به نام خدا

پروفایل حفاظتی
دیواره آتش

آبان ماه ۹۹

نسخه ۲,۲

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 دیواره آتش 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 هریک از این کلاس‌ها حوزه‌ی خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای فایروال در این سند مطرح‌شده است، عبارت‌اند از:

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس دیواره آتش (FFW)
- کلاس حفاظت از داده‌های کاربری
- 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

هریک از این کلاس‌ها، از مجموعه‌ای از خانواده‌ها تشکیل و هر خانواده از مجموعه‌ای عنصر و هر عنصر از مجموعه مؤلفه‌ها تشکیل شده 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.

فهرست

۱ شرح محصول دیواره آتش

این بسته توسعه یافته[۱] الزاماتی را برای ارزیابی آن دسته از تجهیزات شبکه تعریف نموده است که ویژگی‌های امنیتی مربوط به دیواره آتش را پیاده‌سازی می‌نمایند. چنین محصولاتی، تجهیزات یا مجموعه‌ای از تجهیزات

[۱] Extended package(EP)

هستند که از حدود و مرزهای کلی حفاظت می‌نمایند، هم‌چون دیواره آتش‌های اختصاصی، روترها و یا حتی سوئیچ‌هایی که برای کنترل جریان اطلاعات بین شبکه‌های متصل شده طراحی شده‌اند.

در برخی موارد تجهیزات شبکه‌ای که ویژگی‌های امنیتی مربوط به دیواره آتش را پیاده‌سازی می‌نمایند، جهت تفکیک دو شبکه مجزا جهت محصور نمودن شبکه امن یا محافظت شده از یک شبکه غیرقابل اطمینان خارجی هم‌چون اینترنت به کار می‌رود که یکی از حالت‌های ممکن برای استفاده از دیواره آتش است. برای دیواره آتش‌ها معمولاً با داشتن اتصالات شبکه فیزیکی و منطقی چندگانه، طیف وسیعی از تنظیمات ممکن و سیاست‌گذاری‌های جریان اطلاعات شبکه را امکان‌پذیر می‌نمایند.

۱,۱ موارد کاربرد محصول

این بسته توسعه یافته، به طور خاص تجهیزات شبکه‌ای که فیلتر نمودن حالتمند ترافیک لایه ۳ و ۴ شبکه را انجام می‌دهند را آدرس‌دهی می‌کند. یک دیواره آتش فیلتر نمودن حالتمند شبکه، ابزاری است که از سخت‌افزار و نرم‌افزاری تشکیل شده است که به دو یا بیش از دو شبکه مجزا متصل شده است و دارای نقش زیرساختی در تشکیلات کلی شبکه است.

فیلترینگ حالتمند ترافیک یعنی این که فایروال وضعیت هر اتصال را بررسی می‌کند و می‌تواند بسته‌هایی که به یک جریان معتبر تعلق ندارند را کنار بگذارد. اطلاعاتی از قبیل شماره سریال TCP، ACKها و فیلد IP Options نیز در جداول وضعیت پویا نگهداری می‌شوند. علاوه بر ویژگی بیان شده سایر ویژگی‌های مانند شماره پورت‌ها و آدرس‌های IP مبدأ و مقصد نیز مورد بررسی قرار می گیرد.

از این رو این بسته توسعه یافته بر روی پروفایل حفاظتی مربوط به تجهیزات شبکه ایجاد شده است، محصولاتی که مطابق این پروفایل حفاظتی هستند متعهد هستند که عملکرد لازم در پروفایل حفاظتی مربوط به تجهیزات شبکه همراه با عملکردهای اضافی که در این بسته توسعه یافته تعریف شده است را پیاده‌سازی نمایند.

به طور خلاصه، محصولاتی که مطابق این پروفایل حفاظتی هستند جریان اطلاعات (به طور مثال، بسته‌ها) بین شبکه های متصل را بر اساس قوانین تنظیم شده با توجه به ترافیک لایه ۳ و ۴ شبکه را کنترل خواهد کرد.

مجموعه الزامات در این بسته توسعه یافته در یک حوزه محدود شده است تا ارزیابی با سرعت بیشتر و هزینه کمتری انجام شود و سطح امنیتی را به کاربر نهایی ارائه دهد.

۲ تعریف مسائل امنیتی

هر محصول دیواره آتش برای ایفای یک نقش در زیرساخت شبکه طراحی شده است. 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، محصول دیواره آتش باید مجموعه‌ای از حداقل کارکرد امنیتی مشترک[۱] که از همه دستگاه‌های شبکه انتظار می‌رود را ارائه نماید. حداقل کارکرد امنیتی مشترک برای مقابله با تهدیدات مشترک پیش روی دستگاه‌های شبکه، مسئله امنیتی است که یک محصول دیواره آتش مطابق با پروفایل حاضر باید به آن بپردازد. این تهدیدات در مقابل تهدیداتی قرار می‌گیرند که یک کارکرد خاص از یک نوع خاص از دستگاه شبکه را هدف قرار می‌دهند. مجموعه حداقل کارکرد امنیتی مشترک باید قابلیت‌های زیر را داشته باشند:

- برقراری ارتباط با دستگاه‌های مجاز و غیر مجاز شبکه
- توانایی انجام به‌روزرسانی‌های معتبر و امن
- توانایی ممیزی فعالیت‌های دستگاه‌ها
- توانایی ذخیره‌سازی و استفاده امن از داده‌ها و اطلاعات محرمانه سرپرست و دستگاه
- توانایی انجام خودآزمایی برای از کار افتادن مؤلفه‌های حیاتی دستگاه.

[۱] Common security functionality

۲,۱ تهدیدات

در ادامه، تهدیدات پیش روی دستگاه‌های شبکه بر اساس عملکرد این دستگاه‌ها دسته‌بندی شده‌اند. همچنین برای هر تهدید، یک توصیف منطقی از چگونگی پوشش دادن آن در الزامات اصلی، اختیاری و الزامات مبتنی بر انتخاب، ارائه شده است.

۲,۱,۱ ارتباط با دستگاه‌های شبکه

یک محصول دیواره آتش با سایر دستگاه‌های شبکه و موجودیت‌های شبکه ارتباط برقرار می‌کند. مقصد این ارتباط ممکن است از لحاظ منطقی یا جغرافیایی یک دستگاه راه‌دور 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 غیر مجازی را با محصول دیواره آتش برقرار کنند یا ارتباطات مجاز را در معرض خطر قرار دهند. کارکرد امنیتی محصول دیواره آتش باید این قابلیت را داشته باشد که از ترافیک حساس شبکه (مانند ترافیک سرپرستی، ترافیک احرازهویت، ترافیک ممیزی و موارد دیگری از این دست) محافظت نماید. ارتباطات برقرارشده با محصول دیواره آتش را می‌توان به دو دسته تقسیم‌بندی کرد: ارتباطات مجاز و ارتباطات غیر مجاز.

ارتباطات مجاز شامل ترافیکی است که بر اساس خط‌مشی محصول دیواره آتش، اجازه جریان یافتن دارد. ارتباطات مجاز ترافیک حساس شبکه را شامل می‌شود که از آن جمله می‌توان به ترافیک سرپرستی محصول دیواره آتش و ارتباطات آن با یک سرور ممیزی یا احرازهویت اشاره کرد. حفاظت از این ارتباطات نیازمند استفاده از یک کانال امن است. کارکرد امنیتی محصول دیواره آتش 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 غیر مجاز به شمار می‌آیند.

تهدید اصلی علیه ارتباطات محصول دیواره آتش که در این پروفایل حفاظتی به آن پرداخته می‌شود، یک موجودیت غیر مجاز 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 غیر استاندارد و اطلاعات محرمانه سرپرستی ضعیفی به کار گرفته شده باشند، یک عامل تهدید می‌تواند به صورت غیر مجاز 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 غیر استاندارد نه تنها قابلیت هم‌کنش‌پذیری[۱] دستگاه را محدود می‌کند، بلکه ضمانت و اعتماد حاصل از استانداردسازی را نیز از دستگاه می‌گیرد.

۲,۱,۱,۱ دسترسی سرپرستی غیر مجاز

ممکن است عامل تهدید تلاش کند تا با استفاده از ابزارهای بدخواهانه، به محصول دیواره آتش دسترسی سرپرستی پیدا کند. به عنوان مثال، عامل تهدید خود را به عنوان سرپرست به دستگاه معرفی می‌کند، به عنوان دستگاه به سرپرست معرفی می‌نماید، نشست سرپرستی را بازپخش می‌کند (به طور کامل یا بخش‌هایی خاص از آن)، یا حملات مردی در میان را ترتیب می‌دهد تا به نشست‌های سرپرستی 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.

منطق الزام کارکرد امنیتی (SFR):

- نقش سرپرست در الزام FMT_SMR.2 تعریف شده است و توانایی‌های سرپرستی مربوطه نیز در الزامات FMT_SMF.1 و FMT_MTD.1/CoreData تعریف شده‌اند و همچنین توانایی‌های اضافه اختیاری نیز در الزامات FMT_MOF.1/Services و FMT_MOF.1/Functions تعریف شده است.
- اقداماتی که قبل از احرازهویت کردن سرپرست اجازه انجام گرفتن دارند در الزام FIA_UIA_EXT.1 در نظر گرفته شده است و شامل نمایش یک پیغام هشدار موافقت یا توجه می‌باشد که در الزام FTA_TAB.1 مشخص می‌گردد.
- الزام برای فرآیند احرازهویت سرپرست در FIA_UAU_EXT.2 توصیف شده است.
- قفل نشست‌های سرپرست بوسیله FTA_SSL_EXT.1 (برای نشست‌های محلی)، FTA_SSL_EXT.3 (برای نشست‌های راه‌دور) و FTA_SSL_EXT.4 (برای تمامی نشست‌های تعاملی) تضمین می‌شود.
- کانال امن برای ارتباطات سرپرست راه‌دور از طریق FTP_TRP.1/Admin انجام می‌گیرد.
- (اقدامات بدخواهانه که توسط نشست سرپرست انجام شده است به صورت جداگانه در «فعالیت ردیابی نشده» ارائه شده است.)
- (حفاظت از اطلاعات محرمانه سرپرست به صورت جداگانه در "هک شدن گذرواژه " ارائه شده است.)

[۱] Interoperability

۲,۱,۱,۲ رمزنگاری ضعیف

ممکن است عامل تهدید از ضعیف بودن الگوریتم رمزنگاری بهره‌برداری کند یا حملات از پای درآوردن رمزنگاری[۱] را علیه فضای کلید ترتیب دهد. انتخاب نادرست الگوریتم رمزنگاری، مُدها یا اندازه کلیدها به مهاجمان اجازه می‌دهد تا به الگوریتم رمزنگاری حمله کنند یا با حملات جستجوی فراگیر[۲] علیه فضای کلید، دسترسی غیرمجاز بدست آورند و با کمترین تلاش موفق به خواندن، دستکاری یا کنترل ترافیک شوند.

منطق الزام کارکرد امنیتی:

- الزامات تولید و نابودی کلید در FCS_CKM.1 و FCS_CKM.2 ارائه می‌شوند.
- الزامات برای استفاده از طرح‌های رمزنگاری در FCS_COP.1/DataEncryption، FCS_COP.1/SigGen، FCS_COP.1/Hash و FCS_COP.1/KeyedHash تعریف می‌شوند.
- الزامات تولید بیت تصادفی برای پشتیبانی از تولید کلید و پروتکل‌های امن در FCS_RBG_EXT.1 تعریف می‌شوند.
- مدیریت توابع رمزنگاری در FMT_SMF.1 مشخص می‌شود.

۲,۱,۱,۳ کانال‌های ارتباطی غیر قابل 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 پروتکل‌هایی 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 محصول دیواره آتش را به خطر اندازند.

منطق الزام کارکرد امنیتی:

- استفاده عمومی پروتکل‌های امن برای کانال‌های ارتباطی تعریف شده، به صورت سطح بالا در الزامات FTP_ITC.1 و FTP_TRP.1/Admin مشخص شده است؛ برای محصولات توزیع شده، الزامات ارتباطات بین مؤلفه‌ای در FPT_ITT.1 آورده شده است.
- الزامات پروتکل‌های ارتباط امن برای تمامی پروتکل‌های مجاز در FCS_DTLSC_EXT.1، FCS_DTLSC_EXT.2، FCS_DTLSS_EXT.1، FCS_DTLSS_EXT.2، FCS_HTTPS_EXT.1،

---

[۱] Cryptographic exhaust

[۲] Brute force

FCS_IPSEC_EXT.1، FCS_SSHC_EXT.1، FCS_SSHS_EXT.1، FCS_TLSC_EXT.1، FCS_TLSC_EXT.2، FCS_TLSS_EXT.1، FCS_TLSS_EXT.2 تعریف می‌شوند.

- الزامات اختیاری و مبتنی بر انتخاب برای استفاده از گواهی‌نامه‌های کلید عمومی جهت پشتیبانی از پروتکل‌های امن، در FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 تعریف شده‌اند.

۲,۱,۱,۴ *نقاط پایانی با احرازهویت ضعیف*

ممکن است عامل تهدید به پروتکل‌های امنی حمله کند که برای احرازهویت 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 سرپرست 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 محصول دیواره آتش را در معرض خطر قرار دهد.

منطق الزام کارکرد امنیتی:

- استفاده از پروتکل‌های امن مناسب برای احرازهویت کردن نقاط‌پایانی، بوسیله‌ی الزامات FTP_ITC.1 و FTP_TRP.1/Admin تضمین شده است؛ برای محصولات توزیع شده، الزامات احرازهویت برای نقاط‌پایانی در ارتباطات بین مؤلفه‌ای، در FPT_ITT.1 آورده شده است.
- موارد خاص اضافه احتمالی احرازهویت امن در طول ثبت‌نام مؤلفه‌های محصول توزیع‌شده، در FCO_CPC_EXT.1 و FTP_TRP.1/Join بیان شده است.

۲,۱,۲ به‌روزرسانی‌های معتبر

برای حصول اطمینان از صحت کارکرد امنیتی محصول دیواره آتش، لازم است که نرم‌افزار و ثابت‌افزار آن به‌روزرسانی شوند. منبع و محتوای به‌روزرسانی‌ها را باید با استفاده از روش‌های رمزنگاری تأیید کرد؛ در غیر این صورت، یک منبع غیر معتبر می‌تواند به‌روزرسانی خود را به کار گیرد و کارکرد امنیتی محصول دیواره آتش را دور بزند. روش‌های تایید منبع و محتوای به‌روزرسانی نرم‌افزار یا ثابت‌افزار بوسیله ابزارهای رمزنگاری معمولا جاییکه هش‌های به‌روزرسانی‌ها به صورت دیجیتال امضاء شده باشند، طرح‌های امضاء دیجیتال را بکار می‌گیرند.

نسخه‌های به‌روزنشده نرم‌افزارها یا ثابت‌افزارها می‌توانند محصول دیواره آتش را در معرض خطر عوامل تهدیدی قرار دهند که در پی سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده آن‌ها هستند. به‌روزرسانی‌های تأییدنشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تأیید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روزشده

را در معرض خطر عوامل تهدیدی قرار می‌دهند که به دنبال بهره‌گیری از نرم‌افزار یا ثابت‌افزار برای رسیدن به مقاصد خویش هستند.

۲,۱,۲,۱ *به‌روزرسانی‌های مخرب*

ممکن است عامل تهدید یک به‌روزرسانی معیوب و دستکاری‌شده‌ای را برای نرم‌افزار یا ثابت‌افزار محصول دیواره آتش ارائه کند و کارکرد امنیتی دستگاه را در معرض خطر قرار دهد. به‌روزرسانی‌های تأییدنشده یا به‌روزرسانی‌هایی که با استفاده از رمزنگاری ضعیف یا غیر امن تأیید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روزشده را در معرض خطر دستکاری غیر مجاز قرار می‌دهد.

منطق الزام کارکرد امنیتی:

- الزامات برای حفاظت از به‌روزرسانی‌ها در FPT_TUD_EXT.1 ارائه شده است.
- استفاده اختیاری از حفاظت مبتنی بر گواهی‌نامه برای امضاها می‌تواند در FPT_TUD_EXT.2 مشخص گردد، الزامات فرآیند گواهی X509 در FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 مشخص شده است.
- الزامات برای مدیریت به‌روزرسانی‌ها در FMT_SMF.1، برای به‌روزرسانی دستی در FMT_MOF.1/ManualUpdate و الزامات اختیاری برای به‌روزرسانی خودکار در FMT_MOF.1/AutoUpdate مشخص می‌گردد.

۲,۱,۳ فعالیت ممیزی‌شده

سرپرستان می‌توانند با ممیزی فعالیت‌های محصول دیواره آتش، وضعیت دستگاه را به خوبی پایش نمایند. این فرایند امکان بررسی، گزارش‌دهی در خصوص کارکردهای امنیتی، بازسازی رویدادها و تحلیل مشکل امنیتی را برای سرپرست 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 سرپرست 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 غیر مجاز، 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، محصول دیواره آتش باید داده‌های ممیزی را تولید کند و قابلیت ارسال آن‌ها به یک موجودیت شبکه مورد اعتماد (مثال؛ سرور syslog) را داشته باشد.

۲,۱,۳,۱ *فعالیت ردیابی‌نشده*

ممکن است عامل تهدید تلاش کند تا بدون اطلاع سرپرست، به کارکرد امنیتی محصول دیواره آتش دسترسی پیدا کند، آن را تغییر دهد و/یا دستکاری نماید. بدین ترتیب، ممکن است مهاجم راهی برای حمله به محصول دیواره آتش پیدا کند (مثال؛ از طریق پیکربندی‌های نامناسب، ایراد در محصول) و سرپرست نیز آگاه نشود که دستگاه در معرض خطر قرار گرفته است.

