کنسول محلی در حال جریان است، محصول مورد ارزیابی تنها باید بازخورد مبهم[1] را در اختیار سرپرست محصول قرار دهد. **نکته کاربردی:** «بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی هر داده‌ی احراز هویت وارد شده توسط کاربر را به صورت واضح و قابل خواندن نشان نمی‌دهد (مانند انعکاس کلمه عبور)؛ البته ممکن است روند پیشرفت به شکل مبهم نشان داده شود (مانند یک ستاره برای هر کاراکتر). بازخورد مبهم همچنین نشان می‌دهد که محصول مورد ارزیابی در جریان احراز هویت کاربر هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احراز هویت باشد، نمایش نمی‌دهد.		

[1] Obscured feedback

۴-۴ کلاس مدیریت امنیت

توابع مدیریتی مورد نیاز در این بخش، شامل قابلیت‌های مورد نیاز برای پشتیبانی از نقش سرپرست محصول و همچنین مجموعه‌ای از توابع مدیریتی امنیت مورد نیاز برای مدیریت بخش‌های قابل پیکربندی الزامات کارکرد امنیتی (کارکرد مدیریتی محصول)، مدیریت داده‌های محصول مورد ارزیابی (مدیریت داده‌های محصول) و فعال کردن به‌روزرسانی‌های محصول مورد ارزیابی (مدیریت کارکرد در محصول ۱ (۱)/به‌روزرسانی‌های امن) هستند. در کنار این الزامات مدیریتی اصلی، برخی الزامات اختیاری نیز در پیوست اول و تعدادی الزامات انتخابی نیز در پیوست دوم ذکرشده‌اند.

شماره الزام	نام الزام
۲۳	**مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی دستی**
توابع امنیتی هدف ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست امنیتی محصول محدود نماید. **نکته کاربردی ۴۵:** این الزام امکان آغاز به‌روزرسانی دستی را به سرپرستان امنیتی محدود می‌کند.	
۲۴	**مدیریت داده‌های محصول ۱**
توابع امنیتی هدف ارزیابی باید امکان «مدیریت» داده‌های توابع امنیتی هدف ارزیابی را به سرپرست‌های امنیتی محدود کند. **نکته کاربردی ۴۶:** منظور از «مدیریت» می‌تواند هر یک از این اقدامات و موارد دیگری از این دست باشد: تولید، آغاز، بازدید، تغییر پیش‌فرض، تغییر، حذف، پاک کردن و اضافه نمودن. الزام کارکرد امنیتی حاضر همچنین شامل بازگرداندن کلمه عبورکاربری توسط سرپرست امنیتی است. در اینجا شناسه "CoreData" برای تفکیک الزام FMT_MTD.1 از الزام اختیاری FMT_MTD.1 تعریف شده در پیوست A.4.2.1 (FMT_MTD.1/CryptoKeys) است.	
۲۵	**کارکرد مدیریتی محصول ۱**
توابع امنیتی هدف ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد: [اختصاص: • توانایی مدیریت محصول به‌صورت محلی و از راه دور • توانایی پیکربندی بنر دسترسی	

شماره الزام	نام الزام
	• توانایی پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن • توانایی به‌روزرسانی محصول مورد ارزیابی و تائید به‌روزرسانی‌ها با استفاده از قابلیت [انتخاب: امضای دیجیتال، مقایسه درهم‌سازی] پیش از نصب شدن این به‌روزرسانی‌ها • توانایی پیکربندی پارامترهای احرازهویت ناموفق برای FIA_AFL.1 • [انتخاب: • توانایی شروع و متوقف کردن سرویس‌ها. ○ توانایی پیکربندی رفتار ممیزی ○ توانایی تغییر رفتار انتقال داده ممیزی به یک موجودیت فناوری اطلاعات خارجی، بررسی داده‌های ممیزی، عملکرد ممیزی وقتی که فضای ذخیره‌سازی محلی پر است. ○ توانایی پیکربندی لیست خدمات ارائه‌شده در دسترس توسط محصول مورد ارزیابی پیش از شناسایی و احراز هویت یک موجودیت، چنان که در «شناسایی و احراز هویت کاربر[۱]» تشریح شده است. ○ توانایی مدیریت کلیدهای رمزنگاری ○ توانایی پیکربندی کارکرد رمزنگاری ○ توانایی پیکربندی آستانه[۲] برای تجدید کلید SSH ○ توانایی پیکربندی مدت زمان برای SA در IPsec ○ توانایی پیکربندی اثر متقابل بین اجزای هدف ارزیابی ○ توانایی فعال یا غیرفعال کردن بررسی خودکار برای به‌روزرسانی‌ها یا به‌روزرسانی‌های خودکار ○ توانایی فعال‌سازی مجدد حساب کاربری مدیر ○ توانایی تنظیم زمانی که برای مهرهای زمانی استفاده می‌شود. ○ توانایی پیکربندی NTP ○ توانایی پیکربندی مرجع شناسایی همتا ○ توانایی مدیریت انبار اطمینان هدف ارزیابی و تعیین گواهی‌های X509.v3 به عنوان لنگر اطمینان ○ توانایی واردکردن گواهی X509.v3 به انبار اطمینان هدف ارزیابی ○ هیچ قابلیت دیگری]

[۱] FIA_UIA_EXT.1

[۲] Threshold

شماره الزام	نام الزام

نکته کاربردی:

محصول مورد ارزیابی باید کارکردهای لازم برای مدیریت سیستم به‌صورت محلی و مدیریت از راه دور را فراهم آورد.

به طور کلی، این پروفایل حفاظتی، تابع مدیریت امنیتی خاصی که از طریق رابط مدیر محلی یا رابط مدیر از راه دور یا هر دو قابل دسترسی باشد را الزام نمی‌کند. TSS باید با جزئیات مشخص کند که کدام توابع مدیریت امنیتی از طریق کدام رابط‌ها قابل دسترسی هستند. هدف ارزیابی باید قابلیت پیکربندی بنر دسترسی را برای FTA_TAB.1 و قابلیت پیکربندی زمان غیرفعال بودن نشست را برای FTA_SSL_EXT.1 و FTA_SSL.3 ارائه دهد. آیتم "توانایی به‌روزرسانی هدف ارزیابی و تائید به‌روزرسانی‌هایی که از قابلیت امضای دیجیتال استفاده می‌کنند قبل از نصب این به‌روزرسانی‌ها" شامل توابع مدیریتی مربوطه از FMT_MOF.1/ManualUpdate، FMT_MOF.1/AutoUpdate (اگر در ST باشد) و FIA_X509_EXT.2.2 و FPT_TUD_EXT.1.2 و FPT_TUD_EXT.2.2 (اگر در ST باشند و اگر شامل اقدام قابل پیکربندی توسط مدیر باشند) می‌باشند به طور مشابه، انتخاب "توانایی پیکربندی رفتار ممیزی" شامل توابع امنیتی مربوطه از FMT_MOF.1/Services و FMT_MOF.1/Functions (برای تمام این SFR هایی که در سند ST هستند) می‌باشند. اگر هدف ارزیابی توانایی غیرفعال کردن حساب کاربری مدیر از راه دور را از طریق FIA_AFL.1 ارائه کند، نویسنده سند هدف امنیتی باید گزینه "توانایی فعال‌سازی مجدد حساب مدیر" را برای مجوز فعال‌سازی مجدد حساب توسط مدیر محلی، انتخاب کند. اگر هدف ارزیابی برای مدیر توانایی پیکربندی رفتار ممیزی، قبل از شناسایی یا احراز هویت ارائه کند، یا اگر هر کدام از عملکردهای رمزنگاری در هدف ارزیابی قابل پیکربندی باشد، یا اگر ST هدف ارزیابی توزیع شده‌ای را شرح دهد، نویسنده هدف امنیتی باید انتخاب مناسبی انجام دهد یا در انتخاب دوم، گزینه در غیر این صورت "هیچ قابلیت دیگری" را انتخاب کند. (انتخاب دوم ممکن است متناوباً در ST خالی بماند)

اگر هدف ارزیابی از پیکربندی آستانه برای مکانیسم‌های مورد استفاده برای FCS_SSHC_EXT.1.8 یا FCS_SSHS_EXT.1.8 (لازم است برای این تنظیمات FMT_MOF.1/Functions در ST باشد.) پشتیبانی می‌کند، گزینه "توانایی پیکربندی آستانه برای تجدید کلید SSH" باید در سند هدف امنیتی انتخاب شده باشد. اگر هدف ارزیابی محدودیتی برای مقادیر قابل‌قبول آستانه قرار داده است، باید در TSS بیان شود.

اگر هدف ارزیابی از ارتباط امن از طریق IPsec پشتیبانی کند و الزامات FCS_IPSEC_EXT.1 در سند هدف امنیتی باشد، باید در سند هدف امنیتی گزینه "توانایی تنظیم طول عمر IPsec SAs" انتخاب شود. تنظیمات طول عمر برای IPsec SAs لازم است از طریق انتخاب در FCS_IPSEC_EXT.1.7 باشد. (لازم است برای این تنظیمات FMT_MOF.1/Functions در ST باشد.)

اگر هدف ارزیابی به مدیر اجازه تنظیم زمان دستگاهی که در مهرهای زمانی استفاده می‌شود داده باشد، گزینه "توانایی تنظیم زمانی که برای مهرهای زمانی استفاده می‌شود" باید در ST انتخاب شود. اگر هدف ارزیابی اجازه تنظیمات دستی زمان را نداده و فقط متکی به هماهنگی با منابع خارجی زمان مانند سرورهای NTP است، این گزینه نباید انتخاب شود.

اگر هدف ارزیابی از ارتباطات امن از طریق پروتکل IPsec پشتیبانی می‌کند و الزامات FCS_IPSEC_EXT.1 در ST باشد، گزینه

شماره الزام	نام الزام
"توانایی پیکربندی مرجع شناسایی همتا" باید در ST انتخاب شود. ممکن است پیکربندی مرجع شناسایی برای اهداف امنیتی که فقط از آدرس IP و انواع شناسه FQDN پشتیبانی می‌کنند، همانند پیکربندی نام‌های همتا برای اهداف ارتباط باشد. برای اهداف ارزیابی توزیع‌شده، تعامل بین مؤلفه‌های هدف امنیتی قابل تنظیم خواهد بود (FCO_CPC_EXT.1 را ببینید)؛ بنابراین، نویسنده هدف امنیتی گزینه "توانایی پیکربندی اثر متقابل بین اجزای هدف ارزیابی" را برای اهداف ارزیابی توزیع‌شده انتخاب می‌کند. یک مثال ساده، "تغییر پروتکل ارتباطی مطابق FPT_ITT.1 " است. مثال دیگر، "تغییر مدیریت مؤلفه هدف ارزیابی از مدیریت مستقیم از راه دور، به مدیریت از راه دور از طریق یک مؤلفه دیگری از هدف ارزیابی"، است. یک مورد استفاده پیچیده‌تر، "اگر تحقق یک SFR از طریق دو مؤلفه یا بیشتر از هدف ارزیابی به دست آید و مسئولیت‌ها بین دو مؤلفه یا بیشتر قابل تغییر باشد"، است. برای اهداف ارزیابی که کانال registration را پیاده‌سازی کرده‌اند (همان‌طور که در FCO_CPC_EXT.1.2 شرح داده شده است)، نویسنده هدف امنیتی از گزینه "توانایی پیکربندی کارکرد رمزنگاری" در این SFR استفاده می‌کند و به طور متناظر در TSS برای تشریح پیکربندی هر منظر رمزنگاری کانال registration که برای بهبود امنیتی کانال، توسط محیط عملیاتی قابل تغییر است نگاشت می‌شود. (cf. توصیف محتوای رویه‌های آمادگی در [SD, 3.6.1.2])	
۲۶	**نقش‌های امنیتی ۳**
توابع امنیتی هدف ارزیابی باید نقش‌های زیر را نگهداری کند. • سرپرست امنیتی	
۲۷	**نقش‌های امنیتی ۴**
توابع امنیتی هدف ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.	
۲۸	**نقش‌های امنیتی ۵**

شماره الزام	نام الزام

محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند:

- نقش سرپرست امنیتی باید بتواند توابع امنیتی هدف ارزیابی را به صورت محلی مدیریت کند.
- نقش سرپرست امنیتی باید بتواند توابع امنیتی هدف ارزیابی را از راه دور مدیریت کند.

نکته کاربردی:

بر اساس این الزام سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک مکانیسم راه دور مدیریت کند. نویسنده هدف امنیتی باید برای نشان دادن نحوه دستیابی به ارتباط امن FTP_ITC.1، FPT_ITT.1 و/یا FTP_TRP.1/Admin را انتخاب کند.

در این SFR، پیاده‌سازی مدیریت کاربر خود، برای تمامی مؤلفه‌های هدف ارزیابی، در اهداف ارزیابی توزیع شده، الزامی نیست. حداقل یک مؤلفه باید از احراز هویت و شناسایی مدیران امنیتی مطابق با FIA_UIA_EXT.1و FIA_UAU_EXT.2 پشتیبانی کند. احراز هویت سایر مؤلفه‌های هدف ارزیابی به عنوان مدیر امنیتی، می‌تواند از طریق کانال امن (مطابق با FTP_ITC.1یا FPT_ITT.1) با استفاده از مؤلفه‌ای که احراز هویت مدیران را مطابق FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی می‌کند محقق شود. شناسایی کاربران مطابق با FIA_UIA_EXT.1.2 و وابستگی کاربران با قوانین مطابق FMT_SMR.2.2، از طریق مؤلفه‌هایی که احراز هویت مدیران امنیتی را مطابق با FIA_UIA_EXT.1وFIA_UAU_EXT.2 پشتیبانی می‌کنند انجام می‌شود. پشتیبانی از مدیریت[1] محلی مؤلفه‌های تعریف شده در FMT_SMR.2.3، توسط مؤلفه‌های هدف ارزیابی که مدیران امنیتی را از طریق استفاده از کانال امن احراز هویت می‌کنند الزامی نیست.

۲۹	مدیریت کارکرد در محصول IPS۱

توابع امنیتی هدف ارزیابی باید قادر به انجام توابع مدیریتی زیر باشد:

]

۱) فعال‌سازی، غیر فعال‌سازی 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)

[1] administration

شماره الزام	نام الزام
	ث) پروتکل (IPv4 و IPv6) ج) کد و نوع ICMP ۳) به‌روزرسانی (وارد کردن) امضاها ۴) ایجاد امضاهای خاص ۵) پیکربندی کشف رفتارهای غیرعادی ۶) فعال‌سازی و غیر فعال‌سازی اقدامات هنگامی که امضا یا رفتارهای غیرعادی مورد شناسایی قرار می‌گیرند. ۷) تغییر آستانه‌هایی که واکنش‌های IPS را هدف می‌گیرند. ۸) تغییر مدت زمان اقدامات 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 [

۵-۴ کلاس حفاظت از محصول مورد ارزیابی

در این بخش، الزامات مربوط به محصول مورد ارزیابی برای حفاظت از داده‌های امنیتی حساس مانند کلیدها و کلمه‌های عبور، انجام خودآزمایی‌ها برای پایش کارکرد صحیح محصول مورد ارزیابی (شامل از بین بردن نقایص کارکرد میان‌افزار یا ضعف در یکپارچگی نرم‌افزار) و ارائه روش‌های امن برای به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را مرور می‌کنیم. علاوه بر این، محصول مورد ارزیابی باید مهرهای زمانی قابل اعتمادی را برای پشتیبانی از ممیزی صحیح خانواده «تولید داده ممیزی» فراهم آورد.

شماره الزام	نام الزام
۳۰	**محافظت از داده‌های محصول** **(برای خواندن تمامی کلیدهای از پیش به اشتراک گذاشته شده، متقارن و خصوصی) ۱**

توابع امنیتی هدف ارزیابی باید از خواندن تمام کلیدهایی که از پیش به اشتراک گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد.

نکته کاربردی:

هدف از الزام حاضر این است که دستگاه بتواند مانع از افشای غیرمجاز به کلیدها، اطلاعات کلیدها و اعتبارنامه (گواهی‌نامه) احراز هویت شود. این داده‌ها باید تنها برای هدف کارکردهای امنیتی مربوطه، قابل دسترسی باشند و نیازی به دسترسی و نمایش آن‌ها در هر زمان دیگر نخواهد بود. این الزام مانع از مشخص شدن وجود این اطلاعات، در حال استفاده بودن آن‌ها، یا معتبر بودن آن‌ها نیست. با این حال، الزام حاضر امکان خواندن این اطلاعات را کاملاً محدود می‌کند.

۳۱	**حفاظت از کلمه عبور مدیر سیستم ۱**

توابع امنیتی هدف ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.

۳۲	**حفاظت از کلمه عبور مدیر سیستم ۲**

توابع امنیتی هدف ارزیابی باید از خوانده شدن کلمه‌های عبوری که به‌صورت متن ساده[۱] هستند، جلوگیری کند.

نکته کاربردی:

هدف از الزام حاضر این است که داده‌های خام مربوط به احراز هویت از طریق گذرواژه، به شکل واضح ذخیره نشوند و هیچ کاربر یا سرپرست محصول نتواند کلمه عبور متن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصولی که تمام دسترسی‌ها را داشته باشد می‌تواند به‌طور مستقیم حافظه را به‌منظور ضبط کلمه عبور بخواند؛ اما به وی اعتماد می‌شود و فرض می‌گردد که وی این کار را نخواهد کرد. باید کلمه‌های عبور در هنگام ورود به کنسول محلی، مطابق با FIA_UAU.7 مبهم باشند.

۳۳	**خودآزمایی محصول۱**

توابع امنیتی هدف ارزیابی باید مجموعه‌ای از این خودآزمایی‌ها را [انتخاب: در مرحله راه‌اندازی اولیه (روشن شدن دستگاه)، به طور دوره‌ای در حین کارکرد عادی، در صورت درخواست کاربر مجاز، در شرایط [اختصاص: شرایطی که باید در آن‌ها خودآزمایی‌ها را انجام داد]] برای نشان دادن کارکرد صحیح توابع امنیتی هدف ارزیابی انجام دهد: [اختصاص: لیست خودآزمایی‌هایی که باید توسط توابع امنیتی هدف ارزیابی انجام شوند].

تذکر: در صورتی که برای خودآزمایی‌ها از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام «خودآزمایی

[۱] Plaintext

محصول ۲» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه گردد.

نکته کاربردی:

انتظار می‌رود که خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام شوند. سایر گزینه‌ها در صورتی در نظر گرفته می‌شوند که توسعه‌دهنده دستگاه توجیه کند که چرا خودآزمایی در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نمی‌شود. انتظار می‌رود که دست‌کم خودآزمایی‌های لازم برای حصول اطمینان از صحت و یکپارچگی نرم‌افزار و میان‌افزار و کارکرد صحیح توابع رمزنگاری به منظور برآورده کردن الزامات کارکرد امنیتی انجام شوند. اگر تمام خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نشوند، الزام کارکرد امنیتی حاضر چند بار با انتخاب‌های مناسب اجرا می‌شود.

در نسخه‌های آینده از این cPP مجموعه‌ای از خودآزمایی مورد نیاز خواهد بود که شامل حداقل مکانیسم‌ها برای اندازه‌گیری boot است از جمله خودآزمایی مؤلفه‌ها که اندازه‌گیری را انجام می‌دهند.

ممکن است اهداف ارزیابی توزیع نشده از چندین مؤلفه که به اجرای SFR ها کمک می‌کنند تشکیل شده باشد. خودآزمایی باید تمامی نرم‌افزارهایی که به اجرای SFR ها در تمامی مؤلفه‌ها کمک می‌کنند را پوشش دهد.

برای تمامی اهداف ارزیابی توزیع نشده، تمامی مؤلفه‌ها باید خودآزمایی را اجرا کنند. الزاماً به این معنی نیست که هر مؤلفه هدف ارزیابی باید خودآزمایی‌های یکسانی انجام دهد: ST کاربرد انتخاب (برای مثال زمانی که خودآزمایی اجرا می‌شود) و اختصاص نهایی (برای مثال کدام خودآزمایی‌ها باید اجرا شوند) هر مؤلفه هدف ارزیابی را شرح می‌دهد.

نکته کاربردی:

اگر در خودآزمایی‌ها از گواهی‌نامه‌ها استفاده شود (مثلاً برای تائید امضا جهت تائید صحت و یکپارچگی)، گواهی‌نامه‌ها باید از «*FIA_X509_EXT.1/Rev*» انتخاب شوند و بر اساس الزام «الزامات پروتکل X509 (۱)» و الزام «الزامات پروتکل X509 (۲)» تائید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی در نظر گرفته شوند

۳۴	**به‌روزرسانی امن ۱**

توابع امنیتی هدف ارزیابی باید این امکان را به سرپرستان امنیتی بدهد که هم به نسخه فعلی در حال اجرا نرم‌افزار/میان‌افزار هدف ارزیابی و [انتخاب: هم به جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار هدف ارزیابی، به هیچ نسخه نرم‌افزار/میان‌افزار دیگر] دسترسی داشته باشد.

نکته کاربردی:

اگر بتوان به‌روزرسانی امن را بر روی هدف ارزیابی نصب کرده و با تأخیر فعال شود، هر دو نسخه در حال اجرا و نسخه غیرفعال نصب شده باید ارائه شود. در این مورد، گزینه "نسخه اخیراً نصب شده نرم‌افزار/میان‌افزار هدف ارزیابی" لازم است از گزینه‌های FPT_TUD_EXT.1.1 انتخاب شود و لازم است TSS نحوه و زمان فعال شدن نسخه غیرفعال را شرح دهد. اگر تمامی به‌روزرسانی‌های امن به عنوان بخشی از فرآیند نصب فعال شوند، فقط نسخه در حال اجرا لازم به ارائه است. در این مورد، گزینه "هیچ نسخه نرم‌افزار/میان‌افزار دیگری" باید از گزینه‌های FPT_TUD_EXT.1.1 انتخاب شود.

برای اهداف ارزیابی توزیع شده، روش تعیین نسخه‌های نصب شده بر روی هر مؤلفه از هدف ارزیابی باید در راهنمای عملکردی شرح داده شود.
۳۵ **به‌روزرسانی امن ۲**
توابع امنیتی هدف ارزیابی باید این امکان را برای سرپرستان امنیتی فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار توابع امنیتی هدف ارزیابی را به صورت دستی انجام دهد و [انتخاب: از بررسی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی‌های خودکار پشتیبانی کند، از هیچ مکانیسم به‌روزرسانی دیگری پشتیبانی نکند]. **تذکر: در صورتی که نویسنده سند هدف امنیتی برای این الزام گزینه‌های به‌روزرسانی خودکار را انتخاب نماید لازم است الزام «مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/به‌روزرسانی امن» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه نماید.** **نکته کاربردی:** عبارت «انتخاب» در «به‌روزرسانی امن ۲»، بین پشتیبانی از «بررسی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز قائل می‌شود. بررسی خودکار به‌روزرسانی‌ها به یک توابع امنیتی هدف ارزیابی اشاره دارد که بررسی می‌کند تا ببیند به‌روزرسانی جدیدی وجود دارد یا خیر و این امر را به سرپرست محصول اطلاع می‌دهد (مثلاً از طریق یک پیام در طول نشست سرپرست یا فایل‌های log)، اما درواقع انجام به‌روزرسانی نیازمند اقداماتی توسط سرپرست محصول خواهد بود، اما به‌روزرسانی خودکار به یک توابع امنیتی هدف ارزیابی اشاره دارد که به‌روزرسانی‌ها را بررسی می‌کند و در صورت وجود آن‌ها را نصب می‌نماید. TSS اقداماتی که در پشتیبانی هدف ارزیابی هنگام استفاده از گزینه‌های "پشتیبانی از بررسی خودکار به‌روزرسانی‌ها" یا "پشتیبانی از به‌روزرسانی‌های خودکار" درگیر می‌شوند را شرح می‌دهد. زمانی که مقادیر درهم‌سازی منتشر شده (FPT_TUD_EXT.1.3 را ببینید) برای محافظت از مکانیسم به‌روزرسانی امن استفاده می‌شوند، هدف ارزیابی نباید به طور خودکار فایل‌های به‌روزرسانی را با مقادیر درهم‌سازی (یا ادغام شده در فایل‌های به‌روزرسانی یا به طور جداگانه) دانلود کند و نباید به‌روزرسانی را به طور خودکار و بدون هیچ احراز هویت فعالی از مدیر امنیتی نصب نماید؛ حتی در زمانی که مقدار درهم‌سازی محاسبه شده با مقدار درهم‌سازی منتشر شده مطابقت داشته باشد. هنگامی که از مقادیر درهم‌سازی منتشر شده برای محافظت از مکانیسم به‌روزرسانی امن استفاده می‌شود، نباید گزینه "پشتیبانی از به‌روزرسانی خودکار" استفاده شود (هرچند، بررسی خودکار به‌روزرسانی‌ها مجاز است). هدف ارزیابی ممکن است به طور خودکار برای خودش فایل‌های به‌روزرسانی را دانلود کند ولی نه مقدار درهم‌سازی. برای رویکرد درهم‌سازی منتشر شده، همواره درخواست مدیر امنیتی برای دریافت احراز هویت فعال جهت نصب به‌روزرسانی (مطابق جزئیات بیشتر شرح داده شده در FPT_TUD_EXT.1.3) مدنظر است؛ بنابراین نوع مکانیسم به‌روزرسانی به عنوان "آغاز به‌روزرسانی دستی" در نظر گرفته شده است، حتی اگر ممکن باشد فایل‌های به‌روزرسانی به طور خودکار دانلود شوند. رویکرد کاملاً خودکار (بدون دخالت مدیر امنیتی) فقط زمانی که "مکانیسم امضای دیجیتال" در FPT_TUD_EXT.1.3 انتخاب شده باشد می‌تواند مورد استفاده قرار گیرد.

