به نام خدا

پروفایل حفاظتی دیواره آتش

خرداد ۹۵

نسخه ۲,۰

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 که در این سند برای برآورده نمودن الزامات ارائه‌شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز مدیریت راهبردی افتا با مشارکت سازمان فناوری اطلاعات ایران این سند را در راستای این اهداف تهیه نموده است. این سند معرفی کننده‌ی الزامات کارکرد امنیتی برای دیواره آتش است؛ تا تولیدکنندگان محصولات دیواره آتش بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ نموده 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 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

- کلاس دیواره آتش

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

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

فهرست

۱ شرح محصول دیواره آتش ۹
۱,۱ موارد کاربرد محصول ۱۰
۲ تعریف مسائل امنیتی..... ۱۱
۱,۲ تهدیدات ۱۱
۱,۱,۲ ارتباطات با فایروال..... ۱۱
۲,۱,۲ به‌روزرسانی‌های معتبر..... ۱۳
۳,۱,۲ فعالیت ممیزی‌شده ۱۴
۴,۱,۲ داده‌ها و اطلاعات محرمانه فایروال و راهبر ۱۵
۵,۱,۲ از کار افتادن مؤلفه فایروال ۱۶
۶,۱,۲ افشای غیرمجاز اطلاعات..... ۱۶
۷,۱,۲ دسترسی غیرمجاز به خدمات ۱۷
۸,۱,۲ سوءاستفاده از خدمات..... ۱۸
۹,۱,۲ ترافیک مخرب..... ۱۹
۲,۲ فرضیات ۲۰

۱,۲,۲ حفاظت فیزیکی ۲۰
۲,۲,۲ کارکرد محدود ۲۰
۳,۲,۲ راهبر مورد اعتماد ۲۱
۴,۲,۲ به‌روزرسانی منظم ۲۱
۵,۲,۲ امنیت اطلاعات محرمانه راهبر ۲۱
۳,۲ خط‌مشی امنیتی سازمان ۲۱
۱,۳,۲ بنر دسترسی ۲۲
۳ اهداف امنیتی ۲۲
۱,۳ اهداف امنیتی برای محیط عملیاتی ۲۲
۱,۱,۳ امنیت فیزیکی ۲۲
۲,۱,۳ عدم وجود قابلیت رایانش همه‌منظوره ۲۲
۳,۱,۳ راهبر مورد اعتماد ۲۲
۴,۱,۳ به‌روزرسانی ۲۲
۵,۱,۳ امنیت اطلاعات محرمانه راهبر ۲۳
۴ الزامات کارکرد امنیتی ۲۳
۱,۴ کلاس ممیزی امنیت ۳۱

۲,۴ کلاس پشتیبانی رمزنگاری (FCS) ۳۶
۳,۴ کلاس محافظت از داده کاربری ۴۳
۴,۴ کلاس شناسایی و احراز هویت ۴۴
۵,۴ کلاس مدیریت امنیت ۵۰
۶,۴ کلاس حفاظت از محصول مورد ارزیابی ۵۳
۱,۶,۴ آزمون محصول مورد ارزیابی ۵۵
۲,۶,۴ به‌روزرسانی امن ۵۶
۷,۴ کلاس محافظت از داده کاربری ۶۰
۸,۴ کلاس دسترسی به محصول ۶۰
۹,۴ کلاس کانال‌ها/مسیرهای مورد اعتماد ۶۲
۱۰,۴ کلاس دیواره آتش (FFW) ۶۵
۵ الزامات تضمین امنیت ۷۲
۱,۵ کلاس توسعه ۷۳
۱,۱,۵ مشخصات کارکردی ۷۳
۲,۵ کلاس راهنمای کاربر ۷۶
۱,۲,۵ راهنمای کاربردی ۷۷

۲,۲,۵ راهنمای آمادهسازی..... ۸۰
۳,۵ کلاس آزمون ۸۲
۱,۳,۵ آزمون مستقل ۸۲
۴,۵ کلاس آسیبپذیری ۸۴
۱,۴,۵ تحلیل آسیبپذیری..... ۸۴
۵,۵ کلاس پشتیبانی از چرخه حیات ۸۶
۱,۵,۵ قابلیتهای پیکربندی..... ۸۶
۲,۵,۵ حوزه پیکربندی ۸۸
۶ پیوست یک: الزامات اختیاری ۸۹
۱,۶ کلاس ممیزی امنیت..... ۹۰
۲،۴ کلاس مدیریت امنیت..... ۹۳
۲,۶ کلاس حفاظت از محصول مورد ارزیابی..... ۹۶
۳,۶ کلاس دیواره آتش (FFW) ۹۷
۷ پیوست دو: الزامات مبتنی بر انتخاب..... ۹۸
۱,۷ الزامات پروتکل HTTPS..... ۱۰۰
۲,۷ الزامات پروتکل IPsec..... ۱۰۱

۳,۷ الزامات پروتکل SSH Client ۱۱۰
۴,۷ الزامات پروتکلSSH Server ۱۱۳
۵,۷ الزامات پروتکلTLS Client/ احراز هویت ۱۱۵
۶,۷ الزامات پروتکلTLS Client همراه با احراز هویت دوطرفه..... ۱۱۸
۷,۷ الزامات پروتکلTLS Server..... ۱۲۲
۸,۷ الزامات پروتکلTLS Server همراه با احراز هویت دو طرفه ۱۲۴
۹,۷ الزامات خودآزمایی محصول مورد ارزیابی ۱۲۸
۱۰,۷ الزامات به‌روزرسانی امن ۱۲۸

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 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] Extended pavkage(EP)

۱,۱ موارد کاربرد محصول

این بسته توسعه یافته، به طور خاص تجهیزات شبکه‌ای که فیلترینگ حالتمند ترافیک لایه ۳ و ۴ شبکه را انجام می‌دهند را آدرس‌دهی می‌کند. یک دیواره آتش فیلترینگ 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، ACK ها 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 می‌گیرد.

از این رو این بسته توسعه یافته بر روی پروفایل حفاظتی مربوط به تجهیزات شبکه‌ایجاد 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 شبکه‌های 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

۱,۲ تهدیدات

در بخش‌های بعد، تهدیدات پیش‌روی فایروال فیلترینگ ترافیک حالتمند بر اساس کارکردهای دستگاه دسته‌بندی شده‌اند.

۱,۱,۲ ارتباطات با فایروال

فایروال‌ها با سایر دستگاه‌های شبکه و همچنین با سایر موجودیت‌های شبکه ارتباط برقرار می‌کنند. نقطه پایانی این ارتباطات ممکن است از لحاظ جغرافیایی یا منطقی راه دور باشد و از سیستم‌های مختلف دیگری نیز بگذرد. ممکن است سیستم‌های میانی غیرقابل اعتماد باشند و در نتیجه، امکان برقراری ارتباطات غیرمجاز با فایروال یا سوءاستفاده از ارتباطات مجاز توسط مهاجمان وجود داشته باشد. فایروال باید قدرت امنیتی لازم را داشته باشد و بتواند از ترافیک مهم شبکه مانند اطلاعات مدیریتی، احراز هویتی، ممیزی و غیره محافظت نماید. ارتباطات برقرارشده با فایروال به دو دسته تقسیم می‌شوند: ارتباطات مجاز و ارتباطات غیرمجاز.

ارتباطات مجاز شامل ترافیک معمول شبکه است که بر اساس خط‌مشی‌ها، اجازه ارسال آن‌ها به فایروال و دریافت آن‌ها از آن وجود دارد. به عنوان مثال، می‌توان به ترافیک حساس شبکه از جمله ارتباطات فایروال با سرور احراز هویت یا سرور گزارش‌گیری ممیزی اشاره کرد که نیازمند یک کانال امن برای حفاظت از ارتباطات است. فایروال باید تضمین کند که تمام ارتباطات برقرارشده مجاز هستند و همچنین بتواند کانال امنی را برای ترافیک حساس شبکه‌ایجاد نماید. تمامی ارتباطات دیگر، غیرمجاز به شمار می‌آیند.

تهدید اصلی پیش روی ارتباطات فایروال، موجودیت‌های خارجی غیرمجازی هستند که تلاش می‌کنند تا به ترافیک حساس شبکه دسترسی پیدا کنند، آن را تغییر دهند، یا به هر طریقی آن را افشا نمایند. در صورتی که از الگوریتم‌های رمزنگاری نامناسب استفاده شده باشد یا اصولاً این الگوریتم‌ها به کار گرفته نشده باشند، عامل تهدید می‌تواند با کمترین تلاش داده‌های حساس را بخواند و آن‌ها را دست‌کاری یا کنترل نماید. پروتکل‌های تونل‌زنی غیراستاندارد نه تنها قابلیت همکاری فایروال را محدود می‌کنند، بلکه ضمانت و اعتماد کافی را نیز فراهم نمی‌آورند.

دسترسی راهبری غیرمجاز

ممکن است عوامل تهدیدکننده‌ای تلاش کنند تا برای دسترسی راهبری به فایروال، خود را به عنوان راهبر به فایروال معرفی کنند، یک نشست راهبری را بازپخش کنند (به طور کامل یا بخشی از آن)، یا حملات مردی در میانه را ترتیب دهند. بدین ترتیب، عوامل تهدید قادر خواهند بود به نشست راهبری یا نشست‌های بین فایروال و دستگاه‌های شبکه دسترسی پیدا کنند. دسترسی راهبری موفقیت‌آمیز عوامل تهدید، به آن‌ها امکان می‌دهد تا اقدامات خرابکارانه‌ای را انجام دهند و کارکرد امنیتی فایروال و شبکه را به خطر اندازند.

رمزنگاری ضعیف

ممکن است عوامل تهدید از الگوریتم‌های رمزنگاری ضعیف استفاده کنند یا حملات رمزنگاری گسترده‌ای را علیه فضای کلید[۱] انجام دهند. در صورتی که الگوریتم‌های رمزگذاری، حالت‌ها و اندازه کلیدها به درستی انتخاب نشده باشند، مهاجمان می‌توانند الگوریتم‌ها را به خطر اندازند یا حملات گسترده‌ای را علیه فضای کلید ترتیب دهند. بدین ترتیب، مهاجمان قادر خواهند بود با دسترسی غیرمجاز، با کمترین تلاش داده‌ها را بخوانند، دست‌کاری کنند، یا کنترل نمایند.

کانال‌های ارتباطی غیرقابل اعتماد

ممکن است عوامل تهدید فایروال‌هایی را هدف قرار دهند که از پروتکل‌های تونل‌زنی امن استاندارد استفاده نمی‌کنند و در نتیجه نمی‌توانند از ترافیک حساس شبکه محافظت نمایند. مهاجمان می‌توانند از پروتکل‌های دارای طراحی نامناسب یا روش‌های نادرست مدیریت کلید سوءاستفاده کنند و حملات مردی در میانه، بازپخش و سایر حملات خود را انجام دهند. حملات موفق منجر به از دست رفتن محرمانگی و یکپارچگی ترافیک حساس شبکه می‌شوند و می‌توانند فایروال را نیز به خطر اندازند.

---

[۱] key space

نقاط پایانی با احراز هویت ضعیف

ممکن است عوامل تهدید از پروتکل‌های امنی سوءاستفاده کنند که سازوکار احراز هویت نقاط پایانی در آن‌ها ضعیف است (مثلاً از گذرواژه‌های اشتراکی استفاده می‌کنند که قابل حدس هستند یا به متن ساده تبدیل شده‌اند). استفاده از چنین سازوکارهایی، درست مانند استفاده از پروتکل‌هایی است که طراحی نامناسبی داشته باشند. بدین ترتیب، مهاجمان می‌توانند خود را به جای راهبر به دستگاه‌های دیگر معرفی کنند، خود را در جریان شبکه قرار دهند، یا حملات مردی در میانه را ترتیب دهند. در نتیجه، ترافیک حساس شبکه در معرض خطر قرار می‌گیرد و ممکن است محرمانگی و یکپارچگی آن از بین برود. علاوه بر این، ممکن است خود فایروال نیز در معرض خطر قرار گیرد.

۲,۱,۲ به‌روزرسانی‌های معتبر

برای حصول اطمینان از این که فایروال می‌تواند کارکردهای امنیتی خود را به درستی انجام دهد، لازم است که نرم‌افزار و ثابت‌افزار آن به‌روزرسانی شوند. منبع و محتوای به‌روزرسانی باید به روش‌های رمزنگاری تأیید شوند. در غیر این صورت، یک منبع غیر معتبر می‌تواند به‌روزرسانی‌های خود را اعمال نماید و کارکرد امنیتی فایروال را در معرض خطر قرار دهد. روش‌های تأیید به‌روزرسانی‌های ثابت‌افزار و نرم‌افزار با استفاده از ابزارهای رمزنگاری عبارت‌اند از الگوهای امضای رمزنگاری که هش به‌روزرسانی‌های آن‌ها به صورت دیجیتالی امضا شده است.

نسخه‌های به‌روزنشده ثابت‌افزار و نرم‌افزار، فایروال را در معرض خطر عوامل تهدیدی قرار می‌دهند که قصد سوءاستفاده از آسیب‌پذیری‌های آن را دارند. استفاده از به‌روزرسانی‌های تأییدنشده یا به‌روزرسانی‌هایی که با استفاده از روش‌های غیر امن و ضعیف تأیید شده‌اند، باعث می‌شود که نرم‌افزارها و ثابت‌افزارهای به‌روزشده در معرض خطر عوامل تهدید قرار گیرند و توسط آن‌ها تغییر و دست‌کاری شوند.

به‌روزرسانی‌های مخرب

ممکن است عوامل تهدید تلاش کنند تا به‌روزرسانی‌های مخربی را برای نرم‌افزارها و ثابت‌افزارها ارائه کنند و بدین ترتیب، کارکرد امنیتی دستگاه را به خطر اندازند. استفاده از به‌روزرسانی‌های تأییدنشده یا به‌روزرسانی‌هایی که با استفاده از روش‌های غیر امن و ضعیف تأیید شده‌اند، باعث می‌شود که نرم‌افزارها و ثابت‌افزارهای به‌روزشده در معرض خطر عوامل تهدید قرار گیرند و توسط آن‌ها تغییر و دست‌کاری شوند.

۳,۱,۲ فعالیت ممیزی‌شده

ممیزی فعالیت‌های فایروال، ابزار ارزشمندی برای راهبران است تا وضعیت دستگاه‌ها را پایش نمایند. این روش، ابزاری است برای پاسخگویی راهبران، گزارش‌دهی فعالیت‌های مربوط به کارکرد امنیتی، بازسازی رویدادها و تحلیل مشکلات. با تحلیل فعالیت‌های دستگاه، می‌توان موارد کارکرد امنیتی نادرست دستگاه یا به خطر افتادن کارکرد امنیتی را شناسایی کرد. در صورتی که موارد کارکرد امنیتی نامناسب دستگاه ثبت و آزمون نشوند، ممکن است این موارد باز هم بدون آگاهی راهبر رخ دهند. علاوه بر این، اگر سوابق ثبت و نگهداری نشوند، بازیابی شبکه یا درک ابعاد حملات به خوبی صورت نخواهد گرفت. دغدغه‌های دیگر عبارت‌اند از حفاظت از داده‌های ممیزی ثبت‌شده درباره تغییرات یا حذف‌های غیرمجاز. این اتفاق ممکن است درون هدف ارزیابی، یا هنگامی که داده‌های ممیزی در حال انتقال به یک حافظه خارجی هستند رخ دهد.