منطق الزام کارکرد امنیتی:

- الزامات توانایی‌های ممیزی پایه در FAU_GEN.1 و FAU_GEN.2 مشخص شده است و مهرهای زمانی در FPT_STM_EXT.1 ارائه شده است.
- الزامات حفاظت از رکوردهای ممیزی ذخیره‌شده روی محصول، در FAU_STG.1 تعریف شده است.
- الزامات برای مخابره امن رکوردهای ممیزی محلی به موجودیت IT خارجی از طریق کانال امن، در FAU_STG_EXT.1 تعریف شده است.
- الزامات اضافه اختیاری که با ازدست دادن داده‌های ممیزی محلی ذخیره شده سروکار دارد، در FAU_STG_EXT.2/LocSpace و FAU_STG_EXT.3/LocSpace مشخص شده است.
- اگر پیکربندی قابلیت عملکردی ممیزی (اختیاری) توسط محصول فراهم شود، الزامات آن در FMT_SMF.1 مشخص می‌گردد و محدود کردن این قابلیت به سرپرست‌های امنیتی در FMT_MOF.1/Functions مشخص شده است.

۲,۱,۴ داده‌ها و اطلاعات محرمانه دستگاه و سرپرست

محصول دیواره آتش 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 احرازهویت و پیکربندی نرم‌افزار و ثابت‌افزار و اطلاعات محرمانه سرپرستی اشاره کرد. کلیدهای سرپرست و دستگاه، اطلاعات کلید و اطلاعات محرمانه احرازهویت را باید در برابر دستکاری و افشای غیر مجاز محافظت نمود. علاوه بر این، کارکرد امنیتی دستگاه باید تغییر اطلاعات محرمانه پیش‌فرض احرازهویت را (مانند؛ کلمه‌های عبور سرپرست) ملزم نماید.

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 محصول دیواره آتش 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 غیر مجاز امکان می‌دهند تا با استفاده از

اطلاعات محرمانه سرپرست امنیتی، به کارکردهای سرپرستی 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 غیر مجاز مهاجم به داده‌های دستگاه و سرپرست ادامه خواهد یافت.

۲,۱,۴,۱ به خطر افتادن کارکرد امنیتی

ممکن است عامل تهدید داده‌های دستگاه و اطلاعات محرمانه را به خطر اندازد و بدین ترتیب، دسترسی غیر مجاز و مستمری به محصول دیواره آتش 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 سرپرست و استفاده از آن‌ها توسط مهاجم.

منطق الزام کارکرد امنیتی:

- حفاظت از کلیدهای سری/خصوصی در مقابل مصالحه/تراضی شدن در FPT_SKP_EXT.1 مشخص شده است.
- نابودی امن کلیدها در FCS_CKM.4 مشخص شده است.
- اگر مدیریت کلیدها (اختیاری) توسط محصول فراهم شود، الزامات آن در FMT_SMF.1 مشخص می‌گردد و محدود کردن این قابلیت به سرپرست‌های امنیتی در FMT_MTD.1/CryptoKeys مشخص شده است.
- (حفاظت از گذرواژه‌ها به صورت جداگانه در "هک شدن گذرواژه " مشخص شده است.)

۲,۱,۴,۲ هک شدن گذرواژه

ممکن است عامل تهدید از ضعیف بودن گذرواژه‌های سرپرستی 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.

منطق الزام کارکرد امنیتی:

- الزامات طول‌های گذرواژه و کارکترهای موجود در آن، در FIA_PMG_EXT.1 مشخص شده است.
- حفاظت از ورود گذرواژه از طریق بازخورد مبهم در FIA_UAU.7 مشخص شده است.
- اقدامات بدست آوردن تعداد حدآستانه شکست‌های متوالی گذرواژه در FIA_AFL.1 مشخص شده است.
- الزامات ذخیره‌سازی امن گذرواژه‌ها در FPT_APW_EXT.1 مشخص شده است.

۲,۱,۵ از کار افتادن کارکردهای امنیتی دستگاه

سازوکارهای محصول دیواره آتش 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. محصول دیواره آتش برای حصول اطمینان از صحت کارکرد امنیتی خود می‌تواند خودآزمایی‌هایی را در هنگام راه‌اندازی اولیه و همچنین در حین عملیات انجام دهد.

۲,۱,۵,۱ از کار افتادن کارکرد امنیتی

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

منطق الزام کارکرد امنیتی:

- الزامات برای اجرای خودآزمایی (ها) در FPT_TST_EXT.1 مشخص شده است.
- استفاده اختیاری از گواهی‌نامه‌های برای خودآزمایی (ها) در FPT_TST_EXT.2 مشخص شده است. (همچنین پشتیبانی از گواهی‌نامه‌های FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 نیز وجود دارد.)

۲,۲ فرضیات

در این بخش به فروض مربوط به شناسایی تهدیدات و الزامات امنیتی دستگاه‌های شبکه می‌پردازیم. انتظار نمی‌رود که محصول دیواره آتش در هیچ یک 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 محصول دیواره آتش 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

[۱] Roots of trust

ندارد که از دسترسی فیزیکی به دستگاه (که به موجودیت‌های غیر مجاز 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.

۲,۲,۲ کارکرد محدود

چنین فرض می‌شود که دستگاه کارکردهای شبکه را به عنوان کارکرد اصلی خود ارائه می‌کند و سرویس‌ها 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 محصول دیواره آتش عمومی یا استاندارد، هیچ ضمانتی در خصوص حفاظت از داده‌هایی که از آن می‌گذرند ارائه نمی‌کند. محصول دیواره آتش باید از داده‌هایی حفاظت کند که از آن نشأت گرفته یا به آن ارسال شده‌اند. این داده‌ها، داده‌های ممیزی و سرپرستی را در بر می‌گیرند. ترافیکی که صرفاً از محصول دیواره آتش 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 سرپرست مورد اعتماد

چنین فرض می‌شود که سرپرستان امنیتی محصول دیواره آتش 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 سرپرستان امنیتی از اطلاعات محرمانه حساب کاربری و گذرواژه‌هایی با قدرت امنیتی و انتروپی مناسب استفاده می‌کنند و در هنگام سرپرستی دستگاه، اهداف بدخواهانه‌ای در سر ندارند. از محصول دیواره آتش انتظار نمی‌رود که در صورت انجام اقدامات بدخواهاه توسط سرپرست 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، سرپرست نرم‌افزار و ثابت‌افزار محصول دیواره آتش را به صورت منظم به‌روزرسانی می‌کند.

۲,۲,۶ امنیت اطلاعات محرمانه سرپرست

اطلاعات محرمانه سرپرست (کلید خصوصی) که برای دسترسی به محصول دیواره آتش استفاده می‌شوند، توسط پلت‌فرمی که روی آن قرار دارند محافظت می‌گردند.

۲,۲,۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده)

برای اهداف ارزیابی توزیع‌شده فرض می‌شود که دسترس‌پذیری همه‌ی مؤلفه‌های هدف ارزیابی، در راستای کاهش احتمال یک حمله پیش‌بینی نشده (یا یک شکست) روی یک یا چند مؤلفه‌ی هدف ارزیابی، به صورت مناسب بررسی شده است. همچنین فرض می‌شود در راستای دسترس‌پذیری، عملکرد ممیزی در حال اجرا بر روی مؤلفه‌ها، برای تمامی آن‌ها به درستی بررسی شده است.

۲,۲,۸ اطلاعات باقیمانده

سرپرست باید اطمینان یابد که برای اطلاعات باقیمانده حساس (مانند: کلیدهای رمزنگاری، اجزای سازنده کلید، PINs، رمزعبورها و غیره.) روی محصول دیواره آتش، وقتی که تجهیز از محیط عملیاتی حذف یا برداشته می‌شود، امکان دسترسی غیرمجاز وجود ندارد.

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.

منطق الزام کارکرد امنیتی:

- نمایش یک پیغام هشدار موافقت یا توجه الزامی می‌باشد و در الزام FTA_TAB.1 مشخص شده است.

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 با ارزش 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 سرویس‌ها 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 سرپرست مورد اعتماد

سرپرستان 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 سرپرست

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

۳,۱,۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده)

برای اهداف ارزیابی توزیع‌شده سرپرست امنیتی باید اطمینان یابد که دسترس‌پذیری هر مؤلفه‌ی هدف ارزیابی، در راستای کاهش احتمال یک حمله پیش‌بینی نشده (یا یک شکست) روی یک یا چند مؤلفه‌ی هدف ارزیابی، به صورت مناسب بررسی شده است. همچنین سرپرست امنیتی باید اطمینان یابد که عملکرد ممیزی در حال اجرا بر روی مؤلفه‌ها به درستی بررسی شده است.

۳,۱,۸ اطلاعات باقیمانده

سرپرست امنیتی باید اطمینان یابد که برای اطلاعات باقیمانده حساس (مانند: کلیدهای رمزنگاری، اجزای سازنده کلید، PINs، رمزعبورها و غیره.) روی محصول دیواره آتش، وقتی که تجهیز از محیط عملیاتی حذف یا برداشته می‌شود، امکان دسترسی غیرمجاز وجود ندارد.

۴ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول ۴-۱ هستند و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول ۴-۱ 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 مورداشاره 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 ۴-۱ الزامات کارکرد امنیتی

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

شماره الزام	نام الزام	عنصر متناظر با الزام
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۸	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۹	مدیریت 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
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	فیلترینگ حالتمند ۱	FFW_RUL_EXT.1.1
۱۷	فیلترینگ حالتمند ۲	FFW_RUL_EXT.1.2
۱۸	فیلترینگ حالتمند ۳	FFW_RUL_EXT.1.3
۱۹	فیلترینگ حالتمند ۴	FFW_RUL_EXT.1.4
۲۰	فیلترینگ حالتمند ۵	FFW_RUL_EXT.1.5
۲۱	فیلترینگ حالتمند ۶	FFW_RUL_EXT.1.6
۲۲	فیلترینگ حالتمند ۷	FFW_RUL_EXT.1.7
۲۳	فیلترینگ حالتمند ۸	FFW_RUL_EXT.1.8
۲۴	فیلترینگ حالتمند ۹	FFW_RUL_EXT.1.9
۲۵	فیلترینگ حالتمند ۱۰	FFW_RUL_EXT.1.10
۲۶	مدیریت احرازهویت ناموفق ۱	FIA_AFL.1.1
۲۷	مدیریت احرازهویت ناموفق ۲	FIA_AFL.1.2
۲۸	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۲۹	شناسایی و احرازهویت کاربر ۱	FIA_UIA_EXT.1.1
۳۰	شناسایی و احرازهویت کاربر ۲	FIA_UIA_EXT.1.2
۳۱	سازوکار احرازهویت بر اساس رمز عبور ۲	FIA_UAU_EXT.2.1
۳۲	احرازهویت کاربر ۱۰	FIA_UAU.7.1
۳۳	کارکرد مدیریتی محصول ۱/ فایروال	FMT_SMF.1.1/FFW

شماره الزام	نام الزام	عنصر متناظر با الزام
۳۴	مدیریت داده‌های محصول ۱	FMT_MTD.1.1/CoreData
۳۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۳۶	نقش‌های امنیتی ۳	FMT_SMR.2.1
۳۷	نقش‌های امنیتی ۴	FMT_SMR.2.2
۳۸	نقش‌های امنیتی ۵	FMT_SMR.2.3
۳۹	محافظت از داده‌های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1
۴۰	حفاظت از گذرواژه سرپرست محصول ۱	FPT_APW_EXT.1.1
۴۱	حفاظت از گذرواژه سرپرست محصول ۲	FPT_APW_EXT.1.2
۴۲	خودآزمایی محصول ۱	FPT_TST_EXT.1.1
۴۳	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۴۴	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۴۵	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۴۶	مهرهای زمانی ۱	FPT_STM_EXT.1.1
۴۷	مهرهای زمانی ۲	FPT_STM_EXT.1.2
۴۸	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۴۹	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۵۰	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۵۱	پیغام‌های هشدار در رابطه با استفاده محصول۱	FTA_TAB.1.1
۵۲	کانال امن ۱	FTP_ITC.1.1
۵۳	کانال امن ۲	FTP_ITC.1.2
۵۴	کانال امن ۳	FTP_ITC.1.3
۵۵	مسیر امن ۱	FTP_TRP.1.1/Admin
۵۶	مسیر امن ۲	FTP_TRP.1.2/Admin
۵۷	مسیر امن ۳	FTP_TRP.1.3/Admin
الزامات مربوط به پیوست یک		
۵۸	ذخیره‌سازی داده‌های ممیزی محافظت شده ۱	FAU_STG.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۵۹	ذخیره سازی داده‌های ممیزی محافظت شده ۲	FAU_STG.1.2
۶۰	محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی	FAU_STG_EXT.2.1/LocSpace
۶۱	ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی	FAU_STG.3.1/LocSpace
۶۲	الزامات پروتکل X509(۱)/ تبادل داده کاربردی داخل محصول	FIA_X509_EXT.1.1/ITT
۶۳	الزامات پروتکل X509 (۲)/ تبادل داده کاربردی داخل محصول	FIA_X509_EXT.1.2/ITT
۶۴	حفاظت از انتقال داخلی داده‌های اساسی محصول	FPT_ITT.1.1
۶۵	مسیر امن ۱/ پیوند زدن	FPT_TRP.1.1/Join
۶۶	مسیر امن ۲ / پیوند زدن	FPT_TRP.1.2/Join
۶۷	مسیر امن ۳ / پیوند زدن	FPT_TRP.1.3/Join
۶۸	تعریف کانال ثبت‌نام مؤلفه ۱	FCO_CPC_EXT.1.1
۶۹	تعریف کانال ثبت‌نام مؤلفه ۲	FCO_CPC_EXT.1.2
۷۰	تعریف کانال ثبت‌نام مؤلفه ۳	FCO_CPC_EXT.1.3
۷۱	فیلترینگ حالتمند پروتکل‌های پویا	FFW_RUL_EXT.2.1
۷۲	تولید داده ممیزی ۱	FAU_GEN_EXT.1.1
۷۳	محل ذخیره‌سازی داده‌های ممیزی حفاظت شده	FAU_STG_EXT.3.1
۷۴	محل ذخیره سازی داده ممیزی ۴	FAU_STG_EXT.4.1
الزامات مربوط به پیوست دو		
۷۵	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
۷۶	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2
۷۷	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3
۷۸	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4

شماره الزام	نام الزام	عنصر متناظر با الزام
۷۹	الزامات پروتکل DTLS Client/ احرازهویت ۱	FCS_DTLSC_EXT.2.1
۸۰	الزامات پروتکل DTLS Client/ احرازهویت ۲	FCS_DTLSC_EXT.2.2
۸۱	الزامات پروتکل DTLS Client/ احرازهویت ۳	FCS_DTLSC_EXT.2.3
۸۲	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1
۸۳	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2
۸۴	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
۸۵	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
۸۶	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
۸۷	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
۸۸	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
۸۹	الزامات پروتکل DTLS Server/ احرازهویت دوطرفه ۱	FCS_DTLSS_EXT.2.1
۹۰	الزامات پروتکل DTLS Server/ احرازهویت دوطرفه ۲	FCS_DTLSS_EXT.2.2
۹۱	الزامات پروتکل DTLS Server/ احرازهویت دوطرفه ۳	FCS_DTLSS_EXT.2.3
۹۲	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۹۳	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۹۴	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۹۵	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۹۶	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۹۷	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۹۸	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۹۹	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۱۰۰	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۱۰۱	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۱۰۲	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۰۳	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۱۰۴	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۱۰۵	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۱۰۶	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۱۰۷	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۱۰۸	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۱۰۹	الزامات پروتکل NTP (۱)	FCS_NTP_EXT.1.1
۱۱۰	الزامات پروتکل NTP (۲)	FCS_NTP_EXT.1.2
۱۱۱	الزامات پروتکل NTP (۳)	FCS_NTP_EXT.1.3
۱۱۲	الزامات پروتکل NTP (۴)	FCS_NTP_EXT.1.4
۱۱۳	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۱۱۴	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۱۱۵	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۱۱۶	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۱۱۷	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۱۱۸	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۱۱۹	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۱۲۰	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۱۲۱	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۱۲۲	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۱۲۳	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۱۲۴	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3
۱۲۵	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۱۲۶	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۱۲۷	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۱۲۸	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۱۲۹	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۳۰	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۱۳۱	الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۱۳۲	الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۱۳۳	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۱۳۴	الزامات پروتکلTLS Client/ احرازهویت ۱	FCS_TLSC_EXT.2.1
۱۳۵	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.1.1
۱۳۶	الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.1.2
۱۳۷	الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.1.3
۱۳۸	الزامات پروتکل TLS Server (۴)	FCS_TLSS_EXT.1.4
۱۳۹	الزامات پروتکلTLS Server/ احرازهویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۴۰	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۲	FCS_TLSS_EXT.2.2
۱۴۱	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۳	FCS_TLSS_EXT.2.3
۱۴۲	الزامات پروتکل X509(۱) / ابطال	FIA_X509_EXT.1.1/Rev
۱۴۳	الزامات پروتکل X509(۱) / ابطال	FIA_X509_EXT.1.2/Rev
۱۴۴	الزامات پروتکل X509(۳)	FIA_X509_EXT.2.1
۱۴۵	الزامات پروتکل X509(۴)	FIA_X509_EXT.2.2
۱۴۶	الزامات پروتکل X509(۵)	FIA_X509_EXT.3.1
۱۴۷	الزامات پروتکل X509(۶)	FIA_X509_EXT.3.2
۱۴۸	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۴۹	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۵۰	الزامات به‌روزرسانی امن ۶	FPT_TUD_EXT.2.3
۱۵۱	الزامات به‌روزرسانی امن ۷	FPT_TUD_EXT.2.4
۱۵۲	مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار	FMT_MOF.1.1/AutoUpdate

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۵۳	**مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع**	FMT_MOF.1.1/Functions
۱۵۴	**مدیریت رفتار توابع امنیتی/خدمات ۱**	FMT_MOF.1.1/Services
۱۵۵	**مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱**	FMT_MTD.1.1/CryptoKeys

۴,۱ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات عمدی و غیرعمدی موجود درزمینه 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 احرازهویت 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 سرپرستان مسئول بازبینی این اطلاعات را دچار سردرگمی کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت مورداعتماد 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. هرچند 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**

محصول مورد ارزیابی باید بتواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند:

الف) آغاز و اتمام توابع ممیزی؛

ب) تمامی رویدادهای قابل ممیزی برای سطوح ممیزی.