۳۶	به‌روزرسانی امن ۳

توابع امنیتی هدف ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: مکانیسم امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار/ نرم‌افزار در اختیار توابع امنیتی هدف ارزیابی قرار دهد.

تذکر: در صورتی که از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام‌های «الزامات به‌روزرسانی ۴» و «الزامات به‌روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه نماید.

نکته کاربردی:

مکانیسم امضای دیجیتال که در بخش «به‌روزرسانی امن ۳» به آن اشاره شده است، یکی از الگوریتم‌هایی است که در الزام «عملیات رمزنگاری ۱ (۲)» تشریح شده است. درهم‌ساز منتشرشده که در «به‌روزرسانی امن ۳» مورد اشاره قرار گرفته است نیز توسط یکی از توابع تشریح‌شده در الزام «عملیات رمزنگاری ۱ (۳)» تولید می‌شود. نویسنده هدف امنیتی باید مکانیسم اجراشده توسط توابع امنیتی هدف ارزیابی را تعیین نماید. می‌توان از هر دو مکانیسم اجراشده استفاده کرد.

زمانی که برای حفاظت از مکانیسم به‌روزرسانی امن از مقادیر درهم‌سازی منتشر شده استفاده می‌شود، احراز هویت فعال از فرآیند به‌روزرسانی توسط مدیر امنیتی، همواره مورد نیاز است. انتقال امن مقدار درهم‌سازی معتبر از توسعه‌دهنده به مدیر امنیتی، یکی از فاکتورهای کلیدی برای حفاظت از مکانیسم به‌روزرسانی امن هنگام استفاده از درهم‌سازی‌های منتشر شده است و لازم است سند راهنما نحوه اجرای انتقال را شرح دهد. برای تائید مقدار درهم‌سازی امن توسط مدیر امنیتی، موارد استفاده مختلفی ممکن است. مدیر امنیتی می‌تواند مقدار درهم‌سازی منتشر شده را مانند فایل‌های به‌روزرسانی به دست آورد و تا زمانی که درهم‌سازی فایل‌های به‌روزرسانی توسط هدف ارزیابی یا به روش دیگری در حال انجام است، خارج از هدف ارزیابی تائید را انجام دهد. احراز هویت مدیر امنیتی و آغاز به‌روزرسانی امن در این مورد با عنوان "احراز هویت فعال" از به‌روزرسانی امن است. متناوباً، مدیر می‌تواند هدف ارزیابی را با مقدار درهم‌سازی منتشر شده و همچنین با فایل‌های به‌روزرسانی و درهم‌سازی و مقایسه‌های درهم‌سازی انجام شده توسط هدف ارزیابی باهم ارائه دهد. در مورد تائید درهم‌سازی موفق، هدف ارزیابی می‌تواند به‌روزرسانی را بدون هیچ مرحله اضافه‌ای توسط مدیر امنیتی انجام دهد. احراز هویت به عنوان مدیر امنیتی و ارسال مقدار درهم‌سازی به هدف ارزیابی برای "احراز هویت فعال" از به‌روزرسانی امن (در مورد تائید درهم‌سازی موفق) در نظر گرفته شده است، زیرا از مدیر انتظار می‌رود که مقدار درهم‌سازی را فقط برای هدف ارزیابی در زمانی که قصد انجام به‌روزرسانی داشته باشد، بارگذاری کند. تا زمانی که انتقال مقدار درهم‌سازی به هدف ارزیابی توسط مدیر امنیتی انجام شود، بارگذاری فایل‌های به‌روزرسانی توسط مدیر امنیتی قابل انجام است یا به طور خودکار می‌تواند توسط هدف ارزیابی از منبع دانلود شود.

اگر مکانیسم امضای دیجیتال انتخاب شده باشد، تائید امضا باید توسط خود هدف ارزیابی انجام شود. برای گزینه درهم‌سازی منتشر شده، خود هدف ارزیابی می‌تواند همانند مدیر امنیتی تائید نماید. در مورد بعدی استفاده از قابلیت هدف ارزیابی، اختیار تائید ندارد، بنابراین تائید می‌تواند با استفاده از قابلیت غیر هدف ارزیابی، از دستگاه شامل هدف ارزیابی یا با دستگاهی که شامل هدف ارزیابی نباشد، انجام شود.

برای اهداف ارزیابی توزیع شده، باید تمامی مؤلفه‌ها از به‌روزرسانی امن پشتیبانی نمایند. تائید امضا یا درهم‌سازی در به‌روزرسانی باید توسط هر مؤلفه هدف ارزیابی (تائید امضا) یا برای هر مؤلفه هدف ارزیابی (تائید درهم‌سازی) انجام شود.

ممکن است به‌روزرسانی هدف ارزیابی توزیع شده منجر به وضعیتی شود که مؤلفه‌های مختلف هدف ارزیابی، نسخه‌های مختلف نرم‌افزاری را اجرا کنند. مطابق تفاوت‌های بین نسخه‌های مختلف نرم‌افزار، ممکن است با اثر ترکیبی از نسخه‌های مختلف نرم‌افزار در مشکلی در هیچ جا وجود نداشته باشد و یا برای عملکرد هدف ارزیابی بحرانی باشد. TSS باید مکانیسم‌هایی را که از عملکرد متوالی مناسب هدف ارزیابی در طول به‌روزرسانی امن اهداف امنیتی توزیع شده پشتیبانی می‌کنند، با جزئیات مشخص نماید.

نکته کاربردی:

در نسخه‌های بعدی این پروفایل حفاظتی، لازم خواهد شد که برای به‌روزرسانی‌های امن، از یک مکانیسم امضای دیجیتال استفاده شود.

نکته کاربردی:

اگر در مکانیسم تائید به‌روزرسانی از گواهی‌نامه‌ها استفاده شود، این گواهی‌ها باید از FIA_X509_EXT.2.1 انتخاب شده و بر اساس FIA_X509_EXT.1 تائید گردند. علاوه بر این، FPT_TUD_EXT.2 باید در سند هدف امنیتی در نظر گرفته شود.

نکته کاربردی:

در این الزام کارکرد امنیتی، منظور از «به‌روزرسانی»، فرایند جایگزین کردن یک مؤلفه نرم‌افزاری غیر فرار (non-volatile) با یک مؤلفه دیگر است. به مؤلفه اول، تصویر غیر فرار یا تصویر NV و به مؤلفه دوم، تصویر به‌روزرسانی گفته می‌شود. هر چند که تصویر به‌روزرسانی معمولاً جدیدتر از تصویر NV است، اما الزامی در این زمینه وجود ندارد. در مواردی ممکن است مالک سیستم بخواهد مؤلفه را به نسخه قدیمی‌تر برگرداند (مثلاً هنگامی که تولیدکننده مؤلفه یک به‌روزرسانی معیوب را منتشر کند، یا هنگامی که سیستم مبتنی بر یک ویژگی مستندسازی نشده باشد که در به‌روزرسانی جدید وجود ندارد). همچنین، ممکن است مالک سیستم بخواهد به‌روزرسانی را با تصویر NV انجام دهد تا معایب موجود را برطرف نماید.

تمام مؤلفه‌های مجزای میان‌افزار و نرم‌افزار (مانند برنامه‌های کاربردی، درایورها، هسته) محصول مورد ارزیابی لازم است محافظت شوند برای مثال، یا توسط تولیدکننده متناظر امضای دیجیتال شوند و در نهایت توسط مکانیسم به‌روزرسانی تائید گردند و یا باید یک درهم‌سازی برای آن‌ها منتشر شود که نیازمند تائید قبل از به‌روزرسانی است.

۳۷	**مهرهای زمانی معتبر ۱**
توابع امنیتی هدف ارزیابی باید قابلیت ارائه مهرهای زمانی معتبر را برای استفاده خود داشته باشد.	
۳۸	**مهرهای زمانی معتبر ۲**
توابع امنیتی هدف ارزیابی باید [انتخاب: به مدیر امنیتی اجازه تنظیم زمان بدهد، زمان را با یک سرور NTP هماهنگ کند]	

نکته کاربردی:

انتظار می‌رود مهرهای زمانی معتبر با سایر توابع امنیتی هدف ارزیابی مورد استفاده قرار گیرد، مثال: برای تولید داده ممیزی، مجوز بررسی ترتیب رویدادها برای رسیدگی به حوادث و اجازه تعیین زمان واقعی محلی هنگامی که رویدادی رخ داده باشد، به مدیر امنیتی می‌دهد. تصمیم‌گیری در مورد میزان دقت مورد نیاز اطلاعات بر عهده سرپرست است. هدف ارزیابی به اطلاعات زمان و تاریخ خارجی بستگی دارد یا به صورت دستی توسط مدیر امنیتی ارائه می‌شود یا از یک یا بیشتر منبع زمانی خارجی مانند سرورهای NTP استفاده می‌کند. در این الزام، باید از انتخاب گزینه‌های متناظر برگزیده شوند. توصیه می‌شود از ساعت محلی در زمان واقعی استفاده شده و به طور خودکار با یک منبع زمانی خارجی (مانند سرور NTP) هماهنگ شود. توجه داشته باشید که برای ارتباط با منبع زمانی خارجی مانند سرور NTP، استفاده از FTP_ITC.1 اختیاری است. نویسنده سند هدف امنیتی باید در TSS نحوه دریافت اطلاعات زمان و تاریخ خارجی توسط هدف ارزیابی و نحوه نگهداری این اطلاعات را شرح دهد.

عبارت «مهر زمانی معتبر» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده‌های ممیزی را محاسبه کرد. توجه داشته باشید باید تمام تغییرات ناپیوسته زمان انجام شده توسط مدیر یا از طریق یک فرآیند خودکار، ممیزی شوند. هنگامی که زمان توسط هسته یا امکانات سیستم تغییر می‌کند، نیازی به ممیزی نیست؛ مانند روز- که در زمان ناپیوستگی ایجاد نمی‌کند.

برای اهداف امنیتی توزیع شده، انتظار می‌رود مدیر امنیتی از هماهنگی تنظیمات زمانی بین مؤلفه‌های مختلف هدف ارزیابی اطمینان حاصل نماید. باید تمامی مؤلفه‌های هدف ارزیابی هماهنگ باشند و یا باید offset برای هر جفت مؤلفه هدف ارزیابی برای مدیر شناخته شود (به عنوان مثال از طریق هماهنگی بین مؤلفه‌های هدف ارزیابی یا از طریق هماهنگی مؤلفه‌های مختلف هدف ارزیابی با سرورهای NTP خارجی). این مورد شامل مؤلفه‌های هدف ارزیابی هماهنگ با مناطق مختلف زمانی است.

۶-۴ دسترسی به محصول

این بخش به تشریح الزامات امنیتی مربوط به نشست‌های سرپرست محصول مورد ارزیابی می‌پردازد. هم نشست‌های محلی و هم نشست‌های راه دور پایش می‌شوند تا در صورت غیرفعال بودن شناسایی شوند و قفل شدن یا خاتمه یافتن آن‌ها نیز در صورت رسیدن به آستانه زمانی بررسی می‌شود. راهبران باید قادر باشند نشست‌های تعاملی خود را خاتمه دهند. در ابتدای هر نشست باید یک اطلاعیه مشاوره‌ای برای آن‌ها نمایش داده شود.

شماره الزام	نام الزام
۳۹	قفل‌کردن و خاتمه دادن به نشست‌ها ۷

شماره الزام	نام الزام
در مورد نشست‌های تعاملی محلی[۱]، توابع امنیتی هدف ارزیابی باید پس از اتمام زمان غیرفعال بودن که توسط سرپرست امنیتی تعیین شده است، [انتخاب: • نشست را قفل کند – تمام فعالیت‌های مربوط به دستگاه‌های دسترسی به داده‌های کاربری و نمایش این داده‌ها، به جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیرفعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛ • نشست را خاتمه دهد].	
۴۰	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
در مورد نشست‌های تعاملی راه دور[۲]، در صورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، توابع امنیتی هدف ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن نشست توسط سرپرست امنیتی تعیین می‌شود.	
۴۱	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
توابع امنیتی هدف ارزیابی باید به سرپرست آغازکننده اجازه دهد که نشست مدیریتی تعاملی خود را خاتمه دهد.	
۴۲	**پیغام‌های هشدار در رابطه با استفاده محصول ۱**
قبل از ایجاد نشست برای کاربر، توابع امنیتی هدف ارزیابی باید توصیه‌های امنیتی مدیریتی و همچنین پیام هشدار اطلاعیه و توافق‌نامه استفاده از توابع امنیتی هدف ارزیابی را به سرپرست محصول نشان دهد. **نکته کاربردی:** این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک توابع امنیتی هدف ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی یا اتصالات برنامه‌ریزی شده‌ای (مانند تماس‌های راه دور از طریق شبکه) را برقرار می‌کنند، نیازی نیست توسط این الزام پوشش داده شود.	
۴۳	**کانال امن ۱**
توابع امنیتی هدف ارزیابی، باید کانال ارتباطی امنی را با استفاده از [انتخاب: IPsec، SSH، DTLS، TLS، HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احرازهویت، اختصاص: [دیگر قابلیت‌ها]، هیچ قابلیت دیگری] که به طور منطقی از کانال‌های ارتباطی دیگر متمایز است فراهم نماید تا تعیین هویت مطمئنی از نقاط انتهایی ارائه	

[۱] Local
[۲] Remote

شماره الزام	نام الزام
	دهد و از داده‌های کانال در برابر تغییر و افشاء محافظت نموده و تغییرات داده‌های کانال را تشخیص دهد. **تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست ۲ تمامی الزامات مربوط به آن پروتکل تکمیل و به سند ST اضافه گردد.**
۴۴	**کانال امن ۲**
	توابع امنیتی هدف ارزیابی باید به خود یا به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.
۴۵	**کانال امن ۳**
	توابع امنیتی هدف ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: لیست خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی نماید. **نکته کاربردی:** هدف از الزام حاضر این است که ابزاری را برای استفاده از پروتکل رمزنگاری جهت حفاظت از ارتباطات خارجی با موجودیت‌های معتبر IT کارکرد فراهم آورد. منظور از موجودیت‌های معتبر IT موجودیت‌هایی است که توابع امنیتی هدف ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. توابع امنیتی هدف ارزیابی دست‌کم از یکی از پروتکل‌های لیست‌شده استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی ارتباط برقرار کند. اگر ارتباط با یک سرور احراز هویت (مانند RADIUS) برقرار شود، نویسنده هدف امنیتی باید عبارت «سرور احراز هویت» را در الزام «کانال امن ۱» انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های لیست‌شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT (مانند سرور NTP) مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی (برای پروتکل‌هایی که به‌منظور محافظت اتصالات مورد استفاده قرار می‌گیرند) را انجام دهد و موارد مناسب (برای آن موجودیت‌ها) را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی مکانیسم یا مکانیسم‌های پشتیبانی‌شده توسط توابع امنیتی هدف ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند. هر چند که هیچ الزامی در مورد طرف آغازکننده ارتباط وجود ندارد، نویسنده هدف امنیتی در عبارت اختصاص این الزام، خدماتی که توابع امنیتی هدف ارزیابی می‌تواند برای آن‌ها ارتباط با موجودیت IT معتبر آغاز کند را لیست می‌نماید. این الزام بیان می‌دارد که نه‌تنها ارتباطات در هنگام برقراری اولیه حفاظت می‌شوند، بلکه در حین برقراری مجدد ارتباط پس از یک قطعی نیز از آن‌ها محافظت می‌شود. ممکن است بخشی از راه‌اندازی هدف ارزیابی نیاز به تنظیم دستی کانال‌هایی برای حفاظت از سایر ارتباطات وجود داشته باشد. درصورتی‌که پس از یک قطعی، توابع امنیتی هدف ارزیابی تلاش کند تا ارتباطات را به صورت خودکار و با دخالت عامل انسانی (در صورت لزوم) از سر گیرد، ممکن است پنجره‌ای باز شود که مهاجمان بتوانند از

شماره الزام	نام الزام
طریق آن به اطلاعات مهمی دست یابند یا ارتباط را در معرض خطر قرار دهند. در جایی که گواهینامه‌های کلید عمومی برای پشتیبانی از کانال FTP_ITC.1 استفاده شود، FIA_X509_EXT.1/Rev نیز باید استفاده شود (این الزامات فسخ گواهینامه را بررسی می‌کنند) و FIA_X509_EXT.1/ITT که فقط برای استفاده بین مؤلفه‌ای کانال‌های هدف ارزیابی توزیع شده است، تکرار نشود.	
۴۶	**مسیر امن ۱/مدیر**
توابع امنیتی هدف ارزیابی، باید قادر باشد مسیر ارتباطی بین خود و مدیران از راه دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را با استفاده از [انتخاب: IPsec، SSH، DTLS، TLS، HTTPS] فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های ارتباطی در برابر افشاء محافظت نموده و تغییرات داده‌های کانال را تشخیص دهد. **تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.**	
۴۷	**مسیر امن ۲/مدیر**
توابع امنیتی هدف ارزیابی باید به سرپرست راه دور اجازه دهد که ارتباطات را از طریق مسیر امن آغاز کند.	
۴۸	**مسیر امن ۳/مدیر**
توابع امنیتی هدف ارزیابی باید استفاده از مسیر امن را برای احراز هویت اولیه سرپرست و تمام فعالیت‌های راه دور سرپرستی الزامی کند. **نکته کاربردی ۶۲:** این الزام اطمینان حاصل می‌نماید که مدیران راه دور معتبر، تمام ارتباطات رابا توابع امنیتی هدف ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی تمام ارتباطات با توابع امنیتی هدف ارزیابی توسط سرپرستان دوردست، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل شده از طریق این کانال ارتباطی امن، با استفاده از پروتکل انتخاب‌شده در عبارت انتخاب، رمزگذاری می‌شوند. نویسنده هدف امنیتی، مکانیسم یا مکانیسم‌های پشتیبانی‌شده توسط توابع امنیتی هدف ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند.	

۷-۴ کلاس دیواره آتش (FFW)

برای مقابله با مشکل افشای غیرمجاز اطلاعات، دسترسی غیرمجاز به خدمات، سوءاستفاده از خدمات، حملات DoS و شناسایی مبتنی بر شبکه، محصول منطبق با استانداردها باید دارای قابلیت فیلترینگ ترافیک حالتمند باشند. این قابلیت منجر به محدود شدن جریان ترافیک شبکه بین شبکه‌های حفاظت‌شده و سایر شبکه‌ها می‌شود.

بازرسی حالتمند بسته‌ها منجر به ارتقای جریان بسته‌ها از طریق محصول می‌شود. محصول به جای اعمال مجموعه قوانین به هر بسته‌ای که از آن می‌گذرد، تعیین می‌کند که آیا بسته مذکور به یک اتصال «تأییدشده» تعلق دارد یا نه. TCP و UDP باید دارنده حداقلی از ویژگی‌ها باشند تا تعیین شود که آیا یک بسته بخشی از یک نشست برقرارشده است یا خیر. نویسنده هدف امنیتی می‌تواند ویژگی‌های نشست‌های TCP را بسط دهد و در صورت لزوم پروتکل ICMP را اضافه کند.

محصول منطبق با استانداردها می‌توانند از جریان ترافیک شبکه را ثبت و گزارش‌گیری کنند. به ویژه، هدف ارزیابی ابزار لازم را در اختیار راهبران قرار خواهد داد تا قوانین فایروال را به گونه‌ای پیکربندی کنند که در صورت منطبق بودن ترافیک شبکه با قوانین، از آن «گزارش‌گیری» شود. در نتیجه، اطلاعات گزارش‌گیری‌شده سودمندی از رویدادها در دستس خواهد بود.

شماره الزام	نام الزام
۴۹	فیلترینگ حالتمند ۱

توابع امنیتی هدف ارزیابی، باید برروی بسته‌های شبکه‌ای که توسط محصول پردازش میشود، فیلترنمودن حالتمند ترافیک را انجام دهد.

نکته کاربردی:

کلاس فایروال دارای یک عنصر به نام فیلتر نمودن حالتمند ترافیک شبکه است که بر روی بسته‌های شبکه پردازش شده توسط واسط‌های محصول اعمال می‌گردد. هر بسته‌ای که توسط واسط هدف ارزیابی دریافت می‌شود دارای مجموعه قوانینی است که بیانگر این است سیاست اعمال شده‌است یا اینکه مشخص می‌کند که بسته متعلق به یک ارتباط ایجادشده است. عناصر باقیمانده در این مؤلفه جزئیاتی از این سیاست را ارائه می‌دهد این الزام حتی اگر واسط با ترافیک شبکه اشباع شده‌باشد، بازهم اعمال می‌شود.

لازم به یادآوری است که محصول دارای یک پلتفرم زیربنایی است که به هیچ بسته ای اجازه عبور نمی‌دهد مگر آنکه در مجموعه قوانین، قانونی وجود داشته باشد که اجازه عبور آن را بدهد یا آن بسته متعلق به ارتباط ایجادشده است که قبلاً به آن اجازه عبور داده شده باشد. این اصل باید در طول راه‌اندازی هدف ارزیابی به درستی حفظ شود و بر اساس شکست‌هایی است که هدف ارزیابی ممکن است با آن روبرو شود.

۵۰	**فیلترینگ حالتمند ۲**

توابع امنیتی هدف ارزیابی، باید قوانین فیلترنمودن حالتمند ترافیک را با استفاده از فیلدهای پروتکل شبکه زیر تعریف نماید:

- ICMPv4
  - نوع
  - کد
- ICMPv6
  - نوع
  - کد
- IPv4
  - آدرس مبدأ
  - آدرس مقصد
  - پروتکل لایه انتقال
- IPv6
  - آدرس مبدأ
  - آدرس مقصد

- پروتکل لایه انتقال
- [انتخاب: نوع سرایند توسعه یافته IPv6 [اختصاص: لیست فیلدهای که در سرآیند IPv6 توسعه یافته است، هیچ فیلد دیگری]]

- TCP
  - پورت مبدأ
  - پورت مقصد
- UDP
  - پورت مبدأ
  - پورت مقصد
- و واسطه متمایز

نکته کاربردی:

این مؤلفه در زمان ایجاد قوانینی که توسط این الزام اجرا می‌گردند، ویژگی‌های مختلف قابل بکارگیری را شناسایی می نماید. واسط قابل‌اجرا یکی از ویژگی‌های هدف ارزیابی است و بقیه ویژگی‌های شناخته‌شده مرتبط با RFC ها تعریف شده‌است. توجه داشته باشید که "پروتکل لایه انتقال" دارای فیلد IPv4/IPv6 است که پروتکل قابل اجرا را شناسایی می‌کند، مانند TCP، UDP، ICMP، یا GRE. سرآیند IPv6 توسعه‌یافته در RFC 2460 تعریف شده است و نویسنده هدف امنیتی ممکن است فیلدها را درون هر سرآیند توسعه‌یافته پشتیبانی‌شده مشخص میکند، اگر هریک به‌عنوان ویژگی در ایجاد قوانین بازرسی استفاده شوند. همچنین «واسط» که در بالا معرفی شده است پورت خروجی است که ترافیک شبکه اجرایی را دریافت و یا به طور متناوب ارسال خواهد نمود.