توجه داشته باشید که بر اساس این پروفایل حفاظتی مشارکتی، فایروال داده‌های ممیزی را تغییر می‌دهد و این قابلیت را دارد که داده‌های ممیزی را به یک موجودیت شبکه مورد اعتماد (مانند یک سرور syslog) ارسال نماید.

فعالیت ردیابی‌نشده

ممکن است عوامل تهدید تلاش کنند تا بدون اطلاع راهبر به کارکرد امنیتی فایروال دسترسی پیدا کنند و آن را تغییر دهند یا دست‌کاری کنند. در این صورت، مهاجم می‌تواند دستگاه را به خطر اندازد و راهبر نیز هیچ اطلاعی در این زمینه نخواهد داشت.

۴,۱,۲ داده‌ها و اطلاعات محرمانه فایروال و راهبر

فایروال دارای داده‌ها و اطلاعات محرمانه‌ای است که باید به طور امن ذخیره شوند و تنها موجودیت‌های مجاز امکان دسترسی به آن‌ها را داشته باشند. به عنوان مثال، می‌توان به اطلاعات محرمانه احراز هویت، پیکربندی، نرم‌افزار و ثابت‌افزار فایروال برای کانال‌های امن و همچنین به اطلاعات محرمانه راهبر اشاره کرد. کلیدهای راهبر و فایروال، اطلاعات کلید، اطلاعات محرمانه احراز هویت باید در برابر دست‌کاری و افشای غیرمجاز محافظت شوند. علاوه بر این، کارکرد امنیتی فایروال باید به گونه‌ای باشد که از کاربران بخواهد تا اطلاعات محرمانه پیش‌فرض را تغییر دهند (مثلاً لازم باشد که راهبر گذرواژه پیش‌فرض خود را عوض کند).

عدم ذخیره‌سازی امن داده‌ها و اطلاعات محرمانه و مدیریت نادرست آن‌ها (مثلاً وجود اطلاعات محرمانه رمزگذاری‌نشده درون فایل‌های پیکربندی یا در دسترس بودن کلیدهای نشست کانال امن)، نه تنها به مهاجم اجازه می‌دهد که به فایروال دسترسی پیدا کند، بلکه وی را قادر می‌سازد تا از طریق تغییرات به ظاهر مجاز یا حملات مردی در میانه، امنیت شبکه را به خطر اندازد. این حملات به یک موجودیت غیرمجاز امکان می‌دهند تا با استفاده از اطلاعات محرمانه مجاز راهبر، به توابع راهبری دسترسی پیدا کند و آن‌ها را اجرا نماید. موجودیت مذکور همچنین قادر خواهد بود تا به عنوان یک نقطه پایانی مجاز، جریان ترافیک را مختل کند. این امر سبب می‌شود که شناسایی حملات و بازسازی شبکه دشوار گردد و احتمال ادامه یافتن دسترسی غیرمجاز داده‌های راهبر و فایروال وجود داشته باشد.

به خطر افتادن کارکرد امنیتی

ممکن است عوامل تهدید اطلاعات محرمانه و داده‌های فایروال را به خطر اندازند و امکان ادامه یافتن دسترسی به داده‌های فایروال و داده‌های حساس را فراهم آورند. به خطر افتادن اطلاعات محرمانه شامل این موارد است: جایگزین کردن اطلاعات محرمانه فعلی با اطلاعات محرمانه مهاجم، تغییر دادن اطلاعات محرمانه موجود، یا دسترسی به اطلاعات محرمانه فایروال یا راهبر برای استفاده توسط مهاجم.

هک شدن گذرواژه

ممکن است عوامل تهدید از ضعیف بودن گذرواژه راهبری استفاده کنند و امکان دسترسی ویژه به فایروال برای آن‌ها فراهم آید. این دسترسی ویژه مهاجم را قادر می‌سازد تا به ترافیک شبکه دست یابد و از روابط مبتنی بر اعتماد با سایر دستگاه‌های شبکه سوءاستفاده نماید.

۵,۱,۲ از کار افتادن مؤلفه فایروال

ایجاد سازوکارهای امنیتی فایروال معمولاً از سطح پایه و از مرجع اعتماد آغاز می‌شود و سپس به سازوکارهای پیچیده‌تر می‌انجامد. از کار افتادن سازوکارهای امنیتی باعث به خطر افتادن کارکرد امنیتی فایروال می‌شود. خودآزمایی فایروال در جریان راه‌اندازی اولیه و در زمان اجرا، صحت کارکرد امنیتی آن را تضمین می‌نماید.

از کار افتادن کارکرد امنیتی

ممکن است یکی از مؤلفه‌های فایروال در جریان راه‌اندازی اولیه یا در زمان اجرا از کار بیفتد. این امر باعث به خطر افتادن یا از کار افتادن کارکرد امنیتی فایروال می‌شود و آن را در معرض خطر حملات قرار می‌دهد.

۶,۱,۲ افشای غیرمجاز اطلاعات

ممکن است دستگاه‌های حاضر در یک شبکه حفاظت‌شده، در معرض خطرات ناشی از دستگاه‌های خارج از شبکه قرار گیرند که در پی انجام اقدامات غیرمجاز هستند. اگر دستگاه‌های بدخواه خارج از شبکه امکان برقراری ارتباط با دستگاه‌های حاضر در شبکه حفاظت‌شده را داشته باشند یا دستگاه‌های حاضر در شبکه بتوانند ارتباطاتی را با دستگاه‌های خارجی مذکور برقرار کنند، این امکان وجود دارد که دستگاه‌های داخلی در معرض خطر افشای غیرمجاز اطلاعات قرار گیرند.

از چشم‌انداز ورود اطلاعات، فایروال‌های فیلترینگ ترافیک حالتمند تنها دسترسی به برخی از آدرس‌ها و پورت‌های شبکه مقصد را محدود می‌کنند. این محدودیت باعث می‌شود که اسکن پورت شبکه عمومی نتواند به ماشین‌ها یا دستگاه‌های محافظت‌شده دسترسی پیدا کند و همچنین دسترسی به اطلاعات

شبکه محافظت‌شده نیز می‌تواند محدود به اطلاعاتی شود که از طریق پورت‌های پیکربندی‌شده روی گره‌های شناسایی‌شده شبکه قابل حصول هستند (مثلاً صفحات وب یک سرور وب اختصاصی سازمان). علاوه بر این، می‌توان دسترسی را تنها محدود به برخی پورت‌ها و آدرس‌های مبدأ خاص کرد، به شکلی که بتوان برخی شبکه‌ها یا گره‌های خاص را از دسترسی به یک شبکه محافظت‌شده منع نمود و بدین ترتیب، اطلاعات را بیش از پیش در برابر افشای غیرمجاز تحت محافظت قرار داد.

از چشم‌انداز خروج اطلاعات، فایروال‌های فیلترینگ ترافیک حالتمند چگونگی ارتباط گره‌های فعال روی یک شبکه حفاظت‌شده با سایر شبکه‌ها و در نتیجه چگونگی انتشار اطلاعات را محدود می‌نماید. می‌توان برخی شبکه‌های خارجی را به طور کلی مسدود کرد یا امکان خروج اطلاعات را تنها از طریق برخی پورت‌ها و/یا آدرس‌های خاص فراهم نمود. در روشی دیگر، می‌توان نقاط خروج اطلاعات از شبکه را به گونه‌ای مدیریت کرد که ارتباطات خروجی از طریق پراکسی‌ها یا فیلترهای مجاز صورت می‌گیرند. بدین ترتیب، امکان افشای غیرمجاز اطلاعات کاهش خواهد یافت.

افشای شبکه

ممکن است مهاجم تلاش کند تا «نقشه» یک شبکه فرعی را استخراج کند تا بدین ترتیب ماشین‌های روی شبکه را شناسایی کند، آدرس IP ماشین‌ها را به دست آورد و خدمات (پورت‌های) ارائه‌شده توسط این ماشین‌ها را تعیین نماید. با استفاده از این اطلاعات، مهاجم قادر خواهد بود حملاتی را علیه ماشین‌ها انجام دهد.

۷,۱,۲ دسترسی غیرمجاز به خدمات

ممکن است دستگاه‌های خارج از شبکه حفاظت‌شده تلاش کنند تا به آن دسته از خدمات شبکه دست یابند که قرار بوده اجازه دسترسی به آن‌ها تنها از درون شبکه وجود داشته باشد. به طور مشابه، ممکن است دستگاه‌های خارج از شبکه حفاظت‌شده خدماتی را ارائه کنند که دسترسی به آن‌ها از درون شبکه مجاز یا مناسب نیست.

از چشم‌انداز ورود اطلاعات، فایروال‌های فیلترینگ ترافیک حالتمند را می‌توان به گونه‌ای پیکربندی کرد که تنها اجازه دسترسی به آن دسته از سرورهای شبکه وجود داشته باشد که برای مصرف خارجی در نظر گرفته شده‌اند و این دسترسی نیز تنها از طریق برخی پورت‌های خاص ممکن باشد. بدین ترتیب، موجودیت‌های خارج از شبکه حفاظت‌شده چندان قادر نخواهند بود به آن دسته از خدمات یا سرورهای شبکه دسترسی پیدا کنند که تنها برای دسترسی یا مصرف از درون شبکه در نظر گرفته شده‌اند.

از چشم‌انداز خروج اطلاعات، فایروال‌های فیلترینگ ترافیک حالتمند را می‌توان به گونه‌ای پیکربندی کرد که از درون شبکه حفاظت‌شده تنها بتوان به برخی خدمات خارجی خاص (مثلاً بر اساس پورت مقصد) دسترسی پیدا کرد. به عنوان مثال، می‌توان دسترسی به خدمات ایمیل خارجی را مسدود کرد تا امکان دسترسی به سرورهای ایمیل کنترل‌نشده وجود نداشته باشد. توجه داشته باشید که در این صورت، اثربخشی فایروال‌های فیلترینگ ترافیک حالتمند محدود می‌شود، زیرا سرورهای خارجی می‌توانند خدمات خود را روی پورت‌های دیگری ارائه کنند (در این صورت، مثلاً فایروال فیلترینگ برنامه کاربردی سطح حفاظت بالاتری را فراهم خواهد آورد).

دسترسی به شبکه

یک مهاجم با دانستن این که کدام خدمات توسط ماشین‌ها روی شبکه فرعی قرار گرفته‌اند، ممکن است تلاش کند تا حملاتی را علیه آن‌ها ترتیب دهد.

۸,۱,۲ سوءاستفاده از خدمات

دستگاه‌های خارج از شبکه «حفاظت‌شده» می‌توانند به برخی خدمات عمومی ارائه‌شده درون شبکه دسترسی داشته باشند؛ اما گاهی اوقات این دستگاه‌ها تلاش می‌کنند تا در هنگام برقراری ارتباط با این خدمات مجاز، فعالیت‌های غیر مقتضی و غیرمجازی را انجام دهند. همچنین، ممکن است دسترسی به برخی خدمات خاص ارائه‌شده درون شبکه محافظت‌شده، منجر به پدید آمدن مخاطراتی گردد. لازم به ذکر است که فایروال تنها قوانینی را اعمال می‌کند که برای یک واسط شبکه تعیین شده‌اند. اصطلاح شبکه حفاظت‌شده یا مورد اعتماد زمانی معنادار خواهد بود که مجموعه قوانین نیز به طور مناسب و در این راستا تنظیم شده باشند.

از چشم‌انداز ورود اطلاعات، معمولاً چنین فرض می‌شود که موجودیت‌های فعال روی شبکه‌های خارجی محدود به خط‌مشی‌های کاری تنظیم‌شده برای یک شبکه حفاظت‌شده خاص نیستند. با این حال، فایروال‌های فیلترینگ ترافیک حالتمند می‌توانند موارد نقض خط‌مشی‌های مربوط به خدمات عمومی را ثبت کنند.

از چشم‌انداز خروج اطلاعات، فایروال‌های فیلترینگ ترافیک حالتمند را می‌توان تنها به گونه‌ای پیکربندی کرد که امکان اجرا و پایش خط‌مشی‌های کاری شبکه حفاظت‌شده به نحو بهتری وجود داشته باشد. چنان که در مورد سایر تهدیدات شرح داده شد، یک فایروال فیلترینگ ترافیک حالتمند می‌تواند انتشار اطلاعات، دسترسی به سرورهای خارجی و حتی متوقف کردن خدمات را محدود کند (که تمام این موارد به گونه‌ای مربوط به خط‌مشی‌های کاری شبکه حفاظت‌شده هستند و نحوه اجرای خط‌مشی‌ها بر آن‌ها تأثیر می‌گذارد). علاوه بر این، فایروال‌های فیلترینگ ترافیک حالتمند را می‌توان تنها به گونه‌ای پیکربندی کرد که تعاملات رخ‌داده بین شبکه حفاظت‌شده و شبکه خارجی را ثبت کنند و در نتیجه، موارد بالقوه نقض خط‌مشی‌ها را مشخص نمایند.

سوءاستفاده از شبکه

ممکن است مهاجم تلاش کند تا به شکلی مغایر با اهداف و خط‌مشی‌های امنیتی یک سایت، از خدمات صادرشده توسط ماشین‌ها استفاده نماید. به عنوان مثال، ممکن است مهاجم با استفاده از یک سرویس، ماشینی را که برای حمله به کار گرفته است به شکل «ناشناس» در آورد.

۹,۱,۲ ترافیک مخرب

یک فایروال فیلترینگ ترافیک حالتمند، شبکه را در برابر بسته‌های بدخواه یا مخرب حفاظت می‌کند. این فایروال وظیفه حفاظت در برابر حملاتی مانند حمله دست‌کاری اطلاعات وضعیت اتصال و حمله بازپخش را بر عهده دارد. این حملات ممکن است باعث شوند که فایروال یا دستگاه‌های حفاظت‌شده توسط آن، امکان دسترسی غیرمجاز یا حتی انجام حملات DoS را به دست آورند.

ترافیک مخرب

ممکن است مهاجم تلاش کند تا بسته‌های مخربی را به یک ماشین ارسال نماید و بدین ترتیب، پشته شبکه[۱] یا خدمات لیست‌شده روی پورت‌های UDP/TCP یک ماشین هدف را مختل کند.

۲,۲ فرضیات

در این بخش، فرضیات مربوط به شناسایی تهدیدات و الزامات امنیتی فایروال‌ها را مرور می‌کنیم. انتظار نمی‌رود که فایروال هیچ یک از این موارد را تضمین کند. در نتیجه، الزامات برای کاهش خسارت تهدیدات ارائه نشده‌اند.