پ) تمام اقدامات مدیریتی شامل موارد زیر:

- ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)
- تغییرات در داده‌های توابع امنیتی هدف ارزیابی مرتبط با تغییرات پیکربندی (علاوه بر اطلاعات حاکی از ایجاد تغییرات، باید تعیین شود که چه مواردی تغییر کرده‌اند)
- تولید/واردکردن، تغییر، یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز باید ثبت شود)
- تغییر گذرواژه (نام حساب کاربری مربوطه نیز باید ثبت شود)
- [انتخاب: [آغاز و توقف سرویس‌ها، هیچ اقدام دیگر، اختصاص:[لیست سایر کاربردهای ویژه]]]

د) تعداد رویدادهای مشابه که در واحد زمان مشخص روی داده است

ه) تعداد اقدامات متقابل که در واحد زمان مشخص روی داده است.

ت) [انتخاب: دیگر رویدادهای ممیزی لیست 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، مبدا تلاش (به طور مثال IP address)
FIA_UAU_EXT.2	همه مواردی که از ساز و کارهای احراز هویت استفاده می‌کنند.	مبدا 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	هر گونه تلاش برای شروع یک بروزرسانی 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 بروزرسانی؛ نتیجه تلاش بروزرسانی (موفقیت یا شکست)	هیچ اطلاعات اضافه دیگری
FPT_STM.1	تغییرات زمانی	مقادیر جدید و قدیم برای زمان مبدا 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	راه اندازی 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	راه اندازی یک کانال امن پایان کانال امن شکست در عملکرد مسیر امن	شناسایی، شناسه کاربری ادعا شده
FDP-RIP.2	هیچ	هیچ
FF_RUL_EXT.1	قوانین پیکربندی شده با عملیات "ثبت لاگ "	• آدرس مبدا و مقصد • پورت مبدا و مقصد • پروتکل لایه انتقال • اینترفیس های محصول
FMT_SMF.1/FFW	تمام اقدامات مدیریتی داده های محصول (شامل ایجاد، اصلاح و حذف قوانین فایروال)	هیچ

۲	**تولید داده ممیزی ۲**

محصول مورد 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 مولفه‌های کارکردی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در ستون سوم از جدول الزام FAU_GEN.1.1 مشخص‌شده است.

۳	**تولید داده ممیزی ۳**

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

نکته کاربردی:

مؤلفه‌ای که رویداد ممیزی را ثبت می‌نماید، وقتی که یک رویداد قابل ممیزی توسط مؤلفه‌ی دیگری برقرار می‌گردد، باید رویداد را با هویت مؤلفه‌ی که برقرار کننده آن رویداد است، مرتبط سازد.

[۱] Subject

۴	محل ذخیره‌سازی داده‌های ممیزی ۱

محصول باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال امن مطابق با الزام FTP_ITC.1 باشد.

تذکر: در صورتی که هر یک از پروتکل‌های HTTPS،TLS،DTLS،SSH،IPsec 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.

نکته کاربردی:

محصول مورد ارزیابی برای انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به‌جز سرور محصول مورد ارزیابی استفاده می‌کند. ذخیره‌سازی این سوابق ممیزی و اجازه دادن به سرپرست محصول جهت بازبینی این سوابق، توسط محیط عملیاتی صورت می‌گیرد. از آنجاییکه سرور ممیزی خارجی قسمتی از محصول مورد ارزیابی نمی‌باشد، به جزء توانایی‌های انتقال داده‌های ممیزی، الزاماتی برای آن تعریف نمی‌شود. همچنین برای قالب و پروتکل زیرساختی داده‌های ممیزی که باید انتقال یابند، الزاماتی تعیین نمی‌شود. محصول باید توانایی پیکربندی انتقال داده ممیزی به سرور خارجی را بدون مداخله سرپرست داشته باشد. انتقال دستی، نمی‌تواند الزامات را برآورده نماید. ارسال باید به صورت بلادرنگ یا دوره‌ای انجام گیرد. اگر ارسال به صورت بلادرنگ انجام نشود، خلاصه مشخصات محصول چگونگی صورت گرفتن ارسال و بازه ی تکرار که محصول برای ارسال پشتیبانی می‌کند را توصیف می‌نماید. خلاصه مشخصات محصول همچنین بازه‌ی تکرار قابل قبول را پیشنهاد می‌نماید.

برای محصولات توزیع‌شده، هر مؤلفه باید قادر باشد که داده‌های ممیزی را از طریق یک کانال خارجی حفاظت شده، به صورت مناسبی خارج نماید. حداقل یک مؤلفه باید توانایی خارج کردن رکوردهای ممیزی به سرور IT خارجی را داشته باشد.

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 داده های ممیزی را بصورت محلی ذخیره می کند.
- هدف ارزیابی باید یک هدف ارزیابی توزیع شده باشد که داده های ممیزی را روی اجزاء هدف ارزیابی زیر ذخیره می کند:

[اختصاص: شناسایی اجزاء هدف ارزیابی

• هدف ارزیابی یک هدف ارزیابی توزیع شده با ذخیره داده های ممیزی است که به صورت خارجی برای اجزای هدف ارزیابی زیر ارائه شده است. [اختصاص: لیستی از مؤلفه های هدف ارزیابی که داده های ممیزی را بصورت محلی ذخیره نمی کنند و سایر اجزای هدف ارزیابی که داده های ممیزی تولید شده خود را به آنها منتقل می کنند].
۶ **محل ذخیره‌سازی داده‌های ممیزی ۳**
درصورتی‌که حافظه محلی محصول پرشده باشد و ظرفیتی برای ذخیره‌سازی داده‌های ممیزی نداشته 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 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. برای هر محصولات توزیع‌شده، نیاز نمی‌باشد که هر مؤلفه داده‌های ممیزی را به صورت محلی ذخیره نماید ولی به طور کلی محصول باید توانایی ذخیره‌ی محلی داده‌های ممیزی را داشته باشد. هر مؤلفه حداقل باید توانایی ذخیره موقت اطلاعات ممیزی برای مواردی که ارتباط شبکه دچار مشکل می‌شود را داشته باشد. ذخیره موقت نیاز نیس که بر روی حافظه ثابت صورت گیرد، این ذخیره محلی می‌تواند روی حافظه فرار انجام گیرد. برای هر مؤلفه که اطاعات را به صورت محلی ذخیره می‌نماید یا اطلاعات ممیزی را به صورت موقت ذخیره می‌کند، باید مشخص شود هنگام پر شده حافظه، په اقدامی صورت گیرد.

۴,۲ 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[۳]، نابودی کلید و انواع مختلف عملیات رمزنگاری برای رمزگذاری و رمزگشایی AES، تأیید امضا، تولید درهم‌ساز و تولید درهم‌ساز کلید گذاری شده[۴] هستند. این الزامات کارکرد امنیتی، از پیاده‌سازی الزامات مبتنی بر انتخاب و پروتکل لیست شده در پیوست دو پشتیبانی می‌کنند.

---

۱ Overwrite
۲ External log server
۳ Key establishment
۴ Keyed hash generation

شماره الزام	نام الزام
۷	**مدیریت کلید رمزنگاری ۱**

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

نکته کاربردی:

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

اگر محصول مورد ارزیابی به‌عنوان یک دریافت‌کننده در الگوهای استقرار کلید عمل کند و برای پشتیبانی از احرازهویت مشترک پیکربندی نشده باشد، محصول نیاز به پیاده‌سازی تولید کلید ندارد.

در محصول مورد ارزیابی توزیع‌شده، اگر مؤلفه محصول به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند، محصول نیاز به پیاده‌سازی تولید کلید ندارد.

شماره الزام	نام الزام
۸	**مدیریت کلید رمزنگاری ۲**

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: انتشار ویژه NIST 800-56B بازبینی ۱، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛

[۱] Key establishment

[۲] Integer factorization cryptography

شماره الزام	نام الزام
	• الگوهای استقرار کلید منحنی بیضوی[۱] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۲]؛ • الگوهای استقرار کلید میدانی[۳] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته». • الگوی استقرار کلید با استفاده از دیفی-هلمن گروه ۱۴ که این الزامات را رعایت کنند: RFC 3526، بخش۳؛ **نکته کاربردی:** این عنصر درواقع نسخه اصلاح‌شده الزام «مدیریت کلید رمزنگاری۲»[۴] در استاندارد ISO 15408 می‌باشد که به‌جای توزیع کلید، به استقرار کلید می‌پردازد. نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورداستفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. برای دیفی-هلمن گروه ۱۴، نویسنده هدف امنیتی باید به جای انتخاب استقرار کلید میدانی، از الزام کارکردی امنیتی یک انتخاب مناسب انجام دهد. الگوهای استقرار کلید مبتنی بر RSA در بخش ۹، بازبینی ۱، مربوط به NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های بازبینی ۱ مربوط به SP 800-56B است. توجه: اگر محصول مورد ارزیابی در الگوی استقرار کلید به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، الگوی تولید کلید RSA را اجرا نماید. منحنی‌های بیضوی مورداستفاده در الگوهای استقرار کلید، با منحنی‌های مشخص‌شده در الزام «مدیریت کلید رمزنگاری ۱» ارتباط دارند. پارامترهای دامنه مورداستفاده در الگوهای استقرار کلید میدانی، به الگوهای تولید کلید مورداشاره در «مدیریت کلید رمزنگاری ۱» وابسته هستند.
۹	**مدیریت کلید رمزنگاری ۴**
محصول مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: [اختصاص:	

[۱] Elliptic curve-based
[۲] Discrete logarithm cryptography
[۳] Finite filed-based
[۴] FCS_CKM.2

شماره الزام	نام الزام

- برای کلیدهای متن-آشکار در ذخیره‌ساز فرار[۱]، نابودی باید از طریق یک [انتخاب: بازنویسی ساده شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]]، نابودی مرجع کلید که مستقیماً با درخواست زباله‌روبی همراه باشد] انجام شود.
- برای کلیدهای متن-آشکار در ذخیره‌ساز غیرفرار، نابودی باید از طریق فراخوان[۲] یک واسط مهیا شده توسط محصول مورد ارزیابی که [انتخاب:
  - بصورت منطقی مکان ذخیره‌سازی کلید را آدرس می‌دهد و یک بازنویسی [انتخاب: ساده، [اختصاص: تعداد عبورها]-عبور] شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]] را انجام می‌دهد.
  - یک بخشی از توابع امنیتی محصول را برای نابودی انتزاع معرف کلید، می‌سازد]

انجام شود.]

نکته کاربردی:

در قسمت مربوط به انتخاب در گزینه دوم از اولین اختصاص، جاییکه کلیدها برای نابودی بوسیله "یک بخشی از توابع امنیتی محصول " شناسایی می‌شوند، خلاصه مشخصات محصول باید "بخش " مربوطه و واسط مرتبط با آن را تعریف نماید. واسط اشاره شده در الزام می‌تواند در محصولات مختلف، شکل متفاوتی داشته باشد. شاید مشهودترین شکل آن یک برنامه کاربردی روی یک سیستم عامل باشد.

وقتی که روش‌های تخریب مختلفی برای کلیدهای مختلف و/یا موقعیت‌های تخریب مختلف استفاده می‌شود، این روش‌ها و کلیدها/موقعیت‌های متفاوت بکار گرفته شده، در خلاصه مشخصات محصول توصیف می‌شوند. خلاصه مشخصات محصول همه کلیدهای مرتبط استفاده شده در پیاده‌سازی الزامات کارکرد امنیتی را توصیف می‌نماید، همچنین مواردی که محل ذخیره شدن کلیدها بصورت متن آشکار است را شامل می‌شود.

در بعضی از اختصاص‌های بالا، از " شامل هیچ CSP نباشد " استفاده شده است. این جمله به این معنی می‌باشد که محصول از برخی داده خاص استفاده می‌کند که شامل هیچ کدام از مقادیر تولید شده توسط تولیدکننده بیت تصادفی موجود در الزام FCS_RBG_EXT یا مقادیر مشخص لیست شده در این الزام، مثلا موارد لیست شده در اولین انتخاب از اولین اختصاص این الزام نمی‌باشد. در واقع وجود عبارت " شامل هیچ CSP نباشد " برای مطمئن شدن از این موضوع است که حتما بازنویسی داده با دقت انتخاب شده است.

---

[۱] Volatile Storage

[۲] Invocation

شماره الزام	نام الزام
لازم به ذکر است که کلیدهای رمزنگاری در این الزام، شامل کلیدهای نشست نیز می‌شود. همچنین تخریب کلید برای مؤلفه عمومی در جفت کلید نامتقارن، اعمال نمی‌شود.	
۱۰	**عملیات رمزنگاری ۱ (۱)**
محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص [اختصاص: الگوریتم AES که در حالت [انتخاب: CBC، GCM، CTR] و در اندازه‌های کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] استفاده می‌شوند] و با توجه به [اختصاص: استاندارد AES که در ISO 18033-3 تعریف‌شده است، [انتخاب: CBC که در ISO 10116 تعریف‌شده است، GCM که در ISO 19772 تعریف‌شده است، CTR که در ISO 10116 تعریف شده است]] انجام دهد. **نکته کاربردی:** در مورد نخستین انتخاب این الزام، نویسنده هدف امنیتی حالت یا حالت‌های کارکردی AES را انتخاب می‌کند. در مورد دومین انتخاب، نویسنده هدف امنیتی اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب می‌کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[۱] در الزامات کانال امن هستند.	
۱۱	**عملیات رمزنگاری ۱ (۲)**
محصول مورد ارزیابی باید سرویس‌ها امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوریتم امضای دیجیتال RSA و کلید رمزنگاری با اندازه‌های (ماژول‌ها) [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر] • الگوریتم امضای دیجیتال بیضوی و کلید رمزنگاری با اندازه‌های [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 [انتخاب: P-256، P-384، P-521]؛ ISO/IEC 14888-3، بخش ۶,۴] **نکته کاربردی:**	

[۱] Cipher suite

شماره الزام	نام الزام
نویسنده هدف امنیتی الگوریتم(های) مورد استفاده برای اجرای امضای دیجیتال را انتخای می‌کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی انتخاب‌ها و اختصاص‌های مناسب را انجام می‌دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین می نماید. نویسنده هدف امنیتی، با استفاده از انتخاب‌ها و اختصاص‌های این الزام، از شامل شدن تمامی مقادیر پارامترهای ضروری برای مجموعه رمز انتخاب شده بوسیله الزامات سند هدف امنیتی، اطمینان پیدا می‌نماید. نویسنده هدف امنیتی همچنین سازگار بودن انتخاب‌های انجام گرفته شده با دیگر الزامات رمزنگاری را بررسی می‌کند، خصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی شود.	
۱۲	**عملیات رمزنگاری ۱ (۳)**
محصول مورد ارزیابی باید سرویس‌ها درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1، SHA-256، SHA-384، SHA-512] و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی که [اختصاص: ISO/IEC 10118-3:2004] را رعایت کند، ارائه نماید. **نکته کاربردی:** به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، استفاده کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از SHA-1 را بر اساس SP 800-131A فراهم می‌کند. توجه: طبق SP 800-131 A الگوریتم SHA-1 فقط می‌تواند برای عملیات‌های غیر از امضای دیجیتال همچون درهم سازی پسورد و ... استفاده شود. در نسخه‌های آتی این پروفایل حفاظتی، SHA-256 کمینه الزام برای محصولات خواهد بود. انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای الزام «عملیات رمزنگاری ۱(۱)» و الزام «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی).	
۱۳	**عملیات رمزنگاری ۱ (۴)**
محصول مورد ارزیابی باید احرازهویت پیام مبتنی بر کلید درهم‌سازی شده[۱] را بر اساس الگوریتم رمزنگاری خاص [انتخاب:HMAC-SHA-1, HMAC-SHA-256,HMAC-SHA-384, HMAC-SHA-512] و با استفاده از اندازه‌های کلید [اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)] و اندازه‌های 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:**	

[۱] Keyed-hash message authentication

شماره الزام	نام الزام
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**
محصول مورد ارزیابی باید سرویس‌ها تولید بیت تصادفی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG، HMAC_DRBG، CTR_DRBG (AES)] ارائه دهد.	
۱۵	**تولید بیت تصادفی ۲**
RBG قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و CSPs که تولید می‌کند، مطابق با ISO/IEC 18031:2011، باشد. **نکته کاربردی:** در مورد نخستین عبارت این الزام، نویسنده هدف امنیتی حداقل یکی از انواع منابع نویز را انتخاب می‌کند. اگر محصول مورد ارزیابی شامل چند منبع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی از هر یک از انواع منابع پر می‌کند (مثلاً دو منبع نویز مبتنی بر نرم‌افزار و یک منبع نویز مبتنی بر سخت‌افزار). مستندات و آزمون‌های مورد نیاز در فعالیت‌های ارزیابی، باید تکرار گردند تا تمام منابع مشخص شده در هدف امنیتی را پوشش دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها به عناصر اولیه فرایند رمزنگاری (توابع درهم‌ساز و مجموعه‌های رمز) بستگی دارد. نویسنده هدف امنیتی، تابع استفاده شده و شامل عناصر اولیه فرایند رمزنگاری را که در الزام بکار گرفته شده است، انتخاب خواهد کرد. با اینکه تمام توابع درهم‌ساز تعیین‌شده (SHA-1، SHA-256، SHA-384، SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، در پیاده‌سازی‌های CTR_DRBG تنها موارد مبتنی بر AES اجازه استفاده دارند. اگر اندازه کلید برای پیاده‌سازی AES متفاوت با اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تغییر یا تکرار «عملیات رمزنگاری» باشد تا تفاوت اندازه کلید در آن لحاظ گردد. در قسمت انتخاب تعداد بیت آنتروپی مربوط به این الزام، نویسنده هدف امنیتی حداقل تعداد بیت‌های انتروپی تزریق‌شده به RBG را انتخاب می‌کند که این مقدار باید بزرگتر یا مساوی طول هر کلید امنیتی باشد که توسط محصول تولید می‌شود.	