۵۱	فیلترینگ حالتمند ۳

توابع امنیتی هدف ارزیابی، باید امکان انجام عملکردهای زیر را برای هر یک از قوانین فیلتر نمودن حالتمند ترافیک فراهم آورد:

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

نکته کاربردی:

این عنصر، عملکردهایی را تعریف می‌نماید که می‌تواند با قوانینی استفاده شده مطابق با ترافیک شبکه مرتبط گردد. قابل ذکر است که داده‌های گزارش‌گیری شده در الزام ممیزی امنیت معرفی شده‌اند.

آدرس مبدأ و مقصد پورت مبدأ و مقصد پروتکل لایه انتقال واسط هدف ارزیابی	استفاده از قوانین پیکربندی‌شده با عملیات"log"	FFW_RUL_EXT.1
واسط هدف ارزیابی که قادر به پردازش بسته‌ها نیست. شناسه‌ای از قوانین که باعث حذف بسته‌ها می‌شوند.	نشانه‌ای از بسته‌های کاهش‌یافته بعلت ترافیک شبکه خیلی زیاد	

۵۲	فیلترینگ حالتمند ۴

توابع امنیتی هدف ارزیابی، باید امکان اعمال هر یک از قوانین فیلتر نمودن حالتمند ترافیک را بر روی هر یک از واسط های شبکه مجزا فراهم آورد.

نکته کاربردی:

این عنصر محل اعمال قوانین را مشخص می‌کند. به‌طور مشخص، یک توابع امنیتی هدف ارزیابی مطابق با این پروفایل حفاظتی، باید قادر باشد که قوانین فیلتر نمودن را به هر یک از واسط‌های شبکه که در دسترس هستند و قابل متمایز شدن باشند و ترافیک شبکه لایه ۳ و ۴ را به کار می‌برند، اعمال نماید. واسط شبکه مجزا (متمایز) می‌تواند منطقی با فیزیکی باشد اما لزوماً به واسطی که از دید شبکه قابل مشاهده باشد، اشاره ندارد (به طور مثال لازم نیست که حتما به آن واسط آدرس IP اختصاص داده شده باشد).

قابل ذکر است که می‌توان یک مجموعه قوانین مجزا برای هر واسط داشته باشد و یا به‌طور متناوب یک مجموعه قوانین مشترک که بنحوی قوانین را به واسط های مشخصی اعمال کند.

۵۳	فیلترینگ حالتمند ۵

توابع امنیتی هدف ارزیابی باید:

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

- TCP: آدرس مبدأ و مقصد، پورت‌های مبدأ و مقصد، شماره توالی[1]، پرچم‌ها
- UDP: آدرس مبدأ و مقصد، پورت‌های مبدأ و مقصد
- [انتخاب: "ICMP : آدرس مبدأ و مقصد، نوع، [انتخاب: کد، [اختصاص: **لیستی از ویژگی‌های تطبیق**]"، هیچ پروتکل دیگری]

ب) جریان ترافیک موجود را از مجموعه جریان ترافیک ایجاد شده بر اساس [انتخاب: مدت زمان غیرفعال بودن نشست، اتمام جریان اطلاعات موردانتظار]، حذف نماید.

نکته کاربردی:

این عنصر الزام می دارد که پروتکل‌ها شناسایی شوند برای اینکه، توابع امنیتی هدف ارزیابی بتواند وضعیت یک نشست که مجاز به مستقر شدن بوده است را تعیین و مدیریت نماید و برای تصمیم‌گیری‌های جریان ترافیک در برابر پردازش کامل قوانین پیکربندی‌شده مورد استفاده قرار می‌گیرند. هم‌چنین این عنصر الزام می‌دارد صفات عملی که برای تطابق و تعیین نشست مستقر شده با بسته‌های شبکه مورد استفاده قرار می‌گیرند را مشخص نماید.

چنان‌چه ICMP به عنوان پروتکل انتخاب گردد، آدرس میدا و آدرس مقصد برای تعیین متعلق بودن یک بسته به ارتباط ایجادشده مورد استفاده قرار می گیرد. ممکن است از مشخصه‌های «نوع» و «کد» جهت ارائه قابلیت‌های محکمتری استفاده گردد تا مشخص شود که آیا بسته ICMP همان چیزی است که در جریان ارتباط ایجادشده انتظار می‌رفت برای مثال در صورت دریافت نشدن هیچ بسته درخواست echo، نباید انتظار داشت که بسته پاسخ echo بعنوان بخشی از جریان ارسال گردد. بخش اختصاص در انتخاب برای ویژگی‌های ICMP است که ممکن است در پیاده‌سازی‌هایی از ویژگی‌های IPv6 استفاده نمایند.

در قسمت دوم از عنصر بالا، لازم است که مشخص گردد که فایروال چگونه می‌تواند جریان اطلاعات برقرار شده از مجموعه جریان اطلاعاتی برقرارشده بر اساس مشاهده رویدادها حذف نماید. به طور مثال نشست TCP شروع شده توسط نقطه پایان، خاتمه یابد. این نقطه پایان، FIN Flag در بسته TCP است.

اگر پروتکل‌ها به صورت‌های مختلفی به کار روند، انتظار می‌رود که این تفاوت‌ها را در هدف امنیتی معرفی نماید.

۵۴	**فیلترینگ حالتمند ۶**

توابع امنیتی هدف ارزیابی، باید قوانین فیلترنمودن حالتمند ترافیک زیر را به طور پیش‌فرض بر روی تمام ترافیک شبکه اعمال

[1] Sequence number

نماید:

۱- توابع امنیتی هدف ارزیابی باید بسته‌های اطلاعاتی که به صورت نامعتبر قطعه‌بندی شده اند را رد نماید و قادر به [انتخاب: شمردن، ثبت] نمودن آن‌ها باشد.

۲- توابع امنیتی هدف ارزیابی باید بسته‌های قطعه‌بندی شده‌ای که نمی‌توانند به طور کامل مجدداً گردآوری شوند را رد نماید و قادر به [انتخاب: شمردن، ثبت] نمودن آن‌ها باشد.

۳- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ بسته اطلاعاتی شبکه، روی یک شبکه به صورت پخشی[۱] تعریف شده است.

۴- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ بر روی شبکه چندپخشی[۲] تعریف شده است، توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ از بسته اطلاعاتی شبکه به صورت یک آدرس برگشتی[۳] تعریف شده باشد.

۵- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ و یا آدرس مقصد بسته شبکه نامشخص باشد (به عنوان نمونه 0.0.0.0) و یا به صورت آدرس «رزرو شده برای استفاده در آینده» (به عنوان نمونه 240.0.0.0/4) همان‌گونه که در RFC5735 برای IPv4 مشخص شده، تعریف شده باشد.

۶- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ و مقصد بسته اطلاعاتی شبکه 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:2000::/3 نیست) همان‌گونه که در RFC3513 برای IPv6 مشخص شده، تعریف شده باشد.

۷- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه با گزینه‌های IP زیر را رد نماید و قادر به ثبت باشد:

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

۸- [انتخاب: [اختصاص: دیگر قوانین پیش‌فرضی که توسط توابع امنیتی هدف ارزیابی اجرا می‌گردد]، *بدون هیچ قانون دیگر*]

نکته کاربردی:

نسخه‌های آینده این cPP نیاز خواهد داشت که هدف ارزیابی این قوانین پیش‌فرض را بدون اینکه نیاز به اعمال پیکربندی باشد

۵۵	**فیلترینگ حالتمند ۷**

توابع امنیتی هدف ارزیابی، باید قادر به حذف و ثبت مطابق با قوانین زیر باشد:

---

[۱] Broadcast network

[۲] Multicast network

[۳] Loopback address

۱- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدأ آن با آدرس واسط شبکه‌ای که بسته‌های اطلاعاتی شبکه را دریافت نموده برابر باشد را کنار بگذارد و قادر به ثبت باشد. ۲- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدأ و یا مقصد آن یک آدرس link-local است را کنار بگذارد و قادر به ثبت باشد. ۳- توابع امنیتی هدف ارزیابی باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدأ 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. نکته: توجه داشته باشید که این قوانین پیکربندی شوند.

۵۶	**فیلترینگ حالتمند ۸**

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

نکته کاربردی:

این عنصر الزام دارد که سرپرست قادر به تعریف ترتیب است که کدام قوانین فیلترینگ پیکربندی‌شده برای تطابق پردازش شود. قوانین فیلترینگ تنها زمانی قابل‌اجرا هستند که یک نشست مجاز مستقر نشده‌باشد یا یک قانون پویا ایجاد شده‌است.

۵۷	**فیلترینگ حالتمند ۹**

توابع امنیتی هدف ارزیابی باید مانع از عبور جریان بسته‌های شود که هیچ قانونی انطباقی برای آن مشخص نشده است.

نکته کاربردی:

این عنصر الزام دارد، جز زمانی که بسته بخشی از نشست ایجاد شده است، همیشه باید مانع ترافیک شبکه شود هنگامی‌که هیچ قانونی اعمال نشده و هیچ عملیات دیگری نیاز نیست، اگرچه آن‌ها لزوماً ممنوع نیستند.

۵۸	**فیلترینگ حالتمند ۱۰**

توابع امنیتی هدف ارزیابی 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 [انتخاب: شمرده، ثبت] شود.

نکته کاربردی:

منظور از اتصالات نیمه‌باز TCP این است که فرآیند سه‌مرحله‌ی دست‌تکانی همان‌طور که در RFC 793 تعریف‌شده، کامل نشده‌است. اتصالات TCP کامل‌نشده به‌طور مثال آن‌هایی که بخش‌های SYN و SYN-ACK از فرآیند سه مرحله‌ای دست تکانی را تکمیل کرده‌اند. مصرف منابع ارزشمند در میزبان‌های پایانی و دستگاه‌های فیلترینگ حالتمند ترافیک در مسیر ترافیک

و حجم کافی، می‌تواند منجر به انکار شرایط سرویس شود. به‌منظور محافظت خود و هرگونه خدمات حفاظت شده هدفمند، هدف ارزیابی سازگار با استاندارد باید قادر به محدود کردن تعداد اتصالات نیمه‌باز TCP باشد.

۸-۴ کلاس IPS: جلوگیری از نفوذ

شماره الزام	نام الزام
۵۹	**کارکرد IPS مبتنی بر رفتار غیرعادی ۱**

توابع امنیتی هدف ارزیابی باید از تعریف [انتخاب: (انتخاب حداقل یکی یا هر دو): مبنا[۱] (مورد انتظار و تأییدشده)، الگوهای ترافیکی ناهنجار (غیرانتظار)] پشتیبانی کند و شامل مشخصات زیر باشد:

[انتخاب:

- توان عملیاتی[۲] ([اختصاص: عناصر داده‌ها (مثل بیت‌ها، بسته‌ها و غیره) در واحد زمان (مثل دقیقه، ساعت، روز و غیره)])
- زمان روز
- تناوب
- آستانه‌ها
- [اختصاص: روش‌های دیگر]]

و فیلدهای پروتکل شبکه زیر:

[انتخاب: تمامی سرآیند بسته و عناصر داده‌ها که در الزام «کارکرد IPS مبتنی بر امضاء» تعریف شده‌اند؛ [اختصاص: لیست زیرمجموعه سرآیند بسته و عناصر داده‌ها از الزام «کارکرد IPS مبتنی بر امضاء»]]

نکته کاربردی:

مبناها، ترافیک خوب شناخته شده را تعریف می‌کنند (که در الزام «کارکرد IPS مبتنی بر رفتار غیرعادی ۳» مجاز شمرده شده است) در حالی که ترافیک ناهنجار، تعریف «ترافیک متخلف» است که باید با اقدامات دیگری که در الزام «کارکرد IPS مبتنی بر رفتار غیرعادی ۳» تعریف شده با آن مواجه شد.

تناوب را می‌توان چنین تعریف کرد: تعداد دفعات وقوع هر رویداد (مثل شناسایی بسته‌هایی که مطابق با یک امضا هستند) طی یک

[۱] Baselines
[۲] Throughput

بازه مشخص زمانی، مانند تعداد نشست‌های FTP که طی یک ساعت ایجاد می‌شوند. اگر «تناوب‌ها» انتخاب شوند، «خلاصه مشخصات محصول» باید توضیحی از نحوه تعریف تناوب‌ها در توابع امنیتی هدف ارزیابی ارائه کند. آستانه‌ها را می‌توان این‌گونه تعریف کرد: میزان یا درصد انحراف از مرزها یا سطوح مورد انتظار، مثل تعداد مگابایت‌هایی از داده که هر ساعت از FTP عبور می‌کنند. اگر «آستانه‌ها» انتخاب شود، «خلاصه مشخصات محصول» باید توضیحی از نحوه تعریف آستانه‌ها در توابع امنیتی هدف ارزیابی ارائه نماید.	
۶۰	**کارکرد IPS مبتنی بر رفتار غیرعادی ۲**
توابع امنیتی هدف ارزیابی باید از تعریف فعالیت غیرعادی از طریق: [انتخاب: پیکربندی دستی توسط سرپرست، پیکربندی خودکار] پشتیبانی نماید. **نکته کاربردی:** مبنا و ناهنجاری گاهی می‌توانند به صورت دستی توسط سرپرست محصول، پیکربندی/تعریف شوند (یا وراد کردن تعاریف)، یا چیزی که توابع امنیتی هدف ارزیابی بتواند آن را به صورت خودکار با بازرسی ترافیک شبکه طی بازه زمانی مشخص، تعریف/ایجاد کند (به این کار پروفایلینگ نیز گفته می‌شود). لازم نیست که توابع امنیتی هدف ارزیابی IPS قابلیت «پروفایلینگ» شبکه را داشته باشد تا مبنا یا قاعده‌ای را به صورت پویا تعریف کند و اگر توابع امنیتی هدف ارزیابی IPS این کارکرد را داشته باشد، چنین کارکردی به عنوان بخشی از بسته تکمیلی IPS مورد ارزیابی قرار نمی‌گیرد.	
۶۱	**کارکرد IPS مبتنی بر رفتار غیرعادی ۳**

توابع امنیتی هدف ارزیابی باید به عملیات‌های زیر اجازه دهد که با خط‌مشی‌های مبتنی بر رفتارهای غیرعادی IPS ترکیب شوند.
• در هر حالتی، برای هر واسط حسگری: [انتخاب:
  ○ اجازه به جریان ترافیک
  ○ ارسال یک بازنشانی TCP به آدرس مبدأ ترافیک متخلف
  ○ ارسال یک بازنشانی TCP به آدرس مقصد ترافیک متخلف
  ○ ارسال یک پیام غیرقابل دسترسی ICMP [انتخاب‌ها: میزبان، مقصد، پورت]
  ○ تریگر یک ابزار شبکه غیر توابع امنیتی هدف ارزیابی برای بلوکه کردن الگوی ترافیک متخلف]
• در حالت درون‌خطی:
  ○ اجازه به جریان ترافیک	

- بلوکه کردن/ قطع جریان ترافیک

و [انتخاب: اصلاح و ارسال بسته‌ها قبل از اینکه از توابع امنیتی هدف ارزیابی عبور کنند، بدون هیچ اقدام دیگر]

۶۲	**بلوکه کردن آدرس IP ۱**

توابع امنیتی هدف ارزیابی باید از پیکربندی و پیاده‌سازی لیست سیاه و لیست سفید از آدرس‌های IP [انتخاب: آدرس مبدأ، آدرس مقصد] پشتیبانی نماید.

نکته کاربردی:

نوع آدرس‌هایی که در این تابع هدف امنیتی تعریف شده است، محدود است به آدرس‌های IP (مثل یک آدرس IP واحد یا بازه‌ای از آدرس‌های IP) زیرا این بسته تکمیلی IPS، به بازرسی ترافیک IP محدود است. توابع امنیتی هدف‌های ارزیابی از نوع IPS از فعال‌سازی کارکردهایی که جریان ترافیک را بر اساس انواع دیگر آدرس (مثل آدرس‌های MAC) متوقف/ مجاز کنند، جلوگیری نمی‌نماید؛ اما زمانی که از این کارکرد استفاده می‌شود، مستندات دستورالعمل‌ها و «خلاصه مشخصات محصول» باید شرح دهند که چه نوع پیکربندی باعث ایجاد لیست آدرس‌های سفید و سیاه غیر IP شده‌اند تا بر لیست آدرس‌های مبتنی بر IP اولویت یابد.

۶۳	**بلوکه کردن آدرس IP ۲**

توابع امنیتی هدف ارزیابی باید به سرپرستان IPS و [انتخاب: هیچ نقش دیگر [اختصاص: نقش‌های دیگر]] اجازه دهد که عناصر خط‌مشی IPS را پیکربندی نماید: [**انتخاب: قوانین لیست سیاه، قوانین لیست سفید، آدرس IP، [اختصاص: دیگر عناصر خط ومشی IPS]، هیچ عناصر خط و مشی IPS دیگری]**

۶۴	**تحلیل ترافیک شبکه ۱**

توابع امنیتی هدف ارزیابی باید ترافیک شبکه مبتنی بر IP را که به واسطهای حس‌گر توابع امنیتی هدف ارزیابی جریان دارد، مورد تجزیه و تحلیل قرار دهد و نقض خط‌مشی‌هایی IPS که توسط سرپرست تعریف شده را شناسایی نماید.

نکته کاربردی:

اگرچه در مورد برخی از هدف ارزیابی‌ها ممکن است که هر واسط هدف ارزیابی بتواند یک واسط حس‌گر باشد، حتی این قابلیت مورد نیاز نیست. الزامات کارکرد امنیتی از اصطلاح "واسط حس‌گر" استفاده می‌کند که اشاره به هر واسط هدف ارزیابی دارد و یک یا چند سیاست IPS را اعمال می‌کند. یک سیاست IPS تعریف‌شده از نظر اجرایی و مدیریتی شامل هر مجموعه از قوانین برای آنالیز

ترافیک، مسدود کردن ترافیک، تشخیص امضا و/یا تشخیص ناهنجاری‌ها است که بر روی یک یا چند واسط هدف ارزیابی اعمال شده‌است. هدف ارزیابی ممکن است قادر باشد که به سرپرست این اجازه را دهد که اولویت عناصر خط ومشی IPS را پیکربندی کند (لیست سفید، لیست سیاه، قوانین مبتنی بر امضا، قوانین مبتنی بر ناهنجاری)، اما هر قابلیت پیکربندی توسط این EP لازم نیست.

۶۵	**تحلیل ترافیک شبکه ۲**

توابع امنیتی هدف ارزیابی باید پروتکل‌های ترافیک شبکه زیر را پردازش کند (بتواند بازرسی کند):

- پروتکل اینترنت (IPv4)، RFC 791
- پروتکل اینترنت نسخه ۶ (IPv6)، RFC 2460
- پروتکل پیام کنترل اینترنت نسخه ۴ (ICMPv4)، RFC 792
- پروتکل پیام کنترل اینترنت نسخه ۶ (ICMPv6)، RFC 2463
- پروتکل کنترل انتقال (TCP)، RFC 793
- پروتکل داده‌های کاربر (UDP)، RFC 768

نکته کاربردی:

شناسایی (احرازهویت) پروتکل‌های RFC به منزله این نیست که توابع امنیتی هدف ارزیابی باید تضمین کند تمامی بسته‌ها در تمامی اوقات با پروتکل‌های RFC شناسایی‌شده مطابقت دارد. همچنین به منزله این نیست که توابع امنیتی هدف ارزیابی می‌تواند در هر جریان ترافیکی در هر زمانی، تطابق کامل را با RFC اعمال کند. شناسایی پروتکل‌های RFC چارچوب مرجعی است برای فهم محتوای بسته‌ها (سرآیندها، فیلدها، وضعیت‌ها، فرمان‌ها و غیره) که در این الزام کارکرد امنیتی و دیگر الزامات، شناسایی شده‌اند؛ یعنی توابع امنیتی هدف ارزیابی باید بتواند پیاده‌سازی RFC را تا حدی بفهمد که پارامترهای RFC از طریق الزامات کارکرد امنیتی مشخص شود.

۶۶	**تحلیل ترافیک شبکه ۳**

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

- حالت بی‌قاعده (فقط شنود): [اختصاص: لیستی از انواع واسط]،

[۱] Promiscuous

- حالت درون‌خط (داده‌های عبوری): [اختصاص: لیستی از انواع واسط]،
- حالت مدیریت: [اختصاص: لیستی از انواع واسط]،
- [انتخاب:
  - واسط‌هایی با قابلیت راه‌اندازی مجدد نشست: [اختصاص: لیستی از انواع واسط با قابلیت راه‌اندازی مجدد نشست]،
  - [اختصاص: انواع دیگر واسط‌ها]]،
  - و هیچ نوع دیگری از انواع واسط] .

نکته کاربردی:

انواع واسط‌ها ممکن است اترنت، گیگابیت اترنت و غیره باشد. واسط‌های بی‌قاعده، واسط‌هایی هستند که ترافیک شبکه را به منظور بازرسی ترافیک شنود می‌کنند، اما هیچ کارکردی در لایه‌های۲،۳ و بالاتر فراهم نمی‌آورند؛ بنابراین سرویس‌های شبکه بر روی واسط شنود نمی‌شوند و هیچ پشته پروتکل IP بر روی واسط فعال نیست، در نتیجه هیچ آدرس IP به واسطی اختصاص داده نمی‌شود. واسط‌های درون‌خط، جفت واسط‌هایی هستند که مسیری را برای ترافیک شبکه به منظور پیمایش توابع امنیتی هدف ارزیابی فراهم می‌آورند به‌طوری‌که بتوان جریان شبکه را بلوکه و یا توسط توابع امنیتی هدف ارزیابی بلادرنگ ویرایش کرد. واسط‌های بی‌قاعده و درون‌خط معمولاً کارکردهای لایه ۳ و بالاتر را پشتیبانی نمی‌کنند، آن‌ها ممکن است کارکردهای لایه ۲ OSI را فراهم نمایند (با آدرس فیزیکی MAC نسبت داده شده به واسط‌ها) تا اجازه دهند دستگاه‌های شبکه مجاور، ترافیک شبکه را به توابع امنیتی هدف ارزیابی ارسال و یا دریافت کنند.

۶۷	**کارکرد IPS مبتنی بر امضاء ۱**

توابع امنیتی هدف ارزیابی باید از بازرسی محتوای سرآیند بسته‌ها پشتیبانی نماید و بتواند حداقل سرآیند فیلدهای زیر را بازرسی نماید:

- IPv4: نسخه، طول سرآیند، طول بسته، پرچم IP، ID، آفست تکه[۱]، زمان فعالیت (TTL)، پروتکل، سرآیند CheckSum، آدرس مبدأ، آدرس مقصد، گزینه‌های IP.
- IPv6: نسخه، کلاس ترافیک، برچسب جریان، طول محتوا، سرآیند بعدی، محدودیت گام، آدرس مبدأ، آدرس مقصد، سرآیند مسیریاب، گزینه‌های آدرس مبدأ.