۱,۲,۲ حفاظت فیزیکی

فرض بر این است که فایروال در محیط عملیاتی خود به صورت فیزیکی محافظت می‌شود و در معرض حملات فیزیکی که سبب به خطر افتادن امنیت و/یا تداخل در ارتباطات فیزیکی و عملیات آن می‌شوند، قرار ندارد. علاوه بر این، فرض می‌شود که این حفاظت فیزیکی برای امن ماندن فایروال و داده‌های آن کافی است. در نتیجه، این پروفایل حفاظتی مشارکتی شامل الزاماتی برای حفاظت فیزیکی یا کاهش احتمال حملات فیزیکی نیست. پروفایل حفاظتی مشارکتی حاضر از محصولات انتظار ندارد که در برابر دسترسی فیزیکی توسط موجودیت‌های غیرمجاز (به منظور استخراج داده‌ها، دور زدن سایر کنترل‌ها، یا دست‌کاری فایروال به هر ترتیبی) محافظت به عمل آورند.

۲,۲,۲ کارکرد محدود

فرض بر این است که فایروال کارکرد شبکه و فیلترینگ را به عنوان کارکرد اصلی خود ارائه می‌نماید و خدمات و کارکردهایی که در دسته رایانش همه‌منظوره قرار می‌گیرند را ارائه نمی‌کند. به عنوان مثال، فایروال نباید یک پلتفرم رایانشی را برای برنامه‌های کاربردی همه‌منظوره (غیر مرتبط به کارکرد شبکه یا فیلترینگ) ارائه نماید.

---

[۱] network stack

۳,۲,۲ راهبر مورد اعتماد

فرض بر این است که راهبران مجاز فایروال مورد اعتماد هستند و تمام تلاش خود را برای تأمین امنیت سازمان انجام می‌دهند. در واقع فرض می‌شود که راهبران مجاز به خوبی تعلیم داده شده‌اند، از خط‌مشی‌ها تبعیت می‌کنند و به اسناد راهنمای سازمان پایبند هستند. فرض بر این است که راهبران اقدامات لازم را انجام می‌دهند تا اطمینان حاصل کنند که گذرواژه‌ها و اطلاعات محرمانه، قدرت و آنتروپی لازم را دارند. همچنین فرض می‌شود که راهبران در هنگام راهبری فایروال، اهداف خرابکارانه ندارند. از فایروال انتظار نمی‌رود که بتواند در برابر یک راهبر خرابکار که می‌خواهد امنیت آن را به خطر اندازد، از خود محافظت نماید.

۴,۲,۲ به‌روزرسانی منظم

فرض بر این است که نرم‌افزار و ثابت‌افزار فایروال به طور منظم توسط راهبر به‌روز می‌شوند. این به‌روزرسانی‌ها برای از بین بردن آسیب‌پذیری‌ها هستند.

۵,۲,۲ امنیت اطلاعات محرمانه راهبر

اطلاعات محرمانه راهبر (کلید خصوصی) که برای دسترسی به فایروال استفاده می‌شوند، توسط پلتفرم میزبان محافظت می‌شوند.

۳,۲ خط‌مشی امنیتی سازمان

خط‌مشی امنیتی سازمان مجموعه‌ای از قوانین، فعالیت‌ها و رویه‌ها است که توسط سازمان و به منظور پاسخگویی به نیازهای امنیتی ارائه شده‌اند. یک خط‌مشی خاص در بخش بعد تشریح شده است.

۱,۳,۲ بنر دسترسی

هدف ارزیابی باید یک بنر اولیه شامل اطلاعاتی درباره محدودیت‌های کاربرد، موافقت‌نامه‌های قانونی و دیگر اطلاعات مقتضی را به کاربران نشان دهد. کاربران با دسترسی به هدف ارزیابی، رضایت خود را از این موارد اعلام می‌کنند.

۳ اهداف امنیتی

۱,۳ اهداف امنیتی برای محیط عملیاتی

در بخش‌های زیر، اهداف امنیتی برای محیط عملیاتی شرح داده شده‌اند.

۱,۱,۳ امنیت فیزیکی

امنیتی فیزیکی که متناسب با ارزش هدف ارزیابی و داده‌های موجود در آن است، توسط محیط تأمین می‌شود.

۲,۱,۳ عدم وجود قابلیت رایانش همه‌منظوره

هدف ارزیابی هیچ قابلیت رایانش همه‌منظوره‌ای (مانند کامپایلرها یا برنامه‌های کاربردی کاربران) ندارد، مگر خدماتی که برای عملکرد، مدیریت و پشتیبانی از هدف ارزیابی ضروری هستند.

۳,۱,۳ راهبر مورد اعتماد

به راهبران هدف ارزیابی اعتماد می‌شود و فرض بر این است که راهبران مذکور از تمام اسناد راهنما به شکل مطلوبی تبعیت می‌نمایند.

۴,۱,۳ به‌روزرسانی

نرم‌افزار و ثابت‌افزار فایروال به طور منظم توسط راهبر به‌روز می‌شوند. این به‌روزرسانی‌ها برای از بین بردن آسیب‌پذیری‌ها هستند.

۵,۱,۳ امنیت اطلاعات محرمانه راهبر

اطلاعات محرمانه راهبر (کلید خصوصی) که برای دسترسی به هدف ارزیابی استفاده می‌شوند، توسط پلتفرم میزبان محافظت می‌شوند.

۴ الزامات کارکرد امنیتی

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

به‌طورکلی، الزامات کارکرد امنیتی 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.

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

شماره الزام	نام الزام	عنصر متناظر با الزام
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2
۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.1.3
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۸	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۹	مدیریت کلید رمزنگاری ۴	FCS_CKM.4.1
۱۰	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۱	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1(3)
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
۱۴	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۱۵	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۱۶	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۱۷	شناسایی و احراز هویت کاربر ۱	FIA_UIA_EXT.1.1
۱۸	شناسایی و احراز هویت کاربر ۲	FIA_UIA_EXT.1.2
۱۹	سازوکار احراز هویت بر اساس رمز عبور ۲	FIA_UAU_EXT.2.1
۲۰	احراز هویت کاربر ۱۰	FIA_UAU.7.1
۲۱	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۲۲	الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2
۲۳	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۲۴	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2
۲۵	الزامات پروتکل X509 (۵)	FIA_X509_EXT.3.1
۲۶	الزامات پروتکل X509 (۶)	FIA_X509_EXT.3.2
۲۷	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۲۸	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۲۹	مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن	FMT_MOF.1.1(1)/TrustedUpdate
۳۰	مدیریت داده‌های محصول ۱	FMT_MTD.1.1
۳۱	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۳۲	نقش‌های امنیتی ۳	FMT_SMR.2.1
۳۳	نقش‌های امنیتی ۴	FMT_SMR.2.2
۳۴	نقش‌های امنیتی ۵	FMT_SMR.2.3
۳۵	محافظت از داده‌های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1
۳۶	حفاظت از کلمه عبور سرپرست محصول ۱	FPT_APW_EXT.1.1
۳۷	حفاظت از کلمه عبور سرپرست محصول ۲	FPT_APW_EXT.1.2
۳۸	خودآزمایی محصول ۱	FPT_TST_EXT.1.1
۳۹	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۴۰	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۴۱	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۴۲	مهرهای زمانی ۱	FPT_STM.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۴۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۴۴	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۴۵	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۴۶	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
۴۷	کانال امن ۱	FTP_ITC.1.1
۴۸	کانال امن ۲	FTP_ITC.1.2
۴۹	کانال امن ۳	FTP_ITC.1.3
۵۰	مسیر امن ۱	FTP_TRP.1.1
۵۱	مسیر امن ۲	FTP_TRP.1.2
۵۲	مسیر امن ۳	FTP_TRP.1.3
۵۳	فیلترینگ حالتمند ۱	FFW_RUL_EXT.1.1
۵۴	فیلترینگ حالتمند ۲	FFW_RUL_EXT.1.2
۵۵	فیلترینگ حالتمند ۳	FFW_RUL_EXT.1.3
۵۶	فیلترینگ حالتمند ۴	FFW_RUL_EXT.1.4
۵۷	فیلترینگ حالتمند ۵	FFW_RUL_EXT.1.5
۵۸	فیلترینگ حالتمند ۶	FFW_RUL_EXT.1.6
۵۹	فیلترینگ حالتمند ۷	FFW_RUL_EXT.1.7
۶۰	فیلترینگ حالتمند ۸	FFW_RUL_EXT.1.8
۶۱	فیلترینگ حالتمند ۹	FFW_RUL_EXT.1.9

شماره الزام	نام الزام	عنصر متناظر با الزام
۶۲	فیلترینگ حالتمند ۱۰	FFW_RUL_EXT.1.10
الزامات مربوط به پیوست یک		
۶۳	ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۶۴	ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۶۵	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.2.1
۶۶	محل ذخیره‌سازی داده‌های ممیزی ۴	FAU_STG_EXT.3.1
۶۷	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی	FMT_MOF.1.1(1)/Audit
۶۸	مدیریت کارکرد در محصول ۱ (۲)/ ممیزی	FMT_MOF.1.1(2)/Audit
۶۹	مدیریت کارکرد در محصول ۱ (۱)/ اقدامات مدیریتی	FMT_MOF.1.1(1)/AdminAct
۷۰	مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی	FMT_MOF.1.1(2)/AdminAct
۷۱	مدیریت کارکرد در محصول ۱ (۱)/ فضای ذخیره‌سازی ممیزی محلی	FMT_MOF.1.1/LocSpace
۷۲	مدیریت داده‌های محصول ۱/ اقدامات مدیریتی	FMT_MTD.1.1/AdminAct
۷۳	حفظ وضعیت امن در زمان شکست ۱/ فضای ذخیره‌سازی ممیزی محلی	FPT_FLS.1.1/LocSpace
۷۴	فیلترینگ حالتمند ۱۱	FFW_RUL_EXT.2.1
الزامات مربوط به پیوست دو		
۷۵	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۷۶	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۷۷	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۷۸	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۷۹	الزامات پروتکل IPSEC (۲)	FCS _IPSEC_EXT.1.2
۸۰	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۸۱	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۸۲	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۸۳	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۸۴	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۸۵	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۸۶	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۸۷	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۸۸	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۸۹	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۹۰	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۹۱	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۹۲	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۹۳	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۹۴	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۹۵	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4

شماره الزام	نام الزام	عنصر متناظر با الزام
۹۶	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۹۷	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۹۸	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۹۹	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۱۰۰	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۱۰۱	الزامات پروتکلSSH Server (۱)	FCS_SSHS_EXT.1.1
۱۰۲	الزامات پروتکلSSH Server (۲)	FCS_SSHS_EXT.1.2
۱۰۳	الزامات پروتکلSSH Server (۳)	FCS_SSHS_EXT.1.3
۱۰۴	الزامات پروتکلSSH Server (۴)	FCS_SSHS_EXT.1.4
۱۰۵	الزامات پروتکلSSH Server (۵)	FCS_SSHS_EXT.1.5
۱۰۶	الزامات پروتکلSSH Server (۶)	FCS_SSHS_EXT.1.6
۱۰۷	الزامات پروتکلSSH Server (۷)	FCS_SSHS_EXT.1.7
۱۰۸	الزامات پروتکلSSH Server (۸)	FCS_SSHS_EXT.1.8
۱۰۹	الزامات پروتکلTLS Client/ احراز هویت ۱	FCS_TLSC_EXT.1.1
۱۱۰	الزامات پروتکلTLS Client/ احراز هویت ۲	FCS_TLSC_EXT.1.2
۱۱۱	الزامات پروتکلTLS Client/ احراز هویت ۳	FCS_TLSC_EXT.1.3
۱۱۲	الزامات پروتکلTLS Client/ احراز هویت ۴	FCS_TLSC_EXT.1.4
۱۱۳	الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۱	FCS_TLSC_EXT.2.1
۱۱۴	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۲	FCS_TLSC_EXT.2.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۱۵	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۳	FCS_TLSC_EXT.2.3
۱۱۶	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۴	FCS_TLSC_EXT.2.4
۱۱۷	الزامات پروتکلTLS Client/ احراز هویت دو طرفه ۵	FCS_TLSC_EXT.2.5
۱۱۸	الزامات پروتکلTLS Server/ احراز هویت ۱	FCS_TLSS_EXT.1.1
۱۱۹	الزامات پروتکلTLS Server/ احراز هویت ۲	FCS_TLSS_EXT.1.2
۱۲۰	الزامات پروتکلTLS Server/ احراز هویت ۳	FCS_TLSS_EXT.1.3
۱۲۱	الزامات پروتکلTLS Server/ احرازهویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۲۲	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۲	FCS_TLSS_EXT.2.2
۱۲۳	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۳	FCS_TLSS_EXT.2.3
۱۲۴	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۴	FCS_TLSS_EXT.2.4
۱۲۵	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۵	FCS_TLSS_EXT.2.5
۱۲۶	الزامات پروتکلTLS Server/ احرازهویت دو طرفه ۶	FCS_TLSS_EXT.2.6
۱۲۷	خودآزمایی محصول مورد ارزیابی ۲	FPT_TST_EXT.2.1
۱۲۸	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۲۹	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۳۰	مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/ به‌روزرسانی امن	FMT_MOF.1.1(2)/TrustedUpdate

۱,۴ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات موجود در زمینه پیکربندی و/یا کارکرد سیستم را در اختیاردارند، محصول باید این قابلیت را داشته باشد که داده‌های ممیزی موردنیاز را تولید نمایند. ممیزی فعالیت‌های مدیریت سیستم سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سیستم، می‌توان برای طراحی اقدامات اصلاحی از آن‌ها استفاده کرد. ممیزی رویدادهای گزینش‌شده نشان می‌دهد که آیا بخش‌هایی مهم محصول مورد ارزیابی در معرض شکست قرار دارند یا خیر (مثلاً این‌که فرایند رمزنگاری اجرا نشود) و همچنین به شناسایی فعالیت‌های غیرمعمول (مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم) کمک می‌کند. در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به‌اندازه‌ای زیاد شود که محصول مورد ارزیابی یا راهبران مسئول بازبینی این اطلاعات را دچار سردرگمی‌کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت امن 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) تمام اقدامات مدیریتی شامل موارد زیر:

- ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به‌حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)
- تغییرات امنیتی در 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 کلمه عبور (نام حساب کاربری مربوطه نیز باید ثبت شود)
- آغاز و توقف سرویس‌ها
- انتخاب: [هیچ اقدام دیگر، اختصاص: [لیست سایر کاربردهای ویژه]]؛

ت) انتخاب: [دیگر رویدادهای ممیزی لیست در نکته کاربردی ۳].

نکته کاربردی ۱:

با توجه به کارکرد محصول درصورتی‌که لیست «اقدامات مدیریتی» ناقص است، نویسنده سند هدف امنیتی باید در قسمت «اختصاص» که در «انتخاب» قرارگرفته است را استفاده کرده و اقدامات مدیریتی دیگری را به لیست اضافه کند.

نکته کاربردی ۲:

در این الزام «سرویس» اشاره دارد به ارتباطات صورت‌گرفته از طریق کانال امن و مسیر امن، خودآزمایی‌های درخواست شده، به‌روزرسانی امن و نشست‌های مدیریتی سیستم).

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 فعال[1] و نتیجه رویداد (موفقیت یا شکست)؛ و
ب) در مورد هر یک از انواع رویدادهای ممیزی و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات مشخص‌شده در نکته کاربری ۳.