۴,۳ کلاس دیواره آتش (FFW)

برای مقابله با مشکل افشای غیر مجاز اطلاعات، دسترسی غیر مجاز 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
۱۶	**فیلترینگ حالتمند ۱**
محصول، باید برروی بسته‌های شبکه‌ای که توسط محصول پردازش میشود، فیلترنمودن ترافیک را انجام دهد. نکته کاربردی: کلاس فایروال دارای یک عنصر به نام فیلتر نمودن حالتمند ترافیک شبکه می‌باشد که بر روی بسته‌های پردازش شده توسط محصول اعمال می‌گردد. فایروال های که دارای این عنصر می باشند اصطلاحاً فایروال‌های حالتمند نامیده می‌شوند. فایروال های حالتمند قادر به نگهداری و دنبال کردن وضعیت اتصالات شبکه عبوری از خود می باشند. لازم به یادآوری است که محصول که بر اساس این روش کار کند، به هیچ بسته ای اجازه عبور نمی دهد مگر آنکه در مجموعه قوانین، قانونی وجود داشته باشد که اجازه عبور آن را بدهد یا آن بسته متعلق به ارتباطی باشد که قبلا به آن اجازه عبور داده شده باشد.	

۱۷	فیلترینگ حالتمند ۲

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

- ICMPv4
  - نوع
  - کد
- ICMPv6
  - نوع
  - کد
- IPv4
  - آدرس مبدا
  - آدرس مقصد
  - پروتکل لایه انتقال
- IPv6
  - آدرس مبدا
  - آدرس مقصد
  - پروتکل لابه انتقال
  - [انتخاب: نوع سرایند توسعه یافته IPv6 [اختصاص: لیست فیلدهای که در سرآیند IPv6 توسعه یافته است، هیچ فیلد دیگری]]
- TCP
  - پورت مبدا
  - پورت مقصد
- UDP
  - پورت مبدا
  - پورت مقصد

و واسطه متمایز

نکته کاربردی:

این مولفه در زمان ایجاد قوانینی که توسط این الزام اجرا می‌گردند، ویژگی‌های مختلف قابل بکارگیری را تعریف می نماید. 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.
۱۸ فیلترینگ حالتمند ۳
محصول، باید امکان انجام عملکردهای زیر را برای هر یک از قوانین فیلتر نمودن حالتمند شبکه فراهم آورد: • اجازه داده (allow) یا کنار گذاشتن (drop) به همراه 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.
۱۹ فیلترینگ حالتمند ۴
محصول، باید امکان اعمال هر یک از قوانین فیلتر نمودن حالتمند شبکه را بر روی هر یک از واسط های شبکه فراهم آورد. نکته کاربردی: این عنصر محل اعمال قوانین را مشخص می کند. یک محصول مطابق با این پروفایل حفاظتی، باید قادر باشد که قوانین فیلتر نمودن را به هریک از واسط‌های شبکه که در دسترس هستند و قابل مشخص شدن باشند و ترافیک شبکه لایه ۳و ۴ را به کار می‌برند، اعمال نماید. قابل شناسایی به این معنی است که واسط‌ها در داخل محصول منحصربه فرد و قابل شناسایی است و لزوماً به واسطی که از دید شبکه قابل مشاهده باشد، اشاره ندارد (به طور مثال لازم نیست که حتما به آن واسط آدرس اینترنتی اختصاص داده شده باشد). قابل ذکر است که می‌توان یک مجموعه قوانین مجزا برای هر واسط داشته باشد و یا یک مجموعه قوانین مشترک برای واسط های مشخصی اعمال شود.
۲۰ فیلترینگ حالتمند ۵
محصول باید: الف) بسته‌های شبکه را بدون پردازش نمودن قوانین مربوط به فیلترنمودن حالتمند ترافیک قبول نماید، چنانچه آن بسته منطبق با نشستی شروع شده مجازی برای پروتکلهای TCP، UDP و [*ICMP، هیچ پروتکل دیگری*] و بر اساس صفات پروتکلهای شبکه ای زیر باشد: - TCP: آدرس مبدا و مقصد، پورت‌های مبدا و مقصد، شماره توالی[۱]، پرچم‌ها

[۱] Sequence number

- UDP: آدرس مبدا و مقصد، پورت‌های مبدا و مقصد
- [انتخاب: *" ICMP : آدرس مبدا و مقصد، [انتخاب: نوع، کد، [اختصاص: **لیستی از ویژگی‌های تطبیق**]"، هیچ پروتکل دیگری]*

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

نکته کاربردی:

این عنصر الزام می دارد که بر اساس چه صفت یا ویژگی از پروتکلها، محصول می تواند وضعیت یک نشست که مجاز به شروع شدن بوده است را تعیین و مدیریت نماید. هم‌چنین این الزام صفات عملی که برای تطابق و تعیین نشست شروع شده با بسته های شبکه مورد استفاده قرار می گیرند را مشخص می نماید.

چنان‌چه ICMP به عنوان پروتکل انتخاب گردد، آدرس میدا و آدرس مقصد برای تعیین متعلق بودن یک بسته به ارتباط شروع شده قبلی مورد استفاده قرار می گیرد. ممکن است از مشخصه‌های "نوع " و "کد " جهت ارائه قابلیت‌های تطابق محکمتری استفاده گردد تا مشخص شود که آیا بسته ICMP مورد نظر متعلق به یک ارتباط شروع شده قبلی است. برای مثال در صورت دریافت نشدن هیچ بسته درخواست echo، نباید انتظار داشت که بسته پاسخ echo ارسال گردد. بخش اختصاص در این بخش این امکان فراهم می آورد تا صفات دیگری برای پیاده سازی برای استفاده در نسخه IPv6 به این بخش اضافه نمایند.

در قسمت "انتخاب " ویژگی‌های ICMP، بخشی به نام اختصاص وجود دارد که برای انتخاب ویژگی‌های ICMP در پیاده‌سازی‌هایی که ممکن است از ویژگی‌های IPv6 استفاده نمایند، از بخش "اختصاص " کمک گرفته می‌شود.

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 یک رویداد حذف نماید. به طور مثال نشست TCP برقرار شده توسط نقطه پایان، خاتمه یابد. این نقطه پایان، FIN Flag در بسته TCP می‌باشد.

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

۲۱	**فیلترینگ حالتمند ۶**

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

۱- محصول باید بسته‌های اطلاعاتی که به صورت نامعتبر قطعه بندی شده اند را رد نماید و قادر به [انتخاب: شمردن، ثبت] نمودن آنها باشد.

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

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

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

۵- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا و یا آدرس مقصد آن نامشخص باشد (به عنوان نمونه 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- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدا و مقصد بسته اطلاعاتی به صورت آدرس "نامشخص " یا آدرسی که "رزرو شده برای تعریف و استفاده در آینده " (به عنوان نمونه آدرس های تک پخشی که در بازه:2000::/3 نیست) همان‌گونه که در RFC3513 برای IPv6 مشخص شده، تعریف شده باشد.

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

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

۸- [انتخاب: *[اختصاص: دیگر قوانین پیش‌فرضی که توسط محصول اجرا می‌گردد]، بدون هیچ قانون دیگر*]

۲۲	**فیلترینگ حالتمند ۷**

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

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

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

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

---

[۱] Broadcast network
[۲] Multicast network
[۳] Loopback address

۲۳	**فیلترینگ حالتمند ۸**
محصول باید قادر باشد قوانین اجرایی فیلترنمودن حالتمند ترافیک را به ترتیب تعیین شده توسط سرپرست محصول، پردازش نماید.	
۲۴	**فیلترینگ حالتمند ۹**
محصول باید مانع از عبور جریان بسته های شود که هیچ قانونی برای آن مشخص نشده است.	
۲۵	**فیلترینگ حالتمند ۱۰**
محصول باید قادر باشد تعداد اتصالات نیمه باز TCP را مطابق با تعریف سرپرست سیستم محدود نماید. برای رویدادهای که مقدار آن به مقدار حد پیکربندی می رسد، اتصالات جدید باید حذف و رویداد حذف شده باید [انتخاب: شمرده، ثبت] شود.	

۴,۴ کلاس شناسایی و احرازهویت

محصول، یک مکانیزم ورود مبتنی بر گذرواژه را به عنوان ابزاری امن در اختیار سرپرستان قرار می‌دهد تا بتوانند با استفاده از آن با محصول مورد ارزیابی ارتباط برقرار کنند. سرپرست محصول باید یک گذرواژه قدرتمند را تهیه کند و مکانیزمی را برای تغییر منظم آن در نظر گیرد. برای جلوگیری از حملاتی که در آن‌ها فرد مهاجم نوشتن/ورود گذرواژه بوسیله سرپرست را می‌بیند، گذرواژه را باید در هنگام ورود به حالت محو و ناخوانا درآورد. قفل‌کردن و خاتمه دادن نشست را نیز می‌توان برای جلوگیری از ورود غیر مجاز به حساب کاربری استفاده شده قرار داد. گذرواژه‌ها 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
۲۶	**مدیریت احرازهویت ناموفق ۱**
محصول مورد ارزیابی باید وقتی که یک عدد مثبت قابل تنظیم توسط سرپرست در [اختصاص: بازه مقادیر قابل‌قبول]، از تلاش‌های ناموفق احرازهویت مرتبط با تلاش‌های سرپرستان برای احرازهویت راه‌دور اتفاق میافتد را تشخیص دهد.	
۲۷	**مدیریت احرازهویت ناموفق ۲**
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 روی یک تعداد تلاش پی‌درپی احرازهویت ناموفق اعمال می‌شود و برای یک سرپرست در کنسول محلی اعمال نمی‌گردد، زیرا قفل کردن یک سرپرست محلی، مد نظر نمی‌باشد. نیل به این مهم نیازمند وجود حساب‌های سرپرستی محلی و راه‌دور جداگانه یا داشتن مکانیزم احرازهویتی می‌باشد که بتواند تلاش‌های ورود سرپرست محلی و راه‌دور را بصورت متمایز پیاده‌سازی نماید. عبارت "اقدام " در اختصاص این الزام، توسط یک سرپرست محلی اتخاذ می‌گردد و در واقع یک پیاده‌سازی خاص می‌باشد که توسط راهنمای سرپرست[۱] تعریف می‌شود (مثل: بازنشاندن رمزعبور[۲]، بازنشاندن قفل[۳]). نویسنده هدف امنیتی یک از گزینه‌های انتخاب در این الزام را برای کنترل کردن شکست‌های احرازهویت، بسته به نوع پیاده‌سازی کنترل‌کننده در محصول، گزینش می‌نماید.

خلاصه مشخصات محصول باید توصیف نماید که محصول چگونه این اطمینان را ایجاد می‌کند که مسدود شدن موقت یا دائم یک سرپرست راه‌دور بدلیل شکست‌های احرازهویت، باعث بوجود آمدن عدم دسترس‌پذیری سرپرست نمی‌گردد (مثال: با تعریف کردن یک ورود محلی که مسدود سازی برای آن اعمال نمی‌شود). راهنمای محیط عملیاتی مشخص می‌سازد که چگونه همیشه یک دسترسی سرپرست نگه‌داری می‌شود حتی در صورتی که یک سرپرست راه‌دور در اثر موارد مطرح شده در این الزام، مسدود گردد.

۲۸	**مدیریت رمز عبور ۱**

محصول مورد ارزیابی باید قابلیت‌های مدیریت گذرواژه زیر را برای کلمه‌ی عبور سرپرست اجرایی محصول فراهم آورد:

الف) گذرواژه را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: [انتخاب: "(", ")", "*", "&", "^", "%", "$", "#", "@", "!"، [اختصاص: سایر کارکترها]]؛

ب) حداقل طول گذرواژه باید قابل پیکربندی به [اختصاص: کمترین تعداد کارکترهای قابل پشتیبانی توسط محصول] و [اختصاص: تعداد کارکترهای بزرگتر مساوی با ۱۵]باشد.

نکته کاربردی:

نویسنده هدف امنیتی کاراکترهای ویژه قابل استفاده در گذرواژه را انتخاب می‌کند. وی می‌تواند با استفاده از عبارت اختصاص در بند الف، کاراکترهای دیگری را به لیست اضافه کند. منظور از «کلمه‌ی عبور سرپرست اجرایی»، گذرواژه‌هایی هستند که توسط مدیران سیستم در کنسول محلی روی پروتکل‌هایی که از آن‌ها پشتیبانی می‌کنند مانند، SSH و HTTPS، مورد استفاده قرار می‌گیرند. این گذرواژه‌ها گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی که از دیگر الزامات کارکرد امنیتی در محصول پشتیبانی می‌کنند، مورد استفاده قرار می‌گیرند.

---

۱ Administrator guidance
۲ Password reset
۳ Lockout reset

اختصاص مطرح شده در بند ب، باید به بزرگترین مقداری که می‌تواند برای کمینه طول رمزعبور توسط سرپرست پیکربندی شود، تنظیم گردد.	
۲۹	**شناسایی و احرازهویت کاربر ۱**
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 ازهدف ارزیابی]]	
۳۰	**شناسایی و احرازهویت کاربر ۲**
پیش از آن که محصول مورد ارزیابی امکان انجام اقدامات مدیریتی سیستم را فراهم آورد، باید هر مدیرسیستم را ملزم نماید که به صورت موفق شناسایی و احرازهویت گردد. **نکته کاربردی:** این الزام برای کاربران سرویس‌های که به طور مستقیم توسط محصول مورد ارزیابی در دسترس قرار می‌گیرند (چه مدیران سیستم و چه کارشناسان IT خارجی) اعمال می‌شود و در مورد سرویس‌های که از طریق ارتباطات محصول مورد ارزیابی فراهم می‌گردند، اعمال نمی‌شود. از آنجا که موجودیت‌های خارجی پیش از تعیین و احرازهویت تنها باید به چند خدمت محدود (و یا هیچ خدمتی) دسترسی داشته باشند، برای این سرویس‌ها باید عبارت اختصاص تعریف شود و در آن ذکر شوند، در غیر این صورت، باید «هیچ اقدام دیگر» برای عبارت اختصاص، انتخاب می‌گردد. احرازهویت می‌تواند مبتنی بر گذرواژه باشد و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از گذرواژه‌ها 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 یا سرور NTP) این ارتباطات باید بر اساس الزام‌های FTP_ITC.1 انجام شوند که پروتکل آن از شناسایی و احرازهویت پشتیبانی می‌کند. این امر بدین معنی است که نیازی نیست ارتباطاتی از قبیل ایجاد ارتباط IPsec با سرور احرازهویت، در عبارت اختصاص ذکر شوند، زیرا ایجاد ارتباط به معنی آغاز فرایند شناسایی و احرازهویت است. با توجه به نکته کاربردی مطرح شده در الزام FMT_SMR.2، برای محصولات توزیع‌شده، حداقل یکی از مؤلفه‌های محصول باید شناسایی و احرازهویت را برای سرپرست‌های امنیتی، مطابق با الزامات FIA_UIA_EXT.1 و FIA_UAU_EXT.2، اجرا نماید. این امر برای تمامی مؤلفه‌ها ضروری نمی‌باشد. در مواردی که هیچ کدام از مؤلفه‌های این امر را پشتیبانی نمی‌کنند، خلاصه مشخصات محصول باید توضیح دهد که چگونه شناسایی و احرازهویت را برای سرپرست‌های امنیتی انجام می‌دهد.	

۳۱	سازوکار احرازهویت بر اساس رمزعبور ۲

محصول مورد ارزیابی باید یک مکانیزم محلی احرازهویت [انتخاب: مبتنی بر گذرواژه، مبتنی بر کلید عمومی SSH، مبتنی بر گواهینامه [اختصاص: سایر مکانیزم‌های احرازهویت]، هیچ مکانیزم دیگری] را برای احرازهویت کاربر محلی مدیر سیستم فراهم آورد.

نکته کاربردی:

عبارت اختصاص باید برای مشخص کردن تمام مکانیزم‌های محلی احرازهویت پشتیبانی‌شده، اضافه بر موارد ذکر شده را نشان دهد. مکانیزم‌های احرازهویت محلی در واقع آن‌هایی هستند که از طریق کنسول محلی انجام می‌شوند. نشست‌های مدیریتی از راه‌دور (و مکانیزم‌های احرازهویت مربوط به آن‌ها) در الزام FTP_TRP.1/Admin مشخص شده‌اند.

با توجه به نکته کاربردی مطرح شده در الزام FMT_SMR.2، برای محصولات توزیع‌شده، حداقل یکی از مؤلفه‌های محصول باید شناسایی و احرازهویت را برای سرپرست‌های امنیتی، مطابق با الزامات FIA_UIA_EXT.1 و FIA_UAU_EXT.2، اجرا نماید. این امر برای تمامی مؤلفه‌ها ضروری نمی‌باشد. در مواردی که هیچ کدام از مؤلفه‌های این امر را پشتیبانی نمی‌کنند، خلاصه مشخصات محصول باید توضیح دهد که چگونه شناسایی و احرازهویت را برای سرپرست‌های امنیتی انجام می‌دهد.

۳۲	احرازهویت کاربر ۱۰

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

نکته کاربردی:

«بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی داده‌های احرازهویت وارد شده توسط کاربر را به صورت واضح و قابل خواندن نشان نمی‌دهد؛ 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 احرازهویت هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احرازهویت باشد، نمایش نمی‌دهد.