[۱] Fragment

- ICMP: نوع، کد، CheckSum سرآیند و باقی سرآیندها (بر حسب کد و نوع ICMP متفاوت است)
- ICMPv6: نوع، کد و CheckSum سرآیند
- TCP: پورت مبدأ، پورت مقصد، عدد توالی، عدد تصدیق، آفست، رزرو، پرچم‌های TCP، پنجره، CheckSum، نشانگر اضطراری و گزینه‌های TCP
- UDP: پورت مبدأ، پورت مقصد، طول و UDP CheckSum

۶۸	**کارکرد IPS مبتنی بر امضاء ۲**

توابع امنیتی هدف ارزیابی باید از بازرسی داده محتوای بسته‌های داده Paylpad پشتیبانی کند و قادر باشد حداقل عناصر داده زیر را بازرسی کند تا فرایند تطابق الگوهای مبتنی بر رشته‌های داده را اجرا کند:

- داده‌های ICMPv4: کاراکترهایی بیشتر از ۴ بایت اول از سرآیند ICMP
- داده‌های ICMPv6: کاراکترهایی بیشتر از ۴ بایت اول از سرآیند ICMP
- داده‌های TCP (کاراکترهایی بیشتر از ۲۰ بایت 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.
  - [انتخاب: [اختصاص: دیگر انواع بازرسی محتوای TCP، هیچ انواع دیگری از بازرسی TCP payload]
- داده UDP: کاراکترهایی بیشتر از هشت بایت اول سرآیند UDP
- [اختصاص: دیگر انواع بازرسی محتوای بسته‌ها]

علاوه بر این، توابع امنیتی توابع امنیتی هدف ارزیابی باید از بازترکیب استریم پشتیبانی کند یا به جای آن قادر به شناسایی محتوای مخرب باشد، حتی اگر در چند بسته‌ی غیر قطعه‌بندی مختلف تقسیم شده باشد.

۶۹	**کارکرد IPS مبتنی بر امضاء ۳**

توابع امنیتی هدف ارزیابی باید قادر به کشف امضاهای مبتنی بر سرآیند (با استفاده از فیلدهای مشخص شده در الزام شماره‌ی ۸۷ «کارکرد IPS مبتنی بر امضاء ۱») در واسط‌های حسگر IPS باشد.

- حملات IP
  - هم‌پوشانی تکه‌های IP(حمله Teardrop، حمله Bonk و یا حمله Boink)
  - یکسان بودن آدرس IP مبدأ با آدرس IP مقصد (Land attack)
- 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

۷۰	**کارکرد IPS مبتنی بر امضاء ۴**

توابع امنیتی هدف ارزیابی باید بتواند 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)
  - سیل‌آسا ICMP (حمله Smurf، سیل‌آسا ping)
  - سیل‌آسا TCP (مثل سیل‌آسا SYN)
- سیل‌آسا به شبکه (حمله DoS)
  - اسکن پورت و پروتکل اسکن پروتکل IP
  - اسکن پورت TCP
  - اسکن پورت UDP

- اسکن ICMP

نکته کاربردی:

الزامات کارکرد امنیتی حداقل مجموعه‌ای از فیلدهای سرآیند بسته، رشته‌های payload بسته، انواع امضا و الگوهای ترافیک مخرب بالقوه (به‌طور مثال، جریان سیل‌آسا و اسکن) است که هدف ارزیابی ممکن است قادر به تشخیص باشد. امضاهای معتبر از یک، برخی، یا تمام ویژگی‌های ذکرشده در الزامات کارکرد امنیتی تشکیل می‌شود، اما فقط آن‌هایی که در الزامات کارکرد امنیتی لیست شده‌اند توسط ارزیاب تست خواهد شد. مجموعه‌ای از انواع امضا، الگوهای ترافیک، غیره تعریف‌شده در الزامات کارکرد امنیتی به‌صورت لیست جامع و کامل از فعالیت مخرب در نظر گرفته نشده است، هدف الزامات کارکرد امنیتی رسیدگی به حملات از یک IP مبدأ واحد است.

اسکن پورت و پروتکل اشاره به شناسایی حملاتی دارد که آدرس‌های IP هدف را برای سرویس‌های باز کردن/گوش دادن/ پاسخگویی با هدف قرار دادن چندین پروتکل/پورت بر روی یک یا چند آدرس IP هدف با استفاده از الگوهای واضح (شماره ترتیب) از شماره‌های پورت/پروتکل یا توسط شماره‌های پورت/پروتکل تصادفی و/یا تأخیرهای زمانی تصادفی بین انتقال‌ها اسکن می‌کند.

انتظار می‌رود که فروشندگان محصولات IPS، امضاهای از پیش‌تعریف شده‌ای را پشتیبانی خواهند کرد، اما بازرسی اثربخشی امضاهای از پیش تعریف‌شده هدف EP نیست. بجای آن، EP بر روی توانایی هدف ارزیابی برای اجرای تجزیه‌وتحلیل دقیق ترافیک شبکه و امضاهای تعریف‌شده‌ای که ممکن است در طول ارزیابی استفاده شوند، تمرکز دارد، تیم ارزیابی انتظار دارند از امضاهای ساخته‌شده به‌صورت سفارشی استفاده کنند. این مجموعه از انواع امضاها، الگوهای ترافیک، غیره انتخاب شده است: ۱) قرار دادن مرزهای معقول و منطقی در اطراف دامنه تست ۲) ارائه یک نمونه کافی و مناسب از محتوای بسته و الگوهای ترافیک به‌منظور نشان دادن توانایی هدف ارزیابی برای بازرسی محتوای بسته، جمع‌آوری آمارهای الگو ترافیک بر روی یک مدت زمان و ارتباط داده‌های جمع‌آوری‌شده.

یک واسط حس‌گر IPS به هر واسط هدف ارزیابی اشاره دارد که سیاست IPS در حال حاضر اعمال کرده است.

۷۱	**کارکرد IPS مبتنی بر امضاء ۵**

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: [انتخاب:
  - 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 [انتخاب: میزبان، مقصد، پورت]

- هدف‌گیری یک ابزار شبکه غیر توابع امنیتی هدف ارزیابی برای بلوکه کردن الگوی ترافیک متخلف]
- حالت بر خط
  - اجازه به جریان ترافیک
  - بلوکه کردن/ قطع جریان ترافیک
  - و [انتخاب: اصلاح و ارسال بسته‌ها قبل از اینکه از توابع امنیتی هدف ارزیابی عبور کنند، بدون هیچ اقدام دیگری]

۳

۵ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف‌کننده چگونگی ارزیابی محصول است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۵-۱ 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 نیست، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان محصول باشد.

۵-۱-۱مشخصات کارکردی

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** 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 نیست.

مؤلفه‌های محتوایی		
نام خانواده	**عنصر امنیتی**	
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجراکننده کارکرد امنیتی[۱] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲] توصیف نماید.	
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:**	

[۱]-SFR-enforcing TSFI
[۲]-SFR-supporting TSFI

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.3C)** **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** 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.

۵-۲ 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 ارائه‌دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۵-۲-۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	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 مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** 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 مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطهای در دسترس، 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 مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس 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 مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط 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 مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۵-۲-۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** 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.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
	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.

۵-۳ 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 EAL1) تست بر اساس 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.

۵-۳-۱ 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 است. ارزیاب باید در سند «گزارش تست»، طرح تست و نتایج آن را مستند نماید.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1C)** **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: تست مستقل ۱ **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

۵-۴ کلاس آسیب‌پذیری

۵-۴-۱ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند،

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	مشخص نماید.

۵-۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) 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 توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۵-۵-۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، است (بدین معنی که جدا از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب‌گذاری 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.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۵-۵-۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مؤلفه: (ALC_CMS.1.1C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۴

۶ پیوست یک: الزامات اختیاری

چنان که در مقدمه این پروفایل حفاظتی نیز گفته شد، الزامات اولیه (الزاماتی که باید توسط محصول مورد ارزیابی رعایت شوند) در این پروفایل تشریح شده‌اند. علاوه بر این، دو نوع الزامات دیگر نیز وجود دارند که در پیوست‌های یک، دو و سه به آن‌ها پرداخته شده است. نوع اول (پیوست یک و دو) از الزاماتی تشکیل شده است که می‌توان آن‌ها را در سند هدف امنیتی گنجاند، اما برای انطباق با این پروفایل حفاظتی ضروری نیستند. نوع دوم (پیوست سه) از الزاماتی تشکیل شده است که مبتنی بر عبارت‌های انتخاب سایر الزامات کارکرد امنیتی این پروفایل حفاظتی هستند. اگر انتخاب‌های خاصی انجام شده باشند، الزامات پیوست مربوطه نیز باید در متن هدف امنیتی گنجانده شوند (مثلاً پروتکل‌های رمزنگاری انتخاب‌شده در یک الزام کانال امن).

۶-۱ کلاس ممیزی امنیت

درصورتی‌که در محصول مورد ارزیابی فضای حافظه محلی برای داده‌های ممیزی در نظر گرفته شده باشد، محصول مورد ارزیابی می‌تواند ادعا کند که مطابق آنچه در «ذخیره‌سازی رویدادهای ممیزی» گفته شده است، از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری به عمل آورد. فضای حافظه محلی دستگاه‌های شبکه برای ذخیره‌سازی داده‌های ممیزی، محدود است. اگر این حافظه پر شود، امکان از دست رفتن داده‌های ممیزی وجود خواهد داشت. ممکن است یک سرپرست محصول بخواهد اطلاعات مربوط به تعداد داده‌های ممیزی ازدست‌رفته را داشته باشد. این تعداد می‌تواند نشان‌دهنده مشکلات سرور باشد؛ بنابراین، «محل ذخیره‌سازی داده‌های ممیزی» و «محل ذخیره‌سازی داده‌های ممیزی» تهیه شده‌اند تا این قابلیت‌های اختیاری دستگاه‌های شبکه را بیان کنند.

همچنین جدول زیر مربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب است. همان‌طور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

جدول ۲. الزامات انتخابی هدف ارزیابی و رویدادهای قابل ممیزی

ردیف	الزام	رویدادهای ممیزی	لیست سوابق ممیزی اضافی
۱.	FAU_STG.1	هیچ	هیچ
۲.	FAU_STG_EXT.2/LocSpace	هیچ	هیچ
۳.	FAU_STG.3/LocSpace	کمبود فضای ذخیره‌سازی برای رویدادهای ممیزی	هیچ
۴.	FIA_X509_EXT.1/ITT	تلاش ناموفق برای تائید یک گواهینامه	دلیل شکست

۵.	FMT_MOF.1/Services	آغاز و پایان سرویس‌ها	هیچ
۶.	FMT_MTD.1/CryptoKeys	مدیریت کلیدهای رمزنگاری	هیچ
۷.	FPT_ITT.1	آغاز یک کانال امن خاتمه یک کانال امن شکست عملکرد کانال امن	شناسایی آغازکننده و هدف تلاش ناموفق برای برقراری کانال‌های امن
۸.	FTP_TRP.1/Join	آغاز یک مسیر امن خاتمه یک مسیر امن شکست عملکرد مسیر امن	هیچ
۹.	FCO_CPC_EXT.1	فعال‌سازی ارتباط بین یک جفت مؤلفه غیرفعال سازی ارتباط بین یک جفت مؤلفه	هویت جفت نقاط پایانی فعال یا غیرفعال شده

نکته کاربردی:

رویدادهای ممیزی FIA_X509_EXT.1/ITT بر اساس هدف ارزیابی است که با اطمینان از موارد زیر، قادر به تکمیل اعتبار گواهینامه نیست:

- وجود افزونه basicConstraints و پرچم CA که برای تمامی گواهینامه‌های CA به حالت «True» تنظیم شده باشد.
- تائید امضای دیجیتالی CA سلسله مراتبی معتبر
- خواندن/دسترسی به CRL یا دسترسی به سرور OCSP (مطابق انتخاب در سند هدف امنیتی)

اگر هرکدام از این موارد رد شوند، باید یک رویداد ممیزی عدم موفقیت، در لاگ ممیزی نوشته شود.

شماره الزام	نام الزام
۷۲	**ذخیره‌سازی داده‌های ممیزی محافظت شده ۱**
توابع امنیتی هدف ارزیابی باید از پاک شدن غیرمجاز سوابق ممیزی ذخیره شده در دنباله ممیزی جلوگیری نماید.	
۷۳	**ذخیره‌سازی داده‌های ممیزی محافظت شده ۲**
توابع امنیتی هدف ارزیابی باید بتواند از تغییرات غیرمجاز سوابق ممیزی ذخیره شده در دنباله ممیزی جلوگیری نماید.	
۷۴	**شمارش داده‌های ممیزی از دست رفته**
توابع امنیتی هدف ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده‌های ممیزی [انتخاب: از بین رفته، بازنویسی شده، [اختصاص: سایر اطلاعات]] را ارائه کند. توابع امنیتی هدف ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده¬های ممیزی ۳» را انجام می‌دهد. **نکته کاربردی:** این گزینه در صورتی باید انتخاب شود که محصول مورد ارزیابی از این کارکرد پشتیبانی کند. درصورتی‌که حافظه محلی داده‌های ممیزی توسط سرپرست محصول خالی شود، شمارنده‌های مربوط به انتخاب انجام‌شده باید به مقادیر اولیه خود برگردند (این مقدار در اکثر موارد صفر است). اسناد راهنما باید به سرپرست محصول هشدار دهند که خالی کردن حافظه ممکن است سبب از دست رفتن داده‌ها شود. برای اهداف ارزیابی توزیع شده، هر کامپوننتی که شمارش داده‌های ممیزی از دست رفته را پیاده‌سازی کرده است، باید مکانیسم دسترسی و مدیریت این اطلاعات برای مدیر را فراهم نماید. اگر FAU_STG_EXT.2/LocSpace به سند هدف امنیتی اضافه شود، سند هدف امنیتی باید هر وضعیتی که داده ممیزی از دست رفته شمارش نمی‌شود را مشخص نماید.	
۷۵	**نمایش هشدار برای فضای ذخیره‌سازی محلی**
توابع امنیتی هدف ارزیابی باید در صورتی که دنباله ممیزی بیش از ظرفیت ذخیره‌سازی دنباله ممیزی باشد، برای اطلاع‌رسانی به مدیر هشداری ایجاد نماید.	

نکته کاربردی:

درصورتی‌که محصول مورد ارزیابی امکان تولید پیام مربوطه را داشته باشد این گزینه انتخاب می‌شود. درصورتی‌که داده‌های مربوط به رویدادهای قابل‌ممیزی تنها در حافظه محلی ذخیره شده باشند، این هشدار می‌تواند اهمیت بسیار زیادی داشته باشد.

باید اطمینان حاصل نمود که هشدار مورداشاره در «محل ذخیره‌سازی داده‌های ممیزی ۳» را می‌توان به اطلاع کاربر رساند. ارتباط باید از طریق سوابق ممیزی صورت گیرد، زیرا ممکن است در هنگام رخ دادن اتفاق، نشست فعالی برای مدیریت این کار وجود نداشته باشد.

پیام هشدار باید هنگامی که فضای محلی برای ذخیره داده ممیزی در حال پر شدن بود و/یا ممکن باشد هدف ارزیابی به علت فضای محلی ناکافی داده‌های ممیزی را از دست بدهد، مدیر را مطلع نماید.

برای اهداف ارزیابی توزیع شده‌ای که در زمان پر شدن فضای حافظه محلی داده ممیزی هشداری نمایش می‌دهند، باید مشخص شود که کدام مؤلفه‌های هدف ارزیابی از این ویژگی پشتیبانی می‌کنند (اگر به عنوان هدف ارزیابی کلی انتخاب شده باشد، پشتیبانی تمامی مؤلفه‌های هدف ارزیابی از این ویژگی الزامی نیست). هر مؤلفه‌ای که از این ویژگی پشتیبانی می‌کند باید هشداری را خودش یا از طریق مؤلفه دیگری تولید کند.

اگر FAU_STG.3/LocSpace به سند هدف امنیتی اضافه شده باشد، سند هدف امنیتی باید هر حالتی که ممکن است سوابق ممیزی "به طور مخفی از دست روند" را مشخص نماید.

۶-۲ کلاس شناسایی و تائید اعتبار

شماره الزام	نام الزام
۷۶	تائید گواهینامه X509 (۱)

توابع امنیتی مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند:

- تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه با پشتیبانی از حداقل طول مسیر دو گواهی‌نامه
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد
- توابع امنیتی مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است.
- توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) چنان که در RFC 6960 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC 5759 بخش ۵ تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC5280 بخش ۶,۳ تعریف شده است، هیچ روش فسخی] تائید کند
- توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند:
- گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.
- گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
- گواهی‌نامه‌های OCSP ارائه شده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.

نکته کاربردی:

این الزام باید زمانی انتخاب شود که هدف ارزیابی توزیع شده باشد و پروتکل‌های انتخاب شده در FPT_ITT.1 از گواهینامه‌های X509 برای احراز هویت دوطرفه استفاده نمایند. در این مورد، به دلیل وجود الزامات اضافی شامل فعال‌سازی و غیرفعال سازی کانال ITT در FCO_CPC_EXT.1، استفاده از چک لیست فسخ اختیاری است. اگر بررسی فسخ پشتیبانی نشده باشد، نویسنده هدف امنیتی نباید هیچ روش فسخ را انتخاب کند. هرچند، اگر بررسی فسخ گواهینامه پشتیبانی شده باشد، نویسنده هدف امنیتی استفاده از OCSP یا CRL ها را انتخاب می‌کند.

هدف ارزیابی باید قادر به پشتیبانی از حداقل طول مسیر دو گواهینامه باشد. به این معنی که باید از سلسله مراتب گواهینامه شامل حداقل یک گواهینامه اصلی امضا شده توسط خودش و یک گواهینامه شناسایی هدف ارزیابی را پشتیبانی کند.

TSS باید زمان اجرا شدن بررسی لغو را شرح دهد. انتظار می‌رود زمانی که یک گواهینامه در مرحله احراز هویت استفاده می‌شود، بررسی فسخ انجام شود. تائید وضعیت گواهینامه X509 فقط زمانی که در دستگاه بارگذاری می‌شود، کافی نیست.

در صورتی که هدف ارزیابی از عملکردهایی پشتیبانی کند که از هیچ‌کدام از انواع گواهینامه‌های لیست شده در قوانین extendedKeyUsage در FIA_X509_EXT.1.1 پشتیبانی نکند، باید در TSS تعیین شود و بخش مربوطه الزام کاملاً رعایت شده در نظر گرفته شود. هرچند، اگر هدف ارزیابی از عملکردهایی پشتیبانی کند که از هرکدام از انواع این گواهینامه‌ها استفاده می‌کند، باید قوانین متناظر همانند SFR رعایت شوند.

۷۷	تائید گواهینامه X509 (۲)

توابع امنیتی هدف 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.

نکته کاربردی:

این الزام در مورد گواهی‌نامه‌هایی اعمال می‌شود که توسط محصول مورد ارزیابی بکار رفته و پردازش شده باشند. این الزام همچنین اضافه شدن گواهی‌نامه‌ها به لیست گواهی‌نامه‌های معتبر CA را محدود می‌کند.

۳-۶ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام	
۷۸	**حفاظت از انتقال داخلی داده‌های اساسی محصول**	FPT_ITT.1.1
توابع امنیتی هدف ارزیابی باید از افشای داده‌های محصول محافظت نموده و زمانی که با استفاده از [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] بین بخش‌های جداگانه هدف ارزیابی فرستاده شود، تغییرات را تشخیص دهد. **نکته کاربردی:** این الزام فقط برای اهداف ارزیابی توزیع شده و اطمینان از این‌که تمامی ارتباطات بین مؤلفه‌های هدف ارزیابی توزیع شده از طریق استفاده از کانال ارتباطی رمز شده محافظت می‌شوند، تکرار شده است. داده‌های ارسال شده در این کانال ارتباطی امن توسط پروتکل انتخاب شده رمز می‌شوند. نویسنده هدف امنیتی باید کانال‌ها و پروتکل‌های استفاده شده توسط هر جفت مؤلفه ارتباطی در هدف ارزیابی توزیع شده را، مناسب با تکرار این الزام، مشخص نماید. همچنین این کانال ممکن است به عنوان کانال ثبت برای فرآیند ثبت، همان‌طور که در بخش ۳,۳ و FCO_CPC_EXT.1.2 شرح داده شده است، استفاده شود. اگر TLS انتخاب شود، الزامات داشتن شناسه مرجع پیاده‌سازی شده توسط کاربر (FCS_TLSC_EXT.1.2)، برقرار شده است و شناسه ممکن است توسط فرآیند کشف "Gatekeeper" ایجاد شود. TSS باید فرآیند کشف را شرح داده و نحوه تأمین مؤلفه "joining" برای شناسه مرجع مشخص شود.		
۷۹	**مسیر امن ۱/** Join	FTP_TRP.1.1/Join
توابع امنیتی هدف ارزیابی باید یک مسیر ارتباطی بین خود و یکی از مؤلفه‌های متصل که به طور منطقی از سایر مسیرهای ارتباطی متمایز است برقرار نماید و شناسایی مطمئنی از [انتخاب: نقطه پایانی توابع امنیتی هدف ارزیابی، مؤلفه متصل و نقطه پایانی توابع امنیتی هدف ارزیابی] ارائه دهد و از تغییر [انتخاب: و افشای، هیچ] داده‌های تبادل شده محافظت نماید.		
۸۰	**مسیر امن ۲/** Join	FTP_TRP.1.2/Join
توابع امنیتی هدف ارزیابی باید به [انتخاب: توابع امنیتی هدف ارزیابی، کاربران محلی مؤلفه متصل، کاربران راه دور] اجازه آغاز ارتباط توسط مسیر امن را بدهد.		
۸۱	**مسیر امن ۳/** Join	FTP_TRP.1.3/Join
توابع امنیتی هدف ارزیابی باید برای اتصال مؤلفه‌ها به توابع امنیتی هدف ارزیابی تحت محدودیت‌های محیطی مشخص شده در مرجع راهنمای عملیاتی، از مسیر امن استفاده کند. **نکته کاربردی:** این الزام یکی از انواع شناسایی کانال در انتخاب اصلی الزام FCO_CPC_EXT.1.2 را برقرار می‌کند. در FTP_TRP.1.1/Join، "مؤلفه joining"، موجودیت IT است که برای پیوستن به هدف ارزیابی توزیع شده توسط فرآیند ثبت تلاش می‌کند. این الزام نیازمند توانایی مؤلفه‌ها برای برقراری ارتباط امن در طول ایجاد توابع امنیتی هدف ارزیابی توزیع شده (یا زمانی که مؤلفه‌ای به توابع امنیتی هدف ارزیابی توزیع شده موجود اضافه می‌شود) است. در این الزام، زمانی که توابع امنیتی هدف ارزیابی از جفت مؤلفه‌های اولیه ایجاد می‌شوند، ممکن است هرکدام از این مؤلفه‌ها به عنوان توابع امنیتی هدف ارزیابی شناسایی شوند. انتخاب موجود در انتهای FTP_TRP.1.1/Join تشخیص می‌دهد که در برخی موارد ممکن است محرمانگی توسط کانال ارائه		

شماره الزام	نام الزام
۸۲	**مدیریت رفتار توابع امنیتی/ خدمات**
توابع امنیتی هدف ارزیابی توانایی فعال کردن و غیرفعال کردن شروع و متوقف کردن سرویس‌های توابع را به مدیران امنیتی محدود می‌کند. **نکته کاربردی ۷۳:** این الزام باید فقط در صورتی که مدیر امنیتی توانایی آغاز و پایان خدمات را داشته باشد، انتخاب شود. در این مورد، باید گزینه "آغاز و پایان خدمات" در انتخاب موجود در FAU_GEN.1.1 برگزیده شده باشد. عبارت "خدمات" به عنوان FAU_GEN.1.1 تعریف شده است. (نکته کاربردی مربوط به FAU_GEN.1.1 را ملاحظه فرمایید.)	
۸۳	**مدیریت داده‌های محصول ۱**
توابع امنیتی هدف ارزیابی باید امکان مدیریت کلیدهای رمزنگاری را به سرپرست امنیتی محدود کند. **نکته کاربردی ۷۴:** این الزام مدیریت کلیدهای رمزنگاری را به مدیران امنیتی محدود می‌کند. این الزام تنها در صورتی باید انتخاب شود که کلیدهای رمزنگاری قابل مدیریت (مانند: تغییر، پاک کردن، تولید کردن و وارد کردن) توسط مدیر امنیتی باشند. در آن الزام شناسه "CryptoKeys" برای تفکیک این FMT_MTD.1، از FMT_MTD.1 اجباری تعریف شده در بخش ۶,۶,۲,۱ (FMT_MTD.1/CoreData) اضافه شده است.	