نکته کاربردی ۳:
نویسنده هدف امنیتی با توجه به رویدادهای ممیزی ثبت‌شده برای هر یک از الزامات زیر باید اطلاعات مناسب دیگر علاوه بربند الف الزام «تولید داده ممیزی ۲» فراهم کند. برای نمونه توسعه‌دهنده با توجه به الزام «شناسایی و احراز هویت کاربر ۲» برای ثبت رکورد ممیزی علاوه بر اطلاعات بند الف الزام «تولید داده ممیزی ۲» باید آدرس IP منشأ احراز هویت را در رکورد ممیزی (به‌عنوان نمونه در قسمت توضیحات رکورد) ثبت نماید؛ بنابراین این اطلاعات توسط نویسنده سند هدف امنیتی در این قسمت قرار داده می‌شود.

- برای الزام «سازوکار احراز هویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای مکانیسم تعیین هویت و احراز هویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.
- برای الزام «الزامات پروتکل X509» اطلاعات ممیزی مربوط به تلاش ناموفق برای تأیید یک گواهی‌نامه ثبت می‌شود. این اطلاعات باید شامل دلیل شکست باشد.
- برای الزام «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی دستی ثبت می‌شود.
- برای الزام «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود.
- برای الزام «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود.
- برای الزام «مهرهای زمانی» اطلاعات ممیزی مربوط به تغییرات صورت گرفته در زمان ثبت می‌شود. این اطلاعات باید شامل زمان‌های جدید و قدیم، منشأ تلاش (مانند آدرس IP) برای تغییر زمان موفق یا ناموفق باشد.

[1] subject

- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها» اطلاعات ممیزی تمام تلاش‌های صورت گرفته برای باز کردن قفل یک نشست تعاملی ثبت می‌شود.
- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه دور از طریق یک مکانیسم قفل‌کردن نشست ثبت می‌شود.
- برای الزام «قفل‌کردن نشست‌های شروع‌شده توسط محصول و خاتمه دادن به آن‌ها» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست تعاملی ثبت می‌شود.
- برای الزام «کانال امن» اطلاعات ممیزی مربوط به آغاز کردن کانال امن/خاتمه دادن کانال امن/شکست توابع کانال امن ثبت می‌شود. این اطلاعات باید شامل شناسایی دلیل و هدف تلاش ناموفق برای ایجاد کانال امن باشد.
- برای الزام «مسیر امن» اطلاعات ممیزی مربوط به آغاز کردن مسیر امن/خاتمه دادن مسیر امن/شکست توابع مسیر امن ثبت می‌شود. این اطلاعات باید شامل شناسایی هویت ادعاشده توسط کاربر باشد.
- برای الزام «فایروال حالتمند» اطلاعات ممیزی برای اعمال قوانین پیکربندی‌شده با عملیات log ثبت می‌شود. این اطلاعات باید شامل آدرس‌های مبدأ و مقصد، پورت‌های مبدأ و مقصد، پروتکل لایه انتقال، واسط هدف ارزیابی باشد.
- برای الزام «فایروال حالتمند» اطلاعات ممیزی برای وجود نشانه‌ای مبنی بر کنار گذاشته شدن[۱] بسته‌ها به دلیل زیاد بودن ترافیک شبکه ثبت می‌شود. این اطلاعات باید شامل واسط هدف ارزیابی که نمی‌تواند بسته‌ها را پردازش کند، شناسه قوانینی که موجب کنار گذاشته شدن بسته‌ها می‌شوند باشد.

نکته کاربردی ۴:

رویدادهای ممیزی دیگر بر اساس الزامات اختیاری و انتخابی برگرفته‌شده از پیوست‌های یک و دو به محصول مورد ارزیابی اضافه می‌شوند؛ بنابراین، نویسنده هدف امنیتی باید رویدادهای اضافی را اضافه نماید.

[۱] Drop

رویداد ممیزی «الزامات پروتکل X509» 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 مورد اعتماد
- 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.

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.

۴	**محل ذخیره‌سازی داده‌های ممیزی ۱**

محصول باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال مورد اعتماد پیاده‌سازی شده با پروتکل [انتخاب: IPsec،SSH،TLS، TLS/HTTPS] باشد.

تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست ۲ تمامی الزامات مربوط به آن پروتکل تکمیل و به سند ST اضافه گردد.

نکته کاربردی ۵:

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.
۵ **محل ذخیره‌سازی داده‌های ممیزی ۲**
محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.
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 ۶: 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.

[۱] Overwrite

[۲] External log server

۲,۴ کلاس پشتیبانی رمزنگاری (FCS)

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

شماره الزام	نام الزام
۷	**مدیریت کلید رمزنگاری ۱**
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 ۷: نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورداستفاده برای استقرار کلید و احراز هویت 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	

[۱] Key establishment
[۲] Keyed hash generation

شماره الزام	نام الزام
انتخاب باشند. درصورتی‌که برای احراز هویت دستگاه‌ها از الگوهای تولید کلید استفاده شود، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی‌نامه X.509v3 باشد. اگر محصول مورد ارزیابی به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید RSA عمل کند، نیازی نیست که محصول، الگوی تولید کلید RSA را پیاده‌سازی نماید.	
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: شماره ویژه NIST 800-56B، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛ • الگوهای استقرار کلید منحنی بیضوی[۳] که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۴]؛ • الگوهای استقرار کلید میدانی[۵] که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته». نکته کاربردی ۸: این عنصر درواقع نسخه اصلاح‌شده «مدیریت کلید رمزنگاری ۲» است که به‌جای توزیع کلید، به استقرار کلید می‌پردازد.	

۱ Key establishment
۲ Integer factorization cryptography
۳ Elliptic curve-based
۴ Discrete logarithm cryptography
۵ Finite filed-based

شماره الزام	نام الزام
نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورداستفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. الگوهای استقرار کلید مبتنی بر RSA در بخش ۹ از NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های SP 800-56B است. 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 «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: [انتخاب: • در مورد حافظه فرار[۱]، نابودی باید از طریق یک بازنویسی ساده و مستقیم [انتخاب: شامل الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، شامل صفرها] انجام شود و سپس از طریق خواندن تائید شود. o درصورتی‌که داده‌های بازنویسی شده پس از خواندن تائید نشود، فرایند باید مجدداً تکرار شود. • در مورد EEPROM غیر فرار، نابودی باید از طریق یک بازنویسی ساده و مستقیم شامل الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی انجام شود (طبق آنچه در «تولید بیت تصادفی» تشریح شده است) و سپس تأیید از طریق خواندن صورت گیرد. o درصورتی‌که داده‌های بازنویسی شده پس از خواندن تائید نشود، فرایند باید مجدداً تکرار شود. • در مورد حافظه فلش غیر فرار، نابودی باید از طریق [انتخاب: یک بازنویسی ساده و مستقیم شامل صفرها، پاک کردن بلوک] انجام شود و پس از خواندن تائید شود. o درصورتی‌که داده‌های بازنویسی شده پس از خواندن تائید نشود، فرایند باید مجدداً تکرار شود.	

[۱] Volatile memory

شماره الزام	نام الزام
• در مورد حافظه‌های غیر فرار به‌جز فلش و EEPROM، نابودی باید از طریق سه بار بازنویسی با الگوی تصادفی انجام شود، به‌گونه‌ای که این الگو پیش از هر بار بازنویسی عوض شود.]	
۱۰	**عملیات رمزنگاری ۱ (۱)**
محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص که در حالت [انتخاب: CBC، GCM] استفاده می‌شوند و در اندازه‌های کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] و با توجه به استاندارد AES که در ISO 18033-3 تعریف‌شده است، [انتخاب: CBC که در ISO 10116 تعریف‌شده است، GCM که در ISO 19772 تعریف‌شده است] انجام دهد. نکته کاربردی ۹: در مورد نخستین انتخاب عملیات رمزنگاری ۱(۱)، نویسنده هدف امنیتی باید حالت یا حالت‌های کارکردی AES را تعیین کند. در مورد دومین انتخاب، نویسنده هدف امنیتی باید اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[۱] در الزامات کانال امن هستند.	
۱۱	**عملیات رمزنگاری ۱ (۲)**
محصول مورد ارزیابی باید خدمات امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوریتم امضای دیجیتال RSA و اندازه کلیدهای [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر] • الگوریتم امضای دیجیتال بیضوی و اندازه کلیدهای [اختصاص: ۲۵۶ بیتی یا بزرگ‌تر]] با رعایت موارد زیر:	

[۱] cipher suite

شماره الزام	نام الزام
[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 RSASSAPKCS2v1_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 NISTP-256 و P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ ISO/IEC 14888-3، بخش ۶،۴] نکته کاربردی ۱۰: نویسنده هدف امنیتی باید الگوریتم مورداستفاده برای اجرای امضای دیجیتال را تعیین کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید انتخاب‌ها و اختصاص‌های مناسب را انجام دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین نماید.	
۱۲	**عملیات رمزنگاری ۱ (۳)**
محصول مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1, SHA-256, SHA-384, SHA-512] با رعایت استاندارد ISO/IEC 10118-3:2004. ارائه نماید. نکته کاربردی ۱۱: 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. طبق SP 800-131 A الگوریتم SHA-1 فقط می‌تواند برای عملیات غیر از امضای دیجیتال همچون درهم سازی پسورد و ... استفاده شود.	

شماره الزام	نام الزام
انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای «عملیات رمزنگاری ۱(۱)» و «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی).	
۱۳	**عملیات رمزنگاری ۱ (۴)**
محصول مورد ارزیابی باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده[1] را بر اساس الگوریتم رمزنگاری خاص [انتخاب:-HMAC-SHA-1, HMAC SHA-256,HMAC-SHA-384, HMAC-SHA-512] و با استفاده از اندازه کلید [اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)] و اندازه خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح‌شده در بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم ۲ MAC» انجام دهد. نکته کاربردی ۱۲: 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 خدمات 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 نرم‌افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت‌افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست کم	

[1] Keyed-hash message authentication

شماره الزام	نام الزام
	[انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و درهم‌سازهای تولیدشده مورداشاره در بخش جدول C.1 «Security Strength Table for Hash Functions» ISO/IEC 18031:2011 باشد. نکته کاربردی ۱۳: در مورد نخستین عبارت انتخاب در «تولید بیت تصادفی ۲»، هدف امنیتی باید حداقل به یکی از انواع منابع نویز اشاره کند. اگر محصول مورد ارزیابی شامل 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 مورداشاره در فعالیت‌های ارزیابی، تمام منابع مورداشاره در هدف امنیتی را پوشش می‌دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها به عناصر اولیه فرایند رمزنگاری (توابع درهم‌ساز و مجموعه‌های رمز) بستگی دارد. نویسنده هدف امنیتی، تابع مورداستفاده را انتخاب خواهد کرد و عناصر اولیه فرایند رمزنگاری را تعیین خواهد نمود. با اینکه تمام توابع درهم‌ساز تعیین‌شده (SHA-1,SHA-224, SHA-256, SHA-384, SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، تنها اجازه استفاده از موارد مبتنی بر AES در CTR_DRBG وجود دارد. اگر اندازه کلید برای پیاده‌سازی AES متفاوت از اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تغییر یا تکرار «عملیات رمزنگاری» باشد تا تفاوت اندازه کلید در آن لحاظ گردد. در مورد عبارت انتخاب «تولید بیت تصادفی ۲»، نویسنده هدف امنیتی حداقل تعداد بیت‌های آنتروپی تزریق‌شده به RBG را تعیین می‌کند.

۳,۴ کلاس محافظت از داده کاربری

شماره الزام	نام الزام
۱۶	حفاظت از اطلاعات باقیمانده در منابع ۱

محصول باید تضمین کند که هر گونه محتوی اطلاعات قبلی یک منبع را در زمان [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت‌های غیرفعال، غیرقابل دسترس کند. نکته کاربردی ۱۴: در این الزام، منظور از «منابع» بسته‌های شبکه است که از طریق هدف ارزیابی ارسال می‌شوند (نه بسته‌هایی که از طریق سرپرست سیستم «به» هدف ارزیابی فرستاده می‌شوند). نگرانی موجود این است که پس از ارسال یک بسته شبکه، بافر یا حافظه مورد استفاده توسط بسته هنوز شامل داده‌هایی درباره آن باشد و در صورتی که بافر مجدداً استفاده شود، این داده‌ها به بسته جدیدی منتقل شوند.

۴,۴ کلاس شناسایی و احراز هویت

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

شماره الزام	نام الزام
۱۷	مدیریت کلمه عبور ۱
محصول مورد ارزیابی باید قابلیت‌های مدیریت کلمه عبور زیر را برای کلمه عبور سرپرست محصول فراهم آورد:	

الف) کلمه عبور را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: [انتخاب: ,"@" ,"!" "(" ,")" ,"*" ,"&" ,"^" ,"%" ,"$","#"، [اختصاص: سایر کاراکترها]]؛ ب) حداقل طول کلمه عبور باید توسط سرپرست محصول قابل تعیین باشد، کلمه‌های عبور باید بتوانند ۱۵ کاراکتر یا بزرگ‌تر باشند. نکته کاربردی ۱۴: نویسنده هدف امنیتی کاراکترهای ویژه قابل استفاده در کلمه عبور را تعیین می‌کند. وی می‌تواند با استفاده از عبارت اختصاص، کاراکترهای دیگری را به لیست بیفزاید. منظور از «کلمه‌های عبور جایگزین»، کلمه‌های عبوری هستند که توسط مدیران سیستم در کنسول محلی مورداستفاده قرار می‌گیرند. این کلمه‌های عبور روی پروتکل‌هایی استفاده می‌شوند که از آن‌ها پشتیبانی کنند. به عنوان مثال، می‌توان از SSH و HTTPS نام برد. این کلمه‌های عبور گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی مورداستفاده قرار می‌گیرند که از دیگر الزامات کارکرد امنیتی در محصول پشتیبانی می‌کنند.