۴,۵ کلاس مدیریت امنیت

توابع مدیریتی مورد نیاز در این بخش، شامل قابلیت‌های مورد نیاز برای پشتیبانی از نقش سرپرست امنیتی محصول و همچنین مجموعه‌ای از توابع مدیریتی امنیت مورد نیاز برای مدیریت بخش‌های قابل پیکربندی الزامات

[۱] Obscured feedback

کارکرد امنیتی (FMT_SMF.1)، مدیریت کلی داده‌های توابع امنیتی محصول (FMT_MTD.1/CoreData) و فعال کردن به‌روزرسانی‌های محصول (FMT_MOF.1/ManualUpdate) هستند.

برای محصولات توزیع‌شده، مدیریت امنیتی مؤلفه‌های محصول باید برای هر مؤلفه به صورت مستقیم یا از طریق دیگر مؤلفه‌های تحقق بخشیده شود. خلاصه مشخصات محصول باید مشخص نماید که کدام الزامات کارکردی امنیتی مدیریتی و توابع مدیریتی برای هر مؤلفه اعمال می‌گردد (فقط در محصولات توزیع‌شده).

در کنار این الزامات مدیریتی اصلی، برخی الزامات اختیاری نیز در پیوست اول و تعدادی الزامات انتخابی نیز در پیوست دوم ذکر شده‌اند.

شماره الزام	نام الزام
۳۳	کارکرد مدیریتی محصول ۱/ فایروال
محصول مورد ارزیابی باید قادر به انجام عملکرد مدیریتی زیر باشد: • پیکربندی قوانین فایروال	

شماره الزام	نام الزام
۳۴	**مدیریت داده‌های محصول ۱**
محصول مورد ارزیابی باید امکان «مدیریت» داده‌های توابع امنیتی محصول را به سرپرست‌های امنیتی محدود کند. **نکته کاربردی:** منظور از «مدیریت» می‌تواند هر یک از این اقدامات و موارد دیگری از این دست باشد: تولید، آغاز، بازدید، تغییر پیش‌فرض، تغییر، پاک کردن و اضافه نمودن. الزام حاضر همچنین شامل بازگرداندن گذرواژهکاربری به حالت پیش‌فرض توسط سرپرست محصول امنیتی است. عبارت "CoreData" در نام این الزام برای جداسازی آن با الزام ذکر شده در قسمت الزامات اختیاری با نام FMT_MTD.1/CryptoKeys می‌باشد.	
۳۵	**کارکرد مدیریتی محصول ۱**

شماره الزام	نام الزام

محصول مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد:

[اختصاص:

- اداره کردن محصول به‌صورت محلی و راه‌دور
- پیکربندی بنر دسترسی
- پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن
- به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از[انتخاب: امضای دیجیتال، مقایسه درهم‌سازی] پیش از نصب شدن این به‌روزرسانی‌ها
- پیکربندی پارامترهای شکست احرازهویت برای الزام FIA_AFL.1
- [انتخاب:
  - پیکربندی رفتار ممیزی
  - پیکربندی لیست سرویس‌ها ارائه‌شده توسط محصول مورد ارزیابی پیش از شناسایی یا احرازهویت یک موجودیت، مشخص شده در الزام FIA_UIA_EXT.1
  - پیکربندی کارکرد رمزنگاری
  - پیکربندی حدآستانه برای ایجاد مجدد کلید در پروتکل SSH
  - پیکربندی طول عمر برای IPSec SAs
  - پیکربندی تعامل بین مؤلفه‌های محصول
  - فعال‌سازی مجدد حساب سرپرست
  - تنظیم زمان برای مهرهای زمانی
  - پیکربندی شناساننده مرجع برای همتا
  - هیچ قابلیت دیگری]

نکته کاربردی:

محصول مورد ارزیابی باید به طور کلی، قابلیت کارکردی را برای سرپرستی محلی و راه‌دور فراهم آورد. این پروفایل حفاظتی کارکرد مدیریت امنیتی خاصی را برای واسط سرپرستی محلی یا راه‌دور، مشخص نمی‌نماید، بلکه خلاصه مشخصات محصول باید این کار را برای هر واسط معرفی نماید. این کارکردها شامل پیکربندی بنر دسترسی برای الزام FTA_TAB.1 و زمان غیر فعال بودن نشست برای الزام FTA_SSL_EXT.1 و FTA_SSL.3 هستند.

شماره الزام	نام الزام
• آیتم "به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها "، شامل توابع مدیریتی مربوطه در الزامات FMT_MOF.1/ManualUpdate و FMT_MOF.1/AutoUpdate (در صورت ذکر شدن در سند هدف ارزیابی) و الزامات FIA_X509_EXT.2.2 و FPT_TUD_EXT.1.2 و FPT_TUD_EXT.2.2 (اگر شامل اقدام قابل‌پیکربندی توسط سرپرست باشد و در صورت ذکر شدن در سند هدف ارزیابی) می‌باشد. به‌طور مشابه، گزینه "پیکربندی رفتار ممیزی "، شامل توابع مدیریتی مربوطه در الزامات FMT_MOF.1/Services و FMT_MOF.1/Functions (در صورت وجود آن‌ها در سند هدف ارزیابی)، می‌باشد. • اگر محصول امکان مسدودسازی شدن به صورت inline را برای حساب سرپرست راه‌دور قرار داده باشد، آنگاه نویسنده هدف ارزیابی باید گزینه "فعال سازی مجدد حساب سرپرست " را انتخاب کند تا به سرپرست محلی امکان فعال‌سازی مجدد داده شود. • اگر محصول مورد ارزیابی پیش از شناسایی و احرازهویت، امکان پیکربندی رفتار ممیزی و سرویس‌ها موجود را برای سرپرست محصول فراهم کند، یا امکان پیکربندی هر یک از کارکردهای رمزنگاری محصول مورد ارزیابی وجود داشته باشد، نویسنده هدف امنیتی باید گزینه یا گزینه‌های مناسب را در دومین عبارت «انتخاب» برگزیند و در غیر این صورت گزینه «هیچ قابلیت دیگری» را انتخاب کند. • اگر محصول، پیکربندی حدآستانه‌ها برای مکانیزم‌های استفاده شده در الزامات FCS_SSHC_EXT.1.8 و FCS_SSHS_EXT.1.8 (چنین پیکربندی‌هایی نیازمند وجود الزام FMT_MOF.1/Functions در سند هدف ارزیابی می‌باشد) را پشتیبانی کند، آنگاه باید گزینه "پیکربندی حدآستانه برای ایجاد مجدد کلید در پروتکل SSH" در سند هدف ارزیابی آورده شود. همچنین اگر محصول محدودیت‌هایی را در مقادیر قابل قبول برای آستانه‌ها اعمال می‌نماید، این محدودیت‌ها باید در خلاصه مشخصات محصول ذکر گردد. • اگر محصول به سرپرست اجازه تنظیم زمان دستگاه که در مهرهای زمانی استفاده می‌شود را بدهد، آنگاه باید گزینه "تنظیم زمان برای مهرهای زمانی " در سند هدف ارزیابی آورده شود. زمانی که محصول اجازه تنظیم دستی زمان را نمی‌دهد و با یک سرور خارجی مانند سرور NTP، هماهنگی را انجام می‌دهد، گزینه ذکر شده نباید انتخاب گردد. • اگر محصول از ارتباطات امن بوسیله پروتکل IPSec پشتیبانی می‌کند و الزامات FCS_IPSEC_EXT.1 در سند هدف ارزیابی بیان شده است، آنگاه باید گزینه "پیکربندی شناساننده مرجع برای همتا " در سند هدف ارزیابی آورده شود. برای محصولات که فقط از شناساننده‌هایی مانند آدرس IP و FQDN پشتیبانی می‌کنند، پیکربندی شناساننده مرجع ممکن است با پیکربندی نام همتا برای ارتباط، یکسان باشد.	

شماره الزام	نام الزام
• برای محصولات توزیع‌شده، تعامل بین مؤلفه‌های محصول قابل پیکربندی خواهد بود (باتوجه به الزام FCO_CPC_EXT.1). بنابراین، نویسنده سند هدف ارزیابی باید گزینه "پیکربندی تعامل بین مؤلفه‌های محصول " را برای محصولات توزیع‌شده انتخاب نماید. تغییر در مدیریت محصول، از "مستقیماً توسط سرپرستی راه‌دور " به " سرپرستی راه‌دور از طریق مؤلفه‌ی دیگر " می‌تواند به عنوان یک مثال برای پیکربندی تعاملات باشد.	
۳۶	**نقش‌های امنیتی ۳**
محصول باید نقش‌های زیر را نگهداری کند. • سرپرست امنیتی	
۳۷	**نقش‌های امنیتی ۴**
محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.	
۳۸	**نقش‌های امنیتی ۵**
محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند: • نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را به صورت محلی اداره کند. • نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را از راه‌دور اداره کند. **نکته کاربردی:** بر اساس این الزام سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک مکانیزم راه‌دور اداره کند. نویسنده سند هدف ارزیابی باید الزامات FTP_ITC.1، FPT_ITT.1 و/یا FTP_TRP.1/Admin را برای اثبات چگونگی بدست آمدن یک ارتباط امن، انتخاب نماید. برای محصولات توزیع‌شده، نیاز نیست که هر مؤلفه مدیریت خود برای این الزام را پیاده‌سازی کند. حداقل یک مؤلفه باید احرازهویت و شناسایی سرپرستان امنیتی را بر اساس الزامات FIA_UIA_EXT.1 و FIA_UIA_EXT.2 پشتیبانی نماید. برای اعمال شدن احرازهویت در دیگر مؤلفه‌ها، سرپرست امنیتی باید از طریق یک کانال امن (مطابق با الزامات FTP_ITC.1 یا FPT_ITT.1) و مؤلفه‌ای که احرازهویت و شناسایی را پشتیبانی می‌کند، با مؤلفه‌های دیگر ارتباط برقرار نماید. شناسایی کاربرها و ارتباط بین کاربران و نقش‌ها نیز از طریق مؤلفه‌ای که احرازهویت و شناسایی را پشتیبانی می‌کند، انجام می‌گیرد. برای دیگر مؤلفه‌ها نیاز نیست که از سرپرستی محلی مؤلفه (ذکر شده در الزام FMT_SMR.2.3) پشتیبانی کنند.	

۴,۶ کلاس حفاظت از محصول مورد ارزیابی

در این بخش، الزامات مربوط به محصول مورد ارزیابی برای حفاظت از داده‌های امنیتی حساس مانند کلیدها و گذرواژه‌ها، 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
۳۹	**محافظت از داده‌های محصول (کلیدهای متقارن) ۱**
محصول مورد 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 دسترسی غیر مجاز به کلیدها، اطلاعات کلیدها و اطلاعات احرازهویت شود. این داده‌ها باید تنها برای 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 محدود می‌کند.	
۴۰	**حفاظت از گذرواژه سرپرست محصول ۱**
محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	
۴۱	**حفاظت از گذرواژه سرپرست محصول ۲**
محصول مورد ارزیابی باید از خوانده شدن گذرواژه‌هایی که به‌صورت متن ساده[۱] هستند، جلوگیری کند. **نکته کاربردی:** هدف از الزام حاضر این است که داده‌های خام مربوط به احرازهویت از طریق گذرواژه، به شکل واضح ذخیره نشوند و هیچ کاربر و سرپرست محصول نتواند گذرواژه متن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصول که تمام دسترسی‌ها را داشته	

[۱] Plaintext

باشد می‌تواند گذرواژه را بخواند؛ اما به وی اعتماد می‌شود و فرض می‌گردد که وی این کار را نخواهد کرد. گذرواژه‌ها باید مطابق با الزام FIA_UAU.7 هنگام ورود در کنسول محلی، به صورت مبهم باشد.

۴,۶,۱ تست محصول مورد ارزیابی

محصول مورد ارزیابی، برای اینکه برخی شکست‌های مکانیزم‌های امنیتی خود را شناسایی کند، خودآزمایی‌هایی را انجام می‌دهد. میزان و حجم این خودآزمایی‌ها به تصمیم تولیدکننده محصول بستگی دارد؛ اما هر چه خودآزمایی‌های جامع‌تری انجام شوند، پلت‌فرم قابل‌اعتمادتری برای استقرار معماری سازمان پدید خواهد آمد. تعدادی الزام مبتنی بر انتخاب برای این مؤلفه در پیوست دو ارائه شده‌اند.

شماره الزام	نام الزام
۴۲	**خودآزمایی محصول ۱**

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

تذکر: در صورتی که برای خودآزمایی‌ها از مکانیزم امضای دیجیتال استفاده شود نیاز است الزام «خودآزمایی 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 تولیدکننده دستگاه توجیه کند که چرا خودآزمایی در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نمی‌شود. انتظار می‌رود که دست کم خودآزمایی‌های لازم برای حصول اطمینان از صحت و یکپارچگی نرم‌افزار و میان‌افزار و کارکرد صحیح توابع رمزنگاری انجام شوند. اگر خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نشوند، الزام کارکرد امنیتی حاضر چند بار و هر بار با انتخاب‌های مختلف اجرا می‌شود.

شماره الزام	نام الزام
محصولات توزیع‌نشده ممکن است به صورت داخلی شامل چند مؤلفه توزیع شده در راستای اجرای الزامات کارکرد امنیتی باشند. خودآزمایی‌ها باید تمام مؤلفه‌هایی که برای اجرای الزامات کارکرد امنیتی توزیع شده‌اند را پوشش دهد و اگرچه ممکن است در راستای اجرایی شدن الزامات کارکرد امنیتی، این الزامات روی مؤلفه‌ها توزیع شده باشند، ولی بررسی/تایید جامعیت شدن باید تمام نرم‌افزار را پوشش دهد. برای محصولات توزیع‌شده هر مؤلفه ملزم به اجرای خودآزمایی می‌باشد. ولی الزامی وجود ندارد که همه مؤلفه‌ها خودآزمایی یکسانی را اجرا نمایند. نویسنده هدف امنیتی انتخاب‌های ممکن و سپس اختصاص‌های نهایی را برای هر مولفه توصیف می‌نماید. **نکته کاربردی:** اگر در خودآزمایی‌ها از گواهی‌نامه‌ها استفاده شود (مثلاً برای تأیید امضا جهت تأیید صحت و یکپارچگی)، گواهی‌نامه‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب شوند و بر اساس الزام «الزامات پروتکل X509 (۱)» و الزام «الزامات پروتکل X509 (۲)» تأیید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی در نظر گرفته شوند.	

۴,۶,۲ به‌روزرسانی امن

عدم موفقیت سرپرست محصول در تأیید به‌روزرسانی‌های سیستم، ممکن است کل سیستم را در معرض خطر قرار دهد. برای اعتماد به منبع به‌روزرسانی‌ها، سیستم می‌تواند مجموعه‌ای از فرایندها و مکانیزم‌های رمزنگاری را مورداستفاده قرار دهد و با استفاده از آن‌ها، به‌روزرسانی‌ها را تهیه و تدارک ببیند، رمزنگاری به‌روزرسانی‌ها را از طریق مکانیزم امضای دیجیتال بررسی کند و به‌روزرسانی‌ها را روی سیستم نصب نماید. هرچند که الزامی برای انجام خودکار این فرایند وجود ندارد، اسناد راهنما و رویکرد سرپرست محصول برای حصول اطمینان از اعتبار امضا را باید مبنای کار قرار داد.

تعدادی الزام مبتنی بر انتخاب برای این خانواده در پیوست دو ارائه شده‌اند.

شماره الزام	نام الزام
۴۳	**به روز رسانی امن ۱**
محصول مورد ارزیابی باید این امکان را به سرپرستان امنیتی محصول بدهد که به نسخه فعلی نرم‌افزار/میان‌افزار محصول و [انتخاب: جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول، هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول] دسترسی داشته باشد. **نکته کاربردی:**	

شماره الزام	نام الزام
	اگر امکان نصب یک به‌روزرسانی مورد اعتماد که همان لحظه فعال نمی‌گردد یعنی فعال‌سازی آن دارای تاخیر می‌باشد، در محصول وجود داشته باشد، آنگاه باید هر دو نسخه محصول: نسخه مورد استفاده و نسخه نصب شده (به صورت تصویری از غیرفعال بودن آن) فراهم گردد. در این گونه موارد، گزینه " جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول " در انتخاب این الزام، باید منتخب گردد و همچنین در خلاصه مشخصات محصول باید مشخص گردد که چگونه و چه زمانی نسخه غیرفعال، فعال می‌گردد. اگر تمامی به‌روزرسانی‌ها همزمان با نصب فعال می‌گردند، آنگاه فقط نسخه فعلی در حال اجرای محصول باید فراهم گردد و گزینه " هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول " برای انتخاب این الزام برگزیده خواهد شد. برای محصولات توزیع‌شده، نحوه تصمیم‌گیری در رابطه با نسخه‌های نصب شده روی هر مؤلفه در سند راهنمای عملیاتی توضیح داده شده است.
۴۴	**به روز رسانی امن ۲**
	محصول مورد ارزیابی باید این امکان را برای سرپرستان امنیتی محصول فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار محصول مورد ارزیابی را به صورت دستی انجام دهد و [انتخاب: از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی‌های خودکار پشتیبانی کند، از هیچ مکانیزم به‌روزرسانی دیگری پشتیبانی نکند]. **تذکر: در صورتی که نویسنده سند هدف امنیتی برای این الزام گزینه‌های به روزرسانی 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 این الزام، بین پشتیبانی از «جستجوی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز قائل می‌شود. "جستجوی خودکار به‌روزرسانی‌ها " به یک محصول مورد ارزیابی اشاره دارد که جستجو می‌کند تا ببیند به‌روزرسانی جدیدی وجود دارد یا خیر و این امر را به سرپرست محصول اطلاع می‌دهد (مثلاً از طریق یک پیام یا یک پرچم)، اما نصب به‌روزرسانی نیازمند انجام اقداماتی توسط سرپرست محصول خواهد بود، اما "به‌روزرسانی خودکار " به یک محصول مورد ارزیابی اشاره دارد که به‌روزرسانی‌ها را جستجو می‌کند و در صورت وجود آن‌ها را نصب می‌نماید. خلاصه مشخصات محصول باید بیان کند که چه اقداماتی برای پشتیبانی محصول از گزینه‌های "از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند " یا "از به‌روزرسانی‌های خودکار پشتیبانی کند " در قسمت "انتخاب " این الزام، دخیل هستند.