۶-۵ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام
۸۴	**حفاظت از انتقال داخلی داده‌های اساسی محصول**
توابع امنیتی هدف ارزیابی باید از افشای داده‌های محصول محافظت نموده و زمانی که با استفاده از [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] بین بخش‌های جداگانه هدف ارزیابی فرستاده شود، تغییرات را تشخیص دهد. **نکته کاربردی:** این الزام فقط برای اهداف ارزیابی توزیع شده و اطمینان از این‌که تمامی ارتباطات بین مؤلفه‌های هدف ارزیابی توزیع شده از طریق استفاده از کانال ارتباطی رمز شده محافظت می‌شوند، تکرار شده است. داده‌های ارسال شده در این کانال ارتباطی امن توسط پروتکل انتخاب شده رمز می‌شوند. نویسنده هدف امنیتی باید کانال‌ها و پروتکل‌های استفاده شده توسط هر جفت مؤلفه ارتباطی در هدف ارزیابی توزیع شده را، مناسب با تکرار این الزام، مشخص نماید. همچنین این کانال ممکن است به عنوان کانال ثبت برای فرآیند ثبت، همان‌طور که در بخش ۳,۳ و FCO_CPC_EXT.1.2 شرح داده شده است، استفاده شود. اگر TLS انتخاب شود، الزامات داشتن شناسه مرجع پیاده‌سازی شده توسط کاربر (FCS_TLSC_EXT.1.2)، برقرار شده است و شناسه ممکن است توسط فرآیند کشف "Gatekeeper " ایجاد شود. TSS باید فرآیند کشف را شرح داده و نحوه تأمین مؤلفه "joining" برای شناسه مرجع مشخص شود.	
۸۵	**مسیر امن Join/۱**
توابع امنیتی هدف ارزیابی باید یک مسیر ارتباطی بین خود و یکی از مؤلفه‌های متصل که به طور منطقی از سایر مسیرهای ارتباطی متمایز است برقرار نماید و شناسایی مطمئنی از [انتخاب: نقطه پایانی توابع امنیتی هدف ارزیابی، مؤلفه متصل و نقطه پایانی توابع امنیتی هدف ارزیابی] ارائه دهد و از تغییر [انتخاب: و افشای، هیچ] داده‌های تبادل شده محافظت نماید.	
۸۶	**مسیر امن Join/۲**
توابع امنیتی هدف ارزیابی باید به [انتخاب: توابع امنیتی هدف ارزیابی، کاربران محلی مؤلفه متصل، کاربران راه دور] اجازه آغاز ارتباط توسط مسیر امن را بدهد.	
۸۷	**مسیر امن Join/۳**

توابع امنیتی هدف ارزیابی باید برای اتصال مؤلفه‌ها به توابع امنیتی هدف ارزیابی تحت محدودیت‌های محیطی مشخص شده در مرجع راهنمای عملیاتی، از مسیر امن استفاده کند **نکته کاربردی:** این الزام یکی از انواع شناسایی کانال در انتخاب اصلی الزام FCO_CPC_EXT.1.2 را برقرار می‌کند. در FTP_TRP.1.1/Join، "مؤلفه joining"، موجودیت IT است که برای پیوستن به هدف ارزیابی توزیع شده توسط فرآیند ثبت تلاش می‌کند. این الزام نیازمند توانایی مؤلفه‌ها برای برقراری ارتباط امن در طول ایجاد توابع امنیتی هدف ارزیابی توزیع شده (یا زمانی که مؤلفه‌ای به توابع امنیتی هدف ارزیابی توزیع شده موجود اضافه می‌شود) است. در این الزام، زمانی که توابع امنیتی هدف ارزیابی از جفت مؤلفه‌های اولیه ایجاد می‌شوند، ممکن است هرکدام از این مؤلفه‌ها به عنوان توابع امنیتی هدف ارزیابی شناسایی شوند. انتخاب موجود در انتهای FTP_TRP.1.1/Join تشخیص می‌دهد که در برخی موارد ممکن است محرمانگی توسط کانال ارائه نشود (به عنوان مثال، حفاظت از افشای داده‌ها). در این مورد، نویسنده هدف امنیتی باید در TSS، هدف ارزیابی مربوط به محیط برای ارائه محرمانگی را (به عنوان بخشی از محدودیت‌های اشاره شده در FTP_TRP.1.3/Join) مشخص نماید یا تعیین کند که ثبت داده تبادل شده نیازمند محرمانگی نیست (در کدام مورد این ادعا صدق می‌کند). اگر "هیچ" انتخاب شود، ممکن است در سند هدف امنیتی برای بهبود خوانایی این عبارت حذف شود. اختصاص موجود در FTP_TRP.1.3/Join، اطمینان حاصل می‌کند که سند هدف امنیتی هر جزئیات خاص مورد نیاز برای محافظت از محیط ثبت را مشخص کرده است. توجه داشته باشید زمانی که سند هدف امنیتی از FTP_TRP.1/Join برای کانال ثبت استفاده می‌کند، این کانال نمی‌تواند مجدداً به عنوان کانال ارتباطی طبیعی بین مؤلفه‌ای استفاده شود (کانال بعدی باید FTP_ITC.1یاFPT_ITT.1 را رعایت کند). الزامات خاص برای فرآیندهای مقدماتی مربوط به FTP_TRP.1/Join در فعالیت‌های ارزیابی در [SD] تعریف شده‌اند.	
۸۸	حفظ وضعیت امن در زمان شکست ۱/ فضای ذخیره‌سازی ممیزی محلی

توابع امنیتی هدف ارزیابی باید به‌هنگام شکست به‌دلیل «پر شدن حافظه محلی داده‌های ممیزی»، در حالت امن باقی بماند.

نکته کاربردی:
اگر محصول مورد ارزیابی به گونه‌ای پیکربندی شده باشد که در صورت عدم وجود هیچ حافظه دیگری برای ذخیره کردن داده‌های ممیزی، تمام کارکردهای امنیتی را متوقف کند (در حالت کارکرد امن باقی بماند)، این الزام را باید به محصول مورد ارزیابی اضافه کرد. بدین ترتیب، مهاجم نمی‌تواند داده‌های ممیزی دیگری را تولید کند و اقدامات خود را پنهان نماید. انتظار می‌رود که این رفتار در بخش «گزینه‌های دیگر». مربوط به الزام «محل ذخیره‌سازی داده‌های ممیزی ۳» مدل‌سازی شود (در بخش «اختصاص» موجود در «انتخاب»).

۶-۶ کلاس ارتباطات

شماره الزام	نام الزام
۸۹	**تعریف کانال ثبت مؤلفه ۱**
توابع امنیتی هدف ارزیابی باید از مدیر امنیتی درخواست فعال‌سازی ارتباطات بین هر جفت مؤلفه‌های هدف ارزیابی کند، قبل از این‌که چنین ارتباطی قابل انجام باشد.	
۹۰	**تعریف کانال ثبت مؤلفه ۲**
توابع امنیتی هدف ارزیابی باید فرآیند ثبتی که در آن مؤلفه‌ها ایجاد می‌شوند را پیاده‌سازی کند و برای حداقل داده‌های توابع امنیتی هدف ارزیابی از کانال ارتباطی استفاده کند که: [انتخاب: ○ کانالی که الزامات کانال امن را در [انتخاب: FTP_ITC.1، FPT_ITT.1] برآورده می‌کند. ○ کانالی که الزامات کانال ثبت را در FTP_TRP.1/Join برآورده می‌کند. ○ هیچ کانالی]	
۹۱	**تعریف کانال ثبت مؤلفه ۳**
توابع امنیتی هدف ارزیابی باید یک مدیر امنیتی را قادر به غیرفعال سازی ارتباطات بین هر جفت مؤلفه هدف ارزیابی نماید. **نکته کاربردی:** این الزام فقط وقتی هدف ارزیابی توزیع‌شده باشد و دارای مؤلفه‌های متعددی که نیازمند برقراری ارتباط از طریق کانال داخلی توابع امنیتی هدف ارزیابی هستند باشد، مناسب است. زمانی که توابع امنیتی هدف ارزیابی از جفت مؤلفه‌های اولیه ایجاد می‌شوند،	

ممکن است هرکدام از این مؤلفه‌ها به عنوان توابع امنیتی هدف ارزیابی شناسایی شوند.

هدف این الزام اطمینان از وجود فرآیند ثبتی است که قبل از این‌که مؤلفه‌های متصل به توابع امنیتی هدف ارزیابی توزیع‌شده بتوانند با سایر مؤلفه‌های هدف ارزیابی ارتباط برقرار کنند و قبل از اینکه مؤلفه جدید بتواند به عنوان بخشی از توابع امنیتی هدف ارزیابی عمل کند؛ شامل یک مرحله مثبت قابل فعال‌سازی توسط مدیر باشد. ممکن است خود فرآیند ثبت شامل ارتباط با مؤلفه متصل باشد: برخی تجهیزات شبکه از فرآیندی سفارشی برای این مورد استفاده می‌کنند و الزامات امنیتی برای "ارتباطات ثبت" در FCO_CPC_EXT.1.2 تعریف شده‌اند. استفاده از این کانال "ارتباطات ثبت"، متناقض با الزامات FCO_CPC_EXT.1.1 تلقی نمی‌شود. (به عنوان مثال، کانال ثبت می‌تواند قبل از مرحله قابل فعال‌سازی و فقط برای تکمیل فرآیند ثبت، استفاده شود)

انتخاب کانال (برای کانال ثبت) در FCO_CPC_EXT.1.2 اساساً یک انتخاب بین استفاده از کانال امن معمولی که معادل یک کانال استفاده شده برای ارتباط با موجودیت‌های IT خارجی (FTP_ITC.1) است، یا مؤلفه‌های هدف ارزیابی موجود (FPT_ITT.1)، یا نوع مجزای دیگری از کانال که برای ثبت مشخص شده است (FTP_TRP.1/Join)، است. اگر هدف ارزیابی نیازی به کانال ارتباطی برای ثبت نداشته باشد (به عنوان مثال، ثبت توسط مدیر از طریق اقدامات پیکربندی به طور کامل برای هر مؤلفه انجام شده باشد)، انتخاب اصلی در FCO_CPC_EXT.1.2 با گزینه "هیچ کانالی" تکمیل شود.

اگر نویسنده هدف امنیتی نوع کانال FTP_ITC.1/FPT_ITT.1 را در انتخاب اصلی از FCO_CPC_EXT.1.2برگزیده باشد، TSS باید SFR مربوطه‌ای که کانال مورد استفاده را مشخص می‌کند، تعیین کند. اگر نویسنده هدف امنیتی نوع کانال FTP_TRP.1/Join را انتخاب کند، خلاصه مشخصات هدف ارزیابی (که ممکن است در راهنمای عملیاتی باشد)، جزئیات کانال و مکانیسم‌هایی که استفاده می‌کند را شرح می‌دهد (و شرح دهد که فرآیند ثبت چگونه اطمینان می‌یابد که کانال فقط توسط joiner و gatekeeper قابل استفاده است). توجه داشته باشید که نوع کانال FTP_TRP.1/Join ممکن است در محیط عملیاتی، از اقدامات امنیتی درخواست پشتیبانی نماید. (برای جزئیات تعریف FTP_TRP.1/Join را ببینید)

اگر نویسنده هدف امنیتی نوع کانال FTP_ITC.1/FPT_ITT.1 را از انتخاب اصلی FTP_ITC.1/FPT_ITT.1 برگزیده باشد، سند هدف امنیتی باید کانال ثبت را به عنوان تکرار جداگانه‌ای از FTP_ITC.1 یا FPT_ITT.1 تعریف کند و شناسه تکرار را برای FCO_CPC_EXT.1 در نکته کاربردی سند هدف امنیتی ارائه دهد.

توجه داشته باشید که کانال راه‌اندازی و استفاده شده برای ثبت، در صورتی که مطابق با الزامات FTP_ITC.1یا FPT_ITT.1 باشد، ممکن است به عنوان یک کانال ارتباطی داخلی مداوم در نظر گرفته شده باشد؛ به عبارت دیگر کانال ثبت بعد از استفاده بسته می‌شود و کانال جداگانه‌ای برای ارتباطات داخلی استفاده می‌شود.

الزامات خاص برای رویه‌های مقدماتی مربوط به FCO_CPC_EXT.1 در فعالیت‌های ارزیابی در SD تعریف شده است.

۶-۷ کلاس دیواره آتش (FFW)

شماره الزام	نام الزام
۹۲	فیلترینگ حالتمند پروتکل‌های پویا

توابع امنیتی هدف ارزیابی باید به صورت پویا قوانینی را تعریف کرده یا یک نشست مجاز از ترافیک شبکه را برای جریان‌های که از پروتکل‌های شبکه [انتخاب: FTP،SIP،H.323: [اختصاص: دیگر پروتکل‌های پشتیبانی شده]، هیچ پروتکل دیگری] پیروی می‌کنند ایجاد کند.

نکته کاربردی ۷۸:

این الزام پروتکل‌های بسیار پیچیده را مشخص می‌نماید تا فایروال ملزم شود برای آن پروتکل‌ها اجازه جریان یافتن ترافیک شبکه را بدهد، حتی اگر قوانین موجود به طور صریح اجازه جریان یافتن ترافیک شبکه را ندهد. برای مثال، اگر یک کاربر فایل‌ها را منتقل می‌نماید، پروتکل FTP به هر دو اتصال کنترلی و اتصال داده نیاز دارد.

درحالی‌که پورت‌های شناخته شده‌ای وجود دارد: پورت ۲۱(پورت کنترلی بر روی سرور FTP)، پورت ۲۰(پورت داده بر روی سرور در حالت فعال) و پورت‌های تصادفی> ۱۰۲۳ که در سمت کلاینت استفاده می‌گردند.

در حالت غیرفعال، سرور FTP ممکن است از پورت تصادفی>۱۰۲۳ به جای پورت ۲۰ استفاده نماید. اتصال داده توسط کلاینت در حالت غیرفعال راه‌اندازی می‌شود.

برای این نوع از پروتکل‌ها، برقراری اتصال جدید باید مجاز باشد، حتی اگر که مجموعه قوانین[۱]، برقراری اتصال جدید را جلوگیری نمایند (به طور مثال، یک قانون نمی‌تواند پیش‌بینی نماید که چه پورت تصادفی توسط کلاینت یا سرور استفاده می‌گردد و ممکن است به نظر آید که قانون پیش‌فرض، جلوگیری نمودن از اتصال بر روی پورت‌های تصادفی باشد.)

توابع امنیتی هدف ارزیابی، می‌تواند قوانین دینامیکی ایجاد نماید که بر جریان ترافیک حاکم باشد، یا می‌تواند با توجه به انتظاراتی که از پیاده‌سازی پروتکل در RFC مشخص شده است، به صورت ضمنی اجازه برقراری اتصال جدید را بدهد.

قابل ذکر است که این انتظار وجود ندارد که برای هر بسته اطلاعاتی شبکه، اطلاعات بالاتر از لایه چهارم (TCP/UDP) بررسی گردند. این عنصر، نویسنده هدف ارزیابی را ملزم می‌نماید تا شرایطی را مشخص نماید که برای پروتکل‌های مشخصی در داخل فایروال اجازه می‌دهد که ارتباطات مورد انتظار با پورت‌های پیش‌بینی نشده UDP/TCP به صورت صحیح برقرار گردد.

اگر نویسنده هدف امنیتی، پروتکل‌های بیشتری را در برگیرد، نویسنده باید RFC که رفتار پروتکل را مشخص می‌نماید را معرفی نماید؛ همانند FTP در دومین مورد بالا.

---

[۱] Rulset

۷ پیوست دوم: الزامات اختیاری IPS

در این بخش الزامات اختیاری برای ماژول IPS بیان شده است و نویسنده سند هدف امنیتی می‌تواند با توجه به محصول زیرمجموعه‌ای از این الزامات را در سند هدف امنیتی بیان کند.

۷-۱ ممیزی امنیت

شماره الزام	نام الزام
۹۳	**محل ذخیره‌سازی داده‌های ممیزی IPS/۱**
توابع امنیتی هدف ارزیابی باید داده‌های IPS ذخیره شده را از حذف غیرمجاز محافظت نماید.	
۹۴	**محل ذخیره‌سازی داده‌های ممیزی IPS/۲**
توابع امنیتی هدف ارزیابی باید قادر به [جلوگیری] از تغییرات غیرمجاز در داده‌های IPS ذخیره شده، باشد.	
۹۵	**محل ذخیره‌سازی داده‌های ممیزی IPS/۷**
توابع امنیتی هدف ارزیابی در صورت پر شدن دنباله داده IPS، باید [انتخاب: «رویدادهای به هر طریقی تولید شده توسط IPS را نادیده بگیرد»، «جلوگیری از رویدادهای IPS»، «بر روی قدیمی‌ترین داده‌های IPS ذخیره شده دوباره‌نویسی نماید»، [هیچ اقدام دیگری] .]	

۷-۲ الزامات مدیریت امنیت

شماره الزام	نام الزام
۹۶	**مدیریت رفتار توابع امنیتی IPS ۱**
توابع امنیتی هدف ارزیابی باید توانایی تغییر رفتار توابع [جمع‌آوری داده، آنالیز کردن، واکنش] IPS را به [سرپرست مجاز IPS] محدود نماید.	
۹۷	**مدیریت داده‌های محصول IPS ۱**
توابع امنیتی هدف ارزیابی باید توانایی [انتخاب: تغییر پیش‌فرض، پرس‌وجو، ویرایش، حذف، پاک کردن، [اختصاص: عملیات دیگر]] و [اختصاص: لیستی از داده‌های IPS] را به [اختصاص: سرپرست IPS، تحلیل‌گر IPS و دیگر نقش‌های مشخص‌شده در الزام «نقش‌های امنیتی ۳»] محدود کند.	

شماره الزام	نام الزام
نکته کاربردی: هدف امنیتی باید نقش‌هایی که اجازه دسترسی به داده‌های IPS را دارند، مشخص کند (سرپرست IPS، تحلیل‌گر IPS و دیگر نقش‌های مشخص شده در الزام «نقش‌های امنیتی ۳»). هدف امنیتی ممکن است تنها تعدادی از نقش‌های مورد نیاز را معین کند	

۳-۷ الزامات محافظت از هدف ارزیابی

شماره الزام	نام الزام
۹۸	**حفظ وضعیت امن در زمان شکست IPS/۱**
توابع امنیتی هدف ارزیابی باید قادر باشد وضعیت امن را برای واسط‌های درون‌خط وقتی که انواع شکست زیر روی می-دهد حفظ کند: [اختصاص: لیستی از انواع شکست در توابع امنیتی هدف ارزیابی] **نکته کاربردی:** هدف از الزامات کارکرد امنیتی درون بسته تکمیلی IPS این است که به نویسنده هدف امنیتی این اجازه را دهد انواع شکست‌هایی که ممکن است بر روی هدف ارزیابی رخ دهد را تعریف کند که می‌تواند منجر به شکست در شناسایی مؤثر و واکنش نشان دادن به نقص خط‌مشی برای پیمایش ترافیک واسط درون‌خطی شود و همچنین اجازه ندهد که ترافیک از واسط آن‌ها عبور کند. اولین اصلاح " قادر بودن" شامل این است که به سرپرست هدف ارزیابی اجازه دهد که هدف ارزیابی را به‌منظور اجازه دادن به ترافیک برای پیمایش واسط‌های درون‌خطی پیکربندی کند، زمانی که هدف ارزیابی به‌طور جزئی شکست خورد، اما به‌منظور ارائه تضمین اینکه هدف ارزیابی قادر به مسدود کردن ترافیک است اگر برای انجام این کار پیکربندی شده باشد. هدف از الزامات کارکرد امنیتی، همان‌طور که در CC قسمت ۲ گفته شد، این است" اطمینان از اینکه هدف ارزیابی همیشه الزامات کارکرد امنیتی خود را به صورت دسته‌بندی‌های شناسایی‌شده از شکست‌ها درون توابع امنیتی هدف ارزیابی اجرا خواهد کرد". از آنجا که برخی از SFR ها نیاز به بازرسی داده دارند و بازرسی موقعی که واسط شبکه شکست می‌خورد نمی‌تواند رخ دهد، همیشه درست نخواهد بود که "تمام" الزاماً کارکرد امنیتی در صورت شکست مؤلفه‌های خاص اجرا خواهد شد.	
۹۹	**انتقال داده‌های امنیتی در داخل محصول ۱**
توابع امنیتی هدف ارزیابی باید از [افشاء شدن یا تغییر] داده توابع امنیتی هدف ارزیابی خود زمانی که بین [اختصاص:	

شماره الزام	نام الزام
لیستی از بخش‌های مجزای توابع امنیتی هدف ارزیابی] منتقل می‌گردد با استفاده از [انتخاب: با یک یا بیش از یکی از پروتکل‌های:IPSEC،SSH،TLS،HTTPS] محافظت نماید. **نکته کاربردی:** مطابق موارد انتخاب شده در این الزام؛ سند هدف امنیتی باید شامل حداقل یکی از SFR های زیر که در پروفایل حفاظتی مبتنی بر انتخاب تعریف شده‌اند باشد: FCS_IPSEC_EXT.1, FCS_HTTPS_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1 FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, and FCS_TLSS_EXT.2 همچنین سند هدف امنیتی مناسب شامل اهداف اختیاری TRUSTED_COMMUNICATIONS خواهد بود.	

۴-۷ الزامات تخصیص منابع

شماره الزام	نام الزام
۱۰۰	**تخصیص منابع IPS/۱**
توابع امنیتی هدف ارزیابی باید حداکثر سهمیه را برای منابع تخصیص دهد: [منابعی که از نظارت بر روی ترافیک شبکه پشتیبانی کنند] که [موجودیت‌های فعال] می‌توانند همزمان استفاده کنند. **نکته کاربردی:** هدف ارزیابی‌های سازگار با استاندارد، سهمیه‌هایی را بر روی منابع پایان‌پذیر که مورد استفاده برای پشتیبانی از بازرسی ترافیک شبکه است، تحمیل می‌کنند که "subject" (جریان‌های ترافیک شبکه بازرسی‌شده) بتوانند همزمان استفاده شوند. هدف از این الزامات این است که اطمینان حاصل شود هدف ارزیابی در چنین راهی که جریان داده در سرتاسر واسطهای حس‌گر که می‌توانند بیشتر از مقدار ترافیکی که محصول قادر به بازرسی آن است، مستقر نمی‌شوند. اگر جریان (حجم/سرعت) داده که بازرسی می‌شود بیشتر از سهمیه‌بندی تعریف‌شده باشد، هدف ارزیابی باید هشدار را که در اثر تجاوز بیش از سهمیه مجاز است، آغاز کند. برای مثال: زمانی که هدف ارزیابی درون‌خطی مستقر شود، تجاوز از سهمیه ممکن است منجر به حذف (رها شدن) توابع امنیتی هدف ارزیابی (نه ارسال) و شکست به‌منظور ارزیابی ترافیک شبکه شود؛ یا زمانی که هدف ارزیابی درون‌خطی مستقر نشود، تجاوز از سهمیه ممکن است منجر شود ترافیک بدون بازرسی ارسال شود. در هر صورت، تجاوز بیش از حد از سهمیه منجر به" نقض امنیتی" مربوط *FAU_ARP* شود که توابع امنیتی هدف ارزیابی ممکن است در بازرسی برخی ترافیک شبکه شکست بخورد.	

۷-۵ الزامات IPS: جلوگیری از نفوذ

در این بخش الزاماتی با توجه به پیاده‌سازی عملیات نرمال‌سازی بسته‌های شبکه در IPS می‌تواند به سند هدف امنیتی اضافه شود.