۱۸	شناسایی و احراز هویت کاربر ۱
محصول 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: [انتخاب: هیچ اقدامی، [اختصاص: لیست خدمات، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های خارجی]]	
۱۹	شناسایی و احراز هویت کاربر ۲
پیش از آن که محصول مورد ارزیابی امکان انجام اقدامات مدیریتی سیستم را فراهم آورد، باید مدیرسیستم را احراز هویت نماید. نکته کاربردی ۱۵: این الزام برای کاربران خدماتی 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 خدماتی که از طریق ارتباطات محصول مورد ارزیابی فراهم می‌گردند، اعمال نمی‌شود. از آنجا که موجودیت‌های	

خارجی پیش از تعیین و احراز هویت تنها باید به چند خدمت محدود (و یا هیچ خدمتی) دسترسی داشته باشند، این خدمات باید در عبارت اختصاص ذکر شوند. در غیر این صورت، باید «هیچ اقدام دیگر» را انتخاب کرد. احراز هویت ممکن است مبتنی بر کلمه عبور باشد و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از کلمه‌های عبور پشتیبانی می‌کند (مانند SSH)، یا اینکه بر اساس گواهی‌نامه انجام شود (مانند SSH و TLS). در مورد ارتباط با موجودیت‌های IT خارجی (مانند یک سرور ممیزی یا سرور NTP) این ارتباطات باید بر اساس الزامات «کانال امن» انجام شوند که پروتکل آن از تعیین و احراز هویت پشتیبانی می‌کند. این امر بدین معنی است که نیازی نیست ارتباطاتی از قبیل ایجاد ارتباط IPsec با سرور احراز هویت، در عبارت اختصاص ذکر شوند، زیرا ایجاد ارتباط به معنی آغاز فرایند تعیین و احراز هویت است.	
۲۰	سازوکار احراز هویت بر اساس رمز عبور ۲
محصول مورد ارزیابی باید یک مکانیسم احراز هویت مبتنی بر کلمه عبور، [انتخاب: [اختصاص: سایر مکانیسم‌های احراز هویت]، هیچ مکانیسمی] را برای احراز هویت مدیران سیستم فراهم آورد. نکته کاربردی ۱۶: عبارت اختصاص باید تمام مکانیسم‌های احراز هویت پشتیبانی‌شده را نشان دهد. مکانیسم‌های احراز هویت محلی از طریق کنسول محلی انجام می‌شوند. نشست‌های مدیریتی از راه دور (و مکانیسم‌های احراز هویت مربوط به آن‌ها) در الزامات «مسیر امن» مشخص شده‌اند.	
۲۱	احراز هویت کاربر ۱۰
هنگامی که فرایند احراز هویت در حال جریان است، محصول مورد ارزیابی تنها باید بازخورد مبهم[1] را در اختیار سرپرست محصول قرار دهد. نکته کاربردی ۱۷:	

[1] Obscured feedback

«بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی داده‌های احراز هویت 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 احراز هویت هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احراز هویت باشد، نمایش نمی‌دهد.

۲۲	**الزامات پروتکل X509 (۱)**

محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید نماید:

- تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه
- پایان یافتن مسیر گواهی‌نامه با یک گواهی‌نامه CA امن
- 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) چنان که در RFC 2560 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC 5759 تعریف شده است] تأیید کند.
- محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند:
  - گواهی‌نامه‌های مورداستفاده برای تأیید 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 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 ۱۸:
در این الزام قوانین مورداستفاده برای تأیید گواهی‌نامه‌ها لیست گردیده است. نویسنده هدف امنیتی وضعیت فسخ گواهی را توسط پروتکل OCSP یا CRL تائید می‌کند. لازم است برای پروتکل‌های استفاده شده در الزامات «مسیر امن» و «کانال امن» از گواهی استفاده شود لذا فیلد extendedKeyUsage باید بر اساس قوانین تائید گردند.

۲۳	**الزامات پروتکل X509 (۲)**

محصول مورد ارزیابی تنها در صورت از پیش تنظیم شدن افزونه مربوط به BasicConstraints و پرچم CA به حالت «TRUE»، یک گواهی‌نامه را به عنوان گواهی CA می‌پذیرد.

نکته کاربردی ۱۹:
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.

۲۴	**الزامات پروتکل X509 (۳)**

محصول مورد ارزیابی باید برای پشتیبانی از احراز هویت در [انتخاب: IPsec, TLS, HTTPS, SSH] و همچنین برای [انتخاب: امضای کد برای به‌روزرسانی نرم‌افزار سیستم، امضای کد برای تأیید صحت و یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده نماید.

نکته کاربردی ۲۰:

نویسنده سند هدف امنیتی در این الزام پروتکلی را انتخاب می‌نماید که در الزام ۴۸ «کانال امن ۱» آن پروتکل را انتخاب نموده است. گواهی‌نامه‌ها را به صورت اختیاری برای به‌روزرسانی‌های امن نرم‌افزار سیستم (به‌روزرسانی امن) و برای تأیید صحت و یکپارچگی (خودآزمایی محصول مورد ارزیابی۲) مورداستفاده قرار داد.	
الزامات پروتکل X509 (۴)	**۲۵**
اگر محصول مورد ارزیابی نتواند اتصال مورد نیاز برای تأیید اعتبار یک گواهی‌نامه را برقرار کند، باید [انتخاب: به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند، گواهی‌نامه را بپذیرد، گواهی‌نامه را نپذیرد]. نکته کاربردی ۲۱: برای بررسی وضعیت فسخ یک گواهی‌نامه غالباً باید اتصالی برقرار گردد که برای دانلود کردن یک CRL و جستجوی OCSP مورد استفاده قرار گیرد. در قسمت «انتخاب» این الزام تعیین می‌گردد در صورت عدم برقراری این اتصال چه اقدامی باید صورت گیرد. در صورت معتبر بودن گواهی بر اساس قوانین اشاره شده در «الزامات پروتکل X509»، گواهی توسط محصول مورد پذیرش قرار می‌گیرد. حال چنانچه یکی از قوانین نقض گردد، محصول مورد ارزیابی نباید آن گواهی را بپذیرد. در صورتی که نویسنده سند هدف امنیتی از بین گزینه‌های مطرح شده در بخش «انتخاب» گزینه‌ی «به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند» را انتخاب نماید لازم است در الزام شماره‌ی ۲۱ «کارکرد مدیریتی محصول» کارکرد مربوطه را نیز انتخاب نماید.	
الزامات پروتکل X509 (۵)	**۲۶**
محصول مورد ارزیابی باید مطابق با آنچه در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند این اطلاعات را درخواست فراهم نماید:	

• کلید عمومی[۱] • [انتخاب: اطلاعات مخصوص به دستگاه[۲]، Common Name، Orgsnization، Organization Unit، Country].
نکته کاربردی ۲۲: کلید عمومی در واقع بخش عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آنچه در الزامات «مدیریت کلید رمزنگاری» شرح داده شده است، توسط محصول مورد ارزیابی تولید می‌شود.

۲۷	**الزامات پروتکل X509 (۶)**
محصول مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.	
۲۸	**مدیریت احراز هویت ناموفق ۱**
محصول، باید [انتخاب: [اختصاص: یک عدد صحیح مثبت]، یک عدد مثبت قابل تنظیم توسط سرپرست [اختصاص: از یک بازه عددی قابل‌قبول]] از تلاش‌های ناموفق احراز هویت را نسبت به آخرین احراز هویت موفق مشخص نمایند.	
۲۹	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین‌شده رسید، از آن بیشتر شد]، توابع امنیتی هدف ارزیابی باید [اختصاص: اقداماتی را که بدین منظور در نظر گرفته شده است] انجام دهند.	

[۱] Public Key

[۲] Device-specific information

۵,۴ کلاس مدیریت امنیت

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

شماره الزام	نام الزام
۳۰	مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن
محصول مورد ارزیابی باید امکان فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست امنیتی محصول محدود نماید. نکته کاربردی ۲۳: این الزام امکان آغاز به‌روزرسانی دستی را به سرپرست محصول امنیتی محدود می‌کند.	
۳۱	مدیریت داده‌های محصول ۱
محصول مورد ارزیابی باید امکان «مدیریت» داده‌های محصول را به سرپرست محصول محدود کند. نکته کاربردی ۲۴: 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 کلمه عبور کاربری به حالت پیش‌فرض توسط سرپرست محصول امنیتی است.	
۳۲	کارکرد مدیریتی محصول ۱

شماره الزام	نام الزام

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

- مدیریت محصول به‌صورت محلی و از راه دور
- 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 امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها
- [انتخاب:
  - پیکربندی رفتار ممیزی
  - پیکربندی لیست خدمات ارائه‌شده توسط محصول مورد ارزیابی پیش از شناسایی یا احراز هویت یک موجودیت، مطابق با الزامات «شناسایی و احراز هویت کاربر»
  - پیکربندی کارکرد رمزنگاری
  - هیچ قابلیت دیگری]

نکته کاربردی ۲۵:

محصول مورد ارزیابی باید برای مدیریت سیستم به‌صورت محلی و از راه دور کارکردهای لازم را فراهم آورد. برای مثال با توجه به الزام شماره ۴۷ «پیغام‌های هشدار در رابطه با استفاده محصول» کارکرد پیکربندی بنر و بر اساس الزامات ۴۴ الی ۴۶«قفل‌کردن و خاتمه دادن به نشست‌ها» کارکرد زمان غیرفعال بودن نشست را پشتیبانی می‌نماید. همچنین کارکرد «به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها» با توجه به کارکردهای مدیریتی در الزام شماره ۲۹ «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» و الزام شماره‌ی ۱۱ «مدیریت کارکرد در محصول ۱ (۲)/ به‌روزرسانی امن» و الزام شماره ۲۴ «الزامات پروتکل X509(۴)» و «الزامات به‌روزرسانی امن۵» است.

شماره الزام	نام الزام
چنانچه محصول مورد ارزیابی پیش از شناسایی و احراز هویت، امکان پیکربندی رفتار ممیزی و خدمات موجود را برای سرپرست محصول فراهم نماید، یا در صورت وجود امکان پیکربندی هر یک از کارکردهای رمزنگاری محصول مورد ارزیابی، نویسنده سند هدف امنیتی باید در عبارت «انتخاب» گزینه یا گزینه‌های مناسب را برگزیند و در غیر این صورت گزینه‌ی «هیچ قابلیت دیگری» را انتخاب نماید.	
۳۳	**نقش‌های امنیتی ۳**
محصول باید نقش‌های زیر را نگهداری کند. • سرپرست محصول	
۳۴	**نقش‌های امنیتی ۴**
محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.	
۳۵	**نقش‌های امنیتی ۵**
محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند: • سرپرست محصول باید بتواند محصول مورد ارزیابی را به صورت دستی مدیریت کند. • سرپرست محصول باید بتواند محصول مورد ارزیابی را از راه دور مدیریت کند. نکته کاربردی ۲۶: بر اساس این محصول، سرپرست محصول باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک مکانیسم راه دور مدیریت کند (IPsec, SSH, TLS, HTTPS).	

۶,۴ کلاس حفاظت از محصول مورد ارزیابی

در این بخش، الزامات مربوط به محصول مورد ارزیابی برای حفاظت از داده‌های امنیتی حساس مانند کلیدها و کلمه‌های عبور، انجام خودآزمایی‌ها برای پایش کارکرد صحیح محصول مورد ارزیابی (شامل از بین بردن نقایص کارکرد میان‌افزار یا ضعف در یکپارچگی نرم‌افزار) و ارائه روش‌های امن برای به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را مطرح می‌گردد. 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
۳۶	**محافظت از داده‌های محصول (کلیدهای متقارن) ۱**
محصول مورد ارزیابی باید از خواندن تمام کلیدهایی که از پیش به اشتراک‌گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد. نکته کاربردی ۲۷: هدف از این الزام است که دستگاه بتواند مانع از دسترسی غیرمجاز به کلیدها، اطلاعات کلیدها و اطلاعات احراز هویت 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.	
۳۷	**حفاظت از کلمه عبور سرپرست محصول ۱**
محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	
۳۸	**حفاظت از کلمه عبور سرپرست محصول ۲**

محصول مورد ارزیابی باید از خوانده شدن کلمه‌های عبوری که به‌صورت متن ساده[۱] هستند، جلوگیری کند.

نکته کاربردی ۲۸:
هدف این الزام ذخیره نشدن داده‌های خام مربوط به احراز هویت از طریق کلمه عبور، به شکل واضح است به گونه‌ای که هیچ کاربر و سرپرست محصول نتواند کلمه عبور متن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصولی با دسترسی کامل می‌تواند کلمه عبور را بخواند؛ اما این امر با فرض اعتماد به سرپرست و عدم خواندن کلمه عبور توسط سرپرست است.

۱,۶,۴ آزمون محصول مورد ارزیابی

محصول مورد ارزیابی، برای اینکه برخی شکست‌های مکانیسم‌های 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 بخش در پیوست دو ارائه شده‌اند.)

شماره الزام	نام الزام
۳۹	خودآزمایی محصول۱
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].	

[۱] Plaintext

شماره الزام	نام الزام
تذکر: در صورتی که برای خودآزمایی‌ها از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام شماره ۱۲۷ «خودآزمایی محصول مورد ارزیابی ۲» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه گردد.	
نکته کاربردی ۲۹: 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.	
نکته کاربردی ۳۰: 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 «الزامات پروتکل X509» تأیید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در هدف امنیتی گنجانده شود.	

۲,۶,۴ 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 مکانیسم‌های رمزنگاری را مورداستفاده قرار دهد و با استفاده از آن‌ها، به‌روزرسانی‌ها را تهیه و تدارک ببیند، رمزنگاری به‌روزرسانی‌ها را از طریق مکانیسم 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. (برای این خانواده، تعدادی الزام مبتنی بر انتخاب در پیوست دو ارائه شده‌اند).

شماره الزام	نام الزام
۴۰	**به‌روزرسانی امن ۱**
محصول مورد ارزیابی باید این امکان را به سرپرست محصول بدهد که هم به نسخه فعلی نرم‌افزار و میان‌افزار محصول مورد ارزیابی و هم به جدیدترین نسخه نصب‌شده آن‌ها دسترسی داشته باشد. نکته کاربردی ۳۱: نسخه فعلی (مورداستفاده)، ممکن است جدیدترین نسخه نصب‌شده نباشد. به عنوان مثال، ممکن است تعدادی از به‌روزرسانی‌ها نصب شوند، اما پیش از اجرای آن‌ها نیاز به راه‌اندازی مجدد سیستم باشد؛ بنابراین، جستجوها[۱] باید بتواند هم به نسخه مورداستفاده و هم به آخرین نسخه نصب‌شده دسترسی داشته باشند.	
۴۱	**به‌روزرسانی امن ۲**
محصول مورد ارزیابی باید این امکان را برای سرپرست محصول امنیتی فراهم کند که به‌روزرسانی نرم‌افزار و 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 مکانیسم به‌روزرسانی دیگری پشتیبانی نکند].	

[۱] Query

شماره الزام	نام الزام
تذکر: در صورتی که نویسنده سند هدف امنیتی برای این الزام گزینه‌های به‌روزرسانی خودکار را انتخاب نماید لازم است الزام شماره ۱۳۰ «مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲) / به‌روزرسانی امن» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند. نکته کاربردی ۳۲: در این الزام بین گزینه‌های «جستجوی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز وجود دارد. «جستجوی خودکار به‌روزرسانی‌ها» به محصولی اشاره دارد که برای یافتن به‌روزرسانی جدید جستجو نموده و این امر را به سرپرست اطلاع می‌دهد (مثلاً از طریق یک پیام یا یک پرچم)؛ در این حالت نصب به‌روزرسانی منوط به انجام برخی اقدامات توسط سرپرست است. گزینه‌ی «به‌روزرسانی خودکار» به محصولی اشاره دارد که به منظور یافتن به‌روزرسانی جدید جستجو نموده و در صورت وجود به طور خودکار آن را نصب می‌نماید.	
۴۲	**به‌روزرسانی امن ۳**
محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: مکانیسم امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد. **تذکر: در صورتی که از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام‌های شماره ۱۲۸ «الزامات به‌روزرسانی ۴» و شماره ۱۲۹ «الزامات به‌روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.** نکته کاربردی ۳۳:	

شماره الزام	نام الزام
مکانیسم امضای دیجیتالی که در این الزام به آن اشاره شده است، یکی از الگوریتم‌های ذکر شده در الزام شماره‌ی ۱۱ «عملیات رمزنگاری ۱ (۲)» است. درهم‌ساز منتشرشده در این الزام توسط یکی از الزام ۱۲ «**عملیات رمزنگاری ۱ (۳)**» تولید می‌شود. نویسنده هدف امنیتی باید توسط «انتخاب» یک یا هر دو مکانیسم اجراشده توسط محصول را تعیین نماید. نکته کاربردی ۳۴: در نسخه‌های بعدی این پروفایل حفاظتی، لازم خواهد شد که برای به‌روزرسانی‌های امن، از یک مکانیسم امضای دیجیتال استفاده شود. نکته کاربردی ۳۵: در صورت استفاده از گواهی برای تائید به‌روزرسانی، این گواهی باید از «الزامات پروتکل X509 (۳)» انتخاب شوند و بر اساس الزامات «الزامات پروتکل X509» تأیید گردند. همچنین الزام شماره ۱۲۸ «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی لحاظ شود. نکته کاربردی ۳۶: در این الزام 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. هرچند 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.	