شماره الزام	نام الزام
	وقتی که برای حفاظت از مکانیزم به‌روزرسانی مورداعتماد، مقادیر هش‌شده منتشر شده است، محصول نباید به صورت خودکار فایل (ها) به‌روزرسانی به همراه مقدار هش را (ممکن است همراه فایل یا به صورت جدا از فایل باشد) دانلود کند و به صورت خودکار بدون هیچ‌گونه مجوز فعال[۱] از سرپرست امنیتی نصب کند، حتی برای مواردی که مقادیر محاسبه شده هش با مقادیر منتشر شده منطبق باشد. در این مورد نباید گزینه "از به‌روزرسانی‌های خودکار پشتیبانی کند " استفاده گردد (بررسی خودکار برای وجود به‌روزرسانی مانعی ندارد). در این گونه موارد باید همیشه یک مجوز فعال از سرپرست امنیتی وجود داشته باشد و گزینه "به‌روزرسانی دستی " باید انتخاب گردد، اگرچه ممکن است فایل (ها) به طور خودکار دانلود شده باشند. به‌روزرسانی‌های کاملا خودکار فقط باید در حالتی که از مکانیزم امضاء دیجیتال استفاده شده باشد، انتخاب گردد.
۴۵	**به روز رسانی امن ۳**
	محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: مکانیزم امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احرازهویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد. **تذکر: در صورتی که از مکانیزم امضای دیجیتال استفاده شود نیاز است الزام‌های «الزامات به روز رسانی ۴» و «الزامات به روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.** **نکته کاربردی:** مکانیزم امضاء دیجیتال که در این الزام به آن اشاره شده است، یکی از الگوریتم‌هایی است که در الزام «عملیات رمزنگاری ۱ (۲)» تشریح شده است. همچنین درهم‌ساز مورد استفاده در این الزام نیز توسط یکی از توابع تشریح‌شده در الزام «عملیات رمزنگاری ۱ (۳)» تولید می‌شود. نویسنده هدف امنیتی باید مکانیزم اجرا شده توسط محصول مورد ارزیابی را تعیین نماید، هر دو مکانیزم نیز می‌تواند مورد استفاده قرار گیرد. وقتی که از مقادیر هش منتشر شده برای امن کردن مکانیزم به‌روزرسانی مورداعتماد استفاده می‌شود، یک "مجوز فعال " برای فرآیند به‌روزرسانی، از طرف سرپرست امنیتی نیاز است. به علاوه، مخابره امن مقدار هش موثق[۲] از توسعه‌دهنده/تولید کننده محصول به سرپرست امنیتی، یکی از فاکتورهای کلیدی برای حفاظت از مکانیزم به‌روزرسانی مورداعتماد است و سند راهنما باید چگونگی انجام این انتقال/مخابره را توضیح دهد. برای تصدیق[۳] مقدار هش مورداعتماد توسط سرپرست امنیتی، چندین روش امکان‌پذیر می‌باشد.

[۱] active authorization
[۲] Authentic hash value
[۳] Verification

شماره الزام	نام الزام

سرپرست امنیتی می‌تواند مقدار هش را مانند فایل(ها) به‌روزرسانی بدست آورد و در حالی که هش کردن فایل(ها) در درون محصول در حال انجام است، تصدیق هش را خارج از محصول انجام دهد.

وقتی تصدیق هش موفق باشد، محصول می‌تواند بدون هیچ گام اضافه دیگری از طرف سرپرست امنیتی، به‌روزرسانی را انجام دهد. احرازهویت شدن به عنوان سرپرست امنیتی و فرستادن مقدار هش به محصول معادل با "مجوز فعال " برای به‌روزرسانی امن، درنظر گرفته می‌شود (وقتی تصدیق هش باموفقیت انجام شود)، زیرا انتظار می‌رود وقتی که به‌روزرسانی مد نظر باشد، سرپرست مقدار هش را روی محصول بارگذاری کند.

اگر مکانیزم امضاء دیجیتال انتخاب گردد، تصدیق امضاء بوسیله خود محصول انجام می‌گیرد. برای مکانیزم هش منتشرشده، تصدیق هم بوسیله سرپرست امنیتی و هم محصول قابل انجام است.

برای محصولات توزیع شده، همه مؤلفه‌ها باید از به‌روزرسانی امن پشتیبانی کنند. تصدیق امضاء یا هش به‌روزرسانی، باید بوسیله هر مؤلفه محصول (تصدیق امضاء) یا برای هر مؤلفه محصول (تصدیق هش) انجام گیرد.

نکته کاربردی:

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

نکته کاربردی:

اگر در مکانیزم تأیید به‌روزرسانی از گواهی‌نامه‌ها استفاده شود، این گواهی‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب شده و بر اساس «الزامات پروتکل X509» تأیید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» 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 آن را به نسخه قدیمی‌تر برگرداند و این کار ایرادی ندارد (مثلاً هنگامی که شرکتی یک به‌روزرسانی معیوب را منتشر کند، یا هنگامی که سیستم مبتنی بر کارکرد 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 نرم‌افزار (مانند برنامه‌های کاربردی، درایورها، هسته و میان‌افزار[۱]) محصول مورد ارزیابی باید توسط تولیدکننده، امضای دیجیتال شوند و در نهایت توسط مکانیزم به‌روزرسانی تأیید گردند. از آن‌جا که ممکن است مؤلفه‌ها توسط تولیدکننده‌های

[۱] Firmware

شماره الزام	نام الزام
مختلف امضا شوند، لازم است که فرایند به‌روزرسانی هم تصویر NV و هم تصویر به‌روزرسانی تولیدشده توسط یک تولیدکننده واحد (مثلاً تأیید از طریق مقایسه کلیدهای عمومی) یا امضاشده توسط کلیدهای امضای معتبر را تأیید کند (مثلاً تأیید گواهی‌نامه‌ها در صورت استفاده از گواهی‌نامه‌های X.509).	
۴۶	**مهرهای زمانی ۱**
محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان[۱] برای استفاده خودش را داشته باشد.	
۴۷	**مهرهای زمانی ۲**
توابع امنیتی هدف ارزیابی باید [انتخاب: به مدیر امنیتی اجازه تنظیم زمان بدهد، زمان را با یک سرور NTP هماهنگ کند] **نکته کاربردی:** مهرهای زمانی قابل‌اطمینان جهت استفاده با دیگر توابع امنیتی محصول، مورد نظر می‌باشند؛ به عنوان مثال، برای تولید داده ممیزی جهت اجازه دادن به سرپرست امنیتی که بتواند با بررسی کردن ترتیب رویدادها، وقایع را بازنگری کند و زمان واقعی که وقایع رخ داده است را تعیین نماید. تصمیم در مورد سطح دقت اطلاعات (از لحاظ میزان دقیق بودن زمان رویدادها) به عهده سرپرست می‌باشد. محصول به اطلاعات خارجی زمان و تاریخ وابسته است، این اطلاعات می‌تواند به صورت دستی توسط سرپرست امنیتی تهیه گردند یا به وسیله استفاده از یک یا چند منبع خارجی مانند سرور NTP بدست آورده شوند. بنابراین گزینه مناسب در "انتخاب " این الزام باید باید برگزیده شود. استفاده از یک ساعت بلادرنگ محلی با قابلیت همگام‌سازی خودکار با یک منبع خارجی (مثلا؛ سرور NTP) توصیه می‌گردد، ولی الزام نمی‌باشد. همچنین برای ارتباط با یک منبع خارجی، استفاده از الزام FTP_ITC.1 اختیاری می‌باشد ولی نویسنده سند هدف امنیتی باید مشخص سازد که چگونه اطلاعات زمان و تاریخ بوسیله محصول دریافت و نگهداری می‌گردد. عبارت «مهرهای زمانی قابل‌اطمینان» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ناپیوسته ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده ممیزی را محاسبه کرد. توجه شود که تمامی تغییرات ناپیوسته زمان؛ بوسیله سرپرست یا به صورت خودکار توسط فرآیند، باید ممیزی گردد. اگر زمان بوسیله هسته یا خود سیستم تغییر کند، نیاز به ممیزی نمی‌باشد، این تغییرات دیگر در حوزه تغییرات ناپیوسته زمان، قرار نمی‌گیرند.	

[۱] Reliable time stamps

۴,۷ دسترسی به محصول

این بخش به تشریح الزامات امنیتی مربوط به نشست‌های سرپرست محصول محصول مورد ارزیابی می‌پردازد. هم نشست‌های محلی و هم نشست‌های راه‌دور پایش می‌شوند تا در صورت غیر فعال بودن شناسایی شوند و قفل شدن یا خاتمه یافتن آن‌ها نیز در صورت رسیدن به آستانه زمانی بررسی می‌شود. سرپرستان 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
۴۸	**قفل‌کردن و خاتمه دادن به نشست‌ها ۷**
در مورد نشست‌های تعاملی محلی[۱]، محصول مورد ارزیابی باید پس از اتمام زمان غیر فعال بودن که توسط سرپرست محصول تعیین شده است، [انتخاب: • نشست را قفل کند – تمام فعالیت‌های مربوط به دسترسی به داده‌های کاربری و نمایش این داده‌ها، به جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیر فعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احرازهویت نماید؛ • نشست را خاتمه دهد].	
۴۹	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
در مورد نشست‌های تعاملی راه‌دور[۲]، درصورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود.	
۵۰	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۵۱	**پیغام‌های هشدار در رابطه با استفاده محصول ۱**
قبل از ایجاد نشست برای کاربر سرپرست، توابع امنیتی مورد ارزیابی باید توصیه‌های امنیتی مدیریتی و همچنین پیام هشدار اطلاعیه و توافق‌نامه استفاده از محصول مورد ارزیابی را به سرپرست محصول نشان دهد.	

[۱] Local interactive sessions
[۲] Remote

شماره الزام	نام الزام
نکته کاربردی: این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی مانند تماس‌های راه‌دور از طریق شبکه را برقرار می‌کنند، نیازی به رعایت این الزام نخواهند داشت.	

۴,۸ کلاس کانال‌ها/مسیرهای مورداعتماد

برای پرداختن به مسائل مربوط به انتقال داده‌های حساس از جایی دیگر به محصول مورد ارزیابی و از محصول مورد ارزیابی به جایی دیگر، اهداف ارزیابی مطابق با استانداردها مسیر ارتباطی بین خود و نقاط پایانی را رمزگذاری می‌کنند. این کانال‌ها با استفاده از یک یا چند مورد از این پنج پروتکل استاندارد ایجاد می‌شوند: IPsec, TLS, DTLS, HTTPS و SSH. این پروتکل‌ها توسط RFC هایی تعیین می‌شوند که گزینه‌های پیاده‌سازی مختلفی را در اختیار کاربران قرار می‌دهند. در مورد برخی از این گزینه‌ها الزاماتی نیز جود دارد (مخصوصاً گزینه‌های مربوط به مقادیر اولیه رمزنگاری). هدف این است که قابلیت همکاری و مقاومت در برابر حملات رمزنگاری افزایش یابد. این پروتکل‌ها علاوه بر حفاظت در برابر افشای اطلاعات (و شناسایی تغییرات ایجادشده)، امکان احرازهویت دوطرفه را نیز برای هر یک از نقاط پایانی فراهم می‌آورند و این کار را به صورت امن و با استفاده از روش‌های رمزنگاری انجام می‌دهند. بدین معنی که حتی اگر یک مهاجم بدخواه نیز در بین دو نقطه پایانی حضور داشته باشد، هرگونه تلاش وی برای اینکه خود را به عنوان یکی از طرفین ارتباط معرفی کند، شناسایی خواهد شد.

شماره الزام	نام الزام
۵۲	**کانال امن ۱**
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احرازهویت، اختصاص: [دیگر قابلیت‌ها]، هیچ قابلیت‌های دیگری] که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. **تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH، DTLS،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.**	
۵۳	**کانال امن ۲**

شماره الزام	نام الزام
محصول مورد ارزیابی باید اجازه داشته باشد یا به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
۵۴	کانال امن ۳

محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: لیست سرویس‌های که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی نماید.

نکته کاربردی:

هدف از الزام حاضر فراهم کردن روشی است که جهت حفاظت ارتباطات خارجی با موجودیت‌های معتبر IT، از پروتکل رمزنگاری استفاده گردد. منظوراز موجودیت‌های معتبر IT، موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست کم از یکی از پروتکل‌های ذکر شده در الزام «کانال امن ۱» استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی، ارتباط برقرار کند. اگر ارتباط با یک سرور احرازهویت (مانند؛ RADIUS) برقرار شود، نویسنده هدف امنیتی باید عبارت «سرور احرازهویت» را در دومین "انتخاب " الزام «کانال امن ۱» انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های ذکر شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی را انجام دهد و موارد مناسب را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی مکانیزم یا مکانیزم‌های پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل در 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، سرویس‌های که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباط با موجودیت IT معتبر آغاز کند را لیست می‌نماید.

این الزام بیان می‌دارد که نه تنها ارتباطات در هنگام برقراری اولیه حفاظت می‌شوند، بلکه در حین برقراری مجدد ارتباط پس از یک قطعی نیز از آن‌ها محافظت می‌شود. ممکن است نیاز به تنظیم دستی کانال‌هایی برای حفاظت از سایر ارتباطات وجود داشته باشد. درصورتی‌که پس از یک قطعی، محصول مورد ارزیابی تلاش کند تا ارتباطات را به صورت خودکار و با دخالت عامل انسانی از سر گیرد، ممکن است پنجره‌ای باز شود که مهاجمان بتوانند از طریق آن به اطلاعات مهمی دست یابند یا ارتباط را در معرض خطر قرار دهند.

۵۵	مسیر امن ۱

محصول، باید با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] مسیر ارتباطی امنی را میان خود و سرپرست‌های راه‌دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات در داده کانال را تشخیص دهد.

تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،DTLS،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.

شماره الزام	نام الزام
۵۶	مسیر امن ۲
توابع امنیتی مورد ارزیابی باید به سرپرست راه‌دور اجازه دهد که ارتباطات را از طریق مسیر امن آغاز کند.	
۵۷	مسیر امن ۳
توابع امنیتی مورد ارزیابی باید استفاده از مسیر امن را برای احراز هویت اولیه سرپرست و تمام فعالیت‌های راه دور سرپرستی الزامی کند. **نکته کاربردی:** این الزام اطمینان حاصل می‌نماید که سرپرست‌های راه‌دور مجاز، تمام ارتباطات با محصول مورد ارزیابی را، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل شده از طریق این مسیر، با استفاده از پروتکل انتخاب‌شده در عبارت "انتخاب "، رمزگذاری می‌شوند. نویسنده سند هدف امنیتی، مکانیزم یا مکانیزم‌های پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند.	

۵ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف کننده 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	برچسب گذاری 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 نمی‌باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

۵,۱,۱ مشخصات کارکردی

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

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه دهنده 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 نمی‌باشد.

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 اجرا کننده 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:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره 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.

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

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

۵,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه دهنده	
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:** 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 دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع 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.
	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 توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه دهنده 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 بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	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:** 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 براساس کارکردی که برای محصول در نظر گرفته شده و واسطهایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج تست و تحلیل آسیب‌پذیری باید در گزارش تست لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

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 می‌باشد. ارزیاب باید در سند «گزارش تست»، طرح تست و نتایج آن را مستند نماید.

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

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)**

مؤلفه‌های اقدامات ارزیاب	
	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:** توسعه دهنده 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	**نام عنصر: آسیب‌پذیری ۱**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
(AVA_VAN)	**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 براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۵,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (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، می‌باشد (بدین معنی که جدا ار برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1C)** **شرح مؤلفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری 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 توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱**

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
	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)** **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.

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 و دو به آن‌ها پرداخته شده است. نوع اول (پیوست حاضر) از الزاماتی تشکیل شده است که می‌توان آن‌ها را در هدف امنیتی گنجاند، اما برای انطباق با این پروفایل حفاظتی ضروری نیستند. نوع دوم (پیوست دو) 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).

اگر محصول هر کدام از الزمات اختیاری را انجام دهد، توصیه شده است که فروشنده محصول قابلیت‌های عملکردی مرتبط را به سند هدف امنیتی اضافه نماید. بنابراین در نکات کاربردی مطرح شده در ادامه، عبارت "این گزینه باید انتخاب گردد..." تکرار شده است؛ اما این عبارت همچنین برای تاکید کردن روی این موضوع است که الزام وقتی انتخاب می‌گردد که قابلیت‌های عملکردی مرتبط توسط محصول فراهم شده باشد و نیاز نمی‌باشد که جهت انطباق با این پروفایل حفاظتی، محصول حتما قابلیت‌های عملکردی را پیاده‌سازی نماید. نویسندگان سند هدف امنیتی آزاد هستند که؛ هیچ، برخی یا تمامی الزامات مطرح شده در این بخش را انتخاب نمایند. این واقعیت که محصول از یک قابلیت عملکردی مشخص پشتیبانی می‌نماید، به معنی اضافه کردن تمامی الزامات این بخش به سند هدف امنیتی نمی‌باشد.

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 آن چه در «ذخیره‌سازی رویدادهای ممیزی» گفته شده است، از دستکاری غیر مجاز 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 ۳/ فضای ذخیره‌سازی ممیزی محلی» و «ذخیره‌سازی رویدادهای ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی» تهیه شده‌اند تا این قابلیت‌های اختیاری دستگاه‌های شبکه را بیان کنند.