شماره الزام	نام الزام
۱۰۱	**نرمال‌سازی ترافیک ۱**
توابع امنیتی هدف ارزیابی باید قادر به بازرسی بر بسته‌های کپسوله شده از طریق [انتخاب: GRE، IP-in-IP، IPv4-in-IPv6، MPLS، PPTP، [اختصاص: دیگر روش‌های کپسوله سازی]، هیچ روش دیگر] باشد.	
۱۰۲	**نرمال‌سازی ترافیک ۲**
توابع امنیتی هدف ارزیابی باید قادر به نرمال‌سازی IP برای بازترکیب بسته‌های تکه‌تکه شده برای نظارت و [انتخاب: • برای داده جمع شده در واسطهای promiscuous: در صورتی که نتوان بازترکیب بسته را انجام داد، یک پیام هشدار تولید شود. • برای داده جمع شده در واسطهای درون‌خط: بسته‌های تکه‌تکه شده را هدایت نکرده و یک هشدار تولید کرده که نمی‌توان بسته موجود را بازترکیب کند.]	
۱۰۳	**نرمال‌سازی ترافیک ۳**
توابع امنیتی هدف ارزیابی باید قادر به نرمال‌سازی TCP برای جریان‌های ترافیک از طریق توابع امنیتی هدف ارزیابی در حالتی که توابع امنیتی هدف ارزیابی در مد درون‌خط مستقر شده داشته باشد و از هدایت [انتخاب: بسته‌های تکراری، بسته‌های تغییر داده شده، بسته‌های خارج از توالی،[انتخاب:[اختصاص: سایر انواع بسته‌ها که باید فرستاده شوند]، هیچ بسته دیگری] جلوگیری کند.	

۵

۸ پیوست سه: الزامات مبتنی بر انتخاب

چنان که در مقدمه این پروفایل حفاظتی نیز گفته شد، الزامات اولیه (الزاماتی که باید توسط محصول مورد ارزیابی یا پلتفرم‌های مربوطه رعایت شوند) در متن این پروفایل حفاظتی گنجانده شده‌اند. بر اساس انتخاب‌هایی که در بخش‌های مختلف این پروفایل حفاظتی انجام می‌شوند، الزامات دیگری نیز مطرح خواهند شد. الزامات زیر به همین منظور ارائه شده‌اند.

همچنین جدول زیر مربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب است. همان‌طور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

جدول ۳. الزامات مبتنی بر انتخاب و رویدادهای قابل ممیزی

ردیف	الزام	رویدادهای ممیزی	لیست سوابق ممیزی اضافی
۱.	FCS_DTLSC_EXT.1	شکست در برقراری یک نشست DTLS	دلیل شکست
۲.	FCS_DTLSC_EXT.2	شکست در برقراری یک نشست DTLS	دلیل شکست
۳.	FCS_DTLSC_EXT.2	تشخیص حملات replay	هویت (به عنوان مثال، آدرس IP منبع) منبع حمله replay
۴.	FCS_DTLSS_EXT.1	شکست در برقراری یک نشست DTLS	دلیل شکست
۵.	FCS_DTLSS_EXT.1	تشخیص حملات replay	هویت (به عنوان مثال، آدرس IP منبع) منبع حمله replay
۶.	FCS_DTLSS_EXT.2	شکست در برقراری یک نشست DTLS	دلیل شکست
۷.	FCS_DTLSS_EXT.2	تشخیص حملات replay	هویت (به عنوان مثال، آدرس IP منبع) منبع حمله replay
۸.	FCS_HTTPS_EXT.1	شکست در برقراری یک نشست HTTPS	دلیل شکست
۹.	FCS_IPSEC_EXT.1	شکست در برقراری یک IPsec SA	دلیل شکست
۱۰.	FCS_NTP_EXT.1	پیکربندی time server جدید حذف time server پیکربندی شده	هویت سرور زمانی جدید/حذف شده
۱۱.	FCS_SSHC_EXT.1	شکست در برقراری یک نشست SSH	دلیل شکست
۱۲.	FCS_SSHS_EXT.1	شکست در برقراری یک نشست SSH	دلیل شکست
۱۳.	FCS_TLSC_EXT.1	شکست در برقراری یک نشست TLS	دلیل شکست
۱۴.	FCS_TLSC_EXT.2	شکست در برقراری یک نشست TLS	دلیل شکست

ردیف	الزام	رویدادهای ممیزی	لیست سوابق ممیزی اضافی
.۱۵	FCS_TLSS_EXT.1	شکست در برقراری یک نشست TLS	دلیل شکست
.۱۶	FCS_TLSS_EXT.2	شکست در برقراری یک نشست TLS	دلیل شکست
.۱۷	FIA_X509_EXT.1/Rev	تلاش ناموفق برای تائید یک گواهینامه	دلیل شکست
.۱۸	FIA_X509_EXT.2	هیچ	هیچ
.۱۹	FIA_X509_EXT.3	هیچ	هیچ
.۲۰	FPT_TST_EXT.2	شکست در خودآزمایی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)
.۲۱	FPT_TUD_EXT.2	شکست در به‌روزرسانی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)
.۲۲	FMT_MOF.1/AutoUpdate	فعال‌سازی یا غیرفعال سازی بررسی خودکار برای به‌روزرسانی‌ها یا به‌روزرسانی‌های خودکار	هیچ
.۲۳	FMT_MOF.1/Functions	تغییر رفتار انتقال داده ممیزی به موجودیت IT خارجی، مدیریت داده ممیزی، عملکرد ممیزی زمانی که فضای ذخیره‌سازی ممیزی محل پر شده باشد.	هیچ

نکته کاربردی ۸۳:

رویدادهای ممیزی FIA_X509_EXT.1/Rev بر اساس هدف ارزیابی است که با اطمینان از موارد زیر، قادر به تکمیل اعتبار گواهینامه نیست:

- وجود افزونه basicConstraints و پرچم CA که برای تمامی گواهینامه‌های CA به حالت «True» تنظیم شده باشد.
- تائید امضای دیجیتالی CA سلسله مراتبی معتبر
- خواندن/دسترسی به CRL یا دسترسی به سرور OCSP (مطابق انتخاب در سند هدف امنیتی)

اگر هرکدام از این موارد رد شوند، باید یک رویداد ممیزی عدم موفقیت، در لاگ ممیزی نوشته شود.

۸-۱ کلاس ممیزی امنیت

۸-۱-۱- تولید داده‌های ممیزی امنیت

شماره الزام	نام الزام	
۱۰۴	تولید داده ممیزی ۱	FAU_GEN_EXT.1.1
توابع امنیت هدف ارزیابی قادر به تولید سوابق حسابرسی برای هر مؤلفه هدف ارزیابی است. سوابق حسابرسی ایجاد شده توسط توابع امنیت هدف ارزیابی از هر مؤلفه محصول مورد ارزیابی شامل زیرمجموعه رویدادهای مربوط به ممیزی امنیت است که می‌توانند روی مؤلفه هدف ارزیابی اتفاق بیفتند.		
۱۰۵	**محل ذخیره‌سازی داده‌های ممیزی حفاظت شده**	FAU_STG_EXT.3.1
توابع امنیتی هدف ارزیابی از هر مؤلفه هدف ارزیابی که داده‌های ممیزی امنیتی را به‌صورت محلی ذخیره می‌کند، وقتی فضای ذخیره محلی داده‌های ممیزی پر باشد، باید اقدامات زیر را انجام دهد: [اختصاص: جدول مؤلفه‌ها و برای هر مؤلفه عملکرد آن مطابق موارد زیر انتخاب شده است: [انتخاب: داده‌های ممیزی جدید را دور بیندازد، سوابق ممیزی قبلی را طبق قانون زیر رونویسی کند: [اختصاص: قانون برای رونویسی سوابق ممیزی قبلی] [اختصاص: سایر اقدامات]]].		
۱۰۶	محل ذخیره‌سازی داده ممیزی ۴	FAU_STG_EXT.4.1
هر مؤلفه هدف ارزیابی که داده‌های ممیزی امنیتی را به صورت محلی ذخیره نمی‌کند، می‌تواند داده‌های ممیزی امنیتی را به‌صورت محلی بافر کند تا زمانی که به یک مؤلفه دیگر هدف ارزیابی که آن را ذخیره یا انتقال می‌دهد، انتقال داده شود. [انتخاب: FPT_ITT.1، FPT_ITC.1].		

۸-۲ الزامات پروتکل DTLS Client

شماره الزام	نام الزام	
۱۰۷	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
توابع امنیتی هدف ارزیابی باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید: [انتخاب: o TLS_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 3268 o TLS_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 3268		

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289

[

نکته کاربردی:

توسط این الزام مجموعه رمزهای مورد آزمایش در تنظیمات ارزیابی محدود می‌شوند. نویسنده سند هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با

نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 6347 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید DTLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این cPP، نسخه DTLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.		
۱۰۸	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2
توابع امنیتی هدف ارزیابی باید تائید کند که [انتخاب: شناسه ارائه شده با شناسه مرجع طبق RFC 6125 بخش ۶، آدرس IPv4 در CN یا SAN، آدرس IPv6 در CN یا SAN، آدرس IPv4 در SAN، آدرس IPv6 در SAN، شناسه در RFC 5280 پیوست A [انتخاب: id-at-commonName، id-at-countryName، id-at-dnQualifier، idat-generationQualifier، id-at-givenName، id-at-initials، id-at-localityName، id-at-name، id-atorganizationalUnitName، id-at-organizationName، id-at-pseudonym، id-at-serialNumber، idat-stateOrProvinceName، id-at-surname، id-at-title] و نه انواع خصوصیات دیگر] مطابقت داشته باشد. **نکته کاربردی:** قوانین تائید هویت در بخش ۶ از RFC 6125 شرح داده شده است. شناسه مرجع از طریق پیکربندی (به عنوان مثال، تنظیم نام یک سرور پست الکترونیکی یا سرور احراز هویت) توسط مدیر (به عنوان مثال، در یک URL در مرورگر وب یا کلیک بر روی یک لینک) یا توسط یک کاربرد وابسته به سرویس کاربردی (به عنوان مثال، یک پارامتر از API) برقرار می‌شود. کلاینت بر اساس دامنه منبع شناسه مرجع مجزا و نوع سرویس کاربردی (مانند HTTP، SIP، LDAP)، تمامی شناسه‌های مرجعی که قابل‌قبول هستند را برقرار می‌کند، مانند یک "نام عمومی" برای فیلد "Subject Name" یک گواهینامه و یک نام DNS (case-insensitive)، نام URL و نام سرویس برای فیلد "Subject Alternative Name ". سپس کلاینت این لیست تمامی شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه شده در گواهینامه سرور DTLS مقایسه می‌کند. روش مورد ترجیح برای تائید این است که Subject Alternative Name از نام DNS، نام URL، یا نام سرویس استفاده کند. برای هدف پس‌سازگاری[۱] تائید با استفاده از نام عمومی مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. در نهایت، کلاینت باید از ایجاد شناسه‌های مرجع با استفاده از wildcards اجتناب نماید. هرچند، اگر شناسه‌های ارائه شده حاوی wildcards باشند، کلاینت باید از بهترین روش منطبق پیروی کند؛ این بهترین شیوه‌ها در فعالیت ارزیابی به دست می‌آیند.		
۱۰۹	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3

[۱] backwards compatibility

توابع امنیتی هدف ارزیابی باید فقط در صورتی که گواهینامه سرور معتبر باشد کانال امن را برقرار سازد. همچنین توابع امنیتی هدف ارزیابی باید [انتخاب: – هیچ مکانیسم لغو سرپرستی پیاده‌سازی نشود. – در صورت شکست توابع امنیتی هدف ارزیابی، به مجوز مدیریت برای ایجاد ارتباط به [انتخاب: مطابقت با شناسه مرجع، تائید مسیر گواهی، تائید تاریخ انقضا، تعیین وضعیت لغو] از گواهی سرور ارائه شده نیاز دارید.		
۱۱۰	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
توابع امنیتی هدف ارزیابی باید در Client Hello، [انتخاب: Supported Elliptic Curves Extension را ارائه ندهد، Supported Elliptic Curves Extension را به همراه NIST curve های[انتخاب: secp256r1، secp384r1، secp521r1، ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192] ارائه دهد و هیچ منحنی دیگری] **نکته کاربردی:** اگر مجموعه رمزهای با منحنی elliptic در FCS_DTLSC_EXT.1.1 انتخاب شده باشد، انتخاب یک یا چند منحنی الزامی است. اگر هیچ مجموعه رمزی با منحنی elliptic در FCS_DTLSC_EXT.1.1 انتخاب نشده باشد، باید گزینه " Supported Elliptic Curves Extension را ارائه ندهد " انتخاب شود. این الزام منحنی‌های elliptic مجاز را برای احراز هویت و پذیرش کلید منحنی‌های NIST ازFCS_COP.1/SigGen و FCS_CKM.1وFCS_CKM.2 محدود می‌کند. این تعمیم برای کلاینت‌هایی که از Elliptic Curve ciphersuites پشتیبانی می‌کنند، است.		

۸-۳ الزامات پروتکل DTLS Client/احراز هویت

۱۱۱	الزامات پروتکل DTLS Client / احراز هویت (۱)	FCS_DTLSC_EXT.2.1
توابع امنیتی هدف ارزیابی باید احراز هویت متقابل را با استفاده از گواهینامه X.509 نسخه ۳، پشتیبانی کند.		
۱۱۲	الزامات پروتکل DTLS Client / احراز هویت (۲)	FCS_DTLSC_EXT.2.2
توابع امنیتی هدف ارزیابی باید در صورت دریافت پیامی حاوی invalid MAC [انتخاب: نشست DTLS را خاتمه دهد، رکورد را بی‌سروصدا دور بیندازد.]		
۱۱۳	الزامات پروتکل DTLS Client / احراز هویت (۳)	FCS_DTLSC_EXT.2.3

توابع امنیتی هدف ارزیابی باید پیام‌هایreplayed را برای موارد زیر شناسایی کرده و بدون پاسخ دور بریزد:

- سوابق DTLS قبلاً دریافت شده
- سوابق DTLS آن‌قدر قدیمی‌باشند که متناسب پنجره لغزان نباشند.

شناسایی کرده و بی‌صدا از بین ببرد.

۸-۴ الزامات **پروتکل** DTLS Server

۱۱۴	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1

توابع امنیتی هدف ارزیابی باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید:

[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289

]

نکته کاربردی:

مجموعه رمزهای آزمایش شده در تنظیمات ارزیابی توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 6347 و RFC 5246 وجود داشته باشد، الزامی است.
به علت اینکه نسخه‌های جدید DTLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند.
در نسخه آینده این cPP، نسخه DTLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.

۱۱۵	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2

توابع امنیتی هدف ارزیابی باید اتصال کلاینت‌هایی که درخواست [لیست نسخه‌های پروتکل] دارند، رد نماید.

نکته کاربردی:

این نسخه از cPP، هدف ارزیابی را الزام به رد نسخه DTLS ۱ نمی‌کند. در نسخه آینده این cPP، تمامی اهداف ارزیابی الزام به رد نسخه DTLS ۱ خواهند بود.

۱۱۶	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3

در صورتی که اعتبار کلاینت DTLS تائید نشود، توابع امنیتی هدف ارزیابی نباید برای اتصال handshake اقدام به تلاش نماید.

نکته کاربردی:

فرآیند تائید کلاینت DTLS، در بخش ۴,۲,۱ از RFC 6347 (DTLS 1.2) و RFC 4347 (DTLS 1.0) شرح داده شده است. هدف ارزیابی کلاینت DTLS را طی برقراری ارتباط (Handshaking) و قبل از اینکه توابع امنیتی هدف ارزیابی پیام Server

Hello ارسال نماید، تائید کند. پس از دریافت ClientHello، سرور DTLS، به همراه کوکی[۱] HelloVerifyRequest ارسال می‌کند. کوکی، پیام امضا شده‌ای است که از توابع درهم‌سازی کلید شده مشخص شده در FCS_COP.1/KeyedHash استفاده می‌کند. سپس کلاینت DTLS یک ClientHello دیگری به پیوست کوکی ارسال می‌کند. اگر سرور DTLS با موفقیت کوکی امضا شده را تائید کند، کلاینت از آدرس IP جعلی استفاده نمی‌کند.		
۱۱۷	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
توابع امنیتی هدف ارزیابی باید برای TLS از [انتخاب: کلید RSA را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت]، پارامترهای Diffie-Hellman با اندازه[انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت] گروه‌های Diffie-Hellman [انتخاب: ffdhe2048 ، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192 ، هیچ گروه دیگری]، منحنی‌های ECDHE [انتخاب: secp256r1 ، secp384r1 ، secp521r1] و هیچ منحنی دیگری] استفاده کند.		
۱۱۸	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
در صورت دریافت پیامی شامل MAC نامعتبر، توابع امنیتی هدف ارزیابی باید [انتخاب: نشست DTLS را خاتمه دهد، سوابق را بدون پاسخ دور بریزد[۲]] . **نکته کاربردی:** Message Authentication Code (MAC) تابع درهم‌ساز کلیدشده مشخص شده در FCS_COP.1/KeyedHash است. MAC، در مرحله DTLS handshake تبادل می‌شود و برای حفظ صحت پیام‌های دریافت شده از فرستنده در طول تبادل داده DTLS استفاده می‌شود. در صورتی که MAC تائید نشود، باید نشست خاتمه یابد یا باید سوابق بدون پاسخ رها شوند.		
۱۱۹	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
توابع امنیتی هدف ارزیابی باید پیام‌های replayed را برای موارد زیر شناسایی کرده و بدون پاسخ دور بریزد: ○ سوابق DTLS قبلاً دریافت شده ○ سوابق DTLS آن‌قدر قدیمی‌باشند که متناسب پنجره لغزان نباشند. **نکته کاربردی:** شناسایی Replay در بخش ۴,۱,۲,۶ از DTLS 1.2 (RFC 6347) و بخش ۴,۱,۲,۵ از DTLS 1.0 (RFC 4347) شرح داده شده است. برای هر سوابق دریافت شده، دریافت‌کننده سوابق حاوی دنباله شماره‌ای که در پنجره دریافت لغزان قرار دارد را تائید می‌کند و دنباله شماره هر سوابق دریافت شده دیگر را در طول نشست تکرار نمی‌کند.		

[۱] cookie
[۲] Silently discard the record

"Silently Discard" به این معنی است که هدف ارزیابی بسته‌ها را بدون پاسخ دور بریزد.		
۱۲۰	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
توابع امنیتی هدف ارزیابی باید از [انتخاب: هیچ از سرگیری جلسه یا بلیت‌های جلسه، از سرگیری نشست بر مبنای session ID بر اساس RFC 4346(TLS1.1) یا RFC5246(TLS1.2)، از سرگیری نشست بر مبنای بلیت‌های نشست با توجه به RFC 5077] پشتیبانی کند.		

۸-۵ الزامات پروتکل DTLS Server / احراز هویت متقابل

۱۲۱	الزامات پروتکل DTLS Server / احراز هویت متقابل (۱)	FCS_DTLSS_EXT.2.1
توابع امنیتی هدف ارزیابی باید احراز هویت متقابل DTLS Client را با استفاده از گواهینامه X.509 نسخه ۳، پشتیبانی کند.		
۱۲۲	الزامات پروتکل DTLS Server / احراز هویت متقابل (۲)	FCS_DTLSS_EXT.2.2
زمانی که کانال مورد اعتماد ایجاد می‌شود، اگر گواهینامه کلاینت معتبر نباشد به صورت پیش‌فرض توابع امنیتی هدف ارزیابی نباید یک کانال مورد اعتماد را ایجاد کند. همچنین توابع امنیتی هدف ارزیابی باید: [انتخاب: – هیچ مکانیسم لغو سرپرستی را اجرا نکند. – در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تائید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
۱۲۳	الزامات پروتکل DTLS Server / احراز هویت متقابل (۳)	FCS_DTLSS_EXT.2.3
درصورتی‌که نام مشخص‌شده[۱] (DN) یا نام مستعار موجودیت فعال[۲] (SAN) در یک گواهینامه با شناسه مورد انتظار برای همتا مطابقت نداشته باشد، محصول نباید کانال امن را برای کلاینت برقرار سازد.		

۸-۶ الزامات پروتکل IPSec

[۱] Distinguished name
[۲] Subject Alternative Name

نقاط پایانی ارتباطات دستگاه‌های شبکه ممکن است با یکدیگر فاصله منطقی یا جغرافیایی داشته باشند، یا ممکن است مسیر ارتباط از تعداد زیادی سیستم غیر قابل‌اعتماد دیگر بگذرد. کارکرد امنیتی دستگاه شبکه باید این قابلیت را داشته باشد که از ترافیک حساس منتقل‌شده حفاظت نماید (مانند ترافیک سرپرست محصول، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست). یکی از راه‌های ایجاد کانال ارتباطی بین دستگاه شبکه و یک موجودیت IT خارجی، به گونه‌ای که این ارتباط را بتوان از هر دو طرف احراز هویت کرد، استفاده از IPsec است.

IPsec جزء مؤلفه‌های ضروری این پروفایل حفاظتی به شمار نمی‌آید. اگر یک محصول مورد ارزیابی از پروتکل IPsec استفاده کند و انتخاب مربوطه را در «کانال امن» و/یا «مسیر امن» انجام دهد. نیاز است الزامات این پروتکل به سند هدف امنیتی اضافه گردد.

IPsec یک پروتکل همتا به همتا است و بنابراین نیازی به تفکیک الزامات کلاینت و سرور وجود ندارد.

شماره الزام	نام الزام	
۱۲۴	**الزامات پروتکل IPSEC (۱)**	FCS_IPSEC_EXT.1.1

در توابع امنیتی هدف ارزیابی باید معماری IPsec را بر اساس آنچه در RFC 4301 مشخص شده است، پیاده‌سازی شود.

نکته کاربردی:

بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه‌داده خط‌مشی امنیتی (SPD) استفاده کرد. با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند:

۱- «PROTECT» از بسته‌ها (مثلاً رمزگذاری آن‌ها)

۲- «BYPASS» از سرویس IPSEC (مثلاً عدم رمزگذاری)

۳- «DISCARD» بسته (مثلاً دور ریختن بسته).

پایگاه‌داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به لیست‌های کنترل دسترسی به مسیریاب، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف‌نظر از روشی که به کار گرفته می‌شود، قوانینی وجود دارند که بسته‌ها باید از آن‌ها پیروی کنند و اقدامات باید بر اساس آن‌ها انجام شوند.

باید ابزارهایی برای تنظیم این قوانین وجود داشته باشند، اما رویکردی عمومی و کلی در این زمینه وجود ندارد. قاعده کلی این است که SPD باید بتواند بسته‌های IP را از یکدیگر تمایز دهد و قوانین مربوطه را در مورد آن‌ها اعمال نماید. ممکن است چند SPD وجود داشته باشند (یک پایگاه داده برای هر واسط شبکه)، اما الزامی در این زمینه وجود ندارد.

شماره الزام	نام الزام	
۱۲۵	**الزامات پروتکل IPSEC (۲)**	FCS_IPSEC_EXT.1.2

توابع امنیتی هدف ارزیابی باید اسمی داشته باشد خط‌مشی پایانی موجود در SPD با هر چیز مطابقت داشته باشد. در غیر این‌صورت غیرمنطبق است و دور انداخته می‌شود.