شماره الزام	نام الزام
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 مکانیسم به‌روزرسانی تأیید گردند. از آنجا که ممکن است مؤلفه‌ها توسط تولیدکننده‌های 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).	
۴۳	**مهرهای زمانی ۱**
محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی معتبر را داشته باشد. نکته کاربردی ۳۷: محصول مورد ارزیابی به خودی خود اطلاعات معتبری را درباره زمان فعلی و مکان محصول مورد ارزیابی ارائه نمی‌کند. این اطلاعات بستگی به اطلاعات خارجی درباره زمان و تاریخ دارند که یا به صورت دستی توسط سرپرست محصول و یا توسط سرور NTP فراهم آمده‌اند. عبارت «مهر زمانی معتبر» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده‌های ممیزی را محاسبه کرد.	

۷,۴ کلاس محافظت از داده کاربری

شماره الزام	نام الزام
۱	حفاظت از اطلاعات باقیمانده در منابع ۱

[۱] Firmware

محصول باید تضمین کند که هر گونه محتوی اطلاعات قبلی یک منبع را در زمان [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت‌های غیرفعال، غیرقابل دسترس کند.

نکته کاربردی ۱۴:

در این الزام، منظور از «منابع» بسته‌های شبکه است که از طریق هدف ارزیابی ارسال می‌شوند (نه بسته‌هایی که از طریق سرپرست سیستم «به» هدف ارزیابی فرستاده می‌شوند). نگرانی موجود این است که پس از ارسال یک بسته شبکه، بافر یا حافظه مورد استفاده توسط بسته هنوز شامل داده‌هایی درباره آن باشد و در صورتی که بافر مجدداً استفاده شود، این داده‌ها به بسته جدیدی منتقل شوند.

۸,۴ کلاس دسترسی به محصول

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

شماره الزام	نام الزام
۲	قفل‌کردن و خاتمه دادن به نشست‌ها ۷
در مورد نشست‌های تعاملی محلی[۱]، محصول مورد ارزیابی باید پس از اتمام زمان غیرفعال 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 غیرفعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛	

[۱] Local

شماره الزام	نام الزام
• نشست را خاتمه دهد].	
۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۵
در مورد نشست‌های تعاملی راه دور[۱]، 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.	
۴	قفل‌کردن و خاتمه دادن به نشست‌ها ۶
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۵	پیغام‌های هشدار در رابطه با استفاده محصول ۱
قبل از ایجاد نشست برای سرپرست محصول، محصول مورد ارزیابی باید توصیه‌های امنیتی مدیریتی و همچنین تأییدیه استفاده از محصول مورد ارزیابی را به سرپرست محصول نشان دهد. نکته کاربردی ۳۸: این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی مانند تماس‌های راه دور از طریق شبکه را برقرار می‌کنند، نیازی به رعایت این الزام نخواهند داشت.	

[۱] Remote

۹,۴ کلاس کانال‌ها/مسیرهای مورد اعتماد

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 چهار پروتکل استاندارد ایجاد می‌شوند: IPsec, TLS, 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 احراز هویت 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
۶	**کانال امن ۱**
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احرازهویت، اختصاص: [دیگر قابلیت‌ها]] 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،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.**	
۷	**کانال امن ۲**
محصول مورد ارزیابی باید اجازه داشته باشد یا به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	

شماره الزام	نام الزام
۸	**کانال امن ۳**

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

نکته کاربردی ۳۹:

هدف از الزام حاضر این است که ابزاری را برای استفاده از پروتکل رمزنگاری جهت حفاظت از ارتباطات خارجی با موجودیت‌های معتبر IT کارکرد فراهم آورد. منظور از موجودیت‌های معتبر IT موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست کم از یکی از پروتکل‌های لیست‌شده استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی ارتباط برقرار کند. اگر ارتباط با یک سرور احراز هویت (مانند RADIUS) برقرار شود، نویسنده هدف امنیتی باید عبارت «سرور احراز هویت» را در «کانال امن ۱» انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های لیست‌شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT (مانند سرور NTP) مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی را انجام دهد و موارد مناسب را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی مکانیسم یا مکانیسم‌های 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. اگر TLS انتخاب شده باشد، نویسنده هدف امنیتی به جای «الزامات پروتکلTLS Client/ احراز هویت» از «الزامات پروتکلTLS Client/ احراز هویت دستی» استفاده خواهد کرد.

هرچند که هیچ الزامی در مورد طرف آغازکننده ارتباط وجود ندارد، نویسنده هدف امنیتی در عبارت اختصاص بخش «کانال امن ۳»، خدماتی 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.

شماره الزام	نام الزام
۹	**مسیر امن ۱**
محصول، باید مسیر ارتباطی امنی که به طور منطقی از کانال‌های دیگر متمایز است را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, HTTPS] فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی 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،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.**	
۱۰	**مسیر امن ۲**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کند.	
۱۱	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه سرپرست محصول و تمام فعالیت‌های راه دور سرپرستی الزامی‌کند. نکته کاربردی ۴۰: این الزام اطمینان حاصل می‌نماید که مدیران سیستم معتبر، تمام ارتباطات از راه دور را با محصول مورد ارزیابی، 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 هدف امنیتی، مکانیسم یا مکانیسم‌های 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.	

۱۰,۴ کلاس دیواره آتش (FFW)

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

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

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

شماره الزام	نام الزام
۱۲	**فیلترینگ حالتمند ۱**
محصول، باید بر روی بسته‌های شبکه‌ای که توسط محصول پردازش می‌شود، فیلترینگ ترافیک را انجام دهد. نکته کاربردی ۴۱:	

کلاس فایروال دارای یک عنصر به نام فیلترینگ حالتمند ترافیک شبکه است که بر روی بسته‌های پردازش شده توسط محصول اعمال می‌گردد. فایروال‌های که دارای این عنصر می‌باشند اصطلاحاً فایروال‌های حالتمند نامیده می‌شوند. فایروال‌های حالتمند قادر به نگهداری و دنبال کردن وضعیت اتصالات شبکه عبوری از خود می‌باشند.
لازم به یادآوری است که محصول که بر اساس این روش کار کند، به هیچ بسته‌ای اجازه عبور نمی‌دهد مگر آنکه در مجموعه قوانین، قانونی وجود داشته باشد که اجازه عبور آن را بدهد یا آن بسته متعلق به ارتباطی باشد که قبلاً به آن اجازه عبور داده شده باشد.

۱۳	**فیلترینگ حالتمند ۲**

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

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

- IPv6
  - آدرس مبدأ
  - 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 مبدأ
  - پورت مقصد
- UDP
  - پورت مبدأ
  - پورت مقصد
- و واسطه متمایز

نکته کاربردی ۴۲:

این مؤلفه در زمان ایجاد قوانینی که توسط این الزام اجرا می‌گردند، ویژگی‌های مختلف قابل به‌کارگیری را تعریف می‌نماید. 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.

۱۴	**فیلترینگ حالتمند ۳**

محصول، باید امکان انجام عملکردهای زیر را برای هر یک از قوانین فیلترینگ حالتمند شبکه فراهم آورد: • اجازه داده (allow) • کنار گذاشتن (drop) • گزارش‌گیری (log) نکته کاربردی ۴۳: 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.
۱۵ **فیلترینگ حالتمند ۴**
محصول، باید امکان اعمال هر یک از قوانین فیلترینگ حالتمند شبکه را بر روی هر یک از واسط‌های شبکه فراهم آورد. نکته کاربردی ۴۴: این عنصر محل اعمال قوانین را مشخص می‌کند. یک محصول مطابق با این پروفایل حفاظتی، باید قادر باشد که قوانین فیلترینگ را به هریک از واسط‌های شبکه که در دسترس هستند و قابل مشخص شدن باشند و ترافیک شبکه لایه ۳ و ۴ را به کار می‌برند، اعمال نماید. قابل شناسایی به این معنی است که واسط‌ها در داخل محصول منحصربه‌فرد و قابل شناسایی است و لزوماً به واسطی که از دید شبکه قابل مشاهده باشد، اشاره ندارد (به طور مثال لازم نیست که حتماً 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 واسط‌های مشخصی اعمال شود.
۱۶ **فیلترینگ حالتمند ۵**
محصول باید:

الف) بسته‌های شبکه را بدون پردازش نمودن قوانین مربوط به فیلترینگ 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 شبکه‌ای زیر باشد:

- TCP: آدرس مبدأ و مقصد، پورت‌های مبدأ و مقصد، شماره توالی[۱]، پرچم‌ها
- UDP: آدرس مبدأ و مقصد، پورت‌های مبدأ و مقصد
- [انتخاب: *"ICMP: آدرس مبدأ و مقصد، [انتخاب: نوع، کد، [اختصاص: **فهرستی از ویژگی‌های تطبیق**]"، هیچ پروتکل دیگری*]

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

نکته کاربردی ۴۵:

این عنصر الزام می‌دارد که بر اساس چه صفت یا ویژگی از پروتکل‌ها، محصول می‌تواند وضعیت یک نشست را که مجاز به شروع شدن بوده است تعیین و مدیریت نماید. هم‌چنین این الزام صفات عملی که برای تطابق و تعیین نشست شروع شده با بسته‌های شبکه مورد استفاده قرار می‌گیرند را مشخص می‌نماید.

چنانچه ICMP به عنوان پروتکل انتخاب گردد، آدرس مبدأ و آدرس مقصد برای تعیین متعلق بودن یک بسته به ارتباط شروع شده قبلی مورد استفاده قرار می‌گیرد. 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 می‌آورد تا صفات دیگری برای پیاده‌سازی 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.

[۱] Sequence number

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 است.

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

۱۷	**فیلترینگ حالتمند ۶**

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

۱- محصول باید بسته‌های اطلاعاتی را که به صورت نامعتبر قطعه‌بندی شده‌اند رد نماید و قادر به [انتخاب: شمردن، ثبت] آن‌ها باشد.

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

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

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

۵- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ 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.

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

۶- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد نماید و قادر به ثبت باشد که آدرس مبدأ و مقصد بسته اطلاعاتی به صورت آدرس «نامشخص» یا آدرسی که «رزرو شده برای تعریف و استفاده در آیند» (به عنوان نمونه آدرس‌های تک‌پخشی 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 گزینه‌های IP زیر را رد نماید و قادر به ثبت باشد:

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

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

۱۸	**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 مبدأ 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 مبدأ 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 مبدأ آن متعلق به شبکه‌های مرتبط با واسط شبکه‌ای که آن بسته‌ها را دریافت کرده است، نباشد را کنار بگذارد و قادر به ثبت باشد.

۱۹	**فیلترینگ حالتمند ۸**

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

۲۰	**فیلترینگ حالتمند ۹**

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

۲۱	**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 می‌رسد، اتصالات جدید باید حذف و رویداد حذف شده باید [انتخاب: شمرده، ثبت] شود.

۵ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

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

۱,۵ کلاس توسعه

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

۱,۱,۵ مشخصات کارکردی

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:**

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

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط 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:**

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

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	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.

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.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	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»، «آزمون» و «آسیب‌پذیری» ارائه شده است.

۲,۵ کلاس راهنمای کاربر

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

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

دستورالعمل نصب موفقیت‌آمیز محصول در محیط

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

دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۱,۲,۵ راهنمای کاربردی

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

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

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

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

۲,۲,۵ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

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

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

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.

۳,۵ کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از

طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای محصول در نظر گرفته شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۱,۳,۵ آزمون مستقل

«آزمون 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 آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی است. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

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

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

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

۴,۵ کلاس آسیب‌پذیری

۱,۴,۵ تحلیل آسیب‌پذیری

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

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

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

۵,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۱,۵,۵ قابلیت‌های پیکربندی

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

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

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

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

۲,۵,۵ حوزه پیکربندی

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	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).

۱,۶ کلاس ممیزی امنیت

درصورتی‌که در محصول مورد ارزیابی فضای حافظه محلی برای داده‌های ممیزی در نظر گرفته شده باشد، محصول مورد ارزیابی می‌تواند ادعا کند که مطابق آنچه در «ذخیره‌سازی رویدادهای ممیزی» گفته شده است، از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری به عمل آورد. فضای حافظه محلی دستگاه‌های شبکه برای ذخیره‌سازی داده‌های ممیزی، محدود است. اگر این حافظه پر شود، امکان از دست رفتن داده‌های ممیزی وجود خواهد داشت. ممکن است یک سرپرست محصول بخواهد اطلاعات مربوط به تعداد داده‌های ممیزی ازدست‌رفته را داشته باشد. این تعداد می‌تواند نشان‌دهنده مشکلات سرور باشد؛ بنابراین، «محل ذخیره‌سازی داده‌های ممیزی» و «محل ذخیره‌سازی داده‌های ممیزی» تهیه شده‌اند تا این قابلیت‌های اختیاری دستگاه‌های شبکه را بیان کنند.
همچنین جدول زیر مربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب است. همان‌طور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۱	محل ذخیره‌سازی داده‌های ممیزی	نگرانی درباره کمبود فضای حافظه برای رویدادهای ممیزی	
۲	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی	تغییر و تصحیح رفتار در انتقال داده‌های ممیزی به یک موجودیت IT خارجی	

۳	مدیریت کارکرد در محصول ۱ (۲)/ ممیزی	تغییر و تصحیح رفتار در مدیریت داده‌های ممیزی	
۴	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی	تغییر و تصحیح رفتار محصول	
۵	مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی	شروع و پایان خدمت	
۶	مدیریت کارکرد در محصول ۱ / فضای ذخیره‌سازی ممیزی محلی	تغییر و تصحیح رفتار کارکرد ممیزی هنگامی که حافظه ممیزی کم است	
۷	مدیریت داده‌های محصول ۱/ اقدامات مدیریتی	تغییر و تصحیح، حذف، تولید/ ورود کلیدهای رمزنگاری شده	

شماره الزام	نام الزام
۲۲	محل ذخیره‌سازی داده‌های ممیزی ۱
محصول مورد ارزیابی باید از پاک شدن غیرمجاز داده‌های ممیزی جلوگیری نماید.	
۲۳	محل ذخیره‌سازی داده‌های ممیزی ۲
محصول مورد ارزیابی باید از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری نماید.	
۲۴	محل ذخیره‌سازی داده‌های ممیزی ۳
محصول مورد ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده‌های ممیزی [انتخاب: از بین رفته، بازنویسی شده، [اختصاص: سایر اطلاعات]] را ارائه کند. محصول مورد ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده‌های ممیزی ۳» را انجام می‌دهد. نکته کاربردی ۴۶: این گزینه در صورتی باید انتخاب شود که محصول مورد ارزیابی از این کارکرد پشتیبانی کند. درصورتی‌که حافظه محلی داده‌های ممیزی توسط سرپرست محصول خالی شود، شمارنده‌های مربوط به انتخاب انجام‌شده باید به مقادیر اولیه خود برگردند (این مقدار در اکثر موارد صفر است). اسناد راهنما باید به سرپرست محصول هشدار دهند که خالی کردن حافظه ممکن است سبب از دست رفتن داده‌ها شود.	
۲۵	محل ذخیره‌سازی داده‌های ممیزی ۴

محصول مورد ارزیابی باید در هنگام نیاز به کاربر هشدار دهد که حافظه ذخیره‌سازی داده‌های ممیزی در حال اتمام است و/یا محصول، داده‌های ممیزی را در اثر کم بودن حافظه ذخیره‌سازی از دست خواهد داد.