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

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 تایید 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 آغاز کننده 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 مولفه غیرفعالسازی ارتباط بین یک جفت مولفه	هویت جفت نقاط پایانی فعال یا غیرفعال شده

نکته کاربردی:

رویداد ممیزی «الزامات پروتکل X509(۱) و (۲)/ تبادل داده کاربردی داخل محصول» در صورتی رخ می‌دهد که محصول مورد ارزیابی نتواند از موارد زیر اطمینان حاصل نماید و گواهی‌نامه‌ها را تأیید کند:

- وجود افزونه basicConstraints و تأیید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تأیید امضای دیجیتال CA سلسله مراتبی مورداعتماد
- خواندن و دسترسی به CRL یا دسترسی به سرور OCSP

اگر هر یک از این موارد وجود نداشته باشند، باید یک رویداد ممیزی با نتیجه شکست را در سوابق ممیزی ثبت نمود.

شماره الزام	نام الزام
۵۸	**ذخیره‌سازی داده‌های ممیزی محافظت شده ۱**
محصول مورد ارزیابی باید از پاک شدن غیرمجاز داده‌های ممیزی جلوگیری نماید.	
۵۹	**ذخیره سازی داده‌های ممیزی محافظت شده ۲**
محصول مورد ارزیابی باید از دستکاری غیرمجاز داده‌های ممیزی جلوگیری نماید.	
۶۰	**محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی**
محصول مورد ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده‌های ممیزی [انتخاب: از بین رفته، بازنویسی شده را، [اختصاص: سایر اطلاعات]] ارائه کند. محصول مورد ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده‌های ممیزی ۳» را انجام می‌دهد. **نکته کاربردی:** این گزینه باید انتخاب گردد، در صورتی 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). سند راهنما باید به سرپرست محصول هشدار دهد که خالی کردن حافظه ممکن است سبب از دست رفتن داده‌ها شود. برای محصولات توزیع‌شده، هر مؤلفه که از دست رفتن داده ممیزی را شمارش می‌کند باید مکانیزمی را برای سرپرست فراهم آورد که امکان دسترسی به اطلاعات و مدیریت اطلاعات داشته باشد. اگر این الزام در سند هدف امنیتی بیان گردد آنگاه نویسنده سند هدف امنیتی باید به صورت واضح هر شرایطی را که در آن شمارش از دست رفتن ممیزی انجام نمی‌گیرد، توضیح دهد.	
۶۱	**ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی**
در صورتی که حجم داده‌های ممیزی از ظرفیت ذخیره‌سازی محلی داده‌های ممیزی فراتر رود/سرریز کند، محصول مورد ارزیابی باید با تولید اخطار، سرپرست را اگاه نماید. **نکته کاربردی:**	

این گزینه باید انتخاب گردد، درصورتی‌که محصول مورد ارزیابی امکان تولید پیام برای سرپرست را وقتی حافظه محلی در نظر گرفته شده برای داده ممیزی پر می‌شود، داشته باشد. 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 مورد اشاره در «محل ذخیره‌سازی داده‌های ممیزی ۳» را می‌توان به اطلاع سرپرست رساند. از آنجاییکه نمی‌توان تضمین کرد که در هنگام رخ دادن این رویداد (پر شدن حافظه)، نشست فعالی برای سرپرست اجرایی وجود داشته باشد، ارتباط باید از طریق سوابق ممیزی صورت گیرد.

وقتی که حافظه محلی برای ذخیره‌سازی داده ممیزی پر شد یا محصول به دلیل حافظه ناکافی با خطر از دست دادن داده مواجه شد، پیغام هشدار باید سرپرست را آگاه نماید.

برای محصولات توزیع‌شده که امکان نمایش پیغام هشدار را پیاده‌سازی می‌کنند، باید توضیح داده شود که کدام مؤلفه این ویژگی را پشتیبانی می‌نماید (وقتی که این ویژگی برای یک محصول انتخاب می‌گردد، نیاز نیس که تمامی مؤلفه‌های محصول آن را پشتیبانی نمایند). در نهایت هر مؤلفه‌ای که این ویژگی را پشتیبانی می‌کند، باید یک پیغام هشدار را بوسیله خودش یا از طریق دیگر مؤلفه‌ها تولید نماید.

اگر این الزام در سند هدف امنیتی آورده شود، آنگاه نویسنده سند هدف امنیتی باید شرایطی را که تحت آن داده به صورت غیرقابل مشاهده حذف می‌شود، ذکر نماید.

۶,۲ کلاس شناسایی و احرازهویت

شماره الزام	نام الزام
۶۲	**الزامات پروتکل X509 (۱) / تبادل داده کاربردی داخل محصول**
محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند: • تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است	

- محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 6960، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵، هیچ روش فسخ] تأیید کند.
- محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید 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-kp1 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.

نکته کاربردی:

این الزام باید انتخاب گردد، در صورتی که محصول توزیع‌شده باشد و پروتکل (های) انتخاب شده در الزام FPT_ITT.1 از گواهی‌نامه‌های X.509 برای احرازهویت نظیر استفاده نمایند. در این مورد، از آنجاییکه الزامات اضافه‌ای در الزام FCO_CPC_EXT.1 در رابطه با فعال و غیرفعال‌سازی کانال ITT وجود دارد، استفاده از لیست فسخ اختیاری می‌باشد. در صورتی که بررسی لیست فسخ پشتیبانی نمی‌شود، نویسنده سند هدف امنیتی باید گزینه "هیچ روش فسخ " را انتخاب نماید. به هر حال، درصورت پشتیبانی، نویسنده سند هدف امنیتی باید مشخص نماید که از OCSP یا RCL استفاده می‌گردد.

محصول باید از حداقل طول مسیر برای دو گواهی‌نامه پشتیبانی کند. بدین معنی که محصول باید از یک سلسله مراتب گواهی‌نامه که حداقل از گواهی‌نامه ریشه خود-امضاء[۱] و گواهی‌نامه هویت محصول تشکیل شده باشد، پشتیبانی نماید.

سند خلاصه مشخصات محصول باید مشخص نماید که چه مواقعی بررسی وضعیت فسخ انجام می‌گیرد. انتظار می‌رود که وقتی از گواهی‌نامه در احرازهویت استفاده می‌گردد، وضعیت فسخ نیز بررسی گردد. بررسی وضعیت یک گواهی‌نامه X509 فقط وقتی که روی دستگاه بارگذاری می‌شود، کافی نمی‌باشد.

اگر محصول از هیچ کدام از موارد مطرح شده در قوانین extendedKeyUsage پشتیبانی نمی‌کند، این وضعیت باید در سند خلاصه مشخصات محصول شرح داده شود.

۶۳	**الزامات پروتکل X509 (۲) / تبادل داده کاربردی داخل محصول**

[۱] Self-signed root certificate

محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد. **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.

۶,۳ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام
۶۴	**حفاظت از انتقال داخلی داده‌های اساسی محصول**
محصول باید از آشکارسازی داده توابع امنیتی محصول حفاظت کند و دستکاری/اصلاح در داده را وقتی که بین قسمت‌های مختلف محصول از طریق [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] مخابره می‌شود، تشخیص دهد. **نکته کاربردی:** این الزام فقط برای محصولات توزیع‌شده قابل اعمال می‌باشد و اطمینان پیدا می‌کند که تمام ارتباطات میان مؤلفه‌های محصول از طریق یک کانال ارتباطی رمزگذاری شده، حفاظت می‌گیرد. داده‌ای که از طریق این کانال ارتباطی مورداعتماد عبور داده می‌شود، بوسیله پروتکل انتخاب شده در عبارت "انتخاب " این الزام، رمزگذاری می‌گردد. نویسنده هدف امنیتی باید کانال‌ها و پروتکل‌های مورد استفاده توسط هر کدام از مؤلفه‌های یک ارتباط را مشخص نماید. این کانال ممکن است به عنوان کانال ثبت‌نام (داخل فرآیند ثبت‌نام در الزام FCO_CPC_EXT.1.2، توضیح داده شده است) استفاده گردد.	
۶۵	**مسیر امن ۱/ پیوند زدن**

محصول مورد ارزیابی باید مسیر ارتباطی میان خود و یک مؤلفه پیوندی[۱] که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم نماید و [انتخاب: نقطه‌پایانی توابع امنیتی محصول، هر دو مورد (مؤلفه پیوندی و نقطه‌پایانی توابع امنیتی محصول)] را به صورت مطمئن شناسایی کرده و داده‌های تبادلی را در برابر تغییر [انتخاب: و افشاء، هیچ مورد دیگری] محافظت نماید.	
۶۶	**مسیر امن ۲/ پیوند زدن**
محصول مورد ارزیابی باید به [انتخاب: توابع امنیتی محصول، مؤلفه پیوندی] اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
۶۷	**مسیر امن ۳/ پیوند زدن**
محصول مورد ارزیابی باید برای پیوند مؤلفه‌ها به توابع امنیتی تحت شرایط/قیدهای محیط عملیاتی تعریف شده که در راهنمای عملیاتی مورد اشاره قرار گرفته است، استفاده از کانال امن را الزامی کند. **نکته کاربردی:** این الزام (FTP_TRP.1/Join)، یکی از انواع کانال را که در اولین "انتخاب " در الزام FCO_CPC_EXT.1.2 بیان شده است، پیاده‌سازی می‌کند. عبارت "مؤلفه پیوندی " در الزام «مسیر امن ۱/پیوند زدن» در واقع یک موجودیت IT می‌باشد که تلاش می‌کند از طریق فرآیند ثبت‌نام، به محصول توزیع‌شده بپیوندد. هدف از الزام این است که برای مؤلفه‌ها امکان ارتباط با یک شیوه امن در زمان تشکیل توابع امنیتی فراهم گردد. دومین "انتخاب " در الزام «مسیر امن ۱/پیوند زدن» در واقع بیان می‌کند که در برخی موارد، کانال ممکن است محرمانگی (حفاظت از آشکارسازی داده) را فراهم نکند. بنابراین، نویسنده هدف امنیتی باید در خلاصه مشخصات محصول بیان کند که در این مورد آیا محصول محرمانگی را روی محیط الزام می‌کند (از طریق "شرایط/قیدهای محیط عملیاتی تعریف شده " در همین الزام) یا اینکه داده تبادل شده نیاز به محرمانگی ندارد. توجه شود که وقتی از FTP_TRP.1/Join برای کانال ثبت‌نام استفاده شود، سپس این کانال نمی‌تواند به عنوان یک کانال عادی ارتباطات میان مؤلفه‌ای مورد استفاده قرار گیرد. باید از FPT_ITT.1 یا FTP_ITC.1 استفاده شود.	

۶,۴ کلاس ارتباطات

شماره الزام	نام الزام
۶۸	**تعریف کانال ثبت‌نام مؤلفه ۱**
محصول باید سرپرست امنیتی را ملزم کند که قبل از اتفاق افتادن ارتباط میان هر جفت مؤلفه از محصول، برای آن‌ها یک ارتباط فعال نماید.	

[۱] Joining

۶۹	تعریف کانال ثبت‌نام مؤلفه ۲
محصول باید یک فرآیند ثبت‌نام را پیاده‌سازی کند که در آن مؤلفه‌ها یک کانال ارتباطات را منتشر و استفاده کنند که این کانال حداقل برای داده توابع امنیتی محصول از [انتخاب: • یک کانال که الزامات کانال امن را مطابق [انتخاب: FTP_ITC.1، FPT_ITT.1] رعایت کند. • یک کانال که الزامات کانال ثبت‌نام امن را مطابق FTP_TRP.1/Join رعایت کند. • هیچ کانالی] استفاده نماید.	
۷۰	تعریف کانال ثبت‌نام مؤلفه ۳
محصول باید یک سرپرست امنیتی را فعال نماید که بتواند کانال ارتباطات میان هر جفت مؤلفه از محصول را غیرفعال نماید. **نکته کاربردی:** این الزام (FCO_CPC_EXT.1) فقط وقتی که محصول توزیع‌شده باشد و در نتیجه چند مؤلفه داشته باشد که نیاز به ارتباط از طریق کانال داخلی داشته باشند، قابل اعمال می‌باشد. انتخاب کانال در الزام «تعریف کانال ثبت‌نام مؤلفه ۲» اساساً یک انتخاب است بین اینکه از یک کانال امن معمولی که معادل است با الف) کانالی که برای ارتباط با موجودیت‌های خارجی (FTP_ITC.1) یا مؤلفه‌های محصول (FPT_ITT.1) استفاده می‌شود، یا ب) کانالی که برای ثبت‌نام بکار می‌رود (FTP_TRP.1/Join)، استفاده شود. در صورتی که محصول بدلیل امکان اقدامات پیکربندی قابل انجام توسط سرپرست محصول، نیاز به کانال ثبت‌نام نداشته باشد، آنگاه گزینه "هیچ کانالی " برای انتخاب الزام «تعریف کانال ثبت‌نام مؤلفه ۲» برگزیده می‌شود. اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه سند خلاصه مشخصات محصول باید تکرارهایی از الزام را که برای مشخص کردن استفاده محصول لازم است، تشریح نماید. درصورتی که FTP_TRP.1/Join انتخاب گردد، سند خلاصه مشخصات محصول (در صورت امکان با کمک سند راهنمای عملیاتی) باید جزییات کانال و مکانیزم‌هایی را که استفاده می‌کند تشریح نماید. اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه در سند هدف امنیتی باید کانال ثبت‌نام به عنوان یکی از تکرارهای الزام FPT_ITT.1 یا FTP_ITC.1 با یک نام مشخص (مثال؛ FPT_ITT.1/Join)، در قالب نکته کاربردی به الزام «تعریف کانال ثبت‌نام مؤلفه ۱» اضافه و اجرا گردد.	

۶,۵ کلاس دیواره آتش (FFW)

شماره الزام	نام الزام
۷۱	فیلترینگ حالتمند پروتکل‌های پویا

محصول مورد ارزیابی باید بتواند به صورت پویا قوانینی را تعریف کرده و 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 می کنند ایجاد کند.

نکته کاربردی:

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 راه اندازی 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 داینامیکی 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.

[۱] rulset

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 پروتکهای 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.

۷ پیوست دو: 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 رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب می‌باشد. همانطور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

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

ردیف	الزام	رویدادهای ممیزی	لیست سوابق ممیزی اضافی
.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
.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 تایید 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 بروزرسانی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)
.۲۲	FMT_MOF.1/AutoUpdate	فعالسازی یا غیرفعالسازی بررسی خودکار برای بروزرسانی‌ها یا بروزرسانی‌های 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:

رویداد ممیزی «الزامات پروتکل X509(۱) و (۲)/ ابطال» در صورتی رخ می‌دهد که محصول مورد ارزیابی نتواند از موارد زیر اطمینان حاصل نماید و گواهی‌نامه‌ها را تأیید کند:

- وجود افزونه basicConstraints و تأیید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تأیید امضای دیجیتال CA سلسله مراتبی مورداعتماد
- خواندن و دسترسی به CRL یا دسترسی به سرور OCSP

اگر هر یک از این موارد وجود نداشته باشند، باید یک رویداد ممیزی با نتیجه شکست را در سوابق ممیزی ثبت نمود.

۷,۱ تولید داده های ممیزی امنیت

شماره الزام	نام الزام	
۷۲	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 زیر مجموعه رویدادهای مربوط به ممیزی امنیت است که می توانند روی مؤلفه هدف ارزیابی اتفاق بیفتند.		
۷۳	**محل ذخیره‌سازی داده‌های ممیزی حفاظت شده**	FAU_STG_EXT.3.1
توابع امنیتی هدف ارزیابی از هر مؤلفه هدف ارزیابی که داده های ممیزی امنیتی را بصورت محلی ذخیره می کند، وقتی فضای ذخیره محلی داده های ممیزی پر باشد، باید اقدامات زیر را انجام دهد: [اختصاص: جدول مولفه ها و برای هر مؤلفه عملکرد آن مطابق موارد زیر انتخاب شده است: [انتخاب: داده های ممیزی جدید را دور بیندازد، سوابق ممیزی قبلی را طبق قانون زیر رونویسی کند: [اختصاص: قانون برای رونویسی سوابق ممیزی قبلی] [اختصاص: سایر اقدامات]]].		
۷۴	محل ذخیره سازی داده ممیزی ۴	FAU_STG_EXT.4.1
هر مؤلفه هدف ارزیابی که داده های ممیزی امنیتی را به صورت محلی ذخیره نمی کند، می تواند داده های ممیزی امنیتی را بصورت محلی بافر کند تا زمانی که به یک مؤلفه دیگر هدف ارزیابی که آن را ذخیره یا انتقال می دهد، انتقال داده شود. [انتخاب: FPT_ITT.1، FPT_ITC.1].		

۷,۲ الزامات پروتکل DTLS Client

شماره الزام	نام الزام

۷۵	الزامات پروتکل DTLS Client (۱)

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

- [انتخاب:
- TLS_RSA_WITH_AES_128_CBC_SHAمطابق 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_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_SHA256مطابق 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 با5289 RFC
- 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_128_CBC_SHA384مطابق با RFC 5289

- [ ].

نکته کاربردی:

مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده تست شوند، توسط این الزام محدود شده‌اند.

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط تست، استفاده گردند، ضروری می‌باشد. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نمی‌باشد ولی در صورت ادعای انطباق با RFC 6347، الزامی است.

در نسخه‌های آتی این پروفایل حفاظتی، DTLS v1.2 برای همه محصولات الزامی می‌گردد.

۷۶	**الزامات پروتکل DTLS Client (۲)**

محصول باید مطابقت شناسه[۱] ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.