۱۲۶	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
توابع امنیتی هدف ارزیابی باید [انتخاب: مد انتقال، مد تونل] پیاده‌سازی کند. **نکته کاربردی:** نویسنده هدف امنیتی باید حالت‌های پشتیبانی شده برای عملکرد IPsec را انتخاب نماید.		
۱۲۷	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
توابع امنیتی هدف ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است، پروتکل ESP مربوط به IPSEC را با استفاده از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106)] به همراه الگوریتم درهم‌سازی امن HMAC مبتنی بر SHA، [انتخاب: HMAC-SHA-1، HMAC-SHA-256، HMAC-SHA-384، HMAC-SHA-512، هیچ الگوریتم دیگری] پیاده‌سازی کند. **نکته کاربردی:** زمانی که یک الگوریتم AES-CBC انتخاب شود، باید حداقل یک HMAC مبتنی بر SHA نیز انتخاب شود. اگر فقط یک الگوریتم AES-GCM انتخاب شده باشد، HMAC مبتنی بر SHA تا زمانی که AES-GCM هر دو عملکرد محرمانگی و یکپارچگی را برآورده می‌کند، الزامی نیست. ممکن است Ipsec از یک نسخه کوتاه توابع HMAC مبتنی بر SHA موجود در انتخاب‌ها، استفاده کند. در صورت استفاده از خروجی کوتاه، باید در TSS مشخص شود.		
۱۲۸	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
توابع امنیتی هدف ارزیابی باید یکی از این پروتکل‌ها را پیاده‌سازی کند: [انتخاب: • IKEv1، با استفاده از مد اصلی برای تبادلات[۱] در فاز اول، طبق آنچه در RFC 4109, RFCs 2407,2408,2409، [انتخاب: هیچ RFC دیگر برای اعداد متوالی بسط‌یافته، RFC4304 برای اعداد متوالی بسط‌یافته] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز] • IKEv2، مطابق با آنچه در RFC 5996 تشریح شده است و [انتخاب: بدون پشتیبانی از پیمایش NAT[۲]، با پشتیبانی اجباری از پیمایش NAT چنان که در بخش ۲,۲۳ از RFC 5996 تشریح شده است] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز]]. **نکته کاربردی:** اگر محصول مورد ارزیابی برای دو پروتکل IKEv1 یا IKEv2 از الگوریتم درهم‌ساز SHA-2 استفاده کند، نویسنده سند هدف		

[۱] exchanges
[۲] NAT traversal

امنیتی باید RFC 4868 را انتخاب نماید. اگر هدف ارزیابی از HMAC های کوتاه شده مبتنی بر SHA، همان‌طور که در RFC 4868 شرح داده شده است، استفاده کند، باید در TSS مشخص شود.		
۱۲۹	**الزامات پروتکل IPSEC (۶)**	FCS_IPSEC_EXT.1.6
توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که برای رمزگذاری پی‌آیند[۱] در پروتکل [انتخاب: IKEv1،IKEv2]، از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128، AES-GCM-192، AES-GCM-256] استفاده شده است. الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-192 و AES-CBC-256 در RFC 3602 تشریح شده‌اند. همچنین AES-GCM-128، AES-GCM-192 و AES-GCM-256 درRFC5282 تشریح شده‌اند.) **نکته کاربردی:** AES-GCM-128، AES-GCM-192 و AES-GCM-256 تنها در صورتی انتخاب می‌شوند که IKEv2 نیز انتخاب شده باشد، همچنین هیچ RFC ای وجود ندارد که AES-GCM را برای IKEv1 تعریف کرده باشد.		
۱۳۰	**الزامات پروتکل IPSEC (۷)**	FCS_IPSEC_EXT.1.7
توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که [انتخاب: • سرپرست امنیتی می‌تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب: ○ تعداد بایت‌ها، ○ مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد. [پیکربندی کند. • سرپرست امنیتی می‌تواند طول عمر IKEv2 SA را بر اساس [انتخاب: ○ تعداد بایت‌ها، ○ مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد. [پیکربندی کند. **نکته کاربردی:** نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در FCS_IPSEC_EXT.1.5 صورت گرفته است) را انتخاب می‌کند. نویسنده سند هدف امنیتی همچنین طول عمر را بر اساس مقادیر یا بر اساس زمان (ترکیبی از این دو) انتخاب می‌کند. برای رعایت این الزام، لازم است که مدت زمان توسط سرپرست محصول قابل پیکربندی		

[۱] Payload

باشد (بر اساس دستورالعمل‌هایی که در سند شرح محصول ذکرشده‌اند). محدودیت‌های Hardcoded این الزام را برآورده نمی‌کند. به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۱۳۱	**الزامات پروتکل IPSEC (۸)**	FCS_IPSEC_EXT.1.8

توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که [انتخاب:

- سرپرست امنیتی می‌تواند طول عمر SA فاز دوم IKEv1 را بر اساس [انتخاب:
  - تعداد بایت‌ها،
  - مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.

]

پیکربندی کند.

- سرپرست امنیتی می‌تواند طول عمر IKEv2 Child SA را بر اساس [انتخاب:
  - تعداد بایت‌ها،
  - مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.

]

پیکربندی کند.

نکته کاربردی:

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در FCS_IPSEC_EXT.1.5 صورت گرفته است) را انتخاب می‌کند. نویسنده سند هدف امنیتی همچنین طول عمر را بر اساس مقادیر یا بر اساس زمان (ترکیبی از این دو) انتخاب می‌کند. برای رعایت این الزام، لازم است که مدت زمان توسط سرپرست محصول قابل پیکربندی باشد (بر اساس دستورالعمل‌هایی که در سند شرح محصول ذکرشده‌اند). محدودیت‌های Hardcoded این الزام را برآورده نمی‌کند. به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۱۳۲	**الزامات پروتکل IPSEC (۹)**	FCS_IPSEC_EXT.1.9

توابع امنیتی هدف ارزیابی 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 FCS_RBG_EXT.1 مشخص شده است و دست‌کم طول آن [اختصاص: تعداد بیت‌های (یک یا بیش از یک) باشد که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره‌شده باشد] تولید نماید.

نکته کاربردی:

از آنجایی که در پیاده‌سازی ممکن است گروه‌های مختلف Diffie-Hellman در مذاکره برای استفاده در SA مجاز باشند الزام FCS_IPSEC_EXT.1.9 می‌تواند مقادیر متعددی داشته باشند. نویسند سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید – بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر ارزش منحصربه‌فرد برای پر کردن قسمت اختصاص هر مورد به کار می‌رود. برای مثال، اگر فرض کنیم در پیاده‌سازی گروه DH ۱۴ (2048-bit MODP) و گروه ۲۰ (ECDH با استفاده Curve P-384 در NIST) پشتیبانی می‌شود، با توجه به جدول ۲، تعداد بیت‌های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است.		
۱۳۳	**الزامات پروتکل IPSEC (۱۰)**	FCS_IPSEC_EXT.1.10
توابع امنیتی هدف ارزیابی باید نانس‌های مورداستفاده در تبادلات [انتخاب: IKEv1، IKEv2] با طول [انتخاب: ▪ [اختصاص: قدرت امنیتی مربوط به گروه Diffie-Hellman مذاکره‌شده]؛ ▪ حداقل ۱۲۸ بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی مذاکره‌شده (PRF)] را تولید کند. **نکته کاربردی:** ، اگر IKEv2 نیز انتخاب شده باشد (همان‌طور که در RFC5996 اجباری شده است)، نویسنده سند هدف امنیتی باید دومین گزینه را برای طول نانس انتخاب کند. نویسنده سند هدف امنیتی مجاز است هر یک از گزینه‌ها را برای IKEv1 انتخاب نماید. در اولین گزینه برای طول نانس، از آنجایی که در پیاده‌سازی ممکن است مذاکره کردن برای استفاده از گروه‌های مختلف Diffie-Hellman در ساخت تضمین‌های امنیتی مجاز باشد، اختصاص FCS_IPSEC_EXT.1.10 می‌تواند مقادیر متعددی داشته باشد. نویسنده سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید – بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر ارزش منحصربه‌فرد برای پر کردن قسمت اختصاص هر مورد به کار می‌رود. برای مثال، اگر فرض کنیم در پیاده‌سازی گروه DH ۱۴ (2048-bit MODP) و گروه ۲۰ (ECDH با استفاده Curve P-384 در NIST) پشتیبانی می‌شود، با توجه به جدول ۲، تعداد بیت‌های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است. به این دلیل که نانس‌ها ممکن است پیش از اینکه در مورد گروه DH مذاکره شود، مبادله شوند، توصیه می‌شود نانس به‌کاررفته به اندازه کافی بزرگ باشد که همه پیشنهادهای محصول انتخاب‌شده در تبادل را پشتیبانی نماید.		
۱۳۴	**الزامات پروتکل IPSEC (۱۱)**	FCS_IPSEC_EXT.1.11
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که همه پروتکل‌های IKE، گروه‌های DH [انتخاب: – [انتخاب: ۱۴ (2048-bit MODP)، ۱۵ (3072-bit MODP)، ۱۶ (4096-bit MODP)، ۱۷ (6144-bit MODP)، ۱۸ (8192-bit MODP)] با توجه به RFC 3526		

- [انتخاب: ۱۹ (2048-bit Random ECP)، ۲۰ (384-bit Random ECP)، ۲۱ (521-bit Random ECP)، ۲۴ (2048-bit MODP به همراه 256-bit POS)] با توجه به RFC 5114 را پشتیبانی می‌کنند.		
۱۳۵	**الزامات پروتکل IPSEC (۱۲)**	FCS_IPSEC_EXT.1.12
توابع امنیتی هدف ارزیابی باید به صورت پیش‌فرض بتواند اطمینان حاصل نماید که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۱ IKEv1، IKEv2 IKE_SA] مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۲ IKEv1، IKEv2 CHILD_SA] مذاکره شده است، باشد. **نکته کاربردی:** نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند.		
۱۳۶	**الزامات پروتکل IPSEC (۱۳)**	FCS_IPSEC_EXT.1.13
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که همه پروتکل‌های IKE احراز هویت همتا را با استفاده از [انتخاب: RSA، ECDSA] که از گواهی‌های X.509v3 مطابق با RFC4945 و [انتخاب: کلیدهای پیش‌اشتراکی، هیچ روش دیگری] استفاده می‌کند، انجام می‌دهند. **نکته کاربردی:** حداقل یک روش احرازهویت همتا مبتنی بر کلید عمومی مطابق با این پروفایل حفاظتی مورد نیاز است؛ یک یا چند طرح کلید عمومی توسط نویسنده هدف امنیتی انتخاب می‌شود تا مشخص شود چه چیزی پیاده‌سازی شده است. نویسنده هدف امنیتی همچنین اطمینان حاصل می‌کند که الزامات FCS الگوریتم‌های مورد استفاده به منظور پشتیبانی از آن روش‌ها را لیست کرده است (قابلیت‌های تولید کلید، اگر فراهم شده است). قابل ذکر است TSS شرح خواهد داد کدام یک از این الگوریتم‌ها استفاده شده است (برای مثال، RFC2409 سه روش احرازهویت با استفاده از کلیدهای عمومی؛ هر یک از پشتیبانی شده‌ها در TSS شرح داده خواهد شد).		
۱۳۷	**الزامات پروتکل IPSEC (۱۴)**	FCS_IPSEC_EXT.1.14
توابع امنیتی هدف ارزیابی باید کانال امن را فقط در صورتی که شناسه ارائه شده در گواهینامه دریافت شده با شناسه پیکربندی شده مرجع تطابق داشته و شناسه ارائه شده و مرجع یکی از انواع [انتخاب: SAN: آدرس IP، SAN: نام کامل واجد شرایط دامنه (FQDN)[1]، SAN: کاربر FQDN، CN: آدرس IP، CN: نام کامل واجد شرایط دامنه (FQDN) نام مشخص‌شده[1] (DN)] و [انتخاب: هیچ نوع شناسه مرجع دیگری، [اختصاص: سایر انواع شناسه مرجع پشتیبانی شده]] باشد، برقرار سازد.		

[1] Fully Qualified Domain Name

نکته کاربردی:

زمانی که از گواهینامه‌های RSAیا ECDSA برای احرازهویت همتا استفاده شود، شناسه و گواهینامه‌های ارائه شده به شکل DN، آدرس IP، FQDN یا FQDN کاربر می‌باشند. شناسه مرجع، شناسه‌ای است که هدف ارزیابی انتظار دارد در طول احراز هویت IKE از همتا دریافت شود. شناسه ارائه شده، شناسه‌ای است که در گواهینامه همتا قرار دارد. نویسنده هدف امنیتی باید انواع شناسه ارائه شده و مرجع پشتیبانی شده را انتخاب کند و ممکن است به صورت اختیاری انواع پشتیبانی شده بیشتری را نیز در انتخاب دوم اختصاص دهد. به جز نوع شناسه DN، ممکن است هدف ارزیابی شناسه را در نام عمومی یا Subject Alternative Name (SAN) یا هردو، پشتیبانی کند.

Subject Alternative Nameبا استفاده از نام‌هایDNS، نام‌های URI یا نام‌های Service، روش ترجیحی برای تائید است. تائید با استفاده از نام عمومی برای هدف پس‌سازگاری[۲] مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است.

الگوریتم‌های گواهینامه همتای پشتیبانی شده همانند FCS_IPSEC_EXT.1.13 هستند.

۸-۷ الزامات پروتکل NTP

شماره الزام	نام الزام
۱۳۸	**الزامات پروتکل NTP (۱)**
توابع امنیتی هدف ارزیابی باید تنها از نسخه‌های NTP زیر استفاده کند: [انتخاب: NTP v3 ((RFC 1305)، NTP v4 (RFC 5905)]	
۱۳۹	**الزامات پروتکل NTP (۲)**
توابع امنیتی هدف ارزیابی باید زمان سیستم را با استفاده از [انتخاب: • احراز هویت با استفاده از [انتخاب: SHA1, SHA256, SHA384, SHA512، AES-CBC-128، AES-CBC-256] به عنوان الگوریتم (های) Digest پیام • [انتخاب: IPsec, DTLS] برای فراهم کردن ارتباط امن بین خودش و منبع زمانی NTP] به‌روزرسانی کند.	
۱۴۰	**الزامات پروتکل NTP (۳)**
توابع امنیتی هدف ارزیابی نباید مهر زمانی NTP را از آدرس‌های Broadcast و/یا Multicast به‌روزرسانی کند.	

[۱] Distinguished name

[۲] backwards compatibility

۱۴۱	الزامات پروتکل NTP (۴)
توابع امنیتی هدف ارزیابی باید پیکربندی حداقل سه منابع زمانی NTP را پشتیبانی کند. **نکته کاربردی ۱۰۹:** هدف ارزیابی باید از پیکربندی حداقل ۳ منبع زمانی پشتیبانی کند، اگرچه الزامی نیست هدف ارزیابی پیکربندی شده، همیشه از این حداقل ۳ منبع زمانی استفاده کند.	

۸-۸ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۱۴۲	الزامات پروتکل HTTPS (۱)
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را پیاده‌سازی کنند. **نکته کاربردی:** نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان جزئیات بیشتری را به TSS اضافه کرد.	
۱۴۳	الزامات پروتکل HTTPS (۲)
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS پیاده‌سازی کند.	
۱۴۴	الزامات پروتکل HTTPS (۳)
درصورتی‌که گواهی‌نامه همتا[۱] اراده شده باشد، توابع امنیتی هدف ارزیابی باید [انتخاب: نیاز به احراز هویت کلاینت نداشته باشد، اتصال را برقرار ننماید، برای برقراری اتصال درخواست احراز هویت نماید، هیچ اقدام دیگری انجام ندهد]. **نکته کاربردی:** اگر HTTPS در FTP_TRP.1/Admin یا FTP_ITC.1 انتخاب شده باشد، اعتبار توسط تائید شناسه، مسیر گواهینامه، تاریخ انقضاء و وضعیت لغو طبق RFC 5280، تعیین می‌شود. اعتبار گواهینامه بر اساس آزمون اجراشده برای FIA_X509_EXT.1/Rev ارزیابی می‌شود. اگر HTTPS در FPT_ITT.1 انتخاب شده باشد، اعتبار گواهینامه بر اساس آزمون اجراشده برای FIA_X509_EXT.1/ITT ارزیابی می‌شود.	

[۱] Peer certificate

۸-۹ الزامات پروتکل SSH Client

شماره الزام	نام الزام	
۱۴۵	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251، 4252، 4253، 4254، 5647، 5656، 6187، 6668،8332] پیاده‌سازی نماید. **نکته کاربردی:** نویسنده سند هدف امنیتی انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجراشده‌ای که با عنوان "REQUIRED" مشخص شده‌اند ولی در عناصر بعد از این بخش لیست نشده‌اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند. RFC 5647 only applies to the RFC compliant implementation of GCM; a TOE that only implements the “@openssh.com” variant of GCM should not select 5647. aes*- gcm@openssh.com is specified in Section 1.6 of the OpenSSH Protocol Specification (https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31).		
۱۴۶	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه در RFC4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر کلمه عبور، هیچ روش دیگری].		
۱۴۷	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3

همان‌طور که در RFC4253 توضیح داده‌شده است، توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH کنار گذاشته شوند. **نکته کاربردی:** RFC4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول مناسبی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.		
۱۴۸	**الزامات پروتکل SSH Client (۴)**	FCS_SSHC_EXT.1.4
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی انتقال SSH، از الگوریتم‌های رمزنگاری[انتخاب: aes128-cbc، aes256-cbc، aes128-ctr، aes256-ctr، AEAD_AES_128_GCM، AEAD_AES_256_GCM، aes128-gcm@openssh.com, aes256-gcm@openssh.com]استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند. **نکته کاربردی:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم MAC استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM فقط به عنوان الگوریتم‌های رمزنگاری قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند.		
۱۴۹	**الزامات پروتکل SSH Client (۵)**	FCS_SSHC_EXT.1.5
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که پیاده‌سازی احراز هویت مبتنی بر کلید عمومی SSH، از انتخاب [x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-،ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256 x509v3-، x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521،x509v3-ecdsa-sha2-nistp256 nistp521 rsa2048-sha256] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند. **نکته کاربردی:** اگر x509v3-ecdsa-sha2-nistp256 x509v3-ssh-rsa ، x509v3-ecdsa-sha2-nistp384یا x509v3-rsa2048-sha256 - انتخاب شده باشند، باید لیستی از گواهینامه‌های معتبر مجاز از FCS_SSHC_EXT.1.9انتخاب شوند و SFR های FIA_X509_EXT در پیوست B، کاربردی هستند. It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH.		
۱۵۰	**الزامات پروتکل SSH Client (۶)**	FCS_SSHC_EXT.1.6

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, AEAD_AES_256_GCM، ضمنی] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC رد می‌شوند. **نکته کاربردی ۹۹:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم‌های رمزنگاری استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم MAC قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند. RFC 6668 استفاده از الگوریتم‌های sha2 در SSH را مشخص می‌کند.		
۱۵۱	**الزامات پروتکل SSH Client (۷)**	FCS_SSHC_EXT.1.7
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, ecdh-sha2-nistp256و [انتخاب: diffie-hellman-group14- sha256, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellmangroup18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.		
۱۵۲	**الزامات پروتکل SSH Client (۸)**	FCS_SSHC_EXT.1.8
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در اتصالات SSH کلیدهای یکسان برای آستانه بیشتر از یک ساعت و بیشتر از یک گیگابایت تبادل داده، استفاده نشود. لازم است پس از رسیدن به هر یک از آستانه‌ها، تجدید کلید انجام شود. **نکته کاربردی:** این الزام، دو آستانه تعریف می‌کند. یکی برای حداکثر فاصله زمانی که کلیدهای همان نشست می‌توانند استفاده شوند و دیگری برای حداکثر مقدار داده‌ای که می‌توان با کلیدهای همان نشست انتقال داد. هر دو آستانه باید اجرا شوند و تجدید کلید باید روی هرکدام از آستانه‌ها که زودتر رسید، انجام شود. برای آستانه حداکثر داده منتقل شده، باید مجموع داده‌های ورودی و خروجی محاسبه شود. تجدید کلید بر روی تمامی کلیدها (رمزنگاری، حفظ صحت) برای ترافیک ورودی و خروجی اعمال می‌شود. برای هدف ارزیابی، اجرای آستانه‌های کمتر از حداکثر مقادیر تعریف شده در الزام قابل‌قبول است. برای هر آستانه قابل تنظیم مربوط به این الزام، باید سند راهنما نحوه تنظیم آستانه را مشخص کند. مقادیر مجاز باید هم در سند راهنما مشخص شوند و هم باید کمتر یا برابر آستانه‌های مشخص شده در این الزام باشند، یا هدف ارزیابی نباید مقادیر خارج از آستانه‌های تعریف شده در این الزام را بپذیرد.		
۱۵۳	**الزامات پروتکل SSH Client (۹)**	FCS_SSHC_EXT.1.9

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که کاربر SSH، سرور SSH را با استفاده از یک پایگاه داده محلی احراز هویت می‌کند و نام هر میزبان را با کلید عمومی متناظر آن یا [انتخاب: فهرستی از مراجع صدور گواهی مطمئن، هیچ روش دیگری] همان‌طور که در RFC 4251 بخش ۴,۱ تشریح شده است مطابقت می‌دهد. **نکته کاربردی:** تنها در صورتی می‌توان گزینه «لیست مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521 در FCS_SSHC_EXT.1.5 انتخاب‌شده باشد.

۸-۱۰ الزامات پروتکل SSH Server

شماره الزام	نام الزام	
۱۵۴	**الزامات پروتکل SSH Server (۱)**	FCS_SSHS_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل SSH مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، [انتخاب: ۴۲۵۶، ۴۳۴۴، ۵۶۴۷، ۵۶۵۶، ۶۱۸۷، ۶۶۶۸، ۸۲۶۸،۸۳۰۸ بخش ۳,۱، ۸۳۳۲] پیاده‌سازی نماید. **نکته کاربردی:** نویسنده سند هدف امنیتی انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجراشده‌ای که با عنوان "REQUIRED" مشخص شده‌اند ولی در عناصر بعد از این بخش لیست نشده‌اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند.		
۱۵۵	**الزامات پروتکل SSH Server (۲)**	FCS_SSHS_EXT.1.2
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC4252 توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: مبتنی بر کلید عمومی، مبتنی بر کلمه عبور.		
۱۵۶	**الزامات پروتکل SSH Server (۳)**	FCS_SSHS_EXT.1.3
همان‌طور که در RFC4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک اتصال انتقال SSH کنار گذاشته شوند. **نکته کاربردی:** RFC4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول مناسبی» داشته باشند یا کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی و با در نظر گرفتن بیشترین اندازه بسته که		

قابل‌پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.		
۱۵۷	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [انتخاب: aes128- cbc, aes256-cbc, aes128-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com, aes256-gcm@openssh.com] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.		
نکته کاربردی: RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم MAC استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم‌های رمزنگاری قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند.		
۱۵۸	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که پیاده‌سازی احراز هویت مبتنی بر کلید عمومی SSH، از [انتخاب: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند.		
نکته کاربردی: اگر x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384یا x509v3-ecdsa-sha2-nistp521 انتخاب شده باشند، SFR های FIA_X509_EXT در پیوست B، کاربردی هستند. It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH		
۱۵۹	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256، ضمنی] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.		
نکته کاربردی: RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم‌های رمزنگاری استفاده شده		

باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم MAC قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند. RFC 6668 استفاده از الگوریتم‌های sha2 در SSH را مشخص می‌کند.		
۱۶۰	**الزامات پروتکل SSH Server (۷)**	FCS_SSHS_EXT.1.7
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, ecdh-sha2-nistp256] و [انتخاب: diffie-hellman-group14- sha256, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellmangroup18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521 , هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.		
۱۶۱	**الزامات پروتکل SSH Server (۸)**	FCS_SSHS_EXT.1.8
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که اتصالات SSH کلیدهای یکسان برای آستانه بیشتر از یک ساعت و بیشتر از یک گیگابایت تبادل داده، استفاده نشود. لازم است پس از رسیدن به هر یک از آستانه‌ها، تجدید کلید انجام شود. **نکته کاربردی:** این الزام، دو آستانه تعریف می‌کند. یکی برای حداکثر فاصله زمانی که کلیدهای همان نشست می‌توانند استفاده شوند و دیگری برای حداکثر مقدار داده‌ای که می‌توان با کلیدهای همان نشست انتقال داد. هر دو آستانه باید اجرا شوند و تجدید کلید باید روی هرکدام از آستانه‌ها که زودتر رسید، انجام شود. برای آستانه حداکثر داده منتقل شده، باید مجموع داده‌های ورودی و خروجی محاسبه شود. تجدید کلید بر روی تمامی کلیدها (رمزنگاری، حفظ صحت) برای ترافیک ورودی و خروجی اعمال می‌شود. برای هدف ارزیابی، اجرای آستانه‌های کمتر از حداکثر مقادیر تعریف شده در الزام قابل‌قبول است. برای هر آستانه قابل تنظیم مربوط به این الزام، باید سند راهنما نحوه تنظیم آستانه را مشخص کند. مقادیر مجاز باید هم در سند راهنما مشخص شوند و هم باید کمتر یا برابر آستانه‌های مشخص شده در این الزام باشند، یا هدف ارزیابی نباید مقادیر خارج از آستانه‌های تعریف شده در این الزام را بپذیرد.		