نکته کاربردی ۴۷:
درصورتی‌که محصول مورد ارزیابی امکان تولید پیام مربوطه را داشته باشد این گزینه انتخاب می‌شود. درصورتی‌که داده‌های مربوط به رویدادهای قابل‌ممیزی تنها در حافظه محلی ذخیره شده باشند، این هشدار می‌تواند اهمیت بسیار زیادی داشته باشد.
باید اطمینان حاصل نمود که هشدار مورداشاره در «محل ذخیره‌سازی داده‌های ممیزی ۳» را می‌توان به اطلاع کاربر رساند. ارتباط باید از طریق سوابق ممیزی صورت گیرد، زیرا ممکن است در هنگام رخ دادن اتفاق، نشست فعالی برای مدیریت این کار وجود نداشته باشد.

۲،۴ کلاس مدیریت امنیت

شماره الزام	نام الزام
۲۶	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی
محصول مورد ارزیابی باید امکان تعیین یا تغییر رفتار در مورد انتقال داده‌های ممیزی به یک موجودیت IT خارجی را به سرپرست محصول محدود کند. نکته کاربردی ۴۸: اگر پروتکل انتقال داده‌های ممیزی به یک موجودیت IT خارجی بر طبق «محل ذخیره‌سازی داده‌های ممیزی ۱» قابل پیکربندی باشد، باید همواره FMT_MOF.1(1)/Audit را انتخاب کرد.	
۲۷	مدیریت کارکرد در محصول ۱ (۲)/ ممیزی
محصول مورد ارزیابی باید امکان تعیین یا تغییر رفتار در مورد مدیریت داده‌های ممیزی را به سرپرست محصول محدود کند. نکته کاربردی ۴۹: این الزام تنها در صورتی باید انتخاب شود که مدیریت داده‌های ممیزی، قابل پیکربندی باشند. عبارت «مدیریت داده‌های ممیزی» به گزینه‌های مختلف «انتخاب» و «اختصاص» در «محل ذخیره‌سازی داده‌های ممیزی ۲» و «محل ذخیره‌سازی داده‌های ممیزی ۳» و «محل ذخیره‌سازی داده‌های ممیزی» اشاره دارد.	
۲۸	مدیریت کارکرد در محصول ۱ (۱)/ اقدامات مدیریتی
محصول مورد ارزیابی باید امکان تغییر رفتار در مورد ارائه خدمات امنیتی محصول را به سرپرست محصول محدود کند. نکته کاربردی ۵۰: این الزام تنها در صورتی باید انتخاب شود که رفتار محصول در زمینه ارائه خدمات امنیتی، قابل پیکربندی باشد.	

۲۹	مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی
محصول مورد ارزیابی باید امکان فعال و غیرفعال کردن توابع «ارائه خدمات» را به سرپرست محصول محدود کند. نکته کاربردی ۵۱: «مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی» تنها در صورتی باید انتخاب شود که سرپرست محصول امکان شروع و متوقف کردن خدمات را داشته باشد.	
۳۰	مدیریت کارکرد در محصول ۱ (۱)/ فضای ذخیره‌سازی ممیزی محلی
محصول مورد ارزیابی باید امکان تعیین و تغییر رفتار در مورد کارکرد ممیزی در هنگام پر شدن حافظه محلی داده‌های ممیزی را به سرپرست محصول محدود کند. نکته کاربردی ۵۲: این الزام تنها در صورتی باید انتخاب شود که رفتار «کارکرد ممیزی در هنگام پر شدن حافظه محلی داده‌های ممیزی»، قابل پیکربندی باشد.	
۳۱	مدیریت داده‌های محصول ۱/ اقدامات مدیریتی
محصول مورد ارزیابی باید امکان تغییر، پاک کردن، تولید کردن و وارد کردن کلیدهای رمزنگاری را به سرپرست محصول محدود کند. نکته کاربردی ۵۳: این الزام تنها در صورتی باید انتخاب شود که کلیدهای رمزنگاری قابل تغییر، پاک کردن، تولید کردن و وارد کردن توسط سرپرست محصول باشند.	

۲,۶ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام
۳۲	حفظ وضعیت امن در زمان شکست ۱/ فضای ذخیره‌سازی ممیزی محلی
محصول مورد ارزیابی باید به‌هنگام شکست به‌دلیل «پر شدن حافظه محلی داده‌های ممیزی»، در حالت کارکرد امن باقی بماند. نکته کاربردی ۵۴: اگر محصول مورد ارزیابی به گونه‌ای پیکربندی شده باشد که در صورت عدم وجود هیچ حافظه دیگری برای ذخیره کردن داده‌های ممیزی، تمام کارکردهای امنیتی را متوقف کند (در حالت کارکرد امن باقی بماند)، این الزام را باید به محصول مورد ارزیابی اضافه کرد. بدین ترتیب، مهاجم نمی‌تواند داده‌های ممیزی دیگری را تولید کند و اقدامات خود را پنهان نماید. انتظار می‌رود که این رفتار در بخش «گزینه‌های دیگر»). مربوط به الزام «محل ذخیره‌سازی داده‌های ممیزی ۳» مدل‌سازی شود (در بخش «اختصاص» موجود در «انتخاب»).	

۳,۶ کلاس دیواره آتش (FFW)

شماره الزام	نام الزام
۳۳	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 می‌کنند ایجاد کند.

نکته کاربردی ۵۵:

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

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

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

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

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

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

[۱] rulset

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

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۱	الزامات پروتکل HTTPS	شکست در ایجاد یک نشست HTTPS	دلایل شکست
۲	الزامات پروتکل IPSEC	شکست در ایجاد یک SA مربوط به پروتکل IPSEC	دلایل شکست
۳	الزامات پروتکل SSH Client	شکست در ایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۴	الزامات پروتکلSSH Server	شکست در ایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۵	الزامات پروتکلTLS Client/ احراز هویت	شکست در ایجاد یک نشست TLS	دلایل شکست

۶	الزامات پروتکلTLS Client/ احراز هویت دو طرفه	شکست در ایجاد یک نشست TLS	دلایل شکست
۷	الزامات پروتکلTLS Server/ احراز هویت	شکست در ایجاد یک نشست TLS	دلایل شکست
۸	الزامات پروتکلTLS Server/ احراز هویت دو طرفه	شکست در ایجاد یک نشست TLS	دلایل شکست
۹	خودآزمایی محصول مورد ارزیابی۲	شکست در خودآزمایی	دلایل شکست (شامل شناساگر گواهینامه‌های غیر معتبر)
۱۰	الزامات به‌روزرسانی امن	شکست در به‌روزرسانی	دلایل شکست (شامل شناساگر گواهینامه‌های غیر معتبر)
۱۱	مدیریت کارکرد در محصول ۱ (۲)/ به‌روزرسانی امن	فعال‌سازی و غیر فعال‌سازی جستجوی خودکار به‌روزرسانی یا بروز رسانی خودکار	

۱,۷ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۳۴	الزامات پروتکل HTTPS (۱)
محصول مورد ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را اجرا کنند. نکته کاربردی ۵۶: نویسنده ST باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان عناصری را به این مؤلفه افزود یا اطلاعاتی را به خلاصه مشخصات محصول (فصل آخر سند ST) اضافه کرد.	
۳۵	الزامات پروتکل HTTPS (۲)
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۳۶	الزامات پروتکل HTTPS (۳)
درصورتی‌که گواهی‌نامه همتا[۱] نامعتبر باشد، محصول مورد ارزیابی باید [انتخاب: اتصال را برقرار ننماید، برای برقراری اتصال درخواست احراز هویت نماید، هیچ اقدام دیگری انجام ندهد]. نکته کاربردی ۵۷: اعتبار بر اساس مسیر گواهی‌نامه، تاریخ انقضا و وضعیت لغو بر اساس RFC 5280 تعیین می‌شود.	

[۱] peer certificate

۲,۷ 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 غیرقابل اعتماد دیگر بگذرد. کارکرد امنیتی دستگاه شبکه باید این قابلیت را داشته باشد که از ترافیک حساس منتقل‌شده حفاظت نماید (مانند ترافیک سرپرست محصول، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست). یکی از راه‌های ایجاد کانال ارتباطی بین دستگاه شبکه و یک موجودیت ITخارجی، به گونه‌ای که این ارتباط را بتوان از هر دو طرف احراز هویت کرد، استفاده از IPsec است.

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

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

شماره الزام	نام الزام
۳۷	الزامات پروتکل IPSEC (۱)
در محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آنچه در RFC 4301 مشخص شده است، پیاده‌سازی شود. نکته کاربردی ۵۲: بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه داده 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- «BBYPASS» از سرویس IPSEC (مثلاً عدم رمزگذاری) ۳- «DISCARD» بسته (مثلاً دور ریختن بسته). پایگاه داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به فهرست‌های کنترل دسترسی به مسیریاب، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف‌نظر از روشی که به کار گرفته می‌شود، قوانینی وجود دارند که بسته‌ها باید از آن‌ها پیروی کنند و اقدامات باید بر اساس آن‌ها انجام شوند. باید ابزارهایی برای تنظیم این قوانین وجود داشته باشند، اما رویکردی عمومی و کلی در این زمینه وجود ندارد. قاعده کلی این است که SPD باید بتواند بسته‌های IP را از یکدیگر تمایز دهد و قوانین مربوطه را در مورد آن‌ها اعمال نماید. ممکن است چند SPD وجود داشته باشند (یک پایگاه داده برای هر واسط شبکه)، اما الزامی در این زمینه وجود ندارد.	
۳۸	الزامات پروتکل IPSEC (۲)
محصول مورد ارزیابی باید خط و مشی در پایگاه داده SPD داشته باشد که تمام موارد غیر منطبق را دور بریزد.	
۳۹	الزامات پروتکل IPSEC (۳)
محصول مورد ارزیابی باید مد انتقال و [انتخاب: مد تونل، هیچ مد دیگر] پیاده‌سازی کند.	

۴۰	الزامات پروتکل IPSEC (۴)

محصول مورد ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است چارچوب ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری AES-CBC-128, AES-CBC-256 و [انتخاب: AES-GCM-128، AES-GCM-256، هیچ الگوریتم دیگر] و همچنین الگوریتم درهم سازی امن (SHA) مبتنی بر HMAC، پیاده‌سازی کند.

الگوریتم‌های رمزنگاری AES-CBC-128, AES-CBC-256 در RFC 3602 تشریح شده‌اند. همچنین AES-GCM-128 و AES-GCM-256 در RFC 4106 تشریح شده‌اند.)

۴۱	الزامات پروتکل IPSEC (۵)

محصول مورد ارزیابی باید یکی از این پروتکل‌ها را به کار گیرد: [انتخاب:

- IKEv1، با استفاده از مد اصلی برای انتقال در فاز اول، طبق آنچه در RFC 4109, RFCs 2407,2408,2409، [انتخاب: هیچ RFC دیگر برای اعداد متوالی بسط‌یافته، RFC4304 برای اعداد متوالی بسط‌یافته] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز]

- IKEv2، مطابق با آنچه در RFC 5996 تشریح شده است و [انتخاب: بدون پشتیبانی از پیمایش NAT[۱]، 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 ۵۳:

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.

[۱] NAT traversal

۴۲	الزامات پروتکل IPSEC (۶)
محصول مورد ارزیابی باید اطمینان حاصل کند که برای رمزگذاری پی آیند[۱] در [انتخاب: IKEv2،IKEv1]، از الگوریتم‌های رمزنگاری AES-CBC-128 و AES-CBC-256 (طبق آنچه در RFC 3602 تشریح شده است) و [انتخاب: AES-GCM-128, AES-GCM-256 مطابق آنچه درRFC 5282 تشریح شده است، هیچ الگوریتم دیگر] استفاده شده است. نکته کاربردی ۵۴: AES-GCM-128 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.	
۴۳	الزامات پروتکل IPSEC (۷)

[۱] Payload

	محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب: • سرپرست محصول می‌تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.] پیکربندی کند. • سرپرست محصول می‌تواند طول عمر IKEv2 SA را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.] پیکربندی کند. نکته کاربردی ۵۵: نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در «الزامات پروتکل IPSEC (۵)» 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). به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در اسناد راهنمای تولیدشده برای سند شرح محصول گنجاند.
۴۴	الزامات پروتکل IPSEC (۸)

محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب: • سرپرست محصول می‌تواند طول عمر SA فاز دوم IKEv1 را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.] پیکربندی کند. • سرپرست محصول می‌تواند طول عمر IKEv2 Child SA را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.] پیکربندی کند. نکته کاربردی ۵۶: نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در «الزامات پروتکل IPSEC (۵)» 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). به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SAرا باید در اسناد راهنمای تولیدشده برای سند شرح محصول گنجاند.	
۴۵	الزامات پروتکل IPSEC (۹)

محصول باید مقدار x را که در تبادل کلید IKE DiffieHellman (x در $g^x \bmod p$) به کار می‌رود، با استفاده از تولیدکننده بیت تصادفی که در FCS_RBG_EXT.1 مشخص شده است و دست‌کم طول آن [اختصاص: تعداد بیت‌های (یک یا بیش از یک) باشد که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره‌شده باشد] تولید نماید. نکته کاربردی۵۷: از آنجایی که در پیاده‌سازی ممکن است گروه‌های مختلف Diffie-Hellman در مذاکره برای استفاده در SA مجاز باشند الزام «الزامات پروتکل IPSEC (۹)» می‌تواند مقادیر متعددی داشته باشند. 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.	
۴۶	الزامات پروتکل IPSEC (۱۰)

محصول 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 کاربردی۵۸: 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 «الزامات پروتکل IPSEC (۱۰)» 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.	
۴۷	الزامات پروتکل IPSEC (۱۱)
محصول باید اطمینان حاصل نماید که همه پروتکل‌های IKE، گروه‌های DH ۱۴ (2048-bit MODP) و [انتخاب: گروه ۱۹ (2048-bit Random ECP)، گروه ۵ (1536-bit MODP)، گروه ۲۴ (2048-bit MODP به همراه 256-bit POS)، گروه ۲۰ (384-bit Random ECP)، [اختصاص: سایر گروه‌های DH که توسط محصول پیاده‌سازی می‌شوند]، هیچ گروه DH دیگری] را پشتیبانی می‌کنند.	
۴۸	الزامات پروتکل IPSEC (۱۲)

محصول باید به صورت پیش‌فرض بتواند اطمینان حاصل نماید که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [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 کاربردی۵۹: نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند.