نکته کاربردی:

قوانین مربوط به تأیید شناسه در بخش ۶ از RFC 6125 توضیح داده شده‌اند. شناسه مرجع توسط سرپرست (مثلاً واردکردن یک URL در مرورگر وب یا کلیک کردن روی یک لینک)، توسط پیکربندی (مثلاً پیکربندی نام یک سرور ایمیل یا سرور احرازهویت) یا توسط یک برنامه کاربردی (مثلاً یک پارامتر از یک API) بر اساس سرویس برنامه کاربردی، تعیین می‌شود. کلاینت بر مبنای دامنه منبع و نوع سرویس برنامه کاربردی (مثلاً؛ HTTP، SIP، LDAP) مربوط به یک شناسه مرجع منحصربه‌فرد، همه شناسه‌های مرجع قابل‌قبول؛ نظیر یک Common Name برای قسمتName Subject از گواهی‌نامه و نام (حساس به بزرگ و کوچک بودن حروف) DNS، URI و سرویس برای قسمت Subject Alternative Name را منتشر می‌نماید. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور DTLS مقایسه می‌کند.

روش ترجیحی برای تایید شناسه، Subject Alternative Name می‌باشد که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تایید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه[۲]، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.

۷۷	**الزامات پروتکل DTLS Client (۳)**

محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].

[۱] Identifier

[۲] Background

نکته کاربردی: اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود. اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.

۷۸	**الزامات پروتکل DTLS Client (۴)**
محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1، ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.	

نکته کاربردی:

اگر در الزام «الزامات پروتکل DTLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل DTLS Client (۱)» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت "Supported Elliptic Curves Extension را ارائه نکند " باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احرازهویت و توافق کلید را به منحنی‌های NISTاز الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۷,۳ الزامات پروتکل DTLS Client/ احراز هویت

۷۹	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.		
۸۰	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 بی سر و صدا دور بیاندازد.		
۸۱	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 آن قدر قدیمی باشند که متناسب پنجره لغزان نباشند.

شناسایی کرده و بی‌صدا از بین ببرد.

۷,۴ الزامات پروتکل DTLS Server

۸۲	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_SHAمطابق 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_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_128_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 را که پشتیبانی می‌شوند 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 مجددا مورد بررسی قرار می‌گیرند.

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

۸۳	الزامات پروتکل DTLS Server (۲)	

توابع امنیتی هدف ارزیابی باید اتصال کلاینت‌هایی که درخواست [هیچ] 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.

۸۴	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3

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

نکته کاربردی:

فرآیند تایید 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، تایید 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 تایید کند، کلاینت از آدرس IP جعلی استفاده نمی‌کند.		
۸۵	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، 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.		
۸۶	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 می‌باشد. 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 تایید نشود، باید نشست خاتمه یابد یا باید سوابق بدون پاسخ رها شوند.		
۸۷	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 قبلا دریافت شده ○ سوابق DTLS انقدر قدیمی باشند که متناسب پنجره لغزان نباشند. **نکته کاربردی:**		

[۱] cookie

[۲] Silently discard the record

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، دریافت کننده سوابق حاوی دنباله شماره‌ای که در پنجره دریافت لغزان قرار دارد را تایید می‌کند و دنباله شماره هر سوابق دریافت شده دیگر را در طول نشست تکرار نمی‌کند. "Silently Discard" به این معنی است که هدف ارزیابی بسته‌ها را بدون پاسخ دور بریزد.		
۸۸	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
توابع امنیتی هدف ارزیابی باید از [انتخاب: هیچ از سرگیری جلسه یا بلیت های جلسه، از سرگیری نشست بر مبنای session ID بر اساس RFC 4346(TLS1.1) یا RFC5246(TLS1.2)، از سرگیری نشست بر مبنای بلیت های نشست با توجه به RFC 5077] پشتیبانی کند.		

۷,۵ الزامات پروتکل DTLS Server /احرازهویت دوطرفه

۸۹	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.		
۹۰	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 مکانیزم لغو سرپرستی را اجرا نکند. – در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تایید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
۹۱	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.		

[۱] Distinguished name
[۲] Subject Alternative Name

۷,۶ الزامات پروتکل HTTPS

شماره الزام	نام الزام	
۹۲	**الزامات پروتکل HTTPS (۱)**	FCS_HTTPS_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را اجرا 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.		
۹۳	**الزامات پروتکل HTTPS (۲)**	FCS_HTTPS_EXT.1.2
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.		
۹۴	**الزامات پروتکل HTTPS (۳)**	FCS_HTTPS_EXT.1.3
درصورتی‌که گواهی‌نامه همتا[۱] ارائه 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، [اختصاص: اقدام دیگر]].		

۷,۷ الزامات پروتکل IPsec

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 محصول دیواره آتش باید این قابلیت را داشته باشد که از ترافیک حساس منتقل‌شده حفاظت نماید (مانند ترافیک سرپرست محصول، ترافیک احرازهویت، ترافیک ممیزی و موارد دیگری از این دست). یکی از راه‌های ایجاد کانال ارتباطی بین محصول دیواره آتش و یک موجودیت IT خارجی، به گونه‌ای که این ارتباط را بتوان از هر دو طرف احرازهویت کرد، استفاده از IPsec است. IPsec یک پروتکل همتا به همتا است و بنابراین نیازی به تفکیک الزامات کلاینت و سرور وجود ندارد.

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

[۱] Peer certificate

در توابع امنیتی هدف ارزیابی باید معماری IPsec را بر اساس آن چه در RFC 4301 مشخص شده است، پیاده‌سازی شود. **نکته کاربردی:** بر اساس RFC 4301 برای پیاده سازی 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. صرف نظر 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.		
۹۶	**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.		
۹۷	**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.		
۹۸	**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. اکر 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 Ipsecاز یک نسخه کوتاه توابع HMAC مبتنی بر SHA موجود در انتخاب‌ها، استفاده کند. در صورت استفاده از خروجی کوتاه، باید در TSS مشخص شود.		
۹۹	**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 که 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 که 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 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.		
۱۰۰	**الزامات پروتکل IPSEC (۶)**	FCS_IPSEC_EXT.1.6
توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که برای رمزگذاری پی‌آیند[۳] 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:**		

[۱] exchanges
[۲] NAT traversal
[۳] Payload

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.		
۱۰۱	**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.

[

پیکر بندی 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.

[

پیکر بندی 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 ذکر شده‌اند). محدودیت های Hardcoded این الزام را برآورده نمی کند. به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۱۰۲	**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 ذکر شده‌اند). محدودیت های Hardcoded این الزام را برآورده نمی کند. به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.	
۱۰۳	**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.1مشخص 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 از NIST در Curve P-384) پشتیبانی می‌شود، با توجه به جدول ۲، تعداد بیت‌های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است.		
۱۰۴	**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 (همان طور 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.

۱۰۵	**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: ۱٤ (2048-bit MODP)، ۱٥ (3072-bit MODP)، ۱٦ (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)، ۲٤ (2048-bit MODP به همراه 256-bit POS)] با توجه به RFC 5114

] را پشتیبانی می‌کنند.

۱۰۶	**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.		
۱۰۷	**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 شده‌است. نویسنده هدف امنیتی همچنین اطمینان حاصل می‌کند که الزمات FCS الگوریتم‌های مورد استفاده به منظور پشتیبانی از آن روش‌ها را لیست کرده است (قابلیت‌های تولید کلید، اگر فراهم شده‌است). 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 پشتیبانی‌شده ها در TSS شرح داده خواهدشد).		
۱۰۸	**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)[۱]، SAN: کاربر FQDN، CN: آدرس IP، CN: نام کامل واجد شرایط دامنه (FQDN) نام مشخص‌شده[۲] (DN)] و [انتخاب: هیچ نوع شناسه مرجع دیگری، [اختصاص: سایر انواع شناسه مرجع پشتیبانی شده]] باشد، برقرار سازد. **نکته کاربردی:**		

[۱] Fully Qualified Domain Name
[۲] Distinguished name

زمانی که از گواهینامه‌های RSAیا ECDSAبرای احرازهویت همتا استفاده شود، شناسه و گواهینامه‌های ارائه شده به شکل DN، آدرس IP، FQDN یا FQDN کاربر می باشند. 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 تایید است. تایید با استفاده از نام عمومی برای هدف پس‌سازگاری[1] 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.

۷,۸ الزامات پروتکل NTP

شماره الزام	نام الزام	
۱۰۹	**الزامات پروتکل NTP (۱)**	FCS_NTP_EXT.1.1
توابع امنیتی هدف ارزیابی باید تنها از نسخه‌های NTP زیر استفاده کند: [انتخاب: NTP v3 ((RFC 1305)، NTP v4 (RFC 5905)		
۱۱۰	**الزامات پروتکل NTP (۲)**	FCS_NTP_EXT.1.2
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] بروزرسانی کند.		
۱۱۱	**الزامات پروتکل NTP (۳)**	FCS_NTP_EXT.1.3
توابع امنیتی هدف ارزیابی نباید مهر زمانی NTP را از آدرس‌های Broadcast و/یا Multicast بروزرسانی کند.		

[1] backwards compatibility

۱۱۲	الزامات پروتکل NTP (۴)	FCS_NTP_EXT.1.4
توابع امنیتی هدف ارزیابی باید پیکربندی حداقل سه منابع زمانی NTP را پشتیبانی کند. **نکته کاربردی:** هدف ارزیابی باید از پیکربندی حداقل ۳ منبع زمانی پشتیبانی کند، اگر چه الزامی نیست هدف ارزریابی پیکربندی شده، همیشه از این حداقل ۳ منبع زمانی استفاده کند.		

۷,۹ الزامات پروتکل SSH Client

شماره الزام	نام الزام	
۱۱۳	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، 8332،6668] 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 الگورتیم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجرا شده‌ای 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).		
۱۱۴	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 که در RFC4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر کلمه عبور، هیچ روش دیگری].		
۱۱۵	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3

همان طور 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 درنظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.		
۱۱۶	**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 و AEAD_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.		
۱۱۷	**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 [ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-256, rsa-sha2-512, x509v3-ssh-rsa, 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-ssh-rsa ، x509v3-ecdsa-sha2-nistp384 یا x509v3-rsa2048-sha256 - انتخاب شده باشند، باید لیستی از گواهینامه‌های معتبر مجاز از FCS_SSHC_EXT.1.9 انتخاب شوند و SFRهای 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.		
۱۱۸	**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:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همانطور که در RFC 5647شرح 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.		
۱۱۹	**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-nistp256] وانتخاب: 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.		
۱۲۰	**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 قابل قبول 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.		

۱۲۱	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.		

۷,۱۰ الزامات پروتکل SSH Server

شماره الزام	نام الزام	
۱۲۲	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 الگورتیم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجرا شده‌ای که با عنوان "REQUIRED" مشخص شده‌اند ولی در عناصر بعد از این بخش لیست نشده‌اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند.		
۱۲۳	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.		
۱۲۴	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.	
۱۲۵	**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 و AEAD_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.	
۱۲۶	**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، SFRهای FIA_X509_EXTدر 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	
۱۲۷	**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 5647شرح 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.		
۱۲۸	**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.		
۱۲۹	**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 قابل قبول 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.		

۷,۱۱ الزامات پروتکل TLS Client

شماره الزام	نام الزام	
۱۳۰	**الزامات پروتکلTLS 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_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_SHA256مطابق 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_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_128_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 5246 وجود داشته باشد، الزامی است.

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

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

۱۳۱	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.2

توابع امنیتی هدف ارزیابی باید تایید 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 مربوط به تأیید 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 تایید این است که Subject Alternative Name از نام DNS، نام URL، یا نام سرویس استفاده کند. برای هدف پس‌سازگاری[۱] تایید 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 بدست می‌آیند.		
۱۳۲	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 مکانیزم لغو سرپرستی پیاده سازی نشود. – در صورت شکست توابع امنیتی هدف ارزیابی، به مجوز مدیریت برای ایجاد ارتباط به [انتخاب: مطابقت با شناسه مرجع، تأیید مسیر گواهی، تأیید تاریخ انقضا، تعیین وضعیت لغو] از گواهی سرور ارائه شده نیاز دارید.] **نکته کاربردی:** اگر TLS در FTP_ITC یا FTP_TRP.1/Adminانتخاب شده باشد، اعتبار توسط تایید شناسه، مسیر گواهینامه، تاریخ انقضاء و وضعیت لغو مطابق با RFC 5280، تعیین می‌شود. اعتبار گواهینامه بر اساس آزمون اجرا شده برای FIA_X509_EXT.1/Rev ارزیابی می‌شود. اگر TLS در FPT_ITT انتخاب شده باشد، اعتبار گواهینامه بر اساس آزمون اجرا شده برای FIA_X509_EXT.1/ITT ارزیابی می‌شود.		
۱۳۳	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.4

[۱] backwards compatibility

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.1.1مجموعه‌های 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 منحنی های 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 می‌کنند، الزامی است.

۷,۱۲ الزامات پروتکل TLS Client/ احرازهویت

شماره الزام	نام الزام	
۱۳۴	**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.		

۷,۱۳ الزامات پروتکل TLS Server

شماره الزام	نام الزام	
۱۳۵	**الزامات پروتکلTLS 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_SHAمطابق 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_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 مجددا مورد بررسی قرار می‌گیرند.

در نسخه آینده این cPP، نسخه TLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.		
۱۳۶	**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 1.0رد 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 هیچ کدام توسط نویسنده سند هدف امنیتی قابل حذف است.		
۱۳۷	**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] 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.1تنظیمات پارامترهای پذیرش کلید برای برقراری قدرت امنیتی ارتباط TLS، الزامی می‌کند.		
۱۳۸	**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 براساس شناسه‌های نشست با توجه به RFC4346(TLS1.1) یا RFC 5246(TLS1.2)، از سرگیری نشست مبتنی بر بلیت های با توجه به RFC 5077]پشتیبانی کنند.		

۷,۱۴ الزامات پروتکل TLS Server/ احرازهویت دو طرفه

شماره الزام	نام الزام	
۱۳۹	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱**	
توابع امنیتی هدف ارزیابی باید در ارتباط TLS با احرازهویت دوطرفه TLS کلاینت‌ها، از گواهینامه های X509v3 استفاده کند.		
۱۴۰	**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 مکانیزم لغو سرپرستی را اجرا نکند. – در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تایید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
۱۴۱	**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.		

۷,۱۵ الزامات شناسایی و احرازهویت

شماره الزام	نام الزام	
۱۴۲	**اعتبارسنجی گواهینامه X509 (۱)**	FIA_X509_EXT.1.1/Rev
توابع امنیتی مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند: • تأیید گواهی‌نامه RFC 5280 و تأیید 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 تأیید 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 تأیید کند • توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید 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.		
۱۴۳	**اعتبارسنجی گواهینامه X509 (۲)**	FIA_X509_EXT.1.2/Rev
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 تایید گواهینامه‌ها را لیست کرده است. نویسنده سند هدف امنیتی وضعیت لغوی که با استفاده از OCSP یا CRLها تایید می‌شود را اتخاب می‌کند. ممکن است پروتکل‌های کانال/مسیر امن استفاده از آن گواهینامه‌ها را الزام کند. این استفاده مستلزم آن است که قوانین extendedKeyUsage تایید 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، پشیبانی نکند؛ باید در TSS مشخص شده باشد و بخش مربوط به SFR به طور کلی عمکردهای 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 بروزرسانی‌های امن (اگر انتخاب شده باشد)، انجام شود. تایید وضعیت گواهینامه X.509 فقط زمانی که در دستگاه بارگذاری می‌شود کافی نیست. تایید 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.2در همه موارد باشد، به جز زمانی که فقط SSH در FTP_ITC.1یا 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.		
۱۴۴	**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 تأیید اعتبارسنجی، [اختصاص: سایر کاربردها]، هیچ کاربرد اضافی دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.		
۱۴۵	**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.2.1شامل IPsec، TLS، HTTPS می‌باشد؛ 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.1.5انتخاب شده باشد، باید ST حاوی SSH باشد. ممکن است گواهینامه‌ها به صورت اختیاری برای بروزرسانی‌های امن نرم‌افزار سیستم (FPT_TUD_EXT.2) و برای تایید صحت (FPT_TST_EXT.2) استفاده شوند. معمولا 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 درFIA_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.1نفی 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 تایید اعتبار گوهینامه مورد نیاز نیست و این الزام به طور قطعی رعایت می‌شود. سند هدف امنیتی باید شامل FIA_X509_EXT.2در همه موارد باشد، به جز زمانی که فقط SSH در FTP_ITC.1یا 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.2در سند هدف امنیتی باشد.		
۱۴۶	**درخواست‌های گواهینامه X509 (۱)**	FIA_X509_EXT.3.1
توابع امنیتی مورد ارزیابی باید مطابق با آنچه که 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 آن چه در FCS_CKM.1 شرح داده‌شده است، توسط هدف ارزیابی تولید می‌شود.		
۱۴۷	**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

۷,۱۶ الزامات به‌روزرسانی امن

۱۴۸	**الزامات به‌روزرسانی امن ۴**	FPT_TUD_EXT.2.1
درصورتی‌که گواهینامه امضای کد آن غیر معتبر اعلام‌شده است، توابع امنیتی هدف ارزیابی نباید یک به‌روزرسانی را نصب نماید.		
۱۴۹	**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.]		
۱۵۰	**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].		
۱۵۱	**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.		

۷,۱۷ کلاس های مدیریت امنیت

۱۵۲	**مدیریت رفتار توابع امنیتی/بروزرسانی 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 "بروزرسانی خودکار " فقط زمانی ممکن است انتخاب شود که از امضاهای دیجیتال برای اعتبار بروزرسانی امن استفاده شده باشد.		
۱۵۳	**مدیریت رفتار توابع امنیتی/بروزرسانی 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 که 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).		
۱۵۴	**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.		
۱۵۵	**مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱**	FMT_MTD.1.1/CryptoKeys
توابع امنیتی هدف ارزیابی باید توانایی مدیریت کلید های رمزنگاری را به سرپرست امنیتی محدود کند.		

۸ مراجع

- **collaborative Protection Profile for Network Devices V2.2e 23-March-2020**
- **PP-Module for Stateful Traffic Filter Firewalls Version 1.4 + Errata 20200625 25-June-2020**