۸-۱۱ الزامات پروتکل TLS Client/ احراز هویت

شماره الزام	نام الزام	
۱۶۲	**الزامات پروتکل TLS Client**	FCS_TLSC_EXT.1.1
توابع امنیتی هدف ارزیابی باید [انتخاب: TLS 1.2 (RFC5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کرده و تمامی نسخه‌های TLS و SSL را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید با پشتیبانی از مجموعه‌های رمز زیر باشد: ○ [انتخاب:		

- [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268]
- TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289

.]]

نکته کاربردی:

مجموعه رمزهای آزمایش شده در تنظیمات ارزیابی توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 5246 وجود داشته باشد، الزامی است.

به علت اینکه نسخه‌های جدید TLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند.

در نسخه آینده این cPP، نسخه TLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.

۱۶۳	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.2

توابع امنیتی هدف ارزیابی باید تائید کند که [انتخاب: شناسه ارائه شده با شناسه مرجع طبق RFC 6125 بخش ۶، آدرس IPv4 در CN یا SAN، آدرس IPv6 در CN یا SAN، آدرس IPv4 در SAN، آدرس IPv6 در SAN، شناسه در RFC 5280 پیوست A [انتخاب: id-at-commonName، id-at-countryName، id-at-dnQualifier، id-at-generationQualifier، id-at-givenName، id-at-initials، id-at-localityName، id-at-name، id-at-organizationalUnitName، id-at-organizationName، id-at-pseudonym، id-at-serialNumber، id-at-stateOrProvinceName، id-at-surname، id-at-title] و نه انواع خصوصیات دیگر] مطابقت داشته باشد.

نکته کاربردی:

قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده‌شده‌اند. شناسه مرجع توسط مدیر (مثلاً واردکردن یک URL در مرورگر وب یا کلیک کردن روی یک لینک)، توسط پیکربندی (مثلاً پیکربندی نام یک سرور ایمیل یا سرور احراز هویت) یا توسط یک برنامه کاربردی (مثلاً یک پارامتر از یک API) بر اساس سرویس برنامه کاربردی، تعیین می‌شود. بر مبنای دامنه منبع از شناسه مرجع منحصربه‌فرد و نوع سرویس برنامه کاربردی (مثلاً HTTP، SIP، LDAP)، client همه شناسه‌های مرجعی که قابل‌قبول هستند را نظیر یک Common Namee برای قسمت Name Subject از گواهینامه و یک نام DNS (حساس به بزرگ و کوچک بودن حروف)، نام URL و نام سرویس برای قسمت Subject Alternative Name.

سپس client لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند.

روش مورد ترجیح برای تائید این است که Subject Alternative Name از نام DNS، نام URL، یا نام سرویس استفاده کند. برای هدف پس‌سازگاری[۱] تائید با استفاده از نام عمومی مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. در نهایت، کلاینت باید

[۱] backwards compatibility

از ایجاد شناسه‌های مرجع با استفاده از wildcards اجتناب نماید. هرچند، اگر شناسه‌های ارائه شده حاوی wildcards باشند، کلاینت باید از بهترین روش منطبق پیروی کند؛ این بهترین شیوه‌ها در فعالیت ارزیابی به دست می‌آیند.		
۱۶۴	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.3
توابع امنیتی هدف ارزیابی باید فقط در صورتی که گواهینامه سرور معتبر باشد کانال امن را برقرار سازد. همچنین توابع امنیتی هدف ارزیابی باید [انتخاب: – هیچ مکانیسم لغو سرپرستی پیاده‌سازی نشود. – در صورت شکست توابع امنیتی هدف ارزیابی، به مجوز مدیریت برای ایجاد ارتباط به [انتخاب: مطابقت با شناسه مرجع، تائید مسیر گواهی، تائید تاریخ انقضا، تعیین وضعیت لغو] از گواهی سرور ارائه شده نیاز دارید.] **نکته کاربردی:** اگر TLS در FTP_ITC یا FTP_TRP.1/Admin انتخاب شده باشد، اعتبار توسط تائید شناسه، مسیر گواهینامه، تاریخ انقضاء و وضعیت لغو مطابق با RFC 5280، تعیین می‌شود. اعتبار گواهینامه بر اساس آزمون اجراشده برای FIA_X509_EXT.1/Rev ارزیابی می‌شود. اگر TLS در FPT_ITT انتخاب شده باشد، اعتبار گواهینامه بر اساس آزمون اجراشده برای FIA_X509_EXT.1/ITT ارزیابی می‌شود.		
۱۶۵	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.4
توابع امنیتی هدف ارزیابی باید در Client Hello، [انتخاب: Supported Elliptic Curves Extension را ارائه ندهد، Supported Elliptic Curves Extension را به همراه NIST curve های[انتخاب: secp256r1، secp384r1، secp521r1، ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192] ارائه دهد و هیچ منحنی دیگری] **نکته کاربردی:** اگر در FCS_TLSC_EXT.1.1 مجموعه‌های رمز بیضوی انتخاب‌شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است. اگر در FCS_TLSC_EXT.1.1 هیچ‌کدام از مجموعه‌های رمز بیضوی انتخاب‌نشده باشند، سپس "عدم نمایش افزونه پشتیبانی منحنی‌های بیضوی" باید انتخاب شود. این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می کنند، الزامی است.		

۸-۱۲ الزامات پروتکلTLS Client همراه با احراز هویت

شماره الزام	نام الزام	
۱۶۶	الزامات پروتکلTLS Client/ احراز هویت ۱	FCS_TLSC_EXT.2.1
توابع امنیتی هدف ارزیابی باید با استفاده از گواهینامه X.509v3، از احراز هویت دوطرفه پشتیبانی نماید.		

۸-۱۳ الزامات پروتکلTLS Server

شماره الزام	نام الزام	
۱۶۷	**الزامات پروتکل TLS Server ۱**	FCS_TLSS_EXT.1.1

توابع امنیتی هدف ارزیابی باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] را پیاده‌سازی نماید و تمامی نسخه‌های TLS و SSL دیگر را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید از مجموعه‌های رمز زیر پشتیبانی نماید:

[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

].

نکته کاربردی:

مجموعه‌های رمز که باید در پیکربندی ارزیابی تست شوند، توسط این الزام محدود شده‌اند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 5246 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید TLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این cPP، نسخه TLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.

۱۶۸	**الزامات پروتکل TLS Server ۲**	FCS_TLSS_EXT.1.2

توابع امنیتی هدف ارزیابی باید اتصال‌های کاربرانی را که درخواست SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، TLS1.2، هیچ‌کدام] دارند، رد نماید.

نکته کاربردی:

تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در FCS_TLSS_EXT.1.1 انتخاب‌نشده است، در اینجا انتخاب شود. در صورتی که گزینه هیچ‌کدام انتخاب شود، عبارت هیچ‌کدام توسط نویسنده سند هدف امنیتی قابل حذف است.

۱۶۹	**الزامات پروتکل TLS Server ۳**	FCS_TLSS_EXT.1.3

توابع امنیتی هدف ارزیابی باید [انتخاب: کلید RSA با اندازه کلید [انتخاب: ۲۰۴۸ بیت و ۳۰۷۲ بیت، ۴۰۹۶ بیت] پیاده‌سازی کند، پارامترهای EC Diffie-Hellman را بر روی منحنی‌های NIST [انتخاب: secp256r1، secp384r1، secp521r1] و هیچ منحنی دیگری تولید کند، پارامترهای Diffie-Hellman را با اندازه [انتخاب: ۳۰۷۲ بیت، ۲۰۴۸ بیت،۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت] همچنین گروه‌های Diffie-Hellman را با [انتخاب: fdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] ایجاد نماید.]

نکته کاربردی:

اگر در بخش FCS_TLSS_EXT.1.1 سند هدف امنیتی مجموعه رمزهای DHE یا ECDHE لیست شده باشند، سند هدف امنیتی باید شامل Diffie-Hellman یا منحنی‌های NIST لیست شده در این الزام باشد. FMT_SMF.1 تنظیمات پارامترهای پذیرش کلید برای برقراری قدرت امنیتی ارتباط TLS، الزامی می‌کند.

۱۷۰	**الزامات پروتکل TLS Server ۴**	FCS_TLSS_EXT.1.4
توابع امنیتی هدف ارزیابی باید از [انتخاب: بدون از سرگیری نشست یا بلیت نشست، از سرگیری نشست بر اساس شناسه‌های نشست با توجه به RFC4346(TLS1.1) یا RFC 5246(TLS1.2)، از سرگیری نشست مبتنی بر بلیت‌های با توجه به RFC 5077]پشتیبانی کنند.		

۸-۱۴ الزامات پروتکل TLS Server همراه با احراز هویت دوطرفه

شماره الزام	نام الزام	
۱۷۱	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱**	FCS_TLSS_EXT.2.1
توابع امنیتی هدف ارزیابی باید در ارتباط TLS با احرازهویت دوطرفه TLS کلاینت‌ها، از گواهینامه‌های X509v3 استفاده کند.		
۱۷۲	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۲**	FCS_TLSS_EXT.2.2
زمانی که کانال مورد اعتماد ایجاد می‌شود، اگر گواهینامه کلاینت معتبر نباشد به صورت پیش‌فرض توابع امنیتی هدف ارزیابی نباید یک کانال مورد اعتماد را ایجاد کند. همچنین توابع امنیتی هدف ارزیابی باید: [انتخاب: – هیچ مکانیسم لغو سرپرستی را اجرا نکند. – در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تائید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
۱۷۳	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳**	FCS_TLSS_EXT.2.3
اگر شناسه مندرج در یک گواهینامه با شناسه مورد انتظار کلاینت مطابقت نداشته باشد، توابع امنیتی هدف ارزیابی نباید یک کانال قابل اعتماد ایجاد کند. اگر شناسه یک FQDN باشد آنگاه توابع امنیتی هدف ارزیابی باید شناسه‌ها را با توجه به RFC 6125 با هم انطباق دهد، در غیر این صورت توابع امنیتی هدف ارزیابی باید شناسه را از گواهینامه parse کرده آن را با شناسه مورد انتظار کلاینت که در شرح خلاصه محصول، توصیف شده است، انطباق دهد.		

۸-۱۵ الزامات پروتکل X509

شماره الزام	نام الزام	
۱۷۴	**اعتبارسنجی گواهینامه X509 (۱)**	FIA_X509_EXT.1.1
توابع امنیتی مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند:		

- تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه با پشتیبانی از حداقل طول مسیر از سه گواهینامه
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.
- توابع امنیتی مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است.
- توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) چنان که در RFC 6960 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در بخش ۵ از RFC 5759 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در بخش ۶,۳ از RFC 5280 تعریف شده است] را تائید کند
- توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند:
  - گواهی‌نامه‌های مورد استفاده برای به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف « Code Signing» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند
  - گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.
  - گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
  - گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.

۱۷۵	**اعتبارسنجی گواهینامه X509 (۲)**	FIA_X509_EXT.1.2

توابع امنیتی مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints ارائه شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.

نکته کاربردی:

الزام FIA_X509_EXT.1.1/Rev قوانین تائید گواهینامه‌ها را لیست کرده است. نویسنده سند هدف امنیتی وضعیت لغوی که با استفاده از OCSPیا CRL ها تائید می‌شود را انتخاب می‌کند. ممکن است پروتکل‌های کانال/مسیر امن استفاده از آن گواهینامه‌ها را الزام کند. این استفاده مستلزم آن است که قوانین extendedKeyUsage تائید شده باشد. اگر هدف ارزیابی عملکردی را که از هر نوع گواهینامه لیست شده در قوانین extendedKeyUsage از FIA_X509_EXT.1.1 استفاده می‌کند، پشتیبانی نکند؛ باید در TSS مشخص شده باشد و بخش مربوط به SFR به طور کلی عملکردهای مورد پذیرش را در نظر می‌گیرد. هرچند، اگر هدف ارزیابی از عملکردهایی پشتیبانی کند که از هرکدام از انواع این گواهینامه‌ها استفاده می‌کند، بای‌د قوان‌ی‌ن متناظر همانند SFR رعایت شوند.

هدف ارزیابی باید قادر به پشتیبانی از حداقل طول مسیر سه گواهینامه باشد. به این معنی که باید از سلسله مراتبی حاوی

حداقل یک گواهینامه اصلی self-signed، گواهینامه CA فرعی و گواهینامه هویت هدف ارزیابی باشد، پشتیبانی کند. انتظار می‌رود اعتبارسنجی در یک گواهینامه CA اصلی امن؛ در ذخیره اصلی مدیریت شده توسط پلتفرم، به پایان برسد. TSS باید زمان اجرای بررسی لغو را شرح دهد. انتظار می‌رود بررسی لغو، زمانی که گواهینامه در یک مرحله احراز هویت استفاده می‌شود و زمان انجام به‌روزرسانی‌های امن (اگر انتخاب شده باشد)، انجام شود. تائید وضعیت گواهینامه X.509 فقط زمانی که در دستگاه بارگذاری می‌شود کافی نیست. تائید وضعیت لغو گواهینامه‌های X.509 در طول شروع به کار خودآزمایی‌ها الزامی نیست. (اگر گزینه استفاده گواهینامه‌های X.509 برای خودآزمایی انتخاب شده باشد) FIA_X509_EXT.1.2/Rev بر روی گواهینامه‌هایی که توسط توابع امنیتی هدف ارزیابی استفاده یا پردازش شده‌اند اعمال می‌شود و گواهینامه‌هایی که ممکن است به عنوان گواهینامه‌های CA امن اضافه شوند را محدود می‌کند. سند هدف امنیتی باید شامل FIA_X509_EXT.2 در همه موارد باشد، به جز زمانی که فقط SSH در FTP_ITC.1 یا FPT_ITT.1 و ssh-rsa، ecdsa-sha2-nistp256 یا ecdsa-sha2-nistp384 انتخاب شده باشد و/یا احراز هویت محدود به ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384و/یا ecdsa-sha2-nistp521 باشد. علاوه بر این، اگر FPT_TUD_EXT یا FPT_TST_EXT برای استفاده از گواهینامه‌های X509 انتخاب شده باشد، باید FIA_X509_EXT.1/Rev در سند هدف امنیتی باشد.		
۱۷۶	**احراز هویت گواهینامه X509 (۱)**	FIA_X509_EXT.2.1
توابع امنیتی مورد ارزیابی باید برای پشتیبانی از احراز هویت در [انتخاب: IPsec، TLS، HTTPS، SSH، DTLS] و همچنین برای [انتخاب: امضای کد برای به‌روزرسانی نرم‌افزار سیستم، امضای کد برای تائید اعتبارسنجی، [اختصاص: سایر کاربردها]، هیچ کاربرد اضافی دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.		
۱۷۷	**احراز هویت گواهینامه X509 (۲)**	FIA_X509_EXT.2.2
اگر توابع امنیتی مورد ارزیابی نتواند اتصال مورد نیاز برای تعیین اعتبار یک گواهی‌نامه را برقرار کند، توابع امنیتی هدف ارزیابی باید [انتخاب: به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند، گواهی‌نامه را بپذیرد، گواهی‌نامه را نپذیرد]. **نکته کاربردی:** انتخاب نویسنده هدف امنیتی در FIA_X509_EXT.2.1 شامل IPsec، TLS، HTTPS است؛ اگر این پروتکل‌ها در FTP_ITC.1.1 یا FPT_ITT.1 باشند. اگر احراز هویتی غیر ازssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384و/یا ecdsasha2-nistp521 در FCS_SSHC_EXT.1.5یا FCS_SSHS_EXT.1.5 انتخاب شده باشد، باید ST حاوی SSH باشد. ممکن است گواهینامه‌ها به صورت اختیاری برای به‌روزرسانی‌های امن نرم‌افزار سیستم (FPT_TUD_EXT.2) و برای تائید صحت (FPT_TST_EXT.2) استفاده شوند.		

معمولاً باید برای بررسی وضعیت لغو یک گواهینامه، دانلود یک CRL یا جستجو با استفاده از OCSP ارتباطی برقرار شود. انتخاب موجود در FIA_X509_EXT.2.2 برای شرح رفتار رویدادی در حالتی است که چنین ارتباطی برقرار نشده باشد (برای مثال، به علت خطای شبکه). اگر هدف ارزیابی، گواهینامه معتبری مطابق تمام قوانین دیگر موجود در FIA_X509_EXT.1 تعیین کرده باشد، رفتار مربوط به انتخاب، اعتبار را تعیین می‌کند. هدف ارزیابی باید گواهینامه را در صورتی که هر قانون اعتبارسنجی دیگری را در FIA_X509_EXT.1 نفی می‌کند، نپذیرد. اگر گزینه‌های تنظیمات مدیر توسط نویسنده هدف امنیتی انتخاب شده باشد، باید عملکردهای متناظر در FMT_SMF.1 را نیز انتخاب کند. انتخاب باید شامل الزامات اعتبارسنجی FCS_IPSEC_EXT.1.14، FCS_TLSC_EXT.1.3 و FCS_TLSC_EXT.2.3 باشد.

اگر هدف ارزیابی توزیع شده باشد و FIA_X509_EXT.1/ITT انتخاب شده باشد، گواهینامه بررسی لغو اختیاری است. این مورد ناشی از اقدامات احراز هویت اضافی برای فعال‌سازی و غیرفعالسازی کانال امن داخلی هدف ارزیابی است؛ همان‌طور که در FCO_CPC_EXT.1 تعریف شده است. در این مورد، ارتباطی برای تائید اعتبار گواهینامه مورد نیاز نیست و این الزام به طور قطعی رعایت می‌شود.

سند هدف امنیتی باید شامل FIA_X509_EXT.2 در همه موارد باشد، به جز زمانی که فقط SSH در FTP_ITC.1 یا FPT_ITT.1 و ssh-rsa، ecdsa-sha2-nistp256 یا ecdsa-sha2-nistp384 انتخاب شده باشد و/ یا احراز هویت ecdsa-sha2-nistp521 نیز انتخاب شده باشد. علاوه بر این، اگر FPT_TUD_EXTیا FPT_TST_EXT گواهینامه‌های X509 را انتخاب کرده باشد، باید FIA_X509_EXT.2 در سند هدف امنیتی باشد.

۱۷۸	**درخواست‌های گواهینامه X509 (۱)**	FIA_X509_EXT.3.1

توابع امنیتی مورد ارزیابی باید مطابق با آنچه در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند این اطلاعات را در درخواست ارائه کند: کلید عمومی[۱] و [انتخاب: اطلاعات مخصوص به دستگاه[۲]، Common Name، Orgsnization، Organization Unit، Country].

نکته کاربردی:

کلید عمومی در واقع بخش کلید عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آنچه در FCS_CKM.1 شرح داده‌شده است، توسط هدف ارزیابی تولید می‌شود.

۱۷۹	**درخواست‌های گواهینامه X509 (۲)**	FIA_X509_EXT.3.2

توابع امنیتی مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.

[۱] Public Key

[۲] Device-specific information

۱۸۰	**الزامات به‌روزرسانی امن ۴**	FPT_TUD_EXT.2.1
توابع امنیتی مورد ارزیابی قبل از نصب هر به‌روزرسانی، اعتبار گواهی امضای کد را بررسی کند.		
۱۸۱	**الزامات به‌روزرسانی امن ۵**	FPT_TUD_EXT.2.2
اگر اطلاعات لغو برای گواهی در زنجیره اعتماد موجود نباشد، گواهینامه معتبری نیست تا به عنوان مهار مطمئن تعیین شده باشد، توابع امنیتی هدف ارزیابی باید [انتخاب: update را نصب نکند، اجازه بدهد که در این موارد سرپرست محصول در مورد پذیرش update تصمیم بگیرد.]		
۱۸۲	**الزامات به‌روزرسانی امن ۶**	FPT_TUD_EXT.2.3
هنگامی‌که گواهینامه به علت انقضای آن، غیر معتبر اعلام‌شده است، توابع امنیتی هدف ارزیابی باید [انتخاب: اجازه بدهد که در این موارد سرپرست محصول در مورد پذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد].		
۱۸۳	**الزامات به‌روزرسانی امن ۷**	FPT_TUD_EXT.2.4
هنگامی‌که گواهینامه به علتی غیر از انقضای آن، غیر معتبر اعلام‌شده است، یا اطلاعات ابطال آن در دست نباشد توابع امنیتی هدف ارزیابی نباید اجازه update دهند.		

۸-۱۶ الزامات به‌روزرسانی امن

۸-۱۷ کلاس مدیریت امنیت

۱۸۴	مدیریت رفتار توابع امنیتی/به‌روزرسانی خودکار ۱	FMT_MOF.1.1/AutoUpdate

توابع امنیتی هدف ارزیابی باید قابلیت [انتخاب: فعال‌سازی، غیرفعال سازی] کارکردهای [انتخاب: جستجو برای به‌روزرسانی خودکار، به‌روزرسانی خودکار] را برای سرپرست امنیتی فراهم آورد.

نکته کاربردی:

این الزام تنها زمانی قابل پیاده‌سازی است که محصول امکان پشتیبانی از بررسی به‌روزرسانی خودکار و به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال سازی این قابلیت را بدهد. فعال‌سازی و غیرفعال سازی قابلیت بررسی به‌روزرسانی خودکار و/یا به‌روزرسانی خودکار به سرپرست امنیتی محدود می‌شود. گزینه "به‌روزرسانی خودکار" فقط زمانی ممکن است انتخاب شود که از امضاهای دیجیتال برای اعتبار به‌روزرسانی امن استفاده شده باشد.

۱۸۵	مدیریت رفتار توابع امنیتی/به‌روزرسانی خودکار ۲	FMT_MOF.1.1/Functions

توابع امنیتی هدف ارزیابی باید توانایی [انتخاب: تعیین رفتار، تغییر رفتار] توابع [انتخاب: انتقال داده‌های ممیزی به موجودیت IT خارجی، مدیریت داده‌های ممیزی، عملکرد ممیزی زمانی که فضای حافظه محلی ممیزی پر شده باشد] را به سرپرست امنیتی محدود کند.

نکته کاربردی:

این الزام تنها در صورتی باید انتخاب شود که یک یا چند مورد از سناریوهای زیر اعمال شده باشد:

- اگر پروتکل انتقال برای انتقال داده‌های ممیزی به یک موجودیت IT خارجی، مطابق آنچه در FAU_STG_EXT.1.1 تعریف شده است قابل تنظیم باشد، گزینه "انتقال داده ممیزی به موجودیت IT خارجی" باید انتخاب شود.
- اگر مدیریت داده‌های ممیزی قابل تنظیم باشد، "مدیریت داده ممیزی" باید انتخاب شود. اصطلاح "مدیریت داده ممیزی" به گزینه‌های مختلف برای انتخاب و اختصاص در الزامات FAU_STG_EXT.1.2، FAU_STG_EXT.1.3 و FAU_STG_EXT.2/LocSpace اشاره می‌کند.
- اگر رفتار عملکرد ممیزی زمان پر شدن فضای ذخیره‌سازی ممیزی محلی قابل تنظیم باشد، گزینه "عملکرد ممیزی زمانی که فضای ذخیره‌سازی ممیزی محلی پر شده باشد" باید انتخاب شود.

انتخاب اول برای "تعیین رفتار" و "تغییر رفتار" باید به صورت مناسب انتخاب شود. ممکن است بر اساس انتخاب دوم، لازم به انتخاب‌های مختلفی برای انتخاب اول باشد (برای مثال، "مدیریت داده ممیزی" ممکن است "تعیین رفتار" و "تغییر رفتار" را برای انتخاب اول الزام کند و از طرف دیگر "توابع امنیتی هدف ارزیابی" ممکن است فقط "تغییر رفتار" را الزام کند). در آن صورت، FMT_MOF.1/Functions باید با افزایش شماره پیوست تکرار شود. (به عنوان مثال، FMT_MOF.1/Functions1، FMT_MOF.1/Functions2، غیره).

۱۸۶	**مدیریت رفتار توابع امنیتی/خدمات ۱**	FMT_MOF.1.1/Services
توابع امنیتی هدف ارزیابی باید قابلیت **شروع و متوقف کردن** ~~توابع~~ **سرویس‌ها** را به سرپرست امنیتی محدود سازد.		
۱۸۷	**مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱**	FMT_MTD.1.1/CryptoKeys
توابع امنیتی هدف ارزیابی باید توانایی مدیریت کلیدهای رمزنگاری را به سرپرست امنیتی محدود کند.		