۴۹	الزامات پروتکل IPSEC (۱۳)
محصول 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.	
۵۰	الزامات پروتکل IPSEC (۱۴)
محصول باید کانال امن را فقط با همتاهای دارای گواهی معتبر برقرار سازد.	

۳,۷ الزامات پروتکل SSH Client

شماره الزام	نام الزام
۵۱	الزامات پروتکل SSH Client (۱)
محصول باید پروتکل SSH را مطابق با RFC های 4251، 4252، 4253، 4254 و [انتخاب: RFC های 5647، 5656، 6187، 6668، هیچ RFC دیگری] پیاده‌سازی نماید. نکته کاربردی ۶۰:	

نویسندهST انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد.	
۵۲	الزامات پروتکل SSH Client (۲)
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه در RFC4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر کلمه عبور.	
۵۳	الزامات پروتکل SSH Client (۳)
همان طور که در RFC4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH کنار گذاشته شوند. نکته کاربردی۶۱: 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.	
۵۴	الزامات پروتکل SSH Client (۴)
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری: aes256-cbc,aes128-cbc, [انتخابAEAD_AES_256_GCM AEAD_AES_128_GCM, هیچ الگوریتم رمزنگاری دیگری] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
۵۵	الزامات پروتکل SSH Client (۵)

محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند.	
۵۶	الزامات پروتکل SSH Client (۶)
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] و [انتخاب:AEAD_AES_128_GCM, AEAD_AES_256_GCM، هیچ الگوریتمMAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
۵۷	الزامات پروتکل SSH Client (۷)
محصول باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, ecdh-sha2-nistp256] و [انتخاب: ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۵۸	الزامات پروتکل SSH Client (۸)
محصول باید اطمینان حاصل نماید که کلید اتصال SSH حتماً بعد از ارسال تعداد$\overline{2^{28}}$ بسته با آن کلید، تجدید شود.	
۵۹	الزامات پروتکل SSH Client (۹)
محصول 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 کاربردی۶۲: تنها در صورتی می‌توان گزینه «لیست مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256 یا x509v3-ecdsa-sha2-nistp384 در «الزامات پروتکل SSH Client (۵)» انتخاب‌شده باشد.	

۴,۷ الزامات پروتکلSSH Server

شماره الزام	نام الزام
۶۰	الزامات پروتکلSSH Server (۱)
محصول باید پروتکل SSH مطابق با RFC های 4251، 4252، 4253، 4254 و [انتخاب: RFC های 5647، 5656، 6187، 6668، هیچ RFC دیگری] را پیاده‌سازی نماید. نکته کاربردی۶۳: نویسندهST انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد.	
۶۱	الزامات پروتکلSSH Server (۲)
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC4252 توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر کلمه عبور.	
۶۲	الزامات پروتکلSSH Server (۳)
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 کاربردی۶۴:	

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.	
الزامات پروتکلSSH Server (۴)	**۶۳**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری: aes256-cbc,aes128-cbc, [انتخابAEAD_AES_256_GCM AEAD_AES_128_GCM, هیچ الگوریتم رمزنگاری دیگری] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
الزامات پروتکلSSH Server (۵)	**۶۴**
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند.	
الزامات پروتکلSSH Server (۶)	**۶۵**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] و [انتخاب:AEAD_AES_128_GCM, AEAD_AES_256_GCM، هیچ الگوریتمMAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
الزامات پروتکلSSH Server (۷)	**۶۶**
محصول باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, ecdh-sha2-nistp256] و [انتخاب:	

ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۶۷	الزامات پروتکلSSH Server (۸)
محصول باید اطمینان حاصل نماید که کلید اتصال SSH حتماً تا قبل از پایان ارسال تعداد$2^{\overline{28}}$ بسته با آن کلید، تجدید شود.	

۵,۷ الزامات پروتکلTLS Client/ احراز هویت

شماره الزام	نام الزام
۶۸	الزامات پروتکلTLS Client/ احراز هویت ۱
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: • [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] • [انتخاب: مجموعه‌های رمز اختیاری: o LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o 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_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_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

- هیچ مجموعه رمز دیگری]].

نکته کاربردی ۶۵:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند.

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.

۶۹	الزامات پروتکلTLS Client/ احراز هویت ۲
محصول باید تأیید نماید که با توجه به RFC 6125، شناسه[۱] ارائه‌شده با شناسه مرجع مطابقت داشته باشد. نکته کاربردی۶۶: قوانین مربوط به تأیید شناسه در بخش ۶ از RFC 6125 توضیح داده‌شده‌اند. شناسه مرجع توسط کاربر (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 قسمتName 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.	
۷۰	الزامات پروتکلTLS Client/ احراز هویت ۳
محصول باید کانال امن را فقط در صورتی برقرار سازد که گواهی همتا معتبر باشد. نکته کاربردی۶۷: اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC5280 تعیین می‌گردد. اعتبار گواهی بر اساس «الزامات پروتکل X509» آزموده می‌شود.	
۷۱	الزامات پروتکلTLS Client/ احراز هویت ۴

[۱] identifier

محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب:secp256r1, secp384r1, secp521r1 , یا هیچ گزینه دیگری] در پیام ClientHello ارائه دهد. نکته کاربردی۶۸: اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» مجموعه‌های رمز بیضوی انتخاب‌شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است. اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز بیضوی انتخاب‌نشده باشند، هیچ‌کدام از منحنی‌ها نباید انتخاب شوند. این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های «عملیات رمزنگاری» و «مدیریت کلید رمزنگاری ۱» و «مدیریت کلید رمزنگاری ۲» محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۶,۷ الزامات پروتکلTLS Client همراه با احراز هویت دوطرفه

شماره الزام	نام الزام
۷۲	الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۱
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: • [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] • [انتخاب: مجموعه‌های رمز اختیاری: o LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o 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_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_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

- هیچ مجموعه رمز دیگری]].

نکته کاربردی۶۹:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند.

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
۷۳	الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۲
محصول باید تأیید نماید که با توجه به RFC 6125، شناسه[۱] ارائه‌شده با شناسه مرجع مطابقت داشته باشد. نکته کاربردی ۷۰: قوانین مربوط به تأیید شناسه در بخش ۶ از RFC 6125 توضیح داده‌شده‌اند. شناسه مرجع توسط کاربر (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 قسمتName 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.	
۷۴	الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۳
محصول باید کانال امن را فقط در صورتی برقرار سازد که گواهی همتا معتبر باشد. نکته کاربردی ۷۱:	

[۱] identifier

اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC5280 تعیین می‌گردد. اعتبار گواهی بر اساس «الزامات پروتکل X509» آزموده می‌شود.	
الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۴	**۷۵**
محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب:secp256r1, secp384r1, secp521r1 , یا هیچ گزینه دیگری] در پیام ClientHello ارائه دهد. نکته کاربردی۷۲: اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» مجموعه‌های رمز بیضوی انتخاب‌شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است. اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز بیضوی انتخاب‌نشده باشند، هیچ‌کدام از منحنی‌ها نباید انتخاب شوند. این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های «عملیات رمزنگاری» و «مدیریت کلید رمزنگاری ۱» و «مدیریت کلید رمزنگاری ۲» محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.	
الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۵	**۷۶**
محصول باید با استفاده از گواهینامه X.509v3، از احراز هویت دوطرفه پشتیبانی نماید. نکته کاربردی۷۳: استفاده از گواهی‌های نسخه سوم X.509 برای محصول در «الزامات پروتکل X509 (۳)» توضیح داده‌شده است. با توجه به این الزام، کاربر حتماً قابلیت ارائه گواهی به سرور TLS به‌منظور احراز هویت دو طرفه را داشته باشد.	

۷,۷ الزامات پروتکلTLS Server

شماره الزام	نام الزام
۷۷	الزامات پروتکلTLS Server/ احراز هویت ۱
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: • [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] • [انتخاب: مجموعه‌های رمز اختیاری: o LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492 o TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246 o TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246	

o TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289 • هیچ مجموعه رمز دیگری]]. نکته کاربردی۷۴: مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
الزامات پروتکلTLS Server/ احراز هویت ۲	**۷۸**
محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، TLS1.2، هیچ‌کدام] دارند، رد نماید. نکته کاربردی۷۵:	

تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در «الزامات پروتکلTLS Server/ احراز هویت ۱» انتخاب‌نشده است، در اینجا انتخاب شود.

۷۹	الزامات پروتکلTLS Server/ احراز هویت ۳

محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری]، [انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید. نکته کاربردی۷۶: اگر در بخش «الزامات پروتکلTLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهایDHE یا ECDHE لیست شده باشند، سند ST باید شامل Diffie-Hellman یا منحنی‌هایNIST لیست شده در این الزام باشد.

۸,۷ الزامات پروتکلTLS Server همراه با احراز هویت دو طرفه

شماره الزام	نام الزام
۸۰	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۱

محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:

- مجموعه‌های رمز اجباری:
- [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268]
- [انتخاب: مجموعه‌های رمز اختیاری:

- LS_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_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_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

- هیچ مجموعه رمز دیگری]].

نکته کاربردی۷۷:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
۸۱	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۲
محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، TLS1.2، هیچ‌کدام] دارند، رد نماید. نکته کاربردی۷۸: تمام نسخه‌های SSL و نسخه ۱,۰ TLS رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در «الزامات پروتکلTLS Server احراز هویت دستی ۴» انتخاب‌نشده است، در اینجا انتخاب شود.	
۸۲	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۳
محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری]، [انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید. نکته کاربردی۷۹: اگر در بخش «الزامات پروتکلTLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهایDHE یا ECDHE لیست شده باشند، سند ST باید شامل Diffie-Hellman یا منحنی‌هایNIST لیست شده در این الزام باشد.	
۸۳	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۴

محصول باید با استفاده از گواهینامه‌های X.509v3 احراز هویت دو طرفه کلاینت TLS را پشتیبانی نماید. نکته کاربردی ۸۰: استفاده از گواهی‌های نسخه سوم X.509 برای محصول در «الزامات پروتکل X509 (۳)» توضیح داده‌شده است. در کنار این الزام، باید در این استفاده گواهی‌های کلاینت نیز برای احراز هویت مشترک پشتیبانی شوند.	
۸۴	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۵
درصورتی‌که گواهی همتا معتبر نباشد، محصول نباید کانال امن را برقرار سازد. نکته کاربردی ۸۱: اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC5280 تعیین می‌گردد. اعتبار گواهی بر اساس «الزامات پروتکل X509» آزموده می‌شود.	
۸۵	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۶
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 برقرار سازد. نکته کاربردی ۸۲: ممکن است شناسه همتا در قسمت Subject یا Alternative Name Extention از گواهینامه باشد. شناسه مورد انتظار ممکن است پیکربندی شود، با Domain Name، آدرس IP، نام کاربری یا آدرس ایمیل استفاده‌شده توسط همتا مقایسه شود یا به‌منظور مقایسه به یک سرور دایرکتوری ارسال شود. برای این منظور مقایسه بیتی انجام می‌شود.	

[۱] distinguished name

[۲] Subject Alternative Name

۹,۷ الزامات خودآزمایی محصول مورد ارزیابی

شماره الزام	نام الزام
۸۶	خودآزمایی محصول مورد ارزیابی۲
اگر برای آزمون‌های خودآزمایی از یک گواهینامه استفاده شود و آن گواهینامه غیر معتبر اعلام‌شده باشد، محصول باید در آزمون خودآزمایی ناموفق باشد. نکته کاربردی۸۳: گواهینامه‌ها را می‌توان به‌صورت اختیاری برای آزمون‌های خودآزمایی استفاده کرد (خودآزمایی محصول۱). اگر برای آزمون‌های خودآزمایی از گواهینامه‌ها استفاده شود، سند هدف امنیتی باید شامل این مورد باشد. اگر در «الزامات پروتکل X509 (۳)» «امضای کدها برای تأیید صحت» انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی۲» باشد. اعتبار به‌وسیله مسیر گواهینامه، تاریخ انقضاء و وضعیت ابطال مطابق با «الزامات پروتکل X509» تعیین می‌گردد.	

۱۰,۷ الزامات به‌روزرسانی امن

شماره الزام	نام الزام

۸۷	الزامات به‌روزرسانی امن ۴
درصورتی‌که گواهینامه امضای کد آن غیر معتبر اعلام‌شده است، محصول نباید یک به‌روزرسانی را نصب نماید.	
۸۸	الزامات به‌روزرسانی امن ۵
هنگامی‌که گواهینامه به علت انقضای آن، غیر معتبر اعلام‌شده است، محصول باید [انتخاب: اجازه بدهد که در این موارد سرپرست محصول در موردپذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد]. نکته کاربردی۸۴: گواهینامه‌ها را می‌توان به‌صورت اختیاری برای امضای کدها در به‌روزرسانی‌های نرم‌افزار سیستم استفاده کرد (الزامات به‌روزرسانی امن ۳). اگر برای اعتبارسنجی به‌روزرسانی‌ها از گواهینامه‌ها استفاده شود، سند هدف امنیتی باید شامل این مورد بشود. اگر در «الزامات پروتکل X509 (۳)» «امضای کدها برای به‌روزرسانی‌های نرم‌افزار سیستم» انتخاب‌شده باشد، سند هدف امنیتی باید شامل «الزامات به‌روزرسانی امن» باشد. اعتبار به‌وسیله مسیر گواهینامه، تاریخ انقضاء و وضعیت ابطال مطابق با «الزامات پروتکل X509» تعیین می‌گردد. برای گواهینامه‌های منقضی، نویسنده هدف امنیتی انتخاب می‌کند که گواهینامه پذیرفته شود، رد شود یا تصمیم‌گیری در خصوص پذیرش یا رد گواهینامه به سرپرست محصول واگذار شود.	
۸۹	مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/ به‌روزرسانی امن
محصول باید قابلیت فعال‌سازی و غیر فعال‌سازی کارکردهای [انتخاب: جستجو برای به‌روزرسانی خودکار، به‌روزرسانی خودکار]را برای سرپرست محصول فراهم آورد. نکته کاربردی۸۵:	

این الزام تنها زمانی قابل پیاده‌سازی است که محصول امکان پشتیبانی از به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیر فعال‌سازی این قابلیت را بدهد. فعال‌سازی و غیر فعال‌سازی قابلیت به‌روزرسانی خودکار به سرپرست محصول محدود می‌شود.